Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«____» червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітній ступень бакалавр

освітня програма Кібербезпека
(назва освітньо-професійної програми)

на тему: Засоби захисту цілісності інформації з використанням блокчейн технології

Виконавець: студент IV курсу, групи КБ-41

_____ **Олександр СТЕПАНЕЦЬ**
(підпис) (ім'я,ПРІЗВИЩЕ)

	Ім'я, прізвище	**Підпис**
Керівник	Сергій ДАКОВ	

Нормоконтроль	Єлена БОГУСЛАВСЬКА	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентові **КБ-41** (група) **Степанець Олександр Володимирович** (Прізвище Ім'я По-батькові)

Тема кваліфікаційної роботи Засоби захисту цілісності інформації з використанням блокчейн технології

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №3 від 20.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Документації та технічні специфікації криптовалюти, дані блокчейну, транзакції, блоки, адреси гаманців.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Аналіз основних відомостей криптовалюти і локчейн технологій
Аналіз загальнодоступної інформації про кібератаки в криптопросторі.
Розробка рекомендацій по підвищенню безпеки використання криптовалют.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Полягає в розробці рекомендацій по підвищенню безпеки

використання криптовалют та технології блокчейн.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 13 жовтня 2022 року

Завдання видав _____ (підпис) Сергій ДАКОВ (ініціали, прізвище)

Завдання прийняв до виконання _____ (підпис) Олександр СТЕПАНЕЦЬ (ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Отримання завдання	25.10.2022 – 28.11.2022	*виконано*
2	Аналіз літератури	29.11.2022 – 03.01.2023	*виконано*
3	Аналіз джерел	04.01.2023 –19.01.2023	*виконано*
4	Збір відомостей щодо взломів в криптовалюті	22.01.2023 – 27.03.2023	*виконано*
5	Аналіз рішень криптогаманців	28.03.2023 – 15.04.2023	*виконано*
6	Розробка рекомендацій по підвищенню безпеки використання криптовалют.	15.04.2023 – 02.05.2023	*виконано*
7	Написання тексту атестаційної роботи	03.05.2023 – 16.05.2023	*виконано*
8	Оформлення пояснювальної записки	16.05.2023 – 01.06.2023	*виконано*
9	Підготовка та оформлення роботи до захисту	02.06.2023 – 12.06.2023	*виконано*

Завдання видав _____ (підпис) Сергій ДАКОВ (ініціали, прізвище)

Завдання прийняв до виконання _____ (підпис) Олександр СТЕПАНЕЦЬ (ініціали, прізвище)

Термін подання кваліфікаційної роботи до ЕК 12 червня 2023 року

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 62 сторінок основного тексту, 6 таблиць та 2 формули. Список використаних джерел містить 14 найменувань і займає 1 сторінку.

Метою роботи є розробка рекомендацій по підвищенню безпеки використання криптовалют і технології блокчейн.

Об'єктом дослідження є процес захисту інформації при використанні блокчейн технологій.

Предметом дослідження є методи забезпечення безпеки в системах криптовалюти та блокчейн технологій.

Методи дослідження дипломної роботи:

- аналіз літератури;
- аналіз документів;
- порівняння;

Розроблені рекомендації призначені для користувачів, що хочуть забезпечити безпеку своїх персональних даних у блокчейні.

Ключові слова: Криптовалюта, блокчейн, криптогаманець, криптобіржі.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

SHA-256 - Secure Hash Algorithm 256-bit

LMD-GHOST - Latest Message-Driven Greedy Heaviest-Observed Sub-Tree

PoW – Proof-of-Work

PoS – Proof-of-Stake

CEX – Centralized Exchange

DEX – Decentralized Exchange

DeFi – Decentralized finance

DYOR – Do Your Own Research

ЗМІСТ

ВСТУП

В останні кілька років криптовалюти та блокчейн-технології набули значення у сферах фінансів, економіки та технологій. Забезпечуючи нові можливості для безпеки, швидкості та децентралізації, ці винахідливі ідеї змінюють спосіб, яким ми бачимо та використовуємо гроші.

Ця кваліфікаційна робота присвячена вивченню та аналізу функціонування блокчейн-технологій і криптовалют. Криптовалюти, такі як Bitcoin, Ethereum та інші, стали популярні як у інвесторів, так і у підприємців і розробників. Їхній новий метод фінансових операцій дозволяє проводити швидкі, безпечні та ефективні транзакції без посередників.

Натомість блокчейн забезпечує безпеку, цілісність і децентралізацію мережі криптовалюти. Ця революційна технологія забезпечує прозорість і довіру, створюючи розподілені реєстри транзакцій, які не можуть бути змінені чи підроблені.

Метою цієї кваліфікаційної роботи є вивчення та оцінка технічних аспектів криптовалют і блокчейн технологій, а також того, як вони впливають на суспільство та фінансову систему. У цій роботі будуть розглянуті основні принципи, які лежать в основі криптовалюти, процеси консенсусу, криптографічні методи та розробка смарт-контрактів. Будуть також розглянуті питання безпеки, небезпеки та проблеми, пов’язані з роботою з криптовалютами та блокчейн-технологіями.

Тому **метою роботи** є розробка рекомендацій по підвищенню безпеки використання криптовалют і технології блокчейн.

Об’єктом дослідження є процес захисту інформації при використанні блокчейн технологій.

Предметом дослідження є методи забезпечення безпеки в системах криптовалюти та блокчейн технологій.

Практична цінність роботи полягає в розробці рекомендацій для захисту персональних даних і коштів користувачів при використанні криптовалют і технології блокчейн.

Ця кваліфікаційна робота буде корисним для студентів, дослідників, фахівців з кібербезпеки та всіх зацікавлених осіб, які хочуть дізнатися більше про роботу криптовалюти та блокчейн-технологій. Розвиток у цих областях може мати значний вплив на майбутні фінансові та технологічні інновації, тому важливо розуміти їхні цінності та потенціал.

РОЗДІЛ 1
ОПИС БЛОКЧЕЙН ТЕХНОЛОГЇ

1.1 Аналіз технології блокчейн і документації Bitcoin.

Блокчейн - це загальнодоступна база даних, яка оновлюється і використовується на багатьох комп'ютерах у мережі.

"Блок" означає дані і стан, що зберігаються в послідовних групах, відомих як "блоки". Якщо ви відправляєте BTC будь-кому, дані транзакції повинні бути додані в блок, щоб вона була успішною.

"Ланцюжок" ("чейн") означає той факт, що кожен блок криптографічно посилається на свій батьківський об'єкт. Іншими словами, блоки з'єднуються один з одним. Дані в блоці не можуть бути змінені без зміни всіх наступних блоків, що потребуватиме згоди всієї мережі.

Кожен комп'ютер у мережі повинен узгодити кожен новий блок і ланцюжок загалом. Такі комп'ютери називають "вузлами". Вузли гарантують, що всі, хто взаємодіє з блокчейном, мають одні й ті самі дані. Щоб досягти цієї розподіленої угоди, блокчейну потрібен механізм консенсусу.

Зараз Bitcoin використовує консенсус-механізм доказу роботи. Це означає, що будь-хто, хто хоче додати нові блоки даних у ланцюжок, повинен вирішити складну головоломку, для чого потрібно багато обчислювальної потужності. Розв'язання головоломки підтверджує, що ви витратили обчислювальні ресурси. Цей процес називається майнінгом. Майнінг зазвичай здійснюється методом перебору і помилок, але успішне додавання блоку винагороджується в BTC.

Нові блоки транслюються на ноди, перевіряються і підтверджуються, таким чином оновлюючи стан блокчейн мережі для всіх.

У підсумку, коли ви відправляєте кому-небудь BTC, транзакція повинна бути проведена і включена в новий блок. Потім оновлений стан передається всій мережі.

Також важливо знати, що SHA-256 (Secure Hash Algorithm 256-bit) є однією з криптографічних хеш-функцій, яка приймає на вхід послідовність даних будь-якої довжини і генерує хеш-значення фіксованої довжини 256 біт (32 байти). Вона була розроблена Національним інститутом стандартів і технологій США (NIST) та стала широко використовуваною в різних криптографічних застосуваннях, включаючи криптовалюти.

Для криптовалюти SHA-256 є основною хеш-функцією, використовуваною в біткоїні та інших багатьох криптовалютах. В біткоїні вона використовується для хешування блоків, транзакцій та інших даних, а також для Proof-of-Work (доказ роботи) алгоритму, який вимагає вирішення складної обчислювальної задачі для майнерів.

Передумовами створення Біткоїна є те, що повністю одноранговий устрій системи електронних грошей дозволяє здійснювати електронні транзакції між учасниками безпосередньо, минаючи будь-які фінансові інститути.

Частково, це завдання вирішує використання цифрових підписів, але необхідність довіреної особи для контролю за подвійною витратою позбавляє цей підхід основних переваг. Bitcoin - це децентралізоване вирішення проблеми подвійної витрати з використанням одноранговой (пірингової) мережі. Мережа ставить мітки часу на транзакції, з'єднуючи їх у ланцюжок доказів виконаної роботи на основі хешування. Сформовані таким чином записи неможливо змінити, не виконавши заново всього обсягу обчислень. Найдовша версія ланцюжка слугує не тільки підтвердженням черговості подій, а й доводить, що над нею виконав роботу найбільший обчислювальний сегмент мережі. Доти, доки більша частина обчислювальних потужностей контролюється вузлами, не об'єднаними з метою атакувати мережу, вони будуть генеруватимуть найдовший ланцюжок, випереджаючи будь-яких зловмисників. Пристрій самої мережі дуже простий: повідомлення розсилаються на основі принципу "найменших витрат", а вузли можуть залишати мережу і знову підключатися до неї в будь-який момент, приймаючи найдовшу версію ланцюжка для відновлення пропущеної історії транзакцій.

Інтернет-комерція в більшості випадків спирається на фінансові установи, які виступають у ролі довірених посередників для проведення електронних платежів.

Така схема добре працює для більшості транзакцій, але в її основі лежить довіра, що тягне за собою певні проблеми. Необхідне посередництво фінансових інститутів перешкоджає здійсненню незворотних транзакцій. Ціна цих послуг збільшує вартість транзакцій і встановлює мінімальну їхню ціну, роблячи непрактичним проведення нечастих і невеликих транзакцій. Крім того, відсутність незворотних транзакцій збільшує і вартість сервісів, чиї послуги є нескасованими.

Оскільки платіж можна анулювати, продавець змушений бути насторожі, вимагаючи від покупця більше інформації, ніж у принципі необхідно. І певний відсоток шахрайства приймається просто як неминучість. Ці націнки і невизначеності з платіжками можуть бути подолані в разі оборудок з паперовою готівкою, однак механізму для проведення прямих електронних транзакцій не існує.

Необхідна платіжна система, заснована на криптографії, а не на довірі, яка дозволила б будь-яким двом учасникам здійснити переказ коштів безпосередньо, без участі посередника. Обчислювальна дорожнеча скасування транзакцій захистила б продавців від шахрайства, а легкоздійсненні механізми ескроу захистили б покупців. Bitcoin є вирішенням проблеми подвійної витрати, засноване на розподіленому одноранговому сервері міток часу, який своєю обчислювальною потужністю підтверджує хронологічний порядок транзакцій. Система перебуває в безпеці, поки під сукупним контролем її чесних учасників перебуває більше обчислювальної потужності, ніж під контролем групи зловмисників, що діють спільно зловмисників.

Для опису транзакцій визначимо електронну монету як послідовність цифрових підписів. Черговий власник відправляє монету наступному, підписуючи хеш попередньої транзакції та публічний ключ майбутнього власника і приєднуючи цю інформацію до монети.

Одержувач може перевірити кожен підпис, щоб підтвердити коректність усього ланцюга.

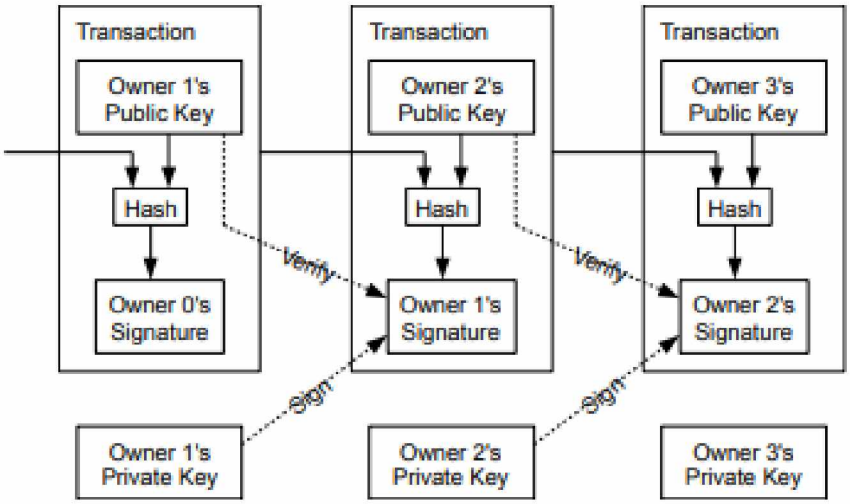

Рисунок 1.1 – Схема транзакцій

Проблема, зрозуміло, в тому, що одержувач не може визначити, скільки разів колишній власник витратив цю монету. Традиційне рішення полягає в перевірці центральною довіреною особою ("монетним двором" або емітентом) кожної транзакції. Після будь-якого платежу монета повертається до емітента, який випускає нову її версію; і тільки безпосередньо отриманим таким чином монетам можна довіряти. Недолік цього підходу в тому, що від компанії-емітента залежить доля всієї грошової системи, оскільки вона подібно до банку контролює кожну транзакцію, що проходить через неї.

Адресат має знати, що ніхто з попередніх власників не підписав транзакцію, яка передує за часом тій, що перебуває в ланцюжку відправленої йому монети. Для наших цілей лише перша транзакція з кількох є істинною, тому ми не повинні турбуватися про пізні спроби подвійної витрати. У централізованій моделі емітент знав про всі транзакції і вирішував, у якому порядку вони йдуть. Щоб позбавити схему від посередника, учасникам необхідно відкрито публікувати транзакції [1], а також вміти приходити до згоди щодо єдиного порядку їх проходження. Одержувачу потрібен доказ того, що для кожної транзакції з ланцюжка більшість користувачів згодні вважати її першою.

Почнемо опис рішення із сервера міток часу. Його робота полягає в хешуванні блоку даних, на який потрібно поставити мітку, і відкритій публікації цього хешу, як

у газеті або Usenet-постах [2-5]. Мітка часу показує, що в даний момент конкретні дані існували і тому потрапили в хеш блоку. Кожен хеш включає в себе попередню мітку: так вибудовується ланцюг, де чергова ланка зміцнює всі попередні.

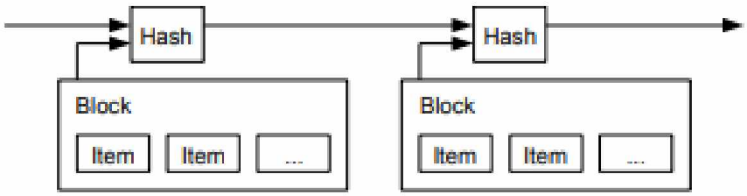

Рисунок 1.2 – Схема з чого складається хеш

Щоб реалізувати розподілений одноранговий сервер міток часу, використовується схема "доказу роботи", подібну до системи Hashcash Адама Бека [6]. Суть полягає в пошуку такого значення, чий хеш (наприклад, SHA-256) починався б із деякого числа нульових бітів. Потрібно виконати обсяг роботи, що експоненціально залежний від числа нулів, але для перевірки знайденого значення достатньо обчислити лише один хеш.

У такому сервері міток часу пошук значення з потрібним хешем відбувається шляхом перебору значення ітерованого поля-добавки (nonce) в блоці даних. Щойно блок, що задовольняє умові, знайдено, його вміст не можна змінити, не виконавши заново всієї роботи. І якщо він не є останнім у ланцюжку, ця робота охоплює і переобчислення всіх блоків, що йдуть за ним.

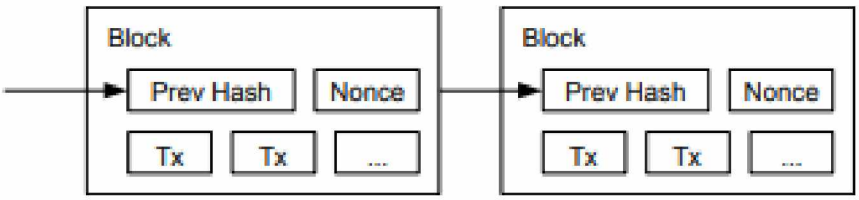

Рисунок 1.3 – Схема з чого складається блок

Доказ роботи через хешування також вирішує питання про визначення версії, підтримуваної більшістю. Якщо голосом вважається одна IP-адреса, то таку схему можна скомпрометувати, якщо контролювати великий діапазон адрес. Ця схема заснована на принципі "один процесор - один голос". Найдовший із хеш-ланцюжків висловлює думку більшості, яка вклала в нього найбільшу кількість ресурсів. Якщо більше половини обчислювальної потужності належить чесним вузлам, то ланцюжок чесних транзакцій зростатиме швидше і випередить будь-який конкуруючий ланцюг. Щоб внести зміни в будь-який з минулих блоків, атакуючому доведеться виконати заново роботу над цим блоком і всіма наступними, а потім наздогнати і перегнати чесних учасників за новими блоками. Нижче буде показано, що ймовірність такого успіху у зловмисника, що володіє меншими ресурсами, експоненціально зменшується залежно від числа блоків.

Для компенсації зростаючої обчислювальної потужності процесорів і коливання числа працюючих вузлів у мережі, складність хешування повинна змінюватися, щоб забезпечувати рівномірну швидкість генерації блоків. Якщо вони з'являються занадто часто - складність зростає, і навпаки.

Система працює за такими правилами:

1) Нові транзакції розсилаються всім вузлам.

2) Кожен вузол об'єднує транзакції, що надійшли, у блок.

3) Кожен вузол намагається підібрати хеш блоку, що задовольняє поточну складність.

4) Щойно такий хеш знайдено, цей блок відправляється в мережу.

5) Вузли приймають блок, тільки якщо всі транзакції в ньому коректні й не використовують уже витрачені кошти.

6) Свою згоду з новими даними вузли висловлюють, починаючи роботу над наступним блоком і використовуючи хеш попереднього як нові вихідні дані.

Учасники завжди вважають істинною найдовшу версію ланцюжка і працюють над її подовженням. Якщо два вузли одночасно опублікують різні версії чергового блоку, то хтось із решти пірів отримає раніше одну версію, а хтось - іншу. У такому випадку кожен почне працювати над своєю версією ланцюжка, зберігши іншу на

випадок, якщо вона виявиться продовжена раніше. Двоїстість зникне, щойно буде отримано новий блок, який продовжить будь-яку з гілок, і ті вузли, що працювали над конкуруючою версією, переключатись на неї.

Нові транзакції не обов'язково мають досягати всіх вузлів. Якщо про них знатиме досить багато вузлів, незабаром вони потраплять в один із блоків. Правила розсилки блоків теж не є суворими щодо втрачених повідомлень. Як тільки вузол, що пропустив один із блоків, отримає вже наступний за ним, він запросить інформацію, якої бракує, щоб заповнити очевидний пропуск.

За замовчуванням, перша транзакція в блоці є спеціальною, що створює нову монету, яка належить творцеві блоку. Така схема заохочує чесних учасників мережі, стимулюючи їх підтримувати роботу мережі, а також вирішує питання про початковий розподіл грошової маси за відсутності центрального емітента. Рівномірне збільшення кількості монет в обігу можна порівняти з видобутком золота, в який золотошукачі теж вкладають свої ресурси. У ролі останніх у нашому випадку виступають процесорний час і електрика.

Іншим способом стимулювання може бути комісія за транзакції. Якщо вхідна сума платежу більша за вихідну, то різниця є комісією за переказ і додається до базового значення нагороди за знайдений блок у першій транзакції. Як тільки сумарний обсяг грошової маси досягне заздалегідь встановленого максимуму, єдиним джерелом заохочення роботи над блоками залишаться комісії, при цьому позбавлені інфляції.

Така форма стимулювання може також сприяти зменшенню випадків шахрайства. Якщо жадібний зловмисник здатен виділити більше обчислювальних потужностей, ніж усі чесні учасники, він може обманювати продавців, анулюючи свої транзакції і повертаючи кошти, або ж спрямувати свої ресурси на генерацію нових блоків і монет. Більш вигідним для нього є варіант "гри за правилами", який забезпечує отримання більше половини всіх нових грошей, ніж варіант "саботажу системи" і підтримання свого капіталу на постійному рівні.

Як тільки остання транзакція в монеті-ланцюжку опиниться всередині досить старого блоку, всі попередні їй транзакції в ланцюжку можуть бути видалені з метою

очищення дискового простору. Щоб хеш блоку залишився незмінним, усі транзакції в блоці зберігаються у вигляді хеш-дерева Меркла [7][2][5] і лише його корінь включають у хеш блоку. Таке рішення використовується для оптимізації використання дискового простору.

Розмір старих блоків може бути зменшено за рахунок видалення непотрібних гілок цього дерева, зберігати проміжні хеші необов'язково.

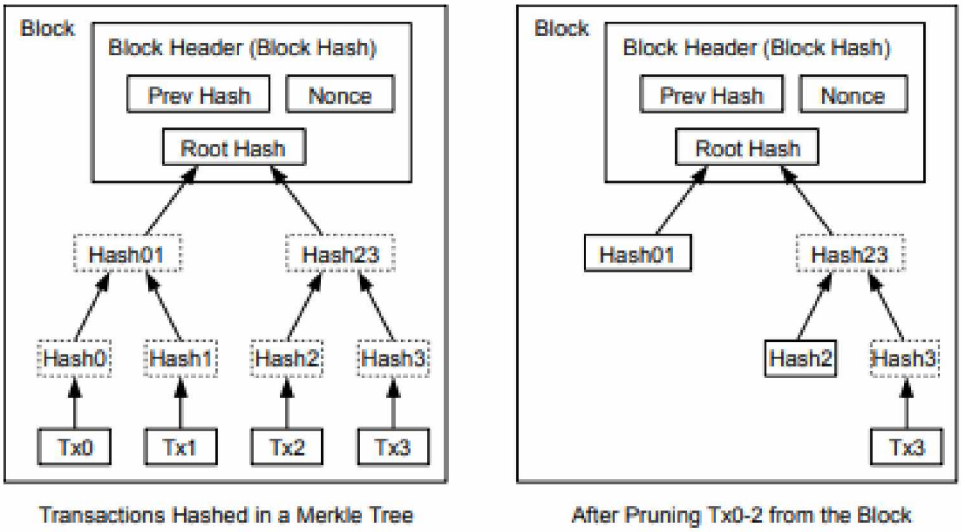

Рисунок 1.4 – Економія дискового простору

Заголовок порожнього блоку становитиме близько 80 байт. З розрахунку швидкості генерації блоку раз на десять хвилин отримуємо 80*6*24*365=4.2 Мб на рік. Для середньостатистичного на 2008 рік комп'ютера з 2 Гб оперативної пам'яті з урахуванням закону Мура, що пророкує зростання на 1.2 Гб на рік, зберігання даних не буде проблемою, навіть якщо усі заголовки блоків перебуватимуть у пам'яті.

Верифікація транзакцій можлива без запуску повнофункціонального вузла. Користувачеві необхідно лише зберігати заголовки блоків найдовшого ланцюжка, який він отримав від інших вузлів, і запитувати хеш-піддерево для необхідної транзакції. Він не може перевірити коректність транзакції самостійно, але отримавши посилання на блок, у якому вона перебуває, він може переконатися в тому, що цей блок і всі наступні прийняті та підтверджені мережею.

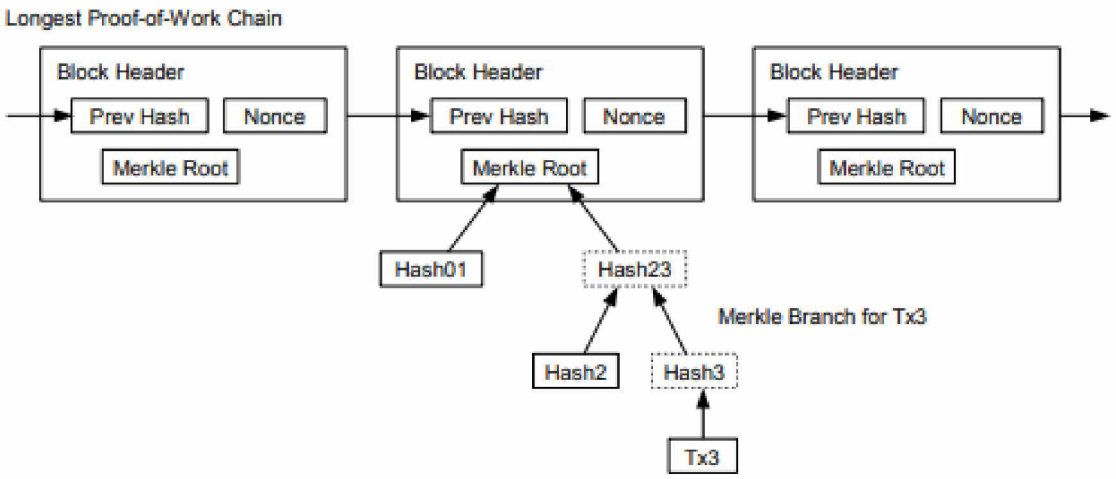

Рисунок 1.5 – Схема спрощенної системи перевірки

На такий метод перевірки можна покладатися, поки мережа хоча б наполовину перебуває під контролем чесних учасників, тобто поки зловмисник не заволодіє великими ресурсами. Звичайні вузли можуть перевіряти транзакції самостійно, але якщо нападник генерує найдовший ланцюг блоків, то своїми сфабрикованими транзакціями він може скомпрометувати спрощену схему.

Однією зі стратегій протидії цьому може бути розсилка сигналів тривоги від звичайних пірів, які отримують "помилковий" блок. Такий сигнал змушуватиме програму-клієнт завантажувати блок повністю, щоб самостійно підтверджувати некоректність даних. Компанії, часто приймаючі платежі, можливо, будуть підключатися до мережі у звичайному режимі для більшої незалежності, безпеки та швидкості перевірки.

Незважаючи на те, що можна оперувати окремими монетами, створювати спеціальну, транзакцію для кожного цента було б занадто незручно. Для підтримки поділюваних і об'єднуваних сум транзакції містять кілька входів і виходів.

Звичайна транзакція матиме такий вигляд: або один вхід від попереднього великого платежу, або кілька входів, що акумулюють невеликі суми, і не більше двох виходів: один є власне платежем, а інший, якщо необхідно, повертає "решту" назад відправнику.

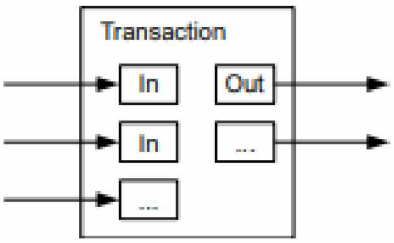

Рисунок 1.6 - Транзакції з використанням кількох входів і виходів

Необхідно зазначити, що збільшення зв'язків, коли транзакція залежить від кількох, а ті своєю чергою залежать від ще більшої кількості, не є проблемою, оскільки немає необхідності отримувати повну і незалежну копію історії транзакції.

Традиційна банківська модель підтримує необхідний рівень конфіденційності, надаючи доступ до інформації лише сторонам-учасницям і довіреній третій особі. Необхідність відкритої публікації транзакцій виключає такий підхід, однак конфіденційність як і раніше, можна зберегти, якщо публічні ключі будуть анонімними. Відкритою буде інформація про те, що хтось відправив комусь деяку суму, але без прив'язки до конкретних особистостей. Стільки ж даних розкривається і на фондових біржах, які публікують час і обсяг приватних угод, не вказуючи, між ким саме їх було здійснено.

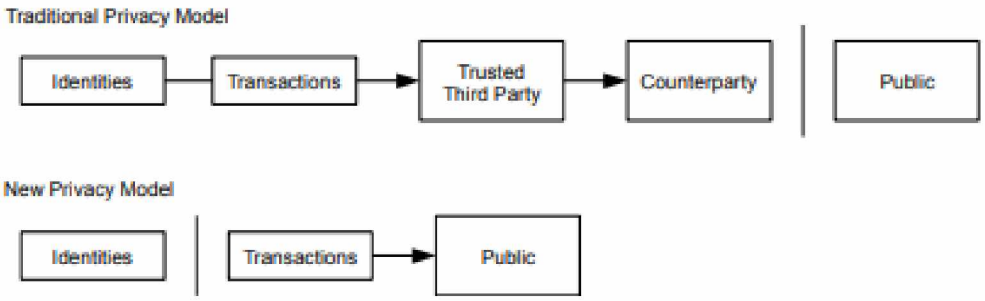

Рисунок 1.6 – Моделі конфіденційності

Додатковим захистом буде генерація нової пари "відкритий/закритий ключ" для кожної транзакції: це запобігатиме зв'язуванню різних платежів з їхнім

загальним відправником або адресатом. Деякого публічного зв'язування все ж не уникнути: транзакції з кількома входами доводять, що ці суми належать одній особі. Ризик полягає в тому, що розкриття особи власника ключа може призвести до розкриття і всіх належних йому транзакцій.

Розглянемо сценарій, у якому зловмисник намагається генерувати довший ланцюг блоків, ніж чесні учасники. Навіть якщо він досягне успіху, це не призведе до того, що можна буде створювати гроші з повітря, привласнювати собі чужі монети або вносити інші довільні зміни. Вузли ніколи не приймуть некоректну транзакцію або блок, що її містить. Атакуючий може лише намагатися змінити одну зі своїх транзакцій, щоб повернути собі гроші.

Перегони між чесними учасниками і нападником можна уявити як біноміальне випадкове блукання. Успішна подія, коли "хороший" ланцюг подовжується на один блок, призводить до збільшення відриву на одиницю, а неуспішна, коли черговий блок створює зловмисник, - до його скорочення. Імовірність атакуючого надолужити різницю в кілька блоків така сама, як і в задачі про "розорення гравця". Уявімо, що гравець має необмежений кредит, починає з деяким дефіцитом і в нього є нескінченно багато спроб, щоб відігратися.

Імовірність того, що він досягне успіху, як і ймовірність зловмисника наздогнати чесних учасників, обчислюється таким чином [8]:

p = імовірність появи блоку в чесному ланцюжку

q = імовірність того, що блок створить атакувальник

qz = імовірність того, що атакувальник надолужить різницю в z блоків

$$q_z = \begin{cases} 1 & \text{if } p \le q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Рисунок 1.7 – Імовірність наздогнати чесних учасників

У разі p > q ймовірність зменшується експоненціально зі зростанням числа блоків, на яке відстає зловмисник. Оскільки всі ставки проти нього, без вдалого ривка на початку його шанси на успіх стають мізерно малими.

Розглянемо тепер, як довго одержувачу платежу варто чекати, перш ніж він буде повністю впевнений, що колишній власник не зможе скасувати транзакцію. Ми припускаємо, що зловмисник-відправник дозволяє адресату деякий час вірити, що платіж було проведено, після чого повертає гроші собі. Одержувач дізнається про це, але шахрай сподівається, що буде вже занадто пізно.

Адресат створює нову пару ключів і повідомляє свій публічний ключ відправнику просто перед підписанням транзакції. Це не дозволить відправнику заздалегідь почати працювати над ланцюжком і провести транзакцію в той момент, коли він буде достатньо везучий, щоб зробити ривок уперед. Після відправлення платежу шахрай починає потай працювати над паралельною версією ланцюжка, що містить альтернативну транзакцію.

Одержувач чекає, поки транзакцію не буде додано в блок і поки той не буде продовжено ще z блоками. Йому невідомий прогрес зловмисника, але якщо середня швидкість генерації чесних блоків - відома величина, то число блоків нападника підпорядковується розподілу Пуассона з математичним очікуванням:

$$\lambda = z\frac{q}{p}$$

Рисунок – 1.8 - розподіл Пуассона з математичним очікуванням

З результатів досліджень, видно, що ймовірність падає експоненційно зі зростанням z.

У цій частині роботи було розказано про систему електронних транзакцій, яка не ґрунтується на довірі. Побудова схеми почалася з традиційного представлення монет на основі цифрових підписів, що забезпечує контроль володіння, але допускає подвійну витрату. Цю проблему ми вирішили за допомогою пірингової мережі та схеми "доказу роботи" для запису публічної історії транзакцій.

Спроба зловмисника, який не володіє більшою частиною ресурсів мережі, змінити старі записи, обчислювально стає практично нездійсненною. Сильною стороною мережі є простота її структури. Усі вузли працюють самостійно, іноді обмінюючись інформацією. Немає необхідності в ідентифікації, оскільки повідомлення не йдуть за якимось певним маршрутом, а на основі принципу "найменших витрат".

Вузли можуть залишати мережу і знову підключатися, приймаючи найдовший ланцюжок блоків як підтвердження пропущеної історії транзакцій. Вони висловлюють свою згоду прийняти коректний блок у ланцюжок, використовуючи свої обчислювальні потужності для подовження цього ланцюга, або незгоду (якщо блок містить невірні дані), не продовжуючи цей ланцюжок. Будь-які необхідні правила протоколу можуть бути реалізовані через цей механізм голосування.

1.2 Аналіз функціонування Ethereum

Ефір (ETH) - це власна криптовалюта Ethereum. Мета ефіру - створити ринок для обчислень. Такий ринок забезпечує учасникам економічний стимул для перевірки та виконання транзакційних запитів і надання обчислювальних ресурсів мережі.

Доказ частки (PoS) лежить в основі механізму консенсусу Ethereum. Ethereum увімкнув механізм proof-of-stake у 2022 році, оскільки він є більш безпечним, менш енергоємним та кращим для впровадження нових рішень з масштабування у порівнянні з попередньою архітектурою доказу роботи [9].

Доказ частки лежить в основі певних механізмів консенсусу, які використовуються в блокчейні для досягнення розподіленого консенсусу. Під час доказу частки майнери доводять, що їхній капітал знаходиться під загрозою, витрачаючи енергію. В Ethereum використовується proof-of-stake, коли валідатори явно вносять капітал у формі ETH в смарт-контракт на Ethereum. Ці ETH виступають в якості застави, яка може бути знищена, якщо валідатор поводиться

нечесно або ліниво. Валідатор відповідає за перевірку дійсності нових блоків, що поширюються мережею, а також іноді сам створює і поширює нові блоки.

Proof-of-stake має низку покращень у порівнянні з застарілою системою підтвердження виконання робіт, що вже застаріла:

краща енергоефективність - немає необхідності використовувати багато енергії на обчислення доказу роботи нижчі бар'єри для входу, зниження вимог до обладнання - немає необхідності в елітному обладнанні, щоб мати шанс створювати нові блоки

знижений ризик централізації - доказ частки повинен призвести до збільшення кількості вузлів, що забезпечують безпеку мережі через низьку потребу в енергії потрібно менше емісії ETH для стимулювання участі економічних санкцій за неправомірну поведінку роблять атаки в стилі 51% експоненціально дорожчими для зловмисника порівняно з доказом роботи спільнота може вдатися до соціального відновлення чесного ланцюжка, якщо атака 51% подолає криптоекономічний захист. Але також треба розуміти, що така модель навпаки робить мережу централізованою, тому що більшість монет належать малій кількості учасників ринку, котрі і будуть приймати більшість рішень.

Для участі в якості валідатора користувач повинен внести 32 ETH в депозитний контракт і запустити три окремі частини програмного забезпечення: клієнт виконання, клієнт консенсусу і валідатор. Після внесення ETH користувач приєднується до черги активації, яка обмежує швидкість приєднання нових валідаторів до мережі. Після активації валідатори отримують нові блоки від однорангових учасників мережі Ethereum. Транзакції, що містяться в блоці, повторно виконуються, а підпис блоку перевіряється, щоб переконатися, що блок дійсний. Потім валідатор надсилає голос (який називається атестацією) на користь цього блоку по всій мережі.

У той час як при proof-of-work час створення блоків визначається складністю майнінгу, при proof-of-stake темп є фіксованим. Час в proof-of-stake Ethereum ділиться на слоти (12 секунд) і епохи (32 слоти). У кожному слоті випадковим чином обирається один валідатор, який буде пропонувати блок. Цей валідатор відповідає за створення нового блоку і його розсилку іншим вузлам мережі. Також у

кожному слоті випадковим чином обирається комітет валідаторів, голоси яких використовуються для визначення дійсності запропонованого блоку.

Нижче наведено наскрізне пояснення того, як виконується транзакція в системі Ethereum proof-of-stake.

Користувач створює і підписує транзакцію своїм приватним ключем. Зазвичай цим займається гаманець або бібліотека, така як ether.js, web3js, web3py тощо, але під капотом користувач робить запит до вузла за допомогою Ethereum JSON-RPC API. Користувач визначає кількість газу, яку він готовий заплатити в якості чайових валідатору, щоб заохотити його включити транзакцію в блок. Чайові виплачуються валідатору, в той час як базова комісія спалюється.

Транзакція надсилається клієнту виконання Ethereum, який перевіряє її дійсність. Це означає, що відправник має достатньо ETH для виконання транзакції і підписав її правильним ключем.

Якщо транзакція дійсна, клієнт виконання додає її до свого локального пулу пам'яті (списку очікуваних транзакцій), а також транслює її іншим вузлам через мережу пліток рівня виконання. Коли інші вузли дізнаються про транзакцію, вони також додають її до свого локального пулу пам'яті. Просунуті користувачі можуть утриматися від трансляції транзакції і замість цього переслати її в спеціалізовані будівники блоків, такі як Flashbots Auction. Це дозволяє їм організувати транзакції в майбутніх блоках для отримання максимального прибутку (MEV).

Один з вузлів мережі є пропонентом блоку для поточного слоту, який попередньо був обраний псевдовипадковим чином за допомогою RANDAO. Цей вузол відповідає за створення і трансляцію наступного блоку, який буде додано до блокчейну Ethereum, а також за оновлення глобального стану. Вузол складається з трьох частин: клієнт виконання, клієнт консенсусу і клієнт валідатора. Клієнт виконання об'єднує транзакції з локального пулу пам'яті у "корисне навантаження" і виконує їх локально, генеруючи зміну стану. Ця інформація передається клієнту консенсусу, де корисне навантаження виконання запаковується як частина "маякового блоку", який також містить інформацію про винагороди, штрафи,

відсікання, атестації і т.д., що дозволяє мережі узгодити послідовність блоків на чолі ланцюжка.

Інші вузли отримують новий маячковий блок у мережі пліток рівня консенсусу. Вони передають його своєму клієнту виконання, де транзакції повторно виконуються локально, щоб переконатися, що запропонована зміна стану є дійсною. Потім клієнт-валідатор підтверджує, що блок дійсний і є логічним наступним блоком в ланцюжку (це означає, що він будується на ланцюжку з найбільшою вагою підтверджень, як визначено в правилах вибору форків). Блок додається до локальної бази даних у кожному вузлі, який його засвідчує.

Транзакцію можна вважати "фіналізованою", тобто такою, що не може бути скасована, якщо вона стала частиною ланцюжка з "супермажоритарним зв'язком" між двома контрольними точками. Контрольні точки виникають на початку кожної епохи, і для того, щоб мати зв'язок супермажоритарності, вони обидві повинні бути засвідчені 66% від загальної кількості стейків ETH в мережі.

Більш детальну інформацію про фінал можна знайти нижче.

Транзакція має "фінальність" в розподілених мережах, коли її частина блоку не може змінитися без втрати значної кількості ETH. В Ethereum з доказом частки це відбувається за допомогою блоків "контрольних точок". Перший блок в кожній епосі є контрольною точкою. Валідатори голосують за пари чекпоінтів, які вони вважають дійсними. Якщо пара чекпоінтів привертає голоси, що представляють принаймні дві третини від загальної кількості стейків ETH, чекпоінти оновлюються. Пізніша з них (цільова) стає "виправданою". Більш рання з них вже є виправданою, оскільки вона була "цільовою" в попередню епоху. Тепер вона стає "фіналізованою". Щоб повернути фіналізований блок, зловмисник повинен взяти на себе зобов'язання втратити щонайменше третину від загальної кількості стейккоінів ETH. Оскільки для фіналізації необхідна більшість у дві третини голосів, зловмисник може перешкодити мережі досягти фіналізації, проголосувавши однією третиною від загального стеку. Існує механізм захисту від цього: витік бездіяльності Він активується щоразу, коли ланцюжок не може завершитися протягом більш ніж чотирьох епох. Витік бездіяльності вимиває стейк ETH з валідаторів, які голосують

проти більшості, дозволяючи більшості відновити більшість у дві третини і завершити ланцюжок.

Запуск валідатора - це зобов'язання. Очікується, що валідатор повинен підтримувати достатнє апаратне забезпечення і зв'язок для участі в перевірці блоків і пропозиції. Натомість валідатор отримує оплату в ETH (його стейкінговий баланс збільшується). З іншого боку, участь в якості валідатора також відкриває нові можливості для користувачів атакувати мережу з метою особистої вигоди або саботажу. Щоб запобігти цьому, валідатори втрачають винагороду ETH, якщо вони не беруть участь у роботі, коли їх просять, а їхній наявний стек може бути знищений, якщо вони поводяться нечесно. Існує два основних типи поведінки, які можна вважати нечесними: пропонування декількох блоків в одному слоті (еквівокація) і надання суперечливих атестацій. Кількість нарізаних ETH залежить від того, скільки валідаторів також нарізають приблизно в той самий час. Це так званий "кореляційний штраф", і він може бути незначним (~1% стека для одного валідатора, який слейсить самостійно) або може призвести до знищення 100% стека валідатора (масова слейсингова подія). Він накладається посередині періоду примусового виходу, який починається з негайного штрафу (до 0,5 ETH) на 1-й день, кореляційного штрафу на 18-й день і, нарешті, викидання з мережі на 36-й день. Вони отримують незначні атестаційні штрафи щодня, оскільки присутні в мережі, але не подають голоси. Все це означає, що скоординована атака буде дуже дорого коштувати зловмиснику.

Коли мережа працює оптимально і чесно, на чолі ланцюжка завжди знаходиться тільки один новий блок, і всі валідатори це підтверджують. Однак валідатори можуть мати різні погляди на голову ланцюжка через затримку в роботі мережі або через те, що пропонент блоку висловився неоднозначно. Тому клієнтам консенсусу потрібен алгоритм, щоб вирішити, якому з них віддати перевагу. Алгоритм, який використовується в доказі частки Ethereum, називається LMD-GHOST, і він працює, визначаючи форк, який має найбільшу вагу атестацій в своїй історії.

Загроза атаки 51%(відкриється в новій вкладці) все ще існує для proof-of-stake, як і для proof-of-work, але вона ще більш ризикована для зловмисників. Зловмиснику знадобиться 51% стека ETH. Потім він може використовувати власні атестації, щоб переконатися, що бажаний форк має найбільше накопичених атестацій. "Вага" накопичених атестацій - це те, що консенсусні клієнти використовують для визначення правильного ланцюжка, тому зловмисник міг би зробити свій форк канонічним. Однак перевага доказу частки над доказом роботи полягає в тому, що спільнота має гнучкість у проведенні контр-атаки. Наприклад, чесні валідатори можуть вирішити продовжувати будувати ланцюжок меншості та ігнорувати форк зловмисника, заохочуючи додатки, біржі та пули робити те ж саме. Вони також можуть вирішити примусово видалити зловмисника з мережі і знищити його стек ETH. Це потужний економічний захист від атаки 51%.

Атаки 51% - це лише один з різновидів зловмисних дій. Погані юзери можуть спробувати атакувати з далекої відстані (хоча гаджет фінальності нейтралізує цей вектор атаки), "реорги" з близької відстані (хоча підвищення пропозиції і терміни атестації пом'якшують це), атаки з відскакуванням і балансуванням (також пом'якшуються підвищенням пропозиції, і ці атаки в будь-якому випадку були продемонстровані тільки в ідеалізованих умовах мережі) або лавинні атаки (нейтралізуються правилом алгоритмів вибору форків, які враховують тільки останнє повідомлення).

В цілому, доказ частки, як він реалізований в Ethereum, виявився більш економічно безпечним, ніж доказ роботи.

Стейкінг полегшує участь окремих осіб у забезпеченні безпеки мережі, сприяючи децентралізації, але це не так, творець Ефіріуму може наклепати будь яку кількість коїнів, а це слідує за собою відхід від децентралізації і скупчення влади у руках найбільших тримачів Ефіріума. Вузол валідатора може бути запущений на звичайному ноутбуці. Стекінг-пули дозволяють користувачам робити стейки, не маючи 32 ETH. Доказ стекінгу молодший і менш перевірений в боях в порівнянні з доказом роботи

Стейкінг більш децентралізований. Економія від масштабу не застосовується так само, як при майнінгу PoW. Proof-of-stake складніше реалізувати, ніж proof-of-work

Підтвердження частки пропонує більшу криптоекономічну безпеку, ніж підтвердження роботи користувачам потрібно запустити три частини програмного забезпечення, щоб взяти участь у підтвердженні частки в Ethereum. Для стимулювання учасників мережі потрібно менше випускати нових ETH.

1.3 BNB Smart Chain: принципи роботи та екосистема

BNB Smart Chain (Binance Smart Chain) є блокчейн-платформою, розробленою компанією Binance, яка є однією з найбільших криптовалютних бірж у світі. BNB Smart Chain створена для підтримки децентралізованих додатків (DApps) та смарт-контрактів, а також для забезпечення швидкості та масштабованості [10].

Основні характеристики BNB Smart Chain:

BNB Smart Chain побудована на технології Ethereum Virtual Machine (EVM), що робить її сумісною з Ethereum. Це означає, що розробники можуть легко переносити свої додатки з Ethereum на BNB Smart Chain або створювати нові додатки без необхідності вивчати нові технології.

BNB Smart Chain має паралельну ланку, що дозволяє прискорити обробку транзакцій і підвищити продуктивність мережі. Це досягається шляхом розділення мережі на дві частини: основну ланку (mainnet) і паралельну ланку (sidechain). Головна ланка відповідає за консенсус та безпеку, тоді як паралельна ланка забезпечує швидкість обробки транзакцій.

BNB Smart Chain пропонує низькі витрати на транзакції, що робить її привабливою для користувачів та розробників. Вартість газу на BNB Smart Chain значно нижча, ніж на Ethereum, що дозволяє здійснювати ефективні та доступні операції.

Власникам токену Binance Coin (BNB) доступний процес стейкінгу, який дозволяє заробляти пасивний дохід у вигляді винагороди за участь у забезпеченні безпеки та консенсусу мережі.

BNB Smart Chain має сильну підтримку з боку екосистеми Binance, що включає криптовалютну біржу Binance, гаманці, інструменти для розробників та інші сервіси. Це створює сприятливі умови для розвитку і використання BNB Smart Chain.

На BNB Smart Chain можна розробляти та виконувати різноманітні додатки, використовуючи смарт-контракти. Це відкриває можливості для фінансових послуг, децентралізованих бірж, ігор, систем голосування та багатьох інших сфер.

BNB Smart Chain є важливим гравцем у світі блокчейн-технологій, надаючи розробникам та користувачам потужну та ефективну платформу для створення та використання децентралізованих додатків. Її широка підтримка та інтеграція в екосистему Binance роблять її привабливим варіантом для інновацій та розвитку криптовалютного простору.

1.4 Приклади використання основних блокчейнів:

Кожен з блокчейнів - Bitcoin, Ethereum та BNB Smart Chain - використовується для різних цілей. Ось кілька прикладів використання кожного з них:

- Bitcoin:

Засіб обміну: Bitcoin став першою криптовалютою і має значну популярність як засіб обміну. Його використовують для переказування коштів між особами без посередництва банків чи фінансових установ.

Зберігання вартості: Багато людей використовують Bitcoin як засіб збереження вартості, аналогічний до золота чи інших традиційних активів. Простими словами Bitcoin є першою криптовалютою в чому і полягає його фундаментальна цінність.

- Ethereum:

Смарт-контракти: Ethereum є платформою, що надає можливість програмувати та виконувати смарт-контракти. Він використовується для створення децентралізованих додатків (DApps), автоматизації угод та створення власних токенів.

Децентралізовані фінанси (DeFi): Ethereum є основою для розробки та функціонування різноманітних децентралізованих фінансових інструментів, таких як децентралізовані біржі (DEX), грошові ринки, стейблкоїни та інші фінансові протоколи.

- BNB Smart Chain:

Децентралізовані фінанси (DeFi): BNB Smart Chain розвивається як платформа для децентралізованих фінансових послуг. Вона підтримує розробку та функціонування DeFi додатків, включаючи DEX, грошові ринки, громадські та приватні ланцюжки та інші фінансові інструменти.

Екосистема Binance: BNB Smart Chain є частиною екосистеми Binance, одного з найбільших криптовалютних гігантів. Вона надає можливість швидкого та вигідного переказу BNB токенів та інших активів, що базуються на Binance Chain.

1.5 Arbitrum рішення другого рівня для глобалізації Ethereum.

Arbitrum є масштабованою розширенням блокчейну Ethereum, яке пропонує високопродуктивні та швидкі транзакції, зменшення вартості та підвищення масштабованості додатків, побудованих на базі Ethereum [11].

Основна ідея Arbitrum полягає в тому, що він дозволяє використовувати "ланцюжки ланцюжків" (chain-to-chain) або "ланцюжки проксі" (rollup chains) для обробки транзакцій поза основним ланцюжком Ethereum. Розширення використовує механізм, що називається "Optimistic Rollup", для забезпечення високої продуктивності та надійності.

Основний принцип роботи Arbitrum наступний:

Передача на ланцюжок Arbitrum: Коли користувач хоче виконати транзакцію на ланцюжку Arbitrum, він відправляє її на "міст" (bridge) між Ethereum та Arbitrum.

Міст діє як проміжний шар, який забезпечує безпечну передачу токенів та даних між основним ланцюжком Ethereum і ланцюжком Arbitrum.

Обробка транзакцій на ланцюжку Arbitrum: Після передачі на ланцюжок Arbitrum транзакція обробляється на "ланцюжку проксі" або "ланцюжку ланцюжків". Цей ланцюжок виконує логіку транзакцій і вирішує станові проблеми, пов'язані з масштабуваністю. Транзакції відбуваються швидко та ефективно, оскільки основна обробка відбувається поза основним ланцюжком Ethereum.

Зворотна передача на основний ланцюжок: Після виконання транзакцій на ланцюжку Arbitrum, дані про стан та результати транзакцій можуть бути відправлені назад на основний ланцюжок Ethereum. Це забезпечує зворотну сумісність і забезпечує, що інформація про стан актуалізується на основному ланцюжку.

Arbitrum використовує технологію роллапів (rollups), яка дозволяє збирати багато транзакцій разом в одній транзакції, що дозволяє значно зменшити витрати на газ та підвищити продуктивність мережі. Це дозволяє додаткам, побудованим на базі Ethereum, працювати швидше та ефективніше.

Оголошення та впровадження Arbitrum відбувається під наглядом Offchain Labs, компанії, яка спеціалізується на розробці масштабованих рішень для блокчейнів. Arbitrum стає однією з важливих технологій, спрямованих на вирішення проблем масштабованості Ethereum та поліпшення його функціональності для майбутнього розвитку децентралізованих додатків та екосистеми блокчейну.

1.6 Avalanche – альтернатива Ethereum

У кваліфікаційній роботі буде розглянуто технічний опис блокчейну Avalanche (AVAX). Блокчейн Avalanche є високошвидкісною, масштабованою та безпечною платформою, яка пропонує інноваційні рішення для децентралізованих додатків та фінансових послуг. В даному розділі буде розкрито принципи роботи блокчейну Avalanche, його консенсусний протокол та архітектуру мережі [12].

1. Принципи роботи блокчейну Avalanche

Блокчейн Avalanche працює на основі новаторського консенсусного протоколу, відомого як Avalanche. Його основна ідея полягає в тому, що він використовує принципи "м'якого голосування" (soft voting) та "вузлів-сенсорів" (sensor nodes) для досягнення консенсусу в мережі.

М'яке голосування - це процес, за якого вузли вибирають між різними альтернативними шляхами висловлення своїх уподобань. Вузли виконують голосування, надаючи перевагу певним варіантам, а результати голосування використовуються для визначення консенсусу в мережі. Цей механізм дозволяє швидко та ефективно досягнути згоди між вузлами.

Вузли-сенсори використовуються для перевірки правильності інформації, що надходить в мережу. Вони аналізують та перевіряють транзакції, блоки та інші дані, що передаються в мережі, та надають інформацію про їхню правильність та достовірність. Це сприяє безпеці та надійності мережі, оскільки неправильні або шкідливі дані можуть бути виявлені та відкинуті.

2. Консенсусний протокол блокчейну Avalanche

Консенсусний протокол Avalanche є основним складовим блоком блокчейну Avalanche. Він забезпечує досягнення консенсусу щодо правильного стану блокчейну та послідовного виконання транзакцій.

Протокол Avalanche використовує принципи "критичності" (criticality) та "об'єднання" (ties) для визначення переваги певних транзакцій або блоків над іншими. Він базується на ідей підтримки "консенсусу за варіантами" (opt-in consensus), де вузли вибирають, які блоки або транзакції вони вважають правильними.

Протокол Avalanche використовує ітеративний процес для досягнення консенсусу. Кожен вузол запитує інших вузлів про їхню думку щодо правильності певного блоку або транзакції. Вузли відповідають, висловлюючи свої уподобання за допомогою голосів.

Протокол динамічно змінює вагу голосу кожного вузла на основі отриманих відповідей. Чим більше вузлів підтримує певний варіант, тим більше ваги отримує цей варіант. Після кількох ітерацій процесу голосування визначається консенсус щодо правильності блоку або транзакції.

Важливо зазначити, що блокчейн Avalanche може працювати в режимі "прямого консенсусу" (direct consensus), де вузли вибирають один певний варіант, або в режимі "статистичного консенсусу" (statistical consensus), де вибирається найбільш ймовірний варіант згідно з розподілом голосів.

3. Архітектура мережі блокчейну Avalanche

Архітектура мережі блокчейну Avalanche складається з трьох основних компонентів: вузли мережі, консенсусний протокол та механізм спілкування між вузлами.

Вузли мережі - це комп'ютери або сервери, що підтримують блокчейн Avalanche. Вони зберігають повну копію блокчейну та виконують операції з обробки транзакцій та майнінгу нових блоків. Вузли спілкуються між собою, передаючи інформацію про нові блоки та транзакції.

Консенсусний протокол Avalanche використовується для досягнення консенсусу в мережі. Він визначає правила голосування, обробки голосів та визначення правильності блоків та транзакцій. Консенсусний протокол забезпечує відповідність між вузлами та забезпечує безпеку мережі.

Механізм спілкування між вузлами дозволяє передавати повідомлення та інформацію між вузлами мережі. Він може використовувати різні протоколи та мережеві технології для забезпечення ефективного обміну даними. Механізм спілкування дозволяє вузлам мережі взаємодіяти, обмінюватися блоками та транзакціями та забезпечувати синхронізацію та безпеку мережі.

Загальна архітектура мережі блокчейну Avalanche забезпечує високу продуктивність, масштабованість та безпеку. Це робить його привабливим вибором для децентралізованих додатків, фінансових послуг та інших випадків використання, які вимагають швидкого та надійного блокчейн-рішення.

1.7 LayerZero - оптимізація та прискорення мережі Ethereum

LayerZero перша надійна платформа сумісності omnichain, яка не передбачає жодних проміжних транзакцій. Завдяки використанню двох незалежних, ненадійних

поза ланцюжкових об'єктів, Oracle і Relayer, LayerZero здатний забезпечити дійсну доставку, не вимагаючи дорогої крос-ланцюжкової реплікації кінцевих машин або проміжних токенів. Цей протокол розроблено таким чином, що не виключає використання довільних служб ретранслятора, що гарантує відсутність змови між ретранслятором і Oracle. Протокол LayerZero дозволяє здійснювати власні транзакції між підтримуваними ланцюгами, тоді як новий дизайн кінцевої точки LayerZero можна легко розширити для підтримки будь-якого ланцюжка. На додаток до цього, дизайн Endpoint досить легкий, щоб працювати на дорогих ланцюжках рівня 1, таких як Ethereum, без непомірних витрат. Представлено практичне дослідження того, як реалізувати підтримку ланцюжків на основі EVM у LayerZero, використовуючи еталонну реалізацію Relayer у поєднанні з децентралізованою мережею оракула Chainlink, щоб забезпечити між ланцюгові транзакції через LayerZero. LayerZero — це основа, яка з'єднає різні екосистеми блокчейнів і дозволить безперебійно переміщувати ліквідність, дані та ідеї між мережами та спільнотами [13].

Висновки за розділом 1

Блокчейн Bitcoin є першим і найвідомішим блокчейном, який започаткував революцію у сфері криптовалют. Його основними характеристиками є децентралізація, безпека і невідворотність транзакцій.

Блокчейн Ethereum є розширеним блокчейном, який підтримує виконання смарт-контрактів. Він надає більш широкі можливості для створення децентралізованих додатків і токенів на базі блокчейну.

Binance Smart Chain є блокчейн платформою, яка була розроблена на базі Ethereum Virtual Machine (EVM) - віртуальної машини Ethereum. Це дозволяє Binance Smart Chain забезпечити сумісність з екосистемою Ethereum, зокрема здійснювати виконання смарт-контрактів та розробку децентралізованих додатків (DApps).

Arbitrum є масштабованим рішенням для масового використання Ethereum. Він пропонує високу швидкість і низькі комісії, використовуючи технологію Layer 2, що дозволяє розширити можливості мережі Ethereum.

Avalanche є блокчейн платформою, яка надає швидкість, масштабованість і безпеку для розробки децентралізованих додатків. Вона підтримує виконання смарт-контрактів і високу продуктивність.

Layerzero є технологічною платформою, яка пропонує швидкість і масштабованість для розробки децентралізованих додатків. Вона базується на інноваційних протоколах і забезпечує високу продуктивність мережі.

У результаті вивчення цих блокчейнів стало очевидним, що кожна з цих платформ має свої унікальні особливості, які можуть бути корисними в різних сферах застосування. Розуміння цих технологій дозволяє розширити можливості розробки додатків на блокчейні та ефективно використовувати їх у практичних сценаріях.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ КІБЕРБЕЗПЕКИ В КРИПТОВАЛЮТІ

2.1 Дослідження різновидів гаманців

Власники токенів можуть зберігати криптовалюту в різних типах гаманців. Але зазвичай вони належать до двох основних категорій: кастодіальних і некастодіальних. Кастодіальний гаманець, як-от Binance Custody, зберігає ваші активи та надає вам приватний ключ від вашого гаманця. Крім того, ваш звичайний акаунт Binance може використовуватися як кастодиальний гаманець. Але ви маєте повний контроль над своїми активами, якщо використовуєте некастодіальний гаманець. Некастодільні гаманці включають Binance Chain Wallet і MetaMask і тд. Як кастодіальні, так і некастодіальні гаманці мають переваги та недоліки. Давайте розглянемо їхні відмінності, щоб ви знали, коли використовувати один [14].

Необхідно мати цифровий гаманець. Якщо ви хочете здійснювати транзакції, торгувати на криптобіржі або використовувати блокчейн-додатки, вам це знадобиться. Таким чином, важливо знати, як працюють криптовалютні гаманці. Також важливо знати, що відрізняє кастодіальні та некастодіальні постачальники гаманців.

Криптогаманці, також відомі як «гаманці», є програмами або апаратним засобом, які дозволяють зберігати, керувати та використовувати криптовалюту. Користувачі можуть здійснювати транзакції та зберігати цифрові активи, такі як біткоїни, ефіри тощо, за допомогою цих інструментів.

Створення приватного ключа: під час створення гаманця створюється приватний ключ, який необхідний для доступу до криптовалюти. Приватний ключ — це унікальний, випадковий номер, який використовується для підпису кожної транзакції.

Виведення публічного ключа: приватний ключ може бути використаний для створення публічного ключа. Платежі та перевірка підписів можна проводити за допомогою публічного ключа.

Створення адреси гаманця: щоб отримати криптовалюту, вам потрібно створити адресу гаманця, яку можна створити за допомогою публічного ключа. У більшості випадків адреса представляється рядком символів, таких як випадковий номер або хеш публічного ключа.

Збереження приватного ключа: уникати несанкціонованого доступу до приватного ключа дуже важливо. Криптогаманці можуть використовувати апаратні пристрої або використовувати пароль для шифрування приватного ключа.

Для підписання транзакцій користувач повинен використовувати свій приватний ключ. Підпис забезпечує підтвердження цілісності та автентичності транзакції.

Мережева взаємодія: криптогаманці підключаються до відповідних блокчейн-мереж, щоб виконувати транзакції та отримувати інформацію про стан рахунків. Вони використовують різні протоколи для взаємодії з вузлами мережі, наприклад протокол ядра Bitcoin, протокол віртуальної машини Ethereum (EVM) тощо.

Баланс і історія транзакцій: Криптогаманці показують користувачеві інформацію про попередні транзакції, а також баланс його криптовалютних активів. Вони можуть робити багато речей, наприклад імпортувати гаманці з інших країн, створювати нові транзакції та переглядати історію транзакцій.

Третя сторона зберігає приватні ключі в кастодіальному гаманці криптовалюти. Це означає, що третя сторона буде мати доступ до та контролювати ваші секретні ключі від вашого імені. Іншими словами, у вас не буде ні повного контролю над своїми грошима, ні можливості підписувати транзакції. Кастодіальний гаманець, однак, має свої переваги.

На початку існування Bitcoin всі користувачі повинні були створювати та контролювати свої приватні ключі та гаманці. Хоча «бути власним банком» має багато переваг, для менш досвідчених користувачів це може бути незручно та навіть ризиковано. Якщо ваші приватні ключі будуть пошкоджені або втрачені, ви назавжди

втратите доступ до своїх криптоактивів. Згідно з даними аналізу блокчейну, існує ймовірність того, що понад 3-7 мільйонів біткоїнів можуть бути втрачені назавжди.

Крім того, були випадки, коли приватні ключі належали лише початковому власнику криптовалюти, тому спадкоємці не могли отримати доступ до активів. Подаючи доступ до своїх активів зберігачу, ви можете запобігти таким ситуаціям.

Звернувшись до служби підтримки, ви все одно зможете отримати доступ до свого акаунту та активів, навіть якщо ви забули свій пароль від криптовалютної біржі. Ви несете відповідальність за безпеку своєї криптовалюти, якщо ви використовуєте некастодіальний гаманець.

Таким чином, часто краще використовувати послугу кастодіального гаманця. Але це також означає, що ви довіряєте третій стороні свої приватні ключі. Ось чому важливо вибрати надійного постачальника чи біржу.

Насамперед потрібно вивчити основні дані про постачальника послуг зберігання, включаючи його правила, послуги, методи зберігання приватних ключів і страхування. Наприклад, Binance Custody, який перевіряється та регулюється, пропонує стандартну страховку для корпоративних акаунтів Binance. Крім того, вона пропонує індивідуальні можливості страхування, такі як страхування від злочинів. У Binance Custody використовується гаманець з мультипідписом, також відомий як multisig, щоб усунути централізовані ризики, які вимагають, щоб кілька сторін схвалили транзакції криптовалюти, перш ніж вони могли відбутися.

Некастодіальний гаманець – це гаманець, приватні ключі якого мають лише власник. Користувачі, яким важливо мати повний контроль над своїми грошима, знайдуть цей варіант найкращим. Ви можете торгувати криптовалютою прямо зі своїх гаманців, оскільки немає посередників. Це хороший варіант для досвідчених інвесторів і трейдерів, які знають, як захистити та контролювати свої особисті ключі та seed фрази.

Для взаємодії з децентралізованою біржею (DEX) або децентралізованим додатком (DApp) вам знадобиться некастодіальний гаманець. Uniswap, SushiSwap, PancakeSwap і QuickSwap є популярними децентралізованими біржами, які вимагають некастодіальний гаманець.

Хорошими прикладами постачальників некастодіальних гаманців є Trust Wallet і MetaMask. Пам'ятайте, що з цими гаманцями ви повністю відповідаєте за збереження своїх приватних ключів і seed фрази.

Плюси та мінуси кастодіальних гаманців: Як ми вже говорили, головним недоліком кастодіальних гаманців є те, що вам потрібно довіряти третій стороні свої гроші та приватні ключі. Цим постачальникам послуг у більшості випадків також знадобиться верифікація особи (KYC). Перевагою, однак, є спокій і комфорт. Вам не доведеться турбуватися про втрату приватного ключа, і ви будете мати можливість звертатися до служби підтримки, якщо виникнуть проблеми. Щоб використовувати кастодіальні послуги, переконайтеся, що ви вибрали надійного постачальника, який надає високу безпеку та страхове покриття. Ви повинні шукати кастодіальні сервіси, які мають ліцензію та відповідають стандартам.

Некастодіальні гаманці дозволяють вам мати повний контроль над своїми грошима та ключами, не використовуючи сторонніх посередників. Іншими словами, ви можете бути власним банком, а ваші активи — ваші. Крім того, оскільки вам не потрібно чекати схвалення на зняття, некастодіальні транзакції зазвичай виконуються швидше. Нарешті, ви не сплачуєте додаткових комісій за зберігання, які можуть бути дорогими залежно від постачальника послуг, якщо ви не маєте зберігача.

Одним із недоліків використання некастодіальних гаманців є те, що вони вони більш складні для користувача. Ця проблема має бути вирішена в майбутньому, коли постачальники некастодіальних послуг розвинуться.

Звичайно, ви також відповідаєте за свої ключі та повинні вживати запобіжних заходів, коли користуєтеся ними. Це означає, що ви повинні довіряти собі, а не комусь іншому.

Гарячі та холодні гаманці — це дві простіші категорії гаманців.

Гарячі гаманці: Інтернет-гаманці, такі як MyEtherWallet, Blockchain.com і Coinbase. Вони легко доступні за допомогою веб-браузера для швидкого доступу до криптовалют.

Мобільні гаманці: наприклад, Exodus, Trust Wallet. Це додатки для смартфонів, які дозволяють зберігати криптовалюту на мобільних пристроях.

Холодні гаманці:

Паперові гаманці: Це фізичні документи, на яких вказані приватні ключі та публічні адреси криптовалют. Наприклад, генерація гаманця за допомогою сервісу Bitaddress або застосунку, які генерують приватні ключі та публічні адреси для друку.

Жорсткі гаманці (hardware wallets): Наприклад, Ledger Nano S, Trezor, KeepKey. Це фізичні пристрої, які зберігають приватні ключі офлайн і дозволяють підписувати транзакції безпосередньо на пристрої, забезпечуючи вищий рівень безпеки.

2.2 Дослідження найкращих рішенн гаманців

Але в будь-якому випадку важливо робити власне дослідження та визначити, чому певні рішення кращі. З досвіду власного використання можу сказати, що ці рішення є хорошими. Однак без дотримання заходів кібербезпеки майже не важливо, яким чином ви користуєтеся гаманцем і де. У кінці цього розділу буде описано, як захистити ключі та гроші. Крім того, для звичайних користувачів є чудові інструменти, такі як Trezor, який забезпечує надзвичайну безпеку під час зберігання криптовалют. Він є надійним пристроєм для зберігання цифрових активів, оскільки він захищає приватні ключі від зовнішніх загроз. Trezor підтримує широкий спектр криптовалют і має простий інтерфейс, який легко використовувати. Крім того, він має функцію резервного копіювання, яка дозволяє легко відновити доступ до гаманця у випадку, якщо пристрій втратить або пошкоджено. Trezor отримав більшу довіру користувачів і експертів з безпеки завдяки своєму відкритому програмному забезпеченню.

MetaMask — це популярне розширення гаманця, яке дозволяє легко керувати криптовалютою безпосередньо у веб-браузері. Він дозволяє легко отримати доступ до різноманітних блокчейн-платформ і додатків децентралізованих фінансів. MetaMask має простий інтерфейс, що робить його простим у використанні навіть для новачків. Крім того, він підтримує кілька мереж блокчейн і підтримує функцію взаємодії з смарт-контрактами.

Trust Wallet — це мобільний гаманець, який працює на платформах Android і iOS. Він не тільки безпечно зберігає криптовалюту, але й дозволяє користувачам легко керувати своїми активами. У Trust Wallet доступні різні криптовалюти та блокчейн-мережі. Крім того, він має функцію децентралізованого обміну, яка дозволяє людям обмінювати гроші безпосередньо у своєму гаманці. Популярність Trust Wallet полягає в тому, що він надзвичайно безпечний, оскільки приватні ключі користувача шифруються на пристрої.

2.3 Основні тенденції криптовалютного шахрайства 2023

За даними Федеральної регуляторної служби, десять основних тенденцій криптовалютного шахрайства, на які слід звернути увагу у 2023 році, такі:

1. Інвестиційні афери: Інвестиційні шахрайства супроводжуються обіцянками «швидко розбагатіти» і «без ризику», які часто ініціюється через додатки для онлайн-знайомств або соціальні мережі. У цих шахрайських схемах криптовалюта може використовуватися як оплата, так і інвестиція. Інвестована криптовалюта прямим чином потрапляє в гаманець шахрая.

2. Романтичні шахрайства: вони полюють на стосунки і можуть бути інвестиційними або платіжними. Зловмисник намагається завоювати довіру користувача, надаючи інвестиційні поради, щоб запустити свою схему. Після встановлення контакту жертва проситься відправити криптовалюту шахраю, і вона може зробити це.

3. Шахрайство під виглядом представника бізнесу, уряду або роботи: у схемі зловмисник представляється як надійний онлайн-джерело, як-от Amazon, FedEx або банк користувача, і переконує користувачів надіслати йому гроші, купивши криптовалюту. Часто криптовалюта, яку продають шахраї, є шахрайською.

4. Шахрайство з витягуванням килима: інвестиційні шахраї пропонують нову криптовалюту або невзаємозамінний токен (NFT), щоб отримати гроші. Ця схема відома як шахрайство з витягуванням килима. Коли ініціатори проекту отримують гроші, вони зникають, не даючи інвесторам можливості повернути гроші.

5. Фішингові афери: фішинг-шахраї використовують електронні листи зі шкідливими посиланнями, щоб зібрати персональні дані, такі як ключова інформація про криптогаманці користувачів. Шахрай може отримати необмежений доступ до криптовалюти жертви, якщо він отримає достатньо інформації. Цей тип шахрайства також може бути здійснений за допомогою методу, відомого як «смішинг».

6. Шахрайство в соціальних мережах: Федеральна регуляторна комісія заявила, що половина тих, хто повідомив про втрати криптовалюти з 2021 року, стверджували, що шахрайство почалося з оголошення, посту або повідомлення в соціальних мережах. Instagram, Facebook, WhatsApp і Telegram були найпопулярнішими платформами.

7. Фінансові піраміди: Способи оплати в криптовалютних пірамідах такі ж, як і в традиційних пірамідах. Шахраї отримують гроші від нових інвесторів, щоб заплатити старим інвесторам, не створюючи жодних законних інвестиційних можливостей і залишаючи інвесторів без правового захисту.

8. Шахрайство з оновленням: криптоплатформи — це тип програмного забезпечення, який час від часу потребує оновлення. Оскільки споживачі звикли, що оновлення є частиною інноваційних технологій, споживачі звикли до цього. Їх легко обманювати, змусивши віддати свої приватні ключі в рамках «оновлення», яке виявиться шахрайським.

9. Шахрайство зі зміною SIM-карти: коли хтось отримує копію SIM-карти вашого мобільного телефону, щоб отримати доступ до даних вашого телефону, це називається підміною SIM-карти. Шахраї можуть викрасти двоетапні коди автентифікації, необхідні для відкриття його криптогаманця, отримавши дані користувача. Це дозволяє їм отримати доступ до коштів і даних на рахунку.

10. Підроблені криптобіржі та криптогаманці: недосвідчених користувачів криптовалют можуть заманити інвестувати в нову можливість обміну високовартісною криптовалютою або в неіснуючий «дешевий» біткойн. Доки жертва не втратить свої інвестиції, шахраї рекламують інвестиції за ціною, нижчою за ринкову. Фальшивий криптогаманець - це шкідливе програмне забезпечення, яке заражає комп'ютер і викрадає приватний ключ користувача.

2.4 Найбільші криптоатаки 2022

- Ronin Network: $625 млн.

Найбільша криптоатака 2022 року відбулася в березні. Зловмиснику вдалося пограбувати мережу Ronin Network, яка пропонує популярну гру Axie Infinity. Це дало йому 173 600 ETH і "улов" у розмірі $25,5 млн, тобто загальна вартість пограбування на той момент становила $625 млн.

Зловмисник використав зламаний приватний ключ для підписання двох транзакцій з виведення коштів з Ronin Bridge.

На той час на сайті було дев'ять валідаторів, і для авторизації транзакцій потрібна була більшість підписів (тобто щонайменше п'ять). Хакери успішно їх отримали. Це були ключі чотирьох валідаторів Ronin Sky Mavis і одного стороннього валідатора, контрольованого DAO Axie. Хакер зміг отримати їх через бекдор у вузлі Ronin RPC. Наразі Crosschain збільшив кількість валідаторів та запровадив додатковий захист. Однак повернути довіру гравців все ще складно.

- Wormhole: $325 млн.

У лютому міст Wormhole втратив близько 120 000 токенів Wrapped Ether (WETH), які на той момент коштували близько 325 мільйонів доларів США. Хакерам вдалося обійти перевірку протоколу і викарбувати токени WETH, продавши близько 94 000 з них за ETH в мережі Ethereum. Решту обміняли на інші альткоїни в мережі Solana.

Команда wormhole запропонувала виплатити 10 мільйонів доларів США в якості винагороди, якщо хакери схаменуться і повернуть кошти. Однак вони не відреагували на цю пропозицію. Материнська компанія Wormhole, Jump Crypto, покрила втрачені 120 000 ETH зі своїх резервів, щоб уникнути значної інфляції, яка б похитнула довіру користувачів до мосту.

- Nomad Bridge: 190 мільйонів доларів.

Ще одним постраждалим крос-ланцюговим протоколом став проект Nomad, з якого в серпні було виведено майже всі кошти (понад 190 мільйонів доларів США). На відміну від інших експлойтів, інцидент з мостом Nomad не був здійснений однією організацією або групою і торкнувся сотень адрес.

Під час першої підозрілої транзакції, яка, ймовірно, є джерелом експлойту, було виведено 100 Wrapped BTC (WBTC). За цим послідувала серія подібних імітацій. Сотні користувачів почали шпигувати за "успішними транзакціями" і виводити всі свої цифрові активи подібним чином.

Експерти пояснили це серйозною помилкою в контракті Replica. Ця помилка дозволяла хакерам відправляти токени без авторизації. Після цього імітатор замінював оригінальну адресу на свою, а потім повторював транзакцію.

- Beanstark Farms: 182 мільйони доларів.

Цей протокол стейблкоінів на основі Ethereum втратив всі свої заставлені активи на суму $182 млн. Інцидент стався 17 квітня і був викликаний вразливістю в системі управління протоколом. Компанія PeckShield, що займається онлайн-безпекою, вважає, що зловмисник використовував флеш-кредити для накопичення великої кількості контрольних токенів STALK. Це дало йому право робити власні пропозиції (BIP-18 і BIP-19).

Загалом зловмиснику вдалося вивести з різних криптоактивів близько 80 мільйонів доларів США. Згодом стейблкоіни BEAN знецінилися по відношенню до долара. Хакери відмили вкрадені кошти в Tornado Cash, тому зараз мало шансів їх відстежити. Однак, перш ніж зникнути, зловмисник відправив 250 000 доларів США на гаманець Crypto Donation в Україні.

- Wintermute: 162 мільйони доларів США.

У вересні Wintermute, один з відомих британських маркет-мейкерів, втратив приблизно 162 мільйони доларів США через свою DeFi-операцію. Проект також має централізовані фінансові та позабіржові ринки (на щастя, вони не постраждали).

Ось як Certik описує злом. Він був спричинений не використанням смарт-контрактів, а вразливим приватним ключем, який використовувався для атаки на платформу. Експерти вказують на витік через популярний генератор персональних адрес Profanity. Компанія використовувала цей метод для економії газу.Ситуація ускладнювалася тим, що маркет-мейкер мав 200 мільйонів доларів США заборгованості перед різними платформами. Зокрема, він заборгував 92 мільйони доларів США (в USDT) на платформі TrueFi. Однак Wintermute зміг погасити кредит 14 жовтня, всього за день до закінчення терміну виплати позики TrueFi.

- Mango Markets: 114 мільйонів доларів США

У жовтні DeFi платформа Mango Markets зазнала експлуатації на суму 114 мільйонів доларів США. Зловмисник маніпулював даними цінового оракула і зміг отримати доступ до великих криптовалютних кредитів з недостатнім забезпеченням. Він інвестував 5 млн доларів США в платформу Mango Markets і згодом відкрив довгу позицію в MNGO-PERP. Це спричинило зростання ціни MNGO, збільшивши заставну вартість його депозиту. Завдяки цьому виверту користувач отримав значний кредит на платформі.

Потім автор атаки (до речі, його звуть Абрахам Айзенберг) зробив пропозицію протоколу. Він зажадав, щоб Mango використовував кошти, що залишилися, для погашення безнадійних боргів у протоколі, але спільнота відкинула цю ідею. Тоді на голосування було винесено пропозицію, в якій хакерам пропонувалося повернути вкрадені токени на суму 67 мільйонів доларів США. Решта 47 мільйонів доларів США мали залишитися як винагорода за виявлення експлойта.

Цей інцидент вважається скоріше маніпулюванням ринком, ніж зломом або експлойтом. Принаймні, самі автори називають його "високоприбутковою стратегією". Однак, оскільки це був значний збиток для платформи.

- Blockchain BNB: 100 мільйонів доларів США

На початку жовтня мережа BNB Chain зазнала збитків, коли було використано міжланцюговий міст Binance Bridge. Це дозволило карбувати "зайві" токени BNB.

Початкові оцінки злочину були близькі до 600 мільйонів доларів США, але розробники повідомили, що зловмисники витратили від 100 до 110 мільйонів доларів США. Вони пояснюють, що експлойт був виконаний на токен-хабі BSC, який є мостом між ланцюжком маяків BNB і мережею ланцюжків BNB. Причиною стала помилка в смарт-контрактах, яка давала змогу хакерам підробляти транзакції та переказувати гроші на власні адреси.

2.4 Найбільші взломи 2023

1. Злом біржі Bitrue (23 мільйони доларів)

Популярна криптовалютна біржа Bitrue стала жертвою масштабного злому у квітні 2023 року, унаслідок якого було викрадено $23 млн в Ethereum, Gala та інших криптовалютах. Кіберзлочинці використовували систему гарячих гаманців біржі, отримавши доступ до одного з чотирьох гарячих гаманців, на яких зберігається 5% усіх активів біржі. Однією з основних причин зберігання коштів на біржах, коли торгівля не ведеться, є те, що їхні заходи безпеки поширюються на кошти користувачів. Біржі не застраховані державою тією самою мірою, що й банки.

2. Загадка криптокита (10 мільйонів доларів США)

Унаслідок загадкового хакерського інциденту у квітні цього року крипто-кити та ранні інвестори втратили 10 мільйонів доларів США зі своїх рахунків на 11 різних блокчейнах, здебільшого Ethereum. Хакери націлилися на людей зі значними пакетами акцій, використовуючи вразливості в мультисигових контрактах з відкритим вихідним кодом, які використовуються для захисту активів. Атака обійшла заходи безпеки в контрактах, що дало змогу хакерам отримати доступ до приватних ключів і вивести кошти. Причина злому досі не до кінця зрозуміла, а збереження закритих ключів в автономному режимі дало б змогу запобігти цьому злому на невизначений час.

3. Deus Finance (6 мільйонів доларів США).

Deus Finance, децентралізований фінансовий протокол (DeFi), постраждав від порушення безпеки 5 травня, втративши понад 6 мільйонів доларів США внаслідок атаки на стабільну криптовалюту DEI. Злом почався зі смарт-ланцюжка BNB (BSC), а потім націлився на мережу Arbitrum, внаслідок чого розгортання ARB/ETH втратили понад 5 мільйонів доларів США. Передбачається, що першопричиною вторгнення стала базова помилка в реалізації контракту на токен.

Після атаки Deus Finance призупинила всі контракти і спалила токени DEI, щоб запобігти подальшим збиткам. Це не вперше, коли Deus Finance стикається з порушенням безпеки. у березні 2022 року протокол був унаслідок чого було втрачено понад 3 мільйони доларів США в Dei і Ether. Викрадені кошти були спрямовані через крипто-мікшер Tornado Cash, як з'ясувала компанія PeckShield. Deus Finance - це децентралізований торговельний майданчик для торгівлі цифровими активами і нецифровими активами, такими як товари, на блокчейні Ethereum.

4. Злом Trust Wallet за допомогою соціальної інженерії (4 мільйони доларів США).

Користувачі Trust Wallet зазнали збитків у розмірі 4 мільйонів доларів США після того, як хитрі хакери використовували тактику соціальної інженерії, щоб обійти заходи безпеки. Зловмисники обманом змусили користувачів розкрити конфіденційну інформацію, що дало їм змогу отримати доступ до їхніх рахунків і спустошити їх. Шахраї, які видають себе за інвесторів Web3, під час особистої зустрічі переконують вас завантажити PDF, що містить шкідливе ПЗ, щоб вкрасти облікові дані вашого гаманця.

Атаки з використанням соціальної інженерії, такі як фішинг і спуфінг, стають дедалі поширенішими, оскільки на міжнародних заходах збираються ключові фігури і співробітники індустрії блокчейн. Стає дедалі важливішим, щоб люди були пильними і проактивними, щоб захистити свої особисті дані та пристрої.

5. Скандал у Твіттері Kucoin ($22 тис.)

Шахраї зламали акаунт Kucoin у Twitter і провели фальшиву кампанію з роздачі криптовалюти, змушуючи користувачів, які нічого не підозрюють, відправляти кошти на невідомий рахунок. Ця сума може здатися дріб'язковою порівняно з іншими

зломами, але вона надзвичайно лякає: за такого великого обсягу спілкування через Twitter та інші платформи соціальних мереж крадіжка облікових даних у набагато більших масштабах призвела б до втрати $22, 600. Втрата 600 доларів була б на декілька порядків гіршою, ніж ця втрата в $22, 600.

Kucoin пообіцяв відшкодувати збитки користувачам, які відправили гроші на фальшиві роздачі, але більш значні втрати були пов'язані з питанням безпеки особистих або робочих облікових даних.

Висновки за розділом 2

У результаті аналізу розділу про криптогаманці і криптовзломи, було виявлено, що безпека криптовалютних активів має вирішальне значення для користувачів. Відповідно до цього, розробка та впровадження ефективних заходів безпеки є невід'ємною складовою успішного використання криптовалютних технологій та блокчейну. У цьому розділі були виявлені різні загрози та вразливості, пов'язані з криптогаманцями, такі як фішинг, втрати приватних ключів і викрадення приватних ключів. Ці загрози можуть призвести до незворотних втрат криптовалютних активів та інформації.

З метою забезпечення безпеки криптовалютних активів рекомендується використовувати надійні гаманці, забезпечувати фізичну безпеку приватних ключів, використовувати двофакторну аутентифікацію та бути обережними в мережі.

Оцінка розділу підтверджує, що розроблені рекомендації можуть сприяти підвищенню безпеки використання криптовалютних технологій та блокчейну. Ретельне дотримання цих рекомендацій допоможе користувачам захистити свої криптовалютні активи від потенційних загроз і втрати.

РОЗДІЛ 3
ЗАХИСТ ЦІЛІСНОСТІ

3.1 Виконання транзакцій в різних блокчейнах

Принципи роботи транзакцій в блокчейні. На рисунку 3.1 зображено скрін, що є складовою процесів виконання та прикладів транзакцій в блокчейнах. Перший перевод я робив з CEX біржі Binance на свій гаманець MetaMask

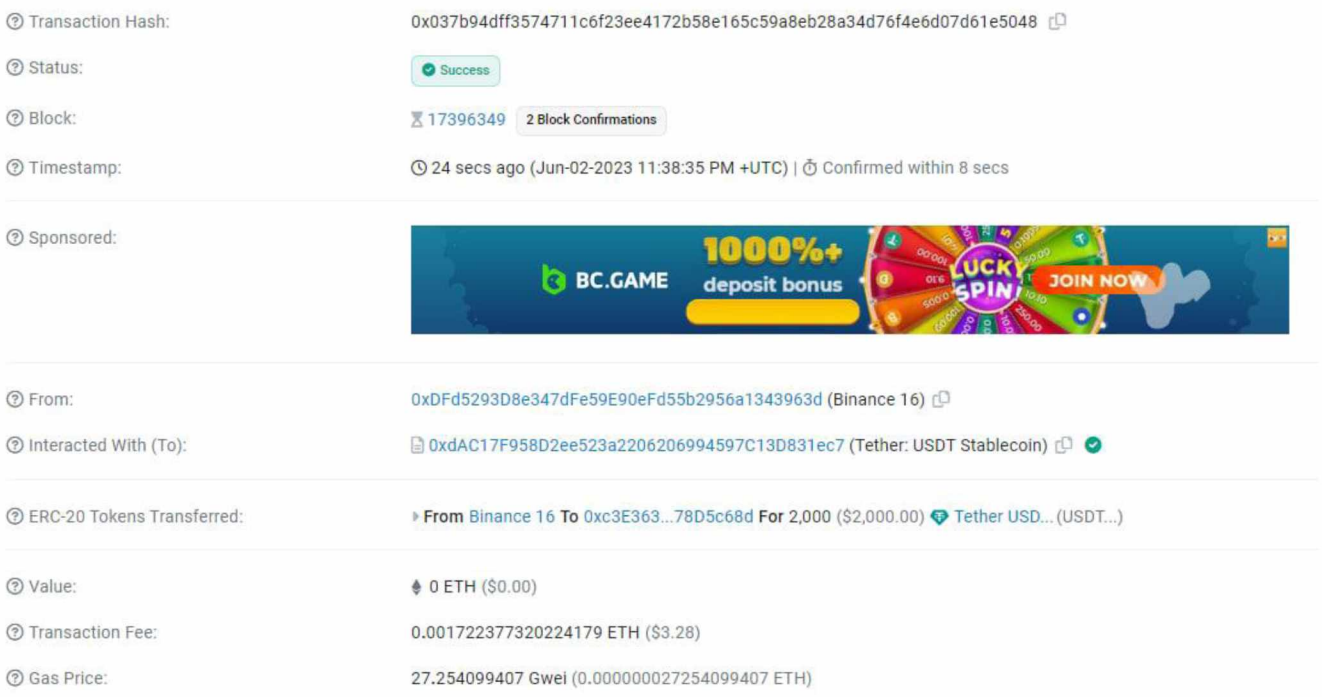

Рисунок 3.1 – Etherscan дані про зроблену транзакцію

Строка Transaction Hash – вказує хеш транзакції по котрому її можна відшукати і перевірити.

Строка Status – повідомляє, в якому стані знаходиться транзакція – чи вона була успішно виконана чи сталася помилка.

Строка Block – показує номер блоку, в якому записана транзакція. Підтвердження блоків показують, скільки блоків було додано з моменту створення транзакції.

Строка Timestamp – записує дату та час коли транзакція була зроблена.

Строка From – вказує відправника транзакції.

Строка Interacted With (To) – додає приймаючу сторону транзакції. Також це може бути адреса смарт-контракту.

Строка ERC-20 Tokens Transferred – вносить список переданих ERC-20 токенів в транзакції.

Строка Transaction Fee – сума, сплачена виробнику блоку за обробку транзакції.

Строка Gas Price – вартість одиниці газу, вказана для транзакції, в ефірах та гвей. Чим вища вартість газу, тим більше шансів потрапити в блок.

Строка Value – Вартість транзакції в Ефірі та фіатній валюті. Примітка: Ви можете натиснути на фіатну вартість (якщо вона доступна), щоб побачити історичну вартість на момент транзакції.

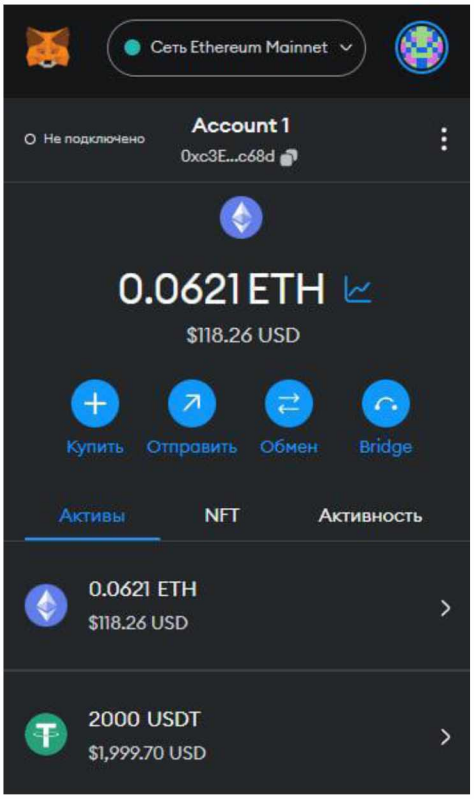

Рисунок 3.2 – MetaMask гаманець

Після успішного завершення транзакції, гроші були зараховані на аккаунт MetaMask

Далі на сайті Stargate було здійснено підкючення гаманця для подальшого використання екосистеми LayerZero для переводу USDT з мережі ETH на BNB SMART CHAIN.

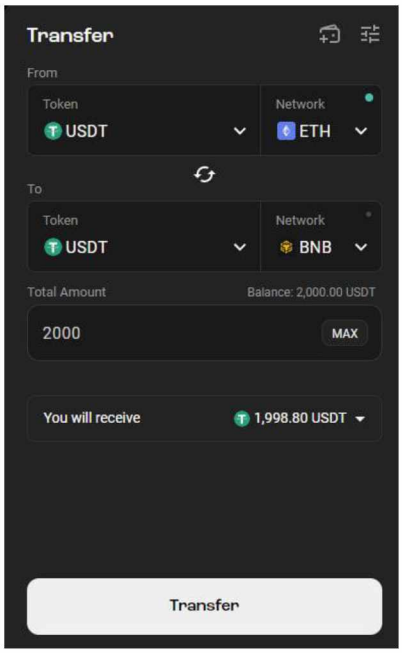

Рисунок 3.3 – stargate перевод

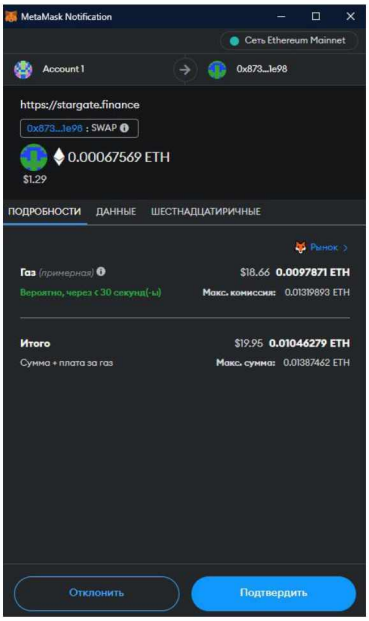

Рисунок 3.4 – підтвердження транзакції у мережі ETH в MetaMask

Як виглядало підтвердження транзакції у MetaMask, в ціну транзакції входить сума + плата за газ.

Рисунок 3.5 – stargate процес переводу

Як на самому Stargate виглядала передача токенів з мережі ETH в BNB SMART CHAIN.

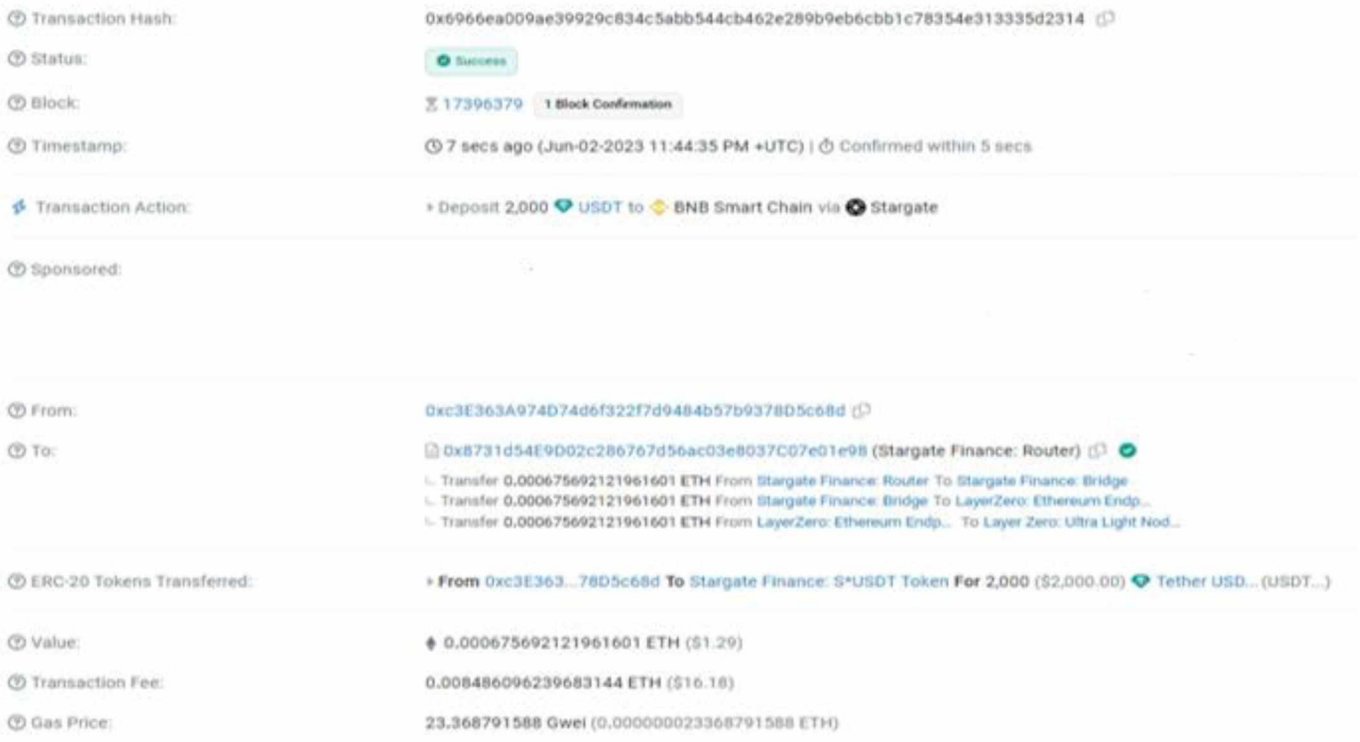

Рисунок 3.6 – Etherscan дані про перевод

Після переводу USDT в мережу BNB SMART CHAIN, використали сайт PancakeSwap для переводу в BUSD.

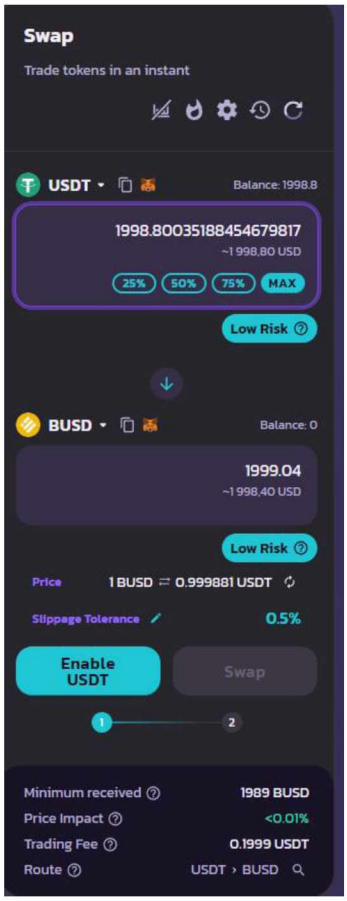

Рисунок 3.7 – PancakeSwap трансфер USDT в BUSD

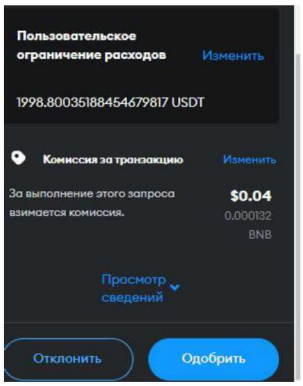

Рисунок 3.8 – підтвердження транзакції на BNB SMART CHAIN в MetaMask

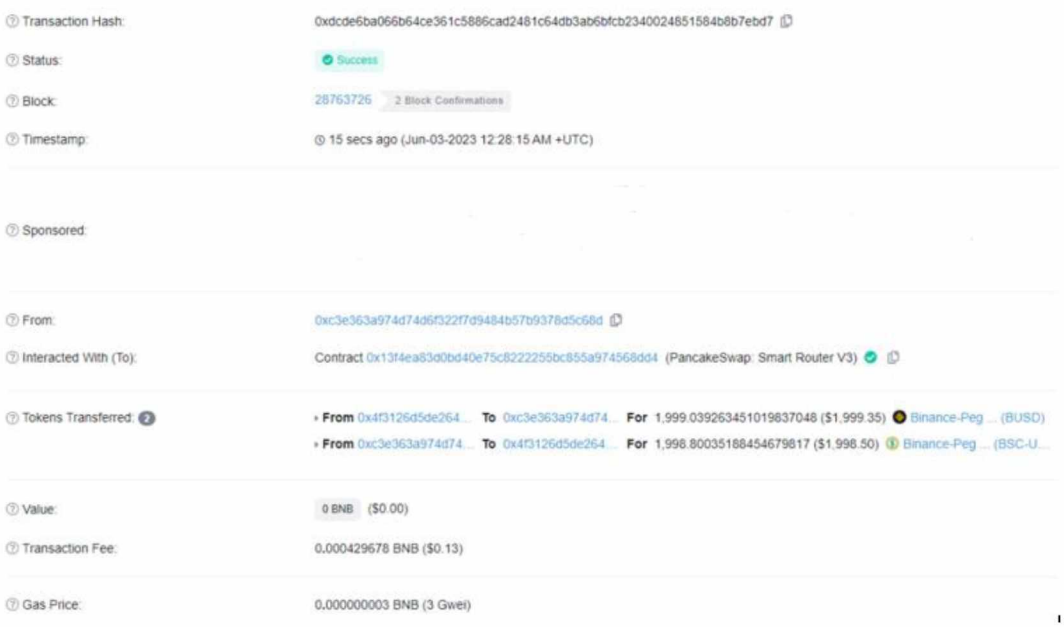

Рисунок 3.9 – Etherscan дані про сваp

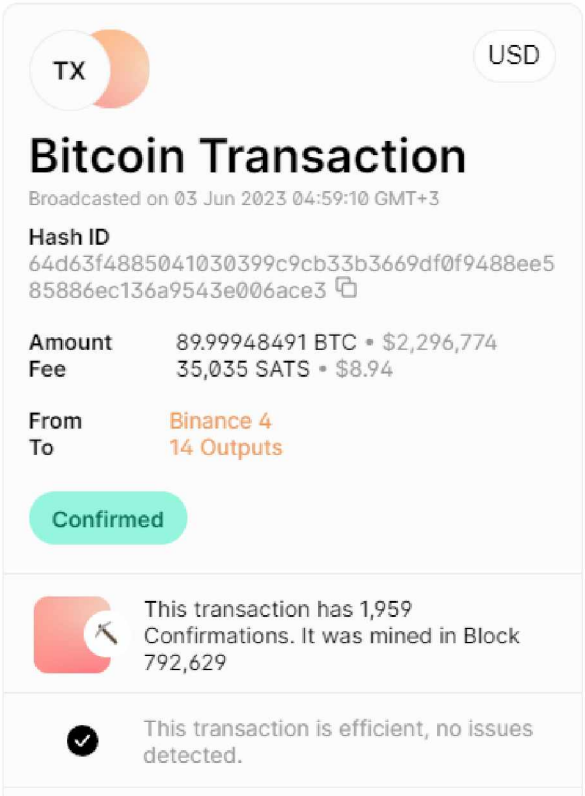

Рисунок 3.10 - Транзакція в Bitcoin(скорочено)

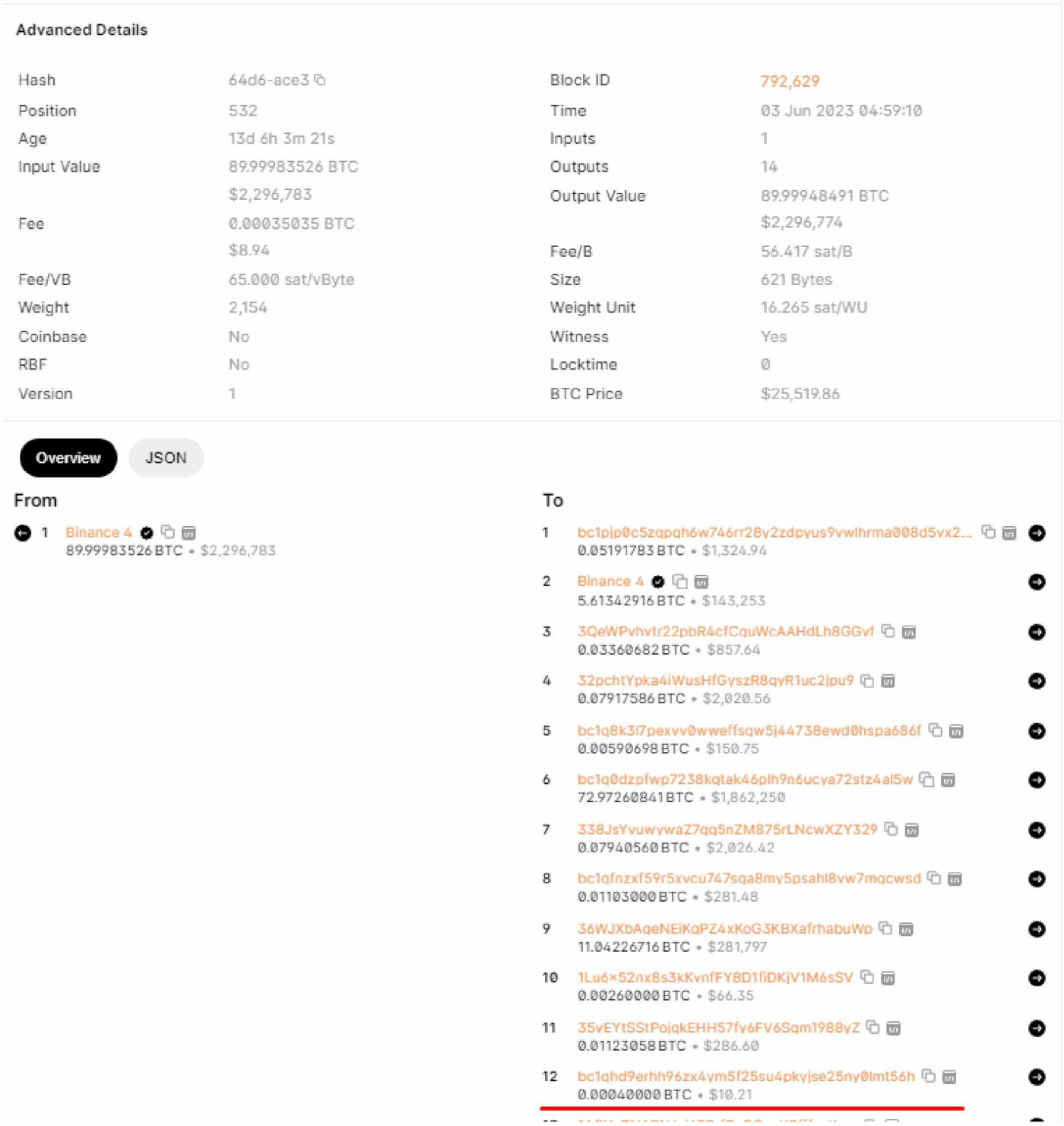

Рисунок 3.11 – Транзакція в Bitcoin ч.2 (розвернуто)

Транзакция в біткоїні почалася з гарячого гаманця на біржі Binance і була спрямована на чотирнадцять різних гаманців, передбачала пересилання валюти від одного адреси до інших.

У процесі транзакції були надані адреси отримувачів і кількість біткоїнів, яку потрібно перевести на кожен з цих гаманців. Після того, як транзакція була підтверджена мережею біткоїн, кошти були успішно переведені на відповідні адреси отримувачів. Червоним позначена адреса на котру була відправлена транзакція.

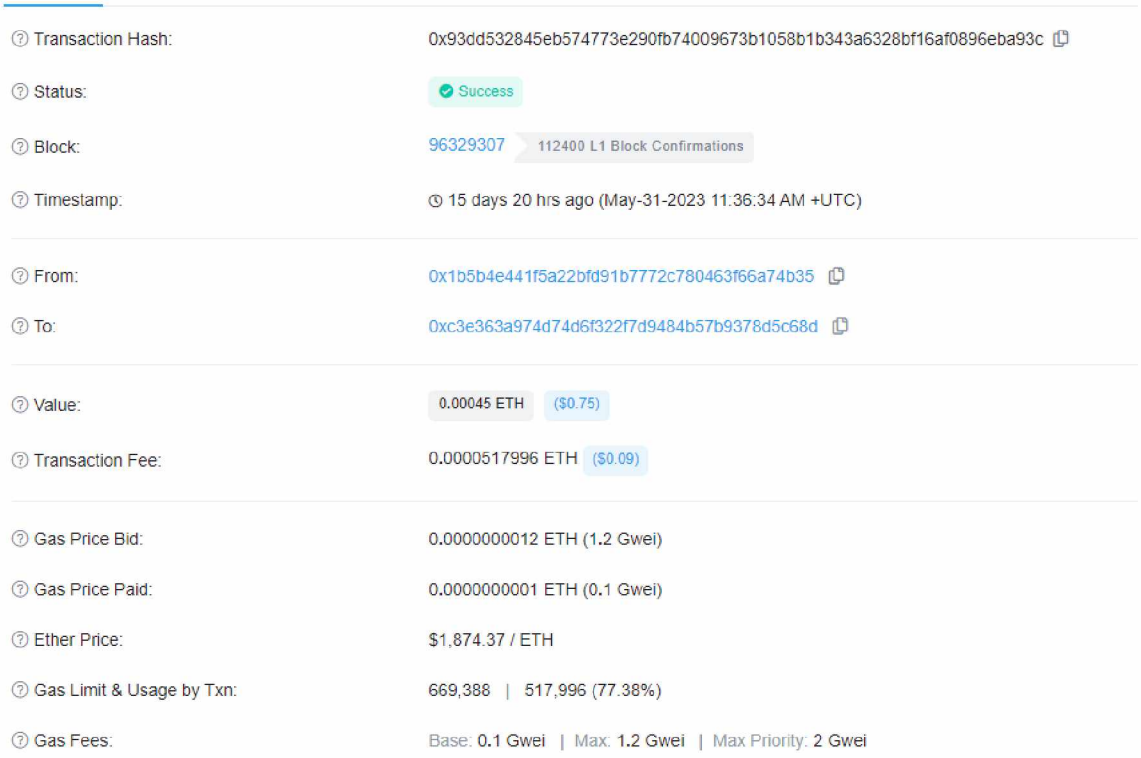

Рисунок 3.12 – Arbiscan дані про транзакцію

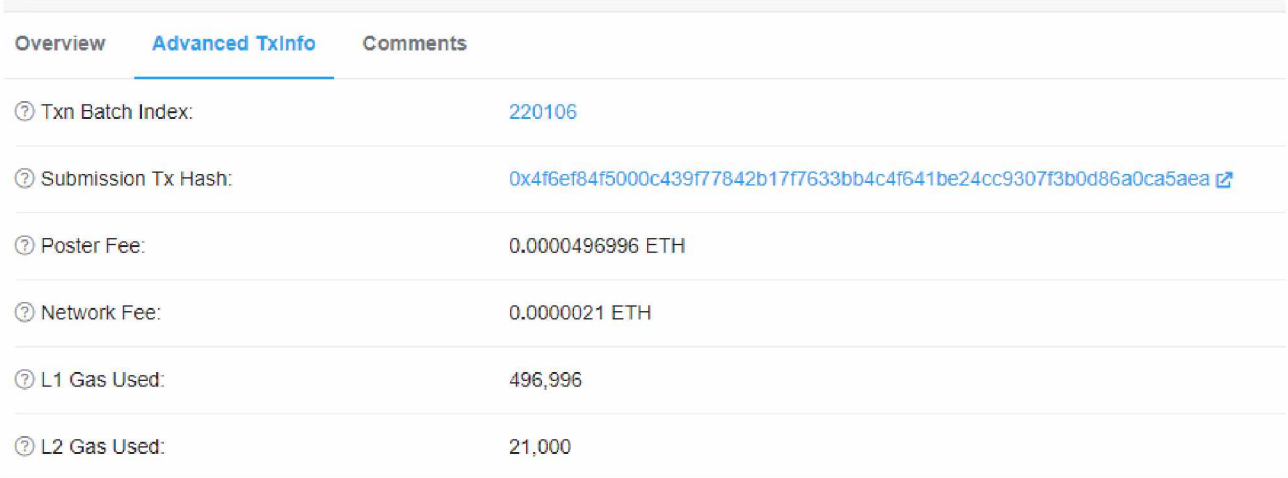

Рисунок 3.13 – продвинута інформація про транзакцію

3.2 Розробка рекомендацій по підвищенню безпеки використання криптовалют і технології блокчейн.

Для цієї кваліфікаційної роботи я провів подкаст з діючим спеціалістом у сфері кібербезпеки в криптовалюті Юрієм Мелащенко, він дав перелік рекомендацій для забезпечення безпеки коштів і уникнення шахрайства, котрі я доповнив:

1. Більшість взломів типові.

Технологія блокчейн передбачає аудит смарт-контрактів для криптопроектів. Деякі економлять і проходять недорогий аудит, інші не економлять і витрачають більше. Інші проводять аудит регулярно, а деякі – нерегулярно. Кібербезпека і безпека смарт-контрактів – це процес, а не результат. Тобто він може на якийсь час бути актуальним, але треба це робити завжди. Кібербезпека, безпека – це не стан. Ось це треба головне пам'ятати. Втратити гроші набагато швидше і простіше, ніж потім їх відновити.

2. Втрата грошей швидше і простіше, ніж їх відновлення. Багато людей не інвестують у кібербезпеку, оскільки вважають, що проблеми обійдуть їх стороною. Але коли такі проблеми все ж стаються, в блокчейні транзакції немає можливості скасувати. Якщо це не якийсь фейковий блокчейн.

3. Уникайте переходу на підозрілі веб-сторінки, особливо ті, які намагаються підманити ваші особисті дані або кредитну інформацію. Будьте обережними при отриманні повідомлень електронною поштою, соціальних мереж або інших джерел. Шахраї можуть намагатися видати себе за представників платформи або гаманця, щоб отримати ваші конфіденційні дані. Перевіряйте автентичність джерела та ніколи не надавайте особисту інформацію безпосередньо через недостовірні канали зв'язку. Завжди перевіряйте URL-адресу та переконайтесь, що ви належним чином захищені.

4. Зробіть багато гаманців, наприклад Metamask. Для підключення к неперевіреним сайтам і перевірці нових проектів. Це допоможе прибрати людський фактор при користуванні і захистить кошти на ваших основних гаманцях

5. Ніколи не зберігайте активний гаманець на комп'ютері: Уникайте тримати активний гаманець на комп'ютері, особливо на машинах, які підключені до Інтернету.

Це допомагає запобігти несанкціонованому доступу до ваших криптовалютних активів.

6. Розгляньте можливість використання окремого телефону або пристрою для зберігання вашого гаманця. Це дозволить вам утримувати ваші криптовалютні активи в безпеці, окремо від основного пристрою, який використовується для інших цілей. Найкращий девайс для цього Google Pixel на GrapheneOS.

7. Активуйте двофакторну аутентифікацію на всіх ваших криптовалютних платформах і гаманцях. Це забезпечить додатковий рівень захисту, оскільки для доступу до вашого облікового запису потрібні будуть і ваш пароль, і унікальний код, який змінюється з часом.

8. Перевіряйте адреси перед виконанням транзакцій: Перед відправленням криптовалюти перевірте адресу отримувача двічі. Шахраї можуть намагатися підставити вам неправильну адресу, тому будьте уважні та упевнені в правильності введеної адреси.

9. Уникайте публічного розголошення деталей, про гаманці і свої статки в криптовалюті. Це може використовуватися зловмисниками для отримання доступу до вашого гаманця або викрадання вас для розголошення приватних ключей.

10. Оновлюйте програмне забезпечення: Регулярно оновлюйте програмне забезпечення своїх гаманців та платформ. Виробники постійно вдосконалюють безпеку, виправляють вразливості і надають нові функції. Іноді неоновлення програмного забезпечення може призвести до збоїв у безпеці, а іноді навпаки нове програмне забезпечення може мати свіжі баги, котрі приведуть до витоку приватних ключів.

11. Підтримуйте антивірусне програмне забезпечення: Встановіть і підтримуйте оновлене антивірусне програмне забезпечення на вашому пристрої. Це допоможе виявити й усунути можливі загрози шкідливого програмного забезпечення, які можуть намагатися отримати доступ до ваших криптовалютних даних. Також, гарним рішенням буде використання Apple техніки.

12. Знайте своїх посередників: Ретельно досліджуйте платформи та сервіси, з якими ви працюєте. Переконайтеся, що вони мають сильну репутацію та надійність.

Уникайте надавати особисту інформацію або надсилати кошти ненадійним особам чи платформам.

Висновки до розділу 3

Порівняння транзакцій, які проводяться в мережах Bitcoin, Ethereum, Arbitrum і Binance Smart Chain (BNB) наведено нижче:

Bitcoin (BTC):

Підтвердження транзакції займає зазвичай від десяти до шестидесяти хвилин.

Висока комісія: Стан мережі та обсяг транзакції можуть зробити комісію високою.

Середній обсяг транзакцій на блок становить приблизно 1 МБ

Ethereum (ETH):

Підтвердження транзакції займає зазвичай від п’ятнадцяти секунд до п’яти хвилин.

Висока комісія: Якщо мережа переповнена, комісії можуть бути високими.

Середній обсяг транзакцій на блок становить приблизно п’ятнадцять-двадцять транзакцій.

Arbitrum:

Час, необхідний для підтвердження транзакції, зазвичай становить кілька секунд або менше.

Низькі комісії: зазвичай вартість комісії значно нижча, ніж у Ethereum.

Середній обсяг транзакцій на блок: це залежить від обсягу блоку, але зазвичай можуть бути більше.

(BNB):

Підтвердження транзакції займає зазвичай від трьох до п’яти секунд.

Низькі комісії: зазвичай ціни нижчі, ніж у мережі Ethereum.

Середній обсяг транзакцій на блок: порівняно з Ethereum, мережа Binance Smart Chain може приймати більше транзакцій на блок.

Загалом, час підтвердження та комісія залежить від мережі. У порівнянні з Bitcoin і Ethereum, Arbitrum і Binance Smart Chain пропонують швидші транзакції та низькі комісії. При виборі найкращого рішення для конкретних потреб слід враховувати особливості кожної мережі.

ВИСНОВКИ

У підсумку кваліфікаційної роботи, були розглянуті ключові аспекти криптовалют та технології блокчейн. Робота включала розділ про аналіз основних криптовалютних систем, їх принципів роботи, переваг та викликів, а також вивчення різноманітних застосувань технології блокчейн

У розділі про безпеку криптовалют були розглянуті загрози, пов'язані з приватними ключами, криптогаманцями та криптовзломами. Запропоновані рекомендації щодо забезпечення безпеки криптовалютних активів можуть допомогти користувачам уникнути потенційних ризиків та втрати коштів

Робота також включала в себе розповсюдження знань про криптовалюту та блокчейн. Було виявлено, що освіта та інформаційна грамотність грають важливу роль у сприйнятті та використанні криптовалютних технологій. Розроблені рекомендації щодо поширення знань можуть сприяти підвищенню обізнаності та розумінню криптовалют серед широкої громадськості.

Результати досліджень та рекомендації можуть бути корисними для широкого спектру зацікавлених сторін, включаючи користувачів криптовалют, експертів у галузі кібербезпеки.DYOR.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.

1. W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

2. H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999

3. S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

4. D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

5. S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

6. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

7. R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

8. W. Feller, "An introduction to probability theory and its applications," 1957.

9. Buterin V. Ethereum Whitepaper [Електронний ресурс] / Vitalii Buterin. – 2014. – Режим доступу до ресурсу: https://ethereum.org/en/whitepaper/#ethereum-whitepaper.

10. Zhao C. Binance Whitepaper [Електронний ресурс] / C. Zhao, R. Wang, J. Hofbauer. – 2018. – Режим доступу до ресурсу: https://whitepaper.io/document/10/binance-whitepaper.

11. Harry Kalodner H. Arbitrum Whitepaper [Електронний ресурс] / H. Harry Kalodner, S. Steven Goldfeder, X. Xiaoqi Chen. – 2018. – Режим доступу до ресурсу: https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-kalodner.pdf.

12. Yin M. Avalanche Consensus Protocol Whitepaper [Електронний ресурс] / M. Yin, K. Sekniqi. – 2019. – Режим доступу до ресурсу: https://assets.website-files.com/5d80307810123f5ffbb34d6e/6009805681b416f34dcae012_Avalanche%20Consensus%20Whitepaper.pdf.

13. Pellegrino B. LayerZero: Trustless Omnichain Interoperability Protocol [Електронний ресурс] / B. Pellegrino, R. Zarick, C. Banister. – 2021. – Режим доступу до ресурсу: https://layerzero.network/pdf/LayerZero_Whitepaper_Release.pdf.

14. Wood J. Custodial Wallets vs. Non-Custodial Crypto Wallets [Електронний ресурс] / Jackson Wood. – 2022. – Режим доступу до ресурсу: https://www.coindesk.com/learn/custodial-wallets-vs-non-custodial-crypto-wallets/