Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інформаційно-аналітичних технологій та менеджменту
(повна назва)
Кафедра Інформатики
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

ДОСЛІДЖЕННЯ ТА ВИКОРИСТАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЇ ДЛЯ РОЗРОБКИ САЙТУ ТОКЕНІЗАЦІЇ МОНЕТ
(тема)

Виконав:
студент 2 курсу, групи ІНФм-21-1

Андрєєва А.Ю.
(прізвище, ініціали)

Спеціальності 122 Комп'ютерні науки
(код і повна назва спеціальності)

Тип програми освітньо-професійна

Освітня програма Інформатика
(повна назва освітньої програми)

Керівник доц. Руденко Д.О.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Кобилін О.А.
(підпис) (прізвище, ініціали)

2022 р.

Харківський національний університет радіоелектроніки

Факультет Інформаційно-аналітичних технологій та менеджменту
(повна назва)

Кафедра Інформатики
(повна назва)

Рівень вищої освіти другий (магістерський)

Спеціальність 122 Комп'ютерні науки
(код і повна назва)

Тип програми освітньо-професійна

Освітня програма Інформатика
(повна назва освітньої програми)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Андрєєвій Анастасії Юріївні
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження та використання блокчейн-технології для розробки сайту токенізації монет

затверджена наказом по університету від 9 листопада 2022 року №1469Ст

2. Термін подання студентом роботи до екзаменаційної комісії 25 листопада 2022 р.

3. Вихідні дані до роботи науково-методична та науково-технічна література, матеріали конференцій, дані інтернет-мережі.

4. Перелік питань, що потрібно опрацювати в роботі

1. Аналіз сучасного стану розвитку технологій блокчейн.
2. Дослідження принципів токенізації.
3. Дослідження різновидів систем блокчейн.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п. 5 включається до завдання за рішенням випускової кафедри) актуальність технологій блокчейн, постановка задачі, технологія токенізації монет, принцип роботи блокчейн-технології, порівняння блокчейн технологій, напрямки майбутніх досліджень.

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата
Консультант з дотримання діючих стандартів та норм	доц. Творошенко І. С.		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Отримання завдання на кваліфікаційну роботу	09.11.2022	
2	Аналіз завдання, підбір літератури	09.11.22-10.11.22	
3	Аналіз літератури з досліджуваної проблеми	10.11.22-12.11.22	
4	Аналіз проблеми	12.11.22-14.11.22	
5	Дослідження технології блокчейн	14.11.22-20.11.22	
6	Аналіз процесу токенізації	20.11.22-23.11.22	
7	Оформлення пояснювальної записки	23.11.22-30.11.22	
8	Перевірка на плагіат	30.11.22	
9	Рецензування	02.12.21	
10	Підготовка презентації та доповіді	03.12.22-04.12.22	
11	Занесення роботи в електронний архів	04.12.22	
12	Попередній захист кваліфікаційної роботи	05.12.22	

Дата видачі завдання 9 листопада 2022 р.

Студент _____
(підпис)

Керівник роботи _____ доц. Руденко Д.О.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ/ABSTRACT

Пояснювальна записка до кваліфікаційної роботи: 60 с., 1 табл., 30 рис., 40 джерел.

БЛОКЧЕЙН, ТОКЕНІЗАЦІЯ, МОНЕТИ, ТОКЕН, САЙТ ТОКЕНІЗАЦІЇ МОНЕТ, КРИПТОВАЛЮТИ, ТЕХНОЛОГІЯ РОЗПОДІЛЕНОЇ КНИГИ, ТРАНЗАКЦІЇ, SHA 256, ЛАНЦЮЖОК.

Об’єктом дослідження є технологія блокчейн в застосуванні процесу токенізації монет.

Метою дослідження є розробка сайту токенізації монет за допомогою засобів проєктування інформаційних систем та технології блокчейн.

Використано технологію блокчейн, її можливості, ключові компоненти, поняття токенізації монет. Проведено дослідження аналогів, моделювання структури, досліджено та використано технології блокчейн в процесі розробки сайту токенізації монет. В ході розробки залучено наступний стек технологій: Vue 2, MetaMask, Smart Contract, Ethereum, BNB. Розроблювана програмна система призначення для використання в Україні та за кордоном.

У результаті дослідження здійснена програмна реалізація вебзастосунку для токенізації монет.

BLOCKCHAIN, TOKENIZATION, COINS, TOKEN, COIN TOKENIZATION SITE, CRYPTOCURRENCIES, DISTRIBUTED LEDGER TECHNOLOGY, TRANSACTIONS, SHA 256, CHAIN.

The object of the research is blockchain technology in the application of the coin tokenization process.

The purpose of the research is to develop a web application using information systems design tools and blockchain technology for the development of a coin tokenization site.

Blockchain technology, its capabilities, key components, concepts of tokenization coins are used. Research of analogues, modeling of the structure was carried out, blockchain technologies were researched and used in the process of developing a coin tokenization site. During development, the following technology stack is involved: Vue 2, MetaMask, Smart Contract, Ethereum, BNB. A software assignment system is being developed for use in Ukraine and abroad.

As a result of the research, a software implementation of a web application for tokenization of coins was carried out.

ЗМІСТ

Перелік умовних позначень, символів, одиниць, скорочень і термінів 6
Вступ 7
1 Огляд основних методів 9
1.1 Технологія блокчейн 9
1.1.1 Аналіз технології блокчейн 9
1.1.2 Можливості технології блокчейн 11
1.1.3 Ключові компоненти технології блокчейн 13
1.1.4 Типи блокчейн-мереж 14
1.1.5 Блокчейн-протоколи 15
1.2 Поняття токенізації 16
1.3 Огляд аналогів 20
1.4 Постановка задачі дослідження 22
2 Моделі блокчейн-технології 24
2.1 Блокчейн-технологія 24
2.2 Принцип токенізації 30
3 Програмна реалізація сервісу токенізації монет 36
3.1 Вибір середовища 36
3.2 Інструкція користувача 38
3.3 Тестування розробленого сервісу 53
Висновки 55
Перелік джерел посилання 56
Додаток А Порівняння публічного та приватного блокчейну 60

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ПЗ – програмне забезпечення

БД – база даних

ПК – персональний комп’ютер

СКБД – система керування базами даних

ICO – Initial Coin Offering (первинна пропозиція монет)

BNB – Binance Coin (монета Бінанс)

AMM – Automated Market Maker (автоматизований маркет-мейкер)

ВСТУП

Блокчейн – новітня технологія, інтерес до якої виріс разом із популярністю криптовалют. Сьогодні її широко обговорюють не лише у світі фінансів. Блокчейн вже намагаються використовувати для зберігання та обробки персональних даних та ідентифікації, у маркетингу та комп'ютерних іграх.

У дослівному перекладі блокчейн – це безперервний ланцюжок блоків. У ній містяться всі записи про угоди. На відміну від звичайних баз даних, змінити чи видалити ці записи не можна, можна лише додати нові.

За останні роки система блокчейн розвивається та стає все більш популярною. Дану систему використовують все частіше.

Блокчейн був представлений як технологія, що лежить в основі Біткоїна – першої криптовалюти. Про це можна думати, як про інфраструктуру для криптовалюти – якби криптовалюти були автомобілями, блокчейн був би дорогою.

Криптовалюти, які використовують систему блокчейну, набувають все більшої впевненості та стають все більш розповсюдженими – деякі країни на законодавчому рівні признають криптовалюти на рівні звичних грошей.

Токенізація – це процес заміни фізичних чи юридичних активів токенами на блокчейні. Токенізувати можна практично все: від прав на витвір мистецтва і квартиру до контрактів на постачання нафти.

На побутовому рівні ми зустрічаємося з токенізацією, коли, наприклад, розплачуємося карткою: банки отримують не самі карти, а їх цифровий формат у вигляді токена. Таким чином, конфіденційна інформація не потрапляє до чужих рук.

Токенізація стала популярною концепцією в 2017 році на хвилі зростаючої популярності смарт-контрактів та ICO (Initial Coin Offering – «первинна пропозиція [розміщення] монет»). Тоді безліч проєктів зібрало величезні суми під гаслом токенізації якоїсь галузі чи індустрії [1]. При

цьому не так багато стартапів справді здійснили обіцянки, які вони дали інвесторам. Причина в тому, що для справжньої токенізації потрібна наявність регулювання, а воно тільки починає прийматися. Відповідно, і процес створення та введення в загальне застосування токенізованих активів може зайняти чимало часу. Тому це лише початок шляху.

Проте немає сумнівів, що вже в недалекому майбутньому людство почне все більше використовувати системи блокчейну в будь-яких галузях (в багатьох він вже пристосований до використання, в інших – знайде своє застосування з часом) [2]. Хоча серед експертів точаться деякі суперечки про майбутнє криптовалют, про світле майбутнє технології блокчейн сперечатися не доводиться.

Актуальність дослідження полягає у тому, що не дивлячись на всі недоліки системи блокчейн, очевидно, в майбутньому вона посідатиме точно не останнє місце серед актуальних та необхідних технологій. Більш того, усі недоліки системи будуть намагатися вирішити та нівелювати. Немає великих сумнівів щодо того, що це буде вдалим.

Крім того, використання технології блокчейн має забезпечити швидкі, надійні та прозорі транзакції з security-токенами, усунути кілька ланок у ланцюзі посередників, знизити комісії та загальні транзакційні витрати.

Саме тому створення сайту для токенізації монет зараз, коли ця галузь ще не досягла «буму» свого розвитку та містить колосальний потенціал, є як ніколи актуальним.

1 ОГЛЯД ОСНОВНИХ МЕТОДІВ

1.1 Технологія блокчейн

1.1.1 Аналіз технології блокчейн

Технологія блокчейн – вдосконалений механізм бази даних, який дозволяє організувати відкритий обмін інформацією у рамках бізнес-мережі. База даних блокчейна зберігає дані в блоках, пов’язаних між собою в ланцюжок. Дані хронологічно послідовні, оскільки не можна видаляти або змінювати ланцюжок без консенсусу з боку мережі. В результаті можна використовувати технологію блокчейн для створення незмінного або безстрокового реєстру для відстеження замовлень, платежів, рахунків та інших транзакцій. Система має вбудовані механізми, які запобігають несанкціонованому введенню транзакцій та створюють узгодженість у загальному поданні цих транзакцій.

Традиційні технології баз даних створюють низку проблем, пов’язаних з урахуванням фінансових операцій. Розглянемо приклад із продажем нерухомості. Після передачі грошей право власності переходить до покупця. Як покупець, так і продавець можуть самостійно реєструвати грошові операції, але жодної зі сторін не можна довіряти. Отримавши гроші, продавець може легко стверджувати, що він їх не отримав, а покупець може стверджувати, що гроші надіслано, навіть якщо це не так.

Щоб уникнути можливих юридичних проблем, довірена третя сторона повинна контролювати та підтверджувати транзакції [3]. Присутність цього центрального органу як ускладнює угоду, так й створює єдину вразливу точку. Від порушень у центральній базі даних постраждають обидві сторони.

Блокчейн передбачає такі проблеми шляхом створення децентралізованої, захищеної від несанкціонованого доступу системи для запису операцій. У разі угоди з нерухомістю блокчейн створює єдиний реєстр для покупця та продавця. Усі транзакції мають бути схвалені обома

сторонами та автоматично оновлюватись у їх реєстрах у режимі реального часу. Будь-яка невідповідність історії транзакцій позначиться у всьому реєстрі. Ці властивості технології блокчейн зробили її популярною у різних секторах. Наприклад, вони використовувалися під час створення цифрової валюти Bitcoin.

Блокчейн являє собою інноваційну технологію, що розвивається, яку впроваджують у різних галузях [4].

Слід розглянути приклади використання блокчейн-технології в різних сферах.

Блокчейн-технології вже використовуються в енергетичних компаніях для створення однорангових платформ для торгівлі енергоносіями та спрощення доступу до відновлюваних джерел енергії. Як приклад розглянемо такі види використання:

– енергетичні компанії, робота яких заснована на блокчейні, створили торгову платформу для продажу електроенергії між приватними особами. Власники будинків із сонячними батареями використовують цю платформу для продажу надлишків сонячної енергії сусідам. Процес практично повністю автоматизований: розумні лічильники створюють транзакції, а блокчейн їх записує;

– завдяки ініціативам блокчейн-краудфандингу користувачі можуть спонсорувати та утримувати сонячні батареї в районах, де немає доступу до електроенергії. Також після встановлення сонячних батарей спонсори можуть отримувати орендну плату.

Традиційні фінансові системи (наприклад, банки та фондові біржі) також використовують блокчейн-сервіси для управління онлайн-платежами, рахунками та ринковою торгівлею. Наприклад, інвестиційна холдингова компанія Singapore Exchange Limited, яка надає послуги з торговельних операцій по всій Азії, використовує технологію блокчейн для більш ефективного міжбанківського розрахунку [5]. Впровадження технології

блокчейн вирішило кілька проблем, серед яких пакетна обробка та ручна звірка кількох тисяч фінансових транзакцій.

Компанії зі сфери мультимедіа та розваг використовують блокчейн для керування даними про авторські права. Перевірка авторських прав грає ключову роль щодо справедливої винагороди творців. Для фіксації факту продажу чи передачі контенту, захищеного авторським правом, потрібно кілька транзакцій. Sony Music Entertainment Japan використовує блокчейн-сервіси для підвищення ефективності технічних засобів захисту авторських прав [6]. Успішне застосування стратегії блокчейна дозволило збільшити ефективність захисту авторських прав, знизивши витрати.

Роздрібні компанії використовують блокчейн для відстеження переміщення товарів між постачальниками та покупцями. Наприклад, Amazon подала патент на систему розподіленого реєстру, яка використовуватиме технологію блокчейн для перевірки справжності всіх товарів, що продаються на платформі [7]. На Amazon продавці можуть відображати свої глобальні ланцюжки поставок, дозволяючи учасникам (виробникам, кур'єрам, дистриб'юторам, кінцевим та вторинним користувачам) додавати події до реєстру після реєстрації в центрі сертифікації.

1.1.2 Можливості технології блокчейн

Важливо переглянути основні можливості технології блокчейн, такі як:

– децентралізація;

– незмінність;

– консенсус.

Децентралізація у блокчейні означає передачу контролю та прийняття рішень від централізованого суб'єкта (окремої особи, організації або їх групи) до розподіленої мережі. Прозорість децентралізованого блокчейну

дозволяє нівелювати довіру учасників один до одного [8]. Ці мережі стримують їхню владу або контроль одна над одною, що зберігає функціональні можливості мережі.

Незмінність означає, що дані неможливо змінити. Жоден учасник не може втрутитися в транзакцію після її внесення до Реєстру. Якщо запис містить помилку, для її виправлення необхідно додати нову транзакцію. У мережі будуть відображені обидві транзакції.

Система блокчейну встановлює набір правил, за допомогою яких учасники схвалюють транзакції. Нові транзакції можна реєструвати лише за згодою більшості учасників мережі.

До переваг блокчейн-технологій слід віднести розширені можливості забезпечення безпеки, підвищену ефективність, швидший аудит.

Розширені можливості забезпечення безпеки – блокчейн забезпечує високий рівень безпеки та довіри, якої потребують сучасні цифрові транзакції. Завжди є ризик, що хтось маніпулюватиме базовим програмним забезпеченням, щоб заробити гроші нечесним шляхом. Але три принципи блокчейну – криптографія, децентралізація та консенсус – забезпечують максимально безпечну базову систему, до якої практично неможливо втрутитися [9]. Система не має слабких місць і жоден користувач не зможе внести зміни до запису транзакцій.

Підвищена ефективність – операції між комерційними структурами можуть бути трудомісткими та займати багато часу, особливо щодо відповідності вимогам за участю третіх сторін. Такі особливості блокчейн, як прозорість та використання смарт-контрактів, прискорюють подібні ділові операції та роблять їх ефективнішими.

Швидший аудит – компанії повинні мати можливість генерувати, обмінювати, архівувати та відновлювати електронні операції надійним способом, що піддається перевірці. Записи зберігаються у хронологічно незмінному порядку. Така прозорість даних значно прискорює аудит.

1.1.3 Ключові компоненти технології блокчейн

До ключових компонентів, що лежать в основі технології блокчейну, належать наступні:

- розподілений реєстр;
- смарт-контракти;
- криптографія з відкритим ключем.

Розподілений реєстр – це загальна база даних у блокчейн-мережі, в якій зберігаються копії транзакцій (наприклад, у вигляді загального файлу, що редагується всіма учасниками). У більшості текстових редакторів будь-який користувач із правами редагування може видалити файл повністю [10]. Однак, технології розподілених реєстрів мають суворі правила щодо того, хто і як може редагувати файл. Наприклад, не можна видаляти записи після реєстрації.

Підприємства використовують смарт-контракти для самостійного управління комерційними угодами без залучення третьої сторони. Смарт-контракти – це програми в блокчейн-системі, що автоматично запускаються при дотриманні заданих умов. Транзакції записуються до Реєстру, якщо вони відповідають умовам перевірки «якщо, то» [11]. Наприклад, у логістичної компанії може бути укладено смарт-контракт, за яким оплата здійснюється автоматично після прибуття товару до порту.

Криптографія з відкритим ключем – це система безпеки, що дозволяє однозначно ідентифікувати учасників блокчейн-мережі. Система генерує два різні ключі для кожного користувача мережі. Один ключ – публічний, загальний для всіх учасників мережі. Другий – унікальний приватний ключ. Поєднання приватного та публічного ключів розблокують дані в реєстрі [12].

Наприклад, є два користувача мережі. Перший користувач записує транзакцію, зашифровану його приватним ключем. Другий користувач може розшифрувати її за допомогою свого публічного ключа. Таким чином, другий користувач може переконатися, що перший здійснив транзакцію. Якби

перший користувач скористався недійсним приватним ключем, другий не зміг б скористатися своїм публічним ключем.

1.1.4 Типи блокчейн-мереж

У блокчейні існує чотири основних типи децентралізованих або розподілених мереж:

– публічний блокчейн;
– приватний блокчейн;
– гібридний блокчейн;
– блокчейн-консорціуми.

Публічні блокчейни не вимагають дозволів і дозволяють будь-кому, хто бажає, приєднатися до мережі. Усі учасники блокчейну мають рівні права на читання, редагування та перевірку інформації. Для обміну та майнінгу таких криптовалют, як Bitcoin, Ethereum та Litecoin, в основному використовуються публічні блокчейни [13].

Приватні блокчейни, які можна назвати керованими, контролюються однією організацією. Уповноважений орган визначає, хто може бути учасником і які права в мережі вони мають. Приватні блокчейни децентралізовані лише частково, оскільки включають обмеження доступу. Приклад приватного блокчейна є Ripple – платформа для обміну цифрової валюти [14].

Гібридний блокчейн поєднує функції як приватних, так і публічних мереж. Підприємства можуть створювати як приватні, так і публічні системи дозволів. Таким чином, вони контролюють доступ до певних даних блокчейну, але при цьому підтримують загальнодоступний доступ до інших даних. Вони використовують смарт-контракти, що дозволяють публічним учасникам упевнитися у проведенні приватних транзакцій. Наприклад,

гібридні блокчейни можуть надавати публічний доступ до цифрової валюти, зберігаючи приватний доступ до банківської валюти.

Блокчейн-консорціумом управляє група організацій. Вибрані заздалегідь організації поділяють відповідальність за функціонування блокчейну та визначення прав доступу до даних. Блокчейн-консорціуми часто віддають перевагу компаніям-однодумцям, які отримують вигоду із загальної відповідальності [15]. Наприклад, Global Shipping Business Network – це некомерційний блокчейн-консорціум, що спеціалізується на цифровізації судноплавної галузі та розширенні співробітництва між операторами морських перевезень.

1.1.5 Блокчейн протоколи

Термін «блокчейн-протокол» відноситься до різних типів блокчейн-платформ для розробки застосунків. Кожен блокчейн-протокол адаптує базові принципи блокчейну до конкретних галузей чи застосунків. Нижче наведено деякі приклади блокчейн-протоколів.

Hyperledger Fabric – це проєкт з відкритим вихідним кодом, орієнтований на розробку інструментів та бібліотек. Компанії можуть використовувати його для швидкого та ефективного створення приватних блокчейн-застосунків. Hyperledge Fabric – модульна платформа загального призначення. Платформа пропонує унікальні можливості для ідентифікації та контролю доступу. Завдяки цим можливостям платформа підходить для відстеження ланцюжків поставок, торговельного фінансування, завдань лояльності та винагороди, а також для безготівкових розрахунків з фінансових активів.

Ethereum – це децентралізована блокчейн-платформа з відкритим вихідним кодом, яка використовується для створення публічних блокчейн-застосунків. Ethereum Enterprise призначено для комерційного використання.

Corda – блокчейн-проєкт з відкритим вихідним кодом для бізнесу [16]. Corda дозволяє створювати сумісні блокчейн-мережі, що гарантують строгу конфіденційність транзакцій. Компанії можуть використовувати технологію смарт-контрактів Corda для проведення швидких та безпечних угод. Більшість користувачів є фінансовими установами.

Quorum – це похідний від Ethereum блокчейн-протокол із відкритим вихідним кодом. Він призначений для використання в приватному блокчейні, де тільки один учасник володіє всіма вузлами, а також блокчейн-консорціумі, де кожен учасник володіє частиною мережі.

1.2 Поняття токенізації

В якійсь мірі можна уявляти блокчейн як реєстр рахунків користувачів, що ведеться в якомусь віртуальному децентралізованому комп'ютері.

На рахунку фіксується число віртуальних монет, що належить відповідному користувачеві – уявних об'єктів, характерних для даного блокчейну. Користувачі мають доступ до цього реєстру в тому сенсі, що кожен з них може зробити переклад монет зі свого рахунку на рахунок іншого користувача.

Для деяких цілей віртуальні монети, що зберігаються на рахунках у блокчейні, є зручною заміною справжніх («фіатних») грошей.

Для багатьох користувачів привабливою рисою віртуальних грошей є децентралізований характер блокчейну: на відміну від банку, блокчейн не може збанкрутувати.

Віртуальні монети, такі як Bitcoin або Ether, це просто запис у віртуальному реєстрі. Вони не мають «внутрішньої» вартості – тому, що вони не дають своїм власникам прав на будь-які цінності в реальному світі.

Віртуальні монети мають цінність виключно як зручний засіб платежу та накопичення – як свого часу у полінезійців раковини каурі [17]. Цінність

віртуальних монет походить не із закону чи договору, а скоріше зі звичаїв обороту.

Деякі блокчейни (такі як Ethereum, але не Bitcoin) дають користувачам можливість створювати та розміщувати в блокчейні власні комп'ютерні програми, які називаються смарт-контрактами.

Програма розміщується у віртуальному реєстрі на окремому рахунку та реагує на зовнішні сигнали від користувачів, які можуть надсилати на адресу цього рахунку монети або дані. У відповідь на подібні сигнали програма виконує передбачені її алгоритмом дії: змінює значення своїх внутрішніх змінних або спрямовує на ті чи інші адреси монети чи дані.

Поле можливого застосування смарт-контрактів дуже широке. Зокрема, вони можуть використовуватись для автоматизації виконання деяких договорів (звідки й назва смарт-контракт).

Але можливі інші варіанти використання смарт-контрактів: проведення голосувань, створення віртуальних організацій, випуск токенів тощо.

Якщо даний блокчейн підтримує досить багату мову програмування, то не важко написати смарт-контракт, який реалізує в собі реєстр власників деяких уявних об'єктів (токенів), характерних для даного смарт-контракту, так, що кожен користувач може переводити токени зі свого рахунку на рахунок іншого користувача [18].

Технічні характеристики токенів визначаються особливостями смарт-контакту, у якому ведеться реєстр утримувачів токенів. Згідно з прийнятим у блокчейні Ethereum стандартом ERC-20, у реєстрі фіксується лише загальна кількість токенів, що належить кожному користувачеві. Це означає, що токени не мають індивідуальної визначеності – так само, як і безготівкові гроші. Такі токени називають «взаємозамінними» (fungible) [19].

Подібні токени можна використовувати, зокрема, як свідоцтво про право на частку в активах чи доходах якогось бізнесу, тобто як аналог цінних паперів (security tokens). При цьому слід пам'ятати, що токен по суті своїй є не більше ніж запис у віртуальному реєстрі і сам не дає ніяких прав на частку

в бізнесі і т.п. Всі такі права мають договірну природу і, як правило, фіксуються в документі, що публікується емітентом, про випуск токенів (white paper).

Термін «токенізація» любить використовувати преса, але в нього немає певного правового значення [20]. По суті йдеться про те, що володар прав на витвір мистецтва випускає токен в якомусь блокчейні та оголошує, що разом із цим токеном передасть всі або деякі зі своїх прав на цей твір.

Відповідно, конкретне значення «токенізації» не визначено. Все залежить від конкретних умов випуску токена або двостороннього договору між продавцем та покупцем токена. Зрозуміло, за бажання того ж таки правового ефекту можна досягти без будь-якої токенізації, а просто підписанням договору [21].

Але картину як фізичний об’єкт «записати» у токен, звісно, не можна. Якщо мова йде про цифрове зображення, файл із цим зображенням в принципі можна записати безпосередньо в блокчейн (як значення однієї зі змінних відповідного смарт-контракту).

Однак зберігати дані в блокчейні дорого: вартість транзакцій зі створення смарт-контракту та подальшої передачі токена може виявитися позамежною [22]. З огляду на це до токену зазвичай прив’язують лише посилання на вебсторінку, де зберігається зображення.

Так чи інакше, важливо розуміти, що права на зображення у будь-якому випадку визначаються не тим, де воно записане, і не тим, хто має до нього фізичний доступ, а договором між власником прав на зображення та покупцем токена [23].

Проте, подібний прецедент був – у 2021 року преса повідомляла, що одна з «блокчейн-компаній» купила картину Бенксі за 95 тис. доларів, після чого публічно спалила її та «конвертувала в NFT-токен», який потім продала за 380 тис. доларів [24].

Мабуть, значною мірою це була просто рекламна акція блокчейн-компанії: за невеликі гроші її ім’я прогриміло по всьому світу. Схоже, у

організаторів акції непогане почуття гумору, оскільки сама картина є знущанням над ринком мистецтва: вона зображує аукціон картин і називається «Дебіли» (Morons). Поряд з аукціоністом намальовано напис у рамочці, що говорить: «Повірити не можу, що ці дебіли справді купують це лайно» [25].

Через те, що цифровий токен є правом на якийсь конкретний актив, який може мати цінність, важливо було придумати спосіб, у якому процес створення токена був прозорий та безпечний.

Більше того, можна уявити, що хтось вирішить створити токени на ділянку землі. Нам доводиться довіряти комусь, що ця ділянка землі реально є і знаходиться за зазначеною адресою (тут можуть бути вказані будь-які характеристики активу). Існує небезпека довіри. По-перше, є ризик, що цієї ділянки немає. По-друге, немає гарантії, що на одну ділянку не створено у сотні разів більше токенів, ніж їх має бути. Уявіть, що хтось розділив ділянку не на 1000 частин за «соткою», а 100 000 частин за соткою. Він просто сказав усім покупцям, що токенів лише 1000, а продав їх у сто разів більше [26].

Подібний сценарій множинного створення зобов'язань відбувається прямо зараз – будь-який центральний банк світу здійснює випуск (емісію) грошей на суму, що багаторазово перевищує його банківські резерви – часткове резервування [27].

Для того, щоб уникнути вищезгаданих прикладів, було створено новий облік грошей та нового виду активу – токенів (адже токени самі стали активами після того, як їх стало можливо купувати/продавати).

Саме для цього технологія блокчейн підходить якнайкраще – всі операції зі створенням токенів можна відстежити.

Блокчейн (ланцюжок блоків) – це розподілена база даних (розподілений реєстр даних), у якої пристрої зберігання даних не підключені до спільного єдиного центру обробки та зберігання інформації (серверу), вся інформація зберігається на багатьох комп'ютерах у всьому світі [28].

В результаті використання блокчейн для токенізації, будь-яку спробу несанкціонованого втручання в реєстр токенів на активи буде видно та припинено.

Більш того, завдяки блокчейну відпадає потреба в посередниках при купівлі/продажу токена на актив. Токен можна також швидко та легко купити/продати, як біткойн або іншу криптовалюту. Це порівняння приведене через те, що саме криптовалюти функціонують на технології блокчейну і їх з кожним днем можна буде купити все простіше.

Саме тому було вирішено дослідити технології блокчейну, та в ході дипломного дослідження розробити сайт токенізації монет із залучення технології блокчейн [29]. В процесі розробки необхідно проаналізувати конкурентні аналогічні сервіси.

1.3 Огляд аналогів

Біткоїн та інші криптовалюти з’явилися з «маніфестом» про незалежність та децентралізованість, але при цьому звичайні криптовалютні біржі сьогодні більше схожі на сайти брокерів фондових ринків. Частина з них, крім реєстрації, потребує повної верифікації особистості користувачів, а в деяких випадках і підтвердження права розпоряджатися криптовалютою [30].

Відповіддю індустрії, а також головним трендом 2020 року стали проєкти децентралізованих фінансів або DeFi (Decentralized finance) [31].

Тож слід розглянути найкращий з аналогів розроблюваного сервісу – PancakeSwap.finance.

Платформа PancakeSwap.finance – це децентралізована біржа, що працює у мережі Binance Smart Chain (BSC) [32]. Біржа не вимагає реєстрації, її користувачі не мають «особистого кабінету» у звичному сенсі. Для роботи з біржею користувачеві достатньо «пов’язати» свій гаманець із сайтом. Зараз

PancakeSwap підтримує безліч гаманців та універсальний конектор «WalletConnect». Але найзручнішим рішенням як для PancakeSwap, так і для інших децентралізованих майданчиків є гаманець-розширення MetaMask (рис. 1.1).

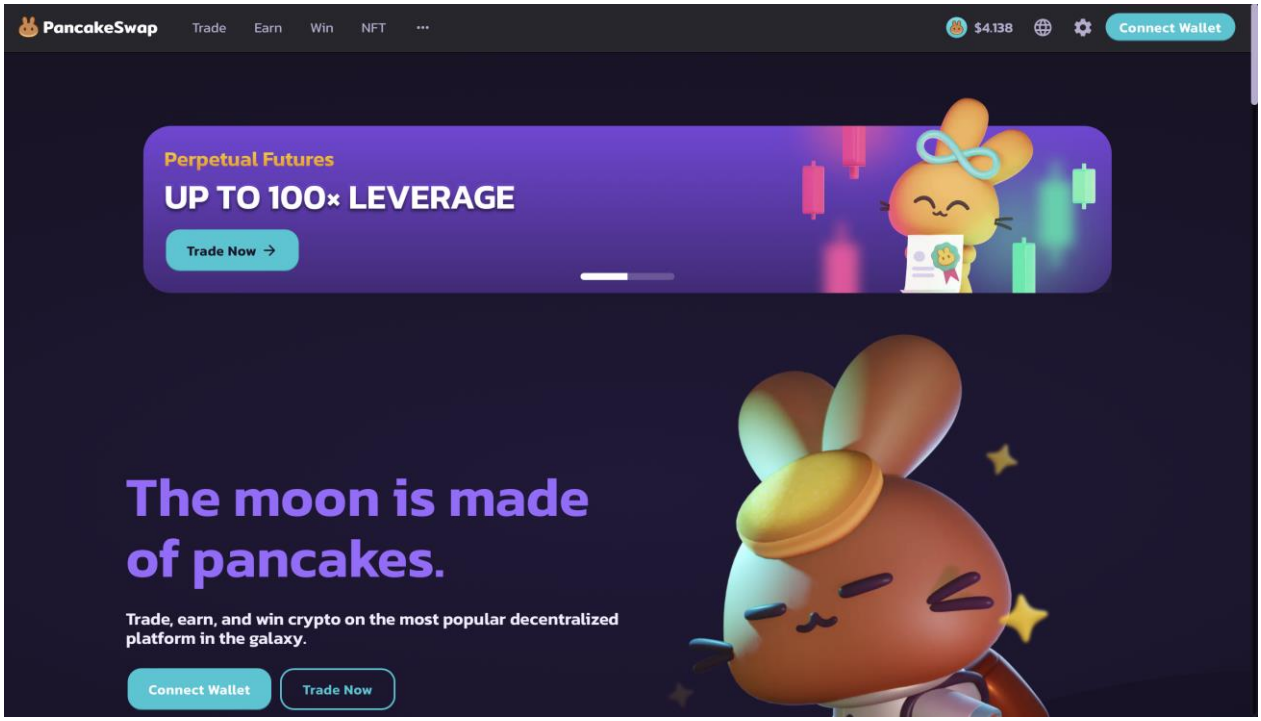

Рисунок 1.1 – Головна сторінка сервісу PancakeSwap.finance

Як і всі децентралізовані майданчики, біржа PancakeSwap працює на підставі смарт-контракту. Фактично, сайт біржі – це зовнішній інтерфейс, який зв’язує кошти користувачів із цим контрактом [33]. Усі угоди на біржі проходять у рамках блокчейну і не контролюються будь-ким безпосередньо. Розробники біржі можуть контролювати її роботу шляхом поновлення контракту, але не шляхом змін у блокчейні.

На сьогоднішній день майданчик підтримує такі операції:

– продаж та купівля токенів;
– розміщення коштів у пулах ліквідності;
– фармінг токенів;
– продаж карток передбачень;

– лотерея.

Переодично на PancakeSwap проходять колекційні контести та змагання трейдерів.

Щоб почати використовувати біржу PancakeSwap, необхідно встановити та налаштувати гаманець MetaMask, а також додати до нього мережу Binance Smart Chain (BSC). Після цього потрібно поповнити гаманець токенами BNB – ці нативні токени мережі BSC знадобляться для оплати транзакцій. Найпростіше купити BNB прямо на біржі Binance.

Після підготовчого етапу слід перейти на офіційний сайт біржі Pancakeswap.finance.

Слід обрати MetaMask і підтвердити цю дію у спливаючому вікні гаманця [34]. При з'єднанні з біржею, у верхньому правому куті з'явиться останні цифри/літери адреси гаманця.

Далі можна перейти до підрозділу «Обмін» у розділі «Угоди», обрати монети для обміну.

Вибравши токени та вказавши суми, можна проводити обмін. У спливаючому вікні з підтвердженням транзакції можна ще раз перевірити суму обміну та найменування монет.

Після підтвердження на сайті з'явиться вікно підтвердження у гаманці MetaMask. Коли обмін здійснено, спливе відповідне повідомлення на біржі, а гаманець MetaMask запропонує додати новий токен до списку монет [35].

Тепер у гаманці мають відобразитися куплені монети.

PancakeSwap – це найбільший AMM (Automated Market Maker) Binance Smart Chain (BSC) з інноваційними функціями [36].

1.4 Постановка задачі дослідження

Об'єктом дослідження є технологія блокчейн в застосуванні процесу токенізації монет.

Метою дослідження є розробка сайту токенізації монет за допомогою засобів проєктування інформаційних систем та технології блокчейн.

Використати технологію блокчейн, її можливості, ключові компоненти, поняття токенізації монет. Провести дослідження аналогів, змоделювати структури, дослідити та використати технології блокчейн в процесі розробки сайту токенізації монет. В ході розробки залучити наступний стек технологій: Vue 2, MetaMask, Smart Contract, Ethereum, BNB.

Для досягнення мети необхідно вирішити такі завдання:

– дослідити технологію блокчейн;

– провести аналіз процесу токенізації;

– провести дослідження аналогів;

– використати технологію блокчейн в процесі розробки сервісу токенізації монет.

Готовий програмний сервіс необхідно протестувати за допомогою функціонального тестування вебзастосунку. Необхідно створити тестові випадки та чеклісти, що покривають головний функціонал системи.

2 МОДЕЛІ БЛОКЧЕЙН-ТЕХНОЛОГІЇ

2.1 Блокчейн-технологія

Блокчейн – найновіша технологія, зацікавленість до якої виросла разом із популярністю криптовалют. Сьогодні її широко обговорюють не лише у світі фінансів. Блокчейн вже намагаються використовувати для зберігання та обробки персональних даних та ідентифікації, у маркетингу та комп'ютерних іграх.

У дослівному перекладі блокчейн – це безперервний ланцюжок блоків. У ній містяться всі записи про угоди – хоч із цибулинами тюльпанів у ботанічному саду. На відміну від звичайних баз даних, змінити чи видалити ці записи не можна, можна лише додати нові.

Блокчейн ще називають технологією розподілених реєстрів, тому що весь ланцюжок угод та актуальний список власників зберігають на своїх комп'ютерах безліч незалежних користувачів. Навіть якщо один або кілька комп'ютерів дадуть збій, інформація не буде знищена.

Слід розібрати поняття, які часто використовуються під час обговорення блокчейну.

Актив – щось цінне: наприклад гроші, майно, цінні папери, інформація. Активи можуть існувати у реальному світі, як, наприклад, квартира чи автомобіль, а можуть бути повністю цифровими.

Транзакцією є процес передачі активів від однієї особи до іншої. Передавати можуть не лише сам актив, а й права власності на нього від одного власника іншому. Це також транзакція.

Облік транзакцій – це фіксація всіх переходів активу або права на нього від однієї людини до іншої [37]. І тут постає ключове питання: наскільки механізм підтвердження передачі прав надійний та конфіденційний?

Наприклад, один користувач може вручити іншому документ, який підтверджує, що тепер будь-який його актив передається у власність іншій

людині. Може надіслати цей документ поштою або передати кимось. А головне, він повинен повідомити відповідну установу, що тепер в активу є новий власник. І в базі даних установи має з'явитися відповідний запис.

Уявімо тепер, що велика книга власників активів постраждала від повені. Усі записи зникли. А пошта чи володар втратив документ. Як тепер користувачу довести свої права власності?

На жаль, таке іноді відбувається. Припустимо, було вирішено перевести сотню євро другові, який виявився без грошей за кордоном. Проблеми із системами банку, хакерські атаки, шахрайство чи помилки співробітників можуть спричинити збій на будь-якому з цих етапів. Таке, звичайно, трапляється рідко, але все ж таки буває. І тоді записи про транзакції можуть зникнути або змінитись, а проведення операцій може бути призупинено.

Ці операційні ризики є неминучими, якщо облік ведуть конкретні організації та записи про транзакції зберігаються тільки в одному місці. Технологія блокчейн знижує такі ризики, оскільки пропонує систему обліку з урахуванням розподілених реєстрів.

У блокчейні реєстр власників не зберігається на сервері однієї організації. Його копії одночасно оновлюються на багатьох незалежних комп'ютерах, об'єднаних через інтернет. Це називається розподіленими реєстрами.

У блокчейні реєстри із даними про власників активів неможливо підробити, адже ці дані зберігаються на комп'ютерах багатьох учасників мережі. А щоб інформація у всіх користувачів була абсолютно повною та вірною, у блокчейні ввели поняття «консенсус».

Якщо деякі учасники мережі вимикають свої комп'ютери і частина транзакцій не відобразиться або їх записи виявляться невірними, це не вплине на роботу мережі. Процедура консенсусу, тобто досягнення згоди дозволить відновити правильну інформацію [38].

Що, якщо один із користувачів навмисно чи випадково внесе до своєї книги неправильний запис? Наприклад, що користувач віддав свій актив іншій людині. Все просто: перед тим, як записати наступний рядок, усі користувачі звіряють свої книги. Вірним визнається той варіант, який зафіксовано у більшості.

У реальних блокчейн-мережах за певний період відбувається кілька транзакцій. І записи про транзакції включаються до одного блоку.

Блок – це запис у розподіленому реєстрі про кілька транзакцій. У ньому відбито, хто кому та коли переклав якийсь обсяг активів.

Всі блоки послідовно з'єднують в один послідовний ланцюг.

Ланцюг блокчейна нерозривний, оскільки кожен блок містить посилання на попередній. Блоки не можна змінити або видалити, можна додати нові. Таким чином, завжди можна відновити історію переходів конкретного активу з рук в руки та дізнатися про його нинішнього власника.

У користувачів у блокчейні є суворе правило: вони не можуть нічого виправляти чи видаляти у своїх книгах. Транзакції не можна скасувати. Якщо користувач передав свій актив іншому користувачу, передумати, відіграти все назад і передарувати актив іншій людині він вже не може.

Нові блоки у ланцюг додають майнери.

Майнери виконують у блокчейні кілька функцій:

– зберігають копії блокчейну та тим самим захищають інформацію від втрати або підробки;

– підтверджують транзакції;

– перевіряють транзакції, які зареєстрували інші майнери.

Як правило, кількість майнерів не обмежена. Чим їх більше, тим така мережа надійніша. Майнерами можуть стати усі охочі. Для цього їм потрібні спеціалізовані комп'ютери та програмне забезпечення.

За підтримку роботи мережі майнери одержують нагороду.

Нагорода – як правило, це комісії від усіх учасників транзакцій, записаних у блоці, та винагорода від самої мережі. Мережа генерує цю винагороду за певним алгоритмом.

Навіщо майнерам стежити за порядком у своєму блокчейні? Відповідь проста: майнер, який реєструє транзакцію, отримує за це нагороду.

Саме так відбувається зазвичай із криптовалютами: нагорода – це певна кількість самих криптомонет. Вони виникають буквально з повітря та потрапляють на рахунок майнера. Так відбувається випуск нових одиниць віртуальних грошей і загальна кількість віртуальної валюти збільшується. Але при цьому найчастіше є обмеження: коли сума монет сягає певного максимуму, їх випуск припиняється. Далі майнери можуть працювати лише за винагороду від учасників.

Це приклад ланцюжка блокчейну: кожен блок містить час і результати всіх попередніх транзакцій. Алгоритм налаштований так, що кожні 10 хвилин якийсь майнер додає до ланцюга новий блок та видобуває 5 нових одиниць криптовалюти.

Але хто саме з багатьох майнерів завоює право додати блок і отримати за нього винагороду? Для цього більшість блокчейн-мереж генерують спеціальні завдання.

Припустимо, користувач оголошує конкурс серед майнерів. Він вигадує їм математичне завдання – і хто перший знайде рішення, той і додасть наступний запис у блокнот. Щасливчику, що зробить це найшвидше, користувач обіцяє подарувати одну одиницю певної монети. І ще одну йому подарує блокчейн – як плату за працю.

Імовірність удачі для майнера – що саме він вирішить запропоновану мережею математичне завдання першим, приєднає блок та отримає за цю винагороду – найчастіше залежить від потужності обладнання. Чим продуктивнішими є його комп’ютери, тим більше шансів заробити.

Куди і як саме майнери та учасники транзакцій одержують переклади? Для цього вони використовують анонімні цифрові гаманці.

Гаманець – це спеціальний ідентифікатор. У ньому зберігається запис про стан рахунку учасника (і це не обов’язково гроші, а будь-які активи). Гаманець дозволяє дізнатися всю історію транзакцій конкретного учасника.

Найчастіше такі гаманці анонімні – вони не дозволяють дізнатися, хто саме приймає чи відправляє з нього активи.

У більшості блокчейнів і майнери, і власники активів невідомі. Тобто ніхто не знає, що який гаманець кому належить.

У цьому є й небезпека. Якщо власник гаманця, наприклад, забуде його номер, ніяк не зможе довести, що рахунок належить саме йому. Все, що зберігалося в гаманці, виявиться втраченим назавжди.

Дані електронних гаманців та транзакції у блокчейні захищені шифруванням.

Як гарантувати, що інформація про транзакції та стан гаманця буде вірною, повною та конфіденційною? Як отримати доступ до своїх активів в умовах анонімності? Такі завдання вирішує криптографія та шифрування – як один із її методів.

У блокчейн-мережах покупець та продавець активу підтверджують транзакцію за допомогою криптографічних ключів – спеціальних унікальних цифрових кодів.

Вгадати послідовність символів цифрового коду криптографічних ключів практично неможливо. Це робить технологію блокчейн однією з найкращих для фінансових транзакцій. Але в той же час вже були випадки злому гаманців, тому їх краще підключати до мережі лише на час проведення транзакцій, а решту часу зберігати офлайн.

Таким чином, підсумовуючи все викладене вище, на рисунку 2.1 приведено схему роботи блокчейну на прикладі криптовалют.

Рисунок 2.1 – Схема роботи блокчейну на прикладі криптовалют

Особливості технології розподілених реєстрів:

– актив може бути будь-яким: наприклад, акції, цифрові токени, права на нерухомість, золото чи книги;

– транзакції відбуваються практично миттєво, але на їхнє підтвердження може знадобитися час, який саме – визначає алгоритм консенсусу конкретної блокчейн-мережі;

– угоди конфіденційні та анонімні: покупець вказує лише номер свого криптогаманця;

– комісії є мінімальними, оскільки замість централізованих посередників транзакції реєструють майнери. Комісії – це їхня винагорода за підтримку роботи блокчейн-мережі. Але майнерів зазвичай дуже багато і

конкуренція між ними висока – це дозволяє утримувати комісії на низькому рівні;

– права покупців надійно захищені: скасувати чи змінити вже укладені угоди неможливо. Якщо людина справді придбала щось – наприклад, певні монети чи квартиру, – ніякий шахрай не зможе довести, що вони належать йому. Усі угоди зафіксовані в ланцюжку блоків.

Інформація надійно зберігається, оскільки історія всіх операцій записана в блокчейні та розподілена по всіх учасників мережі. Кожен блок містить інформацію про всі попередні операції «з початку часів».

2. 2 Принцип токенізації

Токенізація замінює конфіденційний елемент даних, наприклад, номер банківського рахунку, неконфіденційною заміною, відомою як маркер. Маркер – це рандомізований рядок даних, який не має суттєвої чи корисної цінності чи значення. Це унікальний ідентифікатор, який зберігає всю відповідну інформацію про дані без шкоди для їх безпеки.

Система токенізації пов’язує вихідні дані з маркером, але не надає жодного способу розшифрувати маркер і відкрити вихідні дані. Це на відміну від систем шифрування, які дозволяють розшифровувати дані за допомогою секретного ключа.

Токенізація, що стосується обробки платежів, вимагає заміни номера кредитної картки або рахунку на токен. Маркер не має користі та не пов’язаний з обліковим записом чи особою.

16-значний номер основного рахунку (PAN) клієнта замінюється довільно створеним індивідуальним буквено-цифровим ідентифікатором. Процес токенізації усуває будь-який зв’язок між транзакцією та конфіденційними даними, що обмежує ризик порушень, що робить його корисним для обробки кредитних карток.

Токенізація даних захищає номери кредитних карток і номери банківських рахунків у віртуальному сховищі, тому організації можуть безпечно передавати дані через бездротові мережі. Щоб токенізація була ефективною, організації повинні використовувати платіжний шлюз для безпечного зберігання конфіденційних даних.

Платіжний шлюз – це торгова послуга, яку пропонує постачальник послуг електронної комерції, яка дозволяє здійснювати прямі платежі або обробку кредитних карток. Цей шлюз безпечно зберігає номери кредитних карток і генерує випадковий маркер.

Коли продавець обробляє кредитну картку клієнта, PAN замінюється маркером. 1234-4321-8765-5678 замінюється, наприклад, на 6f7%gf38hfUa.

Продавець може застосувати ідентифікатор маркера для збереження записів про клієнта, наприклад, 6f7%gf38hfUa підключено до John Smith. Потім токен передається платіжному процесору, який детокенізує ідентифікатор і підтверджує платіж. 6f7%gf38hfUa стає 1234-4321-8765-5678.

Платіжний процесор є єдиною стороною, яка може читати маркер; це не має сенсу ні для кого іншого. Крім того, токен корисний лише для цього одного торговця.

Основна відмінність між токенізацією та шифруванням полягає в тому, що токенізація використовує «токен», тоді як шифрування використовує «секретний ключ» для захисту даних.

Основна проблема шифрування даних полягає в тому, що воно оборотне. Зашифровані дані призначені для відновлення до початкового, незашифрованого стану. Безпека шифрування залежить від алгоритму, який використовується для захисту даних. Складніший алгоритм означає безпечніше шифрування, яке складніше розшифрувати.

Проте все шифрування по суті може бути зламано. Потужність вашого алгоритму та обчислювальна потужність, доступна зловмиснику, визначатимуть, наскільки легко зловмисник зможе розшифрувати дані.

Таким чином, шифрування краще описати як обфускацію даних, а не як захист даних. Шифрування ускладнює доступ до вихідної інформації, захищеної в зашифрованих даних, але це не неможливо.

Рада зі стандартів безпеки PCI та подібні організації, що відповідають вимогам, розглядають зашифровані дані як конфіденційні, оскільки вони є зворотними. Тому організації повинні захищати зашифровані дані.

На відміну від шифрування, токенізацію даних неможливо скасувати. Замість того, щоб використовувати алгоритм, який можна зламати, система токенізації замінює конфіденційні дані шляхом відображення випадкових даних, тому маркер не можна розшифрувати. Маркер є заповнювачем, не має істотного значення.

Справжні дані зберігаються в окремому місці, наприклад на захищеній зовнішній платформі. Вихідні дані не потрапляють у ваше IT-середовище. Якщо зловмисник проникає у ваше середовище та отримує доступ до ваших токенів, він нічого не отримує. Таким чином, токени не можна використовувати для злочинних дій.

PCI та інші стандарти безпеки не вимагають від організацій захисту токенізованих даних.

Токенізація може надати кілька важливих переваг для захисту конфіденційних даних клієнтів:

– покращена гарантія клієнтів: токенізація пропонує додатковий рівень безпеки для вебсайтів електронної комерції, підвищуючи довіру споживачів;

– підвищена безпека та захист від злому: за допомогою токенізації підприємствам не потрібно отримувати конфіденційну інформацію на своїх вхідних терміналах, зберігати її у внутрішніх базах даних або передавати дані через свої інформаційні системи. Це захищає бізнес від порушень безпеки;

– токенізація даних покращує безпеку пацієнтів: організації можуть використовувати рішення для токенізації для сценаріїв, які охоплюються HIPAA (Health Insurance Portability and Accountability Act). Замінивши захищену в електронному вигляді інформацію про здоров’я (ePHI) і закриту

персональну інформацію (NPPI) на токенізоване значення, організації охорони здоров'я зможуть краще дотримуватися норм HIPAA;

– токенізація робить банківські платежі кредитними картками більш безпечними – індустрія платіжних карток повинна відповідати широким стандартам і правилам. Рішення для токенізації забезпечують спосіб захисту даних власників карток, таких як дані магнітного свайпу, номер основного рахунку та інформація про власника картки. Компанії можуть легше відповідати галузевим стандартам і краще захищати інформацію клієнтів.

На рисунку 2.2 приведено схему роботи токенізації.

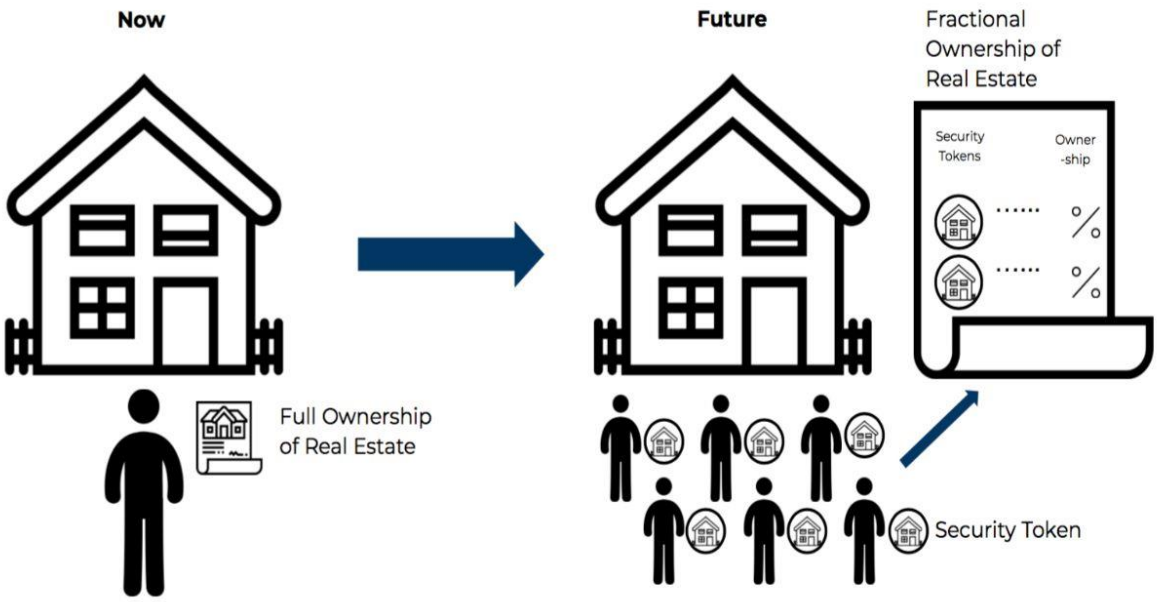

Рисунок 2.2 – Схема роботи токенізації

В результаті використання блокчейн для токенізації будь-яку спробу несанкціонованого втручання в реєстр токенів на активи буде видно та припинено.

Більш того, завдяки блокчейну відпадає потреба в посередниках при купівлі/продажу токена на актив. Токен можна також швидко та легко купити/продати, як біткойн або іншу криптовалюту. Це порівняння приведене через те, що саме криптовалюти функціонують на технології блокчейну і їх з кожним днем можна буде купити все простіше.

2.3 Модель сервісу токенізації монет

Під час проєктування сервісу було розроблено діаграму прецедентів, яка відображає увесь скоуп дій, доступних користувачеві (рис. 2.3).

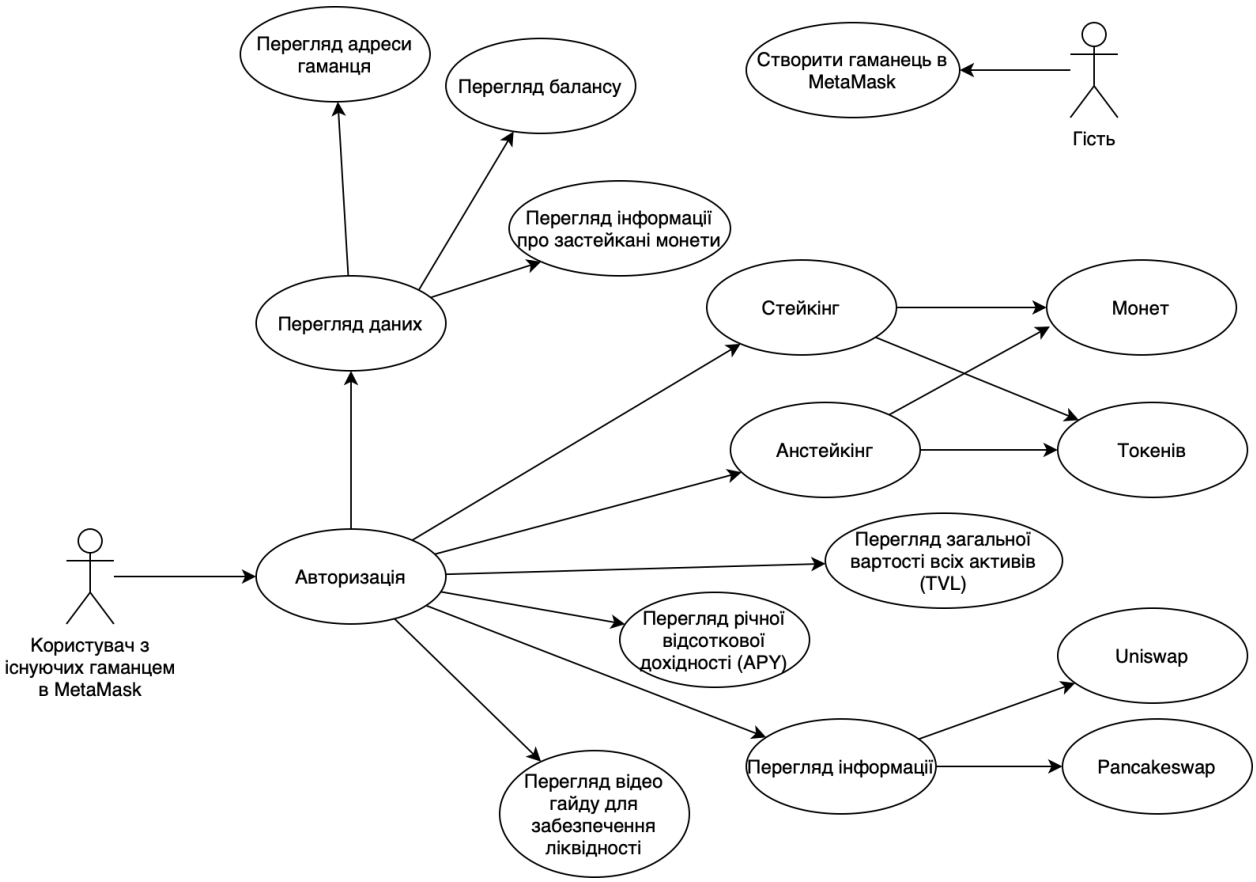

Рисунок 2.3 – Діаграма прецедентів

Так з приведеної вище діаграми зрозуміло, що користувач може авторизуватися шляхом підключення гаманця MetaMask, після чого йому доступний увесь функціонал сервісу:

– перегляд адреси підключеного гаманця;
– перегляд балансу гаманця користувача;
– перегляд інформації про застейкані монети;
– стейкінг:
    1) монет;
    2) токенів;

– анстейкінг:

1) монет;
2) токенів;

– перегляд загальної вартості всіх активів (TVL);

– перегляд річної відсоткової дохідності (APY);

– перегляд інформації, яка може виконуватися за допомогою переходу на сервіс:

1) Uniswap;
2) PancakeSwap;

– перегляд відео гайду для забезпечення ліквідності.

Гість не може відвідувати приведений вище сервіс, так як для його використання необхідно мати наявний гаманець в MetaMask. Проте після створення відповідного гаманця та авторизації за допомогою його гість стає повноцінним користувачем системи.

Система повинна містити зручні та інформаційні повідомлення про помилки, за допомогою яких користувач зможе розуміти, що пішло не так. Також сервіс повинен містити інформаційні повідомлення для випадків обробки даних, за допомогою яких користувач зрозуміє, на якому саме етапі обробки даних знаходиться система в даний момент.

Також в подальших версіях програмного забезпечення планується розширення функціональності, що доступна користувачам сервісу.

3 ПРОГРАМНА РЕАЛІЗАЦІЯ СЕРВІСУ ТОКЕНІЗАЦІЇ МОНЕТ

3.1 Вибір середовища

У рамках кваліфікаційної роботи було досліджено та використано блокчейн-технології, а також залучено наступний стек технологій:

– Vue 2;
– Metamask;
– Smart contracts;
– Ethereum;
– BNB.

Приведені вище технології було відібрано як найбільш підходящі для розробки, зосередженої довкола технології блокчейн та процесу токенізації.

Vue – це фреймворк JavaScript для створення інтерфейсів користувача. Він створений на основі стандартних HTML, CSS і JavaScript і забезпечує декларативну та компонентну модель програмування, яка допомагає ефективно розробляти інтерфейси користувача, прості чи складні.

MetaMask – це програмний криптовалютний гаманець, який використовується для взаємодії з блокчейном Ethereum. Це дозволяє користувачам отримувати доступ до свого гаманця Ethereum через розширення браузера або мобільний застосунок, який потім можна використовувати для взаємодії з децентралізованими програмами. MetaMask розроблено ConsenSys Software Inc., компанією, що розробляє блокчейн-програмне забезпечення, що зосереджується на інструментах та інфраструктурі на основі Ethereum.

Ethereum – це технологія, яка є «домом» для цифрових грошей, глобальних платежів і програм. Спільнота створила бурхливу цифрову економіку, нові сміливі способи заробітку в Інтернеті для творців і багато

іншого. Він відкритий для всіх, де б людина не була – все, що потрібно, це Інтернет.

Ethereum – це технологія для створення застосунків і організацій, зберігання активів, транзакцій і спілкування без контролю з боку центральної влади. Щоб використовувати Ethereum, не потрібно передавати всі особисті дані – людина контролює власні дані та те, що надається. Ethereum має власну криптовалюту Ether, яка використовується для оплати певної діяльності в мережі Ethereum.

Останнім, але не найменш важливим, варто переглянути BNB (Binance Coin), щоб кінцево зрозуміти увесь стек технологій, які використовувались для розробки застосунку.

Індустрія криптовалют та блокчейнів включає численні проєкти та активи, спрямовані на різні цілі. Нерідко можна побачити проєкти, спрямовані на вирішення подібних потреб.

Наприклад, існує кілька криптобірж. Хоча кожна біржа може відрізнятися за конструкцією та функціями, вони прагнуть надати криптотрейдерам місце для обміну своїми активами в ширшому сенсі. Іноді біржа криптовалют може мати власний актив, який використовується для певних цілей на пов’язаній біржі, наприклад знижки на комісію на торговій платформі.

Binance Coin (BNB) біржі Binance є одним із таких активів криптобіржі. Монета Binance (BNB) починалась як актив, проданий під час первинної пропозиції монет (ICO) Binance, та стала засобом, за допомогою якого користувачі біржі Binance могли платити менше торгових комісій на платформі після запуску біржі.

Відтоді BNB зберіг свою роль у зростаючій екосистемі Binance, оскільки Binance перетворився на більше, ніж біржу цифрових активів.

3.2 Інструкція користувача

Головна сторінка системи виглядає наступним чином (рис. 3.1).

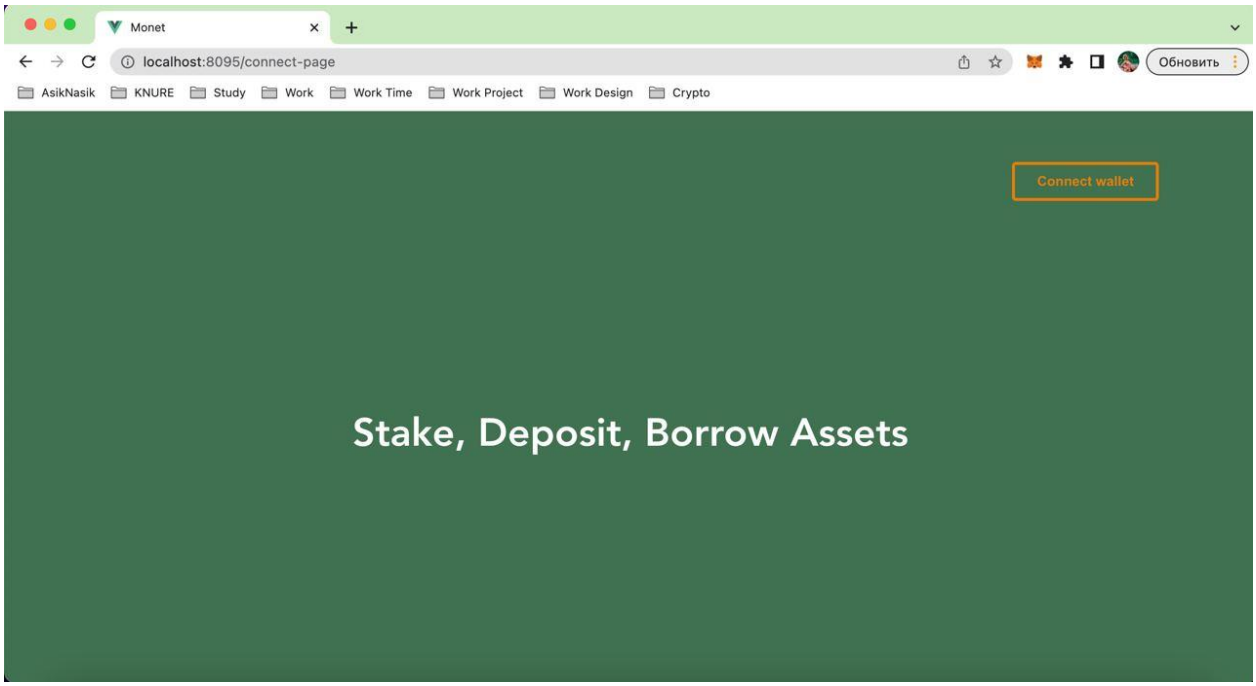

Рисунок 3.1 – Головна сторінка сервісу

На даній сторінці користувач може лише підключити свій гаманець для того, щоб перейти до користування сервісом.

В той самий час в сервісі також наявна обробка обмежень, таких як запобігання помилок, які не нестимуть користувачу інформації або які зможуть призвести до некоректного відпрацювання системи. Таким чином, наприклад, реалізується і обробка помилки, коли користувач не має розширення MetaMask, або воно відключено – тоді користувач побачить інформативне повідомлення, яке допоможе йому зрозуміти, в чому виникла помилка, що можна побачити на рисунку 3.2.

Так користувач може побачити повідомлення «Connection error, install Metamask or check the network», яке надає вичерпну інформацію щодо того, як саме виправити помилку. Також повідомлення виділено червоним

кольором, що допоможе користувачу одразу виділити його серед інтерфейсу.

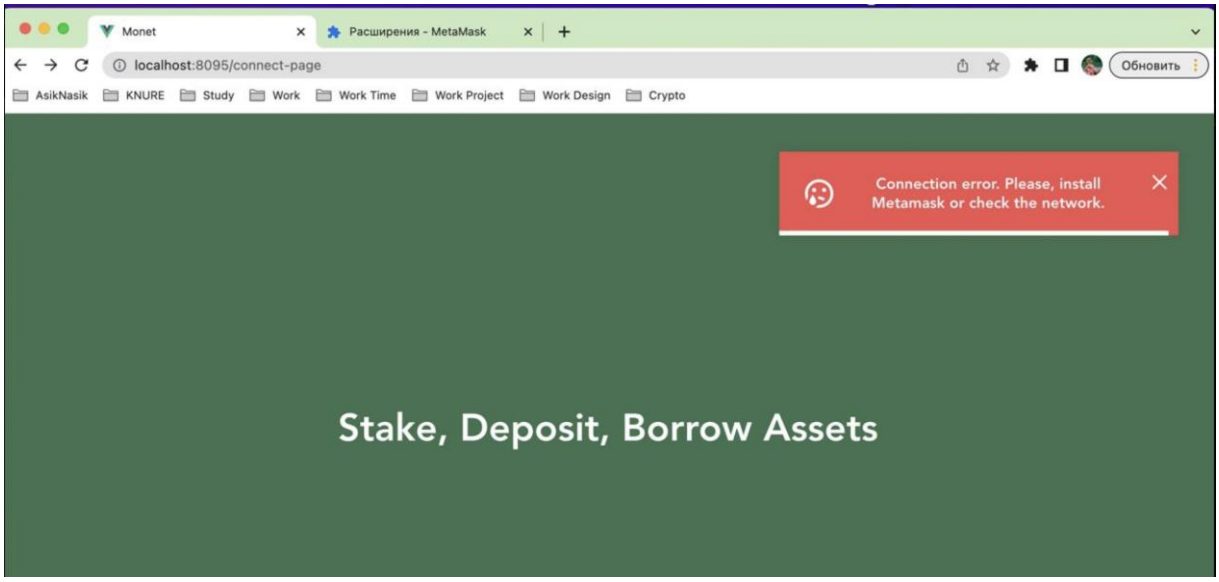

Рисунок 3.2 – Повідомлення користувача про помилку під час під’єднання гаманця

У випадку, якщо користувач бачить наведену вище помилку, йому слід перейти до налаштувань та переглянути, чи увімкнено в нього відповідне розширення (рис. 3.3).

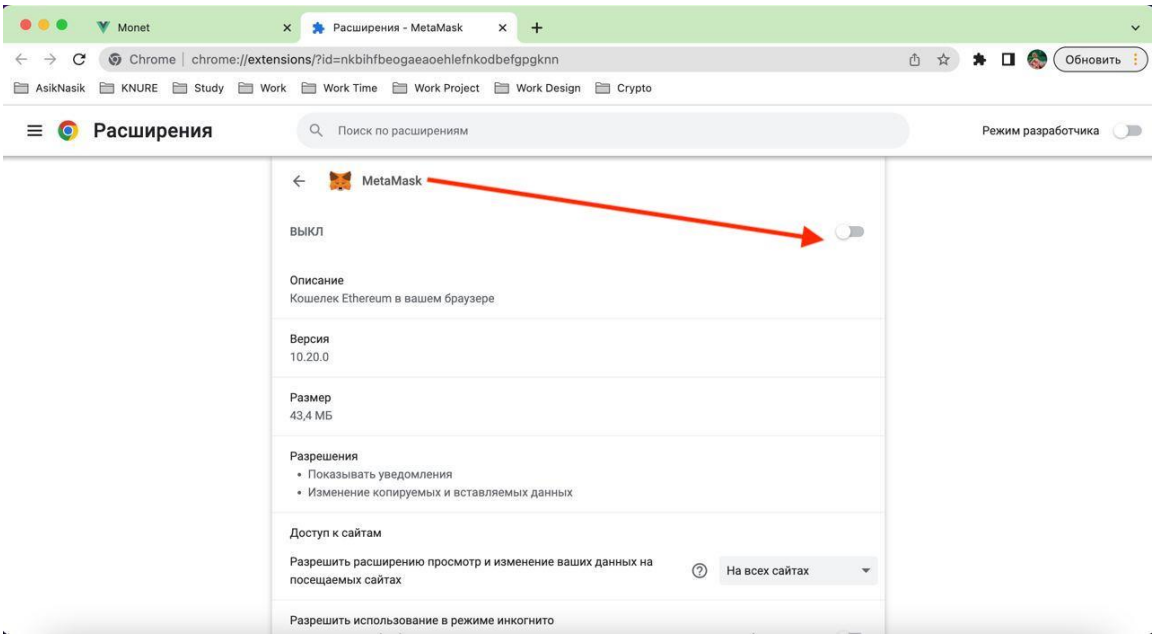

Рисунок 3.3 – Сторінка налаштувань браузеру з розширенням MetaMask

На рисунку 3.4 приведено приклад відображення сторінки налаштувань з увімкненим розширенням MetaMask.

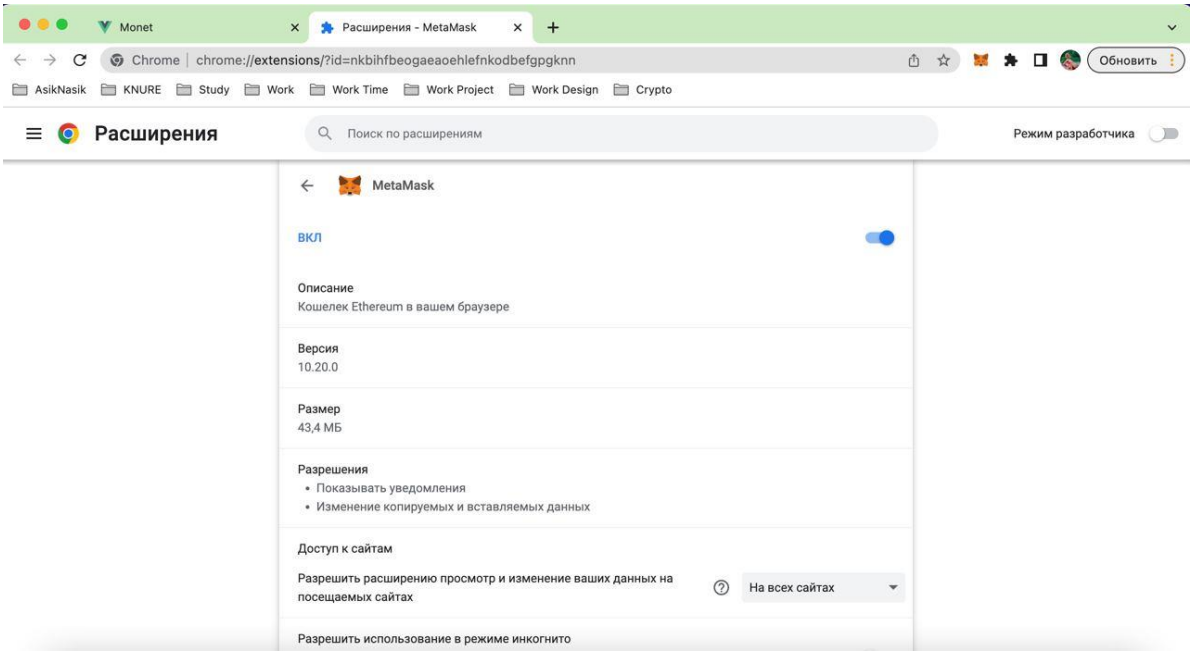

Рисунок 3.4 – Сторінка налаштувань браузеру з увімкненим розширенням MetaMask

Після цього користувач може повертатись на початкову сторінку.

На цьому етапі усі подальші дії виконає розширення MetaMask – у додатковому вікні, яке буде відкрито за допомогою розширення, слід налаштувати власний гаманець.

Коли користувач вже матиме гаманець, він зможе лише увести відповідний пароль та продовжити використання сервісу, що і можна переглянути на рисунку 3.5, де розширення MetaMask відкриває відповідне додаткове вікно.

В той самий момент програмний вебсервіс також відкриває відповідне модульне вікно з текстом «Awaiting for you to connect your wallet», що інформує користувача про те, що очікується відповідь від розширення. Так користувач завжди розумітиме, на якому саме етапі обробки запиту знаходиться розроблюваний сервіс.

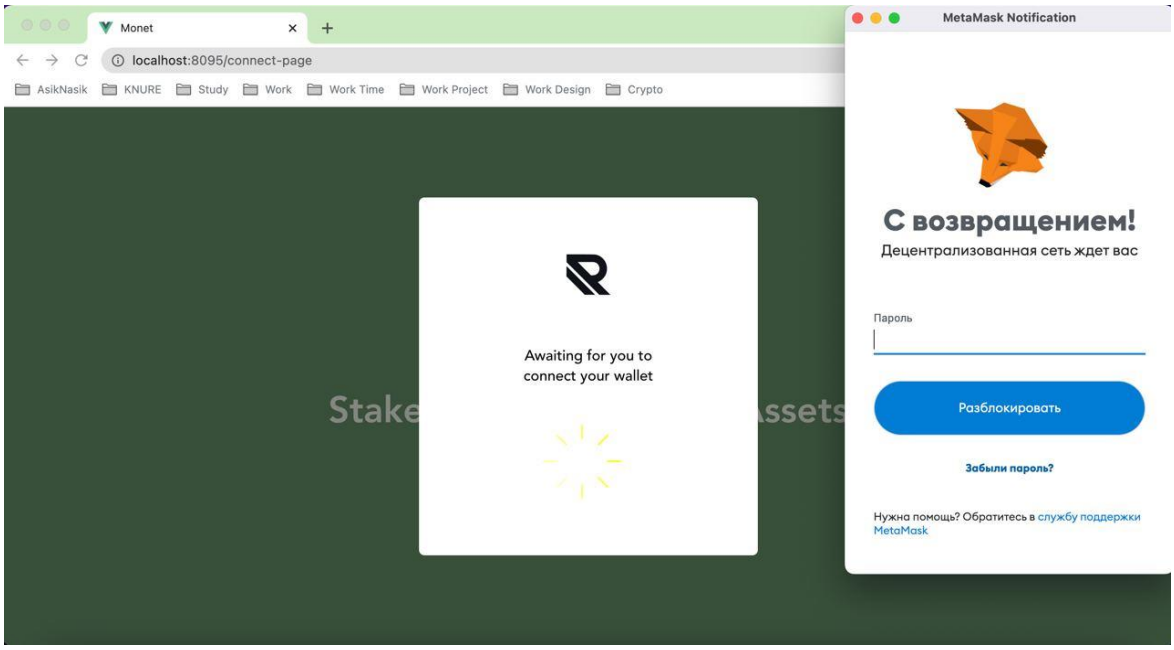

Рисунок 3.5 – Розширення MetaMask очікує на введення паролю від гаманцю

Практика створення інформуючих повідомлень вважається гарною, бо тоді користувач завжди матиме розуміння, що саме відбувається з системою.

Після авторизації користувач може переглянути головний екран сервісу, де зібрано усю необхідну інформацію, яку слід знати (рис. 3.6) за нашою монетою.

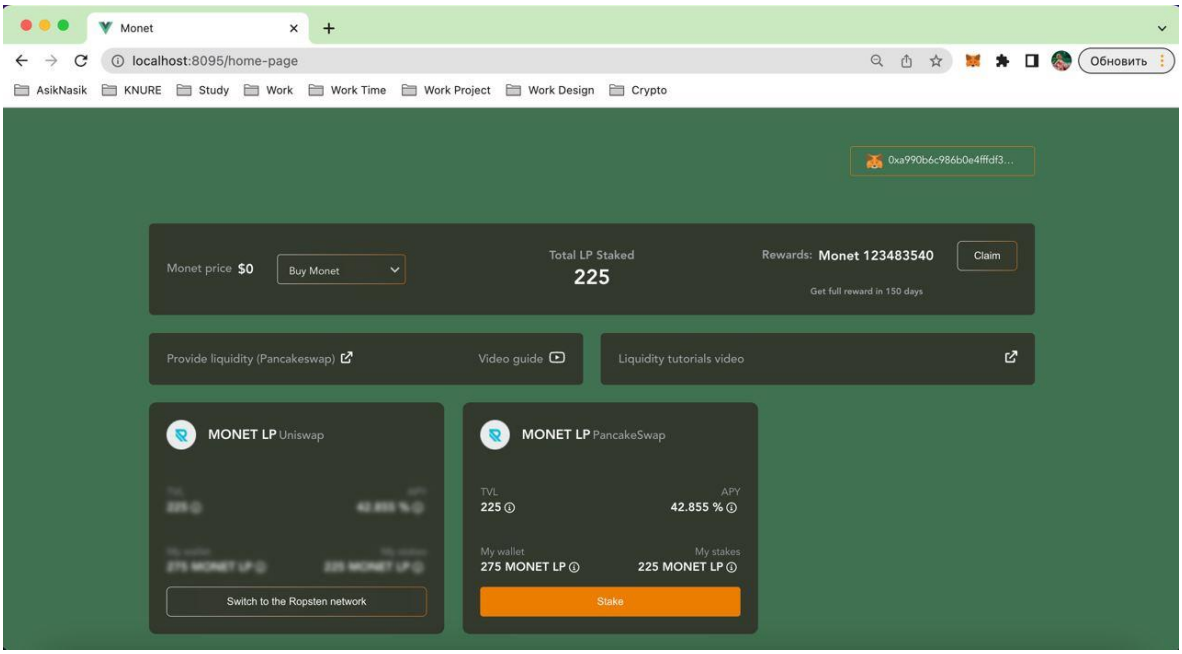

Рисунок 3.6 – Головний екран сервісу зі всією інформацією про монету

Так, наприклад, на рисунку 3.7 відкрито дропдаун (випадаючий список) з посиланнями на сторінки пулів, з якими виконано інтеграцію.

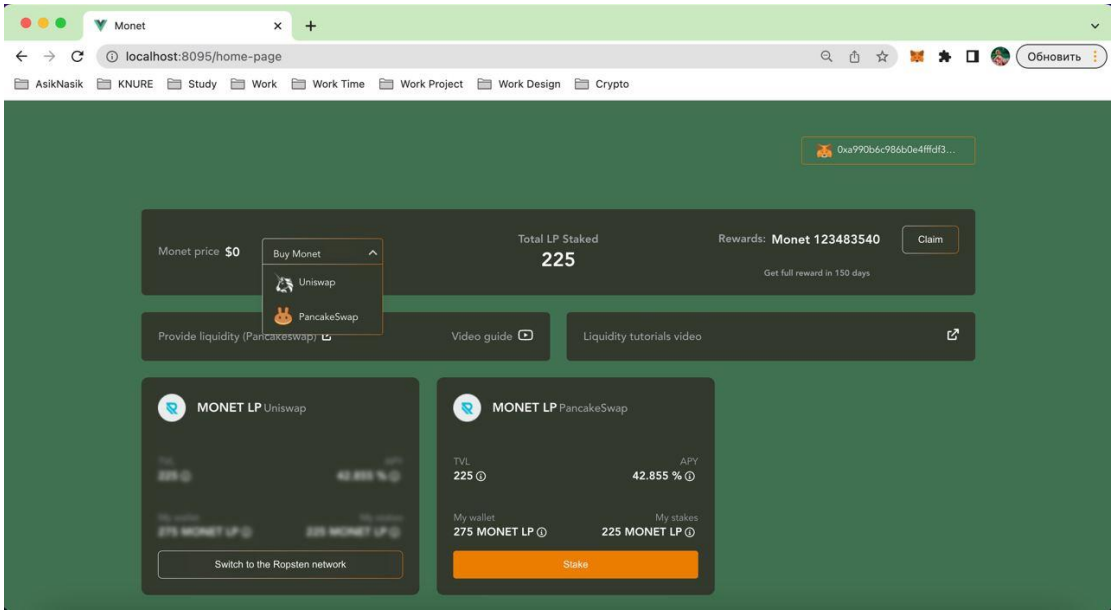

Рисунок 3.7 – Перегляд пулів, з якими виконано інтеграцію

Натискаючи на посилання Uniswap, користувач буде переправлений на відповідну сторінку (рис. 3.8).

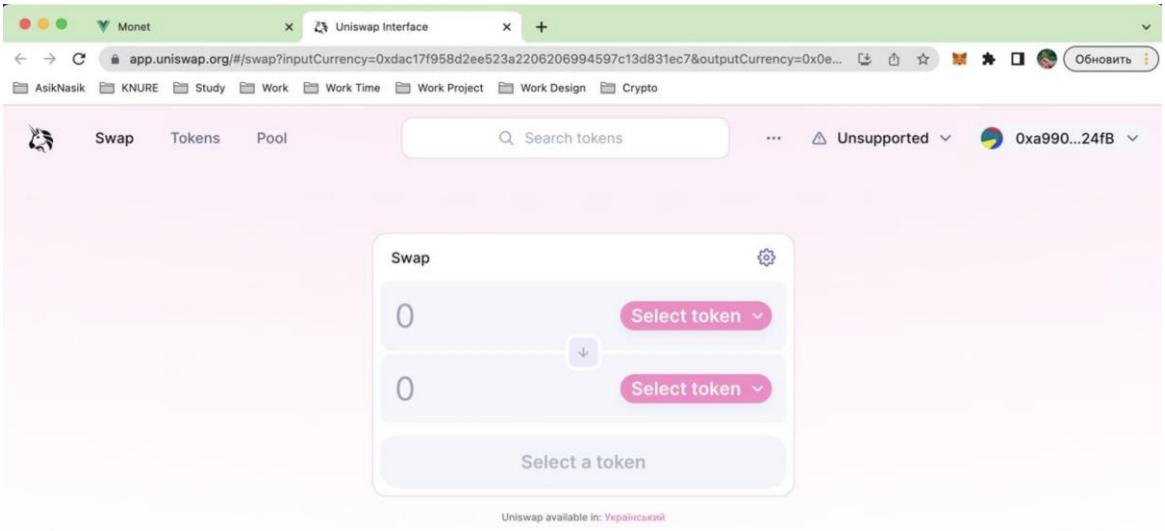

Рисунок 3.8 – Редірект на сторінку сервісу Uniswap

Так само при натисканні на посилання PancakeSwap користувача буде переправлено тепер вже на головну сторінку даного сервісу (рис. 3.9).

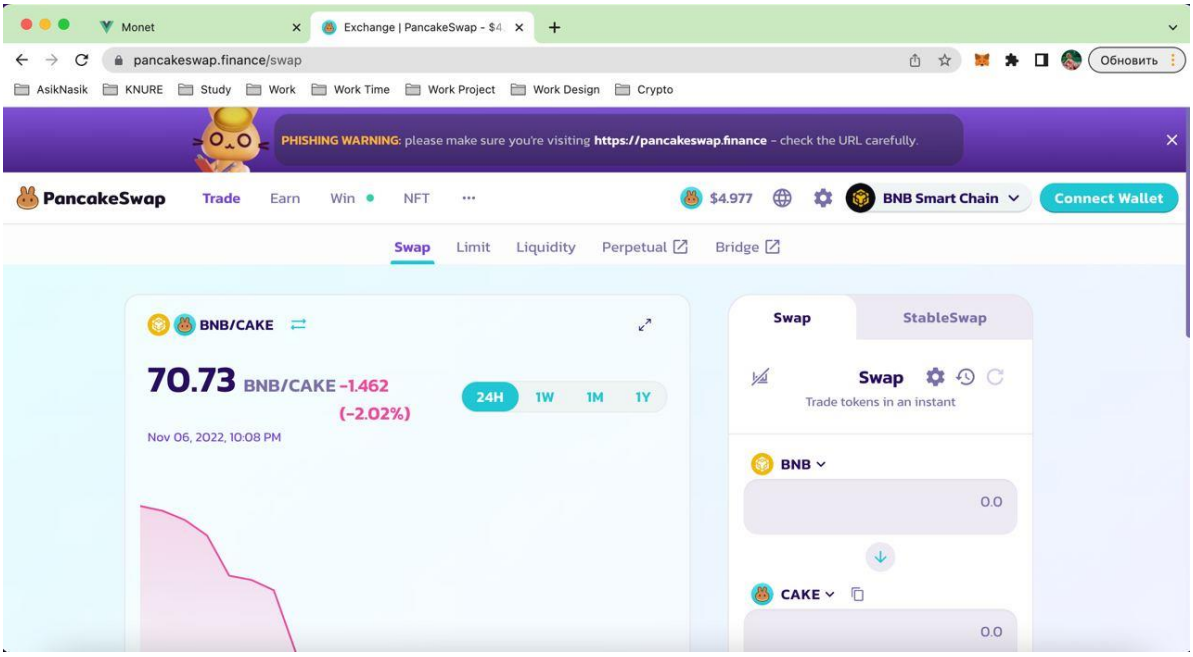

Рисунок 3.9 – Редірект на сторінку сервісу PancakeSwap

Якщо, знаходячись на головній сторінці сервісу (для зареєстрованого користувача), натиснути на кнопку Provide liquidity (Pancakeswap), користувач буде перенаправлений на відповідну сторінку сервісу Pancakeswap, що можна побачити на рисунку 3.10.

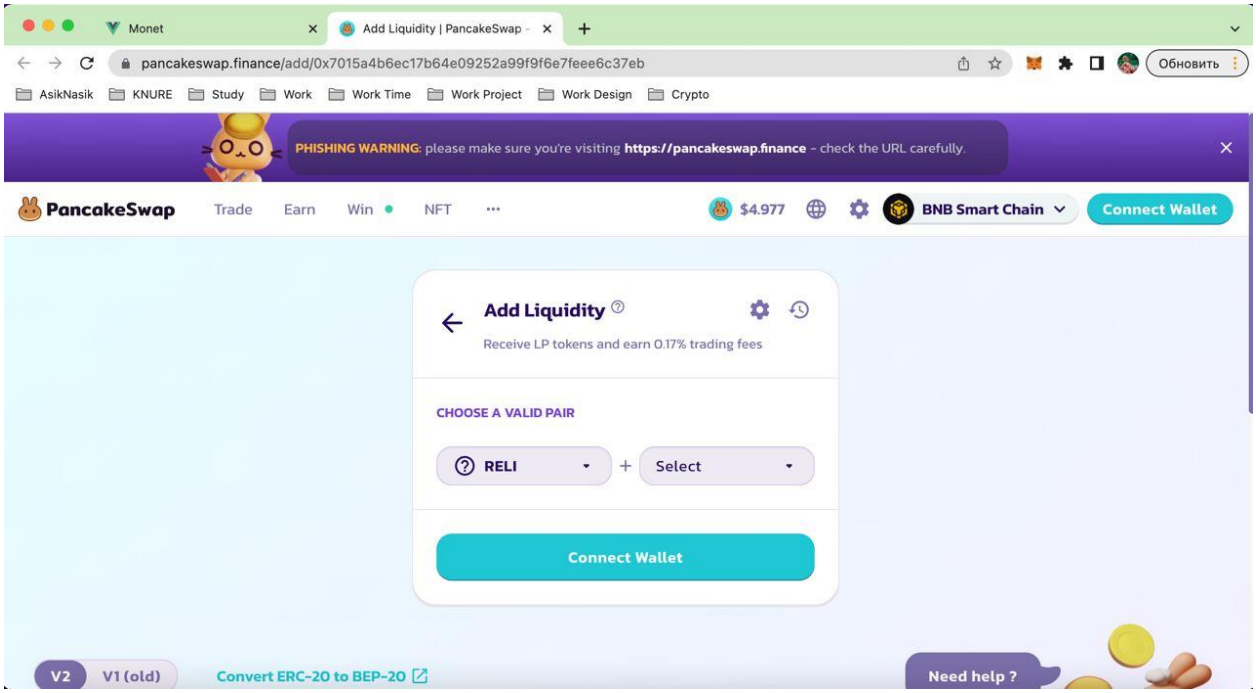

Рисунок 3.10 – Редірект на сторінку сервісу Pancakeswap при натисканні кнопки Provide liquidity (Pancakeswap)

Відповідно на даній сторінці користувач може провести забезпечення ліквідності за допомогою сервісу Pancakeswap.

За необхідності користувач також може перейти за посиланням на відповідне відео, яке надасть йому можливість переглянути інструкцію та розібратися як правильно зробити необхідні дії (рис. 3.11). Для цього слід натиснути на головній сторінці кнопку «Video guide».

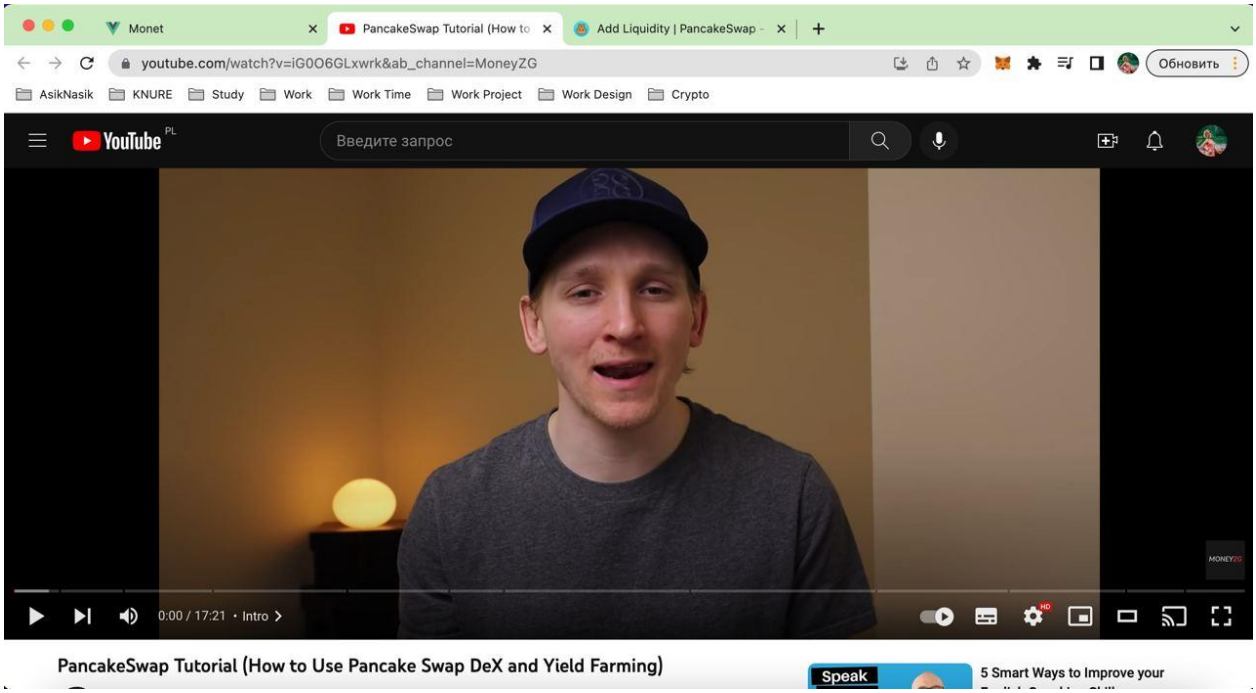

Рисунок 3.11 – Відео, яке відкривається по натисканню на кнопку «Video guide»

Також головна сторінка має кнопку «Liquidity tutorials video», по натисканню на яку користувач може перейти на сторінку зі статтею, яка також містить усі необхідні дані (рис. 3.12).

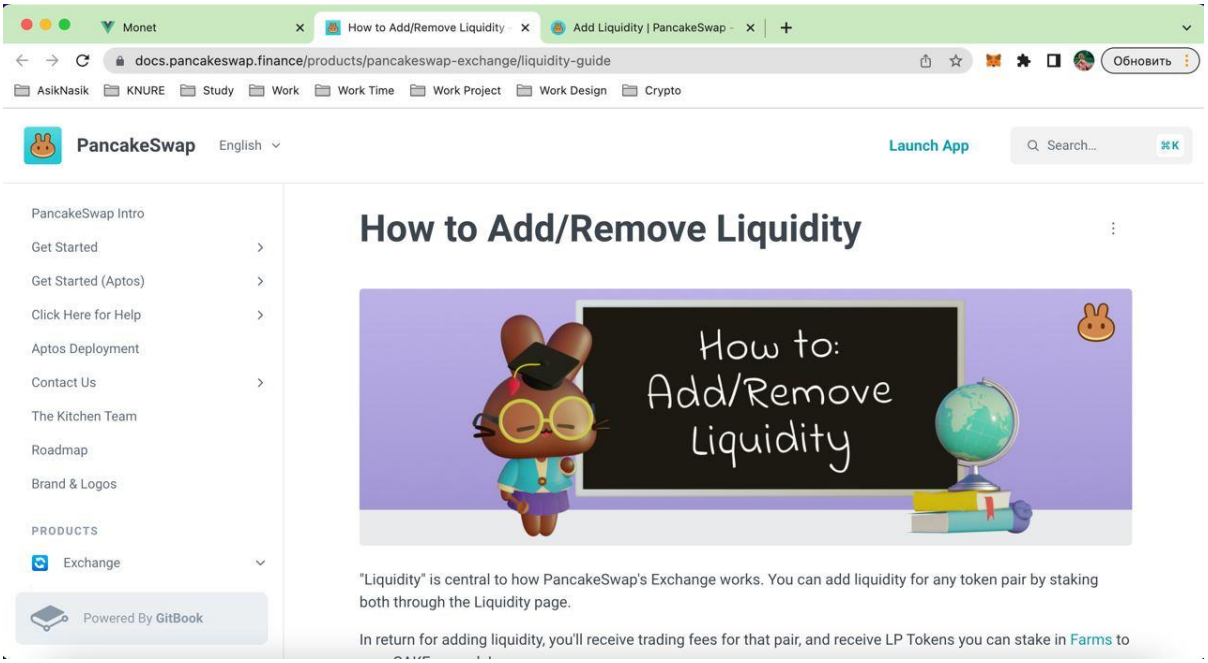

Рисунок 3.12 – Стаття, яка відкривається по натисканню кнопки «Liquidity tutorials video»

При натисканні кнопки «Stake» на головній сторінці відкривається вікно, де користувач може застейкати монети (рис. 3.13).

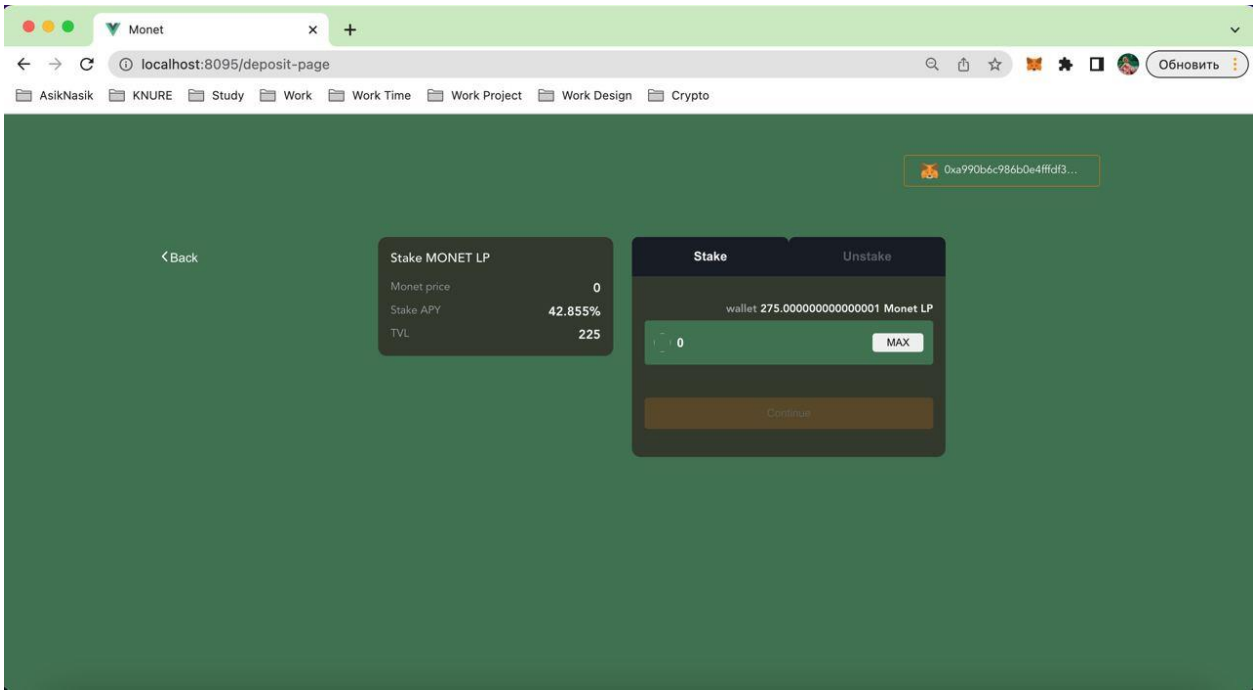

Рисунок 3.13 – Сторінка для стейкінгу монет

Криптостейкінг – це процес блокування криптохолдингів з метою отримання винагород або відсотків. Криптовалюти побудовані за допомогою технології блокчейн, у якій крипто-транзакції перевіряються, а отримані дані зберігаються в блокчейні. Стекінг – це ще один спосіб описати перевірку цих транзакцій у блокчейні.

Залежно від типу криптовалюти, з якою людина працює, і її підтримуваних технологій, ці процеси перевірки називаються «доказом частки» або «доказом роботи». Кожен із цих процесів допомагає криптомережам досягти консенсусу або підтвердження того, що всі дані транзакцій доповнюються тим, що їм потрібно.

Але для досягнення цього консенсусу потрібні учасники. Ось що таке стейкинг – інвестори, які активно тримають або зберігають свої криптовалютні активи у своєму криптовалютному гаманці, беруть участь у процесах досягнення консенсусу цих мереж. Стейкери, по суті, схвалюють і перевіряють транзакції в блокчейні.

За це мережі винагороджують цих інвесторів. Конкретні нагороди залежатимуть від мережі.

Можна розглядати криптостейкінг як подібний до внесення готівки на ощадний рахунок. Вкладник отримує відсотки за свої гроші, поки вони знаходяться в банку, як винагороду від банку, який використовує гроші для інших цілей (кредитування тощо). Стейкінг монет схожий за своєю суттю на отримання відсотків.

Для проведення стейкінгу необхідно виконати підтверження операції, для чого користувачу знову необхідно розширення MetaMask, яке відкриває в модульному вікні усю інформацію про відповідну дію (рис. 3.14).

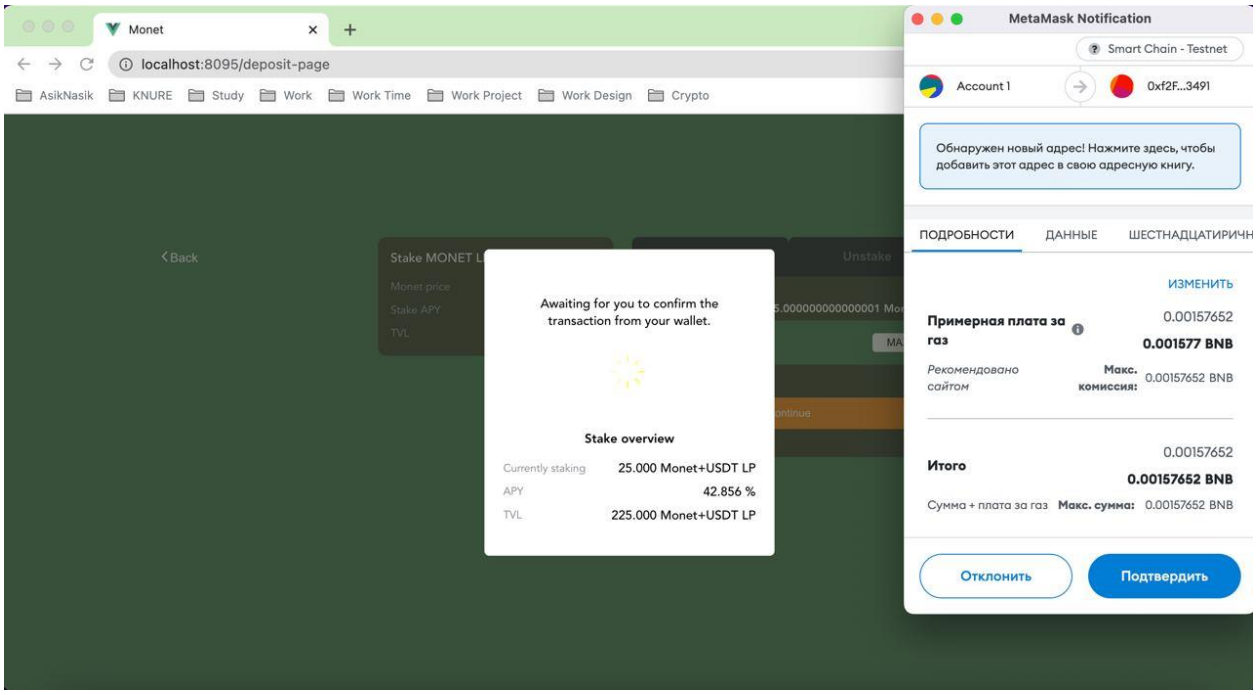

Рисунок 3.14 – Розширення MetaMask очікує на підтвердження операції

Підтвердження успішності проведеної операції також можна переглянути за допомогою розширення MetaMask, що приведено на рисунку 3.15.

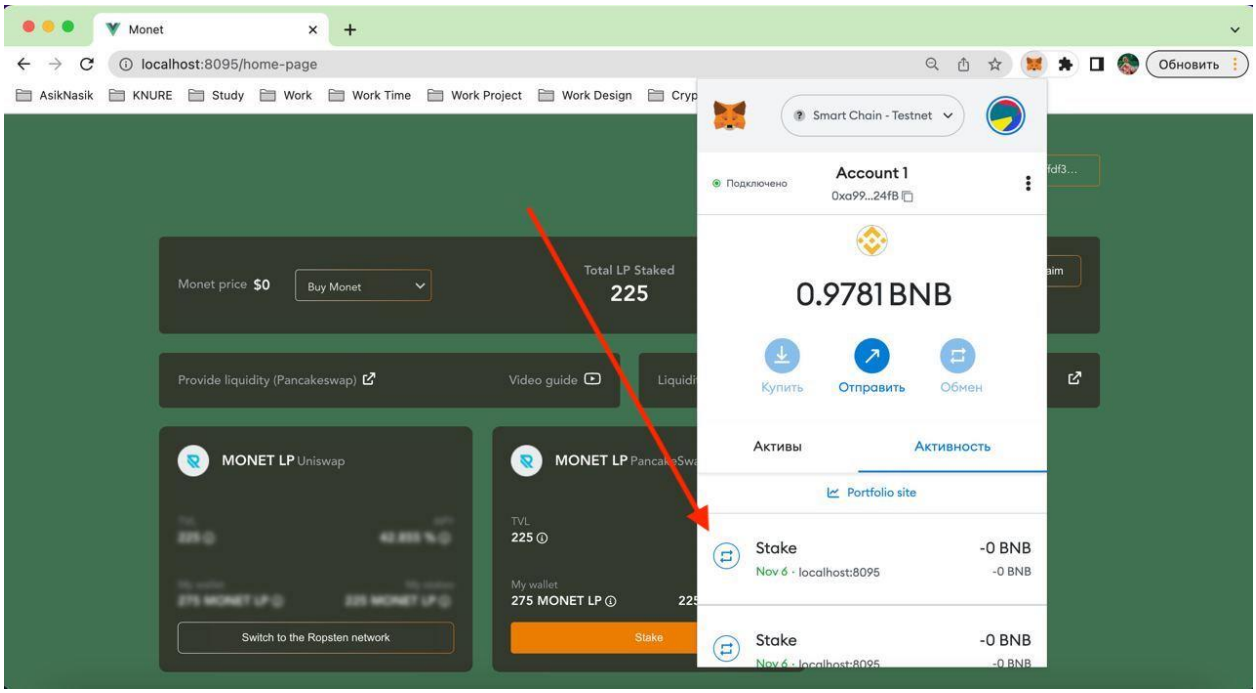

Рисунок 3.15 – Підтвердження проведеної операції в розширенні MetaMask

Після виконання операції слід оновити головну сторінку, щоб сервіс завантажив оновлені дані з серверу (рис. 3.16).

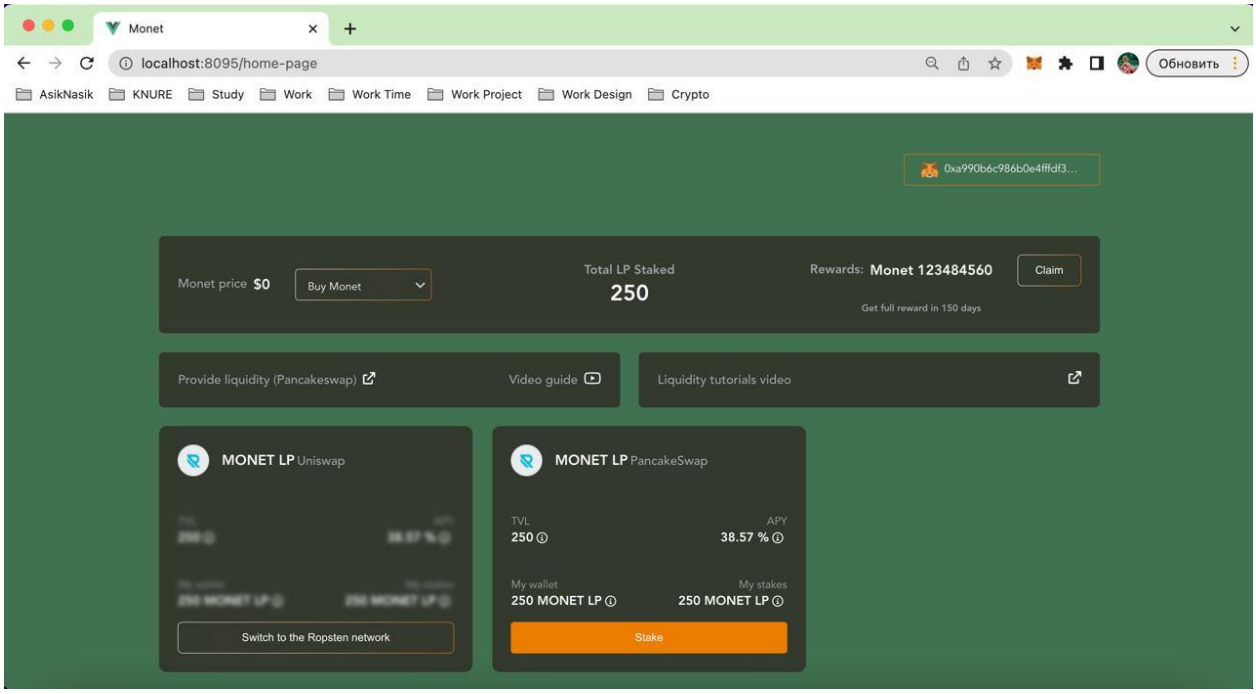

Рисунок 3.16 – Оновлена сторінка після проведення операції

На оновленій сторінці можна побачити, що дані картки Pancakeswap були змінені, баланс також змінюється відповідно проведених операцій, та число застейканих монет тепер також змінене.

Після стейкінгу монет ваші монети все ще у вашому розпорядженні. Користувач, по суті, запускає ці застейкані («поставлені») монети в роботу, і він можете позбутися їх, якщо захоче ними торгувати. Процес звільнення може бути не миттєвим; з деякими криптовалютами слід робити ставки монет протягом мінімального періоду часу.

Таким чином за допомогою розробленого сервісу також можна виконати так званий анстейкінг монет (рис. 3.17).

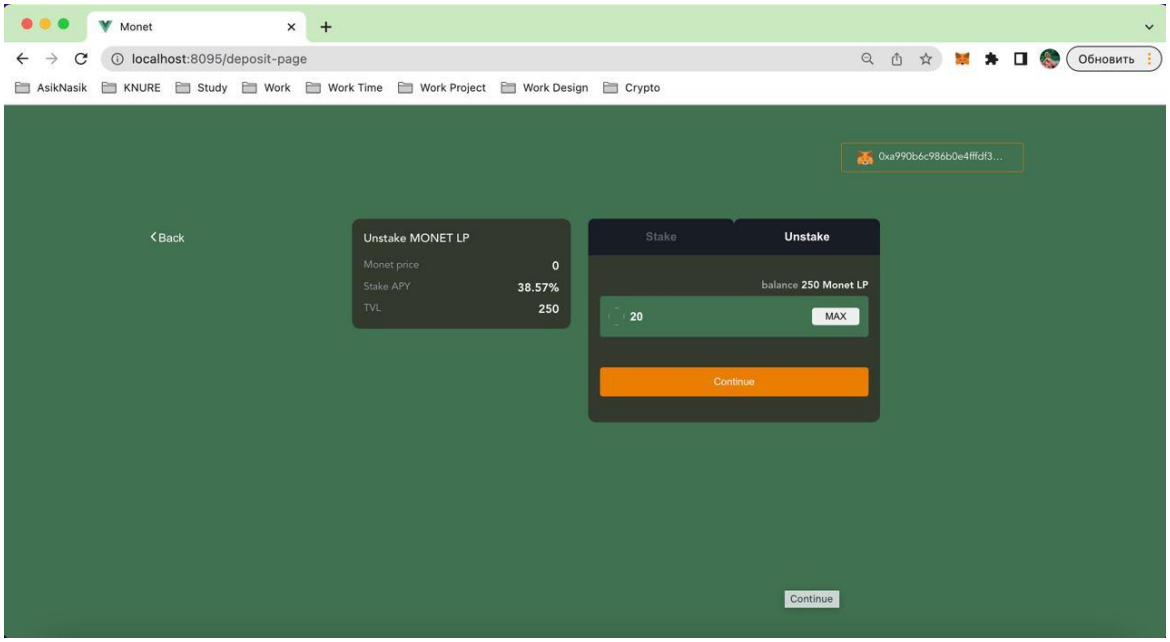

Рисунок 3.17 – Приклад анстейкінгу монет

Надалі користувач повинен знову підтвердити або відмінити операцію.

Також під час стейкінгу чи анстейкінгу монет виконано обробку помилок. Таким чином, якщо користувач відмінить операцію стейкінгу у відповідному вікні MetaMask, йому висвітиться червоне повідомлення помилки, яке міститиме інформацію щодо того, що саме відбулося – «Error! The operation was rejected» (рис. 3.18).

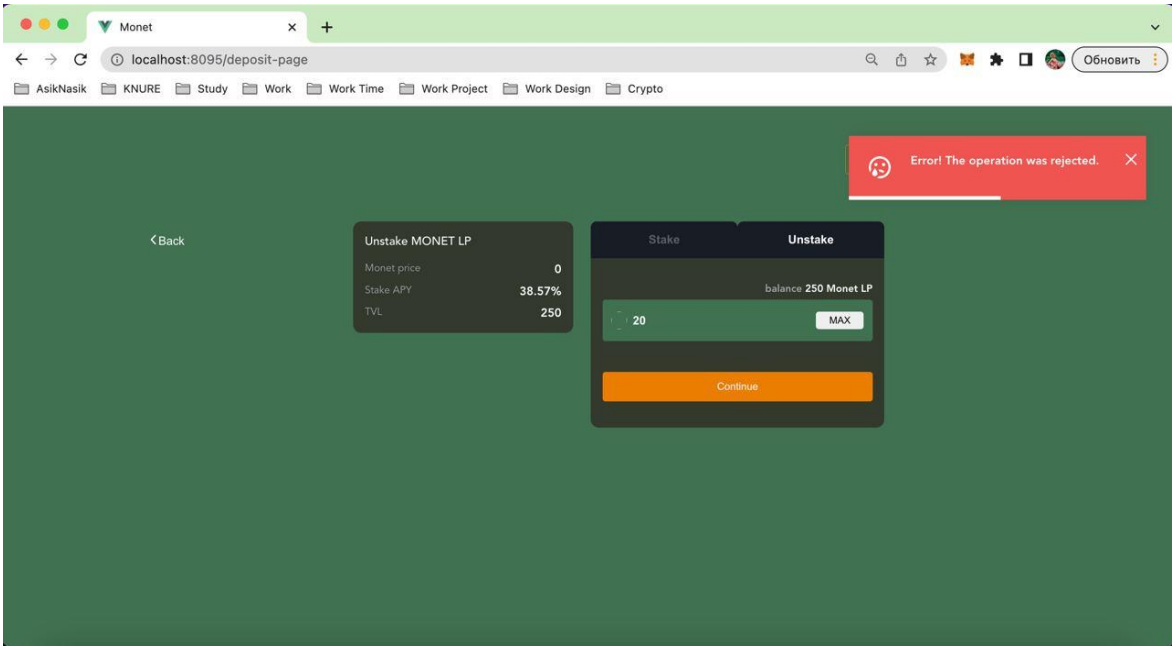

Рисунок 3.18 – Приклад повідомлення про помилку операції

У разі ж підтвердження операції слід почекати, поки MetaMask виконає операцію, і після цього можна оновлювати сторінку. Перевірити статус операції можна за допомогою того ж розширення MetaMask (рис. 3.19). Так дане розширення може відображати статуси операції, і, наприклад, статус операції «в очікуванні» означає, що операція ще не завершена і немає сенсу вже оновлювати сторінку.

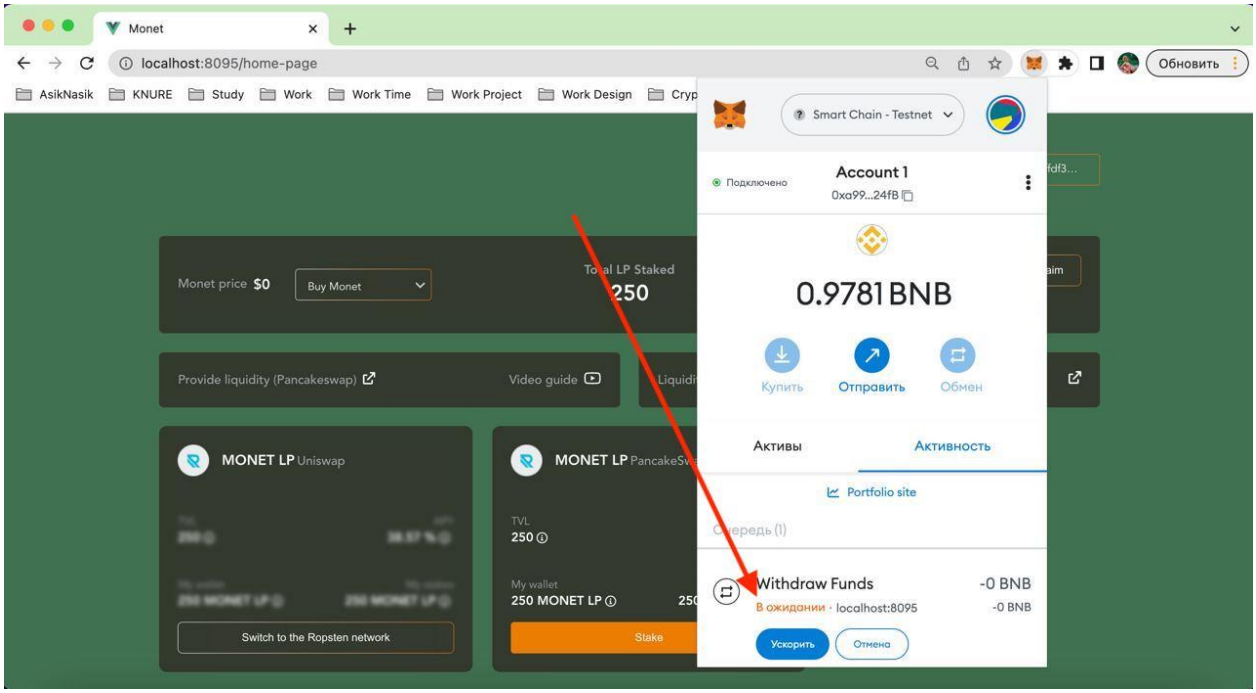

Рисунок 3.19 – Перегляд статусу операції в розширенні MetaMask

Якщо на головній сторінці сервісу користувач натисне кнопку «Claim», йому слід буде підтвердити, що він точно бажає провести вивід ревардів (рис. 3.20).

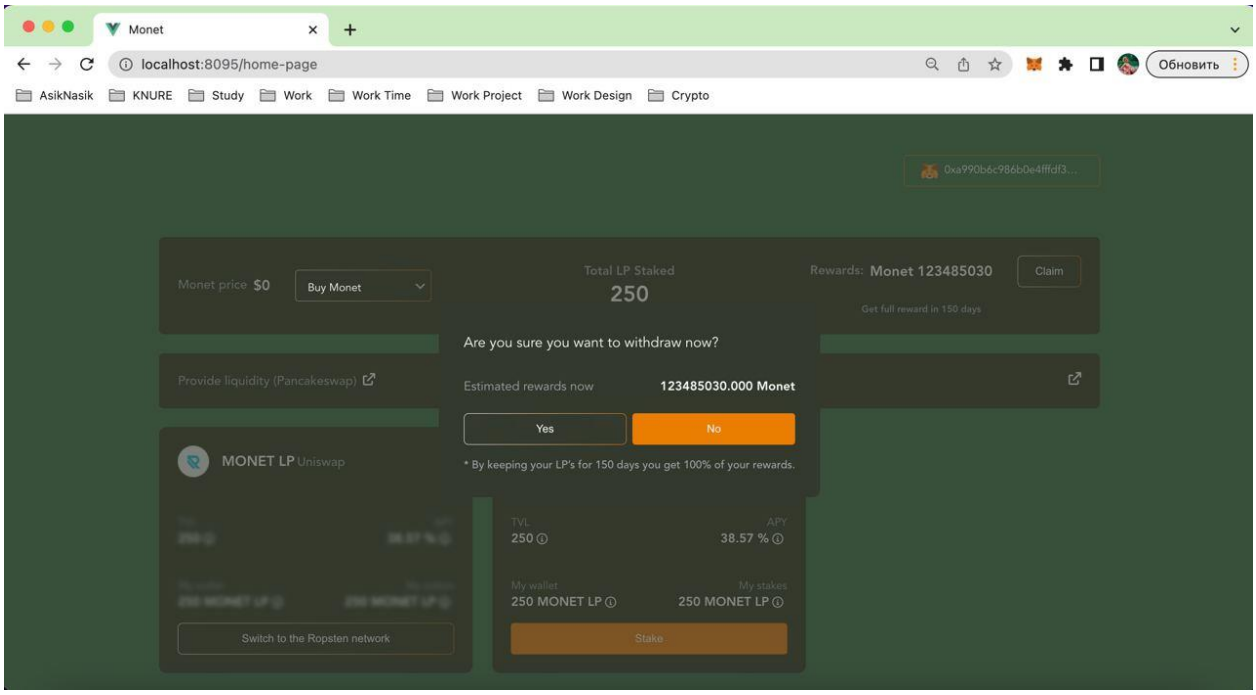

Рисунок 3.20 – Підтвердження операції виводу ревардів в сервісі

У випадку відміни операції вікно закриється, якщо ж користувач підтвердить її, то йому слід буде знову підтвердити операцію в розширенні MetaMask (рис. 3.21).

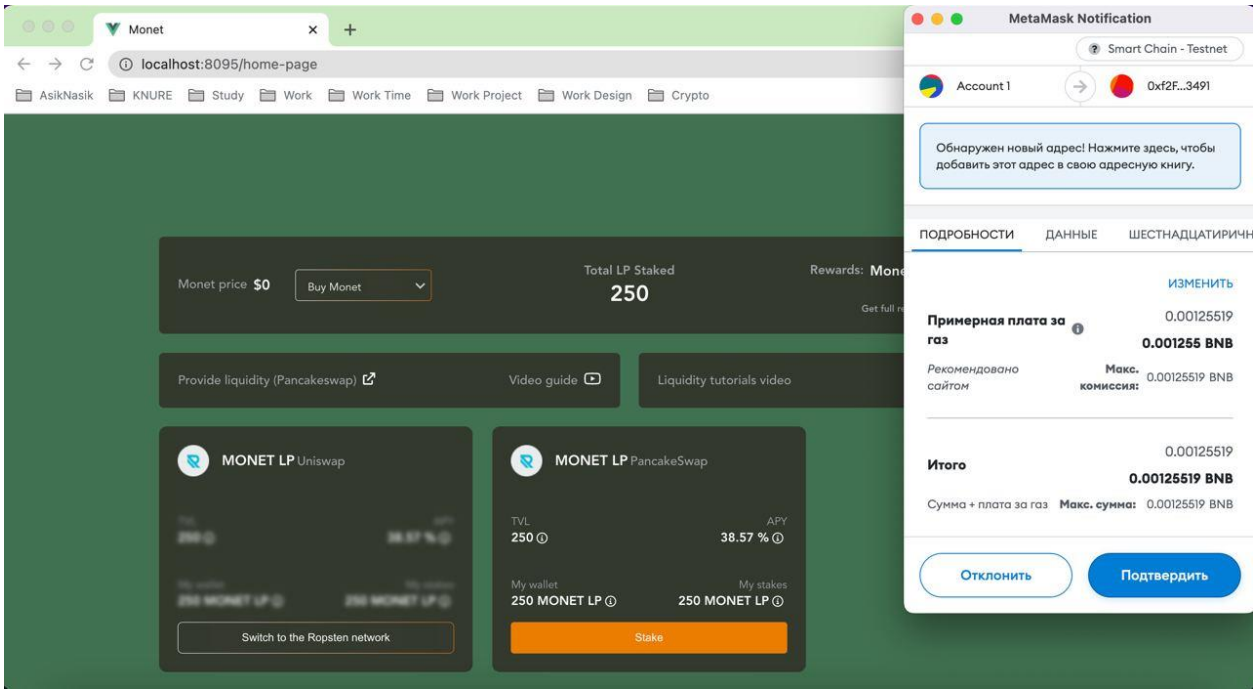

Рисунок 3.21 – Підтвердження операції виводу ревардів в розширенні MetaMask

Після цього реварди будуть зняті, а баланс в MetaMask – поповнений. Це можна побачити на головній сторінці сервісу (рис. 3.22).

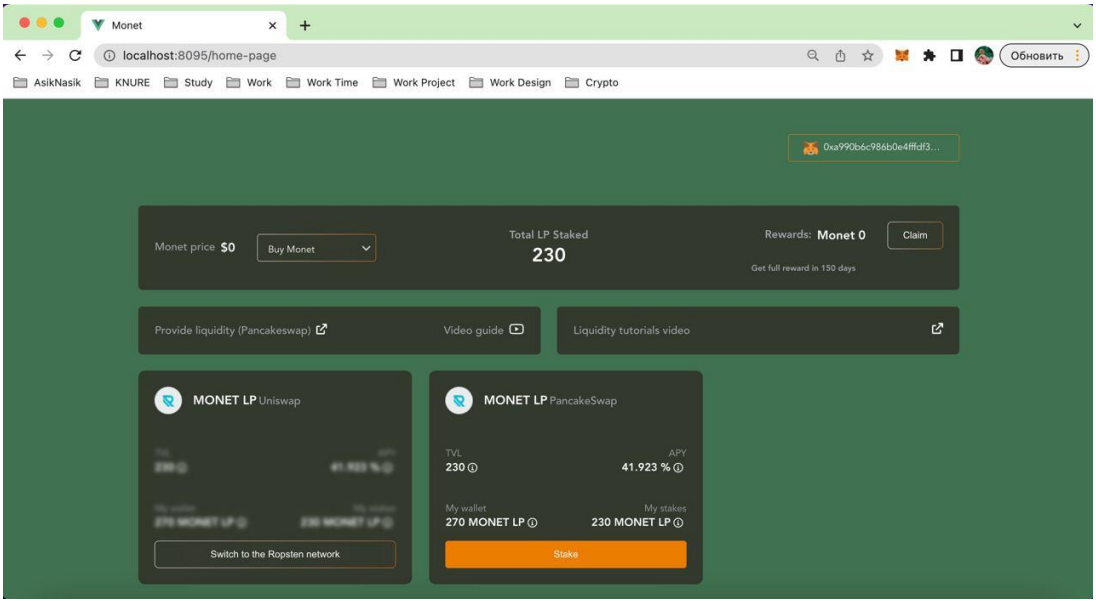

Рисунок 3.22 – Перегляд зняття ревардів на головній сторінці сервісу

Також операцію зняття ревардів можна побачити і в розширенні MetaMask – баланс тестового токену Monet змінено (рис. 3.23).

Описані вище дії користувача містять увесь сценарій дій, які доступні користувачу.

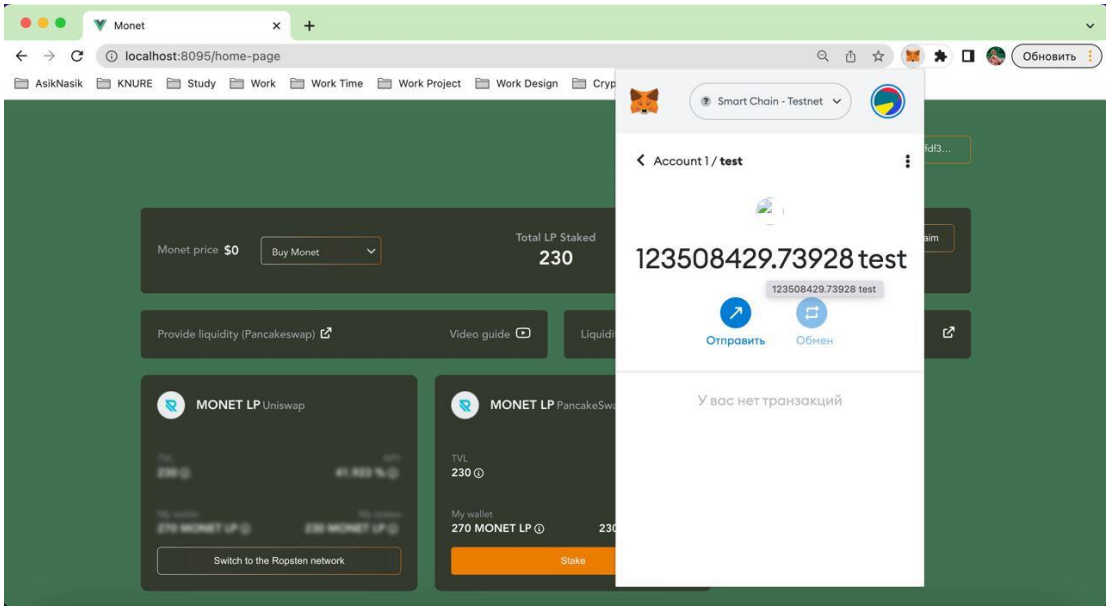

Рисунок 3.23 – Перегляд зняття ревардів в розширенні MetaMask

3.3 Тестування розробленого сервісу

Під час розробки сервісу було виконано функціональне тестування. Таким чином було складено тестові випадки, які перевірялись на вебсервісі. У випадку, коли система не відповідала вимогам тесту, створювався баг-репорт.

Для збереження тестових артефактів було використано сервіс Jira, який дозволяє зберігати і тестові випадки, і баг репорти зі зручним збереженням інформації щодо стану проведення тестування.

Jira – це система відстеження помилок, проблем і управління проєктами, розроблена Atlassian і вперше випущена в 2002 році. Система пропонує рішення як для розробників, так і для зацікавлених сторін, які не є розробниками.

Так для тестування сервісу було складено 32 тестові випадки. Розглянемо найбільш важливі та показові тестові випадки.

На рисунку 3.24 приведено тестовий випадок найвищого пріоритету – користувач повинен мати можливість підключити гаманець MetaMask до сервісу.

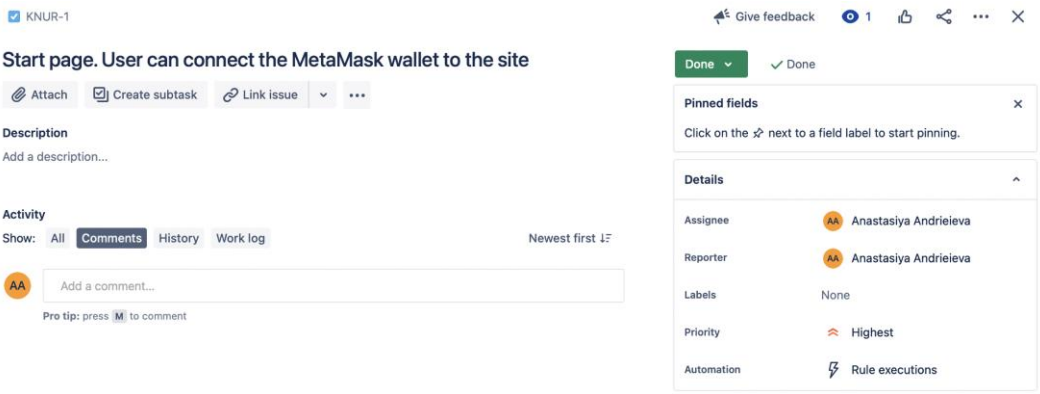

Рисунок 3.24 – Тестовий випадок підключення гаманця до сервісу

Іншим прикладом тестового випадку є тест, який призначений для перевірки, що користувач отримає чіткі повідомлення про помилки на кожній сторінці, де ці помилки можуть виникати (рис. 3.25).

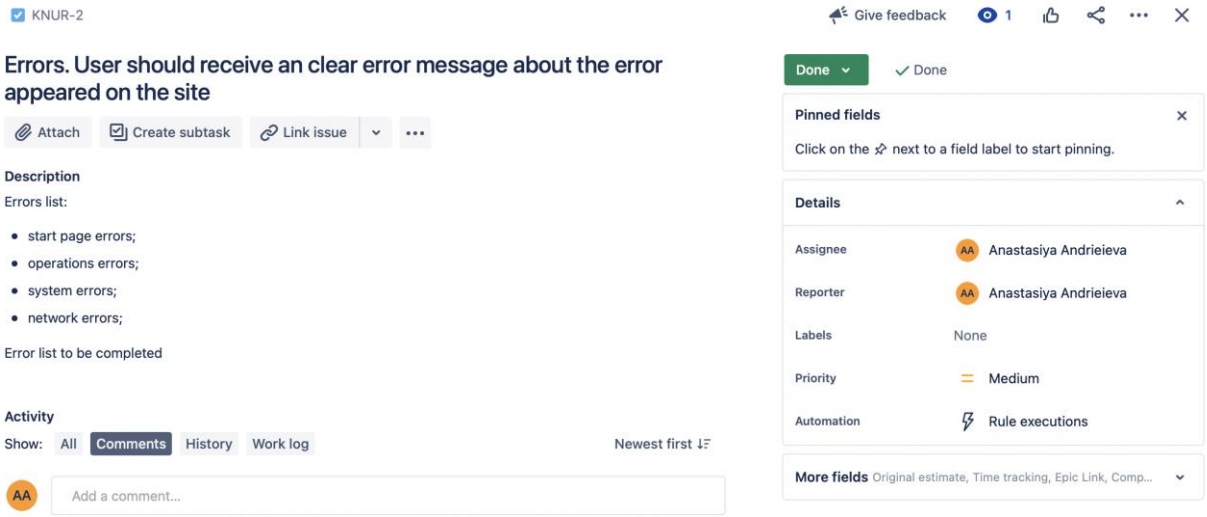

Рисунок 3.25 – Тестовий випадок для помилок на сервісі

У випадку знаходження помилок створювались відповідні баг репорти, приклад яких можна побачити на рисунку 3.26 – користувач перенаправлявся на пусту сторінку при натисканні на кнопку «PancakeSwap».

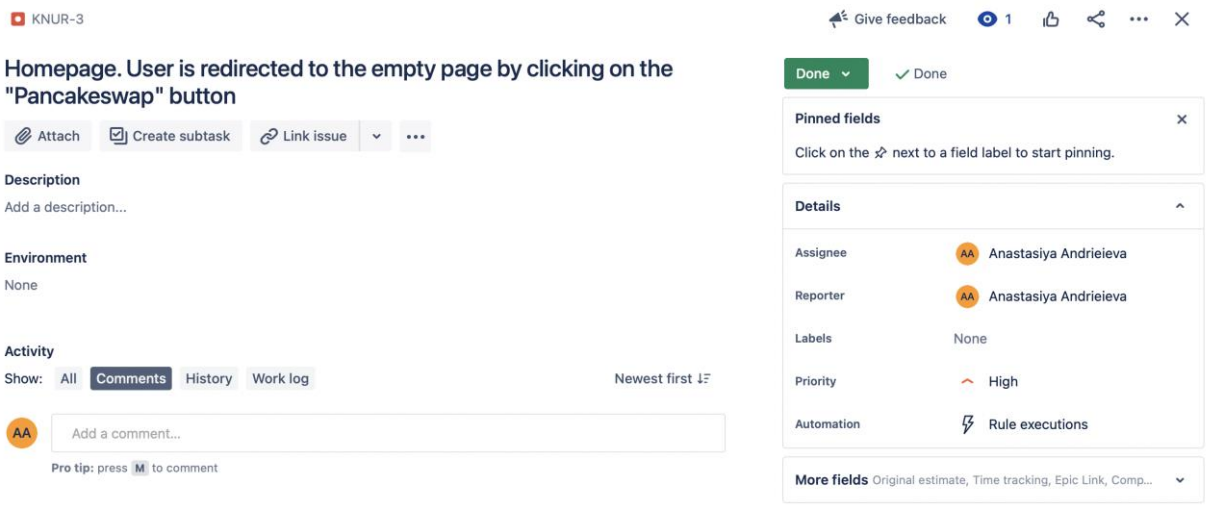

Рисунок 3.26 – Приклад баг репорту

Використаний сервіс Jira дозволяє зручно та наочно працювати з тасками, тестами та баг репортами, одразу переглядаючи їх на головній дошці. Використання подібного сервісу допоможе контролювати стан розробки системи та не втратити жодного багу.

ВИСНОВКИ

У рамках кваліфікаційної роботи було розроблено та реалізовано вебзастосунок для токенізації монет.

Також було досліджено технологію блокчейн та поняття і процес токенізації. Результатом кваліфікаційної роботи є розроблений вебзастосунок, із залученням засобів проєктування інформаційних систем та технології блокчейн для розробки сайту токенізації монет.

Використано технологію блокчейн, її можливості, ключові компоненти, поняття токенізації, монет.

В ході виконання кваліфікаційної роботи отримано наступні результати:

– досліджено технологію блокчейн;

– проведено аналіз процесу токенізації;

– проведено дослідження аналогів;

– використано технологію блокчейн в процесі розробки сервісу токенізації монет.

В ході розробки залучено наступний стек технологій: Vue 2, MetaMask, Smart Contract, Ethereum, BNB. Розроблювана програмна система призначення для використання в Україні та за кордоном.

Результати дослідження апробовано у вигляді 2 тез доповідей під час II Міжнародної науково-практичної конференції «SCIENCE AND INNOVATION OF MODERN WORLD» [39] та XLVII Міжнародної науково-практичної інтернет-конференції «ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ СУЧАСНОЇ НАУКИ В КРАЇНАХ ЄВРОПИ ТА АЗІЇ» [40].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Глибовець, А., & Точицький, В. (2017). Алгоритм токенізації та стемінгу для текстів українською мовою.

2. Генкин, А., & Михеев, А. (2017). Блокчейн: Как это работает и что ждет нас завтра. Альпина Паблишер.

3. Радченко, В. А., & Руденко, Д. А. (2010). Исследование возможности применения подхода реструктуризации гетерогенных источников данных в задачах интеграции информации.

4. Гусак, О. Ю., Кобзев, И. В., & Руденко, Д. А. (1999). Исследование вероятности блокировки соединения в WDM оптических сетях с произвольно распределенным входным потоком заявок. Радиоэлектроника и информатика, (2 (7)), 92-93.

5. Al-Shaibani, H., Lasla, N., & Abdallah, M. (2020). Consortium blockchain-based decentralized stock exchange platform. IEEE Access, 8, 123711-123725.

6. Cooperative, L. (2018). A Preliminary Review of blockchain in the Music Industry. Available at SSRN 3280838.

7. Руденко Д.О., Танянський О.С. (2021). Принципи передобробки даних для машинного навчання. Матеріали IV Міжнародної науково-практичної дистанційної конференції "TOPICAL ISSUES OF MODERN SCIENCE, SOCIETY AND EDUCATION", Харків, 381-385.

8. Гусак, О. Ю., Кобзев, И. В., & Руденко, Д. А. (1999). Модель протокола TCP-Reno с бесконечным источником заявок. Радиоэлектроника и информатика, (3 (8)), 64-66.

9. Shafronenko, A. Y., & Rudenko, D. A. (2020). ONLINE RECURRENT METHOD OF CREDIBILISTIC FUZZY CLUSTERING. ВВК 91, 37.

10. Филатов, В. А., Руденко, Д. А., & Гринева, Е. Е. (2014). Средства интеграции неоднородных данных в корпоративных информационно-телекоммуникационных системах.

11. Літошенко, А. В. (2017). Технологія блокчейн: переваги та неочевидні можливості використання у різних галузях. Економіка та держава, (8), 77-78.

12. Панасюк, І. В. (2019). Криптографічні алгоритми для генерації ключів на основі технології Блокчейн (Master's thesis, КПІ ім. Ігоря Сікорського).

13. Bhosale, J., & Mavale, S. (2018). Volatility of select crypto-currencies: A comparison of Bitcoin, Ethereum and Litecoin. Annu. Res. J. SCMS, Pune, 6.

14. Bodyanskiy, Y. V., Shafronenko, A., & Rudenko, D. (2019). Online Neuro Fuzzy Clustering of Data with Omissions and Outliers based on Completion Strategy. In CMIS (pp. 18-27).

15. Чирун, В. А., Танянский, С. С., & Руденко, Д. А. (2003). Повышение эффективности работы интегрированных информационных систем подразделений ОВД Украины. Право і Безпека, (2,№ 2), 188-190.

16. Танянский, С. С., Тулупов, В. В., & Руденко, Д. А. (2006). Модификация ограничений на ведение данных для обеспечения целостности крупномасштабных информационных систем. Вестник Национального технического университета Харьковский политехнический институт. Серия: Информатика и моделирование, (23), 137-144.

17. O Zeleniy, D Rudenko, V Lyubchenko, V Lyashenko (2022) Image Processing as an Analysis Tool in Medical Research.

18. Гринева, Е. Е., Танянский, С. С., & Руденко, Д. А. (2012). Однозначность ограничений целостности при модификации семантики базы данных. Вестник Херсонского национального технического университета, (1), 149-154.

19. Karandikar, N., Chakravorty, A., & Rong, C. (2021). Blockchain based transaction system with fungible and non-fungible tokens for a community-based energy infrastructure. Sensors, 21(11), 3822.

20. ВО Гороховатський, ДО Руденко, ТО Сірик (2019) Дослідження системи ієрархічних ознак при блочному поданні опису у складі множини ключових точок зображення.

21. Li, X., Wu, X., Pei, X., & Yao, Z. (2019, March). Tokenization: Open asset protocol on Blockchain. In 2019 IEEE 2nd International Conference on Information and Computer Technologies (ICICT) (pp. 204-209). IEEE.

22. D Rudenko, O Serhiienko, O Zeleniy, V Lyashenko (2022) Model for Predictive Analysis of International Trade Based on the Dynamics of Stock Indices (Example of Data from the USA, Canada and UK).

23. Valeonti, F., Bikakis, A., Terras, M., Speed, C., Hudson-Smith, A., & Chalkias, K. (2021). Crypto collectibles, museum funding and OpenGLAM: challenges, opportunities and the potential of Non-Fungible Tokens (NFTs). Applied Sciences, 11(21), 9931.

24. Kharitonova, Y. S., & Rahmatulina, R. S. (2020, October). Technological Convergence and the Future of Copyright. In International Scientific and Practical Conference (pp. 267-274). Springer, Cham.

25. Руденко, Д. О., & Мальков, Ю. А. (2011). Об одном подходе к управлению распределенными системами баз данных. Вестник Херсонского национального технического университета, (2 (41)), 193-196.

26. Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized finance. Journal of Financial Regulation, 6(2), 172-203.

27. Monga, S., & Singh, D. (2022). MRBSChain a novel scalable medical records binance smart chain framework enabling a paradigm shift in medical records management. Scientific Reports, 12(1), 1-12.

28. Руденко, Д. А., Танянский, С. С., & Филатов, В. А. (2005). МУЛЬТИАГЕНТНЫЙ ПОДХОД К ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ В СИСТЕМЕ ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ.

29. Choi, N., & Kim, H. (2019). A Blockchain-based user authentication model using MetaMask. Journal of Internet Computing and Services, 20(6), 119-127.

30. Pramulia, D., & Anggorojati, B. (2020, November). Implementation and evaluation of Blockchain based e-voting system with Ethereum and Metamask. In 2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS) (pp. 18-23). IEEE.

31. Lee, W. M. (2019). Using the metamask chrome extension. In Beginning Ethereum Smart Contracts Programming (pp. 93-126). Apress, Berkeley, CA.

32. Shevchuk, T. D., Karpenko, B. A., Pereskokov, D. D., & Sivtseva, N. G. (2021). Cryptocurrency: analysis of its usage and prospects. Молодежный вестник ИрГТУ, 11(2), 146-150.

33. Morrow, M. J., & Zarrebini, M. (2019). Blockchain and the tokenization of the individual: Societal implications. Future Internet, 11(10), 220.

34. Konashevych, O. (2020). General concept of real estate tokenization on blockchain. European Property Law Journal, 9(1), 21-66.

35. Gupta, A., Rathod, J., Patel, D., Bothra, J., Shanbhag, S., & Bhalerao, T. (2020, October). Tokenization of Real Estate Using Blockchain Technology. In International Conference on Applied Cryptography and Network Security (pp. 77-90). Springer, Cham.

36. Gupta, S., & Sadoghi, M. (2021). Blockchain transaction processing. arXiv preprint arXiv:2107.11592.

37. Bach, L. M., Mihaljevic, B., & Zagar, M. (2018, May). Comparative analysis of Blockchain consensus algorithms. In 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1545-1550). Ieee.

38. Oliveira, L., Zavolokina, L., Bauer, I., & Schwabe, G. (2018). To token or not to token: Tools for understanding Blockchain tokens.

39. Андрєєва, А., & Руденко, Д. (2022). ЯК БЛОКЧЕЙН ТОКЕНІЗАЦІЯ ЗМІНЮЄ СВІТ.

40. Андрєєва, А., & Митцева, О. (2022). ВИВЧЕННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ЯК НОВА ДИСЦИПЛІНА У ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ.