Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему
Метод аналізу та оцінювання протоколів консенсусу для блокчейнів з доказом роботи(PoW) та без (PoS)

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

КРМКБ.180126.22.01.08 ПЗ

Виконав: студент 2 курсу, група КБм-22-1 Підпис Гунявий Д.А.

Керівник доц., к.т.н, доцент Підпис Чешун В.М.

Нормоконтролер старший викладач Підпис Мостовий С.В.

До захисту допускаю:
Зав. кафедри кібербезпеки, к.т.н., доц Підпис Кльоц Ю.П.

15 грудня 2023 р.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень) Тема, мета кваліфікаційної роботи, наукова новизна, практична значимість, публікації. Дослідження предметної області. Математична модель методу. Теоретична реалізація методу. Аналіз методу. Висновки.

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали і посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В. Старший викладач кафедри кібербезпеки		

7. Дата видачі завдання «01» вересня 2023р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Вибір напряму дослідження і узгодження тематики КРМ з керівником	01.06.2023	
2	Ознайомлення з предметною областю; формулювання мети і задач дослідження; визначення об'єкта і предмета дослідження	05.09.2023	
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	08.09.2023	
4	Робота над розділом 2 – розробка моделей і методів для вирішення поставленої задачі	01.10.2023	
5	Робота над розділом 3 – теоретична розробка методів	20.10.2023	
6	Робота над розділом 4 – аналіз запропонованих методів	20.11.2023	
7	Робота над науковою публікацією	30.11.2023	
8	Погодження отриманих результатів, оформлення пояснювальної записки згідно вимог	01.12.2023	
9	Попередній захист роботи	18.11.2023	
10	Захист роботи на засіданні ЕК	15.12.2023	

Студент Підпис Д.А. Гунявий Ініціали, прізвище

Керівник проекту (роботи) Підпис В.М. Чешун Ініціали, прізвище

Хмельницький, 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Освітній рівень Магістр

Галузь знань 12 Інформаційних технологій

Спеціальність 125 Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"30" 08 2023 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

Гунявому Денису Андрійовичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод аналізу та оцінювання протоколів консенсусу для блокчейнів з доказом роботи(PoW) та без (PoS)

Керівник роботи Чешун Віктор Миколайович

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

кандидат технічних наук, доцент

Затверджена наказом № 30 ректора університету, додаток №25 від 15.08.2023

2. Строк подання студентом проекту (роботи) на кафедру 11.12.2023

3. Вихідні дані до проекту (роботи) Виявленні нових аспектів та особливостей використання протоколів PoW та PoS у блокчейн-системах та їх впливу на кібербезпеку, аналіз гібридних протоколів консенсусу

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Дослідження протоколів консенсусу з доказом роботи та без. Аналіз впливу блокчейну на кібербезпеку. Постановка задачі дослідження. Математична модель протоколів консенсусу. Теоретична реалізація гібридного протоколу консенсусу. Аналіз отриманих результатів. Висновки.

АНОТАЦІЯ

Тема кваліфікаційної роботи: Метод аналізу та оцінювання протоколів консенсусу для блокчейнів з доказом роботи(PoW) та без (PoS)

Автор роботи: Гунявий Денис Андрійович

Керівник роботи: к.т.н., доц. Чешун Віктор Миколайович

Загальний обсяг роботи: 68 сторінок, 16 рисунків, 1 таблиця, 2 додатки, 47 посилань.

Ключові слова: блокчейн, PoW, PoS.

Основні завдання дослідження включають вивчення принципів і функцій протоколів PoW і PoS, аналіз конкретних реалізацій, порівняльний аналіз їх переваг і недоліків, а також визначення впливу кожного протоколу на безпеку мережі системи.

В роботі представлено теоретична реалізація гібридного алгоритму консенсусу та його аналіз, також розглядаються основні механізми консенсусу в блокчейні, такі як доказ роботи (PoW) і доказ частки (PoS). Досліджуються переваги та недоліки кожного алгоритму, а також обговорюється важливість розробки нових алгоритмів, які поєднують найкращі характеристики обох методів.

05.12.2023

ANNOTATION

Theme of the qualification work: A method for analyzing and evaluating consensus protocols for blockchains with and without proof of work (PoW)

Author of the work: Huniavyi Denys Andriiovych

Mentor: Ph.D. Cheshun Viktor Mykolaiovych

Total volume of work: 68 pages, 16 figures, 1 tables, 2 appendices, 47 links.

Keywords: blockchain, PoW, PoS.

The main objectives of the study include the study of the principles and functions of the PoW and PoS protocols, the analysis of specific implementations, a comparative analysis of their advantages and disadvantages, and the determination of the impact of each protocol on the security of the system's network.

The paper presents a theoretical implementation of the hybrid consensus algorithm and its analysis, and discusses the main consensus mechanisms in the blockchain, such as proof of work (PoW) and proof of stake (PoS). The advantages and disadvantages of each algorithm are explored, and the importance of developing new algorithms that combine the best characteristics of both methods is discusse

05.12.2023.

ЗМІСТ

ВСТУП

У сучасному світі, де технологічний прогрес швидко змінює картину економічного та соціального розвитку, кібербезпека та блокчейн-технології стають ключовими напрямками для досліджень та впроваджень. Спеціалісти у галузі кібербезпеки та розробники блокчейн-рішень постійно вдосконалюють методи та засоби для забезпечення надійності, конфіденційності та цілісності інформації.

Актуальність дослідження полягає в тому, що в сучасному світі, де технологічний прогрес диктує умови розвитку, особлива увага приділяється аналізу та оцінці протоколів консенсусу в галузі кібербезпеки та блокчейнів. Ця тема стає надзвичайно актуальною в контексті загроз кібербезпеці та стрімкого розвитку блокчейн-технологій, особливо для країни, яка активно впроваджує їхні досягнення[1].

Метою кваліфікаційної роботи є систематизація, аналіз та оцінка протоколів консенсусу для блокчейнів з доказом роботи (PoW) та без (PoS). Основні завдання дослідження включають дослідження принципів та функцій протоколів PoW та PoS, аналіз конкретних реалізацій, порівняльний аналіз їхніх переваг та недоліків, а також визначення впливу кожного протоколу на кібербезпеку системи.

Об’єктом дослідження є протоколи консенсусу для блокчейнів, зокрема їхні реалізації з доказом роботи та без нього. Дослідження фокусується на аспектах, пов'язаних з ефективністю, масштабованістю та забезпеченням кібербезпеки.

Предметом дослідження стають процеси та явища, що виникають в результаті використання протоколів консенсусу в блокчейн-системах, з урахуванням їх взаємодії з кібербезпекою.

Для досягнення поставлених завдань потрібно:

а) використовуючи аналітичні методи виявити способи вдосконалення методу аналізу протоколів консенсусу з доказом роботи та без;

б) визначити основні положення використання блокчейн технологій у кібербезпеці;

в) розробити математичну модель PoW та PoS;

г) зробити теоретичну реалізацію технологій;

д) реалізувати експеремент з гібридним алгоритмом консенсусу.

Наукова новизна даної роботи полягає в:

1. Виявленні нових аспектів та особливостей використання протоколів PoW та PoS у блокчейн-системах та їх впливу на кібербезпеку.

2. Реалізація гібридного протоколу консенсусу PoW та PoS.

Проведене дослідження має визначити ступінь новизни та внести внесок у розвиток області.

Практичне значення отриманих результатів полягає у тому, що вони можуть бути використані для розробки та вдосконалення блокчейн-систем з урахуванням вибору енергоефективного протоколу консенсусу.

Публікації. За темою магістерської роботи було опубліковано 3 тези доповідей.

1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Блокчейн-технології

У сучасному інформаційному суспільстві цифрові технології проникли в усі сфери життя, а забезпечення безпеки мережі стало дуже важливим і незамінним завданням. Однак, з іншого боку, традиційні методи забезпечення безпеки, засновані на централізованих структурах і централізованих даних, стикаються з проблемою зростання кіберзагроз. На цьому тлі технологія блокчейн виникла як реакція на відсутність довіри до централізованих систем і набула дедалі більшого значення у сфері кібербезпеки.

Блокчейн – це розподілена база даних, яка записує та зберігає інформацію у вигляді взаємопов’язаних блоків. Кожен блок містить хеш-код попереднього блоку, час створення та саме повідомлення. Однією з ключових характеристик блокчейну є незмінність, що означає[2], що записану інформацію неможливо змінити. Це робить систему надійною та відрізняється від традиційних централізованих баз даних. Технологія блокчейн широко використовується в мережевій безпеці:

– захист від кібератак;

– ідентифікація та автентифікація;

– смарт-контракти: які використовують блокчейн, дозволяють автоматизовано виконувати та здійснювати угоди, що сприяє уникненню шахрайства та забезпечує дотримання умов угод.

Однією з ключових переваг блокчейну в області кібербезпеки є його здатність унеможливити зміну чи видалення даних. Це робить систему менш вразливою до атак, спрямованих на знищення чи модифікацію інформації.

Блокчейн може вдосконалити процес ідентифікації та автентифікації, забезпечуючи безпеку особистих даних та усунення ризиків, пов'язаних з централізованими базами даних.

Однак, разом із всіма перевагами, блокчейн також стикається з мінусами, такими як швидкість транзакцій та високі витрати на енергію. Для того, щоб забезпечити більш широке впровадження блокчейн-технологій в кібербезпеці, необхідно вирішити ці проблеми[3].

Блокчейн – це розподілена, незмінна та децентралізована книга, що складається з ланцюжка блоків, і кожен блок містить набір даних. Блоки пов'язані між собою за допомогою криптографічних методів і утворюють хронологічний ланцюжок інформації[4]. Структура блокчейну розроблена для забезпечення безпеки даних за допомогою механізму консенсусу, який має мережу вузлів, які узгоджують дійсність транзакцій перед додаванням їх до блокчейну.

Блок в блокчейні – це комбінація трьох основних компонентів[5]:

– заголовок містить такі метадані, як позначка часу з випадковим числом, що використовується в процесі видобутку, і хеш попереднього блоку;

– розділ даних містить основну та актуальну інформацію, таку як транзакції та смарт-контракти, які зберігаються в блоці;

– хеш – це унікальне криптографічне значення, яке працює як представник усього блоку, який використовується для перевірки.

Час блоку – це час, необхідний для створення нового блоку в блокчейні. Різні блокчейни мають різний час блокування, який може варіюватися від кількох секунд до хвилин або також у години. Коротший час блокування може дати швидші підтвердження транзакцій, але результат має вищі шанси на конфлікти, але довший час блокування може збільшити час для підтвердження транзакцій, але зменшити ймовірність конфліктів. Децентралізація є ключовою особливістю технології блокчейн[6]. У децентралізованому блокчейні немає єдиного центрального органу, який міг би контролювати мережу. При децентралізації повноваження щодо прийняття рішень розподіляються між мережею вузлів, які спільно перевіряють і погоджують транзакції, які потрібно додати до блокчейну. Цей децентралізований характер технології блокчейн сприяє прозорості, довірі та безпеці[7]. Це також зменшує ризик покладатися на єдину точку відмови та мінімізує ризики маніпулювання даними.

Технологія блокчейн – це структура, яка зберігає публічні записи транзакцій, також відомі як блок, у кількох базах даних, відомих як «ланцюжок», у мережі, з'єднаній через однорангові вузли. Зазвичай таке сховище називають «цифровою книгою».

Кожна транзакція в цій книзі авторизована цифровим підписом власника, який засвідчує транзакцію та захищає її від підробки. Отже, інформація, яка міститься в цифровій книзі, є високозахищеною.

Простіше кажучи, цифровий реєстр схожий на електронну таблицю Google, яку використовують численні комп'ютери в мережі, в якій зберігаються записи про транзакції на основі фактичних покупок. Захоплюючий кут полягає в тому, що будь-хто може бачити дані, але не може їх пошкодити[8].

Ці типи транзакцій можуть бути підроблені дуже швидко. Люди, які знайомі з цією правдою, часто обережно ставляться до використання таких типів транзакцій, звідси еволюція сторонніх платіжних програм за останні роки. Але ця вразливість, по суті, є причиною створення технології Blockchain[9].

Облік даних і транзакцій є важливою частиною бізнесу. Часто ця інформація обробляється вдома або передається через третю сторону, як-от брокери, банкіри чи юристи, що збільшує час, вартість або і те, і інше для бізнесу. На щастя, Blockchain дозволяє уникнути цього тривалого процесу та сприяє швидшому переміщенню транзакції, тим самим заощаджуючи час і гроші.

Більшість людей припускає, що Blockchain і Bitcoin можна використовувати як взаємозамінні, але насправді це не так. Блокчейн – це технологія, здатна підтримувати різноманітні додатки, пов'язані з багатьма галузями, як-от фінанси, ланцюг поставок, виробництво тощо, але біткойн – це валюта, яка покладається на технологію блокчейну, щоб бути безпечною[10].

Блокчейн – це технологія, яка має багато переваг у все більш цифровому світі. До них відносяться:

– високий рівень безпеки, де блокчейн використовує функцію цифрового підпису для проведення транзакцій без шахрайства. Це означає, що дані не можуть бути пошкоджені або змінені без спеціального цифрового підпису.

– децентралізація блокчейну, що означає, що транзакції здійснюються за взаємною згодою користувачів. Це призводить до більш плавних, безпечніших і швидших транзакцій[11].

– можливість автоматизації полягає у тому, що блокчейн програмований і може автоматично генерувати систематичні дії, події та платежі, коли виконуються критерії тригера.

Блокчейн складається з ланцюжка блоків, які містять інформацію про транзакції. Кожен блок містить хеш попереднього блоку, що забезпечує зв'язок між блоками та запобігає їхньому зміні.

Щоб додати новий блок до блокчейну, мережа вузлів повинна узгодити його дійсність. Цей процес називається механізмом консенсусу[12].

Остаточність означає необоротне підтвердження транзакцій у блокчейні [13]. Якщо транзакція додається до блоку і блок підтверджується мережею, вона стає незмінною і не може бути скасована.

Блокчейн – це поєднання трьох провідних технологій[13]:

– криптографічні ключі;

– однорангова мережа, що містить спільну книгу;

– обчислювальний засіб для зберігання транзакцій і записів мережі.

Ключі криптографії складаються з двох ключів – закритого та відкритого. Ці ключі допомагають виконувати успішні транзакції між двома сторонами. Кожна особа має ці два ключі, які вони використовують для створення захищеного посилання цифрової ідентифікації. Ця захищена ідентифікація є найважливішим аспектом технології Blockchain. У світі криптовалют цей ідентифікатор називається «цифровий підпис» і використовується для авторизації та контролю транзакцій[14].

Цифровий підпис об'єднується з одноранговою мережею; велика кількість осіб, які діють як органи влади, використовують цифровий підпис, щоб досягти консенсусу щодо транзакцій, серед інших питань. Коли вони санкціонують угоду, вона засвідчується математичною перевіркою, що призводить до успішної захищеної транзакції між двома підключеними до мережі сторонами. Підводячи

підсумок, користувачі Blockchain використовують криптографічні ключі для виконання різних типів цифрових взаємодій у одноранговій мережі[15].

Існує кілька типів блокчейнів, а саме публічні, приватні та консорціальні. Публічні блокчейни, такі як Bitcoin та Ethereum, відкриті для громадськості та вимагають мінімальної централізації. Приватні блокчейни призначені для використання обмеженими групами людей чи організацій. Консорціальні блокчейни поєднують елементи обох попередніх типів, забезпечуючи баланс між централізованістю та децентралізацією[16].

1.2 Блокчейн технології та кібербезпека

Технологія блокчейн стає найвищою зброєю в боротьбі з кіберзлочинністю. Це не лише інноваційна технологія, яка революціонізує спосіб зберігання та обміну даними, але й потужний інструмент кібербезпеки.

Blockchain забезпечує безпечну, прозору та незмінну платформу для зберігання та обміну цифровими даними. Використовуючи потужність технології розподіленої книги, організації можуть гарантувати, що їхні дані захищені від маніпуляцій, несанкціонованого доступу та зловмисних атак будь-яка спроба отримати несанкціонований доступ до одного чи кількох комп’ютерів з наміром завдати шкоди є кібератакою. Він намагається вивести з ладу комп’ютери, викрасти дані або використати зламану комп’ютерну систему для подальших атак[17].

У жовтні 2020 року Google опублікувала подробиці попередньої кібератаки, розпочатої проти її серверів у вересні 2017 року. У звіті інцидент описується як іноземна атака розподіленої відмови в обслуговуванні (DDoS), яка посилювалася протягом шестимісячної кампанії. Це була найбільша атака такого роду в історії.

DDoS-атака на клієнта Amazon Web Services (AWS) у лютому 2020 року стала наймасштабнішою атакою на AWS і однією з найбільших публічно розкритих атак на будь-кого.

До 2025 року дослідники Cybersecurity Ventures прогнозують збитки в усьому світі на 10,5 трильйонів доларів (приблизно 32 000 доларів на людину в США). Кібератаки відбуваються кожні 39 секунд і накопичують до 30 000 зломів на день.

Зловмисники використовують розподілену природу Інтернету, щоб зберегти анонімність і подолати опір своїм атакам. Звичайний метод DDoS працює шляхом зараження кількох вузлів у різних доменах для формування напівскоординованої мережі під назвою «Ботнет». Ці окремі боти викрадають для здійснення атак на високо централізовані цілі, що часто дає хакерам асиметричну перевагу. Розглянемо рисунок 1.1 для розуміння типів кібератак[19].

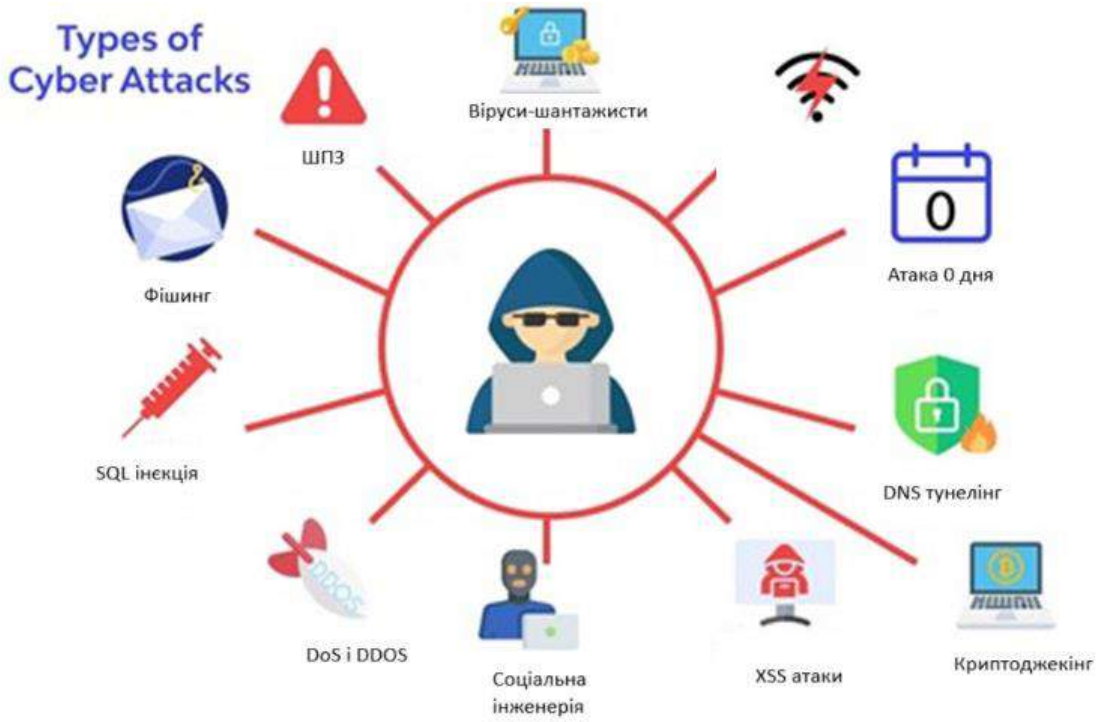

Рисунок 1.1 – Типи кібератак

Більш розподілене розгортання програмного забезпечення, керування базами даних і протоколи безпеки роблять цілі менш вразливими, розподіляючи поверхні атак і покладаючись на менш централізовану довіру. Ключ до цього децентралізованого підходу може полягати в рішенні, яке вже має кілька функцій, які роблять його стійким до атак блокчейну. У разі успіху кібератаки можуть

завдати шкоди підприємствам. Кібератаки можуть завдати різноманітної шкоди, від збою роботи служб до викрадення конфіденційних даних. Їх можна використовувати, щоб знищувати веб-сайти, мережі та системи, а також припиняти роботу служб і викрадення особистої інформації[20]. Кібератаки також можуть бути використані для цілей критичної інфраструктури, що призведе до відключень електроенергії, забруднення води та інших пошкоджень. Вони можуть спричинити цінні простої, втрату даних або маніпуляції, а також втрату грошей через викуп. Крім того, простой може призвести до серйозних перебоїв у наданні послуг і фінансових втрат, наприклад:

– атаки DoS, DDoS і зловмисне програмне забезпечення можуть спричинити збої системи або сервера;

– DNS-тунелювання та атаки SQL-ін’єкції можуть змінювати, видаляти, вставляти або викрадати дані з системи;

– фішинг і експлойт-атаки нулевого дня дозволяють зловмисникам проникнути в систему, щоб завдати шкоди або викрасти цінну інформацію.

Технологія блокчейн має кілька корисних застосувань у сфері кібербезпеки, наприклад:

– децентралізована безпека – технологія блокчейн дозволяє створювати децентралізовані системи безпеки. Завдяки тиражуванню даних на кількох вузлах у мережі хакерам стає важче зламати систему, оскільки їм потрібно буде скомпрометувати декілька вузлів одночасно. Це потужна функція для захисту даних, систем і програм;

– дані, що зберігаються в Blockchain, є незмінними і не можуть бути змінені або видалені після їх запису. Ця функція може бути використана для створення захищених від несанкціонованого доступу журналів аудиту та журналів транзакцій[21]. Використовуючи Blockchain, стає майже неможливим змінити або фальсифікувати дані, що може бути дуже корисним для виявлення та запобігання шахрайству;

– смарт-контракти – це самовиконувані контракти, де умови угоди між покупцем і продавцем записуються безпосередньо в рядку коду. Технологія

блокчейн забезпечує безпечну платформу для розгортання смарт-контрактів, які можна використовувати для автоматизації процесів і усунення потреби в посередниках;

– криптографічна безпека – технологія блокчейн покладається на криптографічні алгоритми для захисту транзакцій і даних. Використання криптографічних хешів і цифрових підписів допомагає запобігти фальсифікації даних і забезпечити цілісність інформації, що зберігається в Blockchain;

– технологію блокчейн, зображену на рисунку 1.2, також можна використовувати для створення децентралізованих систем керування ідентифікацією.

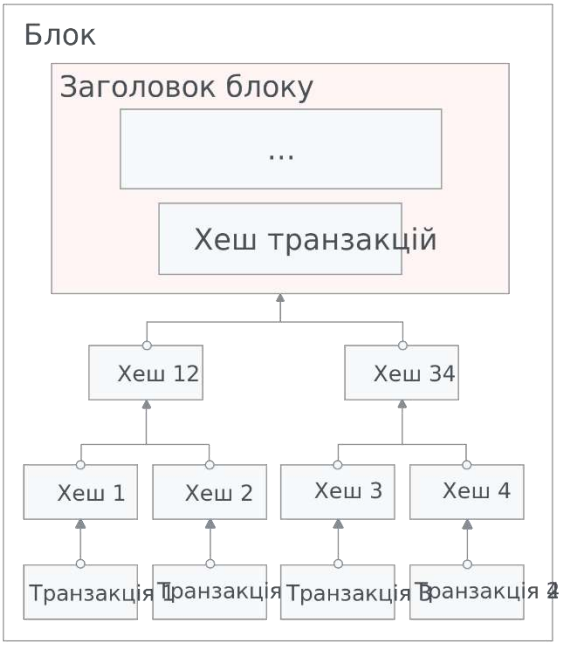

Рисунок 1.2 – Блокчейн технології

Використовуючи Blockchain, люди можуть контролювати свою особисту інформацію, зменшуючи ризик крадіжки особистих даних та інших типів кібератак[22]. Загалом поєднання децентралізованої безпеки, незмінних записів, безпечних смарт-контрактів, криптографічної безпеки та децентралізованого керування ідентифікацією робить технологію Blockchain цінним інструментом у боротьбі з кіберзагрозами.

Технологію блокчейн можна використовувати для запобігання витоку даних, крадіжці особистих даних, кібератакам або злочинним діям у транзакціях.

Це гарантує конфіденційність і безпеку даних, які є основою як кібербезпеки так і блокчейну, зображено на рисунку 1.3. Дійсно, це може покращити кіберзахист, будучи платформою для запобігання шахрайським діям за допомогою механізмів консенсусу[23].

Блокчейн може також виявляти фальсифікацію даних через такі основні характеристики, як операційна стійкість, шифрування даних, можливість аудиту, прозорість і незмінність.

Рисунок 1.3 – Основи безпеки блокчейну

Конфіденційність є однією з основних властивостей блокчейн надає широкі можливості для забезпечення анонімності користувача. Ключі користувача є єдиною ланкою між користувачем і його даними. Однак ці ключі також легко анонімізувати. У результаті, будучи відкритим і пропонуючи широкі можливості для відстеження транзакцій, Blockchain дозволяє користувачам підтримувати безпрецедентний рівень анонімності.

Цілісність даних, так як блокчейни розроблені як книги, де кожен блок пов’язаний із сусідніми блоками за допомогою криптографічних хеш-функцій. Таким чином, після запису транзакції в Blockchain її не можна змінити або видалити. Будь-які зміни, внесені до вже записаних даних, обробляються як нові транзакції.

Доступність наявність багатьох вузлів забезпечує стійкість Blockchain, навіть якщо деякі вузли недоступні. І оскільки кожен вузол у мережі має копію розподіленої книги, правильний блокчейн залишається доступним для інших однорангових вузлів навіть у випадку скомпрометованого вузла.

Існує декілька типів систем керування доступом, а саме DAC, RBAC і ABAC. Контроль доступу на основі атрибутів (ABAC) може бути переосмислений у майбутньому з рішенням доступу користувача до транзакцій на основі ідентифікації. Дані, що зберігаються та переміщуються всередині рішення на основі блокчейну, зашифровані. Таким чином, його можна використовувати для створення надійнішої та безпечнішої ідентифікації та керування доступом[24].

Парадигма інфраструктури відкритих ключів (PKI) часто визнається хорошою технікою безпеки. Проте він базується на кількох визначених проблемах. Розумний контракт можна налаштувати для виклику певних операцій PKI, сутності можуть мати кілька атрибутів для автентифікації за допомогою відкритого ключа/адреси Ethereum.

Ланцюжок системи доменних імен (DNS) виник як добре відома ініціатива змінити інфраструктуру DNS і захистити її від атак спуфінгу. Він замінює сертифікати X.509 інфра-відомістю відкритого ключа, стійкого до MITM. Це сприяє використанню мережі DNS на основі Ethereum для підключення клієнтів і серверів імен, а не централізації кореневого сервера системи. Служби запобігання DDoS також можуть одночасно розгортати розподілену книгу для IP-адрес із чорного списку, зменшуючи небезпеку єдиної точки збою для централізованого рівня веб-додатків.

Можна створити OTP-генерацію на основі Ethereum, яка безпосередньо не взаємодіє з програмою користувача, але сильно обмежена смарт-контрактом.

Потужна комбінація HashCash і смарт-контрактів пропонує набір інструментів безпеки, які є розповсюдженими, одноранговими, на основі криптографії та часто з відкритим кодом.

Запобігання маніпулюванню даними: поєднання хешування та криптографії з децентралізованою структурою надає Blockchain його найпотужнішу функцію,

як-от незмінність. Це допомагає захистити цілісність даних і виявити будь-який тип підробки даних. Keyless Signature Infrastructure (KSI) – це нова технологія, розроблена компанією під назвою Guardtime, яка замінює інфраструктуру відкритих ключів (PKI). KSI додає автентифікацію до існуючих функцій PKI[25].

Захист особистих даних: публікація ключів на Blockchain усуває ризик розповсюдження помилкових ключів і крадіжки ідентифікаційних даних. Тривають різні проекти, спрямовані на усунення необхідності видачі сертифікатів центральними органами влади. Ці досягнення зробили технологію Blockchain більш надійною з точки зору автентифікації та усунення будь-якої можливості бути єдиною точкою відмови.

Запобігання DDoS: наразі система DNS покладається на кешування. Це було підтверджено 21 жовтня 2016 року, коли мільйони користувачів у США були відрізані від основних веб-сайтів. Децентралізована природа Blockchain пропонує вирішення цієї проблеми рисунок 1.4.

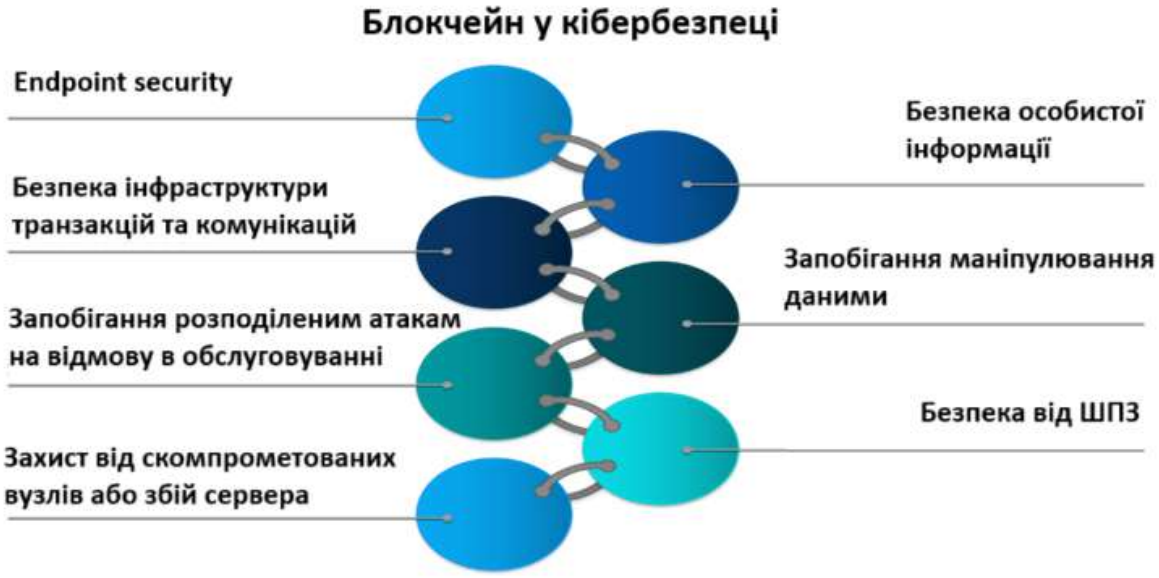

Рисунок 1.4 – Блокчейн в кібербезпеці

Процес ланцюжка блокчейнів: блоки в книзі блокчейнів розташовані в порядку та складаються разом для виконання транзакцій. Блок складається з заголовка та тіла. Усі блоки мають часові позначки та підписи їх творців. Блоки

утворюють ланцюжок, визначаючи покажчик на попередній блок. Заголовок містить криптографічний хеш попереднього блоку, що забезпечує незмінність останнього блоку.

Розподілена архітектура: розподілена мережа є стабільною в роботі, оскільки не має єдиної точки відмови. Ризик поширюється на багато вузлів, і атака на будь-який окремий вузол або кілька вузлів не скомпрометує реєстр. Таким чином, децентралізація робить мережу Blockchain менш привабливою мішенню для атак програм-вимагачів. Навпаки, інформація, що зберігається централізовано, більш сприйнятлива до атак, ніж інформація, що зберігається на кількох вузлах [26].

Основними властивостями блокчейна є децентралізація та шифрування. Кожен користувач має закритий ключ для додавання блоків і внесення змін, а також відкритий ключ, щоб надати іншим доступ до бази даних і спостерігати за змінами. Оскільки Blockchain є розподіленою системою, отримати облікові дані користувача для доступу до систем набагато складніше, якщо не неможливо, і щоб видалити весь Blockchain, кожен вузол потрібно знищити вручну (рисунок 1.5).

Покращення ідентифікації та керування доступом – технологія децентралізовано зберігає облікові дані в Blockchain, знижуючи ризики вторгнення в систему та шахрайства з доступом, оскільки хакерам потрібно використовувати точки входу, щоб отримати доступ до даних. Ми повністю усвідомлюємо, що помилка співробітника є основною причиною крадіжки облікових даних, які централізовано зберігаються та керуються.

Відстеження змін у блокчейні допомагає запобігти несанкціонованим змінам даних і крадіжці. Будь-які зміни, які ви вносите в Blockchain, є незворотними, тому ви не можете повернутися назад і скасувати їх. Крім того, оновлення або нові дані не видаляють і не замінюють старі дані; натомість вони будуть записані у верхній частині Blockchain із правом власності та міткою часу, що дозволить відстежити їх у разі атаки та дозволить відстежувати джерело.

Забезпечення резервування, так як, розподілений блокчейн постійно присутній у багатьох місцях. Оскільки різні комп’ютери зберігають копії даних

Blockchain, у разі ненавмисної чи навмисної маніпуляції ви можете знайти вихідні дані в інших джерелах.

Рисунок 1.5 – Як блокчейн змінить кібербезпеку

DDoS-атаки – це часті кібератаки, які намагаються перевантажити корпоративні системи запитами, призвести до збою та зробити їх непридатними для використання. DDoS-атаки є простими, оскільки частини DNS зберігаються централізовано та сприйнятливі до атак і крадіжок, які можуть бути використані для знищення систем. Використання децентралізованого блокчейну мінімізує крадіжки DNS і DDoS-атаки. Крім того, кібератаки миттєво виявляються та запобігаються шляхом запобігання проникненню зловмисних даних у систему, оскільки кожна модифікація блоку в Blockchain має бути підтверджена іншими блоками.

1.3 Протоколи консенсусу (PoW та PoS)

PoW це найстаріший і найпопулярніший на даний момент механізм консенсусу. Примітно, що перша згадка про алгоритми датується винаходом мережі Bitcoin. Цікаво, що дослідження алгоритму сягають початку 90-х років, коли Моні Наор і Синтія Дворк опублікували статтю в 1993 році. У статті автори досліджували потенціал алгоритму для запобігання шахрайству.

У 1999 році інший дослідник криптографії, Маркус Якобссон, ввів термін «Proof-of-Work» і він закріпився до тих пір, поки Сатоші Накамото не здивував світ винаходом біткойна. Зокрема, мережа блокчейнів біткойнів є просто реалізацією досліджень, перші кроки яких датуються 1993 роком.

Алгоритм PoW залишається найпопулярнішим, тому що він один з небагатьох, який не може бути скомпрометований. З технічної точки зору, це один із тих алгоритмів, які можуть досягти візантійської відмовостійкості. Примітно, що візантійська відмовостійкість (BFT) – це просто здатність системи протистояти збоям, які пов’язані з проблемою візантійських генералів.

Це означає, що мережа може успішно уникати ситуацій, коли деякі вузли можуть намагатися діяти проти консенсусу. У контексті технології блокчейн очевидно, що мережі блокчейну не мають центрального органу для модерування транзакцій. Замість цього публічна книга розподіляється між усіма учасниками, отже, технологія блокчейну також відома як технологія розподіленої книги (DLT) [27].

Враховуючи цінну інформацію, яка зберігається в публічних бухгалтерських книгах, існує висока ймовірність того, що деякі зловмисники можуть захотіти спричинити помилки заради егоїстичних вигод. Таким чином, ці погані актори представляють проблему візантійських генералів. Таким чином, мережа блокчейнів повинна мати візантійську відмовостійкість, щоб уникнути таких проблем.

Proof of Work – це консенсусний алгоритм блокчейну Bitcoin. Його називають «Доказом роботи», тому що він вимагає певного типу роботи – зазвичай комп’ютерної обробки – від вузлів-учасників (майнерів) у мережі

Bitcoin. Якщо наразі не враховувати пули для майнінгу, то це особлива група користувачів біткойнів, які називаються майнерами, які здійснюють перевірку транзакцій у блокчейні. Майнери завантажили повний блокчейн Bitcoin і вирішили запустити його на потужних комп'ютерах рисунок 1.6.

Рисунок 1.6 – Майнинг

Ці користувачі (вузли) у мережі Bitcoin називаються «майнерами», тому що вони перевіряють і доводять точність транзакції в процесі, який називається майнінг – подібно до обчислення складної математичної задачі. Протягом цього процесу майнерів стимулюють діяти так, щоб принести користь усім членам біткойн-спільноти, оскільки чесність окупається.

Після того, як запит на запис і завершення транзакції поширюється в блокчейні, зазвичай транзакції з найвищою запропонованою комісією вибираються для переходу в наступний блок у блокчейні.

Щоб досягти консенсусу щодо дійсного блоку в ланцюжку блоків, алгоритм біткойна передбачає параметр складності, який має бути виконаний, щоб блок був дійсним. Ця «складність» регулярно змінюється мережею Bitcoin залежно від обчислювальної потужності майнерів. Складність можна зменшити або

збільшити, щоб підтримувати постійну швидкість додавання нових блоків.

Для цілей криптографії до блоку додається довільне число, яке називається nonce (абревіатура від «число, що використовується лише один раз»). Майнери змінюють nonce, доки не буде знайдено значення, яке надає хешу блоку необхідний рівень складності. Після виконання цієї вимоги блок не можна змінити без повторного виконання роботи[28]. Потім вузол «хешує» вибраний набір даних. Слово «перемішувати» походить від французького слова «hacher», що означає «подрібнити на дрібні шматочки». Під час хешування алгоритм, який називається хеш-функцією, використовується для перетворення одного значення (вибраного набору даних) у вихідне значення фіксованого розміру – хеш-значення, таким чином маскуючи вихідне значення.

Хеш-функцію не можна обробити, тобто хеш-значення не можна використовувати для визначення вихідних даних. Таким чином, хеш-значення є «відбитком пальця», який забезпечує ретельну автентифікацію та гарантує, що переданий вміст не було підроблено. Кожне хеш-значення містить інформацію про всі попередні мережеві транзакції.

Щойно згенерований хеш перевіряється на поточну складність. Хеш-значення завжди має містити певну кількість нульових біт. Якщо хеш відповідає критеріям складності, він транслюється іншим майнерам у мережі. Якщо ні, вибирається та хешується інший nonce. Майнери генерують багато хешів з різними nonces, поки не знайдуть той, який відповідає необхідним критеріям. Цей повторюваний процес відомий як «видобуток», і тепер ви знаєте, чому він потребує так багато енергії.

Кожного разу, коли з’являється новий блок, з’являється новий шанс отримати винагороду для іншого майнера. З цієї причини перевірка транзакцій у блокчейні біткойн схожа на нескінченну золоту лихоманку, коли тисячі майнерів по всьому світу одночасно майніть, щоб першими виявити блок.

Справжнім блокчейном біткойн завжди вважається найдовша версія блокчейну біткойн. Якщо між більшістю учасників мережевих майнерів виникне суперечка щодо правил обробки та перевірки транзакцій, така дискусія може

зрештою призвести до незалежного ланцюга блокчейну, так званого форку. Однак у більшості випадків у майнерів немає реальних причин порушувати правила через величезну вартість часу та грошей, необхідних для безперервного видобутку.

Іншим недоліком процесу підтвердження роботи є те, що більші майнінгові пули мають більшу обчислювальну потужність при доступі, а отже, більші шанси видобутку дійсних блоків, що ставить окремих майнерів у невигідне становище.

Такі протоколи, як Lightning Network, мають на меті покращити швидкість і масштабованість мережі Bitcoin. На даний момент Lightning Network реалізована лише в дуже простому вигляді, це протокол другого рівня на вершині мережі біткойн, призначений для зняття тиску великої кількості транзакцій із центрального блокчейну біткойнів.

Інші механізми та алгоритми можуть бути кращими за Proof of Work, проте Proof of Work є найбільш добре запровадженим і перевіреним часом проти атак з точки зору відносного зародження біткойна та технології блокчейн. Висока вартість також є фактором зміцнення консенсусу та стримування учасників мережі від виділення ресурсів альтернативним мережам. Отже, висока ймовірність того, що алгоритм підтвердження роботи буде постійно вдосконалюватися розробниками для усунення його недоліків рисунок 1.7.

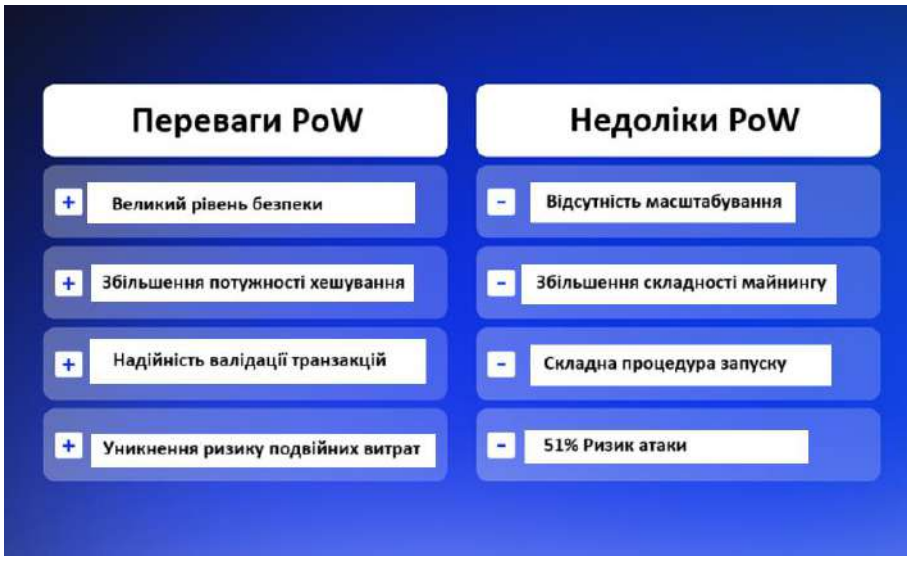

Рисунок 1.7 – Переваги і недоліки PoW

У двох словах, алгоритм консенсусу – це набір правил, які керують мережею блокчейн. Це угода щодо правил конкретного блокчейну та того, як користувачі можуть брати участь у мережі.

Алгоритм консенсусу Proof of Stake (PoS) – це набір правил, що регулюють мережу блокчейну та створення її нативної монети, тобто він має ту саму мету, що й алгоритм Proof of Work (PoW), у тому сенсі, що він є інструмент для досягнення консенсусу. На відміну від PoW, у процесі немає майнерів.

Натомість учасники мережі, які хочуть брати участь у підтвердженні дійсності мережевих транзакцій і створенні блоків у мережі PoS, повинні мати певну частку в мережі, наприклад, помістивши певну суму валюти мережі в гаманець, підключений до свого блокчейну[29].

Це відомо як «розміщення ставки» або «ставка». Творець блоку в системі PoS обмежений створенням блоків, пропорційних його чи її частці в мережі.

Алгоритм Proof-of-Stake (PoS) працює наступним чином.

1. Учасники мережі володіють певною кількістю монет криптовалюти, які вони можуть вкласти в ставку (stake) як гарантію своєї участі в мережі.

2. Вибір блоку, який буде доданий до блокчейну, здійснюється на основі випадкового алгоритму, але з урахуванням ваги ставки учасників. Чим більше монет вкладено в ставку, тим більша ймовірність, що учасник буде обраний для формування нового блоку.

3. Обраний учасник стає "заготовкою" для формування нового блоку. Він перевіряє транзакції, створює новий блок та підписує його своїм приватним ключем.

4. Новий блок додається до блокчейну, і учасник отримує винагороду за свою роботу, яка може складатися з транзакційних комісій та новостворених монет.

5. Ітерація процесу повторюється знову, де новий обраний учасник здійснює формування наступного блоку.

Цей процес дозволяє PoS мережам досягти консенсусу шляхом використання власностей (ставки) учасників, а не обчислювальної потужності, як у Proof-of-Work (PoW).

Таким чином, мережі PoS базуються на детермінованих алгоритмах, тобто валідатори блоків обираються залежно від характеру ставки. Наприклад, вибір балансу рахунку як єдиного критерію, за яким визначається наступний дійсний блок у блокчейні, потенційно може призвести до небажаної централізації. Це означатиме, що заможні учасники мережі отримають великі переваги.

Мережі PoS засновані на детермінованих алгоритмах, тобто валідатори блоків обираються залежно від характеру ставки. З цієї причини існують різні методи відбору для визначення ставки або їх комбінація. Різні криптовалюти, які використовують PoS, використовують різні варіанти визначення «ставок».

Приклади таких варіантів включають ефективний баланс монет на рахунку, стаціонарний час, коли токени повинні бути в блокчейні.

З одного боку, PoS усуває деякі слабкі місця системи PoW, що стоїть за криптовалютами, такими як біткойн. PoS фактично усуває перешкоди для входу в процес перевірки. Користувачам більше не потрібно купувати спеціалізовані комп'ютери лише для того, щоб отримати шанс виграти ту невловиму винагороду за блок. Отже, PoS вимагає менше обчислювальної потужності, ніж PoW, і, отже, також має менший вплив на навколишнє середовищер[30].

З іншого боку, деякі мережі PoS мають серйозні недоліки, залежно від варіантів, які використовуються для визначення частки в мережі. Виробники блоків деяких монет можуть володіти неймовірною потужністю, якщо кількість виробників блоків у мережі невелика, і вони можуть підтверджувати всі транзакції. Проте повноваження продюсера можуть бути автоматично скасовані щоразу, коли він або вона робить щось проти інтересів мережі. Якщо, наприклад, виробник монети EOS не працює над будь-яким блоком протягом 24 годин, резервна копія швидко займає його місце.

Друга велика слабкість полягає в тому, що ряд систем PoS віддають перевагу заможним користувачам - чим більше монет ви ставите, тим більше ви

можете проголосувати. Такі мережі, як Cardano, вже вирішили цю проблему, впровадивши рандомізований вибір виробників блоків. У цьому випадку заможніші користувачі все ще мають більше шансів стати виробником блоків, але зовнішній вплив «криптокитів» – учасників, які тримають набагато більше монет певної мережі, ніж середній користувач – зменшується.

Нарешті, існує проблема в мережі Proof-of-Stake, відома як «нічого не поставлено на карту». У мережі PoW рідко трапляється, що два майнери створюють блок майже одночасно в результаті затримки в часі. Це призводить до тимчасової плутанини в мережі, і вузли повинні досягти консенсусу щодо дійсного блоку. Отже, майнерам потрібно вибрати, на яку версію блокчейну витрачати свої ресурси, таким чином обходячи інші можливості.

Однак, як і в системі PoS, підробка нових блоків потребує мало ресурсів, валідатор може вирішити продовжити роботу над кількома версіями розгалуження та підробити нові блоки. Оскільки немає альтернативних витрат для підробки в конкретному блокчейні, «ніщо не поставлено на карту» для користувачів, які створюють блоки. Як наслідок, користувачі могли майнити на конкуруючих гілках блокчейну, щоб максимізувати суму комісії за транзакції, яку вони отримують. Щоб вирішити цю проблему, більшість монет PoS мають додаткові механізми захисту, вбудовані в їхній протокол.

Алгоритм консенсусу делегованого підтвердження частки (DPoS) є різновидом протоколу консенсусу Proof of Stake. Користувачі мережі обирають достатню кількість делегатів, яких також називають свідками, щоб забезпечити децентралізацію мережі. Обрані делегати перевіряють транзакції та генерують блоки. Якщо делегат отримує винагороду за блок, він зазвичай ділиться нею з тими гаманцями, які проголосували за нього і також мають частку в мережі.

Якщо представнику не вдається перевірити транзакції або в мережі виникають інші збої, цей механізм консенсусу забезпечує швидке виявлення розбіжностей і заміну виробників блоків, які не відповідають консенсусу.

На даний момент біткойн залишатиметься серед провідних криптовалют. Однак, у світлі потреби в енергоефективних механізмах консенсусу, алгоритми

Proof of Stake (PoS), швидше за все, продовжуватимуть відігравати важливу роль у майбутньому індустрії блокчейну в цілому. Наразі понад 400 криптовалют використовують PoS як алгоритм консенсусу. У наступних статтях ми глибше розглянемо алгоритми консенсусу та треті сторони, які надають альтернативи провідним механізмам консенсусу[31].

Вибираючи консенсусний алгоритм, важливо починати з цілей, яких ви хочете досягти.

Подумайте, чи хочете ви приватний чи публічний блокчейн. Якщо приватний, PoA є кращим механізмом, якщо публічний, PoW або PoS є найкращим варіантом.

1.4 Постановка завдання дослідження

Метою даного дослідження є покращення існуючих протоколів консенсусу в області блокчейн технологій з фокусом на протоколах Proof of Work (PoW) та Proof of Stake (PoS). Дослідження спрямоване на аналіз, оцінку та подальший розвиток цих протоколів для оптимізації їх ефективності та відповідності вимогам сучасного середовища кібербезпеки.

Завдання дослідження включають:

– аналіз існуючих протоколів PoW та PoS: провести глибокий аналіз та порівняння існуючих протоколів консенсусу з використанням Proof of Work та Proof of Stake. Оцінити їхню сильну та слабку сторону, а також ідентифікувати можливості для вдосконалення;

– розробка нових методик аналізу: розробити нові методи аналізу для оцінки рівня безпеки, масштабованості та децентралізації протоколів PoW та PoS. Визначити ключові параметри, які впливають на їхню ефективність;

– експериментальне моделювання та тестування: використовуючи отримані результати аналізу, розробити експериментальні моделі для тестування

та порівняння різних варіантів протоколів консенсусу. Оцінити їх продуктивність та стійкість до атак;

– впровадження покращень: на основі результатів дослідження та експериментів розробити та запропонувати конкретні покращення для існуючих протоколів PoW та PoS. Зосередити увагу на збільшенні швидкодії, зменшенні енергоспоживання та підвищенні рівня безпеки;

– розробка рекомендацій щодо вибору протоколу: на основі отриманих результатів розробити рекомендації для вибору конкретного протоколу консенсусу в залежності від конкретних умов та завдань системи;

– це дослідження спрямоване на створення нових знань та розробку практичних рекомендацій для подальшого розвитку протоколів консенсусу в контексті блокчейн технологій та кібербезпеки.

2 АНАЛІТИЧНИЙ ОГЛЯД СУЧАСНИХ ПОКРАЩЕНЬ ПРОТОКОЛІВ КОНСЕНСУСУ

2.1 Математична модель PoW

Доказ роботи (PoW) — базова концепція криптографії та технології блокчейн. Це основний механізм, який дозволяє децентралізованим мережам досягати консенсусу між учасниками, які не обов’язково довіряють один одному. PoW передбачає розв’язання складних математичних задач, які вимагають значних обчислювальних зусиль, щоб запобігти втручанню зловмисників у роботу мережі. Ця стаття має на меті заглибитися в математичну модель, яка керує Proof of Work і як вона захищає системи блокчейну.

У системі PoW учасники (їх часто називають майнерами) змагаються у вирішенні криптографічних головоломок. Перший майнер, який знайде рішення, яке відповідає певним критеріям, має право додати новий блок транзакцій до блокчейну та отримує винагороду певною кількістю токенів криптовалюти. Цей процес називається майнінгом.

Криптографічна головоломка в системі PoW зазвичай включає в себе пошук значення, яке при хешуванні за допомогою криптографічної хеш-функції дає результат, що відповідає певним умовам. Хеш-функція - це математичний алгоритм, який приймає вхідні дані (або "повідомлення") і повертає рядок байтів фіксованого розміру. Результат, відомий як хеш, виглядає випадковим і суттєво змінюється навіть при невеликій зміні вхідних даних.[32]

Умова, яку майнери повинні виконати, зазвичай полягає в тому, що хеш заголовка блоку повинен бути меншим або дорівнювати цільовому значенню. Це цільове значення змінюється з часом, щоб підтримувати постійну швидкість створення блоків у мережі.

Математично цей процес можна описати наступним чином.

Нехай H - криптографічна хеш-функція, x - вхідні дані для хеш-функції (які включають дані блоку і nonce), а T - цільове значення. Майнери повинні знайти таке значення nonce, що:

$$H(x) \leq T . \quad (2.1)$$

Nonce - це випадкова величина, яку майнери змінюють при кожній спробі згенерувати новий хеш. Оскільки хеш-функції є детермінованими (однакові вхідні дані завжди дають однаковий вихід), але розроблені для імітації випадковості, майнери повинні займатися перебором методом грубої сили, випробовуючи багато різних нонсів, поки не знайдуть той, який генерує хеш, що задовольняє цільову умову.

Безпека методу підтвердження вакансії полягає в його складності та неможливості швидко знайти правильне випадкове число. Робота, необхідна для пошуку правильних випадкових чисел (і, отже, вирішення головоломки), виправдовує витрати на обчислення. Ці зусилля можуть перешкодити зловмисній поведінці, оскільки зловмиснику потрібно буде контролювати більше половини обчислювальної потужності мережі, щоб маніпулювати блокчейном – атака, відома як атака 51%.

Крім того, як тільки блок додається до блокчейну, його зміна вимагатиме повторного виконання роботи для цього блоку і всіх наступних блоків, що є непрактичним, якщо не неможливим через кумулятивну роботу мережі.

Складність головоломки в системі PoW є динамічною; хоча загальна потужність хешування мережі коливається, вона змінюється, щоб блоки генерувалися з постійною швидкістю. Наприклад, біткойн прагне створювати новий блок кожні 10 хвилин. Якщо блоки створюються занадто швидко через збільшення обчислювальної потужності мережі, складність збільшиться, таким чином зменшуючи цільове значення T. І навпаки, якщо блоки створюються надто повільно, складність зменшується за рахунок збільшення T [33] .

2.2 Математична модель PoS

Нехай B – запропонований новий блок, який вважається дійсним в рамках даного протоколу:

$$\text{hash}\left(\text{hash}\left(B_{prev}, A, t\right)\right) \leq \text{bal}(A) * \frac{M}{D}, \tag{2.2}$$

де $D \in [1, M]$ – складність даного блоку; A – адреса користувача; t – мітка часу; B_{prev} – попередній блок в ланцюгу.

Введемо значення $T(r)$ як кількість часу в секундах, необхідного для генерації блоку B мінтером, r – кількість спроб підбору значень в секунду. Згідно з умовами, які накладаються даним протоколом на мітку часу, допускається 7200 різних значень t, тобто, область перебору, порівняно з PoW, значно менша. Зважаючи на це, будемо припускати, що кількість спроб r = 1.

Аналогічно попереднім обчисленням, будемо припускати, що всі дійсні блоки в протоколі консенсусу задовольняють умові: $U \leq \theta \leq 1$, де $U \sim Un[0, 1]$ – рівномірно розподілена випадкова величина, отримана шляхом гешування певних даних та нормалізації даної величини таким чином, щоб її значення знаходилось на проміжку [0, 1]. [34]

Proof of Stake – частинний випадок даної умови зі значенням $\theta = bal(A)/D$. Нехай N – кількість спроб, необхідних для отримання значення, що задовольняє нерівності. В такому випадку, можемо покласти $T(r) = T$. Розглянемо розподіл величини T:

$$\Pr\{T \leq t\} = \Pr\{N \leq t\} = 1 - \Pr\{N > t\} = 1 - \left(1 - \frac{\text{bal}(A)}{D}\right)^t =$$

$$= 1 - \exp\left(\ln\left(1 - \frac{\text{bal}(A)}{D}\right) * t\right), \tag{2.3}$$

Введемо додаткове припущення, згідно з яким баланс кожного мінтера є значно меншим, ніж загальна сума валюти в системі. В такому випадку, зважаючи на значення $D = 1/Tex \sum a\ bal(a)$, можемо допустити, що $bal(A)\ D << 1$, тому $ln($ $1 - bal(A)\ D\ ) \approx -bal(A)\ D$. Тоді:

$$\mathrm{P\ r}\{T\ \leq\ t\}\ =\ 1\ -\ \exp(\ -\frac{\mathrm{bal}(A)}{D} * t\ )\ . \qquad (2.4)$$

Отже, бачимо, що час, необхідний для отримання нового дійсного блоку розподілений експоненціально з параметром $\lambda = -\frac{\sum_{i=1}^{n} \mathrm{bal}(Ai)}{D}$. Тоді за властивістю експоненціального розподілу, отримуємо імовірність згенерувати дійсний блок мінтером i:

$$\mathrm{Pr}\{\mathrm{Tb}\ =\ \mathrm{Ti}\} = \frac{\mathrm{bal(Ai)}}{\sum_{j=1}^{n} bal(A_j)}. \qquad (2.5)$$

Це означає, що мінтінг у протоколі Proof of Stake є справедливим, тобто, мінтер з часткою балансу p має імовірність p згенерувати наступний дійсний блок[35].

Математична модель, що лежить в основі Proof of Stake, базується на теорії ймовірності і теорії ігор. Основна ідея полягає в тому, щоб зробити так, щоб валідаторам було вигідніше діяти чесно, ніж намагатися підірвати систему. Ось як це зазвичай працює.

1. Випадковий вибір. Алгоритм PoS вибирає валідаторів випадковим чином, але ймовірність бути обраним зважується на кількість валюти, яку учасник поставив на карту. Це можна представити у вигляді функції розподілу ймовірностей, де P(x) – це ймовірність бути обраним валідатором, а x – це сума ставки.

2. Підробка блоків – після обрання валідатори відповідають за перевірку транзакцій, створення нових блоків і додавання їх до блокчейну. Потім вони отримують винагороду у вигляді комісії за транзакції або новостворених монет.

3. Щоб запобігти нечесній поведінці, системи PoS часто включають механізм "відсікання". Якщо валідатора спіймають на спробі шахрайства (наприклад, валідації шахрайських транзакцій або створення блоків на міноритарному форку), частина його частки може бути забрана.

4. Довгострокові атаки і проблема "нічого на кону". PoS також повинна враховувати потенційні вразливості, притаманні тільки її системі. Наприклад, оскільки створення блоків не є ресурсоємним, ніщо не заважає валідаторам підтримувати кілька форків блокчейну, що призводить до проблеми "нічого на кону". Щоб протистояти цьому, протоколи PoS часто включають правила, які карають за таку поведінку, або реалізують такі механізми, як "контрольні точки", де попередні хеші блоків жорстко кодуються в програмному забезпеченні, щоб запобігти реорганізації після певного моменту.

5. Делегований доказ частки (DPoS). Деякі моделі PoS вводять рівень делегування, коли зацікавлені сторони голосують за невелику кількість делегатів, які підтверджують транзакції і створюють блоки. Це може створити більш масштабовану мережу, але вводить додаткові рівні в математичну модель, часто включаючи елементи систем репутації і теорії голосування.

Безпека PoS базується на припущенні, що більшість зацікавлених сторін зацікавлені в підтримці стабільної та чесної мережі. Вартість придбання контрольного пакета акцій мережі має бути дуже високою, що робить атаку невигідною.

Це відповідає принципу візантійської відмовостійкості, який означає, що навіть якщо деякі вузли виходять з ладу або поводяться зловмисно, доки ці вузли не складають більшості, розподілена система може працювати нормально.

Ключовим компонентом математичної моделі PoS є структура стимулів. Валідатори отримують винагороду за участь у процесі консенсусу, що заохочує їх зберігати кошти та підтримувати активне управління.Винагорода повинна бути ретельно відкалібрована, щоб гарантувати, що вона достатня для мотивації чесної поведінки, але не настільки висока, щоб викликати надмірну інфляцію в криптовалюті.

2.3 Критичний аналіз нових розробок у сфері PoW та PoS протоколів

Спочатку розглянемо алгоритм консенсусу Proof of Work (PoW) та його інновації, а саме:

– сучасні PoW алгоритми, як Equihash, спрямовані на зменшення енергоспоживання, що важливо для екологічної стійкості. Перехід на більш енергоефективні майнінгові пристрої в Bitcoin також сприяє цьому напрямку;

– розробка ASIC-резистентних алгоритмів допомагає уникнути централізації майнінгу, забезпечуючи рівні умови для всіх учасників мережі;

– вдосконалення хеш-функцій та механізмів верифікації транзакцій зменшують час і обчислювальну потужність, необхідну для добування блоку;

– систематичне зменшення нагороди за блок у Bitcoin кожні чотири роки регулює інфляцію та стимулює майнерів, ця дія має назву Халвінг;

– другий рівень рішень для швидких транзакцій, який знижує навантаження на основний блокчейн.

На черзі нові технології PoS, які я дізнався з різних статей та науково-популярних журналів:

– PoS значно знижує енергоспоживання, оскільки консенсус досягається не через майнінг, а через стейкінг;

– механізми покарань, такі як "слешинг", запобігають шахрайству та забезпечують чесну участь у мережевому консенсусі;

– оновлення, як Casper в Ethereum, полегшують валідацію блоку та транзакцій, покращуючи масштабованість;

– перехід Ethereum з PoW на PoS значно знизив енергоспоживання та покращив масштабованість мережі;

– розділення блокчейна на декілька сегментів для паралельної обробки транзакцій покращує продуктивність;

– користувачам надано можливість делегувати свої стейки іншим валідаторам, що сприяє більш ефективному управлінню мережею.

Цей огляд висвітлює ключові покращення та інновації в алгоритмах PoW та PoS, які спрямовані на збалансування ефективності, безпеки та масштабованості в блокчейнах. Обидва алгоритми продовжують еволюціонувати з метою вирішення сучасних викликів у криптовалютних мережах [36].

2.4 Впровадження квантових обчислень у блокчейн

Впровадження квантових обчислень у блокчейн технології є однією з найбільш обговорюваних тем у галузі криптографії та кібербезпеки. Квантові комп’ютери мають потенціал радикально змінити пейзаж сучасних технологій, включаючи блокчейн, завдяки своїй здатності виконувати обчислення набагато швидше, ніж їх класичні аналоги.

Квантові обчислення можуть впливати на протоколи консенсусу, які є основою блокчейн мереж. Наприклад, алгоритми Proof of Work (PoW), які використовуються в Bitcoin, залежать від складності криптографічних головоломок. Квантовий комп'ютер здатний розв'язати ці головоломки набагато швидше, ніж класичний комп'ютер, що ставить під загрозу безпеку PoW-мереж через можливість так званої квантової атаки 51%.

Proof of Stake (PoS) та інші алгоритми консенсусу, які залежать від криптографічного підпису, також можуть бути вразливими перед квантовими алгоритмами, зокрема перед алгоритмом Шора, який може ефективно розкладати великі числа на прості множники та розв'язувати задачу дискретного логарифмування.

Квантові обчислення мають потенціал радикально змінити блокчейн-технології. З одного боку, вони можуть поставити під загрозу безпеку існуючих блокчейн-мереж, які використовують класичну криптографію. З іншого боку, квантові обчислення також можуть запропонувати ряд переваг, таких як збільшення швидкості транзакцій, покращення масштабованості та підвищення безпеки.

Найбільшою загрозою від впровадження квантових обчислень у блокчейн є те, що квантові комп'ютери можуть зламати класичні криптографічні алгоритми, які використовуються для забезпечення безпеки блокчейн-мереж. Наприклад, алгоритм Proof of Work (PoW), який використовується в Bitcoin, ґрунтується на криптографічних головоломках, які майнери повинні розв'язати, щоб додати новий блок до блокчейна.

Наразі існує лише два загальнодоступних блокчейн-проекти, які оголошено повністю квантово-стійкими: квантово-стійкий реєстр і пост-квантовий біткойн. Quantum Resistant Ledger (QRL) позиціонує себе як «постквантовий захищений блокчейн зі схемою підпису з підтримкою стану та безпрецедентною безпекою». Для цього протокол QRL використовує «визначений IETF XMSS, схему безпечного підпису на основі прямого хешу з мінімальними припущеннями безпеки». XMSS – це розширена схема підпису Merkle, що використовує дерева Merkle. Кожен вузол у цих деревах позначено криптографічним хешем блоку даних. Дерево Merkle можна визначити як «повний хеш усіх хешів усіх транзакцій в одному блоці в існуючій мережі блокчейн». Quantum Resistant Ledger стверджує, що його “розширена” схема підпису Меркла є ефективнішою і безпечнішою, ніж традиційні схеми підпису Меркла, хоча це важко довести без справді ефективного квантового комп’ютера, який міг би її протестувати.[37]

Вважається, що схеми хешування на основі стану, такі як підписи Merkle, більш стійкі до квантового злому, ніж RSA або криптографія на основі еліптичної кривої. Однак схеми хешування стану, такі як XMSS, можуть бути вразливими, якщо ключ використовується кілька разів.

Інші протоколи консенсусу, які залежать від криптографічного підпису, також можуть бути вразливими перед квантовими алгоритмами. Наприклад, алгоритм Proof of Stake (PoS), який використовується в Ethereum, ґрунтується на тому, що майнери, які мають найбільші позиції в мережі, мають більший шанс валідувати блоки. Однак квантовий комп'ютер може зламати криптографічні підписи, які використовуються для визначення того, хто має право валідувати блоки, що може призвести до централізації мережі.

Крім потенційних загроз безпеці, квантові обчислення також можуть запропонувати ряд переваг для блокчейн-мереж. Наприклад, квантові обчислення можуть використовуватися для:

– збільшення швидкості транзакцій, тобто, квантові обчислення можуть пропонувати значне прискорення у верифікації транзакцій і обробці блоків. Це може зробити блокчейн-мережі більш ефективними та придатними для використання в реальному світі;

– покращення масштабованості, завдяки своїй високій обчислювальній потужності, квантові комп'ютери можуть допомогти блокчейн-мережам обробляти більшу кількість транзакцій одночасно. Це може зробити блокчейн-мережі більш доступними для більшої кількості користувачів;

– квантова криптографія, через використання квантових ключів і квантової розподачі ключів може забезпечити новий рівень безпеки для блокчейн-мереж. Квантові ключі не можуть бути зламані квантовими комп’ютерами, що може зробити блокчейн-мережі більш стійкими до атак.

2.5 Двокроковий блокчейн протокол

Для того, щоб дослідити безпеку протоколу, подібного до біткойна, Гарай та ін. [38], а потім Пасс та ін. [39] створили перші криптографічні моделі, слідуючи формулюванню Канетті про виконання "реального світу". У цьому розділі ми запозичуємо багато ідей з їхніх формулювань. Я також розширю їх моделі, щоб дозволити використання більшої кількості протоколів блокчейнів, наприклад, 2-хоп блокчейнів.

Основи комунікації для протоколів блокчейну сформульовані через функціонал F_{NET}, який фіксує атомарну неавтентифіковану трансляцію "відправити всім" в умовах асинхронного зв'язку. Функціонал параметризується верхньою межею Δ на мережеву затримку, і взаємодіє з гравцями під керівництвом супротивника. Більш конкретно, функціонал працює наступним

чином. Кожного разу, коли вона отримує повідомлення від гравця, вона зв'язується з опонентом і просить його вказати час доставки повідомлення. Зауважте, що якщо вказаний час доставки перевищує верхню межу затримки Δ, функціонал не буде виконувати інструкцію суперника, а лише затримає повідомлення на максимальну кількість раундів Δ. При цьому жодне повідомлення не затримується більше, ніж на Δ раундів. Крім того, опонент може прочитати усі повідомлення, надіслані усіма чесними гравцями, перш ніж прийняти рішення про свою стратегію.

Я визначаю два типи гравців PoW-майнер і PoS-власник, які відповідають двом типам ланцюжків, а саме, PoW-ланцюжок і PoS-ланцюжок; і два типи раундів, які виконують по черзі: PoW-раунд і PoS-раунд. Ці два типи ланцюгів пов'язані між собою і ростуть разом (з однаковою швидкістю). При цьому пара ланцюгів, що включає PoW-ланцюг і PoS-ланцюг, повинна складатися з двох ланцюгів приблизно однакової довжини. Якщо PoW-ланцюг або PoS-ланцюг в цій парі зростає занадто швидко, така пара стає недійсною. Зверніть увагу, що майнери PoW і власники PoS грають різні ролі в нашій моделі, але без співпраці цих двох типів гравців наша модель не може бути безпечною. У нашій моделі, не втрачаючи загальності, ми припускаємо, що всі PoW-майнери мають однакову обчислювальну потужність, а всі PoS-власники мають однаковий розмір частки. Зауважте, що це "ідеалізована модель". В реальності кожен окремий чесний PoW-майнер або PoS-власник може мати різну обчислювальну потужність/частку; тим не менш, ця ідеалізована модель не приносить в жертву загальності, оскільки можна уявити, що реальні чесні PoW-майнери/ PoS-власники є просто кластерами деякої довільної кількості чесних ідеалізованої моделі PoW-майнерів/ PoS-власників. Зауважимо, що учасники протоколу ніколи не можуть бути впевнені в кількості учасників виконання протоколу, враховуючи неавтентифіковану природу моделі комунікації. Крім того, для простоти, в цій моделі розглядається лише автономна статична модель, а кількість гравців фіксується в ході виконання протоколу. У кожному раунді PoW-майнери мають можливість пропорційно до своїх обчислювальних потужностей створювати блоки, що підтверджують роботу

мережі. Більш конкретно, при отриманні повідомлень, які включають багато пар ланцюжків від мережі, кожен майнер вибере найкращу дійсну пару ланцюжків, а потім використає свою обчислювальну потужність для вирішення головоломки PoW, щоб розширити найкращу пару ланцюжків в цьому раунді. З іншого боку, в кожному PoS-раунді PoS-власник з похідною ідентичністю від нового PoS-блоку попереднього PoS-раунду може згенерувати новий PoS-блок, а потім додати новий блок до найкращої пари ланцюжків з його локальної точки зору. Зауважте, що для кожного PoS-власника ймовірність бути обраним базується на розмірі частки, яку він має. Деталі виконання блокчейну представлено нижче.

Гібридна реалізація $\{F_1,F_2,F_{NET}\}$ протоколу блокчейну з 2-ма хопами. Існуючі строгі формулювання застосовуються для 1-хоп протоколів (наприклад, протокол Накамото), де система підтримується одним типом гравців, тобто PoW-майнерами. Тут ми переходимо від 1-хоп протоколів до 2-хоп протоколів (тобто, гібридних протоколів з доказом роботи/доказом частки) і представимо їх формальне трактування.

Слідуючи формулюванню Канетті про виконання "реального світу", представляємо абстрактну модель для гібридного протоколу блокчейну з доказом роботи/доказом частки $\Pi = (\Pi^w,\Pi^s)$ у гібридній моделі $\{F_1,F_2,F_{NET}\}$ де Π^w та Π^s позначають код, що виконується PoW-майнерами та PoS-власниками відповідно. Ми розглядаємо виконання протоколу блокчейну $\Pi = (\Pi^w,\Pi^s)$, який керується середовищем $Z(1\kappa)$ (де κ - параметр безпеки параметр безпеки), яке активує n кількість PoW-майнерів та n˜ кількість PoS-власників. Виконання відбувається в раундах. Не втрачаючи загальності, вважатимемо, що непарні раунди відповідають PoW-майнерам, а парні раунди відповідають PoS-власникам. Середовище Z може "керувати" учасниками протоколу через супротивника A, який може динамічно корумпувати чесних учасників, але таке корумпування потребує певного часу, тобто 2Δ раундів, щоб бути ефективною.

Більш конкретно, гібридне виконання $\{F_1,F_2,F_{NET}\}$ відбувається наступним чином. Кожна сторона у виконанні ініціалізується початковим станом state0. Цей стан включає всю початкову загальнодоступну інформацію протоколу П,

наприклад, генетичний блок. Спочатку середовище Z активує супротивника A і надає інструкції для супротивника. Виконання відбувається в раундах, і в кожному раунді сторона протоколу може бути активована середовищем або функціоналом.

У наших умовах майнери PoW мають обмежену можливість надавати докази своєї роботи. Щоб врахувати це, всі PoW-майнери мають доступ до набору фізичних ресурсів F^{*}_{rRO}, який керує величезною "фермою обчислювальних пристроїв", і ці пристрої надаються середовищем Z через супротивника. Для того, щоб використати обчислювальну потужність функціоналу, кожен гравець повинен зареєструвати обчислювальні послуги F^{*}_{rRO} або відключити ці послуги у певний момент часу. Дійсно, це відображає динамічне налаштування обчислювальних потужностей де різні гравці можуть споживати обчислювальні ресурси протягом різних проміжків часу. Функціональність F^{*}_{rRO} абстрагується від процесу майнінгу, подібного до майнінгу біткоїна; це спрощує розробку та аналіз протоколів заснованих на такій екосистемі майнінгу. Тут кожен PoW-майнер може надіслати один пошуковий запит до F^{*}_{rRO}, який споживає одну одиницю обчислювальної потужності, що надається в кожному раунді виконання. Крім обчислювальних послуг, система також надає сервіси верифікації, які дозволяють будь-якому гравцю перевіряти розв'язки багато разів, або обчислювальні сервіси, які дозволяють будь-якому гравцю виконувати регулярні випадкові запити до оракула багато разів. Більш конкретно, у будь-який момент часу PoW-майнер W_i може відправити команду реєстру (WORK-REGISTER,W_i) щоб попросити про реєстрацію. Функціонал потім просить супротивника вказати, чи може гравець зареєструватися чи ні. Якщо супротивник дозволяє гравцю W_i використовувати обчислювальний ресурс (Wi надано обчислювальний ресурс), то функціонал запише (W_i,b_i), де $b_i = 1$. Якщо гравець скасовує реєстрацію послуг, цей біт буде буде скинуто до 0, що означає, що ресурс більше не буде надано цьому гравцю. Зауважте, що тут ми дозволимо середовищу Z (через супротивника) вказує, хто отримає обчислювальний ресурс, а хто ні не отримає.

Функціонал працює в раундах, і для кожного раунду задає біт $b_i^w = 0$ для кожного зареєстрованого гравця W_i, що означає, що гравцю W_i надається одна одиниця обчислювального ресурсу. Відмітимо, що, якщо обчислювальна одиниця була використана гравцем W_i при видачі пошукового запиту, то біт $b_i^w = 0$ скидається до 1, і тоді цей гравець не зможе посилати інші пошукові запити. Зареєстрований PoW-майнер W_i може надіслати запит на пошук PoW-розв'язку, і він може знайти його лише з певною ймовірністю p. Точніше кажучи, після того, як він запитав обчислювальні сервіси з функціоналу обчислювальні сервіси від функціоналу за командою (SEARCH,h,W_i), функціонал перевіряє чи існує запис (Wi bi); це означає, що функціонал перевіряє, чи існує запис (W_i); це означає, що функціонал перевіряє, чи цьому гравцеві вже надано необхідний обчислювальний ресурс. Якщо ресурс надано, і b w i = 0, що означає, що цей гравець не використав ресурс, виділений у поточному раунді, функціонал з ймовірністю p вибере випадкову пару (w,h) і запише запис (W_i, (h,w), h). Якщо W_i запитує більше одного разу у цьому раунді, функціонал не буде виконувати жодних пошукових запитів, оскільки ресурс вже використано.

Як обговорювалося вище, це "ідеалізована" інтерпретація ситуації, коли всі майнери мають однакову кількість обчислювальних потужностей; тим не менш, ця ідеалізована модель не приносить в жертву загальності. Противнику A може виконати не більше t запитів за раунд, де t - кількість пошкоджених PoW-майнерів. Таким чином, обчислювальна потужність витрачається на запити функціоналу обмежену кількість разів. Зауважимо, що ми не перші, хто сформулював налаштування обчислювальних ресурсів. Більш ранні спроби можна можна знайти в. Ми стверджуємо, що наш функціонал F^*_{rRO} є більш строгим, ніж попередні роботи; явно моделюємо, як обчислювальний ресурс управляється і розподіляється від середовища до сторін. У цій моделі кожна сторона може зареєструватися і отримати обчислювальний ресурс під контролем середовища. При цьому модель природним чином враховує приєднання нових гравців або повернення старих гравців. Крім того, наша функція F^*_{rRO} тісно пов'язана з F_{Tree} в, але відрізняється від неї. У використовується підхід "для кожного протоколу"

підхід "на протокол". Тобто, для різних протоколів блокчейну, скажімо, протоколу GHOST, має бути визначений різний варіант F_{Tree} повинен бути визначений інший варіант. Ми використовуємо інший підхід: ми абстрагуємося від суті базових ресурсів, а наш ресурсний функціонал випадкового оракула F^{*}_{rRO} можна використовувати для різних блокчейн-протоколів на основі PoW. протоколів блокчейну на основі PoW, і нам не потрібно переглядати налаштування для кожного протоколу. Зауважимо, що наша функція F^{*}_{rRO} є дуже дорогим в тому сенсі, що в кожному часовому вікні може бути задіяна велика кількість обчислювальних ресурсів. багато обчислювальних ресурсів може бути надано у кожному часовому вікні. У цій роботі будемо використовувати цей фізичний ресурс (тобто обчислювальну потужність) разом з іншим віртуальним ресурсом (тобто, часткою) - F^{*}_{rCERT} для проектування Bitcoin як блокчейну. Зауважте, що набір віртуальних ресурсів F^{*}_{rCERT} набагато дешевше.

Як обговорювалось функціонал F^{*}_{rRO} реалізується функціоналом випадкового оракула F_{RO}. Позначимо $\varphi * F^{*}_{rRO}$ ідеальний протокол для ідеального функціоналу F^{*}_{rRO}, а π^{*}_{rRO} як протокол у F_{RO}-гібридну модель. В ідеальному протоколі φ^{*}_{rRO}, гравці є фіктивними, оскільки вони просто пересилають повідомлення отримані з середовища Z на функціонал F^{*}_{rRO}, а потім пересилають повідомлення, отримані від функціоналу до середовища. З іншого боку, після отримання повідомлень від середовища, гравці у π^{*}_{rRO} виконують протокол, а потім передають виходи у середовище. Зауважте, що ми дозволяємо кожному PoW-майнеру отримати лише одну одиницю обчислювальної потужності (один шанс на запит до випадкового оракула) за раунд. По суті, протокол π^{*}_{rRO} є ядром блокчейну на основі PoW (наприклад, Bitcoin). Неформально, π^{*}_{rRO} виконує наступні два основні кроки: по-перше, кожен майнер PoW може "видобувати" рішення головоломки хеш-нерівності; після цього будь-які інші гравці (PoW-майнери або PoS-власники) можуть перевірити знайдений розв'язок.

Раніше було визначено декілька фундаментальних властивостей безпеки для 1-хопових протоколів блокчейну: властивість спільного префікса, властивість якості ланцюга та властивість зростання ланцюга [40]. Інтуїтивно зрозуміло, що

властивість зростання ланцюжка стверджує, що ланцюжки чесних гравців повинні рости лінійно до кількості раундів. Властивість спільного префікса вказує на узгодженість будь-яких двох ланцюжків чесних гравців, окрім останніх к блоків. Властивість якості ланцюжка має на меті виразити кількість внесків чесних блоків, які містяться у достатньо довгій та неперервній частині чесного ланцюга. Зокрема, для параметрів N та $\mu \in (0,1)$, відношення чесних внесків у неперервній частині чесного ланцюжка має нижню межу μ. Будемо дотримуємося того ж духу при визначенні властивостей безпеки для 2-хепового протоколу блокчейну.

Оскільки кожен PoS-ланцюг і PoW-ланцюг існують в нашій системі як пара, що має однакову структуру і росте з однаковою швидкістю, ми в основному зосередимося на спільному префіксі, якості ланцюга і властивостях росту ланцюга для PoS-ланцюга. Цікаво, що спільний префікс і зростання ланцюга для PoW-ланцюга явно випливають з PoS-ланцюга, але якість ланцюжка для PoW-ланцюжка не може бути показана з PoS-ланцюжка, оскільки противник може контролювати більшу частину обчислювальних потужностей в наших умовах. Тому ми окремо розглянемо властивість росту ланцюжка для PoW-ланцюга.

2.6 Висновки

Доказ роботи (PoW) і доказ частки (PoS) є двома основними механізмами консенсусу, які використовуються в блокчейнах. Обидва алгоритми мають свої переваги та недоліки, і в даний час проводяться дослідження з метою розробки нових алгоритмів, які поєднують у собі найкращі якості PoW та PoS.

Упровадження квантових обчислень у блокчейн може мати як позитивні, так і негативні наслідки. З одного боку, квантові комп'ютери можуть поставити під загрозу безпеку існуючих блокчейн-мереж, які використовують класичну криптографію. З іншого боку, квантові обчислення також можуть запропонувати ряд переваг для блокчейн-мереж, таких як збільшення швидкості транзакцій, покращення масштабованості та підвищення безпеки.

Очікується, що впровадження квантових обчислень у блокчейн відбудеться в найближчі роки. Це матиме значний вплив на розвиток блокчейн-технологій, і важливо бути готовим до цих змін.

Ось деякі конкретні рекомендації, які можна вжити для підготовки до впровадження квантових обчислень у блокчейн:

– розробка квантово-стійких алгоритмів консенсусу. Важливо розробити нові алгоритми консенсусу, які будуть стійкими до атак квантових комп'ютерів;

– перехід на квантову криптографію. Квантова криптографія може забезпечити новий рівень безпеки для блокчейн-мереж;

– обробка даних про потенційні загрози. Важливо бути в курсі останніх досліджень у галузі квантових обчислень і блокчейну, щоб бути готовим до потенційних загроз.

Впровадження квантових обчислень у блокчейн - це важливий етап у розвитку цієї технології. Майбутнє квантових обчислень і блокчейна вкрай невизначене і може стати одним із визначальних факторів у майбутньому інформатики. Блокчейн допоміг демократизувати Інтернет, створив криптовалюти та породив найбільші у світі розподілені обчислювальні мережі у формі популярних блокчейнів, таких як Bitcoin та Ethereum.

Навпаки, квантові обчислення, які все ще перебувають на ранніх стадіях, мають потенціал допомогти у вирішенні багатьох найважливіших наукових і технологічних проблем нашого часу, просуваючи технологію так, як ми ще не можемо передбачити.

Якщо квантові обчислення та блокчейн зіткнуться, це може стати безпрецедентною катастрофою. Однак, якщо криптографія продовжуватиме розвиватися для створення все більш квантово-стійких методів шифрування, або якщо саме квантове шифрування буде інтегровано в блокчейни, поєднання цих перспективних технологій може допомогти створити більш безпечний, демократичний Інтернет і матиме більший потенціал для позитивного розвитку вплив на світ.

3 РОЗРОБКА ГІРБРИДНОГО ТА КВАНТОВОГО ПРОТОКОЛУ КОНСЕНСУСУ

3.1 Огляд квантового протоколу консенсусу PoW

Новий протокол консенсусу PoW на основі бозонної дискретизації. Бозонна дискретизація спочатку була розроблена для демонстрації квантової переваги завдяки зниженим вимогам до ресурсів порівняно з іншими квантовими алгоритмами. Бозонні семплери є спеціалізованими фотонними пристроями, які обмежені в тому сенсі, що вони не здатні ні до практичних застосувань у хімії, фізиці багатьох тіл та інформатиці. Сформулювали практичне застосування варіанту бозонної дискретизації, який називається грубозернистою бозонною дискретизацією (CGBS) [41]. Ця схема передбачає групування вихідної статистики бозонної вибірки однакового розміру у фіксовану кількість бінів відповідно до деякої заданої тактики розбиття. Перевагою розбиття вихідного розподілу ймовірностей є поліноміальна кількість вибірок, необхідних для перевірки фундаментальної властивості розподілу, на відміну від експоненціальної кількості вибірок, необхідних без розбиття. Хоча бозонні семплери не можуть бути довільно масштабовані через відсутність корекції помилок, ми стверджуємо, що прискорення, яке вони забезпечують, є достатньо значним, щоб виправдати їх використання для консенсусу PoW. Блокчейн на основі фотоніки вже досліджувався раніше. Optical PoW використовує HeavyHash, невелику модифікацію протоколу Bitcoin, де в середину майнінгу вставляється матрично-векторний продукт на основі фотонної сітки. Це вже було інтегровано в оптичні криптовалюти Bitcoin і Kaspa. Нещодавно більш енергоефективний варіант під назвою LightHash був протестований на мережах до 4 фотонів [42]. Обидва ці протоколи використовують пасивні лінійні оптичні мережі, що діють на когерентні входи, які реалізують матричне множення на вектор когерентних амплітуд. Вважається, що фотонна реалізація цього матричного множення може

досягти прискорення на порядок порівняно з традиційним апаратним забезпеченням ЦП. Вони використовують класичне прискорення, пов'язане з фотонною реалізацією цієї операції, і не використовують жодних квантових переваг. Хоча цей метод використовує багатомодовий інтерферометр, подібний до того, що описується в цій роботі, він не використовує власне квантові стани світла і фактично є іншою формою класичних обчислень з використанням світла. На противагу цьому, метод бозонної дискретизації використовує квантові повторні джерела з процесами, які стають експоненціально складнішими за кількістю фотонів для моделювання за допомогою класичного обладнання, незалежно від того, чи є воно фотонним чи ні.

Криптографія з відкритим ключем, яка сьогодні використовується в блокчейні, базується на парах пов'язаних ключів (відкритих і закритих), згенерованих за допомогою односторонніх функцій. Хоча легко обчислити публічний ключ з приватного, зворотна операція є обчислювально нерозв'язною. Це робить приватні ключі надзвичайно складними для вгадування або грубого підбору, забезпечуючи таким чином безпеку мереж блокчейн. Хеш-функції є ще одним прикладом односторонніх функцій з широкою криптографічною корисністю. Точніше кажучи, односторонні функції легко обчислюються для всіх входів у своїй області, але їх важко інвертувати за зображенням будь-якого невідомого входу. Тобто, якщо задано функцію,

$$\mathrm{f}\,(x) \;=\; y, \tag{3.1}$$

y легко обчислити для всіх вхідних даних x, але обчислити x для заданого y складно. З точки зору обчислень, поняття "легко" і "важко" відносяться до алгоритмів поліноміального та суперполіноміального часу відповідно до розміру вхідних даних. Тому, в загальному випадку, інверсія односторонніх функцій знаходиться в межах класу складності NP, оскільки перевірка будь-якого попереднього зображення можлива за поліноміальний час, на відміну від його явного обчислення. Ці односторонні функції мають важливе значення у різних

додатках, включаючи криптографію та протоколи автентифікації. Їхнє існування все ще залишається відкритою гіпотезою, і якщо його буде доведено, то це матиме серйозні теоретичні наслідки, пов'язані з обчислювальною складністю, включаючи теорему про P /= NP, що зумовлює зацікавленість у їхньому відкритті. Тим не менш, існує багато сприятливих кандидатів для односторонніх функцій, тобто функцій, для яких не існує алгоритмів інверсії за поліноміальний час. Важливо зазначити, що не існує строгого доказу неіснування таких алгоритмів обернення.

Загальна хеш-функція - це одностороння функція, яка має три основні властивості:

– вхідні дані можуть бути будь-якого розміру;

– його вихід завжди має фіксований розмір;

– його має бути легко обчислити.

Криптографічна хеш-функція має декілька додаткових вимог:

– стійкість до колізій: Хеш-функція H вважається стійкою до колізій, якщо неможливо знайти два значення x та y, де H(x)=H(y) і x≠ y;

– приховування: Хеш-функція H є прихованою, якщо неможливо знайти x, якщо задано H(r x), де r - секретне значення, яке вибирається з розподілу ймовірностей з високою мінімальною ентропією;

У деяких існуючих класичних реалізаціях блокчейну, зокрема в Bitcoin, для цілей PoW використовується часткове інверсне хешування. Тут майнери змагаються у пошуку бітових рядків, які хешують до вихідного рядка з певною кількістю початкових нулів. Кількість необхідних початкових нулів визначає складність розв'язання цієї задачі. Оскільки хеш-функції дуже неструктуровані, найкращим класичним підходом до пошуку таких розв'язків є використання грубої сили для хешування випадкових вхідних рядків до тих пір, поки випадково не буде знайдено задовільний результат. Після того, як розв'язок знайдено, інші вузли можуть перевірити його, просто хешувавши його. Бозонна дискретизація за станами була мотивована як спроба побудувати хешфункцію - односторонню вирішальну функцію - з задачі бозонної дискретизації. Зауважимо, що таке

означення хеш-функції відрізняється від звичайних хеш-функцій, оскільки вона не перебуває в НП, оскільки класичний верифікатор не може ефективно перевірити вихідний хеш, знаючи стан входу. Тут ми не використовуємо цю конструкцію повної хеш-функції безпосередньо, але, надихаючись нею, застосовуємо пікову ймовірність біна як ознаку роботи пристрою для бозонної дискретизації.

Хоча класичний верифікатор не може перевірити пікову ймовірність біна, враховуючи початковий стан, незалежні квантово-бозонні семплери будуть наближатися до тієї ж самої оціненої пікової ймовірності біна. Цього достатньо для цілей консенсусу, коли вибірки, надані різними сторонами, можна перехресно перевірити на збіжність з однією і тією ж оцінкою, незважаючи на те, що класичний верифікатор не є ефективним для визначення того, чи ця оцінка правильна.

Звичайний вказівник зберігає адресу даних у пам'яті, що полегшує доступ до них. З іншого боку, хеш-покажчик - це покажчик, який зберігає криптографічний хеш даних разом з їхньою адресою в пам'яті. Таким чином, хеш-покажчик вказує на дані, увімкнувши при цьому перевірку (миготіння). Крім того, зв'язаний список - це лінійна колекція елементів даних, де кожен елемент містить як дані, так і вказівник на попередній елемент. Порядок зв'язаного не задається їхнім фізичним розміщенням у пам'яті (wiki). Таким чином, блокчейн - це зв'язаний список з хешем вказівник на попередній елемент, який допомагає при перевірці даних попереднього елемента.

Бозонна дискретизація – це проблема дискретизації багатомодової фотостатистики на виході рандомізованого оптичного інтерферометра. Ця проблема являє собою протокол зашумлених квантів проміжного масштабу (NISQ), природно придатний для фотонної реалізації. Як і інші протоколи NISQ, бозонна дискретизація не вважається універсальною для квантових обчислень і не покладається на корекцію помилок, що обмежує масштабованість. Тим не менш, було показано, що це класично неефективний, але квантово-механічно ефективний протокол, що робить його придатним для демонстрації квантової

переваги, яка, як тепер вважається, була досягнута. На відміну від задач прийняття рішень, які дають остаточну відповідь на питання, бозонна вибірка - це задача вибірки, де метою є відбір зразків для вимірювання з великого стану суперпозиції, що виходить з пристрою. Оскільки бозонна вибірка не є НП-задачею, повна задача не може бути ефективно перевірена за допомогою класичних або квантових комп'ютерів. Дійсно, навіть інший ідентичний бозонний семплер не може бути використаний для верифікації, оскільки результати є ймовірнісними і загалом унікальними, що виключає пряме порівняння результатів як засіб верифікації. Тим не менше, обмежені версії проблеми, такі як грубозерниста бозонна вибірка, описана нижче, можуть бути використані для верифікації.

Загальну постановку задачі бозонної дискретизації проілюстровано на рис. 3.1. Вхідний стан формується за допомогою пасивної лінійної оптики, що складається з променевих розгалужувачів і фазообертачів, які реалізують перетворення Гейзенберга на операторах створення фотонів, де U - унітарна матриця M × M, що представляє багатомодове лінійне оптичне перетворення.

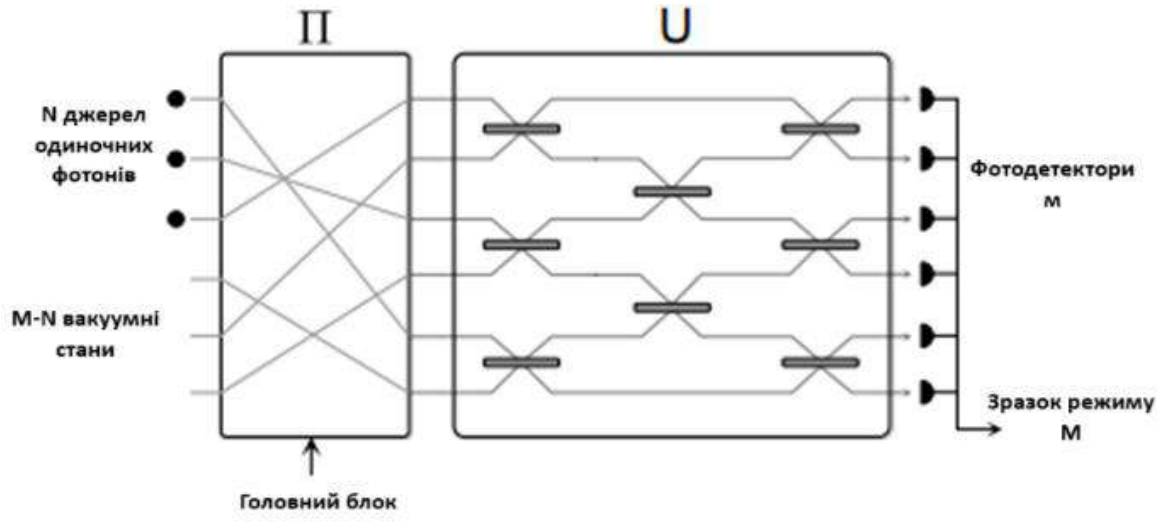

Рисунок 3.1 – Ілюстрація використання пристрою для бозонної дискретизації

Спочатку падає N фотонів у перших N модах, а решта M - N мод перебувають у стані вакууму. Потім моди проходять перестановку П залежно від інформації заголовка блоку, яка на практиці може бути здійснена простою

перестановкою місць однофотонних входів. Потім фотони проходять через інтерферометричну схему глибиною M, яка описується унітарною функцією U. Нарешті, фотони детектуються на вихідних портах M, забезпечуючи запис вимірювань зразка. Оператор створення фотонів на вході відображається на лінійну комбінації операторів створення над вихідними модами. Лінійне оптичне перетворення U вибирається рівномірно випадковим чином з міри Хаара, що є важливим для теоретичного доведення складності. В роботі було показано, що для будь-якого M × M, що будь-яке лінійне оптичне перетворення M × M вигляду, можна розкласти у мережу з не більше ніж O(M2) променевих розгалужувачів і фазообертачів, гарантуючи, що ефективна фізична реалізація завжди можлива ефективна фізична реалізація. Як показано на рис. 2, кількість детекторів дорівнює кількості режимів M. На практиці кількість детекторів можна зменшити, використовуючи мультиплексування в інших ступенях свободи, таких як часовий ступінь свободи. Наприклад, в архітектурі, де режими кодуються в часі, достатньо одного детектора з часовою роздільною здатністю для виявлення і розрізнення всіх режимів.

Ми розглядаємо консенсус PoW з двома типами розбиття, один з яких використовується для перевірки, щоб відловити шахраїв, а інший - для винагороди майнерів. Перший можна ефективно обчислити на класичних комп'ютерах, тоді як другий не має відомих класичних обчислень, хоча він має ефективну квантову оцінку. Після успішного видобутку блоку, результати обох розподілів будуть додані до блокчейну, тобто одна частина може бути ефективно перевірена класичними комп'ютерами, в той час як інша частина не може. Це стимулюватиме вузли, які використовують бозонні пристрої для перевірки попередніх блоків у блокчейні, перевіряти попередні блоки. Протокол проілюстровано на рис. 3.2, а його детальний опис наведено нижче.

1.У мережі створюється транзакція або пакет транзакцій. Всі вузли знають наступний набір вхідних параметрів:

$$Pm = \{N, M, U, d^{(mb)}, d^{(sb)}, Tmine, \epsilon, \beta, R, P\}, \quad (3.2)$$

який вважається постійним протягом багатьох блоків, але може бути змінений в залежності від складності задачі.

2. Створюється новий блок b_j, який представляє цю транзакцію. Він має заголовок header(b_j), який містить підсумкову інформацію про блок, включаючи набір параметрів Pm, хеш, отриманий з транзакцій у блоці, хеш заголовка попереднього блоку разом з його валідаційним записом Rec(b_{j-1}) (обговорюється на кроці 7), і мітку часу.

3. Новий блок надсилається кожному вузлу мережі. Всі вузли вкладають токени для участі. Зауважте, що цей протокол відрізняється від протоколу з підтвердженням частки, оскільки тут всі майнери вкладають однакову кількість токенів, і ймовірність успішного видобутку блоку не залежить від вкладеної суми.

4. Майнери реалізують бозонну вибірку за допомогою пристроїв, подібних до зображених на рисунку 3.1, використовуючи N фотонів, що вводяться у M режимів, впорядкованих {1, 2,..., M}. Хеш заголовка відображається у перестановку на модах за допомогою наперед визначеної функції a.

Ця перестановка, яка залежить від поточного блоку, використовується для визначення розташування N вхідних фотонів у вхідному стані бозонного семплера. Кожен вузол і збирає набір відліків, позначений s_i, розміром $|s_i|$, і фіксує кожен відлік у наборі шляхом хешування цього відліку разом з міткою часу і деяким приватним випадковим бітовим рядком. Зафіксовані зразки передаються у мережу. Множину фіксованих зразків для вузла і позначимо s_i. Метою трансляції хешованих версій зразків є запобігання нечесним майнерам від простого копіювання зразків чесних майнерів.

5. Після деякого наперед визначеного часу майнінгу, видобуток оголошується завершеним і нові зразки не приймаються. Всі майнери розкривають свої набори зразків $\{s_i\}$, а також випадкові бітові рядки, пов'язані з кожним зразком, щоб ці набори можна було порівняти з зафіксованими наборами $\{s_i\}$. Якщо для деякої вершини і набори не збігаються, ця вершина вилучається з подальшого розгляду раунду майнінгу, а майнер втрачає свою частку.

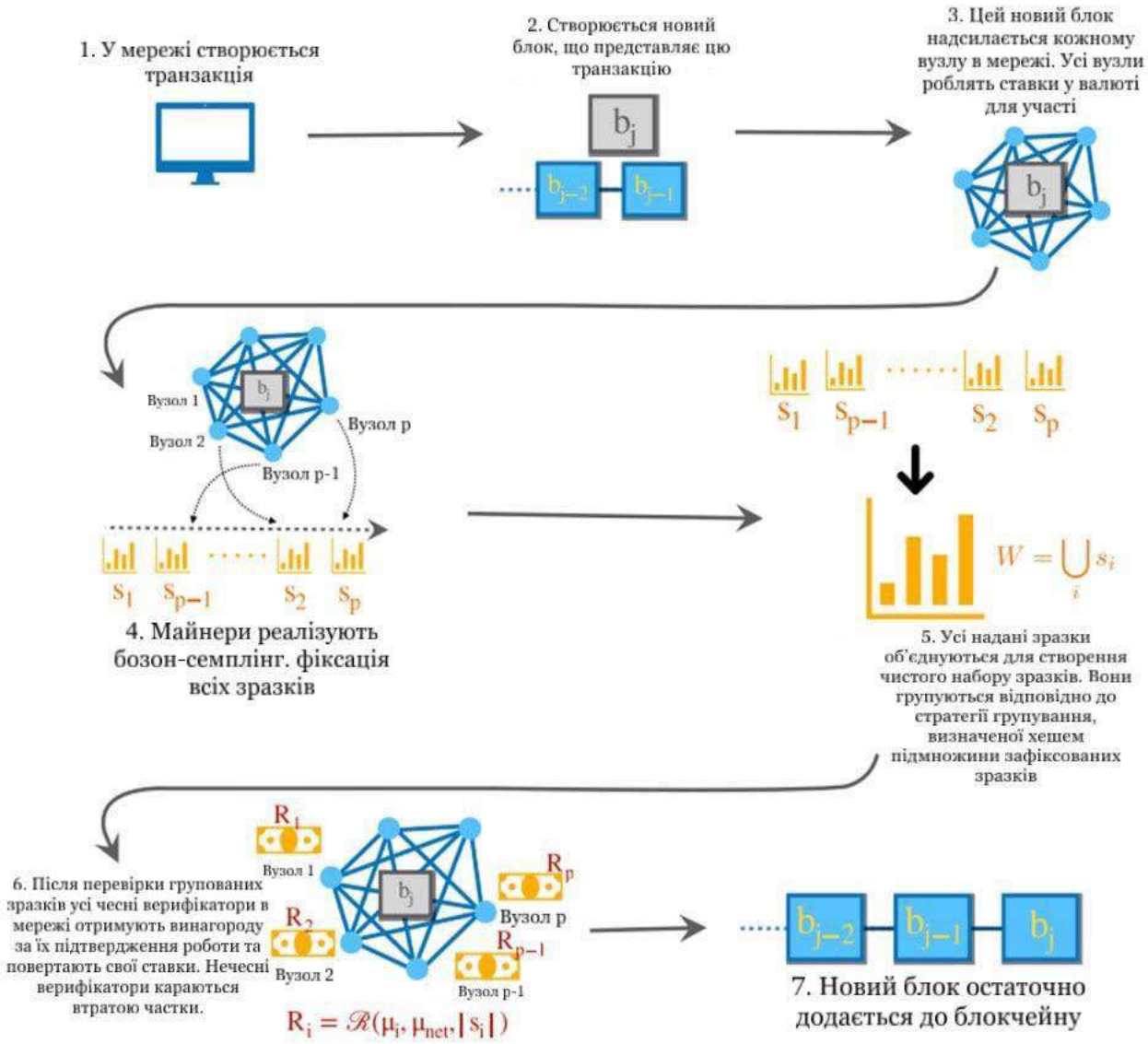

Рисунок 3.2 – Блокчейн-архітектура з включенням процедури бозонної дискретизації

6. Цей етап складається з трьох кроків: етап перевірки з використанням біннінгу режимів для виявлення нечесних майнерів крок бінінгу стану для визначення успішності майнінгу, крок критерію успішності майнінгу та крок виплати винагороди/штрафу.

7. Новий блок b_j додається до блокчейну.

3.2 Гібридні протоколи консенсусу PoW, PoS

Важливо відзначити, що в блокчейні Nakamoto PoW, заснованому на алгоритмі PoW, припущення для захисту системи полягає в тому, що безпеки системи є те, що зловмисні майнери контролюють менше половини обчислювальних потужностей, оскільки в такому випадку вони можуть розгалуження дійсного блокчейну, що порушує консенсус протоколу блокчейну.

У цій системі, щоб захиститися від такої атаки, нам потрібно об'єднати два різних ресурси: фізичний ресурс (тобто, обчислювальну потужність) і віртуальний ресурс (тобто, стейк). Послідовно, ми маємо два типи блокчейнів (PoW-ланцюг і PoS-ланцюг), яким відповідають два типи раундів - PoW-раунд і PoS-раунд, що виконуються по черзі, утворюючи 2-hop блокчейн. Зауважимо, що в реальності один гравець може виконувати обидві ролі - PoW-майнера і PoS-власника; однак, не втрачаючи загальності, ми розглядаємо ці дві ролі окремо. Для того, щоб зв'язати їх жорстко, схема зіставляє кожен PoW-блок не більше ніж з 1 стейкхолдером. Тільки стейкхолдер, який має привілей, може згенерувати відповідний PoS-блок з кожного PoW-блоку.

PoW-ланцюжки і PoS-ланцюжки, що існують в нашій системі представлені у вигляді пар, і кожен гравець локально зберігає пару ланцюжків. Таким чином, два учасники ланцюжка кожної дійсної пари ланцюжків повинні мати однакову структуру.

Зараз представимо основний протокол, який описує поведінку PoW-майнерів і PoS-власників. Процедури Реалізації PoW і PoS дещо відрізняються. З одного боку, у виконанні PoW майнери шукають доказові рішення за допомогою F^{*}_{rRO}. З іншого боку, у виконанні PoS, власники PoS слідкують за зростанням PoW-ланцюга і використовують це для розширення PoS-ланцюга через F^{*}_{rCERT}. Загалом, PoW-майнери і PoS-власники збирають інформацію про блокчейн з мережевої функціональності F_{NET}, виконують певну перевірку і генерують блоки, а потім діляться своїми станами з мережею через F_{NET}.

Розглянемо, як працює ця модель для PoW майнера.

Перший майнер, який вирішить загадку, отримує винагороду у вигляді криптовалюти. У зображенні описується алгоритм, який використовується майнерами для вирішення загадок.

Спочатку майнер отримує від мережі набір ланцюжків блоків. Майнер вибирає найкращий ланцюжок блоків, який містить його локальний ланцюжок блоків. Потім майнер намагається продовжити свій локальний ланцюжок блоків, додавши до нього новий блок. Для цього майнер звертається до функції $F_{RO,}$ яка використовує його обчислювальну потужність для вирішення математичної загадки. Якщо майнер знаходить рішення загадки, він отримує винагороду у вигляді криптовалюти.

Майнер також оновлює свій локальний ланцюжок блоків, додавши новий, щойно згенерований блок[45].

Ось більш детальний опис алгоритму.

1. Майнер починає з локального ланцюжка блоків, який він створив самостійно.

2. Майнер отримує від мережі набір ланцюжків блоків.

3. Майнер вибирає найкращий ланцюжок блоків, який містить його локальний ланцюжок блоків.

4. Майнер звертається до функції F_{RO}, щоб створити новий блок для свого локального ланцюжка блоків.

5. Майнер чекає, поки функція F_{RO} знайде рішення математичної загадки.

6. Якщо функція F_{RO} знаходить рішення загадки, майнер отримує винагороду у вигляді криптовалюти.

7. Майнер додає новий блок до свого локального ланцюжка блоків.

Тепер розглянемо дії PoS-холдера.

1. Кожний учасник мережі, який має ставку, реєструється у функціональності F_{CERT}.

2. Функціональність F_{CERT} періодично генерує випадковий номер, який називається "бінарної випадковою маяком".

3. Учасники мережі, які мають найбільшу ставку, мають більший шанс бути обраними для створення нового блоку.

4. Вибраний учасник мережі звертається до функціональності F_{CERT} для отримання підпису для нового блоку.

5. Функціональність F_{CERT} генерує підпис для нового блоку.

6. Учасник мережі, який створив новий блок, додає його до свого локального ланцюжка блоків і поширює його по мережі.

Ось більш детальний опис кожного кроку алгоритму:

Крок 1: Реєстрація у функціональності $F_{CERT.}$

Учасники мережі, які хочуть брати участь у створенні нових блоків, повинні зареєструватися у функціональності F_{CERT}. Для цього вони відправляють функціональності F_{CERT} повідомлення з інформацією про свою ставку.

Крок 2: Генерація випадкового номера.

Функціональність F_{CERT} періодично генерує випадковий номер, який називається "бінарної випадковою маяком". Цей номер використовується для визначення того, хто буде обраний для створення нового блоку.

Крок 3: Вибір учасника для створення нового блоку.

Функціональність F_{CERT} сортує учасників мережі за розміром їхніх ставок. Учасники з найбільшою ставкою мають більший шанс бути обраними для створення нового блоку.

Крок 4: Запит на підпис для нового блоку.

Вибраний учасник мережі звертається до функціональності F_{CERT} для отримання підпису для нового блоку. Підпис використовується для підтвердження того, що блок був створений легітимним учасником мережі.

Крок 5: Генерація підпису для нового блоку.

Функціональність F_{CERT} генерує підпис для нового блоку за допомогою секретного ключа, який є відомий лише їй.

Крок 6: Додавання нового блоку до локального ланцюжка блоків.

Учасник мережі, який створив новий блок, додає його до свого локального ланцюжка блоків. Цей ланцюжок блоків є копією ланцюжка блоків, який існує в мережі.

Крок 7: Поширення нового блоку по мережі.

Учасник мережі, який створив новий блок, поширює його по мережі. Інші учасники мережі перевіряють підпис нового блоку і додають його до своїх локальних ланцюжків блоків, якщо він є дійсним.

Опишемо правила, за якими для досягнення консенсусу обирається єдина допустима пара ланцюгів.

Грубо кажучи пара ланцюжків є найкращою допустимою парою, якщо вона має найдовший допустимий PoW-ланцюжок. Ми вводимо процес BestValid, який запускається локально PoW-майнерами або PoS-власниками для вибору найкращої пари ланцюжків.

Процес BestValid параметризується предикатом перевірки вмісту V (-) та початковим ланцюжком Cinit, де V (-) визначає правильну структуру інформації, яка зберігається у блокчейні, як у [19], і приймає на вхід множину пар ланцюгів C 0. Інтуїтивно зрозуміло, що процес перевіряє всі пари ланцюгів (C,C˜) у C’ 0 а потім знаходить допустимі пари ланцюгів з найдовшим PoW-ланцюгом.

Підкреслимо, що оскільки кожен валідний PoS-блок прив'язаний до PoW-блоку, і кожен PoW-блок або PoS-блок є валідним, якщо його однорангові блоки є валідними. Таким чином, пара ланцюжків є валідною, якщо всі пари блоків у цій парі є валідними. А валідна пара блоків по відношенню до PoW-майнерів повинна складатися з двох ланцюжків (PoW-ланцюжок і PoS-ланцюжок) однакової довжини однакової довжини. З іншого боку, валідна пара ланцюгів по відношенню до PoS-власників може мати PoW-ланцюг довшим за PoS-ланцюг на один блок, оскільки PoW-ланцюг може бути розширений на один новий блок у попередньому PoW-раунді. При цьому, якщо гравець, який виконує цей процес, є PoS-власником і якщо існує новий PoW-блок, цей блок буде валідуватися окремо, оскільки відповідний йому PoS-блок ще не ще не згенерований.

Таким чином, для кожної пари ланцюжків процес спочатку перевіряє, чи довжина PoW-ланцюжка в парі довша за PoS-ланцюжок на один блок і валідує спочатку цей новий PoW-блок, а потім оцінює кожну блок-пару в цій парі ланцюжків.

Як вже було сказано, PoS-блоки генеруються з PoW-блоків; таким чином, PoS-блоки без PoS-блоки без відповідних PoW-блоків не є валідними. Більш детально BestValid працює наступним чином. На вхід подається набір ланцюжків C 0 та індекс Type, де Type ∈ {PoW-miner,PoS-holder}. Для кожної пари ланцюжків (C,C˜) процес перевіряє кожен PoW-блок разом з відповідним йому PoS-блоком. Однак, у кожному раунді може з'явитися новий PoW-блок без жодного PoS-блоку (це відбувається тільки у PoS-раундах). Тому, якщо len(C)-1 = len(C˜) і Type = PoS-holder (це означає, що означає, що з'явився новий PoW-блок), то він валідує цей блок окремо, а потім валідує кожну пару блоків у розглянутій парі ланцюжків.

Нехай блок C є новим блоком, нам потрібно перевірити, що (1) C[l] пов'язаний з попереднім PoW-блоком з попереднім PoW-блоком і PoS-блоком коректно, (2) PoW-головоломка розв'язана коректно. Для перевірки першої умови умови, BestValid запитує ресурсний випадковий оракул F^{*}_{rRO} за командою обчислює правильний вказівник. Якщо цей вказівник не дорівнює вказівнику, що зберігається у C[`], ця пара ланцюжків є недійсною і буде вилучена з набору ланцюжків C 0. Для перевірки другої умови BestValid запитує ресурсний випадковий оракул $F^{*}_{rRO}$ за командою (RO-VERIFY,C[`]), якщо він отримує (RO-VERIFIED,⊥) від функціоналу, то C[`] є недійсним, що робить недійсною всю пару ланцюжків (C,C˜).

Деякі дослідники запропонували комбінацію PoW і PoS, щоб уникнути недоліків обох. Теоретична здійсненність такого комбінованого методу також була перевірена.

У цій роботі було використано агент-модель блокчейн-системи для моделювання її енергоспоживання, справедливості та надійності. За допомогою цієї моделі оцінено та порівняно ефективність механізмів PoS, PoW та змішаного консенсусу.

Вузловий агент, $x \in X$, генерується з модуля генерації вузлів. Вузловий агент є учасником системи блокчейн.

Кожен агент зберігає три змінні: обчислювальну потужність (C_i), індекс надійності (R_i) та кількість монет (CA_i). Агенти вузла майнять за допомогою обчислювальних потужностей і можуть отримувати винагороду, коли створюють блок. Індекс надійності використовується для того, щоб показати лояльність кожного вузлового агента до системи. Майнинг визначається як кількість монет (CO_i), помножена на час утримання (ht_i). Корисність часу зберігання зменшується з плином часу.

Блок-агент ($y \in Y$) представляє собою блок, згенерований з системи блокчейн. Кожен агент блоку володіє двома змінними: міткою часу (T_j) та індексом складності (d_j). Мітка часу забезпечує відстежуваність ланцюжка, а індекс складності вказує на складність майнінгу.

Модуль генерації вузлів визначає генерацію вузлів. Ми визначаємо індекс приросту (I_i), щоб позначити привабливість вузла для решти вузлів на ринку. Модуль генерації блоків: цей модуль відповідає за генерацію блоків. Агенти блоків визначити індекс ступеня складності. Кожна вершина надає свій розв'язок (S_i) головоломки (P_j).

Розв'язок вузла виражається рівнянням 1 для механізму PoW і рівнянням 2 для механізму PoS.

Вузол, який надасть мінімальний розв'язок, буде творцем блоку і отримає винагороду у вигляді монети.

Ця модель складається з вузлів, які генерують блоки та модулі оцінки. Система спочатку генерує деякі початкові вузли, а потім запускає модуль генерації вузлів кожні 1,440 хвилин. Блок генерується кожні десять хвилин, після чого система оцінюється. Структура моделі показана на рисунку 3.3.

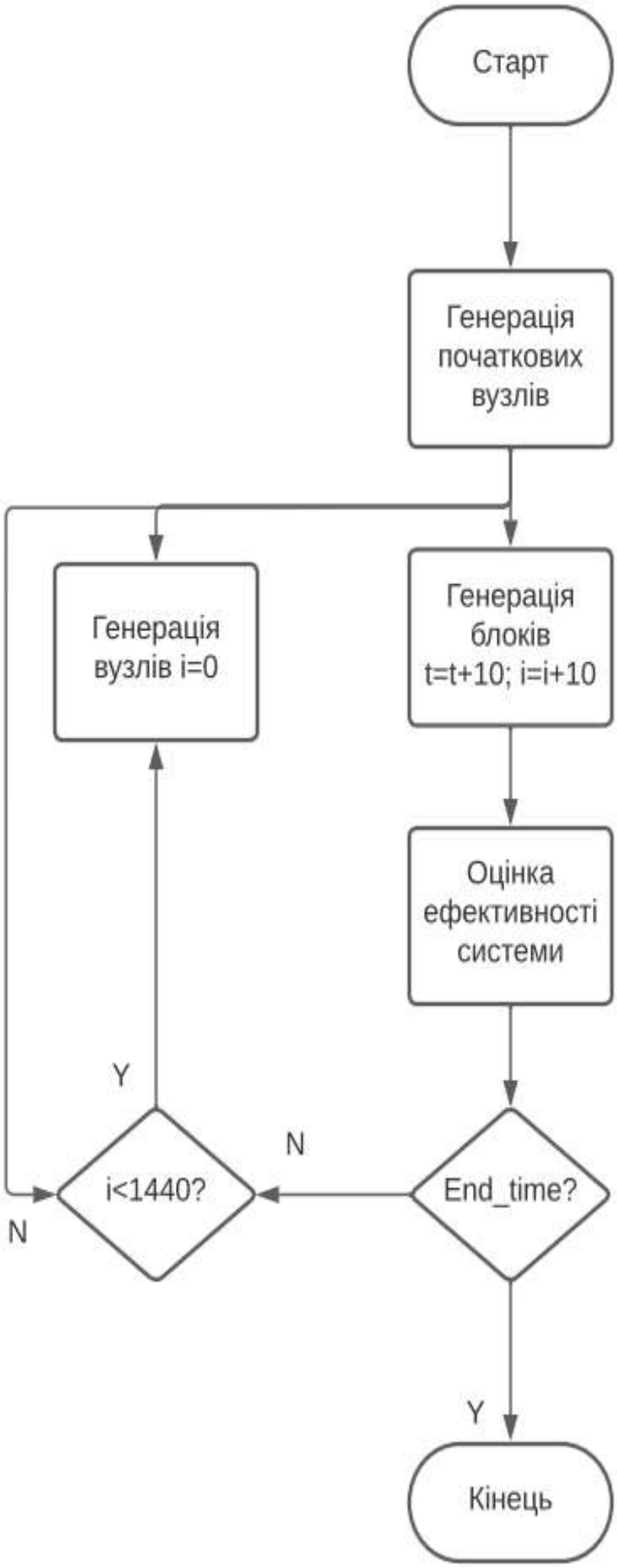

Рисунок 3.3 – Структура агент-орієнтованої моделі

3.3 Висновки

Гібридні протоколи консенсусу, які поєднують елементи Proof of Work (PoW) та Proof of Stake (PoS), а також інноваційні підходи, такі як процедура бозонної дискретизації, вирішують кілька критичних проблем, з якими стикаються блокчейн-мережі.

Проблеми та питання, які вирішують PoW і PoS:

– однією з основних критик PoW є величезне споживання енергії, необхідне для майнінгу. PoS значно знижує енергетичні вимоги, оскільки консенсус досягається не через обчислювальну роботу, а через доказ володіння монетами;

– гібридний підхід може зменшити ризик атаки 51%, оскільки зловмиснику потрібно буде контролювати не тільки більшу частину обчислювальної потужності, але й значну частку монет у мережі;

– PoW схильний до централізації, коли невелика кількість майнерів контролює більшу частину хешрейту. PoS сприяє більшої децентралізації, оскільки влада розподіляється залежно від кількості володіння монетами;

При застосування PoW з включенням процедури бозонної дискретизації могло б теоретично вирішити декілька проблем:

– класичні PoW системи можуть бути вразливими до квантових атак. Використання квантових принципів у майнінгу може допомогти створити системи, які є стійкими до квантових комп'ютерів;

– квантові системи можуть обробляти інформацію ефективніше, ніж класичні комп'ютери, зменшуючи енергетичні витрати і час, необхідний для виконання складних обчислень;

– використання квантових технологій може забезпечити новий рівень криптографічної безпеки, завдяки принципам непередбачуваності та заплутаності квантових станів;

– квантова дискретизація може використовуватися для генерації унікальних ідентифікаторів, які можуть допомогти у подальшому розподіленні мережевих ресурсів і запобігти централізації.

Однак, слід пам'ятати, що це лише гіпотетичне розмірковування, оскільки наразі не існує визначення або застосування "процедури бозонної дискретизації" у блокчейн технологіях. Окрім вирішення проблем, які існують у традиційних консенсусних протоколах, гібридні протоколи та процес дискретизації Бозе також можуть принести нові можливості мережам блокчейн.

Наприклад, гібридні протоколи можна використовувати для створення більш безпечних і ефективних децентралізованих програм. Наприклад, гібридні протоколи, які поєднують PoW і PoS, можна використовувати для створення систем голосування, які є стійкими до атак і забезпечують чесне представництво всіх учасників.[46]

Процес бозонової дискретизації може бути використаний для створення нової криптографії, більш стійкої до квантових атак. Наприклад, квантова дискретизація може бути використана для створення нових алгоритмів шифрування, які не можуть бути зламані квантовими комп’ютерами.

4 ПРАКТИЧНЕ ЗАСТОСУВАННЯ

4.1 Реалізація експеременту з гібридним алгоритмом консенсусу

Ми розглядаємо фіксований ринок зі 100 учасниками.

Тривалість кожного експерименту становить 300 000 хвилин (тобто 30 000 циклів).

Обчислювальна потужність, індекс надійності вузлів та ступінь складності блоків генеруються випадковим чином.

Виходячи з наведеного вище опису, розглянуто шість експериментів (названих "режимами").

Режим 1 повністю використовує механізм PoS. Наступні режими збільшують період на 20% один за одним, щоб прийняти механізм PoW. І режим 6 використовує механізм PoW протягом усього періоду.

Налаштування режимів моделювання показано в таблиці 4.1, і кожен режим моделюється десять разів.

Таблиця 4.1 – Режими моделювання

	Pow	Pos
Режим 1: PoS	0%	100%
Режим 1: 0.2PoW	20%	80%
Режим 1: 0.4PoW	40%	60%
Режим 1: 0.6PoW	60%	40%
Режим 1: 0.8PoW	80%	20%
Режим 1: PoW	100%	0%

4.2 Результати моделювання та їх аналіз

Першим показником ефективності є енергоспоживання. Рисунок 4.1 показує, що енергоспоживання кожного режиму є відносно стабільним.

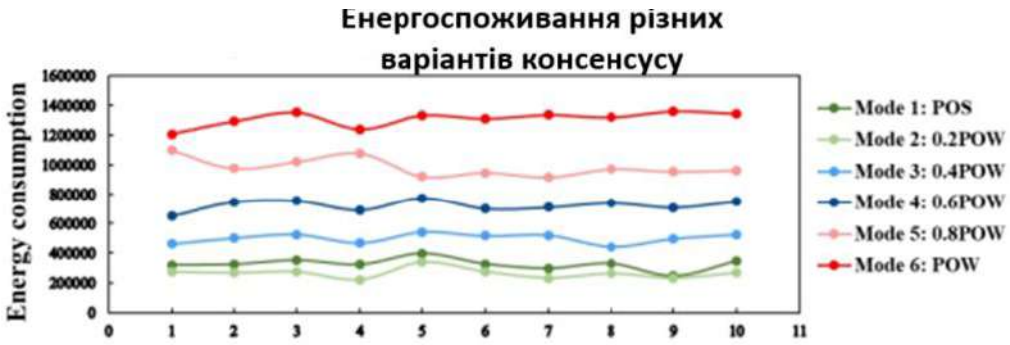

Рисунок 4.1 - Енергоспоживання різних режимів консенсусу

Як правило, чим довший період роботи механізму PoW, тим більше енергії споживається. Однак режим 2 мав мінімальне споживання енергії, а не режим 1. Впровадження механізму PoW у початковий 20% період споживає менше енергії, ніж повне впровадження механізму PoS. Статистику споживання енергії для кожного режиму консенсусу показано у вигляді блок-схеми на рисунку 4.2.

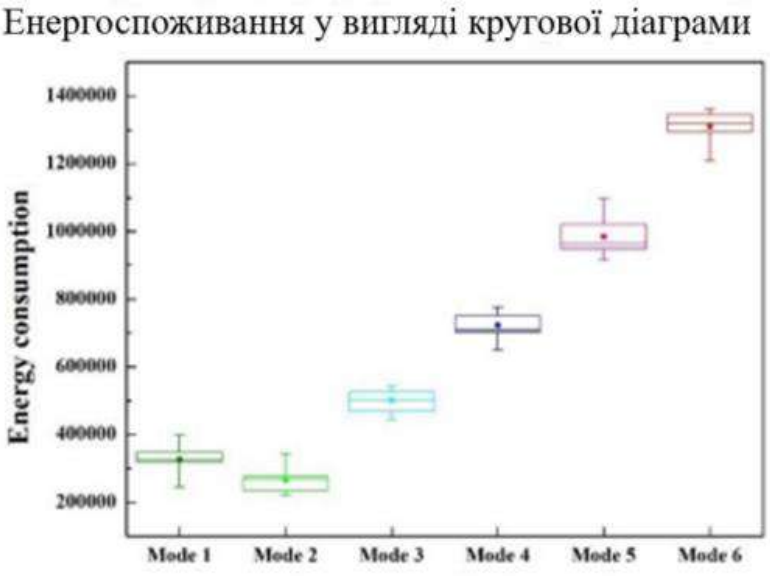

Рисунок 4.2 - Статистика енергоспоживання у вигляді кругової діаграми

Щоб зрозуміти, чому енергоспоживання Режиму 2 нижче, ніж Режиму 1, ми досліджуємо процес споживання енергії в різних режимах консенсусу. Як показано на Рисунку 4.3, хоча Режим 2 споживає більше енергії, ніж Режим 1 в початковий 20% період, Режим 1 вичерпує енергію швидше, ніж Режим 2 в період, що залишився. Крім того, ми бачимо, що поточний загальний обсяг карбування монет у способі 2 більший, ніж у способі 1 у решту 80% періоду, як показано на Рисунку 4.5. Поточний загальний обсяг карбування монет є ефективним способом зменшення споживання енергії. Чим більше децентралізовано монет, тим більше загальний обсяг карбування, оскільки корисність карбування зменшується з часом, і це буде зрозуміло при успішному майнінгу. Крім того, це можна пояснити тим, що процес PoW на початковому етапі робить розподіл ресурсів більш обґрунтованим і збільшує загальний випуск монет, що набагато більше сприяє загальному зниженню енергоспоживання.

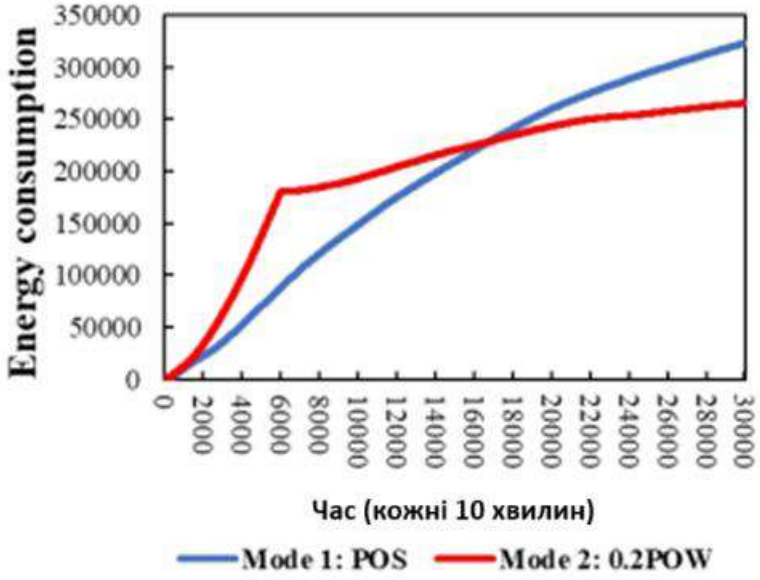

Рисунок 4.3 – Процес споживання енергії

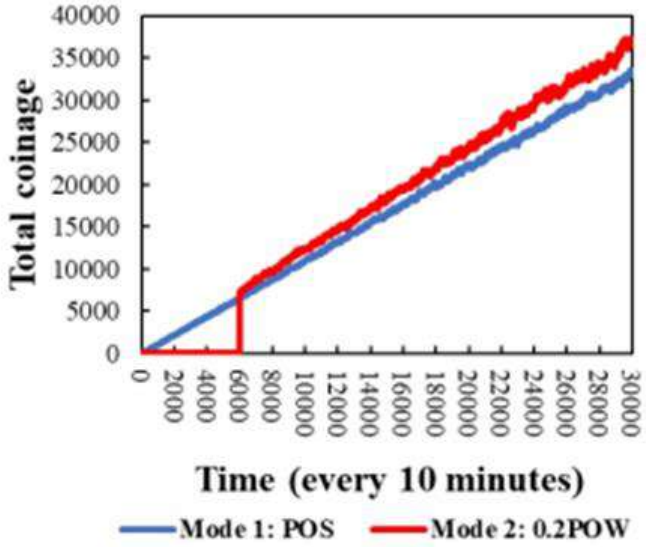

Рисунок 4.4 – Поточна статистика загального карбування монет

Розподіл монет, якими володіють вузли, використовується для вимірювання індексу справедливості системи. Як показано на Рисунку 4.5, більшість вузлів володіють невеликою кількістю монет, в той час як деякі вузли отримують величезну кількість монет в Режимі 1. Чим довше використовується механізм PoW, тим більш справедливим буде розподіл монет. Ми виявили, що дисперсія механізму PoS є особливо великою у порівнянні з PoW та змішаним механізмом.

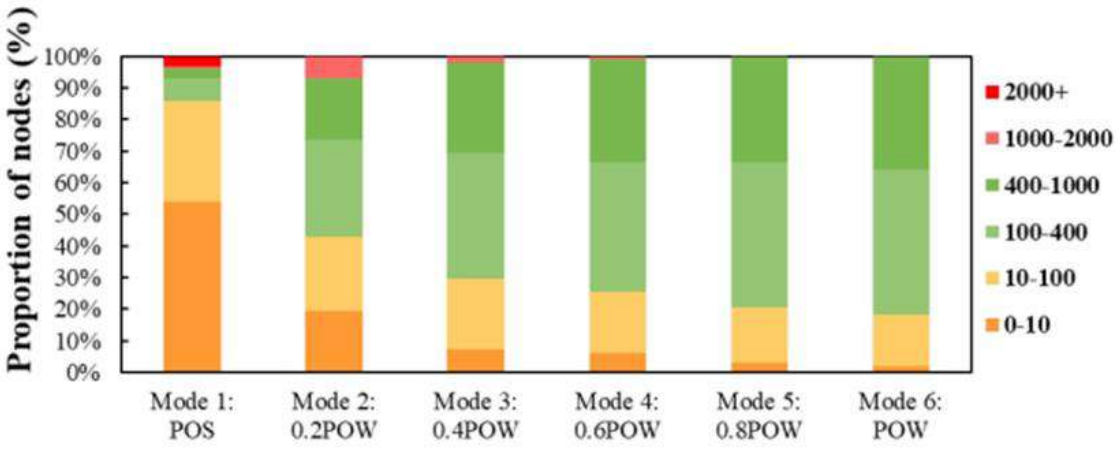

Рисунок 4.5 – Розподіл монет

Для оцінки надійності системи ми використовуємо функцію надійності. Індекс надійності режиму 1 сильно коливається, в той час як інші режими відносно стабільні, як показано на рисунку 4.6. Це пояснюється тим, що початкові вузли мають переваги при використанні механізму PoS, і надійність цих початкових вузлів безпосередньо визначає надійність всієї системи.

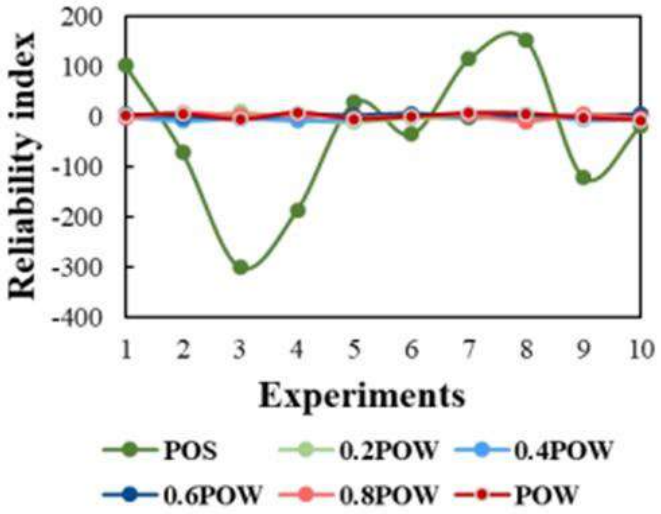

Рисунок 4.6 – надійність системи

4.3 Оцінка можливостей практичного впровадження

У гібридній системі PoW/PoS певні аспекти перевірки транзакцій і створення блоків виконуються майнерами PoW, а інші - валідаторами PoS. Існує кілька способів побудови такої системи:

1. Чергування фаз: Блокчейн може чергувати фази PoW і PoS. Наприклад, PoW можна використовувати для створення нових блоків, а PoS - для перевірки транзакцій всередині цих блоків.

2. Паралельна робота: Обидва механізми можуть працювати паралельно, при цьому майнери PoW працюють над створенням нових блоків, а валідатори PoS відповідають за завершення транзакцій, додаючи додатковий рівень безпеки.

3. Багаторівневий підхід: Блокчейн може використовувати PoW для своєї базової структури, а рівень PoS - для щоденних транзакцій і рішень щодо управління.

Основні переваги впровадження гібридного протоколу включають в себе наступні:

1. Підвищена безпека: поєднання обчислювальної складності PoW з економічною вигодою PoS може створити більш безпечну мережу, стійку до різних типів атак.

2. Енергоефективність: зменшуючи залежність від енергоємного майнінгу, гібридна система може значно знизити вплив блокчейн-операцій на навколишнє середовище.

3. Децентралізація: включення PoS дозволяє розширити участь в процесі досягнення консенсусу, що може призвести до більш децентралізованої мережі.

4. Масштабованість: завдяки потенціалу більш швидкої перевірки транзакцій через PoS, гібридна система може поліпшити масштабованість в порівнянні з традиційними блокчейнами PoW.

Незважаючи на свої переваги, існує кілька викликів, які слід враховувати при впровадженні гібридного протоколу блокчейну:

1. Складність: інтеграція двох різних механізмів консенсусу може створити складну систему, яку важче розробляти, підтримувати і захищати.

2. Проблеми переходу: для існуючих блокчейнів, які хочуть перейти на гібридну модель, перехід без порушення роботи мережі або втрати довіри може бути складним.

3. Балансування: знайти правильний баланс між елементами PoW і PoS, щоб обидва були ефективними і вигідними, може бути непросто.

4. Нові вектори атак: поєднання двох механізмів може призвести до появи нових вразливостей або векторів атак, які необхідно усунути.

Можливість реалізації гібридного блокчейн-протоколу, який поєднує в собі сильні сторони PoW і PoS, є захоплюючою перспективою для майбутнього технології блокчейн. Така система може запропонувати підвищену безпеку,

покращену енергоефективність, більшу децентралізацію та кращу масштабованість. Однак складність інтеграції цих механізмів і потенційні проблеми повинні бути ретельно продумані і вирішені шляхом ретельного тестування і розробки [47].

Оскільки простір блокчейну продовжує розвиватися, ми можемо побачити більше проектів, які експериментують з гібридними протоколами, розширюючи межі можливого за допомогою цієї трансформаційної технології.

4.4 Висновки

Режим роботи гібридного протоколу консенсусу, який поєднує елементи PoW і PoS, залежить від конкретних потреб і цілей блокчейн-мережі.

Режим 2, в якому PoW використовується в початковий період, а потім поступово замінюється PoS, є хорошим вибором для мереж, які хочуть:

– почати з високої безпеки, забезпеченої PoW;

– знизити споживання енергії, поступово перемикаючись на PoS;

– розширити децентралізацію, дозволяючи більшій кількості учасників брати участь в процесі досягнення консенсусу.

Режим 6, в якому PoW використовується протягом усього періоду, є хорошим вибором для мереж, які хочуть:

– забезпечити найвищу безпеку, можливу з PoW;

– знизити ризик атаки 51%;

– уникати централізації влади, яка може виникнути в системах PoS.

Інші режими роботи гібридних протоколів також можуть бути доречними в конкретних ситуаціях. Наприклад, режим, в якому PoW використовується для створення нових блоків, а PoS - для перевірки транзакцій, може бути хорошим вибором для мереж, які хочуть забезпечити високу безпеку створення блоків і високу масштабованість перевірки транзакцій[48].

ВИСНОВКИ

Метою даного дослідження було покращення існуючих протоколів консенсусу в області блокчейн технологій з фокусом на протоколах Proof of Work (PoW) та Proof of Stake (PoS).

У даній роботі розглядаються основні механізми консенсусу в блокчейнах, такі як доказ роботи (PoW) і доказ частки (PoS). Досліджуються переваги та недоліки кожного з цих алгоритмів, а також обговорюється важливість розробки нових алгоритмів, які поєднують найкращі характеристики обох підходів.

Також висвітлено можливі наслідки впровадження квантових обчислень у блокчейн. Зазначається, що хоча це може становити загрозу для існуючих мереж, використовуючи класичну криптографію, однак водночас квантові обчислення можуть призвести до збільшення швидкості транзакцій, покращення масштабованості та підвищення безпеки[49].

Наведено конкретні рекомендації для підготовки до впровадження квантових обчислень у блокчейн, такі як розробка квантово-стійких алгоритмів консенсусу, перехід на квантову криптографію та обробка даних про потенційні загрози.

Обговорили режими роботи гібридних протоколів консенсусу, які комбінують PoW і PoS. Режими 2 і 6 вважаються оптимальними в різних ситуаціях, надаючи можливість почати з високої безпеки і поступово переходити до менш енергозатратного та менш централізованого підходу.

Також розглянуто гіпотетичне використання "процедури бозонної дискретизації" у контексті PoW з метою вирішення проблем, таких як квантова стійкість, ефективність, безпека та розподілення.

Ще можна виділити основні моменти:

– Proof of Work (PoW) є основним механізмом, що дозволяє досягати консенсусу в децентралізованих мережах шляхом розв'язання складних математичних задач[50];

– протоколи PoW та PoS використовуються у блокчейн-системах і мають вплив на кібербезпеку;

– дослідження показує, що PoS продовжує відігравати важливу роль у майбутньому індустрії блокчейну;

– вибір протоколу консенсусу залежить від поставлених цілей та потреб проекту, таких як децентралізація та тип блокчейну (приватний або публічний).

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. URL: https://bitcoin.org/bitcoin.pdf. (дата звернення: 12.09.2023).

2. Яковлєв С. В. Конспект лекцій з дисципліни «Спеціальні розділи криптографії». — 2017.

3. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. — 2015.

4. BitFury Group. Proof of Stake versus Proof of Work. URL: https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf (дата звернення: 14.09.2023)

5. Iddo Bentov, Charles Lee, Alex Mizrahi, Meni Rosenfeld. Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. — URL: https://eprint.iacr.org/2014/452.pdf (дата звернення: 15.09.2023)

6. Proof of burn. — URL: https://en.bitcoin.it/wiki/Proof_of_burn (дата звернення: 16.09.2023)

7. NEM Technical Reference. Version 1.2.1. — URL: https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf (дата звернення: 14.09.2023)

8. Secret sharing. — URL: https://en.wikipedia.org/wiki/Secret_sharing (дата звернення: 18.09.2023)

9. Брюс Шнайєр. Прикладна криптографія. 2 видання. — 2002

10. Ліфшиц Ю. Конспект лекцій з дисципліни «Сучасні задачі криптографії». — 2005.

11. Asmuth C., Bloom J. A modular approach to key safeguarding. — URL: https://ieeexplore.ieee.org/abstract/document/1056651 (дата звернення: 19.09.2023)

12. Иванцов А.М., Рацеев С.М. О применении эллиптических кривых в некоторых проверяемых схемах разделения секрета. — URL: http://apu.npomars.com/images/pdf/49_4.pdf. (дата звернення: 21.09.2023)

13. What is Cryptocurrency: Everything You Must Need To Know! — URL: https://blockgeeks.com/guides/ what-is-cryptocurrency/ (дата звернення: 22.09.2023)

14. Proof of burn – Bitcoin Wiki — URL: https://en.bitcoin.it/wiki/Proof_of_burn. (дата звернення: 22.09.2023)

15. Proof of Burn (Cryptocurrency) – Investopedia. — URL: https://www.investopedia.com/terms/p/proof-burn-cryptocurrency.asp. (дата звернення: 23.09.2023)

16. Bentov, I., Gabizon, A., and Mizrahi, A. 2014. Cryptocurrencies without Proof of Work. Preprint. URL: http://www.cs.technion.ac.il/~idddo/CoA.pdf. (дата звернення: 22.09.2023)

17. Bitcoin wiki. P2SH. URL: https://github.com/bitcoin/bips/blob/master/-0016.mediawiki. (дата звернення: 26.09.2023)

18. Hearn, M. 2011. Bitcoin wiki: Contracts. URL: https://en.bitcoin.it/wiki/Contracts. (дата звернення: 27.09.2023)

19. Maxwell, G. 2011b. Bitcoin wiki: Zero knowledge contingent payment. URL: https://en.bitcoin.it/wiki/Zero_ Knowledge_Contingent_Payment. (дата звернення: 27.09.2023)

20. Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. Cryptology ePrint Archive. URL: https://eprint.iacr.org/2014/452.pdf. (дата звернення: 28.09.2023)

21. T. Lee, M. Ray, and M. Santha, Strategies for quantum races (2018).

22. S. Park and N. Spooner, The superlinearity problem in post-quantum blockchains, Cryptology ePrint Archive, Paper 2022/1423 (2022), URL:https://eprint.iacr.org/ 2022/1423. (дата звернення: 29.09.2023)

23. S. Aaronson and A. Arkhipov, The computational complexity of linear optics, in Proceedings of the FortyThird Annual ACM Symposium on Theory of Computing, STOC '11 (Association for Computing Machinery, New York, NY, USA, 2011) p. 333–342.

24. G. M. Nikolopoulos and T. Brougham, Decision and function problems based on boson sampling, Phys. Rev. A 94, 012315 (2016).

25. G. M. Nikolopoulos, Cryptographic one-way function based on boson sampling, Quantum Information Processing 18, 10.1007/s11128-019-2372-9 (2019).

26. J. Dubrovsky, L. Kiffer, and B. Penkovsky, Towards optical proof of work, Cryptoecon. Syst. 11 (2020).

27. S. Pai, T. Park, M. Ball, B. Penkovsky, M. Dubrovsky, N. Abebe, M. Milanizadeh, F. Morichetti, A. Melloni, S. Fan, O. Solgaard, and D. A. B. Miller, Experimental evaluation of digitally verifiable photonic computing for blockchain and cryptocurrency, Optica 10, 552 (2023).

28. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction (Princeton University Press, USA, 2016).

29. T. Gard, K. R. Motes, J. P. Olson, P. P. Rohde, and J. P. Dowling, From atomic to mesoscale (World Scientific, 2015) Chap. An introduction to boson-sampling, p. 167.

30. J. A. Garay, A. Kiayias, and N. Leonardos. The bitcoin backbone protocol: Analysis and applications. In E. Oswald and M. Fischlin, editors, EUROCRYPT 2015, Part II, volume 9057 of LNCS, pages 281–310. Springer, Heidelberg, Apr. 2015.

31. Koutsoupias, M. Kyropoulou, and Y. Tselekounis. Blockchain mining games. In Pro-ceedings of the 2016 ACM Conference on Economics and Computation (EC), pages 365–382, 2016.

32. A.Miller, A. E. Kosba, J. Katz, and E. Shi. Nonoutsourceable scratch-off puzzles to discourage bitcoin mining coalitions. In I. Ray, N. Li, and C. Kruegel:, editors, ACM CCS 15, pages 680–691. ACM Press, Oct. 2015.

33. Yonatan Sompolinsky, Yoad Lewenberg, and Aviv Zohar. 2016. SPECTRE: A Fast and Scalable Cryptocurrency Protocol. IACR Cryptology ePrint Archive 2016 (2016), 1159.

34. Pinzon C. Double-Spend Attack Models with Time Advantage for Bitcoin / C. Pinzon, C. Rocha // Electronic Notes in Theoretical Computer Science. – 2016. – Vol. 329. – P. 79-103.

35. Crosby M, Pattanayak P, Verma S, and Kalyanaraman 2016 Blockchain technology: Beyond bitcoin Applied Innovation 211

36. Saleh F 2019 Blockchain without waste: Proof-of-stake SSRN 3183935

37. Athey S, Parashkevov I, Sarukkai V, and Xia J 2016 Bitcoin pricing, adoption, and usage: Theory and evidence SSRN 2826674

38. King S and Nadal S 2012 Ppcoin: Peer-to-peer crypto-currency with proof-of-stake (self-published paper)

39. Poelstra A 2014 Distribution consensus from proof of stake is impossible (self-published paper)

40. Bentov I, Lee C, Mizrahi A, and Rosenfeld M 2014 Proof of activity: Extending bitcoin's proof of work via proof of stake (IACR Cryptology ePrint Archive) p 452 Duong T, Chepurnoy A, Fan L, and Zhou H S 2018 Twinscoin: a cryptocurrency via proof-of-work and proof-of-stake Proc. The 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts (ACM press) pp 1-13

41. Duong T, Fan L, and Zhou H S 2016 2-hop blockchain: Combining proof-of-work and proof-ofstake securely (IACR Cryptology ePrint Archive) p 71

42. Zubov V. An Electronic Signature Within The Digital Economy. Proceedings of the II International Scientific Conference GCPMED 2019 - "Global Challenges and Prospects of the Modern Economic Development". 2019. P.621-625.

43. TrustChain: A Sybil-resistant scalable blockchain / Pim Otte, Martijn de Vos, Johan Pouwelse // Scienct Direct. – 2017. – URL: https://www.sciencedirect.com/science/article/pii/S0167739X17318988. (дата звернення : 30.11.2023)

44. Y. Sompolinsky and A. Zohar. Secure high-rate transaction processing in bitcoin. In R. Bohme and ¨ T. Okamoto, editors, FC 2015, volume 8975 of LNCS, pages 507–527. Springer, Heidelberg, Jan. 2015.

45. O. Schrijvers, J. Bonneau, D. Boneh, and T. Roughgarden. Incentive compatibility of bitcoin mining pool reward functions. In Financial Cryptography and Data Security (FC), 2016.

46. T. Okamoto and K. Ohta. Universal electronic cash. In J. Feigenbaum, editor, CRYPTO’91, volume 576 of LNCS, pages 324–337. Springer, Heidelberg, Aug. 1992.

47. Bentov, A. Gabizon, and A. Mizrahi. Currencies without proof of work. In Bitcoin Workshop Financial Cryptography and Data Security (FC), 2016.

48. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. — 2015.

49. Pinzon C. Double-Spend Attack Models with Time Advantage for Bitcoin / C. Pinzon, C. Rocha // Electronic Notes in Theoretical Computer Science. – 2016. – Vol. 329. – P. 79-103.

50. G. M. Nikolopoulos, Cryptographic one-way function based on boson sampling, Quantum Information Processing 18, 10.1007/s11128-019-2372-9 (2019).

ДОДАТОК А

Копії наукових публікацій

стеганоконтейнер [1,2]. Важливо дотримувати однаковий рівень або діапазон інтенсивності дії при проведенні порівняльного аналізу.

3. Вилучення ЦВЗ. Вилучення ЦВЗ проводиться відповідно до методу вбудовування, об'єм зчитаного ЦВЗ повинен відповідати об'єму вбудовуваного. Застосовувати додаткові заходи при відтворенні даних ЦВЗ не можна, навіть якщо ці заходи передбачаються при вилученні використаним стеганографічним алгоритмом.

4. Оцінка стійкості ЦВЗ. Стійкість ЦВЗ оцінюється за допомогою різних методів [2]. Наприклад, використовується коефіцієнт помилкових бітів (Bit Error Rate), який застосовується при оцінці модифікацій бітової послідовності [3]:

$$BER\left(S,S^{''}\right)=\frac{\sum p_i}{N}$$

де N – загальна кількість біт, p_i=1, якщо $s_i \neq s_i^{''}$ і p_i=0, якщо $s_i \neq s_i^{''}$, де s_i – біт початкового зображення, $s_i^{''}$ – біт кінцевого зображення.

При $BER(S,S^{''})$=0 вбудовані і вилучені дані ЦВЗ співпадають. При $BER(S,S^{''})$=1 будь-який біт вхідного зображення відрізняється від вихідного (має місце «негатив»). Вважають, що при $BER(S,S^{''})\geq 0.5$ вбудовані дані втрачено.

5. Рівень викривлення. Властивість ЦВЗ, вбудованого в стеганоконтейнер, протистояти різним атакам, які пов'язані з різними причинами (алгоритм впровадження цифрового водяного знака, коефіцієнт сили вбудовування P, зовнішня дія, тощо).

У протилежність зовнішнім атакам, властивості яких можна відтворити для будь-яких стеганоконтейнерів ЦВЗ, вбудованих різними стеганографічними алгоритмами, параметри P і метод впровадження є унікальними для будь-якого стеганографічного алгоритму [3]. Створюючи єдині початкові умови, які використовуються при порівняльному аналізі стійкості ЦВЗ, зазвичай стежать за таким параметром рівня модифікацій, які з'являються при вбудовуванні ЦВЗ.

Список використаних джерел та літератури

1. Дурняк Б. В., Музика Д. В., Сабат В. І. Стеганографічні методи захисту документів. Львів : Укр. акад. друкарства, 2014. 159 с.
2. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. Київ : Вид-во DIRECTLINE, 2019. 714 с.
3. Belim S. V., Vilkhovskiy D. E. Method of detecting hidden data transmission via the Koch-Zhao steganographic algorithm. Journal of Physics: Conf. Series 1210 (2019) 012012. doi:10.1088/1742-6596/1210/1/012012.

УДК 004.056:621.397.3:004.942

Гунявий Д.А., студент,
Джулій В.М., к.т.н., доцент,
Чешун В.М., к.т.н., доцент
Хмельницький національний університет

ОЦІНКА СТІЙКОСТІ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ

Стеганосистема цифрового водяного знаку (ЦВЗ) повинна будуватись так, щоб мінімізувати імовірність виникнення помилок, оскільки будь-яка помилка може привести до неправильної роботи стеганодетектора. Щодо запобігання виникненню помилок надважливою є стійкість ЦВЗ. Схема оцінювання стійкості ЦВЗ до зовнішніх дій схематично представлена на рисунку 1 (з використанням дискретного вейвлет-перетворення - ДВП).

Рисунок 2 – Схема оцінки стійкості цифрових водяних знаків

Оцінка стійкості ЦВЗ до зовнішніх дій включає наступні етапи:

1. Впровадження ЦВЗ. При проведенні досліджень на предмет порівняння стійкості ЦВЗ до різних зовнішніх дій, необхідне забезпечення однакових початкових умов для впровадження ЦВЗ [1]. Дана вимога пред'являється, в першу чергу, до стеганоконтейнеру. ЦВЗ може бути будь-яким, а його тотожність при використанні різних стеганоалгоритмів може не виконуватися. Якщо ЦВЗ виробляється випадковим чином, то результати будуть більш якісними. Об'єми ЦВЗ роблять рівними, так як ця вимога впливає на властивості ЦВЗ (стійкість тощо).

2. Зовнішня дія на стеганоконтейнер з ЦВЗ. Зовнішня дія на стеганоконтейнер може бути довільною і повною, тобто на весь

ВІЙСЬКОВИЙ ІНСТИТУТ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ЗБІРНИК
ТЕЗ ДОПОВІДЕЙ

XIX Міжнародної науково-практичної конференції

«Військова освіта і наука: сьогодення та майбутнє»

10 листопада 2023 року

Київ – 2023

ВІЙСЬКОВИЙ ІНСТИТУТ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ТЕЗИ ДОПОВІДЕЙ

Всеукраїнської науково-практичної конференції молодих вчених, ад'юнктів, слухачів, курсантів і студентів

**"Молодіжна військова наука
у Київському національному університеті
імені Тараса Шевченка"**

27 квітня 2023 року

За загальною редакцією начальника Військового інституту Київського національного університету імені Тараса Шевченка бригадного генерала Анатолія Шевченка

Київ – 2023

Гунявий Д.А. (ХмНУ)
к.т.н., доц. Чешун В.М. (ХмНУ)

АНАЛІЗ ПРОТОКОЛІВ КОНСЕНСУСУ У БЛОКЧЕЙН-ТЕХНОЛОГІЯХ: ВПЛИВ ДОКАЗУ РОБОТИ (POW) ТА ДОКАЗУ ЧАСТКИ (POS) НА ЕФЕКТИВНІСТЬ, БЕЗПЕКУ ТА СТІЙКІСТЬ

Порівняльний аналіз Proof of Work (PoW) і Proof of Stake (PoS) є важливим аспектом розуміння їх впливу на ефективність, безпеку та стабільність мережі блокчейн.

Механізм Proof of Work (PoW) використовує так званний «пазл», який майнер повинен вирішити, щоб отримати доступ до додавання нових блоків. «Пазл» має рівень складності, що налаштовується, і вирішується шляхом обчислення значення nonce; як тільки значення nonce отримано, воно додається до інформації заголовка блоку і пропускається через хеш-функцію SHA-256 для отримання хеш-значення. Якщо отримане хеш-значення нижче встановленого порогу, то отримане значення nonce приймається і майнер може додати блок до блокчейну. Потім майнер транслює цей блок всій мережі, і всі вузли мережі підтверджують справжність хеш-значення і додають блок до блокчейну. Механізм PoW забезпечує безпеку блокчейну, оскільки він вимагає значних обчислювальних ресурсів для створення нового блоку. Це ускладнює для зловмисників підробку транзакцій або створення хибних блоків[1].

Доказ частки (PoS), який спочатку був запропонований для Peercoin, був використаний як альтернатива PoW для усунення надмірне енергоспоживання вузлів. З моменту виборів пропозиції блоку на основі балансу рахунку здається несправедливі, багато запропонованих рішень включають розмір ставки. Хоча PoS є енергоефективним у порівнянні з PoW, він не стійкий до атак. Відповідно, кілька блокчейн-рішень спочатку використовують PoW і поступово трансформуються в PoS.

Основна відмінність між PoW і PoS полягає в тому, як вони визначають валідатори блоків. Proof of Stake є найпопулярнішою альтернативою Proof of Work. Цей механізм консенсусу розроблено для подолання деяких обмежень PoS, таких як масштабованість і споживання енергії. У механізмі PoS учасники називаються валідаторами. Їм не потрібне потужне обладнання для перевірки пристрою. Замість цього вони повинні атакувати (блокувати) рідний блокчейн криптовалюти. На основі суми криптовалюти, поставленої на ставку, мережа вибирає переможця, який отримує частку комісії за транзакції з блоків, які він підтверджує. Чим більше токенів у ставки, тим вищий шанс бути обраним валідатором.

Вибір між цими механізмами залежить від конкретних потреб і цілей блокчейн мережі.

к.т.н., доц. Джулій В.М. (ХмНУ)
Димбовський М.В. (ХмНУ)

ДОСЛІДЖЕННЯ АКТУАЛЬНИХ ЗАГРОЗ БЕЗПЕКИ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Визначення переліку актуальних загроз безпеки інформації, оцінка ефективності системи захисту є невід'ємною частиною життєвого циклу

Гунявий Д.А. (ХмНУ)
канд.техн.наук, доц. Чешун В.М. (ХмНУ)

ФІЗИЧНИЙ ТА ПРОГРАМНИЙ ЗАХИСТ ІНФОРМАЦІЇ І ВЗАЄМОЗАЛЕЖНА ОЦІНКА ПАРАМЕТРІВ БЕЗПЕКИ

Регулярна поява нових загроз вимагає постійного вдосконалення технологій і систем захисту об'єктів інформаційної діяльності, адже у випадку успішної реалізації атаки об'єкту (підприємству, організації тощо) може бути завдано непоправної шкоди.

В сучасних умовах система захисту реалізується із застосуванням комплексного поєднання технологій і засобів фізичного (технічного тощо) та програмного захисту інформації [1]. Фізичний захист забезпечує захист фізичного середовища зберігання і обробки інформації і забезпечується, зокрема, технічними засобами контролю доступу, системами відеоспостереження, датчиками руху та іншими засобами, які забезпечують безпеку приміщення, а також засобами, які забезпечують надійність і безпеку роботи серверного, мережевого та іншого обладнання системи [1]. Програмний захист базується на використанні для забезпечення безпеки інформації саме програмних засобів: антивірусних програм, мережевих файрволів, систем виявлення вторгнень та інших програмних засобів, які забезпечують захист від кібератак та вірусів, програмних засобів шифрування, програмних систем авторизації та аутентифікації користувачів тощо. До складу програмного захисту можуть входити найрізноманітніші програмні технології, які забезпечують конфіденційність даних та захист від несанкціонованого доступу до них [2]. Комплексне забезпечення фізичного та програмного захисту інформації є основною складовою сучасної інформаційної безпеки.

Поряд з комплексністю підходів до забезпечення захисту інформації, урахування взаємозв'язків і залежностей технологій фізичного та програмного захисту інформації постає передумовою якості оцінювання і підвищення ефективності її захисту. Розглянуто можливості проведення оцінок у ряді важливих завдань інформаційної безпеки: оцінка апріорних і апостеріорних ризиків; оцінка показників умовної ентропії реалізованості загроз при поєднанні технологій захисту інформації; оцінка ефективності комплексного застосування фізичного та програмного захисту як взаємозалежних систем.

Взаємозалежна оцінка дозволяє забезпечити більш повне і точне визначення загроз і ризиків, що сприяє підвищенню ефективності захисту від кібератак та інших загроз.

Список використаних джерел:

1. Kelly O'Brien. Cyber & Physical Security: Why You Need Both. Compass IT Compliance, January 27, 2022. URL:https://www.compassitc.com/blog/cyber-physical-security-why-you-need-both.

2. Mahmudova Shafagat. About Some Methods for Software Security. Transactions on Networks and Communications; Volume 7, No. 2, April 2019. P. 14-19. DOI:10.14738/tnc.72.6334

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Гунявого Дениса Андрійовича
ПІБ здобувача вищої освіти

Студента ФІТ, 2 курсу, групи КБм-22-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

14.11.2023
дата


підпис

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1016003519

Дата перевірки:
13.12.2023 22:14:58 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
13.12.2023 22:42:16 EET

ID користувача:
100008300

Назва документа: **ГунявийД на плагіат_merged**

Кількість сторінок: 69 **Кількість слів:** 14365 **Кількість символів:** 109865 **Розмір файлу:** 1.45 MB **ID файлу:** 1015687332

2.44%
Схожість

Найбільша схожість: 0.52% з Інтернет-джерелом (https://futurenow.com.ua/shho-take-kvantovyj-blokchejn)

2.14% Джерела з Інтернету	244	Сторінка 71
0.48% Джерела з Бібліотеки	49	Сторінка 72

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	79

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 11%**

	Документ		Сумарний збіг по Базі Даних	
ID: 123078 Назва: Метод аналізу та оцінювання протоколів консенсусу для блокчейнів з доказом роботи(PoW) та без (PoS) Додано в БД: 2023-12-13 Автора: Гунявий Д.А. Керівники: Чешун В.М. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	90751	1385	487 (1%)	6 (0%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Метод аналізу та оцінювання протоколів консенсусу для блокчейнів з доказом роботи(PoW) та без (PoS)

Автор: Гунявий Денис Андрійович

Спеціальність: 125 – Кібербезпека

Освітня програма: освітньо-професійна

Науковий керівник: Чешун Віктор Миколайович, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 99%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 100%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100 %, визнається роботою з високою унікальністю тексту і допускається до захисту.

Керівник роботи _____ В.М. Чешун

Гарант ОП _____ В.Ю. Тітова

Завідувач кафедри кібербезпеки _____ Ю.П. Кльоц

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «магістр»

Магістр: Гунявий Денис Андрійович

Тема: Метод аналізу та оцінювання протоколів консенсусу для блокчейнів з доказом роботи (PoW) та без (PoS)

Галузь знань: 12 – Інформаційні технології

Спеціальність: 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «магістр»:

кількість листів креслень _____; кількість сторінок записки 68

1. Короткий зміст кваліфікаційної роботи та прийнятих рішень: в рамках роботи запропоновано метод удосконалення існуючих протоколів консенсусу для блокчейну.

2. Висновок про відповідність кваліфікаційної роботи завданню: Кваліфікаційна робота магістра у повній мірі відповідає поставленому завданню у теоретичній, та практичній частинах.

3. Характеристика виконання виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: Вступ кваліфікаційної роботи висвітлює актуальність теми роботи, декларує мету, цілі і завдання дослідження, описує наукову новизну та практичну цінність результатів дослідження. У першому розділі проводиться дослідження предметної області, аналізується розвиток та поточний стан блокчейн технологій та їх ролі у кібербзпеці. У другому розділі складається математична модель протоколів консенсусу на основі обгрунтованих автором роботи вимог, впровадження квантових обчислень у блокчейн. Третій розділ містить опис запропонованого гібридного алгоритму консенсусу. Четвертий розділ присвячено дослідженням можливостей та апробації запропонованого методу, а також містить аналіз його енергоефективності.

4. Позитивні сторони роботи: Кваліфікаційна робота є послідовним продовженням тематики еволюції блокчейн технологій і має перевагою вдосконалення алгоритмів консенсусу за рахунок покращення енергоефективності

5. Негативні сторони роботи: Відсутній розгляд питань та рекомендації щодо практичного впровадження запропонованого методу.

6. Оцінка графічного оформлення та пояснювальної записки роботи: Графічне оформлення виконане якісно та у відповідності до теми кваліфікаційної роботи з дотриманням стандартів. Пояснювальна записка відповідає нормам оформлення текстових документів університету.

7. Відгук про роботу в цілому В загальному кваліфікаційна робота студента заслуговує позитивної оцінки. Матеріал дипломної роботи структурований та чіткий. Але видно що потрібно більше досліджень у напрямку блокчейн технологій. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Наукова новизна та практична цінність роботи присутня.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи: Представлена кваліфікаційна робота, за сумою позитивних та негативних сторін, науковою новизною, актуальністю та практичною цінністю заслуговує на оцінку «добре»

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Мартинюк Валерій Володимирович
Завідувач кафедри автоматизації комп'ютерно-інтегрованих технологій та робототехніки, доктор технічних наук, професор

«14» 12 2023. (підпис)

ХНУ. Зам. 54, тир. 6000, 2007.