НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

«На правах рукопису»
УДК 004.056.5:519.2+519.7

«До захисту допущено»
В.о. завідувача кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2025 р.

Дипломна робота

на здобуття ступеня магістра
за освітньо-професійною програмою
«Математичні методи криптографічного захисту інформації»
зі спеціальності: 113 Прикладна математика
на тему: **«Аналіз залежності часу обробки транзакції від її параметрів для різних типів протоколів консенсусу в блокчейні»**

Виконав:
студентка II курсу, групи ФІ-32мн
Коваленко Дар'я Юріївна _____

Керівник:
професор кафедри ММЗІ
ННФТІ КПІ ім.Ігоря Сікорського,
д.т.н.,професор
Ковальчук Людмила Василівна _____

Консультант:
аспірант кафедри ММЗІ
ННФТІ КПІ ім.Ігоря Сікорського
Вихло Антон Андрійович _____

Рецензент:
доцент кафедри ІБ
ННФТІ КПІ ім.Ігоря Сікорського
Барановський Олексій Миколайович _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студентка _____

Київ — 2025

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

Рівень вищої освіти — другий (магістерський)
Спеціальність — 113 Прикладна математика,
ОПП «Математичні методи криптографічного захисту інформації»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2025 р.

ЗАВДАННЯ
на дипломну роботу

Студентка: Коваленко Дар'я Юріївна

1. Тема роботи: «*Аналіз залежності часу обробки транзакції від її параметрів для різних типів протоколів консенсусу в блокчейні*», науковий керівник дипломної роботи: професор кафедри ММЗІ

ННФТІ КПІ ім.Ігоря Сікорського,

д.т.н.,професор Ковальчук Людмила Василівна,

затверджені наказом по університету №__ від «__» _____ 2025 р.

2. Термін подання студентом роботи: «__» _____ 2025 р.

3. Об'єкт дослідження: процеси обробки та пріоритизації транзакцій у блокчейн-мережах з різними протоколами консенсусу та їх вразливість до атак випередження.

4. Предмет дослідження: математичні моделі та кількісні характеристики залежності часу обробки транзакцій від розміру комісії та їх вплив на ефективність атак випередження в блокчейн-мережах з різними протоколами консенсусу.

5. Перелік завдань: провести аналіз наукової літератури та технічної документації щодо механізмів обробки транзакцій у блокчейн-мережах з різними протоколами консенсусу; формалізувати математичні моделі атак

випередження та визначити фактори, що впливають на їх ефективність; розробити методологію збору та обробки емпіричних даних для дослідження залежності часу обробки транзакцій від розміру комісії; сформувати репрезентативні вибірки транзакцій для блокчейн-мереж з різними протоколами консенсусу (PoW, PoS, протоколи з секвенсорами); дослідити наявність та силу статистичного зв'язку між розміром комісії транзакції та часом її обробки для кожного типу протоколу; визначити математичні моделі, що найбільш точно описують виявлені залежності, та оцінити їхні параметри; розробити та формалізувати модель ймовірності успіху атаки випередження в умовах різних співвідношень кількості транзакцій у мемпулі та розміру блоку; провести порівняльний аналіз вразливості різних типів протоколів консенсусу до атак випередження на основі емпіричних даних; розробити алгоритм вибору оптимальної стратегії захисту від атак випередження з урахуванням характеру залежності часу обробки від комісії та стану мемпулу.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу: Презентація доповіді.

7. Орієнтовний перелік публікацій: планується доповідь на всеукраїнській конференції.

8. Дата видачі завдання: 10 вересня 2024 р.

Календарний план

Студент	_____	Коваленко Д.Ю.
Керівник	_____	Ковальчук Л.В.

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання	Примітка
1	Узгодження теми роботи із науковим керівником	01-15 вересня 2024 р.	Виконано
2	Опрацювання наукової літератури та технічної документації щодо блокчейн-технологій та протоколів консенсусу	Вересень-жовтень 2024 р.	Виконано
3	Розробка методології збору та аналізу даних про транзакції в різних блокчейн-мережах	Жовтень - листопад 2024	Виконано
4	Збір та формування вибірок транзакцій для блокчейн-мереж з протоколами PoW, PoS та секвенсорами. Проведення статистичного аналізу залежностей між комісією та часом обробки транзакцій	Січень - лютий 2025	Виконано
5	Формалізація моделей атак випередження та розробка методології оцінки ймовірності їх успіху при різних співвідношеннях M/N. Побудова та оцінка параметрів математичних моделей для різних типів протоколів. Розробка методики аналізу вразливості блокчейн-систем до атак випередження на основі статистичного визначення характеру залежності між комісією та часом обробки.	Лютий - Березень 2025	Виконано
6	Порівняльний аналіз результатів для різних типів протоколів та формулювання висновків	Березень - квітень 2025	Виконано
7	Оформлення та захист дипломної роботи	Квітень-травень 2025	Виконано

РЕФЕРАТ

Кваліфікаційна робота містить: 99 стор., 4 рисунки, 4 таблиці, 15 джерел, 0 додатків.

Дане дослідження було проведено з метою встановлення характеру та кількісних характеристик залежності часу обробки транзакцій від розміру комісії для різних типів протоколів консенсусу в блокчейн-мережах та оцінки їх вразливості до атак випередження.

Об'єктом дослідження є процеси обробки транзакцій у блокчейн-мережах з різними протоколами консенсусу (Proof of Work, Proof of Stake, протоколи з секвенсорами) та взаємозв'язок між параметрами транзакцій і їх вразливістю до атак випередження. У ході роботи було проведено порівняльне дослідження блокчейн-мереж з протоколами консенсусу типу Proof of Work, Proof of Stake та протоколів з секвенсорами. Розроблено методологію збору та статистичної обробки даних для аналізу залежності часу обробки транзакцій від розміру комісії. Зібрано та опрацьовано вибірку з понад 1,1 млн транзакцій.

Досліджено математичні моделі атак випередження, розроблено методологію оцінки ймовірності їх успіху в залежності від характеристик блокчейн-мережі. Запропоновано методику оцінки ризиків атак випередження, яка передбачає: визначення наявності залежності між комісією та часом обробки, застосування відповідних математичних моделей залежно від результатів аналізу, та обчислення ймовірності успіху атаки з урахуванням поточного стану мемпулу.

Практичне значення результатів полягає в можливості їх використання для оптимізації параметрів транзакцій користувачами блокчейн-мереж, мінімізації ризику успішних атак випередження через застосування розроблених теорем і алгоритмів, а також вдосконалення протоколів консенсусу розробниками.

БЛОКЧЕЙН, ПРОТОКОЛИ КОНСЕНСУСУ, PROOF OF WORK,

PROOF OF STAKE, СЕКВЕНСОРИ, КОМІСІЯ ТРАНЗАКЦІЇ, ЧАС ОБРОБКИ, АТАКИ ВИПЕРЕДЖЕННЯ, МЕМПУЛ

ABSTRACT

The qualification work contains: 99 pages, 4 figures, 4 tables, 15 sources, 0 appendices.

This research was conducted to establish the nature and quantitative characteristics of the dependence of transaction processing time on fee size for different types of consensus protocols in blockchain networks and to assess their vulnerability to frontrunning attacks.

The object of research is transaction processing in blockchain networks with different consensus protocols (Proof of Work, Proof of Stake, protocols with sequencers) and the relationship between transaction parameters and their vulnerability to frontrunning attacks. During the work, a comparative study of blockchain networks with Proof of Work, Proof of Stake, and sequencer-based consensus protocols was conducted.

A methodology for collecting and statistical processing of data was developed to analyze the dependence of transaction processing time on fee size. A sample of over 1.1 million transactions was collected.

Mathematical models of frontrunning attacks were studied, and a methodology for estimating the probability of their success depending on the characteristics of the blockchain network was developed. A methodology for assessing the risks of frontrunning attacks was proposed, which includes: determining the existence of a dependency between the fee and processing time, applying appropriate mathematical models depending on the analysis results, and calculating the probability of attack success taking into account the current state of the mempool.

The practical significance of the results lies in the possibility of using them to optimize transaction parameters by blockchain network users, minimize the risk of successful frontrunning attacks through the application of the developed theorems and algorithms, and improve consensus protocols by developers.

BLOCKCHAIN, CONSENSUS PROTOCOLS, PROOF OF WORK,

PROOF OF STAKE, SEQUENCERS, TRANSACTION FEE, PROCESSING TIME, FRONTRUNNING ATTACKS, MEMPOOL

ЗМІСТ

Перелік умовних позначень, скорочень і термінів 12
Вступ 14
1 ОСНОВНІ ТЕОРЕТИЧНІ ПОНЯТТЯ БЛОКЧЕЙНУ 18
1.1 Опис технології блокчейн 18
1.1.1 Структура блоку та механізми формування ланцюга 20
1.1.2 Механізми формування ланцюга 22
1.1.3 Криптографічні хеш-функції 25
1.2 Смарт-контракти 27
1.3 Аналіз протоколів консенсусу в блокчейн-мережах 29
1.3.1 Протокол Proof of Work (PoW) 31
1.3.2 Протокол Proof of Stake (PoS) 34
1.3.3 Протоколи з секвенсорами (Layer 2 рішення) 38
1.4 Математичні моделі обробки транзакцій у блокчейн-мережах 42
1.4.1 Теорія черг у контексті блокчейн-транзакцій 42
1.4.2 Ймовірнісні моделі включення транзакцій у блоки 43
1.4.3 Фактори, що впливають на час обробки транзакцій 44
1.5 Залежність часу обробки транзакцій від розміру комісії 44
1.5.1 Теоретичні моделі залежності 44
1.5.2 Вплив навантаження на мережу 45
Висновки до розділу 1 46
2 ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ЗАЛЕЖНОСТІ ЧАСУ ОБРОБКИ ВІД КОМІСІЇ 48
2.1 Теоретична модель атаки випередження 48
2.1.1 Сутність та типи атак випередження 49
2.1.2 Формалізація моделі атаки заміщення 50
2.1.3 Формалізація моделі атаки вставки 52
2.1.4 Вплив параметрів мережі на ймовірність успіху атаки 54
2.2 Методологія дослідження залежності часу обробки від комісії 55

2.2.1 Вибір блокчейн-мереж для дослідження 55
2.2.2 Методи збору даних 56
2.2.3 Методи попередньої обробки та фільтрації даних 57
2.2.4 Методи статистичного аналізу 58
2.3 Зв'язок між атаками випередження та залежністю часу обробки від комісії 59
2.3.1 Теоретичні передумови впливу часу обробки на успішність атаки 59
2.3.2 Значення залежності часу-комісії для оцінки вразливості мережі 61
2.3.3 Обґрунтування важливості емпіричного дослідження 62
Висновки до розділу 2 63
3 ТЕОРЕТИЧНІ ТА ЕМПІРИЧНІ РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ АТАК ВИПЕРЕДЖЕННЯ 65
3.1 Обчислення ймовірності випередження транзакції 65
3.1.1 Модель ймовірності випередження при повному включенні транзакцій у блок ($M \leqslant N$) 67
3.1.2 Модель ймовірності випередження при обмеженні розміром блоку ($M > N$) 69
3.1.3 Аналітичні приклади для моделі з $M > N$ при різних співвідношеннях M/N 72
3.2 Аналіз отриманих результатів 78
3.3 Розрахунок та інтерпретація коефіцієнтів кореляції 80
3.3.1 Коефіцієнт кореляції Пірсона 80
3.3.2 Коефіцієнт кореляції Спірмена 81
3.3.3 Коефіцієнт кореляції Кендалла 82
3.3.4 Порівняння та інтерпретація різних коефіцієнтів кореляції 83
3.4 Побудова регресійних моделей 85
3.5 Алгоритм вибору оптимальної стратегії захисту від атак випередження 89
Висновки до розділу 3 92

Висновки 94

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

API (Application Programming Interface) – інтерфейс програмування додатків, набір визначень взаємодії різнотипного програмного забезпечення.

BTC – Bitcoin, перша та найвідоміша криптовалюта.

DApp (Decentralized Application) – децентралізований додаток, що працює на блокчейн-платформі.

DeFi (Decentralized Finance) – децентралізовані фінанси, сукупність фінансових додатків на блокчейні.

ETH – Ethereum, блокчейн-платформа з підтримкою смарт-контрактів.

Layer 2 – технологічні рішення другого рівня, що працюють поверх основного блокчейну для підвищення масштабованості.

MSE (Mean Squared Error) – середньоквадратична помилка, міра точності статистичної моделі.

PoS (Proof of Stake) – доказ частки володіння, один з механізмів консенсусу в блокчейні.

PoW (Proof of Work) – доказ виконаної роботи, механізм консенсусу в блокчейні.

R^2 – коефіцієнт детермінації, статистичний показник, що відображає частку дисперсії залежної змінної, пояснену моделлю.

TPS (Transactions Per Second) – кількість транзакцій за секунду, показник продуктивності блокчейн-мережі.

MEV-боти (Miner Extractable Value) – автоматизовані програми, які аналізують мемпул блокчейну й маніпулюють порядком або включенням транзакцій у блоки, щоб отримати додатковий прибуток через арбітраж, атаки випереджння чи сендвіч-атаки.

ϕ (фі) – розмір комісії за транзакцію.

T – час обробки транзакції (час до включення в блок).

ρ (ро) – коефіцієнт кореляції Спірмена.

τ (тау) – коефіцієнт кореляції Кендалла.

χ^2(хі-квадрат) – статистичний критерій для перевірки гіпотез про відповідність емпіричного розподілу теоретичному.

Блок – сукупність транзакцій, що розглядаються як одиниця обробки в блокчейн-мережі.

Блокчейн – розподілена база даних, що зберігає інформацію про всі транзакції учасників системи у вигляді "ланцюжка блоків".

Валідатор – учасник блокчейн-мережі, який підтверджує транзакції в системах з протоколом PoS.

Комісія – плата за проведення транзакції в блокчейн-мережі.

Майнер – учасник блокчейн-мережі, який підтверджує транзакції в системах з протоколом PoW.

Мемпул (mempool) – пул непідтверджених транзакцій, які очікують на включення в блок.

Протокол консенсусу – механізм досягнення згоди щодо стану блокчейну серед учасників мережі.

Секвенсор – компонент Layer 2 рішень, відповідальний за упорядкування та групування транзакцій перед їх обробкою.

Смарт-контракт – програмний код, що автоматично виконується в блокчейн-мережі при виконанні визначених умов.

Транзакція – мінімальна операційна одиниця в блокчейн-мережі, що представляє певну дію (переказ коштів, виклик смарт-контракту тощо).

Атака випередження (frontrunning) – маніпуляція порядком обробки транзакцій з метою отримання вигоди.

ВСТУП

Актуальність дослідження. Блокчейн-технології стали однією з найвпливовіших інновацій останніх років, трансформуючи численні галузі завдяки забезпеченню безпеки та прозорості транзакцій без централізованих посередників. Різноманітні протоколи консенсусу – Proof of Work (PoW), Proof of Stake (PoS) та протоколи з секвенсорами – мають власні особливості обробки транзакцій, що впливають на їх ефективність та безпеку.

Користувачі блокчейн-платформ щодня стикаються з необхідністю визначення оптимального розміру комісії для транзакцій, прагнучи мінімізувати витрати, забезпечити швидку обробку та захист від атак. Атаки випередження, при яких зловмисник маніпулює порядком обробки транзакцій, становлять серйозну загрозу, завдаючи значних фінансових збитків. Згідно з дослідженнями, щомісяця відбуваються тисячі таких атак, а їх вартість сягає мільйонів доларів.

Існує фундаментальна гіпотеза про зворотну залежність між комісією транзакції (ϕ) та часом її обробки (T): при збільшенні комісії очікується зменшення часу обробки. Проте характер цієї залежності відрізняється для різних протоколів консенсусу. Для PoW-блокчейнів ця залежність може бути значною через економічні стимули майнерів. У PoS-системах вона може бути менш вираженою через детерміновані слоти для блоків. А в протоколах із секвенсорами комісія може мати мінімальний вплив через алгоритми пакетної обробки.

Важливим є також аналіз випадків, коли залежність часу від комісії стає невираженою. У таких умовах вразливість до атак визначається ймовірнісними моделями, пов'язаними зі співвідношенням кількості транзакцій у мемпулі (M) та розміру блоку (N).

Попри зростаючу популярність блокчейн-технологій, математичні моделі, що описують взаємозв'язок між параметрами транзакцій,

швидкістю їх обробки та вразливістю до атак випередження, залишаються недостатньо дослідженими. Тому актуальним є формальне кількісне дослідження цих залежностей та їх впливу на безпеку різних типів блокчейн-мереж.

Мета дослідження полягає у встановленні характеру та кількісних характеристик залежності часу обробки транзакцій від розміру комісії для різних типів протоколів консенсусу в блокчейн-мережах та оцінці їх вразливості до атак випередження.

Для досягнення поставленої мети сформульовано такі **завдання**:

1) Провести критичний аналіз наукової літератури та технічної документації щодо механізмів обробки транзакцій у блокчейн-мережах з різними протоколами консенсусу.

2) Формалізувати математичні моделі атак випередження та визначити фактори, що впливають на їх ефективність.

3) Розробити методологію збору та обробки емпіричних даних для дослідження залежності часу обробки транзакцій від розміру комісії.

4) Сформувати репрезентативні вибірки транзакцій для блокчейн-мереж з різними протоколами консенсусу.

5) Дослідити наявність та силу статистичного зв'язку між розміром комісії транзакції та часом її обробки для кожного типу протоколу.

6) Визначити математичні моделі, що найбільш точно описують виявлені залежності, та оцінити їхні параметри.

7) Розробити та формалізувати модель ймовірності успіху атаки випередження в умовах різних співвідношень кількості транзакцій у мемпулі та розміру блоку.

8) Провести порівняльний аналіз вразливості різних типів протоколів консенсусу до атак випередження на основі емпіричних даних.

9) Розробити методику оцінки вразливості до атак випередження, що дозволяє: визначити наявність залежності між комісією та часом обробки для конкретного блокчейну, обчислити ймовірність успіху атаки за відповідними математичними моделями з урахуванням стану мемпулу,

та надати користувачу кількісні показники ризику для прийняття обґрунтованого рішення.

Об'єктом дослідження є процеси обробки транзакцій у блокчейн-мережах з різними протоколами консенсусу (Proof of Work, Proof of Stake, протоколи з секвенсорами) та взаємозв'язок між параметрами транзакцій і їх вразливістю до атак випередження.

Предметом дослідження є математичні моделі та кількісні характеристики залежності часу обробки транзакцій від розміру комісії та їх вплив на ефективність атак випередження в блокчейн-мережах з різними протоколами консенсусу.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: теорія ймовірностей, математична статистика, кореляційний та регресійний аналіз, теорія черг, аналіз часових рядів, методи емпіричного аналізу даних.

Наукова новизна отриманих результатів полягає в тому, що:

1) Вперше формалізовано математичні моделі оцінки ймовірності успіху атаки випередження в умовах різних співвідношень кількості транзакцій у мемпулі (M) та розміру блоку (N);

2) Розроблено методологію емпіричного дослідження залежності часу обробки транзакцій від розміру комісії з урахуванням особливостей різних протоколів консенсусу;

3) Встановлено характер залежності часу обробки від комісії для блокчейнів з різними протоколами консенсусу;

4) Розроблено методику аналізу вразливості блокчейн-систем до атак випередження, що ґрунтується на: статистичному визначенні наявності залежності між комісією та часом обробки для конкретного блокчейну; застосуванні відповідних імовірнісних моделей залежно від результатів аналізу – формул з дослідження [1] при наявності залежності або розроблених теоретичних моделей при випадковому порядку включення транзакцій; обчисленні ймовірності успіху атаки випередження для оцінки ризиків та прийняття користувачем рішення

щодо параметрів транзакції.

Практичне значення результатів полягає в можливості їх використання для оптимізації параметрів транзакцій користувачами блокчейн-мереж, мінімізації ризику успішних атак випередження через застосування розроблених теорем і алгоритмів, а також вдосконалення протоколів консенсусу розробниками.

1 ОСНОВНІ ТЕОРЕТИЧНІ ПОНЯТТЯ БЛОКЧЕЙНУ

У даному розділі представлено теоретичний фундамент блокчейн-технологій, розкрито їхні базові принципи функціонування, особливості різних типів протоколів консенсусу та математичні моделі обробки транзакцій. Аналіз зосереджено на характеристиках, які безпосередньо впливають на процеси обробки транзакцій та можуть зумовлювати відмінності у залежності часу обробки від параметрів транзакцій для різних типів блокчейн-мереж.

1.1 Опис технології блокчейн

Блокчейн-технологія є одним із найбільш революційних інноваційних рішень останніх десятиліть у сфері інформаційних технологій. Її розвиток пройшов значний еволюційний шлях від теоретичної концепції до практичної реалізації в різноманітних галузях, особливо у фінансах та управлінні даними.

Історично концепція блокчейну започаткована у 1991 році науковцями Стюартом Хабером та Скоттом Сторнеттою, які розробили систему криптографічно захищених блоків, де кожен новий блок містив посилання на попередній. Проте справжній прорив відбувся у 2008 році, коли було опубліковано працю «Bitcoin: A Peer-to-Peer Electronic Cash System» [2] під псевдонімом Сатоші Накамото. Ця робота не лише представила теоретичний фундамент, але й запропонувала практичну імплементацію першої криптовалюти Bitcoin, що функціонувала на основі блокчейн-технології.

Означення 1.1. Блокчейн – це впорядкована послідовність блоків $\mathcal{B} = (B_0, B_1, \ldots, B_n)$, де B_0 – початковий блок, а кожен наступний блок B_i $(i > 0)$ містить криптографічний хеш попереднього блоку $H(B_{i-1})$,

забезпечуючи цілісність та незмінність історії.

Ключовою інновацією блокчейну є забезпечення консенсусу між розподіленими вузлами мережі без необхідності в централізованому довіреному посереднику. Таким чином, блокчейн вирішує класичну проблему «візантійських генералів» у розподілених системах, що раніше вважалась нерозв'язною без центрального координатора [3].

Кожен блок B_i можна представити як структуру даних, що складається з двох основних компонентів:

$$B_i = (header_i, transactions_i) \tag{1.1}$$

де $header_i$ – заголовок блоку, який містить метадані, а $transactions_i$ – множина транзакцій, включених у блок.

Основними характеристиками блокчейну, що визначають його унікальність як технології, є:

1) **Децентралізація.** На відміну від традиційних централізованих систем, де контроль та управління даними здійснюються єдиним центральним органом, блокчейн функціонує як розподілена мережа вузлів, кожен з яких має повну або часткову копію всього ланцюга. Математично це можна представити як множину вузлів $\mathcal{N} = \{N_1, N_2, \ldots, N_k\}$, де кожен вузол N_j підтримує копію блокчейну $\mathcal{B}_j$, причому в ідеальному випадку $\mathcal{B}_1 = \mathcal{B}_2 = \ldots = \mathcal{B}_k$.

2) **Незмінність (immutability).** Після включення блоку в ланцюг та його підтвердження достатньою кількістю наступних блоків, практично неможливо змінити інформацію без зміни всіх наступних блоків. Це забезпечується властивостями криптографічних хеш-функцій, де навіть незначна зміна вхідних даних призводить до кардинально іншого результату.

3) **Прозорість та аудитованість.** Всі транзакції в блокчейні є публічними та доступними для перевірки всіма учасниками мережі, що забезпечує повну прозорість операцій.

4) **Безпека на основі консенсусу.** Блокчейни використовують різні механізми консенсусу для забезпечення узгодженості стану системи між усіма вузлами мережі, незважаючи на можливу наявність зловмисних учасників.

З точки зору доступу до мережі та прав участі, блокчейни поділяються на три основні категорії:

– **Публічні блокчейни** – системи з відкритим доступом, де будь-хто може брати участь у процесі консенсусу, верифікувати транзакції та створювати блоки без необхідності отримувати дозвіл. Прикладами є Bitcoin та Ethereum. Вони забезпечують максимальну децентралізацію та стійкість до цензури, але часто мають обмеження щодо масштабованості та приватності.

– **Приватні блокчейни** – системи, де доступ до мережі та права на участь у консенсусі контролюються однією організацією. Такі блокчейни забезпечують більшу продуктивність та приватність порівняно з публічними, але жертвують децентралізацією. Вони часто використовуються в корпоративному середовищі для оптимізації внутрішніх процесів.

– **Консорціумні блокчейни** – гібридний підхід, де процес консенсусу контролюється обмеженою кількістю заздалегідь обраних вузлів, що належать різним організаціям. Такі системи дозволяють різним організаціям співпрацювати без повної довіри одна до одної, зберігаючи певний рівень децентралізації та забезпечуючи достатню продуктивність.

1.1.1 Структура блоку та механізми формування ланцюга

Для детального розуміння функціонування блокчейну та процесів, що впливають на час обробки транзакцій, необхідно проаналізувати внутрішню структуру блоків та механізми їх об'єднання в єдиний ланцюг. Саме ці елементи визначають технічні параметри обробки транзакцій та

впливають на їх пріоритизацію в мережі.

Означення 1.2. Блок B_i у блокчейні – це структура даних, що складається з заголовка $header_i$ та тіла $body_i$, де заголовок містить метадані, а тіло – список транзакцій та додаткову службову інформацію.

Заголовок блоку $header_i$ типово включає наступні компоненти:

$$header_i = (version_i, prevHash_i, merkleRoot_i, timestamp_i, difficulty_i, nonce_i) \tag{1.2}$$

де:

– $version_i$ – версія протоколу блокчейну, що використовувалася для створення блоку;

– $prevHash_i = H(header_{i-1})$ – хеш заголовка попереднього блоку, що забезпечує криптографічний зв'язок між блоками;

– $merkleRoot_i$ – корінь дерева Меркла, що представляє всі транзакції в блоці;

– $timestamp_i$ – часова мітка створення блоку;

– $difficulty_i$ – параметр складності для механізму консенсусу (особливо важливий для Proof of Work);

– $nonce_i$ – довільне число, що використовується в процесі майнінгу для знаходження хешу з необхідними властивостями.

Тіло блоку $body_i$ містить список транзакцій та, залежно від блокчейн-платформи, може включати додаткові дані:

$$body_i = (transactions_i, extraData_i) \tag{1.3}$$

де $transactions_i = \{tx_{i,1}, tx_{i,2}, \ldots, tx_{i,m_i}\}$ – множина з m_i транзакцій, включених у блок B_i, а $extraData_i$ – додаткові дані, специфічні для конкретної блокчейн-системи.

Важливим елементом структури блоку є дерево Меркла (Merkle tree), яке забезпечує ефективну перевірку включення транзакції в блок без необхідності передачі всього блоку.

Означення 1.3. Дерево Меркла – це бінарне дерево, листками якого є хеші транзакцій, а кожен внутрішній вузол є хешем конкатенації його дочірніх вузлів. Корінь дерева ($merkleRoot_i$) включається в заголовок блоку.

Формально, для n транзакцій $(tx_1, tx_2, \ldots, tx_n)$ початкові листові вузли дерева Меркла формуються як:

$$L_i = H(tx_i), \quad i \in \{1, 2, \ldots, n\} \tag{1.4}$$

Внутрішні вузли обчислюються рекурсивно:

$$V_i = H(V_{2i} \,\|\, V_{2i+1}) \tag{1.5}$$

де $\|$ позначає операцію конкатенації.

Використання дерева Меркла дозволяє:

– Ефективно перевіряти включення транзакції в блок з логарифмічною складністю $O(\log m_i)$;

– Зменшити обсяг даних, необхідних для підтвердження наявності транзакції;

– Забезпечити цілісність всього набору транзакцій за допомогою одного хешу $merkleRoot_i$.

Така структура особливо важлива для реалізації «легких» клієнтів (SPV – Simplified Payment Verification), які не зберігають повну копію блокчейну, але можуть ефективно перевіряти включення конкретних транзакцій.

1.1.2 Механізми формування ланцюга

Блокчейн-мережа постійно отримує нові транзакції від користувачів. Ці транзакції спочатку зберігаються в розподіленому пулі непідтверджених транзакцій (мемпул). Процес обробки цих транзакцій та включення їх у блоки можна формалізувати наступним чином:

1) Транзакції надходять від користувачів та розповсюджуються мережею, формуючи пул непідтверджених транзакцій (мемпул): $\mathcal{T}_{unconfirmed}$.

2) Валідатори (або майнери) вибирають підмножину транзакцій $\mathcal{T}_{selected} \subseteq \mathcal{T}_{unconfirmed}$ для включення в новий блок. Цей відбір зазвичай базується на пріоритизації за розміром комісії, що створює економічні стимули для швидшої обробки.

3) На основі відібраних транзакцій формується кандидат на новий блок: $B_{candidate}$:

$$B_{candidate} = (header_{candidate}, \mathcal{T}_{selected}) \tag{1.6}$$

4) За допомогою механізму консенсусу визначається, який з кандидатів буде додано до ланцюга як новий блок B_{n+1}:

$$B_{n+1} = \mathcal{C}(\mathcal{B}, \{B^1_{candidate}, B^2_{candidate}, \ldots\}) \tag{1.7}$$

5) Новий блок розповсюджується мережею, і кожен вузол перевіряє його валідність перед включенням до своєї локальної копії блокчейну:

$$\mathcal{B} \leftarrow \mathcal{B} \cup \{B_{n+1}\} \tag{1.8}$$

Цей процес має важливі наслідки для дослідження часу обробки транзакцій, оскільки саме на етапах 2 і 3 визначається, які транзакції будуть включені в поточний блок, а які залишаться в пулі очікування. Економічна модель більшості блокчейнів стимулює валідаторів включати транзакції з вищими комісіями раніше, що створює пряму залежність між розміром комісії та часом обробки.

Через розподілений характер блокчейн-систем та затримки в комунікації між вузлами можуть виникати ситуації, коли різні валідатори майже одночасно створюють конкуруючі блоки. Це призводить до тимчасових розгалужень ланцюга, відомих як «форки» (forks).

Теорема 1.1 (Про вирішення форків)**.** *Нехай існують дві*

конкуруючі версії блокчейну $\mathcal{B}_1 = (B_0, B_1, \ldots, B_n, B^1_{n+1}, \ldots, B^1_{n+k})$ *та* $\mathcal{B}_2 = (B_0, B_1, \ldots, B_n, B^2_{n+1}, \ldots, B^2_{n+l})$, *що мають спільний префікс* $(B_0, B_1, \ldots, B_n)$. *Тоді, згідно з правилом найдовшого ланцюга, мережа вибере:*

$$\mathcal{B}_{accepted} = \begin{cases} \mathcal{B}_1, & \text{якщо } k > l \\ \mathcal{B}_2, & \text{якщо } l > k \\ \text{визначається додатковими правилами}, & \text{якщо } k = l \end{cases} \quad (1.9)$$

Вирішення конфліктів за правилом найдовшого ланцюга (або його варіаціями) є ключовим механізмом для забезпечення єдиного погляду на стан системи серед всіх учасників мережі. Проте цей механізм вводить поняття «імовірнісної фіналізації» – стану, коли блок з високою ймовірністю вже не буде виключений з основного ланцюга через реорганізацію.

Означення 1.4. Блок B_i вважається фіналізованим з ймовірністю p в системі з правилом найдовшого ланцюга, якщо ймовірність того, що він буде виключений з основного ланцюга через появу альтернативної довшої версії, не перевищує $1 - p$.

Для систем Proof of Work ця ймовірність експоненційно зменшується з «підтверджень»):

$$P(\text{реорганізація глибиною} > k) \leqslant e^{-\lambda k} \quad (1.10)$$

де λ – параметр, що залежить від розподілу обчислювальної потужності між чесними та потенційно зловмисними учасниками мережі.

Концепція фіналізації має пряме відношення до часу обробки транзакції, оскільки визначає, коли транзакцію можна вважати «підтвердженою» з достатньою впевненістю. Для різних застосувань можуть вимагатися різні рівні впевненості (кількість підтверджень), що також впливає на практичний час, необхідний для прийняття транзакції

як остаточної.

Розглянувши структурні елементи блокчейну та механізми формування ланцюга, стає очевидним, що ключовим компонентом, який забезпечує узгодженість стану розподіленої системи, є протокол консенсусу. Саме цей протокол визначає не лише безпеку та надійність мережі, але й принципові характеристики обробки транзакцій, включаючи час їх підтвердження та вплив комісії на пріоритизацію.

1.1.3 Криптографічні хеш-функції

Після розгляду структури блоків та механізмів формування ланцюга, важливо детально проаналізувати криптографічні хеш-функції – фундаментальний елемент, що забезпечує безпеку та цілісність всієї блокчейн-системи. Хеш-функції відіграють ключову роль на різних рівнях функціонування блокчейну, від зв'язування блоків між собою до підтвердження автентичності транзакцій та роботи протоколів консенсусу.

Означення 1.5. Криптографічна хеш-функція є детермінованим алгоритмом, що перетворює вхідні дані довільної довжини на вихідний рядок фіксованої довжини (хеш-значення), який задовольняє наступним властивостям:

– Ефективність обчислення – для будь-якого вхідного значення x хеш-значення $H(x)$ має обчислюватися за поліноміальний час;

– Стійкість до пошуку прообразу – для заданого хеш-значення h обчислювально складно знайти будь-яке вхідне значення x таке, що $H(x) = h$;

– Стійкість до пошуку колізій другого роду – для заданого вхідного значення x_1 обчислювально складно знайти інше вхідне значення $x_2 \neq x_1$ таке, що $H(x_1) = H(x_2)$;

– Стійкість до пошуку колізій – обчислювально складно знайти будь-які два різні вхідні значення $x_1 \neq x_2$ такі, що $H(x_1) = H(x_2)$.

У блокчейн-системах криптографічні хеш-функції виконують наступні основні ролі:

– Зв'язування блоків – хеш попереднього блоку включається в заголовок наступного ($prevHash_i = H(header_{i-1})$), формуючи криптографічно захищений ланцюг;

– Формування дерева Меркла – кожна транзакція τ хешується окремо, а на кожному внутрішньому рівні дерева Меркла обчислюється:

$$h_{\text{parent}} = \text{SHA256}(h_{\text{left}} \| h_{\text{right}}), \tag{1.11}$$

де $\|$ позначає конкатенацію хешів. Це забезпечує ефективну перевірку належності транзакцій до блоку з логарифмічною складністю [4];

– Створення «головоломок» для Proof of Work – пошук значення *nonce* такого, що:

$$H(header \| nonce) < T \tag{1.12}$$

де T – цільове значення, що визначає складність майнінгу;

– Генерація адрес – створення публічних адрес гаманців через хешування публічних ключів користувачів;

– Забезпечення цілісності цифрових підписів – хешування повідомлень перед підписанням.

В мережі Bitcoin та багатьох інших блокчейн-системах широко використовується хеш-функція SHA-256, розроблена Національним інститутом стандартів і технологій США (NIST) [5]. Для підвищення безпеки в Bitcoin використовується подвійне хешування:

$$H_{BTC}(x) = \text{SHA256}\big(\text{SHA256}(x)\big), \tag{1.13}$$

де x – бінарна послідовність даних (наприклад, серіалізована транзакція), а вихід $H(x)$ має довжину 256 біт.

SHA-256 перетворює вхідні дані на 256-бітний (32-байтний) хеш, що забезпечує високий рівень криптографічної стійкості. Завдяки властивості

лавинного ефекту, навіть мінімальна зміна у вхідних даних призводить до повністю іншого хеш-значення, що робить будь-які маніпуляції з історією транзакцій одразу помітними.

Безпека блокчейну безпосередньо залежить від криптографічної стійкості використовуваних хеш-функцій. Для 256-бітної хеш-функції, згідно з «парадоксом днів народження», знаходження колізій теоретично вимагає приблизно 2^{128} операцій, що з сучасними обчислювальними можливостями вважається практично недосяжним.

Криптографічні хеш-функції істотно впливають на час обробки транзакцій через:

– Регулювання складності майнінгу, що визначає середній час між блоками;

– Ефективність верифікації транзакцій та блоків мережею;

– Оптимізацію структур даних, таких як дерева Меркла.

1.2 Смарт-контракти

Смарт-контракти суттєво розширили можливості блокчейну, перетворивши його з простої системи платежів на універсальну платформу для різноманітних додатків. Ця інновація відкрила нові горизонти для автоматизації складних бізнес-процесів без потреби в довірених посередниках.

Смарт-контракт – це програмний код, який автоматично виконуватиметься у блокчейні при виконанні заздалегідь визначених умов. Він дозволятиме формувати, контролювати та надавати інформацію про власність активами без потреби посередника. Вперше термін запропонував Нік Сабо у 1997 році [6], а практичну реалізацію широкого масштабу забезпечила платформа Ethereum у 2015 році [7].

На відміну від звичайних програм, смарт-контракти існують у розподіленому середовищі блокчейну. При розгортанні контракт отримує унікальну адресу, за якою до нього можна звертатися. Типова взаємодія

зі смарт-контрактом відбувається через транзакцію наступного формату:

$$\tau_{\text{contract}} = \big(from, to, value, data\big), \tag{1.14}$$

де *from* – адреса користувача, що ініціює виклик; *to* – адреса контракту; *value* – кількість криптовалюти, що передається; *data* – закодовані аргументи та ідентифікатор функції, яку потрібно викликати.

Коли така транзакція потрапляє в блок, кожен вузол мережі виконує операції, передбачені в контракті. Оскільки виконання детерміноване (з однаковими вхідними даними завжди отримуємо однакові результати), всі вузли досягають однакового стану. Це забезпечує надійну роботу в недовірчому середовищі – ключову перевагу смарт-контрактів.

Смарт-контракти застосовуються для реалізації децентралізованих фінансів (DeFi), невзаємозамінних токенів (NFT), систем голосування та інших децентралізованих додатків. Головні переваги:

– **Автоматизація.** Виконання бізнес-логіки без участі довіреного посередника.

– **Незмінність.** Код контракту та його стан зберігаються в блокчейні й не можуть бути змінені після розгортання.

– **Прозорість.** Усі виклики та зміни стану контракту доступні для аудиту.

При всіх перевагах смарт-контрактів, вони стикаються з серйозними викликами безпеки. Найгучніший інцидент – зламування The DAO у 2016 році, коли було викрадено еквівалент 60 мільйонів доларів через вразливість повторного входу.

Особливо гостро стоїть проблема атак випередження, яка безпосередньо стосується теми цієї роботи, але більш детально буде описана згодом:

Означення 1.6. Атака випередження (frontrunning) – це маніпуляція порядком обробки транзакцій, при якій зловмисник,

виявивши вигідну транзакцію в пулі очікування, створює власну з вищою комісією, щоб вона була оброблена раніше, отримуючи тим самим неправомірну вигоду.

Такі атаки особливо поширені в кількох сценаріях:

– Арбітраж на децентралізованих біржах – зловмисник бачить велику транзакцію купівлі, яка підніме ціну активу, і робить власну купівлю перед нею, а продаж – після.

– Кіберсквотинг у сервісах реєстрації доменних імен – зловмисник перехоплює спробу зареєструвати цінне ім'я.

– Перехоплення голосувань у DAO – маніпуляція результатами, використовуючи інформацію про голоси інших учасників.

– Маніпуляції аукціонами – зловмисник отримує перевагу, підвищуючи ставки в останній момент з гарантією включення в блок.

Дослідження Daian та ін. [8] виявило, що лише в Ethereum щомісяця відбуваються тисячі таких атак, а їх загальна вартість обраховується мільйонами доларів. Ще гірше, що безліч так званих MEV-ботів (Miner Extractable Value) автоматизують ці атаки, постійно сканують мемпул, шукаючи прибуткові можливості.

Ефективність таких атак прямо залежить від характеру взаємозв'язку між комісіями та часом обробки транзакцій у різних протоколах консенсусу – саме те, що становить основний предмет даного дослідження.

Розуміння природи цих атак та механізмів їх попередження неможливе без глибокого аналізу того, як різні протоколи консенсусу обробляють транзакції та як вони пріоритизують їх включення в блоки.

1.3 Аналіз протоколів консенсусу в блокчейн-мережах

Маючи розуміння базової структури блокчейну та смарт-контрактів, варто перейти до критично важливого компонента – механізмів

досягнення консенсусу. Саме протоколи консенсусу визначають, як сотні або тисячі розподілених вузлів мережі домовляються про єдиний стан системи без центрального авторитету. Ці протоколи безпосередньо впливають на швидкість обробки транзакцій, їх пріоритезацію та, як наслідок, залежність часу підтвердження від розміру комісії.

Означення 1.7. Консенсус у розподілених системах – процес досягнення угоди щодо єдиного стану системи між незалежними вузлами мережі в умовах можливої ненадійності каналів зв'язку та присутності потенційно зловмисних учасників.

У контексті блокчейн-технологій механізм консенсусу виконує кілька критичних функцій:

1) Підтвердження транзакцій та формування нових блоків

2) Забезпечення узгодженості стану розподіленого реєстру

3) Захист системи від зловмисних дій та атак

4) Стимулювання учасників до підтримки функціонування мережі

Математична формалізація проблеми консенсусу в розподілених системах належить до класу так званих задач візантійської угоди, де необхідно досягти згоди в умовах, коли частина учасників може діяти зловмисно або неправильно через технічні збої.

Дослідження розподілених систем виявили фундаментальні обмеження, що впливають на всі протоколи консенсусу. Зокрема, теорема CAP (Consistency, Availability, Partition tolerance) стверджує, що в умовах мережевого розділення система може забезпечити лише дві з трьох властивостей: узгодженість, доступність і толерантність до розділення мережі [9].

Ще одним важливим результатом є теорема FLP (Fischer, Lynch, Paterson) про неможливість:

Теорема 1.2 (Про неможливість консенсусу FLP)**.** *У асинхронній розподіленій системі неможливо гарантувати консенсус, якщо хоча б один учасник може відмовити, навіть якщо всі повідомлення*

доставляються коректно.

Ця теорема, доведена Фішером, Лінчем та Патерсоном у 1985 році, визначає фундаментальне обмеження для протоколів консенсусу. Однак на практиці блокчейн-системи впроваджують різні механізми, що дозволяють досягати ймовірнісного консенсусу з високим рівнем надійності.

Оцінка ефективності протоколу консенсусу здійснюється за кількома ключовими параметрами:

– Безпека – стійкість до різних типів атак, зокрема до атаки подвійної витрати та атаки Сібіл

– Живучість – здатність системи продовжувати функціонування та обробляти транзакції

– Пропускна здатність – кількість транзакцій, які система може обробити за одиницю часу

– Латентність – час, необхідний для підтвердження транзакції

– Енергоефективність – кількість обчислювальних ресурсів, необхідних для функціонування системи

– Масштабованість – здатність системи підтримувати зростання кількості користувачів та транзакцій

Різні протоколи консенсусу, що застосовуються в блокчейн-технологіях, представляють різні компроміси між цими параметрами, і вибір конкретного механізму залежить від специфіки завдань, які вирішує певна блокчейн-система.

1.3.1 Протокол Proof of Work (PoW)

Протокол Proof of Work (PoW) є історично першим та найбільш широко використовуваним механізмом консенсусу в блокчейн-системах, запровадженим у Bitcoin. Його ключова ідея полягає в забезпеченні консенсусу через виконання складних обчислювальних завдань, вирішення яких потребує значних ресурсів.

Означення 1.8. Proof of Work (доказ виконаної роботи) – механізм консенсусу, в якому право створення нового блоку надається учаснику, що першим розв'язав обчислювально складну криптографічну задачу, правильність розв'язку якої може бути легко перевірена іншими учасниками мережі.

Сутність PoW полягає в пошуку такого значення параметра `nonce`, щоб хеш-функція від заголовка блоку давала результат, менший за цільове значення складності [10]. Математично це можна представити так:

Знайти таке значення *nonce*, що:

$$H(header \| nonce) < T \tag{1.15}$$

де H — криптографічна хеш-функція (зазвичай SHA-256), *header* – заголовок блоку, $\|$ – операція конкатенації, а T – цільове значення, що визначає складність. Чим менше T, тим більша складність.

Цільове значення T визначається через параметр складності D:

$$T = 2^{256}/D \tag{1.16}$$

Майнінг, по суті, є перебором різних значень `nonce` у пошуках такого, що задовольняє вказану умову. При цьому через властивості криптографічних хеш-функцій єдиним ефективним методом є спроба різних значень, що робить процес схожим на лотерею, де ймовірність знаходження дійсного блоку пропорційна обчислювальній потужності учасника.

Унікальною особливістю PoW є автоматичне регулювання складності завдання залежно від сукупної обчислювальної потужності мережі. Це забезпечує приблизно постійний інтервал між блоками, незважаючи на зміни загальної потужності майнінгу.

У Bitcoin корекція відбувається кожні 2016 блоків (приблизно раз на два тижні) за формулою:

$$D_{new} = D_{old} \cdot \frac{T_{expected}}{T_{actual}} \tag{1.17}$$

де $T_{expected}$ — очікуваний час для створення 2016 блоків (2016 × 10 хвилин = 1209600 секунд), а T_{actual} — фактичний час, який знадобився для створення останніх 2016 блоків.

Якщо мережа генерує блоки швидше очікуваного, складність зростає; якщо повільніше — складність знижується. Це забезпечує стабільність системи в довгостроковій перспективі.

В інших PoW-блокчейнах використовуються варіації цього алгоритму. Наприклад, Ethereum (до переходу на PoS) застосовував корекцію складності для кожного блоку, що давало швидшу адаптацію до змін потужності мережі.

Процес знаходження блоку в PoW-системах можна моделювати як пуассонівський процес, де час між подіями (створеннями блоків) має експоненціальний розподіл.

Теорема 1.3 (Про розподіл часу створення блоку в PoW)**.** *Нехай λ – середня кількість блоків, які мережа генерує за одиницю часу, а T – випадкова величина, що представляє час до генерації наступного блоку. Тоді T має експоненційний розподіл з параметром λ, тобто $P(T \leqslant t) = 1 - e^{-\lambda t}$.*

Для Bitcoin з цільовим часом блоку 10 хвилин ($\lambda = 1/600$ блоків на секунду), це означає, що:

– Очікуваний (середній) час між блоками становить $1/\lambda = 600$ секунд

– Стандартне відхилення також дорівнює $1/\lambda = 600$ секунд

– Ймовірність того, що блок буде знайдено протягом 10 хвилин після попереднього, становить $1 - e^{-1} \approx 0.632$ (лише 63.2%)

– Час між блоками може варіюватись від кількох секунд до години і більше

Ця варіативність має критичний вплив на час обробки транзакцій і

створює своєрідну «природну лотерею» для транзакцій у пулі очікування.

Коли майнер знаходить дійсний блок, він має право включити в нього обрані транзакції з пулу очікування. Оскільки розмір блоку обмежений (у Bitcoin максимальний розмір становить приблизно 1 МБ, що обмежує кількість транзакцій до 2000-3000), виникає конкуренція між транзакціями.

Історично в Bitcoin використовувалася проста стратегія максимізації комісій:

1) Майнер сортує транзакції за спаданням відношення комісії до розміру: $\frac{\phi_i}{size_i}$

2) Транзакції додаються до блоку в порядку сортування до досягнення ліміту розміру

З економічної точки зору це створює ринок аукціонного типу, де користувачі конкурують за обмежений ресурс – місце в блоці. Чим вище комісія, тим вище шанс швидкого включення транзакції, що формує пряму залежність між розміром комісії та часом обробки.

1.3.2 Протокол Proof of Stake (PoS)

Протокол Proof of Stake (PoS) був розроблений як альтернатива енергозатратному Proof of Work, зберігаючи при цьому децентралізовану природу блокчейн-систем. Ключова відмінність PoS полягає в тому, що право на створення нових блоків та підтвердження транзакцій залежить не від обчислювальної потужності, а від кількості токенів, які учасник мережі утримує та ставить як заставу.

Означення 1.9. Proof of Stake (доказ частки володіння) – механізм консенсусу, в якому ймовірність вибору учасника для створення нового блоку пропорційна кількості криптовалюти, яку він заблокував (поставив у «стейк») як заставу на підтримку роботи мережі.

На відміну від PoW, де учасники доводять свою легітимність через

витрату обчислювальних ресурсів, у PoS-системах учасники підтверджують свої наміри, блокуючи певну кількість криптовалюти. Чим більша кількість монет заблокована, тим вища ймовірність обрання для створення блоку.

Порівняння основних підходів:

Аспект	**Proof of Work**	**Proof of Stake**
Ресурс для участі	Обчислювальна потужність	Наявна криптовалюта
Процес валідації	Розв'язання криптографічних задач	Випадковий вибір на основі стейку
Нагорода за блок	Нові монети + комісії	Переважно лише комісії
Енергоспоживання	Дуже високе	Мінімальне
Вартість атаки 51%	Обладнання + електроенергія	Покупка 51% монет

Таблиця 1.1 – Порівняння PoW та PoS

У базовій моделі PoS ймовірність вибору учасника (валідатора) i для створення наступного блоку пропорційна його стейку:

$$P_i = \frac{S_i}{\sum_{j=1}^{n} S_j} \tag{1.18}$$

де S_i – розмір стейку валідатора i, а $\sum_{j=1}^{n} S_j$ – загальна кількість монет у стейку.

Сучасні реалізації PoS часто поєднують ці підходи та включають додаткові механізми безпеки. Наприклад, Ethereum 2.0 використовує комбінацію PoS з механізмом Casper для забезпечення безпеки та покарання недобросовісних валідаторів.

Теорема 1.4 (Про стійкість PoS до атак)**.** *У протоколі Proof of Stake з механізмом покарання (slashing) та належною рандомізацією для успішної атаки на ланцюг зловмисникові знадобиться контролювати щонайменше 1/3 загального стейку мережі, за умови, що мережа має достатньо незалежних валідаторів та механізм відбору забезпечує належну випадковість.*

Такі гарантії ґрунтуються, де зловмисник, що контролює значну

частку стейку, має потужний економічний стимул не атакувати мережу, оскільки успішна атака призведе до знецінення його власних активів.

Крім того, на відміну від PoW, де успішна атака 51% дозволяє лише змінювати поточний та майбутній стан блокчейну, в деяких PoS-системах (наприклад, із механізмом «accountable safety») можна криптографічно доводити факт атаки та покарати зловмисника шляхом конфіскації його стейку.

PoS протоколи суттєво відрізняються від PoW в аспектах, які стосуються обробки транзакцій:

– **Час блоку** – більшість PoS-систем мають менший і стабільніший інтервал між блоками. Наприклад, Ethereum 2.0 має блоки кожні 12 секунд, Cardano – кожні 20 секунд, Tezos – кожні 60 секунд.

– **Детермінізм** – на відміну від експоненціального розподілу в PoW, у багатьох PoS-системах валідатори мають визначені слоти для створення блоків, що робить час між блоками більш передбачуваним.

– **Швидша фіналізація** – деякі PoS-протоколи (особливо ті, що використовують BFT-консенсус) можуть забезпечувати «миттєву» фіналізацію, коли підтверджений блок вже не може бути скасований через реорганізацію.

Ці відмінності мають значний вплив на залежність між комісією за транзакцію та часом її обробки. У PoS-системах ця залежність часто слабша, оскільки:

– Блоки створюються з більш регулярними інтервалами;

– Пропускна здатність зазвичай вища, що зменшує конкуренцію за місце в блоці;

– Валідатори мають менше економічних стимулів для пріоритизації транзакцій виключно за комісією.

Протокол Proof of Stake має низку переваг порівняно з Proof of Work:

– Енергоефективність – PoS не потребує значних обчислювальних ресурсів для забезпечення консенсусу, що знижує енергоспоживання у тисячі разів порівняно з PoW;

– Зниження бар'єру входу – для участі в консенсусі не потрібно спеціалізоване обладнання, достатньо мати певну кількість токенів;

– Підвищена пропускна здатність – без необхідності виконувати складні обчислення PoS-системи можуть забезпечувати більшу швидкість обробки транзакцій;

– Економічна безпека – атака на мережу вимагає значних інвестицій у токени системи, а успішна атака знизить їхню вартість, що створює економічний стимул проти зловмисної поведінки;

– Попередження централізації майнінгу – відсутність переваг від спеціалізованого обладнання та економії на масштабі сприяє децентралізації.

Однак PoS має і свої недоліки:

– Проблема «нічого на кону» (Nothing at Stake) – теоретична вразливість, коли валідатори можуть безкоштовно підтримувати кілька конкуруючих ланцюгів

– Централізація багатства – принцип «багаті стають багатшими» може призводити до концентрації влади

– Складність реалізації – більш складні протоколи порівняно з PoW

– Проблеми холодного старту – початковий розподіл токенів часто централізований

– Менша перевіреність часом – відсутність тривалої історії успішного застосування в масштабі Bitcoin

Незважаючи на ці недоліки, тренд переходу від PoW до PoS очевидний у блокчейн-індустрії. Найбільш помітним кроком стало успішне оновлення Ethereum (The Merge) у вересні 2022 року, коли друга за капіталізацією криптовалюта перейшла з PoW на PoS. Цей перехід підтверджує зрілість технології та її готовність до масштабних впроваджень.

Розглянувши основні принципи PoS, можемо перейти до третьої категорії протоколів консенсусу — протоколів з секвенсорами, які представляють наступний етап еволюції блокчейн-технологій та

вирішують проблему масштабованості через обробку транзакцій поза основним ланцюгом.

1.3.3 Протоколи з секвенсорами (Layer 2 рішення)

З розвитком блокчейн-екосистеми та зростанням числа користувачів фундаментальні обмеження базових протоколів PoW і PoS стали очевидними. Обмежена пропускна здатність і високі комісії в періоди підвищеного попиту зробили використання блокчейнів першого рівня (Layer 1) непрактичним для багатьох повсякденних застосувань. Відповіддю на цей виклик стало створення рішень другого рівня (Layer 2), серед яких особливе місце займають протоколи з секвенсорами.

Означення 1.10. Протокол з секвенсором – це рішення масштабування блокчейну, в якому спеціальний компонент (секвенсор) відповідає за збір, упорядкування та групування транзакцій користувачів перед їх агрегованою передачею на базовий блокчейн (Layer 1), зберігаючи при цьому безпеку базового ланцюга.

На відміну від PoW і PoS, які є самостійними протоколами консенсусу, рішення з секвенсорами функціонують як надбудова над існуючими блокчейнами. Їх архітектура зазвичай включає такі компоненти:

– Секвенсор – вузол або група вузлів, відповідальні за обробку транзакцій поза основним ланцюгом

– Смарт-контракт на L1 – зберігає стан системи L2 і обробляє передачу активів між рівнями

– Механізм доказів або оскаржень – забезпечує коректність обробки транзакцій на L2

– Мережа перевіряльників – незалежні вузли, що валідують дії секвенсора

Спрощено процес обробки транзакцій відбувається так:

1. Користувачі надсилають транзакції безпосередньо секвенсору, а не до мережі L1 2. Секвенсор групує транзакції, обробляє їх та створює «пакет» 3. Періодично секвенсор публікує на L1 або дані про всі транзакції, або криптографічний доказ їх коректної обробки 4. L1 смарт-контракт верифікує подану інформацію та оновлює офіційний стан системи

Ця архітектура дозволяє обробляти сотні або тисячі транзакцій у пакеті, розподіляючи фіксовану вартість взаємодії з L1 на велику кількість користувацьких операцій.

У сучасній блокчейн-екосистемі виділяють кілька ключових типів протоколів з секвенсорами:

– Optimistic Rollups – припускають, що всі транзакції валідні за замовчуванням, але дозволяють оскаржити результати протягом "періоду оскарження"(зазвичай 7 днів). Представники: Optimism, Arbitrum, Boba Network.

– Zero-Knowledge Rollups (ZK-Rollups) – використовують криптографічні доведення з нульовим розголошенням для підтвердження валідності пакетів транзакцій. Представники: zkSync, StarkNet, Polygon zkEVM.

– Validium – подібні до ZK-Rollups, але зберігають дані поза основним ланцюгом, що дозволяє ще більше знизити вартість транзакцій. Представники: StarkEx, DeversiFi.

– Plasma – створює дочірні ланцюги, пов'язані з основним блокчейном, з власними механізмами валідації. Представники: Polygon (раніше Matic), OMG Network.

З усіх цих типів найбільшого поширення набули Optimistic і ZK-Rollups, завдяки оптимальному балансу безпеки, масштабованості та сумісності з існуючими програмами.

Взаємодія між L1 та L2 є критичним аспектом протоколів з секвенсорами. Вона включає два основні процеси:

– Депозити ($L1 \rightarrow L2$) – переміщення активів з основного блокчейну

до L2. Зазвичай обробляються швидко, після кількох підтверджень на L1;

– Виходи ($L2 \rightarrow L1$) – виведення активів з L2 назад до L1. Тут процеси суттєво відрізняються:

– В Optimistic Rollups користувачі мають чекати "період оскарження"(зазвичай 7 днів);

– В ZK-Rollups виходи можуть оброблятися одразу після включення доведення в L1.

Безпека протоколів з секвенсорами ґрунтується на кількох рівнях:

1) Успадкована безпека L1 – основний блокчейн забезпечує базовий рівень захисту

2) Криптографічні гарантії – ZK-Rollups використовують математичні доведення, що гарантують цілісність обробки

3) Економічні стимули – секвенсори та перевіряльники часто стейкають кошти як заставу за належну поведінку

4) Механізми виходу – користувачі завжди можуть примусово вивести свої кошти навіть при відмові секвенсора

Одна з головних переваг протоколів з секвенсорами – суттєве підвищення пропускної здатності порівняно з базовими блокчейнами. Залежно від типу протоколу та параметрів мережі, пропускна здатність може досягати:

– Optimistic Rollups: 2,000-4,000 TPS

– ZK-Rollups: 2,000-10,000 TPS

– Validium: до 20,000 TPS

Для порівняння, Ethereum L1 обробляє 15-45 TPS, а Bitcoin — 3-7 TPS.

Механізми обробки транзакцій у протоколах з секвенсорами мають кілька ключових особливостей, що відрізняють їх від традиційних блокчейнів:

1) Попередні підтвердження – секвенсор може надати користувачеві «попереднє підтвердження» транзакції вже через кілька секунд після її отримання, задовго до публікації на L1;

2) Пакетна обробка – транзакції обробляються групами, а не індивідуально;

3) Стиснення даних – використовуються різні техніки для мінімізації обсягу даних, що публікуються на L1;

4) Кілька рівнів фіналізації – від «попереднього підтвердження» до «повної фіналізації» на L1.

Ці особливості суттєво впливають на характер залежності між комісією та часом обробки. На відміну від L1 блокчейнів, де ця залежність зазвичай дуже виражена, у протоколах з секвенсорами вона часто значно слабша або навіть відсутня для певних діапазонів комісій.

Причини цього явища:

– Транзакції часто обробляються пакетами за розкладом, а не за конкурентним принципом;

– Пропускна здатність зазвичай значно перевищує попит (за винятком піків);

– Секвенсори можуть використовувати різні стратегії пріоритизації, не обов'язково базовані лише на розмірі комісії.

У протоколах з секвенсорами залежність між комісією та часом обробки можна схематично представити кусково-лінійною функцією:

– Для транзакцій з комісією нижче мінімального порогу – час обробки може бути дуже великим або невизначеним (транзакція просто не приймається);

– Для транзакцій з комісією в «нормальному» діапазоні – час обробки переважно визначається розкладом пакетування та публікації, а не розміром комісії;

– Для транзакцій з особливо високою комісією – може відбуватися пріоритизація, але ефект зазвичай менший, ніж у L1.

Експериментальні дослідження показують, що в періоди нормального навантаження кореляція між розміром комісії та часом обробки в протоколах з секвенсорами часто статистично незначуща, на відміну від PoW і PoS систем. Ця особливість має важливі наслідки для

захисту від атак випередження, що будуть розглянуті далі в роботі.

1.4 Математичні моделі обробки транзакцій у блокчейн-мережах

Розглянувши особливості різних протоколів консенсусу, перейдемо до аналізу математичних моделей, що описують процеси обробки транзакцій та кількісно характеризують залежність часу обробки від параметрів транзакцій, зокрема від розміру комісії.

1.4.1 Теорія черг у контексті блокчейн-транзакцій

Процес обробки транзакцій у блокчейн-мережах природно моделюється за допомогою теорії черг, де мемпул розглядається як черга, а процес формування блоків – як система обслуговування.

Означення 1.11. Система обробки транзакцій у блокчейн-мережі може бути представлена як система масового обслуговування (СМО), де:

– Потік транзакцій є вхідним потоком заявок

– Валідатори/майнери є серверами обслуговування

– Пул непідтверджених транзакцій (мемпул) є чергою заявок

– Блоки представляють групи одночасно оброблених транзакцій

У найпростішій моделі $M/D/1$ вхідний потік транзакцій є пуассонівським з інтенсивністю λ, час створення блоків є детерміністичним з середнім значенням $1/\mu$, а середній час очікування в черзі обчислюється як $W_q = \frac{\rho}{2\mu(1-\rho)}$, де $\rho = \lambda/\mu$ – коефіцієнт завантаження системи [11].

1.4.2 Ймовірнісні моделі включення транзакцій у блоки

Альтернативним підходом до моделювання процесу обробки транзакцій є розгляд ймовірності включення транзакції в блок залежно від її характеристик. Для кількісного опису залежності часу обробки транзакції від величини комісії ϕ використовуються параметричні регресійні моделі.

Розглянемо чотири основні класи моделей:

1) **Степенева модель**

Очікується, що час обробки T зменшується за степеневим законом зі збільшенням комісії:

$$T(\phi) = a \cdot \phi^{-b} + c \tag{1.19}$$

де $a > 0$, $b > 0$ і $c \geqslant 0$ – параметри, що інтерпретуються як масштабний коефіцієнт, ступінь впливу комісії та асимптотичний мінімальний час обробки.

2) **Експоненційна модель**

Якщо зростання комісії дає швидкий відгук у вигляді експоненційного зниження часу:

$$T(\phi) = a \cdot e^{-b \cdot \phi} + c \tag{1.20}$$

де $a > 0$, $b > 0$ і $c \geqslant 0$. Ця форма підходить, коли існує «пороговий» ефект.

3) **Гіперболічна модель**

Середній час обробки може слідувати гіперболічному закону:

$$T(\phi) = \frac{a}{\phi} + b \tag{1.21}$$

де $a > 0$ і $b \geqslant 0$. Ця модель відображає зворотню пропорційність.

4) **Логарифмічна модель**

У випадку слабкої залежності можна використати логарифмічну модель:

$$T(\phi) = -a \cdot \ln(\phi) + b \tag{1.22}$$

де $a > 0$, b – параметри, що забезпечують зменшення часу обробки при зростанні комісії.

Вибір найбільш доречної моделі здійснюється шляхом оцінки параметрів за методом найменших квадратів на реальних даних та порівняння метрик якості апроксимації (R^2, AIC, BIC), як показано в Розділі 3.

1.4.3 Фактори, що впливають на час обробки транзакцій

Час обробки транзакцій T визначається взаємодією кількох груп факторів:

Внутрішні характеристики транзакцій включають комісію ϕ, розмір транзакції $size$, обчислювальну складність (для смарт-контрактів) та залежності від інших транзакцій.

Характеристики мережі охоплюють середній час створення блоків $1/\mu$, розмір блоку N, поточне навантаження M (кількість транзакцій у мемпулі) та розподіл обчислювальної потужності або валідаторів.

Зовнішні фактори включають цінову волатильність, географічні особливості розподілу вузлів, регуляторні зміни та технічні обмеження мережі.

Врахування цих факторів у моделях дозволяє прогнозувати час обробки транзакцій та оптимізувати параметри для конкретних вимог користувачів.

1.5 Залежність часу обробки транзакцій від розміру комісії

1.5.1 Теоретичні моделі залежності

Для різних типів блокчейн-систем характерні різні форми залежності між розміром комісії та часом обробки транзакцій.

Для блокчейнів з протоколом Proof of Work залежність зазвичай має вигляд степеневої функції:

$$T(\phi) = a \cdot \phi^{-b} + c \tag{1.23}$$

Ця модель відображає значне зменшення часу очікування при збільшенні комісії та існування мінімального часу c, визначеного технічними параметрами мережі.

Для блокчейнів з протоколом Proof of Stake часто спостерігається експоненційна залежність:

$$T(\phi) = \alpha \cdot e^{-\beta \cdot \phi} + \gamma \tag{1.24}$$

Ця форма відображає більш плавну залежність, характерну для систем з детерміністичнішим процесом створення блоків.

Для протоколів з секвенсорами (Layer 2 рішення) залежність може бути близькою до лінійної для малих значень комісії або постійною вище певного порогу:

$$T(\phi) = \begin{cases} m \cdot \phi + n, & \text{якщо } \phi < \phi_{threshold} \\ T_{min}, & \text{якщо } \phi \geqslant \phi_{threshold} \end{cases} \tag{1.25}$$

1.5.2 Вплив навантаження на мережу

Залежність між комісією та часом обробки модифікується під впливом навантаження на мережу. Для аналізу цього впливу використовується модель:

$$T(\phi, load) = T_0(\phi) \cdot g(load) \tag{1.26}$$

де $T_0(\phi)$ – базова функція залежності, а $g(load)$ – функція впливу навантаження.

При збільшенні навантаження необхідно пропорційно збільшувати комісію для збереження того ж часу обробки, що особливо помітно в періоди пікової активності мережі.

Висновки до розділу 1

У даному розділі було проведено всебічний аналіз теоретичних основ функціонування блокчейн-технологій, зокрема різних протоколів консенсусу, та їх впливу на процес обробки транзакцій.

Розглянуто архітектуру та принципи роботи блокчейну, з акцентом на структуру блоків, механізми формування ланцюга та концепцію децентралізації. Проаналізовано три основні типи протоколів консенсусу: Proof of Work, Proof of Stake та протоколи з секвенсорами (Layer 2 рішення). Для кожного типу розглянуто принципи роботи, математичні основи, переваги та недоліки.

Детально охарактеризовано протокол Proof of Work, який використовує механізм розв'язання складних обчислювальних задач для підтвердження транзакцій. Визначено, що цей протокол забезпечує високий рівень безпеки, але характеризується значними енергетичними витратами та обмеженою пропускною здатністю.

Проаналізовано протокол Proof of Stake, який базується на підтвердженні транзакцій відповідно до частки володіння криптовалютою. Показано його переваги щодо енергоефективності та потенційно вищої пропускної здатності порівняно з PoW, а також висвітлено проблеми, пов'язані з початковим розподілом токенів та ризиком централізації влади.

Досліджено протоколи з секвенсорами, які представляють рішення другого рівня (Layer 2) для підвищення масштабованості блокчейну. Проаналізовано їхні особливості, зокрема використання пакетної обробки транзакцій та оптимізацію використання базового блокчейну.

Досліджено економічні аспекти функціонування блокчейн-мереж,

включаючи моделі формування комісій за транзакції, алгоритми відбору транзакцій для включення в блок та економічні стимули учасників мережі. Показано, як ці фактори впливають на час обробки транзакцій та ефективність мережі в цілому.

Проаналізовано математичні моделі, що можуть бути використані для опису процесу обробки транзакцій, включаючи моделі на основі теорії черг та ймовірнісні моделі включення транзакцій у блоки. Розглянуто чотири основні класи регресійних моделей (степенева, експоненційна, гіперболічна та логарифмічна), які описують залежність часу обробки транзакцій від розміру комісії для різних типів протоколів консенсусу.

Визначено фактори, що впливають на час обробки транзакцій, зокрема внутрішні характеристики транзакцій (комісія, розмір, складність), характеристики мережі (середній час створення блоків, розмір блоку, навантаження) та зовнішні фактори (цінова волатильність, географічні особливості, регуляторні зміни).

Особливу увагу приділено залежності часу обробки транзакцій від розміру комісії, яка має різний характер для різних типів блокчейн-систем: степенева для PoW, експоненційна для PoS, та близька до лінійної або константної для протоколів з секвенсорами. Також враховано вплив навантаження на мережу, який модифікує цю базову залежність.

Проведений теоретичний аналіз закладає фундамент для подальшого емпіричного дослідження та інтерпретації його результатів. У наступних розділах буде проведено детальний аналіз теоретичної моделі атаки випередження, розглянуто методологію збору та обробки емпіричних даних, а також представлено результати статистичного аналізу залежності часу обробки транзакцій від розміру комісії для різних типів блокчейн-систем.

2 ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ЗАЛЕЖНОСТІ ЧАСУ ОБРОБКИ ВІД КОМІСІЇ

Даний розділ присвячено теоретичним основам дослідження залежності часу обробки транзакцій від розміру комісії в блокчейн-системах та зв'язку цієї залежності з уразливістю до атак випередження.

У розділі формалізовано математичні моделі різних типів атак випередження, розроблено методологію емпіричного дослідження залежності часу обробки від комісії та встановлено теоретичний зв'язок між характером цієї залежності та ефективністю атак випередження. Особливу увагу приділено обґрунтуванню важливості емпіричного дослідження для верифікації теоретичних моделей та розробки ефективних стратегій захисту від атак випередження.

Розглянуті в розділі теоретичні моделі та методологічні підходи створюють необхідну основу для емпіричного дослідження залежності часу обробки транзакцій від розміру комісії, результати якого представлено в наступному розділі.

2.1 Теоретична модель атаки випередження

У блокчейн-системах, де прозорість транзакцій є одночасно перевагою та вразливістю, значну загрозу становлять атаки випередження (frontrunning). Ці атаки базуються на можливості зловмисника впливати на порядок включення транзакцій у блок, використовуючи публічний характер пулу непідтверджених транзакцій. У контексті даного дослідження розуміння природи атак випередження є критично важливим, оскільки їхня ефективність безпосередньо залежить від характеру взаємозв'язку між комісією за транзакцію та часом її

обробки.

2.1.1 Сутність та типи атак випередження

Означення 2.1. Атака випередження (frontrunning) – це маніпуляція порядком обробки транзакцій, при якій зловмисник, виявивши транзакцію певного типу в мемпулі, створює власну транзакцію, прагнучи забезпечити її пріоритетне включення в блок для отримання неправомірної вигоди [12, 13].

Механізм атаки випередження базується на кількох ключових особливостях блокчейн-систем.

– Публічність мемпулу. Інформація про непідтверджені транзакції доступна всім учасникам мережі, що дозволяє зловмиснику виявляти потенційно вигідні для маніпуляцій транзакції.

– Пріоритизація за комісією. В більшості блокчейн-мереж транзакції з вищою комісією мають пріоритет при включенні в блок, що дає зловмисникові інструмент для впливу на порядок обробки.

– Часова відстань між створенням блоків. Інтервал між блоками (наприклад, приблизно 10 хвилин у Bitcoin) створює «вікно можливостей» для зловмисника.

В залежності від методу впливу на порядок виконання транзакцій, можна виділити три основні типи атак випередження.

Атака заміщення передбачає, що зловмисник створює транзакцію, подібну до виявленої у мемпулі, але з вищою комісією, прагнучи, щоб його транзакція була включена в блок раніше оригінальної. Ця атака особливо ефективна у сценаріях аукціонів, реєстрації доменних імен або у ситуаціях, коли важливим є «першість» транзакції.

При **атаці вставки** зловмисник створює дві транзакції: одну для виконання перед цільовою транзакцією, іншу – після неї. Цей тип атаки часто використовується на децентралізованих біржах (DEX) для

маніпуляції цінами активів. Наприклад, зловмисник може купити актив перед великою транзакцією купівлі, яка підвищить ціну, а потім продати його після неї за вищою ціною.

У випадку **атаки стримування** зловмисник намагається відтермінувати виконання певної транзакції, створюючи велику кількість транзакцій з вищою комісією, які заповнюють блоки, не залишаючи місця для цільової транзакції. Такі атаки часто спрямовані на транзакції від так званих «оракулів», які надають зовнішні дані в блокчейн-системи [14].

Згідно з дослідженнями, атаки випередження становлять значну загрозу для користувачів блокчейн-мереж. За оцінками експертів, щомісяця відбуваються тисячі таких атак, а їх сукупна вартість може сягати мільйонів доларів [15]. Особливо вразливими є децентралізовані фінансові протоколи (DeFi), де невеликі зміни в часі виконання транзакцій можуть призводити до значних фінансових наслідків.

У контексті даного дослідження фокус зосереджено на перших двох типах атак – заміщенні та вставці, оскільки вони найбільш безпосередньо пов'язані з залежністю між комісією та часом обробки транзакцій. Детальна формалізація цих моделей атак дозволить краще зрозуміти значення емпіричного дослідження цієї залежності для оцінки безпеки блокчейн-систем.

2.1.2 Формалізація моделі атаки заміщення

Атака заміщення є одним з найпоширеніших типів атак випередження, особливо в контексті аукціонів та інших сценаріїв, де критичною є «першість» транзакції. Математична формалізація цієї атаки дозволяє кількісно оцінити ймовірність її успіху та залежність цієї ймовірності від параметрів транзакцій та стану мережі.

Модель атаки заміщення можна формалізувати таким чином [1]. Спочатку зловмисник спостерігає за транзакцією жертви з комісією ϕ_v, яка з'являється в мемпулі у момент часу t_0. Далі зловмисник створює

свою транзакцію з комісією $\phi_a > \phi_v$ у момент часу $t_0 + \Delta t$, де Δt – час, необхідний для аналізу транзакції жертви та створення власної транзакції. Атака вважається успішною, якщо транзакція зловмисника буде включена в блок раніше, ніж транзакція жертви.

Ймовірність успіху такої атаки можна оцінити як:

$$P_{success} = P(T_a < T_v) \tag{2.1}$$

де T_a – час до включення в блок транзакції зловмисника, а T_v – час до включення в блок транзакції жертви, починаючи з моменту $t_0 + \Delta t$.

У блокчейн-системах з протоколом консенсусу Proof of Work (PoW), час обробки транзакції з комісією ϕ має експоненційний розподіл з параметром $\lambda(\phi)$, який є функцією від розміру комісії. Це означає, що ймовірність того, що транзакція буде включена в блок у проміжку часу $[0, t]$, визначається як:

$$P(T \leqslant t) = 1 - e^{-\lambda(\phi) \cdot t} \tag{2.2}$$

Враховуючи це, ймовірність успіху атаки заміщення можна виразити як:

$$P_{success} = \frac{\lambda(\phi_a)}{\lambda(\phi_a) + \lambda(\phi_v)} \tag{2.3}$$

Ймовірність успіху цієї атаки залежить від співвідношення параметрів λ, які, у свою чергу, залежать від розмірів комісій. Відповідно, чим сильніша залежність λ від ϕ, тим ефективніше зловмисник може маніпулювати порядком включення транзакцій, просто збільшуючи розмір комісії.

На практиці вид функції $\lambda(\phi)$ залежить від конкретної блокчейн-системи та протоколу консенсусу. Для блокчейнів з PoW протоколом, ця залежність часто має степеневий характер:

$$\lambda(\phi) \propto \phi^b \tag{2.4}$$

де $b > 0$ – параметр, що характеризує силу впливу комісії на швидкість обробки.

Підставляючи це у формулу (2.3), отримуємо:

$$P_{success} = \frac{\phi_a^b}{\phi_a^b + \phi_v^b} \tag{2.5}$$

Це співвідношення демонструє, що ефективність атаки заміщення критично залежить від параметра b, який характеризує залежність між розміром комісії та часом обробки транзакції. Чим більше значення b, тим сильніша ця залежність і тим ефективнішими стають атаки випередження при інших рівних умовах.

Таким чином, емпіричне дослідження характеру залежності часу обробки від комісії має безпосереднє практичне значення для оцінки вразливості блокчейн-систем до атак випередження та розробки механізмів захисту.

2.1.3 Формалізація моделі атаки вставки

Атака вставки є більш складним типом атаки випередження, при якій зловмисник створює дві транзакції, одну для виконання перед цільовою транзакцією, іншу – після неї. Ця стратегія часто використовується на децентралізованих біржах для отримання прибутку від цінового арбітражу.

Процес атаки вставки можна описати наступним чином. Зловмисник спочатку спостерігає за транзакцією жертви з комісією ϕ_v, яка з'являється в мемпулі у момент часу t_0. Виявивши таку транзакцію, він створює дві власні транзакції: першу з комісією $\phi_{a1} > \phi_v$ у момент часу $t_0 + \Delta t$, та другу з комісією $\phi_{a2} < \phi_v$ у той же момент. Атака вважається успішною, якщо перша транзакція зловмисника буде включена в блок раніше, ніж

транзакція жертви, а друга – пізніше.

Ймовірність успіху такої атаки можна представити як добуток ймовірностей двох незалежних подій:

$$P_{success} = P(T_{a1} < T_v) \cdot P(T_{a2} > T_v) \tag{2.6}$$

де T_{a1}, T_{a2} – час до включення в блок першої та другої транзакцій зловмисника відповідно, а T_v – час до включення в блок транзакції жертви.

Використовуючи результати для експоненційного розподілу часу обробки, ці ймовірності можна виразити як:

$$P(T_{a1} < T_v) = \frac{\lambda(\phi_{a1})}{\lambda(\phi_{a1}) + \lambda(\phi_v)} \tag{2.7}$$

$$P(T_{a2} > T_v) = \frac{\lambda(\phi_v)}{\lambda(\phi_{a2}) + \lambda(\phi_v)} \tag{2.8}$$

Об'єднуючи ці вирази, отримуємо загальну ймовірність успіху атаки вставки:

$$P_{success} = \frac{\lambda(\phi_{a1})}{\lambda(\phi_{a1}) + \lambda(\phi_v)} \cdot \frac{\lambda(\phi_v)}{\lambda(\phi_{a2}) + \lambda(\phi_v)} \tag{2.9}$$

Для степеневої залежності $\lambda(\phi) \propto \phi^b$, ця формула набуває вигляду:

$$P_{success} = \frac{\phi_{a1}^b}{\phi_{a1}^b + \phi_v^b} \cdot \frac{\phi_v^b}{\phi_{a2}^b + \phi_v^b} \tag{2.10}$$

Ця формула демонструє, що ефективність атаки вставки також суттєво залежить від параметра b, який характеризує залежність між розміром комісії та часом обробки транзакції. При цьому, на відміну від атаки заміщення, успіх атаки вставки залежить від правильного вибору розмірів комісій для обох транзакцій зловмисника.

Для максимізації ймовірності успіху зловмисник має забезпечити, щоб перша комісія ϕ_{a1} була суттєво вищою за ϕ_v. Це збільшує ймовірність того, що $P(T_{a1} < T_v)$ наближатиметься до 1. Водночас, друга комісія ϕ_{a2}

має бути суттєво нижчою за ϕ_v, щоб забезпечити $P(T_{a2} > T_v) \to 1$.

Емпіричне дослідження характеру залежності часу обробки від комісії має важливе значення не лише для розуміння вразливості блокчейн-систем до атак випередження, але й для розробки стратегій захисту, які могли б зменшити ефективність таких атак.

2.1.4 Вплив параметрів мережі на ймовірність успіху атаки

Окрім залежності часу обробки від розміру комісії, на ймовірність успіху атак випередження впливають й інші параметри блокчейн-мережі, зокрема:

1) **Розмір блоку** (N) – максимальна кількість транзакцій, які можуть бути включені в один блок. Менший розмір блоку створює більшу конкуренцію між транзакціями та може підвищувати значимість комісії для пріоритизації;

2) **Кількість транзакцій у мемпулі** (M) – загальна кількість непідтверджених транзакцій, які очікують на включення в блок. Більший мемпул також посилює конкуренцію;

3) **Середній час між блоками** – визначається протоколом консенсусу та впливає на загальний час обробки транзакцій. Більший інтервал між блоками дає зловмиснику більше часу для аналізу мемпулу та реагування на виявлені транзакції;

4) **Алгоритми відбору транзакцій** – конкретні правила, які використовують майнери для вибору транзакцій з мемпулу. Хоча загальним принципом є максимізація комісій, конкретні алгоритми можуть відрізнятися.

У розділі 3 буде проведено детальне дослідження впливу співвідношення між розміром блоку (N) та кількістю транзакцій у мемпулі (M) на ймовірність успіху атаки випередження, а також виведено аналітичні формули для цієї ймовірності в різних сценаріях.

Емпіричне дослідження характеру залежності часу обробки від

комісії, результати якого будуть представлені в наступному розділі, дозволить більш точно оцінити ризики атак випередження та в майбутньому розробляти ефективні стратегії захисту.

2.2 Методологія дослідження залежності часу обробки від комісії

Для дослідження залежності часу обробки транзакцій від розміру комісії необхідно розробити методологію, яка дозволить зібрати та проаналізувати репрезентативні дані з реальних блокчейн-мереж. У цьому розділі описано підходи до вибору блокчейн-мереж для дослідження, методи збору та обробки даних, а також методи статистичного аналізу, використані для визначення характеру досліджуваної залежності.

2.2.1 Вибір блокчейн-мереж для дослідження

Для забезпечення повноти дослідження та можливості порівняльного аналізу різних протоколів консенсусу важливо обрати репрезентативні блокчейн-мережі. У даному дослідженні було зосереджено увагу на блокчейні Bitcoin як найбільш поширеній та вивченій мережі з протоколом консенсусу Proof of Work.

Bitcoin характеризується використанням протоколу консенсусу Proof of Work, при якому вибір транзакцій для включення в блок здійснюється майнерами, які зазвичай максимізують свій прибуток, надаючи пріоритет транзакціям з вищою комісією. Особливістю цієї мережі є відносно довгий середній час між блоками (близько 10 хвилин), що створює достатнє «вікно можливостей» для спостереження залежності між комісією та часом обробки.

Важливим фактором є також обмежений розмір блоку в мережі

Bitcoin, що створює конкуренцію між транзакціями за включення, особливо в періоди високого навантаження. Публічність та доступність даних про транзакції забезпечує можливість збирати необхідну інформацію для аналізу без значних обмежень.

Вибір Bitcoin як основного об'єкта дослідження обґрунтований тим, що він представляє «класичний» блокчейн з відносно простою моделлю обробки транзакцій, що дозволяє більш чітко виявити базові закономірності залежності часу обробки від комісії. Це надає можливість сформувати фундаментальне розуміння досліджуваної залежності, яке потім може бути застосоване до більш складних блокчейн-систем.

2.2.2 Методи збору даних

Для збору даних про транзакції в мережі Bitcoin було використано спеціалізовані API та публічні сервіси, що надають доступ до історичних блокчейн-даних. Процес збору даних включав кілька ключових етапів.

Спочатку здійснювалось надсилання запитів до спеціалізованих сервісів, що забезпечують доступ до історичної інформації про транзакції, блоки та стан мемпулу. Завдяки цьому було отримано детальні дані про транзакції, включаючи їх параметри (зокрема, розмір комісії) та часові мітки їх появи в пулі очікування.

У межах цього процесу збиралась інформація про момент включення транзакцій до блоку, що дозволило обчислити час очікування кожної транзакції – від моменту її появи в мемпулі до моменту включення в блок. Усі отримані дані зберігалися у структурованому форматі для подальшого аналізу, включаючи ідентифікатори транзакцій, розміри комісій, часові мітки та інші параметри.

Для кожної транзакції було зібрано такі основні характеристики:

– Ідентифікатор транзакції (transaction hash) – унікальний ідентифікатор, що дозволяє однозначно визначити транзакцію в блокчейні;

– Розмір комісії у внутрішніх одиницях блокчейн-мережі (byte для Bitcoin);

– Часові мітки появи в мемпулі та включення в блок;

– Час обробки – різниця між часом включення в блок та часом появи в мемпулі;

– Додаткові параметри – розмір транзакції в байтах, хеш блоку, до якого вона була включена, та інші.

Для дослідження було використано дані з блокчейну Bitcoin за вересень 2024 року. Аналіз включав інформацію з 300 блоків, які містили загалом 1,136,291 транзакцію. Такий часовий проміжок був обраний для забезпечення репрезентативності вибірки, оскільки дозволив охопити періоди з різною завантаженістю мережі – від низької до високої, що суттєво підвищило достовірність отриманих результатів.

2.2.3 Методи попередньої обробки та фільтрації даних

Зібрані дані потребували ретельної попередньої обробки для забезпечення їх якості та релевантності для аналізу. Цей процес включав кілька важливих етапів.

Першим кроком була **фільтрація аномальних значень**. З вибірки були вилучені:

– Транзакції з від'ємним часом обробки (5,694 записів), що могли виникнути внаслідок асинхронності часових міток між вузлами мережі;

– Транзакції з аномально довгим часом обробки (4,280 записів з часом обробки більше 43,370 секунд);

– Транзакції з аномально високими комісіями (20,817 записів з комісією більше 11,916 byte).

Наступним етапом була **нормалізація даних**. Вона передбачала приведення розмірів комісій до єдиних одиниць вимірювання для забезпечення порівнянності даних. Також проводилась нормалізація часових інтервалів для врахування часових зон та коректного обчислення

часу обробки.

Важливою частиною обробки даних була їх **сегментація**. Для зменшення дисперсії та підвищення інтерпретованості залежності між параметрами, дані були згруповані за значенням комісії. Весь діапазон комісій було поділено на 2,000 рівних інтервалів. Для кожного інтервалу обчислено середнє значення комісії та середній час обробки для всіх транзакцій, що до нього потрапили. Інтервали без жодної транзакції були вилучені з подальшого аналізу. Також проводилось групування транзакцій за періодами для врахування можливого впливу часових факторів.

Після фільтрації та обробки для аналізу залишилося 1,105,500 транзакцій, що складає 97.29% від початкового обсягу даних. Зменшення вибірки пов'язане з необхідністю забезпечити високу якість даних для отримання достовірних результатів аналізу.

2.2.4 Методи статистичного аналізу

Для визначення характеру залежності часу обробки транзакцій від розміру комісії було застосовано комплекс методів статистичного аналізу.

Кореляційний аналіз став першим етапом дослідження статистичного зв'язку між комісією та часом обробки. Були обчислені коефіцієнти кореляції Пірсона, Спірмена та Кендалла. Коефіцієнт Пірсона дозволяє оцінити силу та напрямок лінійної залежності між змінними, тоді як коефіцієнти Спірмена та Кендалла не потребують лінійності залежності і є більш стійкими до викидів. Використання трьох різних коефіцієнтів кореляції забезпечило більш повну характеристику статистичного зв'язку між досліджуваними величинами. Для всіх коефіцієнтів кореляції була проведена перевірка їх статистичної значущості.

Регресійний аналіз дозволив визначити форму залежності між комісією та часом обробки. Були побудовані та оцінені моделі різного

типу: лінійна, степенева, експоненційна та логарифмічна. Параметри моделей оцінювались методом найменших квадратів. Для порівняння моделей обчислювались такі метрики як коефіцієнт детермінації (R^2), середньоквадратична помилка (MSE) та інформаційний критерій Акаіке (AIC). На основі цих метрик було обрано оптимальну модель, яка найкраще описує емпіричні дані.

Для проведення статистичного аналізу використовувались сучасні програмні інструменти та бібліотеки, які забезпечують високу точність та надійність обчислень. Комплексне застосування різних методів статистичного аналізу дозволило отримати результати щодо характеру залежності часу обробки транзакцій від розміру комісії.

2.3 Зв'язок між атаками випередження та залежністю часу обробки від комісії

Розуміння характеру залежності часу обробки транзакцій від розміру комісії має не лише теоретичне, але й практичне значення для оцінки вразливості блокчейн-систем до атак випередження та розробки ефективних захисних механізмів. У цьому підрозділі розглядається взаємозв'язок між математичними моделями атак випередження та емпіричним дослідженням залежності часу-комісії, що дозволяє більш точно оцінити ризики та розробити стратегії захисту.

2.3.1 Теоретичні передумови впливу часу обробки на успішність атаки

Як було показано в попередніх підрозділах, ймовірність успіху атак випередження безпосередньо залежить від характеру функції $\lambda(\phi)$, яка пов'язує розмір комісії з параметром експоненційного розподілу часу обробки. Ключова передумова для успішної атаки випередження –

можливість зловмисника впливати на порядок включення транзакцій шляхом маніпулювання розміром комісії.

Теоретичні моделі описують залежність між часом обробки транзакцій та успішністю атак випередження. Для атаки заміщення, ймовірність успіху якої визначається формулою:

$$P_{success} = \frac{\lambda(\phi_a)}{\lambda(\phi_a) + \lambda(\phi_v)} \tag{2.11}$$

вирішальне значення має саме форма функції $\lambda(\phi)$. Чим сильніша залежність між комісією та швидкістю обробки, тим ефективніше зловмисник може маніпулювати порядком включення транзакцій у блок.

У теоретичних моделях часто припускається, що функція $\lambda(\phi)$ має степеневий характер:

$$\lambda(\phi) \propto \phi^b \tag{2.12}$$

де $b > 0$ – параметр, який характеризує силу впливу комісії на швидкість обробки. Значення параметра b є критичним для визначення вразливості блокчейн-системи до атак випередження. Для ілюстрації, можна проаналізувати зміну ймовірності успіху атаки заміщення при різних значеннях параметра b та різних співвідношеннях комісій ϕ_a/ϕ_v:

– При $b = 1$ (лінійна залежність) і $\phi_a = 2 \cdot \phi_v$, ймовірність успіху атаки становить $P_{success} = 2/3 \approx 0.67$.

– При $b = 2$ (квадратична залежність) і тому ж співвідношенні комісій, ймовірність зростає до $P_{success} = 4/5 = 0.8$.

– При $b = 0.5$ (квадратично-коренева залежність) і тому ж співвідношенні комісій, ймовірність знижується до $P_{success} = \sqrt{2}/(1 + \sqrt{2}) \approx 0.59$.

Цей приклад демонструє, що при більших значеннях b навіть незначне збільшення комісії дає зловмиснику значну перевагу. Для атаки вставки ситуація аналогічна – параметр b визначає, наскільки ефективно зловмисник може контролювати порядок включення своїх транзакцій

відносно транзакції жертви.

Важливо зазначити, що теоретичні моделі базуються на припущенні про експоненційний розподіл часу обробки транзакцій з параметром, залежним від розміру комісії. Перевірка цього припущення на реальних даних є важливим завданням емпіричного дослідження.

2.3.2 Значення залежності часу-комісії для оцінки вразливості мережі

Емпіричне дослідження залежності часу обробки від комісії дозволяє перейти від теоретичних моделей до практичної оцінки вразливості блокчейн-систем до атак випередження. Встановлення фактичної форми функції $\lambda(\phi)$ для конкретної блокчейн-мережі дозволяє обчислити реальну ймовірність успіху атак різних типів при різних сценаріях.

Знання конкретних параметрів залежності часу обробки від комісії має значення для різних категорій учасників блокчейн-екосистеми:

Для користувачів блокчейн-систем – ці знання дозволяють обирати оптимальний розмір комісії з урахуванням ризику стати жертвою атаки випередження. Наприклад, для критично важливих транзакцій може бути доцільним встановлення комісії суттєво вищої за середній рівень, щоб мінімізувати ризик атаки.

Для розробників децентралізованих додатків – розуміння характеру залежності дозволяє розробляти протоколи, які менш вразливі до атак випередження. Зокрема, можуть бути впроваджені механізми, які зменшують прозорість намірів користувачів, наприклад, через шифрування параметрів транзакцій або затримку їх розкриття.

Для розробників блокчейн-протоколів – емпіричні дані про характер залежності часу-комісії можуть стати основою для вдосконалення алгоритмів вибору транзакцій, що зменшують

ефективність атак випередження. Наприклад, можуть бути розроблені механізми, які зменшують значення параметра b, тим самим знижуючи вплив комісії на порядок включення транзакцій.

Окрім оцінки загальної вразливості, дослідження залежності часу-комісії дозволяє виявити умови, при яких атаки випередження стають особливо ефективними. Наприклад, можна визначити, як навантаження на мережу впливає на характер залежності та, відповідно, на ймовірність успіху атак. Це дає можливість розробляти адаптивні стратегії захисту, які враховують поточний стан мережі.

Важливим аспектом є також порівняльний аналіз різних блокчейн-систем з точки зору їх вразливості до атак випередження. Різні протоколи консенсусу можуть демонструвати різний характер залежності часу обробки від комісії, і, відповідно, різний рівень вразливості. Це дозволяє оцінювати безпеку різних систем та робити обґрунтований вибір при розробці нових додатків.

2.3.3 Обґрунтування важливості емпіричного дослідження

Теоретичні моделі атак випередження, розглянуті на початку Розділу 2, базуються на певних припущеннях, які потребують емпіричної верифікації. Найбільш критичними є припущення про:

– Експоненційний розподіл часу обробки транзакцій;

– Степеневий характер залежності параметра λ від розміру комісії;

– Незалежність часу обробки від інших факторів, окрім розміру комісії.

Емпіричне дослідження дозволяє перевірити ці припущення та, за необхідності, уточнити теоретичні моделі. Відхилення реальних даних від теоретичних передбачень може вказувати на наявність додаткових факторів, які впливають на процес обробки транзакцій і не враховані в початкових моделях.

Важливість емпіричного дослідження також полягає в можливості

виявлення нових закономірностей та ефектів, не передбачених теоретичними моделями. Наприклад, можуть бути виявлені порогові ефекти, коли залежність часу обробки від комісії різко змінюється при певних значеннях комісії, або нелінійні взаємодії між різними факторами, що впливають на час обробки.

Емпіричні дані дозволяють також оцінити стабільність залежності часу-комісії в часі та при різних умовах. Теоретичні моделі зазвичай передбачають стаціонарний характер цієї залежності, однак на практиці вона може змінюватися залежно від загального навантаження на мережу, активності майнерів, змін у протоколі та інших факторів.

Окрім верифікації теоретичних моделей, емпіричне дослідження має й практичне значення, оскільки дозволяє розробляти конкретні рекомендації для користувачів блокчейн-систем та розробників протоколів. Зокрема, воно може допомогти визначити оптимальний розмір комісії для різних сценаріїв використання та різних умов мережі.

Для боротьби з атаками випередження необхідне глибоке розуміння механізмів їх функціонування, що можливе лише при поєднанні теоретичного аналізу з емпіричним дослідженням. Комплексний підхід, що включає як математичне моделювання, так і аналіз реальних даних, дозволяє розробляти ефективні стратегії захисту, які враховують специфіку конкретних блокчейн-систем.

Висновки до розділу 2

У даному розділі розроблено теоретичні основи дослідження залежності часу обробки транзакцій від розміру комісії та їх зв'язок з атаками випередження в блокчейн-системах. Формалізовано математичні моделі атак заміщення та вставки, які демонструють, що їх ефективність безпосередньо залежить від характеру функції $\lambda(\phi)$, що пов'язує комісію з часом обробки.

Представлено методологію емпіричного дослідження цієї

залежності, включаючи збір та обробку даних з мережі Bitcoin. Обґрунтовано необхідність верифікації теоретичних моделей на основі реальних даних для адекватної оцінки безпеки блокчейн-систем.

Теоретичні моделі та методологічні підходи, розглянуті в цьому розділі, створюють підґрунтя для емпіричного дослідження, результати якого будуть представлені в наступному розділі роботи.

3 ТЕОРЕТИЧНІ ТА ЕМПІРИЧНІ РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ АТАК ВИПЕРЕДЖЕННЯ

У даному розділі представлено результати дослідження залежності часу обробки транзакцій від їх параметрів, зокрема від розміру комісії, та проведено аналіз впливу цієї залежності на вразливість блокчейн-систем до атак випередження. На основі теоретичних моделей, розглянутих у попередньому розділі, формалізовано ймовірність успішного випередження транзакцій при різних умовах мережі, а також проведено емпіричне дослідження характеру залежності часу обробки від комісії на реальних даних.

3.1 Обчислення ймовірності випередження транзакції

Дослідження залежності часу обробки транзакцій від розміру комісії нерозривно пов'язане з безпекою блокчейн-систем, зокрема з атаками випередження. Для розуміння цього зв'язку потрібно глибоко проаналізувати механізми обробки транзакцій у блокчейн-мережах та формалізувати ймовірнісні моделі, що описують взаємодію різних акторів у цих мережах.

У попередньому розділі було розглянуто загальні аспекти блокчейн-технологій, показано, що транзакції з вищою комісією зазвичай обробляються швидше, створюючи природний економічний механізм пріоритезації. Проте існує важливий граничний випадок, який потребує окремого аналізу — ситуація, коли залежність між розміром комісії та часом обробки стає невираженою або відсутньою.

Такий стан може спостерігатися за різних обставин: при низькому завантаженні мережі, коли всі транзакції включаються до блоку незалежно від комісії; при однакових комісіях у кількох транзакціях, що

створює невизначеність у їх пріоритезації; або в деяких протоколах консенсусу, де час обробки визначається іншими факторами.

Вартість випадковості порядку транзакцій полягає в тому, що вона відкриває додаткову поверхню атаки для зловмисників. Навіть без маніпуляцій комісією, просте розуміння статистичної природи процесу включення транзакцій у блок може бути використане для отримання неправомірної переваги.

Для формального аналізу цієї проблеми введемо наступну модель: нехай у мережі з'являються дві транзакції — одна від чесного користувача T_h та одна від потенційного зловмисника T_a. Обидві транзакції мають однакову комісію та подібні характеристики, що виключає детерміновану пріоритезацію однієї над іншою. Зауважимо, що такий сценарій є досить реалістичним у періоди низького навантаження на мережу або в разі, коли зловмисник навмисно підбирає комісію, ідентичну до комісії жертви.

Основне питання, на яке потрібно відповісти: яка ймовірність того, що транзакція зловмисника T_a буде обрана для включення в блок раніше за транзакцію чесного користувача T_h? Від відповіді на це питання залежить оцінка ефективності атаки випередження та розробка механізмів протидії.

Для моделювання цієї ситуації необхідно враховувати співвідношення між кількістю транзакцій у мемпулі (M) та максимальною місткістю блоку (N). Це співвідношення визначає, чи всі транзакції будуть включені до поточного блоку, або ж відбуватиметься конкуренція за обмежений ресурс.

Розглянемо два принципово різних випадки:

1) $M \leqslant N$ – усі транзакції з мемпула гарантовано потраплять до блоку, різниця лише в їхньому порядку;

2) $M > N$ – лише частина транзакцій з мемпула буде включена до поточного блоку, що створює додаткову невизначеність щодо того, чи потрапить конкретна транзакція до блоку взагалі.

Для кожного з цих випадків потрібно розробити окрему математичну модель, яка дозволить кількісно оцінити ймовірність успіху

атаки випередження за умови випадкового порядку включення транзакцій.

3.1.1 Модель ймовірності випередження при повному включенні транзакцій у блок ($M \leqslant N$)

Першим розглянемо випадок, коли всі транзакції з мемпула гарантовано включаються до блоку, тобто $M \leqslant N$. У цій ситуації єдиним фактором, що впливає на успіх атаки випередження, є порядок включення транзакцій.

За відсутності диференціації за розміром комісії або іншими параметрами, можна припустити, що всі можливі перестановки транзакцій мають однакову ймовірність. Тобто порядок, у якому транзакції включаються до блоку, є рівномірно випадковим.

Формалізуємо це припущення математично:

Теорема 3.1 (Ймовірність успішного випередження при повному включенні транзакцій у блок)**.** *Нехай у мемпулі у момент формування блоку міститься M транзакцій, усі з яких гарантовано потрапляють до блоку. Якщо дві транзакції – чесного користувача T_h і зловмисника T_a – мають однакову комісію та включаються до блоку у випадковому порядку, то ймовірність того, що T_a буде розміщена в блоці раніше, дорівнює:*

$$P(T_a < T_h) = \frac{1}{2}. \tag{3.1}$$

Доведення. У даній моделі припускається, що всі M транзакцій формують блок без пріоритетів. Такий сценарій характерний, наприклад, для періодів низького навантаження на мережу або для блоків із високим розміром у відношенні до активності мемпулу. За цих умов усі $M!$ перестановок мають однакову ймовірність.

Ймовірність того, що транзакція T_h буде розміщена на позиції i у

блоці, становить:

$$P(T_h = i) = \frac{1}{M}. \tag{3.2}$$

За фіксованого i, існує $i - 1$ позицій перед T_h, на які може бути розміщено T_a:

$$P(T_a < T_h | T_h = i) = \frac{i-1}{M-1}. \tag{3.3}$$

Ця умова враховує лише ті позиції, на які може потрапити T_a, окрім T_h.

Тоді загальна ймовірність:

$$P(T_a < T_h) = \sum_{i=1}^{M} \frac{1}{M} \cdot \frac{i-1}{M-1}. \tag{3.4}$$

Вона зводиться до:

$$P(T_a < T_h) = \frac{1}{M(M-1)} \sum_{i=1}^{M} (i-1) = \frac{1}{M(M-1)} \cdot \frac{(M-1)M}{2}. \tag{3.5}$$

Після скорочення:

$$P(T_a < T_h) = \frac{1}{2}. \tag{3.6}$$

□

Результат теореми показує, що в умовах повного включення транзакцій до блоку та відсутності детермінованої пріоритезації, ймовірність випередження становить рівно 0.5. Це означає, що в ситуації «чистої випадковості» зловмисник має рівно 50% шансів на успіх атаки випередження.

Важливо підкреслити, що це значення є верхньою теоретичною межею успіху для зловмисника за найбільш сприятливих умов. У реальних мережах майнери (або валідатори) можуть застосовувати різні евристики для визначення порядку транзакцій, наприклад, принцип «першим прийшов — першим обслуговується» (FIFO), що може суттєво знизити шанси зловмисника.

Крім того, у реальних блокчейн-системах існує часова асиметрія –

зловмисник вимушений створювати свою транзакцію після того, як виявить транзакцію жертви в мемпулі, що додає затримку. Ця затримка може впливати на порядок обробки, зменшуючи ймовірність успішного випередження.

Тим не менш, навіть значення ймовірності 0.5 є достатньо високим, аби вважати атаку випередження серйозною загрозою в умовах рівномірно випадкового порядку включення транзакцій. Тому важливо розробляти механізми, які зменшують випадковість у визначенні порядку включення транзакцій та підвищують детермінованість цього процесу.

3.1.2 Модель ймовірності випередження при обмеженні розміром блоку ($M > N$)

Тепер розглянемо більш складний і практично важливий випадок, коли кількість транзакцій у мемпулі перевищує максимальну місткість блоку, тобто $M > N$. У такій ситуації не всі транзакції будуть включені до поточного блоку, що додає важливий аспект невизначеності — транзакція може не потрапити до блоку взагалі.

Цей сценарій є більш характерним для реальних блокчейн-мереж, особливо в періоди високого навантаження. Для моделювання цієї ситуації потрібно враховувати не лише порядок включення транзакцій, але й сам факт їх включення до блоку.

Розширимо нашу модель, формалізувавши успіх атаки випередження для випадку $M > N$:

Теорема 3.2 (Ймовірність успішного випередження при $M > N$)**.** *Нехай M – кількість транзакцій в мемпулі , N – розмір блоку, причому $M > N$. Якщо обидві транзакції T_h і T_a мають однакову комісію, то ймовірність того, що T_a буде включена до блоку і розміщена раніше за T_h, дорівнює:*

$$P_{success} = \frac{N(2M - N - 1)}{2M(M - 1)}. \tag{3.7}$$

Доведення. Розглянемо всі можливі сценарії розміщення транзакцій T_a і T_h щодо блоку B. Ймовірність успішного випередження складається з двох взаємовиключних випадків:

$$P_{success} = P(T_a \in B \wedge T_h \notin B) + P(T_a \in B \wedge T_h \in B) \cdot P(T_a < T_h | T_a, T_h \in B). \tag{3.8}$$

Перший доданок представляє ситуацію, коли транзакція зловмисника включена до блоку, а транзакція жертви — ні. Це автоматично означає успіх атаки.

Розглянемо кожен доданок окремо.

(1) T_a потрапляє до блоку, а T_h — ні ($T_a \in B$, $T_h \notin B$):

Ймовірність перетину подій:

$$P(T_a \in B \wedge T_h \notin B) = P(T_a \in B) \cdot P(T_h \notin B | T_a \in B). \tag{3.9}$$

Ймовірність включення T_a до блоку за умови рівномірного випадкового вибору серед M транзакцій:

$$P(T_a \in B) = \frac{N}{M}. \tag{3.10}$$

За умови, що T_a вже обрана, з $M - 1$ транзакцій, що залишилися, потрібно вибрати додатково $N - 1$ для заповнення блоку. Імовірність, що T_h не буде серед них:

$$P(T_h \notin B | T_a \in B) = \frac{M - N}{M - 1}. \tag{3.11}$$

Отже:

$$P(T_a \in B \wedge T_h \notin B) = \frac{N}{M} \cdot \frac{M - N}{M - 1}. \tag{3.12}$$

(2) Обидві транзакції потрапляють до блоку, але T_a розміщена раніше за T_h ($T_a \in B$, $T_h \in B$, і $T_a < T_h$):

Для цього випадку маємо:

$$P(T_a \in B \wedge T_h \in B) = P(T_a \in B) \cdot P(T_h \in B | T_a \in B). \tag{3.13}$$

Як і в першому випадку, $P(T_a \in B) = \frac{N}{M}$.

Ймовірність включення T_h до блоку за умови, що T_a вже включена:

$$P(T_h \in B | T_a \in B) = \frac{N-1}{M-1}. \tag{3.14}$$

Таким чином:

$$P(T_a \in B \wedge T_h \in B) = \frac{N}{M} \cdot \frac{N-1}{M-1}. \tag{3.15}$$

За умови включення обох транзакцій до блоку, ймовірність того, що T_a буде розміщена раніше за T_h, як показано у теоремі 3.1, становить:

$$P(T_a < T_h | T_a, T_h \in B) = \frac{1}{2}. \tag{3.16}$$

Отже:

$$P(T_a \in B \wedge T_h \in B) \cdot P(T_a < T_h | T_a, T_h \in B) = \frac{N}{M} \cdot \frac{N-1}{M-1} \cdot \frac{1}{2}. \tag{3.17}$$

Підсумовуючи обидва випадки, отримуємо загальну ймовірність успіху атаки випередження:

$$P_{success} = \frac{N}{M} \cdot \frac{M-N}{M-1} + \frac{N}{M} \cdot \frac{N-1}{M-1} \cdot \frac{1}{2} = \frac{N(2M-N-1)}{2M(M-1)}. \tag{3.18}$$

□

Отримана формула дозволяє кількісно оцінити ймовірність успіху атаки випередження в умовах обмеженого розміру блоку. На відміну від попереднього випадку, ця ймовірність залежить від співвідношення між M і N, що відображає вплив завантаженості мережі на безпеку.

Один із найважливіших моментів, який виявляє дана модель, полягає в тому, що в ситуації з конкуренцією за місце в блоці (коли $M > N$) зловмисник має додатковий механізм атаки — не просто випередити транзакцію жертви, але й повністю витіснити її з поточного блоку. Це суттєво розширює поверхню атаки і значно ускладнює захист від атак випередження.

З іншого боку, завантаженість мережі (зростання співвідношення M/N) може також знижувати ймовірність успіху атаки, оскільки з однаковою ймовірністю може бути витіснена і транзакція зловмисника. Отже, вплив завантаженості на безпеку є неоднозначним і потребує детального аналізу для конкретних параметрів мережі.

Для практичного розуміння впливу співвідношення M/N на ймовірність успіху атаки, доцільно розглянути кілька конкретних випадків.

3.1.3 Аналітичні приклади для моделі з $M > N$ при різних співвідношеннях M/N

Для поглибленого розуміння залежності ймовірності успіху атаки випередження від співвідношення кількості транзакцій у мемпулі до розміру блоку, розглянемо кілька характерних випадків. Це дозволить не тільки верифікувати отримані формули, але й отримати важливі практичні висновки щодо безпеки різних конфігурацій блокчейн-мереж.

У кожному випадку підставимо відповідне значення M у формулу ймовірності успіху атаки:

$$P_{success} = \frac{N(2M - N - 1)}{2M(M - 1)}. \tag{3.19}$$

Випадок 1: $M = N + 1$ (мінімальне перевищення розміру мемпула над розміром блоку)

Підставивши $M = N + 1$ у формулу, отримаємо:

$$\begin{aligned} P_{\text{success}} &= \frac{N\big(2(N+1) - N - 1\big)}{2(N+1)\big((N+1) - 1\big)} = \\ &= \frac{N}{N+1} \cdot \frac{(N+1) - N}{(N+1) - 1} + \frac{N}{N+1} \cdot \frac{N-1}{(N+1) - 1} \cdot \frac{1}{2} = \\ &= \frac{N}{N+1} \cdot \frac{1}{N} + \frac{N}{N+1} \cdot \frac{N-1}{N} \cdot \frac{1}{2} = \\ &= \frac{1}{N+1} + \frac{N-1}{2(N+1)} = \frac{2+N-1}{2(N+1)} = \frac{1}{2}. \end{aligned} \tag{3.20}$$

Цей результат показує, що при мінімальному перевищенні розміру мемпула над розміром блоку (на 1 транзакцію), ймовірність успіху атаки випередження залишається рівною 0.5, тобто такою ж, як і у випадку повного включення всіх транзакцій ($M \leqslant N$). Це означає, що граничний перехід від повного включення до ситуації з відбором транзакцій є неперервним, що підтверджує коректність отриманих формул.

Випадок 2: $M = N+2$ (незначне перевищення розміру мемпула над розміром блоку)

Підставивши $M = N + 2$ у формулу, отримаємо:

$$\begin{aligned} P_{\text{success}} &= \frac{N\big(2(N+2) - N - 1\big)}{2(N+2)\big((N+2) - 1\big)} = \\ &\frac{N}{N+2} \frac{(N+2) - N}{(N+2) - 1} + \frac{N}{N+2} \frac{N-1}{(N+2) - 1} \frac{1}{2} = \\ &= \frac{N}{N+2} \frac{2}{N+1} + \frac{N}{N+2} \frac{N-1}{N+1} \frac{1}{2} = \\ &= \frac{2N}{(N+2)(N+1)} + \frac{N(N-1)}{2(N+2)(N+1)} = \\ &= \frac{N^2 + 3N}{2(N+2)(N+1)} = \frac{N(N+3)}{2(N+2)(N+1)}. \end{aligned} \tag{3.21}$$

Для конкретних значень N ця формула дає ймовірність, близьку, але трохи меншу за 0.5. Наприклад, при $N = 100$ (що є типовим розміром

блоку для деяких блокчейн-мереж), отримаємо:

$$P_{success} = \frac{100(100+3)}{2(100+2)(100+1)} = \frac{100 \cdot 103}{2 \cdot 102 \cdot 101} = \frac{10300}{20604} \approx 0.4999. \quad (3.22)$$

Цей результат показує, що при незначному перевищенні розміру мемпула над розміром блоку (на 2 транзакції) ймовірність успіху атаки практично не змінюється порівняно з випадком повного включення транзакцій. Це має важливе практичне значення, оскільки свідчить про те, що навіть незначна конкуренція за місце в блоці майже не впливає на рівень безпеки щодо атак випередження.

Випадок 3: $M = 1.5N$ (помірне перевищення розміру мемпула над розміром блоку)

Підставивши $M = 1.5N$ у формулу, отримаємо (після спрощення алгебраїчних виразів):

$$P_{success} = \frac{4N-2}{3(3N-2)} \quad (3.23)$$

Для $N = 100$:

$$P_{success} = \frac{4 \cdot 100 - 2}{3(3 \cdot 100 - 2)} = \frac{398}{3 \cdot 298} = \frac{398}{894} \approx 0.4452. \quad (3.24)$$

При помірному перевищенні розміру мемпула над розміром блоку (у 1.5 рази) ймовірність успіху атаки вже суттєво знижується — до приблизно 44.5% для $N = 100$. Це показує, що зростання конкуренції за місце в блоці починає відігравати роль у зниженні ризиків атаки випередження.

Випадок 4: $M = 2N$ (значне перевищення розміру мемпула над розміром блоку)

Підставивши $M = 2N$ у формулу, отримаємо:

$$P_{success} = \frac{3N-1}{4(2N-1)} \quad (3.25)$$

Для $N = 100$:

$$P_{success} = \frac{3 \cdot 100 - 1}{4(2 \cdot 100 - 1)} = \frac{299}{4 \cdot 199} = \frac{299}{796} \approx 0.3756. \quad (3.26)$$

При подвійному перевищенні розміру мемпула над розміром блоку ймовірність успіху атаки знижується до приблизно 37.6% для $N = 100$. Це вже суттєве зниження порівняно з початковими 50%, що підтверджує важливу роль завантаженості мережі у формуванні рівня безпеки.

Випадок 5: $M = 3N$ (високе перевищення розміру мемпула над розміром блоку)

Підставивши $M = 3N$ у формулу, отримаємо:

$$P_{success} = \frac{5N - 1}{6(3N - 1)} \tag{3.27}$$

Для $N = 100$:

$$P_{success} = \frac{5 \cdot 100 - 1}{6(3 \cdot 100 - 1)} = \frac{499}{6 \cdot 299} = \frac{499}{1794} \approx 0.2781. \tag{3.28}$$

При потрійному перевищенні розміру мемпула над розміром блоку ймовірність успіху атаки знижується до приблизно 27.8% для $N = 100$. Це вже дуже значне зниження ризику атаки випередження.

Узагальнимо отримані результати у формі таблиці.

Таблиця 3.1 – Аналітичні вирази для ймовірності успіху атаки випередження при різних співвідношеннях M/N

Випадок	Значення M	$P_{success}$
1	$N + 1$	$\frac{1}{2}$
2	$N + 2$	$\frac{N(N+3)}{2(N+2)(N+1)}$
3	$\frac{3}{2}N$	$\frac{4N-2}{3(3N-2)}$
4	$2N$	$\frac{3N-1}{4(2N-1)}$
5	$3N$	$\frac{5N-1}{6(3N-1)}$

Та в числовому вигляді для $N = 100$:

Аналіз отриманих значень імовірності успішного випередження $P_{success}$ показує чітку залежність між співвідношенням кількості

Таблиця 3.2 – Числові значення ймовірності успіху атаки випередження при $N = 100$

Випадок	M	M/N	$P_{success}$
1	101	1.01	0.5
2	102	1.02	0.4999
3	150	1.50	0.4452
4	200	2.00	0.3756
5	300	3.00	0.2781

транзакцій у мемпулі (M) та розміром блоку (N) і ризиком front-running-атаки. Цю залежність доцільно проаналізувати детальніше:

1) У граничному випадку, коли $M = N + 1$, ймовірність успіху зловмисника дорівнює точно 0,5. Це відображає повну симетрію між чесним учасником і атакувальником. Важливим є те, що це значення є точним незалежно від конкретного розміру блоку N, тобто для будь-якої блокчейн-системи з мінімальним перевищенням розміру мемпула над розміром блоку потенційний ризик атаки випередження становить рівно 50%.

2) При незначному перевищенні M над N $(M = N + 2)$, ймовірність лише трохи зменшується (до 0,4999 при $N = 100$), що свідчить про збереження суттєвого ризику front-running-атаки. Ця близькість значення до 0,5 показує, що незначна конкуренція за місце в блоці практично не впливає на безпеку.

3) Зі зростанням співвідношення M/N ймовірність успішного випередження значно знижується. Наприклад, при $M = 1{,}5N$ вона вже становить приблизно 0,4452, при $M = 2N$ — 0,3756, а при $M = 3N$ — лише 0,2781. Це свідчить про те, що підвищена конкуренція за місце в блоці справді може створювати природний бар'єр проти атак випередження.

4) Однак варто зазначити, що навіть при потрійному перевищенні розміру мемпула над розміром блоку $(M = 3N)$ ймовірність успіху атаки

залишається досить високою — майже 28%. Це значення, хоча і значно нижче за початкові 50%, все ще є істотним ризиком безпеки, що потребує додаткових захисних механізмів.

Рисунок 3.1 – Графік залежності ймовірності успіху атаки випередження від співвідношення M/N при $N = 100$

Представлені результати мають важливі практичні наслідки для безпеки блокчейн-систем:

1) Перевантаження мемпулу природним чином знижує шанси зловмисника навіть за рівних умов комісії. Це пов'язано з тим, що конкуренція за місце в блоці посилюється, а випадкове включення починає працювати проти одиночних транзакцій атакувальника.

2) З іншого боку, в умовах низького навантаження на мережу (коли M близьке до N) ризик атаки випередження максимальний, що вимагає додаткових захисних механізмів саме в таких режимах роботи блокчейну.

3) В реальних умовах зловмисник може компенсувати зниження ймовірності успіху атаки при високих значеннях M/N шляхом штучного збільшення кількості власних транзакцій із однаковими параметрами (кластеризація). Створюючи множинні копії своєї транзакції, він ефективно збільшує ймовірність того, що хоча б одна з них буде включена до блоку і виконана раніше за транзакцію жертви.

4) Така стратегія кластеризації особливо ефективна при високих значеннях M/N, коли базова ймовірність успіху для одиночної транзакції низька, але створення множинних копій може значно підвищити загальні шанси на успіх атаки.

Проведений аналіз показує, що співвідношення M/N є важливим параметром для моделювання безпеки протоколу обробки транзакцій. Цей параметр слід враховувати при проєктуванні політик включення транзакцій до блоку та при побудові механізмів захисту від

front-running-атак.

Зокрема, отримані результати обґрунтовують необхідність розробки спеціальних механізмів протидії кластеризації транзакцій, які б могли виявляти та «карати» спроби множинного клонування транзакцій з метою атаки. Такі механізми можуть включати в себе:

1) Детермінований вибір транзакцій для включення в блок, наприклад, на основі хешу транзакції або інших криптографічних примітивів, що значно ускладнить атаки випередження;

2) Механізми виявлення клонів транзакцій з подальшим зниженням пріоритету всіх клонів;

3) Впровадження часових міток при включенні транзакцій до мемпулу та використання їх для пріоритизації транзакцій за принципом FIFO, що зменшить ефективність атак випередження.

Таким чином, отримані теоретичні результати не лише дозволяють кількісно оцінити ризик атак випередження в різних режимах роботи блокчейн-мережі, але й надають основу для розробки ефективних механізмів протидії таким атакам.

3.2 Аналіз отриманих результатів

Відповідно до описаної в Розділі 2 методології було зібрано та опрацьовано дані про транзакції з різних блокчейн-мереж. Попередній аналіз цих даних показав, що залежність між розміром комісії та часом обробки транзакцій має нелінійний характер, особливо для блокчейнів з протоколом Proof of Work. На рисунку 3.2 представлено графік залежності середнього часу обробки від середнього розміру комісії для перших 500 інтервалів із загальної вибірки, де червоною рамкою виділена зона особливого інтересу.

З графіка видно, що залежність має виражений спадний характер для менших значень комісії, але при досягненні певного порогового значення час обробки стає майже константним. Це підтверджує

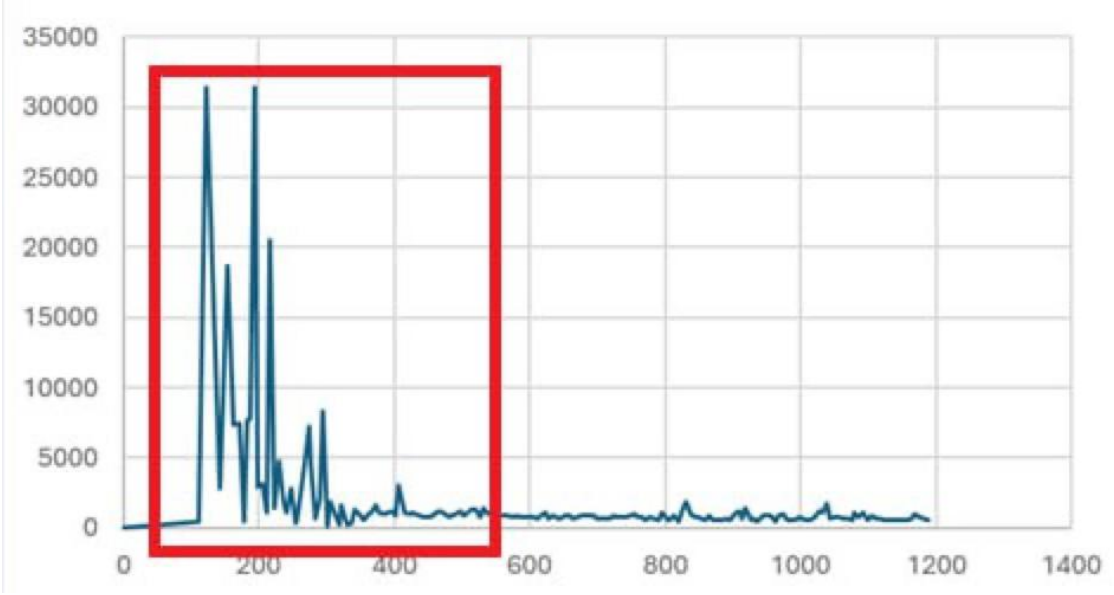

Рисунок 3.2 – Залежність середнього часу обробки транзакцій від середнього розміру комісії

теоретичне припущення про існування асимптотичної нижньої межі часу обробки, яка визначається технічними характеристиками мережі, такими як час генерації блоку.

Для більш детального аналізу був обраний діапазон перших 500 інтервалів, де залежність є найбільш вираженою. Фактично, для аналізу було використано 477 інтервалів, оскільки частина інтервалів була порожньою (не містила жодної транзакції). Детальніший аналіз показав, що в межах цього діапазону спостерігається зворотна залежність: при збільшенні розміру комісії час обробки транзакції зменшується.

Форма залежності візуально нагадує степеневу або експоненційну функцію, що узгоджується з теоретичною моделлю, представленою в Розділі 1, де було припущено, що для блокчейнів з PoW протоколом час обробки може бути апроксимований функцією виду $T = a \cdot \phi^{-b} + c$ або $T = \alpha \cdot e^{-\beta \cdot \phi} + \gamma$, де ϕ – розмір комісії, а T – час обробки.

Важливо зазначити, що при аналізі даних було виявлено особливість, яка потребує окремого розгляду. Серед усіх проаналізованих транзакцій значна частина (приблизно 33%) мала нульовий час обробки. Така ситуація означає, що транзакція була включена до блоку практично

одночасно з моментом її потрапляння до мережі. Враховуючи, що дослідження охоплювало часові інтервали з підвищеною активністю, нульовий час обробки не може бути пояснений порожнім мемпулом.

Ймовірною причиною є використання великими майнінговими пулами приватних мемпулів або пришвидшених каналів передачі транзакцій. Такі пули можуть обробляти транзакції, які надходять через приватні протоколи або партнерські API, минаючи загальний мемпул. Це явище має важливе значення для розуміння реальних процесів формування блоків та може впливати на ефективність атак випередження, розглянутих у Розділі 3.1.

Для коректного аналізу залежності часу обробки від комісії транзакції з нульовим часом обробки були виключені з вибірки, оскільки вони не відображають типовий процес обробки через загальний мемпул.

3.3 Розрахунок та інтерпретація коефіцієнтів кореляції

Для кількісної оцінки взаємозв'язку між розміром комісії та часом обробки транзакцій було проведено різні типи кореляційного аналізу. Оскільки візуальний аналіз даних вказує на нелінійний характер залежності, важливо розглянути не лише традиційний коефіцієнт кореляції Пірсона, який вимірює силу лінійного зв'язку, але й інші міри зв'язку, які можуть краще відображати нелінійні залежності.

3.3.1 Коефіцієнт кореляції Пірсона

Коефіцієнт кореляції Пірсона вимірює силу лінійного зв'язку між двома змінними і визначається формулою:

$$r = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2}} \tag{3.29}$$

де x_i — значення комісії, y_i — значення часу обробки, $\bar{x}$ та $\bar{y}$ — їх

середні значення.

Для вибірки з 477 ненульових інтервалів коефіцієнт кореляції Пірсона склав:

– $r = -0.2684$

– p-значення: $2.5880 \cdot 10^{-9}$

Негативне значення коефіцієнта r підтверджує наявність зворотного зв'язку: збільшення комісії пов'язане зі зменшенням часу обробки. Отримане значення $r = -0.2684$ за шкалою інтерпретації кореляції Пірсона вказує на слабкий до помірного зв'язок між змінними. Для контексту, коефіцієнт кореляції Пірсона інтерпретується наступним чином:

– $|r| < 0.1$ — дуже слабкий зв'язок

– $0.1 \leqslant |r| < 0.3$ — слабкий зв'язок

– $0.3 \leqslant |r| < 0.5$ — помірний зв'язок

– $0.5 \leqslant |r| < 0.7$ — сильний зв'язок

– $|r| \geqslant 0.7$ — дуже сильний зв'язок

Таким чином, отримане значення $r = -0.2684$ знаходиться на межі між слабким та помірним зв'язком. Однак надзвичайно низьке p-значення ($2.5880 \cdot 10^{-9} \ll 0.001$) свідчить про високу статистичну значущість цього зв'язку. Це означає, що, хоча зв'язок не є сильним у лінійному сенсі, він є дуже стабільним і вкрай малоймовірно, що він спостерігається випадково.

Важливо зазначити, що коефіцієнт кореляції Пірсона має обмеження для інтерпретації нелінійних залежностей. Якщо змінні пов'язані через нелінійну функцію (як у нашому випадку), коефіцієнт Пірсона може недооцінювати справжню силу зв'язку. Тому доцільно розглянути інші міри залежності.

3.3.2 Коефіцієнт кореляції Спірмена

Коефіцієнт рангової кореляції Спірмена є непараметричною мірою, яка оцінює, наскільки добре взаємозв'язок між двома змінними може бути

описаний монотонною функцією. Він розраховується за формулою:

$$\rho = 1 - \frac{6 \sum_{i=1}^{n} d_i^2}{n(n^2 - 1)} \tag{3.30}$$

де d_i — різниця між рангами значень комісії та часу обробки, n — кількість спостережень.

На відміну від коефіцієнта Пірсона, коефіцієнт Спірмена не вимагає лінійності зв'язку і є стійким до викидів. Для нашої вибірки коефіцієнт кореляції Спірмена склав:

– $\rho = -0.4733$

– p-значення: $5.3224 \cdot 10^{-28}$

Отримане значення $\rho = -0.4733$ вказує на помірний до сильного монотонний зв'язок між комісією та часом обробки. Цей результат є значно сильнішим, ніж коефіцієнт Пірсона, що вказує на те, що зв'язок між змінними має виражений монотонний, але нелінійний характер.

3.3.3 Коефіцієнт кореляції Кендалла

Ще одним важливим непараметричним показником зв'язку є коефіцієнт кореляції Кендалла, який вимірює порядкову асоціацію між двома вимірюваними величинами. Він розраховується на основі кількості узгоджених та неузгоджених пар спостережень:

$$\tau = \frac{n_c - n_d}{\frac{1}{2} n(n-1)} \tag{3.31}$$

де n_c – кількість узгоджених пар, n_d — кількість неузгоджених пар, n – загальна кількість спостережень.

Для вибірки коефіцієнт тау Кендалла склав:

– $\tau = -0.3408$

– p-значення: $1.0812 \cdot 10^{-28}$

Значення $\tau = -0.3408$ також підтверджує наявність помірного зворотного зв'язку між змінними. Коефіцієнт Кендалла часто має менші

абсолютні значення, ніж коефіцієнт Спірмена, тому отримане значення свідчить про досить стійкий зв'язок.

3.3.4 Порівняння та інтерпретація різних коефіцієнтів кореляції

У таблиці 3.3 наведено порівняння всіх розрахованих коефіцієнтів кореляції.

Таблиця 3.3 – Порівняння різних коефіцієнтів кореляції

Тип коефіцієнта	Значення	p-значення	Інтерпретація
Пірсона (r)	-0.2684	$2.5880 \cdot 10^{-9}$	Слабкий до помірного лінійний зв'язок
Спірмена (ρ)	-0.4733	$5.3224 \cdot 10^{-28}$	Помірний до сильного монотонний зв'язок
Кендалла (τ)	-0.3408	$1.0812 \cdot 10^{-28}$	Помірний монотонний зв'язок

Аналіз різних коефіцієнтів кореляції дозволяє зробити такі висновки:

1) Всі коефіцієнти кореляції мають від'ємне значення, що підтверджує зворотний характер зв'язку між розміром комісії та часом обробки транзакцій. Це повністю узгоджується з теоретичними очікуваннями: зі збільшенням комісії час обробки зменшується.

2) Коефіцієнт кореляції Пірсона для нетрансформованих даних показує найслабший зв'язок, що пояснюється нелінійним характером залежності, який цей коефіцієнт не може адекватно враховувати.

3) Коефіцієнти Спірмена і Кендалла, які вимірюють монотонність зв'язку без вимоги його лінійності, показують значно сильніший зв'язок. Це підтверджує, що зв'язок між комісією та часом обробки є суттєвим, але нелінійним.

4) Особливо показовим є коефіцієнт Спірмена $\rho = -0.4733$, який відображає помірний до сильного монотонний зв'язок і має надзвичайно низьке p-значення ($5.3224 \cdot 10^{-28}$), що свідчить про дуже високу статистичну значущість.

5) Усі коефіцієнти кореляції мають дуже низькі p-значення (порядку 10^{-9} для Пірсона та 10^{-28} для Спірмена і Кендалла), що свідчить про високу статистичну значущість виявлених залежностей і дуже малу ймовірність того, що спостережувані взаємозв'язки є результатом випадкових флуктуацій.

Можна помітити значну різницю між значеннями коефіцієнтів Пірсона і Спірмена (модуль Спірмена майже в 1.8 рази більший за модуль Пірсона). Це є додатковим підтвердженням нелінійного характеру залежності. Якщо б залежність була близькою до лінійної, ці коефіцієнти були б приблизно рівними.

Таким чином, проведений кореляційний аналіз підтверджує існування статистично значущого зворотного зв'язку між розміром комісії та часом обробки транзакцій у досліджуваній блокчейн-мережі. Цей зв'язок має виражений нелінійний характер і може бути найкраще описаний степеневою або експоненційною моделлю, які будуть розглянуті в наступному розділі.

Отримані результати кореляційного аналізу мають важливі наслідки для розуміння поведінки користувачів та майнерів у блокчейн-мережах. Значущий зворотний зв'язок між комісією та часом обробки підтверджує існування економічних стимулів, коли користувачі можуть «купувати» пріоритет своїх транзакцій, а майнери раціонально реагують на ці стимули, включаючи транзакції з вищими комісіями раніше.

У контексті атак випередження, розглянутих у розділі 3.1, емпірично підтверджений зв'язок між комісією та часом обробки означає, що можливості для зловмисника можуть бути ширшими, ніж у теоретичній моделі з однаковими комісіями. Зловмисник може не лише використовувати випадковість включення транзакцій з однаковими параметрами, але й маніпулювати пріоритизацією шляхом встановлення вищої комісії.

Для повного розуміння залежності між комісією та часом обробки

та кількісного прогнозування часу обробки для заданого розміру комісії необхідно побудувати регресійні моделі, які найкраще апроксимують спостережувані дані.

3.4 Побудова регресійних моделей

Для більш точного опису залежності між комісією та часом обробки транзакцій було побудовано кілька регресійних моделей. На основі результатів кореляційного аналізу, проведеного в попередньому розділі, та візуального аналізу даних було визначено, що залежність має нелінійний характер. Тому для апроксимації були обрані наступні функціональні форми:

1) Степенева модель: $T = a \cdot \phi^{-b} + c$

2) Експоненційна модель: $T = a \cdot e^{-b \cdot \phi} + c$

3) Гіперболічна модель: $T = \frac{a}{\phi} + b$

4) Логарифмічна модель: $T = a - b \cdot \ln(\phi)$

де T — час обробки транзакції, ϕ — розмір комісії, a, b, c — параметри моделі.

Для оцінки параметрів моделей було використано метод найменших квадратів. Цей метод мінімізує суму квадратів відхилень між спостережуваними значеннями та значеннями, передбаченими моделлю:

$$\min_{a,b,c} \sum_{i=1}^{n} (y_i - f(x_i; a, b, c))^2 \tag{3.32}$$

де y_i – спостережувані значення часу обробки, x_i — значення комісії, $f(x_i; a, b, c)$ — функція регресійної моделі з параметрами a, b, c.

Для оцінки якості апроксимації та порівняння різних моделей використовувалися наступні метрики:

1) Коефіцієнт детермінації R^2, який показує, яку частку дисперсії

залежної змінної можна пояснити моделлю:

$$R^2 = 1 - \frac{\sum_{i=1}^{n}(y_i - \hat{y}_i)^2}{\sum_{i=1}^{n}(y_i - \bar{y})^2} \tag{3.33}$$

де $\hat{y}_i$ – значення, передбачені моделлю, а $\bar{y}$ – середнє спостережуваних значень.

2) Середньоквадратична помилка (MSE), яка вимірює середній квадрат відхилень:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2 \tag{3.34}$$

3) Інформаційний критерій Акаіке (AIC), який враховує як якість підгонки, так і складність моделі:

$$AIC = 2k + n \cdot \ln\left(\frac{RSS}{n}\right) \tag{3.35}$$

де k – кількість параметрів моделі, RSS — сума квадратів залишків, n – розмір вибірки.

Результати оцінювання параметрів для кожної моделі та показники якості моделей наведено в таблиці 3.4 та на графіку 3.3.

Таблиця 3.4 – Порівняння регресійних моделей

Модель	Параметри	R^2	MSE	AIC
Степенева	$a = 3.25 \times 10^6$ $b = 1.94$ $c = 163.7$	0.685	2.48×10^6	1843.2
Експоненційна	$a = 9843.5$ $b = 0.0057$ $c = 175.3$	0.621	2.97×10^6	1872.8
Гіперболічна	$a = 4.81 \times 10^5$ $b = 192.6$	0.613	3.03×10^6	1876.2
Логарифмічна	$a = 15682.4$ $b = 2143.9$	0.637	2.85×10^6	1869.4

Аналіз результатів показує, що степенева модель демонструє

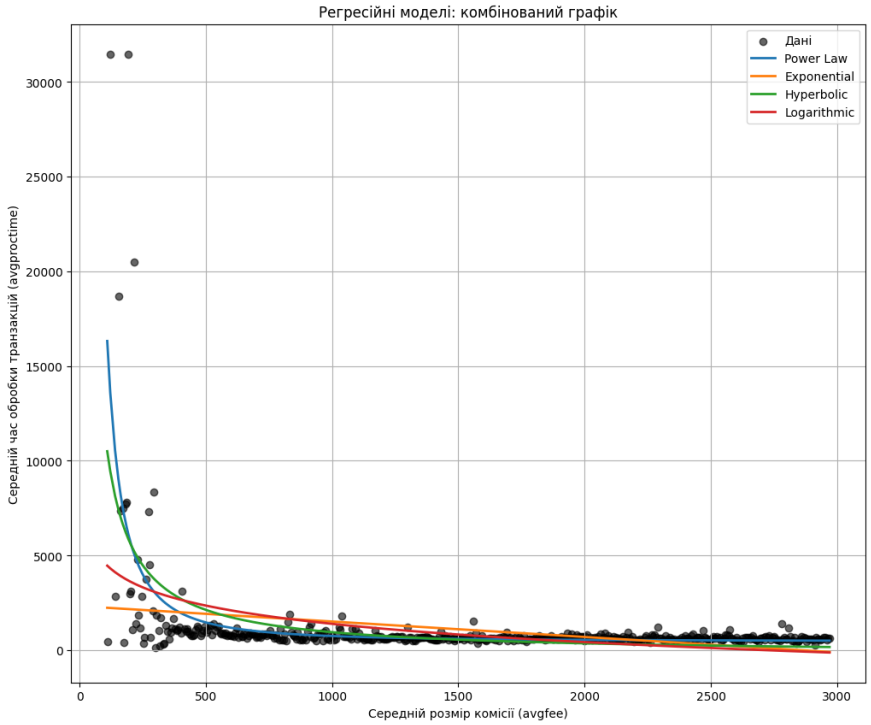

Рисунок 3.3 – Залежності часу обробки від комісії для кожної розглянутої моделі

найкращу якість апроксимації даних, маючи найвищий коефіцієнт детермінації ($R^2 = 0.685$), найнижчу середньоквадратичну помилку (MSE $= 2.48 \times 10^6$) та найнижче значення інформаційного критерію Акаіке (AIC $= 1843.2$).

Порівняння моделей демонструє, що:

1) Степенева модель пояснює близько 68.5% варіативності часу обробки, що є дуже хорошим показником для емпіричних даних з реальної блокчейн-мережі.

2) Експоненційна модель має дещо гіршу продуктивність ($R^2 = 0.621$), але все ж краще описує дані, ніж гіперболічна модель.

3) Логарифмічна модель знаходиться між експоненційною та гіперболічною за якістю апроксимації ($R^2 = 0.637$).

4) Гіперболічна модель, попри свою простоту (лише два параметри), має найнижчу продуктивність серед усіх розглянутих моделей ($R^2 = 0.613$).

Виходячи з результатів порівняння, для подальшого аналізу та прогнозування часу обробки транзакцій буде використовуватися степенева модель:

$$T(\phi) = 3.25 \times 10^6 \cdot \phi^{-1.94} + 163.7 \tag{3.36}$$

Ця модель добре узгоджується з теоретичними очікуваннями щодо характеру залежності у PoW-блокчейнах. Параметр $b = 1.94$ вказує на нелінійний характер спадання часу обробки при збільшенні комісії, а параметр $c = 163.7$ відображає існування мінімального порогового часу обробки, нижче якого неможливо опуститися навіть при дуже високих комісіях.

Інтерпретація параметрів степеневої моделі має важливе практичне значення:

1) Параметр $a = 3.25 \times 10^6$ є масштабним коефіцієнтом, який визначає загальний рівень залежності. Його високе значення вказує на сильну початкову залежність часу обробки від комісії при малих значеннях комісії.

2) Параметр $b = 1.94$ визначає швидкість зменшення часу обробки при збільшенні комісії. Значення близьке до 2 означає, що подвоєння комісії призводить до зменшення компоненти часу обробки, залежної від комісії, приблизно в 4 рази ($2^{1.94} \approx 3.84$). Це показує дуже сильну нелінійність залежності.

3) Параметр $c = 163.7$ представляє асимптотичний мінімальний час обробки, який визначається технічними характеристиками мережі (зокрема, середнім часом створення блоку). Незалежно від розміру комісії, час обробки не може бути меншим за цю величину.

Графічно залежність, описана степеневою моделлю, представлена на рисунку 3.4, де точками показано емпіричні дані, а суцільною лінією — апроксимацію степеневою моделлю.

Отримана степенева модель дозволяє не лише описати

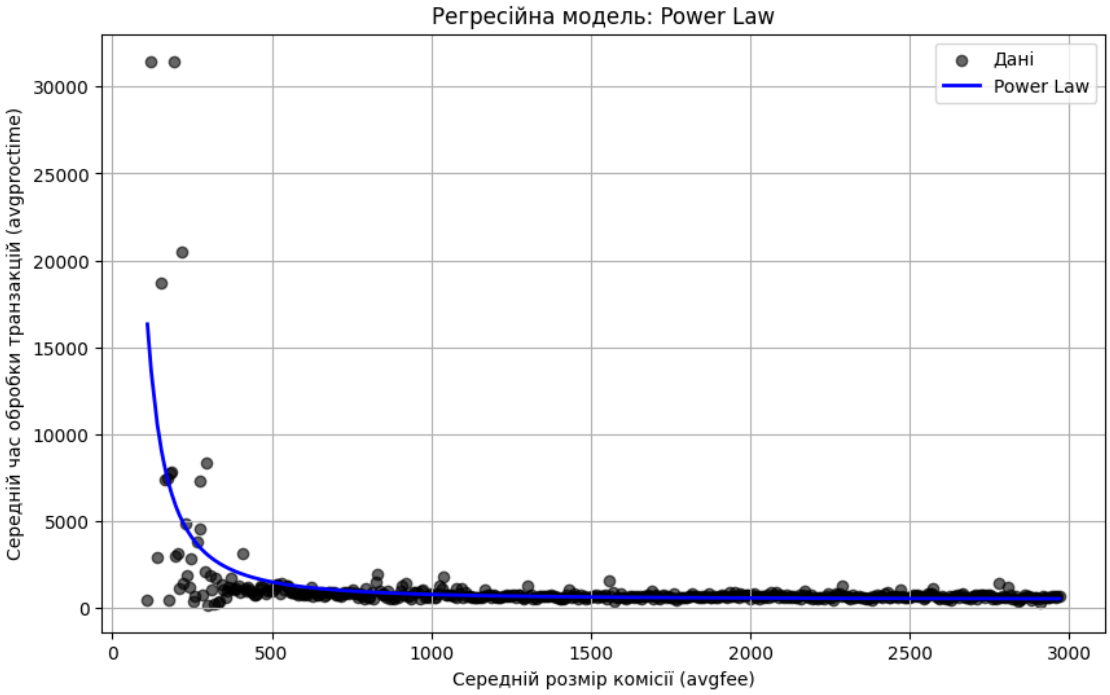

Рисунок 3.4 – Апроксимація залежності часу обробки від комісії степеневою моделлю

спостережувану залежність, але й зробити практичні висновки щодо оптимального вибору розміру комісії.

Для практичного використання отриманої моделі можна обчислити очікуваний час обробки для різних значень комісії, що допоможе користувачам блокчейн-мережі приймати обґрунтовані рішення щодо вибору оптимального розміру комісії залежно від своїх вимог до швидкості обробки транзакції.

3.5 Алгоритм вибору оптимальної стратегії захисту від атак випередження

На основі проведеного теоретичного та емпіричного дослідження запропоновано диференційований підхід до захисту від атак випередження. Ключова особливість цього підходу полягає в тому, що він не надає універсального алгоритму захисту, а дозволяє визначити рівень

ризику для конкретного блокчейну та конкретної ситуації, даючи користувачу можливість самостійно прийняти рішення щодо прийнятності виявлених ризиків.

Далі описано покроковий алгоритм дій для аналізу вразливості до атак випередження та прийняття рішення щодо транзакцій:

Крок 1: Визначення наявності та характеру залежності між комісією та часом обробки

Для цього необхідно:

1) Зібрати репрезентативну вибірку транзакцій з досліджуваної блокчейн-мережі.

2) Провести попередню обробку та фільтрацію даних.

3) Обчислити коефіцієнти кореляції за емпіричними даними (r, ρ, τ).

4) Оцінити силу виявленої залежності, використовуючи насамперед коефіцієнт Спірмена (ρ) як найбільш придатний для нелінійних залежностей.

Крок 2: Вибір відповідної математичної моделі

Залежно від результатів Кроку 1:

1) Якщо виявлена статистично значуща залежність (модуль коефіцієнта Спірмена $|\rho| > 0.3$):

а) Визначити функціональну форму залежності (степенева, експоненційна, гіперболічна або логарифмічна).

б) Оцінити параметри моделі за допомогою регресійного аналізу.

в) Застосувати класичні формули для оцінки ймовірності успіху атаки випередження [1]:

$$P_{success} = \frac{\lambda(\phi_a)}{\lambda(\phi_a) + \lambda(\phi_v)},$$

де параметр λ залежить від розміру комісії за степеневим законом $\lambda(\phi) \propto \phi^b$, а b визначається з емпіричних даних.

2) Якщо залежність слабка або відсутня ($|\rho| < 0.3$):

а) Оцінити поточне співвідношення кількості транзакцій у

мемпулі (M) до розміру блоку (N).

б) Застосувати розроблену в даній роботі модель для випадку випадкового включення транзакцій:

i. Для $M \leqslant N$:

$$P_{success} = \frac{1}{2}$$

ii. Для $M > N$:

$$P_{success} = \frac{N(2M - N - 1)}{2M(M - 1)}$$

Крок 3: Прийняття рішення користувачем

На основі обчисленої ймовірності успіху атаки випередження:

1) Користувач оцінює критичність своєї транзакції та потенційні втрати від успішної атаки.

2) Визначає прийнятний для себе рівень ризику.

3) Приймає одне з рішень:

а) Якщо обчислена ймовірність успіху атаки перевищує прийнятний рівень ризику:

i. У випадку наявності залежності $T(\phi)$ — збільшити комісію для зниження ймовірності успіху атаки.

ii. У випадку відсутності залежності — відкласти транзакцію до періоду з більш сприятливим співвідношенням M/N або застосувати додаткові захисні механізми.

б) Якщо обчислена ймовірність успіху атаки нижче прийнятного рівня ризику — виконати транзакцію з початковими параметрами.

Запропонований підхід відрізняється від універсальних алгоритмів захисту тим, що визнає різноманітність блокчейн-мереж та їх специфічні характеристики. Замість надання фіксованих рекомендацій, він дозволяє кількісно оцінити ризики атак випередження в конкретній ситуації та прийняти обґрунтоване рішення з урахуванням особливостей кожної блокчейн-мережі.

Важливо зазначити, що характер залежності часу обробки від

комісії може змінюватися з часом, особливо при змінах протоколу консенсусу або значних коливаннях активності користувачів. Тому регулярна переоцінка параметрів моделі є необхідною умовою для підтримання ефективності аналізу ризиків.

Висновки до розділу 3

У цьому розділі було проведено дослідження ймовірнісних моделей атак випередження та емпіричний аналіз залежності часу обробки транзакцій від розміру комісії.

На основі теоретичного аналізу було досліджено теоретичні моделі атак випередження при випадковому порядку включення транзакцій та проведено емпіричний аналіз залежності часу обробки від розміру комісії.

Розроблено математичні моделі для оцінки ймовірності успіху атаки випередження для двох сценаріїв: при повному включенні транзакцій з мемпулу в блок ($M \leqslant N$) та при обмеженому розмірі блоку ($M > N$). Встановлено, що ймовірність успіху атаки зменшується зі зростанням співвідношення M/N, що створює природний захисний механізм проти атак випередження в періоди високого навантаження на мережу.

Проведений аналіз показав, що для різних мереж вплив комісії на час обробки транзакції може бути різним, від суттєвого до нехтувано малого. Причому навіть суттєва залежність може визначатись різними функціями для різних блокчейнів. Тому перед аналізом ризиків, пов'язаних з атаками випередження, необхідно спочатку проаналізувати характер цієї залежності з використанням статистичних інструментів.

Для блокчейн-мережі Bitcoin усі типи кореляційних коефіцієнтів показали наявність статистично значущого зворотного зв'язку між розміром комісії та часом обробки транзакцій: коефіцієнт Пірсона ($r = -0.2684$, p-значення $= 2.5880 \cdot 10^{-9}$), коефіцієнт Спірмена ($\rho = -0.4733$, p-значення $= 5.3224 \cdot 10^{-28}$) та коефіцієнт Кендалла ($\tau = -0.3408$, p-значення $= 1.0812 \cdot 10^{-28}$). Виходячи з отриманих значень

коефіцієнтів, ця залежність описується спадною нелінійною функцією.

Серед розглянутих регресійних моделей степенева модель показала найкращі результати з коефіцієнтом детермінації $R^2 = 0.685$, що дозволило формалізувати залежність у вигляді $T(\phi) = 3.25 \times 10^6 \cdot \phi^{-1.94} + 163.7$. Параметр $b = 1.94$ вказує на сильну нелінійність залежності, а параметр $c = 163.7$ відображає мінімальний поріг часу обробки, нижче якого неможливо опуститися навіть при дуже високих комісіях.

На основі отриманих результатів розроблено методику аналізу вразливості до атак випередження, яка передбачає: визначення наявності та характеру залежності між комісією та часом обробки для конкретного блокчейну, застосування відповідних математичних моделей залежно від результатів аналізу, та обчислення ймовірності успіху атаки з урахуванням поточного стану мемпулу. Ця методика дозволяє користувачам блокчейн-мереж оцінювати ризики та приймати обґрунтовані рішення щодо параметрів своїх транзакцій.

ВИСНОВКИ

Дана робота була присвячена дослідженню залежності часу обробки транзакцій від розміру комісії в блокчейн-мережах та впливу цієї залежності на вразливість до атак випередження. З огляду на стрімкий розвиток блокчейн-технологій та зростаючу кількість атак на користувачів цих мереж, ця тема є надзвичайно актуальною.

В ході роботи було проведено аналіз теоретичних основ блокчейну, особливостей різних протоколів консенсусу та їх впливу на процес обробки транзакцій. Зокрема, було встановлено, що різні протоколи консенсусу – Proof of Work, Proof of Stake та протоколи з секвенсорами – мають фундаментальні відмінності у механізмах пріоритизації транзакцій, які впливають на характер залежності між комісією та часом обробки.

Була розроблена методологія дослідження цієї залежності, яка включила методи збору даних, їх попередньої обробки та фільтрації, а також статистичного аналізу. Це дозволило провести емпіричне дослідження для блокчейну Bitcoin та отримати результати, які можуть бути корисними для подальших досліджень інших блокчейн-мереж.

Одним з ключових теоретичних досягнень роботи стала розробка і математичне обґрунтування моделей для оцінки ймовірності успіху атаки випередження в умовах випадкового порядку включення транзакцій. Доведено, що для випадку, коли всі транзакції з мемпулу включаються до блоку, ймовірність успіху атаки становить точно 0.5. Цей результат є логічним, оскільки за відсутності детермінованої пріоритизації транзакцій шанси зловмисника та чесного користувача однакові.

Більш цікавим виявився випадок, коли кількість транзакцій у мемпулі перевищує розмір блоку. Тут ймовірність успіху атаки залежить від співвідношення M/N і зменшується з його зростанням. Наприклад, при потрійному перевищенні розміру мемпулу над розміром блоку

ймовірність успіху атаки знижується до приблизно 28%. Це означає, що висока завантаженість мережі створює своєрідний природний захисний механізм проти атак випередження, але не усуває ризик повністю.

Проведений аналіз показав, що для різних мереж вплив комісії на час обробки транзакції може бути різним, від суттєвого до нехтувано малого. Причому навіть суттєва залежність може визначатись різними функціями для різних блокчейнів. Тому перед аналізом ризиків, пов'язаних з атаками випередження, необхідно спочатку проаналізувати характер цієї залежності з використанням статистичних інструментів.

Емпіричне дослідження блокчейн-мережі Bitcoin показало наявність статистично значущого зворотного зв'язку між розміром комісії та часом обробки транзакцій. Усі типи кореляційних коефіцієнтів (Пірсона, Спірмена та Кендалла) підтвердили це, причому ранговий коефіцієнт Спірмена виявився значно вищим за модулем порівняно з лінійним коефіцієнтом Пірсона, що однозначно вказує на нелінійний характер залежності.

Для кількісного опису цієї залежності було побудовано та порівняно чотири різні регресійні моделі. Найкращою виявилася степенева модель, яка пояснює значну частину варіативності часу обробки транзакцій. Отриманий показник степеня вказує на дуже сильну нелінійність залежності. Це означає, що при збільшенні комісії вдвічі час обробки зменшується в кілька разів. Дана інформація є важливою для користувачів блокчейну, що бажають оптимізувати свої витрати на комісію.

Узагальнюючи теоретичні та практичні результати дослідження, було запропоновано структурований підхід до оцінювання вразливості блокчейн-систем до атак випередження. Запропонована методика складається з трьох послідовних етапів: спершу проводиться комплексний статистичний аналіз для встановлення присутності та сили кореляції між транзакційними комісіями та часом підтвердження; далі, залежно від виявленого характеру взаємозв'язку, застосовуються або математичні

формули з попередніх досліджень (за наявності статистично значущої залежності), або розроблені в даній роботі теоретичні моделі для випадків з випадковим порядком включення транзакцій; розраховується числова ймовірність успішної атаки, що дозволяє користувачу прийняти рішення щодо оптимальних параметрів своїх операцій у мережі.

Якщо залежність сильна (модуль коефіцієнта Спірмена більше 0.3), доцільно застосовувати формули, які враховують цю залежність. У цьому випадку користувач може розглянути можливість встановлення комісії вище середнього рівня для захисту критично важливих транзакцій. Якщо ж залежність слабка або відсутня, варто орієнтуватися на розроблені моделі для випадкового порядку включення транзакцій та оцінювати ризики, виходячи з поточного стану мемпулу. На основі обчисленої ймовірності успіху атаки користувач самостійно приймає рішення щодо прийнятності виявлених ризиків.

Важливо відзначити, що отримані результати мають не лише теоретичне, але й практичне значення. Розроблена методика аналізу вразливості може бути використана користувачами блокчейн-мереж для прийняття обґрунтованих рішень щодо параметрів своїх транзакцій. Розробники смарт-контрактів можуть застосовувати ці знання для впровадження захисних механізмів, таких як часові замки, пороги обмеження ковзання ціни та техніки відкладеного розкриття параметрів транзакції.

Також результати дослідження можуть бути корисними для розробників блокчейн-протоколів. Знання про характер залежності часу обробки від комісії та її вплив на безпеку можуть допомогти у вдосконаленні механізмів включення транзакцій у блоки, зменшенні прозорості мемпулу або впровадженні детермінованих алгоритмів вибору транзакцій.

Як і будь-яке дослідження, дана робота має певні обмеження. Емпіричний аналіз було проведено лише для однієї блокчейн-мережі — Bitcoin, яка використовує протокол консенсусу Proof of Work. В

майбутньому було б доречно розширити аналіз на інші типи блокчейн-систем, особливо з протоколами Proof of Stake та з секвенсорами, які теоретично мають демонструвати інший характер залежності.

Також у подальших дослідженнях варто було б розглянути більше факторів, які можуть впливати на час обробки транзакцій, таких як загальне навантаження на мережу, розподіл обчислювальної потужності між майнерами та стратегії вибору транзакцій. Це дозволило б побудувати більш точні моделі та розробити більш ефективні стратегії захисту.

Ще одним напрямком для майбутніх досліджень також могло б стати експериментальне порівняння ефективності різних захисних механізмів проти атак випередження. Це дозволило б не лише теоретично, але й практично оцінити, які саме підходи є найбільш дієвими в різних умовах.

Нарешті, важливим аспектом, який заслуговує на окреме дослідження, є економічні аспекти атак випередження. Зокрема, було б корисно оцінити потенційні прибутки та витрати зловмисників, а також розробити такі механізми стимулювання, які б зменшували привабливість цих атак.

Підсумовуючи, проведене дослідження дозволило детальніше зрозуміти взаємозв'язок між комісією за транзакцію та часом її обробки, а також вплив цього взаємозв'язку на безпеку блокчейн-систем. Отримані результати та розроблені моделі можуть стати основою для подальшого вдосконалення блокчейн-протоколів та підвищення їх захищеності від атак випередження.

ПЕРЕЛІК ПОСИЛАНЬ

[1] Kovalchuk, L.V., Vykhlo, A.A. *Estimation of the Probability of Success of a Frontrunning Attack on Smart Contracts.* Англ. 2025. URL: https://doi.org/10.1007/s10559-024-00725-z.

[2] Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System.* Англ. 2008. URL: https://bitcoin.org/bitcoin.pdf.

[3] Lamport, L., Shostak, R., and Pease, M. *The Byzantine Generals Problem.* Англ. 1982. URL: https://doi.org/10.1145/357172.357176.

[4] Merkle, R. C. *A Digital Signature Based on a Conventional Encryption Function.* Англ. 1987. URL: https://link.springer.com/chapter/10.1007/3-540-48184-2_32.

[5] National Institute of Standards and Technology (NIST). *FIPS PUB 180-4: Secure Hash Standard (SHS).* Англ. 2015. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.

[6] Szabo, N. *Formalizing and Securing Relationships on Public Networks.* Англ. 1997. URL: https://firstmonday.org/ojs/index.php/fm/article/view/548.

[7] Buterin, V. *A Next-Generation Smart Contract and Decentralized Application Platform.* Англ. 2014. URL: https://ethereum.org/en/whitepaper/.

[8] Daian, P. and others. *Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges.* Англ. 2019. URL: https://doi.org/10.1145/3319535.3363197.

[9] Gilbert, S. and Lynch, N. *Brewer's Conjecture and the Feasibility of Consistent, Available, Partition-Tolerant Web Services.* Англ. 2002. URL: https://doi.org/10.1145/564585.564601.

[10] Gervais, A. and others. *On the Security and Performance of Proof of Work Blockchains.* Англ. 2016. URL: https://doi.org/10.1145/2976749.2978341.

[11] Li, Q., Ma, J. Y., and Chang, Y. X. *Blockchain queueing theory.* Англ. 2018. URL: https://arxiv.org/abs/1808.01795.

[12] Eskandari, S., Moosavi, S., and Clark, J. *SoK: Transparent Dishonesty: Front-running Attacks on Blockchain.* Англ. 2020. URL: https://doi.org/10.1007/978-3-030-51280-4_10.

[13] Zhou, L., Qin, K., Torres, C. F., and others. *High-Frequency Trading on Decentralized Exchanges.* Англ. 2021. URL: https://doi.org/10.1109/SP40001.2021.00030.

[14] Daian, P., Goldfeder, S., Kell, T., and others. *Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges.* Англ. 2020. URL: https://doi.org/10.1109/SP40000.2020.00040.

[15] Werner, S. M., Perez, D., Gudgeon, L., and others. *SoK: Decentralized Finance (DeFi) Attacks*. Англ. 2023. URL: https://doi.org/10.1145/3576915.3623098.