КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
Факультет комп'ютерних наук та кібернетики
Кафедра теорії та технології програмування

Кваліфікаційна робота

на здобуття ступеня бакалавра

за спеціальністю 122 Комп'ютерні науки

на тему:

ДЕЦЕНТРАЛІЗОВАНИЙ ВЕБЗАСТОСУНОК ДЛЯ ОБМІНУ КРИПТОВАЛЮТ

Виконав студент
4-го курсу
Богдан СТУКАЛО

(підпис)

Науковий керівник:
доктор фіз.-мат. наук, професор
Степан ШКІЛЬНЯК

(підпис)

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

Студент

(підпис)

Роботу розглянуто і допущено до захисту на засіданні кафедри теорії та технології програмування
«05» червня 2023 р.
протокол № 18
Завідувач кафедри
Микола НІКІТЧЕНКО

(підпис)

Київ – 2023

РЕФЕРАТ

Обсяг роботи: 66 сторінок, основний текст викладено на 51 сторінку, 18 рисунків, 6 додатків, 25 джерел посилань.

КРИПТОВАЛЮТА, ОБМІН КРИПТОВАЛЮТИ, ВЕБЗАСТОСУНОК, API, ETHEREUM, СМАРТ-КОНТРАКТ, БЛОКЧЕЙН.

Об'єктом роботи є процес обміну криптовалют в мережі Ethereum. Предметом роботи є програмний засіб, що дозволяє користувачам здійснювати обмін криптовалют безпосередньо через вебзастосунок в мережі Ethereum.

Метою роботи є розробка та реалізація вебзастосунку, який забезпечує обмін криптовалюти на базі мережі Ethereum.

Методи розроблення: теоретичне дослідження, проєктування та розробка вебзастосунку. Інструменти розроблення: операційна система: Windows 10, середовище програмування: Visual Studio Code, мови програмування: CSS, JavaScript з використанням фреймворку React для побудови користувацького інтерфейсу, JavaScript для реалізації взаємодії вебзастосунку з API та смарт-контрактами.

Результати роботи: проведено огляд технологій, що застосовуються в області блокчейну та криптовалюти, проаналізовано методи використання смарт-контрактів в блокчейн мережі Ethereum розроблено систему для здійснення обміну криптовалют.

Розроблений програмний продукт може використовуватися користувачами, які бажають здійснювати обмін криптовалют в мережі Ethereum.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА ВИЗНАЧЕНЬ

AMM (Automated Market Maker) – механізм, який використовується в децентралізованих фінансових протоколах для автоматичного створення та управління ліквідністю на основі алгоритмів. Він дозволяє користувачам обмінювати одну криптовалюту на іншу без потреби посередників.

AML (Anti-Money Laundering) – це набір правил та процедур, які фінансові установи та організації використовують для запобігання та виявлення відмивання грошей та фінансових злочинів.

CEX (Centralized exchange) – централізована біржа;

DApps (Decentralized apps) – децентралізовані застосунки;

DeFi (Decentralized finances) – екосистема фінансових застосунків, які працюють на блокчейні та надають фінансові послуги без посередництва традиційних фінансових установ;

DEX (Decentralized exchange) – децентралізована біржа;

ICO (Initial coin offering) – метод залучення фінансування, де компанії випускають нові криптовалюти або токени та продають їх для залучення інвестицій;

KYC (Know Your Customer) – це процес перевірки та ідентифікації клієнтів, який фінансові установи виконують для забезпечення відповідності правилам та обмеженням, а також для виявлення можливої фінансової злочинної діяльності;

NFT (Non-fungible token) – це унікальний токен на основі блокчейну, який не може бути замінений або замінений іншим токеном, оскільки має унікальні характеристики та властивості, що дають можливість відстежувати власність і автентичність цифрових активів, таких як мистецтво, музика,

відео тощо;

POS (Proof-of-stake) – це алгоритм консенсусу, в якому учасники мережі вкладають свої монети в гаманці для отримання права на створення нових блоків відповідно до розміру їхнього стейку;

POW (Proof-of-work) – це алгоритм консенсусу, в якому учасники мережі витрачають обчислювальну потужність на вирішення складних математичних задач для підтвердження та створення нових блоків.

ВСТУП

Оцінка сучасного стану об’єкта розробки. На сьогоднішній день криптовалюти набувають все більшої популярності та зацікавленості як серед індивідуальних користувачів, так і серед компаній та фінансових установ. Це відбувається через переваги криптовалют, такі як децентралізація, приватність, швидкість та низькі комісії. Ринок обміну криптовалют розширюється швидкими темпами, з'являються нові обмінні платформи та сервіси, що надають можливість торгувати та обмінювати різні криптовалюти. Однак, багато з цих платформ є централізованими біржами (CEX), що може вплинути на безпеку та контроль користувачів над їх активами. У сфері обміну криптовалют є декілька важливих викликів, зокрема, безпека, швидкість та надійність операцій, прозорість, легкість використання та інтеграція з різними блокчейн-мережами. Багато обмінних платформ також мають обмеження щодо доступності та регулювання, що можуть ускладнити обмін та використання криптовалют. В останні роки децентралізовані біржі (DEX) стали популярними варіантами для обміну криптовалют. DEX дозволяють користувачам здійснювати прямі обміни без посередництва централізованих організацій, забезпечуючи більшу безпеку, контроль над приватними ключами та прозорість операцій.

Актуальність роботи та підстави для її виконання. Криптовалюти, такі як Bitcoin, Ethereum та інші, зарекомендували себе як інноваційний та перспективний фінансовий інструмент [1]. Зростання інтересу до криптовалют супроводжується потребою в зручних та надійних вебзастосунках для обміну криптовалютами, що викликає актуальність розробки вебзастосунку для обміну криптовалют. Централізовані обмінні платформи, які зараз широко використовуються для обміну криптовалют, мають свої недоліки, такі як вразливість до кібератак, ризик втрати коштів, обмеженість доступу та

потенційна цензура. Розробка децентралізованого вебзастосунку для обміну криптовалют може вирішити ці проблеми, надаючи користувачам більшу безпеку, контроль над власними активами та відсутність посередників. На сучасному ринку криптовалют існує потреба в розробці вебзастосунків, які не тільки надають можливість обміну криптовалют, але й мають додатковий функціонал для управління портфелем, аналізу ринку, надання статистики тощо. Такий розширений вебзастосунок може забезпечити зручність та ефективність у використанні для користувачів криптовалют. Отже, актуальність розробки вебзастосунку для обміну криптовалют випливає зі зростання популярності криптовалют, потреби у зручних рішеннях для обміну, проблем централізованих платформ та потреби у розширеній функціональності та зручності для користувачів.

Мета й завдання роботи. Головною метою цієї роботи є розробка вебзастосунку на блокчейні Ethereum, який надає можливість користувачам обмінювати криптовалюти, відображає статистику актуальних цін для криптовалюти та має інтеграцію функціоналу відстеження поточного газу в мережі Ethereum, який необхідний для проведення транзакції. Для досягнення цієї мети поставлено такі завдання:

- провести дослідження наявних систем та технологій, які дозволяють обмінювати криптовалюти, з метою отримання глибшого розуміння їх принципів та функціоналу;
- поглибити знання у криптографії та блокчейн-технологіях, щоб мати достатній рівень експертизи для розробки та впровадження вебзастосунку для обміну криптовалют;
- реалізувати використання смарт-контракту, який відповідатиме алгоритму обміну криптовалют та забезпечуватиме автоматизовану обробку транзакцій;

● розробити інтерфейс вебзастосунку, який дозволятиме користувачам обмінювати криптовалюти, отримувати актуальну інформацію про газ в мережі Ethereum, а також актуальні ціни криптовалют, динаміку їх зросту чи падіння та ринкову капіталізацію;

● реалізувати необхідні операції для взаємодії з мережею Ethereum, зокрема для роботи з DEX, забезпечуючи можливість виконання транзакцій, доступ до контрактів;

● навести приклади застосування розробленого вебзастосунку для обміну криптовалют, демонструючи його потенціал та переваги у реальних ситуаціях.

Об'єкт, методи й засоби розроблення. Об'єктом кваліфікаційної роботи є процес обміну криптовалют в мережі Ethereum. Предметом роботи є розроблений програмний засіб, що дозволяє користувачам здійснювати обмін криптовалютами безпосередньо через вебзастосунок в мережі Ethereum.

Реалізації програмного засобу передувало проєктування системи та дослідження смарт-контрактів. Розробка ґрунтувалась на результатах досліджень методів та алгоритмів, що використовуються для обміну криптовалют. Були вивчені особливості мережі Ethereum, механізм розробки та виконання смарт-контрактів в загальному контексті та в контексті блокчейну Ethereum.

Для розробки основної частини програмного продукту було використано такі мови програмування: CSS, JavaScript та React для фронтенду, та JavaScript для бекенду, що включає роботу зі смарт-контрактами та API. Використання CSS, JavaScript та React у фронтенді дозволяє створювати інтуїтивно зрозумілий та естетичний користувацький інтерфейс, а також забезпечує динамічну поведінку сторінки. JavaScript використовується також у бекенді для роботи зі смартконтрактами, які виконують логіку обміну, та для взаємодії з API, що дозволяє отримувати актуальну інформацію про криптовалюти та їхні ціни.

Розробка програмного забезпечення проводилась на операційній системі Windows 10. Для створення проєкту було використано середовище розробки Visual Studio Code.

Можливі сфери застосування. Вебзастосунок для обміну криптовалют може служити як платформа для торгівлі різними криптовалютами та токенами. Він надає можливість користувачам купувати, продавати та обмінювати криптовалюти з іншими учасниками мережі, забезпечуючи швидкі, безпечні та децентралізовані операції. Також застосунок може надавати різноманітні інструменти для аналізу ринку, трекінгу цін токенів, газу в мережі Ethereum. Це дозволяє користувачам відстежувати рухи цін, знаходити можливості для торгівлі та приймати обґрунтовані рішення щодо криптовалютних операцій.

РОЗДІЛ 1. БЛОКЧЕЙН ТЕХНОЛОГІЇ

У 2009 році блокчейн технології вийшли з експериментального стану і стали суттєвою інновацією в цифровому світі. Їх революційна сила проявляється у забезпеченні децентралізації, безпеки та надійності обміну інформацією та активами між учасниками мережі. В основі блокчейну лежить концепція розподіленого реєстру, де дані зберігаються в блоках, що містять хеш-посилання на попередній блок, створюючи ланцюжок блоків. Ця технологія вже знайшла застосування в багатьох галузях, включаючи фінанси, мистецтво, благодійність, надаючи нові можливості для безпеки, прозорості та ефективності. Розуміння блокчейну є ключовим для розуміння потенціалу цієї інноваційної технології та її впливу на майбутнє цифрового світу.

1.1 Загальний огляд

Блокчейн – це база даних транзакцій, яка оновлюється та спільно використовується багатьма комп'ютерами у мережі [2]. Кожного разу, коли додається новий набір транзакцій, його називають "блоком", а оскільки дані, що зберігаються в блоці містять посилання на попередній блок, вони утворюють ланцюг "чейн" – звідси походить термін блокчейн. На рис. 1.1 наведене схематичне зображення блокчейна, де кожен блок складається з наступних елементів:

1) Заголовок (Header): використовується для ідентифікації конкретного блоку в усьому ланцюжку блокчейну. Він обробляє всі блоки в блокчейні. Також в заголовку блоку містяться три набори метаданих блоку.
2) Попередня адреса/хеш блоку (Previous Block Address/Hash): використовується для з'єднання $i+1$-го блоку з i-м блоком за допомогою

хешу (посилання на хеш попереднього (батьківського) блоку в ланцюжку).

3) Відмітка часу (Timestamp): це рядок символів, який унікально ідентифікує документ або подію та вказує, коли він був створений. Система перевіряє дані в блоку та призначає час або дату створення.

4) Число Nonce (Nonce): номер Nonce, який використовується лише один раз. Це центральна частина доказу роботи в блоку. Він порівнюється з актуальною ціллю, якщо він менший або рівний поточній цілі.

5) Корінь Меркля (Merkle Root): це тип структури даних, який складається з різних блоків даних. Дерево Меркля зберігає всі транзакції в блоку, створюючи цифровий відбиток усієї транзакції. Воно дозволяє користувачам перевіряти, чи може транзакція бути включена до блоку чи ні.

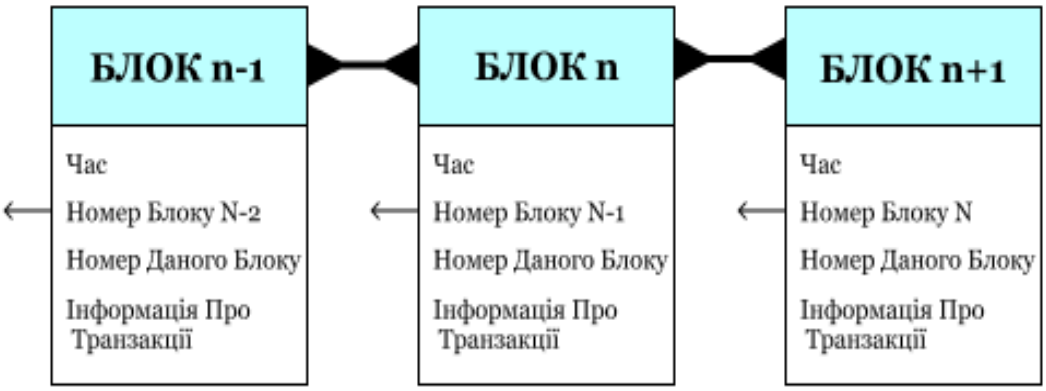


Рисунок 1.1 – Схематичне зображення блокчейну

Більшість блокчейнів є публічними, ви можете лише додавати дані, але не видаляти їх. Якщо хтось хотів би змінити будь-яку інформацію або використати систему зловмисним способом, він мусить це зробити на більшості комп'ютерів у мережі, що являє собою складно реалізовану задачу. Саме це робить

блокчейни, такі як Ethereum та Bitcoin, високобезпечними.

Основні характеристики блокчейну включають в себе наступні аспекти:

1) Децентралізація: блокчейн не має центральної влади або управління. Він заснований на розподіленій мережі вузлів, які спільно підтримують та перевіряють блокчейн. Децентралізована система має розподілений контроль та владу між різними учасниками або вузлами, що дозволяє уникнути одного центрального пункту контролю та прийняття рішень. У такій системі рішення приймаються локально, а ресурси та влада розподілені серед учасників. Це забезпечує більшу прозорість, надійність та стійкість до вторгнень. Схематичне порівняння централізованої та децентралізованої системи зображено на рис. 1.2.

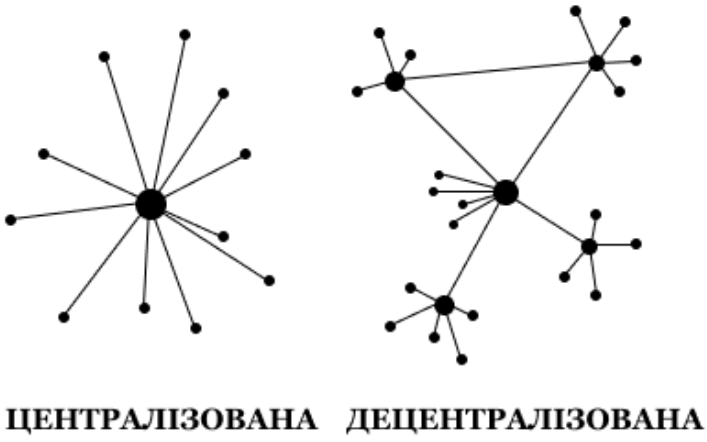


Рисунок 1.2 Централізована та децентралізована система

2) Незмінність: коли інформація додається до блокчейну, вона стає майже неможливою до зміни або видалення. Це забезпечує безпеку і надійність даних.

3) Криптографічна безпека: блокчейн використовує криптографію для захисту даних та забезпечення безпеки транзакцій. Хеш-функції та підписи

забезпечують конфіденційність та цілісність даних.

4) Консенсус: блокчейн використовує консенсусні протоколи для досягнення згоди між вузлами мережі щодо стану блокчейну. Це дозволяє уникнути подвійного витрати та забезпечити правильність транзакцій. Консенсусні протоколи - це механізми, які використовуються в блокчейні для досягнення згоди між різними вузлами мережі щодо стану блокчейну та правильності транзакцій. Деякі з найпоширеніших консенсусних протоколів включають PoW та PoS.

5) Відкритий доступ: переважно блокчейни є відкритими, що означає, що будь-хто може приєднатися до мережі, переглядати та виконувати операції в блокчейні.

Існує достатня кількість блокчейнів, які використовуються у різних сферах. Найвідомішими з них є Bitcoin та Ethereum, про що свідчить ринкова капіталізація, де Bitcoin стабільно займає перше місце, а Eth – друге місце [3]. Отже, розглянемо їх детальніше.

Bitcoin є першим і найвідомішим криптовалютним блокчейном. Він був запущений в 2009 році під керівництвом Сатоші Накамото [4]. Bitcoin використовує консенсусний алгоритм Proof-of-Work (PoW). PoW – це алгоритм, де майнери витрачають обчислювальну потужність на розв'язання складних завдань, щоб підтвердити нові блоки в блокчейні. Кожен блок містить список транзакцій, підписаних цифровими підписами, та посилання на попередній блок у формі хешу. Це забезпечує незмінність даних в блокчейні Bitcoin [4].

Ethereum є відкритою блокчейн-платформою, яка дозволяє розробникам створювати та виконувати смарт-контракти [2]. Він був запущений у 2015 році і став одним з найпопулярніших та найбільш впливових блокчейнів: на якому побудована вагома кількість розвинутих застосунків dApp [5].

Початково, Ethereum використовував алгоритм доказу роботи, подібний до біткоїна, де валідатори витрачали обчислювальну потужність для розв'язання складних математичних завдань (алгоритм консенсусу PoW). Успішне вирішення цих завдань дозволяло їм додавати нові блоки до блокчейну та отримувати ефіри як нагороду за свою працю. Проте, цей підхід має певні недоліки, такі як високе енергоспоживання та обчислювальну складність. Тому Ethereum перейшов з алгоритму консенсусу PoW на PoS, що означає перехід до алгоритму доказу володіння.

PoS – це алгоритм консенсусу, в якому володіння криптовалютою визначає право на створення та підтвердження нових блоків в блокчейні [6]. Учасники мережі, які утримують певну кількість монет, відомі як "стейкери", мають шанс бути обраними для генерації нового блоку пропорційно до свого володіння. Замість розрахунку складних математичних задач, як у випадку PoW (Proof of Work), стейкери використовують свої монети як гарантію надійності мережі. Перехід на PoS має декілька переваг, включаючи зменшення енергозатрат, високу масштабованість та більшу ефективність використання ресурсів. Цей алгоритм дозволяє забезпечити швидкі транзакції та низькі комісії, що робить його привабливим для використання в блокчейн-мережах [2].

1.2 Роль мережі Ethereum в контексті криптовалют та блокчейн технологій

Мережа Ethereum відіграє важливу роль в контексті криптовалют та блокчейн технологій. Це доводить наступна статистика:

1) Кількість побудованих децентралізованих застосунків в екосистемі Ethereum – більш ніж 4000 dApp [5];
2) Середня кількість транзакцій на добу – 1.073млн. [2];

3) Вартість активів що знаходяться у децентралізованих фінансових застосунках (DeFi), в економіці цифрової платформи Ethereum - 50.63млрд долларів [2];

Однією з головних відмінностей мережі Ethereum в порівнянні з Bitcoin є ширші можливості створення та виконання смарт-контрактів [6]. Смарт-контракти є програмними кодами, що автоматизують виконання угод та умов між різними сторонами. Вони дозволяють створювати розумні децентралізовані застосунки (DApps), які можуть бути використані для різноманітних цілей, від фінансових послуг до голосування та ланцюжка постачання. Завдяки своїй гнучкості та широкому спектру можливостей, мережа Ethereum стала платформою вибору для розробників та проектів у галузі блокчейн технологій. Вона сприяє інноваціям, децентралізації та побудові нових економічних моделей. Багато успішних проектів, включаючи Initial Coin Offerings (ICO) та Decentralized Finance (DeFi), реалізовані на базі мережі Ethereum.

Мережа Ethereum, окрім своєї ролі в контексті криптовалют та блокчейн технологій, має широкий спектр застосувань у різних галузях. Ось декілька прикладів:

1) Смарт-контракти та децентралізовані застосунки (DApps): Ethereum надає розробникам можливість створювати смарт-контракти, які можуть автоматизувати угоди та процеси без посередництва. Це дає можливість для створення та розвитку додатків на різні тематики, включаючи фінансові послуги, ігри, мистецтво.

2) Децентралізовані фінанси (DeFi): Ethereum є основою для розробки різноманітних фінансових додатків, які працюють на основі блокчейну. Такі проєкти, як протоколи для кредитування, обміну та ставок, дозволяють користувачам отримувати фінансові послуги без посередників на основі

технології блокчейну.

3) Розподілене обчислення та хмарні послуги: Ethereum може використовуватися для розподіленого обчислення, де кілька комп'ютерів працюють разом для виконання складних завдань. Це може мати застосування в певних галузях наукових досліджень, аналізі даних та обробці великих обсягів інформації.

4) Управління цифровими активами: Ethereum надає можливість створювати та управляти цифровими активами, які можуть бути використані для репрезентації реальних активів, таких як нерухомість, мистецтво чи права власності. Це дозволяє створювати нові форми власності та торгівлі цифровими активами.

1.3 Смарт-контракти в мережі Ethereum

Смарт-контракт для Ethereum – це програма, написана на мові програмування Solidity, яка зберігається на блокчейні Ethereum і автоматично виконує угоди або домовленості, записані в ньому [7].

Мова програмування Solidity була спеціально розроблена для роботи з блокчейном. Solidity надає розширений функціонал для опису логіки смарт-контрактів, включаючи обробку транзакцій, управління станом, виконання умовних операцій та багато іншого [7]. Смарт-контракти в Ethereum зберігаються на блокчейні і мають власну адресу. Вони можуть містити логіку, умови виконання, функції та дані.

Основна перевага смарт-контрактів в Ethereum – це їхнє автоматизоване виконання без необхідності довіряти третім особам. Вони дозволяють забезпечити безпеку, незмінність та прозорість угод, оскільки кожна операція записується на блокчейні і перевіряється всіма вузлами мережі.

Смарт-контракти в мережі Ethereum використовуються для різних цілей, таких як децентралізовані фінансові послуги (DeFi), створення токенів, децентралізовані біржі, голосування та управління громадськими ресурсами. Вони відкривають широкі можливості для розробників та користувачів, щоб створювати та використовувати різноманітні децентралізовані застосунки.

Звичайним прикладом смарт-контракту може бути контракт ордера на купівлю/продаж активу. В цьому прикладі, дві сторони (покупець і продавець) укладають угоду через смарт-контракт, що автоматично виконує обмін активами при виконанні певних умов. Наприклад, може бути створений смарт-контракт для купівлі/продажу токенів. Покупець визначає кількість токенів, яку він хоче придбати, і встановлює ціну, за якою він готовий купити. Продавець, у свою чергу, вказує кількість токенів, яку він хоче продати, і ціну продажу. Коли ці дві сторони укладають угоду, і ціна покупки співпадає з ціною продажу, смарт-контракт автоматично переводить власність токенів від продавця до покупця, а відповідний платіж у криптовалюті здійснюється від покупця до продавця.

Смарт-контракти дозволяють автоматизувати процес укладання угод і забезпечують незмінність та безпеку операцій. Всі умови угоди кодуються в смарт-контракті, що дозволяє сторонам уникати потенційних суперечок або міжособових непорозумінь.

1.4 Переваги і недоліки використання блокчейн технологій

Використання блокчейн-технологій має свої переваги і недоліки, які варто розглянути.

Переваги використання блокчейн технологій:

1) Децентралізація: блокчейн дозволяє уникнути централізованих

посередників, забезпечуючи прямі пірингові з'єднання між учасниками мережі.

2) Безпека: блокчейн забезпечує високий рівень безпеки за рахунок криптографічних протоколів та розподіленої природи мережі.

3) Прозорість: блокчейн діє як публічний реєстр, до якого всі учасники мережі мають доступ, що забезпечує прозорість операцій.

4) Надійність: блокчейн має вбудовану механіку перевірки та підтвердження транзакцій, що дозволяє уникнути фальсифікації та маніпуляцій.

5) Ефективність: використання блокчейн технологій може спростити та прискорити процеси, які раніше вимагали багато проміжних кроків та затрат.

Недоліки використання блокчейн технологій:

1) Масштабованість: Деякі блокчейн мережі можуть мати обмежену масштабованість, що обмежує їх потенційне використання у великому обсязі операцій.

2) Витрати: Запуск та підтримка блокчейн мереж може вимагати значних витрат на обладнання та енергію.

3) Приватність: Хоча блокчейн забезпечує прозорість, це може порушувати приватність учасників мережі, що може бути неприйнятним для деяких сфер діяльності.

4) Регуляторна неоднозначність: Існують питання стосовно регуляторного статусу блокчейн технологій, що може створювати правові ризики та неоднозначності.

1.5 Переваги та недоліки у використанні DEX і CEX

DEX (Decentralized Exchange) та CEX (Centralized Exchange) – це два основних типи криптовалютних обмінників.

DEX (Decentralized Exchange) є децентралізованою платформою для обміну криптовалют, де торгівля відбувається без необхідності довіряти централізованому посереднику. У DEX, торгівля відбувається безпосередньо між учасниками за допомогою смарт-контрактів на блокчейні. DEX надають користувачам більшу приватність, безпеку та контроль над їхніми коштами [8].

Переваги платформи DEX:

1) Децентралізація: DEX працюють на основі блокчейн технологій і не потребують посередницьких організацій. Це означає, що користувачі мають повний контроль над своїми коштами та приватністю.

2) Безпека: Транзакції в DEX відбуваються безпосередньо між учасниками без необхідності довіряти централізованому посереднику. Це знижує ризик втрати коштів внаслідок хакерських атак або шахрайства.

3) Відкритість та прозорість: DEX базуються на блокчейн технології, що забезпечує прозорість операцій та відкритий доступ до даних. Користувачі можуть перевірити транзакції та стан ринку в реальному часі.

Недоліки платформи DEX:

1) Обмежена ліквідність: У порівнянні з CEX, децентралізовані обмінники можуть мати обмежену ліквідність на деякій криптовалютній парі, оскільки торгівля відбувається між учасниками мережі.

2) Обмежені функціональні можливості: Деякі функціональності, такі як маржева торгівля або відкладені замовлення, можуть бути обмежені в DEX через його децентралізовану природу.

CEX (Centralized Exchange) є централізованою платформою для обміну криптовалют, де торгівля відбувається через посередництво централізованої організації. У CEX, користувачі довіряють свої кошти та особисті дані платформі, яка виконує роль посередника в обмінних операціях. CEX зазвичай

мають вищу ліквідність та розширений функціонал, але можуть потребувати більшої верифікації та втручання з боку посередників.

Переваги платформи CEX:

1) Висока ліквідність: централізовані обмінники часто мають значно вищий рівень ліквідності, оскільки вони об'єднують торгові замовлення з багатьох користувачів.

2) Розширений функціонал: CEX зазвичай надають широкий спектр функціональних можливостей, включаючи маржеву торгівлю, ордер-бук, інструменти аналізу ринку та інші.

Недоліки платформи CEX:

1) Централізований контроль: У CEX користувачі мають довіряти платформі збереження своїх коштів, що може створювати ризик безпеки та недовіри.

2) Менша приватність: Використання CEX може потребувати проходження процедур верифікації та надання особистих даних.

Порівняння платформ DEX та CEX:

1) DEX забезпечують більшу приватність та безпеку, оскільки не потребують довіри до централізованого посередника.

2) CEX можуть мати вищу ліквідність та більш розширений функціонал.

3) DEX пропонують більш прозору та децентралізовану модель, водночас CEX можуть мати кращий інтерфейс та більш зручний процес торгівлі.

1.6 Криптовалютні гаманці

Криптовалютний гаманець – це програмне або апаратне забезпечення, яке дозволяє зберігати, керувати та пересилати криптовалюту. Гаманець містить

пари криптографічних ключів: приватний ключ, який дозволяє власнику гаманця підписувати транзакції, та публічний ключ, який використовується для отримання платежів.

Гаманці можуть бути реалізовані у різних форматах:

1) Програмні гаманці: Це програми, які встановлюються на комп'ютер або мобільний пристрій. Вони надають інтерфейс для зберігання та керування криптовалютою. Прикладами програмних гаманців є Metamask, Argent, Phantom, Trust Wallet та багато інших. Наприклад, в Trust Wallet серед опцій керування є наступні: купівля криптовалюти, підтримка децентралізованих фінансових застосунків (DeFi), перегляд NFT в гаманці, обмін токенів та стейкінг [9].

2) Апаратні гаманці: Це пристрої, спеціально розроблені для зберігання криптовалюти. Вони забезпечують високий рівень безпеки, оскільки приватні ключі зберігаються у фізичному пристрої та не викриваються в Інтернеті. Деякі популярні апаратні гаманці включають Ledger Nano S, Trezor, KeepKey та інші.

Також варто зазначити, що гаманець може мати різні типи інтерфейсів: веб-інтерфейс, мобільний додаток, десктопний додаток або навіть командний рядок.

Чи може бути гаманець без інтерфейсу? Так, існують так звані "холодні" гаманці, які зазвичай є апаратними гаманцями. Вони не мають прямого підключення до Інтернету і забезпечують зберігання приватних ключів офлайн. Вони використовуються з метою забезпечення вищого рівня безпеки шляхом збереження ключів у відокремленому фізичному пристрої.

Прикладом одного з найрозповсюдженіших гаманців є Metamask. Він є популярним програмним гаманцем для криптовалюти Ethereum та децентралізованих застосунків, який надає інтерфейс у веб-браузері [10].

Користувачі можуть встановити Metamask як розширення для браузера та використовувати його для зберігання криптовалюти, підпису транзакцій та взаємодії з децентралізованими застосунками на базі Ethereum.

РОЗДІЛ 2. ТЕОРЕТИЧНЕ ОБҐРУНТУВАННЯ

У сучасному цифровому середовищі криптовалюти стали значною частиною фінансової системи та привертають увагу як інвесторів, так і користувачів. Один з важливих аспектів використання криптовалют – це їх обмін між різними акторами. З метою спрощення та автоматизації процесу обміну криптовалют виникла необхідність у розробці вебзастосунків, які забезпечують зручний та безпечний обмін криптовалют між користувачами.

2.1 Загальний огляд та вимоги до вебзастосунків для обміну криптовалют

Вебзастосунок для обміну криптовалют – це онлайн-сервіс, який надає можливість користувачам обмінювати різні види криптовалют [3]. Він забезпечує інтерфейс для взаємодії з криптовалютними гаманцями, дозволяючи користувачам здійснювати операції з криптовалютами за допомогою зручного і інтуїтивно зрозумілого інтерфейсу.

Вебзастосунок для обміну криптовалюти може бути розроблений у вигляді CEX або DEX. Оскільки принципи роботи децентралізованого та централізованого обмінника відрізняються – відповідно відрізняються і вимоги до них.

Основними вимогами для CEX є:

1) Реєстрація та перевірка користувачів: централізований обмінник повинен мати процес реєстрації користувачів, що включає процедуру верифікації особи для дотримання правил Анти-відмивання грошей (AML) і Захисту особистих даних (KYC).
2) Централізоване управління коштами: на CEX кошти користувачів зберігаються на централізованому гаманці, контроль над яким має обмінник. Користувачі використовують цей гаманець для здійснення

торгівлі криптовалютами.

3) Забезпечення ліквідності: централізовані обмінники забезпечують ліквідність на своїх платформах, шляхом укладання угод з ринковими ліквідаторами або залученням маркет-мейкерів.
4) Управління безпекою: CEX відповідають за забезпечення безпеки коштів користувачів шляхом застосування різноманітних заходів безпеки, таких як захист від хакерських атак та зловживань [11].

Основними вимогами для DEX є:

1) Розробка смарт-контрактів: DEX використовують смарт-контракти для виконання обміну криптовалют. Розробники повинні мати знання Solidity або інших мов програмування смарт-контрактів, а також розуміння блокчейн-технологій.
2) Інтеграція з блокчейн: DEX повинні бути здатні взаємодіяти зі специфічним блокчейном, зазвичай Ethereum. Розробники повинні мати розуміння роботи блокчейну, механізмів транзакцій та розробки додатків на блокчейні.
3) Інтеграція криптовалютного гаманця: DEX повинні мати можливість інтегруватися з криптовалютними гаманцями, щоб дозволити користувачам безпосередньо управляти своїми криптовалютами під час обміну. Це важливий функціонал, який дозволяє забезпечити зручну та безпечну передачу активів та сприяти високому рівню контролю користувачів над їхніми коштами.
4) Інтерфейс користувача: DEX повинні мати інтуїтивно зрозумілий та зручний інтерфейс користувача, що дозволяє легко взаємодіяти з функціями обміну криптовалют.
5) Ліквідність: розробники DEX повинні створити механізми для забезпечення ліквідності, наприклад, за допомогою протоколів

децентралізованої ліквідності (наприклад, AMM). Це дозволить користувачам здійснювати обмін криптовалют уникаючи проблем, пов’язаних з нестачею ліквідності [12].

З вищевказаного можна зробити висновок, що CEX і DEX мають свої відмінності в термінах архітектури, ліквідності, контролю над активами та безпеки, що впливає на функціональність та спосіб взаємодії з користувачами.

2.2 Інтеграція криптовалютного гаманця

Інтеграція криптовалютного гаманця в DEX є важливим аспектом розробки та функціоналу таких платформ. Цей процес передбачає забезпечення можливості безпосередньої взаємодії користувачів з їхніми криптовалютними активами, які зберігаються у їхніх гаманцях. Інтеграція гаманця дозволяє користувачам контролювати та управляти своїми коштами під час обміну на DEX.

Цей процес інтеграції включає розробку інтерфейсу, який забезпечує взаємодію між DEX та криптовалютним гаманцем. Вона може включати функції, такі як автоматична синхронізація балансу гаманця з DEX, можливість перегляду та керування активами у гаманці, а також безпосереднє виконання транзакцій з використанням гаманця. Для забезпечення безпеки та конфіденційності, інтеграція гаманця може вимагати використання криптографічних протоколів та засобів аутентифікації.

Інтеграція криптовалютного гаманця в DEX відкриває нові можливості для користувачів, дозволяючи їм безпосередньо управляти своїми активами під час торгівлі, збільшуючи рівень контролю та безпеки. Цей функціонал стає важливою складовою децентралізованих обмінників криптовалют, дозволяючи користувачам користуватися перевагами децентралізації, забезпечуючи одночасно зручність та безпеку обміну криптовалют [13].

2.3 Смарт-контракт для обміну криптовалюти

Смарт-контракт для обміну криптовалюти в децентралізованому обміннику криптовалют (DEX) є ключовим компонентом, який забезпечує автоматизований процес обміну активів між учасниками мережі. Цей смарт-контракт має на меті забезпечити безпечний та надійний обмін криптовалют без посередників.

У розробці смарт-контракту для обміну криптовалюти в DEX використовуються мови програмування, такі як Solidity, яка є найпоширенішою мовою програмування для смарт-контрактів на платформі Ethereum [7]. Смарт-контракт визначає правила обміну, включаючи ціну, обсяг та умови обміну між двома сторонами.

Смарт-контракт для обміну криптовалют в DEX може мати вбудовані функції, які забезпечують безпеку та цілісність транзакцій. Деякі з таких функцій можуть включати:

1) Блокування коштів: смарт-контракт може використовувати механізми блокування коштів, щоб забезпечити, що обидві сторони виконують свої зобов'язання перед обміном. Це дозволяє уникнути ситуацій, коли одна сторона не виконує своїх зобов'язань.
2) Перевірка балансу: смарт-контракт може містити логіку перевірки балансу користувача перед здійсненням транзакції. Це допомагає запобігти виконанню недостатньо фінансово забезпечених транзакцій.
3) Автоматична маркет-мейкер система: у деяких смарт-контрактах використовується автоматична маркет-мейкер система, яка автоматично встановлює ціни та забезпечує ліквідність для торгівлі. Це дозволяє учасникам безпосередньо обмінюватися криптовалютами без потреби залучення посередників [2].

Для розробки смарт-контракту для обміну криптовалюти в DEX

необхідно враховувати особливості платформи, на якій він буде використовуватись, а також забезпечити високу безпеку та надійність контракту. Крім того, важливо провести тестування та аудит смарт-контракту, щоб переконатись в його правильному функціонуванні та відсутності вразливостей.

2.4 Основні принципи роботи DEX

Децентралізовані обмінники криптовалют (DEX) працюють на основі різних принципів, які забезпечують їх функціонування. У цьому розділі будуть розглянуті два основних принципи роботи DEX: автоматична маркет-мейкер система (AMM) та система замовлень (order book).

Автоматична маркет-мейкер система (AMM) – автоматична маркет-мейкер система є одним з ключових елементів DEX [14]. Ця система використовує смарт-контракти для автоматичного встановлення цін і забезпечення ліквідності на платформі обміну. AMM використовує формулу, яка визначає ціну активів на основі співвідношення їх обсягів у різних торгових парах. Це дозволяє учасникам безпосередньо обмінюватися криптовалютами, не розраховуючи на традиційну систему замовлень та посередників.

Розглянемо механізм пулів ліквідності для AMM. У пулах ліквідності для AMM вкладники мають можливість внести свої активи у вирівнювальний пул, використовуючи певний відсоток кожного активу. При обміні активів між учасниками, цей пул забезпечує необхідну ліквідність та ціновий розрахунок за допомогою математичних формул.

Наприклад, уявімо, що пул AMM містить два активи: Ethereum (ETH) і DAI. Пул має певний розподіл активів, наприклад, 50% ETH і 50% DAI. Учасники можуть внести свої активи в пул відповідно до цього розподілу.

Якщо користувач бажає обміняти 1 ETH на DAI, він надсилає 1 ETH в пул. Оскільки пул має встановлений розподіл активів, автоматично буде визначено, скільки DAI буде надано користувачу в обмін на його 1 ETH, враховуючи поточні ціни і розподіл активів в пулі.

Цей механізм дозволяє учасникам безпосередньо обмінюватися активами в пулі, без необхідності шукати контрагента для обміну. При цьому, через математичні формули, ціна активів автоматично розраховується з урахуванням стану пулу.

До переваг AMM можна віднести:

1) Ліквідність: AMM дозволяє забезпечити постійну ліквідність на платформі обміну, оскільки вона не залежить від наявності контрагентів для кожної торгівельної пари. Це забезпечує учасникам можливість безперервно обмінювати активи за актуальними цінами.
2) Зменшення впливу ринкових маніпуляцій: оскільки AMM використовує математичні формули для визначення цін, вона зменшує можливість ринкових маніпуляцій, таких як штучне зміщення цін або збиткові угоди [14].
3) Простота використання: AMM дозволяє користувачам безпосередньо обмінювати активи, не потребуючи складних процедур розміщення замовлень. Це робить процес торгівлі більш доступним для новачків і зменшує бар'єри входу.

До недоліків AMM можна віднести:

1) Імперманентні втрати: при використанні AMM користувачі можуть зіткнутися з імперманентними втратами у випадку стрімкого зросту ціни одного з активів. Це означає, що вартість їхніх активів може змінитися під час обміну через коливання цін, що може призвести до зменшення їхнього загального вартості.

2) Високі комісії: деякі AMM можуть вимагати високих комісій за транзакції на блокчейні. Це може стати обмеженням для менших торгових обсягів або частої торгівлі.

Система замовлень (order book) – деякі DEX також використовують систему замовлень, схожу на ту, що використовується на централізованих біржах. У цій системі користувачі можуть розміщувати замовлення на купівлю або продаж активів з вказаною ціною і обсягом. Замовлення реєструються у публічному order book, і якщо ціна і обсяг відповідають, тоді відбувається автоматичний обмін [15]. Цей підхід дозволяє учасникам самостійно встановлювати ціни та управляти своїми замовленнями.

До переваг Order Book можна віднести:

1) Контроль над цінами: Order Book дає можливість трейдерам встановлювати власні ціни купівлі або продажу активів. Вони можуть встановлювати лімітні замовлення зі специфічними цінами, що дозволяє їм контролювати вартість своїх торгівельних операцій.
2) Глибина ринку: Order Book дозволяє відображати глибину ринку, тобто кількість активів, доступних для купівлі або продажу за різними цінами. Це дозволяє трейдерам бачити попит та пропозицію на ринку та приймати обґрунтовані рішення щодо своїх торговельних стратегій.

До недоліків Order Book можна віднести:

1) Ризик маніпуляцій: Order Book вразливий до різних видів маніпуляцій, таких як ордерботи, фронтраннінг та інші схеми, які можуть використовуватись зловмисниками для отримання нечесної переваги.
2) Залежність від технічних аспектів блокчейну: Order Book у DEX працюють на базі блокчейну, і їх ефективність та швидкість можуть залежати від технічних обмежень та масштабування самого блокчейну. Це може призводити до затримок та перебоїв у виконанні замовлень.

РОЗДІЛ 3. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

3.1 Огляд проблеми

Огляд переваг та недоліків існуючих децентралізованих бірж має вирішальне значення для розробки ефективного та зручного вебзастосунку DEX. Актуальність такого дослідження полягає в необхідності зрозуміти переваги та недоліки, що присутні у сучасних децентралізованих біржах, з метою покращення та впровадження нових практик. Цей науковий дослід спрямований на аналіз деяких найпопулярніших DEX на ринку, для встановлення ключових факторів успіху, а також ідентифікації потенційних обмежень та недоліків, що можуть бути покращені у розроблюваному нами DEX.

3.2 Огляд застосунку Curve Finance

Curve Finance є децентралізованим обмінником, що спеціалізується на обміні стейблкоїнов (стабільних криптовалют, які прив'язані до реальних активів або валют) [16]. Він набув великої популярності в Ethereum-спільноті завдяки своїй унікальній функціональності та можливостям.

На перший погляд, інтерфейс Curve має зрозумілу структуру з основними елементами, такими як поля для вибору токенів, розрахунку обміну та відображення відповідних даних (див. рис. 3.1). Однак, варто зазначити, що наявність додаткових функцій, таких як налаштування ваги активів або розширені опції, може створювати більше інформаційних елементів та вимагати більшої уваги від користувача. Додаток має певний рівень складності та завантаженості через широкий спектр функцій, які пропонує платформа. Також через наявність надлишковості в даному додатку страждає швидкодія та швидкість завантаження сторінок.

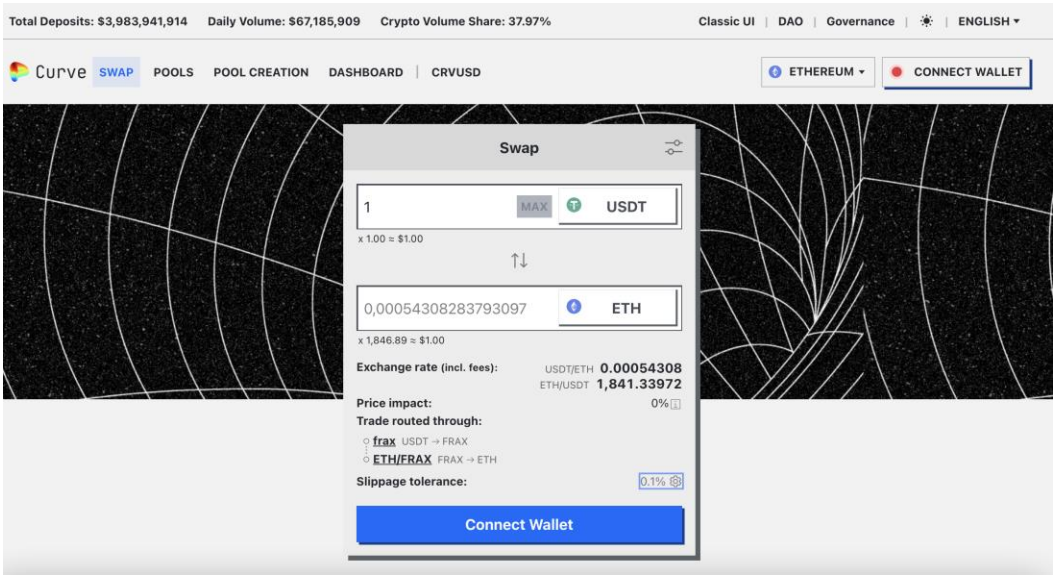


Рисунок 3.1 – Головне меню обмінника Curve Finance

Після ретельного аналізу обміннику було зроблено висновки про наступні переваги та недоліки даного децентралізованого застосунку.

Переваги застосунку Curve Finance:

1) Широкий функціонал та деталізація: Curve Finance пропонує широкий спектр функціональних можливостей та деталізацію для користувачів. Платформа дозволяє налаштувати та оптимізувати обмін токенів у більш докладний спосіб.
2) Надійність: Curve використовує розумні контракти на блокчейні Ethereum, що робить процес обміну безпечним та надійним. Активи залишаються під контролем користувачів, і вони можуть проводити торгівлю без необхідності передавати їх на централізовані біржі.
3) Автоматичні ринки ліквідності: Curve використовує концепцію AMM, що дозволяє безперервний обмін активів навіть при відсутності протилежних пропозицій. Це забезпечує високу швидкість обміну,

сприяє зручній торгівлі та доступу до різних активів.

Недоліки застосунку Curve Finance:

1) Складний інтерфейс: один з основних недоліків Curve полягає в тому, що його інтерфейс може бути складним для новачків та незвичайним для користувачів звичайних централізованих бірж. Розуміння та використання всіх функцій Curve може вимагати певної технічної грамотності.
2) Повільне завантаження: інтерфейс Curve може бути перевантаженим багатьма функціями та опціями, що призводить до повільного завантаження сторінок та взаємодії з платформою. Це може створювати нестабільність та незручності для користувачів, особливо при використанні на мобільних пристроях з обмеженими ресурсами.
3) Відсутність статистики криптовалюти: Одним з недоліків Curve є обмежена наявність статистики та аналітичних інструментів, які можуть надавати користувачам більш детальне розуміння ринку та торговельних умов.

3.3 Огляд застосунку CowSwap

CowSwap – децентралізована платформа обміну на мережі Ethereum, яка пропонує широкий функціонал та забезпечує зручність для користувачів [17].

Одна з головних переваг обмінника CowSwap полягає в його мінімалістичному дизайні та зручності інтерфейсу. Користувачам надається інтуїтивно зрозумілий та легко навігований інтерфейс, що спрощує процес обміну токенів. Всі необхідні функції та опції доступні на платформі, що дозволяє користувачам легко налаштувати свої угоди та здійснювати обмін активами без зайвих зусиль (див. рис. 3.2).

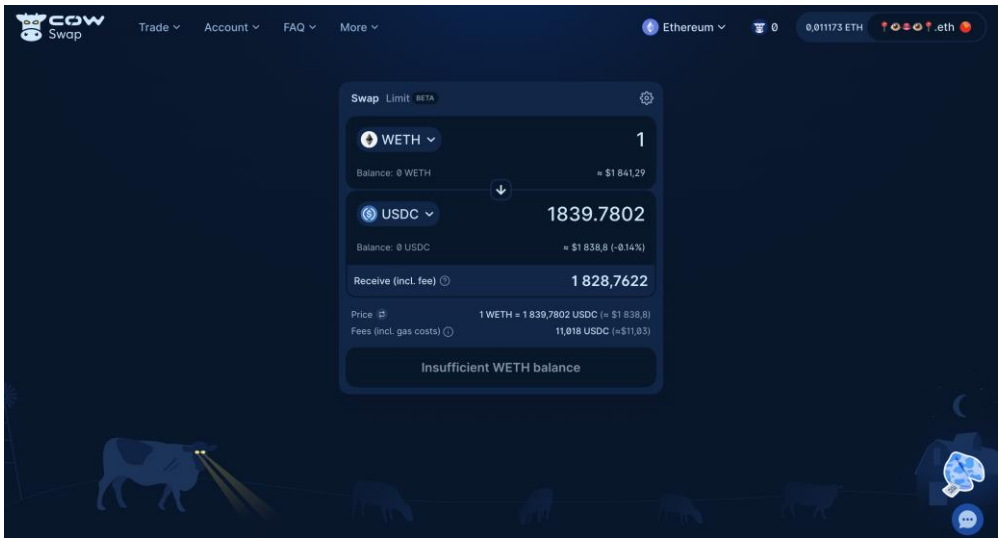


Рисунок 3.2 – Головне меню обмінника CowSwap

У CowSwap є вкладка "Tokens overview", яка надає користувачам можливість перегляду балансу їх гаманців у токенах (див. рис. 3.3) .

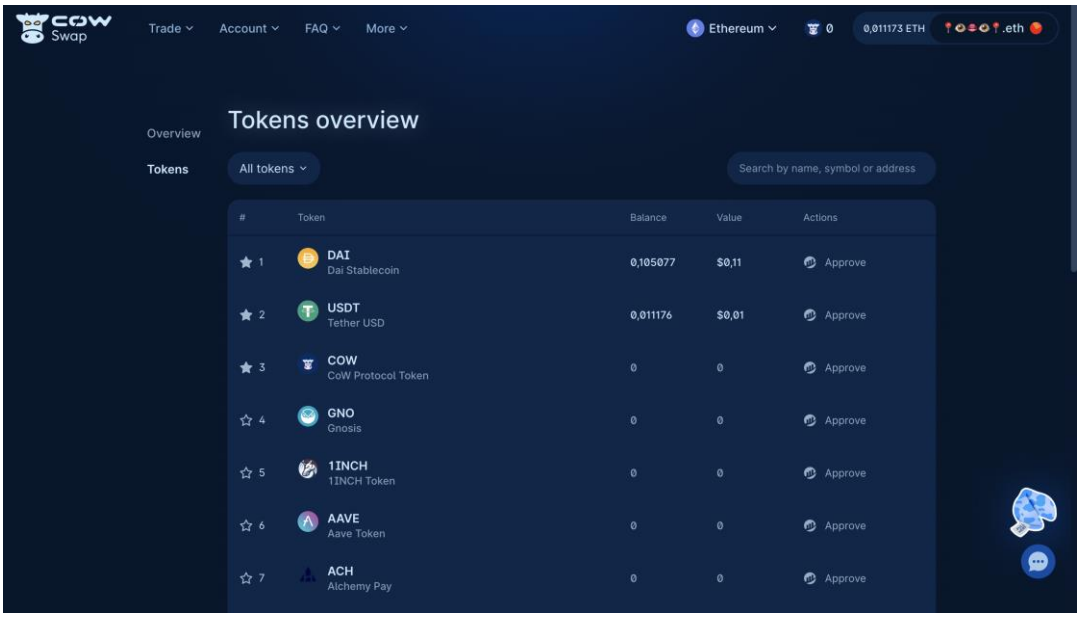


Рисунок 3.3 – Вікно огляду свого портфоліо в обміннику CowSwap

Ця функція дозволяє швидко перевірити наявність та кількість різних токенів, які знаходяться в гаманці користувача.

Однак, варто відзначити, що інформацію про баланс токенів також можна переглянути у вебгаманці Metamask або інших аналогічних гаманцях. Ця можливість є вбудованою функцією багатьох Ethereum гаманців і дозволяє користувачам легко відстежувати свої активи.

Тому, хоча вкладка "Tokens" у CowSwap надає зручний спосіб перегляду балансу токенів, ця функція може не вважатись дуже корисною для тих, хто вже користується Metamask або подібними гаманцями, де така інформація також доступна.

Після ґрунтовного аналізу обмінника були отримані наступні висновки щодо його переваг і недоліків.

Переваги застосунку CowSwap:

1) Простота та зручність інтерфейсу: CowSwap надає інтуїтивно зрозумілий та легко навігований інтерфейс, що спрощує процес обміну токенів. Це робить платформу зручною для новачків та недосвідчених користувачів криптовалют.
2) Автоматичні ринки ліквідності: CowSwap використовує концепцію AMM, що дозволяє забезпечити безперервний обмін активів навіть у випадку відсутності протилежних пропозицій.
3) Надійність та безпека: CowSwap покладає великий акцент на надійність та безпеку своїх користувачів. Використання смарт-контрактів на мережі Ethereum дозволяє забезпечити автоматичні та надійні транзакції без необхідності в довіреній стороні.

Недоліки застосунку CowSwap:

1) Обмежена кількість токенів: CowSwap може мати обмежений перелік токенів, доступних для обміну. Це може обмежити вибір користувачів та ускладнити обмін активами, якщо потрібні специфічні або менш популярні токени.

2) Низька ліквідність окремих токенів: Окремі токени можуть мати обмежену ліквідність. Це може призвести до менш конкурентоспроможних цін та обмежень в обсязі обміну для деяких менш популярних активів.
3) Обмежена аналітична функціональність: CowSwap має обмежений набір аналітичних інструментів, що можуть ускладнити користувачам отримання повної картини ринку та глибокого аналізу динаміки цін. Відсутність розширених аналітичних функцій може обмежувати здатність користувачів приймати обґрунтовані рішення щодо торгівлі та розміщення замовлень.

3.4 Огляд застосунку SushiSwap

SushiSwap є децентралізованим обмінником, який надає користувачам зручність, широкий функціонал та інтуїтивно зрозумілий інтерфейс (див. рис. 3.4) [18].

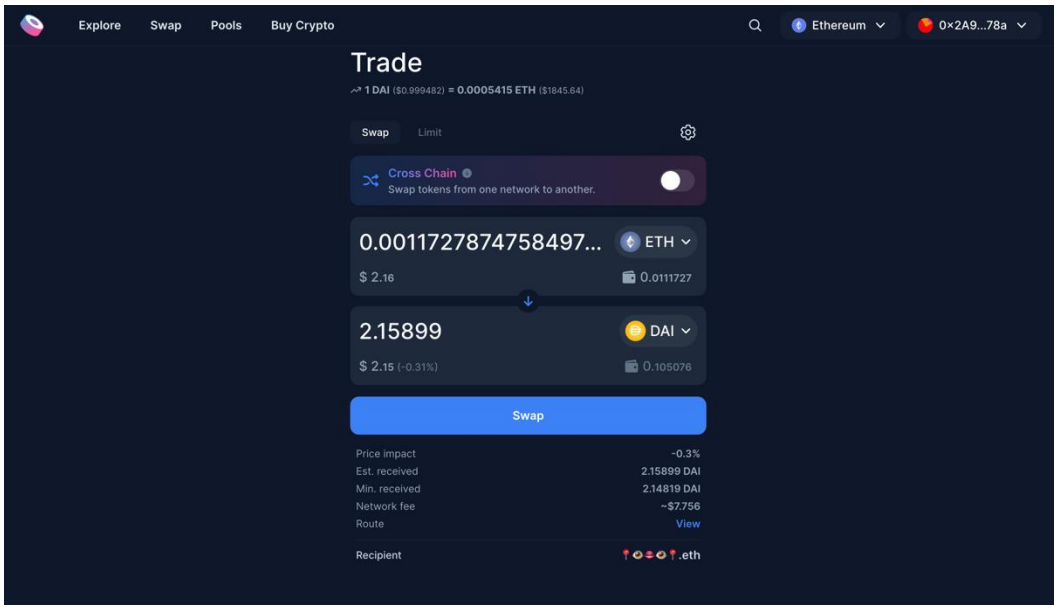


Рисунок 3.4 – Головне меню обмінника SushiSwap

Однією з головних переваг SushiSwap є його зручність для користувачів.

Платформа пропонує широкий спектр криптовалютних пар для обміну, дозволяючи користувачам здійснювати торгівлю з різних активів.

Щодо інтерфейсу, SushiSwap пропонує інтуїтивно зрозумілий та легкий у використанні інтерфейс. Користувачі можуть легко навігуватись по сайту, здійснювати обмін та управляти своїми активами без зайвих складнощів.

SushiSwap, як і багато інших децентралізованих обмінників, використовує підхід автоматичних ринків ліквідності (AMM) для забезпечення обміну активів. Це означає, що SushiSwap спирається на пули ліквідності та алгоритми, які автоматично встановлюють ціни та вирівнюють ринки.

Зважаючи на аналіз SushiSwap, можна виділити наступні переваги та недоліки.

Переваги застосунку SushiSwap:

1) Широкий вибір торгових пар: SushiSwap надає користувачам можливість обмінювати різні криптовалюти через широкий вибір торгових пар. Це дозволяє користувачам здійснювати обмін зручно та швидко, забезпечуючи доступ до різних активів на платформі.
2) Ефективний механізм автоматичних ринків ліквідності: SushiSwap використовує AMM, що дозволяє безперервний обмін активів без необхідності чекати протилежних пропозицій. Це забезпечує високу ліквідність та швидкість обміну, що полегшує процес торгівлі для користувачів.
3) Простий та інтуїтивно зрозумілий інтерфейс: SushiSwap має зручний та легкий у використанні інтерфейс, який дозволяє користувачам швидко орієнтуватись і здійснювати обмін активами. Це полегшує взаємодію з платформою та забезпечує комфортну торгівлю.

   Недоліки застосунку SushiSwap:

   1) Відсутність аналітичних інструментів: SushiSwap не надає

достатньої статистичної інформації та аналітичних інструментів для детального аналізу ринку та прийняття обґрунтованих рішень. Це може ускладнити користувачам отримання повної картини ринку та розуміння його динаміки.

2) Ризик недостатньої ліквідності на деяких торгових парах: Як і у багатьох інших DEX, SushiSwap може стикатися з проблемою недостатньої ліквідності на деяких торгових парах. Це може призводити до значних розбіжностей у цінах та обмежувати можливості торгівлі для користувачів.

3.5 Постановка задачі

Після огляду DEX, представлених на ринку децентралізованих обмінників, стало очевидним, що в цілому багато з них можуть задовольнити базові потреби користувачів. Однак, виявлено деякі недоліки, які можна покращити і реалізувати в нашому власному DEX.

Відсутність аналітичних інструментів є одним з основних недоліків, виявлених під час аналізу. Багато існуючих DEX не надають достатньої статистичної інформації, такої як динаміка цін, ринкова капіталізація та інші аналітичні показники, які допомагали б користувачам отримувати більш детальну картину ринку та зробити обґрунтовані рішення.

Загальний аналіз показав, що деякі DEX мають надмірний та заплутаний дизайн, що може призводити до складнощів у користуванні та вимагати значних зусиль для ознайомлення з функціоналом. Перевантаження сайту та повільне завантаження сторінок також виявилися серйозними проблемами, які можуть негативно вплинути на швидкодію та взаємодію з платформою.

Також велика кількість DEX мають обмежений обсяг ліквідності, особливо для менш популярних або нових токенів. Це може призводити до недостатньої доступності активів для обміну, а також до великих розбіжностей

в цінах між обмінниками. Користувачі, які шукають менш поширені активи або певні пари обміну, можуть зіткнутися з проблемами з виконанням своїх угод через обмежену ліквідність на певних DEX.

Враховуючи ці недоліки, визначено постановку задачі для розробки власного DEX включає наступне:

1) Розробка аналітичних інструментів: платформа буде включати аналітичні інструменти, які допоможуть користувачам отримати доступ до детальної статистики криптовалют. Це надасть користувачам більше інформації для прийняття обґрунтованих рішень.
2) Створення юзер-френдлі інтерфейсу: будемо розробляти зручний та інтуїтивно зрозумілий інтерфейс, зосереджуючись на простоті взаємодії та легкому навігуванні для користувачів, незалежно від їх рівня досвіду з криптовалютами. Зменшення перевантаженості та виключення зайвих функцій допоможуть полегшити користування та покращити швидкодію платформи.
3) Вибір AMM для моделі обмінника: враховуючи різноманіття децентралізованих обмінників, більшість з них використовують модель автоматичних ринків ліквідності (AMM). Ця модель є важливою альтернативою традиційному ордер-буку, оскільки пропонує ряд переваг, які роблять її більш зручною та ефективною для користувачів.
4) Забезпечення ліквідності: одним з ключових аспектів при розробці DEX є розробка та впровадження ефективного рішення для забезпечення достатньої ліквідності, щоб користувачі могли здійснювати обмін без обмежень та затримок.
5) Використання безпечного смарт-контракту: важливо, щоб смарт-контракт був розроблений з дотриманням найкращих практик безпеки. При розробці DEX важливо забезпечити надійну та безпечну платформу, де користувачі можуть обмінюватись токенами без ризику

втрати активів через шахрайство чи кібератаки.

6) Впровадження газ трекера: зважаючи на відносно високі ціни на комісії в мережі Ethereum ще одним важливим додатком є впровадження газ трекеру. Цей інструмент надасть користувачам інформацію про вартість газу під час транзакцій, допомагаючи їм приймати інформовані рішення та управляти своїми активами.

Зробивши ці покращення та реалізуючи наші власні ідеї, ми прагнемо створити DEX, який буде надійним, функціональним та зручним для користувачів, забезпечуючи їм доступ до розширеного функціоналу, аналітичних інструментів та швидкої взаємодії.

РОЗДІЛ 4. ПРОЄКТУВАННЯ ТА РОЗРОБКА ВЕБЗАСТОСУНКУ ДЛЯ ОБМІНУ КРИПТОВАЛЮТ

4.1 Вибір моделі обміну криптовалют у застосунку

Вибір моделі обміну криптовалют в вебзастосунку є важливим етапом проєктування, оскільки це визначає функціональність, ефективність та легкість використання платформи.

В даній кваліфікаційній роботі, вибір моделі DEX на основі AMM з використанням смарт-контракту агрегатора 1inch [19] обумовлений кількома перевагами та факторами:

1) Переваги AMM: Модель AMM, яка використовується в DEX, дозволяє безпосередньо обмінюватися криптовалютами без потреби розміщення ордерів у традиційному форматі. Це забезпечує простоту та швидкість обміну, а також зменшує витрати на комісії та уникнення проблем з ліквідністю. Крім того, AMM забезпечує автоматизоване формування цін на основі алгоритмів, що дозволяє уникнути недоліків традиційної моделі з ордерами.
2) Висока ліквідність: використання агрегатора 1inch, який надає доступ до багатьох обмінників, дозволяє отримати високу ліквідність. Це означає, що користувачі отримують доступ до найкращих курсів обміну та можуть легко виконувати обмін без проблем з виконанням замовлень.
3) Користувацький досвід: модель DEX на основі AMM та використання агрегатора дозволяє забезпечити зручний та інтуїтивно зрозумілий користувацький досвід. Користувачам не потрібно розміщати ордери або очікувати співпадіння, а замість цього вони можуть безпосередньо обмінюватися криптовалютами за найкращими доступними курсами.

4) Доступність та надійність: використання смарт-контракту 1inch дозволяє отримати доступ до багатьох обмінників, що забезпечує більшу гнучкість та надійність. Це означає, що незалежно від доступності конкретного обмінника, користувачі завжди матимуть можливість здійснити обмін.
5) Аудит контракту: смарт-контракт 1inch пройшов аудит, що підтверджує його надійність та безпеку [19]. Аудит контракту дозволяє перевірити, що контракт відповідає встановленим стандартам безпеки та немає потенційних вразливостей, що можуть бути використані для атак.

Враховуючи всі ці переваги, вибір моделі DEX на основі AMM та використання агрегатора 1inch дозволяє створити вебзастосунок для обміну криптовалют, який забезпечує простоту, швидкість, високу ліквідність та зручний користувацький досвід. Крім того, аудит контракту та доступ до багатьох обмінників забезпечують надійність та безпеку операцій з криптовалютами.

Відповідно до обраної моделі вебзастосонку була розроблено UML-діаграму прецедентів, що наведена у додатку А.

4.2 Реалізація основного функціоналу вебзастосунку для обміну криптовалют

Вебзастосунок для обміну криптовалют є мультифункціональним інструментом, що використовує декілька ключових компонентів для реалізації своєї функціональності. Цими компонентами являються дві основні сторінки веб-додатку, що виконують провідну роль, вони називаються "Swap" (див. рис. 4.1) та "Tokens".

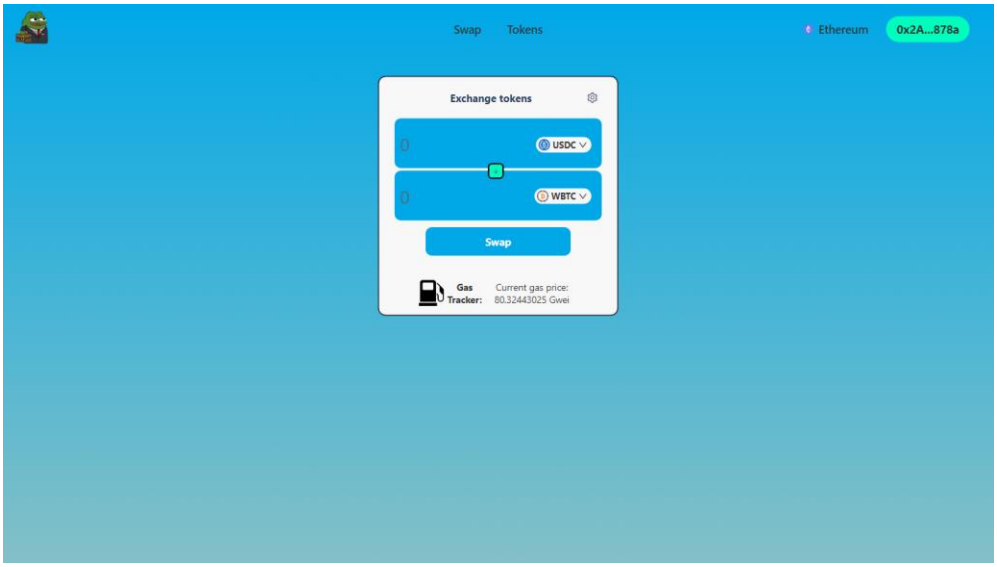


Рисунок 4.1 Сторінка «Swap» вебзастосунку для обміну криптовалют

Компонент Swap є центральним елементом веб-додатку. Це сторінка, на якій відбувається безпосередньо обмін криптовалюти. При використанні даної сторінки користувачі мають можливість обмінювати одну криптовалюту на іншу за встановленими курсами. На цій сторінці присутня форма (зображена на рис. 4.2), де користувачі вказують криптовалюту, яку вони хочуть обміняти, і криптовалюту, яку вони хочуть отримати, а також вставляють в поле кількість криптовалюти, яку вони хочуть обміняти.

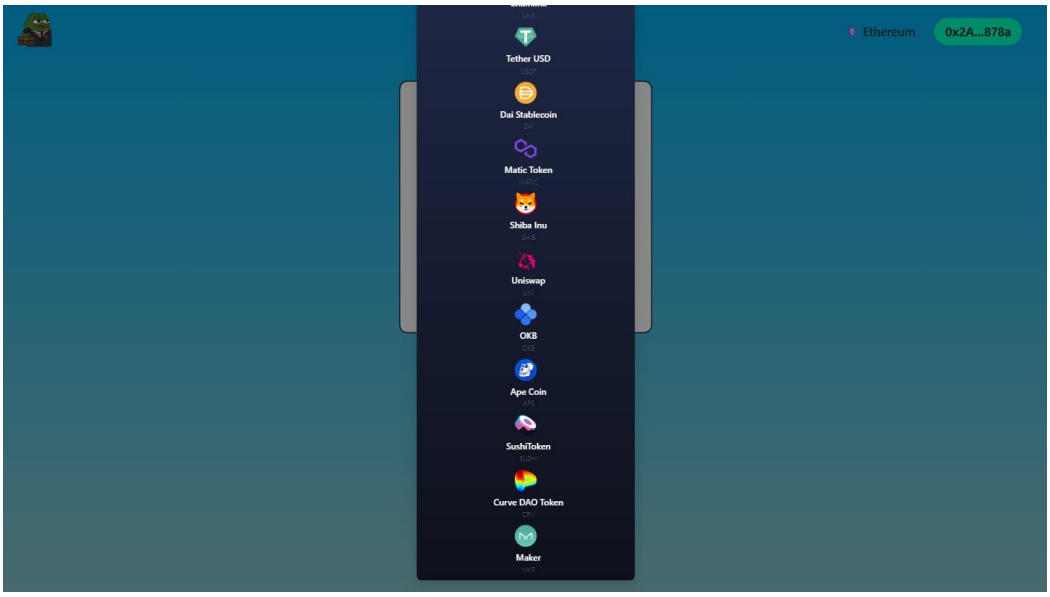


Рисунок 4.2 Меню вибору криптовалюти для обміну

Компонент Tokens (зображений на див. рис. 4.3) слугує для надання додаткової інформації про криптовалюти. Він містить в собі деталізовану інформацію про різні криптовалюти, таку як їх поточна вартість, обсяг торгів, історію цін та інше.

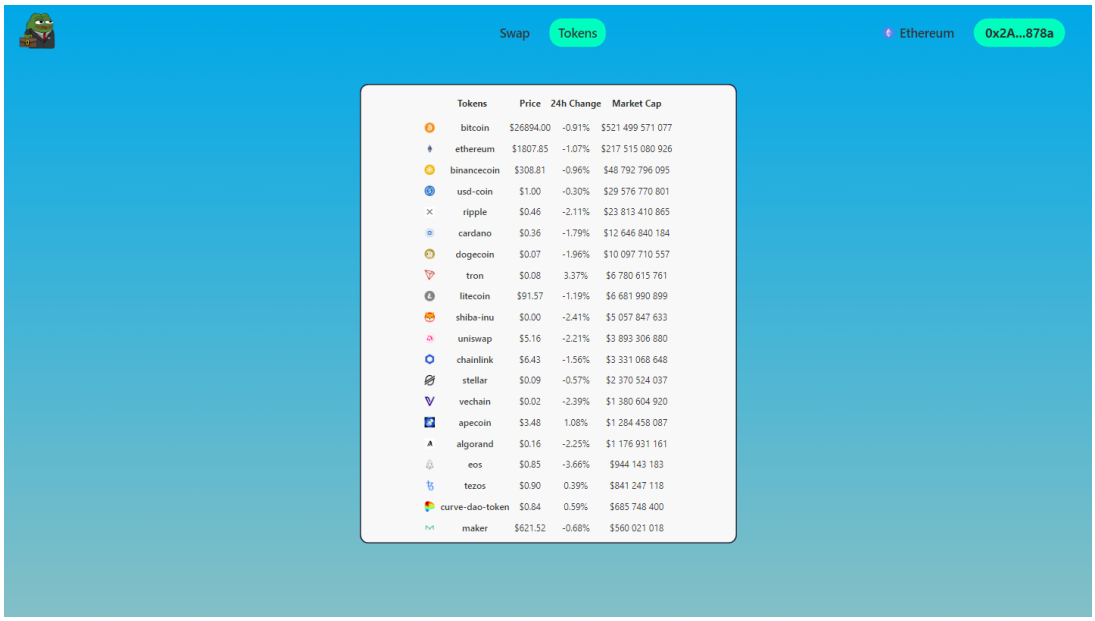


Рисунок 4.3 Сторінка «Tokens» вебзастосунку для обміну криптовалют

Для забезпечення навігації між цими двома компонентами у веб-додатку використовується система маршрутизації зокрема компонент Routes із бібліотеки React Router [20]. Ця бібліотека дозволяє створювати динамічні переходи між різними сторінками або компонентами в односторінкових веб-додатках. Кожному компоненту присвоюється конкретний шлях (URL), і коли користувач переходить по цьому URL, відображається відповідний компонент.

Так, наприклад, користувач може перейти на сторінку обміну криптовалюти, звернувшись до стандартного посилання localhost:3000, а для отримання додаткової інформації про криптовалюти такої, як ціна, динаміка, капіталізація, він може перейти на сторінку localhost:3000/tokens. Це дозволяє створювати веб-додаток, який ефективно відповідає на дії користувачів,

забезпечуючи плавний та інтуїтивно зрозумілий досвід користування. Лістинг коду, що відповідає за старт вебзастосунку та маршрутизацію "App.js" наведений у додатку Б.

Повернемося до модуля "Swap", який є головною частиною інтерфейсу обміну криптовалюти. Як вже було зазначено, модуль включає в себе взаємодію з криптовалютними токенами, обробку вводу користувача, та налаштування параметрів обміну.

Бек-енд обмінника криптовалюти розроблений за допомогою Node.js і бібліотеки Express.js. Головна задача бек-енду полягає у взаємодії з Moralis API [21] для отримання даних про актуальні ціни криптовалюти. Вся ця робота відбувається в маршруті "/tokenPrice", де виконується асинхронний запит до Moralis API за адресами токенів, які надаються у вигляді параметрів запиту. При успішному розгортанні бек-енду та під’єднанню до API маємо наступний вивід в консолі (див. рис. 4.4). Лістинг фрагменту коду файлу index.js, що відповідає за бек-енд наведений у додатку В.

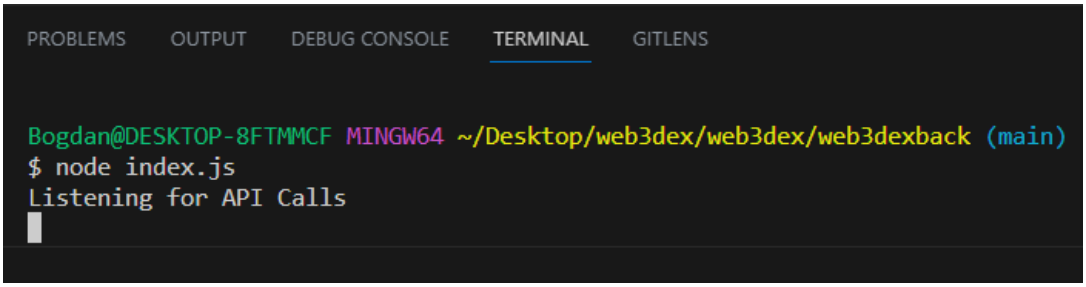


Рисунок 4.4 – Вивід в консолі при розгортанні бек-енд файлу index.js

На фронт-енді ціни на криптовалюту отримуються через запити до бек-енду. Ми використовуємо бібліотеку axios [22] для здійснення GET запиту до нашого Express серверу, передаючи адреси двох токенів як параметри запиту. Після отримання відповіді, ми оновлюємо стан компоненту, використовуючи отримані ціни.

Наступним кроком побудови вебзастосунку є під'єднання крипто-

гаманця. Використовується бібліотека wagmi [23] для взаємодії з крипто-гаманцем MetaMask [10]. Коли користувач натискає кнопку "Connect Wallet", викликається метод wagmi.connect() з бібліотеки wagmi. Цей метод відкриває вікно MetaMask, де користувачу запропоновано підключити свій гаманець до вебзастосунку.

Після того, як користувач затвердив підключення, wagmi.connect() повертає об'єкт, що містить адресу гаманця користувача і методи для виконання транзакцій. Об'єкт зберігається в стані компонента, і його можна використовувати для відправки токенів при обміні.

Останнім кроком в реалізації функціоналу обміну є налаштування взаємодії з 1inch API [19] для безпосереднього обміну криптовалюти. Робиться це наступним чином:

1) Функція fetchPrices(one, two) використовує бібліотеку Axios для виконання GET-запиту до API агрегатора 1inch і отримання цін на токени. Вона приймає два параметри: one - адреса першого токена, і two - адреса другого токена. Результат отримується у відповідь з сервера у форматі JSON і зберігається у стані змінної prices.
2) Функція fetchDexSwap() також використовує бібліотеку Axios для здійснення GET-запиту до API агрегатора 1inch для здійснення обміну токенів. Вона відправляє запит з параметрами, такими як адреса першого токена (token_one.address), адреса другого токена (token_two.address), кількість першого токена (token_one_amount) та адреса власника гаманця (address). Запит також включає параметр slippage, який встановлюється в змінній slippage.
3) У функції fetchDexSwap(), після успішного отримання відповіді з сервера, обробляється отримана інформація. Значення кількості другого токена (toTokenAmount) перетворюється в правильний формат

з врахуванням десяткових знаків, і зберігається в стані змінної token_two_amount.

4) Функція fetchDexSwap() також оновлює стан змінної tx_details з даними про транзакцію, які отримані з сервера.
5) Використовується бібліотека useSendTransaction для надсилання транзакції. Функція sendTransaction() викликається, якщо в стані змінної tx_details є значення для поля to (адреса одержувача токенів) і якщо користувач підключений до мережі (is_connected).
6) Використовується бібліотека useWaitForTransaction для очікування підтвердження транзакції. Змінна isLoading слугує для відстеження стану транзакції. При завантаженні (тобто якщо транзакція ще не підтверджена), відображається повідомлення про очікування транзакції за допомогою компонента message_api.open(). Після успішного виконання транзакції з'являється повідомлення про успішне завершення, а якщо транзакція не вдалася, – повідомлення про невдалу спробу.

Лістинг фрагменту коду компоненти Swap з реалізацією обміну наведено у додатку Г.

4.3 Інтеграція додаткового функціоналу для аналізу криптовалюти

4.3.1 Газ трекер: використання API для відстеження поточного газу у мережі Ethereum

Додавання функціоналу газ трекера до децентралізованої біржі (DEX) має кілька переваг:

1) Відстеження поточного газу: За допомогою газ трекера, користувачі DEX можуть бачити поточну ціну газу в мережі Ethereum. Це дозволяє

їм приймати інформовані рішення про вартість виконання транзакцій на мережі.

2) Оптимальне налаштування газу: Знання поточної ціни газу допомагає користувачам вибрати оптимальні параметри газу для своїх транзакцій. Вони можуть встановити відповідну комісію, щоб забезпечити швидку обробку своїх транзакцій або зекономити кошти, вибравши меншу комісію.
3) Зменшення ризику: Знання ціни газу допомагає уникнути випадків, коли користувачі виплачують надмірну комісію за виконання транзакцій. Вони можуть оцінити ризик і вибрати комісію, яка є вигідною і прийнятною для них.

Функціонал газ трекера в коді працює наступним чином:

1) У компоненті GasTracker використовується стан змінних gasPrice і error, які зберігають поточну ціну газу і повідомлення про помилку відповідно.
2) Використовується useEffect для виклику функції getGasPrice при першому відображенні компонента. Це дозволяє отримати поточну ціну газу під час завантаження компонента.
3) У функції getGasPrice виконується POST-запит до API інфраструктури Infura [24] для отримання ціни газу. Запит містить JSON-об'єкт з полями jsonrpc, method, params та id, які відповідають специфікації JSON-RPC для отримання ціни газу.
4) Відповідь з сервера містить ціну газу в форматі Wei. Ціна газу перетворюється з Wei на Gwei шляхом ділення на 1e9, і результат зберігається в стані змінної gasPrice.
5) Якщо виникає помилка під час отримання ціни газу, встановлюється повідомлення про помилку в стані змінної error.

6) Якщо є повідомлення про помилку, воно відображається у вигляді тексту. Якщо ж є поточна ціна газу, вона відображається у вигляді тексту з префіксом "Current gas price: " і одиницею виміру "Gwei".

Лістинг фрагменту коду компоненти газ трекеру наведений у додатку Д.

Таким чином, компонент GasTracker використовує API для отримання поточної ціни газу в мережі Ethereum і відображення її для користувача. Це допомагає користувачам DEX приймати розумні рішення про комісію газу та зменшує ризик надмірного витрачання коштів на транзакції.

4.3.2 Токен трекер: використання API для відстеження цін криптовалют з динамікою росту та падіння

Додавання функціоналу токен трекера до децентралізованої біржі (DEX) має кілька переваг:

1) Відстеження цін криптовалют: За допомогою токен трекера, користувачі DEX можуть бачити поточні ціни різних криптовалют. Це дозволяє їм визначити найвигідніші умови для обміну та приймати інформовані рішення щодо торгівлі.
2) Динаміка росту та падіння: Токен трекер надає користувачам інформацію про зміну цін криптовалют протягом останніх 24 годин. Це дозволяє користувачам оцінити тенденції ринку та зробити кращі торгові рішення.
3) Відображення ринкової капіталізації: Токен трекер також відображає ринкову капіталізацію криптовалют. Це допомагає користувачам оцінити загальну вартість криптовалютного ринку та вибрати потенційно перспективні активи для торгівлі.

Функціонал токен трекера в коді працює наступним чином:

1) У компоненті Tokens використовується стан змінної cryptoData, яка

зберігає дані про криптовалюти.

2) Використовується useEffect для виклику функції fetchCryptoData при першому відображенні компонента. Це дозволяє отримати дані про криптовалюти з зовнішнього API.
3) У функції fetchCryptoData виконується GET-запит до API Coingecko [25] для отримання інформації про ціни та інші дані криптовалют. Отримані дані перетворюються і зберігаються в змінній updatedCryptoData.
4) Компонент візуалізує дані криптовалют у вигляді таблиці з декількома стовпцями. У першому стовпці відображаються логотипи криптовалют, у наступних стовпцях відображаються назви, ціни, зміна за останні 24 години та ринкова капіталізація криптовалют.

Лістинг фрагменту коду компоненти токен трекера наведено у додатку Е.

Таким чином, компонент Tokens використовує API для отримання інформації про ціни криптовалют та відображення їх для користувачів DEX. Це дозволяє користувачам відстежувати ціни та зміни ринку, що поліпшує їх можливості аналізу криптовалюти.

4.4 Тестування обміну криптовалют в мережі Ethereum

Розроблений вебзастосунок для обміну криптовалют необхідно протестувати.

Для тестування скористаємось даним алгоритмом:

1) Коннект гаманця: користувач має під’єднати свій Metamask гаманець, натискнувши кнопку Connect.
2) Вибір токенів: користувач обирає токени, які він бажає обміняти. Це може бути виконано за допомогою інтерфейсу, який надає список доступних токенів, їх логотипи та назви. Користувач обирає токен, який він хоче обміняти, а також токен, на який він хоче обміняти.
3) Вибір кількості: користувач вказує кількість токенів, яку він бажає обміняти. Це може бути введено за допомогою текстового поля, де користувач вводить кількість токенів.
4) Вибір slippage: slippage (проковзування) вказує максимально припустиму різницю у ціні між моментом відправлення транзакції та моментом виконання обміну. Користувач може вибрати відповідне значення slippage, яке відповідає його ризиковим настановам та торговельним стратегіям. Це може бути здійснено за допомогою інтерфейсу з варіантами вибору slippage (наприклад, 0.5%, 2.5%, 5% тощо).
5) Апрув: перед здійсненням обміну, необхідно здійснити апрув токенів, щоб дозволити контракту DEX доступ до токенів на адресі користувача. Користувач погоджується на апрув і запускає транзакцію. Для цього використовується відповідний метод API, який надає доступ до функціоналу апруву та відправки транзакцій.
6) Обмін: після успішного апруву, користувач запускає процес обміну.

Використовуючи метод API, надається інформація про токени, кількість токенів, адресу користувача і, додаткові параметри, такі як slippage.

Застосуємо цей алгоритм для тестування нашого вебзастосунку:

1) Натискаємо кнопку Connect ті під'єднаємо наш гаманець Metamask. Отримуємо діалогове вікно з підтвердженням під'єднання (див. рис.4.5). Обираємо наш гаманець та натискаємо "далі". Бачимо, що гаманець успішно підєднався до вебзастосунку. Перші та останні цифри адреси гаманця відображаються у вебзастосунку (див. рис. 4.6).

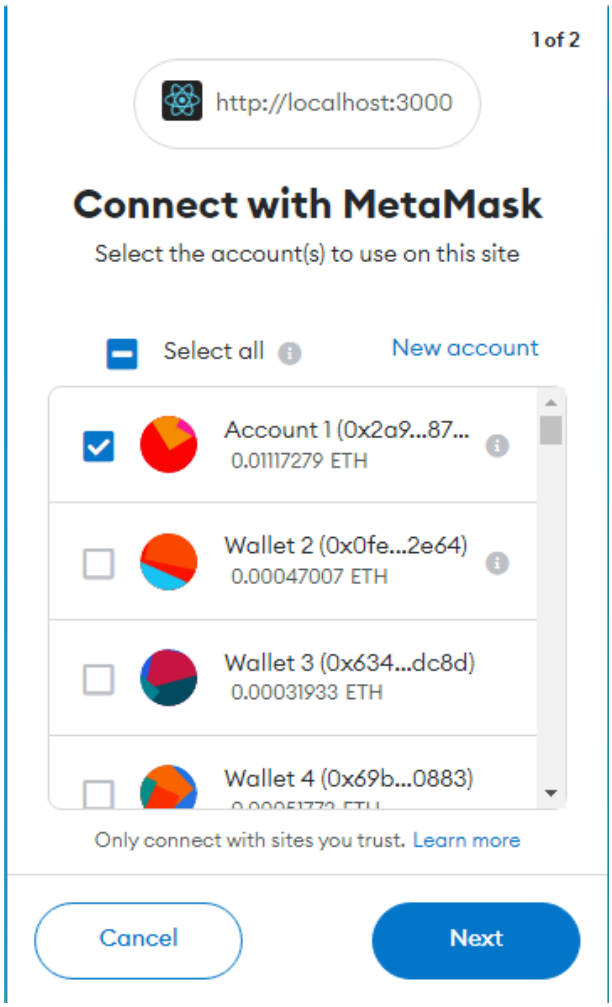


Рисунок 4.5 – Під'єднання гаманця Metamask до вебзастосунку

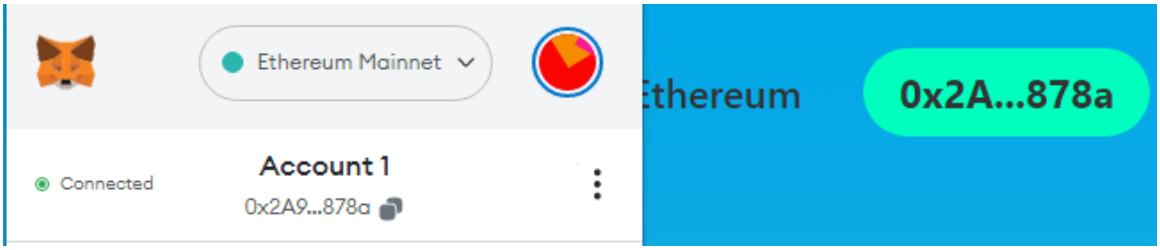


Рисунок 4.6 – Під’єднаний до вебзастосунку гаманець Metamask

2-3) Обираємо торгову пару, відкриваючи контекстне вікно (див. рис. 4.7). Нехай для зразку це буде пара DAI – LINK, в якій ми хочему обміняти 1 стейблкоїн DAI (див. рис. 4.8). Наш початковий баланс на гаманці складає 1.1 стейбкоїн DAI та 0.001 токенів LINK (див. рис. 4.9).

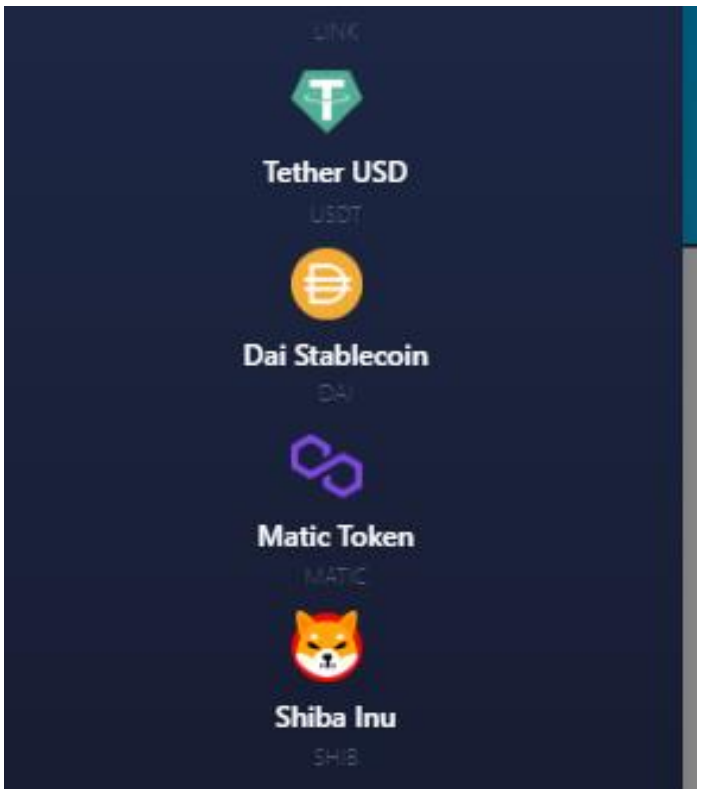


Рисунок 4.7 – Контекстне вікно вибору криптовалюти для торгової пари

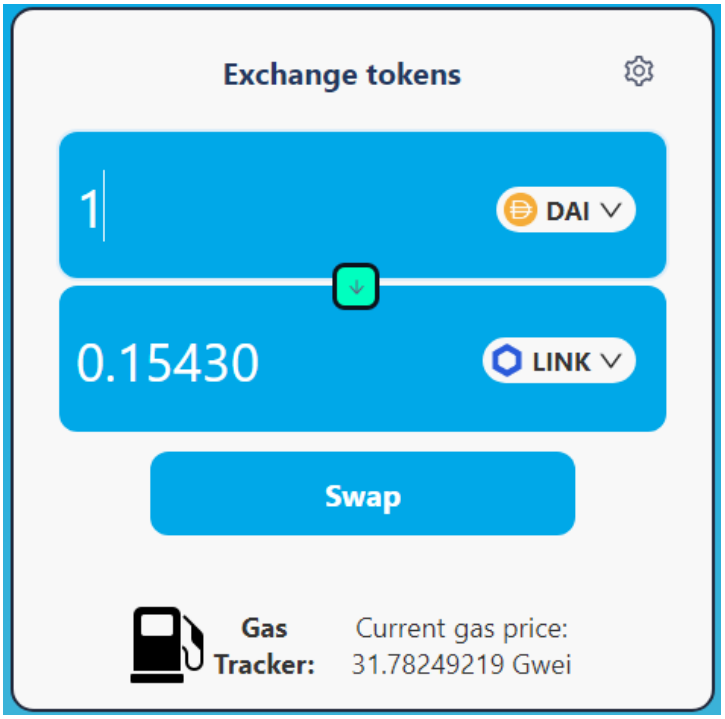


Рисунок 4.8 – Вікно обміну з обраною торговою парою DAI – LINK

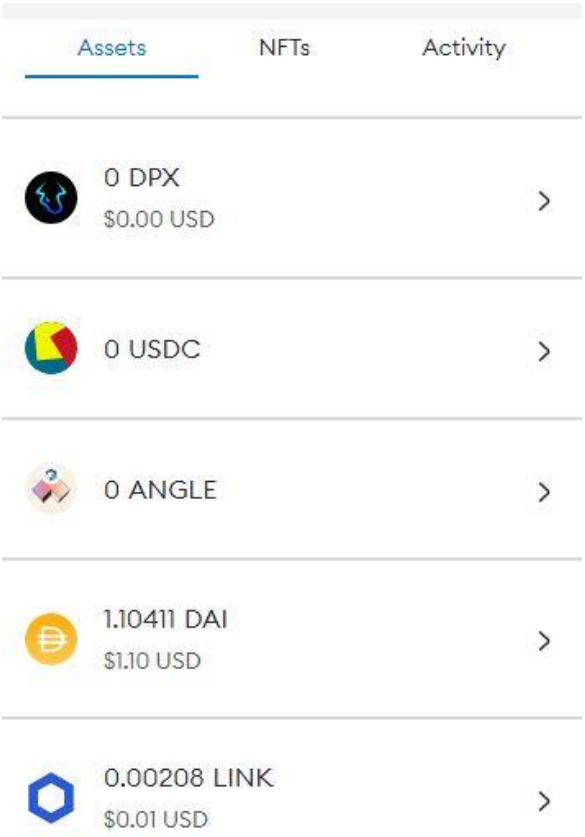


Рисунок 4.9 – Початковий баланс крипто гаманця перед обміном

4) Натискаємо на коліщатко та обираємо мінімальний slippage – 0.5% (див. рис. 4.10).

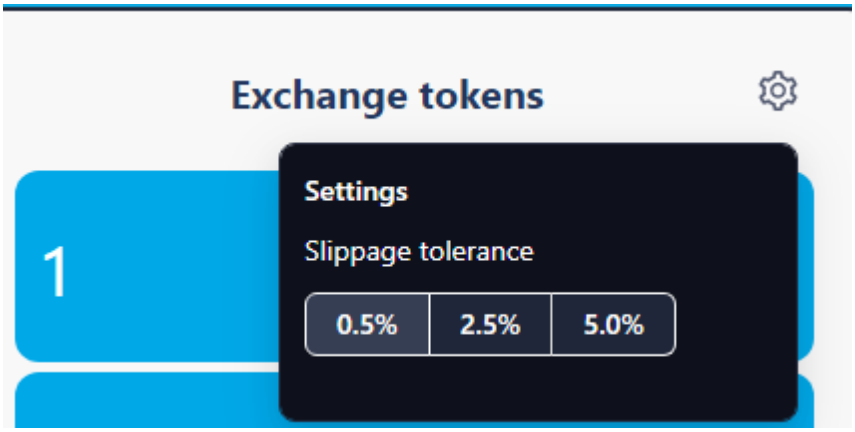


Рисунок 4.10 – Налаштування значення slippage

5) Натискаємо кнопку Swap. Отримуємо запит на апрув від крипто гаманця (див. рис.4.11). Підтверджуємо його.

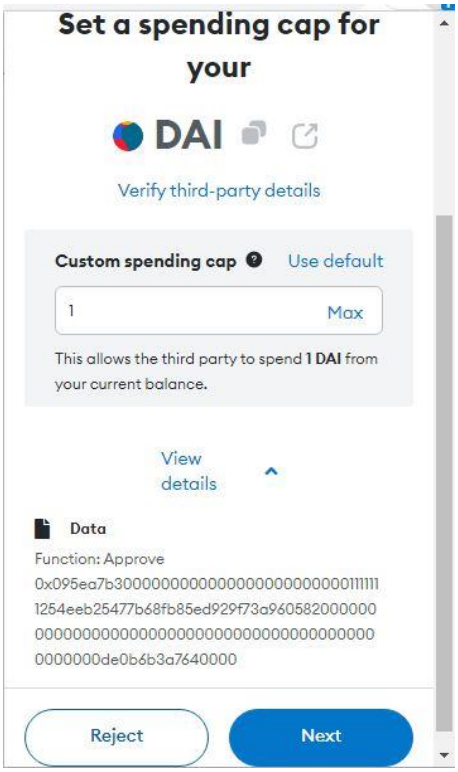


Рисунок 4.11 – Надання дозволу на використання токена DAI перед обміном

6) Отримуємо ще один запит від крипто гаманця на обмін токенів Підтверджуємо його та завершаємо обмін. Як результат, ми обміняли наші токени DAI на токени LINK, що відображається в нашому крипто гаманці (див. рис.4.12).

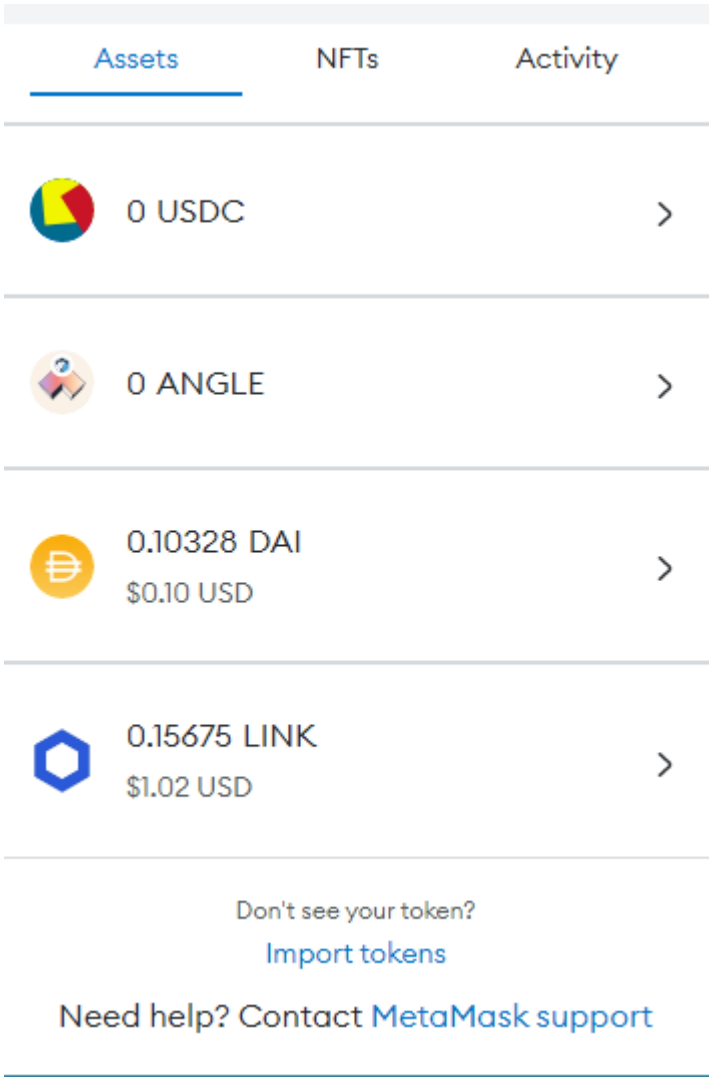


Рисунок 4.12 – Кінцевий баланс крипто гаманця після обміну

Тестування пройшло успішно, а отже наш вебзастосунок для обміну криптовалют успішно виконує свої функції.

ВИСНОВКИ

У даній роботі розроблено вебзастосунок на блокчейні Ethereum, який надає можливість користувачам обмінювати криптовалюти, відображає статистику актуальних цін для криптовалюти та має інтеграцію функціоналу відстеження поточного газу в мережі Ethereum для проведення транзакцій. Для досягнення цієї мети були поставлені відповідні завдання, які були успішно виконані.

В процесі розробки проведено дослідження наявних систем та технологій, що дозволяють обмінювати криптовалюти, для отримання глибшого розуміння їх принципів та функціоналу. Також були поглиблені знання у блокчейн-технологіях для забезпечення належного рівня експертизи при розробці та впровадженні вебзастосунку для обміну криптовалют.

Досліджено та обрано для впровадження алгоритм проведення обміну криптовалют, який забезпечує безпечну передачу активів між користувачами. Також реалізовано використання смарт-контракту, який відповідає алгоритму обміну криптовалют та забезпечує автоматизовану обробку транзакцій.

Розроблено інтерфейс вебзастосунку, який дозволяє користувачам обмінювати криптовалюти. Також реалізовані необхідні операції для взаємодії з мережею Ethereum, зокрема для роботи з DEX, забезпечуючи можливість виконання транзакцій, доступ до контрактів та отримання актуальної інформації про токени на блокчейні Ethereum.

Можливості вебзастосунку для обміну криптовалют є широкими. Він може служити платформою для торгівлі різними криптовалютами та токенами, забезпечуючи безпечні та децентралізовані операції. Також він надає різноманітні інструменти для аналізу ринку, трекінгу цін токенів та відстеження поточного газу в мережі Ethereum. Це дозволяє користувачам відстежувати рухи цін та приймати обґрунтовані рішення щодо

криптовалютних операцій.

Таким чином, розроблений вебзастосунок для обміну криптовалют в мережі Ethereum успішно виконує поставлені завдання та має потенціал для застосування в реальних ситуаціях. Його функціонал дозволяє користувачам здійснювати безпечний та зручний обмін криптовалюти та отримувати актуальну інформацію про ринок криптовалюти.

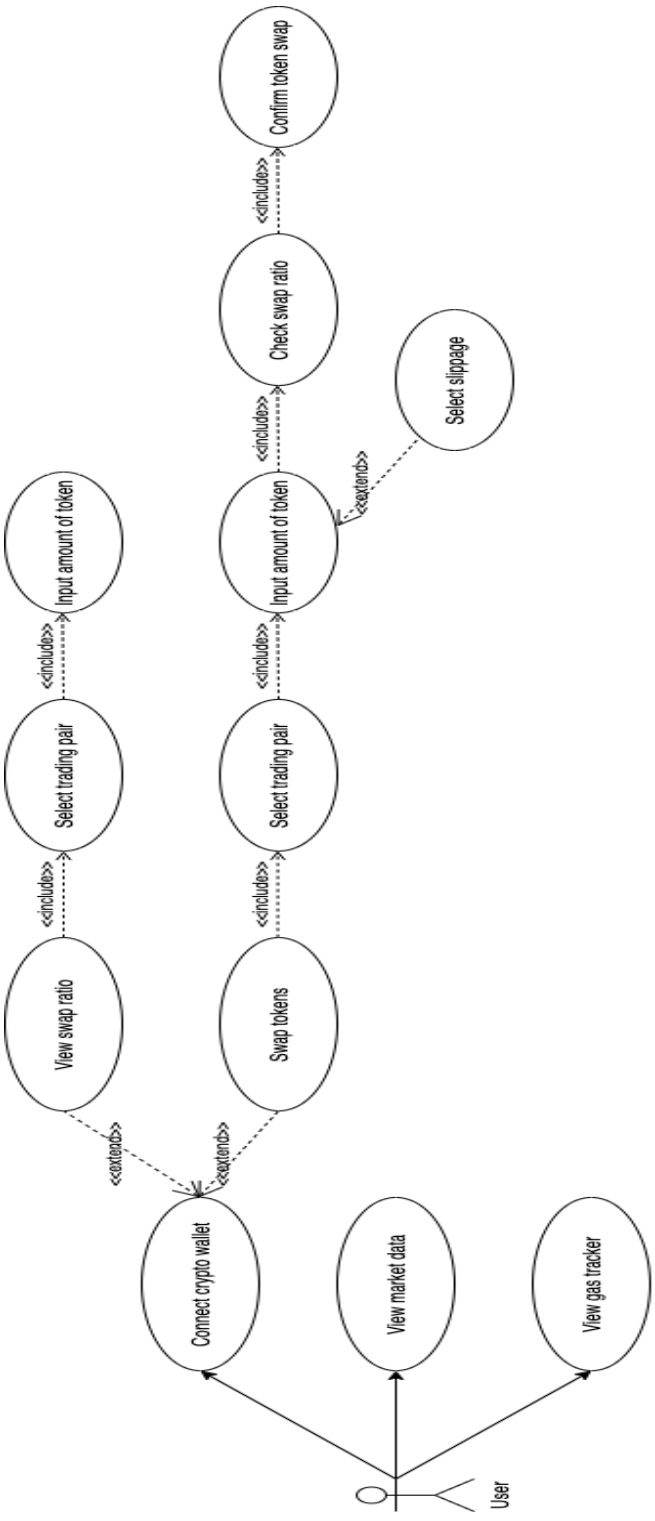
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. The Bitcoin standart / Saifedean Ammous. – John Wiley & Sons, Inc., 2018. – 304с.
2. Ethereum [Електронний ресурс] – режим доступу до ресурсу: https://ethereum.org/whitepaper
3. CoinMarketCap [Електронний ресурс] – режим доступу до ресурсу: https://coinmarketcap.com/
4. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Електронний ресурс] / Satoshi Nakamoto – Режим доступу до ресурсу: https://bitcoin.org/bitcoin.pdf.
5. DappRadar [Електронний ресурс] – режим доступу до ресурсу: https://dappradar.com/rankings/protocol/ethereum
6. Mastering Ethereum, by Andreas M. Antonopoulos, Gavin Wood / A. M. Antonopoulos, G. Wood. – O'Reilly Media, Inc., 2018. – 424с.
7. Solidity Documentation [Електронний ресурс] – режим доступу до ресурсу: https://docs.soliditylang.org/
8. Blockchain Basics: A Non-Technical Introduction in 25 Steps / Daniel Drescher, – Apress, 2017. – 270с.
9. Trust Wallet [Електронний ресурс] – режим доступу до ресурсу: https://trustwallet.com/
10. Metamask [Електронний ресурс] – режим доступу до ресурсу: https://metamask.io/
11. Cryptocurrency: How Bitcoin and Digital Money are Challenging the Global Economic Order / Michael J. Casey, Paul Vigna. – St. Martin's Publishing Group., 2015. – 357с.
12. How to DeFi: Advanced / Lucius Fang, Benjamin Hor, Erina Azmi. – Independently published., 2021. – 296с.
13. Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond / Chris Burniske, Jack Tatar. – McGraw Hill., 2017 – 368с.

14. DeFi and the Future of Finance / C. R. Harvey, A. Ramachandran, J. Santoro. – Wiley, 2021. – 200c.
15. Automated Market Makers: A Practical Guide to Decentralized Exchanges and Cryptocurrency Trading / Miguel Ottina, Peter Johannes Steffensen, Jesper Kristensen. – Apress, 2023. – 304c.
16. Curve Finance [Електронний ресурс] – режим доступу до ресурсу: https://resources.curve.fi/
17. Cow Protocol overview[Електронний ресурс] – режим доступу до ресурсу: https://docs.cow.fi/
18. SushiSwap Docs [Електронний ресурс] – режим доступу до ресурсу: https://docs.sushi.com/
19. 1inch Network Docs [Електронний ресурс] – режим доступу до ресурсу: https://docs.1inch.io/
20. React Router [Електронний ресурс] – режим доступу до ресурсу: https://reactrouter.com/en/main
21. Moralis Web3 documentation [Електронний ресурс] – режим доступу до ресурсу: https://docs.moralis.io/
22. Axios [Електронний ресурс] – режим доступу до ресурсу: https://axios-http.com/docs/intro
23. Wagmi React hooks for Ethereum [Електронний ресурс] – режим доступу до ресурсу: https://wagmi.sh/
24. Infura documentation [Електронний ресурс] – режим доступу до ресурсу: https://docs.infura.io/infura/
25. Coingecko API documentation [Електронний ресурс] – режим доступу до ресурсу: https://www.coingecko.com/en/api/documentation

ДОДАТКИ

Додаток А. Діаграма прецедентів для використання вебзастосунку для обміну криптовалют



Додаток Б. Лістинг фрагменту коду файлу App.js

```
import "./App.css";
import {Routes, Route} from "react-router-dom";
import { useConnect, useAccount } from "wagmi";
import { MetaMaskConnector } from "wagmi/connectors/metaMask";
import Header from "./components/Header";
import Swap from "./components/Swap";
import Tokens from "./components/Tokens";


function App() {
  const { address, isConnected } = useAccount();
  const { connect } = useConnect ({
    connector: new MetaMaskConnector(),
  });

  return (

    <div className="App">
      <Header connect={connect} isConnected={isConnected} address={address} />
      <div className="mainWindow">
        <Routes>
          <Route path="/" element={<Swap isConnected={isConnected} address={address} />} />
          <Route path="/tokens" element={<Tokens />} />
        </Routes>
      </div>
    </div>
  )
}

export default App;
```

Додаток В. Лістинг фрагменту коду файлу index.js

```
const express = require("express");
const Moralis = require("moralis").default;
const app = express();
const cors = require("cors");
require("dotenv").config();
const port = 3001;

app.use(cors());
app.use(express.json());

app.get("/tokenPrice", async (req, res) => {

  const {query} = req;

  const res_One = await Moralis.EvmApi.token.getTokenPrice({
    address: query.addressOne
  })

  const res_Two = await Moralis.EvmApi.token.getTokenPrice({
    address: query.addressTwo
  })

  const usdPrices = {
    tokenOne: res_One.raw.usdPrice,
    tokenTwo: res_Two.raw.usdPrice,
    ratio: res_One.raw.usdPrice/res_Two.raw.usdPrice
  }

  return res.status(200).json(usdPrices);
});

Moralis.start({
  apiKey: process.env.MORALIS_KEY,
}).then(() => {
  app.listen(port, () => {
    console.log(`Listening for API Calls`);
  });
});
```

Додаток Г. Лістинг фрагменту коду файлу Swap.js

```
async function fetchPrices(one, two) {

  const res = await axios.get('http://localhost:3001/tokenPrice', {
    params: {addressOne: one, addressTwo: two}
  })

  setPrices(res.data)
}

async function fetchDexSwap() {
   const allowance = await axios.get(`https://api.1inch.io/v5.0/1/approve/allowance?tokenAddress=${tokenOne.address}&wa

  if(allowance.data.allowance === "0") {

    const approve = await axios.get(`https://api.1inch.io/v5.0/1/approve/transaction?tokenAddress=${tokenOne.address}`)

    setTxDetails(approve.data);
    console.log("not approved")
    return
  }

  const tx = await axios.get(
    `https://api.1inch.io/v5.0/1/swap?fromTokenAddress=${tokenOne.address}&toTokenAddress=${tokenTwo.address}&amount=${
  )

    let decimals = Number(`1E${tokenTwo.decimals}`)
    setTokenTwoAmount((Number(tx.data.toTokenAmount)/decimals).toFixed(5));

    setTxDetails(tx.data.tx);

  }

useEffect(()=>{

  fetchPrices(tokenList[0].address, tokenList[1].address)

}, [])


useEffect (()=>{

  if(txDetails.to && isConnected){
    sendTransaction();
  }
}, [txDetails])
```

Додаток Д. Лістинг фрагменту коду файлу GasTracker.js

```
import React, { useEffect, useState } from 'react';
import axios from 'axios';
import GasStationIcon from '../img/GasStationIcon.png';

const GasTracker = () => {
  const [gasPrice, setGasPrice] = useState('');
  const [error, setError] = useState('');

  useEffect(() => {
    const getGasPrice = async () => {
      try {
        const response = await axios.post('https://mainnet.infura.io/v3/22c6179195d
          jsonrpc: '2.0',
          method: 'eth_gasPrice',
          params: [],
          id: 1,
        });

        const gasPriceInWei = response.data.result;
        const gasPriceInGwei = gasPriceInWei / 1e9;
        setGasPrice(gasPriceInGwei);
      } catch (error) {
        setError('Error fetching gas price');
        console.log('Error fetching gas price:', error);
      }
    };

    getGasPrice();
  }, []);


  return (
    <div className='gas'>
      <img src={GasStationIcon} alt='Gas Station' className='gas_icon' />
      <h3 className='gas_header'>Gas Tracker: </h3>
      {error && <p>{error}</p>}
      {gasPrice && (
        <div>
          <p className='gas_info'> Current gas price: {gasPrice} Gwei</p>
        </div>
      )}
    </div>
  );
};

export default GasTracker;
```

Додаток Е. Лістинг фрагменту коду файлу Tokens.js

```
import React, { useEffect, useState } from "react";

const Tokens = () => {
  const [cryptoData, setCryptoData] = useState([]);

  useEffect(() => {
    const fetchCryptoData = async () => {
      try {
        const response = await fetch(
          "https://api.coingecko.com/api/v3/coins/markets?vs_currency=usd&ids=chainlink,polygon,uniswap
        );
        const data = await response.json();

        const updatedCryptoData = data.map((crypto) => {
          const token = crypto.id;
          const price = crypto.current_price || 0;
          const change24h = crypto.price_change_percentage_24h || 0;
          const marketCap = crypto.market_cap || 0;
          const iconUrl = crypto.image;
          return { token, price, change24h, marketCap, iconUrl };
        });

        setCryptoData(updatedCryptoData);
      } catch (error) {
        console.log("Error fetching crypto data:", error);
      }
    };

    fetchCryptoData();
  }, []);

  return (
    <div className="tokens_box">
      <div className="tokens_box_content">
        <div className="tokens_column tokens_column_logo">
          {cryptoData.map((crypto) => (
            <div className="token_entry" key={crypto.token}>
              <img
                src={crypto.iconUrl}
                alt={crypto.token}
                className="token_icon"
                style={{ width: "18px", height: "18px" }}
              />
            </div>
          ))}
        </div>
        <div className="tokens_column">
          <h4 className="tokens_column_header">Tokens</h4>
```