НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет інформатики та обчислювальної техніки

Кафедра інформаційних систем та технологій

До захисту допущено:

Завідувач кафедри

_____ Олександр РОЛІК

«___»_____2023 р.

Дипломний проєкт

на здобуття ступеня бакалавра
за освітньо-професійною програмою «Інформаційні управляючі системи та технології»
спеціальності 126 «Інформаційні системи та технології»
на тему: «Мобільний застосунок для обміну криптовалют з використанням технології блокчейн»

Виконав:
студент IV курсу, групи ІС-93
Трохимець Максим Миколайович _____

Керівник:
Доцент, к.т.н., доцент,
Резніков Сергій Анатолійович _____

Рецензент:
Доцент, к.т.н., доцент,
Баклан Ігор Всеволодович _____

Засвідчую, що у цьому дипломному проєкті немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2023 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Факультет інформатики та обчислювальної техніки
Кафедра інформаційних систем та технологій

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 126 «Інформаційні системи та технології»

Освітньо-професійна програма «Інформаційні управляючі системи та технології»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Олександр РОЛІК
«___»_____20__ р.

ЗАВДАННЯ

на дипломний проєкт студенту

Трохимцю Максиму Миколайовичу

1. Тема проєкту «Мобільний застосунок для обміну криптовалюти з використанням технології блокчейну», керівник проєкту Резніков Сергій Анатолійович, доцент кафедри ІСТ, затверджені наказом по університету від «31» травня 2023 р. № 2101-с.

2. Термін подання студентом проєкту: «12» червня 2023 р.

3. Вихідні дані до проєкту: Інформація про обмінний курс конкретної криптовалюти, розроблений застосунок для використання обмінного пункту криптовалют, сума обміненої валюти чи криптовалюти.

4. Зміст пояснювальної записки: Аналіз аналітичних та практичних механізмів відстеження платежів на основі технології блокчейн. Розробка мобільного застосунку для обміну криптовалют з використанням технології блокчейн для автоматизації обмінних операцій і формування найбільш раціонального кошика криптовалют за рахунок використання смартфонів і мобільних обчислень.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслеників, плакатів, презентацій тощо): Д1 – Схема реєстрації користувача, Д2 – Компоненти Android-застосунку, Д3 – Модель покупки криптовалюти, Д4 – Модель події надсилання криптовалюти, Д5 – Модель події реєстрації.

6. Дата видачі завдання: «27» лютого 2023 р.

Календарний план

№ з/п	Назва етапів виконання дипломного проєкту	Термін виконання етапів проєкту	Примітка
1	Вивчення рекомендованої літератури	08.03.2023	Виконано
2	Аналіз існуючих методів	20.03.2023	Виконано
3	Постановка та формалізація задачі	27.03.2023	Виконано
4	Розробка програмного забезпечення	08.05.2023	Виконано
5	Налагодження програми	13.05.2023	Виконано
6	Оформлення пояснювальної записки	23.05.2023	Виконано
7	Подання ДП на попередній захист	29.05.2023	Виконано
8	Подання ДП на основний захист	12.06.2023	Виконано

Студент Максим ТРОХИМЕЦЬ

Керівник Сергій РЕЗНІКОВ

РЕФЕРАТ

Дипломний проєкт складається зі вступу, трьох розділів та висновків до них, загальних висновків, списку використаних джерел, додатків, загальним обсягом робота складає 68 сторінок, має 33 рисунки, 5 діаграм(креслеників), 1 сторінку додатків. Список використаних джерел містить 24 найменування і займає 3 сторінки.

Мета роботи – розробка мобільного застосунку для обміну криптовалюти з використанням технології блокчейну для автоматизації обмінних операцій і формування найбільш раціонального кошика криптовалют за рахунок використання смартфонів і мобільних обчислень.

Предметом дослідження є теоретичні та практичні механізми відстеження платежів на основі технології блокчейну.

У вступі обґрунтовується актуальність теми роботи, визначаються мета дослідження та завдання, які необхідно вирішити для досягнення цієї мети, можливі результати дослідження.

У першому розділі розповідається основи технології блокчейну, концепцію блокчейну, а також впровадження та застосування технології блокчейну у світі. Також приділяється увага формуванню державних механізмів регулювання використання криптовалют та технології блокчейну.

У другому розділі роботи розглядаються результати застосування технології блокчейну у фінансово-економічній сфері. Зокрема, сучасні методи використання технології блокчейну у бухгалтерському обліку та аудиті, у фінансових послугах та в управлінні державними фінансами.

У третьому розділі розглядається програмна розробку із запровадженням технології блокчейну. Аналізуючи майбутні проекти з використанням технології блокчейну, було запропоновано механізми вирішення основних проблем.

Ключові слова: безпека, блокчейн, криптоактиви, технологія блокчейн, фінансово-економічний сектор, цифрові технології.

ABSTRACT

The thesis consists of an introduction, three sections and conclusions to them, general conclusions, a list of used sources, appendices, the total volume of the work is 68 pages, it has 33 images, 5 diagrams(schemes), and 1 page of appendices. The list of used sources contains 24 items and occupies 3 pages.

The purpose of the work is to analyze problems and develop a mobile application for cryptocurrency exchange through the implementation of blockchain technology.

The subject of the study is the theoretical and practical mechanisms of tracking payments based on blockchain technology.

The introduction substantiates the relevance of the topic of the work, defines the purpose of the research and tasks that must be solved to achieve this goal, possible research results.

The first chapter covers the basics of blockchain technology, the concept of blockchain, and the implementation and application of blockchain technology in the world. Attention is also paid to the formation of state mechanisms for regulating the use of cryptocurrencies and blockchain technology.

The second section of the work examines the results of applying blockchain technology in the financial and economic sphere. In particular, modern methods of using blockchain technology in accounting and auditing, financial services and public finance management.

The third chapter considers software development with the introduction of blockchain technology. Analyzing future projects using blockchain technology, mechanisms for solving the main problems were proposed.

Keywords: blockchain, blockchain technology, cryptoassets, digital technologies, financial and economic sector, security

Номер рядка	Формат	Позначення	Найменування	Кільк. аркушів	Номер екзем.	Примітка
1			Документація загальна			
2						
3			Знову розроблена			
4	А4	ІС-93.260БАК.004 ПЗ	Пояснювальна записка	62		
5	А3	ІС-93.260БАК.004 Д1	Схема реєстрації користувача	1		
6	А3	ІС-93.260БАК.004 Д2	Компоненти Android-	1		
7			застосунку			
8	А3	ІС-93.260БАК.004 Д3	Модель покупки криптовал.	1		
9	А3	ІС-93.260БАК.004 Д4	Модель події надсилання	1		
10			криптовалюти			
11	А3	ІС-93.260БАК.004 Д5	Модель події реєстрації	1		
12			користувача			
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						

Зм.	Аркуш	№ докум.	Підпис	Дата	ІС93.260БАК.004 ТП		
Розроб.		Трохимець М.М.			Мобільний застосунок для обміну криптовалют з використанням технології блокчейн Відомість проєкту	Літ. Т	Аркуш 1 / Аркушів 1
Керівн.		Резніков С.А.				КПІ ім. Ігоря Сікорського Група ІС-93	
Затв.							

Пояснювальна записка
до дипломного проєкту
на тему:
« Мобільний застосунок для обміну криптовалют з використанням технології блокчейн »

Київ – 2023 року

ЗМІСТ

СПИСОК ТЕРМІНІВ ТА СКОРОЧЕНЬ

Трейдери — це учасники торгів на фондовій біржі, які отримують прибуток від торгових операцій з купівлі-продажу якогось цінного активу (акцій, валюти тощо).

Ліквідність - економіка, в якій власність цінних активів швидко продається за цінами, близькими до ринкових. Чим легше та швидше актив можна конвертувати до повної вартості, тим він ліквідніший.

Криптовалюта — це цифрова віртуальна валюта, яка використовує асиметрично зашифровані криптографічні алгоритми для забезпечення безпеки транзакцій. Криптовалюти також відомі як криптовалюти.

Асиметричне шифрування — це метод шифрування даних за допомогою пари пов’язаних ключів: відкритого та закритого ключів.

Торгівля криптовалютою – це різновид інтернет-трейдингу, який відбувається на біржі криптовалют.

Forex, FOReign Exchange – міжбанківський міжнародний валютний ринок.

Біткойн - це цифрова валюта, криптовалюта.

Біткойн можна торгувати в обмін на товари чи послуги, які приймають біткойн як оплату.

Альткойн — це будь-яка цифрова криптовалюта, крім біткойна.

Термін походить від «альтернативи біткойнам» і використовується для опису криптовалюти, яка не є біткойном.

ETH – Ethereum(етер), цифрова валюта, криптовалюта.

Етер можна торгувати в обмін на товари чи послуги, які приймають біткойн як оплату. Також це найбільш популярна криптовалюта та блокчейн для ознайомлення зі світом криптовалют.

EVM – Ethereum Virtual Machine(віртуальна машина Ethereum), середовище для виконання смарт-контрактів.

ETC – Ethereum Classic, блокчейн, який виникнув в результаті хардфорку основого блокчейну Ethereum.

BSC – Binance Smart Chain, блокчейн від компанії Binance, який взяв за основу блокчейн Ethereum.

DeFi – Decentralized Finances, загальна назва для аналогів традиційних фінансових інструментів, реалізованих у децентралізованій архітектурі

Fiat тендер – це валюта або валюта, вартість якої визначається не її внутрішньою вартістю чи гарантією обміну на золото чи інші валюти, а скоріше з дозволу уряду використовувати її як засіб платежу.

ВСТУП

Останніми роками в усьому світі відзначається величезний інтерес до криптовалют і технології блокчейну, що лежить в основі їх створення. До віртуальних грошей ставлення різних офіційних влад досить насторожене. Технологія блокчейну привертає пильну увагу фахівців та активно просувається зацікавленими офіційними та діловими колами у практичну сферу.

Оскільки блокчейн це глобальна база даних, що не належить нікому і має широке поширення, внесення змін є надзвичайно складним навіть для операторів зберігання даних.

Хоча блокчейн часто асоціюється з криптовалютою, останнім часом все більше фахівців розглядають його можливості в сфері бізнесу та управління окрім фінансів. Технологію блокчейн також розглядають як засіб, який може замінити банки як посередників у фінансових транзакціях, і саме банки виявляють до неї найбільший інтерес. Банк Англії з 2017 р. розпочав модернізацію своєї фінансової інфраструктури на базі технології блокчейну.

Зазначені вище фактори підкреслюють практичне значення та актуальність обраної теми дипломного проєкту.

Метою дипломного проєкту – розробка мобільного застосунку для обміну криптовалюти з використанням технології блокчейну для автоматизації обмінних операцій і формування найбільш раціонального кошика криптовалют за рахунок використання смартфонів і мобільних обчислень.

Завдання роботи:

- розкрити поняття та сутність технології відстеження шахрайських платежів в блокчейні.
- вивчити правове регулювання випуску та обігу криптовалюти.
- виявити проблеми застосування цієї технології.
- проаналізувати перспективи застосування технології та запропонувати свій застосунок.

Об'єктом дослідження є міжнародна та українська практика випуску та обігу криптовалют, а також їх обміну.

Предметом дослідження є криптовалюта та технологія блокчейну у зовнішній економічній діяльності.

Методи дослідження: аналіз нормативно-правових актів та спеціальної літератури; вивчення вітчизняної та закордонної практики здійснення операцій криптовалютами; статистичний метод.

Теоретичною основою роботи послужили праці таких авторів, як Ю. С. Осипов., А.І. Бубель, А.А. Лавринович, А.І Краснова.

Практичну базу роботи становили розроблені методи обміну криптовалют.

Структурно робота складається з вступу, трьох розділів, висновків та списку використаних джерел. У першому розділі описується поняття, сутність, криптовалюти та блокчейну, а також розкривається суть технології розрахунків криптовалют. У другому розділі розкривається опис технічного завдання ідеться про ознайомлення з середовищами. У третій главі проводиться аналіз проблем впровадження технології криптовалюти та блокчейну. У висновку зроблено основні висновки.

1 ТЕОРЕТИЧНІ АСПЕКТИ ВИВЧЕННЯ КРИПТОВАЛЮТ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ БЛОКЧЕЙН. ОГЛЯД АНАЛОГІВ

1.1. Теоретичні основи

1.1.1. Опис предметного середовища

Принцип роботи блокчейну.

Незважаючи на те, що блокчейн є системою, в якій кожен учасник може здійснити транзакцію, не всі учасники мають однакові ролі. Учасники поділяються на операторів (майнерів/валідаторів), які здійснюють транзакції, мережевих регуляторів, що відповідають за реєстрацію, і звичайних користувачів.

Процес формування блоку складається з кількох етапів.

а) Перший етап - визначення транзакції. Відправник створює транзакцію, яка містить інформацію про адресу одержувача, деталі транзакції (суму коштів, товари тощо) і криптографічний цифровий підпис, що підтверджує її справжність і легітимність. Вузли мережі отримують сповіщення про транзакцію і перевіряють її дійсність шляхом розшифрування електронного підпису. Якщо транзакція пройшла перевірку, вона стає очікувати включення в блок.

б) Створення блоку. Блоки, які містять інформацію про транзакції, поєднуються в "ланцюжок" за допомогою складних математичних алгоритмів. Нові блоки завжди додаються в кінець ланцюжка. Один з вузлів мережі періодично збирає незавершені транзакції, формує з них блок і відправляє його для перевірки та приєднання до ланцюжка іншим учасникам мережі.

в) Перевірка блоку. Вузли, відповідальні за перевірку блоку, запитують інші вузли оператора для підтвердження створеного блоку. Вони запускають ітераційний процес, який вимагає схвалення від інших вузлів оператора, щоб блок був визнаний дійсним.

Процес шифрування, відомий як хешування, виконується різними комп'ютерами, що працюють в одній мережі. Якщо всі комп'ютери отримують однаковий результат обчислення, то блоку присвоюється унікальний цифровий підпис (підпис).

г) Прикріплення блоку до ланцюга. Він відбувається після схвалення всіх транзакцій у блоці. Після оновлення реєстру та створення нового блоку, цей блок стає незмінним і неможливим до підробки. Його можна тільки доповнювати новими записами. Важливо зауважити, що оновлення реєстру відбувається одночасно на всіх комп'ютерах мережі.

Основне завдання технології блокчейн полягає у вирішенні координації між учасниками системи, які спільно працюють для досягнення спільної мети, при цьому не довіряючи один одному.

Криптологи часто використовують приклад "завдання візантійських генералів", яке полягає в розробці єдиної стратегії дій для генералів, яка б забезпечила перемогу, навіть якщо деякі генерали є зрадниками та намагаються спотворити інформацію. Блокчейн досягає цього шляхом використання механізмів консенсусу.

Блокчейн володіє вражаючими можливостями, особливо у контексті систем, де немає взаємної довіри між сторонами. Він забезпечує надійність зберігання особистих даних, роблячи їх захищеними від несанкціонованих змін з метою шахрайства. Більше того, технологія блокчейна відкриває можливості для проведення різних транзакцій без потреби в посередниках, що призводить до вагомої економії коштів і часу. Це особливо релевантно для фінансових установ.

1.1.2 Передумови виникнення електронних грошей та їх інтерпретація

У середині 1980-х років, американець Девід Чаум вперше висунув ідею електронних грошей. Розвиток системи Чаума відіграв важливу роль у розвитку електронних грошей. Введення "сліпого цифрового (електронного) підпису" стало ключовим фактором, який забезпечив, анонімність фінансових операцій, а також захист від шахрайства [7]. Це дозволило поширитись першим електронним платіжним системам у країназ Заходу на початку 1990-х років, коли Інтернет набув популярності. Офіційне визнання електронних грошей банками ЄС відбулося у 1994 році. Пізніше, Європарламентом та Радою Європейського Союзу були прийняті Директиви 2000/46/ЄС та 2009/110/ЄС, які

регулюють угоди, пов'язані з електронними грошима. Крім того, існує ряд документів від міжнародних банківських установ, включаючи матеріали Банку міжнародних розрахунків та Європейського центрального банку (ЄЦБ), які охоплюють різні аспекти цього питання, такі як вимоги до емітентів електронних грошей, нагляд та захист від шахрайства.

Проте, в сучасній економічній науці ще не існує цілісної теорії електронних грошей. Серед економістів не спостерігається єдності у розумінні концепції електронних грошей, оцінки їх важливості для економіки суттєво розбігаються, а перспективи електронних грошей в майбутньому оцінюються по-різному. Термін "електронні гроші" має різні визначення, включаючи те, що міститься в Директиві 2009/110/ЄС, електронні гроші — це «грошова вартість, подана у вимоги до емітенту, що зберігається на електронному пристрої, зокрема магнітні, випускаються отримання коштів за платіжним операціям і приймаються фізичною або юридичною особою, відмінним від установи-емітента ЭГ». У закордонній економічній літературі поширені такі тлумачення цього поняття: 1) дематеріалізована/електронна форма банкноти, яка видається шляхом перетворення на електронну форму грошової вартості; 2) фінансовий продукт із передплаченою вартістю; 3) засіб обміну, який видається приватним емітентом і є обіцянкою емітента сплатити еквівалентну суму. [7].

Українське законодавство, зокрема Постанова № 481 Національного банку України "Положення про електронні гроші в Україні", надає таке визначення: "Одиниці вартості, які зберігаються на електронному пристрої, приймаються як засіб платежу особами, іншими, ніж особа, яка їх видала, і є грошовим зобов'язанням цієї особи, що виконується у готівковій або безготівковій формі" [11].

Ці визначення мають схожий сенс, що можна помітити при порівнянні з Директивою 2009/110/46.

З погляду Національного банку України (а також інших міжнародних банківських установ, наприклад, Європейського центрального банку), картки з електронним носієм, такі як передплачені телефонні, паливні, подарункові та

подібні, не вважаються електронними грошима, хоча формально вони відповідають вищезазначеним визначенням. Основна різниця полягає в тому, що платежі за передплаченою карткою не є готівкою, оскільки такі операції оплачуються один раз - при купівлі передплаченої картки; тоді як із електронними засобами кожна нова подія є новим платежем. Також не вважаються електронними грошима: 1) операції інтернет-банкінгу зі звичайними рахунками та коштами у звичайних державних валютах; регулярні грошові перекази через інтернет-портали; 2) пластикові банківські картки, що є сучасним засобом доступу до банківського аккаунта, у системах, які здійснюють платежі електронними засобами, банківські рахунки використовуються лише при введенні/виводі грошей із системи; карткові або поточні рахунки користувачів, а також консолідований рахунок емітента ЕГ; 3) віртуальні валюти, які задіяні у рамках окремих інтернет-порталів (це псевдо грошова форма приватного обміну, незалежно від способу купівлі та викупу) [11]. Таким чином, з юридичної точки зору електронні гроші - грошове зобов'язання емітента, який мусить обміняти ЕГ на паперові гроші на вимогу пред'явника; а з технічного погляду - електронний запис певної суми вартості, яка захищена відповідними криптографічними алгоритмами. В економічному плані електронні засоби не можна однозначно віднести до готівкових чи безготівкових грошей — це скоріше якась третя форма грошей. Однак через малу поширеність і відносну новизну електронних грошей вони мають внутрішню суперечність - з одного боку, є платіжним засобом, з іншого - зобов'язання емітента, що підлягає виконанню в традиційних неелектронних грошах. Цей парадокс можна пояснити історичною аналогією: колись банкноти теж виглядали як зобов'язання, що підлягає відплаті дорогоцінними металами або монетами, а зараз прямого зв'язку між банкнотами та дорогоцінними металами немає.

В майбутньому очікується, що електронні гроші будуть використовуватися поряд з готівкою та безготівковими грошима. Вони можуть стати провідною формою грошей за умови вирішення багатьох проблем, пов'язаних з їх використанням [7]. Проте більш ймовірний сценарій, за якого ЕГ займуть свою

нішу на ринку, а саме сферу мікроплатежів (мобільних та не тільки платежів, які зазвичай не перевищують $20), де використання готівкових та безготівкових платежів обмежене. економічно недоцільно.

Існують дві основні категорії електронних грошей: карткові та мережеві. Карткові гроші базуються на використанні смарт-карт - багатофункціональних пластикових карток з вбудованими мікропроцесорами. На цих чіпах зберігається грошовий файл, який є еквівалентом переданих заздалегідь грошей емітенту карток. Карткові гроші не такі зручні у порівнянні з мережею, тому що вимагають спеціального обладнання – картридерів.

Друга група електронних грошей включає мережеві гроші, також відомі як гроші на програмній основі. Вони представлені у вигляді грошового файлу, що виділяється організатором розрахунків при отриманні традиційних грошей. Ці гроші зберігаються на жорстких дисках персональних комп'ютерів або інших знімних носіях і передаються під час здійснення платежів через електронні канали зв'язку, зокрема через Інтернет. Мережеві гроші використовуються для оплати товарів і послуг в інтернет-магазинах та можуть бути обмінені на традиційні гроші. За своєю природою цей вид електронних грошей ближче до безготівкових банківських грошей [11].

Операції з електронними грошима здійснюються через електронні платіжні системи (ЕПС), які призначені для здійснення платіжних операцій в мережі Інтернет. Для здійснення операцій з електронними грошима, включаючи рахунки на інтернет-порталах, використовуються електронні гаманці - конкретні програми та пристрої. Найбільш відомими електронними платіжними системами у світі є WebMoney, E-Gold та PayPal, який є найпоширенішим способом оплати в Інтернеті. В даний час більш як 230 мільйонів людей у 190 країнах використовують PayPal [12].

1.1.3 Смарт-контракти

Смарт-контракти – основа роботи з блокчейном. Смарт-контракти - це комп'ютерні програми, які запускаються на блокчейні і виконують угоди

автоматично та безпосередньо залежно від заданих умов. Вони є віртуальними контрактами, які забезпечують довіру та незмінність виконання угод між сторонами без посередництва. Вони автоматизують виконання угод, що дозволяє ефективно та швидко виконувати умови контракту без необхідності додаткових дій від сторін. Вони виконуються автоматично та безперервно, коли задані умови стають справжніми.

Смарт-контракти самостійно виконуються без необхідності довіри до третіх сторін. Вони засновані на програмованій логіці, яка гарантує, що угоди будуть виконані у відповідності до заданих правил та умов. Також вони забезпечують високий рівень безпеки завдяки використанню криптографічних методів та блокчейн технології. Інформація, що зберігається в смарт-контрактах, є захищеною та незмінною, завдяки розподіленому реєстру, який перевіряє та фіксує кожну транзакцію.

Блокчейн технологія, на якій ґрунтуються смарт-контракти, забезпечує високий рівень прозорості. Усі угоди та транзакції, що здійснюються за допомогою смарт-контрактів, є публічними та доступними для перегляду всіма учасниками мережі.

Смарт-контракти, які зберігаються в блокчейні, є незмінними. Після створення та розгортання їхній вміст не може бути змінений без погодження всіма сторонами, що гарантує надійність та невідворотність виконання угод.

Смарт-контракти працюють в децентралізованому середовищі, де керування та контроль здійснюються не однією центральною організацією, а всіма вузлами мережі. Це забезпечує рівновагу влади та запобігає одній стороні контролювати угоди.

Смарт-контракти не обмежені географічними межами або традиційними бюрократичними процесами. Вони можуть бути виконані та використані будь-де в світі, забезпечуючи глобальну доступність та використання.

Смарт-контракти дозволяють сторонам виконувати угоди без необхідності повної взаємної довіри. Вони доводяться до виконання на основі заданих умов та програмованої логіки, що забезпечує надійність та об'єктивність [4].

Рисунок 1.1 – Візуалізація смарт-контракту

1.1.4 Приклади застосування смарт-контрактів

Виведення коштів з крипто-гаманця може бути складним та потенційно небезпечним процесом. Смарт-контракти надають ефективний та безпечний спосіб автоматизувати цей процес, забезпечуючи точність та надійність транзакцій.

Смарт-контракти виконують перевірку балансу крипто-гаманця для визначення наявності достатньої суми для виводу коштів. Вони перевіряють, чи є достатньо коштів на балансі гаманця, щоб покрити запит на виведення.

Також вони можуть перевіряти автентичність виводу коштів шляхом перевірки підпису транзакції. Що забезпечує, що тільки власник крипто-гаманця може ініціювати вивід коштів.

Після підтвердження балансу та автентичності смарт-контракти виконують транзакцію виводу коштів. Вони автоматично ініціюють переказ від крипто-гаманця до вказаного отримувача або адреси.

Смарт-контракти можуть включати механізми для відстеження статусу транзакції. Вони можуть надати інформацію про підтвердження та підтверджену кількість блоків, що підтвердили транзакцію.

Смарт-контракти можуть включати автоматичні перевірки, щоб уникнути шахрайства та помилок. Наприклад, вони можуть перевіряти достатність коштів, валідність адреси отримувача та інші умови перед виведенням коштів.

Смарт-контракти використовують криптографічні методи для забезпечення безпеки та захисту від несанкціонованого доступу до коштів. Вони шифрують дані та використовують підписи для підтвердження автентичності транзакцій.

Смарт-контракти можуть бути використані для автоматичного виводу коштів з криптобіржі після виконання певних умов, таких як досягнення певного балансу або підтвердження транзакцій.

Тобто шляхів застосування смарт-контрактів дуже багато, в нашому застосунку, на даному етапі буде імплементовано лише один – «Підтвердження балансу, автентичності та виводу коштів».

1.1.5 Блокчейн Ethereum

Ethereum є одним з найпопулярніших та найвідоміших блокчейнів, який був запущений в 2015 році. Він створений для підтримки смарт-контрактів, що є програмами, які автоматично виконують умови, записані в них. Ethereum використовує свій власний криптовалютний токен під назвою Ether (ETH), який використовується для оплати виконання смарт-контрактів та виконання транзакцій на мережі.

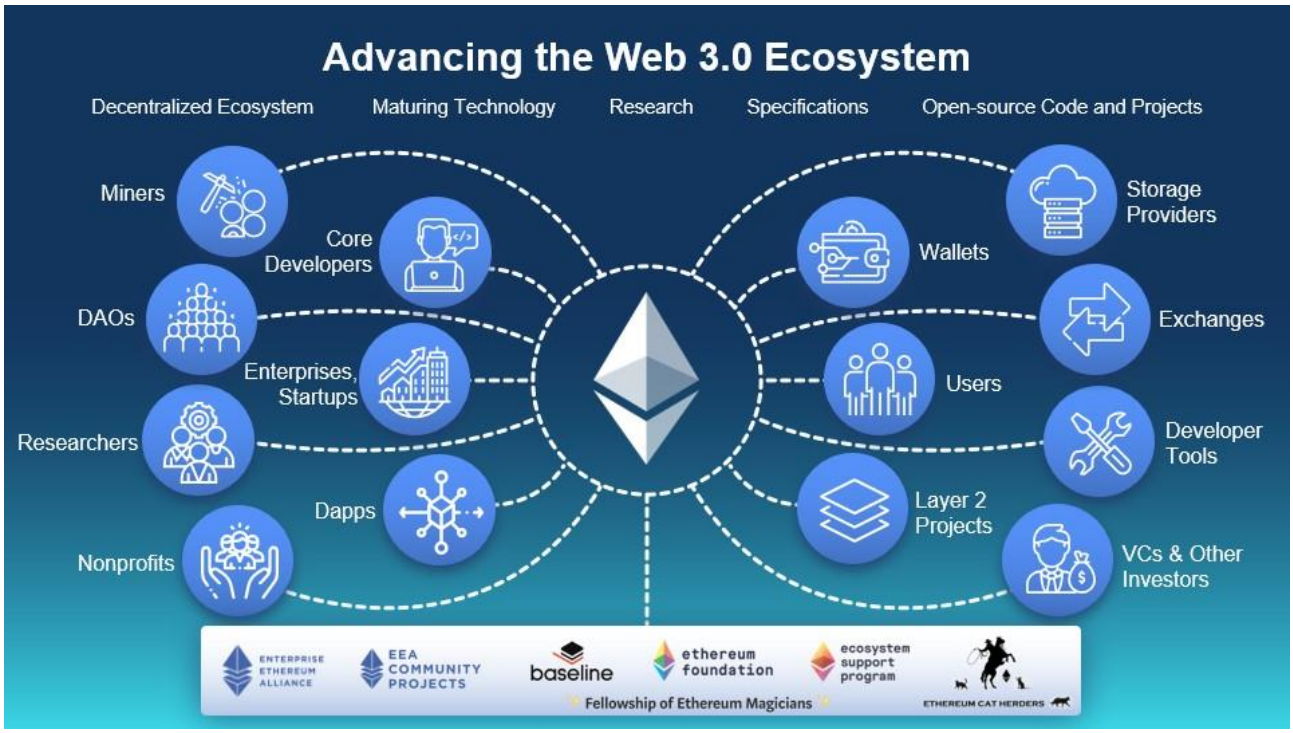


Рисунок 1.2 – Екосистема блокчейну Ethereum

Одним з основних елементів Ethereum є його віртуальна машина Ethereum (EVM). EVM є середовищем виконання смарт-контрактів, де вони можуть бути створені, виконані та взаємодіяти між собою. EVM використовує мову програмування Solidity, спеціально розроблену для створення смарт-контрактів на Ethereum. Завдяки гнучкості та потужній функціональності Ethereum і EVM стали важливими факторами в розвитку децентралізованих додатків (DApps) та екосистеми DeFi (децентралізовані фінанси).

Існує також багато інших блокчейнів, які відводяться від Ethereum і базуються на його технології. Ці блокчейни відомі як форки Ethereum або альтернативні блокчейни. Два найвідоміших приклади цього – ETC і BSC.

ETC виник після того, як в 2016 році відбувся хардфорк Ethereum, пов'язаний зі зламом розумного контракту на платформі The DAO. Після хардфорка було створено новий ланцюжок блоків Ethereum, а оригінальний ланцюжок став відомим як Ethereum Classic.

Ethereum Classic зберігає оригінальну версію Ethereum і не має змін, які були зроблені після хардфорка.

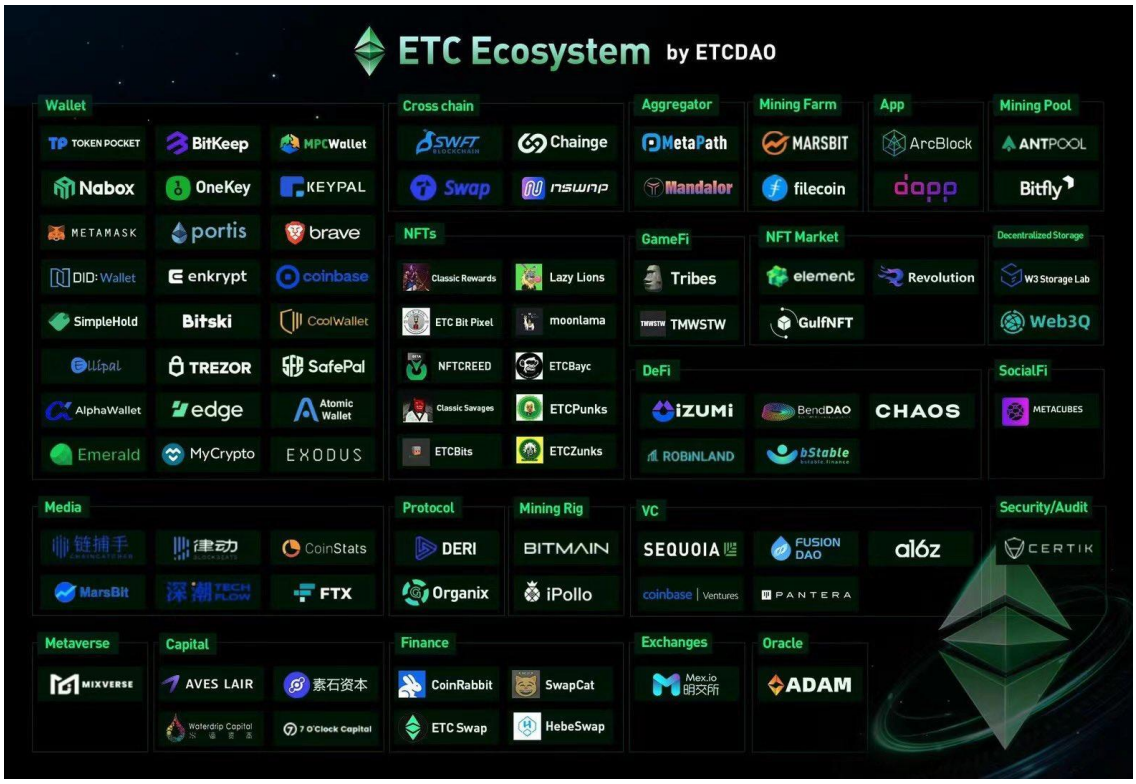


Рисунок 1.3 – Екосистема блокчейну ETC

Загалом, Ethereum відіграв важливу роль у розвитку блокчейн-технологій та забезпеченні інфраструктури для смарт-контрактів та децентралізованих додатків. Його відкритість та гнучкість сприяли розвитку широкої спільноти розробників та інновацій у галузі блокчейну.

Більшість користувацьких блокчейнів створюються на основі Etherum'а, адже він має великий обсяг детальної та зрозумілої документації, величезний спектр різних сфер та приймів застосування, а також глобальне ком'юніті. [3]

1.2 Огляд наявних мобільних додатків для обміну криптовалюти з використанням технології блокчейн

Fondy – застосунок, що підтримує 3D Secure платежі.

Протоколи безпеки платіжних систем Visa і Mastercard захищають бізнес від необґрунтованих претензій власників карток. Таким чином, оплата з введенням 3D Secure ототожнюється з операцією з введення PIN-коду і не може бути оскаржена, якщо послуги були надані платнику в повному обсязі. Крім того, платіжні системи суворо регламентують передачу відповідальності за

шахрайські платежі від продавця до банку-емітента, якщо продавець підтримує протокол 3D Secure, а емітент або конкретна карта-емітент ні.

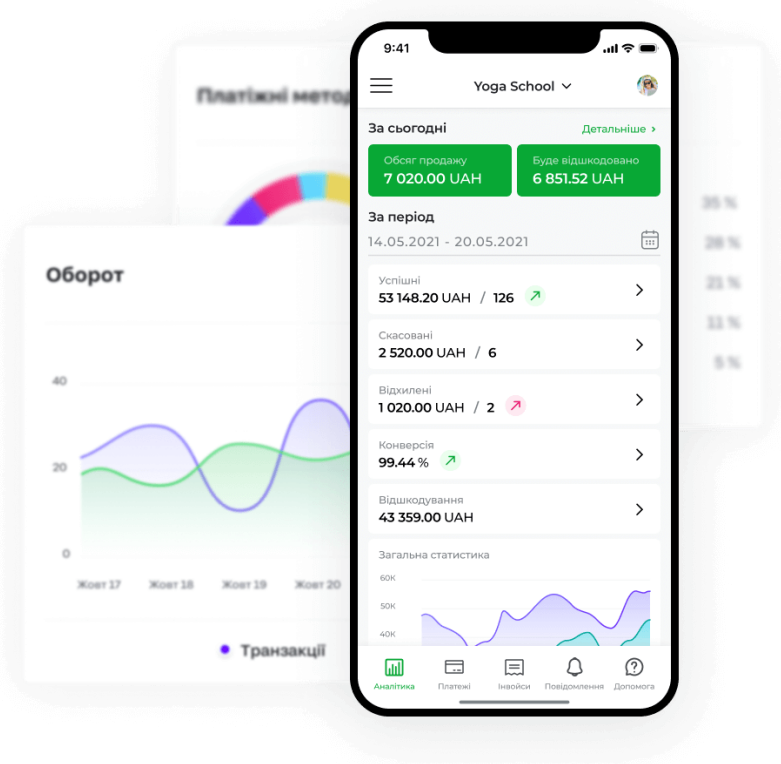


Рисунок 1.4 – Fondy

Fondy також піклується про всю претензійну роботу та пов’язані з нею бюрократичні процеси, звільняючи підприємців від втрати часу та ресурсів.

Інша програма Venmo використовується для дослідження безпеки. У своєму дослідженні вони шукали технічні та соціальні вразливості та виявили кілька проблем у додатку. Вони також дали декілька пропозицій команді Venmo щодо покращення їхньої програми.

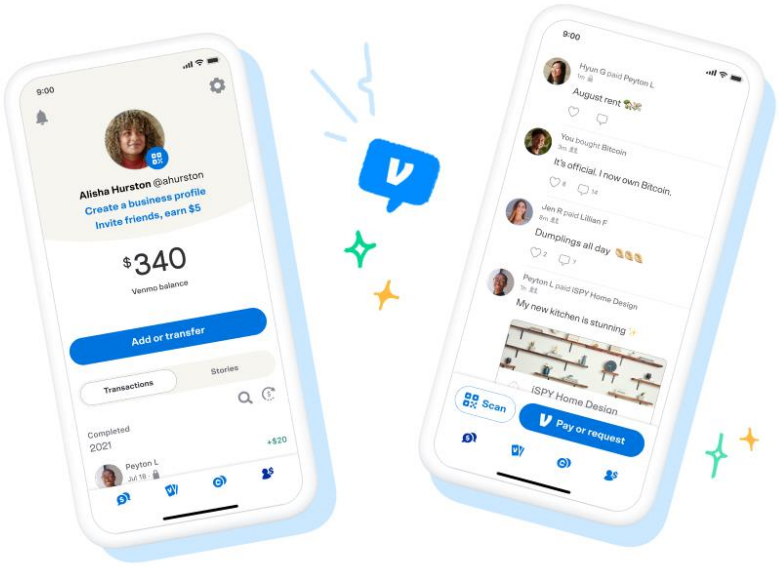


Рисунок 1.5 – Venmo

Дослідницька група завантажила APK-файл версії Venmo для Android, потім використала утиліту dex2jar для декомпіляції файлу та спробувала з'ясувати, як працює програма. Вони також переглянули веб-додаток платіжної системи Venmo і знайшли приватну кінцеву точку API, яка надає деякі виклики API, які не є публічними документами. Ці API використовуються як веб-додатком, так і додатком Android. Перевіривши API та весь процес щодо того, як працюють офіційні програми Venmo, включно з програмою Android та відповідним веб-додатком, вони виявили кілька проблем із безпекою.

Для виявлених проблем безпеки дослідницька група запропонувала свої рішення, включаючи збільшення довжини та встановлення обмежень швидкості для текстового повідомлення авторизації, виправлення відомих помилок безпеки шляхом дотримання політики безпеки в усій системі та випадкового розкриття секретних значень, а також покращення веб-сайту. дизайн, який дозволяє користувачам легше ідентифікувати інших користувачів. Для цільової програми Square Cash є деякі огляди та коментарі, але звіт про аналіз громадської безпеки недоступний.

На Investing.com (рисунок 1.6) можна побачити котирування близько 100 тисяч фінансових інструментів на 70 біржах з усього світу.

Ці інструменти включають акції, облігації, товари, ф'ючерси та опціони. Ви можете створити свій інвестиційний портфель та синхронізувати його із сервісом. Оповіщення, що настроюються, гарантують, що ви ніколи не пропустите важливу подію під час торгівлі.

Технічний аналіз доступний з графіками та рекомендаціями щодо купівлі або продажу. Крім традиційних інструментів, Investing.com також пропонує інформацію про криптовалюти: Bitcoin, Ethereum, Ripple, Litecoin та інші. Усього підтримується понад 20 криптовалют.

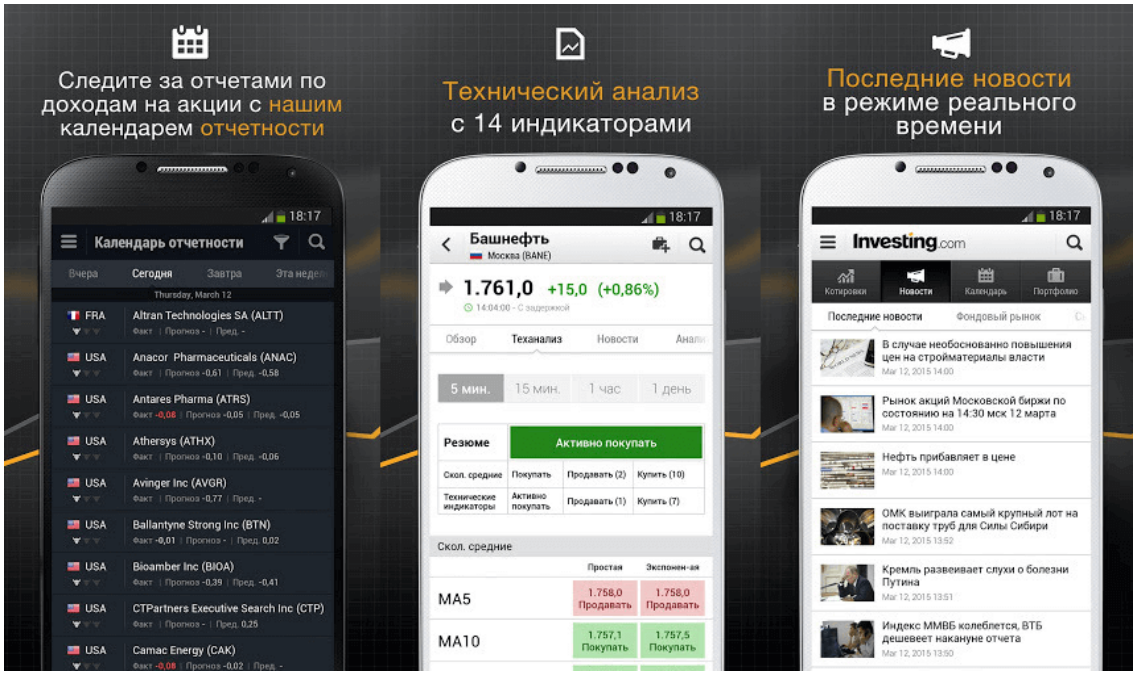


Рисунок 1.6 – Investing.com

Robinhood (рисунок 1.7) – дозволяє торгувати онлайн на великих біржах без комісій. Автори програми вирішили, що технології повинні допомагати займатися брокерською діяльністю з мінімальними накладними витратами. Просто завантажте програму, підключіться до свого банку, поповніть свій рахунок, і все готове.

Для відкриття рахунку Robinhood потрібен мінімальний баланс у розмірі 2000 доларів США. Це нормативна вимога. Ви також можете заробити до 500 доларів, запросивши друзів до Robinhood.

Також Robinhood пропонує заробляти на криптовалютах без будь-яких комісій. Для цього вам знадобиться обліковий запис Robinhood Crypto. Мінімальна сума для покупки становить 0,10 долара США для біткойнів та 0,01 долара США для Ethereum.

Незважаючи на простоту, програма використовує той же сучасний механізм захисту, що і традиційні фінансові установи. Компанія-розробник є членом FINRA та SIPC. В даний час програма доступна лише для жителів США, але розробники оголосили плани розширення.

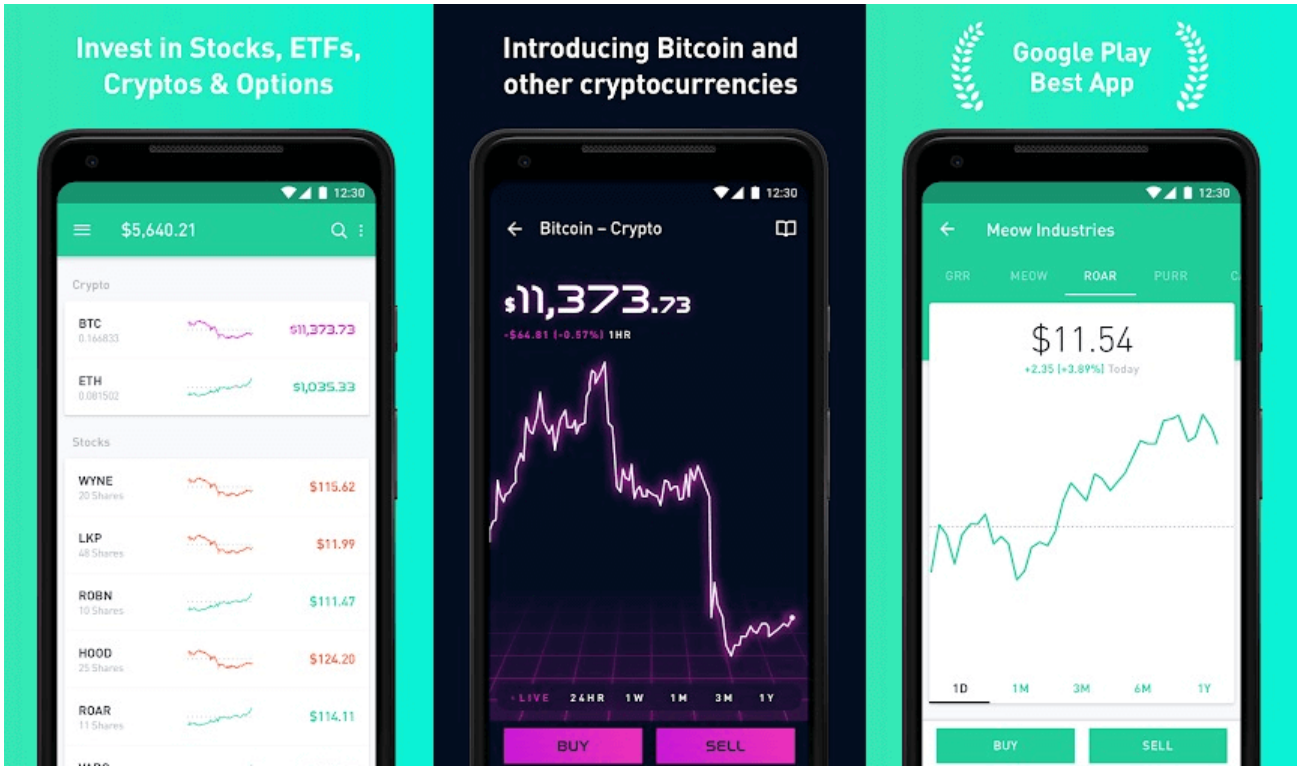


Рисунок 1.7 – Robinhood

Webull (рисунок 1.8) — глобальний постачальник торгових даних та розробник однієї з найкращих програм. Ця програма допоможе вам відслідковувати зміни на фондовому ринку, вивчати фондові індекси, котирування акцій та Forex.

В окремій вкладці можна прочитати поточні новини. Доступна синхронізація з обліковим записом Google Finance. Це допоможе вам краще

контролювати свій інвестиційний портфель. Доступно 22 технічні індикатори (наприклад, MA, EMA, BOLL, MACD, KDJ).

В даний час торгівля акціями на платформі доступна лише громадянам США. Сервіс можна використовувати для отримання повідомлень про зміну ціни на вказане значення. Існують віджети, що настроюються, які можна розмістити на екрані смартфона. Вам навіть не доведеться запускати програму, щоб переглянути котирування потрібної компанії.

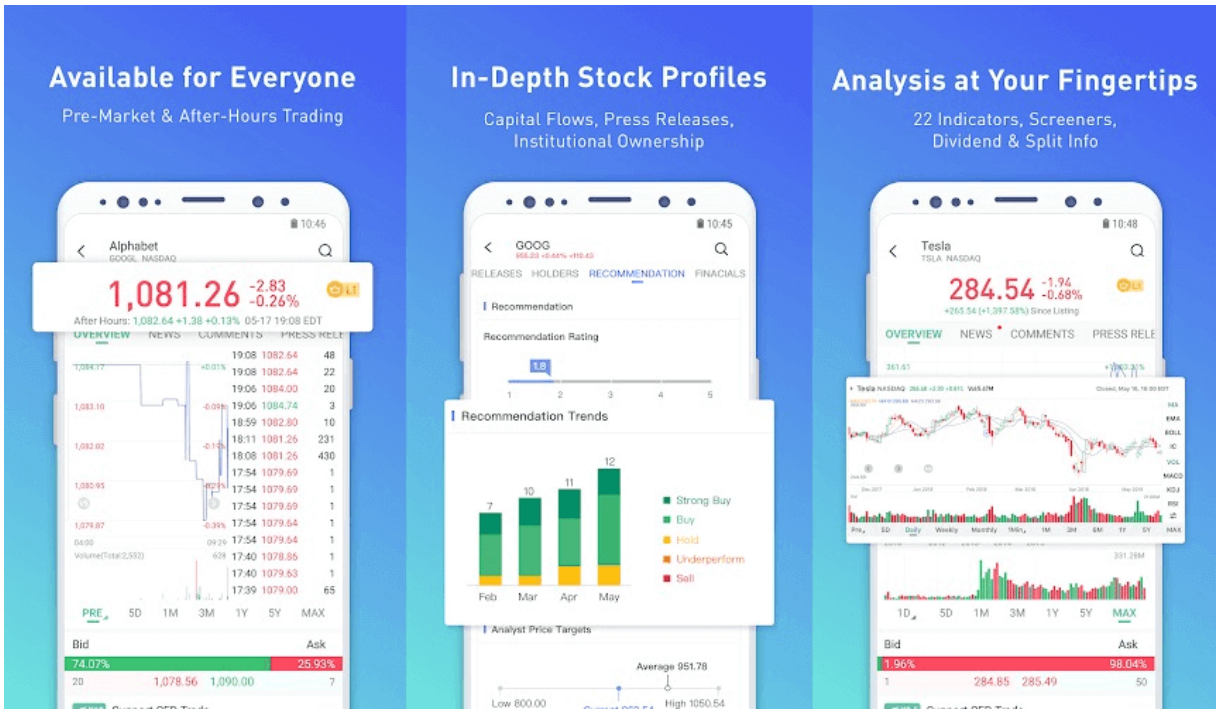


Рисунок 1.8 - Webull

1.3 Опис технічного завдання

Розробити онлайн біржу для покупки та продажу криптовалют. Програма має бути адаптивною та кросплатформовою. В програмі має показуватись ціна криптовалюти та відображатись зміни цін на графіках.

Програмною реалізацією буде система, яка матиме повний функціонал для купівлі, продажу та обміну криптовалют. Програма повинна бути підтримувана на всіх Android пристроях, надійною, бути простою у користуванні та ефективно виконувати свої запропоновані функції, а саме:

– збір інформації про всі торгові пари на біржі;

– аналіз кожної валютної пари на предмет курсової вартості та наявності ордерів на купівлю чи продаж;

– створення ордерів на купівлю чи продаж криптовалют;

– візуалізація поточної ситуації на ринку (курс, обсяги торгів);

Проаналізувавши сферу торгівлі криптовалютами та наявні аналоги програмного забезпечення прогнозування курсу криптовалюти, можна визначити наступні функціональні вимоги до дипломного проекту, що розробляється:

1. система повинна надавати можливість обміну (купівлі або продажу) біткойну або інших криптовалют.

2. система збирає поточну ціну криптовалют Bitcoin, Ethereum і Ripple.

3. програмна система повинна візуалізувати аналізи та прогнози, виконані за допомогою графіків, діаграм і таблиць, що показують результати основних алгоритмів.

4. система повинна дозволяти адміністраторам реєструвати уповноважених осіб, які можуть вручну редагувати тон тексту.

На основі наведених вище функціональних вимог визначаються нефункціональні вимоги системи розробки:

1) Веб-дизайн повинен коректно відображатися у веб-браузерах Google Chrome, Mozilla Firefox, Safari, Microsoft Edge.

2) Веб-дизайн повинен правильно відображатися як на мобільних, так і на настільних комп’ютерах.

3) Ролі користувача, довіреної особи та системного адміністратора повинні бути реалізовані в розробленій веб-програмі.

4) Система повинна бути готова до розширення обсягів криптовалют і ICO монет, їх курси повинні бути прогнозованими.

5) Візуалізація результатів системи та інтерфейс користувача мають бути легкими для розуміння.

Варто зазначити, що обмінні операції та спекуляції на біржах криптовалют такі самі, як і на інших біржових системах. Для отримання прибутку необхідно купити валюту дешевше за курсом, а через певний проміжок часу здійснити продаж дорожче за ціну покупки.

Отримати прибуток, торгуючи електроними грошима, не становитиме проблеми для тих, хто знає основи торгівлі на ринку акцій або вже власне криптовалют. Саме такі знання повинні бути закладені в алгоритмі, який буде описаний далі.

Далі програмна реалізація носить назву “Cryptowallet”, у поточній роботі буде представлена версія 1.0.1. Мажорну версію системи буде оголошено після ретельного подальшого тестування та подальшого доопрацювання функціоналу програми.

1.4 Ознайомлення з середовищами для розробки застосунку

Android займає 86% світового ринку. Прогнозується, що приблизно такий саме рівень збережеться і в майбутньому. Хоча застосунки для iOS дозволяють охопити аудиторію з більшою купівельною спроможністю, ніж користувачі Android (рисунок 1.9).

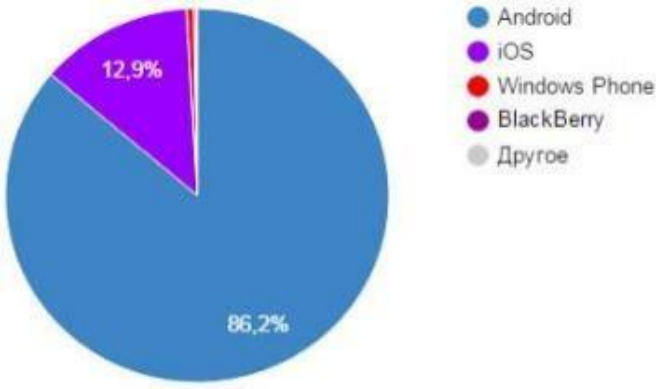


Рисунок 1.9 – Ринок мобільних операційних систем

Хоча Android є лідером за кількістю користувачів, у деяких частинах світу Apple досі домінує на ринку. Це країни з вищим рівнем життя в Північній

Америці, Південній Америці, Європі та Азії. Android лідирує в країнах, що розвиваються (рисунок 1.10).

Рисунок 1.10 – Карта користувачів за регіонами

Розробка iOS є швидшою та дешевшою з точки зору фрагментації. Android має багато версій і багато пристроїв. Це ускладнює розробку та тестування програм, що призводить до витрат часу та грошей. Тільки Apple використовує ОС iOS, а кількість смартфонів і планшетів обмежена.

Apple отримує на 45% більше доходу від користувача, ніж Android. Крім того, користувачі iOS на 10% частіше роблять покупки в програмі, ніж користувачі Android.

Застосунки для iPhone мають високу якість і привабливий дизайн. Багато успішних людей обирають iOS, оскільки вона пропонує простий і зручний у використанні інтерфейс, який економить час користувачів. Операційна система iOS також вважається безпечнішою в порівнянні з Android, завдяки строгій перевірці магазину застосунків App Store. Це запобігає завантаженню вірусів та забезпечує додатковий захист користувачів. У порівнянні з Google Play, де можна знайти різноманітні застосунки, включаючи різний спам, App Store заздалегідь перевіряє всі нові завантаження. Це свідчить про високу якість та стандарти контролю якості продуктів [8].

На початковому етапі розробки мобільного застосунку було вирішено, що проект буде орієнтований на одну з найпопулярніших та широко використовуваних операційних систем для мобільних пристроїв - Android. Ця операційна система має безліч переваг перед своїми конкурентами, такими як iOS, Microsoft і BlackBerry. Деякі з найбільших переваг:

1. Операційна система Android є найпопулярнішою операційною системою у світі (рисунок 1.11)

2. Android є open-source операційною системою

3. ПЗ для розробки мобільних застосунків безкоштовне і доступне для всіх операційних систем

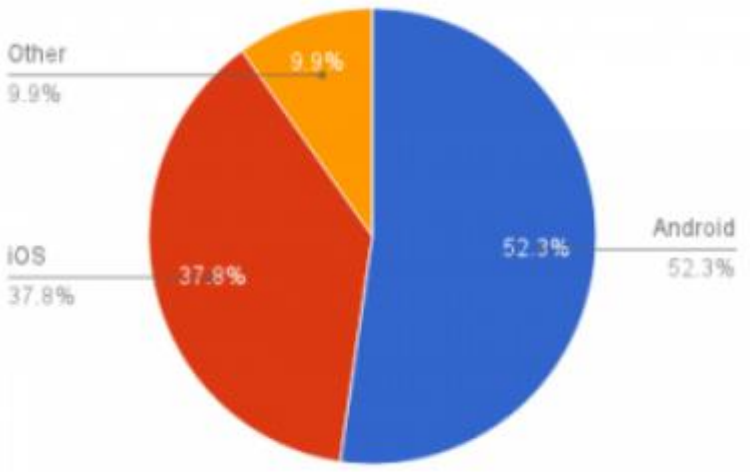


Рисунок 1.11 – Частка пристроїв на різних ОС для мобільних пристроїв

Android Studio. Один з найважливіших аспектів у розробці будь-якої програми - це вибір інтегрованого середовища розробки (IDE). Для створення додатків на платформі Android існує кілька варіантів, таких як Eclipse, NetBeans та Android Studio. В даному випадку було вибрано Android Studio, яка з 2013 року доступна безкоштовно (рис. 1.12). Android Studio є універсальною IDE від Google, бо вона допомагає створювати та тестувати програми для різних пристроїв, таких як смартфони, планшети, ноутбуки і годинники з операційною системою Android. Ця IDE дійсно зручна з кількох причин:

1. Зручний редактор коду, який допомагає кодувати та пропонує такі функції як: доповнення, рефакторинг та аналіз коду

2. Наявність великої колекції готових шаблонів розробки ПЗ і бібліотек компонентів

3. Можливість виконання попередніх перевірок ПЗ на помилки

4. Вбудований емулятор Android (рис. 1.13)

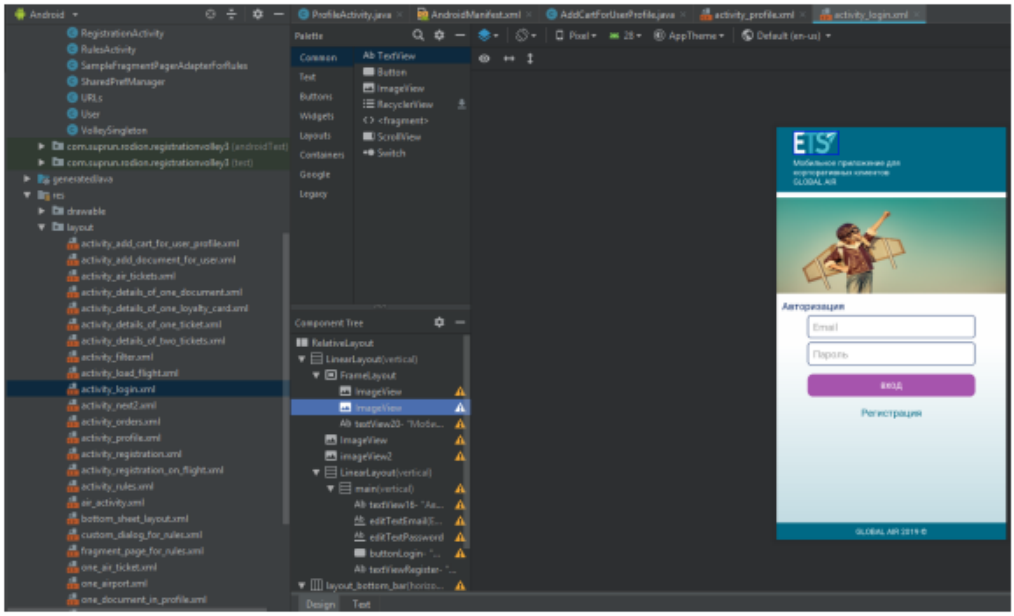


Рисунок 1.12 – Android studio

Емулятор Android є віртуальним пристроєм, який може імітувати роботу будь-якого пристрою на платформі Android.

Він використовується як цільова платформа для тестування мобільних додатків. Унікальна функція емулятора полягає у можливості перегляду показників продуктивності під час запуску застосунку. (рис. 1.14).

Рисунок 1.13 – Емулятор у Android Studio

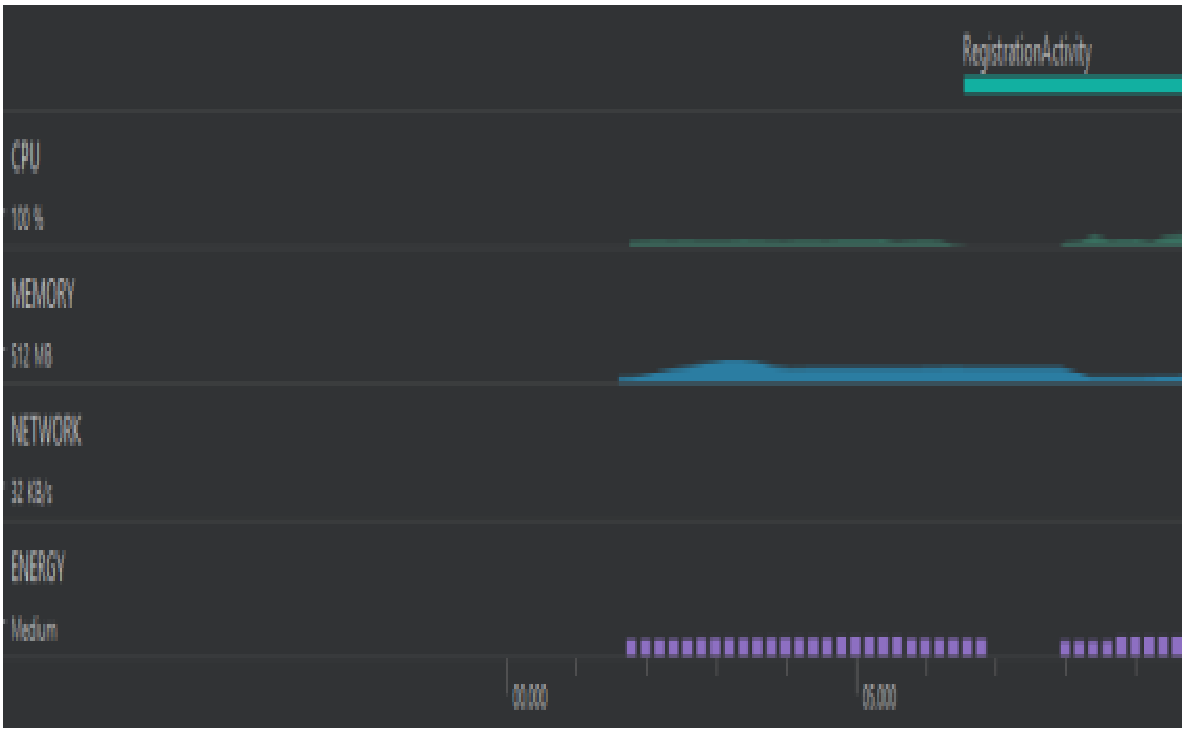


Рисунок 1.14 – Показники продуктивності в Android Studio

Мова програмування, яка використовується для розробки мобільних додатків у середовищі розробки Android Studio, називається Java. Вибір мови Java має декілька переваг:

1. Java є однією з найпоширеніших і популярних мов програмування в світі

2. Ця мова програмування є строго типізованою та об'єктно-орієнтованою, що сприяє простоті розробки та високій продуктивності.

3. Безпека. Java є однією з найбезпечніших мов програмування насьогодні.

Також частина застосунків робиться за допомогою мови Kotlin, яка теж доволі популярна для написання застосунків під Android, детальне порівняння можна побачити на рисунку 1.15. До найбільших переваг мови Java можна віднести більшу стабільність та технічну підтримку, більшу популярність(а отже більше ком’юніті та більше посібників і порад) та легкість в опануванні.

Parameter	Java	Kotlin
Static memebers	Almost the same. Thinking of the solution is the most time-consuming part	Almost the same. Thinking of the solution is the most time-consuming part
Perfomance	Almost the same. Both compile to ByteCode	Almost the same. Both compile to ByteCode
Stability	Has stable versions with long-term maintenance	Almost the same. Both compile to ByteCode
Documentation	Good, easy to find	Good, a little bit harder to find
Popularity	Extremely popular worldwide	Not so popular worldwide
Community	Mostly Indian, very broad	Mostly Russian, comparatively little
Talent pool	Not in the top-list	In the list of the most popular technologies 2020 according to StackOverflow Dev Survey
Easiness to learn	Easy to learn	Can be tricky to learn if you are not a good abstract thinker

Рисунок 1.15 – Порівняння мов Java та Kotlin в мобільній розробці

Висновки до розділу 1

В першому розділі розповідається про теоретичні аспекти відслідковування шахрайських платежів в блокчейні. Також розповідається про класифікацію систем електронних грошей, про їх переваги та недоліки. Ведеться огляд наявних застосунків для відстеження шахрайських платежів.

Процес формування блоку складається з кількох основних етапів.

а) Початковий крок - визначення транзакції. Відправник створює транзакцію, яка включає адресу одержувача, деталі транзакції (суму грошей, товари та їх кількість тощо) та криптографічний цифровий підпис для підтвердження її ідентичності та легітимності. Вузли мережі отримують повідомлення про транзакцію та перевіряють її правомірність, шляхом розшифровки цифрового підпису. Якщо транзакція успішно проходить перевірку, вона очікує на включення до блоку.

б) Блоки, що містять інформацію про транзакції, з'єднані в "ланцюг" за допомогою складних математичних алгоритмів, які забезпечують криптографічну та хронологічну стабільність.

Нові блоки завжди додаються лише в кінець ланцюга і ніяк інакше.

Один з вузлів мережі періодично збирає незавершені транзакції, формує з них блок і відправляє його на підтвердження іншим учасникам мережі для перевірки та додавання до ланцюга.

2 ОПИС ПРОГРАМНОГО ЗАСТОСУНКУ

2.1 Класифікація систем обміну криптовалют

В Україні на сьогоднішній день представлені різноманітні світові електронні гроші та системи електронних платежів. Кожна компанія старається знайти найефективніший спосіб проведення електронних транзакцій, багато з яких мають патентовані технології. Сучасні електронні гроші можуть існувати у двох основних формах: через мережі або на основі смарт-карт. Вони, подібно до паперових грошей, поділяються на фідуціарні (фіатні) та безфідуціарні. Фідуціарні гроші є варіантом грошей, що належать певній платіжній системі, і представляють собою одну з національних валют. "Оскільки держава зобов'язує громадян приймати фіатні гроші за плату, їх емісія, викуп та обіг відбуваються згідно з чинним законодавством та регулюються центральним банком". Нефіатні гроші є одиницею вартості недержавних платіжних систем. Ці електронні гроші представляють собою форму кредитних фінансових ресурсів та регулюються правилами недержавних платіжних систем [11].

Webmoney Transfer - платіжна система, що з'явилася 25 листопада 1998 - найпоширеніша і надійна електронна платіжна система для фінансових операцій в режимі реального часу, створена для користувачів всесвітньої павутини. Будь-хто може стати користувачем системи. Платіжним засобом у системі є титульні знаки, які називаються WebMoney, або скорочено WM. Усі WM зберігаються у про електронних гаманцях. Найбільш поширені гаманці чотирьох типів:

- WMZ - доларові гаманці;
- WME – гаманці для зберігання євро;
- WMU – гаманці для зберігання української гривні

PayCash – це електронна платіжна система. Він розпочав свою роботу на початку 1998 року і позиціонується, перш за все, як доступний засіб швидких, ефективних та безпечних грошових розрахунків у мережі Інтернет.

Головною перевагою даної платіжної системи є використання власних унікальних розробок у сфері фінансової криптографії високо оцінених західними

експертами. Платіжна система PayCash має низку престижних нагород та патентів, серед яких «Сертифікат особливого визнання Конгресу США». На даний момент технологію PayCash використовують такі відомі платіжні системи як Cyphermint PayCash (США), DramCash (Вірменія), PayCash (Україна).

PayCash базується на технології цифрових грошей. З погляду користувача (продавця або покупця) технологія PayCash є набір «електронних гаманців», у кожного з яких є свій власник. Усі гаманці підключені до єдиного процесингового центру, який обробляє інформацію, отриману від власників. Завдяки сучасним технологіям, користувачі можуть здійснювати операції зі своїми грошима, не відходячи від комп'ютера. Технологія дозволяє переводити цифрову готівку з одного гаманця на інший, зберігати її в інтернет-банку, конвертувати, виводити із системи на традиційні банківські рахунки або інші платіжні системи.

Поширення електронних грошей обумовлено економічними факторами, у тому числі дешевизною їх обігу, та низкою неекономічних факторів, у тому числі зручністю для споживача під час здійснення платежів.

У цілому нині більшість сучасних дослідників вважають, що еквіваленти коштів є короткострокові високоліквідні фінансові вкладення, вільно конвертовані у певні суми коштів і які характеризуються невеликим ризиком зміни їх вартості.

З бухгалтерського погляду електронні гроші є новий об'єкт вивчення. Для подальшого вивчення методологічних та організаційних проблем їх обліку доцільно розглянути їхню класифікацію.

Класифікація є допоміжним інструментом для вирішення подальших досліджень актуальних проблем обліку електронних грошей [6].

Класифікація електронних грошей представлена на рисунку 2.1.

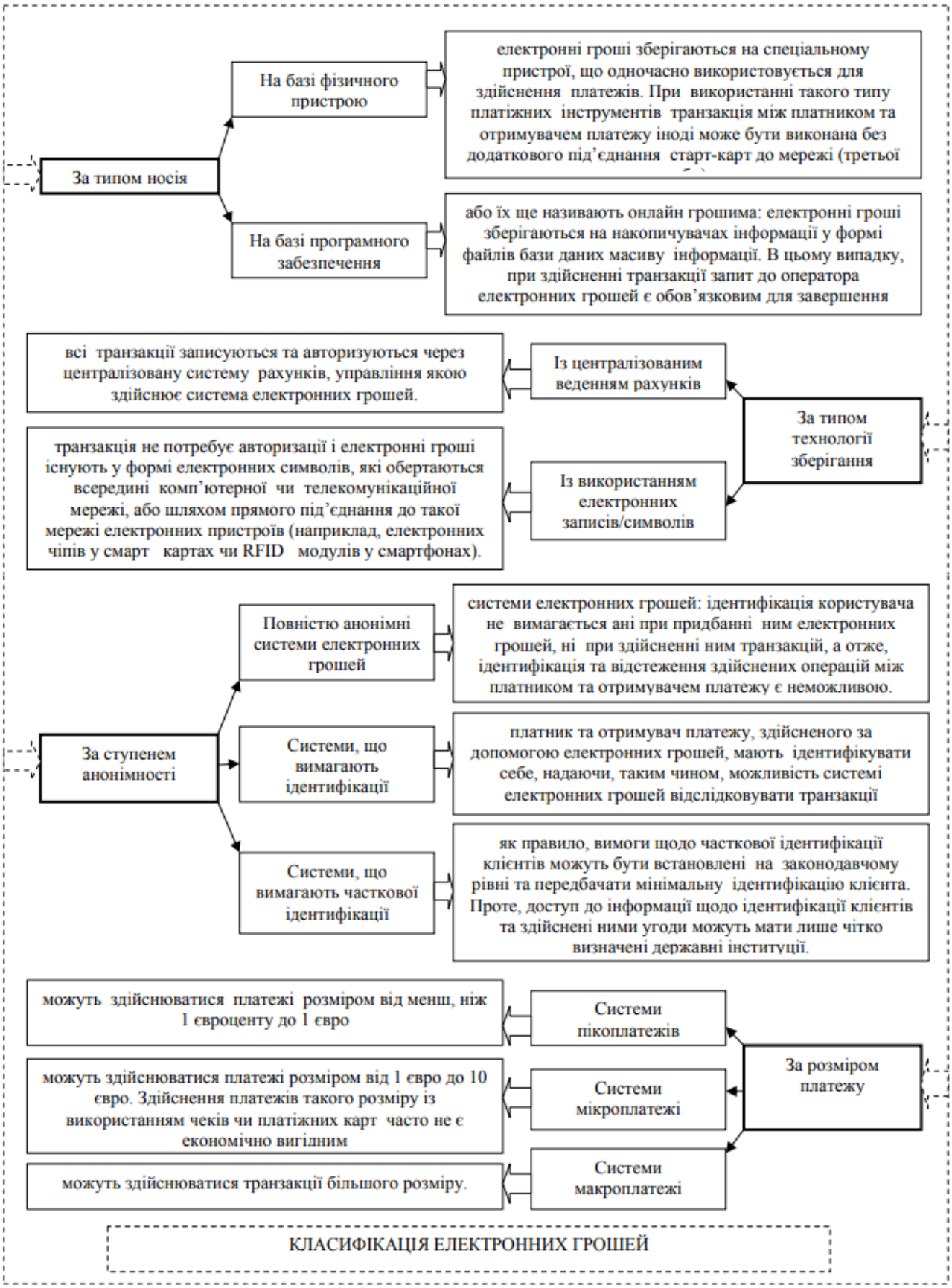


Рисунок 2.1 – Класифікація електронних грошей

2.2 Переваги та недоліки криптовалюти

Електронні гроші (криптовалюти) найправильніше порівнювати з готівкою, тому що обіг безготівкових грошей обов'язково персоніфікований і відомі реквізити обох сторін. У разі платежів електронними грошима достатньо знати реквізити отримувача грошей.

Криптовалюти мають такі переваги перед готівкою:

– відмінна подільність та інтегрованість – при оплаті немає потреби у здачі;

– висока переносимість – величина суми не пов'язана з габаритними чи ваговими розмірами грошей, як у випадку з готівкою;

– дуже низька вартість випуску електронних грошей – не потрібно карбувати монети та друкувати банкноти, використовувати метали, папір, фарби тощо;

– немає потреби фізично перераховувати гроші, ця функція переноситься на накопичувач або платіжний засіб;

– простіше, ніж у разі готівки, організувати фізичний захист електронних грошей;

– момент оплати фіксується електронними системами, знижується вплив людського фактора;

– при оплаті мерчантові неможливо приховати кошти від оподаткування;

– простота використання – стати власником електронного гаманця може кожен, оскільки його створення не викликає жодних труднощів, а робота з рахунками спрощена.

– криптовалюти не потрібно перераховувати, упаковувати, перевозити та складати у спеціальні сховища;

– ідеальна живучість – криптовалюти з часом не втрачають своїх якостей;

– досконала якісна однорідність — окремі екземпляри криптовалюти не мають унікальних властивостей (наприклад, подряпини на монетах);

– безпека — захист від крадіжки, підробки, зміни номіналу тощо забезпечується криптографічними та електронними засобами.

Проте на сьогоднішній день система не позбавлена низки недоліків:

– існує відсутність належного правового регулювання також призводить до незахищеності користувачів з точки зору можливості витребування коштів, розміщених у платіжній системі, отримання компенсацій у разі збоїв програмного забезпечення, а також з точки зору збереження конфіденційності персональних даних. надав. Питання соціально-економічного характеру, такі як захист прав споживачів, конкуренція, доступність, широта застосування, викликають особливе занепокоєння у фінансових органів • незважаючи на відмінну портативність, електронні гроші потребують спеціальних засобів зберігання та обігу;

– як і у разі готівки, при фізичному знищенні носія електронних грошей неможливо відновити грошову вартість власнику;

– немає розпізнавання – без спеціальних електронних пристроїв неможливо просто та швидко визначити, що це за об'єкт, сума тощо;

– засоби криптографічного захисту, за допомогою яких захищаються системи електронних грошей, ще не мають тривалої історії успішної експлуатації;

– теоретично зацікавлені особи можуть спробувати відстежити персональні дані платників та обіг електронних грошей поза банківською системою

– також системи електронних грошей здаються привабливими для реалізації різних схем, пов'язаних із легалізацією доходів, одержаних злочинним шляхом (так зване відмивання грошей). Анонімність платежів може призвести до того, що емітенти стикаються з зростаючими труднощами у застосуванні традиційних методів виявлення та запобігання злочинній діяльності.

Нижче наведено схематичне позначення недоліків електронних грошей (рисунок 2.2)

Рисунок 2.2 – Недоліки електронних грошей

Таким чином, всі користувачі електронних грошей ризикують зіткнутися з проблемою, що й користувачі традиційних форм грошей – необхідністю забезпечення безпеки та конфіденційності розрахунків. Впровадження електронних грошей призводить до появи додаткових зобов'язань, ризиків та витрат. Криптозахист електронних грошей традиційно розглядався як потенційно небезпечна річ. Зараз законодавство, що обмежує регулювання шифрування та кодування, почало серйозно заважати розвитку внутрішньої та міжнародної торгівлі, насамперед це стосується електронних систем «постачальник-клієнт», що працюють в мережі Інтернет [9].

2.3 Вимоги до технічного забезпечення

Структурно-функціональний розділ.

Програми Android використовують у своїй роботі вікна (схожі на Windows), однак у цій системі зазначені вікна мають іншу назву – Activity (Активність) [9].

При розробці програми необхідно максимально оптимізувати код і кількість дій, тому що велика кількість дій може призвести до збоїв у роботі програми та доставляти незручності користувачеві.

Функціональна структура мобільного додатку повинна включати:

– зручний інтерфейс;

– завантажувати інформацію з бази даних по протоколу HTTP;

– прості та зрозумілі механізми взаємодії з додатком;

– авторизація та автентифікація користувача;

– можливість пошуку за допомогою фільтрів характеристик

Інтерфейс користувача повинен враховувати такі принципи:

– Зручність. Використовуйте усталені та знайомі стандарти для використання програм в операційній системі Android. Кнопки, посилання та поля мають бути помітними та мати такі розміри, щоб користувачі могли їх натискати.

– Інформаційна архітектура. Зважаючи на обмеження розмірів, структура елементів відображення повинна бути максимально простою та зручною. Екран повинен мати оптимальну кількість кнопок і позначення шляхів користувача.

– Дизайн. Дизайн мобільного додатку має бути зрозумілим.

– Спеціальні дії. Обмежте кількість обов’язкових полів, щоб звільнити користувачів від довгих текстових записів.

Надайте дані "за замовчуванням", коли це можливо. Колірне рішення повинно бути в м'яких тонах, які приємні оку. Усі сторінки (екрани мобільного додатку) мають відповідати одному стилю, який базується на власному інтерфейсі Material Design. Під час роботи на пристрої бажаною орієнтацією екрана є книжкова. Мова інтерфейсу - українська.

Технічне забезпечення. Вся інформація в додатку повинна зберігатися в базі даних і бути доступною багаторазово.

Заявка підлягає наступним загальним технічним вимогам:

– операційна система Android 5.0 і вище;

– процесор - Qualcomm Snapdragon 625 1 ГГц або краще;

– оперативна пам'ять - 1 Гб і вище;

– екран дисплея - починаючи з 3,5 дюймів по діагоналі, починаючи з роздільної здатності 960*640;

– дисковий простір - близько 70 МБ при використанні;

– постійне підключення до Інтернету.

2.4 Опис архітектури програмного забезпечення

Структура програмного забезпечення визначає, як системи взаємодіють на рівні їх складових елементів. Компоненти, які використовуються у ваших системах, призначені для виконання конкретних завдань або набору завдань. Структура програмного забезпечення надає основу, на якій всі програмні засоби в компанії можуть бути змінені, створені або вилучені.

Структура програмного забезпечення впливає на якість, продуктивність, обслуговування та успіх системи з точки зору дизайну. Якщо компанія не розглядає структуру програмного забезпечення на регулярній основі, вона стикається з потенційними довгостроковими наслідками, такими як проблеми, що можуть призвести до несправностей, злому або низької продуктивності їх систем.

У сучасних системах існують загальні шаблони структури програмного забезпечення, які називаються архітектурними шаблонами для програмного забезпечення. Часто для створення цілісної системи використовуються різні архітектурні шаблони, особливо коли система розвивалась протягом довгого часу або була побудована різними розробниками.

2.4.1 Опис класів

У мові Java клас є будівельним блоком, який дозволяє використовувати об'єктно-орієнтоване програмування. Це визначений користувачем тип даних, який містить власні поля даних і методи, до яких можна отримати доступ та використовувати, створивши екземпляр цього класу. У JavaScript клас схожий на шаблон для об'єкта.

Наприклад, розглянемо клас "Автомобіль". Може бути багато автомобілів з різними назвами та марками, але всі вони матимуть спільні властивості, такі як 4 колеса, обмеження швидкості, діапазон пробігу і т.д. Таким чином, "Автомобіль" є класом, а колеса, обмеження швидкості, пробіг - його полями.

Клас - це визначений користувачем тип даних, який містить поля даних і методи. Поля даних - це змінні, а методи - функції, які використовуються для

маніпулювання цими змінними. Разом вони визначають властивості та поведінку об'єктів у класі.

У прикладі класу "Автомобіль" полями даних будуть обмеження швидкості, пробіг і т.д., а методами можуть бути гальмування, збільшення швидкості і т.д.

Об'єкт - це екземпляр класу. Коли клас визначений, пам'ять не виділяється, але коли створюється об'єкт (екземпляр класу), пам'ять виділяється.

Оголошення класу та створення об'єктів У Java клас визначається за допомогою ключового слова "class", після якого йде ім'я класу. Тіло класу визначається всередині фігурних дужок і закінчується крапкою з комою в кінці. Створення об'єктів: коли клас визначений, визначається лише специфікація об'єкта; пам'ять або сховище не виділено. Щоб використовувати дані і методи, визначені в класі, потрібно створити об'єкти.

Синтаксис:

ClassName ObjectName;

Доступ до полів даних і методів: Доступ до полів даних і методів класу можна отримати за допомогою оператора крапка ('.') з об'єктом. Наприклад, якщо ім'я об'єкта - obj, і ви хочете отримати доступ до методу з ім'ям printName(), ви повинні написати obj.printName().

Доступ до полів даних: Доступ до загальнодоступних полів даних також здійснюється за допомогою оператора крапка ('.'), але об'єкт не може мати прямий доступ до приватних полів даних. Доступ до полів даних залежить від модифікатора доступу цих полів даних.

Модифікатори доступу (відкритий, приватний, захищений) контролюють доступ до полів даних і методів класу.

Клас є шаблоном або планом, який об'єднує властивості та функції сутності. Ви можете розмістити всі сутності або об'єкти з подібними атрибутами під одним покрівлею, відомою як клас. Класи реалізують основні принципи: інкапсуляція, приховування даних, абстракція. У Java класи діють як типи даних, що можуть мати кілька об'єктів або екземплярів цього класу.

Розглянемо в якості прикладу клас Products:

```
class Products
{
        Products();

        function Create(var count_tov, var count_day, var num);
        function Print();
        function Method1();


        function Method2();
        function Method3();
        function save();
private:
        var arr;
        var product_name;
        var prognoz;
};
```

В ньому є конструктор, деструктор. У приватній частині зберігаються змінні.

Ще в ньому є декілька функцій, що зберігаються у публічній секції.

В програмі була розроблена наступна структура класів (рис. 2.3)

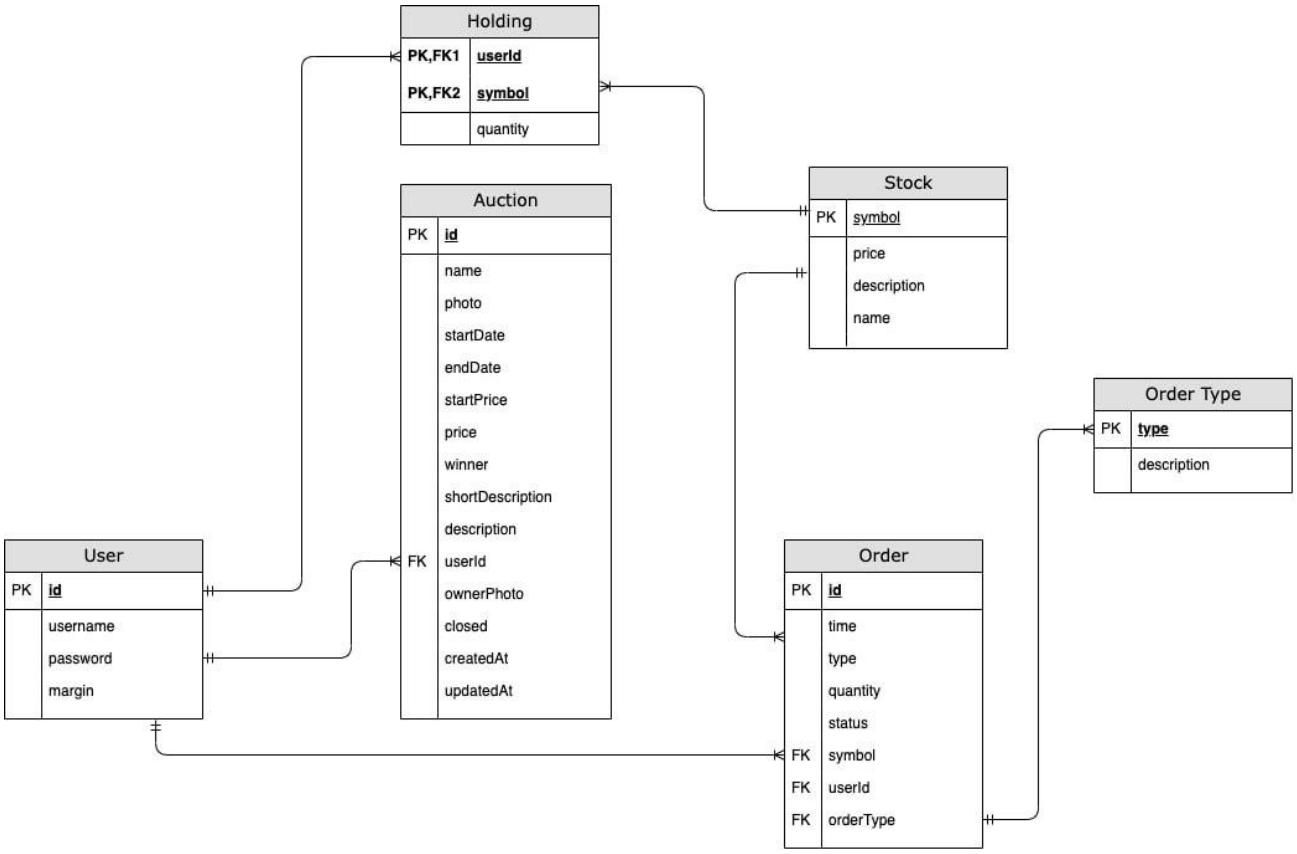


Рисунок 2.3 – Структура класів

2.4.2 Діаграми UML та блок-схеми програми

Програмне забезпечення реалізовано у вигляді веб-додатку. Розроблену таким чином програмну систему можна умовно розділити на дві загальні частини: клієнтську (front end) і серверну (back end).

Кожна з цих частин виконує власну роль, має власних користувачів і виконує власні функціональні та нефункціональні вимоги.

Серверна частина програмного забезпечення для розробки виконує такі функції:

1. Обробка асинхронних запитів у інтерфейсі веб-додатку.

2. Реалізація архітектурного шаблону MVC.

3. Реалізує читання, збереження, оновлення та видалення даних.

4. Щогодини збирає фінансові дані криптовалют, фільтрує та зберігає зібрану інформацію в базі даних.

5. Збір і обробка даних соціальних новин і газетних новин і збереження текстів в базах даних.

6. Прогнози обмінного курсу для вибраних криптовалют.

Клієнтська частина по черзі виконує такі функції:

1. Реалізувати інтерфейс між системою та користувачем

2. Сформувати асинхронний запит на сервер для постійного оновлення даних на сторінці.

3. Візуалізація отриманих прогнозів у вигляді графіків і діаграм.

4. Відповідає за коректність відтворення дизайну сторінки на пристроях з різним дозволом екрану.

Структурна схема системи розробленого додатку складається з багатьох елементів, кожен елемент підключений до іншого модуля в системі і виконує свою призначену роль. Наявні елементи в схемі розділені на такі категорії: системні модулі, бази даних, користувачі системи.

Діаграма компонентів UML (рис. 2.4) показує існуючі компоненти в системі, а також внутрішні та зовнішні інтерфейси, через які компоненти взаємодіють один з одним. На діаграмі виділено дві окремі частини: серверну частину та зовнішню частину програми

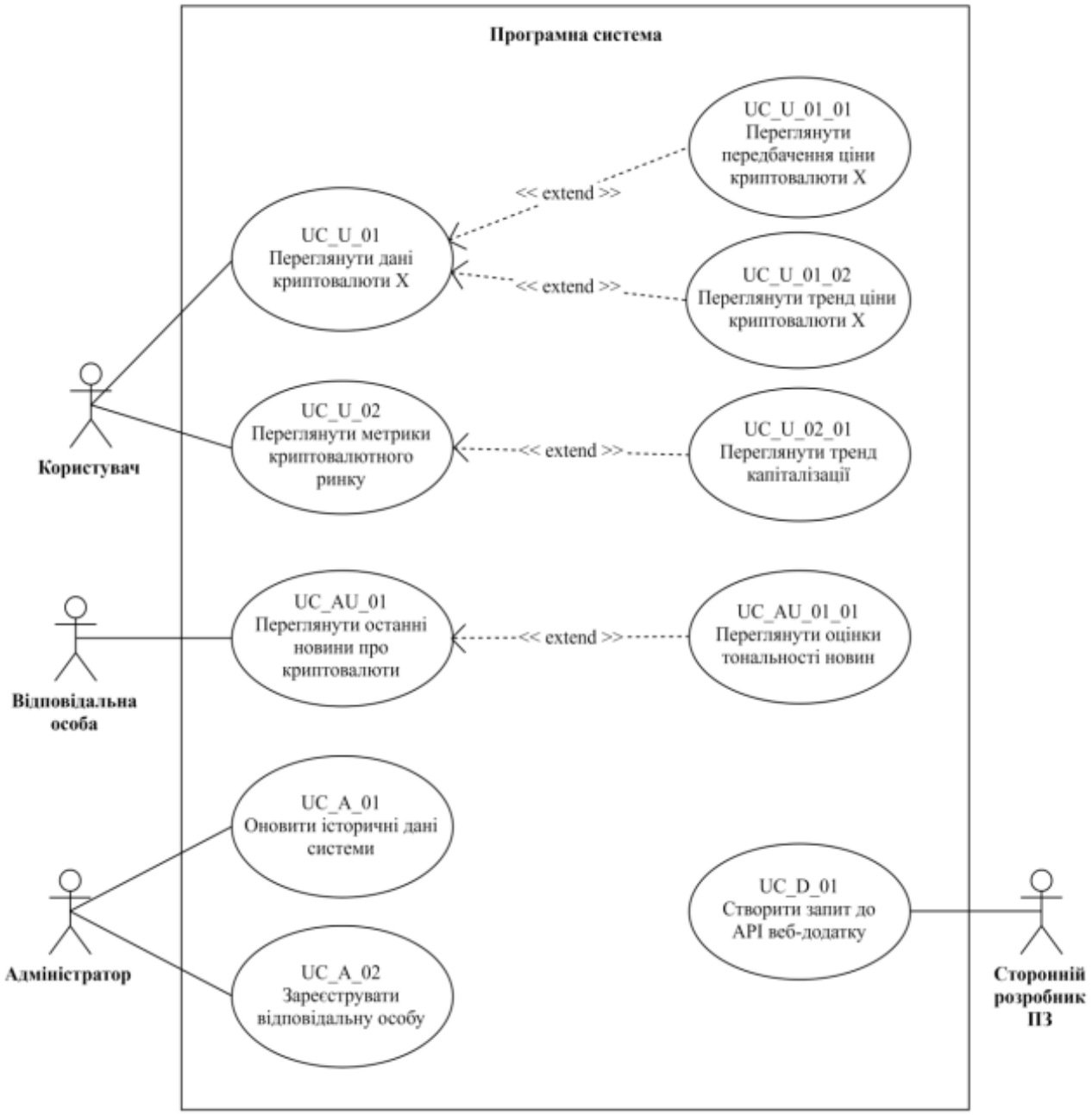


Рисунок 2.4 – UML – діаграма варіантів використання

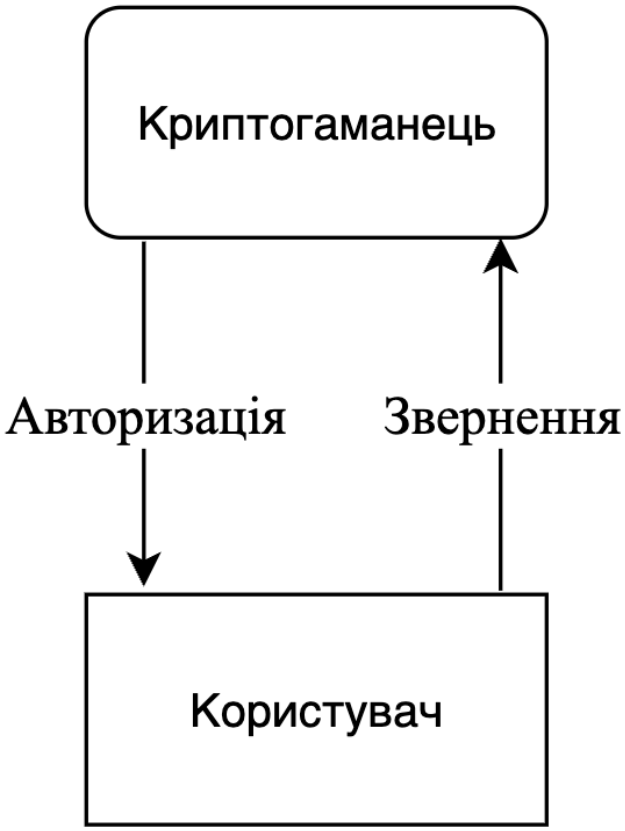


Рисунок 2.5 – Модель події авторизації

Інші моделі(діаграми) такі як: Схема реєстрації(ІС-93.260БАК.004 Д1), Модель події реєстрації(ІС-93.260БАК.004 Д5) можна переглянути в переліку додаткових документів проєкту.

Висновки до розділу 2

На сьогоднішній день вибір мобільних операційних систем досить широкий. Однак характер їх розвитку у кожного з них дуже різний. iOS виключається через високий ризик труднощів у розробці та розповсюдженні додатків, а також високу ціну на публікацію додатків та отримання інструментів розробки. Windows Mobile було виключено через надзвичайно низький рівень проникнення операційної системи та відсутність підтримки розробників.

Тому для розробки мобільного застосунку для обміну криптовалюти була обрана платформа Android.

Як інструмент розробки було обрано Android Studio, яка є новішою платформою на основі Java порівняно з іншими інструментами розробки Android.

3 ЕТАПИ РОЗРОБКИ І СТВОРЕННЯ ПРОГРАМНОГО ДОДАТКУ ДЛЯ ОБМІНУ КРИПТОВАЛЮТ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ БЛОКЧЕЙН

3.1 Розробка власного продукту

3.1.1 Розробка структури даних

Для взаємодії з тією чи іншою криптовалютною біржею знадобиться розробка базового класу, який надасть набір функцій для роботи з біржею, які будуть використовуватись у стратегіях торгівлі. Також у базовому класі буде реалізовано деякі додаткові можливості, не пов'язані із взаємодією з криптовалютними біржами.

Для роботи з криптовалютними біржами будуть потрібні такі базові можливості:

- ініціалізація роботи із зазначеною криптовалютною біржею;
- встановлення валютної пари;
- отримання балансу за поточною парою;
- отримання даних щодо поточної пари;
- отримання відкритих ордерів;
- створення ордера для придбання;
- створення ордера продаж;
- скасування створеного ордера;
- отримання історії угод.

Ініціалізація роботи із зазначеною криптовалютною біржею та встановлення валютної пари відбуватимуться у конструкторі базового класу. У рамках дипломного проекту буде реалізовано ініціалізацію роботи однієї криптовалютної біржі – Poloniex. Для того, щоб досягти незмінності коду у разі зміни криптовалютної біржі або торгової пари, було прийнято рішення вказувати ці параметри в змінних оточення (environment variables).

Це деякі глобальні значення, розташовані лише на рівні операційної системи, доступні програмам. Крім назви криптовалютної біржі та торгової пари можуть знадобитися інші дані, наприклад, секретні ключі для взаємодії з криптовалютною біржею. Різні криптовалютні біржі можуть використовувати

один або два секретні ключі: публічний та приватний. Таким чином, конструктор базового класу також витягуватиме такі дані зі змінних оточення: назву криптовалютної біржі, назву валютної пари та публічний та приватні секретні ключі.

Інші пункти базових можливостей будуть реалізовані у методах, які будуть визначені у базовому класі. Опис цих методів наведено нижче:

– fetchBalance () – функція, яка отримує поточний баланс торгової пари, який охоплює всю кількість валюти, кількість вільних і використовуваних ордерів;

– fetchTicker() – функція, яка отримує деталі щодо поточної валютної пари;

– fetchOpenOrders () – функція, призначена для отримання списку всіх активних ордерів для поточної валютної пари;

– createBuyOrder (amount: number, price: number) – функція, яка отримує два параметри (обсяг та ціну) і створює замовлення на купівлю, яка отримає першу валюту пари, використовуючи другу валюту пари;

– createSellOrder (amount: number, price: number) – функція, яка отримує два аргументи (обсяг та ціну) та ініціює замовлення на продаж, який забезпечить другу валюту пари, використовуючи першу валюту пари;

– cancelOrder (id: number) – метод, який приймає один параметр (унікальний ідентифікатор замовлення) і дозволяє скасувати існуюче замовлення на купівлю чи продаж;

– fetchTradesHistory (since: number = 0) – метод, який містить необов’язковий параметр (мітки часу, з якого потрібні дані) і дозволяє отримувати історію транзакцій із поточної валютної пари.

Також був написаний смарт-контракт мовою Solidity для здійснення виводу криптовалюти з нашого застосунку до іншого гаманця або біржі(застосунок працює на власному блокчейні Trokhymets, тому наразі скористатися смарт-контрактом можна тільки у випадку, якщо у користувача існує криптоадреса у цьому користувацькому блокчейні).

Також варто звернути увагу на те, що кожна криптовалютна біржа має торгову комісію, обмеження при створенні ордера, а також точність при округленні, причому ці значення можуть змінюватись в залежності від тієї чи іншої біржі. Щодо торгової комісії, то деякі криптовалютні біржі використовують прогресивну шкалу, що робить цей параметр динамічним, а отже, він не може бути визначений у базовому класі.

Таким чином, було вирішено створити ще три методи:

– loadFees() – абстрактний метод, що встановлює торгову комісію, який перевизначається під час реалізації тієї чи іншої стратегії;

– loadLimits() – метод, який визначає значення обмежень;

– loadPrecisions() – метод, який визначає значення точності округлень.

Додатково можна переглянути більш детальні схеми(діаграми) для Компонентів Android-додатку (ІС-93.260БАК.004 Д2), а також для моделей Покупки криптовалюти (ІС-93.260БАК.004 Д3) та події надсилання криптовалюти (ІС-93.260БАК.004 Д4) в переліку додаткових документів проєкту.

3.1.2 Написання програмного продукту

Спочатку роботи, було створено логотип додатку. Вид цього логотипу зображено на рис. 3.1

Рисунок 3.1 – Логотип застосунку

Було створено шапку додатку (рис. 3.2), в якому є меню, логотип, кошик та мова інтерфейсу.

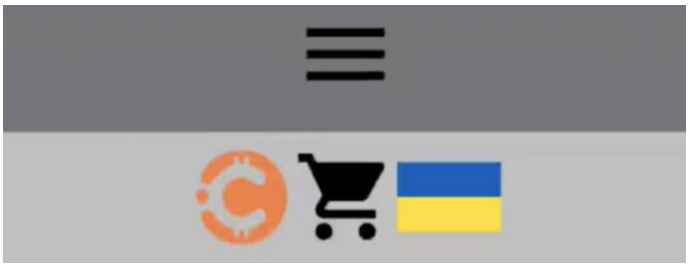


Рисунок 3.2 - header

На рисунку 3.3 зображено випадаючи меню.

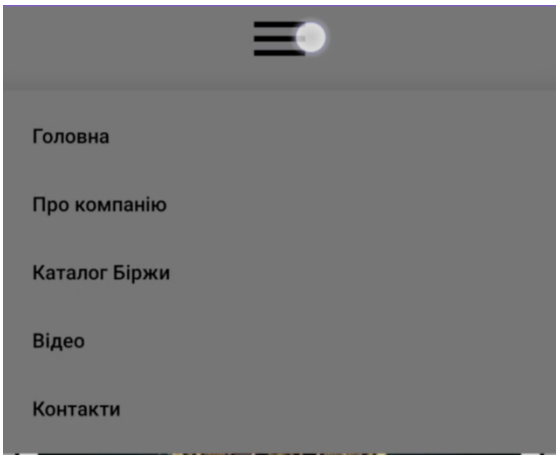


Рисунок 3.3 - Меню

А також було зроблено нижню частину (рис. 3.4).

Рисунок 3.4 - footer

У footer розташовано 4 кнопки:

- home
- portfolio

– market
– profile

3.2 Опис функціоналу

Запускаючи програму перед нами з’являється наступна картинка (рис. 3.5)

Рисунок 3.5 – Вхід в систему

Далі після завантаження ми потрапимо на головну сторінку (рис. 3.6)

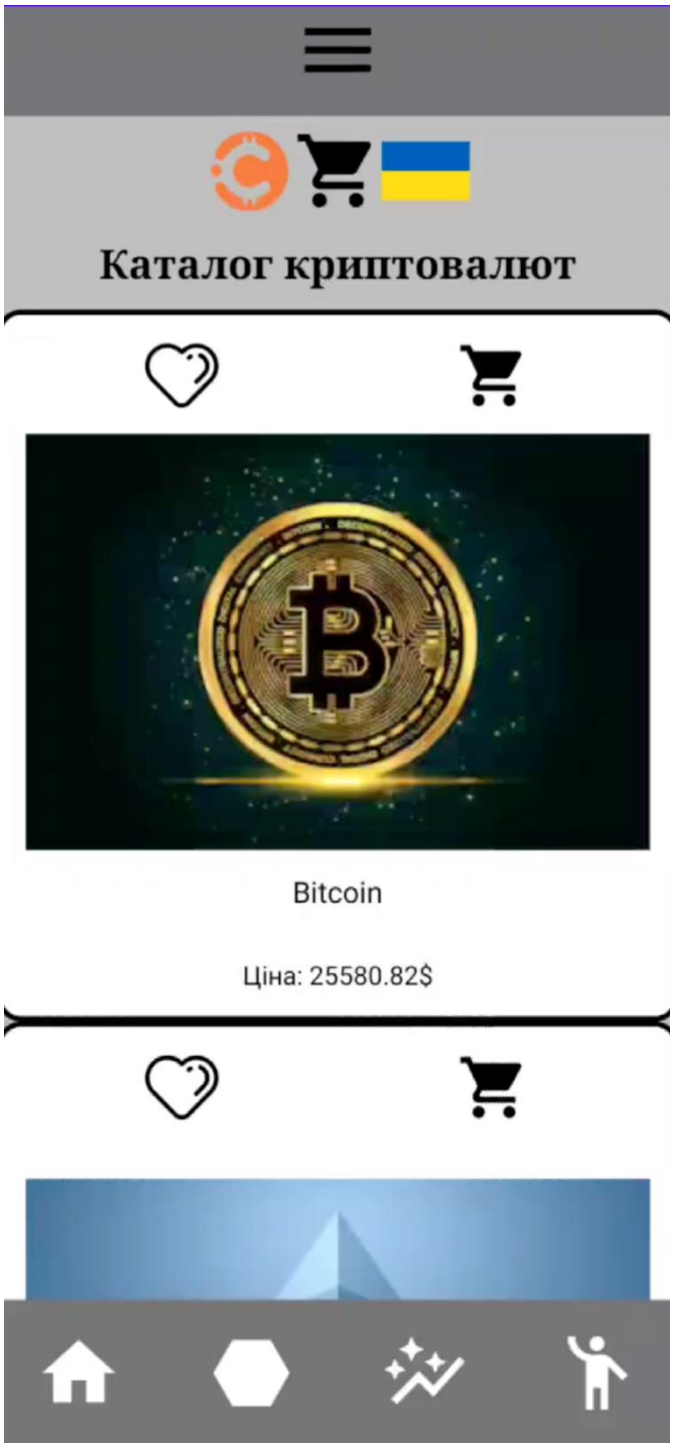


Рисунок 3.6 – Головна сторінка

Далі були розроблені вкладки які знаходяться у нижній частині додатку (footer). Вкладка портфоліо, на ній відображено придбані криптовалюти користувачем (рис. 3.7)

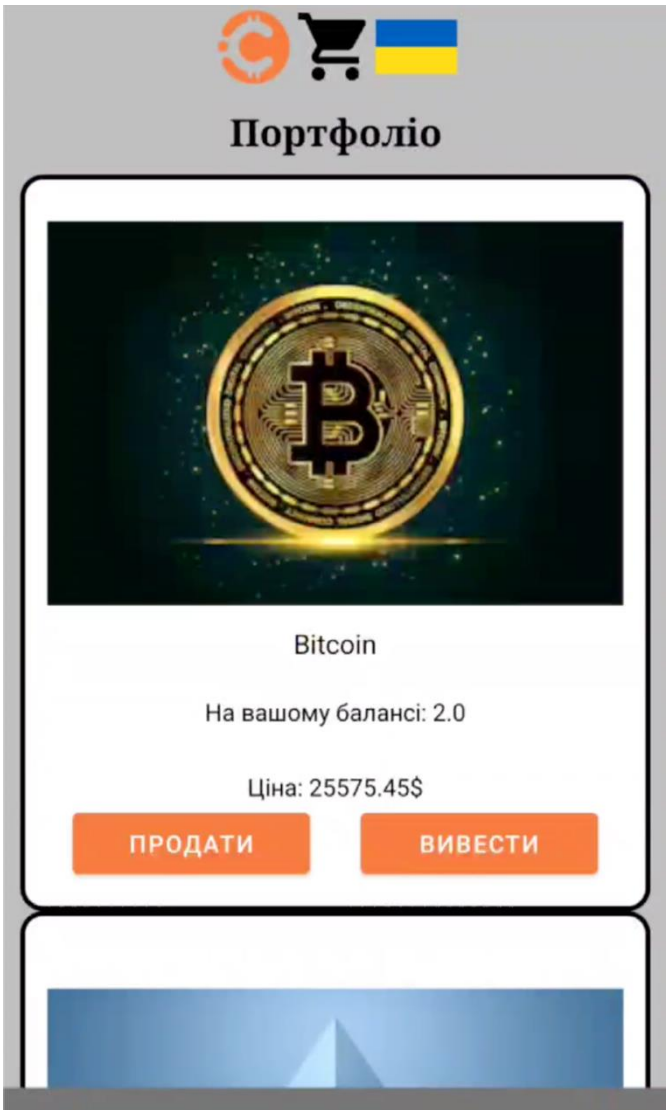


Рисунок 3.7 – Портфоліо

На вкладці «Маркет» зображена інформація про поточну вартість та графіки зростання/спадання ціни криптовалют (рис. 3.8)

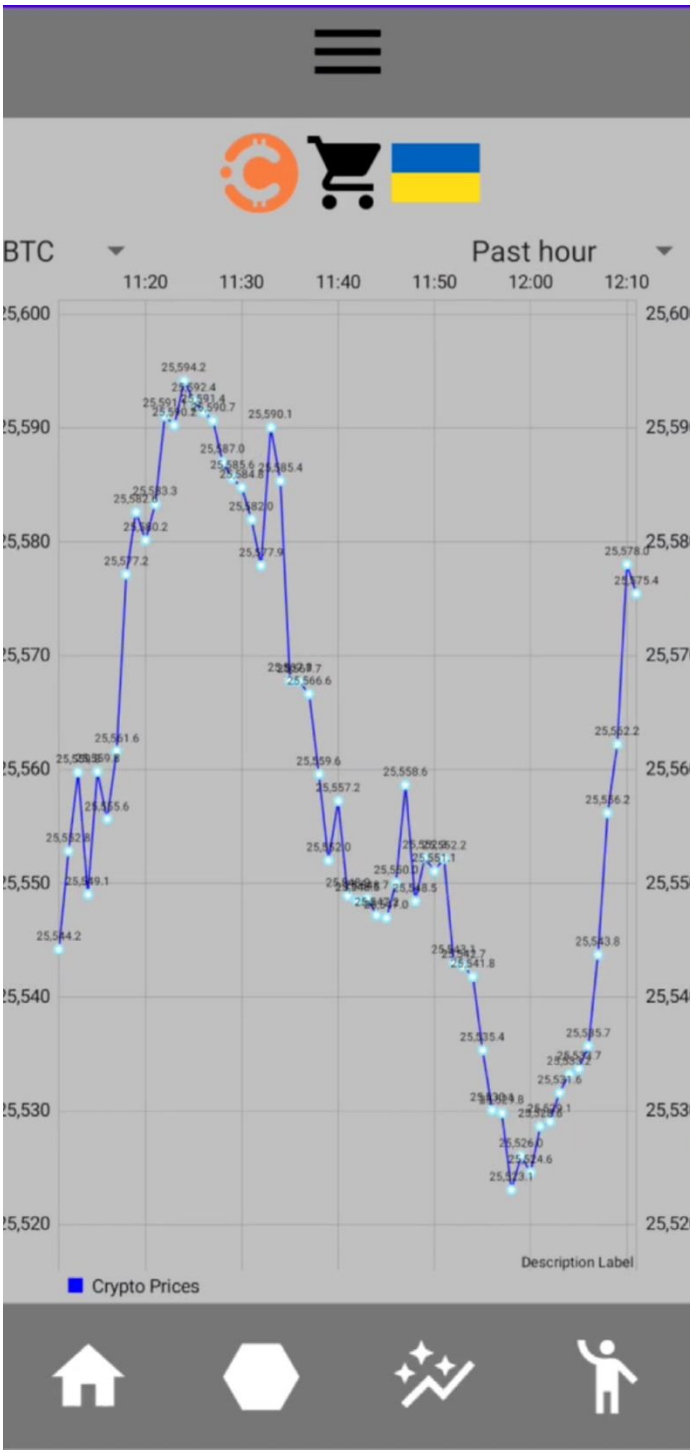


Рисунок 3.8 – Сторінка «Market»

На вкладці «Профіль» відображено профіль користувача. Можна також звернутися у підтримку. (рис.3.9)

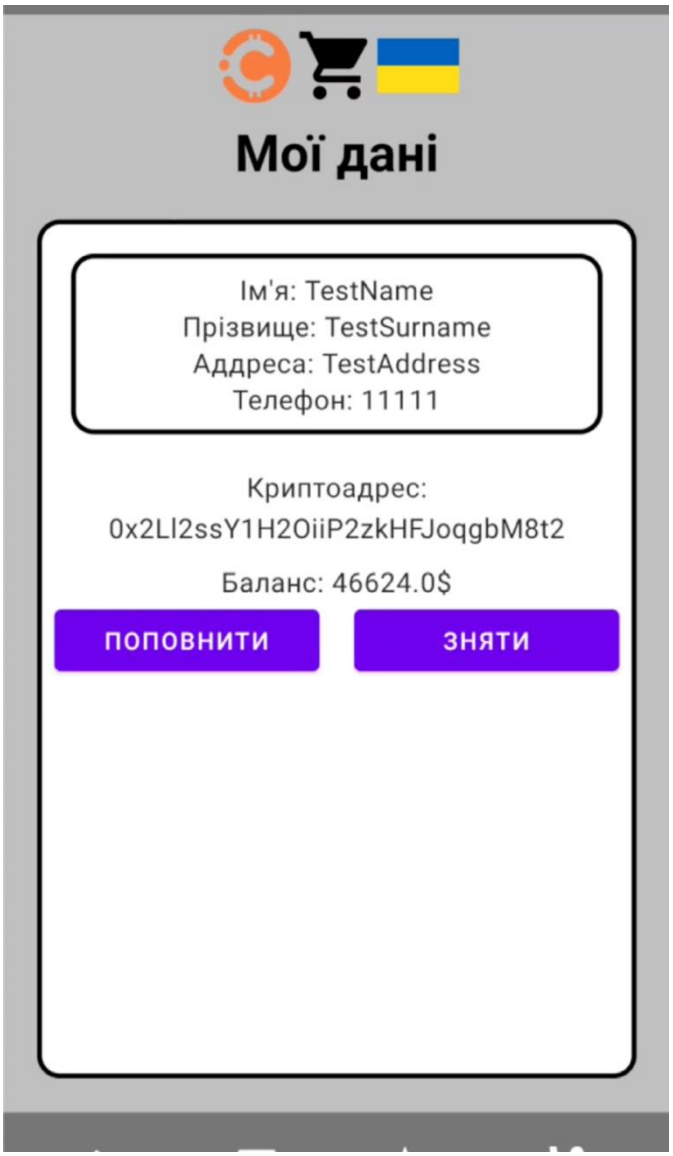


Рисунок 3.9 – Сторінка «Профіль»

3.3 Тестування

Під час тестування помилки які виникали, одразу ж виправлялися. Нижче наведено декілька прикладів тестування мобільного застосунку.

Тестування купівлі/продажу (рис. 3.10)

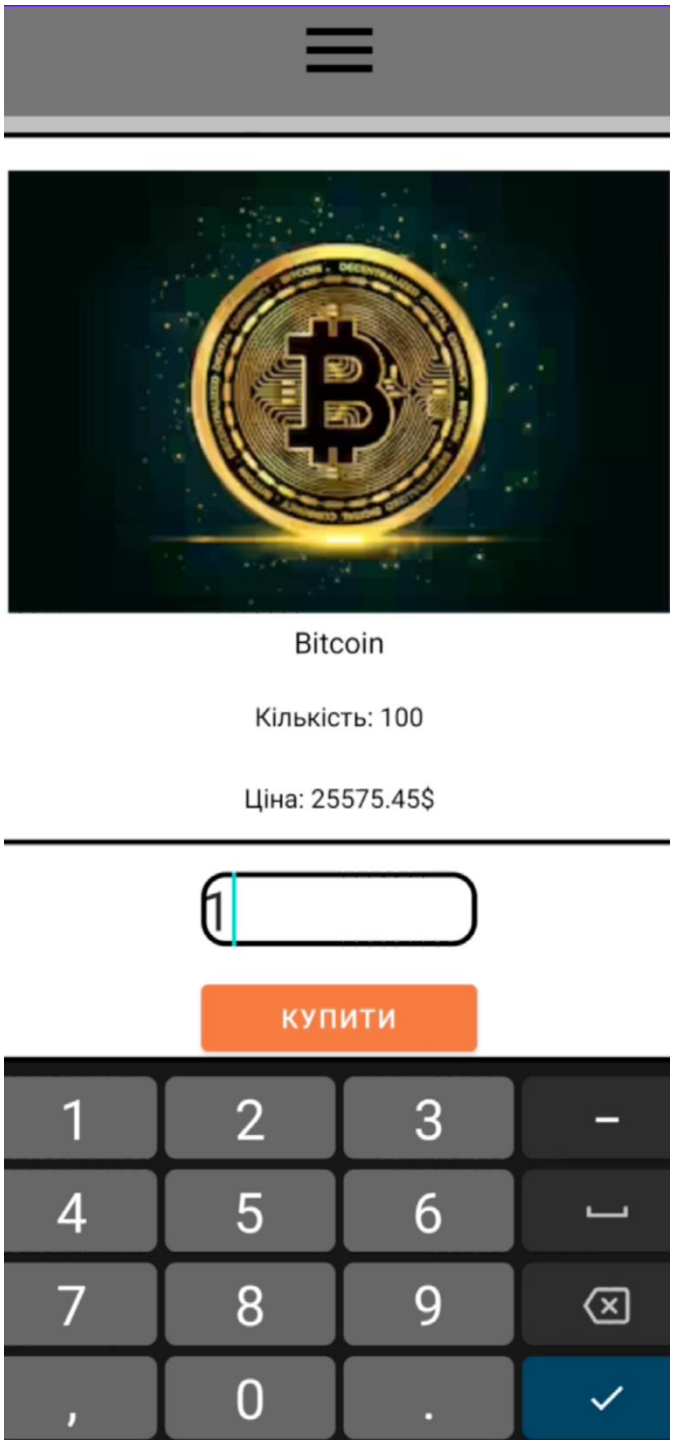


Рисунок 3.10 – Тестування купівлі

.

Виведення криптовалюти з застосунку(рис. 3.11) та застосування смарт-контракту для підтвердження дії(рис. 3.12).

А також тестування функції прогнозування курсу криптовалюти(рис. 3.13).

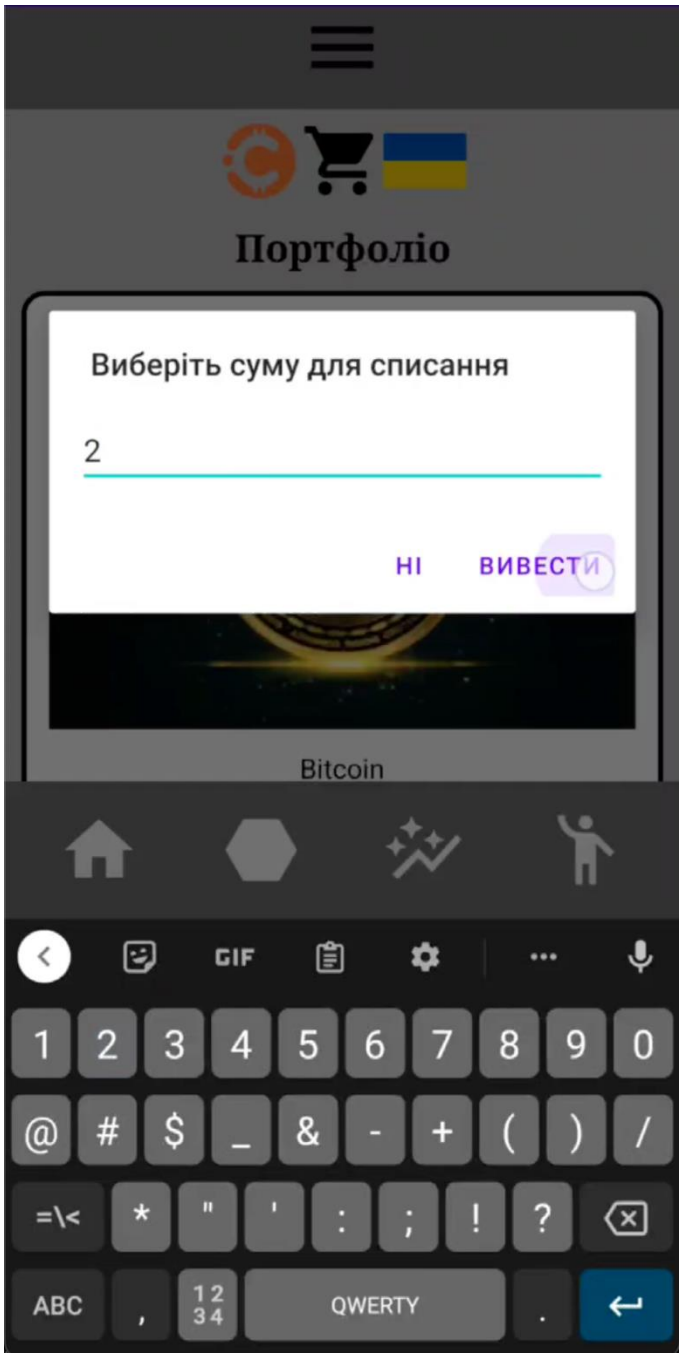


Рисунок 3.11 – Виведення криптовалюти з застосунку

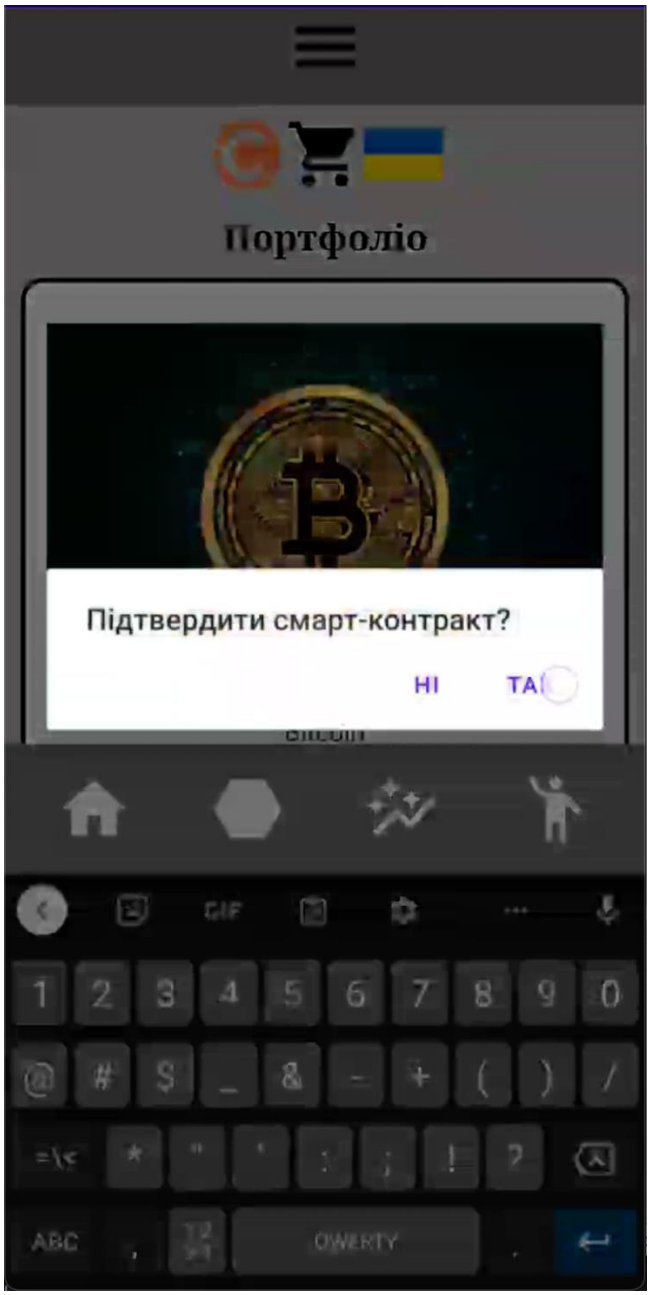
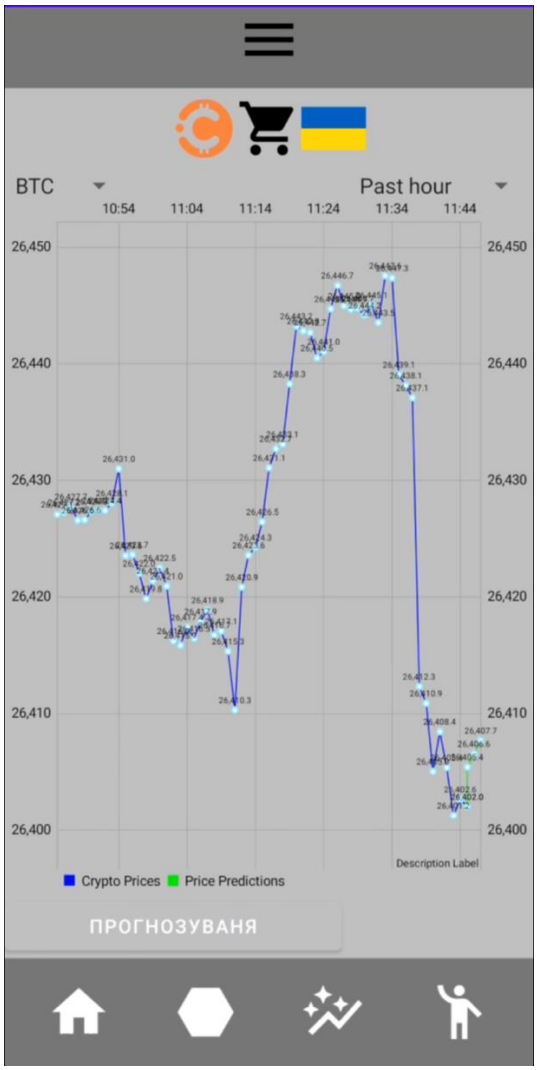


Рисунок 3.12 – Застосування смарт-контракту



Рисунко 3.13 – Прогнозування курсу криптовалюти

Висновки до розділу 3

В цьому розділі описані етапи розробки та створення програмного додатку. Наведено розроблений алгоритм та етапи написання програмного коду. Розроблено структури даних та описується функціонал програми. Також наведений алгоритм тестування, проведений аналіз помилок, які виникають під час тестування і обробляються в програмі.

ВИСНОВКИ

У цьому дипломному проєкті було розглянуто розробку мобільного застосунку для обміну криптовалют з використанням технології блокчейн. Основними цілями роботи було створення зручного та безпечного інструменту для користувачів, що дозволить їм ефективно обмінювати різні криптовалюти та забезпечувати надійне зберігання їх активів.

У процесі роботи були визначені вимоги до мобільного застосунку та проведений аналіз технології блокчейн для вибору найбільш підходящих рішень. Була розроблена архітектура додатку, включаючи базу даних та логіку взаємодії між користувачем та системою.

Крім того, було розроблено інтуїтивно зрозумілий користувацький інтерфейс, який дозволяє зручно взаємодіяти з додатком та здійснювати операції обміну криптовалют в кілька кліків.

Результати роботи показують, що розроблений мобільний застосунок відповідає поставленим вимогам і забезпечує зручну та безпечну платформу для обміну криптовалют. Технологія блокчейн використовується для створення довіреної та надійної інфраструктури, що дозволяє уникнути проблеми подвійного витрачання та забезпечує незмінність та недоступність даних користувачів.

Отримані результати можуть бути використані для подальшого розвитку мобільного застосунку та його впровадження на ринку обміну криптовалют. Застосунок може бути корисним для широкого кола користувачів, які бажають здійснювати швидкі та безпечні операції обміну криптовалют з використанням сучасних технологій блокчейн.

Подальший розвиток застосунку вбачається в інтеграції більшої кількості загальновживаних блокчейнів та криптовалют.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гарднер Л., Грігсбі Д. Розробка веб-сайтів для мобільних пристроїв; Київ, 2013. 528 с.
2. An Empirical Study on Modeling and Prediction of Bitcoin Prices With Bayesian Neural Networks Based on Blockchain Information [Електронний ресурс] // IEEE Xplore Digital Library. – 2017. – Режим доступу: https://ieeexplore.ieee.org/document/8125674/.
3. Онлайн-документація Ethereum. Ethereum. URL: https://ethereum.org/ (дата звернення 25.04.23).
4. Онлайн-документація Solidity. Solidity. URL: https://soliditylang.org/ (дата звернення 26.04.23).
5. Bitcoin Cash: Price of new currency rises after bitcoin's 'hard fork' [Електронний ресурс] // Інтернет-портал 'The Telegraph', 2017. Режим доступу: http://www.telegraph.co.uk/technology/2017/08/01/bitcoin-cash-everything-need-know-bitcoins-hard-fork/.
6. Bitcoin Charts and Graphics [Електронний ресурс] // Інтернет-портал ‘Blockchain.info’, 2017. Режим доступу: https://blockchain.info/charts.
7. Bitcoin Futures Contract Specs - CME Group [Електронний ресурс] // CME Group, 2018. Режим доступу: http://www.cmegroup.com/trading/equity-index/us-index/bitcoin_contract_specifications.html.
8. Bitcoin goes legit in Japan – will be legal currency starting in April [Електронний ресурс] // Інтернет-портал 'Disruptive Asia', 2017. Режим доступу: https://disruptive.asia/bitcoin-legit-japan.
9. Історичний регресійний аналіз Bitcoin. Tyler Virkler [Електронний ресурс] // Інтернет-портал 'Kaggle.com’, 2017. Режим доступу: https://www.kaggle.com/tyvirk/bitcoin-historical-regression-analysis/data.
10. Біткоїни. Як це працює [Електронний ресурс] // Інтернет-портал «Хабрахабр», 2017. Режим доступу: https://habrahabr.ru/post/114642.

11. Bitcoin: A Peer-to-Peer Electronic Cash System [Електронний ресурс] // Офіційний сайт Bitcoin, 2009. Режим доступу: https://bitcoin.org/bitcoin.pdf.

12. Countdown: Bitcoin Will Be a Legal Method of Payment in Japan in Two Months [Електронний ресурс] // Інтернет-портал 'Bitcoin.com', 2017. Режим доступу: https://news.bitcoin.com/countdown-bitcoin-legal-payment-japan-two-months/.

13. Ethereum Charts and Statistics [Електронний ресурс] // Інтернет-портал ‘Etherscan’, 2017. Режим доступу: https://etherscan.io/charts.

14. Ethereum: більше, чим криптовалюти [Електронний ресурс] // Інтернет-портал 'Profit-Hunters', 2017. Режим доступу: https://profit-hunters.biz/ethereum-bolshe-chem-kriptovalyuta.

15. Ethereum-блокчейн і його використання на практиці [Електронний ресурс] // Інтернет-портал ‘Geektimes’, 2017. Режим доступу: https://geektimes.ru/company/wirex/blog/277438/.

16. Fama E., Fisher L., Jensen M., Roll R. The Adjustment of Stock Prices to New Information // International Economic Review. 1969. Вип. 10. N 1. С. 1–21.

17. Fork Watch: Block 478558 Initiates 'Bitcoin Cash' Split – First Blocks Now Mined [Електронний ресурс] // Інтернет-портал 'Bitcoin News', 2017. Режим доступу: https://news.bitcoin.com/fork-watch-first-bitcoin-cash-block-mined.

18. Hype Cycle Research Methodology [Електронний ресурс] // Інтернет-портал 'Gartner.com', 2017. Режим доступу: https://www.gartner.com/technology/research/methodologies/hype-cycle.jsp.

19. Kothari S., Warner J. Econometrics of Event Studies // Handbook of Corporate Finance: Empirical Corporate Finance / Ред. автора Б. Екбо. Elsevier, Північна Голландія, 2007. С. 3–36.

20. Microsoft інтегрує Ethereum с хмарним сервісом Azure [Електронний ресурс] // Інтернет-портал 'Bits Media', 2017. Режим доступу: https://bits.media/news/microsoft-integriruet-ethereum-c-oblachnym-servisom.

21. Palmon D., Sudit E., Yezegel A. The Value of Columnist's Stock Recommendations: an Event Study Approach // Review of Quantitative Finance and Accounting. 2009. Вип. 33. N 3. С. 209–232.

22. Прогноз ціни біткойна -лінійна регресія. Alisa Aleksanyan [Електронний ресурс] // Інтернет-портал 'Kaggle.com', 2017. Режим доступу: https://www.kaggle.com/alisaaleksanyan/prediction-of-bitcoin-price-linear-regression/data.

23. Ripple (XRP) history data [Електронний ресурс] // Інтернет-портал 'Coinmarketcap', 2017. Режим доступу: https://coinmarketcap.com/currencies/ripple/historical-data.

24. Пульсація (XRP). Все про криптовалюту – Bitcoin Wiki [Електронний ресурс] // Bitcoin Wiki, 2018. Режим доступу: https://ua.m.bitcoinwiki.org/wiki/Ripple, вільний – Загл. з екрану.

ДОДАТОК А

QR-код посилання на репозиторій проєкту на Github