Вінницький національний технічний університет
Факультет інформаційних електронних систем
Кафедра інфокомунікаційних систем і технологій

Бакалаврська кваліфікаційна робота на тему:

КОРИГУВАННЯ ІНФОРМАЦІЙНОГО ТРАФІКУ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Виконав: студент 2-го курсу, групи ПЗТ-23мс
спеціальності 172 – Електронні комунікації та радіотехніка
Нагорний Д. М.

Керівник: д.т.н., проф., професор каф. ІКСТ
Крижановський В.Г.
«12» червня 2025 р.

Рецензент: д.т.н., проф., професор каф. ІРТС
Осадчук Я.О.
«12» червня 2025 р.

Допущено до захисту

Завідувач кафедри ІКСТ

д.т.н., проф. Кичак В.М.

«12» червня 2025 р.

Вінниця ВНТУ - 2025 рік

Вінницький національний технічний університет
Факультет інформаційних електронних систем
Кафедра інфокомунікаційних систем та технологій
Рівень вищої освіти перший (бакалаврський)
Галузь знань 17 – Електроніка та телекомунікації
(шифр і назва)
Спеціальність 172 – Електронні комунікації та радіотехніка
(шифр і назва)
Освітня програма – Програмне забезпечення телекомунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКСТ
д.т.н., професор В.М. Кичак
«05» травня 2025 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ

Нагорному Дмитру Максимовичу
(прізвище, ім'я, по батькові)

1. Тема роботи: Коригування інформаційного трафіку телекомунікаційних систем із використанням технології блокчейн
керівник роботи Крижановський Володимир Григорович, докт. техн. наук, професор,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом ВНТУ від "20" березня 2025 року № 97
2. Строк подання здобувачем роботи: 09 червня 2025 року

3. Вихідні дані до роботи: пропускна здатність каналу 10 – 1000 Мбіт/с; середня затримка в мережі 20 – 250 мс; джитер 5 – 50 мс; параметри блокчейн-системи: розмір блоку 0,5 – 2 МБ; частота генерації блоків 1 / 10 – 1 / 60 блоків/с; тривалість підтвердження транзакції 1 – 30 сек; максимальна кількість транзакцій у блоці 1000 – 5000 транзакцій; розбіжність результатів аналітичного та імітаційного моделювання ≤ 5 % .

4. Зміст розрахунково-пояснювальної записки роботи (перелік питань, які потрібно розробити): вступ, роль блокчейн-трафіку в телекомунікаційних мережах та його аналіз, аналіз впливу алгоритмів консенсусу на продуктивність комунікаційних мереж, модель прийняття рішень для вибору оптимальної блокчейн-системи, оцінювання ефективності адаптивного вибору блокчейн-систем, охорона праці.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень):
схема моделі системи для вимірювання змін апаратних параметрів обладнання з вузлом блокчейн-мережі; архітектура мережі зв'язку з інтегрованим блокчейн-шаром та модулем адаптивного алгоритму консенсусу; альтернативна схема інтеграції блокчейн-механізмів у мережеву інфраструктуру; алгоритм вибору консенсусу з урахуванням динаміки мережевого середовища; Блок-схема роботи

модуля моніторингу мережевого трафіку; блок-схема роботи модуля прийнят рішень у блокчейн-мережі; архітектура інтелектуальної транспортної системи (ІТ для сценарію оперативного реагування на надзвичайну подію .

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийня
Спеціальна частина	Крижановський В.Г., професор кафедри ІКСТ	05.05.2025	12.06.2025
Охорона праці	Дембіцька С.В., професор кафедри БЖДПБ	05.05.2025	12.06.2025

7. Дата видачі завдання «05» травня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської кваліфікаційної роботи	Строк виконання етапів роботи	Примітк
1	Формування та затвердження теми та індивідуального завдання бакалаврської кваліфікаційної роботи (БКР)	06.05.2025р.	
2	Виконання спеціальної частини БКР. Перший рубіжний контроль виконання БКР	19.05.2025р.	
3	Виконання спеціальної частини БКР. Другий рубіжний контроль виконання БКР	02.06.2025р.	
4	Виконання розділу «Охорона праці»	06.06.2025р.	
5	Нормоконтроль БКР	09.06.2025р.	
6	Попередній захист БКР	10.06.2025р.	
7	Рецензування БКР	11.06.2025р.	
8	Захист БКР	13.06.2025р.	

Здобувач _____ (підпис) Нагорний Д.М.

Керівник роботи _____ (підпис) Крижановський В.Г.

АНОТАЦІЯ

УДК 621.396

Нагорний Д.М. Коригування інформаційного трафіку телекомунікаційних систем із використанням технології блокчейн. Бакалаврська кваліфікаційна робота зі спеціальності 172 – електронні комунікації та радіотехніка, освітня програма – програмне забезпечення телекомунікаційних систем. Вінниця: ВНТУ, 2025. 105 с.

На укр. мові. Бібліогр.: 45 назв; рис.: 29; табл. 14.

У бакалаврській кваліфікаційній роботі розглянуто проблему зниження втрат блоків інформаційних даних у телекомунікаційних мережах на основі впровадження адаптивного підходу до вибору алгоритмів консенсусу та частоти генерації блоків у блокчейн-системах. Метою дослідження є покращення надійності та продуктивності блокчейн-мереж за рахунок динамічного врахування поточних мережевих характеристик, таких як пропускна здатність, затримка, джиттер тощо. У роботі розроблено аналітичну та імітаційну моделі мережі, що дозволяють здійснювати оцінку ефективності адаптивного підходу. Створено модуль прийняття рішень, який, спираючись на дані моніторингу, здійснює вибір оптимального алгоритму консенсусу в режимі реального часу. Результати моделювання показали зниження втрат транзакційних блоків та підвищення пропускної здатності мережі на 10% у порівнянні зі статичним підходом. Розроблені методики можуть бути використані для масштабування рішення в більших мережах і для адаптації до різних типів блокчейн-архітектур.

Ключові слова: блокчейн, консенсус, телекомунікаційна мережа, адаптивний алгоритм, імітаційне моделювання, мережева характеристика, пропускна здатність.

ABSTRACT

UDC 621.396

Nahornyi D.M. Adjustment of Information Traffic in Telecommunication Systems Using Blockchain Technology. Bachelor’s Qualification Thesis in Specialty 172 – Electronic Communications and Radio Engineering, Educational Program – Software for Telecommunication Systems. Vinnytsia: VNTU, 2025. 105 p.

In Ukrainian. Bibliography: 45 titles; figures: 29; tables: 14.

This bachelor's qualification thesis addresses the problem of reducing information block losses in telecommunication networks through the implementation of an adaptive approach to selecting consensus algorithms and block generation frequency in blockchain systems. The aim of the study is to improve the reliability and performance of blockchain networks by dynamically accounting for current network characteristics such as bandwidth, latency, jitter, and others. The work presents analytical and simulation models of the network, enabling the assessment of the effectiveness of the adaptive approach. A decision-making module was developed, which, based on monitoring data, selects the optimal consensus algorithm in real time. Simulation results demonstrated a 10% reduction in transaction block losses and an increase in network throughput compared to the static approach. The developed methods can be applied to scale the solution to larger networks and adapt it to different types of blockchain architectures.

Keywords: blockchain, consensus, telecommunication network, adaptive algorithm, simulation modeling, network characteristic, bandwidth.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

БЧ – Блокчейн

ІТС – Інтелектуальна транспортна система

СМО – Система масового обслуговування

ADNL – Абстрактний мережевий рівень датаграм

API – Програмний інтерфейс прикладного рівня

BoC – Формат серіалізації комірок у масив байтів (TON)

CIP – Пропозиція щодо вдосконалення блокчейна Cardano

CPU – Центральний процесор

DAG – Направлений ациклічний граф

dApp – Децентралізований застосунок

DLT – Технологія розподіленого реєстру

eUTxO – Розширений вихід невитрачених транзакцій

HTTP – Протокол прикладного рівня передавання даних

IP – Протокол мережевого рівня стеку TCP/IP

IPFS – Розподілена файлова система

SD-IoV – Програмно-визначений Інтернет транспортних засобів

MTU – Максимальна одиниця передавання

NVMe – Інтерфейс доступу до твердотільних накопичувачів

OBU – Бортовий блок

OSI – Еталонна модель взаємодії відкритих систем

RAM – Оперативна пам’ять

SSD – Твердотільний накопичувач

TCP – Протокол керування передаванням

TON – Відкрита мережа Telegram

TPS – Транзакцій за секунду

TTL – Час життя пакета

UDP – Протокол користувацьких датаграм

VPN – Віртуальна приватна мережа

ВСТУП

Актуальність теми. У сучасних умовах безперервного розвитку інформаційних технологій, які сприяють формуванню складних обчислювальних систем для вирішення різнорідних завдань, особливої важливості набуває стабільне та відмовостійке функціонування мереж зв’язку передачі даних, що забезпечують обмін інформацією між компонентами систем. Сучасні інформаційні системи генерують значні обсяги власного трафіку, що вимагає ефективної обробки та маршрутизації між різними пристроями. При цьому виникає необхідність у виділенні пріоритетного трафіку, балансуванні навантаження та адаптації до пікових періодів, що висуває жорсткі вимоги до використовуваних технологій за критеріями обчислювальних ресурсів, обсягу оперативної пам’яті, а також швидкості обробки та передавання даних [1]. Одночасно з цим, все більшої актуальності набувають питання інформаційної безпеки, прозорості дій та контролю за інцидентами, потенційними загрозами і збереженням цілісності даних. У цьому контексті технологія блокчейн розглядається як перспективне рішення, здатне забезпечити високий рівень захищеності, надійності та відстежуваності змін. Водночас, більшість варіантів реалізації блокчейн, зокрема з використанням поширених алгоритмів консенсусу, характеризуються надмірними витратами обчислювальних ресурсів, що обмежує їх широке застосування у ресурсозалежних середовищах [2]. Низка менш ресурсоємних алгоритмів консенсусу дає змогу частково зменшити ці витрати, однак їх впровадження вимагає дотримання додаткових умов, таких як побудова довірених сегментів мережі, забезпечення низьких затримок або створення повнозв’язних топологій, де кожен вузол має прямий зв’язок з усіма іншими. Це спричинило появу численних варіацій алгоритмів консенсусу, адаптованих до специфіки конкретних сценаріїв застосування – від фінансових сервісів, де критичною є швидкість транзакцій, до систем зберігання даних, для яких пріоритетними є надійність і безпека [3].

З урахуванням гетерогенного характеру сучасних мереж зв’язку, відсутність гнучких механізмів передавання блокчейн-трафіку є одним з основних бар’єрів для його впровадження. Впровадження системи динамічного регулювання обсягів і швидкості блокчейн-трафіку відповідно до пріоритетності дозволило б адаптувати навантаження до поточних умов експлуатації – забезпечуючи гнучкість як у випадках високого, так і низького рівня навантаження [4]. Крім управління трафіком, важливими залишаються й вимоги до обчислювальних потужностей. Компоненти сучасних мереж мають різні характеристики продуктивності, і основним їхнім завданням є передавання та обробка даних. Розгортання блокчейн-клієнтів на таких вузлах може значно вплинути на їхню продуктивність, особливо в періоди пікового навантаження. Зважаючи на те, що алгоритми консенсусу визначають обчислювальну складність процесів обробки транзакцій і формування блоків, впровадження механізмів адаптивної регуляції цих алгоритмів відповідно до поточних параметрів мережі та доступних ресурсів є доцільним. Це дозволяє обирати найменш ресурсоємні стратегії обробки в критичні моменти та забезпечити оптимальне використання інфраструктурних ресурсів [5].

Аналіз останніх досліджень. Технологія блокчейн, як один із прикладів реалізації розподіленого реєстру, вже тривалий час перебуває в полі зору наукової спільноти. Питання її інтеграції в існуючі інформаційно-телекомунікаційні системи, вплив на параметри мережевої інфраструктури, а також аналіз доцільності застосування в різних контекстах активно досліджуються науковцями, зокрема V. Buterin, S. Kasahara, Q. Xia, Y. Sun, L. Coссo та іншими [6]. Значна кількість досліджень присвячена аналізу процесів поширення трафіку в мережі, оцінці впливу блокчейн на ключові мережеві характеристики [7], технічній зрілості відповідних рішень для впровадження у вже існуючі системи [8], а також проблематиці інформаційної безпеки. Окрему увагу приділено дослідженню та оптимізації алгоритмів консенсусу [9], що дозволило зробити вагомі кроки у підвищенні ефективності блокчейн-систем. Водночас, адаптація цих алгоритмів до умов функціонування

телекомунікаційних мереж, зокрема з урахуванням їх гетерогенності, пропускної здатності, часових затримок та апаратних обмежень, наразі залишається недостатньо опрацьованою темою [10].

Наявні наукові результати переважно фокусуються на удосконаленні алгоритмів консенсусу та зменшенні енергоспоживання при обробці транзакцій. Проте, подальших досліджень потребує створення цілісних підходів до інтеграції блокчейн-систем у телекомунікаційні мережі, з урахуванням як специфіки мережевої інфраструктури, так і динаміки навантаження [11]. Зазначені дослідження та праці стали основою для розвитку напряму впровадження блокчейн у телекомунікаційний контекст. Представлена дипломна робота є логічним продовженням і водночас доповненням цих наукових напрацювань. Основна увага приділена питанню інтеграції адаптивного алгоритму вибору консенсусу в умовах мереж зв’язку, що враховує особливості різних сегментів мережі, у тому числі на апаратному рівні. Такий підхід дає змогу підвищити точність відповідності використовуваних механізмів консенсусу конкретним умовам функціонування сегменту мережі, знижуючи ймовірність втрат блоків транзакцій та підвищуючи гнучкість системи.

Особливу увагу в роботі зосереджено на концепції мультиконсенсусності як базису адаптивності при виборі алгоритмів консенсусу. Розглянуто її вплив на мережеві характеристики, розроблено модель та методику інтеграції модуля прийняття рішень щодо адаптивного вибору блокчейн-систем у мережах зв’язку.

Результати імітаційного моделювання, представлені в роботі, засвідчують ефективність запропонованого підходу і дозволяють використовувати їх на етапі проектування та впровадження блокчейн-рішень у складні телекомунікаційні системи [12].

Отримані висновки можуть стати основою для побудови систем динамічного вибору алгоритмів консенсусу залежно від пріоритету трафіку на окремих ділянках мережі, а також від інших критичних характеристик, що визначають ефективність функціонування мережі в умовах змінного

навантаження. Робота робить суттєвий внесок у розвиток досліджень щодо інтеграції блокчейн у сучасні мережі зв’язку [13].

Мета та постановка задачі. Метою даної бакалаврської кваліфікаційної роботи є зниження рівня втрат блоків інформаційних даних у телекомунікаційних мережах шляхом впровадження нового підходу до адаптації алгоритмів консенсусу та частоти генерації блоків з урахуванням поточних мережевих характеристик.

Задачами бакалаврської кваліфікаційної роботи є:

- провести аналіз структури мережевих пакетів блокчейн-трафіку та оцінити їхній вплив на компоненти телекомунікаційної інфраструктури;

- дослідити взаємозв’язок між характеристиками блокчейн-систем та обчислювальними можливостями апаратного забезпечення мереж зв’язку;

- здійснити огляд існуючих алгоритмів консенсусу, зокрема їх переваг і недоліків, з метою виявлення обмежень щодо застосування в телекомунікаційному середовищі;

- визначити граничні значення мережевих та апаратних параметрів, за яких ефективність окремих алгоритмів консенсусу є максимальною;

- розробити модель модуля прийняття рішень щодо вибору відповідної блокчейн-системи для конкретної телекомунікаційної мережі з урахуванням її топології, пропускної здатності, затримок, енергоспоживання та архітектурного розміщення;

- сформувати модель оцінювання ефективності модуля адаптивного вибору алгоритму консенсусу з урахуванням поточних характеристик мережі;

- виконати аналітичні обчислення та імітаційне моделювання для визначення рівня відхилень при використанні адаптивного підходу;

- розробити адаптивний алгоритм вибору консенсусу на основі оцінених мережевих параметрів як ключовий елемент модуля прийняття рішень;

- провести аналіз та порівняння результатів аналітичних, імітаційних і експериментальних досліджень для перевірки працездатності розробленого

модуля в реальних умовах, з оцінкою його продуктивності, надійності та безпеки;

- розробити методику інтеграції модуля прийняття рішень до різних телекомунікаційних систем і мереж, включно з описом потенційних сценаріїв застосування;

- сформувати методику оцінки ефективності інтеграції з урахуванням параметрів і конфігурації телекомунікаційної інфраструктури.

Апробація результатів роботи. Основні ідеї роботи доповідались і обговорювались на науковій конференції ВНТУ у 2025 році.

1 РОЛЬ БЛОКЧЕЙН-ТРАФІКУ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ ТА ЙОГО АНАЛІЗ

У контексті сучасних телекомунікаційних систем блокчейн-технологія відіграє все більш важливу роль, зокрема завдяки своїй здатності забезпечувати високий рівень децентралізації, надійності та безпеки передачі даних. Одним із ключових аспектів інтеграції блокчейн у мережі зв’язку є аналіз та оцінка специфіки блокчейн-трафіку — інформаційних потоків, які виникають у процесі функціонування блокчейн-систем.

Блокчейн-трафік характеризується високим рівнем транзакційної навантаженості, значним обсягом службової інформації та специфічними вимогами до пропускної здатності й затримки передачі даних. Він включає в себе пакети з транзакціями, блоками, повідомленнями про статус мережі, запитами на підтвердження та розповсюдження даних серед вузлів (нодів). Така структура трафіку істотно відрізняється від класичних телекомунікаційних потоків, що вимагає розробки нових підходів до його обробки та маршрутизації [14].

Аналіз блокчейн-трафіку дозволяє:

- виявити потенційні вузькі місця в телекомунікаційній інфраструктурі, які обмежують ефективність роботи блокчейн-систем;

- оцінити вплив блокчейн-обміну на загальну продуктивність мережі;

- сформувати вимоги до адаптивних алгоритмів маршрутизації та управління трафіком;

- дослідити вплив мережевих характеристик на швидкодію, надійність і енергоспоживання блокчейн-систем.

Таким чином, блокчейн-трафік виступає не лише як новий тип навантаження на телекомунікаційні мережі, а й як фактор, що зумовлює потребу у переосмисленні архітектурних рішень та стратегії управління мережею. Його всебічний аналіз є критично важливим для забезпечення ефективної інтеграції блокчейн-технологій у сучасні системи зв’язку та створення адаптивних рішень, здатних відповідати вимогам нових типів інформаційного обміну.

1.1 Інтеграція блокчейн-технологій у сучасні телекомунікаційні мережі: виклики та перспективи

Сучасні телекомунікаційні мережі функціонують в умовах стрімкого зростання обсягів передаваних даних, підвищених вимог до безпеки та надійності інформаційного обміну, а також потреби в ефективному управлінні трафіком. У цьому контексті особливу актуальність набуває впровадження технологій розподіленого реєстру, зокрема блокчейну, як одного з найбільш перспективних рішень для забезпечення децентралізованого зберігання та передачі даних [15].

Технологія розподіленого реєстру (TPP) — це узагальнений підхід до організації систем, у яких інформація фіксується, зберігається та синхронізується між багатьма учасниками (вузлами) мережі. Кожен з учасників має доступ до актуальної копії реєстру, що забезпечує прозорість, цілісність та стійкість до змін ззовні.

Блокчейн є специфічною реалізацією TPP, яка функціонує у вигляді послідовного ланцюга блоків, кожен з яких містить певний обсяг даних, хеш-посилання на попередній блок та часову мітку. Така структура гарантує незмінність записаної інформації та унеможливлює несанкціоновані зміни в системі без узгодження з іншими вузлами мережі. Надійність, децентралізованість і криптографічний захист роблять блокчейн важливим інструментом для телекомунікаційних систем, які потребують високого рівня довіри, захисту і відстежуваності транзакцій. Отже, блокчейн-технологія розглядається як перспективний компонент інформаційної інфраструктури, що здатен не лише підвищити захищеність та стабільність телекомунікаційних систем, а й оптимізувати процеси управління трафіком за рахунок надійного обміну даними між учасниками мережі.

У загальному вигляді блокчейн являє собою децентралізовану базу даних, що одночасно зберігається у вигляді ідентичних копій на багатьох пристроях однорангової (peer-to-peer) мережі. Для забезпечення актуальності та

узгодженості даних усі вузли мережі постійно синхронізуються між собою, передаючи інформацію про зміни, валідацію нових записів і включення їх до структури блоків. Варто зазначити, що архітектура блокчейн-мережі не потребує обов'язкового встановлення зв'язків між усіма вузлами («кожен з кожним»), що дає змогу ефективно масштабувати мережу [16].

Ключовою відмінністю блокчейну від традиційних баз даних є відсутність можливості редагування або видалення записаної інформації — єдиним допустимим способом внесення змін є додавання нових даних. Це забезпечує цілісність і незмінність записів.

Блокчейн-системи побудовані на принципах повної децентралізації: більшість вузлів мережі мають однакові права й функціональні можливості. Виняток становлять приватні блокчейн-мережі, що застосовуються в корпоративному секторі та мають специфічні архітектурні особливості відповідно до вимог компаній. Відсутність централізованого керуючого елементу забезпечує високу стійкість до зовнішніх впливів і здатність системи до автономного функціонування навіть у разі виходу з ладу окремих вузлів [17].

Блокчейн-технологія була розроблена з метою формування довіри між учасниками, які не мають безпосереднього зв'язку або довірених посередників. Основними її характеристиками є:

- Децентралізація — управління й зберігання даних розподілено між усіма вузлами мережі;

- Незмінність даних — криптографічний захист і множинність копій унеможливлюють несанкціоновані зміни;

- Прозорість — кожен учасник має доступ до реєстру, що забезпечує відкритість процесів;

- Стійкість до збоїв — система здатна функціонувати за наявності резервних копій, навіть при часткових відмовах.

Першою реалізацією технології блокчейн стала децентралізована платформа Bitcoin, представлена у 2008 році. Вона заклала основи для побудови

систем без потреби у центральних фінансових посередниках, на відміну від традиційних банківських платформ, що домінували на той час.

Проте справжнім технологічним проривом стала поява блокчейн-мережі Ethereum, яка запропонувала універсальну платформу для створення децентралізованих застосунків (dApps) і виконання смарт-контрактів — програмних алгоритмів, які автоматично реалізують логіку угоди за заданих умов. На відміну від Bitcoin, що орієнтований на просту передачу цифрових активів, Ethereum забезпечує розширену функціональність для розробників [18].

У 2014 році були реалізовані ключові інновації Ethereum:

- Смарт-контракти, що самостійно виконують умови договорів;

- Децентралізовані застосунки, які функціонують без централізованого контролю;

- Токени та стандарти, що спростили створення та управління цифровими активами;

- Крос-блокчейн взаємодія, яка відкрила шлях до міжмережевих рішень.

Відкритий вихідний код та гнучкість конфігурації дозволили розробникам реалізовувати як базові сценарії використання (невеликі контракти з інтерфейсом), так і розгортати адаптовані версії блокчейн-мереж — як у публічному просторі, так і в межах корпоративного контуру.

Таким чином, еволюція блокчейн-технологій сформувала різноманітні рішення, серед яких: кросчейн-протоколи, локальні підмережі в межах єдиної мережі, різні алгоритми консенсусу, мережі з різною продуктивністю, а також рішення без зберігання даних. Майже всі ці варіанти вимагають значних обчислювальних ресурсів і стабільного обсягу мережевого трафіку, що є критичними умовами ефективного функціонування блокчейн-систем у телекомунікаційному середовищі [19].

1.2 Структура та архітектура блокчейн-системи

У науково-технічному контексті блокчейн розглядається як розподілена цифрова система зберігання та обміну інформацією, що функціонує на основі криптографічно захищеного ланцюга блоків. Архітектура блокчейн-мережі має модульну, багаторівневу структуру, де кожен рівень виконує чітко визначені функції, забезпечуючи загальну узгодженість, безпечність і стійкість до змін [20].

Загалом структуру блокчейна можна описати як послідовність блоків, кожен з яких містить:

- Заголовок блоку (Block Header): включає хеш попереднього блоку, мітку часу, nonce (використовуваний у процесі майнінгу), кореневий хеш дерева Меркла (для перевірки транзакцій).

- Тіло блоку (Block Body): містить набір підтверджених транзакцій або записів, що відповідають заданим критеріям консенсусу.

- Механізми захисту: реалізовані у вигляді криптографічних алгоритмів хешування та цифрових підписів.

Архітектура блокчейн-системи базується на таких ключових компонентах:

1. Розподілена мережа (P2P-мережа) — всі вузли мережі взаємодіють у децентралізованому середовищі без наявності єдиного керуючого центру.

2. Алгоритм консенсусу — набір протоколів, що забезпечують досягнення згоди між вузлами щодо єдиного стану реєстру (наприклад, Proof of Work, Proof of Stake, Practical Byzantine Fault Tolerance тощо).

3. Смарт-контракти (за наявності) — програмні модулі, що автоматизують виконання логіки транзакцій на основі заздалегідь визначених умов.

4. Криптографічний механізм захисту — забезпечує ідентифікацію користувачів, автентичність транзакцій і цілісність даних.

5. Механізм зберігання та верифікації транзакцій — відповідає за перевірку валідності нових блоків і збереження історії транзакцій.

Таким чином, архітектура блокчейн-систем забезпечує функціонування на основі принципів децентралізації, прозорості, стійкості до фальсифікацій і надійного зберігання даних, що робить її ефективним інструментом для впровадження в сферу телекомунікацій, фінансових технологій, логістики, охорони здоров'я та інших галузей, де необхідне забезпечення довіри та захищеного обміну інформацією [21].

Блокчейн є складною децентралізованою інформаційною системою, яка складається з ряду критично важливих компонентів, кожен з яких відіграє суттєву роль у забезпеченні безпеки, надійності та функціональності мережі. Основними структурними елементами блокчейн-інфраструктури є:

1. Вузли (Nodes) — апаратні пристрої, які беруть участь у функціонуванні блокчейн-мережі. Їхня роль залежить від обчислювальних можливостей і типу реалізованого протоколу:

- Повні вузли (Full Nodes): зберігають повну копію ланцюга блоків, виконують перевірку транзакцій і блоків відповідно до правил мережі. Вони забезпечують: валідацію та підтвердження транзакцій; участь у досягненні консенсусу; повну архівацію історії блокчейна.

- Легкі вузли (Light Nodes): зберігають лише заголовки блоків і покладаються на повні вузли для перевірки транзакцій, що робить їх придатними для пристроїв з обмеженими ресурсами.

- Майнінг-вузли (Mining Nodes): беруть участь у створенні нових блоків та підтвердженні транзакцій за допомогою обчислювальних алгоритмів (Proof of Work, Proof of Stake тощо).

- Вузли-валідатори (Validator Nodes): використовуються в мережах із консенсусними алгоритмами на основі частки (наприклад, PoS) для перевірки та затвердження блоків і транзакцій.

- Делеговані вузли (Delegated Nodes): обираються іншими учасниками мережі (як у DPoS) для виконання визначених функцій, зокрема генерації блоків і підтвердження транзакцій від імені делегуючих сторін.

- Архівні вузли (Archive Nodes): зберігають повну історію станів блокчейна та надають доступ до даних, які можуть бути відсутні у поточних блоках, зокрема для цілей аналітики та аудиту.

2. Блоки (Blocks) — основна структурна одиниця для транспортування даних у системі блокчейн. Кожен блок містить:

- Заголовок блоку: хеш попереднього блоку, мітку часу, nonce та корінь дерева Меркла;

- Тіло блоку: перелік транзакцій, підтверджених у відповідному блоці.

3. Транзакції (Transactions) — елементарні одиниці запису, що фіксують передачу цифрових активів або даних між учасниками мережі. Кожна транзакція включає: адреси відправника та отримувача (унікальні ідентифікатори); обсяг переданих активів або дані щодо виконуваних функцій; криптографічний підпис, який підтверджує справжність та цілісність повідомлення.

4. Хеш-функції (Hash Functions) — математичні алгоритми, що перетворюють вхідні дані на рядок фіксованої довжини (хеш). Їх призначення: формування унікального ідентифікатора для блоку; контроль цілісності інформації — зміна будь-якого фрагмента блоку призводить до зміни хешу.

5. Алгоритми консенсусу (Consensus Mechanisms) — забезпечують досягнення єдиного бачення стану блокчейна всіма вузлами мережі. До найпоширеніших належать: Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS) тощо.

6. Дерева Меркла (Merkle Trees) — спеціалізовані структури даних, що забезпечують ефективне групування та перевірку транзакцій у блоці. Кореневий хеш дерева Меркла використовується для верифікації цілісності великої кількості записів без необхідності зберігання кожного з них.

7. Криптографічні методи (Cryptographic Methods) — забезпечують безпеку і автентичність даних у блокчейні:

- публічні та приватні ключі — використовуються для підпису транзакцій і створення криптографічних адрес;

- еліптична криптографія (ECC) — популярний метод для генерації ключів та цифрових підписів, що поєднує високий рівень захисту та ефективність за розміром ключів.

8. Смарт-контракти (Smart Contracts) — це самовиконувані програмні скрипти, що реалізують логіку угод у децентралізованому середовищі без участі посередників. Після їхнього розгортання в мережі вони не можуть бути зупинені чи змінені, що гарантує незмінність умов договору [22].

1.3 Структура мережевого пакета

Мережевий пакет є основною одиницею передавання даних у комп'ютерних мережах. Він представляє собою структурований блок інформації, який формується відповідно до протоколів мережевої моделі (наприклад, OSI або TCP/IP), і транспортується від джерела до отримувача. Кожен мережевий пакет містить службову (заголовкову) інформацію та корисні (прикладні) дані [23].

Типова структура мережевого пакета включає такі основні компоненти:

1. Заголовок (Header) — службова частина пакета, яка містить інформацію, необхідну для його правильної маршрутизації, доставки та обробки. До складу заголовка можуть входити: MAC-адреси відправника та одержувача (на канальному рівні); IP-адреси джерела та призначення (на мережевому рівні); Номери портів (на транспортному рівні); Прапорці керування, ідентифікатори сесії, номера послідовності тощо.

2. Тіло (Payload/Data) — основна інформаційна частина пакета, що містить корисні дані, які передаються між прикладними рівнями вузлів-учасників.

3. Контрольна сума (Checksum/CRC) — використовується для перевірки цілісності пакета після його доставки, що дозволяє виявити пошкодження даних під час передавання.

4. Завершальний фрагмент (Trailer) — необов'язкова частина, яка може містити додаткову інформацію для перевірки цілісності або завершення сеансу

передачі (найчастіше використовується в специфічних протоколах, наприклад, Ethernet).

З мережевого погляду, передавання інформації в розподілених системах може здійснюватися з використанням транспортних протоколів UDP або TCP. У межах цього дослідження було виконано захоплення та аналіз мережевого трафіку, сформованого в приватній блокчейн-мережі, яка функціонує на базі клієнта з відкритим програмним кодом. Конфігурація цієї мережі імітує структури таких популярних екосистем, як Ethereum, TON та Cardano.

Зазначені мережі були обрані для дослідження через їхню широку популярність та активне використання у практичних реалізаціях блокчейн-рішень.

Захоплення мережевих пакетів здійснювалося за допомогою інструменту Wireshark, при цьому для кожної з блокчейн-мереж були розроблені спеціалізовані протокольні дисектори. Протокольні дисектори — це модулі, які дозволяють інструменту Wireshark інтерпретувати структуру пакетів, розкладаючи їх на окремі поля. Такий підхід забезпечує можливість створення гнучких фільтрів для аналізу даних на основі конкретних атрибутів протоколів.

У якості референсного рішення було обрано мережу Ethereum — одну з найпоширеніших блокчейн-систем, що активно використовується завдяки відкритому вихідному коду, віртуальній машині Ethereum (EVM) та **підтримці смарт-контрактів. Ethereum реалізує алгоритм консенсусу Proof-of-Stake (PoS) і має ключову особливість — наявність глобального стану мережі, що полегшує розробку та інтеграцію додаткових функцій.

Мережеві з’єднання між одноранговими вузлами, які використовують клієнт Ethereum, формуються за допомогою протоколу devp2p, на основі якого побудована однорангова (peer-to-peer) топологія. Вузли devp2p можуть як ініціювати, так і приймати з’єднання через довільні TCP-порти. Виявлення нових вузлів здійснюється через протоколи виявлення discv4/discv5 [24].

Протокол devp2p підтримує два режими роботи:

- Основний режим — використовує TCP як транспортний протокол для стабільної передачі даних.

- Режим виявлення — реалізований на базі UDP і відповідає за початкове виявлення інших вузлів у мережі.

У режимі виявлення клієнт підключається до спеціальних вузлів початкового завантаження (bootstrap nodes), які надають список потенційних однорангових вузлів для встановлення з'єднань. Після синхронізації з такими вузлами клієнт отримує додаткову інформацію про структуру мережі та її актуальний стан. У межах проведеного аналізу було досліджено структуру мережевого пакета протоколу devp2p (див. рисунок 1.1), а також розглянуто приклад пакета з передаванням транзакції (див. рисунок 1.2) [25].

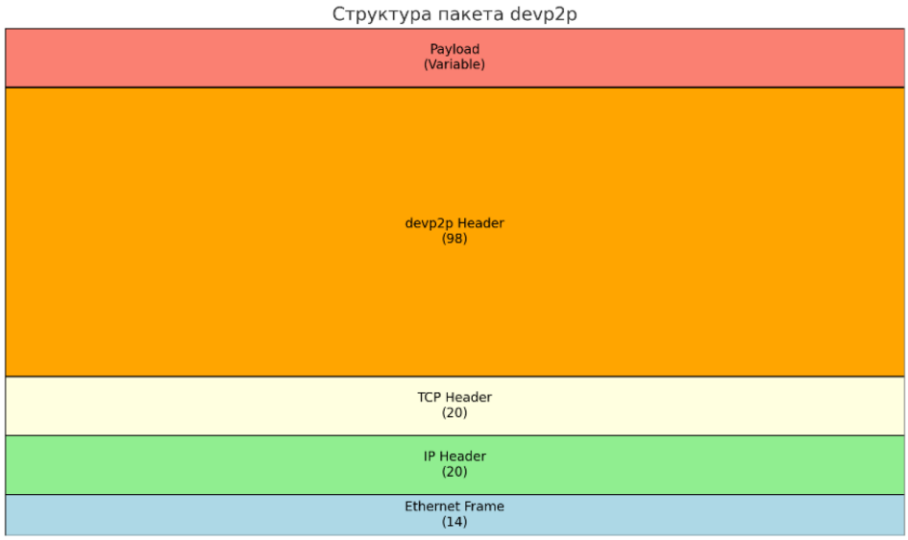

Рисунок 1.1 – Формат пакета протоколу devp2p у мережі блокчейна Ethereum (у дужках зазначено розмір у байтах)

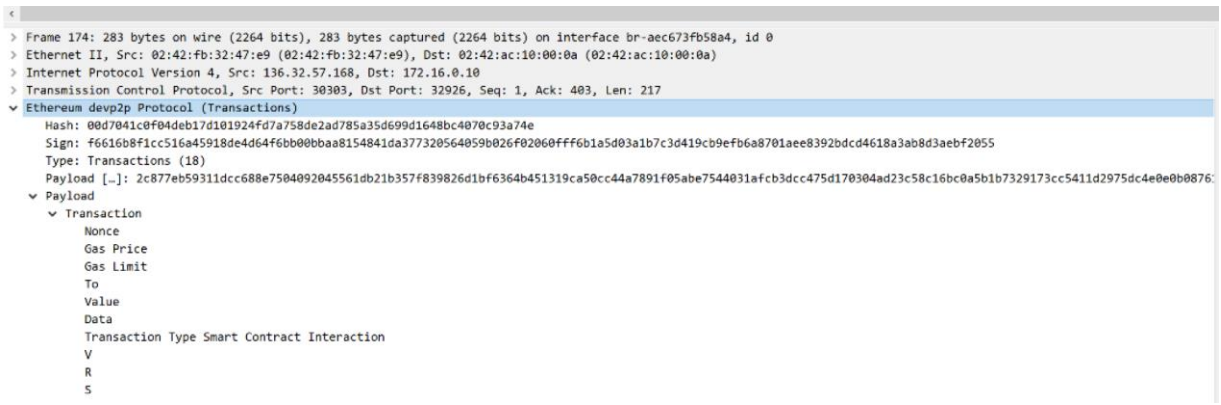

Рисунок 1.2 – Формат мережевого пакета, що використовується для передачі транзакцій у протоколі Ethereum

Заголовок TCP/IP містить кілька ключових компонентів:

- Кадр Ethernet — обгортка на канальному рівні, яка включає MAC-адреси відправника і одержувача.

- IP-заголовок — містить IP-адреси джерела та призначення, забезпечуючи маршрутизацію пакетів у мережі.

- TCP-заголовок — відповідає за керування з’єднанням, містить порти джерела та призначення, а також службову інформацію для забезпечення надійної доставки.

Протокол `devp2p` є основним механізмом однорангової (peer-to-peer) комунікації в мережі Ethereum. Заголовок пакета `devp2p` включає наступні поля:

- Hash (32 байти) — геш повідомлення, що використовується для перевірки цілісності пакета.

- Signature (Sign) (65 байт) — цифровий підпис відправника, який використовується для перевірки автентичності джерела.

- Type (1 байт) — ідентифікатор типу повідомлення, який визначає його зміст: блок, транзакція або повідомлення для виявлення сусідніх вузлів (discovery).

Зміст корисного навантаження залежить від типу повідомлення. Для транзакційної передачі структура має такий вигляд:

- Nonce — порядковий номер транзакції.

- Gas Price — ціна за одиницю обчислювального ресурсу (газу).

- Gas Limit — обмеження на споживання газу.

- To — адреса одержувача.

- Value — сума переказу.

- Data — додаткові дані (наприклад, виклики функцій смарт-контракту).

- V, R, S — компоненти цифрового підпису.

Варто зазначити, що в класичних транзакціях переказу значення поля `Data` зазвичай є порожнім. Натомість у транзакціях, що взаємодіють зі смарт-контрактами, поле `Data` містить інформацію про виклик функцій, що може слугувати непрямою ознакою типу транзакції. Це дозволяє пріоритезувати складні транзакції у разі аналізу мережевого трафіку [26].

Результати аналізу показали, що блоки передаються у декількох пакетах, оскільки їхній розмір може сягати 350 КБ. При максимальному розмірі мережевого пакета 1500 байт блок потребує розбиття на понад 266 пакетів. У середньому нові блоки генеруються кожні 12–14 секунд, що призводить до створення мережевого навантаження на рівні близько 20 пакетів за секунду або приблизно 235 кбіт/с. Для блоків розміром 1 МБ ці показники зростають до 53 пакетів або 631 кбіт/с.

Типова транзакція переказу (розміром ≈245 байт) зазвичай уміщується в один пакет, займаючи близько 40% його об’єму. У свою чергу, транзакції, пов’язані зі смарт-контрактами, мають середній розмір понад 350 байт і займають приблизно 50% пакета. Таким чином, доступна область для корисного навантаження блоку становить близько 1348 байт, що відповідає приблизно 90% загального розміру пакета [27].

TON (The Open Network) — це децентралізована та відкрита інтернет-платформа, що включає такі компоненти, як TON Blockchain, TON DNS, TON Storage та TON Sites. Основою екосистеми є TON Blockchain, який функціонує як розподілений суперкомп’ютер або «суперсервер» з підтримкою алгоритму консенсусу PoS.

TON орієнтований на високу масштабованість, забезпечення кросс-чейн взаємодії та обслуговування мільйонів транзакцій за секунду. Система побудована за принципом віртуальної машини, подібно до Ethereum, і спрямована на формування нового децентралізованого інтернету.

В результаті дослідження було проаналізовано структуру пакета передачі в TON, зокрема особливості передавання транзакцій. Візуальні приклади структури подано на рисунках 1.3 та 1.4 [28].

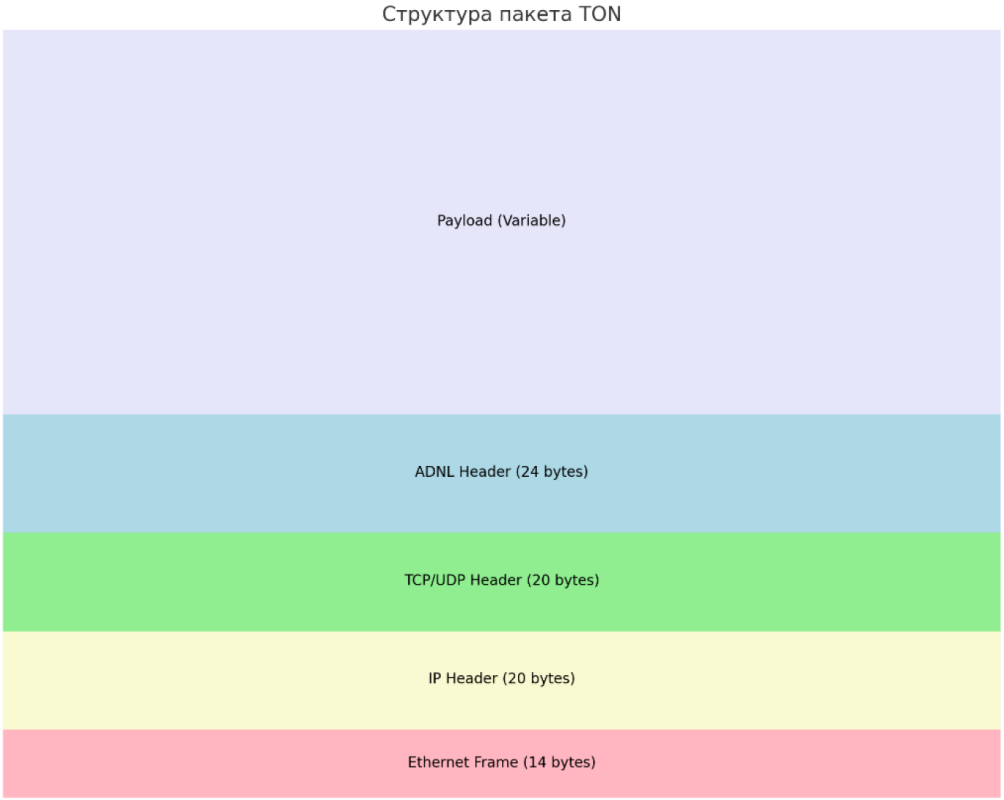

Рисунок 1.3 – Структура пакета передачі даних у мережі TON (розмір полів наведено у байтах)

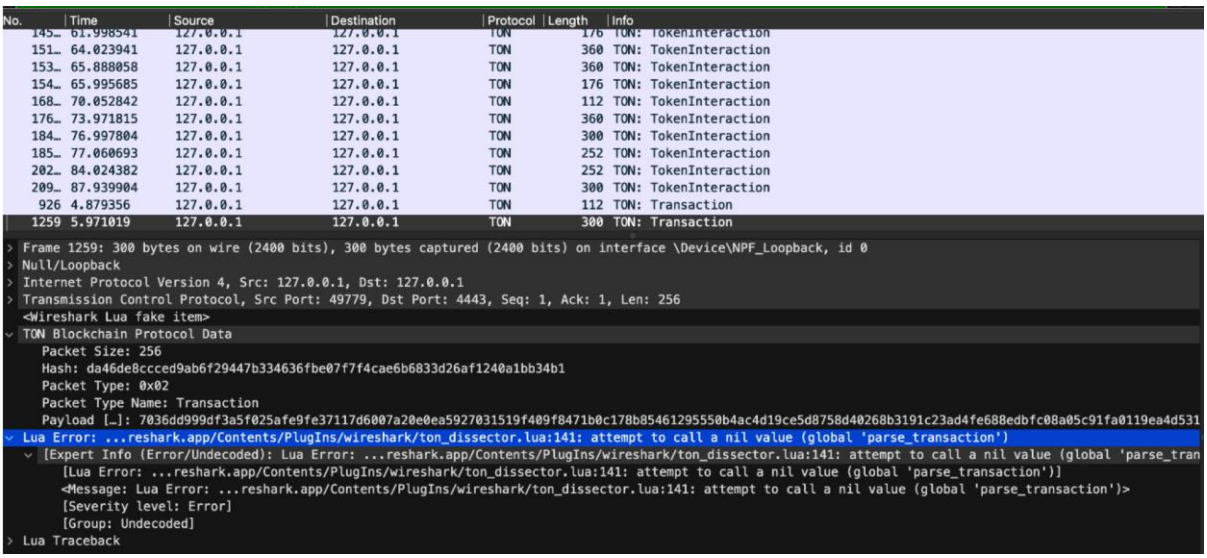

Рисунок 1.4 – Структура мережевого пакета, призначеного для передачі транзакцій у системі TON Blockchain

Передача транзакцій у мережі TON (The Open Network) реалізується через спеціалізовану мережеву інфраструктуру, яка базується на використанні протоколу ADNL (Abstract Datagram Network Layer) поверх класичної моделі TCP/IP. Нижче описано основні компоненти такого пакета.

Мережеве з'єднання організовується відповідно до стандартної моделі OSI, де на канальному, мережевому та транспортному рівнях використовуються такі заголовки:

- Ethernet Frame – кадр канального рівня, що містить MAC-адреси відправника і одержувача (14 байт).

- IP Header – IP-заголовок мережевого рівня, що включає IP-адреси джерела та призначення (20 байт для IPv4 без опцій).

- TCP/UDP Header – транспортний заголовок, який містить інформацію про порти джерела та призначення. Для TCP — 20 байт, для UDP — 8 байт.

ADNL є базовим транспортним протоколом у мережі TON, який забезпечує маршрутизацію, захист даних та підтримку сесійної передачі. Його структура включає:

- Magic Number – унікальний 32-бітовий ідентифікатор, що позначає тип протоколу.

- Session ID – ідентифікатор сесії, який дозволяє встановити безпечне з’єднання між вузлами.

- Message Length – довжина повідомлення в байтах.

- Message Type – однобайтовий індикатор типу переданого повідомлення (наприклад, транзакція, блок, запит стану тощо).

- Checksum / Hash – контрольна сума або хеш повідомлення для перевірки цілісності.

Загальний розмір заголовка ADNL варіюється залежно від реалізації, орієнтовно становить близько 24 байт.

Вміст корисного навантаження залежить від типу повідомлення. У разі передачі транзакції можуть бути включені такі дані: Ідентифікатор транзакції; Параметри одержувача; Сума переказу; Додаткові дані для взаємодії зі смарт-контрактами; Підпис відправника тощо.

У випадку передачі блоків, які можуть досягати сотень кілобайт, використовується механізм розбиття на пакети, які згодом реструктуризуються на приймаючому боці. Для цього застосовується механізм Bag of Cells (BoC) — спеціалізований формат серіалізації, оптимізований для передачі складних структур даних у TON. BoC забезпечує компактність і цілісність структури даних, а також зменшує надмірність [29].

Максимальний розмір одного Ethernet-пакета (MTU) становить 1500 байт. Сумарний обсяг заголовків (Ethernet + IP + TCP + ADNL) — приблизно 78 байт. Таким чином, доступна корисна частина становить приблизно 1422 байти, що складає близько 95% від усього пакета.

За результатами дослідження:

- Середній розмір простої транзакції (переказ без взаємодії зі смарт-контрактом) становить 250–300 байт, тобто займає близько 20% доступного простору.

- Середній розмір транзакцій, пов’язаних зі смарт-контрактами, — 400–600 байт, що відповідає 30–40% корисного навантаження.

- Передача блоків є більш варіативною: їх розмір може коливатися від декількох до сотень кілобайт. Відповідно, один блок може бути розбитий на десятки або сотні мережевих пакетів [30].

1.4 Висновки до розділу 1

Описано базовий сценарій функціонування процесів у блокчейн-мережі. Проведено дослідження мережевого трафіку, що виникає під час синхронізації вузлів блокчейн-мереж, зокрема під час завантаження блоків у мережах Ethereum, TON та Cardano, а також при передачі транзакцій. Надано структури мережевих пакетів, характерних для блокчейн-трафіку. Здійснено аналіз заголовків та полів корисного навантаження при передачі як окремих транзакцій, так і блоків, що містять транзакції. Виконано обчислення та порівняльний аналіз навантаження на пропускну здатність мережі при передачі блокчейн-трафіку. Оцінено обсяг переданих даних у контексті різних типів доступу до мережі Інтернет.

2 АНАЛІЗ ВПЛИВУ АЛГОРИТМІВ КОНСЕНСУСУ НА ПРОДУКТИВНІСТЬ КОМУНІКАЦІЙНИХ МЕРЕЖ

Алгоритми консенсусу є невід'ємною складовою блокчейн-систем, характеризуючись різноманітною логікою функціонування та механізмами прийняття рішень. Особливості реалізації цих алгоритмів безпосередньо впливають на обсяг генерованого мережевого трафіку, а також визначають необхідність виконання додаткових дій з боку інших учасників мережі, зокрема процедур валідації або голосування. Це, у свою чергу, обумовлює потребу в дублюванні переданих даних або створенні додаткового навантаження задля забезпечення відповідності вимогам обраного механізму досягнення консенсусу.

2.1 Поняття алгоритму консенсусу

Алгоритм консенсусу — це формалізований набір правил, що використовується в децентралізованих обчислювальних системах і дозволяє вузлам (учасникам мережі) досягати узгодженого стану даних та приймати спільне рішення щодо додавання нових записів (зокрема, транзакцій або блоків) до розподіленого реєстру. Такий алгоритм забезпечує синхронізацію інформації між усіма учасниками системи, запобігає конфліктам та гарантує цілісність і безпеку даних [27].

Основною функцією алгоритму консенсусу є забезпечення узгодженості даних, тобто гарантія того, що всі вузли мають однакову версію стану системи. Це є критично важливим для стабільної роботи децентралізованих платформ, а також для забезпечення захисту від збоїв і зловмисних дій, зокрема атак типу «подвійне витрачання». Консенсус-механізм гарантує, що до блокчейну додаються лише валідні транзакції, які відповідають встановленим правилам.

Алгоритми консенсусу відіграють ключову роль у функціонуванні блокчейн-мереж, оскільки дозволяють вузлам асинхронно перевіряти та узгоджувати транзакції без необхідності довіри між учасниками [28]. Важливо

зазначити відмінність між відносно повільним процесом створення блоку або пошуку коректного хешу (як, наприклад, у Proof of Work) і швидкою валідацією вже згенерованого хешу іншими учасниками мережі.

Функціонування алгоритму консенсусу можна поділити на кілька послідовних етапів:

1. Ініціація — один або декілька вузлів ініціюють процес, пропонуючи до розгляду нову транзакцію чи блок.

2. Розповсюдження даних — запропоновані дані передаються іншим вузлам мережі для перевірки.

3. Перевірка — кожен вузол перевіряє коректність даних відповідно до встановлених протоколів (включаючи перевірку цифрових підписів, наявність коштів тощо).

4. Голосування — учасники мережі голосують за прийняття або відхилення блоку. Механізм голосування залежить від конкретного типу алгоритму консенсусу: це може бути як вирішення складної обчислювальної задачі, так і очікування своєї черги відповідно до заздалегідь визначеного порядку.

5. Досягнення консенсусу — за визначених умов (наприклад, досягнення певного кворуму) учасники погоджуються щодо нового стану мережі.

6. Додавання до блокчейну — погоджений блок приєднується до ланцюга, а вузли оновлюють локальні копії реєстру.

7. Оновлення стану системи — мережа переходить до нового стану, і обробка наступних транзакцій триває вже на оновленій основі.

2.2 Класифікація (сімейства) алгоритмів консенсусу

На сьогодні існує значна кількість варіацій алгоритмів досягнення консенсусу. Варто зазначити, що створення принципово нових механізмів є досить складним завданням, тому більшість сучасних алгоритмів базуються на вже відомих підходах, які піддаються оптимізації або адаптації до специфічних умов функціонування розподілених систем. З огляду на це, доцільним є

групування (класифікація) алгоритмів за подібністю принципів їх дії та ключових механізмів прийняття рішень [5].

У межах дослідження було застосовано класифікацію алгоритмів консенсусу за характером основного механізму роботи [27], що включає наступні категорії:

1. Алгоритми з візантійською відмовостійкістю [29, 30]: BFT (Byzantine Fault Tolerance); FBA (Federated Byzantine Agreement); PBFT (Practical Byzantine Fault Tolerance); DBFT (Delegated Byzantine Fault Tolerance); SBFT (Simplified Byzantine Fault Tolerance).

2. PoS-подібні алгоритми [31]: DPoS (Delegated Proof of Stake); LPoS (Leased Proof of Stake); PoAuth (Proof of Authority); PoI (Proof of Importance); PoWeight (Proof of Weight); PoR (Proof of Reputation).

3. PoW-подібні алгоритми: PoB (Proof of Burn); PoET (Proof of Elapsed Time); PoC (Proof of Capacity); PoA (Proof of Activity).

4. Альтернативні алгоритми з унікальною механікою: PoRes (Proof of Research); DAG (Directed Acyclic Graph).

Зважаючи на те, що більшість алгоритмів консенсусу відтворюють базову логіку з певними адаптаціями, для подальшого дослідження були обрані найбільш репрезентативні з різних категорій: PoW, PoS, DPoS, PBFT, PoR, PoA, PoET та FBA. Ці алгоритми реалізують ключові механіки трьох основних типів (візантійська відмовостійкість, доказ частки, доказ роботи). Алгоритми з категорії альтернативних підходів до консенсусу не були включені до моделювання, оскільки вони, як правило, мають вузькоспеціалізоване призначення та не адаптовані до типових сценаріїв роботи блокчейн-систем загального призначення.

З метою оцінки впливу обраних алгоритмів консенсусу на характеристики мережі зв’язку було проведено моделювання за допомогою мови програмування Python. У межах симуляції були реалізовані програмні класи, що описують основну логіку кожного з алгоритмів консенсусу. На рисунку 2.1 представлено результати моделювання, які демонструють вплив алгоритмів PoW, PoS, PoET та

DPoS на наповнення пулу непідтверджених транзакцій — параметра, що є показовим з точки зору обсягу оброблюваних даних у системі. Накопичення в пулі свідчить про формування черги, а його переповнення — про втрату транзакцій, які не можуть бути збережені та, відповідно, не будуть доступні вузлам для обробки та включення до блоків.

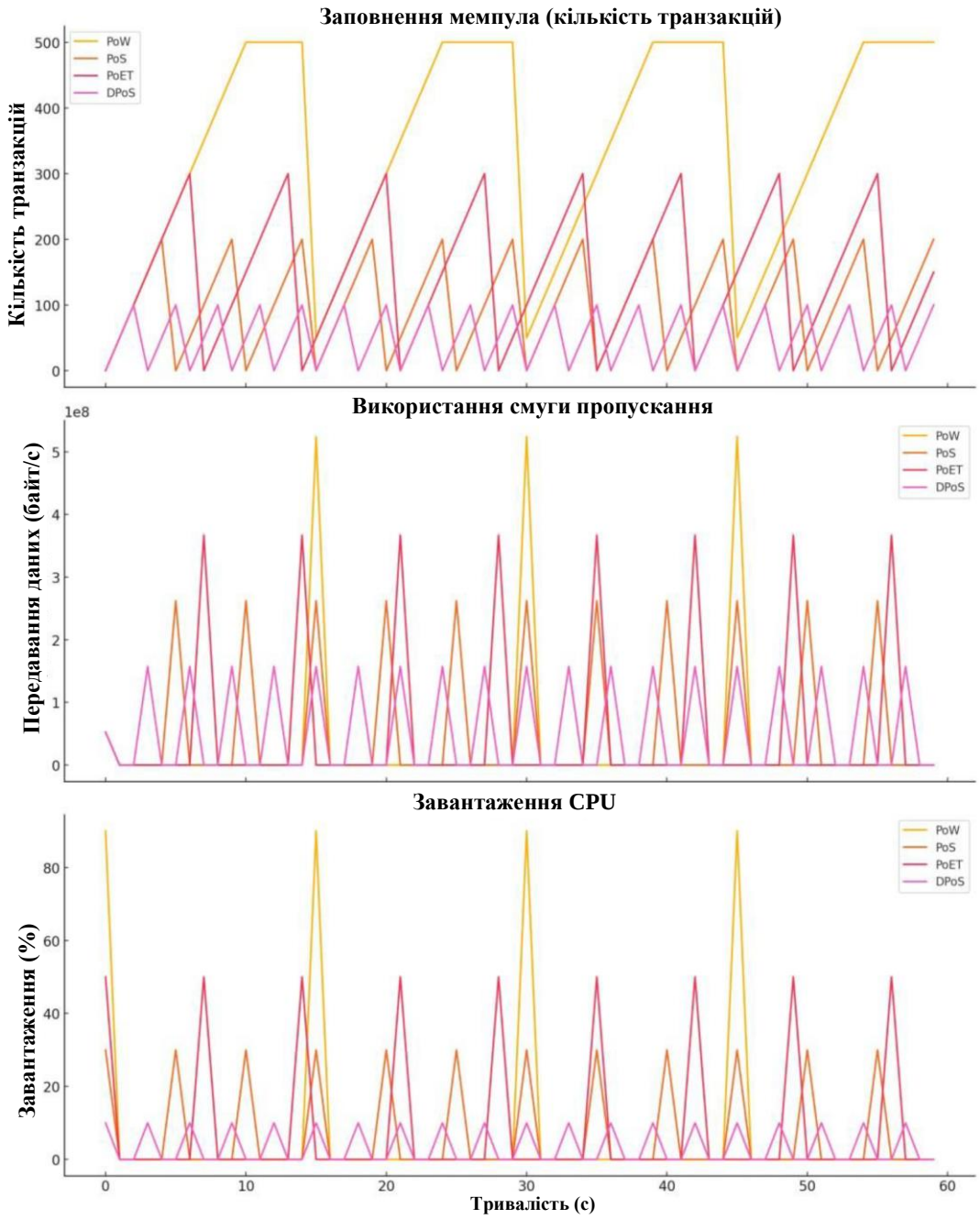

Рисунок 2.1 – Оцінювання впливу алгоритмів консенсусу на ключові параметри функціонування мережі

Висновки за результатами аналізу графіка заповнення пулу непідтверджених транзакцій: PoW: спостерігається постійне накопичення транзакцій з періодичним очищенням кожні 15 секунд; PoS: очищення відбувається частіше (кожні 5 секунд), що знижує рівень накопичення транзакцій; PoET: демонструє середній рівень заповнення пулу з рівномірним очищенням; DPoS: практично відсутнє накопичення транзакцій завдяки високій частоті їх обробки.

Висновки за результатами аналізу графіка використання смуги пропускання: PoW: наявні високі імпульсні навантаження кожні 15 секунд через передачу великих блоків; PoS і PoET: фіксуються помірні рівномірні навантаження завдяки меншому інтервалу між блоками; DPoS: характерні низькі, але часті передачі, що мінімізують навантаження на мережу.

Ось науково-технічний переклад та перефразування вашого фрагмента українською мовою, адаптованого для включення до розділу експериментального аналізу в дипломній роботі:

Аналіз графіка, що відображає завантаження центрального процесора (CPU) під час моделювання, дозволяє зробити такі висновки:

- PoW (Proof of Work): демонструє високе навантаження на процесор через потребу у виконанні великої кількості обчислень для пошуку хешу, який відповідає складності.

- PoS (Proof of Stake) та PoET (Proof of Elapsed Time): характеризуються помірним навантаженням, що відповідає меншій інтенсивності обчислювальних операцій.

- DPoS (Delegated Proof of Stake): показує мінімальне використання процесора, оскільки участь у створенні блоків делегована обмеженій кількості вузлів, і обчислювальні операції значною мірою спрощені.

Отримані результати наочно демонструють відмінності у продуктивності алгоритмів консенсусу та їх вплив на обчислювальні ресурси вузлів мережі. Спостерігається явне розділення між підходами з високим енергоспоживанням (PoW) та менш ресурсоємними рішеннями (PoS, PoET, DPoS). Особливу увагу

слід приділити алгоритму PoW, який, попри високі обчислювальні витрати, має важливу перевагу у вигляді механізму адаптивного регулювання складності. Ця властивість забезпечує стабільний час створення блоків і дозволяє: зменшити навантаження на валідаційні вузли; уникати пікового перевантаження мережі; ефективно реагувати на аномальну транзакційну активність, зокрема при можливих атаках типу Denial of Service (DoS), рівномірно розподіляючи навантаження між вузлами та утруднюючи проведення таких атак.

Проведене моделювання підтвердило суттєві відмінності у впливі алгоритмів консенсусу на параметри функціонування мережі зв’язку, а також продемонструвало потенціал динамічного вибору алгоритму залежно від поточного стану мережі. Такий підхід дозволяє адаптивно регулювати навантаження, підвищуючи ефективність та стабільність функціонування децентралізованої системи.

2.3 Інтенсивність використання апаратної інфраструктури

У рамках дослідження навантаження на апаратні ресурси було проведено експеримент, що передбачав вимірювання рівня завантаження центрального процесора, оперативної пам’яті та накопичувача (жорсткого диска) під час генерації порожніх блоків у розгорнутій приватній блокчейн-мережі з типовою конфігурацією. Параметри конфігурації включали: інтервал генерації блоків – 12–14 секунд; максимальний розмір блока – до 350 КБайт (порожній блок – близько 152 байт); використання алгоритму консенсусу Proof of Stake (PoS).

Застосування порожніх блоків у даному дослідженні обумовлено потребою у демонстрації мінімальних вимог до ресурсів для обраного механізму консенсусу. Це дозволило виключити вплив обробки транзакцій та оцінити базове навантаження, зумовлене лише самим механізмом PoS.

На рисунку 2.2 подано графіки, що відображають динаміку використання апаратних ресурсів під час роботи мережі.

Рисунок 2.2 – Графіки вимірювання навантаження блокчейн-мережі при генерації порожніх блоків

За результатами експерименту встановлено, що врахування апаратного навантаження є критично важливим при проектуванні та виборі алгоритму консенсусу. Навіть за умов генерації порожніх блоків, алгоритм PoS демонструє відносно високе навантаження на процесор, що може призводити до: зменшення продуктивності вузла; сповільнення обробки інших мережевих процесів, не пов’язаних із блокчейн-компонентом; нераціонального використання ресурсів у періоди низької транзакційної активності. Таким чином, в умовах простоїв або обмеженої доступності обчислювальних потужностей, доцільно розглядати можливість адаптивного вибору більш оптимального алгоритму консенсусу, зокрема такого, що мінімізує вплив на апаратні компоненти системи.

Для забезпечення коректності експерименту було проведено вимірювання трьох рівнів навантаження на той самий вузол мережі: низького, середнього та високого. Для цього був створений модельний тестовий стенд, схема якого наведена на рисунку 2.3.

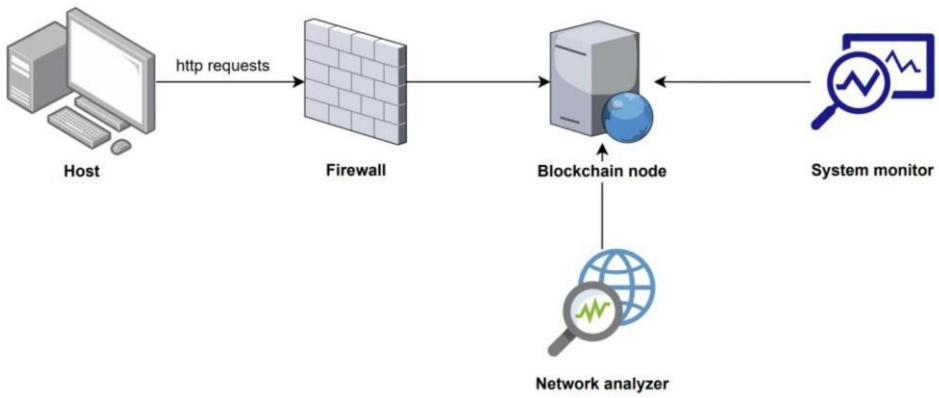

Рисунок 2.3 – Схема моделі системи для вимірювання змін апаратних параметрів обладнання з вузлом блокчейн-мережі

Для оцінки реакції апаратного забезпечення сервера, на якому розгорнуто вузол блокчейн-мережі, було проведено тестування з використанням 10, 1000 та 1500 паралельних потоків, які безперервно викликали метод sendTransaction, генеруючи транзакційне навантаження.

За результатами вимірювань встановлено, що в одному потоці в середньому за одну секунду відправляється 7 транзакцій. Відповідно, кількість запитів до вузла блокчейн-мережі в межах одного потоку становить 7 транзакцій на секунду. Для 10, 1000 та 1500 потоків ця величина складає відповідно 70, 7000 та 10500 викликів методу відправки транзакцій на секунду.

Схема відправки запитів у межах паралельних потоків наведена на рисунку 2.4. Спочатку в основному потоці здійснюється підключення до вузла блокчейн-мережі, потім відбувається підготовка даних для транзакцій (обсяг газу, адреси, приватний ключ для підпису транзакції), після чого в окремих потоках запускається процес відправки транзакцій.

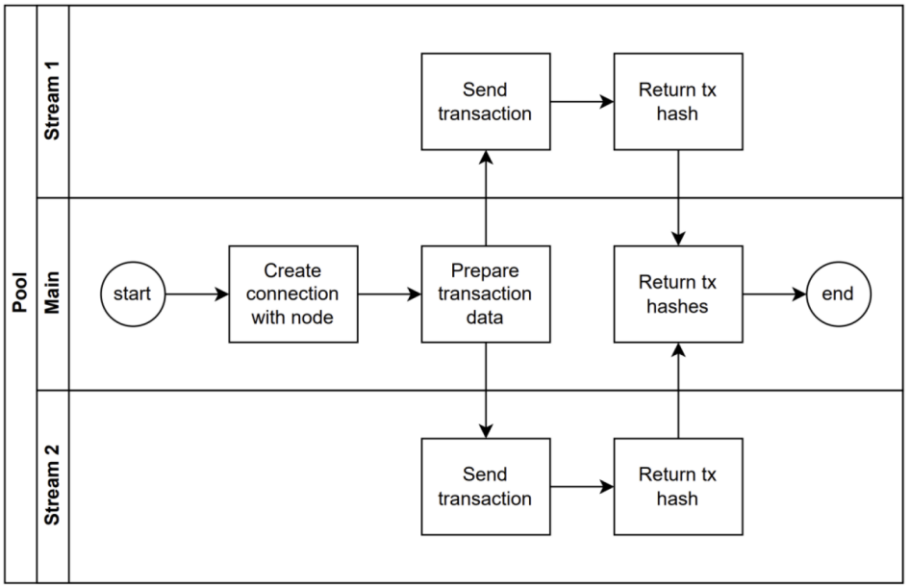

Рисунок 2.4 – Схема відправлення транзакцій в межах паралельних потоків

На рисунку 2.5 наведено результати вимірювання навантаження на апаратне забезпечення вузла блокчейн-мережі під час тестування з 10 паралельними потоками.

Графіки свідчать, що параметри навантаження практично не відрізняються від стану простою: завантаження CPU та оперативної пам’яті (RAM) залишаються без суттєвих змін.

Рисунок 2.5 – Результати вимірювання навантаження при 10 паралельних потоках

Водночас фіксується невелике зростання обсягу мережевого трафіку та кількості переданих пакетів, пік якого досягає 1300 пакетів на секунду.

На рисунку 2.6 представлено результати реакції апаратних компонентів при запуску 1000 паралельних потоків.

У цьому випадку спостерігається різке зростання завантаження центрального процесора (CPU) з 8–10% до 75–78%. Споживання оперативної пам’яті (RAM) також зростає майже вдвічі — з 1,8 ГБ до 3 ГБ.

Крім того, значно зростає мережеве навантаження, а кількість мережевих пакетів у піковому значенні сягає 26 000 пакетів на секунду.

Ось переклад і адаптація тексту українською мовою у науково-технічному стилі для включення в дипломну роботу:

Під час тестування з 1500 паралельними потоками на графіках фіксується зростання всіх основних метрик навантаження. Завантаження центрального процесора (CPU) збільшується до 75–78%, а в пікових значеннях досягає 80%. Споживання оперативної пам’яті (RAM) зростає до 3,8 ГБ. Також суттєво зростає обсяг мережевого трафіку та кількість мережевих пакетів, пік якої становить 17 400 пакетів на секунду. Порівняльний аналіз з експериментом, що включав 1000 паралельних потоків, демонструє цікаву особливість: при 1000 потоках спостерігається більше навантаження на мережу, проте менше споживання оперативної пам’яті, ніж при 1500 потоках.

Цей факт свідчить про активацію механізмів внутрішньої оптимізації, які допомагають обробляти надмірне навантаження на мережу. Подібна поведінка є особливістю реалізації конкретного клієнта блокчейн-мережі.

На рисунку 2.7 демонструється результат аналогічного експерименту із запуском 1500 паралельних потоків, що дозволяє оцінити поведінку вузла при ще більш інтенсивному транзакційному навантаженні.

У межах розглянутої концепції передбачається, що вузли блокчейн-мережі можуть бути розміщені безпосередньо на мережевому обладнанні [32] (рисунок 2.8).

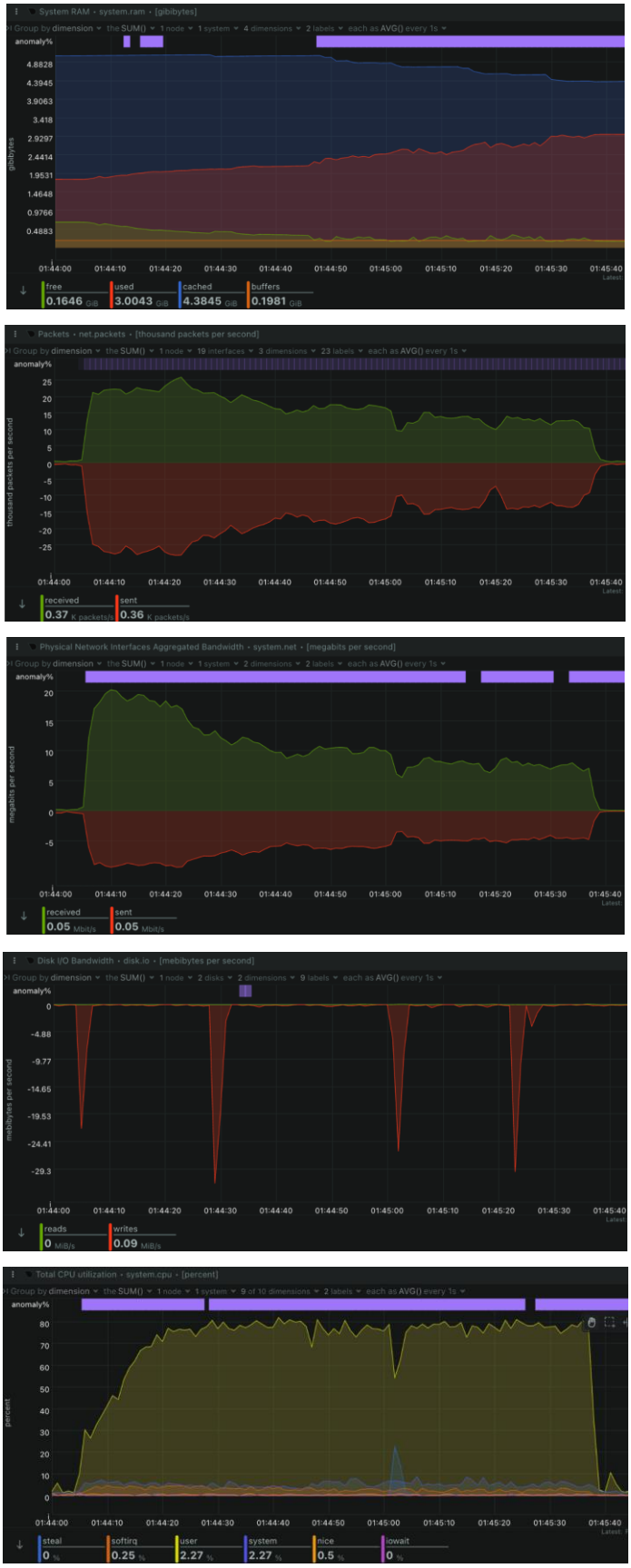

Рисунок 2.6 – Результати вимірювання навантаження при 1000 паралельних потоках

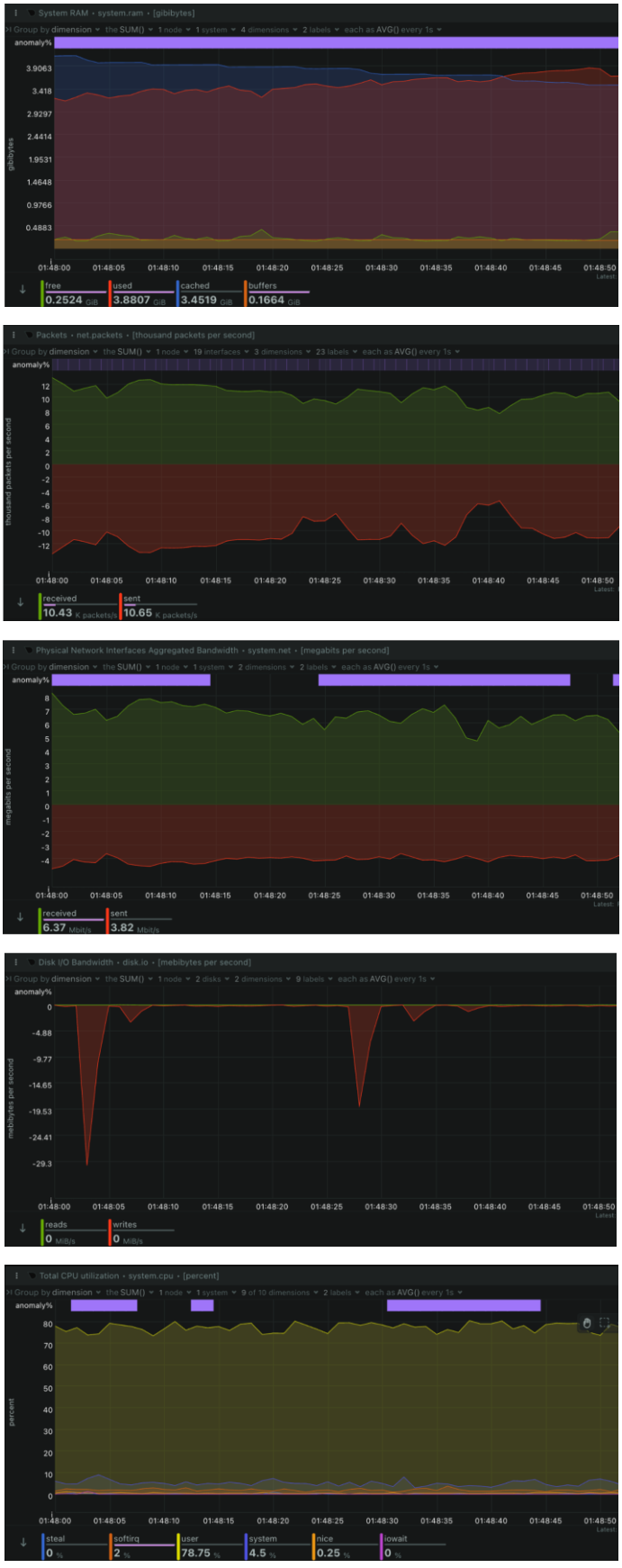

Рисунок 2.7 – Результати вимірювання навантаження при 1500 паралельних потоках

Блокчейн-вузол функціонує на рівні прикладного шару (рівень 7 моделі OSI). Для його повноцінної роботи необхідна надійна підтримка на мережевому рівні (рівень 3) та транспортному рівні (рівень 4), з використанням відповідних протоколів IP та TCP/UDP. Таким чином, інтеграція блокчейн-вузла відбувається на рівні мережевої інфраструктури, починаючи з рівня 3, з особливою увагою до стабільності та ефективності з'єднання на рівнях 3 і 4, що є критичними для забезпечення безперервного функціонування прикладного рівня.

Для оцінки можливості використання мережевого обладнання для розгортання сучасних реалізацій блокчейн-клієнтів розглянуто модель маршрутизатора Cisco ISR 4451-X, яка належить до високопродуктивного мережевого обладнання корпоративного класу. Основні технічні характеристики наведено нижче: Процесор (CPU): багатоядерний процесор з тактовою частотою приблизно 2.5 ГГц; Оперативна пам'ять (RAM): від 8 до 16 ГБ; Пропускна здатність: до 10 Гбіт/с з увімкненими сервісами; Середнє навантаження на CPU: при середньому навантаженні — 30–50%; при піковому навантаженні — 70–90%. Призначення пристрою: забезпечення високошвидкісної маршрутизації з підтримкою розширених мережевих сервісів, зокрема VPN, QoS, фільтрації трафіку (Firewall) та ін.

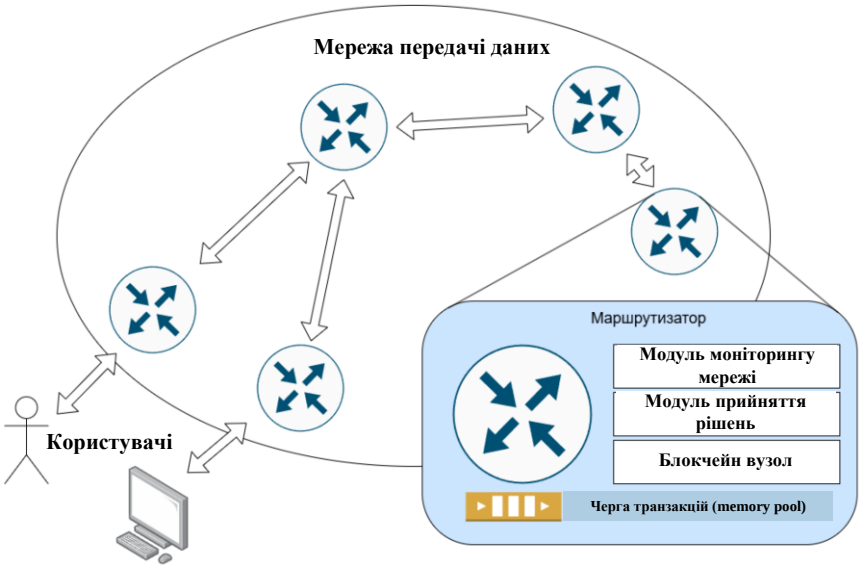

Рисунок 2.8 – Архітектура мережі зв'язку з інтегрованим блокчейн-шаром та модулем адаптивного алгоритму консенсусу

Для оцінки можливості використання мережевого обладнання у реалізаціях сучасних блокчейн-клієнтів розглянемо технічні характеристики комутатора серії Cisco Catalyst 9500: Центральний процесор (CPU): спеціалізовані мікросхеми (ASIC), оптимізовані для високошвидкісної обробки трафіку; Оперативна пам’ять: 16 ГБ; Пропускна здатність: до 480 Гбіт/с; Середнє завантаження процесора: при типовому навантаженні: 5–15% (основне навантаження пов'язане з управлінськими функціями), при піковому навантаженні: 20–30%. Дане обладнання призначене для високошвидкісної комутації в ядрах мереж з підтримкою базових функцій маршрутизації.

Паралельно, розглянемо офіційні вимоги до апаратного забезпечення повноцінного вузла блокчейн-мережі Ethereum (у режимі основної мережі з повною синхронізацією даних та обробкою транзакцій): Процесор: від 4 ядер; Оперативна пам’ять: 8–16 ГБ; Накопичувач: щонайменше 1 ТБ; Мережеве підключення: від 25 Мбіт/с, бажано провідне. Слід зазначити, що мережа Ethereum є однією з найнавантаженіших публічних блокчейн-мереж, із щоденним обсягом транзакцій на надзвичайно високому рівні [11]. Тому вимоги до повного вузла не завжди коректно екстраполювати на більш легкі клієнти, які, ймовірно, використовуватимуться у розподіленій мережевій архітектурі, виконуючи лише обмежену функціональність, зокрема ретрансляцію або підпис транзакцій. Попри це, навіть за наведених вимог до вузла основної мережі, розміщення блокчейн-вузлів на мережевому обладнанні із достатньою продуктивністю є технічно можливим. Крім того, в окремих випадках доцільним є використання спеціалізованих апаратних платформ, призначених для функціонування в якості блокчейн-вузлів, що наведено на рисунку 2.8.

З урахуванням зростання популярності децентралізованих систем та обмежень традиційних архітектур, доцільним є розгляд альтернативної схеми підключення блокчейн-вузлів до мережі зв’язку, орієнтованої на підвищення ефективності, гнучкості та адаптивності. На рисунку 2.9 відображено альтернативну модель, у якій блокчейн-шар інтегрується не лише на прикладному рівні (рівень 7 OSI), а частково переносить елементи логіки

консенсусу на прикордонні вузли мережі, зокрема на рівень шлюзів, маршрутизаторів та SDN-контролерів.

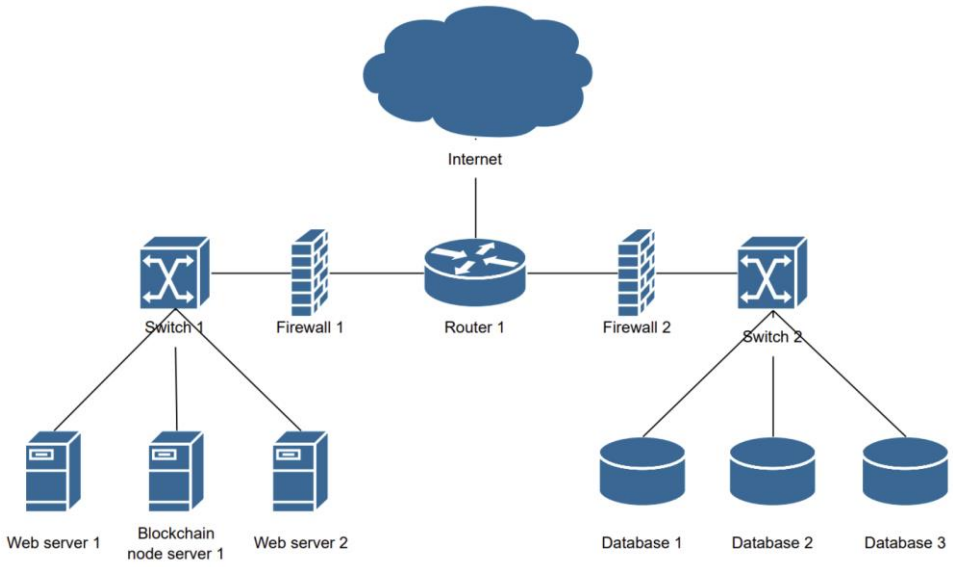

Рисунок 2.9 – Альтернативна схема інтеграції блокчейн-механізмів у мережеву інфраструктуру

Основні особливості альтернативної схеми:

- Гібридна реалізація вузлів: частина функціоналу блокчейн-вузла (наприклад, обробка транзакцій, шифрування, кешування) виконується на мережевому обладнанні за допомогою спеціалізованих модулів або віртуалізованих контейнерів.

- Використання SDN (Software Defined Networking): контролери SDN динамічно керують маршрутизацією трафіку блокчейн-сервісів, забезпечуючи ізоляцію, пріоритезацію та балансування навантаження.

- Механізми консенсусу адаптовані до мережевого контексту: у разі надмірної транзакційної активності або DoS-подібної атаки можливе автоматичне перемикання на консенсус із меншою обчислювальною складністю (наприклад, з PoW на DPoS або PoA).

- Кешування та підпис транзакцій на прикордонних вузлах: дозволяє зменшити кількість повторного трафіку та навантаження на центральні вузли

блокчейн-мережі. Переваги такої архітектури: Зниження затримок при передачі транзакцій; Оптимізація споживання мережевих та апаратних ресурсів; Можливість масштабування за рахунок модульності та розподілу функціональності; Покращена стійкість до аномальних навантажень і атак. Таким чином, запропонована альтернативна архітектура дозволяє інтегрувати блокчейн-системи безпосередньо у мережеву інфраструктуру, перерозподіливши навантаження та адаптуючи роботу блокчейн-мережі до умов конкретного мережевого середовища.

Для реалізації архітектури, представленої на рисунку 2.9, передбачається використання як мережевого, так і обчислювального обладнання, здатного забезпечити стабільну роботу блокчейн-вузлів на прикладному рівні (7-й рівень OSI). Деякі виробники пропонують спеціалізовані рішення, зокрема сервери корпоративного рівня, орієнтовані на розгортання вузлів публічних або приватних блокчейн-мереж.

Одним з рекомендованих рішень для розгортання вузла головної мережі Ethereum є сервер Dell PowerEdge R750, який забезпечує необхідну продуктивність для підтримки повного вузла з постійною синхронізацією, обробкою транзакцій і участю у створенні блоків.

Характеристики Dell PowerEdge R750: CPU: Два процесори Intel Xeon Scalable (3-го покоління), кожен з 16–28 ядрами, тактова частота 2.4–3.6 ГГц; Оперативна пам’ять: 64–512 ГБ DDR4; Накопичувач: NVMe SSD обсягом 2–8 ТБ; Мережева підсистема: два порти 10–25 Гбіт/с.

Середні навантаження вузла Ethereum: CPU: 40–60% при обробці транзакцій; RAM: 16–32 ГБ для кешування; Мережа: середнє завантаження – 100–200 Мбіт/с, пікове – до 500 Мбіт/с (наприклад, при інтенсивній синхронізації).

Для реалізації блокчейн-інфраструктури у корпоративному середовищі або для цілей тестування доцільно використовувати більш прості сервери, наприклад, Dell PowerEdge T340, який забезпечує достатній рівень продуктивності при нижчих витратах.

Характеристики Dell PowerEdge T340: CPU: Intel Xeon E-2124, 4 ядра, частота 3.3 ГГц; Оперативна пам’ять: 16–32 ГБ DDR4; Накопичувач: SSD 1–2 ТБ; Мережа: два гігабітні Ethernet-порти.

Навантаження приватного вузла: CPU: 20–40% при транзакційній активності; RAM: 8–16 ГБ; Мережа: середнє завантаження – 10–50 Мбіт/с, пікове – до 100 Мбіт/с.

Таким чином, вибір апаратного забезпечення залежить від призначення блокчейн-вузла: для головної мережі Ethereum потрібні високопродуктивні сервери з потужними CPU та швидкими SSD, тоді як для розробки, тестування чи приватного використання достатньо серверів середнього рівня. В обох випадках важливу роль відіграє мережева підсистема, оскільки блокчейн-вузли інтенсивно взаємодіють із мережею зв’язку.

2.4 Граничні мережеві параметри для адаптивного перемикання алгоритмів досягнення консенсусу

Проведене моделювання та емпірично отримані дані в межах дослідження впливу на апаратні компоненти, а також мережеві характеристики [4, 13], розглянуті в попередніх підрозділах, дали змогу визначити допустимі граничні параметри, за яких доцільне перемикання алгоритму консенсусу, а також забезпечується його найвища ефективність. Відповідні значення наведено в таблиці 2.1.

Завантаження CPU, % – характеризує обсяг обчислювальних ресурсів, необхідних для підтримки функціонування алгоритму консенсусу. Наприклад, алгоритм PoW вимагає високого рівня завантаження процесора через інтенсивні обчислення хеш-функцій, тоді як алгоритми PoS і DPoS мають значно нижчі вимоги до обчислювальних потужностей.

Використання оперативної пам’яті, МБ – відображає обсяг оперативної пам’яті, необхідний для обробки транзакцій, підтримки пулу непідтверджених транзакцій, а також для формування нових блоків. Зокрема, алгоритм DPoS

демонструє нижчий рівень споживання пам’яті порівняно з PoW завдяки меншій складності обчислювальних процедур.

Таблиця 2.1 – Діапазони мережевих характеристик каналу зв’язку, що впливають на ефективність роботи алгоритмів консенсусу

Алгоритм	**PoW**	**PoS**	**DPoS**	**PBFT**	**PoR**	**PoA**	**PoET**	**FBA**
Пропускна спроможність (B), Мбіт/с	10-100	5-50	5-50	10-100	10-100	10-100	10-100	10-100
Затримка (L), мс	100-200	50-100	50-150	50-100	50-100	50-120	100-200	50-150
Джитер (J), мс	10-30	10-20	10-30	5-15	5-15	10-30	20-50	10-20
Розмір блоку (St), КБ	500-2000	250-500	250-1000	100-1000	100-1000	500-2000	500-1000	100-1000
Частота транзакцій (ft), транзакцій/с	1-10	1-10	10-50	10-50	10-50	5-30	5-30	5-20
Частота генерації 1 блока (Tblock), с	10-30	5-15	5-10	3-10	3-15	10-20	10-15	5-10
Заповненість memory pool (Mpool), % *	30-50	30-60	20-40	20-50	20-40	30-50	30-50	20-40
Завантаженість CPU, %	60-90	40-70	30-60	50-70	50-80	30-50	40-60	40-70
Використання пам’яті, МБ	1024-2048	512-1024	256-512	512-1024	512-2048	512-1024	256-512	512-1024
Використання диска, МБ/с	20-50	10-30	5-20	10-30	10-40	10-20	5-20	5-15

Використання дискової підсистеми, МБ/с – показує інтенсивність операцій читання та запису даних на диск. Для алгоритмів типу PoW і PoR характерне підвищене дискове навантаження, оскільки вони часто генерують великі об’єми даних та активно використовують постійне сховище.

Характеристики алгоритмів консенсусу, подані в таблиці, сформовані на основі комплексного аналізу: поєднання теоретичних моделей, експериментальних даних та результатів імітаційного моделювання. У дослідженні враховано інформацію з наукових джерел, присвячених порівнянню різних алгоритмів консенсусу, а також дані моніторингу функціонування реальних блокчейн-мереж, зокрема Bitcoin, Ethereum, Hyperledger Fabric та EOS.

Імітаційне моделювання дозволило розширити результати дослідження, протестувавши алгоритми в широкому спектрі сценаріїв, включаючи високу інтенсивність транзакцій та перевантаження пулу непідтверджених транзакцій. Для нових і недостатньо вивчених алгоритмів, зокрема PoET, значення параметрів були уточнені за допомогою екстраполяції наявних даних та теоретичного аналізу архітектурних особливостей.

2.5 Висновки до розділу 2

Проведено класифікацію алгоритмів консенсусу за сімействами з виокремленням найбільш доцільних реалізацій, які доцільно використовувати під час розробки адаптивного алгоритму. Виконано аналіз та оцінку впливу блокчейн-трафіку на характеристики каналу зв’язку та його пропускну здатність.

Представлено діапазони мережевих характеристик каналу зв’язку, які впливають на ефективність функціонування алгоритмів консенсусу. Дані отримано за результатами імітаційного моделювання на основі наявних досліджень. Загальна кількість ключових мережевих параметрів, які доцільно враховувати для ефективного вибору блокчейн-систем у комунікаційних мережах, не перевищує десяти, з урахуванням реальних порогових значень їх діапазонів.

3 МОДЕЛЬ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ВИБОРУ ОПТИМАЛЬНОЇ БЛОКЧЕЙН-СИСТЕМИ

Ключовим завданням модуля прийняття рішень щодо вибору блокчейн-системи є визначення найбільш ефективного алгоритму консенсусу в конкретний момент часу з урахуванням поточних мережевих та апаратних характеристик. Окрім цього, враховується швидкість розповсюдження інформації про зміну алгоритму консенсусу, що дозволяє мінімізувати втрати блоків і транзакцій під час адаптації системи.

3.1 Принцип роботи модуля прийняття рішень

Модуль прийняття рішень функціонує на основі аналізу поточних мережевих та апаратних параметрів з метою вибору оптимального алгоритму консенсусу, який забезпечує максимальну ефективність роботи блокчейн-системи в даних умовах. У процесі роботи модуль:

1. Здійснює моніторинг ключових характеристик середовища, зокрема завантаження процесора, використання пам’яті, дискової активності, пропускної здатності каналу зв’язку, затримок та інтенсивності транзакційного потоку.

2. Порівнює отримані значення з емпірично визначеними граничними діапазонами для кожного з доступних алгоритмів консенсусу.

3. Приймає рішення щодо доцільності перемикання на інший алгоритм консенсусу, якщо поточний не забезпечує належної ефективності.

4. Ініціює процес зміни алгоритму з урахуванням швидкості розповсюдження інформації в мережі, щоб мінімізувати ризики втрати блоків і транзакцій у перехідний період. Таким чином, модуль забезпечує динамічну адаптацію блокчейн-системи до змін умов середовища з метою підтримання стабільної та ефективної роботи.

Відповідно до проведеного аналізу сучасних досліджень на перетині технологій блокчейн і телекомунікаційних мереж, одним із найактуальніших

напрямів є модернізація та вдосконалення алгоритмів консенсусу з метою отримання більш універсального та ефективного рішення [24]. Проте для розв’язання цієї задачі може бути застосований альтернативний підхід — розробка адаптивного алгоритму динамічного вибору алгоритму консенсусу з урахуванням поточного стану апаратного забезпечення, на якому розгорнуто вузол блокчейн-мережі, а також характеристик каналу зв’язку.

Загальна блок-схема принципу функціонування адаптивного алгоритму наведена на рисунку 3.1.

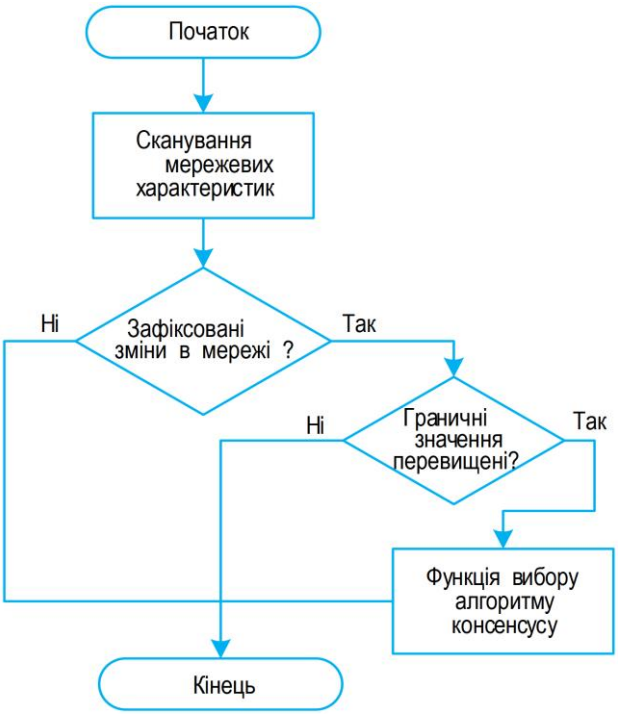

Рисунок 3.1 – Алгоритм вибору консенсусу з урахуванням динаміки мережевого середовища

У межах запропонованої концепції кожен вузол блокчейн-мережі має власний модуль оцінювання мережевих характеристик у момент часу T, що забезпечує прийняття рішення щодо доцільності зміни алгоритму консенсусу та відповідного коригування параметрів формування нових блоків даних.

Після ухвалення рішення про зміну алгоритму консенсусу, інформація про оновлені правила створення та валідації блоків передається від ініціативного

вузла до інших вузлів мережі з метою забезпечення синхронної зміни глобального алгоритму консенсусу. Цей процес включає кілька етапів передачі даних, тривалість і ефективність яких залежать від кількості активних з'єднань вузла. На рисунку 3.2 представлено загальну схему сценарію зміни алгоритму консенсусу у відповідь на зміну мережевих параметрів.

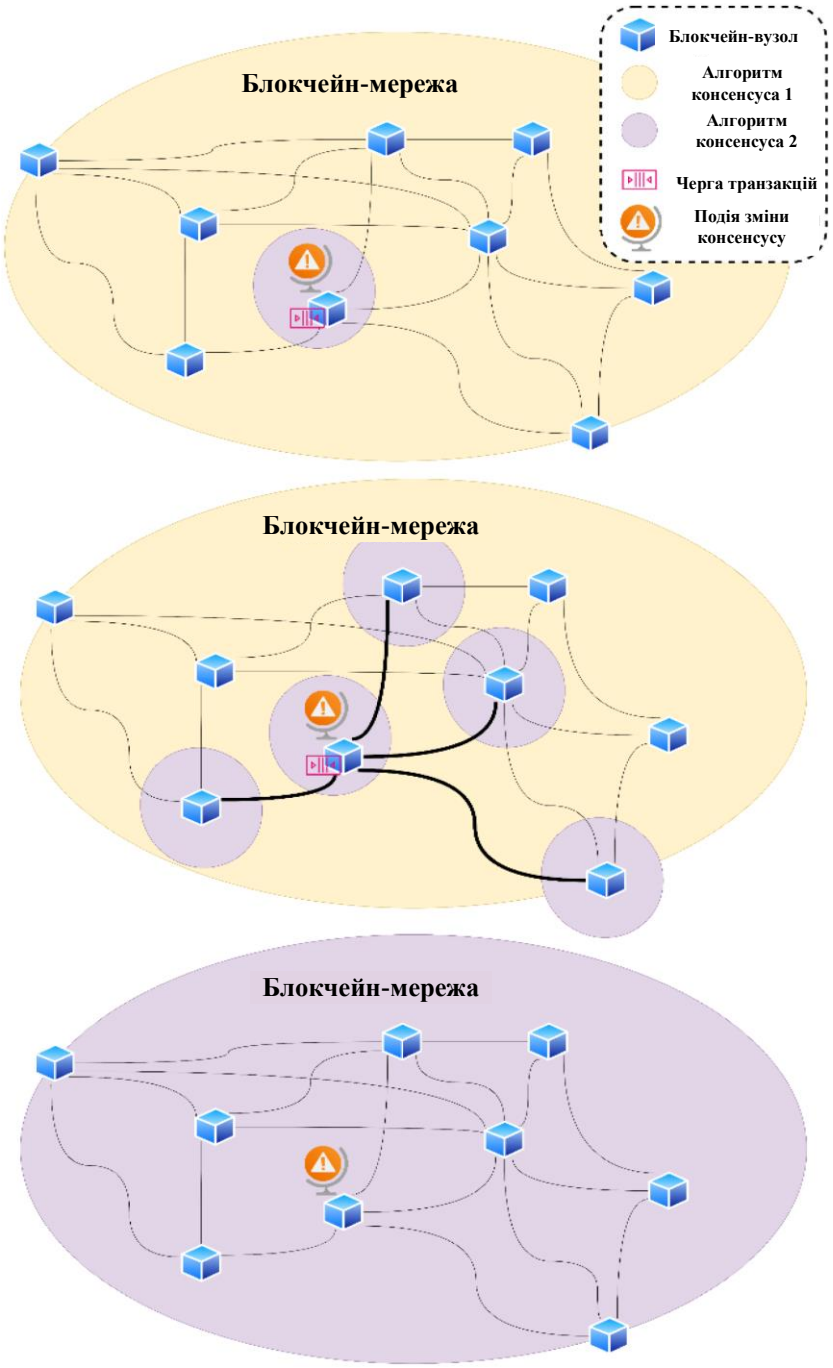

Рисунок 3.2 – Схема передачі інформації про оновлення консенсусу між вузлами мережі

Як показано на схемі, другим етапом після виявлення потреби у зміні алгоритму консенсусу є передача відповідного повідомлення. Першими отримують повідомлення ті вузли, адреси яких відомі початковому вузлу, з яким ведеться синхронізація. Після отримання повідомлення ці вузли ініціюють подальнє розповсюдження запиту на зміну алгоритму консенсусу по мережі.

Однак ефективність запропонованого підходу обмежується кількістю пристроїв у мережі та кількістю їхніх з'єднань, а також кількістю «рівнів» передачі інформації. Чим менше активних зв'язків має вузол мережі, тим більша кількість етапів необхідна для поширення інформації до периферії мережі (аналогічно до принципів, притаманних графовим структурам). Це обмеження зумовлено особливостями функціонування мережі під час зміни алгоритму консенсусу, оскільки кожен вузол продовжує формування блоків транзакцій. Блок транзакцій, створений згідно з правилами алгоритму консенсусу 1, не може бути валідований вузлом, який на момент перевірки вже працює за іншим алгоритмом, що призводить до втрати таких блоків і, відповідно, до затримок в обробці транзакцій. Програмний компонент, який встановлюється на обладнання, реалізує два основні модулі — модуль моніторингу та модуль прийняття рішень, відповідно до запропонованої концепції.

Алгоритм функціонування модуля моніторингу наведено на рисунку 3.3, а його програмна реалізація представлена в додатку В.

Модуль моніторингу виконує контроль за станом ключових мережевих характеристик, значення яких слугують основою для прийняття рішення щодо необхідності зміни алгоритму консенсусу. Моніторинг мережевого трафіку реалізовано у вигляді системи, що здійснює аналіз і оцінювання мережевих пакетів у режимі реального часу з метою оптимізації роботи інфраструктури зв'язку. Для захоплення та обробки пакетів використовується бібліотека Scapy, яка надає змогу отримувати основні метрики, такі як пропускна здатність, затримка та джиттер — ці параметри дозволяють оцінити якість мережевого з'єднання.

Процес функціонування модуля моніторингу складається з кількох етапів. На першому етапі здійснюється збір даних: кожен захоплений пакет аналізується, фіксується його розмір і мітка часу, що формує інформаційне середовище для подальшого аналізу активності мережі.

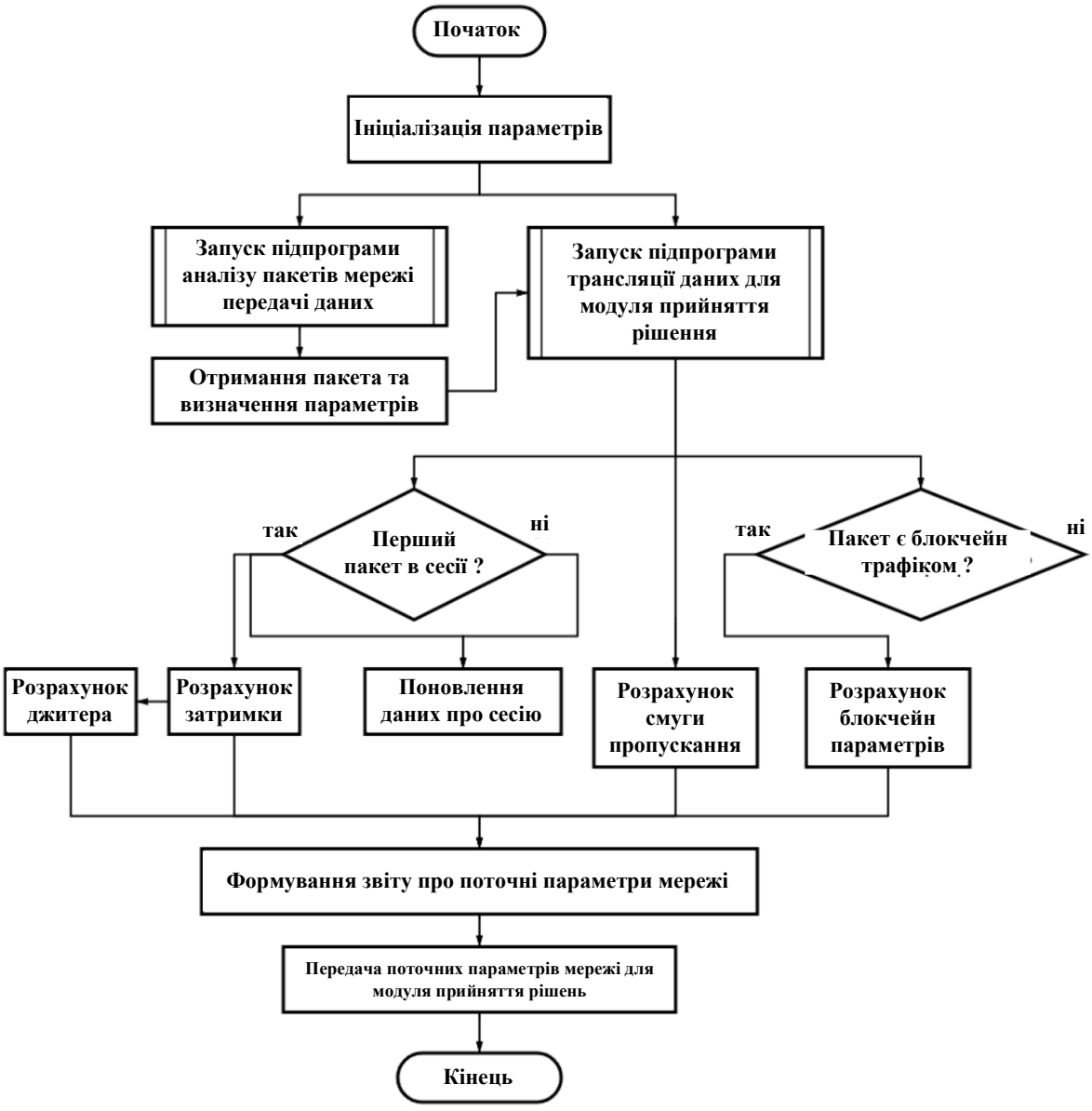

Рисунок 3.3 – Блок-схема роботи модуля моніторингу мережевого трафіку

На другому етапі виконується аналіз затримок між послідовними пакетами, що дозволяє виявити можливі проблеми з продуктивністю. Далі розраховуються такі метрики, як пропускна здатність, середній розмір пакета, середня затримка

та джиттер. Отримані дані зберігаються у лог-файл, який використовується модулем прийняття рішень.

Алгоритм роботи модуля прийняття рішень наведено на рисунку 3.4, а його програмна реалізація також представлена у додатку В.

Модуль прийняття рішень адаптивного вибору алгоритму консенсусу в блокчейн-мережі призначений для динамічного керування вибором алгоритму консенсусу залежно від поточних умов функціонування мережі. Основна ідея полягає в підвищенні продуктивності системи за рахунок автоматичного підбору найбільш ефективного алгоритму консенсусу у відповідь на зміни значень ключових мережевих метрик.

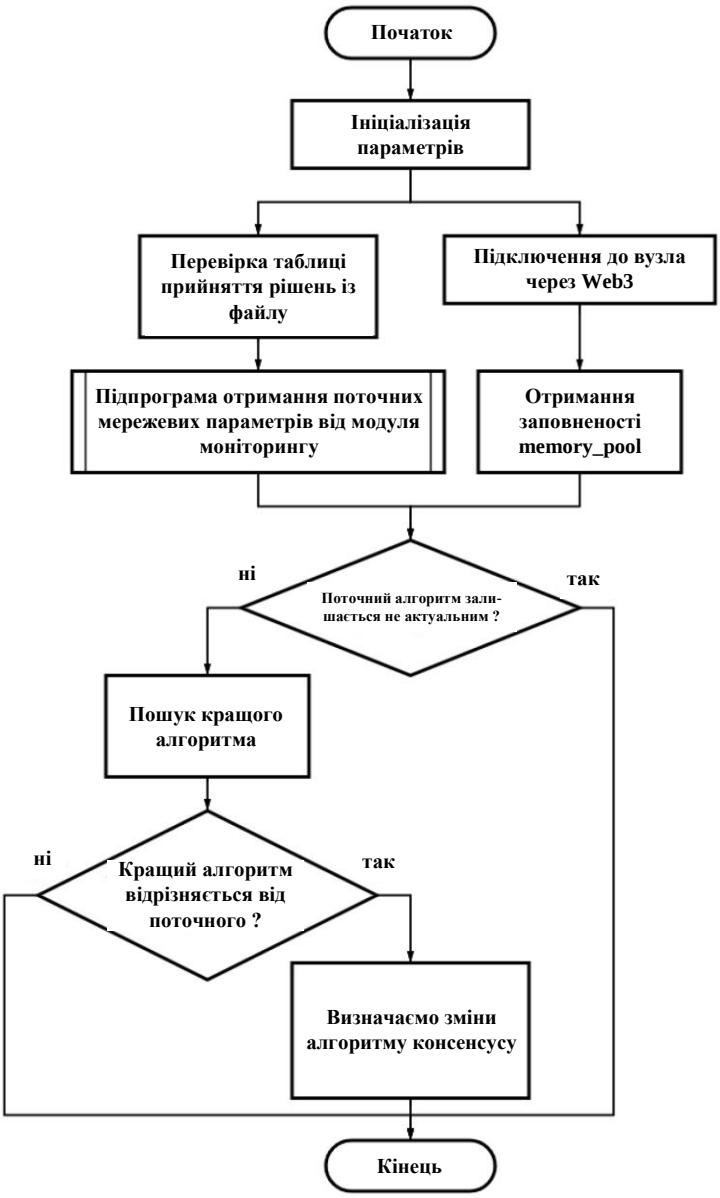

Рисунок 3.4 – Блок-схема роботи модуля прийняття рішень у блокчейн-мережі

На основі зібраних метрик модуль здійснює аналіз відповідності поточного алгоритму консенсусу умовам, заданим у таблиці відповідності. У разі невідповідності виконується пошук альтернативних алгоритмів, які краще відповідають поточному стану мережі. За потреби модуль ініціює переключення на інший, більш придатний алгоритм консенсусу. Факт переходу фіксується у лог-файлі, що дозволяє здійснювати моніторинг змін та аналізувати їхній вплив на продуктивність мережі. Алгоритм функціонує в циклічному режимі з періодичним оновленням значень метрик і перевіркою доцільності зміни алгоритму через задані часові інтервали. Це забезпечує своєчасне реагування на зміни в мережевому середовищі та підтримку оптимального рівня ефективності роботи блокчейн-системи.

3.2 Імітаційне моделювання мережі з модулем адаптивного прийняття рішення для алгоритму консенсусу

Імітаційне моделювання відіграє ключову роль у розробці алгоритмів для мереж і описі процесів. Воно являє собою метод дослідження поведінки складних систем шляхом створення їх комп’ютерної моделі та проведення експериментів з метою аналізу та прогнозування різноманітних сценаріїв функціонування. Такий підхід дозволяє отримати цінну інформацію щодо роботи системи без необхідності її розгортання в реальних умовах, що є особливо важливим у контексті складних розподілених систем, зокрема таких, як блокчейн.

Актуальність імітаційного моделювання для модуля прийняття рішень зумовлена низкою чинників. По-перше, блокчейн-мережі є розподіленими системами з великою кількістю взаємодіючих вузлів, що ускладнює аналітичне дослідження всіх аспектів їх функціонування. Наприклад, поведінка мережі залежить від численних змінних, таких як інтенсивність користувацького та блокчейн-трафіку, параметри консенсусу, поточна пропускна здатність мережі,

затримки та джиттер. Імітаційне моделювання дозволяє врахувати ці параметри та їх взаємозв’язки, формуючи реалістичну картину функціонування мережі.

По-друге, модуль прийняття рішень щодо адаптивного вибору консенсусу блокчейн-мережі потребує тестування в умовах, максимально наближених до реальних. Зокрема, необхідно враховувати, як зміни таких параметрів, як розмір блоку чи частота його генерації, впливають на продуктивність системи, рівень затримок та заповненість пулу необроблених транзакцій. Проведення подібних експериментів у реальному середовищі супроводжується значними витратами часу та ресурсів, а також ризиком виникнення збоїв. Імітаційне моделювання усуває ці ризики, надаючи безпечне середовище для перевірки гіпотез і коригування алгоритмів. Крім того, імітаційне моделювання дозволяє досліджувати поведінку мережі за різних алгоритмів консенсусу. Кожен із них має власні особливості, що впливають на споживання ресурсів, розподіл навантаження та мережеві характеристики. Моделювання дає змогу оцінити, як адаптивний алгоритм реагуватиме на зміну умов у мережі, яка використовує той чи інший механізм консенсусу. Це має вирішальне значення для забезпечення універсальності та гнучкості розроблюваного алгоритму.

Однією з ключових переваг імітаційного моделювання є можливість проведення стрес-тестування системи. Наприклад, можна змоделювати різке зростання користувацького трафіку, збої у роботі окремих вузлів чи інші нестандартні ситуації, щоб оцінити стійкість модуля та його здатність адаптуватися до змін. Це дозволяє виявити потенційні вразливості модуля прийняття рішень ще до його впровадження в реальну мережу. Імітаційне моделювання також є важливим інструментом для оцінювання ефективності модуля прийняття рішень. Порівнюючи результати функціонування мережі до та після впровадження модуля, можна отримати об’єктивні дані щодо підвищення продуктивності, зниження затримок та оптимізації використання ресурсів. Крім того, моделювання дозволяє прогнозувати довгострокові наслідки змін у параметрах мережі, що дає змогу уникнути хибних рішень.

Для представлення підсумкової моделі блокчейн-мережі з модулем прийняття рішень було застосовано метод імітаційного моделювання з використанням програмного забезпечення AnyLogic (рис. 3.5).

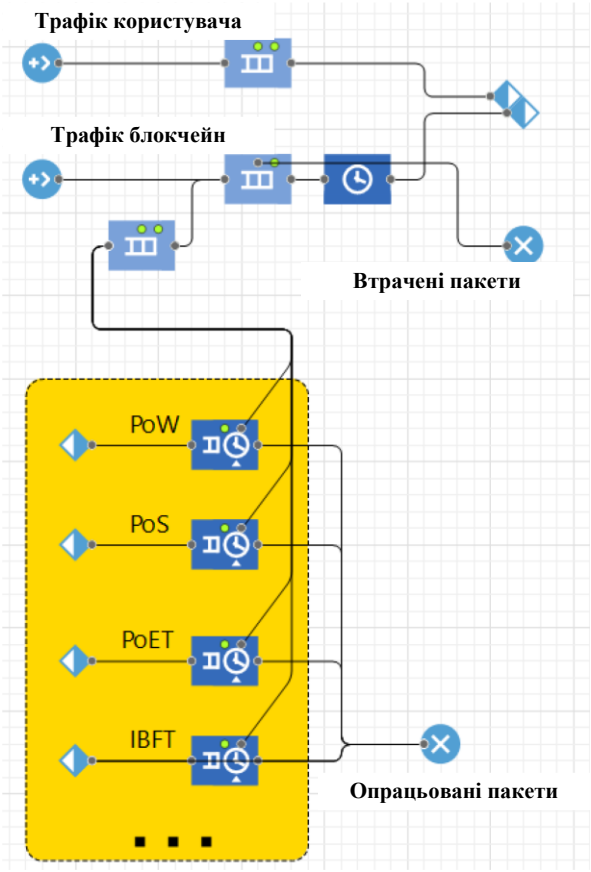

Рисунок 3.5 – Імітаційна модель у середовищі AnyLogic

Джерелом навантаження виступає користувацький трафік та трафік блокчейн-мережі, що включає транзакції та блоки. У межах описаної моделі цей тип трафіку може бути охарактеризований як регулярний і стаціонарний, що дозволяє описати його за допомогою функції розподілу $B_k(t)$ та перетворення Лапласа–Стільтьєса [50, 51], згідно з формулою (3.1).

$$b_k^{(m)} = \int_0^\infty t^m dB_k(t) \qquad (3.1)$$

У моделі вважається, що пакети блокчейн-трафіку мають нижчий пріоритет порівняно з пакетами користувацького трафіку. Пріоритетність проявляється на етапі вибору нової заявки для обробки — перевага надається користувацькому трафіку.

Також доцільно розглянути використання концепції абсолютного пріоритету, яка полягає в такому функціонуванні системи: у разі надходження заявки з вищим пріоритетом система зобов’язана перервати обробку поточної заявки одним із способів — видалити її з системи, призупинити обробку для вивільнення ресурсів або повернути її в чергу. Після завершення обробки пріоритетних заявок система повертається до обробки менш пріоритетного потоку. Проте у поточній моделі мережі такий підхід розглядається як неефективний, тому застосовується лише концепція відносного пріоритету обробки потоків.

У подальшій частині моделі для блокчейн-трафіку передбачено пул непідтверджених транзакцій, а також вихідний потік непідтверджених (необроблених) транзакцій, які не потрапили до пулу. Його основне призначення — відображення ефективності алгоритму консенсусу в аспекті обробки транзакційного потоку за поточних мережевих умов.

На наступному етапі моделі блокчейн-трафік і користувацький трафік об’єднуються та передаються на обробку алгоритмом консенсусу. Об’єднаний трафік додатково аналізується модулем моніторингу та модулем прийняття рішень з метою визначення доцільності переключення мережі на більш ефективний алгоритм консенсусу.

У разі, якщо для обробки пріоритетного користувацького трафіку в мережі недостатньо ресурсів, відповідний трафік виходить із системи необробленим і не передається далі. Втрати користувацького трафіку є малоймовірними та описуються формулою (3.1), що визначає ймовірність зайнятості всіх каналів обслуговування. Для блокчейн-трафіку, який є менш пріоритетним і більш схильним до відмови в обробці, передбачено вбудований у блокчейн-механізм — повернення транзакцій до пулу непідтверджених.

Обробка пакетів і транзакцій здійснюється у великому модулі, що представляє собою множину можливих станів системи у момент часу t. Цей модуль може бути представлений графом переходів марковських процесів [32] (див. рис. 3.6).

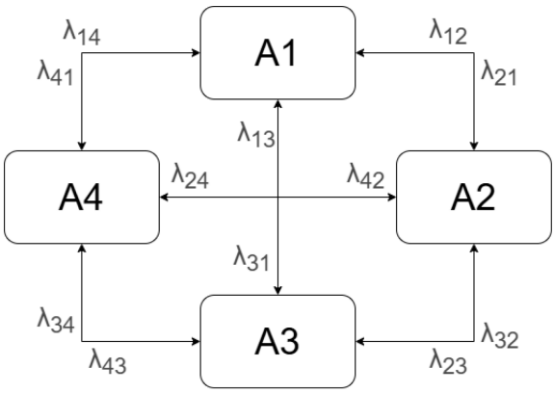

Рисунок 3.6 – Імітаційна модель у середовищі AnyLogic

Виходячи з наведеного графа, можна стверджувати, що ймовірність переходу системи зі стану S_i у стан S_j за проміжок часу Δt наближено дорівнює добутку інтенсивності переходу на тривалість цього інтервалу, що описується формулою (3.2).

$$P_{\Delta t}(S_i \to S_j) \approx \lambda_{ij} \Delta t \qquad (3.2)$$

У якості сценарію моделювання було розглянуто випадок збільшення навантаження користувацького трафіку. Очікувана поведінка системи передбачала перемикання алгоритму консенсусу блокчейн-мережі на менш ресурсоємний варіант у разі спрацювання запрограмованих тригерів.

На рисунку 3.7 наведено результати аналітичного та імітаційного моделювання зміни використання пропускної здатності.

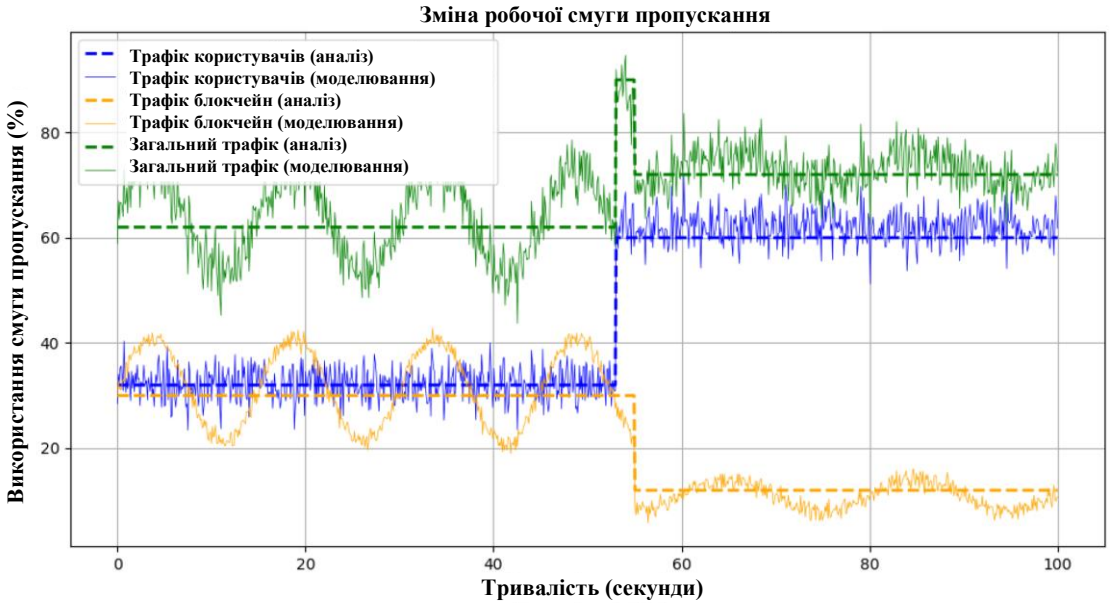

Рисунок 3.7 – Порівняння результатів аналітичного та імітаційного моделювання

Можна помітити, що у даному сценарії тригером для запуску протоколу перемикання алгоритму консенсусу стало перевищення рівня використання пропускної здатності понад 80%. Після цього модуль прийняття рішень зменшив активність блокчейн-мережі, тим самим вивільнивши ресурси для обслуговування користувацького трафіку.

3.3 Результати комп'ютерного моделювання

За допомогою методу імітаційного моделювання були сформовані та проаналізовані однорідні сценарії з однаковими мережевими характеристиками, але з різними алгоритмами консенсусу.

Результати моделювання підтвердили важливість використання модуля прийняття рішення щодо зміни алгоритму консенсусу для ефективного управління навантаженням у блокчейн-мережі, особливо за умов високої інтенсивності трафіку та суттєвих змін у параметрах мережі. Наприклад, алгоритм Proof of Work (PoW) [53, 54], незважаючи на його широке застосування,

продемонстрував низьку ефективність за умов збільшення транзакційного потоку (див. рис. 3.8). Втрати корисного навантаження блокчейн-трафіку сягали приблизно 30%, що свідчить про неспроможність даного алгоритму ефективно обробляти інтенсивні потоки транзакцій. Це призводило до збільшення часу підтвердження транзакцій, зростання пулу непідтверджених транзакцій і, відповідно, погіршення загальної якості обслуговування.

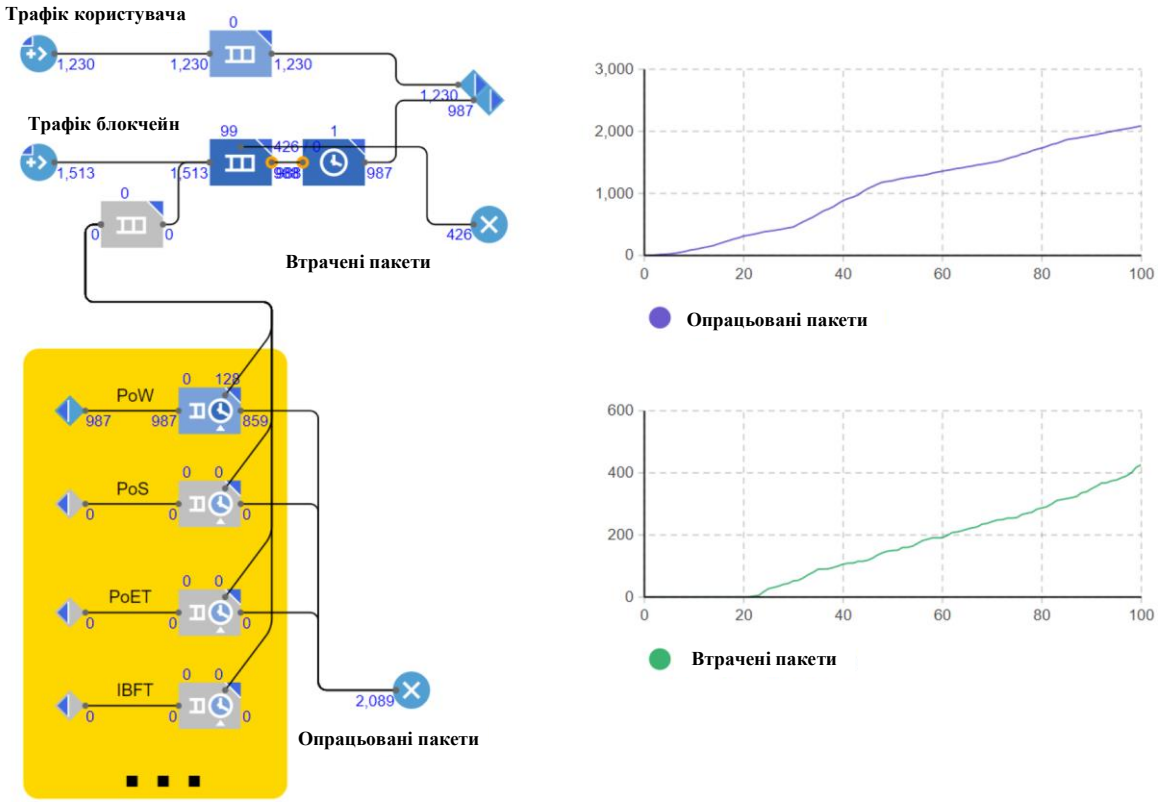

Рисунок 3.8 – Імітаційна модель роботи алгоритму консенсусу PoW

Запровадження механізму адаптації до мережевих умов у межах модуля прийняття рішення, який забезпечує перемикання між різними алгоритмами консенсусу, суттєво змінило ситуацію. У ході імітаційного моделювання було показано, що при активації модуля адаптації мережа автоматично перейшла з PoW на більш придатний алгоритм Proof of Stake (PoS) в умовах підвищеного навантаження. Це дозволило значно зменшити затримки та підвищити пропускну здатність мережі. Надалі, із подальшим зростанням заповненості пулу

непідтверджених транзакцій та ускладненням умов їх обробки, мережа перейшла до використання алгоритму IBFT, який забезпечив стабільну роботу навіть за високого рівня навантаження.

Аналіз показав, що адаптивний підхід дозволяє не лише мінімізувати втрати, але й підвищити ефективність використання мережевих ресурсів. Зокрема, перехід від PoW до PoS, а згодом до IBFT (PBFT) (див. рис. 3.9) [25] дозволив опрацювати транзакційний потік майже без втрат, зберігаючи стабільну роботу мережі та підтримуючи мінімальні затримки передавання даних. Це підкреслює, що адаптивні механізми забезпечують більш гнучкий і точний розподіл ресурсів, ніж статичні підходи.

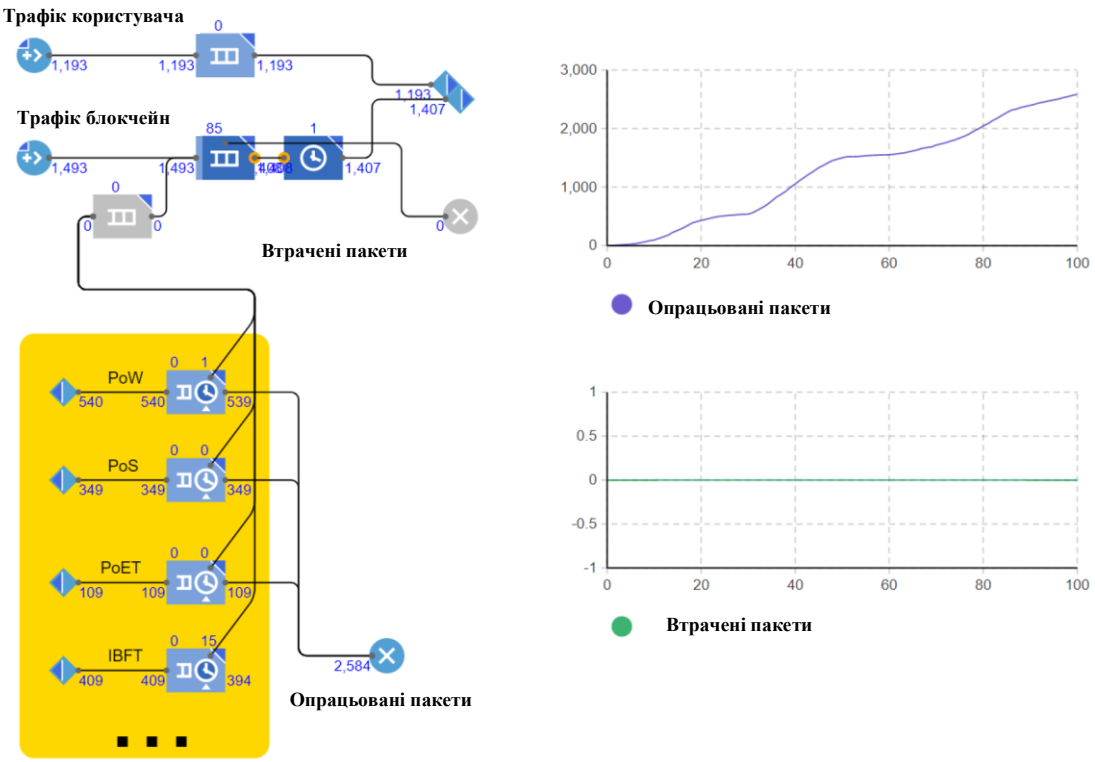

Рисунок 3.9 – Імітаційна модель роботи модуля прийняття рішень з адаптивного перемикання алгоритмів консенсусу в блокчейн-мережі

Слід також зазначити, що перемикання між алгоритмами консенсусу відбувалося в режимі реального часу, що стало можливим завдяки безперервному моніторингу мережевих характеристик і автоматичному

коригуванню параметрів. Це дозволило не лише ефективно реагувати на змінні навантаження, а й запобігати виникненню вузьких місць, таких як переповнення пулу необроблених транзакцій чи значне зростання джитеру.

Результати моделювання також демонструють переваги модуля прийняття рішень в умовах довготривалої роботи мережі. Наприклад, у сценаріях, де навантаження на мережу змінювалося протягом тривалого часу, модуль прийняття рішень дозволяв зберігати стабільну продуктивність мережі, оптимізуючи параметри без необхідності втручання операторів. Це підтверджує, що впровадження подібного підходу робить мережу більш автономною та стійкою до зовнішніх факторів, включаючи різке збільшення кількості транзакцій або нестабільність інфраструктури.

З наукової точки зору отримані результати підкреслюють необхідність подальшого розвитку адаптивних механізмів для блокчейн-мереж. Поєднання моніторингу, аналізу та динамічного коригування параметрів дозволяє суттєво підвищити продуктивність мережі, її масштабованість та стійкість. Більше того, імітаційне моделювання підтвердило, що подібні системи можуть ефективно застосовуватись не лише в блокчейн-середовищі, але й в інших розподілених системах, що потребують адаптації до змінних умов.

Таким чином, результати імітаційного моделювання доводять, що запропонований модуль прийняття рішень не лише покращує поточні показники роботи мережі, але й відкриває можливості для її стійкого розвитку в умовах змінних вимог та навантажень.

3.4 Висновки до розділу 3

Запропоновано концепцію модуля прийняття рішень з адаптивного вибору алгоритму консенсусу блокчейн-мережі залежно від мережевих характеристик, апаратних показників обладнання та особливостей ділянки мережі зв’язку.

Розроблено аналітичну модель мережі з інтегрованим блокчейном.

Створено імітаційну модель мережі з модулем прийняття рішень з адаптивного вибору алгоритму консенсусу блокчейн-системи з використанням програмного забезпечення AnyLogic; проведено імітаційне моделювання, яке підтвердило, що відхилення між аналітичними розрахунками та результатами моделювання не перевищує 5%.

4 ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ АДАПТИВНОГО ВИБОРУ БЛОКЧЕЙН-СИСТЕМ

Розроблений модуль прийняття рішень має низку обмежень, зумовлених принципами функціонування блокчейн-технології, зокрема швидкістю генерації блоків та кількістю учасників, серед яких відбувається розповсюдження інформації. Для ефективного використання модуля необхідно розробити модель оцінки ефективності запропонованого підходу з урахуванням особливостей та структури мережі зв’язку.

4.1 Оцінка часу синхронізації вузлів мережі на прикладі інтелектуальної транспортної системи (ITS)

Оцінка часу синхронізації вузлів може розглядатися на прикладі реєстрації даних про інциденти, таких як координати, час події, а також транспортні засоби-свідки (або потенційні свідки) [5, 16, 27]. Схема взаємодії представлена на рисунку 4.1. Для реалізації оперативного реагування системи на зміни та запуск одного із заздалегідь визначених сценаріїв необхідна наявність таких компонентів: датчики, мобільний додаток та інші елементи системи, що передають сигнал про подію; смарт-контракт у блокчейн-мережі, який фіксує ключову інформацію про інцидент (дата, час, координати, ідентифікатори учасників); система IPFS для зберігання детальнішої інформації та файлів (опційно); модуль прослуховування подій смарт-контракту, який відстежує появу нових записів та передає відповідний сигнал екстреним службам у разі виникнення надзвичайної ситуації.

З урахуванням запропонованої архітектури можливі два основних сценарії взаємодії з вразимими учасниками дорожнього руху (VRU).

У сценарії 1 передбачається, що інформація про VRU, який перебуває на маршруті руху транспортного засобу, була своєчасно виявлена, сигнал передано

до блоків RSU та OBU, і надзвичайна ситуація була попереджена завдяки оперативній реакції всієї системи.

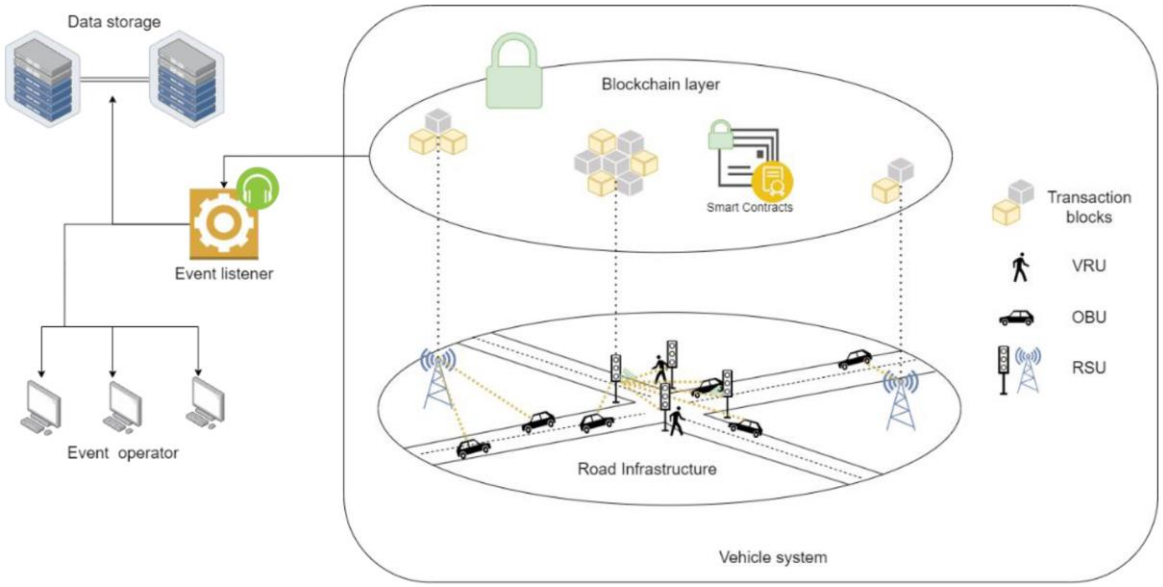

Рисунок 4.1 – Архітектура інтелектуальної транспортної системи (ITS) для сценарію оперативного реагування на надзвичайну подію

Сценарій 2 передбачає, що інформація про VRU була отримана із запізненням або не отримана зовсім, а реакції з боку RSU та OBU виявилося недостатньо. У такому випадку дані про інцидент фіксуються у блокчейн-мережі, здійснюється виклик екстрених служб, а також зберігається інформація про сегмент інциденту з визначеним радіусом для подальшого аналізу та з’ясування обставин [18–21].

В інтелектуальних транспортних системах (ITS), що базуються на технології блокчейн, критично важливими параметрами є швидкість поширення інформації між вузлами мережі та синхронізація. Це зумовлено необхідністю забезпечення своєчасної передачі даних, що безпосередньо впливає на ефективність управління трафіком та оперативність прийняття рішень.

Нижче наведено основні чинники, що визначають швидкість розповсюдження інформації та синхронізації у блокчейн-мережі:

- Архітектура блокчейн-мережі: топологія мережі (кількість і розташування вузлів); алгоритм консенсусу; пропускна здатність каналів зв’язку між вузлами.

- Обсяг і частота переданих даних: кількість та розмір транзакцій/блоків; частота оновлення інформації про стан трафіку.

- Обчислювальна потужність та продуктивність вузлів: тактова частота процесора; обсяг оперативної пам’яті; ефективність алгоритмів обробки даних.

- Мережева інфраструктура: швидкість і стабільність інтернет-з’єднання; затримки передачі даних (латентність); наявність резервних каналів зв’язку.

Серед зазначених чинників найбільш суттєвими є: Розмір блоку – чим більший обсяг блоку, тим більше часу потрібно на його передачу, що безпосередньо впливає на швидкість; Пропускна здатність мережі – визначає максимальний обсяг даних, які можуть бути передані за одиницю часу; Затримка передачі – може істотно впливати на загальний час доставки блоку; Час перевірки – перед передачею вузли мають верифікувати блок, що також потребує часу. Зазначені параметри чинять комплексний вплив на швидкість передачі блоків у мережі та на подальше їх поширення. Базове рівняння для оцінки середньої швидкості розповсюдження блоку V між вузлами може бути подано у вигляді:

$$V = \frac{S}{T}, \tag{4.1}$$

де S — розмір блока (у байтах або мегабайтах), T — середній час передачі блока (у секундах).

Втім, для врахування ключових чинників, що впливають на швидкість розповсюдження даних у мережі, аналітична модель має бути доповнена часовою структурою процесу передачі (формула 4.2).

$$T = T_{propagation} + T_{validation} + T_{network-delay}, \tag{4.2}$$

де $T_{propagation}$ — час поширення блока між вузлами, $T_{validation}$ — час, необхідний для перевірки блока, $T_{network\text{-}delay}$ — затримки в мережі. Для забезпечення високої швидкості розповсюдження інформації система повинна бути оптимізована за всіма вказаними параметрами. Висока швидкість розповсюдження інформації є ключовим чинником, що забезпечує своєчасне реагування інтелектуальної транспортної системи на зміни дорожньої ситуації та прийняття оптимальних управлінських рішень. Відповідно до наведених формул (4.1, 4.2), швидкість розповсюдження інформації (синхронізації) в мережі складається з трьох компонентів.

Розглянемо детальніше аспект швидкості валідації та створення блоків. Цей компонент залежить від архітектури мережі, зокрема від алгоритму консенсусу, розміру блока та інших параметрів мережі. Для дослідження цього параметра був використаний метод моделювання із застосуванням утиліти SIMBA, яка є удосконаленою версією BlockSim [62, 63]. Основним завданням моделювання було дослідити швидкість розповсюдження інформації (синхронізації мережі) залежно від відстані між вузлами. Для проведення моделювання були задані параметри мережі з малою відстанню між вузлами (рисунок 4.2) та великою відстанню між вузлами, після чого була проведена симуляція, в ході якої фіксувався факт відправлення блоків транзакцій з одних вузлів та їх отримання іншими (рисунок 4.3).

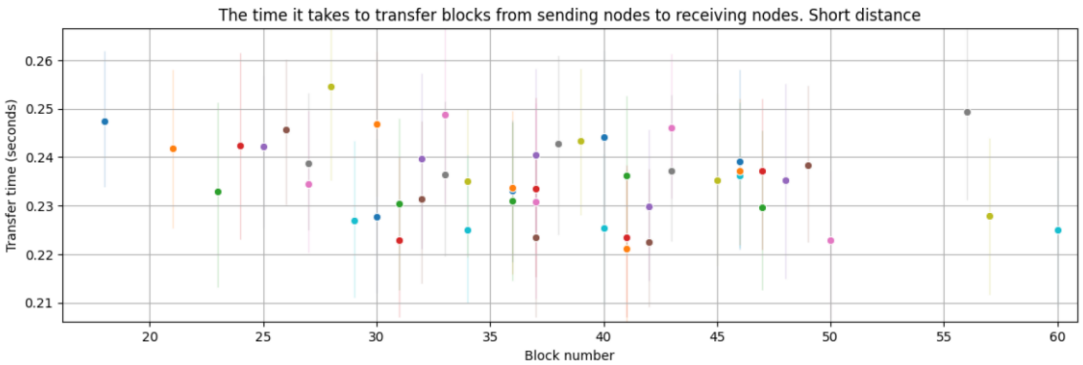

Рисунок 4.2 – Передача блока між вузлами, розташованими на близькій відстані

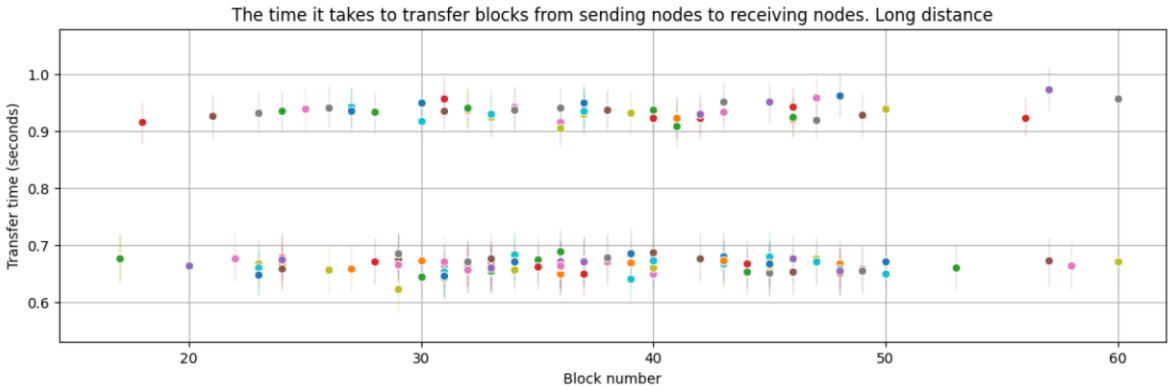

Рисунок 4.3 – Передача блока між вузлами, розташованими на великій відстані

Кожну групу вузлів, яким було надіслано новий блок від вузла-відправника або вузла-творця блоку, можна відобразити на графіку у вигляді одноколірної лінії з позначкою посередині, що вказує середній час передачі блоку даних.

На графіках також спостерігаються випадки, коли одному блоку відповідає кілька таких груп вузлів.

Якщо на одній осі розташовані дві або більше точок різних кольорів, це свідчить про те, що блок, надісланий вузлами, був отриманий іншими вузлами, що ініціювало подальший процес розсилання блоку на інші вузли. Інакше кажучи, був запущений і підтриманий процес синхронізації мережі кількома учасниками. Отже, осі, на яких розташовано дві або більше точок, відповідають вузлам, що синхронізувалися між собою.

За результатами моделювання видно, що швидкість синхронізації мережі для віддалених вузлів може сягати близько 1 секунди, що є досить хорошим показником порівняно зі швидкістю створення та перевірки транзакцій, а також створення блоків у системі [24, 25].

Проте для сценаріїв оперативного реагування більш релевантним є графік вузлів, розташованих близько один до одного, швидкість синхронізації яких становить приблизно 0,25 секунди. Це пов’язано з тим, що вузли у проектованій

архітектурі будуть розміщені у достатній близькості один до одного та до центрів управління для швидкого реагування на надзвичайні ситуації.

Отриманий результат демонструє прийнятний рівень швидкості та підтверджує можливість застосування сценаріїв швидкого реагування в запропонованій архітектурі з інтеграцією технології блокчейн.

4.2 Модель оцінювання ефективності модуля адаптивного вибору алгоритму консенсусу

Оцінка ефективності модуля прийняття рішення безпосередньо залежить від кількості створених блоків, які не будуть втрачені в процесі переходу між алгоритмами консенсусу [27, 28].

Для оцінки загальної кількості блоків, створених за початковим алгоритмом консенсусу B_{old}, необхідно обчислити інтеграл, що представляє собою добуток кількості вузлів N, інтенсивності генерації блоків λ та ймовірності того, що вузол ще не отримав інформацію про зміну алгоритму консенсусу $P_{uninformed}$, протягом часу від t=0 до $t=T_{full}$ — повного часу переключення всіх вузлів мережі:

$$B_{old} = N\lambda \int_0^{T_{full}} P_{uninformed}(t)dt = N\lambda \int_0^{T_{full}} e^{-\beta t}dt \qquad (4.3)$$

Виконавши необхідні математичні перетворення, отримаємо наступний вираз для оцінки кількості блоків, створених за початковим алгоритмом консенсусу протягом часу перемикання:

$$B_{old} = N\lambda\left(\frac{1-e^{-\beta T_{full}}}{\beta}\right) \qquad (4.4)$$

Якщо $\beta T_{full} \gg 1$, а також $e^{-\beta T_{full}} \approx 0$, і тоді

$$B_{old} \approx \frac{N\lambda}{\beta} \tag{4.5}$$

У такому випадку загальна кількість блоків, створених усіма вузлами за період часу T, визначається як добуток кількості вузлів, інтенсивності генерації блоків кожним вузлом та тривалості розрахункового періоду:

$$B_{total} = N\lambda T, \tag{4.6}$$

Отже, з урахуванням періоду переходу мережі на новий алгоритм консенсусу, доцільно ввести поняття «корисних» блоків — тобто таких, які гарантовано приймаються мережею та не втрачаються внаслідок асинхронності або колізій під час зміни протоколу. Корисні блоки — це блоки, створені після завершення процесу переключення всіх вузлів на новий алгоритм консенсусу, тобто після моменту часу T_{full}:

$$B_{useful} = N\lambda\left(T - T_{full}\right) \tag{4.7}$$

Ефективність η адаптивного алгоритму доцільно визначити як відношення кількості корисних блоків до загальної кількості створених блоків у межах досліджуваного періоду часу. Це дозволяє кількісно оцінити, наскільки успішно система справляється з адаптацією без втрат продуктивності. Математично це виражається наступною формулою:

$$\eta = \frac{B_{useful}}{B_{total}} = \frac{N\lambda\left(T - T_{full}\right)}{N\lambda T} = 1 - \frac{T_{full}}{T} \tag{4.8}$$

Вираз (4.8) показує, що ефективність η зменшується лінійно зі зростанням часу розповсюдження інформації T_{full}:

$$\eta = 1 - \frac{T_{full}}{T} = 1 - \frac{D(G)}{cT} \quad (4.9)$$

За умови фіксованого загального часу спостереження T, ефективність адаптивного вибору алгоритму консенсусу η визначається рядом параметрів мережі. Зокрема:

- Діаметром графа зв'язності D(G): зі зростанням діаметра графа зростає загальний час поширення інформації T_{full}, що негативно впливає на ефективність. Тобто, при збільшенні D(G), значення η зменшується.

Частотою передачі службових повідомлень c: зі збільшенням частоти обміну повідомленнями між вузлами час синхронізації мережі скорочується, що, у свою чергу, підвищує ефективність модуля. Тобто, при зростанні c, значення η збільшується.

Крім того, важливо враховувати вплив частоти передачі транзакцій на процес формування блоків. Частота генерації транзакцій λ прямо впливає на навантаження в мережі, що може призводити до зниження швидкості передачі службових повідомлень та, відповідно, зменшення ефективної пропускної здатності каналу зв’язку для критично важливої службової інформації.

У такому випадку частоту обміну службовими повідомленнями доцільно розглядати як функцію від навантаження транзакційного трафіку, тобто:

$$c = c_0 - k\lambda_{tx}, \quad (4.10)$$

де c_0 базова частота передачі (тобто частоти обміну службовими повідомленнями за відсутності транзакцій); коефіцієнт k відображає зменшення частоти обміну при зростанні навантаження на мережу внаслідок зростання частоти транзакцій λ, узагальнена математична модель для оцінки ефективності η адаптивного алгоритму:

$$\eta = 1 - \frac{D(G)}{(c_0 - k\lambda_{tx})T} \quad (4.11)$$

З урахуванням того, що діаметр графа D(G) зазвичай залежить від кількості вузлів N, для топологій типу «малий світ» (small-world networks) або випадкових графів справедлива оцінка $D(G) \approx \log N$:

$$\eta = 1 - \frac{\log N}{(c_0 - k\lambda_{tx})T}, \tag{4.12}$$

Тепер розширимо модель, додавши до неї залежність від часу генерації блоків T та розміру блоків B_{size} з коефіцієнтом α для коригування рівня впливу розміру блоку на мережу. Час генерації блоків і їх розмір — ключові параметри, оскільки при активній генерації транзакцій у мережі починає формуватись буфер (черга), який у блокчейні є пулом непідтверджених транзакцій, що впливає на навантаження мережі та ефективність роботи консенсусу [31, 32].

З урахуванням зазначених додаткових параметрів, модель набуде наступного вигляду:

$$\eta = 1 - \frac{D(G) * \alpha * B_{size}}{(c_0 - k\lambda_{tx}) * T * T_{block}} \tag{4.13}$$

Виходячи з наведених вище виразів, можна зробити такі висновки: ефективність розраховується у відсотках як відношення втрачених блоків до загальної кількості блоків з урахуванням набору параметрів; при збільшенні кількості вузлів N ефективність η зменшується логарифмічно, оскільки збільшується діаметр графа; при збільшенні частоти передачі с ефективність η зростає, оскільки зменшується час поширення інформації; при збільшенні часу створення блоку T ефективність η зростає, оскільки зменшується кількість некоректно створеної інформації; при збільшенні частоти створення транзакцій ефективність η зменшується, якщо λ_{tx} суттєво впливає на с.

Модель дозволяє кількісно оцінити вплив параметрів мережі на доцільність використання адаптивного модуля вибору консенсусу в блокчейн-системах у

складі розподілених кіберфізичних систем (зокрема — інтелектуальних транспортних мереж).

Таким чином, досягнення високої ефективності модуля адаптивного перемикання консенсусу вимагає не лише оптимізації топології мережі та протоколів синхронізації, а й контролю рівня транзакційного навантаження для запобігання деградації продуктивності мережі.

4.3 Інтеграція модуля прийняття рішень адаптивного вибору блокчейн-систем

Інтеграція модуля прийняття рішень адаптивного вибору блокчейн-систем є складним завданням, спрямованим на підвищення ефективності роботи мережі в умовах змінних характеристик передавання даних. Основною особливістю цього підходу є здатність алгоритму, який лежить в основі модуля, динамічно адаптувати параметри блокчейн-мережі залежно від поточного стану мережі передавання даних, таких як пропускна здатність, затримка, джитер, завантаження пулу непідтверджених транзакцій та навантаження на центральний процесор. Це дозволяє підвищити продуктивність мережі, зменшити затримки під час передавання даних та забезпечити стійкість до навантажень.

Модуль прийняття рішень адаптивного вибору консенсусу блокчейн-мережі передбачає використання аналітичної моделі, яка регулярно оцінює стан мережі, відстежуючи ключові мережеві характеристики. На основі цих даних відбувається динамічне коригування параметрів, зокрема розміру блоку, частоти генерації блоків, складності обчислень для консенсусу, а також максимальної кількості транзакцій у блоці. Така архітектура дозволяє гнучко реагувати на зміни в мережі, наприклад, на збільшення користувацького трафіку або тимчасові стрибки інтенсивності передавання даних.

Для кожного алгоритму консенсусу адаптивний підхід має свої особливості. В алгоритмі PoW найважливішим параметром є складність обчислень, яка

безпосередньо впливає на час підтвердження блоку [25, 26]. В умовах перевантаження мережі алгоритм може знижувати складність, скорочуючи час генерації блоків і зменшуючи навантаження на мережу. У PoS основна увага приділяється механізму вибору валідатора, де адаптивний алгоритм може регулювати частоту генерації блоків і кількість транзакцій у блоці.

В алгоритмі DPoS ключовим завданням є перерозподіл навантаження між делегатами, що дозволяє уникнути перевантажень на окремих вузлах [27–29]. У випадку PoET адаптивний підхід може впливати на тривалість часових інтервалів очікування [30], регулюючи загальне навантаження на систему [31, 32].

Методика інтеграції модуля прийняття рішень.

Крок 1. Аналіз мережі передавання даних і блокчейн-архітектури.

На першому етапі необхідно провести глибокий аналіз мережевих компонентів і фізичних пристроїв мережі.

Цей етап включає збір статистичних даних системи, а також дослідження граничних значень мережевих характеристик, структури блокчейн-мережі: розподіл вузлів, підтримувані алгоритми консенсусу та архітектурні обмеження. Результати аналізу використовуються для вибору параметрів адаптації.

Крок 2. Розробка аналітичної моделі мережі та алгоритму консенсусу.

Уточнюється раніше представлена математична модель, що описує роботу мережі залежно від її параметрів. Вона має враховувати потоки користувацького та блокчейн-трафіку, параметри блокчейн-мережі (розмір блоку, частоту генерації тощо).

Окремо для кожного алгоритму консенсусу описуються специфічні аспекти, які можуть піддаватися адаптації.

Крок 3. Інтеграція модуля моніторингу мережевих характеристик.

Модуль моніторингу впроваджується у вузли мережі з метою відстеження даних про пропускну здатність, затримку, джитер і поточне навантаження на вузол (CPU, пам'ять, диск).

Регулярний моніторинг заповненості пулу непідтверджених транзакцій і швидкості обробки транзакцій також входить до функціоналу модуля моніторингу.

Агрегована інформація надходить до модуля прийняття рішень у режимі реального часу.

Крок 4. Інтеграція адаптивного модуля прийняття рішень.

Основою адаптивного підходу є модуль, який аналізує зібрані дані та ініціює зміни параметрів блокчейн-мережі з метою коригування навантаження на мережу передавання даних.

На цьому етапі відбувається інтеграція модуля у вузли мережі. Модуль використовує набір правил і умов для зміни параметрів мережі.

Крок 5. Калібрування параметрів адаптивного алгоритму.

На основі початкового моніторингу здійснюється уточнення параметрів. Коригуються оптимальні порогові значення для кожного мережевого показника, налаштовуються часові інтервали реакції модуля на зміни в мережі, а також уточнюється логіка адаптації для різних сценаріїв.

Крок 6. Оцінка ефективності та коригування на основі реальних даних.

Після розгортання модуля прийняття рішень необхідно регулярно оцінювати його ефективність. Для цього виконуються обчислення і порівняння мережевих характеристик до та після впровадження адаптивного підходу.

Також на цьому етапі проводиться аналіз можливих проблем, зокрема надмірної реакції модуля на незначні зміни в мережі. За потреби алгоритм доопрацьовується з урахуванням нових умов роботи.

Крок 7. Підготовка методичних рекомендацій і масштабування.

Після успішної інтеграції та стабілізації модуля необхідно сформувати методичні рекомендації для адміністраторів мережі — інструкції з налаштування параметрів адаптації.

Для подальшого розвитку модуля та мережі в цілому слід опрацювати сценарії масштабування на більші мережі або нові алгоритми консенсусу, а також розробити підходи до інтеграції з різними рівнями мережевої

інфраструктури, включно з використанням хмарних технологій для підвищення продуктивності.

Представлена методика забезпечує комплексний підхід до інтеграції модуля прийняття рішень адаптивного вибору консенсусу блокчейн-мережі, що дозволяє не лише підвищити продуктивність блокчейн-системи, а й зробити її більш стійкою до змін у характеристиках передавання даних.

4.4 Оцінювання ефективності адаптивного вибору блокчейн-систем з урахуванням характеристик трафіку в мережах зв'язку

Оцінювання ефективності адаптивного підходу до вибору блокчейн-системи в умовах змінних параметрів мережевого трафіку є важливим етапом верифікації працездатності запропонованої архітектури. Така методика дозволяє кількісно визначити, наскільки вдало адаптивний механізм справляється з реальними навантаженнями, забезпечує стабільність функціонування системи та підвищення її продуктивності.

Крок 1. Визначення початкових параметрів

Необхідно визначити загальну кількість вузлів у мережі, середню частоту генерації блоків та часовий інтервал, на якому розраховується ефективність. Ці параметри є ключовими для подальших обчислень.

Крок 2. Визначення загальної кількості блоків

Слід обчислити загальну кількість блоків, створених усіма вузлами за заданий період часу. Це значення стане основою для подальшої оцінки ефективності модуля прийняття рішень.

Крок 3. Визначення приблизної кількості блоків, створених неактуальним алгоритмом консенсусу

Для обчислення кількості блоків, згенерованих застарілим алгоритмом консенсусу протягом певного періоду, необхідно провести відповідні розрахунки. Цей процес передбачає множення кількості вузлів на рівень генерації блоків та ймовірність обізнаності про новий алгоритм. Отриманий

результат дозволяє оцінити, скільки блоків було створено вузлами, які ще не отримали інформацію про оновлення системи.

Крок 4. Розрахунок ефективності модуля прийняття рішень адаптивного вибору консенсусу блокчейн-мережі

Ефективність модуля можна визначити за формулою. Це дозволяє кількісно оцінити, наскільки краще працює адаптивний модуль у порівнянні зі статичним алгоритмом консенсусу.

Підставивши відповідні значення часу поширення інформації, можна виявити залежність ефективності від діаметра мережі, який характеризує максимальну відстань між вузлами. Частота генерації транзакцій також може істотно впливати на навантаження в мережі та, відповідно, на час передачі повідомлень між вузлами.

Крок 5. Вплив діаметра мережі на ефективність

Для графів з властивостями «малого світу» або випадкових графів можна встановити залежність між діаметром і кількістю вузлів. Це дозволяє додатково спростити обчислення ефективності модуля прийняття рішень.

Крок 6. Висновки щодо впливу різних факторів на ефективність

У підсумку можна зробити низку висновків щодо впливу окремих факторів на ефективність запропонованого підходу:

- Збільшення кількості вузлів призводить до логарифмічного зниження ефективності, оскільки зростає діаметр мережі.

- Підвищення швидкості передачі даних сприяє зростанню ефективності завдяки зменшенню затримок.

- Збільшення часу генерації блоків потенційно може підвищити ефективність, оскільки зменшується ймовірність конфліктів.

- Зростання частоти створення транзакцій може знизити ефективність, особливо якщо це суттєво впливає на швидкість передачі інформації у мережі.

4.5 Висновки до розділу 4

Проведено оцінювання швидкості розповсюдження інформації мережею в межах модельного стенда ITS. Розроблено модель оцінювання ефективності модуля прийняття рішень для адаптивного вибору алгоритму блокчейн-системи, яка враховує низку параметрів. Проведено апробацію розробленої моделі оцінювання ефективності з використанням аналітичних розрахунків та імітаційного моделювання. Представлено методики інтеграції модуля прийняття рішень та оцінювання його ефективності.

5 ОХОРОНА ПРАЦІ

Соціальна значимість охорони праці полягає у її позитивному впливі на продуктивність та якість суспільного виробництва, що досягається шляхом безперервного поліпшення умов праці. Забезпечення належного рівня охорони праці сприяє підвищенню загальної безпеки трудової діяльності, зменшенню кількості нещасних випадків на виробництві та зниженню професійної захворюваності. Крім того, створення безпечних та здорових умов праці позитивно впливає на психологічний клімат у колективі, підвищує задоволеність працівників своєю роботою та сприяє зростанню їхньої мотивації. Інвестиції в охорону праці є не лише соціально відповідальним кроком, але й економічно вигідним рішенням, що призводить до зменшення витрат, пов’язаних з лікарняними виплатами, компенсаціями та втратою кваліфікованих кадрів.

Аналіз умов праці проводимо на робочому місці, де здійснювалося дослідження на тему «Коригування інформаційного трафіку телекомунікаційних систем із використанням технології блокчейн», яке обладнане комп’ютером із відповідним програмним забезпеченням. На розробника, відповідно до Гігієнічної класифікації праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу, могли мати вплив такі небезпечні та шкідливі виробничі фактори:

1. Фізичні: підвищена запиленість та загазованість повітря робочої зони; підвищений рівень шуму на робочому місці; підвищена чи понижена вологість повітря; підвищений рівень статичної електрики; підвищений рівень електромагнітного випромінювання; недостатня освітленість робочої зони.

2. Психофізіологічні: розумове перевантаження; перенапруга аналізаторів; статичне перевантаження.

Відповідно до визначених факторів формуємо рішення щодо безпечного виконання роботи.

5.1 Технічні рішення щодо безпечного виконання роботи

5.1.1 Обладнання приміщення та робочого місця

Розміри приміщення, в якому проводилися дослідження (зокрема його площа та об’єм), перш за все повинні бути достатніми для комфортного розміщення працівників та необхідного технічного обладнання. Згідно з НПАОП 0.00-7.15-18, на одного співробітника, що працює з комп’ютером, має припадати не менше 6,0 м² площі та 20 м³ об’єму. Фактичні розміри робочого приміщення становлять 18,8 м² площі та 60,2 м³ об’єму, що забезпечує на одного працівника 6,3 м² площі та 20,1 м³ повітря. Таким чином, отримані показники повністю відповідають встановленим нормативним вимогам.

Організація робочого місця дослідника, включаючи взаємне розташування всіх його компонентів, відповідає антропометричним, фізичним та психологічним критеріям, визначеним ДСТУ 8604:2015. При його облаштуванні особливу увагу було приділено характеру виконуваної роботи та забезпечено оптимальне розміщення необхідного обладнання, а також достатній робочий простір для зручного виконання всіх потрібних рухів та переміщень.

Раціональне планування робочого місця передбачає чіткий порядок і сталість розміщення предметів, засобів праці і документації. Те, що потрібно для виконання робіт частіше, розташоване в зоні легкої досяжності робочого простору.

Основні вимоги щодо роботи на ПК включають такі аспекти:

- заборонено залишати комп'ютери та їхні пристрої без нагляду;

- підключати і відключати роз'єми кабелів пристроїв ПК лише при вимкненій напрузі, щоб уникнути нещасних випадків;

- перед включенням пристроїв та окремих блоків ПК необхідно переконатися у надійності кріплення провідників заземлення, справності кабелів і роз'ємів електричної мережі;

- у разі виявлення запаху горілого в пристроях ПК негайно вимкнути обладнання, не включати його повторно та звернутися до спеціаліста для технічного обслуговування;

- для запобігання порушень і підтримання працездатності, дотримуватися графіку перерв для відпочинку під час роботи на ПК. Необхідно передбачити короткі перерви для відпочинку кожні 40-45 хвилин роботи за дисплеєм. Загальний час, проведений за монітором, не повинен перевищувати 4 години на день та 20 годин на тиждень.

5.1.2 Електробезпека приміщення

Для гарантування електробезпеки обладнання та захисту користувачів комп’ютерів від ураження електричним струмом, приміщення з комп'ютеризованими робочими місцями повинні бути обладнані необхідними технічними засобами захисту, що відповідають вимогам ДСТУ Б В.2.5-82:2016. Згідно з Правилами улаштування електроустановок (ПУЕ), дане приміщення належить до категорії приміщень без підвищеної електричної небезпеки.

Електроживлення приладів, периферійних пристроїв комп’ютера, а також обладнання для обслуговування, ремонту та налагодження ПК забезпечується окремою груповою трипровідною мережею, що включає фазний, нульовий робочий та нульовий захисний провідники. Нульовий захисний провідник використовується для здійснення заземлення (занулення) електроприймачів.

Комп’ютери, периферійні пристрої, обладнання для їхнього обслуговування, ремонту та налагодження, а також інше технічне обладнання, таке як апарати керування, контрольно-вимірювальні прилади та освітлювальні пристрої, повинні відповідати встановленому класу зони згідно з Правилами улаштування електроустановок (ПУЕ) та бути оснащені налагодженою апаратурою захисту від коротких замикань та інших аварійних ситуацій. Під час монтажу та експлуатації електромереж необхідно вжити всіх можливих заходів для повного виключення ймовірності виникнення електричного джерела

займання внаслідок короткого замикання та перевантаження проводів. Рекомендується мінімізувати використання проводів з легкозаймистою ізоляцією, віддаючи перевагу, де це можливо, матеріалам з негорючою ізоляцією. Всі ці запобіжні заходи спрямовані на гарантування безпечної експлуатації електрообладнання та запобігання пожежам і аваріям.

Слід також забезпечити сумісність електрообладнання та електричних мереж з системою заземлення та робочою напругою. Усі електричні проводи та кабелі підлягають обов'язковому заземленню, а стан заземлюючих пристроїв необхідно регулярно перевіряти. Особливу увагу слід приділити захисту від накопичення статичної електрики, що є актуальним при роботі з електронними пристроями. Для цього рекомендується застосовувати антистатичні матеріали та спеціальні засоби для зняття статичного заряду.

При виявленні будь-яких відхилень у функціонуванні електрообладнання або виникненні підозри на нештатну роботу електричних систем слід негайно припинити його експлуатацію та звернутися до компетентного спеціаліста для проведення діагностики та усунення несправності. Регулярна оцінка стану та працездатності електроустаткування є необхідною для запобігання потенційним негативним наслідкам, які можуть бути спричинені його поломкою або неналежним використанням.

5.2 Технічні рішення з гігієни праці та виробничої санітарії

5.2.1 Мікроклімат

Нормування мікроклімату на робочому місці відбувається згідно ДСН 3.3.6.042-99. Дослідження, яке було проведене, за енерговитратами відноситься до категорії I а (енерговитрати до 139Дж/с). Допустимі параметри мікроклімату для цієї категорії наведені в табл. 5.1.

Таблиця 5.1 – Параметри мікроклімату

Період року	Допустимі		
	t,°C	W, %	V, м/с
Теплий	22-28	55	0,1-0,2
Холодний	21-25	75	0,1

Для досягнення необхідних за нормативами параметрів мікроклімату в приміщенні передбачено такі заходи:

Для забезпечення відповідності параметрів мікроклімату в приміщенні встановленим нормам передбачено наступний комплекс заходів:

- У холодну пору року для підтримання оптимальної температури використовується централізована система парового опалення.

- Необхідні метеорологічні умови для комфортного робочого середовища забезпечуються за допомогою системи кондиціонування, яка здійснює регулювання температури та вологості повітря.

Для підтримання нормативного рівня вологості в приміщенні регулярно проводиться вологе прибирання поверхонь та видалення забруднень.

Персонал проходить систематичне навчання та інструктажі щодо важливості дотримання нормативних параметрів мікроклімату та правильного використання систем опалення та кондиціонування для досягнення цієї мети.

5.2.2 Склад повітря робочої зони

У повітрі досліджуваного приміщення потенційно можуть бути присутні такі шкідливі речовини, як пил, вуглекислий газ та озон. Основним джерелом озону є офісне обладнання, зокрема принтер. Пил проникає до приміщення з зовнішнього середовища. Гранично допустимі концентрації (ГДК) виявлених шкідливих речовин у повітрі наведені у таблиці 5.2.

Таблиця 5.2 – ГДК шкідливих речовин у повітрі

Назва речовини	ГДК, мг/м^3		Клас небезпечності
	Максимально разова	Середньо добова	
Пил нетоксичний	10	4	4
Озон	0,16	0,03	1
Вуглекислий газ	3	1	4

Підтримка відповідних параметрів повітря в робочій зоні забезпечується завдяки системі кондиціювання та регулярному вологому прибиранню приміщення.

5.2.3 Виробниче освітлення

У приміщенні, де здійснюється дослідження використовується штучне та природне освітлення. Робочі місця по відношенню до світлових прорізів повинні розташовуватися так, щоб природне світло падало збоку, переважно зліва.

Норми освітленості при штучному освітленні та КПО (для III пояса світлового клімату згідно з вимогами ДБН В.2.5-28:2018 «Природне і штучне освітлення») при природному та сумісному освітленні зазначені у таблиці 5.3.

Таблиця 5.3 - Норми освітленості в приміщенні

Характеристика зорової роботи	Найменший розмір об'єкта розрізнювання	Розряд зорової роботи	Підрозряд зорової роботи	Контраст об'єкта розрізнення з фоном	Характеристика фона	Освітленість, лк		КПО, %			
						Штучне освітлення		Природнє освітлення		Сумісне освітлення	
						Комбіноване	Загальне	Верхнє або верхнє і бокове	Бокове	Верхнє або верхнє і бокове	Бокове
Дуже високої точності	Від 0,15 до 0,3	II	г	великий	світлий	750	200	7	2,5	4,2	1,5

Для забезпечення належного рівня освітленості в приміщенні регулярно проводиться очищення віконного скла та світильників від пилу. Для контролю рівня природного освітлення використовуються жалюзі. У випадках недостатнього природного світла застосовується загальне штучне освітлення, що створюється за допомогою світлодіодних (LED) ламп. Залежно від потреб приміщення можуть використовуватись різні типи LED-ламп, наприклад, лінійні LED-трубки, панельні світильники або точкові LED-світильники, що дозволяє створити оптимальне освітлення для різних робочих зон.

5.2.4 Виробничий шум

Шум є несприятливим фактором робочого середовища, що негативно позначається на самопочутті та працездатності людини. Тривалий вплив шуму може спричинити погіршення зору, слуху, підвищення артеріального тиску та послаблення концентрації уваги. Інтенсивний та тривалий шумовий вплив здатен викликати функціональні порушення серцево-судинної та нервової систем. Для умов виконання роботи допустимі рівні звукового тиску повинні наведені в таблиці 5.4 (згідно ДСН 3.3.6.037-99).

Таблиця 5.4 – Допустимі рівні звукового тиску і рівні звуку для постійного широкополосного шуму

Характер робіт	Допустимі рівні звукового тиску (дБ) в стандартизованих октавних смугах зі середньогеометричними частинами (Гц)									Допуст-мий рівень звуку, дБА
	32	63	125	250	500	1000	2000	4000	8000	
Виробничі приміщення	86	71	61	54	49	45	42	40	38	50

Рівень шуму в досліджуваному приміщенні відповідає встановленим нормам. В разі появи підвищеного рівня шуму, необхідно усунути або знизити його джерело. Це можна зробити за допомогою звукопоглинаючих матеріалів, які поглинають звукові хвилі, або шляхом раціонального планування приміщення, яке дозволить зменшити відбиття шуму від стін, стелі та підлоги.

5.2.5 Виробничі випромінювання

У процесі роботи з ПК працівник зазнає впливу електромагнітного випромінювання. Тривала дія цього випромінювання, особливо низькочастотних полів, що генеруються обладнанням, може становити ризик для здоров'я. Зокрема, такі поля можуть спричиняти порушення фізіологічних функцій, включаючи головний біль, розлади сну, зниження здатності до концентрації уваги та підвищення ймовірності розвитку серцево-судинних захворювань. Допустимі значення параметрів неіонізуючих електромагнітних випромінювань на робочому місці в процесі дослідження наведені в таблиці 5.5.

Таблиця 5.5 – Допустимі значення параметрів неіонізуючих електромагнітних випромінювань

Найменування параметра	Допустимі значення
Напруженість електричної складової електромагнітного поля на відстані 50см від поверхні відеомонітора	10В/м
Напруженість магнітної складової електромагнітного поля на відстані 50см від поверхні відеомонітора	0,3А/м
Напруженість електростатичного поля не повинна перевищувати: для дорослих користувачів для дітей дошкільних установ і що вчаться середніх спеціальних і вищих учбових закладів	20кВ/м 15кВ/м

Мінімізація впливу електромагнітного випромінювання на працівника досягається шляхом дотримання оптимального режиму праці та відпочинку. Такий режим передбачає: регулярні робочі перерви для зменшення навантаження на очі, шию та спину; активний відпочинок, що сприяє зняттю стресу та покращенню кровообігу; а також збалансоване харчування та достатній сон для підтримки загального стану здоров’я.

5.3 Пожежна безпека

Першочерговим завданням є запобігання пожежам шляхом усунення умов для утворення горючих або вибухонебезпечних середовищ та джерел займання. На підприємстві необхідно вжити дієвих заходів пожежної безпеки для мінімізації ризиків для персоналу та обмеження матеріальних втрат у випадку пожежі. Забезпечення пожежної безпеки об’єкта включає систему запобігання пожежам, протипожежний захист та комплекс організаційно-технічних заходів. Головна мета пожежної безпеки полягає у дотриманні нормативних вимог та недопущенні виникнення пожеж. У разі їх виникнення, ключовими цілями є локалізація розповсюдження вогню, своєчасне виявлення та ліквідація загоряння, а також захист життя та здоров’я людей і збереження матеріальних цінностей. Дане приміщення належить до категорії «Д». Ефективна система пожежної безпеки є запорукою збереження людських життів та матеріальних цінностей. Регулярний аудит та вдосконалення протипожежних заходів є невід'ємною частиною відповідального управління підприємством. Інвестування в пожежну безпеку є не витратою, а стратегічним внеском у стабільність та безпеку бізнесу.

5.3.1 Технічні рішення системи запобігання пожежі

У приміщенні виявлено ряд факторів, що несуть потенційну загрозу виникнення пожежі, а саме: перевантаження електромережі та надмірне нагрівання струмопровідних елементів і з’єднань; недотримання правил використання технічного обладнання; недостатній рівень електробезпеки, що включає перевантаження електромереж та неефективне заземлення, здатні призвести до перегріву та короткого замикання; порушення правил експлуатації електроприладів, наприклад, їх некоректне підключення або залишення без нагляду у ввімкненому стані; а також несправність електрообладнання, зокрема пошкодження ізоляції, зношені кабелі та дефекти в електричних пристроях.

Система запобігання пожежі включає комплекс таких заходів: систематична перевірка цілісності ізоляційних матеріалів; облаштування спеціально визначених місць для куріння; регулярне проведення протипожежних навчань та інструктажів для персоналу; недопущення накопичення займистих матеріалів у приміщенні; а також встановлення системи грозозахисту. Впровадження цих заходів спрямоване на мінімізацію ймовірності виникнення пожежі, забезпечення безпеки працівників та збереження майна, а також на дотримання вимог нормативних документів з пожежної безпеки. Про будь-які несправності протипожежного обладнання необхідно негайно повідомляти до пожежної служби. Важливим елементом є також контроль за справністю електрообладнання та недопущення його перевантаження. Регулярне прибирання приміщень від пилу та горючого сміття також є важливим превентивним заходом. Крім того, слід проводити роз'яснювальну роботу серед персоналу щодо правил пожежної безпеки та їх неухильного дотримання.

5.3.2 Технічні рішення системи протипожежного захисту

Технічні рішення системи протипожежного захисту для досліджуваного приміщення зосереджені на ранньому виявленні загоряння, обмеженні його поширення на початковій стадії та забезпеченні можливості безпечної евакуації. Зважаючи на невелику кількість обладнання акцент робиться на первинних засобах пожежогасіння.

У приміщенні передбачено встановлення одного порошкового вогнегасника типу ВП-3 на висоті, що не перевищує 1,5 метра від рівня підлоги до його нижньої частини, у місці, яке забезпечує безперешкодне повне відчинення дверей. Для чіткої ідентифікації місця розташування вогнегасника буде розміщено відповідний вказівний знак на видних ділянках стін на висоті від 2,0 до 2,5 метра від підлоги.

Крім того, рекомендовано встановити хоча б один димовий пожежний сповіщувач. Димові сповіщувачі є найбільш ефективними для виявлення пожежі на ранній стадії, особливо при горінні електронного обладнання, яке часто супроводжується виділенням диму. Для підвищення рівня безпеки та оперативності реагування на можливе загоряння, бажано інтегрувати димовий сповіщувач з системою оповіщення про пожежу. Також слід забезпечити регулярну перевірку працездатності сповіщувача та своєчасну заміну елементів живлення для гарантування його безперебійної роботи. Розміщення димового сповіщувача в найбільш ймовірному місці виникнення пожежі, наприклад, поблизу електрообладнання, значно підвищить ефективність раннього виявлення.

Електропроводка виконана згідно з вимогами ПУЕ та має надійну ізоляцію. Електрична мережа оснащена автоматичними вимикачами (автоматами) відповідного номіналу для захисту від перевантажень та коротких замикань. Усі працівники пройшли інструктаж з пожежної безпеки, знають місця розташування первинних засобів пожежогасіння та порядок дій у разі пожежі. На видному місці розміщений план евакуації з приміщення у випадку пожежі.

Застосування цих технічних рішень у комплексі з організаційними заходами дозволяє забезпечити достатній рівень протипожежного захисту для приміщення, створюючи безпечне робоче середовище та мінімізуючи потенційні ризики, пов’язані з виникненням пожежі. Регулярний контроль стану електромережі та первинних засобів пожежогасіння, а також періодичне проведення протипожежних тренувань підтримують належний рівень готовності до можливих надзвичайних ситуацій. Дотримання цих заходів є запорукою збереження життя та здоров'я працівників, а також матеріальних цінностей підприємства.

ВИСНОВКИ

У роботі розроблено та протестовано модуль прийняття рішень для вибору блокчейн-системи з метою зменшення кількості втрачених блоків транзакцій з урахуванням впливу мережевих характеристик. Процес розробки включав кілька ключових етапів, кожен із яких був ретельно проаналізований і оптимізований для досягнення максимальної ефективності:

1. Проведено аналіз мережевих характеристик та архітектури блокчейн-мережі. Найважливішими параметрами для адаптації стали: пропускна здатність, затримка, джиттер, а також інші характеристики, що впливають на стабільність роботи мережі. Сформовано теоретичну основу для динамічного регулювання параметрів роботи блокчейн-мережі залежно від змін у мережевих умовах.

2. Розроблено аналітичну модель мережі зв’язку з блокчейном. У процесі розробки уточнено основні параметри, такі як розмір блоку, частота генерації блоків та типи консенсусу, які можуть адаптуватися залежно від поточного стану мережі. Створення моделі дозволило точно охарактеризувати поведінку мережі та виявити можливі слабкі місця, що потребують удосконалення.

3. Розроблено імітаційну модель мережі зв’язку з модулем прийняття рішень щодо вибору блокчейн-системи для зниження кількості втрачених транзакційних блоків. Результати аналітичного розрахунку та імітаційного моделювання продемонстрували розбіжність не більше ніж 5%.

4. Інтегровано модуль моніторингу мережевих характеристик. Модуль є ключовою ланкою системи, що дозволяє в реальному часі відстежувати такі параметри, як пропускна здатність мережі, затримка, джиттер, а також завантаження процесора та пам’яті вузлів. Ці дані дозволяють алгоритму приймати рішення щодо доцільності перемикання на більш відповідний алгоритм консенсусу відповідно до поточного навантаження.

5. Інтегровано адаптивний модуль прийняття рішень, який на основі зібраних даних може в режимі реального часу змінювати параметри роботи мережі. Модуль приймає рішення про перемикання між алгоритмами

консенсусу, що дозволяє оптимізувати роботу блокчейн-мережі та зменшити час обробки транзакцій. В результаті імітаційного моделювання було продемонстровано, що модуль здатен суттєво покращити продуктивність мережі, зменшуючи втрати даних та підвищуючи пропускну здатність за умов підвищеного навантаження. Отримані результати показали, що використання системи з модулем прийняття рішень та адаптивною зміною консенсусу на 10% ефективніше, ніж при застосуванні статичного алгоритму консенсусу. Також було проаналізовано можливі проблеми, такі як надмірна реакція модуля на незначні зміни в мережі, що дозволило внести відповідні коригування в його роботу.

6. На завершальному етапі підготовлено методики інтеграції модуля прийняття рішень і оцінки його ефективності, які передбачають можливість використання у більших мережах і з іншими алгоритмами консенсусу. Методики також включають рекомендації щодо інтеграції з різними рівнями мережевої інфраструктури, що забезпечує гнучкість і масштабованість рішення в майбутньому.

Проведене дослідження продемонструвало, що використання адаптивності при виборі та зміні алгоритмів консенсусу в блокчейн-мережах дозволяє не лише підвищити ефективність системи в умовах змінних мережевих характеристик, але й значно покращити стійкість та продуктивність мереж, забезпечуючи їхню довговічність і масштабованість в умовах високих навантажень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. S. Zhang, L. Ni, W. Xie, G. Li and H. Sun, "Research on Self-Adaptive Consensus Method Based on Blockchain," 2022 IEEE 14th International Conference on Advanced Infocomm Technology (ICAIT), Chongqing, China, 2022, pp. 292-297, doi: 10.1109/ICAIT56197.2022.9862639.

2. A. H. Mohammed, A. A. Abdulateef and I. A. Abdulateef, "Hyperledger, Ethereum and Blockchain Technology: A Short Overview," 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2021, pp. 1-6, doi: 10.1109/HORA52670.2021.9461294.

3. S. Barac, I. Botički, G. Perković, V. Radošević and I. Terzić, "Cardano - What Is It and How to Start Working with It," 2023 46th MIPRO ICT and Electronics Convention (MIPRO), Opatija, Croatia, 2023, pp. 1727-1732, doi: 10.23919/MIPRO57284.2023.10159944.

4. B. H. Swathi, M. S. Meghana and P. Lokamathe, An Analysis on Blockchain Consensus Protocols for Fault Tolerance, 2021 2nd International Conference for Emerging Technology (INCET), Belagavi, India, 2021, pp. 1-4, doi: 10.1109/INCET51464.2021.9456310.

5. J. Pan, Z. Song and W. Hao, "Development in Consensus Protocols: From PoW to PoS to DPoS," 2021 2nd International Conference on Computer Communication and Network Security (CCNS), Xining, China, 2021, pp. 59-64, doi: 10.1109/CCNS53852.2021.00020.

6. J. Alotaibi and L. Alazzawi, "SaFIoV: A Secure and Fast Communication in Fog-based Internet-of-Vehicles using SDN and Blockchain," 2021 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS), 2021, pp. 334-339, doi: 10.1109/MWSCAS47672.2021.9531857.

7. K. Mershad and B. Said, "A Blockchain Model for Secure Communications in Internet of Vehicles," 2020 IEEE/ACS 17th International Conference on Computer Systems and Applications (AICCSA), 2020, pp. 1-6, doi: 10.1109/AICCSA50499.2020.9316498.

8. M. B. Mollah et al., "Blockchain for the Internet of Vehicles Towards Intelligent Transportation Systems: A Survey," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4157-4185, 15 March15, 2021, doi: 10.1109/JIOT.2020.3028368.

9. L. Lei, P. Ma, C. Lan and L. Lin, "Continuous Distributed Key Generation on Blockchain Based on BFT Consensus," 2020 3rd International Conference on Hot Information-Centric Networking (HotICN), Hefei, China, 2020, pp. 8-17, doi: 10.1109/HotICN50779.2020.9350834

10. M. Bachmann, L. H. Acosta, J. Götz, D. Reinhardt and K. David, "Collision Avoidance for Vulnerable Road Users: Privacy versus Survival?," NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 2022, pp. 1-6, doi: 10.1109/NOMS54207.2022.9789710.

11. I. Rashdan and S. Sand, "Link-Level Performance of Vehicle-to-Vulnerable Road Users Communication Using Realistic Channel Models," 2024 18th European Conference on Antennas and Propagation (EuCAP), Glasgow, United Kingdom, 2024, pp. 1-5, doi: 10.23919/EuCAP60739.2024.10501335.

12. M. Rupp and L. Wischhof, "Evaluation of the Effectiveness of Vulnerable Road User Clustering in C-V2X Systems," 2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS), Berlin, Germany, 2023, pp. 1-5, doi: 10.1109/COINS57856.2023.10189204.

13. P. R. Nair and D. R. Dorai, "Evaluation of Performance and Security of Proof of Work and Proof of Stake using Blockchain," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, pp. 279-283, doi: 10.1109/ICICV50876.2021.9388487.

14. S. Yan, "Analysis on Blockchain Consensus Mechanism Based on Proof of Work and Proof of Stake," 2022 International Conference on Data Analytics, Computing and Artificial Intelligence (ICDACAI), Zakopane, Poland, 2022, pp. 464-467, doi: 10.1109/ICDACAI57211.2022.00098.

15. M. A. Majumdar, M. Monim and M. M. Shahriyer, "Blockchain based Land Registry with Delegated Proof of Stake (DPoS) Consensus in Bangladesh," 2020

IEEE Region 10 Symposium (TENSYMP), Dhaka, Bangladesh, 2020, pp. 1756-1759, doi: 10.1109/TENSYMP50017.2020.9230612.

16. J. Mišić, V. B. Mišić and X. Chang, "Delegated Proof of Stake Consensus with Mobile Voters and Multiple Entry PBFT Voting," GLOBECOM 2022 - 2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 2022, pp. 6253-6258, doi: 10.1109/GLOBECOM48099.2022.10001051.

17. S. M. S. Saad, R. Z. R. M. Radzi and S. H. Othman, "Comparative Analysis of the Blockchain Consensus Algorithm Between Proof of Stake and Delegated Proof of Stake," 2021 International Conference on Data Science and Its Applications (ICoDSA), Bandung, Indonesia, 2021, pp. 175-180, doi: 10.1109/ICoDSA53588.2021.9617549.

18. A. Pal and K. Kant, "DC-PoET: Proof-of-Elapsed-Time Consensus with Distributed Coordination for Blockchain Networks," 2021 IFIP Networking Conference (IFIP Networking), Espoo and Helsinki, Finland, 2021, pp. 1-9, doi: 10.23919/IFIPNetworking52078.2021.9472787.

19. Y. Lu, S. Wang, and Y. Chen, “Blockchain-Enabled Secure Information Traffic Routing in Communication Networks,” IEEE Trans. on Network Science and Engineering*, vol. 7, no. 3, pp. 1458–1470, Aug. 2020.

20. A. K. Gupta and D. Pal, “Traffic Congestion Mitigation in Telecommunication Networks Using Blockchain Technology,” in Proc. IEEE International Conference on Communications (ICC), 2021, pp. 1632–1637.

21. R. Smith, L. Johnson, and M. Patel, “Intelligent Blockchain for Future Communications and Networking: Technologies, Trends and Applications,” IEEE Journal on Selected Areas in Communications, vol. 40, no. 12, pp. 3001–3015, Dec. 2022.

22. L. Chen, P. Liu, and R. Kumar, “Approaches to Modeling Blockchain Systems in Telecommunication Networks,” in Proc. 2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, 2020, pp. 203–208.

23. S. Bayraktar, S. Göran, and T. Serif, “Blockchain Interoperability for Future Telecoms,” Telecom, vol. 6, no. 1, Art. no. 20, Mar. 2025.

24. A. Li and Y. Zhao, “Blockchain Applications in Telecommunications: A Review,” IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 120–137, Mar. 2020.

25. V. Singh, “Blockchain-based Solutions for Information Traffic Optimization in Next-Generation Telecom Networks,” IEEE Network, vol. 35, no. 2, pp. 56–62, Mar. 2021.

26. M. Al-Bassam and H. R. Sheikh, “Smart Contracts for Automated Traffic Flow Management in Telecommunication Networks,” in Proc. IEEE International Symposium on Network Computing and Applications, 2020, pp. 199–205.

27. J. Patel, N. Kumar, and S. Rana, “Blockchain Scaling Solutions for High-Volume Telecommunication Traffic,” IEEE Access, vol. 9, pp. 10012–10025, 2021.

28. R. Gupta and A. Verma, “Improving Quality of Service in Telecommunications with Blockchain-based Traffic Management,” IEEE Trans. on Emerging Topics in Computing, vol. 8, no. 4, pp. 649–658, Oct. 2020.

29. L. Chen and H. Zhang, “Ensuring Data Integrity and Security in Telecommunication Systems Using Blockchain Technology,” IEEE Communications Magazine, vol. 59, no. 3, pp. 68–74, Mar. 2021.

30. R. Thompson, “Decentralized Traffic Management in Next-Generation Telecom Networks Using Blockchain,” in Proc. IEEE Global Communications Conference (GLOBECOM), 2022, pp. 1–6.

31. F. Rossi and G. Bianchi, “Integration of Blockchain Technology in 5G/6G Networks for Traffic Optimization,” IEEE Wireless Communications, vol. 28, no. 5, pp. 40–47, Oct. 2021.

32. P. Kumar, S. N. Singh, and D. Verma, “Consensus Algorithms in Blockchain for Real-Time Telecommunication Networks,” in Proc. IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2022, pp. 85–90.

33. H. Sun, Y. Li, and Z. Chen, “Blockchain-based Network Function Virtualization for Efficient Traffic Management in Telecom Networks,” IEEE Trans. on Network and Service Management, vol. 17, no. 4, pp. 2672–2682, Dec. 2020.

34. B. Martinez and E. Lopez, “Blockchain-Enabled Event-Driven Architectures for Dynamic Traffic Management in Telecommunications,” IEEE Internet Computing, vol. 25, no. 3, pp. 40–50, May 2021.

35. Наказ від 08.04.2014 № 248 Про затвердження Державних санітарних норм та правил Гігієнічна класифікація праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу - [Електронний ресурс] - Режим доступу: http://online.budstandart.com/ua/catalog/topiccatalogua/labor-protection/14._nakazy_ta_rozpor_183575/248+58074-detail.html

36. ДСТУ 8604:2015 Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги - [Електронний ресурс] - http://online.budstandart.com/ua/catalog/doc-page?id_doc=71028

37. ДСТУ Б В.2.5-82:2016 Електробезпека в будівлях і спорудах. Вимоги до захисних заходів від ураження електричним струмом- [Електронний ресурс] - Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=65395

38. ДБН В.2.5-28:2018 Природне і штучне освітлення - [Електронний ресурс] - Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=79885

39. ДСН 3.3.6.037-99 Санітарні норми виробничого шуму, ультразвуку та інфразвуку. - [Електронний ресурс] - Режим доступу: http://document.ua/sanitarni-normi-virobnichogo-shumu-ultrazvuku-ta-infrazvuku-nor4878.html

40. ДСН 3.3.6.042-99 Санітарні норми мікроклімату виробничих приміщень. - [Електронний ресурс] - Режим доступу: http://mozdocs.kiev.ua/view.php?id=1972

41. НПАОП 0.00-7.15-18 Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями. - [Електронний ресурс] - Режим доступу: http://sop.zp.ua/norm_npaop_0_00-7_15-18_01_ua.php

42. Правила улаштування електроустановок - [Електронний ресурс] - Режим доступу: http://www.energiy.com.ua/PUE.html

43. НАПБ А.01.001-14 Правила пожежної безпеки в Україні [Електронний ресурс] - Режим доступу: http://zakon.nau.ua/doc/?code=z1410-04

44. ДСТУ Б В.1.1-36:2016 Визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпек. URL: https://dbn.co.ua/load/normativy/dstu/dstu_b_v_1_1_36/5-1-0-1759

45. ДБН В.1.1.7-2016 Пожежна безпека об’єктів будівництва - [Електронний ресурс] - Режим доступу: http://www.poliplast.ua/doc/dbn_v.1.1-7-2002..pdf

Додаток А

(обов’язковий)

ІЛЮСТРАТИВНА ЧАСТИНА

КОРИГУВАННЯ ІНФОРМАЦІЙНОГО ТРАФІКУ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ БЛОКЧЕЙН

назва бакалаврської кваліфікаційної роботи

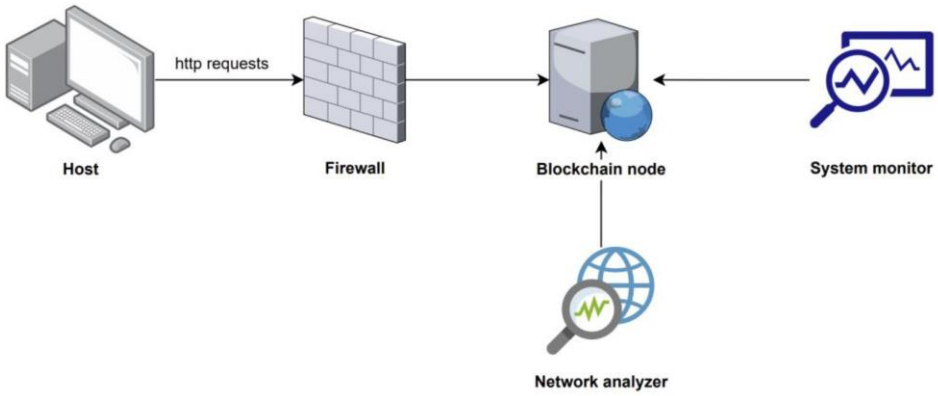

Рисунок 1 – Схема моделі системи для вимірювання змін апаратних параметрів обладнання з вузлом блокчейн-мережі

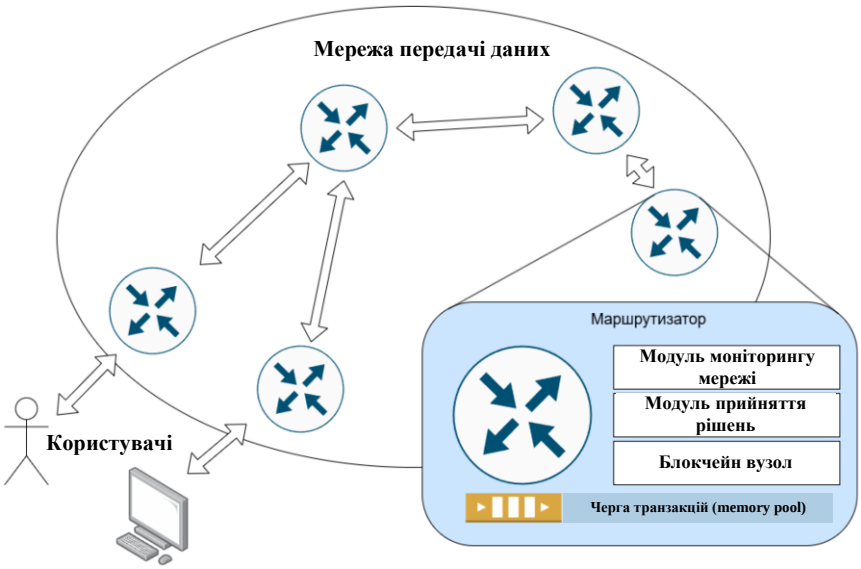

Рисунок 2 – Архітектура мережі зв’язку з інтегрованим блокчейн-шаром та модулем адаптивного алгоритму консенсусу

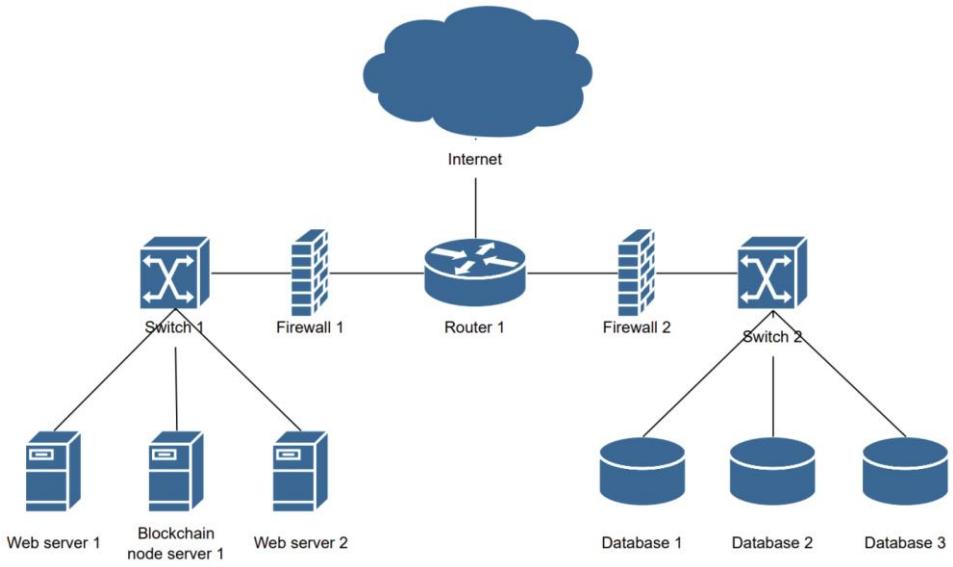

Рисунок 3 – Альтернативна схема інтеграції блокчейн-механізмів у мережеву інфраструктуру

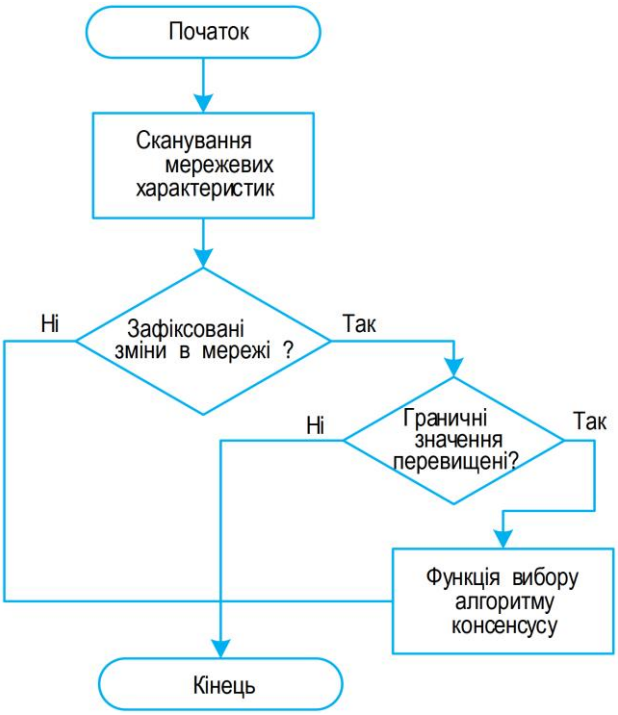

Рисунок 4 – Алгоритм вибору консенсусу з урахуванням динаміки мережевого середовища

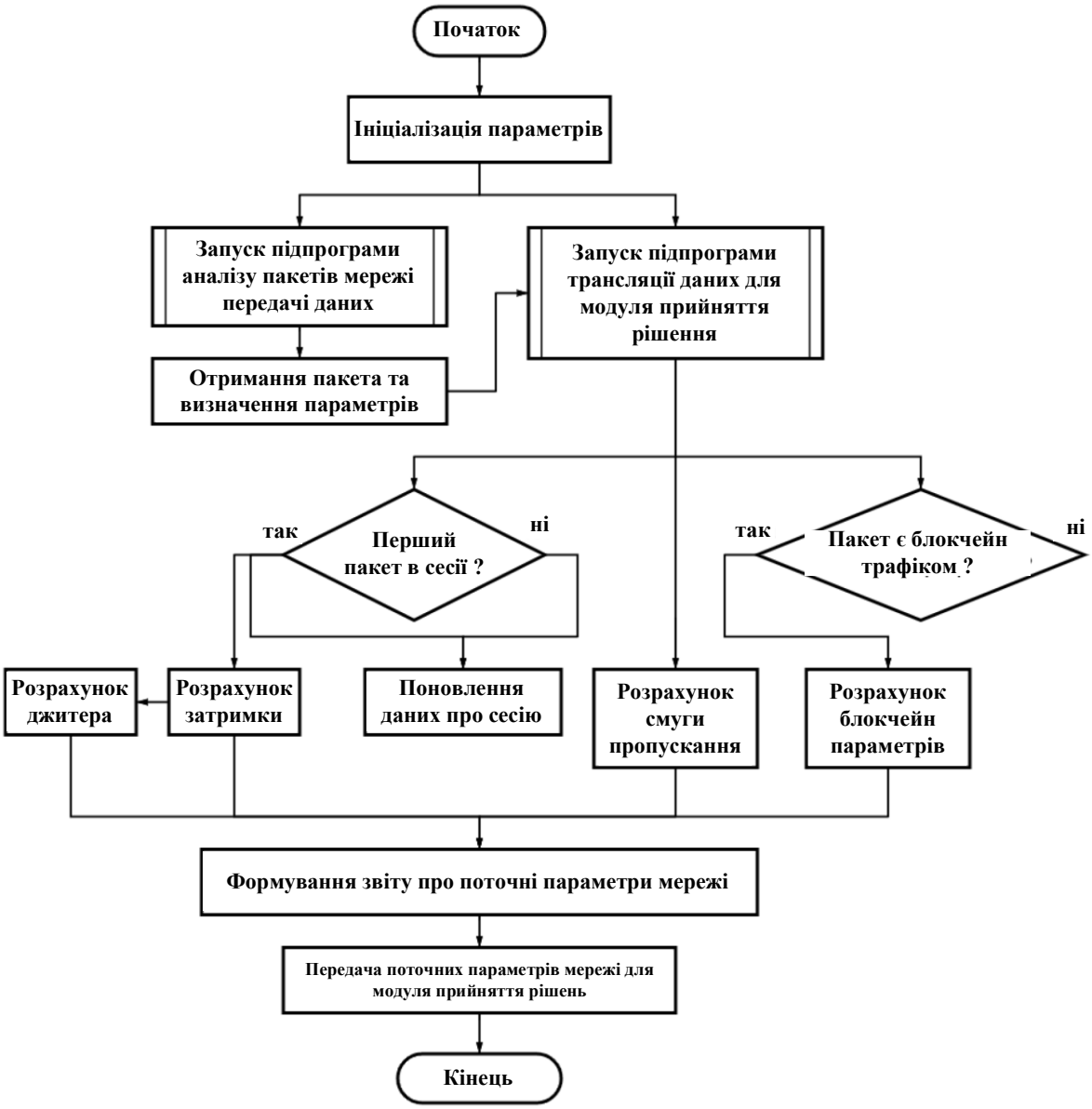

Рисунок 5 – Блок-схема роботи модуля моніторингу мережевого трафіку

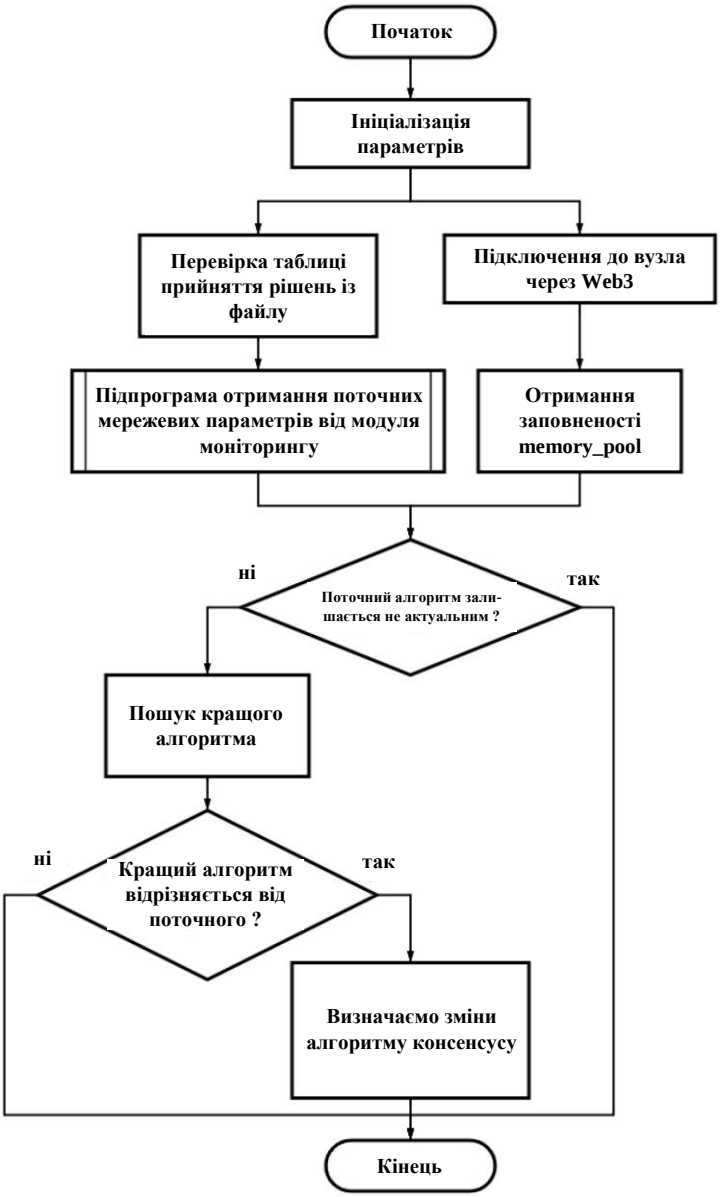

Рисунок 6 – Блок-схема роботи модуля прийняття рішень у блокчейн-мережі

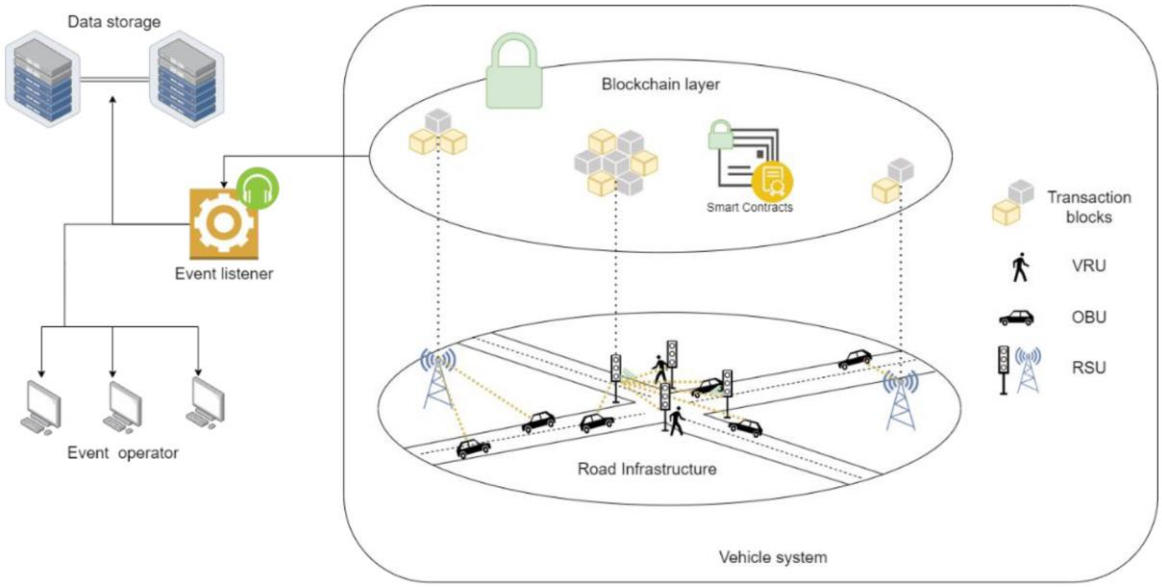

Рисунок 7 – Архітектура інтелектуальної транспортної системи (ITS) для сценарію оперативного реагування на надзвичайну подію

Додаток Б

ПРОТОКОЛ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Назва роботи: Коригування інформаційного трафіку телекомунікаційних систем із використанням технології блокчейн

Тип роботи: бакалаврська кваліфікаційна робота
(бакалаврська кваліфікаційна робота / магістерська кваліфікаційна робота)

Підрозділ кафедра ІКСТ, факультет ІЕС, група ПЗТ-23мс
(кафедра, факультет, навчальна група)

Коефіцієнт подібності текстових запозичень, виявлених у роботі системою StrikePlagiarism 10,37 %

Висновок щодо перевірки кваліфікаційної роботи (відмітити потрібне)

☑ Запозичення, виявлені у роботі, є законними і не містять ознак плагіату, фабрикації, фальсифікації. Роботу прийняти до захисту

☐ У роботі не виявлено ознак плагіату, фабрикації, фальсифікації, але надмірна кількість текстових запозичень та/або наявність типових розрахунків не дозволяють прийняти рішення про оригінальність та самостійність її виконання. Роботу направити на доопрацювання.

☐ У роботі виявлено ознаки плагіату та/або текстових маніпуляцій як спроб укриття плагіату, фабрикації, фальсифікації, що суперечить вимогам законодавства та нормам академічної доброчесності. Робота до захисту не приймається.

Експертна комісія:

Кичак В.М., завідувач кафедри ІКСТ _____
(прізвище, ініціали, посада) (підпис)

Васильківський М.В., гарант ОПП _____
(прізвище, ініціали, посада) (підпис)

Особа, відповідальна за перевірку _____ Васильківський М.В.
(підпис) (прізвище, ініціали)

З висновком експертної комісії ознайомлений(-на)

Керівник _____ Крижановський В.Г., професор кафедри ІКСТ
(підпис) (прізвище, ініціали, посада)

Здобувач _____ Нагорний Д.М.
(підпис) (прізвище, ініціали)