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

«На правах рукопису»
УДК 004.056.53:004.7:519.2

«До захисту допущено»
Завідувач кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2026 р.

Дипломна робота

на здобуття ступеня бакалавра
за освітньо-професійною програмою
«Математичні методи криптографічного захисту інформації»

зі спеціальності: 113 Прикладна математика
на тему: **«Оцінка ймовірності атаки егоїстичного майнінгу на блокчейн»**

Виконав:
студент IV курсу, групи ФІ-23
Задорожна Катерина Ігорівна _____

Керівник:
професор кафедри ММЗІ, доктор наук, професор
Ковальчук Людмила Василівна _____

Рецензент:
доцент кафедри ММАД, доктор філософії, доцент
Яйлимова Ганна Олексіївна _____

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

Київ — 2026

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

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

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2026 р.

ЗАВДАННЯ
на дипломну роботу

Студент: Задорожна Катерина Ігорівна

1. Тема роботи: «*Оцінка ймовірності атаки егоїстичного майнінгу на блокчейн*», науковий керівник дисертації: професор кафедри ММЗІ, доктор наук, професор Ковальчук Людмила Василівна,

затверджені наказом по університету №__ від «__» _____ 2026 р.

2. Термін подання студентом роботи: «__» _____ 2026 р.

3. Об'єкт дослідження: процес досягнення консенсусу та формування ланцюга блоків у децентралізованих мережах на базі алгоритму Proof-of-Work.

4. Предмет дослідження: стратегії атаки егоїстичного майнінгу з урахуванням часових затримок синхронізації мережі.

5. Перелік завдань:

1) Проведення огляду опублікованих джерел за тематикою дослідження.

2) Дослідження опублікованих статей, присвячених аналізу атаки егоїстичного майнінгу.

3) Математична формалізація процесу генерації блоків з урахуванням мережевих затримок і безперервного характеру часу.

4) Здійснення порівняльного аналізу стратегій зловмисника за умови знаходження ним одного блоку.

5) Дослідження доцільності атаки на прикладі числових параметрів, наближених до умов функціонування реальних мереж.

6) Виведення аналітичної формули для розрахунку загальної очікуваної фінансової вигоди зловмисника.

7) Проведення перевірки отриманої формули на основі параметрів, наближених до реальних.

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

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

8. Дата видачі завдання: 10 вересня 2025 р.

Календарний план

№ з/п	Назва етапів виконання бакалаврської дисертації	Термін виконання	Примітка
1	Узгодження теми роботи із науковим керівником	01-15 вересня 2025 р.	Виконано
2	Огляд опублікованих джерел за тематикою дослідження	Вересень-жовтень 2025 р.	Виконано
3	Аналіз атаки егоїстичного майнінгу та огляд наявних досліджень атаки	Листопад-грудень 2025 р.	Виконано
4	Математична формалізація процесу функціонування блокчейн-мережі в умовах безперервного часу	Січень-лютий 2026 р.	Виконано
5	Порівняльний аналіз стратегій зловмисника та визначення умов доцільності атаки	Березень-квітень 2026 р.	Виконано
6	Виведення аналітичної формули для розрахунку загальної очікуваної фінансової вигоди зловмисника	Квітень-травень 2026 р.	Виконано
7	Оформлення дипломної роботи	Травень-червень 2026 р.	Виконано

Студент _____ Катерина ЗАДОРОЖНА

Керівник _____ Людмила КОВАЛЬЧУК

РЕФЕРАТ

Кваліфікаційна робота містить: 60 стор., 21 рисунок, 2 таблиці, 8 джерел.

Метою дослідження є розробка узагальненого математичного методу для розрахунку очікуваної вигоди зловмисника та порівняльний аналіз прибутковості чесної і атакуючої стратегій з урахуванням мережевих затримок.

Об'єктом дослідження є процес досягнення консенсусу та формування ланцюга блоків у блокчейн-мережах на базі алгоритму Proof-of-Work.

Предметом дослідження є стратегії атаки егоїстичного майнінгу з урахуванням часових затримок мережевої синхронізації.

У ході роботи було отримано явні вирази для імовірностей успіху атак за різних стратегій, отримано явний вираз для функції прибутку з урахуванням можливого часу синхронізації мережі. Також для додаткового підтвердження адекватності отриманих аналітичних результатів отримано числові результати, обчислені з використанням отриманих аналітичних формул. Це дозволило довести, що наявність затримок експоненційно знижує необхідний поріг хешрейту пулу для успішної атаки.

БЛОКЧЕЙН, ПРОТОКОЛ КОНСЕНСУСУ, ЕГОЇСТИЧНИЙ МАЙНІНГ, МЕРЕЖЕВА ЗАТРИМКА

ABSTRACT

The qualification paper contains: 60 pages, 21 figures, 2 tables, 8 references.

The aim of the research is the development of a generalized mathematical method for calculating the expected payoff of an attacker and a comparative analysis of the profitability of honest and attacking strategies, taking into account network delays.

The object of the study is the process of achieving consensus and forming a chain of blocks in blockchain networks based on the Proof-of-Work algorithm.

The subject of the study is selfish mining attack strategies, taking into account the time delays of network synchronization.

During the work, explicit expressions for the probabilities of successful attacks under different strategies were obtained, and an explicit expression for the profit function was derived, taking into account the possible network synchronization time. Also, to further confirm the adequacy of the obtained analytical results, numerical results calculated using the derived analytical formulas were obtained. This allowed proving that the presence of delays exponentially reduces the necessary hashrate threshold of the pool for a successful attack.

BLOCKCHAIN, COMMITTED CONSENSUS PROTOCOL, SELFISH MINING, NETWORK DELAY

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

C_n^k — кількість всіх варіантів вибору k елементів з n без урахування їх порядку.

Cat_i — число Каталана з індексом i.

ВСТУП

Актуальність дослідження. Останнім часом технологія блокчейн надзвичайно швидко розвивається. Ця технологія є основою децентралізованих фінансів. Незважаючи на дуже високий рівень надійності, блокчейн-мережі мають вразливості. Однією з найнебезпечніших є атака егоїстичного майнінгу (Selfish Mining). Зловмисник має змогу несправедливо отримувати надто велику частку винагороди за рахунок прихованих знайдених блоків і публікації їх у зручний момент.

Незважаючи на рівень небезпеки цієї атаки, вона недостатньо досліджена. Більшість існуючих досліджень цієї атаки розглядають її лише в ідеальних умовах, у дискретному часі та ігнорують наявність затримок мережі. Таке спрощення призводить до хибного висновку, що поріг безпеки мережі становить 50% обчислювальної потужності. У реальних умовах наявність затримок суттєво впливає на конкурентну боротьбу майнерів. Тому дослідження даної атаки, враховуючи безперервний характер часу та мережеві затримки, є актуальним і необхідним завданням для точної оцінки вразливості сучасних блокчейн-систем.

Метою дослідження є розробка узагальненого математичного методу для розрахунку очікуваної вигоди зловмисника та порівняльний аналіз прибутковості чесної і атакуючої стратегій з урахуванням мережевих затримок.

Для досягнення мети необхідно розв'язати **задачу дослідження**, яка полягає у таких завданнях:

1) Провести огляд опублікованих джерел за тематикою дослідження.

2) Дослідити опубліковані статті, присвячені аналізу атаки егоїстичного майнінгу.

3) Здійснити математичну формалізацію процесу генерації блоків з

урахуванням мережевих затримок і безперервного характеру часу.

4) Здійснити порівняльний аналіз стратегій зловмисника за умови знаходження ним одного блоку.

5) Дослідити умови доцільності атаки на прикладі реальних числових параметрів мережі.

6) Вивести аналітичну формулу для розрахунку загальної очікуваної фінансової вигоди зловмисника.

7) Провести перевірку отриманої формули на основі реальних параметрів.

Об'єктом дослідження є процес досягнення консенсусу та формування ланцюга блоків у блокчейн-мережах на базі алгоритму Proof-of-Work.

Предметом дослідження є стратегії атаки егоїстичного майнінгу з урахуванням часових затримок синхронізації мережі.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: методи теорії ймовірностей, комбінаторного аналізу, зокрема числа Каталана та строга теорема Бертрана.

Наукова новизна отриманих результатів полягає у наступному:

– *Удосконалено* підхід до порівняльного аналізу стратегій зловмисника для атак із обмеженою глибиною у 2 блоки та визначення критеріїв їхньої фінансової вигідності.

– *Вперше запропоновано* узагальнену аналітичну формулу підрахунку фінансової вигоди для затяжних атак довільної глибини.

Практичне значення результатів полягає в тому, що отримана аналітична формула не має жорстких обмежень щодо довжини атаки та дозволяє з високою точністю прогнозувати фінансову доцільність дій зловмисника у реальних мережах. Застосування виведеної формули до параметрів мережі Bitcoin дозволяє кількісно оцінити фінансові ризики та визначити точний поріг хешрейту, за якого атака перетворюється на прибуткову. Результати роботи можуть бути використані для оптимізації алгоритмів синхронізації та підвищення загального рівня безпеки

блокчейн-мереж.

1 ТЕОРЕТИЧНІ ОСНОВИ ТЕХНОЛОГІЇ БЛОКЧЕЙН ТА АНАЛІЗ АТАКИ ЕГОЇСТИЧНОГО МАЙНІНГУ

У цьому розділі детально розглянуто технологію блокчейн та принципи роботи кожної її складової. Після цього проаналізовано атаку егоїстичного майнінгу та стратегію її реалізації.

1.1 Блокчейн

Уперше у 2009 році технологію блокчейн було запропоновано як технічну основу біткоїна, що зумовило її початкову орієнтацію на криптовалютні системи [8]. У 2013 році технологію блокчейн почали застосовувати і в інших сферах. Нині ця технологія досліджується у багатьох інноваційних галузях, таких як криптовалюти, смарт-контракти, комунікаційні системи, охорона здоров'я, Інтернет речей, фінансові системи, протидія цензурі, електронне голосування, розподілене походження даних тощо [3].

Означення 1.1. Блокчейн (або ланцюг блоків) — це розподілена база даних, пристрої зберігання якої не підключені до єдиного сервера. Він містить безперервно зростаючу впорядковану послідовність записів — так званих блоків, кожен з яких має часову мітку та посилання на попередній блок. Блокчейн є незмінним: після включення транзакції до блокчейну її неможливо модифікувати.

На сьогодні використовуються три основні класи блокчейнів: приватні, публічні та консорціумні [5].

Означення 1.2. Приватний блокчейн [5] — це блокчейн із жорстко контрольованим доступом, до якого жоден учасник або валідатор не може приєднатися без дозволу адміністратора. Такі блокчейни зазвичай

використовуються приватними компаніями у випадках, коли небажаним є публічний доступ до блоків, що містять конфіденційну інформацію.

Означення 1.3. Публічний блокчейн [5] — це блокчейн із відкритим доступом, до якого може приєднатися будь-який користувач, що має підключення до мережі Інтернет, із можливістю здійснення транзакцій та перевірки блоків.

Означення 1.4. Консорціумний блокчейн [5] — це напівдецентралізований блокчейн, у якому управління доступом і функціонуванням системи здійснюється спільно кількома організаціями, а не однією централізованою стороною.

1.2 Компоненти блокчейну

Технологія блокчейну може здаватися складною, однак її архітектуру можна спростити шляхом розгляду кожного компонента окремо. Цей підхід ґрунтовно описано у статті [6], яку використано за основу для написання цього підрозділу.

Тут розглядаються основні компоненти: криптографічні хеш-функції, транзакції, асиметрична криптографія, адреси, реєстри, блоки та спосіб, у який блоки з'єднуються між собою.

Розглянемо детальніше **криптографічні хеш-функції**.

Означення 1.5. Хешування — це метод застосування криптографічної хеш-функції, який обчислює відносно унікальний вихід для вхідних даних майже будь-якого розміру. Це дозволяє різним учасникам незалежно брати вхідні дані, обчислювати їхній хеш і отримувати однаковий результат, що доводить незмінність даних. Навіть найменша зміна у вхідних даних призведе до повністю іншого вихідного значення.

Криптографічні хеш-функції мають такі важливі властивості безпеки:

– **Стійкість до знаходження прообразу.** Це означає, що хеш-функція є односторонньою: обчислювально неможливо визначити вхідне значення за заданим вихідним значенням.

– **Стійкість до знаходження другого прообразу.** Це означає, що обчислювально неможливо знайти будь-яке інше значення, яке для заданого входу дає той самий хеш. Єдиним рішенням є лише повний перебір абсолютно всіх можливих вхідних значень, що є обчислювально нереалістичним.

– **Стійкість до колізій.** Це означає, що практично неможливо підібрати два різних вхідних значення, які дають однаковий результат хешування.

Однією з криптографічних хеш-функцій, що широко використовується у багатьох реалізаціях блокчейну, є алгоритм Secure Hash Algorithm із довжиною виходу 256 біт (SHA-256).

У блокчейн-мережах криптографічні хеш-функції використовуються для багатьох завдань: виведення адрес, створення унікальних ідентифікаторів, захисту даних блоку, захисту заголовка блоку.

Означення 1.6. Криптографічний nonce — це довільне число, яке використовується лише один раз.

Транзакції також є важливою складовою блокчейну.

Означення 1.7. Транзакція відображає взаємодію між сторонами. Наприклад, у випадку криптовалют транзакція становить передачу криптовалюти між користувачами блокчейн-мережі.

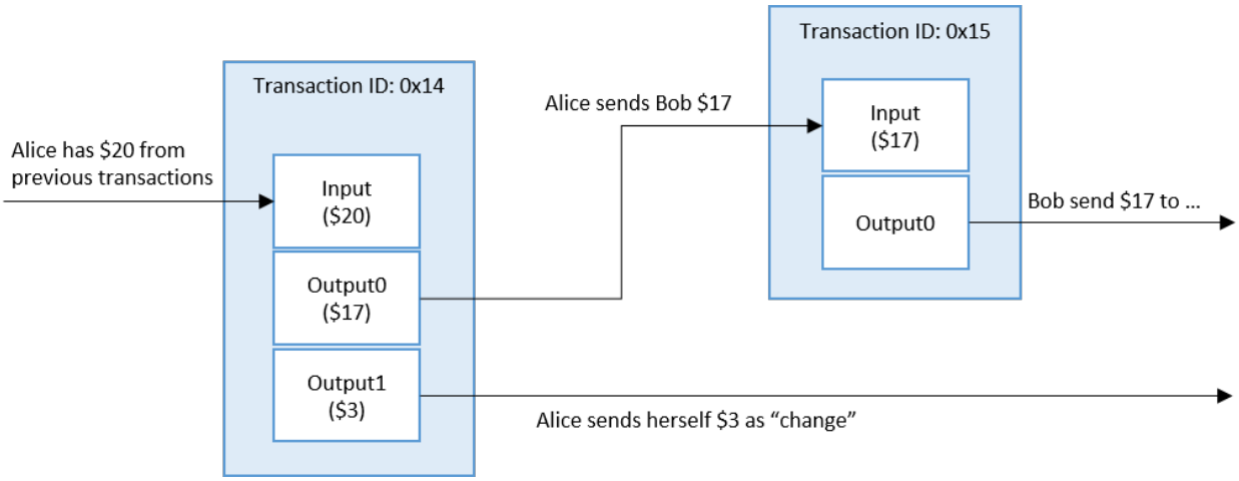

Рисунок 1.1 – Приклад транзакції з криптовалютою

Кожен блок у блокчейні може містити нуль або більше транзакцій.

Дані, з яких складається транзакція, можуть відрізнятися залежно від конкретної реалізації блокчейну, однак сам механізм здійснення транзакцій загалом залишається однаковим. Користувач надсилає інформацію до блокчейн-мережі. Надіслана інформація може включати адресу відправника (або інший релевантний ідентифікатор), відкритий ключ відправника, цифровий підпис, входи транзакції та виходи транзакції.

Одна транзакція з криптовалютою зазвичай вимагає щонайменше такої інформації, хоча може містити й більше:

– **Входи** — зазвичай являють собою список цифрових активів, які мають бути передані. Транзакція посилається на джерело цифрового активу, забезпечуючи його походження, тобто або на попередню транзакцію, у якій цей актив був переданий відправнику, або, у випадку створення нових цифрових активів, на подію їх виникнення. Оскільки вхід транзакції є посиланням на минулі події, самі цифрові активи не змінюються. У випадку криптовалют це означає, що вартість не може бути додана до наявних цифрових активів або вилучена з них. Натомість один цифровий актив може бути розділений на кілька нових активів із меншою вартістю, або кілька активів можуть бути об’єднані для

утворення меншої кількості нових активів із відповідно більшою вартістю. Поділ або об'єднання активів визначається у виходах транзакції.
Відправник також повинен надати доказ того, що він має доступ до зазначених входів, зазвичай шляхом цифрового підпису транзакції, тим самим доводячи володіння закритим ключем.

– **Виходи** — зазвичай являють собою облікові записи, які стають отримувачами цифрових активів, а також визначають кількість активів, що передаються. Кожен вихід містить інформацію про обсяг переданих цифрових активів, ідентифікатор нового власника (або власників), а також набір умов, які необхідно виконати для витрачання цих активів. Якщо наданих цифрових активів більше, ніж потрібно, надлишкові кошти мають бути явно повернуті відправникові, що реалізує механізм «видачі решти».

Тепер розглянемо **асиметричну криптографію**.

Технологія блокчейну використовує асиметричну криптографію, що оперує парою ключів: відкритим і закритим ключами, які математично пов'язані між собою. Відкритий ключ є публічно доступним без зниження безпеки процесу, але закритий ключ повинен залишатися таємним. Хоча між двома ключами існує зв'язок, закритий ключ не може бути ефективно визначений на основі знання відкритого ключа. Можна зашифрувати дані за допомогою закритого ключа, а потім розшифрувати їх відкритим ключем. Або ж навпаки: зашифрувати відкритим ключем, а розшифрувати закритим.

Асиметрична криптографія створює довірчий зв'язок між користувачами, які не знають один одного або не довіряють один одному, забезпечуючи механізм перевірки цілісності та автентичності транзакцій і водночас дозволяючи транзакціям залишатися публічними. Для цього транзакції мають цифровий підпис.

Деякі блокчейн-мережі використовують **адресу**, яка є коротким буквено-цифровим рядком символів, отриманим із відкритого ключа користувача за допомогою криптографічної хеш-функції разом із

деякими додатковими даними, наприклад номером версії та контрольними сумами. Більшість реалізацій блокчейну використовують адреси як кінцеві точки «кому» і «від кого» в транзакції. Адреси є коротшими за відкриті ключі і не є секретними.

Також важливо розглянути **зберігання закритого ключа**.

У деяких блокчейн-мережах, особливо в мережах без дозволів, користувачі повинні самостійно керувати своїми закритими ключами та безпечно їх зберігати.

Означення 1.8. Гаманець — це програмне забезпечення, яке забезпечує безпечне зберігання закритих і відкритих ключів та відповідних адрес, а також може виконувати додаткові функції, зокрема облік цифрових активів користувача.

Якщо користувач втрачає закритий ключ, то будь-який цифровий актив, пов'язаний із цим ключем, також втрачається, оскільки обчислювально неможливо відтворити той самий закритий ключ. Якщо закритий ключ викрадено, зловмисник отримає повний доступ до всіх цифрових активів, які контролюються цим закритим ключем.

Наступна важлива складова блокчейну — **реєстри**.

Означення 1.9. Реєстр — це сукупність транзакцій.

На сучасному етапі реєстри зберігаються в цифровій формі, часто у великих базах даних, які належать і керуються централізованою довіреною третьою стороною, тобто власником реєстру, від імені спільноти користувачів. Такі реєстри з централізованою власністю можуть бути реалізовані як у централізований, так і в розподілений спосіб, тобто або на одному сервері, або на координованому кластері серверів.

Розглянемо детальніше **блоки**.

Користувачі надсилають кандидатні транзакції до блокчейн-мережі за допомогою програмного забезпечення, такого як настільні застосунки, застосунки для смартфонів, цифрові гаманці, вебсервіси тощо. Програмне

забезпечення надсилає ці транзакції до одного або кількох вузлів у межах блокчейн-мережі. Обрані вузли можуть бути як повними вузлами, що не публікують блоки, так і вузлами, що публікують блоки. Подані транзакції потім поширюються до інших вузлів мережі, але саме по собі це ще не розміщує транзакцію в блокчейні. Для багатьох реалізацій блокчейну після того, як незавершена транзакція була розповсюджена між вузлами, вона повинна чекати в черзі, доки вузол, що публікує блоки, не додасть її до блокчейну.

Транзакції додаються до блокчейну, коли відповідний вузол публікує блок. Блок містить заголовок блоку та дані блоку. Заголовок блоку містить метадані цього блоку. Дані блоку містять список перевірених на дійсність та автентичність транзакцій, які були надіслані до блокчейн-мережі.

Дійсність і автентичність забезпечуються перевіркою того, що транзакція має правильний формат і що постачальники цифрових активів у кожній транзакції, перелічені у значеннях «входу» транзакції, кожен окремо криптографічно підписали транзакцію. Це підтверджує, що постачальники цифрових активів мали доступ до закритого ключа, яким можна було підписати передання наявних цифрових активів. Інші повні вузли перевірятимуть дійсність та автентичність усіх транзакцій в опублікованому блоці і не прийматимуть блок, якщо він містить недійсні транзакції.

Слід зазначити, що кожна реалізація блокчейну може визначати власні поля даних, однак багато систем використовують поля даних, подібні до таких:

– **Заголовок блоку**

  – номер блоку;

  – хеш-значення заголовка попереднього блоку;

  – хеш-представлення даних блоку, яке може формуватися різними способами, зокрема шляхом побудови дерева Меркла з подальшим збереженням кореневого хешу або шляхом обчислення хешу об'єднаних даних блоку;

– часова мітка;

– розмір блоку;

– значення nonce — для блокчейн-мереж, що використовують майнінг.

– **Дані блоку**

– список транзакцій та подій реєстру, включених до блоку;

– інші дані.

Технологія блокчейн використовує **ланцюгове з'єднання блоків**.

Блокчейн формується як безперервний ланцюг послідовно пов'язаних блоків. Надійна прив'язка кожного нового елемента до попереднього забезпечується тим, що в його заголовку жорстко зафіксовано хеш-значення попередника.

Будь-яка спроба модифікувати дані у вже записаному блоці неминуче змінить його власний хеш. Оскільки наступні блоки посилаються на нього, це спровокує лавиноподібну зміну всіх подальших хешів аж до кінця ланцюга. Завдяки цій властивості непомітно підмінити або видалити історію транзакцій неможливо — мережа миттєво розпізнає порушення криптографічних зв'язків і відхилить скомпрометовану версію.

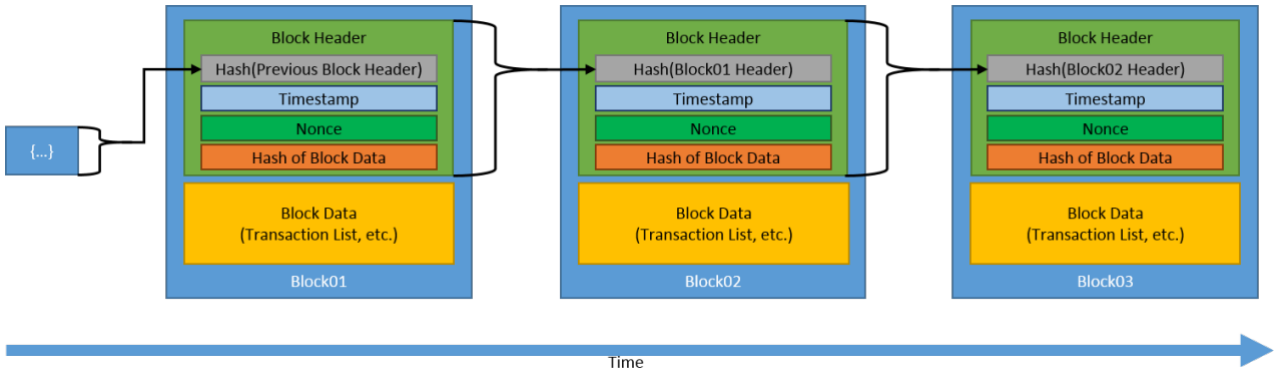

Рисунок 1.2 – Ланцюг блоків

1.3 Модель консенсусу

Ключовим аспектом технології блокчейну є визначення того, який вузол публікує наступний блок. Це завдання вирішується за допомогою моделей консенсусу, які дозволяють учасникам мережі, що не довіряють один одному, узгоджено формувати спільний стан системи.

У мережах без дозволів вузли змагаються за право додавання нового блоку, зазвичай з метою отримання винагороди у вигляді криптовалюти або комісій за транзакції. При цьому учасники мережі можуть бути взаємно недовірливими та ідентифікуватися лише за публічними адресами.

Початковий стан блокчейну визначається генезис-блоком — заздалегідь заданим першим блоком. Кожен наступний блок додається відповідно до обраної моделі консенсусу та повинен бути дійсним, що дозволяє будь-якому вузлу незалежно перевірити коректність блокчейну.

Основні властивості блокчейн-системи:

– початковий стан системи є узгодженим (генезис-блок);

– користувачі дотримуються спільної моделі консенсусу;

– кожен блок пов'язаний із попереднім через хеш-значення його заголовка (крім генезис-блоку);

– кожен блок може бути незалежно перевірений будь-яким вузлом мережі.

У разі виникнення кількох дійсних ланцюгів у більшості блокчейн-мереж застосовується правило вибору «довшого» ланцюга, тобто такого, у який вкладено найбільше обчислювальних ресурсів.

Важливою особливістю блокчейну є відсутність потреби в довіреній третій стороні, оскільки кожен учасник мережі може самостійно перевірити цілісність системи.

Модель консенсусу повинна забезпечувати узгодження стану системи навіть за наявності зловмисних учасників. У блокчейн-мережах із контрольованим доступом, де між учасниками існує певний рівень

довіри, можуть використовуватися менш ресурсоємні моделі консенсусу.

Далі розглянемо модель консенсусу Proof of Work.

Proof of Work передбачає, що вузол отримує право додати новий блок до блокчейну, якщо він першим знаходить розв'язок обчислювально складної задачі. Розв'язок цієї задачі є доказом виконаної роботи, причому сама задача є складною для розв'язання, але легкою для перевірки іншими вузлами мережі.

Зазвичай задача формулюється як необхідність знайти таке значення, при якому хеш-значення заголовка блоку є меншим за певне цільове значення. Для цього вузли багаторазово змінюють параметр nonce та обчислюють хеш заголовка блоку, доки не буде знайдено відповідне значення. Таким чином, процес пошуку розв'язку є обчислювально затратним і базується на переборі.

Складність задачі регулюється шляхом зміни цільового значення, що дозволяє підтримувати стабільну частоту створення блоків. Наприклад, у системі Bitcoin складність коригується таким чином, щоб новий блок створювався приблизно кожні десять хвилин.

Важливою властивістю моделі Proof of Work є незалежність спроб розв'язання задачі: попередні обчислення не впливають на ймовірність успіху в майбутньому. Це стимулює вузли припиняти поточні обчислення та починати роботу над новим блоком після отримання дійсного блоку від іншого вузла.

Після знаходження розв'язку вузол розповсюджує новий блок мережею, а інші вузли перевіряють його коректність шляхом одноразового обчислення хешу. У разі відповідності умовам задачі блок додається до блокчейну.

Модель Proof of Work вимагає значних обчислювальних ресурсів, що зумовлює високі енергетичні витрати. Водночас вона забезпечує стійкість мережі до атак.

Означення 1.10. Майнінг — це процес, у межах якого учасники блокчейн-мережі виконують обчислювально складні операції для

додавання нових блоків до блокчейну відповідно до моделі консенсусу Proof of Work [4, 7].

Означення 1.11. Майнер — це учасник мережі, що здійснює цей процес.

Процес майнінгу відбувається за допомогою багаторазового обчислення хеш-функції з різними вхідними значеннями. Обчислювальна потужність майнера напряму впливає на ймовірність знаходження коректного розв'язку, ці величини є пропорційними.

Якщо майнер успішно впорався із завданням і знайшов розв'язок, він публікує блок у мережу, після чого інші вузли визначають, чи є коректним цей блок. У випадку, коли блок виявляється дійсним, він додається до блокчейну, а майнер отримує винагороду у вигляді новостворених одиниць криптовалюти та комісій за транзакції.

Для підвищення ефективності вузли можуть об'єднуватися у майнінгові пули, розподіляючи обчислювальне навантаження та отриману винагороду між учасниками пулу.

1.4 Атака егоїстичного майнінгу (Selfish Mining)

У цьому підрозділі використано позначення та твердження з роботи [1], які необхідні у подальшому викладенні.

Система складається з множини майнерів $1, \ldots, n$, де кожен майнер i має обчислювальну потужність m_i, причому

$$\sum_{i=1}^{n} m_i = 1.$$

Майнери є раціональними та прагнуть максимізувати власний дохід, допускаючи відхилення від протоколу.

Майнери можуть об'єднуватися в пули, які діють як єдиний агент із сумарною обчислювальною потужністю. Дохід пулу визначається як

очікувана частка блоків, включених до найдовшого ланцюга.

Стратегія егоїстичного майнінгу дозволяє пулу отримувати дохід, що перевищує його частку обчислювальної потужності.

Розглядається модель із двома групами:

– егоїстичний пул (міноритарний);

– чесні майнери (більшість).

Ключова ідея стратегії полягає у змушенні чесних майнерів виконувати обчислення над застарілою гілкою блокчейну.

Це досягається шляхом приховування знайдених блоків і створення приватної гілки. Егоїстичний пул:

– не публікує знайдені блоки одразу;

– підтримує приватну гілку;

– розкриває блоки у стратегічні моменти.

У результаті чесні майнери продовжують майнити на коротшій публічній гілці, яка згодом відкидається, що призводить до марної витрати їхніх обчислювальних ресурсів.

Рішення пулу залежать від різниці довжин приватної та публічної гілок.

Розглянемо приклади сценаріїв із різними довжинами публічного та приватного ланцюгів.

Коли публічна гілка довша за приватну, егоїстичний пул відстає. Через різницю в обчислювальній потужності між егоїстичними майнерами та іншими, шанси егоїстичних майнерів наздогнати головний ланцюг, майнячи на власній приватній гілці, є дуже малими. Тому егоїстичний пул просто приймає основний ланцюг, коли його приватна гілка відстає. Коли інші знаходять нові блоки і публікують їх, пул оновлюється і майнить на поточній вершині публічного ланцюга.

Коли егоїстичний пул знаходить блок, він опиняється у вигідному положенні, маючи перевагу в один блок над публічною гілкою, на якій працюють чесні майнери. Замість того щоб одразу опублікувати цей блок і повідомити інших майнерів, егоїстичні майнери зберігають його в

таємниці. У цей момент можливі два варіанти: або чесні майнери знаходять новий блок і ліквідовують перевагу пулу, або пул знаходить другий блок і збільшує свою перевагу.

У першому сценарії, коли чесні майнери знаходять блок і нівелюють перевагу пулу, пул негайно публікує свою приватну гілку (довжини 1). Це створює ситуацію невизначеності, де може перемогти будь-яка гілка. Егоїстичні майнери одностайно переходять на свою гілку, а чесні майнери обирають, на якій гілці майнити, залежно від того, яку інформацію вони отримали швидше. Якщо пул встигає знайти наступний блок раніше за частину чесних майнерів, він одразу публікує його і отримує винагороду за обидва блоки. Якщо чесні майнери знаходять блок після опублікованого пулом блоку, пул отримує винагороду за свій блок, а чесні майнери — за свій. Якщо ж чесні майнери знаходять блок після свого ж блоку, вони отримують винагороду за два блоки, а пул — нічого.

У другому сценарії, коли пул знаходить другий блок, він отримує перевагу у два блоки. Після цього пул продовжує майнити на своїй приватній гілці і публікує по одному блоку щоразу, коли інші знаходять блок. Оскільки пул є меншістю, його перевага з часом зменшиться до одного блоку з великою ймовірністю. У цей момент чесні майнери вже дуже близько, тому пул публікує всю приватну гілку. Оскільки вона довша за публічну на один блок, усі майнери приймають її як основну, і пул отримує винагороду за всі свої блоки. Після цього система повертається до стану з одним ланцюгом, поки пул знову не створить розгалуження.

Тепер можна проаналізувати очікувані винагороди для системи, в якій егоїстичний пул має обчислювальну потужність α, а інші — $(1 - \alpha)$.

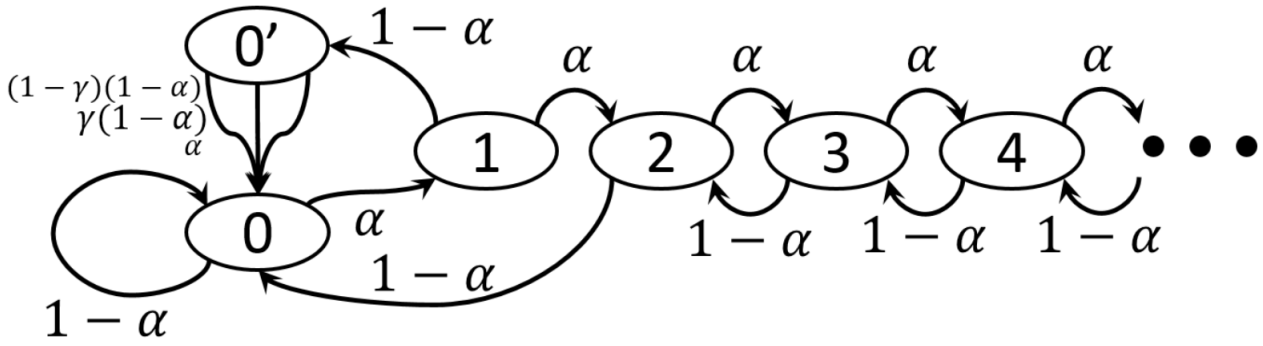

Рисунок 1.3 – Розвиток системи у вигляді автомата станів

Стани системи відображають перевагу йогоїстичного пулу — різницю між кількістю неопублікованих блоків у приватній гілці та довжиною публічної гілки. Нульова перевага поділяється на стани 0 і $0'$. Стан 0 — це стан, коли не існує розгалужень; тобто є лише один глобальний публічний найдовший ланцюг. Стан $0'$ — це стан, коли існують дві публічні гілки довжини один: основна гілка і гілка, яка раніше була приватною для егоїстичних майнерів і була опублікована, щоб зрівнятися з основною гілкою.

Переходи на малюнку відповідають подіям майнінгу, що здійснюються або егоїстичним пулом, або іншими учасниками, із середньою частотою α та $(1 - \alpha)$ відповідно.

Очікувані винагороди визначаються через частоти переходів між станами.

Очікувані винагороди від егоїстичного майнінгу визначаються через врахування частот, пов'язаних з кожним переходом стану автомата, та обчислення відповідних винагород. Розглянемо різні випадки та опишемо пов'язані з ними події, що викликають переходи станів.

Якщо пул має приватну гілку довжини 1 і інші майнери знаходять один блок, пул негайно публікує свою гілку, що призводить до появи двох публічних гілок довжини 1. Усі майнери егоїстичного пулу майнять на гілці пулу, оскільки знаходження наступного блоку на цій гілці принесе

винагороду пулу. Чесні майнери майнять на тій гілці, про яку вони дізналися першою. Через γ позначено частку чесних майнерів, які обирають майнити на блоці пулу, а решта $(1-\gamma)$ майнить на іншій гілці.

Для станів $s = 0, 1, 2, \ldots$ з частотою α пул знаходить блок, і перевага збільшується на одиницю до $s+1$. У станах $s = 3, 4, \ldots$ з частотою $(1-\alpha)$ чесні майнери знаходять блок, і перевага зменшується на одиницю до $s-1$.

Якщо інші майнери знаходять блок, коли перевага дорівнює двом, пул публікує свою приватну гілку, і система переходить у стан із нульовою перевагою. Якщо інші майнери знаходять блок, коли перевага дорівнює одному, система переходить у стан $0'$, описаний раніше.

Із стану $0'$ можливі три переходи, всі до стану 0 із сумарною частотою 1:

– пул знаходить блок на своїй раніше приватній гілці (частота α);

– інші майнери знаходять блок на раніше приватній гілці (частота $\gamma(1-\alpha)$);

– інші майнери знаходять блок на публічній гілці (частота $(1-\gamma)(1-\alpha)$).

Проаналізувавши цей автомат станів, можна обчислити розподіл ймовірностей по простору станів. Отримуємо такі рівняння:

$$\begin{cases} \alpha p_0 = (1-\alpha)p_1 + (1-\alpha)p_2, \\ p'_0 = (1-\alpha)p_1, \\ \alpha p_1 = (1-\alpha)p_2, \\ \forall k \geqslant 2: \ \alpha p_k = (1-\alpha)p_{k+1}, \\ \sum_{k=0}^{\infty} p_k + p'_0 = 1. \end{cases}$$

Розв'язуючи ці рівняння, отримуємо:

$$p_0 = \frac{\alpha - 2\alpha^2}{\alpha(2\alpha^3 - 4\alpha^2 + 1)},$$

$$p_0' = \frac{(1-\alpha)(\alpha - 2\alpha^2)}{1 - 4\alpha^2 + 2\alpha^3},$$

$$p_1 = \frac{\alpha - 2\alpha^2}{2\alpha^3 - 4\alpha^2 + 1},$$

$$\forall k \geqslant 2: \quad p_k = \left(\frac{\alpha}{1-\alpha}\right)^{k-1} \cdot \frac{\alpha - 2\alpha^2}{2\alpha^3 - 4\alpha^2 + 1}.$$

Розподіл ймовірностей по станах є основою для аналізу доходу егоїстичного пулу і чесних майнерів.

Винагорода за знайдений блок належить майнеру лише в тому випадку, якщо цей блок потрапляє до основного ланцюга. Нижче наведено опис винагород у кожному випадку.

(a) У будь-якому стані, окрім наявності двох гілок довжини 1, пул знаходить блок. Пул додає блок до своєї приватної гілки, збільшуючи перевагу на одиницю. Винагорода за цей блок визначиться пізніше.

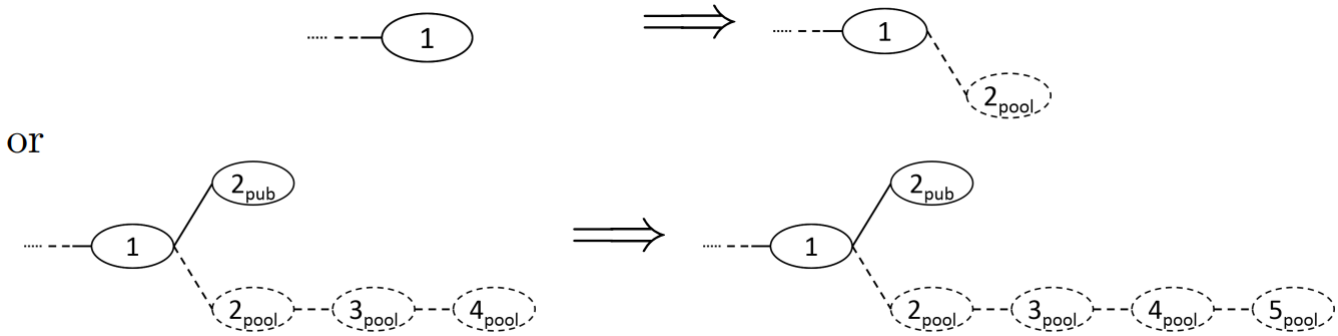

Рисунок 1.4

(b) Існували дві гілки довжини 1, пул знаходить блок. Пул публікує свою секретну гілку довжини 2 і отримує винагороду 2.

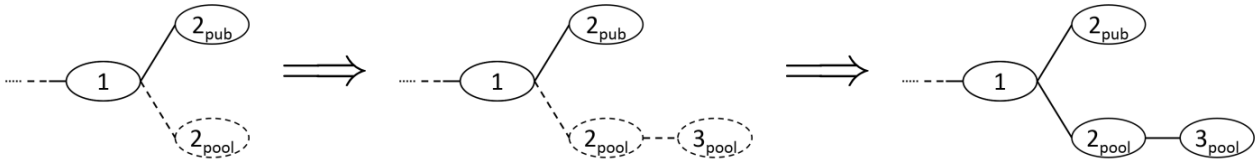

Рисунок 1.5

(c) Існували дві гілки довжини 1, інші знаходять блок після вершини пулу. Пул і інші отримують по 1: інші — за новий блок, пул — за попередній.

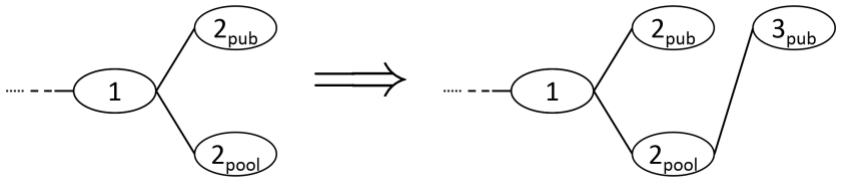

Рисунок 1.6

(d) Існували дві гілки довжини 1, інші знаходять блок після своєї гілки. Інші отримують винагороду 2.

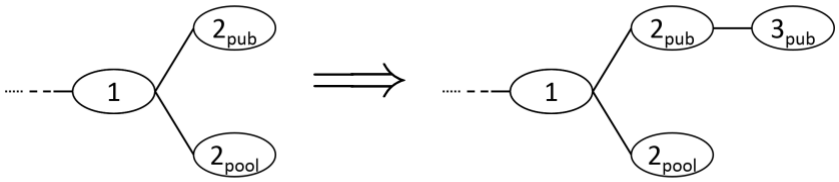

Рисунок 1.7

(e) Немає приватної гілки, інші знаходять блок. Інші отримують винагороду 1, і всі майнять на новій вершині.

(f) Перевага дорівнювала 1, інші знаходять блок. Тепер є дві гілки довжини 1, і пул публікує свій блок. Пул майнить на своїй гілці, інші розділяються. Через γ позначається частка інших майнерів, які обирають не пулову гілку. Винагорода ще не визначена, бо залежить від того, яка гілка переможе.

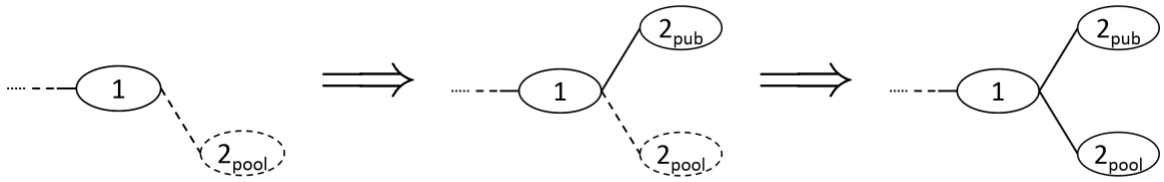

Рисунок 1.8

(g) Перевага була 2, інші знаходять блок. Перевага зменшується до 1. Пул публікує свою гілку, всі переходять на неї, і пул отримує винагороду 2.

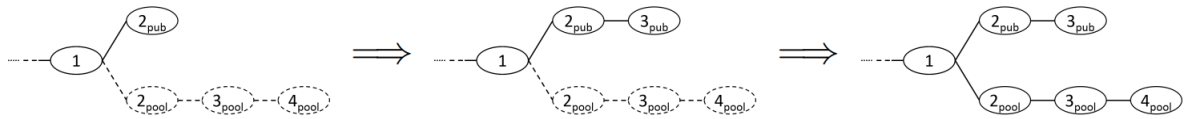

Рисунок 1.9

(h) Перевага була більше 2, інші виграють. Вони зменшують перевагу, але вона залишається $\geqslant 2$. Їхній блок не потрапить у ланцюг. Пул публікує свій блок і отримує 1.

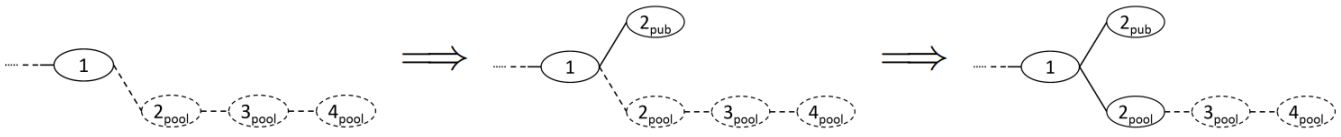

Рисунок 1.10

Тепер обчислюємо доходи:

$$r_{\text{others}} = p'_0 \cdot \gamma(1-\alpha) + p'_0 \cdot (1-\gamma)(1-\alpha) \cdot 2 + p_0 \cdot (1-\alpha),$$

$$r_{\text{pool}} = p'_0 \cdot \alpha \cdot 2 + p'_0 \cdot \gamma(1-\alpha) + p_2 \cdot (1-\alpha) \cdot 2 + P[i > 2](1-\alpha).$$

Навмисне розгалуження призводить до того, що чесні майнери працюють над блоками, які не потрапляють у блокчейн. Це зменшує ефективність, і:

$$r_{\text{pool}} + r_{\text{others}} < 1.$$

Протокол компенсує це, регулюючи складність так, щоб у середньому блок створювався кожні 10 хвилин.

Отже, реальний дохід — це відносна частка блоків у головному ланцюгу:

$$R_{\text{pool}} = \frac{r_{\text{pool}}}{r_{\text{pool}} + r_{\text{others}}} = \frac{\alpha(1-\alpha)^2\left(4\alpha + \gamma(1-2\alpha)\right) - \alpha^3}{1 - \alpha\left(1 + (2-\alpha)\alpha\right)}.$$

Для підтвердження теоретичного аналізу результати порівнюються з результатами симуляції протоколу Bitcoin. У симуляції використовується модель, що відображає основні властивості протоколу, при цьому процес знаходження блоків генерується методом Монте-Карло.

У експерименті розглядається система з 1000 майнерів з однаковою обчислювальною потужністю, де частка α формує егоїстичний пул, а решта дотримується стандартного протоколу. У випадку форку частка γ майнерів обирає гілку пулу.

Результати симуляції узгоджуються з теоретичним аналізом.

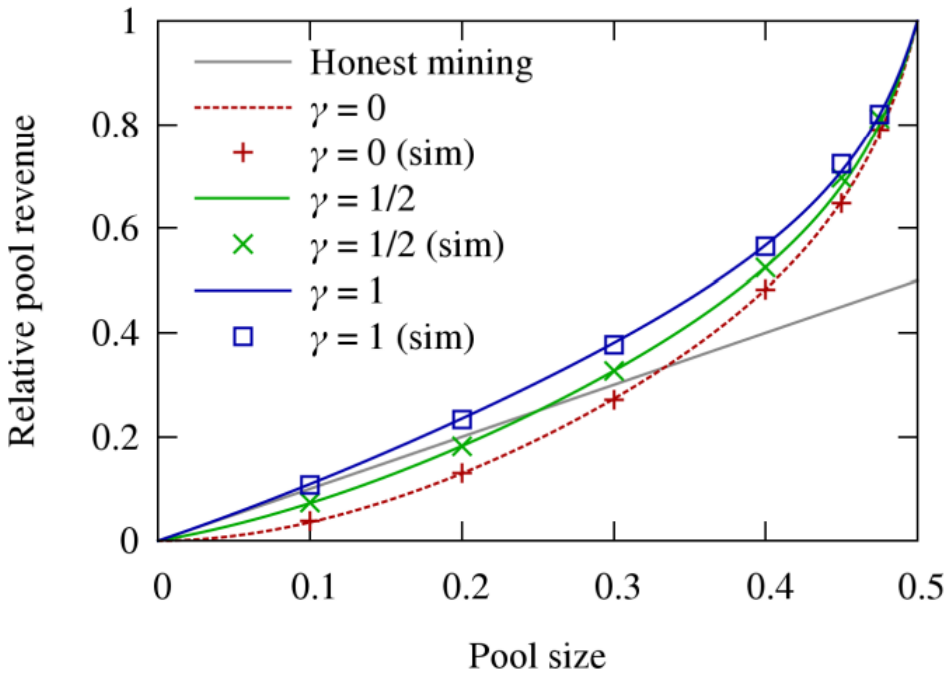

Рисунок 1.11

Коли дохід пулу, заданий у рівнянні

$$R_{\text{pool}} = \frac{r_{\text{pool}}}{r_{\text{pool}} + r_{\text{others}}} = \frac{\alpha(1-\alpha)^2\,(4\alpha + \gamma(1-2\alpha)) - \alpha^3}{1 - \alpha(1 + (2-\alpha)\alpha)},$$

перевищує α, пул отримує дохід, більший за той, що відповідає його частці обчислювальної потужності при використанні стратегії егоїстичного майнінгу. Таким чином, його учасники отримують більший дохід, ніж при чесному майнінгу. Цей вираз є справедливим лише для $0 \leqslant \alpha \leqslant \frac{1}{2}$.

Отримані вирази дозволяють не лише оцінити дохід егоїстичного пулу, але й визначити умови успішності атаки. Зокрема, параметри α та γ безпосередньо впливають на ймовірність того, що приватна гілка пулу випереджатиме публічну та буде прийнята мережею як основна. Таким чином, аналіз цих параметрів створює основу для подальшої оцінки ймовірності успішної реалізації атаки йогоїстичного майнінгу.

Розв'язуючи цю нерівність, отримуємо наступне твердження.

Твердження 1.1. *[1] Для заданого γ пул розміру α отримує дохід,*

більший за свою частку, якщо

$$\frac{1-\gamma}{3-2\gamma} < \alpha < \frac{1}{2}.$$

Це проілюстровано на рисунку 1.11, де показано дохід пулу для різних значень γ при зміні розміру пулу від 0 до 0,5.

Пул ризикує лише тоді, коли він приховує один блок, і чесні майнери можуть знайти конкуруючий блок. Для $\gamma = 1$ пул може швидко поширити свою гілку, тому всі чесні майнери майнять на ній. У цьому випадку пул не несе ризику, і його дохід завжди більший, ніж при чесному майнінгу, тобто поріг дорівнює нулю.

В іншому крайньому випадку, при $\gamma = 0$, поріг становить $\frac{1}{3}$. При $\gamma = \frac{1}{2}$ поріг дорівнює $\frac{1}{4}$.

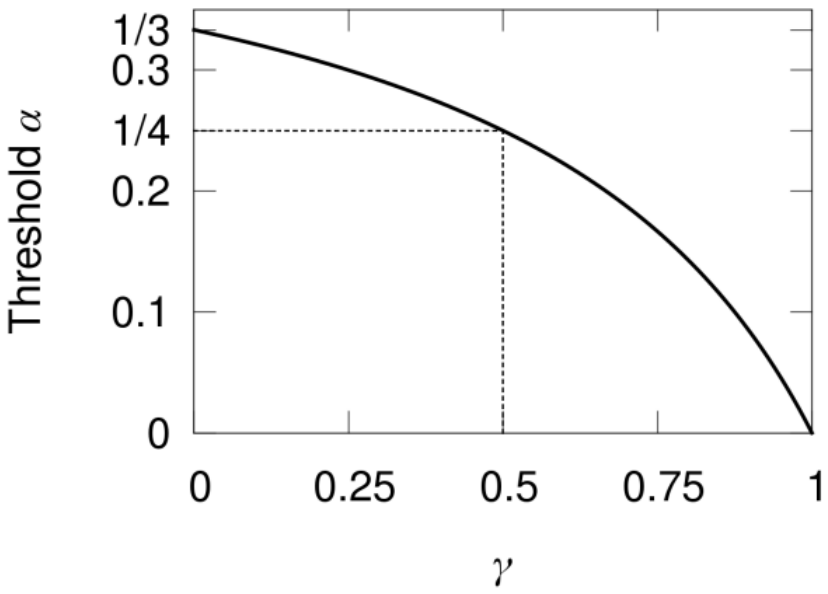

Рисунок 1.12 – Залежність порогу від γ

Нахил функції доходу пулу R_{pool} як функції розміру пулу є більшим за одиницю вище порогу.

Твердження 1.2. *[1] Для пулу, який використовує стратегію егоїстичного майнінгу, дохід кожного учасника зростає зі збільшенням*

розміру пулу, якщо розмір пулу перевищує поріг.

Слід зазначити, що наведена модель базується на ряді припущень. Зокрема, вважається, що чесні майнери дотримуються стандартного протоколу, час поширення блоків є незначним, а параметр γ узагальнює мережеві затримки та порядок отримання інформації майнерами. Крім того, модель розглядає стаціонарний режим роботи системи та не враховує динамічні зміни обчислювальної потужності мережі. Ці припущення необхідно враховувати при оцінці ймовірності реалізації атаки на практиці.

Було доведено, що щойно обчислювальна потужність егоїстичного пулу перевищує поріг, він може збільшити свій дохід, використовуючи стратегію егоїстичного майнінгу. У цей момент раціональні майнери будуть віддавати перевагу приєднанню до егоїстичного пулу, щоб збільшити свої доходи.

Крім того, учасники пулу будуть зацікавлені у прийнятті нових учасників, оскільки це збільшить їхній власний дохід. Таким чином, егоїстичний пул буде зростати без протидії з боку будь-якого механізму, поки не стане більшістю.

Як тільки майнінговий пул, егоїстичний чи ні, досягає більшості, він отримує контроль над блокчейном. У цьому випадку стратегія егоїстичного майнінгу стає непотрібною, оскільки інші майнери вже не можуть перевищити швидкість пулу. Натомість пул більшості може отримувати весь дохід системи, просто дотримуючись стандартного протоколу і ігноруючи блоки, створені поза пулом. Також у нього немає стимулу приймати нових учасників.

На цьому етапі мережа втрачає свою децентралізовану природу, як це було задумано спочатку.

Висновки до розділу 1

У першому розділі досліджено базові принципи функціонування технології блокчейн, її архітектуру та ключові компоненти. Окрему увагу приділено алгоритму консенсусу Proof of Work, який є фундаментом більшості сучасних криптовалют.

Головним акцентом розділу став детальний аналіз атаки егоїстичного майнінгу. Ця вразливість доводить: навіть якщо учасники мережі технічно не порушують правил протоколу, їхня виключно раціональна поведінка може загрожувати безпеці системи. Для глибокого розуміння механізму цієї атаки було розглянуто математичну модель у вигляді автомата станів, яка чітко ілюструє динаміку системи залежно від стратегічних рішень майнерів.

Завдяки цій моделі отримано аналітичні вирази для оцінки очікуваних доходів як егоїстичного пулу, так і чесної мережі. Було продемонстровано, що за певних співвідношень обчислювальної потужності зловмисника та швидкості поширення інформації в мережі егоїстичний пул здатен отримувати надприбуток, який перевищує його реальну частку хешрейту.

Отже, підсумовуючи, можна стверджувати, що ефективність егоїстичного майнінгу критично залежить від імовірнісних характеристик процесу генерації блоків та особливостей їх поширення. Ці теоретичні висновки створюють необхідне підґрунтя для переходу до подальшого розширеного аналізу фінансової доцільності такої атаки.

2 МАТЕМАТИЧНА ФОРМАЛІЗАЦІЯ ТА АНАЛІЗ АТАКИ ЕГОЇСТИЧНОГО МАЙНІНГУ В УМОВАХ МЕРЕЖЕВИХ ЗАТРИМОК

Безпека та стабільність блокчейн-мереж критично залежать від мережевих затримок. Врахування цих затримок дає змогу отримати нові результати в аналізі атаки егоїстичного майнінгу, що й буде здійснено у цьому розділі.

2.1 Математична формалізація процесу функціонування блокчейн-мережі в умовах безперервного часу

На даний момент існує велика кількість робіт, де розглядається атака егоїстичного майнінгу. Але зазвичай у цих роботах не враховуються часові затримки мережі. Без урахування параметрів мережі, зокрема часу синхронізації, результати цих досліджень мають суттєву похибку.

З огляду на це, у даній роботі розглядається атака егоїстичного майнінгу в умовах безперервного часу і з урахуванням мережевих затримок. У цьому розділі буде наведено базову математичну формалізацію процесу генерації блоків. За основу цього підрозділу було взято ймовірнісний апарат, запропонований авторами у [2]. Хоча у цій статті аналізується атака подвійної витрати, ймовірності успішного створення та розповсюдження блоків є універсальними. Вони слугуватимуть фундаментом для наших подальших дій.

Розглянемо загальну структуру блокчейн-мережі з довільним консенсусом, яка має одну спільну властивість: майнер, який створює наступний блок, обирається випадковим чином із множини всіх майнерів безпосередньо під час генерації блоку. Прикладом такого протоколу консенсусу є Proof-of-Work. Після створення блоку майнер повинен

поділитися ним з іншими учасниками мережі. Цей обмін може зайняти певний ненульовий час, який залежить від параметрів мережі.

Визначимо α як загальну інтенсивність генерації блоків у мережі:

$$\alpha = \alpha_H + \alpha_M,$$

де α_H, α_M — інтенсивності генерації блоків чесними майнерами та зловмисником відповідно.

Також визначимо Δ_H та Δ_M як часові затримки для чесних майнерів і зловмисника відповідно. Ми робимо припущення на користь зловмисника і вважаємо, що $\Delta_M \leq \Delta_H$ та визначимо $\Delta = \Delta_H - \Delta_M \geq 0$ як різницю між часовими затримками.

Значення $p_H = \frac{\alpha_H}{\alpha}$ та $p_M = \frac{\alpha_M}{\alpha}$ є частками чесних майнерів та зловмисника відповідно. У випадку протоколу консенсусу PoW ці значення дорівнюють відповідним хешрейтам; для інших протоколів ці значення є частками якихось інших ресурсів.

Далі ми отримаємо формулу для визначення ймовірності того, що наступний блок буде знайдений і розповсюджений швидше чесними чи егоїстичними майнерами. Для цього нам потрібно описати наступні величини та зв'язки між ними:

– T_H — випадкова величина, яка дорівнює часу, витраченому чесними майнерами на створення одного блоку;

– T'_H — випадкова величина, яка дорівнює часу, витраченому чесними майнерами на створення одного блоку та його розповсюдження по всіх вузлах (принаймні чесних) у мережі;

– T_M — випадкова величина, яка дорівнює часу, витраченому зловмисними майнерами на створення одного блоку;

– T'_M — випадкова величина, яка дорівнює часу, витраченому зловмисними майнерами на створення одного блоку та його розповсюдження по всіх вузлах (принаймні зловмисних) у мережі.

Випадкові величини T_H та T_M мають експоненціальні розподіли:

$$F_{T_H}(t) = P(T_H < t) = 1 - e^{-\alpha_H t},$$
$$F_{T_M}(t) = P(T_M < t) = 1 - e^{-\alpha_M t},$$

для параметрів $\alpha_H > 0, \alpha_M > 0$.

У наших позначеннях виконуються такі рівності:

$$T'_H = \Delta_H + T_H, \quad T'_M = \Delta_M + T_M.$$

Позначимо p_H ймовірність того, що чесні майнери створять наступний блок раніше, ніж зловмисні (за умови, що вони почали створювати цей блок одночасно), і $p_M = 1 - p_H$ — ймовірність протилежної події.

$$p_H = \frac{\alpha_H}{\alpha_H + \alpha_M}, \quad p_M = \frac{\alpha_M}{\alpha_H + \alpha_M}.$$

Також позначимо p'_H ймовірність того, що чесні майнери створять наступний блок і розповсюдять його по всіх вузлах мережі (принаймні по всіх чесних вузлах) раніше, ніж це зроблять зловмисні майнери, і p'_M — ймовірність протилежної події, $p'_M = 1 - p'_H$. Тоді:

$$p'_H = P(T'_H < T'_M), \quad p'_M = P(T'_M < T'_H)$$

і $p'_H + p'_M = 1$.

Лема 2.1. *[2] Для заданої мережі з параметрами $\alpha, \alpha_H, \alpha_M, \Delta_H$ та Δ_M ймовірність p'_M того, що наступний блок буде створений зловмисником, дорівнює:*

$$p'_M = 1 - e^{-\alpha_M \Delta} p_H.$$

Ймовірність p'_H того, що наступний блок буде створений чесними

майнерами, дорівнює:

$$p'_H = e^{-\alpha_M \Delta} p_H.$$

2.2 Порівняльний аналіз стратегій зловмисника та умови доцільності атаки

Розглянемо ситуацію, коли егоїстичний майнер знаходить блок швидше за чесних учасників мережі. Перед ним постає вибір: опублікувати знайдений блок одразу (тобто діяти згідно зі стандартним протоколом як чесний майнер) чи приховати його та почати атаку. Приховування блоку дає шанс на отримання більшої винагороди в майбутньому, однак несе ризик повної втрати винагороди за вже знайдений блок.

Розглядається сценарій із фіксованою глибиною розгалуження, що обмежена двома блоками. Тобто аналізується атака, що завершується, щойно одна зі сторін (чесна мережа або зловмисник) першою сформує ланцюг із двох послідовних блоків.

Для оцінки прибутковості введемо додаткові параметри, які для кожного згенерованого блоку вважатимемо фіксованими величинами:

– r — фіксована винагорода, що виплачується за один успішно знайдений блок;

– l — фіксовані витрати ресурсів на генерацію одного блоку.

Також припустимо, що час синхронізації пулу зловмисника дорівнює нулю ($\Delta_M = 0$). Таке припущення має сенс, оскільки йому не потрібно витрачати час на розповсюдження знайденого блоку іншим вузлам мережі. Натомість чесні майнери працюють децентралізовано, тому для них характерна затримка $\Delta_H > 0$, адже передача даних між ними потребує певного часу.

Розглянемо **перший сценарій** (назвемо його S_1), за якого зловмисник обирає чесну стратегію і публікує перший знайдений блок

одразу. Оскільки блок стає частиною основного ланцюга, зловмисник гарантовано отримує за нього чистий прибуток у розмірі $(r - l)$. Після цього розпочинається конкуренція за наступний (другий) блок, під час якої можливі два варіанти розвитку подій:

1) **Наступний блок також знаходить зловмисник.** Ймовірність цієї події дорівнює p'_M. У такому випадку зловмисник успішно знаходить два блоки поспіль. Його чистий прибуток за кожен знайдений блок становить $(r - l)$, отже, загальна вигода дорівнюватиме сумі цих прибутків: $2(r - l)$.

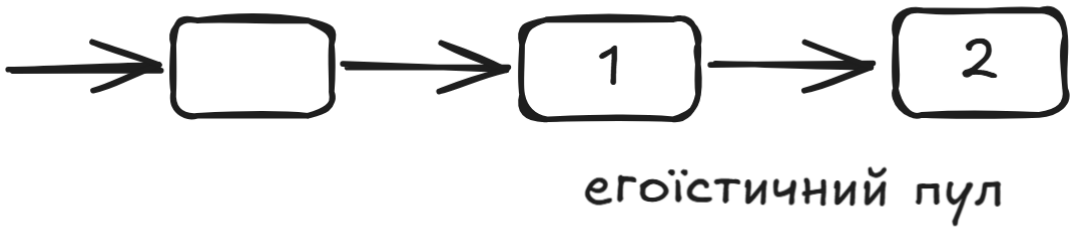

Рисунок 2.1

2) **Наступний блок знаходять чесні майнери.** Ймовірність цієї події дорівнює $1 - p'_M$. У цьому випадку зловмисник отримує чистий прибуток за перший знайдений блок у розмірі $(r - l)$, однак зазнає марних витрат l на спробу згенерувати другий блок. Тоді його загальна вигода становитиме $(r - l) - l$.

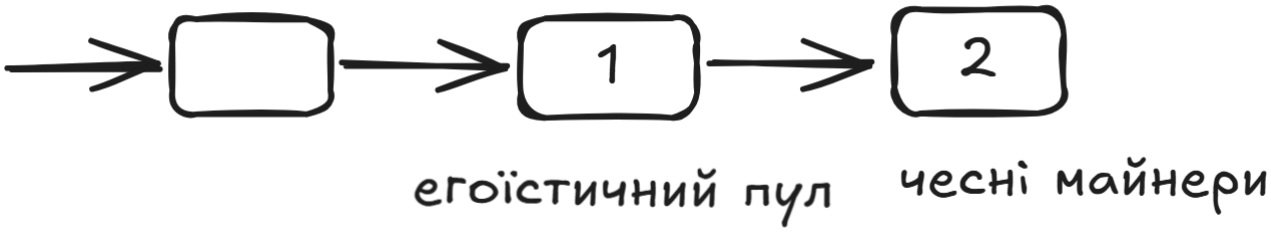

Рисунок 2.2

Тоді загальна очікувана вигода зловмисника від реалізації сценарію S_1 обчислюється як сума гарантованого прибутку за перший блок та очікуваних результатів конкуренції за другий блок:

$$U(S_1) = (r - l) + p'_M(r - l) - (1 - p'_M)l.$$

Тепер розглянемо **другий сценарій** (S_2), за якого зловмисник приховує свій перший знайдений блок і починає атаку. У цьому випадку можливі три варіанти розвитку подій:

1) **Наступний блок також знаходить зловмисник.** Ймовірність цієї події дорівнює p'_M. У такому випадку зловмисник успішно знаходить два блоки поспіль і публікує їх, перемагаючи в конкуренції. Його чистий прибуток за кожен знайдений блок становить $(r-l)$, отже, загальна вигода дорівнюватиме сумі цих прибутків: $2(r - l)$.

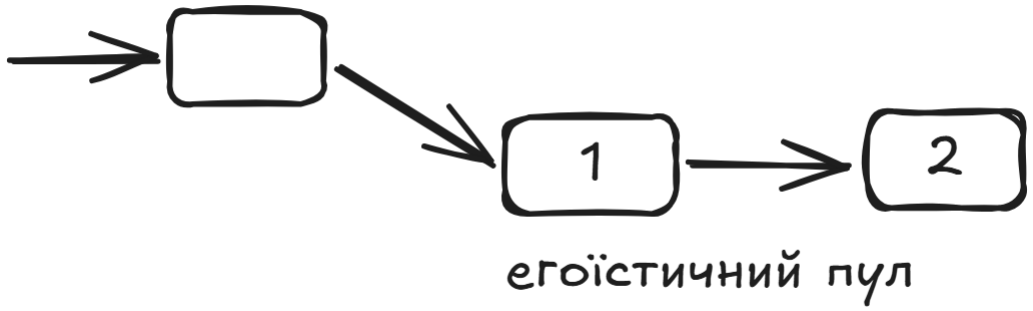

Рисунок 2.3

2) **Другий блок знаходять чесні майнери, а третій — зловмисник.** Ймовірність такої послідовності подій дорівнює $(1 - p'_M)p'_M$. У цьому випадку чесні майнери спочатку зрівнюють рахунок, але наступним блоком зловмисник виривається вперед. Він публікує свій ланцюг із двох блоків, і оскільки він довший, мережа приймає його. Його чистий прибуток за кожен знайдений блок становить $(r - l)$, отже, загальна вигода дорівнюватиме сумі цих прибутків: $2(r - l)$.

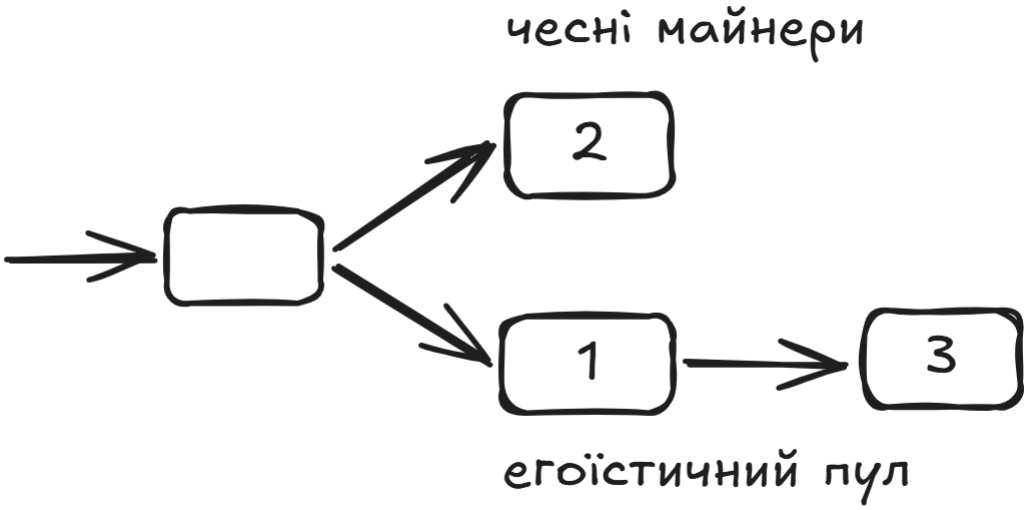

Рисунок 2.4

3) **Наступні два блоки поспіль знаходять чесні майнери.** Ймовірність цієї події дорівнює $(1 - p'_M)^2$. У цьому випадку чесні майнери формують ланцюг із двох блоків швидше. Прихований блок зловмисника відкидається мережею, і він не отримує жодної винагороди. Оскільки зловмисник встиг витратити свої ресурси на виготовлення двох блоків, за такого сценарію він зазнає збитків у розмірі $2l$.

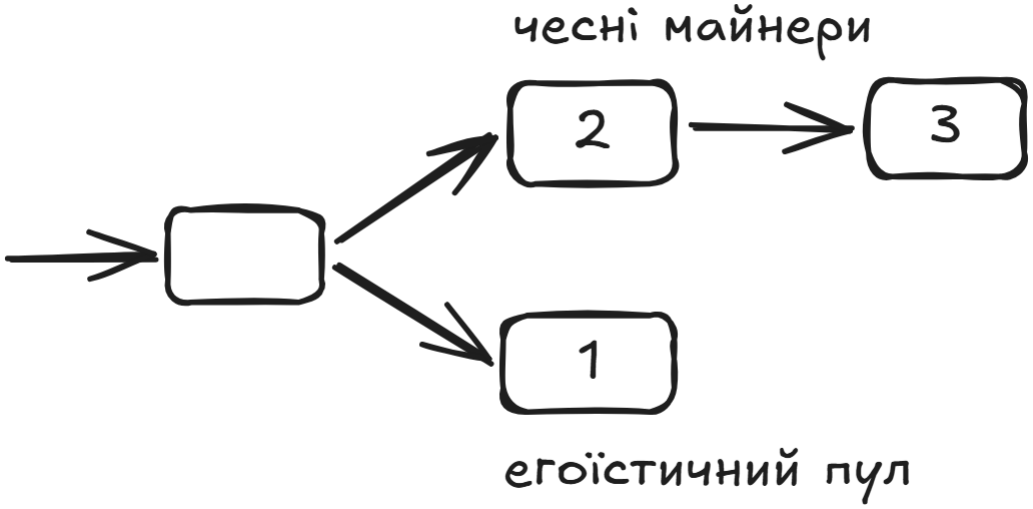

Рисунок 2.5

Загальна очікувана вигода зловмисника від реалізації сценарію S_2 обчислюється як сума добутків ймовірностей кожного з варіантів розвитку подій на відповідну їм чисту вигоду:

$$U(S_2) = p'_M \cdot 2(r-l) + (1-p'_M)p'_M \cdot 2(r-l) - (1-p'_M)^2 \cdot 2l.$$

Щоб визначити, за яких умов атака стає вигіднішою за чесну стратегію, нам потрібно розв'язати нерівність $U(S_1) \leq U(S_2)$.

Спочатку розкриємо дужки та максимально спростимо вирази для обох сценаріїв:

$$U(S_1) = (r-l) + p'_M(r-l) - (1-p'_M)l = r - l + p'_M r - p'_M l - l + p'_M l = \\ = p'_M r + r - 2l;$$

$$U(S_2) = p'_M \cdot 2(r-l) + (1-p'_M)p'_M \cdot 2(r-l) - (1-p'_M)^2 2l = \\ = 2p'_M r - 2p'_M l + 2p'_M r - 2(p'_M)^2 r - 2p'_M l + 2(p'_M)^2 l - 2l + 4p'_M l - 2(p'_M)^2 l = \\ = -2(p'_M)^2 r + 4p'_M r - 2l.$$

Тепер прирівняємо спрощені функції та скоротимо отриманий вираз:

$$p'_M r + r - 2l \leq -2(p'_M)^2 r + 4p'_M r - 2l,$$
$$p'_M r + r - 2l + 2(p'_M)^2 r - 4p'_M r + 2l \leq 0,$$
$$2(p'_M)^2 r - 3p'_M r + r \leq 0,$$
$$2(p'_M)^2 - 3p'_M + 1 \leq 0.$$

Знайдемо корені утвореного квадратного рівняння:

$$2(p'_M)^2 - 3p'_M + 1 = 0,$$
$$D = (-3)^2 - 4 \cdot 2 \cdot 1 = 1,$$
$$x_1 = \frac{-(-3) - 1}{2 \cdot 2} = \frac{1}{2},$$
$$x_2 = \frac{-(-3) + 1}{2 \cdot 2} = 1.$$

Парабола гілками вгору, тому наша нерівність виконується на проміжку $0{,}5 \leq p'_M \leq 1$. Але оскільки p'_M — це ймовірність, вона не може бути більшою за 1. Тому можемо просто сказати, що атака стає вигідною за умови, що $p'_M \geq 0{,}5$.

Тепер підставимо в отриманий вираз значення $p'_M = 1 - e^{-\alpha_M \Delta} p_H$:

$$p'_M \geq 0{,}5,$$
$$1 - e^{-\alpha_M \Delta} p_H \geq 0{,}5,$$
$$e^{-\alpha_M \Delta} p_H \leq 0{,}5,$$
$$p_H \leq \frac{0{,}5}{e^{-\alpha_M \Delta}},$$
$$p_H \leq \frac{e^{\alpha_M \Delta}}{2}.$$

Оскільки $p_H + p_M = 1$, ми можемо виразити цю умову через частку ресурсів зловмисника:

$$1 - p_M \leq \frac{e^{\alpha_M \Delta}}{2},$$
$$p_M \geq 1 - \frac{e^{\alpha_M \Delta}}{2}.$$

Але оскільки ми вважаємо, що $\Delta_M = 0$:

$$\Delta = \Delta_H - \Delta_M = \Delta_H.$$

Підставимо у формулу, отриману на минулому кроці:

$$p_M \geq 1 - \frac{e^{\alpha_M \Delta}}{2},$$
$$p_M \geq 1 - \frac{e^{\alpha_M \Delta_H}}{2}.$$

Тепер ми можемо сформулювати теорему, головний результат цього підрозділу.

Теорема 2.1. *Нехай у заданій мережі зловмисник знаходить блок першим. У випадку, коли боротьба зупиняється тієї миті, коли чесні або егоїстичні майнери першими знаходять 2 блоки, стратегія приховування знайденого блоку є вигіднішою за його негайне опублікування (тобто дотримання протоколу) тоді і тільки тоді, коли частка чесних майнерів задовольняє умову:*

$$p_H \leq \frac{e^{\alpha_M \Delta_H}}{2},$$

або якщо частка егоїстичних майнерів задовольняє умову:

$$p_M \geq 1 - \frac{e^{\alpha_M \Delta_H}}{2}.$$

2.3 Аналіз отриманих результатів

Отримавши вирази $p_H \leq \frac{e^{\alpha_M \Delta_H}}{2}$ та $p_M \geq 1 - \frac{e^{\alpha_M \Delta_H}}{2}$, можна зробити висновок, що саме Δ_H виступає каталізатором атаки. За ідеальних умов, коли $\Delta_H = 0$, поріг безпеки становить $p_M = 1 - \frac{1}{2} = 0{,}5$ (тобто 50%). Але якщо врахувати обов'язкові затримки синхронізації, цей поріг експоненційно зменшується. Це підтверджує, що за умов, наближених до реальних, мережі стають значно вразливішими до цієї атаки.

Для наочної демонстрації цього ефекту проведемо покроковий розрахунок критичного порогу p_M для мережі із заданою інтенсивністю генерації блоків пулом зловмисника $\alpha_M = 0{,}001$ с^{-1} та середньою

мережевою затримкою $\Delta_H = 20$ с.

Підставимо ці значення у виведену формулу межі прибутковості:

$$p_M = 1 - \frac{e^{0{,}001 \cdot 20}}{2} = 1 - \frac{e^{0{,}02}}{2}$$

Використовуючи наближене значення експоненти $e^{0{,}02} \approx 1{,}0202$, отримуємо:

$$p_M = 1 - \frac{1{,}0202}{2} = 1 - 0{,}5101 = 0{,}4899 \approx 0{,}4900$$

Отже, затримка всього у 20 секунд знижує поріг необхідної потужності для успішної атаки з 50% до 49%. Проведемо аналогічні розрахунки для інших типових значень затримок мережі та зведемо отримані результати до таблиці 2.1.

Таблиця 2.1 – Залежність порогу безпеки p_M від затримки Δ_H (при $\alpha_M = 0{,}001$ с$^{-1}$)

Δ_H (с)	α_M	p_M
1	0,001	0,4995
5	0,001	0,4975
20	0,001	0,4900
100	0,001	0,4475

На основі даних з таблиці можна переконатися, що навіть незначне зростання параметра Δ_H суттєво знижує поріг необхідного хешрейту зловмисника. Це доводить, що у мережах з повільною синхронізацією навіть егоїстичний пул середнього розміру може бути прибутковим.

2.4 Аналіз очікуваної вигоди зловмисника

Узагальнимо ситуацію, за якої зловмисник, першим знайшов блок і вирішує приховати його та ініціювати атаку егоїстичного майнінгу. Метою цього підрозділу є виведення формули для підрахунку очікуваної вигоди зловмисника для випадку, коли конкурентна боротьба зупиняється тієї миті, коли чесна мережа або егоїстичний пул першими знайдуть не 2, а n блоків, де $n > 2$.

Для цього ми будемо аналізувати всі можливі сценарії боротьби між чесною мережею та зловмисником. Кожен сценарій можна подати як шлях у дереві станів, де кожен крок — це знаходження нового блоку з імовірністю p'_M (для зловмисника) або $1 - p'_M$ (для чесних майнерів).

Простір усіх можливих варіантів розвитку подій доцільно розділити на дві неперетинні підмножини:

– **Позитивні сценарії** — ситуації, в яких зловмиснику вдається сформувати довший ланцюг і успішно завершити атаку, отримавши вигоду.

– **Негативні сценарії** — ситуації, в яких зловмисник не встигає випередити чесну мережу за n блоків.

Аналіз негативних сценаріїв. Негативний сценарій завершується в момент, коли чесні майнери знаходять і розповсюджують рівно n блоків. При цьому зловмисник за цей самий час міг знайти m блоків, де $0 \leq m \leq n - 2$. Загальна довжина такого сценарію (сумарна кількість блоків, знайдених чесною мережею та зловмисником) дорівнює $k = n + m$, відповідно $n \leq k \leq 2n - 2$.

Для підрахунку ймовірності реалізації одного такого сценарію довжини k необхідно перемножити ймовірність того, що чесні майнери знайдуть n блоків ($(1 - p'_M)^n$), та ймовірність того, що зловмисник знайде m блоків ($(p'_M)^m$): $(1 - p'_M)^n (p'_M)^m$.

Проте необхідно також врахувати кількість таких сценаріїв довжини

k.

Щоб визначити кількість таких унікальних траєкторій, необхідно проаналізувати допустиму послідовність знаходження блоків чесною мережею та зловмисником.

Оскільки точно відомо, що фінальним знайденим блоком буде n-й за рахунком блок чесних майнерів (адже саме він завершує конкурентну боротьбу їхньою перемогою), він фіксується. Тепер розглянемо гонку, що відбувається між початково знайденим прихованим блоком зловмисника та цим кінцевим фіксованим блоком. Оскільки егоїстичні майнери зі старту мають перевагу в один прихований блок, для того, щоб зловмисник жодного разу не перегнав чесну мережу, необхідно, щоб у відкритій боротьбі чесні майнери завжди мали строго більше знайдених блоків. Гонка завершується, коли зловмисник знаходить m блоків, а чесна мережа — $n-1$ блоків, причому виконується умова $m < n-1$.

Сформульована умова відповідає класичній задачі, яку описує строга теорема Бертрана про балотування. Підставимо наші параметри у формулу теореми і отримаємо точну кількість таких сценаріїв:

$$\frac{n-m-1}{n+m-1} C^{m}_{n+m-1}.$$

Отже, на даному етапі визначено ймовірність реалізації негативних сценаріїв для кожної фіксованої кількості блоків m $(0 \leq m \leq n-2)$, знайдених зловмисником, а також розраховано комбінаторну кількість таких унікальних траєкторій.

Фінансові збитки зловмисника формуються з марно витрачених ресурсів на генерацію m блоків, видобутих під час конкуренції, одного початкового прихованого блоку, а також одної марної спроби майнінгу, над якою зловмисник працював у момент публікації чесною мережею свого фінального n-го блоку. Таким чином, сумарні збитки зловмисника для одного такого сценарію становлять $(m+2)l$.

Щоб обчислити математичне сподівання загальних збитків

зловмисника у випадку його поразки, необхідно просумувати добутки збитків, імовірності та комбінаторної кількості шляхів для всіх можливих значень m:

$$S_{neg} = \sum_{m=0}^{n-2}(m+2)l \cdot (1-p'_M)^n (p'_M)^m \cdot \frac{n-m-1}{n+m-1} C^m_{n+m-1}.$$

Аналіз позитивних сценаріїв. Позитивні траєкторії будуються як продовження конкурентної боротьби, що не завершилася перемогою чесної мережі на попередніх етапах.

Повернемося до ситуації, коли егоїстичні майнери мають перегнати чесну мережу, поки вона не знайде і опублікує два блоки. У такому випадку очікувана вигода зловмисника за позитивні сценарії дорівнює $p'_M \cdot 2(r-l) + (1-p'_M)p'_M \cdot 2(r-l)$, а очікувані збитки лише за один негативний сценарій дорівнюють $(1-p'_M)^2 \cdot 2l$.

Якщо розглядати ситуацію, обмежену 3 або більше блоками, складові очікуваної вигоди від позитивних сценаріїв попереднього рівня повністю зберігаються. Але у зловмисника з'являється додаткова можливість випередити чесну мережу, трансформувавши негативні траєкторії з минулого етапу у виграшні.

Враховуючи, що в усіх таких негативних траєкторіях з минулого етапу чесні майнери вже знайшли і опублікували $n-1$ блок, вони перебувають всього за один крок до перемоги. Тому зловмисник для перемоги зобов'язаний безперервно знаходити наступні блоки поспіль, поки не пережене чесну мережу.

Отже, з кожної негативної траєкторії з минулого етапу з'являється рівно одна позитивна траєкторія на даному етапі.

Для розрахунку сумарної очікуваної вигоди від усіх нових позитивних траєкторій, сформованих на даному етапі, необхідно врахувати їхню кількість, ймовірність та фінансову вигоду кожного сценарію.

Щоб успішно завершити атаку, зловмисник повинен знайти $n-1$ блок

(не враховуючи початковий прихований блок). Під час створення кожної нової позитивної траєкторії чесна мережа вже встигає сформувати ланцюг із $n-1$ блоку, а ймовірність реалізації такого сценарію становить:

$$(1-p'_M)^{n-1}(p'_M)^{n-1}.$$

У разі успіху зловмисник отримує винагороду за n блоків, при цьому витрачаючи ресурси на їх генерацію. Отже, чиста фінансова вигода одного сценарію становить $n(r-l)$.

Щоб знайти загальну вигоду за всі нові позитивні траєкторії, утворені на даному етапі, залишилося знайти лише кількість таких нових позитивних сценаріїв.

Кількість таких унікальних траєкторій можна виразити через числа Каталана. Числа Каталана описують кількість можливих шляхів Діка на квадратній ґратці, тобто маршрутів з точки (0,0) в точку (k,k), кроки при цьому відбуваються лише праворуч або вгору, і при цьому шляхи ніколи не перетинають головну діагональ.

У нашому випадку крок праворуч — знайдений і опублікований блок чесною мережею, крок угору — знайдений і прихований блок зловмисником. Головна діагональ відображає стан рівності знайдених блоків обома сторонами. Перетин цієї діагоналі означає перемогу зловмисника, оскільки завдяки одному початковому прихованому блоку його ланцюг стає довшим.

Оскільки нам потрібно знайти кількість таких траєкторій, коли зловмисник вперше зрівнює рахунок лише на фінальному етапі, для підрахунку застосовується послідовність Каталана.

Кількість таких унікальних сценаріїв, за яких обидві сторони знаходять по $i = n-1$ блоків до моменту фінальної перемоги зловмисника, обчислюється за відповідною формулою Каталана:

$$Cat_{i-1} = \frac{1}{i}C_{2i-2}^{i-1}.$$

Для обчислення сумарної очікуваної вигоди від усіх позитивних сценаріїв необхідно врахувати як випадок миттєвого успіху атаки, так і траєкторії затяжної конкуренції. Початковий доданок $p'_M \cdot 2(r-l)$ відображає базовий сценарій, за якого зловмисник миттєво знаходить перший блок у відкритій гонці й одразу публікує ланцюг із двох блоків. Для випадків тривалого протистояння, коли зловмисник випереджає чесну мережу на етапах генерації від 2 до n блоків, параметр i (що відображає кількість кроків боротьби) змінюється в діапазоні від 1 до $n-1$.

Відповідно, формула для підрахунку загальної вигоди від всіх позитивних сценаріїв набуває вигляду:

$$S_{pos} = p'_M \cdot 2(r-l) + \sum_{i=1}^{n-1}(i+1)(r-l) \cdot (1-p'_M)^i (p'_M)^i \cdot \frac{1}{i} C_{2i-2}^{i-1}.$$

Ми вивели формули для підрахунку вигоди зловмисника від всіх позитивних сценаріїв і збитків від всіх негативних сценаріїв. Тоді, щоб знайти загальну очікувану вигоду, потрібно від S_{pos} відняти S_{neg}:

$$S = S_{pos} - S_{neg} = p'_M \cdot 2(r-l) + \sum_{i=1}^{n-1}(i+1)(r-l)(1-p'_M)^i (p'_M)^i \frac{1}{i} C_{2i-2}^{i-1} - \\ - \sum_{m=0}^{n-2}(m+2)l \cdot (1-p'_M)^n (p'_M)^m \frac{n-m-1}{n+m-1} C_{n+m-1}^{m}.$$

Отже, ми довели наступну теорему.

Теорема 2.2. *Нехай у заданій мережі зловмисник знаходить блок першим, вирішує приховати його та ініціювати атаку егоїстичного майнінгу за такого сценарію: конкурентна боротьба зупиняється тієї миті, коли егоїстичні майнери випереджають чесну мережу, знайшовши більше одного блоку, або чесні майнери знаходять і публікують n блоків. Загальна очікувана вигода зловмисника*

обчислюється за формулою:

$$S = p'_M \cdot 2(r-l) + \sum_{i=1}^{n-1}(i+1)(r-l)(1-p'_M)^i(p'_M)^i\frac{1}{i}C_{2i-2}^{i-1} - \\ - \sum_{m=0}^{n-2}(m+2)l \cdot (1-p'_M)^n(p'_M)^m\frac{n-m-1}{n+m-1}C_{n+m-1}^{m}.$$

2.5 Числовий аналіз очікуваної вигоди зловмисника для параметрів мережі Bitcoin

Щоб продемонструвати роботу виведеної формули, проведемо розрахунок на основі приблизних параметрів мережі Bitcoin.

Визначимо параметри на основі актуальної статистики мережі Bitcoin після халвінгу, який відбувся навесні 2024 року.

Загальна винагорода за блок (r) складається з фіксованої винагороди (3,125 BTC) та середніх комісій за транзакції (близько 0,175 BTC). Разом виходить 3,3 BTC. Якщо взяти ринковий курс біткоїна приблизно на рівні 75 000\$, то отримуємо винагороду: $3{,}3 \cdot 75\,000 = 247\,500$\$.

Собівартість генерації (l) обчислюється на основі фіксованої винагороди за блок (3,125 BTC) та середніх ринкових витрат на майнінг. Оскільки видобуток одного біткоїна наразі оцінюється у близько 55 000\$, загальні витрати ресурсів на створення одного блоку розраховуються як добуток цих величин: $3{,}125 \cdot 55\,000\$ = 171\,875$\$.

Оскільки складність завжди підлаштовується так, щоб генерувався один блок рівно кожні 10 хвилин, інтенсивність мережі (α) дорівнює $\frac{1}{600}$ с^{-1}.

Мережева затримка (Δ_H) в середньому дорівнює приблизно 10 с.

Чистий прибуток за кожен успішний блок становить: $r - l = 247\,500 - 171\,875 = 75\,625$\$.

Оберемо сценарій, за якого пул зловмисника контролює 35% обчислювальної потужності мережі ($p_M = 0.35$, $p_H = 0.65$).

Інтенсивність генерації пулу становить $\alpha_M = p_M \cdot \alpha = 0.35/600 \approx 0.000583$ с$^{-1}$.

Скористаємось Лемою 2.1:

$$p'_M = 1 - e^{-\alpha_M \Delta_H} p_H = 1 - e^{-0.00583} \cdot 0.65 \approx 1 - 0.9942 \cdot 0.65 \approx 0.3538.$$

Розглянемо випадок, коли атака обмежується глибиною $n = 3$ блоки.

Розрахунок для глибини обмеження $n = 3$ ($p_M = 0.35$): Очікуваний фінансовий дохід від позитивних сценаріїв:

$$\begin{aligned} S_{pos} &= 2p'_M(r-l) + 2(r-l)p'_M(1-p'_M) + 3(r-l)(p'_M)^2(1-p'_M)^2 = \\ &= 2(0.3538)(75\,625) + 2(75\,625)(0.3538)(0.6462) + \\ &+ 3(75\,625)(0.3538)^2(0.6462)^2 \approx 53\,512 + 34\,580 + 11\,863 = 99\,955\$. \end{aligned}$$

Очікувані фінансові збитки від негативних сценаріїв:

$$\begin{aligned} S_{neg} &= 2l(1-p'_M)^3 + 3lp'_M(1-p'_M)^3 = \\ &= 2(171\,875)(0.6462)^3 + 3(171\,875)(0.3538)(0.6462)^3 \approx \\ &\approx 92\,764 + 49\,220 = 141\,984\$. \end{aligned}$$

Загальний очікуваний прибуток зловмисника ($p_M = 0.35$) для обмеження $n = 3$ становить:

$$S = S_{pos} - S_{neg} = 99\,955 - 141\,984 = -42\,029\$$$

Отже, цей розрахунок доводить, що для пулу з хешрейтом 35% затримка у 10 секунд є недостатньою для подолання порогу прибутковості за умови обмеження у 3 блоки.

Проведемо такий самий підрахунок, якщо атака обмежена 6 блоками.

Розрахунок для глибини обмеження $n = 6$ ($p_M = 0.35$):

Очікуваний фінансовий дохід від позитивних сценаріїв:

$$\begin{aligned}
S_{pos} &= 2p'_M(r-l) + 2(r-l)p'_M(1-p'_M) + 3(r-l)(p'_M)^2(1-p'_M)^2 + \\
&+ 8(r-l)(p'_M)^3(1-p'_M)^3 + 25(r-l)(p'_M)^4(1-p'_M)^4 + \\
&+ 84(r-l)(p'_M)^5(1-p'_M)^5 = \\
&= 2(0.3538)(75\,625) + 2(75\,625)(0.3538)(0.6462) + \\
&+ 3(75\,625)(0.3538)^2(0.6462)^2 + 8(75\,625)(0.3538)^3(0.6462)^3 + \\
&+ 25(75\,625)(0.3538)^4(0.6462)^4 + 84(75\,625)(0.3538)^5(0.6462)^5 \approx \\
&\approx 53\,512 + 34\,582 + 11\,867 + 7\,240 + 5\,176 + 3\,977 = 116\,354\$.
\end{aligned}$$

Очікувані фінансові збитки від негативних сценаріїв:

$$\begin{aligned}
S_{neg} &= 2l(1-p'_M)^6 + 12lp'_M(1-p'_M)^6 + 36l(p'_M)^2(1-p'_M)^6 + \\
&+ 70l(p'_M)^3(1-p'_M)^6 + 84l(p'_M)^4(1-p'_M)^6 = \\
&= 2(171\,875)(0.6462)^6 + 12(171\,875)(0.3538)(0.6462)^6 + \\
&+ 36(171\,875)(0.3538)^2(0.6462)^6 + 70(171\,875)(0.3538)^3(0.6462)^6 + \\
&+ 84(171\,875)(0.3538)^4(0.6462)^6 \approx \\
&\approx 25\,234 + 53\,564 + 56\,860 + 39\,115 + 16\,601 = 191\,374\$.
\end{aligned}$$

Загальний очікуваний прибуток зловмисника ($p_M = 0.35$) для обмеження $n = 6$ становить:

$$S = S_{pos} - S_{neg} = 116\,354 - 191\,374 = -75\,020\$.$$

Порівнюючи результати для $n = 3$ ($-42\,029\$$) та $n = 6$ ($-75\,020\$$), можна зробити висновок, що атака за таких параметрів не є прибутковою, і ця прибутковість зменшується при затягуванні боротьби. Зловмисник витрачає додаткові ресурси, які навряд чи згодом окупляться.

Щоб остаточно продемонструвати роботу запропонованого математичного підходу, тепер проведемо розрахунки для великого майнінгового пулу, який контролює 45% обчислювальної потужності мережі ($p_M = 0.45$, $p_H = 0.55$).

Інтенсивність генерації такого пулу становить $\alpha_M = p_M \cdot \alpha = 0.45/600 = 0.00075$ с$^{-1}$.

Знову скористаємось Лемою 2.1:

$$p'_M = 1 - e^{-\alpha_M \Delta_H} p_H = 1 - e^{-0.0075} \cdot 0.55 \approx 1 - 0.9925 \cdot 0.55 \approx 0.4541.$$

Розрахунок для глибини обмеження $n = 3$ ($p_M = 0.45$):

Очікуваний фінансовий дохід від позитивних сценаріїв:

$$\begin{aligned} S_{pos} &= 2p'_M(r-l) + 2(r-l)p'_M(1-p'_M) + 3(r-l)(p'_M)^2(1-p'_M)^2 = \\ &= 2(0.4541)(75\,625) + 2(75\,625)(0.4541)(0.5459) + \\ &+ 3(75\,625)(0.4541)^2(0.5459)^2 \approx \\ &\approx 68\,683 + 37\,493 + 13\,946 = 120\,122\$. \end{aligned}$$

Очікувані фінансові збитки від негативних сценаріїв:

$$\begin{aligned} S_{neg} &= 2l(1-p'_M)^3 + 3lp'_M(1-p'_M)^3 = \\ &= 2(171\,875)(0.5459)^3 + 3(171\,875)(0.4541)(0.5459)^3 \approx \\ &\approx 55\,921 + 38\,092 = 94\,013\$. \end{aligned}$$

Загальний очікуваний прибуток зловмисника ($p_M = 0.45$) для обмеження $n = 3$ становить:

$$S = S_{pos} - S_{neg} = 120\,122 - 94\,013 = 26\,109\$.$$

Для значення параметра $p_M = 0.35$ атака не була прибутковою, проте для $p_M = 0.45$ спостерігається інша тенденція. Тепер атака для зловмисника стала фінансово вигідною.

Розрахунок для глибини обмеження $n = 6$ ($p_M = 0.45$):

Аналогічний розрахунок проведемо для затяжної атаки.

Очікуваний фінансовий дохід від позитивних сценаріїв:

$$\begin{aligned} S_{pos} &= 2(0.4541)(75\,625) + 2(75\,625)(0.4541)(0.5459) + \\ &+ 3(75\,625)(0.4541)^2(0.5459)^2 + 8(75\,625)(0.4541)^3(0.5459)^3 + \\ &+ 25(75\,625)(0.4541)^4(0.5459)^4 + 84(75\,625)(0.4541)^5(0.5459)^5 \approx \\ &\approx 68\,683 + 37\,493 + 13\,946 + 9\,218 + 7\,141 + 5\,945 = 142\,426\$. \end{aligned}$$

Очікувані фінансові збитки від негативних сценаріїв:

$$\begin{aligned} S_{neg} &= 2(171\,875)(0.5459)^6 + 12(171\,875)(0.4541)(0.5459)^6 + \\ &+ 36(171\,875)(0.4541)^2(0.5459)^6 + 70(171\,875)(0.4541)^3(0.5459)^6 + \\ &+ 84(171\,875)(0.4541)^4(0.5459)^6 \approx \\ &\approx 9\,088 + 24\,765 + 33\,735 + 29\,774 + 16\,223 = 113\,585\$. \end{aligned}$$

Загальний очікуваний прибуток зловмисника ($p_M = 0.45$) для затяжної атаки з обмеженням $n = 6$ становить:

$$S = S_{pos} - S_{neg} = 142\,426 - 113\,585 = 28\,841\$.$$

На основі цих розрахунків можна зробити висновок, що якщо частка пулу досягає 45%, атака стає прибутковою, і доцільно не зупинятися на обмеженні у 3 блоки. Зі збільшенням тривалості конкурентної боротьби очікувана фінансова вигода зростає.

Для зручності зведемо всі розраховані фінансові показники до підсумкової таблиці.

Таблиця 2.2 – Порівняльний аналіз очікуваної вигоди зловмисника

p_M	n	S_{pos}	S_{neg}	S
0.35 (35%)	3	99 955$	141 984$	**-42 029$**
	6	116 354$	191 374$	**-75 020$**
0.45 (45%)	3	120 122$	94 013$	**26 109$**
	6	142 426$	113 585$	**28 841$**

Висновки до розділу 2

У цьому розділі ми розглянули атаку егоїстичного майнінгу з урахуванням безперервного характеру часу та наявності затримок мережі. Такий підхід дозволив отримати точніші результати. Ми змогли проаналізувати, наскільки суттєво мережеві затримки впливають на успіх атаки.

Було досліджено, яка стратегія є фінансово вигіднішою для зловмисника після знаходження одного блоку: його приховання та ініціювання атаки чи негайна публікація. Для сценарію, коли егоїстичні майнери пробують перегнати чесну мережу, поки вона не знайде і опублікує два блоки, було визначено точні межі прибутковості. Отримані результати підтвердили вразливість систем з великою затримкою.

Також обмеження у 2 блоки було розширено до n блоків. Було виведено універсальну формулу для підрахунку загальної фінансової вигоди зловмисника. Отримана формула не має жорстких обмежень і може застосовуватися для будь-якої тривалості конкурентної гонки. Це дозволить у майбутньому проводити аналіз найбільш доцільного сценарію для зловмисника з обмеженням в n блоків.

На основі цього виразу було проведено розрахунки для параметрів,

наближених до характеристик мережі Bitcoin. Це дозволило наочно продемонструвати роботу формули та визначити, за яких умов атака стає доцільною для зловмисника.

ВИСНОВКИ

У цій роботі ми дослідили рівень безпеки децентралізованих блокчейн-мереж під час атаки егоїстичного майнінгу з урахуванням мережевих затримок. Усі завдання, поставлені на початку дослідження, були успішно виконані.

1) У ході роботи було проведено огляд опублікованих джерел за тематикою дослідження. Аналіз літератури показав, що проблема вразливості консенсусу Proof-of-Work залишається відкритою, а існуючі аналітичні підходи потребують адаптації до практичних умов функціонування мереж.

2) Виконано ґрунтовне дослідження наукових статей, присвячених безпосередньо аналізу атаки егоїстичного майнінгу. З'ясовано, що більшість базових підходів ідеалізують умови, розглядаючи дискретний час та ігноруючи фізичні затримки поширення інформації. Це призводить до хибного припущення, що поріг безпеки мережі становить 50% обчислювальної потужності.

3) Здійснено математичну формалізацію процесу генерації блоків. На відміну від класичних підходів, розроблений математичний апарат повністю враховує безперервний характер часу та мережеві затримки. Було доведено, що наявність затримок експоненційно підвищує ймовірність перемоги зловмисника в конкурентній боротьбі.

4) Проведено порівняльний аналіз стратегій зловмисника за умови знаходження ним одного початкового блоку. Було визначено чіткі критерії прибутковості: коли саме приховування блоку та ініціювання атаки стає фінансово вигіднішим за чесну публікацію.

5) Проведено дослідження умов доцільності атаки на прикладі числових параметрів, наближених до функціонування реальної мережі. Розрахунки підтвердили, що мережева затримка суттєво знижує поріг необхідної потужності пулу, дозволяючи зловмисникам з хешрейтом

менше 50% успішно здійснювати атаки.

6) Виконано завдання щодо розширення умов атаки: виведено універсальну аналітичну формулу для розрахунку загальної очікуваної фінансової вигоди зловмисника при глибині атаки до n блоків. Використавши методи теорії ймовірності, комбінаторного аналізу, числа Каталана та строгу теорему Бертрана про балотування, вдалося розробити математичний апарат, який не має жорстких обмежень і може застосовуватись до будь-якої тривалості конкурентної гонки.

7) Здійснено успішну перевірку отриманої формули на основі параметрів, наближених до актуальних характеристик мережі Bitcoin. Числовий аналіз наочно довів працездатність формули.

Напрямки подальших досліджень. Оскільки розроблений математичний апарат знімає обмеження на довжину атаки, найпершим перспективним напрямком є визначення, яка саме стратегія (чесна публікація чи приховування) є фінансово найбільш доцільною для пулу при будь-якій довільній кількості блоків n та заданих параметрах мережі. Крім того, в наступних роботах варто звернути увагу на дослідження більш складних сценаріїв, за яких у мережі одночасно діють кілька незалежних пулів-зловмисників. Також доцільно було б розглянути випадки, коли винагорода та витрати на створення одного блоку є не фіксованими, а динамічними величинами.

ПЕРЕЛІК ПОСИЛАНЬ

[1] Eyal I. та other. *Majority is not Enough: Bitcoin Mining is Vulnerable*. Англ. 2013.

[2] Kovalchuk L. та other. *Decreasing Security Threshold Against Double Spend Attack in Networks with Slow Synchronization*. Англ. 2019.

[3] Saad M. та other. *Exploring the Attack Surface of Blockchain*. Англ.

[4] Nakamoto та other. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008.

[5] Vokerla R. R. та other. *An Overview of Blockchain Applications and Attacks*. Англ.

[6] Dylan Y. та other. *Blockchain Technology Overview*. Англ. 2018.

[7] Zheng та other. *An Overview of Blockchain Technology: Architecture, Consensus and Future Trends*. 2017.

[8] Соколова Т. Н. та Волошин И. П. *Преимущества и недостатки технологии блокчейн*. Рос.