Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

Галузь знань 12 – Інформаційні технології

Спеціальність 123 –Комп'ютерна інженерія

на тему «*Блокчейн-базована система підтримки криптовалютних операцій для ОС Android*»

КвРКІП. 180244.18.02.28 ПЗ

Виконав: студент 2 курсу, група КІ2м-22-1 _____ Тимчук П.В.
Ініціали, прізвище

Керівник доцент _____ Грига В.М.
Науковий ступінь, вчене звання Підпис Ініціали, прізвище

До захисту допускаю:
Зав. кафедри КІІС, д.т.н., проф.
Т.О. Говорущенко
30 05 2024 р.

Хмельницький, 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Комп'ютерної інженерії та інформаційних систем

Освітній рівень магістр

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма Освітньо-наукова програма «Комп'ютерна інженерія та програмування»

ЗАТВЕРДЖУЮ

Зав. кафедри Т.О.Говорущенко

"01" 09 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Тимчуку Петру Володимировичу
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Блокчейн-базована система підтримки криптовалютних операцій для ОС Android

Керівник проекту (роботи) Говорущенко Т.О., д.т.н., професор
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 09.01.2024 р. № 1

2. Строк подання студентом проекту (роботи) на кафедру 01.05.2024 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Технічний огляд блокчейн-базованої системи

Проектування архітектури системи

Реалізація блокчейн-базованої системи

Дослідження та інновації у блокчейн-базованих системах

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6. Консультанти розділів кваліфікаційної роботи магістра

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прий
Нормоконтроль	Лисенко С.М., професор кафедри КІС		
Антиплагіат	Нічепорук А.О., доцент кафедри КІС		

7. Дата видачі завдання «_06_»_____09_____2022р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи магістра	Термін виконання етапів проекту (роботи)	Примі
1	Вибір напряму дослідження та узгодження тематики КвРМ з керівником	05.09.2024	викона
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	05.10.2024	викона
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	05.11.2024	викона
4	Робота над розділом 2 – розробка моделей для вирішення поставленої задачі	05.12.2024	викона
5	Робота над науковою статтею	05.01.2024	викона
6	Робота над розділом 3 – розробка методів для вирішення поставленої задачі	15.02.2024	викона
7	Робота над розділом 4 – проектування та розробка ПЗ для вирішення поставленої задачі, експериментальна частина	05.04.2024	викона
8	Оформлення пояснювальної записки згідно вимог	15.04.2024	викона
9	Попередній захист ДРМ	18.04.2024	викона
10	Захист ДРМ на засіданні ЕК	До 10.05.2024	

Студент _____ П.В. Тимчук
Підпис Ініціали, прізвище

Керівник роботи _____ В.М. Грига
Підпис Ініціали,

РЕФЕРАТ

Тема кваліфікаційної роботи магістра: Блокчейн-базована система підтримки криптовалютних операцій для ОС Android.

Автор роботи: Тимчук Петро Володимирович

Керівник роботи: Грига Володимир Михайлович

Пояснювальна записка: 95 с., 34 рис., 12 табл., 3 дод., 86 джерел.

КРИПТОВАЛЮТА, ХЕШИНГ, БЛОКЧЕЙН, ОПЕРАЦІЇ, ТЕСТУВАННЯ, ANDROID, СИСТЕМА, ПІДТРИМКА.

Об’єктом дослідження є процес розроблення системи підтримки криптовалютних операцій для ОС Android.

Предметом дослідження є аналітика мобільного додатку на базі Android базованої-блокчейн системи.

Метою кваліфікаційної роботи магістра є розроблення мобільного додатку блокчейн-базованої системи на базі ОС Android.

Для розв’язання поставлених задач використовувалися методи тестування програми написаної на базі C++, а аткож аналітика всього періоду існування криптовалюти.

Наукова новизна отриманих результатів:

− набув подальшого розвитку алгоритм хешування, який ускладнює підбір варіантів для вирішення криптографічних завдань та у порівнянні з відомими має менший час генерації одного блока даних на 20%.

− набула подальшого розвитку інформаційна технологія, яка використовується для управління транзакціями криптовалюти на мобільних пристроях та включає нові механізми безпеки, такі як біометрична автентифікація та захист даних на основі криптографії. Це було досягнуто за допомогою впровадження нових програмних і технічних рішень, які спрямовані на підвищення захищеності користувацьких даних і оптимізацію взаємодії з блокчейном.

Практична значимість отриманих результатів полягає у надані користувачам Android використовувати базовану-блокчейн систему підтримки для операцій на даній платформі та в зручному використанні багатьох можливих криптовалютних ресурсів.

Публікації. За темою кваліфікаційної роботи опубліковано тези на XXIV Всеукраїнській науково-технічній конференції молодих вчених, аспірантів та студентів «СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ» [86].

Структура та об’єм кваліфікаційної роботи. Кваліфікаційна робота складається з вступу, чотирьох розділів, висновку та додатків, її повний зміст сторінок, основний зміст викладено на 95 сторінках, 4-х додатків, містить 34 рисунки, 12 таблиць, включає 86 найменувань вітчизняної та зарубіжної літератури

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

АПЗ - антивірусне програмне забезпечення

БД - база даних

БПР - блок прийняття рішень

ГА - генетичний алгоритм

ОС - операційна система

ПЗ - програмне забезпечення

СВВ - система виявлення вторгнень

ЕС - експертна система

DDoS - Distributed Denial of Service (розподілена відмова в обслуговуванні)

IDS - система виявлення вторгнень

АС – автоматизована система.
ПІР – клієнт, що бере участь у роздачі.
ІС – інформаційна система.
ПЗ – програмне забезпечення.
ПП – програмний продукт.
БД – база даних.
ASIC – інтегральна схема для специфічного застосування.
FPGA – програмована користувачем вентильна матриця.
GPU – графічний процесор.
CPU – центральний процесор.
RAM – оперативна пам'ять.
SEED – багатослівний термін.
P2P – пірінгова мережа.
Хеш – функція, що перетворює вхідні дані будь-якого розміру в дані фіксованого розміру.

ВСТУП

У сучасному світі криптовалюти та технології блокчейну набули значного значення в економіці, фінансах та інших сферах. Це привело до необхідності розробки та впровадження нових інноваційних систем, спрямованих на поліпшення та забезпечення безпеки операцій з криптовалютами. Однією з таких систем є блокчейн-базована система підтримки криптовалютних операцій для операційної системи Android [1-3].

Актуальність роботи. З урахуванням швидкого розвитку ринку криптовалют та зростаючої популярності мобільних платформ, важливо розробити зручні та безпечні інструменти для керування криптовалютними активами безпосередньо з пристроїв на базі ОС Android. Блокчейн-базована система підтримки криптовалютних операцій відповідає цим потребам та може стати ефективним інструментом для користувачів криптовалют.

Поставленою метою є розробка та реалізація функціональної та безпечної системи підтримки криптовалютних операцій для операційної системи Android. Ця мета досягається шляхом вирішення наступних основних завдань:

1. Аналіз технологій блокчейну та криптовалют.
2. Визначення потреб користувачів та функціональних вимог до системи.
3. Розробка та реалізація системи підтримки криптовалютних операцій для ОС Android.
4. Тестування та оцінка ефективності розробленої системи.

Окрім того, у даній роботі використовується підхід машинного навчання для покращення безпеки та забезпечення автоматичного виявлення та усунення можливих загроз безпеці в операціях з криптовалютами. Моделі машинного навчання використовуються для аналізу транзакцій та ідентифікації потенційно шкідливих дій користувачів.

Окрім того, у даній роботі викладено вимоги до методології, які включають в себе використання методів машинного навчання для покращення безпеки та

забезпечення автоматичного виявлення та усунення можливих загроз безпеці в операціях з криптовалютами.

Для розв’язання поставлених задач використовуються основні положення**:**

5. Принципи блокчейн технології**:** Глибокий розуміння принципів роботи блокчейну дозволить ефективно розробити систему, яка забезпечить надійну та безпечну підтримку криптовалютних операцій на платформі Android.

6. Методи машинного навчання**:** Використання алгоритмів машинного навчання допоможе виявляти та протидіяти можливим загрозам безпеки, а також покращить виявлення шаблонів операцій користувачів для підвищення ефективності та безпеки системи.

7. Аналіз потреб користувачів: Вивчення та аналіз потреб користувачів дозволить врахувати їхні вимоги та забезпечити зручний та інтуїтивно зрозумілий інтерфейс системи для оптимального взаємодії з нею.

8. Функціональні вимоги до системи: Визначення та формулювання функціональних вимог до системи допоможе чітко визначити функції, які система повинна виконувати, та забезпечить відповідність вимогам користувачів.

9. Розробка та реалізація системи: Система буде розроблена з використанням сучасних методів програмування та відповідатиме стандартам безпеки та ефективності.

1 ОГЛЯД ТА АНАЛІЗ БЛОКЧЕЙН-БАЗОВАНОЇ СИСТЕМИ

1.1 Роль блокчейн технології в криптовалютних операціях

Blockchain забезпечує безпечне зберігання важливих даних. У своїй відомій формі розподілені бази даних складаються з блоків, які посилаються один на одного у вигляді ланцюга. спеціально створений код, який базується на даних конкретного блоку за допомогою певного алгоритму. Хеш гарантує, що дані в блоці будуть захищені. Ви можете взяти блок, змінити його дані та створити новий хеш.Independent reweaving: коли блокхешу змінюється, він змінюється, що є явним порушенням і є транзакцією, яка може бути помічена. Незважаючи на те, що спроба змінити послідовність блокчейну та хешувати транзакції порушить стабільність системи. Ця система може зберігати медичні, контракти, фінансові та логістичні дані.Створення смарт-контрактів за допомогою технології блокчейну може автоматизувати виконання угод без посередництва третьої сторони. Основні переваги блокчейну включають високий рівень безпеки, децентралізацію (немає центрального керування), невід'ємність (всі дані в блокчейні можуть бути вилучені або змінені без згоди більшості учасників системи) і прозорість (всі дані доступні для всіх учасників мережі). У сучасному світі блокчейн технологія є важливою, впливаючи на багато сфер життя та галузі економіки. Вона гарантує децентралізацію, тобто відсутність централізованого контролю над даними, що робить її надійним і незмінним, зображено на рисунку 1.1.

Блокчейн може підвищити відкритість фінансових операцій, усунути проміжності та значно спростити та зменшити вартість транзакцій у фінансовому секторі. В інших сферах, таких як логістика, медицина, нерухомість і урядова служба, блокчейн може покращити ефективність адміністративних процесів, ідентифікацію людей, безпеку медичних записів і відстеження даних. Крім того, блокчейн дозволяє створювати програми, відомі як «розумні контракти», які автоматично виконують умови договору в певних обставинах.

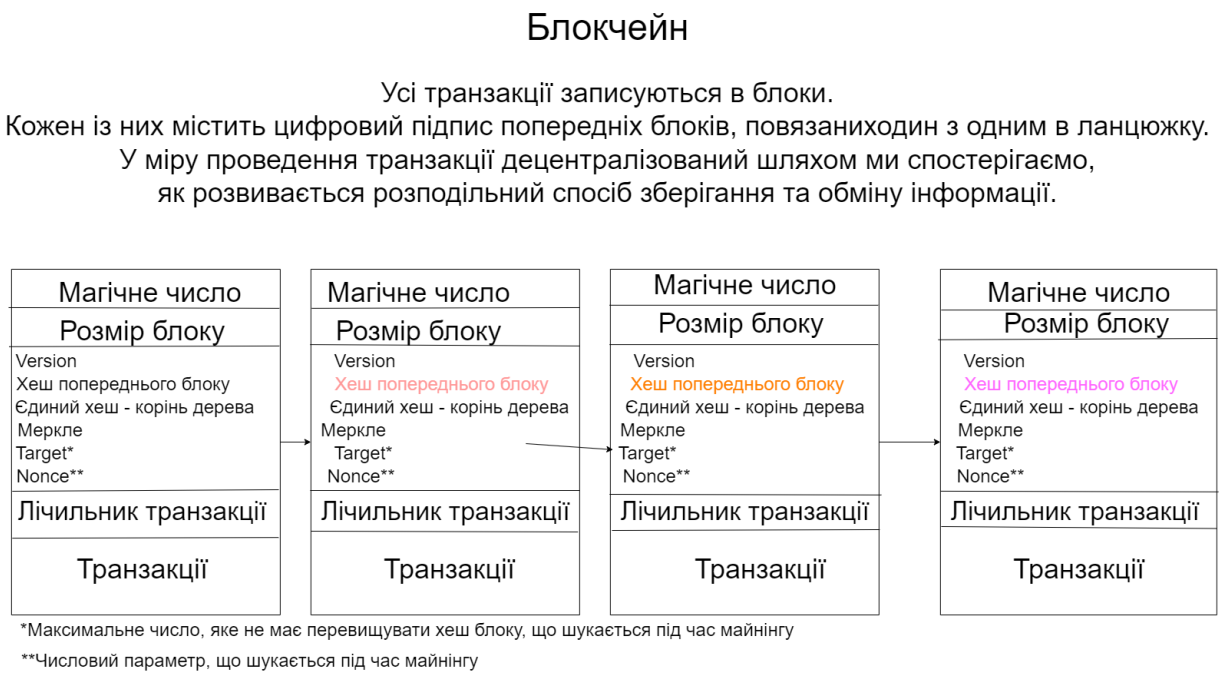


Рисунок 1.1 – Схема технології блокчейну

Блокчейн створює безпечні та невідмінні записи, які можна використовувати для ведення договорів, ідентифікації осіб, зберігання та передачі цифрових активів та багато іншого. Крім того, ця технологія відкриває двері для нових інноваційних застосувань, які можуть покращити ефективність бізнесу, зробити гроші прозорішими та покращити доступність послуг для всіх користувачів. Насправді блокчейн-технологія має значно ширший спектр застосування, ніж те, що зазвичай асоціюється з криптовалютами. Вона стала революційною технологією, яка змінює спосіб сприйняття та обробки даних, забезпечуючи відкритість, невідмінність, безпеку та децентралізацію.

Це робить блокчейн придатним для використання в будь-якій сфері, де є потреба в стандартизації та автоматизації процесів.

Таким чином, ключова функція блокчейну в сучасному світі полягає в тому, щоб він був інструментом для створення надійних, децентралізованих систем обміну інформацією та цифрових активів, які гарантують безпеку, ефективність і відкритість для всіх користувачів.

Розвиток і дослідження в галузі блокчейн технологій продовжують розширювати їхні застосування та можливості. Інтеграція блокчейну з іншими

технологіями, такими як штучний інтелект (ШІ), Інтернет речей (IoT) та обчислення на краю (edge computing), є одним із таких напрямків. Наприклад, блокчейн може використовуватися для захисту та безпеки даних, зібраних з пристроїв IoT, а також для забезпечення безпеки та конфіденційності в Інтернеті речей.

Це особливо важливо в областях, де збирається велика кількість даних, наприклад у сферах охорони здоров'я, логістики та виробництва. Що стосується штучного інтелекту, блокчейн може бути використаний для створення децентралізованих систем обробки та аналізу даних. Це дозволяє різним джерелам зберігати та обмінюватися даними без потреби в централізованих платформах. Обчислення на краю, також відоме як обчислення на краю, стосується обробки даних на пристроях, які знаходяться ближче до їх джерела. Блокчейн дозволяє створювати розподілені системи обробки даних, які використовують можливості кожного пристрою в мережі, щоб забезпечити довіру та безпеку в обчисленнях на краю.

Таким чином, інтеграція блокчейну з іншими сучасними технологіями може призвести до нових можливостей і розширити сфери застосування технології в різних сферах життя. Технологія є життєво важливою для безпеки, надійності та прозорості транзакцій криптовалюти. У блокчейні записується кожна транзакція, яка відбувається в криптовалютній мережі. Кожен блок потім зв'язується з іншими блоками, утворюючи ланцюжок. Кожен у мережі може перевірити та переглянути журнал транзакцій, створений за допомогою цієї процедури, яка дозволяє створювати журнал транзакцій, який не може бути змінений.

Використовуючи криптографію, блокчейн-технологія гарантує безпеку та невідмінність даних. Кожна транзакція підписується цифровим підписом, який гарантує, що вона автентична та непорушна. Крім того, блокчейн є системою, яка є децентралізованою, що означає, що дані не зберігаються в одному місці, а розподіляються по різним частинам мережі. Оскільки необхідно отримати контроль над більшістю вузлів, спроби змінити або підмінити дані стають складними.

Прозорість є важливою частиною блокчейн-технології в криптовалютних транзакціях. Як наслідок того, що журнал транзакцій доступний для всіх учасників

мережі, кожен може перевірити та підтвердити легітимність будь-якої транзакції. Оскільки спільнота користувачів знайде та усуне будь-які незаконні дії, це запобігає шахрайству та підозрілим діям.

Підводячи підсумок, блокчейн-технологія забезпечує безпеку, невідмінність і прозорість транзакцій для криптовалютних операцій. Вона дозволяє учасникам мережі будувати довірчі відносини та забезпечує стійкий до змін і атак журнал транзакцій.

Це досягається завдяки наявності консенсусного протоколу, який є основною частиною будь-якої мережі Blockchain. Алгоритм консенсусу — це процес, за допомогою якого всі члени мережі Blockchain досягають консенсусу щодо поточного стану розподіленої книги. Таким чином, консенсусні алгоритми створюють надійність мережі Blockchain і створюють довіру між невідомими однолітками в розподіленому обчислювальному середовищі.

По суті, консенсус-протокол гарантує, що кожен новий блок даних, який додається до блокчейну, представляє єдину версію істини, яка є узгодженою усіма компонентами блокчейну. Целі протоколу blockchain консенсусу включають досягнення згоди, співпрацю, рівні права для кожного вузла та обов’язкову участь кожного вузла в процесі консенсусу. Звідси випливає, що мета алгоритму консенсусу полягає в тому, щоб знайти спосіб досягти спільної згоди, яка буде корисною для всієї мережі.

Сам blockchain складається з блоків, і найцікавіше в тому, як ці блоки створюються під час видобутку. Заголовок і тіло blockchain складають блок (рис. 1.1).

Заголовки блокчейну складаються з неповторної послідовності символів, які ідентифікують певний блок або транзакцію в мережі блокчейну. Цей алгоритм хешування, як правило, використовується для створення цієї послідовності, яка є унікальним підписом даних, який можна використовувати для перевірки цілісності блоку. Зазвичай заголовок містить попередній хеш блоку, дані нової транзакції, дату та інші метадані, необхідні для роботи протоколу блокчейну. Заголовок блокчейну має вирішальне значення для забезпечення безпеки та надійності всієї системи, а також для створення унікальної ідентифікації кожного блоку.

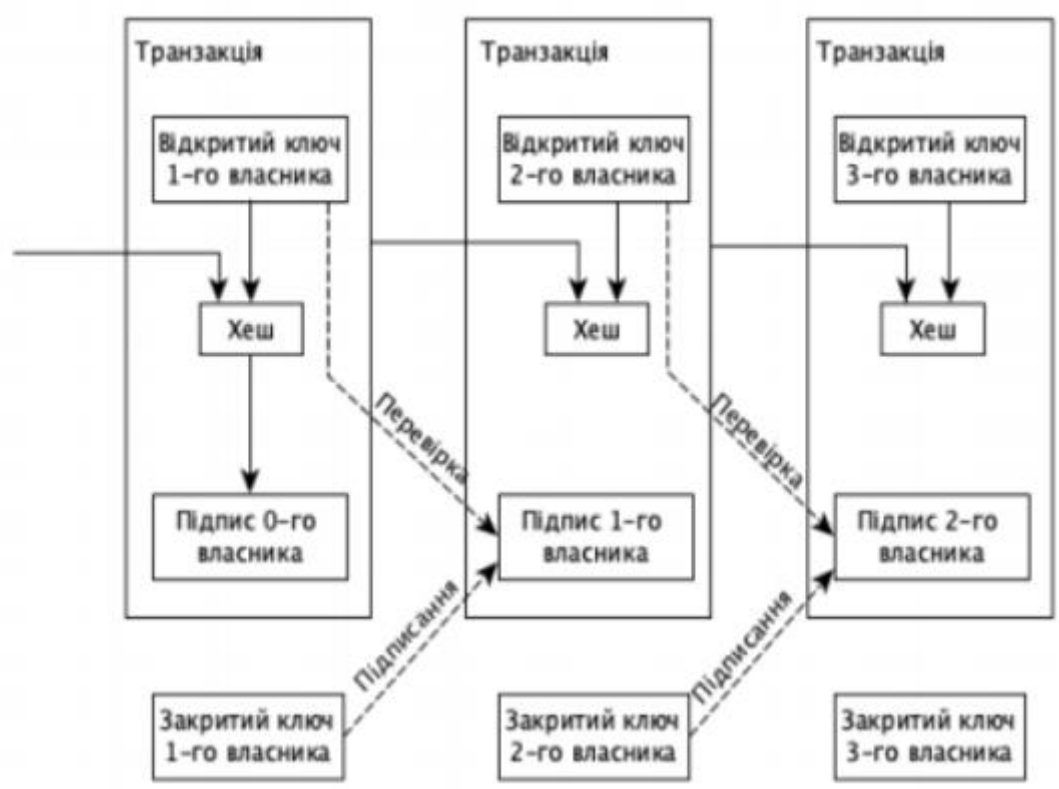


Рисунок 1.2 – Загальна схема структури ланцюга блоків

Тіло блоку містить прототип списку записів. Оскільки ключ попереднього блоку зберігається в заголовку кожного блоку, блоки в blockchain пов’язані за допомогою ключів. Це вирішальне рішення, яке також забезпечує захищеність blockchain, є технічно розумним.

1.2 Виклики та проблеми інтеграції криптовалют на мобільних пристроях

Відповідно до контексту та сфери застосування, інтеграція криптовалют може зіткнутися з різними проблемами. Одним із найпоширеніших питань є те, що широка громадськість не розуміє та не приймає криптовалют. Через те, що криптовалюти пов’язані зі злочинністю, волатильністю цін і відсутністю регулювання, багато людей не розуміють, як працюють криптовалюти і бояться їх. Регуляторні нерівності між країнами та регіонами є ще однією проблемою. Нечіткі правила щодо використання та оподаткування криптовалют у багатьох країнах ускладнюють їх використання в бізнесі та фінансових операціях. Навіть у країнах, де є закони, вони часто змінюються,

що робить планування та реалізацію проектів, пов’язаних із криптовалютами, складніше.

При інтеграції криптовалют також можуть виникнути технічні обмеження. Наприклад, масштаб блокчейнів може перешкоджати обробці великої кількості транзакцій, що обмежує їх використання в великих фінансових системах. Крім того, важливо враховувати проблеми безпеки, такі як ймовірність кібератак на біржі та гаманці криптовалют, що може призвести до втрати коштів і втрати довіри до систем.

Нарешті, проблеми зі стабільністю та нестабільністю криптовалют також можуть перешкоджати їх використанню в економічних операціях. Планування та бюджетування можуть стати складними через великі коливання цін, які також можуть підвищити ризик для компаній і споживачів. Таким чином, інтеграція криптовалют зіткнулася з низкою проблем, таких як нерівність регулювання, технічні обмеження, проблеми безпеки та волатильність цін. Розробка стратегій, які враховують ці проблеми та шукають рішення, є необхідною для успішної інтеграції цих технологій.

Складність інтерфейсу та користувацький досвід можуть викликати проблеми під час інтеграції криптовалют. Через технічну складність і неінтуїтивний інтерфейс використання гаманців для проведення транзакцій може бути складним, навіть для тих, хто досвідчений у використанні криптовалют. Це особливо важливо для масової адопції, оскільки більшість людей віддають перевагу практичності та зручності у використанні інструменти, зображено на рисунку 1.3.

Розробка блокчейн-систем залежить від практичності та простоти використання інструментів. Користувачі хочуть мати можливість ефективно використовувати технологію, не докладаючи багато зусиль або не маючи достатнього досвіду.

Інструменти повинні бути простими у використанні та не вимагати складних дій, щоб бути практичними. Це може включати інтерфейси, які легко зрозуміти, прості та зрозумілі інструкції та мінімальну потребу в ручному втручанні користувача. Наприклад, користувачі повинні мати можливість легко виконувати операції з криптовалютами або підписувати угоди через простий веб-інтерфейс або мобільний додаток без необхідності вивчати складні технічні поняття.

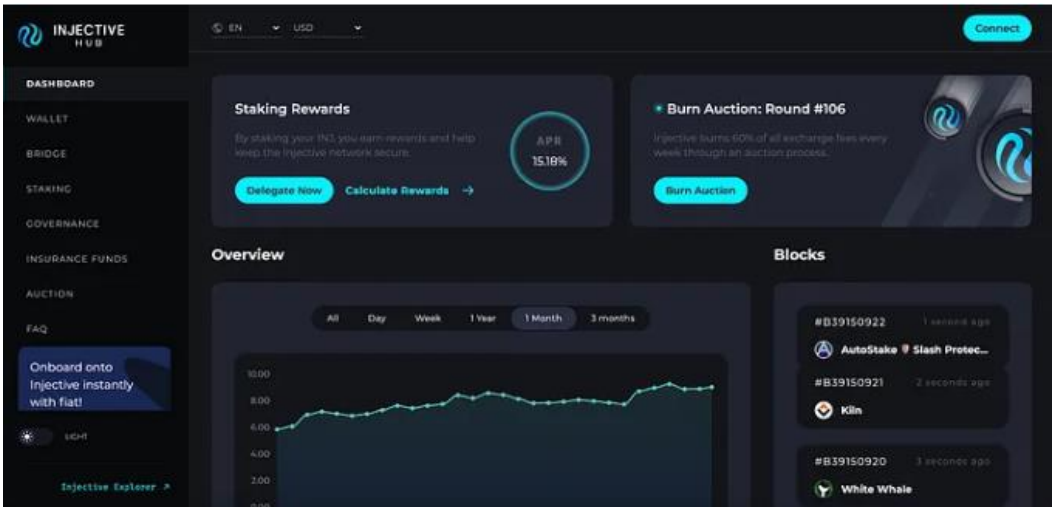


Рисунок 1.3 – Інтерфейс для використання гаманця

Крім того, велика кількість шахрайських схем, шахрайських бірж і масового обману може призвести до сумнівів щодо легітимності та надійності криптовалютних проектів. Це може призвести до зниження довіри до криптовалюти та ускладнити їх інтеграцію до фінансових і бізнес-систем. Для компаній, які хочуть приймати криптовалюту як засіб оплати, інтеграція криптовалют також може вимагати значних витрат на інфраструктуру та розробку. Розробка безпечних систем оплати, підтримка криптовалютних гаманців і інтеграція з існуючими фінансовими та бухгалтерськими системами можуть бути частиною цього.

Як наслідок, інтеграція криптовалюти потребує вирішення проблем, пов’язаних із користувацьким досвідом, легітимністю та надійністю проекту, а також значних витрат на розробку та інфраструктуру, щоб вона була успішна. Для вирішення цих проблем необхідно використовувати комплексний підхід і співпрацювати з регуляторами, учасниками ринку та технологічними партнерами, щоб створити стійку та ефективну інтеграцію криптовалют у сучасні системи.

Інтеграція криптовалют на мобільних пристроях стикається з кількома проблемами та труднощами, які варіюються залежно від технологій і умов. Безпека є однією з головних проблем. Кібератаки часто атакують мобільні пристрої, тобто їх можна взламати або використовувати для крадіжки особистих даних або криптовалют. Такі атаки можуть бути спрямовані на гаманці для зберігання криптовалют або програмне забезпечення, яке використовується для роботи з

криптовалютами. Таким чином, розробники повинні створювати найбільш безпечні засоби захисту, такі як багаторівнева аутентифікація та шифрування даних.

Складність використання та інтуїтивність інтерфейсу є ще однією важливою проблемою. Через складність і непрактичність мобільних додатків або інших інструментів, які вони повинні використовувати для отримання, зберігання або використання криптовалют, багато потенційних користувачів можуть відмовитися від криптовалют. Масштабованість також має бути врахована.

Збільшення обсягу транзакцій може призвести до проблем для відомих криптовалютних мереж, таких як Bitcoin або Ethereum. Це може призвести до затримок у проведенні транзакцій або до збільшення вартості виконання транзакцій. Мобільні пристрої мають обмежені ресурси, такі як потужність обчислення та швидкість Інтернет-з'єднання, тому масштабованість є особливо важливою, зображено на рисунку 1.4.

Рисунок 1.4 – Аналітичні дані Bitcoin, а також його монету

Загалом, інтеграція криптовалют на мобільних пристроях може стати корисним інструментом для розширення доступу до цифрових фінансових послуг, але це вимагає вирішення низки складних питань, таких як масштабованість, безпека та інтуїтивність інтерфейсу. Безпека та простота інтерфейсу є важливими для успіху впровадження блокчейн-систем.

Безпека включає захист від кібератак, забезпечення безпеки та конфіденційності даних, а також захист від несанкціонованого доступу до особистих

даних користувачів і фінансових активів. Це можна досягти за допомогою шифрування даних, двофакторної аутентифікації, аудиту безпеки та постійних патчів і оновлень для виправлення вразливостей.

Щоб інтерфейс був простим для користувачів, вони повинні знати, як використовувати систему без додаткових інструкцій. Це можна зробити за допомогою чітко зрозумілої навігації, зрозумілих піктограм і мінімального використання технічного жаргону. Інтерфейс повинен бути простим у використанні навіть для людей, які не знайомі з технікою.

Якщо хочете використовувати криптовалюту на мобільних пристроях, ви можете зіткнутися з ще однією проблемою: ви повинні знати, як працювати зі стандартними фінансовими системами. Через регуляторні обмеження або страх перед новими технологіями банки та інші фінансові установи можуть відмовитися співпрацювати з компаніями, які пропонують послуги з криптовалюти. Користувачі, які хочуть обмінювати криптовалюти на традиційні фіатні валюти або здійснювати перекази між різними фінансовими системами, можуть зіткнутися з проблемами через це.

Проблема стійкості гаманців і мобільних додатків також має бути врахована. Втрата приватного ключа та інші види атак можуть зашкодити зберіганню криптовалютних активів на мобільному пристрої.

На основі порівнянь 82 функцій хешування було обрано алгоритм хешування scrypt і він був модифікований для кращого захисту даних шляхом поєднання з іншим алгоритмом хешування yescrypt, зображено на рисунку 1.5.

Коли майнери створюють монети для майбутніх транзакцій, блокчейн використовує консенсус Proof of Work.

В блокчейн-мережах доказ роботи (PoW) — це метод консенсусу, який використовується для підтвердження транзакцій і забезпечення безпеки системи. Цей метод дозволяє майнерам, учасникам мережі, вирішувати складні математичні завдання, які вимагають великих обчислювальних ресурсів. Рішення цих завдань вимагає багато часу та електроенергії, що робить процес майнінгу дорогим і ресурсомістким. Майнер отримує право створити новий блок транзакцій у блокчейні

та отримати винагороду у вигляді криптовалюти. Це рішення забезпечує цілісність і безпеку системи, оскільки його легко перевіряють інші учасники мережі. Основна ідея PoW полягає в тому, що атака на мережу стає надзвичайно дорогою через витрати на обчислювальну потужність і електроенергію, що робить атаки економічно невигідними.

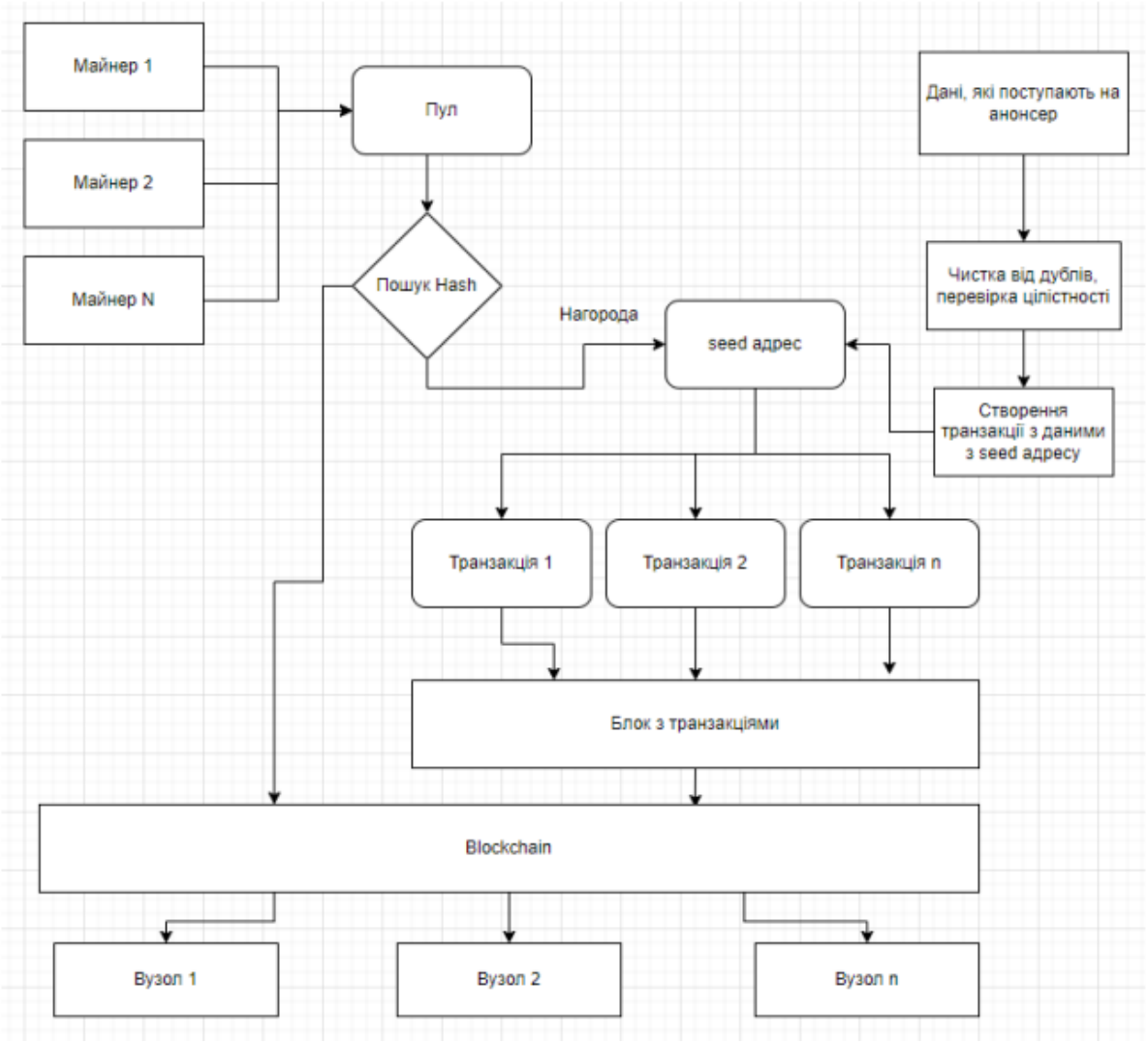


Рисунок 1.5 – Алгоритм опрацювання даних у блокчейн

1.3 Переваги використання блокчейну для операцій на платформі Android

Використання блокчейну для операцій на платформі Android має кілька значних переваг,які варто розглянути більш детально. Однією з найважливіших переваг є

безпека. За допомогою криптографічних методів шифрування та децентралізованої структури даних блокчейн забезпечує високий рівень безпеки. Надійність і безпека операцій на платформі Android підвищуються завдяки захисту інформації, яка зберігається в блокчейні, від несанкціонованого доступу та маніпуляцій. Додатковою перевагою є прозорість операцій. Блокчейн дозволяє кожному учаснику мережі переглядати та перевіряти публічний реєстр транзакцій. Оскільки користувачі можуть легко відстежувати всі етапи та дії блокчейну, це підвищує довіру до операцій.

Окрім того, блокчейн дозволяє здійснювати мікроплатежі та перекази коштів безкоштовно та миттєво. Для людей, які використовують мобільні пристрої, це особливо важливо, оскільки вони шукають простий і швидкий спосіб платити або відправляти гроші. Крім того, блокчейн дозволяє використовувати смарт-контракти, тобто програми, які автоматично виконують умови угод у певних ситуаціях. Це може спростити та автоматизувати кілька процесів, таких як оплата за послуги або переказ коштів, що призводить до більшої продуктивності та надійності.

Загалом, підтримка блокчейну в операціях на платформі Android відкриває нові можливості для безпечного, прозорого та ефективного виконання фінансових та інших операцій на мобільних пристроях. Зокрема, слід звернути увагу на те, що блокчейн може допомогти отримати доступ до фінансових послуг мільйонам людей по всьому світу, які не мають доступу до традиційних банківських установ. Люди можуть створювати фінансові інструменти, такі як мікрокредити та страхові поліси, без посередництва банків завдяки технологіям блокчейну та смарт-контрактам. Забезпечуючи доступ до необхідних фінансових послуг на мобільних пристроях, це може вирішити проблеми фінансової відокремленості мільйонів людей по всьому світу.

Крім того, блокчейн може сприяти створенню нових типів цифрових ідентифікацій, які можна використовувати для безпечного та ефективного доступу до різних платформ і послуг на мобільних пристроях. Це може включати отримання доступу до банківських послуг, реєстрацію медичних даних для отримання медичних послуг або навіть електронний бюлетень для демократичних виборів. Крім того, важливо відзначити, що блокчейн може забезпечити токенізацію та прозору систему

управління активами. Це може допомогти відкрити нові способи інвестування та торгівлі різними активами, такими як нерухомість, акції та навіть мистецтво, надаючи інвесторам у всьому світі більшу ліквідність і доступність через платформи на базі Android.

Таким чином, блокчейн відкриває нові можливості для фінансової включеності, цифрової ідентифікації та управління активами на платформі Android, що сприяє створенню фінансового світу, який є більш доступним, справедливим і продуктивним для всіх користувачів. Зокрема, блокчейн на платформі Android може підвищити надійність і прозорість постачання товарів і послуг. Додавання даних про походження продукту до блокчейну може допомогти відстежити його шлях від виробника до споживача. Це особливо корисно в сферах, де важлива точність і якість продуктів, таких як харчові продукти, ліки або продукти розкоші. Блокчейн гарантує, що інформація про товари є правдивою та недоступною для фальсифікації.

Крім того, блокчейн має потенціал сприяти розвитку нових видів культурного контенту та цифрового мистецтва. Унікальні цифрові твори мистецтва, музика, література тощо можна створювати та продавати за допомогою цифрових маркерів, які зберігаються в блокчейні. Це створює нові можливості для художників, творчих особистостей та культурних установ отримувати прямий дохід від своєї роботи. Це також дає колекціонерам можливість зберігати та торгувати цифровими активами. Однак окрім того, блокчейн може сприяти розвитку нових видів культурного контенту та цифрового мистецтва. Унікальні цифрові твори мистецтва, музика, література тощо можна створювати та продавати за допомогою цифрових маркерів, які зберігаються в блокчейні. Це створює нові можливості для художників, творчих особистостей та культурних установ отримувати прямий дохід від своєї роботи. Це також дає колекціонерам можливість зберігати та торгувати цифровими активами.

Таким чином, блокчейн на платформі Android дозволяє створювати нові цифрові твори мистецтва та культури, покращувати прозорість постачання товарів і сприяти розвитку цифрових індустрій мистецтва та культури. Використання блокчейну для операцій на платформі Android також забезпечує покращення системи голосування та підвищення участі громадян у прийнятті важливих рішень. Технологія

блокчейну дозволяє створювати надійні та безпечні цифрові системи голосування, які гарантують прозорість і неможливість фальсифікації результатів голосування. За допомогою своїх мобільних пристроїв громадяни зможуть брати участь у голосуванні, що спростить і збільшить доступність процесу, а також дозволить швидко та ефективно підрахувати результати голосування. Це може покращити демократію та залучити громадян до влади.

Крім того, блокчейн може служити основою для створення нових типів децентралізованих медіа-платформ, які дозволять творцям контенту отримувати належні винагороди за свою роботу без використання централізованих платформ. Це може допомогти створити більш прозору та справедливою систему розподілу прибутків у медіа-індустрії, а також дати творчим особам більшу свободу слова. Блокчейн також може гарантувати безпеку та захист особистих даних у сфері медичних послуг. За допомогою блокчейну медичні записи зберігаються безпечно та конфіденційно, а смарт-контракти дозволяють керувати даними. Пацієнти зможуть керувати своїми медичними даними та надавати їх медичним працівникам за потребою, що призведе до більшої ефективності та безпеки медичного обслуговування.

Таким чином, блокчейн на платформі Android може створити нові можливості для людей брати участь у демократичних процесах, створювати децентралізовані медіа-платформи та забезпечувати захист особистих даних у сфері медичних послуг. Використання блокчейну для операцій на платформі Android також дозволяє реалізувати програмні рішення для ефективного управління ланцюжком постачання. Технологія блокчейну дозволяє створити децентралізовану систему, яка може відстежувати та контролювати, як товар подорожує від постачальників до кінцевих споживачів. Компанії можуть ефективно відстежувати кожен етап ланцюжка постачання та швидко реагувати на потенційні проблеми. Такий метод підвищить ефективність і надійність постачальницького ланцюжка, а також створить більшу довіру як до бізнес-партнерів, так і до споживачів.

Створення децентралізованих ринків і платформ для обміну ресурсами є ще однією перспективою використання блокчейну на платформі Android. Блокчейн

дозволяє створювати майданчики, на яких користувачі можуть обмінюватися різними активами, включаючи цифрові токени, валюту та медичні послуги. Це збільшує конкуренцію та інновації на ринку, відкриває нові можливості для бізнесу та окремих осіб отримати доступ до різноманітних ресурсів і послуг. Крім того, на платформі Android блокчейн може сприяти створенню розумних міст і інтелектуальних систем управління міськими послугами. Блокчейн дозволяє створювати системи відстеження даних для різних цілей, включаючи енергоефективність, транспортні мережі та комунальні послуги. Це дозволить містам краще використовувати ресурси, скоротити витрати та покращити якість життя людей.

1.4 Аналіз існуючих рішень та систем підтримки криптовалют для мобільних пристроїв

Існує широкий спектр варіантів і систем підтримки криптовалют для мобільних пристроїв, які відрізняються за функціональністю, безпекою та простотою використання. Інші надають додаткові можливості, такі як зберігання та переказ криптовалют, тоді як інші розширюють можливості торгівлі, повсякденного використання криптовалюти та навіть інвестування. Для криптовалют доступні різні мобільні додатки та гаманці, такі як Coinbase, Blockchain Wallet, Trust Wallet, Exodus тощо. Вони пропонують зручний інтерфейс для зберігання та керування активами криптовалюти, а також підтримують кілька популярних криптовалют.

Користувачі можуть використовувати деякі з цих програм, щоб купувати та продавати криптовалюти, проводити обмін криптовалюти на звичайну валюту та навіть отримати доступ до різних фінансових послуг. Окрім гаманців для криптовалют, є також мобільні програми, які дозволяють торгувати на криптовалютних біржах, такі як Binance, Kraken, Coinbase Pro тощо.

Користувачі можуть виконувати ці завдання прямо з мобільного пристрою, торгуючи різними криптовалютами, виконуючи різноманітні замовлення та проводячи аналіз ринку, зображено на рисунку 1.6. Під час аналізу ринку було виявлено збільшення інтересу до криптовалют і блокчейн-технологій. Це відображає

збільшення капіталізації ринку та широке прийняття цих технологій у фінансових і технологічних сферах.

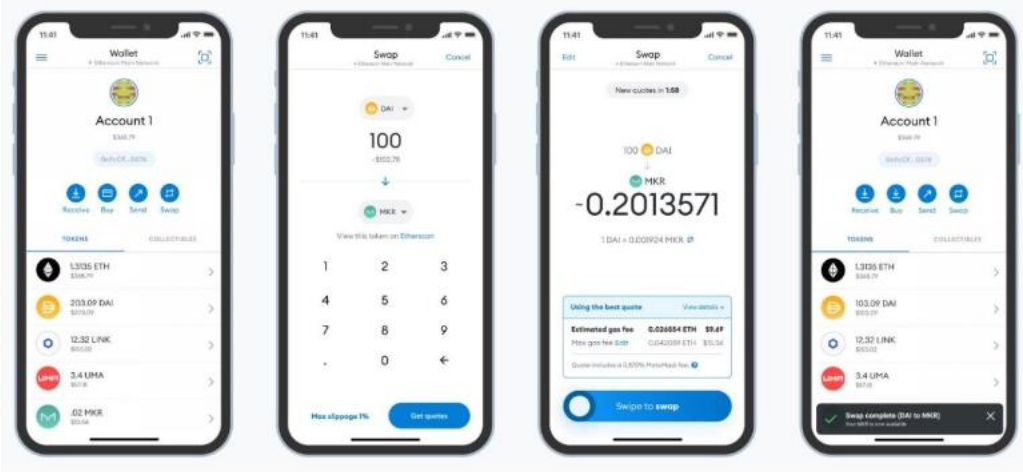


Рисунок 1.6 –Інтерфейс MetaMask, в якому є криптовалютний ринок з різними валютами

Деякі компанії також пропонують мобільні додатки, які дозволяють використовувати криптовалюту в щоденних операціях, наприклад, додатки для платежів у різних магазинах або сервіси, які дозволяють відправляти гроші в криптовалюті друзям і родичам. Загалом, мобільний криптовалютний ринок постійно розвивається, надаючи користувачам різноманітні можливості для зберігання, торгівлі та використання криптовалюти на своїх мобільних пристроях. На додаток до гаманців і бірж, існують також мобільні додатки та сервіси, які дозволяють користувачам отримувати криптовалюту як винагороду за виконання різних завдань або виконання певних дій. Наприклад, деякі програми пропонують криптовалютні винагороди за участь у опитуваннях, виконання ігор або перегляд реклами. Це може мотивувати користувачів вивчати криптовалюту ще більше та залучати нових учасників до екосистеми криптовалют. Крім того, деякі платформи та мобільні додатки надають можливість отримувати кредити

Люди, які мають криптовалютні активи та потребують фінансової підтримки, або ті, хто хоче використовувати свої активи як забезпечення для отримання кредиту, можуть вважати це корисним. Нарешті, важливо зазначити, що мобільні платіжні

системи, які базуються на технологіях блокчейну та криптовалютних активах, на сьогоднішній день активно розвиваються. Користувачі можуть здійснювати платежі в криптовалюті у реальному часі за допомогою цих систем, які гарантують швидкі та надійні транзакції без необхідності використання посередників або банківських установ.

Таким чином, мобільні програми та сервіси для криптовалют постійно розширюють свої можливості, пропонуючи користувачам різноманітні способи отримання, зберігання та використання криптовалюти прямо з їхніх мобільних пристроїв.

Упровадження технології Near Field Communication (NFC) для безконтактних операцій з криптовалютою є однією з останніх тенденцій у сфері мобільних додатків для криптовалют. Деякі програми дозволяють користувачам здійснювати транзакції з криптовалютою, мобільні платежі та навіть перекази коштів просто за допомогою зчитування NFC-тегів або сканування QR-кодів з мобільного пристрою. Це робить транзакції з криптовалютою більш простими та доступними, особливо зараз, коли безготівкові та безконтактні технології стають все більш популярними.

Крім того, деякі мобільні програми почали підтримувати функції криптовалютних кредитних карт. Це означає, що користувачі можуть використовувати кредитну картку для доступу до криптовалютних активів і використовувати їх для покупок у магазинах, ресторанах та інших місцях, де приймаються пластикові картки.

Це підвищує ліквідність криптовалюти та робить її зручною для використання в щоденних фінансових операціях. Розширення можливості використання криптовалют на мобільних пристроях і зростання їх доступності серед звичайних користувачів сприяє подальшому зростанню популярності та повсякденного використання криптовалют.

Проблеми, пов’язані з використанням криптовалюти на мобільних пристроях. Під час використання криптовалюти на мобільних пристроях існує ряд проблем, які можуть вплинути на безпеку, зручність і продуктивність роботи з цифровими активами. Безпека є однією з найважливіших проблем. Шкідливе програмне

забезпечення, фішингові атаки та інші небезпеки, які можуть призвести до крадіжки криптовалют, часто атакують мобільні пристрої. Мобільні пристрої часто підключені до незахищених мереж Wi-Fi, що збільшує ймовірність перехоплення даних [6].

Низька потужність мобільних пристроїв порівняно з настільними комп'ютерами чи спеціалізованими апаратними гаманцями є ще однією значною проблемою. Це може вплинути на швидкість і продуктивність обробки транзакцій, а також на здатність пристрою виконувати складніші криптографічні операції. Крім того, зберігання великих блокчейн-даних на мобільному пристрої може бути складним через обмежений обчислювальний ресурс і пам'ять. Однак, підтримка та постійні оновлення мобільних додатків є життєво важливими для безперебійної роботи та надійності. Отож, варто проводити кампанії, які навчають користувачів, як безпечно використовувати криптовалюту на мобільних пристроях.

Криптографічні ключі розраховуються за допомогою односторонніх хеш-функцій. Маючи ключ, неможливо дізнатися про вхідні дані, а також неможливо використати інший набір даних, що дає такий самий ключ. 19 Тому при втраті ключа, втрачається і можливість використання цих даних. Це приведено в таблиці нижче, на даних стрічках було використано алгоритм хешування sha256.

Зручність використання є ще однією великою проблемою. Мобільні програми для роботи з криптовалютами часто мають менш зручні інтерфейси через складні інтерактивні елементи та обмежений розмір екрана. Відсутність правил і згоди щодо дизайну таких додатків може призвести до труднощів у навігації та використанні їхніх функцій, особливо для новачків.

На використання криптовалют на мобільних пристроях також впливають проблеми масштабованості. Синхронізація з блокчейном може затягнутися через обмежену пропускну здатність мобільних мереж, що може призвести до затримок у підтвердженні транзакцій. Це особливо важливо в мережах, які мають багато користувачів і високу завантаженість.

Регулювання та конфіденційність є технічними проблемами. Багато мобільних додатків, призначених для роботи з криптовалютами, можуть збирати особисті дані користувачів, що створює ризики для конфіденційності.

Таблиця 1.1 – Вхідні дані і ключ

Вхідні дані	Ключ
Blockchain	625da44e4eaf58d61cf048d168aa6f5e492dea166d8bb54ec06c30de07db57e1
Blockchain.	d70efa3d07ce636c2843270e3a67094e60889d5fbd6829a113b14716ee1c0c4f
Blockchain1	0fc6e34f6899f5e2ca06688e49bb42cc104a45d5bb86c55eafe8c7d588204a48
Blockchain)	afab0a78635c83245a27ae3e41286a72507202b5d790de37a89b433a899c3815

Усі дані blockchain зберігаються на вузлах користувачів blockchain-мережі. Усі користувачі мережі мають рівні права і обов’язки, узагалі кажучи, можуть робити все, що завгодно, в тому числі безуспішно намагатися обманути інших користувачів та намагатись змінити ланцюг блоків. Заборонити цього їм ніхто не може, тому що всі знаходяться в рівних умовах, мають рівні права, і в однаковій мірі можуть виконувати чи навіть порушувати свої обов'язки.

1.5 Технічні аспекти безпеки та конфіденційності в системі підтримки криптовалютних операцій

Технічні елементи безпеки та конфіденційності в системі підтримки криптовалютних операцій є важливими для забезпечення надійності та довіри до системи. Для досягнення цих цілей використовуються різні підходи та технології. Криптографічний захист є життєво важливим для безпеки криптовалютних операцій.

Це досягається за допомогою криптографічних протоколів, таких як хеш-функції, які використовуються для підпису та перевірки транзакцій, а також шифрування, яке захищає конфіденційність особистих даних користувачів. Багатофакторна аутентифікація також є важливою частиною безпеки. Вона дозволяє підвищити захист, вимагаючи від користувачів надати додаткову інформацію для

ідентифікації, таку як пароль разом із кодом, відбитком пальця або іншими факторами.

Для запобігання несанкціонованому доступу до системи система повинна бути захищена від вторгнень. Це може включати використання систем виявлення зламів, виявлення невідомих пристроїв або підозрілої поведінки та моніторинг мережевої активності. Для забезпечення безпеки ключі доступу до криптовалют можуть зберігатися в холодних гаманцях, які є офлайн і пропонують більшу захист, ніж гарячі гаманці, які є онлайн. Audit безпеки є важливою частиною системи безпеки. Регулярні аудити забезпечують стабільну та безпечну роботу системи, виявляючи та виправляючи потенційні уразливості та помилки.

Крім вищезазначених факторів, існують інші інновації та технічні рішення, які можна використовувати для підвищення безпеки та конфіденційності систем підтримки криптовалютних операцій:

Для забезпечення надійного регулювання цифрових фінансів важливим завданням є підвищення безпеки та конфіденційності систем підтримки криптовалютних операцій. Використання багатофакторної аутентифікації (MFA) є одним із основних підходів до підвищення безпеки. Вимагаючи від користувачів підтвердити свою особу за допомогою різних незалежних каналів, таких як біометричні дані, паролі або коди для мобільних пристроїв, цей метод додає додатковий захист.

Застосування апаратних гаманців є ще одним важливим елементом підвищення безпеки. Апаратні гаманці зберігають приватні ключі в захищеному місці, що запобігає крадіжці цих ключів через зловмисне програмне забезпечення, яке працює на комп’ютерах або мобільних пристроях. Завдяки можливостям шифрування та підпису транзакцій без прямого підключення до Інтернету ці гаманці підвищують рівень захисту. Захист від атак "phishing" та соціальної інженерії: Розробка ефективних методів для розпізнавання та запобігання атакам "phishing" та соціальній інженерії, які можуть спрямовуватися на користувачів криптовалютних платформ з метою крадіжки даних або грошей [7].

Ці технічні рішення спрямовані на підвищення безпеки та конфіденційності систем підтримки криптовалютних операцій і надання користувачам криптовалют надійної та безпечної інфраструктури. Зокрема, у сфері безпеки криптовалютних операцій можуть застосовуватися нові технології, такі як квантові обчислення та глибоке навчання (deep learning). [8]

Глибоке навчання може використовуватися для аналізу великих обсягів даних і виявлення аномалій у поведінці користувачів, що дозволяє швидко виявляти потенційні загрози та вторгнення. Щоб забезпечити ще вищий рівень криптографічної стійкості, квантові обчислення можуть використовувати квантові алгоритми шифрування та підпису. Такі винахідливі методи можуть покращити безпеку та надійність систем, які підтримують операції з криптовалютою.

Крім того, інформація, яка зберігається в системі криптовалютних операцій, може бути захищена за допомогою технології, відомої як «гомоморфне шифрування». Ця технологія дозволяє обробляти зашифровані дані без необхідності їх розшифрування, зберігаючи конфіденційність навіть під час обчислень або аналізу даних. Такий метод може бути корисним для захисту конфіденційних даних користувачів і транзакцій у системі криптовалютних операцій. Використання технології, відомої як «криптографія з пороговим розподілом», є ще одним інноваційним методом. Цей тип технології дозволяє різним учасникам ділити ключі доступу або іншу конфіденційну інформацію, що робить доступ можливим лише за наявності певної кількості частин ключа. [9]

Це забезпечує додаткову безпеку, оскільки не дозволить отримати доступ до конфіденційної інформації без належної згоди інших учасників, навіть якщо один із учасників скомпрометований. Такий підхід може бути корисним для захисту системи криптовалютних операцій від атак, спрямованих на отримання конфіденційних ключів або інших особистих даних.

1.6 Визначення ключових вимог до системи для забезпечення її функціональності та ефективності

Для забезпечення функціональності та ефективності блокчейн-системи необхідно визначити основні вимоги. Безпека є першочерговою. Це включає використання сучасних методів шифрування для захисту даних, використання багатофакторної аутентифікації для перевірки користувачів і безпечне зберігання приватних ключів у апаратних гаманцях. Програмне забезпечення також повинно регулярно оновлюватись, щоб усунути потенційні вразливості.

Друга важлива вимога стосується ефективності системи. Враховуючи обмежені обчислювальні ресурси та пам’ять мобільних пристроїв, блокчейн-додатки повинні бути оптимізовані для роботи на них. Створення швидкого доступу до мережі блокчейну, мінімізація споживання енергії та ефективне управління ресурсами є всіма прикладами цього. Навіть на пристроях середнього рівня додаток повинен працювати стабільно та забезпечувати швидке завантаження.

Зручність використання є важливою. Щоб користувачі з різним рівнем технічної підготовки могли легко отримати доступ до основних функцій, інтерфейс користувача має бути легко зрозумілим і простим у використанні. Підтримка кількох мов і інтеграція з мобільними сервісами, такими як контакти та сповіщення, можуть значно покращити користувацький досвід.

Сучасні методи захисту даних, такі як zk-SNARKs, дозволяють проводити транзакції без розкриття персональних даних. Впровадження технологій, які гарантують анонімність транзакцій, таких як CoinJoin, є важливим.

Масштабованість системи є важливою вимогою. Блокчейн-додатки повинні бути здатними швидко обробляти велику кількість користувачів і транзакцій. Розширення інфраструктури та інтеграція з різними блокчейн-мережами для забезпечення високої пропускної здатності та стійкості до навантажень є частиною цього [10].

Нарешті, легальна робота системи залежить від дотримання регуляторних вимог. Це включає дотримання правил боротьби з відмиванням грошей (AML) і

впровадження систем ідентифікації користувачів (KYC). Система повинна бути здатною адаптуватися до змін у регуляторному середовищі та відповідати міжнародним і місцевим стандартам.

Таким чином, безпека, продуктивність, зручність використання, конфіденційність, масштабованість і регуляторна відповідність є важливими факторами, які необхідно враховувати, щоб блокчейн-система на основі ОС Android була функціональною та ефективною.

Для того, щоб блокчейн-система на ОС Android була функціональною та ефективною, необхідно враховувати низку додаткових факторів. Ці фактори включають основні вимоги до безпеки, продуктивності, зручності використання, конфіденційності, масштабованості та регуляторної відповідності.

Інтероперабельність є важливою вимогою. Система повинна мати здатність взаємодіяти з іншими блокчейн-мережами та програмами, щоб забезпечити безшовний обмін даними та транзакції між різними платформами. Це дозволяє користувачам виконувати операції в широкому екосистемному контексті та в межах однієї мережі, що значно підвищує цінність і простоту використання.

Зверніть увагу на розширюваність і модульність системи. Архітектура додатку повинна дозволяти легко додати нові функції та інтегрувати їх з іншими сервісами без значних змін у фундаментальній структурі. Це гарантує гнучкість і можливість швидко реагувати на нові потреби та тенденції ринку. Підтримка офлайн-режиму є ще однією важливою вимогою. Мобільні програми повинні бути здатні працювати без постійного підключення до Інтернету, зберігаючи інформацію локально та синхронізуючи її з мережею блокчейну, коли вони підключені до Інтернету. Це дозволить додатку продовжувати працювати навіть у випадку тимчасової втрати зв’язку.

1.7 Висновок

Технічний огляд блокчейн-базованої системи включає декілька ключових елементів, які відображають значення, переваги та технічні вимоги для того, щоб

підтримувати криптовалютні операції безпечно та ефективно на мобільних пристроях, зокрема на платформі Android.

Завдяки своїм децентралізованим, прозорим і захищеним від маніпуляцій властивостям блокчейн технологія є життєво важливою для операцій, пов'язаних із криптовалютою. Вона надає надійний механізм для ведення записів і верифікації транзакцій без необхідності використання центрального посередника. Це зменшує ймовірність шахрайства та корупції, підвищуючи загальну стійкість системи. Користувачі криптовалют дуже вдячні за те, що блокчейн дозволяє здійснювати транзакції швидко та з низькими комісіями.

Використання блокчейну для операцій, які працюють на платформі Android, має значні переваги. Android має великий потенціал для поширення криптовалютних програм, оскільки він є однією з найпопулярніших мобільних платформ у світі. Блокчейн-технологія, яка включена в Android, дозволяє користувачам здійснювати транзакції з будь-якого місця у будь-який час. Це робить криптовалютні операції простими та доступними. Крім того, широкі можливості масштабування та висока безпека блокчейна роблять його ідеальним вибором для мобільних криптовалютних платформ.

Аналіз існуючих систем підтримки криптовалют для мобільних пристроїв показує, що ринок містить кілька зрілих і добре розроблених додатків, таких як Trust Wallet, Coinbase і Binance. Багато функцій можна виконувати цими програмами, наприклад управління портфоліо, проведення транзакцій, доступ до бірж і аналітичні інструменти. Впроваджуючи багаторівневу аутентифікацію та шифрування даних, вони також підкреслюють безпеку.

У системі підтримки криптовалютних операцій технічні аспекти безпеки та конфіденційності включають захист від несанкціонованого доступу, забезпечення цілісності даних і конфіденційності транзакцій. Використання криптографічних методів, таких як асиметричне шифрування, хешування та цифрові підписи, є важливою частиною. Для захисту від нових загроз система повинна включати механізми виявлення та запобігання шахрайству.

Для того, щоб система була функціональною та ефективною, вона повинна мати високу продуктивність, низькі затримки в проведенні транзакцій, масштабованість для обробки великої кількості користувачів і транзакцій.

2. **РЕАЛІЗАЦІЯ АРХІТЕКТУРИ БЛОКЧЕЙН-БАЗОВАНОЇ СИСТЕМИ**

2.1 Вибір блокчейн платформи для інтеграції з ОС Android

При виборі блокчейн платформи для інтеграції з операційною системою Android важливо врахувати кілька ключових факторів.

По перше це спрощеність інтеграції: Платформа повинна мати зручні та документовані інструменти для розробки мобільних додатків, що дозволяють легко взаємодіяти з блокчейн системою. Це може включати мобільні SDK та набір API, які спрощують розробку та інтеграцію, а далі низька вартість транзакцій: Для мобільних додатків важливо мати можливість здійснювати транзакції з малими сумами без високих комісій. Тому обирайте блокчейн платформу з низькою вартістю транзакцій, щоб забезпечити ефективність і прийнятність для користувачів.

По-друге масштабованість оскільки мобільні додатки можуть мати велику кількість користувачів, важливо обирати платформу, яка здатна масштабуватися та працювати стабільно при великому навантаженні, однак також безпека є ключовим аспектом для будь-якої блокчейн платформи, особливо коли мова йде про мобільні додатки, які можуть бути піддані ризику кібератак. Оберіть платформу з надійними механізмами безпеки та захисту даних [11].

По-третє підтримка функціональності переконайтеся, що обрана платформа підтримує всі необхідні функціональні можливості для вашого мобільного додатку. Наприклад, якщо вам потрібно здійснювати смарт-контракти, переконайтеся, що платформа підтримує їхнє виконання на мобільних пристроях.

Інформація та підтримка: Обирайте платформу, яка надає достатню документацію та підтримку розробників, щоб ви могли швидко вирішувати будь-які проблеми чи питання під час інтеграції.

Розгляньте такі платформи, як Ethereum, Hyperledger Fabric, Corda або спеціалізовані мобільні блокчейн рішення, які можуть задовольнити ваші вимоги щодо інтеграції з операційною системою Android. При виборі блокчейн-платформи для інтеграції з операційною системою Android також необхідно враховувати додаткові фактори.

Професійна спільнота та екосистема обирайте платформу з активною та великою професійною спільнотою розробників та підтримкою великої кількості ресурсів, таких як форуми, блоги, онлайн-курси тощо. Це дозволить отримувати швидку допомогу та розв'язання проблем у випадку виникнення питань.

Сумісність з мобільними технологіями переконайтеся, що обрана платформа підтримує технології, які широко використовуються в мобільній розробці, такі як Java або Kotlin для Android. Це дозволить зручно інтегрувати блокчейн функціональність в ваші Android додатки.

Відкритий джерело коду підтримка відкритого джерела коду може бути важливою з точки зору прозорості та можливості перевірки безпеки блокчейн платформи. Відкритий код також дає змогу внести свої власні внески та модифікації до системи. Регуляторні питання переконайтеся, що обрана блокчейн платформа відповідає законодавству та регуляторним вимогам, що можуть стосуватися вашого регіону або сфери діяльності. Наприклад, деякі блокчейн платформи можуть мати обмеження щодо обробки особистих даних.

Перш ніж приймати остаточне рішення щодо платформи блокчейн для інтеграції з операційною системою Android, розгляньте всі ці аспекти та проведіть ретельний аналіз. Щоб вибрати блокчейн-платформу для інтеграції з операційною системою Android, зверніть увагу на вимоги користувачів до низьких комісій і високої швидкості роботи. Крім того, враховуйте потенційні вимоги до захисту приватності та конфіденційності даних; це може вимагати використання блокчейн-платформ, які підтримують анонімні або приватні транзакції.

Отож подумати про можливість використання блокчейн платформи, яка пропонує гнучкість у виборі консенсус-алгоритмів. Адже можна вибрати алгоритм, який найкраще відповідає потребам вашого додатку та дозволяє досягти оптимальної продуктивності та швидкості операцій за допомогою цього інструменту. Врахуйте також екосистему блокчейн платформи та доступність розширень і інструментів для розробників. Це може включати SDK для розробки мобільних додатків, інструкції та приклади використання, а також можливість використовувати вже готові смарт-контракти або створювати власні.

Не менш важливим є розвиток проекту та підтримка спільноти. У випадку виникнення проблем або потреби в допомозі, вибір платформи з активною та дружньою спільнотою розробників може дозволити вам отримати доступ до корисної інформації, порад і рішень. Нарешті, розгляньте можливість провести тестування та експерименти з різними платформами блокчейну, щоб визначити, яка найкраще відповідає потребам і вимогам вашого проекту.

Щоб вибрати блокчейн-платформу для інтеграції в операційну систему Android, важливо враховувати ймовірність розвитку подій у майбутньому та перевіряти, чи сумісна платформа з іншими технологіями. Щоб переконатися, що програми залишаються актуальними та конкурентоспроможними й у майбутньому, важливо обирати платформу, яка активно розвивається та має потенціал для майбутнього зростання.

Важливо також подумати про можливість інтеграції з існуючими рішеннями та проектами блокчейну. Вибір певної блокчейн-платформи може спростити та пришвидшити розробку вашого проекту, якщо він використовує смарт-контракти або інші функції, які вже працюють на цій платформі. Крім того, розгляньте гібридні або мультиплатформені рішення. Ці рішення дозволять використовувати різні блокчейн платформи для різних частин вашого проекту. Це може підвищити вашу гнучкість і дозволити вам вибрати найкраще рішення для кожного конкретного випадку використання.

Нарешті, розгляньте можливість використання децентралізованих рішень для обробки транзакцій і зберігання даних на мобільних пристроях клієнтів. Це може забезпечити більшу безпеку та приватність даних, одночасно зменшуючи навантаження на централізовані сервери. Щоб вибрати блокчейн-платформу для роботи з операційною системою Android, важливо враховувати витрати. Оберіть платформу з вигідними умовами для вас як розробника, включаючи абонентські платежі, комісії за користування та ціни транзакцій, а також інші витрати, які можуть виникнути під час розробки та використання блокчейн-додатків.

Зверніть також увагу на готовність до розвитку та масштабність. Виберіть платформу, яка може легко адаптуватися до зростання кількості користувачів і

транзакцій, і яка пропонує механізми для майбутніх розробок. Крім того, варто подумати про можливість втілення додаткової функціональності, такої як смарт-контракти або взаємодія з додатками інших розробників. Оберіть платформу, яка підтримує різноманітні можливості та інтеграції, які можуть знадобитися вашому проекту. Безпека також є важливою.

Виберіть платформу, яка має надійні механізми захисту від кібератак і злому, а також функції для забезпечення конфіденційності даних. Крім того, враховуйте важливість інтеграції з платформою, а також наявність підтримки спільноти та документації. Оберіть платформу, яка пропонує достатньо даних і ресурсів для розробки та підтримки вашої програми. інтерфейс вашого додатку.

Оскільки масштабування вашого додатку може значно вплинути на його продуктивність та ефективність, зверніть увагу на можливість зростання користувачів і обсягу транзакцій. Ви також повинні подумати про ступінь децентралізації та контролю, який ви хочете мати над вашим додатком. Виберіть платформу, яка відповідає вашим вимогам щодо гнучкості управління та розподіленості. Не забувайте про те, наскільки дорогими та доступними є рішення. Оберіть платформу, яка відповідає вашим грошима та має функції, які вам потрібні для вашого додатку.

2.2 Технології, які лежать в основі блокчейну

Еліптичні криві, ECDSA та ключі є основами блокчейна [51-53]. Алгоритми криптографії є основою блокчейна. Одним із таких алгоритмів є ECDSA Digital Signature Algorithm, який використовує еліптичні криві (elliptic curve) і кінцеві поля (finite field) для підпису даних, щоб інші люди могли підтвердити, що підпис є справжнім, щоб запобігти підробці. Підпис і верифікація ECDSA виконуються за допомогою кількох арифметичних операцій.

Нехай маємо поле K, а кубічна крива над алгебраїчним замиканням поля K є еліптичною кривою над цим полем. Це задається рівнянням третього степеня з коефіцієнтами поля K і «точкою на нескінченності». Криві Вейерштрасса є однією з

різновидів еліптичних кривих [54-56]. Кожну таку криву можна представити як рівняння виду: y2 = x3 + ax + b. У мережі криптовалюти Bitcoin коефіцієнти формули еліптичної кривої a = 0 і b = 7. Графік функції зображено на рисунку 2.1.

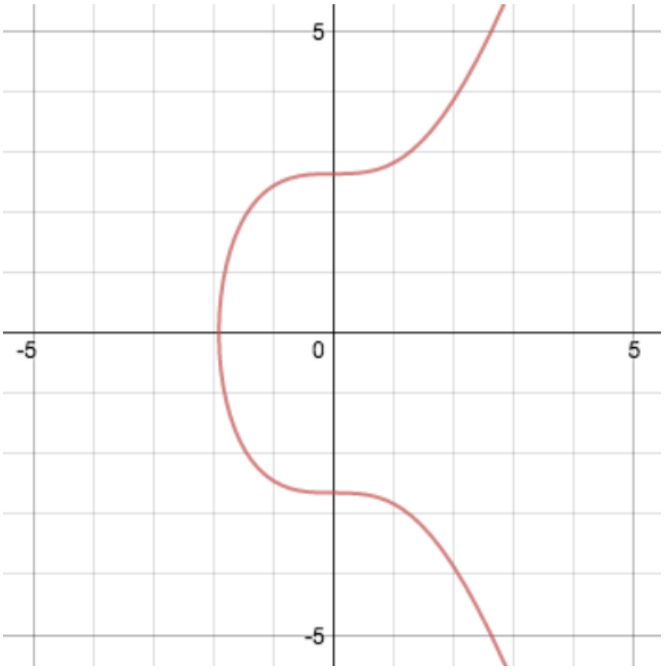


Рисунок 2.1 – Графік функції

Невертикальна лінія, яка перетинає дві недотичні точки на кривій, перетинає третю точку на кривій є однією з цікавих характеристик еліптичних кривих. Точку R називають сумою двох точок на кривій P + Q, яка є відображенням точки -R, яка була створена шляхом продовження прямої (P, Q) до перетину з кривою щодо осі X [57][58][59]. Зображено на рисунку 2.2.

Основою криптографії та безпеки блокчейн-технологій є ключі та еліптичні криві (ECDSA). В криптографії еліптичні криві використовуються завдяки своїм властивостям, які дозволяють створювати надзвичайно безпечні та ефективні алгоритми. В основі цих алгоритмів лежать математичні структури, які мають певні характеристики, такі як висока стійкість до атак і компактність ключів. Алгоритм цифрового підпису ECDSA використовує еліптичні криві для створення та перевірки цифрових підписів. Використовуючи його для захисту та аутентифікації даних, він

гарантує, що транзакції, які відбуваються в блокчейн-мережі, походять від справжніх власників приватних ключів і не були змінені після підписання.

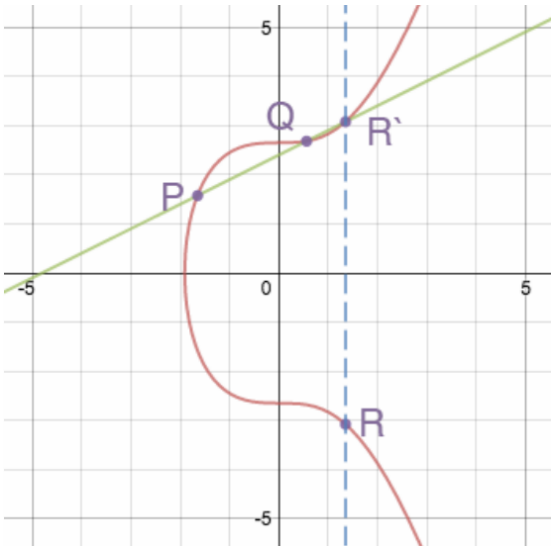


Рисунок 2.2 – Еліптична крива в Bitcoin

Для прикладу, якщо провести пряму через дві точки з координатами виду P (a, b) і Q (a, -b), то ця пряма буде паралельна осі ординат. У цьому випадку не буде третьої точки перетину. Тому, щоб розв’язати цю проблему, вводиться так звана точка нескінченності, або точка нескінченності, яку позначає O. Отже, якщо немає перетину,рівняння приймає вигляд: P + Q = O.

В цьому випадку просто проводиться дотична до точки Q, якщо ми хочемо накласти точку саму на себе або подвоїти її. Відображається точка перетину симетрично щодо осі X. Зображено на рисунку 2.3.

Безпека транзакцій у блокчейн-системах залежить від ключів. Приватні ключі, які слід зберігати в секреті, використовуються для підпису транзакцій, надаючи їм правовий статус і дозволяючи виконувати операції. Користувачі можуть перевіряти автентичність підписів, отримуючи публічні ключі, які доступні для всіх учасників мережі. Це дозволяє їм впевнитися, що транзакції не були підроблені. Забезпечення безпеки транзакцій полягає в запобіганні ризикам та забезпеченні високого рівня надійності та конфіденційності, а також щоб захиститись потрібно пройти двох-

етапну перевірку, за допомогою якої точно можна підняти рівень захисту тим що використовуючи.

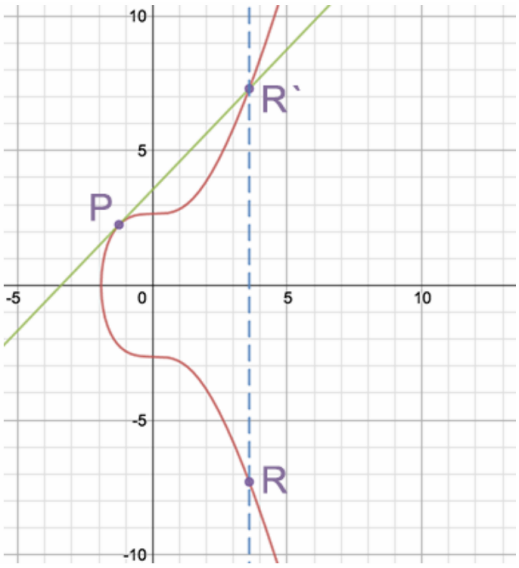


Рисунок 2.3 - Еліптична крива в Bitcoin

Скалярне множення, R = aP, отримане додаванням точки P самої до себе, виконується за допомогою цих двох операцій. Для прикладу: 35

$$P = 7P \; R = P + (P + (P + (P + P))))))$$

R - це результат скалярного множення точки;

P- точка на еліптичній кривій;

7 – це скаляр.

Зазвичай можна спростити процес скалярного множення, поєднавши операції додавання та подвоєння точок. Наприклад, R = 7P, R = P + 6P, R = P + 2 (3P). R = (P + 2P). У цьому випадку 7P розділили на два етапи подвоєння точок і два етапи додавання точок.

Еліптична крива над кінцевим полем, яка використовується в еліптичній криптографії, є розтягнутою над певним кінцевим полем. В еліптичної криптографії кінцеве поле можна представити таким чином зумовлений набір додаткових чисел, який використовується для отримання результатів кожного обчислення

$$X3 + ax + b = y2 \pmod p \qquad (2.1)$$

x – це абциса точки;

a – це додатонок, який напряму залежить від x;

b – коефіцієнт;

y – це ордината точки на кривій;

mod p – це операція, яка вказує на взяття остачі від ділення.

Зокрема, 9 мод 7 = 2. У цьому випадку ми маємо поле, яке починається від 0 до 6, і всі операції по модулю 7, над яким би числом вони не виконувалися, дадуть результат, який потрапляє в цей діапазон. Хоча графік цієї кривої не буде схожим на еліптичну криву, усі вищезгадані властивості функції (додавання, множення та крапка в нескінченності) залишаються дійсними. На кінцевому полі по модулю 67 є еліптична крива біткойна, y 2 = x 3 +7. Зображено на рисунку 2.4.

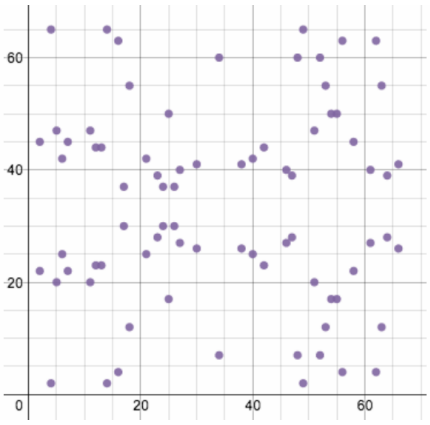


Рисунок 2.4 - Еліптична крива в Bitcoin по модулю 67

Це множина точок, у яких всі знаки x і y є цілими числами в діапазоні від 0 до 66. Як тільки вони досягнуть бар'єру 67, прямі лінії, намальовані на цьому графіку, будуть ніби «обертатися» навколо поля. Вони продовжуватимуть рухатися з іншого кінця поля, зберігаючи той самий нахил, але зі зрушенням. Наприклад, якщо додати точки (2, 22) і (6, 25). Зображено на рисунку 2.5. Еліптичні криві, які використовуються в Bitcoin, дозволяють створювати безпечні криптографічні протоколи з меншими обчислювальними витратами порівняно з традиційними криптографічними системами, що робить їх важливою частиною інфраструктури криптовалют. Використання еліптичних кривих у Bitcoin відіграє важливу роль у

забезпеченні безпеки та конфіденційності транзакцій, оскільки вони роблять систему більш стійкою до кібератак і надають користувачам високий рівень захисту.

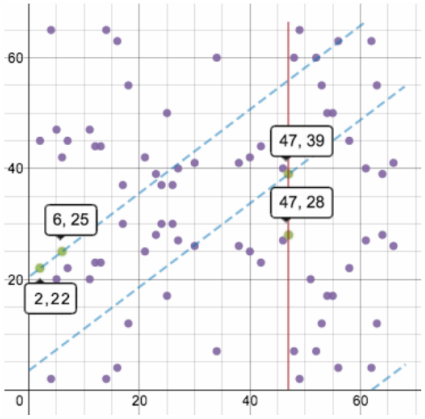


Рисунок 2.5 - Еліптична крива в Bitcoin по модулю 67

Протоколи, такі як біткойн, вибирають параметри еліптичної кривої та відображають їх у кінцевому полі, яке встановлено для всіх користувачів протоколу. Використовуване рівняння, просте значення по модулю поля та базова точка, яка потрапляє на криву, є параметрами.

На графіку можна показати порядок базової точки, який залежить від інших параметрів і визначається кількістю разів, коли точка може бути додана до самої себе, поки її нахил не стане нескінченним або не стане вертикальною лінією. Базову точку вибирають, щоб порядок був великим простим числом.

Для своєї базової точки, порядку та простого модуля біткойн використовує дуже великі числа. Насправді кожна практична програма ECDSA має величезне значення. Безпека алгоритму залежить від великих значень, які непрактичні для методу грубої сили.

Візьмемо приклад еліптичної кривої для Bitcoin: y 2= x3+ 7.Стандартний модуль складатиметься з цифр 2256–232–29–28–27–26–24–1 = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F

Таким чином, базова точка буде наступною: 04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26C3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8

У шістнадцятковому записі координата X виділена жирним шрифтом. Координата Y йде відразу після неї.Це виглядає так: BAAEDCE6 AF48A03B BFD25E8C D0364141

Сімейство рішень еліптичних кривих над кінцевими полями включає цю конкретну реалізацію під назвою secp256k1, цей набір Параметри є частиною сімейства стандартів, запропонованих SEC для використання в криптографії.

Алгоритм цифрового підпису ECDSA і еліптична крива secp256k1 використовуються для біткоїна. Секретний ключ ECDSA складається з випадкового числа між значенням порядку та одиницею.

Секретний ключ множиться на значення базової точки, щоб створити відкритий ключ, який містить транзакції блокчейна. Секретний ключ = відкритий ключ * G, згідно з рівнянням.

Це показує, що максимальна кількість секретних ключів, тобто біткоїн-адрес, є нормальною та відповідною. Тим не менш, через величезний порядок, який становить 2x256 степенів, неймовірно випадково або навмисно підібрати секретний ключ іншого користувача.

2.3 Реалізація інтерфейсу користувача для зручного управління криптовалютними операціями

Упровадження зручного інтерфейсу користувача для управління криптовалютними операціями є важливим фактором, який сприяє прийняттю та ефективному використанню блокчейн-технологій. Система повинна мати простий інтерфейс, щоб люди з різним рівнем технічної підготовки могли легко користуватися нею. Забезпечити простоту та зручність при виконанні основних завдань, таких як перевірка балансу, надсилання та отримання криптовалют, керування ключами та перегляд історії транзакцій, є основним завданням.

Дизайн інтерфейсу повинен бути логічним, простим у використанні та простим у використанні. Важливо використовувати прості іконки та текстові підказки, щоб користувачі могли швидко орієнтуватися в програмі. Наприклад, кнопки, необхідні

для виконання основних операцій, мають бути розташовані на зручному місці на екрані та мають бути великими та добре видимими., а також головний екран аккаунту зображено на рисунку 2.6.

Рисунок 2.6 - Головний екран, де є різні види електроних коштів

Для підвищення безпеки і зручності, інтерфейс повинен підтримувати багатофакторну аутентифікацію. Це може включати використання біометричних даних, таких як відбитки пальців або розпізнавання обличчя, що забезпечує швидкий та безпечний доступ до облікового запису.

Однією з ключових функцій інтерфейсу є відображення балансу користувача. Це повинно бути реалізовано у вигляді простого і зрозумілого індикатора, що відображає поточний баланс у вибраній криптовалюті та, за можливості, еквівалент у фіатній валюті. Це дозволяє користувачам легко відстежувати свої активи. Однак головним фактором в візуалізації є інвестиції великих компаній, зображений на рисунку 2.7. Блокчейн дозволяє користувачам перевіряти стан своїх активів і рух коштів через глобальну мережу, зберігаючи історію транзакцій у розподіленому реєстрі. Це підвищує прозорість системи та довіру до неї, а також дозволяє користувачам контролювати свої гроші без посередництва центральних установ.

Рисунок 2.7 – Візуалізації інвестування різних топових фірм у дану систему

Для того, щоб зробити інтерфейс користувача зручним для управління криптовалютними операціями, необхідно врахувати кілька важливих моментів. Перш за все, інтерфейс повинен бути простим у використанні, щоб користувачі без попереднього досвіду могли швидко зрозуміти його функції. Це досягається за допомогою простих і логічних елементів, чітких іконок і зрозумілих інструкцій. Наприклад, головна сторінка інтерфейсу повинна містити основні функції, такі як відображення балансу, останні транзакції та швидкі посилання на дії, які найчастіше виконуються.

Важливо створити дизайн, який є мінімалістичним і зосереджений на основних функціях, не перевантажуючи користувача зайвими елементами. Це полегшує сприйняття інтерфейсу та запобігає плутанині. Оскільки користувачі можуть взаємодіяти з криптовалютами на різних пристроях, таких як смартфони, планшети та десктопи, респонсивний дизайн є важливим. Інтерфейс повинен автоматично адаптуватися до розмірів екрану, щоб зробити його зручним для використання роботи в будь-яких умовах.

Інтерфейс складається з панелі керування. Вона повинна показувати баланс, останні транзакції та зміни курсу криптовалют. Користувачі повинні мати можливість адаптувати панель до своїх потреб, додаючи або видаляючи віджети, які відображають необхідні дані.

Одним із основних завдань є ведення портфоліо. Щоб користувачі могли легко переглядати, додавати та видаляти криптовалюти зі свого портфоліо, вони повинні це

зробити. Використання графіків і діаграм для візуалізації даних допомагає краще зрозуміти розподіл активів і динаміку їх змін з часом. Це дозволяє клієнтам приймати більш розумні інвестиційні рішення.

Проведення транзакцій має бути максимально простим. Користувачі повинні мати можливість купувати, продавати та обмінювати криптовалюту швидко та просто. Проведення попереднього перегляду комісій і підтвердження транзакцій робить процес більш прозорим і запобігає помилкам.

Для користувачів, які бажають аналізувати ринок і свої інвестиції, аналітика та звітність є важливими компонентами. Інтерфейс повинен містити інструменти для перегляду даних, аналітики, індикаторів і графіків, щоб допомогти людям приймати розумні рішення. Крім того, надзвичайно важливо забезпечити можливість створювати звіти про фінансову діяльність, які можуть бути корисними для податкових або інших потреби.

Безпека будь-якого криптовалютного інтерфейсу є життєво важливою. Багаторівнева аутентифікація, включаючи двофакторну аутентифікацію (2FA), шифрування даних та інші методи, повинні бути введені, щоб захистити облікові записи та транзакції користувачів. Це включає постійні оновлення безпеки та спостереження за підозрілими діями.

Технологія інтерфейсу вимагає використання сучасних бібліотек і фреймворків. Фронтенд можна реалізувати за допомогою React або Angular, які пропонують зручність розробки та високу продуктивність. Бекенд, який базується на Node.js або Python, дозволяє обробляти запити та взаємодіяти з блокчейном ефективно. Інтеграція API гаманців і криптовалютних бірж гарантує актуальність даних і можливість проведення транзакцій у режимі реального часу.

Для забезпечення високої якості користувацького досвіду важливо проводити тестування інтерфейсу з реальними користувачами, збирати відгуки та вносити корективи відповідно. Це покращить зручність використання та допоможе виявити потенційні проблеми. Регулярні оновлення та вдосконалення інтерфейсу дозволять йому залишатися відповідним сучасним потребам і вимогам користувачів.

Таким чином, створення зручного інтерфейсу користувача для управління криптовалютними операціями вимагає комплексного підходу, який включає дизайн, безпеку, сучасні технології та постійне вдосконалення на основі відгуків користувачів.

2.4 Комунікаційний протокол для взаємодії мобільного додатку з блокчейн-вузлами

Протокол, який використовується для взаємодії мобільних додатків з блокчейн-вузлами, є важливим компонентом, який гарантує безпечну та ефективну інтеграцію користувача з децентралізованими мережами. Основною метою протоколу є забезпечення передачі даних між додатком і блокчейном, щоб гарантувати цілісність, автентичність і своєчасність обробки даних.

Механізми аутентифікації та авторизації, шифрування даних, обробка транзакцій, синхронізація з блокчейном і обробка помилок є основними складовими протоколу.

Перші кроки в будь-якій взаємодії з блокчейн-вузлом є авторизація та аутентифікація. Користуючі повинні підтвердити свою особу за допомогою криптографічних ключів. Приватний ключ підписує запити, підтверджуючи, що вони виходять від законного власника, тоді як публічний ключ використовується для ідентифікації. Це гарантує, що тільки авторизовані користувачі можуть виконувати інші операції або надсилати транзакції.

Наступним важливим елементом є шифрування даних. Для того, щоб будь-які дані, які передаються між блокчейн-вузлом і мобільним додатком, були захищені від перехоплення та злому, їх потрібно зашифрувати. Щоб гарантувати, що дані залишаються захищеними під час передачі, протокол HTTPS, який використовується разом із протоколом Transport Layer Security (TLS), використовується, зображено на рисунку 2.8. TLS є важливим елементом кібербезпеки, що використовується для захисту конфіденційної інформації, такої як особисті дані, фінансова інформація та комерційні дані, від несанкціонованого доступу та зловживання.

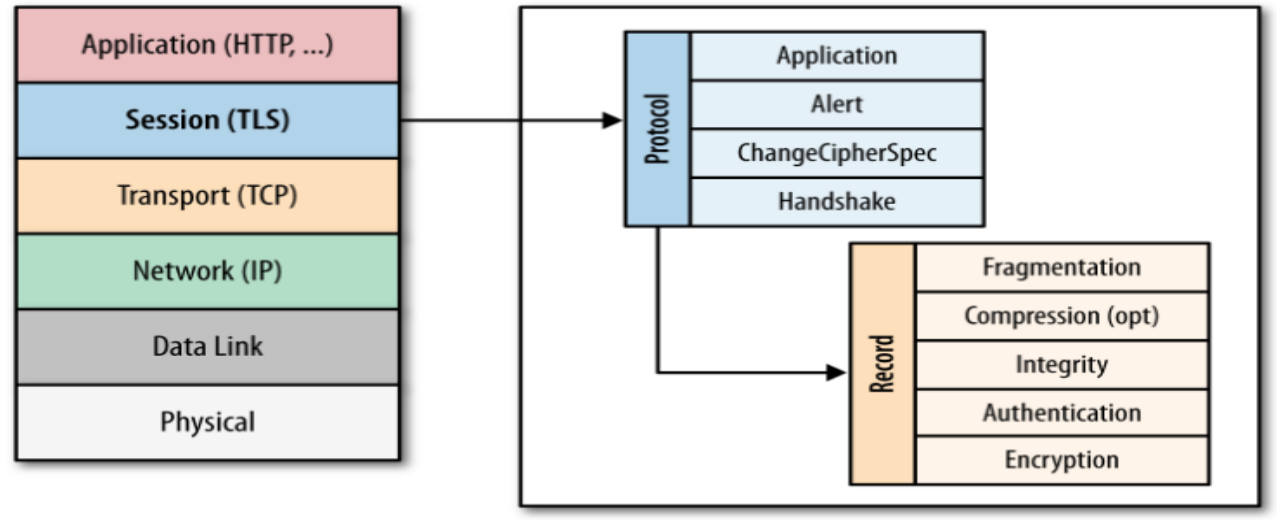


Рисунок 2.8 – Протокол TLS (SSL) у стеку протоколів Інтернету показано на схемі [36]

Обробка транзакцій включає створення, підписання та передачу транзакцій до блокчейну. За допомогою приватного ключу користувач створює транзакцію в мобільному додатку та передає її до блокчейн-вузла. Коли підпис перевіряється, модуль включає транзакцію до черги на обробку. Транзакція додається до блокчейну після її підтвердження.

Актуальність даних у мобільному додатку гарантується синхронізацією з блокчейном. Додаток регулярно запитує у вузла інформацію про останні блоки та транзакції, щоб оновлювати локальну копію блокчейну або кеш. Це дозволяє користувачам переглядати найновіші дані про свої активи та стан мережі.

Для того, щоб додаток працював добре, його потрібно обробляти помилки. Мобільний додаток повинен бути здатним ідентифікувати та адекватно реагувати на різноманітні помилки, від незначних збоїв у зв’язку до серйозних проблем із блокчейн-вузлами. Це може включати повідомлення користувача про проблеми, повторні спроби відправки запиту або переключення на інший вузол у разі відмови поточного.

Мобільний додаток також може оптимізувати взаємодію з блокчейном за допомогою різних методів, наприклад кешування даних, що зменшує кількість

запитів до вузла, і використання асинхронних викликів, щоб гарантувати безпеку користувацького досвіду.

API, які надають блокчейн-вузли, можуть бути включені в протокол. Ці API можуть виконувати багато завдань, наприклад, взаємодіяти з розумними контрактами, переглядати історію транзакцій і запитувати баланс адреси. Такі API полегшують інтеграцію та дозволяють швидко отримувати необхідні дані.

SDK та бібліотеки, розроблені для конкретних блокчейнів, також можуть бути використані для підвищення безпеки та продуктивності мобільного додатку. Обробка даних блокчейну, створення транзакцій і управління ключами – це рішення для взаємодії з мережами, які пропонують ці інструменти, зображено на рисунку 2.9.

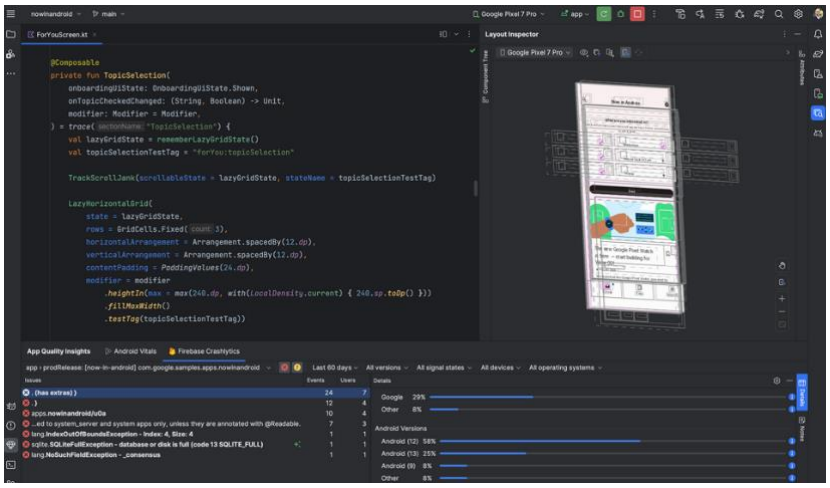


Рисунок 2.9 – Екран Android SDK, для створення мобільного додатку

Таким чином, протокол комунікації, який використовується для взаємодії мобільних додатків з блокчейн-вузлами, є складною системою, яка гарантує безпечну та ефективну передачу даних, обробку транзакцій, стійкість до помилок і синхронізацію даних. Використання сучасних методів криптографії, безпечних протоколів передачі даних, ефективних алгоритмів обробки та надійних інструментів для інтеграції з блокчейнами є кількома способами його реалізації. У сучасних методах криптографії використовується широкий спектр алгоритмів шифрування, хешування та підпису, щоб гарантувати безпеку даних у цифровому світі. Вони включають асиметричні алгоритми, такі як RSA та ECC, симетричні шифри, такі як

AES, і хеш-функції, такі як SHA-256. Вони захищають конфіденційність, цілісність і автентичність даних у різних областях, від фінансів до Інтернету речей.

2.5 Інтеграція з додатковими функціями Android для покращення користувацького досвіду (наприклад, NFC, біометрична автентифікація)

Інтеграція з додатковими функціями Android для покращення користувацького досвіду може включати в себе використання різноманітних функцій, таких як NFC (Near Field Communication) і біометрична автентифікація, для забезпечення зручності та безпеки користувачів. Давайте розглянемо кожну з цих функцій та їх можливі застосування в додатках для Android.

По-перше NFC (Near Field Communication) - це технологія бездротового зв'язку, яка дозволяє обмінюватися даними між пристроями на невеликій відстані (зазвичай декілька сантиметрів). Це може бути використано для різних цілей, таких як мобільні платежі додатки можуть використовувати NFC для проведення безконтактних платежів через мобільні пристрої. Передача даних NFC може бути використано для швидкого обміну даними між пристроями, наприклад, обмін контактами, URL або іншими короткими інформаційними елементами. Керування пристроями NFC теги можуть бути використані для включення або виключення різних функцій пристрою, таких як Bluetooth або Wi-Fi. Біометрична автентифікація використовує біологічні характеристики користувача, такі як відбиток пальця, розпізнавання обличчя або сканування очей, для підтвердження ідентичності.

Додатки можуть використовувати біометричну автентифікацію для забезпечення додаткового рівня безпеки та зручності для користувачів, наприклад розблокування додатків замість введення пароля або PIN-коду користувач може скористатися своїм відбитком пальця або обличчям для розблокування додатків. Підтвердження транзакцій в додатках, що використовують фінансові операції, біометрична автентифікація може бути використана для підтвердження транзакцій і підвищення рівня безпеки.

Загалом, інтеграція цих додаткових функцій в додатки для Android може значно поліпшити користувацький досвід, забезпечуючи зручність, безпеку та ефективність використання програмного забезпечення на мобільних пристроях.

Звісно, окрім NFC та біометричної автентифікації, інтеграція з додатковими функціями Android може включати також використання інших специфічних можливостей платформи для поліпшення користувацького досвіду. Ось ще декілька прикладів.

Голосовий контроль додатки можуть використовувати голосові команди для управління функціями та виконання дій. Наприклад, користувач може дати голосову команду для надсилання повідомлення, виклику контакту або відтворення мультимедійного вмісту.

Камера та додатки розпізнавання об'єктів використання камери для розпізнавання об'єктів або сцен може поліпшити функціональність додатків. Наприклад, додаток для покупок може дозволити користувачеві зробити фотографію товару, щоб знайти інформацію про нього або порівняти ціни.

Геолокація додатки можуть використовувати геолокацію для надання користувачам контекстуальної інформації або пропозицій. Наприклад, сервіси доставки можуть використовувати геолокацію для визначення місця розташування користувача та пропонування актуальних пропозицій у місцевих закладах.

Використання жестів додатки можуть підтримувати використання жестів для швидкого доступу до функцій або виконання певних дій. Наприклад, жест може бути використаний для швидкого відкриття головного меню або переходу до певної сторінки додатка.

Дана система є дуже корисно при тому коли треба розплатитись за що, і під рккою немає ні карти ні налічних грошей тоді за допомогою вбудовану систему NFC в сучасні телефони допоможе без додаткових зусиль оплатити всі ваші покупки за допомою зручних сервісів. Оплата зображенна на рисунку 2.10.

Рисунок 2.10 – Оплата за допомогою NFC

Ці функції дозволяють розширити можливості додатків для Android та створити більш зручне та інноваційне користувацьке середовище.

Звісно, на платформі Android є ще багато інших можливостей для поліпшення користувацького досвіду. Наприклад, можливість налаштування сповіщень та повідомлень дозволяє додаткам забезпечувати користувачам інформаційний контент вчасно та зрозуміло.

Додатки також можуть використовувати функцію "Dark Mode" для зменшення напруги на очі вночі та поліпшення енергоефективності на пристроях з AMOLED-екранами. Крім того, інтеграція зі специфічними API Android, такими як Android Wear для роботи з розумними годинниками, або Android Auto для інтеграції з автомобільною системою, відкриває нові можливості для розробників створювати додатки, які працюють в різних екосистемах користувачів.

Загалом, інтеграція з додатковими функціями Android дозволяє розробникам створювати додатки, які не лише забезпечують більше функціональності, а й стають більш зручними та привабливими для користувачів завдяки використанню передових технологій та інтерфейсів. Додатковою можливістю для покращення користувацького досвіду на платформі Android є інтеграція з функцією "App Actions". Ця функція дозволяє додаткам пропонувати контекстно-залежні дії та рекомендації користувачам прямо з домашнього екрана або рядка пошуку. Наприклад, якщо користувач регулярно використовує певний функціонал додатка в певний час дня,

система може запропонувати відкрити цей додаток або виконати відповідну дію безпосередньо з домашнього екрана.

Крім того, інтеграція з функціями мультимедіа, такими як фреймворки для відтворення аудіо та відео, може додати до додатків різноманітні можливості, включаючи потокове відтворення музики та відео, використання аудіо- та відео-запису, а також інтеграцію з різними онлайн-сервісами. Також важливою можливістю є підтримка адаптивного дизайну та різних режимів екрану, що дозволяє додаткам працювати оптимально на різних пристроях та в різних режимах, включаючи смартфони, планшети, Chromebooks та інші.

Інтеграція з цими додатковими функціями допомагає створювати додатки, які не лише забезпечують розширені можливості, але й дозволяють користувачам більш комфортно взаємодіяти зі своїми пристроями та отримувати більше користі від використання програмного забезпечення на пл Звісно, інтеграція з додатковими функціями Android може включати інтерактивність зі сповіщеннями.

Додатки можуть використовувати розширені сповіщення для надання користувачам можливості взаємодії безпосередньо з сповіщеннями. Наприклад, користувач може відповісти на повідомлення, виконати певні дії або навіть запустити певні функції додатка без необхідності відкривати сам додаток. Також важливою можливістю є інтеграція з функціями доступності.

Додатки можуть підтримувати різні можливості доступності, такі як читання екрану, мовні налаштування, збільшення розміру шрифту тощо, щоб забезпечити зручніше використання для людей з обмеженими можливостями.

Нарешті, інтеграція з хмарними сервісами може дозволити додаткам зберігати дані користувачів у безпечному та доступному місці в Інтернеті, щоб забезпечити синхронізацію даних між різними пристроями користувача та резервне копіювання. Використання цих додаткових можливостей Android дозволяє створювати додатки, які є більш гнучкими, зручними та доступними для широкого кола користувачів, забезпечуючи таким чином високий рівень задоволення від використання додатків на платформі Android.атформі Android.

2.6 Розроблення архітектури системи

Архітектура системи складається з кількох модулів:

- блокчейн-модуль запису та читання, блокчейн.
- модуль перевірки інформації та очистки даних від повторення.
- Модуля для тимчасових даних і опрацювання, а також інші функції.

Цей тип архітектури відрізняється тим, що він поділений на основні модулі, призначені для опрацювання даних у блокчейні. Таким чином, цю систему можна використовувати для багатьох проектів, які мають будь-які дані.Для спрощення побудови проекту архітектуру було розділено на шість модулів:

- Announcement — модуль для обробки даних клієнта.

- Scrape — це модуль, який дозволяє передавати дані клієнтам.

- Tracker — це модуль, який обробляє тимчасові вхідні дані. Основним операційним модулем для обробки вхідних і вихідних даних є сортування та очищення, який має багато функцій, які полегшують роботу системи.

- BigData — це модуль опрацювання великих даних, тобто записів Blockchain — це модуль для реплікації по нодах, який побудований на основі блокчейну та використовує алгоритм Scrypt, де адреса служить ідентифікатором даних.

Діаграма класів, яка відповідає загальному вигляду архітектури системи, показана на рисунку 2.11. Червоний колір покриває основні модулі.

Особливістю даної системи є те, що класи Tracker, Announce і Scrape можна використовувати як для вхідних, так і для вихідних даних. Три основні модулі системи: сортування та очищення, великі дані та blockchain. Підтримка архітектури базової на блокчейні на операційній системі Android складається з кількох основних модулів. У модулі користувача є класи для користувачів системи. У цьому класі користувача зберігаються ідентифікатор користувача, ім’я, електронна пошта та пароль, а також методи реєстрації, входу та виходу користувача. Модуль аутентифікації керує аутентифікацією користувачів і включає клас аутентифікації з атрибутами та станом аутентифікації токену, а також методи аутентифікації та валідації токену.

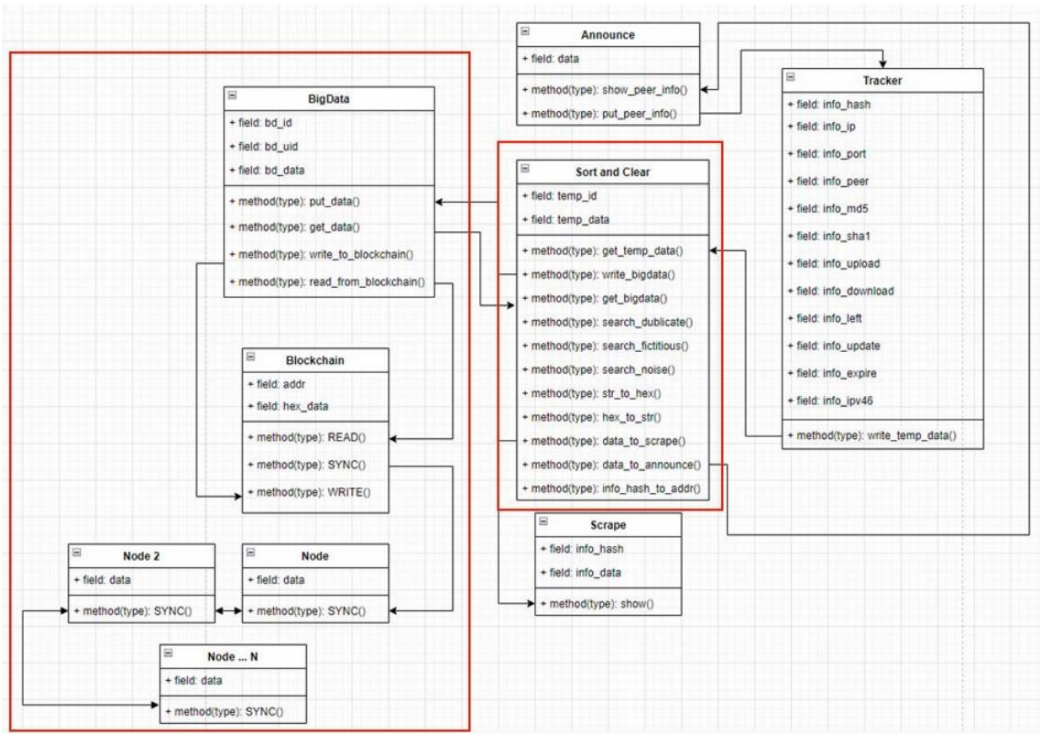


Рисунок 2.11 – Діаграма класів архітектури модулів

Таблиця 2.1 Атрибути класу «Announce»

Атрибут	Опис
Data	Вхідні дані, які поступають на анонсер

Таблиця 2.2 Методи класу «Announce»

Метод	Опис
Show_peer_info	Метод видобуткуданих та демонтрація його кліенту
Put_peer_info	Запис всіх вхідних даних в Tracker.

Таблиця 2.3 Атрибути класу «Tracker»

Атрибут	Опис
Info_hash	Інформація про хеш-ключ, є ідентифікатор
Info_ip	Інформація про IP клієнта, у числовому форматі

Кінець таблиці 2.3 Атрибути класу «Tracker»

Info_port	Інформація про порт клієнта
Info_peer	Інформація про ID піра клієнта
Info_md5	Хеш сума md5 для контроля цілісних даних
Info_sha1	Хеш сума sha1 для контроля цілісних даних
Info_upload	Інформація про роздане
Info_download	Інформація про скачане
Info_left	Інформація про те, скільки залишилось скачати
Info_update	Часова мітка останнього оновлення піру
Info_expire	Часова мітка неактуальності піра
Info_ipv46	IP адреса клієнта у вигляді IPv4, IPv6

Таблиця 2.5 Атрибути класу «Sort and Clear»

Атрибут	Опис
Temp_id	Ідентифікатор даних
Temp_data	Безпосередньо дані, що можуть бути в різних форматах

Таблиця 2.6 Методи класу «Sort and Clear»

Метод	Опис
Get_temp_data()	Видобуток тимчасових даних з бази даних
Write_bigdata()	Запис даних із тимчасової таблиці великих даних
Get_bigdata()	Читання даних із тимчасової таблиці великих даних

Кінець таблиці 2.6 Методи класу «Sort and Clear»

Search_dublicate()	Пошук та очистка дублікатів даних
Search_fictitions()	Пошук та очистка даних від фіктивних даних
Search_noise()	Пошук та очистка даних від шуму
Str_to_hex()	Перетворення стрічкових даних в hex вигляд
Hex_to_str()	Перетворення стрічкових даних в hex вигляду в стрічкові дані
Data_to_scrape()	Перетворення bencode, дані про сідів
Data_to_announce()	Перетворення bencode, дані про пірів
Info_hash_to_addr()	Перетворення info_hash в адресу на блокчейн мережі

Таблиця 2.7 Атрибут класу «BigData»

Атрибут	Опис
Bd_id	Ідентифікатор для тимчасовоїтаблиці
Bd_uid	Ідентифікатор uid, що дорівнює адресу в блокчейні
Bd_data	Дані в hex форматі

Таблиця 2.8 Методи класу «BigData»

Метод	Опис
put_data()	Запис даних
get_data()	Видобування даних
write_to_blockchain()	Запис великих даних у блокчейн через RPC API
read_from_blockchain()	Читання великих даних із блокчейну через RPC API

Таблиця 2.9 Атрибут класу «Blockchain»

Атрибут	Опис
addr	Ідентифікатор даних у блокчейні
hex_data	Великі дані у форматі hex

Таблиця 2.10 Методи класу «Blockchain»

Метод	Опис
READ()	Читання даних у блокчейн, де ідентифікатор адреса
WRITE()	Запис даних у блокчейн, де ідентифікатор адреса
SYNC()	Синхронізація даних з різними вузлами блокчейну

На рисунку 2.11 представлені дані, які чекають опрацювання та їх наступний запис у блокчейн.

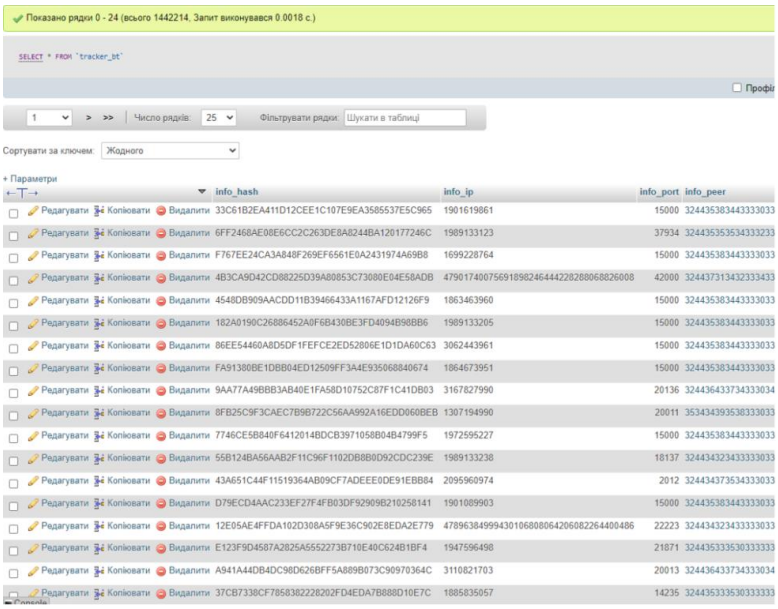


Рисунок 2.11 - Невідсортовані дані, отримані з анонсера за п’ять хвилин роботи системи, 1442214 записів

Перетворення ідентифікатора info_hash в адресу на мережі блокчейн, де будуть виконуватися транзакції даних. Зазвичай ідентифікатор info_hash представляє хеш-значення, отримане за допомогою криптографічних хеш-функцій, таких як SHA-1 або SHA-256. Цей хеш дозволяє перевірити цілісність і автентичність даних, надаючи унікальний ідентифікатор блоку даних або файлу. Можна виділити кілька основних класів для архітектури модулів системи підтримки на основі блокчейну для операційної системи Android. Клас користувача представляє користувача системи з його ідентифікатором, іменем, електронною поштою та паролем. Реєстрація, вхід і вихід користувача — це методи цього класу.

Клас аутентифікації відповідає за перевірку користувачів. Він містить характеристики та стан аутентифікації токену, а також методи валідації та аутентифікації токену.

Таблиця 2.11 Генерація ідентифікатоар в Blockchain мережі

info_hash ідентифікатор	33C61B2EA411D12CEE1C107E9EA3585537E5C965
Адреса на Blockchain	2ExVocnskqgHXHmPSVZRBk5LWb8NsCXmf9
Закритий ключ для доступа до адреси	5JyQFzBdYyg6LF9xdNkC59nC6FPJ8PJSQPRvVn8on946YASVr6j

На рис. 2.12 показано дані, які вже зареєстровані в блокчейні та синхронізовані між двома нодами підтвердження, де OP_RETURN є хешованим великим даним. Хешовані великі дані використовуються для забезпечення безпеки та цілісності великих обсягів інформації. Цей процес полягає у створенні унікального "відбитка" або хеш-коду для кожного набору даних, який є невід'ємною частиною криптографічних протоколів та алгоритмів, використовуваних у різних сферах, включаючи кібербезпеку, фінанси та обробку даних. Це дозволяє ефективно виявляти будь-які зміни в даних та захищати їх від несанкціонованого доступу та маніпуляцій.

Хешовані великі дані є ефективним інструментом для перевірки цілісності та автентифікації великих обсягів інформації.

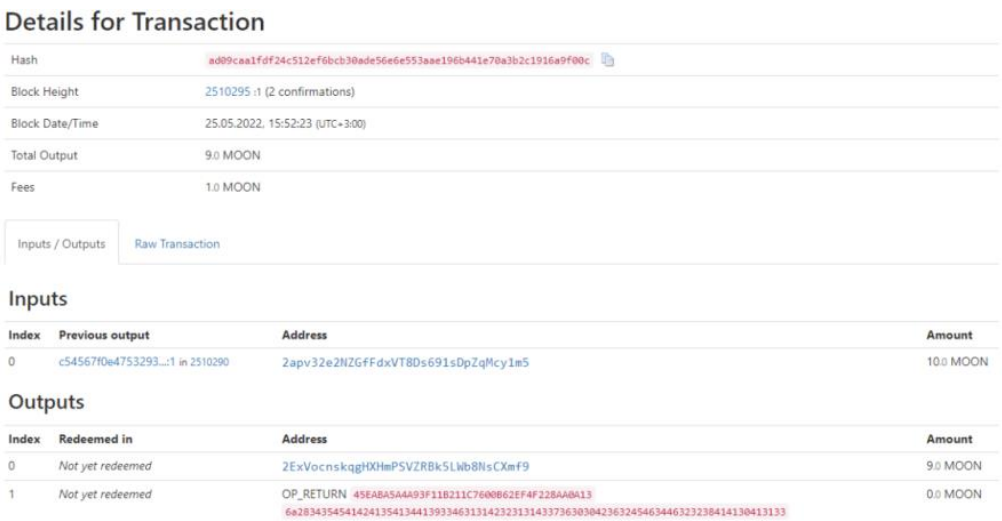


Рисунок 2.12 – Транзакція, яка вже назавжди записана в Blockchain

На рисунку 2.13 показано адресу 2ExVocnskqgHXHmPSVZRBk5LWb8NsCXmf9 із ідентифікатором рівня 33C61B2EA411D12CEE1C107E9EA3585537E5C965, яка містить інформацію про кількість пірів. Транзакція, яка була вже задокументована в блокчейні, є важливою частиною історії цієї блокчейн-мережі. Коли транзакція отримає підтвердження та включена до блоку, який додається до ланцюжка блоків, вона стає важливою частиною історії блокчейну. Це означає, що неможливо видалити або змінити цю транзакцію без внесення змін до самого блокчейну. Через криптографічну стійкість блокчейн-технології це майже неможливо. Здатність криптографічних алгоритмів залишатися стійкими до спроб розшифрування чи злому, навіть за наявності великої кількості обчислювальних ресурсів або доступу до шифрованої інформації, називається криптографічною стійкістю. Криптографічні алгоритми повинні бути стійкими до таких атак, як перебір ключів, злам шифру, внесення змін у шифрований текст та інші криптоаналітичні атаки, щоб забезпечити криптографічну стійкість. Цей аспект забезпечує захист конфіденційності, цілісності та доступності шифрованих

даних, і він є життєво важливим для використання криптографічних методів у сучасних системах безпеки та захисту інформації.

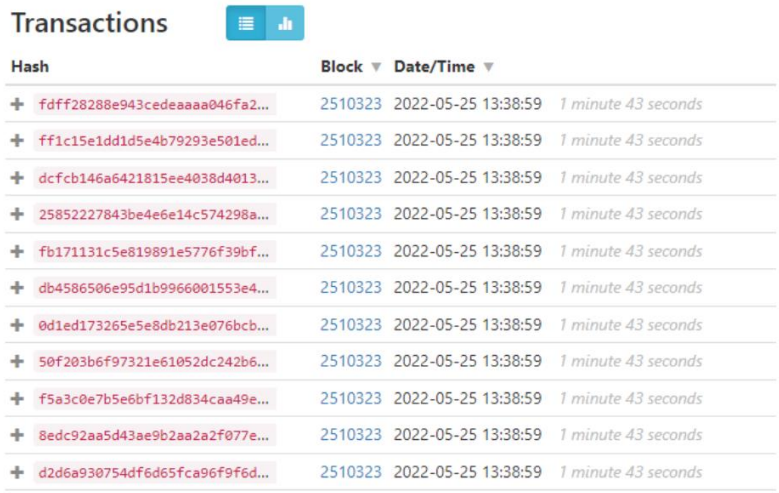


Рисунок 2.13 – Список транзакцій, які містять в собі інформацію про кількість пірів

На рисунку 2.14 показано приклад того, як блокчейн даної системи побудований: він складається з seed адрес, на які приходять монети за допомогою майнінгу. Враховуючи низьку складність цього блокчейну, для майнінга використано три сервери конфігурації: AMD Ryzen 9 5950X [16c / 32t] (3.4 GHz) з 128 GB DDR4 ECC RAM і 2 x 3.84TB NVMe. Можете записувати транзакції в блоках, використовуючи монети, які позначені як монети з одним виходом. У кожному блокі встановлено рівні розміру 10 MB, що дає можливість записувати велику кількість даних у один блок (рис. 2.15). Потрібно мати закритий ключ адреси, щоб отримати ці дані. Секретний криптографічний ключ, який використовується в криптовалютних системах, таких як Bitcoin, для підпису транзакцій і забезпечення безпеки фінансових операцій, називається закритим ключем адреси. Щоб створити криптографічний підпис за допомогою його закритого ключа, власник адреси або гаманця може підтвердити свою ідентичність і авторство транзакцій, що надходять із цієї адреси.

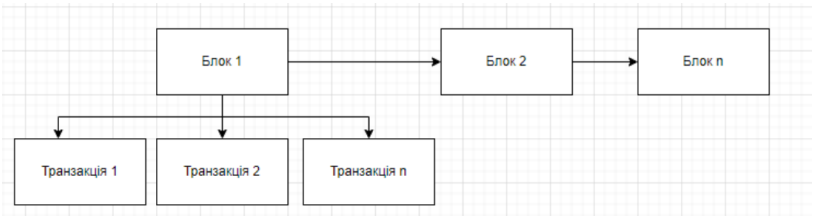


Рисунок 2.14 – Структура блокчейну в системі

Timestamp	Block	Hash	Amount (YTN)	Balance (YTN)	TX Type
2022-05-20 08:29	1167164	321b08aa1dd6d6dd3115b02eafdf84b7380aad9b97d2eba4425403e9ed236d2c	25.01607251	201311.25769456	
2022-05-20 02:09	1166985	c72598af9b9ba5102418a848c9336bf2eaf0550c547087212f577204e8e9fb52	25.00000000	201286.24162205	
2022-05-20 01:29	1166962	354caaefddff0ddc42f5bb3a158f802b7cabe6322fe4845ff21094def4cdf4f5	25.00000000	201261.24162205	
2022-05-19 23:22	1166901	c7fae9b5b20cdc063ff173168e773667319aa8a2a8f1213dc357447f3f114448	25.00000000	201236.24162205	
2022-05-19 22:53	1166882	9e1ca330ea497af33ac3f2910a96211f50c79c34177a4734195b31d27d4e41af	25.00000000	201211.24162205	
2022-05-19 19:56	1166802	fac77ec015b5c0d8e9d41f0e86f51d9847193c7a3fde72022ac8fa163ae99d5f	25.00000000	201186.24162205	
2022-05-19 10:23	1166520	78760b2aa432992b4525fa6571e9d5b3510338695ecc3471a243e677e7e170b1	25.00000000	201161.24162205	
2022-05-19 09:23	1166493	4a7d657c1a83471476769 27cd2d260cfa047c44c84653a83f1a1b1ea0366a4d4	25.10000000	201136.24162205	
2022-05-19 06:43	1166420	450a97705d97416b054b052dca534474985156f6b80f95a72e3b02189f1eee1a	25.00000000	201111.14162205	
2022-05-19 04:43	1166351	2c07f21f9ded7cb796f278094a9841134f3cb7c2284664812a29b3d731df4877	25.00000000	201086.14162205	
2022-05-19 03:59	1166331	04e9d5ed155f627ff75452cbc30cc179f5acac0cf2c9b5302ed37f557823f933	25.00000000	201061.14162205	
2022-05-19 03:35	1166319	a964a676957ff56c66915ebeaee431bf520385f7dd96c19c81496e99c74249ab	25.00000000	201036.14162205	
2022-05-19 01:31	1166260	67b20a4da6ec6c7b2ed675c89322e0e287415a7e7e15c7af95443b998e309fe4	25.10000000	201011.14162205	
2022-05-18 22:54	1166185	8854cab1cefb49f3a85f897eb66e5f1d46a3b14cdab2da722066b37b1faabd6b	25.00000000	200986.04162205	
2022-05-18 20:24	1166107	1816efc60ee8ee9e8eaa8c4c0e132008827010722e68e2e1952d4f1244bf6216	25.00000000	200961.04162205	
2022-05-18 19:34	1166082	0b635cf0c01ac744b6b8656bc253742096e8d5f9be8bf12c35efc8c537099ae6	25.14468830	200936.04162205	
2022-05-18 19:26	1166076	d644144a79bdb038789765abe5fc068afb30628003b6f8ea8da3c17350e05382	25.08469991	200910.89693375	
2022-05-18 18:35	1166051	ee37652916c5b634aabac93fd19638dca4ca85124f2212d5750ca456c80d8630	25.00000000	200885.81223384	

Рисунок 2.15 – Генерація монет за допомогою майнінгу для наступних транзакцій у блокчейн на seed адресу

2.7 Висновок

Дизайн архітектури системи для криптовалютних операцій на платформі Android включає кілька важливих елементів, які гарантують функціональність, безпеку та масштабованість.

Процес вибору блокчейн-платформи для інтеграції в операційну систему Android є вирішальним кроком, який визначає продуктивність і можливості майбутньої системи. Такі платформи, як Solana, Ethereum і Binance Smart Chain, є найкращими варіантами, оскільки вони мають широкий спектр функцій, таких як надійну підтримку розробників, високу пропускну здатність і розумні контракти.

Вибір базується на кількох критеріях, включаючи продуктивність, екосистему розробників, безпеку та підтримку мобільних SDK.

Детальне планування структури даних і методів їх обробки необхідне для створення і послідовного опрацювання інформаційної моделі великих даних. Моделювання транзакцій, використання даних і взаємодія з блокчейном є частиною цього.

Для ефективного зберігання та обробки даних необхідно враховувати обсяг даних, необхідний для обробки, безпеку та швидкість доступу. Для аналізу великих масивів даних у режимі реального часу може бути виправданим використання технологій, таких як Hadoop чи Spark.

Для того, щоб інтерфейс користувача був зручним для користувача для управління криптовалютою, його дизайн повинен бути спрямований на створення простого та функціонального інтерфейсу користувача, який дозволить користувачам легко виконувати операції з криптовалютою. Це включає створення адаптивного дизайну для різних розмірів екрану, інтеграцію з графічними бібліотеками для візуалізації даних, такими як D3.js або Chart.js, і гарантію високої продуктивності для швидкого реагування на дії користувачів.

Для того, щоб мобільні програми могли взаємодіяти з блокчейн-вузлами, протокол комунікації повинен забезпечити надійне та безпечне з’єднання між клієнтською частиною та блокчейном. Ефективний обмін даними залежить від використання RESTful API або WebSocket в реальному часі. Для забезпечення безпеки та стабільності протокол має включати процедури аутентифікації та авторизації, шифрування даних і обробки помилок.

Інтеграція функцій Android, таких як NFC та біометрична автентифікація, значно покращує досвід користування. Користувачі можуть здійснювати швидкі та безконтактні платежі за допомогою NFC. Наприклад, біометрична автентифікація за допомогою відбитків пальців або розпізнавання обличчя підвищує безпеку, забезпечуючи швидкий і надійний доступ до додатків. Такі функції роблять використання програми більш безпечним і зручним.

Успіх платформи залежить від забезпечення відмовостійкості та масштабованості системи, щоб вона могла обробляти велику кількість транзакцій. Для забезпечення стабільної роботи системи навіть під високими навантаженнями це включає використання кластерів серверів, впровадження резервних копій і реплікацій даних і балансування навантаження.

3 РЕАЛІЗАЦІЯ БЛОКЧЕЙН-БАЗОВАНОЇ СИСТЕМИ

3.1 Розробка мобільного додатку для ОС Android з урахуванням визначених вимог

Розробка мобільного додатку для ОС Android вимагає уважного урахування різних вимог для досягнення успішного результату. У процесі розробки додатку важливо врахувати такі аспекти:

Функціональність додатку необхідно чітко визначити функціональні можливості додатку, відповідно до потреб його майбутніх користувачів. Це може включати функції, такі як реєстрація користувачів, авторизація, відображення контенту, обробка оплати та інші.

Користувацький інтерфейс важливо створити зручний та інтуїтивно зрозумілий інтерфейс, який дозволить користувачам легко взаємодіяти з додатком та використовувати його функції без зайвих складнощів, зображено на рисунку 3.1.

Рисунок 3.1 –інтерфейс панелі керування програмою ОС Android.

Дизайн естетика та зручність дизайну мають велике значення для привабливості додатку для користувачів. Необхідно розробити візуальну концепцію, яка відповідає цілям та аудиторії додатку.

Безпека забезпечення безпеки даних користувачів є пріоритетом. Додаток повинен використовувати надійні методи шифрування та захисту для зберігання та обробки конфіденційної інформації, зображено на рисунку 3.2.

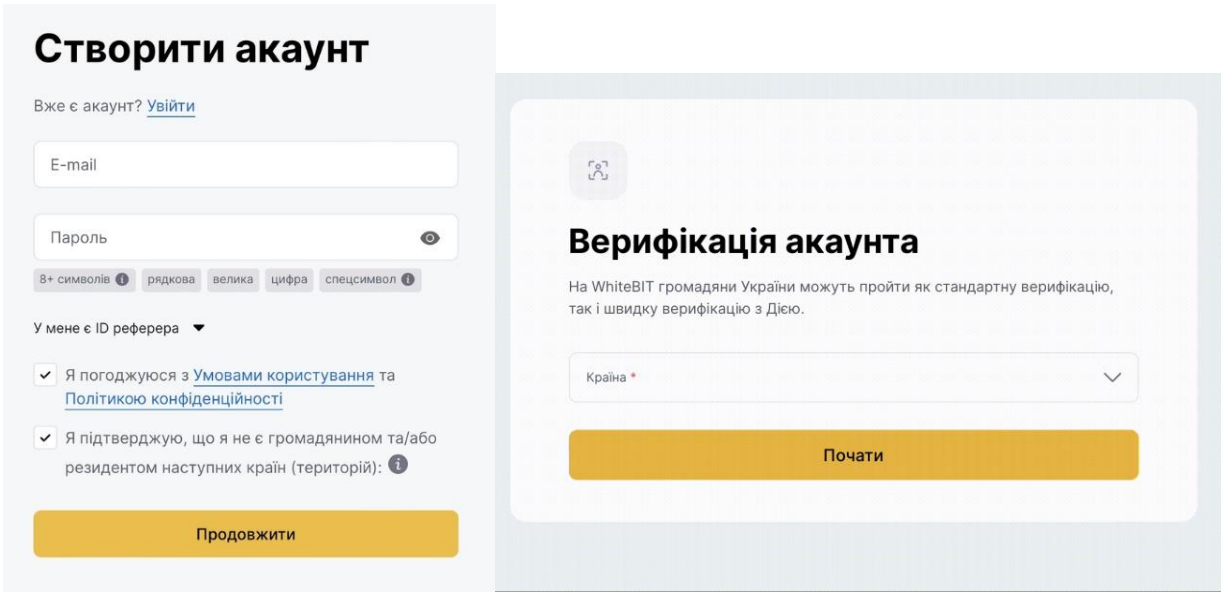


Рисунок 3.2 – Створення кабінету та верифікація для безпечного використання додатку.

Продуктивність важливо, щоб додаток працював ефективно та швидко на різних пристроях, незалежно від їх характеристик та версії ОС Android.

Тестування перед випуском виробу важливо провести тестування, яке включає функціональне тестування, тестування на відмовостійкість, тестування на сумісність з різними пристроями та інші види тестування, щоб гарантувати якість продукту. Врахування цих вимог у процесі розробки дозволить створити додаток, який відповідає потребам користувачів та забезпечує їм позитивний досвід використання. Розробка мобільного додатку для ОС Android, який є блокчейн-базованою системою підтримки криптовалютних операцій, вимагає уважного аналізу, проектування та розробки з урахуванням основних вимог. Це означає розробку додатку, який дозволяє

користувачам здійснювати різні операції з криптовалютами, включаючи створення гаманців, відправлення та отримання транзакцій, перегляд балансу та історії операцій, інтеграцію з блокчейн-мережами та забезпечення високого рівня безпеки та приватності для користувачів.

Щоб гарантувати успішну та надійну реалізацію продукту, необхідно враховувати багато важливих моментів під час розробки додатку для взаємодії з блокчейном.

Безпека є одним із найважливіших елементів. Через те, що вони децентралізовані, блокчейн-додатки дуже вразливі. Отже, важливо вивчити та використовувати найкращі практики безпеки, такі як шифрування даних, захист від кібератак, безпечне зберігання приватних ключів і перевірка вхідних даних.

Другим важливим фактором є швидкість. Користувачі очікують миттєвої відповіді від додатків, тому програми повинні оптимізувати роботу, щоб скоротити час відповіді та збільшити продуктивність. Користувацький досвід також важливий. Інтуїтивно зрозумілий і зручний інтерфейс додатку дозволяє користувачам мати позитивний досвід використання та легко взаємодіяти з ним.

Масштабованість також має бути врахована. Додаток повинен бути розроблений таким чином, щоб він міг адаптуватися до збільшення кількості операцій і користувачів. Оскільки багато країн ще не повністю регулюють блокчейн-технологію, важливо дотримуватися відповідних законів і правил.

Тестування також відіграє важливу роль у процесі розробки. До випуску продукту на ринок важливо провести ретельне тестування, щоб знайти та виправити помилки.

Зрештою, розробка додатків для взаємодії з блокчейном є складним процесом, який вимагає уваги багатьох важливих елементів, таких як безпека, швидкодія, користувацький досвід, масштабованість, дотримання правил і тестування. Крім того, важливо постійно вдосконалювати додаток, щоб залишатися конкурентоспроможним і залишатися актуальним на ринку, враховуючи зміни в технологічному середовищі та потреби користувачів.

3.2 Інтеграція системи з основними блокчейн-вузлами та мережами криптовалют

У процесі інтеграції системи з основними блокчейн-вузлами та мережами криптовалют необхідно враховувати кілька важливих елементів, а також інноваційні рішення, які з'явилися останнім часом. Насамперед потрібно розгорнути та налаштувати вузли відповідних блокчейн-мереж, наприклад Bitcoin, Ethereum та інші популярні криптовалюти.

Це дозволяє підключитися до блокчейн-мережі та взаємодіяти на рівні протоколу. Зазвичай для цього використовуються офіційні клієнти або програмне забезпечення з відкритим кодом. Після налаштування вузлів необхідно інтегрувати API, щоб забезпечити взаємодію між блокчейн-вузлами та системою. За допомогою API системи можуть відправляти та отримувати транзакції, отримувати інформацію про баланс, підтверджувати транзакції, отримувати дані про блоки та інші необхідні дані. Звичайні блокчейни мають добре задокументовані API, що полегшує роботу.

Синхронізація даних у блокчейн-мережі є життєво важливою, щоб гарантувати, що інформація залишається актуальною. Це можна зробити за допомогою WebSocket або іншого механізму, який дозволяє отримувати оновлення в реальному часі з мережі. Наприклад, багато систем використовують функцію підписки на події, щоб отримувати сповіщення про нові блоки або транзакції. Це дозволяє системі швидко відповідати на зміни в блокчейні.

Додаткові інструменти, такі як балансувальники навантаження, кластери вузлів і механізми резервного копіювання даних, можуть використовуватися для забезпечення надійності та масштабованості інтеграції. Алгоритми консенсусу, розмір блоків і час підтвердження транзакцій — це деякі з технічних елементів, які мають значення для окремих блокчейн-мереж, зображено на рисунку 3.3. Розподілена мережа комп'ютерів (вузлів), які взаємодіють між собою для обробки та зберігання даних у формі блоків даних, які постійно змінюються та оновлюються, відома як блокчейн-мережа. Кожен блок містить дані про кількість транзакцій або подій, які учасники мережі підтвердили та підписали.

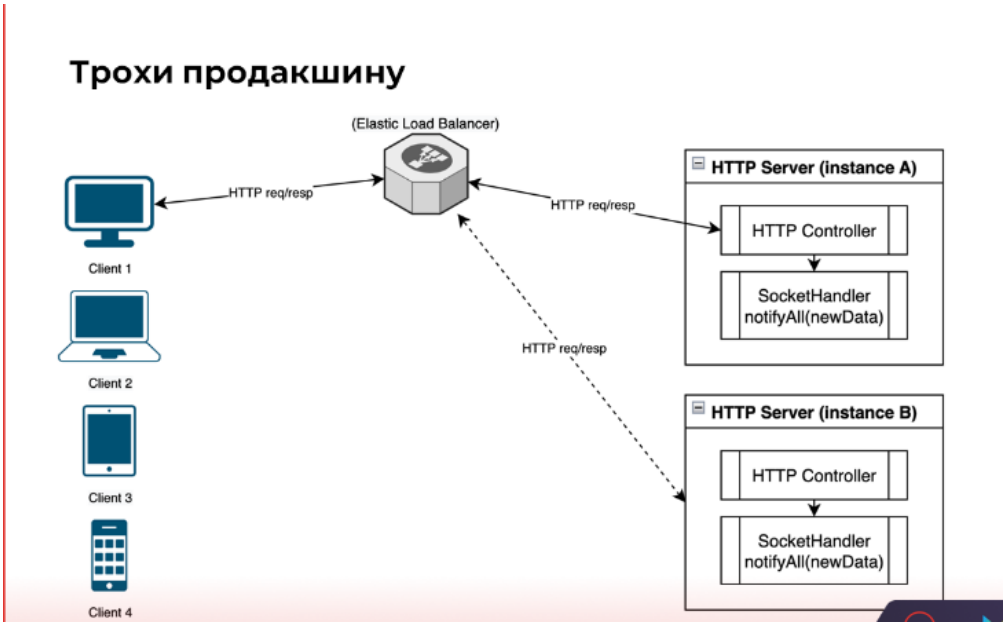


Рисунок 3.3 – Ініціація з’єднання WebSocket

Крім того, необхідно враховувати регуляторні та правові вимоги, які можуть відрізнятися залежно від юрисдикції. Це може включати вимоги щодо зберігання та звітності даних, а також захисту персональних даних користувачів. Для роботи з розумними контрактами, особливо на платформах як Ethereum, важливо мати можливість взаємодіяти з контрактами через ABI. Це дозволяє виконувати функції, пов’язані з контрактом, проводити транзакції та отримувати інформацію. Інтеграція в протоколи децентралізованої фінансової (DeFi) стає все більш важливою. Це означає, що ви можете взаємодіяти з різними фінансовими послугами, такими як стейкінг, позики, кредити та децентралізовані біржі (DEX). Масштабування залишається важливим компонентом. Набирає популярності використання шарових рішень (Layer 2) для підвищення продуктивності та зниження транзакційних витрат. Наприклад, з’єднання з Lightning Network для Bitcoin або Rollups для Ethereum дозволяє обробляти більше транзакцій з меншою вартістю та швидшою обробкою. Крім того, спостереження та аналітика є важливими. Регулярний моніторинг таких елементів, як транзакції, продуктивність вузлів, стан мережі та інші, сприяє стабільності та ефективності системи. Використання інструментів аналітики дозволяє оптимізувати процеси та краще зрозуміти поведінку користувачів. Інтеграція з оракульськими службами, які надають зовнішні дані, для розумних контрактів,

включає інновації. Доступ до реальних даних дозволяє створювати більш складні та корисні смарт-контракти. Крім того, слід звернути увагу на нові криптографічні технології, такі як zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge), які покращують масштабованість і конфіденційність транзакцій. Цей тип технологій має потенціал значно покращити безпеку та конфіденційність інтегрованих рішень. Впровадження систем автоматизованого тестування та валідації інтеграції є важливим компонентом. Це включає тестування контрактів, API, вузлів та інших системних компонентів, щоб переконатися, що вони працюють правильно та виявити потенційні проблеми на ранніх стадіях, зображено на рисунку 3.4.

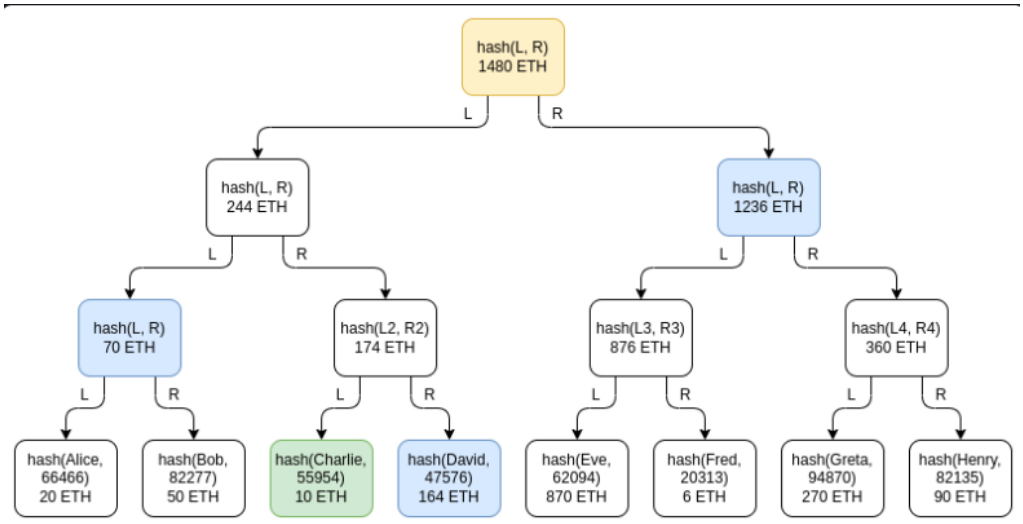


Рисунок 3.4 – Блок-схема хешингу zk-SNARKs [45]

В кінцевому підсумку процес інтеграції вимагає постійного моніторингу та обслуговування вузлів, щоб гарантувати безпеку роботи. Це включає оновлення програмного забезпечення до найновіших версій, відстеження мережевого трафіку та реагування на потенційні інциденти або атаки. Це гарантує стабільне функціонування системи та дозволяє швидко вирішувати будь-які технічні проблеми. Під час розробки програми, яка працює з блокчейном, важливо враховувати, що система повинна забезпечувати стабільне функціонування, незважаючи на зміни в навколишньому середовищі. Це означає, що програмне забезпечення повинно бути добре написане, оптимізоване та масштабоване, щоб воно могло ефективно виконувати велику

кількість завдань. Крім того, додаток повинен містити механізми швидкого виявлення та вирішення будь-яких потенційних технічних проблем.

3.3 Тестування розробленого додатку для перевірки його працездатності та безпеки

Тестування програмного забезпечення, розробленого для перевірки його працездатності та безпеки, є складним і важливим процесом, який складається з багатьох аспектів. Щоб гарантувати, що додаток працює належним чином і є захищеним від будь-яких загроз, воно потребує ретельного планування, виконання та аналізу результатів. Визначення вимог до програми є першим кроком до тестування. Це передбачає знання функціональних і нефункціональних вимог, які були встановлені в процесі розробки. Нефункціональні вимоги включають елементи, такі як надійність, сумісність, продуктивність і безпека. Функціональні вимоги визначають, що додаток повинен робити. Визначення вимог дозволяє створити чіткі стандарти для оцінки роботи та безпеки програми. Після визначення вимог наступним кроком є створення сценаріїв для тестування. Всі аспекти функціональності програми, включаючи основні та крайні випадки використання, повинні бути включені до тестових сценаріїв. Крім того, вони повинні включати тести на продуктивність і безпеку, щоб визначити потенційні вразливості додатку. Для повної оцінки програми важливо створити сценарії тестування як позитивних, так і негативних. Наступним кроком є налаштування середовища тестування. Це середовище повинно бути якнайближче до реальних умов, у яких працює додаток. Всі необхідні апаратні та програмні частини, такі як сервери, бази даних, мережеве обладнання та інші залежності, повинні бути включені в тестове середовище. Для отримання точних результатів тестування важливо правильно налаштувати тестове середовище. Різне тестування є важливою частиною процесу перевірки програмного забезпечення. Тестувальники перевіряють, чи працює додаток відповідно до очікувань, виконуючи розроблені тестові сценарії вручну. Проблеми з автоматизованими тестами, такі як проблеми з інтерфейсом користувача або досвідом

користувача, можна виявити шляхом ручного тестування. Крім того, при незвичайних взаємодіях з додатком тестувальники можуть виявити непередбачувані помилки. Автоматизоване тестування є ще одним важливим компонентом перевірки безпеки та працездатності програми. Автоматизовані тести дозволяють швидко та ефективно перевіряти велику кількість сценаріїв тестування, значно зменшуючи час і витрати на тестування. Інструменти автоматизованого тестування можуть бути налаштовані для виконання тестів на функціональність, продуктивність, безпеку тощо. Автоматизовані тести повинні регулярно оновлюватися, щоб вони відповідали поточному стану додатку. Тестування продуктивності є важливим для визначення здатності програми працювати в реальному часі. Це включає тести на стабільність і навантаження, які оцінюють стійкість програми під час тривалого використання; і тести на навантаження та стрес, які оцінюють здатність програми витримати значні навантаження. Тестування продуктивності допомагає виявити проблеми та оптимізувати програму, щоб вона працювала краще під навантаженням. Тестування безпеки є важливою частиною перевірки програмного забезпечення, зображено графічним описом на рисунку 3.5.

Рисунок 3.5 – QWASP тестувальна технологія [48]

Проект Open Web Application Security, або QWASP, є групою експертів з кібербезпеки, які зосереджені на покращенні безпеки веб-додатків. OWASP

розробляє інструменти, інструкції та поради для виявлення та ліквідації різноманітних загроз безпеці веб-додатків, таких як SQL-ін’єкції, крос-сайтовий скриптінг і вразливості з контролю доступу. Усі члени спільноти кібербезпеки можуть безкоштовно використовувати їхні матеріали та проекти.

Це включає виявлення та усунення вразливостей, які зловмисники можуть використовувати для пошкодження програми. Тестування безпеки включає перевірку відповідності додатку стандартам безпеки, аналіз коду на наявність вразливостей і тестування на проникнення, що імітує атаки зловмисників. Використання програм для автоматизованого тестування безпеки зменшує ризик експлуатації вразливостей і дозволяє швидко виявляти потенційні проблеми. Регресійне тестування є важливою частиною тестування програми. Після внесення змін до коду програми це тестування проводиться, щоб переконатися, що зміни не викликали нових проблем або помилок. Регресійне тестування гарантує, що програмне забезпечення залишається стабільно та працездатним після внесення виправлень і оновлень. Залежно від складності та обсягу змін, регресійне тестування може виконуватися як вручну, так і автоматизовано. Тестування сумісності є ще одним важливим етапом перевірки програми. Це перевіряє роботу програми на різних браузерах, платформах, операційних системах та пристроях. Тестування сумісності є важливим для забезпечення широкого охоплення користувачів, оскільки воно гарантує, що додаток працює коректно в різних середовищах і конфігураціях обладнання. Щоб переконатися, що додаток працює безперебійно, важливо враховувати різні версії операційних систем, браузерів та інші залежності. На додаток до технічних аспектів важливим є тестування зручності використання додатку. Це включає оцінку того, наскільки легко виконувати основні завдання, наскільки простий інтерфейс користувача та наскільки додаток відповідає очікуванням користувачів.

Залучення реальних користувачів для проведення тестів і збору коментарів може бути частиною процесу тестування зручності використання. Це допомагає виявити проблеми з функціональністю та дизайном, які впливають на задоволеність користувачів. Перевірка інтеграції з іншими системами та сервісами є ще одним важливим компонентом тестування. Це включає компоненти, які взаємодіють з

програмою, такі як тестування API, перевірка сумісності з базами даних, серверні сервіси та інші. Тестування інтеграції гарантує, що всі частини системи працюють одна з одною належним чином і що між ними не виникає проблем при обміні даними. Після завершення тестування та вирішення проблем важливе проведення приймального тестування. Це тестування проводиться, щоб переконатися, що додаток відповідає всім встановленим вимогам та стандартам якості. Кінцеві користувачі або замовники перевіряють, чи відповідає додаток їхнім очікуванням. Приймальне тестування є останнім кроком перед тим, як програму можна запустити в продуктивне середовище. Документування процесу тестування також є важливою частиною. Журнали тестування, звіти про помилки, результати тестів та інші відповідні документи є частиною цього. Документація забезпечує прозорість процесу тестування для всіх зацікавлених сторін, допомагає відстежувати прогрес тестування та аналізувати проблеми та виправлення. Після впровадження програми в продуктивне середовище необхідно продовжувати моніторинг його роботи. Це включає регулярне оновлення програми для усунення вразливостей і проблем, виявлення та реагування на інциденти безпеки та збір і аналіз метрик продуктивності. Постійний моніторинг сприяє підтримці високої якості та безпеки програми протягом його життєвого циклу. У процесі тестування людина має вирішальне значення, крім технічних аспектів. Це включає навчання та підтримку тестувальників, надання їм необхідних ресурсів і інструментів, а також створення приємного робочого середовища. Успішне тестування додатку залежить від ефективної взаємодії та спілкування розробників, тестувальників та інших учасників проекту.

3.4 Розроблення алгоритму хешування

Розробка алгоритму хешування: алгоритм хешування scrypt був обраний на основі порівнянь 82 функцій хешування, і він був модифікований, щоб покращити захист даних, додавши його до іншого алгоритму хешування yescrypt. Майнеры створюють монети для майбутніх транзакцій, використовуючи консенсус Proof of Work для побудови самого блокчейна.

Алгоритм хешування, який був розроблений для роботи, включає наступні кроки. Визначення вихідної інформації Підготовка вихідних даних, а також форматування та кодування Якщо обробляється велика кількість інформації, її можна розділити на окремі блоки. використання хеш-функції, яка була спеціально розроблена для використання у вихідних даних. Ця функція може містити алгоритми та операції, які відрізняються від традиційних хеш-функцій. Обробка результатів дозволяє отримати готовий хеш, який можна використовувати для перевірки цілісності або ідентифікації даних. Застосування хеш-функції до вихідних даних може потребувати додаткової обробки, щоб отримати кінцевий хеш. — Параметри складності пошуку функції (рис. 3.6)

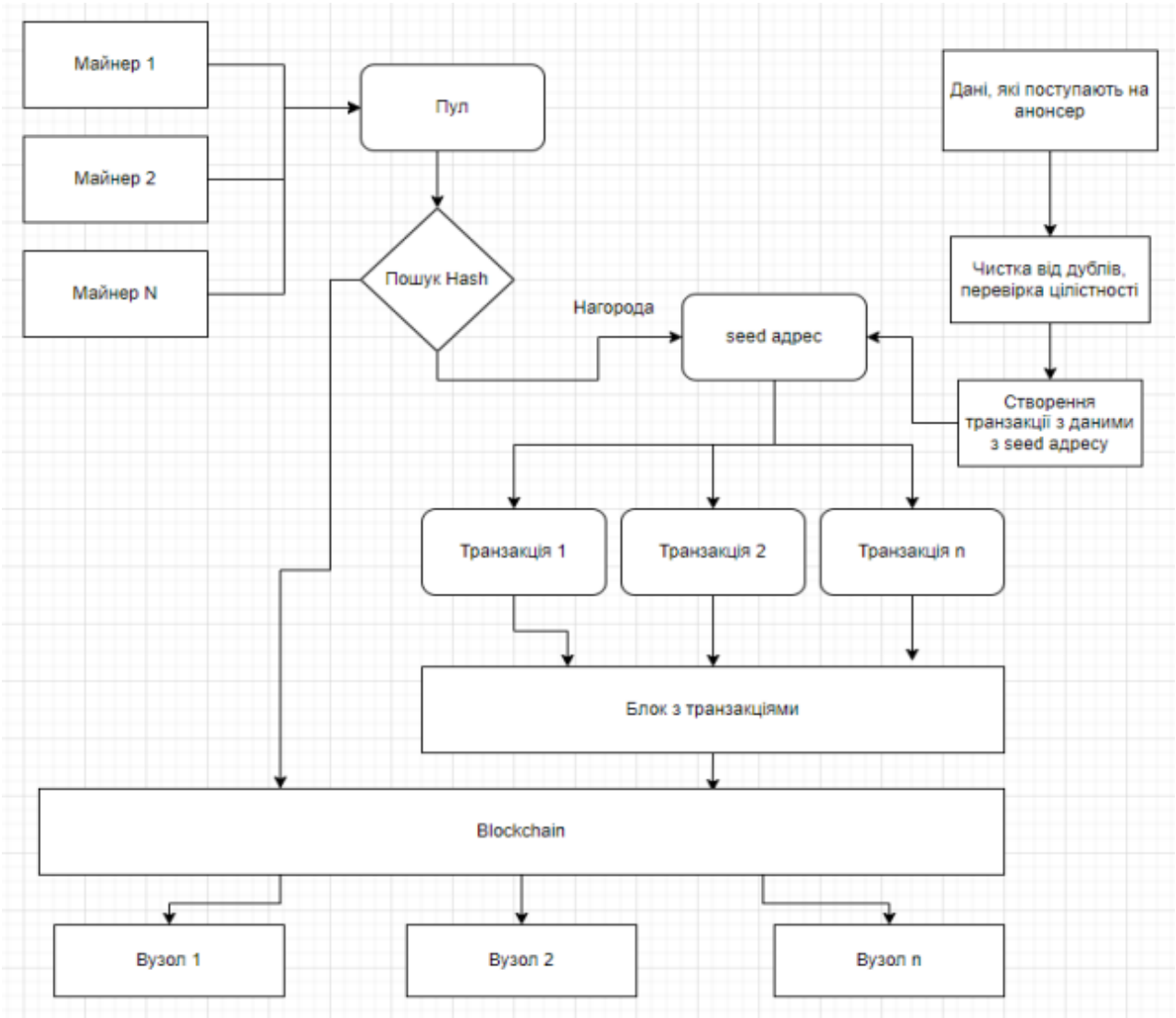


Рисунок 3.6 – Алгоритм опрацювання даних у блокчейн

Для майнінгу цього хеш-алгоритму можна використовувати CPU, GPU та ASIC-схеми, а час генерації одного блока становить 1 хв. Блок містить 100 мегабайтів, а транзакції можуть мати максимум 100 мегабайтів за хвилину. Використовується консенсус Proof of Work (PoW), коли майнери необхідні для емісії. Алгоритм має більше переваг, ніж недоліків, оскільки він працює достатньо швидко для пошуку нових блоків і підтвердження транзакцій. Це може включати комбінування або конкатенацію хеш-значень різних блоків, обчислення контрольної суми або використання певних алгоритмів для обробки вихідного хешу.

3.5 Вдосконалення системи на основі отриманих результатів тестування та початкових проектів

Основним етапом життєвого циклу розробки програмного забезпечення є завершення системи на основі результатів тестування та пілотних проектів. Аналіз даних, виявлення проблем, розробка та впровадження покращень і повторне тестування для підтвердження ефективності змін є частиною цього процесу. Вдосконалення системи сприяє високій якості, стабільності та безпеці програмного забезпечення, що є важливим для задоволення потреб користувачів і досягнення бізнес-цілей. Аналіз результатів тестування та пілотних проектів є першим кроком у процесі вдосконалення системи. Це стосується збору та систематизації даних про продуктивність системи, виявлені помилки, користувацький досвід та інші важливі елементи. Аналіз даних допомагає зрозуміти проблеми, які впливають на роботу системи, і де потрібно вдосконалення. Важливо використовувати різноманітні методи аналізу, такі як статистичний аналіз, лог-файли, відгуки користувачів та інші джерела даних для отримання повної картини. Після аналізу даних не потрібно визначати найважливіші вдосконалення. Це включає оцінку важливості проблем, їхнього впливу на користувачів і бізнес-процеси, а також ресурсів, необхідних для їх вирішення. Принцип пріоритетності допомагає визначити, які покращення повинні бути впроваджені першочергово, щоб система та користувачі були максимально задоволені. При визначенні пріоритетів важливо враховувати як короткострокові, так

і довгострокові цілі. Наступним важливим кроком є розробка стратегії вдосконалення. План повинен містити детальний опис змін, які будуть впроваджені, включаючи технічні вимоги, відповідальних осіб, необхідні ресурси та терміни виконання. Щоб оцінити ефективність впровадження кожного вдосконалення, важливо також визначити критерії успіху. План вдосконалення забезпечує систематичний підхід до покращення системи та допомагає команді координувати свою роботу. Процес вдосконалення системи включає розробку та впровадження технічних покращень. Написання нового коду, виправлення помилок, оптимізація процесів і алгоритмів, інтеграція нових модулів і функцій є всіма прикладами цього процесу. Щоб забезпечити надійність і стабільність системи, важливо дотримуватися принципів якості коду, таких як модульність, повторне використання коду, тестування та документування. Для забезпечення належного впровадження покращень розробники повинні співпрацювати з тестувальниками та іншими зацікавленими сторонами. Після впровадження нових версій системи необхідно провести ретельну перевірку, щоб переконатися, що всі зміни в системі працюють належним чином і не викликають нових проблем. Щоб переконатися, що нові зміни не впливають на існуючі функціональні можливості системи, тестування повинні включати функціональні, безпекові та регресійні тести. Для досягнення необхідно використовувати як ручні, так і автоматизовані методи тестування.

Процес вдосконалення системи залежить від оцінки результатів тестування. Це включає виявлення потенційних проблем, аналіз результатів тестів і оцінку ефективності внесених змін. Щоб вдосконалити систему, важливо, щоб результати тестування були відкритими та записані. Оцінка результатів допомагає приймати рішення щодо готовності системи до роботи в продуктивному середовищі. Результати тестування можуть вказати на необхідність додаткових вдосконалень і змін. Це може включати усунення нових помилок, оптимізацію продуктивності або додавання нових функцій, які користувачі запропонували під час пілотних проектів. У процесі вдосконалення системи важливо забезпечити гнучкість і адаптивність, щоб мати можливість швидко реагувати на нові проблеми та вимоги. Після завершення тестування та внесення необхідних покращень наступним кроком є впровадження

системи в робоче середовище. Важливо скласти детальний план впровадження, який включатиме процедури, терміни та відповідальних осіб. Щоб зменшити потенційні ризики та гарантувати безперебійний перехід на нову систему, впровадження повинно бути ретельно сплановано та організовано. Забезпечити достатню підтримку користувачів під час впровадження, включаючи навчання, технічну підтримку та інші необхідні ресурси, є важливим. Після впровадження системи в робочу середу важливо продовжувати її моніторинг. Це включає постійний збір даних про роботу системи, виявлення потенційних проблем і аналіз відгуків користувачів. Забезпечуючи високу якість і стабільність системи, моніторинг допомагає виявити нові проблеми на ранніх стадіях і оперативно реагувати на них. Крім того, важливо регулярно оновлювати систему та створювати нові покращення на основі зібраних даних та зворотнього зв'язків. Важливо враховувати організаційні та управлінські аспекти вдосконалення системи, крім технічних аспектів. Підтримка користувачів, управління змінами та стратегії комунікації входять до цього. Зміна внутрішніх процесів і організаційної структури може бути необхідною для вдосконалення системи, тому важливо забезпечити належне управління цими змінами. Завдяки взаємодії з користувачами та іншими зацікавленими сторонами можна отримати підтримку та залучення всіх, хто бере участь у процесі вдосконалення. Документація вдосконалення системи є важливою частиною. Аналізи продуктивності, звіти про тестування та журнали змін є частиною цього. Документація забезпечує прозорість процесу для всіх зацікавлених сторін і допомагає відстежувати прогрес у вдосконаленні. Крім того, він є основою для подальшого вдосконалення системи в майбутньому, яку в вигляді блок-схеми зображено на рисунку 3.7.

Відгуки користувачів є важливою частиною вдосконалення системи. Оскільки користувачі безпосередньо використовують систему у своїй роботі, вони є важливими учасниками процесу вдосконалення. Створення зручних каналів для зворотного зв'язку є життєво важливим, щоб користувачі могли легко повідомляти про свої відчуття, проблеми та пропозиції. Зворотний зв'язок допомагає зрозуміти, як користувачі сприймають систему, і визначає місця покращення. Під час процесу вдосконалення системи також важливо забезпечити постійне навчання та підтримку

користувачів. Надання технічної підтримки, надання ресурсів і постійне навчання є частиною цього. Навчання зменшує ймовірність помилок і проблем у роботі, а також допомагає користувачам зрозуміти нові функції та можливості системи. Для успішного впровадження та використання системи необхідна підтримка користувачів.

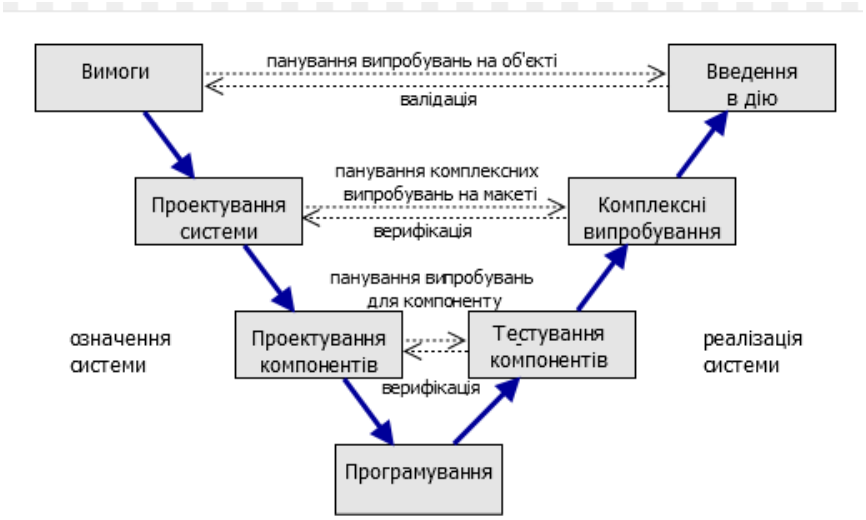


Рисунок 3.7 – Блок-схема для реалізації та тестування.

3.6 Підтримка та оновлення розробленого додатку з урахуванням змін у блокчейн-технологіях та вимог користувачів

Забезпечення того, що розроблений додаток буде ефективним і ефективним у довгостроковій перспективі, залежить від його підтримки та оновлення відповідно до змін у блокчейн-технологіях і вимог користувачів. Необхідно мати стратегію, яка дозволяє додатку залишатися актуальним і корисним, оскільки вимоги користувачів і блокчейн-технології змінюються швидко. Постійний моніторинг змін у блокчейн-технологіях є першим кроком у підтримці та оновленні додатку. Це включає спостереження за новинами, науковими дослідженнями, технічними оновленнями та іншими джерелами інформації, які містять інформацію про нові досягнення в цій галузі. Важливо бути в курсі останніх тенденцій, включаючи нові алгоритми консенсусу, удосконалення безпеки, зміни в протоколах та інші інновації. Постійний

моніторинг допомагає виявляти можливості для вдосконалення додатку та запобігати потенційним проблемам із застарілими технологіями. Аналітика потреб користувачів є другою важливою частиною. Користувачі є основними споживачами додатку, і вони мають різні потреби та очікування. Постійний збір даних від користувачів через різні канали, такі як інтерв'ю, опитування та відгуки на платформах, є важливим. Це допомагає користувачам зрозуміти найважливіші функції та можливості додатку, проблеми, з якими вони стикаються під час його використання, і які покращення вони хотіли б бачити у майбутньому. Аналіз вимог користувачів допомагає розробникам визначити найважливіші потреби та пріоритети під час планування оновлень. Розробка стратегії оновлень додатків повинна базуватися на змінах у блокчейн-технологіях і потребах користувачів. Впровадження нових функцій, виправлення помилок, оптимізація продуктивності та розширення існуючих можливостей повинні бути частиною стратегії. Важливо визначити пріоритети для оновлень за технічними та користувальними аспектами.

Одним із важливих етапів оновлення додатку є розробка нових функцій. Впровадження нових алгоритмів консенсусу, інтеграція з новими блокчейн-платформами, покращення безпеки тощо може бути частиною цього. Ретельне планування та тестування нових функцій має вирішальне значення для забезпечення їхньої надійності та відповідності вимогам користувачів. Розробка нових функцій повинна бути спрямована на підвищення цінності для користувачів і підтримку конкурентоспроможності додатку на ринку.

Не менш важливим є вдосконалення існуючих можливостей додатку. Це може включати заходи, спрямовані на покращення зручності та ефективності використання додатку, такі як оптимізація продуктивності, покращення інтерфейсу користувача та виправлення помилок, серед іншого. Регулярний аналіз продуктивності програми має вирішальне значення для виявлення місць для покращення. Додаток працює стабільно та безперебійно завдяки виправленню помилок і оптимізації продуктивності, що є важливим для задоволення потреб користувачів. Одним із найважливіших компонентів підтримки та оновлення додатків є безпека, особливо щодо блокчейн-технологій. Важливо регулярно проводити аудити безпеки, щоб

знайти потенційні проблеми та вирішити їх. Оновлення криптографічних алгоритмів, впровадження нових механізмів захисту даних, покращення автентифікації користувачів та інші дії можуть бути частиною цього. Забезпечення високого рівня безпеки підвищує довіру до додатку та захищає користувачів від потенційних атак і зловмисників. Процес оновлення програми залежить від його тестування. Ретельне тестування нових функцій і вдосконалень є життєво важливим для того, щоб переконатися, що вони працюють належним чином і не викликають нових проблем. Щоб максимізувати точність і ефективність, тестування повинно включати ручні та автоматизовані методи. Крім того, необхідно провести регресійне тестування, щоб переконатися, що нові зміни не впливають на існуючі функції програми. Після завершення тестування нових версій програмного забезпечення важливо гарантувати, що вони будуть впроваджені в продуктивне середовище. Це може включати оновлення програм на серверах, оновлення програм на мобільних телефонах через магазини програм та інші події. Щоб забезпечити безперебійну роботу програми та мінімізувати потенційні ризики, важливо ретельно планувати процес впровадження. Після впровадження програми необхідно перевіряти його роботу, щоб знайти потенційні проблеми. Підтримка користувачів є важливою частиною підтримки та оновлення додатків. Це включає надання користувачам корисних ресурсів, навчання та технічну підтримку, а також створення документації. Важливо створити доступні канали підтримки, такі як служба підтримки, онлайн-форуми та бази знань. Підтримка користувачів гарантує високу задоволеність користувачів і зменшує ймовірність проблем. Важливо враховувати не лише технічні аспекти, але й організаційні та управлінські аспекти підтримки та оновлення додатку. Це включає управління проектами, управління змінами та координацію роботи команди. Щоб гарантувати своєчасне та якісне виконання оновлення, необхідно ефективне управління процесом. Організаційні елементи також включають залучення користувачів до процесу вдосконалення додатку, інформування їх про нові функції та покращення. Аналіз ринку та конкурентів також є частиною підтримки та оновлення додатку. Важливо стежити за новими тенденціями та інноваціями в блокчейн-технологіях і вивчати дії конкурентів. Це сприяє виявленню нових можливостей для

покращення програми та підвищення її конкурентоспроможності. Аналіз ринку також включає вивчення нових технологій, які можна впровадити в додаток, щоб підвищити його функціональність і цінність для користувачів.

Забезпечення якості та ефективності додатку залежить від постійного вдосконалення процесів розробки та підтримки. Впровадження нових інструментів і методів розробки, підтримки та тестування додатків, оптимізація внутрішніх процесів, навчання команди та інші заходи є частиною цього процесу. Важливо створити культуру постійного вдосконалення, щоб підтримка та команда розробників завжди була орієнтована на підвищення якості та ефективності своєї роботи. Ще одним важливим елементом є використання сучасних інструментів і технологій для розробки та підтримки додатків. Використання систем управління версіями, систем автоматизованого тестування, інструментів для моніторингу та аналізу продуктивності, систем управління проектами та інших інструментів може бути частиною цього.

3.7 Висновок

Розробка, інтеграція, тестування, впровадження та підтримка мобільного додатку для криптовалютних операцій на базі Android включають ключові елементи, які складають результати реалізації системи на практиці.

Первочерговим завданням, яке забезпечує основу для всієї системи, є розробка мобільного додатку для операційної системи Android відповідно до визначених вимог.

Розробка включає створення інтерфейсу користувача, який є простим і простим у використанні, а також виконання основних функцій, таких як перегляд балансу, виконання транзакцій і управління портфоліо. Створення продуктивного та надійного додатку можливо за допомогою сучасних інструментів і фреймворків, таких як Android Studio та Kotlin. У сфері безпеки велика увага приділяється впровадженню шифрування даних і біометричної автентифікації.

Для того, щоб система могла працювати належним чином, вона повинна включати основні блокчейн-вузли та мережі криптовалют. Це стосується налаштування роботи з відомими блокчейн-платформами, такими як Ethereum, Bitcoin і Binance Smart Chain. Додатки можуть взаємодіяти з блокчейн-вузлами за допомогою відповідних API та SDK.

Це дозволяє їм перевіряти баланси, відправляти та отримувати транзакції та отримувати поточну інформацію про мережу. Інтеграція забезпечує надійний і ефективний зв'язок між програмами та блокчейн-мережами.

Першою частиною процесу пошуку та вирішення потенційних проблем до випуску продукту є тестування розробленого додатку для перевірки його працездатності та безпеки.

Це включає тестування продуктивності для забезпечення стабільної роботи під навантаженням, тестування безпеки для виявлення вразливостей і функціональне тестування для перевірки, що всі функції працюють належним чином. Використання реальних пристроїв і емуляторів гарантує, що додаток працюватиме правильно в різних умовах.

Здійснення пілотних проектів для оцінки функціонування системи в реальному житті та збору відгуків користувачів дозволяє перевірити додаток на практиці. Початкові проекти дають корисну інформацію про те, як система працює з користувачами та реальними даними, і допомагають виявити проблеми або недоліки, які не були помічені під час тестування. Відгуки користувачів допомагають розробникам визначити, які частини програми потребують вдосконалення.

Вдосконалення системи на основі результатів тестування та пілотних проектів є важливим етапом вдосконалення продукту. Аналіз результатів тестування та відгуків користувачів дозволяє визначити проблеми та внести відповідні корективи.

Це може включати оптимізацію продуктивності, виправлення вразливостей безпеки, покращення інтерфейсу користувача та додавання нових функцій, які підвищують цінність продукту для користувача. При оптимізації продуктивності алгоритму хешування можуть бути використані різні методи, такі як вдосконалення алгоритмів хешування для зменшення обчислювальної складності, використання

оптимізованих структур даних для збереження хеш-таблиць або вдосконалення методів обробки даних для швидкого виявлення колізій та ефективного вирішення конфліктів.

4 ДОСЛІДЖЕННЯ ТА ІННОВАЦІЇ У БЛОКЧЕЙН-БАЗОВАНИХ СИСТЕМАХ

4.1 Сучасні тенденції у блокчейн-технології

Сьогоднішні тенденції в галузі блокчейн-технологій показують, що нові протоколи та рішення створюються та впроваджуються для покращення масштабування, безпеки та інтероперабельності. Платформи, такі як Solana, Polkadot і Cardano, привернули увагу завдяки своїм інноваціям і здатності вирішувати існуючі проблеми в блокчейн-екосистемах.

Polkadot — це блокчейн-платформа, мета якої полягає в тому, щоб створити багатоланцюгову екосистему, в якій різні блокчейни можуть взаємодіяти один з одним і обмінюватися даними без втрати безпеки. Здатність підтримувати «парачейни», спеціалізовані блокчейни, які можуть працювати паралельно та бути пов’язані через основний ланцюг Polkadot, є основною інновацією Polkadot. Це дозволяє досягти високої масштабованості та ефективності, одночасно зберігаючи децентралізацію та безпеку, а також у даної платформи є і свій блокчейн-додаток зображено на рисунку 4.1.

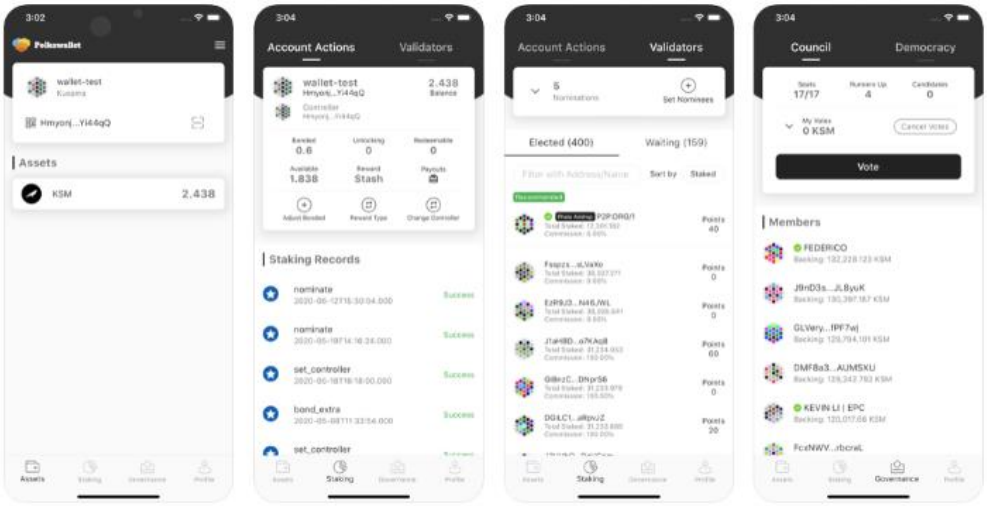


Рисунок 4.1 – Інтерфейс додатку PolkaWallet.

Cardano є ще однією платформою блокчейну, яка прагне створити більш безпечне та масштабоване середовище для розробки децентралізованих програм.

Cardano використовує механізм консенсусу, який називається Ouroboros, який є варіантом Proof of Stake (PoS). Цей механізм дозволяє досягти високого рівня безпеки та енергоефективності, одночасно мінімізуючи негативний вплив блокчейн-технології на навколишнє середовище, зображено на рисунку 4.2.

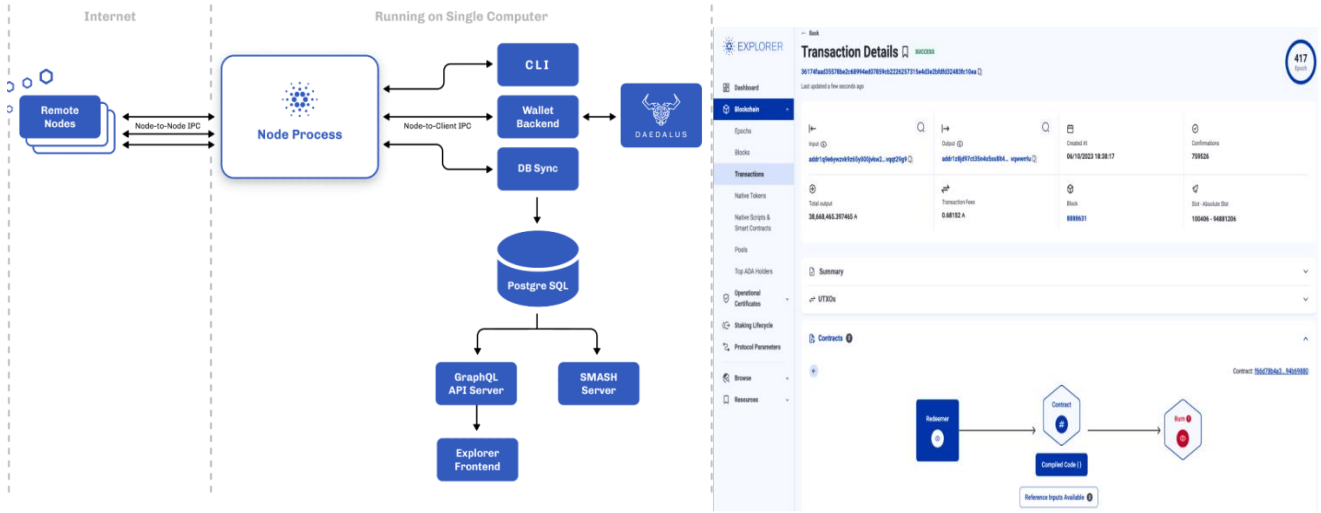


Рисунок 4.2 – Архітектуру Cardano, а також і інтерфес транзакції [49]

Solana відома низькими комісіями та високою швидкістю транзакцій. У результаті використання нового механізму консенсусу під назвою Proof of History (PoH) ця платформа може значно підвищити продуктивність. Solana має здатність обробляти тисячі транзакцій в секунду, що робить її привабливою для децентралізованих фінансів (DeFi) та інших додатків, які потребують високої пропускної здатності.

Децентралізовані фінанси (DeFi) є однією з найбільш динамічних і швидко розвиваються сфер в екосистемі блокчейну. Користувачі можуть здійснювати фінансові операції без посередників, таких як банки чи фінансові установи, за допомогою DeFi-додатків. У числі цих програм є програми, які використовують смарт-контракти для кредитування, позичання, обміну активами та управління активами. Децентралізація фінансів дозволяє людям у всьому світі отримати доступ до фінансових послуг, що створює нові можливості для фінансової інклюзивності.

Використання цифрових активів змінюється завдяки розвитку незаміних токенів (NFT). Витвори мистецтва, музика, відео або навіть віртуальні землі можуть

бути створені за допомогою NFT, що дозволяє створювати унікальні цифрові об’єкти. Художники, музиканти та інші творці отримують нові можливості завдяки цій технології, яка дозволяє їм без посередників взаємодіяти з аудиторією та монетизувати свою творчість, зображено на рисунку 4.3.

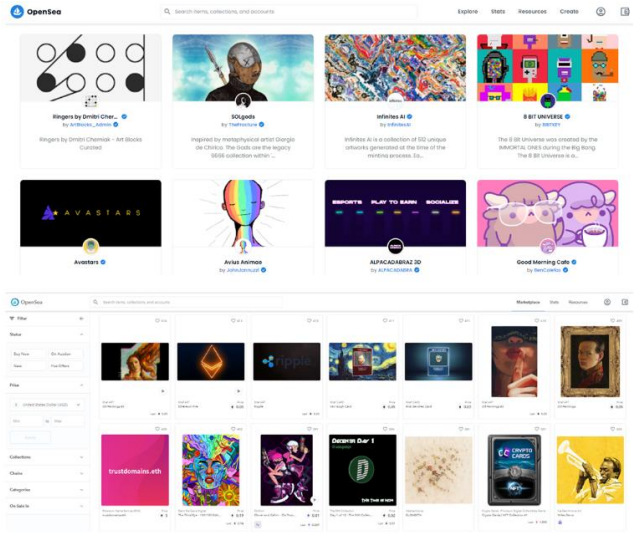


Рисунок 4.3 – Головний інтерфей OpeanSea, де можна або придбати, або продати NFT картинку

Розвиток технологій також включає оновлення існуючих блокчейн-систем. Цей процес можна побачити на Ethereum 2.0. Це велике оновлення мережі Ethereum включає перехід від Proof of Work (PoW) до Proof of Stake (PoS), що значно знижує споживання енергії мережі та підвищує масштабованість. Ethereum 2.0 також вводить механізм шардингу, який розділяє мережу на менші частини, відомі як шашди. Це дозволяє обробляти більше транзакцій одночасно.

Ці зміни та тенденції свідчать про постійний розвиток і еволюцію блокчейн-технологій, які стають більш зрілими та готовими до широкого впровадження в багатьох галузях. Однак OpeanSea, це є платформа з великою кількістю NFT зображенн, а також вона дає можливість на цьому заробити.

4.2 Дослідження ефективності блокчейн системи

Дослідження ефективності блокчейн-систем зосереджується на безпеці, енергоспоживанні та ефективності. Ці дослідження допомагають виявити майбутні вдосконалення та оптимізувати роботу блокчейн-платформ, щоб їх можна було використовувати для більшого кількості людей.

Однією з основних тем досліджень є ефективність блокчейн-систем. Багато додатків, особливо фінансових і децентралізованих, потребують високої швидкості та пропускної здатності транзакцій. Через обмежену кількість транзакцій, які можуть оброблятися в одиницю часу, традиційні блокчейн-системи, такі як Bitcoin та Ethereum, мають проблеми з масштабованістю. Щоб вирішити ці проблеми, нові протоколи, такі як шардинг Ethereum та Lightning Network для Bitcoin, дозволяють підвищити продуктивність і забезпечити більш високу пропускну здатність, зображено на рисунку 4.4.

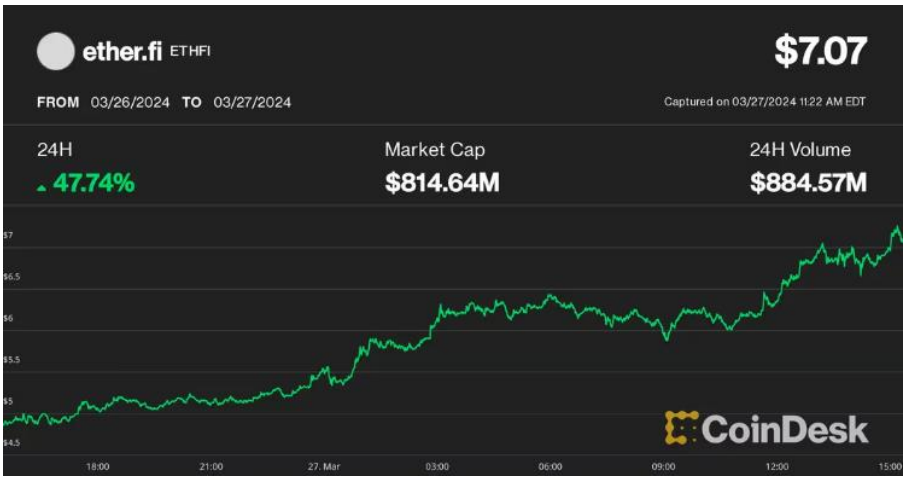


Рисунок 4.4 – Графік росту Etherium

Ефективність блокчейн-систем також залежить від споживання енергії. У мережах, таких як Bitcoin, використовується механізм консенсусу Proof of Work (PoW), який споживає багато енергії, що викликає занепокоєння щодо екологічної безпеки. Наукова діяльність у цій сфері зосереджена на розробці альтернативних методів консенсусу, таких як підтвердження частки (PoS) та його варіації. Ці методи

зберігають децентралізацію та безпеку мережі, одночасно значно знижують споживання енергії.

Безпека блокчейн-систем є критично важливою для функціонування та довіри користувачів. Аналіз вразливостей у криптографії, механізмах консенсусу та смарт-контрактах є частиною досліджень безпеки. Безпека смарт-контрактів особливо важлива, оскільки помилки в коді можуть призвести до великих втрат грошей. Таким чином, розробники знаходять і вирішують потенційні проблеми за допомогою процедур формальної верифікації та аудиту коду. нові методи, такі як використання квантової криптографії, досліджуються для забезпечення стійкості блокчейн-систем до майбутніх загроз.

За допомогою порівняння блокчейн-технологій з традиційними системами можна визначити їхні переваги та недоліки. Хоча блокчейн забезпечує високу безпеку та децентралізацію, він може споживати більше енергії, ніж централізовані системи. Аналіз цих елементів допомагає визначити, коли використання блокчейну є найбільш ефективним і вигідним.

Оцінка вартості впровадження блокчейн-технологій включає оцінку економічної доцільності та повернення інвестицій (ROI). Хоча впровадження блокчейн-систем може вимагати значних початкових витрат на розробку, інтеграцію та підтримку, воно також може принести значні переваги, такі як зниження витрат на операції, підвищення безпеки та прозорості процесів. Що стосується прийняття рішень щодо впровадження блокчейн-технологій, оцінка ROI допомагає організаціям.

4.3 Використання штучного інтелекту та машинного навчання

Інтеграція штучного інтелекту (AI) та машинного навчання (ML) у блокчейн-системи відкриває нові можливості для покращення їх функціональності, безпеки та користувацького досвіду. Ці технології дозволяють автоматизувати процеси, аналізувати великі обсяги даних і надавати рішення, які підходять конкретним потребам кожного клієнта.

Аналіз транзакцій та штучний інтелект Використання штучного інтелекту для аналізу транзакцій блокчейну допомагає виявити аномалії та підозрілі активності. Машинне навчання може використовувати історичні дані для пошуку патернів, які вказують на потенційні шахрайства чи злочинні дії. Це дозволяє створювати ефективні системи виявлення та моніторингу, які можуть зменшити ризик фінансових втрат і швидко реагувати на загрози. передбачення ринкових тенденцій. Аналіз ринкових даних і прогнозування цін криптовалют також можуть бути виконані за допомогою штучного інтелекту. Щоб передбачити майбутні зміни ринку, моделі машинного навчання можуть використовувати історичні дані, тренди в соціальних медіа, обсяг торгівлі та інші економічні показники. Це допомагає інвесторам і трейдерам приймати розумні рішення.

Автоматизація повсякденних операцій AI може автоматизувати багато рутинних завдань, таких як обробка транзакцій, управління користувацькими обліковими записами та дотримання правил. Це можна зробити за допомогою впровадження AI у блокчейн-системи. Це підвищує продуктивність системи та знижує витрати на її обслуговування.

Покращена безпека. Аналізуючи поведінку користувачів у режимі реального часу та знаходячи підозрілу активність, штучний інтелект може значно покращити безпеку блокчейн-систем. Можна використовувати машинне навчання для виявлення аномалій за допомогою приватних ключів, доступу до облікових записів та проведення транзакцій, що допомагає запобігти зламу облікових записів та крадіжці криптовалют.

Персоналізація досвіду користувача На основі аналізу поведінки користувачів штучний інтелект може створювати більш персоналізований досвід користувача. Рекомендації щодо інвестицій, оптимізація налаштувань безпеки, персоналізовані повідомлення та інші функції можуть підвищити задоволення користувачів від взаємодії з блокчейн-системами.

4.4 Потенціал технології Інтернет речей (IoT) у блокчейн-системах

Нові можливості для створення більш безпечних, ефективних і прозорих систем з’явилися завдяки інтеграції технологій Інтернету речей (IoT) та блокчейну. Поєднання цих двох технологій дає нові можливості для автоматизації та децентралізації процесів, а також вирішує багато проблем, пов’язаних із безпекою даних, управлінням і моніторингом пристроїв.

Інтернету речей із блокчейном. Інтернет речей складається з мережі взаємопов’язаних пристроїв, які використовують Інтернет для збору та обміну даними. Блокчейн дозволяє створити децентралізовану платформу для зберігання та управління даними, що гарантує їхню безпеку, прозорість і цілісність. Смарт-контракти дозволяють автоматизувати взаємодію між пристроями, що зменшує потребу в посередниках і збільшує продуктивність процесів, зображено на рисунку 4.5.

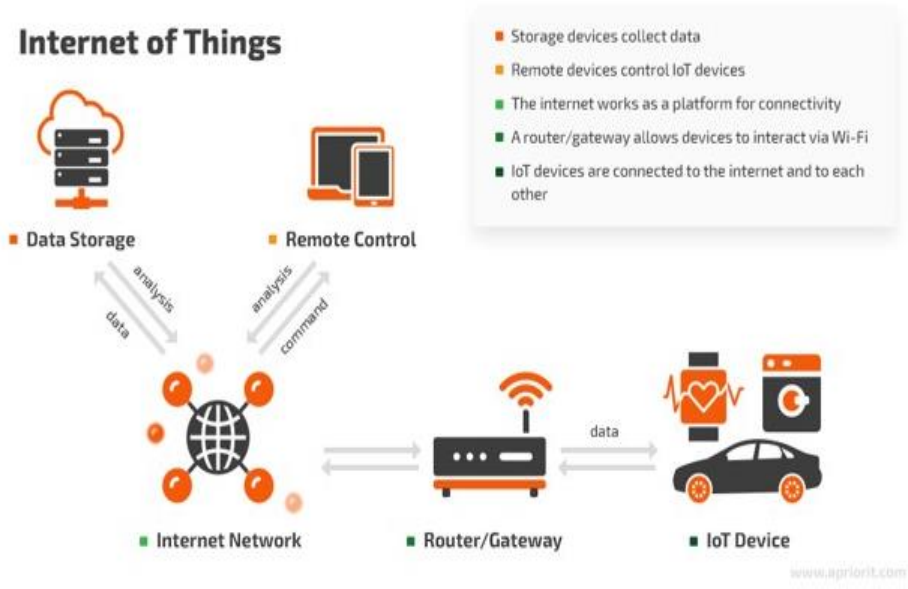


Рисунок 4.5 – Зображено суть інтернет речей, та різні інтелектуальні пристрої

Інтелектуальне управління логістикою використовує блокчейн для забезпечення автентичності товарів і відстеження їх переміщення. Наприклад, розумні контейнери можуть автоматично повідомляти про своє розташування, температуру та стан до блокчейну, що дозволяє всім учасникам ланцюга поставок отримати актуальну та перевірену інформацію.

Перешкоди та проблеми з інтеграцією Інтеграція IoT і блокчейн дозволяє створювати нові бізнес-моделі, знижувати витрати на управління та обслуговування та підвищувати безпеку даних. Але обмежена пропускна здатність блокчейн-мереж, висока вартість транзакцій і складність масштабування - це деякі з проблем, з якими вона також стикається. Розробка нових протоколів і оптимізація, які можуть забезпечити ефективну та вигідну інтеграцію, є необхідною для вирішення цих проблем.

Безпека пристроїв Інтернету речей за допомогою блокчейну. Безпека даних і захист пристроїв від кібератак є однією з головних проблем у сфері Інтернету речей. Блокчейн може захистити дані, записуючи кожну транзакцію у постійний реєстр. Це робить практично неможливим підробку даних або несанкціонований доступ до пристроїв. Це збільшує загальний рівень захисту IoT-систем і знижує ймовірність кібератак.

У майбутньому блокчейн і Інтернет речей У майбутньому очікується, що поєднання Інтернету речей і блокчейн стане ще тіснішим, щоб дати нові можливості різним сферам, таким як медицина, сільське господарство, розумні міста та промисловість. Наприклад, блокчейн може бути використаний у медицині для зберігання та управління даними про стан здоров’я пацієнтів, гарантуючи, що ці дані залишаються конфіденційними та доступними лише авторизованим особам. Блокчейн і IoT можуть допомогти в сільському господарстві відстежувати, де виробляється продукти харчування, і контролювати умови зберігання.

4.5 Перспективи розвитку блокчейн-технологій

Перспективи розвитку блокчейн-технологій надзвичайно різноманітні та широкі. Багато галузей вже були змінені цією технологією, але здається, що вона ще може зрости.

Фінанси, медицина, логістика та багато інших галузей вже відчувають наслідки блокчейну. У сфері фінансів блокчейн дозволяє створювати децентралізовані платформи для кредитування, торгівлі та управління активами. Це підвищує

прозорість, знижує витрати та надає широкому колу користувачів доступ до фінансових послуг. Блокчейн використовується в медицині для зберігання медичних записів, що робить їх безпечними та доступними лише для призначених осіб. Блокчейн підвищує продуктивність ланцюга постачання та знижує ризики шахрайства, оскільки логістичні компанії використовують його для забезпечення автентичності товарів і відстеження їхнього переміщення.

Потенціал для розробки інноваційних бізнес-моделей. Нові бізнес-моделі, такі як децентралізовані автономні організації (DAO), можна створити за допомогою блокчейну. Ці моделі працюють без центрального керівництва та приймають рішення за допомогою голосування учасників. Це дозволяє створювати більш гнучкі та відкриті системи управління, які можуть швидко змінюватися відповідно до потреб ринку.

Коли справа доходить до подальшого розвитку технології, проблеми та виклики, пов’язані з масштабуванням блокчейн, залишаються важливими питаннями. Поточні блокчейн-системи стикаються з проблемами, які можуть обмежити їхню здатність обслуговувати великі кількості даних і користувачів. Ці проблеми включають обмеження швидкості транзакцій і пропускної здатності. Розробка нових протоколів, таких як шардинг і міжланцюгова взаємодія, може допомогти подолати ці проблеми та гарантувати масштабованість блокчейн-мереж.

Уряди та регулятори також відіграють важливу роль у розвитку блокчейну. Розвиток інновацій і залучення інвестицій у блокчейн-проекти можна стимулювати за допомогою сприятливих регуляторних умов. Водночас регулятори повинні забезпечити захист прав споживачів і перешкоджати незаконному використанню блокчейн. Справедливе регулювання може забезпечити стійкий розвиток технологій і її інтеграцію в різні сфери економіки.

Виглядає, що майбутнє блокчейн-технологій є яскравим і перспективним. Відповідно до зростання популярності децентралізованих фінансів (DeFi), криптовалют і інших блокчейн-додатків, все більше підприємств і організацій починають звертати увагу на цю технологію. Розширення впровадження блокчейн у різних сферах буде сприяти створенню нових протоколів, збільшенню

продуктивності та зниження вартості транзакцій. Крім того, інтеграція з сучасними технологіями, такими як штучний інтелект і Інтернет речей, відкриє нові можливості для інновацій і покращення поточних процесів.

4.6 Визначення стратегії підтримки та популяризації розробленого додатку на ринку криптовалют та мобільних додатків.

Стратегія підтримки та популяризації розробленого додатку на ринку криптовалют і мобільних додатків є складним і багатогранним завданням, яке вимагає ретельного аналізу ринкових умов, вивчення потреб цільової аудиторії та розробки ефективних стратегій комунікації та маркетингу.

У цьому розділі ми розглянемо основні елементи стратегії, такі як брендування та позиціонування, створення контенту та маркетингових кампаній, взаємодія зі спільнотою та партнерами, підтримка та оптимізація користувацького досвіду, а також спостереження та аналіз результатів.

Брендування та позиціонування: створення сильного бренду та чітке визначення позиціонування на ринку є першим кроком у стратегії підтримки та популяризації додатку. Створення унікальної назви, логотипу, дизайну та візуальної ідентичності, яка відображає цінності та характеристики додатку, є частиною цього процесу. Впізнаваність, диференціація та зв’язок з цільовою аудиторією є основними компонентами брендування.

Розробка контенту та маркетингові кампанії: для успішної популяризації додатку важливо створити цільовані маркетингові кампанії та контент, які спрямовані на різні демографічні групи.

Це може включати створення захоплюючого та корисного контенту для різних каналів комунікації, включаючи інфографіку, соціальні медіа, блоги та відеоролики. Персоналізація, співпраця з впливовими людьми та створення унікальних історій успіху користувачів є важливими компонентами ефективної маркетингової стратегії.

Взаємодія зі спільнотою та партнерами: створення сприятливого середовища для обміну досвідом, ідеями та думками є важливим компонентом стратегії. Це може

включати проведення вебінарів, форумів, івентів та інших заходів для підвищення спільної участі. Крім того, встановлення партнерських відносин з іншими компаніями та сервісами у сфері криптовалют і мобільних додатків є важливим, щоб працювати разом над просуванням продукту та розширенням його функцій.

Оптимізація користувацького досвіду та підтримки: надання чудового користувацького досвіду та підтримки є важливими компонентами ефективної стратегії. Це означає не тільки додавання нових функцій та покращення інтерфейсу, але й організацію навчальних матеріалів, активну відповідь на проблеми користувачів і постійне вдосконалення процесу обслуговування клієнтів.

Моніторинг та аналіз результатів: постійна оцінка ефективності дій і аналіз того, як вони вплинули на показники успішності додатку, є не менш важливими. Це може включати метрики успіху, такі як збільшення активності користувачів, популярність у соціальних мережах і кількість конверсії.

На основі даних можна змінити план і вдосконалити його, щоб максимізувати ефективність. Активна участь у програмах стимулювання користувачів може бути ще одним компонентом плану підтримки та популяризації додатку.

Це може включати бонуси, знижки, промокоди або програми лояльності, щоб мотивувати користувачів продовжувати використовувати додаток. Такі програми можуть залучити нових користувачів і утримувати поточну аудиторію. Наприклад, участь у розіграшах призів, отримання кешбеку за використання додатку або надання спеціальних привілеїв активним користувачам можуть підвищити зацікавленість користувачів і активність у продукті.

Такий підхід дозволяє залучити увагу користувачів і забезпечити їхню лояльність до програми. Це сприяє підвищенню популярності та успішного впровадження програми на ринку мобільних додатків і криптовалют, а також додаткові аспекти якими є:

Локалізація: Локалізація додатку має бути розглянута відповідно до цільової аудиторії та ринку. Це включає переклад контенту та інтерфейсу на мову, яку використовують користувачі, а також адаптацію функцій до законодавства та потреб регіону.

Участь у спеціалізованих заходах та конференціях: Активна участь у спеціалізованих заходах та конференціях, які стосуються криптовалюти та мобільних додатків, може допомогти популяризувати додаток і створити важливі контакти в галузі.

Підтримка інновацій і новаторських рішень: така стратегія може включати постійне вдосконалення додатку за допомогою впровадження нових функцій і технологій, щоб задовольнити потреби користувачів, а також забезпечити конкурентоспроможність продукту на ринку.

4.7 Висновок

Важливо відзначити, що блокчейн-технології стрімко розвиваються, щоб адаптуватися до нових проблем і вимог. Платформи, такі як Solana, Polkadot і Cardano, продемонстрували свою готовність до впровадження нових підходів у вирішенні проблем масштабованості та інтероперабельності, а також їхню інноваційність. Ці платформи не тільки збільшують продуктивність блокчейн-мереж, але й створюють нові можливості для створення децентралізованих додатків і послуг, які можуть суттєво змінити існуючі бізнес-моделі та галузі.

Незамінні токени (NFT) і децентралізовані фінанси (DeFi) демонструють потенціал для кардинальних змін у фінансових системах і ринках цифрових активів, тому вони продовжують набирати популярність. Додатки децентралізованої фінансової системи дозволяють користувачам отримати доступ до фінансових послуг без посередників, що зменшує витрати та підвищує прозорість операцій. За допомогою NFT митці, музиканти та інші творці отримують нові можливості монетизувати свою творчість і взаємодіяти з аудиторією у новому способі

Удосконалення існуючих блокчейн-систем, особливо Ethereum 2.0, демонструють бажання підвищити продуктивність і енергоефективність. Перехід від Proof of Work (PoW) до Proof of Stake (PoS), який зменшує енергоспоживання та підвищує масштабованість мережі, є важливим кроком у цьому напрямку. Ці зміни роблять блокчейн-системи більш ефективними та більш екологічними.

Для подальшого розвитку та впровадження блокчейн-систем важливо проводити дослідження їх ефективності. На ефективність блокчейн-мереж впливають такі фактори, як продуктивність, енергоспоживання та безпека. Підвищення пропускної здатності та зниження витрат на транзакції є результатом пошуку нових способів консенсусу та оптимізації існуючих рішень, що робить блокчейн більш привабливим для широкого використання.

Штучний інтелект (AI) і машинне навчання (ML) стали частиною блокчейн-систем, що відкриває нові можливості для покращення їх безпеки та функціональності. Як наслідок, AI значно покращує загальну ефективність блокчейн-систем, а також допомагає прогнозувати ринкові тенденції та виявляти шахрайські дії. Досвід, більш індивідуалізований за допомогою штучного інтелекту, підвищує задоволеність користувачів і сприяє більшому впровадженню блокчейн-технологій.

Удосконалення автоматизації та оптимізації процесів є основним напрямком використання AI та ML у блокчейні. Системи з розумними контрактами, побудовані на блокчейні, можуть використовувати штучний інтелект для моніторингу ринку, прийняття рішень на основі складних алгоритмів і автоматичного виконання умов контракту. Наприклад, це може включати оптимізацію торгівельних стратегій на фондовому ринку або автоматичне виконання угод у умовах великого обсягу транзакцій.

Крім того, машинне навчання може бути використане для аналізу великих кількостей даних, що зберігаються в блокчейні, щоб знайти закономірності, спрогнозувати тенденції та використовувати ці дані для прийняття рішень. Наприклад, алгоритми машинного навчання можуть використовуватися для прогнозування цін на криптовалюту, пошуку шахраїв або попередження про потенційні атаки на мережу.

Також можна використовувати штучний інтелект і машинне навчання, щоб покращити виявлення та запобігання кібератак, а також покращити механізми ідентифікації та автентифікації користувачів.

ВИСНОВКИ

У магістерській роботі за результатами виконаних теоретичних та практичних досліджень розроблено блокчейн-базовану систему на підтримці операційної системи Android.

У першому розділі описано блокчейн-технології, які забезпечують безпеку, прозорість і децентралізацію криптовалютних операцій. Інтеграція криптовалют на мобільних пристроях стикається з кількома проблемами, включаючи обмежені ресурси та високий рівень безпеки. Тим не менш, використання блокчейну на платформі Android має численні переваги, включаючи високу безпеку транзакцій і простоту використання. Як показав аналіз існуючих рішень, існує широкий спектр систем, доступних на ринку, але багато з них мають свої обмеження та проблеми. При розробці системи безпека та конфіденційність є важливими аспектами. Забезпечення функціональності, ефективності та безпеки системи є основними вимогами.

У другому розділі вибрано блокчейн-платформу для впровадження в операційну систему Android, що є важливим кроком, який закладає основу для подальшої розробки. Створення гаманця криптовалют для виконання основних завдань, таких як зберігання, відправка та отримання криптовалют, є основною частиною системи. Упровадження зручного інтерфейсу користувача робить управління криптовалютою більш простим. Комунікаційний протокол дозволяє мобільному додатку взаємодіяти з блокчейн-вузлами, що гарантує надійність і швидкість обробки транзакцій. Функції Android, такі як NFC та біометрична автентифікація, покращують досвід користування. Для обробки великої кількості транзакцій важливо забезпечити масштабованість і відмовостійкість.

У третьому розділі розроблено мобільний додаток для операційної системи Android включає розгляд стандартних вимог, інтеграцію з основними блокчейн-вузлами та мережами криптовалют, а також тестування безпеки та працездатності. Пілотні проекти дозволяють оцінити функціонування системи в реальному світі та отримати відгуки користувачів. Система адаптується до потреб користувачів завдяки результатам тестування та пілотних проектів. Необхідно підтримувати та оновити

додаток, щоб він міг адаптуватися до змін у блокчейн-технологіях і потреб користувачів.

У четвертому розділі досліджено результати ефективності впровадження системи, що є важливим етапом для оцінки її успішності Щоб розширити функціональні можливості програми, його можна інтегрувати з іншими платформами та сервісами. Аналіз тенденцій на ринку та конкурентного середовища допомагає змінити стратегію розвитку. Дослідження, спрямовані на покращення безпеки, швидкості та масштабованості системи, сприяють її розвитку. Визначення стратегії підтримки та популяризації програми на ринку криптовалют і мобільних додатків є важливим для його успішного впровадження та прийняття користувачами.

Інформаційна технологія набула подальшого розвитку, забезпечуючи нові можливості та вдосконалення для підтримки криптовалютних операцій на мобільних пристроях.

Впровадження результатів роботи дозволили підвищити безпеку та зручність криптовалютних операцій на мобільних пристроях, забезпечити надійну взаємодію з блокчейн-вузлами та створити основу для подальшого розвитку та вдосконалення системи. Інформаційна технологія набула подальшого розвитку, забезпечуючи нові можливості та вдосконалення для підтримки криптовалютних операцій на мобільних пристроях.

За темою кваліфікаційної роботи магістра опубліковані тези на науковій конференції, що підкреслює важливість та актуальність досліджень у цій галузі.

1. Тимчук П.В., Грига В.М. Блокчейн-базована система підтримки криптовалютних операцій для ОС Android // Матеріали XXIV Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів «СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ», 18 – 19 квітня 2024 року, м. Одеса, Україна, С. 279-281.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Zimmerman P. Blockchain structure and cryptocurrency prices Staff working Paper Bank of England. URL: https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2020/blockchain structure-and-cryptocurrency-prices.pdf (дата звернення: 21.04.2024)

2. Biktimirov M. R. et al. Blockchain technology: Universal structure and requirements // Automatic Documentation and Mathematical Linguistics. URL: https://link.springer.com/article/10.3103/S0005105517060036 (дата звернення: 21.04.2024)

3. Zheng Z. et al. Blockchain challenges and opportunities: A survey International journal of web and grid services. URL: https://allquantor.at/blockchainbib/pdf/zheng2018blockchain.pdf (дата звернення: 21.04.2024)

4. Belotti M. et al. A vademecum on blockchain technologies: When, which, and how IEEE Communications Surveys Tutorials. URL: https://ieeexplore.ieee.org/document/8760539 (дата звернення: 21.04.2024)

5. Nofer M. et al. Blockchain Business & Information Systems Engineering. URL: https://link.springer.com/article/10.1007/s12599-017-0467-3 (дата звернення: 21.04.2024)

6. Elrom E. Blockchain Nodes The Blockchain Developer: Practical Guide for Designing, Implementing, Publishing, Testing, and Securing Distributed Blockchain-based Projects Elad Elrom. Apress Berkeley CA. URL: https://link.springer.com/article/10.1007/s12599-017-0467-3 (дата звернення: 21.04.2024)

7. Kushch S., Prieto-Castrillo F. Blockchain for dynamic nodes in a smart city IEEE 5th World Forum on Internet of Things (WF IoT). URL: https://wfiot.jkjmanagement.com/papers/1570523247.pdf123 (дата звернення: 21.04.2024)

8. Florian M. et al. Erasing data from blockchain nodes IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). URL: https://ieeexplore.ieee.org/document/8802472 (дата звернення: 21.04.2024)

9. Zhang R., Xue R., Liu L. Security and privacy on blockchain ACM Computing Surveys (CSUR). 30. URL: https://dl.acm.org/doi/pdf/10.1145/3316481 (дата звернення: 21.04.2024)

10. Li X. et al. A survey on the security of blockchain systems Future Generation Compute Systems. URL: https://www.sciencedirect.com/science/article/abs/pii/S0167739X17318332 (дата звернення: 21.04.2024)

11. Stephen R., Alex A. A review on blockchain security International Conference on Recent Advancements and Effectual Researches in Engineering Science and Technology (RAEREST) : Materials Science and Engineering. URL: https://iopscience.iop.org/article/10.1088/1757-899X/396/1/012030/pdf (дата звернення: 21.04.2024)

12. Karame G., Capkun S. Blockchain security and privacy // IEEE Security & Privacy. URL: https://www.computer.org/csdl/magazine/sp/2018/04/msp2018040011/13rRUxBJhE9 (дата звернення: 21.04.2024)

13. Moubarak J., Filiol E., Chamoun M. On blockchain security and relevant attacks IEEE Middle East and North Africa Communications Conference (MENACOMM) URL: https://ieeexplore.ieee.org/document/8371010 (дата звернення: 21.04.2024)

14. Park J. H., Park J. H. Blockchain security in cloud computing: Use cases, challenges, and solutions Symmetry. URL: https://www.mdpi.com/2073-8994/9/8/164 (дата звернення: 21.04.2024)

15 Bach L. M., Mihaljevic B., Zagar M. Comparative analysis of blockchain consensus algorithms 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). URP: https://ieeexplore.ieee.org/abstract/document/8400278124 (дата звернення: 21.04.2024)

16. Lashkari B., Musilek P. A comprehensive review of blockchain consensus mechanisms. URL: https://ieeexplore.ieee.org/abstract/document/9376868 (дата звернення: 21.04.2024)

17. Mingxiao D. et al. A review on consensus algorithm of blockchain international conference on systems, man, and cybernetics (SMC). URL: https://ieeexplore.ieee.org/abstract/document/8123011(дата звернення: 21.04.2024)

18. Klinkmüller C. et al. Mining blockchain processes: extracting process mining data from blockchain applications Management Business Process Management: Blockchain and Central and Eastern Europe. URL: https://link.springer.com/chapter/10.1007/978-3-030-30429-4_6L (дата звернення: 21.04.2024)

19. Islam N. et al. Is blockchain mining profitable in the long run? IEEE Transactions on Engineering Management. URL: https://ieeexplore.ieee.org/abstract/document/9325951 (дата звернення: 21.04.2024)

20. Yalcin H., Daim T. Mining research and invention activity for innovation trends: case of blockchain technology Scientometrics. URL: https://link.springer.com/article/10.1007/s11192-021-03876-4 (дата звернення: 21.04.2024)

21. Dorfleitner G., Muck F., Scheckenbach I. Blockchain applications for climate protection: A global empirical investigation Renewable and Sustainable Energy Reviews. URL: https://www.sciencedirect.com/science/article/abs/pii/S1364032121006638 (дата звернення: 21.04.2024)

22. Qureshi A., Megías Jiménez D. Blockchain-based multimedia content protection: Review and open challenges Applied Sciences. URL: https://www.mdpi.com/2076-3417/11/1/1 (дата звернення: 21.04.2024)

23. Wei P. C. et al. Blockchain data-based cloud data integrity protection mechanism Future Generation Computer Systems. URL: https://www.sciencedirect.com/science/article/abs/pii/S0167739X19313494125 (дата звернення: 21.04.2024)

24. Boireau O. Securing the blockchain against hackers Network Security URL: https://www.magonlinelibrary.com/toc/nese/2018/1 (дата звернення: 21.04.2024)

25. B. Rawat D., Chaudhary V., Doku R. Blockchain technology: Emerging applications and use cases for secure and trustworthy smart systems Journal of Cybersecurity and Privacy. URL: https://www.mdpi.com/2624800X/1/1/2 (дата звернення: 21.04.2024)

26. Li H. et al. A blockchain-based public auditing protocol with self-certified public keys for cloud data Security and Communication Networks. URL: https://downloads.hindawi.com/journals/scn/2021/3091104.pdf (дата звернення: 21.04.2024)

27. Sagiroglu S., Sinanc D. Big data: A review 2013 international conference on collaboration technologies and systems (CTS). URL: https://ieeexplore.ieee.org/abstract/document/6567202 (дата звернення: 21.04.2024)

28. Shakhovska N. et al. Big Data analysis in development of personalized medical system Procedia Computer Science. URL: https://www.sciencedirect.com/science/article/pii/S187705091931676X (дата звернення: 21.04.2024)

29. Yaqoob I. et al. Big data: From beginning to future International Journal of Information Management. URL: https://www.sciencedirect.com/science/article/abs/pii/S0268401216304753 (дата звернення: 21.04.2024)

30. Fan J., Han F., Liu H. Challenges of big data analysis National science review. URL: https://academic.oup.com/nsr/article/1/2/293/1397586 (дата звернення: 21.04.2024)

31. Vijayarani S., Sharmila S. Research in big data: an overview Informatics Engineering, an International Journal (IEIJ). URL: https://www.researchgate.net/publication/339551786_RESEARCH_IN_BIG_DATA_AN_OVERVIEW (дата звернення: 21.04.2024)

32.What is Consensus Algorithm In Blockchain & Different Types Of Consensus Models BangBit Technologies. URL: https://medium.com/@BangBitTech/what-isconsensusalgorithm-in-blockchain-different-types-of-consensus-models-12cce443fc77 (дата звернення: 21.04.2024)

33. Григорчук К. Обзор 9 алгоритмов блокчейн консенсуса Кирилл Григорчук DigitalForest. URL: https://digiforest.io/blog/blockchain-consensus-algorithms. (дата звернення: 21.04.2024)

34. What Are Public Keys and Private Keys? Ledger Academy. URL: https://www.ledger.com/academy/blockchain/what-are-public-keys-and-privatekeys. (дата звернення: 21.04.2024)

35. Haber S. How to Time-Stamp a Digital Document S. Haber, W. Scott Stornetta. Morristown, 1991. 19 с. (Bellcore).

36. Williams S. 20 Real-World Uses for Blockchain Technology Sean Williams The Motley Fool. URL: https://www.fool.com/investing/2018/04/11/20-real-world-uses-forblockchain-technology.aspx. (дата звернення: 21.04.2024)

37. Conway L. Blockchain Explained Luke Conway Investopedia. URL: https://www.investopedia.com/terms/b/blockchain.asp#:~:text=By%20spreading%20its%20operations%20across,the%20processing%20and%20transaction%20fees (дата звернення: 21.04.2024)

38. Clavin J. Blockchains for Government: Use Cases and Challenges J. Clavin, S. Duan, H. Zhang DGOV. URL: https://dl.acm.org/doi/fullHtml/10.1145/3427097. (дата звернення: 21.04.2024)

39. Solidity Documentation URL: https://docs.soliditylang.org/en/v0.5.3/index.html. (дата звернення: 21.04.2024)

40. Thomas L. Blockchain Applications in Healthcare Liji Thomas. URL: https://www.newsmedical.net/health/Blockchain-Applications-in-Healthcare.aspx. (дата звернення: 21.04.2024)

41.Soni N. Evolution of Blockchain Neha Soni. URL: https://medium.com/@nehasoni1812/evolutionofblockchainf243f7509fe6#:~:text=Stefan%20Konst%20published%20his%20theory,linked%20together%20using%20cryptographic%20methods.. (дата звернення: 21.04.2024)

42.How Walmart used blockchain to increase supply chain transparency: The Leadership Network URL:https://theleadershipnetwork.com/article/how-walmart-used-blockchainto-increase-supply-chain-transparency (дата звернення: 21.04.2024)

43.The History of Blockchain Technology URL: https://101blockchains.com/history-of-blockchaintimeline/. (дата звернення: 21.04.2024)

44. Cryptography Hash functions. URL: https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm (дата звернення: 21.04.2024)

45. Smart Contracts: The Ultimate Guide for the Beginners. URL: https://101blockchains.com/smartcontracts/ (дата звернення: 21.04.2024)

46.Майнинг. URL:https://ua.bitcoinwiki.org/wiki/%D0%9C%D0%B0%D0%B9%D0%BD%D0%B8%D0%BD%D0%B3 (дата звернення: 21.04.2024)

47. Что такое Алгоритм Консенсуса в Blockchain. URL: https://academy.binance.com/ru/blockchain/what-isa-blockchainconsensusalgorithm (дата звернення: 21.04.2024)

48. J. Golosova, A. Romanovs, “The Advantages and Disadvantages of the Blockchain Technology”, Riga, 2018

49. What’s a Peer-to-Peer (P2P) Network?

URL: https://www.computerworld.com/article/2588287/networking-peer-to-peernetwork.html (дата звернення: 21.04.2024)

50. Blockchain Architecture Basics: Components, Structure, Benefits & Creation Режим доступу до ресурсу: https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture (дата звернення: 21.04.2024) (дата звернення: 21.04.2024)

51. Что такое децентрализация биткоин и криптовалют URL:https://prostocoin.com/blog/decentralizatio (дата звернення: 21.04.2024)

52. BubbleTone - первая децентрализованная телекоммуникационная экосистема. URL:https://cyberway.golos.io/@ambicia/5blgxwbubbletonepervayadecentralizovannaya-telekommunikacionnaya-ekosistema (дата звернення: 21.04.2024)

53. SCTelecom. IRBIS Network Decentralized telecommunications network. URL:https://safecalls.io/ieo/docs/SCTelecomWPv1.2.pdf? (дата звернення: 21.04.2024)

54. Blockchain for telecom roaming, fraud user identification, and overage management. URL:https://developer.ibm.com/technologies/blockchain/patterns/blockchain-fortelecom-roaming-fraud-and-overage-management (дата звернення: 21.04.2024)

55. Hayes A. Blockchain Facts: What Is lt, How It Works, and How It Can Be Used Investopedia. URL:https://www.investopedia.com/terms/b/blockchain.asp#:~:text=By%20spreading%20its%20operations%20across,the%20processing%20and%20transaction%20fees. (дата звернення: 21.04.2024)

56. Javaid M., Haleem A., Singh R. P., Suman R., Khan S. A review of Blockchain Technology applications for financial services. BenchCouncil Transactions on Benchmarks, Standards and Evaluations. 2022.

57. Keatinge T. Virtual currencies and terrorist financing: assessing the risks and evaluating responses. Policy Department for Citizens’ Rights and 44 Constitutional Affairs. Brussels, 2018. URL: http://www.europarl.europa.eu/supporting-analyses. (дата звернення: 21.04.2024)

58. Malcolm A. Blockchain Principles: Understanding Blockchain Technology. 2021. URL:https://www.businesstechweekly.com/financeandaccounting/fintech/blockchain-principles/. (дата звернення: 21.04.2024)

59. Melendez S. Why You Could Soon Be Voting In A Blockchain-Powered Election. URL:https://www.fastcompany.com/40547127/voting-blockchainstartupdemo-turns-controversial-in-sierra-leone. (дата звернення: 21.04.2024)

60. Meylan P. A. Blockchains Will Change the Way the World Votes. URL: https://www.csis.org/analysis/blockchains-will-change-way-world-votes. (дата звернення: 21.04.2024)

61. Chen M. S., Han J., Yu P. S. Data mining: an overview from a database perspective *Transactions on Knowledge and data Engineering*. URL: https://ieeexplore.ieee.org/abstract/document/553155 (дата звернення: 21.04.2024)

62. Hand D.J. Principles of data mining Drug safety. URL: https://link.springer.com/article/10.2165/00002018-200730070-00010 (дата звернення: 21.04.2024)

63. Legout A., Urvoy-Keller G., Michiardi P. Understanding bittorrent: An experimental perspective. URL: https://hal.inria.fr/inria-00000156v3/document130 (дата звернення: 21.04.2024)

64. Qiu D., Srikant R. Modeling and performance analysis of BitTorrent-like peer-to-peer networks. *ACM SIGCOMM computer communication review*. URL: https://dl.acm.org/doi/pdf/10.1145/1015467.1015508 (дата звернення: 21.04.2024)

65. Johnsen J. A., Karlsen L. E., Birkeland S. S. Peer-to-peer networking with BitTorrent Department of Telematics, NTNU. URL: http://web.cs.ucla.edu/classes/cs217/05BitTorrent.pdf (дата звернення: 21.04.2024)

66. Arthur D., Panigrahy R. Analyzing BitTorrent and related peer-to-peer networks *Proceedings of the seventeenth annual ACM-SIAM symposium on Discrete algorithm 2020*. Vol. 11, no. 1. P. 121–133.

67. Development of the system to integrate and generate content considering the cryptocurrent needs of users 1. Lytvyn, V., Vysotska, V., Kuchkovskiy, V., Bobyk, I., Malanchuk, O., Ryshkovets, Y., Panasyuk, V. *Eastern-European Journal of Enterprise Technologies*. 2022. Vol. 11, no. 1. P. 66–73.

68. Application of Online Marketing Methods and SEO Technologies for Web Resources Analysis within the Region Kuchkovskiy, V., Andrunyk, V., Krylyshyn, M., Chyrun, L., Vysotskyi, A., Chyrun, S., Brodovska, I. *In Computational Linguistics and Intelligent Systems (COLINS 2021 5th International Conference*, Lviv, 22–23 April 2021, CEUR workshop proceedings. Aachen, CEUR-WS. Vol. 057, no. 03.

69. Кучковський В. В., Шаховська Н. Б. Блокчейн як база-даних, його використання, опис розумних контрактів і майбутній потенціал. *Моделювання та інформаційні технології*. URL: http://nbuv.gov.ua/UJRN/Mtit_2019_87_16.131 (дата звернення: 21.04.2024)

70. Кучковський В. В. Алгоритми консенсуса блокчейн систем *Вісник Хмельницького національного університету*. Серія: Технічні науки. URL: http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/08/7-2.pdf (дата звернення: 21.04.2024)

71. Литвин В. В., Висоцька В. А., Кучковський В. В., Дуткевич С. Ю., Наум О. Метод інтеграції та управління контентом мережі інформаційних ресурсів туризму згідно з потребами *користувача Вісник Національного університету "Львівська політехніка*". Серія: Інформаційні системи та мережі. URL:https://science.lpnu.ua/sites/default/files/journalpaper/2019/feb/15577/181912maket-22-36.pdf (дата звернення: 21.04.2024)

72. Литвин В. В., Висоцька В. А., Кучковський В. В., Оливко Р. М. Архітектура інформаційної системи інтеграції та формування контенту прокриптовалюти на основі аналізу діяльності бірж *Вісник Національного університету "Львівська політехніка"*. Серія: Інформаційні системи та мережі. URL:https://science.lpnu.ua/sites/default/files/journalpaper/2019/feb/15579/181912maket-43-60.pdf (дата звернення: 21.04.2024)

73. Architecture of system for content integration and formation based on cryptographic consumer needs Lytvyn, V., Kuchkovskiy, V., Vysotska, V., Markiv, O., & Pabyrivskyy, *IEEE 13th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT*). URL: https://ieeexplore.ieee.org/abstract/document/8526669 (дата звернення: 21.04.2024)

74. Kuchkovskiy, V., Shakhovska, N. Information technology of Blockchain: Database, smart contracts, architecture *IEEE 14th International Conference on Computer Sciences and Information Technologies (CSIT).* URL: https://ieeexplore.ieee.org/abstract/document/8929885 (дата звернення: 21.04.2024)

75. Кучковський В. В. Алгоритми консенсусу Trends in science and practice of today: abstracts of XXVIII *International scientific and practical conference*. URL: https://isg-konf.com/wp-content/uploads/2021/05/XXVIII-ConferenceJune-01-042021.pdf стр.502 (дата звернення: 21.04.2024)

76. Кучковський В. В. Змішані алгоритми консенсусу Trends in science and practice of today: abstracts of XXVIII. *International scientific and practical conference*. URL: https://isg-konf.com/wp-content/uploads/2021/05/XXVIII-ConferenceJune-01-042021.pdf ст.502 (дата звернення: 21.04.2024)

77. Проненко Т. В. Практичне застосування блокчейн технології у медицині In Технічні та математичні науки. Студентський науковий форум.

78. Полівода, К. А. Блокчейн–один із головних технологічних проривів останнього часу *Матеріали II Всеукраїнської науково-практичної Інтернетконференції студентів, аспірантів і молодих вчених "Розвиток послуг та інновацій в цифровій економіці*". ст. 251–253. URL :https://sci.ldubgd.edu.ua/bitstream/123456789/9555/1/Zbirnyk_4_19.pdf#page=251 (дата звернення: 21.04.2024)

79. Осядлий, В., & Москаленко, А. Система керування медичними даними на основі блокчейн-технологій. Measuring and computing devices in technological processes. Vol. 1, no. 1. P. 13–25.

80. Khrystynets, N., Miskevych, O., Mazurenko, V. Технології Blockchain для оптимізації процесів документообігу. *Computer-integrated technologies: education, science, production.* URL: http://cit-journal.com.ua/index.php/cit/article/view/172 (дата звернення: 21.04.2024)

81. Rüth J. et al. Digging into browser-based crypto mining. *Proceedings of the Internet Measurement Conference (IMC' 18*). URL :https://dl.acm.org/doi/10.1145/3278532.3278539 (дата звернення: 21.04.2024)

82. Uchibeke U. U. et al. Blockchain access control ecosystem for big data security *2018 IEEE International Conference on Internet of Things (iThings) and 133IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData*). URL: https://ieeexplore.ieee.org/document/8726516 (дата звернення: 21.04.2024)

83. Tariq N. et al. The security of big data in fog-enabled IoT applications including blockchain: A survey Sensors. URL: https://www.mdpi.com/1424-8220/19/8/1788 (дата звернення: 21.04.2024)

84. Li J. et al. Blockchain-based public auditing for big data in cloud storage. *Information Processing & Management*. URL: https://doi.org/10.1016/j.ipm.2020.102382 (дата звернення: 21.04.2024)

85. Hasan M. K. et al. Blockchain technology on smart grid, energy trading, and big data: security issues, challenges, and recommendations. *Wireless Communications and Mobile Computing*. URL: https://www.hindawi.com/journals/wcmc/2022/9065768/ (дата звернення: 21.04.2024)

86. Тимчук П.В., Грига В.М. Блокчейн-базована система підтримки криптовалютних операцій для ОС Android. *Матеріали XXIV Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів «СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»*, 18 – 19 квітня 2024 року, м. Одеса, Україна, С. 279-281.

ДОДАТОК А

(обов'язковий)

ЛІСТИНГ Блокчейн-базована система підтримки криптовалютних операцій для ОС Android

Модуль «Створення гаманця на C++».

```
#include <openssl/evp.h>
#include <openssl/rand.h>
#include <openssl/sha.h>
#include <iostream>
#include <vector>
#include <string>
#include <iomanip>
#include <sstream>

// Функція для генерації випадкових байтів
std::vector<unsigned char> generateRandomBytes(int length) {
    std::vector<unsigned char> bytes(length);
    RAND_bytes(bytes.data(), length);
    return bytes;
}

// Функція для створення приватного ключа
std::vector<unsigned char> generatePrivateKey() {
    return generateRandomBytes(32); // 256-бітний ключ
}

// Функція для створення публічного ключа з приватного ключа
std::vector<unsigned char> generatePublicKey(const
std::vector<unsigned char>& privateKey) {
    // Приклад реалізації залежить від специфічного алгоритму
криптовалюти (наприклад, ECDSA для Bitcoin)
    std::vector<unsigned char> publicKey; // Це потрібно
реалізувати
```

```
        // ...
        return publicKey;
    }

    // Функція для створення адреси з публічного ключа
    std::string generateAddress(const std::vector<unsigned char>&
publicKey) {
        // Створення адреси залежить від специфіки криптовалюти
        unsigned char hash[SHA256_DIGEST_LENGTH];
        SHA256(publicKey.data(), publicKey.size(), hash);

        std::stringstream ss;
        for (int i = 0; i < SHA256_DIGEST_LENGTH; ++i)
            ss << std::hex << std::setw(2) << std::setfill('0') <<
(int)hash[i];

        return ss.str();
    }

    int main() {
        std::vector<unsigned char> privateKey = generatePrivateKey();
        std::vector<unsigned char> publicKey =
generatePublicKey(privateKey);
        std::string address = generateAddress(publicKey);

        std::cout << "Private Key: ";
        for (auto byte : privateKey)
            std::cout << std::hex << std::setw(2) << std::setfill('0')
<< (int)byte;
        std::cout << std::endl;

        std::cout << "Public Key: ";
        for (auto byte : publicKey)
            std::cout << std::hex << std::setw(2) << std::setfill('0')
<< (int)byte;
```

```
    std::cout << std::endl;

    std::cout << "Address: " << address << std::endl;

    return 0;
}
```

Модуль «Інтеграція з Android через JNI».

```
// wallet.cpp
#include <jni.h>
#include <string>
#include "wallet.h"

extern "C" JNIEXPORT jstring JNICALL
Java_com_example_wallet_MainActivity_generateAddress(JNIEnv* env, jobject /* this */) {
  std::vector<unsigned char> privateKey = generatePrivateKey();
  std::vector<unsigned char> publicKey = generatePublicKey(privateKey);
  std::string address = generateAddress(publicKey);
  return env->NewStringUTF(address.c_str());
}
```

Модуль «Java-код для виклику C++ функцій через JNI».

```
package com.example.wallet;

public class MainActivity extends AppCompatActivity {

   static {
      System.loadLibrary("wallet");
   }

   public native String generateAddress();

   @Override
   protected void onCreate(Bundle savedInstanceState) {
      super.onCreate(savedInstanceState);
      setContentView(R.layout.activity_main);

      TextView addressView = findViewById(R.id.addressView);
      addressView.setText(generateAddress())
```

ДОДАТОК В

(обов'язковий)

Тези

УДК 004.8

БЛОКЧЕЙН-БАЗОВАНА СИСТЕМА ПІДТРИМКИ КРИПТОВАЛЮТНИХ ОПЕРАЦІЙ ДЛЯ ОС ANDROID

ТИМЧУК П.В. (petya.timchuk5@gmail.com)
ГРИГА В.М. (gr.volodymyr2018@gmail.com)
Хмельницький національний університет
Прикарпатський національний університет імені Василя Стефаника

Ця робота включає аналіз ефективної системи підтримки криптовалютних операцій для операційної системи Android з використанням блокчейн-технології. Для швидкої та надійної розробки використано мову програмування Python та фреймворк Django, а також базу даних MySQLite та MongoDB для гнучкості та потужності. HTML, CSS та JavaScript використано для створення зручного та привабливого зовнішнього вигляду. За допомогою API, розробленої для інтеграції з телеграм-ботами, користувачі можуть легко отримувати сповіщення про свої криптовалютні операці. Її функціональний аналіз підтвердив, що вона надійна, стабільно працює та зручна у використанні.

Постановка проблеми та актуальність. З появою різноманітних криптовалют і зростанням популярності їх використання для різних фінансових операцій, таких як перекази та покупки, з'являється потреба в зручних і безпечних засобах для управління цими операціями [1,2]. Такі системи необхідні для забезпечення безпеки та конфіденційності під час здійснення операцій з криптовалютою, а також для надання простих інструментів для управління та моніторингу. Блокчейн-технологія надає децентралізовану, безпечну платформу для здійснення та відстеження криптовалютних операцій, що дозволяє вирішити багато з цих проблем. Наразі існуючі системи підтримки криптовалютних операцій для операційної системи Android не завжди забезпечують достатню безпеку та зручність для користувачів. Вони часто можуть бути уразливими до кібератак або не гарантувати достатньо конфіденційності особистих даних користувачів [3]. Отже, необхідно створювати безпечні, інноваційні та нові рішення для

Мета та завдання роботи. Розробка розширеного набору функцій є ключовим завданням цього проекту. У ньому буде підтримка різних протоколів криптовалют, а також основні можливості, необхідні для проведення операцій з криптовалютами. Серед цих можливостей є ведення статистики, аналіз фінансових потоків, управління портфелем криптовалют та підтримка ряду протоколів. Забезпечення високого рівня безпеки та захисту персональних даних користувачів від кібератак і несанкціонованого доступу до фінансових активів є важливою складовою цього проекту. Це охоплює використання сучасних стандартів безпеки та технології шифрування, протоколи двофакторної аутентифікації та детальне вивчення і контроль потенційних загроз безпеції. Забезпечити сумісність системи та максимальну продуктивність для різних моделей і версії мобільних пристроя на базі Android є надзвичайно важливим завданням. Програми будуть ефективно працювати на всіх типах пристрої при застосуванні передових технології розробки і оптимізованим кодом.

Викладення суті роботи. При виконанні поставленої задачі було розробленно онлайн додаток, для безпосереднього використання оплати схожої до оплати кредитною картою, а також двохфакторної автроизацією щоб забезпечити безпечний вхід до додатку який поєднує в собі цілу систему, обміну валюти покупки за валюта та багато іншого. Для авторизації в додатку потрібено ваша електрона адреса та придуманний вами пароль, а також підключення до номеру телефону це і є другий етап безпекий.

На рис. 1 розробленого системний додаток для підтримки та реалізації криптовалютних систем. Показано початкову сторінку із регістраційним полем та полем аутенфікції.

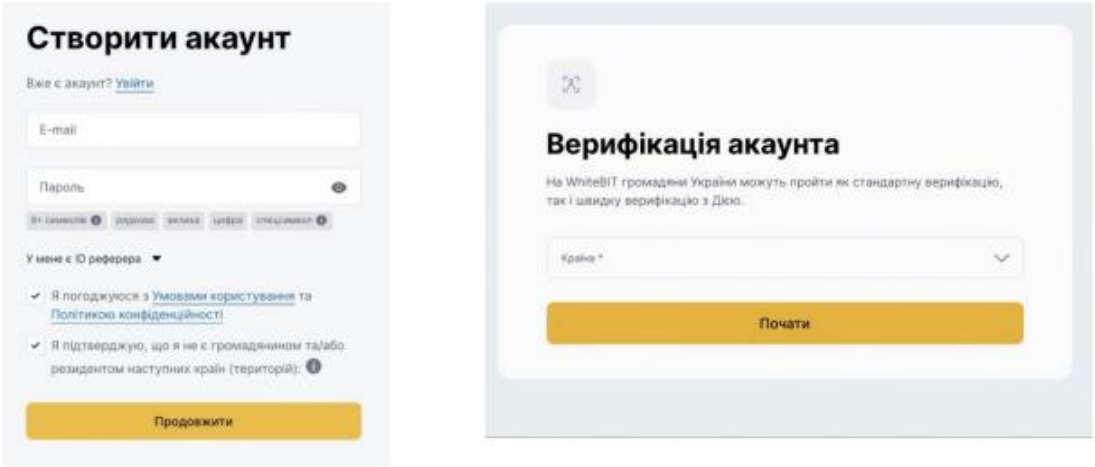


Рис 1. – Інтерфейс для регістрації та верифікації.

На рис. 2 показано інтерфейс панелі керування сервісу, де показано скільки є активів у даних валютах, скільки вони коштують в реальних грошах та графіки цінової категорії, а також можна редагувати свої дані та переказ валюти та останні витрати.

На рис 3. представлено сторінку кабінету користувача.

Рис. 2 – Інтерфейс панелі керування програмою для ОС Android.

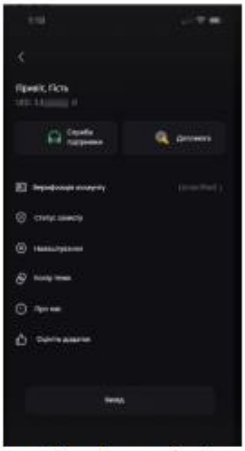


Рис. 3. – Інтерфейс кабінету користувача.

Висновок. Таким чином, система, яка базується на блокчейні, підтримує операції з криптовалютою на операційній системі Android. Це дозволило автоматизувати використання заощаджень криптовалюти, наприклад, перекази, придбання нової валюти або доповнення існуючої. Серед переваг цього сервісу є зручність, стабільність, гнучкість та надійний захист. Дану систему можна використовувати на ринку крипто валют.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Zimmerman P. Blockchain structure and cryptocurrency prices // Staff working Paper / Bank of England. – 2020. – No 855, February 2020. – P.1-75. URL: https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2020/blockchain-structure-and-cryptocurrency-prices.pdf
2. Biktimirov M. R. et al. Blockchain technology: Universal structure and requirements // Automatic Documentation and Mathematical Linguistics. – 2017. – Vol. 51 (6). – P. 235-238. URL: https://link.springer.com/article/10.3103/S0005105517060036
3. Zheng Z. et al. Blockchain challenges and opportunities: A survey // International journal of web and grid services. – 2018. – Vol. 14, No 4. – P. 352-375. URL: https://allquantor.at/blockchainbib/pdf/zheng2018blockchain.pdf

ДОДАТОК В

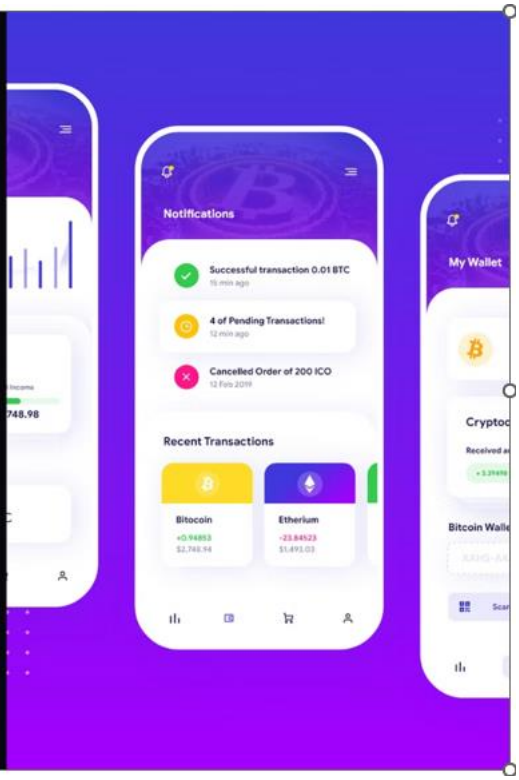
(обов’язковий)

Тези

Блокчейн-базована система підтримки криптовалютних операцій для ОС Android

Представляємо інноваційну блокчейн-платформу, яка пропонує надійне та зручне рішення для здійснення криптовалютних транзакцій на мобільних пристроях з ОС Android. Ця система поєднує передові технології шифрування та розподіленого реєстру, забезпечуючи високий рівень безпеки та прозорості фінансових операцій.

Виконав студент
Група КІ-2м-22-1
Тимчук Петро



Вступ

Мобільний додаток, що ми пропонуємо, дозволить користувачам легко та безпечно здійснювати операції з криптовалютами. Ця блокчейн-базована система забезпечить високий рівень конфіденційності та прозорості всіх транзакцій. Наш додаток інтегрується з основними гаманцями криптовалют та надає інтуїтивно зрозумілий інтерфейс для управління коштами.

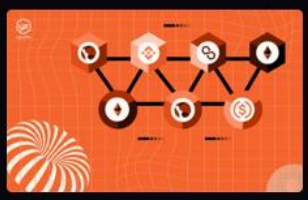
Що таке блокчейн?

Структура блокчейну

Блокчейн - це розподілена база даних, яка зберігає записи про всі транзакції у вигляді «блоків», з'єднаних в ланцюжок за допомогою криптографії.

Децентралізована мережа

Блокчейн працює на основі децентралізованої мережі, в якій немає єдиного управляючого центру. Кожен учасник мережі зберігає копію бази даних.



Транзакції в блокчейні

Нові транзакції підтверджуються та додаються до блокчейну учасниками мережі. Це забезпечує високий рівень безпеки та прозорості системи.

Безпека та конфіденційність в блокчейн-екосистемі

Криптографічний захист

Блокчейн-технологія використовує потужні криптографічні методи, що забезпечують високий рівень захисту даних від несанкціонованого доступу та підробки.

Захист конфіденційності

Завдяки анонімності транзакцій та конфіденційності особистих даних, блокчейн гарантує недоторканність приватного життя користувачів.

Надійний захист

Децентралізований характер блокчейну унеможливлює точковий злам чи злом всієї системи, забезпечуючи надійний захист від кіберзагроз.

Інтеграція з гаманцями криптовалют

1 **Сумісність з провідними криптогаманцями**

Наша блокчейн-базована система підтримує підтримує найпопулярніші гаманці криптовалют, такі як Ethereum Wallet, Coinbase Wallet та Trust Wallet, забезпечуючи зручну та безпечну інтеграцію інтеграцію для користувачів.

2 **Підтримка основних криптовалют**

Додаток дозволяє здійснювати операції з Bitcoin, Ethereum, Litecoin та іншими популярними криптовалютами, надаючи користувачам всебічний доступ до світу цифрових активів.

3 **Синхронізація балансів та історії транзакцій**

Наша система автоматично синхронізує баланси та історію транзакцій з підключеними криптовалютними гаманцями, забезпечуючи повну прозорість та контроль над фінансовими операціями.

4 **Надійність та безпека**

Інтеграція з перевіреними та надійними криптовалютними гаманцями гарантує високий рівень безпеки ваших цифрових активів та конфіденційність ваших фінансових операцій.

Функціональність мобільного додатку

Зручний інтерфейс

Мобільний додаток має інтуїтивно зрозумілий та легкий в навігації інтерфейс. Усі основні функції доступні за кілька кліків, що полегшує управління криптовалютними операціями.

Інтеграція з гаманцями

Додаток дозволяє безпечно підключати ваші криптовалютні гаманці та здійснювати операції з різними цифровими валютами безпосередньо в мобільному додатку.

Моніторинг транзакцій

Додаток надає зручні інструменти для моніторингу всіх ваших криптовалютних транзакцій, включаючи історію платежів, баланси та статистику.

Безпека та конфіденційність

Безпека даних та збереження конфіденційності користувачів є пріоритетним завданням. Додаток використовує передові методи шифрування та аутентифікації.

Процес здійснення транзакцій

1 **Авторизація**
Вхід в особистий обліковий запис

2 **Вибір валюти**
Вибір криптовалюти для проведення операції

3 **Введення суми**
Вказання необхідної суми транзакції

4 **Підтвердження**
Підтвердження та відправка платежу

Процес здійснення криптовалютних транзакцій в нашому додатку є легким та зручним. Користувач може з легкістю авторизуватись в особистому кабінеті, обрати бажану криптовалюту, ввести суму та підтвердити платіж. Весь процес проходить в безпечному та конфіденційному режимі завдяки технології блокчейн.

Аналітика та моніторинг операцій

Ключовою функціональністю мобільного додатку є надання користувачам повного набору інструментів для аналітики та моніторингу криптовалютних операцій. Завдяки інтуїтивному інтерфейсу та зручним візуалізаціям, користувачі можуть легко відстежувати всі свої транзакції, аналізувати історію та статистику, а також прогнозувати майбутні тенденції.

100K	95%	24/7
Транзакцій	**Прозорість**	**Моніторинг**
Відстеження детальної історії понад 100 000 виконаних транзакцій.	Ступінь прозорості фінансових операцій, завдяки повному аудиту в блокчейні.	Цілодобовий моніторинг ринку, курсів валют та сповіщення про важливі події.

Масштабованість та продуктивність системи

Горизонтальне масштабування

Система розроблена з використанням модульної архітектури, що дозволяє легко додавати нові вузли для обробки зростаючої кількості користувачів та транзакцій.

Відмовостійка архітектура

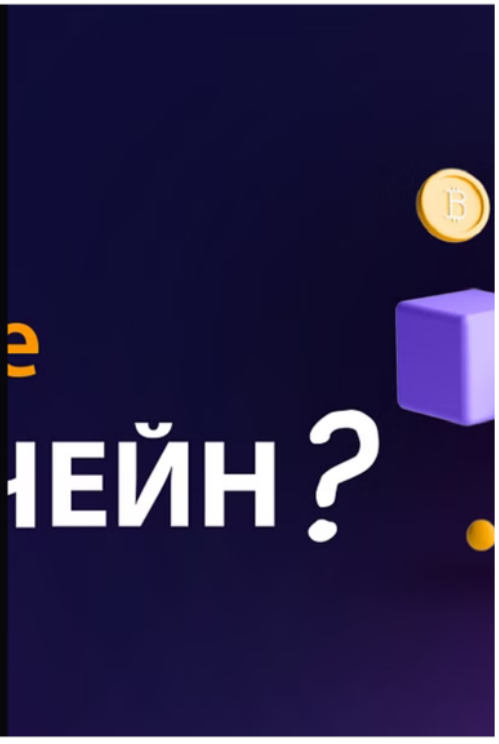
Система використовує кластерну конфігурацію з автоматичним балансуванням навантаження, що забезпечує безперебійну роботу навіть при виході з ладу окремих вузлів.

Оптимізація продуктивності

Використання сучасних технологій, таких як обчислення в пам'яті та паралельні обчислення, дозволяє досягати високої швидкості обробки транзакцій.

Перспективи розвитку та майбутні можливості

Блокчейн-базована система підтримки криптовалютних операцій для ОС Android має величезний потенціал розвитку в майбутньому. Очікується, що що ця технологія стане невід'ємною частиною фінансових послуг, забезпечуючи безпечні, прозорі та ефективні транзакції.



UNICHECK
by Turnitin

Ім'я користувача:
Кафедра КІ

ID перевірки:
1016294048

Дата перевірки:
29.05.2024 12:04:44 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
29.05.2024 16:10:46 EEST

ID користувача:
100005591

Назва документа: Тимчук_Блокчейн-базована система підтримки криптовалютних операцій для ОС Android

Кількість сторінок: 40 Кількість слів: 21107 Кількість символів: 162282 Розмір файлу: 7.65 MB ID файлу: 1016088554

6.53%
Схожість

Найбільша схожість: 5.06% з Інтернет-джерелом (https://lpnu.ua/sites/default/files/2022/radaphd/21254/disertaciya_0.p..

6.44% Джерела з Інтернету 108 ..... Сторінка 42

0.68% Джерела з Бібліотеки 53 ..... Сторінка 43

0.37% Цитат

Цитати 5 ..... Сторінка 44

Посилання 1 ..... Сторінка 44

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи 13

Wed May 29 06:32:12 EEST 2024, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 13%**

ID: 127628 Назва: МКР Блокчейн-базована система підтримки криптовалютних операцій для ОС Android Додано в БД: 2024-05-29 Автора: Тимчук П.В. Керівники: Грига В.М. Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	149205	1210	965 (1%)	18 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Тимчук Петро Володимирович

Тема: Блокчейн-базована система підтримки криптовалютних операцій для ОС Android

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість сторінок записки 95.

1. Короткий зміст роботи та прийнятих рішень: Метою роботи є розроблення мобільного додатку блокчейн-базованої системи на базі ОС Android.

2. Висновок про відповідність роботи дипломному завданню: Кваліфікаційна робота магістра відповідає виданому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі було проведено огляд та аналіз аналогічних систем, розглянуто особливості блокчейну та аналітику, а також визначені проблеми поставленого завдання. У другому розділі реалізовано архітектуру та запропоновано використання алгоритму криптографії, даний метод є основою для розрахунку базованої-блокчейн системи та зміни криптовалютних значень. Розроблена архітектура системи дозволяє різні варіації використання із виявленням різних чинників, які впливають на характеристики системи. У третьому розділі вибрано мову реалізації та її апаратні складові, які встановлюють різні параметри, а також обрано систему тестування даного додатку і оцінювання в реальному часі. У четвертому розділі досліджено сучасні тенденції та більш ефективні блокчейн системи, а також як можна ефективно до цього додати використання штучного інтелекту і машинного навчання. Використання потенціалу IoT технології блокчейн системи, а також безпосередньо перспективи у розвитку

блокчейн технології і визначення стратегії підтримки та популяризації розробленого додатку на криптовалютному ринку.

4. Позитивні сторони роботи: Отримано два пункти наукової новизни.

5. Негативні сторони роботи: Було допрацьовано чи удосконалено вже існуючі алгоритми та технології рішення задачі, замість створення власних.

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації.

7. Відгук про роботу в цілому: В загальному робота була виконана на задовільному рівні.

8. Інші зауваження: Відсутні.

9. Оцінка дипломної роботи: Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи вважаю, що робота заслуговує оцінки «задовільно» ( ).

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи)
Мартинюк Валерій Володимирович
зав. каф. АКІТ та Р

"30" 05 2024 р. (підпис)

Завідувачу кафедри КІІС
д-р.техн.наук, проф. Говорущенко Т. О.

Тимчука Петра Володимировича
ПІБ здобувача вищої освіти

ФІТ, 2 курсу, групи КІ2м-21-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

22 квітня 2023 року

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОМАЦІЙНИХ СИСТЕМ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Блокчейн-базована система підтримки криптовалютних операцій для ОС Android

Автор: Тимчук Петро Володимирович

Спеціальність: 123 – Комп'ютерна інженерія

Освітня програма: освітньо-наукова

Науковий керівник: Грига В.М. к.т.н., доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах є збіг зі звітом з науково-дослідної практики автора Тимчука Петра Володимировича "Блокчейн-базована система підтримки криптовалютних операцій для ОС Android", який було додано в репозитарій ХНУ 21 березня 2024 року;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з джерелами на один фрагмент речення;
4) У якості запозичень у деяких місцях системою зафіксовано послідовності чотирирозрядних двійкових кодів та поєднання латинських символів українськими скороченнями та індексами у формулах. Такі модифікації не можуть бути розглянуті як переробка тексту, вони відносяться до використання спеціальних символів та форматування, яке є типовим для математичних та технічних виразів.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості Unicheck, складає 6.53% і адресується до 108 першоджерел, та системою Anti-Plagiarism складає 0% що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ В.М. Грига

Гарант ОП _____ О.С. Савенко

Завідувач кафедри КІІС _____ Т.О. Говорущенко