МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

Факультет прикладної математики та інформатики
(повне найменування назва факультету)

Кафедра інформаційних систем
(повна назва кафедри)

ДИПЛОМНА РОБОТА

РОЗРОБКА ЗАСТОСУНКУ З ВИКОРИСТАННЯМ ВЕБ-3 ТЕХНОЛОГІЙ

Виконав(ла): студент(ка) групи ПМІ-44
спеціальності 122 – комп'ютерні науки
(шифр і назва спеціальності)

Пришляк Б. А.
(підпис) (прізвище та ініціали)

Керівник Бернакевич І. Є.
(підпис) (прізвище та ініціали)

Рецензент _____
(підпис) (прізвище та ініціали)

2023

ЗМІСТ

АНОТАЦІЯ

Об’єкт дослідження: Технологія блокчейн.

Мета роботи: Необхідно дослідити технологію блокчейн, описати її теоретичні відомості, особливості, переваги, недоліки, розвиток та зародження. Також важливо розглянути різні сфери використання блокчейну, зокрема фінансову, медичну та державний сектор. Провести аналіз ключових особливостей технології.

У практичній частині проекту потрібно розробити смарт-контракт та веб-застосунок, в якому використовуються цифрові транзакції, за приклад було взято маркетплейс.

Ключові слова: БЛОКЧЕЙН, ETHEREUM, СМАРТ КОНТРАКТ, ЕЛЕКТРОННИЙ ГАМАНЕЦЬ, ЦИФРОВА ТРАНЗАКЦІЯ, КРИПТОВАЛЮТА, ВЕБ-3.

ВСТУП

Інформаційні технології все більше проникають у всі сфери нашого життя, а одна з найцікавіших і перспективних технологій останнього часу - блокчейн. Вперше концепція блокчейну була описана багато років тому, але її перше практичне застосування стало можливим у 2008 році з появою криптовалюти Bitcoin, яка базується на цій технології. З кожним днем блокчейн набуває все більшої популярності і розширює свій спектр застосування.

Блокчейн - це новий спосіб зберігання інформації, що представляє собою децентралізовану базу даних, утворену послідовним ланцюжком зв'язаних між собою блоків. Основні переваги цієї технології - надійність, стійкість до відмов та безпека. За короткий час вже було виявлено багато можливостей використання блокчейну, таких як зберігання цифрових активів, ідентифікаційна інформація, захист авторських прав, голосування та багато іншого.

Криптовалюти стали однією з найбільш обговорюваних і спірних тем в мережі, а їх сумарна капіталізація зростає з кожною хвилиною. Загалом, через нестабільність фіатних грошей та численні світові кризи, довіра до банків та фіатних грошей поступово зменшується. Тому багато розвинутих країн вже починають використовувати блокчейн у державному секторі, щоб забезпечити більш надійні дані та зменшити роль людського фактору, що сприяє зменшенню рівня корупції.

Тому, моєю метою є дослідити доцільність використання технології блокчейн у різних сферах діяльності, оцінити перспективи її розвитку та створити веб-застосунок, який використовуватиме цю технологію.

1. ТЕХНОЛОГІЯ БЛОКЧЕЙН: ОСОБЛИВОСТІ, ІСТОРІЯ ТА РОЗВИТОК.

1.1. Поняття блокчейну

Блокчейн - це термін, створений з комбінації двох англійських слів: "block" (блок) і "chain" (ланцюг). Блок представляє собою файл з певними характеристиками, такими як частота створення, розмір та дані. Дані в блоках зашифровані за допомогою криптографічних алгоритмів. Ланцюг відображає зв'язок між блоками і формує логічну послідовність, де кожен новий блок містить посилання на попередній блок. Цей спосіб зберігання інформації майже унеможливлює підробку даних, оскільки будь-яка зміна в блоці призводить до зміни його посилання, що спричиняє "ланцюжкову реакцію" і відхиляє зміну.

Основна відмінність блокчейна від типових баз даних полягає в тому, що бази даних використовують таблиці для зберігання інформації, тоді як блокчейн використовує блоки, що пов'язані один з одним. Блокчейн є децентралізованою базою даних (P2P), де вся інформація розподіляється по багатьом машинах, які можуть знаходитись у різних частинах світу, без центрального сервера. Ці комп'ютери називаються вузлами.

Блокчейн також є прозорою системою, де кожен має можливість переглянути інформацію про будь-який блок. Крім того, блокчейн використовує криптографічні алгоритми для забезпечення безпеки системи, які забезпечують незмінність блоку транзакцій та аутентифікацію.

Хешування - це криптографічна техніка, яка перетворює вхідний масив даних будь-якої довжини на стрічку фіксованої довжини. Хеш-функції, що використовуються в блокчейні, повинні задовольняти умову відсутності колізій, тобто неможливість отримати однаковий хеш з різних наборів вхідних даних.

Хеші використовуються для вказівки суміжних блоків у ланцюгу блоків. У блокчейні всю інформацію в блоках хешують для створення вказівника за

допомогою бінарного дерева хешів, так званого дерева Меркла(див. рис. 1.1). Це означає, що навіть найменша зміна в блоку призведе до зміни хешу цього блоку і, відповідно, всього ланцюжка.

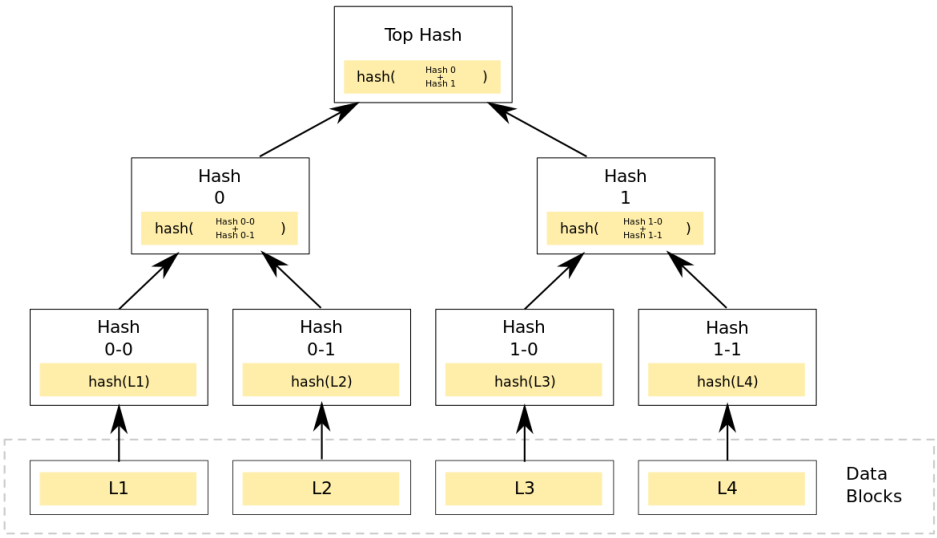

Рисунок 1.1 Дерево Маркла

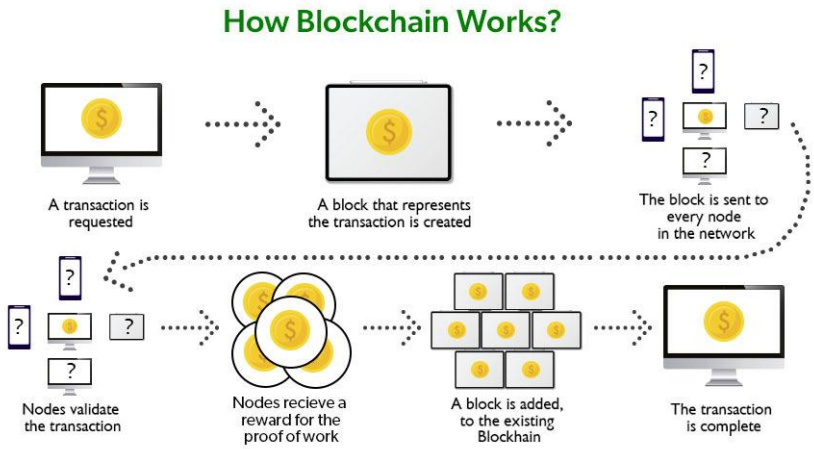

Рисунок 1.3 Принцип роботи технології блокчейн

Також у блокчейні використовуються цифрові підписи, які базуються на криптографії з відкритим ключем. Відкритий ключ використовується для перевірки електронного підпису і є доступним для всіх. Закритий ключ, натомість, зберігається в таємниці і використовується для створення електронного підпису.

Відкритий ключ може бути обчислений за допомогою закритого ключа, але неможливо зворотнє обчислення . Ініціатор транзакції підписує дані своїм закритим ключем, шифрує повідомлення за допомогою публічного ключа одержувача, а одержувач розшифровує дані за допомогою свого закритого ключа. Таким чином, тільки власник приватного ключа, якому адресована транзакція, може розшифрувати повідомлення. Підпис використовується для підтвердження того, що саме цей користувач ініціював транзакцію. Знаючи повідомлення, підпис та публічний ключ підписанта, можна підтвердити його автентичність.

1.1.1 Історія виникнення технології блокчейн

У 1991 році двома американськими вченими, Скоттом Сторнеттом та Стюартом Габером, була опублікована робота, в якій вперше описана технологія, яка нагадує сучасний блокчейн. Ця технологія дозволяла отримувати інформацію про час створення та модифікації електронних документів. Звичайна клієнт-серверна архітектура, яка використовувалася тоді, мала деякі недоліки, такі як можливість "прослуховування" мережі, сумніви в безпеці сервера, повільна обробка даних і великий обсяг пам'яті для зберігання інформації.

З метою поліпшення цієї системи, були запропоновані покращення, включаючи використання криптографічно захищених хеш-функцій. Замість передачі всього документа на сервер, відправлялося лише хеш-значення цього документа. Це дозволяло зменшити обсяг передаваних даних і збільшити швидкість передачі. Іншим покращенням було впровадження цифрового підпису.

Проте одна проблема залишалася: сервер міг видавати недостовірні часові мітки. Для її вирішення було запропоновано два способи. Перший полягав у використанні централізованого сервера, який створював часові мітки таким чином, що ускладнювало процес створення недостовірних міток. Другий спосіб

передбачав розподіл процесу підтвердження достовірності між іншими користувачами.

Підхід з використанням серверу передбачав виконання наступних кроків:

a. Після отримання запиту від користувача, сервер надсилав сертифікат, що містив хеш, ідентифікаційний номер (ID) клієнта, часову мітку, порядковий номер та з'єднувальну інформацію (ЗІ). ЗІ включала часову мітку, хеш, ID та хеш ЗІ попереднього сертифіката.
b. При обробці наступного запиту сервер надсилав клієнту ID наступного запиту. Таким чином, кожен клієнт мав достатньо інформації про попередній та наступний сертифікати. Для перевірки достовірності інформації було достатньо перевірити збіжність інформації, рухаючись по вибудованій ієрархії.

Однак, існувала можливість обману системи шляхом створення "фейкового" ланцюга, який мав більшу довжину, ніж фактично перевірялась системою. Це означало, що при перевірці система може обійти лише "фейкову" частину ланцюга і не виявити недостовірність інформації, наданої сервером.

Останнім рішенням було розподілити процес підтвердження між іншими користувачами. Запроваджено захищену схему, в якій кожен користувач може підписувати повідомлення, а також доступний псевдорандомний генератор для всіх користувачів. Якщо клієнт бажає поставити мітку часу на документ, він використовує хеш документа як початкове значення генератора. Генератор повертає кортеж, що містить ідентифікатори інших користувачів в мережі. Клієнт надсилає повідомлення кожному користувачеві з кортежу, вказуючи хеш документа та свій ідентифікатор. Кожен з них ставить свою часову мітку і надсилає результат назад клієнту. Таким чином, клієнт отримує масив часових міток, згенерованих іншими учасниками мережі.

Мережа без використання серверу має значно більше переваг: час отримання відповіді є швидшим, а клієнтам не потрібно зберігати великі сертифікати з з'єднувальною інформацією.

Ще одним значущим проривом у 2009 році було створення блокчейн-системи для збереження транзакцій з використанням криптовалюти Bitcoin, розробленої однією або групою осіб під псевдонімом Сатоші Накамото. Проект став надзвичайно успішним, і щодня все більше людей починають використовувати Bitcoin для проведення операцій та зберігання коштів. До сьогоднішнього дня Bitcoin є лідером на ринку криптовалют.

1.1.2 Типи блокчейн-платформ

Зазвичай виділяють три типи блокчейн-платформ:

- Публічні платформи
- Приватні платформи
- Гібридні (консорціум) платформи.

Публічні блокчейн-платформи дозволяють усім користувачам приєднатися до них без обмежень. Будь-хто може переглядати інформацію у блоках, долучатися до їх створення та верифікації, залишаючись анонімним. Такі платформи мають кілька переваг, зокрема:

- Високий рівень довіри: завдяки алгоритмам підтвердження, користувачам не потрібно хвилюватись про довіру до окремих вузлів системи.
- Захищеність: збільшення кількості вузлів у мережі робить її більш стійкою до зловмисних атак.
- Прозорість: інформація про кожен блок доступна для всіх користувачів.
-

Проте публічні блокчейн-платформи також мають свої недоліки:

- Низька швидкість обробки транзакцій: через велику кількість вузлів, швидкість верифікації транзакцій може бути низькою. Вищий рівень безпеки може призводити до зниження швидкості.
- Високе споживання електроенергії: задіяність тисяч машин у процесі створення нових блоків та підтвердження транзакцій може вимагати значних енергетичних ресурсів.

Публічні блокчейн-платформи зазвичай використовуються для зберігання та обміну криптовалютами. Приклади публічних блокчейн-платформ включають Bitcoin та Ethereum.

Приватні блокчейн-платформи обмежують участь користувачів, допускаючи до мережі лише обраних осіб і зазвичай використовуються всередині організацій. Контролююча організація відповідає за безпеку, права користувачів та доступ до мережі. Хоча приватні платформи мають схожу структуру з публічними, вони є значно меншими. Такі системи не можна повністю назвати децентралізованими, оскільки фактичний контроль знаходиться в руках конкретної організації. Ідентифікація користувачів зазвичай проста, оскільки анонімність не є необхідною.

Приватні блокчейн-платформи мають кілька переваг:

- Швидкість: через меншу кількість вузлів порівняно з публічними платформами, швидкість обробки транзакцій значно вища.
- Масштабування: організації можуть легко збільшувати або зменшувати кількість вузлів у мережі в залежності від потреб.

Проте приватні блокчейн-платформи також мають свої недоліки:

- Побудова довіри: оскільки анонімність відсутня, потрібно розробити механізми довіри для передачі конфіденційної інформації.
- Низький рівень безпеки: через обмежену кількість вузлів, рівень безпеки нижчий, ніж у публічних блокчейн-платформ. Існує ризик атаки на систему шляхом отримання доступу до системи управління, оскільки повна децентралізація відсутня.

- Централізованість: потрібна система контролю доступу та ідентифікації. Це створює вразливість приватної системи, оскільки доступ до контролера може дати повний доступ до всієї системи.

Приватні блокчейн-платформи зазвичай використовуються для голосувань, цифрової ідентифікації та аудиту. Приклади приватних блокчейн-платформ включають Fabric і Corda.

Гібридні блокчейн-платформи поєднують в собі характеристики як публічних, так і приватних платформ. Вони контролюються кількома організаціями, і доступ до інформації в блоках обмежений лише певними користувачами. В таких системах можна визначати, яка інформація є загальнодоступною, а яка повинна залишатися конфіденційною. Гібридні платформи можуть успадковувати переваги і недоліки як публічних, так і приватних блокчейн-платформ.

Ці гібридні платформи широко використовуються в банківській та державній сферах. Приклади таких платформ включають Dragonchain і R3. Важливо враховувати, що неможливо однозначно визначити, який тип блокчейн-платформи є найкращим. Вибір залежить від індивідуальних потреб замовника, оскільки кожен тип має свої переваги і недоліки.

1.1.3 Типи консенсусу

Блокчейн системи представляють собою децентралізовані структури, де учасники взаємодіють згідно з набором правил.

Консенсус в блокчейні - це алгоритм, який визначає правила та функції для досягнення узгодженості між усіма учасниками мережі. Через консенсус у системі формується надійність.

На сьогоднішній день існує багато алгоритмів консенсусу, які забезпечують різний рівень безпеки та швидкості обробки транзакцій. Деякі з

найпоширеніших алгоритмів включають Proof of Work (PoW), Proof of Stake (PoS) та Delegated Proof of Stake (DPoS).

Алгоритм Proof of Work є одним з перших та найбільш поширених. У цьому алгоритмі всі вузли мережі беруть участь у створенні блоків. Майнери змагаються, щоб сформувати новий блок з останніми транзакціями. Кожен майнер має доступ до цього списку та вирішує складну математичну задачу, яка підтверджує валідність транзакцій.

Особливістю алгоритму є те, що для його виконання потрібні великі обчислювальні ресурси, але перевірка результату є простою.

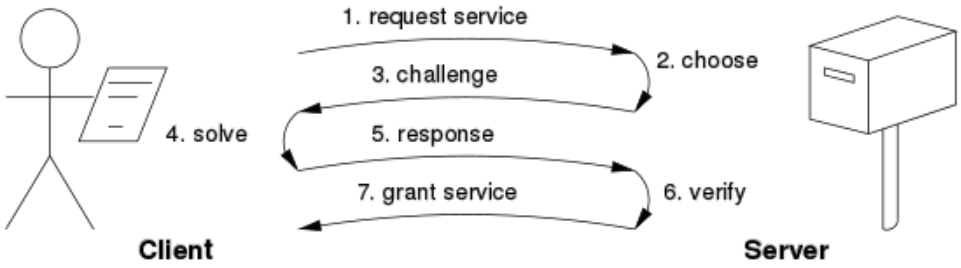

Рисунок 1.3 Принцип роботи алгоритму Proof of Work

В процесі роботи кожен майнер генерує хеш-значення, яке отримується шляхом обчислення хеш-функцією (наприклад, SHA-256) оброблених даних. Якщо будь-яка транзакція була змінена, хеш-значення також зміниться. Щоб ускладнити процес обчислення хеш-значень, алгоритм встановлює обмеження для цільового значення хешу. Результат хешування не повинен перевищувати цю ціль. Для досягнення цього, до даних додається неконтрольоване число, відоме як nonce, яке змінює значення хешу. Щоб збільшити складність обчислень, значення цільового хешу зменшується, що змушує майнерів перебирати більше значень nonce. Коли майнер отримує хеш, який відповідає умовам пошуку, він повідомляє про це всі інші машини, які повинні підтвердити правильність обчислень.

Алгоритм PoW має переваги в надійності та простоті, але має й недоліки, такі як висока енерговитратність та низька швидкість обробки транзакцій. Через

це багато систем розглядають перехід на інший алгоритм, відомий як Proof of Stake (PoS).

Алгоритм Proof of Stake (PoS) визначає, що чим більше криптовалюти має майнер (наприклад, у власності), тим більший внесок він має у створенні наступного блоку, що збільшує його шанси на генерацію нового блоку. Різні реалізації можуть використовувати різні показники для визначення "ціни". Наприклад, якщо майнер володіє n% загальної кількості криптовалюти, то його теоретичний шанс на створення наступного блоку становить n%. Головна ідея алгоритму полягає в тому, щоб ускладнити атаки шляхом підвищення вартості, а не рівня ресурсів.Алгоритм Proof of Stake має переваги в надійності та енергоефективності, але може створювати схильність до формування монополій.

Алгоритм Delegated Proof of Stake (DPoS) є модифікацією PoS. В ньому користувачі обирають "свідків" (witnesses), які мають підтверджувати наступні блоки. Кожен користувач голосує за свого обраного свідка, і вага голосу залежить від його "ціни". Якщо свідок має погану репутацію, він може бути заміщений. DPoS має переваги у швидкості обробки транзакцій та масштабованості порівняно з PoS.

Існують інші алгоритми, але вони не так поширені на даний момент. Кожна система вибирає відповідний алгоритм в залежності від своїх потреб. Розробники з усього світу працюють над новими алгоритмами, які будуть поєднувати вимоги безпеки, швидкості та надійності.

1.2 Що таке Web3

Централізація була корисною для мільярдів людей, які змогли підключитися до глобальної мережі Інтернет та використовувати стабільну та надійну інфраструктуру. Однак, внаслідок централізованого підходу, деякі великі організації набули значної влади над Інтернетом і приймають

односторонні рішення щодо того, що дозволено або заборонено. Web3 є відповіддю на цю проблему. Замість монополії великих технологічних компаній, Web3 використовує децентралізований підхід і створюється, керується та належить користувачам. Web3 передає владу індивідуальним особам, а не корпораціям. Перш ніж ми поговоримо про Web3, давайте розглянемо, як ми дійшли до цього пункту.

Багато людей вважають, що Інтернет є невід'ємною частиною сучасного життя. Він був розроблений і розвивається вже деякий час. Сьогоднішній Інтернет відрізняється від початкової версії, і для кращого розуміння цього факту історію Інтернету можна розділити на два етапи - Веб 1.0 і Веб 2.0.

У 1989 році Тім Бернерс-Лі, працюючи в CERN у Женеві, розробляв протоколи, які згодом стали основою глобальної мережі. Його ідея полягала в створенні відкритих децентралізованих протоколів, які дозволяють обмінюватися інформацією будь-де на планеті. Перша його розробка, відома як "Веб 1.0", відбулася протягом приблизно 1990-2004 років. Веб 1.0 передбачав створення в основному статичних веб-сайтів, належних компаніям, і взаємодію користувачів практично не передбачалося - індивідуальні особи рідко створювали контент. Це призвело до того, що Веб 1.0 був відомий як "мережа для читання".

З переходом до Веб 2.0, який розпочався в 2004 році з появою соціальних мереж, мережа стала більш інтерактивною. Замість простого читання, користувачі отримали можливість створювати власний контент і взаємодіяти між собою. Однак, зростання числа людей в мережі призвело до зміцнення деяких провідних компаній, які контролювали значну частку трафіку та створеної в мережі цінності. Веб 2.0 також стимулював модель доходів, засновану на рекламі. Хоча користувачі могли створювати контент, вони не володіли ним і не отримували вигоди від його монетизації.

Гевін Вуд, співзасновник Ефіріуму, винайшов концепцію "Веб 3.0" незабаром після запуску Ефіріуму в 2014 році. Він висловив рішення проблеми, яку відчували багато прихильників криптографії: традиційна мережа вимагає

надмірної довіри. Більшість існуючих мереж, які люди знають і використовують сьогодні, ґрунтуються на довірі до обмеженої кількості приватних компаній, що діють на користь суспільства.

Термін "Web3" став універсальним для позначення нового ідеалу Інтернету. У своїй суті, Web3 використовує блокчейн, криптовалюти та NFT (Non-Fungible Token) для повернення контролю користувачам у вигляді власності. Найкраще це сформульовано у повідомленні 2020 року на Twitter: "Web1 був доступний тільки для читання, Web2 - для читання-запису, Web3 - для читання-запису-власності". Таким чином, Web3 надає можливість не лише читати і записувати інформацію в мережі, але й володіти цією інформацією як власність.

Основні концепції Web3:

- Децентралізація: Web3 пропонує розподіл прав власності між творцями та користувачами, уникнувши контролю великими централізованими організаціями.

- Бездозвольність: Web3 надає рівні можливості для всіх, ніхто не виключається і всі мають рівний доступ до участі.

- Нативні платежі: Web3 використовує криптовалюту для здійснення платежів та переказів коштів в Інтернеті, уникнувши потреби в традиційних банківських та платіжних системах.

- Відсутність потреби в довірі: Web3 працює за допомогою стимулів та економічних механізмів, не потребуючи полагодження на довірені треті особи.

Отже, Web3 пропонує децентралізований інтернет, де кожен має можливість брати участь, використовуючи криптовалюту та залучаючи економічні стимули замість довіри до централізованих організацій.

1.2.1 Володіння

Web3 надає унікальну можливість володіти цифровими активами. У порівнянні з Web2, де внутрішньоігрові предмети або цифрові активи пов'язані безпосередньо з обліковим записом гравця, Web3 пропонує пряме володіння за допомогою невзаємозамінних токенів (NFT). Це означає, що ви маєте повний контроль над своїми активами, і навіть творці гри не можуть їх відібрати.

Наприклад, якщо ви припините використовувати певну гру, ви збережете власність і можливість продавати або обмінювати свої внутрішньоігрові предмети на відкритих ринках. Це дозволяє вам відновити частину або всю вартість, яку ви вклали у ці активи. Таким чином, Web3 забезпечує безпрецедентний рівень прав власності, дозволяючи вам контролювати свої цифрові активи незалежно від рішень творців гри чи зміни умов гри.

1.2.2 Опір цензурі

У Web3 ваші дані зберігаються у блокчейні. Коли ви вирішите залишити платформу, ви можете взяти з собою свою репутацію, підключивши її до іншого інтерфейсу, який чіткіше відповідає вашим цінностям.

Web 2.0 вимагає, щоб творці контенту довіряли платформам і не змінювали правила, але стійкість до цензури є природною особливістю платформи Web3.

У традиційних платформах вам потрібно створювати окремі облікові записи для кожної з них. Наприклад, у вас можуть бути облікові записи на Twitter, YouTube та Reddit. Якщо ви хочете змінити своє ім'я або фото профілю, вам потрібно зробити це окремо для кожного облікового запису. Деякі платформи дозволяють вам увійти за допомогою облікових записів у соціальних

мережах, але це також може призвести до проблеми цензури. Всього за один клік, ці платформи можуть заблокувати вас і відібрати доступ до всього вашого онлайн-життя. Що ще гірше, багато платформ вимагають від вас надавати особисту інформацію для створення облікового запису, на яку вам потрібно довіряти цим компаніям. У свою чергу, Web3 вирішує ці проблеми, дозволяючи вам контролювати свою цифрову ідентичність за допомогою Ethereum-адреси та профілю ENS. Використання Ethereum-адреси забезпечує вам єдиний вхід на різноманітні платформи, що є безпечним, несхильним до цензури та анонімним.

1.2.3 Децентралізовані автономні організації

У Web3 ви можете стати співвласником платформи, використовуючи токени, які виступають як акції компанії. DAO (децентралізовані автономні організації) дозволяють забезпечити колективне володіння платформою та приймати рішення щодо її майбутнього. DAO визначаються як смарт-контракти, які автоматизують децентралізоване ухвалення рішень щодо розподілу ресурсів (токенів). Власники токенів голосують за використання ресурсів, і програмний код автоматично виконує результати голосування. У Web3 існує багато спільнот, які вважаються DAO, але кожна з них може мати різний рівень децентралізації та автоматизації за допомогою коду. В даний час проводиться дослідження для вивчення потенціалу розвитку DAO в майбутньому.

1.2.4 Нативні платежі

Платіжна інфраструктура Web2 базується на участі банків та платіжних систем, що утруднює доступ до неї для людей без банківських рахунків або тих, хто проживає у віддалених регіонах або інших країнах. У порівнянні з цим, Web3 використовує токени, такі як ETH, для безпосереднього переказу грошей прямо у браузері без потреби в довіреній третій стороні.

1.3 Криптовалюта

Web3 і криптовалюта дійсно мають тісний зв'язок. В даний час криптовалюта є досить популярним та відомим явищем, але багатьом людям все ще складно зрозуміти його суть. Я намагатимусь пояснити вам основні поняття криптовалюти.

Криптовалюта є цифровою валютою, яка базується на технології блокчейн. Вона відрізняється від звичайних фіатних валют, таких як гривня або долар, оскільки не має центрального органу, який контролює її вартість. Замість цього, вартість криптовалюти визначається спільнотою користувачів та власників, які активно взаємодіють у криптовалютному середовищі в Інтернеті. Криптовалютою можна розраховуватися за товари та послуги, якщо це підтримується відповідними постачальниками. Однак, сьогодні більшість людей, які мають криптовалюту, використовують її переважно як інвестиційний інструмент, а не для повсякденних платежів.

1.3.1 Токени

Токени є спеціальними об'єктами, що виникають на платформах зі смарт-контрактами, таких як Ethereum. Вони дозволяють користувачам створювати, випускати і взаємодіяти з цими токенами, які виникають на основному блокчейні. Токени мають широке застосування в різних галузях, не обмежуючись тільки блокчейн-технологіями. У загальному сенсі, токен - це одиниця обліку, що може бути розглянута як спеціальна нотатка в певній інформаційній системі. Криптотокени, зокрема, є записами спеціального типу в блокчейні. Вони відрізняються від популярних криптовалют тим, що їх архітектура базується на блокчейнах інших криптовалют, наприклад, Ethereum або Solana. Криптотокени можна розглядати як цифрову реалізацію цінних паперів або інших активів.

1.4 Смарт-контракти

Смарт-контракт - це угода, яка оформлена у вигляді комп'ютерного коду і може бути укладена, змінена або розірвана тільки за допомогою відповідної комп'ютерної програми. Ці угоди стають все більш популярними, оскільки спрощують життя їх учасників шляхом автоматизації процесів. Смарт-контракти базуються на технології блокчейну, яка дозволяє здійснювати транзакції без посередництва фінансових установ. Тому сторонам смарт-контракту необхідно вибрати середовище для укладання такої угоди. Зазвичай цим середовищем є Ethereum.

Смарт-контракт - це складна угода, яка включає різні компоненти для свого належного функціонування. На додаток до середовища, в якому укладається угода, смарт-контракт має такі "реквізити":

- Сторони контракту - це учасники, які зобов'язуються виконувати умови угоди.

- Активи - це предмети, які підлягають обміну або перетворенню за угодою.

- Умови договору - це правила, за якими сторони зобов'язуються діяти і обмінюватись активами.

- Джерела зовнішньої інформації - це джерела, які надають додаткову інформацію для виконання умов контракту. Наприклад, вони можуть постачати дані про ціни товарів або фактичну виконану роботу.

Створення смарт-контракту вимагає певних навичок програмування, оскільки кодування алгоритму дій є одним із етапів. Наприклад, смарт-контракт може визначати, що коли одна сторона заплатить певну суму криптовалюти

іншій стороні, то виконуватимуться певні дії або активи будуть передані. Смарт-контракти можуть мати різні форми, включаючи такі як "сейф", де доступ до активів може бути обмежений до певної дати.

Цікавим прикладом застосування смарт-контрактів є їх використання в онлайн-продажах, таких як покупка одягу або техніки через інтернет-магазини. У цьому випадку, умови договору купівлі-продажу будуть встановлюватися у смарт-контракті. Коли ви зробите замовлення, оплата за товар буде фіксуватися в блокчейні, а кошти будуть заблоковані. Після того, як ви отримаєте своє замовлення і підтвердите його доставку або відповідність, сума буде автоматично перерахована на рахунок продавця.

Такий підхід за допомогою смарт-контрактів може суттєво спростити процес торгівлі, особливо якщо в контракті враховуються стандарти або специфікації товарів, а також передбачаються штрафи за доставку некондиційної продукції. Правильно сформульовані умови договору можуть забезпечити інтереси обох сторін, забезпечуючи безпеку і довіру в процесі онлайн-продажів.

2. ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН

2.1 Напрямки застосування блокчейну

З блокчейном технологія поступово проникає в нові галузі діяльності, підкреслюючи свої переваги порівняно з іншими рішеннями. Одним з найпоширеніших застосувань блокчейну до цього часу є ведення обліку криптовалютних активів. Багато державних та комерційних організацій вже почали тестувати або впроваджувати блокчейн для своїх потреб. Блокчейн привертає нових прихильників завдяки своїм перевагам у порівнянні з іншими технологіями. Основною перевагою блокчейну є його децентралізоване сховище даних, що робить його майже невразливим до втрати або пошкодження даних при великій кількості вузлів. Крім того, блокчейн забезпечує високий рівень захисту даних.

2.2 Криптовалюти та фінансовий сектор

Криптовалюти стали першими проектами, що використали блокчейн-технологію. Внаслідок численних криз і конфліктів людство почало шукати альтернативні способи зберігання своїх заощаджень, що призвело до загальної недовіри до банків і фінансових установ. Поява криптовалют на ринку викликала великий інтерес. Капіталізація криптовалют швидко зросла і досягла обсягів, що перевищують щорічний ВВП розвинутих країн. Багатьох привабила ідея відсутності централізованого органу, який контролює обіг валют.

Серед переваг використання криптовалют порівняно з банками можна виділити такі: доступність цілодобово, фіксовані комісії незалежно від місцезнаходження, швидка обробка транзакцій, збереження анонімності, простота використання з будь-якого пристрою з підключенням до Інтернету, відсутність централізованого сервера з користувачами даних і неможливість відхилити транзакцію залежно від обставин. У порівнянні з банками, де

банкрутство може статись, а валюта певної країни може швидко втратити вартість, криптовалюти зазвичай не прив'язані до конкретної території. Проте вони також не є стабільними, і тому були створені стейблкоїни - криптовалюти, прив'язані до резервів звичайної валюти або певних товарів, таких як дорогоцінні метали або нафта. Курс стейблкоїнів змінюється в залежності від активу, до якого вони прив'язані.

2.3 Охорона здоров’я

Багато організацій у сфері охорони здоров'я вже використовують технологію блокчейн для збереження даних своїх пацієнтів та медичних записів. Ця технологія дозволяє зашифрувати дані за допомогою публічних та приватних ключів, забезпечуючи доступ до записів лише обмеженій групі користувачів. Пацієнти можуть надавати свій приватний ключ лише тим особам, яким дозволено переглядати їх приватну інформацію. Використання блокчейну дозволяє забезпечити надійне зберігання медичних записів, гарантуючи їх незмінність та доступність усім лікарям, які обслуговують пацієнта. Це допомагає уникнути помилок та непорозумінь між лікарями, а також забезпечує пацієнтів тим, що їхні дані захищені від хакерських атак та можливого зловживання. Багато проектів вже успішно впроваджують цю технологію в медичній сфері.

2.4 Реєстри прав власності, договори

Використання блокчейну для фіксації прав власності особи над майном є дуже цікавим і доцільним рішенням. В першу чергу, безпека збереження даних важлива, оскільки втрата цих даних може призвести до втрати права власності на майно. Блокчейн забезпечує надійну імутабельність всіх записів, зроблених від початку функціонування мережі. Це означає, що зловмисники не зможуть шахрайським шляхом заволодіти чужим майном. Навіть у разі атаки на один з

вузлів, інтегритет та доступність мережі не будуть порушені. Використання блокчейну для фіксації прав власності забезпечує надійність та захищеність власності особи, спрощує процес доведення права власності та запобігає можливим спробам шахрайства.

2.5 Ланцюги поставок

Використання ланцюгів поставок може суттєво зменшити поширення хвороб і збитки, пов'язані з ними, а також забезпечити відстеження походження товару та його шляху. В даний час виявлення партій продуктів, які постачаються невеликими підприємствами або фермерами, є складною задачею. У разі виявлення небезпечних або інфікованих продуктів одним отримувачем практично неможливо вилучити ці продукти з інших місць реалізації. Шляхом розробки системи відстежування, такої як та, що розробляється IBM (International Business Machines Corporation) та Walmart, можна швидко відслідковувати "погані" товари та подавати сигнали про необхідність їх вилучення. Наприклад, ресторан або магазин, які отримали партію товару, що спричинила недуги у покупців, за допомогою блокчейн-системи можуть швидко відслідковувати цю партію товару, ідентифікувати дистриб'ютора та постачальника цих продуктів. Якщо товар дійсно пошкоджений, постачальник отримає відмітку, і всі, хто купував такі товари або мав з ними пов'язані дії, отримають повідомлення про небезпеку. Крім того, цю систему можна використовувати для позначення продуктів, які мають мітки "органічні", "вибір року" або інші, щоб підтвердити їх валідність.

2.6 Державний сектор

Використання блокчейну у сфері державного управління має широкі можливості і застосування. Наприклад, Американський центр контролю захворювань розглядає можливість використання блокчейну для збереження інформації про випадки важких або заразних хвороб, таких як гепатит, COVID-19 та інші. Якщо один штат виявляє випадок захворювання, то інші штати мають бути негайно повідомлені, щоб прийняти необхідні заходи для захисту населення. Це дозволяє краще контролювати поширення захворювань, швидко обмежувати дії осіб в зонах інфекційних спалахів.

Таке використання блокчейну дозволяє поліпшити систему моніторингу та реагування на захворювання, сприяє ефективній координації між різними медичними організаціями та урядовими структурами. Важливою перевагою є безпека і незмінність даних у блокчейні, що дозволяє надійно зберігати і передавати медичну інформацію без ризику втрати чи зміни.

Міністерство внутрішньої безпеки США визначило 16 галузей критичної інфраструктури, таких як енергетика, транспорт, медицина, фінанси та інші. Безперервна робота цих систем є критично важливою, оскільки навіть коротка перерва в їх функціонуванні може призвести до серйозних економічних збитків або небезпеки для людей.

Використання блокчейну є особливо ефективним у цих галузях і вже широко використовується. Наприклад, в серпні 2019 року Міністерство енергетики США розробило проект "Енергетичний інтернет" на основі блокчейну. Цей проект дозволяє власникам будинків придбати електроенергію від розподілених джерел, таких як вітряні ферми. Ця платформа сприяє кращому регулюванню споживання енергії, де споживачі можуть вибирати найкращий час для використання електроенергії залежно від її ціни. Чим більший попит, тим вища ціна. Проект вже співпрацює з провідними постачальниками та дослідницькими центрами, а всі учасники мережі можуть в режимі реального часу відслідковувати рівень витрат енергії та доступність енергетичних ресурсів.

Цікавим проектом, який отримує підтримку від японського Міністерства охорони довкілля, є система виміру та обміну відновлюваної енергії, побудована

на блокчейн-технології. В рамках цього проекту використовується криптовалюта для створення системи обміну, де енергія конвертується в обмінну валюту. Ціна встановлюється на основі попиту та ціни передачі енергії.

Також в Малакці, малайзійському місті, планується створення блокчейн-міста майбутнього. В цьому місті будуть розташовані розкішні готелі, вілли з видом на море, шале та водні атракціони. Першим кроком у реалізації цього проекту буде запуск власної криптовалюти DMI, яка буде використовуватися для оплати послуг. Туристи також матимуть змогу обмінювати свою валюту на DMI-монети та здійснювати платежі за допомогою телефонів або комп'ютерів. Прогнозується, що це інноваційне блокчейн-місто зможе приймати близько трьох мільйонів туристів щороку.

У 2018 році двадцять дві країни Європейського Союзу підписали документ, що розглядає потенціал використання блокчейну для перетворення електронних сервісів у Європі. За останніми даними, в ці проекти вже було інвестовано близько 350 мільйонів євро. Експерти Європи вважають, що всі громадські сервіси мають майбутнє, пов'язане з блокчейном, оскільки це забезпечить громадянам впевненість у захисті та надійності їх персональних даних.

У Естонії була розроблена широка платформа з онлайн доступом до ідентифікаційних даних, медичної інформації та "держави в смартфоні". Близько 99% медичних даних оцифровано і доступно з будь-якого пристрою. Всі ці дані зберігаються у блокчейні.

Грузія та Швеція впровадили систему реєстрації прав власності на землю та продажу нерухомості на основі блокчейну, що призвело до зменшення корупції у цій сфері.

Мальта використовує блокчейн для збереження студентських дипломів, шкільних табелів та нагород, що сприяє збереженню приватності особистих даних, зменшенню бюрократії та полегшенню доступу до ресурсів.

Україна також впроваджує блокчейн через платформу "Дія" для збереження критично важливих даних. Уряд уклав угоду з американською

компанією BitFury у 2017 році для переходу державних реєстрів на блокчейн, що спрощує реєстрацію фізичних осіб та підприємств. Міністерство аграрної політики також представило оновлений земельний кадастр на блокчейні, що полегшує роботу підприємців.

Багато інших країн, включаючи бідні держави Африки та Близького Сходу, також долучаються до використання блокчейну. Це свідчить про широкий спектр застосування цієї технології у сферах, що мають стратегічне значення для держави, забезпечуючи доступність, надійність та безпеку даних.

3. РОЗРОБКА ВЕБ-З ЗАСТОСУНКУ НА ПРИКЛАДІ МАРКЕТПЛЕЙСУ

3.1 Використані технології

Angular - це фреймворк для розробки веб-додатків, який створено компанією Google. Він дозволяє розробникам побудувати потужні односторінкові додатки з високою продуктивністю та масштабованістю.

Основні особливості Angular:

1. Використання TypeScript: Angular використовує мову програмування TypeScript, що дозволяє писати більш безпечний та структурований код.

2. Компонентна архітектура: Angular базується на компонентній архітектурі, де додаток розбивається на незалежні компоненти, які включають шаблони HTML, стилі CSS та логіку. Це сприяє розширюваності та повторному використанню компонентів.

3. Директиви: Angular має вбудовані директиви, які дозволяють змінювати вміст та поведінку компонентів на основі даних або стану додатку.

4. Сервіси та залежності: Angular використовує механізм сервісів та залежностей для обміну даними та функціональністю між компонентами. Це спрощує управління залежностями та сприяє створенню багаторазових сервісів.

5. Роутинг: Angular надає можливість налаштовувати роутинг, що дозволяє переходити між сторінками додатку без перезавантаження сторінки.

Angular є потужним фреймворком, який використовують великі компанії та розробники по всьому світу для створення веб-додатків різного масштабу та складності. Він надає зручні інструменти та практики для розробки якісних та ефективних додатків. У своєму застосунку я використовував Angular для написання фронтенд-частини.

Node.js - це виконавче середовище JavaScript, яке дозволяє розробникам створювати серверні додатки та мережеві сервіси. Воно ефективно використовує ресурси та асинхронну модель програмування для обробки багатьох запитів одночасно. Node.js також надає широкий вибір модулів та пакетів для розширення функціональності додатків. Завдяки активній спільноті розробників і підтримці, Node.js є популярним інструментом для побудови швидких та масштабованих веб-додатків. У своєму застосунку я використовував Node.js для написання бекенд-частини.

MongoDB - це система керування базами даних з моделлю даних NoSQL, яка є потужним, гнучким та масштабованим інструментом. Вона призначена для зберігання, організації та обробки великого обсягу структурованих та неструктурованих даних. MongoDB володіє гнучкою схемою, потужними інструментами пошуку, а також підтримкою агрегацій. Вона широко використовується в різних проектах, включаючи веб-додатки, аналітичні системи та проекти з обробки великих обсягів даних , завдяки своїй ефективності та масштабованості. А також ця база даних найкраще себе показує у комбінації з Node.js тому я обрав саме її.

Solidity - це мова програмування, спеціально призначена для створення розумних контрактів на блокчейн-платформі Ethereum. Вона має схожий синтаксис з мовами програмування, такими як JavaScript, що дозволяє легше вивчати та використовувати її розробникам. Solidity використовується як важливий інструмент для розробників, які працюють з Ethereum та блокчейн-технологіями.

Goerli - це одна з тестових мереж Ethereum, яка була запущена з метою тестування і розробки додатків на базі блокчейну Ethereum без витрат реальних

коштів і ризику втрати Ether. Додатки, які успішно пройшли тестування на мережі Goerli, можуть бути безпечно впроваджені на основну мережу Ethereum. На мережу Goerli я деплоїв свій смарт контракт.

3.2 Моделі бази даних

У моєму застосунку я використовую дві моделі бази даних, і це моделі User та Wallet, у моделі User є такі поля як:

- email – email користувача
- username – username користувача
- firstName - ім’я користувача
- lastName - прізвище користувача
- password - пароль користувача
- sugar - внутрішня умовна валюта

У той час як у моделі Wallet є поля:

- type - що відповідає типу гаманця
- name - що відповідає назві гаманця
- address - що відповідає цифровій адресі гаманця
- userId - що відповідає id юзера якому належить цей гаманець

3.3 Бекенд

Як вже згадувалось раніше, для бекенду я обрав мову програмування Node.js. Я скористався фреймворком Express.js, який надає простий спосіб створення сервера та визначення маршрутів для обробки HTTP-запитів.

У моєму застосунку є auth контроллер(див. рис. 3.1), який відповідає за авторизацію, тобто реєстрацію та логін користувачів. Після реєстрації або логіну генерується jwt токен, який в подальшому буде надсилатись у хедері кожного

запиту з фронтенд сторони застосунку аби уникнути шахрайства та підтвердити аутентифікацію користувача.

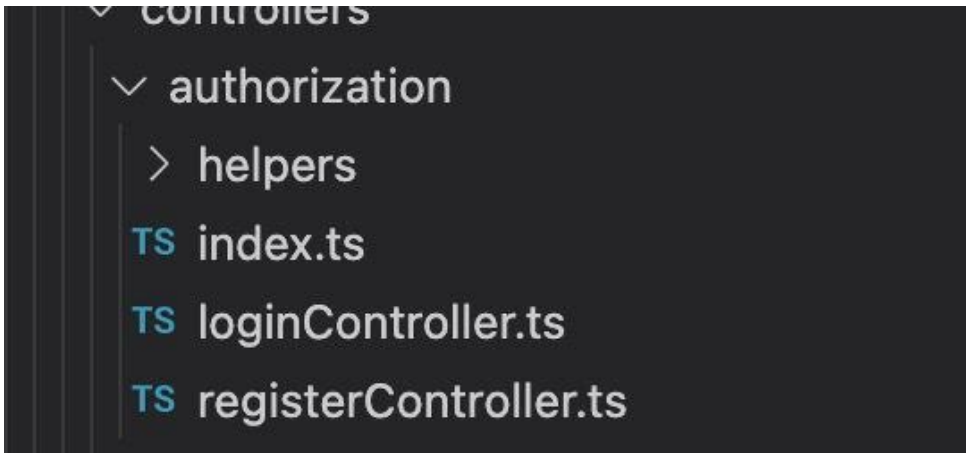

Рисунок 3.1 auth контроллер

Також присутній user контроллер(див. рис. 3.2) завдяки якому ми можемо отримати дані про користувача щоб правильно відображати його username sugar wallet та інші поля моделі.

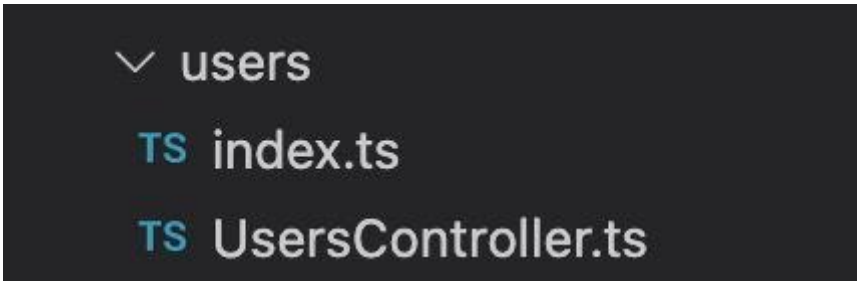

Рисунок 3.2 user контроллер

І останнім контроллером є wallet контроллер(див. рис. 3.3), він відповідає за додавання та видалення рахунку користувача.

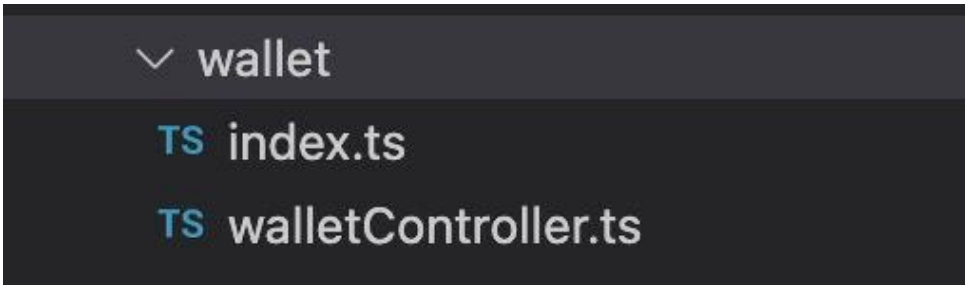

Рисунок 3.3 wallet контроллер

Але найважливішою частиною мого бекенду є contract сервіс(див. рис. 3.4), який нараховує баланс відповідно до транзакції яка поступила на розумний контракт, в ньому є чотири варіанти його роботи, якщо транзакція рівна нулю то зарахування не відбудеться, якщо транзакція рівна 5.0 USDT - нараховано буде 1000 умовної валюти, 10.0 USDT – 2500 умовної валюти та 20.0 USDT – 5000 умовної валюти.

```
export const TransferListener = async (): Promise<void> => {
  const provider = new ethers.providers.WebSocketProvider(process.env.GOERLI_NODE_URL);

  logger.log(await provider.getBlockNumber());

  const contract = new ethers.Contract(contractAddress, abi, provider);

  contract.on("*", async (from) => {
    const [data] = await contractRepo.findFirst<Prisma.UserFindFirstArgs>({
      where: {
        wallets: {
          some: {
            address: from.args[0],
          },
        },
      },
      select: {
        id: true,
        sugar: true,
      },
    });

    switch (formatUnits(from.args[2]._hex, 18)) {
      case "5.0":
        addSugar(data, 1000);
        break;
      case "10.0":
        addSugar(data, 2500);
        break;
      case "20.0":
        addSugar(data, 5000);

        break;
    }

    logger.log(JSON.stringify(data));
  });

  provider.on("block", (el) => logger.log(el));
};
```

Рисунок 3.4 contract сервіс

Смарт контракт(див. рис. 3.5) як було зазначено вище я написав мовою Solidity. У цьому контракті створюється токен USDT (Tether) на основі вбудованого контракту ERC20PresetFixedSupply з OpenZeppelin. Імпортується

контракт ERC20PresetFixedSupply з бібліотеки OpenZeppelin. Цей контракт надає зручний спосіб створити ERC20-токен з фіксованою постачальністю.

Контракт має приватну змінну supply, яка вказує загальну кількість токенів USDT, що буде випущена. Значення цієї змінної встановлюється на 213,000,000,000 USDT .

Контракт має конструктор, який викликає конструктор базового контракту ERC20PresetFixedSupply. В конструкторі передається ім'я токену ("SWAP Token"), символьний код ("USDT"), загальна постачальність токену та адреса, яка стає власником всіх токенів (адреса виконавця транзакції, яка розгортає контракт).

Цей контракт створює ERC20-токен USDT з фіксованою постачальністю і надає можливість взаємодіяти з ним, включаючи передачу токенів, отримання балансу тощо.

Після цього я деплою (див. рис. 3.6) смарт контракт по адресі на рисунку 3.7.

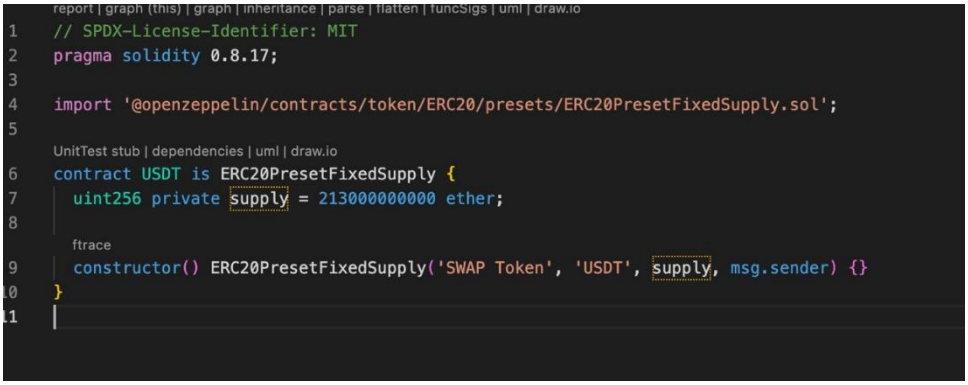

Рисунок 3.5 Смарт контракт

```
import { ethers } from 'hardhat';
import { USDT_CONTRACT } from '../../../libs/lib-api-interface/src';

async function main() {

  const Lock = await ethers.getContractFactory('Staking');
  const lock = await Lock.deploy(USDT_CONTRACT);

  await lock.deployed();
}

// We recommend this pattern to be able to use async/await everywhere
// and properly handle errors.
main().catch((error) => {
  console.error(error);
  process.exitCode = 1;
});

```

Рисунок 3.6 Деплой смарт контракту

```
lib-api-interface > src > lib > constants > TS USDT_CONTRACT.ts > ...
export const USDT_CONTRACT = '0x43053b996A4905A0ba461dCc7aA332A0b1cba050';
```

Рисунок 3.7 Адреса за якою буде задеплоєний смарт контракт

3.4 Фронтенд частина

Для фронтенд частини свого застосунку я використовував фреймворк Angular, мовою розмітки є html а для запису стилів я обрав scss.

На рисунку 3.8 зображена сторінка реєстрації у якій є шість полів, таких як firstname, lastname, username, email, password, confirm password.

Рисунок 3.8 Сторінка реєстрації

На рисунку 3.9 зображена сторінка логіну у якій є два поля: email та password.

Рисунок 3.9 Сторінка логіну

Після того як користувач авторизується він буде направлений на основну сторінку застосунку (див. рис. 3.10). Ця сторінка представляє з себе маркетплейс фотографій які є у наявності, якщо користувач захоче дізнатись інформацію про фото та його ціну він може натиснути на нього та перед ним відкриється модальне вікно як на рисунку 3.11. Фото має свою рідкість дату створення категорію та ціну.

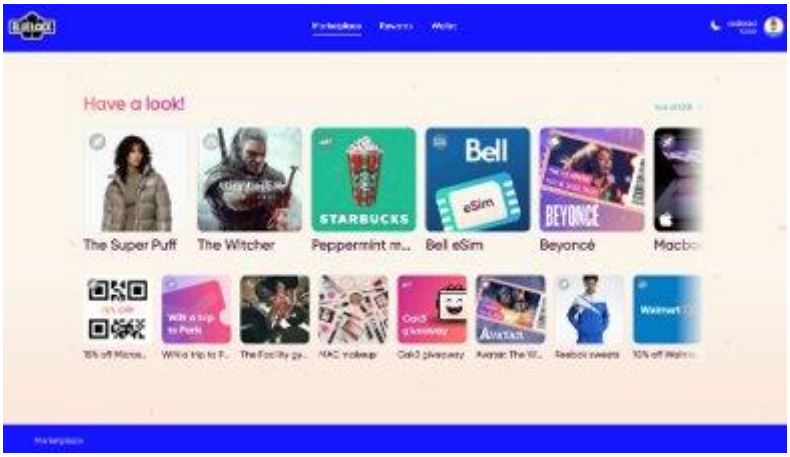

Рисунок 3.10 Основна сторінка

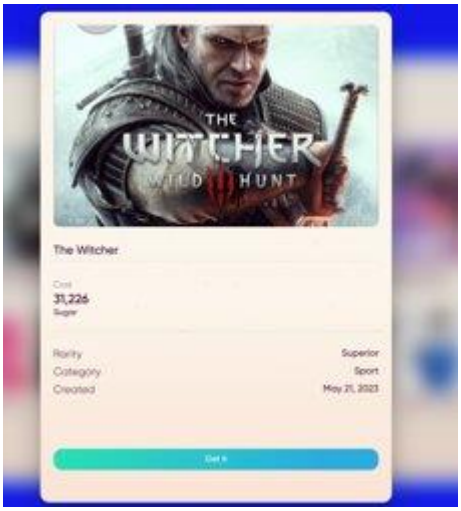

Рисунок 3.11 Модальне вікно з інформацією про фото

Щоб отримати внутрішню умовну валюту в першу чергу користувачу потрібно завантажити розширення для браузера - Metamask і після цього додати Metamask гаманець.

MetaMask - це популярний криптовалютний гаманець та розширення для веб-переглядачів, яке дозволяє користувачам взаємодіяти з децентралізованими додатками на блокчейні Ethereum. Він надає зручний інтерфейс для управління криптовалютними активами та здійснення транзакцій на блокчейні без необхідності використовувати повноцінні Ethereum-клієнти.

На фронтенд частині щоб підключити Metamask гаманець я відслідковував події Metamask і якщо розширення надавало доступ до гаманця - я додавав його у гаманці у застосунку. Це можна помітити на рисунку 3.12.

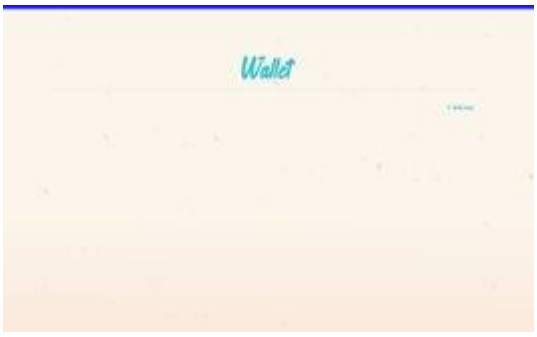

Рисунок 3.11 Сторінка з гаманцем

Рисунок 3.11 Модальне вікно з вибором гаманця

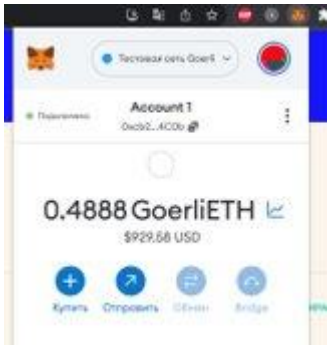

Рисунок 3.12 Браузерне розширення Metamask

Рисунок 3.12 Модальне вікно з обраним гаманцем

Тепер, коли користувач додав гаманець він може натиснути на кнопку додати і він буде направлений на сторінку де він зможе вибрати яку кількість умовної валюти він хоче купити(див. рис. 3.13), є три варіанти це 1000, 2500 та 5000 одиниць умовної валюти.

Коли користувач обирає один із запропонованих варіантів перед ним з’являється сторінка з вибором методу оплати (див. рис. 3.14).

Обравши метод оплати користувач буде направлений на сторінку підтвердження транзакції (див. рис. 3.15) де після її підтвердження буде нарахована умовна валюта.

Рисунок 3.13 Сторінка з вибором кількості умовної валюти для купівлі

Рисунок 3.14 Сторінка з вибором методу оплати

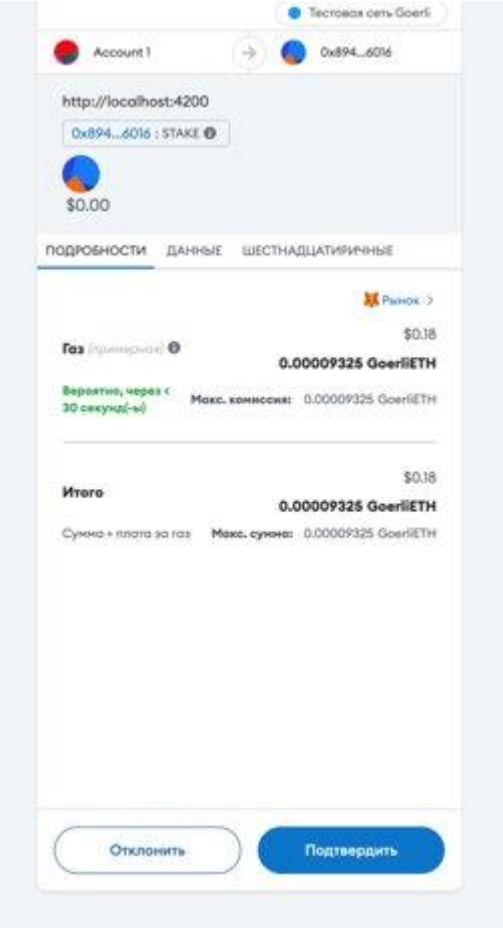

Рисунок 3.15 Сторінка Metamask з підтвердженням транзакції

Отож, умовна валюта була нарахована та звіт по транзакції можна переглянути на онлайн ресурсі goerli.etherscan. Тепер у користувача достатньо умовної валюти і він може обрати фото для покупки. Для цього потрібно у хедері вибрати вкладку “rewards” і користувач буде направленій на сторінку на якій знаходяться всі фото (див. рис. 3.16), фото подіяються на “у наявності” та “немає у наявності”, після покупки фото під назвою “Macbook Pro” як можна помітити на рисунку 3.17, фото змінило свій статус на “немає в наявності”.

Рисунок 3.15 Умовні одиниці були нараховані

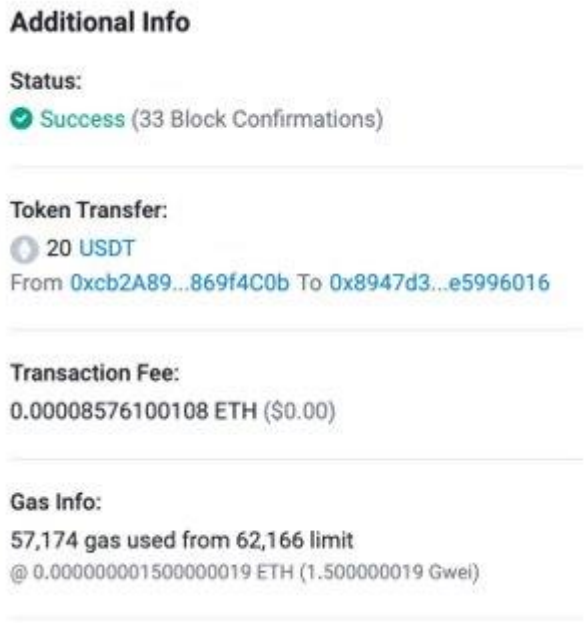

Рисунок 3.15 Звіт по транзакції взятий з goerli.etherscan

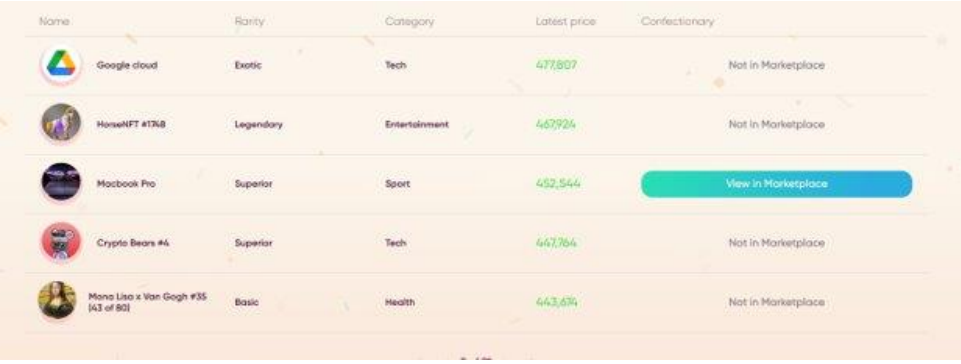

Рисунок 3.15 Сторінка rewards

Рисунок 3.16 Предмет більше не є у наявності

ВИСНОВКИ

У сучасному цифровому світі розробка застосунків з використанням веб 3 технологій стає все більш актуальною. Веб 3 технології, такі як блокчейн та розумні контракти, надають нові можливості для розробки інноваційних та безпечних додатків.

Розробка застосунків на основі веб 3 технологій дозволяє створювати додатки, які не залежать від централізованих організацій і мають покращену прозорість, безпеку та надійність. Використання блокчейну дозволяє забезпечити безпеку та недоступність для змін даних, а розумні контракти забезпечують автоматизовану виконавчу логіку без посередництва.

Основною перевагою веб 3 технологій є їхній потенціал для революції в різних галузях, таких як фінанси, логістика, охорона здоров'я, громадська безпека та багато інших. Розробники, які мають глибоке розуміння веб 3 технологій, можуть використовувати їх для створення інноваційних та ефективних рішень, які задовольняють потреби сучасного цифрового суспільства.

Однак, розробка застосунків з використанням веб 3 технологій також вимагає додаткових знань та розуміння специфіки цих технологій. Розробники повинні бути готові до викликів, пов'язаних з безпекою, масштабованістю та інтеграцією з існуючими системами.

Загалом, розробка застосунків з використанням веб 3 технологій відкриває нові перспективи для інновацій та розвитку сучасного цифрового світу. Знання та вміння розробників у цих технологіях стають ключовими для успіху у цьому швидкозмінному і перетворюваному середовищі.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Angular documentation [Електронний ресурс] – Режим доступу: https://angular.io/docs
2. Node.js documentation [Електронний ресурс] – Режим доступу: https://nodejs.org/en/docs
3. MongoDB documentation [Електронний ресурс] – Режим доступу: https://www.mongodb.com/docs/
4. Web3.js documentation [Електронний ресурс] – Режим доступу: https://web3js.readthedocs.io/en/v1.10.0/
5. Information about blockchain [Електронний ресурс] – Режим доступу: https://www.blockchain.com/
6. Smart contracts information [Електронний ресурс] – Режим доступу: https://www.investopedia.com/terms/s/smart-contracts.asp
7. Ethereum documentation [Електронний ресурс] – Режим доступу: https://ethereum.org/en/developers/docs/
8. Metamask [Електронний ресурс] – Режим доступу: https://metamask.io/