КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
Факультет комп'ютерних наук та кібернетики
Кафедра математичної інформатики

«До захисту допущено»
Завідувач кафедри
В.М. Терещенко

_____
(підпис)

«___» _____20___ р.

Кваліфікаційна робота
на здобуття ступеня бакалавра

за спеціальністю 122 Комп'ютерні науки

на тему:

БЛОКЧЕЙН ТЕХНОЛОГІЇ

Виконав студент 4 курсу
Дудін В'ячеслав Юрійович

_____
(підпис)

Науковий керівник:
професор, доктор фіз.-мат. наук
Анісімов Анатолій Васильович

_____
(підпис)

Засвідчую, що в цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____
(підпис)

Київ – 2022

РЕФЕРАТ

Обсяг роботи 61 сторінка, 16 ілюстрацій, 3 таблиці, 24 джерела посилань.

BITCOIN, ТЕХНОЛОГІЯ РІВНИЙ ДО РІВНОГО, ІНФРАСТРУКТУРА ВІДКРИТОГО КЛЮЧА, ДОКАЗ ЧАСТИНИ ВИКОНАНОЇ РОБОТИ, ДОКАЗ ВИКОНАНОЇ РОБОТИ, ОДНОСТОРОННЯ ХЕШ-ФУНКЦІЯ.

Об’єктом роботи виступають криптовалюти, як інструмент безготівкових розрахунків у платіжній системі різних країн та біржі, пов'язані з активами в криптовалюті, а також весь процес проведення транзакцій. Предметом роботи є програмний засіб для обміну криптовалюти на різних біржах.

Метою роботи є розробка програмного засобу для торгівлі криптовалютою з використанням стратегій максимально доходу при одночасному зниженні ризику.

Методи розроблення: аналіз та синтез, класифікація, візуалізація, авторегресійний аналіз та прогнозування динаміки котирувань криптовалют. В якості інструменту обрано Python та декілька модулів для реалізації інтерфейсу і створення запитів до криптовалютних бірж. Модуль PyQt – набір розширень фреймворку Qt для мови програмування Python. Бібліотека CCXT для підключення та торгівлі з криптовалютними біржами.

Результати роботи: висвітлено основні теоретичні аспекти об’єкта дослідження; здійснено порівняльний аналіз існуючих сучасних криптовалют та технологій їх побудови; досліджено аналіз обраних факторів та виділити найбільш статистично значущі для побудови засобу; розроблено програмне забезпечення для обміну криптовалюти на різних біржах.

Отримані результати можуть використовуватися для розробки рекомендацій щодо інвестування коштів у криптовалюту, а також для вдосконалення стратегії розвитку компаній, що займаються розробкою блокчейн.

Використання інструментальних засобів та методів створення системи робота виконувалася сумісно з роботами зі знаходження алгоритмів арбітражу.

ЗМІСТ

С.

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧЕННЯ 4

ВСТУП 5

РОЗДІЛ 1 ОСОБЛИВОСТІ КРИПТОВАЛЮТИ BITCOIN ТА РОЗПОДІЛЕНОЇ СИСТЕМИ BLOCKCHAIN 8

1.1 Аналіз систем управління базами даних 8

1.2 Концепція побудови технології blockchain 13

1.3 Особливості принципів роботи цифрової валюти bitcoin 17

РОЗДІЛ 2 РІЗНОВИДИ КРИПТОВАЛЮТ ТА МЕХАНІЗМ КОНСЕНСУСУ 26

2.1 Існуючі різновиди криптовалют 26

2.2 Емісія криптовалюти 31

2.3 Механізми досягнення консенсусу 38

РОЗДІЛ 3 РОЗРОБКА ПРОГРАМНОГО ЗАСОБУ АРБІТРАЖНОЇ СИТУАЦІЇ 44

3.1 Середовище розробки та опис програми 44

3.2 Опис алгоритму роботи для програмного забезпечення 48

3.3 Реалізація інтерфейсу створеного програмного забезпечення 54

ВИСНОВКИ 57

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ 59

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧЕННЯ

BM – Block Managers, менеджер блоків;

BTC – Bitcoin, платіжна система, яка застосовує однойменну одиницю для обліку операцій;

ECDSA – Elliptic Curve Digital Signature Algorithm, алгоритм для створення цифрового підпису з відкритим ключем;

ETH – Ethereum, платформа на базі блокчейна;

IDE – Integrated Design Environment, інтегроване середовище розробки;

LBM – Local Block Managers, локальний менеджер блоків;

LSB – Lightweight Scalable Blockchain, легкий масштабований блокчейн;

OBM – Overlay Block Managers, менеджер накладених блоків;

P2P – Peer to Peer, технологія рівний до рівного;

PKI – Public Key Infrastructure, інфраструктура відкритого ключа;

PoS – Proof of Stake, доказ деякої частини виконаної роботи;

PTV – Percentage of Transactions to be Verified, відсоток транзакцій, який потрібно підтвердити;

PoW – Proof of Work, доказ виконаної роботи;

RFID – Radio Frequency IDentification, радіочастотна ідентифікація;

SHA-256 – Secure Hash Algorithm, хеш-функція, одна з основних функцій безпечного алгоритму хешування;

БД – база даних;

ПЗ – програмне забезпечення;

СППР – система підтримки прийняття рішень.

ВСТУП

Оцінка сучасного стану об’єкта розробки. Поява цифрових грошей та їх різноманітні види, як можливі альтернативи існуючим паперовим грошам відчутно викликає занепокоєння не лише в економістів, а також і у пересічних громадян – користувачів сучасних фінансових послуг в умовах роботи глобальної мережі Інтернет. На даний момент в економіці відсутнє однозначне трактування поняття криптовалюти. Цей факт суттєво уповільнює впровадження офіційних документів з боку держав щодо їх легітимізації, а також розвитку у перспективі [3].

У зв'язку з цим особливої актуальності набувають питання, що стосуються визначення сфер застосування та впровадження криптовалют. З розвитком та впровадженням науково-технічного прогресу у сферу фінансів також стали розвиватися різного роду засоби платежів. Потім з'явилася криптовалюта – наслідок удосконалення обчислювальної техніки та розвитку ІТ.

Поява криптовалют – одна з ключових причин підвищення попиту на глобальні соціальні та економічні зміни у зв'язку з розвитком та впровадженням у різноманітні сфери діяльності інформаційно-телекомунікаційних технологій. Рівень довіри громадян до держави знижується по всьому світу [15].

Найпрогресивніша частина суспільства налаштована на заміщення держави групою сервісних компаній, що працюють на конкурентній основі. Специфіка криптовалюти полягає у використанні технології Blockchain. Ця технологія є децентралізованою і позбавлена різних недоліків щодо безпеки здійснення платежів та зберігання різної інформації з транзакцій [17].

Ступінь розробленості теми обумовлена використанням наукових наук праць та практичних досліджень наступних авторів: К. Мацуура, П. Друкер, І.Д. Звєрєв,

В.П. Максимова, М.М. Скаткін, П.Р. Атутов, В.С. Ільїн. Роботи містять фундаментальні основи та погляди, що перетинаються з тематикою даної роботи.

Актуальність роботи та підстави для її виконання. Можливості арбітражу стають все більш поширеними в криптосекторі і пропонують трейдерам привабливий спосіб максимізувати прибуток з меншим ризиком. Криптоарбітражна торгівля – це процес купівлі цифрового активу на одній біржі та одночасного продажу на іншій з вищою ціною [5]. Це допомагає отримувати прибуток за рахунок процесу, пов'язаного з обмеженими ризиками. Правильна реалізація наддасть можливість початківцям в криптовалюті не нести збитки, а також дозволить навчити розробників використовувати різноманітну інформацію біржі в програмній реалізації.

Мета й завдання роботи. Мета дипломної роботи – розробка програмного засобу для торгівлі криптовалютою на біржі, з використанням стратегій максимально доходу при одночасному зниженні ризику.

Для досягнення вказаної мети необхідно виконати наступні завдання:

- висвітлити основні теоретичні аспекти об’єкта дослідження;
- здійснити порівняльний аналіз існуючих сучасних криптовалют та технологій їх побудови;
- дослідити аналіз обраних факторів та виділити найбільш статистично значущі для побудови засобу;
- розробити програмне забезпечення для обміну криптовалюти на різних біржах.

Об'єкт, методи й засоби розроблення. Об’єктом дослідження дипломної роботи виступають криптовалюти, як інструмент безготівкових розрахунків у платіжній системі різних країн та біржі, пов'язані з активами в криптовалюті, а також процес проведення транзакцій.

Для вирішення поставлених завдань використані наступні методи: аналіз та синтез, класифікація, візуалізація, розрахунок коефіцієнтів фінансового потенціалу, авторегресійний аналіз та прогнозування динаміки котирувань криптовалют, розрахунок показників інвестиційної привабливості фінансових інструментів.

В якості інструменту створення програмного засобу використовується мова програмування Python та декілька модулів для реалізації інтерфейсу і створення запитів до криптовалютних бірж. Модуль PyQt – це набір розширень фреймворку Qt для мови програмування Python. Бібліотека CCXT використовується для підключення та торгівлі з криптовалютними біржами та службами обробки платежів по всьому світу. Вона забезпечує швидкий доступ до ринкової інформації для аналізу, зберігання, візуалізації, алгоритмічної торгівлі, розробки індикаторів, програмування ботів, тестування стратегій та розроблення відповідного програмного забезпечення [11].

Можливі сфери застосування. Отримані результати можуть використовуватися для розробки рекомендацій щодо інвестування коштів у криптовалюту, а також для вдосконалення стратегії розвитку компаній, що займаються розробкою блокчейн.

Взаємозв'язок з іншими роботами. Використання інструментальних засобів та методів створення інформаційної системи робота виконувалася сумісно з роботами зі знаходження алгоритмів арбітражу для криптовалют.

РОЗІДЛ 1 ОСОБЛИВОСТІ КРИПТОВАЛЮТИ BITCOIN ТА РОЗПОДІЛЕНОЇ СИСТЕМИ BLOCKCHAIN

1.1 Аналіз систем управління базами даних

За останні роки технологія Blockchain дуже стрімко почала отримувати популярність в нашій країні. Хоча у світі вже давно існують та успішно працюють продуктивні рішення побудовані на основі Blockchain, такі як Bitcoin – інноваційна мережа для виконання платежів та цифрова валюта, Brave – браузер, проводить анонімні платежі власникам сайтів, та багато інших неймовірно успішних реалізацій [10].

Blockchain в самому найпростішому розумінні це розподілена система управління базами даних, до якої будь-який користувач може безпечно підключитись та здійснити транзакційний код. Транзакції зберігаються в спеціальних блоках даних, які створюються так, що ними неймовірно складно маніпулювати після того часу, як вони потрапили до системи Blockchain. Для того, щоб довільний блок потрапив до Blockchain необхідно виконати верифікацію даного блоку і добавити його до системи. Blockchain може вирішувати такі проблеми, як: швидкість виконання транзакцій, безпека та висока доступність.

Зараз розрізняють три системи керування базами даних: централізовані, децентралізовані та розподілені.

Централізовані системи

Централізовані системи мають лише одну точку управління, в якій відбувається весь контроль за системою (рис. 1.1). Всі процеси здійснюються тільки в даній точці, і в ній же приймаються рішення. Однак, це робить таку систему дуже слабкою, адже при будь-якому збою – єдиний центр управління обрушить всю систему [5].

Переваги централізованої системи:

- При відносно великому масштабі, система позбавляє від подвійної роботи, яка іноді виникає при присутності декількох точок управління. В системі тільки одна точка управління, тому не потрібно змушувати багато точок виконувати однакові функції, що звісно дає економію при колосальних масштабах системи.
- Легка реалізація та всі рішення приймаються вкрай швидко, так як наявна лише одна точка управління.

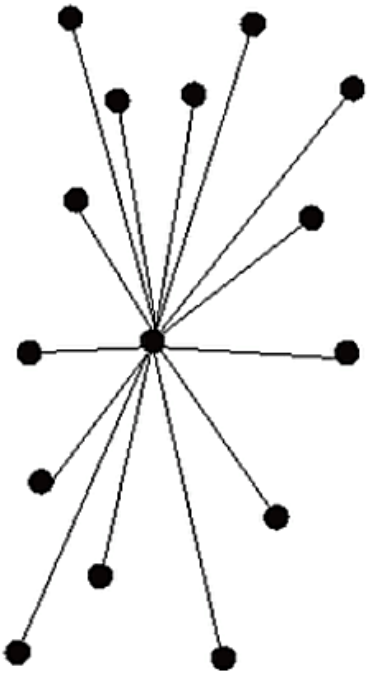

Рисунок 1.1 – Централізована система управління

Недоліки централізованої системи:

- Залежність тільки від однієї точки управління. Присутність однієї точки управління робить систему дуже уразливою, так як довільна атака на дану точку управління дестабілізує систему. Нескладно представити ситуацію

із сервером, коли атакується одне джерело інформації та немає резервних копій, – дані будуть втрачені.

- Система тільки з однією точкою управління дуже бюрократична за суттю, що додає в неї багато ієрархій та шарів.
- Система непрозора та схильна до шахрайства.

Приклади централізованих систем: центральний процесор сервера; банківські системи; франшизи громадського харчування («McDonalds»).

Децентралізовані системи

Децентралізовані системи – системи, в яких присутні декілька точок управління і диверсифіковані повноваження (рис. 1.2). Це дозволяє зробити систему менш чутливою до збоїв – вихід з ладу однієї точки управління ніяк не призведе до повного падіння всієї системи. Ієрархія даної системи наближена до горизонтальної у порівнянні з централізованою системою [5].

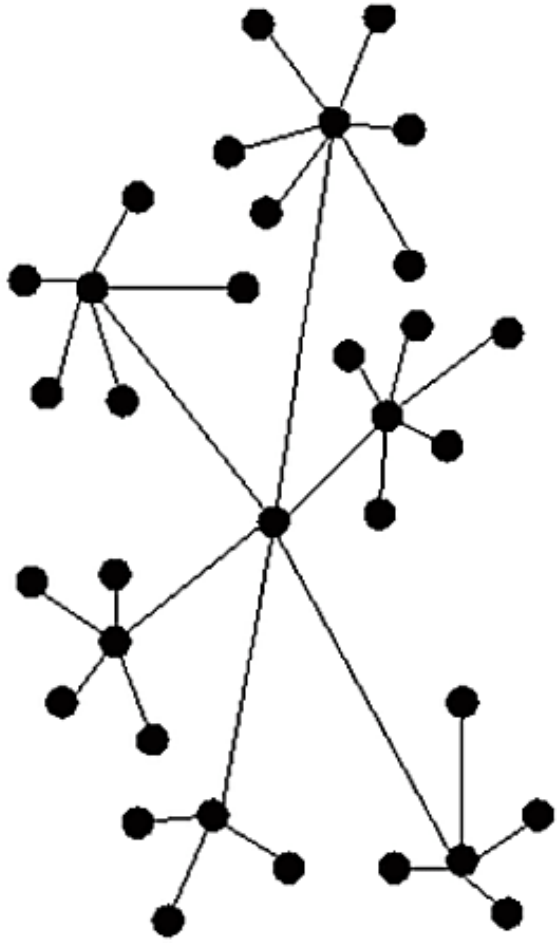

Рисунок 1.2 – Децентралізована система управління

Переваги децентралізованої системи:

- Система менше схильна до збоїв та атак, так як в ній декілька точок управління. Збій тільки в одній точці не приведе до дестабілізації системи, як у випадку з централізованою системою.
- В системі рішення приймаються на рівні, наближеному до користувача. Тобто, у органів (точок), які схвалюють рішення, набагато більше даних про кінцевого користувача (якщо це про продукт) або про людей (якщо це уряд).

Недоліки децентралізованої системи:

- Негативний економічний ефект, який пов'язаний зі збільшенням об'ємів системи. У даній системі через збільшення точок управління можна одержати «проблему дублювання завдань».
- Не дивлячись на те, що такі системи надійніші за централізовані, вони схильні до збоїв, тому їх не можна визнати повністю надійними.

Приклади децентралізованих систем: уряд, де є центральні та місцеві органи влади; системи постачання, такі як «Johnson&Johnson»; хмарні бази даних.

Розподілені системи

У розподілених системах довільна точка – це точка управління (рис. 1.3). Тому системи фактично несприйнятливі до виходу із ладу. Це не значитиме, що їх не можна зламати, однак, щоб створити падіння такої системи, зловмисник зобов'язаний взяти під свій контроль або змінити більше ніж 50% точок управління. Затрати на те, щоб здійснити подібне самостійно, зведуть нанівець майже всю частину прибутку та зроблять недоцільним з економічного боку спроби злому. Ієрархія даних систем повністю горизонтальна. Будь-яка точка управління дорівнює кожній іншій точці управління, і довільний суб'єкт та учасник системи є точкою управління. [15]

Переваги розподіленої системи:

- Відсутність посередників.
- Дану систему економічно недоцільно зламувати, що робить її надійною і найбезпечнішою з вище названих систем.
- Розподілена система прозора, завдяки чому здійснення шахрайства стає малоймовірним.

Недоліки централізованої системи:

- Дані системи вважаються новими, та їх технології перебувають в процесі постійного удосконалення.
- Для стабілізації даних систем потрібно багато часу і капіталізація.

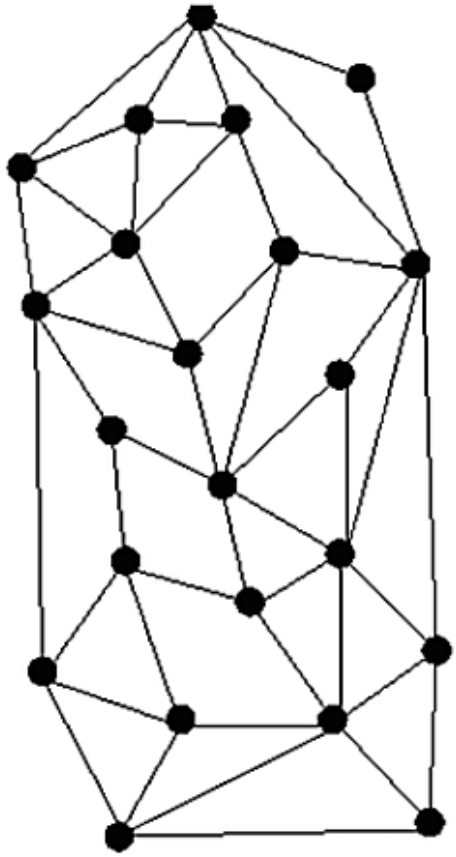

Рисунок 1.3 – Розподілена система управління

Приклади розподілених систем: мережі блокчейн; криптовалюта.

Блокчейн – це децентралізований цифровий реєстр, який дозволяє реєструвати транзакції без прийняття участі фінансового посередника, наприклад, банку. До суттєвих переваг блокчейну у порівнянні з існуючими платіжними системами відносять:

- зниження транзакційних витрат;
- децентралізація;
- прозорість.

1.2 Концепція побудови технології blockchain

Структура даних blockchain – пов'язаний між собою список блоків транзакцій, які упорядковані «в зворотному напрямі» [3]. Blockchain може зберігатися у базі даних або файлі. Фраза «блоки пов'язані назад» означає, що будь-який блок в ланцюзі має посилання на попередній блок. Blockchain часто зображується у вигляді вертикальної піраміди з блоками, які розташовані один над іншим, перший блок – платформа для всіх блоків, які розташовані вище [7].

Подібне представлення у вигляді складених блоків є причиною для застосовування таких термінів, як «висота» для позначення розміру відстані між першим блоком та «вершиною», яка вказує на доданий блок [7]. Кожний блок в blockchain визначається хеш-кодом [4], який згенеровано з використанням SHA-256 [6] – криптографічного алгоритму, використаного до заголовка блоку.

Будь-який блок посилається на попередній блок-предок, застосовуючи для цього хеш-код в заголовку попереднього блоку. Кожний блок включає хеш-код власного батька всередині заголовку. Послідовність хеш-кодів, що зв'язують блок із батьком створює ланцюжок. Даний ланцюжок тягнеться до першого з коли-небудь створених блоків, який називають блоком генезису.

Довільний блок має тільки одного єдиного батька. Блок може тимчасово мати декілька дочірніх блоків. Кожний із дочірніх блоків посилається на один єдиний батьківський блок.

Отримує зміни хеш-код дочірнього блоку у випадку, коли міняється хеш-код батьківського блоку. У випадку, коли отримує зміни батьківський блок, також отримує зміни і його хеш-код. Хеш-код батьківського блоку, який отримав зміни, відповідно потребує зміни в дочірньому блоці на посилання «хеш-коду попереднього блоку». Це свою чергу змінює хеш-код даного дочірнього блоку та надалі змінює посилання у попереднього блоку. Він змінює хеш-код власного попереднього блоку, і таким самим чином далі по ланцюгу. Каскадний ефект таких

змін забезпечує, що в разі, якщо за блоком фігурувало багато поколінь, в цей блок не можна добавити зміни без обов’язкового перерахунку всіх наступних за ним блоків. Чим довшим є такий ланцюг блоків, тим глибша історія в blockchain робиться незмінною.

Головною складовою одиницею blockchain є блок. Блок відображає структуру даних, специфічний контейнер, що об'єднує транзакції для включення в єдину загальнодоступну бухгалтерську книгу обліку [6]. Складовими частинами блоку є заголовок (Head), який містить метадані, за заголовком слідує довгий список транзакцій (Payload), (рис. 1.4.), та вони за обсягом займають велику частину всього блоку, що продемонстровано на рис. 1.4. Розмір такого блоку – 80 байт, середня транзакція – не менш ніж 250 байтів, в середньому блок може поміщати більше 500 угод [8]. Отже, повністю заповнений транзакціями блок за обсягом в тисячу разів більший, ніж заголовок.

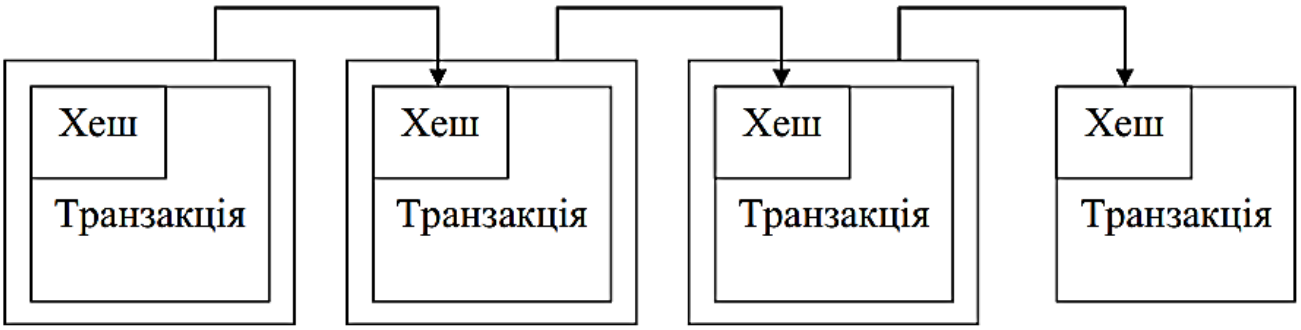

Рисунок 1.4 – Структура блоку транзакцій

Блоки, які потрапили в blockchain, що є дуже важливим, змінам не піддається. Будь-яке редагування даних про транзакції в blockchain заборонене. Можливо тільки дописувати нові блоки. Заголовок блока містить наступну інформацію: дата й час створення блоку, версія блоку, хеш-код заголовку блока, хеш-код попереднього блоку, спеціальні параметри nonce та bits, які вносяться при майнінгу та хеш-код усіх транзакцій в блоці [8].

Хеш-код заголовку блока об’єднує попередній блок з наступним в ланцюзі blockchain. Хеш-код прописується до наступного блоку, як хеш-код попереднього блоку, і так далі по ланцюжку.

В заголовку зберігається також хеш-код транзакцій поточного блоку. Він реалізується за алгоритмом, відомим, як дерево Меркла (Merkle tree) [4], інша назва – бінарне дерево хешів (рис. 1.5) [9].

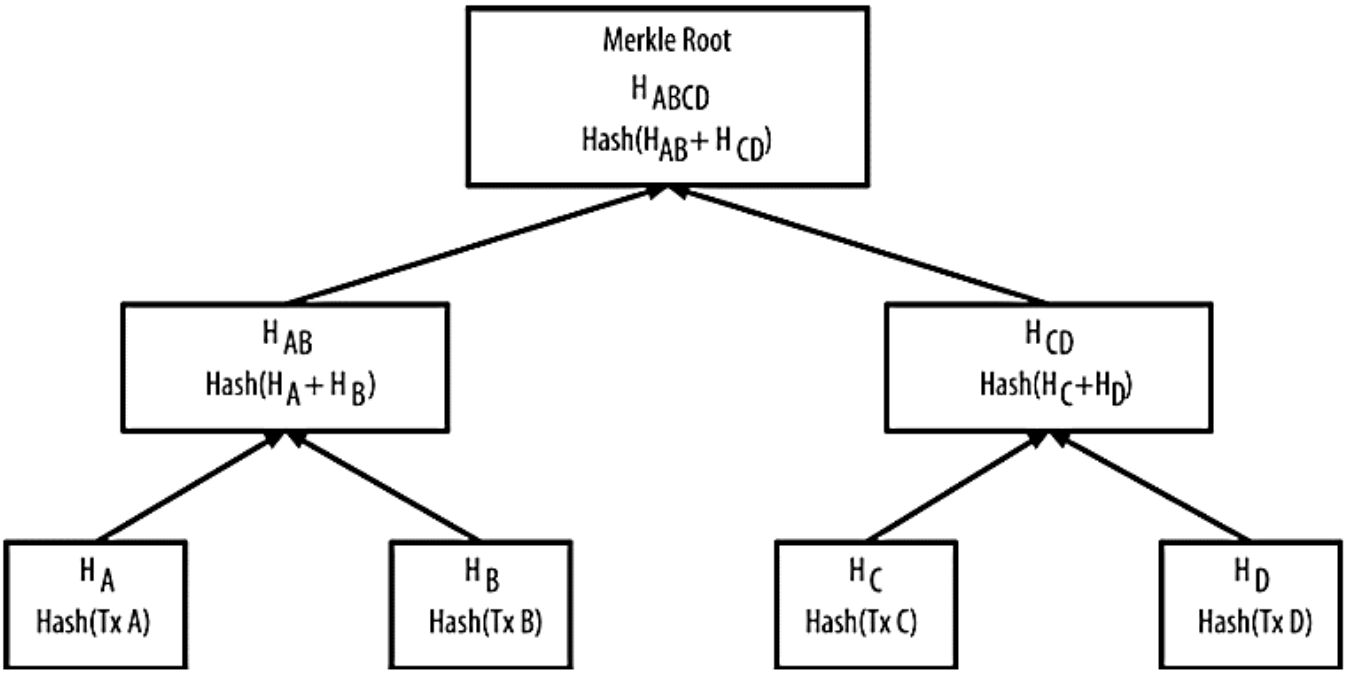

Рисунок 1.5 – Бінарне дерево хешей

На першому етапі обраховуються хеш-коди всіх транзакцій. Потім рахується сума всіх хеш-кодів пар транзакцій, далі обчислюються хеш-коди від суми отриманих пар хеш-кодів, по такій самій системі і далі, доки не одержимо єдиний хеш-код.

Заголовки дозволяють відслідковувати вміст відповідних блоків.

В blockchain біткойна записані транзакції у вигляду «З «address1» відправлено «N» біткойнів на «address2»». Транзакція, яка записана до блоку blockchain,

насправді складніша, тому що протокол біткойна містить поняття: Входи (In або Inputs) та Виходи (Out або Outputs) [9].

В електронних валютах транзакції через Входи (один або декілька) посилаються на Виходи (один або декілька) попередніх транзакцій та генерують Виходи (один або декілька) для використання в наступних транзакціях.

Нова транзакція *C* має в собі посилання на дві різні вхідні транзакції – *A* і *B*. На рис. 1.6 зображено, що вкінці на вході у транзакції отримаємо 0.008 BTC (0.005 + 0.003), і надалі розділяються на два виходи – на першу адресу надсилається 0.003 BTC, на іншу адресу відправляється 0.004 BTC. Залишок (0.001 BTC) формує комісію для майнера [8].

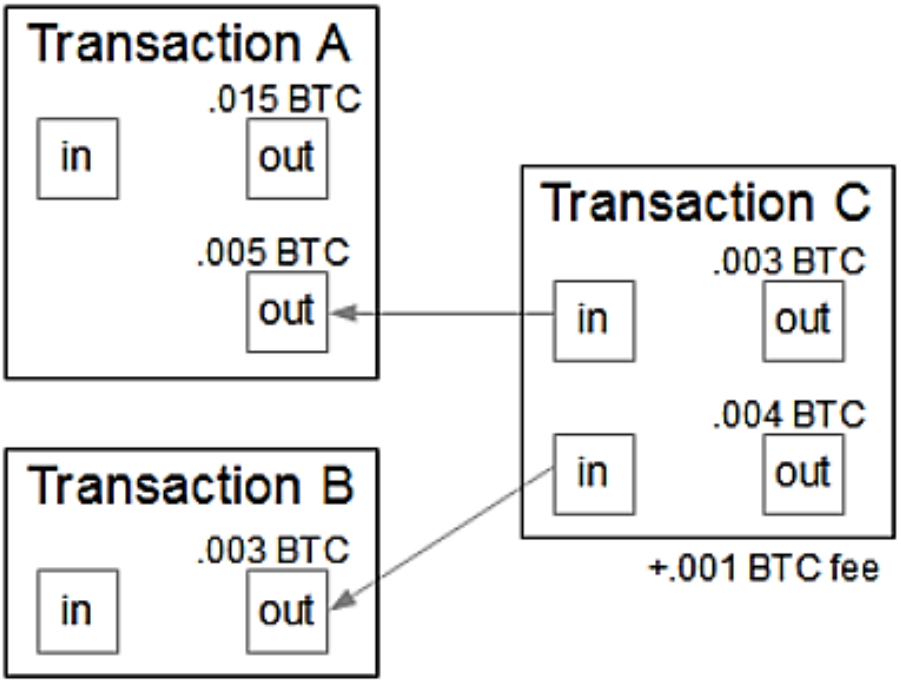

Рисунок 1.6 – Нова транзакція з посиланнями на дві вхідні транзакції

Блоком генезиса називають перший блок в blockchain [10]. Він створений десять років тому і є спільним предком для всіх блоків в blockchain [11]. Тому, якщо взяти довільний блок та простежити історію ланцюжка, то в кінцевому підсумку відлік дійде до даного блоку. Кожний вузол в blockchain завжди починається з

одного блоку, тому що блок генезису закодований статично в програмному забезпеченні клієнта, а це означає, що він не може змінюватися. Будь-який вузол завжди зберігає інформацію про хеш-код блоку генезису та його структуру, фіксований момент часу, коли він створений, та єдину транзакцію в блоці. Тому, кожний вузол має відправну точку для blockchain, своєрідний надійний «корінь», з якого завжди можна будувати безпечний blockchain.

Вузли всередині поміщають локальну копію blockchain, розпочинаючи з блоку генезиса. Локальна копія blockchain безперервно оновлюється, доповнюючись з кожною появою нових блоків. Отримавши вхідні блоки з мережі, вузол здійснює перевірку блоків, і далі зв'язує з існуючим вже ланцюжком на основі хеш-коду попереднього блока.

Наприклад, вузол має 277313 блоків в копії blockchain локально. Цей вузол «роздивляється» вміст поля previousblockhash нового блока, в якому знаходиться хеш-код «батьківського» блока. Цей хеш-код вузол вже знає який хеш-код останнього блоку в ланцюзі на висоті величини 277313. Саме цей новий блок стає дочірнім блоком останнього блока в ланцюзі та розширює поточний blockchain. Вузол доставляє новий блок в кінець існуючого ланцюга, що робить blockchain довшим з новою висотою, які рівна 277314 [12].

1.3 Особливості принципів роботи цифрової валюти bitcoin

Біткойн – це протокол, який реалізує платіжну систему та незалежну валюту [2]. Якщо розглядати інші платіжні системи або електронні гроші, наприклад, SWIFT, PayPal – це платіжні системи, що оперують вже існуючими валютами: євро, долар, фунт тощо. Біткойн є як платіжною системою, так і окремою валютою, це незалежна платіжна система, тобто немає організації, яка контролює її роботу [30].

Застосовуючи біткойн, можна відправити платіж будь-кому та куди завгодно. Для цього тільки потрібен доступ до мережі, адреса отримувача та цифровий гаманець. Обмеження, які характерні для міжнародного переказу відсутні. Не потребується ніяких додаткових дозволів для здійснення платежу.

Тому біткойн зацікавив людей, які підтримували свободу системи без цензурування. Як тільки ціна біткойну почала зростати, він почав привертати увагу підприємців і спекулянтів, що спробували заробити на коливанні курсу.

Для звичайної людини інтерес представляють відсутність потреби в реєстрації та можливість здійснювати платежі без залучення третіх сторін. На момент 2021 року по всьому світу біткойн використовували мільйони людей, а тисячі компаній приймають в якості оплати [38]. Деякі країни, зокрема Японія, признали його законним засобом платежу [9].

Блок транзакцій

Поняття blockchain в контексті біткойн – це база даних, яка включає транзакції, і вона загальна для всіх вузлів, які залучені до системи біткойн. Особливість її полягає в тому, що будь-який наступний блок підтверджує цілісність попереднього блоку, який, в свою чергу, підтверджує цілісність попереднього по відношенню до нього блоку і так до genesis block [19].

Забезпечується односторонній зв'язок всіх блоків та підтверджується факт того, що блок створений після появи попереднього. Дана організація інформації гарантує, що блок створений при наявності визнання всієї історії транзакцій за весь час існування біткойн. Кожен блок складається з двох частин: включених транзакцій та заголовка блоку.

Для того, щоб транзакція вважалась підтвердженою, її формат і підписи повинні перевірити майнери і далі групу транзакцій записати в спеціальну структуру [19]. Дані в блоках можна швидко ще раз перевірити. Довільний блок завжди містить інформацію про попередній блок. Всі блоки можна об’єднати в

один ланцюжок, який містить інформацію про виконані операції в цій базі. Найперший блок в ланцюжку – Genesis block, за яким учасники мають можливість створювати наступні блоки. Особливість genesis block полягає в тому, що він не розповсюджується при синхронізації вузлів, так як він має порядковий номер 0 та закладений до програмного забезпечення вузла мережі [19].

Блок складається з заголовка і списку транзакцій. У системі біткойнів першою транзакцією в блоці завжди вказується отримання комісії, яка стане винагородою користувачеві за створений блок.

Далі йдуть всі транзакції, які ще не записані в попередні блоки. Для транзакцій в блоці застосовується деревоподібне хешування, аналогічне формування хеш-суми для файлу в протоколі BitTorrent. Транзакції, крім нарахування комісії за створення блоку, містять всередині атрибута input посилання на транзакцію з попереднім станом.

Створений блок буде прийнятий іншими користувачами, якщо числове значення хешу заголовка рівне або нижче деякого числа, величина якого періодично змінюється. Так як результат хешування (функції SHA-256) є незворотним, немає алгоритму отримання необхідного результату, крім випадкового перебору. Якщо хеш не задовольняє умові, то в заголовку змінюється параметр nonce і хеш перераховується.

Зазвичай необхідна велика кількість перерахунків. Коли варіант знайдений, вузол відправляє отриманий блок іншим підключеним вузлам, які здійснюють перевірку блоку. Якщо помилки відсутні, то блок вважається доданим в ланцюжок і наступний блок зобов'язаний включити в себе його хеш [2].

Структура блоку

В таблиці 1.1 представлена структура блоку, яка передається мережею біткойн.

Таблиця 1.1 – Структура блоку в Біткоін

Поле	Значення	Розмір (у байтах)
MagicNo	0xD9B4BEF9	4
BlockSize	величина кількості байтів у блоці, включаючи всі дані транзакцій	4
BlockHeader	складається з шести полів	80
TxCounter	кількість транзакцій у блоці	1-9
Transactions	перелік транзакцій	N/A

У блоці передбачається кілька полів, перше з них – MagicNo – спеціальне константне число. Для протоколу біткойн воно завжди займає 4 байти і має саме таке значення. Застосовується воно для ідентифікації потоку інформації. Припустимо, є канал передачі, де проходить інформація від різних протоколів. Щоб визначити, що в деякий проміжок часу почався блок біткойн, можна застосовувати пошук по цьому значенню [2].

Після нього йде поле blockSize, яке також займає 4 байти і містить значення кількості байтів у блоці, включаючи всі дані транзакцій. За ним йде заголовок блоку, він складається з шести полів і завжди дорівнює 80 байтам [2].

Нижче розташовується лічильник транзакцій. Кількість транзакцій у блоці може бути настільки великою, що лічильник має розмір від 1 до 9 байт. Після йдуть дані самих транзакцій, їх розмір не визначений. На практиці блок може мати розмір від 100 байт і до 1 MB [2].

Ключовою складовою блоку є його заголовок. Тема блоку містить 6 полів. Їх перевіряють всі вузли мережі, навіть полегшені. Верифікація будь-якого поля виконується за суворо встановленими правилами, основні з яких навряд чи будуть змінені у майбутньому.

Розглянемо структуру заголовку блоку. У першому полі записується версія – 4 байти. Вона відповідає версії протоколу, за якою працював творець блоку. Далі

йде хеш-значення попереднього блоку, тобто хеш-значення від заголовку попереднього блоку, яке має довжину 256 біт.

Важливо відзначити, що хеш-значення отримано у результаті застосування подвійного хешування за допомогою хеш-функції SHA-2. Це поле містить 32 байти даних. Нижче знаходиться отримане спеціальним чином хеш-значення від усіх транзакцій у блоці – 32 байти, після чого слідує часова позначка (Unix Timestamp), яку встановлюють рівній часу створення блоку – 4 байти.

Після цього йде параметр складності – так званий bits – 4 байти. Останній параметр – nonce, який називають вирішенням завдання PoW конкретно для цього блоку. Він теж має розмір 4 байти. В результаті заголовок блоку в Біткоін завжди займає 80 байт [2].

Підтвердження транзакцій

Допоки транзакцію не було включено в блок, система вважає, що кількість біткойнів на якійсь із адрес залишається незмінною. У цей час існує технічна можливість оформити декілька різних транзакцій з передачі з однієї адреси одних і тих же біткойнів різним одержувачам. Але як тільки одна з подібних транзакцій буде включена до блоку, інші транзакції з цими біткойнами система вже буде ігнорувати.

Присутня невеличка ймовірність, що під час розгалуження дві подібні транзакції потрапляють до блоків різних гілок. Кожна з них вважатиметься правильною, лише при відмиранні гілки одна з транзакцій стане вважатися помилковою. При цьому час здійснення операції не буде мати значення. Таким чином, попадання транзакції до блоку є підтвердженням її достовірності незалежно від наявності інших транзакцій з тими ж біткойнами.

Транзакція вважається достатньо підтвердженою, лише якщо вона включена до найдовшого ланцюга та після блоку, у якому вона міститься, присутні ще 5 блоків. Інакше кажучи, потрібно дочекатися 3 – 6 підтверджень [2]. Якщо

враховувати, що блок з'являється в середньому 1 раз в 10 хвилин, нескладно порахувати, що повне підтвердження транзакції може зайняти до однієї години.

Відповідь на запитання, чому потрібно саме 6 підтверджень, надає математичний розрахунок: якщо один ланцюг випереджає інший на 5 блоків, при тому ж розподілі обчислювальної потужності, ймовірність «обігнати» той, що довший вкрай мала. У своїй статті Накамото Сатоші математично доводить це на основі наступного положення [30]:

$$q_z = \{1, \qquad \text{якщо } p \le q \quad \frac{q^z}{p}, \qquad \text{якщо } p > q$$

p – ймовірність, що наступний блок буде знайдений чесним вузлом;

q – ймовірність, що наступний блок буде знайдений атакуючим;

q_z – ймовірність, що атакуючий коли-небудь наздожене основний ланцюг, якщо він почав альтернативний z блоків назад.

Для прикладу, якщо зловмисник володіє 10% обчислювальної потужності усих валідаторів, а чесні вузли працюють в мережі з швидкою доставкою повідомлень, то ця імовірність буде меншою за 1/1000 [2].

Принцип роботи Біткойн

Біткойн існує лише у вигляді записів у розподіленій базі, в якій в загальнодоступному відкритому (незашифрованому) вигляді зберігаються геть всі транзакції, із зазначенням біткойн-адрес відправників/одержувачів, але абсолютно без інформації щодо реального власника цих адрес. У базі немає окремих записів про поточну кількість біткойнів у будь-якого власника. Лише на підставі ланцюжків транзакцій може стати зрозумілою поточна кількість біткойнів, пов'язаних з тією чи іншою біткойн-адресою. Тобто можна побачити, що на адресу надійшов 1 біткойн, а по іншій транзакції на цю ж адресу надійшло 2 біткойна, третя транзакція відправила з цієї адреси 1 біткойн. Але в базі не зберігається окремого запису, скільки всього зараз біткойнів числиться за даними адреси – просто надається можливість будь-якої миті це легко порахувати. Такі підрахунки автоматично

роблять клієнтські програми, користувач може і не помічати роздробленості інформації [21].

Ключі

Кожен користувач системи має змогу генерувати необмежену кількість пар ключів (алгоритм ECDSA [19]). Розмір закритого ключа становить 256 біт, а відповідного йому відкритого ключа – 512 біт [2]. Основне використання ключів – створення біткойн-адреси і підтвердження правомочності формування транзакцій. Але вони можуть використовуватися і для цифрового підпису або шифрування при листуванні. Створення нової пари ключів автономне і не вимагає підключення до мережі Інтернет.

Створені ключі зазвичай зберігають в спеціально-відведеному для цього зашифрованому файлі wallet.dat («гаманці»). Користувач вигадує пароль тільки для доступу до інформації з файлу «wallet.dat», тобто для доступу до своєї пари ключів. Для розпорядження біткойнів наявність цього файлу не є обов'язковою – у більшості випадків буде достатньо будь-яким довільним чином отримати закритий ключ [2].

Зберігати ключі можна на будь-якому носії, не лише на карті пам'яті, але і в паперовому вигляді. Існують різгоманітні онлайн гаманці, наприклад, Blockchain.info [40] або Coinbase [41], які досить прості у використанні. Але проблеми з сайтом такого сервісу можуть призводити до втрат.

Адресація

Адреси створюються за допомогою генерації асиметричної пари криптографічних ключів для чого не потрібне підключення до інтернету. Людина може мати необмежену кількість адрес, створюючи їх за своїм бажанням. Кожній потенційній адресі відповідає баланс, виражений в біткойнах. Всі адреси з ненульовим балансом записані в децентралізовану ланцюжок блоків транзакцій, захищену від змін [2].

Біткойн-адреса є послідовністю байт, отриманих в результаті перетворення відкритого ключа. Найчастіше кодуванням Base58 адресу записують як рядок довжиною до 34 літер латинського алфавіту і цифр. Перший символ адреси є завжди одиницею для звичайних адрес або трійкою для адрес створених з використанням мультипідпісу. Частина символів є контрольною сумою, яка перевіряє правильність основної частини адреси, яка, в свою чергу, є повністю випадковим результатом операцій хешування відкритого ключа. Адреси також можуть бути відображені у вигляді QR-кодів і інших штрих-кодів, придатних для машинного зчитування, наприклад, мобільними пристроями [2].

Якщо секретний ключ загублений, біткойн-мережа не прийме ніяких інших доказів права власності. Створити для існуючого адреси новий ключ неможливо, так як унікальній парі ключів завжди відповідає своя адреса.

Транзакції

Біткойни можуть бути передані будь-кому, хто повідомить коректну біткойн-адресу або відкритий ключ. Для передачі біткойнів поточний власник створює нову транзакцію, яка крім вказівок про кількість переданих біткойнів містить підписаний ініціатором хеш попередньої транзакції, по якій біткойни були отримані. Попередня транзакція стає «входом» поточної транзакції. Також вказується публічний ключ або біткойн-адреса нового одержувача («вихід»). Транзакція широкомовним запитом по відкритих каналах без шифрування відправляється в мережу. Решта вузли мережі, перш ніж прийняти транзакцію до обробки, перевіряють підписи. Правильність підпису свідчить, що ініціатор дійсно є власником секретного ключа для адреси «виходу».

Транзакції підтримують будь-яку кількість «входів» (посилань на попередні транзакції, в тому числі на користь різних адрес) і «виходів» (вказівки про одержувачів). Значення з усіх «входів» підсумовуються, і сума розподіляється по «виходах» [2].

Скасувати стандартну транзакцію неможливо, навіть при явній помилці або шахрайстві. Однак передбачено використання мультипідписів, в тому числі для угод за участю арбітра, що може забезпечити повернення біткойнів при невиконанні контрагентами обумовлених умов.

Передача біткойнів зводиться до вказівки умов подальшого розпорядження ними. Умови формуються із застосуванням відкритих ключів. Для наступної операції з цими біткойнами потрібен відповідний електронний підпис із застосуванням секретних ключів, що і буде виконанням умов. Мережа перевіряє підписи парними відкритими ключами. Окремі транзакції об'єднують разом з іншими транзакціями в спеціальну структуру. Інформація в блоках відкрита, не шифрується, її можна швидко перевірити ще раз. Кожен блок завжди містить свій порядковий номер і хеш попереднього блоку [9].

РОЗДІЛ 2 РІЗНОВИДИ КРИПТОВАЛЮТ ТА МЕХАНІЗМ КОНСЕНСУСУ

2.1 Існуючі різновиди криптовалют

Bitcoin – найпопулярніша криптовалюта, яка представляє собою небанківські гроші, що передбачають їх використання для розрахунків у мережі. Ця валюта стала родоначальницею цифрових грошей і зуміла свого часу продемонструвати феноменальну динаміку зростання.

3 січня 2009 року були створено перші 50 біткойнів, а перша їхня транзакція відбулася вже через тиждень – 12 січня 2009 року. Цього дня Сатоші Накамото відправив Хелу Фінні 10 біткойнів. Перший обмін біткойнів на національні гроші відбувся у вересні 2009 року.

Варто повторити, що біткойн не підкріплений ніякими матеріальними цінностями на відміну від звичайних грошових коштів. Ні емісійний фонд, ні банки не займаються підтримкою курсу криптовалюти. Це випливає з того, що криптовалюта з моменту її створення не була орієнтована на дане підкріплення. Ціноутворення у ній знаходиться в прямій залежності від реального попиту та пропозиції на біткойн [19].

Суть даної криптовалюти полягає в тому, що її вартість протягом часу тільки збільшуватиметься. Це пояснюється тим, що витрати на створення кожної нової монети перевищують вартість попередньої. Для захисту від інфляції запроваджено обмеження максимальної кількості монет, воно становить 21 мільйон, після чого вона просто залишатиметься у відкритому доступі та користуванні. Як і раніше, користувачі можуть займатися емісією валют, розплачуватись ними за покупки та послуги, а також заробляти на курсі BTC по відношенню до гривні та долара. Як скорочення замість «Bitcoin» часто пишуть латинські BTC. Такий запис схожий на

коди валют, однак подібний код міжнародним стандартом ISO 4217 поки що не надано. Найменшою одиницею біткойн нині є Сатоші (Satoshi). Сатоші – це одна стомільйонна біткойну (0,00000001 BTC). SHA256 – саме на цьому алгоритмі побудований класичний біткойн.

З часом стали зароджуватися й інші криптовалюти, які також набирають популярності та беруть участь у транзакціях [17].

Ethereum (від англійського слова ether – «ефір», Ефіріум) – платформа для створення децентралізованих онлайн-сервісів на базі блокчейну, працюючих з урахуванням розумних контрактів. Принцип роботи полягає в тому, що сторони підписують розумний контракт, використовуючи методи, аналогічні підписанню відправлення коштів у криптовалютних мережах. Після підписання сторонами договір набирає чинності. Для забезпечення автоматизованого виконання зобов'язань договору, обов'язково потрібне середовище, яке дозволяє повністю автоматизувати виконання пунктів договору. Це означає, що розумні контракти зможуть існувати лише всередині середовища, що має безперешкодний доступ виконуваного коду до об'єктів договору.

Усі умови контракту повинні мати математичний опис та чітку логіку виконання. У зв'язку з цим, перші розумні контракти мають на меті формалізації найпростіших взаємин, які складаються з малої кількості умов. Отримавши безперешкодний доступ до об'єктів договору, розумний контракт відстежує за зазначеними умовами порушення або досягнення пунктів і приймає рішення, базуючись на запрограмованих умовах. Таким чином, основний принцип розумного контракту полягає у повній автоматизації та достовірності виконання договірних відносин у блокчейні [20].

Вона створена засновником журналу «Bitcoin Magazine» Віталієм Бутеріним. Її технологія дає можливість реєстрації будь-яких угод із довільними активами на основі розподіленої бази контрактів типу blockchain, не вдаючись до звичайних

традиційних юридичних процедур. Ця можливість більш конкурентна по відношенню до системи реєстрації угод біткойна.

Журнал The Economist вважає, що ця технологія знаменує новий етап фінансових технологій. Офіційно проект запущено у 2015 році. На відміну від біткойна, ефір є відкритим співтовариством, і його засновники та розробники відомі широкый публіці. У проекті можна здійснювати транзакції будь-якого типу, він представляє собою щось подібне до програмованого модуля, в якому всі учасники зайняті написання смарт-контрактів. Що стосується майнінгу (видобуток криптовалюти в блокчейні, методами обчислення криптографічних алгоритмів), то він можливий тільки на ПК з 64-розрядним Windows. Ethash (DaggerHashimoto) – алгоритм шифрування, що знайшов застосування у криптовалюті Ethereum.

Ріппл (XRP, Ripple) – криптовалютна платформа для платіжних систем, яка орієнтована на операціях з обміном валют без поворотних платежів. Розроблено компанією Ripple. Система запущена у 2012 році. Планується, що у системі буде випущено 100 мільярдів таких монет. Заробити її майнінгом теж не вийде, бо всі монети вже здобуті системою та розподіляються учасникам. Їх можна або купити через біржу, або отримати безкоштовно, беручи участь у розподілених обчисленнях. Алгоритм шифрування ECDSA.

Лайткойн (LTC, litecoin) – електронна платіжна система, що використовує однойменну криптовалюту. Litecoin з'явився в 2011 році, завдяки інженеру Google – Чарльзу Лі [21]. Однією з небагатьох відмінностей лайткоїну є швидкість обробки транзакцій – вона швидше ніж у біткойна.

Якщо в біткойні блоки створюються кожні десять хвилин, то в Litecoin це здійснюється швидше – кожні 2,5 хвилини. Тому Litecoin може обробити більше транзакцій, ніж у системі біткойна. Кількість криптовалюти обмежена, і не перевищує 84 мільйони одиниць. Алгоритм шифрування Scrypt. Доджкойн (Dodge, dodgecoin) була представлена 8 грудня 2013 року. Dogecoin створений програмістом

з Портланду, Біллі Маркусом. Він хотів створити криптовалюту, яка була б ближчою для великої демографічної групі, а також дистанціюватися від історії біткойна [22].

Даш (Dash, DASH), раніше відома як Darkcoin та XCoin – відкрита децентралізована платіжна система у формі криптовалюти на базі блокчейна, що використовує механізм анонімних транзакцій. Запуск «даша» стався ще 2014-го року. Він отримав назву «темної конячки» через свою специфіку та первісної назви. Програму-гаманець можна завантажити прямо з офіційного сайту компанії. У даної системи висока анонімність та швидкість проведення розрахунків. Може буде випущено до 22 мільйонів дашів, хоча на практиці це число може бути меншим.

Щодня на біржах проводиться угод на кілька десятків тисяч доларів. Повний розрахунок створеного блоку проводиться за 2,5 хвилини, як і у лайткоїну. Як і більшість криптовалют, у DASH немає централізованого управління – емісія відбувається при майнінгу. З отриманого майнерами винагороди 90% розподіляються між майнерами та операторами майстернод. Інші 10% прямують на фінансування схвалених проектів [23].

Monero (XMR) – криптовалюта на основі протоколу CryptoNote, орієнтована на підвищену анонімність транзакцій. CryptoNote – протокол прикладного рівня, на базі якого створено сімейство анонімних криптовалют, найвідомішими з яких є Bytecoin та Монера. Анонімність у CryptoNote створена за рахунок застосовування кільцевих підписів та одноразових адрес [24]. Криптовалюта з'явилася 18 квітня 2014 року. Емітується за допомогою спеціальних криптопрограм. Має високий рівень надійності та захисту, а тому входить у десятку топ популярних цифрових грошей.

Загалом до 2018 року у світі відомо понад 2000 видів різної цифрової валюти (таблиця 2.1), багато з яких вже встигли припинити своє існування. У просторах інтернету їх називають «Альткоіни№ (англ. Altcoins) – назва всіх криптовалют, крім

біткойну. Ключовою особливістю криптовалют є відсутність будь-якого зовнішнього та внутрішнього адміністратора. Тому податкові, банки, судові та інші приватні або державні органи не мають можливості впливати на транзакції довільних учасників платіжної системи.

Таблиця 2.1 – Системний аналіз різних видів криптовалют

Криптовалюта	**Рік випуску**	**Скорочення**	**Алгоритм шифрування**
Augur	2015	REP	Smart contract
Bitcoin	2009	BTC	SHA-256
ByteCoin	2012	BCN	CryptoNight
Dash	2014	DASH	X11
Dashcoin	2014	DSH	CryptoNight
DigiByte	2014	DGB	SHA256
Dogecoin	2013	DOGE	Scrypt
Einsteinium	2014	EMC2	Scrypt
Ethereum	2015	ETH	Dagger-Hashimoto
EthereumClassic	2015	ETC	Dagger-Hashimoto
Expanse	2015	EXP	Dagger-Hashimoto
FoldingCoin	2014	FLDC	Stanford Folding
Gridcoin	2013	GRC	BOINC
Litecoin	2011	LTC	Scrypt
Monero	2014	XMR	CryptoNight
Nautiluscoin	2014	NAUT	NXT
Navcoin	2014	NAV	X13
NEM	2015	XEM	blockchain
Peercoin	2012	PPC	SHA-256
PinkCoin	2014	PINK	X11
Potcoin	2014	POT	Scrypt
Ripple	2013	XRP	ECDSA
Siacoin	2015	SC	blake2b

Steemit	2016	STEEM	SHA-256
Syscoin	2014	SYS	Scrypt
Vcash	2014	XVC	Blake25
VertCoin	2014	VTC	Lyra2RE
ViaCoin	2014	VIA	Scrypt

Передача криптовалют необоротна – ніхто не в змозі заблокувати, скасувати, оскаржити або примусово (без приватного ключа) виконати транзакцію. Проте учасники правочину мають право добровільно тимчасово взаємно блокувати свої криптовалюти, як заставу або встановити, що для завершення/скасування угоди потрібна згода всіх сторін.

Так як загальна популярність та попит на онлайн-валюту збільшилися з моменту їх створення, а саме біткойна в 2009 році, то виникають побоювання, що така нерегульована та непідвладна глобальна економіка, яку пропонують криптовалюти, може стати загрозою для суспільства та світової економіки загалом. Дане занепокоєння виникає у зв'язку з тим, що цифрові гроші можуть стати, і в міру їх розвитку стають, інструментами для анонімних інтернет-злочинців.

2.2 Емісія криптовалюти

З появою поняття криптовалюти доцільно використовувати такі поняття, як майнінг та майнер. Майнінг (від англійського слова mining – видобуток корисних копалин) означає видобуток криптовалют, тобто здійснювати емісію криптовалюти, відповідно, майнер (від англійської слова miner – шахтар) – це той, хто здійснює майнінг.

Емісія нової валюти відбувається за заздалегідь заданим алгоритмом. На емісію не може впливати держава або приватна особа, як це відбувається, наприклад, у національних валютах, коли держава на законодавчому рівні регулює

розмір емісії. Емісія криптовалют є винагородою за проведення транзакцій. Під час проведення транзакції всі операції записуються в блок. Кожен блок має бути підтверджений відповідно до алгоритму хешування, що дозволяє гарантувати правильність проведення операції [16].

Майнінг – це спосіб отримання нових блоків (монет) криптовалюти за допомогою вирішення комп'ютером певних криптографічних, математичних та інших видів обчислень. Це приносить певну кількість електронних грошей, що вносяться до загальної скарбнички та реєструються у громадській «бухгалтерській книзі» (blockchain).

Майнеру необхідно підібрати хеш, який підходить до всіх транзакцій у мережі та забезпечить отримання «особливого ключа». Хеш, який шукає майнер являє собою код, що складається з хеша попереднього блоку, суми контрольних чисел транзакцій, що відбулися за останні 10 хвилин (бо саме за цей час формується один блок) та випадкового числа. Як тільки один з майнерів знаходить шуканий хеш, блок закривається і майнер отримує свою винагороду. Приклад хешей для однієї і тієї ж фрази, але з різними значеннями додаткового параметра представлено на рисунку 2.1.

```
«Hello, world!1» => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
«Hello, world!0» => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
«Hello, world!1» => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
«Hello, world!2» => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
«Hello, world!4248» => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
«Hello, world!4249» => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
«Hello, world!4250» => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

Рисунок 2.1 – Хеші з однаковими фразами, але різними додатковими параметрами

Як було зазначено вище, за підтвердження кожного блоку транзакцій надається певна винагорода. На початковому етапі генерації блоків вона становило 50 біткойнів за блок. Після формування кожних 210 000 блоків розмір винагороди знижується вдвічі [6].

Перше зменшення розміру винагороди відбулося 28 листопада 2012 року [28] і знизилося вдвічі (до 25 BTC). У середньому зменшення відбувається кожні чотири роки. У липні 2016 року розмір винагороди опустився до позначки 12,5 монет за підтвердження блоку транзакцій. Наступне зниження –2020-й, коли винагорода за здобутий блок складе 6,75 біткойн. Звідси випливає, що чим швидше відбувається підтвердження блоку, тим швидше буде досягнуто максимальна кількість монет у системі.

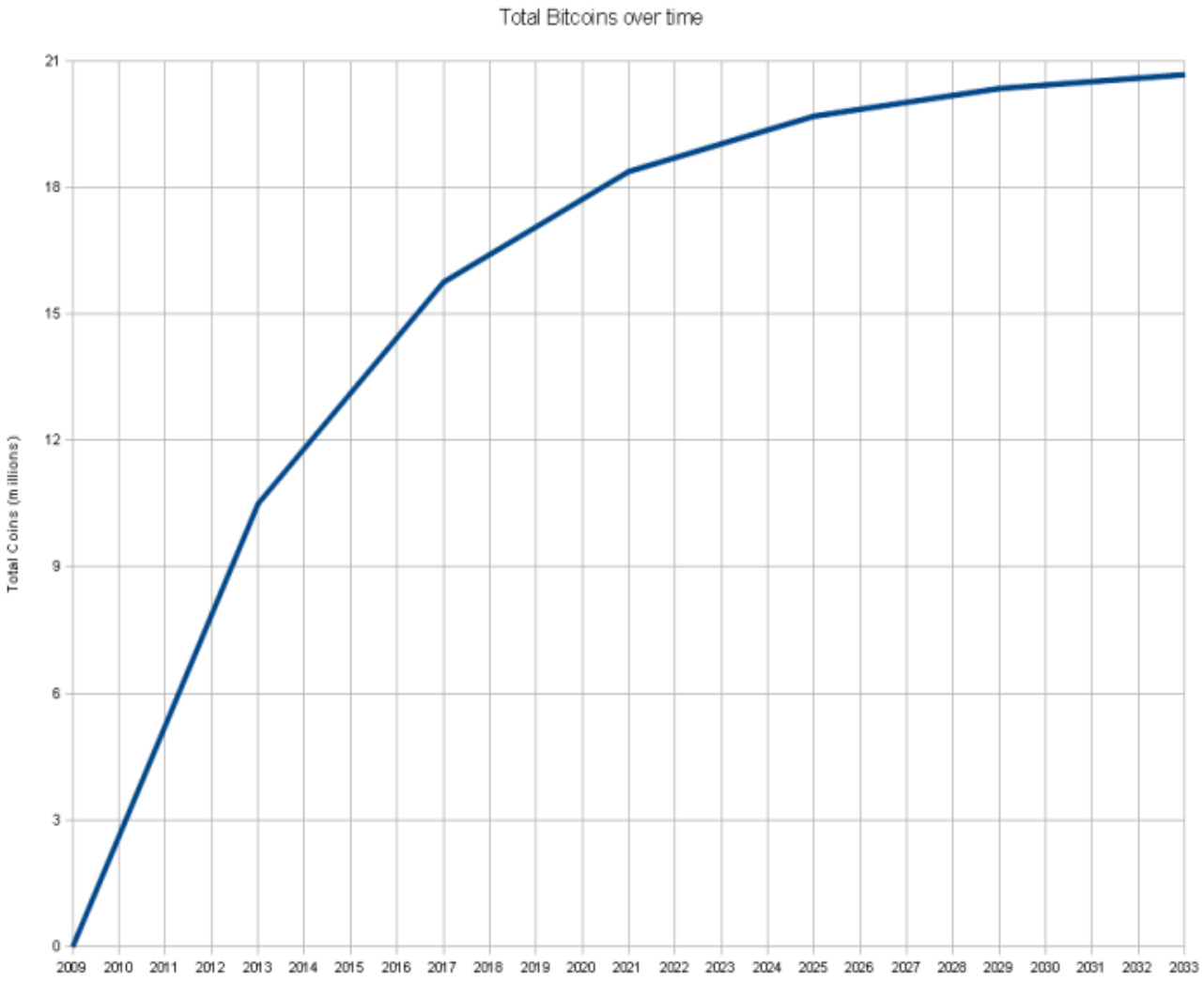

Рисунок 2.2 – Графік зміни складності обчислення

Оскільки неможливо передбачити кількість обчислювальних потужностей, які використовують користувачі для обробки транзакцій, це могло дуже сильно впливати на розмір емісії нової валюти та розподіл її між користувачами системи. Це, в свою чергу, може призвести до сильної залежності курсу від вартості обчислювальних потужностей та електроенергії.

Однак для цього в алгоритмі передбачено перерахунок складності отримання черговий ключ для підтвердження блоку. Цей параметр перераховується кожні 2016 блоків таким чином, щоб підтримувати середню швидкість формування

розподіленої БД на рівні 2016 блоків на два тижні. В результаті один блок повинен створюватися приблизно раз на десять хвилин.

Перерахунок складності можливий завдяки записам усередині їх транзакцій часу створення. Зміна обчислювальної складності за весь час існування мережі представлено на рисунку 2.2 [19].

Таким чином, розподіл нагороди за перевірку блоків також відбувається кожні десять хвилин. Оскільки існує лише одне число, яке служить ключем для підтвердження блоку транзакцій, а майнингом поточного блоку можуть займатися десятки чи сотні тисяч користувачів.

Майнінг не єдина технологія створення нових блоків, існує таке поняття як Форжинг (від англійського слова Forging – кування) або Мінтинг (від англійського слова Minting – карбування монет) – це створення в різних криптовалютах нових блоків у blockchain на базі підтвердження частки володіння з можливістю одержати винагороду у формі комісійних зборів та нових одиниць.

Різні криптовалюти можуть мати додаткові умови для участі у форжингу. Наприклад, Nxt (криптовалюта) дозволяє приєднатися до процесу лише для тих сум, які мають не менше 1440 блоків підтверджень [31]; Emercoin вимагає, щоб активи, що беруть участь в оцінці частки були депоновані (заморожені) не менше 30 днів. В цьому випадку винагорода стає схожою на нарахування відсотків за вкладом. Зазвичай використовується лише одна технологія (PoW або PoS), але в Деякі криптовалюти використовують комбінації з них.

Для видобутку криптовалюти достатньо мати комп'ютер із великою обчислювальною потужністю. Спочатку вважалося, що для майнингу головним складовою комп'ютера був процесор. Але пізніше майнери усвідомили, що використання відеокарт для видобутку криптовалюти є більш ефективним, оскільки за її допомогою процес майнінгу відбуватиметься набагато швидше. При виборі відеокарти саме для майнингу, головним чином необхідно враховувати обсяг

відеопам'яті, тип пам'яті, розрядність шини, можливість розгону та охолодження. Тобто, перший крок – придбання потужної відеокарти та її встановлення. Максимальна кількість відеокарт – 6 штук. Продуктивні пристрої відрізняються високою тепловіддачею. Досягати вона може 120 градусів за Цельсієм. З цієї причини необхідно забезпечити належне охолодження для запобігання перегріву. Вихід із положення – встановлення додаткового вентиляційного обладнання, що дозволяє досягти ряд переваг: попередження перегріву; збільшення терміну експлуатації комп'ютера; підвищення продуктивності майнингу. Ігнорування необхідності охолодження призводить до швидкої деформації напівпровідників на платах.

Суть всього процесу дуже проста: чим потужніша ваша відеокарта, тим більша у неї пропускна здатність (Гбайт/сек), більша частота пам'яті, тим більше мегахешів за секунду (MH/s, одиниця виміру швидкості) вона може обробляти і тим більше криптовалюти отримувати.

Комплекс для виробництва криптовалюти має в IT середовищі назву – ферми для майнингу криптовалют (Crypto Mining Farm). Ферма репрезентує собою сукупність потужних комп'ютерів та необхідні обчислення.

Заробіток від майнингу ферми залежить від наступних факторів:

- виробник чіпів відеокарт. Різні відеокарти заточені під видобуток конкретної криптовалюти. Наприклад, на моделях Nvidia (модель відеокарти) зручно майнити Zcash (криптовалюта), на AMD (модель відеокарти) – Ефір (криптовалюта). Неправильний вибір відеокарти веде до зменшення продуктивності, що негативно впливає на дохід майнера;
- кількість відеокарт. Чим більше відеокарт, тим вища потужність.

Найкращий варіант – покупка безлічі пристроїв із середніми показниками. Часи видобутку біткойну через стаціонарні комп'ютери вже скінчилися.

Для видобутку криптовалютного «золота» – біткойна застосовують інтегральні схеми особливого призначення ASIC-майнери (абревіатура от англійської application-specific integrated circuit). Це невелика установка служить для єдиного завдання – видобуток криптовалюти. Жодних інших завдань ASIC не вирішує. Ключовий показник майнерів – це електроспоживання та хешрейт. У розробку подібного обладнання майнингу біткойна вкладено чимало коштів, і створити його самостійно, своїми руками не вийде. Творці ASIC пристроїв значно зуміли збільшити швидкість видобутку віртуальних монет та при цьому знизити рівень споживання електроенергії.

В даний час розрізняють три основні види майнингу.

Одиночний майнинг. Під цим видом майнингу розуміється те, що вирішення криптографічного рівняння здійснюється самостійно, тобто використовуючи лише свій персональний комп'ютер. Перевага соло майнінгу полягає в тому, що всі видобуті в блоці монети не потрібні ні з ким поділяти. Основними недоліками даного виду майнінгу є те, що пошук рентабельного блоку може зайняти велику кількість часу, а також те, наскільки вдало обрано криптовалюту.

Майнинг через пули. Пули (від англійського слова pool – басейн) – це сервери, які можуть об'єднувати потужності персонального комп'ютера відразу багатьох майнерів для підвищення ймовірності знаходження блоку, тим самим розподіляючи завдання. Обчислювальна потужність сервера складається з потужностей ПК всіх учасників пулу, що дає змогу видобути новий блок за досить короткий проміжок часу [3].

Нагорода за блок, який здобув пул, поділяється між усіма його учасниками згідно з контрактом. Тому, у пула набагато більше шансів на отримання винагороди, ніж у одиночного майнера. Сайти пулів зазвичай вказують на офіційні сайти криптовалют у розділі «pool» або на тематичних форумах, таких як «Bitcoin

Talk »[13]. Основні критерії вибору пулу – це загальна потужність видобутку обраної криптовалюти та комісія при виведенні.

Хмарний майнинг. Під хмарним майнингом розуміється випадок, коли майнер платить гроші будь-якій компанії за обладнання, після чого дана компанія бере на себе відповідальність за встановлення обладнання та його налаштування для роботи. Переваги цього виду майнингу полягає в тому, що майнеру не потрібно мати якихось спеціальних знань. Йому достатньо платити гроші сервісу та отримувати дохід. Ще однією перевагою хмарного майнингу вважається те, що майнеру не обов'язково купувати обладнання цілком. Він може придбати будь-яку частину обладнання (у цьому випадок, дохід буде пропорційний до вкладеної суми). У цього виду майнінгу існують такі недоліки, як наявність націнки при покупці обладнання та неможливість повернення свого обладнання під час закриття підприємства [23].

Заробіток на криптовалюті залежить від собівартості «видобутку» чергової монети. Тут є елемент ризику через високу волатильність криптовалют. Але водночас створює непогані можливості з погляду окупності. Як правило, це місяці, а не роки, як у звичайному бізнесі.

Слід зазначити, що не тільки волатильність криптовалюти є негативним фактором. Швидке старіння техніки – такий самий ризик, як і мінливість ціни самої валюти. Це відбувається через постійне вдосконалення технічних засобів – зміни поколінь пристроїв. Навіть якщо пристрої не застаріють морально, вони перестають бути ефективними у закладених принципах роботи.

Для рівномірного зростання мережі та залучення нових учасників з метою її стійкості відбувається збільшення складності обчислення ключа блоку – це породжує зростання конкуренції серед майнерів. Витрати майнерів полягають у придбанні високопродуктивного обладнання та вартості електрики для його роботи. Таким чином, кожен новий біткойн має під собою реальний матеріальний ресурс,

що є кінцевим. Для появи нової монети потрібен час для обчислень, обладнання та електрика.

2.3 Механізми досягнення консенсусу

Інформація у blockchain повинна бути цілісною та добре захищеною від зловмисників. Алгоритми консенсусу прямо виконують такі функції, тому вони найважливіший елемент технології blockchain.

Оскільки дані у blockchain розподілені та немає одного серверу, розподілені учасники системи зобов'язані якось погоджувати валідацію транзакцій, які надходять до мережі. Важливо відділяти алгоритм консенсусу від поняття протоколу [9].

Протокол прописує правила, за якими працює система – як повинні взаємодіяти учасники мережі, яку інформацію вони можуть передавати та які вимоги до вдалої валідації блоків. Алгоритм втілює роль механізму, який здійснює перевірку, що правила встановлені протоколом виконуються – він валідує підписи та баланси, що підтверджують транзакції, а також виконує перевірку блоків.

Консенсус означає, що всі сторони погоджуються щодо конкретного рішення. Що стосується мережі blockchain, члени мережі досягають консенсусу щодо вмісту blockchain. Blockchain – це децентралізована система, що складається з різноманітних суб'єктів, які діють залежно від власних інтересів та наявних у них даних. Кожен раз, коли транзакція транслюється по мережі, вузли мають можливість включити дану транзакцію в копію реєстру або проігнорувати її. Коли більшість учасників мережі приймають дане рішення про прийняття деякого стану – досягається консенсус.

Основною проблемою в багатоагентних системах і розподілених обчисленнях є досягнення надійності системи при наявності неробочих процесів.

Найчастіше для цього необхідно, щоб процеси скоординували між собою певне значення, яке необхідне під час обчислення. Такі процеси описуються як консенсус. Для того, щоб консенсусний протокол був безпечним, він повинен бути відмовостійким. [23]

Зараз існує багато алгоритмів консенсусу, що застосовуються в різних протоколах blockchain:

- Apache Kafka;
- PoS (Proof-of-Stake);
- PoW (Proof-of-Work);
- PoC (Proof-of-Capacity);
- BFT (Byzantian-Fault-Tolerance);
- PoET (Proof-of-Elapsed-Time);
- DPoS (Delegated-Proof-of-Stake);
- BFT (Byzantian-Fault-Tolerance).

Proof-of-Work (PoW)

Один з популярних консенсусів, адже почав застосовуватися ще у Біткойні. Насправді, концепція Proof-of-Work описана ще у 1993 році в роботі «Pricing via Processing Or Combatting Junk Mail, Advances in Cryptology» авторства Дворк Синтії та Наор Моні. Хоча термін тоді ще не був введений, автори запропонували ідею того, що для отримання доступу до загального ресурсу, користувач зобов'язаний обрахувати достатньо складну, але обчислювальну задачу, аби запобігти зловживанням ресурсів [10].

Термін з’явився у 1999 році в статті «Proofs of Work and Bread Pudding Protocols» Аpі Джуелс та Маркуса Якобссона [11]. Тобто мета концепції така, що майнерам дається задача, яку вони зобов'язані порахувати за деякий проміжок часу (у Bitcoin цей час становить близько 10 хвилин). Задача – «Знайти значення x, щоб хеш SHA(x) містив N старших нульових бітів».

У Bitcoin час вирішення задачі сталий, тому що кількість біт, яку необхідно вирахувати динамічна та повністю залежить від кількості учасників. Функція, яка вираховується – SHA-256. Коли один учасник мережі знайде правильну відповідь, усі інші просто звіряються з ним. І коли більшість завалідує знайдену відповідь – консенсус досягнуто та блок записано.

Майнери мають свою зацікавленість у цьому, адже за будь-яку записану та підтверджену транзакцію вони одержують плату. І якщо людина, хоче щоб її транзакція найшвидше потрапила до мережі, можна запропонувати майнерам більшу плату – тоді час очікування підтвердження транзакції зменшиться. Але у такого алгоритму є недолік – він вимагає велику кількість енерговитрат та потужне апаратне забезпечення.

Proof-of-Stake (PoS)

Інший за популярністю алгоритм консенсусу вперше реалізований у валюті PeerCoin у 2012 році. Нода, яка має найбільшу кількість токенів має більше шансів згенерувати наступний блок. Тобто чим більший баланс, тим у найкращому становищі знаходиться нода.

У даному підході майнерам доводиться хешувати дані, але тут складність залежить від балансу. У порівнянні з Proof-of-Work, даний алгоритм не вимагає великих енерговитрат. Також до переваг можна віднести те, що для проведення атаки на мережу, зловмиснику потрібно отримати більше токенів і тоді йому стане невигідно знецінювати власний токен. Але тут також є недоліки – може появитися група осіб, яка спробує тримати токени тільки у своїх руках. У такому випадку під сумнів може ставитися сама ідея децентралізованої мережі [10].

Delegated-Proof-of-Stake (DPoS)

Delegated-Proof-of-Stake – альтернатива Proof-of-Work та разом з тим удосконалення Proof-of-Stake. Алгоритм запропонований у 2014 році

Деніелом Ларимером та застосовується у криптовалютах Steem, Bitshares, Lisk та Ark [12].

Мета алгоритму полягає у тому, що учасник може віддати свою «роботу» іншим. Можна делегувати свій голос іншому учаснику мережі, і той буде підтримувати роботу мережі від вашого імені. Оскільки це удосконалений PoS, то чим більший баланс токенів, тим більшу вагу має голос учасника мережі. У такій системі винагорода за записаний блок розділяється між учасниками, що проголосували за того, хто записав блок.

Перевага у порівнянні з класичним Proof-of-Stake – учасники мотивовані працювати чесно, адже у довільний момент за вас можуть перестати голосувати. Також він працює швидше за класичний варіант.

Proof-of-Authority (PoA)

Термін Proof-of-Authority запропонований у 2017 році одним із засновників мережі Ethereum Гевіном Вуду [13]. Блоки записують перевірені валідатори, що заздалегідь обираються та є модераторами системи. Тут має цінність репутація, а не кількість токенів.

Таким чином blockchain за певним алгоритмом обирає валідатора, який добавить наступний блок.

Важливо зазначити, що просто так стати валідатором дуже важко, адже потрібно вкласти деяку кількість фінансів, а також заробити довіру інших учасників мережі, аби вони голосували за нього. Такий процес гарантує, що валідатором стане не пересічна людина.

Proof-of-Importance (PoI)

Proof-of-Importance зараз активно використовується у криптовалюті NEM. Даний алгоритм надає перевагу користувачам, які здобули хорошу репутацію у мережі – «спочатку ви працюєте на репутацію, потім репутація працює на вас». Репутація підвищується з активним життям у екосистемі blockchain та взаємодії з

іншими учасниками. Чим краща репутація – тим більший шанс на створення наступного блоку [14].

Proof-of-Importance вирішує проблему Proof-of-Stake, коли один учасник або група людей мають можливість контролювати всю мережу, отримавши більше токенів. Тут же кількість токенів на балансі не збільшують шанси на створення блоку. Крім того, коштами потрібно активно користуватися, адже торгувати ними вигідніше, ніж просто тримати на балансі.

Таблиця 2.2 – Порівняльний аналіз алгоритмів знаходження консенсусу

Алгоритм	**Ціль**	**Переваги**	**Недоліки**	**Приклади застосування**
Proof of Work, PoW	Забезпечення складності у формі обчислювального завдання, щоб надати можливість обміну даними між ненадійними учасниками.	Важко досягти відмови в обслуговування (атака DDoS неефективна) Відкритий для всіх, у кого є обладнання, щоб вирішити обчислювальне завдання.	Високе обчислювальне навантаження, високе енергоспоживання Потенціал для 51% атаки, отримавши достатню обчислювальну потужність.	Bitcoin, Ethereum та багато інші
Proof of Stake, PoS	Забезпечення менш складної у обчислювальному плані перешкоди для додавання нових блоків, ніж у PoW, щоб надати можливість обміну даними між ненадійними учасниками.	Менш вимогливий у обчисленнях, ніж PoW. Відкритий для всіх.	Зацікавлені сторони контролюють систему. Існує можливість формуванню пулу зацікавлених сторін для створення централізованої влади. Потенціал для 51% атаки.	Ethereum, Casper, Krypton
Delegated PoS	Створення механізму консенсусу через «демократію», де учасники голосують (використовуючи криптографічно підписані повідомлення), щоб вибрати та	Вибрані делегати економічно мотивовані залишатися чесними. Менш вимогливий у обчисленнях, ніж PoW	Найменша різноманітність вузлів, ніж у PoW або в чистих реалізаціях PoS Оскільки всі делегати «відомі», у виробників блоків може бути стимул	Bitshares, Steem, Cardano, EOS

	відкликати права делегатів		змовлятися, ставлячи під загрозу безпеку	
Proof of Authority/ Identity, PoA, PoI	Створити централізований процес погодження, щоб мінімізувати час створення блоків та швидкість підтвердження	Швидкий час підтвердження. Дозволяє збільшити темпи виробництва блоків. Може використовуватися в sidechain, які використовують іншу модель консенсусу	Вважається, що валідуючий вузол не був скомпрометований. Існує центральна точка відмови	Ethereum Kovan testnet, POA Chain

Продовження таблиці 2.2

Round-robin	Забезпечити систему для додавання блоків серед довірених вузлів	Низька обчислювальна потужність. Ідея проста в розумінні.	Вимагає великої довіри серед вузлів.	MultiChain
Proof of Elapsed Time, PoET	Забезпечення більше економічної моделі консенсусу за рахунок гарантій безпеки, пов'язаних з PoW.	Менш вимогливий у обчисленнях, ніж PoW	Вимога по апаратному забезпеченню для синхронізації часу, до, наприклад, Intel SGX	Hyperledger Sawtooth

Біткойн вирішив проблему консенсусу наступним чином: для кожного нового блоку йде багаторазовий перерахунок із перебором різноманітних варіацій параметра nonce, тобто блок буде прийнято, якщо хеш менший за деяке значення, що задає складність обчислення. Оскільки вихідна інформація функції хешування розподілена рівномірно – неможливо створити блок, щоб легко задовольнити умову. Між майнинговими комп'ютерами в мережі йде гонка за пошуком необхідного параметра nonce. Як тільки мета досягається, комп'ютер майнінгу передає даний блок до мережі, та інші учасники перевіряють транзакції. Оскільки ціль полягає в тому, щоб не надавати багато повноважень одній організації або людині, необхідно вибрати обмежений ресурс, який буде витрачено на перевірку блоку.

Залежно від типу blockchain-системи застосовуються різноманітні алгоритми досягнення консенсусу. Мета алгоритму полягає в тому, щоб забезпечити існування однієї єдиної історії транзакцій, і щоб дана історія не містила суперечливі або неприпустимі транзакції. Наприклад, будь-який обліковий запис не повинен витратити більше ресурсів, ніж містить, або двічі витрачати той самий ресурс. У таблиці 2.2 представлено порівняння основних алгоритмів.

РОЗДІЛ 3 РОЗРОБКА ПРОГРАМНОГО ЗАСОБУ АРБІТРАЖНОЇ СИТУАЦІЇ

3.1 Середовище розробки та опис програми

Python – це мова програмування високого рівня та загального призначення з відкритим вихідним кодом. Python розроблений, щоб підкреслити легкість для читання коду за рахунок значного використання прогалин. Написання програм на Python займає менше часу в порівнянні з будь-якими іншими мовами [14].

Переваги Python:

1. Простота. Python вважається мінімалістичною мовою, тому що за допомогої неї дуже легко писати і читати код
2. Безкоштовна. Python – це безкоштовна мова з відкритим вихідним кодом. Завдяки цій функції Python зміг створити навколо себе сильне співтовариство, яке тільки зміцнює його і допомагає розвиватися.
3. Сумісність. Розробник може використовувати мову Python, не турбуючись про будь-які проблеми сумісності, тому що Python сумісний з численними платформами.
4. Об'єктно-орієнтована. Python підтримує як процедурно-орієнтоване, так і об'єктно-орієнтоване програмування.
5. Надійні стандартні бібліотеки. Спільнота Python сформувала велику кількість різних бібліотек, за допомогою яких розробник може управляти документацією, виконувати модульне тестування, організовувати бази даних, створювати графічний користувальницький інтерфейс.
6. Розробка через тестування. Розробник може використовувати Python для швидкого створення прототипу програмного додатка.

Недоліки мови Python

1. Неефективний з точки зору пам'яті. Займає більше місця через динамічний розподіл, а також через те, що змінні не ініціалізуются.

2. Довгий час роботи. Мовам-інтерпретаторів потрібно більше часу для запуска, оскільки вони спершу не компілюють код в бінарний код.

3. Не підходить для апаратного програмування. Мови високого рівня не використовуються для програмування обладнання.

4. Слабкість для мобільних обчислень. Python – не найкраща мова для роботи, якщо потрібно працювати над мобільними додатками.

5. Неефективна многопоточність. Python використовує загальне блокування інтерпретатора, який дозволяє виконувати тільки один потік за раз.

PyCharm – одна з найпопулярніших IDE для Python. Для цього існує безліч причин, в тому числі той факт, що він розроблений JetBrains, розробником популярної IDE IntelliJ IDEA, яка є однією з великої трійки Java IDE і самої JavaScript IDE WebStorm. Підтримка веб-розробки за допомогою Django – ще одна вагома причина. Існує безліч факторів, які роблять PyCharm одним з найбільш повних і всеосяжних інтегрованих середовищ розробки для роботи з мовою програмування Python [14].

Основна причина, по якій Pycharm створила IDE, полягала в програмуванні на Python і роботі на декількох платформах, таких як Windows, Linux і macOS. IDE включає інструменти аналізу коду, відладчик, інструменти тестування, а також параметри контролю версій. Він також допомагає розробникам створювати плагіни за допомогою різних доступних API. IDE дозволяє працювати з декількома базами даних безпосередньо, без інтеграції з іншими інструментами. Він також має гарний користувальницький інтерфейс, який можна налаштувати відповідно до потреб за допомогою плагінів.

Особливості PyCharm:

- інтелектуальний редактор коду;
- доступність інструментів інтеграції;
- наука про дані і машинне навчання;
- Google App Engine;
- інтегроване налагодження і тестування;
- розробка різних технологій;
- навігація по проекту і коду;
- рефакторинг;
- дистанційна розробка.

Арбітраж криптовалют – це використання цін на Вашу користь. Торгівля криптовалютою існує вже кілька років, проте ціни на криптовалюти варіюються від однієї біржі до іншої. Кожна криптовалюта має свою цінність для певних криптовалют, і це може бути викликано кількома причинами. Криптоарбітраж допомагає трейдерам скористатися різницею у ціні, купуючи криптовалюту на одній біржі та негайно продаючи її на іншій. Торгівля криптовалютою досить складна, та існує кілька ризиків, головним чином через нестабільність криптовалютного ринку. Не можливо передбачити коли ціни можуть злетіти або знизитись. Для отримання прибутку потрібно проаналізувати закономірності в графіках цін, щоб передбачити майбутній рухЗ [3].

Головна ціль проекту – створити програмне забезпечення, яке торгуватиме криптовалютою на біржі, з використанням стратегій для максимізації прибутку при одночасному зниженні ризику. Програма створена у виді клієнту, в якому реалізовано інтерфейс користувача. Для створення клієнту використано мову програмування Python та декілька модулів для реалізації графічного інтерфейсу і створення запитів до криптовалютних бірж.

Для створення графічного інтерфейсу використано модуль PyQt – це набір розширень графічного фреймворку Qt для мови програмування Python, виконаний у вигляді розширення. В додатку реалізовано вибір біржі на яку буде відправлятися запит для отримання котирування, які використовуються для обчислення по стратегії. Після обробки даних – результат виводиться в інтерфейсі [6].

Для відправки запитів необхідно отримати API-інтерфейси, які дозволять боту отримати доступ до будь-яких бірж для арбітражу. Бібліотека CCXT використовується для підключення та торгівлі з криптовалютними біржами та службами обробки платежів по всьому світу. Вона забезпечує швидкий доступ до ринкових даних для зберігання, аналізу, візуалізації, розробки індикаторів, алгоритмічної торгівлі, тестування стратегій, програмування ботів та розроблення відповідного програмного забезпечення (рис. 4.1).

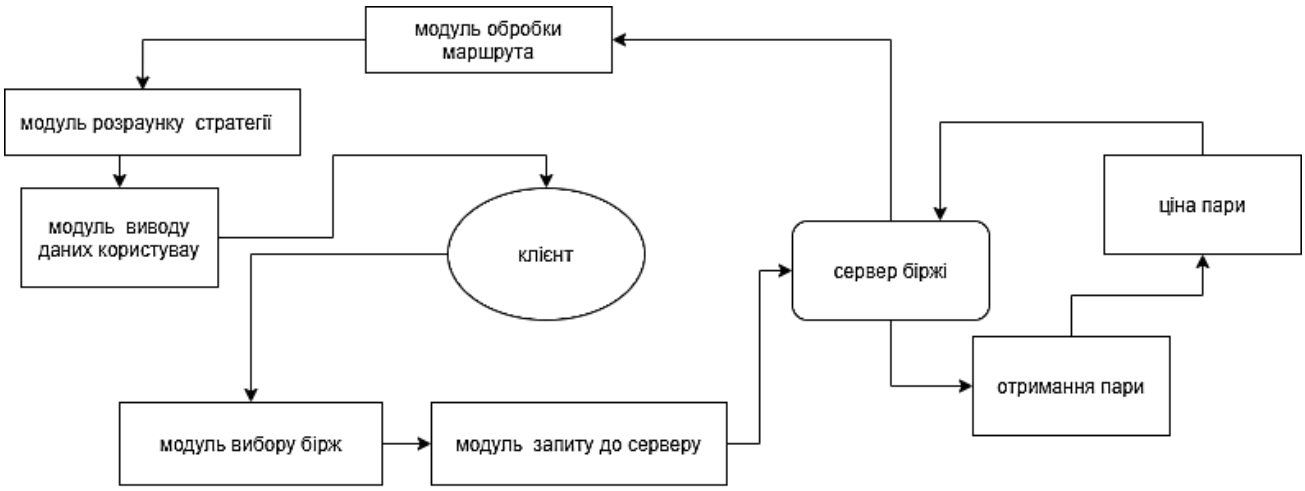

Рисунок 4.1 – Схема роботи програмного засобу

Функції:

- моніторинг спредів всередині бірж (Gdax, Bitfinex, Bitstamp);
- можливість налаштування кількох валютних пар (BTC/EUR, ETH/USD);
- повідомлення про пороги спреду;

- автоматична торгівля за налаштованими порогами спреду;
- широкі можливості налаштування (валютні пари, порогові значення кожного каналу повідомлень чи торгівлі, історичні дані тощо)

Системні вимоги:

- процесор Intel Pentium IV/Xeon 2,4 ГГц;
- оперативна пам'ять 1024 Мб;
- жорсткий диск 40Гб;
- USB-порт;
- SVGA-відеокарта.

3.2 Опис алгоритму роботи для програмного забезпечення

Для знаходження можливостей, які є прибутковими, можна виконати деякі обчислення, щоб визначити, чи не переоцінений курс, а це означає, що існує розбіжність у ціні при торгівлі між трьома різними активами, що призведе до прибутку, якщо наші ордери будуть виконані правильно.

Замовлення можуть надходити по двох різних шляхах, і обидва призводять до того, що вони починаються і закінчуються одним і тим самим активом. Розглянемо кожен окремо, оскільки обрахунки для кожного трохи відрізняється.

Для довільного шляху будемо розраховувати курс, і якщо результат більший за 1, він вважається завищеним. Це не обов'язково означає, що це вигідно, важливо враховувати торгові комісії, які також стягуватимуться з кожного заповненого ордера [11].

Для того, щоб курс став прибутковим, він має бути більшим, ніж сума комісійних зборів за кожну угоду. Припустимо, що кожен ринок має комісію тейкера 0,2%, тому курс має бути більше 1+0,002+0,002+0,002 або 1,006, щоб він став прибутковим.

Спочатку визначимо такі точки даних:

- стартовий актив: USD;
- торгова пара A: BTC-USD;
- торгова пара B: LTC-BTC;
- торгова пара C: LTC-USD;
- торгові збори: припустимо, що кожна пара має комісію тейкера 0,2%.

Нижче наведено два можливі шляхи реалізації та відповідні формули курсу.

Шлях першого порядку

1. Покупка за «торговельною парою A». З USD купляємо BTC.
2. Покупка за «торговельною парою B». З BTC купляємо LTC.
3. Продати за «торговельною парою C». Продаж LTC за USD.

Формула курсу шляху першого порядку (рис. 4.2):

(1 / попит «Торгівельна пара A») * (1 / попит «Торгівельна пара B») *

* (пропозиція «Торгівельна пара C»)

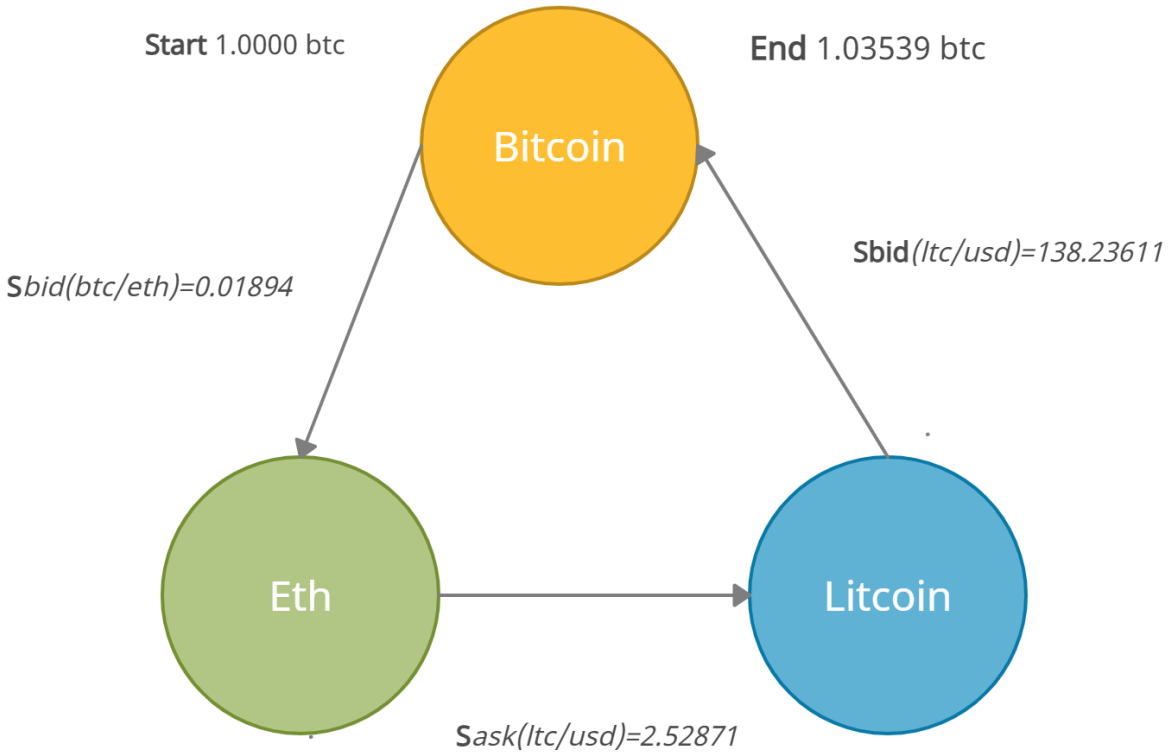

Рисунок 4.2 – Шлях першого порядку

Шлях другого порядку

1. Покупка за «торговельною парою С». З USD купляємо LTC.
2. Продати «Торгівельну пару В». Продаж LTC за BTC.
3. Продати по «торговій парі А». Продаж BTC за USD.

Формула курсу шляху другого порядку (рис. 4.3):

(1 / пропозиція «Торгівельна пара С») * (пропозиція «Торгівельна пара В») * * (пропозиція «Торгівельна пара А»)

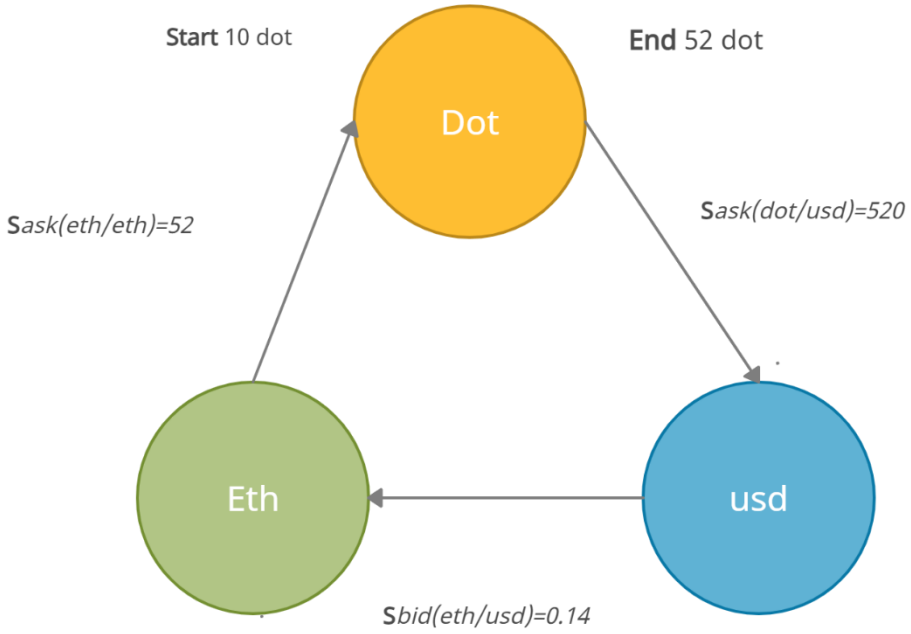

Рисунок 4.3 – Шлях другого порядку

При використанні даної торгової стратегії слід мати на увазі дві важливі речі: прослизання та вимоги до точності ринкових даних.

Прослизання

Прослизання відбувається, коли отримується гірша ціна, ніж очікувалося, через те, що заповнили кілька замовлень у книзі замовлень. Наприклад, припустимо, що потрібно купити BTC в книзі замовлень BTC-USD, і вона має запит у розмірі 0,1 BTC за ціною 20 000 доларів США, потім наступний – 0,2 BTC за ціною 20 100 доларів США. Якщо купляти 0,15 BTC, отримаємо перші 0,1 за курсом 20 000 доларів, а потім останні 0,5 за ціною 20 100 доларів. Через це, якщо потрібно уникнути прослизання – необхідно переконатися, що ордер не перевищує розмір, який потрібно заповнити, оскільки трикутний арбітраж буде включати три різні ордери.

Точність даних

Вимоги до точності даних – це кількість десяткових знаків, яку кожен ринок підтримує під час обміну як сум, так і ставок замовлень. Біржі встановлюють ці обмеження, щоб клієнти не могли торгувати виключно невеликими сумами, і кожна пара на біржі може допускати різну кількість десяткових знаків. Якщо виникне можливість арбітражу, для якої буде потрібно сума ордера 0,65201 BTC на двох ринках, але на одному ринку дозволено лише три десяткові знаки, виникне не можливість подавати дані ордери [18].

Виявлення можливостей арбітражу

Перший крок – виявити можливості арбітражу в режимі реального часу. Час відіграє важливу роль, оскільки, як тільки виявлено розбіжність в обміні між ринками, арбітраж має бути виконана швидко. Якщо подивіться на екран торгових комісій у Binance, то можна побачити, що існують окремі комісії для «Творців» та «Тейкерів», останні є неринковими угодами, та арбітражні ордери мають бути обмежені лімітними ордерами, інакше втратимо волатильність ринку.

```
USDT-> BTC-> AR-> USDT 0,441%
```

Рисунок 4.4 – Трикутний арбітраж

Трикутник (рис. 4.4) є угодою USDT для торгівлі BTC, для торгівлі AR за USDT, що генерує 0,441%, тому 100 USDT принесли 44 центи в даному арбітражі, що, можливо, зайняло б не більше 2 секунд.

Наведені вище дані є важливим ключем, оскільки не було такого ж арбітражу, доступного в потрібний час, тому він зник. Якби ініціювали угоду на BTC, то вона могла бути виконана, але тоді угода на AR могла б не відбутися. Не можливо бути впевненим лише у такій інформації. Можливо, через секунду обмін USDT/BTC більше не був доступний за граничною ціною: BTC/USDT, але тепер, коли є BTC,

можливо, що залишилися 2 можливі угоди. Це не можливо знати, коли виконується арбітражний обмін [15].

Кожен виклик REST API займає щонайменше 200 мс, залежно від того, де виконується ваш код. Сервери розташовані у різних країнах. Лімітний ордер не є миттєвим, для повернення може знадобитися ще 500 мс, тому загальний час для 3 лімітних ордерів може реально збільшитися до ~2 секунд. Звичайно, може виникнути деяка нездатність виконати лімітний ордер, який зазначено в цей момент, тому існує безліч причин, через які виконання арбітражу може не завершитися. Існує безліч способів, якими виконання арбітражу може не завершитися в межах вікна, в якому існує можливість арбітражу.

Розглянемо наступну можливість арбітражу (рис. 4.5).

```
USDT-> SUSD-> BTC-> USDT 0,0077%
```

Рисунок 4.5 – Приклад можливого арбітражу

Він залишається відкритим протягом кількох секунд, достатнього часу для виконання всіх трьох угод, проте прибуток варіюється від 0,0077% до 0,0282%. Якби використали 100 доларів США, це призвело б до прибутку менше 1 центу після сплати комісійних.

Розглянемо основні властивості арбітражу для створюваної системи:

1. Можливості арбітражу існують, але обмежені через торгові комісії. Біржа стягуватиме 0,075% вартості угоди за кожну з 3 транзакцій в арбітражі. Також пам'ятаємо, що це є транзакції Taker, тому що вони є лімітними ордерами.
2. Арбітражні трикутники часто не триває довше встановленого часу (секунди), коли вони ідентифікуються. Час PING для бірж (~20 мс) з часом

прийому-передачі лімітного ордера на ПОКУПКУ або ПРОДАЖ. Навіть виклик API типу пошуку займе щонайменше 200 мс.

3. Немає способу дізнатися, чи залишиться арбітражний набір із 3 бірж доступним на момент його виявлення. Не можливо знати, чи зміниться ціна наступної валюти через 50 мс після першого обміну.
4. Деякі довгострокові арбітражні повноваження визначені як такі, що мають дуже низьку маржу прибутку. Важливо врівноважити розмір прибутку з відносним ризиком, існує реальний ризик незавершених угод, тому прибуток має це виправдовувати.

Потрібно захопити дані арбітражу, а потім проаналізувати їх, щоб побачити скільки можливостей арбітражу існує і скільки з них тривало не менше 2-3 секунд. З них будемо розраховувати розмір прибутку. Отже, організуємо нормалізований словник результатів, щоб виділити кількість послідовностей кожного унікального обміну, виявленого під час збору даних.

З результатів легко визначити – більшість знайдених арбітражних можливостей мають єдину послідовність. Насправді потрібна послідовність як мінімум із 4–5, щоб мати достатньо часу, тобто для тривалого відкриття для виконання угод. Щоб виділити даний крок, порахуємо кількість послідовностей за і розглянемо, який % угод для цього збору даних був би досить довгим, щоб здійснити угоду [6].

10% можливостей арбітражу під час даного прогону залишалися б відкритими досить довго, щоб можна виконувати угоди за умови розумної двосторонньої відповіді на виклики API. Але це означає, що 90% цих можливостей арбітражу, мабуть, залишаться із незавершеними торговими «трикутниками», з деякими криптовалютними монетами в гаманці, які не були обмінені, як планувалося. 90% цих можливостей арбітражу, ймовірно, залишили б незавершені торгові

«трикутники», з деякими криптовалютними монетами в гаманці, які не були обмінені, як планувалося, і залишалися схильними до волатильності.

Середній прибуток за довгими угодами в цьому прогоні становив би 0,05%.

Якби проводили обміни, починаючи зі 100 USDT, отримали б у середньому 5 центів прибутку. Але 90% незавершених угод залишилися б схильними до волатильності цих монет, що легко призвело б до збитків, які набагато перевищують прогнозований прибуток.

3.3 Реалізація інтерфейсу створеного програмного забезпечення

Запускаючи програмний додаток з'явиться головний екран (рис. 4.6), що містить панель для виконання основних дій та основну інформацію (ціни криптовалют на даний момент, декілька бірж на вибір, тощо).

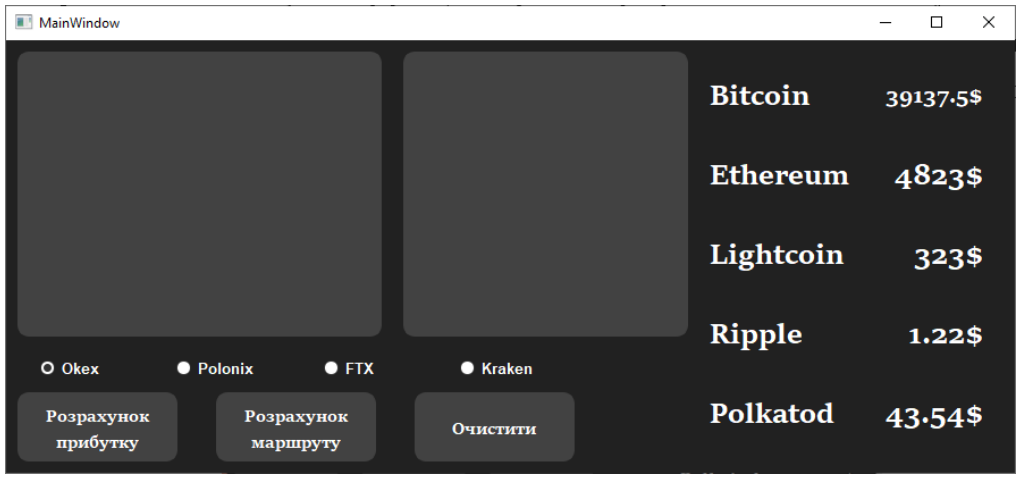

Рисунок 4.6 – Головна сторінка програми

Кнопка розрахунок маршруту відповідає за пошук всіх можливих валют на біржі. Для активації потрібно вибрати біржу на якій планується розрахувати всі можливі маршрути. Після цього натиснути на кнопку розрахувати маршрут і вона

відфільтрує непотрібні криптовалюти і знайде маршрут для здійснення арбітражної ситуації та виведе результат в праву колонку програми.

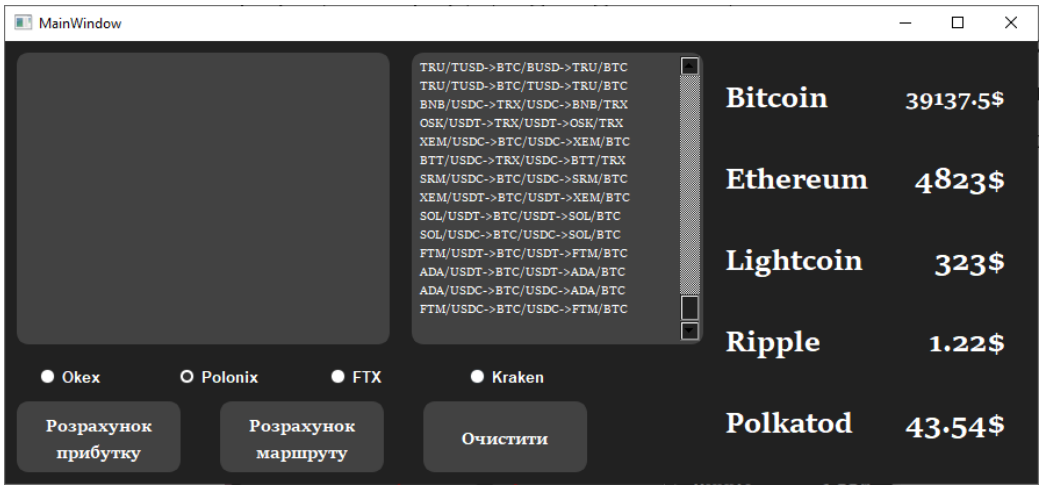

Рисунок 4.7 – Алгоритм виконання необхідних дій

Алгоритм дій:

1. Лейбл (виводить результат кнопки розрахунок маршруту).
2. Вибір біржі.
3. Розрахунок.

Після розрахунку маршруту, потрібно дізнатися ціни кожної валюти і розрахувати прибуток, а також вивести всі пари, які відображатимуть позитивний результат. Для цього потрібно натиснути розрахунок прибутку (рис. 4.8).

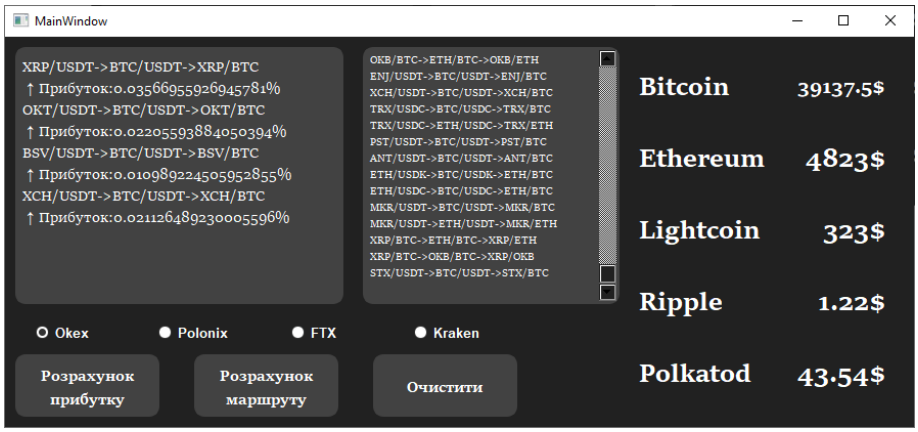

Рисунок 4.8 – Виведення результату розрахунку

Після розрахунку виведуться на екран угоди. Такі розрахунки можна робити і з іншими біржами але для цього потрібно очистити всі поля. Для цього реалізована окрема кнопка, після натиснення на неї зникне вся інформація (рис. 4.9).

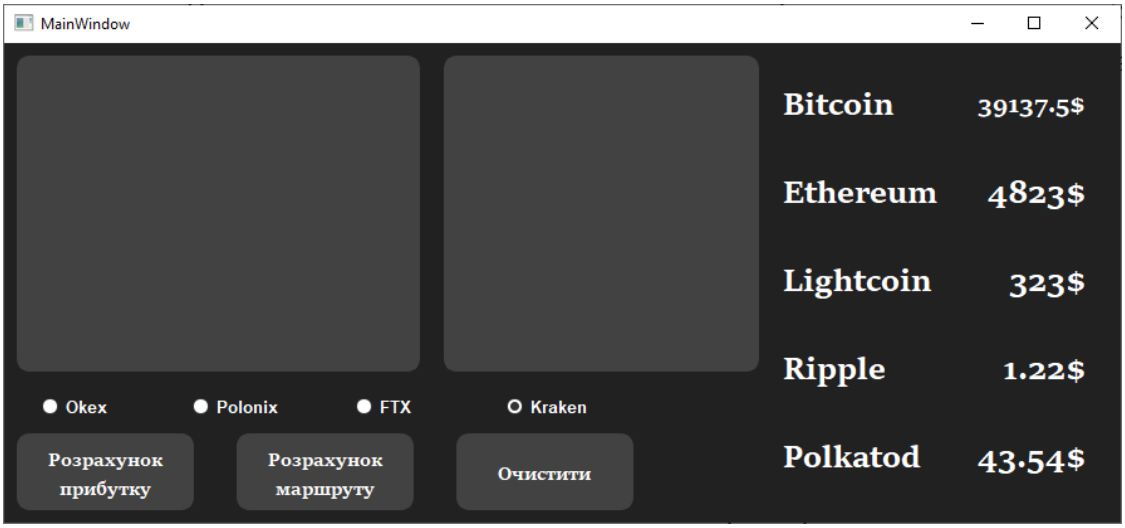

Рисунок 4.9 – Вигляд головного вікна після очищення

ВИСНОВКИ

На теперішній час ринкова оцінка всіх криптовалют становить приблизно 2,3 трлн доларів США, що надає величезну можливість для зростання інвестованого капіталу, про що свідчить різке підвищення цін на криптовалюти та ринкову капіталізацію в 2021 році. На протилежному боці цієї можливості ринок криптовалюти містить багато ризиків та волатильність.

Більшість сучасних уявлень про інвестування в криптовалюту ґрунтується на принципах покупки та зберігання, але бажано автоматичне вирішення з метою збереження та збільшення інвестованого капіталу за обмеженої участі трейдерів. Враховуючи величезні можливості, потрібне програмне забезпечення, яке допоможе здійснювати торги криптовалютою як новачкам, так і досвідченим інвесторам в криптовалюту.

Головна ціль роботи – створення програмного засобу для криптовалютної торгівлі, яке кожен може завантажувати, редагувати та налаштовувати для реалізації своїх власних торгових стратегій. Існує безліч доступних криптоботів для трейдерів, але повинно бути рішення, в якому код може налаштовуватися відповідно до цілей, тимчасового горизонту та профілю ризику кожного трейдера. Багато доступних торгових ботів є пропрієтарними, а інші написані за допомогою Gekko Trading Bot Software.

Після проведення досліджень стало зрозуміло, чому багато криптотрейдерів відмовилися від використання арбітражу як стратегії. Насамперед: комісія за транзакцію, хоч і невелика, має значний ефект, якщо не досягається достатньо високий рівень зниження комісій на біржі, то арбітражних ситуацій можливо не знайти взагалі.

Затримка API, з обмеженим тимчасовим вікном знаходиться між часткою секунди та 1-2 секундами, це невеликий проміжок часу, протягом якого можна надійно виконати 3 угоди. Навіть якщо торговий код знаходиться поруч із серверами біржі, затримка виклику REST API є великою проблемою.

Маржа часто дуже мала, навіть якщо комісія за транзакцію невисока. І маржа, що використовує цю стратегію, повинна покривати невід'ємний ризик незавершених угод, в яких монети, що залишилися, схильні до волатильності, що неминуче. Торгівля криптовалютою це складний процес і трейдеру, який буде використовувати створений програмний засіб повинен розуміти ризики .

Під час вивчення описаної проблеми та для реалізації даного проекту проведено моніторинг роботи криптовалюти, а також вивчено значну кількість літературних та електронних джерел, що описують та вивчають обрану тему.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Ben-David A. FairplayMP: a system for secure multi-party computation / A. Ben-David, N. Nisan, B. Pinkas // ACM CCS 2018. – 2018. – P. 257-266.
2. Bitcoin Series 24: The Mega-Master Blockchain List [Електронний ресурс] / Ledra Capital – многопользовательская частная группа, ориентированная на растущие крупные компании в сферах высшего образования, средств массовой информации и технологий. – Режим доступу: http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-masterblock chain-list (дата звернення: 08.04.2022).
3. Bitcoin's Largest Competitor Hacked: Over $59 Million "Ethers" Stolen In Ongoing Attack [Електронний ресурс] / Режим доступу: https://www.zerohedge.com/news/2020-06-17/bitcoins-largest-competitorhacked-over-59-million-ethers-stolen-ongoing-attack (дата звернення: 10.04.2022).
4. Camenisch J. Concepts and languages for privacy-preserving attribute-based authentication / J. Camenisch, M. Dubovitskaya, R. Enderlein, A. Lehmann, G. Neven, C. Paquin, F. Preiss // IFIP Working Conference on Policies and Research in Identity Management. – Vol. 19. – 2020. – P. 25-44.
5. Camenisch J. On the Portability of Generalized Schnorr Proofs / J. Camenisch, A. Kiayias, M. Yung // EUROCRYPT 2019 (LNCS). – Vol. 5479. – 2019. – P. 425-442.
6. Camenisch J. Practical UC-Secure Delegatable Credentials with Attributes and Their Application to Blockchain / J. Camenisch, M. Drijvers, M. Dubovitskaya // ACM Conference on Computer and Communications Security. – 2021. – P. 683-699.
7. Chase M. Malleable Proof Systems and Applications / M. Chase, M. Kohlweiss, A. Lysyanskaya, S. Meiklejohn // EUROCRYPT 2022 (LNCS). – Vol. 7237. – 2022. – P. 281-300.

8. Coinmarketcap [Електронний ресурс]. – Режим доступу: https://coinmarketcap.com/ (дата звернення: 19.03.2022).
9. Mrantz M. Fundamental analysis for dummies / M. Mrantz – Hoboken: Wiley Publishing Inc., – 2019. – 387 p.
10. Nagpal R. 17 blockchain platforms – a brief introduction [Електронний ресурс] / Режим доступу: https://medium.com/blockchain-blog/17-blockchain- platforms-a-brief-introduction-e07273185a0b (дата звернення: 25.04.2022).
11. Tapscott D. Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World / Don Tapscott, Alex Tapscott / Blockchain – K.: Information Systems, 2019 – С. 100-150.
12. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments / Joseph Poon, Thaddeus Dryja – K.: 2019. – С. 5-54.
13. Vessenes P. Ethereum Contracts are Going to be Candy for Hackers [Електронний ресурс] / Режим доступу: https://vessenes.com/ethereumcontracts-are-going-to-be-candy-for-hackers (дата звернення: 07.04.2022).
14. Алгоритмы консенсуса в блокчейне: техническая часть [Електронний ресурс]. Режим доступу: https://crypto-fox.com/faq/algoritmyi-konsensusa/ (дата звернення 24.04.2022).
15. Беляева К. С. Розробка засобів верифікації протоколу консенсусу в децентралізованих системах / Беляева К.С., Пенко В.Г. // Інформатика, інформаційні системи та технології: тези доповідей шістнадцятої всеукраїнської конференції студентів і молодих науковців Одеса, 19 квітня 2020 р. – Одеса, 2020. – С.61-62.
16. Галушка Є.О. Сутність криптовалют та перспективи їх розвитку / Галушка Є.О., Пакон О.Д. // «Молодий вчений» – № 4 (44), 2019. – С.7-18.
17. Гострик О. М. Прогнозування валютних криз методами теорії складних мереж / О. М. Гострик, К. В. Соловйова //Проблеми та перспективи розвитку

економіки освіти регіону: матеріали IX Міжнародної науково-практичної конференції аспірантів, молодих учених та науковців. – Кременчук: КІДУ імені Альфреда Нобеля, 2018. – С. 219-220.

18. Загородній А. Г. Державне регулювання ринку криптовалют: необхідність, моделі та форми. Фінансовий ринок: інституції та інструменти: матеріали XVII Міжн.наук.конф., 3–6 червня 2020 р. Львів: Видавництво Львівської політехніки, 2020. – С. 41-42.
19. Закон України «Про платіжні системи та переказ коштів в Україні»: прийнятий Верховною Радою України 05.04.2001 № 2346-III: редакція від 06.11.2016 на підставі 1664-19 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2346-14 (дата звернення: 17.04.2022).
20. Лубенець І. Огляд цифрових криптовалют [Електронний ресурс] / Блог експертів про фінанси – 2020 – Режим доступу: http://www.prostoblog.com.ua/lichnye/byudzhet/obzor_tsifrovyh_kriptovalyut. (дата звернення: 03.04.2022).
21. Молчанова Е. Глобальна сервісна природа сучасних криптовалют // Міжнародна економічна політика. – № 1. – 2020. – С. 60-79.
22. Осмоловская А. С. Смарт-контракты: функции и применение / А. С. Осмоловская // Бізнес в економіці знань. – 2018. – №2. – С. 54-56.
23. Поливка Н. Криптовалюти і «різноманітні біткойни» / Н. Поливка // Юридична Газета online. [Електронний ресурс]. – Режим доступу: http://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/kriptovalyuti-i-riznomanitni-bitkoini.html (дата звернення: 28.04.2022).
24. Синявська О. О. Прогнозування динаміки курсів криптовалют на основі причинно-наслідкових зв’язків із ключовими індикаторами / О.О. Синявська, І.В. Халімончук / Проблеми та перспективи розвитку фінансово-кредитної системи України: збірник матеріалів III Всеукраїнської науково-практичної

on-line конференції. – Суми: Сумський державний університет, 2018. – С. 327-330.