ISSN 2707-1898 (print)
Український журнал інформаційних технологій
Ukrainian Journal of Information Technology
http://science.lpnu.ua/uk/ujit
https://doi.org/10.23939/ujit2023.02.060
Article received 21.09.2023 p.
Article accepted 26.10.2023 p.
UDK 004.75/.62
Correspondence author
N. S. Cherkas
nazarii.s.cherkas@lpnu.ua

УДК 004.75/.62

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

ЯВИЩЕ MAXIMAL EXTRACTABLE VALUE (MEV) В МЕРЕЖАХ БЛОКЧЕЙН ТА ЙОГО ВПЛИВ НА БЛОКЧЕЙН ЕКОСИСТЕМУ

З появою технології смарт-контрактів у мережах блокчейн уможливилась реалізація складних протоколів децентралізованих фінансів, які з часом набули значної популярності та досягли показника Total Value Locked (TVL) понад 150 мільярдів доларів США. Мережі блокчейн, надаючи такі гарантії, як незмінність, відкритість, децентралізованість та безпека, все ж не здатні забезпечити прогнозовану послідовність транзакцій у вихідних блоках, що стало причиною появи явища Maximal Extractable Value (MEV) – максимальної "екстрактованої" вигоди, доступної певним учасникам мережі (майнерам, валідаторам), які мають ексклюзивну можливість впливати на впорядкування транзакцій. У цій роботі виконано ґрунтовний огляд явища MEV та з'ясовано його вплив на екосистему мереж блокчейн. Окреслено безпосередню проблему прогнозованої послідовності транзакцій у мережах блокчейн, наведено огляд численних наукових публікацій за темою екстракції MEV, що дало змогу здійснити ретроспективний аналіз цього явища, систематизувати його найпоширеніші прояви та проаналізувати сучасні тенденції розвитку.

У ході ретроспективного аналізу виявлено паралелі зі схожими маніпуляціями в галузі високочастотної алгоритмізованої торгівлі на класичних фінансових майданчиках та зроблено важливий висновок щодо напряму вирішення проблеми MEV у протоколах децентралізованих фінансів. Систематизовано напрями сучасних досліджень явища MEV, проаналізовано методи та засоби досліджень, а також наведено безпосередні приклади екстракції MEV в мережі Ethereum з наявними оцінками її масштабів.

У підсумку виділено переважання негативного впливу явища MEV на мережі блокчейн і децентралізовані фінанси та на основі аналізу окремої підкатегорії наявних публікацій виявлено, що все ще не запропоновано ефективного вирішення проблеми екстракції MEV. Це зумовлює актуальність подальших досліджень у напрямі подолання негативних впливів MEV на мережі блокчейн та протоколи децентралізованих фінансів.

Ключові слова: блокчейн; смарт-контракти; розподілені системи; однорангові мережі; криптографія.

Вступ / Introduction

Поява технології смарт-контрактів, зокрема бурхливе її поширення в мережі Ethereum, уможливило реалізацію алгоритмів фінансових послуг у мережах блокчейн. Смарт-контракти являють собою програмні компоненти, код яких зберігається в мережі блокчейн та процедури якого можуть викликати учасники мережі або напряму інші смарт-контракти. Окрім того, смарт-контракти мають певний стан, який оновлюється після відпрацювання коду смарт-контракту та є незмінним – попередні зміни стану неможливо перезаписати.

Смарт-контракти реалізуються засобами мови програмування, яка дає змогу описати всю необхідну логіку виконання. Однією із найпопулярніших мов програмування смарт-контрактів є Solidity, в деяких мережах блокчейн також можна використовувати JavaScript, Rust та Python.

Будь-які зміни стану смарт-контрактів здійснюються в атомарний спосіб – або виконуються повністю в межах транзакції, або повністю відкочуються. Як тільки транзакція, яка викликає смарт-контракт, отримує підтвердження мережі, його код запускається всіма вузлами мережі блокчейн, забезпечуючи фіксацію зміни стану кожним з учасників мережі. Це зумовлює узгодження стану між всіма вузлами мережі. Вартість ресурсів (процесорний час, пам'ять), витрачених на виконання коду смарт-контракту, автоматично оплачує учасник мережі, який ініціював запуск коду та надіслав транзакцію. Ці та інші можливості смарт-контрактів забезпечують їх композиційність, коли різні компоненти фінансового алгоритму можуть реалізувати різні смарт-контракти, даючи змогу створювати складні архітектури фінансових протоколів.

У такий спосіб реалізовуються протоколи децентралізованих криптовалютних бірж, майданчиків децентралізованого кредитування, систем автоматизованого управління портфоліо, та різних алгоритмічних криптоактивів на зразок стейблкойнів та деривативів [54]. Протоколи децентралізованих фінансів надають такі переваги, як некастодіальність операцій, бездозвільність, відкрита аудитованість та (псевдо)анонімізованість. Відтак, їх популярність та використання різко зростали із 2019 р. і досяги показника Total Value Locked (TVL) понад 150 мільярдів доларів США [1].

У цій статті наведемо огляд явища Maximal Extractable Value (MEV), яке спричинене відсутністю сталої та прогнозованої послідовності транзакцій у вихідних блоках мереж блокчейн. Це явище розпочалося із появою смарт-контрактів у мережах блокчейн та з часом набуло значного поширення, охопивши протоколи

децентралізованих фінансів, мережі рівнів L1/L2 та міжмережеву блокчейн-комунікацію. Учасники мережі блокчейн з ексклюзивним доступом до впорядкування транзакцій (майнери, валідатори, сіквенсери) мають змогу маніпулювати послідовністю транзакцій та здійснювати атаки на випередження задля присвоєння собі вигоди, яку мали на меті отримати інші учасники.

Актуальність проблеми явища MEV в мережах блокчейн полягає в його значущому негативному впливі на блокчейн-екосистему та в серйозних системних ризиках для функціонування мереж блокчейн. Це своєю чергою зумовлює важливість досліджень самого явища MEV, а також напрямів зменшення його негативних ефектів. Зважаючи на схожість природи цього явища з подібними проявами у світі класичних фінансів, методи вирішення схожих проблем централізованими інституціями неможливо застосувати у децентралізованому світі однорангових мереж блокчейн, що ускладнює пошук ефективного вирішення цієї проблеми.

Об'єкт дослідження – явище MEV у мережах блокчейн – максимальна "екстрактована" вигода, яку певні учасники мережі можуть отримати завдяки ексклюзивному доступу до впорядкування транзакцій.

Предмет дослідження – етапи розвитку явища MEV в мережах блокчейн, найпоширеніші випадки експлуатації цього явища та його переважно негативний вплив на блокчейн-екосистему. Увагу також звернено на напрацювання у напрямі подолання ризиків, спричинених екстракцією MEV.

Мета роботи – здійснити огляд виконаних досліджень та публікацій на тему екстракції MEV у мережах блокчейн, виконати ретроспективний аналіз розвитку цього явища, виокремити його найпоширеніші прояви, систематизувати методи і засоби, використовувані під час його дослідження, оцінити масштаби екстракції MEV та окреслити майбутні перспективні напрями досліджень.

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

- виконати огляд ранніх досліджень маніпуляцій послідовністю транзакцій та атак на випередження у мережах блокчейн;
- детально розглянути безпосередньо явище MEV у мережах блокчейн;
- виокремити поширені типи екстракції MEV та проаналізувати розвиток і поширення цього явища протягом останніх років;
- виконати огляд досліджень цієї проблеми, методів, застосовуваних у подібних дослідженнях, та поточних оцінок масштабів екстракції MEV;
- підсумувати ризики, які спричиняє явище MEV для функціонування мереж блокчейн, та оцінити дослідження в напрямі їх подолання.

Аналіз останніх досліджень та публікацій. *Ранні дослідження маніпуляцій послідовністю транзакцій та атак на випередження.* Можливості заробітку на маніпуляціях послідовністю транзакцій помітили ще в часи бурхливого розквіту краудфаундингових ініціатив ICO (Initial Coin Offering) у 2017–2018 рр. [20], коли різноманітні проєкти, що стосувалися блокчейн-технологій, залучали інвестиції за допомогою емісії та продажу інвесторам нових токенів. Ці операції відбувались в мережі блокчейн та часто мали ознаки аукціонів з обмеженням за кількістю придбання однією адресою, за часом або інші обмеження. Куплені токени, по суті, можна було вважати інструментом інвестування або криптоактивом, який у майбутньому міг забезпечити великий заробіток інвестору. Відтак це спонукало майнерів маніпулювати послідовністю транзакцій, щоб забезпечити купівлю ICO токенів із контрольованих ними адрес та водночас "придушити" або сповільнити подібні транзакції інших користувачів мережі. Одним із таких ICO, під час якого вперше помітили маніпуляції, було розміщення проєкту Status.im [47] із залученням більше ніж 100 мільйонів доларів США. Розміщуючи майнінг, пул F2Pool, на який припадало близько 23 % всього тогочасного хеш-рейту мережі Ethereum, здійснив маніпуляції послідовністю транзакцій на випередження та навмисно увів у блок більше транзакцій інших користувачів, які були явно неуспішними відповідно до умов аукціону, щоб максимізувати дохід ще й від комісій з транзакцій [10].

Згодом у статті [2] було описано можливі атаки на випередження у протоколі децентралізованої криптовалютної біржі Bancor [3]. Пізніше в іншій відомій статті [13] автори описали випадок випередження автоматизованими ботами під час спроби відновлення помилково заблокованих активів у протоколі децентралізованої криптовалютної біржі Uniswap [27]. В останньому випадку внаслідок помилки токени було відправлено за неправильною адресою-смарт контракту, звідки їх міг отримати будь-хто, викликавши певний його метод. Інформацію про те, що сталось, мав учасник мережі, який припустився помилки, проте завдяки трасованості смарт-контрактів та відкритості даних будь-хто інший міг помітити в мемпулі транзакцію на відновлення токенів та перехопити її, замінивши своєю. Це, врешті, і зробили автоматизовані боти-перехоплювачі. Все частіші випадки маніпуляцій послідовності транзакцій та атак на випередження у мережах блокчейн спонукали запропонуватити одну з перших класифікацій таких явищ у публікації [10]. У ній було подано визначення атак на випередження як таких, що відбуваються внаслідок ексклюзивного доступу певної сторони до привілейованої ринкової інформації про майбутні транзакції та угоди. Також проведено паралель з атаками на випередження у світі класичних фінансів та класифіковано атаки на випередження на атаки з переміщенням транзакцій, атаки зі вставлянням транзакцій та атаки з придушенням транзакцій, введено два варіанти кожної з атак – асиметричний та масований, з прикладами застосування цих атак у різних протоколах децентралізованих фінансів.

Формалізація явища Maximal Extractable Value (MEV). Вперше термін Maximal Extractable Value (MEV) – максимальної "екстрактованої" вигоди було введено в роботі [6], у якій комплексно проаналізовано атаки на випередження та маніпуляції послідовністю транзакцій. Автори зауважили схожість природи цих явищ із подібними проявами в світі класичних фінансів. Подібно до високочастотної алгоритмізованої торгівлі у класичних фінансах, у мережах блокчейн були розгорнуті автоматизовані програмовані боти, які використовували повторне надсилання транзакцій зі збільшеною комісією

задля випередження транзакцій інших учасників мережі, зокрема користувачів протоколів децентралізованих фінансів. Цеявище отримало назву *пріоритезованих аукціонів комісій* (PGA) та загалом негативно вплинуло на всіх користувачів мережі Ethereum, спричиняючи істотні стрибки вартості комісій на транзакції. В згаданій роботі було досліджено діяльність цих ботів та змодельовано їхню поведінку за допомогою [36]. Таке моделювання дало можливість виділити окремі стратегії роботи автоматизованих ботів за умов PGA та виявити феномен ботів-конкурентів, які координуються задля збільшення прибутку та зменшення комісій за свої транзакції.

Додатково було вказано на серйозні системні ризики від значних заробітків, які доступні майнерам завдяки здійсненню атак на випередження та маніпуляцій послідовністю транзакцій. Можливість такого заробітку стимулює майнерів та валідаторів експлуатувати уразливості алгоритмів консенсусу для штучної реорганізації блокчейну із відгалуженням ланцюжка блоків (рис. 1), що дає змогу переписати історію транзакцій та присвоїти частину прибутку інших учасників мережі собі. Такі махінації дестабілізують роботу мереж блокчейн та підривають загалом віру учасників мережі у гарантії, які вона повинна давати відповідно до реалізованих алгоритмів консенсусу.

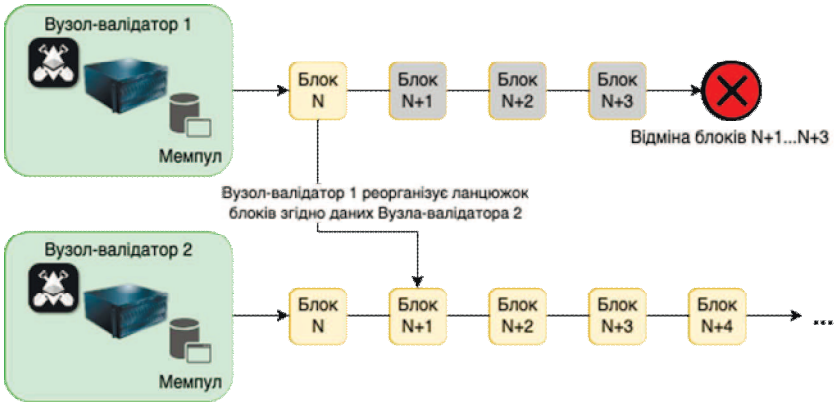

Рис. 1. Реорганізація блокчейну із відгалуженням ланцюжка блоків / Blockchain reorganization with chain fork

Згадане дослідження недарма в назві містить термін “Flashboys 2.0”, відсилаючи до відомої книги Flash Boys: A Wall Street Revolt [31] – бестселера, який чи не вперше розкрив явище алгоритмічної високочастотної торгівлі (HFT) на ринках цінних паперів, використання нею інсайдерської інформації та негативний вплив цього явища на ринки загалом. Попри те, що атаки на випередження та маніпуляції послідовністю транзакцій є зарегульованими на класичних ринках цінних паперів, HFT трейдерам все одно вдається знаходити нові можливості, що відповідно змушує регуляторів оновлювати свої правила [50]. Отже, можна говорити про паралелі між світом класичних фінансів та децентралізованими фінансами в мережах блокчейн, за винятком того, що в мережах блокчейн, завдяки їх децентралізованій природі, упровадження регуляцій є складним та малоефективним. Саме тому існує потреба в інших методах та засобах зменшення негативних ефектів явища екстракції MEV у мережах блокчейн.

В економічній науці під екстракцією вигоди (value extraction) з певного ринку або активу розуміють отримання вигоди стороною, яка має доступ до таких переваг:

- інформаційна асиметричність;
- мережевий ефект;
- популярність бренду;
- масштабування.

Аналогічно, деякі учасники мережі блокчейн – майнери, валідатори або розробники автоматизованих ботів, користуються схожими перевагами для отримання додаткового заробітку за рахунок інших учасників мережі. Також, говорячи про термінологію, варто згадати, що в роботі [6] вжито термін Miner Extractable Value, який із часом, завдяки переходу все більшої кількості протоколів на алгоритми консенсусу Proof-of-stake, трансформувався у загальніший термін Maximal Extractable Value, маючи на меті розширення контексту цього поняття. Крім цього, були спроби введення у обіг терміна Blockchain Extractable Value [43] але він не набув поширення. Тому далі в статті ми використовуємо саме термін Maximal Extractable Value (MEV). Вищезгадана публікація [6], як і більшість інших, зосереджується на проявах MEV у блокчейн-мережі Ethereum, яка нині є найширше використовуваним блокчейном із підтримкою смарт-контрактів. Аналогічно надалі будемо також мати на увазі екстракцію MEV саме в цій мережі, хоча це явище так само проявляється і в інших блокчейнах на зразок Solana, Cosmos тощо.

Результати дослідження та їх обговорення / Research results and their discussion

Огляд досліджень явища MEV у мережах блокчейн виявив, що найпоширеніші випадки експлуатації цього явища такі:

1. Атаки на випередження (frontrunning) – виявлення майнером, валідатором або іншим учасником (за допомогою автоматизованого програмованого бота) прибуткової транзакції в мемпулі або в закритих каналах транзакцій та випередження її у вихідній послідовності транзакцій, які входять у блок. Такі атаки можуть бути доволі узагальненими – коли сторона, яка атакує, автоматизований програмований бот, постійно сканує мемпул на наявність транзакцій, які можна реплікувати, вказавши свою адресу та збільшивши комісію для випередження [10]. Як правило, такі транзакції стосуються протоколів децентралізованих фінансів та викликa-

ють певний смарт-контракт. Попередній аналіз прибутковості транзакції здійснюється автоматизовано, засобами локального тестування та налагодження смарт-контрактів. Приклад реальної атаки на випередження можна побачити в блоці [11], де транзакцію [19] випереджено іншою транзакцією MEV екстрактора – [18] (взято зі звіту [55]).

2. Атаки на перехоплення (backrunning) – маніпуляція, яку здійснює майнер, валідатор або інший учасник (засобами автоматизованого програмованого бота) з тим, щоб забезпечити місце своєї транзакції одразу за цільовою транзакцією іншого учасника. Зазвичай це роблять, щоб скористатись різкою зміною ціни криптоактиву, яка можлива у разі або купівлі/продажу значної його кількості, або отримання транзакції з вузла-Оракула (Oracle) про оновлення ціни криптоактиву [43].

3. Арбітраж на децентралізованих криптовалютних біржах (arbitrage) – під арбітражем, в широкому розумінні цього явища у класичному світі фінансів, розуміють стратегію, за допомогою якої трейдери здійснюють купівлю та продаж активів одночасно на різних біржах або на одній біржі в різних ринкових умовах, щоб отримати прибуток, скориставшись різницею у цінах на активи (цінні папери, деривативи, валюти, товари тощо). Подібно арбітраж відбувається на децентралізованих криптовалютних біржах – трейдери намагаються визначити різницю в ціні криптовалюти на різних біржах, наприклад, на Uniswap [27] та Curve [48], та надсилають відповідні транзакції на купівлю/продаж між ними, щоб одержати свій прибуток на різниці в ціні. Екстракція MEV у разі арбітражу може здійснюватись в пасивний або проактивний спосіб. У першому випадку екстратори MEV стежать за відмінностями у ціні на різних біржах та здійснюють арбітраж у випадку, коли ймовірний прибуток перевищує затрати на виконання транзакцій. В другому випадку MEV екстрактори відстежують транзакції в мемпулі з тим, щоб визначити арбітражні транзакції інших учасників, копіюють їх та забезпечують (доступними їм способами) випередження транзакцій інших арбітражерів. Окрім цього, екстрактори MEV намагаються визначити транзакції, які потенційно впливають на ціну криптоактиву – це купівлі/продажі великих обсягів або отримання оновлення ціни з вузлів-Оракулів (Oracles), маючи на меті якомога швидше використати можливості арбітражу, випереджуючи будь-кого іншого [53]. Зазначимо, що, на відміну від інших проявів MEV, арбітраж загалом оцінюють як позитивне явище, яке дає змогу синхронізувати ціну між різними майданчиками та забезпечує так званий процес визначення ціни (price discovery) [54]. Також важливо розуміти, що говорити про явище MEV в арбітражі на децентралізованих криптовалютних біржах можна лише тоді, коли маніпулюють послідовністю транзакцій учасники, які або мають привілейований доступ до формування такої послідовності у вихідних блоках (майнери, валідатори), або які збільшують комісії за випереджувальні транзакції, спричиняючи аукціони PGA. Отже, не увесь арбітраж відбувається із використанням MEV [55].

4. Сендвіч-атаки (sandwich) – суть сандвіч-атак, відомих також у світі класичних фінансів [53], полягає в комбінації атак на випередження та перехоплення з метою маніпуляції ціною криптоактиву на децентралізованих криптовалютних біржах, які працюють на основі алгоритму автоматизованого маркет-мейкера (AMM). Атаку, спрощено, здійснюють так (рис. 2):

1. Екстрактор MEV відстежує у мемпулі (або в закритих каналах) транзакцію на купівлю або продаж великого обсягу криптовалюти, наприклад, токен *Y* купують за токен *X*.
2. Екстрактор MEV випереджує цю транзакцію своєю, в якій купує ту саму криптовалюту *A* за ціною, яку на той момент очікує учасник-жертва атаки. Це своєю чергою збільшує ціну токена *Y*.

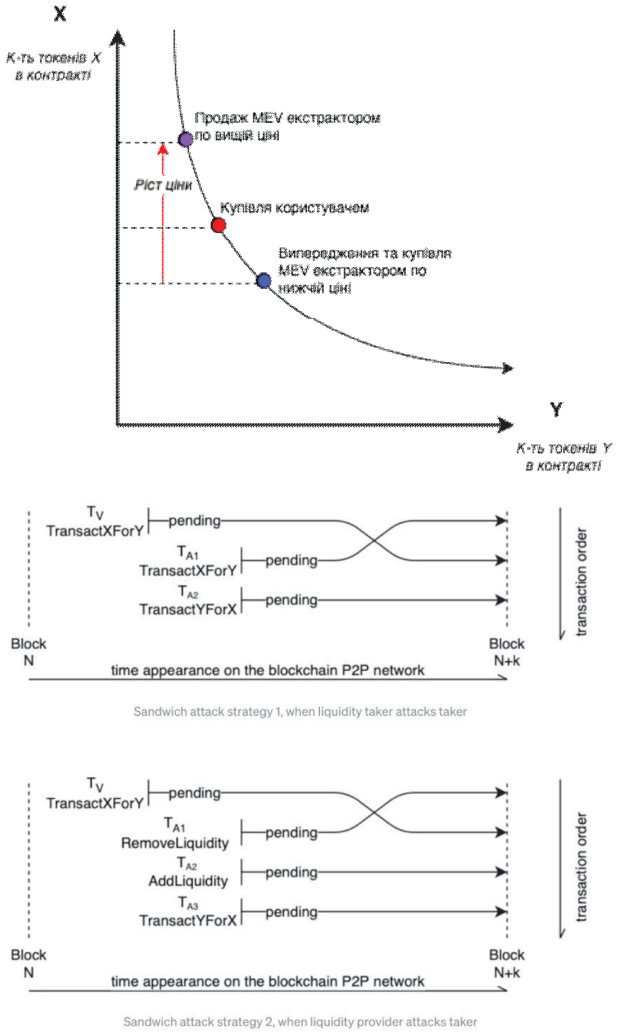

Рис. 2. Сендвіч-атака на алгоритм автоматизованого маркет-мейкера в децентралізованих криптовалютних біржах / Sandwich attack on AMM in decentralized exchanges [8]

3. Транзакція учасника-жертви атаки виконується, відповідно токен *Y* купують вже за завищеною ціною через збільшений зсув ціни (slippage). Це ще підвищує ціну токена *Y*.
4. Одразу після цього екстрактор MEV здійснює перехоплення та продає токен *Y* за ціною, яка зростала протягом кроків 2 та 3, отримуючи свій прибуток. Натомість учасник – жертва атаки, який мав на меті здійснити купівлю за вигідною для нього ціною, зазнає збитків.

Також існує дещо змінений варіант атаки, коли екстрактор MEV є надавачем ліквідності токена *Y* в пулі ліквідності децентралізованої криптовалютної біржі та відповідно не має потреби його купувати, а маніпулює ці-

ною завдяки виведенню та повторному введенню токена *Y* до пулу ліквідності. Цей тип атак, зокрема, можливий через прозорість механізму керування ціною автоматизованим маркет-мейкером, відтак сторона, яка атакує, може чітко визначити наміри учасника-жертви та потенційну зміну ціни [57]. У випадку сандвіч-атак маніпуляції послідовністю транзакцій майже завжди здійснює сторона, яка має привілейований доступ до вихідної послідовності транзакцій у блоці, тобто майнер або валідатор. Іншим учасникам за допомого збільшення комісій (PGA) все ж важко забезпечити чітку послідовність транзакцій, необхідну для здійснення атаки. Цей тип атак – один із найбільш загрозливих та прибуткових. Приклад такої атаки можна знайти в блоці [12] де випереджувальною була транзакція [16], транзакцією учасника-жертви – [17] та фінальною перехоплювальною транзакцією – [15] (взято зі звіту [55]).

5. Ліквідації в протоколах децентралізованого кредитування – протоколи децентралізованого кредитування дають можливість брати в кредит певний тип криптовалюти в обмін на заставу у вигляді різних криптоактивів (криптовалют, стейблкойнів, NFT тощо). Для прикладу, користувач може взяти в кредит певну кількість стейблкойнів USDC під заставу криптовалюти ETH. Механізм дефолту за кредитом в таких протоколах працює із залученням сторонніх учасників-ліквідаторів, які відстежують зміну ціни заставного криптоактиву за допомогою вузлів-Оракулів (Oracles) (або іншими каналами) та у випадку дефолту позики ініціюють процедуру її ліквідації – виплачують позику замість позичальника, отримуючи за це заставні криптоактиви за зниженою ціною [44]. Оскільки таку процедуру може ініціювати будь-який учасник, котрий найшвидше визначив ознаки дефолту за позикою, це робить її привабливою для експлуатації MEV – маніпуляції послідовністю транзакцій та атаки на випередження можуть використовуватись, щоб отримати найшвидший доступ до ліквідації позики та винагороди у вигляді криптоактиву за заниженою ціною (який можна одразу продати дорожче) [53]. Окрім такої "класичної" експлуатації MEV у протоколах децентралізованого кредитування, є ще складніші схеми екстракції – наприклад, експлуатант MEV з доступом до великих капіталів може спробувати маніпулювати ціною заставного криптоактиву, щоб ініціювати ліквідацію пов'язаних позик, а пізніше – маючи змогу маніпулювати послідовністю транзакцій у вихідному блоці, затримати транзакції позичальника, котрий намагається поповнити свою заставу задля уникнення ліквідації.

6. Інші випадки – до інших випадків екстракції MEV належать снайпінг-атаки на NFT, міжпротокольна екстракція MEV, атаки на децентралізовані протоколи реєстрації доменних імен тощо [37]. Ці випадки все ж спостерігаються рідше, ніж перераховані вище, але загалом можна стверджувати, що різноманіття можливостей екстракції MEV зростає із розвитком мереж блокчейн та протоколів децентралізованих фінансів.

Розвиток та поширення явища MEV. Розглядаючи розвиток явища MEV, неможливо не згадати про дослідницьку фірму Flashbots, засновниками якої є автори загаданої вище роботи [6]. Ця фірма, створена якраз в час актуалізації явища MEV (2020 р.), поставила мету вести дослідження та розроблення в напрямку зменшення негативних ефектів екстракції MEV в мережах блокчейн, зосереджуючись, зокрема, на мережі Ethereum. Відтак фірма Flashbots розробила платформу аукціонів MEV зі спеціалізованим розширенням програмного клієнта вузла мережі Ethereum, закритими каналами транзакцій і компонентами для ретрансляції та конструювання блоків (рис. 3).

Суть роботи цієї платформи полягала в забезпеченні закритого аукціону першої ціни (first-price sealed-bid auction) між майнерами і валідаторами та іншими користувачами, котрими можуть бути як експлуатанти MEV, так і звичайні учасники мережі, які хочуть приховати вміст своїх ще не підтверджених транзакцій (наприклад, купівлю/продаж у значних обсягах). По суті, Flashbots та інші схожі платформи MEV аукціонів намагаються сприяти процесу MEV задля того, щоб він став децентралізованішим, відкритішим та ефективнішим, на противагу намаганням унеможливити MEV явище як таке (рис. 4). Як правило, платформи-аукціони MEV забезпечують дві ключові можливості – приватність ще не підтверджених транзакцій та атомарність бандлів з транзакціями (часткове виконання бандла неможливе).

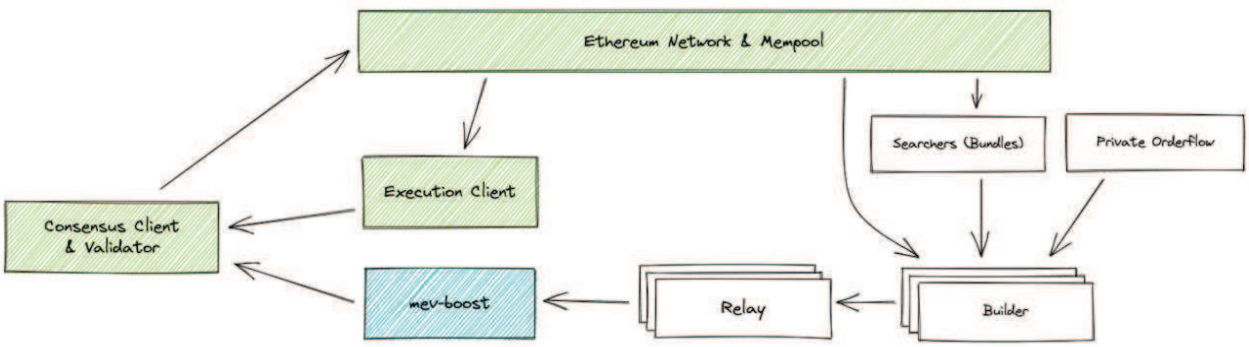

Рис. 3. Архітертура MEV-Boost / MEV-Boost architecture [34]

Рис. 4. Схема роботи аукціонів MEV / Working scheme of MEV auctions

Деякі з досліджень [53] виявили, що найбільшим досягненням Flashbots аукціонів сьогодні є зменшення комісій на транзакції для всіх учасників мережі Ethereum та згадана можливість прихованого надсилання транзакцій, щоб запобігти їх випередженню екстракторами MEV. Незважаючи на відкритість питання щодо ефективності вирішення проблеми MEV засобами аукціонів Flashbots, їх використання з часом зростало шаленими темпами – перед відомим оновленням Merge в мережі Ethereum програмний клієнт MEV-Geth [21] вузла мережі від Flashbots використовував на 99 % всіх вузлів мережі, після згаданого оновлення – 90 % вузлів оперують розширенням MEV-Boost [34] [56]. Тому в спільноті користувачів мережі Ethereum з часом почали з'являтись побоювання щодо ризиків централізації засобів MEV проєктами, за якими стоїть команда Flashbots. Варто згадати, що крім Flashbots є також інші подібні платформи, наприклад Eden Network [9] від відомої компанії, колишнього майнера Ethermine, але їхнє використання порівняно менш поширене.

З розвитком досліджень та дискусій навколо явища MEV у 2021 р. розпочалась робота над стандартом Proposer Builder Separation (PBS) [42] в мережі Ethereum, котрий має на меті відділити функцію формування блоків та визначення послідовності транзакцій від безпосередньої публікації блоків у одноранговій мережі з тим, щоб ці дві функції не виконував одночасно той самий вузол-валідатор протоколу Proof-of-stake. За задумом розробників, можливість формування блоків буде забезпечена будь-яким учасникам мережі, а вузол-валідатор вибиратиме для публікації блок з найбільшою винагородою. Своєю чергою, валідатор, вибравши варіант сформованого блока, наперед не матиме доступу до його вмісту (використовуючи криптографічну схему зобов'язання), а відтак не зможе маніпулювати послідовністю транзакцій [25] (рис. 5).

Стандарт PBS розробляється для вирішення таких завдань:

- перше і найголовніше завдання – зменшення негативних ефектів MEV та забезпечення його прозорості та децентралізації;
- також поставлено завдання збільшити стійкість мережі Ethereum до цензурування трафіку транзакцій – ця проблема загострилась із появою платформ аукціонів, які почали слугувати центральною точкою для фільтрації трафіку транзакцій;
- додатковим завданням є збільшення пропускної здатності мережі – така модуляризація сприятиме впровадженню механізму масштабування Danksharding, який може збільшити потужності мережі – вона оброблятиме до 100 000 транзакцій за секунду.

Робота над цим стандартом все ще на стадії дослідження і потребує вирішення низки відкритих питань. Говорячи про PBS в мережі Ethereum, варто знову згадати про платформу-аукціон MEV-Boost [34], яка заявляє про реалізацію цього стандарту. Варто уточнити, що сам стандарт ще не є 100 % фіналізованим, проте MEV-Boost реалізує його основні ідеї та слугує майданчиком для перевірки самої його концепції.

Наявні платформи-аукціони MEV, як і стандарт PBS, оперують поняттями користувач (user), програмний гаманець (wallet), трейдер-шукач (searcher), конструювальник блоків (builder) та постачальник безпеки (security provider). Для кращого розуміння екосистеми, яка з часом розвинулась навколо явища MEV, та сама команда Flashbots ввела у вжиток фреймворк ланцюжка постачання – MEV Supply Chain (рис. 6).

Цей фреймворк використовують для формалізації процесу екстракції MEV, позначення його учасників та залежностей між ними. Згадана термінологія в тому чи іншому вигляді використовується в контексті різних типів мереж блокчейн та платформ-аукціонів MEV.

Поширившись мережами рівня L1 (Ethereum, Solana, Cosmos та інші), явище MEV зачепило також міжмережеву взаємодію на рівні L1. У випадку міжмережевої екстракції джерелом MEV є все ті ж можливості заробітку на арбітражі між різними майданчиками. Наприклад, децентралізована біржа криптовалют Uniswap V2 [27] підтримує різні EVM-сумісні мережі блокчейн, як-от Ethereum або Binance Smart Chain. Переказ токенів з однієї мережі до іншої здійснюється засобами компонентів-мостів (bridges), які зазвичай реалізовано за допомогою смарт-контрактів. Відтак, екстрактори MEV намагаються маніпулювати послідовністю транзакцій в блоках кожної з мереж, які беруть участь у кросмережевій схемі арбітражу. Приклади таких схем міжмережевого арбітражу можна знайти за посиланням. Автори статті [37] виконали детальний огляд цього явища та окреслили низку відкритих питань, які потребують подальшого дослідження. Також суміжною те-

мою є екстракція MEV в мережах блокчейн L2, де вихідну послідовність транзакцій контролюють вузли-секвенсери (sequencers). Подібно до екстракції MEV на рівні L1, ці вузли мають змогу здійснювати атаки на випередження та інші маніпуляції послідовністю транзакцій. Ґрунтовна публікація [23] вперше виділила це явище з категорії міжмережевого MEV, а пізніша стаття [29] визначила динаміку розвитку MEV в мережах L2 та акцентувала на потребі децентралізації секвенсерів задля зменшення негативних ефектів MEV. Ця публікація також наголосила на важливості подальших досліджень у цьому напрямі, пов'язуючи це з перспективами перенесення рівня виконання транзакцій у мережі Ethereum з рівня L1 на рівень L2.

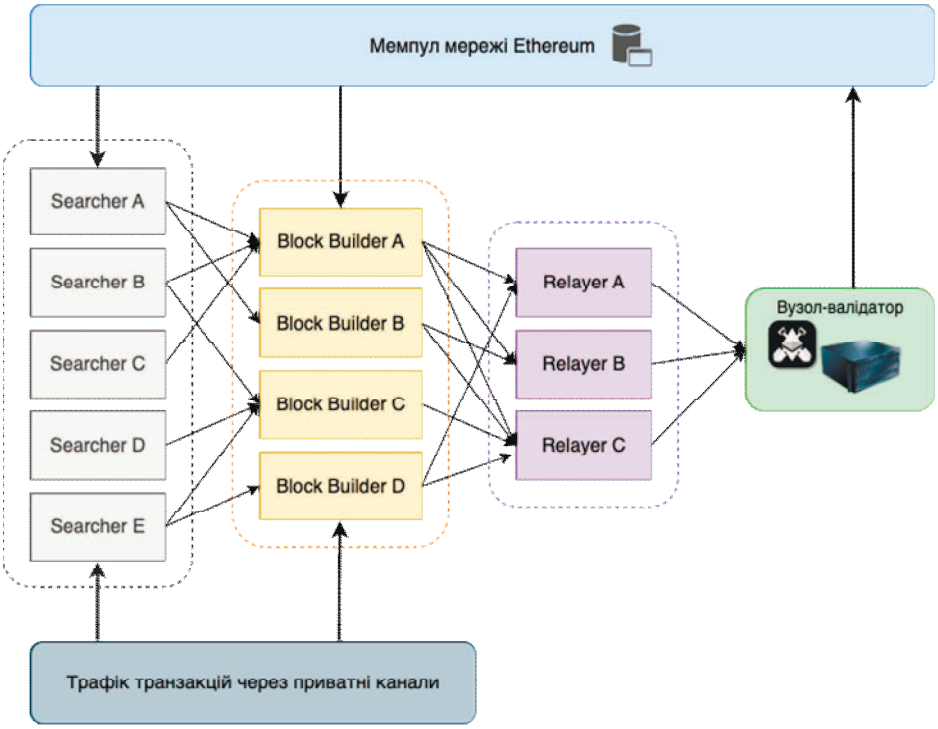

Рис. 5. Архітектура Ethereum за стандартом PBS / Ethereum architecture according to PBS standard

Рис. 6. Фреймворк MEV Supply Chain / MEV Supply Chain framework

Оцінки явища MEV. Починаючи з перших досліджень явища MEV, актуальним було питання оцінювання масштабів, природи та наслідків цього явища. Оцінка явища MEV – вкрай важливе завдання, яке охоплює такі напрями:

- вплив явища MEV на користувачів мереж блокчейн – масштаби заробітку екстракторів MEV та відповідно втрат звичайних користувачів, частка MEV закладена в ціну криптоактивів;
- рівень децентралізації мереж блокчейн та реалізованих протоколів – наскільки потужності екстрактування MEV або засоби сприяння (напр. аукціони MEV) є централізовано керованими, або, навпаки, наскільки децентралізованими;
- уразливості алгоритмів консенсусу та системний ризик їх експлуатації учасниками майнерами та валідаторами, зацікавленими в значних заробітках від екстракції MEV;
- регуляторна оцінка явища MEV та ймовірні контролювальні заходи в майбутньому.

Водночас ефективна оцінка MEV доволі ускладнена через децентралізовану та динамічну природу мереж блокчейн, в яких нові транзакції постійно прибувають через вузли одноранговой мережі, розкиданої по всіх кутках світу (рис. 7). Унаслідок цього фіналізація стану відбувається із затримкою, протягом якої можливі реорганізації блокчейну та відгалуження від основного ланцюжка блоків.

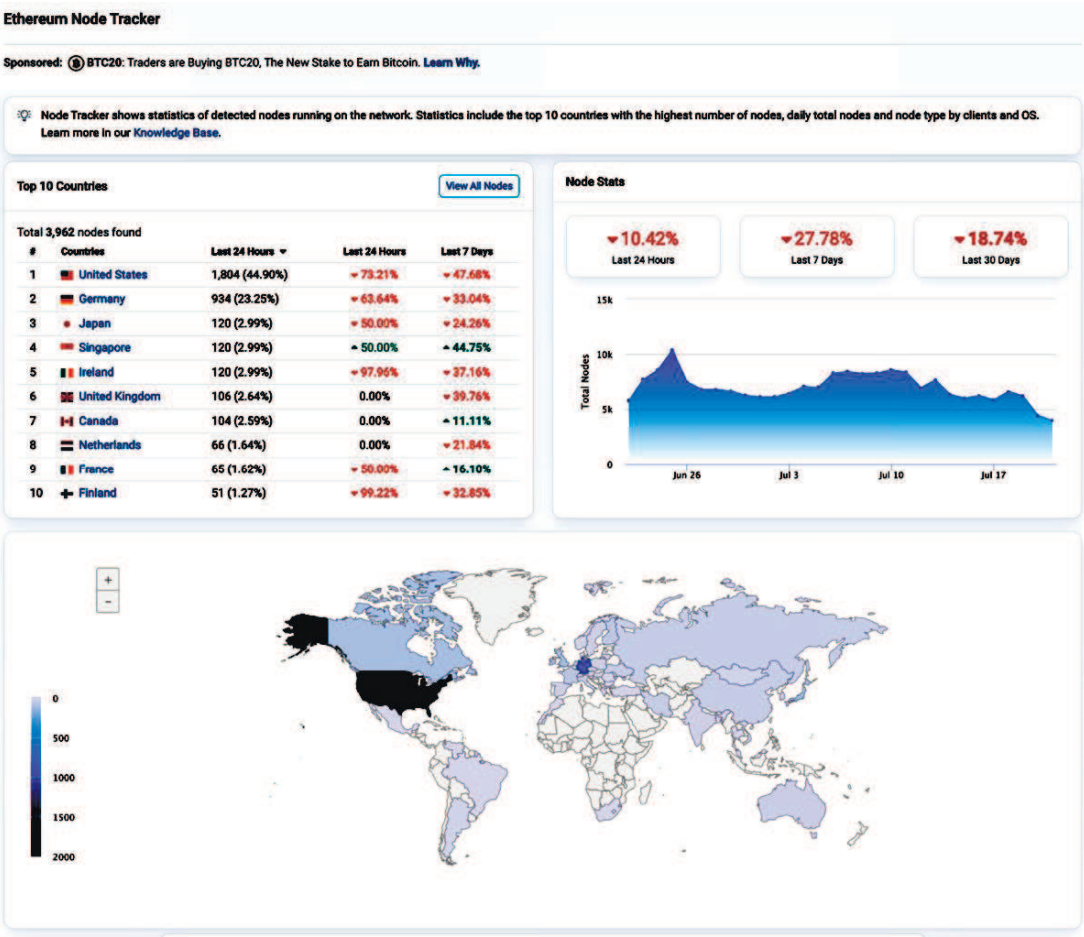

Рис. 7. Карта вузлів мережі Ethereum / Ethereum network nodes map [14]

Окрім наведених вище факторів, оцінювання ускладнюють прихованість частини трафіку транзакцій (які надходять приватними каналами), варіативність типів екстракції MEV та загальна складність екосистеми мереж блокчейн, різноманіття смарт-контрактів, проблематичність відстеження їх оновленьтощо. Саме тому для оцінювання та дослідження явища MEV використовують такі методи або їх комбінації:

- емпіричні дослідження із використанням аналізу відкритих даних мережі блокчейн; аналіз може бути ретроспективним та звертати увагу на певний діапазон підтверджених блоків або поточним, охоплювати потік ще не підтверджених транзакцій у мемпулі. Такий тип досліджень використано в працях [43], [40] (алгоритм на основі теорії графів), [53], [10] [50] та [52];
- в окрему підкатегорію можна виділити роботи, які використовують методи машинного навчання, наприклад [39];
- використання алгоритмічної теорії ігор для моделювання та симуляції стратегій поведінки різних учасників мережі блокчейн у випадку екстракції MEV; ці підходи, зокрема, використано в працях [6] [32] [28] та [30];
- використовують також інші підходи, такі як, наприклад, формальні методи [4], [22] та економічне моделювання [41].

Щодо оцінювання заробітків екстракторів MEV та відповідно (частково) втрат користувачів мереж блок-

чейн, можемо звернути увагу на подібні оцінки щодо мережі Ethereum. Згідно з даними фірми Flashbots, від початку періоду збирання даних 1 січня 2020 року до всім відомого оновлення Merge, тобто до 15 вересня 2022 року, оцінка MEV становила 675 623 114 доларів США, а згодом, після оновлення, з використанням аукціону MEV – MEV-Boost, на 22 липня 2023 року оцінка в MEV в криптовалюті ETH становила 245 453 ETH, що на момент написання статті відповідає 462 433 452 доларам США (згідно зі статистикою [35]), тобто сумарна оцінка перевищує мільярд доларів США. Варто зазначити, що ця цифра є лише нижньою граничною оцінкою, оскільки не враховує екстракцію MEV, здійснену за межами інфраструктури та каналів Flashbots та безпосередніх маніпуляцій послідовністю транзакцій або атак майнерів та валідаторів на випередження. Схожі оцінки згадано в публікаціях [43] та [40]. Якщо ж говорити про "найвдалішу" екстракцію MEV, то, наприклад, автоматизований арбітражний бот зміг заробити більше ніж 3 мільйони доларів, перехопивши транзакцію [51] з обміном значного об'єму криптовалюти. Або ж можна згадати автоматизованого MEV бота "jaredfromsubway.eth", котрий лише на комісії за транзакції витратив 7 мільйонів доларів за березень–квітень 2023 року (згідно з [45]), що дає змогу уявити масштаби явища MEV у мережі Ethereum.

Обговорення результатів дослідження. Опрацювавши масив публікацій за тематикою екстракції MEV в мережах блокчейн, вдалось виокремити два основні напрями досліджень цього явища:

- аналіз безпосередньо самого явища MEV, оцінка його масштабів та поширення, емпіричні дослідження та теоретичне моделювання, а також огляд цієї проблематики з регуляторної позиції;
- пошук методів і засобів зменшення негативних ефектів екстракції MEV у мережах блокчейн, ураховуючи розроблення нових алгоритмів консенсусу, захищених реалізацій смарт-контрактів та MEV аукціонів, здатних демократизувати доступ до MEV.

Цю роботу варто зарахувати саме до першого напряму досліджень, тому нижче наведемо низку публікацій безпосередньо за напрямом аналізу та оцінки явища MEV у мережах блокчейн.

Робота [10] досліджує проблему атак на випередження в мережах блокчейн, проводячи паралелі зі схожими маніпуляціями на фінансових ринках у 1970-ті роки. В публікації проаналізовано випадки атак на випередження у 25 популярних децентралізованих додатках, розгорнутих умережі Ethereum, а також поведінку вузлів-майнерів у межах процедури ICO проєкту Status.im, наведено класифікацію наявних способів захисту від таких атак.

Робота [43] розглядає явище MEV, використовуючи термін Blockchain Extractable Value (BEV), який згодом перестали широко вживати. Незважаючи на це, публікація варта уваги, оскільки в ній здійснено важливу оцінку доходів від екстракції MEV та виявлено потенційні ризики для безпеки мереж блокчейн. Дослідження містить ретроспективний аналіз ранніх проявів MEV та зауважено істотні ризики для стабільності роботи алгоритмів консенсусу в мережах блокчейн.

Робота [50] аналізує атаки на випередження, які здійснюються в мережі Ethereum, та виокремлює три типи таких атак – зміщення (displacement), вставляння (insertion) та подавлення (suppression). Запропоновано методологію для ідентифікації згаданих типів атак на масиві історичних данихі з транзакціями мережі Ethereum та наведено результати її застосування для аналізу 11 мільйонів блоків – виявлено 200 000 випадків атак загалом на 18,41 мільйона доларів США.

Робота [40] досліджує явище MEV в мережі Ethereum та акцентуєна здатності вузлів-майнерів використовувати привілейований доступ до впорядкування транзакцій задля збільшення свого доходу. Автори роботи запропонували алгоритм для виявлення випадків експлуатації MEV, застосували його та визначили, що переважна більшість прибутків від екстракції дістається саме учасникам-майнерам. Також у публікації зазначено, що приватні транзакції відіграють важливу роль в екстракції MEV, становлять значну частину прибутку майнерів. У статті також виявлено можливі загрози для безпеки мережі Ethereum, пов'язані із проявами MEV.

Робота [53] досліджує ефективність рішення від дослідницької організації Flashbots, що визначено як пул приватних транзакцій (ППТ), спрямованих на зменшення негативних ефектів MEV в мережі Ethereum. Дослідження показує, що учасники-майнери, які співпрацюють з Flashbots, домінують в мережі та отримують значно більше прибутку, сприяючи централізації та вертикалізації процесу екстракції MEV. Ця публікація підсумовує, що хоча Flashbots і вирішує значну частину проблеми MEV, проте інші ППТ також розгорнуті в мережі Ethereum та сприяють зростанню масштабів екстракції MEV.

Отже, за результатами роботи, можна сформулювати наукову новизну і практичну значущість результатів дослідження.

Наукова новизна отриманих результатів дослідження: за результатами детального огляду виконаних досліджень та публікацій здійснено ретроспективний аналіз розвитку явища MEV в мережах блокчейн, виокремлено його найпоширеніші прояви, систематизовано методи і засоби, використані у дослідженнях цього явища. Проаналізовано запропоновані рішення стосовно мінімізації негативних ефектів явища MEV та зроблено важливий висновок щодо неможливості використання рішень таких проблем з класичного світу фінансів у децентралізованих мережах блокчейн.

Практична значущість результатів дослідження: результати дослідження ознайомлюють із актуальною проблемою екстракції MEV у мережах блокчейн, вказують на подальші напрями поширення цього явища блокчейн екосистемою (крос-мережева взаємодія та рівень L2) та окреслюють можливості зменшення негативних ефектів MEV. Це, своєю чергою, можуть використовувати як інші науковці – для вибору напряму подальших досліджень, так і установи та організації, які бажають оцінити ризики інтеграції з мережами блокчейн та протоколами децентралізованих фінансів.

Висновки / Conclusions

Підсумовуючи, варто ще раз наголосити на здебільшого негативному впливі явища MEV на мережі блокчейн, протоколи децентралізованих фінансів та їх користувачів. Конкретніше, йдеться про такі ризики:

- втрата користувачами частини прибутку – MEV часто слугує "невидимим" податком, який стягується на користь учасників мережі з привілейованим доступом до впорядкування транзакцій, таких як майнери, валідатори або ж власники автоматизованих ботів;
- перевантаження мережі та зростання вартості комісій на транзакції – здебільшого внаслідок некоординованих аукціонів PGA;
- ризики стабільності роботи алгоритмів консенсусу – внаслідок заохочення екстракцією MEV до штучної реорганізації блокчейну та створення відгалужень від основного ланцюжка блоків;
- централізація можливостей екстракції MEV однією стороною, а відтак вертикальна інтеграція та монополізація – наприклад, учасник-валідатор може намагатись виконувати роль конструювальника блоків (builder) та екстрактора MEV (searcher) завдяки ефектам масштабу;
- збільшення цензурування трафіку транзакцій – як згадано вище, аукціони MEV з часом почали відігравати роль центральних вузлів, які намагаються фільтрувати транзакції згідно із інструкціями регуляторних органів;
- підвищена увага регуляторних органів та намагання взяти під контроль прояви MEV.

Наведені ризики є вкрай критичними для мереж блокчейн та їхніх користувачів, тому нині активно ведеться дослідницька робота в напрямі їх подолання.

Ґрунтовний огляд поточних рішень зменшення негативних ефектів MEV [56] виявив, що уже сформувалось дві "школи" вирішення проблеми екстракції MEV у мережах блокчейн:

- платформи-аукціони MEV на зразок MEV-Boost від Flashbots, котрі намагаються децентралізувати екстракцію MEV та зробити її прозорішою та ефективнішою;
- розроблення методів і засобів унеможливлення MEV – зазвичай це або нові алгоритми консенсусу, або нові реалізації смарт-контрактів, на яких працюють протоколи децентралізованих фінансів;

Детальний огляд методів і засобів зменшення негативних ефектів явища MEV виходить за межі цієї статті, але більшість публікацій сходяться на тому, що фінального рішення, яке б остаточно на практиці усунуло цю проблему, поки що не знайдено, а відтак робота в цьому напрямку триває, прикладом чого можуть слугувати публікації [56], [57], [24], [5] та [26]. Це, своєю чергою, зумовлює актуальність подальших досліджень в напрямі подолання негативних впливів MEV на мережі блокчейн та протоколи децентралізованих фінансів.

References

[1] Auer, R., Haslhofer, B., Kitzler, S., Saggese, P., & Friedhelm, V. (n.d.). The Technology of Decentralized Finance (DEFI) Industrial Organization, International Macroeconomics and Finance and Banking and Corporate Finance. Retrieved from: www.cepr.org

[2] Bancor Is Flawed. (n.d.). Retrieved August 13, 2023, from: https://hackingdi-stributed.com/2017/06/19/bancor-is-flawed/

[3] Bancor Network. (n.d.). Retrieved August 13, 2023, from: https://bancor.network/

[4] Bartoletti, M., & Zunino, R. (2023). A theoretical basis for Blockchain Extractable Value. Retrieved from: http://arxiv.org/abs/2302.02154

[5] Baum, C., Hsin-yu Chiang, J., David, B., Kasper Frederiksen, T., & Gentile, L. (2021). SoK: Mitigation of Front-running in Decentralized Finance.

[6] Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., & Juels, A. (2019). Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. https://doi.org/10.48550/arxiv.1904.05234

[7] Danksharding / ethereum.org. (n.d.). Retrieved August 13, 2023, from: https://- ethereum.org/en/roadmap/danksharding/

[8] DEFI Sandwich Attack Explain. In this article, I am going to… / by achinta das / Coinmonks /Medium. (n.d.). Retrieved August 21, 2023, from: https://medium.com/coinmonks/defi-sandwich-attack-explain-776f6f43b2fd

[9] Eden Network – Multichain Infrastructure for Maximal Value | Eden Network – Multichain Infrastructure for Maximal Value. (n.d.). Retrieved August 13, 2023, from: https://www.edennetwork.io/

[10] Eskandari, S., Moosavi, S., & Clark, J. (2019). SoK: Transparent Dishonesty: front-running attacks on Blockchain. https://doi.org/10.48550/arxiv.1902.05164

[11] Ethereum Blocks #10281528 / Etherscan. (n.d.). Retrieved August 13, 2023, from: https://etherscan.io/block/10281528

[12] Ethereum Blocks #16133912 / Etherscan. (n.d.). Retrieved August 13, 2023, from: https://etherscan.io/block/16133912

[13] Ethereum is a Dark Forest. (n.d.). Retrieved August 13, 2023, from: https://www.paradigm.xyz/2020/08/ethereum-is-a-dark-forest

[14] Ethereum Node Tracker / Etherscan. (n.d.). Retrieved August 21, 2023, from: https://etherscan.io/nodetracker

[15] Ethereum Transaction Hash (Txhash) Details / Etherscan. (n.d.). Retrieved August 13, 2023, from: https://etherscan.io/tx/0x0e2c50e60c180b645aa5c62f80-202242ad34b1ba163964999d5f4c9aad2037d0

[16] Ethereum Transaction Hash (Txhash) Details . Etherscan. (n.d.). Retrieved August 13, 2023, from: https://etherscan.io/tx/0x2ed629dd81fb6c5541402-775fc0217a2df04066cba5f2eb96b1dc53082ddeb6 b

[17] Ethereum Transaction Hash (Txhash) Details / Etherscan. (n.d.). Retrieved August 13, 2023, from: https://etherscan.io/tx/0x50ca4302caf14a4475 d-19a4b4cbdd522195136a17dcba68287529be2f21a4fd3

[18] Ethereum Transaction Hash (Txhash) Details / Etherscan. (n.d.). Retrieved August 13, 2023, from: https://etherscan.io/tx/0x5169bccd1893130995ebc25fa3-74366284b723ded44f379d0977af3f144d1a8 f

[19] Ethereum Transaction Hash (Txhash) Details / Etherscan. (n.d.). Retrieved August 13, 2023, from: https://etherscan.io/tx/0xe0c3dcfbb00c03492d1520-a63ecf0a83f4beade2949616054d0f4b19196d79eb

[20] Fenu, G., Marchesi, L., Marchesi, M., & Tonelli, R. (2018). The ICO phenomenon and its relationships with ethereum smart contract environment. 2018 IEEE 1st International Workshop on Blockchain Oriented Software Engineering, IWBOSE 2018 – Proceedings, 2018 January, 1–7. https://doi.org/10.1109/IWBOSE.2018.8327568

[21] GitHub – flashbots/mev-geth: Go implementation of MEV-Auction for Ethereum. (n.d.). Retrieved August 13, 2023, from: https://github.com/flashbots/mev-geth

[22] Guo, A. (2023). Invariance properties of maximal extractable value. Retrieved from: http://arxiv.org/abs/2304.11010
[23] Ha, F., & Michellis, D. (2021). MEV on L2.
[24] Heimbach, L., & Wattenhofer, R. (2022). SoK: Preventing Transaction Reordering Manipulations in Decentralized Finance. https://doi.org/10.1145/3558535.3559784
[25] Heimbach, L., Kiffer, L., Torres, C. F., & Wattenhofer, R. (2023). Ethereum's Proposer-Builder Separation: Promises and Realities. Retrieved from: http://arxiv.org/abs/2305.19037
[26] Heimbach, L., Zürich, E., Ch, S. H., Wattenhofer, R., & Switzerland, Z. (n.d.). Eliminating Sandwich Attacks with the Help of Game Theory; Eliminating Sandwich Attacks with the Help of Game Theory. ASIA CCS, 15. https://doi.org/10.1145/3488932.3517390
[27] Home / Uniswap Protocol. (n.d.). Retrieved August 13, 2023, from: https://uniswap.org/
[28] Judmayer, A., Stifter, N., Schindler, P., & Weippl, E. (2021). Estimating (Miner) Extractable Value is Hard, Let's Go Shopping! Retrieved from: https://github.com/
[29] L2 MEV wat – Taiko Labs. (n.d.). Retrieved August 13, 2023, from: https://taiko.mirror.xyz/VjNjFws6OOVez5YCDMwjy4BUiDqZBHYDvcW4-JZGDkc
[30] Lehar, A., & Parlour, C. A. (2023). Battle of the Bots: Flash loans, Miner Extractable Value and Efficient Settlement Battle of the Bots: Flash loans, Miner Extractable Value and Efficient Settlement Preliminary and incomplete.
[31] Lewis, M. (2014). Flash Boys: A Wall Street Revolt. W.W. Norton & Company.
[32] Mazorra, B., Reynolds, M., & Daza, V. (2022). Price of MEV: Towards a Game Theoretical Approach to MEV. Retrieved from: http://arxiv.org/abs/2208.13464
[33] MEV Explore. (n.d.). Retrieved August 13, 2023, from: https://explore-.flashbots.net/
[34] MEV-Boost in a Nutshell. (n.d.). Retrieved August 13, 2023, from: https://boost.flashbots.net/
[35] mevboost.pics / MEV-Boost Dashboard. (n.d.). Retrieved August 13, 2023, from: https://mevboost.pics/
[36] Nisan, Noam. (2007). Algorithmic game theory. Cambridge University Press.
[37] Obadia, A., Salles, A., Sankar, L., Chitra, T., Chellani, V., & Daian, P. (2021). Unity is Strength: A Formalization of Cross-Domain Maximal Extractable Value. https://doi.org/10.48550/arxiv.2112.01472
[38] Odos. (n.d.). Retrieved August 13, 2023, from: https://www.odos.xyz/arbitrage
[39] Park, S., Jeong, W., Lee, Y., Son, B., Jang, H., & Lee, J. (2023). Unraveling the MEV Enigma: ABI-Free Detection Model using Graph Neural Networks. Retrieved from: http://arxiv.org/abs/2305.05952
[40] Piet, J., Fairoze, J., & Weaver, N. (2022). Extracting Godl [sic] from the Salt Mines: Ethereum Miners Extracting Value. https://doi.org/10.48550/arxiv.2203.15930
[41] Poux, P., De Filippi, P., & Deffains, B. (2022). Maximal Extractable Value and the Blockchain Commons. Retrieved from: https://ssrn.com/abstract=4198139
[42] Proposer-builder separation / ethereum.org. (n.d.). Retrieved August 13, 2023, from: https://ethereum.org/en/roadmap/pbs/
[43] Qin, K., Zhou, L., & Gervais, A. (2021). Quantifying Blockchain Extractable Value: How dark is the forest? https://doi.org/10.48550/arxiv.2101.05511
[44] Qin, K., Zhou, L., Gamito, P., Jovanovic, P., & Gervais, A. (2021). An Empirical Study of DeFi Liquidations: Incentives, Risks, and Instabilities. https://doi.org/10.1145/3487552.3487811
[45] sealaunch.xyz у Твіттері: "A MEV bot is eating your lunch. jaredfro-msubway.eth MEV bot is the top gas ETH spender in the last 24H, spending 455ETH ($950 k) and using 7 % of total gas of the network In the last 2 months it spent more than 3.720ETH ($7M) in gas fees and performed more than 180 k transactions https://t.co/IGMJY7skkq" / X. (n.d.). Retrieved August 13, 2023, from: https://twitter.com/SeaLaunch_/status/1648436056717688832
[46] State of research: increasing censorship resistance of transactions under proposer/builder separation (PBS) – HackMD. (n.d.). Retrieved August 13, 2023, from: https://notes.ethereum.org/@vbuterin/pbs_censorship_resistance
[47] Status – Private, Secure Communication. (n.d.). Retrieved August 13, 2023, from: https://status.im/
[48] Swap – Curve. (n.d.). Retrieved August 13, 2023, from: https://-curve.fi/#/ethereum/swap
[49] The Merge | ethereum.org. (n.d.). Retrieved August 13, 2023, from: https://ethereum.org/en/roadmap/merge/
[50] Torres, C. F., Camino, R., & State, R. (2021). Frontrunner Jones and the Raiders of the Dark Forest: An Empirical Study of Frontrunning on the Ethereum Blockchain. https://doi.org/10.48550/arxiv.2102.03347
[51] Transaction Flow Chart / EigenTx:0xb55d4267a3565fdc8bada2638f97ed0bb3-1aa40bf8d4b304086dbdc1ca7d7844. (n.d.). Retrieved August 13, 2023, from: https://eigenphi.io/mev/eigentx/0xb55d4267a3565fdc8bada2638f97ed0bb31aa40bf8d4b304086dbdc1ca7d7844
[52] Wahrstätter, A., Zhou, L., Qin, K., Svetinovic, D., & Gervais, A. (2023). Time to Bribe: Measuring Block Construction Markets.
[53] Weintraub, B., Torres, C. F., Nita-Rotaru, C., & State, R. (2022). A Flash (bot) in the Pan: Measuring Maximal Extractable Value in Private Pools. https://doi.org/10.1145/3517745.3561448
[54] Werner, S. M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., & Knottenbelt, W. J. (2021). SoK: Decentralized Finance (DeFi). https://doi.org/10.48550/arxiv.2101.08778
[55] What is MEV Anyway? – Coin Metrics. (n.d.). Retrieved August 13, 2023, from: https://coinmetrics.io/special-insights/what-is-mev-anyway/
[56] Yang, S., Zhang, F., Huang, K., Chen, X., Yang, Y., & Zhu, F. (2022). SoK: MEV Countermeasures: Theory and Practice. Retrieved from: https://arxiv.org/abs/2212.05111
[57] Zhou, L., Qin, K., & Gervais, A. (2021). A2MM: Mitigating Frontrunning, Transaction Reordering and Consensus Instability in Decentralized Exchanges. Retrieved from: http://arxiv.org/abs/2106.07371

N. S. Cherkas, A. Y. Batiuk

Lviv Polytechnic National University, Lviv, Ukraine

MAXIMAL EXTRACTABLE VALUE (MEV) IN BLOCKCHAIN NETWORKS AND ITS IMPACT ON BLOCKCHAIN ECOSYSTEM

The advent of smart contract technology in blockchain networks has ushered in a new era of possibilities for implementing complex decentralized finance protocols. Over time, these protocols have gained significant traction, reaching a Total Value Locked (TVL) of over 150 billion US dollars. While blockchain networks offer inherent benefits such as immutability, transparency, decentralization, and security, they still grapple with a critical challenge – the inability to ensure a predictable order of transactions within produced blocks. This limitation has given rise to the Maximal Extractable Value (MEV) phenomenon.

MEV represents the maximum potential benefit that certain network participants, primarily miners and validators, can extract by wielding their exclusive capability to influence transaction order. In this work, we embark on an exhaustive exploration of the MEV phenomenon and delve deep into its impact on the broader blockchain ecosystem. We shed light on the pressing issue of transaction ordering in blockchain networks and provide an in-depth survey of the vast body of scholarly publications focused on MEV extraction.

This comprehensive review allowed us to conduct a retrospective analysis of the MEV phenomenon, categorize its most common manifestations, and uncover current development trends. Intriguingly, during this analysis, parallels were drawn with similar manipulations witnessed in the realm of high-frequency algorithmic trading within traditional financial markets.

A vital conclusion that emerged from our study pertains to possible strategies for addressing the MEV problem within decentralized finance protocols. We systematically outline the current research directions concerning MEV, explore the methodologies and tools employed in these studies, and present concrete examples of MEV extraction within the Ethereum network, accompanied by quantitative estimations.

In summary, the MEV phenomenon has cast an overwhelming negative impact on blockchain networks and decentralized finance. Our analysis of existing publications within a specific subcategory reveals the current absence of an effective solution to the MEV extraction problem. This underscores the importance of further research aimed at mitigating the adverse effects of MEV on blockchain networks and decentralized finance protocols.

Keywords: blockchain; smart contracts; distributed systems; peer-to-peer networks' cryptography.

Інформація про авторів:

Черкас Назарій Степанович, аспірант, кафедра автоматизованих систем управління.
Email: nazarii.s.cherkas@lpnu.ua

Батюк Анатолій Євгенович, канд. техн. наук, доцент, кафедра автоматизованих систем управління.
Email: abatyuk@gmail.com; https://orcid.org/0000-0001-7650-7383

Цитування за ДСТУ: Черкас Н. С., Батюк А. Є. Явище maximal extractable value (mev) в мережах блокчейн та його вплив на блокчейн екосистему. *Український журнал інформаційних технологій.* 2023. Т. 5, № 2. С. 60–71.

Citation APA: Cherkas, N. S., & Batiuk, A. Y. (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