**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА**

Факультет прикладної математики та інформатики
(повне найменування назва факультету)

Кафедра інформацініх систем
(повна назва кафедри)

# Магістерська робота

"Розробка блокчейна та криптовалюти засобами .Net"

Виконав: студент групи ПМІМ-22с
спеціальності
122 "комп'ютерні науки"
(шифр і назва спеціальності)

Саакян Н.А
(підпис) (прізвище та ініціали)

Керівник Дреботій Р.Г.
(підпис) (прізвище та ініціали)

Рецензент Вовк О.В.
(підпис) (прізвище та ініціали)

Львів – 2022

***ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА***

Факультет Факультет прикладної математики та інформатики

Кафедра Кафедра інформаціних систем

Спеціальність 122 "комп'ютерні науки"
(шифр і назва)

**«ЗАТВЕРДЖУЮ»**

**Завідувач кафедри** - Г. Шинкаренко

" 08" 09 **2022 року**

# ЗАВДАННЯ

## НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Саакян Нікіта Арменович
( прізвище, ім'я, по батькові)

1 .Тема роботи
Розробка блокчейну та криптовалюти засобами .Net

керівник роботи Дреботій Роман Грегорович, кандидад фіз-мат наук, доцент
( прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені Вченою радою факультету від " " 2022 року №

2. Строк подання студентом роботи 12 грудня 2022 року

3. Вихідні дані до роботи
Досліджування ринку криптовалюти, аналіз алгоритмів блокчейну, власна реалізація криптовалюти та блокчейну

4. Зміст магістерської роботи (перелік питань, які потрібно розробити)
вступ, теорія, розробка власної системи, висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
зображення фрагментів коду, демонстрація результата

6. Консультанти розділів роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |

| | | | |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

7. Дата видачі завдання

**Керівник роботи** ( підпис ) (прізвище та ініціали) Дреботій Р.Г.

## КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів магістерської роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1. | Аналіз літератури та джерел за темою дипломної. | вересень | виконано |
| 2 | Аналітичний огляд і постановка задачі. | жовтень | виконано |
| 3. | Порівняльний аналіз існуючих реалізацій. | листопад | виконано |
| 4. | Загальна розробка архітектури. | листопад | виконано |
| 5. | Розробка технолоії блокчейн. | грудень-березень | виконано |
| 6. | Розроботка криптовалюти на основі блокчейну. | квітень-червень | виконано |
| 7. | Реалізація ptp переводу. | липень-серпень | виконано |
| 8. | Реалізація веб-додатку. | вересень-листопад | виконано |
| 9. | Оформлення дипломної роботи. | листопад-грудень | виконано |
| 10. | Підготовка до захисту та попередній захист дипломного проекту . | листопад-грудень | виконано |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Студент Саакян Н.А.**

( підпис ) (прізвище та ініціали)

Розробка блокчейна та криптовлюти через .net

**ЗМІСТ**

# ПЕРЕЛІК ВИКОРИСТАНИХ СКОРОЧЕНЬ

| | |
|---|---|
| БМ | блочейн мережа |
| БТ | блочейн технології |
| ПЗ | програмне забезпечення |
| ЦП | цифровий підпис |
| ECDSA | Elliptic Curve Digital Signature Algorithm |

# ВСТУП

***Актуальність теми дослідження.*** Протягом останніх десяти років дискусії, пов'язані з технологіями блокчейн і криптовалютою, в світі не тільки не замовкають, але навпаки викликають все більший інтерес і не тільки з боку фінансових інститутів, а й населення і державних структур. Передумовами даної зацікавленості послужили різні фактори: це і світова нестабільність економічних відносин, превалювання окремих резервних валют над національними, глобальна цифровізація економіки і стирання кордонів, криза довіри до діючої фінансової та платіжної систем та ін. У цих умовах в учасників світової економіки став формуватися запит на пошуки відповідей на дані питання, так як еволюційні закони людства такі, що люди намагаються постійно шукати більш вигідні та зручні сервіси і товари. І поява таких нових віртуальних платіжних засобів, як криптовалюта, можливо, стало одним з відповідей на зазначені виклики.

Привабливою особливістю криптовалютних платежів є те, що транзакції між суб'єктами проводяться безпосередньо, без участі посередників, не задіюючи при цьому фінансові установи. З огляду на цей фактор, популярність криптовалюти в світі зростає все більше і більше, що підтверджується обсягом капіталізації ринку криптовалюти, який до 20 червня 2021 року досяг 867,2 млрд.дол. США [1].

***Проблематика дослідження.*** В даний час фахівці прийшли до висновку про ряд проблемних моментів у розвитку системи блокчейн, так само як і те, що дана технологія була дещо передчасно названа універсальною і досконалою. Отже, блокчейн-технологія функціонує з деякими обмеженнями: система блокчейн не має бездоганного рівня секретності. За умовами технології формується реєстр, який дозволяє обмінюватися трафіком між учасниками системи і отримувати дані по всіх виконаних транзакціях. Отже, вказати на високу секретність транзакцій, що проводяться по блокчейн-технології, неможливо, так як система початково

створена як прозора, щоб ефективно функціонувати і здійснювати задум розробників. Але велике число учасників системи, здатних отримати інформацію про транзакції, нерідко змушує відмовитися від блокчейна, якщо Програмний продукт потребує підвищеної конфіденційності даних і операцій; сценарій захисту технології блокчейна передбачає застосування асиметричних криптографічних рішень, що дозволяють ідентифікувати і аутентифікувати сторони, які отримують доступ до системи, так само як і при вході на акаунт для проведення транзакції. Проведення транзакцій здійснюється тільки при супроводі розпорядження електронним підписом. Якщо електронний підпис стає відомим стороннім в результаті помилки, випадковості, перехоплення даних, то акаунт не можна розглядати як захищений; система блокчейн характеризується необґрунтовано високими експлуатаційними витратами, так як система має категорію обмежено масштабованої; систему блокчейн не слід характеризувати як гнучку технологію, так як робота блокчейна досягається в результаті узгодження безлічі архітектурних елементів, принципів і протоколів, суміщених і адаптованих для виконання конкретних функцій; система не має високої довіри з точки зору закону; система має труднощі з регуляцією еволюції технології блокчейн нормами законодавства; є складність завоювання довіри серед населення.

Потенційно ця технологія охоплює всі без винятку сфери економічної діяльності. Однак, незважаючи на всі переваги, вона не є універсальною. Також її використання в технології створення криптовалюти має ряд обмежень і проблем, які, в зв'язку зі зростаючим впливом криптовалюти, потрібно обов'язково враховувати і не можна ігнорувати.

***Мета дослідження.*** Метою даної дослідження виступає аналіз сучасних технологій, методів та моделей здійснення крипто валютних операцій та розробка блокчейну та крипто валюти через .net.

# РОЗДІЛ 1
# ТЕОРЕТИЧНІ АСПЕКТИ КРИПТО ВАЛЮТНИХ ТЕХНОЛОГІЙ

## 1.1 Поняття крипто валюти

Однією з новацій останнього часу стала поява особливого виду валют, який отримав назву «криптовалюта». Даний феномен привертає до себе особливу увагу, при цьому більшість авторів в основному розглядають технічні аспекти обігу криптовалюти. Тим часом однобока вивченість криптовалют з позиції опису технічної моделі функціонування не дозволяє розкрити їх сутність як економічної категорії, а також перешкоджає швидкому створенню адекватних формально-інституціональних норм, що регламентують процедури емісії та обігу. Як наслідок, виникає закономірний дисбаланс – коли економічні нововведення випереджають розвиток законодавства, що регулює взаємовідносини суб'єктів у сфері розрахунків і платежів, що, в свою чергу, посилює можливі ризики на макро- і мікрорівнях.

На сьогоднішній день у світі існує понад 500 видів криптовалют, загальна капіталізація яких на 20 червня 2021 року досяг 867,2млрд.дол. США [1]. Проте, найбільшого поширення набули лише Bitcoin і Litecoin. Дані види криптовалюти приймаються всіма існуючими біржами і обмінними пунктами. Решта криптовалют побудовані на базі відкритого коду Bitcoin і практично нічим від нього не відрізняються, тобто по суті, вони є похідними інструментами Bitcoin. Цим і пояснюється їх менша популярність.

Незважаючи на стрімке зростання популярності, сьогодні не існує єдиного, визнаного в світі визначення криптовалют, яке б однозначно розкривало їх сутність і економічну природу. Певною мірою це пояснюється новизною даного інструменту і різноманітністю технічних рішень, реалізованих в системах електронних розрахунків. Так, у світі по-різному ставляться до криптовалют, наприклад, у Канаді та Нідерландах – як до валюти, а в Австрії, Фінляндії та Німеччині – як до «commodity» –

товару/сировини [2]. В україномовній мережі Інтернету досить коректне і повне визначення поняття «крипто валюта» дано у Вікіпедії, де криптовалюта розглядається як вид цифрової валюти, емісія і облік якої засновані на асиметричному шифруванні і застосуванні різних криптографічних методів захисту, таких як Proof-of-work і Proofof-stake [3]. На основному сайті Bitcoin – одного з виду криптовалют, який набув найбільшого поширення, криптовалюта позначена як інноваційна мережа платежів і новий вид грошей, який використовує p2p технологію, що функціонує без центрального контролюючого органу або банку, обробка транзакцій і емісія здійснюються колективно, зусиллями мережі [4]. Ще одне, що заслуговує на увагу, визначення дано у статті «Applications of blockchain technology beyond cryptocurrency» і звучить наступним чином: «за своїм призначенням криптовалюта нічим не відрізняється від інших платіжних систем, так як дозволяє продавати і купувати товари і послуги. Принципова відмінність від інших платіжних засобів полягає в способі випуску (емісії) платіжних одиниць і організації системи їх зберігання і проведення платежів» [5].

На думку автора, існуючі формулювання поняття криптовалюта не в повній мірі розкривають суть аналізованого феномена.

По-перше, в наявних визначеннях не відображений децентралізований характер емісії криптовалюти. Представляється особливо важливим врахувати, що в процесі утворення нових платіжних інструментів задіяні комп'ютерні потужності мільйонів учасників (дані взяті по відкритих електронних гаманцях) [6], об'єднаних в одній пірінговій мережі, де немає центрального сервера, і кожен окремо взятий комп'ютер цієї мережі є сервером. Таким чином, вся робота з обліку та зберігання історії транзакцій розподіляється між усіма учасниками.

По-друге, криптовалюта являє собою зашифрований спеціальною програмою код в розпорядженні власника, який фіксується і зберігається на електронному носії і приймається як засіб платежу іншими користувачами і організаціями. Звідси можна стверджувати, що криптовалюта є різновидом

електронних грошей. У свою чергу необхідно пояснити, що під електронними грошима в широкому сенсі розуміються грошові зобов'язання емітента в електронному вигляді, які знаходяться на електронному носії в розпорядженні користувача [7]. Причому дані грошові зобов'язання відповідають наступним трьом критеріям: фіксуються і зберігаються на електронному носії; випускаються емітентом при отриманні від інших осіб грошових коштів в обсязі, не меншому, ніж емітована грошова вартість; приймаються як засіб платежу іншими (крім емітента) організаціями.

По-третє, у випадку з криптовалютами ідентифікація власників і фіксація факту їх зміни засновані на найсучасніших криптографічних методах захисту, при цьому весь обсяг інформації у вигляді спеціальних блоків зберігається на кожному сервері (комп'ютері, учаснику пірінгової мережі). Зламати або обійти цей захист наявними потужностями на сьогоднішній день не представляється можливим.

Виходячи з осмислення механізму функціонування і обігу поняття «крипто валюта», представляється доцільним під «крипто валюта» розуміти особливий різновид електронних грошей, функціонування яких засноване на децентралізованому механізмі емісії та обігу і, які представляють собою складну систему інформаційно-технологічних процедур, побудованих на криптографічних методах захисту, що регламентують ідентифікацію власників і фіксацію факту їх зміни.

Класифікувати крипто валюту є можливість на кілька основних типів по її сутності і призначенню (таблиця 1.1).

Таблиця 1.1 – Класифікація криптовалюти

| Криптовалюта | | | | |
|---|---|---|---|---|
| Гроші | Товар, власність, майно | Одиниця обліку в інформаційній системі | Грошовий сурогат (вексель, чек) | Засіб накопичення |

Виходячи з класифікації можна зробити висновок про те, що криптовалюта є універсальним фінансовим інструментом, так як може виступати в різних якостях і в сферах, і вказаний список з розвитком технологій можна буде продовжувати.

Узагальнивши всі зазначені вище поняття «крипто валюта», є можливість дати своє авторське визначення: криптовалюта – це віртуальна валюта, заснована на криптографічних методах захисту, яка може виступати в якості платіжного засобу, майна і як засіб зберігання вартості в базі даних, при цьому вона не емітується і нічим не забезпечена.

## 1.2 Аналіз технічних рішень для здійснення крипто валютних операцій

Криптовалюті притаманні деякі властивості електронних фіатних грошей, такі як безготівкова форма, конвертованість, проведення віддалених операцій, але при цьому є істотні відмінності, а саме децентралізація, відсутність посередників і емісії.

Разом з тим всі учасники в мережі здійснюють миттєві операції між собою, без посередників, тому цю мережу називають одноранговою або пірінговою (в перекладі з англійської мови – peer to peer – рівний до рівного).

Існують три основних легальних способи придбання криптовалюти.

Здійснення Майнінг за допомогою комп'ютерних ферм, призначених для проведення обчислень за заданим алгоритмом. (При цьому у випадку з біткойнами Майнер отримують винагороду за кожен видобутий блок в розмірі 6,25 біткойнів, розмір винагороди змінюється кожні 4 роки) [8].

Підключення до хмарних майнінгових сервісів за невелику абонентську плату для здійснення майнінгових операцій. Майнінг – це спосіб отримання криптовалюти, заснований на вирішенні математичних обчислень за допомогою комп'ютерів [9].

Здійснення покупки за поточним курсом на біржі або безпосередньо у дилерів.

Процедура проведення транзакції на прикладі оплати криптовалютою за певний товар, виглядає наступним чином:

1. Покупець направляє в мережу зі свого гаманця певну кількість криптовалюти у вигляді блоку транзакції із зашифрованим хешем.

2. Новий блок розсилається всім учасникам мережі для перевірки його на валідність.

3. У разі підтвердження транзакції всіма учасниками мережі, новий блок приєднується до попередніх блоків, які містять інформацію про всі попередні транзакції.

4. Після завершення зазначених процедур криптовалюта переводиться до продавця (рисунок 1.1).

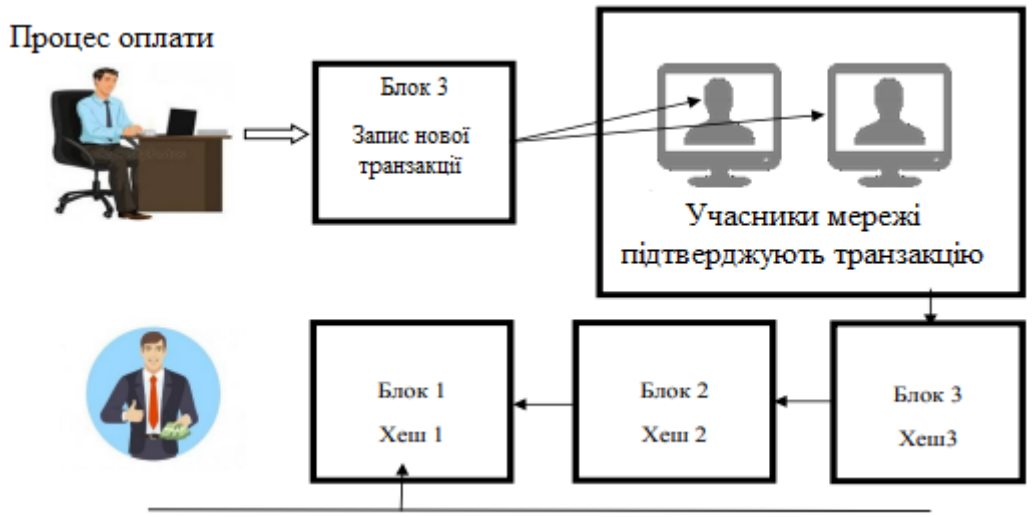



Рисунок 1.1 – Схема транзакції

До основних переваг криптовалюти можна віднести високу ступінь надійності, так як їх практично неможливо підробити.

Крім того, криптовалюта є дефляційним інструментом і виключає ризики інфляції, так як має обмежений ліміт емісії. Також в криптовалютних транзакціях відсутня Комісія при здійсненні переводу або вона незначна, а також забезпечується збереження і незмінність даних записаних транзакцій в

блокчейн, що також є привабливою стороною для користувачів. Децентралізованість платформи тобто відсутність центральної регулюючої системи, викликає багато суперечок, але в більшості випадків її визнають позитивною якістю.

Разом з тим поряд з наявними перевагами, криптовалюта має безліч недоліків, найбільш значущі з них: Висока волатильність криптовалюти і її незабезпеченість є основними причинами негативного сприйняття з боку державних органів і фінансових інститутів.

Основною перешкодою для імплементації криптовалюти у фінансову систему є неможливість контролювання її емісії. Державні банки не мають можливості контролювати операції з випуску та обігу криптовалюти, відповідно цей фактор викликає певну недовіру держави і населення до даного фінансового інструменту. Відсутність нормативного регулювання обороту криптовалюти і гарантій по поверненню заощаджень в разі втрати криптовалютних ключів також можна віднести до недоліків.

Викликає багато критики анонімність користувачів криптовалют з точки зору появи ризиків зростання шахрайських дій з її використанням. І нарешті, для того щоб грамотно оперувати з криптовалютою, необхідні знання не тільки у фінансовій сфері, потрібно володіти також навичками сучасних цифрових технологій.

**Висновки до розділу**

У рамках першого розділу окреслено поняття «криптовалюта» на основі аналізу сучасних наукових надбань, так під криптовалютою розуміємо віртуальну валюту, засновану на криптографічних методах захисту, яка може виступати в якості платіжного засобу, майна і як засіб зберігання вартості в базі даних, при цьому вона не емітується і нічим не забезпечена.

Проаналізовано сучасні технічні рішення для здійснення крипто валютних операцій.

# РОЗДІЛ 2
# СУЧАСНИЙ СТАН КРИПТО ВАЛЮТНИХ ТЕХНОЛОГІЙ

## 2.1 Методи та моделі здійснення крипто валютних операцій

Криптовалюта може бути передана будь-кому, хто повідомить коректну крипто-адресу або відкритий ключ. Для передачі криптовалюти поточний власник створює нову транзакцію, яка, крім вказівок про кількість переданої криптовалюти, містить підписаний ініціатором хеш попередньої транзакції, по якій криптовалюта була отримана. Попередня транзакція стає «входом» поточної транзакції. Також вказується публічний ключ або крипто-адреса нового одержувача ( «вихід») (рис. 2.1). Транзакція широкомовним запитом по відкритих каналах без шифрування відправляється в мережу. Решта вузлів мережі, перш ніж прийняти транзакцію до обробки, перевіряють підписи. Правильність підпису свідчить, що ініціатор дійсно є власником секретного ключа для адреси «виходу».

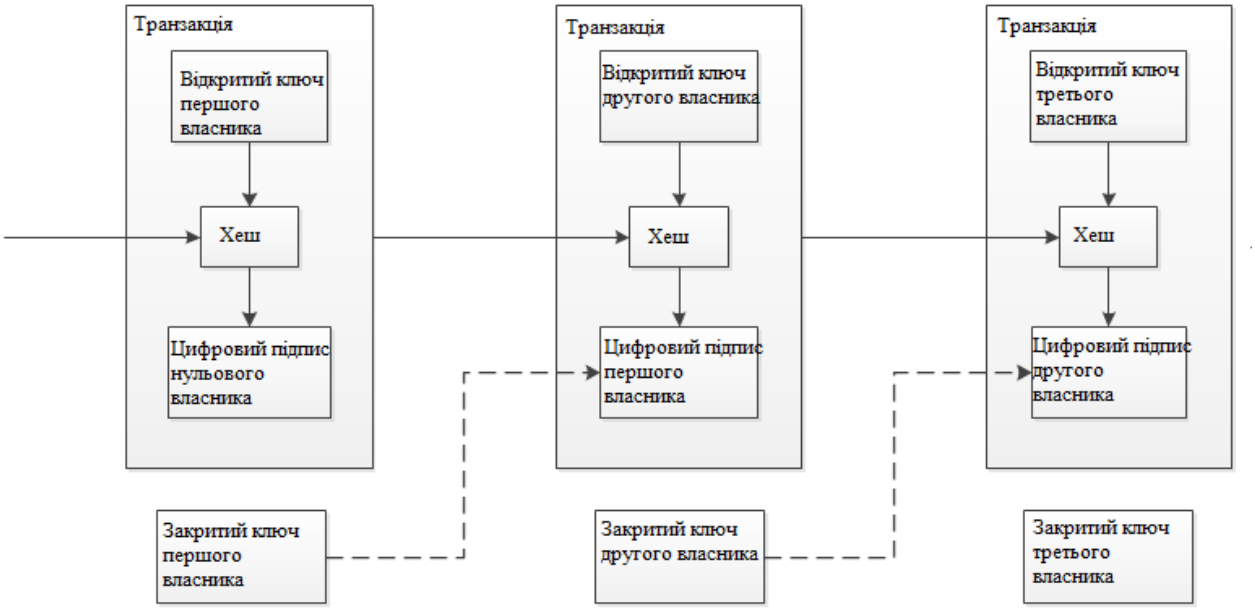



Рисунок 2.1 – Спрощена структура послідовних транзакцій з одним входом і одним виходом

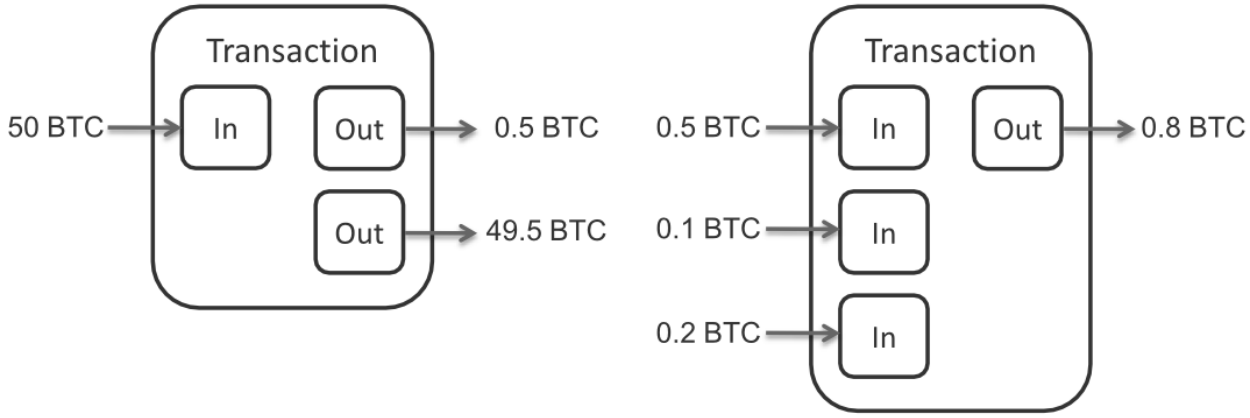



Рисунок 2.2 – Приклади множинних входів і виходів у транзакціях [11]

Окремі транзакції об'єднують разом з іншими транзакціями в спеціальну структуру – блок. Інформація в блоках відкрита, не шифрується, її можна швидко перевірити ще раз.

Кожен блок завжди містить свій порядковий номер і хеш попереднього блоку. Всі блоки можна вибудувати в один ланцюжок, який містить інформацію про всі скоєні операції з криптовалютою.

Перша транзакція в блоці завжди формується автоматично і передає винагороду за створення блоку [12]. Решту наповнення блоку беруть з черги транзакцій, які ще не були записані в попередні блоки. Не всякий сформований блок буде прийнятий іншими учасниками. Потрібно, щоб числове значення хешу заголовка не перевищувало встановленого значення (параметр «складність»). Чим менше задано значення, тим менше ймовірність виконання умови. У службовій області блоку виділено місце для довільних значень. Якщо хеш заголовка незадовільний, довільні значення замінюються на нові і розрахунок хешу повторюється. Результат хешування (функції SHA-256) непередбачуваний, тому немає алгоритму цілеспрямованої зміни довільної області для досягнення бажаного результату. Зазвичай потрібна велика кількість перерахунків.

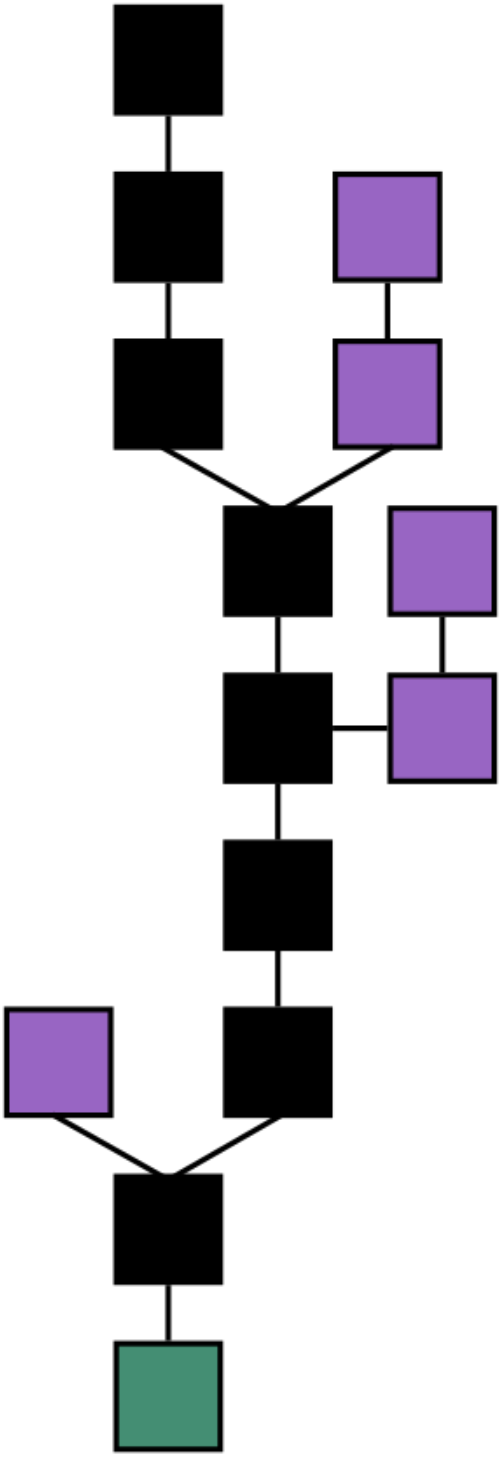


Рисунок 2.3 – Основна послідовність блоків (чорні) є найдовшою від початкового (зелений) до поточного. Побічні гілки (фіолетові) відсікаються

Збереження даних щодо транзакцій здійснюється із застосуванням методу Меркла [13]. Даний підхід запропонований у 1979 році Ральфом

Мерклом. Базується метод на побудові дерева, яке містить листя, вузли та коріння (рис. 2.4)

Листя дерева Меркла є хеш-значеннями для блоків даних щодо проведених транзакцій, які необхідно зібрати в структуру. Вузол дерева є значенням, яке було отримано внаслідок конкатенації та подальшого хешування двох дочірніх вузлів або листя. Корінь дерева Меркла також є вузол, що знаходиться на вершині дерева.

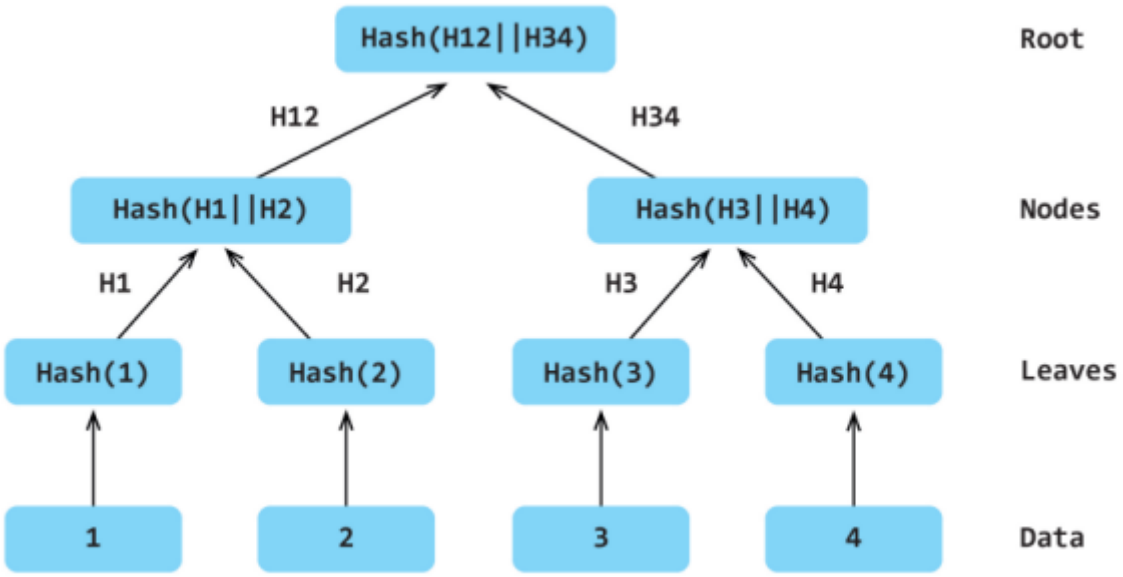



Рисунок 2.4 – Дерево Меркла

Цілістність даних щодо транзакцій перевіряється за допомогою обчислення хеш-коду у відповідності до методу Меркла (рис. 2.5). Математично це виглядає як:

$$\langle\left(h_n^i, h_n^{i+1}\right), \left(h_{n-1}^i, h_{n-1}^{i+1}\right), \ldots, \left(h_1^i, h_1^{i+1}\right), h_0\rangle$$

де:

$h$ – хеш-код блоку даних;

$i$ – номер поточного блоку;

$n$ – загальна кількість блоків у блокчейні.

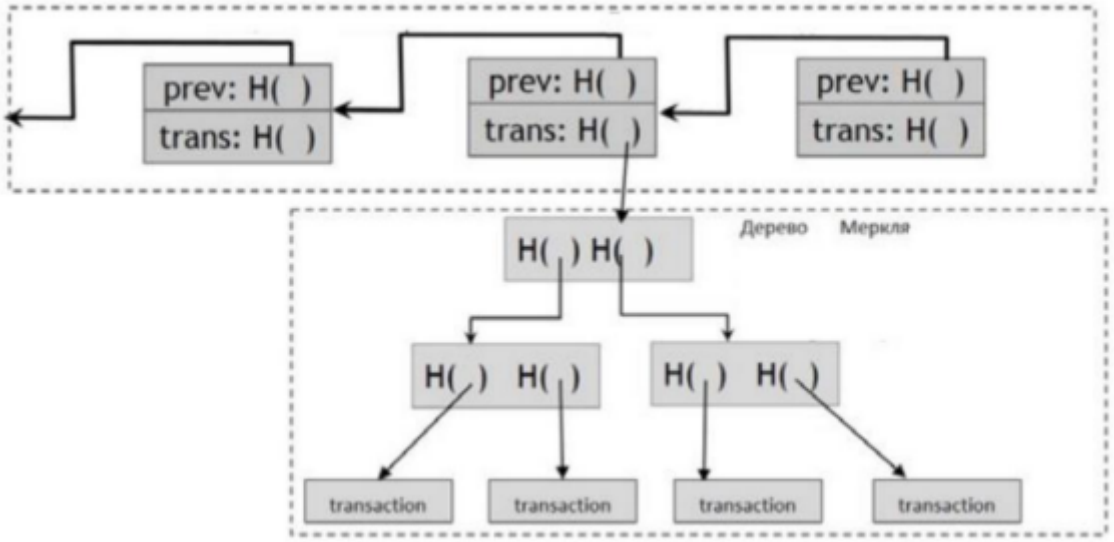



Рисунок 2.5 – Принцип формування ланцюжка блоку транзакцій у відповідності до методу Меркля

Виявлення розбіжностей у вузлах схематично представлено на рисунку 2.6.

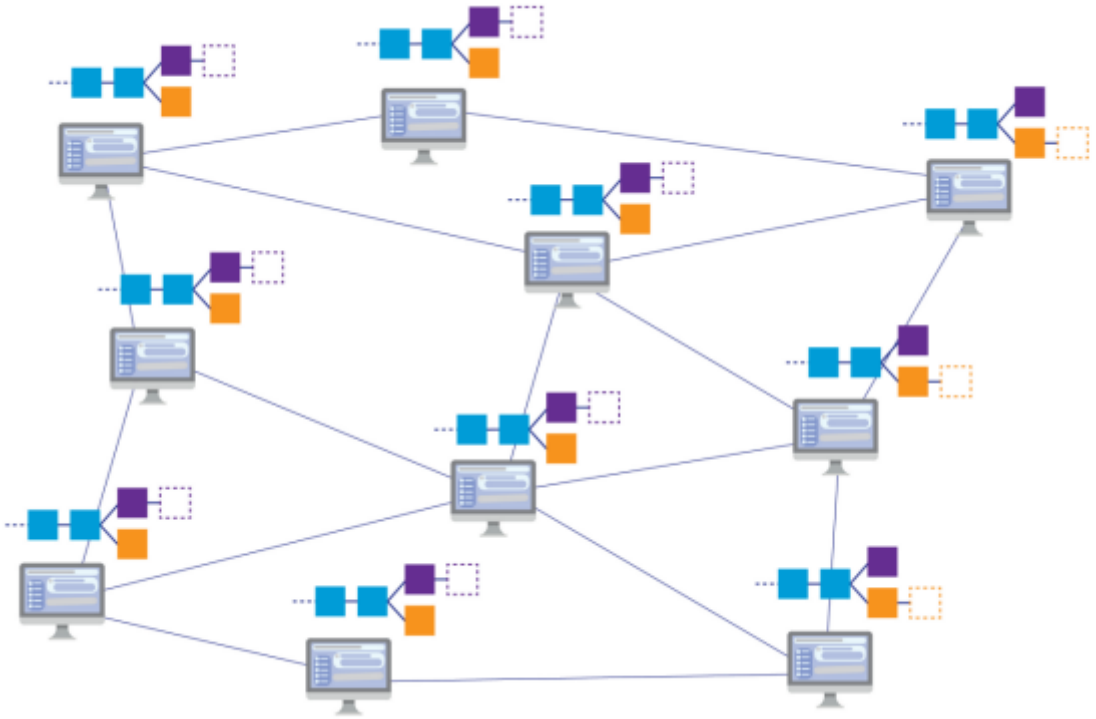


Рисунок 2.6 – Схема виявлення розбіжностей

Блоки які не відповідають дійсності видаляються. Учасники процесу транзакцій виявляються недостовірну інформацію та вказують на неї. При цьому результати перевірки однієї і тієї ж транзакції можуть бути різними.

Враховуючи той факт, що передача крипто валюти відбувається у мережі Інтернет, а кожен окремий учасник формує власну мережу передачі в якій різна обчислювальна потужність та часовий простір, формування ланцюгів відбувається різної довжини (рис. 2.7).

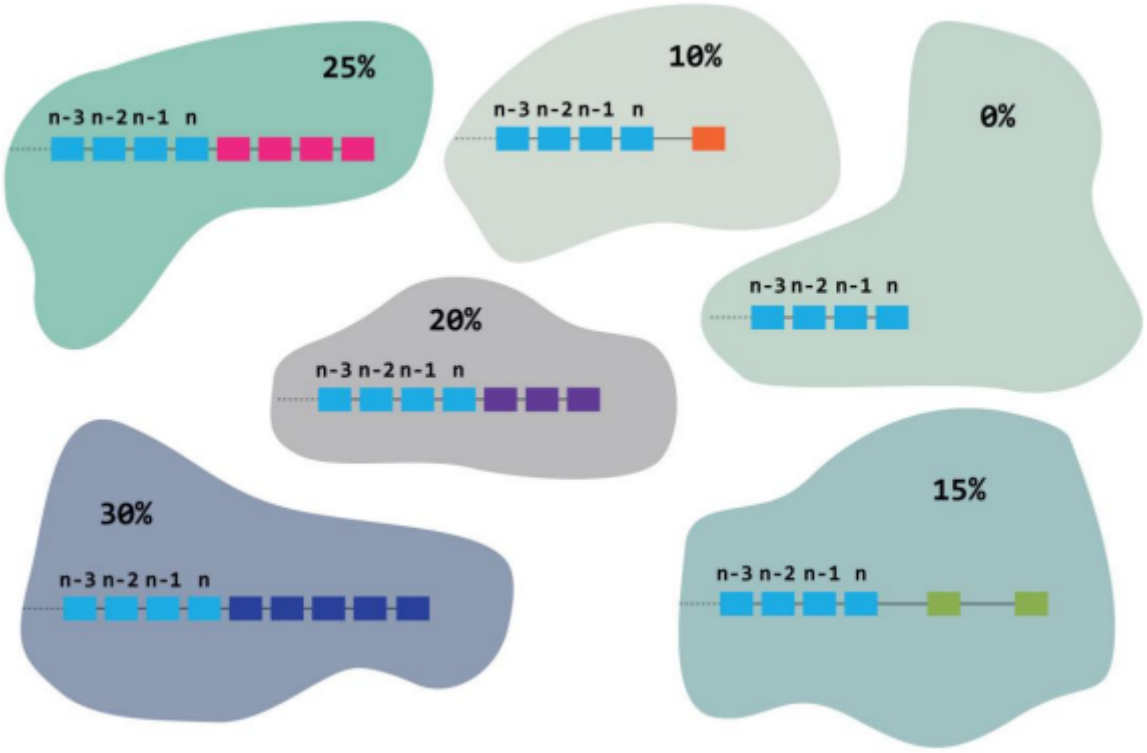



Рисунок 2.7 – Мережа формування ланцюгів блоків

У разі, коли з’єднання відновиться, вузли мережі починають синхронізуватися між собою, та як наслідок виходить загальна схема після повної синхронізації усіх під мереж задіяних у передачі крипто валюти (рис. 2.8).

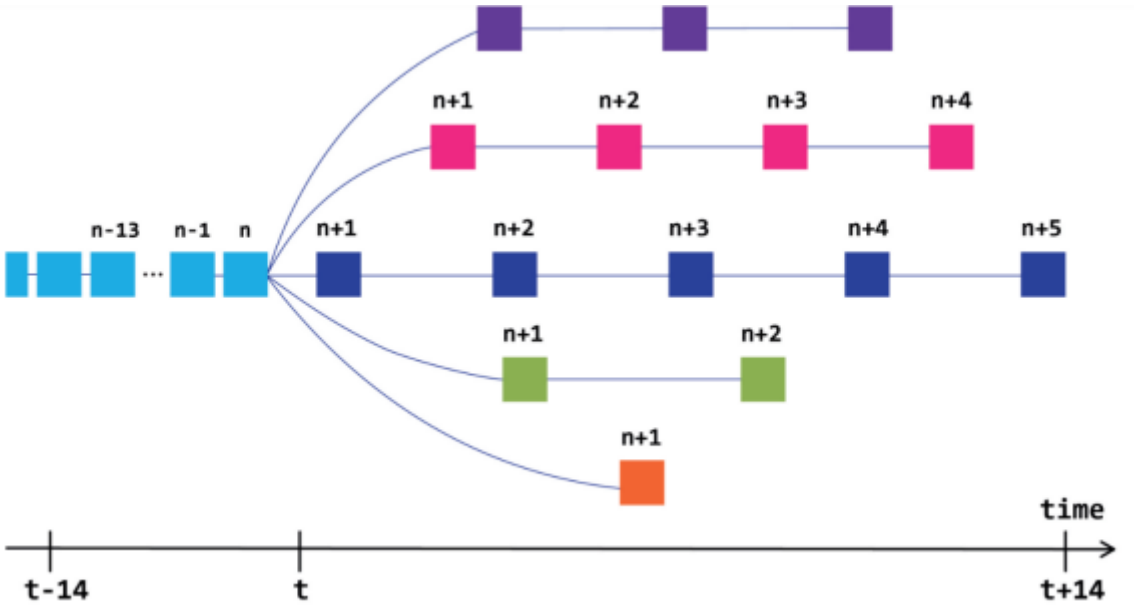



Рисунок 2.8 – Загальна схема після повної синхронізації усіх під мереж задіяних у передачі крипто валюти

## 2.2 Алгоритм реалізації блокчейн

Як відомо, блокчейн (ланцюг блоків) – це багаторівнева і багатофункціональна інформаційна технологія, призначена для надійного обліку різних активів, що включає в себе функції зберігання, комунікації та архівування [14].

У випадку з криптовалютами блокчейн виступає як розподілений реєстр, в якому підтверджені транзакції зберігаються в блоках, а самі блоки зв'язуються між собою єдиним ланцюгом, при цьому вся інформація про транзакції шляхом складних обчислень набуває унікальний вид хешкоду. Специфіка технології передбачає, що в кожен наступний блок транзакцій включається «хеш» початкової транзакції. Це багаторазово збільшує складність підбору ключів і робить ланцюжок надійно захищеним від злому, як показано на рисунку 2.9.

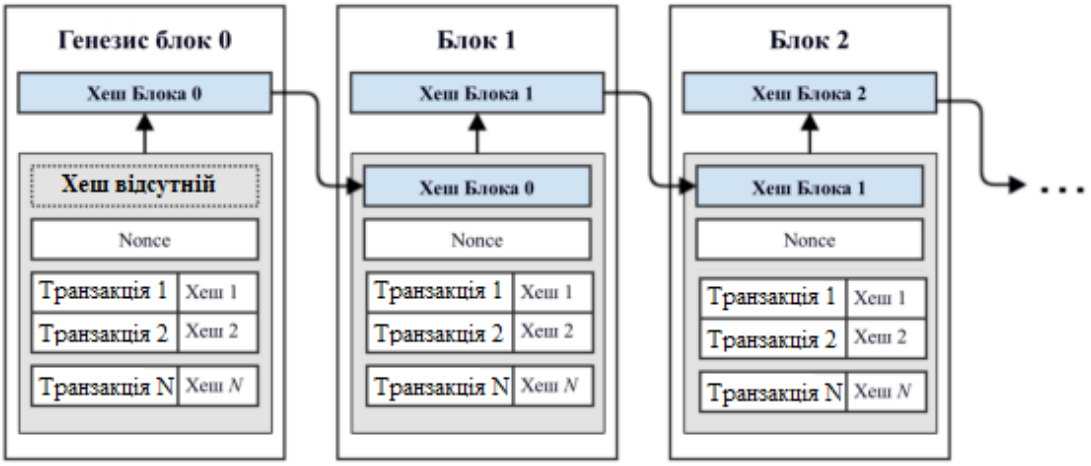



Рисунок 2.9 – Структура блокчейн-транзакції

Кожен блок в блокчейні посилається на попередній блок, даний зв'язок реалізовано за допомогою хеш-значень. Необхідно відзначити, що існує так званий блок генезису (genesis block). Це найперший блок, у якого немає батьківського блоку на відміну від інших. Далі детально розглянемо типову структуру блокчейн мережі.

Кожен блок в блокчейн мережі складається з двох головних частин – заголовка (head) і тіла (payload). Head містить інформацію, яка відповідає за стабільність, а також імутабельність мережі. Payload – містить список всіх транзакцій, які повинні бути збережені в даному блоці і потрапити в блокчейн-мережу (БМ) [15]. На (рис. 2.10) приведена структура блоків БМ.

У класичній блокчейн мережі Head містить наступні поля:

- номер версії блоку (ver_block);
- хеш попереднього блоку (prev_block);
- хеш усіх транзакцій у поточному блоці (mrkl_root);
- тимчасову мітку, коли був створений блок (timestamp);
- «bits» і «nonce» параметри використовуються при Майнінгу.

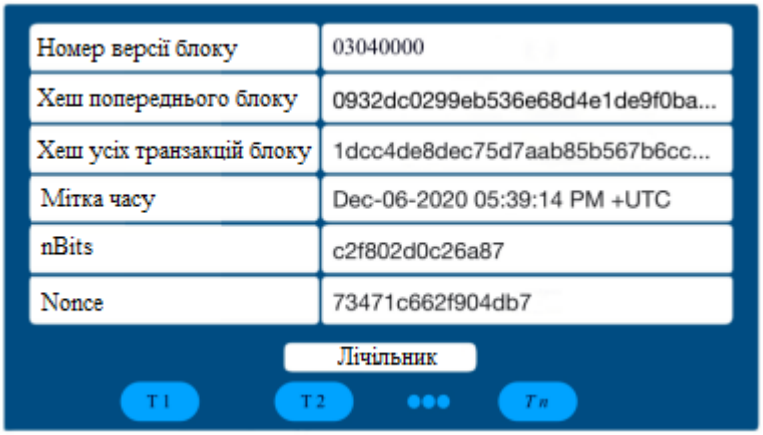



Рисунок 2.10 – Структура блоку

Як раніше згадувалося payload складається з лічильника транзакцій і списку всіх транзакцій які входять в поточний блок. Також існує максимальна кількість транзакцій, яку може містити блок. Дане значення залежить від розміру транзакції. Для того щоб перевірити справжність транзакції використовується механізм асиметричної криптографії [16].

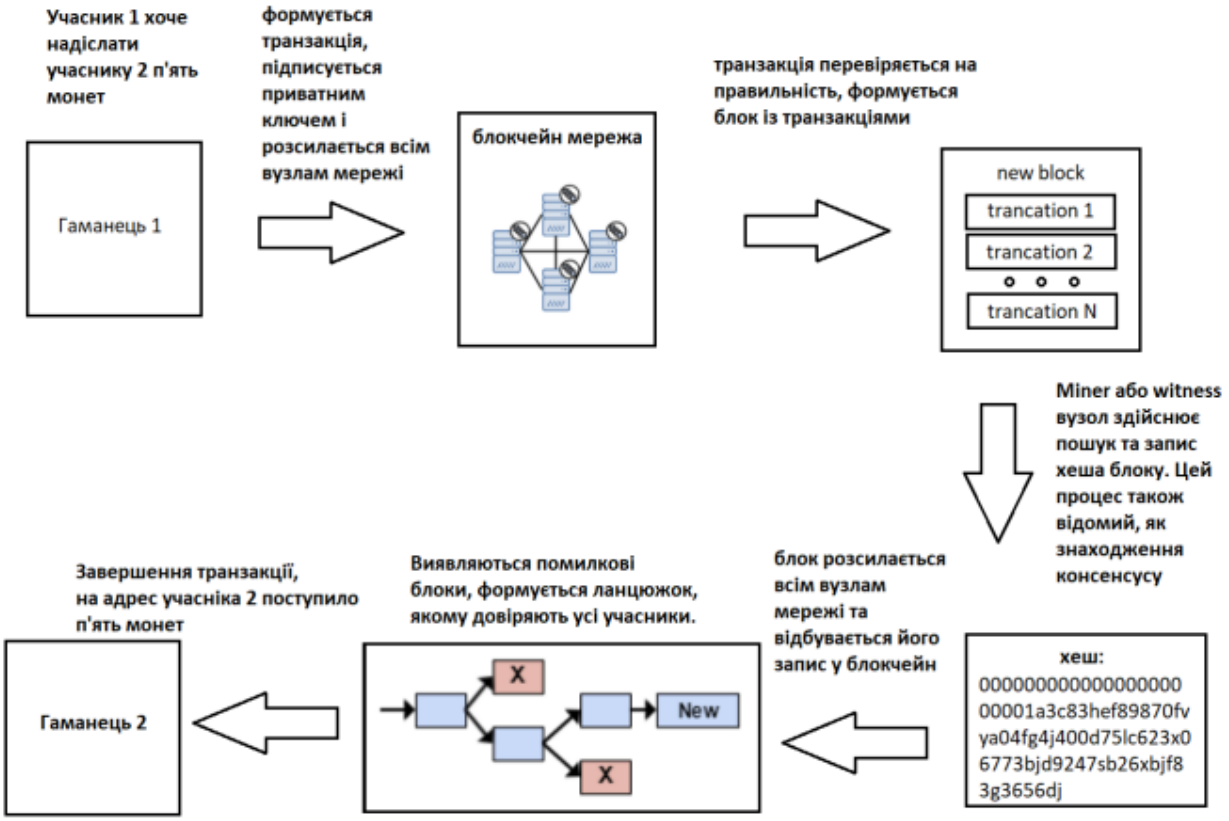



Рисунок 2.11 – Схема алгоритму реалізації блокчейн

Цифровий підпис – це криптографічний алгоритм, застосовуваний Користувачем до документа (Повідомлення), який використовується для перевірки справжності та цілісності документа (повідомлення), а також для посвідчення авторства по відношенню до документа (Повідомлення) [17]. Криптографія з відкритими ключами (public-key cryptography) і хеш-функції надають математичні засоби, що дозволяють ефективно використовувати цифровий підпис. Відзначимо, що використання хешування і цифрових підписів є необхідним для блокчейн технології (БТ). Хешування дає можливість кожному з учасників мережі визначити поточний стан блокчейна. А підписи забезпечують доказ того, що всі транзакції були здійснені тільки справжніми власниками. Для більшого розуміння розглянемо докладний приклад використання цифрового підпису в БТ (рис. 2.12).

Кожному користувачеві блокчейн мережі належить пара, відкритого і закритого ключів. Закритий ключ користувач використовує для здійснення угод. Угоди, підписані цифровим підписом, поширюються по всій блокчейн мережі і за допомогою відкритих ключів можна отримати доступ до них. Відкриті ключі доступні кожному користувачеві блокчейн мережі.

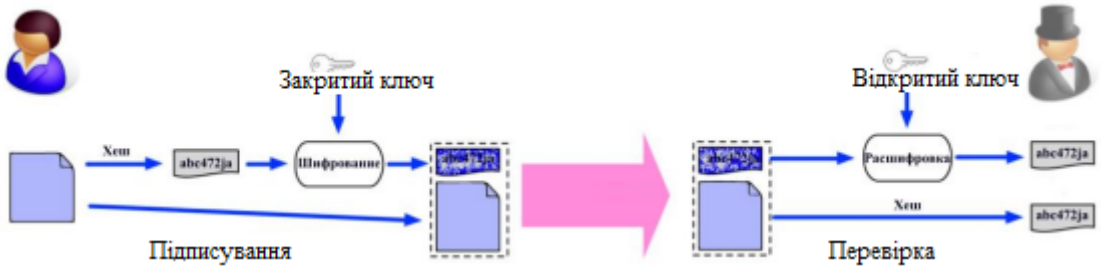



Рисунок 2.12 – Схема використання цифрового підпису в БТ

Базовий алгоритм підписання документа (Повідомлення) цифровим підписом включає два етапи: етап підписання та етап перевірки. Розглянемо приклад, описаний на (рис. 2.12). Скажімо, Аліса хоче підписати транзакцію. Спочатку їй необхідно обчислити хеш-значення самої транзакції.

Використовуючи свій закритий ключ Алісі необхідно зашифрувати отримане хеш-значення транзакції. Потім зашифрований хеш із вихідними даними Аліса надсилає Бобу. Для перевірки достовірності отриманих даних Бобу необхідно виконати розшифрування даних за допомогою відкритого ключа Аліси. Потім Бобу потрібно обчислити хеш-значення вихідних даних, використавши ту ж хеш-функцію, якою скористалася Аліса. І шляхом порівняння даних, отриманих на етапі розшифрування і обчислення хеш-значення Боб, може зробити висновки про справжність транзакції. У блокчейн мережах в якості алгоритмів цифрових підписів використовується Elliptic Curve Digital Signature Algorithm (ECDSA) [18].

**Висновки до розділу**

У рамках другого розділу наведено результати дослідження основних методів та моделей здійснення крипто валютних операцій. Зазначається, що для передачі криптовалюти поточний власник створює нову транзакцію, яка, крім вказівок про кількість переданої криптовалюти, містить підписаний ініціатором хеш попередньої транзакції, по якій криптовалюта була отримана. Попередня транзакція стає «входом» поточної транзакції. Описано метод Меркла, який базується на побудові дерева, яке містить листя, вузли та коріння та відповідає за збереження даних щодо транзакцій.

Наведено детально алгоритм реалізації блокчейн. Наголошено, що у випадку з криптовалютами блокчейн виступає як розподілений реєстр, в якому підтверджені транзакції зберігаються в блоках, а самі блоки зв'язуються між собою єдиним ланцюгом, при цьому вся інформація про транзакції шляхом складних обчислень набуває унікальний вид хешкоду. Специфіка технології передбачає, що в кожен наступний блок транзакцій включається «хеш» початкової транзакції.

# РОЗДІЛ 3
# ПРАКТИЧНІ АСПЕКТИ ЗДІЙСНЕННЯ КРИПТО ВАЛЮТНИХ ОПЕРАЦІЙ

## 3.1 Розробка веб-додатку для здійснення крипто валютних операцій

Для реалізації веб-додатку для здійснення крипто валютних операцій обрано каскадну модель життєвого циклу (рис. 3.1), яка реалізує, принцип одинарного виконання кожного з основних процесів і етапів в їх визначених рамках. Перехід на наступний етап реалізується після того, як буде проведена робота на поточному етапі, і відкатів на здійсненній стадії не передбачено. Кожен етап закінчується придбанням певного результату, який використовується в якості базової інформацій для наступного етапу.


Рисунок 3.1 – Етапи розробки веб-додатку для здійснення крипто валютних операцій

Загальна структура клієнт-серверної взаємодії з боку сервера представлена на рис. 3.2.

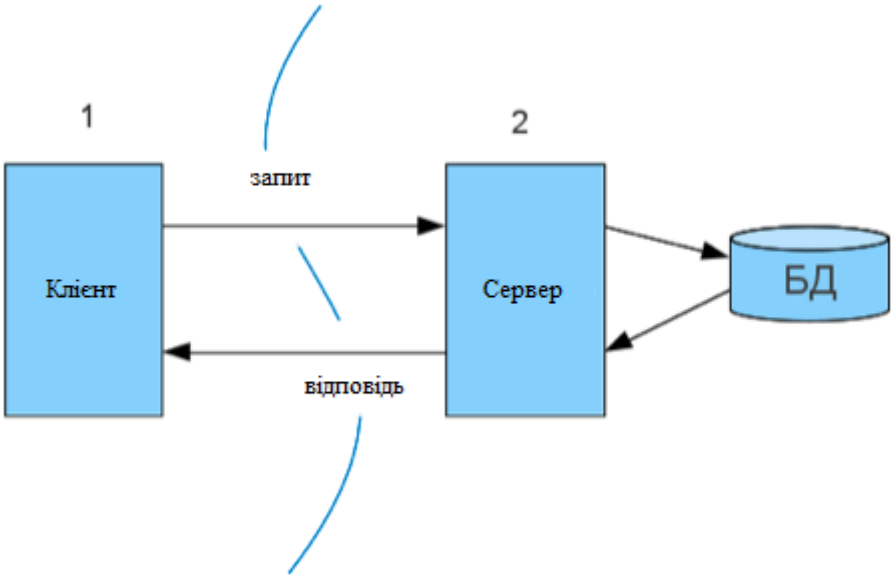



Рисунок 3.2 – Загальна структура клієнт-серверної взаємодії з боку сервера

Однак, у рамках роботи розглянемо цей же погляд з боку клієнта, і у зв'язку з цим, немає ніякої різниці між двуланковою і три ланковою архітектурою.

Може бути безліч клієнтів, які використовують один акаунт для спілкування з сервером.

Кожен клієнт, як правило, має своє власне локальне сховище. Таким чином, у ряді випадків, локальне сховище може бути синхронізоване з хмарою, і, відповідно, з кожним із клієнтів. Оскільки це окремий випадок і не впливає на архітектуру програми, опускаємо його.

Реалізація веб-додатку для здійснення крипто валютних операцій відбувається за допомогою .NET SDK 5.0 та Visual Studio Community Edition.

Код для класу транзакцій реалізується як:

```
public class Block
{
    public int Height { get; set; }
    public Int64 TimeStamp { get; set; }
    public byte[] PrevHash { get; set; }
    public byte[] Hash { get; set; }
    public Transaction[] Transactions { get; set; }
    public string Creator { get; set; }
}
```

Визначення нової транзакції описується функцією:

```
// Створення нової транзакції
var trx1 = new Transaction
{
   TimeStamp = DateTime.Now.Ticks,
   Sender = "Bob",
   Recipient = "Billy",
   Amount = 10,
   Fee = 0.01
};

// Створення нової транзакції
var trx1 = new Transaction
{
   TimeStamp = DateTime.Now.Ticks,
   Sender = "John",
   Recipient = "Ivanka",
   Amount = 20,
   Fee = 0,01
 };

// Створення нової транзакції
var trx1 = new Transaction
{
   TimeStamp = DateTime.Now.Ticks,
   Sender = "Robert",
   Recipient = "Antonio",
   Amount = 30,
   Fee = 0.01
```

Метод *AddTransactionToPool* у класі Blockchain

```
// пул транзакцій
public List<Transaction> TransactionPool = new List<Transaction>();


// Додати транзакцію до пулу
public void AddTransactionToPool(Transaction trx)
{
    TransactionPool.Add(trx);
}
```

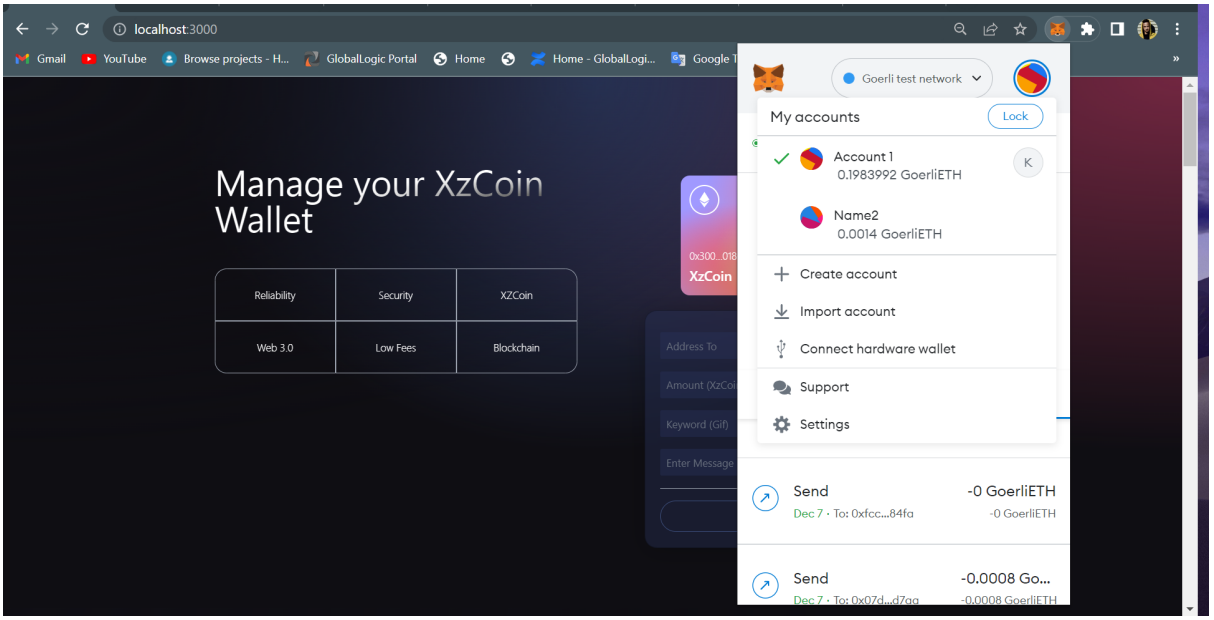
Формуємо останній блок

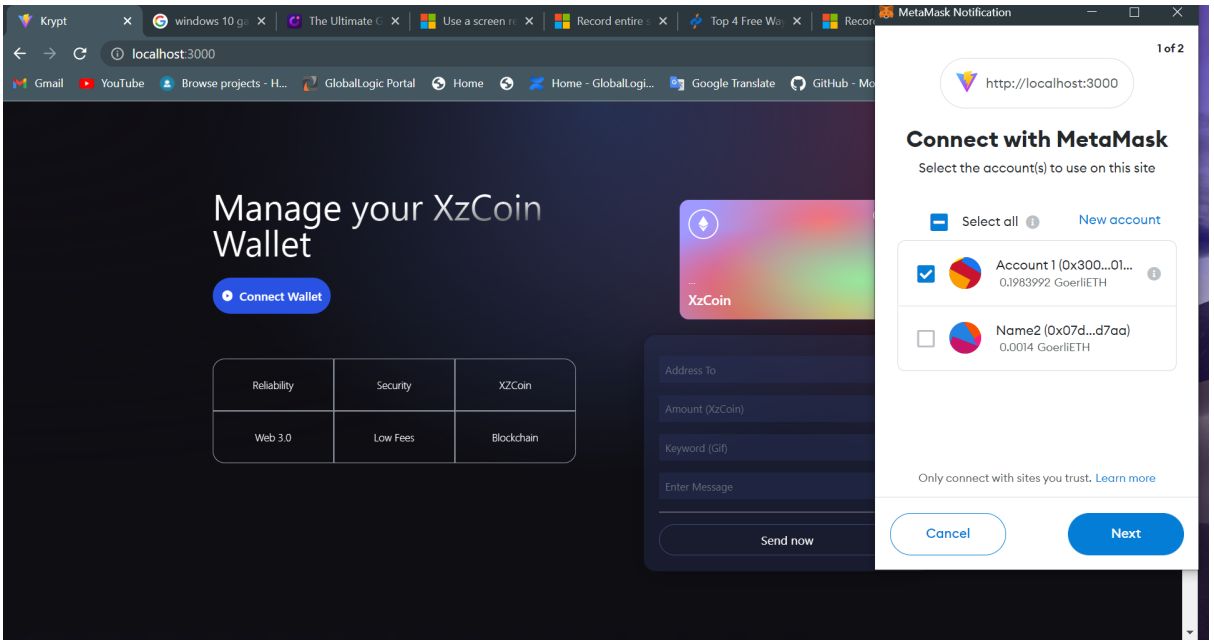
```
public void PrintLastBlock()
{
   Console.WriteLine("\n\n==== Останній блок ====");
   var lastBlock = GetLastBlock();
   PrintBlock(lastBlock);
}
```

Надалі проведемо тестування створеного веб-додатку.

### 3.2 Тестування додатку для здійснення крипто валютних операцій

```
====================
Height          : 1
Version         : 1
Timestamp       : 29.05.2022 03:00:00
Hash            : 2e858f847d61bcf7fbee889fc4c8ccbbfe72a5bbb5f1e7c8804d652d3015b24a
Merkle Hash     : ea45ed84dd4d10402e138b83e5b84c8b875d42e01489b0c808d5158e27d513aa
Prev. Hash      : -
Validator       : 5B51TvVoEyxaqg8yeBg8Ht6HMbFypPGJNFQsn8BB324M
Difficulty      : 1
Num of Txs      : 2
Total Amount    : 5000000000
Total Fee       : 0
Size            : 1753
Build Time      : -598
Transactions:
   ID           : d711ec6d8fa515dc4e9ec1b293de949bc3677099ed29bb5d642c81c27b847012
   Timestamp    : 19.05.2022 13:28:24
   Sender       : 9SBqYME6T5trNHXqdsYPMPha4yWQbzxd4DPjJBR7KG9A
   Recipient    : 9SBqYME6T5trNHXqdsYPMPha4yWQbzxd4DPjJBR7KG9A
   Amount       : 2,000,000,000.00
   Fee          : 0.0000
   - - - - - -
   ID           : bbf3dfd19a4ddad2f74e7b62f6751d266cb5853cb069958cd0ca2ebbf86d2497
   Timestamp    : 19.05.2022 13:28:24
   Sender       : 3pXA6G3o2bu3Mbp9k2NDfXGWPuhCMn4wvZeTAFCf4N5r
   Recipient    : 3pXA6G3o2bu3Mbp9k2NDfXGWPuhCMn4wvZeTAFCf4N5r
```




## Висновки до розділу

У рамках третього розділу здійснено розробку блокчейну, криптовалюти та веб-додатку для здійснення крипто валютних операцій та проведено його тестування. Під час тестування збоїв та недоліків у роботі програми не виявлено, що говорить про високу якість розробки та можливість впровадження у реальну практику за потребою.

# ВИСНОВКИ

У межах виконання даної магістерської роботи проведено аналіз сучасних технологій, методів та моделей здійснення крипто валютних операцій та розроблено блокчейну та крипто валюту через .net. На основі вищевикладеного варто зробити наступний висновок:

Під криптовалютою розуміємо віртуальну валюту, засновану на криптографічних методах захисту, яка може виступати в якості платіжного засобу, майна і як засіб зберігання вартості в базі даних, при цьому вона не емітується і нічим не забезпечена. Криптовалюті притаманні деякі властивості електронних фіатних грошей, такі як безготівкова форма, конвертованість, проведення віддалених операцій, але при цьому є істотні відмінності, а саме децентралізація, відсутність посередників і емісії.

Зазначається, що для передачі криптовалюти поточний власник створює нову транзакцію, яка, крім вказівок про кількість переданої криптовалюти, містить підписаний ініціатором хеш попередньої транзакції, по якій криптовалюта була отримана. Попередня транзакція стає «входом» поточної транзакції. Описано метод Меркла, який базується на побудові дерева, яке містить листя, вузли та коріння та відповідає за збереження даних щодо транзакцій.

Наведено детально алгоритм реалізації блокчейн. Наголошено, що у випадку з криптовалютами блокчейн виступає як розподілений реєстр, в якому підтверджені транзакції зберігаються в блоках, а самі блоки зв'язуються між собою єдиним ланцюгом, при цьому вся інформація про транзакції шляхом складних обчислень набуває унікальний вид хешкоду. Специфіка технології передбачає, що в кожен наступний блок транзакцій включається «хеш» початкової транзакції.

Для реалізації веб-додатку для здійснення крипто валютних операцій обрано каскадну модель життєвого циклу, яка реалізує, принцип одинарного виконання кожного з основних процесів і етапів в їх визначених рамках.

Реалізація веб-додатку для здійснення крипто валютних операцій відбувається за допомогою .NET SDK 5.0 та Visual Studio Community Edition.

Під час тестування збоїв та недоліків у роботі програми не виявлено, що говорить про високу якість розробки та можливість впровадження у реальну практику за потребою.

# СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Щотижневий огляд ринку криптовалют від Huobi Global. – Електронний ресурс. – Режим доступу. – https://insider-media.net/life/shhotiznevii-oglyad-rinku-kriptovalyut-vid-huobi-global

2. Khan A., Salah K. IoT security: Review, blockchain solutions, and open challenges // Future Generation Computer Systems. 2018. Vol. 82. pp. 395-411.

3. Reyna A., Martín C., Chen J., Soler E., Díaz M. On blockchain and its integration with IoT. Challenges and opportunities // Future generation computer systems. 2018. Vol. 88. pp. 173-190.

4. Panarello A., Tapas N., Merlino G., Longo F., Puliafito A. Blockchain and IoT integration: A systematic survey // Sensors. 2018. Vol. 18. № 8. pp. 2575.

5. Miraz H., Ali M. Applications of blockchain technology beyond cryptocurrency // Annals of Emerging Technologies in Computing (AETiC). 2018. Vol. 2. № 1. pp. 20-26.

6. Sanyal, Shouvik & Laddunuri, Madan & Subramanian, Sp Mathiraj & Bose, Vijay & Booshan, Bharath & Shivaram, Chethan & Bettaswamy, Manasa & Booshan, Shabista & Thangam, Dhanabalan. (2022). Enhancing Cybersecurity Through Blockchain Technology Enhancing Cybersecurity Through Blockchain Technology. 10.4018/978-1-6684-5284-4.ch011.

7. Liu Z., Luong C., Wang W., Niyato D., Wang P., Liang YC., Kim DI. A survey on blockchain: A game theoretical perspective // IEEE Access. 2019. Vol. 7. pp. 47615-47643.

8. Conti M., Kumar S., Lal C., Ruj S. A survey on security and privacy issues of bitcoin // IEEE Communications Surveys & Tutorials. 2018. Vol. 20. № 4. pp. 3416-3452.

9. Khalilov M., Levi A. A survey on anonymity and privacy in bitcoin-like digital cash systems // IEEE Communications Surveys & Tutorials. 2018. Vol. 20. № 3. pp. 2543-2585.

10. Purwono, Purwono & Ma'arif, Alfian & Rahmaniar, Wahyu & Haq, Qazi Mazhar Ul & Herjuno, Dimas & Naseer, Muchammad. (2022). Blockchain Technology. 8. 199-205. 10.26555/jiteki.v8i2.24327.

11. Lao L., Li Z., Hou S., Xiao B., Guo S., Yang Y. A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling // ACM Computing Surveys (CSUR). 2020. Vol. 53. № 1. pp. 1-32.

12. Butun I., Osterberg P., Song H. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures // IEEE Communications Surveys & Tutorials. 2019. Vol. 22. № 1. pp. 616-644.

13. Ferrag A., Shu L., Yang X., Derhab A., Maglaras L. Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges // IEEE access. 2020. Vol. 8. pp. 32031-32053.

14. Pradeep, Vijayan & R, Pushvin & V, Raghavendra & Rakshith,. (2022). Blockchain Technologies. International Journal of Advanced Research in Science, Communication and Technology. 396-399. 10.48175/IJARSCT-5839.

15. Wang Q., Yu J., Peng Z., Bui C., Chen S., Ding Y., Xiang Y. Security Analysis on dBFT protocol of NEO // International Conference on Financial Cryptography and Data Security. 2020. pp. 20-31.

16. Habib, Gousia & Sharma, Sparsh & Ibrahim, Sara & Ahmad, Imtiaz & Qureshi, Shaima & Ishfaq, Malik. (2022). Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. Future Internet. 14. 341. 10.3390/fi14110341.

17. Clott C., Hartman B., Beidler B. Sustainable blockchain technology in the maritime shipping industry // Maritime Supply Chains. 2020. pp. 207-228.

18. Kalogiratos, Athanasios & Kantzavelou, Ioanna. (2022). Blockchain Technology to Secure Bluetooth. 10.48550/arXiv.2211.06451.