Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Методи побудови та захисту децентралізованих систем на основі технології блокчейну

(тема)

Виконав:

студент II курсу, групи СПм-22-5

Шевчук Є.В.
(прізвище, ініціали)

Спеціальність

123 «Комп'ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма

Системне програмування
(повна назва освітньої програми)

Керівник: доц. Федорченко В.М.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп'ютерна інженерія»
(код і повна назва)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
"____" _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Шевчуку Євгену Вадимовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Методи побудови та захисту децентралізованих систем на основі технології блокчейну

затверджена наказом по університету від " 01 " квітня 2024 р. № 257 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 15 червня 2024 р.

3. Вхідні дані до роботи

1) ДСТУ щодо обробки інформації;
2) нормативно правові та законодавчі акти України;
3) періодичні видання;
4) науково-методичні розробки вітчизняних та зарубіжних авторів;
5) літературні джерела;
6) матеріали практики.

4. Перелік питань, що потрібно опрацювати у роботі

1) аналіз предметної області;
2) аналіз основних вразливостей блокчейн;
3) проектування децентралізованого блокчейна з оптимальним захистом і ефективністю.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) Слайд-презентація – 22 слайди.

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Огляд структури децентралізованого		
	блокчейну	02.04.2024-13.04.2024	
2	Огляд вразливостей і атак на		
	децентралізований блокчейн	13.04.2024-27.04.2024	
3	Проєктування децентралізованого блокчейну		
	з оптимальними показниками захисту і		
	ефективності	27.04.2024-26.05.2024	
4	Перевірка чернетки кваліфікаційної роботи та		
	внесення змін до неї керівником	26.05.2024-01.06.2024	
5	Оформлення кваліфікаційної роботи	01.06.2024-05.06.2024	
6	Підготовка презентації та доповіді	05.06.2024-12.06.2024	
7	Рецензування роботи	12.06.2024-15.06.2024	

Дата видачі завдання 1 квітня 2024 р.

Студент _____
(підпис)

Керівник роботи _____ доц. Федорченко В.М.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 62 с., 16 рис., 1 дод., 35 джерел.

БЛОКЧЕЙН, ВРАЗЛИВІСТЬ, АТАКА, ДЕЦЕНТРАЛІЗАЦІЯ, ПРОЄКТУВАННЯ.

Метою кваліфікаційної роботи є проєктування децентралізованої блокчейн мережі, яка буде мати оптимальні параметри захисту від загроз і атак а також бути достатньо ефективною. Об’єктом дослідження є блокчейн. Предметом дослідження є децентралізована блокчейн мережа.

У ході виконання кваліфікаційної роботи проведено аналіз та опис предметної області, описано структуру рівнів децентралізованого блокчейна, проаналізовані основні вразливості і атаки на децентралізований блокчейн, спроектовано оптимальний блокчейн по показникам захисту і ефективності.

Результатами можуть користуватися архітектори децентралізованих блокчейн мереж для виявлення вразливостей їх мереж і проєктування більш надійних і оптимальних мереж

ABSTRACT

Master’s thesis: 62 pages, 16 figures, 1 appendices, 35 sources.

BLOCKCHAIN, VULNERABILITY, ATTACK, DECENTRALIZATION, DESIGNING.

The major goal of this thesis is to design a decentralized blockchain network that will have optimal protection parameters against threats and attacks, as well as be sufficiently efficient. The object of research is blockchain. The subject of research is a decentralized blockchain network.

In the course of the qualification work, an analysis and description of the subject area was carried out, the structure of the levels of the decentralized blockchain was described, the main vulnerabilities and attacks on the decentralized blockchain were analyzed, and the optimal blockchain was designed in terms of protection and efficiency indicators.

The results can be used by architects of decentralized blockchain networks to identify vulnerabilities in their networks and design more reliable and optimal networks

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

DDoS – розподілена атака відмови в обслуговуванні (англ., Distributed Denial-of-Service)

DeFi – децентралізовані фінанси (англ., decentralized finance)

DPoS – делигований доказ накопичення (англ., Delegated Proof of Stake)

IP – меж мережевий протокол (англ., Internet Protocol)

NFT – невзаємозаміняємий токен (англ., non-fungible token)

P2P – децентралізована мережка (англ., peer-to-peer)

PoS – доказ накопичення (англ., Proof of Stake)

PoW – доказ роботи (англ., Proof of Work)

RLP – префікс рекурсивної довжини (англ., Recursive-length prefix)

SHA – алгоритм хешування (англ., Secure Hash Algorithm)

TCP – протокол управління передачею (англ., Transmission Control Protocol)

TEE – довірене середовище виконання (англ., Trusted Execution Environment)

ВСТУП

Сьогодні блокчейн використовується в багатьох сферах, таких як:

- фінанси: децентралізовані фінанси (DeFi), смартконтракти, криптовалюти;
- логістика: відстеження ланцюгів постачання, запобігання контрафакту;
- охорона здоров'я: зберігання медичних записів, обмін даними;
- державне управління: цифрові ідентифікатори, голосування, прозорість урядових процесів.

Блокчейн – це не просто технологія, це нова парадигма довіри. Він дає нам можливість створювати децентралізовані системи, які не підлягають контролю жодної особи чи організації. Але той факт що її ніхто не контролює безпосередньо не означає що блокчейн неможливо якимось чином зламати. Оскільки ця технологія вже достатньо важлива для різних сфер діяльності, і часто пов’язана з фінансами дуже важливою стає тема розгляду методів побудови та захисту блокчейну, які як зменшать ризики втручання зловмисників в систему, так і вірогідно збільшать її продуктивність, а значить зменшить комісії для користувачів.

Вирішення проблеми захисту та оптимізації блокчейну дуже нагальне питання, не зважаючи на те що із року в рік технології захисту покращуються, ці технології достатньо молоді і чимало вразливостей буде знайдено в найближчому майбутньому, до того ж після створення блокчейн мережі, поміняти її архітектуру для забезпечення кращої безпеки стає доволі проблематично.

Метою цієї роботи є проєктування децентралізованої блокчейн мережі, яка буде мати оптимальні параметри захисту від загроз і атак а також бути достатньо ефективною. Об’єктом дослідження є блокчейн. Предметом дослідження є децентралізована блокчейн мережа.

1 АНАЛІЗ АРХІТЕКТУРИ І РІВНІВ БЛОКЧЕЙНУ

1.1 Конценпція блокчейну

Blockchain зобов’язаний своєю назвою тому, як він зберігає дані транзакцій – у блоках, пов’язаних разом, щоб утворити ланцюжок. З ростом кількості транзакцій зростає і блокчейн. Блоки записують і підтверджують час і послідовність транзакцій, які потім реєструються в блокчейні в межах окремої мережі, що регулюється правилами, погодженими учасниками мережі. «Кожен блок містить хеш (цифровий відбиток або унікальний ідентифікатор), пакети останніх дійсних транзакцій із мітками часу та хеш попереднього блоку. Попередній хеш блоку пов’язує блоки разом і запобігає зміні будь-якого блоку або вставці блоку між двома наявними блоками». Теоретично цей метод робить блокчейн захищеним від втручання [1-5].

Чотири ключові концепції блокчейну: Спільна книга. Спільна книга – це розподілена система записів, яка «тільки для додавання» використовується в бізнес-мережі. «Завдяки спільній книзі транзакції реєструються лише один раз, усуваючи дублювання зусиль, типове для традиційних бізнес-мереж». Дозволи. Дозволи забезпечують безпеку транзакцій, їх автентифікацію та можливість перевірки. «Завдяки можливості обмежувати участь у мережі організації можуть легше дотримуватися правил захисту даних, таких як ті, що передбачені в Законі про перенесення та підзвітність медичного страхування (HIPAA)» та Загальному регламенті ЄС щодо захисту даних (GDPR). Розумні контракти. Розумний контракт – це «угода або набір правил, які регулюють бізнес-операцію; він зберігається в блокчейні та виконується автоматично як частина транзакції». Консенсус. Завдяки консенсусу всі сторони погоджуються на транзакцію, перевірену мережею. Блокчейни мають різні механізми консенсусу, включаючи підтвердження частки, мультипідпис і PBFT (практична візантійська відмовостійкість). У кожній блокчейн-мережі є різні учасники, які виконують

такі ролі, зокрема: Користувачі блокчейну. Учасники (зазвичай бізнес-користувачі) з дозволами приєднуватися до мережі блокчейн і проводити транзакції з іншими учасниками мережі. Регулятори. Користувачі блокчейну зі спеціальними дозволами для контролю за транзакціями, що відбуваються в мережі. Оператори мережі блокчейн. Особи, які мають спеціальні дозволи та повноваження на визначення, створення, керування та моніторинг мережі блокчейн. Центри сертифікації. Особи, які видають і керують різними типами сертифікатів, необхідних для запуску дозволеного блокчейну.

Розглянемо просту схему блокчейна (рисунок 1.1), кожен блок має в собі хеш і хеш минулого блоку, цей хеш збирається із кореня дерева меркла яке існує для того щоб перевіряти всі минулі транзакції, також воно слугує у вигляді ідентифікатора блоку транзакцій.

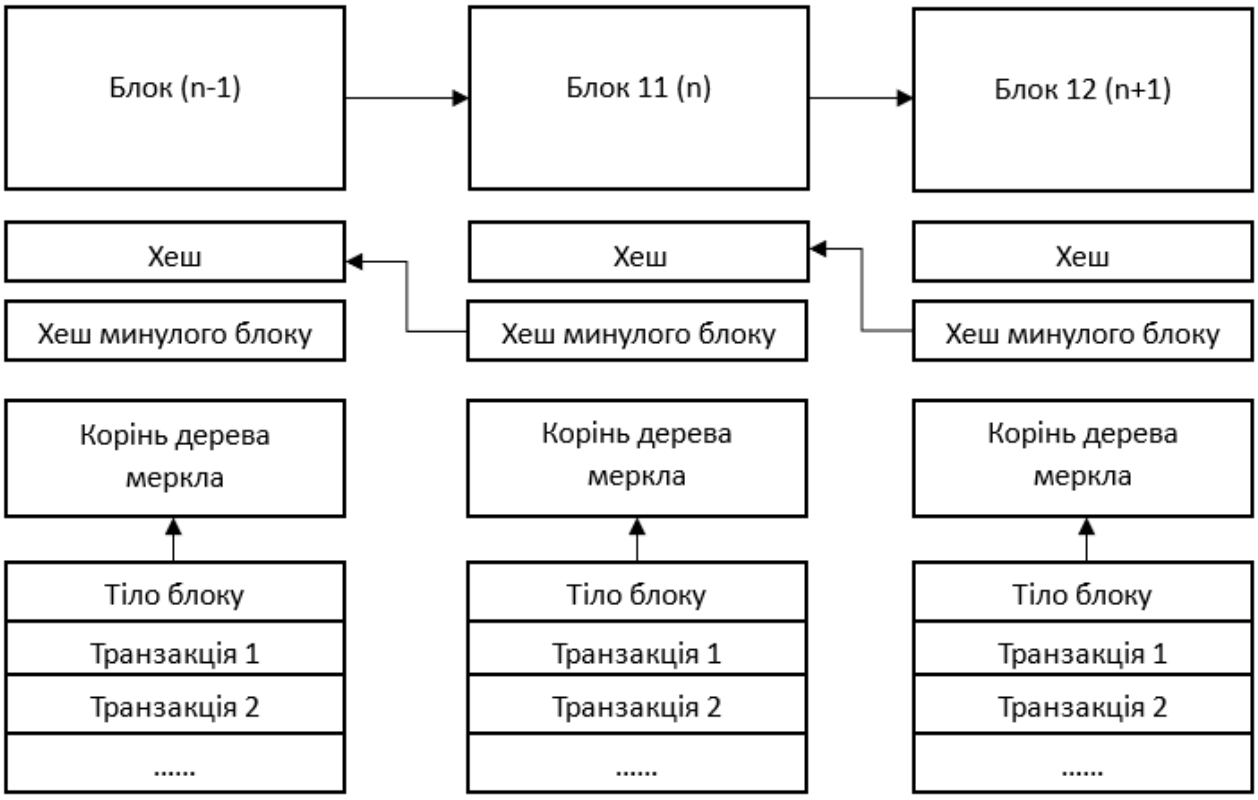

Рисунок 1.1 – Схема простого блокчейна

1.2 Рівні блокчейну

1.2.1 Прикладний рівень

Прикладний рівень є кінцевим продуктом усієї системи, що пропонує користувачам певні продукти, як-от гаманець, кредитування, ставки тощо.

Прикладний рівень починається зі смартконтракту, програмованого коду, який керує змінами станів. Він може функціонувати як умовне депонування, платіжний канал або сховище та відомий під різними назвами в різних екосистемах, як-от «програми» в Solana та «ланцюговий код» у Hyperledger. Розумні контракти є частою мішенню для хакерів, оскільки будь-яка критична помилка в їх коді може бути використана для отримання незаконної вигоди.

Зазвичай користувачі не взаємодіють зі смартконтрактом безпосередньо. Натомість вони покладаються на інтерфейс програми Web3 або API. Вебсайт Uniswap є прикладом децентралізованої програми, яка поєднує інтерфейс і розумні контракти.

1.2.2 Рівень послуг та додаткових компонентів

Сервісний рівень створює взаємозв’язок Web3, усуваючи перешкоди та забезпечуючи плавну взаємодію. Додаткові елементи включають децентралізовані автономні організації (DAO), які допомагають адмініструвати та комунікувати в таких мережах, як Arbitrum і Polygon, але відсутні в Bitcoin та Ethereum. Oracles з’єднує додатки Web3 з реальними даними про ціноутворення активів, сприяючи обчисленням поза мережею. Гарячі гаманці зберігають активи в мережі, але також служать точками доступу, наприклад, Metamask або Kaikas – рідний гаманець для Klaytn. І нарешті, дослідники блоків відстежують працездатність ланцюга,

допомагаючи виявляти технічні збої та порушення безпеки та завчасно пом’якшувати проблеми.

1.2.3 Рівень протоколу (консенсусу).

Механізм консенсусу – це саморегульований стек програмних протоколів, записаних у код блокчейну, який синхронізує мережу для узгодження стану цифрової книги. Це робиться шляхом підтримки єдиного набору даних – взаємно узгодженої версії історії транзакцій блокчейну – замість використання кожного вузла або комп’ютера в мережі для окремого збереження власної копії бази даних у повному обсязі. Попри те, що під час програмування мережевого стандарту верифікації слід враховувати різноманітні консенсусні механізми, кожен підхід спрямований на дискредитацію шахраїв у їхніх спробах заперечити записи [6, 7, 8].

Консенсус працює таким чином що вузли вводять дані з транзакції, що очікує на розгляд, а потім звітують зі статусом схвалення або відхилення, коли запит буде перехресно перевірено з його записами. Наприклад, якщо користувач намагається обробити транзакцію, використовуючи раніше витрачені монети, які вже були враховані, цей запит буде легко відхилено щодо незмінної книги, що підтверджується несхваленням більшості. Користувачів, які не дотримуються консенсусу, часто блокують у мережі. У випадку, якщо вузол хоче оскаржити запис, йому доведеться подати запит на відкликання всієї мережі. Якщо більше ніж дві третини однорангових вузлів схвалюють, транзакція підтверджується, розповсюджується та постійно записується в блокчейн.

На цей момент, існують три основні механізми консенсусу які блокчейни використовують для створення і валідації блоків транзакцій. PoW – proof of work, широко відомий механізм в якому для того, щоб підтверджувати транзакції потрібно використовувати потужності процесорів або відеокарт [9, 10], найвідоміший його представник це Bitcoin. PoS – proof

of stake механізм який активно набирає свою популярність, в цьому механізмі консенсусу вузол який створює блоки, відомий як валідатор, вибирається залежно від того яку частину активів блокчейну вони вносять як заставу, але й це тільки дає їм шанс бути вибраними, вузли вибираються випадково, чим більше застава ти більше шанс бути вибраним (рисунок 1.2) і отримати винагороду [11, 12], вибирається не одна нода для обробки, а одразу декілька, також вони перевіряють результати один одної, цей рисунок також можна віднести до PoW єдиною різницею слугує спосіб, по якому ця нода вибирається. DPoS (рисунок 1.3) – delegated proof of stake це механізм консенсусу який трохи нагадує PoS, але в випадку з DPoS замість того щоб всі вузли брали участь, власники валюти обирають делегатів, які відповідають за додавання нових блоків [13, 14]. Також можна побачити що існують слідуючи ноди, ці ноди нічого не записують в блок транзакцій, але слідкують за тим щоб ці транзакції були правильними (працюють без винагородження).

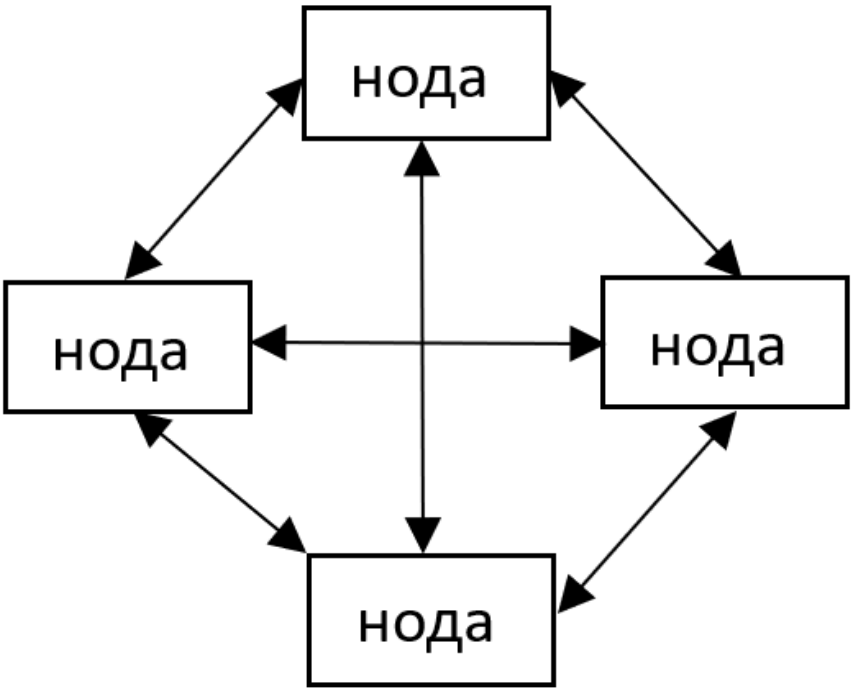

Рисунок 1.2 – PoS

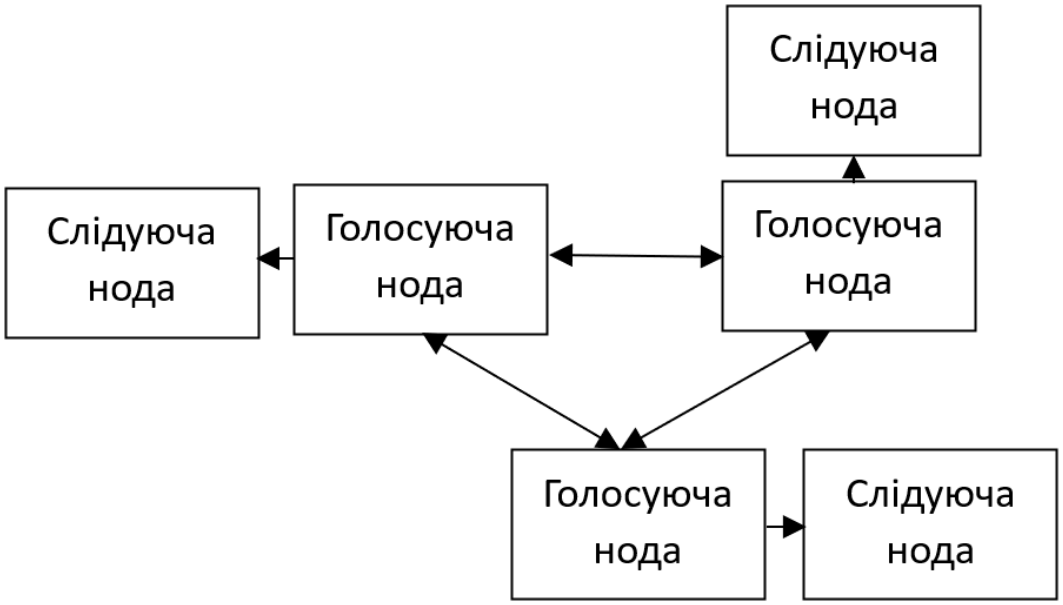

Рисунок 1.3 – DPoS

1.2.4 Мережевий рівень

Мережевий рівень забезпечує ефективне виявлення та взаємодію між одноранговими вузлами. Як правило, вузол знаходить завантажувальний вузол, який сканує доступні однорангові вузли та ініціює з’єднання. Коли інформація поширюється, вона захищається за допомогою довіреного середовища виконання (TEE) для підтримки цілісності. Обслуговування сесії вузла різниться в різних мережах; наприклад, Ethereum використовує рекурсивні префікси довжини, що визначає час, потрібний вузлам для пошуку, автентифікації та обміну даними.

1.2.5 Рівень даних

Рівень даних технології блокчейн в першу чергу стосується зберігання та структури даних. Він містить блокчейн, лінійну послідовність блоків, які зберігають інформацію про транзакції. Залежно від конкретного блокчейну

структура даних може варіюватися від простого списку транзакцій, такого як той, що використовується біткойнами, до складнішої структури, як-от trie стану Ethereum, яка зберігає інформацію про стан контракту.

Хоча специфіка додавання транзакцій і хешування тут не в центрі уваги, важливо зазначити, що рівень даних відіграє певну роль у підтримці цілісності та конфіденційності. Це рівень, на якому визначено більшість криптографічних примітивів, що використовуються в протоколі – алгоритми підписів, криптографічні бібліотеки та пари відкритих і закритих ключів, і які мають бути прив'язані до стандартів високого рівня безпеки.

Асиметричне шифрування є критично важливим компонентом, а пара публічно-приватних ключів зберігає конфіденційність даних. Відкритий ключ пов'язаний з адресою гаманця, а закритий ключ надає контроль над активами, пов'язаними з цією адресою.

Кожна транзакція супроводжується цифровим підписом, криптографічним механізмом, який підтверджує контроль правильного приватного ключа, не розкриваючи його, забезпечуючи таким чином безпеку. Криптографічні підписи генеруються такими алгоритмами підпису, як Алгоритм цифрового підпису еліптичної кривої, Рівест-Шаміра-Адлемана тощо.

1.2.6 Рівень апаратного забезпечення та інфраструктури

Архітектура блокчейну поширюється на апаратне забезпечення та інфраструктуру. На цьому рівні – у консенсусних протоколах Proof-of-Work – працюють майнери та валідатори, при цьому майнери створюють нові блоки за допомогою спеціалізованого обладнання (графічний процесор, вентилятор, стабілізатор) і електроенергії, а валідатори запускають вузли для майнінгу блоків. Що стосується зберігання даних, деякі блокчейни вибирають сторонні децентралізовані хостинги даних, такі як Filecoin, IPFS, Arweave або Firebase, через обмеження місткості.

Вузли, або клієнти, бувають трьох типів: повні, легкі та архівні вузли. Повні вузли зберігають стан усього ланцюга, беруть участь у консенсусних процесах і надають дані за запитом. Легкі вузли містять лише підсумки блоків, а архівні вузли зберігають дані транзакцій від блоку генезису до теперішнього часу, доступні для запитів користувачів.

Рівень інфраструктури також включає віртуальні машини, які діють як операційні системи та розміщують смартконтракти. Блокчейни часто мають рідні віртуальні машини, такі як віртуальна машина Avalanche для Avalanche і віртуальна машина Ethereum для Ethereum. Однак блокчейн також може бути сумісний з іншими віртуальними машинами.

2 АНАЛІЗ ВРАЗЛИВОСТЕЙ БЛОКЧЕЙНУ

2.1 Класифікація блокчейн атак

Блокчейн атаки діляться на атаки консенсусу, мережі, і атаки клієнту, атаки механізму консенсусу наймасштабніші, наслідками успішної атаки може бути повний занепад мережі, або дуже великий урон, атаки клієнту, це атаки направлені на одну або декілька нод або клієнтів, для того щоб викрасти ресурси конкретних нод, атака мережі задіває саму мережу, якою користується блокчейн, якщо він не достатньо добре захищений, то таким чином можно викрасти багато даних.

2.2. Основні блокчейн атаки

2.2.1 Атака Sybil

Атака Sybil має на меті захоплення мережі за допомогою кількох облікових записів в онлайн-мережі або мережі користувачів. Мета полягає в тому, щоб зіпсувати систему та маніпулювати нею на свою користь [15, 16].

Наприклад, атака Sybil може проявлятися як фальсифікація голосування на виборах або в системі онлайн-голосування. Крім того, це може включати створення кількох облікових записів у соціальних мережах на таких платформах, як X (Twitter), щоб поширювати фальсифіковану інформацію або, що ще гірше, ділитися шкідливими посиланнями, призначеними для збирання конфіденційної інформації користувачів.

У випадку публічних блокчейнів атаки Sybil зазвичай намагаються подолати автентичні вузли в мережі блокчейнів. У разі успіху зловмисники Sybil отримують повноваження змінити блокчейн, скомпрометувавши повноцінність мережі в процесі.

Щоб уточнити, остаточність блокчейну – це ідея про те, що після запису в блокчейн транзакцію неможливо змінити або скасувати. Ця концепція є фундаментальною для того, щоб транзакції в блокчейні вважалися дійсними та надійними. Наприклад, остаточність блокчейну необхідна, щоб запобігти використанню однієї й тієї ж криптовалюти більше одного разу (подвійне витрачання). Подібним чином, остаточність також життєво важлива для гарантії того, що результати смарт-контрактів і функцій децентралізованих програм є надійними та незворотними.

У світі криптографії атаки Sybil включають створення кількох мережевих вузлів у спробі здійснити контроль над мережею блокчейну. Загалом кажучи, криптовузол – це один комп'ютер, який є частиною мережі блокчейн. Кожен вузол окремо зберігає всю інформацію в блокчейні, завдяки чому вузли перевіряють один одного. Під час атаки Sybil один поганий актор створює кілька фальшивих вузлів, щоб обманом змусити мережу вважати шахрайські облікові записи законними.

Якщо зловмиснику вдасться залучити в мережу достатню кількість шкідливих вузлів, він зможе використати цей вплив проти чесних вузлів для своєї вигоди. Наприклад, у мережі блокчейн, де майнери голосують за пропозиції, зловмисник може використовувати кілька ідентифікаційних даних, щоб перевершити легітимні вузли. Зловмисники також можуть перехоплювати та аналізувати конфіденційні дані користувачів, наприклад IP-адреси, порушуючи конфіденційність і безпеку користувачів.

Часто кінцевою метою зловмисника Sybil є атака 51%. Це відбувається, коли одна сутність отримує понад 50% хеш-потужності (обчислювальної) мережі. Це дає зловмиснику можливість переписувати частини блокчейну, що означає, що він може змінити порядок транзакцій, заблокувати транзакції від перевірки або навіть скасувати свої власні транзакції, що призведе до подвійних витрат Можна побачити приклад атаки sybil (рисунок 2.1), де відключені від мережі чесні ноди, це ноди які були відключені від основної мережі та наразі аутентифікують транзакції sybil нод як дійсні

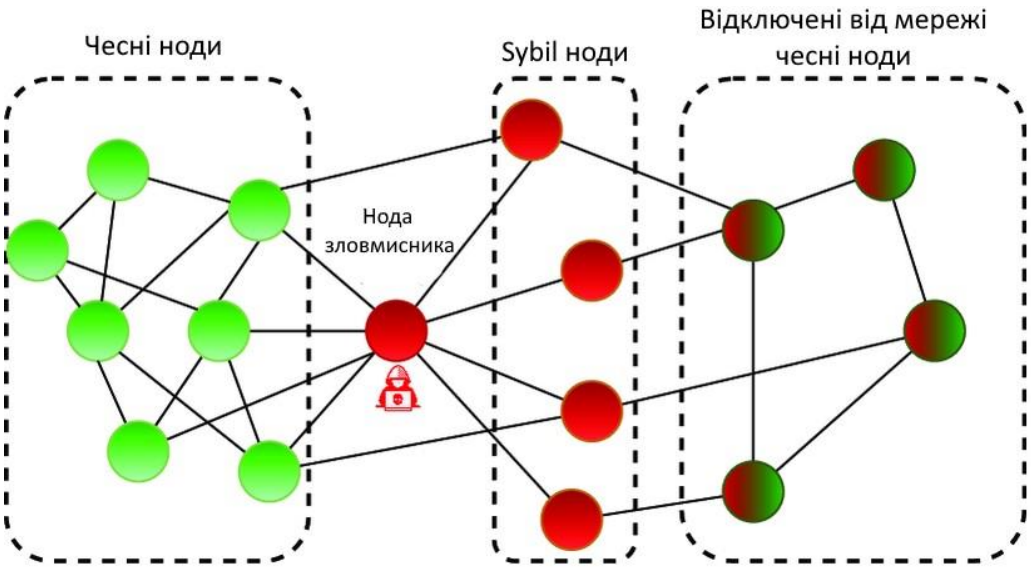

Рисунок 2.1 – Атака sybil

2.2.2 Eclipse атака

Атаки Eclipse передбачають ізоляцію зловмисником певного користувача або вузла в одноранговій (P2P) мережі. Під час виконання атаки eclipse зловмисник намагається перенаправити вхідні та вихідні з’єднання цільового користувача з його законних сусідніх вузлів на вузли, контрольовані зловмисником, тим самим ізолюючи ціль у середовищі, яке повністю відокремлено від фактичної мережевої активності. Шляхом обфускації законного поточного стану реєстру блокчейну зловмисник може маніпулювати ізольованим вузлом різними способами, що може призвести до неправомірних підтверджень транзакцій і блокувати збої в майнінгу. Оскільки атаки затемнення покладаються на використання сусідніх вузлів цілі, легкість, з якою ці атаки можуть бути успішно виконані, значною мірою залежить від базової структури цільової мережі блокчейн. Хоча децентралізована архітектура більшості протоколів криптовалюти робить їх відносно складними (і відносно рідкісними) порівняно з іншими типами онлайн-атак, атаки затемнення все ще становлять потенційну загрозу вашій онлайн-безпеці.

Атаки eclipse криптовалюти можливі через те, що вузли всередині децентралізованої мережі не можуть одночасно з’єднуватися з усіма іншими вузлами через обмеження пропускної здатності, і натомість повинні з’єднуватися з обмеженим набором сусідніх вузлів. У результаті зловмиснику потрібно лише скомпрометувати з’єднання цілі з цим обмеженим набором вузлів, а не атакувати всю мережу, як це відбувається під час атаки Sybil.

Щоб ізолювати та скомпрометувати вузол, зловмисник зазвичай використовує ботнет або фантомну мережу, створену з хост-вузлів, щоб наповнити цільовий вузол завалом IP-адрес, з якими ціль може синхронізуватися під час наступного підключення. з мережею блокчейн. Після цього зловмисник чекатиме, поки ціль успішно відновить з’єднання зі зловмисними вузлами, або використає атаку розподіленої відмови в обслуговуванні (DDoS), щоб змусити ціль повторно приєднатися до мережі.

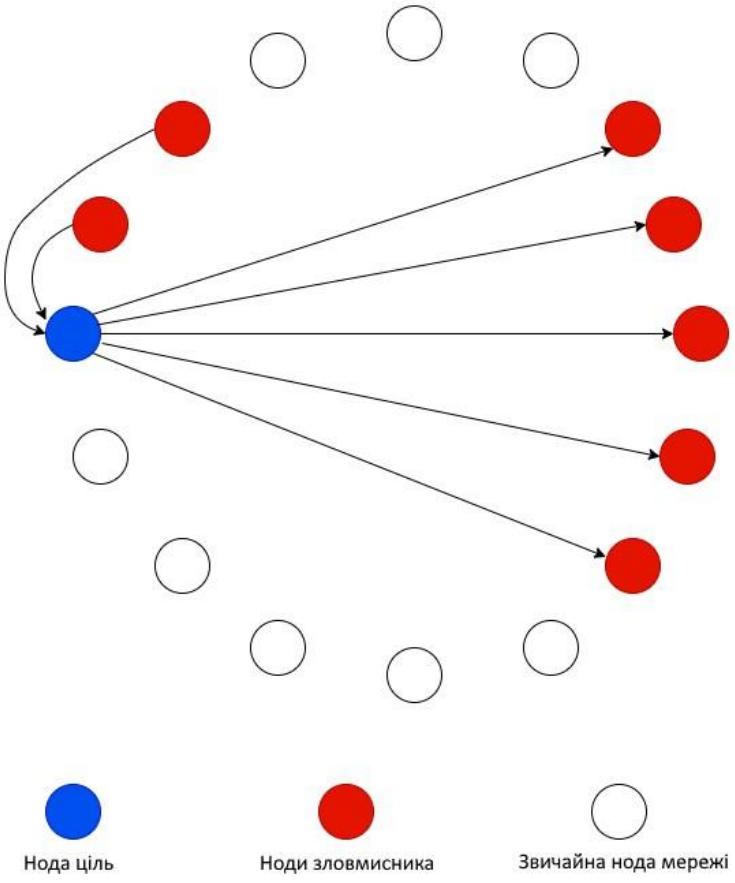

Рисунок 2.2 – Атака eclipse

Хоча може знадобитися кілька спроб, перш ніж цільовий вузол буде успішно скомпрометований, як тільки жертва приєднається до вузлів, контрольованих зловмисником, зловмисник може передати помилкові дані жертві, яка часто нічого не підозрює.

Можна побачити що атака eclipse успішно скомпрометувала ноду ціль (рисунок 2.2), яка не має підключення до звичайних нод мережі.

2.2.3 Атака підслуховування

Витік інформації, який інакше називають атакою підслуховування, має низький рівень серйозності.

Під час атаки підслуховування зловмисник стежить за мережею, щоб отримати приватні дані. Витягнувши конфіденційні дані, вони використовували їх для компрометації будь-якої частини мережі.

2.2.4 DDoS

DDoS (розподілена відмова в обслуговуванні) – це атака на кібербезпеку, під час якої зловмисники переповнюють мережу, програму, сервер або систему спам-трафіком або фальшивими транзакціями.

Намір полягає в тому, щоб уповільнити та порушити роботу системи чи мережі, таким чином перешкоджаючи обробці та підтвердженню законних транзакцій і перешкоджаючи справжнім користувачам використовувати систему, мережу чи протокол.

Блокчейни не захищені від DDoS-атак, оскільки всі ми знаємо, що вузли перевіряють транзакції, і, як ми бачили в минулому, зловмисники можуть наповнювати блокчейни спам-транзакціями, що сповільнює пропускну здатність блокчейну, зменшуючи його доступність до справжньої. користувачів, оскільки законні транзакції не будуть перевірені вчасно.

2.2.5 Alien атака

Перш за все, ми спочатку визначимо концепцію однорідного ланцюга, яка належить до системи блокчейнів, яка використовує той самий або сумісний протокол, що й інші блокчейни.

Alien атака, також відома як забруднення пулу адрес, належить до методу атаки, який спонукає вузли одного ланцюга вдиратися та забруднювати один одного. Основною причиною вразливості є те, що та сама система ланцюга не визначає несхожі вузли в протоколі зв'язку.

Alien атака на Ethereum означає, що однорідні ланцюги Ethereum (зокрема, загальнодоступні ланцюги, які використовують протокол виявлення вузлів Ethereum P2P discv4, включаючи Ethereum і Ethereum Classic) не можуть розрізнити, чи належать вузли до одного ланцюга через використання сумісних протоколів рукостискання. Метод атаки, який змушує пули адрес забруднювати один одного, погіршує продуктивність зв'язку вузла та, зрештою, спричиняє блокування вузла.

2.2.6 Rug pull

Rug pull відноситься до будь-якого зловмисного маневру, який виконують розробники, щоб залишити проєкт і вийти з усіма грошима інвесторів. Хоча rug pull є неетичним, а іноді навіть незаконним, вони часто здаються законними, а інвестори навіть не підозрюють про приховані загрози. Витягування здебільшого впливає на зони DeFi, NFT і Metaverse Web3, але може статися з будь-якими іншими проєктами.

Звичайна схема rug pull проста в розгортанні. Розробники створюють токен із привабливою назвою та новаторськими обіцянками. Вони стверджують, що їх токен відповідає майже всім вимогам користувачів і може помножити свої інвестиції на 10, 100, 1000 або навіть більше. Коли ціна шахрайського токена зростає, у продукт вливається більше грошей, доки пул

не стане настільки великим, що розробники раптом вирішили вкрасти все це багатство.

Процес крадіжки полягає в наступному: розробники продають або вилучають всю ліквідність з проєкту, підштовхуючи ціну до нуля. Шахраї також можуть використовувати backdoor в смартконтрактах, щоб вкрасти кошти інвесторів.

Існує 3 основних типи rug pull:

- Liquidity theft: творці вилучають усі монети з фонду фінансування. У результаті вартість, заблокована в токені, зникає, а інвестори залишаються з нікчемними активами;

- обмеження замовлень на продаж: творці кодують розумний контакт із вбудованими обмеженнями на продаж, тобто лише вони можуть продавати токени. Однак більшість інвесторів нічого не знають про ці обмеження. Розробники заманюють їх, стверджуючи, що обмеження є тимчасовими або виникли через технічну проблему, яку можна вирішити за кілька днів. Однак після того, як інвестори купують багато токенів, розробники просто отримують прибуток, продаючи всі ці активи та залишаючи людям нікчемний актив;

- Pump and dump: шахраї швидко купують великий обсяг токенів («памп»), щоб значно підвищити його вартість і привабливість в очах наявних і потенційних інвесторів. Водночас вони проводять агресивні маркетингові кампанії, привабливі для інвесторів. Їх мета - переконати інвесторів, що покупка цього токена є єдино правильним рішенням для них. В результаті інвестори бачать, що токен приносить 10-кратну або навіть 100-кратну віддачу, і входять у цей проєкт. Коли ажіотаж досягає свого піка, творці скидають усі свої токени, щоб отримати величезні прибутки, залишаючи таким чином користувачів з копійками.

Rug pull має 2 загальні форми:

- Hard rug pull, розробники використовують кодування, щоб обдурити інвесторів. Вони вбудовують приховані речі в контракт, і після того, як

інвестують свої гроші в проєкт, користувачі не можуть виконувати будь-які дії з їхніми активами. Таким чином, вони блокуються в проєкті, а шахраї отримують повну владу для маніпуляцій з маркерами;

- Soft rug pull, часто має характер «накачування та скидання». Користувачі можуть вийти з проєкту, коли захочуть, але вони бояться втратити великі прибутки, тому не залишають проєкт, поки його творці не вийдуть з усіма своїми грошима.

2.2.7 False Top-Up атака

Атаки на підроблені депозити стосуються тактики, коли зловмисники використовують вразливі місця або системні помилки в обробці депозитних операцій на біржі. Вони надсилають дані підроблених транзакцій на адреси гаманців біржі, які біржа помилково ідентифікує як законні запити на депозит, і згодом зараховує відповідні цифрові активи або валюти на обліковий запис зловмисника. Застосовуючи цю тактику, зловмисники можуть отримати цифрові активи без оплати, що призведе до втрати активів для бірж.

2.2.8 Length Extension атака

Атака Length Extension – це тип атаки, коли зловмисник може використовувати хеш і довжину першого повідомлення для обчислення хешу для контрольованого зловмисником другого повідомлення, не потребуючи знання вмісту першого повідомлення. Це проблематично, коли хеш використовується як код автентифікації повідомлення, і повідомлення та довжина секрету відомі, оскільки зловмисник може включити додаткову інформацію в кінці повідомлення та створити дійсний хеш без знання секрету. Такі алгоритми, як MD5, SHA-1 і більшість SHA-2, які базуються на конструкції Меркле–Дамгорда, сприйнятливі до такого роду атак. Усічені

версії SHA-2, включаючи SHA-384 і SHA-512/256, не сприйнятливі, як і алгоритм SHA-3. HMAC також використовує іншу конструкцію і тому не вразливий до Length Extension атак.

2.2.9 51% атака

Атака 51% – це атака на блокчейн, де група контролює понад 50% потужності хешування – обчислень, які вирішують криптографічну головоломку мережі. Потім ця група вводить у мережу змінений блокчейн у дуже конкретній точці блокчейну, яка теоретично приймається мережею, оскільки зловмисники володітимуть більшою частиною [17, 18].

Змінити історичні блоки – транзакції, заблоковані до початку атаки – було б надзвичайно важко навіть у разі атаки 51%. Чим далі транзакції, тим складніше їх змінити. Було б неможливо змінити транзакції до контрольної точки, де транзакції стають постійними в блокчейні.

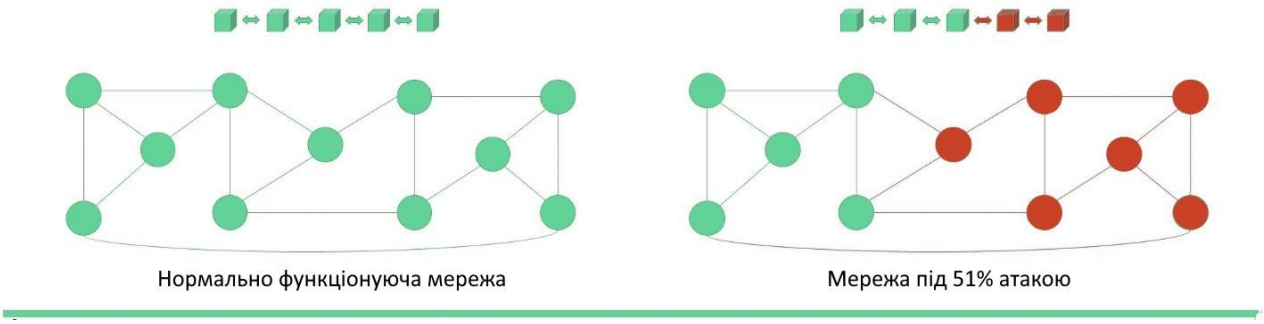

Рисунок 2.3 – Атака 51%

Можна побачити приклад атаки 51% (рисунок 2.3) де зловмисники заволоділи більшою частиною мережі, і тепер створюють свої блоки транзакцій.

3 ПРОЄКТУВАННЯ БЛОКЧЕЙНУ

3.1 Реалізація інформаційного рівня

Існує багато структур для реалізації інформаційного рівня розглянемо оптимальні рішення, на меті вибору підходу до створення цього рівня має бути як максимальна захищеність, так і не над висока вартість транзакції, також важливо залишати блокчейн достатньо швидким. Розглянемо актуальні підходи з погляду ефективності і захищеності:

а) дерево Меркла:

Ефективність:

Ефективні для перевірки консистентності даних завдяки своїй бінарній структурі.

Вимагають логарифмічного часу для верифікації (залежно від кількості листків).

Захист:

Відмінна цілісність даних та стійкість до втручань.

Зміна даних призводить до іншого хешу кореня Мерклівого дерева;

б) дерева Меркла-Патріції (Trie):

Ефективність:

Ефективна обробка ключів змінної довжини (наприклад, адрес Ethereum).

Мінімізація зайвого зберігання даних.

Захист:

Забезпечує цілісність та консистентність даних.

Складна реалізація, але надійна;

в) Послідовні списки:

Ефективність:

Прості та прямолінійні.

Не ефективні для перевірки консистентності даних (при лінійному обході).

Захист:

Обмежені можливості цілісності даних.

Не призначені для стійкості до втручань;

г) хеш-таблиці:

Ефективність:

Ефективне отримання даних за ключами.

Зазвичай використовуються для зберігання смартконтрактів.

Захист:

Не призначені для цілісності даних. Вимагають додаткових механізмів для стійкості до втручань;

д) дерева Меркла зі смугами (Merkle Bucket Tree):

Ефективність:

Воно поєднує переваги дерев Меркла (для перевірки цілісності) та хеш-смуг (для зменшення обчислювальних витрат).

Захист: Дерево Меркла зі смугами забезпечує баланс між ефективністю та цілісністю даних.

Проаналізувавши підходи наведені вище можна зробити вибір на користь дерева Меркла-Патріції через його надійність та швидкість, а також маємо реальний приклад децентралізованого блокчейну який побудований на цьому принципі – Etherium, який є одним із передових блокчейнів в плані захисту і ефективності.

Далі важливо мати достатньо швидкий та надійний алгоритм хешування і шифрування, є 2 найкращі рішення: SHA-256, Keccak-256. Не зважаючи на те що більшість блокчейнів написана із використання SHA-256 (сімейство SHA-2), за роки свого існування в цьому алгоритмі виявили велику кількість вразливостей, на томість набагато новіший і надійніший Keccak-256 (сімейство SHA-3) хоч і використовується в набагато меншій кількості блокчейнів, але вже довів свої переваги в світі блокчейну. Також

важливим плюсом Keccak-256 має більш надійний захист проти таких атак як length extension attacks. Keccak-256 має більшу гнучкість в довжині виводу.

Наступним важливим кроком є проєктування блоку транзакцій.

Транзакція нашого блокчейну буде складатися із метаданих, кешу, і інформації (рисунок 3.1). Метадані необхідні для того щоб забезпечити як прозорість блокчейну так і його надійність і захищеність, кеш потрібен для обозначення з якими адресами буде взаємодіяти транзакція, інформація потрібна більше для створення контрактів в блокчейні.

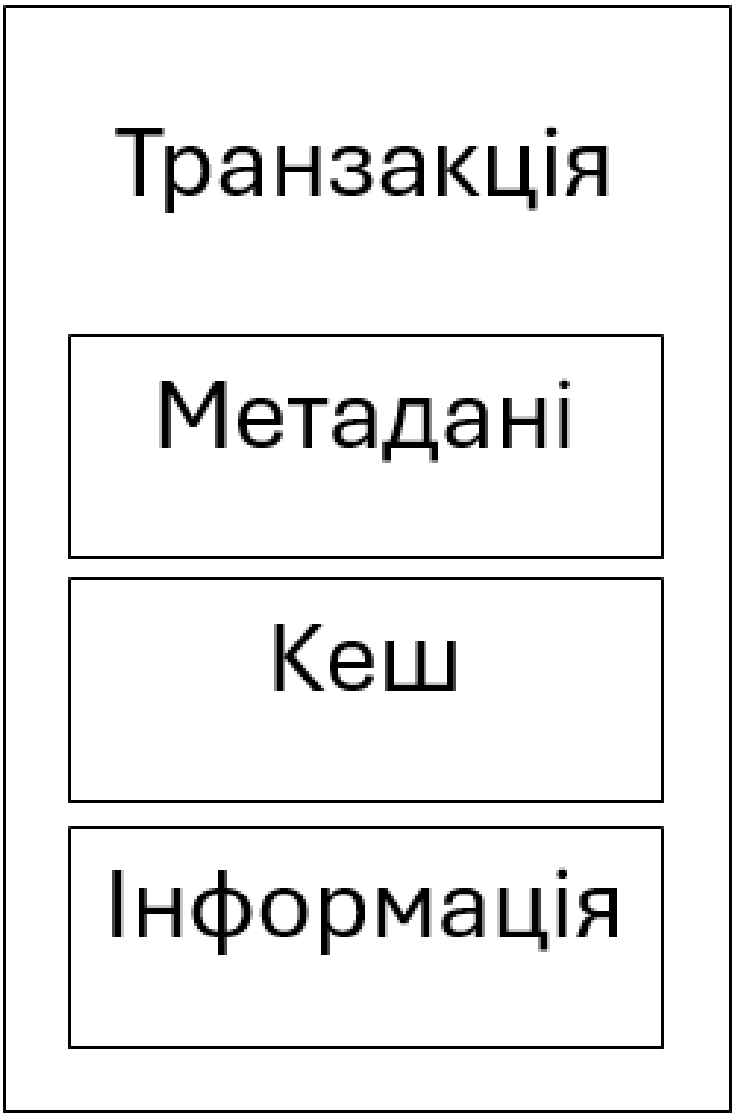

Рисунок 3.1 – Схема транзакції

Далі більш детально спроєктуємо частину транзакції відповідальну за метадані (рисунок 3.2). Параметр номер блоку відповідає за номер блоку в якому дана транзакція була виконана, індекс транзакції відповідає за номер транзакції в блоці транзакції, хеш це унікальний ідентифікатор відповідальний за доказ того що транзакція валідна, і хеш блоку транзакції це доказ того що весь блок з транзакціями валідний, хеші в нашому блокчейні створені за допомогою наведеного вище алгоритму Keccak-256, ідентифікатор ланцюжка відповідальний за те що транзакція відноситься саме до цієї блокчейн мережі, від кого це параметр відповідальний за адресу ініціатора транзакції, куди це параметр відповідальний за адресу отримувача транзакції, числовий ідентифікатор по типу індексу транзакції, але він збільшується на 1 при кожній спробі створити транзакцію, r, s, v це частини криптографічної сигнатури які допомагають впевнитися що транзакція цілісна і валідна, r і s це два числа які разом утворюють цифрову сигнатуру, ця сигнатура доводить що транзакція була підписана конкретним користувачем, v показує в якому саме ланцюжку була створена транзакція цей параметр по суті аналог існуючого в самій транзакції ідентифікатора ланцюжка, значення це кількість переданих при транзакції крипто токенів, вартість це ціна саме обробки транзакції тобто комісія мережі, тип транзакції показує нам що саме зробила ця транзакція, наприклад транзакція може бути простим переказом або слугувати для створення контракту.

Нижче можна побачити приклад метаданих транзакції (рисунок 3.3), з реальними значеннями.

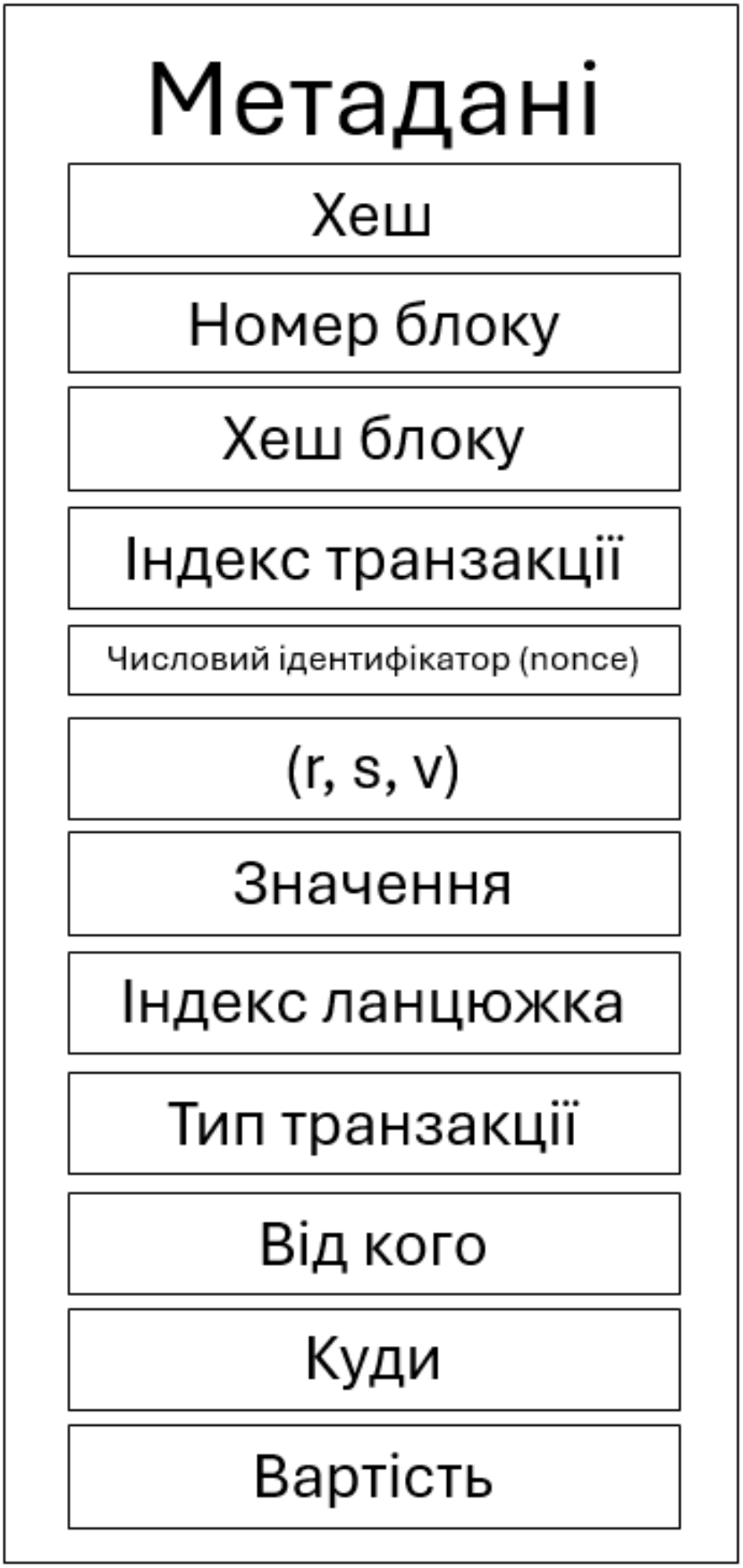

Рисунок 3.2 – Схема метаданих транзакції

```
{
   "blockHash":"0x479c9dca8a806183261d7b3c2c69844a1a5cb3eae7e10b4d8298f3c6cf207346",
   "blockNumber":15499910,
   "chainId":"0x1",
   "from":"0x1ecc89fd4fc4ded8543204854ab4596aec69eb47",
   "gas":134434,
   "hash":"0x6582df4448ce1eb37b5c3365fe869ce43282eda92d78f2a6e0e7ad065deea081",
   "nonce":4205,
   "r":"0x423ff6d0f848e83b7b46572956e28a4b72ceb8b10f6f68d9b378e0e0de9f1b94",
   "s":"0x712e01d03c25d8f75179e9232b56d45f943a05f7f51ee318b7ad1946806ada4",
   "to":"0xbeefbabeea323f07c59926295205d3b7a17e8638",
   "transactionIndex":2,
   "type":"0x2",
   "v":"0x0",
   "value":15499910
}
```


Рисунок 3.3 – Приклад метаданих транзакції

Далі йде реалізація схеми виконання (рисунок 3.4), вона складається із заголовку і транзакцій також його можна назвати блоком транзакцій. Транзакції в цій схемі це просто масив транзакцій які були наведені вище (рисунок 3.1).

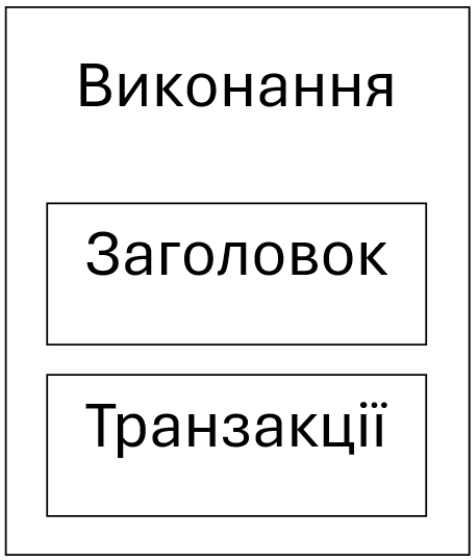

Рисунок 3.4 – Схема виконання транзакції

Далі більш детально спроєктуємо схему заголовка блоку транзакцій (рисунок 3.5). Батьківський хеш це хеш минулого блоку транзакцій, позначка

часу це звичайна часова мітка, номер блоку фактично є його ідентифікатором, розмір це розмір блоку в байтах, вартість це ціна за обробку всіх транзакцій в блоці, logsBloom необхідний для зменшення ваги блокчейну, він зберігає всі адреси контрактів які виконували якісь дії, stateRoot, receiptsRoot і transactionsRoot виконані із розглянутих вище деревом меркла, stateRoot зберігає в собі весь стан блокчейну, transactionsRoot дозволяє ноді верифікувати цілісність блоку транзакцій, receiptsRoot слугує для підсумку всіх транзакцій в блоці. Додаткова інформація для хешу (nonce) вже була в схемі транзакцій, але тут вона створюється не із чисел, а зі спеціальної зашифрованої додаткової інформації.

Рисунок 3.5 – Схема заголовка виконання транзакції

3.2 Реалізація мережевого рівня

Мережевий рівень відповідає за ефективну та безпечну взаємодію між нодами, які називаються вузлами. Цей рівень є ключовим для забезпечення децентралізованості блокчейну та дозволяє здійснювати транзакції між вузлами без посередництва. Побудуємо мережевий рівень який буде складатися із наступних компонентів:

а) виявлення нод

Виявлення – це процес пошуку інших вузлів у мережі. Це робиться за допомогою невеликого набору завантажувальних вузлів (вузлів, адреси яких жорстко закодовано у клієнті, щоб їх можна було негайно знайти та приєднати клієнт до однорангових вузлів). Ці завантажувальні вузли існують лише для того, щоб представити новий вузол набору однорангових вузлів — це їхнє єдине призначення, вони не беруть участі у звичайних клієнтських завданнях, таких як синхронізація ланцюга, і вони використовуються лише під час першого запуску клієнта. Протокол, який використовується для взаємодії між вузлом і початковим вузлом, є модифікованою формою Kademlia, яка використовує розподілену хеш-таблицю для спільного використання списків вузлів. Кожен вузол має версію цієї таблиці, що містить інформацію, необхідну для підключення до найближчих однорангових вузлів. Ця «близькість» не є географічною — відстань визначається подібністю ідентифікатора вузла. Таблиця кожного вузла регулярно оновлюється як функція безпеки. Наприклад, у Discv5 вузли протоколу виявлення також можуть надсилати «оголошення», які відображають підпротоколи, які підтримує клієнт, дозволяючи одноранговим вузлам домовитися про протоколи, які вони обидва можуть використовувати для спілкування. Відкриття починається з гри в пінг-понг. Успішний PING-PONG "зв'язує" новий вузол із початковим вузлом. Початкове повідомлення, яке сповіщає початковий вузол про існування нового вузла, що входить у мережу, є PING. Цей PING містить хешовану інформацію про новий вузол,

початковий вузол і мітку часу закінчення терміну дії. Завантажувальний вузол отримує PING і повертає PONG, що містить хеш PING. Якщо хеші PING і PONG збігаються, зв’язок між новим вузлом і початковим вузлом перевіряється, і кажуть, що вони «з’єднані». Після приєднання новий вузол може надіслати запит FIND-NEIGHBOURS початковому вузлу. Дані, які повертає завантажувальний вузол, містять список однорангових вузлів, до яких може приднатися новий вузол. Якщо вузли не зв’язані, запит FIND-NEIGHBOURS завершиться невдало, тому новий вузол не зможе увійти в мережу. Як тільки новий вузол отримує список сусідів від початкового вузла, він починає обмін PING-PONG з кожним із них. Успішний пінг-понг зв’язує новий вузол із сусідами, роблячи можливим обмін повідомленнями;

б) протоколи мережі

Протоколи мережі відповідають за взаємодію, DevP2P сам по собі є цілим набором протоколів, які існують для створення та підтримки однорангової мережі. Коли нові вузли входять у мережу, їх взаємодія регулюється протоколами в стеку DevP2P. Усі вони розташовані поверх TCP і включають транспортний протокол RLPx, дротовий протокол і кілька підпротоколів. RLPx – це протокол, який регулює ініціювання, автентифікацію та підтримку сеансів між вузлами. RLPx кодує повідомлення за допомогою RLP (префікс рекурсивної довжини), який є дуже ефективним методом кодування даних у мінімальну структуру для надсилання між вузлами. Сеанс RLPx між двома вузлами починається з початкового криптографічного рукостискання. Це передбачає надсилання вузлом повідомлення авторизації, яке потім перевіряється одноранговим вузлом. Після успішної перевірки одноранговий вузол генерує повідомлення підтвердження авторизації для повернення до вузла-ініціатора. Це процес обміну ключами, який дозволяє вузлам спілкуватися конфіденційно та безпечно. Успішне криптографічне рукостискання потім запускає обидва вузли, щоб надіслати повідомлення «привіт» один одному «по дроту». Дротовий протокол ініціюється успішним обміном повідомленнями

привітання. Повідомлення привітання містять: версія протоколу ідентифікатор клієнта порт ідентифікатор вузла список підтримуваних підпротоколів Це інформація, необхідна для успішної взаємодії, оскільки вона визначає, які можливості спільно використовуються між обома вузлами, і налаштовує зв'язок. Існує процес узгодження підпротоколів, у якому порівнюються списки підпротоколів, які підтримуються кожним вузлом, і ті, які є спільними для обох вузлів, можуть бути використані в сеансі. Разом із повідомленнями привітання протокол дротового зв'язку також може надсилати повідомлення «від'єднання», яке попереджає однорангового вузла про те, що з'єднання буде закрито. Протокол дротового зв'язку також включає повідомлення PING і PONG, які періодично надсилаються, щоб підтримувати сеанс відкритим. Таким чином, RLPx і обмін дротовим протоколом встановлюють основи зв'язку між вузлами, забезпечуючи основу для обміну корисною інформацією відповідно до певного підпротоколу.

Технології використані для проєктування нашого дуже сильно знижує ризики таких атак як підслуховування, sybil і eclipse.

3.3 Рівень консенсусу

Консенсусний рівень є основою будь-якої мережі блокчейну, виконуючи життєво важливу роль, сприяючи узгодженню між вузлами щодо справжнього стану блокчейну.

Оптимальним варіантом буде PoS. PoS – це спосіб довести, що валідатори вклали в мережу щось цінне, що може бути знищено, якщо вони діятимуть нечесно. У доказі частки Ethereum валідатори явно вкладають капітал у формі токенів у смартконтракт. Тоді валідатор відповідає за перевірку того, що нові блоки, що розповсюджуються через мережу, дійсні, а також час від часу сам створює та розповсюджує нові блоки. Якщо вони намагаються обдурити мережу (наприклад, пропонуючи кілька блоків, коли

вони повинні надіслати один, або надсилаючи суперечливі атестації), частина або весь їхній капітал може бути знищений.

Щоб взяти участь у якості валідатора, користувач повинен внести 32 токени у депозитний контракт і запустити три окремі частини програмного забезпечення: клієнт виконання, клієнт консенсусу та клієнт валідатора. Після внесення своїх токенів користувач приєднується до черги активації, яка обмежує кількість нових валідаторів, які приєднуються до мережі. Після активації валідатори отримують нові блоки від однорангових користувачів у мережі. Транзакції, доставлені в блоці, виконуються повторно, щоб перевірити, чи дійсні запропоновані зміни в стані блокчейну, і перевіряється підпис блоку. Потім валідатор надсилає голос (званий атестацією) на користь цього блоку через мережу. У той час як у proof-of-work час блоків визначається складністю майнінгу, у proof-of-stake темп є фіксованим. Час у proof-of-stake поділяється на слоти (12 секунд) і епохи (32 слоти). Один валідатор вибирається випадковим чином, щоб бути пропонентом блоку в кожному слоті. Цей валідатор відповідає за створення нового блоку та надсилання його на інші вузли в мережі. Також у кожному слоті випадковим чином обирається комітет валідаторів, чиї голоси використовуються для визначення дійсності запропонованого блоку. Розподіл налаштованого валідатора на комітети важливий для збереження керованого навантаження на мережу. Комітети розподіляють набір валідаторів так, щоб кожен активний валідатор атестував у кожній епосі, але не в кожному слоті.

Транзакції в нашому PoS будуть виконуватися наступним чином (рисунок 3.6). Користувач створює та підписує транзакцію своїм закритим ключем, робить запит до вузла. Транзакція надсилається клієнту виконання блокчейну, який перевіряє її дійсність. Це означає, що відправник має достатньо токенів для виконання транзакції, і він підписав її правильним ключем. Якщо транзакція дійсна, клієнт виконання додає її до свого локального пам’ятного пулу (списку транзакцій, що очікують на розгляд), а також транслює її іншим вузлам через мережу плиток рівня виконання. Коли

інші вузли дізнаються про транзакцію, вони також додають її до свого локального mempool. Один із вузлів у мережі є пропонентом блоку для поточного слота, який попередньо був обраний псевдовипадковим чином за допомогою RANDAO. Цей вузол відповідає за створення та трансляцію наступного блоку, який буде додано до блокчейну, і оновлення глобального стану. Вузол складається з трьох частин: клієнта виконання, клієнта консенсусу та клієнта валідатора. Клієнт виконання об’єднує транзакції з локального мемпулу в «корисне навантаження виконання» та виконує їх локально для генерації зміни стану. Ця інформація передається до консенсусного клієнта, де корисне навантаження виконання загортається як частина «маякового блоку», який також містить інформацію про винагороди, штрафи, скорочення, атестації тощо, що дозволяє мережі узгодити послідовність блоків на початку ланцюга. Зв’язок між клієнтами виконання та клієнтами консенсусу описано більш детально в розділі Підключення клієнтів консенсусу та клієнтів виконання. Інші вузли отримують новий блок маяка в мережі плиток консенсусного рівня. Вони передають його своєму клієнту виконання, де транзакції повторно виконуються локально, щоб переконатися, що запропонована зміна стану дійсна. Потім клієнт валідатора засвідчує, що блок дійсний і є логічним наступним блоком у їхньому представленні ланцюга (це означає, що він будується на ланцюжку з найбільшою вагою атестацій, як визначено в правилах вибору форка). Блок додається до локальної бази даних у кожному вузлі, який його засвідчує. Транзакцію можна вважати «завершеною», якщо вона стала частиною ланцюжка з «переважною ланкою» між двома контрольними точками. Контрольні точки виникають на початку кожної епохи, і вони існують, щоб врахувати той факт, що лише підмножина активних валідаторів підтверджує в кожному слоті, але всі активні валідатори підтверджують у кожній епосі. Таким чином, лише між епохами можна продемонструвати «зв’язок супербільшості».

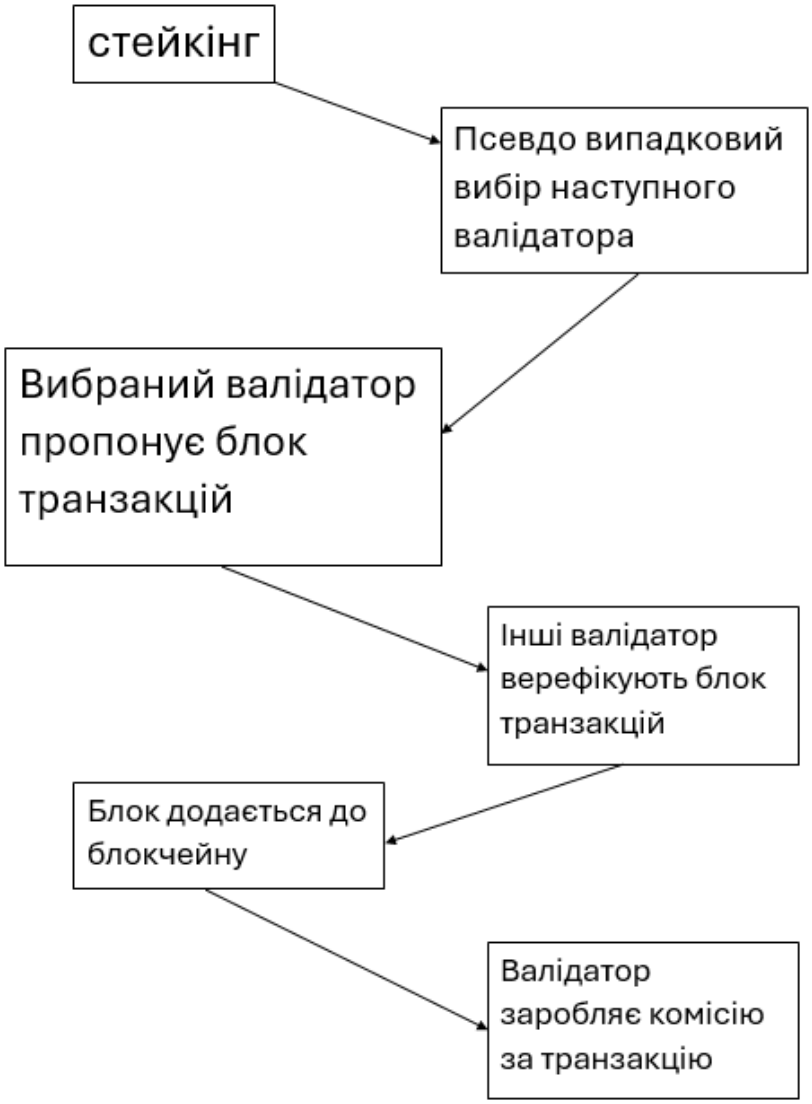

Рисунок 3.6 – Схема спроєктованого PoS

Транзакція має «завершеність» у мережі, коли вона є частиною блоку, який не може змінитися без спалювання великої кількості токенів. На proof-of-stake це управляється за допомогою блоків «контрольних точок». Перший блок у кожній епосі – контрольна точка. Валідатори голосують за пари контрольних точок, які вони вважають дійсними. Якщо пара контрольних точок привертає голоси, що становлять щонайменше дві третини від загальної суми поставлених токенів, контрольні точки оновлюються. Остання з двох (ціль) стає «виправданою». Раніше з двох уже виправдано, оскільки

воно було «мішенню» в попередню епоху. Тепер його оновлено до "завершеного". Щоб скасувати завершений блок, зловмисник зобов’язується втратити принаймні одну третину загального запасу поставленого капіталу токенів. Оскільки остаточність вимагає більшості у дві третини, зловмисник може перешкодити досягненню мережі остаточності, проголосувавши однією третиною від загальної частки. Існує механізм захисту від цього: витік неактивності. Це активується щоразу, коли ланцюг не вдається завершити протягом більше ніж чотирьох епох. Витік неактивності позбавляє від валідаторів блокчейну, які голосують проти більшості, дозволяючи більшості відновити більшість у дві третини та завершити ланцюжок.

Запуск валідатора є зобов’язанням. Очікується, що валідатор підтримуватиме достатнє обладнання та підключення для участі в перевірці блоку та пропозиції. Натомість валідатор отримує плату в токенах (їхній баланс ставок збільшується). З іншого боку, участь у якості валідатора також відкриває нові шляхи для користувачів для атаки на мережу з метою особистої вигоди чи саботажу. Щоб запобігти цьому, валідатори втрачають винагороди, якщо вони не беруть участі, коли їх викликають, і їхня наявна частка може бути знищена, якщо вони поводитимуться нечесно. Дві основні поведінки можна вважати нечесними: пропонування кількох блоків в одному слоті (двозначність) і подання суперечливих підтверджень. Обсяг скорочення токенів залежить від того, скільки валідаторів також скорочується приблизно в той самий час. Це відоме як «кореляційний штраф», і воно може бути незначним (~1% частки для одного валідатора зменшується самостійно) або може призвести до знищення 100% частки валідатора (маса різка подія). Він накладається на півдорозі через період примусового виходу, який починається з негайного штрафу у день 1, штрафу за кореляцію в день 18 і, нарешті, виключення з мережі в день 36. Вони отримують незначні штрафи за атестацію щодня оскільки вони присутні в мережі, але не подають голоси. Усе це означає, що скоординована атака буде дуже дорогою для зловмисника.

Загроза атаки 51% все ще існує для proof-of-stake, як і для proof-of-work, але це ще ризикованіше для зловмисників. Зловмиснику знадобиться 51% поставлених токенів. Потім вони могли використовувати власні атестації, щоб переконатися, що їхній кращий форк – це той, який має найбільшу кількість атестацій. «Вага» накопичених атестацій – це те, що консенсус-клієнти використовують для визначення правильного ланцюга, щоб цей зловмисник міг зробити свій форк канонічним. Однак сильна сторона proof-of-stake над proof-of-work полягає в тому, що спільнота має гнучкість у організуванні контратаки. Наприклад, чесні валідатори можуть вирішити продовжувати будувати ланцюжок меншості та ігнорувати форк зловмисника (рисунок 3.7), заохочуючи програми, біржі та пули робити те саме. Вони також можуть прийняти рішення примусово видалити зловмисника з мережі та знищити свій капітал. Це сильний економічний захист від атаки 51%. 51% атак є лише одним із видів шкідливої діяльності. Зловмисники можуть намагатися здійснити атаки на далекі відстані (хоча гаджет остаточності нейтралізує цей вектор атаки), «реорганізації» на короткі відстані (хоча прискорення пропонента та кінцеві терміни атестації пом’якшують це), атаки відскоку та балансування (також пом’якшуються за допомогою посилення пропонента, і ці атаки мають у будь-якому випадку було продемонстровано лише в ідеалізованих умовах мережі) або лавинні атаки (нейтралізовані правилом алгоритмів вибору розгалуження, що передбачає врахування лише останнього повідомлення).

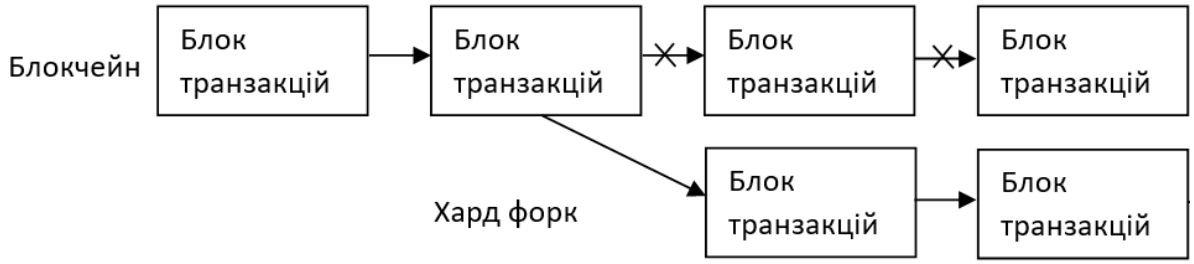

Рисунок 3.7 – Хард форк

Структура нашого PoS блоку (рисунок 3.8) складається із адміністрування, консенсусу і виконання, виконання яке ми розглядали вище (рисунок 3.4).

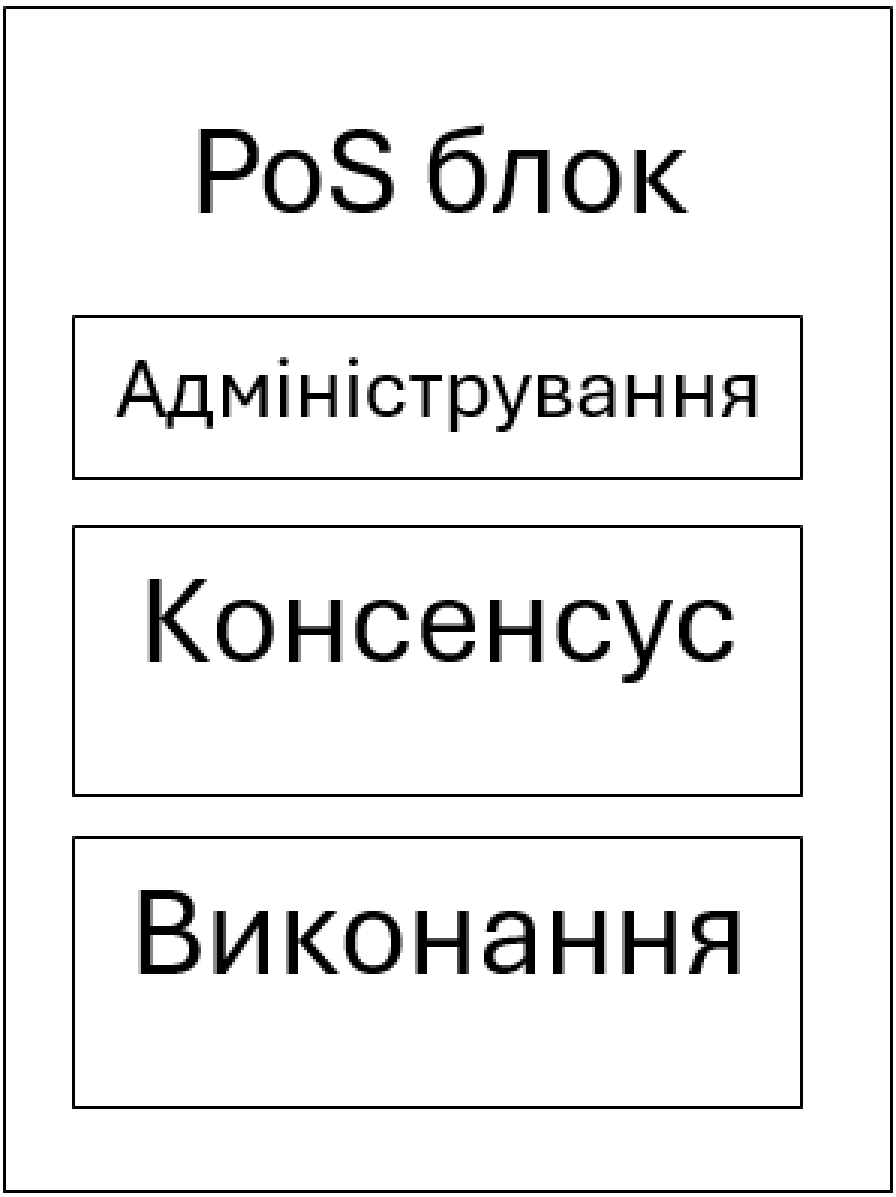

Рисунок 3.8 – PoS блок

Розглянемо більш детально адміністрування (рисунок 3.9), воно складається із номеру блоку, індексу валідатору який показує нам на валідатора який валідував цей блок, stateRoot і parentRoot це стан блокчейну і корінь минулого блоку, такі самі значення для дерева меркла які були

наведені вище. Randao це параметр який дозволяє робити псевдорандомний вибір валідатора.

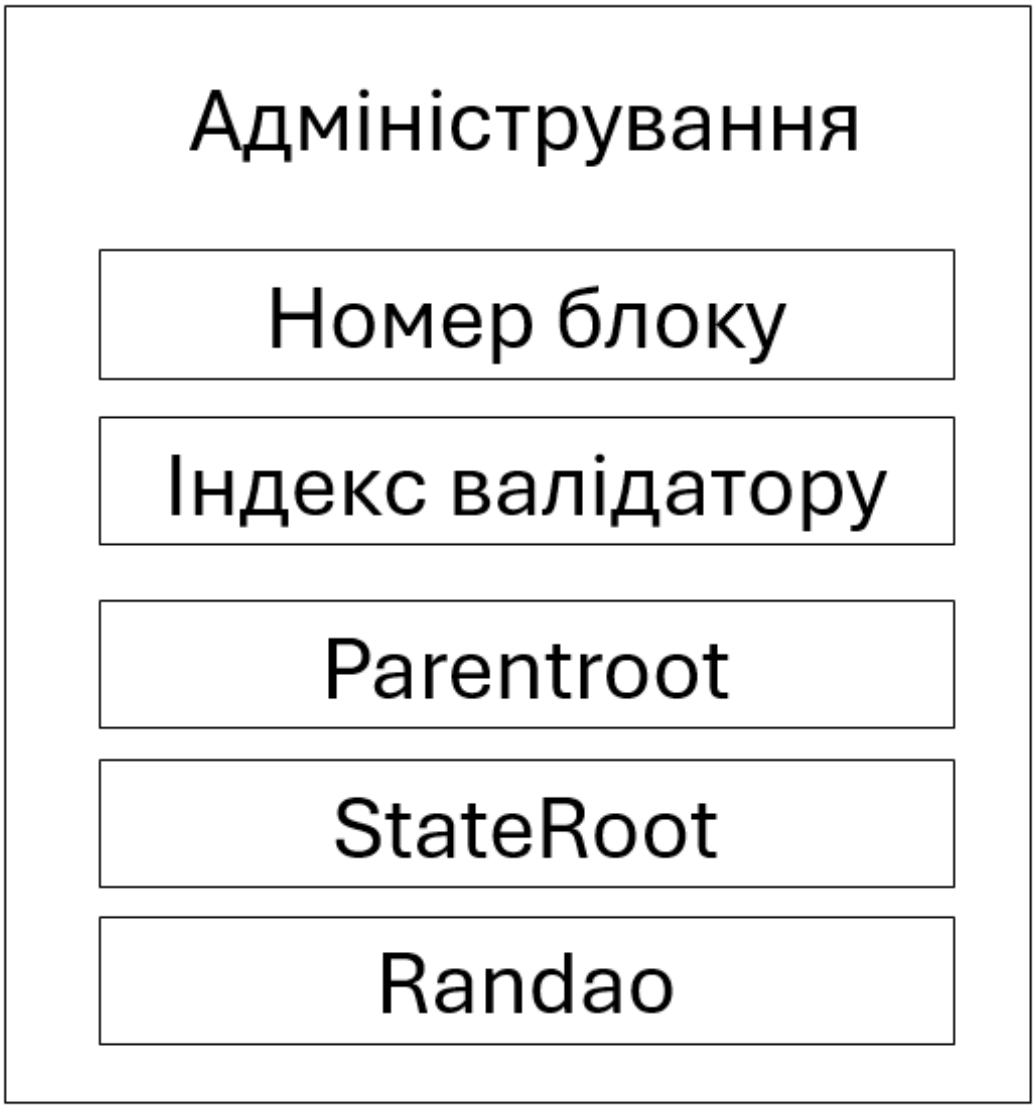

Рисунок 3.9 – Адміністрування PoS блоку

Розглянемо більш детально структуру і параметри спроектованої консенсус частини (рисунок 3.10). Атестації – це лист всіх підписів які атестували цей блок, proposer slashings і atteter slashings існують для того щоб конфіскувати в валідаторів і атестаторів застейканий капітал які вчинили злочинні дії, а також видаляти їх із валідаторів і атестаторів. Sync committee bits – ефективне представлення членства в комітеті атестаторів, Sync

committee signature – це підпис яким комітет бере на себе відповідальність за блок або епоху. Voluntary exits – виводи із контракту стейкінгу, Депозити – означає кількість депозитів валідаторів включених в цей блок пропонуйочою нодою, deposit count – кількість валюти в стейкінг контракті, deposit root – хеш кореня дерева меркла, яке зберігає в собі кількість токенів які лежать на депозиті в стейкінг контракті.

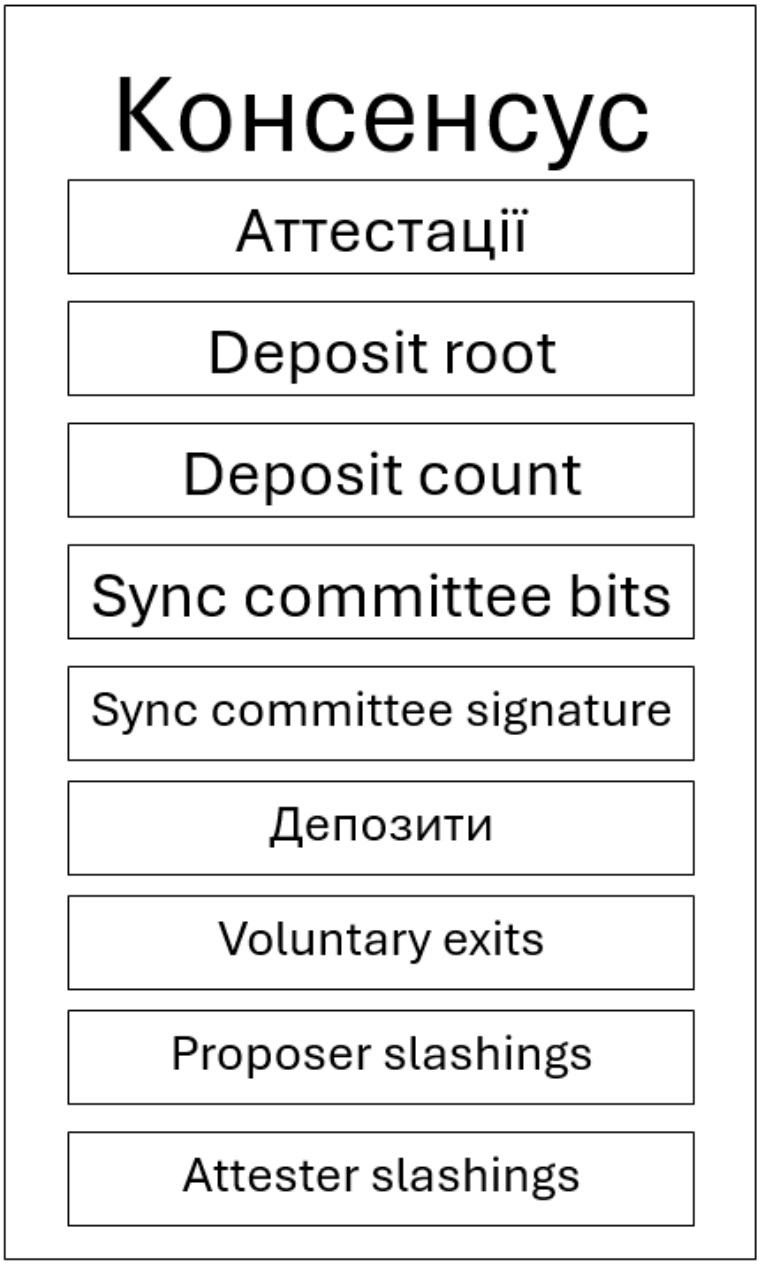

Рисунок 3.10 – Адміністрування PoS блоку

В першому розділі ми розглянули 6 рівнів блокчейну, але для проектування децентралізованого блокчейну із оптимальним захистом і ефективністю 3 не рзглянуті тут рівні не несуть такого значення, рівень послуг і додаткових компонентів каже сам за себе, сам цей рівень є необов’язковим, рівень апаратного забезпечення і інфраструктури неважливий через те що наша ціль децентралізований блокчейн, який буде працювати на системах інших користувачів, які будуть отримувати за це винагороди, а прикладний рівень було частково реалізовано в попердніх розділах, тільки необхідна мінімальна реалізація.

ВИСНОВКИ

В рамках кваліфікаційної роботи було наведено методології побудови децентралізованих блокчейн мереж проведено огляд передових механізмів для побудови, виявлені їх переваги та недоліки.

Підставою для даної роботи є актуальність теми захисту і побудови децентралізованої блокчейн мережі. Після проведення аналітичного дослідження цієї проблеми не залишилося жодних сумнівів в її актуальності.

Кваліфікаційна робота складається з трьох розділів. В першому розділі було описаний принцип концепції роботи децентралізованого блокчейну, його основні компоненти та слої, детально досліджено складові компонентів, зо що вони відповідають. В другому розділі було розглянуто класифікацію атак на блокчейн, головні атаки та вразливості децентралізованого блокчейну, а також способи якими можна знизити ризики їх появи. В третьому розділі було спроєктовано децентралізований блокчейн з оптимальними параметрами захисту і ефективності, блокчейн було максимально захищено від проаналізованих в другому розділі вразливостей, а також спроєктовано на основі аналізу побудови блокчейну з першого розділу.

Теоретична цінність роботи полягає в аналізі поширених вразливостей, проєктуванню блокчейна який буде мінізувати ризики використання цих вразливостей.

Використовуючи цю роботу можна як пободувати оптимальний по параметрам захисту і ефективності блокчейн, так і знайти і усунути вразливості вже наявного.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. 51% Attack: The Concept, Risks & Prevention [Електронний ресурс]. – Режим доступу: https://hacken.io/discover/51-percent-attack/

2. Шевчук Є. В., Федорченко В. М. Аналіз основних вразливостей і способів захисту механізму консенсусу в децентралізованих блокчейн системах. Національний університет “Полтавська політехніка імені Юрія Кондратюка”. Системи управління, навігації та зв’язку. 2024., № 3. С. 72-76.

3. Architectural Patterns for Blockchain Systems and Application Design [Електронний ресурс] – https://www.mdpi.com/2076-3417/13/20/11533

4. Blockchain Architecture Layers: A Comprehensive Guide [Електронний ресурс] – https://hacken.io/discover/blockchain-architecture-layers/

5. Blockchain Common Vulnerability List [Електронний ресурс] – Режим доступу: https://github.com/slowmist/Cryptocurrency-Security-Audit-Guide/blob/main/Blockchain-Common-Vulnerability-List.md

6. Blockchain design principles [Електронний ресурс] – https://wesoftyou.com/web3/blockchain-design-principles/

7. Blockchain Facts: What Is It, How It Works, and How It Can Be Used [Електронний ресурс] – Режим доступу: https://www.investopedia.com/terms/b/blockchain.asp

8. Blockchain Vulnerabilities and Attacks [Електронний ресурс] – Режим доступу: https://www.linkedin.com/pulse/blockchain-vulnerabilities-attacks-yeshwanth-n/

9. Blockchain Security: Common Vulnerabilities and How to Protect Against Them [Електронний ресурс] – Режим доступу: https://hacken.io/insights/blockchain-security-vulnerabilities/

10. Blockchain: The Future of Digital Art and Design [Електронний ресурс] – https://www.smu.edu/meadows/newsandevents/news/2024/blockchain-

the-future-of-digital-art-and-design

11. Consensus Mechanisms In Blockchain: A Deep Dive Into The Different Types [Електронний ресурс] – Режим доступу: https://hacken.io/discover/consensus-mechanisms/

12. Designing a Blockchain Architecture: Types, Use Cases, and Challenges [Електронний ресурс] – https://medium.com/mobindustry/designing-a-blockchain-architecture-types-use-cases-and-challenges-9894fb7b58e

13. Design of blockchain-based applications using model-driven engineering and low-code/no-code platforms: a structured literature review [Електронний ресурс] – https://link.springer.com/article/10.1007/s10270-023-01109-1

14. Design principles for blockchain [Електронний ресурс] – https://merge.rocks/blog/design-principles-for-blockchain

15. Gaffney P., Sonlin K., Blockchain Explained: Your Ultimate Guide to the Tokenization of Finance: Authors Unite Publishing, 2023. 314 p.

16. How does blockchain work [Електронний ресурс] – Режим доступу: https://online.stanford.edu/how-does-blockchain-work

17. How to design a blockchain application architecture [Електронний ресурс] – https://www.highenfintech.com/blogs/how-to-design-a-blockchain-application-architecture/

18. How to design a blockchain application architecture [Електронний ресурс] – https://www.leewayhertz.com/how-to-design-a-blockchain-app-architecture/

19. Lantz L., Cawrey D., Mastering Blockchain. Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications: O'Reilly, 2021. 272 p.

20. Layers of Blockchain Explained [Електронний ресурс] – https://www.lcx.com/layers-of-blockchain-explained/

21. The Developer’s Guide to Blockchain Development [Електронний ресурс] – https://www.xilinx.com/products/design-tools/resources/the-developers-guide-to-blockchain-development.html

22. Understanding Blockchain Technology [Електронний ресурс] – Режим доступу: https://www.forbes.com/advisor/investing/cryptocurrency/what-is-blockchain/

23. Understanding Double-Spending and How to Prevent Attacks [Електронний ресурс] – Режим доступу: https://www.investopedia.com/terms/d/doublespending.asp

24. What is Blockchain Technology [Електронний ресурс] – Режим доступу: https://www.coindesk.com/learn/what-is-blockchain-technology/

25. What Is a Consensus Mechanism [Електронний ресурс] – Режим доступу: https://builtin.com/blockchain/consensus-mechanism

26. What Are Consensus Mechanisms in Blockchain and Cryptocurrency [Електронний ресурс] – Режим доступу: https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp

27. What Is Proof-of-work (PoW)? All You Need to Know [Електронний ресурс] – Режим доступу: https://blockworks.co/news/what-is-proof-of-work

28. What Is Proof of Work (PoW) in Blockchain [Електронний ресурс] – Режим доступу: https://www.investopedia.com/terms/p/proof-work.asp

29. What Does Proof-of-Stake (PoS) Mean in Crypto [Електронний ресурс] – Режим доступу: https://www.investopedia.com/terms/p/proof-stake-pos.asp

30. What is proof of stake [Електронний ресурс] – Режим доступу: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-proof-of-stake

31. What is Delegated Proof of Stake (DPoS)? Your Comprehensive Guide to DPoS [Електронний ресурс] – Режим доступу: https://medium.com/unicorn-ultra/what-is-delegated-proof-of-stake-dpos-your-comprehensive-guide-to-dpos-07fd5185b108

32. What Is Delegated Proof-of-Stake (DPoS) [Електронний ресурс] – Режим доступу: https://www.ledger.com/academy/what-is-delegated-proof-of-stake-dpos

33. What is blockchain [Електронний ресурс] – Режим доступу: https://www.ibm.com/topics/blockchain

34. What is blockchain experience design and why it matters [Електронний ресурс] – https://merge.rocks/blog/what-is-blockchain-experience-design-and-why-it-matters

35. What are blockchain layers [Електронний ресурс] – https://www.skrill.com/en/crypto/the-skrill-crypto-academy/advanced/what-are-blockchain-layers/