Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

Магістр
(назва освітнього ступеня)

на тему: Дослідження та застосування моделі «Proof of Rank» в технологіях BlockChain

Виконав: студент 6 курсу, групи СТм-61
спеціальності 126 Інформаційні системи та технології
(шифр і назва спеціальності)

_____ Чорний Я. М.
(підпис) (прізвище та ініціали)

Керівник _____ проф. Сверстюк А.С.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ доц. Никитюк В.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ доц. Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ _____
(підпис) (прізвище та ініціали)

м. Тернопіль – 2025

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ доц. Боднарчук І.О.
(підпис) (прізвище та ініціали)
« 17 » 11 . 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня магістр
(назва освітнього ступеня)

за спеціальністю 126 Інформаційні системи та технології
(шифр і назва спеціальності)

студенту Чорному Ярославу Миколайловичу

1. Тема роботи Дослідження та застосування моделі «Proof of Rank» в технологіях BlockChain

Керівник роботи Сверстюк Андрій Степанович, д.т.н, проф. каф. КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом по університету від « 27 » листопада 2025 року № 4/7-1040

2. Термін подання студентом роботи 16.12.2025

3. Вихідні дані до роботи наукові літературні джерела

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1 Аналіз предметної області.
2. Теоретична частина.
3. Практичні аспекти застосування алгоритму Proof of Rank
4. Охорона праці та безпека в надзвичайних ситуаціях

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Тема роботи. 2. Актуальність дослідження. 3. Мета, задачі, об'єкт, предмет дослідження
4. Наукова новизна, практичне значення роботи, апробація. 5. Алгоритм реєстрації транзакції (принцип роботи блокчейна). 6. Основні види консенсусів. 7. Основні види алгоритмів консенсусу. 8. Порівняння алгоритмів Блокчейн. 9. Порівняння додаткових параметрів алгоритмів Блокчейн. 10. Діаграма концепції консенсусу Proof of Rank.
11. Схема роботи алгоритму Proof of Rank. 12. Застосування Proof of Rank у блокчейн-проектах
13, 14. Програмна реалізація алгоритму. 15. Додавання нової ноди в мережу блокчейн.
16. Властивості алгоритму Proof of Rank, отримані експериментальним шляхом .
17. Основні результати дослідження.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Гурик О.Я., доцент каф. МТ		
Безпека в надзвичайних			
ситуаціях	Теслюк В.М., проректор з АГРБ		

7. Дата видачі завдання 17.11.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Затвердження теми кваліфікаційної роботи	27.11.25	Виконано
2	Аналіз літературних джерел	28.11.25–30.11.25	Виконано
3	Обґрунтування актуальності дослідження	01.12.25–03.12.25	Виконано
4	Аналіз предмету дослідження та предметної області	04.12.25–06.12.25	Виконано
5	Проведення дослідження методів та засобів аналітичного опрацювання даних	07.12.25 –08.12.25	Виконано
6	Оформлення розділу «Аналіз предметної області»	09.12.25–10.12.25	Виконано
7	Оформлення розділу «Теоретична частина»	12.12.25–13.12.25	Виконано
8	Оформлення розділу «Практичні аспекти застосування алгоритму Proof of Rank»	13.12.25–14.12.25	Виконано
9	Оформлення розділу «Охорона праці та безпека в надзвичайних ситуаціях»	15.12.25–16.12.25	Виконано
10	Нормоконтроль	15.12.25–17.12.25	Виконано
11	Перевірка на плагіат	15.12.25–17.12.25	Виконано
12	Попередній захист роботи	15.12.25	Виконано
13	Захист кваліфікаційної роботи	23.12.25	

Студент _____ Чорний Я.М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Сверстюк А.С.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дослідження та застосування моделі «Proof of Rank» в технологіях BlockChain // Кваліфікаційна робота освітнього рівня «Магістр» // Чорний Ярослав Миколайлович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем та програмної інженерії, кафедра комп'ютерних наук, група СТм–61 // Тернопіль, 2025 // С. – 74, рис. – 18, табл.– 6, слайдів – 17, додат. – 3, бібліогр. – 40.

Ключові слова: Proof of Rank, блокчейн, валідатор блоку, консенсус, нода, ранжування, транзакція

У рамках дослідження проводився аналіз принципів роботи блокчейн алгоритму Proof of Rank.

У ході дослідження проведено аналіз функціонування алгоритму Proof of Rank, оцінено його переваги та недоліки, вивчено практичні аспекти його впровадження в блокчейн-системах, наведено порівняння з аналогічними алгоритмами консенсусу, а також надано практичні приклади його застосування.

Аналіз проведених досліджень дозволяє оцінити існуючі тенденції у галузі блокчейну, виявити основні принципи та проблеми алгоритмів консенсусу, а також розглянути перспективи розвитку даної технології. Отримані дані послужать основою для подальшого аналізу та досліджень.

Аналіз та дослідження алгоритму Proof of Rank дозволяє глибше зрозуміти його принципи роботи, його місце серед інших алгоритмів консенсусу, а також переваги перед іншими існуючими консенсусами.

ANNOTATION

Research and application the “Proof of Rank” model in Blockchain technologies // Chornyi Iaroslav // Ternopil Ivan Pul'uj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Computer Science, STm-61 group // Ternopil, 2025 // P. - 74, Fig. - 17, Table – 6, Slide - 18, References - 40.

Keywords: Proof of Rank, blockchain, block validator, consensus, node, ranking, transaction

Thesis analyzed the principles of the Proof of Rank blockchain algorithm.

The study analyzed the functioning of the Proof of Rank algorithm, assessed its advantages and disadvantages, studied the practical aspects of its implementation in blockchain systems, compared it with similar consensus algorithms, and provided practical examples of its application.

The analysis of the conducted research allows us to assess existing trends in the blockchain industry, identify the main principles and problems of consensus algorithms, and consider the prospects for the development of this technology. The data obtained will serve as the basis for further analysis and research.

Analysis and research of the Proof of Rank algorithm allows us to better understand its principles of operation, its place among other consensus algorithms, and its advantages over other existing consensuses.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ СКОРОЧЕНЬ І ТЕРМІНІВ

BFT (Byzantine Fault Tolerance) - властивість системи, яка забезпечує її здатність функціонувати надійно, навіть якщо деякі вузли системи працюють некоректно або зловмисно (тобто поводяться «по візантійськи»).

DPoS (Delegated Proof of Stake) – Делегований Доказ Частки, алгоритм консенсусу.

PoA (Proof of Activity) – Доказ Активності, алгоритм консенсусу.

PoR (Proof of Rank) – Доказ Рангу, алгоритм консенсусу.

PoS (Proof of Stake) – Доказ Володіння, алгоритм консенсусу.

PoST (Proof of Space and Time) – Доказ Простору і Часу, алгоритм консенсусу.

PoW (Proof of Work) – Доказ Роботи, алгоритм консенсусу.

PoWeight (Proof of Weight) – Доказ Ваги, алгоритм консенсусу.

БД – база даних.

Валідатори – учасники блокчейну, які вибираються для створення нових блоків та перевірки транзакцій на основі кількості закладених ними монет.

Консенсус (у блокчейні) – механізм, що дозволяє всім учасникам розподіленої мережі (вузлам) досягати спільної згоди щодо стану даних та валідності нових транзакцій, що забезпечує безпеку та надійність системи без центрального органу.

Транзакція (у блокчейні) – це запис про передачу активів (наприклад, криптовалюти) або прав власності між учасниками мережі, який додається до блоку і записується в розподілений реєстр.

ЗМІСТ

ВСТУП

Актуальність теми. У сучасному світі блокчейн-технології стали набирати більшої популярності у користувачів мережі Інтернет завдяки своєму потенціалу трансформувати різні аспекти суспільного та економічного життя. Блокчейн спровокував зміни у фінансових та банківських сферах – додалися нові системи платежів, у логістиці та, в тому числі медицині, завдяки блокчейну покращилася прозорість та надійність даних. Таким чином технологія, що описується, показує свою універсальність і перспективність.

Дослідники та розробники активно працюють над удосконаленням існуючих алгоритмів консенсусів та розробкою нових варіантів підтверджень транзакцій. Основні види робіт спрямовані на підвищення ефективності: скорочення часу верифікації транзакцій; збільшення пропускної спроможності мережі; масштабованість - здатність мережі обслуговувати велику кількість транзакцій; безпека - захист від атак та забезпечення безперервної працездатності мережі.

У роботі досліджуватиметься алгоритм консенсусу, який пропонує унікальну перевагу та можливість для оптимізації блокчейн-мереж. Даному механізму надано назву «Доказ рангу» (PoR). На відміну від класичних алгоритмів, таких як «Доказ роботи (PoW) та «Доказ володіння» (PoS), які використовують обчислювальні чи фінансові ресурси для досягнення консенсусу, PoR пропонує інноваційний механізм, що базується на рейтингу учасників мережі. Цей підхід покликаний підвищити ефективність та безпеку процесу консенсусу, а також зменшити енерговитрати.

Оскільки технологія блокчейн продовжує поширюватися в різних секторах, розуміння та оцінка нових алгоритмів консенсусу, таких як PoR, стають необхідними для підтримки розробки стійких та масштабованих блокчейн-рішень. Актуальність роботи визначається потенціалом використання алгоритму PoR для вирішення ключових проблем, із якими стикаються існуючі механізми консенсусу.

Мета дослідження: програмна реалізація механізму PoR та демонстрація його ефективності шляхом порівняння результатів із альтернативними алгоритмами.

Для досягнення мети, в роботі поставлено та розв'язано **такі задачі:**

- дати визначення поняття консенсусу в блокчейні;
- розкрити роль консенсусу в блокчейні;
- дослідити існуючі алгоритми консенсусу для визначення їх переваг та недоліків;
- зробити порівняння алгоритмів за основними характеристиками;
- розібрати основні принципи роботи алгоритму PoR;
- оцінити переваги та недоліки алгоритму PoR;
- проаналізувати застосування PoR у блокчейн-проектах;
- навести технічні особливості реалізації алгоритму;
- провести порівняння з іншими алгоритмами консенсусу;
- визначити ефективність та безпеку використання алгоритму PoR;
- довести перевагу використання алгоритму PoR.

Об'єкт дослідження: алгоритм PoR.

Предмет дослідження: оцінка ефективності алгоритму PoR порівняно з іншими алгоритмами консенсусу.

Наукова новизна роботи:

- проведено показове порівняння PoR з іншими алгоритмами консенсусу;
- розраховані показники ефективності механізму PoR.

Практичне значення одержаних результатів. Одержані результати розкривають загальні тенденції у розвитку блокчейн-технологій та способи їх оптимізації для підвищення ефективності та безпеки реальних блокчейн операцій (у децентралізованих фінансових послугах, банківських операціях, при електронному голосуванні, логістичні і митні процеси та ін.)

Апробація. Окремі результати роботи були представлені на наукових конференціях як опубліковані тези:

1. Чорний Я.М. Принципи роботи алгоритму Proof of Rank // XIV Міжнародна науково-практична конференція молодих учених та студентів «Актуальні задачі сучасних технологій», Тернопіль, 11-12 Грудня 2025 р. с. 320-372.

2. Чорний Я.М. Застосування алгоритму Proof of Rank у блокчейн-проектах // Інформаційні моделі, системи та технології: Праці XIII наук.-техн. конф. Тернопіль, 17-18 грудня 2025 р. с. 96 -97.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Поняття консенсусу в блокчейні

Перед тим, як давати визначення поняття консенсусу в блокчейні, необхідно описати роботу технології блокчейну. Блокчейн (Blockchain – ланцюжок блоків) – це інноваційна технологія зберігання даних, яка ґрунтується на концепції децентралізованого розподіленого реєстру. На відміну від традиційних централізованих БД, де інформація зберігається на центральному сервері, блокчейн - це низка блоків, де кожен з них володіє інформацією щодо транзакцій чи подій. Тобто, блокчейн є вдосконаленою БД, що дає змогу організувати публічне обмінювання інформацією в рамках мережі. Цифровий реєстр містить збережені дані у блоках, котрі зв’язані між собою в один ланцюжок. Ці дані є хронологічно послідовними, так як не можна видаляти чи вносити зміни в ланцюжок без консенсусу зі сторони мережі [1].

У блокчейні кожна транзакція відображає передачу як фізичних, так і цифрових активів з одного боку в інший. Ці дії вимагають незалежного запису до блоку та подальшої перевірки. Перевірка та запис забезпечуються учасниками мережі, котрі називаються вузлами. Вони обмінюються інформацією за допомогою асиметричної системи шифрування та хешування для забезпечення безпеки та ідентифікації відправників та одержувачів. Коли один із вузлів бажає додати дані в блокчейн, створюється новий блок, який потім додається в ланцюжок завдяки алгоритму консенсусу (перевірки), що діє в мережі. Така система забезпечує надійність та цілісність даних, а також виключає можливість зміни інформації без згоди більшості учасників мережі [2]. Принцип роботи блокчейну та ілюстрація цього процесу представлені на рис. 1.1.

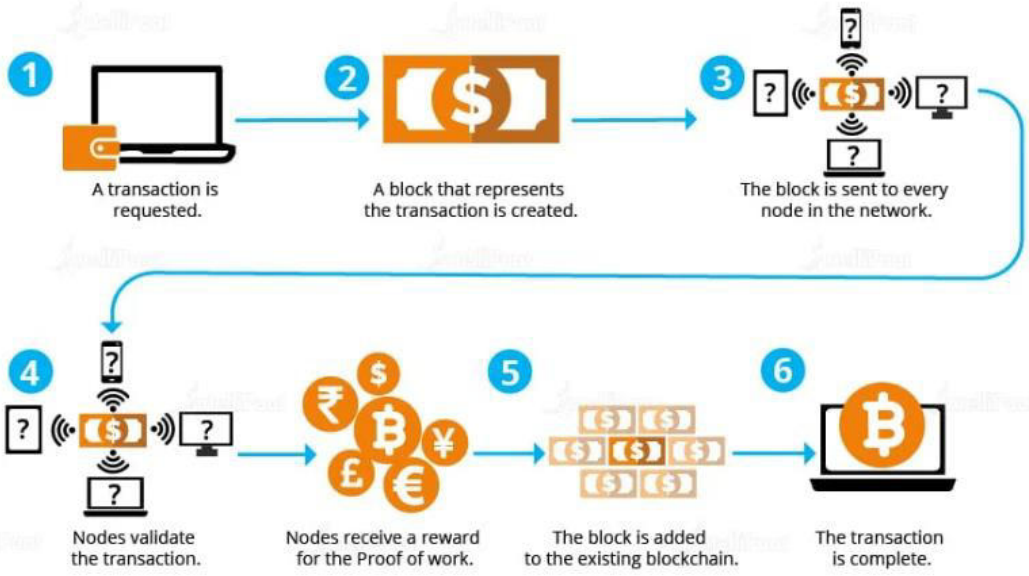

Рисунок 1.1 – Алгоритм реєстрації транзакції (принцип роботи блокчейна)

Перша частина включає реєстрацію транзакції в блокчейні. Блок даних містить інформацію про наступні деталі: учасники угоди, опис події транзакції, час проведення операції, місце здійснення транзакції, причини проведення правочину, обсяг переданих активів, умови правочину.

Друга частина – досягнення консенсусу. Переважна частина учасників розподіленої власне блокчейн-мережі (реєстру) мають погодитися з тим, що записана транзакція є дійсною. Правила узгодження можуть відрізнятися у залежності від типу мережі.

Після досягнення консенсусу транзакції записуються до блоків. Кожному новому блоку надається криптографічний хеш, який зв'язує блоки в ланцюжок. Візуальна послідовність блокчейн ланцюга представлена на рис. 1.2. Якщо вміст блоку змінюється, змінюється також його хеш, що дозволяє виявити підроблені дані. Ланцюжки блоків безперервно пов'язані між собою, і зміна даних у блокчейні неможлива. Кожен новий блок підтверджує цілісність попереднього, забезпечуючи надійність всього ланцюжка.

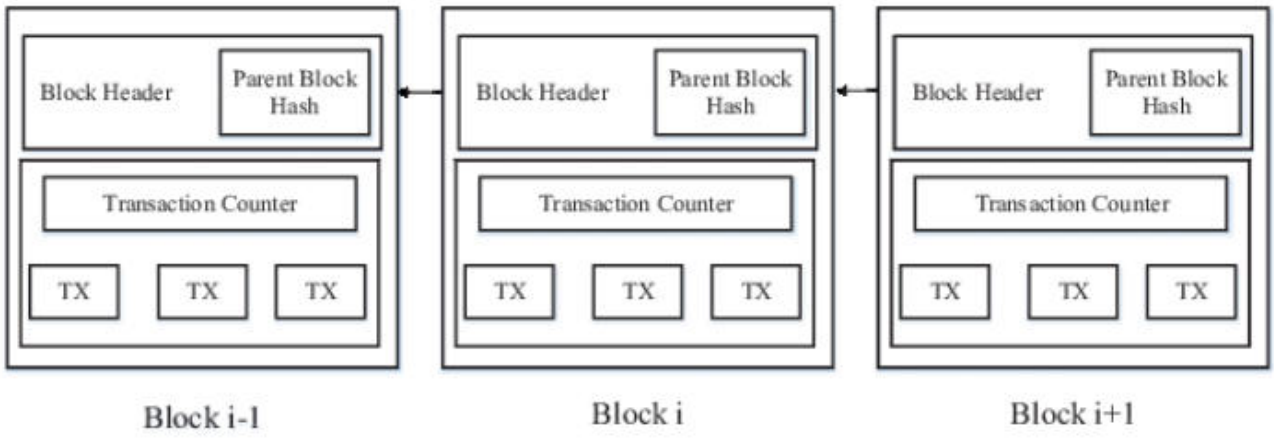

Рисунок 1.2 – Послідовність блоків у Блокчейн мережі

Останнім етапом є надання спільного доступу до реєстру для всіх учасників. Після завершення всіх операцій система поширює фінальну копію центрального реєстру для усіх учасників мережі. Візуальна схема представлена на рис. 1.3.

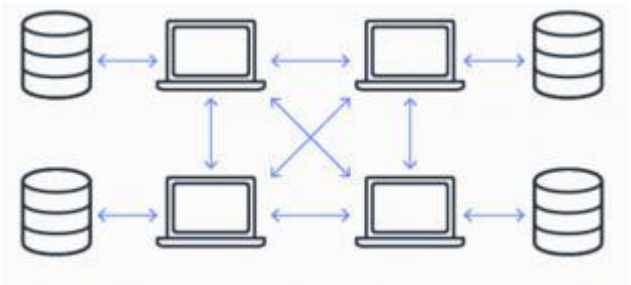

Рисунок 1.3 – Надання загального доступу до реєстру

Таким чином, зв'язок між блоками втілюється шляхом присвоєння кожному блоку певної нумерації, при цьому кожен блок має свою власну властиво хеш-суму і хеш-суму попереднього блоку [3]. Детальна структура блоку представлена на рис. 1.4.

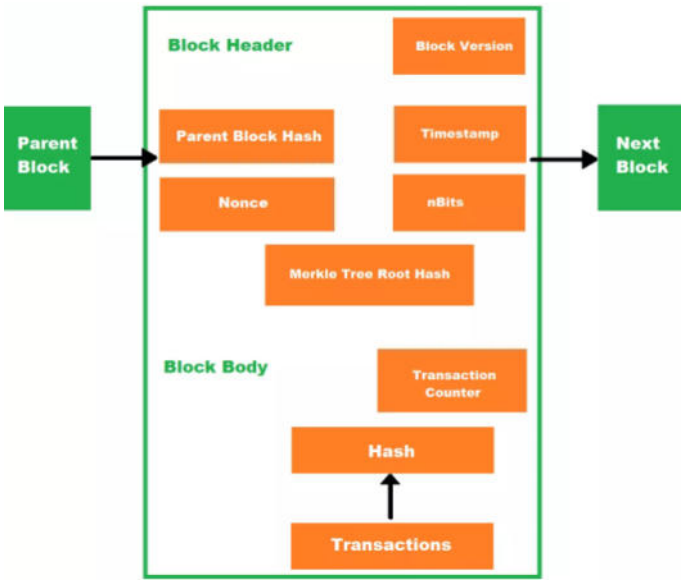

Рисунок 1.4 – Структура блоку у блокчейні

Якщо інформація в блоці змінюється, це призведе до зміни хеш-суми. Правила побудови послідовностей блоків вимагають, щоб зміна хеш-суми записувалася в наступний блок, що тягне за собою зміну його власної хеш-суми. Варто відмітити, що за дотримання цієї умови попередні блоки не будуть змінюватися. На рис. 1.5 показано схему отримання хешу транзакцій [4].

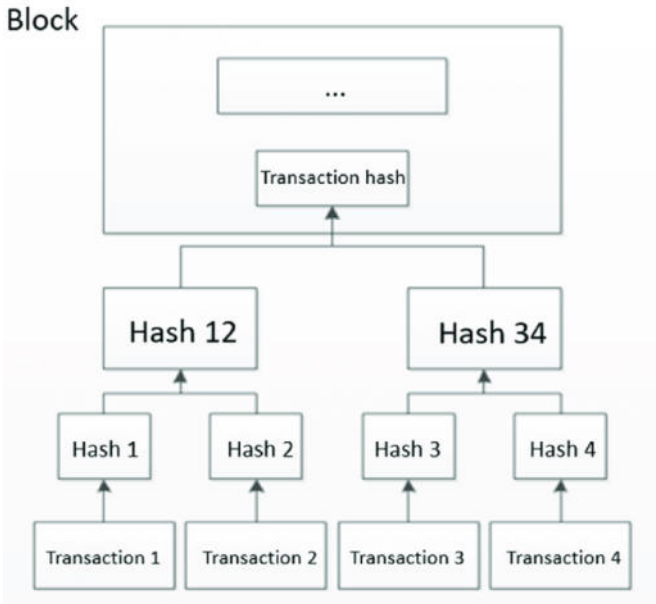

Рисунок 1.5 – Схема отримання хешу транзакцій

Якщо зміни потрібно внести в останній блок ланцюжка, це можна зробити

з невеликими зусиллями, але, якщо блок, який потрібно змінити, має продовження в ланцюжку, це може виявитися складним завданням.

Мережа з клієнт-серверною архітектурою має централізоване управління даними та доступом. Вся логіка системи та інформація зберігаються на сервері, що дозволяє скоротити вимоги до продуктивності клієнтських пристроїв та забезпечити швидку обробку даних. Перевагою такої системи є відкритість даних: відсутня єдина точка відмови, як у разі БД, котра розташована на одному сервері, і висока стійкість до відмови: при припиненні функціонування одного або декількох вузлів працездатність мережі не порушується. Саме тому в наш час блокчейн система знаходить широке застосування у різних галузях: фінансові розрахунки, ідентифікація користувачів чи у кібербезпеці.

Досягнення консенсусу в блокчейні означає досягнення одноголосної згоди між усіма вузлами мережі щодо правильності та послідовності додавання нових блоків. Це забезпечує безпеку та надійність мережі, оскільки зміна або підробка даних у блокчейні потребує зміни даних у всіх блоках ланцюжка, що дуже важко через розподілену та захищену структуру мережі. Саме консенсус є ключовим аспектом блокчейна, що забезпечує його цілісність та надійність.

Механізми консенсусу є методами, які застосовуються для досягнення згоди між учасниками мережі. Саме такі сукупності правил сприяють захисту мережі від шкідливих дій та кібератак [5].

Алгоритм консенсусу є засобом для узгодження змін, котрі вносяться до блокчейну. Його метою є гарантія, що жодні з учасників мережі не мають права довільно додавати, видаляти чи змінювати дані у розподіленому реєстрі [6]. Реалізація алгоритмів консенсусу здійснюється через мережеві програми, які з високою швидкістю проводять перевірку даних на всіх вузлах мережі, досліджують транзакції та узгоджують зміни.

Пристрої блокчейна, а також у контексті алгоритмів консенсусу, відомі як ноди, є обчислювальними пристроями, підключеними до розподіленої мережі, які беруть участь у процесі перевірки транзакцій, а також її обробки. Вони задіяні у виконанні різних функцій: передача блоків даних, зберігання,

автентифікація транзакцій та реалізація смарт-контрактів. Види нод включають повні ноди, які зберігають всю історію транзакцій і можуть проводити нові транзакції, а також легкі ноди, які використовуються тільки для підтвердження перекладів і записують лише заголовки блоків, займаючи менше місця.

Термін «валідатори» відноситься до вузлів, які мають право перевіряти та затверджувати транзакції відповідно до правил алгоритму консенсусу. Цей статус також може бути надано нодам, які перевіряють дані оракулів. Оракули - алгоритми, що надають блокчейну інформацію із зовнішнього світу, наприклад, про поточну вартість валюти. Для запобігання можливим спробам дезінформації, до системи додаються додаткові перевіряючі вузли.

Існує широкий спектр різних механізмів консенсусу, способи їх застосування залежать від типу блокчейна а також від варіантів його використання. Незважаючи на відмінності в алгоритмах: масштабованості, енергоспоживання та безпеки, мета консенсусу єдина – забезпечити надійність та цілісність записів. Більш детальна візуальна інформація про основні види механізмів консенсусу представлена у табл. 1.1, де наведено основні типи консенсусів, що використовуються в блокчейні для досягнення згоди.

В даний час існує безліч варіантів досягнення консенсусу. Історія появи блокчейну та алгоритмів консенсусу включає кілька ключових етапів, починаючи з розвитку криптографії та комп'ютерних технологій.

Ідеї про цифрові гроші вперше з'явилися на початку 1980-х років. Одним із прикладів є робота [7] 1983 року, де запропоновано концепцію цифрової валюти з використанням криптографічних методів [7].

У 2008 році Сатоші Накамото опублікував документ, який описує концепцію криптовалюти Bitcoin та її базовий протокол. Це стало відправною точкою у розвиток технології блокчейн. 3 січня 2009 року було створено перший блок у мережі Bitcoin, відомий як блок Genesis. Ця подія символізує початок реальної експлуатації технології блокчейну. У наступні роки спостерігалося зростання інтересу до блокчейну та розробка різних проектів та застосування цієї технології за межами криптовалют.

Таблиця 1.1 – Основні види консенсусів

Найменування	Опис
Proof Of Work (PoW)	Коли користувач ініціює транзакцію, майнери чи суперкомп'ютери намагаються вирішити проблему чи головоломку, щоб перевірити її
Proof of Stake (PoS)	Користувачеві рекомендується витрачати більше, доки він не стане валідатором для створення блоку
Delegated Proof-of-Stake(DPoS)	Те саме, що і POS, але користувачі з великою кількістю монет можуть голосувати та обирати «Довірителів»
Leased Proof of Stake (LPoS)	Користувачі зможуть створювати власні токени та використовувати їх на своїх фермах для підвищення безпеки
Proof of Elapsed Time (далі PoET)	Аналогічно PoW, але різниця в тому, що він більше фокусується на споживанні
Byzantine Fault Tolerance (BFT)	Система здатна бути надійною, навіть за наявності нечесних, зламаних компонентів
Simplified Byzantine Fault Tolerance (SBFT)	Один валідатор може зв'язати запропоновані транзакції та створювати новий блок
Delegated Byzantine Fault Tolerance (DBFT)	Забезпечує великомасштабну участь у консенсусі через голосування з доручення
Directed Acyclic Graphs (DAG)	Не мають структури даних Блокчейн і можуть обробляти транзакції асинхронно.
Proof of Activity (PoA)	Використовують як PoS, так і PoW, щоб забезпечити своєчасне отримання призових
Proof of Importance (Pol)	Користувач, який часто відправляє та отримує транзакції, отримає за це плату
Proof of Capacity (PoC)	За допомогою цього протоколу можна використовувати ємність або простір жорсткого диска
Proof of Burn (PoB)	Користувачі відправляють монети для спалювання і отримують винагороду в залежності від суми.
Proof of Weight (PoWeight)	Схожий на PoS, але відмінність в тому, що він залежить від інших факторів, які називаються вагами

Разом із розвитком блокчейна стали з'являтися різні алгоритми консенсусу, такі як PoW, PoS, DPoS та інші. Кожен із них пропонує свій підхід

до забезпечення згоди у децентралізованих мережах. З кожним днем кількість алгоритмів консенсусу продовжує зростати, а існуючі алгоритми постійно оновлюються та вдосконалюються. Це відбувається у відповідь на постійний розвиток технологій блокчейн та появу нових вимог та викликів [8]. Нові алгоритми спрямовані на покращення масштабованості, безпеки та ефективності. Таким чином, завдяки динамічному характеру індустрії блокчейн алгоритми консенсусу продовжують розвиватися і з'являтися, демонструючи постійне прагнення до поліпшення та інновацій.

Основні етапи консенсусу включають:

- пропозиція блоків. Учасники мережі пропонують нові блоки, що містять набір транзакцій, які вони хочуть додати у блокчейн;
- перевірка транзакцій. Запропоновані транзакції перевіряються на їх правильність і валідність за допомогою заздалегідь визначених правил та умов, встановлених протоколом блокчейну ;
- вибір лідера чи ініціатора блоку. Залежно від конкретного механізму консенсусу, учасники мережі можуть ставити свої ресурси на кон, щоб бути обраними як ініціатори блоків;
- підтвердження та розповсюдження блоку. Після вибору лідера або ініціатора блоку цей блок підтверджується іншими учасниками мережі та поширюється по всій мережі;
- отримання консенсусу. Учасники мережі порівнюють отримані блоки та погоджуються про найдовший ланцюжок блоків (або ланцюжок з найбільшим обсягом роботи, залежно від застосовуваного механізму). Це дозволяє всім учасникам досягти спільної згоди щодо послідовності блоків;
- додавання блоку в ланцюжок. Як тільки консенсус досягнуто, блок буде додано до ланцюжка блоків, і він стане невід'ємною частиною блокчейна;
- нагородження учасників. У деяких механізмах консенсусу учасники, які вклали ресурси у процес досягнення консенсусу, нагороджуються за свої зусилля. Це може бути виплата нових криптовалютних одиниць чи комісійних зборів за транзакції.

Це загальна схема роботи консенсусу в блокчейні, проте конкретні кроки і деталі можуть відрізнятися залежно від протоколу консенсусу і алгоритму блокчейна, що застосовується.

Алгоритми досягнення консенсусу відіграють ключову роль у забезпеченні повної децентралізації блокчейнів. Завдяки децентралізованій структурі блокчейну відсутній централізований орган, який контролює та оновлює реєстр транзакцій. Натомість зацікавлені сторони в мережі повинні дійти згоди про додавання транзакцій до блокчейну на рівних умовах [9].

Подібний механізм консенсусу в масштабних БД є неможливим без інтелектуальних та складних алгоритмів, здатних автоматично перевіряти нові записи та пов'язувати транзакції з усіма пристроями у мережі [10].

Відсутність відповідного алгоритму консенсусу змусила б децентралізовані системи поступитися місцем централізованим джерелам, які зберігають і обробляють дані в одному місці, роблячи інформацію схильною до кібератаків і спроб втручання з боку осіб, які отримали доступ до цього місця розташування.

1.2 Існуючі алгоритми консенсусу

У світі блокчейну існує множина різних алгоритмів консенсусу, кожен із яких призначений для забезпечення безпеки та надійності децентралізованих систем (рис. 1.6). У сучасних децентралізованих мережах блокчейн консенсус забезпечує узгодженість та надійність даних. Різні протоколи і алгоритми консенсусу були розроблені для вирішення різних проблем, таких як стійкість до атак, енергоефективність, масштабованість та ін.

PoW - це один із перших і найбільш широко застосовуваних алгоритмів консенсусу в блокчейні [11]. Суть його полягає в тому, щоб учасники мережі доводили свою роботу, виконуючи певні обчислювальні завдання, які називають «доказами роботи». Ці завдання, зазвичай, вимагають значних обчислювальних ресурсів та часу для виконання, що робить їх складними для

маніпуляцій чи атак.

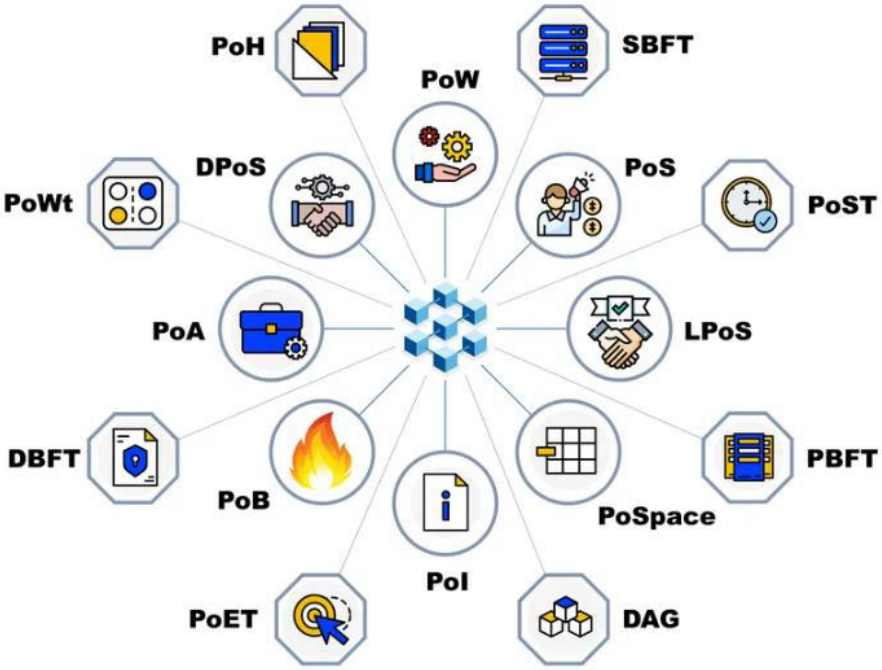

Рисунок 1.6 – Основні види алгоритмів консенсусу

PoW заснований на перетворенні електричної енергії на цифрову «вагу» блокчейна, забезпечуючи неможливість підробки блокчейнів PoW, таких як Bitcoin. Цей процес створює структуру, що забезпечує розподілену мережу стійкістю до збоїв. PoW заснований на математичній задачі, яку необхідно вирішити, щоб отримати значення нижче за певний поріг (nonce), що створює наступний блок, який транслюється в мережу.

Лідери блоків, ті, хто створює наступний блок, вибираються у форматі лотереї пропорційно їх обчислювальним можливостям (тобто хеш-потужності). Простіше кажучи, найдовший ланцюжок має найбільшу кількість роботи і, отже, найбільшу потужність. Цей процес забезпечує захист від атак та забезпечує децентралізацію мережі блокчейн.

У механізмі консенсусу PoW є два основні учасники: майнери та оператори повних вузлів. На мережі біткоїну повні вузли є програмними клієнтами, що запускають програмне забезпечення Bitcoin, яке автоматично перевіряє та поширює транзакції та блоки в мережі. Процес роботи алгоритму PoW представлений на рис. 1.7. Цей механізм консенсусу забезпечує безпеку та

стійкість мережі блокчейн, вимагаючи від учасників виконання складних обчислювальних задач для формування нових блоків і власне підтвердження транзакцій [12].

З використанням криптографічних підтверджень та дотримання правил консенсусу в мережі Біткоїн, оператори повних вузлів є основою мережі та фінальними перевіряючими стани мережі. Повні клієнти вузлів також можуть виконувати функції майнінгу та відкидають неприпустимі блоки та транзакції у мережі. Іншими словами, операторам повних вузлів доводиться ухвалювати рішення, які транзакції вони додадуть (або не додадуть) до блоку.

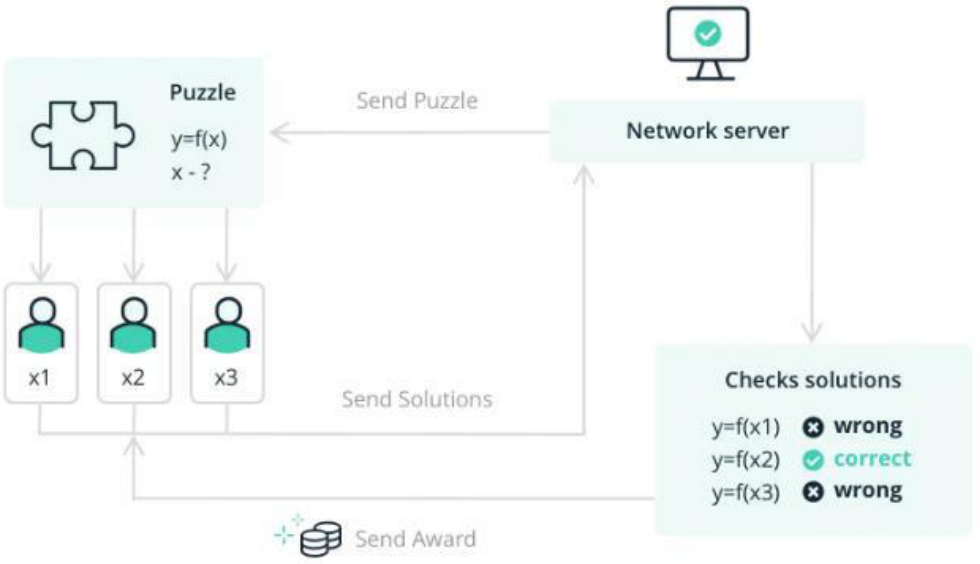

Рисунок 1.7 – Proof of Work

Перевагами алгоритму PoW є: підвищений рівень безпеки завдяки тому, що для атаки на мережу потрібна величезна кількість обчислювальної потужності; децентралізована природа; майнери підтримують роботу мережі, забезпечуючи перевірку транзакцій та створення нових блоків.

Недоліки алгоритму PoW:

- алгоритм вимагає величезних витрат енергії для проведення складних розрахунків, що веде до негативного впливу на довкілля та витрат на електроенергію;
- можливість централізації майнінгу до рук великих майнінгових

пулів, що загрожує децентралізації мережі;

- потрібне дороге спеціалізоване обладнання для ефективного майнінгу, що створює бар'єри для входження нових учасників;
- обмеження в масштабуванні через обмежену пропускну спроможність мережі та збільшення складності майнінгу зі зростанням числа учасників.

Другим найвідомішим алгоритмом консенсусу є PoS - це механізм консенсусу в блокчейні, який ґрунтується на володінні криптовалютою. На відміну від PoW, де майнери застосовують обчислювальну потужність для формування нових блоків і отримання нагород, у «Доказі частки» ймовірність створення блоку та одержання винагороди перебуває у залежності від кількості і тривалості володіння криптовалютою. Цей підхід покликаний знизити енерговитрати, пов'язані з майнінгом, та забезпечити більш рівномірний розподіл влади у мережі. Власники криптовалюти, або «стейкери», беруть участь у процесі консенсусу, голосуючи за наступний блок на основі їхньої частки в мережі. Це сприяє безпеці мережі, оскільки атакуючим буде складніше підконтролювати більшу частину стейкінгу [11].

Для того, щоб стати валідатором на блокчейні з доказом частки, необхідно «стейкати» певну кількість відповідної монети. Наприклад, валідатори мережі ETH повинні застейкати 32 ETH для валідації транзакцій. Ця частка діє як запорука, гарантуючи, що валідатор діє чесно. Зазвичай, що більша частка валідатора, то більш довірчим він для системи і вищий шанс створити наступний блок [12]. Запропоновані блоки валідаторами потім поширюються по іншій множині, яка перевіряє і додає схвалений блок блокчейн.

PoS містить такі основні компоненти:

- стейкінг. Учасники мережі повинні закласти (застейкати) свої монети як гарантію своєї участі та чесної поведінки;
- вибір валідаторів. Зазвичай вибір валідаторів здійснюється випадковим чином чи основі кількості монет, закладених кожним учасником;
- створення блоків та перевірка транзакцій. Валідатори створюють

нові блоки, включаючи в них перевірені транзакції, і додають їх у блокчейн;

- нагороди та штрафи: валідатори отримують нагороди у вигляді комісій за створення блоків та перевірку транзакцій. Однак вони також можуть бути штрафовані за неправильну поведінку, таку як спроби шахрайства або невиконання своїх обов'язків ;
- фіналізація блоків. Після того, як блок створений та перевірений, він фіналізується та додається до ланцюжка блоків без можливості зміни.

Це основні компоненти механізму PoS, який забезпечує безпеку та надійність блокчейн-мережі за рахунок участі її учасників та їхньої зацікавленості у підтримці цілісності мережі.

Перевагами PoS є енергоефективність, оскільки алгоритм не вимагає великих обчислювальних ресурсів, масштабованість, оскільки не потребує важких обчислень.

Недоліки PoS:

- нерівномірний розподіл багатства. Потребує вкладення монет, що може створити бар'єр нових учасників і посилити нерівність ;
- проблеми безпеки. Можливі атаки, які можуть порушити цілісність мережі ;
- відсутність убудованого механізму доказу роботи алгоритму [13]. Не вимагає виконання фактичної роботи для створення нових блоків, в чому деякі критики бачать як загрозу безпеці та децентралізації.

Ще одним із найвідоміших алгоритмів консенсусу є DPoS. Він заснований на механізмі PoS, але є більш продуктивною його версією. DPoS – механізм, при якому учасники обирають делегатів для перевірки транзакцій та створення нових блоків [12]. Учасники мережі голосують за делегатів на основі їхньої репутації та ефективності. Відображення роботи алгоритму представлено рис. 1.8.

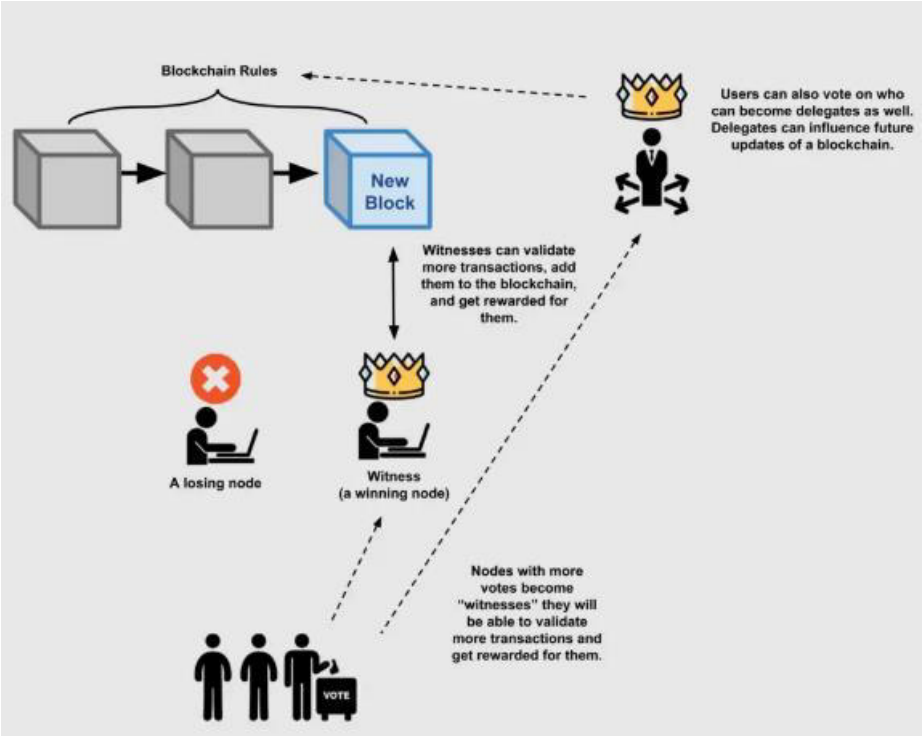

Рисунок 1.8 – DPoS

Основні компоненти алгоритму DPoS включають [14]:

- свідки. Це учасники, обрані спільнотою для перевірки та створення нових блоків у блокчейні. Делегати одержують цю роль на основі голосування інших учасників мережі ;
- стейкери. Це учасники мережі, які мають криптовалютні монети, і вони використовують їх для голосування за делегатів. Чим більше монет у стейкера, тим більше ваги його голосу ;
- голосування. Стейкери голосують за делегатів, яких хочуть бачити в ролі свідків блокчейну. Голоси стейкерів враховуються під час виборів делегатів ;
- створення блоків. Вибрані делегати мають право створювати нові блоки у блокчейні. Вони перевіряють транзакції і додають в блоки, який потім додаються в ланцюжок .

DPoS забезпечує швидкий консенсус і більш високу масштабованість, оскільки обмежує кількість необхідних делегатів, ефективно використовує ресурси завдяки меншій кількості учасників, які беруть участь у підтвердженні транзакцій, забезпечує демократичний процес вибору делегатів, що сприяє

чесності та прозорості системи [15].

Однак цей алгоритм також має свої недоліки, такі як ризик недостатньої децентралізації через обмежену кількість делегатів, необхідність активної участі учасників у голосуванні за делегатів, щоб забезпечити стабільну роботу мережі, можливість атаки 51%, особливо в мережах з невеликою кількістю делегатів, що може підірвати безпеку блокчейна [16].

Далі розглянемо PoA – це гібридний алгоритм консенсусу, що поєднує принципи PoW та PoS, що працюють на основі циклів.

На початку кожного циклу PoW майнери конкурують за створення нових блоків, використовуючи PoW для підтвердження транзакцій та генерації блоків. Після того, як PoW цикл завершується, настає фаза PoS, де учасники, у яких є монети в мережі, можуть ставити їх у заставу для участі у голосуванні та підтвердженні блоків.

PoA забезпечує баланс між безпекою та ефективністю завдяки використанню PoW та PoS. Цей алгоритм дозволяє знизити енерговитрати, характерні для PoW, та забезпечити більшу децентралізацію, як у PoS. Однак він також може зіткнутися з проблемою атаки 51% і вимагає участі власників монет у мережі для забезпечення безпеки та голосування.

Ще одним поширеним алгоритмом мережі блокчейн є PoST. Механізм PoST заснований на ідеї використання фізичного простору та часу для створення та підтвердження нових блоків у блокчейні. У цьому алгоритмі учасники доводять, що вони виділили та використовують певну кількість вільного місця на своєму пристрої (простір) та утримують цю інформацію протягом певного періоду часу (час).

Процес роботи алгоритму включає реєстрацію учасників, генерацію унікальних доказів, перевірку простору і часу, а також створення і підтвердження нових блоків. Користувачі, які можуть надати більший обсяг простору та часу, мають більший шанс на створення нових блоків та отримання винагороди.

Основні компоненти алгоритму PoST включають [17]:

- простір. Учасники доводять, що вони виділили певну кількість вільного місця на своєму пристрої для зберігання даних блокчейну;
- час. Учасники також доводять, що вони утримують цю інформацію протягом певного періоду часу. Це підтверджує їхню постійну участь у мережі та захищає її від різних атак;
- реєстрація. Учасники реєструються в мережі та генерують унікальні докази свого простору та часу;
- верифікація. Мережа перевіряє, що учасники дійсно виділили вказаний простір та утримують його протягом заданого періоду часу;
- створення блоків. Учасники, які успішно пройшли перевірку, можуть мати право на створення нових блоків у блокчейні.

Ці компоненти працюють разом для забезпечення безпеки та ефективності алгоритму PoST у блокчейн-мережі.

Алгоритм PoST має низку переваг, таких як економічна ефективність та децентралізованіша мережа за рахунок ефективного використання ресурсів. Однак його впровадження може бути складним через вимогу розробки нової інфраструктури, а також існує ризик можливих атак 51% та низької швидкості транзакцій через тимчасові затримки на перевірку [18].

Алгоритм PoWeight - це форма консенсусу, де право голосу чи вага у системі залежить від деякого параметра, зазвичай пов'язаного з фінансовими чи репутаційними показниками учасників мережі. У PoWeight учасники мережі можуть отримати вагу або право голосу в залежності від кількості монет, якими вони володіють, часу, проведеного у мережі, або інших критеріїв [19]. Чим більша вага в учасника, тим більше його вплив на процес прийняття рішень у мережі.

Основна ідея PoWeight – зробити процес консенсусу більш справедливим та демократичним, даючи учасникам мережі можливість впливати на прийняття рішень відповідно до їхнього внеску до мережі. Основні компоненти алгоритму консенсусу Proof of Weight включають:

- ваговий коефіцієнт. Учасники мережі отримують ваговий коефіцієнт

залежно від певних параметрів: кількість монет у гаманці користувача, термін їх зберігання, обсяг даних, що зберігаються, або унікальна змінна;

- право голосу. Ваговий коефіцієнт визначає право учасника голосувати або впливати на прийняття рішень у мережі. Чим більша вага, тим більший вплив учасника на консенсус;
- процес голосування. Учасники можуть використовувати свій ваговий коефіцієнт для участі у процесі голосування щодо прийняття рішень у мережі;
- розрахунок ваги. Система повинна мати механізм розрахунку вагового коефіцієнта учасників, який може бути заснований на наборі заздалегідь визначених правил або параметрів.

Ці компоненти в сукупності забезпечують роботу консенсусу PoWeight, дозволяючи учасникам мережі робити свій внесок у прийняття рішень та забезпечувати стабільність та безпеку мережі.

Переваги алгоритму консенсусу PoWeight:

- демократичність. Учасники мережі отримують можливість впливати на прийняття рішень відповідно до їхнього внеску до мережі, що сприяє більш справедливому розподілу влади;
- ефективність. Оскільки ваговий коефіцієнт може бути пов'язаний з різними параметрами, такими як кількість монет або час у мережі, алгоритм може бути більш ефективним та економічним порівняно з іншими методами консенсусу;
- менше споживання енергії. PoWeight може бути менш енергоємним, що сприяє екологічній стійкості.

Недоліками алгоритму є такі умови, якщо невелика кількість учасників з великою вагою почне домінувати в прийнятті рішень, це може призвести до централізації в мережі. Якщо вибір критеріїв для визначення вагового коефіцієнта учасників може бути складним і схильним до маніпуляцій, тоді це може мати негативний вплив на безпеку та стабільності мережі. Також потрібна необхідність створення механізму розрахунку вагового коефіцієнта та захисту від маніпуляцій робить алгоритм PoWeight більш складним у реалізації та

підтримці.

1.3 Висновки до першого розділу

Консенсус у блокчейні відіграє ключову роль у забезпеченні узгодженості та надійності даних у децентралізованих мережах. Загальна схема роботи консенсусу включає етапи пропозиції, валідації та прийняття блоків, а також додавання їх у ланцюжок блоків. Важливо, щоб консенсус забезпечував безпеку та надійність мережі, а також враховував вимоги до ефективності та масштабованості блокчейну.

Кожен з розглянутих алгоритмів (PoW, PoS, DPoS, PoA, Po Weight) має свої переваги та недоліки, а також різні способи визначення та підтвердження правильності транзакцій у мережі. PoW є одним із найпоширеніших і початкових алгоритмів, але він стикається з проблемами енергоспоживання та масштабованості. PoS та його варіанти, такі як DPoS, прагнуть вирішити ці проблеми, але можуть зіткнутися з проблемою централізації [20]. PoA та Po Weight пропонують нові підходи до консенсусу, враховуючи різні параметри та вагові коефіцієнти учасників мережі.

Вибір алгоритму консенсусу залежить від цілей проекту та прагнення забезпечити баланс між децентралізацією, масштабованістю та безпекою мережі. При виборі враховуються такі фактори, як безпека, децентралізація, масштабованість, екологічна стійкість, продуктивність та гнучкість для розвитку. Команди розробників повинні старанно брати до уваги усі переваги, а також й недоліки кожного алгоритму консенсусу, щоб вибрати найбільш підходящий для свого проекту.

2 ТЕОРЕТИЧНА ЧАСТИНА

2.1 Ландшафт консенсусів: аналіз та порівняння

Для алгоритмів досягнення консенсусу існують чотири основні категорії характеристик: структурні, пов'язані з безпекою, із продуктивністю, ті що належать до винагород. Структурні характеристики визначають організацію вузлів у мережі та його ролі у процесі консенсусу. Методи організації вузлів включають формування комітетів, їх структуру та правила для включення вузлів. Комітети можуть бути статичними або динамічними, а їх склад може визначатись голосуванням або лотереєю. Ці характеристики формують дерево структурних властивостей алгоритмів, що дозволяє краще зрозуміти їхню організацію та функціонування. Ієрархічне дерево властивостей представлене на рис. 2.1.

Рисунок 2.1 – Структурні властивості алгоритмів консенсусу

Характеристики блоку та винагороди відіграють ключову роль у роботі різних криптовалютних алгоритмів. Вони визначають різні параметри, такі як загальна кількість доступної криптовалюти, винагорода за формування блоку та середній час створення нового блоку. Ці аспекти безпосередньо чи опосередковано впливають на процес досягнення консенсусу в блокчейн-

мережі. Наприклад, майнери мотивуються винагородою за створення нового блоку, що стимулює їх участь у криптографічному процесі, необхідному для досягнення згоди у мережі [21]. Структура винагород та властивості блоку наведені на рис. 2.2.

Рисунок 2.2 – Структура винагород та властивості блоку

Далі розглянемо характеристики ефективності. Ця група властивостей використовується з метою оцінки кількісних параметрів алгоритмів консенсусу. Сюди включаються наступні аспекти: максимальна допустима кількість недоступних вузлів в алгоритмі, кількість транзакцій, що обробляються алгоритмом за певний час, можливість масштабування мережі та функціональності без погіршення продуктивності, час, необхідний для узгодження транзакцій та включення блоку в ланцюжок, а також енергоспоживання алгоритму [21]. Ці показники продуктивності зображені на діаграмі на рис. 2.3.

Рисунок 2.3 – Структура характеристики ефективності

На завершення представимо властивості забезпечення безпеки. Цей сегмент включає такі характеристики, як наявність/відсутність обов'язкової аутентифікації вузлів, які беруть активну участь у процесі досягнення консенсусу. Алгоритми також аналізуються з погляду захищеності від різних видів атак. Властивості забезпечення безпеки механізмів консенсусу представлені на діаграмі рис. 2.4.

Рисунок 2.4 – Структура забезпечення безпеки

Почнемо порівняння найвідоміших та основних алгоритмів PoW та PoS. Це два фундаментальні алгоритми консенсусу, які використовуються в

блокчейн мережах для забезпечення узгодженості та безпеки транзакцій. Обидва ці алгоритми мають свої особливості, переваги та недоліки [22].

Алгоритм консенсусу PoW був вперше введений разом з появою Біткоїна. Його головною метою було забезпечення формування нових блоків і дотримання мережевої безпеки. У початкові періоди PoW успішно функціонував, проте його недоліки стали очевидними зі збільшенням популярності криптовалюти.

При алгоритмі PoW учасники мережі, які називають майнерами, конкурують за право сформувати новий блок у блокчейні, розв'яжуючи складні математичні завдання. Майнер, який першим вирішить завдання та додасть блок, одержує у винагороду криптовалюту. Цей процес вимагає значних обчислювальних потужностей та енергії [23].

В алгоритмі PoS замість майнерів використовуються «стейкери», які підтверджують транзакції та створюють нові блоки, виходячи з кількості криптовалюти, яку вони володіють і заморозили в мережі. Чим більше монет у стейкера, тим більша ймовірність, що його буде обрано для створення блоку. Тут немає потреби у значних обчислювальних ресурсах, але стейкери можуть зіткнутися з проблемою централізації, оскільки багатші учасники з великою кількістю монет мають більше впливу.

Однією з головних переваг PoW є його високий рівень безпеки через власне розподілену природу майнінгу. Однак він вимагає великих витрат на енергію та обладнання, що зменшує його екологічну ефективність. Водночас, PoS більш екологічний та економічно ефективний, але може бути менш безпечним через проблему централізації та потенційну вразливість для атаки.

Крім того, PoS може забезпечити більш високу швидкість транзакцій та масштабованість завдяки відсутності необхідності вирішувати складні обчислювальні завдання. Це може бути особливо важливо у мережах із високою завантаженістю та великим обсягом транзакцій.

Порівняння алгоритмів представлено на рис. 2.5. Обидва алгоритми мають унікальні характеристики і переваги, і вибір, власне, між PoW і PoS перебуває у

прямій залежності від визначених цілей проекту, його стадії розвитку та філософії команди розробників [24].

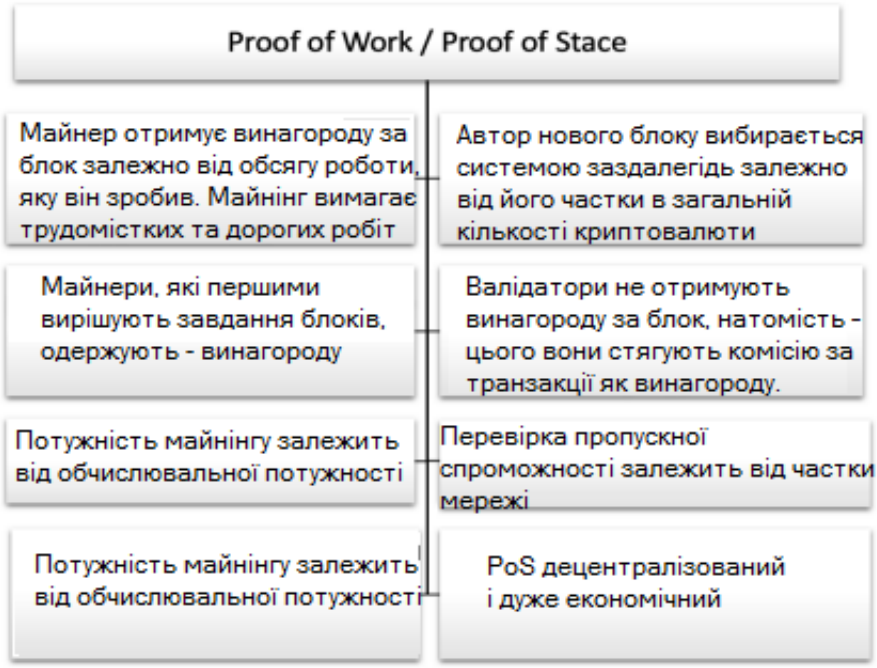

Рисунок 2.5 – Порівняння алгоритмів PoW та PoS

PoA поєднує у собі елементи PoW та PoS. У PoA майнери спочатку доводять свою активність у PoW, а потім доводять володіння монетами у PoS.

PoA, поєднуючи обидва підходи, прагне балансу між безпекою та енергоефективністю, використовуючи PoW для перевірки активності та PoS для розподілу права на створення блоків. Цей алгоритм є гібридом PoW та PoS, поєднуючи переваги обох.

У цьому алгоритмі відбувається балансування безпеки та енергоефективності: PoA використовує PoW для забезпечення безпеки та PoS для створення блоків, що дозволяє знизити енергоспоживання порівняно з чистим PoW. Також знижується ймовірність атак 51%. В алгоритм PoA є складність реалізації, оскільки потрібно більш складний механізм, ніж у простих алгоритмів, що може вимагати більше часу на розробку та тестування.

Вибір між цими алгоритмами залежить від конкретних цілей проекту та важливості для нього певних характеристик, таких як безпека, ефективність та

децентралізація.

При порівнянні наступного алгоритму DPoS спиратимемося на попередні моделі консенсусів. Механізм DPoS демонструє високий рівень захисту та можливість масштабування, забезпечуючи більш високу пропускну спроможність транзакцій за секунду порівняно з PoS. Архітектура DPoS включає множину елементів, які ефективно підтверджують транзакції та керують блокчейном [25]. Цей механізм демонструє більш високу ефективність у порівнянні з PoS або PoW, хоча вони використовуються набагато ширше ніж DPoS.

PoS - це альтернатива механізму PoW, що найбільш часто використовується , так як вона створювалася для подолання багатьох його недоліків. PoS розробляє вирішення проблем, пов'язаних із витратами на майнінг, та збільшенням швидкості додавання нових блоків у ланцюг, що веде до більш швидкої обробки транзакцій. Замість використання електричної та обчислювальної потужності для майнінгу, валідатори купують монети та беруть участь у процесі стейкінгу.

Алгоритм PoS має свої недоліки, включаючи потенційну централізацію процесу перевірки транзакцій через більший вплив учасників із найбільшою кількістю монет. Для усунення цієї проблеми і було створено алгоритм DPoS, де відповідальність за перевірку транзакцій передається обраним делегатам, забезпечуючи тим самим більш високу швидкість транзакцій та пропускну спроможність мережі. Візуальне порівняння механізмів консенсусу PoS та DPoS на рис. 2.6 ілюструє відмінності у їх підходах до забезпечення безпеки та децентралізації мережі.

DPoS - це механізм узгодження, що ґрунтується на виборі довірених вузлів, за які голосують учасники мережі. Незважаючи на численні переваги мереж, що використовують DPoS, немає певної відповіді на питання, який механізм консенсусу є найкращим. DPoS перевершує своїх попередників (PoW, PoS) у багатьох аспектах, проте він також має деякі недоліки.

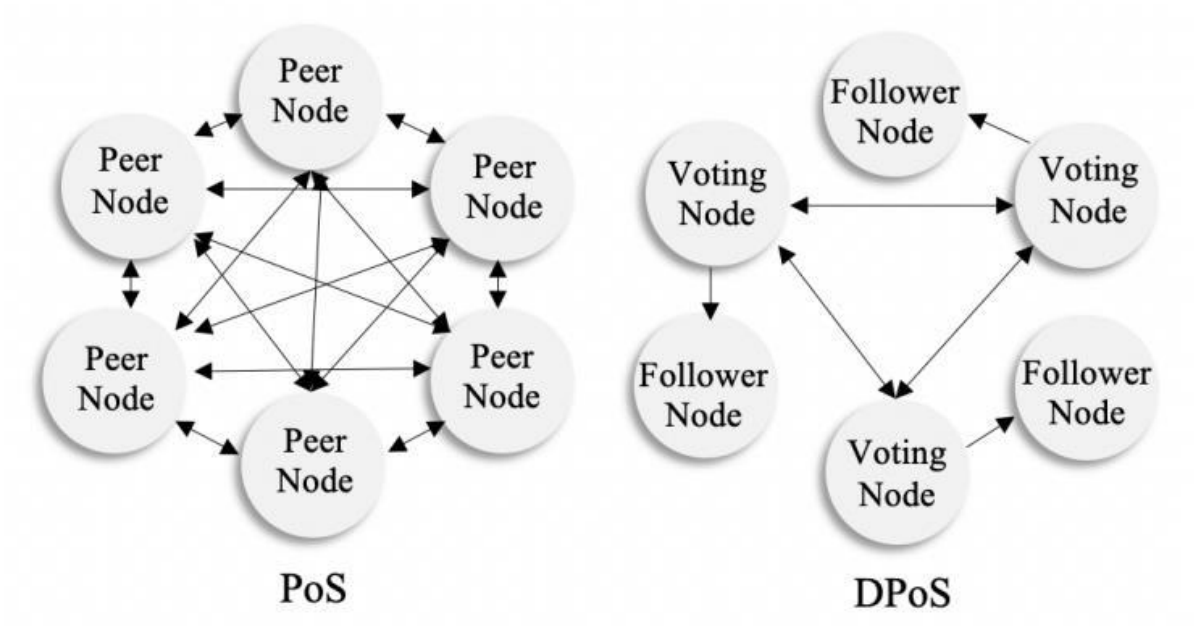

Рисунок 2.6 – Порівняння механізмів PoS та DPoS

Алгоритм PoWeight є новим механізм консенсусу, який також як і DPoS поєднує елементи PoS та інші інновації для забезпечення безпеки та ефективності блокчейн-мережі [26].

PoWeight, на відміну від PoW, який вимагає значних енерговитрат на майнінг, забезпечує більш ефективне використання ресурсів, оскільки він заснований на частці володіння активів у мережі, а не на обчислювальній потужності. PoWeight має більш високу ступінь децентралізації, оскільки власники активів можуть брати участь у процесі голосування та прийняття рішень, тоді як у PoW майнінг часто контролюється великими майнерськими пулами.

PoWeight може запропонувати складніші механізми стимулювання та мотивації учасників мережі завдяки вазі їх активів. Може бути стійкішим до атак 51% порівняно з деякими варіантами PoS, оскільки учасники мережі можуть мати більш значне фінансове вкладення системи. Також на відміну від DPoS, де делегати обираються голосуванням, PoWeight може ґрунтуватися на складніших алгоритмах визначення ваги активів та управління ними, що може забезпечити більш справедливу та ефективну систему управління мережею. Proof of Weight може запропонувати ширший спектр можливостей для розвитку

економічної моделі та механізмів стимулювання, оскільки вага активів може бути пов'язана з різними параметрами та діями в мережі.

Загалом, PoWeight є інноваційним підходом до механізму консенсусу, який поєднує кращі аспекти інших алгоритмів, таких як PoW, PoS та DPoS, з метою забезпечення більш ефективної, безпечної та стійкої блокчейн-мережі.

Перейдемо до порівняння показників продуктивності алгоритму. Результати випробувань, включаючи якісні характеристики та ключові показники, представлені у Додатку Б. Також для детальнішого аналізу представимо порівняння алгоритмів за такими характеристиками: тип блокчейн мережі, продуктивність, розроблені дозволи. У роботі подано загальний порівняльний аналіз протоколів консенсусу (табл 2.1).

Таблиця 2.1 – Порівняння алгоритмів Блокчейн

Протокол консенсусу	**Тип блокчейн мережі**	**Продуктивність**	**Розроблені рішення**
PoW	Відкрита	Низька	Bitcoin-NG, Byzcoin, Bitcoin
PoS	Відкрита	Висока	Tendermint, Ethereum
DPoS	Відкрита	Висока	EOS, BitShares
PoA	Відкрита	Середня	Decred, Enecuum
PoWeight	Відкрита	Висока	Filecoin

Порівняння алгоритмів консенсусу за додатковими параметрами, таким як використання простору на жорсткому диску, вимога спеціального обладнання, обмеженість обчислювальних ресурсів за часом, витрачання великої кількості часу, висока стійкість до атак, висока обчислювальна потужність, перевага між великою кількістю валюти в гаманці, та можливість фіктивних транзакцій наведено у табл. 2.2.

Таблиця 2.2 – Порівняння додаткових параметрів алгоритмів Блокчейн

Параметр	PoW	PoS	DPoS	PoA	PoWeight
Використання простору на жорсткому диску	Так	Ні	Ні	Ні	Ні
Потрібне спеціальне обладнання	Так	Ні	Ні	Так	Так
Обчислювальні ресурси обмежені за часом	Так	Ні	Ні	Ні	Ні
Витрачання великої кількості часу	Так	Ні	Ні	Так	Так
Висока стійкість до атак	Так	Так	Так	Так	Так
Висока обчислювальна потужність	Так	Ні	Ні	Так	Так
Перевага між великою кількістю валюти у гаманці	Ні	Так	Так	Ні	Так
Можливість фіктивних транзакцій	Ні	Ні	Ні	Ні	Ні

Таким чином, різні алгоритми мають різну продуктивність, виражену через швидкість обробки транзакцій, ефективне використання ресурсів і масштабованість. Деякі алгоритми, такі як DPoS та PoA, можуть забезпечити більш високу продуктивність та масштабованість у порівнянні з PoW.

Питання безпеки також різняться залежно від алгоритму. Наприклад, PoW забезпечує високу стійкість до атак за рахунок високої обчислювальної потужності, в той час як алгоритми PoS та DPoS зазвичай вимагають менше ресурсів, але можуть бути менш стійкими до різних атак.

Деякі алгоритми, такі як PoW, прагнуть більш децентралізованої природи, тоді як інші, наприклад DPoS, можуть бути більш централізованими через меншу кількість учасників, що приймають рішення.

Деякі алгоритми, такі як PoA і PoWeight, мають більшу гнучкість і ефективність у вирішенні певних завдань завдяки своїм особливостям.

Отже, вибір конкретного алгоритму консенсусу залежить від конкретних потреб та вимог мережі, в.т.ч. швидкість обробки транзакцій, безпеку, ступінь децентралізації та масштабованість. Кожен алгоритм має свої сильні та слабкі сторони, і вибір має ґрунтуватися на компромісі між цими факторами [27].

2.2 Proof of Rank як алгоритм консенсусу

2.2.1 Введення до алгоритму

У цій кваліфікаційній роботі алгоритм PoR пропонуватиметься і розглядатиметься як ефективніша альтернатива представленим алгоритмам у першому розділі, оскільки він націлений на обробку значно більшої кількості транзакцій на секунду, порівняно з іншими існуючими механізмами. PoR - це алгоритм консенсусу, заснований на рангах, який буде ефективним рішенням для блокчейнів. У PoR валідатори блоків не створюють стейки монет, а натомість мають власний ранг, тому алгоритм застосовує значення ідентифікаторів. Таким чином блокчейни, що використовують PoR, будуть захищені перевіреними вузлами, які вибираються випадковим чином на основі довіри.

Алгоритм PoR не вимагає виконання складних завдань для підтримки зв'язку між вузлами, відповідно валідаторам не потрібне особливе обладнання для підтримки мережі. Модель PoR обмежується певною кількістю валідаторів блоків, що сприяє масштабованості системи. Перевірка блоків та транзакцій заздалегідь здійснюється затвердженими вузлами, які виступають у ролі модераторів системи (якісні, середні та нижчі ранги). Перевірка та підтвердження блоків проводиться вищим рангом. Цей механізм забезпечує конфіденційність за рахунок використання переваг технології блокчейн.

Роблячи висновок із вищеописаної інформації. PoR - це алгоритм консенсусу, який ґрунтується на принципі ранжування вузлів у мережі. Ось основні засади роботи цього алгоритму:

- кожен вузол у мережі має свій ранг, що визначається на основі різних факторів, таких як історія участі в мережі, кількість ресурсів, час;
- вузли з більш високим рангом (вищий ранг) мають більшу вагу при формуванні нових блоків і підтвердження транзакцій. Це означає, що більш довірені вузли грають активнішу роль роботі мережі;

- прагне справедливого розподілу прав та обов'язків між учасниками мережі, що сприяє децентралізації системи.
- оскільки ранг вузлів заснований на їх довіреності та значущості, атаки на систему, спрямовані на зміну блокчейну або маніпуляцію даними, стають більш складними та утрудненими;
- вузли, що беруть участь в алгоритмі PoR, можуть отримувати винагороду за свою активну роботу в мережі. Це сприяє мотивації учасників підтримувати свій ранг та вкладати більше ресурсів у мережу;
- може бути більш ефективним і масштабованим порівняно з деякими іншими алгоритмами консенсусу, оскільки він оптимізує використання ресурсів та управління участю вузлів у мережі.

Алгоритм PoR забезпечує справедливість, безпеку та ефективність роботи мережі завдяки використанню ранжування вузлів та обліку їхньої довіреності та активності.

Таким чином, ключовими деталями залежності узгодженого алгоритму PoR є:

- діючі і заслуговують на довіру вузли, тобто. валідатори, які мають ідентифікувати себе;
- стандарт затвердження валідатора. Метод вибору валідаторів має бути однаковим до всіх кандидатів.

Основна мета описаного механізму полягатиме у встановленні довіри до особи валідатора. Процес повинен виключати з гри несумлінних учасників. Таким чином, кожен валідатор піддається однорідним процедурам, які забезпечують цілісність та надійність системи. Цей механізм спрямований на підтримку довіри та безпеки в мережі, забезпечуючи видалення невідповідних гравців та гарантуючи дотримання встановлених стандартів.

Таким чином, алгоритм PoR буде інноваційним механізмом консенсусу, який відрізняється від традиційних підходів, таких як PoW або PoS. На відміну від PoW, який вимагає значних обчислювальних ресурсів, та PoS, який наголошує на кількості застейканих монет, PoR буде ґрунтуватися на ранг

учасників у мережі.

В рамках алгоритму PoR валідатори блоків не створюють стейки монет або вирішують складні задачі. Натомість, їх вибір заснований на їх ранзі в мережі. Це дозволяє скоротити енерговитрати, необхідні для підтримки мережі, та забезпечує більш ефективну та екологічно чисту систему.

Також однією з ключових особливостей PoR буде обмеження кількості валідаторів блоків (вищий ранг). Це забезпечує масштабованість системи, оскільки фіксована кількість учасників управляє перевіркою блоків та транзакцій. Завдяки цьому підходу система зберігатиме високу продуктивність і надійність навіть за збільшення кількості учасників.

Крім того, PoR сприятиме підвищенню конфіденційності, надаючи компаніям можливість використовувати переваги блокчейн-технології для забезпечення безпеки та надійності своїх даних. PoR можна буде застосовувати в блокчейн-мережах, де потрібен ефективний механізм вибору учасників, заснований на їх ранзі, наприклад, системах управління цифровими активами або в платформах для спільної роботи.

Таким чином, алгоритм Proof of Rank буде інноваційним підходом до забезпечення консенсусу в блокчейн-мережах, який в рамках проекту націлений об'єднати в собі високу продуктивність, економічність і безпеку, роблячи його привабливим вибором для різних додатків і галузей.

2.2.2 Принципи роботи алгоритму

В алгоритмі PoR блоки згруповані в слоти, що становлять множини груп. На кожному етапі або раунді генератори блоків вибираються на початку. Блокчейн PoR підтримує певну кількість валідаторів, які мають право генерувати блоки (вони називаються найвищими валідаторами). Кожному валідатору, що має найвищий ранг, призначається один блоковий слот, в якому блоки формуються. Тривалість раунду визначається кількістю діючих валідаторів, що беруть участь у блокчейні. Генератори блоків мають право

формувати блоки, незалежно від частки у відповідному блокчейні та власників облікових записів, що делегують їм частину своєї частки.

Наповнення валідаторів, що діють, може бути змінено. У механізмі є можливість додавання нових учасників та видалення існуючих. Будь-які зміни у механізмі вимагають схвалення з боку підгрупи діючих валідаторів шляхом їхнього підпису. Для завершення процесу затвердження сума ваги цих валідаторів має перевищувати або бути рівною порогу остаточності [28].

Модуль, який застосовується в блокчейнах PoR, включає наступні операції, які полегшують процес оновлення прав:

- вузол, який прагне стати валідатором, спочатку має надіслати транзакцію реєстрації в ноди (команда реєстрації повноважень);
- транзакція оновлення повинна включати загальний мультипідпис, в який внесли свій внесок досить активних валідаторів, щоб сума їх ваг BFT перевищувала поріг остаточності (Команда Оновлення Рангу – Update Rank).

Система з високим ступенем BFT здатна підтримувати цілісність та працездатність, навіть якщо до 1/3 вузлів у мережі діють аномально.

Для створення моделі достатньо використовувати механізм консенсусу, заснований на доказі рангу, де ранг вузла формується на основі його впливу та відповідності іншим вузлам у мережі. У запропонованому алгоритмі новий блок створюється вузлом з вищим рангом, після чого він перевіряється та підтверджується іншими вузлами (якісними, середніми, нижчими). Концепція роботи механізму консенсусу представлена на рис. 2.7.

Алгоритм консенсусу PoR є механізмом, заснованим на ранжируванні учасників у мережі за їх статусом та призначенням певних ролей у процесі підтвердження блоків [28]. Докладніший механізм роботи є таким:

- ранжування учасників. Учасники мережі ранжуються на чотири рівні: вищий ранг, якісний ранг, середній ранг та нижчий ранг, залежно від їхнього статусу та рейтингу в мережі;

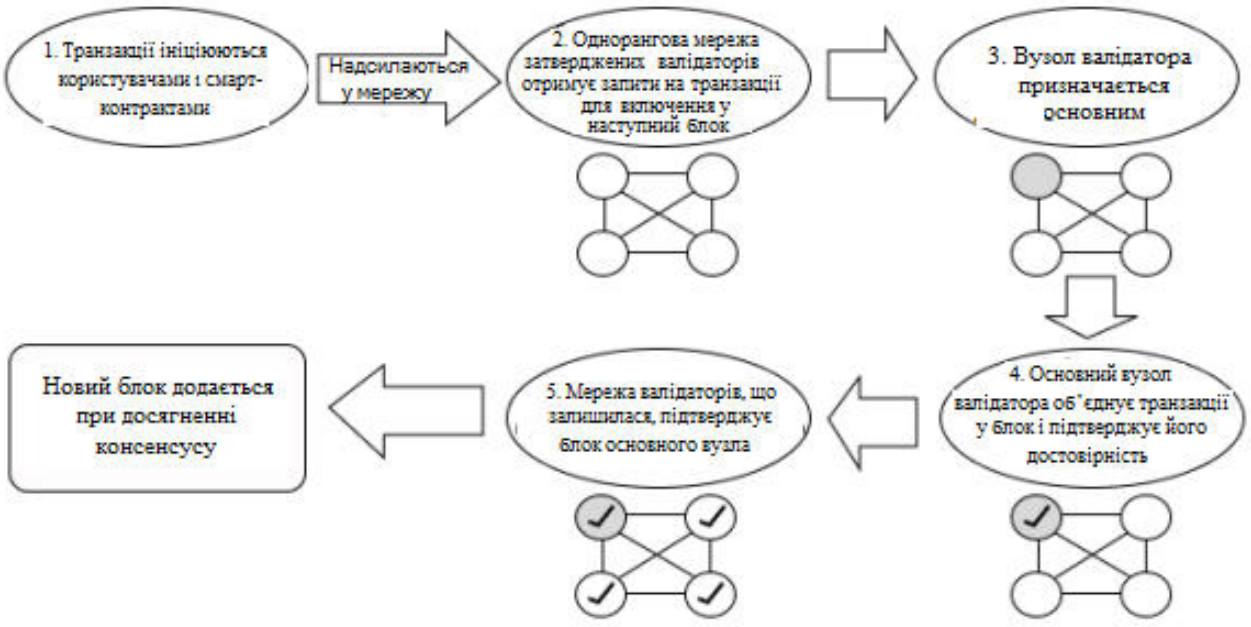

Рисунок 2.7 – Діаграма концепції консенсусу PoR

- вибір підтверджуючого. З появою нового блоку якісні та середні валідатори з-поміж учасників вищого рангу проводять голосування для вибору одного з них, хто здійснюватиме підтвердження блоку;
- перевірка та підтвердження. Вибраний валідатор перевіряє та підтверджує блок, не фіналізуючи його, але лише засвідчуючи його коректність та достовірність;
- перевірка іншими рангами. Учасники з рангами якісного, середнього та низького рівнів починають перевірку підтвердженого блоку та виносять вердикт про його коректність;
- результати голосування. Залежно від результатів голосування учасники отримують певну кількість очок, які впливають на їхній рейтинг у мережі. При правильному підтвердженні блоку учасники отримують додаткові очки, а у разі помилкового підтвердження їхній рейтинг знижується;
- фіналізація блоку. При позитивному результаті перевірки блок фіналізується, якщо виявляються помилки, відбувається повторна перевірка і перепідтвердження;
- розподіл комісійних. Грошова комісія за проведення транзакцій у мережі розподіляється між усіма учасниками, причому основна частина комісії

дістається учасникам з вищим рангом, а частина, що залишилася, розподіляється між рештою залежно від їх рангу.

Алгоритм PoR є детермінованим та забезпечує оптимальну стійкість до відмов, допускаючи невелику кількість несправних процесів у мережі. Загальна складність зв'язку алгоритму може бути оцінена залежно кількості учасників і структури мережі. Завершення процесу консенсусу досягається через кілька повідомлень, забезпечуючи швидку обробку транзакцій та ефективне функціонування мережі. Схема роботи алгоритму PoR представлена на рис. 2.8.

Рисунок 2.8 – Схема роботи алгоритму PoR

У механізмі голосування в алгоритмі PoR братимуть участь вузли мережі, які мають якісні та середні ранги. Сам процес голосування складатиметься з наступних етапів:

- ініціація голосування. У якийсь момент виникає необхідність ухвалення рішення в мережі, наприклад, формування нового блоку або зміна конфігурації системи;
- вибір учасників. У голосуванні беруть участь лише певні вузли мережі, які мають певний ранг та відповідають певним критеріям активності та

надійності;

- голосування. Учасники голосують за запропоновані варіанти рішення. Голосування може відбуватися шляхом надсилання транзакцій із зазначенням обраного варіанту або з використанням інших механізмів;
- підрахунок голосів. Система підраховує голоси та визначає, яке рішення набрало більшу кількість голосів;
- ухвалення рішення. На основі результатів голосування система приймає рішення та виконує відповідні дії, наприклад, створює новий блок або вносить зміни до системи.

Механізм голосування в алгоритмі PoR забезпечує демократичне управління мережею та дозволяє приймати рішення на основі консенсусу серед вузлів мережі, що беруть участь.

В алгоритмі PoR оцінка ваг рангу відбуватиметься на основі впливу та підпорядкування вузла іншим вузлам у мережі. Кожен вузол має певний ранг, який відображає його статус та важливість у системі. Оцінка ваги рангу здійснюється шляхом аналізу дій вузла, його активності, надійності та інших параметрів, які визначають його вплив на функціонування мережі. Чим вище ранг вузла, тим більша його вага у процесі прийняття рішень та формування нових блоків. Ця система дозволяє надійно керувати вузлами в мережі, забезпечуючи цілісність та стабільність роботи блокчейну.

В алгоритмі PoR нагорода за участь може бути реалізована по-різному залежно від конкретної реалізації та конфігурації мережі. Вузли з високим рангом, вибрані для генерації нових блоків, можуть отримувати винагороду за кожен створений блок. Це заохочує вузли до активної участі в мережі та забезпечує їхню зацікавленість у підтримці її працездатності.

Вузли мережі, що беруть участь у перевірці та підтвердженні нових блоків, можуть також отримувати винагороду за свою діяльність. Це стимулює учасників до більш активної участі у забезпеченні безпеки та цілісності мережі. Також вузли, які беруть участь у голосуванні з різних питань у мережі (наприклад, зміни протоколу або важливих рішень) можуть отримувати

винагороду за свої голоси. Це дозволяє стимулювати участь у процесі прийняття рішень та забезпечує демократичність управління мережею.

Крім основних винагород, можуть бути передбачені додаткові стимули для вузлів, які демонструють високу активність, надійність чи внесок у розвиток мережі. Це може бути реалізовано через різні бонуси, заохочення чи премії.

Нагорода за участь в алгоритмі PoR відіграє важливу роль у мотивації учасників мережі та забезпечує їхню зацікавленість у підтримці та розвитку блокчейн-екосистеми.

Переваги алгоритму консенсусу PoR:

- демократичність управління. Алгоритм PoR забезпечує демократичне керування мережею блокчейну. Участь у голосуванні мають вузли з певним рангом, що дозволяє приймати рішення на основі консенсусу серед вузлів, що беруть участь;
- ефективність вибору валідаторів. Оскільки тільки вузли з певним рангом можуть брати участь у голосуванні, це дозволяє знизити можливість включення ненадійних або шкідливих вузлів у процес формування блоків;
- масштабованість. Модель PoR обмежується на фіксованій кількості валідаторів блоку, що забезпечує масштабованість системи.

Недоліки алгоритму консенсусу PoR:

- складність реалізації. Впровадження алгоритму PoR вимагає розробки складних механізмів для оцінки рангу вузлів та організації голосування, що може вимагати значних витрат часу та ресурсів;
- складність оцінки рангу. Визначення рангу вузлів може бути складним і схильним до маніпуляцій, особливо в умовах атаки або зміни переваг учасників мережі.

Таким чином, алгоритм PoR матиме потенціал для забезпечення демократичного управління та підвищення безпеки мережі блокчейну, проте його успішна реалізація потребує уважного проектування та врахування множини факторів, включаючи захист від атак та забезпечення рівноправності учасників.

2.2.3 Proof of Rank у порівнянні з альтернативними консенсусними механізмами

З п 2.2. випливає, що механізм підтвердження повноважень (PoR) сприяє збільшенню швидкості перевірки транзакцій компетентними органами. Оскільки блоки формуються в строго передбачуваній послідовності на основі числа валідаторів, блокчейн забезпечуватиме більш високу швидкість обробки транзакцій, ніж алгоритми PoR або PoS. Крім того, механізм підтвердження повноважень сприяє підвищенню ефективності системи блокчейн за рахунок покращення масштабованості та зниження витрат на енергію.

Згідно з проведеним дослідженням та значущістю поняття безпеки, механізм PoR матиме більш високий ступінь захисту від атак на 51% порівняно з алгоритмом PoW [27]. Це зумовлено тим, що PoR буде неможливо компрометувати мережу шляхом контролю більше 51% обчислювальної потужності, як це можливо в PoW.

Почнемо детальне порівняння алгоритмів, першим учасником виступить механізм PoW. Порівняння алгоритму PoR з PoW включає різні аспекти, такі як продуктивність, безпека, енергоефективність і децентралізація.

В PoW продуктивність визначається обчислювальною потужністю, необхідною для вирішення складних математичних завдань, що може призвести до значних затримок обробки транзакцій [31]. PoR забезпечуватиме більш високу продуктивність за рахунок ефективного механізму формування рангу вузлів, що дозволить обробляти більшу кількість транзакцій в одиницю часу.

Поняття безпеки грає велику роль області блокчейна. Атаки на PoW можливі за наявності 51% обчислювальної потужності, що робить систему вразливою для атак. PoR буде більш стійким до атак на 51%, оскільки атакуючий необхідно мати не тільки велику кількість обчислювальної потужності, але й високий ранг, що ускладнює успішну атаку.

Ще одним порівняльним показником може бути поняття енергоефективності. PoW вимагає значних обчислювальних ресурсів та

електроенергії для майнінгу блоків, що призводить до високих енерговитрат та екологічних проблем [31]. PoR буде більш енергоефективним, оскільки процес формування рангу вузлів не вимагає значних обчислювальних ресурсів і може бути реалізований з використанням менш енергоємних методів.

Також порівняємо організаційні структури механізмів. PoW забезпечує децентралізацію за рахунок поширення учасників мережі, але при цьому існує ризик централізації в руках великих майнерів або пулів майнерів. PoR також сприяє децентралізації, оскільки формування рангу вузлів відбувається на основі їхньої активності та надійності, а не обчислювальної потужності. Це дозволяє розподілити владу у мережі більш рівномірно.

Перейдемо до порівняння консенсусу PoR з PoS. Порівняння алгоритмів можна провести за кількома ключовими аспектами, такими як структура, механізм консенсусу, безпека та продуктивність.

У PoS право на генерацію нових блоків та валідацію транзакцій залежить від кількості монет, які вузол тримає у своєму гаманці. У PoR ранг вузла формується на основі його впливу та підпорядкування іншим вузлам мережі. Вузли з більш високим рангом мають більше прав та впливу в системі.

У PoS нові блоки створюються та підтверджуються учасниками з найбільшою кількістю монет у гаманці. PoR використовує механізм голосування серед вузлів з певним рангом для ухвалення рішень у мережі. За швидкістю транзакцій PoR може бути ефективнішим завдяки своєму механізму голосування, який дозволяє швидше приймати рішення в мережі.

PoS забезпечує високий рівень безпеки, але може бути вразливим до атак на 51% у разі концентрації великої кількості монет у невеликої кількості учасників. PoR навпаки, надаватиме стійкість до атак на 51% завдяки системі рангів, що робить його менш схильним до атак проти ПоS.

Порівняння наступного алгоритму PoA проводитимо за принципом зіставлення з механізмом PoS.

У PoA право на генерацію блоків та валідацію транзакцій залежить від активності учасника та його внеску до мережі. У PoR вузли з більш високим

рангом мають більше прав та впливу в системі.

У PoA нові блоки генеруються учасниками, що пройшли процес підтвердження активності, який може включати виконання виконання завдань або проведення транзакцій. PoR використовує механізм голосування серед вузлів з певним рангом для ухвалення рішень у мережі.

PoA забезпечує високий рівень безпеки, але може бути вразливим до атак у разі компрометації великої кількості активних учасників PoR, як було описано вище, забезпечує стійкість до атак на 51% завдяки системі рангів, що робить його менш схильним до атак по порівнянню з PoA.

Наступне порівняння - PoR з DPoS. Почнемо з показника децентралізації. У DPoS децентралізація може бути зменшена через концентрацію влади в руках небагатьох обраних делегатів, які приймають рішення від імені всієї мережі. Алгоритм PoR здебільшого буде орієнтований підвищення децентралізації з допомогою розподілу ролей у мережі з урахуванням рангу вузлів. Учасники мережі отримують ранг залежно від їхнього впливу та підпорядкування іншим вузлам.

У DPoS рішення ухвалюються делегатами, обраними спільнотою. Це може призвести до появи централізованих структур управління, відповідно вразливість DPoS до атак на 51% може бути вищою. В алгоритмі PoR керування мережею здійснюється на основі голосування серед вузлів з високим рангом. Це робить процес прийняття рішень більш демократичним та широко представленим.

Що стосується питання продуктивності, обидва алгоритми (DPoS і PoR) мають хорошу продуктивність. DPoS завдяки вибору делегатів для ухвалення рішень, а PoR через механізм голосування, який сприяє швидкому ухваленню рішень.

Порівняння алгоритму PoR з алгоритмом PoWeight можна провести за декількома ключовими аспектами, включаючи структуру, механізм консенсусу, безпеку та продуктивність.

PoWeight використовує вагу монети, що належить вузлу, визначення його

права створення нових блоків. Вузли з великою кількістю монет мають більшу вагу та більше шансів стати обраними для створення блоків. У PoR ранг вузла формується на основі його впливу та підпорядкування іншим вузлам мережі. Вузли з більш високим рангом мають більше прав та впливу в системі.

У PoWeight нові блоки створюються вузлами в залежності від їхньої ваги монети. Вузли з великою вагою мають більше шансів створення блоку. PoR використовує механізм голосування серед вузлів з певним рангом для ухвалення рішень у мережі.

PoWeight також забезпечує безпеку завдяки розподілу прав на створення блоків відповідно до ваги монети, але може бути вразливим до атак на контроль більшості монет. PoR, як було згадано вище, надає стійкість до атак на 51% завдяки системі рангів, що робить його менш схильним до атак порівняно з PoWeight.

Продуктивність PoWeight залежить від кількості монет, що беруть участь у мережі, і може бути менш стабільною, ніж PoR. PoR може бути більш ефективним у обробці транзакцій завдяки своєму механізму голосування, який дозволяє швидше приймати рішення у мережі.

2.3 Висновки до другого розділу

У цьому розділі було проведено порівняння різних алгоритмів консенсусу.

Порівняння алгоритму PoR із PoW, PoS, PoA, DPoS, PoWeight показує, що PoR може запропонувати більш високу продуктивність, стійкість до атак та енергоефективність, зберігаючи при цьому принципи децентралізації. Кожен з цих алгоритмів має свої плюси і мінуси, та, властиво, вибір між ними залежить саме від тих потреб і цілей, котрі визначені розробниками блокчейн-системи.

3 ПРАКТИЧНІ АСПЕКТИ ЗАСТОСУВАННЯ АЛГОРИТМУ PROOF OF RANK

3.1 Застосування Proof of Rank у блокчейн-проектах

Алгоритм PoR є потенційно перспективним консенсусним механізмом, який може знайти широке застосування в різних галузях, включаючи фінансові технології, державні системи та логістику. Ось більш докладний розгляд прикладів використання PoR у цих сценаріях [30].

Область фінансових технологій:

- банківські операції. PoR може використовуватися для забезпечення безпеки та цілісності банківських транзакцій. Ранг вузлів може залежати від їхньої надійності, що дозволяє створювати довіру до учасників мережі;
- децентралізовані фінансові послуги (DeFi) PoR може бути застосований у DeFi -проектах для голосування щодо прийняття рішень про внесення змін до протоколів або управління фондами. Це забезпечує демократичне управління та захищає мережу від атак.

Державні системи:

- електронне голосування. PoR може бути застосованим для забезпечення власне безпеки та прозорості в системах електронного голосування. Ранг вузлів може залежати від їхнього статусу, що дозволяє створювати довіру до процесу голосування;
- управління державними даними. PoR може забезпечити захист державних даних та забезпечити їх цілісність. Ранг вузлів може визначатися їхніми рольовими правами та доступом до конфіденційної інформації.

Процес логістики:

- управління ланцюжком поставок. PoR може використовуватися для відстеження та керування транспортуванням товарів у ланцюжку поставок. Вузли з більш високим рангом можуть отримувати переваги за участю у обробці та моніторингу вантажів;

- митні процеси. Алгоритм може забезпечити безпеку та ефективність митних процесів. Вузли з високим рангом можуть мати переваги під час перевірки та реєстрації товарів на кордонах

У медичній галузі PoR може бути застосованим для забезпечення безпечного та конфіденційного обміну медичною інформацією, а також управління доступом до медичних даних та електронних медичних карт. Модель PoR може допомогти захистити персональні дані пацієнтів та забезпечити цілісність та достовірність медичної інформації [30].

Також з другого розділу даної роботи було виявлено, що алгоритм PoR є покращеною і безпечнішою моделлю консенсусу, яка може бути успішно застосована в мережі блокчейн.

PoR забезпечує високий рівень безпеки завдяки своїй моделі, що базується на ранзі вузлів. Вузли з більш високим рангом мають більше довіри та впливу в мережі, що допомагає запобігати атакам на консенсус та підтримувати цілісність даних.

PoR дозволяє створювати блоки прогнозованої послідовності на основі рангу вузлів. Це сприяє збільшенню швидкості обробки транзакцій та підвищенню продуктивності мережі блокчейн. Завдяки цьому покращується користувальницький досвід та знижуються комісії за транзакції.

PoR забезпечує прозорість та надійність процесу власне прийняття рішень через застосування рангу вузлів. Це дозволяє учасникам мережі легко перевіряти та підтверджувати дії, що здійснюються в мережі, що сприяє підвищенню довіри до системи.

PoR забезпечує демократичне управління мережею блокчейн, оскільки рішення приймаються на основі консенсусу серед вузлів мережі, що беруть участь. Це робить мережу більш відкритою та доступною для всіх учасників, що сприяє її розвитку та поширенню [30].

PoR має високий ступінь стійкості до різних видів атак завдяки своїй моделі, що базується на ранзі вузлів. Саме це і дає змогу мережі бути менш уразливою до атак 51% та інших форм маніпуляції мережею.

Використання алгоритму PoR у мережі блокчейн, а також у представлених областях може призвести до значного покращення її безпеки, ефективності та прозорості, що зробить її більш привабливою для широкого кола користувачів та розробників.

Також у рамках кваліфікаційної роботи важливо відзначити перспективи розвитку алгоритму PoR. Ось кілька ключових аспектів огляду перспектив розвитку PoR.

Насамперед планується поступово вдосконалити алгоритм по ходу його роботи та дій учасників у мережі. Дослідження щодо вдосконалення самого алгоритму PoR можуть включати розробку нових методів оцінки рангу вузлів, покращення механізмів голосування та вирішення конфліктів, а також оптимізацію процесів формування та перевірки блоків. Ці покращення можуть підвищити безпеку, ефективність та стійкість мережі, а також розширити її можливості застосування.

Також важливою частиною є дослідження нових галузей застосування. Перспективи розвитку PoR можуть включати пошук нових областей застосування алгоритму в різних секторах економіки та суспільного життя. Наприклад, дослідження можуть бути спрямовані на адаптацію PoR для використання у галузі охорони здоров'я.

Інтеграція з іншими технологіями. Дослідження можуть також зосередитись на інтеграції PoR з іншими передовими технологіями, такими як штучний інтелект, інтернет речей (IoT). Такі інтеграції можуть створити нові можливості для використання PoR у різних сценаріях, наприклад, для розробки автономних систем управління та моніторингу, розумних контрактів та автоматизації бізнес- процесів.

Ще одним важливим аспектом подальшого розвитку PoR є стандартизація та регулювання його застосування у різних галузях та сферах діяльності. Дослідження можуть включати розробку стандартів та нормативів, а також аналіз питань безпеки, конфіденційності та відповідності законодавству під час використання PoR.

Не можна не відзначити можливість розвитку PoR у галузі освіти. Дослідження та проекти в цій галузі можуть сприяти підвищенню обізнаності та розуміння серед фахівців та широкої публіки про переваги та можливості реалізованого та аналізованого консенсусу PoR.

Таким чином, огляд поточних досліджень та перспектив розвитку алгоритму PoR дозволяє оцінити його потенціал для вдосконалення, розширення областей застосування та створення нових рішень для сучасних викликів та потреб.

3.2 Програмна реалізація алгоритму

Для програмної реалізації консенсусу PoR використовувалася мова програмування Python, середовище розробки PyCharm. Нижче показані імпорти для коректної роботи механізму (лістинг 3.1).

Лістинг 3.1 – Код імпорту

```
import hashlib
import json
import random
import sys
from math import log
from time import time, sleep
from uuid import uuid4
import requests
from flask import Flask, jsonify, request.
```

Модуль sha256 використовувався для хешування блоків. Лістинг 3.2 містить реалізацію методу hash().

Лістинг 3.2 – Реалізація методу hash()

```
    @staticmethod
def hash(block: dict):
    to_hash = json.dumps(block)
    return sha256(to_hash.encode()).hexdigest().
```

Цей код приймає словник блоку, перетворює його на рядок JSON, потім обчислює хеш SHA-256 цього рядка і повертає його у вигляді шістнадцяткового представлення [27].

Фреймворк flask для розподілених і web -реалізацій програми. Flask - це легкий фреймворк для створення web -додатків мовою Python. Він дозволяє швидко створювати web -додатки та web -сервіси з мінімальним обсягом коду [29]. Нижче наведено фрагмент ініціалізації вузла (лістинг 3.3).

Лістинг 3.3 – Фрагмент коду ініціалізації вузла

```
app = Flask(__name__)
address = ''
blockchain = Blockchain(.
```

Тут створюється екземпляр програми Flask. Параметр ' _name _' передається як аргумент, щоб Flask міг точно визначити, де знаходиться застосунок і де шукати ресурси, такі як шаблони та статичні файли. Це дозволяє Flask правильно налаштувати шляхи до ресурсів

Далі створюється екземпляр класу blockchain і вузол запускається на адресу, вказану у вузлі. Лістинг 3.4 містить код ініціалізації блокчейна :

Лістинг 3.4 – Програмний код ініціалізації блокчейна

```
class Blockchain:
def __init__(self):
    self.authority = None
    self.blocs = []
    self.peers = set()
    self.mempool = []
    self.forge(prev_hash='genesis', curr_hash=None.
```

Отже, цей код створює екземпляр класу blockchain з початковими параметрами та ініціалізує блокчейн. Після цього можна буде додавати нові блоки та виконувати інші операції з блокчейном відповідно до логіки алгоритму.

Лістинг 3.5 демонструє код розробки нового блоку.

Лістинг 3.5 – Створення нового блоку

```
    def forge(self, prev_hash: Optional[str], curr_hash:
Optional[str]):
    bloc = {
        'previous_hash': prev_hash or
self.previous_block['current_hash'],
        'current_hash': '',
        'timestamp': int(time()),
        'transactions': self.mempool[:]
    }
bloc['current_hash'] = curr_hash or self.hash(bloc)
self.blocs.append(bloc).
```

Блок містить такі елементи: таймстамп - тимчасова мітка, current_hash - підпис творця блоку, що складається з хеша, хеш попереднього блоку, список транзакцій. Після формування нового блоку, список транзакцій обнулюється для збирання нових транзакцій. Після створення блок додається в мережу [31]. Щоб підтвердити блок, необхідно творцю блоку синхронізувати блок з іншими валідаторами.

Створення нової транзакції наведено у лістингу 3.6.

Лістинг 3.6 – Код створення нової транзакції

```
 def new_transaction(self, sender: str, content: dict):
if self.authority is not None:
    requests.post(
        f'http://{self.authority}/transaction/create',
        json=content
    )
    return
self.mempool.append({
    'sender': sender,
    'content': content
})
if len(self.mempool) == FORGE_TRIGGER:
    self.forge(prev_hash=None, curr_hash=None)
    self.mempool.clear().
```

Спочатку необхідно переконатися в тому, що необхідні поля знаходяться серед POST даних. Після відбувається створення нової транзакції та повертається результат. Код отримання усіх блоків показано у лістингу 3.7.

Лістинг 3.7 – Одержання всіх блоків

```
@app.route('/')
def base():
    return flask.jsonify({
        'message': f'running on {address}',
        'chain': blockchain.blocs
    }).
```

В рамках алгоритму PoR, вузол, який має ранг, відіграє ключову роль у підтвердженні блоків. Поданий код демонструє механізм роботи з блокчейном, включаючи створення блоків, додавання транзакцій та отримання ланцюга блоків.

Далі було створено метод додавання нової ноди в мережу блокчейн. Для тестування даної функціональності використовувався інструмент Postman, що дозволяє надсилати HTTP -запити та отримувати відповіді [32]. Для реєстрації нової ноди було сформовано запит, який містить необхідну інформацію про нову ноду та адресу, за якою вона буде доступна. Подробиці запиту представлені на рис. 3.1. Цей метод дозволяє динамічно розширювати мережу блокчейн шляхом додавання нових вузлів, що сприяє поліпшенню її масштабованості та стійкості

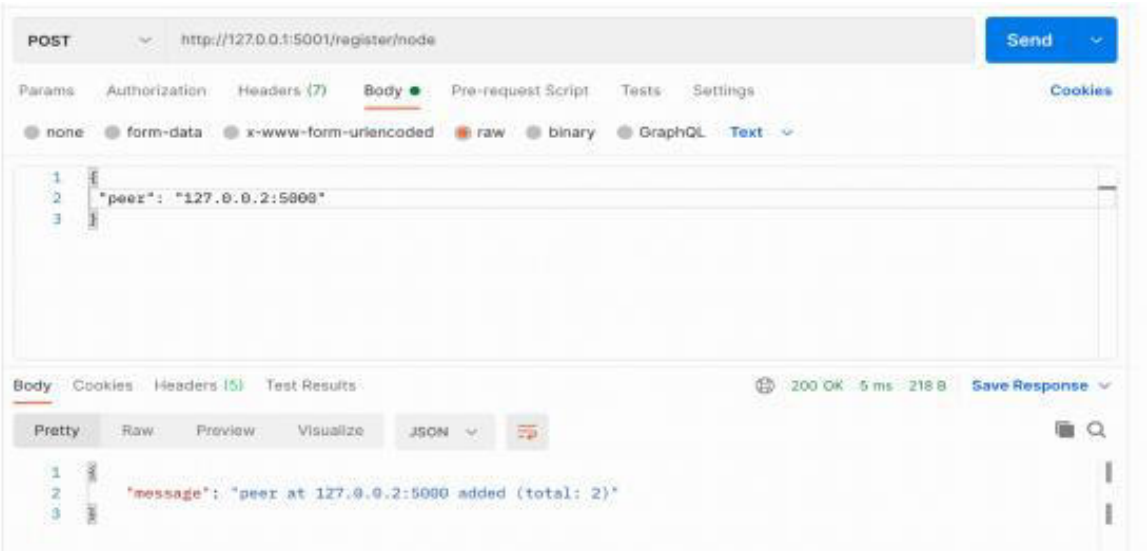

Рисунок 3.1 – Реєстрація нової ноди

Надсилається запит на реєстрацію нової ноди, при успішному виконанні

коду повертається повідомлення: "{"message": "peer at ip added"}". При неправильному запиті буде відповідна відповідь. На рис. 3.2 показаний результат запиту на встановлення рангу валідатору.

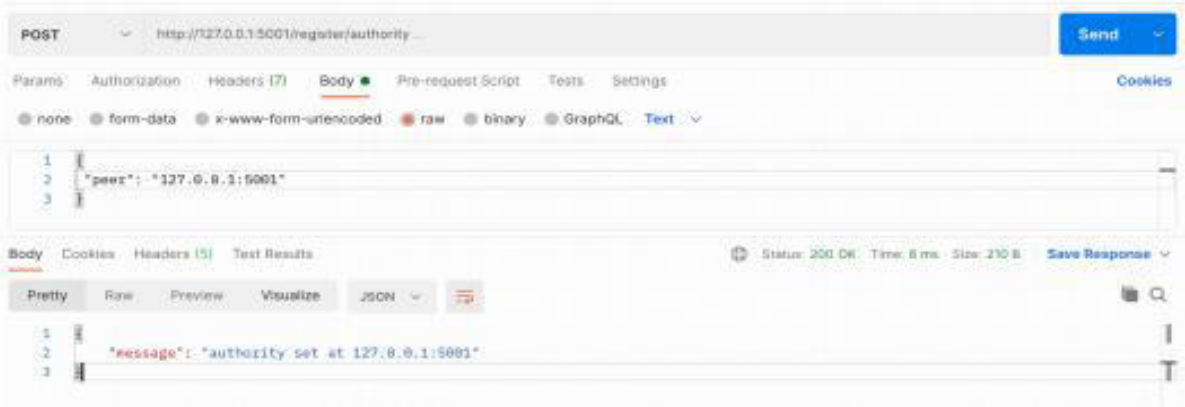

Рисунок 3.2 –Встановлення рангу валідатора

Лістинг 3.8 відображає реалізацію встановлення рангу ноді

Лістинг 3.8 – Код встановлення рангу ноді

```
@app.route('/register/authority', methods=['POST'])
def set_auth():
    payload = request.get_json(force=True)

    if not payload['peer']:
        return flask.jsonify({
            'message': 'authority\'s address missing'
        }), 400

    blockchain.set_authority(payload['peer'])

    return flask.jsonify({
        'message': f"authority set at {payload['peer']}"
    }).
```

Цей код є кінцевою точкою (endpoint) API Flask, яка обробляє POST запити за маршрутом /register/authority. Після отримання запиту POST за цим маршрутом, витягуються дані з тіла запиту у форматі JSON за допомогою request.getJson(force=Tme). Далі перевіряється, що у отриманих даних є ключ «peer», що містить адресу authority. Якщо цей ключ відсутній, повертається

помилка 400 із повідомленням про відсутність адреси authority. Потім викликається метод set_authority() об'єкта blockchain, щоб встановити authority у блокчейні. Наприкінці повертається JSON -відповідь з повідомленням про успішне встановлення authority та адресою authority, яка була встановлена.

Докладніше з кодом для реалізації механізму можна ознайомитись у Додатку В.

3.3 Аналіз ефективності та безпеки алгоритму

Для розрахунку ефективності були проведені експерименти, для цього було підготовлено тестове середовище, що включає необхідне програмне забезпечення та апаратні ресурси. Для створення мережевої моделі були використані віртуальні машини на базі операційної системи Mac. Експерименти були розділені на кілька етапів, кожен з яких охоплював певні аспекти алгоритму роботи PoR.

Представимо загальну оцінку продуктивності алгоритму ранжування учасників мережі:

- загальна кількість учасників у мережі: $N = 100$;
- кількість учасників, для яких проводиться ранжування = 50;
- час виконання ранжування одного учасника: $t = 0.01$ секунди.

Підставивши ці значення у формулу, отримаємо:

$$T_{\text{ранжування}} = \frac{100}{50} * 0{,}01 = 0{,}02 \text{ секунд}$$

Оцінка ефективності алгоритму вибору лідера:

- кількість учасників, серед яких обирається лідер = 100;
- час, витрачений вибір лідера: $t_{\text{вибору}} = 0.2$ секунди.

Використовуючи ці дані, проведемо розрахунок:

$$T_{\text{вибір лідера}} = \frac{1}{100} * 0{,}2 = 0{,}002 \text{ секунд}$$

Експерименти перевірки блоків можуть включати кількість тестових блоків, час виконання перевірки кожного блоку, кількість успішно перевірених блоків і кількість блоків, в яких були виявлені помилки:

- загальна кількість тестових блоків: $N = 200$;
- час виконання перевірки одного блоку: варіюється від 0,5 до 3 секунд;
- кількість успішно перевірених блоків: 180;
- кількість блоків із помилками: 20.

Для порівняння консенсусу з іншими механізмами будемо використовувати структуру таблиць, наведених у підрозділі 2.1. Параметри за форматом мережі та показниками продуктивності представлені у табл. 3.1.

Таблиця 3.1 – Показники алгоритму PoR

Протокол консенсусу	**Тип блокчейн мережі**	**Продуктивність**
PoR	Відкрита	Висока

Загальні властивості, отримані експериментальним шляхом: структурні властивості самого блоку в блокчейн мережі, безпеки, продуктивності наведені в табл. 3.2.

Таблиця 3.2 – Загальні властивості алгоритму PoR

		PoR
Структурні властивості	Тип вузлів	Вищий, якісний середній, нижчий
	Тип структури	Децентралізована
	Базовий механізм	Голосування багатоетапне

Продовження таблиці 3.2

		PoR
Властивості блоку та винагороди	Дата створення першого блоку	-
	Винагорода за блок	Ранжоване
	Загальна пропозиція	-
	Середній час створення блоку	3 сек
Властивості безпеки	Невідмовність	Вузли не можуть відхиляти відповідальність за виконання роботи
	Опірність	Стійкий до атак 51%
	Вектор атаки	Спроби маніпуляції рангами учасників мережі
Властивості продуктивності	Відмовостійкість	Висока
	Пропускна спроможність	~ 79 транзакцій у сек.
	Масштабованість	Забезпечено
	Затримка	0,02-2 сек

Додаткові параметри механізму консенсусу PoR представлені у табл. 3.3. Також варто звернути увагу на технічні деталі та інноваційні методи, які можуть бути впроваджені для покращення продуктивності та безпеки механізму PoR.

Виходячи з відповідей на показники для алгоритму PoR, можна зробити висновок, що даний алгоритм має ряд переваг:

- низькі вимоги до спеціального обладнання та обчислювальних ресурсів, що робить його доступнішим для участі в консенсусі;
- висока стійкість до атак гарантує безпеку та надійність роботи мережі;
- можливість запобігання фіктивним транзакціям сприяє підтримці цілісності блокчейн-системи;

- перевага для учасників з великою кількістю валюти в гаманці може стимулювати активну участь та збільшення зацікавленості у розвитку мережі.

Таблиця 3.3 – Додаткові властивості алгоритму PoR

Додаткові властивості	**PoR**
Використання простору на жорсткому диску	Так
Потрібне спеціальне обладнання	Ні
Обчислювальні ресурси обмежені за часом	Ні
Витрачання великої кількості часу	Ні
Висока стійкість до атак	Так
Висока обчислювальна потужність	Ні
Перевага між великою кількістю валюти у гаманці	Так
Можливість фіктивних транзакцій	Ні

3.4 Висновки до третього розділу

У цьому розділі роботи наведено фрагменти основного програмного коду для реалізації алгоритму PoR.

Результати проведених експериментів дають змогу зробити висновок про те, що алгоритм PoR демонструє хорошу продуктивність та надійність за різноманітних умовах експлуатації. Таким чином, алгоритм PoR є більш ефективною і зручною моделлю консенсусу, що забезпечує безпеку, надійність роботи блокчейн-системи в порівнянні з іншими алгоритмами.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Режими праці і відпочинку при роботі з ЕОМ

Нервово-емоційне напруження, втома очей, гіподинамія, підвищене навантаження на кисті верхніх кінцівок та хребет – усе це негативний вплив на організм людини при роботі з комп'ютером.

В даному випадку для збереження здоров'я працюючих, запобігання професійним захворюванням і підтримки працездатності передбачаються внутрішньозмінні регламентовані перерви для відпочинку.

Основним нормативно-правовим документом, який регламентує всі питання, пов'язані із охороною праці, в т.ч. і при роботі з ЕОМ, є [37].

Вимоги при роботі з ЕОМ визначають Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин - ДСанПІН 3.3.2.007-98.

Внутрішньозмінні режими праці і відпочинку містять додаткові нетривалі перерви в періоди, що передують появі стомлення і зниження працездатності.

При виконанні робіт, що належать до різних видів трудової діяльності, за основну роботу з візуальними дисплейними терміналами (ВДТ) слід вважати таку, що займає не менше 50% робочого часу. Впродовж робочої зміни мають передбачатися: перерви для відпочинку і вживання їжі (обідні перерви); перерви для відпочинку і особистих потреб (згідно з трудовими нормами); додаткові перерви, що вводяться для окремих професій з урахуванням особливостей трудової діяльності.

Тривалість обідньої перерви визначається чинним законодавством про працю і правилами внутрішнього трудового розпорядку підприємства, організації чи установи. Як правило, тривалість такої перерви становить 40 – 60 хвилин. Тривалість та кількість інших внутрішньозмінних регламентованих перерв залежить від характеру трудової діяльності, напруженості і важності праці і визначається диференційовано для кожної професії.

За характером трудової діяльності розрізняють три професійні групи, згідно з діючим класифікатором професій [38]:

– розробники програм (інженери-програмісти) виконують роботу переважно з відеотерміналом та документацією при необхідності інтенсивного обміну інформацією з ЕОМ і високою частотою прийняття рішень;

– оператори ЕОМ виконують роботу, пов'язану з обліком інформації, одержаної з ВДТ за попереднім запитом, або тієї, що надходить з нього;

– оператор комп'ютерного набору виконує одноманітні за характером роботи з документацією та клавіатурою і нечастими нетривалими переключеннями погляду на екран дисплея, з введенням даних з високою швидкістю.

Правилами встановлюються такі внутрішньозмінні режими праці та відпочинку при роботі з ЕОМ при 8-годинній денній робочій зміні в залежності від характеру праці:

– для розробників програм із застосуванням ЕОМ слід призначати регламентовану перерву для відпочинку тривалістю 15 хвилин через кожну годину роботи за ВДТ;

– для операторів із застосуванням ЕОМ слід призначати регламентовані перерви для відпочинку тривалістю 15 хвилин через кожні дві години;

– для операторів комп'ютерного набору слід призначати регламентовані перерви для відпочинку тривалістю 10 хвилин після кожної години роботи.

У всіх випадках, коли виробничі обставини не дозволяють застосувати регламентовані перерви, тривалість безперервної роботи з ВДТ не повинна перевищувати 4 години.

При 12-годинній робочій зміні регламентовані перерви повинні встановлюватися в перші 8 годин роботи аналогічно перервам при 8-годинній робочій зміні, а протягом останніх чотирьох годин роботи, незалежно від характеру трудової діяльності, через кожну годину тривалістю 15 хвилин. Необхідно зазначити, що перерви під час роботи не повинні бути строго визначені за часом, а необхідно передбачати певний творчий індивідуальний підхід.

Для запобігання втоми під час деяких перерв доцільно виконувати спеціальні вправи, які наведені у ДСанПІН 3.3.2.007-98. Також ці санітарні правила визначають Відстань від екрана до ока фахівців, які працюють за комп'ютером.

Окрім ДНАОП та ДСанНіП, які регламентують вимоги безпеки та санітарно-гігієнічні вимоги до обладнання робочих місць користувачів ВДТ, є ще інші нормативні акти загального призначення, які необхідно враховувати під час організації роботи користувачів ВДТ. Важливим нормативним актом є [39].

Гігієнічна класифікація праці необхідна для оцінки конкретних умов та характеру праці на робочих місцях. На основі такої оцінки приймаються рішення, спрямовані на запобігання або максимальне обмеження впливу несприятливих виробничих факторів.

4.2 Вплив електромагнітного імпульсу ядерного вибуху на елементи виробництва та заходи захисту

У воєнний час при застосуванні ядерної зброї проти України на електронно-обчислювальне обладнання в першу чергу буде впливати електромагнітний імпульс (ЕМІ) ядерного вибуху у вигляді короткого імпульсу, який вражає головним чином електричну та електронну апаратуру. ЕМІ виникають в основному в результаті взаємодії гамма-випромінювання з атомами навколишнього середовища. На утворення ЕМІ йде невелика кількість ядерної енергії, але він здатен викликати високі імпульси струмів та напруг в кабелях повітряних і підземних ліній зв'язку, сигналізації, управління, електропередачі, в антенах радіостанцій. Вплив ЕМІ може привести до згортання чутливих електронних та електричних елементів, зв'язаних з великими антенами чи відкритими дротами, а також до порушень в обчислювальних пристроях. Вплив ЕМІ необхідно враховувати для всіх електричних та електронних систем. Для найбільш важливих приладів треба використовувати засоби захисту і підвищувати їх стійкість до ЕМІ [40].

Особливістю ЕМІ, як вражаючого фактору є його здатність розповсюджуватись на десятки і сотні кілометрів в оточуючому середовищі. Тому ЕМІ може вплинути своєю дією на об'єкти, там де вибухова хвиля, світлове випромінювання, проникаюча радіація втрачають своє значення, як вражаючі фактори. При наземних та низьких повітряних вибухах в лініях зв'язку та електрозабезпечення виникають напруги, які можуть викликати пробій ізоляції провідників та кабелів відносно землі, пробій ізоляції елементів приладів підключених до повітряних і підземних ліній. Степінь враження залежить від наведеного імпульсу напруги чи струму і також електричної міцності обладнання.

Найбільш піддані впливу ЕМІ системи зв'язку, сигналізації, управління. Використані в цих системах кабелі та апаратура мають обмежену електричну міцність не більше 10кВ імпульсної напруги, тоді як наведені імпульси напруги від ЕМІ можуть перевищувати ці значення. Найбільш піддана впливу ЕМІ апаратура виконана на напівпровідниках та інтегральних схемах, працюючих на малих струмах і напругах, і значить відчутних до впливу зовнішніх електричних і магнітних кіл, в тому числі і елементи програмного засобу для управління процесом міграції віртуальних машин в обчислювальній хмарі. ЕМІ пробиває ізоляцію, спалює елементи електричних схем радіоапаратури, викликає коротке замикання в радіопристроях, іонізацію діелектриків, змінює або повністю стирає магнітний запис. Встановлено, що при дії ЕМІ на апаратуру найбільша напруга наводиться на вході. В транзисторах відбувається така залежність: чим більший коефіцієнт підсилення транзистора, тим менша його електрична міцність.

ЕМІ пошкоджує також резистори, викликає іскріння в їх міжконтактних з'єднаннях і деяких областях провідної поверхні. Найбільшу небезпеку ЕМІ представляє для апаратури, яка встановлена в особливо міцних спорудах, які витримують великі тиски ударної хвилі. В цих спорудах апаратура не виходить з ладу від механічних пошкоджень, але ЕМІ може вивести з ладу всю незахищену апаратуру системи зв'язку, сигналізації і керування. Найбільших значень досягають напруги, які наводяться між кабелем і землею. Напруженість електромагнітного поля всередині споруди в деяких випадках недостатня для

того, щоб вивести з ладу апаратуру, але такі поля в змозі викликати короткочасний збій роботи радіотехнічних пристроїв.

Розглянемо можливі шляхи рішення задачі захисту від ЕМІ. Ідеальним захистом від ЕМІ виявилося б повне укриття приміщення, в якому розміщена радіоелектронна апаратура, металевим екраном [40]. Водночас зрозуміло, що практично забезпечити такий захист у ряді випадків неможливо, тому що для роботи апаратури часто потрібно забезпечити її електричний зв'язок із зовнішніми пристроями. Тому використовуються менш надійні засоби захисту, такі, як струмопровідні сітки, або плівкові покриття для вікон, щільникові металеві конструкції для повітрезабірників і вентиляційних отворів і контактні пружинні прокладки, розміщувані по периметру дверей і люків.

Більш складною технічною проблемою рахується захист від проникнення ЕМІ в апаратуру через різноманітні кабельні входи. Радикальним рішенням даної проблеми міг би стати перехід від електричних мереж зв'язку до практично не схильних до впливу ЕМІ волоконно-оптичних. Проте заміна напівпровідникових приладів у всьому спектрі виконуваних ними функцій електронно-оптичними пристроями можлива тільки у віддаленому майбутньому. Тому в даний час в якості засобів захисту кабельних входів найбільші широко використовуються фільтри, у тому числі волоконні, а також іскрові розрядники, металлоокисні варистори і високошвидкісні зенеровські діоди.

Всі ці засоби мають як переваги, так і недоліки. Так, ємнісно-індуктивні фільтри достатньо ефективні для захисту від ЕМІ малої інтенсивності, волоконні фільтри захищають у відносно вузькому діапазоні надвисоких частот. Іскрові розрядники мають значну інерційність й в основному придатні для захисту від перевантажень, що виникають під впливом напруг і струмів, що наводяться в обшивці літака, кожусі апаратури й оплетенні кабеля.

Металоокисні варистори є напівпровідниковими приладами, що різко підвищують свою провідність при високій напрузі. Проте, при застосуванні цих приладів у якості засобів захисту від ЕМІ варто враховувати їх недостатньо високу

швидкодію і погіршення характеристик при кількаразовому впливі навантажень. Ці недоліки відсутні у високошвидкісних зенеровських діодах, дія яких заснована на різкій лавиноподібній зміні опору від високого значення практично до нуля, при перевищенні прикладеної до них напруги граничного розміру. Крім того на відміну від варисторів характеристики зенеровських діодів після багатократних впливів високих напруг і переключень режимів не погіршуються.

Найбільш раціональним підходом до проектування засобів захисту від ЕМІ кабельних входів є створення таких роз'ємів у конструкції яких передбачені спеціальні заходи, що забезпечують формування елементів фільтрів і установку вмонтованих зенеровських діодів. Використання роз'ємів подібної конструкції дозволить вирішити проблему обмеження малогабаритних характеристик пристрою захисту. Складність рішення задачі захисту від ЕМІ і висока вартість розроблених для цього засобів і методів змушують піти по шляху їхнього вибіркового застосування в особливо важливих системах зброї і військової техніки [40]. Такий же шлях обраний і для захисту систем, що мають велику протяжність, керування і зв'язку. Проте основним методом вирішення проблеми спеціалісти вважають створення так званих розподілених мереж зв'язку

4.3 Висновки до четвертого розділу

В цьому розділі розглянуто важливі питання охорони праці та безпеки в надзвичайних ситуаціях, зокрема описані вимоги до режимів праці і відпочинку при роботі з ЕОМ, а також вплив ЕМІ ядерного вибуху на елементи виробництва та заходи захисту.

ВИСНОВКИ

У процесі написання кваліфікаційної роботи вирішені наступні завдання:

– дано докладні визначення поняття консенсусу в блокчейні;

– розкрито ролі механізмів, розібрано існуючі алгоритми консенсусу;

– оцінено переваги та недоліки існуючих на сьогоднішній день алгоритмів;

– проведено глибоке порівняння алгоритмів за основними характеристиками;

– представлено деталі у блокчейн-проектах;

– наведено технічні особливості реалізації алгоритму;

– проведено показове порівняння PoR з іншими алгоритмами;

– продемонстровано показники ефективності механізму PoR;

– доведено переваги використання PoR.

Проведений аналіз алгоритму PoR дозволяє зробити висновок про його значний внесок у область розробки консенсус-механізмів у блокчейн-технологіях. У рамках роботи було здійснено ретельний аналіз ключових параметрів та властивостей алгоритму PoR, а також його застосування в різних сценаріях використання.

В результаті аналізу було виявлено, що алгоритм PoR має низку переваг та ефективно справляється з основними завданнями консенсусу в блокчейн-мережах. Його використання дозволяє забезпечити високий рівень безпеки, надійність та ефективність функціонування мережі блокчейн.

Таким чином, у ході виконання роботи було досягнуто поставленої мети та вирішено всі представлені завдання. Базуючись на проведеному аналізі можна констатувати, що алгоритм PoR є важливим інструментом у сучасних блокчейн-технологіях, що сприяє широкому застосуванню в різних галузях.

На закінчення проведеної роботи з розробки алгоритму PoR можна відзначити значний внесок цього механізму в область блокчейн-технологій та його потенціал для подальшого розвитку.

Розробка алгоритму PoR є важливим кроком у розвитку блокчейн-технологій і відкриває нові перспективи для створення інноваційних рішень у галузі розподілених систем. Результати роботи можуть бути корисними як для дослідників, так і для розробників блокчейн-додатків, сприяючи подальшому розвитку цієї галузі.

ПЕРЕЛІК ДЖЕРЕЛ

1. Consensus Mechanisms In Blockchain. [Електронний ресурс] – Режим доступу: https://hacken.io/discover/consensus-mechanisms/ (дата звертання: 14.11.2025).

2. How Does Blockchain Work? [Електронний ресурс] – Режим доступу: https://intellipaat.com/blog/tutorial/blockchain-tutorial/how-does-blockchain-work/ (дата звертання: 14.11.2025).

3. Structure of a Block in Blockchain [Електронний ресурс] – Режим доступу: https://www.theengineeringprojects.com/2021/06/structure-of-a-block-in-blockchain.html (дата звертання: 15.11.2025).

4. The scheme of obtaining a hash of transactions in cryptocurrencies. [Електронний ресурс] – Режим доступу: https://www.researchgate.net/figure/The-scheme-of-obtaining-a-hash-of-transactions-in-cryptocurrencies-Source_fig1_347677094 (дата звертання: 15.11.2025).

5. Consensus Mechanisms. [Електронний ресурс] – Режим доступу: https://codefinity.com/courses/v2/0de038c2-b2a2-4df1-9e55-d563c652cd11/a787201f-ec94-4fad-9ae2-cebe833acdb1/867d4e59-df45-4515-b9f9-f197227ebe09 (дата звертання: 15.11.2025).

6. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. [Електронний ресурс] – Режим доступу: https://bitcoin.org/bitcoin.pdf (дата звертання: 16.11.2025).

7. Chaum, David. Blind signatures for untraceable payments // Advances in Cryptology. — 1983. — Vol. 82. — P. 199–203. — doi:10.1007/978-1-4757-0602-4_18.

8. Exploring the Latest Trends in Blockchain Technology for 2025. [Електронний ресурс] – Режим доступу: https://peiko.space/blog/article/blockchain-trends (дата звертання: 18.11.2025).

9. Кучковський В.В Інформаційна технологія блокчейн для опрацювання великих даних : дис. … доктор філософії : 122 “Комп’ютерні науки”. / Кучковський В.В; НУ Львівська Політехніка. — Львів, 2022. — 135.

10. Кучковський В. В. Алгоритми консенсусу // Trends in science and practice of today : abstracts of XXVIII International scientific and practical conference (Ankara, Turkey; June 01 – 04, 2021). – 2021. – С. 502–505.

11. León Vollerigh. Blockchain Governance. Tectum, 1st Edition 2022, 216 pages.

12. Proof of History, Proof of Stake, Proof of Work - Explained [Електронний ресурс] – Режим доступу: https://www.helius.dev/blog/proof-of-history-proof-of-stake-proof-of-work-explained (дата звертання: 24.11.2025).

13. Різниця між PoW та PoS (Proof of Stake vs Proof of Work) [Електронний ресурс] – Режим доступу: https://blog.whitebit.com/uk/the-difference-between-proof-of-stake-and-proof-of-work/ (дата звертання: 26.11.2025).

14. Trom Dao Delegated Proof-of-Stake Consensus/ San Francisco, 2018 - URL: https://tron.network/static/doc/white_paper_v_2_0.pdf (дата звертання: 28.11. 2024).

15. Що таке Delegated Proof-of-Stake? [Електронний ресурс] – Режим доступу: https://blog.whitebit.com/uk/what-is-delegated-proof-of-stake/ (дата звертання: 27.11.2025).

16. Що таке Delegated Proof Of Stake, і до чого тут стейкінг? [Електронний ресурс] – Режим доступу: https://crypta.kyiv.ua/obrazovanie-i-sovety/shho-take-delegated-proof-of-stake-i-do-chogo-tut/ (дата звертання: 27.11.2025).

17. Proof of Space and Time. [Електронний ресурс] – Режим доступу: https://chiapower.org/chia-proofs-of-space/PoST/ (дата звертання: 28.11.2025).

18. UA: Що таке Space and Time? [Електронний ресурс] – Режим доступу: https://medium.com@dmitryzlvk/що-таке-space-and-time-e8a751b6e058 (дата звертання: 28.11.2025).

19. Proof of Weight (PoW) Consensus Mechanism in Blockchain. [Електронний ресурс] – Режим доступу: https://www.geeksforgeeks.org/computer-

networks/proof-of-weight-pow-consensus-mechanism-in-blockchain/ (дата звертання: 29.11.2025).

20. BitFury Group Proof of Stake versus Proof of Work (version 1.0)/ - [Електронний ресурс] – Режим доступу: https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf (дата звертання: 30.11.2025).

21. Технологія блокчейн: за межами біткойна. Прикладні інновації. [Електронний ресурс] – Режим доступу: https://www.sciencedirect.com/science/article/pii/S2405452617303322 (дата звернення: 30.11.2025).

22. Криптографія та мережева безпека: принципи та практика (7-е вид.) [Електронний ресурс] – Режим доступу: https://www.pearson.com/us/higher-education/program/Stallings-Cryptography-andNetwork-Security-Principles-and-Practice-7th-Edition/PGM282084.html. (дата звернення: 30.11.2025).

23. Технологія блокчейн: за межами біткойна. [Електронний ресурс] – Режим доступу: https://www.sciencedirect.com/science/article/pii/S240545261630368X (дата звернення: 30.11.2025).

24. ТОП-15 протоколів та алгоритмів консенсусу в блокчейні. [Електронний ресурс] – Режим доступу: https://coin24.io/ua/articles/top-15-protokolov-i-algoritmov-konsensusa-v-blokcheyneX (дата звернення: 30.11.2025).

25. Пояснення Delegated Proof of Stake. [Електронний ресурс] – Режим доступу: https://www.binance.com/uk-UA/academy/articles/delegated-proof-of-stake-explained (дата звернення: 30.11.2025).

26. Understanding Proof of Weight: A New Consensus in Blockchain. [Електронний ресурс] – Режим доступу: https://www.cliffsnotes.com/study-notes/27777059 (дата звернення: 30.11.2025).

27. Li X. et al. A survey on the security of blockchain systems // Future Generation Computer Systems. 2020. Vol. 107. P. 841-853.

28. Чорний Я.М. Принципи роботи алгоритму Proof of Rank // XIV Міжнародна науково-практична конференція молодих учених та студентів «Актуальні задачі сучасних технологій», Тернопіль, 11-12 Грудня 2025 р. с. 370-372..

29. Легкість та гнучкість: основи Flask для веброзробки програмного забезпечення. [Електронний ресурс] – Режим доступу: https://pnn.com.ua/ua/blog/detail/lightweight-and-flexible-flask-fundamentals-for-software-web-development (дата звернення: 02.12.2025).

30. Чорний Я.М. Застосування алгоритму Proof of Rank у блокчейн-проектах // Інформаційні моделі, системи та технології: Праці XIII наук.-техн. конф. Тернопіль, 17 -18 грудня 2025р. с. 96 - 97.

31. Когут Ю.І. Технології блокчейн та криптовалюта: ризики та кібербезпека. Сідкон, 2022. 316 с.

32. Schwartz D., Youngs N., Britto A. The Ripple Protocol Consensus Algorithm, Ripple Labs Inc White Paper. Ripple Labs Inc, [Електронний ресурс] – Режим доступу: https://ripple.com/files/ripple_consensus_whitepaper.pdf (дата звертання: 05.12.2025).

33. Vyacheslav Nykytyuk, Vasyl Dozorskyy, Nataliia Kunanets, Volodymyr Pasichnyk, Oleksandr Matsiuk, Ihor Bodnarchuk: Electrical Probe-Signal Processing and Criterion for the Determination of Time Parameters of the Teeth Filling Material Polymerization Process in Dentistry. 4th IDDM 2021: Valencia, Spain. P. 54-63

34. Zagorodna, N., Skorenkyy, Y., Kunanets, N., Baran, I., Stadnyk, M. Augmented Reality Enhanced Learning Tools Development for Cybersecurity Major. CEUR Workshop Proceedings., 2022, 3309, pp. 25–32. https://ceur-ws.org/Vol-3309/short1.pdf.

35. Микитишин А. Г., Митник М. М., Стухляк П. Д. Телекомунікаційні системи та мережі. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2017. 384 с.

36. Лупенко С. А., Пасічник В. В., Тиш Є. В. Комп’ютерна логіка. Львів: Видавництво «Магнолія - 2006». 2015. 354 с.

37. Закон України «Про охорону праці». [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2694-12 - (дата звертання 06.05.2025).

38. Класифікатор професій ДК 003:2010/ [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/rada/show/va327609-10 - (дата звертання 06.05.2025).

39. Гігієнічна класифікація умов праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу. – К.: МОЗ України, 1998. – 34 с.

40. Безпека в надзвичайних ситуаціях. Методичний посібник для здобувачів освітнього ступеня «магістр» всіх спеціальностей денної та заочної (дистанційної) форм навчання / укл.: Стручок В. С. Тернопіль: ФОП Паляниця В. А., 2022. 156 с.

ДОДАТКИ

ДОДАТОК А
Тези конференції

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя
Маріборский університет (Словенія)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедиміната (Литва)
Краківський економічний університет (Польща)
Вроцлавський економічний університет (Польща)
Університет «Опольська Політехніка» (Польща)
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Вінницький національний аграрний університет
Львівський національний університет ім. І. Франка
Головне управління Пенсійного фонду в Тернопільській області
Наукове товариство ім. Шевченка
Тернопільський обласний комунальний інститут післядипломної педагогічної освіти
Сумський державний педагогічний університет
Запорізький національний університет

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник

тез доповідей

XIV Міжнародної науково-технічної конференції молодих учених та студентів

11-12 грудня 2025 року

УКРАЇНА
ТЕРНОПІЛЬ – 2025

УДК 004.653
Я.М. Чорний, студент гр. СТм-61
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПРИНЦИПИ РОБОТИ АЛГОРИТМУ PROOF OF RANK

Ya. M. Chornyi

PRINCIPLES OF PROOF OF RANK ALGORITHM

Блокчейн спровокував зміни у фінансових та банківських сферах – додалися нові системи платежів, у логістиці та, в тому числі медицині, завдяки Блокчейну покращилася прозорість та надійність даних. Для досягнення консенсусу у Блокчейн-мережах використовуються різні алгоритми. В роботі досліджується алгоритм

консенсусу, який пропонує унікальну перевагу та можливість для оптимізації блокчейн-мереж. Даному механізму надано назву «Доказ рангу» (Proof of Rank, далі PoR). Цей алгоритм націлений на обробку значно більшої кількості транзакцій на секунду, порівняно з іншими існуючими механізмами

В алгоритмі PoR блоки згруповані в слоти, що становлять множини груп. На кожному етапі або раунді генератори блоків вибираються на початку. Блокчейн PoR підтримує певну кількість валідаторів, які мають право генерувати блоки (вони називаються найвищими валідаторами). Кожному валідатору, що має найвищий ранг, призначається один блоковий слот, в якому блоки формуються. Тривалість раунду визначається кількістю діючих валідаторів, що беруть участь у блокчейні. Генератори блоків мають право формувати блоки, незалежно від частки у відповідному блокчейні та власників облікових записів, що делегують їм частину своєї частки [1].

Алгоритм PoR не вимагає виконання складних завдань для підтримки зв'язку між вузлами, відповідно валідаторам не потрібне особливе обладнання для підтримки мережі. Модель PoR обмежується певною кількістю валідаторів блоків, що сприяє масштабованості системи. Перевірка блоків та транзакцій заздалегідь здійснюється затвердженими вузлами, які виступають у ролі модераторів системи (якісні, середні та нижчі ранги). Перевірка та підтвердження блоків проводиться вищим рангом. Цей механізм забезпечує конфіденційність за рахунок використання переваг блокчейн/

Наповнення валідаторів, що діють, може бути змінено. У механізмі є можливість додавання нових учасників та видалення існуючих. Будь-які зміни у механізмі вимагають схвалення з боку підгрупи діючих валідаторів шляхом їхнього підпису. Для завершення процесу затвердження сума ваги цих валідаторів має перевищувати або бути рівною порогу остаточності.

Модуль, який застосовується в блокчейнах PoR, включає наступні операції, які полегшують процес оновлення прав:

- вузол, який прагне стати валідатором, спочатку має надіслати транзакцію реєстрації в ноди (команда реєстрації повноважень);
- транзакція оновлення повинна включати загальний мультипідпис, в який внесли свій внесок досить активних валідаторів, щоб сума їх ваг BFT перевищувала поріг остаточності (Команда Оновлення Рангу – Update Rank).

Система з високим ступенем BFT здатна підтримувати цілісність та працездатність, навіть якщо до 1/3 вузлів у мережі діють аномально.

Для створення моделі достатньо використовувати механізм консенсусу, заснований на доказі рангу, де ранг вузла формується на основі його впливу та відповідності іншим вузлам у мережі. У запропонованому алгоритмі новий блок створюється вузлом з вищим рангом, після чого він перевіряється та підтверджується іншими вузлами (якісними, середніми, нижчими). Концепція роботи механізму консенсусу представлена на рис. 1.

Рисунок 1 – Діаграма концепції консенсусу PoR

Алгоритм консенсусу PoR є механізмом, заснованим на ранжируванні учасників у мережі за їх статусом та призначенням певних ролей у процесі підтвердження блоків. Докладніший механізм роботи є таким [1]:

- ранжування учасників. Учасники мережі ранжуються на чотири рівні: вищий ранг, якісний ранг, середній ранг та нижчий ранг, залежно від їхнього статусу та рейтингу в мережі;
- вибір підтверджуючого. З появою нового блоку якісні та середні валідатори з-поміж учасників вищого рангу проводять голосування для вибсру одного з них, хто здійснюватиме підтвердження блоку;
- перевірка та підтвердження. Вибраний валідатор перевіряє та підтверджує блок, не фіналізуючи його, але лише засвідчуючи його коректність та достовірність;
- перевірка іншими рангами. Учасники з рангами якісного, середнього та низького рівнів починають перевірку підтвердженого блоку та виносять вердикт про його коректність;
- результати голосування. Залежно від результатів голосування учасники отримують певну кількість очок, які впливають на їхній рейтинг у мережі. При правильному підтвердженні блоку учасники отримують додаткові очки, а у разі помилкового підтвердження їхній рейтинг знижується;
- фіналізація блоку. При позитивному результаті перевірки блок фіналізується, якщо виявляються помилки, відбувається повторна перевірка і перепідтвердження;
- розподіл комісійних. Грошова комісія за проведення транзакцій у мережі розподіляється між усіма учасниками, причому основна частина комісії дістається учасникам з вищим рангом, а частина, що залишилася, розподіляється між рештою залежно від їх рангу.

Література

1. Proof of History, Proof of Stake, Proof of Work - Explained URL: https://www.helius.dev/blog/proof-of-history-proof-of-stake-proof-of-work-explained (дата звертання: 24.11.2025)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XIII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

17-18 грудня 2025 року

ТЕРНОПІЛЬ
2025

УДК 004.653
Я. Чорний
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЗАСТОСУВАННЯ АЛГОРИТМУ PROOF OF RANK У БЛОКЧЕЙН-ПРОЕКТАХ

UDC 004.653
Ya. Chornyi

APPLICATION OF THE PROOF OF RANK ALGORITHM IN BLOCKCHAIN PROJECTS

Алгоритм Proof of Rank (далі – PoR) є потенційно перспективним консенсусним механізмом, який може знайти широке застосування в різних галузях, включаючи фінансові технології, державні системи та логістику [1]. Ось більш докладний розгляд прикладів використання PoR у цих сценаріях.

Область фінансових технологій:

- банківські операції. PoR може використовуватися для забезпечення безпеки та цілісності банківських транзакцій. Ранг вузлів може залежати від їхньої надійності, що дозволяє створювати довіру до учасників мережі;
- децентралізовані фінансові послуги (DeFi) PoR може бути застосований у DeFi-проектах для голосування щодо прийняття рішень про внесення змін до протоколів або управління фондами. Це забезпечує демократичне управління та захищає мережу від атак.

Державні системи:

- електронне голосування. PoR може бути використаний для забезпечення безпеки та прозорості в системах електронного голосування. Ранг вузлів може залежати від їхнього статусу, що дозволяє створювати довіру до процесу голосування;
- управління державними даними. PoR може забезпечити захист державних даних та забезпечити їх цілісність. Ранг вузлів може визначатися їхніми рольовими правами та доступом до конфіденційної інформації.

Процес логістики:

- управління ланцюжком поставок. PoR може використовуватися для відстеження та керування транспортуванням товарів у ланцюжку поставок. Вузли з більш високим рангом можуть отримувати переваги за участю у обробці та моніторингу вантажів;
- митні процеси. Алгоритм може забезпечити безпеку та ефективність митних процесів. Вузли з високим рангом можуть мати переваги під час перевірки та реєстрації товарів на кордонах

У медичній галузі PoR може бути застосованим для забезпечення безпечного та конфіденційного обміну медичною інформацією, а також управління доступом до медичних даних та електронних медичних карт. Модель PoR може допомогти захистити персональні дані пацієнтів та забезпечити цілісність та достовірність медичної інформації.

Алгоритм PoR є покращеною і безпечнішою моделлю консенсусу, яка може бути успішно застосована в мережі блокчейн [2].

PoR забезпечує високий рівень безпеки завдяки своїй моделі, що базується на ранзі вузлів. Вузли з більш високим рангом мають більше довіри та впливу в мережі, що допомагає запобігати атакам на консенсус та підтримувати цілісність даних.

PoR дозволяє створювати блоки прогнозованої послідовності на основі рангу вузлів. Це сприяє збільшенню швидкості обробки транзакцій та підвищенню продуктивності мережі блокчейн. Завдяки цьому покращується користувальницький досвід та знижуються комісії за транзакції.

PoR забезпечує прозорість та надійність процесу власне прийняття рішень через застосування рангу вузлів. Це дозволяє учасникам мережі легко перевіряти та підтверджувати дії, що здійснюються в мережі, що сприяє підвищенню довіри до системи.

PoR забезпечує демократичне управління мережею блокчейн, оскільки рішення приймаються на основі консенсусу серед вузлів мережі, що беруть участь. Це робить мережу

більш відкритою та доступною для всіх учасників, що сприяє її розвитку та поширенню.

PoR має високий ступінь стійкості до різних видів атак завдяки своїй моделі, що базується на ранзі вузлів. Саме це і дає змогу мережі бути менш уразливою до атак 51% та інших форм маніпуляції мережею.

Використання алгоритму PoR у мережі блокчейн, а також у представлених областях може призвести до значного покращення її безпеки, ефективності та прозорості, що зробить її більш привабливою для широкого кола користувачів та розробників [2].

Також у рамках роботи важливо відзначити перспективи розвитку алгоритму PoR. Ось кілька ключових аспектів огляду перспектив розвитку PoR.

Насамперед планується поступово вдосконалити алгоритм по ходу його роботи та дій учасників у мережі. Дослідження щодо вдосконалення самого алгоритму PoR можуть включати розробку нових методів оцінки рангу вузлів, покращення механізмів голосування та вирішення конфліктів, а також оптимізацію процесів формування та перевірки блоків. Ці покращення можуть підвищити безпеку, ефективність та стійкість мережі, а також розширити її можливості застосування.

Також важливою частиною є дослідження нових галузей застосування. Перспективи розвитку PoR можуть включати пошук нових областей застосування алгоритму в різних секторах економіки та суспільного життя. Наприклад, дослідження можуть бути спрямовані на адаптацію PoR для використання у галузі охорони здоров'я.

Інтеграція з іншими технологіями. Дослідження можуть також зосередитись на інтеграції PoR з іншими передовими технологіями, такими як штучний інтелект, інтернет речей (IoT). Такі інтеграції можуть створити нові можливості для використання PoR у різних сценаріях, наприклад, для розробки автономних систем управління та моніторингу, розумних контрактів та автоматизації бізнес-процесів.

Ще одним важливим аспектом подальшого розвитку PoR є стандартизація та регулювання його застосування у різних галузях та сферах діяльності. Дослідження можуть включати розробку стандартів та нормативів, а також аналіз питань безпеки, конфіденційності та відповідності законодавству під час використання PoR.

Не можна не відзначити можливість розвитку PoR у галузі освіти. Дослідження та проекти в цій галузі можуть сприяти підвищенню обізнаності та розуміння серед фахівців та широкої публіки про переваги та можливості реалізованого та аналізованого консенсусу PoR.

Таким чином, огляд поточних досліджень та перспектив розвитку алгоритму PoR дозволяє оцінити його потенціал для вдосконалення, розширення областей застосування та створення нових рішень для сучасних викликів та потреб.

Література

1. Consensus Mechanisms In Blockchain. [Електронний ресурс] – Режим доступу: https://hacken.io/ discover/consensus-mechanisms/ (дата звертання: 14.11.2025).
2. León Vollerigh. Blockchain Governance. Tectum, 1st Edition 2022, 216 pages.

Додаток Б

Порівняльна таблиця механізмів консенсусу

		PoW	PoS	PoA	DPoS	PoWeight
Структурні властивості	Тип вузлів	Майнер	Стейкінг	Вузли мережі	Валідатори	Валідатори
	Тип структури	Децентралізована (без комітету)	Одиночний комітет	Множинний комітет	Множинний комітет	Одиночний або Мншожинний комітети
	Базовий механізм	Лотерея	Лотерея	Лотерея	Голосування	Вік, Лотерея
Властивості блоку та винагороди	Дата створення першого блоку	3.01.2009	12.08.2012	2016	2016	2017
	Винагорода за блок	6,25 BTC	2 ETH	30% DCR	1 EOS	2 ALGO
	Загальна пропозиція	21 млн BTC	120 млн ETH	21 млн DCR	1 млрд EOS	10 млрд ALGO
	Середній час створення блоку	10 хвилин	15 сек	5 хв	8 сек	5 сек
Властивості безпеки	Невідмовність	Вузли не можуть відхиляти відповідальність за виконання роботи	Не можна відмовитись від обов'язків	Гарантія участі всіх вузлів у процесі створення блоків	Масштабуємо	Налаштований
	Опірність	Стійкий до атак 51% і Sybil	Стійкий до атак 51%	Стійкий до атак 51%	Підвищена безпека	атаки 51%, Сібілла та DDoS
	Вектор атаки	Створення фальшивих блоків	Атаки множинних ставок	Подвійні підписи	Атака «Подвійні витрати», частково централізований	Sybil, DDoS
Властивості продуктивності	Відмовностійкість	Висока	Середня	Середня	Висока	Середня
	Пропускна здатність	~ 7 транзакцій у с.	30 транзакц. у сек.	~ 21 транзак. у сек.	~ 46 транзакц. у сек.	~ 67 транзак. у сек.
	Масштабованість	Обмежена	Висока	Низька	Висока	Середня
	Затримка	10 хвилин	5-7 сек			менше 1 секунди

ДОДАТОК В

Програмний код алгоритму Proof of Rank (фрагмент)

```
import hashlib import json import random
import sys
from math import log
from time import time, sleep
from uuid import uuid4
import requests
from flask import Flask, jsonify, request

app = Flask( _name_ )

def send_data_other_nodes(send_data_other_nodes_dict, address): for
element in send_data_other_nodes_dict:
url = f"http://{element}/register_node"
requests.post(url, json={"nodes": [address]}}, .json()


    class Blockchain:
    def  _init_ (self, address):
        self.current_node = address
        self.time_start = time()
        self.chain = []
        self.nodes = []
        self.mempool = {}
       self.reputation = {} # Репутація вузлів
       self.votes = {} # Голоси за кожен блок, ключ – хеш блоку
        self.send_other_node_info(address)
        self.synchronize_chain()
    def inf_node(self):
        return {"node address": self.current_node,
                "time start": self.time_start,
                "chain": self.chain,
                "nodes": self.nodes,
                "reputation": self.reputation, # Репутація вузлів
                 "votes": self.votes, # Голоси за кожен блок, ключ -
    хеш блоку
                 "mempool": self.mempool}

    def add vote(self, vote, self vote: bool = False):

            result = {"vote_node": vote['vote_node'], 'miner':
    vote['miner'],
                  'vote': vote['vote'],
                  'reputation':
self.reputation.get(vote['vote_node'], 0),
                'ageCount': vote['time_vote_node']}
            if self.vote:

            self.votes[vote['block_hash']] = []
            self.votes[vote['block_hash']].append(result)


            self.votes[vote['block_hash']].append(result)
```

```
    def broadcast_vote(self, vote):

        """Відправляє голос лідерові."""

        try:
requests.post(f'http://{vote["miner"]}/receive_vote', json=vote)
except requests.exceptions.ConnectionError:

pass

    def resolve_votes(self, block_hash):
        consent = sum(vote['reputation'] for vote in
self.votes.get(block_hash, []) if vote['vote'] == "consent")
objection = sum(vote['reputation'] for vote in
self.votes.get(block_hash, [])
        if vote[' sum(self.reputation.values())
        if consent >= (2 / 3 * total_reputation):
            return True, self.votes.get(block_hash, []) elif
        objection >= (2 / 3 * total_reputation):
            return False, self.votes.get(block_hash, [])
        return None

    def recalculationRaiting(self, result, receiveMsg): a
        = 0
        sumValueConsent, sumValueObjection = 0, 0
        consentArray, objectionArray = [], []
        for element in receiveMsg:
            if element['vote'] == "consent":
           consentArray.append(element)
            sumValueConsent += element['reputation']
            else:
                objectionArray.append(element)
                sumValueObjection += element['reputation']

        if result:
            for i in consentArray:

                if i['ageCount'] < 18: a = 0.3
                else:
                    a = 0.7
                val = a * log((((i['reputation'] * 100) /
sumValueConsent) / 100) * 10, 10)
                print(val)
                      i['reputation'] += val
                    for j in objectionArray:
    ……..
```