КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій
(факультет)

Управління проєктами
(кафедра)

ПОЯСНЮВАЛЬНА ЗАПИСКА ДО АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ НА ЗДОБУТТЯ ОСВІТНЬОГО РІВНЯ «БАКАЛАВР»

на тему: **«Розробка інформаційної системи з управління криптовалютними активами в інтернет-середовищі»**

Пасічник Марія Сергіївна
(прізвище, ім’я та по батькові студента повністю)

Київ 2024 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій
(факультет)

Управління проєктами
(кафедра)

ЗАТВЕРДЖУЮ
Завідувач кафедри УП
Бушуєв С.Д.
_____

„ ___” _____2024 року

ПОЯСНЮВАЛЬНА ЗАПИСКА ДО АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ НА ЗДОБУТТЯ ОСВІТНЬОГО РІВНЯ «БАКАЛАВР»

на тему: «Розробка інформаційної системи з управління криптовалютними активами в інтернет-середовищі»

Пасічник Марія Сергіївна
(прізвище, ім’я та по батькові студента повністю)

Виконала : студентка 4-го курсу, групи ІСТ-УП-41.

Спеціальності: 126 «Інформаційні системи та технології».
(шифр і назва напряму підготовки, спеціальності)

Освітньо-професійна програма: «Управління проєктами» Пасічник М.С
(прізвище та ініціали)

Керівник проф. Веренич О.В. .
(прізвище та ініціали)

Рецензет _____.
(прізвище та ініціали)

Київ 2024 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: Автоматизації і інформаційних технологій.
Кафедра: Управління проєктами.
Освітній рівень: «бакалавр за ОПП».
Спеціальність: 126 «Інформаційні системи та технології».
Освітньо-професійна програма: Управління проєктами.

ЗАТВЕРДЖУЮ
Завідувач кафедри УП
Бушуєв С.Д.
_____

„ ___” _____2024 року

З А В Д А Н Н Я
ДО ВИКОНАННЯ АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО РІВНЯ «БАКАЛАВР»

Пасічник Марія Сергіївна_

1. Тема роботи: «Розробка інформаційної системи з управління криптовалютними активами в інтернет-середовищі"»»
затверджена наказом ректора КНУБА № 357/2 від «15» 02 2024 р.
2. Керівник роботи: Веренич Олена Володимирівна професор кафедри управління проєктами.
3. Строк подання студентом роботи до захисту: червень 2024 року .
4. Зміст пояснювальної записки за розділами:
Р.1. Аналіз предметної області та постановка задачі.
Р.2. Розробка інформаційного забезпечення.
Р.3. Розробка програмного забезпечення.
Р.4. Управління проєктом розробки.

6. Календарний план виконання АВР

Види робіт та їх зміст	Дата виконання
Р.1. Аналіз предметної області та постановка задачі	Лютий 2024 р.
Р.2. Розробка інформаційного забезпечення	Березень 2024 р.
Р.3. Розробка програмного забезпечення	Квітень 2024 р.
Р.4. Управління проєктом створення веб-сайту	Травень 2024 р.
Остаточне оформлення роботи	Червень 2024 р.
Попередній захист роботи на кафедрі	Червень 2024 р.

7. Консультанти розділів АВР

Розділ	Прізвище, ініціали та посада консультанта, представника комісії	дата	підпис

8. Дата видачі завдання: 15 лютого 2024 року

Керівник _____ Олена ВЕРЕНИЧ
(підпис) (ім’я та прізвище)

Бакалавр _____ Марія ПАСІЧНИК
(підпис) (ім’я та прізвище)

АНОТАЦІЯ

Пасічник М.С. Розробка інформаційної системи з управління криптовалютними активами в інтернет-середовищі.

Атестаційна випускна робота бакалавра за освітньою програмою: «Управління проєктами», спеціальності: «Інформаційні системи та технології». – Київський національний університет будівництва і архітектури. – Київ, 2024.

Робота спрямована на розробку крипто-гаманця, що поєднує в собі можливості крипто-валютних та фіатних транзакцій через інтеграцією з API – Binance, 0xpay, LiqPay, SMART-contract . Крипто-гаманець створює зручне та безпечне середовище для управління цифровими активами, дозволяючи користувачам здійснювати перекази, обмін та зберігання різних видів валют.У реалізації даного проекту використовуються сучасні технології та мови програмування, що включають React TypeScript, REDUX, Fastify, PostgreSQL.

Ключові слова: Fiat, SMART-contract, WEB3, Binance, crypto, 0xpay, Fastify, криптовалюта, банк, Blockchain, транзакції, TypeScript, Fastify, Etherum, blockchain, LiqPay, PostgreSQL, ETH, BTC, TRON, MATIC, ZK-Rollups, Etherum, .

SUMMARY

Pasichnyk M.S. Development of an information system for managing cryptocurrency assets in the online environment.

Bachelor's thesis for the degree of Bachelor of Science in the educational program: "Project Management", specialty: "Information Systems and Technologies". - Kyiv National University of Construction and Architecture. - Kyiv, 2024.

The work is aims to develop a crypto wallet that combines the capabilities of cryptocurrency and fiat transactions through integration with APIs - Binance, 0xpay, LiqPay, SMART-contract. The crypto wallet creates a convenient and secure environment for managing digital assets, allowing users to make transfers, exchange and store different

currencies. The implementation of this project uses modern technologies and programming languages, including React TypeScript, REDUX, Fastify, PostgreSQL.

Keywords: Fiat, SMART-contract, WEB3, Binance, crypto, 0xpay, Fastify, cryptocurrency, bank, Blockchain, transactions, TypeScript, Fastify, Etherum, blockchain, LiqPay, PostgreSQL, ETH, BTC, TRON, MATIC, ZK-Rollups, Etherum,ZK-Rollups

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ ТА ТЕРМІНІВ

NSTX – Nexus Secure Token and crypto keeper (власна назва). Nexus – зв'язок, різних криптовалют та токенів в одному гаманці. STX скорочено від S.T.A.C.K (Secure token and crypto keeper) – надійне зберігання токенів та валют .

MVP – minimal viable product (мінімально життєздатний, з мінімально необхідним функціоналом продукт).

ПЗ – програмне забезпечення.

СУБД – система управління базами данних.

DAPPS – децентралізована система, що створена на blockchain – протоколах таких як Etherum, або з застосуванням SMART контрактів.

SMART-contract (SMART контракт) – це діджитал контракт . програмний код, що зберігається в Blockchain.

Base – Blockchain 2 рівня (L2) для розробки на його основі фінансових додатків, торгівлі на децентралізованих біржах (DEX), розгортання кредитних сервісів та випуску токенів (NFT).

DEX – це тип криптовалютної біржі, яка працює без центрального керування.

Web3 – концепція за основу якої взято використання (dApps), смарт-контракти криптовалют.

P2P – в контексті криптовалют і Blockchain, P2P відноситься до способу передачі цифрових активів або даних безпосередньо між учасниками мережі.

Hot wallet – гарячий гаманець.Це криптовалютний гаманець, який підключений до Інтернету.

Ledger Nano X – фізичний, “холодний криптогаманець” для зберігання та управління цифровими активами.

Trezor – це апаратний криптогаманець, який використовується для безпечного зберігання криптовалют.

DeFi (Decentralized Finance) – це концепція фінансових систем, яка функціонує без посередників, таких як банки або фінансові інститути, за допомогою смарт-контрактів на блокчейн-платформах.

Cold wallet – Холодний гаманець - це криптовалютний гаманець, який не підключений до Інтернету, що робить його більш безпечним для зберігання великих сум криптовалют.

TPS – (transactions per second), пропускна здатність до обробки транзакцій.

Offchain – оффчейн-протокол, що обробляє транзакції поза Blockchainом.Виконуються на рівні L2.

HMAC (Hash-Based Message Authentication Code) – метод що використовує хеш-функцію разом з секретним ключем для створення коду аутентифікації повідомлення

SHA-256 (Secure Hash Algorithm 256-bit) – хеш функція, що перетворює дані будь-якої довжини у фіксований 256-бітний хеш. Забезпечу цілісності даних та створення цифрових підписів у Blockchain-системах.

2FA (2 Factor Auth) – вид аутентифікації користувача який вимагає два незалежних способи підтвердження особи користувача.

ВСТУП

В атестаційній випускній роботі (АВР), буде розглянуто актуальність та можливості управління фінансовими активами в онлайн середовищі. З розвитком інформаційних технологій, розвивається цифрова економіка та можливості для зберігання та управління фінансами, як традиційними (фіатними), так і цифровими (криптовалютами).

Фіатні активи – це звичайні гроші, такі як долар чи євро, які використовуються щоденно для розрахунків в інтернет середовищі та реальному світі. Криптовалюта на відміну від фіатних активів, існує виключно в цифровому вигляді і в своїй основі використовує криптографію для захисту транзакцій. Криптографія дозволяє проводити операції та перевіряти цифрові активи без залучення банків чи інших посередників. Це означає, що можна безпечно обмінюватися грошима напряму між користувачами. У цифровій економіці це має велике значення, оскільки дозволяє значно знизити витрати на комісії з переказів, пришвидшити транзакції і підвищити рівень безпеки та конфіденційності користувачів.

Цифрова економіка відрізняється тим, що в ній фінансові операції здійснюються переважно в електронному вигляді, часто без фізичного контакту між учасниками. Без посередників таких як банки, операції можуть відбуватися миттєво, незалежно від географічного положення користувачів. Це забезпечує нові можливості для бізнесу та клієнтів.

В рамках атестаційної роботи було проведено проектування та розробку онлайн криптогаманця, який поєднує в собі можливості транзакцій в криптовалютних та фіатних активах. Фіатні активи будуть розглянуті виключно у вигляді цифрових активів. В рамках проекту передбачається реалізація можливості обміну криптовалют та фіатних коштів за декількома напрямками – трансфер, переказ, депозит, кредитування. Ця функціональність надасть користувачам розгорнутий функціонал та зручність у використанні онлайн криптогаманця, дозволяючи їм легко конвертувати свої цифрові активи з одного типу в інший.

Завдяки інтеграції з API провідних платіжних систем 0xpay, PayPal та інтеграції даних з Binance біржі, користувачі зможуть ефективно та безпечно здійснювати фінансові операції. Мета роботи розробка проекту інформаційної системи з управління криптовалютними активами в інтернет-середовищі.

Об’єктом дослідження є процеси з управління цифровими криптовалютними та фіатними активами в інтернет середовищі. До цих процесів відносяться наступні об’єкти :

1. Фіатні активи які використовуються для повсякденних розрахунків в електронному вигляді. Вони підлягають регулюванню центральних банків та фінансових установ.

2. Криптовалюти – цифрові активи, що використовують криптографічні методи для забезпечення безпеки транзакцій та підтвердження власності. Найвідомішими прикладами є Bitcoin та Ethereum.

3. Інтернет середовище – веб-платформи, мобільні додатки та інші цифрові сервіси, що надають можливість управління фінансовими активами.

Предметом дослідженн є технології та методи, що будуть використанні для розробки онлайн криптогаманця. Для досягнення мети проекту необхідно виконати наступні завдання:

1.Проаналізувати сучасний стан та перспективи розвитку онлайн криптогаманців.

2.Спроектувати архітектуру онлайн криптогаманця.

3. Обрати технологію для розробки системи. Проаналізувати та обрати відповідні технології для розробки онлайн криптогаманця. Описати переваги використання TypeScript, React, Fastify, та Vite.

4. Створити модулі для обробки транзакцій з криптовалютами та фіатними активами.Забезпечити інтеграцію з API платіжних систем 0xPay, PayPal та біржі Binance.

5. Інтегрувати Ethereum Blockchain та смарт-контракти для забезпечення безпеки та прозорості транзакцій. Інтегрувати ZK-Rollups для підвищення масштабованості та зниження вартості транзакцій.

6. Створити зручний та інтуїтивно зрозумілий інтерфейс для користувачів.

7. Забезпечити функціональність для реєстрації, авторизації, перегляду балансу та здійснення транзакцій.

8. Запуск та підтримка системи. Налаштувати механізми підтримки та оновлення системи.

РОЗДІЛ 1 АНАЛІТИЧНИЙ ОГЛЯД. ПОСТАНОВКА ЗАВДАННЯ

1.1 Актуальність теми

Із швидким розвитком інформаційних технологій, цифрова економіка та сфера фінансів також набули змін. Глобальна мережа Інтернет, полегшила обмін інформацією та ведення торгівлі без врахування географічних кордонів. Зростання глобальної торгівлі та міжнародних транзакцій вимагає швидких та ефективних способів оплати, що популяризує онлайн транзакції, та робить їх привабливими та перспективними для багатьох бізнесів та клієнтів, особливо у сферах електронної комерції та онлайн послуг.

Завдяки цьому клієнти все частіше звертаються до послуг онлайн-банкінгу, електронних платіжних систем та криптовалютних платформ. Криптовалютні гаманці є невід'ємною частиною Інтернет середовища, забезпечуючи можливість зберігання, передачі та обміну цифрових активів. Визначальною особливістю криптовалют є те, що вони, як правило, не випускаються центральними органами влади, що робить їх теоретично несприйнятливими до державного втручання чи маніпуляцій.

Криптовалюта — це форма цифрових активів, заснована на Blockchain – (децентралізований цифровий реєстр, спільна база данних, що спільно використовується вузлами комп’ютерної мережі). Найголовніша перевага Blockchain — неможливість зміни чи видалення даних. Дані в ньому пов'язані між собою за допомогою криптографії у блоках, і це означає що введені дані не підлягають видаленню чи змінам. Для Bitcoin транзакції реєструються у загальнодоступний розподілений реєстр – Blockchain, дані по вартості транзакцій доступні для перегляду будь-кому, проте особисті дані учасників транзакцій не викриваються. Це робить криптовалютні операції більш прозорими, та привабливими для тих країн, що мають нестабільну економіку та обмеженний доступ до традиційних фінансових послуг. Крипто гаманці, транзакції яких

засновані на Bitcoin - обробляються в рази швидше за традиційні банківські перекази, мають низькі комісії та децентралізовану структуру.

За даними компанії Chainalysis 2023 Crypto Crime [16], у 2023 році було втрачено понад $3.2 млрд через атаки та недостатню безпеку криптовалютних гаманців. Із аналізу Elliptic - The State of Bitcoin 2022 [8] близько 20% всього Bitcoin на разі є недоступними через втрату приватних ключів, що використовуються для безпеки крипто гаманця в якості шифрування та паролю. Також для багатьох користувачів криптовалютні гаманці є складними у використанні. Опитування CoinGecko показало, що 40% користувачів вважають їх занадто складними у використанні.

Більшість криптогаманців не підтримують всі типи криптовалют, або не можуть інтегруватись з іншими сервісами.

Створення криптогаманця що використовує Blockchain у фінансовій сфері, підкріплюється зазначеними дослідженнями та статистичними даними, які демонструють значні проблеми в сфері безпеки, зручності використання та інтероперабельності криптовалютних гаманців. Ці проблеми потребують вирішення, що надасть можливість широкому колу користувачів безпечно та зручно використовувати криптовалютні гаманці, сприяючи розвитку цифрової економіки.

1.2 Аналіз існуючих криптогаманців

Серед діючих криптогаманців, що націлені на управління фінансовими активами, існує декілька типів рішень зі збереження фінансів. Кожен тип має свої переваги та недоліки, які впливають на вибір певних криптогаманців в залежності від потреб користувачів. Серед них криптогаманці поділяються на гарячі (підключені до Інтернету) та холодні (не підключені на постійній основі), а також апаратні та програмні.

Hardware wallet (апаратний гаманець) – це фізичний пристрій, спеціально розроблений для безпечного зберігання приватних ключів криптовалюти. На відміну від програмних гаманців, які зберігаються на комп'ютері або смартфоні,

апаратні гаманці зберігаються в автономному режимі, що робить їх більш стійкими до злому.

Лідерами ринку серед таких гаманців є Ledger Nano X [13] та Trezor [19]. Дослідження компаній Ledger і Trezor [20] показують ефективність апаратних рішень для забезпечення безпеки приватних ключів. У звітах та статтях, опублікованих цими компаніями, наведені конкретні приклади використання їх продуктів.

Всі апаратні гаманці є холодними гаманцями, але не всі холодні гаманці є апаратними. Апаратні гаманці пропонують додатковий рівень зручності та безпеки порівняно з іншими типами холодних гаманців, але вони також дорожчі.

Cold wallet (холодний гаманець) – це криптовалютний гаманець, який не підключається до інтернету і не взаємодіє з будь-якими смарт-контрактами. Багато холодних гаманців підтримують широкий спектр криптовалют, що робить їх зручними для зберігання різних активів. Більшість холодних гаманців надають резервні фрази, які можна використовувати для відновлення ваших приватних ключів у разі втрати або пошкодження пристрою.

Hot wallet (гарячий гаманець) – це тип криптовалютного гаманця, що напряму постійно підключений до Інтернету. Hot wallet може бути веб-гаманцем, мобільними додатком або програмою на комп'ютері.

Функціонал включає зберігання, відправку та отримання фінансів швидко та зручно. Проте транзакції можуть бути вразливими до онлайн-атак, що може призвести до викрадення коштів.

Таблиця 1.1

Порівняння “гарячих” та “холодних” гаманців

	Гарячі гаманці	Холодні гаманці
Ціна	Безкоштовні для користувачів; Криптогаманці інколи платять комісію за збережені на них криптовалюти	Вартість пристрою 50 - 300 $
Використання	Для онлайн торгівлі	Тривале зберігання коштів
Кібербезпека	Оскільки вони підключені до Інтернету, вони потенційно можуть бути вразливі до злому	Надійні. Захищені від кібератак , але можуть бути фізично втрачені
Захист від втрат активів	Мають можливості відновлення та резервного копіювання, і до них можна отримати доступ із кількох пристроїв	Більшість із них мають варіанти відновлення та резервного копіювання втраченого пароля, але не для втраченого пристрою.
Зручність виконання платежів	Гарячі гаманці легко доступні, оскільки гаманець уже підключений до Інтернету	Холодні гаманці потребують додаткового кроку для підключення до Інтернету через USB, Wi-Fi або QR-код

Із широко використаних у цифровому середовищі лідерами ринку серед “гарячих гаманців” є Exodus Web3.0 Wallet та MetaMask. “Холодні гаманці” є також розповсюдженими серед клієнтів, проте перевага надається більше “гарячим гаманцям”. Онлайн криптогаманець який планується створити, є саме “гарячим гаманцем”, основною метою якого є забезпечення зручності та швидкого доступу до коштів для щоденних операцій. Гарячі гаманці дозволяють миттєво здійснювати транзакції та взаємодіяти з різними сервісами та додатками, що є важливим для активних користувачів криптовалют.

Таким чином, для проекту онлайн криптогаманця, основний акцент робиться на використання гарячих гаманців через їхню зручність та функціональні можливості, які задовольняють потреби цільової аудиторії.

1.2.1 Exodus Web3.0 Wallet

Криптогаманець заснований на мережі Base, Etherum. Base – L2 Blockchain, що працює поверх Etherum, тому транзакції та інші фінансові операції в даній мережі набагато швидші та дешевші ніж операції на базовому рівні Etherum. Etherum (ETH) – Blockchain-платформа для децентралізованих додатків, та друга за капіталізацією криптотвалюта. Велика кількість проектів у сфері DeFi та NFT [18] побудована саме на основі цієї платформи.

DeFi (Decentralized Finance) – це концепція фінансових систем, яка функціонує без посередників, таких як банки або фінансові інститути, за допомогою смарт-контрактів на блокчейн-платформах. DeFi дозволяє користувачам надавати та брати позики, обмінювати активи, страхуватися та виконувати інші фінансові операції безпосередньо один з одним, використовуючи децентралізовані платформи.

NFT (Non-Fungible Token) – це унікальний цифровий актив, який представляє собою право власності або доказ автентичності для конкретного об'єкта або контенту, такого як мистецтво, музика, відео, ігрові предмети тощо. На відміну від

криптовалют, які є взаємозамінними (фунгібельними), кожен NFT є унікальним і не може бути обміняний на інший рівнозначний токен. NFT використовуються для створення і торгівлі унікальними цифровими активами в різних індустріях, особливо в сфері мистецтва і розваг.

L2 – класифікація технології Blockchain, що характеризується на її більшій масштабованості, доступності та безпеці. L2 – протокол, вдосконалений варіант мереж нижчого рівня таких, як L0 та L1. Основна ціль – розвантажити базовий Blockchain із частини транзакцій, знизити саме таке навантаження та підвищити загальну ефективність. Це також надає доступ до криатовалют без івисоких комісій і затримок. Blockchain рівня L2 обробляє транзакції швидше, ніж Blockchain рівня L1, і замість них повертає результати обробки даних у Blockchain L1, що значно пришвидшує процес. Всі операції проводяться в рази швидше та ефективніше.

Перевагами криптогаманця Exodus є простота в інтеграції із веб-браузерами та мобільними платформами. Є можливість підключення Exodus до апаратного гаманця Trezor для підвищення заходів безпеки. Має функціонал трейдингу – купівлі криптовалютних активів та їх перепродажу на біржі, з метою заробітку на різниці в ціні за певний період часу.

За даними CoinGecko [4], на початку 2024 року кількість користувачів Exodus становила понад 10 мільйонів осіб. За звітом компанії Exodus, у період з січня по березень 2024 року обсяг транзакцій через гаманець зросла на 25%. Мережа Base має не повну підтримку в гаманці, а саме відображає лише відправлені транзакції, і для отримання повної історії необхідно безпосередньо відвідувати Base за адресою вашого рахунку.

1.2.2 MetaMask

MetaMask це браузерний криптогаманець побудований на базі технології Ethereum і підтримує активи, пов’язані з цією мережею. За даними опитування, проведеного DappRadar [8] у 2023 році, користувачі високо оцінили можливості MetaMask для взаємодії з децентралізованими додатками, але висловили незадоволення складністю додавання нових мереж. Для роботи з іншими EVM - мережами, користувачі вручну повинні їх додати в налаштуваннях.

MetaMask не підтримує Bitcoin, що є проблемою для багатьох, хто хотів б зберігати всі свої криптовалюти в одному гаманці. MetaMask використовує Ethereum і пов’язані з Ethereum мережі. На даний момент MetaMask підтримує лише кілька мереж, і лише активи, доступні в цих мережах, можна зберігати на цьому крипто-гаманці. В цей перелік включені Solana, Cardano, XRP, Litecoin, Bitcoin, Polkadot. MetaMask отримує високі оцінки за функціональність та інтеграцію з dApps, але критично оцінюється за відсутність підтримки різних Blockchainів та мереж.

Не сумісний з EVM. Для того щоб ресурс, по оплатам підтримувався на MetaMask, він повинен бути сумісний із віртуальною машиною Ethereum. Це обмеження ускладнює інтеграцію з іншими Blockchain. Захист даних у криптогаманці MetaMask відбувається за допомогою пароля та коду фрази. Якщо клієнт втрачає фразу пароль від гаманця, що складається з 12 слів, MetaMask не зможе відновити вам доступ до нього. Із недоліків - стягує комісію, не на пряму а за допомогою third-part сервісів, комісія яких становить від 1-5% від суми транзакції.Це може бути значною витратою, особливо при великих обсягах операцій.

MetaMask є непоганим варіантом криптогаманця для взаємодії з криптоактивами та децентралізованими додатками але має низку обмежень і проблем, що можуть стати причиною втрати клієнтів із часом, і втрати однієї з лідерських позицій на ринку.

1.3. Огляд області застосування криптовалютних гаманців

Область застосування криптовалюти та криптовалютних гаманців доволі широка та потребує більш детального розгляду. В багатьох сферах життя, що повязані із цифровими активами, криптовалютні гаманці стають невід'ємною частиною глобальної фінансової екосистеми. Основні аспекти використання онлайн криптогаманців та впливу, підкріплені останніми статистичними даними і трендами наведено далі.

Криптовалютні операції, такі як обмін та перекази залежать від стейблкоінів (stablecoins). Стейблкоїн (Stablecoin) – це тип криптовалюти, вартість якої прив'язана до стабільного активу, такого як фіатна валюта (наприклад, долар США, євро) або товар (наприклад, золото). Основна мета стейблкоїнів – зменшити волатильність, яка характерна для більшості криптовалют, забезпечуючи стабільнішу вартість для користувачів.

Вартість фіат-забезпечених стейблкоїнів прив'язана до фіатної валюти, яка зберігається як резервний актив. Прикладом є USDT (Tether) [17], який підтримується резервами доларів США. Криптовалютно-забезпечені стейблкоїни підтримуються іншими криптовалютами як резервний актив. Наприклад, DAI забезпечений криптовалютою Ether (ETH).

Стейблкоїни є важливими для цифрової економіки, оскільки вони дозволяють користувачам уникнути високої волатильності традиційних криптовалют, зберігаючи переваги швидких і дешевих транзакцій, що забезпечуються блокчейн-технологією.

У 2023 році стейблкоїни (stablecoins), такі як USDT, показали значне зростання в кількості платіжних транзакцій, перевищивши Bitcoin у другій половині року, згідно з даними Chainalysis [5]. Загальний обсяг торгівлі криптовалютами у 2023 році досяг $36.6 трлн, зі значним збільшенням активності в останньому кварталі завдяки очікуванню на ETF для Bitcoin, за даними CoinGecko.

У 2023 році стейблкоїни (stablecoins), такі як USDT, показали значне зростання в кількості платіжних транзакцій, перевищивши Bitcoin у другій половині року, згідно з даними Chainalysis []. Загальний обсяг торгівлі криптовалютами у 2023 році досяг $36.6 трлн, зі значним збільшенням активності в останньому кварталі завдяки очікуванню на ETF для Bitcoin, за даними CoinGecko [5].

ETF – (exchange trading fund) єдиний біржовий інвестиційний фонд, акціями якого торгують на біржі, ціна його привязана до певної криптовалюти. Той хто володіє ETF, інвестує в портфель фонду проте не володіє активами напряму.

В Україні заблоковані перекази між валютними та на валютні картки, тому перекази в криптовалюті дозволять швидко та з низькими комісіями переказувати кошти між країнами без участі традиційних банківських систем, уникаючи проблем, пов'язаних з валютними обмеженнями, затримками обробки транзакцій, високими банківськими комісіями та валютним контролем [23].

Інвестори використовують криптовалюти для захисту своїх активів від інфляції або нестабільності фіатних валют. Користувачі, що займаються трейдингом на криптовалютних біржах можуть купувати та продавати криптовалюти для отримання прибутку від коливань курсів. Криптовалютні гаманці часто мають вбудовані функції для відстеження вартості активів та управління інвестиціями та трейдингу. Bitcoin виріс на 155.2%, а Ethereum на 90.5% у 2023 році, відображаючи сильну довіру інвесторів та поширення - CoinGecko[4].

Кількість бізнесів, що приймають криптовалютні платежі, залишилася стабільною, при цьому деякі компанії повідомляють про значну частку своїх продажів через криптовалютні транзакції. Наприклад, Hostinger бачить майже чверть своїх продажів через криптоплатежі повідомляє Best Bitcoin & Crypto Payment Processor [21].

1.4 Основні проблеми

Користувачами криптовалютного гаманця можуть бути як клієнти, що діють в особистих інтересах, так і бізнеси. Серед індивідуальних клієнтів це переважно люди віком від 25 до 45 років, як чоловіки, так і жінки.

Вони цікавляться інвестуванням, технологіями та фінансовою незалежністю. Для них важливі безпека, конфіденційність, швидкість і простота у використанні.

Серед бізнесів користувачами криптовалютних гаманців можуть бути компанії, які займаються електронною комерцією та іншими секторами, що використовують або приймають криптовалютні та фіатні платежі. Для них критично важлива безпека транзакцій, універсальність у підтримці різних криптовалют, а також надійність і стабільність роботи системи. Основні потреби обох груп клієнтів включають гарантію безпеки активів, підтримку різних криптовалют і Blockchainів, інтуїтивно зрозумілий інтерфейс, стабільність роботи гаманця, низькі та прозорі комісії, легкість інтеграції з популярними децентралізованими додатками та можливість додавання нових функцій у майбутньому.

Однак існують певні проблеми при використання клієнтами криптогаманців. Загрози хакерських атак та шахрайство ставить під питання збереження приватних ключів і доступу до криптогаманця. Недостатня підтримка різних криптовалют у MetaMask та Exodus гаманцях призводить до зменшення кількості клієнтів. Складність налаштування та використання деяких гаманців, а також недостатньо зручний інтерфейс є перешкодою. Нестабільна робота гаманців, що може призвести до втрати доступу до активів, і високі комісії за транзакції, які часто не зрозумілі користувачам, також є значними проблемами.

Діаграма причинно-наслідкових зв'язків (діаграма Ісікави), що зображує потенційні проблеми та наслідки для нового криптовалютного гаманця, показує, що розробка гаманця з урахуванням п'яти ключових аспектів може значно покращити його прийняття та ефективність. Важливі аспекти включають покращену безпеку з двофакторною аутентифікацією (2FA) та біометричною ідентифікацією, розширену

універсальність для підтримки більшої кількості Blockchain і криптовалют, простий інтерфейс, надійність та прозорість з низькими комісіями за транзакції. Діаграма Ісікави – наведена на рисунку 1.1 (див.додаток 6).

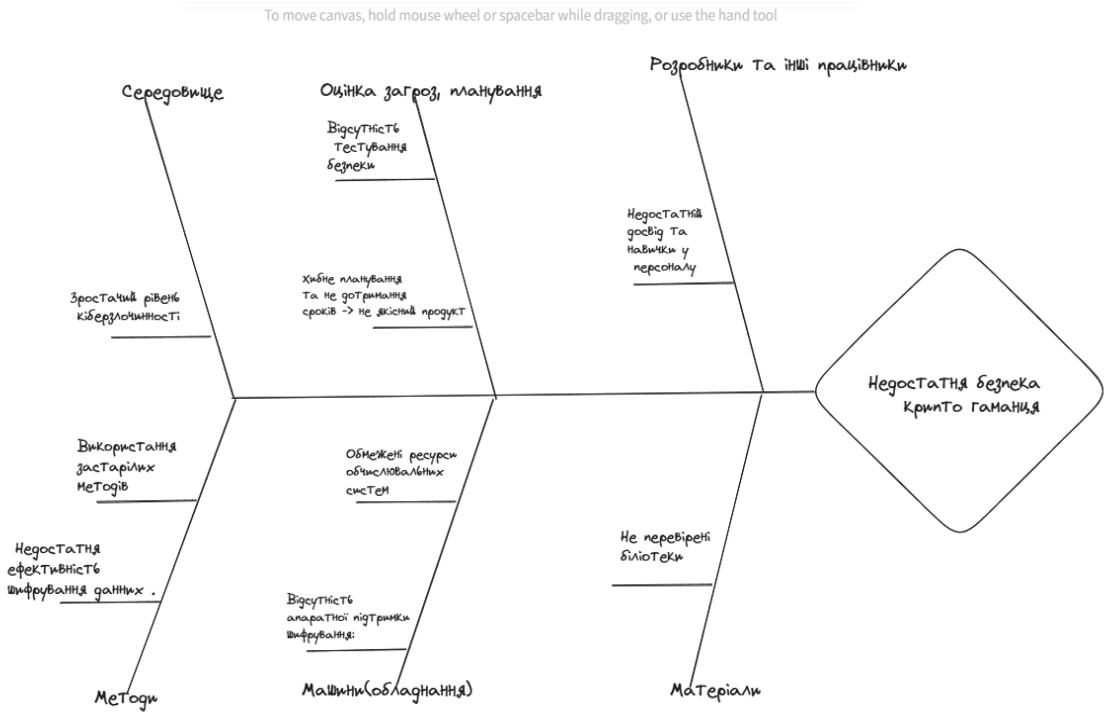


Рисунок 1.1 Діаграма Іссікави

Розробка нового криптовалютного гаманця який буде відповідати сучасним вимогам безпеки, універсальності та простоти використання, є актуальною та перспективною задачею та він буде кращим завдяки наступним пунктам :

1. Покращеній безпеці - 2FA аутентифікації, біометричної аутентифікації.

2. Розширеній універсальності - підтримка більшої кількості Blockchainів і криптовалют.

3. Простому інтерфейсу - інтуїтивно зрозумілий як для новачків, так і для досвідчених користувачів.

4. Високій надійності

5. Прозорими та низькими комісіям за транзакції.

Зараз криптовалюти та цифрові гаманці стали невід'ємними у різних фінансових операціях, від платежів і торгівлі до DeFi та NFT. За статистичними

даними та дослідженнями, Exodus і MetaMask займають лідируючі позиції в своїх категоріях, проте мають ряд недоліків. Опитування CoinGecko [4] також показало, що 40% користувачів вважають криптовалютні гаманці занадто складними у використанні.

Провівши дослідження та аналіз існуючих систем, є ряд факторів, що критично обмежують масове прийняття в повсякденне життя криптовалют, особливо серед нових користувачів. Відсутність підтримки різних криптовалют та інтеграції з іншими фінансовими сервісами створює додаткові перешкоди для користувачів. Дослідження, опубліковане в IEEE Access [9], підкреслює необхідність покращення інтероперабельності між Blockchain-системами та вирішення певних питань. Проблеми зручності та інтероперабельності можна вирішити забезпеченням інтуїтивно зрозумілого інтерфейсу та підтримкою більшої кількості криптовалют і платформ, ніж конкуренти.

Невизначеність щодо регуляторних вимог та правового статусу криптовалют у різних країнах також є значною перешкодою. Різні юрисдикції мають різні підходи до регулювання криптовалют, що може створювати правову нестабільність для користувачів та компаній.

Введення воєнного стану в Україні спричинило певні регуляторні зміни на фінансовому ринку, цим зумовивши ряд обмежень для здійснення міжнародних переказів та здійснення валютного обміну. Введено обмеження на купівлю віртуальних активів, сумою не більше 100 000 грн. на місяць. Дані обмеження поки не розповсюджуються на P2P операції або продаж криптовалют за фіатні кошти. Незважаючи на обмеження, криптовалюти є альтернативним способом проведення валютних обмінних та міжнародних операцій. Для уникнення проблем необхідно чітко визначити регуляторні рамки, щоб зменшити ризики та підвищити довіру користувачів.

Отже, для підвищення якості інтеграції в сучасний світ та функціональності криптовалютних гаманців необхідно зосередитися на покращенні зручності використання, забезпеченні високого рівня безпеки, вирішенні проблем

інтероперабельності та усуненні регуляторних невизначеностей. Це дозволить залучити більше користувачів та сприяти розвитку криптовалютної екосистеми.

1.5. Цілі проектування

Розробка інформаційної системи для збереження та управління цифровими активами передбачає розробку онлайн криптогаманця, який вирішить основні проблеми вже існуючих рішень серед криптогаманців. А саме криптогаманці MetaMask та Exodus не забезпечують одночасно високий рівень безпеки, універсальності та зручності використання, що обумовлює необхідність проектування нового, більш досконалого рішення. Складність використання, ненадійність, високі комісії та відсутність інтеграції з dApps підкріплюють необхідність створення нового рішення.

Дослідження з безпеки та зручності користування опубліковані в статтях Journal of Cryptology та IEEE Security & Privacy [29]. Документація Bitcoin [25], Ethereum, Solana та інших Blockchain-платформ [9], забезпечили більш детальний огляд технологій, що будуть використанні при подальшому проектуванні та розробці. Основна увага приділялася останнім дослідженням у галузі безпеки криптовалютних гаманців, методам шифрування, технологіям зберігання ключів та інтеграції з децентралізованими додатками (dApps).

Цілі проектування та розробки онлайн криптогаманця включають технічні аспекти безпеки, зручність використання, оптимізацію швидкості проведення операцій, підтримку інтроперабельності. Для вирішення цих проблем необхідно дослідити підходи, які зможуть забезпечити інтуїтивно зрозумілий інтерфейс та підтримку різних криптовалют і платформ. Двохфакторна аутентифікація (2FA) та біометричні методи є найбільш ефективними для захисту доступу до гаманців. Використання U2F ключів, також показують високу ефективність.Існуючі методи шифрування та аутентифікації можуть бути ефективно інтегровані в нові криптовалютні гаманці з метою підвищення їхньої безпеки.

Проект інформаційної системи з управління криптовалютними активами в інтернет-середовищі, а саме створення інтуїтивно зрозумілого та інтероперабельного додатку, який підтримуватиме різні криптовалюти та Blockchain-платформи. Онлайн криптогаманець має надати можливість оперувати

цифровими фінансовими активами через онлайн-інтерфейс з мобільних та стаціонарних пристроїв, забезпечуючи високий рівень безпеки та прозорості транзакцій.

1.6. Висновки до розділу 1

Проведений аналіз існуючих рішень і вивчення потреб цільових користувачів дозволили дійти до кількох важливих висновків. Процес розробки криптовалютного гаманця вимагатиме інноваційного підходу до безпеки, враховуючи зростання цифрових загроз. Важливим аспектом стане впровадження нових методів захисту даних та зберігання криптовалютних ключів, включаючи використання апаратних рішень та вдосконалених алгоритмів шифрування.

Крім того, ключовою є орієнтація на користувацький досвід, що передбачає створення простого у використанні інтерфейсу, який задовольнятиме потреби як новачків, так і досвідчених користувачів криптовалют. Проектування архітектури гаманця повинно враховувати масштабованість та адаптивність, забезпечуючи ефективне горизонтальне масштабування з урахуванням збільшення кількості користувачів та транзакцій.

Забезпечення відповідності регуляторним нормам є необхідним для легітимності та довіри користувачів до гаманця. Важливо також врахувати інтеграцію з децентралізованими екосистемами, що дозволить користувачам максимально використовувати можливості криптовалютних активів у сфері децентралізованих фінансів (DeFi).

Процес розробки включатиме проектування технічної інфраструктури, написання коду, тестування компонентів системи та впровадження механізмів захисту даних. Це дозволить створити надійний, безпечний та зручний інструмент для управління криптовалютними активами, який відповідатиме сучасним вимогам ринку.

РОЗДІЛ 2
ІНФОРМАЦІЙНЕ ТА МАТЕМАТИЧНЕ ЗАБЕЗПЕЧЕННЯ

2.1 Аналіз предметної області

Продуктом розробки є інформаційна система з управління фінансовими активами в інтернет середовищі. Для проектування проведемо дослідження ролі об’єктів в функціонуванні онлайн криптогаманця. Кожен з об’єктів впливає на загальну ефективність, безпеку та зручність. Проведення комплексного аналізу цих об'єктів дозволяє створити надійний та зручний онлайн криптогаманець, що відповідатиме потребам користувачів та регуляторним вимогам. Система має наступні інформаційні об’єкти :

Користувачі – є основними хто взаємодіє з криптогаманцем. Вони можуть бути індивідуальними користувачами або бізнесами, кожен з яких має свої специфічні вимоги та потреби. Їхні потреби та досвід користування визначають вимоги до системи. Дослідження користувачів допомагає зрозуміти, як забезпечити безпеку, зручність і функціональність гаманця.

Криптовалютні активи, такі як Bitcoin, Ethereum та інші токени, є основним об'єктом, яким користуються гаманці. Вивчення цих активів необхідне для розуміння механізмів їх зберігання, управління та транзакцій. Крім того, різні криптовалюти можуть мати різні технічні особливості та вимоги. Система повинна підтримувати різні криптовалюти, що визначає функціональність та привабливість гаманця.

Транзакції є основною функцією криптогаманця, оскільки користувачі здійснюють платежі, отримують кошти та виконують інші фінансові операції. Аналіз транзакцій дозволяє виявити вузькі місця у функціональності гаманця та підвищити ефективність обробки фінансових операцій.

Blockchain використовується для проведення транзакцій , і є також важливим аспектом. Він є розподіленим реєстром, який записує всі транзакції з криптовалютою та забезпечує прозорість та незмінність транзакцій.

Об’єкти дослідження :

1. Користувачі
2. Криптовалюти
3. Транзакції
4. Безпека
5. Blockchain

Система містить наступні інформаційні об’єкти (рис. 2.2) :

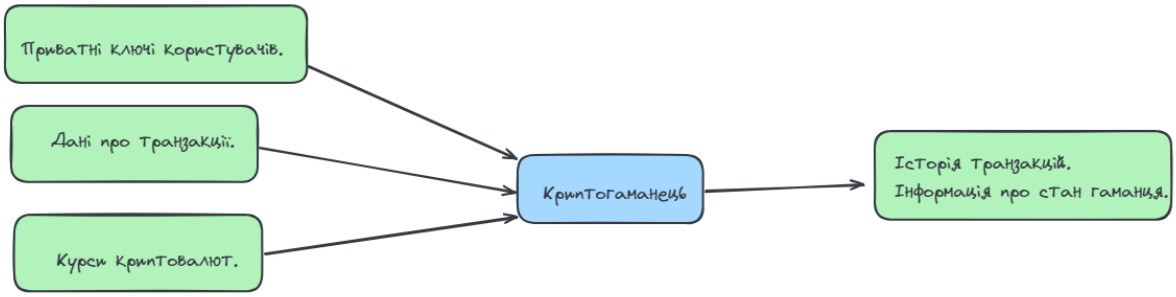


Рисунок 2.2. Діаграма вхідних та вихідних даних системи

Більш детальний огляд вхідних та вихідних даних системи наведено на в табл.2.2). Таблиця 2.2 (див.додаток 1) допоможе визначити чіткі обмеження на вхідні та вихідні дані, що забезпечить ефективне функціонування та безпеку системи криптогаманця на основі Blockchainy Ethereum.

На основі аналізу предметної області та визначених об'єктів дослідження (користувачі, криптовалюти, транзакції, безпека, Blockchain), спроектовано систему, яка забезпечуватиме ефективне, безпечне та зручне використання криптогаманця.

На основі таблиці 2.3 (див.додаток 2) здійснено моделювання контекстної діаграми функціонування криптогаманця, з можливостями проведення криптовалютних та фіатних транзакцій.

Кожен користувач може мати багато гаманців, але кожен гаманець належить лише одному користувачеві. (One-to-Many. User -> Wallet)

Кожен гаманець може мати багато транзакцій, але кожна транзакція належить лише одному гаманцю. (One-to-Many. Wallet -> Transaction)

Кожен користувач може бути стороною у багатьох транзакціях, але кожна транзакція має лише одного відправника і одного отримувача. (Many-to-Many. User <-> Transaction). Діграму даних відносин наведено на (рис.2.3)

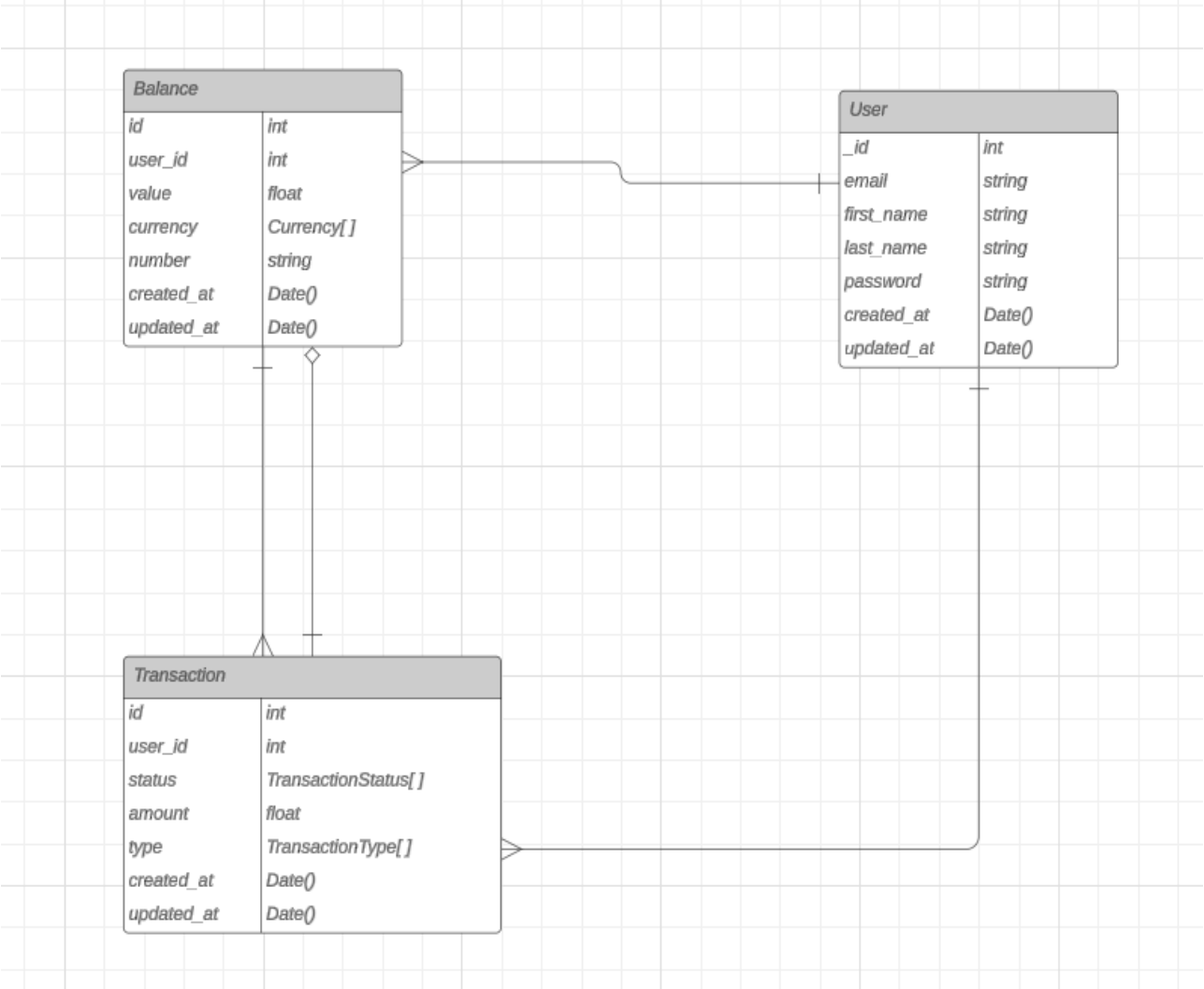


Рисунок 2.3 UML-діаграма класів

Діаграма прецедентів допомагає ідентифікувати різних акторів (користувачів, системи чи зовнішні системи), які будуть взаємодіяти з інформаційною системою. Наприклад, це можуть бути звичайні клієнти, адміністратори, платіжні системи або блокчейн-мережі.

Кожен прецедент або сценарій взаємодії (наприклад - "здійснення транзакції", "перегляд балансу", "додавання нового активу") дозволяє детально визначити, які саме операції повинна підтримувати система. Діаграма наведена на (рис.2.4).

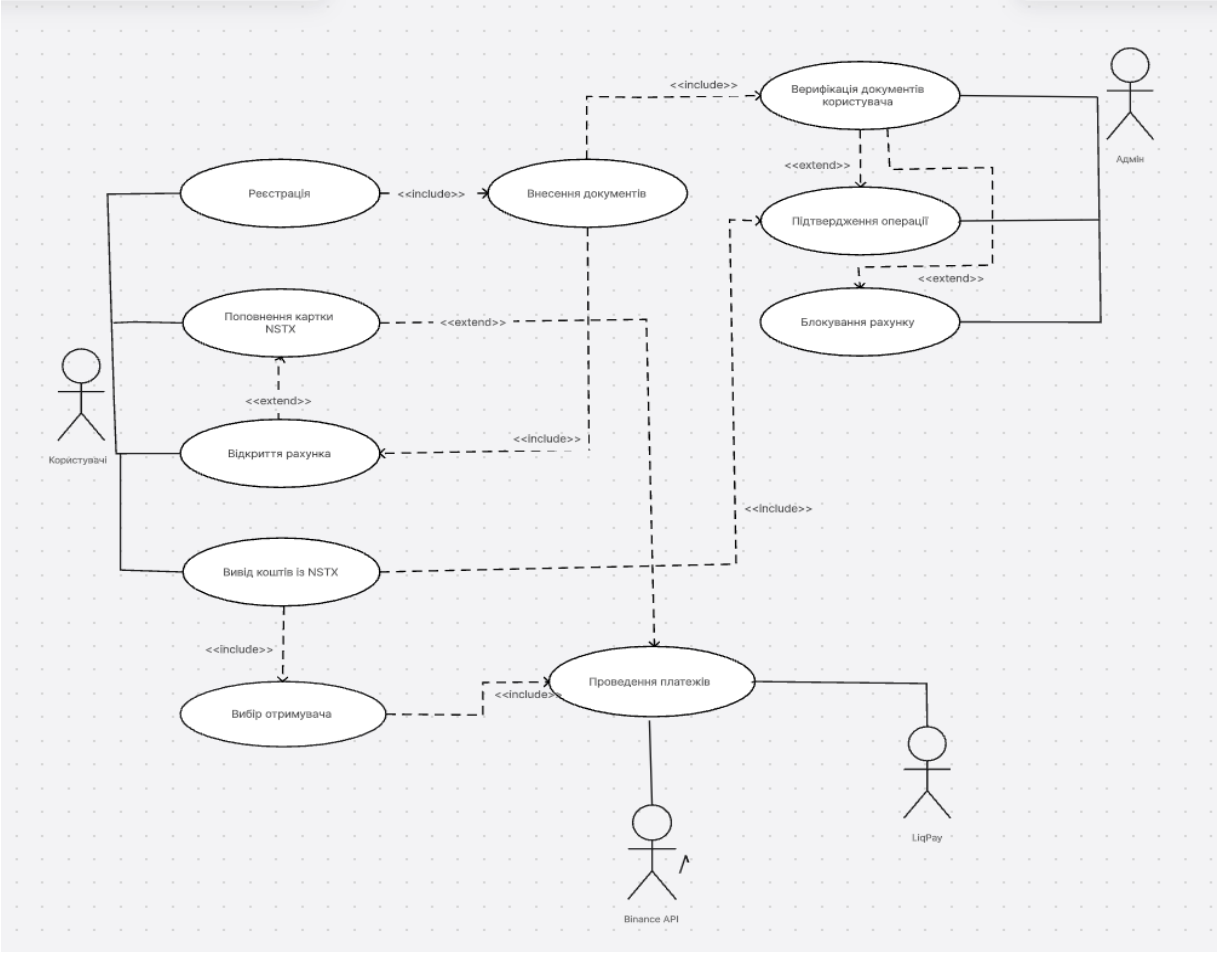


Рисунок 2.4 USE – CASE (діаграма прецедентів)

2.2 Проектування системи

Проектування системи включатиме в себе наступні етапи - визначення функціональних вимог , архітектуру системи, опис технологій, бізнес-логіку , що взаємодіють та безпосередньо мають вплив на якість та надійність системи.

2.2.1 Архітектура системи

Обираючи архітектуру для криптогаманця на основі Blockchainy Ethereum, важливо враховувати кілька ключових аспектів, таких як безпека, масштабованість, децентралізація та зручність використання для кінцевого користувача. Із попереднього аналізу відомо, що децентралізована архітектура дозволяє кожному користувачеві контролювати свої фінансові активи, оскільки приватні ключі зберігаються лише на пристрої користувача. Це зменшує ризик втрати коштів через атаки або порушення безпеки.

Згідно з дослідженням провідного інституту з безпеки даних, Symantec, децентралізовані мережі можуть зменшити ризики порушення безпеки. У своєму звіті Internet Security Threat Report 2022 [37], Symantec зазначає, що централізовані системи стають частішою мішенню для кібератак, тоді як розподілені системи мають більшу стійкість.

Використання смарт-контрактів у Blockchain дозволяє уникнути необхідності участі посередників у фінансових операціях, що забезпечує швидкість та надійність транзакцій.

Для розробки криптогаманця за основу було взято децентралізовану архітектуру (dApps). Так як криптогаманець на основі Blockchainy Ethereum має децентралізовану архітектуру, він є більш надійним та безпечним для зберігання та проведення цифрових транзакцій з криптовалютними та фіатними активами.

Створено дерево цілей що дозволяє чітко визначити та структурувати всі завдання, необхідні для успішної розробки криптогаманця. Кожна ціль має свої підцілі, які в свою чергу поділяються на конкретні завдання. Це допомагає краще

зрозуміти обсяг роботи, забезпечити послідовність у досягненні цілей і підвищити ефективність розробки проекту (рис. 2.6 , додаток 7).

2.3 Математичне та алгоритмічне забезпечення

Рішення, які будуть використані при розробці онлайн криптогаманця, обираються тільки після детального огляду функціонуючих систем, існуючих проблем та методів їх вирішення. Після цього проводиться аналіз технічних вимог до розроблюваного програмного забезпечення та вибір математичного й алгоритмічного забезпечення.

Математичне забезпечення в даному проекті включає алгоритми шифрування та захисту даних, які є фундаментальними для безпеки цифрових і криптовалютних активів.

Процес управління проєктом включає визначення завдань, планування ресурсів та контроль виконання кожного етапу. Функціональні вимоги до інформаційної системи збереження цифрових та криптовалютних активів повинні враховувати специфіку проекту, забезпечуючи ефективність та безпеку системи. Ось основні аспекти процесу управління проектом та ключові функціональні вимоги:

- Особистий кабінет користувача. Аутентифікація, створення облікового запису, зміна/відновлення паролю. Реєстрація за електронною адресою.

- Аутентифікація. Використання двухфакторної аутентифікації при вході і забезпечення надійноості конфіденційних та особистих даних. Вхід за електронною поштою вказаною при реєстрації.

- Відкриття нового рахунку, з можливістю вибору основної валюти. USDT \ USD\UAN.

- Real-time оновлення курсів валют.

- Поповнення рахунку гаманця за допомогою LiqPay.

- Переказ коштів та фіатних ресурсів. Можливість отримання переказів. Вибір шляху переказу – на інший рахунок у системі, чи на зовнішній рахунок.

- Обмін критовалют та фіатних коштів. Підтримка ринкових та лімітних замовлень для обміну.

- Шифрування конфіденційних даних користувачів.

- Взаємодія Blockchainом на основі Etherum через SMART-contract.

- Захист від SQL ін’єкцій та проникнення в БД.

- Надсилання деталей транзакцій на електронну пошту.

- Зберігання цифрових активів у електронному середовищі.

- Перегляд балансу.

- Історія транзакцій по кожному з відкритих рахунків користувача.

- Детальна інформація по кожній транзакції (час, сумма , тип , статус)

- Інтеграція з API Binance для отримання торгових даних, створеня трансферів .

- Інтеграція з API 0xpay для фіатних транзакцій.

- Інтеграція з API LiqPay для підтримки платіжних операцій.

Із даних по функціональних вимогам, які необхідні для системи, можна зробити аналіз та вибір математичного забезпечення, алгоритмів.

2.3.1 Etherum та L2 – рішення

Трилема масштабованості, відома також як трилема блокчейну, стверджує, що блокчейн-системи можуть досягти лише двох із трьох властивостей одночасно: масштабованості, безпеки та децентралізації. Розв'язання проблеми масштабованості є критично важливим для створення надійного та ефективного криптогаманця. Використання технологій Layer 2, шардінгу, інтеграція з іншими блокчейнами та вдосконалення смарт-контрактів є перспективними напрямками для досягнення цієї мети. Це дозволить забезпечити швидкі, безпечні та децентралізовані транзакції для користувачів криптогаманця.

Ось короткий огляд трилеми.

1. Масштабованість. Здатність обробляти велику кількість транзакцій у короткий час.
2. Безпека. Забезпечення захисту від атак і зловживань.
3. Децентралізація. Розподіл контролю над мережею між багатьма учасниками, що забезпечує відкритість і стійкість до цензури.

Розглянемо рішення необхідні для вирішення першого пункту із трилеми маштабованості криптогаманця.

А саме інтеграцію рішень L2, ціль яких полягає в тому, щоб впоратися з обмеженнями, пов'язаними з пропускною здатністю та часом обробки транзакцій у мережі Ethereum. Blockchain має проблему, яка полягає в тому, що складно й майже неможливо створити Blockchain-мережу, яка одночасно володіє трьома ключовими характеристиками. А саме створення одночасно швидкої, безпечної і децентралізованої мережі . Архітектура Blockchainів побудованих на основі Etherum та Bitcoin, з самого початку не розрахована на високу пропускну спроможність. TPS в Bitcoin – 15, у Etherum – 5-7. Перевага полягає в можливості переказувати активи між адресами L1 використовуючи при цьому "другий рівень", яким може бути як окремий Offchain-протокол, так і окремий Blockchain.

Рішення L2 дозволяють переказувати активи між адресами L1 швидше та дешевше, ніж це можливо на самому основному Blockchaini. Це робиться шляхом

обробки транзакцій поза основним Blockchainom, а потім запису їх в основний Blockchain лише для остаточного підтвердження. Рішення другого рівня можуть обробляти значно більше транзакцій, ніж основний Blockchain. Транзакції на другому рівні, як правило, підтверджуються значно швидше, ніж транзакції на основному Blockchaini.

Рішення другого рівня залежать від основного Blockchain, і якщо основний Blockchain буде зламано, це може вплинути і на рішення другого рівня. Проте рішення L2 є перспективним способом вирішення проблеми масштабування Blockchainy. Головною технологією level-2 є Технологія ZK-Rollups (Zero-Knowledge Rollups) - це метод масштабування Ethereum, який дозволяє значно зменшити витрати на операції та підвищити швидкість обробки транзакцій, залишаючи при цьому важливі принципи децентралізації і приватності. Основна ідея полягає в тому, щоб використовувати цифрові докази (zero-knowledge proofs) для перевірки правильності транзакцій без необхідності виконання всіх розрахунків на основному ланцюгу блоків Ethereum.

Переваги ZK-Rollup – витрати на Gas (операційні витрати) можуть бути значно знижені, оскільки обчислення виконуються поза головним ланцюгом Ethereum. Також значно підвищує масштабованість мережі Ethereum, обробляючи більше транзакцій за одиницю часу. Алгоритм дії полягає в тому, що усі транзакції групуються (збираються) разом та обробляються на вторинному ланцюгу, відомому як Rollup chain. Також в основі використовуються математичні докази (zero-knowledge proofs), що верифікують транзакцій. Це забезпечує високий рівень безпеки та ефективності, оскільки не потрібна перевірка кожної транзакції учасниками мережі.

2.3.2 Смарт-контракти

Смарт-контракт – угода між двома або кількома сторонами, у формі комп’ютерного коду. Він так само як і будь-який звичайний контракт, встановлює певні умови угоди. На відміну від традиційного контракту, умови SMART-

контракту виконується автоматично при виконанні певних умов. Після виконання коду, його фактично неможливо скасувати або змінити.

Смарт-контракти поширюються у децентралізованій мережі Blockchain. Це дозволяє розробникам створювати додатки, що використовують всі переваги Blockchain, такі як безпека, надійність та доступність, пропонуючи також вдосконаленний функціонал peer-to-peer.

Смарт-контракти розширюють базову ідею блокчейну – передачу та отримання коштів без посередників, таких як банки, дозволяючи автоматизувати та децентралізувати практично будь-які угоди чи транзакції, незалежно від їх складності. Оскільки вони працюють на блокчейні Ethereum, смарт-контракти забезпечують високу безпеку, прозорість та незмінність виконання умов контрактів. Алгоритмом проведення таких транзакцій з використанням смарт-контрактів є :

1. Користувач аутентифікується у своєму криптогаманці за допомогою свого приватного ключа або іншим методом аутентифікації (наприклад, 2FA або біометрична аутентифікація).

2. Користувач обирає адресу, з якої він хоче відправити кошти, та перевіряє свій баланс на цій адресі.Формування транзакції

3. Користувач формує транзакцію, яка включає:

1. Адреса смарт-контракту
2. Метод смарт-контракту (наприклад, transfer, approve)
3. Параметри методу (адреса отримувача, сума переказу тощо)
4. Вартість комісії (gas price)
5. Ліміт комісії(gas limit)

4. Користувач підписує транзакцію своїм приватним ключем, що гарантує авторизацію і безпеку. Це захищає транзакцію, підтверджуючи її справжність та авторизацію.

5. Підписана транзакція надсилається до мережі Ethereum для обробки.

6. Нода (node) – це будь-який комп'ютер, який є частиною блокчейн-мережі криптовалюти , ноди обмінюються інформацією про блоки та транзакції через P2P-

протоколи. Нода включає транзакцію у блок і додає блок до Blockchainy, підтверджуючи транзакцію.

7. Віртуальна машина Ethereum (EVM) виконує код смарт-контракту відповідно до умов транзакції. Це може включати оновлення стану смарт-контракту та виконання передбачених функцій.

8. Транзакція вважається підтвердженою після включення в блок і отримання необхідної кількості підтверджень від інших майнерів.

9. Користувач отримує підтвердження про успішне виконання транзакції та оновлений баланс у своїй криптогаманці.

Для смарт-контрактів можуть бути інтегровані рішення ZK-Rollups для підвищення ефективності та зменшення витрат на комісії, об'єднуючи транзакції і генеруючи криптографічні докази їх валідності. Це дозволяє масштабувати мережу, зберігаючи децентралізацію і безпеку.

2.3.3 Переваги SMART-контракт

Смарт-контракт може бути створений та розгорнутий на Blockchain ким завгодно. Код смарт-контрактів є прозорим і публічно перевіреним, що означає, що будь-яка зацікавлена сторона може бачити, який саме логічний вивід слідує після його виконання та отримання цифрових активів. В мережі Ethereum код кожного контракту зберігається на Blockchain, що дозволяє будь-якій зацікавленій стороні перевірити код контракту та поточний стан, щоб перевірити його функціональність.

Коли смарт-контракт отримує кошти від користувача, його код виконується всіма вузлами в мережі, щоб досягнути згоди щодо результату та результируючого потоку вартості. Саме це дозволяє смарт-контрактам безпечно працювати без будь-якого центрального органу, навіть коли користувачі здійснюють складні фінансові транзакції з невідомими сутностями. Після розгортання на Blockchain смарт-контракти, як правило, не можна змінити, навіть їхнім творцем.

2.3.4 Алгоритм транзакцій в мережі Etherum

Gas — це розмір комісії, за певну дію чи транзакцію. Чим вище ціна цього газу, яку відправник готовий заплатити, тим пріоритетніша його транзакція в мережі Ethereum і тим охочіше її обробляють.

ERC-20 – стандарт токенів в Blockchaini Etherum. Токени ERC-20 – це смарт-контракти, які містять важливі та необхідні для роботи цих токенів алгоритми. Смарт-контракт USDT (ERC-20) містить прив'язку його до курсу долара та функції блокування транзакцій для адрес, що знаходяться в чорному списку компанії Tether, емітента стейблкоіна USDT.

Кожна транзакція токенів EPC-20 в Blockchaini ETH використовує приблизно в 3.3 рази більше Gas, чим звичайна проста транзакція. Комісія мережі не залежить від кількості відправлених токенів і не обчислюється у відсотках від суми, що відправляється [29].

У різних Blockchainax можуть бути однакові адреси гаманців .Токени ERC-20 підходить для транзакцій лише в Blockchaini ETH . При відправці транзакцій токенів в іншу мережу але на той же адрес, є ризик втратити свої активи. Після виконання транзакції весь невикористаний Gas повертається на адресу відправника.

Якщо значення Gas Limit буде навмисно дуже занижено або користувач спробує відправити стільки, скільки не має на балансі гаманця, то транзакція не відбудеться і буде відхилена з помилкою - Out of Gas. Витрачений при цьому на запуск смарт-контракту газ не повернеться на адресу. Комісія завжди сплачується відправником, незалежно від того успішна транзакція чи ні.

Важливим моментом для проведення транзакцій в Blockchaini ETH, є нумерація транзакцій. Кожна вихідна транзакція з адреси криптогаманця отримує унікальний номер та виконується відповідно до цього порядку. Цей номер, відомий як NONCE, завжди починається з 0.

Перша транзакція, що виходить з гаманця, матиме NONCE - 0. Ці значення використовуються для відстеження та захисту Blockchainy від фейкових, помилкових або шахрайських транзакцій.Порушення порядку а саме випадкове

виконання транзакцій, а також повторне використання вже використаного NONCE в мережі Ethereum є неприпустимими.

Віртуальна машина Ethereum (EVM), відповідальна за перевірку кожного смарт-контракту на валідність та відповідність алгоритмам мережі, не дозволить відправити транзакцію з NONCE 1, доки не буде підтверджена транзакція з NONCE 0, а також не допустить відправлення транзакції з тим самим NONCE (подвійна витрата). Etherum мережа існує на багатьох тисячах вузлів (компютерів, нод) по всьому світу тому є дуже стійкою до атак і, по суті, нездатною вийти з ладу внаслідок їх. Якщо один комп'ютер виходить з ладу, це не має значення, оскільки тисячі інших продовжують підтримувати мережу.

Майнери - це користувачі, які використовують свою обчислювальну потужність комп'ютерів для вирішення складних математичних завдань у мережі криптовалют, таких як Ethereum.

У мережі майнери займаються обробкою транзакцій, а також для створенням нових блоків у Blockchaini. У мережі Ethereum майнери також виконують схожі завдання, але, крім того, вони також перевіряють смарт-контракти та інші додаткові функції. У мережі Ethereum майнери отримують Ether (ETH) за свою роботу.

Транзакції, що проводятться в мережі зберігаються в блоках на Blockchaini. Майнери перевіряють ці блоки перед їхнім записом у мережі та використанням їх як історії транзакцій або цифрового реєстру. Майнінг, який використовується для перевірки транзакцій, відомий як метод proof-of-work (PoW). Кожен блок має унікальний 64-значний код, який ідентифікує його. Майнери витрачають свою обчислювальну потужність на пошук цього коду, доводячи його унікальність.

Перевагою ETH є те, що користувачі самі контролюють свої дії і можуть взаємодіяти з іншими учасниками мережі без третіх сторін. У мережі Ethereum кожен вузол має власну копію Ethereum Virtual Machine (EVM). Коли користувач відправляє транзакцію в смарт-контракт на Ethereum, вузли запускають контракт та вхідні транзакції через свої EVM.

У віртуальному середовищі кожен вузол може побачити, яким буде кінцевий результат - чи призведе він до успішного виконання транзакції чи ні. Якщо всі вузли

досягають одного й того ж результату в EVM, зміни вносяться. Оновлений стан Ethereum мережі фіксується в Blockchaini. Алгоритм взаємодії Ethereum Virtual Machine (EVM) див.на (рис.2.7).

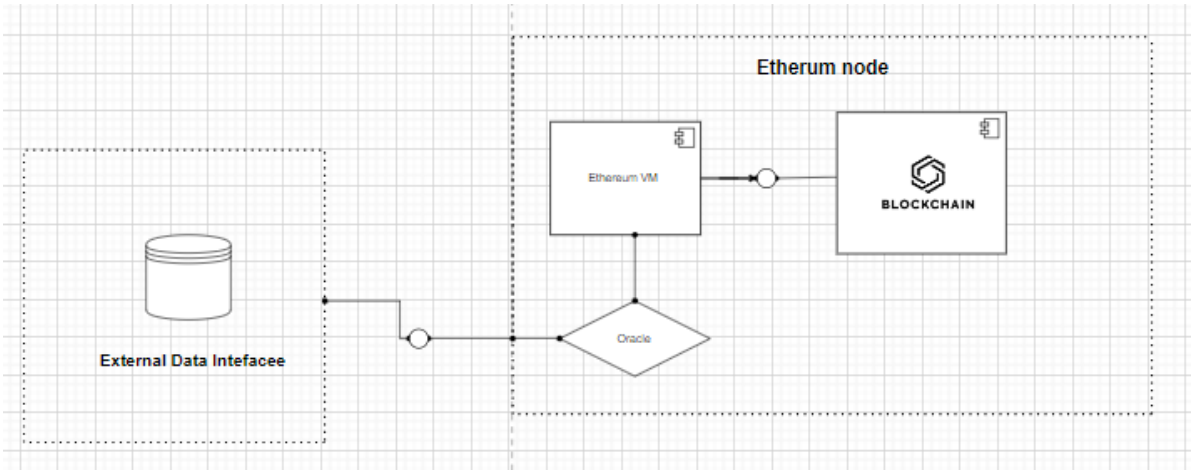


Рисунок 2.7 Алгоритм Ethereum Virtual Machine (EVM)

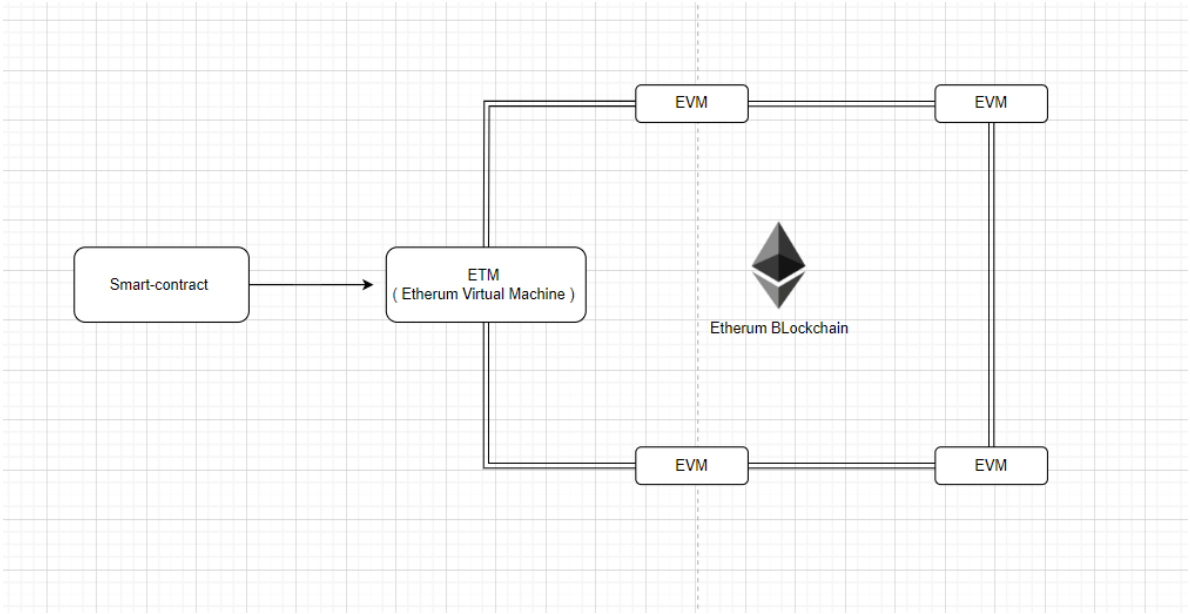


Рисунок 2.8 Алгоритм смарт-контракт в Blockchain ETH

Користувач ініціює транзакцію з криптогаманця, в якій передаються необхідні дані, дані для виконання смарт-контракту. Транзакція передається за допомогою протоколів HTTPS по вузлам (нодам, Node) компютерної мережі.

Вузли – node перевіряють транзакцію і статус користувача , за допомогою власних алгоритмів мережі ETH. Після верифікації транзакції, створюється новий запис для створення блоку даних в реєстрі.

Новий блок даних назавжди реєструється в вже існуючій послідовності блоків. Користувачу повертаються дані про успішне виконання транзакції.

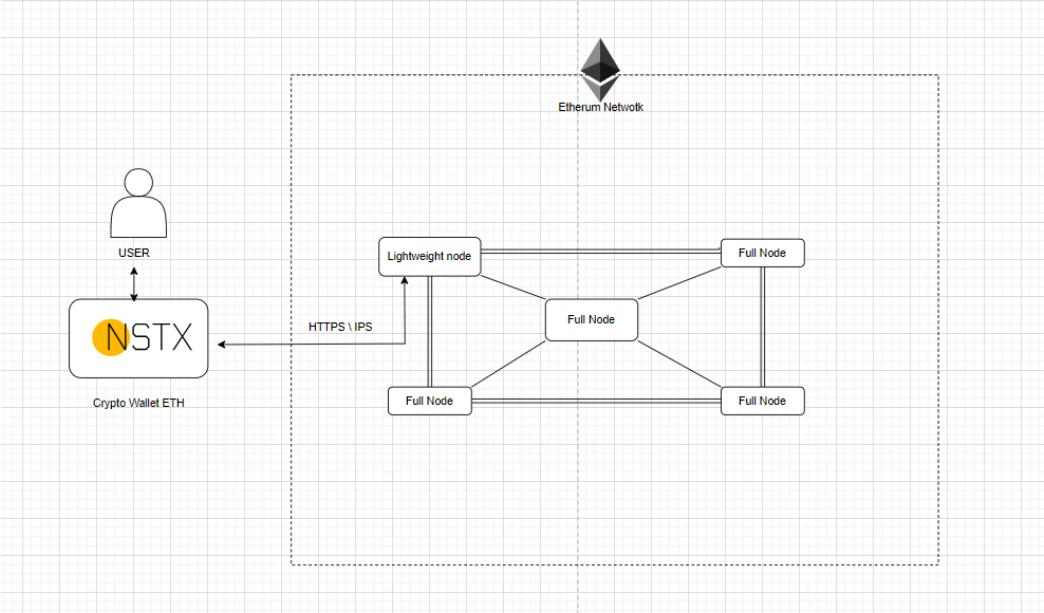


Рисунок 2.9 Алгоритм транзакцій в Blockchain

2.4 Календарний план

Розробка та впровадження проекту мають певні обмеження, які необхідно враховувати для досягнення успіху. Необхідно стежити за виконанням і термінами робіт, щоб уникнути затримок і забезпечити своєчасне завершення всіх етапів проекту. Календарний план дозволяє чітко визначити часові рамки для кожного завдання, що сприяє ефективному розподілу ресурсів та уникненню перевитрат часу.

Термін на виконання всього проекту встановлений на 245 днів, з початком з 21.03.2024 до 21.11.2024. Це конкретне часове обмеження вимагає точного планування і дотримання графіку виконання робіт, щоб встигнути завершити проект у встановлений строк. Календарний план допомагає детально розподілити

всі завдання в межах цього періоду, що сприяє організації процесу та уникненню перевантажень або простоїв.

Загальна вартість проекту не повинна перевищити – 900 000 грн. Це фінансове обмеження вимагає ретельного планування бюджету та контролю за витратами на кожному етапі проекту. Календарний план дозволяє відстежувати використання ресурсів та фінансів, що допомагає уникнути перевитрат і забезпечити дотримання бюджетних обмежень. Календарний план наведено у таблиці 2.4 (див.додаток 3).

Календарний план дозволяє ефективно керувати обмеженнями по виконанню робіт і термінам, дотримуватись встановлених строків виконання проекту та контролю витрат, забезпечуючи тим самим успішне виконання проекту в межах встановлених ресурсів та часу.

Висновки до розділу 2

У цьому розділі детально розглянутий алгоритм транзакцій в мережі Ethereum, зокрема, використання смарт-контрактів та комісії (Gas). Ethereum є провідною платформою для розробки децентралізованих додатків (dApps) та смарт-контрактів, що забезпечує функціонування багатьох фінансових і технологічних інновацій.

Розроблено календарний план та визначено обмеження для реалізації проекту.

Децентралізована природа Ethereum робить мережу стійкою до атак і несправностей окремих вузлів, що гарантує її високу надійність та безперервну роботу.

Ethereum є потужною платформою для розробки децентралізованих додатків, що забезпечує високу безпеку, надійність та ефективність завдяки використанню смарт-контрактів, механізму Gas та алгоритмів консенсусу. Однак, висока вартість Gas та складність у користуванні можуть бути викликами для новачків, що підкреслює важливість розвитку інтуїтивно зрозумілих рішень для користувачів.

РОЗДІЛ 3 ПРОЕКТНІ РІШЕННЯ

Даний розділ присвячений технічній частині атестаційної випускної роботи (АВР), а саме опису проектних рішень, що стануть основою для продукту крипто гаманця. Буде описано мінімально необхідний функціонал системи для його первинного запуску, побудовано модель спринта та календарний план з розробки.

Перед впровадженням будь-якого технологічного продукту, важливо провести аналіз можливих ризиків. Для криптогаманця це особливо важливо через високу чутливість до безпеки та конфіденційності даних. Тут описано безпекові стандарти та технології які використані для досягнення високої якості та надійності продукту.

Вибір технічних рішень повинен бути обгрунтованим та підтримуватися аналітичними даними та дослідженнями. Важливо зробити правильний вибір на початковому етапі проекту, щоб уникнути проблем та забезпечити успішну реалізацію і подальший розвиток. В даному розділі будуть описуватись використані технології та мови програмування, які використовуються для реалізації проекту онлайн криптогаманця. Описано інтеграцію з системами контролю версій, сервісами для автоматизованого тестування, засобами для автоматизації розгортання.

3.1 Середовище розробки

Розробка системи онлайн криптогаманця потребує зручне та високотехнічне рішення середовища для розробки . Із відомих на даний момент варіантів є VisualStudio та WebStorm.

Visual Studio в першу чергу орієнтований на розробку програм для екосистеми Microsoft, такі як програми на мові C#, .NET, та інші. У разі як ваш проект може використовувати веб-технології, які орієнтовані на інші платформи. Visual Studio початково не є вузько спеціалізованим середовищем для веб-розробки , і може не мати повного пакету підтримки розробки на Node.js або або ReactJS,

порівняно з WebStorm. Visual Studio, розроблений компанією Microsoft, широко використовується для розробки різноманітних програм, включаючи веб-програми на мовах, таких як JavaScript, TypeScript, HTML, та CSS. Він має розширену підтримку мов програмування та фреймворків, а також вбудовані інструменти для розробки, тестування та налагодження програм. Visual Studio може бути використаний для розробки як клієнтської, так і серверної частин програмного забезпечення.

WebStorm, розроблений компанією JetBrains, спеціалізується на розробці веб-програм та підтримує широкий спектр мов програмування, фреймворків та інструментів, які часто використовуються для веб-розробки. WebStorm має ряд унікальних функцій, таких як інтелектуальний аналіз коду, автоматичне доповнення та підказки, що робить процес розробки більш продуктивним та ефективним. Має велику кількість розширень, які ддопомагають у процесі візуалізації та розробки продукту. WebStorm інтегрується з багатьма іншими корисними інструментами, такими як системи контролю версій (наприклад, Git), середовища віртуалізації (наприклад, Docker), системи тестування та інші.

За обраним стеком технології а саме React, TypeScript, Node – вибір кращого середовища для розробки переважає за WebStorm. Тому, що це може сприяти швидкому та ефективному процесу розробки, забезпечуючи високу якість коду та зручність управління проектом.

3.2.1 Etherum Blockchain, ERC-20, SMART-контракт

Основна взаємодія криптогаманця завжди буде з Blockchainom Etherum. Smart-контракти та ERC-20

Дані по транзакціям:

- Дані транзакцій повинні бути відповідно підписані для підтвердження їх автентичності та унікальності. Використання криптографічного підпису забезпечить автентифікацію та цілісність даних.

- Формат вхідних даних для транзакцій повинен відповідати стандартам, прийнятим у Blockchain-мережі. Наприклад, формат адреси гаманця та структура транзакцій повинні відповідати вимогам протоколу Blockchain-мережі.
- Великі обсяги даних можуть бути розділені на декілька транзакцій.

Аутентифікація користувача:

- Вхідні дані, такі як приватні ключі, повинні бути зашифровані та надійно захищені від несанкціонованого доступу. Зберігання приватних ключів в зашифрованому вигляді допомагає уникнути можливості несанкціонованого доступу.
- Дані користувача мають бути достовірними та підтвердженими перед виконанням будь-яких транзакцій. Це може вимагати використання механізму двофакторної аутентифікації або інших методів аутентифікації.

Мережеві дані:

Дані, які відправляються через мережу, повинні бути шифрованими та захищеними від перехоплення. Використання шифрування допомагає зберегти конфіденційність даних під час передачі через мережу**.**

Обмеження на вихідні дані системи:

Стан рахунку:

- Дані про баланс та історію транзакцій повинні бути доступні лише для відповідного користувача. Використання публічного та приватного ключів допомагає забезпечити, що тільки власник гаманця може отримати доступ до своїх даних.
- Дані про стан рахунку, які виходять, повинні бути цілісними та невідредагованими. Перевірка цілісності та автентичності даних є важливою для запобігання будь-яким змінам у вихідних даних.

Підтвердження транзакцій:

- Результати транзакцій повинні бути підтверджені та підписані відповідними сторонами для забезпечення їх автентичності та цілісності. Підписання даних

допомагає перевірити, що дані були створені автентичним джерелом і не були змінені в процесі передачі.

- Вихідні дані повинні включати унікальний ідентифікатор транзакції, підписану підтвердженням та іншу необхідну інформацію. Ці дані служать як доказ виконання транзакції та підтвердження її унікальності.

Дані смарт-контрактів:

- Інформація пов'язана з смарт-контрактами, повинна бути коректною та відповідати вимогам смарт-контракту. Це включає в себе валідацію всіх вхідних даних перед їх передачею смарт-контракту.
- Результати виконання смарт-контрактів повинні бути відповідним чином підписані та підтверджені для забезпечення їх цілісності та автентичності. Використання криптографічного підпису гарантує, що дані не були змінені після виконання смарт-контракту.

3.2.2 Система LiqPay

Однією з вимог до функціоналу криптогаманця, є можливість поповнювати рахунок з інших карток. Для цьогот підходить сервіс LiqPay що надає широкий спектр методів оплати, включаючи картки Mastercard/VISA/UnionPay/Простір, PrivatPay, Apple Pay, Google Pay, FacePay24 та інші. Це робить платіжний сервіс вкрай зручним для користувачів, які мають різні уподобання щодо способів оплати.

Широкий функціонал LiqPay дозволяє не лише приймати платежі на сайтах та у мобільних додатках, але й отримувати виплати від мікрофінансових і страхових організацій, а також відправляти грошові перекази з картки на картку. Це робить сервіс універсальним і вигідним для різних бізнес-потреб.

Дослідивши сервіс, він має доволі високий рівень безпеки та підтверджує свою надійність сертифікатами PCI DSS, Verified by Visa і Mastercard SecureCode. Технології введення додаткового пароля безпеки для проведення оплати, такі як 3-D Secure, додають додатковий шар захисту для користувачів. Процес оплати та проведення платежів в LiqPay складається з трьох етапів, що дозволяє забезпечити надійність та безпеку транзакцій, одночасно забезпечуючи швидкість та зручність для користувачів.

Висновоки по сервісу LiqPay наступні - він виступає не лише як засіб для приймання платежів, але і як комплексне платіжне рішення, що забезпечує безпеку, швидкість та зручність для користувачів і підприємств. Його унікальні можливості та високий стандарт обслуговування роблять його привабливим вибором для прроекту криптогаманця.

3.2.3 Рішення Frontend та Backend

Обравши сервіси та необхідні технології, що будуть інтегруватись з проектом онлайн криптогаманця, необхідно обрати наступні технлогії для реалізації самого коду та бізнес-логіки проекту. Для веб-додатків , в інформаційному забезпеченні обрано декілька певних рішень.

Забезпечення для клієнтської частини додатку включає наступні рішення :

Перше рішення це мова програмування TypeScript. TypeScript – високорівнева мова програмування, розроблена компанією Microsoft, яка додає статичну типізацію зі змогою додавати типові анотації до JavaScript.

TypeScript призначений для розробки великих застосунків і інтерпретується в JavaScript. Так як TypeScript є розширенням JavaScript, всі програми JavaScript синтаксично правильні для TypeScript, але вони можуть не пройти перевірку типів з міркувань безпеки. Це є вдосконалим рішенням JavaScript, через наявність перевірки типів даних які приймають функції. Типи даних статично попередньо необхідно визначити та описати. Це забезпечує більшу надійність програмного забезпечення та запобігає виникненню більшості помилок при його роботі.

В парі до TypeScript використовують бібліотеку React, що є декларативною, і дозволяє розробникам створювати повторно використовувані компоненти користувацького інтерфейсу. React використовує підхід Virtual DOM (Document Object Model), який оптимізує продуктивність відображення, мінімізуючи оновлення DOM. React швидкий і працює добре з іншими інструментами та бібліотеками.

Забезпечення для серверної частини додатку включає наступні рішення :

Fastify – веб-фреймворк для створення Backend API , побудований на базі HAPI та Express , та на данний момент одним із найбільш високо ефективних та продуктивних рішень для створення маштабованих екосистем організацій та продуктів. В парі з pinologger забезпечить швидкодію серверної частини криптогаманця та надійність. Використання строгої типізації TypeScript знизить до мінімума помилки та надходження хибних данних з клієнтської сторони.

Vite Це програмне забезпечення для збірки WEB-додатків різних рівнів, що полегшує процес розробки та збірки full-stack проектів. Vite дозволяє створити середовище для фреймворків, таких як TypeScript + React з Fastify, що значно прискорює процес розробки.

PostgreSQL – система управління базами даних (СУБД) відповідає стандарту SQL там, де така відповідність не суперечить традиційним можливостям або не

може призвести до поганих архітектурних рішень. PostgreSQL підтримує часткові, бітові та виразові індекси. Він також забезпечує успадкування таблиць та матеріалізовані види. PostgreSQL є об'єктно-орієнтованою реляційною базою даних, а не просто реляційною базою даних, і багато з його розширених можливостей пов'язані з цим.

Сервіси, що використовуватиме криптогаманець.

Система LiqPay. LiqPay – найбільша електронна платіжна система для переказу коштів, онлайн-платежів, відкриття рахунків та оплати кредитними або дебетовими картками. Вона гарантує повну бещпеку данних та захищає від будь-яких зловмиснецьких атак. Платіжна платформа пропонує програму Buyer Protection та захищає практично всі покупки в інтернет-магазинах, з якими вона пов'язана.

Таким чином, якщо той хто надає певні послуги - (поповнення криптовалютного балансу гаманця) не виконує свої умови, або неякісно це робить,то власник рахунку може повернути сплачену суму без будь-яких проблем.

Обмеження в системі LiqPay**.** Мінімальна та максимальа сума транзакції залежить від валюти та типу транзакції.Для транзакцій в гривнях мінімальна сума становить 1 грн, а максимальна - 500 000 грн. Потрібно вказати повне ім'я, адресу електронної пошти та країну проживання платника та одержувача. Може знадобитися додаткова інформація, наприклад, номер телефону або дата народження.

LiqPay підтримує різні типи транзакцій, такі як надсилання та отримання платежів, оплата товарів та послуг, виведення коштів на банківський рахунок. Деякі типи транзакцій можуть бути недоступні в певних країнах.

Дані від LiqPay, що приходять у відповідь на виклики з фронтенд частини онлайн криптогаманця включають – підтвердження транзакції, а саме LiqPay надсилає платнику та одержувачу електронні листи з підтвердженням транзакції. Платник та одержувач можуть переглядати історію своїх транзакцій та деталі кожної транзакції, такі як сума транзакції, валюта, дата та час транзакції,

інформація про платника та одержувача на веб-сайті LiqPay або в мобільному додатку.

LiqPay пропонує різні звіти про транзакції, які власники бізнесу можуть використовувати для відстеження своїх продажів.

3.3 Інтерфейс

Попереденій аналіз конкурентів висвітив проблему вже існуючих систем та рішень які є на ринку цифрових додатків для управління активами. Мета спроектувати систему та інтерфейс так, щоб бути максимально комфортними та інтуїтивно зрозумілими для будь-якого користувача, як для новачка так і для професіонала у цій сфері.

При розробці дизайну варто уникати використання зайвих елементів, що будуть відволікати чи не мати прямого користувальницбкого призначення. Це такі елементи, як зайві кнопки, меню, що можуть зробити інтерфейс менш зрозумілим та заплутати користувачів.

Бритва Окамма – методологічний принцип , при якому із всіх рішень необхідно обрати те, що володіє найменшими труднощами. Даний принцип орієнтований на те, що просте – більш пріоритетне перед складним. Це означає, що ми повинні уникнути пошуку занадто складних рішень для задач, які ставить перед нами проект та сконцентруватись на тому, що працює в даному контексті рішення проблеми. Цей принцип використовується в різних ситуаціях як засіб швидкого прийняття рішень, якщо вони неочевидні. Згідно до цього методу у контексті створення дизайну, розробник повинен віддавати перевагу простим та інтуїтивно зрозумілим рішенням, що не мають зайвих деталей, складнощів.

Застосування принципу бритви Окамма в дизайні крипто-гаманця робить його простим, ефективним та зручним для користувачів. Це сприяє кращому досвіду та спрощує інтеграцію в повсякденне використання крипто-гаманців.

Проте слід пам'ятати, що простота не повинна йти на шкоду безпеці. Криптогаманець NSTX матиме хоч і простий дизайн, але не нудний. Інтерфейс повинен бути привабливим та сучасним.

Прототипи та дизайн прокту наведені на (рис. 3.10) та (рис. 3.11) див. додаток 10-11.

3.4 Проектування БД

Для проектування бази даних (БД) попередньо було здійснено аналіз сутностей, необхідних для функціонування системи. У цьому розділі розглянуто цей процес. При створенні архітектури бази даних для системи криптогаманця на основі Blockchain Ethereum необхідно дотримуватися принципів наведених далі.

Архітектура системи заснована на Blockchaini Ethereum (ETH), який є платформою для децентралізованих додатків (dApps), де дані розподіляються між безліччю вузлів (Node), забезпечуючи високу стійкість та надійність системи. Blockchain використовує розподілений реєстр для зберігання даних, що дозволяє уникнути вразливостей у разі виходу з ладу одного з вузлів. При проектуванні важливо також використовувати зручні системи для управління БД та перевірені рішення.

PostgreSQL – це база даних з відкритим кодом, яка є надійним інструментом для вирішення багатьох питань, пов'язаних із забезпеченням надійності, гнучкості та подальшої підтримки даних. На відміну від інших систем управління базами даних (СУБД), PostgreSQL може підтримувати реляційні та нереляційні системи, що робить його найбільш сумісним та стабільним рішенням для наого проекту, який базується на Blockchain Ethereum та смарт-контрактах ERC-20.

PostgreSQL підтримує різноманітні типи та структури даних, включаючи мережеві адреси, дані у форматі JSON та геометричні дані для координат геопозицій. Ці дані можуть бути збережені та оброблені в базі даних, що дозволяє ефективно управляти різноманітними типами інформації.

Для більш зручного використання та управління PostgreSQL ми будемо використовувати PgAdmin4. Цей потужний, відкритий інструмент управління базами даних є об'єктно-реляційною системою, яка повністю сумісна з можливостями PostgreSQL. PgAdmin має інтуїтивно зрозумілий графічний інтерфейс, що робить його одним з кращих виборів для розробників Backend.

Інструмент дозволяє підключатися до баз даних не тільки локально, а й віддалено, підтримуючи широкий спектр версій PostgreSQL та операційних систем. PgAdmin є незамінним інструментом, який пропонує комплекс функцій для ефективного управління базою даних PostgreSQL.

Для розгляду архітектури бази даних та її компонентів, можна переглянути спроектовану базу даних на рисунку 3.1 (див. додаток 8)

3.5 Програмний код та алгоритми

У цьому розділі описується структура програмного коду та основні алгоритми, які використовуються для реалізації функціональності криптогаманця на основі Ethereum та смарт-контрактів ERC-20.

Архітектура програмного коду наступна. Програмний код криптогаманця розділений на кілька модулів, кожен з яких відповідає за окремі аспекти системи:

1. Frontend. Інтерфейс користувача розроблений за допомогою React та TypeScript. Включає компоненти для аутентифікації, управління балансом, створення та перегляду транзакцій.

2.Backend. Серверна частина реалізована на базі Fastify, забезпечуючи швидкий та ефективний обробник запитів. Використовується для обробки запитів від клієнта, взаємодії з Blockchainom Ethereum та управління базою даних PostgreSQL.

3. База даних. Використовується PostgreSQL для зберігання інформації про користувачів, транзакції та інші метадані. Для управління базою даних застосовується PgAdmin.

Опишемо архітектуру проекту в середовищі розробки. Структура Frontend (клієнтської частини) складається з наступних модулів :

1. Dist. Містить скомпільовані вихідні файли клієнтського додатку, що генеруються після процесу збирання.

2. Node_modules. Залежності npm (Node Package Manager) для клієнтського додатку.

3. public. Папка з файлами що інтерпретуються та компілюються безпосередньо браузером. Містить загальні стилі, назву проекту, мета-теги.

4. API**.** Надсилання запитів на сервер.

5. Asets**.** Статичні ресурси, зображення, логотипи, svg.

6. Components**.** Компоненти React, які можна повторно використовувати в усьому додатку та мають кастомні стилі

7. Hooks**.** Хуки React, які інкапсулюють логіку, яку можна повторно використовувати в різних компонентах.

8. Interfaces**.** Статична типізація інтерфейсів TypeScript

9. Layout**.** Містить основний контейнер, сайдбар меню та хедер.

10. Pages. Компоненти сторінок

11. Routes. Налаштування маршрутизації React Router.

12. App.css, App.tsx. Корневі файли.

13. index.css, index.tsx. Точка входу програми React та її глобальні стилі.

14. theme.tsx. Конфігурація для теми Mui

15. vite-env.d.ts. Файл декларацій TypeScript для Vite, інструменту збирання, який ставить за мету забезпечити швидший і більш легкий досвід розробки для сучасних веб-проектів.

Backend структура.

1. netlify – папка що містить налаштування для деплою в хмарне середовище.
2. Prisma – інструмент ORM (Object-Relational Mapping) для роботи з базами даних.
3. Hooks – користувацькі хуки, які, ймовірно, використовуються для бізнес-логіки або абстрагування загальних функціональних можливостей.
4. Module – модулі для кожного з сервісів, таких як сервіс з траназкціями, балансами.
5. .gitignore для ігнорування непотрібних файлів у Git.Є файли конфігурації для Netlify та Vite.

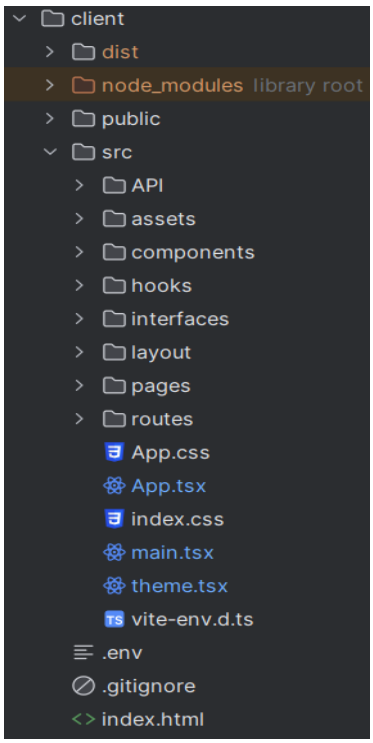


Рисунок 3.2 Архітектура Frontend модулів

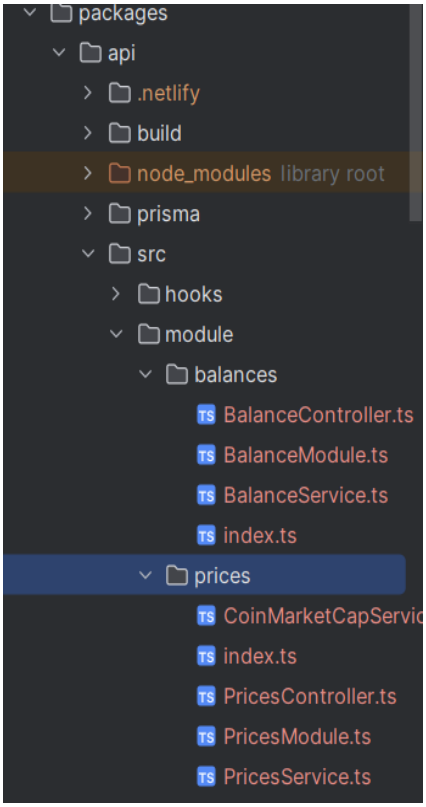


Рисунок 3.3 Архітектура Backend модулів

Дана архітектура проекту має чітке розділенням між клієнтським та серверним кодом. Клієнтська частина побудована за допомогою сучасних веб-

технологій, таких як React і TypeScript, тоді як серверна частина використовує модульний підхід із сервісами, контролерами та, можливо, ORM для взаємодії з базою даних. Така структура допомагає підтримувати чисту та організовану кодову базу, що полегшує її керування, масштабування та відладку.

Структура проектного коду , що зображена на (рис. 3.3) та (рис. 3.2) є ефективним рішенням, всі файли поділено за функціональними категоріями (components, hooks, layout, pages, routes).Наявність точки входу (index.tsx) та файлів стилів (App.css). Є зручною для подальшого маштабування проекту.

Функції та алгоритми Frontend аутентифікації та реєстрації.

1. Logout – вихід із криптогаманця, а саме відюується видалення токену користувача із sessionStorage та вихід із криптогаманця.
2. Register – реєстрація нових користувачів, система отримує введені користувачем дані через форму реєстрації. • Пароль хешується з використанням безпечного алгоритму (наприклад, bcrypt) для зберігання в базі даних.
3. Login – для входу в аккаунт. Алгоритм аутентифікації користувача Користувач вводить свої облікові дані –> система перевіряє правильність введених даних –> Якщо дані правильні, користувач отримує доступ до свого гаманця –> якщо дані неправильні, користувач отримує повідомлення про помилку.
4. GetUser – для отримання даних по користувачу , та перевірку токену . Якщо користувач знайдений, отримання його даних (ім'я, електронна пошта, транзакції, гаманці).

```
export const logout = async (): Promise<void> => {  Show usages  pasichmaria
    const response : AxiosResponse<any, any>  = await axios.get( url: "/logout",  config: {
        withCredentials: true,
    });
    return response.data;
};

export const register = async (data: {  Show usages  pasichmaria
    email: string;
    password: string;
    firstName: string;
    lastName: string;
}): Promise<User> => {
    const response : AxiosResponse<any, any>  = await axios.post( url: "/sign-up", data,  config: {
        withCredentials: true,
    });
    return response.data;
};
```

Рисунок 3.4 Запити реєстрації та виходу з аккаунта

```
export const login = async ({  Show usages  pasichmaria
    email,
    password,
}: {...}): Promise<string> => {
    const response : AxiosResponse<any, any>  = await axios.post(
        url: "/login",
        {email: email...},
        {...},
    );S
    return response.data.accessToken;
};
```

Рисунок 3.5 Запит на вхід до аккаунту

```
40      return response.data;
41  };
42
43  export const getUser = async (): Promise<User> => {  Show usages  pasichmaria
44      const response : AxiosResponse<any, any>  = await axios.get( url: "/users/me",  config: {
45          withCredentials: true,
46          headers: {
47              Authorization: `Bearer ${sessionStorage.getItem( key: "token")}`,
48          },
49      });
50      return response.data;
51  };
52
```

Рисунок 3.6. Запит на отримання даних по користувачу

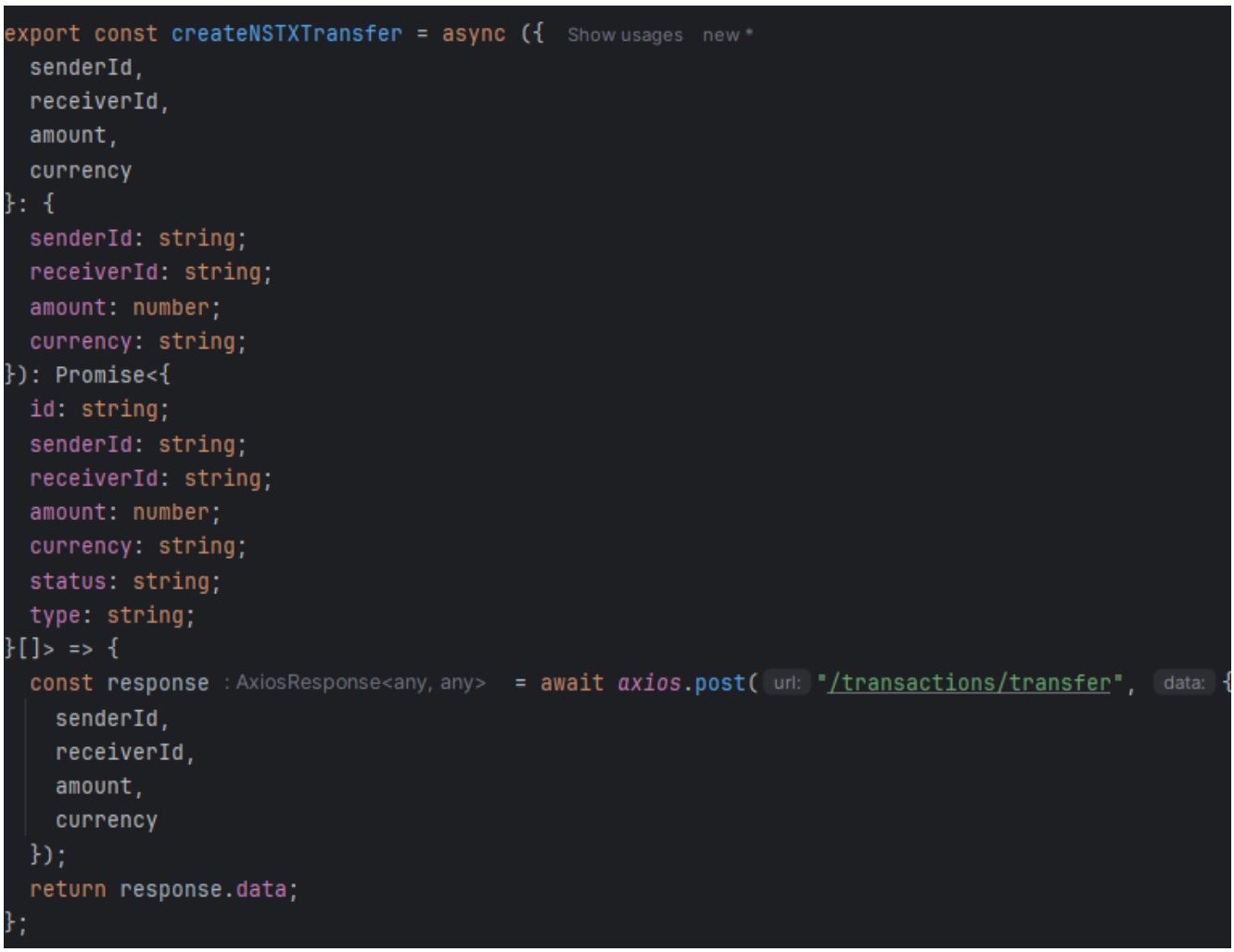


Рисунок 3.7 Запит для проведення транзакції.

3.6 Висновки до розділу 3

Обрані технології та архітектурні підходи, такі як використання Ethereum-Blockchainy, смарт-контрактів ERC-20 та інтеграція з технологіями ZK-Rollups, демонструють прагнення до забезпечення високого рівня безпеки, масштабованості та ефективності системи. Вибір PostgreSQL як основної системи управління базами даних обґрунтовано її здатністю підтримувати як реляційні, так і нереляційні дані, що є критично важливим для зберігання та обробки різноманітних типів даних, необхідних для функціонування криптогаманця. Інтеграція з інструментом управління PgAdmin забезпечує зручність та

ефективність у повсякденній роботі з базою даних, що додатково підвищує продуктивність команди розробників.

Архітектура системи, включаючи її децентралізовану природу, була обрана для забезпечення високого рівня безпеки та надійності. Децентралізація дозволяє уникнути єдиних точок відмови, підвищує стійкість до атак та забезпечує безпеку збережених даних. Такий підхід також сприяє підвищенню прозорості транзакцій, що є важливим для довіри користувачів до системи. Використання сучасних технологій, таких як TypeScript, React, Fastify та Vite, забезпечує високу продуктивність розробки та підтримку сучасних стандартів у створенні інтерфейсу користувача та серверної частини. Це дозволяє досягти високої якості програмного продукту та зручності його використання.

Загалом, проведені проектні рішення забезпечують надійну, безпечну та зручну систему криптогаманця, яка відповідає сучасним вимогам користувачів та нормативних органів. Врахування всіх технічних та архітектурних аспектів під час проектування дозволяє забезпечити стабільне та ефективне функціонування системи, сприяючи розвитку цифрової економіки та забезпечуючи високу задоволеність користувачів.

РОЗДІЛ 4 УПРАВЛІННЯ ПРОЕКТОМ СТВОРЕННЯ КРИПТОГАМАНЦЯ

Управління проектом створення криптогаманця включає кілька ключових етапі необхідних для забезпечення успішної розробки, впровадження та підтримки системи. Для ефективного керування проектом обрано підхід Scrum, який дозволяє гнучко реагувати на зміни вимог та забезпечує постійниу взаємодію з замовником. У проекті визначені цілі, зацікавлені сторони, ризики та план завершення і випуску продукту.

4.1 Визначення цілей проекту

Першим, що є критично важливим для управління проектом – визначення його цілей. Для визначення основних цілей проекту необхідно визначити цілі та рішення для них, встановити пріоритети задач. Це дозволить сконцентруватись на найважливіших аспектах проекту та забезпечити їх успішне виконання. Цілі проекту мають бути узгоджені з усіма зацікавленими сторонами та відповідати бізнес-цілям та вимогам.

Із дослідження існуючих рішень в першому розділі існує декілька проблем які необхідно уникнути при розробці нового криптогаманця. Основними цілями розробки крптогаманця є :

1. Безпека проведення транзакцій та зберігання криптовалютних активів для користувачів шляхом використання передових криптографічних методів та механізмів захисту від фейкових, помилкових або шахрайських транзакцій.
2. Створити інтуїтивно зрозумілий та легкий у використанні інтерфейс, який дозволить користувачам легко здійснювати транзакції та керувати своїми активами.
3. Забезпечити підтримку стандарту ERC-20 , інтеграцію з Ethereum та можливість взаємодії зі смарт-контрактами на його базі.

4. Підвищення маштиабованості завдяки використанню технології Zero-Knowledge Rollups
5. Сумісність криптогаманця з іншими системами та Blockchain рішеннями.

Маючи дані проблеми побудовані дерева проблем та дерева рішень проекту розробки онлайн криптогаманця на рисунку 2.6 (див. додаток 7)

4.2 Зацікавлені сторони проекту

Стейкхолдери – зацікавлені сторони, що мають безпосередньо прямий вплив на формування та управління проектом. До списку стейкхолдерів відносяться як користувачі, так і бізнес-партнери, керівники та учасники проекту. Стейкхолдери поділяються на дві групи – внутрішні та зовнішні.

До внутрішніх зацікавлених сторін відноситься, команда проекту яка включає :

1.Проектний керівник (Project manager). Відповідальний за загальне керівництво проектом, визначення цілей і стратегій розвитку.

2. CTO - відповідальний за технічну архітектуру і технічні аспекти проекту.

3. Frontend розробники, розробляють візуальну частину криптогаманця.

4. Backend розробники, відповідальні за розробку серверної частини додатку, баз данних. Відповідальні за реалізацію Blockchain-частини проекту, таку як смарт-контракти.

5.QA – Тестування функціональності та якості програмного забезпечення.

6. Дизайнер. Розробляє інтерфейс, що відповідний вимогам бізнесу.

Зовнішні зацікавлені сторони проекту.

1. Клієнти. Як і звичайні користувачі так і великі бізнеси.
2. Крипто-комюніті зацікавлене у розвитку та впровадженні Blockchain-технологій. Спільноти, обговорюються питання розвитку та використання Blockchainy, криптовалют та криптогаманців.
3. Venture investors (венчурні фонди) та приватні інвестори, які фінансують розвиток проекту.
4. Особи або організації, що фінансують проект та мають інтерес у його успішному виконанні.
5. Біржі криптовалют та крипто обмінники мають інтерес у співпраці або інтеграції з криптогаманцем для спрощення торгівлі.

Складено діаграму зацікавлених сторін проекту, що включає як і зовнішніх так і внутрішніх стейкхолдерів. Кожен із них відіграє важливу роль у розробці, впровадженні та подальшому використаннці онлайн криптогаманця, тому врахування їх інтересів та потреб є ключовим для успіху проекту.

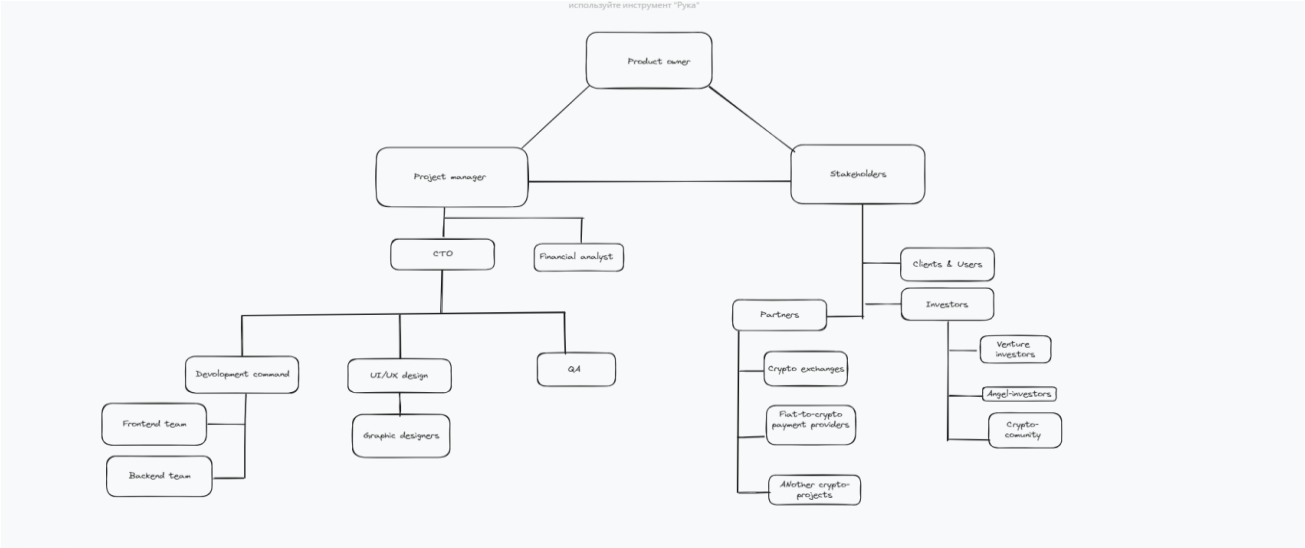


Рисунок 4.3 Зацікавлені сторони проекту

4.3 Ризики проекту

Ідентифікація ризиків є етапом який передбачає виявлення всіх потенційних ризиків, які можуть негативно вплинути на проект. Основні джерела ризиків включають в себе зовнішні та внутрішні. Внутрішні ризики пов'язані з процесами, ресурсами та управлінням всередині організації. Зовнішні ризики виникають через фактори, які знаходяться поза контролем організації. Розглянемо кожну категорію детальніше.

1. Технічні ризики. Відносяться до внутрішніх ризиків , та мають високий вплив на проект. Нові технології можуть зробити поточні рішення застарілими, та нові стандарти можуть вимагати значних змін у проекті. Неправильна реалізація смарт-контрактів може призвести до фінансових втрат. Складнощі при інтеграції з Blockchainom Ethereum або іншими зовнішніми системами.

2. Операційні ризики. Це збої в інфраструктурі роботи серверів, хмарного середовища чи провайдера API мають високий вплип на проект.

3. Невірне управління версіями на GIT може призвести до проблем із сумісністю, проблем на QA та production.

4. Ризики управління проектом включають недостатнє фінансування що призведе до затримок або зупинки проекту. Невідповідність графіку робіт може призвести до пропущених дедлайнів. Брак кваліфікованих фахівців або неправильний розподіл ресурсів. Відсутність необхідних навичок та знань у членів команди.

До зовнішніх ризиків відносимо ті ризики, на які ми не маємо прямий вплив, і можемо лише спрогнозувати і уникнути хоча б частково їх.

1. Нестабільність ринку криптовалют може вплинути на попит на криптогаманці.

2. Зростаюча конкуренція може призвести до зменшення ринкової частки та доходів.

3. Зовнішні хакерські атаки можуть призвести до втрати даних та фінансових втрат.

4. Втрата або крадіжка приватних ключів. Користувачі можуть втратити свої приватні ключі або стати жертвами фішинг-атак.

5. Нові закони або зміни в існуючому законодавстві можуть вплинути на функціонування криптогаманця.

6. Можливі обмеження з боку урядових органів щодо використання криптовалют.

7. Загальна економічна нестабільність може вплинути на інвестиції та попит на криптовалютні послуги.

8. Зміни в суспільних настроях щодо криптовалют можуть вплинути на використання криптогаманців.

Висновки до розділу . Ефективне управління ризиками збільшує шанси на успіх проекту, мінімізує втрати та забезпечує його стійкий розвиток.

4.4 SCRUM підхід до управління

В даному підрозділі розглянуто Scrum підхід до управління розробкою інформаційної системи з управління фінансовими активами. Scrum обрано для управління проектом створення онлайн криптогаманця з декількох причин, а саме для розробки складних програмних продуктів у динамічному середовищі. Scrum дозволить гнучно управляти та вносити правки, завдяки своїй гнучкій структурі.

Кожен спринт на проекті буде тривати 1 тиждень (7 днів), і в кінці кожного спринту команда переглядає виконану роботу та адаптує плани на основі отриманого зворотного зв'язку. Це дозволяє швидко реагувати на зміни вимог або виявлення нових проблем. Що робить даний підхід кращим рішенням для розробки складних програмних продуктів у динамічному середовищі. Гнучкість Scrum дозволяє знижувати ризики шляхом регулярних перевірок та адаптацій, що зменшує ймовірність невідповідності кінцевого продукту початковим вимогам.

Кожного дня проводяться daily meet – зідвони у спеціальній програмі, а саме в Slack для вирішення проблем та питань які виникли в попередні дні, та обговорення виконаних задач. В кінці кожного спринта (кожні 7 днів), проходить Sprint Review. Проводиться демонстрація виконаної роботи, де зацікавлені сторони можуть оцінити прогрес та внести свої коментарі та правки. Кожен учасник команди розробки розповідає про виконану роботу. Також необхідно проводити sprint retrospective – піж час ретроспективи команда обговорює, що спрацювало добре, що потрібно покращити, і як можна зробити процес ще ефективнішим.

За основу підходу Scrum взято ітеративний метод, завдяки регулярним перевіркам результатів роботи в кінці кожного спринту, можна оперативно вносити необхідні зміни та покращення. Завдяки чітко визначеним цілям спринту команда знає, на чому потрібно зосередитися в поточний момент, що сприяє більш ефективному використанню ресурсів. Scrum забезпечує гнучкість, прозорість, ефективність та постійне вдосконалення, що є критично важливим для успішної розробки та впровадження криптогаманця.

Для ще кращого підходу для управління проектом, разом підходом Scrum використано додаток Jira. Jira – використовується для відслідковування та систематизації задач, перевірки статусу їх виконання та кращої комунікації розробників та менеджера проекту.

Для ефективного управління спринтом у Jira, важливо коректно заповнювати всі необхідні поля для кожного завдання. Це дозволяє тримати проект під контролем, відстежувати прогрес і забезпечувати прозорість для всіх зацікавлених сторін. Задачі мають story points estimate – визначення, відносної складності та енергозатрат на виконання певної задачі, людиною. Використовується для планування строків реалізації продукту, оцінки прогресу команди та при плануванні спринта, щоб не запланувати зайве. Важливою метрикою є кількість сторі поінтів, яку команда може поставити за календарний період. Число поінтів за спринт - це продуктивність команди (velocity).

Для планування спринту необхідно вносити наступні дані до спринту Jira

1. Summary (Заголовок) – інформативний заголовок, який дає зрозуміти суть завдання.

2. Description (Опис) – детальний опис завдання, включаючи всі необхідні деталі, кроки для виконання та вимоги.

3. Epic Link (Посилання на Epic) – вибір (Epic), до якого належить це завдання.

4. Priority (Пріоритет) – визначення пріотритету завдання. Один з варіантів "High" (Високий), "Medium" (Середній), "Low" (Низький).

5. Assignee (Виконавець) – вібр людини, що відповідальна за виконання завдання.

6. Labels (Мітки) – слова або мітки, які допомагають у пошуку та фільтрації завдань. Приклад: UI,Frontend, Balance.

7. Sprint (Спринт) –вибір спринта до якого належить це завдання.

8. Story Points (Оцінка в Story Points). Оцінка складності завдання в Story Points.

9. Критерій прийняття – критерії, за якими буде визначено, чи виконано завдання успішно.Приклад - користувач бачить свій баланс на головній сторінці після входу в систему. Дані оновлюються в реальному часі.

10. Attachments (Вкладення). Файли або документи, що додаються до завдання. На основі критеріїв створимо спринт у вигляді таблиці, табл. 4.6 (див. додаток 5). Для того щоб визначити складність завдання використовуються Story Point Їх класивікація наступна :

1 Story Point. Дуже просте завдання, яке можна швидко виконати (написання простого тесту).

2-3 Story Point. Середньої складності завдання, яке потребує певних зусиль та часу такіяк розробка компонента інтерфейсу.

5-8 Story Point. Складне завдання, яке потребує значної роботи та координації. Наприклад інтеграція з новим API.

13+ Story Points. Дуже складне завдання з великою кількістю невідомих (рефакторинг основної частини коду).

Планування задачі першого спринта в Jira.

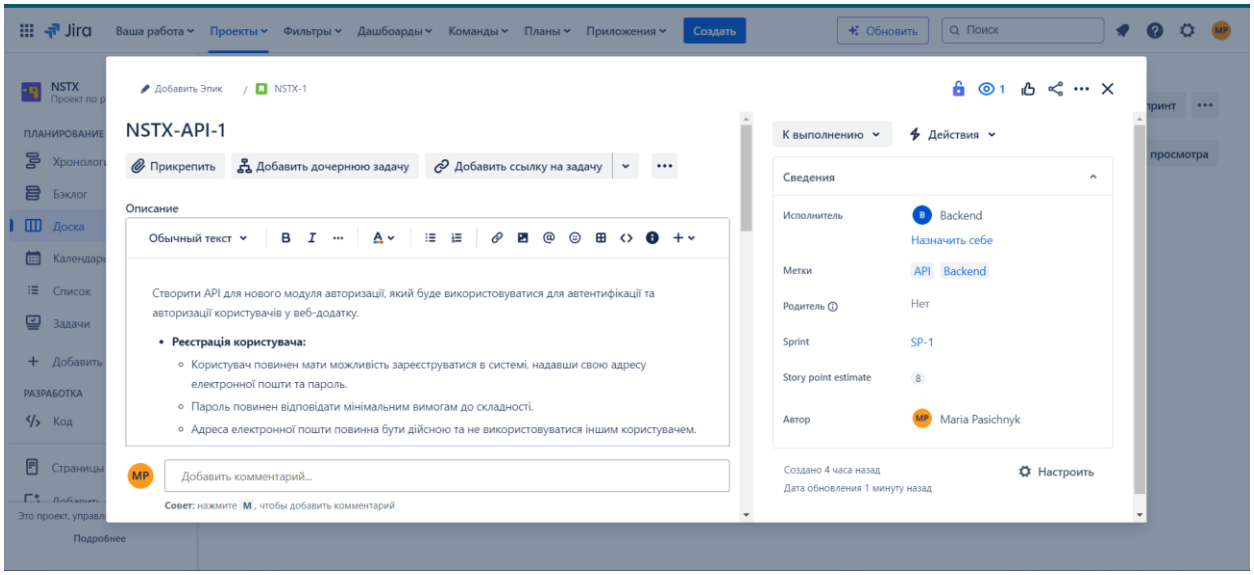


Рисунок 4.4 Планування спринта

- **Управління користувачами:**
  - Адміністратор повинен мати можливість переглядати список користувачів.
  - Адміністратор повинен мати можливість редагувати інформацію про користувача.
  - Адміністратор повинен мати можливість видаляти користувачів.
- **Безпека:**
  - API повинен використовувати протокол HTTPS для захисту даних.
  - Паролі користувачів повинні зберігатися у вигляді хешів.
  - Токени доступу повинні бути підписані цифровим підписом.
  - API повинен бути захищений від атак CSRF.

Технічні вимоги:

- API повинен бути розроблений на основі REST.
- API повинен відповідати стандартам JSON Web Token (JWT) для авторизації.
- API повинен бути документований за допомогою Swagger або подібного інструменту.
- API повинен бути протестований за допомогою автоматизованих інструментів тестування.

Критерії прийняття:

- Всі функціональні вимоги виконані.
- API відповідає всім технічним вимогам.
- API протестований та пройшов усі тестові сценарії.
- API задокументований за допомогою Swagger або подібного інструменту.

Рисунок 4.5 Вимоги задачі спринта

Висновки до розділу : обравши Jira та Scrum підхід для управління задачами проекту використовується ітеративний підхід до розробки, що забезпечить гнучкусть та швидке реагування на зміни.

ДОДАТКИ

Додаток 1
Таблиця 2.2

Обмеження на вхідні та вихідні дані

Об’єкт	Вхідні дані	Вихідні дані
Користувачі	Дані для авторизації та верифікації	
Криптовалютні активи	Транзакції	Актуальний баланс після проведення транзакції
Транзакції	Запит з даними на транзакцію , отримувач, сума, тип транзакції.	Статус транзакціі Унікальний ідентифікатор (id)
Баланс	Дані по вхідним та вихідним транзакціям	Актуальний баланс
Blockchain	Дані про транзакції, які включають адресу відправника, адресу отримувача, суму криптовалюти та підпис відправника.	Адреса відправника та отримувача, сума транзакції та час її проведення. Історія транзакцій. Підтвердження транзакції.

Додаток 2
Таблиця 2.3

Обмеження на вхідні та вихідні дані

Клас	Атрибути	Взаємодія
User	ID (primary key) Email (пошта) First_name (ім’я) Last_Name (прізвище) Password (пароль)	Користувач створює та керує своїм гаманцем, здійснює аутентифікацію для доступу до гаманця, зміна паролю та особистих данних.
Balance	Id (primary key) User_id (id власника) Value Currency Updated_at Created_at	Баланс можна створити, з різними криптовалютами в основі. Можна поповнити, заморозити.
Transaction	Id User_id Status Type Amount Currency Created_at Updated_at	Транзакцію можна створити, переказ , депозит , трансфер .

Додаток 3
Таблиця 2.4

Календарний план проекту

№	Назва роботи	Тривалість	Дата початку
1	Узгодження всіх деталей та вимог до проекту та підписання договору з замовником	28 днів	21.03.2024
2	Розробка технічного завдання	10 днів	21.04.2024
3	Графічний дизайн та інтерфейс сайту	30 днів	3.05.2024
4	Розробка функціональних модулів	90 днів	5.06.2024
5	Маркетингова компанія	30 днів	5.09.2024
6	Тестування	20 днів	20.10.2024
7	Передача замовнику та запуск проекту на хостинг	10 днів	11.11.2024

Закінчення табл.2.4

Календарний план проекту

Дата кінця	Резерв днів	Оцінка тривалості	Оцінка загальної та погодинної вартості робіт
18.04.2024	3 дні	56 годин	70000 грн 1250 г/год
1.05.2024	2 дні	60 годин	60 000 грн 1000 г / год
02.06.2024	3 дні	40 годин	40 000 грн 1000 г / год
3.09.2024	2 дні	360 годин	600 000 грн 1600 г / год
5.10.2024	5 днів	90 годин	50000 грн
10.11.2024	1 день	40 годин	40 000 грн 1000 г /год
21.11.2024	0 днів	10 годин	40 000 грн

Додаток 4
Таблиця 4.5

Управління ризиками проекту

Ризик	Категорія	Ймовірність	Вплив	Стратегія реагування	Відповідальна особа
Вразливості у програмному забезпеченні	Внутрішній	Висока	Високий	Регулярні коди-рев'ю та безпекові аудити	Lead Developer
Кібератаки	Зовнішній	Висока	Високий	Впровадження багаторівневої безпеки	Security Specialist
Зміни в законодавстві	Зовнішній	Середня	Високий	Постійний моніторинг законодавства, консультації з юристами	Legal Advisor
Недостатній бюджет	Внутрішній	Середня	Середній	Перегляд бюджету, залучення інвесторів	Project Manager
Відставання від графіка	Внутрішній	Середня	Високий	Перегляд пріоритетів, додаткові ресурси	Scrum Master
Недостатня кваліфікація команди	Внутрішній	Середня	Високий	Навчання та тренінги для команди	HR Manager

Додаток 5
Таблиця 4.6

Задачі спринта

A	B	C	D	E
День	Завдання	Відповідальний	Story Points	Стан
1-2	Розробка API для нового модуля авторизації (реєстрація)	Backend 1	4	У процесі
1-2	Створення інтерфейсу користувача для реєстрації	Frontend 1	3	У процесі
3-4	Розробка API для нового модуля авторизації (вхід)	Backend 2	2	У процесі
3-4	Створення інтерфейсу користувача для входу	Frontend 2	2	У процесі
5	Реалізація логіки скидання пароля	Backend 1	3	У процесі
6-7	Розробка інтерфейсу адміністрування користувачів	Frontend 1	4	У процесі
8	Написання тестових сценаріїв для нового модуля	QA	4	Не розпочато
9-10	Проведення інтеграційного тестування нового модуля	QA	4	Не розпочато
9-10	Виправлення помилок, виявлених під час тестування	Front + Backend	2	Не розпочато

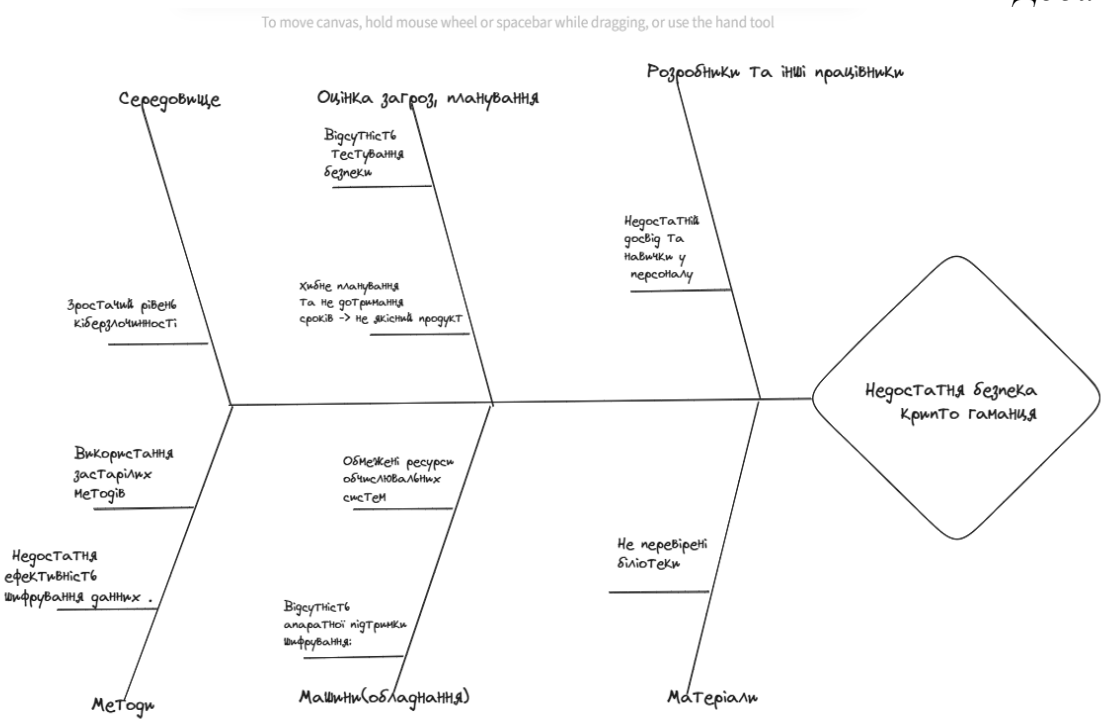


Рисунок 1.1 Діаграма Іссікави

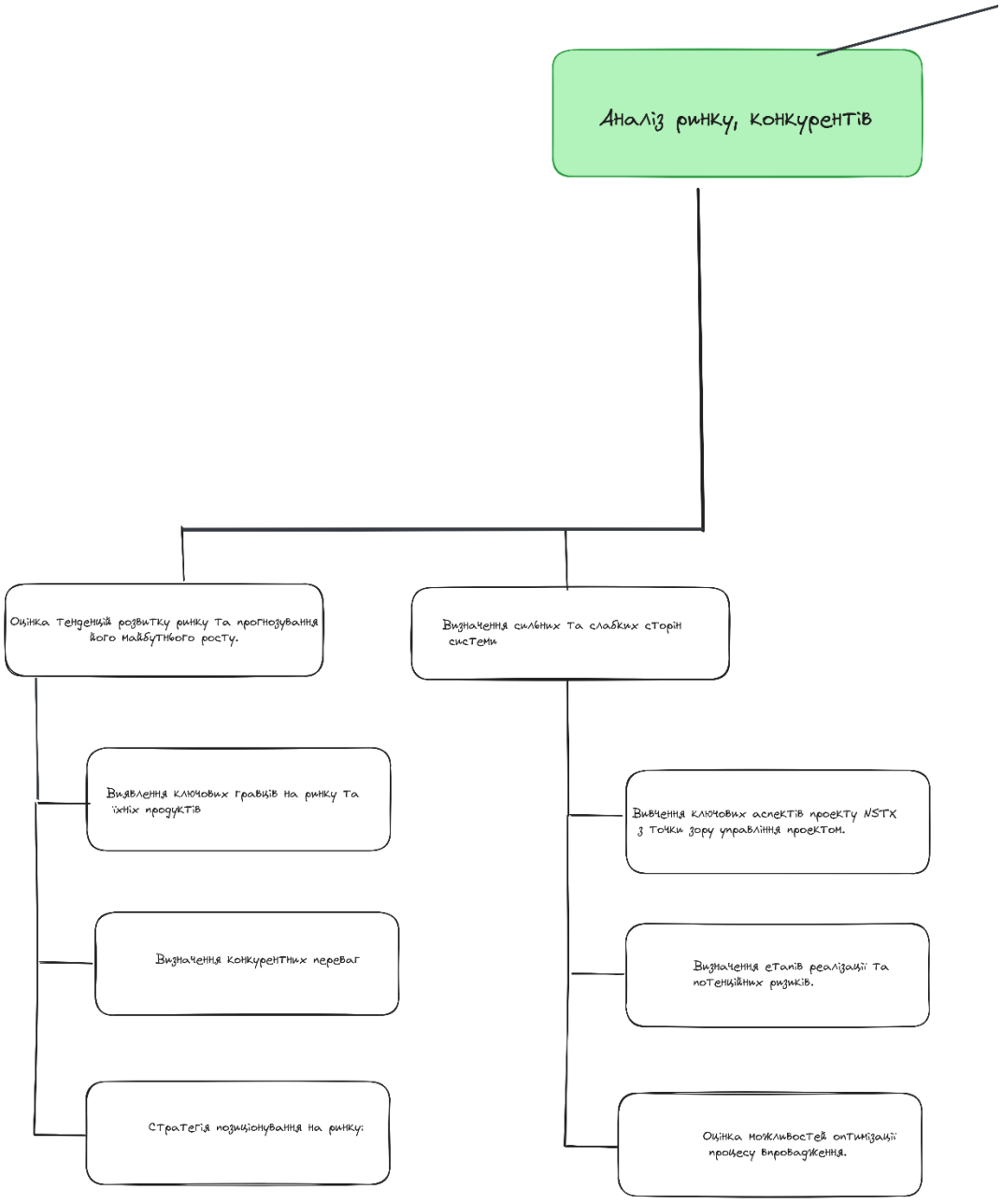


Рисунок 2.6 Дерево цілей проекту (част. 1)

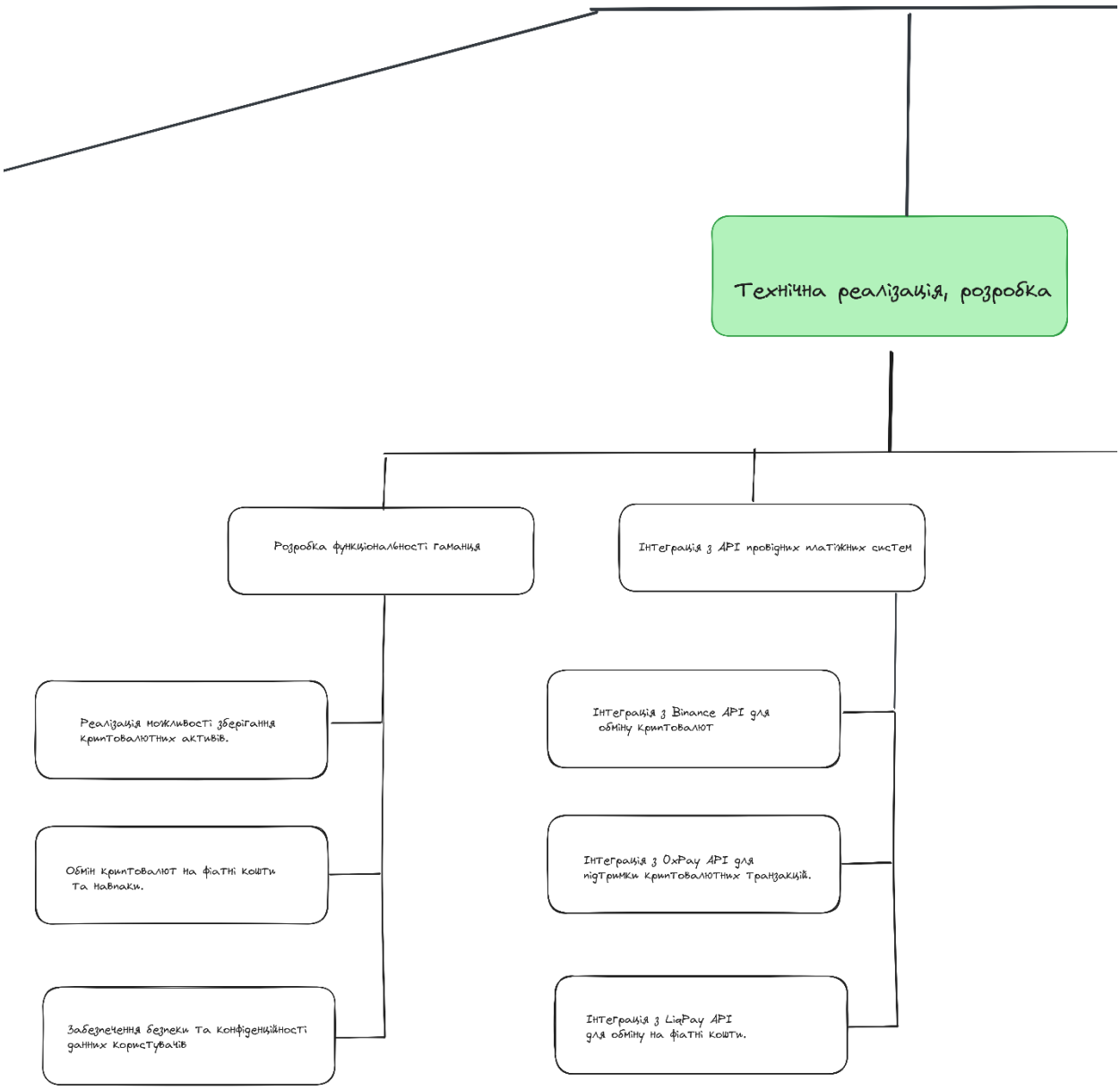


Рисунок 2.6 Дерево цілей проекту (част. 2)

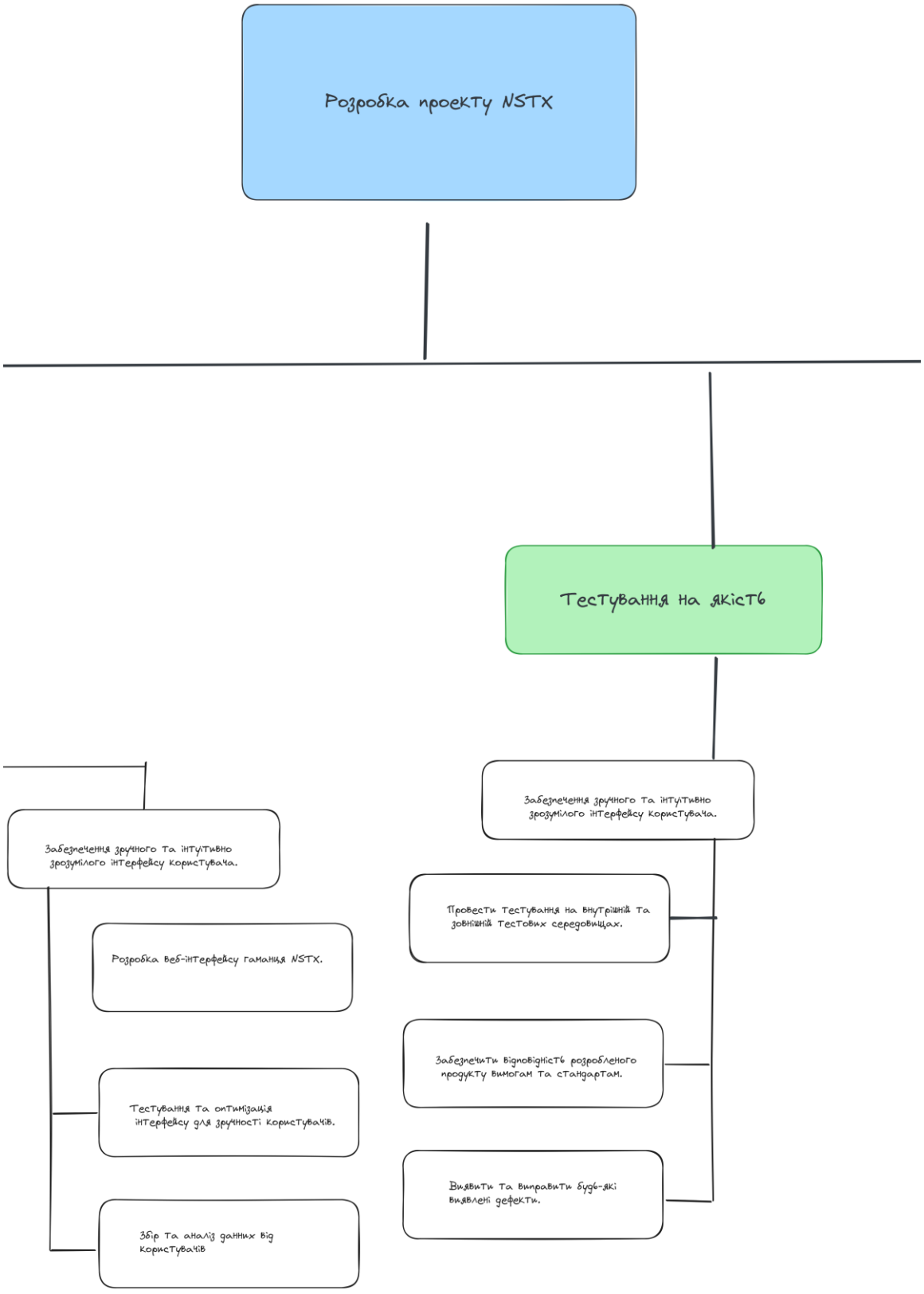


Рисунок 2.6 Дерево цілей проекту (част. 3)

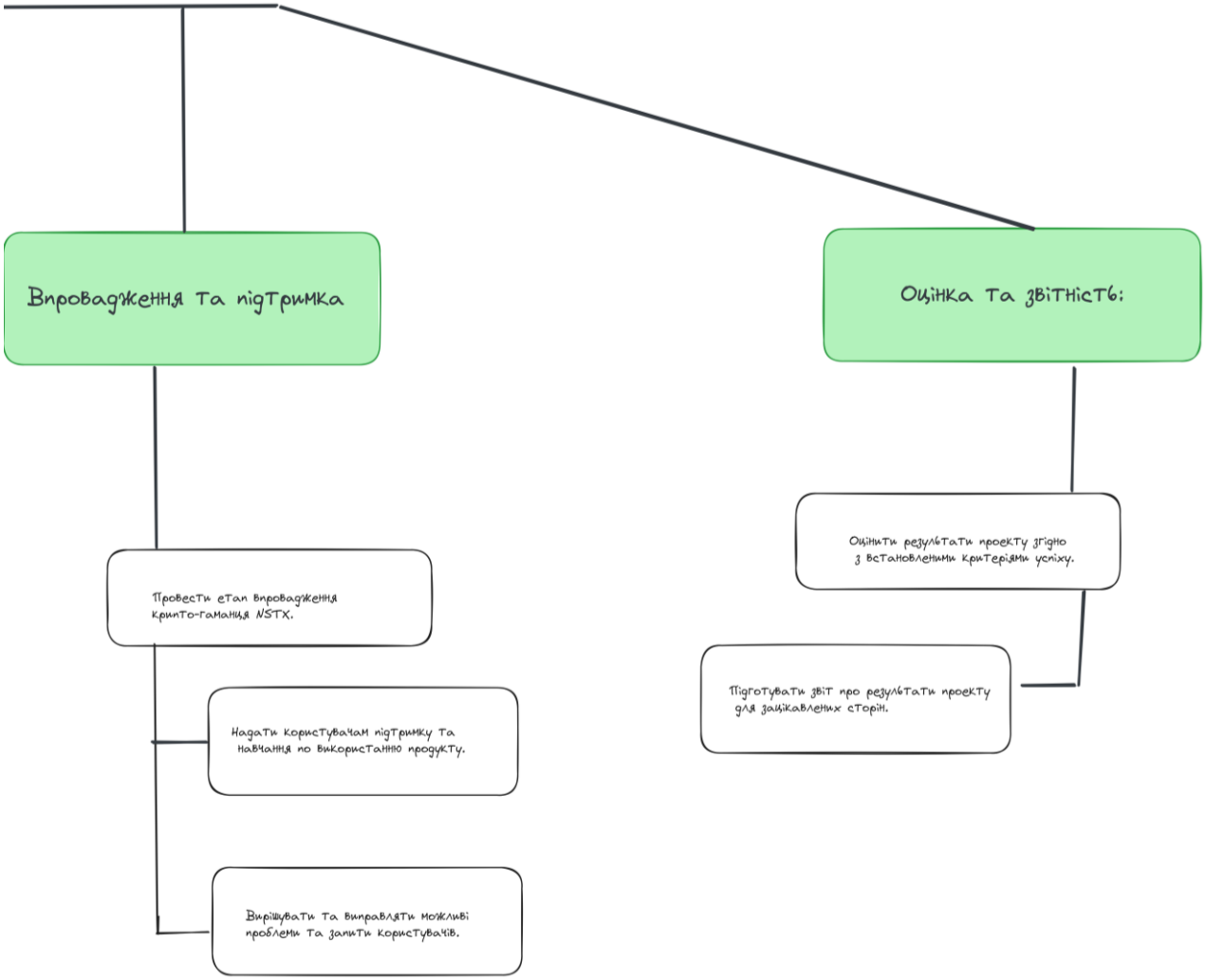
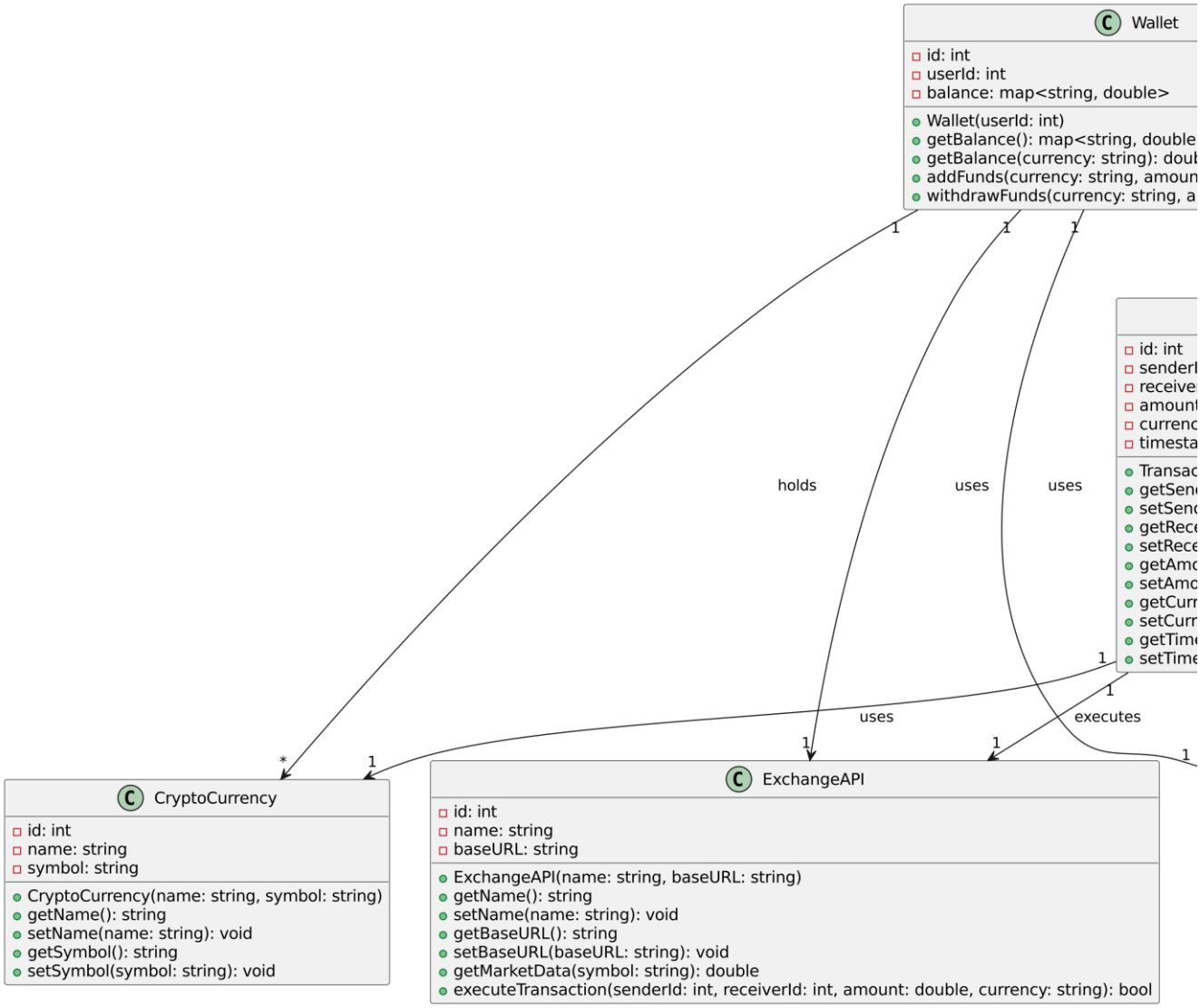


Рисунок 2.6 Дерево цілей проекту (част. 4)



лд

Рисунок 3.1 Діаграма бази даних (част. 1)

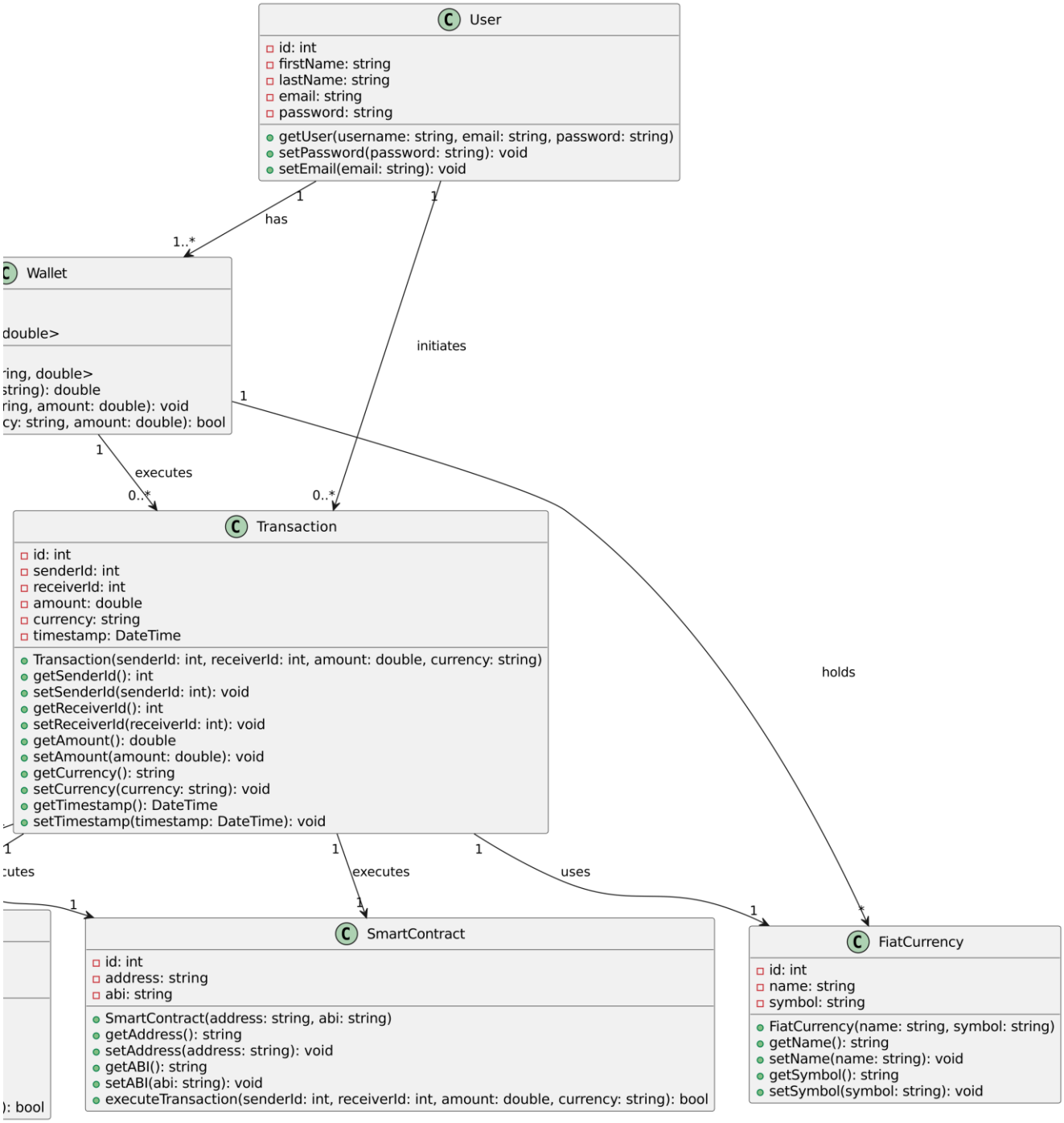


Рисунок 3.1 Діаграма бази даних (част. 2)

Додаток 9

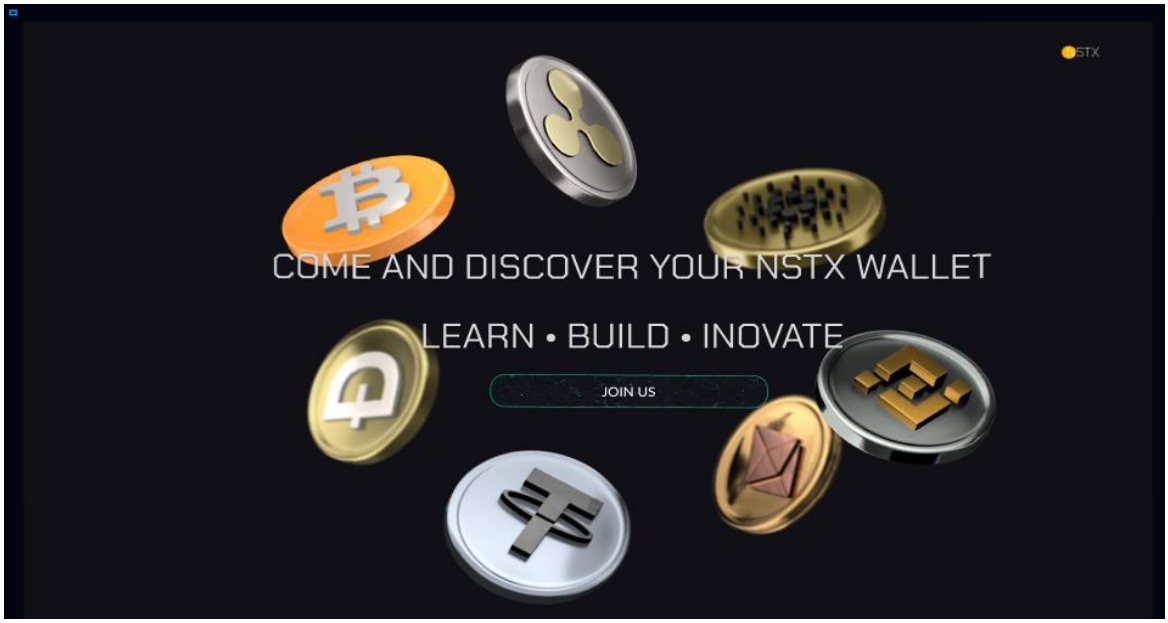


Рисунок 3.10 Дизайн онлайн криптогаманця

Додаток 10

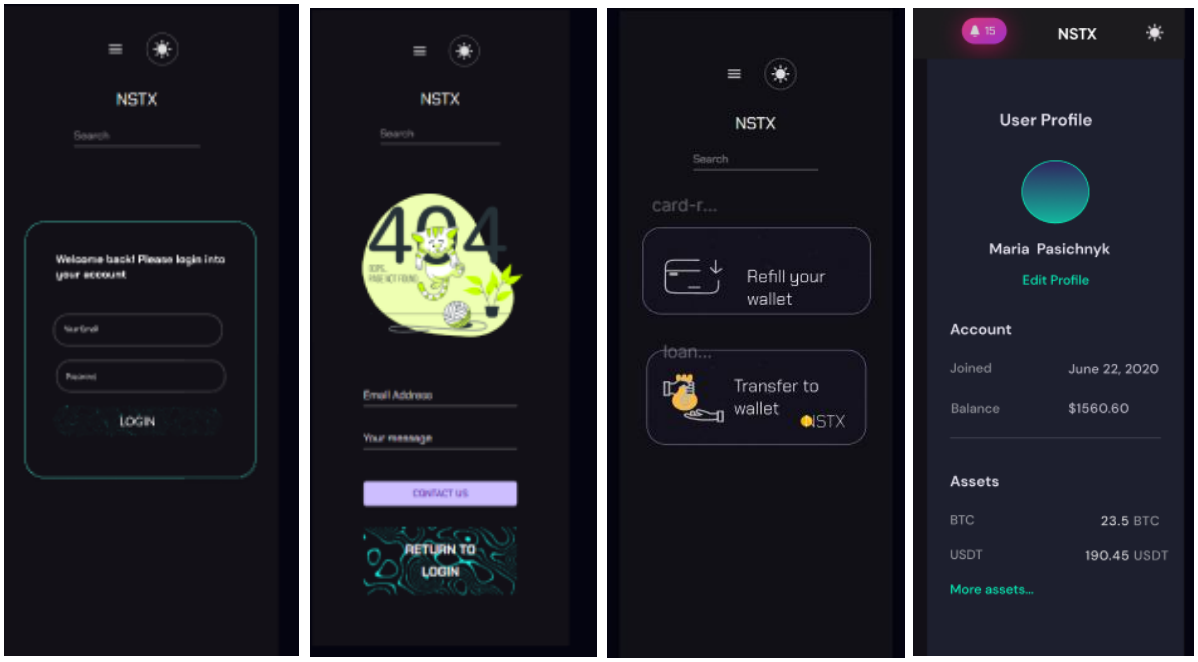


Рисунок 3.11 Дизайн онлайн криптогаманця

Додаток 11

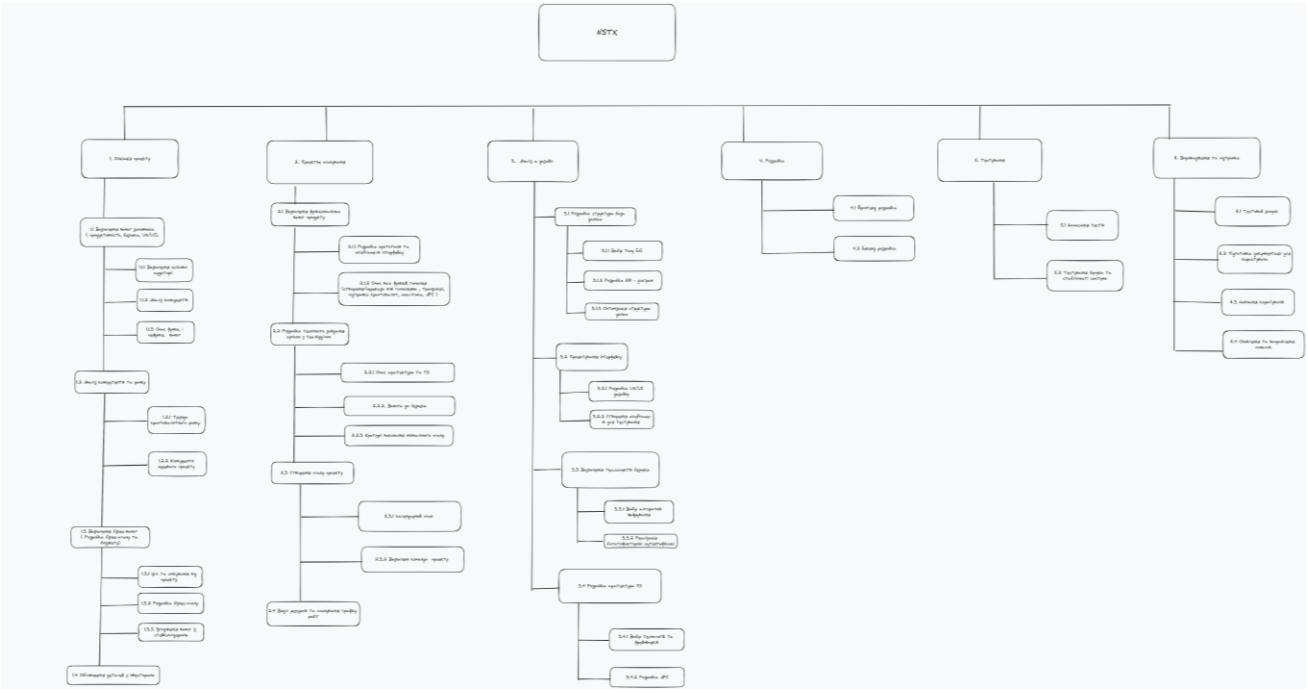


Рисунок 4.1 Завдання проекту

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. Інтернет-ресурс

1.Anahit Avetisyan. Biggest crypto hacks Q1 , 2024 [Електронний ресурс] // – Режим доступу: https://gncrypto.news/news/biggest-crypto-hacks-in-q1-2024/

2.Binaryx. DeFi - революційна технологія у наданні децентралізованих фінансових послуг – [Електронний ресурс] // – Режим доступу: https://www.binaryx-hub.com/blog/defi-revolucijna-texnologija?utm_source=google&utm_medium=cpc&utm_term=defi%20%D1%86%D0%B5&utm_campaign=csr&gad_source=1&gclid=CjwKCAjw1K-zBhBIEiwAWeCOF4-cOs8CdpuM6iuzsDCkt7WTlRU76zGydL1D3fT5z_2vGwTkh3I7GRoCT_EQAvD_BwE

3.Chainalysis 2023 Crypto Crime [Електронний ресурс] // – Режим доступу: https://go.chainalysis.com/2023-Crypto-Crime-Report.html

4.CoinGesko Cold Wallet Exodus. Дослідження холодного гаманця Exodus [Електронний ресурс] // – Режим доступу: https://www.coingeckoë.com/learn/hot-wallet-vs-cold-wallet

5.CoinGesko User Expirience Survey 2022 – Дослідження користувацького досвіду використання криптогаманців [Електронний ресурс] // – Режим доступу: https://www.coingecko.com/en/research/publications/crypto-user-experience-survey-2022

6.CryptoCompare. Графіки цін та порівняння криптовалют – [Електронний ресурс] // – Режим доступу: https://www.cryptocompare.com/

7.Delloitte internal-auditors-guide-to-blockchain – What Is a Spot Bitcoin [Електронний ресурс] // – Режим доступу:https://www2.deloitte.com/us/en/pages/risk/articles/internal-auditing-guide-to-blockchain.html

8. DappRadar. The World’s Dapp Store – [Електронний ресурс] // – Режим доступу:DappRadar - The World’s Dapp Store | Blockchain Dapps Ranked

8. Elliptic. Thevstate of Bitcoin – [Електронний ресурс] // – Режим доступу https://www.elliptic.co/resources/state-of-cross-chain-crime-report

9.IEEEXPLORE. IEEE Access Special Section Editorial: Blockchain Technology: Principles and Applications – [Електронний ресурс] // – Режим доступу: https://ieeexplore.ieee.org/abstract/document/9509863

10.Jacob Wade Forbes Media LLC – What Is a Spot Bitcoin [Електронний ресурс] // – Режим доступу: https://www.forbes.com/advisor/investing/cryptocurrency/spot-bitcoin-etfs/#:~:text=With%20the%20approval%20of%20spot,More%20liquidity.

11.Jacob Wade. SPOT Bitcoin ETFs : 2024– What Is a Spot Bitcoin [Електронний ресурс] // – Режим доступу: https://www.forbes.com/advisor/investing/cryptocurrency/spot-bitcoin-etfs/#:~:text=With%20the%20approval%20of%20spot,More%20liquidity

12.Kraken, Proof-of-Work vs. Proof-of-Stake Securing the chain– What Is a Spot Bitcoin [Електронний ресурс] // – Режим доступу:https://www.kraken.com/ru-ru/research#ki_reports_monthly_reports

13.Ledger Nano X // Холодний криптогаманець – [Електронний ресурс] // – Режим доступу: https://shop.ledger.com/ru/products/ledger-nano-x/pastel-green.

14.MC.today. – Криптовалюта [Електронний ресурс] // – Режим доступу: https://mc.today/uk/kriptovalyuta/

15.SimilarWeb. Інструмент аналізу трафіку веб-сайтів – [Електронний ресурс] // – Режим доступу : https://www.similarweb.com/

16.The Chainalisis Crypto Crime 2024 [Електронний ресурс] // – Режим доступу: https://go.chainalysis.com/crypto-crime-2024.html

17.The Economist. What are stablecoins, such as Tether? – [Електронний ресурс] // – Режим доступу: https://www.economist.com/the-economist-explains/2021/12/16/what-are-stablecoins-such-as-tether

18.The Economist. What is an NFT? – [Електронний ресурс] // – Режим

доступу: https://www.economist.com/the-economist-explains/2021/10/12/what-is-an-nft?ppccampaignID=&ppcadID=&ppcgclID=&utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=18151738051&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-response.anonymous&gad_source=1&gclid=CjwKCAjw1K-zBhBIEiwAWeCOFznmLFP_mLgyfuORDT8M8OGLZC5yUtELY3BS7hX0dPNEayxJfwhK9xoCBkMQAvD_BwE&gclsrc=aw.ds

19.Trezor // Холодний криптогаманець – [Електронний ресурс] // – Режим доступу: – https://trezor.io/.

20.Trezor. – Supported coins // Звіт – [Електронний ресурс] // – Режим доступу: https://trezor.io/learn/c/supported-coins

21.Vilius Barbaravičius. Coingate – Record Year for Crypto Payments Growth: 2023 Report [Електронний ресурс] // – Режим доступу: https://coingate.com/blog/post/crypto-payments-report-2023

22.Investopedia – What Is a Blockchain[Електронний ресурс] // – Режим доступу: https://www.investopedia.com/terms/b/blockchain.asp

23.Кредобанк. Обмеження на перекази та зняття коштів – [Електронний ресурс] // – Режим доступу: https://kredobank.com.ua/private/stay-safe/questions

24.CoinDesk. Here's Why Bitcoin's Not Keeping Pace With Nasdaq – [Електронний ресурс] // – Режим доступу: https://www.coindesk.com/

2. Книга

25.Andreas Antonopoulos. Mastering Bitcoin: Programming the Open Blockchain 2nd Edition. – Sebastopol, CA, USA. O'Reilly Media – 704 ст. – 2023.

26.Extreme Programming (XP) – Ron Jeffries , Mike Hendrickson , Ann Anderso – CA, USA. Addison-Wesley – 2021. – 401 ст.

3. Стаття

27. DeCloak – Enable Secure and Cheap Multi-Party Transactions on Legacy Blockchains by a Minimally Trusted TEE Network – Qian Ren; Yue Li; Yingjun Wu; Yuchen Wu; Hong Lei; Lei Wang; Bangdao Chen // Академічний журнал Publication Year – 2024, Page(s): 88 – 103

28.Financial Crimes Enforcement Network. "FAQs: Final CIP Rule," Pages 1, 8.

29.Xu Song. Institute of Electrical and Electronics Engineers IEEE Transactions on Information Forensics and Security – Xu Song,Saihui Hou,Yan Huang,Chunshui Cao,Xu Liu,Yongzhen Huang // Академічний журнал – 2024.

4. Додаткові посилання

30.Google Drive. Pasichnyk M.S – Діаграма цілей проекту – [Електронний ресурс] //Режимдоступу: https://drive.google.com/file/d/1fy3aTSC1T7B8ulh3XjRS4nfhZNmTcN4t/view

31.Google Drive. Pasichnyk M.S – Діаграма взаємодії з Etherum Virtual Machine – [Електронний ресурс] // – Режим доступу: https://drive.google.com/file/d/1b9_E4EaEl1yqCjtkwmB7NXwY4CuZIpN9/view?usp=sharing

32.Google Drive. Pasichnyk M.S – Алгоритм смарт-контракт в Blockchain ETH– [Електронний ресурс] // – Режим доступу:

https://drive.google.com/file/d/1b9_E4EaEl1yqCjtkwmB7NXwY4CuZIpN9/view?usp=sharing

33.Google Drive. Pasichnyk M.S – Діаграма Blockchain транзакції – [Електронний ресурс] // – Режим доступу : https://drive.google.com/file/d/1b9_E4EaEl1yqCjtkwmB7NXwY4CuZIpN9/view?usp=sharing

34.Google Drive. Pasichnyk M.S – Діаграма бази даних – [Електронний ресурс] // – Режим доступу : https://drive.google.com/file/d/1-0zq4Q-ZUMi5S0Scl0blKwqNwwoAfb0i/view

35.Google Drive. Pasichnyk M.S – Ризики проекту – [Електронний ресурс] // – Режим доступу: XT7M7X9JgfGVzQo/edit?gid=0#gid=0

36.Figma. Pasichnyk M.S – Макет дизайну проекту – [Макет сайту] // – Режим доступу: https://www.figma.com/design/gA0nvxVPRFKOVwKfzwiAR0/Untitled?m=dev&node-id=66-1047&t=2rnGG9kiQsaGRHP2-1

37. Symantec. Internet Security Threat Report 2022 – [Електронний ресурс] // – Режим доступу: https://www.insight.com/en_US/content-and-resources/brands/symantec/internet-security-threat-report.html