Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій

Кафедра програмних систем і технологій

УДК 004.42

На правах рукопису

ВИПУСКНА КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

Тема: "Децентралізований протокол для автоматизованого забезпечення ліквідності на Ethereum"

Спеціальність – 121 "Інженерія програмного забезпечення"

ПОЯСНЮВАЛЬНА ЗАПИСКА
ВКБР.ІПЗ - 22.00.00.000 ІПЗ

Студент
ІПЗ-41_____/Дмитро ШАЛАЄВ/

Науковий керівник
к. ф.-м. н., доц._____/Ольга СУПРУН/

Допускається до захисту
з питань нормоконтролю
_____**/Тамара ЧАПОВСЬКА/**

Київ-2021

Рішенням Екзаменаційної комісії
випускна кваліфікаційна робота студента

_____

захищена з оцінкою

_____

Голова Екзаменаційної комісії
д.т.н., проф. Віктор ВИШНІВСЬКИЙ

Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра програмних систем і технологій
Освітньо-кваліфікаційний рівень бакалавр
Спеціальність 121 “Інженерія програмного забезпечення”

ЗАТВЕРДЖЕНО
Зав. кафедри програмних систем і технологій
_____ (Олексій БИЧКОВ)

ЗАВДАННЯ

НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

` Шалаєву Дмитру Миколайовичу

1. **Тема випускної кваліфікаційної бакалаврської роботи “Децентралізований протокол для автоматизованого забезпечення ліквідності на Ethereum”**

керівник роботи Ольга СУПРУН, к.ф.-м.н., доцент

затверджені на засіданні кафедри програмтних систем і технологій, протокол № 6 від „11”листопада 2020р.

2. Строк здачі студентом закінченої роботи „__” _____ 2020 р.

3. Вихідні дані до роботи підручники, навчальні посібники, статті, Інтернет-ресурси

4. Зміст пояснювальної записки (перелік питань, що їх належить розробити)

Аналітична частина:

- обґрунтувати актуальність розробки та використання протоколу для автоматизованого забезпечення ліквідності в децентралізованій мережі;
- дослідити існуючі системи;
- визначити переваги та недоліки існуючих систем;

Практична частина

- визначити особливості архітектурного рішення;
- спроектувати структуру системи;
- розробити систему;
- проаналізувати результати розробленої системи.

5. Консультанти з роботи із зазначенням розділів роботи, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Розділ 1. Огляд існуючих рішень	Ольга СУПРУН		
Розділ 2. Проектування та розробка системи	Ольга СУПРУН		
Розділ 3. Результат роботи програми	Ольга СУПРУН		

6. Дата видачі завдання 11 листопада 2020р.

Керівник _____ /Ольга СУПРУН/

Завдання прийняв до виконання _____/Дмитро ШАЛАЄВ/

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назви етапів бакалаврської роботи	Термін виконання етапів роботи	Відмітка про виконання
1.	Уточнення постановки задачі	17.11.2020	
2.	Аналіз літератури	05.01.2021	
3.	Аналіз існуючих систем забезпечення ліквідності	25.01.2021	
4.	Обґрунтування вибору рішення	01.02.2021	

5.	Опис архітектури	05.02.2021	
6.	Побудова архітектури	27.03.2021	
7.	Розроблення програмного забезпечення	01.04.2021	
8.	Тестування розробленого програмного забезпечення	03.05.2021	
9.	Оформлення і друк пояснювальної записки	24.05.2021	
10.	Оформлення презентації	31.05.2021	
11.	Отримання рецензії	12.06.2021	
12.	Затвердження пояснювальної записки роботи завідувачем кафедри	15.06.2021	
13.	Захист дипломної роботи	22.06.2021	

Студент – бакалавр _____/Дмитро ШАЛАЄВ/

Керівник роботи _____ /Ольга СУПРУН/

АНОТАЦІЯ

Випускна кваліфікаційна бакалаврська робота: 53 с., 14 рис., 1 додаток, 7 джерел.

Тема: Децентралізований протокол для автоматизованого забезпечення ліквідності на Ethereum.

Об'єкт дослідження: технологія смарт-контрактів, децентралізований обмін активів та забезпечення ліквідності.

Предмет дослідження: децентралізований протокол на основі технології смарт-контрактів.

Мета роботи: розробка протоколу для забезпечення ліквідності з використанням технології смарт-контрактів.

Результати дослідження: Оцінено можливість використання технології для реалізації децентралізованого протоколу забезпечення ліквідності та обміну активів на Ethereum та розроблені старт-контракти на мові Solidity.

Висновок: В результаті виконання роботи було розроблено протокол децентралізованого забезпечення ліквідності та обміну активів на Ethereum на основі технології та описано економічне обґрунтування проекту. Розроблений протокол та веб-додаток представляє з себе сукупність:

- блокчейну на основі існуючої блокчейн платформи Ethereum;
- смарт-контрактів на мові Solidity для взаємодії з блокчейном, логіка управління ліквідністю та обміну активів, зберігання інформації про обмін і ліквідність;
- клієнтську частину веб-додатку для взаємодії з системою.

БЛОКЧЕЙН АРХІТЕКТУРА, ТЕОРІЯ ІНТЕЛЕКТУАЛЬНИХ КОНТРАКТІВ, АЛГОРИТМ РОБОТИ ДЕЦЕНТРАЛІЗОВАНОЇ БІРЖІ, БЛОК, ЦИФРОВИЙ ПІДПИС, ETHERIUM, BITCOIN

АННОТАЦИЯ

Выпускная квалификационная бакалаврская работа: 53 с., 14 рис., 1 приложение, 7 источников.

Тема: Децентрализованный протокол для автоматизированного обеспечения ликвидности на Ethereum.

Объект исследования: технология смарт-контрактов, децентрализованный обмен активов и обеспечение ликвидности.

Предмет исследования: децентрализованный протокол на основе технологии смарт-контрактов.

Цель работы: разработка протокола для обеспечения ликвидности с использованием технологии смарт-контрактов.

Результаты исследования: Оценено возможность использования технологии для реализации децентрализованного протокола обеспечения ликвидности и обмена активов на Ethereum и были разработаны смарт-контракты на языке Solidity.

Вывод: В результате выполнения работы был разработан протокол децентрализованного обеспечения ликвидности и обмена активов на Ethereum на основе технологии и описано экономическое обоснование проекта. Разработанный протокол и веб-приложение представляет из себя совокупность:

- блокчейна на основе существующей блокчейн платформы Ethereum;
- смарт-контрактов на языке Solidity для взаимодействия с блокчейном, логика управления ликвидностью и обмена активов, хранения информации об обмене и ликвидности;
- клиентскую часть веб-приложения для взаимодействия с системой.

БЛОКЧЕЙН АРХИТЕКТУРА, ТЕОРИЯ ИНТЕЛЛЕКТУАЛЬНЫХ КОНТРАКТОВ, АЛГОРИТМ РАБОТЫ ДЕЦЕНТРАЛИЗОВАННОЙ БИРЖИ, БЛОК, ЦИФРОВАЯ ПОДПИСЬ, ETHERIUM, BITCOIN

ANNOTATION

Final qualifying bachelor's work: 53 p., 14 fig., 1 appendix, 7 sources.

Topic: Decentralized protocol for automated liquidity provisioning on Ethereum.

Object of research: smart contract technology, decentralized asset exchange and liquidity provision.

Subject of research: decentralized protocol based on smart contract technology.

Purpose: development of a protocol to ensure liquidity using smart contract technology.

Results: As a result of the study, the possibility of using the technology to implement a decentralized protocol for providing liquidity and exchanging assets on Ethereum was assessed and smart contracts were developed in the Solidity language.

Conclusion: As a result of the work, a protocol for decentralized liquidity provision and the exchange of assets on Ethereum based on the technology was developed and the economic justification of the project was described. The developed protocol and web application is a collection of:

- blockchain based on the existing Ethereum blockchain platform;
- smart contracts in the Solidity language for interacting with the blockchain, logic for managing liquidity and exchanging assets, storing information about exchanges and liquidity;
- the client part of the web application to interact with the system.

BLOCKCHAIN ARCHITECTURE, THEORY OF INTELLECTUAL CONTRACTS, DECENTRALIZED EXCHANGE OPERATION ALGORITHM, BLOCK, DIGITAL SIGNATURE, ETHERIUM, BITCOIN

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ETH – Ethereum coin

BTC – Bitcoin coin

DeFi – це фінансові інструменти у вигляді сервісів і додатків, створених з використанням блокчейн технології

CEX – централізована біржа

DEX – децентралізована біржа

KYC – процедура перевірки і ідентифікації клієнта за допомогою його державних документів

ERC20 – це стандарт токенів на Ethereum

Liquidity provider / LP / Постачальник ліквідності – це той, хто вкладає еквівалентну вартість двох токенів ERC20 у пул ліквідності в парі і отримують винагороду.

DApp – децентралізований додаток

DAO – децентралізована автономна організація

ВСТУП

Smart contract на даний момент є однією з найбільш обговорюваних технологій і в своєму роді революційною інновацією, якій вже знайдено велику кількість застосувань в самих різних сферах.

Smart Contract – комп'ютерний алгоритм/программа, призначений для цифрової обробки, перевірки або забезпечення виконання взаємодії або виконання контракту, що дозволяє виконувати надійні транзакції (певний набір операцій) без нагляду/контролю третіх сторін.

До сьогодення обмін та зберігання активів (акції компаній, валюти і т.п.) здійснюється у централізованій манер, тобто є керуюча компанія яка надає послуги з зберігання/обміну/управління, такі компанії мають головний недолік - клієнти таких компаній повинні їй довіряти майже “на слово” і мати на увазі, що їх кошти не належать їм і можуть бути втрачені назавжди доки є в управлінні таких компаній. Користуючись таким підходом користувач має віддавати свої кошти в управління якійсь третій стороні, або навіть не мати доступу до послуг таких компаній із-за свого місця проживання або соціального статусу. Це є дуже небезпечно.

Саме в цій роботі запропоновано новий підхід, який дасть змогу користуватися послугами обміну активів, заробляти на них відсотки, надаючи ліквідність іншим користувачам. І все це буде децентралізовано, без керуючого центру або групи людей, які можуть цензурувати дії користувачів. Це буде продукт, який надасть змогу кожному бажаючому з будь-якої точки планети використовувати інструменти децентралізованих фінансів. У цьому допоможе децентралізована мережа Ethereum та smart contracts.

Головними перевагами зберігання та обробки даних в smart contract є безпека і прозорість, економія часу, коштів, швидке вирішення питань. Недоліками виступає складність створення, мала кількість досвіду, може мати баги в коді контракту, створеному програмістом.

Метою випускної кваліфікаційної роботи є розробка децентралізованого протоколу для автоматизованого забезпечення ліквідності та обміну активів на Ethereum.

Відповідно до поставленої мети в роботі вирішувалися наступні завдання:

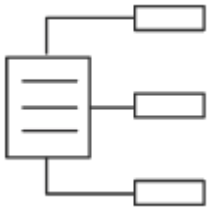
1. Аналіз та огляд існуючих інструментів для забезпечення ліквідності та обміну активів.
2. Розробка структури системи і схеми роботи смарт контрактів.
3. Розробка сервісу і смарт-контрактів.
4. Тестування і підведення підсумків.

РОЗДІЛ 1
ОГЛЯД ТЕХНОЛОГІЇ BLOCKCHAIN

Блокчейн - це спільна, незмінна база даних, яка полегшує процес реєстрації транзакцій та відстеження активів у діловій мережі. Актив може бути матеріальним (будинок, автомобіль, готівка, земля) або нематеріальним (інтелектуальна власність, патенти, авторські права, брендинг). Практично все, що має цінність, можна відстежувати та торгувати в мережі блокчейнів, зменшуючи ризик та зменшуючи витрати для всіх залучених[1].

Чому блокчейн важливий: бізнес працює на інформації. Чим швидше він отриманий і чим точніший, тим краще. Блокчейн ідеально підходить для передачі цієї інформації, оскільки він забезпечує негайну, спільну та повністю прозору інформацію, що зберігається у незмінній базі, до якої можуть отримати доступ лише дозволені учасники мережі. Мережа блокчейнів може відстежувати замовлення, платежі, рахунки, виробництво та багато іншого. І оскільки учасники поділяють єдиний погляд на істину, ви можете бачити всі деталі транзакції в кінці, надаючи вам більшої впевненості, а також нові ефективність та можливості.

Ключові елементи блокчейн технології:



Технологія розподіленої книги. Усі учасники мережі мають доступ до розподіленої книги та її незмінного запису транзакцій. За допомогою цієї спільної книги транзакції реєструються лише один раз, усуваючи дублювання, характерне для традиційних ділових мереж.

Незмінні записи. Жоден учасник не може змінити або підробити транзакцію після її запису до спільної книги. Якщо запис транзакції включає помилку, для усунення помилки необхідно додати нову транзакцію, і тоді обидві транзакції будуть видимими.

Розумні контракти. Набір правил - так званий розумний контракт - зберігається на блокчейні і виконується автоматично. Розумний контракт може визначати умови переказу корпоративних облігацій, включати умови страхування подорожей та багато іншого.

Типи мереж блокчейнів:

1. Загальнодоступні мережі блокчейнів. Публічний блокчейн - це той, до якого може приєднатися та взяти участь кожен, наприклад, біткойн. Недоліками можуть бути значні обчислювальні потужності, незначна або відсутність конфіденційності для транзакцій та слабка безпека. Це важливі міркування для випадків використання корпоративного блокчейна на підприємствах.
2. Приватні мережі блокчейнів. Приватна мережа блокчейнів, подібна до публічної мережі блокчейнів, є децентралізованою одноранговою мережею. Однак одна організація керує мережею, контролюючи, кому дозволено брати участь, виконувати консенсус-протокол та вести спільну книгу. Залежно від випадку використання, це може значно підвищити довіру та впевненість між учасниками. Приватний блокчейн можна запускати за корпоративним брандмауером і навіть розміщувати в приміщенні.

3. Дозволені мережі блокчейнів. Компанії, які створюють приватний блокчейн, як правило, створюють дозволену мережу блокчейнів. Важливо зазначити, що загальнодоступні мережі блокчейнів також можуть бути дозволені. Це встановлює обмеження щодо того, кому дозволено брати участь у мережі та в яких транзакціях. Учасники повинні отримати запрошення або дозвіл приєднатися.
4. Блокчейни консорціуму. Кілька організацій можуть розділити обов'язки щодо ведення блокчейну. Ці попередньо відібрані організації визначають, хто може подавати транзакції або отримувати доступ до даних. Блокчейн консорціуму ідеально підходить для бізнесу, коли всі учасники повинні мати дозвіл і нести спільну відповідальність за блокчейн.

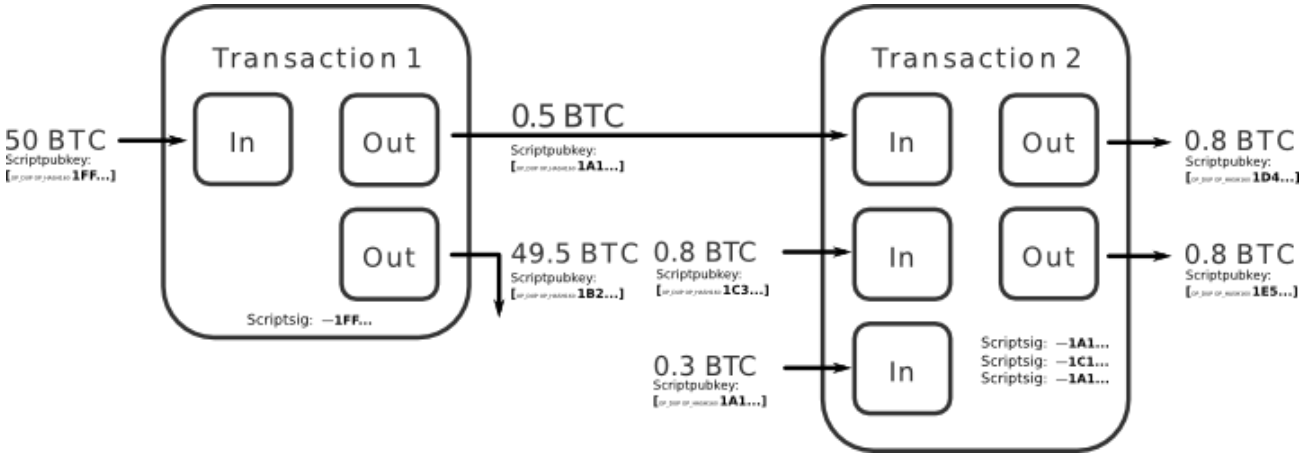


Рис. 1.1. Процес транзакції в біткойн блокчені

Якщо ви додаєте записи в blockchain, їх не можна змінити. Існує можливість скасувати зміни, але це вважається практично неможливим, оскільки для цього буде потрібна непоправна кількість обчислювальних ресурсів. Тому вам потрібно бути обережним, коли ви додаєте в нього інформацію.

1.1. Тенденції розвитку blockchain

Індустрія фінансових послуг - відкрита сфера, яка широко використовує технологію блокчейн, але не єдина. Forbes згадує охорону здоров'я, краудфандинг та спільний доступ до подорожей.

Подорожі.

Технологію блокчейн можна використовувати для таких речей, як:

- Відстеження багажу, особливо при декількох рейсах в одному маршруті та міжнародних рейсах;
- Визначення пасажирів, економія часу та скорочення ліній та часу очікування;
- Здійснення та приймання платежів за послуги;

Музика.

Зростання цифрової музики створив проблеми щодо таких питань, як піратство та компенсація за виконавців. Блокчейн може:

- Допомогти запобігти піратству (незаконному обміну) музичними файлами
- Використовуватися для компенсації виконавцям придбаних пісень та альбомів;

Кібербезпека.

Навіть така гігантська компанія, як Lockheed Martin, використовує Blockchain у своїх зусиллях з кібербезпеки. Блокчейн може:

- Допомогти захистити конфіденційні дані завдяки своїй функції криптографії;
- Усунути необхідність паролів, оскільки користувачів та пристрої можна аутентифікувати за допомогою відкритого та приватного ключів;

Людські ресурси.

Технологія блокчейн - це природне рішення для поліпшення трудомістких та дорогих процедур управління персоналом. Наприклад, він може:

- Усунути необхідність проводити індивідуальні перевірки потенційних працівників - транзакції блокчейну можуть зберігати дані про особу та історію зайнятості;
- Відстежувати платежі та витрати, роблячи речі, такі як сплата податків, набагато простішими як для роботодавців, так і для працівників;

Блокчейн як варіант використання у банківській діяльності.

Блокчейн знаходить відмінне використання в банківській діяльності. Відтепер користувач підтверджує свою особу в кожному банку, до якого він звертається, знову і знову. Чи можна полегшити процес за допомогою Blockchain? Відповідь - так. Ми можемо використовувати смарт-контракти, технології Blockchain.

1.2. Походження blockchain

У розвитку Інтернету можна вказати на знакові події, які можна використовувати для розподілу процесу на етапи. Серед цих важливих орієнтирів - створення перших широкомасштабних комп'ютерних мереж у 1960-х, розвиток системи електронної пошти в 1970-х, створення Ethernet пізніше у цьому десятилітті, запуск Всесвітньої мережі в 1990-х та створення перших браузерів і пошукових систем пізніше в тому десятилітті, серед інших. Після кожного з цих знакових подій Інтернет різко змінився.

Кожен крок був ключовим у створенні Інтернету, якого ми знаємо і на який покладаємось сьогодні.

Подібним чином можна озирнутися на розробку блокчейну, а також розділити його на етапи, які відзначаються важливими розробками та

винаходами. Технологія блокчейн існує лише частину часу, який має Інтернет, тому, ймовірно, все ще мають бути важливі події. Однак навіть зараз експерти почали ділити історію блокчейну щонайменше на три важливі етапи.

Етап 1: Біткойн та цифрові валюти

Поки ідеї, які могли б увійти в блокчейн, кружляли в спільнотах інформатики, саме псевдонім розробник біткойнів Сатосі Накамото описав блокчейн. Таким чином, технологія блокчейн почалася з мережі Біткойн. Хоча блокчейн з тих пір спостерігається у багатьох інших сферах, в якомусь сенсі він був розроблений спеціально для цієї цифрової валюти та для більш широкого просування цілей цифрових валют.

На самих ранніх етапах блокчейн створив основну передумову спільної публічної книги, яка підтримує мережу криптовалют. Ідея Сатоші про блокчейн використовує 1 мегабайт (МБ) блоків інформації про транзакції з біткойнами. Блоки пов’язані між собою за допомогою складного процесу криптографічної перевірки, утворюючи незмінний ланцюг.

Навіть у своїх найперших видах технологія блокчейн створила багато центральних особливостей цих систем, які залишаються і сьогодні. Справді, блокчейн біткойнів залишається в основному незмінним з цих перших зусиль.

Етап 2: Розумні контракти(Smart Contracts)

Із часом розробники почали вірити, що блокчейн може робити більше, ніж просто документувати транзакції. Наприклад, засновники Ethereum мали думку, що активи та довірчі угоди також можуть отримати вигоду від управління блокчейном. Таким чином, ethereum представляє друге покоління технології блокчейну.

Основним нововведенням, яке спричинив Ethereum, стала поява смарт-контрактів. Як правило, контракти в основному бізнесі управляються між двома окремими суб'єктами господарювання, іноді з іншими суб'єктами, які

допомагають у процесі нагляду. Розумні контракти - це ті, які самостійно управляють блокчейном. Вони викликані такою подією, як проходження терміну придатності або досягнення певної цінової цілі; у відповідь смарт-контракт керує собою, вносячи коригування за необхідності та без участі сторонніх організацій.

На даний момент ми все ще можемо використати невикористаний потенціал розумних контрактів. Таким чином, чи справді ми перейшли до наступного етапу розвитку блокчейну, дискусійно.

Етап 3: Майбутнє

Однією з головних проблем, з якими стикається блокчейн, є масштабування. Біткойн все ще турбує час обробки транзакцій та вузькі місця. Багато нових цифрових валют намагалися переглянути свій блокчейн, щоб вирішити ці проблеми, але з різним ступенем успіху.

У майбутньому одна з найважливіших розробок, що прокладає шлях для технології блокчейну в майбутньому, швидше за все, пов’язана з масштабованістю.

Окрім цього, постійно відкриваються та впроваджуються нові програми технології блокчейн.

Важко точно сказати, куди ці розробки приведуть технологію та криптовалютну галузь в цілому. Прихильники блокчейну, мабуть, знайдуть це неймовірно захоплюючим; з їхньої точки зору, ми живемо в епоху епохальної технології, яка продовжує зростати і розвиватися.

1.3. Ethereum (ETH) блокчейн

У Всесвіті Ethereum існує єдиний канонічний комп’ютер (який називається віртуальна машина Ethereum, або EVM), стан якого погоджуються всі в мережі Ethereum. Кожен, хто бере участь у мережі Ethereum (кожен вузол Ethereum), зберігає копію стану цього комп’ютера. Крім того, будь-який учасник може

транслювати запит для цього комп'ютера на довільне обчислення. Щоразу, коли такий запит транслюється, інші учасники мережі перевіряють, перевіряють та виконують («виконують») обчислення. Це спричиняє зміну стану в EVM, яка фіксується та поширюється по всій мережі.

Запити на обчислення називаються запитами на транзакції; запис усіх транзакцій, а також поточний стан EVM зберігається у блокчейні, який, у свою чергу, зберігається та узгоджується усіма вузлами.

Криптографічні механізми гарантують, що після перевірки транзакцій та додавання у блокчейн їх неможливо підробити пізніше; ті ж механізми також гарантують, що всі транзакції підписуються та виконуються з відповідними «дозволами» (ніхто не повинен мати можливості надсилати цифрові активи з рахунку Аліси, крім самої Аліси)[2].

Ключові визначення

- Ефір - це транзакційний coin, який використовується для сплати за операції в мережі Ethereum.
- Мережа Ethereum використовує технологію блокчейн, щоб зменшити зберігання споживчих даних та проведення операцій централізованими сервісами.
- Ефір - друга за величиною капіталізації крипто-валюта у світі, за загальною ринковою вартістю він поступається лише біткоіну (BTC).
- Розробники Ethereum почали працювати над переходом мережі на новий алгоритм консенсусу від підтвердження виконаної роботи (PoW) до системи підтвердження володіння часткою (PoS).

1.3.1. Розуміння ефіру (ETH)

Призначення Ether(ETH), криптовалюти, полягає у забезпеченні існування ринку для обчислень. Такий ринок забезпечує економічний стимул для учасників

перевіряти / виконувати запити на транзакції та надавати обчислювальні ресурси мережі.

Будь-який учасник, який транслює запит на транзакцію, також повинен запропонувати деяку кількість ефіру в мережу, як нагороду, яка буде надана тому, хто врешті-решт виконає роботу з перевірки транзакції, її виконання, передачі її в блокчейн і трансляції в мережу. .

Сума сплаченого ефіру є функцією тривалості обчислення. Це також заважає зловмисним учасникам навмисно засмічувати мережу, вимагаючи виконання нескінченних циклів або ресурсоємних сценаріїв, оскільки ці актори будуть постійно платити свої кошти.

1.3.2. Відмінність Ethereum від біткойна

Біткойн був першою криптовалютою і був в обігу з 2009 року. Ефіріум - це набагато новіший розвиток, який почне діяти в 2015 році.

За час між біткойнами та випуском Ефіріуму з’явилося багато інших криптовалют. Однак здебільшого вони обмежувались спробами вдосконалити аспекти ефективності роботи біткоіна - наприклад, збільшенням швидкості транзакцій або покращенням безпеки або анонімності транзакцій.

Ефіріум, звичайно, швидший за біткойн - транзакції, як правило, здійснюються за секунди, а не за хвилини. Хоча він все ще заснований на блокчейні і працює як накопичувач цінності, його шанувальники та євангелісти розглядають його як платформу для розподілених обчислень, яка постачається зі власною вбудованою валютою під назвою Ether.

Хоча блокчейн біткойнів можна просто зобразити як базу даних рахунків (або гаманців) із кількістю валюти, що зберігається в кожному, мережевий блокчейн Ethereum - це більш складна конструкція, здатна зберігати

комп'ютерний код / додатки , які можуть використовувати потужність процесора для виконання.

Мережа Ethereum також дозволяє створювати інші криптовалюти або токени, використовуючи той же протокол, що і Ether, але розподілений на різних блокчейнах, які можуть бути загальнодоступними або приватними. Біткоін не має такої змоги. Це означає, що вони можуть створюватися організаціями для представлення акцій, права голосу або як засіб підтвердження особи чи посвідчення особи[3].

1.4. Децентралізований протокол для автоматизованого забезпечення ліквідності та обміну активів

Централізована біржа (Binance, CEX.io, Kraken або OKEx) має власну книгу замовлень. При цьому кожне замовлення реєструється та перевіряється. Для забезпечення коректності дані обмінюються внутрішньо через виділені сервери та проходять централізовані процеси безпеки. Як правило, CEX працюють під регуляторним наглядом і мають вбудовану розгалужену політику знання своїх клієнтів.

Одночасно централізовані біржі активно здійснюють репресії проти шахраїв, дотримуючись чинного законодавства з метою запобігання відмиванню грошей.

Початківці, зокрема, використовують цей тип обміну, оскільки централізована структура забезпечує зручну платформу, що робить покупку та управління цифровими валютами особливо простими.

Обсяг замовлень та транзакцій, як правило, значно вищий, ніж у DEX. Це також пов’язано з тим, що вузли мережі не потребують оновлення в режимі реального часу. Як результат, швидкість торгів дуже висока. Однак описана раніше простота платформи вимагає, щоб приватні ключі інтегрованих гаманців залишалися на біржі. Отже, доступ до крипто-активів безпосередньо пов’язаний

з обліковими даними користувача. Якщо шахрай отримає доступ до облікових даних за допомогою фішингу або зламу, він матиме прямий доступ до збережених крипто-активів.

За CEX стоїть комерційна компанія. Щоб створити хороший досвід для користувачів, ці компанії часто пропонують широкий спектр послуг підтримки. Вони також дозволяють купувати криптовалюти проти фіатної валюти і, як правило, мають широкий спектр торгових пар. Централізовані біржі мають фіксовані комісійні, які виникають при торгівлі. Концептуально криптобіржа працює за тим же принципом, що і будь-яка інша біржа. Алгоритм відповідності регулює попит і пропозицію, а книга замовлень зберігає замовлення користувачів.

1.4.1. DEX - децентралізована біржа

Децентралізована біржа також пропонує основні функції CEX. Сюди входять Automated Market Maker (AMM), місце торгівлі, система відповідності та функції безпеки. Різниця до централізованих бірж полягає в тому, що всі ці функції децентралізовані.

З цією метою DEX не базується на внутрішніх серверах та власній IT-інфраструктурі, а діє як децентралізований додаток (dApp) на блокчейні.

Обмін регулюється за допомогою розумних контрактів, в яких сторони залучають кожну депозит активів, призначених для обміну.Користувачі децентралізованих бірж використовують такі біржі, головним чином завдяки двом характеристикам: анонімності та високій безпеці.

DEX є анонімними, оскільки для торгівлі майже не потрібні дані користувачів. Часто користувачам потрібна лише публічна адреса, щоб мати можливість торгувати на децентралізованій біржі. Немає третіх сторін (органів влади чи фінансових регуляторів), які б здійснювали моніторинг або нав'язування правил щодо біржі як децентралізованої програми. Ще однією причиною його успіху є високий рівень безпеки. Хоча користувачі CEX не мають контролю над

своїми приватними ключами, DEX не пропонує інтегрованого гарячого гаманця, а приватні ключі залишаються у власності користувачів.

1.4.2. Пул ліквідності та обмін активів

Пули ліквідності є однією з основних технологій, що лежать в основі екосистеми DeFi. Вони є невід'ємною частиною автоматизованих маркет-мейкерів (AMM).

Сама по собі ідея надзвичайно проста. Пул ліквідності - це в основному кошти, зібрані у велику цифрову купу. Пул ліквідності - це сукупність коштів, заблокованих у смарт-контракті. Пули ліквідності використовуються для сприяння децентралізованій торгівлі, кредитуванню та багатьом іншим функціям, які розглянемо пізніше. Користувачі, які називаються постачальниками ліквідності (LP), додають однакову вартість двох токенів у пулі, щоб створити ринок.

В обмін на надання своїх коштів вони заробляють комісійні з торгів, що відбуваються в їх пулі, пропорційно їх частці в загальній ліквідності.

Оскільки будь-хто може бути постачальником ліквідності, AMM зробили ринок більш доступним. Одним з перших протоколів, що використовував пули ліквідності, був Bancor.

Щоб зрозуміти, чим відрізняються пули ліквідності, давайте розглянемо фундаментальний блок електронних торгів - книгу замовлень.

Простіше кажучи, книга замовлень - це сукупність відкритих на даний момент замовлень для даного ринку. Система, яка узгоджує замовлення між собою, називається механізмом узгодження. Поряд із відповідним механізмом, книга замовлень є ядром будь-якої централізованої біржі (CEX).

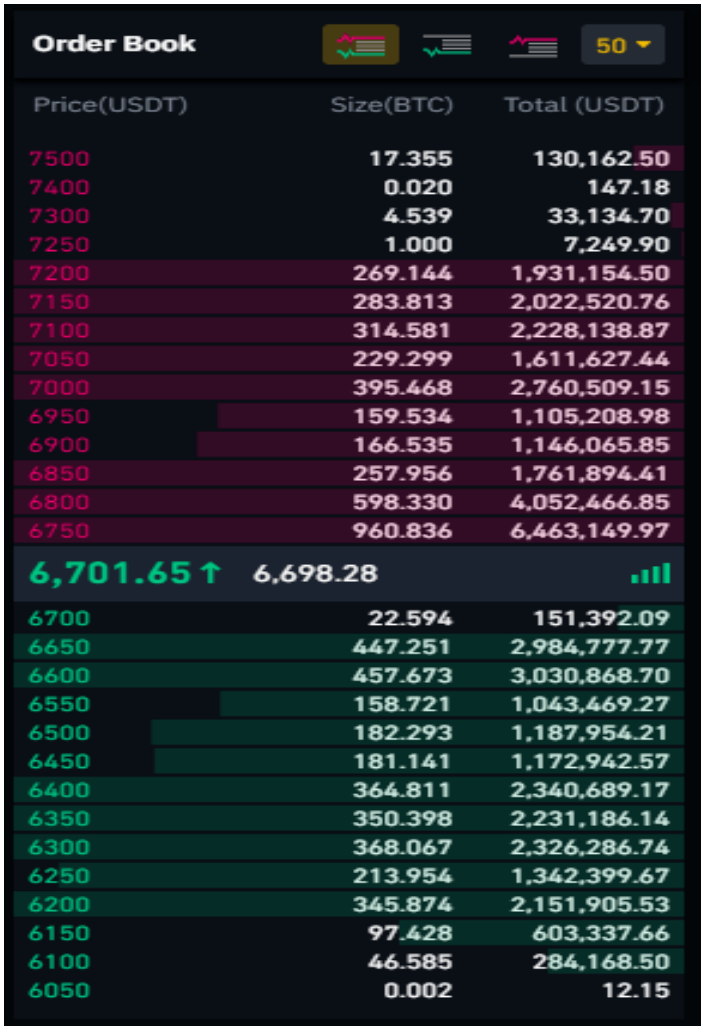


Рис. 1.2. Книга замовлень централізованої біржі

Однак торгівля DeFi передбачає здійснення торгів через мережу без централізованої сторони, що тримає кошти. Це представляє проблему, коли мова йде про замовлення книг. Кожна взаємодія з книгою замовлень вимагає плати за газ, що робить набагато дорожчим здійснення торгів.

1.4.3. Наслідки використання blockchain в забезпеченні ліквідності та обміну активів

Децентралізований обмін вільний від державних вимог, нормативних актів та моніторингу. Користувачі стикаються один з одним прямою торгівлею, і третя

сторона не бере участь в обміні. Кожен користувач має повний доступ до своїх приватних ключів і, отже, до своїх крипто-активів.

Анонімність, безумовно, є однією з основних причин торгівлі на DEX. Не існує процедури аутентифікації, немає KYC та особистих документів, завантажених на сервери за кордоном. Зазвичай достатньо особистої адреси у відповідному блокчейні, і торгівля може розпочатися. Обмін персональними даними між біржею та владою не здійснюється.

Зазвичай дешева торгівля з великою кількістю торгових пар відбувається через децентралізовану серверну мережу. Це надзвичайно мінімізує ризик хакерської атаки і робить недоступність через збої сервера практично неможливою. Оскільки DEX знаходиться безпосередньо на блокчейні, він не може націлювати атаку на центральний сервер.

РОЗДІЛ 2
ЗАСТОСОВУВАНІ ТЕХНОЛОГІЇ SMART CONTRACT

Проект, що розробляється, представляє собою протокол із набору смарт-контрактів написаних на мові Solidity та веб-додаток, з використанням REACT JS для реалізації клієнтського інтерфейсу, і Ethereum JavaScript API web3 для взаємодії з блокчейном.

2.1. Смарт-контракт

На дуже базовому рівні ви можете думати про смарт-контракт, як про своєрідну програму : сценарій, який при виклику з певними параметрами виконує певні дії або обчислення, якщо виконуються певні умови. Наприклад, простий інтелектуальний контракт постачальника може створити і передати право власності на цифровий актив, якщо абонент надсилає ефір конкретному одержувачу.

Будь-який розробник може створити розумний контракт і зробити його загальнодоступним для мережі, використовуючи блокчейн як рівень даних, за плату, що виплачується мережі. Потім будь-який користувач може зателефонувати за допомогою смарт-контракту для виконання його коду, знову ж таки за плату, сплачену мережі.

Таким чином, за допомогою смарт-контрактів розробники можуть створювати та розгортати довільно складні додатки та послуги, спрямовані на користувача: ринки, фінансові інструменти, ігри тощо[4].

2.1.1. Причини появи смарт-контрактів

Використання смарт-контрактів усуває необхідність в посередниках, значно знижуючи операційні витрати.

Хоча протокол біткоін вже багато років підтримує смарт-контракти, вони були популяризовані співзасновником Ethereum Віталіком Бутеріним. При цьому кожен блокчейн може створити інший метод реалізації смарт-контрактів.

2.1.2. Основи роботи смарт-контрактів

Розумні контракти засновані на технології blockchain. Це розподілений реєстр, який є децентралізованою системою, яка існує завдяки багатьом комп'ютерам, підключеним до однієї мережі.

Блокчейн дозволяє користувачам здійснювати операції, передавати інформацію та матеріальну цінність без банків та посередників.

Смарт-контракти - це програми, які створюються на основі комп'ютерної логіки і передаються у вигляді коду. Саме тому сторони договору можуть бути впевнені, що всі умови будуть дотримані, і жоден з учасників не зможе змінити умови чи інтерпретувати для себе. Кодекс - закон розумних договорів.

Принцип роботи блокчейна та смарт-контрактів:

• Ви хочете зробити транзакцію. Ця транзакція надсилається в комп'ютерну систему рівноправних вузлів (їх називають нодами);

• Вузлова мережа підтверджує стан транзакції та користувача;

• Після підтвердження транзакція поєднується з іншими транзакціями і утворює новий блок цифрового реєстру, який займає унікальне місце у ланцюзі блокчейн і не може бути змінений. Тоді транзакція вважається завершеною.

Тобто код смарт-контракту виконується в той момент, коли надійде транзакція або повідомлення. Це можна зробити з вашого рахунку, надіславши транзакцію або через інший розумний контракт, надіславши повідомлення. Код не має доступу до Інтернету, він також обмежений у доступі між смарт-контрактами.

Розумні контракти відповідають лише транзакціям. Засновник Ethereum пояснює роботу розумних контрактів так: актив або валюта передаються програмі, після чого вона починає стежити за виконанням умов договору.

Як тільки вони завершені, продавець отримує гроші, а покупець отримує товар. Роботу розумних контрактів можна порівняти з машиною продажу. Киньте монету і дістаньте товар без посередників, без допомоги сторонніх осіб.

Транзакція - це повідомлення, яке надсилається з одного облікового запису в інший обліковий запис (який може бути однаковим або порожнім).
Він може включати в себе двійкові дані (які називаються “корисним навантаженням”) і ефір. Якщо цільовий обліковий запис містить код, цей код виконується, а корисне навантаження надається в якості вхідних даних.

Якщо цільовий обліковий запис не встановлено (транзакція не має одержувача або одержувач встановлений на нуль), транзакція створює новий контракт.

При створенні кожної транзакції нараховується певна кількість газу, метою якого є обмеження обсягу робіт, необхідних для виконання операції, і одночасно оплатити це виконання. Поки EVM виконує транзакцію, газ поступово виснажується відповідно до конкретних правил.

Ціна на газ - це вартість, встановлена творцем транзакції, який повинен платити газ gas_price * gas перед відправкою рахунку. Якщо деякий газ залишиться після виконання, він повертається творцю таким же чином.
Якщо газ використовується в будь-якій точці (тобто він буде негативним), спрацьовує виключення поза газом, яке повертає всі модифікації, внесені в стан у поточному кадрі виклику.

2.1.3. Використання розумних контрактів

Найпростіший приклад використання розумних контрактів - це багатопідпис. За допомогою такого підпису сторони угоди можуть заморозити певну кількість монет на блокчейні, щоб у разі необхідності їх витратити підписи більше половини учасників[5].

Ця умова договору забезпечує безпеку коштів, вкладених у проект. У разі відмови кошти будуть повернені інвестору автоматично. Якщо збір заявленої суми був успішним, то учасники, які підписують багато підписів, активують свої ключі, підтверджуючи цілісність проекту, в який вони інвестують.

Смарт-контракти можуть бути використані для будь-якої фінансової діяльності у сфері страхування, реєстрації чи передачі майна, кредитування. Найбільш широко використання розумних договорів спостерігається у сфері бізнесу, де передбачені платежі та дії, передбачені платежами.

Сфери, в яких можна реалізувати смарт-контракти:

- Цифрова ідентичність. Розумні контракти забезпечують можливість контролю ваших даних, цифрових активів та репутації. Вирішіть, які дані можуть бути розкриті контрагентам, а які ні;
- можливість швидко перетворити його в готівку без значних фінансових втрат;
- Фінансові установи можуть використовувати фінансові договори для запису фінансових даних. Це допоможе об'єднати всі дані в єдиний реєстр та спростити обмін інформацією між організаціями. Це зменшить витрати на аудит та покращить подання фінансової звітності;
- Технологія смарт-контрактів забезпечує передачу майна без шахрайства;
- Завдяки розумним контрактам ви можете відслідковувати весь ланцюжок поставок товарів у режимі реального часу. Через Інтернет можна фіксувати переміщення товарів від магазину до полиці супермаркету;
- У галузі автомобільного страхування розумний контракт може зберігати страховий поліс, а також запис історії водіння автомобіля. Ви можете відправити запити в Інтернет речей, які можна встановити в машині, після події, і таким чином швидко встановити причину аварії;

2.1.4. Переваги і недоліки смарт-контрактів

Смарт-контракти мають такі переваги:

- Швидкість. Смарт контракти передбачають автоматизований процес і в більшості випадків не вимагають особистої участі, що заощаджує дорогоцінний час.

- Незалежність. Смарт-контракти виключають можливість втручання третіх сторін. Гарантія на транзакцію - сама програма, яка, на відміну від посередників, не дасть підстави сумніватися в її цілісності.

- Надійність. Дані, записані в blockchain, не можуть бути змінені або знищені. Якщо одна сторона угоди не виконує свої зобов'язання, інша сторона буде захищена умовами інтелектуального договору.

- Немає помилок - Автоматична система для виконання транзакцій і видалення людського фактора забезпечує високу точність при виконанні контрактів.

- Заощадження. Смарт-контракти можуть забезпечити значну економію за рахунок усунення витрат для посередників і скорочення операційних витрат, а також можливість для сторін працювати разом на більш вигідних умовах.

Смарт-контракти мають такі недоліки:

- Відсутність регулювання. У міжнародно-правовій області відсутні концепції «blockchain», «розумний контракт» і «криптовалюта».
- Складність реалізації. Інтеграція інтелектуальних контрактів з елементами реального світу часто займає багато часу, грошей, і зусилля.
- Неможливість зміни інтелектуального контракту. Парадоксально, що один з головних плюсів інтелектуальних контрактів також можна розглядати як конфлікт.

  Якщо сторони досягають більш вигідного угоди або виникають нові фактори, вони не зможуть змінити контракт. З цієї причини варіанти

додаткових угод повинні бути реалізовані в міру розробки нових blockchain платформ.

2.1.5. Порівняння розумних і “тупих” контрактів

«Тупі» контракти - це договори, які сильно покладаються на дії інших людей у функціональності. Ось чому їм потрібна довірена третя (юридична) сторона. При такому договорі люди легко вводяться в оману або обманюються.

Розумний контракт:

- Це програма або протокол транзакцій, який використовує блокчейн у своїй роботі;
- На основі коду
- Написано комп'ютерною мовою;
- Умови договору не можуть бути змінені;
- Умови договору автоматично виконуються всіма учасниками процесу;
- У разі порушення умов договору автоматично виникають штрафи, штрафи або санкції, передбачені договором;

Звичайний контракт:

- Паперова версія документів;
- Засновані на законі та законодавстві;
- Написано юридичною мовою;
- Умови договору можуть бути змінені, переписані або трактовані по-різному;
- Умови договору можуть бути невиконані або погано виконані;
- Якщо ви порушите умови договору, ви повинні звернутися до суду;
- Угоди реалізуються з багатьма посередниками. Необхідна допомога нотаріуса, адвоката та звернення до державних служб;

- Ймовірність шахрайства, хабарництва дуже висока.

2.1.6. Умови, що потрібні для створення смарт-контракту

Щоб створити інтелектуальний контракт, потрібно:

- Предмет контракту. Програма повинна мати доступ до товарів або послуг за контрактом для автоматичного блокування та розблокування;
- Цифрові підписи. Всі учасники ініціюють угоду шляхом підписання контракту зі своїми приватними ключами;
- Умови контракту. Умови смарт-контракту мають форму точної послідовності операцій. Усі учасники повинні підписати ці умови;
- Децентралізована платформа. Інтелектуальний контракт розгортається до Blockchain цієї платформи і розподіляється між вузлами платформи.

2.2. Solidity

Мова була створена в серпні 2014 року Гейвіном Вудом. Надалі розробка мови була під керівництвом Крістіана Райтвізнера командою Solidity в рамках проекту Ethereum. Це одна з чотирьох мов (Solidity, Serpent, LLL і Mutan), спроектованих для трансляції в байт код віртуальної машини Ethereum. Мова набула широкого поширення з появою технології блокчейн, зокрема технологій на основі Ethereum, для створення програмного забезпечення розумних контрактів[6].

Solidity статично типізована JavaScript-подібна мова програмування, створена для розробки самовиконуваних контрактів, що виконуються на віртуальній машині Ethereum (EVM). Програми на мові Solidity транслюються в байткод EVM.

РОЗДІЛ 3

ДЕЦЕНТРАЛІЗОВАНИЙ ПРОТОКОЛ ДЛЯ АВТОМАТИЗОВАНОГО ЗАБЕЗПЕЧЕННЯ ЛІКВІДНОСТІ НА ETHEREUM

В процесі виконання роботи був розроблений протокол для автоматизованого забезпечення ліквідності та обміну активів(ERC20 coins) на основі технології blockchain, з використанням блокчейну Ефіріуму та смарт-контрактами.

При розробці додатку використовувалися такі технології:

- REACT js
- Мова JavaScript;
- Ethereum Web3;
- Мова Solidity.

Для реалізації клієнтської частини використовувалися REACT js та мова JavaScript.

Для реалізації протоколу була вибрана мова Solidity.

Для взаємодії з блокчейном, і смарт-контрактами зокрема, використовувалося Ethereum JavaScript API Web3. Це дозволяє працювати з смарт-контрактами, та використовувати функціонал, який було написано в них з нашого веб-додатку.

3.1. Схема роботи протоколу

Автоматизований протокол ліквідності, який працює на основі постійної формули продукту і реалізований в системі смарт-контрактів, що не можна

оновити, на блокчейні Ethereum. Він позбавляє потреби в надійних посередниках, надаючи пріоритет децентралізації, цензурному опору та безпеці.

Кожен смарт-контракт протоколу або пара управляє пулом ліквідності, що складається із резервів двох токенів ERC-20.

3.1.1. Учасники екосистеми

Екосистема насамперед складається з двох типів користувачів: постачальників ліквідності та трейдерів. Постачальників ліквідності стимулюють вносити токени ERC-20 до загальних пулів ліквідності. Трейдери можуть обміняти ці токени між собою за фіксовану плату в розмірі 0,30% (яка надходить постачальникам ліквідності). Розробники можуть безпосередньо інтегруватися зі смарт-контрактами, щоб забезпечити нові захоплюючі взаємодії з токенами, торговими інтерфейсами, досвідом роздрібної торгівлі тощо.

Загалом, взаємодія між цими класами створює позитивний цикл зворотного зв'язку, що сприяє розвитку цифрових економік шляхом визначення загальної мови, за допомогою якої токени можна об’єднувати, торгувати та використовувати.

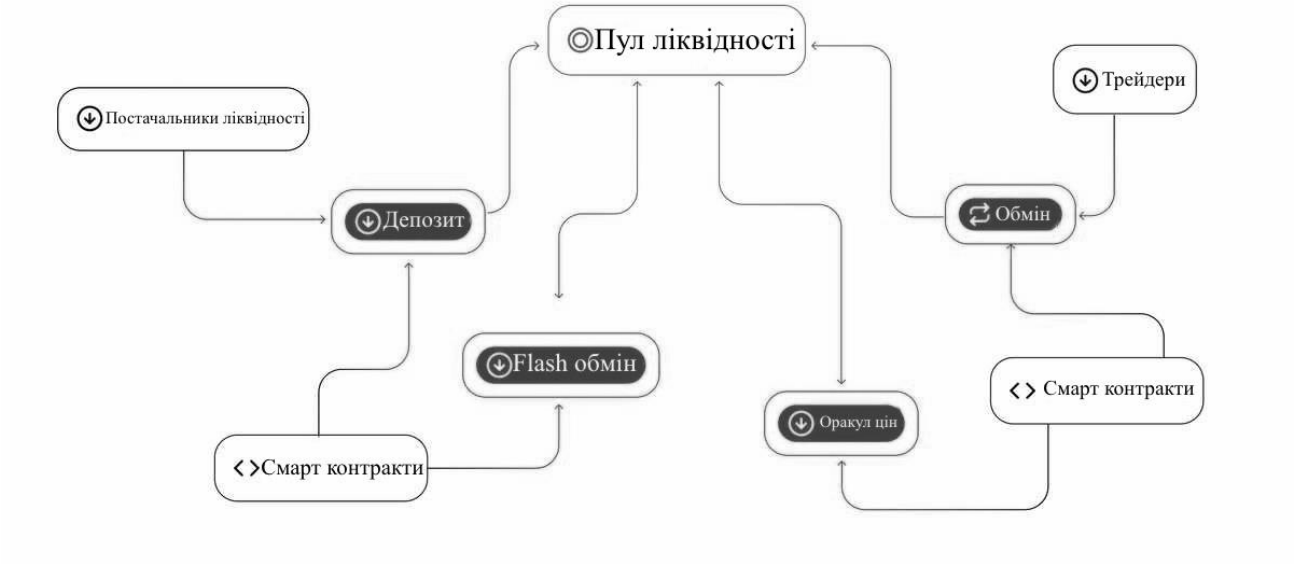


Рис. 3.1. Учасники екосистеми

Постачальники ліквідності або ЛП не є однорідною групою:

- Пасивні LP - це власники ERC-20, які хочуть пасивно інвестувати свої активи для накопичення торгових зборів.
- Професійні LP орієнтовані на маркетинг як свою основну стратегію. Зазвичай вони розробляють власні інструменти та способи відстеження своїх позицій ліквідності в різних проектах DeFi.
- Токен-проекти іноді вирішують стати LP, щоб створити ліквідний ринок для свого токена. Це дозволяє легше купувати та продавати токени, а також розблоковує взаємодію з іншими проектами DeFi.
- Нарешті, деякі піонери DeFi досліджують складні взаємодії щодо забезпечення ліквідності, такі як стимульована ліквідність, ліквідність як забезпечення та інші експериментальні стратегії.

У протокольній екосистемі існує кілька категорій торговців:

- Спекулянти використовують різноманітні інструменти та товари, створені спільнотою, для обміну токенами за допомогою ліквідності, витягнутої з протоколу.
- Арбітражні боти шукають прибуток, порівнюючи ціни на різних платформах, щоб знайти перевагу. (Хоча це може здатися добувчим, ці боти насправді допомагають вирівняти ціни на більш широких ринках Ефіріуму та підтримувати справедливість).
- Користувачі DAPP купують токени для використання в інших додатках на Ethereum.
- Розумні контракти, які виконують торгівлі за протоколом шляхом реалізації функцій обміну (від продуктів, таких як агрегатори DEX, до власних скриптів Solidity).

У всіх випадках за торгівлю передбачена однакова фіксована комісія за торгівлю за протоколом. Кожен з них важливий для підвищення точності цін та стимулювання ліквідності.

3.1.2. Модулі смарт контрактів

Протокол забезпечення ліквідності та обміну активів це - система смарт-контрактів. Core контракти забезпечують основні гарантії безпеки для всіх сторін, які взаємодіють з протоколом. Периферійні контракти взаємодіють з одним або кількома основними контрактами, але самі не є частиною ядра[7].

Core(Ядро)

Ядро складається з одиночної factory(фабрики) та безлічі пар ліквідності(pairs), де фабрика відповідає за створення та індексацію. Ці контракти досить мінімальні, навіть брутальні. Просте обґрунтування цього полягає в тому, що контракти з меншим функціоналом легше мігрувати, менш схильні до помилок і більш функціонально-елегантні. Мабуть, найбільшим плюсом цієї конструкції є те, що багато бажаних властивостей системи можна затвердити безпосередньо в коді, залишаючи мало місця для помилок. Однак одним мінусом є те, що основні контракти є дещо неприємними для користувачів. Насправді, безпосередня взаємодія з цими контрактами не рекомендується для більшості випадків використання. Натомість слід використовувати периферійний контракт.

Factory(фабрика)

Фабрика несе загальний байт-код, відповідальний за живлення пар. Його основна робота - створити один і лише один розумний контракт на унікальну пару токенів.

Pairs(пули ліквідності)

Пари мають дві основні цілі: виступати в ролі автоматизованих маркет-мейкерів та відстежувати залишки токенів пулу.

Вони також надають дані, які можна використовувати для побудови децентралізованих оракулів щодо цін.

3.1.3. Процес забезпечення ліквідності

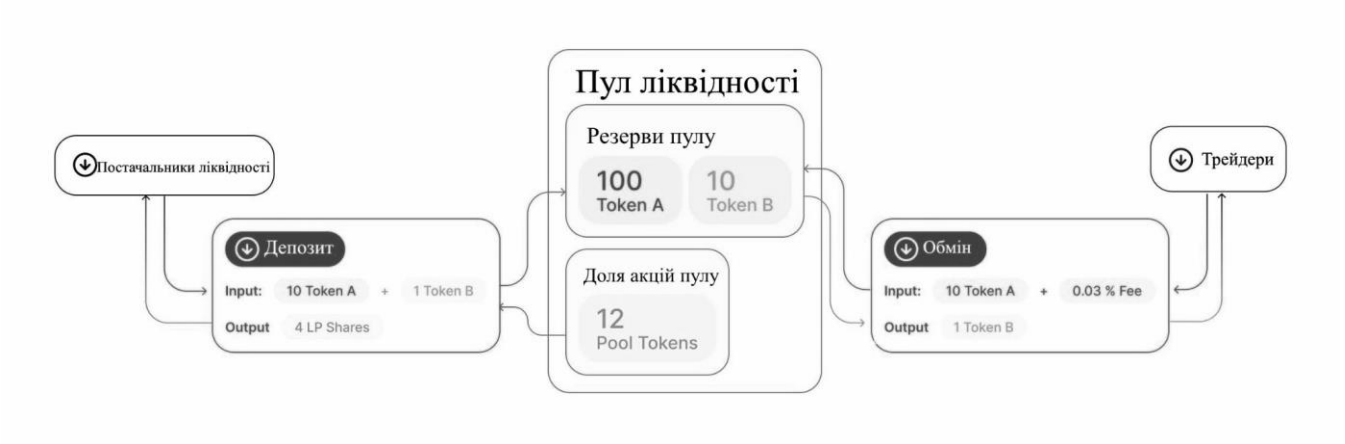


Рис. 3.2. Схема пулу ліквідності та взаємодії з ним

Будь-хто може стати постачальником ліквідності (LP) для пулу, депонуючи еквівалентну вартість кожного базового токена в обмін на токени пулу. Ці токени відстежують пропорційні частки LP у загальних резервах і можуть бути погашені за базові активи в будь-який час.

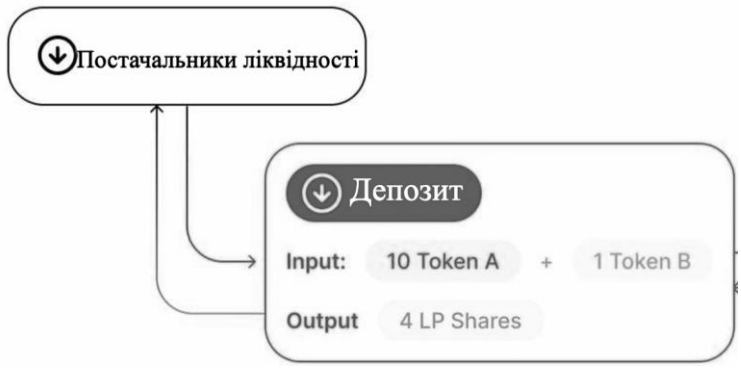


Рис. 3.3. Депозит ліквідності користувачем

Пари ліквідності виступають в ролі автоматизованих маркет-мейкерів, готових прийняти один токен за інший, доки зберігається формула "постійного товару".

Ця формула, найбільш просто виражена як **x * y = k**, стверджує, що торгівлі не повинні змінювати добуток (k) резервних залишків пари (x та y).

Оскільки k залишається незмінним порівняно з системою відліку торгівлі, її часто називають інваріантом. Ця формула має бажану властивість, яку великі

торгівлі (відносно резервів) виконують із експоненціально гіршими темпами, ніж менші.

На практиці протокол застосовує до угод 0,30% комісії, яка додається до резервів. В результаті кожна торгівля фактично збільшує k. Це функціонує як виплата LP, яка здійснюється, коли вони спалюють свої токени пулу, щоб вивести свою частину загальних резервів.

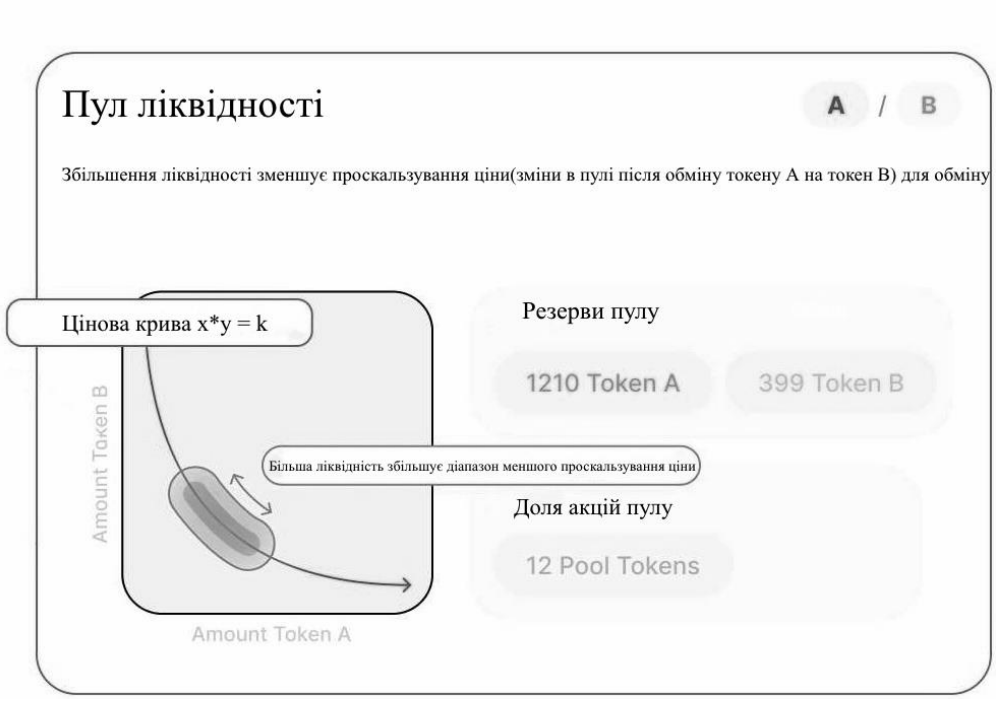


Рис. 3.4. Схема пари ліквідності

Slippage - Сума, за якою ціна рухається в торговій парі між поданням транзакції та її виконанням.

3.1.4. Процес обміну активів

Свопи(обмін**)** - це найпоширеніший спосіб взаємодії з протоколом. Для кінцевих користувачів обмін дається просто: користувач вибирає токен ERC-20, яким вони володіють, і токен, на який він хотів би його торгувати. Виконуючи своп, продаються поточні токени на пропорційну суму бажаних токенів, мінус плата за своп, яка присуджується постачальникам ліквідності.

На традиційному ринку книг замовлень значне замовлення на придбання ринку може вичерпати наявну ліквідність попереднього ліміт-продажу та продовжувати виконуватись за наступним ліміт-продажем за вищою ціною. В результаті кінцева ціна виконання замовлення знаходиться десь посередині між двома лімітно-цінами продажу, за якими було заповнене замовлення.

Вплив на ціну так само впливає на ціну виконання свопу, але є результатом іншої динаміки. При використанні автоматизованого маркет-мейкера відносна вартість одного активу з точки зору іншого безперервно змінюється під час виконання свопу, залишаючи остаточну ціну виконання десь між тим, де відносна ціна почалася - і закінчилася.

Ця динаміка впливає на кожен своп із використанням протоколу,оскільки він є невід'ємною частиною дизайну AMM.

Оскільки обсяг ліквідності, наявний у різних цінових точках, може змінюватися, вплив ціни на певний розмір свопу змінюється відносно обсягу ліквідності, наявної в будь-якій точці цінового простору. Чим більша ліквідність, доступна за даною ціною, тим менший вплив ціни на даний розмір свопу. Чим менша ліквідність, тим вищий вплив на ціну.

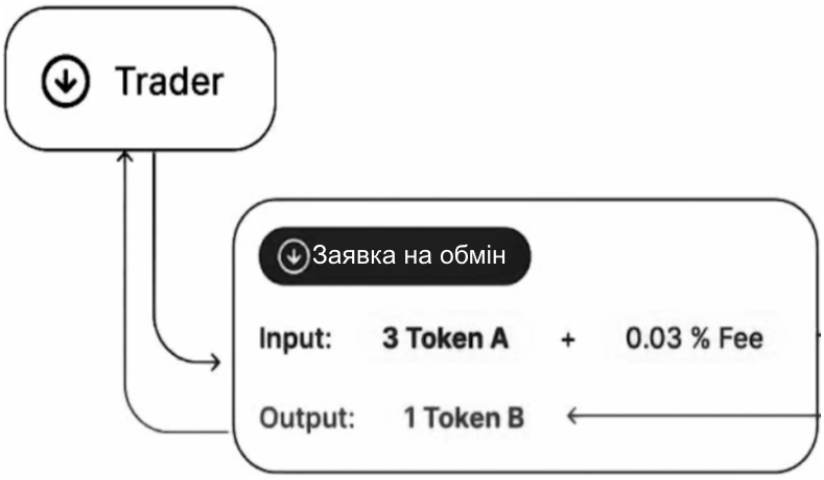


Рис. 3.4. Схема заявки на обмін активів

Далі визначаємо як пул ліквідності визначає ціну активів і працює при їх обміні. Ціна визначена співвідношенням активів у пулі. Уявіть, що ви хочете поміняти 50 A токенів на якомога більше B токенів зі свого смарт-контракту.

Перш ніж обмінятись, наші смарт-контракти повинні контролювати 50 A токенів. Найпростіший спосіб це зробити, визвати transferFrom на A контракті з власником, встановленим на msg.sender:

```
uint amountIn = 50 * 10 ** A.decimals();

A.transferFrom(msg.sender, address(this), amountIn);
```

Далі при обміні кількість B токенів у пулі зменшується що викликає дефіцит і у результаті збільшує ціну B токенів відносно A

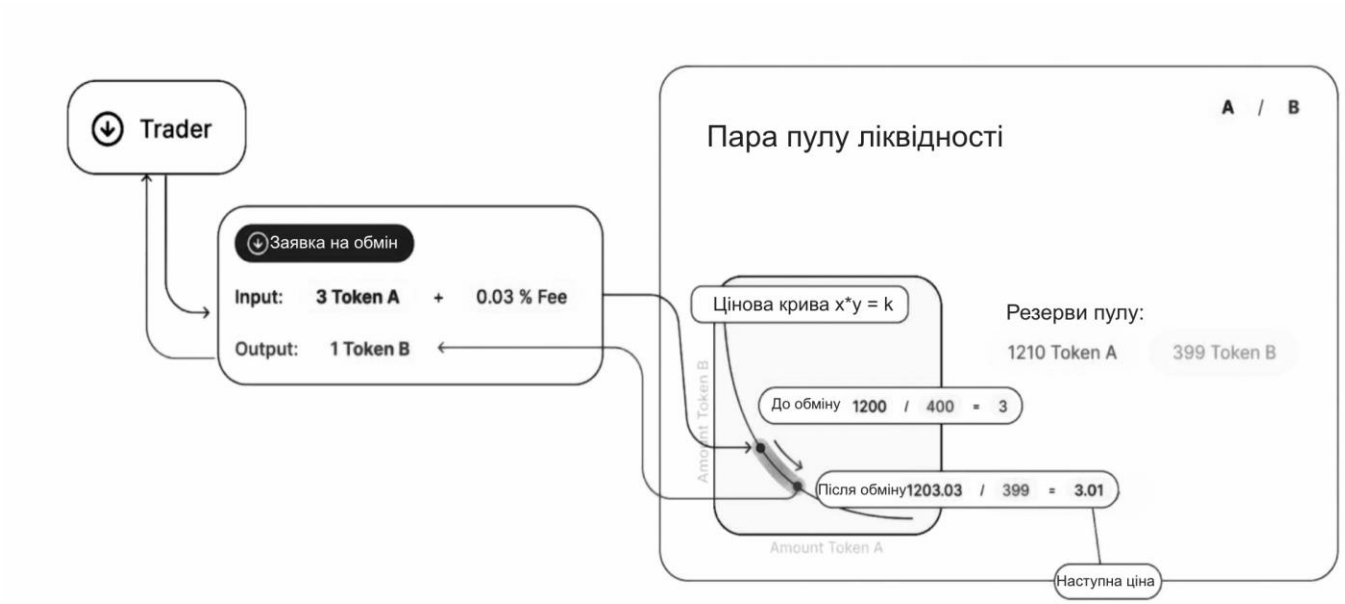


Рис. 3.5. Зміни у пулі ліквідності в момент обміну

3.2. Опис інтерфейсу сервісу

Дизайн системи я намагався зробити якомога простішим, як зрозуміло на ньому немає ні реєстрації ні інших відволікаючих речей. На головній сторінці (рис.4.) представлена форма створення обміну активів.

У верхній частині веб-додатку розташована навігаційна панель, з вкладками:

- Swap
- Pool
- Network ID
- Balance info

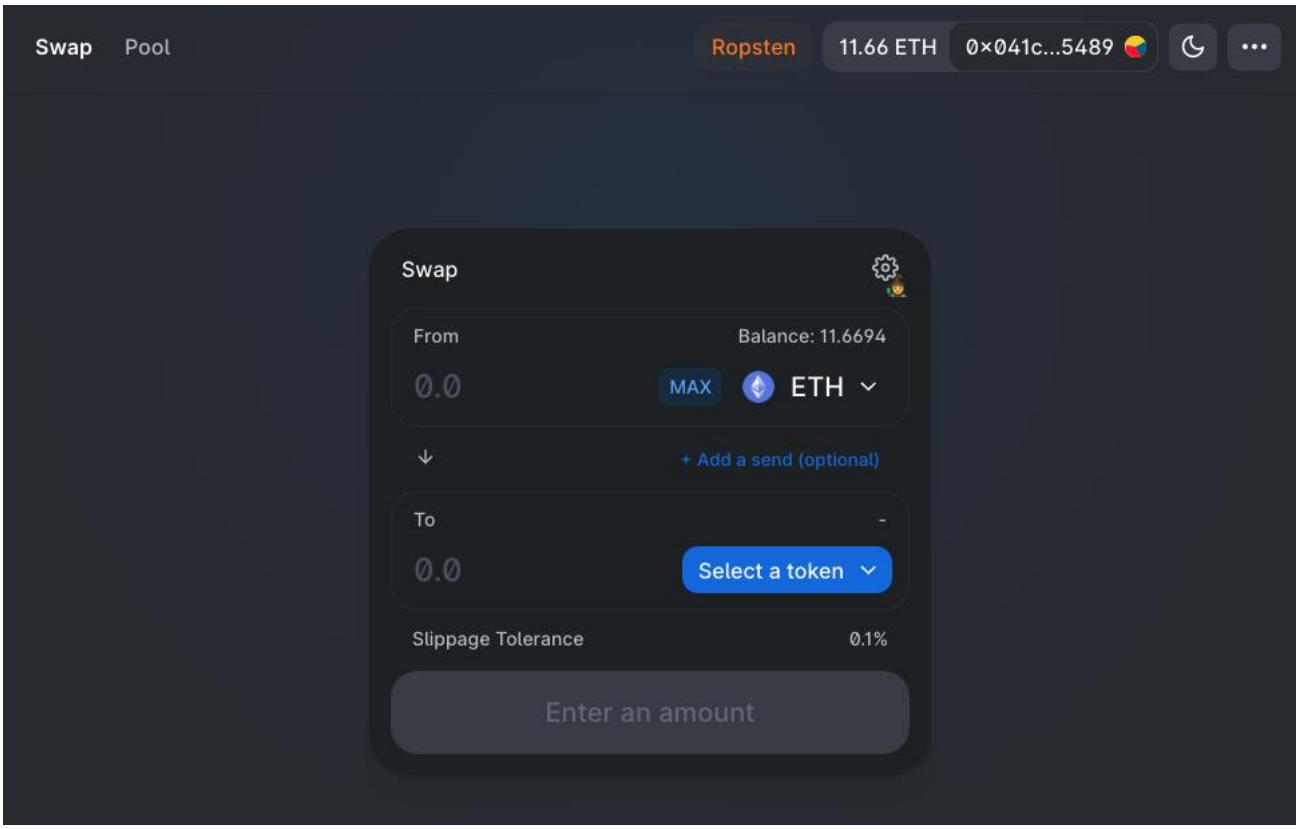


Рис. 3.6. Головна сторінка сайту

Першим кроком треба підключити гаманець (metaMask) до DApp. Саме після підключення гаманця веб застосунок матиме змогу перевірити баланс та надсилати транзакції користувачеві для підписання.

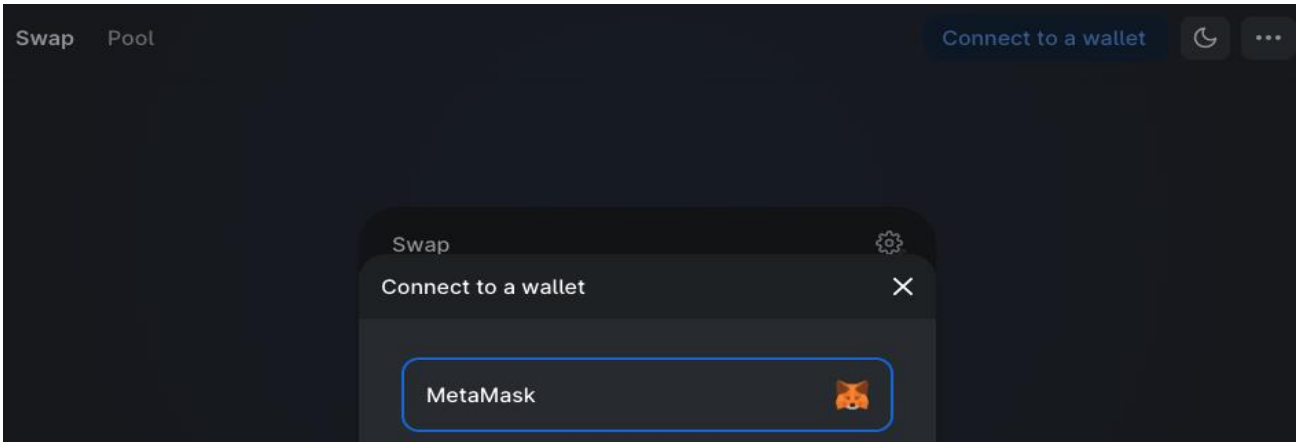


Рис. 3.7. Форма підключення гаманця.

Наступним кроком користувач має змогу вибрати який з його гаманців підключи.

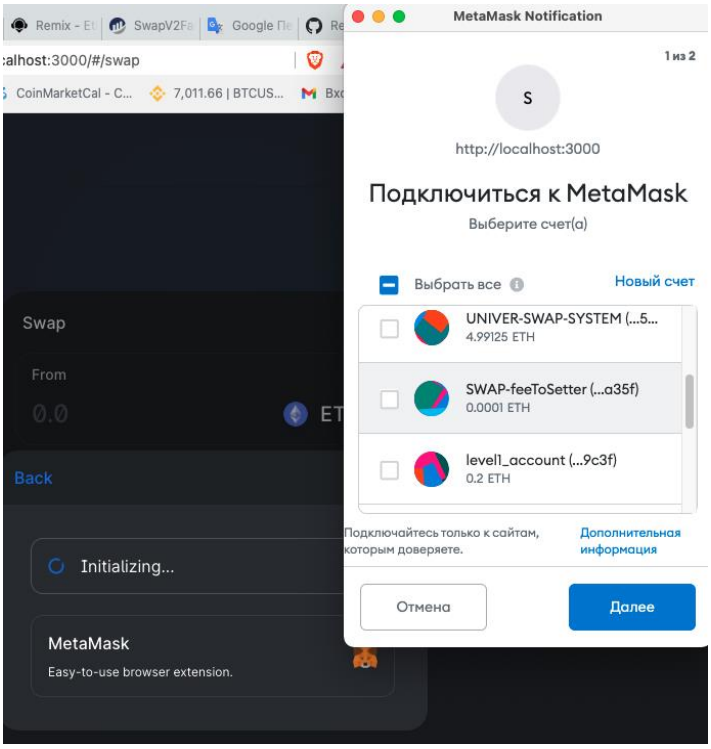


Рис. 3.8.Форма вибору гаманця для підключення.

Забезпечення ліквідності, як було описано вище пул ліквідності це пара активів які додаються до загальної ліквідності, а ті хто забезпечує пул ліквідності отримують винагороду у вигляді розподілення комісій згенерованих трейдерами.

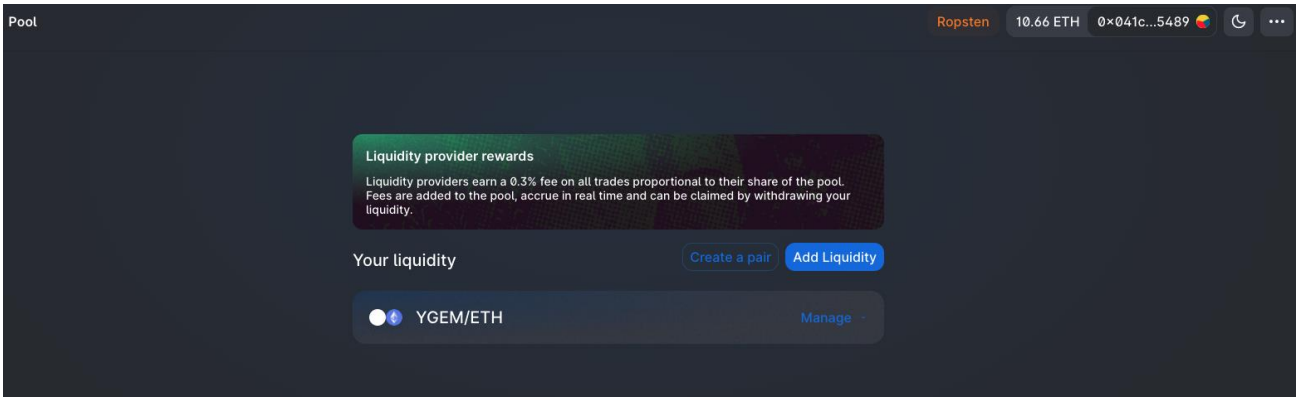


Рис. 3.9.Сторінка для менеджменту забезпеченою ліквідністю

На Рис. 3.9. відображена сторінка на якій користувач може переглянути свої вклади.

На ній ми маємо такі кнопки як:

1. Create a pair - визиває форму створення пулу ліквідності, якщо його ще немає у протоколі.
2. Add Liquidity - визиває форму для забезпечення ліквідністю вже існуючий пул.

Як приклад слід розпочати з Create a pair, тобто ми створимо новий пул в якому трейдери можуть здійснювати обмін токенізованого долара до гривні, а власники доларів та гривні можуть забезпечувати ліквідність пулу в децентралізований манер і заробляти на комісіях від обміну.

* Токенізовані(ERC20) долар і гривню я створив окремо, їх можна переглянути в мережі *Ropsten Testnet Network.*

Відповідні адреси смарт-контрактів долару та гривні:

UNIVER_SWAP_COIN_USDT - 0xdbe8f4aeb1bbac6ea8fc17e79ded954570a34369
UNIVER_SWAP_COIN_UAH - 0x9d5f6e229b401b24f309042341608ddf48f5aedc

Далі користувачеві треба вказати кількість токенів якою він хоче забезпечити пул ліквідності,а їх співвідношення калькулюється автоматично і являє собою первинну ціну активів (UAH per USDT).

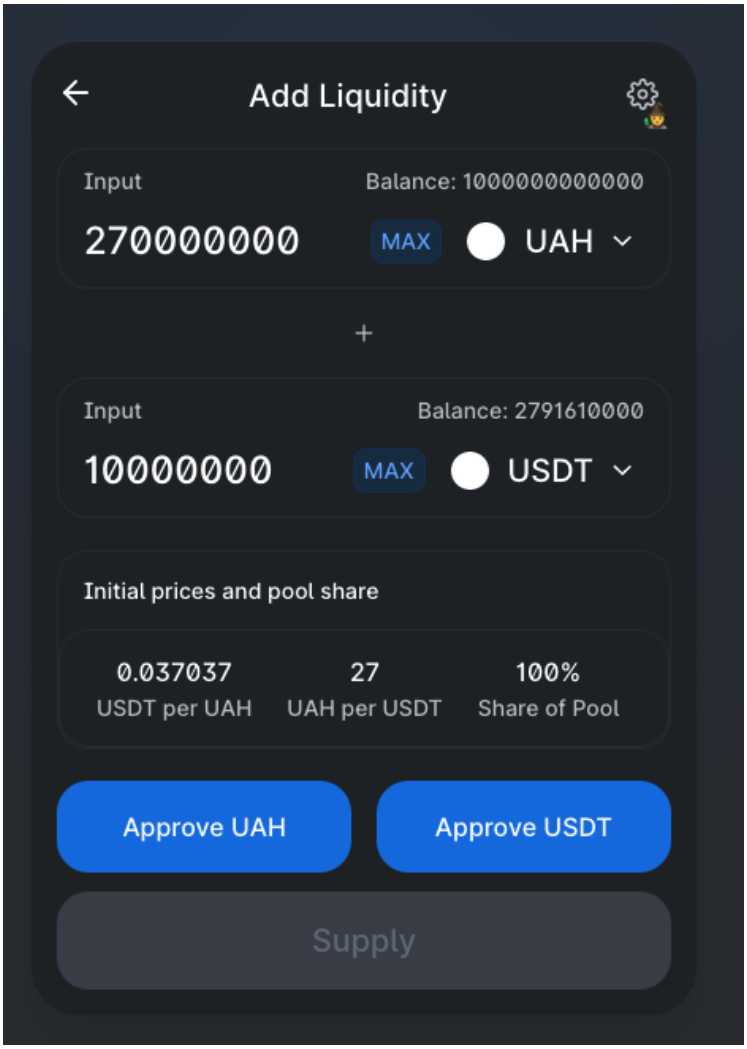


Рис. 3.10. Форма забезпечення пулу ліквідністю

Наступним кроком буде підтвердити(ERC20 approve) UAH та USDT для використання смарт контрактами протоколу (PROTOCOL FACTORY).

Рис. 3.10.1. Приклад методу ERC20 approve

Та натиснути кнопку Supply, яка сформує транзакцію на виклик методу addLiquidity у нашому протоколі та запуститься її в блокчейн.

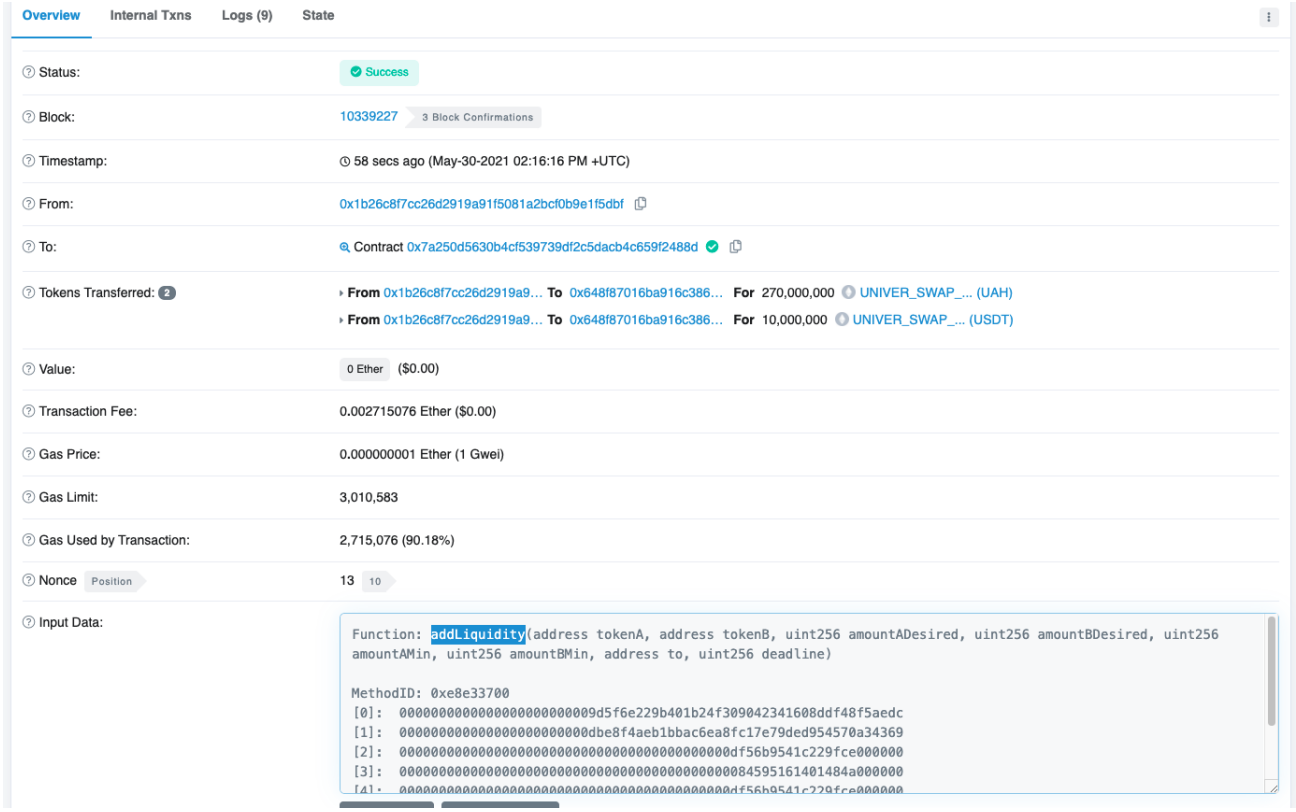


Рис. 3.11. Приклад Транзакції в блокчейні яка забезпечує пулу ліквідність

Після підтвердження транзакції майнерами ми маємо вихідні дані нашої долі в пулі ліквідності.

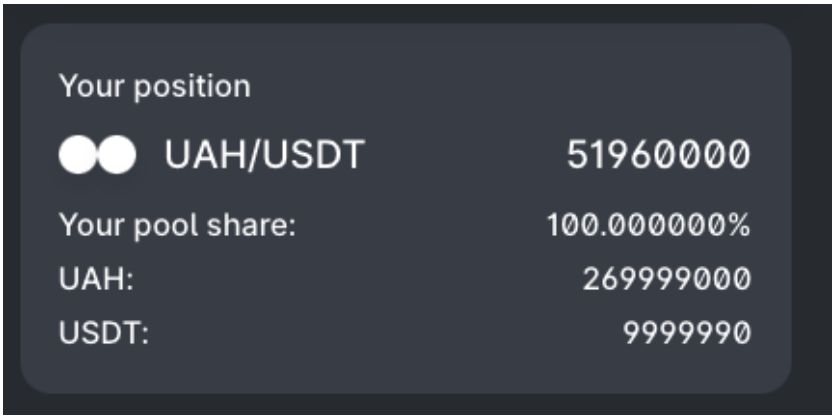


Рис. 3.12. Інформація про персональну ліквідність.

Swap(обмін) - саме те для чого пул забезпечують ліквідністю.Після того як ми забезпечили пул ліквідністю, інші користувачі децентралізованої мережі, або сам представник ліквідності можуть здійснювати обмін активів за описаним вище алгоритмом.

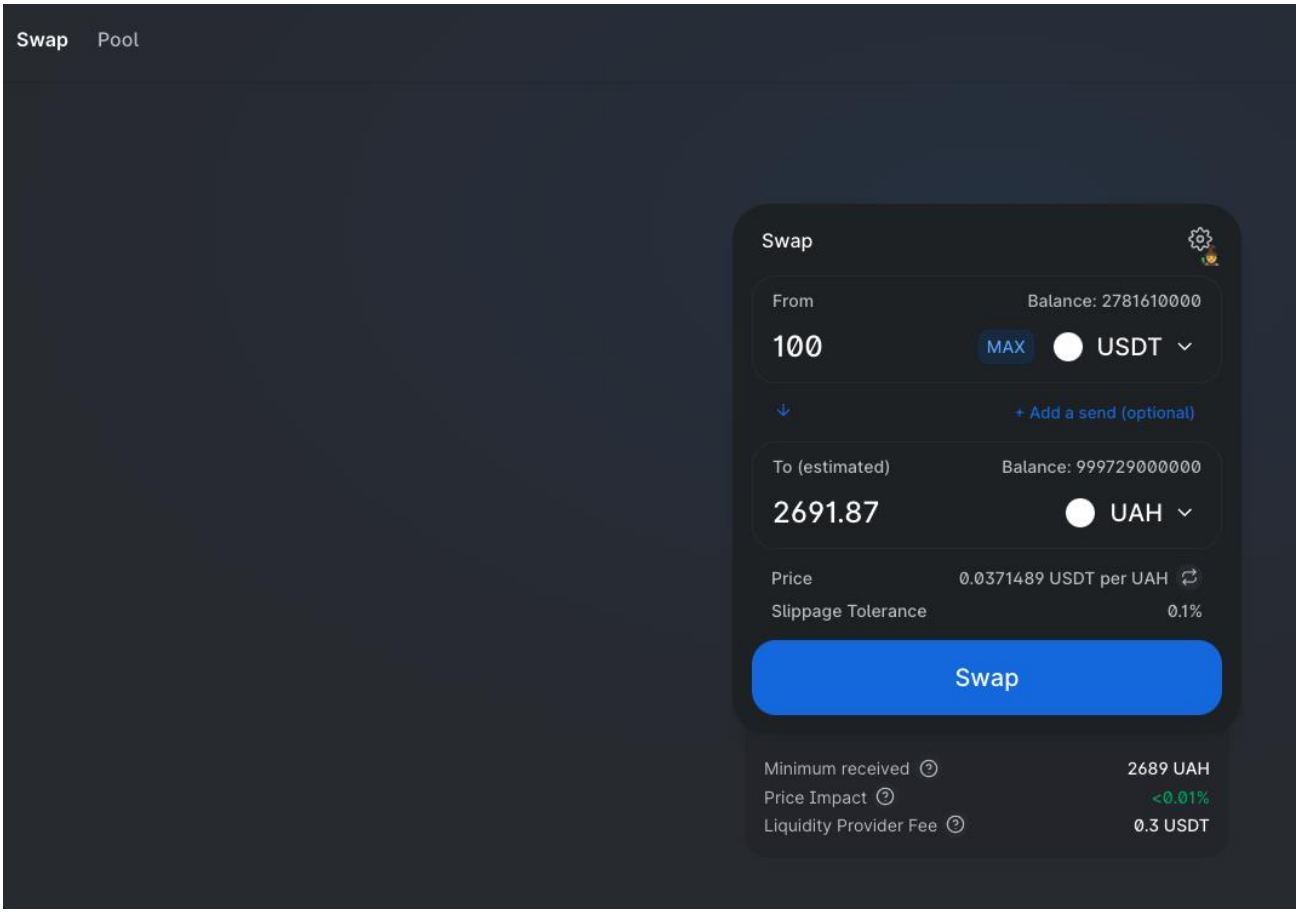


Рис. 3.13. Форма обміну активів.

Таким чином я обмінюю 100 USDT на UAH, по курсу який задається самим протоколом у блокчейні (смарт-контрактами). Я додаю USDT до пулу, а пул виділяє мені UAH по курсу - 0.3% комісій які будуть розподілені між постачальниками ліквідності .

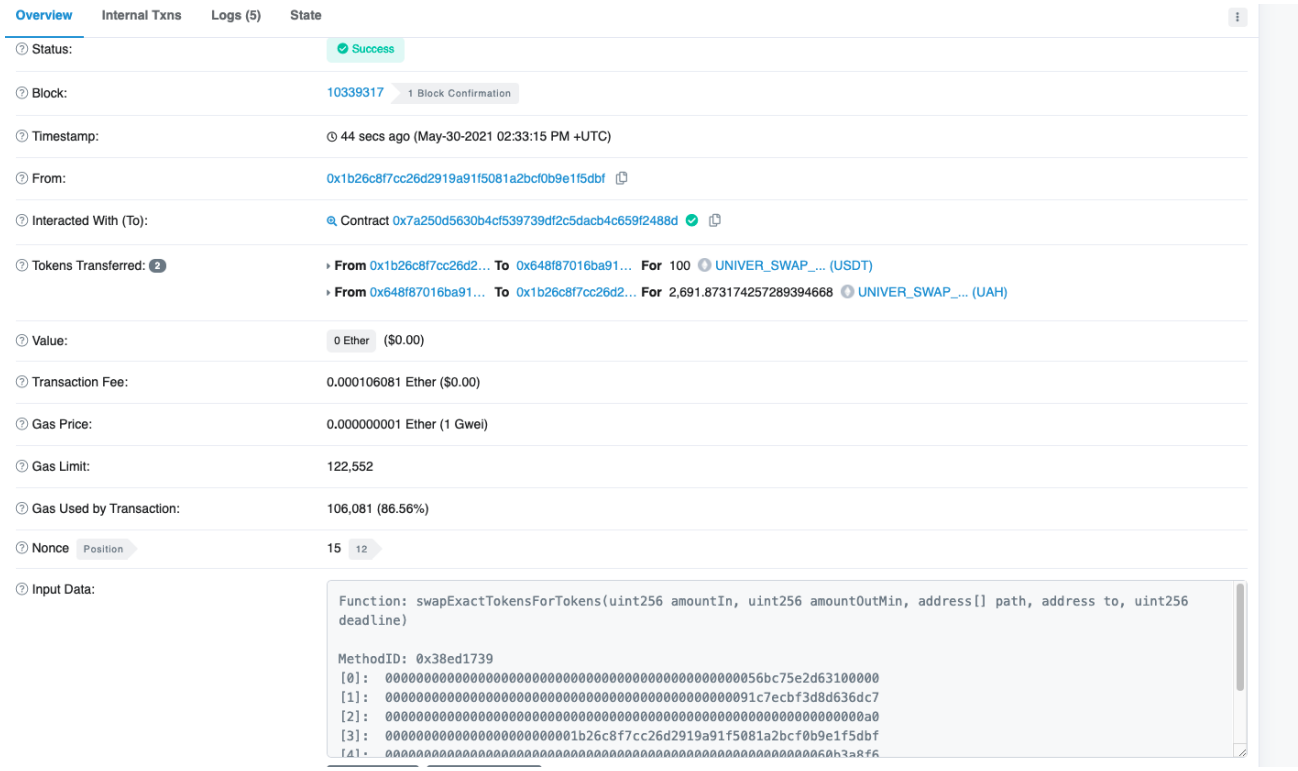


Рис. 3.14. Приклад транзакції обміну активів.

РОЗДІЛ 4
ФІНАНСОВЕ ОБҐРУНТУВАННЯ ПРОЕКТУ

Результати проведеного аналізу технології blockchain і можливості її використання в області децентралізованого забезпечення ліквідності та обміну активів дозволяють створити комерційну реалізацію сервісу. Для цього необхідно провести ряд організаційно-економічних заходів з метою оцінити економічну привабливість проекту. Для досягнення цієї мети були виділені наступні завдання:

- опис сервісу та протоколу загалом;
- аналіз ринку користувачів;
- визначення витрат на дослідницький проект.

4.1. Опис розробленої системи

Розроблюваний протокол та веб-додаток призначений для децентралізованого забезпечення ліквідності та обміну активів. Головною відмінністю від існуючих сервісів є використання технології blockchain, що дозволяє забезпечити найбільшу захищеність та одночасно з цим прозорість системи і конфіденційність по відношенню до користувачів.

Серед основних характеристик протоколу можна виділити наступні:

- безпека;
- надійність;
- прозорість;
- змога інтегрування з іншими протоколами;
- конфіденційність;
- зручність користування;
- висока продуктивність.

4.2. Аналіз ринку користувачів

Аналізований ринок користувачів складається насамперед з людей які не мають доступу до традиційних інструментів фінансово-технічної сфери. Одними з самих головних переваг є конфіденційність, простота в використанні, можливість використання іншими протоколами, саме тому головними користувачами будуть люди та програми які цінують ці якості.

4.3. Стратегія розвитку

Стратегія маркетингу включає заходи по встановленню товарної, збутової політики, ціноутворення, реклами та просування продукту. Також стратегія маркетингу повинна описувати позиціонування продукту на ринку.

Існує безліч сервісів для обміну крипто-активів, але всі вони засновані на традиційних базах даних, що робить їх уразливими.

На основі технології blockchain на даний момент немає повністю готових і добре себе зарекомендованих проектів, більшість з них знаходяться на стадії розробки.

Стратегія розвитку – проникнення на ринок з новим продуктом.

Розповсюдження Продукту передбачено у вигляді веб-сервісу та протоколу, до якого звертатимуться користувачі та розробники . Географічна зона поширення не обмежена і в поточний момент сервіс розроблений англійською мовою, але в планах є реалізувати сервіс на декількох мовах.

Для просування продукту передбачається популяризація серед амбіціозних розробників у сфері DEFI та користувачів крипто-систем, використовувати конференції в області інформаційних технологій і технології Blockchain з метою залучення уваги до продукту. Сам продукт я повністю народним благом, доступним кожному, вільним від регуляторів. Усі прибутки розподіляються згідно з долею вкладеного між тими хто забезпечує ліквідність для торгів і без комісій винахідникам та розробникам.

ВИСНОВКИ

В ході виконання роботи був розроблений протокол та сервіс для децентралізованого забезпечення ліквідності та обміну активів на основі технології blockchain, що включає:

- Смарт-контракти протоколу;
- Блокчейн Ethereum;
- Клієнтську частину веб-додатку, за допомогою якої користувачі взаємодіють з розробленою системою.

Є багато переваг використання цього протоколу перед традиційними біржами криптовалют. Інвестори, які використовують цей протокол, можуть обміняти свої криптовалюти безпосередньо зі своїх гаманців Ethereum, тому біржі не потрібно зберігати свої кошти. Це значно знижує ризик злому, додаючи рівень безпеки, якого централізовані біржі не можуть досягти. Більше того, інвесторам не потрібно створювати рахунок, це дозволяє їм торгувати криптовалютами анонімно.

Оскільки протокол децентралізований, жодна організація не контролює біржу, ніхто не може зупинити торгівлю активами.

Розроблений протокол володіє наступними характеристиками:

- безпека, що забезпечується незмінюваністю blockchain і необхідністю підтвердження дії всіма вузлами ланцюга;
- прозорість, що забезпечується завдяки blockchain;
- конфіденційність за рахунок зберігання транзакцій із зазначенням адрес електронного гаманця і контракту, а не імені користувача;
- інноваційність;

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Blockchain. URL:https://en.wikipedia.org/wiki/Blockchain
2. Dannen, Chris «Introducing Ethereum and Solidity». 2017
3. "A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses". ISSN 0360-0300.
4. Abhishek Chakravarty Prototyping a Blockchain Smart Contract. URL: https:/medium.com/@chakrvyuh/prototyping-a-blockchain-smart-contract-78877464e38e
5. Что такое смарт-контракты простым языком. URL:https://prostocoin.com/blog/smart-contract
6. Documentation Of Solidity. URL: https://solidity.readthedocs.io
7. Ethereum DApp documentation. URL: https://www.ethereum.org/en/latest.

ДОДАТОК А

Код смарт-контрактів протоколу :
https://github.com/DmytroShalaiev/Liquidity-protocol-production