ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Дослідження побудови оптимальних рішень у децентралізованих системах на основі блокчейну»

на здобуття освітнього ступеня магістра

зі спеціальності 122 Комп'ютерні науки

(код, найменування спеціальності)

освітньо-професійної програми Комп'ютерні науки

(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Данило КАНЄВСЬКИЙ

(підпис) *(Ім'я, ПРІЗВИЩЕ здобувача)*

Виконав:

здобувач вищої освіти Данило КАНЄВСЬКИЙ

група КНДМ-63

Керівник: Сергій Іщеряков

науковий ступінь, вчене звання к.т.н., професор

Рецензент:

науковий ступінь, вчене звання _____

(Ім'я, ПРІЗВИЩЕ)

Київ 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Комп'ютерних наук
Ступінь вищої освіти Магістр
Спеціальність Комп'ютерні науки
Освітньо-професійна програма Комп'ютерні науки

ЗАТВЕРДЖУЮ
Завідувач кафедрою Комп'ютерних наук

_____Віктор ВИШНІВСЬКИЙ
«_____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Канєвському Данилу Вікторовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Дослідження побудови оптимальних рішень у децентралізованих системах на основі блокчейну
керівник кваліфікаційної роботи Сергій ІЩЕРЯКОВ к.т.н., професор,
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» 10.2023р. №145
2. Строк подання кваліфікаційної роботи «29» грудня 2023р.
3. Вихідні дані до кваліфікаційної роботи: науково-технічна література, аналіз і дослідження блокчейнів.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
   Аналіз технічних основ блокчейну, його розвитку та сучасного стану
   Дослідження застосування блокчейну у фінансовій сфері
   Розробка власного продукту з агрегації ліквідності та пошуку найкращої ціни
5. Перелік графічного матеріалу: *презентація*
   1. Блокчейн та його основи
   2. Застосування блокчейну у сфері фінансів
   3. Дослідження актуальності теми агрегації ліквідності

4. Аналіз власного продукту, його проблем та способів покращення

6. Дата видачі завдання «19» жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз та розвиток блокчейн технологій та їх застосування у фінансовій сфері	19.10-06.11.23	
2	Дослідження основних принципів і компонентів блокчейну, включаючи механізми консенсусу	06.11-14.11.23	
3	Аналіз безпеки, прозорості та поточного стану блокчейн технологій	14.11-19.11.23	
4	Розробка та математичний опис власного рішення для агрегації ліквідності та пошуку найкращих цін	19.11-24.11.23	
5	Реалізація та тестування модулів моніторингу та оптимізації в рамках розробленого рішення	25.11-03.12.23	
6	Оцінка обмежень, викликів та можливостей для майбутніх досліджень у контексті блокчейн та децентралізованих фінансових систем	03.12-15.12.23	
7	Оформлення роботи: вступ, висновки, реферат	15.12-20.12.23	
8	Розробка демонстраційних матеріалів	21.12-29.12.23	

Здобувач вищої освіти _____ Данило КАНЄВСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Сергій ІЩЕРЯКОВ
(підпис) ***(Ім'я, ПРІЗВИЩЕ)***

РЕФЕРАТ

Текстова частина магістерської роботи: 77 с., 4 табл., 11 рис., 12 джерел.

Наукове завдання – дослідити побудову оптимальних рішень у децентралізованих системах на основі блокчейну.

Мета роботи – аналізувати застосування блокчейн технологій у сфері фінансів та розробити власне рішення для агрегації ліквідності і пошуку найкращої ціни на ринку.

Об'єкт дослідження – децентралізовані системи на основі блокчейну.

Предмет дослідження – блокчейн технології та їх застосування в фінансовій сфері, зокрема в агрегації ліквідності та оптимізації транзакцій.

Короткий зміст роботи: У роботі проведено детальний аналіз блокчейну, його розвитку, технічних аспектів та застосування у фінансах. Розглянуто приклади децентралізованих фінансових рішень, таких як Uniswap, 1inch, Balancer. Також було розроблено власне рішення, що включає модулі моніторингу та оптимізації для пошуку найкращих цін на ринку.

Робота включає аналіз проблем агрегації ліквідності, опис та порівняння різних алгоритмів розв'язку, а також реалізацію та тестування власного продукту. Також проведено аналіз продукту, можливі недоліки та способи підвищення якості роботи.

КЛЮЧОВІ СЛОВА: БЛОКЧЕЙН, ДЕЦЕНТРАЛІЗОВАНІ СИСТЕМИ, ФІНАНСИ, АГРЕГАЦІЯ ЛІКВІДНОСТІ, ОПТИМАЛЬНЕ РІШЕННЯ, КРИПТОВАЛЮТИ, АЛГОРИТМ РЮКЗАКА

ABSTRACT

Textual part of the master's thesis: 77 pages, 9 tables, 6 figures, 12 sources.

Research objective – to investigate the construction of optimal solutions in decentralized systems based on blockchain.

The goal of the work – to analyze the application of blockchain technologies in the financial sector and develop a proprietary solution for liquidity aggregation and finding the best market price.

Research object – decentralized systems based on blockchain.

Subject of research – blockchain technologies and their application in the financial sector, specifically in liquidity aggregation and transaction optimization.

Summary of the work: This work conducts a detailed analysis of blockchain, its development, technical aspects, and application in finance. Examples of decentralized financial solutions such as Uniswap, 1inch, Balancer have been considered. A proprietary solution has been developed, which includes monitoring and optimization modules for finding the best market prices.

The work includes an analysis of liquidity aggregation problems, description and comparison of various solution algorithms, as well as the implementation and testing of the proprietary product. The analysis of the product, potential shortcomings, and ways to improve its functionality have also been conducted.

KEYWORDS: BLOCKCHAIN, DECENTRALIZED SYSTEMS, FINANCE, LIQUIDITY AGGREGATION, OPTIMAL SOLUTION, CRYPTOCURRENCIES, KNAPSACK ALGORITHM

ЗМІСТ

ВСТУП **9**
1 АНАЛІЗ ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМ НА ОСНОВІ БЛОКЧЕЙНУ **10**
1.1 Основи блокчейну 10
1.2 Історичний розвиток блокчейну 12
1.3 Технічні основи та базові компоненти блокчейну 14
1.4 Механізми Консенсусу: Proof of Work проти Proof of Stake 18
1.5 Безпека та прозорість блокчейну 23
1.6 Аналіз сучасного стану блокчейну 26
2 ВИКОРИСТАННЯ БЛОКЧЕЙНУ У СФЕРІ ФІНАНСІВ **30**
2.1 Блокчейн у фінансовій сфері 30
2.2 Криптовалюти та цифрові активи 37
2.3 Блокчейн у традиційних фінансових системах 41
2.4 Кейс-стаді та приклади 44
3 РОЗРОБКА ВЛАСНОГО РІШЕННЯ АГРЕГАЦІЇ ЛІКВІДНОСТІ І ПОШУКУ НАЙКРАЩОЇ ЦІНИ **47**
3.1 Проблема та складність агрегації ліквідності у децентралізованих системах 47
3.2 Математичний опис проблеми рюкзака 49
3.3 Порівняння алгоритмів розв'язку проблеми рюкзака 51
3.4 Розробка рішення з використанням алгоритму Рюкзака 54
3.5 Реалізція окремих модулів продукту 57
3.5.1 Реалізація модуля моніторингу 57
3.5.2 Реалізція модуля оптимізації 59
3.6 Перевірка та тестування 62
3.6.1 Тестування модуля моніторингу 62
3.6.2 Тестування модуля оптимізації 66
3.7 Обмеження, виклики та майбутні перспективи 70
ВИСНОВКИ **73**
ПЕРЕЛІК ПОСИЛАНЬ **74**
ДОДАТОК А **75**

ВСТУП

У сучасному світі, де технології розвиваються з неймовірною швидкістю, блокчейн вирізняється як одна з найбільш обговорюваних та інноваційних технологій. Ця технологія, що лежить в основі таких криптовалют як Bitcoin і Ethereum, показала свою актуальність та доцільність у різноманітних сферах діяльності, від фінансів до управління цифровими активами.

Використання блокчейну набуває особливої ваги у контексті децентралізованих фінансових систем. Вона пропонує безпечну, прозору та надійну альтернативу традиційним централізованим фінансовим установам. Відсутність централізованого контролю та здатність до самоуправління роблять децентралізовані системи більш стійкими до зовнішніх втручань та маніпуляцій.

Водночас, розробка та побудова децентралізованих систем на основі блокчейну вимагає глибоких знань і розуміння не тільки в сфері блокчейн технологій, але й в областях криптографії, мережевих технологій та комп'ютерних наук. Також важливим аспектом є розробка алгоритмів для оптимізації та ефективності роботи цих систем.

У цій дипломній роботі ми зосередимося на дослідженні побудови оптимальних рішень у децентралізованих системах, зокрема на вивченні та аналізі різних підходів та методик, які можуть бути застосовані для підвищення ефективності та безпеки таких систем. Мета полягає в тому, щоб визначити найбільш ефективні та надійні методики для оптимізації роботи децентралізованих систем на базі блокчейну, що є актуальною та важливою темою у сфері сучасних технологій.

1 АНАЛІЗ ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМ НА ОСНОВІ БЛОКЧЕЙНУ

1.1 Основи блокчейну

Блокчейн можна описати як цифрову книгу обліку, де записи про транзакції або дані групуються в "блоки". Кожен новий блок інформації зв'язаний з усіма попередніми блоками, утворюючи ланцюг, звідси і походить назва "блокчейн" (ланцюг блоків).

Основна ідея полягає в тому, що дані розподілені по мережі і не зосереджені в одному центральному місці. Це означає, що всі записи є відкритими і верифікованими учасниками мережі, забезпечуючи прозорість і безпеку даних без необхідності централізованої контрольної системи.

З техночної точки зору, блокчейн — це розподілена база даних, що складається з блоків, пов'язаних і захищених за допомогою криптографії. Кожен блок містить криптографічний хеш попереднього блоку, часову мітку і транзакційні дані. Ця технологія вперше була запропонована в 2008 році анонімною особою або групою осіб під псевдонімом Сатоші Накамото і стала основою для першої цифрової валюти, Bitcoin.

Такий підхід може бути використаний не тільки для криптовалют, але й у багатьох інших застосуваннях, таких як смарт-контракти, децентралізовані фінансові послуги, системи управління постачаннями, ідентифікації, голосування, проведення аукціонів та багато іншого.

Особливістю блокчейну є те, що він дозволяє досягти високого рівня довіри і безпеки в мережі без потреби в центральному регуляторі. Це відбувається завдяки використанню розподіленого реєстру, де кожен учасник мережі має копію всіх записів, а нові записи додаються тільки після верифікації більшістю учасників.

Такий підхід вирішує проблему "подвійного витрачання" у випадку з криптовалютами і забезпечує прозорість і незмінність записів у всіх інших застосуваннях. Одночасно з цим, блокчейн має свої виклики і обмеження, такі як масштабованість, споживання енергії і правові аспекти.

Відповідно можемо сформувати декілька унікальних характеристик, які роблять його особливо корисним для широкого спектра застосувань:

1. **Децентралізація**: На відміну від традиційних баз даних, які зберігаються на центральному сервері, блокчейн розподіляє свої дані по мережі комп'ютерів. Це означає, що немає єдиного контрольного пункту, який може бути вразливим для атак, помилок або цензури.

2. **Прозорість**: Всі транзакції, що зберігаються на блокчейні, є публічними і можуть бути переглянуті всіма учасниками мережі. Ця прозорість забезпечує високий рівень довіри та підзвітності.

3. **Незмінність**: Після того, як транзакція додана до блокчейну, змінити її надзвичайно складно. Кожен блок містить унікальний хеш попереднього блоку, утворюючи ланцюг.

4. **Безпека**: Блокчейн використовує криптографічні алгоритми для захисту даних. Це означає, що дані можуть бути переглянуті та змінені лише учасниками, які мають відповідні криптографічні ключі, забезпечуючи високий рівень безпеки.

5. **Розподілений Консенсус**: В блокчейні для додавання нового блоку до ланцюга потрібно, щоб більшість учасників мережі погодились на його дійсність. Це відомо як механізм консенсусу, який допомагає запобігати фальсифікації та подвійному витрачанню в мережі.

6. **Програмованість**: Блокчейн дозволяє створювати складні правила і логіку в смарт-контрактах, які автоматично виконуються, коли виконуються певні умови. Це розширює можливості застосування блокчейну далеко за межі простих транзакцій.

1.2 Історичний розвиток блокчейну

Історичний розвиток блокчейну має свої корені в декількох десятиліттях розвитку цифрових технологій і криптографії. До появи першої криптовалюти, концепції, пов'язані з розподіленими базами даних і криптографічним захистом інформації, вже активно обговорювалися та розроблялися в академічних колах.

Ранні концепції розподіленого реєстру і цифрової безпеки були запропоновані в 1980-х та 1990-х роках, але ключовий момент у розвитку блокчейну настав з роботою Стюарта Хабера і В. Скотта Сторнетти. У 1991 році вони вперше висунули ідею ланцюга блоків для забезпечення цифрової безпеки, створивши систему, що використовувала хешування для забезпечення інтегральності цифрових документів [1].

Важливим етапом у розвитку блокчейну стала робота в області криптографії, особливо створення асиметричної криптографії, яка дозволила безпечний обмін ключами між сторонами. Ці розвитки заклали фундамент для створення блокчейну який ми його знаємо сьогодні.

Знаковою подією в історії блокчейну стало опублікування документа "Bitcoin: A Peer-to-Peer Electronic Cash System" анонімною особою або групою осіб під псевдонімом Сатоші Накамото в 2008 році. Цей документ представив світу перший працюючий блокчейн, який став основою для Bitcoin.

Починаючи з 2009 року, коли Bitcoin було запущено, технологія блокчейну почала швидко розвиватися, виходячи за рамки криптовалют. На ринку з'явилися нові криптовалюти, а також інші застосування блокчейну, включаючи смарт-контракти та децентралізовані додатки (DApps).

Після свого становлення з появою Bitcoin, блокчейн продовжував розвиватися та адаптуватися, зазнаючи значних змін у своїй структурі та застосуванні. На сьогоднішній день блокчейн представляє собою глобальну екосистему з різноманітними варіантами та застосуваннями.

Останніми роками блокчейн трансформувався в технологію, що лежить в основі широкого спектра децентралізованих застосувань, від фінансів до управління ланцюгами постачань, від цифрового авторського права до систем голосування.

У період з 2009 по 2023 рік, блокчейн технологія відзначилася швидким розвитком різних типів мереж, які включають публічні, приватні, консорціумні та гібридні системи. Публічні блокчейни, як Bitcoin і Ethereum, набули великої популярності та визнання, забезпечуючи повну децентралізацію та відкритість.

Окрім розвитку різних типів блокчейнів, значним був прогрес у розробці алгоритмів та механізмів консенсусу. Proof of Work, який був революційним для Bitcoin, поступово доповнювався або замінювався більш ефективними та екологічними механізмами, такими як Proof of Stake та його варіації (Delegated Proof of Stake, Proof of Authority).

Застосування блокчейну виросло далеко за межі криптовалют, охоплюючи такі сфери, як фінанси, забезпечення ланцюгів постачання, голосування, ідентифікація та цифрове мистецтво. Розвиток смарт-контрактів, який почався з Ethereum, відкрив широкі можливості для автоматизації та інновацій у блокчейні, перетворивши його на потужний інструмент для створення децентралізованих додатків (DApps).

На сьогоднішній день блокчейн продовжує свій розвиток, адаптуючись до нових викликів та можливостей. Він зміцнює свої позиції як ключова технологія в багатьох інноваційних проектах, від фінансових операцій до цифрової ідентичності, створюючи нові горизонти для досліджень, розвитку та застосування.

Цей розділ дипломної роботи має на меті надати читачу глибоке розуміння того, як блокчейн розвивався з часу свого винайдення і як він перетворився з теоретичної концепції на технологію, яка зараз має глобальний вплив. Вивчення історичного розвитку дозволяє зрозуміти поточний стан технології блокчейну та її можливі майбутні траєкторії розвитку.

1.3 Технічні основи та базові компоненти блокчейну

У цьому розділі ми зосередимося на технічних аспектах блокчейну, детально розглядаючи що таке блоки, вузли та майнери, та як вони співпрацюють для підтримки функціонування блокчейн мережі.

Блок у контексті блокчейну можна порівняти зі сторінкою в цифровій книзі обліку. Кожен блок містить пакет транзакцій, які були здійснені у мережі. Ці транзакції можуть включати різні види даних, від фінансових операцій, як у випадку з криптовалютами, до контрактів чи інших важливих інформацій [2].

Будь-який блок складається з трьох основних частин:

- Заголовок блоку, який містить метадані, такі як хеш попереднього блоку, часову мітку, хеш самого блоку, і, у випадку блокчейнів, що використовують Proof of Work/Stake, цільовий хеш та nonce.
- Список транзакцій, які були здійснені у мережі і включені до блоку після процесу верифікації.
- Унікальний ідентифікатор або хеш, який виникає в результаті криптографічного хешування вмісту блоку.

Хеш попереднього блоку забезпечує цілісність ланцюга, оскільки будь-яка зміна в одному блоку змусить змінити хеші у всіх наступних блоках, роблячи маніпуляції практично неможливими. Ця структура забезпечує безпеку та незмінність даних у блокчейні. Також це продемонстровано на рис. 1.1.

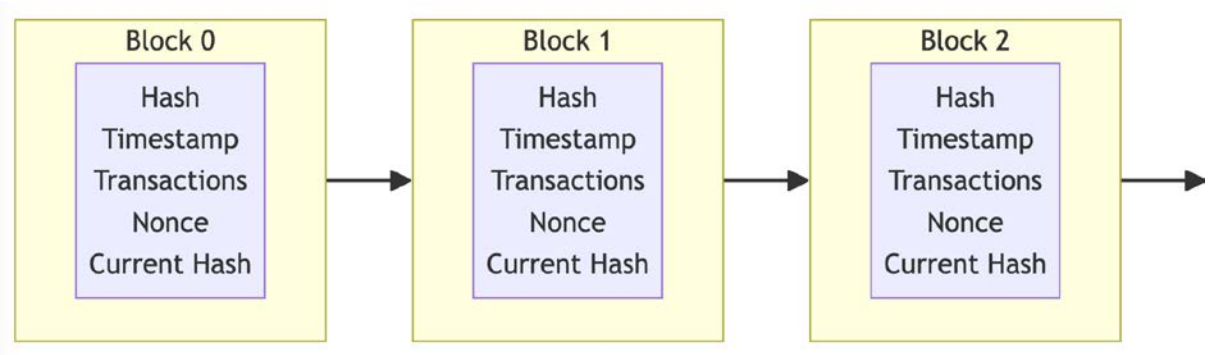

Рисунок 1.1 - Структура блоку в блокчейні

Вузли (nodes) є основними компонентами мережі блокчейну. Вони можуть бути розглянуті як окремі комп'ютери або сервери, які зберігають копію блокчейну і у деяких випадках беруть участь у процесі верифікації та затвердження транзакцій. Вузли гарантують децентралізацію мережі, оскільки вони розташовані по всьому світу і належать різним особам або організаціям. Ці вузли працюють разом, щоб підтримувати цілісність та прозорість блокчейну, перевіряючи нові транзакції та блоки через процес консенсусу.

Майнери є спеціалізованими вузлами в мережі, які беруть участь у процесі майнінгу - вони використовують обчислювальні ресурси для розв'язання складних математичних завдань, необхідних для додавання нових блоків до блокчейну. В мережах, що використовують Proof of Work, такі як Bitcoin, майнінг є способом досягнення консенсусу та забезпечення безпеки мережі. Майнери отримують винагороду у вигляді криптовалюти за кожен успішно доданий блок, що стимулює їх участь у мережі.

Кожен з цих елементів відіграє ключову роль у функціонуванні блокчейну. Блоки забезпечують зберігання та інтеграцію даних, вузли підтримують стабільність та децентралізацію мережі, а майнери вносять свій вклад у обробку транзакцій та забезпечення безпеки. Разом вони створюють ефективну, безпечну та прозору систему, яка лежить в основі блокчейн технології.

Знаючи основні компоненти блокчейну, можемо описати процес взаємодії між користувачем, вузлом та майнером у блокчейні є ключовим для розуміння того, як

саме функціонує ця технологія. Ця взаємодія відбувається у декілька етапів, кожен з яких важливий для підтримки цілісності та безпеки мережі. Детальна схема зображена на рис. 1.2.

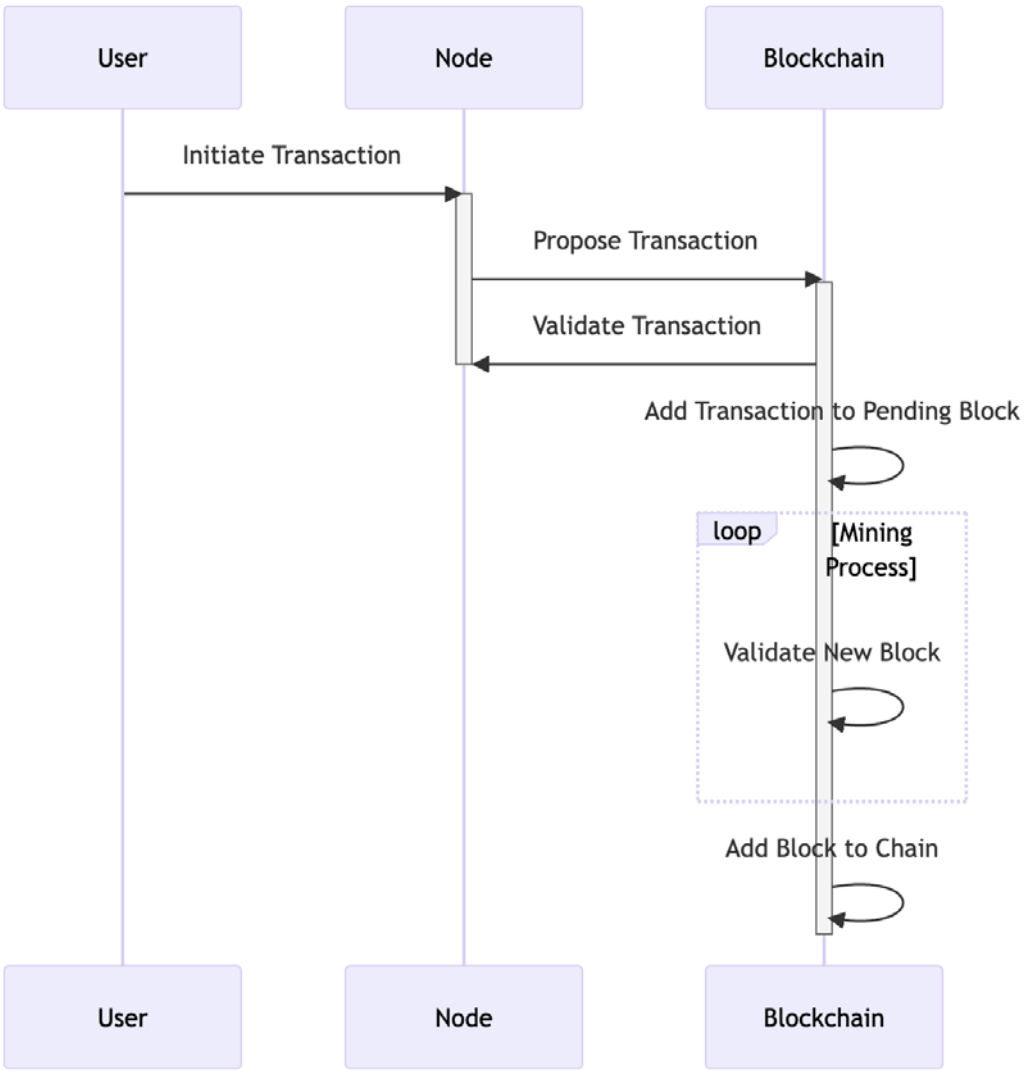

Рисунок 1.2 - Процес взаємодії користувача з блокчейном

- **Ініціація Транзакції Користувачем**

Усе починається, коли користувач блокчейну ініціює транзакцію. Це може бути, наприклад, передача криптовалюти, виконання смарт-контракту чи запис даних до блокчейну. Користувач використовує свій приватний ключ для підпису транзакції, що забезпечує її автентичність та безпеку. Після цього транзакція відправляється у мережу блокчейну.

- **Перевірка та Поширення Транзакції Вузлами**

Коли транзакція потрапляє в мережу, вона спочатку надходить до вузлів. Вузли блокчейну перевіряють транзакцію на відповідність правилам мережі, включаючи перевірку цифрового підпису. Після успішної верифікації транзакція додається до пулу непідтверджених транзакцій, чекаючи на включення до наступного блоку. Важливо, що інформація про транзакцію розповсюджується між усіма вузлами мережі, забезпечуючи її децентралізацію.

- **Формування Блоку Майнерами**

Майнери відіграють ключову роль у процесі додавання нових транзакцій до блокчейну. Вони вибирають транзакції з пулу непідтверджених транзакцій та формують з них новий блок. У блокчейнах, які використовують Proof of Work, майнери змагаються між собою, щоб знайти вірний хеш для нового блоку, виконуючи складні обчислення. Майнер, який першим вирішує цю задачу, отримує право додати блок до ланцюга і отримує за це винагороду.

- **Додавання Блоку до Ланцюга та Підтвердження Транзакції**

Коли новий блок формується, він відправляється на всі вузли мережі для підтвердження. Вузли перевіряють блок і, якщо він відповідає усім правилам, додають його до своїх копій блокчейну. З цього моменту транзакції, які містяться в блоку, вважаються підтвердженими.

Ця взаємодія між користувачами, вузлами та майнерами є фундаментом для забезпечення безпеки, прозорості та ефективності блокчейн мереж. Кожен елемент системи відіграє свою роль, сприяючи безперервному та надійному обміну даними в мережі.

1.4 Механізми Консенсусу: Proof of Work проти Proof of Stake

Proof of Work (PoW), або доказ виконання роботи, є одним з основних механізмів консенсусу, що використовується в блокчейн технологіях, зокрема у таких як Bitcoin. Цей механізм був створений для запобігання кібератакам, таким як подвійне витрачання та Sybil-атаки, і забезпечення безпеки та стабільності мережі. Ось як він працює:

1. **Формування блоку:** майнер збирає транзакції з пулу непідтверджених транзакцій і формує новий блок.

2. **Обчислення хешу:** щоб блок був доданий до ланцюга, майнер повинен знайти вірний хеш, який відповідає певній умові (наприклад, хеш повинен починатися з певної кількості нулів). Цей процес відомий як "виконання роботи" (mining).

3. **Використання обчислювальної потужності:** знаходження вірного хешу вимагає значних обчислювальних зусиль, оскільки це досягається методом проб і помилок. Майнери використовують потужні комп'ютери для виконання мільйонів або навіть мільярдів обчислень за секунду.

4. **Досягнення консенсусу:** перший майнер, який знаходить вірний хеш, розповсюджує блок у мережі. Інші вузли мережі перевіряють блок (включно з вірністю хешу) і додають його до своїх копій блокчейну.

5. **Винагорода за майнінг:** майнер, який успішно додає блок, отримує винагороду у вигляді криптовалюти (наприклад, новостворені біткойни у випадку з Bitcoin) та транзакційні комісії.

Детальна схема всього процесу зображена на рис. 1.3.

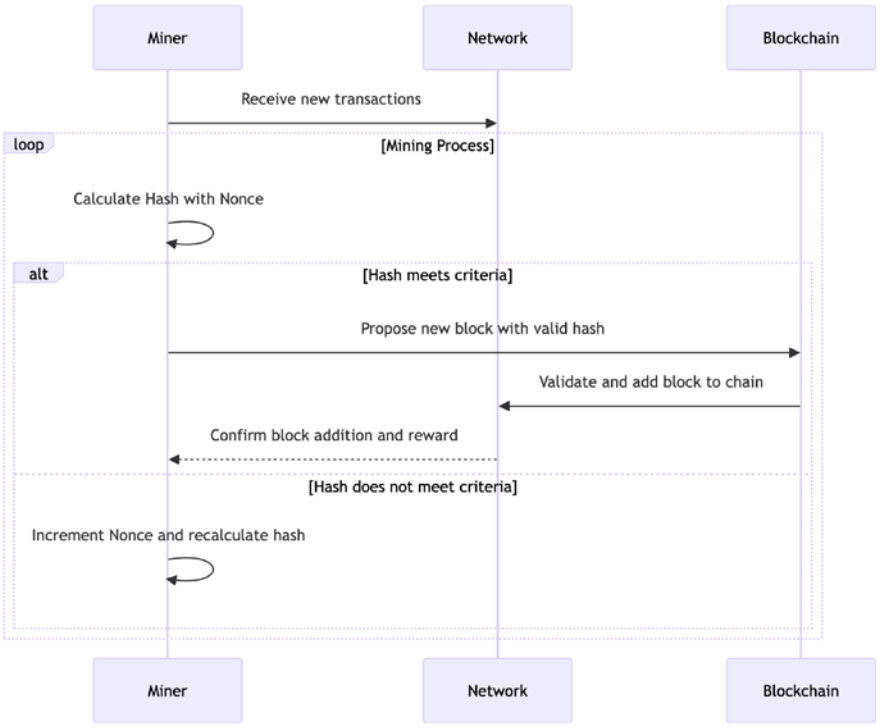

Рисунок 1.3 – Процес створення блоку в PoW

Одним з найбільших недоліків PoW є його високе споживання енергії. Майнінг вимагає великих обчислювальних потужностей, що призводить до значного споживання електроенергії. Це створює екологічні проблеми і піддає PoW критиці з точки зору сталого розвитку.

Незважаючи на критику, PoW залишається одним з найбільш надійних механізмів консенсусу. Висока вартість майнінгу обмежує можливість атак, оскільки потенційний нападник повинен буде витратити колосальні ресурси для контролю більшості обчислювальної потужності мережі, що робить такі атаки непрактичними.

Підсумовуючи, PoW є ключовим елементом безпеки в таких блокчейн мережах, як Bitcoin. Він забезпечує безпеку та цілісність даних, хоча і потребує значних обчислювальних та енергетичних ресурсів.

Proof of Stake (PoS), або доказ володіння, представляє собою альтернативний механізм консенсусу до Proof of Work, який зосереджується на зниженні енерговитрат та підвищенні ефективності процесу валідації транзакцій у блокчейні.

Відмінність PoS полягає у способі вибору валідаторів (учасників, які додають нові блоки до ланцюга) та способі забезпечення безпеки мережі. Також розглянемо алгоритм PoS на рис. 1.4.

У системах PoS валідатори блоків вибираються на основі кількості монет або токенів, які вони тримають і "заморожують" як заставу. Цей процес називається "стейкінгом". Чим більше монет учасник заморожує, тим більше шансів у нього стати валідатором наступного блоку. Валідатори вибираються за допомогою різних алгоритмів, залежно від конкретної імплементації PoS, але загальна ідея полягає в тому, що учасники з більшою часткою володіння мають більший вплив на мережу.

Однією з ключових переваг PoS є значне зниження енерговитрат порівняно з PoW, оскільки валідаторам не потрібно використовувати велику обчислювальну потужність для вирішення складних математичних задач. Замість цього, безпека мережі забезпечується економічними стимулами: валідатори, які діють нечесно або намагаються маніпулювати системою, ризикують втратити свої "заморожені" монети.

В PoS валідатори отримують винагороду за додавання блоків, яка може складатися як з новостворених монет, так і з транзакційних комісій. Це створює стимул для учасників тримати свої монети та підтримувати мережу, сприяючи її стабільності та безпеці.

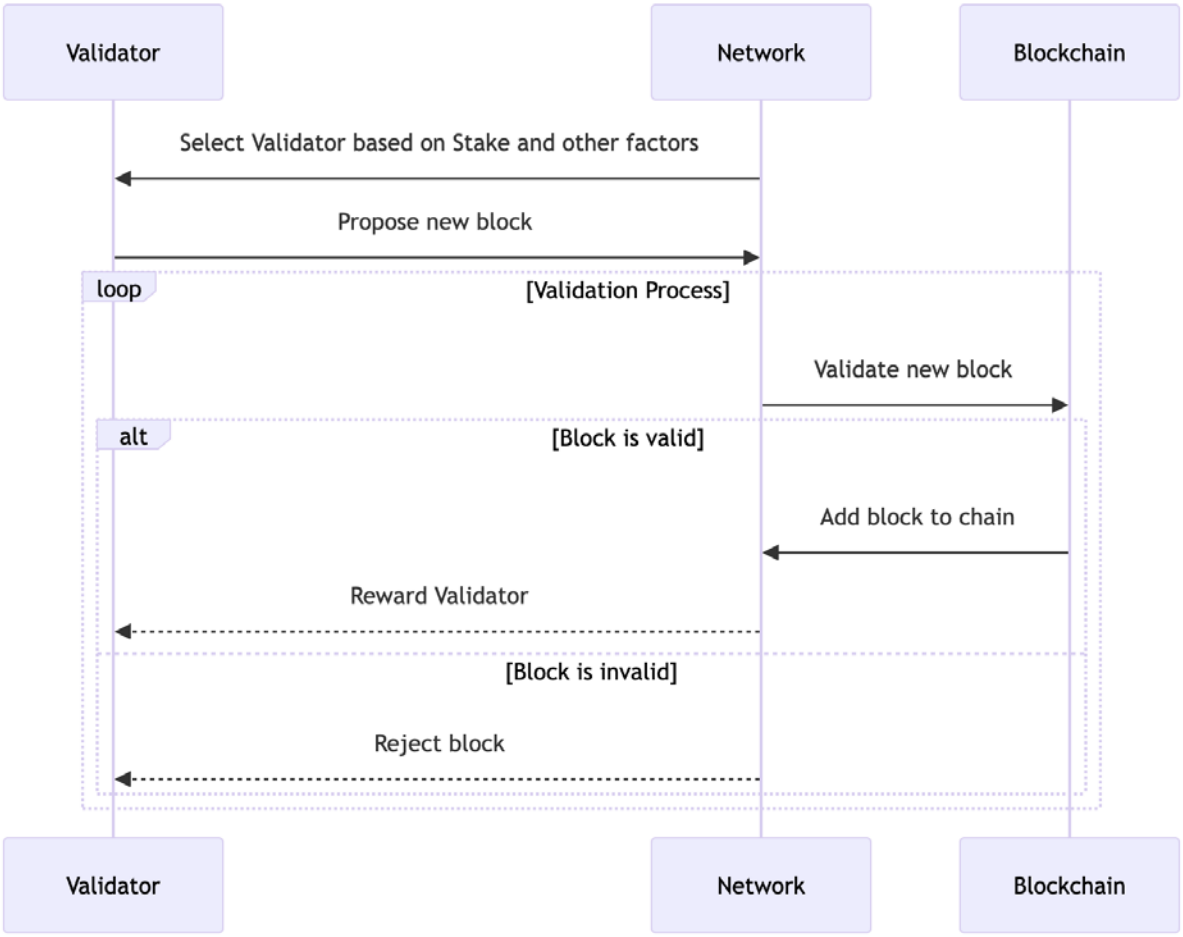

Рисунок 1.4 – Процес створення блоку в PoS

Такий підхід дозволяє створити більш стійку та екологічно чисту систему, яка може ефективно масштабуватися. Однак, PoS також має свої виклики та потенційні проблеми, такі як ризик централізації у випадку, коли великі власники монет мають значний вплив на мережу. З цієї причини, багато сучасних блокчейнів шукають шляхи поєднання переваг обох систем, PoW та PoS, для створення більш збалансованої та безпечної мережі.

PoW і PoS мають різні підходи до забезпечення безпеки та досягнення консенсусу в блокчейні. PoW вважається більш надійним з точки зору безпеки, але водночас є досить енерговитратним. Натомість, PoS пропонує екологічніший і потенційно більш масштабований варіант, хоча деякі експерти вказують на потенційні ризики, пов'язані з концентрацією влади у руках великих власників токенів.

Обидва механізми мають свої переваги та недоліки, і вибір між ними часто залежить від конкретних цілей та вимог блокчейн проекту. Останнім часом спостерігається тенденція до розвитку та впровадження гібридних систем, які намагаються поєднати переваги обох механізмів.

PoS, що використовується в Ethereum 2.0, пропонує альтернативний підхід, де валідатори визначаються на основі кількості вкладених коштів, що значно знижує енерговитрати. Такий підхід покращує екологічні аспекти блокчейну, однак може спричинити концентрацію влади серед великих вкладників. У підсумку, вибір механізму консенсусу значно впливає на безпеку, прозорість та ефективність функціонування блокчейн систем, вимагаючи від забудовників зваженого підходу для забезпечення оптимального балансу між цими ключовими характеристиками.

У контексті безпеки та прозорості блокчейну, порівняльний аналіз механізмів консенсусу Proof of Work (PoW) та Proof of Stake (PoS) виявляє їхні ключові відмінності та вплив на загальну структуру мережі. PoW, як основа Bitcoin, вимагає значних обчислювальних ресурсів для валідації транзакцій, що забезпечує високий рівень безпеки через складність математичних завдань. Однак, цей підхід пов'язаний з великими енергетичними витратами та потенційними екологічними ризиками.

1.5 Безпека та прозорість блокчейну

Криптографія відіграє вирішальну роль у забезпеченні безпеки та прозорості блокчейн технології. Це наука про зашифровування та дешифрування інформації, яка у випадку блокчейну використовується для забезпечення конфіденційності, цілісності та невіддільності даних. Криптографія дозволяє користувачам блокчейну безпечно обмінюватися даними без потреби в довірі до третьої сторони.

Основні алгоритми криптографії в блокчейні:

- **Хеш-функції:** Хеш-функції є ключовою складовою блокчейну. Вони перетворюють вхідні дані будь-якого розміру в рядок фіксованої довжини, який служить унікальним цифровим відбитком цих даних. Важливою характеристикою хеш-функцій є те, що вони є односторонніми, тобто неможливо відновити вихідні дані, знаючи лише їх хеш. Біткойн, наприклад, використовує SHA-256, одну з найпопулярніших хеш-функцій.
- **Асиметрична криптографія:** Асиметрична криптографія, або криптографія з відкритим ключем, використовує пару ключів - приватний та публічний. Приватний ключ залишається у конфіденційності у власника, тоді як публічний ключ може бути відкритим для всіх. Це дозволяє користувачам створювати цифровий підпис, використовуючи свій приватний ключ, який може бути перевірений будь-ким за допомогою публічного ключа.
- **Цифрові Підписи:** Цифрові підписи забезпечують автентичність та невіддільність транзакцій у блокчейні. Коли користувач підписує транзакцію своїм приватним ключем, він гарантує, що транзакція була ініційована ним, і цей підпис може бути підтверджений будь-ким, хто має його публічний ключ.

Також розглянемо основні алгоритми, які використовуються у найбільших блокчейнах. Розглянемо всі алгоритми на табл. 1.1.

Таблиця 1.1 - Порівняння алгоритмів криптографії у різних блокчейнах

Алгоритм	**Блокчейн**	**Опис**	**Застосування**
SHA-256	Bitcoin	Хеш-функція, що створює унікальний цифровий відбиток даних.	Використовується для майнінгу та створення біткойн-адрес. Гарантує цілісність транзакцій та унікальність даних.
ECDSA	Ethereum	Алгоритм асиметричної криптографії з відкритим ключем.	Використовується для створення цифрових підписів, забезпечуючи автентичність транзакцій.
Scrypt	Litecoin	Хеш-функція, орієнтована на великий обсяг пам'яті.	Використовується для майнінгу, дозволяючи ширшому колу користувачів брати участь у процесі та сприяючи децентралізації.

Ці криптографічні інструменти разом створюють систему, де даними можна обмінюватися безпечно і прозоро. Хеш-функції забезпечують цілісність даних усередині блокчейну, переконуючись, що будь-які зміни в даних будуть легко виявлені. Асиметрична криптографія та цифрові підписи забезпечують, що транзакції можуть бути безпечно здійснені та верифіковані у мережі без потреби в централізованому посереднику.

Завдяки цим механізмам криптографії, блокчейн забезпечує високий рівень безпеки та прозорості, роблячи його ідеальним для застосувань, де цінується надійність і незмінність даних.

Блокчейн технологія відзначається своєю здатністю до забезпечення цілісності даних та прозорості, що є важливими аспектами для будь-якої системи обміну інформацією або цінностями [3].

Цілісність даних в блокчейні забезпечується завдяки кільком основним факторам. Криптографічне хешування є одним з них, дозволяючи кожному блоку в блокчейні містити унікальний хеш попереднього блоку, що створює нерозривний ланцюг. Ця особливість гарантує, що будь-які зміни в даних будуть легко виявлені. Розподілене зберігання даних також вносить свій вклад у цілісність, оскільки кожен вузол у мережі зберігає копію всієї блокчейн бази даних. Це створює систему, де маніпулювати або втрачати дані без виявлення майже неможливо. Протоколи консенсусу, такі як Proof of Work або Proof of Stake, забезпечують додатковий рівень перевірки, гарантуючи, що всі вузли у мережі погоджуються на дійсність нових блоків перед їх додаванням до ланцюга.

Що стосується прозорості, блокчейн дозволяє будь-кому переглядати транзакції та блоки, особливо в публічних мережах. Це означає, що діяльність у мережі може бути перевірена і відстежена ким завгодно, забезпечуючи високий рівень прозорості. Легкість відстеження транзакцій і взаємодій в мережі робить блокчейн ідеальним для систем, де потрібний високий рівень аудиту та відстежуваності, таких як фінансові послуги, ланцюги постачання, голосування та багато інших.

Таким чином, блокчейн не тільки забезпечує безпеку та надійність системи через цілісність даних, але й відкриває нові можливості для створення прозорих, децентралізованих і автоматизованих рішень для різних сфер діяльності.

1.6 Аналіз сучасного стану блокчейну

Сучасний стан технології блокчейну характеризується швидким розвитком і зростанням, охоплюючи не тільки фінансові застосування, але й багато інших сфер діяльності. З моменту свого винайдення як основи для Bitcoin, блокчейн еволюціонував у багатофункціональну технологію з широким спектром застосувань.

Однією з ключових тенденцій у розвитку блокчейну є відхід від першого покоління блокчейнів, зосереджених переважно на криптовалютах, до другого і третього поколінь, які включають смарт-контракти, децентралізовані фінансові послуги (DeFi) та децентралізовані автономні організації (DAO). Це розширення можливостей відкриває нові горизонти для інновацій у сферах, таких як цифрове мистецтво (через NFT), медіа, охорона здоров'я, логістика та багато інших [3].

Прозорість і безпека блокчейну продовжують привертати увагу не тільки стартапів, але й великих корпорацій та урядових структур, що досліджують цю технологію для підвищення ефективності та зниження ризиків у своїх операціях. Наприклад, використання блокчейну для слідкування ланцюгів постачання дозволяє забезпечити прозорість та підвищити довіру між споживачами і постачальниками.

Технологічний прогрес у розвитку блокчейну також включає покращення шкальованості та зниження енерговитрат. Інновації, такі як шардінг (розподіл даних між різними вузлами для підвищення продуктивності мережі) та перехід Ethereum з Proof of Work на Proof of Stake у рамках його оновлення Ethereum 2.0, свідчать про зусилля спільноти зробити блокчейн більш стійким та екологічно чистим.

Сучасний розвиток блокчейну також відкриває широкі можливості для його застосування в різноманітних сферах, дозволяючи вирішувати сучасні проблеми з високим рівнем ефективності та безпеки.

Аукціони та Торги

Блокчейн може бути використаний для створення прозорих та безпечних платформ для проведення аукціонів та торгів. Завдяки незмінності даних та децентралізації, учасники можуть бути впевнені в чесності та прозорості процесу, а також в неможливості маніпуляцій з боку організаторів або третіх сторін.

Вибори та Голосування

Однією з найбільш обговорюваних можливостей блокчейну є його використання для організації виборів та голосувань. Блокчейн може забезпечити безпеку, анонімність та незмінність голосів, значно знижуючи ризики шахрайства та підвищуючи довіру до виборчих процесів.

Банкінг та Фінансові Операції

У фінансовому секторі блокчейн пропонує нові можливості для проведення транзакцій, забезпечення кредитів та управління активами. Він може використовуватися для створення більш ефективних, безпечних та прозорих фінансових систем, знижуючи витрати та спрощуючи процеси, особливо в міжнародних операціях.

Лотереї

Блокчейн також може бути застосований для створення прозорих та справедливих систем лотерей. Завдяки криптографічним гарантіям та децентралізації, учасники можуть бути впевнені в чесності розіграшів та правильному розподілі виграшів.

У загальному, блокчейн демонструє свою спроможність до реалізації широкого спектру сучасних рішень, пропонуючи новітні підходи до вирішення проблем в різних сферах. Від фінансів до громадського управління, від торгівлі до соціальних ініціатив, блокчейн стає все більш важливим інструментом в сучасному цифровому світі.

Крім того, інтеграція блокчейну з іншими передовими технологіями, такими як штучний інтелект (ШІ) та Інтернет речей (IoT), відкриває нові можливості для

створення комплексних, інтелектуальних систем, здатних самостійно реагувати на зміни у навколишньому середовищі та приймати рішення на основі даних з блокчейну.

В цілому, сучасний стан блокчейн технології характеризується динамічним розвитком, зростанням застосувань у різних галузях та постійними інноваціями, що спрямовані на підвищення ефективності, безпеки та доступності цієї технології.

Розглянувши стан технології блокчейну, легко зрозуміти що швидкий розвиток та зростання цієї технології відкривають нові можливості у найрізноманітніших сферах, від фінансів та логістики до виборів та цифрового мистецтва. Такий широкий спектр застосувань і постійні інновації вказують на потенціал блокчейну як революційної технології. Однак, поряд з цими перспективами, важливо також усвідомлювати ряд викликів та обмежень, які стоять перед блокчейн технологіями.

У сучасному стані блокчейн технології існує низка викликів та обмежень, які важливо враховувати для повного розуміння потенціалу та обмежень цієї інноваційної системи. Однією з основних проблем є масштабованість, адже з ростом кількості користувачів та транзакцій, деякі блокчейни, особливо ті, які використовують механізм Proof of Work, можуть стикатися з уповільненням обробки транзакцій і збільшенням часу відгуку.

Це безпосередньо пов'язано з іншою значною проблемою - споживанням енергії. Висока енерговитратність, особливо в системах з Proof of Work, як у Bitcoin, викликає занепокоєння щодо екологічної стійкості цих мереж. Велике споживання електроенергії для майнінгу ставить під сумнів довгострокову ефективність та прийнятність цих систем в умовах глобальної екологічної кризи.

Ці виклики включають питання масштабованості, енерговитратності, проблеми централізації влади та контролю, а також забезпечення приватності та анонімності. Також вони стикаються з регуляторними викликами, що можуть впливати на їхнє широке прийняття та розвиток.

Крім того, виникають питання централізації та контролю. Наприклад, у мережах, де великі майнінгові пули домінують, виникає ризик централізації влади, що може негативно вплинути на децентралізований характер блокчейну. Це також стосується зберігання та контролю приватних ключів, які є важливим елементом безпеки в блокчейн системах.

Приватність та анонімність у блокчейні - ще один аспект, який вимагає уваги. Забезпечення приватності користувачів при збереженні прозорості та відкритості блокчейну є складним завданням, яке потребує ретельного балансування між різними інтересами.

Окремо стоять питання регуляторного контролю та законодавчих вимог, які досі залишаються невизначеними в багатьох регіонах. Невизначеність у правовому полі може стримувати розвиток та широке прийняття блокчейну, оскільки потенційні користувачі та розробники можуть бути невпевнені щодо майбутніх регуляторних змін.

В цілому, блокчейн стоїть перед низкою викликів, які потребують інноваційних рішень та подальших досліджень. Розвиток технологій та адаптація до нових вимог і очікувань є ключовими для подальшого розвитку та успішного впровадження блокчейн технологій.

2 ВИКОРИСТАННЯ БЛОКЧЕЙНУ У СФЕРІ ФІНАНСІВ

2.1 Блокчейн у фінансовій сфері

Блокчейн пропонує новаторські можливості у фінансовому секторі, які перетворюють традиційні підходи та відкривають нові горизонти для розвитку. Від децентралізованих фінансових сервісів до управління активами, блокчейн вносить революційні зміни у спосіб, яким ми взаємодіємо з фінансовими системами.

У сфері децентралізованих фінансових сервісів (DeFi), наприклад, блокчейн дозволяє створювати платформи для пірингових фінансових операцій. Децентралізовані біржі (DEX), такі як Uniswap, використовують смарт-контракти для автоматизації обміну криптовалют, усуваючи необхідність централізованого посередника. Формула ціноутворення Uniswap, яка враховує кількість двох різних токенів у пулі ліквідності, дозволяє підтримувати стабільність та ефективність торгів.

Токенізація активів, як ще один приклад, перетворює традиційні активи на цифрові токени, що забезпечує легший доступ до різних ринків. Платформи для токенізації, такі як RealT, дозволяють користувачам купувати частки нерухомості у формі токенів, роблячи інвестиції більш доступними та ліквідними. Кожен токен представляє частку власності на нерухомість, забезпечуючи прозорість та ефективність транзакцій.

Крос-бордер платежі та перекази стають швидшими та ефективнішими завдяки використанню блокчейну. Ripple (XRP) є одним з прикладів, який використовує свою криптовалюту для спрощення міжнародних банківських транзакцій, зменшуючи час та витрати порівняно з традиційними системами. XRP діє як міст між різними валютами, забезпечуючи швидке та зручне конвертування.

Крім цього, блокчейн також знаходить застосування у ланцюгах постачань у фінансовій сфері. Проекти, такі як IBM Blockchain, використовують блокчейн для забезпечення прозорості ланцюгів постачань. Завдяки блокчейну, кожна транзакція чи переміщення активів фіксується, забезпечуючи точне відстеження фінансових потоків.

Ці приклади вказують на зростаюче впровадження блокчейну у фінансовій сфері, відкриваючи нові шляхи для інновацій та ефективності [10]. Вони свідчать про розширення можливостей блокчейну за межі простого обміну криптовалютами та вказують на його потенціал як на могутню інструментальну платформу для сучасного фінансового світу.

Продовжуючи тему застосувань блокчейну у фінансовій сфері, важливим аспектом є розуміння відмінностей між централізованими та децентралізованими біржами, а також розгляд конкретних прикладів їх використання.

Централізовані Біржі

Централізовані біржі (CEX) є традиційними платформами для торгівлі активами, включаючи криптовалюти. Такі платформи, як Coinbase або Binance, контролюються однією компанією та забезпечують інтерфейс для купівлі, продажу та трейдінгу різноманітних криптовалют. Вони виступають як посередники між покупцями та продавцями, надаючи платформу для виконання торгових операцій. Централізовані біржі часто надають додаткові послуги, такі як кастодіальні рішення, маржинальну торгівлю та інші фінансові інструменти.

Основними перевагами централізованих бірж є висока швидкість транзакцій, зручність інтерфейсу користувача та наявність регуляторного нагляду. Однак, вони також стикаються з критикою через питання безпеки та приватності, оскільки централізація може зробити їх вразливими для хакерських атак.

Децентралізовані Біржі

Навпаки, децентралізовані біржі (DEX), такі як Uniswap або SushiSwap, пропонують альтернативний підхід до торгівлі криптовалютами. У DEX немає центрального органу, який би зберігав кошти користувачів або контролював торгівлю.

Головною перевагою DEX є вищий рівень безпеки та приватності, оскільки користувачі контролюють свої приватні ключі та не передають їх третім сторонам. Крім того, вони забезпечують більшу децентралізацію та відсутність однієї точки відмови. Проте, децентралізовані біржі часто мають менш інтуїтивні інтерфейси та можуть пропонувати менший вибір торгових інструментів порівняно з централізованими біржами. Розглянемо різницю між цими підходами на рис. 2.1.

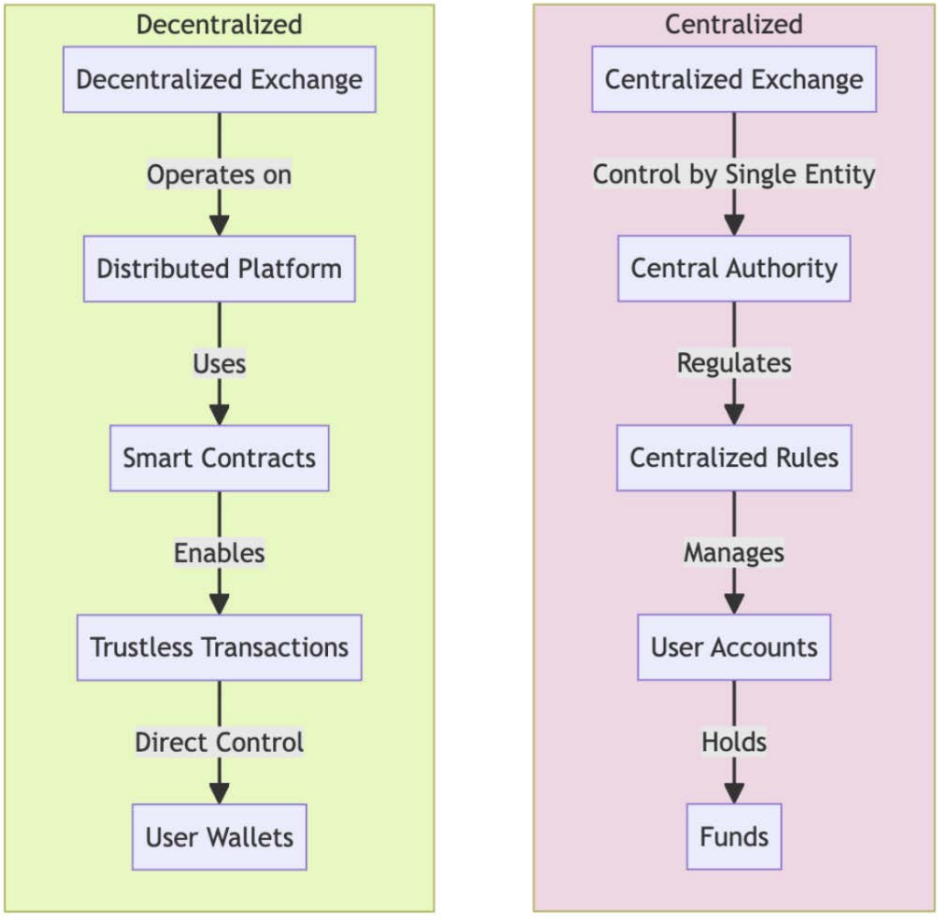

Рисунок 2.1 - Порівняння централізованого та децентралізованого підходу

Розуміння різниці між централізованими та децентралізованими біржами є ключовим для вибору відповідної платформи залежно від потреб користувача. Кожна з цих моделей має свої переваги та недоліки, і вибір залежить від таких факторів, як потреба у безпеці, швидкість транзакцій, регуляторні вимоги та зручність користування. Ми ж своєю чергою, сконцетруємось саме на децентралізованих рішеннях.

Децентралізовані фінанси, або DeFi, є однією з найбільш інноваційних та перспективних областей застосування блокчейну. DeFi представляє собою екосистему фінансових інструментів та сервісів, які функціонують на основі блокчейн технологій, зокрема використовуючи смарт-контракти на платформах, таких як Ethereum. Ця сфера включає в себе різноманітні фінансові послуги, такі як позики, страхування, деривативи, обмін активами та інвестиційні платформи.

Однією з ключових особливостей DeFi є повна децентралізація, що означає відсутність центрального органу, який контролює систему. Це створює систему, де відносини між сторонами регулюються кодом смарт-контрактів, а не централізованою інституцією, як у традиційних фінансових системах.

Особливості реалізації DeFi включають використання технологій блокчейну для створення прозорих, відкритих для перевірки та безпечних фінансових продуктів. Це включає автоматизацію через смарт-контракти, які забезпечують виконання погоджених умов без необхідності втручання зовнішніх посередників. Це дозволяє користувачам безпосередньо взаємодіяти один з одним, знижуючи витрати та збільшуючи ефективність.

DeFi також характеризується сильним співтовариством та культурою співпраці. Розробники, користувачі та інвестори активно спілкуються у різних мережах, таких як форуми, соціальні мережі та конференції, щоб обговорювати ідеї, розробки та покращення. Це сприяє швидкому розвитку та інноваціям у сфері DeFi.

Децентралізовані фінанси також пропонують нові підходи до вирішення традиційних фінансових задач. Наприклад, використання DeFi дозволяє

здійснювати позики та кредитування без необхідності банків як посередників. Також DeFi відкриває можливості для створення децентралізованих страхових продуктів та інвестиційних інструментів, які можуть бути доступні широкому колу користувачів по всьому світу.

DeFi є справжнім втіленням ідей децентралізації та фінансової інклюзії, пропонуючи новітні рішення для старих проблем і створюючи безліч можливостей для інновацій у фінансовому секторі.

Тож тепер ми можемо виявити як ключові переваги, так і потенційні недоліки цього підходу, порівнюючи його з традиційними фінансовими системами.

Переваги DeFi

1. **Децентралізація:** Однією з головних переваг DeFi є відсутність централізованого контролю, що знижує ризик збоїв, пов'язаних з однією точкою відмови, та зменшує залежність від традиційних фінансових інституцій.

2. **Фінансова інклюзія:** DeFi відкриває доступ до фінансових послуг для ширшого кола людей, зокрема для тих, хто традиційно виключений з фінансової системи.

3. **Прозорість та автоматизація:** Смарт-контракти пропонують високий рівень прозорості та автоматизують виконання фінансових угод, забезпечуючи ефективність та надійність.

4. **Інноваційні фінансові продукти:** DeFi стимулює розвиток нових фінансових інструментів, які можуть бути більш гнучкими та інноваційними, ніж у традиційному банкінгу.

Недоліки DeFi

1. **Високий ризик втрати коштів:** оскільки DeFi все ще є відносно новою сферою, існує ризик втрати коштів через недоліки в смарт-контрактах, хакерські атаки або волатильність ринку.

2. **Комплексність та технічні бар'єри:** для звичайних користувачів DeFi може здаватися складним через технічну природу блокчейну та криптовалют.

3. **Відсутність регуляції:** відсутність чіткого регулювання у сфері DeFi може спричинити правову невизначеність та відсутність захисту для інвесторів.

4. **Складнощі у скалінгу:** хоча блокчейн пропонує багато переваг, існують технічні виклики, пов'язані зі скалінгом цих систем, щоб вони могли ефективно обробляти велику кількість транзакцій.

У підсумку, DeFi пропонує революційний підхід до фінансових послуг, що відрізняється від традиційних методів значною гнучкістю, доступністю та інноваційністю. Однак, як і будь-яка нова технологія, вона має свої виклики та обмеження, які потребують ретельного вивчення та вдосконалення.

Також розглянемо основні компоненти та послуги, які формують цю екосистему. DeFi не обмежується одним конкретним додатком або сервісом, а складається з цілого набору інструментів і продуктів, що разом створюють комплексне фінансове середовище.

Автоматизовані маркет-мейкери використовують алгоритми для забезпечення ліквідності в мережі DeFi. Наприклад, Uniswap використовує модель x * y = k для забезпечення ліквідності між парами токенів. Ця формула забезпечує, що загальний продукт двох запасів токенів залишається константою, що дозволяє автоматично визначати ціни на активи.

Децентралізовані платформи кредитування, такі як Compound або Aave, дозволяють користувачам брати або надавати позики безпосередньо через смарт-контракти. Ці платформи використовують складні алгоритми для автоматичного визначення процентних ставок на основі пропозиції та попиту на ринку.

DeFi також включає **децентралізовані страхові сервіси**, які забезпечують захист від різних ризиків, пов'язаних із криптовалютними операціями. Ці сервіси, такі як Nexus Mutual, використовують блокчейн для створення повністю прозорих страхових полісів, де умови захисту та виплати визначаються смарт-контрактами.

Токенізація активів в DeFi дозволяє конвертувати традиційні активи, такі як нерухомість або акції, у цифрові токени, які можна легко купувати, продавати або обмінювати на децентралізованих платформах. Це забезпечує більшу ліквідність та доступність для широкого кола інвесторів.

DAO - це організації, керовані смарт-контрактами, де рішення приймаються голосуванням учасників. Вони дозволяють демократично управляти проектами в екосистемі DeFi, надаючи учасникам можливість впливати на розвиток та управління проектами.

Кожен з цих компонентів відіграє ключову роль у формуванні екосистеми DeFi. Вони разом створюють багатошарову, інтегровану систему, яка пропонує новітні фінансові послуги, засновані на прозорості, децентралізації та автоматизації. Використання блокчейну та смарт-контрактів у цих сервісах розширює можливості традиційних фінансових систем, роблячи їх доступнішими, ефективнішими та безпечнішими.

Наявність децентралізованих страхових сервісів, токенізація традиційних активів та демократичне управління через DAO відкривають нові можливості для ефективного управління активами та ризиками. Це демонструє силу блокчейну як інструменту, що може змінити обличчя сучасних фінансів, надаючи користувачам більше контролю, прозорості та безпеки. DeFi, як інноваційна екосистема, не тільки відкриває двері для нових видів інвестицій та фінансових стратегій, але й сприяє створенню більш відкритого та інклюзивного фінансового майбутнього.

2.2 Криптовалюти та цифрові активи

В обговоренні криптовалют та цифрових активів неможливо оминути Bitcoin та Ethereum, які є двома найбільш значущими та впливовими криптовалютами на сучасному ринку. Ці цифрові валюти не лише стали піонерами у сфері блокчейн та криптовалют, але й продовжують формувати основу цієї швидкозростаючої індустрії [5].

Bitcoin, створений у 2009 році невідомою особою або групою під псевдонімом Satoshi Nakamoto, є першою криптовалютою та найбільш відомим прикладом використання блокчейн технології. Він був розроблений як децентралізована цифрова валюта для здійснення пірингових платежів без потреби у посередниках, таких як банки чи інші фінансові інститути. Центральною особливістю Bitcoin є його обмежена кількість – лише 21 мільйон монет, що забезпечує його захист від інфляції.

В той же час, **Ethereum** був запущений у 2015 році, представляє собою не лише криптовалюту (Ether), але й децентралізовану платформу, яка дозволяє розробникам створювати смарт-контракти та децентралізовані додатки (dApps). Це розширило можливості блокчейну, дозволивши йому використовуватися не тільки для фінансових транзакцій, але й для різноманітних інших застосувань, включаючи DeFi, NFTs (незамінні токени) та багато іншого.

Поза Bitcoin та Ethereum, існує множина інших криптовалют, кожна з яких пропонує унікальні характеристики та застосування. До таких валют відносяться Ripple (XRP), який спрощує міжнародні грошові перекази, Litecoin, створений як "срібло до золота Bitcoin", Cardano, який прагне створити більш стійку та безпечну блокчейн платформу, та багато інших. Кожна з цих криптовалют має свою унікальну вартість та призначення в екосистемі цифрових активів.

Ці криптовалюти та технології, які вони представляють, сформували основу сучасного цифрового фінансового світу. Вони продовжують розвиватися та

адаптуватися, пропонуючи нові можливості та виклики, які постійно трансформують цифровий ландшафт.

Від Bitcoin і Ethereum перейдемо до іншої важливої категорії в світі криптовалют – стейблкоїнів. Стейблкоїни були створені з метою вирішення проблеми волатильності, яка є характерною для більшості криптовалют, включаючи Bitcoin та Ethereum. Ця категорія цифрових активів покликана поєднувати найкращі характеристики криптовалют – безпеку, прозорість та швидкість транзакцій – зі стабільністю традиційних валют. Застосування зображено на рис. 2.2.

Однією з перших та найвідоміших стейблкоїнів є Tether (USDT), який був запущений у 2014 році. USDT прив'язаний до долара США у співвідношенні 1:1, що означає, що кожен токен USDT має бути підтриманий еквівалентною кількістю доларів США, яка зберігається в резервах. Цей підхід дозволяє забезпечити стабільність ціни стейблкоїну, незважаючи на коливання на криптовалютному ринку.

Інший важливий приклад стейблкоїну – USD Coin (USDC), який також прив'язаний до долара США і підтримує свою цінність у співвідношенні 1:1. USDC керується кількома фінансовими установами, які гарантують наявність доларового резерву, еквівалентного кількості випущених монет.

Спосіб дотримання ціни у 1 долар для цих стейблкоїнів заснований на постійному управлінні резервами. Це означає, що за кожен випущений токен USDT або USDC існує еквівалентна сума в доларах США, яка зберігається в резерві. Такий підхід забезпечує довіру інвесторів до стабільності цих криптовалют, роблячи їх популярним вибором для зберігання коштів та виконання транзакцій без ризику значної втрати вартості.

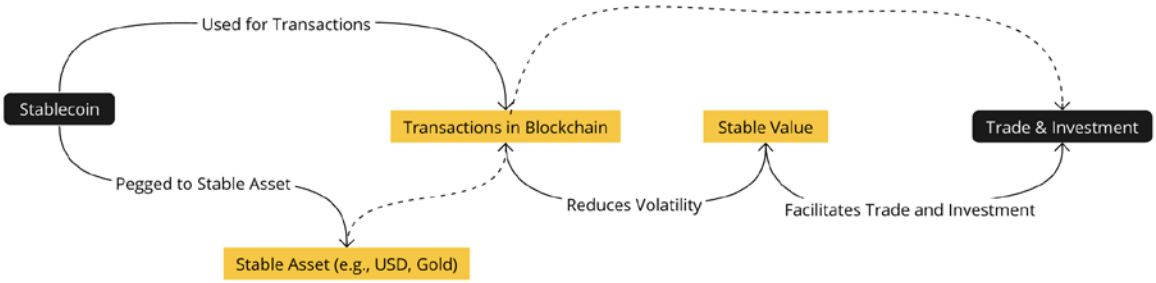

Рисунок 2.2 - Використання стейблкоїнів у DeFi

В контексті обговорення стейблкоїнів, важливо згадати про DAI – ще один значний гравець на ринку стейблкоїнів. DAI відрізняється від таких стейблкоїнів, як USDT та USDC, своїм унікальним підходом до підтримки стабільності ціни.

DAI – це стейблкоїн, який створений та управляється через децентралізовану платформу MakerDAO на блокчейні Ethereum. Він прив'язаний до долара США, але відрізняється від USDT та USDC тим, що його стабільність не забезпечується прямими резервами в доларах, а реалізується за допомогою складної системи смарт-контрактів та колатералізованих активів [4].

Механізм підтримки ціни **DAI** базується на колатералізації інших криптовалют, зокрема Ethereum. Користувачі можуть заблокувати свої криптовалюти в смарт-контрактах MakerDAO як заставу та отримати DAI в обмін. Ця система використовує комплексні алгоритми для забезпечення стабільності ціни DAI, регулюючи пропозицію та попит на стейблкоїн.

Основною перевагою DAI є його децентралізація та прозорість, оскільки стейблкоїн не залежить від одного центрального емітента або контролюючого органу. Це забезпечує додатковий рівень безпеки та довіри для користувачів, які шукають стабільну альтернативу традиційним валютам у світі криптовалют.

DAI став популярним вибором в екосистемі DeFi, де він використовується для торгівлі, позик та інших фінансових операцій, яким потрібна стабільність ціни без прямої прив'язки до традиційних фінансових систем. Використання DAI ілюструє,

як інновації у сфері блокчейну та криптовалют можуть пропонувати альтернативні підходи до забезпечення фінансової стабільності та ефективності.

Стейблкоїни, такі як USDT та USDC, DAI, стали фундаментальною частиною екосистеми криптовалют, пропонуючи місток між традиційними фінансами та світом криптовалют. Вони відіграють ключову роль у забезпеченні стабільності та надійності в операціях, пов'язаних із криптовалютами, особливо в контексті децентралізованих фінансів (DeFi).

У цьому розділі було проведено всебічний аналіз криптовалют та цифрових активів, з особливою увагою на Bitcoin, Ethereum та основні стейблкоїни. Bitcoin, як перша та найбільш відома криптовалюта, є піонером у цій сфері, визначаючи основні тенденції та напрямки розвитку ринку. Ethereum, з іншого боку, вніс значний вклад у розширення можливостей блокчейну за рахунок смарт-контрактів, що відкрило дорогу для численних інноваційних застосувань. Стейблкоїни, такі як USDT та DAI, забезпечують стабільність та надійність у світі криптовалют, пропонуючи валюти, прив'язані до традиційних активів, що знижує ризик волатильності.

Цей розділ демонструє, що криптовалюти та цифрові активи представляють собою складний і багатогранний сектор, який постійно розвивається та еволюціонує. Розуміння різних типів криптовалют та їхніх унікальних особливостей є критично важливим для глибокого аналізу цієї швидко змінюваної галузі. Від Bitcoin та Ethereum до стейблкоїнів, кожна криптовалюта вносить свій вклад у різноманітність та гнучкість ринку, що відкриває нові можливості для інвесторів, розробників та звичайних користувачів.

2.3 Блокчейн у традиційних фінансових системах

Блокчейн технологія знаходить все більше застосувань у традиційних фінансових системах, пропонуючи новітні рішення для банківської справи, страхування та управління активами. У сучасному світі, де цифрові технології стрімко проникають у всі сфери життя, фінансова індустрія не залишається осторонь від інновацій. Блокчейн, як революційна технологія, відкриває нові горизонти у способах здійснення фінансових операцій, пропонуючи безпрецедентний рівень безпеки, прозорості та ефективності.

Розглянемо основні аспекти інтеграції блокчейну в традиційні фінансові структури, включаючи вплив на банківську систему, страхування та управління активами. Особлива увага буде приділена аналізу випадків використання блокчейну у цих сферах, виявленню потенціалу для оптимізації існуючих процесів та визначенню можливих викликів і обмежень при імплементації цих технологій. Таким чином, цей розділ надасть глибоке розуміння того, як блокчейн може трансформувати традиційні фінансові системи, відкриваючи нові можливості для їх розвитку та модернізації.

У банківській сфері блокчейн використовується для оптимізації платіжних систем та забезпечення безпеки транзакцій [6]. Наприклад, використання блокчейну для міжбанківських розрахунків може суттєво скоротити час та витрати, пов'язані з переказами коштів, особливо у міжнародному масштабі. Також блокчейн може використовуватися для створення ефективніших систем для здійснення та відстеження кредитних операцій, зменшуючи ризики та підвищуючи прозорість.

В рамках розгляду використання блокчейну в традиційних фінансових системах, особливу увагу слід приділити ролі великих компаній, таких як PayPal, які вступають на ринок блокчейну. Ці компанії мотивовані прагненням інтегрувати інноваційні технології для підвищення ефективності своїх послуг, збільшення прозорості та забезпечення кращих умов для своїх користувачів.

Наприклад, PayPal, один з найбільших гравців у сфері цифрових платежів, нещодавно анонсував запуск свого стейблкоїна PYUSD, який відбувся 7 серпня 2023 року. Цей крок демонструє визнання потенціалу блокчейн технології у сфері фінансових послуг. PYUSD – це стейблкоїн, прив'язаний до долара США, що забезпечує стабільність та надійність для користувачів, які хочуть використовувати цифрові валюти без високої волатильності, характерної для традиційних криптовалют.

Великі компанії, такі як PayPal, заходять на ринок блокчейну з ряду причин. По-перше, це можливість збільшити свій вплив у сфері цифрових платежів та фінансових технологій. По-друге, інтеграція блокчейну дозволяє їм забезпечити більшу безпеку та ефективність транзакцій. Крім того, вони можуть пропонувати нові продукти та послуги, такі як криптовалютні транзакції та стейблкоїни, що відкриває нові ринки та можливості для росту.

У банківській справі, страхуванні та управлінні активами, використання блокчейну може забезпечити більшу автоматизацію процесів, скорочення витрат, підвищення прозорості операцій та поліпшення умов взаємодії з клієнтами. Це включає все, від упровадження смарт-контрактів для автоматичного врегулювання страхових виплат до використання блокчейну для підтримки та відстеження різних типів активів у сфері управління активами. В результаті, великі компанії можуть не тільки оптимізувати свої внутрішні процеси, але й пропонувати своїм клієнтам інноваційні та безпечні фінансові рішення.

У сфері страхування блокчейн може внести вагомий вклад у підвищення ефективності та прозорості процесів. Використання блокчейну для страхових полісів та клеймів може допомогти автоматизувати виплати та скоротити можливість шахрайства. Це також дозволяє страховикам ефективніше управляти ризиками та забезпечувати більш точну оцінку ризиків на основі надійних даних.

Управління активами з використанням блокчейну відкриває нові можливості для автоматизації та зниження витрат. Це включає в себе токенізацію активів, що

дозволяє розбивати великі активи, такі як нерухомість або твори мистецтва, на менші частки, які можуть бути легко куплені та продані. Такий підхід може зробити інвестиції доступнішими та ліквіднішими. Також ця технологія дозволяє забезпечити більшу прозорість та ефективність у веденні обліку та аудиті інвестиційних портфелів.

Visa, як один з лідерів у галузі глобальних платіжних систем, розширила свої можливості використання стабільних монет, інтегрувавши блокчейн Solana для проведення платежів [9]. Цей крок був здійснений у рамках пілотної програми та відображає потенціал Solana у забезпеченні швидких, масштабованих та економічно ефективних транзакцій, що є важливим для платіжних компаній. Особливостями Solana, які роблять її привабливою для платежів, є висока пропускна спроможність, низькі та передбачувані транзакційні витрати, а також спроможність обробки транзакцій паралельно, що забезпечує ефективність мережі.

Цей крок з боку Visa свідчить про визнання великими традиційними фінансовими компаніями потенціалу блокчейну та його впливу на сучасну платіжну індустрію. Використання інноваційних блокчейнів, як Solana, дозволяє компаніям, таким як Visa, розширювати свої можливості в області швидких та ефективних платежів, забезпечуючи водночас низькі витрати та високу надійність.

В цьому розділі ми розглянули, як блокчейн технологія інтегрується в традиційні фінансові системи, особливо у банківській справі, страхуванні та управлінні активами. Від PayPal та їхнього стейблкоїна PYUSD до Visa та її інтеграції з блокчейном Solana, ми бачимо, як великі фінансові компанії активно використовують блокчейн для підвищення ефективності, зменшення витрат та надання інноваційних рішень своїм клієнтам. Це підкреслює зростаючу роль блокчейну в еволюції фінансового сектору, вказуючи на значний потенціал для подальших інновацій та розвитку.

2.4 Кейс-стаді та приклади

У світі, де фінансові технології постійно розвиваються, блокчейн відіграє вирішальну роль, пропонуючи нові можливості для трансформації традиційних фінансових систем. Зокрема, різноманітні фінансові платформи, які базуються на блокчейні, показують, як ця технологія може бути використана для створення більш ефективних, безпечних та прозорих фінансових послуг. Давайте розглянемо декілька ключових прикладів таких платформ, як Binance, Uniswap, 1inch, та Paraswap, кожна з яких внесла свій унікальний вклад у світ криптовалют та децентралізованих фінансів.

Binance, заснована у 2017 році під керівництвом Чанпен Чжао, швидко зарекомендувала себе як одна з провідних криптовалютних бірж світу. Компанія відзначилася своєю здатністю швидко адаптуватися до змінних умов ринку та потреб користувачів, пропонуючи широкий спектр криптовалют та інших цифрових активів. Особливою характеристикою Binance є її власний блокчейн Binance Chain, який був розроблений для оптимізації швидкості та ефективності транзакцій на платформі.

Ця біржа приваблює широкий круг трейдерів та інвесторів, які цінують можливість торгівлі різноманітними активами, включаючи можливості маржинальної торгівлі та ф’ючерсів. Незважаючи на високу ліквідність та великий вибір активів, Binance може здаватися складною для новачків у криптовалютній сфері, вимагаючи певного рівня попереднього знання та досвіду в криптовалютній торгівлі.

Binance також відома своєю інноваційністю та розвитком нових продуктів, що сприяє зростанню та популярності криптовалют серед широкого кола користувачів. Її вплив на ринок криптовалют є значним, оскільки вона продовжує розширювати свої послуги та впроваджувати нові технологічні рішення для своїх користувачів.

У світі криптовалют та блокчейну існує значна різниця між централізованими та децентралізованими фінансовими рішеннями, що демонструється на прикладі таких платформ як Binance та Uniswap. Ці платформи представляють два різні підходи до торгівлі та обміну криптовалют, кожен з яких має свої унікальні характеристики та переваги для користувачів.

Uniswap, запущений у 2018 році, швидко здобув репутацію одного з провідних децентралізованих обмінників у світі криптовалют. Ця платформа дозволяє користувачам безпосередньо торгувати Ethereum та ERC-20 токени, уникаючи потреби в централізованих посередниках, що відкриває нові можливості для децентралізованої торгівлі та інвестицій.

Основною аудиторією Uniswap є ті, хто цікавиться децентралізованою торгівлею та інвестиціями в проєкти на базі Ethereum, забезпечуючи їм зручну та легко доступну платформу для обміну токенів. Завдяки своїй унікальній моделі створення ліквідності, Uniswap спрощує обмін токенів та забезпечує користувачам доступ до широкого спектру криптовалютних активів.

Uniswap працює на блокчейні Ethereum, що забезпечує високу ступінь децентралізації та безпеки. Однак, у періоди великого навантаження на мережу Ethereum, користувачі можуть зіткнутися з високими комісіями за транзакції. Незважаючи на це, Uniswap залишається однією з найпопулярніших платформ у світі децентралізованих фінансів, відіграючи ключову роль у розвитку екосистеми DeFi та надаючи користувачам доступ до інноваційних фінансових інструментів.

Переходячи від Uniswap, який надає унікальний досвід децентралізованої торгівлі, ми приходимо до іншого значущого гравця у світі DeFi – 1inch. Запущений у 2019 році, 1inch відразу заявив про себе як агрегатор декількох децентралізованих бірж (DEX), що дозволяє користувачам знаходити найвигідніші ціни на різноманітних платформах. Ця платформа зорієнтована на трейдерів, які шукають не тільки оптимізовані ціни, але й швидкі та ефективні транзакції в екосистемі децентралізованих фінансів.

Значення 1inch полягає у забезпеченні користувачам зручного доступу до найкращих цін на ринку, що робить її важливим інструментом для досвідчених трейдерів. Ця платформа відіграє важливу роль у розвитку децентралізованих фінансових рішень, демонструючи, як інновації в блокчейн технології можуть пропонувати більш ефективні та гнучкі способи торгівлі цифровими активами.

Ми детально розглянули кілька ключових фінансових платформ, що використовують блокчейн, таких як Binance, Uniswap, 1inch, та Paraswap. Ці платформи ілюструють різні способи застосування блокчейн технологій у фінансовому секторі, кожна з яких має свої унікальні особливості, переваги та виклики.

Аналіз цих проектів показує, що успіх у світі блокчейн фінансів часто залежить від декількох ключових факторів:

1. Інновації та адаптація: платформи, які швидко адаптуються до змін у технологіях та потребах ринку, часто досягають більшого успіху.

2. Безпека та довіра: у світі, де цифрові активи часто стають мішенями для шахраїв, надійність та безпека є ключовими для залучення та утримання користувачів.

3. Легкість використання та доступність: платформи, які пропонують інтуїтивно зрозумілі інтерфейси та зручність використання, забезпечують краще залучення користувачів.

Вивчення цих фінансових платформ на базі блокчейну виявляє глибокі трансформації, які відбуваються у фінансовому секторі. Від централізованих бірж, як Binance, до повністю децентралізованих платформ, як Uniswap та 1inch, блокчейн розширює можливості для інновацій, безпеки та ефективності. Кожна з цих платформ вносить свій вклад у розвиток екосистеми криптовалют, підкреслюючи важливість технологічних інновацій та користувацького досвіду у досягненні успіху в цій швидко зростаючій галузі.

3 РОЗРОБКА ВЛАСНОГО РІШЕННЯ АГРЕГАЦІЇ ЛІКВІДНОСТІ І ПОШУКУ НАЙКРАЩОЇ ЦІНИ

3.1 Проблема та складність агрегації ліквідності у децентралізованих системах

Агрегація ліквідності у децентралізованих фінансових системах (DeFi) є складним завданням, яке вимагає розробки спеціалізованих алгоритмів та рішень. В децентралізованому світі, де існує безліч обмінників та торгових платформ, знаходження оптимального шляху для обміну токенів часто стає складною задачею. Різні платформи пропонують різні ціни та рівні ліквідності, і для користувача важливо знайти найкращі можливі умови для своєї торгової операції.

Пошук найкращої ліквідності та маршрутів обміну токенів є ключовим для ефективної та вигідної торгівлі в DeFi [12]. Це не тільки забезпечує користувачам кращі ціни, але й мінімізує комісії та затримки в транзакціях. Однак, враховуючи велику кількість токенів і можливих шляхів обміну, автоматизація цього процесу вимагає складних алгоритмів.

Проблема, яку ми прагнемо вирішити, полягає у знаходженні найкращої ціни для обміну токена А на токен Б у децентралізованому фінансовому просторі. Ця задача є особливо складною через високу волатильність та динамічність криптовалютного ринку, де ціни та умови обміну змінюються щосекунди.

У світі децентралізованих фінансів (DeFi) існує безліч різних пулів ліквідності та обмінних платформ, кожна з яких може пропонувати різні умови для обміну одних токенів на інші. Це створює складну мережу можливих маршрутів обміну, де кожен маршрут може включати прямі обміни між токенами або кілька проміжних етапів з використанням додаткових токенів. Така структура робить важким вибір оптимального шляху обміну, оскільки кожен додатковий етап може впливати на загальну ціну та ефективність транзакції.

Для користувача, який прагне обміняти токен А на токен Б за найкращою можливою ціною, важливо враховувати не тільки поточні ціни на прямі обміни, але й потенційні переваги використання проміжних токенів та різних пулів ліквідності. Однак, через велику кількість можливих комбінацій та швидкі зміни умов на ринку, ручний вибір оптимального маршруту стає практично нереалізовним. Можливо маршрути обміну токенів зображено на рис. 3.1.

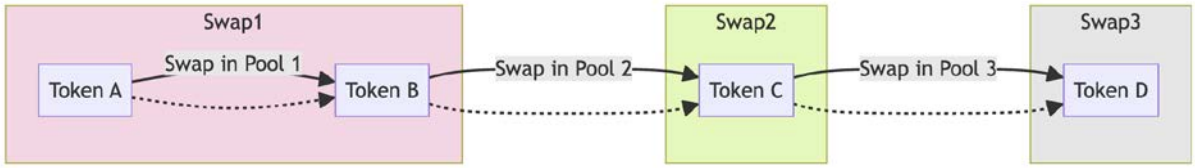

Рисунок 3.1 - обмін токенів між багатьма пулами

В цьому контексті, розробка алгоритму, який може швидко аналізувати різні варіанти та визначати найкращі маршрути обміну, стає ключовою для підвищення ефективності та зниження витрат у децентралізованому фінансовому середовищі. Такий алгоритм дозволить автоматизувати процес вибору найвигідніших умов обміну, враховуючи всі можливі опції та зміни на ринку в реальному часі.

Для вирішення цієї проблеми ми плануємо розробити алгоритм, заснований на принципах задачі про рюкзак (Knapsack problem). Цей алгоритм буде аналізувати різні маршрути обміну та ліквідність на різних платформах, щоб знайти оптимальний шлях для обміну токенів. Використання принципів задачі про рюкзак дозволить нам ефективно вирішити проблему оптимізації, враховуючи обмежені ресурси та максимізуючи потенційний прибуток від торгової операції [11].

Цей алгоритмічний підхід відіграє важливу роль у сучасному децентралізованому фінансовому ландшафті, де вміння швидко та ефективно аналізувати ринкову інформацію є ключовим фактором успіху. У наступному розділі ми детально розглянемо архітектуру та принципи роботи запропонованого алгоритму, що дозволить нам знайти найкращі можливості торгівлі на ринку DeFi.

3.2 Математичний опис проблеми рюкзака

Проблема рюкзака є класичною задачею NP-повних проблем оптимізації в області інформатики та математичного програмування. Вона полягає в відборі підмножини предметів, що мають задану вартість та вагу, з метою максимізації загальної вартості, не перевищуючи заданої ліміту ваги (або іншого обмежувального ресурсу).

Формально, проблема Knapsack задається наступною множиною даних:

- $\square$ - кількість предметів
- $\square_{\square}$- вага і-го предмета
- $\square_{\square}$ - вартість і-го предмета
- $\square$ - максимальна вага рюкзака

Необхідно знайти підмножину $\{\square_1, \square_2, \ldots, \square_{\square}\}$ з $\square$ предметів, яка задовольняє наступним умовам:

- $\square_{\square_1} + \square_{\square_2} + \square_{\square_3} + \ldots + \square_{\square_{\square}} \leq \square$
- $\square_{\square_1} + \square_{\square_2} + \square_{\square_3} + \ldots + \square_{\square_{\square}} \geq \square\square\square_{\square \subseteq \{1,2,\ldots,\square\}}\{\square_{\square}\}$,
- *де* $\square_{\square} = \sum_{\square \square \square} \square_{\square}$

Проблема Knapsack вперше була описана в 1930-х роках німецьким математиком Даніелем Гурвіцом. Вона була використана для моделювання проблеми вибору товарів для перевезення в обмеженому вантажному просторі [7].

Існує ряд варіантів проблеми Knapsack, які відрізняються від стандартної постановки. Одним з таких варіантів є проблема поліноміального Knapsack. У цій проблемі вага кожного предмета є кратна деякому числу $\square$. Це дозволяє

використовувати більш ефективні алгоритми розв'язку, ніж для стандартної постановки.

Іншим варіантом є проблема Knapsack з обмеженнями. У цій проблемі крім обмеження на загальну вагу рюкзака можуть бути присутні й інші обмеження, наприклад, обмеження на максимальну кількість предметів певного типу.

На ринку децентралізованих фінансових систем, проблему рюкзака можна застосувати для оптимізації вибору маршрутів обміну токенів. Тут, "вага" кожного маршруту може представляти собою вартість або комісію за транзакцію, а "вартість" - потенційну вигоду або доступну ліквідність. Метою є максимізація загальної "вартості" (оптимальні умови обміну) при дотриманні обмежень на "вагу" (мінімізація загальних витрат або комісій).

У контексті DeFi, можна застосувати алгоритм, заснований на методі динамічного програмування, для аналізу всіх можливих маршрутів обміну та їх комбінацій, щоб знайти найбільш вигідний шлях. Такий підхід вимагає аналізу великої кількості даних та швидких обчислень, що є важливим у середовищі, де умови ринку швидко змінюються.

Використання алгоритму рюкзака у децентралізованих фінансових системах може значно підвищити ефективність та прибутковість торговельних операцій, дозволяючи користувачам мінімізувати витрати та оптимізувати вибір маршрутів обміну.

У цьому розділі було надано короткий математичний аналіз проблеми рюкзака, який є ключовим для розуміння оптимізації ресурсів у блокчейн-системах. Через детальне вивчення цієї класичної задачі оптимізації ми отримали глибше розуміння того, як можна ефективно вирішувати складні задачі розподілу та вибору ресурсів в контексті блокчейну.

3.3 Порівняння алгоритмів розв'язку проблеми рюкзака

Проблема Knapsack є NP-повною, що означає, що **не існує** відомого алгоритму, який може знайти оптимальне рішення за поліноміальний час. Однак існує ряд алгоритмів, які можуть знайти близькі до оптимальних рішення за поліноміальний час [8].

Для вирішення проблеми рюкзака існує кілька підходів. Один з найпростіших - це жадібний алгоритм, який обирає предмети з найвищим співвідношенням вартості до ваги, але він не завжди гарантує оптимальний результат. Цей підхід ефективний для фракційної проблеми рюкзака, де можливе часткове включення предметів, але не завжди надає оптимального рішення для задачі 0/1 рюкзака.

Одним з найефективніших алгоритмів для вирішення проблеми Knapsack є алгоритм динамічного програмування. Цей алгоритм працює, будуючи таблицю, яка містить максимальну вартість підмножини предметів з заданим загальним вагою.

Алгоритм динамічного програмування працює наступним чином:

Для кожного □ від 1 до □ і кожного □ від 0 до □:

- *Якщо* $□_□ > □$, то $□(□, □) = 0$
- *Якщо* $□_□ \leq □$, то$□(□, □) = □□□(□(□ - 1, □), □(□ - 1, □ - □_□) + □_□)$

Цей метод розбиває задачу на менші підзадачі, розв'язуючи кожну з них тільки один раз і зберігаючи їх рішення.

Метод гілок та меж є ще одним підходом, який використовує стратегію вилучення підмножин для визначення оптимального рішення, обмежуючи простір пошуку за допомогою обчислення верхніх та нижніх меж рішень. Цей метод особливо ефективний, коли потрібно знайти точний оптимальний розв'язок задачі 0/1 рюкзака, але може бути обчислювально важким для великих даних.

В контексті децентралізованих фінансових систем, ці алгоритми можуть бути застосовані для оптимізації маршрутів обміну токенів. Динамічне програмування,

наприклад, може бути використане для аналізу всіх можливих маршрутів обміну, оцінюючи загальну вигоду від кожного маршруту за допомогою формули загальної вартості транзакції. Такий підхід дозволить знайти найефективніші шляхи для обміну токенів, враховуючи змінні умови ринку та динаміку цін.

При роботі з алгоритмами, особливо при розв'язанні складних оптимізаційних задач, таких як проблема рюкзака, важливо не лише розуміти логіку їхньої роботи, а й оцінювати їхню ефективність у різних умовах. Ефективність алгоритму може визначатися різними параметрами, серед яких одним із ключових є час виконання.

Для того, щоб зрозуміти, як різні підходи до вирішення проблеми рюкзака впливають на ефективність, ми напишемо скрипт [Додаток А], що імплементує три популярні алгоритми: жадібний пошук, динамічне програмування та метод гілок та меж. За допомогою цього скрипта, ми проведемо заміри часу виконання кожного алгоритму з використанням різної кількості елементів.

Зібрані дані можна відобразити у таблиці 3.1 для кращого візуального уявлення:

Таблиця 3.1 - Порівняння алгоритмів до розв’язку проблеми рюкзака

Кількість елементів	Жадібний пошук (мс)	Динамічне програмування (мс)	Метод гілок та меж (мс)
10	0.0457	22.4890	0.1158
100	0.0405	196.9780	0.0624
1000	0.4434	2426.4932	0.4145
10000	2.7285	30281.4671	2.6744

Ці дані вимірювань часу виконання різних алгоритмів для вирішення проблеми рюкзака дозволяють зробити порівняльний аналіз ефективності кожного

алгоритму залежно від кількості елементів. Основні аспекти для порівняння - це час виконання та масштабування алгоритмів при збільшенні кількості елементів.

Таким чином, ми зможемо зробити обґрунтований вибір алгоритму залежно від конкретних умов та вимог до задачі, яку ми вирішуємо.

Відповідно можемо зробити висновки:

1. **Жадібний пошук** є найшвидшим методом у цьому випадку, особливо для менших наборів даних. Однак цей метод може не завжди знаходити оптимальне рішення, оскільки він вибирає локально оптимальні рішення на кожному етапі, не враховуючи загальний контекст.

2. **Динамічне програмування** показує значно більший час виконання, особливо при збільшенні кількості елементів. Цей метод гарантує знаходження оптимального рішення, але його ефективність сильно зменшується при роботі з великими даними через значну кількість обчислень.

3. **Метод гілок та меж** демонструє хороші результати, будучи швидшим за динамічне програмування, але трохи повільнішим за жадібний пошук. Цей метод є ефективним компромісом між швидкістю та точністю, особливо для великих наборів даних.

Вибір підходящого алгоритму залежить від специфіки задачі та обсягу даних, де кожен метод має свої переваги в залежності від контексту застосування, тобто від конкретної ситуації: для швидкого, але не завжди оптимального рішення можна використовувати жадібний пошук (жадібний пошук виявився найшвидшим, але не завжди найточнішим методом), для точного рішення при невеликій кількості даних - динамічне програмування, а для великих наборів даних - метод гілок та меж.

3.4 Розробка рішення з використанням алгоритму Рюкзака

У цьому розділі ми застосуємо проблему рюкзака для розробки рішення на блокчейні, яке дозволить знаходити найкращу ціну для обміну токена А на токен Б. Основна ідея полягає у створенні алгоритму, здатного моніторити та аналізувати різні ціни на ринку, щоб ідентифікувати найбільш вигідні умови обміну.

1. **Моніторинг Цін на Ринку**: Алгоритм буде регулярно перевіряти ціни на різних ліквідності пулах, таких як Uniswap, Curve, Balancer тощо. Це включає збір даних про поточні ціни обміну, доступну ліквідність та комісійні витрати на кожній з цих платформ.

2. **Використання Проблеми Рюкзака для Оптимізації Обміну**: Коли виникає потреба знайти найкращу ціну для обміну токенів, алгоритм буде використовувати жадібний метод пошуку, заснований на проблемі рюкзака. В цьому контексті, "вага" кожного маршруту обміну може представляти комісійні витрати або інші збитки, пов'язані з транзакцією, а "вартість" - потенційну вигоду від операції.

Вибір жадібного пошуку для нашого алгоритму агрегації ліквідності та оптимізації обміну токенів заснований на кількох важливих факторах. По-перше, жадібний пошук є одним з найпростіших алгоритмів для реалізації, що дозволяє нам швидко розробити та тестувати рішення. Це особливо важливо в динамічному та швидкозмінному світі децентралізованих фінансів, де швидкість розвитку та адаптації рішень може мати значний вплив на їх успіх та ефективність.

По-друге, незважаючи на свою простоту, жадібний алгоритм може бути дуже ефективним у певних сценаріях, особливо коли йдеться про вибір оптимальних маршрутів у фінансових операціях. Жадібний метод дозволяє швидко оцінювати різні варіанти обміну та вибирати найбільш вигідні умови, враховуючи такі фактори, як доступна ліквідність, ціни обміну та комісійні ставки.

Окрім того, враховуючи обмежені обчислювальні ресурси, особливо в контексті інтеграції з блокчейн платформами, жадібний алгоритм забезпечує баланс

між точністю рішень та необхідністю швидкого реагування на зміни ринкових умов. Це робить його ідеальним вибором для реалізації алгоритму, спрямованого на забезпечення ефективності та конкурентоспроможності в децентралізованих фінансових системах.

Продукт буде складатися з двох основних модулів:

1. **Модуль Моніторингу**: Він буде відповідальний за збір даних з різних джерел, включаючи ціни на обмін, ліквідність пулів та комісійні ставки. Цей модуль буде використовувати API платформ або інші технічні засоби для отримання актуальної інформації.

2. **Модуль Оптимізації**: Використовуючи дані, зібрані модулем моніторингу, цей модуль буде застосовувати жадібний алгоритм рюкзака для визначення найкращого маршруту обміну. Він розраховуватиме оптимальний баланс між вартістю обміну та витратами на комісії, щоб максимізувати загальну вигоду від транзакції.

Для забезпечення актуальності та точності інформації, а також для підвищення надійності та безпеки операцій, алгоритм буде інтегровано з блокчейн платформами. Це дозволить використовувати переваги децентралізації та прозорості блокчейну, забезпечуючи ефективну та безпечну оптимізацію обмінних операцій.

Для інтеграції нашого алгоритму, заснованого на проблемі рюкзака, з технологією блокчейну, ми оберемо *Ethereum Mainnet* як основну платформу. Вибір *Ethereum* пояснюється кількома ключовими факторами:

1. **Популярність і Запит на Ринку**: Ethereum Mainnet є однією з найпопулярніших та широко використовуваних блокчейн платформ. Це забезпечує високу ймовірність наявності значного попиту серед користувачів на такого типу рішення, особливо в контексті оптимізації обмінних операцій у децентралізованих фінансових системах.

2. **Розвинена Інфраструктура**: Ethereum Mainnet володіє добре розвиненою інфраструктурою, включаючи індексери, майнери, RPC провайдери та інші важливі елементи. Ця розвинута інфраструктура сприяє швидкому та ефективному розвитку та імплементації нових рішень, забезпечуючи необхідні технічні ресурси та інструменти.

3. **Багатий Екосистема Проєктів**: Наявність великої кількості проєктів та додатків на Ethereum Mainnet створює сприятливе середовище для розробки та інтеграції нашого алгоритму. Це включає доступ до різноманітних джерел ліквідності, інструментів аналізу ринку та спільноти розробників.

Використання Ethereum Mainnet дозволить нам швидко інтегрувати наш алгоритм в існуючу екосистему, надаючи користувачам доступ до інноваційного інструменту для оптимізації їхніх торговельних стратегій. Завдяки поєднанню теоретичних переваг алгоритму рюкзака з практичними можливостями Ethereum Mainnet, ми зможемо створити потужне, надійне та корисне рішення, яке відповідає потребам сучасних користувачів децентралізованих фінансових систем.

Це важливо, враховуючи, що багато децентралізованих фінансових застосунків і платформ уже базуються на Ethereum, що відкриває широкі можливості для взаємодії та синергії.

Використовуючи Ethereum Mainnet, ми також зможемо забезпечити високий рівень безпеки та надійності для нашого рішення. Ethereum мережа відома своєю стабільністю та активною розробницькою спільнотою, що постійно працює над поліпшенням інфраструктури та безпеки. Це гарантує, що наше рішення буде стійке до зовнішніх загроз та забезпечить користувачам безпечне середовище для виконання їхніх транзакцій. Врешті-решт, це не тільки зміцнить довіру до нашого продукту, але й відкриє нові перспективи для його розвитку та адаптації в майбутньому.

3.5 Реалізція окремих модулів продукту

3.5.1 Реалізація модуля моніторингу

Модуль моніторингу є ключовою складовою нашої системи пошуку найкращої ціни для обміну токенів. Цей модуль відповідає за збір та аналіз даних про ціни з різних джерел ліквідності, таких як Uniswap, Curve, Balancer, та інших популярних DeFi платформ.

Модуль моніторингу складається з декількох окремих компонентів, кожен з яких відповідає за збір даних з конкретного джерела. Кожен компонент працює автономно та має наступні основні функції:

1. **Регулярне Оновлення Даних**: Компоненти моніторять зміни цін на відповідних платформах, автоматично оновлюючи інформацію через задані інтервали часу.

2. **Зберігання Даних**: Зібрані дані від кожного джерела зберігаються у централізованій системі зберігання даних, такій як Redis. Це дозволяє забезпечити швидкий доступ до актуальної інформації для подальшої обробки.

3. **Стандартизація Даних**: Для забезпечення сумісності та легкості інтеграції, дані з різних джерел приводяться до єдиного формату.

Зібрані та оброблені дані про ціни та ліквідність стають доступними для **Модуля Оптимізації**, який використовує цю інформацію для вирішення задачі пошуку найкращих маршрутів обміну. Модуль моніторингу забезпечує постійне оновлення даних, гарантуючи, що Модуль Оптимізації оперує найактуальнішою та точною інформацією.

Ефективність та точність Модуля Моніторингу мають безпосередній вплив на успіх загального рішення. Швидке виявлення змін на ринку та надання точних даних для оптимізації обмінних операцій є критично важливими для забезпечення конкурентоспроможності та вигоди для користувачів нашої системи.

Модуль моніторингу в нашій системі забезпечується потужною комбінацією технологій, кожна з яких відіграє важливу роль у зборі та обробці ринкових даних. Використання NodeJS як середовища виконання JavaScript дозволяє створювати швидкі та ефективні серверні застосунки, здатні обробляти великі обсяги даних, що є необхідним для моніторингу динамічного ринку криптовалют.

Infura, виступаючи як надійний RPC провайдер, надає модулю моніторингу легкий доступ до Ethereum блокчейну, дозволяючи ефективно отримувати актуальні дані про стан та транзакції у мережі. Це допомагає забезпечити точність та актуальність інформації, яка збирається для аналізу.

TheGraph використовується як індексер даних, що дозволяє модулю моніторингу ефективно запитувати історичні та актуальні дані з блокчейну Ethereum. Ця технологія є ключовою для забезпечення доступу до глибокого аналізу ринкової ситуації та важливих метрик.

Нарешті, Redis використовується для швидкого зберігання та отримання даних про ціни та інші ринкові показники. Його висока швидкість і ефективність у роботі з даними в пам'яті робить його ідеальним вибором для забезпечення оперативної роботи модуля моніторингу.

Завдяки цій інтегрованій технологічній інфраструктурі, модуль моніторингу здатний надійно та ефективно збирати, обробляти та зберігати ключові дані, необхідні для визначення оптимальних маршрутів обміну токенів в децентралізованих фінансових системах. Покажемо це на рис. 3.2.

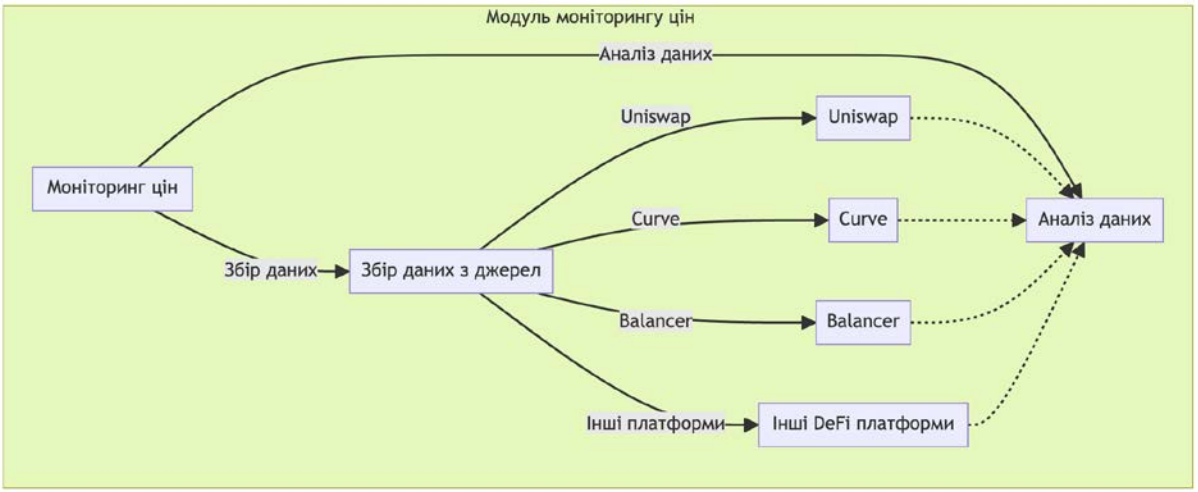

Рисунок 3.2 - Архітектура модуля моніторингу цін

Ці технології разом формують потужну та надійну інфраструктуру для модуля моніторингу, забезпечуючи його здатність ефективно збирати, обробляти та зберігати великі обсяги ринкових даних, що є ключовим для успішного пошуку оптимальних маршрутів обміну токенів.

3.5.2 Реалізція модуля оптимізації

Модуль оптимізації є важливою складовою нашої системи, призначеною для визначення найкращих маршрутів обміну токенів згідно з запитами користувачів. Він складається з двох ключових частин: серверної інфраструктури та функціональної логіки оптимізації.

Перша частина модуля оптимізації включає сервер, який обробляє запити користувачів. Сервер відповідає за кілька важливих аспектів:

- **Обробка запитів**: Сервер приймає та аналізує запити від користувачів, які шукають найкращі ціни для обміну токенів.
- **Авторизація та безпека**: Забезпечує авторизацію користувачів і гарантує безпеку даних, які передаються через систему.
- **Взаємодія з модулем моніторингу**: Сервер має доступ до актуальних даних про ціни, зібраних Модулем Моніторингу, для використання в оптимізації.

Друга частина модуля оптимізації відповідає за фактичний пошук найкращої ціни для обміну певної пари токенів:

- **Обробка запитів**: Коли користувач робить запит на отримання найкращої ціни для обміну токенів, модуль аналізує запит та ініціює процес оптимізації.
- **Актуальні дані про ціни**: Модуль має доступ до останніх даних про ціни з Модуля Моніторингу, включаючи інформацію про різні пули ліквідності та їхні умови обміну.
- **Використання жадібного алгоритму для проблеми рюкзака:** За допомогою жадібного алгоритму, модуль оптимізації ефективно аналізує можливі маршрути обміну та вибирає оптимальний варіант, максимізуючи вигоду користувача та мінімізуючи витрати.

Модуль оптимізації відіграє критичну роль у забезпеченні ефективності та вигоди для користувачів системи. Він не тільки дозволяє користувачам швидко знаходити найкращі ціни для обміну токенів, але й забезпечує високий рівень безпеки та надійності обробки запитів. Завдяки інтеграції з передовими технологіями та алгоритмами, модуль оптимізації стає ключовим елементом для досягнення оптимальних результатів у децентралізованих фінансових системах. Архітектура цього модуля зображена на рис. 3.3.

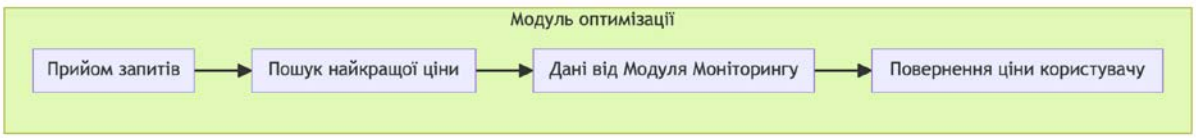

Рисунок 3.3 - Архітектура модуля оптимізації

У реалізації Модуля Оптимізації ми використовуємо кілька ключових технологій, щоб забезпечити його ефективність та надійність. Для оброблення запитів користувачів ми вибрали ExpressJS, який є гнучким та швидким фреймворком для створення веб-додатків на NodeJS. ExpressJS дозволяє легко створювати та управляти серверними маршрутами, забезпечуючи ефективну обробку запитів.

Що стосується авторизації, ми використовуємо JSON Web Tokens (JWT), які є зручним способом для безпечної передачі інформації між клієнтом та сервером. JWT дозволяє нам забезпечити захист ідентифікаційних даних користувачів. Крім того, за необхідності, система може бути легко адаптована для використання OAuth, що дозволить інтегрувати більш складні сценарії авторизації.

Функціональний компонент оптимізації, який відповідає за власне пошук найкращих цін для обміну токенів, розроблено на чистому NodeJS. Ми ухвалили рішення не використовувати сторонні бібліотеки, щоб забезпечити максимальну контрольованість та оптимізацію нашого рішення. Це дозволяє модулю швидко обробляти великі обсяги даних та виконувати складні обчислення необхідні для визначення оптимальних маршрутів обміну.

Для зберігання даних використовується Redis, який є високопродуктивною базою даних в пам'яті. Використання Redis дозволяє нам швидко зберігати та отримувати інформацію, необхідну для оптимізації, забезпечуючи високу швидкість відгуку системи.

Ця комбінація технологій дозволяє нам створити надійний, ефективний та безпечний Модуль Оптимізації, який може швидко обробляти запити користувачів та забезпечувати найкращі умови обміну токенів у децентралізованих фінансових системах.

В цілому, реалізація Модуля Оптимізації відіграє критичну роль у забезпеченні ефективності та надійності нашого рішення. Цей модуль демонструє потенціал блокчейн технологій у вирішенні складних задач у децентралізованих фінансових системах, пропонуючи користувачам швидкі та точні рішення для їхніх торговельних потреб.

3.6 Перевірка та тестування

3.6.1 Тестування модуля моніторингу

Тестування Модуля Моніторингу є важливим кроком для забезпечення його надійності та точності. Наступні підходи до тестування допоможуть перевірити, чи ефективно модуль збирає актуальні ціни для можливих пар токенів.

1. Тест оновлення даних:

- Перевірка, чи модуль успішно оновлює дані про ціни з різних джерел, таких як Uniswap, Curve, Balancer.
- Сценарії: Порівняння зібраних даних з відомими цінами на момент тестування, перевірка частоти оновлень.

2. Тест зберігання даних:

- Перевірка, чи дані коректно зберігаються у Redis і чи можуть бути швидко витягнуті для подальшого аналізу.
- Сценарії: Запис даних про ціни в Redis та їхнє зчитування, перевірка цілісності та актуальності даних.

3. Тест відповідності формату даних:

- Перевірка, чи дані з різних джерел приводяться до єдиного стандартизованого формату.
- Сценарії: Порівняння форматів даних з різних джерел, перевірка їх консистентності та уніфікації.

4. Тест реагування на зміни ринку:

- Перевірка, чи модуль моніторингу швидко реагує на зміни цін на ринку.
- Сценарії: Симуляція ринкових змін та перевірка швидкості відгуку модуля.

Кожен з цих тест кейсів має своє ключове значення для забезпечення загальної ефективності та надійності модуля оптимізації. Проведення цих тестів дозволяє не тільки виявити потенційні недоліки у роботі модуля, але й оцінити його здатність адаптуватися до динамічних умов ринку та задовольняти потреби користувачів у пошуку найкращих цін.

Для тестування можуть бути використані автоматизовані тестові фреймворки та скрипти, що дозволяють емулювати різні сценарії та перевіряти роботу модуля в умовах, близьких до реальних. Також можна використовувати інструменти моніторингу та логування для відстеження роботи модуля в режимі реального часу.

Можливості для тестування Модуля Моніторингу включають різноманітні методики, що дозволяють гарантувати його точність та ефективність. Однак, у конкретній реалізації цього проекту було обрано мануальне тестування за допомогою Postman. Це дозволяє ретельно перевіряти кожну частину системи, надаючи безпосередній контроль над процесом тестування та дозволяє швидко виявити можливі проблеми або недоліки у функціонуванні модуля. Мануальне тестування за допомогою Postman є ефективним способом перевірки інтеграції модуля з різними джерелами даних та його здатності коректно обробляти та зберігати інформацію про ціни, процес тестування зображено на рис. 3.4 та 3.5.

Ефективне тестування Модуля Моніторингу забезпечить, що він здатен точно та своєчасно збирати ринкові дані, що є критично важливим для успішної роботи всієї системи оптимізації обміну токенів.

Головна мета проведення тестування модуля моніторингу полягала у перевірці актуальності збирання даних та цін. Зокрема, було важливо порівняти інформацію, яку зберігає наша система, з реальними даними, доступними на ринку. Це дозволило оцінити, наскільки точно модуль відображає поточні ринкові умови.

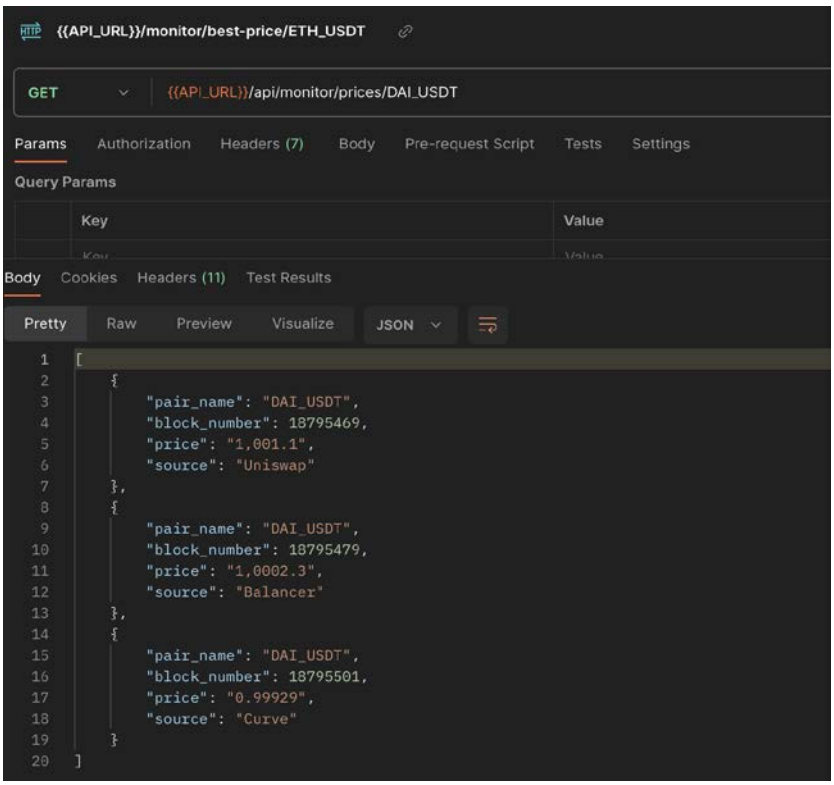

Рисунок 3.4 - Результат роботи програми по моніторингу цін для торгової пари DAI-USDT

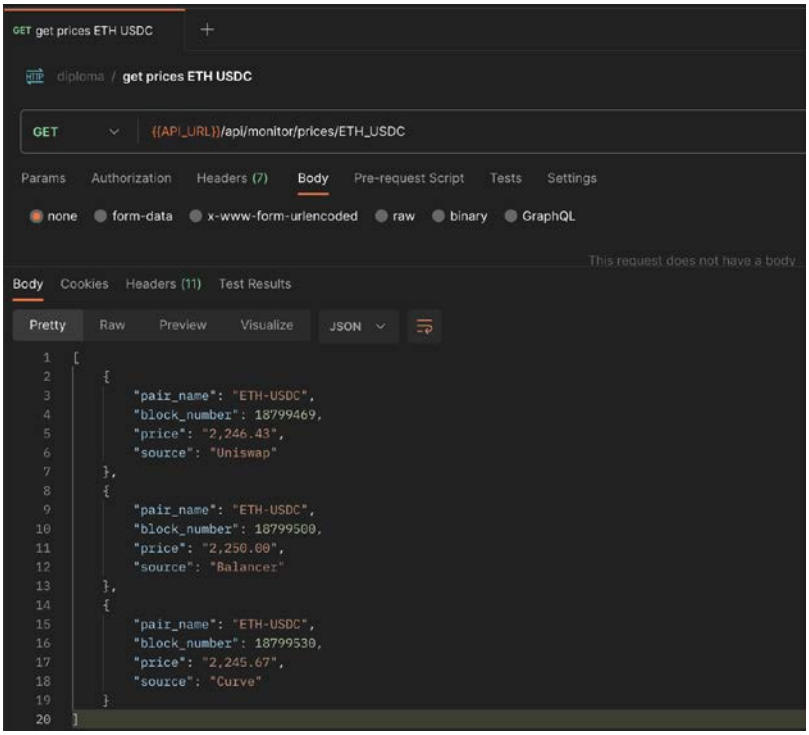

Рисунок 3.5 - Результат роботи програми по моніторингу цін для торгової пари ETH-USDC

Відповідно, зробимо аналогічні запити для всіх потрібних пар.

Тепер продемонструємо, результати тестування у табл. 3.2:

Таблиця 3.2 - Результати порівнянь роботи модуля моніторингу та реальних даних

Пара токенів	Номер блоку в системі	Номер блоку в блокчейні	Ціна в системі	Ціна в блокчейні	Джерело
ETH-USDC	18799469	18799442	2,246.43	2,240.2	Uniswap
DAI-USDT	18799469	18799446	0.9991	1.00123	Balancer
USDC-USDT	18799469	18799445	1.0012	1.0099	Uniswap
WBTC-USDT	18799469	18799460	42,233.1	41,765.2	Balancer
ETH-UNI	18799469	18799436	361.164	359.164	Balancer
TUSD-LEND	18799469	18799444	1.18954	1.1294	Curve
LINK-DAI	18799469	18799436	14.667	15.117	Curve

Результати тестування показали, що дані, зібрані модулем моніторингу, несуттєво відрізняються від актуальних цін, які присутні на ринку.

Ці результати свідчать про те, що модуль моніторингу здійснює точне збирання даних, забезпечуючи високу актуальність інформації. Невелике відставання в номерах блоків та цінах є прийнятним у контексті динамічності криптовалютного ринку.

На основі отриманих результатів можна зробити висновок, що модуль моніторингу реалізовано добре, і він здатний надійно збирати та відображати поточні ринкові умови. Це забезпечує міцну основу для ефективної роботи всієї системи оптимізації обміну токенів.

3.6.2 Тестування модуля оптимізації

Тестування модуля оптимізації важливе для переконання у його здатності ефективно знаходити найкращу ціну для торгової пари. Нижче наведені ключові тест кейси, які можуть бути використані для оцінки функціональності цього модуля:

1. Тест правильності пошуку цін:

- Мета: Переконатися, що модуль правильно збирає дані про ціни з Модуля Моніторингу.
- Сценарій: Запуск модуля для збору цін на різні торгові пари, порівняння отриманих цін з актуальними ринковими цінами.

2. Тест ефективності вибору найкращої ціни:

- Мета: Перевірка, чи модуль коректно обирає найкращу ціну серед зібраних даних.
- Сценарій: Симуляція запитів на обмін для різних пар токенів, аналіз результатів вибору найкращої ціни.

3. Тест реакції на зміни ринку:

- Мета: Оцінити, наскільки швидко модуль реагує на зміни ринкових цін.
- Сценарій: Моделювання зміни ринкових умов та перевірка, чи відображає модуль ці зміни у своїх рекомендаціях.

4. Тест надійності та стабільності:

- Мета: Переконатися, що модуль стабільно працює протягом тривалого часу без помилок або збоїв.
- Сценарій: Довготривалий запуск модуля з постійними запитами, моніторинг стабільності його роботи.

5. Тест швидкості обробки запитів:

- Оцінити швидкість реакції модуля на запити користувачів.
- Сценарій: Симулювання великої кількості одночасних запитів та вимірювання часу відповіді модуля.

6. Тест масштабованості:

- Визначити здатність модуля масштабуватися відповідно до збільшення обсягів даних.
- Сценарій: Поступове збільшення кількості даних, які обробляє модуль, та аналіз впливу на його продуктивність.

Проведення цих тестів допоможе гарантувати, що модуль оптимізації не тільки ефективно виконує свої основні функції, але й здатний адаптуватися до змінних умов ринку та забезпечує стабільність та надійність роботи у довгостроковій перспективі.

Тестування Модуля Оптимізації може включають різноманітні методики, що дозволяють гарантувати його точність та ефективність. Однак, так само як і для Модуля Моніторингу, у конкретній реалізації цього проекту було обрано мануальне тестування за допомогою Postman.

Процес тестування зображено на рис. 3.6.

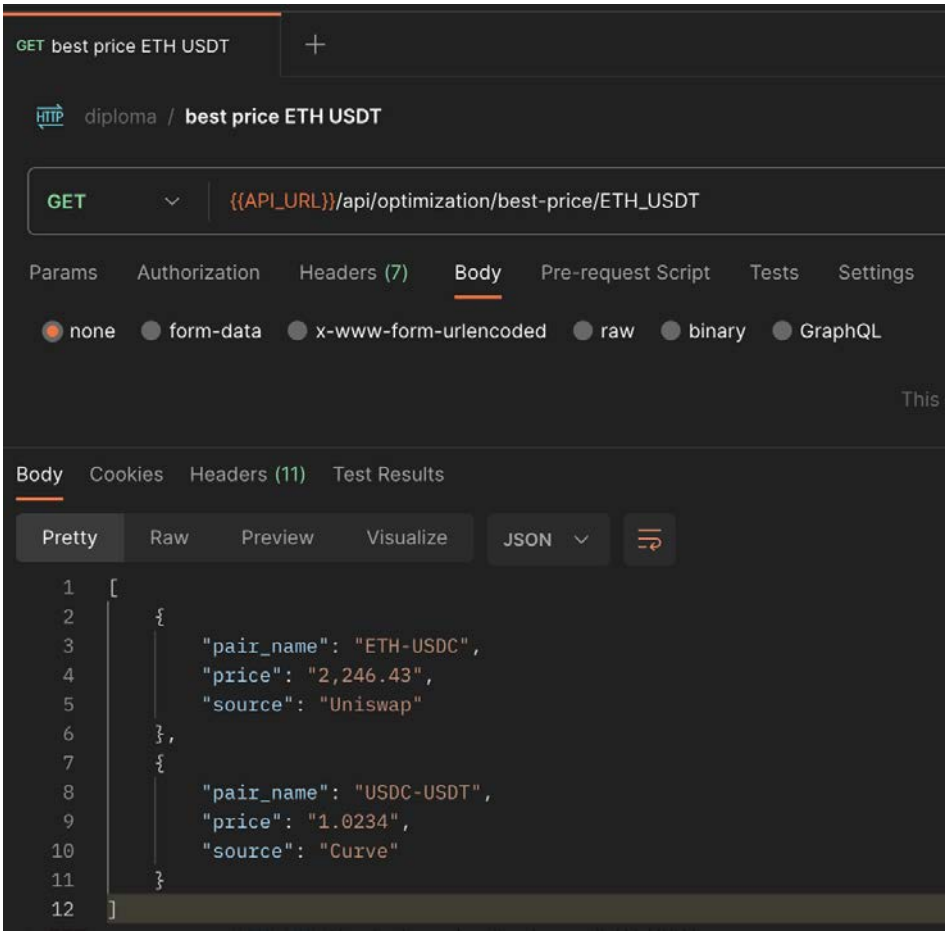

Рисунок 3.6 - Результат роботи програми по пошуку найкращої ціни

Порівняння цін, отриманих за допомогою нашого Модуля Оптимізації, з цінами на агрегаторі 1inch може бути ефективним методом тестування. Такий підхід дозволяє перевірити точність алгоритму у визначенні найкращих цін і оцінити його конкурентоспроможність на ринку. Виявлення відмінностей у цінах може вказувати на потребу у доробці алгоритму або на проблеми з даними, що використовуються для обчислень. Це також допомагає забезпечити, що наш алгоритм є надійним та ефективним у реальних умовах ринку.

Мета тестування полягала у перевірці ефективності Модуля Оптимізації у пошуку найкращих цін на ринку. Особлива увага приділялася порівнянню наших цін з цінами, які надає агрегатор 1inch, щоб оцінити точність та конкурентоспроможність нашого алгоритму. Сформуємо дані у табл. 3.3:

Таблиця 3.3 - Результати порівнянь пошуку найкращих цін між системою та агреготором 1inch

Пара токенів	Пропонуємий маршрут	Ціна в системі	Ціна на 1inch	Відхилення
ETH-USDC	ETH-USDC	2,220.2	2,234.45	0.6 %
ETH-USDT	ETH-USDC-USDT	2,218.45	2,235.91	0.7 %
DAI-UNI	DAI-UNI	0.16	0.1623	1.4 %
WBTC-USDT	WBTC-USDC-USDT	42,511.96	42,552.96	0.09 %
TUSD-LEND	TUSD-LEND	0.72	0.858	16 %

Результати показали, що для деяких торгових пар ціни, запропоновані нашим Модулем Оптимізації, відрізняються несуттєво від цін на агрегаторі 1inch. Наприклад, для пари ETH-USDC відхилення склало всього 0.6%, а для WBTC-USDT - 0.09%. Однак, у деяких випадках, як наприклад TUSD-LEND, відхилення досягло 16%, що вказує на потенційні можливості для оптимізації та покращення системи.

Такі результати вказують на те, що хоча Модуль Оптимізації в більшості випадків демонструє хороші результати, є деякі аспекти, які потребують додаткового удосконалення. Це може включати поліпшення алгоритмів визначення цін, оновлення даних або зміни у виборі маршрутів обміну.

Тестування підкреслює важливість постійної оцінки та вдосконалення системи, забезпечуючи, що Модуль Оптимізації може точно та ефективно визначати найкращі ціни на ринку, будучи конкурентоспроможним порівняно з іншими рішеннями на ринку.

3.7 Обмеження, виклики та майбутні перспективи

У поточній реалізації нашої системи оптимізації обміну токенів є декілька обмежень, які потребують уваги для покращення. Наразі використовуються лише три основні джерела цін - Uniswap, Balancer та Curve. Це обмежує нашу здатність знаходити найкращі ціни через обмежену кількість джерел. Хоча ці платформи мають значний вплив на ринок, інтеграція додаткових джерел може значно збільшити точність та ефективність системи. Однак, інтеграція нових джерел в систему - непростий процес, оскільки кожне джерело має свої унікальні характеристики. Тому існує потреба у розробці більш універсального підходу до збору та аналізу цін.

Крім того, поточний жадібний алгоритм для проблеми рюкзака, який використовується для пошуку найкращих цін, може бути не найефективнішим в деяких складних сценаріях. Використання більш складних алгоритмів, як-от методи динамічного програмування, може підвищити точність та ефективність системи. Такі покращення дозволять створити більш надійну та точну систему, здатну визначати оптимальні умови обміну в децентраліПоточна система оптимізації обміну токенів має значний потенціал для розширення та покращення. Одним із можливих напрямків розвитку є додавання функціоналу для відслідковування ціни на газ в Ethereum Mainnet, який є критично важливим для визначення загальної вартості транзакцій. Цей параметр може бути інтегрований у алгоритм підбору кращої ціни, забезпечуючи більш комплексний та точний аналіз.

Крім того, система наразі працює лише на Ethereum Mainnet, але її можна розширити на інші блокчейн платформи. Таке розширення не тільки підвищить універсальність та гнучкість системи, але й забезпечить доступ до ширшого спектру ринкових можливостей та ліквідності.

Що стосується обмежень вибраних технологій, як NodeJS, Redis та TheGraph, вони є ефективними для поточного рівня навантаження, але можуть виявитися недостатніми для високонавантажених систем. У такому випадку, можна розглянути

використання мов програмування, як Rust або Go, які пропонують кращу продуктивність та масштабованість. Вибір цих технологій може значно підвищити ефективність обробки даних, особливо в умовах високої кількості транзакцій та динамічності ринку.

Загалом, ці покращення та розширення можуть забезпечити системі більшу гнучкість, надійність та здатність адаптуватися до швидко змінних умов ринку, забезпечуючи користувачам кращі умови для обміну токенів.

зованих фінансових системах.

У контексті розвитку нашої системи оптимізації обміну токенів існує кілька важливих напрямків для майбутніх досліджень та розширення.

1. **Cross-Chain Swaps**: Одним з актуальних напрямків є розвиток технологій для обміну токенами між різними блокчейн платформами. Реалізація cross-chain swaps відкриває можливості для більш широких торгових стратегій та забезпечує доступ до різноманітних активів на різних платформах. Це вимагає розробки складних механізмів інтеграції та обміну між різними блокчейнами.

2. **Gasless Transactions і Auctions**: Іншим перспективним напрямком є дослідження та реалізація газлесс (gasless) транзакцій та аукціонів. Це включає розробку механізмів, де транзакції можуть виконуватися без прямої участі користувача, а замість цього виконуватися третіми сторонами, які отримують за це вигоду. Це може значно знизити вартість та складність транзакцій для кінцевих користувачів.

3. **MEV-Resistant Solutions**: Проблема MEV (Miner Extractable Value) є важливою темою у сучасному блокчейні. Розробка MEV-resistant систем може допомогти забезпечити справедливіше та прозоріше ціноутворення, уникаючи маніпуляцій з цінами та інших видів експлуатації. Це особливо важливо для забезпечення чесності та довіри до системи обміну токенів.

Кожен із цих напрямків має потенціал радикально змінити підходи до торгівлі криптовалютами та управління активами. Вони вимагають глибокого технічного аналізу та інноваційних рішень, але можуть принести значні переваги у вигляді більшої ефективності, безпеки та зручності для користувачів. Розвиток у цих напрямках відкриває шлях до створення більш гнучких та потужних систем оптимізації обміну в майбутньому.

Цей розділ висвітлив ключові обмеження та виклики, що стоять перед нашою системою оптимізації обміну токенів, а також намітив шляхи для майбутніх досліджень і розвитку. Від розробки cross-chain swaps, які розширюють можливості торгівлі між різними блокчейн платформами, до впровадження gasless транзакцій і аукціонів для зниження вартості та складності угод, кожен напрямок має потенціал значно вдосконалити поточну систему.

Особлива увага приділена проблемі MEV та розробці MEV-resistant рішень, що сприятиме створенню більш справедливого та прозорого середовища для торгівлі. Інновації в цих областях не тільки вирішать існуючі обмеження, але й відкриють нові горизонти для розвитку систем обміну токенів, роблячи їх більш ефективними, безпечними та доступними для широкого кола користувачів. Таким чином, цей розділ підкреслює важливість продовження досліджень та розробки в області блокчейн технологій, наголошуючи на потенціалі, який ці напрямки відкривають для майбутнього цифрового фінансового світу.

ВИСНОВКИ

У рамках цієї дипломної роботи було проведено всебічний аналіз блокчейн технологій та їх застосування в сфері фінансів. Розглядались різні децентралізовані рішення, такі як Uniswap, 1inch, Balancer, які демонструють потенціал блокчейну у створенні надійних та ефективних фінансових систем.

Важливою частиною дослідження стало створення власного продукту, що складається з двох основних модулів - Модуля моніторингу та Модуля оптимізації. Цей продукт забезпечує відслідковування актуальних ринкових цін та здатний ефективно знаходити найкращі умови для обміну токенів. Такий підхід відкриває нові перспективи у сфері децентралізованих фінансових операцій та показує, як можна використовувати блокчейн для підвищення ефективності та надійності фінансових систем.

Також варто зазначити, що наша система оптимізації обміну токенів, хоча й ефективна у своєму поточному стані, все ж має деякі обмеження, які вимагають уваги та подальшого розвитку. Використання обмеженої кількості джерел цін ставить певні рамки для виявлення найкращих цін, обмежуючи можливості системи у повному охопленні ринку. Таким чином, подальше удосконалення та розширення системи є ключовими для забезпечення її ефективності та відповідності широкому спектру потреб користувачів.

Загалом, цілі дослідження були досягнуті: проведено глибокий аналіз блокчейн технологій, вивчено різноманітні децентралізовані рішення, та розроблено власний продукт. Результати цього дослідження можуть бути використані для подальшого розвитку децентралізованих фінансових систем та впровадження інноваційних рішень у цій сфері.

ПЕРЕЛІК ПОСИЛАНЬ

1. Lewis, Antony. The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Derivatives Investments, Futures Trading, Digital Assets, NFT).
2. Bashir, Imran. Blockchain Consensus: An Introduction to Classical, Blockchain, and Quantum Consensus Protocols.
3. Тапскотт, Дон; Тапскотт, Алекс. Блокчейн-революція: Як технологія, що лежить в основі біткойна та інших криптовалют, змінює світ.
4. «Що таке MakerDAO (DAI)?», [https://academy.binance.com/uk/articles/a-guide-to-makerdao-and-dai].
5. «Guide to DeFi tokens and altcoins», [https://www.coinbase.com/learn/crypto-basics/defi-tokens-and-altcoins].
6. Tapscott, Don; Tapscott, Alex. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.
7. Kellerer, Hans; Pferschy, Ulrich; Pisinger, David. Knapsack Problems.
8. Lance Fortnow: The Golden Ticket: P, NP, and the Search for the Impossible.
9. «A deep dive on Solana, a high performance blockchain network», [https://usa.visa.com/solutions/crypto/deep-dive-on-solana.html].
10. Antonopoulos, Andreas; Wood, Gavin Ph.D. Mastering Ethereum: Building Smart Contracts and DApps.
11. Bolfing, Andreas. Cryptographic Primitives in Blockchain Technology: A mathematical introduction.
12. Elrom, Elad. The Blockchain Developer: A Practical Guide for Designing, Implementing, Publishing, Testing, and Securing Distributed Blockchain-based Projects.

ДОДАТОК А

```
// index.js

function knapsack(items, capacity) {
	// Сортуємо предмети за ставкою вартості на одиницю ваги
	items.sort((a, b) => a.value / a.weight - b.value / b.weight)

	// Створюємо масив, який буде містити підмножину предметів, які ми вибрали
	let packed = []

	// Проходимо по всіх предметах
	for (let i = 0; i < items.length; i++) {
		// Якщо вага предмета не перевищує максимально дозволену, то додаємо його в
рюкзак
		if (items[i].weight <= capacity) {
			packed.push(items[i])
			capacity -= items[i].weight
		}
	}

	// Повертаємо підмножину предметів, які ми вибрали
	return packed
}

function knapsackDP(items, capacity) {
	// Створюємо таблицю
	const table = new Array(items.length + 1)

	// Заповнюємо перші два рядки таблиці
	for (let i = 0; i <= items.length; i++) {
		table[i] = new Array(capacity + 1).fill(0)
	}

	// Заповнюємо решту таблиці
	for (let i = 1; i <= items.length; i++) {
		for (let j = 1; j <= capacity; j++) {
			// Якщо вага предмета не перевищує максимально дозволену, то додаємо
його в рюкзак
			if (items[i - 1].weight <= j) {
				table[i][j] = Math.max(table[i - 1][j], table[i - 1][j - items[i - 1].weight] +
items[i - 1].value)
			} else {
				table[i][j] = table[i - 1][j]
			}
		}
	}

	// Повертаємо підмножину предметів, яка відповідає максимальному значенню в таблиці
	return getPackedItems(items, table, capacity)
}

// Створюємо структуру, яка буде представляти вузол дерева пошуку
class Node {
	constructor(value, weight, isPacked, left, right) {
		this.value = value
```

```
this.weight = weight
                this.isPacked = isPacked
                this.left = left
                this.right = right
        }
}

function bound(node, n, W, items) {
        if (node.weight >= W) return 0

        let profitBound = node.value
        let j = node.level + 1
        let totWeight = node.weight

        while (j < n && totWeight + items[j].weight <= W) {
                totWeight += items[j].weight
                profitBound += items[j].value
                j++
        }

        if (j < n) {
                profitBound += (W - totWeight) * (items[j].value / items[j].weight)
        }

        return profitBound
}

function knapsackBranchAndBound(items, W) {
        items.sort((a, b) => b.value / b.weight - a.value / a.weight)

        let Q = []
        let maxProfit = 0
        let n = items.length
        let u = new Node(-1, 0, 0)

        Q.push(u)

        while (Q.length !== 0) {
                u = Q.shift()

                if (u.level === n - 1) continue

                let v = new Node(u.level + 1, u.value, u.weight)

                // Перевіряємо наступний предмет
                if (v.level < n) {
                        v.weight += items[v.level].weight
                        v.value += items[v.level].value

                        if (v.weight <= W && v.value > maxProfit) {
                                maxProfit = v.value
                        }

                        v.bound = bound(v, n, W, items)

                        if (v.bound > maxProfit) {
```

```
                        Q.push(new Node(v.level, v.value, v.weight))
                    }
                }

                // Перевіряємо вузол без наступного предмета
                v.weight = u.weight
                v.value = u.value
                v.bound = bound(v, n, W, items)

                if (v.bound > maxProfit) {
                    Q.push(new Node(v.level, v.value, v.weight))
                }
            }

            return maxProfit
}

function getPackedItems(items, node, capacity) {
            let packed = []
            let i = items.length
            let j = capacity

            while (i > 0 && j > 0) {
                if (node.isPacked === true && items[i - 1].weight <= j) {
                    packed.push(items[i - 1])
                    j -= items[i - 1].weight
                }
                i--
            }

            return packed
}
function generateItems(count) {
            // Генеруємо випадкові ваги
            const weights = Array.from(Array(count), () => Math.random() * 10000)

            // Генеруємо випадкові вартості
            const values = Array.from(Array(count), () => Math.random() * 10000)

            // Створюємо масив предметів
            const items = []
            for (let i = 0; i < count; i++) {
                items.push({
                    weight: weights[i],
                    value: values[i]
                })
            }

            return items
}

function getPackedValue(items, packed) {
            let value = 0
            for (const item of packed) {
                value += item.value
            }
            return value
```

```
}

// Генеруємо 10000 предметів

// Максимальна вага рюкзака
const capacity = 10000

function doTest(itemsAmount) {
	for (const amount of itemsAmount) {
		const items = generateItems(amount)
		// Вимірюємо час виконання алгоритмів
		const greedyStart = performance.now()
		const greedyPacked = knapsack([...items], capacity)
		const greedyEnd = performance.now()

		const dpStart = performance.now()
		const dpPacked = knapsackDP([...items], capacity)
		const dpEnd = performance.now()

		const bbStart = performance.now()
		const bbPacked = knapsackBranchAndBound([...items], capacity)
		const bbEnd = performance.now()

		console.log(' ')
		console.log('Для загальної кількості елементів: ', amount)
		// Виводимо результати
		console.log('Жадібний пошук:')
		console.log('Час виконання: ' + (greedyEnd - greedyStart) + ' мс')

		console.log('Динамічна програмування:')
		console.log('Час виконання: ' + (dpEnd - dpStart) + ' мс')

		console.log('Метод гілок та меж:')
		console.log('Час виконання: ' + (bbEnd - bbStart) + ' мс')
	}
}

doTest([10, 100, 1000, 10000])
```