ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «ДОСЛІДЖЕННЯ СПОСОБІВ ВИКОРИСТАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ»

на здобуття освітнього ступеня магістра
зі спеціальності 126 Інформаційні системи та технології
освітньо-професійної програми Інформаційні системи та технології

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ *Дмитро ГАРНИК*

Виконав: здобувач вищої освіти гр. ІСДМ-62

Дмитро ГАРНИК
Ім'я ПРІЗВИЩЕ

Керівник Оксана ТКАЛЕНКО
к.т.н., Ім'я ПРІЗВИЩЕ
доцент

Рецензент_____
Ім'я ПРІЗВИЩЕ

Київ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Інженерії програмного забезпечення автоматизованих систем

Ступінь вищої освіти - «Магістр»

Спеціальність - 126 – Інформаційні системи та технології

Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедрою
Інженерії програмного забезпечення автоматизованих систем
_____Каміла СТОРЧАК
«____» _____20___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ СТУДЕНТУ
Гарнику Дмитру Олексійовичу
(прізвище, ім'я, по батькові здобувача)

1.Тема кваліфікаційної роботи: «Дослідження способів використання блокчейн-технологій»

керівник кваліфікаційної роботи Оксана ТКАЛЕНКО, к.т.н., доцент
(ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від «19» жовтня 2023 року № 145.

2. Строк подання кваліфікаційної роботи: 28 січня 2023 року.

3. Вихідні дані до кваліфікаційної роботи: Методи PuTTY, Solidity, Vyper, Console, Docker, Ubuntu, Contabo;
Протоколи SSH;
Бібліотеки Solidity.
Науково-технічна література з питань, пов'язаних з наукою про дані.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження особливостей блокчейн-технології.

2. Інструменти для встановлення мережевого з’єднання із нодою Shardeum.
3. Дослідження справностьі технології блокчейн на основі проєкту Shardeum .

5. Перелік ілюстративного матеріалу: *презентація*

6. Дата видачі завдання: 20 жовтня 2023 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	20.10.23 – 26.10.23	Виконано
2	Дослідження методів та технологій обробки даних	27.10.23 – 11.11.23	Виконано
3	Аналіз виникнення криптовалют та блокчейну	12.11.23 – 15.11.23	Виконано
4	Дослідження способів використання блокчейн технологій	15.11.23 – 20.11.23	Виконано
5	Реалізація використання технології блокчейн на прикладі проєкту Shardeum	20.11.23 – 10.12.23	Виконано
6	Оцінка продуктивності та ефективності мережі	10.12.23 – 11.12.23	Виконано
8	Розробка рекомендацій для вдосконалення блокчейну Shardeum	11.12.23 – 12.12.23	Виконано
9	Вступ, висновки, реферат	12.12.23 – 13.12.23	Виконано
10	Подання роботи в деканат	28.12.23	Виконано
11	Попередній захист роботи	15.12.23	Виконано

Здобувач вищої освіти _____ Дмитро ГАРНИК
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник роботи
кваліфікаційної роботи _____ Оксана ТКАЛЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 111 стор., 26 рис., 36 джерел.

Мета роботи – з'ясувати яким чином працює технологія Blockchain та знайти її недоліки і переваги.

Об'єкт дослідження – методи та способи забезпечення проведення транзакцій за допомогою Blockchain.

Предмет дослідження – способи утворення мережевих вузлів та забезпечення їхнього функціонування в мережі Shardeum.

Короткий зміст роботи: Проаналізовані літературні джерела, здійснена класифікація всіх можливих технологій Blockchain, встановлено та досліджено мережевий вузол від проєкту Shardeum, також окреслено та висунуто ряд можливих шляхів підвищення ефективності даної технології.

КЛЮЧОВІ СЛОВА: ДАНІ, КРИПТОВАЛЮТА, БЛОКЧЕЙН-ТЕХНОЛОГІЇ, МЕТОДИ, МЕРЕЖА, СЕРВЕР, ГАМАНЕЦЬ

ABSTRACT

The text part of the qualification work for the master's degree: 111 pages, 26 figures, 36 sources.

The purpose of the work is to find out how Blockchain technology works and to find its disadvantages and advantages.

Object of research - methods and ways to ensure transactions using Blockchain.

The subject of research - is the ways of creating network nodes and ensuring their functioning in the Shardeum network.

Summary of the work: The article analyzes the literature, classifies all possible Blockchain technologies, establishes and studies the network node from the Shardeum project, and outlines and puts forward a number of possible ways to improve the efficiency of this technology.

KEYWORDS: DATA, CRYPTOCURRENCY, BLOCKCHAIN TECHNOLOGIES, METHODS, NETWORK, SERVER, WALLET

ЗМІСТ

ВСТУП

Блокчейн, що являється новітньою технологією здобув шалений інтерес паралельно із зростанням криптовалют. Криптовалюта представляє собою електронні реєстри, які фіксують загальну інформацію про користувача та його фінансові операції. Кошти зберігаються на відповідних електронних гаманцях та пересилаються за допомогою криптограіфічних методів, одним із яких є технологія блокчейн.

У 2008 році автор під псевдонімом Сатосі Накамоту висунув ідею про створення блокчейну. А вже у 2009 році відбулась її реалізація, в той же час було створено основну складову Bitcoin, що застосовує технологію блокчейн задля створення відкритого реєстру транзакцій в мережі. Саме завдяки блокчейну Bitcoin став першою криптовалютою. Блокчейном називають ланцюжок блоків, які містять відповідну інформацію вбудовану за принципами, яка зберігається на великій кількості комп'ютерів. Система здатна приймати різні конфігурації відповідно до застосування. Блокчейн часто порівнюють із великою книгою, де кожен представник гаманця із криптовалютою має самостійну та ідентичну копію. Записи у всіх книгах є ідентичними та правдивими, інший учасник системи не здатен підробити чи втрутитись в них. Також слід зазначити, що блокчейн не має контролера, система управляється лише учасниками та забезпечується математичними обчисленнями, це гарантує безпеку цифрової валюти від зламу та підробок.

Також поява блокчейну слугувала початком для створення смарт-контрактів, що почали своє практичне застосування за п'ять років після появи технології, на базі Ethereum. Зараз існує велика кількість платформ, які дозволяють застосовувати смарт-контракти, але Ethereum лишається однією із найпоширеніших для їх реалізації. Розширення блокчейну в різних галузях, окрім просто відправлення та отримання цифрових грошей є сучасною досить розвиненою тенденцією. Відомо, що криптовалюта Bitcoin продемонструвала як криптографія та ретельно

розроблені економічні стимули створюють безпечний метод зберігання та управління інформацією, включаючи і особисті дані.

Актуальність теми. В наш час досить важко забезпечити швидку і дешеву транзакцію у будь-яку частину світу за малий проміжок часу. Людство розвивається шаленими темпами, великої популярності набувають комп'ютерні мережі та відповідні сервіси. Сьогодні важко уявити будь-яку сферу діяльності, де б не використовувалися інформаційні технології. Все далі стає необхідним розвивати та удосконалювати способи збереження та передачі інформації. Саме тому, ми вирішили дослідити детальніше дану тему з метою покращення технологій, використовуючи проєкт Shardeum.

Мета роботи. З'ясувати яким чином працює технологія Blockchain та знайти її недоліки і переваги.

Завдання дослідження:

- Проаналізувати літературні джерела;
- Класифікувати можливі технології Blockchain;
- Встановити та дослідити мережевий вузол від проєкту Shardeum;
- Окреслити шляхи підвищення ефективності даної технології.

Об'єкт дослідження. Методи та способи забезпечення проведення транзакцій за допомогою Blockchain.

Предмет дослідження. Способи утворення мережевих вузлів та забезпечення їхнього функціонування в мережі Shardeum.

Методи дослідження. Статистичні, аналітичні, математичні.

Наукова новизна результатів роботи полягає в наступному:

- Виконано аналіз роботи даної мережі та досліджено її вразливість.
- Запропоновані рішення для подолання проблем в мережі Shardeum, які являються базовими та необхідними для коректної роботи блокчейну.

Практичне значення одержаних результатів. Отримані в ході дослідження результати свідчать про те, що запропонований метод дозволяє забезпечити надійний обмін інформацією, ґрунтуючись на технології блокчейн. Цей метод може бути розширений та застосований в різних областях.

Апробація результатів магістерської роботи. Гарник Д.О. «Використання технології «блокчейн» у телекомунікаціях». Тези доповіді на І Всеукраїнській науково-технічній конференції "Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу України і Світу". – Київ, 28 листопада 2023 року.

Публікації. Гарник Д.О. «Дослідження проблеми оптимізації продуктивності в мові програмування Java». Стаття у загальногалузевому науково-виробничому журналі «Зв'язок», м.Київ - №5, 2021. – С.15-20.

РОЗДІЛ 1 КРИПТОВАЛЮТА ТА БЛОКЧЕЙН ТЕХНОЛОГІЇ

1.1 Аналіз виникнення криптовалют та блокчейну

Протягом останніх років зацікавленість людей у понятті блокчейну та криптовалют стрімко зростає. Вони проникають до певних сегментів ринку, рухаючись хвилями зі зростанням та спаданням. На сьогодні криптовалюти стали глобальним явищем, яким зацікавлені все більше осіб та організацій. Криптовалюта — це різновид цифрової валюти, яка є альтернативною формою оплати через онлайн-систему, створеною за допомогою алгоритмів шифрування. Це означає, що криптовалюта функціонує і як валюта, і як віртуальна система обліку. Такі гроші можуть бути використані для купівлі та як інвестиційні внески. Вони не вимагають від фінансових установ чи банків перевірки переказу коштів (транзакцій). Лише потім операції будуть записуватися у блокчейн, так звану комірку, яка відслідковує та реєструє активи та транзакції без можливості їх змінити [10].

Проте, важливо відзначити, що багато людей помиляються, пов'язуючи термін блокчейну лише з криптовалютою. Насправді, сфера потенційного використання блокчейну виявляється надзвичайно широкою, а використання блокчейн-технології для створення криптовалют – це лише одна з її можливих застосувань. На сьогодні технологією блокчейну користуються приватні підприємства, контролюючи рух коштів на своїх рахунках, медичні, освітні навчальні заклади, логістичні компанії для захисту даних про всі операції, що проводяться в ланцюгу постачання тощо. Але криптовалюта займає переважну більшість порівняно з іншими сферами, тому саме її варто розглядати детальніше. Багато хто не знає, що історія створення першої криптовалюти сягає далеко до того моменту, як стало відомо про криптовалюту Bitcoin [12].

Близько 20 років тому в Нідерландах вже робили спробу відмовитись від грошей та замінити їх пластиковими картами на автозаправочних станціях, тим самим відкинувши потребу носити з собою готівкові гроші водіям, так як оплачувати за пальне вони могли вже картами. Це дозволило уникнути нічних крадіжок. Чи, наприклад, американський криптограф Девід Чаум створив технологію "сліпого цифрового підпису", яка дозволяла здійснювати безпечні та конфіденційні транзакції, забезпечуючи приватність даних. Пізніше Чаум заснував компанію DigiCash, яка, хоч і зазнала банкрутства у 1998 році, але внесла значний внесок у розвиток концепції цифрових валют. Ідеї та криптографічні рішення DigiCash вплинули на численні стартапи 1990-х, включаючи такий відомий сервіс, як PayPal, що зробив революцію у створенні онлайн-платежів [4].

Це дозволило користувачам швидко та безпечно переказувати гроші через Інтернет. Після укладення угоди з eBay, PayPal здобула доступ до величезної аудиторії користувачів, що дозволило їй стрімко зростати. Дотепер PayPal залишається одним з провідних платіжних сервісів, служачи прикладом для наслідування [12].

У 1998 році ще один американський розробник Вей Дай вигадав систему електронних грошей, яку він назвав B-money, що мала бути анонімною та розподіленою. Дай пропонував два різних протоколи, один з яких потребував створення синхронного та надійного каналу зв'язку. Концепція B-Money значно відрізнялась від Bitcoin і не отримала подальшого розвитку. B-Money використовував цифрові псевдоніми для переказу валюти через децентралізовану мережу та передбачав автономне виконання контрактів без участі третьої сторони. Hashcash, розроблена в середині 1990-х, стала однією з успішних цифрових валют до народження Bitcoin. Вона використовувала алгоритм Proof-of-Work для створення та розподілу нових монет. Однак у 1997 році, з причини нестачі обчислювальної потужності, Hashcash втратила ефективність і зникла. У свій час Hashcash була дуже популярною, і багато з її принципів стали основою для системи Bitcoin [10].

Поява Bitcoin у 2009 році призвела до народження нового покоління цифрових валют. Основними відмінностями Bitcoin стали його децентралізація та використання технології блокчейн. Створюючи Bitcoin, планувалося спробувати побудувати цифрову грошову систему як однорангову мережу без центрального органу, призначену для обміну файлами, і саме це рішення лягло в основу криптовалюти [12].

Створення цифрової валюти потребувало створення мережі платежів, що містить рахунки, баланси та транзакції. Однією з ключових проблем, яку кожна платіжна система онлайн має вирішити, є запобігання подвійним витратам, коли одна й та ж сума витрачається двічі. У типових системах це вирішується через центральний сервер, що веде реєстр балансів. Але в децентралізованій мережі такого центрального сервера немає. Тому для вирішення цієї проблеми кожен учасник мережі повинен мати доступ до списку всіх транзакцій та мати можливість перевірити кожну з них. Це необхідно для протидії різним видам атак, включаючи подвійні витрати. Якщо вузли мережі не погоджуються навіть щодо одного балансу, це може спричинити неполадки, оскільки для належної роботи потрібен єдиний консенсус.

У централізованих системах при різних конфліктах або суперечностях рішення приймається централізованим органом. Але до створення Bitcoin мало хто вірив, що можна досягти консенсусу без центрального органу. Bitcoin був створений розробником чи групою розробників під псевдонімом Сатосі Накамото 2009 року.Протягом восьми років ретельно вивчається інформація про засновника біткоїна різними дослідниками. Але нікому з них так і не вдалося знайти реальних даних з біографії Накамото: ні про вік, ні про місце народження, ні про освіту автора. Знайти можна було лише відомості про наукові праці Накамото, з яких видно, що Накамото ідеально володіє і японською і англійською мовами [10].

31 жовтня 2008 року вийшла стаття «Bitcoin: A Peer-to-Peer Electronic Cash System». Там було описано всі можливості та технічні характеристики віртуальної валюти біткоїну. Ця робота набула гучності у світовій фінансовій системі під

назвою "білою книги" криптовалюти. До списку підозрюваних осіб було внесено американського вченого Ніка Сабо, який займався цифровими валютами в кінці 90-х, але не реалізував свій проект. Хоча сам Сабо заперечив той факт. Іншим підозрюваним став австралійський бізнесмен Крейг Райт, який сам назвав себе засновником першої криптовалюти. Він навіть опублікував багато статей. Однак жодна з них не була присвячена виключно біткоїну. І хоча люди і повірили в те, що це зробив Крейг Райт, але журналісти поставилися до цього скептично. Райт розповідав журналістам тільки те, що хотів, не відповідаючи на запитання, що змогли б підтвердити його причетність до винаходу. Без сумнівів, що бізнесмен є чудовим програмістом та власником потужного обладання для роботи з біткоїном, але йому далеко до Накамото. Райта оголосили шахраєм [25].

На засновника біткоїна на сьогодні є багато претиндентів. Але під підозру потрапляють першочергово англомовні вчені, так як людина, яка вважається японцем, врядчи буде так досконало володіти англійською мовою. Існує думка, що цим могли б займатися китайські хакери. Втім цілі даних дій залишаються загадкою. Накамото спілкувався протягом двох років з різними людьми і говорив, що створив цифрову валюту для того, щоб та не була підконтрольною певній людині, групі людей чи організації. Автор не передбачив вирішення проблеми подвійної витрати. Користувач ніколи не передасть двом іншим користувачам той самий цифровий актив. Перша транзакція буде дійсною. Друга отримає статус «ignored» [18].

Проєкт із запуском біткоїна був реалізований у 2009 році. Стан Сатоші становить $20 млрд за приблизними підрахунками. Накамото володіє кожним 12-м біткоїном. І тільки за сприяння Накамото у будь-який момент може статися дестабілізація цифрової валюти. З 2011 року ніяких нових статей геніального автора не з’являлося. Свій відхід Сатоші пояснив появою нових проектів. Але його постать і зараз вимагає відповідей на багато питань. Автор не увійшов до списку найбагатших людей за даними "Форбс", залишаючись інтригуючим міфічним генієм [26].

Станом на 2022 рік ринкова капіталізація криптовалют становила близько 1,8 трильйона доларів, більшість суми якої припадала на біткоїн та ефір, з ринковою капіталізацією приблизно 750 мільярдів доларів і 350 мільярдів доларів. Незважаючи на існування безлічі криптовалют, 20 найбільших монет складають приблизно 1,55 трильйона доларів на ринку. Значні суми грошей у криптовалютах не могли не привернути увагу зловмисників. Перша велика крадіжка сталася в лютому 2014 року, коли третя за розміром біржа біткоїнів у світі (Mt. Gox) оголосила про банкрутство через крадіжку близько 650 000 біткоїнів, оцінка яких становила тоді приблизно 380 мільйонів доларів [10].

В кінці 2021 року і на початку 2022 року відбувся найбільший злом криптовалюти, коли з біржі Ronin Network, яка дозволяла гравцям онлайн-гри Axie Infinity конвертувати токени, зароблені в грі, в криптовалюту, було викрадено 625 мільйонів доларів США в Ether (Etherum) і USDC (стейблкоїн, прив'язаний до долара США). Федеральне бюро розслідувань виявило, що за цією крадіжкою стояла група північнокорейських хакерів Lazarus. Криптовалюти викликали різні думки та обговорення. Деякі економісти висловлюють погляд, що криптовалюти можна розглядати лише як об'єкти спекуляції. З цієї точки зору, криптовалюти не є засобами обміну, оскільки їх рідко використовують для купівлі або продажу товарів та послуг; вони не є засобом збереження вартості, оскільки їхня вартість може різко коливатися з часом; і вони не є розрахунковою одиницею, оскільки дуже мало товарів та послуг оцінено в перерахунках до криптовалюти. Прихильники криптовалют зауважують, що ця технологія ще не може повністю замінити традиційні гроші. Особлива критика дісталась біткоїнам через їхнє велике споживання енергії. Висока рентабельність біткоїнів спонукала до створення багатьох великих майнінгових операцій з тисячами спеціально оптимізованих комп'ютерів, що, в свою чергу, призвело до значного споживання електроенергії (0,5 % Світової електроенергії). Захисники біткоїнів говорили про те, що криптовалюта може сприяти переходу Світу на альтернативні джерела енергії, забезпечуючи ефективне використання вітрової та сонячної енергії під час періодів низького навантаження [4].

Станом на 2022 рік лише дві країни, Сальвадор та Центральноафриканська Республіка, визнали біткоїн законним засобом платежу. Декілька інших країн, в тому числі і Китай, повністю заборонили криптовалюту через високий рівень споживання енергії мережами майнінгу та через використання криптовалюти для відмивання грошей. Понад 40 інших країн заборонили криптовалютну торгівлю, роботу бірж криптовалют та право працювати з ними банкам [4].

1.2 Форми та види криптовалют

Цифрова валюта – електронні гроші, що мають властивості звичайних (фіатних) грошей. Вона може бути як регульованою, так і нерегульованою. Цей загальний термін охоплює всі види електронних грошей, які існують в цифровому просторі. До цифрової валюти належать віртуальні валюти і криптовалюти. Іноді цифрові гроші відомі як "кіберготівка". Віртуальну валюту, яка представляє собою одну з категорій цифрової валюти. Усі віртуальні валюти є цифровими (онлайн), але не всі цифрові валюти можуть вважатися віртуальними [5].

Криптовалюта — це підкатегорія віртуальних валют, яка створена за допомогою криптографічних методів та математичних обчислень, в основному на основі технології блокчейн. Криптовалюта поєднує в собі як цифровість, так і віртуальність, оскільки існує в цифровому просторі і зашифрована криптографічними алгоритмами. Вона поширена у формі токенів та монет (включаючи DeFi-токени), де токени є активами, які існують в блокчейні. Токени створюються на існуючому блокчейні і можуть використовуватися як валюта. Монети (біткоїн, альткоїни (включаючи стейблкоїни), які можуть бути віртуальними, цифровими (або матеріальними). Монети схожі на традиційні гроші та мають свій власний блокчейн [5].

Токен – це одиниця обліку, яка представляє цифровий баланс у певному активі. Облік токенів здійснюється в блокчейні, а доступ до них здійснюється через спеціалізовані додатки з використанням схем електронного підпису. Токени можуть відрізнятися за видами, такими як акції компаній (equity tokens), утилітарні

токени (utility tokens), які відображають цінність в межах онлайн-платформи, і токени, які підкріплені реальними активами (asset-backed tokens), такі як товари або послуги (наприклад, кількість кілограмів моркви чи годин роботи далекобійників, чи вартість одного квитка в театрі). Обробка транзакцій токенів може бути централізованою (під управлінням однієї організації), або децентралізованою (під управлінням заздалегідь визначеного алгоритму). Токени також можуть бути пов'язані з реальними активами, і їх ціна може визначатися додатковими факторами.

Крім того, токени не мають власної системи блокчейн. Головна відмінність від монет полягає в тому, що токени можуть бути емітовані як централізовано, так і децентралізовано. Токени можна купувати через онлайнові торговельні сервіси (біржі і обмінники), або в особистих угодах (покупець і продавець домовляються особисто). Сам процес торгівлі токенами ідентичний процесу торгівлі криптовалютами. Крім того, утанови, що створюють токени часто вбудовують в веб-сторінки своїх проектів можливість купівлі токенів через традиційні електронні засоби платежу. У процесах передачі і зберігання токени схожі на криптовалюти. Для цього використовуються спеціальні програми-гаманці, які реалізують зберігання і обробку ключів, а також формування і підписання транзакцій. Як правило, ці програми входять в інфраструктуру платформи токенізації [4].

Токен NFT- скорочення від «non-fungible token» (невзаємозамінний токен). Це означає, що кожен NFT є унікальним і неповторюваним цифровим об'єктом, який зберігається в блокчейні. Іншими словами- це унікальні цифрові активи, що представляють право власності на певні об'єкти, такі як віртуальні квитки на концерти або рідкісні твори мистецтва. NFT зберігаються в блокчейні, що означає, що їх не можна легко змінювати, копіювати чи дублювати. Фактично, це ті ж токени, але абсолютно неповторні. Кожен токен має свою унікальність і не може бути замінений чи обмінений. Важливою особливістю є те, що NFT доступні тільки в цифровому просторі [4].

На сьогоднішній день існує кілька платформ, які надають можливість користувачам створювати власні токени, включаючи особисті. Цей процес, фактично, не є заплутаним і складним – для цього лише потрібно використовувати особистий, унікальний файл і власний криптогаманець. Коли користувач завантажує свій цифровий файл, система трансформує його в запис у блокчейні і, тим самим, створюється готовий токен. З цим токеном можна здійснювати різні дії, включаючи його розміщення на аукціонах для подальшого продажу та отримання гонорару. Також слід відзначити, що в деяких випадках кількість доступних завантажень може бути обмежена власником, що призводить до підвищення цінності NFT – адже чим менше осіб володіє ним, тим вищою є його вартість. Таким чином, навіть незалежно від кількості завантажень, відбувається виняткове розподілення гонорарів, які отримують як власник файлу, так і платформа, де було створено відповідний NFT. Якщо ж інший користувач бажає придбати цей токен, він може легко зв'язатися безпосередньо з його творцем та перерахувати кошти. Відповідно до виконаної операції, він негайно отримує унікальний сертифікат, де вказані всі деталі та блокчейн-дані. Ця інформація може бути збережена на будь-якому придатному пристрої, включаючи смартфони, ноутбуки та персональні комп'ютери. Актуальною ціною NFT є 0,018308 $ (NFT/USD) [4].

NFT – це цифрові активи, які користуються блокчейн-технологією для забезпечення їхньої унікальності та безпеки. Для NFT існують спеціалізовані маркетплейси, які створюють безпечне середовище для різних колекціонерів, щоб вони могли купувати, обмінювати та продавати свої невзаємозамінні токени на блокчейні. У травні 2014 року Кевін Маккой вперше введе в Світ NFT. Як лідер у галузі NFT-мистецтва, він зі своєю дружиною створив перший NFT під назвою "Quantum". "Quantum" – це відеоцикл, що складається з восьмикутника, заповненого колами, дугами та іншими геометричними фігурами, які мають спільний центр. У 2021 році цей історичний NFT був проданий на аукціоні за рекордну суму в 7 мільйонів доларів.

Феномен NFT зараз охопив увесь світ. Сьогодні NFT – це не просто колекційні цифрові активи, але і цінні об'єкти, які мають різноманітні застосування

як у фізичному, так і в віртуальному світі. NFT набувають все більшої популярності як засіб для художнього самовираження та інвестицій у цифровому просторі. Вони також знайшли своє застосування в іграх, де NFT стали комбінацією інвестиційного активу і корисного інструменту, який надає гравцям унікальні можливості. З ростом та розширенням світу NFT, їх корисність стане важливішою, ніж лише колекціонування зображень у форматі JPEG. Аналогічно до оцінки фізичних об'єктів мистецтва, цінність NFT в значній мірі визначається взаємодією між попитом та пропозицією. Зі зростанням попиту через рідкість, корисність та спекуляцію, ціни на NFT також підвищуються [12].

Для придбання та продажу NFT існують різні платформи та методи. Ви можете купити NFT за фіксованою ціною, взяти участь у аукціонах або придбати їх на Binance NFT. Також є різні способи продажу ваших власних NFT. Ви можете використовувати відповідний маркетплейс, рекламувати свої роботи в соціальних мережах, організовувати розіграші, проводити прямі трансляції (AMA), долучатися до NFT-спільнот на платформах спільноти, створювати власний вебсайт і співпрацювати з інфлюенсерами.

Для створення власних NFT також знадобляться кілька кроків, включаючи наявність криптовалюти для оплати комісії за карбування, наявність криптовалютного гаманця для зберігання криптовалюти, вибір блокчейну для створення невзаємозамінного токена і багато інших аспектів. Зрозуміло, що зацікавленість у невзаємозамінних токенах (NFT) призвела до великого попиту на колекціонування та мистецтво NFT. Існує кілька популярних варіантів використання NFT, включаючи:

- художні NFT: цифрові твори мистецтва, які можуть бути створені художниками та продані в формі NFT;
- колекційні NFT: представляють рідкісні або обмежені серією предмети, які можуть бути дорогоцінними для колекціонерів;
- фінансові NFT: коли деякі NFT можуть мати фінансовий характер;
- ігрові NFT: використовуються у відеоіграх як віртуальні предмети та активи;
- музичні NFT: артисти можуть випускати музичні твори у формі NFT;

- NFT реальних активів: наприклад, нерухомість, картини, прикраси тощо можуть бути представлені у вигляді NFT;
- NFT для логістики: можуть використовуватися для відстеження та управління логістичними процесами.

Більшість NFT одночасно можуть мати лише одного власника. Проте з'явилися також фракційні NFT, які дозволяють поділити один NFT на частини, що дозволяє декільком людям володіти частинами того ж NFT [4].

Біткоїн та NFT подібні за використанням блокчейн-технології, але вони відрізняються важливими аспектами. Хоча і Біткоїн, і NFT функціонують на блокчейні та користуються криптографією для забезпечення безпеки та автентичності, вони слугують різним цілям і мають відмінності. Біткоїн є взаємозамінною криптовалютою. Це означає, що кожна одиниця має однакову вартість і може бути використана для обміну. Навпаки, NFT унікальні і невзаємозамінні, і кожен має свою індивідуальну цінність. Біткоїн призначений для функції грошей та використовується для обміну та зберігання вартості. NFT використовуються для представлення унікальних цифрових активів, які можуть включати мистецтво, музику, ігрові предмети та інше. Біткоїн є взаємозамінним та може мати багатьох власників, тоді як NFT мають обмежене власництво, і кожен NFT може мати лише одного власника. Біткоїн має фінансову цінність та використовується як криптовалюта. NFT можуть мати різноманітні цінності, включаючи художню, колекційну або практичну цінність в залежності від їх змісту.

Отже, не дивлячись на спільність у використанні блокчейну, Біткоїн і NFT представляють різні види цифрових активів зі своїми властивостями та призначеннями.

Якщо підсумувати вищесказане, то можливо виділити ключові риси NFT:

- унікальність: кожен NFT має свою унікальну ідентичність, що робить його відмінним від інших токенів. Це дозволяє визначати права власності на цифрові об'єкти в інтернеті;

- неподільність: власник NFT має контроль над об'єктом, пов'язаним з токеном. Це може бути цифровий мистецький твір, аудіофайл, відео, власність в ігровому світі тощо;
- публічна реєстрація: всі NFT-транзакції реєструються в глобальному реєстрі блокчейну, що надає цим токену гарантію автентичності та неможливість підробки;
- сумісне спільне функціонування: NFT можуть бути використані в різних екосистемах, включаючи цифрові майданчики, ігри та інші онлайн-середовища;
- різноманітність застосувань: від колекціонування цифрових мистецьких творів до використання NFT у віртуальних іграх, музиці, справжній імовірності і багатьох інших сферах;
- підтвердження автентичності та походження: NFT дозволяють встановити походження і автентичність цифрових активів, що робить їх важливими для мистецтва та колекціонування.

Ця нова технологія принесла із собою ряд нових можливостей, але також викликала обговорення та питання, зокрема щодо екологічного впливу майнінгу NFT та правового статусу власності на цифрові об'єкти. Незважаючи на це, NFT залишаються важливим явищем в світі цифрових активів та мистецтва [12].

Токенізація має низку значущих переваг і можливостей, вона дозволяє торгувати активами швидше, оскільки не потрібно виконувати фізичний обмін активів або влаштовувати складні процедури їхнього перепродажу. Блокчейн, на якому базується токенізація, забезпечує високий рівень безпеки завдяки криптографічному забезпеченню і надійній обліку транзакцій. Токенізація може прибрати необхідність в посередниках, оскільки багато процесів може бути автоматизовано за допомогою смарт-контрактів на блокчейні. Це робить торгівлю більш прозорою та дешевою. Токенізація відкриває можливості для розвитку додаткових модулів, таких як: створення інвойсів, регулярні платежі та картки поповнення, що поліпшують користувацький досвід. Токени можуть бути

інтегровані у мобільні додатки та інші інтерфейси, що робить їх легко доступними для звичайних користувачів [4].

Серед ризиків токенізації є втрата або крадіжка особистих ключів, які надзвичайно важко відновити, приватність в публічних системах блокчейн. В публічних блокчейнах дані транзакцій відкриті для громадського доступу, і забезпечення повної конфіденційності може бути складною задачею. Та проблеми масштабування, децентралізовані системи блокчейну можуть стикатися з обмеженнями щодо пропускної здатності та швидкості обробки транзакцій, що обмежує їхню масштабованість.

Альткоїни та біткоїн являють собою складний цифровий продукт, який є зашифрований та має свій криптокод. Лише після обробки інформації та пройшовши певну трансформацію стає можливим отримати цифрові гроші. Біткоїн залишається найвідомішою і найбільшою криптовалютою за ринковою капіталізацією. Це глобальна однорангова електронна платіжна система, яка дозволяє користувачам здійснювати транзакції без посередників, таких як банки чи інші фінансові установи.

Платіжна система Bitcoin має кілька особливостей:

- видобуванням біткоїнів можуть займатися всі, встановивши спеціальне програмне забезпечення. Але у Bitcoin є обмежений ресурс. Його виробництво (емісія) обмежене програмним шляхом, і максимальна можлива кількість у обігу обмежена 21 мільйоном BTC;
- користувачі , укладаючи угоди один з одним, можуть минати центральний орган управління (peer-to-peer система). Біткоїн може передаватись прямо з електронного гаманця на гаманець, без посередництва банків, платіжних систем (таких як SWIFT чи Visa) або інших фінансових посередників;
- Система є децентралізованою, і копії блокчейна (історії всіх транзакцій, що були здійснені) зберігаються на різних пристроях користувачів;
- чим більше транзакцій в мережі, - тим більше комісій, і тим дорожча транзакція.

Таким чином, біткоїн управляється лише кодом, закладеним у мережу її творцем. Курс BTC залежить тільки від ринкових умов і вартість біткоїну формують самі учасники угод. Це означає, що ніхто не може контролювати всю мережу та стати подібним до центрального банку як монополіст. Саме завдяки біткоїну створився та розповсюдився термін "криптовалюта."Альткоїни представляють собою різноманітні цифрові активи, які виникли після біткоїна. На ринку криптовалют до 2022 року вони складали приблизно 40% від загальної капіталізації [12].

Запуск біткоїна та опублікування його відкритого вихідного коду в 2009 році відкрив шлях для створення тисяч інших криптовалют, які стали альтернативою біткоїну і відомі як "альткоїни." Розробники перших альткоїнів часто використовували вихідний код біткоїна як основу, вносячи невеликі зміни для створення нових криптовалют. Цей процес часто називають "форками," що походить від англійського терміну "fork," що означає "розгалуження" або "відгалуження."

Прикладом одного з перших альткоїнів є Litecoin. Він був створений як однорангова криптовалюта та глобальна платіжна мережа, яка мала бути аналогом біткоїна. Проте Litecoin мав важливу відмінність: високу пропускну здатність, завдяки використанню іншого алгоритму шифрування під назвою Script, замість SHA-256, який використовується в біткоїні [4].

На базі Litecoin було створено ще одну популярну криптовалюту, Dogecoin, про яку відомий підприємець Ілон Маск неодноразово писав у своєму Twitter. Інші альткоїни часто ставлять перед собою завдання, відмінні від завдань біткоїна, і це робить їх унікальними та цінними. Наприклад: Ethereum (ETH)- є першим в Світі програмованим блокчейном і відрізняється від біткоїна тим, що дозволяє розробникам створювати та розгортати децентралізовані програми (DApps) та смарт-контракти. Це відкриває широкий спектр можливостей для розробки різних додатків та послуг на основі блокчейну. Альткоїни можуть працювати у власних мережах та використовувати різні варіації технології розподіленого реєстру (DLT). В основному, такі мережі використовують технологію блокчейн. Однак

альтернативні варіації в базовому коді кожного протоколу роблять кожен альткоїн унікальним і призначеним для конкретних цілей. Це лише кілька прикладів альткоїнів і їхніх функцій. На ринку існує багато інших альтернативних криптовалют, які спрямовані на різні завдання та розв'язання [4].

Розглянемо один із прикладів альткоїнів – стейблкоїни, які відрізняються від більшості інших криптовалют тим, що їх курс призначений для підтримання сталої вартості, що робить їх більш придатними для використання як засобу обміну і зберігання вартості, а не лише для спекуляції. Багато стейблкоїнів забезпечені реальними активами, такими як фіатні (випущені за наказом уряду) валюти (наприклад, долар США, євро), золото або інші криптовалюти. Це дозволяє стейблкоїнам підтримувати сталу вартість, оскільки їх курс пов'язаний з цими активами. Головною метою стейблкоїнів є зменшення волатильності в порівнянні з більш традиційними криптовалютами, такими як біткоїн чи ефір. Це робить їх більш привабливими для тих, хто бажає зберігати вартість в криптовалюті без значних коливань цін. Багато стейблкоїнів емітуються централізованими установами чи компаніями, що керують їх виробництво і обіг. Це відрізняє їх від децентралізованих криптовалют, які функціонують без центральної влади. Стейблкоїни, забезпечені фіатними валютами, часто підпадають під регулювання фінансових органів та відповідають стандартам та законам, які визначені для традиційних фінансових інструментів. Стейблкоїни широко використовуються в криптоспільноті як засіб для захисту від волатильності ринку. Вони також використовуються для торгівлі на криптовалютних біржах та як основний засіб обміну у децентралізованих фінансових системах (DeFi). Сутність стейблкоїнів полягає у тому, щоб надати користувачам більшу стабільність у Світі криптовалют і дозволити їм зберігати вартість без ризику значних коливань [12].

Державні цифрові валюти (Central Bank Digital Currencies, CBDC) представляють собою віртуальні гроші, які емітує центральний банк країни. Вони відрізняються від більшості криптовалют, оскільки мають офіційний статус і підкоряються регулюванню урядом.

Ось деякі основні риси державних цифрових валют:

- централізована емісія: CBDC емітується центральним банком країни або іншою державною організацією. Це означає, що вони контролюються державними установами і підпорядковані фінансовим законам;
- прив'язка до національної валюти: більшість CBDC прив'язані до існуючої національної валюти, такої як долар, євро чи юань. Одна одиниця CBDC зазвичай має еквівалент у фіатній валюті, що надає їй стабільність;
- офіційний статус: CBDC визнаються державою як законний засіб обміну, подібно до паперової валюти;
- можливість проведення державної політики: впровадження CBDC може дати державі більший контроль над грошовою політикою, включаючи можливість здійснювати швидке стимулювання чи здержування економіки через вплив на обсяг грошової маси.

Ether, так званий Ефір (ETN), – це друга за величиною криптовалюта, яка була створена у 2015 році і використовується для функціонування програм, створених на основі блокчейн-системи Ефіріуму (Ethereum). Ефіріум (Ethereum) — це універсальна розподілена система смарт-контрактів на базі блокчейн-технології. Вона застосовується для передачі даних усередині цього сервісу. Ефір торгується на біржі так само як і традиційні долари, євро або акції, - через це його курс постійно змінюється [4].

Смарт-контракт — це написаний спеціальною мовою Solidity алгоритм, який автоматично виконується та зберігається у блокчейн-системі. Його не можливо змінити після підписання всіма сторонами. А головне цей алгоритм працює без посередників [1].

На сьогодні існує безліч криптовалют, окрім вище згаданих, найвідомішими з яких є:

- DASH (DASH). Він направлений на зручність для споживача і гнучкому, децентралізованому протоколі управління. Наприклад, користувачі Dash всього за 24 години у 2016 році затвердити збільшення розміру блоку, в той час як у спільноти біткоїнів це зайняло три роки.

- MONERO (XMR). Одна з перших переваг даної криптовалюти – підвищена анонімність. Він кожного разу автоматично засекречує вашу електронну адресу, тому не потрібно турбуватися про те, чи є якийсь слід.
- LITECOIN (LTC). У даній крипті настільки схожий код на код біткоїн, що лайткоїн може використовувати мережу розробників біткоїнів і покращувати її, не починаючи розробки з нуля. Швидкіть лайткоїну в 4 рази перевищує швидкість біткоїну.
- ZCOIN (XZC). ZCoin повністю анонімний і може зайняти місце в тій же стрічці, що і Monero.
- BLOCKNET (BLOCK). Цю криптовалюту найпростіше реалізувати для потреб ринку. Blocknet усуває ризики з боку посередників під час відправки монет для торгівлі на біржі. Ви можете забезпечити 5 000 000 блоків в сервісноді, запускати будь-які гаманці на тому ж комп'ютері, що і цей вузол, і заробляти BLOCK як комісії щоразу, коли хтось торгує валютою, яку підтримує ваш вузол.
- ETHEREUM CLASSIC (ETC). Причина низької ціни ETC, особливо в порівнянні з Ethereum (ETH). В липні 2016 року розділили блок ефіру, щоб відновити втрачені кошти інвесторів DAO (децентралізована автономна організація), відкинувши блокчейн до моменту злому. У спільноті ефіру було багато розбіжностей через незмінність ланцюжка. Частина спільноти вирішила порушити цей «закон», щоб виручити тих, хто постраждав від злому DAO, створивши ETH.
- QTUM (QTUM). Це так званий ефір для Китаю, за винятком того, що це proof-of-stake монета. Це спосіб забезпечення безпеки мережі з різким скороченням споживання електроенергії в порівнянні з системою Proof of Work, як у біткоїнів. Як і ефір, Qtum буде приймає ряд додатків, розроблених третіми сторонами.
- FACTOM (FCT) - Factom пропонує незмінні записи. Це може бути корисним для іпотечної індустрії, де обертаються трильйони доларів, для банків та аудиторської звітності, роздрібної торгівлі з величезними базами даних,

такими як Target, кіностудій з величезними каталогами фільмів, наприклад, Warner Brosерукі, архівів. Factom може змінити саму систему зберігання записів і забезпечить їх вічне існування.

- STRATIS (STRAT). Stratis –спрощує впровадження блокчейну для підприємств. Він пропонує прості і доступні рішення для розробки, тестування і розгортання власних C# блокчейн-додатків. У Stratis ведуть переговори з багатьма великими компаніями, такими як Microsoft, Jaguar, Reuters, Cashaa, AIA Group, RBC Capital Markets, Deutsche Bank і т. д.
- STEEM (STEEM). Steem - це перший токен, який дійсно використовується для того, щоб повідомлення у соціальних мережах від творців контенту, які зберігали б за собою 100% прав власності, а між власниками контенту і його шанувальниками не було б рекламодавців та інших проміжних ланок, -могли б приносити гроші в залежності від того, наскільки вони популярні.
- RIPPLE (XRP). Ripple криптовалюта- технологія розподілених реєстрів (DLT), яка є наступником SWIFT. ЇЇ токен XRP може повністю змінити спосіб відправки грошей на міжнародному рівні. В даний час міжнародні платежі займають кілька днів, а комісії величезні. Відправка грошей з однієї країни в іншу за один день –це занадто довго. XRP може передавати кошти до будь-якої точки світу за чотири секунди і дешево.
- BASIC ATTENTION TOKEN (BAT). Безкоштовний і відкритий інтернет, як ми знаємо, працює на рекламних оголошеннях, тому програми-блокатори реклами набувають все більшого поширення. BAT прагне вирішити цю проблему, створивши взаємовигідну основу між рекламодавцями і користувачами, засновану на інтернет-браузері Brave [30].

1.3 Криптовалютні біржі

Криптовалютні біржі – це це цифрові ринки, які дозволяють користувачам купувати та продавати криптовалюту (Bitcoin, Ethereum, Tether …). Binance Exchange, визнана світовим лідером у сфері торгівлі криптовалютами, володіє

найвищим обсягом торгів. На сьогодні існує великий вибір криптовалютних бірж і кожна має свої переваги в тому чи іншому аспекті. Розглянемо кілька найбільш використовуваних криптовалютних бірж: Binance, WhiteBIT, Bybit, KuCoin [13].

Найбільшою криптовалютною біржою є Binance , заснованою Чанпен Чжао, що народився у 1977 році в провінції Цзянсу, Китай. Заснована у 2017 році, Binance швидко стала лідером у світі за обсягами торгів в січні 2018 року. Компанія, хоча спочатку розташована в Китаї, змінила своє місцезнаходження та штаб-квартиру на Японію в вересні 2017 року, у зв'язку з забороною уряду Китаю щодо торгівлі криптовалютами.Стрімко розширюючи свою глобальну присутність, Binance встановила офіси в Тайвані до березня 2018 року, але через введення більш жорстких норм у Японії та Китаї, вирішила відкрити офіс на Мальті в квітні 2018 року. Додаткові стратегічні кроки були зроблені у партнерстві з урядом Бермудських островів та Мальтовою фондовою біржею для розробки платформи електронної торгівлі [13].

З метою розширення свого впливу в Європі, у 2019 році Binance анонсувала створення Binance Jersey, що є незалежною від основної Binance.com, технічна база якої розташована в Джерсі, пропонуючи пари "фіат-криптовалюта", включаючи євро та британський фунт. В січні 2019 року Binance уклав партнерство з платіжним сервісом Simplex з Ізраїлю, що дозволило користувачам придбати криптовалюту дебетовими та кредитними картками, такими як Visa та Mastercard. За додатковим розширенням глобального впливу, Binance придбала найбільший сервіс обміну криптовалют в Індії, WazirX, та запустила IEO Matic Network. Новим відзначним рішенням є припинення підтримки фіатних депозитів у російських рублях (RUB) з 15 листопада 2023 року, що було анонсовано 1 листопада 2023 року. Громадянам Росії надано час до 31 січня 2024 року, 00:00 (UTC), для виведення коштів через фіатних партнерів компанії або обміну їх на криптовалюту внутрішньобіржовими інструментами. Це рішення прийнято Binance у вересні поточного року, під тиском міжнародної громадськості у зв'язку з російським вторгненням в Україну. Біржа Binance обслуговує більш ніж 150 мільйонів користувачів у 180 країнах світу та славиться своїми низькими витратами на операції та більш ніж 350 доступними

криптовалютами, що робить її привабливим майданчиком для торгівлі Bitcoin, альткоїнів та інших віртуальних активів.

В Binance можливо:

- торгувати криптовалютами;
- здійснювати купівлю і продаж криптовалюти на Binance P2P;
- отримувати відсотки на криптовалюті, використовуючи Binance Earn;
- заробляти чи купувати нові токени у Binance Launchpad;
- працювати з NFT на маркетплейсі Binance NFT.

Binance пропонує кілька варіантів придбання криптовалют такі, як кредитні/дебетові карти, готівкові кошти або Apple Pay/Google Pay. Перед початком торгівлі слід пройти процедуру верифікації особи для облікового запису на Binance.

Для слідкування за цінами криптовалют, їхнім обсягом торгів, популярністю альткоїнів та ринковою капіталізацією використовується Каталог криптовалют Binance. Це практичний інструмент для перевірки історичних цін та обсягів торгів за останні 24 години в режимі реального часу для таких криптовалют, як Bitcoin, Ethereum, BNB та інші. Платформа Binance дозволяє торгувати сотнями криптовалют на спотових, маржинальних, ф'ючерсних ринках. Для початка торгівлі потрібно створити обліковий запис, успішно пройти верифікацію особи, придбати або внести криптовалюту та розпочати торгівлю. Крім того, користувачі можуть отримувати винагороди в понад 180 криптовалют на платформі Binance Earn. Сервіс пропонує багато цифрових активів, таких як Bitcoin, Ethereum та стейблкоїни, для заробітку та участі в програмі отримання винагород [34].

WhiteBIT — популярна українська криптовалютна біржа, яка налічує понад 2 мільйони зареєстрованих користувачів. Загальна кількість торгових пар криптовалют на платформі перевищує 450, зокрема, більше 30 пар є фіатними, тобто зв'язаними з реальними національними валютами. Розмір середньодобового обсягу торгів перевищує вражаючу позначку у $2.5 мільярда. Адміністрацію криптобіржі WhiteBIT здійснює кілька компаній, і на чолі з ними стоїть Clear White Technologies, зареєстрована в Гонконгу. Не дивлячись на те, що в Гонконгу відсутні

конкретні законодавчі акти щодо регулювання криптовалют, це не означає, що діяльність WhiteBIT не піддавалася контролю [16].

Зазначимо, що в березні 2023 року громадська організація "НОН-СТОП" висунула звинувачення на адресу біржі щодо легалізації та відмивання грошей депутатами проросійських партій, заборонених в Україні. Експерти висловлюють припущення, що Володимир Носов виступає як формальна постать, тоді як справжніми власниками біржі є проросійські депутати Дмитро Шенцев та його син Микита Шенцев. Зазначається, що ці особи вклали значні кошти в розвиток та активний маркетинговий піар WhiteBIT з метою задоволення власних комерційних інтересів, легалізації незаконно нажитих коштів та ухилення від сплати податків. На відповідь на звернення громадської організації суд вимагає від НАБУ перевірити зазначені фінансові операції, що ставить під сумнів чесність та легальність діяльності WhiteBIT [16].

Переваги та недоліки SMART стейкінгу – депонування коштів з отриманням відсотків. SMART стейкінг платформи відкриває можливість депонувати понад 60 різних криптовалют з отриманням відсотків. Важливим позитивним аспектом є те, що виплати на провідні альткоїни та біткоїн є досить конкурентними. На нашому веб-сайті зазначено, що ви можете залишити BTC, ETH та USDT з отриманням 28%, 28% та 30% річних відповідно. Це означає, що за 1 біткоїн можна отримати додатково 0,28 BTC. Щоб скористатися цією можливістю, вам потрібно або покупати криптовалюту на біржі, або використовувати ту, що вже є на вашому рахунку. Ще однією перевагою є різноманіття термінів депонування. Якщо ви не бажаєте ризикувати через волатильність ринку, у вас є можливість розмістити активи під відсоток на період від 10 до 20 днів, або навіть на місяць. Крім того, існують і довгострокові варіанти, такі як 3, 9 та 12 місяців. Однак важливим нюансом є те, що ви не можете достроково вивести кошти з плану, не втрачаючи при цьому нараховані на цей момент відсотки [16].

Сінгапурська біржа Bybit була заснована у 2018 році колишніми банкірами та експертами з фінансових і банківських послуг. Голова компанії – Бен Джоу. ByBit виділяється своєю високою продуктивністю, оскільки ядро біржі може

ефективно обробляти понад 100 тисяч транзакцій в секунду. Біржа відзначається надійністю, оскільки кошти користувачів знаходяться тільки в холодних гаманцях, а також надає багатомовну підтримку та забезпечує анонімність торгів без необхідності верифікації. Крім того, вона славиться зручним і зрозумілим в роботі веб-сайтом та володіє одними з найвищих торгових обсягів серед ключових торгових пар на криптовалютному ринку. На початку свого існування біржа спеціалізувалася виключно на торгівлі деривативами, не надаючи можливості обмінювати монети на спотовому ринку. Проте в теперішній час вона пропонує повний спектр послуг, включаючи спотовий ринок, ф'ючерси та інше [14].

Основна мета Bybit полягає в створенні інтуїтивно зрозумілого та інтелектуального торгового досвіду. Торгова система дозволяє налаштовувати рівні тейк-профіту та стоп-лосу для ефективного контролю ризиків, а також отримувати оповіщення про події, пов'язані з обраною стратегією. Більшість коштів користувачів знаходиться на холодних гаманцях, забезпечуючи їх захист від можливих хакерських атак.

Перевагами Bybit є можливість обробки до 100 000 транзакцій на секунду без будь-яких затримок завдяки потужному двигуну (надійність роботи складає 99,99%), висока ліквідність та глибина ринку забезпечують мінімальний вплив угод на цінові показники, відсутність неправомірних ліквідацій завдяки механізму подвійної ціни, вигідні умови оплати для трейдерів завдяки низьким торговим комісіям за системою мейкер-тейкер, платформа працює в багатьох країнах світу, що забезпечує її глобальну доступність та придатність для користувачів з різних регіонів, наявність зручної мобільної програми, доступної в Google Play та App Store, для трейдерів у будь-який час і місце, відсутність обов'язкової верифікації особистості забезпечує простоту реєстрації та анонімність користувачів, 24/7 робота служби підтримки, яка, за відгуками більшості клієнтів, є швидкою та корисною [14].

Слід зазначити також недоліки даної мережі, деякі користувачі висловлюють негативні відгуки, зазначаючи стягування прихованих комісій та замороження рахунків з великими сумами в криптовалюті.

KuCoin представляє собою нерегульований глобальний обмін криптовалют, що базується на Сейшельських островах, і надає свої послуги в понад 200 країнах світу. Її високий торговий об'єм та велика ліквідність роблять цю біржу однією з найефективніших за версією MarketCap у сфері криптовалют. Платформа пропонує широкий вибір понад 600 цифрових валют та понад 1 000 торгових пар. Користувачі мають можливість скористатися різноманітністю ринків, включаючи ринки спот-торгівлі, ф'ючерсів та маржинальної торгівлі, а також ринок P2P для обміну місцевими валютами [15].

Біржа KuCoin була запущена у вересні 2017 року досвідченою командою фахівців з блокчейну і криптовалют: Майклом Ганом, Еріком Доном, Джоном Лі, Топом Лан, Ліндою Лін та іншими. KuCoin, окрім відомих криптовалют, таких як Bitcoin, Ethereum, Monero, Litecoin, також пропонує свій рідний токен KuCoin (KCS). Користувачі розподіляються за рівнями в залежності від своїх балансів KCS і можуть отримувати знижки на комісію в залежності від їхніх обсягів. Зокрема, користувачі, у яких 6 чи більше токенів KCS на рахунку, мають можливість щоденно отримувати винагороди [15].

Переваги біржі:

- платформа пропонує низькі торгові комісії, які стартують від 0.1% за кожну угоду, що сприяє економії коштів для користувачів;
- з більш ніж 600 цифровими активами на платформі, користувачі мають широкі можливості для диверсифікації свого портфеля;
- платформа пропонує понад 1,000 торгових пар, що створює великий простір для торгівлі та забезпечує різноманіття в інвестиційних стратегіях;
- високий обсяг торгів та висока ліквідність гарантують ефективність та швидкість виконання угод;
- платформа дозволяє купувати криптовалюту, використовуючи дебетові та кредитні картки, що спрощує процес інвестування;
- Kucoin надає можливості стейкінгу та кредитування, що дозволяє користувачам заробляти на відсотках та розширювати свої інвестиційні можливості.

Недоліки:

- Kucoin не має ліцензії в США, що може обмежувати доступ до деяких функцій для користувачів з цієї країни;
- клієнтам з США доступні лише базові функції, що може вплинути на їхні можливості на платформі;
- біржа не є дружньою до новачків, і інтерфейс може бути відчутим складним для навігації, що може викликати труднощі для нових користувачів;
- існують обмежені можливості для депозитів у фіатній валюті, що може бути не зручним для деяких користувачів;
- користувачі повідомляють про недостатню якість підтримки клієнтів, що може впливати на рівень задоволення від користування платформою.

1.4 Блокчейн. Еволюція технології блокчейн

Блокчейн – це база даних транзакцій, яка постійно оновлюється та розповсюджується серед безлічі комп'ютерів у мережі. Блокчейн є інноваційною технологією, що дозволяє безпечно, надійно та прозоро зберігати дані за допомогою мережі комп’ютерів. Ця система баз даних використовується для проведення операцій з криптовалютою та для зберігання інформації в різних контекстах. Цифровий реєстр даних у мережі блокчейну формується через послідовно поєднані ланцюги, що містять інформацію про всі проведені операції. Кожен новий набір транзакцій, який додається, називається "блоком". Ось завдяки чому такий ланцюжок блоків було названо "блокчейн". Для кожного блоку встановлено посилання на попередній блок. Перший блок в цьому ланцюгу називається "початковим блоком" або "блоком генезису". Цей блок не має посилань на попередній і, як правило, включається в протокол як випадковий елемент. Нові блоки додаються до системи відповідно до зазначеного набору правил, встановлених протоколом, який називається протоколом консенсусу [22].

Мережа блокчейну захищена від будь-яких зовнішніх втручань завдяки організації блоків, оскільки будь-яке втручання потребувало б погодження всіх

учасників мережі. Це створює систему, що ґрунтується на взаємному обміні віртуальними грошима без посередників через блоки інформації. Кожному учаснику доступна повна історія проведених операцій. На загальнодоступних блокчейнах (наприклад Ethereum) є можливим додати нові дані, але немає можливості видаляти їх. Щоб внести зміни чи змінити інформацію в системі, потрібно було б зробити це одночасно у багатьох комп'ютерах мережі. Зробити це масово не реально, тому використовуючи блокчейни можливо говорити про їх високу безпеку [27].

Перші ідеї щодо технології блокчейн сформувалися наприкінці XX століття і належали американському фізику Вейкфілду Скотту Сторнетту та криптографу Стюарту Хаберу, які працювали в дослідницькому центрі Bellcore. Їхня робота спрямовувалася на створення криптографічно безпечного архіву, який дозволяв би зберігати записи без розкриття їхнього вмісту [9].

У 1991 році Хабер і Сторнетт опублікували в журналі своє відкриття у статті "Як поставити позначку часу на цифровий документ", присвяченій криптографії. Технологія отримала назву "блокчейн", оскільки розподілена електронна книга зберігала елементи даних у цифрових групах, які мали часові позначки і називалися блоками. Кожен блок містив буквено-цифровий код, відомий як "хеш", і підсумовував свої дані. Хеш кожного завершеного блоку також включався до наступного блоку, що робило зміну одного блоку практично неможливою без зміни всіх попередніх. Ця криптографічна система функціонувала для захисту від шахрайства.

Система використовувала криптографічно пов'язану послідовність блоків для зберігання документів із позначками часу, а в 1992 році в неї було додано "дерева Меркла", що підвищило її ефективність, дозволяючи об'єднувати кілька документів в один блок. Проте ця технологія так і не була впроваджена. Дерева Меркла впроваджуються у блокчейнах для гарантування цілісності даних та створення безпечного методу перевірки вмісту блоку. Вони служать для створення цифрових відбитків усіх даних, що містяться у блоці. Процес полягає в хешуванні кожної транзакції у блоці та подальшому створенні хеша для усіх цих хешів,

утворюючи унікальний цифровий відбиток, відомий як корінь Меркла. Цей корінь Меркла включається у заголовок кожного блоку. Якщо дані у блоці будуть змінені, зміниться і корінь Меркла, що призведе до визнання блоку недійсним. Це важливо для забезпечення безпеки збережених у блокчейні даних [22].

Дерева Меркла також використовуються для підтвердження транзакцій у мережі. Порівнюючи корінь Меркла поточного блоку з коренем Меркла попереднього блоку, вузол може переконатися, що всі транзакції, що містяться у блоку, є дійсними. Це сприяє виключенню можливості наявності шахрайських транзакцій у блокчейні. А ще дерева Меркла використовуються для зменшення обсягу блокчейну, дозволяючи вузлам запитувати з мережі лише ті дані, які їм дійсно необхідні. Кожен вузол зберігає копію усього блокчейну, але завдяки кореню Меркла може запитувати у мережі лише ту частину даних, яка йому потрібна. Це сприяє зменшенню обсягу зберіганих даних для кожного вузла і підвищує загальну ефективність блокчейну [10].

У 2004 році Гел Фінні (Гарольд Томас Фінні II) вигадав систему під назвою Reusable Proof of Work (RPoW). Система працювала шляхом отримання невзаємозамінних токенів Proof of Work на основі Hashcash (запропонована у 1997 році Адамом Беком система доказу виконання роботи) і створенні натомість токени з підписом RSA (алгоритм з відкритим ключем, придатним і для цифрового підпису, і для шифрування), які можна було передавати від особи до особи. RPoW вирішила проблему подвійної витрати, зберігаючи право власності на токени, зареєстровані на довіреному сервері, призначеному для перевірки їхньої правильності та цілісності в режимі реального часу.

31 жовтня 2008 року кілька сотень криптографічних фахівців, які були частиною закритого списку розсилки, отримали листа від невідомого автора, який називав себе Сатоші Накамото, про якого інформація вже подавалася вище. Блокчейн - це механізм обробки інформації, де рішення стосовно обробки ухвалюються на основі голосування учасників системи під час застосування протоколу консенсусу [27].

1.5 Основні поняття та складові блокчейн-технології

Блокчейн-технологія складається з різних ключових елементів, загальну характеристику яких ми опишемо нижче. Розпочнемо із консенсусу - це принцип, за яким узгоджуються дані між нодами мережі для підтвердження достовірності інформації у блоках. Алгоритми консенсусу дозволяють досягти згоди без централізованого контролю. Смартконтракт - це угода, визначена комп'ютерною програмою, , умови виконання якої вбудовані в незмінний код і записані в блокчейні. Це забезпечує незмінність та надійність угоди. Блоки - це зв'язані між собою структури даних, що містять інформацію про проведені транзакції. Вони мають посилання на попередні блоки, утворюючи ланцюжок даних. Транзакції - це дані про операції, що відбуваються між користувачами, які групуються в блоках, що утворюють послідовності. Ноди (вузли) - це комп'ютери або пристрої з програмним забезпеченням, які утримують копії блокчейн-мережі, створюють нові блоки, обробляють транзакції, передають та зберігають інформацію. Ноди грають ключову роль у підтримці мережі. Хеш-функції - криптографічні алгоритми, які перетворюють дані в рядок символів фіксованої довжини, створюючи унікальний "хеш" для кожного блока. Ці функції забезпечують захист даних від несанкціонованого доступу та змін. Криптографічні цифрові підписи, вони використовуються для підтвердження автентичності та невідмінності даних, що передаються між користувачами, забезпечуючи безпеку та конфіденційність [28].

Ці складові роблять блокчейн-технологію безпечною, недоступною для змін та втручань зовнішніх факторів і дозволяють використовувати її для збереження даних та виконання транзакцій у різних сферах життя.Технологія блокчейн може бути зрозуміла, якщо її розглядати через поняття "реєстр". Реєстр - це форма систематизації та обліку різної інформації, початково використана для комерційної діяльності в давні часи з метою фіксації та збереження інформації, особливо якщо говорити про гроші та майно. Спочатку цю інформацію записували на глиняних дощечках, а згодом використовували папірус, пергамент і папір. Однак

революційним стало впровадження комп'ютерної техніки, яка дозволила перетворювати інформацію з паперу в цифровий формат [28].

Зараз алгоритми дозволяють створювати цифрові розподілені реєстри, які мають унікальні можливості та властивості, що виходять за рамки традиційних паперових або електронних реєстрів. Технологія блокчейн визначається саме через цей контекст обліку та збереження інформації в цифровому форматі. Розподілений реєстр представляє собою базу даних, яка розділена між численними мережевими вузлами, відомими як "ноди". Кожен вузол отримує дані від інших вузлів і зберігає повну копію реєстру. Важливою характеристикою розподіленого реєстру є його децентралізація, що означає відсутність єдиного центру для зберігання та реєстрації даних. Однак інформація в усіх вузлах розподіленого реєстру повинна бути завжди валідною та актуальною, і це можливо лише завдяки досягненню консенсусу між усіма вузлами. Кожен вузол формує та записує оновлення реєстру незалежно від інших вузлів. Після цього вузли голосують за оновлення, щоб переконатися, що більшість вузлів погоджується з кінцевим варіантом. Процес досягнення згоди щодо однієї з копій реєстру відомий як "консенсус", і цей процес виконується автоматично за допомогою алгоритму консенсусу. Як тільки консенсус досягнутий, розподілений реєстр оновлюється, і остання погоджена версія реєстру зберігається в кожному вузлі [28]. Приклад загальної структури розподіленого реєстру показано на рисунку 1.1.

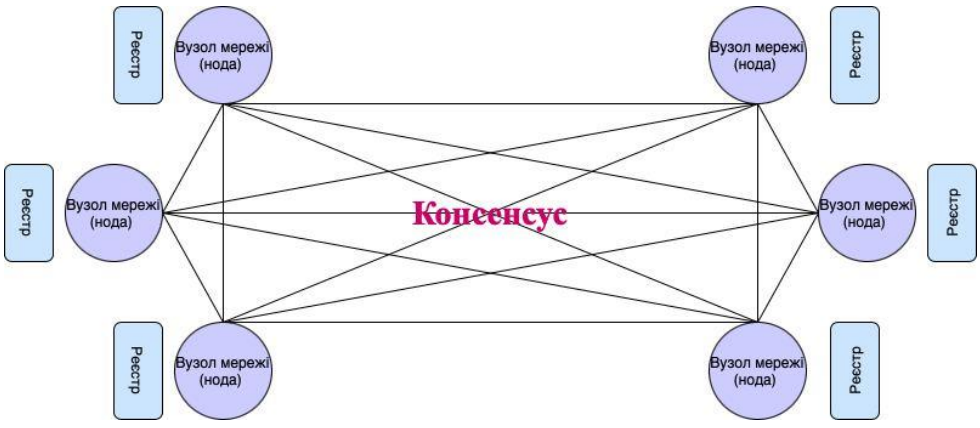

Рисунок 1.1 – Загальна структура розподіленого реєстру

Багато країн вивчають використання технології блокчейну або розподіленого реєстру. Вона може покращити ефективність обігу грошей і забезпечити більшу прозорість у фінансовій системі. Консенсус у блокчейні являється процедурою, що спільно дозволяє учасникам (зокрема, чесним учасникам) досягти єдиної думки про інформацію, яка зберігається в мережі блокчейн. Протоколами консенсусу називають набір правил, які виконують кілька функцій, забезпечують виконання процесу обробки інформації в мережі блокчейн та усувають потенційну неоднозначність у ланцюжку блоків, запобігаючи виникнення гілок у ланцюгу блокчейну (розвиток різних версій ланцюжків). перевіряють чесність учасників мережі. Розглянемо складові консенсусного протоколу:

- правила формування наступного блоку;
- правила вирішення можливих конфліктів, що виникають у мережі через непередбачені обставини або через порушення правил нечесними учасниками мережі;
- механізми стимулювання учасників мережі для підтримки функціонування локчейну та дотримання даного протоколу.

Консенсусний протокл набуває чинності лише при збереженні відповідних правил та механізму [32].

Механізм Proof of Work (PoW) гарантує, що вузол мережі (нода) може перевірити, чи справді виконані обчислення майнера (добувача криптовалюти), який додає новий блок до блокчейну. Цей процес включає в себе спробу знайти такий хеш заголовка блоку, який відповідає поточному рівню складності. Система не потребує централізованих повноважень для підтвердження правильності виконання роботи майнерами, оскільки будь-який вузол може самостійно та миттєво перевірити, чи відповідає знайдений іншим майнером блок вимогам Proof-of-Work. Інші учасники мережі можуть бути впевнені, що певний майнер насправді використовував великі обчислювальні можливості для знаходження конкретного блоку [28].

Основними недоліками протоколу PoW є:

- високі витрати: для майнінгу необхідне спеціальне обладнання, що виконує складні розрахунки. Вартість такого обладнання може бути значною, що робить процес майнінгу ресурсомістким. Це виправляється об'єднанням в пули (обєднання учасників, прибуток і витрати яких надходять до загального фонду і розподіляються між ними пропорційно) або створенням обчислювальних ферм. А розрахунки, які виконуються під час майнінгу, можуть бути марними;
- майнери постійно створюють нові блоки, витрачаючи значну кількість енергії. Однак розрахунки, які вони проводять, ніяк не використовуються в інших галузях. Вони мають єдину мету - забезпечити надійність мережі і не можуть бути використані для практичних цілей у бізнесі, науці чи інших сферах;
- треба також враховувати атаку 50%, що також відома як атака більшості. Це ситуація, коли користувач або група користувачів контролюють більшість видобувальних потужностей. Це дає їм достатньо "сили" для маніпулювання подіями в мережі. Хоча атаку 50% можна спробувати із меншою кількістю видобувальних потужностей, шанси на успіх значно знижуються. Ця атака ускладнює рівноправну участь у процесі, оскільки майнери, які контролюють більшість, отримують винагороду та обмежують можливість іншим брати активну участь;
- повільна швидкість роботи.

Найвідомішим таким протоколом можна вважати повільний, але надійний протокол узгодження Proof-of-Work криптовалюти Bitcoin.

Розглянемо поняття Proof-of-Stake (PoS) - це термін, що перекладається як "доказ володіння часткою". Цей алгоритм працює на принципі, коли мережа надає довіру валідатору, який має значну суму відповідної місцевої валюти. Чим більшу частку має валідатор (stake) в загальній сумі, тим вищі його шанси на генерацію наступного блоку і, відповідно, отримання нагороди. У протоколі Proof-of-Work (PoW) нагороду отримують учасники, які вирішують криптографічні завдання для перевірки транзакцій та створення нових блоків. У блокчейнах, що використовують

PoS (наприклад, Ethereum), значення голосів кожного валідатора залежить від розміру його депозиту (частки) [31].

Значні переваги PoS включають в себе порівняно високу швидкість та енергоефективність. Замість того, щоб конкурувати з іншими, майнери мережі розміщують свої криптоактиви в спеціальному депозиті і чекають на випадкове обрання для виконання функції валідації блокчейну, схоже на те, як коли клієнт кладе гроші в ломбард та чекає на результати.

Переваги Proof-of-Stake (PoS) у порівнянні з Proof-of-Work (PoW):

- немає необхідності великих обсягів електроенергії для забезпечення функціонування блокчейну;
- дякуючи відсутності високого споживання електроенергії, кількість монет, що виділяється для стимулювання майнерів, може бути значно меншою;
- порівняно з PoW, PoS має вищу швидкодію;
- існує можливість застосування економічних санкцій, що робить виконання різноманітних форм атаки на 50% набагато витратнішими, ніж у випадку Proof-of-Work [32].

Смартконтракт - це угода, визначена комп'ютерною програмою, яка працює автономно. Умови виконання угоди вбудовані в незмінний код і записані в блокчейні, забезпечуючи незмінність та надійність угоди. Однією з ключових переваг смартконтрактів порівняно з традиційними угодами є їхнє одночасне виконання та відсутність потреби в довірі між сторонами. Це сприяє оптимізації витрат ресурсів, економії грошей і часу, та надає потужний інструмент для реалізації різноманітних сценаріїв використання [22].

Традиційно контракт визначається як угода між двома або більше сторонами, яка передбачає обмін обіцянками та/або послугами. Часто ці угоди складаються з ряду складових частин. Наприклад, одна обіцянка, така як грошовий платіж, може бути обмінена на іншу обіцянку або послугу, або ж одна послуга може бути обмінена на іншу послугу. В контрактах можуть бути передбачені умови, за яких вони втрачають чинність, та наводитись положення, які регулюють умови обміну, вказуватись терміни виконання. Завдяки цим нюансам, деякі із найпоширеніших

контрактів, такі як угоди про кредитування та працевлаштування, можуть бути досить тривалими та деталізованими. Це важливий механізм, що регулює різноманітні сфери життя і бізнесу, але за останні роки з'явилися інноваційні способи створення та виконання контрактів, зокрема через використання смартконтрактів на блокчейні Ethereum [19].

У смартконтрактах термін "смарт" походить від англійського слова "smart," що означає "розумний." Це вказує на те, що такі контракти виконуються автоматично за допомогою комп'ютерного програмного коду, і вони не обмежені фізичними формами, які ми звичайно асоціюємо із контрактами, такими як паперові документи. Назва "смартконтракт" вже не є новою в 2020-х роках. Але слід зауважити, що вона була вперше запропонована в 1990-х роках юристом і комп'ютерним фахівцем Ніком Сабо. Він був одним з перших прихильників криптовалют та вперше впровадив ідею використання таких контрактів, які автоматизують та спрощують процеси угод, використовуючи технологію блокчейн і програмування.У смартконтрактах обіцянки формулюються у вигляді умов типу "якщо-тоді," які вже давно є стандартом в комп'ютерному програмуванні. Цей принцип схожий на роботу торгового автомата, що був використаний Ніком Сабо для ілюстрації смартконтрактів. Наприклад, коли ви вставляєте гроші в торговий автомат, він автоматично видає вам товар. У випадку смартконтрактів, всі умови угоди заздалегідь визначені в програмному коді і виконуються автономно, без впливу зовнішніх факторів (людських втручань) [22].

Смартконтракти діють на тих самих принципах і представляють собою невід'ємну частину технології блокчейну. Смартконтракти BTC розроблені для використання в мережі Bitcoin та встановлюють конкретні правила для проведення транзакцій, які реєструються в глобальному реєстрі. Смартконтракти Ethereum спеціально створені для підтримки інших смартконтрактів, які також називаються децентралізованими програмами. Ці програми розроблені мовами програмування Solidity і Vyper, які були спеціально створені для створення контрактів і працюють на власних блокчейн-платформах Ethereum.

Смартконтракти мають свої обмеження:

- функціональність смартконтракту обмежена тим, що заздалегідь визначено в його коді. Не можливо рахувати в структурі смартконтракту суб’єктивну думку та зробити його гнучким;
- якщо у коді виявляються помилки або якісь неточності, внесення змін у смартконтракт вимагає значних зусиль та консенсусної підтримки від спільноти та вузлів мережі;
- для внесення реальних даних в блокчейн, які надаються третіми сторонами, таких як вартість долара США, ціна акцій або місцезнаходження товару, потрібно використовувати технології оракулів (обєкти, які отримують та захищають зовнішні дані для блокчейнів, дозволяючи взаємодіяти із зовнішніми системами) які, на приклад, представлені ланцюгами, такими як Chainlink або Band Protocol.

Блокчейн представляє собою послідовність блоків, які об'єднані у хронологічному порядку та захищені криптографічними методами. Кожен блок має свій унікальний хеш-код, який обчислюється на основі вмісту попереднього блоку, і містить корисне навантаження (рис 1.2)

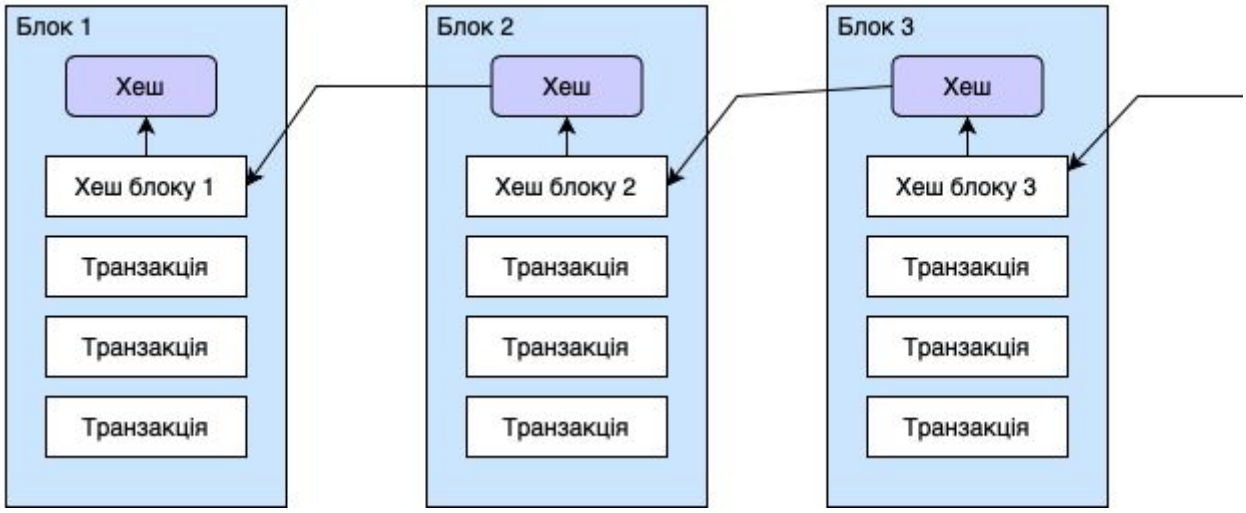

Рисунок 1.2 – Приклад загальної структури та організації блоків

Корисне навантаження може включати різноманітну інформацію, таку як дані про транзакції, операції, укладені договори, відомості про фізичних осіб, суб'єктів підприємницької діяльності, майно і багато іншого. Це навантаження робить

технологію блокчейн корисною для широкого спектра застосувань і сфер, оскільки дозволяє зберігати інформацію в безпечному та незмінному форматі [19].

Важливою особливістю блокчейну є його незмінність та відсутність централізованих контролерів. Дані, розміщені в блоках, не можуть бути вилучені або відредаговані, і кожен учасник мережі має можливість перевірити історію даних від початку до поточного стана. Ця технологія є так званим реєстром записів. Вона знайшла застосування в різних сферах, де важлива надійність, прозорість та безпека зберігання даних. Усі операції фінансових транзакцій зберігаються в блокчейні. Цей реєстр відкритий, що спрощує перевірку статусу фінансової операції шляхом зазначення хешу транзакції чи адреси криптогаманця. Проте блокчейн дозволяє переглядати лише зашифровані дані, не розкриваючи особистої інформації щодо відправника та отримувача переказу [19].

Залежно від типу активу, який потрібно відслідковувати, використовується відповідний веб-сервіс для перегляду блоків. Ці сервіси дозволяють перевірити статус транзакції, оглянути стан мережі, дізнатися актуальний курс цифрових активів та вартість комісій за операції. Кожна мережа блокчейнів стягує комісію за здійснення транзакцій, проте розмір цієї комісії може значно коливатися від однієї мережі до іншої. При підписанні транзакції учасник згоден не лише на зазначений переказ активу, а й на додатковий збір — плату за використання сервісів блокчейну. Розмір цієї комісії встановлюється самою мережею і може змінюватися в залежності від обсягу операцій в ній. Підтвердження транзакції є обов'язковим для запобігання подвійного списання та повторного використання тих самих активів. Щоб транзакція стала остаточною і підтвердженою, вона повинна бути включена в блок. Проте час на включення транзакції в блок може варіюватися залежно від конкретної мережі блокчейнів. Кількість транзакцій, яку може обробити блокчейн за секунду, відрізняється в кожній мережі. Біткоїн обробляє близько 7 операцій за секунду, а Ethereum — до 25.

Термін "хеш" (HASH) має своє коріння в англійському слові "hash", яке вживається для опису змішування. Це достатньо точно передає сутність цього терміну. Також часто використовується термін "хешування", який походить від

англійського "hashing" (розрубання, кришення, змішування та інше). Цей термін з'явився серед фахівців з обробки масивів даних у середині минулого століття. Хеш-функція дозволяла зведення будь-якого масиву даних до встановленої довжини. Наприклад, якщо поділити будь-яке число (незалежно від його довжини) декілька разів на те саме просте число, то залишок від цього поділу можна назвати хешем. Для різних вхідних чисел залишок від поділу (цифри після коми) буде відрізнятися. Хешування є частиною процесу генерації певного виводу з різноманітних вхідних даних різного розміру. Це досягається за допомогою математичних формул, також відомих як хеш-функції (реалізовані у вигляді алгоритмів хешування). Не всі хеш-функції призначені для криптографії, а лише ті, які спеціально розроблені для цієї мети, так звані криптографічні хеш-функції, що лежать в основі криптовалют. Ці функції забезпечують високий рівень цілісності даних та безпеку у блокчейнах та інших розподілених системах [29].

Наглядний приклад хешу зображено на рисунку 1.3

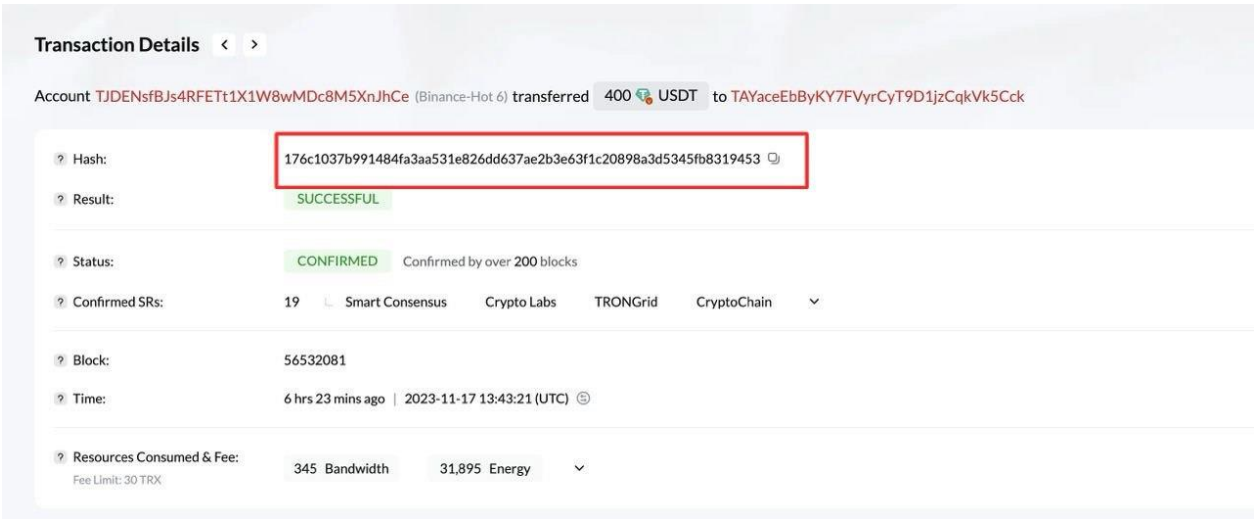

Рисунок 1.3 – Приклад хешу

Ноди (з латин. Вузли) – це точки, які є центрами зв’язку для різних мережевих завдань. Ноди виконують ключову роль у блокчейні, адже саме тут створюються, перевіряються та підтверджуються транзакції та блоки, забезпечується безпека роботи мережі. Якщо говорити простіше, то це комп’ютери, що підключені до певної мережі, наприклад, мережі Біткоїн, що забезпечують її функціонування.У

власників цифрових монет обладнання, яке вони використовують, є мережевим вузлом. Винятком є холдери, які користуються паперовим гаманцем або апаратним сейфом, проте це стосується тільки володіння криптовалютою до тих пір, поки вони не вирішать взяти її у використання [6].

Вебгаманці, які працюють через браузер, підключаються до віддаленого мережевого вузла і виконують роль передавача даних. Кожен майнер також є вузлом, але не кожен мережевий вузол є майнером. Усі мережеві вузли взаємодіють між собою за допомогою протоколу peer-to-peer (P2P). Цей вид звязку дозволяє вузлам обмінюватися інформацією про компоненти мережі та транзакції, що циркулюють в системі криптовалюти. Важливо відзначити, що не кожен вузол містить повний обсяг інформації щодо конкретного блокчейну. Для більш детального розуміння цього питання розглянемо різновиди вузлів. Залежно від того, з якими цілями створюються та використовуються ноди, який обсяг інформації містять, ноди Біткоїна поділяються на звичайні ноди та майстерноди. Звичайні ноди в свою чергу діляться на повні ноди та полегшені ноди. Повний вузол, відомий як Full Node, представляє собою вузол, який зберігає повну копію всього блокчейна, включаючи інформацію про всі записи та транзакції, які виникають на основі протоколу консенсусу. Наприклад, для участі в мережі біткоїну повна нода повинна завантажити та зберігати всі блоки у ланцюгу блоків BTC [6].

Повна нода постійно синхронізується з мережею, щоб отримувати оновлення та записувати нові блоки, що додаються до блокчейну. Саме повні вузли утворюють незамінну основу для правильної роботи блокчейн-мережі, перевіряючи достовірність даних і забезпечуючи безпеку мережі. Полегшені ноди, на відміну від повних, не мають можливості самостійно перевіряти правильність транзакцій та блоків. Вони завантажують лише заголовки блоків і можуть лише перевірити, чи міститься певна транзакція в конкретному блоці. Іншими словами, полегшені вузли покладаються на повні вузли для валідації даних, зокрема на їхню інформацію та можливості валідації. Це робить їх зручними для тих користувачів,

які не бажають або не можуть завантажити весь обсяг блокчейну та виконувати повні функції повних вузлів.

Майстерноди, присутні в окремих блокчейнах, виконують додаткові завдання та отримують винагороду за свою діяльність. Вони вимагають від користувачів завантажити весь блокчейн і встановити спеціальне програмне забезпечення, щоб стати майстернодою. Зазвичай, майстерноди виконують такі функції, як забезпечення додаткової безпеки та участь у процесах прийняття рішень у мережі. Щоб стати майстернодою, користувач повинен виконувати специфічні вимоги, такі як утримання певної кількості монет у гаманці та постійний онлайн-статус. Майстерноди здійснюють певні дії, такі як обробка транзакцій, підтримка мережевої безпеки, вирішення складних завдань чи участь у голосуванні за зміни в блокчейні. За свою активність вони отримують винагороду в криптовалюті, яка працює на даному блокчейні. Майстер-ноди грають важливу роль в роботі блокчейн-мережі та допомагають забезпечити її стійкість та ефективність.

У мережі Біткоїн не передбачено винагороди для власників повних вузлів (нод), і їхня робота полягає у підтримці та обслуговуванні мережі, забезпеченні достовірності та перевірці транзакцій, але вони не мають можливості заробити безпосередньо через майнинг. Але ж ноди не завжди створюються для отримання прибутку. Це підвищує стабільність роботи та безпеку всього ланцюжка. Важко «обдурити» мережу, якщо є багато нод. Окрім того, ті, хто проводить постійно транзакції, покладаються більше на себе, ніж на інших, - для цього і запускають власні ноди. Повні ноди можуть також брати участь у голосуванні щодо розвитку мережі (так звані хардфорки, софтворки). Інвестування виключно в токени з реальною вартістю - це давно не цікаво. Потрібно навчитися купувати і зберігати монети з мінливим курсом, не відштовхуючись від тижневого тренду, а розраховуючи на довгострокову перспективу.

Добування криптовалюти, також відоме як криптомайнінг, представляє собою процес підтримки економіки біткоїнів. Під час криптомайнингу комп'ютери приєднуються до мережі біткоїн та здійснюють перевірку та схвалення транзакцій.

Однак з розвитком криптовалют криптомайнинг став суттєвою галузю. Персональні та домашні комп'ютери більше не мають достатньої потужності для обробки величезної кількості транзакцій. Тому процес криптомайнингу вимагає величезних обсягів енергії для живлення високоефективних комп'ютерів, необхідних для схвалення транзакцій з криптовалютою [8].

Під час використання стейкингу, ми фактично утримуємо свої криптовалютні кошти на наших гаманцях для підтримки операцій в блокчейн-мережі. Це включає перевірку транзакцій та захист мережі. У відповідь на це, отримуємо винагороду, яка часто видається у вигляді додаткових криптовалютних монет. Винагорода за стейкинг є стимулом для учасників, які блокують свої криптовалютні активи для підтримки роботи блокчейн-мережі. Ця винагорода може бути фіксованою сумою криптовалюти або відсотком, який обчислюється в залежності від обсягу криптовалютних активів і тривалості їх блокування.
Важливо відзначити, що винагороди за стейкинг можуть суттєво відрізнятися у різних блокчейн-мережах [6].

Валідатори є активними учасниками мережі, що керують вузлами, перевіряють транзакції та створюють нові блоки в блокчейні. За свою активність вони отримують винагороду. Ці учасники мережі мають високий технічний рівень та готовність інвестувати у необхідне обладнання та електроенергію. Кожна мережа блокчейн має свої вимоги до отримання статусу валідатора. Делегатори представляють собою учасників, які, якщо у них немає достатніх ресурсів або технічних знань для статуса валідатора, можуть активно брати участь у стейкингу як делегатори. Вони "делегують" свої права валідатору, вкладаючи свої монети в стейкинг відповідного валідатора. Далі валідатор виконує технічну роботу, а делегатор отримує частину винагороди за стейкинг. Механізм делегування, у тому числі розподіл винагороди між делегаторами та валідаторами, залежить від правил конкретної блокчейн-мережі. Для користування криптовалютами необхідний криптовалютний гаманець. Гаманці можуть бути програмними, хмарними послугами або зберігатися на нашому комп'ютері чи мобільному пристрої. Гаманці – це інструмент, який дозволяє нам зберігати наші шифровані ключі, які

підтверджують нашу ідентичність та вказують на нашу криптовалюту. Криптовалюта може бути збережена на онлайн-біржах, таких як Coinbase і PayPal, або на апаратних гаманцях, таких як Trezor і Ledger, які призначені для безпечного зберігання криптотокенів. Гаманці можуть бути "гарячими", коли користувачі підключені до Інтернету та мають легкий доступ до своїх криптотокенів, або "холодними", коли криптотокени зашифровані на гаманцях із закритими ключами, паролі яких не зберігаються на підключених до Інтернету комп'ютерах [11].

Біткоїн використовує криптографію з відкритим ключем, в якій користувачі мають відкритий ключ, який доступний всім для перегляда, і закритий ключ, відомий лише їхнім комп'ютерам. Під час транзакції користувачі, які отримують біткоїни, надсилають свої відкриті ключі користувачам, які передають біткоїни. Користувачі, які відправляють монети, підписують свої приватні ключі, і транзакція подається через мережу Біткоїн. Щоб уникнути подвійного витрачання біткоїна, інформація про час та суму кожної транзакції реєструється в файлі ланцюга блоків, який знаходиться на кожному вузлі мережі. Ідентичність користувачів залишається відносно анонімною, але будь-хто може перевірити, що певні біткоїни перевелися. Транзакції групуються в блоки, які утворюють послідовний ланцюг, відомий як блокчейн. Додавання блоків до ланцюга вимагає математичного процесу, що робить це дуже важким завданням для окремих користувачів [8].

Технологія блокчейн, на якій ґрунтується біткоїн, викликала значний інтерес до біткоїна, як платіжного засобу торгівлі без центрального органа. Користувачі запускають біткоїн-клієнт на своїх комп'ютерах, створюючи нові біткоїни. Цей клієнт фактично "видобуває" біткоїни, вирішуючи складні математичні завдання в блоках, які отримують всі користувачі мережі біткоїн. Складність цих завдань поягає у тому, що в середньому кожні шість годин вони вирішуються, не залежно від кількості майнерів. Але користувач отримує певну кількість біткоїнів, якщо вирішує завдання у блоці. Процес майнингу біткоїнів гарантує обмеження їх пропозиції та забезпечення постійного приросту. Приблизно кожні чотири роки

кількість біткоїнів, що видобуваються в блоці, зменшується вдвічі, і максимально можлива кількість біткоїнів складає трохи менше ніж 21 мільйони [11].

Станом на початок 2022 року вже було видобуто понад 19 мільйонів біткоїнів, і передбачається, що максимальна їх кількість буде досягнута приблизно в 2140 році. Метод, який використовується біткоїном для додавання нових блоків до блокчейну через обчислювальну потужність користувачів, називається Proof of Work (доказом роботи). Його використовують більшість криптовалют. Існує інший підхід, відомий як Proof of Stake (доказ частки), в якому можливість підтвердити блок базується на вже наявному обсязі користувача в криптовалюті. Proof of Work поступається Proof of Stake, оскільки він вимагає значно більше енергії. Наприклад, Ether (Ethereum), друга найпопулярніша криптовалюта після біткоїна, вже давно прагнула перейти з Proof of Work на Proof of Stake. Web 3, також відомий як Web 3.0, представляє інноваційну фазу Інтернету, яка базується на блокчейн-технології та інтегрує ключові принципи, такі як децентралізація та токенізація економіки. Інтернет пройшов еволюцію від Web 1.0, який був обмежений переважно читанням, до Web 2.0, що став більш взаємодійною та спільнотно-орієнтованою платформою. Зараз ми спостерігаємо перехід до нового етапу в розвитку мережі - Web 3.0, також відомого як Web3, у сфері цифрових активів [21].

Web3 обіцяє надати індивідам змогу володіти цифровими активами, здійснювати безперешкодні транракції в Інтернеті та мати більший контроль над власними особистими даними. Технологія блокчейн ґрунтується на кількох ключових принципах, які визнаються основними перевагами цієї технології:

1) децентралізація: блокчейн є розподіленим реєстром, і він залишатиметься активним, доки існують активні мережеві вузли;
2) публічний доступ: усі учасники мережі мають доступ до історії транзакцій, і ніхто не має повного контролю над нею;
3) відсутність ієрархії: в мережі блокчейн немає централізованих органів, і вся система базується на взаємодії рівноправних мережевих вузлів;

4) захищеність та прозорість: блокчейн поєднує в собі високий рівень шифрування для захищеності даних та абсолютну прозорість, оскільки інформація про операції відкрита і доступна для перевірки;
5) незмінність даних: дані в блокчейні не можуть бути видалені або змінені, оскільки вони підтверджуються багатьма мережевими вузлами;
6) прозорість: технологія блокчейн забезпечує абсолютну прозорість, оскільки будь-хто може перевірити вірогідність операцій;
7) довірча система: блокчейн є довірчою системою, оскільки транзакції здійснюються безпосередньо між учасниками, підтверджуються мережевими вузлами та не потребують посередників. Це призводить до зменшення вартості транзакцій, швидкості проведення та відсутності потреби в довірі до централізованих організацій. На основі природи та характеристик технології блокчейн можна зробити висновок, що ця технологія володіє найвищим рівнем збереженості, обліку, передавання та ідентифікації даних. Це робить блокчейн вельми популярним та перспективним інструментом у багатьох галузях.

Блокчейн та криптовалютні системи вже розробляють продукти, що відповідають цій концепції. Наприклад, користувачі можуть проводити безпосередні платежі (peer-to-peer) та колекціонувати цифрові активи за допомогою криптогаманців. Багато блокчейн-проєктів мають децентралізовану структуру та дозволяють всім використовувати їхні сервіси [19].

1.6 Класифікація блокчейнів

Поділ блокчейнів на групи, такі як публічні та приватні, базується на ступені доступності інформації для учасників системи. Ступінь відкритості блокчейну може бути обумовлений різними факторами. Перший ключовий фактор, який визначає ступінь публічності блокчейну, – це доступність вихідного коду протоколу. Публічні блокчейни, зазвичай, мають відкритий вихідний код від самого початку розробки, і зміни в ньому публікуються на популярних інтернет-

ресурсах, таких як GitHub. У випадку блокчейнів, які призначені для корпоративних потреб (приватні блокчейни), можливі обидва варіанти - відкритий та закритий вихідний код. Якщо розглядати розробки блокчейну в контексті їхнього використання в державному секторі, можна зауважити, що на сьогодні кількість таких розробок і застосувань у реальних процесах є вкрай обмеженою. Тому не дивно, що більшість блокчейнів, призначених для державного сектора, також будуть мати закритий (приватний) характер [9].

Другим і найважливішим показником є можливість будь-якого користувача приєднуватися до мережі без необхідності отримувати дозвіл чи дозволи. Це саме те, що визначає головну різницю між публічним і приватним блокчейном. Багато відомих блокчейнів на сьогоднішній день є публічними - для того, щоб приєднатися до них, досить завантажити сумісний клієнтський програмний додаток і налагодити зв'язок з іншими рівноправними вузлами мережі. Для активної участі в роботі блокчейн-мережі, зокрема, для перевірки та ретрансляції транзакцій інших користувачів або для створення нових блоків, необхідно встановити та запустити повнофункціональний клієнтський програмний додаток. У деяких випадках може бути достатньо клієнтського програмного додатка з обмеженими можливостями. У публічних блокчейнах, рівень участі користувача завжди визначається ним самостійно та залежить від його власних ресурсів (фінансових чи обчислювальних) [11].

Важливою рисою публічних блокчейнів є і те, що ніхто не може відокремити користувача від розподіленої мережі, оскільки всі учасники публічного блокчейну мають рівні права. Лише інколи інші користувачі можуть блокувати чи ігнорувати користувача, який розсилає некоректні транзакції або намагається передати інформацію, що не відповідає протоколу. Такі дії мають саморегулювальний характер і не встановлюються на рівні протоколу. У приватних блокчейнах, можливість підключення чи відокремлення нових користувачів можуть контролювати певні довірені вузли або групи вузлів, які мають вищий рівень повноважень порівняно з іншими користувачами.

Приватними блокчейнами являються ієрархічні структури, які складаються з двох чи більше рівнів. Пари ключів, які надають доступ до системи, видаються спеціальними адміністративними вузлами і, за потреби, можуть бути відкликані. Це означає, що приватні блокчейни не реалізують в повній мірі головні принципи технології блокчейн, такі як децентралізація та рівноправність учасників. Це може бути суттєвим рішенням для корпоративних систем, оскільки дозволяє керувати доступом та забезпечувати вищий рівень безпеки [9].

За рівнем управління блокчейни можна поділити на чотири групи:

1) Публічні децентралізовані блокчейни. Це блокчейни, в яких всі учасники є рівноправними та залишаються анонімними, і консенсус досягається через голосування вузлів. Вони дозволяють всім бажаючим вільно брати участь у мережі без контроля ззовні. Ці блокчейни є популярними серед користувачів, оскільки будь-яка людина, що має доступ до інтернету, може стати учасником блокчейн-мережі.
2) Публічні блокчейни з делегованим управлінням. Це публічні блокчейни, де використовується система делегованого управління, в якій обраними представникам чи делегатам надається право приймати рішення та здійснювати управління мережею. Це може покращити швидкість та ефективність мережі, але залишає питання щодо централізації.
3) Приватні контрольовані блокчейни. Це приватні блокчейни, які керуються обмеженим колом учасників чи однією організацією. Вони надають більший контроль та конфіденційність, але не досягають рівноправності та децентралізації публічних блокчейнів. Такі блокчейни використовуються приватними підприємцями для своїх цілей: управління ланцюгом постачання, обміну даними чи контролю за фінансовими операціями.
4) Державні блокчейни. Це блокчейни, які контролюються державними органами або урядами. Вони можуть використовуватися для групи публічних послуг та регулювання відомостей, але можуть викликати питання щодо приватності та цензури.

Ця класифікація допомагає краще розуміти різноманітність блокчейнів і їхнє застосування в різних галузях. Очевидно, що повна децентралізація в саморегульованих мережах, точніше кажучи, стихійно регульованих, практично неможлива на практиці. Всі публічні блокчейни мають однорівневу структуру, тому, рано чи пізно, стикаються з певною формою централізації. У зв'язку з цим було зроблено спроби впровадження елементів централізації з метою поліпшення управління та інших показників блокчейну. Ця спроба призвела до появи публічних блокчейнів із дворівневою структурою в 2015 році, де певні вузли мали розширені повноваження. Саме наявність двох і більше рівнів управління в мережі блокчейн з різними рівнями повноважень для кожного рівня є ключовою рисою публічних блокчейнів із делегованим управлінням [11].

Приватні контрольовані (корпоративні) блокчейни представляють собою технологічні рішення, спеціально розроблені для корпоративних потреб. У таких систем кожен вузол має заздалегідь призначений рівень доступу, і, на відміну від публічних блокчейнів, дані не завжди є загальнодоступними навіть для читання. Управління в таких блокчейнах здійснюється за допомогою спеціальних вузлів, які мають підвищені повноваження. Ці вузли відповідають за політику розповсюдження даних та ідентифікацію користувачів і засвідчують внесення даних до блокчейну. Розподілені реєстри для державного застосування в цілому подібні до приватних блокчейнів і також потребують контрольованого доступу до інформації. Проте у державних відомств є особливі вимоги до блокчейну, зокрема, максимальний рівень незмінюваності вже доданої інформації та контроль над додаванням нових даних. В той же час інформація, яка вже міститься у державному блокчейні, у багатьох випадках може бути публічною, оскільки державні органи прагнуть до підвищення прозорості своєї роботи. Отже, можна сказати, що державні блокчейни є окремим випадком корпоративних блокчейнів зі своїми специфічними особливостями, тому вони належать до окремої категорії [8].

Класифікація блокчейну, яка базується на рівні доступу до інформації, може бути подана у формі дворівневої структури, де перший рівень визначає ступінь

доступності для публічності, а другий рівень стосується управління блокчейном. Цю структуру можна ілюструвати графічно, як показано на рисунку 1.4.

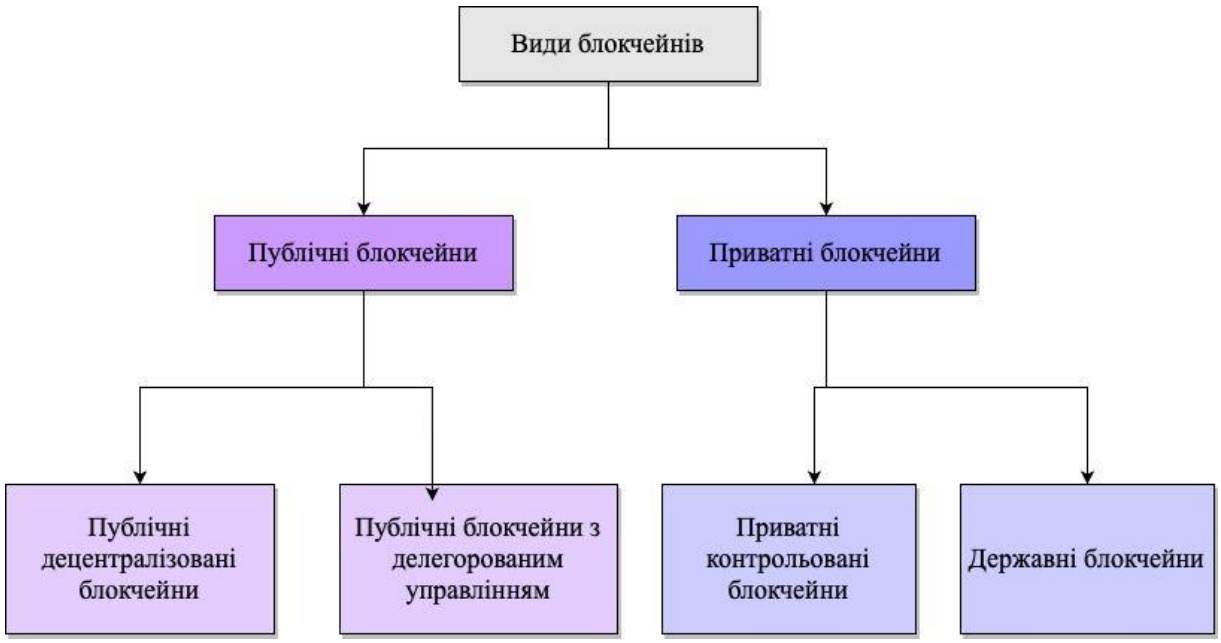

Рисунок 1.4 – Види блокчейнів

Технологія блокчейн об'єднує кілька концептуально різних ідей, включаючи розподілені реєстри для зберігання даних, алгоритми консенсусу та криптографічні механізми для захисту даних.

Основна ідея технології блокчейн полягає в тому, що дані зберігаються без залежності від централізованого сервера або групи серверів. Технологія формує послідовний список записів, які називаються блоками. Кожен блок містить позначку часу та унікальний ідентифікатор (хеш) попереднього блоку. Це "пов'язує" блоки даних, унеможливлюючи зміну вже сформованих блоків без впливу на всю послідовність блоків [33].

1.7 Блокчейн-платформа Ethereum

Існує кілька різних блокчейн-платформ, які варто розглянути. Ethereum – це децентралізована блокчейн-платформа з відкритим вихідним кодом, яка працює завдяки своїй власній криптовалюті Ether (ETH). Ethereum став відомим завдяки смарт-контрактам, які дозволяють розробникам створювати різноманітні

децентралізовані фінансові послуги та додатки. BNB Chain (абревіатура від Build'N Build) будується і розширюється з акцентом на децентралізації. BNB Chain спрямована на підвищення функціональної сумісності та розвиток базової інфраструктури "світового паралельного віртуального середовища", що є кроком вперед у недавніх зусиллях Binance щодо розбудови MetaFi. Polygon – платформа спеціально адаптована для екосистеми Ethereum. Polygon пропонує розробникам платформу для створення блокчейн-мереж, сумісних з Ethereum, та рішення для масштабування, які допомагають покращити продуктивність та швидкість обробки транзакцій [1].

Кожна з цих платформ має свої особливості та застосування, і їх вибір залежить від конкретних потреб та завдань проекту. Розглянемо детальніше відомий блокчейн Ethereum. Блокчейн Ethereum був запущений Віталіком Бутеріним у 2015 році, і його основною криптовалютою є Ether (ETH). На сьогоднішній день Ethereum є другою за ринковою капіталізацією криптовалютою і відомий своєю активною роллю в розвитку NFT (невзаємозамінних токенів), Web3 і DeFi (децентралізованих фінансів) [4].

Важливою частиною блокчейну Ethereum є "основна мережа", яка використовується користувачами для здійснення транзакцій та взаємодії з різними децентралізованими додатками. Однак у грудні 2020 року розробники Ethereum запустили нову мережу, відому як "ланцюжок маяків". Цей ланцюжок маяків фактично став фундаментом для нового Ethereum та вніс істотний внесок у покращення масштабованості та продуктивності мережі [1].

У вересні стався переломний момент для криптоіндустрії — Ethereum Merge (злиття). Злиття означає перехід із моделі Proof-of-Work (PoW) на модель Proof-of-Stake (POS), що змінює майбутнє Ethereum та всього інвестування. Це об’єднання Ethereum Mainnet з Beacon Chain, яка вже запустила PoS, із заміною енергоємного майнингу на стейкинг. Цей процес дозволяє Ethereum зберігати стабільність, одночасно забезпечуючи безпеку, і відкривати шлях для майбутніх оновлень маштабно. Стали з’являтися ноди валідаторів, які можуть отримувати винагороду за свою діяльність в мережі, а не лише за підтримку її функціонування [3].

Отже, Ethereum 2.0, також відомий як ETH2, представляє собою оновлення блокчейну Ethereum. Воно націлене на підвищення швидкості, продуктивності та масштабованості мережі Ethereum шляхом переходу від використання консенсусу Proof-of-Work (PoW) до консенсусу Proof-of-Stake (PoS). В консенсусі PoW майнери витрачають велику кількість обчислювальних ресурсів на розв'язування складних обчислювальних завдань, щоб створити нові блоки та підтримувати мережу. Однак цей підхід має обмежену швидкість обробки та споживає значну кількість енергії. Консенсус PoS дозволяє валідаторам (власникам криптовалюти) замість конкурентної "гонки" за створення блоків просто ставити в заставу свої активи, а потім обираються для створення блоків на основі обсягу активів, які вони володіють. Це дозволяє зменшити обчислювальне навантаження та знизити споживання енергії, що стає більш стабільним та стійким для мережі.

Підсумовуючи сказане, ми розуміємо, що Proof-of-Work (POW) та Proof-of-Stake (POS) - це дві зовсім різні моделі перевірки транзакцій у блокчейні, і вони технічно використовують різні підходи. POW виглядає так: обладнання майнера вирішує складні математичні завдання, використовуючи значну обчислювальну потужність, і це потребує величезних обсягів енергії. За кожен успішно доданий блок до блокчейну майнер отримує винагороду в криптовалюті. Цей процес вже згадувався як майнинг. У POS ситуація трохи інша: створювач нового блоку обирається системою заздалегідь, беручи до уваги не обчислювальні можливості учасників, а кількість криптовалюти, яку вони утримують у своєму гаманці. Цей процес відомий як стейкинг.У POW учасники мережі витрачають енергію і ресурси на вирішення завдань, тоді як у POS вагомою є кількість криптовалюти у власності. Обидва методи мають свої переваги та недоліки, але вони використовуються для забезпечення безпеки та дієвості блокчейну [4].

Ethereum Gas (ETH Gas) представляє собою оплату за здійснення транзакцій в мережі Ethereum. Кожен, хто проводить транзакцію в мережі Ethereum, зобов'язаний сплатити майнерам комісію у формі Ethereum Gas за відстеження та проведення цієї транзакції. Іншими словами при здійсненні операцій з Ethereum або іншими пов'язаними активами, ви оплачуєте Ethereum Gas. Блокчейн Ethereum

працює цілодобово і обробляє транзакції для криптовалюти Ethereum, а також NFT та інших криптовалютних токенів такі як: відправлення та отримання криптовалюти, укладання угод або створення та обміну NFT. Блокчейн Ethereum , працюючи з консенсусом Proof-of-Work (PoW), побудований на мережі комп'ютерів, відомих як майнери, які змагаються за право перевірки наступного блоку транзакцій. За свою роботу майнери отримують винагороду у формі плати за Ethereum Gas. У блокчейні Ethereum оплата за Gas здійснюється в Ether, офіційній криптовалюті мережі. Якщо ми здійснюємо торгівлю криптовалютою або NFT на блокчейні Ethereum, нам потрібно мати достатню кількість Ether (ETH) в своєму гаманці, щоб оплачувати витрати на газ при виконанні транзакцій. Плата за газ у Ethereum виражається у Gwei (Гвеї). 1 Gwei дорівнює 0,000000001 ETH. Це так само як 1 цент = 0,01 долара [1].

Плата за газ в мережі Ethereum залежить від того, наскільки активною та завантаженою є мережа. Під час інтенсивного використання мережі ціни на газ можуть зрости, оскільки попит на обробку транзакцій стає вищим. З іншого боку, коли активність низька і майнери готові приймати нові транзакції, вартість газу може бути меншою.

В кожному блоку мережі Ethereum встановлені два види плати: базова плата та плата за пріоритет. В залежності від характеру вашої транзакції, у користувачів є можливість встановити трохи вищу комісію за більш швидку обробку або трохи меншу за менш пріоритетну транзакцію. Смарт-контракти, оскільки вони вимагають більше обчислень, зазвичай супроводжуються вищими комісіями, особливо під час торгівлі NFT та іншими токенами, що використовують смарт-контракти. При встановленні високих комісій користувачі мають більше шансів на те, що їхні транзакції будуть обрані майнерами для обробки, які, в свою чергу, обирають, які транзакції вони готові обробляти. Вони надають перевагу тим транзакціям, які пропонують вищі комісії, оскільки це дозволяє їм заробити більше грошей. Така конкуренція між майнерами впливає на вартість газу [3].

Гаманець користувачів Ethereum показує очікувані комісії перед тим, як здійснюється транзакція, тому завжди є можливість попередньо їх оцінити. Отже і

є можливим уникнути непередбачуваних комісійних сюрпризів в процесі проведення транзакцій.

Транзакції в мережі Ethereum групуються та перевіряються у блоках, які фіксуються у блокчейні приблизно кожні 15 секунд. Цей неперервний процес дозволяє мережі ефективно обробляти транзакції та забезпечує швидкість операцій. Кожен блок має обмежену потужність для прийому транзакцій. Тому, коли мережа Ethereum перенасичена великою кількістю транзакцій, деякі з них можуть залишатися у черзі, очікуючи на обробку у наступному блоці. Під час підвищеного попиту на Ethereum, також спостерігається зростання вартості газу, яке вимірюється в доларах. Це може призвести до непередбачуваних витрат на комісії для користувачів, які здійснюють транзакції у мережі. Такі ситуації створюють нові виклики та роблять процес використання Ethereum більш динамічним і залежним від поточних обставин на ринку криптовалют. Націнка за транзакції Ethereum (ETH) недавно коливалася від 7 до 45 доларів для звичайних операцій. Однак, у випадку транзакцій, пов'язаних з NFT, витрати можуть значно зростати. Наприклад, при покупці та прийманні NFT активів, користувачі можуть очікувати витрати від 45 до 350 доларів. А при продажу таких активів вартість транзакцій може сягати від 200 до 490 доларів [1].

Ці значення відображають велику варіативність комісій, яка стає характерною особливістю мережі Ethereum, особливо в умовах підвищеного попиту на NFT та інші цифрові активи. За розрахунками Ethereum Foundation, новий метод, який передбачає заміну традиційного майнингу на стейкинг, може значно зменшити споживання енергії на 99,95%. Він стверджує, що для роботи одного вузла не потрібно більше електроенергії, ніж для роботи звичайного персонального комп'ютера. Це призводить до значного зменшення витрат на енергію та сприяє більш сталому та екологічному функціонуванню мережі. Також важливо відзначити, що завдяки цьому підходу оплата за газ значно знижується, оскільки витрати на обслуговування мережі стають значно меншими. Ноди Ethereum [1].

Розрізняючи повні, неповні та архівні ноди Ethereum, важливо розуміти їхні основні особливості і ролі в мережі. Повні ноди Ethereum мають копію всього блокчейна Ethereum, включаючи історіювсіх транзакцій та станів. Вони можуть перевіряти всі нові транзакції та створювати блоки. Це важливі вузли для стійкості та безпеки мережі. Повні ноди не обмежуються зберіганням архіву старих станів, що дозволяє їм бути більш швидкими та менш обтяженими щодо ресурсів. Неповні ноди Ethereum також зберігають копію блокчейна, але вони не містять архіву історичних станів. Вони призначені для транзакцій та перевірки актуального стану мережі, але не можуть надавати історичну інформацію. Вони легші за ресурсами та швидше синхронізуються з мережею, що робить їх популярними для додатків, які не вимагають доступу до всіх історичних даних. Архівні ноди Ethereum- це розширена версія повних нод, які зберігають всі дані, включаючи історичні стани в мережі. Це робить їх ідеальними для дослідників, розробників і тих, хто потребує доступу до всієї історії блокчейну Ethereum. Вони більш важкі за ресурсами та потребують значно більше місця для зберігання, але надають повний доступ до даних, що охоплюють усю історію мережі. Обираючи тип вузла для використання в Ethereum, користувачі мають можливість вибирати, залежно від своїх потреб у функціональності, швидкості та ресурсах [4].

Отже, для того, щоб зрозуміти можливість використовувати блокчейн технологій в повсякденному житті , в даному розділі ми розглянули ключові поняття та складові блокчейну. Ми прослідкували еволюцію криптовалют, в основі якої і лежить блокчейн технологія, розглянули значення криптовалютних бірж; з’ясували основні поняття та складові децентралізованого розподіленого реєстру, а саме: консенсус та протоколи консенсусу, структуру та організацію блоків, дали визначення смартконтрактам, транзакціям, хешам, нодам, дізналися, для чого потрібен криптогаманець та різницю між криптомайнингом і криптостейкінгом. Блокчейн є розподіленим реєстром, що оперує децентралізовано та записує операції з цифровими активами, які можуть представляти будь-що: від нерухомості, грошей, землі до нематеріальних активів, таких як патенти, авторські права та бренди [3].

Ця технологія сприяє зменшенню ризиків і витрат для усіх учасників ринку, а також прискорює виконання великої кількості платежів. Традиційно транзакції у комерційних банках, сервісах грошових переказів, кредитних центрах обробки платежів та інших фінансових сервісах можуть займати навіть декілька днів і супроводжуються комісійними витратами. У банків також існують обмеження за графіком роботи, що не завжди влаштовує клієнтів. З використанням блокчейну користувачі можуть надсилати гроші без географічних та часових обмежень. Операції здійснюються за декілька секунд, а підтвердження транзакцій зазвичай займає від кількох хвилин до декількох годин. Усі платежі в блокчейні є незворотніми, тому важливе поняття підтверджень для захисту від онлайн-шахрайства [1].

Криптовалюта відкриває доступ до фінансових продуктів і сервісів, забезпечуючи свободу від черг у банках і мінімізуючи паперову взаємодію. Керування цифровими активами можна здійснювати за допомогою комп'ютера або смартфона через спеціальний додаток, що дозволяє інвестувати в активи великих компаній та розподіляти кошти більш ефективно. Проаналізувавши вивчену інформацію, ми змогли виділити ключові принципи, на яких грунтується технологія розподіленого реєстру. Далі плануємо детальніше розглянути сфери використання блокчейн технологій та дослідити роботу блокчен технології на прикладі тестування ноди проекту Shardeum, в основі якого лежить блокчейн EVM (Ethereum) [4].

РОЗДІЛ 2 ДОСЛІДЖЕННЯ СПОСОБІВ ВИКОРИСТАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЙ

2.1 Сфери застосування блокчейн технологій

Аби показати, як технологія блокчейну стала універсальною у різних галузях промисловості, потрібно розглянути її розвиток та появу у відповідний час. Розглянемо історію розвитку блокчейну, щоб зрозуміти різноманітні можливості його використання у створених на його основі проєктах. У 2009 році Bitcoin був запропонований як нова фінансова система, що функціонує за допомогою тисяч комп'ютерів по всьому світу. Ця система зробила гроші менш залежними від централізованих установ, пропонуючи мережу комп'ютерів, які використовують блокчейн - особливий вид бази даних, реалізований через розподілений реєстр. Блокчейн надає можливість постійного додавання даних та гарантує безпечний криптографічний запис транзакцій, а також досягає консенсусу між комп'ютерами, що управляють цим процесом. З цього часу, блокчейн став основою для створення численних варіантів використання в різних сферах промисловості [7].

Основна мета блокчейну Bitcoin полягає в тому, щоб спростити процес передачі монет та зафіксувати цю транзакцію унікальним способом, який неможливо буде змінити чи видалити у майбутньому. Починаючи з моменту створення блокчейну Bitcoin, кілька розробників використовували цю технологію та розширювали її функціонал, додаючи нові можливості та напрямки використання. У 2015 році був започаткований блокчейн Ethereum, що впровадив смарт-контракти, які дозволяють програмувати угоди, що обмежуються не тільки фінансовими операціями [20].

У сучасному світі, технологія блокчейну вирішує різноманітні проблеми, що стоять перед учасниками різних галузей, починаючи від фінансів та закінчуючи сільським господарством. На сьогоднішній день існують тисячі блокчейн-платформ, починаючи від повністю децентралізованих систем, таких як Bitcoin, і

закінчуючи приватними корпоративними ітераціями, що контролюються однією компанією для конкретних цілей.

Одним з найбільш розповсюджених способів використання технології блокчейн є її застосування у фінансовій сфері. Використовуючи як розподілений метод фіксації транзакцій, блокчейн виріс у безліч криптогрошових сервісів. Від простих операцій купівлі та продажу з використанням криптовалют до складніших механізмів, таких як децентралізоване фінансування (DeFi) для кредитів, заощаджень, та створення пулів ліквідності [7].

Фінансова перспектива використання криптовалюти надала поштовх людям мати більшу вільність у заробітку та використанні грошей. Таким чином, блокчейн створює додаткові можливості надання фінансових послуг більш широкому колу осіб по всьому світу, особливо тим, хто має обмежений доступ до традиційних фінансових систем. Однак, з огляду на зростання популярності криптовалют упродовж останніх десяти років, було виявлено ще більше нових способів їх використання. Існує безліч варіантів застосування блокчейну, але деякі з них виявляються більш популярними за інші. Зокрема, наразі ми розглянемо шість таких напрямків використання, які завоювали популярність у всьому світі.

Першим напрямком є створення блокчейн-ігор, що відкрило нові можливості для інновацій та усунуло деякі традиційні проблеми, які виникають у галузі ігор. Це економічно вигідно, адже блокчейн дозволяє гравцям володіти цифровими активами у вигляді токенів або предметів у грі. Це створює можливість реальної власності та торгівлі цими активами за межами гри. Гравці можуть зберігати та обмінювати свої власності без посередників. Системи управління ігровими активами стають децентралізованими, відбувається уникнення централізованого контролю ігрових компаній [20].

Це може запобігти маніпулюванню грою та забезпечити більшу прозорість у процесі. Застосована концепція "Play-to-Earn" (Грай-і-Заробляй) Деякі блокчейн-ігри пропонують гравцям заробляти реальні кошти чи токени за участь у грі, розв'язання завдань чи навіть за здійснення інвестицій у гру. Такі ігри дозволяють обмінювати активи чи ресурси між іншими іграми, створюючи унікальний

екосистему для гравців. Також застосована концепція Non-Fungible Tokens (NFT), це цифрові активи, що є унікальними та невзаємозамінними, такі як CryptoKitties, які можуть бути колекціоновані та куплені, а їх власність підтверджується за допомогою блокчейну. Розробники використовують блокчейн для створення унікальних ігрових механік та можливостей, які стають реальними завдяки розподіленій мережі. Ці принципи та інновації роблять дані ігри цікавими та привабливими для гравців, забезпечуючи нові можливості для власництва, торгівлі та участі у грі.

Другим напрямком є застосування блокчейну у сфері нерухомості, дана сфера дійсно відкриває нові можливості та вирішує деякі проблеми, які існують у цій галузі. Блокчейн дозволяє зберігати інформацію про власність нерухомості у децентралізованому та надійному реєстрі, що робить процес покупки, продажу та обміну нерухомістю більш прозорим та надійним. Смарт-контракти, що базуються на цій технології, можуть автоматизувати та умовно виконувати угоди між сторонами без посередників, що сприяє швидкості та надійності транзакцій. Токенізація нерухомості - це процес представлення прав власності на нерухомість у вигляді токенів на блокчейні. Він дозволяє розділяти власність на менші частки, що відкриває шлях для ширшого кола інвесторів та сприяє доступності ринку нерухомості. Блокчейн дозволяє здійснювати краудфандинг проектів нерухомості через токенізацію, надаючи можливість більшій кількості осіб брати участь у фінансуванні нерухомості. Використання цієї технології дозволяє легко переносити власність на нерухомість, зменшуючи бюрократію та час, необхідний для цього процесу. Ці інновації сприяють покращенню ефективності, надійності та доступності цього ринку, роблячи його більш доступним та привабливим для різних учасників, включаючи покупців, продавців та інвесторів [7].

Третім напрямком є застосування блокчейну у галузі страхування, він відкриває широкий спектр можливостей для поліпшення ефективності та надійності, а також зниження шахрайства. Блокчейн гарантує безпеку та перевірку даних, що робить його корисним інструментом для виявлення шахрайства. Така технологія дозволяє стежити за історією транзакцій та виявляти недостовірні

угоди. Цей процес дозволяє створити мережу, де дані можуть бути легко доступними для всіх сторін. Це дозволяє страховим компаніям ефективно керувати даними, ведучи облік страхових полісів та перестрахування. Блокчейн дозволяє страховим компаніям розробляти нові та більш гнучкі моделі страхування, такі як мікрострахування, що дає можливість клієнтам отримувати захист за короткостроковими полісами. Використання смарт-контрактів на блокчейні може автоматизувати процеси виплат та страхових відшкодувань в разі виникнення подій, що покриваються страховим полісом. Блокчейн дозволяє створити безпечну та прозору платформу, яка сприяє збільшенню довіри між сторонами та забезпечує доступ до даних у реальному часі. Ці переваги роблять блокчейн привабливим для цих компаній, що ставлять перед собою завдання забезпечення більш ефективного, надійного та інноваційного обслуговування клієнтів [20].

Четвертим напрямком застосування технологій блокчейн є безпека, саме даний напрямок має значний потенціал у наданні безпеки на різних рівнях, від особистих даних до великих організацій та навіть державних установ. Ось кілька важливих аспектів використання блокчейну у сфері безпеки. Він дозволяє користувачам масштабувати контроль над своєю особистою інформацією, створюючи самосуверенні ідентичності, які можна використовувати безпечно та приватно для різних цілей. Криптографічно захищена передача даних через блокчейн дозволяє забезпечити конфіденційність та цілісність інформації, що передається. Деякі платформи використовують шифрування для забезпечення безпечного обміну повідомлення між користувачами. Блокчейн може забезпечити безпеку для пристроїв IoT, зменшуючи ризики витоку даних або вірусних атак. У бізнес-середовищі блокчейн дозволяє покращити безпеку та надійність шляхом використання розподіленого ведення записів, що ускладнює атаки відмови в обслуговуванні та забезпечує інтегровану систему безпеки. Деякі країни використовують блокчейн для покращення безпеки у державних системах, таких як реєстрація виборців, публічні закупівлі та зберігання документів. Ці застосування блокчейну допомагають у забезпеченні безпеки та захисту даних на

різних рівнях, забезпечуючи більш високий рівень конфіденційності, цілісності та доступності для користувачів та організацій [20].

П’ятим напрямком є мистецтво, NFT (невзаємозамінні токени) стали важливим елементом в сучасному мистецтві та колекціонуванні, привертаючи увагу до унікальності цифрових творів мистецтва. Вони перетворюють цифрові витвори унікальних майстрів на цифрові активи, які можуть бути продані або обмінені на аукціонах чи маркетплейсах за високі ціни. Розвиток NFT відкриває широкі перспективи для творців у мистецтві, музиці, моді та інших сферах, де унікальність та автентичність грають ключову роль. Мистецтво NFT - це більше, ніж просто створення цифрових робіт. Криптомистецтво, де NFT використовується як форма власності цифрових творів, зростає в популярності, надаючи творцям можливість отримати відповідну винагороду за їхню роботу через продаж унікальних токенів. Використання NFT може розширюватися на багато галузей, включаючи цифрове мистецтво, музику, фотографію, відео, а навіть підтвердження автентичності фізичних активів через цифрові записи у блокчейні. Наприклад, вони можуть служити як докази власності для реальних активів, таких як картини, музичні альбоми, нерухомість чи ювелірні вироби. Платформа Binance NFT Market має на меті забезпечити користувачам доступ до найкращих NFT на ринку, пропонуючи можливість досліджувати, придбати та торгувати цифровим мистецтвом та колекціонерськими предметами, використовуючи інфраструктуру та спільноту блокчейну Binance. Це створює ліквідну платформу для запуску та торгівлі NFT, де користувачі можуть отримати доступ до унікальних цифрових активів безпосередньо через свій акаунт Binance [7].

Технологія блокчейну вже вкоренилася в нашому світі і надалі залишатиметься надійним рішенням для багатьох компаній та установ. Такі великі гравці демонструють різноманітність використання блокчейну:

- JP Morgan впроваджує Quorum, корпоративну версію Ethereum, для конфіденційних транзакцій із смарт-контрактами;

- IBM використовує блокчейн у різних галузях, таких як автомобілебудування, банківська справа, охорона здоров'я та роздрібна торгівля, надаючи бізнес-платформи;
- Walmart спільно з IBM шифрує ланцюг постачання харчових продуктів, забезпечуючи безпеку свого товару та прозорість у харчовій екосистемі;
- Alibaba використовує блокчейн для відстеження замовлень у своєму транскордонному відділу електронної комерції Kaola;
- Gucci випускає цифрові колекційні кросівки з доповненою реальністю, захищаючи свою продукцію від підробок за допомогою блокчейну.

Не лише великі компанії використовують блокчейн. Цю технологію можна застосовувати особисто для розширення фінансових можливостей та полегшення повсякденного життя [7].

Шостим, але найпопулярнішим та найпоширенішим напрямком є фінансовий. В даній магістерській кваліфікаційній роботі ми використали технологію блокчейн саме у фінансовій сфері. Якщо ми говоримо про блокчейн з точки зору його можливостей у фінансових транзакціях, слід відзначити переваги та недоліки цієї технології як ключової частини фінансових інновацій. Блокчейн в основному пов'язаний з технологічними новаціями, проте його застосування в міжнародних фінансових транзакціях може також сприяти фінансовим інноваціям через:

- нові підходи до рішень, які виходять за межі традиційних фінансових інструментів, розширюючи їхню сферу застосування;
- заміна традиційних фінансових інструментів з метою поліпшення фінансового стану користувачів та підприємств;
- використання в конкретних сегментах фінансового ринку;
- хеджування високої волатильності ринкових параметрів, особливо в умовах фінансових криз;
- впровадження нових фінансових процесів, прийомів чи стратегій, спрямованих на використання нових продуктів на базі розподіленого реєстру.

Технологія блокчейн змінює бізнес-модель та технічні характеристики традиційних банків. Справжні мотиви для застосування блокчейну у міжнародних фінансових гігантів та місцевих комерційних банків включають:

- зниження витрат та оптимізація переказів активів за допомогою децентралізованого реєстру та автоматизації, що дозволяє побудувати ефективну та прозору модель з низькими витратами.
- ефективний контроль ризиків шляхом використання блокчейну для прямих однорангових транзакцій між позичальниками та кредиторами, що зменшує кредитний ризик та підвищує ефективність управління фондами.
- пошук інноваційних способів отримання прибутку, вкладання у стартапи з технологією блокчейну та розвиток нових фінансових продуктів.
- інновації технології та трансформація традиційного фінансового бізнесу комерційних банків відображаються у всіх аспектах, включаючи банківський бізнес, учасників транзакцій та оптимізацію фінансових послуг. Широке використання блокчейну на підприємствах поки що обмежується відсутністю чіткого регулювання та стандартизації, але впровадження цієї технології в бізнес-процеси підприємств свідчить про початок нової цифрової ери.

Розглянемо застосування технологій у фінансовій сфері на прикладі проєкту Shardeum [20].

2.2 Метод шардингу

Рішення для масштабованості, яке забезпечує одночасно безпеку та децентралізацію - це шардинг, що створює кілька груп валідаторів і дозволяє їм одночасно обробляти транзакції. Внаслідок цього, загальна пропускна здатність транзакцій лінійно зростає зі збільшенням кількості учасників. Першим публічним блокчейном, в якому зловмисник міг з'єднуєватися з жертвою, контролюючи при цьому кілька вузлів. У таких однорангових мережах, де жоден вузол не є повністю надійним, кожен запит розмножується для кількох одержувачів, уникаючи таким чином довіри до єдиного вузла [36].

В той же час користувачі мережі можуть мати кілька ідентифікаторів, фізично пов'язаних з різними вузлами. Ці ідентифікатори можуть застосовуватись для спільного використання ресурсів або мати кілька копій. Це може створити резерв, що перевірятиме цілісність даних, взятих з мережі, незалежно. Однак такий підхід може мати недолік, адже всі доступні сайти, призначені для представлення різних одержувачів запиту, можуть в кінцевому рахунку контролюватися одним і тим самим користувачем. Такий сценарій може виявитися проблематичним, якщо цей користувач виявиться порушником, оскільки він матиме всі повноваження посередника, набувши повної довіри ініціатора сесії. Існує ризик, що зловмисник може легко створювати нові ідентифікатори, що може призвести до закриття наступного сеансу користувача (Рисунок 2.1).

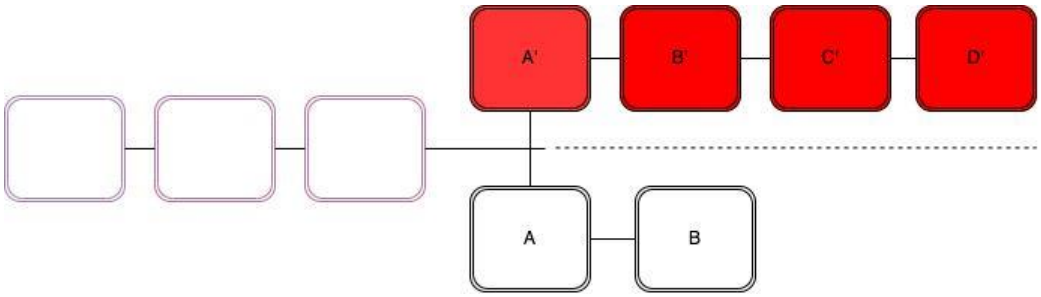

Рисунок 2.1 – Розподіл блокчейну на два, адже шкідливі вузли мають за мету утворити блоки, які не відповідають консенсусу

У даному блокчейні існують два шарди, обидва з якими розгалужуються, коли транзакція включається в блок A в шарді №1 і блок X в шарді №2. При розгалуженні шарди повинні відкидати один ланцюжок і приймати інший. У випадку, коли шард №1 приймає ланцюжок A, B і так далі, а шард №2 - ланцюжок W, X і так далі, консенсус буде підтверджений. Якщо ж шард №1 приймає ланцюжок A, B і так далі, а шард №2 - ланцюжок W, X і т.д., угода буде відхилена і може бути відправлена знову. Якщо шард №1 приймає ланцюжок A, B і т.д., а шард №2 - ланцюжок W, X і т.д., тоді одна частина угоди буде підтверджена (A, B і т.д.), а інша частина - ні (W, X і т.д.).

У промисловості та наукових дослідженнях пропонуються різні рішення для шардингу. У промисловості Zilliqa був першим публічним блокчейном на основі

шардингу, який заявив про пропускну здатність 2800 транзакцій в секунду. Zilliqa використовує PoW як процес реєстрації особи (тобто запобігання атаки Sybil). Дана мережа включає єдиний комітет для обслуговування каталогів та кілька комітетів шардів (мережеве шардування), кожен з яких має сотні вузлів. Транзакції присвоюються різним шардам та обробляються окремо. У наукових кругах також представлені публікації, такі як Omniledger та RapidChain, які пропонують рішення, де кожен шардинг містить підмножину стану блокчейну. Omniledger використовує багатосторонню обчислювальну схему під назвою RandHound, щоб створити безпечне випадкове число, яке використовується для незалежного розподілу вузлів по шардах. Omniledger використовує адаптивну модель, яка дозволяє змінювати місця вузлів з часом, щоб уникнути пошкодження всієї мережі зловмисниками. RapidChain базується на концепції Omniledger та пропонує використовувати правило обмеження для перестановки вузлів без порушення обслуговування [36].

2.3 Основні аспекти технології

Shardeum — це платформа смарт-контрактів 1 рівня на основі EVM із шардованим станом, створена для досягнення горизонтального масштабування. Головною метою Shardeum є забезпечення стабільно низької комісії за транзакції. Найпопулярніші програми на більшості платформ з смарт-контрактами, які пов’язані з торгівлею активами мають проблеми через перевантаженість мережі, що призводить до високої комісії за газ. Ми вважаємо, що для користувачів з всього Світу, котрі бажають розвиватись та використовувати децентралізовані програми, смарт-контракт платформа повинна забезпечувати стабільно низькі комісії за транзакції. Коли запускається нова мережа, комісія за транзакції зазвичай дуже низька, оскільки її використання значно менше ніж пропускна здатність мережі. Користувачі, як правило, задоволені протягом цього часу та мають хибне враження що плата й надалі залишатиметься низькою [17].

Протягом того, як популярність мережі зростає, то пропускна здатність її зменшується тому користувачі повинні бути готовими до збільшення комісії в

проведених транзакціях. Під час пікового завантаження мережі, комісії за транзакції можуть зростати експоненціально. Впровадження платформ смарт-контрактів було серйозно обмежено нездатністю поточних мереж масштабувати та відповідати вищим вимогам TPS зростаючій базі користувачів. З точки зору розробника, багато часу та зусиль витрачається на створення децентралізованих програм. Ресурси інвестуються в написання смарт-контрактів, їх тестування, налагодження, перевірку, створення дружнього інтерфейсу користувача, маркетинг програми, створення спільноти та залучення лояльних користувачів.

Це ресурсомісткі заходи, які вимагають значних вкладень часу, грошей та інших ресурсів. В той час, коли мережа є новою, то комісія за транзакцію лишається низькою, але коли вона набирає популярності, то відповідно комісія зростає. Для розробників смарт-контрактні платформи, які не можуть забезпечити стабільно низькі комісії за транзакції, представляють собою загрозу їхній бізнес-моделі. Кількість енергії, яка використовується мережею для обробки транзакції, неминуче повинна бути оплачена користувачем. Якщо мережа хоче досягти стабільно низьких комісій за транзакції, то енергія, яка використовується для обробки повинна бути якомога меншою. Таким чином, використовуючи алгоритм консенсусу, який не вимагає надзвичайних витрат енергії є обов'язковими. Наявність більшої кількості вузлів у мережі може допомогти підвищити рівень децентралізації та її безпеки, але після певного моменту додавання додаткових вузлів не принесе користі мережі. Багато з них не масштабується, тому що складність консенсусу та обсяг зв’язку зростає, коли до неї приєднується більше вузлів [17].

У мережах, де кожен вузол повинен обробляти кожну транзакцію, додаткові вузли лише додають експлуатаційні витрати на мережу для задоволення потреб децентралізації та безпеки. Це зрештою призводитиме до підвищення комісії за транзакції користувачів. Для блокчейну необхідне горизонтальне масштабування через сегментування щоб оптимально використовувати доступні вузли, підтримувати низькі експлуатаційні витрати мережі та забезпечувати низький рівень комісії для користувачів. Усі вузли, що надають ресурси мережі, повинні

мати можливість працювати прибутково в довгостроковій перспективі. Комісії за транзакції повинні покривати експлуатаційні витрати мережі, якщо вона хоче бути стійкою в довгостроковому періоді. Це означає, що кількість вузлів у мережі має регулюватися на основі пропускної здатності блокчейну.

У моменти, коли TPS мережі зменшується, вона повинна мати можливість зменшити кількість вузлів, інакше комісія за транзакції доведеться збільшити, щоб продовжувати платити всім валідаторам вузлів. Це важливий фактор, який не враховується жодною з існуючих мереж. Основна мета проєкту Shardeum полягає в тому, щоб забезпечити стабільно низькі комісії за транзакції з використанням смарт-контрактів на технології Shardin. Було обрано використовувати Shardeum з EVM. Це не тільки скоротило час розробки, але й зробило дану платформу легко доступною для існуючих смарт-контрактів на базі екосистеми Ethereum.

Атаки методом Sybil є економічно невигідними та дорогими в нерозділених мережах, таких як Ethereum. Шардовані мережі, ризикують піддатися такому типу атак, оскільки вартість захоплення будь-якого шарду набагато нижча ніж більшої частини мережі. Важливою метою Shardeum є забезпечення мережі захисними механізмами, такими, як: розсікання, резервні вузли та обертання вузлів. Мережа Shardeum була створена на основі вищезазначених міркувань захисту. Зокрема, задля мінімізування транзакційних витрат за рахунок ефективного використання доступних ресурсів при максимальному збільшенні масштабованості мережі, децентралізації та безпеки [17].

Дана мережа складається з вузлів перевірки та архіваторів. Вузли перевірки, які очікують приєднання до мережі називаються резервними. Вони зберігають дані про стан облікових записів та призначаються для обробки вхідних транзакцій пов’язаних з обліковими записами в межах діапазону їхніх адрес. Історія транзакцій передається на вузли-архіватори для постійного зберігання. Архіваторні вузли не беруть участі в жодному консенсусі та просто надають послугу зберігання даних мережі наприклад, транзакції та квитанції. Вузли перевірки мають невеликі вимоги до пам’яті та швидку синхронізацію приєднання до мережі, оскільки їм потрібно лише синхронізувати та зберігати стан облікових записів, для яких вони

призначені. Вузли перевірки, які були активними в мережі протягом найдовшого часу, періодично видаляються з мережі для заміненення випадковими вибраними резервними вузлами. Повільне і постійне обертання валідатора вузлів підвищує рівень децентралізації мережі та запобігає адаптації атак на дану мережу. Щоб запустити вузол валідатора, потрібно зробити ставку монети Shardeum під назвою SHM. Якщо валідатор виконує свої обов’язки належним чином, то отримує гарну винагороду, що дозволяє легко покрити операційні витрати на вузол та отримати хороший прибуток [23].

2.4 Процес шардування

Як відзначив Віталік Бутерін, засновник Ethereum, шардування є рішенням для трилеми масштабовності. Найбільш загальний тип шардування, відомий як шардування стану, розбиває вузли у мережі на менші групи, які зберігають підмножину даних стану і обробляють різні набори транзакцій для досягнення паралельної обробки. Пропускна здатність транзакцій у мережі збільшується пропорційно кількості шард у мережі. Шардування стану надає можливість досягти як масштабованості, так і децентралізації, зберігаючи при цьому безпеку. Однак багато з поточних платформ, які використовують шардування стану, роблять це обмеженим чином, і групування транзакцій у блоки додає складності до протоколу шардування. Жодна децентралізована мережа ще не продемонструвала лінійного або автоматичного масштабування [3].

Хоча шардування збільшує пропускну здатність, воно вносить додаткову складність. Більшість реалізацій шардування порушують атомарну комбінуваність, яка дозволяє об'єднувати кілька смарт-контрактів в одній транзакції. Крім того, шардування потенційно може зменшити безпеку мережі, якщо реалізовано недбало. Адверсарі можуть скомпрометувати лише межі відмовостійкості бізантійських фаултів в одному шарді, а не в усій мережі, щоб зупинити шард чи виконати довільні зміни стану.

Адверсарі також можуть запускати інші атаки, такі як атаки захоплення через шарди, нові атаки доступності даних, атаки відтворення, специфічні для шардів, та інші форми атак на шардовані мережі. Тому архітектура цих мереж має бути безпечною, надійною та мінімізувати атаки [3].

2.5 Архітектура валідатора Shardeum

Архітектура вузла перевірки Shardeum поділяється на прошарок протоколу та застосунку. Це дозволяє чітко розділити функції на нижньому рівні, такі як консенсус, синхронізація, розповсюдження інформації та інші, від функцій на рівні застосунку, таких як виконання транзакцій та керування даними стану. Набір інтерфейсних функцій дозволяє прошаркам застосунку та протоколу спілкуватися. Протокольний рівень реалізований програмним забезпеченням Shardus і виступає як модуль для прошарку додатку. Він завантажує модуль та викликає надані ним методи. Крім того, застосунок може реєструвати функції зворотного виклику та обробники подій через методи, надані модулем. Це дозволяє прошаркам обмінюватися даними.

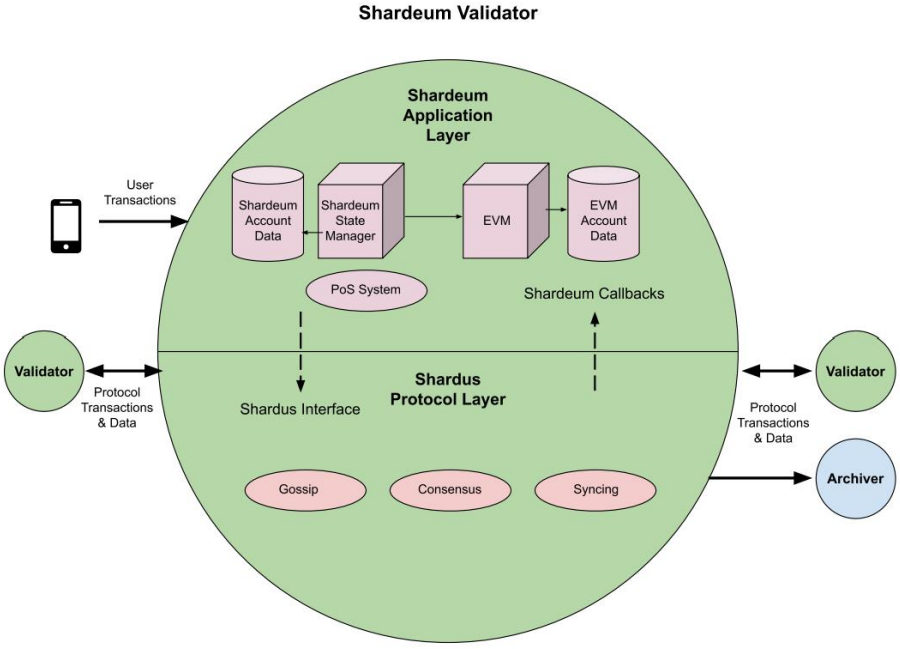

Рисунок 2.2 – Shardeum валідатор

Архіватори вузлів зберігають повний стан і історію мережі. Це дозволяє вузлам перевірки бути легкими з точки зору вимог до ресурсів. Однак архіваторам потрібно бути супервузлами з великою кількістю простору для зберігання оперативної пам'яті, процесорною потужністю та пропускною здатністю. Архіватори не беруть участь у жодному консенсусі і можуть бути запущені професійними операторами вузлів.

У розшареній мережі, такій як Shardeum, дані стану розподілені між багатьма вузлами перевірки, і жоден окремий перевірочний вузол не має всіх даних стану або не знає про всі транзакції. Таким чином, кожен архіваторний вузол повинен встановлювати зв'язки з багатьма вузлами перевірки для узгодження цієї розподіленої інформації. Як тільки повні дані мережі будуть узгоджені архіваторним вузлом, їх можна передавати службам нижчого рівня, які обробляють і відображають дані користувачам. Приклади таких служб включають дослідники, біржі та конектори (сервери RPC в Ethereum) [7].

Незважаючи на те, що кожен архіватор матиме повні дані мережі, буде багато архіваторів, щоб забезпечити надлишковість, так що навіть якщо деякі з них вийдуть з ладу, мережа не буде пошкоджена. В Shardeum ми плануємо мати принаймні 10 архіваторів під час запуску основної мережі (mainnet). Оскільки кожен архіватор підключається приблизно до двох перевірочних вузлів у кожному шарді, розмір шарди 128 може дозволити до 64 архіваторів. Збільшення їхньої кількості не впливає на продуктивність мережі жодним чином, а лише додає більше навантаження на пропускну здатність перевірочних вузлів. Причина наявності багатьох архіваторів полягає лише в забезпеченні резервного зберігання повних даних мережі.

Такі вузли також повинні мати економічну заставу для вступу в мережу. Вузол може бути позначений (slashed), якщо він покине мережу без попереднього запиту про вихід. Архіваторні вузли отримують винагороду за участь в мережі. Очікується, що винагорода за роботу такого архіватора буде приблизно в 10 разів більшою, ніж за роботу перевірочного вузла, оскільки вимоги до обладнання для роботи також будуть набагато вищими.

Крім заробітку на мережі, такі вузли також можуть заробляти, надаючи послугу передплати на дані. Наприклад, біржі будуть потребувати даних та подій для облікових записів, що належать їм, і вони можуть не запускати архіваторний вузол, структура якого зображена на рисунку.

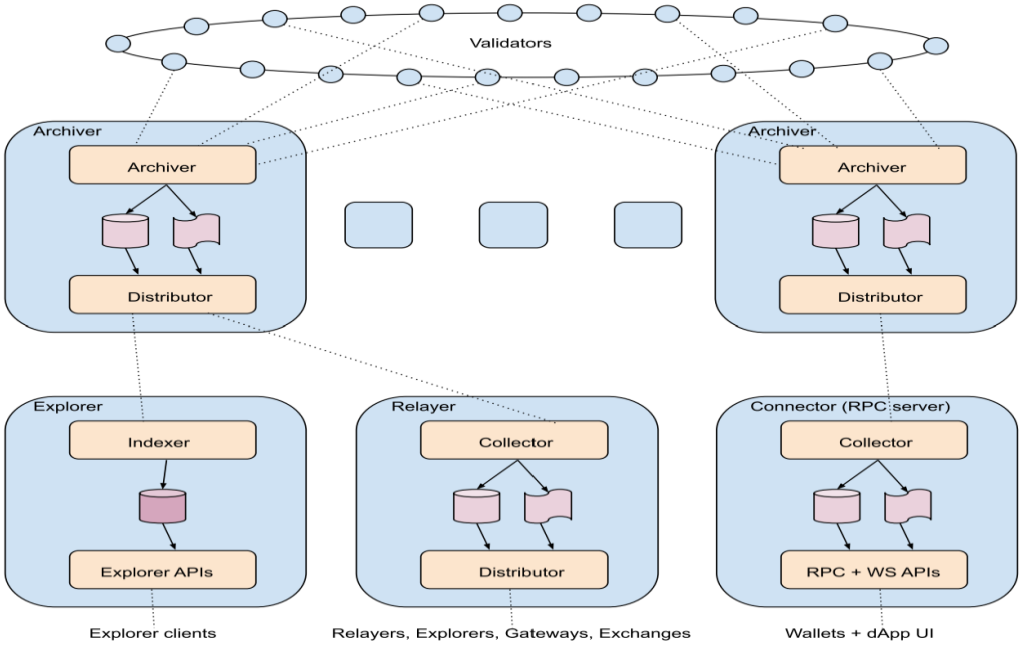

Рисунок 2.3 – Структура архіваторного вузла

У висновку, на фоні платформ які розвиваються для смарт-контрактів, Shardeum презентує інноваційний підхід, що вирішує вроджені виклики трилеми блокчейну. Завдяки використанню кількох новаторських рішень, таких як динамічне шарування стану, лінійне та автоматичне масштабування, атомна композабельність між шардами і доказ кворуму, а також використанню шарованої, безблочної та сумісної з EVM архітектури, Shardeum вирішує проблему між масштабованістю, безпекою та децентралізацією. Він в кінцевому підсумку перетворить широку екосистему web3, відкриваючи еру практично безмежної масштабованості, бездоганної безпеки та небаченої децентралізації, відзначаючи настання першого покоління потужних додатків з мільярдами користувачів [7].

2.6 Використання технології блокчейн на прикладі проєкту Shardeum

Проєкт Shardeum (SHM) – представник блокчейну Ethereum (EVM-based), який використовує технологію Sharding для маштабування мережі. Таку технологію використовують відомі блокчейни як Zilliqa (ZIL), NEAR Protocol (NEAR). Технологія Sharding – це технологія , завдяки якій усі транзакції перевіряються та верифікуються паралельно, а не послідовно як в класичному Ethereum, де будь-яка транзакція має пройти через кожну ноду і кожна нода має підтвердити, що ця транзакція дійсно відповідає усім вимогам і вона справжня. І тільки коли всі ноди підтвердили транзакцію, тоді вона вважається затвердженою. Використовуючи технологію Sharding, не потрібно чекати поки сформується один блок, можливо відразу відправити декілька транзакцій, які розбиваються на блоки і усе підтвердження транзакцій відбувається паралельно, а не послідовно [36].

Завдяки зміненій технології підтвердження транзакцій, їх швидкість збільшується, а ціна знижується. Наприклад, якщо в Ethereum відправляється близько 10 транзакцій за секунду, то тут близько 2000 за секунду. Це не так і багато, якщо порівнювати з швидкістю транзакцій відомих блокчейнів першого рівня , але якщо врахувати, що цей проєкт є новим і швидко розвивається, то він вартий уваги. Це більше ніж в Bitcoin чи Ethereum. Отже, проєкт Shardeum – децентралізований, працює на ефіріумі, створений для того, щоб зменшити комісію на газ та маштабувати мережу за допомогою технології Sharding [7].

На офіційній сторінці Shardeum міститься інформація про кількість смарт-контрактів (на 14.11.2023), їх екосистема налічує 105 проєктів, кількість акаунтів та транзакцій , розписана токеноміка проєкту. Ethereum Virtual Machine (EVM) представляє собою комп'ютерний механізм, який функціонує як децентралізований обчислювальний пристрій, який вміщує множину виконуваних завдань. Ця віртуальна машина становить базу операційної системи Ethereum, що відповідає за запуск виконання та розгортання смарт-контрактів [34].

Основне призначення EVM полягає у впровадженні різноманітних функцій у блокчейні для забезпечення обмеження можливих проблем у розподіленому

реєстрі. Кожен вузол Ethereum використовує EVM для забезпечення узгодженості даних по всьому блокчейну. Платформа Ethereum спрощує використання технології, яка відома як смарт-контракти, що є фрагментами коду, які працюють у середовищі Ethereum. EVM функціонує в повній ізоляції, це означає, що код всередині EVM не має доступу до мережі, файлової системи або інших процесів. В мережі Ethereum існують два типи облікових записів: зовнішні облікові записи (EOA) та контрактні облікові записи, які обробляються однаково в межах EVM.

Абстракція облікових записів прагне скоротити це до одного облікового, у якому як EOA, так і контрактні облікові записи працюють у подібний спосіб. EOA управляються приватними ключами, в той час як контрактні облікові записи знаходяться в межах смарт-контрактів, відомих також як смарт-гаманці. Контракт, записаний у формі смарт-контракту, перетворюється у так званий байт-код (bytecode). Більшість вихідних кодів для них створено мовою програмування Solidity, а потім перетворено на операційні коди для інтерпретації в межах EVM. Після чого EVM використовує операційні коди для виконання певних завдань. Отже, EVM працює як головний децентралізований комп'ютер для виконання всіх видів завдань у мережі блокчейн. Він є одним з найважливіших проєктів у світі криптовалют [35].

Проєкт Shardeum має намір стимулювати проєкти екосистеми для створення нових інноваційних додатків на платформі, а також перенесення популярних додатків, що були створені на інших платформах. Система стимулювання екосистеми також передбачає розвиток різних допоміжних інфраструктур, програмного забезпечення та послуг, необхідних для основної мережі. Наприклад, незалежні децентралізовані мости для передачі активів між Shardeum та іншими мережами. Крім основних валідаторів та архівів, в екосистемі потрібно багато послуг задля розподілу даних та їх доступності для користувачів. Децентралізовані додатки, відомі як dApps, - це додатки, що працюють на платформах смарт-контрактів, усуваючи потребу в централізованих посередниках і, водночас, забезпечуючи прозорість, безпеку та незмінність. У екосистемі Shardeum ми підтримуємо та стимулюємо розробку dApps, які оптимізовані для паралельної

обробки транзакцій або можуть здобути користь від цього. Це особливо корисно для dApps з великим обсягом транзакцій або для тих, що потребують виконання складних обчислень, які можна розбити на менші конкурентні завдання [7].

Транзакції обробляються у порядку черги за принципом "перший прийшов - перший обслужений" (FCFS), цей підхід є корисним, оскільки він забезпечує передбачуваність, справедливість, запобігає високим комісіям через аукціон, пропонує опір MEV і відкриває шлях для нових типів dApps. У аукціонах ставки повинні оброблятися у порядку їхнього виконання. FCFS забезпечує те, що, якщо двоє учасників роблять ставку практично в один час, перевагу отримує той, хто зробив ставку першим. Для подій з обмеженою кількістю місць або особливих видань товарів, система FCFS забезпечує, що першопровідні отримують квитки чи товари без потенційних затримок або обробки не за порядком. Будь-який dApp, де користувачі стоять у черзі на отримання послуги (наприклад, віртуальний очікувальний зал), скористається від FCFS. Це забезпечить справедливість та зменшить потенційні конфлікти. Деякі онлайн-ігри, особливо ті, де гравці змагаються за обмежені внутрішньо-гральні ресурси, можуть використовувати FCFS для визначення порядку отримання цих ресурсів. При випуску нових доменів або доменних розширень обробка FCFS може справедливо визначити, хто отримає певне доменне ім'я, якщо існують зацікавлені сторони. Крім того, ми прагнемо сприяти розвитку dApps, що ґрунтуються на низьких комісіях за транзакції, відкриваючи двері для інноваційних використань, які раніше були непрактичними на інших платформах через високі витрати.

Такі dApps включають, але не обмежуються:

- системи бонусних балів для продавців;
- системи купонів для товарних бізнесів;
- системи голосування для невеликих спільнот;
- платформи масового фінансування, схожі на Kickstarter;
- автоматизовані платіжні рішення;
- послуги членства, схожі на Patreon;
- алгоритмічні стабільні монети;

- ігри з невеликими інвестиціями, такі як лотереї.

Мотивація за підтримку цього напрямку має багатогранний характер. Сприяння dApps, що ґрунтуються на низьких комісіях за транзакції, базується на зобов'язанні внесення широкого спектру додатків, які можуть революціонізувати існуючі галузі та навіть породити цілком нові.

Крім того, вперше dApps можуть масштабуватися до рівнів, які загалом зустрічаються у популярних веб-сервісах типу web2, не досягаючи результатів. Крім того, всі dApps в межах Shardeum підтримують сумісність з Ethereum, що пропонує подвійну перевагу: велика спільнота розробників, знайомих із Ethereum, може легко переходити чи переносити свої проекти на Shardeum, тоді як користувачі отримують користь від широкого сприйняття та довіри, пов'язаного з додатками на основі Ethereum. Для спільноти Shardeum ці стратегії означають майбутнє збільшеної інновації, взаємодії та включення [24].

Багато нових мереж, які надають такий самий або схожий функціонал смарт-контрактів, як Ethereum, були розроблені, щоб заповнити прогалину, залишену Ethereum. Серед цих нових платформ для смарт-контрактів більшість з них пожертвували децентралізацією, щоб досягти вищого TPS. Ми свідомо використовуємо термін "вищий TPS", а не "вища масштабованість", оскільки ці мережі не призначені для масштабування, а просто підвищують планку від 20 TPS Ethereum до вищого максимального TPS. Зазвичай це приблизно 500 TPS. Платформи для смарт-контрактів у цій категорії не використовують шардування і включають такі мережі, як: BNB Chain, Solana та Algorand, щоб згадати лише деякі. Коли ці мережі наближаються до межі свого максимального TPS, вони також зазнають високих плат за газ та повільного оброблення, подібно Ethereum. Ці платформи можуть збільшувати TPS лише в тому випадку, якщо кожен вузол у системі оновлюється для більшого обчислення, зберігання та пропускної здатності. Це називається вертикальним масштабуванням [36].

Однією з перших платформ для смарт-контрактів, яка спробувала шардування, була Zilliqa. Всі вузли у цій платформі зберігали повний стан, і кожну транзакцію отримував кожен вузол. Проте, для перевірки транзакцій мережа була

розділена на кілька партій на основі адресного простору облікових записів. Це називається шардуванням обчислень, оскільки воно розбиває роботу з перевірки транзакцій, яка зазвичай потребує великих обчислень. Але оскільки кожен вузол все ще отримує кожну транзакцію і оновлює стан всіх облікових записів, пропускна здатність мережі та операції зберігання все ще стають вразливим місцем. Zilliqa може досягти вищого TPS, ніж система без шардування обчислень, але вона не є масштабованою, оскільки мережа та зберігання не є шардованою [2].

Більш масштабованим підходом для задоволення зростаючого попиту на децентралізовані додатки є наявність взаємопов'язаної системи з кількох бічних або під-ланцюгів. Такий підхід використовується платформами, такими як Polkadot, Cosmos та Avalanche. Цей підхід можна назвати функціональним шардуванням, коли децентралізовані додатки, які повинні взаємодіяти один з одним, можуть бути запущені на одному бічному ланцюгу. У випадку Polkadot кожен учасник може обробляти приблизно 1000 TPS. Навіть якщо TPS бічного ланцюга може здаватися низьким порівняно з мережами, такими як Solana, можливість мати кілька бічних ланцюгів дозволяє таким платформам масштабуватися, і загальний TPS усіх ланцюгів може перевищити той, який використовує лише вертикальне масштабування. Транзакції між контрактами на одному бічному ланцюгу виконуються швидко та легко [7].

Однак композабельність між контрактами на різних бічних ланцюгах у межах однієї мережі все ще складна через асинхронний характер комунікації між бічними ланцюгами. Замість цього очікується, що активи та повідомлення будуть передаватися між ними для координації взаємодій. Відсутність атомарної композабельності між бічними ланцюгами може ускладнити доступ до ліквідності DeFi, яка розділена між бічними ланцюгами. Якщо бічний ланцюг досягає свого максимального TPS, єдиним способом впоратися з перенавантаженням буде вертикальне масштабування вузлів у ньому або міграція деяких популярних контрактів на інші бічні ланцюги. Найбільш загальним підходом до шардування є розділення адресного простору облікових записів на кілька фіксованих регіонів, які називаються шардами, та призначення підмножин вузлів у мережі різним шардам.

Це називається шардуванням стану. Такий підхід використовується платформами, такими як Near, Harmony та MultiversX (раніше Elrond). Хоча Ethereum спочатку планувала реалізувати шардування стану, новий підхід, прото-данкшардінг, шардує лише дані для досягнення вищої доступності, тоді як виконання відбувається поза ланцюжком. У мережі з шардуванням стану транзакції між контрактами в тому ж самому шарді є швидкими та простими, тоді як транзакції між декількома шардами вимагають координації між ними та виконуються набагато повільніше. Існуючі блокчейни з шардуванням стану повинні асинхронно та послідовно виконувати транзакції, які впливають на більше, ніж один шард; передача транзакцій кожному залученому шарду. Це тому, що транзакції в таких мережах групуються в блоки, а узгодження відбувається на рівні блоків [7].

Отже, транзакції, які впливають на кілька шардів, ризикують бути підтвердженими в одному шарді, але не підтвердженими або скасованими в іншому. Крім того, збереження атомарності обробки транзакцій потребує додаткових рівнів складності. Включаючи транзакції, які впливають на декілька шардів, потребують додаткового часу обробки пропорційно до кількості вузлів, на які вони впливають. Навіть за таких умов шардування стану все ще є корисним, оскільки пропускна здатність всієї мережі зросте пропорційно до кількості її блоків.

Для практичного застосування технології блокчейн ми обрали дослідження та аналіз роботи мережевих вузлів від проєкту Shardeum на основі блокчейну Ethereum. Задля цього спочатку нам необхідно було встановити ноду (мережевий вузол) із дотриманням ряду вимог:

- постійне та стабільне підключення до інтернет-мережі;
- аналогічно постійно увімкнений комп’ютер;
- 250 GB SSD диску;
- чотирьохядерний процесор віком менше 10 років;
- 16 GB оперативної та 4 GB віртуальної пам’яті;
- для роботи на хостингу також необхідно 8 GB оперативної та 8 GB віртуальної пам’яті;

- операційна система ubuntu 20.4.

Нами було обрано сервіс по наданню серверів CONTABO, адже він має ряд переваг:

- низька ціна та якісні послуги;
- повна конфіденційність та контроль над даними;
- підключення користувачів по всій Європі;
- незалежна підтримка від реальних працівників, а не ботів.

Для того, щоб підключитись до сервера CONTABO на Windows нам потрібно було використати програму PuTTY (вільно розповсюджуваний клієнт для протоколів SSH, Telnet, rlogin та чистого TCP) та зареєструватись для подальшої роботи із обраним сервером, оренда сервера обійдеться близько 20 € (Рис 2.1).

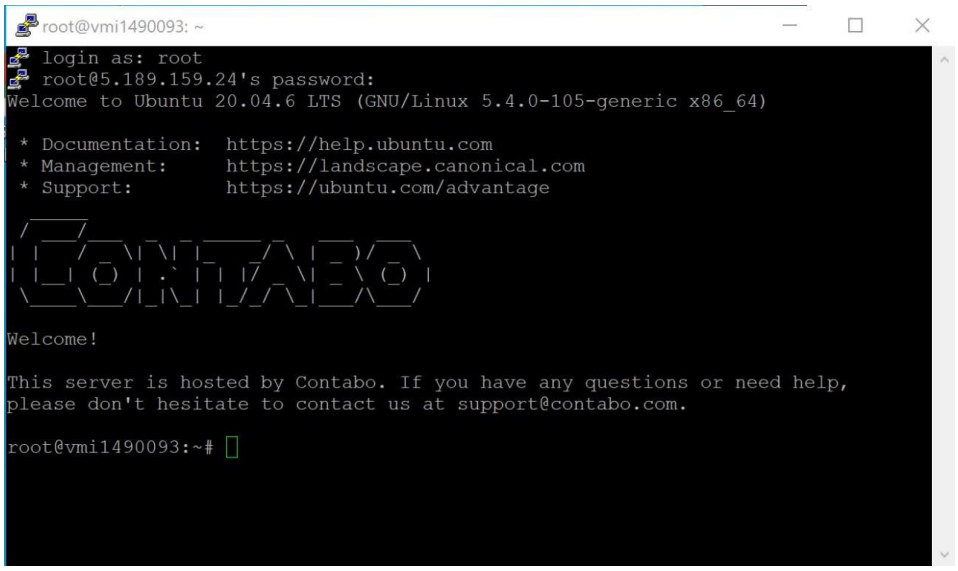

Рисунок 2.4 - Авторизація на сервері CONTABO

Наступним кроком після підключення до сервера CONTABO, здійснюємо встановлення мережевого вузла, в нашому випадку – нода від проєкту Shardeum. Інсталюємо Docker (інструментарій для управління ізольованими Linux-контейнерами), перевіряємо його версію та обов'язково оновлюємо всі утиліти. (Рис 2.2).

Рисунок 2.5 – Вдале інсталювання Docker

Далі встановлюємо Docker-compose та ноду Shardeum із репозиторію GitLab, результат встановлення ноди зображено на рисунку 2.3.

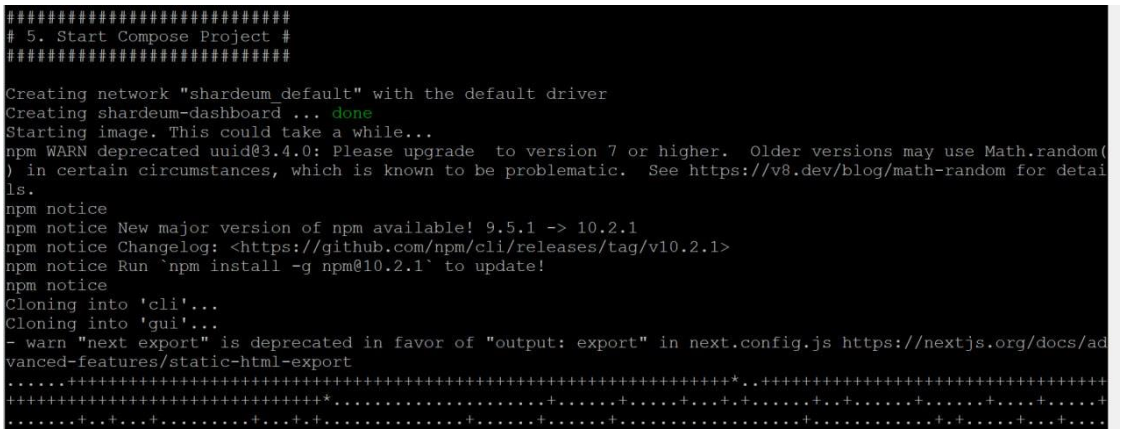

Рисунок 2.6 - Успішне встановлення ноди

Після встановлення ноди необхідно обрати надійний пароль для входу на платформу Shardeum. Також налаштовуємо порти та репозиторій за стандартними умовами налаштувань, наступним кроком є запуск валідатора командою «operator-cli start», далі ми заходимо на платформу Shardeum та вводимо IP-адресу сервера для авторизації мережевого вузла. Переходимо на вкладку Maintenance де можемо побачити вікно даного формату (Рис 2.4).

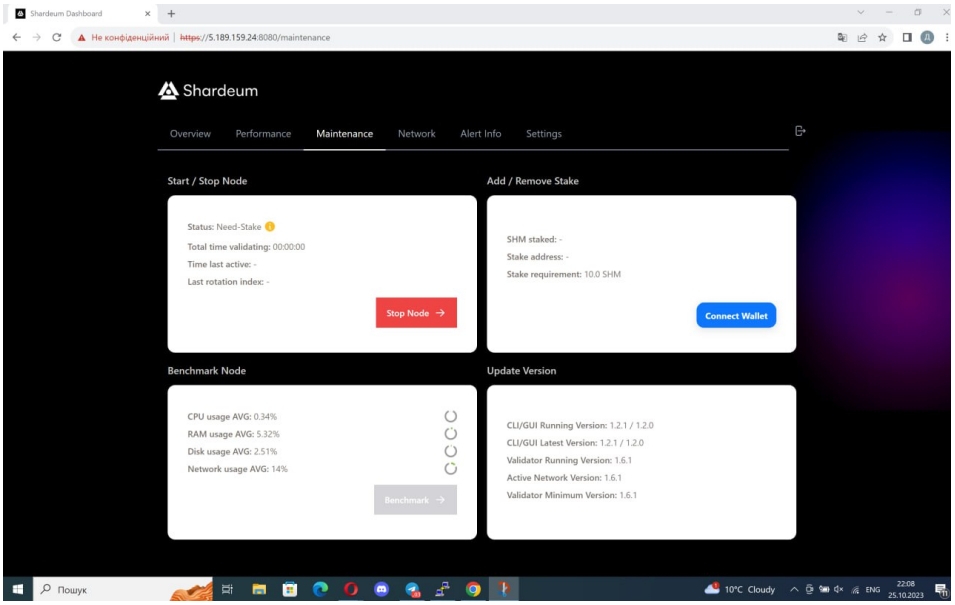

Рисунок 2.7 - Особистий кабінет проєкту Shardeum

Наступним кроком є процес застейкування монети SHM, на сайті додаємо мережу Sphinx 1.X в MetaMask та клеймимо 15 тестових токенів Shardeum на даному сайті (Рис 2.5), потім вводимо посилання на твіт із нашою адресою MetaMask, для цього просто натискаємо внизу на сторінку Tweet Now.

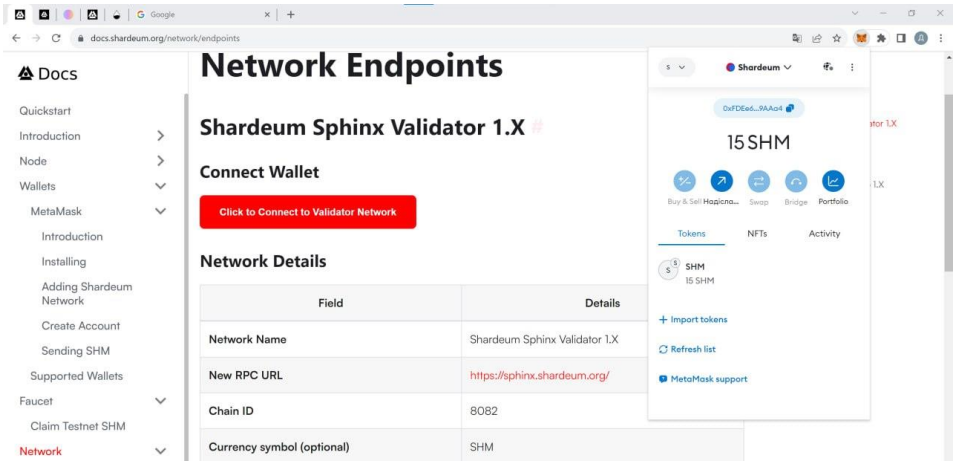

Рисунок 2.8 - Процес отримання тестових токенів

Далі ми отримали 15 SHM і повертаємось в Shardeum Dashboard, в цьому вікні ми прив’язали свій гаманець та обрали кількість токенів, в нашому випадку - 10 та застейкуємо їх застосувавши кілька основних кроків. Перший крок зображено на рисунку 2.6.

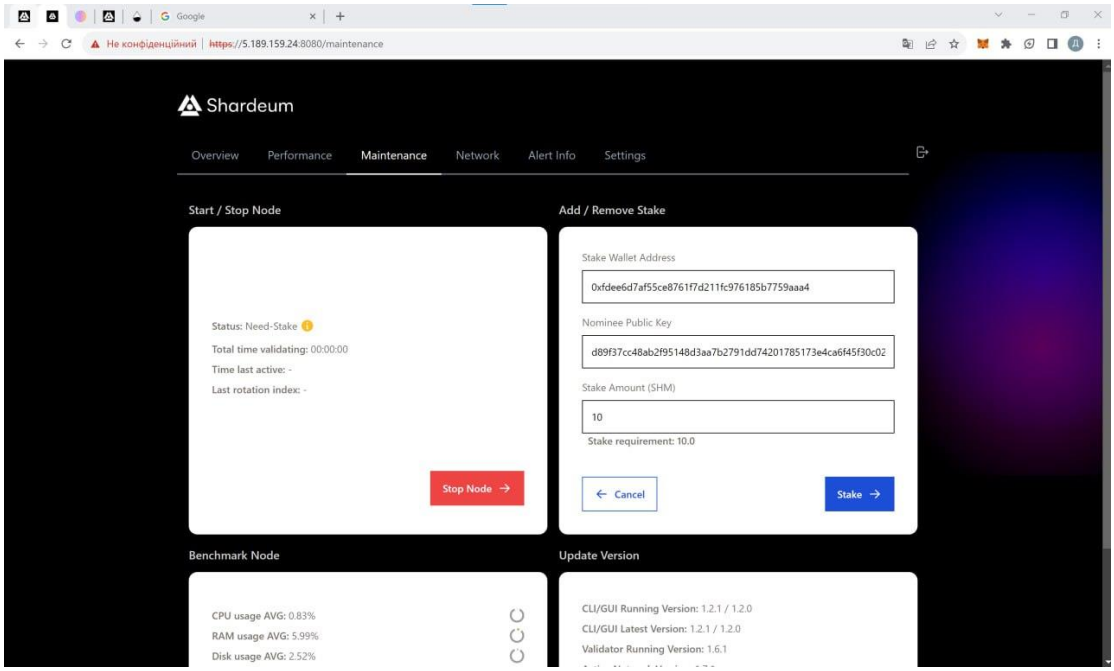

Рисунок 2.9 - Підключення особистого гаманця до ноди

Наступним кроком є транспортування монет SHM з особистого гаманця в мережу Shardeum для старту стейкінгу ноди, даний процес зображений на рисунку 2.7.

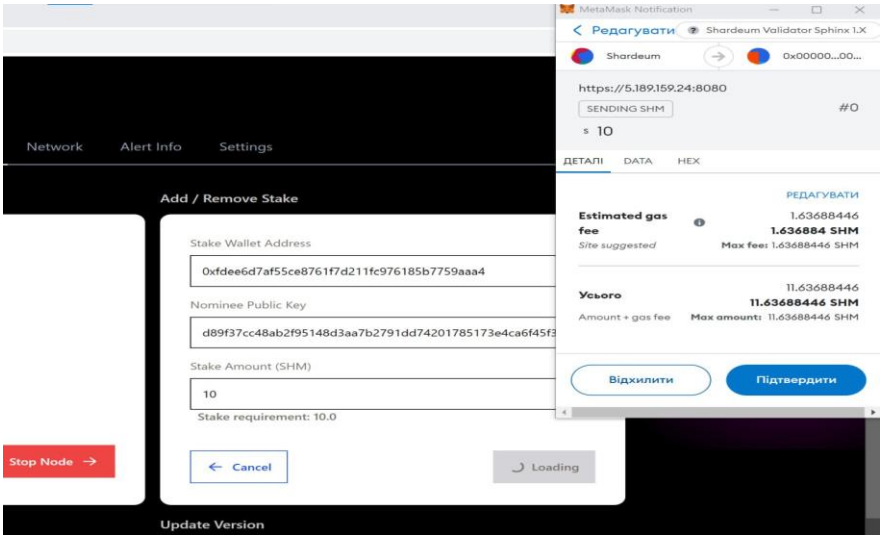

Рисунок 2.10 - Транспортування монет SHM з особистого гаманця в мережу Shardeum для старту стейкінгу ноди

Отримуємо результати проведення даного дослідження, на рисунку 2.8 та 2.9 можемо побачити, що процес транспортування монет SHM з особистого гаманця в мережу Shardeum відбувся успішно, про це свідчить поява повідомлення «Stake succesfull» зверху вікна, та наш screenshot із підтвердженням успішності операції.

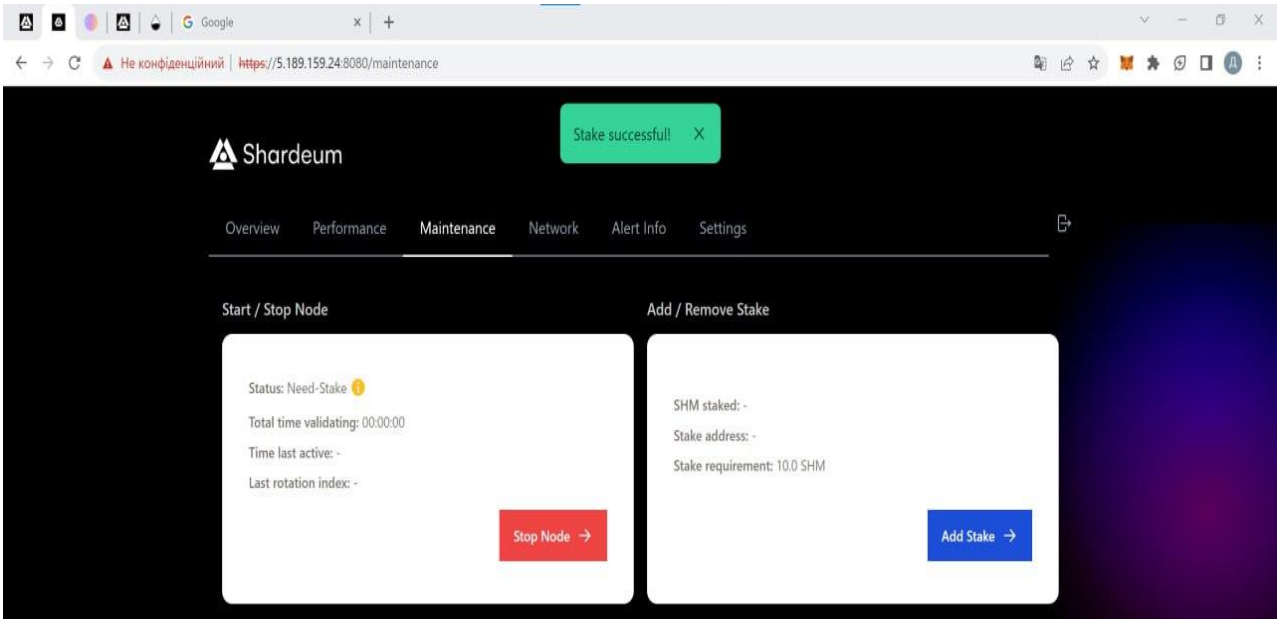

Рисунок 2.11 - Успішне транспортування монет SHM

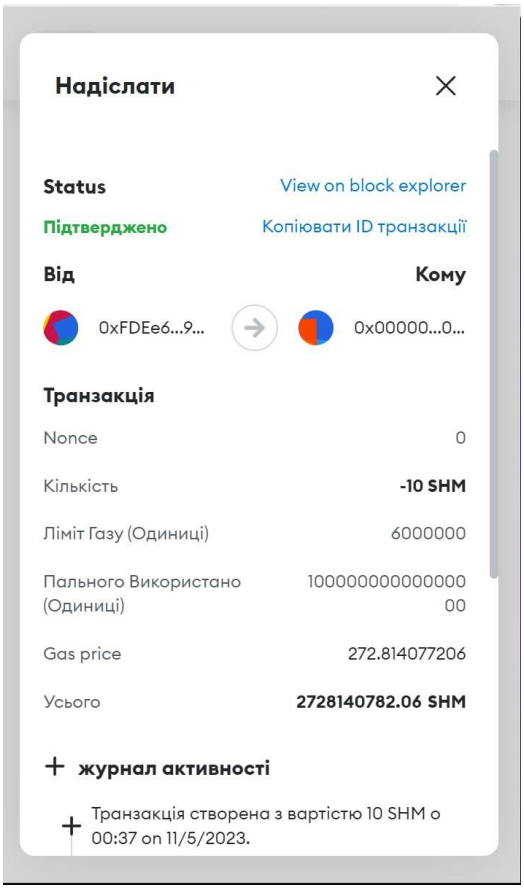

Рисунок 2.12 - Підтверджена транзакція транспортування монет SHM

Останнім кроком є перевірка функціонування поставленої ноди, даний процес зображено на рисунку 2.10.

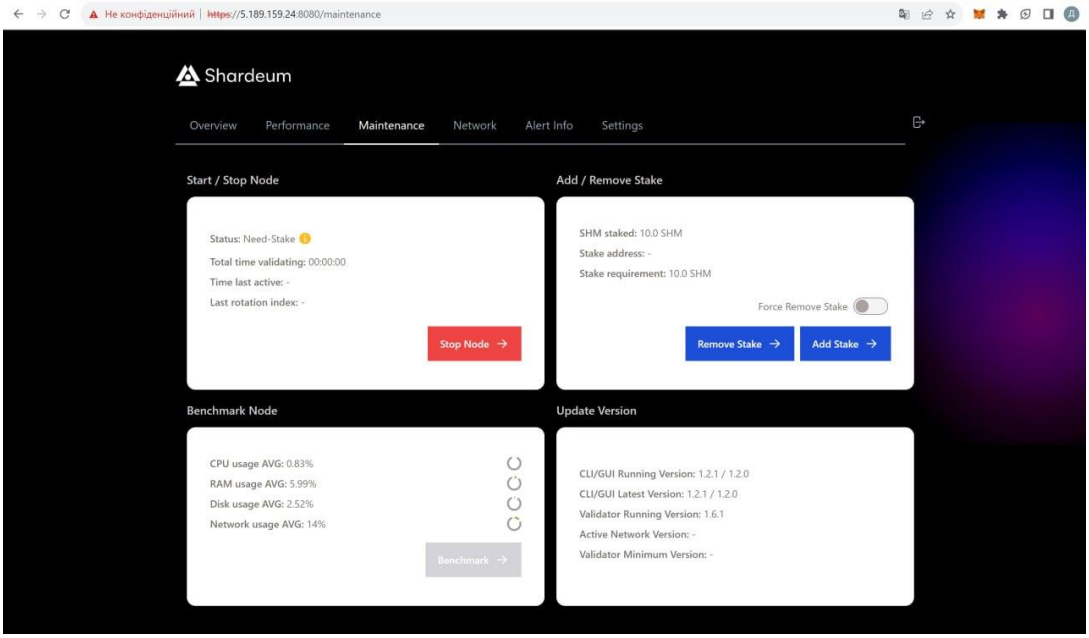

Рисунок 2.13 - Успішне встановлення ноди Shardeum

Періодично ми заходили в Dashboard та перевіряли чи без збоїв працює наша встановлена нода. Кінцевим етапом даного процесу є запит тестових токенів у їхньому Discord каналі на гілці #spinx-faucet-1.5 та стейкання SHM. Канал Discord зображений на рисунку 2.11.

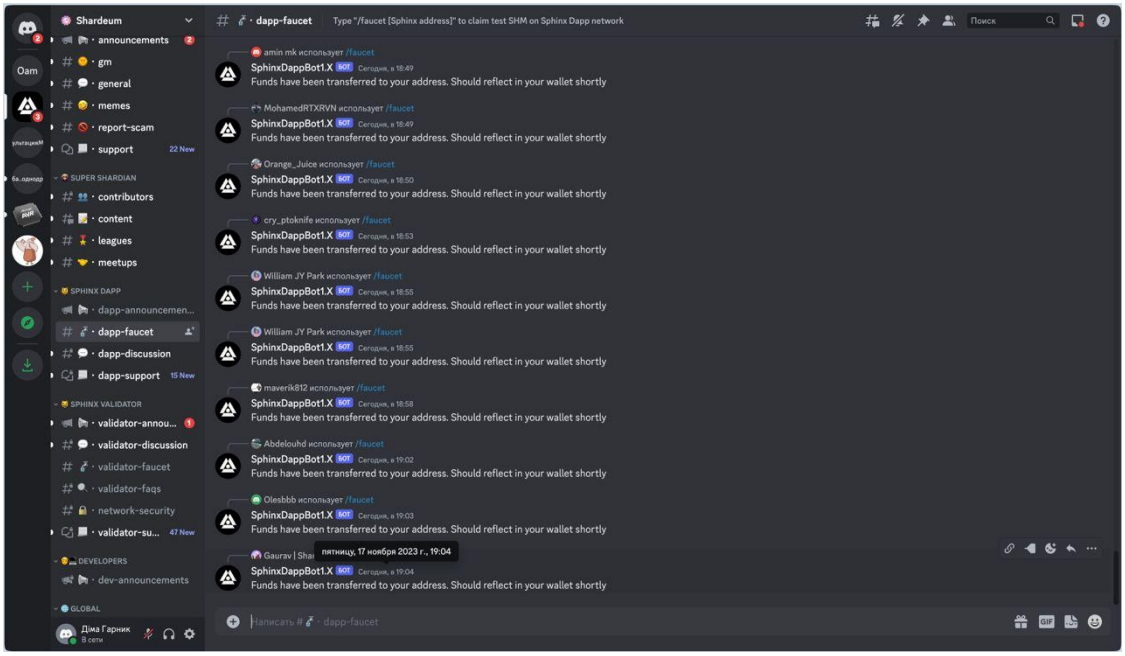

Рисунок 2.14 - Discord - канал на гілці #spinx-faucet-1.5

Отже, виконавши вищезазначені завдання та дослідивши технології блокчейн на основі проєкту Shardeum можемо дійти до висновку, що ми виступили в ролі валідатора, але відомо, що у користувачів, які змогли заблокувати більше монет, зростають шанси для запуску більшої кількість вузлів-валідаторів, і це покращує шанси на обрання їх для підтвердження нових транзакцій, але ми виступили валідатором із меншою кількістю монет і також змогли підтвердити транзакцію та отримати відповідні винагороди. Проєкт є досить доступним у використанні та надає можливість користувачам вступати до проведення транзакцій із мінімальною кількістю монет.

РОЗДІЛ 3

АНАЛІЗ ТА УЗАГАЛЬНЕННЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ

3.1 Оцінка продуктивності та ефективності мережі

Після проведеного нами дослідження було виявлено ряд проблем, які варто виправити, аби продуктивність проєкту збільшувалась в кілька десятків разів. Розглянемо вартість транзакції, вона визначається сумою, яку користувачі сплачують за пересилання токенів. Складність транзакції впливає на розмір комісії: прості операції, такі як переказ SHM, обійдуться дешевше, в той час як більш складні транзакції, наприклад, операції AMM, будуть коштувати значно більше. Наявність можливості регулювання цього параметра надає можливість змінювати дохід мережі, враховуючи щоденний обсяг транзакцій та комісію, оскільки всі отримані комісійні винагороди витрачаються. Цей параметр також може впливати на рівень інфляції чи дефляції активів, направляючи їх до балансу.

Винагорода вузлів визначає, скільки активних вузлів у мережі отримують прибутку в доларовому еквіваленті за годину. Незважаючи на те, що вона визначена в доларах, виплачується у SHM. Зміни цього параметра дозволяють збільшувати чи зменшувати вартість операцій мережі, розраховану як добуток кількості активних вузлів та винагороди для кожного вузла. Оскільки параметр винагороди вузла визначає, як відбувається виділення нових SHM, він може викликати інфляцію або дефляцію активів та налаштовувати їхню рівновагу. Цей параметр також впливає на співвідношення S:A, можливість збільшення або зменшення якого є ще однією його додатковою властивістю. Зі зростанням винагороди за годину мережа може підтримувати більше вузлів при зазначеному APY%, що призводить до збільшення співвідношення S:A. Зменшення винагороди може призвести до того, що мережа не зможе утримувати поточну кількість вузлів при зазначеному APY%, що призведе до зниження співвідношення S:A.

Сума ставки визначається кількістю SHM, яку вузол повинен вкласти для участі в мережі, і виражена в доларовому еквіваленті, але фактично здійснюється в SHM за сталої ціни. Цей параметр може бути частково або повністю втрачений, якщо вузол веде себе некоректно або відстає в обробці, це призводить до того, що оператори працюють з вузлами на відповідному обладнанні. Регулюючи цей параметр, можна збільшити або зменшити річний загальний дохід вузла (% APY) (розрахований як 100 * дохід * 365 / сума залогу), що впливає на співвідношення S:A внаслідок зростання чи зменшення прибутковості роботи вузла. У разі, якщо дохід мережі менший за витрати, відбувається видаток у спадок. Це означає, що мережа не генерує достатньо прибутку, щоб покрити свої витрати на операції вузлів.

У такому випадку мережа видає більше SHM операторам вузлів, ніж вона заробляє з комісій за транзакції, що призводить до збільшення обсягу SHM в обігу і зростання інфляції. Якщо дохід мережі більший за витрати мережі, відбувається видаток у дефляцію. У цьому випадку мережа генерує більше прибутку, ніж потрібно для покриття своїх витрат на операції вузлів. Оскільки всі комісійні винагороди спалюються, мережа стає дефляційною, зменшуючи обсяг SHM в обігу. У випадку, коли дохід мережі дорівнює витратам мережі, настає рівновага видатків. В цьому випадку мережа працює в збалансованому фінансовому стані, утримуючи стабільний обсяг токенів без збільшення або зменшення.

Зміни параметрів, які контролює FDAO, можуть впливати на один із цих станів мережі, забезпечуючи ефективну роботу та плавні зміни. Метою даного проєкту є створення умов, аби вартість транзакції була максимально малою. Якщо вартість монети 1$ та мережа не завантажена, то вартість транзакції становитиме 0,0001$. В нашому випадку можливо здійснити лише симуляцію транзакції та виконати приблизні розрахунки, адже проєкт знаходиться на стадії розробки, і ми не можемо точно дізнатись ціну SHM, тому всі розрахунки були проведені в тестовому режимі. Також слід обговорити роль статичних симуляцій на наочному прикладі. На лівій частині рисунку 3.1 зображено приклад того, що мережа відзначається позитивним доходом і дельтою, що свідчить про те, що вона генерує

більше прибутку від комісій за транзакції, ніж витрачає на оплату вузлів для забезпечення роботи мережі. У такому випадку мережа проявляє дефляційні тенденції, оскільки вона спалює більше SHM з комісій за транзакції, ніж виділяє операторам вузлів.

На правій частині рисунку 3.1 зображено приклад того, як зміна одного з параметрів, що контролюється FDAO, може перемістити мережу в інший режим. При зміні винагороди для вузла $/год з $1 до $1.2 так, щоб урівноважити доходи та витрати мережі, ми досягаємо рівноваги обсягу SHM в обігу мережі.

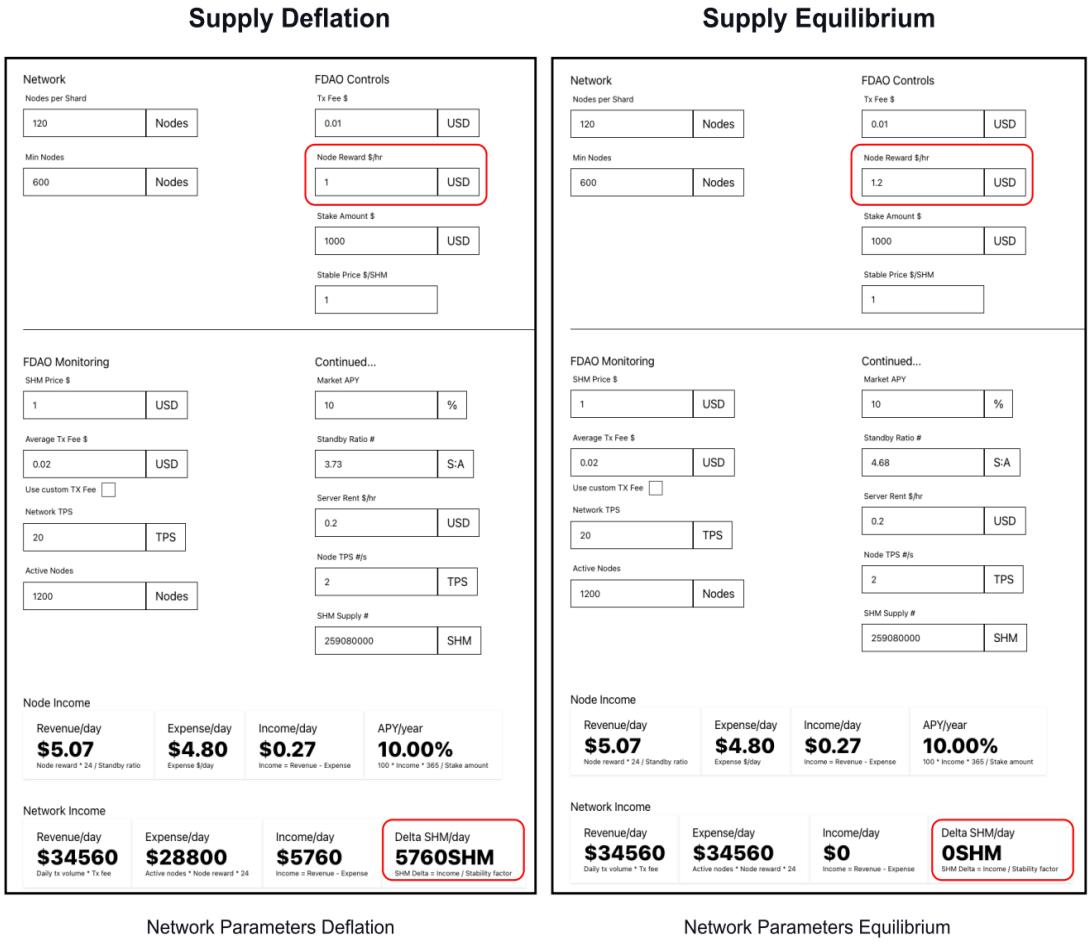

Рисунок 3.1 - Приклад статичних симуляцій

На лівій частині рисунку 3.2 зображено приклад того, як зміна іншої ключової змінної, яку контролює FDAO (комісія за транзакцію $), може вплинути на режим виділення. В даному випадку зміна комісії за транзакцію $ привела до зміни стану

мережі з стану рівноваги на правому зображенні вище до стану інфляції. Після цієї зміни мережа виділяє більше SHM через винагороду вузлів, ніж спалює з отриманих комісій за транзакції.

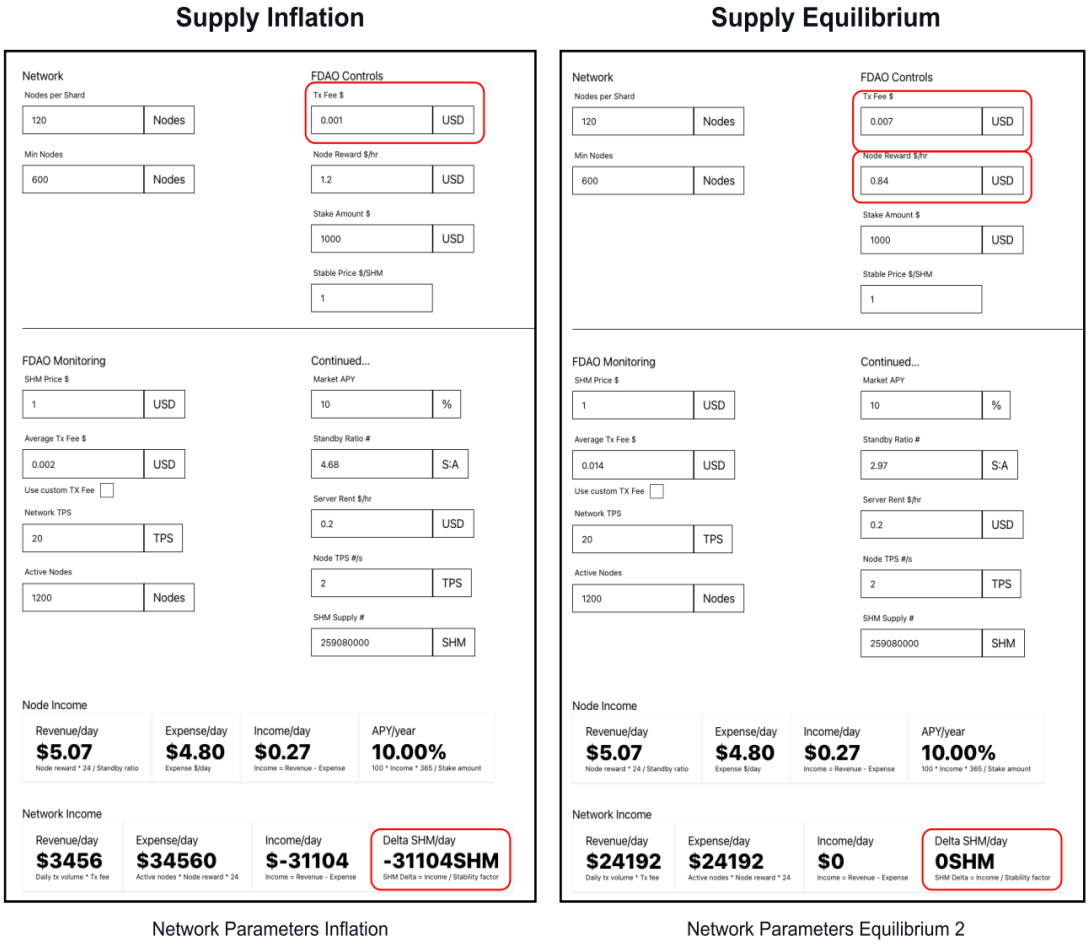

Рисунок 3.2 - Приклад статичних симуляцій

На правій частині рисунку 3.2 зображено приклад того, як зміни контрольованих параметрів FDAO можуть впливати на стан рівноваги обсягу. У цьому випадку змінні комісії за транзакцію $ та винагороди для вузла $/год використовуються для балансування доходів та витрат мережі (проведення більшої кількості сценаріїв зміни параметрів також можливо здійснити).

Отримана кількість монет розподіляється між різними категоріями. Розглянемо на графічному прикладі кількість монет в обіході та для чого вони використовуються (Рис 3.3).

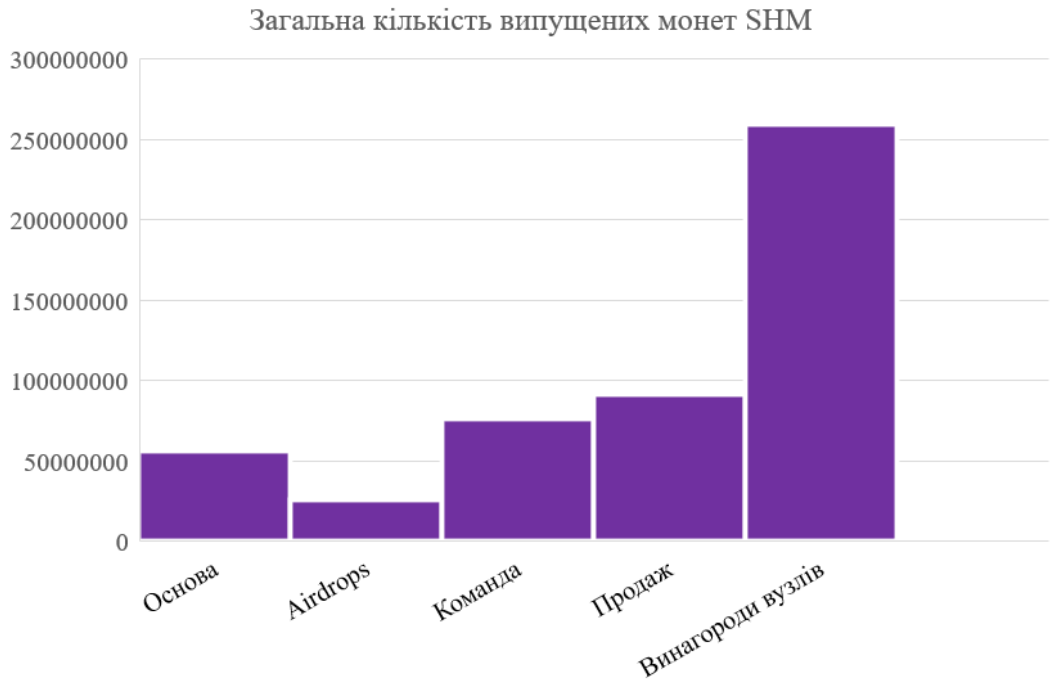

Рисунок 3.3 - Загальна кількість випущених монет SHM

Дані облікові записи отримають SHM відразу після запуску Genesis / mainnet: фондовий рахунок 11% від 508 млн.; 55,88M SHM; стає доступним після запуску основної мережі. На екосистему та Airdrops припадає 5% від 508 млн; 25,4M SHM; стає доступним після запуску основної мережі. Наступні облікові записи почнуть отримувати SHM через 3 місяці (90 днів) після запуску основної мережі 730 щоденними платежами: командний рахунок 15% від 508 млн; 76,2M SHM; приблизно 104 383 SHM на день через 90 днів. Рахунок продажу 18% від 508 млн; 91.44M SHM; приблизно 125 260 SHM на день через 90 днів. Решта 51% відкладено для винагород за вузли; ці монети створюються, коли їх надають, починаючи з запуску основної мережі, на основі вибраного нами налаштування винагороди вузла.

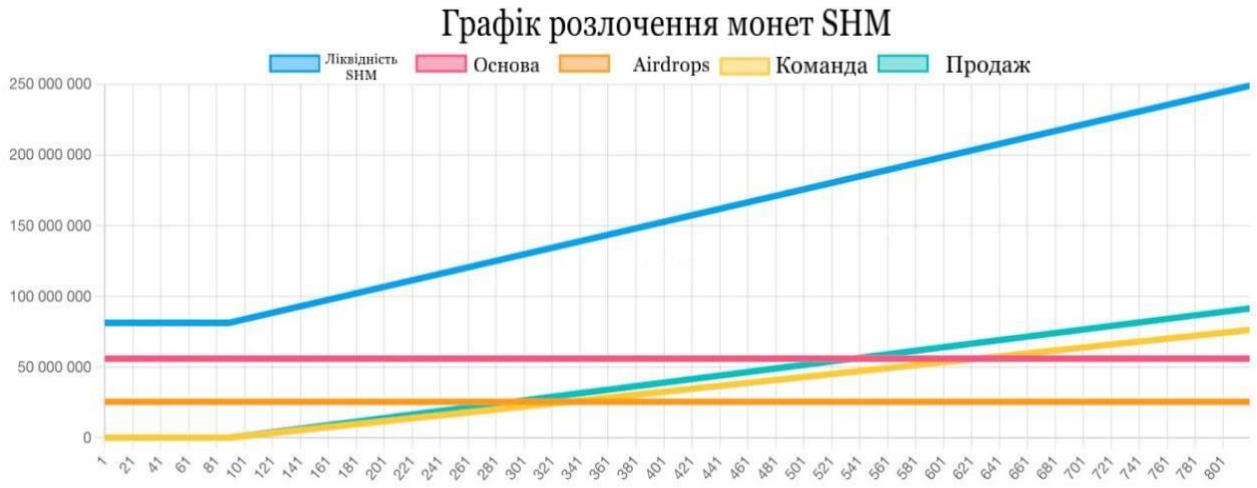

Рисунок 3.4 - Графік розлочення монет SHM

На графіку вище (Рис 3.4) показано ліквідну пропозицію SHM протягом 820 днів після створення мережі, це охоплює весь період набуття права команди та продажу SHM. Це не включає 51% пропозиції SHM, яка буде використана для винагороди за вузли.

3.2 Проблеми та недоліки блокчейну Shardeum

В ході проведеного нами дослідження було виявлено такі проблеми та недоліки блокчейну Shardeum (Рис 3.5, 3.6, 3.7).

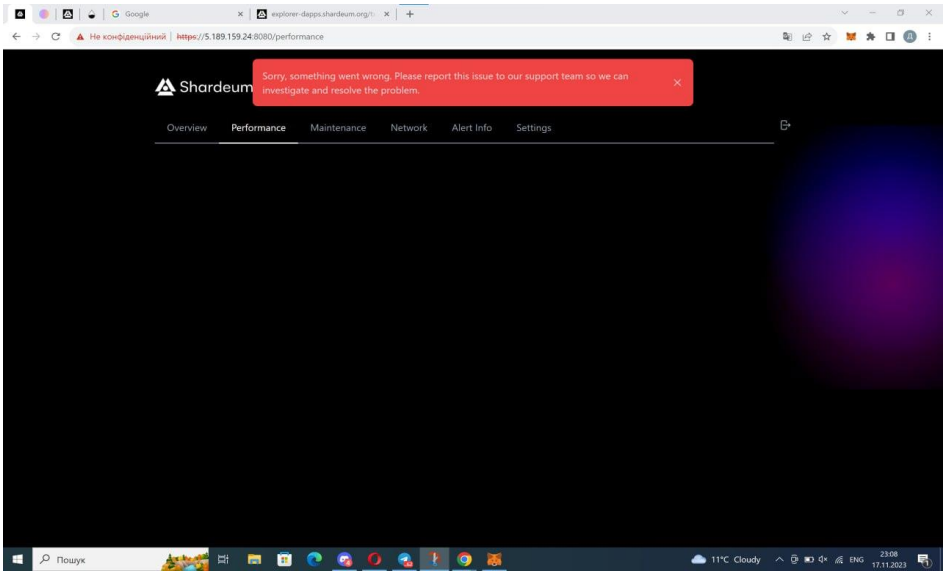

Рисунок 3.5 – Нестабільність роботи проєкту Shardeum

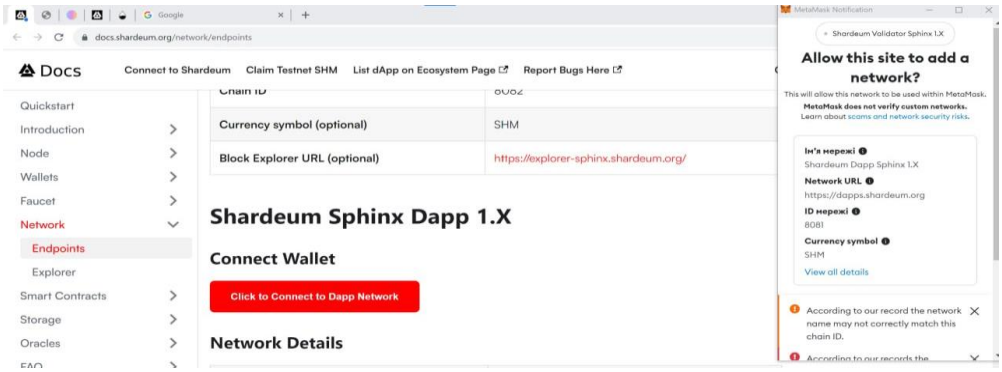

Рисунок 3.6 –Неможливість підключення до мережі блокчейну Shardeum

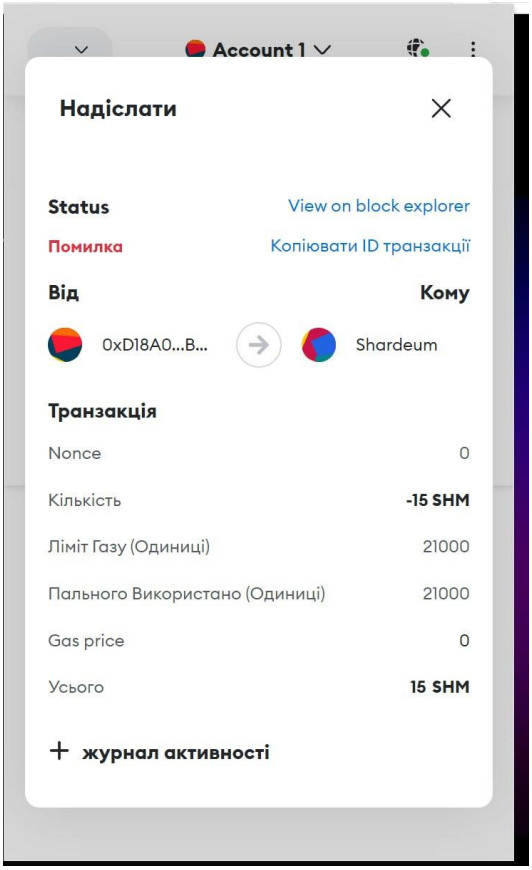

Рисунок 3.7 – Збої роботи мережі вузлів-валідаторів

З вище продемонстрованих рисунків випливають основні недоліки проєкту:

- постійна нестабільність роботи блокчейну;
- періодичні збої роботи мережі вузлів-валідаторів;
- часта неможливість підключення до мережі блокчейну Shardeum;
- систематична затримка транзакцій.

Розглянемо детальніше недоліки роботи досліджуваної мережі, три перші проблеми можна обґрунтувати досить коротко пояснивши це таким чином. Нестабільність процесу призводить до того, що валідатори не можуть надавати достатню кількість потужності для проводження транзакцій і за рахунок цього ми бачимо постійні збої під час роботи мережі, адже від кількості валідаторів напряму залежить стабільність роботи проєкту.

Мінімізація затримки транзакцій вказує на системну здатність зменшувати час між передачею та отриманням даних настільки, наскільки це можливо, впливаючи на практичність взаємодії з користувачем. Зниження часу затримки стає ключовим аспектом сучасних технологій, і воно широко оптимізоване для великої кількості галузей, включаючи промисловість блокчейн. Сфера використання може бути різною, починаючи від геймінгу та закінчуючи фінансовою торгівлею або телекомунікаціями, низька затримка стає важливим елементом для додатків та систем реального часу, які вимагають негайного відгуку.

Прикладом може слугувати важливість низької затримки у високочастотній та алгоритмічній торгівлі в фінансовій галузі, де навіть мілісекунди можуть суттєво впливати на позицію трейдера. У світі онлайн-ігор низька затримка є критичною, вона не дозволяє гравцям швидко та ефективно реагувати в іграх.

Затримка у сфері блокчейну - це загальний час, який витрачається на виконання переказу від моменту подання реальної транзакції в мережу блокчейну до обробки та підтвердження транзакції мережею. Важливо розуміти, що затримка та час виконання переказу тісно пов'язані у світі блокчейну, хоча це не одне й те саме. Остаточність вказує на незмінність підтвердженої операції, яка була додана до мережі. Таким чином, час виконання транзакції представляє собою загальний проміжок часу від подання реального платежу в мережу блокчейн до завершення дії системою. На цьому етапі транзакція вважається остаточною і не може бути змінена. Отже, дуже низька затримка та остаточність мають вирішальне значення не лише для розширення мережі, але й для обробки дуже великої кількості транзакцій за секунду (TPS).

Також слід відзначити, що затримка та масштабованість взаємопов'язані, але не тотожні. Низька затримка спрямована на мінімізацію часу, необхідного для обробки окремих транзакцій, тоді як висока пропускна здатність або масштабованість (зазвичай вимірюється в TPS) підкреслює здатність мережі блокчейну обробляти великий обсяг транзакцій одночасно.

Централізовані мережі, включаючи приватні блокчейни, зазвичай демонструють меншу затримку в порівнянні з децентралізованими мережами блокчейнів. Основною причиною цього відмінного часу затримки є різна архітектура та механізми обробки, які застосовуються в цих двох типах систем. Централізовані сервери, що мають лише одну юридичну особу чи організацію, можуть ефективно та оперативно обробляти та підтверджувати транзакції, оскільки не виникає потреби в узгодженні дійсності кожної транзакції серед різних сторін. Час затримки в централізованих системах переважно залежить від великої кількості факторів, таких як швидкість та потужність апаратного забезпечення сервера, ефективність програмного забезпечення та стан мережі. Крім того, об'єкти, такі як балансування навантаження та обслуговування мережі, разом із методами вертикального масштабування, що включає розширення обчислювальної потужності апаратного забезпечення системи, сприяють вирішенню питання часу затримки.

Розв'язання трилеми щодо масштабованості стає викликом в індустрії блокчейну. Децентралізовані мережі розподіляють навантаження між вузлами по всьому світу, досягаючи консенсусу щодо транзакцій і записуючи їх в розподілену книгу-блокчейн. Важливе значення для публічних мереж мають алгоритми консенсусу та обмеження масштабування, оскільки вони формують основні принципи безпеки та децентралізації у світі блокчейну. Блокчейн-платформи гнучко адаптують розміри блоків відповідно до мережевого навантаження та використовують консенсусні алгоритми. Більші блоки забезпечують значно кращий обсяг транзакцій, але існує ризик централізації та атак. Наприклад, Біткоїн надає перевагу безпеці перед смарт-контрактами. У змаганні за комерційне використання Ethereum розширює можливості блокчейну з використанням смарт-

контрактів. Мережі часто віддають перевагу гібридному розміру блоків, що дозволяє обробляти більше транзакцій, утримуючи розмір, щоб уникнути централізації та атак. Недоліком цього підходу є введення затримок та низької швидкості, зробивши децентралізовані блокчейни менш придатними для застосування у реальному часі, таких як онлайн-ігри, ланцюги поставок, телекомунікації та охорона здоров'я. Спостерігається змагання між мережами в пошуку рішення трилеми блокчейну - підтримки безпеки, децентралізації та масштабованості одночасно.

Затримка та ступінь завершеності мають обернено пропорційний вплив на пропускну здатність. Ключовим фактором є те, що зі збільшенням часу затримки та завершеності пропускна здатність зменшується, що обмежує здатність мережі обробляти велику кількість транзакцій за секунду (TPS). Це спостерігається як у традиційних системах, так і в мережах, що базуються на технології блокчейн, принаймні на більш фундаментальному рівні. Проте затримка в мережі блокчейн має велику кількість рухомих частин, таких як смарт-контракти та механізми консенсусу, які намагаються забезпечити реальні рішення без посередників. Вони розраховані на високий рівень автоматизації через кодування смарт-контрактів. Зниження затримки відіграє більш активну та важливу роль, ніж, наприклад, вимоги до пропускної здатності, коли розглядається масштабованість та пропускна здатність мережі блокчейн. Навіть при нижчій пропускній здатності даних, мережа блокчейн може ефективно функціонувати за умови, що вона має вбудовану оптимальну архітектуру.

Високі та непередбачувані витрати на транзакції є прямим наслідком вертикального масштабування низького TPS та невдачі вирішення трилеми масштабованості, особливо при збільшенні мережевого трафіку. Плата за газ стає значною, що особливо актуально при зростанні обсягів трафіку в мережі. Збільшена затримка призводить до збільшення витрат на обчислення та зв'язок, виконуючи взаємодію користувачів та розробників dapp повільнішою та витратнішою. Незважаючи на перспективу децентралізації, багато інструментів і сервісів використовуваних для створення децентралізованих екосистем

залишаються переважно централізованими. Щоб уникнути перенавантаження мережі та погіршення користувацького досвіду, публічні блокчейни часто вдаються до вертикального масштабування, що включає збільшення обчислювальної потужності їхніх вузлів. Проте цей підхід може зробити фінансово неефективним управління вузлами для звичайних користувачів, що в кінцевому підсумку призводить до зростання витрат на транзакції як для звичайних користувачів, так і для розробників, що створюють додатки.

MEV і передні ризики виникають внаслідок прозорого реєстрування транзакцій у публічних блокчейнах. На фоні обмежень масштабування, налаштованих самою системою, валідатори виявляють мотивацію приділяти перевагу транзакціям із високою комісією, переймаючись обмеженням мережі та намагаючись уникнути перевантаження. Однак виникає проблема, коли валідатори вчиняють навмисні дії, спрямовані на використання великої ціни транзакцій, володіючи можливістю маніпулювати ринком та збільшуючи вартість своїх послуг. Ситуація вдосконалюється, коли зловмисники використовують такий же метод, розміщуючи свою транзакцію перед великою, щоб скористатися різницею в комісіях. Це не лише дозволяє їм отримати несправедливу перевагу, але і фактично дає можливість маніпулювати ринком, завдаючи шкоду громадськості. Дослідження вказують на те, що витрати, понесені користувачами Ethereum через такі маніпуляції, лише у 2023 році перевищили 2 мільярди доларів. Втрати на крипторинку можуть бути набагато більшими. Знижена затримка та негайне завершення стають ще важливішими, оскільки для зловмисників все складнішим є визначення транзакції до їхнього підтвердження у блокчейнах. Блокчейни з низькою затримкою здатні швидше обробляти транзакції, залишаючи зловмисникам менше часу на їх перегляд та використання. Нестабільність часу підтвердження транзакцій у мережі робить стратегії максимального використання автономних протоколів на основі часових позначок непрактичними.

Успіх масового впровадження блокчейнів і відповідних програмних додатків невіддільно пов'язаний із задоволенням користувачів (UX) та мінімізацією транзакційних витрат. Поки екосистемі блокчейну не вдається досягти цих цілей

через архітектурні особливості. У той час, як централізовані системи вдавалися до різних методів зменшення затримок, таких як CDN, периферійні обчислення та розгортання потужних центрів обробки даних по всьому світу, децентралізовані системи блокчейну стикаються з високою затримкою та низькою кінцевістю.

Основна мета - надати обчислювальні дані та сховище користувачеві, роблячи відповідь та час завантаження миттєвими в світі, де вимагається обробка даних у режимі реального часу. Це необхідно для відповіді на потреби таких галузей, як штучний інтелект, автономні транспортні засоби та алгоритмічна торгівля. Наприклад, децентралізовані криптобіржі (DEX), які використовують смарт-контракти, стикаються із складнощами через велику затримку та низьку кінцевість порівняно з централізованими біржами (CEX), що використовують централізовані протоколи. Це призводить до повільної обробки та підтвердження транзакцій, а також ризику скасування підтверджених транзакцій у майбутньому. Такі аспекти стають проблемою для трейдерів DEX, які потребують швидких операцій і миттєвого розрахунку. Це призводить до помилок та поганого досвіду користувача, що, в свою чергу, впливає на ліквідність DEX та високої волатильності цін на криптовалюту.

Атаки на безпеку є серйозною загрозою для блокчейнів рівня 1 (L1), які прагнуть забезпечити високий рівень безпеки та децентралізації. Незважаючи на базовий захист, рішення та застосунки, побудовані на таких блокчейнах, можуть залишатися вразливими через врахування потреб користувачів та їхнього досвіду користувача (UX), що може піддавати сумніву децентралізацію та безпеку L1. Загрози безпеці здебільшого виявляються у формі атак фішингу, зловмисного програмного забезпечення та DoS-атак, що стає особливо актуальним навіть для нових ланцюжків L1, які спрямовані на масштабованість та ефективність газу. Наприклад, DoS- і DDoS-атаки можуть призвести до переповнення мережі великою кількістю непродуктивних транзакцій за допомогою ботів, що може призвести до сповільнення або навіть недоступності для легітимних користувачів. Низька затримка може виявитися корисною в зменшенні цього ризику, так як зловмисникам важче перевантажити мережу, надсилаючи більше транзакцій [21].

В основі Shardeum лежить концепція консенсусу на рівні транзакцій, а не блоків, що дозволяє обробляти транзакції паралельно за допомогою динамічного шардингу із затримкою всього в кілька секунд. Валідатори на Shardeum використовують високий рівень справедливості, перевіряючи та обробляючи транзакції в почергово. Це унеможливлює практику віртуального фронтраннінгу (MEV) та робить початкові транзакції непрактичними, що сприяє зменшенню затримок в мережі. Кожна підтверджена транзакція на Shardeum має негайну остаточність, уникнення необхідності чекати підтвердження кількох блоків. Це новаторське рішення, що гарантує остаточність без затримок. Сегментування стану на Shardeum адаптивно регулюється в залежності від навантаження, що дозволяє обробляти транзакції, які впливають на кілька шардів, одночасно із затримкою всього в кілька секунд. Механізм консенсусу Shardeum підсилює мережеву безпеку та децентралізацію за допомогою регулярної ротації вузлів перевірки, забезпечуючи рівномірний розподіл робочого навантаження. Динамічне сегментування стану дозволяє Shardeum лінійно масштабуватися горизонтально, забезпечуючи високу продуктивність та передбачуваність навіть при складних транзакціях смарт-контрактів.

Shardeum прагне перетворити технологію блокчейн, надаючи швидкі та ефективні рішення для обробки транзакцій, забезпечення безпеки і надійності. Коротко кажучи, Shardeum революціонізує можливості звичайних осіб та комп'ютерів, які можуть стати вузлами у мережі, забезпечуючи низьку та сталу комісію. Це відзначається сталим забезпеченням високоякісного користувацького досвіду, що стає звичним для нас у традиційних мережах Web2. Лінійна масштабованість Shardeum не обмежується лише обробкою транзакцій, вона розповсюджується і на прикладні програм, які працюють в його мережі, забезпечуючи здатність ефективно та швидко функціонувати навіть при зростанні мережі.

3.3 Рекомендації для вдосконалення блокчейну Shardeum

Оптимізація консенсусу стоїть на передовому місці функціональності та ефективності блокчейн-мережі. Перш за все, безперервне вдосконалення алгоритмів консенсусу націлене на забезпечення швидкого та ефективного підтвердження транзакцій у мережі. Це є надзвичайно важливим в умовах високо-динамічних блокчейн-мереж, де кожна транзакція потребує миттєвого опрацювання задля досягнення оптимального користувацького досвіду. Покращення алгоритмів консенсусу дозволяє мережі ефективніше досягати єдиної думки та узгоджувати транзакції значно зменшуючи час, необхідний для цього процесу. Швидке підтвердження транзакцій є ключовим елементом, оскільки це дозволяє мережі збільшити пропускну здатність та забезпечити негайну відповідь на запити учасників мережі. Також важливо активно розглядати можливість впровадження новаторських методів консенсусу. Це відкриває двері для експериментів з передовими технологіями, такими як Proof of Stake (PoS) та іншими продуктивними і безпечними алгоритмами, які можуть виявитися ефективнішими порівняно з традиційними методами. Постійне дослідження та впровадження інновацій сприяє створенню більш гнучких та вдосконалених механізмів консенсусу, що підтримують не лише поточні, а й майбутні потреби блокчейн-середовища. Такий підхід до вдосконалення консенсусу не лише сприяє підвищенню продуктивності та ефективності мережі, але також створює міцну основу для постійного росту та адаптації до непередбачуваних змін у світі криптовалют. Як результат, мережа готова відповідати високим стандартам та вимогам сучасного блокчейн-сектору. Подальше зменшення затримок в обробці транзакцій також слугує ключовим аспектом для підвищення продуктивності та динамічності блокчейн-мережі.

Другим важливим аспектом покращення роботи блокчейну є оптимізація консенсусу, спрямована на цільове скорочення часу між моментом надсилання транзакції та її підтвердженням, це невід'ємний фактор для високонавантажених

мереж, де кожна мілісекунда стає вирішальною для досягнення успіху. Оптимізовані алгоритми консенсусу реалізують цю мету, впливаючи на загальний час обробки транзакцій. Зокрема, вдосконалені механізми дозволяють прискорювати підтвердження транзакцій, ефективно скорочуючи затримки у критичні моменти. Це набуває особливого значення у високонавантажених мережах, де потрібно мінімізувати час обробки для забезпечення миттєвого та ефективного виконання транзакцій. У сучасному динамічному світі блокчейнів, де конкуренція, швидкість та надійність є надзвичайно важливими, оптимізовані алгоритми консенсусу стають вирішальним інструментом для досягнення виняткової ефективності. Зменшення затримок сприяє поліпшенню взаємодії з користувачами, забезпечуючи оперативну реакцію на їхні запити та операції. Такий підхід до оптимізації консенсусу визначає мережу як високоефективну платформу, здатну конкурувати в найбільш вимогливих умовах криптосередовища.

Третім не менш важливим аспектом удосконалення консенсусу є саме ефективна масштабованість, що слугує важливим вектором для забезпечення стійкого та неперервного розвитку блокчейн-мережі. Вдосконалення алгоритмів консенсусу в цьому контексті відіграє ключову роль у створенні можливостей для легкого масштабування, що призводить до послідовного зростання обсягу транзакцій та взаємодії всередині мережі. Оптимізовані алгоритми консенсусу, націлені на ефективну масштабованість, здатність більш ефективно взаємодіяти із збільшенням обсягу транзакцій. Це стає особливо важливим у контексті розвитку блокчейн-технологій, оскільки великий обсяг транзакцій свідчить про зростання популярності та широкого прийняття мережі на глобальному рівні. Збільшення обсягу транзакцій, що призводить до зменшення впливу на продуктивність мережі, має стратегічне значення для її стійкості та конкурентоспроможності. Оптимізовані алгоритми консенсусу, спрямовані на ефективну масштабованість, визначають мережу як гнучку та адаптивну, готову до викликів майбутнього та здатну забезпечити комфортну і безперебійну обробку навантаження будь-якого розміру. Такий підхід сприяє створенню сприятливого середовища для розвитку та прийому технології блокчейн в широкому спектрі використання.

Четвертий аспектом є стійкість до атак, він надає високоефективному консенсусу критичну роль у гарантуванні непохитної безпеки та стабільності блокчейн-мережі. Оптимізовані алгоритми консенсусу в цьому випадку функціонують як потужний щит, захищаючи систему від різноманітних видів атак, забезпечуючи надійність операцій та унеможливлюючи спроби саботажу. Ефективний консенсус допомагає уникнути проблем, пов'язаних із зміщенням (fork) мережі, що може виникнути внаслідок розбіжностей у вузлах стосовно стану мережі чи обробки транзакцій. Внаслідок таких конфліктів система може розділитися на дві або більше гілки, порушуючи єдність мережі. Високоефективний консенсус сприяє швидкому вирішенню конфліктів та відновленню єдності мережі, забезпечуючи стабільну та неперервну роботу. Крім того, ефективний консенсус грає ключову роль у протидії атакам з багатократним витрачанням (double-spending), що представляє собою одну з ключових загроз для децентралізованих фінансових систем. Здатність ефективно обробляти транзакції та швидко підтверджувати їхню легітимність дозволяє ефективно запобігти спробам повторного витрачання одних і тих самих коштів, зробивши мережу більш відсутньою до атак та гарантуючи надійність фінансових операцій. Такий високий рівень стійкості до різних видів атак формує систему як максимально надійну та стійку до небажаних втручань.

П'ятий аспект, який висвітлює використання інноваційних методів консенсусу, пропонує прогресивний погляд на подальший розвиток блокчейн-мережі. Активне вивчення можливостей впровадження передових технологій, таких як PoS (Proof of Stake), PoA (Proof of Authority), або DAG (Directed Acyclic Graph), визначає ключовий етап для оптимізації та вдосконалення ефективності мережі. Використання консенсус-методів, які виходять за межі звичайних підходів, розглядається як важлива можливість для підвищення продуктивності та забезпечення більшої ефективності мережі. Наприклад, PoS дозволяє вузлам, що володіють криптовалютою, ставати валідаторами та отримувати блоки для включення до ланцюжка. Це сприяє економії енергії та ресурсів мережі, а також швидшій та більш ефективній обробці транзакцій. PoA, в іншому контексті,

базується на авторитеті конкретних вузлів з певними привілегіями, що зменшує ризик виникнення конфліктів та підвищує стійкість мережі до різних видів атак. Впровадження інноваційних методів консенсусу в мережі стає важливим кроком у напрямку оптимізації та адаптації до сучасних технологічних викликів. Це надає можливість блокчейну підтримувати високу продуктивність та ефективність, щоб відповідати потребам розвиваючогося світу криптовалют та децентралізованих систем.

Отже, постійне удосконалення алгоритмів консенсусу становить ключовий етап у розвитку Shardeum, спрямований на створення високофункціональної, стійкої та високопродуктивної блокчейн-мережі. Цей процес відкриває унікальні можливості для системи, що дозволяє їй відповідати найновішим вимогам та викликам сучасного криптовалютного оточення.

Перш за все, прагнення до надійності є однією з ключових характеристик, яку Shardeum активно розвиває через постійне удосконалення алгоритмів консенсусу. Мережа вдосконалюється з метою досягнення високого рівня відновлюваності та стійкості, гарантуючи безперебійну та надійну роботу навіть у випадку значного обсягу транзакцій та змінних умов.

Ефективність є ще однією важливою складовою, яку мережа отримує завдяки оптимізації алгоритмів консенсусу. Використання шард, які дозволяють розподілену обробку транзакцій, робить Shardeum високоефективною та економічною платформою для взаємодії між учасниками мережі. Поняття високої продуктивності в контексті Shardeum означає не лише швидке підтвердження транзакцій, але і готовність мережі адаптуватися до різних завдань та викликів. Систематичне удосконалення алгоритмів консенсусу дозволяє мережі впроваджувати нові функції та поліпшення, сприяючи інноваційному розвитку. Узагальнюючи, завдяки постійному удосконаленню алгоритмів консенсусу, Shardeum визначається як блокчейн-мережа, що володіє високою ефективністю, стійкістю та надійністю, готовою відповідати високим стандартам та вимогам сучасного криптовалютного середовища.

ВИСНОВКИ

У даній магістерській роботі було розглянуто всі можливі способи використання технології блокчейн. В першому розділі ми розглянули ключові аспекти та компоненти блокчейну. Ми прослідкували еволюцію криптовалют, основоюяких є технологія блокчейн, вивчили значення криптовалютрних бірж, детально вивчили основні аспекти та складові децентралізованого розповсюдженого розділеного реєстру, такі як консенсус і протоколи консенсусу, структуру та організацію блоків, надали призначення криптогаманця та висвітлили різницю між криптомайнінгом і криптостейкінгом.

Блокчейн є розподіленим реєстром, що функціонує децентралізовано та реєструє операції із цифровими активами, які можуть включати в себе різноманітні об’єкти, від нерухомості, грошей та землі до нематеріальних активів, таких як патенти, авторські права та бренди. Використання цієї технології сприяє зменшенню ризиків і витрат всіх учасників ринку, а також прискорює виконання значної кількості платежів. У порівнянні з традиційними фінансовими установами, такими як комерційні банки, сервіси грошових переказів та кредитні центри, транзакції в блокчейні можуть здійснюватися лише за кілька секунд і не обтяжені значними комісійними витратами. Ця технологія також дозволяє користувачам надсилати гроші без географічних та часових обмежень. Операції виконуються швидко, а підтвердження транзакцій відбувається від кількох хвилин до декількох годин. Важливим елементом є незворотність усіх платежів у блокчейні, що важливо для захисту від онлайн – шахрайства.

Криптовалюта відкриває доступ до фінансових продуктів і сервісів, забезпечуючи свободу від черг у банках і мінімізуючи паперову взаємодію. Управління цифровими активами можна здійснювати за допомогою комп’ютера або смартфона через спеціальний додаток, що дозволяє інвестувати в активи великих компаній та розподіляти кошти більш ефективно. Після проведеного

аналізу вивченої інформації, ми виділили ключові принципи, на яких ґрунтується технологія розподіленого реєстру.

В другому розділі магістерської кваліфікаційної роботи ми виконали дослідження та встановлення мережевого вузла від проєкту Shardeum. Ми виступили в ролі валідатора. Важливо зазначити, що користувачі, які блокують більше монет мають більше шансів стати валідаторами, що покращує їхні шанси на обрання для підтвердження нових транзакцій. Наша роль валідатора із меншою кількістю монет також дозволила успішно підтвердити транзакцію та отримати відповідні винагороди. Проєкт Shardeum є досить доступним у використанні та надає можливість користувачам здійснювати транзакції з мінімальною кількістю монет.

У третьому розділі ми окреслили шляхи підвищення ефективності даної технології. Неперервне вдосконалення алгоритмів консенсусу є вирішальним етапом у розвитку Shardeum, спрямованим на створення блокчейн-мережі, що є високофункціональною, стійкою та високопродуктивною. Цей процес відкриває унікальні можливості для системи, що дозволяє їй відповідати найновішим вимогам та викликам сучасного криптовалютного оточення. Прагнення до надійності є однією із ключових характеристик, яку Shardeum активно розкриває через постійне удосконалення алгоритмів консенсусу. Мережа вдосконалюється для досягнення високого рівня відновлюваності та стійкості, гарантуючи безперебійну та надійну роботу навіть при значному обсязі транзакцій та змінних умовах. Ефективність є ще однією важливою складовою, яку мережа отримує завдяки оптимізації алгоритмів консенсусу. Використання шард, які дозволяють розподілену обробку транзакцій, робить Shardeum високоефективною та економічною платформою для взаємодії між учасниками мережі. Поняття високої продуктивності в контексті Shardeum означає не лише швидке підтвердження транзакцій, але і готовність мережі адаптуватись до різних завдань та викликів. Систематичне удосконалення алгоритмів консенсусу дозволяє мережі впроваджувати нові функції та поліпшення, сприяючи інноваційному розвитку. Узагальнюючи завдяки постійному удосконаленню алгоритмів консенсусу,

Shardeum визначається як блокчейн-мережа, що володіє високою ефективністю, стійкістю та надійністю готовою відповідати високим стандартам та вимогам сучасного криптовалютного середовища.

ПЕРЕЛІК ПОСИЛАНЬ

1. Антонопулос Андреас, Гевін Вуд. Освоюємо Ethereum. Створення смарт-контрактів та децентралізованих додатків.: Ексмо, 2021. 512 с.
2. Баранова О.К. Бабаш. О.В. Інформаційна безпека та захист інформації - 3-тє вид., перероб. та дод. - М.: ІНФРА-М, РІОР, 2016. 226 с.
3. Бутерін Віталік. Більше грошей: що таке Ethereum та як блокчейн змінює світ. - Individuum, 2023. 400 с.
4. Джуліан Хоспс. Про криптовалюту просто. Біткоїн, ефіріум, блокчейн, децентралізація, майнінг, ICO & Co, пер. М. Петруненко, 2019. 110 с.
5. Кудін А.М., Блокчейн і криптовалюти на основі "доказу точності». // Математичне та комп’ютерне моделювання. Серія: технічні науки: збірник наукових праць. Кам’янець-Подільський національний університет імені Івана Огієнка, 2017. 108 с.
6. Кудін А. М., Коваленко Б. А., Швідченко І. В. Технологія блокчейн: питання аналізу та синтезу / Кібернетика і системний аналіз, 2019. – Том 55. 172 с.
7. Кудін А.М., Ковальчук Л.В., Коваленко Б.А. Теоретичні засади та застосування блокчейн-технологій: імплементація нових протоколів консенсусу та краудсорсінг обчислень. // Математичне та комп’ютерне моделювання. Серія: Технічні науки: зб. наук. праць. Кам’янець-Подільський: Кам'янець-Подільськ. нац. ун-т імені Івана Огієнка, 2019. 108 с.
8. Кудін А.М., Селюх П.В. Асиметричні криптографічні протоколи з блокчейн-ядром: проблеми побудови та їх рішення / Фізико-математичне моделювання та інформаційні технології. – Львів: 2021. 180 с.
9. Кудь О., Кучерявенко М., Смичок Євген. Цифрові активи та їх економіко-правове регулювання у світлі розвитку технології блокчейн : монографія. Харків : Право, 2019. 384 с.
10. Лоран Лелу. Блокчейн від А до Я. Все про технології десятиріччя Блокчейн.: Ексмо, 2018. 256 с.
11. Могайар Уільям, Бутерін Віталік. Блокчейн для бізнесу.: Ексмо, 2018. 224 с.

12. Натаніел Поппер. Цифрове золото: неймовірна історія біткойна.: Пер. з. анг. - М.: Вільямс, 2016. 368 с.
13. Офіційний сайт біржі: https://p2p.binance.com (огляд Binance)
14. Офіційний сайт біржі: https://www.bybit.com (огляд ByBit)
15. Офіційний сайт біржі: https://www.kucoin.com (огляд KuCoin)
16. Офіційний сайт біржі: https://whitebit.com/ua (огляд WhiteBIT)
17. Офіційний сайт Shardeum: https://shardeum.org
18. Пол Вінья, Майкл Кейсі. Епоха криптовалют. Як біткоїн і блокчейн змінюють світовий економічний порядок.– М.: МІФ, пер. с анг. Е. Кондукової, 2017. 432 с.
19. Равал С. Децентралізовані програми. // Технологія Blockchain в дії: серія O'Reilly, 2016. 192 с.
20. Рябих А. Русова С. Як заробити на криптовалюті та блокчейні. Пояснюємо на пальцях.: Пітер, 2019. 256 с.
21. Сідак В. С., Артемов В. Ю. Забезпечення інформаційної безпеки в країнах НАТО та ЄС: Навчальний посібник. — К.: КНТ, 2007. 160 с.
22. Тапскотт Дон, Тапскотт Алекс. Технологія блокчейн. Те, що рухає фінансовою революцією сьогодні. Львів: Літопис, 2018. 488 с.
23. Ярочкин В. І. Інформаційна безпека: підручник для студентів вищих навчальних закладів. - М .: Академічний проект; Фонд «Світ», 2003. 640 с.
24. Chris Dannen. Introducing Ethereum and Solidity. — Brooklyn, New York, USA: Apress, 2017. 197 с.
25. Nakamoto Satoshi. Bitcoin: A peer-to-peer electronic cash system. Satoshi Nakamoto, 2008.
26. The Book of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto. e53 Publishing, LLC. 2014 p. 394 с.
27. Puthal D., Malik N. , Mohanty S. P., Kougianos E., and Das G., "Everything you Wanted to Know about the Blockchain", IEEE Consumer Electronics Magazine, Volume 7, Issue 4, July 2018. pp. 06– 14.

28. Consensus Algorithm — [Електронний ресурс]. – Режим доступу: https://whatis.techtarget.com/definition/consensus-algorithm (дата звернення 29.10.2023).
29. Хеш-функції – що це таке? [Електронний ресурс] – Режим доступу URL: https://www. https://habr.com/ru/articles/534596 (дата звернення 11.11.2023).
30. Puddu I., Dmitrienko A., Capkun S. How to forget without hard forks. IACR Cryptology. 2017. — [Електронний ресурс]. – Режим доступу URL: https://eprint.iacr.org/2017/106.pdf (дата звернення 12.11.2023).
31. Опис роботи Delegated Proof-of-stake — [Електронний ресурс]. – Режим доступу URL: https:// https://academy.binance.com/ru/articles/delegated-proof-of-stake-explained (дата звернення 15.11.2023).
32. Kwon J. Tendermint: Consensus without mining. — [Електронний ресурс]. – Режим доступу URL: https:// https://github.com/tendermint/tendermint/wiki/Block-Structure (дата звернення 15.11.2023).
33. Класифікація блокчейнів— [Електронний ресурс]. – Режим доступу URL: https://www.bitbon.space/ru/knowledge-base/distributed- ledger-technologies-blockchain/technological-aspects-of- blockchain/classification-of-blockchains (дата звернення 17.11.2023).
34. The Idea of Smart Contracts — [Електронний ресурс]. – Режим доступу URL: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html (дата звернення 17.11.2023).
35. Solidity — [Електронний ресурс]. – Режим доступу URL: https:// https://docs.soliditylang.org/en/v0.8.10 (дата звернення 20.11.2023).
36. Ethereum virtual machine — [Електронний ресурс]. – Режим доступу URL: https://ethereum.org/en/developers/docs/evm (дата звернення 22.11.2023).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

Для практичного застосування технології блокчейн я обрав дослідження та аналіз роботи мережевих вузлів від проєкту Shardeum на основі блокчейну Ethereum. Задля цього спочатку мені необхідно було встановити ноду (мережевий вузол) із дотриманням ряду вимог:

- постійне та стабільне підключення до інтернет-мережі;
- аналогічно постійно увімкнений комп'ютер;
- 250 GB SSD диску;
- чотирьохядерний процесор віком менше 10 років;
- 16 GB оперативної та 4 GB віртуальної пам'яті;
- для роботи на хостингу також необхідно 8 GB оперативної та 8 GB віртуальної пам'яті;
- операційна система ubuntu 20.4.

5

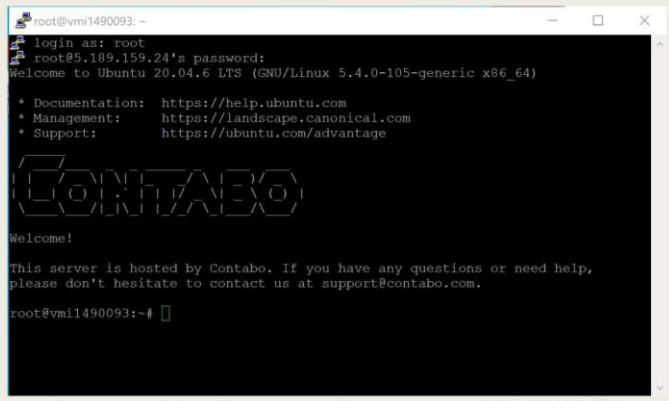

Рисунок 2.4 - Авторизація на сервері CONTABO

Рисунок 2.5 - Вдале інсталювання Docker

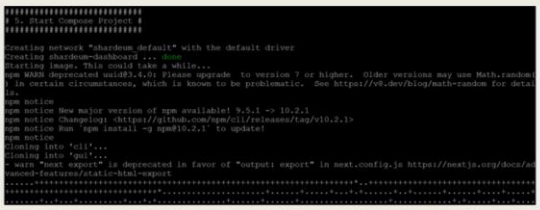

Рисунок 2.6 - Успішне встановлення ноди

6

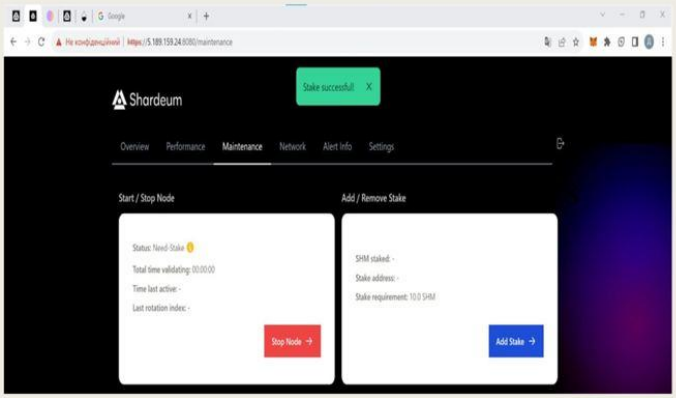

Рисунок 2.11 Успішний стейкінг монет SHM

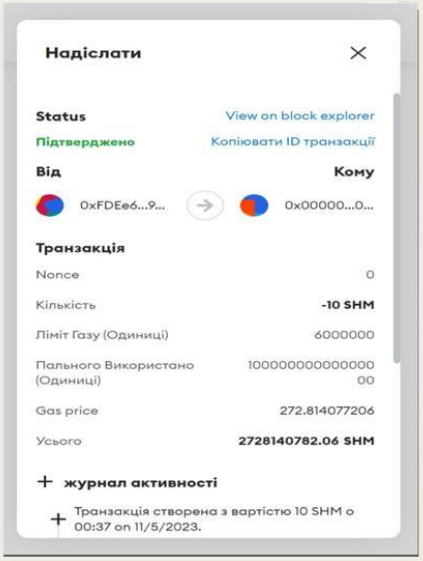

Рисунок 2.12 Успішна транзакція транспортування монет SHM

9

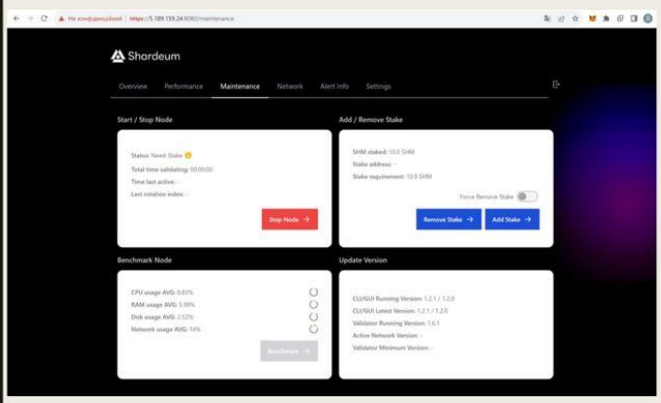

Рисунок 2.13 Успішне встановлення ноди Shardeum

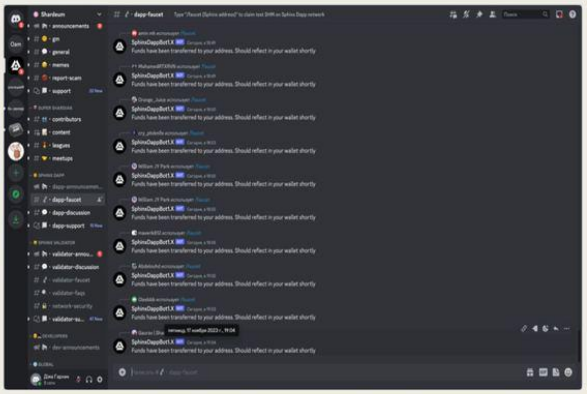

Рисунок 2.14 Discord каналі на гілці #spinx-faucet-1.5

10

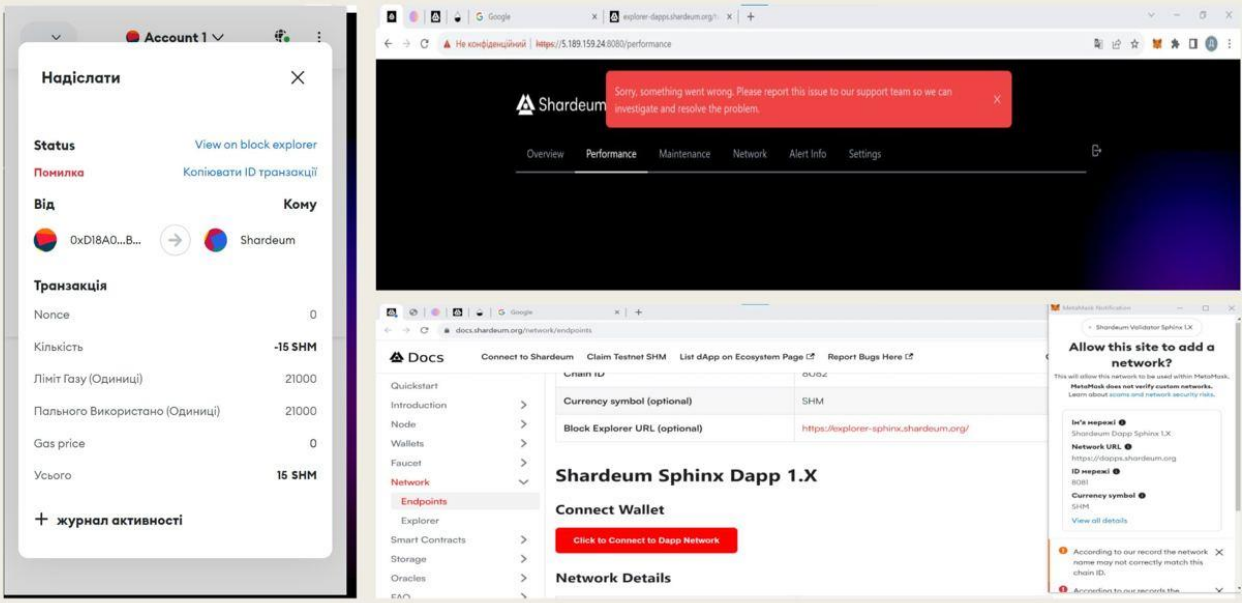

Рисунок 2.15, 2.16, 2.17 – Основні недоліки роботи блокчейну Shardeum

11

Проблеми та недоліки блокчейну Shardeum

В ході проведеного мною дослідження було виявлено такі проблеми та недоліки блокчейну Shardeum:

- постійна нестабільність роботи блокчейну;
- періодичні збої роботи мережі вузлів-валідаторів;
- часта неможливість підключення до мережі блокчейну Shardeum;
- систематична затримка транзакцій.

Рекомендації для вдосконалення блокчейну Shardeum

Нормалізувати роботу головного центру управління нодами у мережі Shardeum.

- Потрібно збільшити потужність серверів у мережі валідаторів.
- Забезпечити стабільну роботу даної технології.
- Збільшити кількість валідаторів для покращення пропускної можливості транзакції.

13