https://doi.org/10.31891/2307-5732-2025-357-83
УДК 004.75/.62

ЧЕРКАС НАЗАРІЙ
Національний університет «Львівська політехніка»
https://orcid.org/0009-0007-9976-6530
e-mail: nazarii.s.cherkas@lpnu.ua
БАТЮК АНАТОЛІЙ
Національний університет «Львівська політехніка»
https://orcid.org/0000-0001-7650-7383
e-mail: anatolii.y.batiuk@lpnu.ua

ВПОРЯДКУВАННЯ ТРАНЗАКЦІЙ ЗА ЛОГІЧНИМИ ЧАСОВИМИ МІТКАМИ ЛАМПОРТА ЯК ЗАСІБ ЗМЕНШЕННЯ MEV-ЕКСТРАКЦІЇ У СМАРТ-КОНТРАКТАХ ETHEREUM

Зростання масштабів явища Maximal Extractable Value (MEV) у мережах блокчейн виявило критичні виклики у забезпеченні справедливого та передбачуваного порядку виконання транзакцій. У мережі Ethereum, де вузли-валідатори мають повний контроль над послідовністю транзакцій, користувачі стикаються з суттєвими ризиками фронтранінгу та атак типу сендвіч, особливо в протоколах децентралізованих фінансів (DeFi), які реалізовані з використанням смарт контрактів зі спільним доступом до поточного стану. Для вирішення цієї проблеми у статті запропоновано гібридний підхід до протидії MEV із використанням логічних часових міток Лампорта, спрямований на реалізацію механізму локального причинно-наслідкового впорядкування транзакцій у межах окремих смарт-контрактів.

Запропонований метод передбачає розширення кожного смарт-контракту, такого як пул ліквідності децентралізованої біржі, локальним лічильником логічних часових міток. Транзакції, що надсилаються до контракту, містять логічні часові мітки, які дозволяють забезпечити виконання транзакцій відповідно до причинно-обумовленого порядку. Важливою перевагою цього методу є те, що він не вимагає змін у глобальному механізмі консенсусу мережі Ethereum, забезпечуючи сумісність із поточною екосистемою. У роботі описано структуру рішення, розглянуто різні стратегії реалізації в межах алгоритму консенсусу, так і поза ним, а також проаналізовано стійкість до таких загроз, як маніпуляція часовими мітками.

Ключові слова: блокчейн, смарт контракти, розподілені системи, одноранговi мережі, криптографія.

CHERKAS NAZARII, BATYUK ANATOLIY
Lviv Polytechnic National University

TRANSACTION ORDERING VIA LAMPORT LOGICAL TIMESTAMPS TO MITIGATE MEV EXTRACTION IN ETHEREUM SMART CONTRACTS

The increasing prevalence of Maximal Extractable Value (MEV) in blockchain networks has highlighted critical challenges in achieving fair and predictable transaction ordering. On Ethereum, where block builders possess unrestricted control over transaction sequencing, users face significant risks from frontrunning and sandwich attacks, particularly within decentralized finance (DeFi) applications interacting with shared contract states. To address this issue, this paper proposes a hybrid MEV mitigation method employing Lamport-style logical clocks, designed to establish a local causal ordering mechanism within individual smart contracts.

The proposed approach equips each smart contract, such as a decentralized exchange liquidity pool, with a local logical timestamp counter. Transactions submitted to the contract carry logical timestamps, enabling the enforcement of a causally consistent execution order. A key benefit of this method is that it does not necessitate alterations to Ethereum's global consensus mechanism, thus ensuring compatibility with the current Ethereum ecosystem, as well as rollups and modular app-chain architectures. The study details the protocol design, explores various implementation strategies for both on-chain and off-chain execution environments, and addresses resilience against adversarial attempts such as timestamp manipulation and denial-of-service attacks.

The primary advantage of this approach lies in its effectiveness in mitigating intra-contract MEV extraction by strictly controlling transaction reordering for conflicting state interactions, while preserving concurrency for non-conflicting transactions. Findings indicate that the use of local Lamport clocks provides a practical, low-overhead solution for MEV-sensitive applications, including decentralized exchanges and rollup sequencing systems.

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

Стаття надійшла до редакції / Received 24.06.2025
Прийнята до друку / Accepted 15.08.2025

Постановка задачі

Останнім часом значно зросли масштаби явища Maximal Extractable Value (MEV), яке є джерелом додаткових прибутків для окремих учасників мереж блокчейн завдяки можливості впливати на порядок виконання транзакцій [1]. У мережі Ethereum вузли-валідатори мають повну свободу у впорядкуванні транзакцій у межах блоку, що створює суттєві ризики для користувачів через можливість проведення атак типу фронтранінг та сендвіч. Особливо актуальним це є у сфері децентралізованих фінансів (DeFi), де транзакції часто працюють із спільним станом (shared state) контрактів, що відкриває широкі можливості для маніпуляцій із порядком виконання транзакцій.

Існуючі методи боротьби з MEV, такі як шифрування транзакцій [2], пакетні аукціони [3] або поділ ролей вузлів мережі (Proposer Builder Separation, PBS) [4], мають низку обмежень, включаючи високу складність реалізації, залежність від зовнішніх компонентів або потребу в істотних змінах алгоритму консенсусу мережі. Відповідно, постає потреба в розробці ефективного і простого у

реалізації механізму, який дозволив би зменшити негативний вплив MEV екстракції, не вимагаючи при цьому суттєвих змін у загальній структурі мережі Ethereum. Метою цього дослідження є запропонувати гібридний підхід до впорядкування транзакцій на основі локальних логічних часових міток Лампорта [5], що забезпечує причинно-обумовлену послідовність виконання транзакцій і дозволяє мінімізувати MEV-екстракцію у смарт-контрактах Ethereum.

Аналіз останніх джерел

Явище Maximal Extractable Value (MEV) вперше було введено та формалізовано в публікації [1]. Ця робота всебічно аналізує вплив атак типу фронтранінг та інших стратегій маніпуляції порядком транзакцій на стабільність децентралізованих криптобірж та системні ризики роботи мережі блокчейн Ethereum. Відтоді тема MEV активно досліджується, зокрема, у таких напрямах, як підвищення точності виявлення MEV-атак, моделювання поведінки учасників у контексті MEV, а також розробка ефективних рішень для зменшення негативного впливу цього явища.

Одним із підходів до зменшення ризиків MEV є використання технологій шифрування транзакцій. Наприклад, проєкт Shutter Network [6] застосовує порогове шифрування, приховуючи деталі транзакцій до моменту їх включення у блок, що суттєво знижує можливості фронтранінгу та інших подібних атак [2]. Втім, використання такого шифрування потребує значних обчислювальних ресурсів, що може впливати на ефективність та масштабування мережі.

Іншим помітним напрямком є використання пакетних аукціонів на зразок описаного в роботі [3], де автори детально розглядають переваги цього методу, який передбачає групування транзакцій для одночасної обробки у визначені часові інтервали, знижуючи перевагу автоматизованих високочастотних ботів. Однак така модель потребує значних змін у структурі роботи бірж, що може спричинити сповільнення роботи та погіршення користувацького досвіду.

Метод Proposer-Builder Separation (PBS), вперше запропонований в публікації [4], активно застосовується в мережі Ethereum у вигляді проекту MEV-Boost [7]. В цьому методі функції формування блоків (block builders) та їх пропозиції (block proposers) розділені, що дозволяє зменшити ризики маніпуляцій із порядком транзакцій. Однак існують ризики централізації builder-операторів, що є предметом активних дискусій [8], [9].

Використання логічних часових міток, запропонованих Леслі Лампортом, також знаходить своє застосування в мереж блокчейн. Даний метод дозволяє визначити причинно-обумовлений порядок подій без глобальної синхронізації часу в розподіленій системі [5]. Сучасні блокчейн-мережі активно використовують цей підхід. Наприклад, мережа TON реалізує механізм шардинг масштабування із локальним впорядкуванням транзакцій в блоках [10], мережа Sui використовує алгоритм консенсусу Mysticeti з причинно-наслідковим впорядкуванням транзакцій [11], а в мережі Sonic вивчається впровадження направлених ациклічних графів (DAG) з локальними часовими мітками [12]. Вартими уваги також є дослідження інтегрованих рішень, які поєднують логічні часові мітки із криптографічними схемами на основі алгоритму commit-reveal та функцій перевіркової затримки [13]. Ці комбінації можуть суттєво підвищити ефективність боротьби з MEV, зберігаючи при цьому прийнятний рівень складності реалізації.

Іншим підходом до мінімізації негативних ефектів явища MEV є розробка нових алгоритмічних моделей стимулів на рівні протоколу консенсусу мережі. Прикладом такої роботи є [14], де автори представили формальні економічні моделі механізмів впорядкування транзакцій. Вони аналізують вплив специфіки механізмів впорядкування на зменшення стимулів до MEV-екстракції, вводячи поняття Incentive-Compatible Fair Ordering (ICFO). Запропоновані моделі можуть бути використані для дизайну нових протоколів децентралізованих бірж (DEX), що орієнтовані на мінімізацію MEV.

Загалом, аналіз джерел демонструє активний науковий інтерес до проблематики MEV та різноманітність запропонованих рішень, кожне з яких має власні переваги та недоліки. Нижче подано порівняльну таблицю з розглянутими методами протидії MEV екстракції, їх особливостями, перевагами та недоліками (таб. 1). Подальші дослідження повинні враховувати як технічні особливості реалізації, так і економічні й соціальні наслідки впровадження нових підходів.

Таблиця 1

Порівняльна таблиця методів протидії MEV екстракції в мережах блокчейн

Метод	Особливості	Переваги	Недоліки
Шифрування транзакцій (Shutter Network)	Порогове шифрування приховує зміст транзакцій до їх виконання	Знижує ризик MEV атак типу фронтранінг	Високі обчислювальні витрати, обмежена масштабованість
Пакетні аукціони (Batch Auctions)	Групове виконання транзакцій у фіксованих часових інтервалах	Зменшення впливу HFT-ботів, більш передбачуваний порядок	Потреба в зміні алгоритмів консенсусу, вплив на UX
Proposer-Builder Separation (PBS)	Відокремлення функцій формування блоку від його пропозиції учасникам мережі	Зменшення маніпуляцій з боку вузлів-валідаторів	Ризики централізації builder-інфраструктури

Продовження Таблиці 1

Метод	Особливості	Переваги	Недоліки
Логічні часові мітки (Lamport timestamps)	Локальний причинно-обумовлений порядок в розподіленій системі без контролю глобального часу	Не потребує змін консенсусу, підтримує паралельність	Потреба в адаптації контрактів та клієнтів
Комбінації з криптографічними commit-reveal схемами	Поєднання причинно-наслідкового впорядкування з криптографічним приховуванням	Посилений захист від MEV, гнучкість	Ускладнення логіки, можливі затримки в формуванні нових блоків
Модель стимулів з впорядкуванням ICFO	Алгоритмічні моделі чесного порядку (Incentive-Compatible Fair Ordering)	Формальна стійкість до MEV, потенціал для нових протоколів DEX	Складність реалізації на рівні консенсусу

Виклад основного матеріалу

Гібридний підхід до зменшення MEV-екстракції базується на використанні локальних логічних часових міток Лампорта [5] для впорядкування транзакцій у межах окремих смарт-контрактів. Метод спрямовано на забезпечення причинно-обумовленого порядку виконання транзакцій, зокрема у протоколах децентралізованих фінансів (DeFi), де транзакції як правило працюють зі спільним станом (shared state), що створює можливості для MEV атак типу фронтранінг та сендвіч [15].

Ключова ідея підходу полягає у розширенні кожного смарт-контракту локальним лічильником логічного часу ℓ, який оновлюється згідно з правилами Лампорта. Кожна транзакція T_i повинна включати логічну часову мітку ℓ_i, яка відображає її локальний причинно-обумовлений порядок в межах взаємодії зі смарт-контрактом. Виконання дозволяється лише тоді, коли $\ell_i \geq \ell_{curr}$, де ℓ_{curr} – поточне значення локального лічильника контракту. Оновлення значення здійснюється за формулою: $\ell_{new} = \max(\ell_i,\ \ell_{curr}) + 1$. Цей механізм гарантує, що транзакції, які мають причинно-наслідковий зв'язок (наприклад, залежність від стану контракту, що змінюється), будуть виконуватись у правильному порядку. Водночас, транзакції без конфліктів можуть виконуватись паралельно, що зберігає ефективність мережі. Перевагою логічних міток є відсутність потреби у глобальній синхронізації часу або координуючих вузлах, що підвищує децентралізацію й стійкість системи.

Для подальшої формалізації вводимо частковий порядок транзакцій $T_i < T_j$, якщо $\ell_i < \ell_j$ і T_i та T_j конфліктують за стан контракту. Наприклад, транзакція T_i оновлює баланс у пулі ліквідності, а інша транзакція T_j читає цей баланс. Без правильного порядку T_j може використовувати неактуальний стан, що відкриває можливість для MEV екстракції. Встановлюючи $T_i < T_j$, гарантується послідовне виконання у межах одного контракту. Також представимо граф виконання транзакцій як орієнтований ациклічний граф $G = (V, E)$, де:

- V – множина транзакцій T_i
- $E: T_i \to T_j$, якщо $\ell_i < \ell_j$ і транзакції мають спільний стан

Цей граф дає змогу візуально представити порядок виконання, що є частково впорядкованим, оскільки не всі транзакції цього потребують. Блок-схему обробки транзакцій в смарт контракті подано на рис. 1:

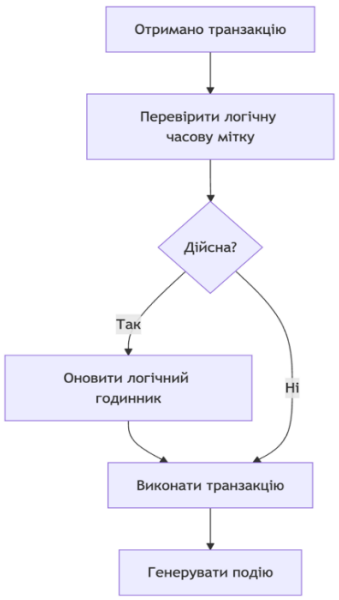

Рис. 1. Блок-схема обробки транзакцій смарт контрактом з використанням часових міток Лампорта

Як згадано вище, у запропонованій архітектурі реалізація здійснюється на рівні окремих смарт-контрактів. Контракт містить внутрішню змінну ℓ – логічний лічильник, а кожна функція, яка змінює стан, перевіряє коректність мітки перед виконанням. Якщо умова $\ell_i \geq \ell_{curr}$ не виконується – транзакція відхиляється (рис. 2). Також, реалізація може бути розширена шляхом зберігання локальних міток для кожного користувача, що забезпечує більш гнучке обмеження доступу до функцій контракту.

```
// Глобальний лічильник для контракту
uint256 public lamportClock;

// Індивідуальні лічильники для кожного користувача
mapping(address => uint256) public userClocks;

// Оновлення стану з перевіркою глобального лічильника
function update(uint256 providedClock) external {
    require(providedClock >= lamportClock, "Stale transaction");
    lamportClock = providedClock + 1;
    // виконання логіки контракту
}

// Операції з перевіркою індивідуального лічильника користувача
function act(uint256 providedClock) external {
    require(providedClock >= userClocks[msg.sender], "Clock too old");
    userClocks[msg.sender] = providedClock + 1;
    // виконання користувацької логіки
}
```

Рис. 2. Приклад інтеграції часових міток Лампорта в код смарт контракту мовою Solidity

Важливою перевагою такого механізму є можливість індивідуалізованого впорядкування, яке дозволяє зберігати причинно-наслідкову послідовність навіть у середовищах з великою кількістю одночасних користувачів. У більш складних системах, зокрема в автоматизованих маркет-мейкерах (AMM), що працюють з кількома парами криптоактивів, логічні мітки можуть застосовуватись не на рівні користувача чи контракту загалом, а безпосередньо на рівні окремих ресурсів — наприклад, конкретних пулів ліквідності. У практичному контексті, DeFi-протоколи зазвичай реалізуються як набір взаємопов'язаних смарт-контрактів. У таких випадках логічні мітки можуть передаватися між контрактами за допомогою внутрішніх викликів, забезпечуючи наскрізне причинно-наслідкове впорядкування в складних сценаріях, таких як композиції DeFi протоколів або арбітраж між різними парами криптоактивів.

Стійкість рішення до MEV атак типу фронтранінг та сендвіч.

MEV атаки типу фронтранінг у контексті Ethereum найчастіше реалізуються через спостереження за чергою очікування (мемпулом) та випереджальну відправку транзакцій з вищою комісією. При використанні логічних часових міток та забезпечені причинно-наслідкового впорядкування, зловмисник не може заздалегідь згенерувати допустиму мітку, оскільки вона залежить від значення, яке буде оновлено лише після обробки попередньої транзакції (включені її в наступний блок). Оскільки сендвіч-атака вимагає, щоб атакуальні транзакції T_{pre} і T_{post} були розміщені навколо цільової T_v, за відсутності доступу до внутрішнього стану контракту в момент виконання, зловмисник не може ані передбачити мітку ℓ_v, ані узгодити свої транзакції з нею. Як наслідок, одна або обидві з транзакцій T_{pre}, T_{post} не задовольнятимуть умову $\ell_i \geq \ell_{curr}$, що призведе до їх скасування. Відтак, будь-яка спроба фронтранінгу буде виявлена як така, що містить «застарілу» мітку, і буде відхилена контрактом згідно правила $\ell_{adv} < \ell_i \Rightarrow T_{adv} < T_i$. Таким чином, запровадження локального причинно-наслідкового впорядкування є ефективною стратегією для обмеження цих класів MEV атак, не змінюючи механізму консенсусу мережі блокчейн.

Приклади використання в протоколах децентралізованих фінансів (DeFi)

У Uniswap V3 [16] кожна своп-операція змінює стан пулу, що робить її вразливою до спекуляцій поточною ціною. Інтеграція логічних міток дозволяє перевірити правильність порядку виконання. Наприклад, користувач може здійснити виклик методу смарт контракту вказуючи своє значення часової мітки, а контракт відповідно дозволяє обробку тільки тоді, коли ця мітка дорівнює або перевищує поточну (рис. 3).

Протокол децентралізованої біржі Curve [17] використовує математичні моделі на основі так званих «плавних» кривих (smooth curves) – для визначення обмінного курсу між активами залежно від їхніх обсягів в пулі ліквідності. Ці криві забезпечують поступову зміну цін, мінімізуючи різкі коливання, але водночас роблять пул чутливим до будь-яких маніпуляцій із порядком транзакцій. Зокрема, арбітражні MEV стратегії можуть скористатися миттєвими змінами стану пулу задля одержання прибутку. Інтеграція логічних часових міток у своп-операції або в функції зміни ліквідності дозволяє гарантувати, що транзакції обробляються в узгодженій і передбачуваній послідовності. Це знижує ризик несанкціонованих дій, які могли б порушити фінансову рівновагу пулу ліквідності децентралізованої криптобіржі.

```solidity
// Глобальний логічний лічильник Лампорта для контролю порядку виконання
uint256 public lamportClock;

// Функція обміну активів у пулі з перевіркою логічної мітки
function swap(uint256 lamportTag, address tokenIn, address tokenOut, uint256 amountIn) external
{
    // Перевірка: мітка має бути не менша за поточне значення лічильника
    require(lamportTag >= lamportClock, "Out of order");

    // Оновлення лічильника Лампорта
    lamportClock = lamportTag + 1;

    // Перевірка балансу відправника (для прикладу)
    require(IERC20(tokenIn).balanceOf(msg.sender) >= amountIn, "Insufficient balance");

    // Переведення токенів до контракту
    IERC20(tokenIn).transferFrom(msg.sender, address(this), amountIn);

    // Логіка обміну: визначення суми на виході, обмін, переказ назад
    uint256 amountOut = getAmountOut(tokenIn, tokenOut, amountIn);
    IERC20(tokenOut).transfer(msg.sender, amountOut);

    // Подія для фіксації обміну
    emit SwapExecuted(msg.sender, tokenIn, tokenOut, amountIn, amountOut);
}

// Визначення суми на виході — спрощено
function getAmountOut(address tokenIn, address tokenOut, uint256 amountIn) internal view
returns (uint256) {
    // Може базуватись на співвідношенні резервів, формулі XY=K, тощо
    return amountIn * 99 / 100; // наприклад, з урахуванням 1% комісії
}

// Подія для журналу
event SwapExecuted(address indexed user, address tokenIn, address tokenOut, uint256 amountIn,
uint256 amountOut);
```

Рис. 3. Метод смарт контракту Uniswap V3 на мові Solidity з перевіркою часових міток

У протоколі Balancer [18], де частки активів у пулі можуть змінюватися за попередньо визначеними алгоритмами або відповідно до рішень, прийнятих учасниками протоколу, правильність порядку транзакцій також має критичне значення. Використання логічних міток гарантує, що лише ті транзакції, які не порушують логіку послідовних змін у складі пулу, будуть виконані. Це унеможливлює навмисне розміщення транзакцій поза контекстом змін, що допомагає захистити протокол від потенційної маніпуляції з боку експлуатантів явища MEV.

Якщо ж говорити про потенційних труднощі, впровадження логічних міток потребує оновлення користувацьких інтерфейсів та клієнтів, що генерують транзакції. Зокрема, користувачам потрібно буде «вгадати» правильну мітку або використовувати проміжний компонент (middleware), який взаємодіє з контрактом, запитуючи останнє значення логічної часової мітки.

Висновки

У цьому дослідженні було запропоновано новий підхід до зменшення впливу явища Maximal Extractable Value (MEV) у мережі Ethereum, що базується на локальному причинно-наслідковому впорядкуванні транзакцій за допомогою логічних часових міток Лампорта. Запропонований механізм дозволяє реалізувати частковий порядок транзакцій у межах смарт-контрактів, не змінюючи глобального механізму консенсусу. Такий підхід не лише знижує ризики фронтранінгу та сендвіч-атак, а й підтримує паралельність виконання неконфліктних транзакцій, що є критично важливим для збереження масштабованості та ефективності мережі.

Реалізація запропонованого рішення можлива без втручання в базову інфраструктуру Ethereum. Смарт-контракти можуть самостійно керувати логічними мітками, перевіряючи їх актуальність під час виконання кожної транзакції. Показано, що цей підхід добре інтегрується в існуючі протоколи децентралізованих бірж (Uniswap, Curve, Balancer) і може бути використаний для підвищення їхньої стійкості до маніпуляцій порядком виконання транзакцій та відповідно MEV атак. Отримані результати підтверджують ефективність запропонованого методу як на теоретичному, так і на прикладному рівні, а блок-схеми та логіка впровадження у вигляді псевдокоду надають практичний інструмент для розробників протоколів.

Подальші дослідження мають бути зосереджені на формальній верифікації властивостей часових міток у контексті специфіки EVM, перевірці на сумісність із L2-протоколами, а також на розробці middleware-компонентів, які автоматично визначають правильну логічну мітку для транзакції. Крім того, перспективним є поєднання каузального впорядкування з іншими методами захисту від MEV – такими як пакетні аукціони та шифрування за схемою commit-reveal. Таким чином, локальне впорядкування транзакцій за логічними мітками Лампорта становить ефективну та практичну відповідь на проблему MEV, відкриваючи шлях до побудови більш стійких та прозорих децентралізованих систем.

Література

1. P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, i A. Juels Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges / P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, i A. Juels. - Квіт 2019. - .

2. S. Dziembowski, S. Faust, i J. Luhn Private Transactions from Threshold Cryptography / S. Dziembowski, S. Faust, i J. Luhn. - .

3. E. Budish Peter Cramton John Shim, S. Athey, L. Ausubel, E. Aze-vedo, S. Barkai, B. Charoenwong, A. Clark-Joseph, J. Cochrane, D. Diamond, D. Duffie, G. Fama, D. Farmer, T. Foucault, A. Fran-kel, M. Gentzkow, L. Glosten, T. Hendershott, A. Hortacsu, L. Jakab, E. Kamenica, B. Kelly, P. Kyle, J. Levin, D. MacKenzie, G. Matvos, A. Menkveld, P. Milgrom, T. Moskowitz, M. Notowidigdo, M. Ostrovsky, D. Parkes, C. Prendergast, A. Roth, G. Saar, J. Shapiro, S. Skouras, A. Skrzypacz, C. Spatt, L. Stole, G. Swerdlin, R. Thaler, B. Weller, M. Wellman, B. Wilson We thank Daniel Davidson, M. Wong, i R. Yang THE HIGH-FREQUENCY TRADING ARMS RACE: FREQUENT BATCH AUCTIONS AS A MARKET DESIGN RESPONSE* / E. Budish Peter Cramton John Shim, S. Athey, L. Ausubel, E. Aze-vedo, S. Barkai, B. Charoenwong, A. Clark-Joseph, J. Cochrane, D. Diamond, D. Duffie, G. Fama, D. Farmer, T. Foucault, A. Fran-kel, M. Gentzkow, L. Glosten, T. Hendershott, A. Hortacsu, L. Jakab, E. Kamenica, B. Kelly, P. Kyle, J. Levin, D. MacKenzie, G. Matvos, A. Menkveld, P. Milgrom, T. Moskowitz, M. Notowidigdo, M. Ostrovsky, D. Parkes, C. Prendergast, A. Roth, G. Saar, J. Shapiro, S. Skouras, A. Skrzypacz, C. Spatt, L. Stole, G. Swerdlin, R. Thaler, B. Weller, M. Wellman, B. Wilson We thank Daniel Davidson, M. Wong, i R. Yang. - Q J Econ. - вип. 130, 2015. - с. 1547–1621.

4. State of research: increasing censorship resistance of transactions under proposer/builder separation (PBS) - HackMD / . [Online]. Available: https://notes.ethereum.org/@vbuterin/pbs_censorship_resistance. [Accessed: 12-Чер-2025].

5. L. Lamport Operating R. Stockton Gaines Systems Editor Time, Clocks, and the Ordering of Events in a Distributed System / L. Lamport. - 1978. - .

6. Shutter | The Highest Standard of Privacy and Fairness. / . [Online]. Available: https://www.shutter.network/. [Accessed: 12-Чер-2025].

7. MEV-Boost in a Nutshell / . [Online]. Available: https://boost.flashbots.net/. [Accessed: 13-Сер-2023].

8. L. Heimbach, L. Kiffer, C. F. Torres, i R. Wattenhofer Ethereum's Proposer-Builder Separation: Promises and Realities / L. Heimbach, L. Kiffer, C. F. Torres, i R. Wattenhofer. - Трав 2023. - .

9. T. Gupta, M. M. Pai B, i M. Resnick THE CENTRALIZING EFFECTS OF PRIVATE ORDER FLOW ON PROPOSER-BUILDER SEPARATION / T. Gupta, M. M. Pai B, i M. Resnick. - .

10. Shards | The Open Network / . [Online]. Available: https://docs.ton.org/v3/documentation/smart-contracts/shards/shards-intro. [Accessed: 12-Чер-2025].

11. S. Blackshear, A. Chursin, G. Danezis, X. Li, M. Logan, A. Menon, T. Nowacki, A. Sonnino, B. Williams, L. Zhang, A. Kichidis, L. Kokoris-Kogias, i S. Lutris Sui Lutris: A Blockchain Combining Broadcast and Consensus / S. Blackshear, A. Chursin, G. Danezis, X. Li, M. Logan, A. Menon, T. Nowacki, A. Sonnino, B. Williams, L. Zhang, A. Kichidis, L. Kokoris-Kogias, i S. Lutris. - Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24), October 14â•fi18, 2024, Salt Lake City, UT, USA. - вип. 1, .

12. S.-M. Choi, J. Park, Q. Nguyen, i A. Cronje FANTOM: A SCALABLE FRAMEWORK FOR ASYNCHRONOUS DISTRIBUTED SYSTEMS A PREPRINT / S.-M. Choi, J. Park, Q. Nguyen, i A. Cronje. - вип. 25, 2018. - .

13. D. Boneh, J. Bonneau, B. Bünz, i B. Fisch Verifiable Delay Functions / D. Boneh, J. Bonneau, B. Bünz, i B. Fisch. - 2019. - .

14. Babu Pillai Blockchain MEV minimisation solution with price guarantee / Babu Pillai. - 2022. - .

15. N. S. Cherkas i A. Ye. Batyuk Maximal extractable value (mev) in blockchain networks and its impact on blockchain ecosystem / N. S. Cherkas i A. Ye. Batyuk. - Ukrainian Journal of Information Technology. - вип. 5, вип. 2, 2023. - с. 60–71.

16. Home | Uniswap Protocol / . [Online]. Available: https://uniswap.org/. [Accessed: 13-Сер-2023].

17. Swap - Curve / . [Online]. Available: https://curve.fi/#/ethereum/swap. [Accessed: 13-Сер-2023].

18. Balancer DeFi AMMs made easy / . [Online]. Available: https://balancer.fi/. [Accessed: 12-Чер-2025].