Міністерство освіти і науки України
Університет митної справи та фінансів

Факультет інноваційних технологій
Кафедра комп'ютерних наук та інженерії програмного забезпечення

Кваліфікаційна робота магістра

на тему: «Застосування технологій блокчейн для підвищення безпеки та прозорості розподілених систем»

Виконав: студент групи К23-1М
Спеціальність 122 «Комп'ютерні науки»
Кабка В.В._____ _____
(прізвище та ініціали)

Керівник к.ф.-м.н., доц. Лебідь О.Ю.
(науковий ступінь, вчене звання, прізвище та ініціали)

Рецензент ДДТУ
(місто роботи)
в.о. завідувача кафедри програмного забезпечення систем_____
(посада)
к.т.н., доцент Жульковський О. О._____
(науковий ступінь, вчене звання, прізвище та ініціали)

Дніпро – 2025

АНОТАЦІЯ

Кабка В.В. Застосування технологій блокчейн для підвищення безпеки та прозорості розподілених систем.

Дипломна робота на здобуття освітнього ступеня магістр за спеціальністю 122 «Комп'ютерні науки» – Університет митної справи та фінансів, Дніпро, 2025.

Магістерська робота присвячена дослідженню технологій блокчейн у контексті підвищення безпеки та прозорості розподілених систем. У роботі розглянуто основні принципи функціонування блокчейн, включаючи децентралізацію, криптографічну захищеність, механізми консенсусу та незмінність даних.

У ході дослідження проведено аналіз існуючих механізмів забезпечення безпеки в розподілених системах, включаючи традиційні централізовані підходи, та доведено переваги блокчейн для запобігання атакам, забезпечення цілісності даних і прозорості взаємодії між учасниками.

Практична частина роботи присвячена моделюванню блокчейн-архітектури для конкретної розподіленої системи, а також її програмній реалізації з урахуванням сучасних вимог до безпеки.

Результати тестування підтвердили, що впровадження блокчейн дозволяє значно підвищити рівень безпеки та прозорості розподілених систем, водночас знижуючи ризики несанкціонованого доступу до даних і шахрайства.

Наукова новизна дослідження полягає в аналізі можливостей інтеграції блокчейн у нові галузі, які раніше не використовували цю технологію, а також у розробці рекомендацій щодо подолання існуючих проблем масштабованості та енергоспоживання.

Ключові слова: блокчейн, безпека даних, прозорість, консенсус, розподілені системи, децентралізація, алгоритми, смарт-контракти.

ABSTRACT

Kabka V.V. Application of blockchain technologies to improve the security and transparency of distributed systems.

Diploma thesis for the degree of Master of Science in specialty 122 «Computer Science» – University of Customs and Finance, Dnipro, 2025.

The master's thesis is devoted to the study of blockchain technologies in the context of increasing the security and transparency of distributed systems. The paper discusses the basic principles of blockchain functioning, including decentralization, cryptographic security, consensus mechanisms, and data immutability.

The study analyzes existing security mechanisms in distributed systems, including traditional centralized approaches, and proves the advantages of blockchain for preventing attacks, ensuring data integrity and transparency of interaction between participants.

The practical part of the work is devoted to modeling the blockchain architecture for a specific distributed system, as well as its software implementation, taking into account modern security requirements.

The test results confirmed that the introduction of blockchain can significantly increase the level of security and transparency of distributed systems, while reducing the risks of unauthorized access to data and fraud.

The scientific novelty of the study is to analyze the possibilities of integrating blockchain into new industries that have not previously used this technology, as well as to develop recommendations for overcoming existing problems of scalability and energy consumption.

Keywords: blockchain, data security, transparency, consensus, distributed systems, decentralization, algorithms, smart contracts.

ЗМІСТ

ВСТУП

Розвиток інформаційних технологій у сучасному світі призводить до постійного удосконалення інструментів та методів обробки даних, що використовуються в різних галузях економіки, фінансів, державного управління та бізнесу [1]. Одним із найбільш перспективних і революційних досягнень останнього десятиліття є технологія блокчей. Спочатку розроблена для забезпечення безпеки та прозорості у фінансових транзакціях, ця технологія швидко здобула популярність і почала застосовуватися у різноманітних сферах діяльності, де важлива безпека даних, довіра між учасниками системи, а також потреба у запобіганні шахрайству та маніпуляціям з інформацією [2].

Застосування блокчейн-технології в розподілених системах, таких як смарт-контракти, криптовалюти, децентралізовані додатки (DApps), має величезний потенціал для підвищення рівня безпеки та прозорості [3]. Сьогодні, в умовах дедалі більших кіберзагроз і зростаючої потреби в анонімності та довірі, саме блокчейн може стати тією основою, яка дозволить побудувати більш надійні та ефективні системи для обробки та зберігання інформації. Поява нових загроз у кіберпросторі та необхідність удосконалення систем захисту роблять дослідження цієї технології надзвичайно актуальним.

Актуальність теми дослідження полягає в тому, що сьогодні зростає кількість розподілених систем, які використовують централізовані механізми для обробки і зберігання даних, що підвищує ризики зловживань і атак на ці системи. Блокчейн як технологія, яка базується на дистрибуції даних серед численних учасників без необхідності централізованого контролю, може стати важливим елементом для забезпечення захисту від несанкціонованого доступу та змін даних. У цьому контексті особливе значення має дослідження можливостей і механізмів впровадження блокчейн у розподілені системи для забезпечення їхньої безпеки та прозорості.

Метою цієї кваліфікаційної роботи є вивчення та аналіз технологій блокчейн з точки зору їхнього застосування для підвищення безпеки та прозорості в розподілених системах. Для досягнення цієї мети передбачається вирішення таких завдань:

– описати основні принципи та архітектуру технології блокчейн;

– проаналізувати існуючі методи забезпечення безпеки в розподілених системах та визначити, яким чином блокчейн може покращити ці методи;

– вивчити застосування блокчейн у різних галузях (фінансовий сектор, постачання, медицина тощо) для покращення прозорості та безпеки;

– розглянути можливості інтеграції блокчейн-технологій у сучасні розподілені системи та визначити їхні переваги і обмеження;

– визначити перспективи розвитку блокчейн та його вплив на еволюцію розподілених систем;

Об’єктом дослідження є розподілені системи, в яких технології блокчейн можуть бути використані для забезпечення безпеки та прозорості. Це можуть бути як бізнес-платформи для обміну фінансовими активами, так і більш специфічні сфери, такі як медицина, юридична діяльність, інтернет речей тощо. Предметом дослідження є саме технології блокчейн, їх особливості та механізми функціонування, а також застосування цих технологій у контексті розподілених систем для підвищення їхньої безпеки та прозорості.

У ході дослідження використовуватимуться такі методи як аналіз літературних джерел, моделювання та порівняння різних типів блокчейн-систем, а також методи оцінки ефективності впровадження блокчейн у реальні розподілені системи. Особливу увагу буде приділено порівнянню переваг і недоліків різних алгоритмів консенсусу та підходів до забезпечення цілісності даних у системах на базі блокчейн.

Практична значимість дослідження полягає у можливості застосування отриманих результатів для покращення безпеки та прозорості розподілених

інформаційних систем. Результати цієї роботи можуть бути використані розробниками програмного забезпечення для створення більш надійних і безпечних розподілених систем, а також організаціями, що прагнуть знизити ризики, пов’язані з обробкою та зберіганням даних у великих мережах. Крім того, дослідження може стати основою для подальших наукових розробок і впроваджень у сфері блокчейн-технологій.

Наукова новизна роботи полягає в тому, що вона не тільки висвітлює можливості застосування технологій блокчейн для підвищення безпеки та прозорості розподілених систем, а й пропонує нові підходи та методи інтеграції блокчейн у специфічні сфери діяльності, в яких ці технології ще не здобули широкого застосування. Результати роботи також можуть слугувати науковою основою для подальших досліджень у цій галузі, сприяючи розвитку нових моделей і алгоритмів для забезпечення безпеки в інформаційних технологіях.

Структура кваліфікаційної роботи. Кваліфікаційна робота магістра складається з трьох розділів. Обсяг кваліфікаційної роботи – 87 сторінок. Робота містить 14 рисунків, список використаних джерел має 17 посилань.

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ ДОСЛІДЖЕННЯ

1.1 Історія розвитку та еволюція блокчейн

Історія розвитку блокчейн-технології бере свій початок в кінці 20 століття, коли інтерес до криптографії та дистрибутивних обчислень почав зростати серед вчених та інженерів, які прагнули створити надійні методи зберігання та обміну даними без необхідності втручання посередників [1, 2]. Технологія дистрибутивних реєстрів, на основі яких виник блокчейн, була визнана перспективною для забезпечення прозорості і цілісності даних у цифровому середовищі. Основним питанням, яке ставилось перед дослідниками, було, як створити систему, в якій дані не можуть бути змінені або підроблені, і в той же час не потрібен центральний орган для їх контролю.

З’явившись на початку 2000-х років, блокчейн спочатку привернув увагу вчених, які працювали в галузі криптографії та цифрових валют. Першим значним кроком стало розроблення концепції криптовалюти Bitcoin, яку в 2008 році представив анонімний розробник або група розробників під псевдонімом Сатоші Накамото. У своїй публікації «Bitcoin: A Peer-to-Peer Electronic Cash System» Накамото виклав ідею, яка стала основою для створення не тільки самого Bitcoin, але й технології, що дозволяла безпечний, дистрибутивний обмін цінностями без потреби у центральному посереднику. Важливими елементами цієї концепції стали використання криптографії для забезпечення безпеки транзакцій, застосування принципу дистрибутивного реєстру для запису всіх операцій, а також механізм консенсусу, який гарантує, що всі учасники мережі погоджуються з правдивістю та порядком даних.

З моменту запуску Bitcoin в 2009 році блокчейн став справжнім інноваційним проривом, який привернув увагу не тільки технічних експертів, але й бізнесменів, урядів та широкої аудиторії. Механізм блокчейн, що лежав

в основі криптовалюти, дозволяв уникнути таких проблем, як подвійне витрачання коштів або маніпуляція даними, що робило Bitcoin надійним і ефективним засобом обміну [3]. Однак, на початкових етапах розвитку технологія блокчейн була переважно прив’язана до криптовалют, і її можливості здавались обмеженими лише фінансовими операціями.

У наступні роки після запуску Bitcoin, інтерес до блокчейн-технології зростав. Одним із найбільших кроків у розвитку блокчейн стало створення Ethereum у 2015 році, який був запропонований Віталієм Бутеріним як платформа для створення децентралізованих додатків і смарт-контрактів. Ethereum додав до концепції блокчейн можливість виконання програм, що дозволило використовувати блокчейн не лише для зберігання даних про фінансові транзакції, але й для більш складних взаємодій у вигляді автоматизованих контрактів, що виконуються за заданими умовами без необхідності в сторонньому контролі.

Одним з ключових аспектів розвитку блокчейн є пошук нових механізмів консенсусу. У той час як у Bitcoin застосовувався механізм Proof of Work (PoW), який вимагав значних обчислювальних потужностей для підтвердження транзакцій і забезпечення безпеки мережі, Ethereum з часом почав інтегрувати альтернативні підходи, такі як Proof of Stake (PoS), де безпека мережі забезпечується не через обчислювальні потужності, а через володіння криптовалютою. Це стало одним з найважливіших етапів розвитку блокчейн, оскільки спростило процес валідації транзакцій і зробило систему більш енергоефективною.

Інтерес до блокчейн-технології значно зріс після 2017 року, коли на ринку з’явилась хвиля первинних пропозицій монет (ICO), що дозволяли стартапам збирати кошти через продаж токенів, випущених на основі блокчейн. Це сприяло значному зростанню інвестицій у нові блокчейн-проекти та прискоренню їх розвитку. Проте цей період також був ознаменований високим рівнем спекуляцій і ризиків, що призвело до

зловживань і введення регуляцій з боку урядів, які почали вивчати можливості контролю за новими криптовалютними проектами.

З 2018 року блокчейн став активно застосовуватись не лише у фінансових сферах, а й у багатьох інших галузях. Одним із значних досягнень стало застосування блокчейн в ланцюгах постачання, де ця технологія дозволяє здійснювати прозорі та незмінні записи про рух товарів, їх походження та обробку. Блокчейн також знайшов застосування в медицині, де використовуються дистрибутивні реєстри для зберігання медичних даних пацієнтів, що дозволяє забезпечити їх безпеку та конфіденційність. Одним з важливих аспектів стало використання блокчейн для створення систем цифрової ідентифікації, що дозволяє захищати особисті дані в інтернеті.

У цей період на блокчейн почали дивитись не лише як на технологію для криптовалют, але й як на інструмент для забезпечення прозорості, безпеки та ефективності в різноманітних сферах. Одним із таких прикладів є застосування блокчейн у державно-приватних ініціативах, де вона використовувалась для голосування, управління правами власності та навіть у виборчих процесах, що дозволяє зменшити рівень шахрайства та забезпечити більшу прозорість у прийнятті рішень [1, 2].

У 2020-х роках блокчейн-екосистема продовжувала розвиватися, адаптуючи нові механізми консенсусу та інші інноваційні підходи. У цей період активно розвивались рішення на базі «Layer 2», які дозволяють зменшити навантаження на основні блокчейн-мережі, зокрема через використання каналу платежів та інших технологій, що сприяють підвищенню масштабованості та зниженню вартості транзакцій.

Однак, незважаючи на всі ці досягнення, блокчейн все ще стикається з рядом проблем, серед яких можна виділити високі енергетичні витрати при використанні деяких моделей консенсусу, необхідність інтеграції з традиційними фінансовими системами, а також правові та регуляторні виклики. Проте ці проблеми не зупиняють розвиток блокчейн, і

продовжуються пошуки рішень, які дозволяють зробити технологію більш доступною, ефективною та сталим інструментом для різних сфер діяльності.

Загалом історію розвитку можна представити у вигляді наступної схеми (рис. 1.1):

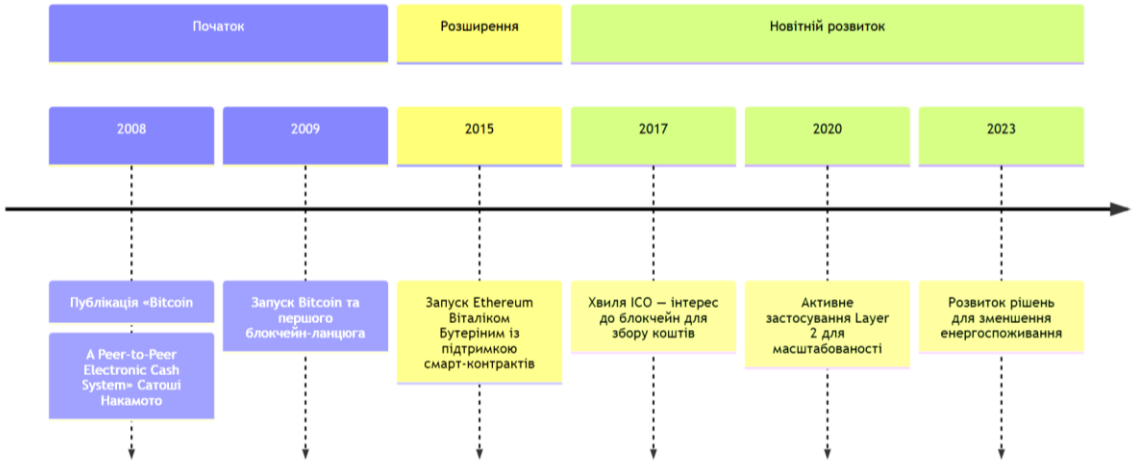

Рисунок 1.1 – Історія розвитку та еволюція блокчейн

Отже, еволюція блокчейн-технології демонструє постійне вдосконалення, що супроводжується все більшим впровадженням цієї технології у різні індустрії та галузі. Від початкових експериментів з криптовалютами до глобальних ініціатив, що змінюють спосіб взаємодії людей та організацій з інформацією, блокчейн залишається однією з найбільш перспективних технологій сучасності, яка продовжує визначати напрямок розвитку цифрових інновацій у майбутньому.

1.2 Основні принципи функціонування технології блокчейн

Технологія блокчейн, з моменту свого виникнення, завоювала значну увагу завдяки своїм основним принципам функціонування, які дозволяють створювати високонадійні, дистрибутивні та незмінні системи для зберігання і передачі інформації. Її функціонування побудовано на ряді принципів, які

забезпечують цілісність, безпеку та прозорість даних у різноманітних сферах, включаючи фінанси, логістику, державне управління та інші галузі [3]. Основними принципами, що лежать в основі технології блокчейн, є дистрибуція, криптографічна захищеність, консенсус, незмінність, прозорість та автономія, які взаємодіють між собою, забезпечуючи ефективне і безпечне функціонування цієї технології.

Одним із основних принципів функціонування блокчейн є дистрибутивність. У традиційних централізованих системах дані зберігаються і обробляються в одному місці, контролюємому єдиним органом або сервером. У випадку блокчейн, дані зберігаються на численних комп'ютерах, або вузлах, розподілених по всьому світу. Кожен з цих вузлів зберігає копії всієї бази даних або частину її, залежно від налаштувань мережі. Такий підхід дозволяє уникнути єдиної точки відмови, що є однією з головних переваг блокчейн перед традиційними централізованими системами. Важливим аспектом є те, що кожен вузол у мережі може виконувати функції перевірки та валідації транзакцій, що забезпечує високий рівень надійності і безпеки в процесі обробки даних. Іншою важливою складовою функціонування блокчейн є криптографія. У блокчейн-системах використовується кілька видів криптографічних методів для забезпечення безпеки транзакцій та захисту даних від несанкціонованого доступу або змін. Одна з основних криптографічних технологій, яка застосовується в блокчейн, – це хешування. Хеш-функції застосовуються для створення унікальних ідентифікаторів для кожного блоку в ланцюзі. Хешування гарантує, що навіть невелика зміна в даних блоку призведе до зміни хешу, що автоматично буде виявлено іншими учасниками мережі. Це забезпечує незмінність даних і запобігає маніпуляціям з ними.

Крім того, для забезпечення конфіденційності та захисту даних блокчейн використовує асиметричне шифрування, яке дозволяє здійснювати безпечні транзакції між учасниками без необхідності знати їхні особисті дані

або використовувати централізовані посередники. У такій системі кожен учасник має пару ключів: публічний ключ, який доступний для всіх і використовується для отримання даних або валідних транзакцій, та приватний ключ, який зберігається в таємниці і використовується для підписання транзакцій [3, 4]. Це дозволяє гарантувати, що тільки власник приватного ключа може ініціювати транзакцію, а інші учасники можуть перевірити її автентичність за допомогою публічного ключа.

Принцип консенсусу є ще одним фундаментальним аспектом роботи блокчейн. В умовах дистрибутивності системи необхідно мати механізм, який дозволяє усім учасникам мережі прийти до єдиного рішення щодо правильності та порядку транзакцій. Це завдання вирішується за допомогою різноманітних механізмів консенсусу, найбільш відомими з яких є Proof of Work (PoW) та Proof of Stake (PoS). У системах, де використовується PoW, учасники мережі, або майнери, вирішують складні математичні задачі для того, щоб підтвердити правдивість транзакцій і додати новий блок до ланцюга. Цей процес вимагає значних обчислювальних ресурсів, але гарантує високий рівень безпеки. Водночас PoS передбачає, що учасники, які володіють певною кількістю токенів або монет в мережі, мають право перевіряти транзакції та додавати нові блоки на основі свого «ставлення» в системі [4, 5]. По суті, той, хто володіє більшим обсягом криптовалюти, має більше шансів бути вибраним для підтвердження транзакцій і отримання винагороди.

Незмінність є ще одним важливим принципом, на якому базується блокчейн. Після того, як блок додано до ланцюга, змінити його або видалити дані стає надзвичайно складно, якщо не неможливо. Це забезпечується через використання криптографії та механізмів консенсусу. Кожен новий блок містить хеш попереднього блоку, що створює ланцюг, в якому дані змінюються лише при одночасному згоді більшості учасників мережі. Таким чином, для того, щоб змінити інформацію в блоках, зловмиснику потрібно буде змінити хеш усіх наступних блоків, що є вкрай важким завданням,

оскільки для цього потрібно буде мати більше обчислювальних потужностей, ніж всі інші учасники мережі.

Прозорість є ще одним важливим принципом блокчейн, який полягає в тому, що всі транзакції, які відбуваються в мережі, доступні для перегляду всім учасникам мережі. Оскільки кожен новий блок є частиною публічного реєстру, всі зміни, що відбуваються в мережі, є відкритими і доступними для перевірки. Це дозволяє забезпечити рівність та прозорість в усіх процесах, які здійснюються в системі, від фінансових транзакцій до перевірки постачання товарів або навіть голосування. Такі характеристики роблять блокчейн надзвичайно корисним інструментом для створення систем довіри без необхідності в централізованих органах контролю [5].

Автономність блокчейн-систем є також однією з її ключових особливостей. Це означає, що блокчейн здатен працювати без постійної участі людини або організації, а всі операції здійснюються на основі чітко визначених правил та алгоритмів, закладених у систему. Всі транзакції в блокчейн обробляються безпосередньо учасниками мережі, і рішення приймаються автоматично через програмний код або смарт-контракти. Смарт-контракти – це програми, які виконуються в блокчейн-мережах і можуть автоматично виконувати угоди або дії при досягненні певних умов. Це дозволяє здійснювати складні бізнес-операції без необхідності втручання посередників. Важливою рисою, яка відрізняє блокчейн від традиційних технологій зберігання даних, є можливість реалізації так званої «глобальної» довіри. Оскільки в блокчейн-системах відсутній єдиний контрольний орган, усі учасники мережі рівні, і довіра до інформації забезпечується через математичні алгоритми та консенсус. Технологія дає змогу перевірити справжність кожної транзакції, а також засвідчити, що дані не були змінені чи підроблені після їх запису в блокчейн [6].

Таким чином, основні принципи функціонування технології блокчейн забезпечують її безпеку, дистрибутивність, прозорість та автономність. Ці

принципи взаємодіють між собою і створюють основу для розвитку надійних та ефективних систем, які здатні змінити різні сфери діяльності – від фінансових технологій до управління даними в медичній сфері та державному секторі. Блокчейн продовжує еволюціонувати, і з кожним роком з'являються нові механізми та покращення, що дозволяють розширювати межі її застосування і створювати нові можливості для користувачів у різних галузях.

1.3 Типи блокчейнів

Типи блокчейнів є важливим аспектом для розуміння можливостей і обмежень цієї технології, оскільки вибір типу блокчейн-мережі залежить від конкретних потреб користувачів, організацій та цілей, які ставляться перед нею. Розрізняють три основні типи блокчейнів [3, 6]: публічний, приватний і консорціумний, кожен з яких має свої особливості функціонування, доступу, безпеки та застосування в різних галузях. Для глибокого розуміння відмінностей між цими типами блокчейнів важливо розглянути їх принципи роботи, механізми доступу та використання консенсусу, а також специфіку застосування в різних сферах.

Типи блокчейнів представлені на рисунку 1.2.

Публічний блокчейн є, мабуть, найвідомішим і найбільш поширеним типом блокчейну, зокрема завдяки своїй ролі в таких криптовалютах, як Bitcoin і Ethereum. Основною характеристикою публічного блокчейну є його відкритість для всіх учасників, що дає можливість будь-якій людині або організації приєднатися до мережі як учасник або валідатор. У публічному блокчейні кожен має рівні права для перегляду, участі в транзакціях і валідації блоків. Це дозволяє забезпечити високу ступінь дистрибуції даних і відсутність централізованого контролю, що є однією з головних переваг цієї технології. Проте через відсутність центрального управління та контролю публічні блокчейни мають свої недоліки, головним з яких є проблема

масштабованості, пов’язана з необхідністю обробки великої кількості транзакцій, а також високими витратами на енергоспоживання в деяких механізмах консенсусу, таких як Proof of Work. У публічному блокчейні всі транзакції є відкритими для перегляду, і будь-який учасник може перевіряти їх легітимність, що забезпечує прозорість, але водночас може призводити до певних проблем конфіденційності, оскільки всі учасники можуть побачити деталі кожної транзакції, хоча й без прив’язки до особистих даних користувачів [7].

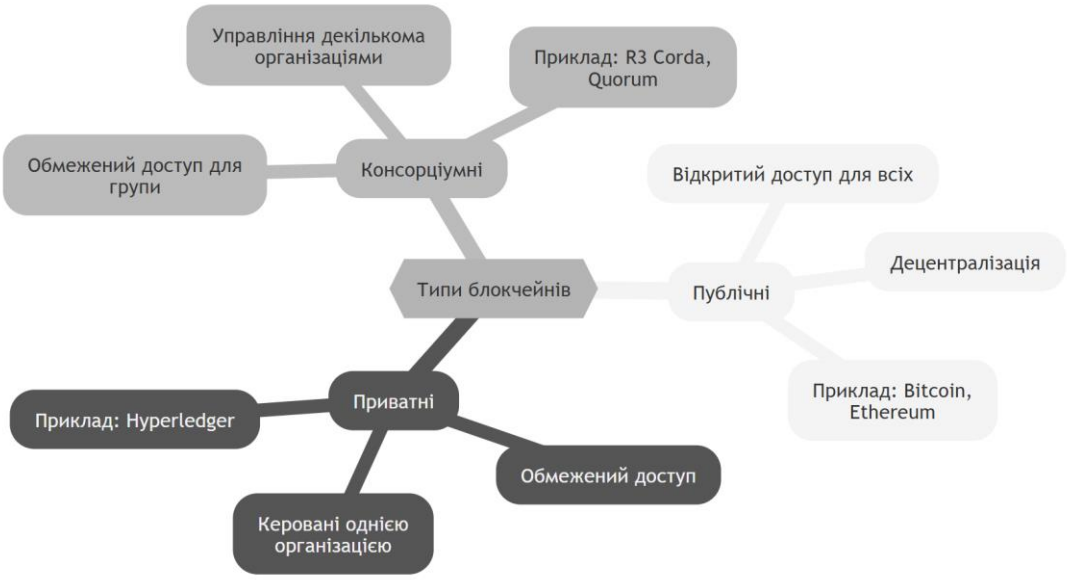

Рисунок 1.2 – Типи блокчейнів

Ще однією важливою особливістю публічних блокчейнів є їх децентралізована природа. Всі учасники мережі рівні, і для прийняття рішень щодо валідності транзакцій і додавання нових блоків використовується механізм консенсусу. У публічному блокчейні може застосовуватися різні типи консенсусу, але найбільш розповсюдженим є Proof of Work (PoW), у якому учасники (майнери) змагаються за право додати новий блок до ланцюга, вирішуючи складні криптографічні задачі. Іншим популярним механізмом є Proof of Stake (PoS), в якому учасники з правом валідації транзакцій

вибираються на основі їхніх активів у мережі [8]. Публічні блокчейни, як правило, є більш відкритими та доступними для використання, однак вони можуть бути менш ефективними у випадках, коли потрібна висока швидкість обробки транзакцій або повна конфіденційність.

Приватні блокчейни є ще одним типом блокчейн-мереж, що кардинально відрізняються від публічних. У приватному блокчейні доступ до мережі обмежений, і лише визначені учасники можуть брати участь у процесі валідації транзакцій і веденні реєстру. Це означає, що приватні блокчейни працюють у закритих або контрольованих середовищах, де доступ до мережі надається лише за запитом або за певними умовами, які визначає централізована структура [8, 9]. Такі мережі застосовуються переважно в корпоративних середовищах, де компанії бажають використовувати переваги блокчейн-технології для забезпечення безпеки та прозорості своїх внутрішніх операцій, зберігання даних або обміну інформацією з іншими учасниками без залучення публічної аудиторії.

Приватні блокчейни мають кілька основних переваг перед публічними, зокрема більший контроль над доступом і підвищену конфіденційність. Оскільки учасники таких мереж є відомими та перевіреними, можна застосовувати менш ресурсомісткі механізми консенсусу, що дозволяє досягати високої швидкості обробки транзакцій. Також приватні блокчейни можуть забезпечувати більшу приватність та конфіденційність даних, оскільки доступ до інформації обмежений і тільки учасники з відповідними правами можуть переглядати або редагувати записані дані [9, 10]. Проте ці переваги приватного блокчейну супроводжуються недоліками, зокрема відсутністю дійсної дистрибуції даних і високим рівнем централізації, що знижує рівень довіри серед учасників і може створювати потенційні ризики зловживань або помилок з боку адміністраторів мережі.

Консорціумний блокчейн, в свою чергу, є гібридним варіантом між публічним і приватним блокчейном. У консорціумному блокчейні доступ до

мережі обмежений, але не тільки однією організацією або окремими учасниками. Замість цього консорціумні блокчейни створюються групами організацій або підприємств, які разом здійснюють управління мережею. Такі блокчейни часто використовуються в тих галузях, де кілька учасників повинні взаємодіяти з одними і тими ж даними, але без розголошення цієї інформації для широкої публіки [10, 11]. Прикладом такого застосування є банківський сектор, де різні банки можуть обмінюватися даними через консорціумний блокчейн, зберігаючи конфіденційність кожної окремої організації, але забезпечуючи прозорість для всіх учасників групи.

Основною перевагою консорціумного блокчейну є можливість дистрибуції довіри серед обмеженої групи учасників, що зменшує ризик маніпуляцій і дозволяє досягати більш високого рівня ефективності в порівнянні з публічними блокчейнами. Оскільки консорціумний блокчейн підтримується кількома учасниками, у ньому можуть застосовуватися менш ресурсоємні механізми консенсусу, ніж у публічних системах, що дозволяє збільшити швидкість транзакцій і зменшити витрати на обробку даних. Проте це також означає, що консорціумний блокчейн може бути менш прозорим і відкритим, ніж публічний, оскільки доступ до мережі має обмежену кількість учасників, і можливість перевірки даних іншими сторонами може бути обмежена.

Загалом, вибір між публічним, приватним і консорціумним блокчейном залежить від специфіки завдання, яке передбачається вирішувати за допомогою цієї технології [10, 12]. Публічні блокчейни ідеальні для ситуацій, де важлива максимальна прозорість, дистрибуція і доступність для широкої аудиторії, в той час як приватні блокчейни більше підходять для корпоративних середовищ, де необхідний високий рівень контролю і конфіденційності. Консорціумний блокчейн є оптимальним варіантом для сценаріїв, де кілька організацій повинні працювати разом, зберігаючи при цьому високий рівень ефективності і довіри між учасниками. Всі ці типи

блокчейнів продовжують еволюціонувати, адаптуючи нові механізми консенсусу та рішення для конкретних потреб ринку, і є невід'ємною частиною майбутнього цифрового середовища.

1.4 Алгоритми консенсусу

Алгоритми консенсусу (рис. 1.3) є фундаментальними елементами будь-якої блокчейн-системи, оскільки вони визначають, яким чином учасники мережі досягають угоди щодо правомірності транзакцій і визначення порядку додавання нових блоків до ланцюга [11, 13]. Вибір алгоритму консенсусу безпосередньо впливає на ефективність, безпеку, дистрибуцію даних і масштабованість блокчейн-мережі, а також на рівень енергетичних витрат і час, необхідний для підтвердження транзакцій. Найбільш популярними алгоритмами консенсусу є Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Byzantine Fault Tolerance (BFT) та кілька інших варіантів, кожен з яких має свої переваги та недоліки, залежно від того, яку задачу вони повинні вирішувати. Оскільки блокчейн є технологією з багатьма застосуваннями в різних сферах, вибір відповідного алгоритму консенсусу є важливою частиною проектування мережі, що використовує цю технологію.

Proof of Work (PoW) є одним з перших і найбільш широко використовуваних алгоритмів консенсусу. Його основна ідея полягає в тому, що для додавання нового блоку до ланцюга учасники мережі повинні вирішити складну математичну задачу. Це завдання передбачає пошук числа, яке відповідає певним криптографічним вимогам (наприклад, певний хеш, що починається з певної кількості нулів). Процес пошуку такого числа потребує великих обчислювальних ресурсів і значної енергії, тому той, хто перший знайде таке число, має право додати новий блок і отримує винагороду у вигляді криптовалюти. Найвідомішим прикладом використання PoW є

блокчейн Bitcoin, де майнери змагаються за право додавати нові блоки, виконуючи обчислювальні задачі.

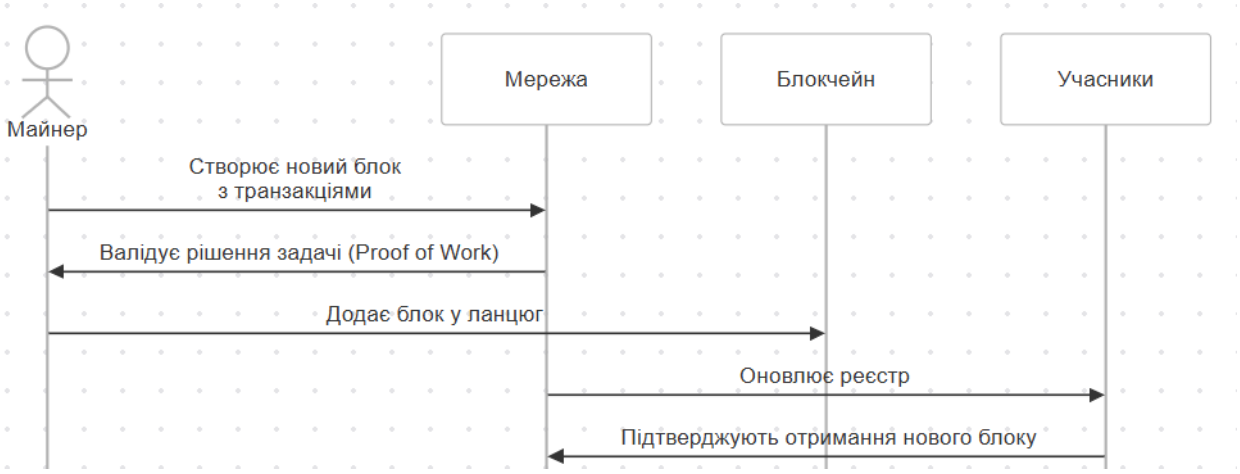

Рисунок 1.3 – Діаграма послідовності для алгоритму консенсусу

Перевагою PoW є його надійність і висока безпека [10, 12]. Оскільки для додавання нового блоку потрібно виконати складну обчислювальну задачу, маніпуляції з даними вимагають великих витрат ресурсів, що робить мережу стійкою до атак. Однак одним з головних недоліків PoW є його енергоємність. Для виконання обчислень майнери повинні використовувати потужне обладнання, що споживає велику кількість електричної енергії, що робить цей алгоритм недостатньо ефективним і стійким до екологічних проблем. Більш того, висока конкуренція за право додавання нових блоків може призводити до високих транзакційних зборів і зниження швидкості обробки транзакцій.

Proof of Stake (PoS) є альтернативним підходом, який пропонує значно зменшити енергетичні витрати, зберігаючи при цьому безпеку мережі. У PoS валідатори (учасники, які відповідають за додавання нових блоків) не повинні виконувати складні обчислювальні задачі. Замість цього вони обираються для підтвердження транзакцій і додавання блоків на основі кількості криптовалюти, яку вони «заморожують» або ставлять у якості застави. Це дозволяє зменшити навантаження на обчислювальні потужності, що, в свою

чергу, знижує енергетичні витрати. У PoS більшість учасників мережі вибираються пропорційно до кількості монет або токенів, якими вони володіють, що зменшує ризик централізації мережі в порівнянні з PoW.

Однією з головних переваг PoS є значно менші енергетичні витрати і більша ефективність у порівнянні з PoW. Водночас PoS вирішує проблему концентрації обчислювальних потужностей у великих центрах обробки даних, що є характерною для PoW. Однак, система PoS також має свої недоліки, серед яких – ризик концентрації монет в руках великої кількості учасників, що може призвести до деякої централізації. Крім того, якщо учасники мережі не мають достатньо монет для участі у валідації, це може привести до зменшення кількості активних учасників, що потенційно знижує безпеку мережі.

Delegated Proof of Stake (DPoS) є варіантом PoS, який дозволяє забезпечити ще більшу ефективність і швидкість транзакцій. У DPoS валідатори не вибираються безпосередньо на основі кількості криптовалюти, якою володіють учасники мережі, а шляхом виборів серед делегатів. Кожен учасник мережі може проголосувати за делегатів, які представлятимуть інтереси всіх учасників при валідації транзакцій і додаванні блоків до ланцюга. Це дозволяє значно знизити кількість необхідних учасників для забезпечення консенсусу і прискорити процес валідації транзакцій, оскільки менша кількість делегатів може швидше дійти до консенсусу.

Основною перевагою DPoS є висока швидкість транзакцій і здатність до масштабування. Оскільки тільки обмежена кількість делегатів бере участь у процесі валідації, процес прийняття рішень значно прискорюється [9, 10]. Проте це також створює ризик централізації, оскільки процес вибору делегатів може бути впливовим і залежать від їхнього фінансового або політичного впливу. З часом це може привести до ситуації, коли великі учасники ринку, що володіють більшою кількістю токенів, отримають надмірну владу в системі.

Byzantine Fault Tolerance (BFT) – це ще один важливий алгоритм консенсусу, що застосовується в деяких блокчейн-мережах, особливо в тих,

які орієнтовані на високу швидкість і надійність. BFT гарантує, що навіть у випадку зловмисників або некоректних учасників мережі консенсус буде досягнутий і система не дозволить маніпуляцій з даними. Ідея BFT полягає в тому, щоб дозволити мережі працювати коректно, навіть якщо деяка частина учасників або вузлів мережі є нечесними або несправними. Одним із найбільш відомих алгоритмів, що використовують принципи BFT, є алгоритм Practical Byzantine Fault Tolerance (PBFT), який активно застосовується у корпоративних та приватних блокчейнах.

Основною перевагою BFT є його висока стійкість до атак і несправних учасників. Це робить його дуже привабливим для застосувань, де важливо забезпечити високий рівень безпеки і довіри, зокрема в фінансових і корпоративних системах. Однак BFT також має свої обмеження, зокрема щодо масштабованості [11, 12]. Для досягнення консенсусу всі учасники повинні активно взаємодіяти між собою, що призводить до значних витрат часу і ресурсів на обробку транзакцій при великій кількості учасників. Тому BFT більше підходить для мереж з обмеженим числом учасників, таких як консорціумні блокчейни.

Загалом, вибір алгоритму консенсусу для блокчейн-системи залежить від конкретних потреб і вимог, що пред’являються до мережі. PoW залишається популярним завдяки своїй високій безпеці і підтвердженій ефективності в розподілених системах, хоча його енергоємність обмежує його застосування. PoS і DPoS є перспективними альтернативами, оскільки вони забезпечують більшу енергоефективність і високу швидкість транзакцій, проте можуть спричиняти деякі ризики, пов’язані з концентрацією контролю. BFT, у свою чергу, є важливим інструментом для приватних і консорціумних блокчейн-мереж, що потребують високого рівня надійності і стійкості до зловмисних дій, але його обмеження в масштабованості роблять його менш підходящим для великих публічних систем. Кожен алгоритм має свої сильні і

слабкі сторони, і вибір між ними залежить від того, які завдання і цілі ставляться перед конкретною блокчейн-системою.

1.5 Аналіз сучасних досліджень

Стаття [1] досліджує потенціал технології блокчейн для підвищення безпеки смарт-систем. Блокчейн є дистрибутивною технологією реєстру, яка забезпечує безпечну, незмінну та прозору платформу для зберігання даних і транзакцій. Спочатку в статті розглядаються основи блокчейн-технології та її переваги з точки зору безпеки. Далі аналізуються визначення смарт-систем та їхні специфічні вимоги до безпеки. Потім досліджується, як блокчейн може задовольнити ці вимоги, розглядаються переваги та недоліки застосування блокчейн для забезпечення безпеки смарт-систем, а також існуючі технології блокчейн та їхні функції безпеки. Стаття також аналізує потенціал цих технологій для покращення безпеки смарт-систем та обговорює їхнє майбутнє. Наприкінці подаються висновки та обговорюються наслідки отриманих результатів.

Стаття [2] спеціалізується на впровадженні технології блокчейн у управління ланцюгами постачання в Алжирі з метою покращення прозорості та безпеки операцій. Вона підкреслює важливість ланцюгів постачання для місцевих бізнесів та глобальної економіки, знайомить з децентралізованою архітектурою та безпечними можливостями технології блокчейн як розподіленого реєстру. Стаття досліджує, як впровадження блокчейн може поліпшити управління ланцюгами постачання в Алжирі, підвищуючи прозорість та безпеку операцій. Спочатку розглядається важливість блокчейн як ключового бізнес-пріоритету та його потенціал для трансформації майбутнього бізнесу через реформи та реконструкцію. Далі надається детальний огляд переваг і обмежень цієї технології, а також аналізуються існуючі рішення для подолання її недоліків. Наприкінці статті представлений

приклад використання блокчейн у фармацевтичному секторі Алжиру, щоб підтвердити ефективність цієї технології в реальних умовах.

Стаття [3] досліджує проблему відсутності системи, яка забезпечує прозорість та безпеку при розподілі спадщини серед спадкоємців, що часто призводить до непорозумінь та руйнування сімейних відносин. Вона розглядає спадщину як сукупність прав, обов'язків і активів, які передаються спадкоємцям після смерті особи, включаючи активи, цінні папери та інші елементи. Проблема полягає в тому, що поточні процеси розподілу спадщини не забезпечують належного рівня прозорості, що ускладнює процес і збільшує ризик конфліктів серед спадкоємців. Метою цього дослідження є підвищення прозорості та безпеки транзакцій з розподілу спадщини за допомогою технології блокчейн. Блокчейн має концепцію перевірки транзакцій через принцип peer-to-peer, що може бути застосовано до процесу розподілу спадщини. Ця технологія гарантує прозорість транзакцій для всіх учасників процесу, а також забезпечує захист даних завдяки вбудованим функціям шифрування. Методологія дослідження базується на якісному підході, що включає вивчення механізмів розподілу спадщини та можливостей технології блокчейн. Результатом дослідження є модель впровадження блокчейн для підвищення прозорості процесу розподілу спадщини та демонстрація даних за допомогою симуляції на платформі Ganache.

Стаття [4] досліджує нову стратегію покращення безпеки та довіри шляхом поєднання технології блокчейн і методів машинного навчання. Така синергія використовує децентралізовані та незмінні властивості блокчейну разом із аналітичними можливостями, що надаються моделями машинного навчання, для досягнення оптимального створення цінності. Детальний аналіз показує ефективність цієї техніки в посиленні заходів безпеки та сприянні прозорості в різних операціях. Стаття демонструє, як інтегрований підхід може вирішити проблеми безпеки сучасних даних, створюючи надійні, довірливі та сильні системи. Завдяки цьому стає можливим розширення

застосування цих безпечних і прозорих технологій, що відкриває нові перспективи для їх використання в інших галузях науки.

Стаття [5] пропонує рішення для редагованого блокчейну на основі мета-транзакцій з використанням zk-SNARK, що сприяє підвищенню анонімності в децентралізованому середовищі. Блокчейн, як незмінний і розподілений реєстр, забезпечує прозорість і безпеку даних, але через питання конфіденційності та безпеки виникає потреба в можливості редагування реєстру. Автори пропонують схему генерації одноразових криптографічних ключів для підписів, що створює різні ключі для кожної транзакції, що допомагає підвищити безпеку та конфіденційність, запобігаючи відстеженню особистості. Для приховування інформації про криптографічні ключі та підписи використовується zk-SNARK, що дозволяє значно зменшити час перевірки транзакцій, навіть якщо вони мають кілька модифікацій, до приблизно 10 мс. Крім того, вводиться схема збору плати за редагування для власників транзакцій, щоб стимулювати видалення замість модифікацій, що дозволяє мінімізувати накладні витрати на виконання редагувань і підтримує компактну історію змін.

Стаття [6] досліджує застосування технології блокчейн для поліпшення механізму аутентифікації в мережах 5G. Хоча технологія 5G дозволяє передавати дані на швидкості до 10 Гбіт/с за допомогою міліметрових хвиль, її обмежене покриття – всього близько 1000 футів – вимагає встановлення численних вишок та антен для забезпечення надійного сигналу і зв’язку. Це, у свою чергу, призводить до частих аутентифікацій, коли користувацьке обладнання (UE) переміщується між клітинками, що створює необхідність у швидкому та ефективному механізмі аутентифікації. Хоча існуючі протоколи аутентифікації 4G можна адаптувати для 5G, вони не здатні ефективно обробляти часті аутентифікації, незважаючи на їх здатність забезпечувати базову безпеку. Тому в статті пропонується використання технології блокчейн, яка має властивості безпеки, анонімності, незмінності та прозорості,

як перспективне рішення для уникнення надмірних аутентифікацій. Запропонована методологія передбачає два етапи: перший – введення нового оптимізованого консенсус-алгоритму, спеціально розробленого для покращення швидкості аутентифікації, другий – зменшення кількості аутентифікацій завдяки використанню результатів аутентифікації, збережених у блокчейні UE-AP, що дозволяє ефективно обробляти надлишкові аутентифікації.

Стаття [7] пропонує нову систему інтеграції всеприсутньої енергетичної Інтернету речей (IoT) на основі технології блокчейн, спрямовану на посилення глибокої інтеграції цих двох технологій. Система дозволяє повною мірою використовувати характеристики блокчейн-технології, такі як прозорість, відкритість та спільний доступ, а також її функції, зокрема смарт-контракти, відстежуваність інформації та децентралізацію. Дослідження показує, що така інтеграція покращує прозорість і спільний доступ до даних в рамках всеприсутнього енергетичного Інтернету речей, що сприяє більш ефективному використанню інформації та технологій в цій сфері.

Стаття [8] обговорює використання технології Інтернету речей (IoT) в охороні здоров’я, що відкриває можливості для значних досягнень у лікуванні та моніторингу пацієнтів, але також викликає серйозні питання щодо безпеки, зокрема захисту конфіденційної медичної інформації та забезпечення надійності мережевого обладнання. Автори пропонують використання блокчейн-технології Multichain як ефективного засобу для підвищення безпеки в контексті IoT в охороні здоров’я, щоб вирішити ці проблеми. Блокчейн Multichain пропонує розподілений, незмінний та стійкий до підробок метод зберігання даних, що гарантує конфіденційність, точність і доступність інформації про пацієнтів, знижуючи ризики, пов’язані з централізованими сховищами даних. Використання архітектури Multichain у системах IoT в охороні здоров’я дозволяє створювати довіру серед різних учасників, зменшує ризик несанкціонованого доступу та покращує безпеку обміну даними між

різними пристроями та платформами. Стаття надає загальний огляд запропонованої методології та її можливих наслідків для посилення безпеки в охороні здоров’я завдяки Інтернету речей.

Стаття [9] обговорює проблеми традиційної системи торгівлі електроенергією, яка базується на централізованій архітектурі і стикається з такими проблемами, як велика кількість учасників, недостатній рівень безпеки даних і ізольованість даних, що обмежує готовність учасників до участі в ринку. Технологія блокчейн, завдяки своїм характеристикам, таким як відкритість, прозорість, відстежуваність, незмінність та слабка централізація, здатна частково вирішити ці проблеми. Стаття пропонує архітектурне рішення для системи торгівлі електроенергією на основі блокчейн-технології, аналізує методи підключення блоків і пропонує новий підхід, відмінний від традиційного, до розподіленого зберігання, гібридного розгортання та гнучкого доступу. Цей підхід дозволяє вирішити проблеми ізоляції даних та недостатньої безпеки у сценаріях торгівлі електроенергією, покращуючи гнучкість доступу до даних.

Стаття [10] обговорює перспективи хмарних ERP-систем, які є ідеалом для бізнесу завдяки можливості співпраці з партнерами, зовнішніми додатками та інформаційними системами. Однак, хмарні ERP-рішення стикаються з проблемами безпеки даних, прозорості та довіри, що вимагає радикальних змін у їх інфраструктурі та функціональності. Метою цього дослідження є поєднання переваг хмарних ERP-систем та технології блокчейн для покращення безпеки даних, відстежуваності транзакцій, прозорості, володіння даними, шифрування та довіри за допомогою запропонованої структури. Для цього спочатку проводиться всебічний аналіз основних проблем сучасних ERP-систем через порівняння хмарних ERP до та після впровадження блокчейн-технології. Далі пропонується загальна структура для хмарних ERP-систем на основі блокчейн, що використовує методи розподіленого реєстру. Наприкінці проводиться оцінка здійсненності та

ефективності цієї структури через вивчення модуля управління ланцюгами постачання.

Стаття [11] розглядає проблему існуючої централізованої моделі торгівлі енергією, яка вже не здатна ефективно взаємодіяти з великою кількістю дистрибутивних енергетичних одиниць в умовах відсутності довіри. Зважаючи на переваги низького енергоспоживання та високої ефективності графенового блокчейну, розроблено архітектуру та процес торгівлі дистрибутивною енергією на основі цієї технології. Торгова система складається з п’яти рівнів: рівня користувача, рівня додатків, рівня контрактів, мережевого рівня та рівня даних, з чіткою загальною архітектурою, самодисциплінованими вузлами та сильною масштабованістю й оптимізацією. Весь процес торгівлі автоматично завершується вчасно через смарт-контракти, що суттєво покращує автоматизацію та інтелектуальність процесу за умови забезпечення прав обох сторін угоди. Порівняльний аналіз різних моделей торгівлі дистрибутивною енергією показує, що модель на основі графенового блокчейну має високу доцільність, новизну та стійкість.

Стаття [12] обговорює застосування технології блокчейн, яка є однією з найвизначніших технологій сучасності завдяки поєднанню криптографії, розподілених обчислень, алгоритмів консенсусу та мережевого зв’язку «peer-to-peer», що забезпечують високий рівень безпеки. Блокчейн відкриває нові можливості для покращення роботи в таких сферах, як ланцюг постачання, фінанси, розумні міста, охорона здоров’я, освіта, електронна комерція та інші. У сфері освіти блокчейн має такий же потенціал застосування, як і в інших сферах, а електронна комерція не є винятком. Тому розроблено модель управління студентами, що інтегрує електронну комерцію на основі блокчейн-технології (SMM-EB). Ця модель підтримується токенами та використовує блокчейн для зберігання інформації про студентів і розподілу нагород у криптовалюті. Студенти можуть використовувати цю валюту для обміну та транзакцій на платформі навчального закладу або в межах електронної

комерції. Завдяки такій системі перевірка особистої інформації студентів і їх досягнень стає швидкою і точною, а також усувається проблема шахрайства в електронній комерції. Завдяки блокчейн-технології ця система гарантує прозорість і цілісність інформації про студентів і транзакцій на платформі, що робить її більш безпечною і ефективною, ніж централізовані системи, які залежать від управління третіми сторонами. Запропонована архітектура може бути повторно використана з перевагами сучасних технологій.

Стаття [13] обговорює необхідність наявності прозорної виборчої системи в демократії, яка відповідає потребам людей і забезпечує передачу влади правильним особам. Водночас традиційні виборчі системи мають значні недоліки, зокрема відсутність належної безпеки та прозорості. У цьому контексті стаття розглядає можливості застосування блокчейн-технології для покращення процесу електронного голосування, зокрема для вирішення проблем довіри, конфіденційності та безпеки. Метою статті є оцінка різних застосувань блокчейн-технологій для реалізації розподілених систем електронного голосування. Деякі з таких застосувань існують лише на стадії проектів, інші вже впроваджені в реальному світі. Застосування блокчейн у системах електронного голосування покращує безпеку, конфіденційність та зменшує витрати, що робить ці системи більш ефективними.

Стаття [14] пропонує рішення для зменшення проблеми накопичення продовольчих запасів, що стало значною загрозою для глобальної продовольчої безпеки в останні роки. Для цього розроблено систему відстеження на основі блокчейн-технології, яка використовує незмінність, прозорість та децентралізований консенсус для створення надійної та аудиторної системи відстеження продовольчого ланцюга постачання. Запропонована система реєструє всі транзакції протягом всього ланцюга постачання – від виробництва до роздрібної торгівлі – на блокчейні. Вона використовує смарт-контракти для автоматизації та забезпечення стандартів обробки, транспортування і постачання продуктів харчування. Крім того,

система має розподілену мережу вузлів, які перевіряють і верифікують дані на блокчейні для забезпечення їх точності та достовірності. Безпека системи покращується завдяки її розподіленій архітектурі, що робить її більш стійкою до шахрайства та підробок. Виробники, постачальники, оптовики та регулятори можуть використовувати блокчейн для отримання реального часу даних про рух продовольчих товарів, що дозволяє швидко реагувати на будь-які ознаки накопичення запасів. Дослідження підкреслює ефективність такої системи у зменшенні практик накопичення запасів і забезпеченні більш рівномірного розподілу продовольчих товарів, що сприяє підвищенню рівня продовольчої безпеки. Стаття завершується пропозицією креативного рішення для покращення продовольчої безпеки для всіх, з підвищенням прозорості, ефективності та підзвітності ланцюга постачання.

Стаття [15] розглядає важливість фармацевтичних продуктів для охорони здоров’я, зокрема їх роль у забезпеченні безпеки та якості догляду за пацієнтами, акцентуючи увагу на відстеженні походження ліків та термінів їх придатності. Проте обмеження в складному та непрозорому ланцюгу постачання фармацевтичних продуктів дозволяють циркулювати підробленим або простроченим лікам, що може призвести до серйозних проблем зі здоров’ям або навіть до смертельних випадків. Для вирішення цієї проблеми стаття пропонує використання блокчейн-технології, яка здатна виявляти шахрайство та помилки, щоб покращити безпеку і прозорість фармацевтичного ланцюга постачання. Блокчейн також змінює управління ланцюгом постачання в фармацевтиці, поєднуючи безпеку і прозорість, створюючи децентралізовану мережу між виробниками, дистриб’юторами, фармацевтами, лікарями і пацієнтами, що гарантує безпеку даних пацієнтів і сприяє співпраці між усіма сторонами. Автор провів дослідження, оглянувши існуючу літературу та спостереження, і запропонував модель інтеграції блокчейн, яка дозволяє зацікавленим сторонам безпечно відстежувати інформацію про фармацевтичні продукти.

Стаття [16] розглядає проблеми традиційних систем управління земельними ресурсами, таких як неефективність, відсутність прозорості та схильність до шахрайства. Хоча цифровізація земельних записів покращила ефективність, вона не вирішила проблеми маніпуляцій, централізованих баз даних і подвійних витрат. Традиційні системи управління лізингом та іпотекою страждають від складності, помилок і відсутності перевірки в реальному часі. Враховуючи великий обсяг даних, що генеруються при кожній операції з землею, таких як передача прав власності, перевірка документів та операції з лізингом або іпотекою, ця стаття пропонує використання блокчейн-технології для вирішення проблем змін і подвійних витрат у традиційних системах, а також для впровадження розподіленого управління даними. Існуючі рішення не повною мірою використовують такі важливі особливості блокчейну, як прозорість, запобігання подвійним витратам, аудит, незмінність і участь користувачів. Це дослідження пропонує всебічну блокчейн-структуру для управління лізингом та іпотекою, яка враховує прозорість, участь користувачів і запобігання подвійним витратам. На відміну від існуючих рішень, наша структура інтегрує ключові характеристики блокчейну для комплексного підходу, встановлюючи безпечний, розподілений і прозорий метод фінансування нерухомості через практичні кейси з власниками землі, банками та фінансовими установами. Система перевіряється за допомогою смарт-контрактів, оцінюється за параметрами вартості та безпеки при перевірці функцій іпотеки та лізингу на основі блокчейну.

Стаття [17] розглядає проблеми, пов’язані з обміну даними в розумних транспортних системах, зокрема питання конфіденційності, безпеки (такі як витоки даних) та ефективності завантаження. Ці труднощі знижують зацікавленість постачальників даних у участі. Для вирішення зазначених проблем дослідження пропонує нову архітектуру, яка базується на асинхронному федеративному навчанні, зосереджену на вирішенні проблем пропускної здатності, безпеки та конфіденційності при обміні даними

транспортних засобів в інтернеті речей (IoT). Основна мета – підвищити надійність та ефективність обміну даними. Для цього використовуються технології блокчейн для покращення безпеки та надійності параметрів моделей, зменшення навантаження на передачу даних і зниження побоювань щодо конфіденційності. Крім того, дослідження застосовує розподілену, ефективну та безпечну архітектуру обміну даними на основі блокчейн, яка дозволяє вибирати вузли, а також оптимізує асинхронну федеративну схему навчання для покращення загальної ефективності. Експериментальні результати показали, що запропонована схема не лише покращує точність навчання, але й значно прискорює швидкість сходження, одночасно підвищуючи захист конфіденційності та якість обслуговування, повністю підтверджуючи ефективність і практичність цього підходу.

1.6 Висновки до першого розділу

Отже, технологія блокчейн пройшла значний шлях від свого виникнення і до сучасного етапу розвитку. Спочатку блокчейн використовувався в контексті криптовалют, таких як Bitcoin, але з часом знайшов застосування в різних сферах – від фінансів до логістики, охорони здоров’я та державних послуг. Еволюція технології включає в себе вдосконалення механізмів консенсусу, забезпечення більшої безпеки, зменшення витрат на енергію та збільшення швидкості транзакцій. Таким чином, блокчейн розвивається не лише в технічному сенсі, а й у контексті його застосування в різноманітних галузях.

Технологія блокчейн є дистрибутивною та децентралізованою, що дозволяє зберігати та передавати дані без посередників. Завдяки цьому досягається висока прозорість і безпека обробки інформації. Принципи функціонування блокчейн включають використання криптографії для захисту даних, механізмів консенсусу для узгодження дій учасників мережі та

постійну доступність для всіх учасників. Висновок полягає в тому, що блокчейн є ефективним інструментом для забезпечення безпечних, прозорих і дистрибутивних процесів обміну інформацією.

Існують різні типи блокчейнів, кожен з яких має свої переваги та обмеження в залежності від потреб користувачів і специфіки застосувань. Публічні блокчейни забезпечують максимальну прозорість та доступність, але можуть страждати від проблем масштабованості і високих витрат на енергію. Приватні блокчейни пропонують більший контроль і конфіденційність, що підходить для корпоративних застосувань, але втрачають деяку перевагу в плані дистрибуції. Консорціумні блокчейни дозволяють кільком організаціям співпрацювати в межах закритої мережі, зберігаючи при цьому ефективність і безпеку, але також мають обмежену прозорість для зовнішніх учасників. Висновок з цього підрозділу – вибір типу блокчейну залежить від конкретних завдань та умов використання, що потребує чіткого визначення вимог перед розгортанням технології.

Алгоритми консенсусу є основними для забезпечення цілісності і безпеки блокчейн-мереж. PoW забезпечує високу безпеку, але вимагає значних енергетичних витрат. PoS та DPoS є енергоефективними альтернативами, зберігаючи при цьому безпеку, проте можуть бути вразливими до централізації. BFT підходить для мереж з обмеженим числом учасників і високоорганізованих середовищ, де важливо забезпечити стійкість до зловмисних дій. Порівняння цих алгоритмів показує, що вибір консенсусу залежить від масштабу і специфіки застосування блокчейн-мережі, а також від потреб у безпеці, швидкості транзакцій і енергетичних витратах.

РОЗДІЛ 2. ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ ТА ПРОЗОРОСТІ РОЗПОДІЛЕНИХ СИСТЕМ

2.1 Механізми забезпечення цілісності даних у блокчейні

Механізми забезпечення цілісності даних у блокчейні є одними з основних аспектів, які забезпечують функціонування цієї технології, зокрема її безпеку, прозорість та довіру серед учасників мережі. Цілісність даних у блокчейні означає, що всі транзакції, збережені в блоках, повинні бути достовірними, незмінними, а також зберігати свою послідовність і відповідність [12, 13]. Оскільки блокчейн функціонує у дистрибутивному середовищі, де всі учасники мають доступ до одних і тих самих даних, забезпечення їх цілісності є одним з головних викликів, який потребує спеціальних технічних підходів і механізмів. Для досягнення цієї мети використовуються різноманітні інструменти, серед яких криптографічні методи, механізми консенсусу, алгоритми перевірки, а також принципи дистрибуції даних та їх реплікації.

Одним із найважливіших аспектів забезпечення цілісності даних є використання криптографії. Блокчейн базується на принципах криптографічного захисту, який дозволяє забезпечити надійність та неможливість зміни вже записаних даних. Кожен блок в блокчейні містить хеш попереднього блоку, що утворює ланцюг з усіх блоків, з’єднаних між собою. Хешування є одностороннім процесом, що означає, що за допомогою хеш-функції можна отримати унікальний цифровий відбиток інформації, але неможливо відновити оригінальну інформацію з отриманого хешу. Якщо в будь-якому з блоків змінюється хоча б один біт даних, то хеш цього блоку змінюється, а отже, змінюються й усі наступні блоки, що робить підробку інформації надзвичайно складною. Така властивість хешування є основою механізму забезпечення цілісності даних у блокчейні, оскільки будь-яка

спроба змінити дані безпосередньо впливає на весь ланцюг блоків і стає відразу помітною для всіх учасників мережі.

Крім хешування, важливим елементом забезпечення цілісності даних є використання цифрових підписів [13, 14]. Кожен учасник блокчейн-мережі має власний публічний і приватний ключі. Приватний ключ використовується для підпису транзакцій, що дає змогу підтвердити їх автентичність і забезпечити цілісність даних. Публічний ключ використовується для перевірки підпису, що гарантує, що транзакція була підписана саме тим учасником мережі, якому належить відповідний приватний ключ. Це створює додатковий рівень безпеки, оскільки змінити підписану транзакцію неможливо без зміни самого вмісту транзакції, що автоматично порушить її цілісність.

Одним із ключових принципів, який також забезпечує цілісність даних у блокчейні, є механізм консенсусу. Механізм консенсусу дозволяє учасникам мережі погоджуватися з тим, які транзакції є правомірними і мають бути занесені до блокчейн-ланцюга. Найпоширенішими алгоритмами консенсусу є Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Byzantine Fault Tolerance (BFT) та інші. Кожен з цих алгоритмів має свої переваги та недоліки, але їхня спільна мета – забезпечити узгодження дій між усіма учасниками мережі. У процесі досягнення консенсусу підтверджуються транзакції, і тільки після цього вони записуються в блоки. Це гарантує, що тільки правомірні і погоджені всіма учасниками транзакції можуть бути збережені в блокчейні, що підтримує цілісність даних.

Особливе значення має також дистрибуція і реплікація даних у блокчейн-мережі. Оскільки блокчейн є дистрибутивною технологією, дані в ньому зберігаються на численних вузлах мережі, що робить неможливою централізовану зміну або втрату даних. Кожен вузол містить копію всього ланцюга блоків, і в разі, якщо один з вузлів спробує змінити інформацію, це стане відразу помітно для інших учасників. Реплікація даних на всіх вузлах

дозволяє створити резервні копії інформації і захищає систему від втрати даних через апаратні збої або зловмисні атаки.

Смарт-контракт – це програма, що автоматично виконується при виконанні певних умов, зазначених у договорі. Вони можуть використовуватися для автоматизації різних операцій і забезпечення виконання угод без необхідності втручання третіх сторін. Смарт-контракти не лише автоматизують процеси, але й допомагають підтримувати цілісність даних, оскільки вся інформація про умови та виконання контракту записується в блокчейні і є доступною для всіх учасників мережі [12, 14]. Цей механізм дає можливість досягти повної прозорості та контролю за виконанням угод, забезпечуючи при цьому високий рівень довіри до даних. Забезпечення цілісності даних у блокчейні не обходиться без певних викликів, зокрема стосовно масштабованості та енергетичних витрат. Наприклад, у разі використання алгоритму Proof of Work (PoW) для досягнення консенсусу потрібен значний обсяг обчислювальних потужностей, що призводить до високих енергетичних витрат. Це може стати обмеженням для масштабування блокчейн-мереж, оскільки зростаюча кількість учасників і транзакцій вимагатиме ще більших потужностей для обробки даних. Однак для зменшення цих витрат розробляються нові алгоритми консенсусу, такі як Proof of Stake (PoS), які здатні забезпечити високу ефективність без необхідності витрачати значні енергетичні ресурси.

Крім того, для забезпечення цілісності даних в блокчейні важливо розглядати також питання зловмисних атак, таких як атаки 51%, де учасники з великою кількістю ресурсів можуть спробувати переписати історію транзакцій. Однак використання дистрибуції даних, криптографічних методів і механізмів консенсусу значно знижує ризики таких атак, роблячи блокчейн високозахищеною технологією.

Загалом, механізми забезпечення цілісності даних у блокчейні є комплексними і багатогранними. Вони базуються на різних технологічних

підходах і методах, які працюють разом, щоб забезпечити максимальний рівень безпеки, надійності та прозорості для всіх учасників мережі. Враховуючи постійний розвиток технології та вдосконалення алгоритмів, можна очікувати, що блокчейн стане ще більш ефективним інструментом для забезпечення цілісності даних у майбутньому.

2.2 Захист від атак у розподілених системах: переваги блокчейн-технології

Розподілені системи, як правило, використовуються для створення мереж, де кілька учасників можуть взаємодіяти та обмінюватися даними без необхідності звертатися до єдиного центрального сервера чи органу управління. Такі системи пропонують значну гнучкість і масштабованість, однак вони також стикаються з низкою загроз і проблем, що стосуються безпеки [13-15]. У той час як традиційні централізовані системи можуть покладатися на єдиний захищений центр для контролю доступу та перевірки транзакцій, розподілені системи потребують більш складних методів захисту, оскільки немає єдиного органу, що контролює всі аспекти мережі. Однією з найбільш інноваційних та ефективних технологій, що пропонує потужні інструменти для захисту від атак у розподілених системах, є блокчейн.

Блокчейн-технологія спочатку була розроблена для підтримки криптовалют, таких як Bitcoin, однак її можливості значно перевищують потреби лише у фінансових операціях. Сьогодні блокчейн розглядається як універсальний механізм для забезпечення безпеки в різних розподілених системах, завдяки своїм властивостям, таким як дистрибуція даних, криптографія, механізми консенсусу та прозорість. Блокчейн може бути використаний для забезпечення захисту від різноманітних типів атак, включаючи зловмисні втручання, саботаж, відмову в обслуговуванні та багато інших. Завдяки своїй дистрибутивній природі, блокчейн надає набагато

більшу стійкість до різних типів атак порівняно з централізованими системами. Ключова перевага цієї технології полягає в тому, що дані зберігаються в кількох копіях на численних учасниках мережі, що робить атаки на єдину точку доступу або сервер надзвичайно складними [11, 12].

Однією з основних характеристик блокчейн-технології є її здатність до забезпечення неможливості зміни або підробки даних. Це досягається через використання криптографічних хеш-функцій, які створюють унікальні цифрові відбитки кожного блоку інформації. Хешування є одностороннім процесом, що означає, що неможливо відновити оригінальні дані за їх хешем. Кожен блок містить хеш попереднього блоку, що утворює ланцюг, в якому кожен новий блок залежить від попереднього. Якщо дані в будь-якому з блоків змінюються, змінюється й хеш, що призводить до порушення цілісності ланцюга. Це робить підробку або зміну інформації в блокчейні фактично неможливою без того, щоб не бути поміченою всіма учасниками мережі. Таким чином, блокчейн забезпечує захист від атак, пов’язаних із змінюванням або маніпулюванням даними, таких як атаки на цілісність інформації.

Крім того, блокчейн використовує механізм консенсусу для узгодження дій усіх учасників мережі. Механізми консенсусу, такі як Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS) та інші, дозволяють забезпечити досягнення загальної згоди про те, які транзакції є правильними та мають бути занесені в блокчейн. Це означає, що навіть у разі спроби зловмисного втручання, мережа в цілому може виявити і відхилити несанкціоновані зміни. Якщо один з учасників намагається змінити інформацію, наприклад, через подвійне витрачання коштів у криптовалютній мережі, всі інші учасники, які мають копії ланцюга блоків, зможуть виявити невідповідність і відхилити таку спробу [12]. У таких випадках блокчейн ефективно захищає систему від атак типу «50% контроль», де зловмисники намагаються отримати контроль над більшою частиною обчислювальних ресурсів або активів мережі, щоб маніпулювати транзакціями.

Ще однією важливою особливістю блокчейн-технології є її дистрибутивна природа. У розподіленій мережі дані не зберігаються в одному місці або на одному сервері. Натомість вони реплікуються на кількох учасниках, що гарантує високий рівень доступності і стійкості до атак типу «відмова в обслуговуванні» (Denial of Service, DoS) або «розподілена відмова в обслуговуванні» (DDoS). Якщо один з учасників мережі або вузлів буде зазнавати атаки чи вийде з ладу, інші учасники мережі продовжуватимуть працювати, забезпечуючи постійну доступність даних. Крім того, для блокчейн-мережі характерна стійкість до маніпуляцій, оскільки для того, щоб змістити чи змінити дані на всіх копіях ланцюга, зловмисник повинен контролювати більшість учасників мережі або ресурси, що зробити надзвичайно складно. Така дистрибуція даних робить мережу менш вразливою до локальних атак, пов’язаних із пошкодженням або втручанням в окремі сервери [13].

Захист від атак у розподілених системах також підтримується через використання механізмів аутентифікації та цифрових підписів. Кожен учасник мережі має пару криптографічних ключів – публічний і приватний. Приватний ключ використовується для підпису транзакцій, що дозволяє підтвердити їхню автентичність і забезпечити їхнє збереження в блокчейні. Публічний ключ дає змогу перевірити підпис та перевірити, чи було підтвердження справжнім. Ці криптографічні методи забезпечують високий рівень безпеки, оскільки тільки той, хто має доступ до приватного ключа, може підписати транзакцію і гарантувати її правомірність.

Окрім цього, блокчейн здатен протистояти атакам на зловмисне відстеження або маніпуляції з транзакціями, таким як атаки на конфіденційність. Деякі сучасні блокчейни, такі як Monero або Zcash, застосовують спеціальні методи для покращення конфіденційності, використовуючи методи обфускації або zk-SNARKs (zero-knowledge succinct non-interactive arguments of knowledge), щоб приховати інформацію про

транзакції, зокрема про сторони, суму та час операцій [16]. Такі підходи дозволяють забезпечити більшу анонімність і захист від атак, що базуються на аналізі ідентифікації користувачів та виведенні інформації про їхні фінансові операції.

Незважаючи на безліч переваг, блокчейн не є абсолютно захищеною технологією, і існують певні виклики, пов’язані з його безпекою. Наприклад, атаки 51%, де зловмисники здобувають контроль над більшістю обчислювальних потужностей у мережі, можуть становити загрозу для цілісності даних. Такі атаки можуть бути ймовірнішими в невеликих або централізованих мережах, де кілька великих гравців контролюють більшу частину ресурсу. Тому для підвищення безпеки блокчейн-мереж необхідно постійно вдосконалювати алгоритми консенсусу, а також забезпечувати більш високий рівень дистрибуції і різноманітності учасників.

Загалом, блокчейн-технологія забезпечує надзвичайно потужний механізм захисту від атак у розподілених системах. Її особливості, такі як використання криптографії, дистрибуція даних, механізми консенсусу і цифрові підписи, роблять блокчейн одним з найбільш надійних інструментів для забезпечення безпеки та цілісності даних у цифровому середовищі. Враховуючи постійний розвиток цієї технології, можна очікувати, що в майбутньому вона стане ще більш стійкою до атак та підвищить рівень захисту у різноманітних розподілених системах.

2.3 Аналіз переваг та обмежень блокчейн у порівнянні з іншими технологіями безпеки

Блокчейн, як технологія, була розроблена для підтримки криптовалют і забезпечення безпечних, прозорих та дистрибутивних записів транзакцій. Однак її можливості значно перевищують потреби тільки у фінансових операціях, і сьогодні блокчейн розглядається як універсальний механізм для

забезпечення безпеки в різних цифрових системах [16]. Порівняння блокчейн з іншими технологіями безпеки, такими як традиційні централізовані системи з використанням серверів і баз даних, або технології криптографічного захисту даних, дозволяє з’ясувати як переваги цієї технології, так і її обмеження в контексті застосування в різних сферах.

Однією з основних переваг блокчейн є його дистрибутивна природа. У традиційних централізованих системах всі дані зберігаються в одному місці, на одному сервері або в базі даних, що робить такі системи вразливими до атак, збоїв або порушень цілісності даних. Наприклад, в разі зламу серверу чи бази даних, зловмисник може отримати доступ до всієї інформації або змінити її. В контексті блокчейну кожен учасник мережі має власну копію даних, і для того, щоб змінити інформацію, зловмисник повинен контролювати більшість учасників мережі, що є надзвичайно складним завданням, особливо в великих дистрибутивних мережах. Блокчейн є стійким до централізованих атак, оскільки немає єдиного центру, який можна атакувати. Всі транзакції та дані розподілені між учасниками мережі, що унеможливлює зміну чи підробку інформації без того, щоб не бути поміченим.

Іншою важливою перевагою блокчейн-технології є використання криптографічних методів для забезпечення безпеки даних [16, 17]. Кожен блок у ланцюгу містить криптографічний хеш попереднього блоку, що забезпечує цілісність інформації. Якщо хоча б один біт даних змінюється, хеш цього блоку також змінюється, і це порушує цілісність всього ланцюга. Така структура робить підробку або зміну інформації практично неможливою, що є критично важливим для забезпечення довіри між учасниками системи. У традиційних централізованих системах для забезпечення безпеки часто використовуються шифрування та інші методи криптографії, але вони можуть бути менш ефективними в разі порушення цілісності серверів або баз даних. Блокчейн дозволяє зберігати дані в незмінному вигляді, що робить технологію ідеальною для застосування в таких сферах, як фінансові операції, управління

ланцюгами поставок, голосування, юридичні контракти та інші критично важливі системи.

Системи блокчейн також мають значну перевагу у прозорості та можливості аудиту. Оскільки всі транзакції в блокчейні є публічно доступними і можуть бути перевірені будь-яким учасником мережі, забезпечується високий рівень прозорості. Кожен учасник може побачити всі здійснені операції, що допомагає знизити ризик шахрайства або корупції. Це є великим плюсом у порівнянні з традиційними централізованими системами, де доступ до даних обмежений, а для аудиту потрібно звертатися до центрального органу, що може привести до зловживань або маніпуляцій з інформацією. У випадку блокчейну, будь-яка спроба змінити вже записану інформацію відразу виявляється завдяки тому, що зміна хешу блоку призводить до зміни всього ланцюга блоків. Це забезпечує високий рівень довіри до системи, оскільки кожен учасник має змогу перевірити правильність і правдивість записаних даних [15-17].

Однак, незважаючи на всі переваги, блокчейн має і свої обмеження, особливо в порівнянні з іншими технологіями безпеки. Одним із найбільших обмежень є масштабованість. Блокчейн-системи, зокрема ті, що використовують алгоритм консенсусу Proof of Work (PoW), мають обмежену пропускну здатність, оскільки кожна транзакція повинна бути перевірена всіма учасниками мережі, а нові блоки додаються до ланцюга через певні інтервали часу. У великих мережах це може призвести до затримок у підтвердженні транзакцій та значних витрат на обчислювальні ресурси, що знижує загальну ефективність системи. Інші технології, такі як централізовані системи або навіть деякі дистрибутивні технології, можуть бути більш ефективними з точки зору швидкості обробки транзакцій, оскільки вони не вимагають перевірки кожної операції всіма учасниками системи. Блокчейн-системи, хоча і мають вищий рівень безпеки та прозорості, не можуть

обробляти таку кількість операцій за секунду, як централізовані системи, що працюють на високопродуктивних серверах.

Ще однією суттєвою проблемою блокчейн-технології є енергетична витратність. Алгоритм консенсусу Proof of Work, який використовується в таких системах, як Bitcoin, потребує великих обчислювальних потужностей для вирішення складних математичних задач, що забезпечують створення нових блоків у ланцюгу. Це призводить до величезних енергетичних витрат і підвищених витрат на обладнання для майнінгу. У порівнянні з іншими технологіями безпеки, де обчислювальні ресурси використовуються менш інтенсивно, блокчейн може бути значно дорожчим у плані витрат на енергію та обладнання. Хоча інші механізми консенсусу, такі як Proof of Stake (PoS), спрямовані на зниження енергетичних витрат, проблема масштабованості та витрат на ресурси залишається актуальною для більшості блокчейн-систем [4].

Додатково, блокчейн не є абсолютно захищеним від усіх видів атак. Хоча блокчейн забезпечує високий рівень захисту від підробки та маніпуляцій, існують інші типи атак, такі як атаки 51%, де зловмисники можуть контролювати більшість ресурсів мережі і таким чином змінювати хід транзакцій. Хоча для таких атак потрібні значні ресурси, вони все ж можуть мати місце в невеликих чи менш дистрибуційних мережах, що є ще однією слабкою стороною блокчейну порівняно з іншими технологіями безпеки, де централізований контроль може бути більш ефективним у виявленні і нейтралізації таких загроз.

Крім того, блокчейн не вирішує питання безпеки на рівні додатків. І хоча сама блокчейн-мережа є надзвичайно стійкою до атак і маніпуляцій з даними, додатки, які працюють на основі блокчейн, можуть бути вразливими до атак, пов’язаних із неправильним програмуванням або експлуатацією помилок в коді смарт-контрактів. Ці вразливості можуть призвести до витоків або маніпуляцій з даними навіть у системах, які на перший погляд здаються абсолютно захищеними.

Враховуючи всі ці переваги та обмеження, блокчейн пропонує унікальну комбінацію високого рівня безпеки, прозорості та дистрибутивної природи, яка робить його надзвичайно привабливим для різних застосувань. Однак важливо зазначити, що блокчейн не є панацеєю від усіх проблем безпеки, і його ефективність значною мірою залежить від конкретних умов застосування, таких як масштаби мережі, тип операцій і потреби в обробці даних. Інші технології безпеки, як то традиційні централізовані системи або сучасні методи криптографії, можуть бути більш підходящими в деяких випадках, де швидкість, масштабованість та ефективність мають більшу вагу. Усі ці фактори слід враховувати при виборі технології безпеки для конкретного випадку.

2.4 Інноваційні досягнення у розвитку алгоритмів консенсусу

Інноваційні досягнення у розвитку алгоритмів консенсусу є одним з найважливіших аспектів еволюції блокчейн-технології, адже саме алгоритми консенсусу забезпечують безпеку, цілісність та надійність дистрибутивних систем. Враховуючи, що блокчейн від самого початку застосовувався в криптовалютних мережах, таких як Bitcoin, основною метою алгоритмів консенсусу було гарантування того, що всі учасники мережі можуть дійти згоди щодо стану реєстру (наприклад, підтвердження транзакцій) без необхідності у централізованому авторитеті [13-15]. Це дозволило створити відкриті, дистрибутивні системи, де безпека і надійність залежать від численних учасників, а не від централізованого контролю.

Алгоритми консенсусу забезпечують узгоджене бачення розподіленої бази даних або реєстру, що особливо важливо в контексті блокчейн-систем, які можуть мати мільйони учасників, де кожен з них може мати власні зацікавленості чи мотивацію змінити інформацію. Оскільки немає єдиного керівного органу, механізми консенсусу стають основним інструментом для

запобігання шахрайству, подвійним витратам і будь-яким іншим спробам маніпулювання системою. В результаті, багато уваги приділяється вдосконаленню алгоритмів консенсусу, що дозволяє збалансувати ефективність, безпеку і масштабованість.

Одним з перших і найвідоміших алгоритмів консенсусу є Proof of Work (PoW), який використовується в Bitcoin. Його основна ідея полягає в тому, що для того, щоб створити новий блок і додати його до ланцюга, учасники мережі повинні вирішити складну математичну задачу, що вимагає великих обчислювальних ресурсів [16]. Це дозволяє забезпечити високу безпеку, оскільки для того, щоб зловмисник змінив інформацію в блокчейні, йому потрібно буде переобчислити значну кількість блоків, що вимагає величезної потужності. Однак на практиці PoW має суттєві недоліки, серед яких надмірна енергоспоживаність і обмежена масштабованість. Це стало причиною для розробки нових, більш ефективних алгоритмів консенсусу, які можуть підтримувати більшу кількість транзакцій та менш енергозатратні.

Інноваційним досягненням став алгоритм Proof of Stake (PoS), який є альтернативою PoW і намагається вирішити проблеми енергетичної витратності. У PoS валідатори обираються для створення нових блоків не на основі того, хто має найбільшу обчислювальну потужність, а на основі кількості криптовалюти, яку вони мають в своїй власності та готовності заморозити на певний час. Цей підхід значно знижує енергетичні витрати, оскільки не потребує складних обчислень для створення нових блоків. Проте PoS також має свої недоліки, зокрема потенційну концентрацію влади серед тих учасників, які володіють великими обсягами валюти, що може зменшити децентралізацію. Тому для забезпечення більшої справедливості і прозорості були розроблені нові варіанти цього алгоритму, такі як Delegated Proof of Stake (DPoS).

DPoS є вдосконаленою версією PoS, в якій криптовалютні власники делегують свої права на валідацію блоків обраним представникам або

делегатам. Це дозволяє зменшити навантаження на мережу, оскільки кількість учасників, які можуть створювати блоки, значно зменшується, а рішення щодо консенсусу приймаються швидше. Однак цей підхід також має свої недоліки, адже може призвести до більшої централізації процесу, оскільки делегати можуть обиратися лише активними учасниками, що має певний вплив на дистрибуцію повноважень у системі.

Іншим важливим досягненням у розвитку алгоритмів консенсусу є використання Byzantine Fault Tolerance (BFT), який був розроблений для забезпечення консенсусу в умовах, де деякі учасники мережі можуть діяти зловмисно або некоректно. В рамках BFT система може досягти консенсусу, навіть якщо частина учасників (до 1/3) є зловмисниками або відмовляються від співпраці [17]. Алгоритм BFT забезпечує високу стійкість до атак і гарантує, що вся система досягне консенсусу в межах прийнятного часу, навіть за умови, що деякі учасники мережі є ненадійними. Однак однією з проблем BFT є те, що його ефективність знижується з ростом кількості учасників у мережі, що призводить до необхідності обмежувати кількість вузлів або розробляти нові підходи до її масштабування.

Practical Byzantine Fault Tolerance (PBFT) є вдосконаленою версією класичного BFT, яка дозволяє досягти консенсусу у системах з великими числами учасників, зберігаючи при цьому ефективність і швидкість. PBFT активно застосовується в приватних та консорціумних блокчейнах, де наявність обмеженого числа учасників дозволяє ефективно працювати з більш складними алгоритмами, що вимагають інтенсивних обчислень.

У той час як всі ці алгоритми консенсусу є важливими етапами еволюції блокчейн-технологій, нові інновації не припиняються. Наприклад, технологія Sharding використовує принцип розподілу даних на менші частини або шард, кожен з яких має власний консенсус, що дозволяє збільшити масштабованість системи. Застосування шардінгу дозволяє кожному окремому сегменту блокчейну працювати незалежно від інших, тим самим зменшуючи

навантаження на загальну мережу та дозволяючи системі ефективно обробляти велику кількість транзакцій.

Ще одним важливим досягненням є Hybrid Proof of Stake and Proof of Work системи, які об’єднують найкращі риси PoW та PoS для забезпечення кращої безпеки і масштабованості [15]. Це дозволяє отримати переваги обох підходів і забезпечити більшу стійкість до атак за рахунок використання двох різних механізмів консенсусу, що дозволяє розподіляти навантаження і знижувати ризики концентрації влади в одних руках.

Крім цього, активно розвиваються і алгоритми консенсусу для специфічних типів блокчейн-систем, таких як Directed Acyclic Graphs (DAG), які не використовують традиційні блоки, а працюють із графами, що дозволяє усунути проблеми, пов’язані з лінійною структурою блокчейнів і масштабуванням. Такі системи, як IOTA і Hedera Hashgraph, активно використовують DAG для досягнення високої пропускної здатності і низьких витрат на транзакції, що робить їх привабливими для використання в інтернеті речей та інших застосуваннях, що вимагають швидкої обробки великих обсягів даних.

Таким чином, інноваційні досягнення в алгоритмах консенсусу мають величезне значення для розвитку блокчейн-технології. Вони дозволяють вирішувати питання, пов’язані з енергетичною витратністю, масштабованістю, дистрибуцією влади та стійкістю до атак. Однак незважаючи на досягнуті успіхи, існує багато викликів, з якими блокчейн-системи ще повинні зіткнутися, щоб забезпечити найкращу ефективність для широкого кола застосувань, і це відкриває нові горизонти для подальших досліджень і вдосконалень у цій сфері.

2.5 Нові підходи до інтеграції блокчейн у розподілені системи

Інтеграція блокчейн-технології в розподілені системи є надзвичайно актуальною проблемою в умовах швидкого розвитку сучасних інформаційних технологій. Блокчейн здобув популярність завдяки своїм особливостям, серед яких прозорість, безпека, дистрибутивність та здатність до забезпечення консенсусу без потреби в центральному авторитеті [11]. Однак ці особливості не можуть бути реалізовані без належної інтеграції блокчейну в розподілені системи, де безпека, надійність і ефективність передачі та зберігання даних стають першочерговими завданнями. Вивчення нових підходів до інтеграції блокчейн у розподілені системи дозволяє краще зрозуміти потенціал цієї технології в різних сферах, від фінансів до логістики та управління даними.

Розподілені системи, як правило, являють собою системи, в яких обчислювальні процеси, зберігання даних і прийняття рішень розподілені між численними комп’ютерами, що знаходяться в різних точках мережі. Така архітектура дозволяє системам працювати ефективно в умовах великого навантаження, а також забезпечує відмовостійкість і високу доступність послуг. Однак при використанні традиційних підходів до управління та забезпечення безпеки в таких системах виникає необхідність у централізованому контролі або у використанні довірених третьої сторони, що може створювати проблеми, зокрема в аспектах конфіденційності та контролю за даними.

Інтеграція блокчейн у розподілені системи дозволяє вирішити багато з цих проблем завдяки здатності блокчейну забезпечувати децентралізований консенсус. Кожен учасник системи може бути одночасно валідатором, який перевіряє транзакції і гарантує їх достовірність. Технологія блокчейн пропонує новий рівень довіри між учасниками, де необхідність у централізованому управлінні відпадає, оскільки всі зміни в базі даних підтверджуються численними учасниками за допомогою механізмів

консенсусу [10]. Це не тільки підвищує безпеку системи, а й дозволяє знижувати витрати на підтримку центральних серверів і адміністрування, забезпечуючи при цьому прозорість усіх дій.

Одним з основних напрямків інтеграції блокчейн у розподілені системи є використання цієї технології для забезпечення цілісності та безпеки даних. Розподілені системи часто зберігають великі обсяги інформації, яка повинна бути доступною в будь-який час, однак водночас ця інформація повинна бути захищена від несанкціонованого доступу та маніпуляцій. Технологія блокчейн може гарантувати, що будь-яка зміна даних в системі буде відображена в розподіленому реєстрі, який є незмінним і не піддається маніпуляціям без консенсусу більшості учасників. Завдяки цьому, навіть якщо частина мережі стане скомпрометованою, решта зможе забезпечити непорушність інформації.

Завдяки своїй структурі, блокчейн є оптимальним інструментом для інтеграції з різними типами розподілених систем. Зокрема, він може бути ефективно використаний для управління дистрибуцією даних у великих мережах, де важливо забезпечити їх достовірність і доступність. Блокчейн надає засоби для створення «розумних контрактів» – автоматизованих угод, які виконуються при виконанні певних умов, що дозволяє значно скоротити час на виконання операцій і мінімізувати ризики помилок чи шахрайства.

Ще одним напрямом інтеграції є використання блокчейну для забезпечення анонімності та конфіденційності в розподілених системах. Хоча блокчейн є публічним реєстром, існують підходи до його використання, які дозволяють зберігати анонімність учасників, не порушуючи принципів прозорості та надійності. Зокрема, застосування спеціалізованих протоколів, таких як zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge), дозволяє забезпечити перевірку правильності транзакцій без необхідності розкривати їх вміст [9]. Ці методи дозволяють захищати особисті дані користувачів у розподілених системах, де конфіденційність є важливим аспектом.

Іншим цікавим напрямком є інтеграція блокчейн з іншими передовими технологіями, такими як Інтернет речей (IoT) та штучний інтелект (AI). Розподілені системи, що включають IoT, складаються з численних пристроїв, які обмінюються даними та виконують різноманітні операції. Використання блокчейн у таких системах дозволяє створювати прозорі та безпечні канали для обміну даними між пристроями, що забезпечує високу ступінь довіри до інформації, що передається. Крім того, завдяки інтеграції блокчейн з AI, можливо автоматизувати прийняття рішень на основі даних, що зберігаються в блокчейні, зберігаючи при цьому високий рівень безпеки і надійності. Ще одним важливим аспектом є використання блокчейн для підтримки інтеграції розподілених систем у більш глобальні інфраструктури [7]. Оскільки блокчейн дозволяє зберігати інформацію у вигляді дистрибутивного реєстру, який доступний усім учасникам системи, він може бути використаний для створення єдиних стандартів та протоколів для глобальних мереж. Це дозволяє знижувати ризики для учасників різних мереж, що обмінюються даними, і підвищує ефективність їх взаємодії. Використання блокчейн також дозволяє знижувати транзакційні витрати, адже він усуває необхідність у посередниках, а це призводить до зменшення витрат на оплату послуг третіх сторін.

Інтеграція блокчейн у розподілені системи також має значення в контексті автоматизації бізнес-процесів. Завдяки використанню розумних контрактів, можна автоматизувати багато аспектів бізнес-операцій, таких як перевірка умов договорів, здійснення платежів, управління ланцюгами постачання та багато іншого. Це знижує ймовірність помилок і шахрайства, а також збільшує ефективність операцій.

Таким чином, інтеграція блокчейн у розподілені системи відкриває нові можливості для створення більш ефективних, безпечних та прозорих інфраструктур, де учасники можуть взаємодіяти без потреби в централізованому управлінні. Завдяки здатності блокчейну забезпечувати дистрибуцію даних, автоматизацію процесів та високий рівень безпеки,

розподілені системи на основі цієї технології можуть стати основою для майбутнього розвитку численних галузей, таких як фінанси, логістика, охорона здоров’я, а також для створення нових бізнес-моделей і інфраструктур.

2.6 Висновки до другого розділу

Перш за все, блокчейн забезпечує цілісність даних завдяки своїй структурі, де інформація, що зберігається в блоках, є незмінною та захищеною від будь-яких несанкціонованих змін. Важливим аспектом є дистрибутивний характер блокчейн-мережі, що дозволяє кожному учаснику контролювати інформацію, підтверджуючи її точність і правильність. Така організація дозволяє забезпечити високу стійкість до атак і підвищити рівень довіри між учасниками системи, оскільки дані неможливо змінити без погодження більшості учасників.

Захист від атак у розподілених системах є одним із основних переваг використання блокчейн-технології. Завдяки своїм механізмам консенсусу та криптографічному захисту, блокчейн забезпечує надійний захист від численних типів атак, включаючи атаки на доступність, маніпуляції з даними та фальсифікацію транзакцій. Крім того, блокчейн знижує потребу в централізованих точках контролю, що в свою чергу мінімізує можливості для злому або зловживання.

Аналіз переваг і обмежень блокчейн у порівнянні з іншими технологіями безпеки дозволяє зробити висновок, що хоча блокчейн має безліч сильних сторін, таких як підвищена безпека, прозорість і децентралізація, він також має певні обмеження, зокрема в контексті масштабованості та енерговитрат. У порівнянні з традиційними централізованими системами блокчейн може мати меншу швидкість обробки транзакцій і вищі витрати на ресурсів, що є важливими факторами для практичного застосування.

Інноваційні досягнення у розвитку алгоритмів консенсусу відкривають нові можливості для оптимізації роботи блокчейн-систем, знижуючи їх енергоспоживання та підвищуючи ефективність. Однак це також вимагає вдосконалення механізмів безпеки, щоб забезпечити їх надійність у нових умовах. Різноманітність алгоритмів консенсусу, таких як Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS) та інші, дозволяє вибирати найбільш підходящий метод для різних типів розподілених систем, враховуючи вимоги до швидкості, безпеки та енергоспоживання.

Важливим етапом є інтеграція блокчейн-технології в існуючі розподілені системи. Використання блокчейну дозволяє створити більш прозорі, безпечні та автоматизовані інфраструктури, що в свою чергу сприяє підвищенню довіри до систем та зниженню витрат на адміністрування. Крім того, блокчейн має потенціал для інтеграції з іншими передовими технологіями, такими як Інтернет речей (IoT) та штучний інтелект (AI), що відкриває нові можливості для автоматизації та безпеки.

Загалом, блокчейн-технології є важливим кроком вперед у розвитку безпечних і прозорих розподілених систем. Однак їх впровадження вимагає вирішення низки технічних, економічних та організаційних проблем, які можуть обмежувати їх широке застосування на поточному етапі розвитку. Тому для досягнення повного потенціалу блокчейн необхідно продовжувати дослідження в галузі вдосконалення алгоритмів консенсусу, оптимізації енергоспоживання та інтеграції з іншими технологіями.

РОЗДІЛ 3. ПРОГРАМНА РЕАЛІЗАЦІЯ

3.1 Постановка задачі

Постановкою задачі визначено необхідність розроблення програмного коду, який демонструє застосування технологій блокчейн для забезпечення безпеки, прозорості та ефективності у розподілених системах.

Вимоги:

– реалізувати механізм побудови блокчейну, який складається з блоків, кожен з яких містить дані про транзакції, часову мітку, хеш попереднього блоку, доказ виконаної роботи (proof-of-work) і хеш самого блоку;

– забезпечити можливість перевірки цілісності ланцюга блоків та виявлення змін;

– реалізувати механізм додавання транзакцій до списку очікування та включення їх до блоків під час їх створення;

– забезпечити можливість передачі додаткових даних у транзакціях;

– реалізувати механізм доказу виконаної роботи з використанням обчислювальних завдань для забезпечення захисту блоків;

– забезпечити можливість реєстрації вузлів у блокчейн-мережі для взаємодії з іншими учасниками системи;

– реалізувати механізм консенсусу для вирішення конфліктів та забезпечення єдиного джерела істини;

– створити програмний інтерфейс для доступу до функціоналу системи через HTTP-запити;

– забезпечити високу стійкість до підробки даних шляхом використання хешування;

– реалізувати механізм складності задачі proof-of-work для підвищення безпеки.

Для реалізації необхідно використовувати мову програмування Python. Застосувати Flask для створення API, hashlib для хешування, а також бібліотеки для роботи з HTTP-запитами та аналізу URL.

Програмна реалізація повинна забезпечувати безпечний розподіл даних у системі, синхронізацію між вузлами мережі та можливість масштабування. Код має бути оптимізованим для легкого тестування та розширення функціоналу.

3.2 Архітектура блокчейну

Архітектура розробленого програмного забезпечення для демонстрації застосування технологій блокчейн є складною багаторівневою системою, що поєднує елементи обчислювальної теорії, криптографії та розподілених систем. Основною метою розробки було створення платформи, здатної забезпечувати прозорість, безпеку та консенсус між учасниками розподіленої мережі, а також забезпечити її функціонування в умовах динамічної взаємодії вузлів. У контексті цієї архітектури розглядаються базові компоненти, включаючи блокчейн, механізм консенсусу, транзакції, функції Proof-of-Work, мережеву взаємодію вузлів, а також прикладний програмний інтерфейс (API), що забезпечує доступ до функціональних можливостей системи. У центрі архітектури лежить клас Blockchain, який є основою всієї системи. Цей клас відповідає за управління ланцюгом блоків, зберігання транзакцій, створення нових блоків та перевірку їхньої цілісності. Ланцюг блоків представлено у вигляді масиву, де кожен блок є словником, що містить атрибути, необхідні для ідентифікації та захисту інформації. Кожен блок включає в себе хеш попереднього блоку, доказ виконаної роботи, список транзакцій, часову мітку створення та унікальний індекс. Генезис-блок створюється автоматично при ініціалізації об’єкта Blockchain. Він є стартовою точкою ланцюга і не має попереднього хешу, що позначається значенням «0».

Однією з ключових функцій архітектури є можливість додавання транзакцій до системи. Транзакції представлені як словники, що включають інформацію про відправника, отримувача, суму переказу, а також додаткові метадані. Це дозволяє зберігати в блокчейні не лише фінансові операції, але й будь-які інші дані, які можуть бути важливими для конкретного застосування. Транзакції зберігаються у списку очікування доти, поки вони не будуть включені в новий блок. Цей підхід дозволяє забезпечити ефективну обробку транзакцій, уникаючи затримок у разі високого навантаження.

Механізм створення блоків базується на алгоритмі доказу виконаної роботи (Proof-of-Work). Цей алгоритм є криптографічною задачею, яка вимагає значних обчислювальних ресурсів для її вирішення, але легко перевіряється. Використання цього механізму забезпечує стійкість до атак, оскільки створення фальшивого блоку або внесення змін до існуючого вимагає перерахунку Proof-of-Work для всіх наступних блоків. Алгоритм реалізовано шляхом пошуку числа, яке при хешуванні разом із попереднім доказом утворює хеш-значення, що відповідає заданій умові складності. Поточна реалізація використовує умову, за якої хеш повинен починатися з чотирьох нулів, однак цей параметр може бути змінений для підвищення або зниження складності системи.

Для забезпечення цілісності блокчейну реалізовано механізм перевірки валідності ланцюга. Він полягає у перевірці відповідності хешів між блоками, а також перевірці доказів роботи. Цей механізм дозволяє миттєво виявляти будь-які зміни в ланцюзі, гарантуючи збереження даних у незмінному вигляді. Така перевірка може бути виконана як локально, так і у процесі синхронізації з іншими вузлами мережі.

Система включає функціональність мережевої взаємодії, що реалізується через реєстрацію вузлів і механізм консенсусу. Вузли представляють собою індивідуальні екземпляри блокчейну, які взаємодіють між собою через HTTP-запити. Кожен вузол може реєструвати інші вузли у

своїй мережі, використовуючи унікальні URL-адреси. Це створює розподілену інфраструктуру, яка дозволяє учасникам системи обмінюватися інформацією про стан ланцюга блоків. Консенсус досягається шляхом порівняння поточного ланцюга з ланцюгами інших вузлів і вибору найдовшого дійсного ланцюга. Цей підхід забезпечує єдине джерело істини у системі та дозволяє вирішувати конфлікти, що можуть виникати через одночасне створення блоків різними вузлами.

Прикладний програмний інтерфейс (API), створений за допомогою Flask, забезпечує доступ до всіх основних функцій системи. API включає маршрути для створення нових блоків, додавання транзакцій, перегляду поточного стану блокчейну, перевірки його цілісності, пошуку транзакцій за певними критеріями, реєстрації вузлів і досягнення консенсусу. Це робить систему зручною для інтеграції з іншими додатками та сервісами. Усі маршрути API ретельно перевіряють вхідні дані, забезпечуючи їхню відповідність очікуваному формату, що зменшує ймовірність помилок і підвищує безпеку системи.

Ключовим аспектом архітектури є її гнучкість і масштабованість. Реалізована система може бути адаптована до різних сценаріїв використання шляхом додавання нових функцій або зміни існуючих. Наприклад, метадані транзакцій можуть бути використані для зберігання даних про товарні операції, медичні записи або документи. Крім того, механізм Proof-of-Work може бути замінений іншими алгоритмами консенсусу, такими як Proof-of-Stake або Delegated Proof-of-Stake, залежно від вимог конкретного застосування.

Для забезпечення надійності й стійкості до збоїв передбачено використання розподіленої архітектури. Усі дані зберігаються у вигляді копій на кожному вузлі мережі, що дозволяє зберігати їх навіть у разі відмови одного або кількох вузлів. Крім того, для забезпечення швидкої синхронізації даних між вузлами реалізовано механізм передачі ланцюга блоків через HTTP-

запити. Це дозволяє вузлам швидко відновлюватися після відключення від мережі та підтримувати актуальність даних.

Криптографічна основа архітектури базується на використанні алгоритму SHA-256 для хешування даних блоків і транзакцій. Цей алгоритм забезпечує високий рівень захисту, оскільки зворотний розрахунок хешу є обчислювально неможливим. Використання хеш-функції дозволяє гарантувати, що навіть найменша зміна даних у блоці призводить до суттєвої зміни хешу, що унеможливлює підробку інформації без виявлення. Крім того, кожен блок містить хеш попереднього блоку, що забезпечує послідовність і зв’язність ланцюга.

Розроблена архітектура є прикладом сучасного підходу до використання блокчейн-технологій для вирішення реальних задач. Вона може бути застосована у різних галузях, включаючи фінанси, логістику, охорону здоров’я та державне управління, забезпечуючи прозорість, безпеку та довіру між учасниками процесу. У подальшому розвиток системи може включати інтеграцію з іншими протоколами та платформами, розширення функціональних можливостей, а також оптимізацію алгоритмів для підвищення продуктивності та зменшення витрат на обчислення.

3.3 Використані технології

Розробка програмного забезпечення для демонстрації застосування технологій блокчейн передбачала використання сучасних інструментів, бібліотек і методів для забезпечення функціональності, безпеки та прозорості системи. Центральною частиною проекту є використання технології блокчейн, яка базується на розподілених обчисленнях і криптографії для забезпечення незмінності та достовірності даних. У цій системі блокчейн реалізовано у вигляді ланцюга блоків, кожен із яких містить список транзакцій, часову мітку, хеш попереднього блоку та доказ виконаної роботи. Для створення цієї

структури застосовано мову програмування Python, яка завдяки своїй простоті і потужності стала оптимальним вибором для реалізації даного проекту.

Python забезпечує багатий вибір бібліотек і фреймворків, які значно спрощують реалізацію складних функціональних можливостей. Наприклад, для створення прикладного програмного інтерфейсу (API) було використано фреймворк Flask. Flask дозволяє швидко розробляти RESTful API, що надає доступ до функціональних можливостей системи через HTTP-запити. Це включає маршрути для створення блоків, додавання транзакцій, перевірки валідності блокчейну, синхронізації вузлів і досягнення консенсусу. Простота інтеграції Flask з іншими бібліотеками Python і модульна структура дозволяють ефективно розширювати та модифікувати систему в майбутньому.

Для забезпечення безпеки і незмінності даних застосовано алгоритм хешування SHA-256, який використовується для створення унікального цифрового підпису кожного блоку. Алгоритм SHA-256 забезпечує високий рівень криптографічного захисту завдяки своїй стійкості до колізій і обчислювальній складності зворотного розрахунку. Хешування застосовується для перевірки цілісності даних у кожному блоці, де кожен новий блок містить хеш попереднього блоку, забезпечуючи нерозривність і зв’язність ланцюга. Такий підхід гарантує, що будь-яка спроба модифікації даних буде легко виявлена.

Ключовою функцією блокчейну є механізм консенсусу, який у цьому проекті реалізовано на основі алгоритму Proof-of-Work (PoW). PoW є фундаментальним компонентом безпеки, оскільки забезпечує стійкість до атак типу «51%» і запобігає створенню фальшивих блоків. Алгоритм PoW передбачає вирішення криптографічної задачі, яка потребує значних обчислювальних ресурсів. Задача полягає у пошуку числа (nonce), яке, у поєднанні з іншими даними блоку, утворює хеш-значення, що відповідає заданій умові складності. У поточній реалізації складність визначається як

кількість нульових бітів на початку хешу, що дозволяє налаштовувати рівень складності залежно від обчислювальної потужності мережі.

Однією з головних технологічних особливостей системи є реалізація розподіленої мережевої взаємодії між вузлами. Вузли мережі представляють собою екземпляри блокчейну, які взаємодіють між собою через HTTP-запити. Реєстрація вузлів здійснюється шляхом збереження їхніх URL-адрес у локальному реєстрі кожного вузла. Це дозволяє будувати масштабовану децентралізовану мережу, де кожен вузол може синхронізувати стан блокчейну з іншими. Для досягнення консенсусу вузли використовують метод порівняння довжини ланцюгів: найдовший дійсний ланцюг приймається як істинний. Це забезпечує цілісність і актуальність даних у мережі навіть у разі розбіжностей між окремими вузлами.

Мережевий рівень архітектури спирається на модуль requests, який є стандартом де-факто для виконання HTTP-запитів у Python. Використання requests дозволяє легко реалізувати клієнт-серверну модель, яка забезпечує обмін даними між вузлами мережі. Завдяки цьому можна виконувати такі операції, як передача нового блоку, оновлення списку транзакцій, синхронізація ланцюгів і реєстрація нових вузлів. Це дозволяє системі функціонувати як єдиний розподілений організм, незважаючи на фізичну ізоляцію вузлів один від одного.

Для забезпечення зручності використання та інтеграції системи з іншими додатками розроблено інтуїтивний API, який надає широкий спектр функціональних можливостей. API підтримує як прості запити для отримання інформації про стан блокчейну, так і складні операції, такі як додавання транзакцій або досягнення консенсусу. Використання JSON як формату обміну даними дозволяє легко інтегрувати систему з іншими сервісами, оскільки JSON є одним із найбільш поширених форматів у сучасній веб-розробці. Крім того, всі маршрути API реалізують перевірку вхідних даних, що забезпечує стабільність роботи системи і запобігає помилкам.

Окрім Flask і requests, у розробці активно використовувалися стандартні бібліотеки Python, такі як hashlib і datetime. Модуль hashlib забезпечує доступ до алгоритмів хешування, включаючи SHA-256, що є основою криптографічного захисту даних у системі. Модуль datetime використовується для створення часових міток, які додаються до кожного блоку. Це дозволяє відстежувати послідовність транзакцій і забезпечує додатковий рівень достовірності даних.

Архітектура системи передбачає можливість її адаптації до різних сценаріїв використання завдяки модульності та масштабованості. Наприклад, Proof-of-Work може бути замінений на інші алгоритми консенсусу, такі як Proof-of-Stake або Practical Byzantine Fault Tolerance (PBFT), залежно від потреб конкретного проекту. Крім того, до системи можна додати нові типи транзакцій, такі як смарт-контракти або складніші фінансові інструменти. Завдяки гнучкій структурі блокчейн може бути використаний у різних галузях, таких як фінанси, логістика, медицина або управління ідентифікацією.

Безпека системи є важливим аспектом, який забезпечується кількома рівнями захисту. По-перше, хешування даних гарантує їхню незмінність і цілісність. По-друге, Proof-of-Work унеможливлює створення фальшивих блоків без значних витрат обчислювальних ресурсів. По-третє, децентралізована архітектура унеможливлює централізовані атаки, оскільки кожен вузол має копію повного ланцюга блоків. Крім того, мережеві запити виконуються через HTTP, що дозволяє легко інтегрувати додаткові засоби захисту, такі як SSL/TLS, для шифрування трафіку між вузлами.

Загалом, використані технології та інструменти демонструють сучасний підхід до розробки розподілених систем на основі блокчейну. Система є прикладом інтеграції обчислювальних методів і криптографії для створення прозорої, надійної та безпечної інфраструктури. Подальший розвиток може включати розширення функціональних можливостей, оптимізацію

продуктивності та інтеграцію з іншими протоколами для забезпечення кросплатформеної взаємодії та підвищення загальної ефективності системи.

3.4 Схема роботи

Процес роботи розробленого програмного забезпечення для демонстрації технологій блокчейн базується на взаємодії між його ключовими компонентами, які забезпечують децентралізовану обробку, збереження та перевірку даних. Система функціонує через створення, передачу і валідацію транзакцій, формування блоків, виконання алгоритму консенсусу та синхронізацію вузлів у розподіленій мережі. Кожен з етапів роботи програмного забезпечення реалізовано з використанням сучасних методів програмування, криптографічних алгоритмів і протоколів передачі даних, що разом формують надійну та безпечну інфраструктуру для демонстрації можливостей блокчейну.

Робота програмного забезпечення починається з ініціалізації ланцюга блоків, що створюється у вигляді об’єкта класу Blockchain. На цьому етапі формується початковий блок, відомий як генезис-блок. Генезис-блок є основою для всього блокчейну і має фіксовані параметри, такі як індекс, часову мітку та початковий хеш. Його створення є необхідним для забезпечення послідовності всіх наступних блоків, оскільки кожен новий блок містить хеш попереднього блоку, що гарантує зв’язність та незмінність даних у ланцюзі. Ініціалізація передбачає також створення базової структури для зберігання непідтверджених транзакцій та механізмів для генерації нових блоків.

Основним завданням програмного забезпечення є обробка транзакцій, які подаються до системи користувачами або зовнішніми додатками через API. Транзакція представляє собою набір даних, що включає інформацію про відправника, отримувача і суму переказу. Для забезпечення гнучкості

використання система дозволяє додавати до транзакції метадані, що можуть містити будь-яку додаткову інформацію, таку як цифрові підписи, ідентифікатори продуктів або послуг, або інші відомості, що є релевантними для конкретного сценарію використання. Транзакції додаються до спеціального пулу, який слугує чергою для їхнього подальшого оброблення. Усі транзакції проходять початкову перевірку, щоб забезпечити їхню відповідність формату і наявність необхідних полів, що знижує ризик помилок у процесі їх обробки.

Наступним кроком є формування блоку, яке відбувається шляхом збору транзакцій із пулу та їх об’єднання у структурований блок. Блок містить заголовок, у якому зберігаються основні параметри, такі як індекс, час створення, хеш попереднього блоку, а також список транзакцій, що увійшли до нього. Формування блоку включає обчислення його Proof-of-Work, що є одним із найважливіших етапів процесу. Алгоритм Proof-of-Work реалізовано таким чином, що його виконання потребує значних обчислювальних ресурсів, але перевірка є простою і швидкою. Метою алгоритму є знайти таке значення nonce, яке при хешуванні разом із іншими даними блоку дає результат, що відповідає певній умові складності. Умову складності можна регулювати, змінюючи кількість нульових бітів на початку хешу, що дозволяє адаптувати систему до змін у потужності мережі. Виконання Proof-of-Work забезпечує безпеку системи, оскільки модифікація будь-якого блоку потребує повторного обчислення всіх наступних блоків, що практично неможливо у розподіленій мережі.

Після успішного виконання Proof-of-Work новий блок додається до ланцюга, і система переходить до синхронізації з іншими вузлами мережі. Синхронізація полягає у передачі даних про новий блок іншим вузлам через HTTP-запити. Інші вузли перевіряють валідність отриманого блоку шляхом повторного обчислення його хешу та перевірки Proof-of-Work. Якщо блок визнається дійсним, він додається до локального ланцюга вузла. У разі

виявлення конфліктів або розбіжностей між ланцюгами, вузли виконують процедуру досягнення консенсусу, що базується на правилі вибору найдовшого дійсного ланцюга. Такий підхід гарантує єдність даних у системі та дозволяє усунути розбіжності, що можуть виникати через затримки у передачі даних або інші мережеві проблеми.

Ключовою особливістю програмного забезпечення є реалізація децентралізованої мережевої архітектури, яка дозволяє кожному вузлу функціонувати незалежно, зберігаючи повну копію ланцюга блоків. Це забезпечує стійкість до збоїв і атак, оскільки видалення або компрометація одного вузла не впливає на загальну працездатність системи. Кожен вузол може реєструвати інші вузли, використовуючи їх URL-адреси, що створює розподілену мережу, де всі вузли рівноправно обмінюються інформацією. Реєстрація нових вузлів і синхронізація даних між ними реалізується за допомогою стандартних протоколів передачі даних, що забезпечує високу швидкість і надійність взаємодії.

API системи є ще одним важливим компонентом, який забезпечує зручний доступ до функціональних можливостей програмного забезпечення. API дозволяє користувачам виконувати такі операції, як додавання транзакцій, створення блоків, перегляд стану ланцюга блоків, реєстрація вузлів і досягнення консенсусу. Дані передаються у форматі JSON, який є стандартом для обміну даними у веб-додатках і забезпечує простоту інтеграції з іншими системами. Усі запити до API проходять перевірку на відповідність очікуваному формату, що запобігає потенційним помилкам і підвищує безпеку системи.

Завдяки реалізації зазначених функціональних можливостей розроблене програмне забезпечення демонструє потенціал технологій блокчейн для створення безпечних і прозорих розподілених систем. Воно забезпечує збереження даних у незмінному вигляді, їхню доступність і актуальність у масштабованій мережі. Подальший розвиток системи може включати

інтеграцію смарт-контрактів, використання альтернативних алгоритмів консенсусу, таких як Proof-of-Stake, або додавання підтримки складніших сценаріїв використання, що зробить систему ще більш універсальною та ефективною.

3.5 Тестування блокчейну

Для початку проведення експериментів необхідно запустити застосунок на будь-якому сервері. Наприклад, локальному (рис. 3.1).

```
 * Serving Flask app 'main'
 * Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on all addresses (0.0.0.0)
 * Running on http://127.0.0.1:5000
 * Running on http://192.168.0.101:5000
Press CTRL+C to quit
```

Рисунок 3.1 – Запуск програмного застосунка на локальному сервері

Після запуску можна перейти за адресою локального хостингу та почати роботу.

Так як застосунок представляє собою серверну частину (backend), то для проведення експериментів більш професійним рішенням буде використання спеціалізованої програми, яка дозволяє надсилати різноманітні HTTP-запити. В даному дослідженні використовується Postman.

Отже, початок роботи здійснюється за допомогою запиту /mine_block (рис. 3.2). Він повертає повідомлення, хеш, proof, час, індекс та транзакцію.

Також сервер може приймати запити на створення транзакцій між відправником та отримувачем (рис. 3.3). Приклад параметрів для цього запиту наведено на рисунку 3.4.

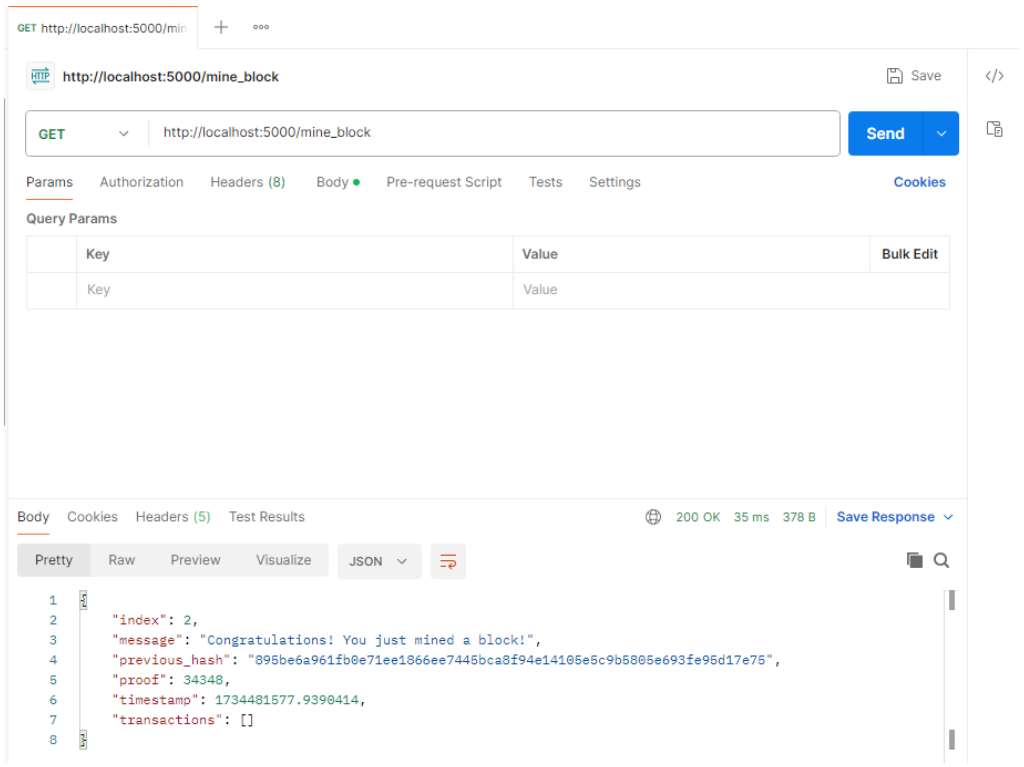

Рисунок 3.2 – Результат виконання запиту /mine_block

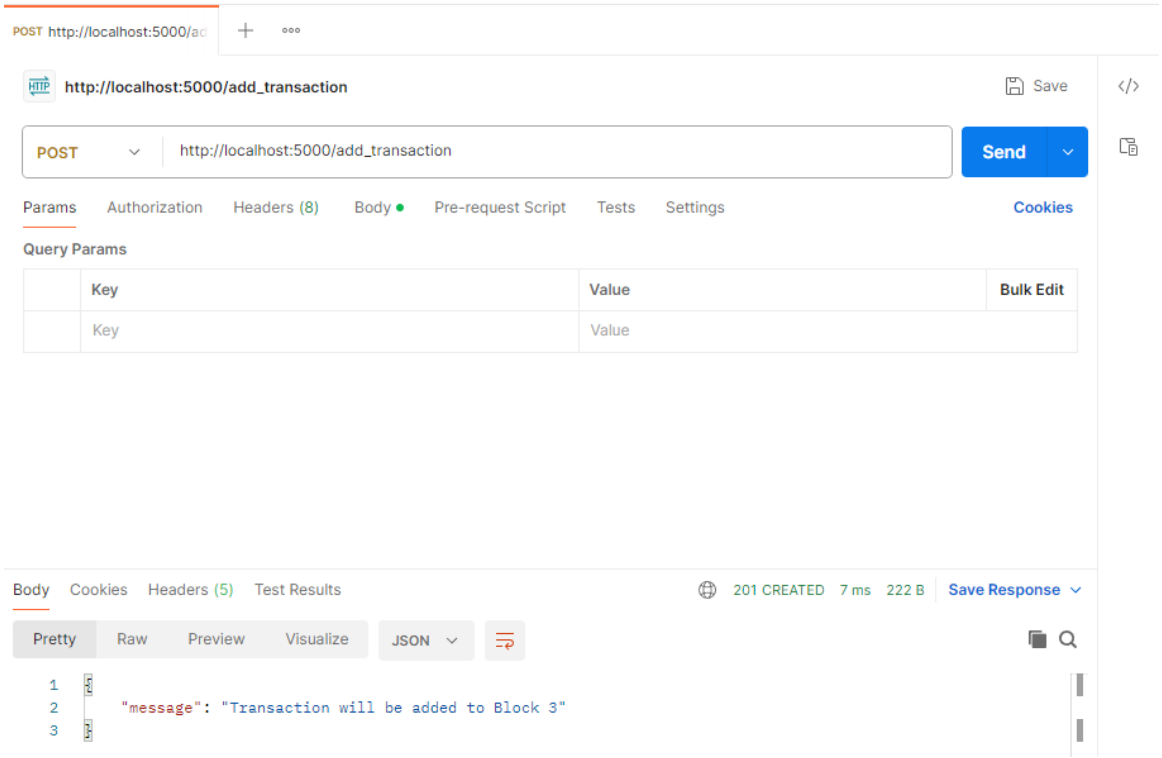

Рисунок 3.3 – Результат виконання запиту /add_transaction

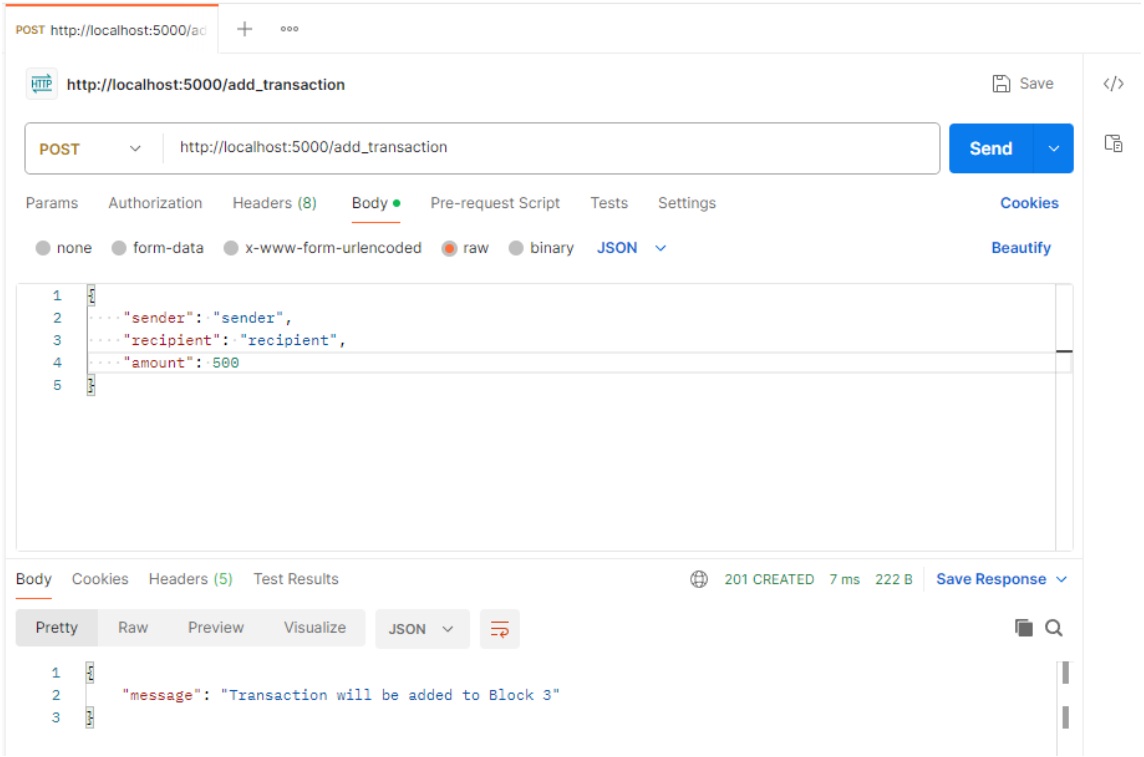

Рисунок 3.4 – Приклад параметрів для запиту /add_transaction

Після початку роботи або здійснення транзакцій існує можливість отримати ланцюг (рис. 3.5). Цей метод повертає увесь ланцюг та супроводжуючу інформацію щодо хешів, індексів, proof, транзакцій тощо.

Наступним доступним HTTP-запитом є /is_valid, який перевіряє валідність ланцюга (рис. 3.6).

Також у застосунку міститься можливість реєстрації нодів (рис. 3.7).

Для вирішення конфліктів використовується окремий HTTP-запит /resolve_conflicts (рис. 3.8).

Також існує можливість отримати транзакції за пошуком (рис. 3.9).

Після здійснення багатьох операцій доцільно ще раз отримати весь ланцюг та переконатися у збереженні даних (рис. 3.10-3.11).

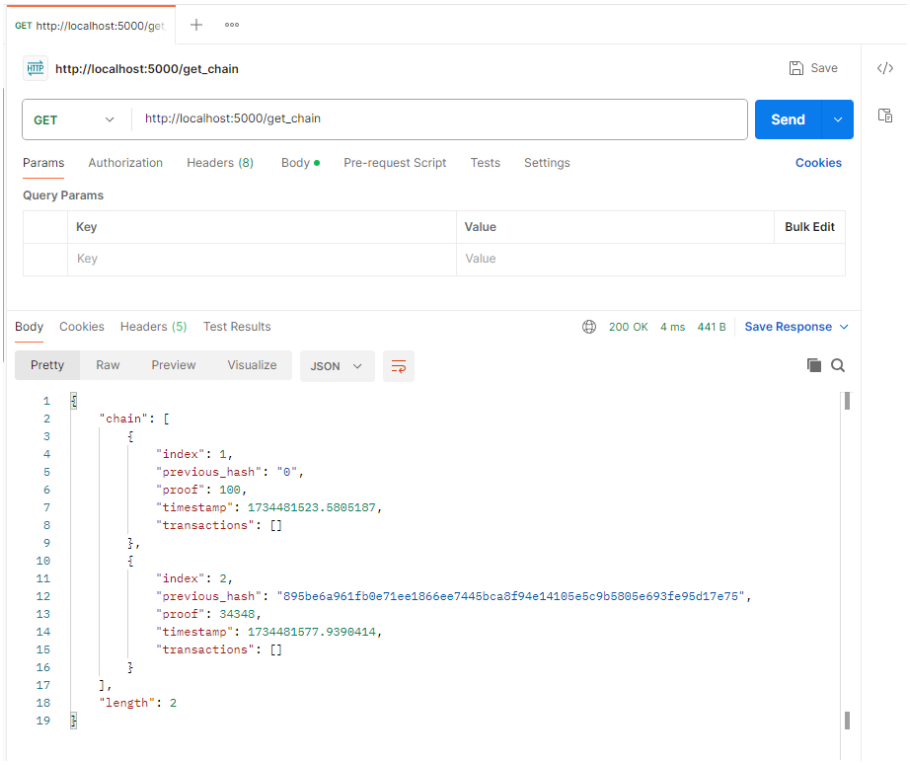

Рисунок 3.5 – Результат виконання запиту /get_chain

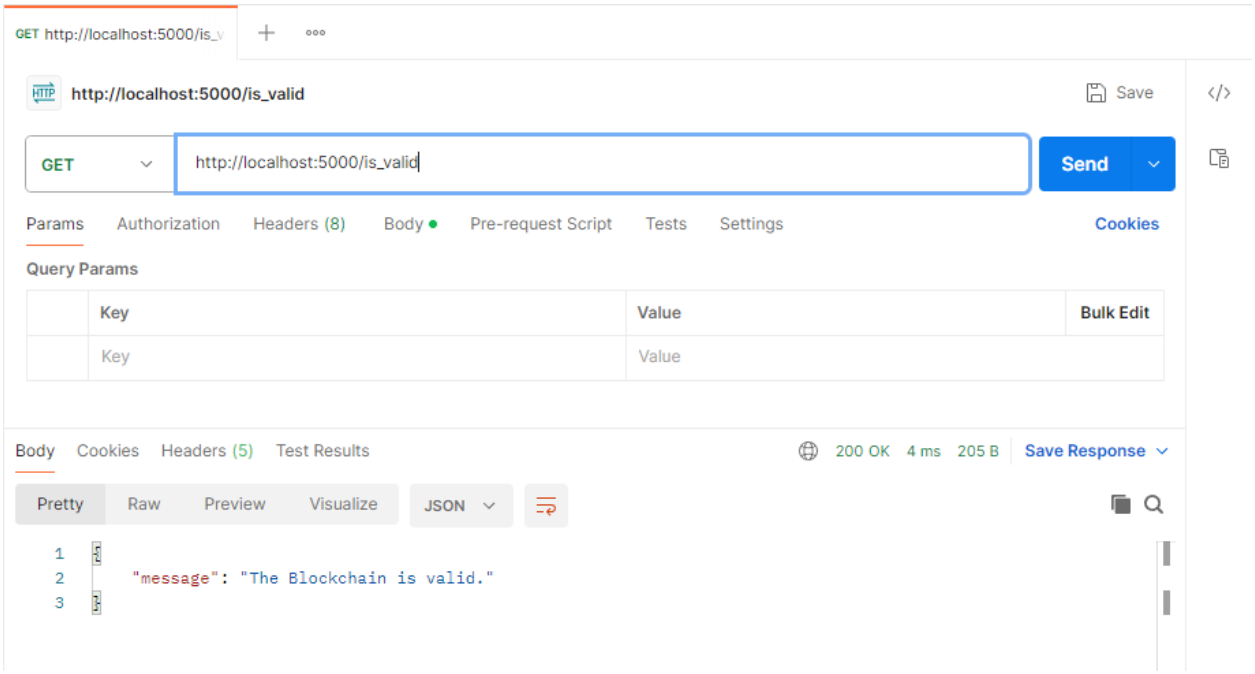

Рисунок 3.6 – Результат виконання запиту /is_valid

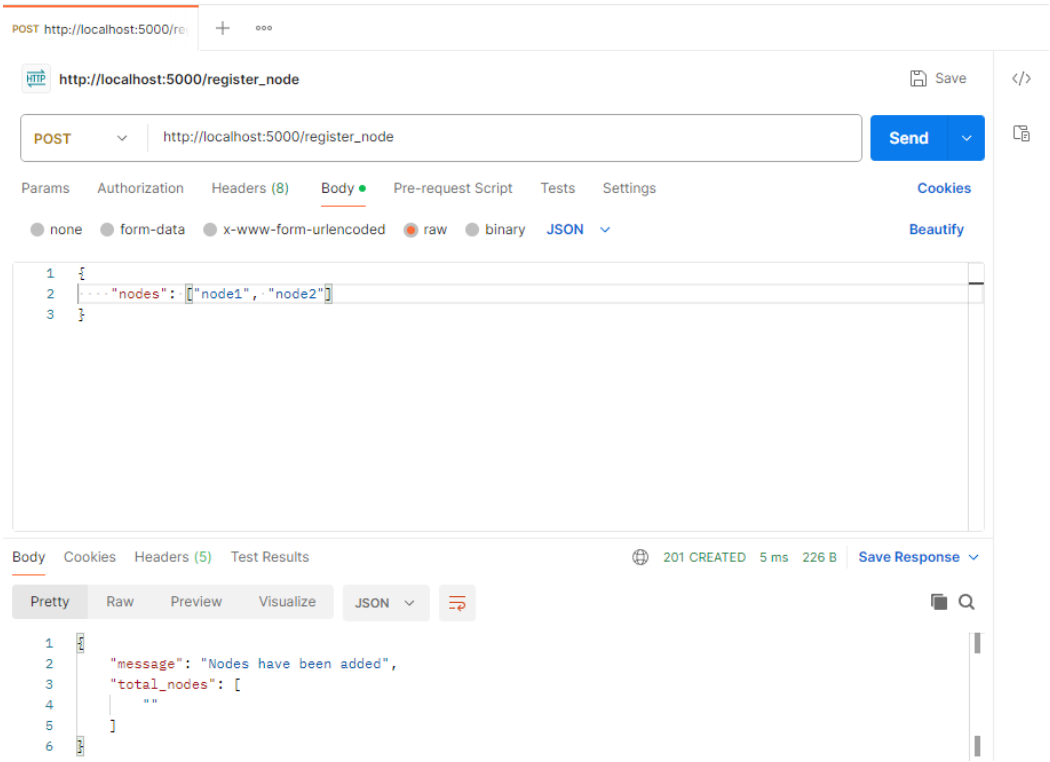

Рисунок 3.7 – Результат виконання запиту /register_node

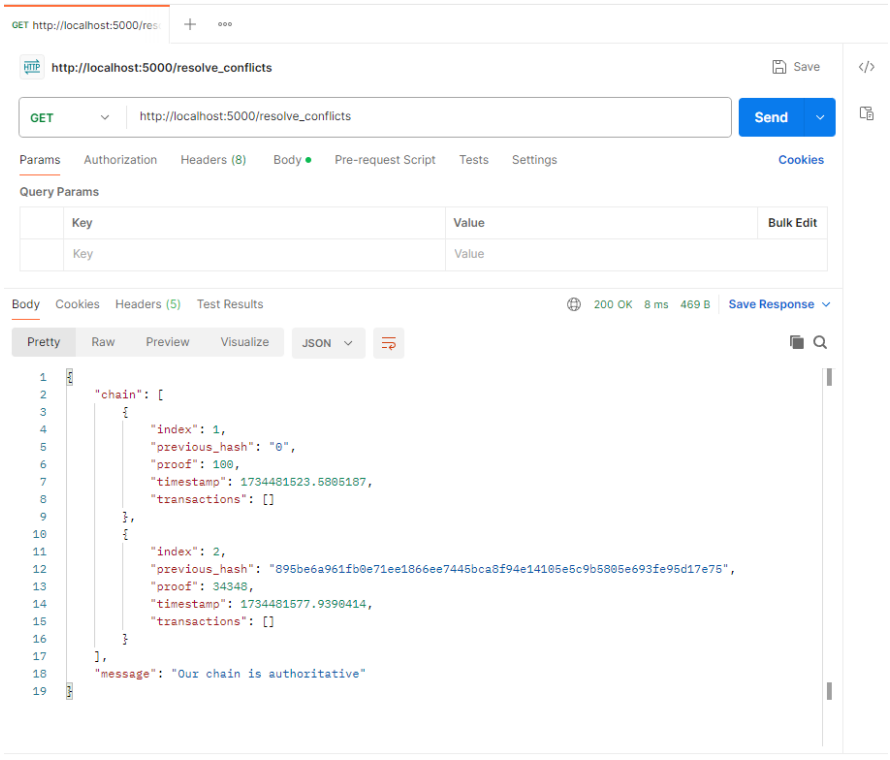

Рисунок 3.8 – Результат виконання запиту /resolve_conflicts

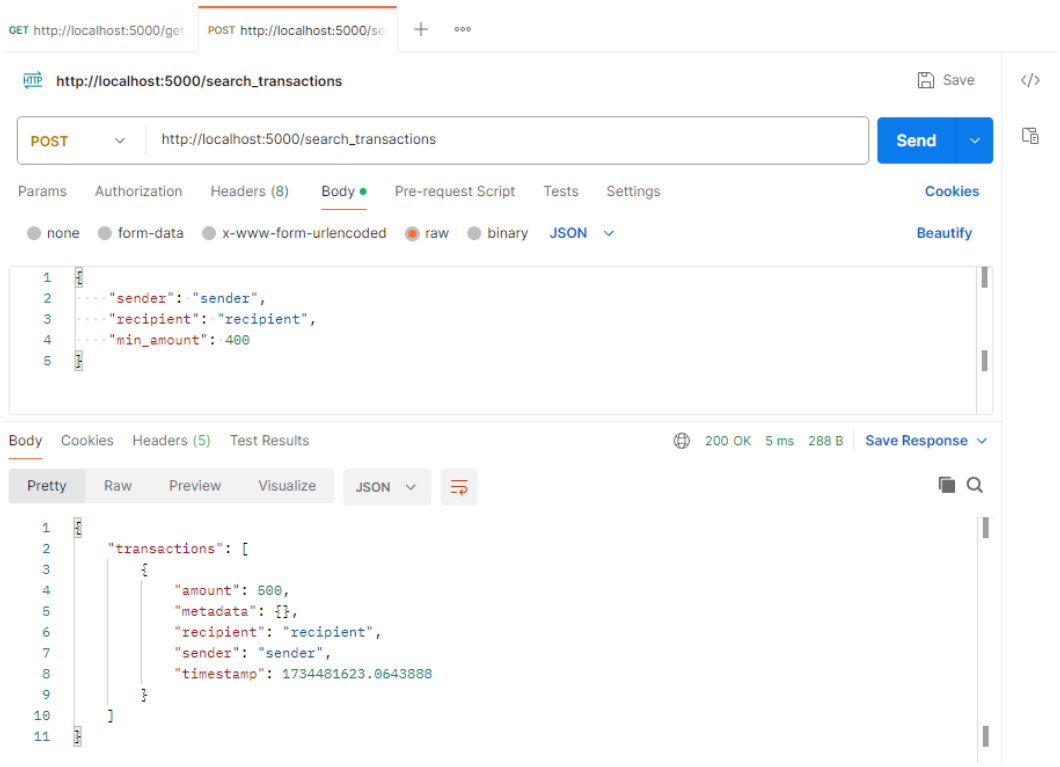

Рисунок 3.9 – Результат виконання запиту /search_transactions

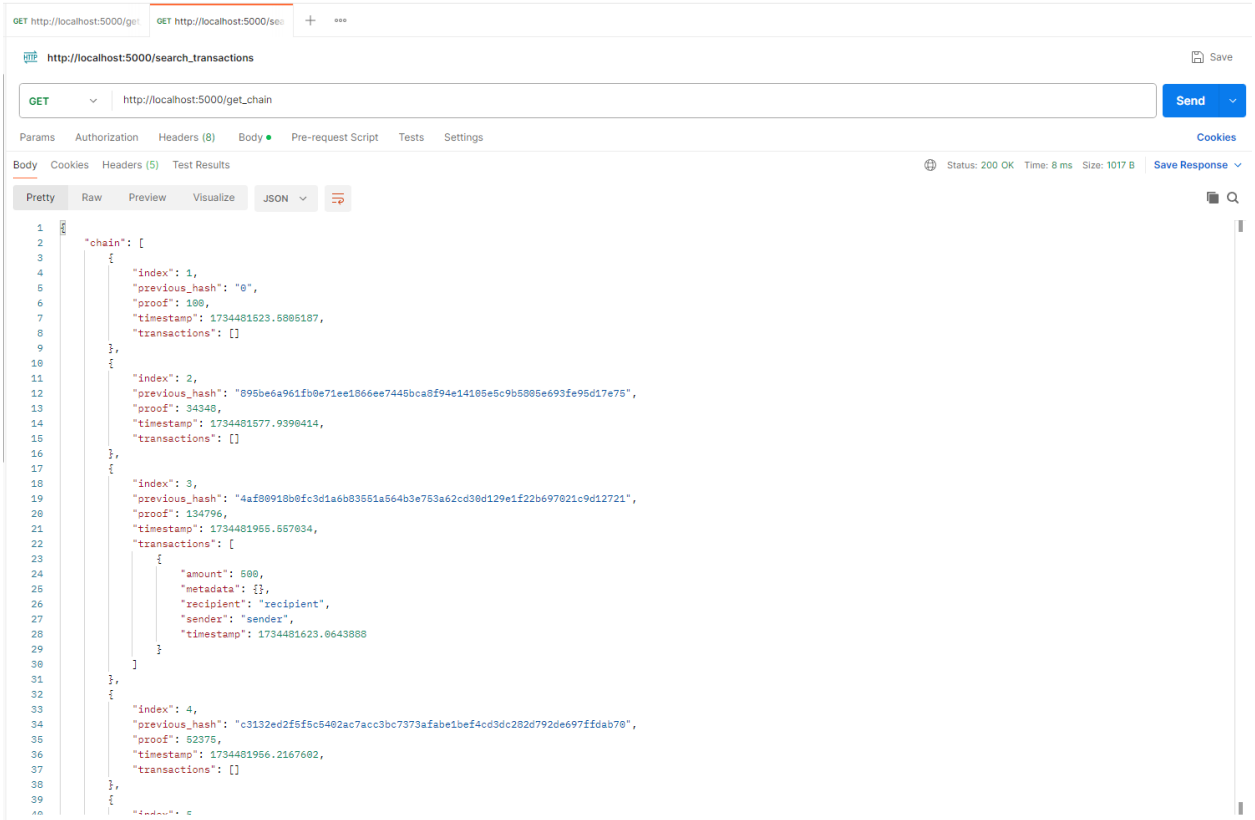

Рисунок 3.10 – Результат виконання запиту /get_chain після декількох дій

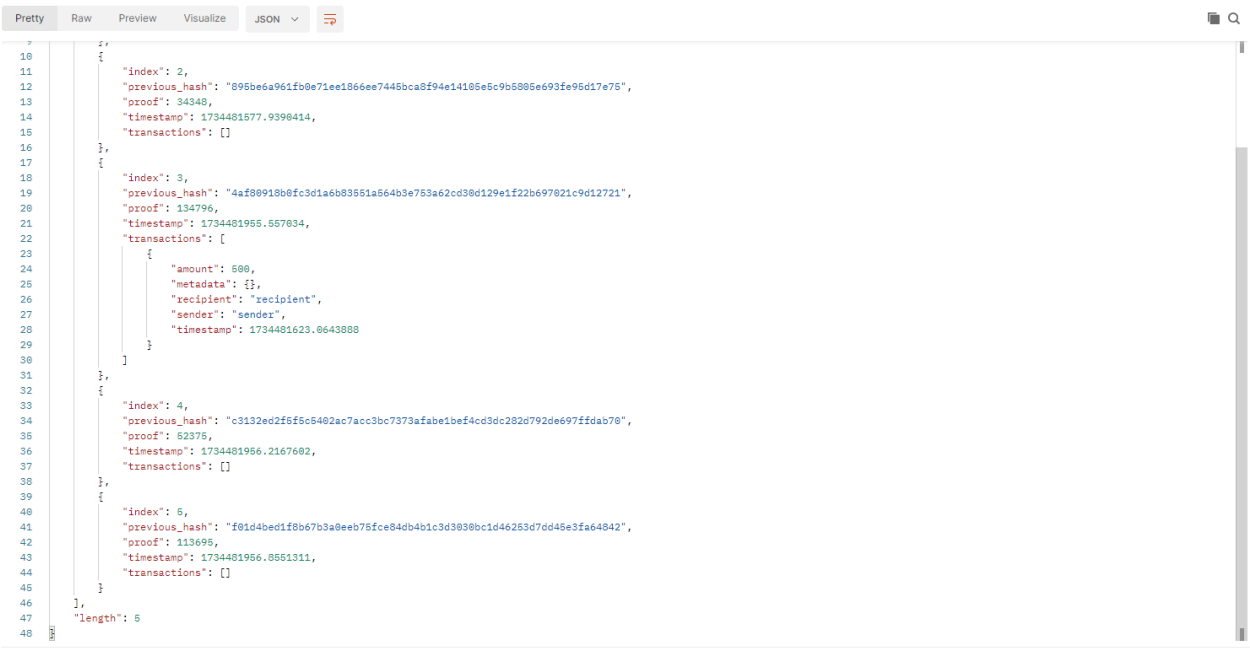

Рисунок 3.11 – Результат виконання запиту /get_chain після декількох дій

3.6 Напрямки подальших досліджень

Подальші дослідження у сфері використання блокчейн-технологій для підвищення безпеки та прозорості розподілених систем відкривають широкий спектр можливостей для вдосконалення існуючих рішень і створення нових підходів. Центральним напрямком досліджень є оптимізація алгоритмів консенсусу, оскільки поточні механізми, такі як Proof-of-Work, мають значні обмеження, включаючи високі енергетичні витрати та обмежену пропускну здатність. Вивчення альтернативних підходів, таких як Proof-of-Stake, Delegated Proof-of-Stake, Practical Byzantine Fault Tolerance та їх гібридних варіантів, може забезпечити суттєве підвищення ефективності і масштабованості систем. Зокрема, одним із пріоритетів є розробка механізмів, здатних забезпечувати високу швидкість обробки транзакцій за умови збереження децентралізованого характеру мережі та стійкості до атак.

Смарт-контракти дозволяють автоматизувати виконання умов угод між сторонами, що відкриває нові горизонти для застосування блокчейну в таких

галузях, як фінанси, логістика, охорона здоров’я та управління ланцюгами постачання. Подальші дослідження в цій галузі можуть включати створення універсальних стандартів для розробки та впровадження смарт-контрактів, що забезпечить їхню сумісність між різними блокчейн-платформами. Також варто звернути увагу на підвищення безпеки смарт-контрактів, оскільки помилки у їхньому коді можуть мати катастрофічні наслідки, зокрема втрату значних обсягів коштів або компрометацію даних.

Значний інтерес викликає також використання блокчейн-технологій для управління цифровою ідентичністю. У цьому контексті дослідження можуть бути спрямовані на розробку рішень, які дозволяють користувачам зберігати і контролювати свої персональні дані без залучення центральних організацій. Це може включати створення децентралізованих платформ для аутентифікації, які гарантують конфіденційність і дозволяють користувачам ділитися лише необхідною інформацією для виконання конкретних операцій. Такий підхід може стати основою для реалізації концепції самоспрямованої ідентичності, яка дозволить зменшити ризики шахрайства та несанкціонованого доступу до даних.

Окремою темою досліджень є інтеграція блокчейну з Інтернетом речей (IoT). Блокчейн може забезпечити високий рівень безпеки та прозорості для розподілених IoT-систем, дозволяючи ефективно управляти мільярдами пристроїв і забезпечуючи їхню взаємодію. Основною метою таких досліджень є створення масштабованих архітектур, які дозволяють зберігати і обробляти великі обсяги даних, що генеруються IoT-пристроями, без перевантаження мережі та збереження високої швидкості обміну інформацією. Крім того, дослідження в цьому напрямку можуть включати розробку спеціалізованих алгоритмів консенсусу, які враховують обмежені обчислювальні ресурси IoT-пристроїв і забезпечують їхню енергоефективність.

Дослідження можуть бути спрямовані на створення систем, які дозволяють зберігати дані про державні контракти, голосування, реєстрацію

майна та інші адміністративні процеси у децентралізованій і незмінній формі. Це дозволить знизити рівень корупції та підвищити довіру громадян до державних інституцій. У цьому контексті особливу увагу слід приділити питанням масштабованості та інтеграції таких систем з існуючими державними базами даних, а також розробці механізмів захисту конфіденційної інформації.

Крім того, перспективним напрямком є застосування блокчейну в медицині, зокрема для зберігання і управління електронними медичними записами. Блокчейн може забезпечити конфіденційність і цілісність медичних даних, дозволяючи пацієнтам контролювати доступ до своєї інформації. Дослідження можуть бути спрямовані на створення платформ, які дозволяють обмінюватися даними між різними медичними установами, зберігаючи при цьому їхню безпеку. Також слід враховувати можливість інтеграції таких платформ із системами штучного інтелекту для аналізу медичних даних і покращення діагностики та лікування.

Зростання популярності блокчейну призводить до значного збільшення обчислювальних потужностей, необхідних для підтримки його роботи, що, у свою чергу, має негативний вплив на довкілля. Розробка нових підходів, таких як алгоритми консенсусу з низьким споживанням енергії або використання відновлюваних джерел енергії для майнінгу, є надзвичайно актуальною. Крім того, дослідження можуть включати аналіз можливостей оптимізації існуючих інфраструктур, що дозволить знизити витрати на обчислення і підвищити ефективність роботи системи.

Окремою темою є дослідження у сфері конфіденційності даних у блокчейні. Незважаючи на те, що блокчейн забезпечує високий рівень захисту від підробки даних, інформація, що зберігається у публічному блокчейні, є доступною для всіх учасників мережі. Це може створювати ризики для конфіденційності, особливо якщо йдеться про чутливі дані. Подальші дослідження можуть бути спрямовані на розробку технологій, які дозволяють

зберігати дані у зашифрованому вигляді або використовувати методи вибіркового розкриття інформації. Це може включати впровадження технологій zero-knowledge proof, що дозволяють підтверджувати істинність певної інформації без її розкриття. У рамках подальших досліджень слід також розглянути питання інтероперабельності між різними блокчейн-платформами. Сучасний ринок блокчейн-технологій є дуже фрагментованим, і більшість платформ працюють ізольовано одна від одної. Це створює бар'єри для впровадження блокчейну у масштабних проєктах, які потребують взаємодії між різними системами. Розробка стандартів для обміну даними між блокчейн-платформами і створення протоколів інтероперабельності є важливим напрямком, що сприятиме розвитку технології в цілому.

Загалом, подальші дослідження у сфері блокчейн-технологій мають значний потенціал для трансформації багатьох галузей. Їхній успішний розвиток вимагатиме тісної співпраці між науковою спільнотою, бізнесом та урядами, що дозволить не лише подолати існуючі обмеження, але й відкрити нові горизонти для використання блокчейну у глобальному масштабі.

3.7 Висновки до третього розділу

Висновки до третього розділу доцільно сформувати наступним чином:

1) постановка задачі спрямована на формулювання ключових цілей створення програмного забезпечення, таких як забезпечення децентралізованості, прозорості, безпеки та масштабованості. Особливий акцент зроблено на оптимізації існуючих блокчейн-рішень і врахуванні вимог до інтеграції у різних сферах. Архітектура блокчейну докладно описує технічну будову системи, включаючи механізми управління транзакціями, створення нових блоків та забезпечення їхньої послідовності. Описано взаємодію вузлів у мережі, перевірку валідності даних та механізми консенсусу, які є основою для функціонування розподіленої системи;

2) використані технології охоплюють як програмні інструменти, так і алгоритми, що застосовуються для забезпечення роботи системи. Детально пояснено вибір мов програмування, бібліотек, хеш-функцій, а також архітектурних підходів, які забезпечують безпеку, ефективність та масштабованість;

3) схема роботи демонструє, як система функціонує в умовах реального використання. Розглянуто сценарії створення транзакцій, синхронізації даних між вузлами, пошуку консенсусу і роботи мережі під навантаженням;

4) тестування є невід'ємною частиною процесу розробки, що забезпечує перевірку коректності роботи програмного забезпечення, виявлення та усунення помилок. Описані методи тестування дозволяють оцінити стабільність і надійність системи у різних сценаріях використання;

5) напрямки подальших досліджень включають аналіз можливостей удосконалення технологій, зокрема оптимізацію енергоспоживання, інтеграцію смарт-контрактів, покращення конфіденційності даних, розвиток інтероперабельності та адаптацію до специфічних галузевих потреб. У цьому контексті визначено перспективи впровадження блокчейну в нових сферах, таких як медицина, Інтернет речей та державне управління.

Загалом, поточний розділ формує цілісне уявлення про технічні аспекти розробки блокчейн-системи, її ключові функціональні особливості, а також можливості для подальшого вдосконалення і адаптації до сучасних викликів.

ВИСНОВКИ

Технологія блокчейн продемонструвала себе як одна з найбільш інноваційних і перспективних розробок сучасності, яка відкриває нові горизонти у сфері захисту даних, прозорості та ефективності функціонування розподілених систем. Основні принципи роботи блокчейну – децентралізація, криптографічний захист і механізми консенсусу – дозволяють створювати системи, які забезпечують не лише високу безпеку зберігання й обробки даних, але й довіру між усіма учасниками, усуваючи потребу в централізованому посереднику. Ця властивість має особливе значення в сучасному світі, де кіберзагрози та загроза маніпуляцій інформацією постійно зростають.

Дослідження підтверджує, що блокчейн може бути ефективно інтегрований у найрізноманітніші галузі, від фінансових послуг до медицини, логістики, державного управління, голосування та управління ланцюгами постачання. Завдяки властивостям незмінності й прозорості блокчейн дозволяє зменшити ризики шахрайства, забезпечити повний контроль над транзакціями та створити середовище, де дані можуть бути легко перевірені, але водночас залишаються захищеними від несанкціонованого доступу. У фінансовому секторі це дозволяє не лише підвищити ефективність, але й знизити витрати за рахунок усунення посередників. У медицині блокчейн може гарантувати конфіденційність медичних даних, а в логістиці – забезпечити повний контроль і відстеження товарів.

Однак розвиток блокчейн-технології не позбавлений викликів. Серед найбільш значущих проблем можна виділити високе енергоспоживання традиційних механізмів консенсусу, таких як Proof of Work, яке є значним обмеженням для масового впровадження. Також масштабованість залишається серйозним бар’єром, адже зі зростанням кількості учасників і транзакцій навантаження на систему зростає, що впливає на швидкість і

ефективність її роботи. Крім того, ризик централізації у деяких алгоритмах консенсусу, таких як Proof of Stake, викликає занепокоєння щодо рівності можливостей для учасників мережі. Регуляторні та юридичні аспекти використання блокчейну також потребують ретельного опрацювання, адже впровадження технології часто стикається з бар'єрами через нерозвиненість правової бази.

У контексті розподілених систем блокчейн виступає ключовим інструментом для забезпечення захисту від атак і підвищення довіри між учасниками. Його здатність автоматизувати процеси за допомогою смарт-контрактів та надавати прозорість без необхідності у централізованому управлінні створює фундамент для створення інноваційних моделей взаємодії. Дослідження показало, що впровадження блокчейн у розподілені системи значно зменшує ризики маніпуляцій і зловживань, одночасно підвищуючи надійність і зменшуючи вартість управління даними.

Загалом, блокчейн має величезний потенціал, щоб стати основою для багатьох галузей у майбутньому. Його універсальність і можливість адаптації під різноманітні потреби робить цю технологію незамінною для вирішення сучасних викликів у сфері безпеки, прозорості та ефективності. Проте для повного розкриття цього потенціалу необхідні подальші наукові дослідження, вдосконалення алгоритмів консенсусу, розвиток енергоефективних рішень та інтеграція з існуючими технологіями. У найближчі роки блокчейн може не лише змінити звичний підхід до роботи з даними, але й сприяти створенню більш справедливого, безпечного й прозорого цифрового світу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. K. Kaur and R. Jaswal, “Exploring the Potential of Blockchain Technology in Enhancing Security of smart systems”, in *2023 3rd Int. Conf. Advance Comput. Innovative Technol. Eng. (ICACITE)*, Greater Noida, India, May 12–13, 2023. IEEE, 2023. https://doi.org/10.1109/icacite57410.2023.10182571

2. S. E. Bellal, S. El Islam Bousiouda, and A. Dekhinet, “Blockchain and Supply Chain in Algeria: Enhancing Transparency and Security of Operations”, in *2023 Int. Conf. Decis. Aid Sci. Appl. (DASA)*, Annaba, Algeria, Sep. 16–17, 2023. IEEE, 2023. https://doi.org/10.1109/dasa59624.2023.10286589

3. Inayatulloh, “Adoption of Blockchain Technology for Digital Heritage to Improve Heritage Security”, in *2024 4th Int. Conf. Sci. Inf. Technol. Smart Admin. (ICSINTESA)*, Balikpapan, Indonesia, Jul. 12, 2024. IEEE, 2024, pp. 56–60. https://doi.org/10.1109/icsintesa62455.2024.10748154

4. R. M. Bommi, B. Sundarambal, C. Karthikeyini, and S. Subramanian, “Enhancing Security and Transparency Through the Integration of Blockchain and Machine Learning”, in *2023 Int. Conf. Data Sci., Agents Artif. Intell. (ICDSAAI)*, Chennai, India, Dec. 21–23, 2023. IEEE, 2023. https://doi.org/10.1109/icdsaai59313.2023.10452600

5. J. W. Heo, G. Ramachandran, and R. Jurdak, “Decentralised Redactable Blockchain: A Privacy-Preserving Approach to Addressing Identity Tracing Challenges”, in *2024 IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, Dublin, Ireland, May 27–31, 2024. IEEE, 2024, pp. 215–219. https://doi.org/10.1109/icbc59979.2024.10634438

6. R. Bala and R. Manoharan, “Blockchain based Secure and Effective Authentication Mechanism for 5G Networks”, in *2022 IEEE Int. Conf. Blockchain Distrib. Syst. Secur. (ICBDS)*, Pune, India, Sep. 16–18, 2022. IEEE, 2022. https://doi.org/10.1109/icbds53701.2022.9936018

7. N. Zhang, N. Zhao, and Y. Qu, “Research on the Integration System of Ubiquitous Power Internet of Things Based on Blockchain Technology”, in *2020 Int. Conf. Robots Intell. System (ICRIS)*, Sanya, China, Nov. 7–8, 2020. IEEE, 2020. https://doi.org/10.1109/icris52159.2020.00094

8. A. Kumar, K. Guleria, I. Sharma, and A. Khan, “Multichain Blockchain Solutions for Ensuring Trust and Transparency in IoT Healthcare Environment”, in *2024 7th Int. Conf. Circuit Power Comput. Technol. (ICCPCT)*, Kollam, India, Aug. 8–9, 2024. IEEE, 2024, pp. 1314–1318. https://doi.org/10.1109/iccpct61902.2024.10672895

9. Y. Jiang, P. Xu, X. Kuang, B. Zhou, P. Xie, and Y. Zhang, “A Design of Electricity Trading System Based on Blockchain Technology”, in *2021 IEEE Int. Conf. Energy Internet (ICEI)*, Southampton, United Kingdom, Sep. 27–29, 2021. IEEE, 2021. https://doi.org/10.1109/icei52466.2021.00036

10. X. Thipphonexai and Y. Guanghui, “Research on analysis and design of cloud ERP based on blockchain technology”, in *2020 Int. Conf. Virtual Reality Intell. Syst. (ICVRIS)*, Zhangjiajie, China, Jul. 18–19, 2020. IEEE, 2020. https://doi.org/10.1109/icvris51417.2020.00198

11. J. Chen, X. Gui, L. Chen, and T. He, “Distributed Energy Trading Model based on Graphene Blockchain”, in *2020 Asia Energy Elect. Eng. Symp. (AEEES)*, Chengdu, China, May 29–31, 2020. IEEE, 2020. https://doi.org/10.1109/aeees48850.2020.9121399

12. K. T. Vo, T. Nguyen, T.-T. Ta, T.-A. Nguyen-Hoang, and N.-T. Dinh, “Student Management Model Integrating E-Commerce Based on Blockchain Technology”, in *2023 15th Int. Conf. Comput. Automat. Eng. (ICCAE)*, Sydney, Australia, Mar. 3–5, 2023. IEEE, 2023. https://doi.org/10.1109/iccae56788.2023.10111175

13. S. Al-Maaitah, M. Qatawneh, and A. Quzmar, “E-Voting System Based on Blockchain Technology: A Survey”, in *2021 Int. Conf. Inf. Technol.*

(ICIT), Amman, Jordan, Jul. 14–15, 2021. IEEE, 2021. https://doi.org/10.1109/icit52682.2021.9491734

14. H. Abbas, M. Hussain, S. Zahid, and R. H. Ahmed, “Enhancing Food Security: A Blockchain-Enabled Traceability Framework to Mitigate Stockpiling of Food Commodities”, in *2023 Int. Conf. IT Ind. Technol. (ICIT)*, Chiniot, Pakistan, Oct. 9–10, 2023. IEEE, 2023. https://doi.org/10.1109/icit59216.2023.10335828

15. A. A. P. Abidin, A. Alamsyah, and H. Irawan, “Blockchain for Traceability and Security in Pharmaceutical Supply Chain”, in *2024 IEEE Int. Conf. Industry 4.0, Artif. Intell., Commun. Technol. (IAICT)*, BALI, Indonesia, Jul. 4–6, 2024. IEEE, 2024, pp. 235–240. https://doi.org/10.1109/iaict62357.2024.10617533

16. L. Junaid, K. Bilal, J. Shuja, A. O. Balogun, and J. J. P. C. Rodrigues, “Blockchain-Enabled Framework for Transparent Land Lease and Mortgage Management”, *IEEE Access*, p. 1, 2024. https://doi.org/10.1109/access.2024.3388248

17. L. Zhang and Y. Wang, “Application Research on Blockchain-based Asynchronous Federated Learning in Data Security Sharing in Vehicle Network”, in *2024 Int. Appl. Comput. Electromagn. Soc. Symp. (ACES-China)*, Xi'an, China, Aug. 16–19, 2024. IEEE, 2024, pp. 1–3. https://doi.org/10.1109/aces-china62474.2024.10699701

ДОДАТКИ

Додаток А

Лістинг програмного коду

```
import hashlib
import json
import time
import uuid
from flask import Flask, jsonify, request
from urllib.parse import urlparse
import requests

class Blockchain:
    def __init__(self):
        self.chain = []
        self.pending_transactions = []
        self.nodes = set()



        self.create_block(previous_hash='0', proof=100)



    def create_block(self, proof, previous_hash):
        block = {
            'index': len(self.chain) + 1,
            'timestamp': time.time(),
            'transactions': self.pending_transactions,
            'proof': proof,
```

```
        'previous_hash': previous_hash
    }
    self.pending_transactions = []
    self.chain.append(block)
    return block


def get_last_block(self):
    return self.chain[-1]


def add_transaction(self, sender, recipient, amount, metadata=None):
    transaction = {
        'sender': sender,
        'recipient': recipient,
        'amount': amount,
        'metadata': metadata or {},
        'timestamp': time.time()
    }
    self.pending_transactions.append(transaction)
    return self.get_last_block()['index'] + 1


@staticmethod
def hash_block(block):
    block_string = json.dumps(block, sort_keys=True).encode()
    return hashlib.sha256(block_string).hexdigest()
```

```
def proof_of_work(self, previous_proof):
    new_proof = 1
    check_proof = False
    while not check_proof:
        hash_operation = hashlib.sha256(
            str(new_proof**2 - previous_proof**2).encode()).hexdigest()
        if hash_operation[:4] == "0000":
            check_proof = True
        else:
            new_proof += 1
    return new_proof


def is_chain_valid(self, chain):
    previous_block = chain[0]
    index = 1
    while index < len(chain):
        block = chain[index]
        if block['previous_hash'] != self.hash_block(previous_block):
            return False
        proof = block['proof']
        previous_proof = previous_block['proof']
        hash_operation = hashlib.sha256(
            str(proof**2 - previous_proof**2).encode()).hexdigest()
        if hash_operation[:4] != "0000":
            return False
        previous_block = block
        index += 1
    return True
```

```
def register_node(self, address):
    parsed_url = urlparse(address)
    self.nodes.add(parsed_url.netloc)


def resolve_conflicts(self):
    neighbours = self.nodes
    new_chain = None

    max_length = len(self.chain)

    for node in neighbours:
        try:
            response = requests.get(f'http://{node}/get_chain')
            if response.status_code == 200:
                length = response.json()['length']
                chain = response.json()['chain']

                if length > max_length and self.is_chain_valid(chain):
                    max_length = length
                    new_chain = chain
        except requests.exceptions.RequestException:
            pass

    if new_chain:
        self.chain = new_chain
        return True
```

```
        return False


    def search_transactions(self, sender=None, recipient=None,
min_amount=None):
        results = []
        for block in self.chain:
            for transaction in block['transactions']:
                if (not sender or transaction['sender'] == sender) and \
                   (not recipient or transaction['recipient'] == recipient) and \
                   (not min_amount or transaction['amount'] >= min_amount):
                    results.append(transaction)
        return results

app = Flask(__name__)

blockchain = Blockchain()

@app.route('/mine_block', methods=['GET'])
def mine_block():
    previous_block = blockchain.get_last_block()
    previous_proof = previous_block['proof']
    proof = blockchain.proof_of_work(previous_proof)
    previous_hash = blockchain.hash_block(previous_block)
    block = blockchain.create_block(proof, previous_hash)
    response = {
        'message': 'Congratulations! You just mined a block!',
        'index': block['index'],
        'timestamp': block['timestamp'],
```

```
        'transactions': block['transactions'],
        'proof': block['proof'],
        'previous_hash': block['previous_hash']
    }
    return jsonify(response), 200

@app.route('/add_transaction', methods=['POST'])
def add_transaction():
    json_data = request.get_json()
    required_fields = ['sender', 'recipient', 'amount']
    if not all(key in json_data for key in required_fields):
        return 'Missing fields', 400
    index = blockchain.add_transaction(
        sender=json_data['sender'],
        recipient=json_data['recipient'],
        amount=json_data['amount'],
        metadata=json_data.get('metadata')
    )
    response = {'message': f'Transaction will be added to Block {index}'}
    return jsonify(response), 201

@app.route('/get_chain', methods=['GET'])
def get_chain():
    response = {
        'chain': blockchain.chain,
        'length': len(blockchain.chain)
    }
    return jsonify(response), 200
```

```
@app.route('/is_valid', methods=['GET'])
def is_valid():
    valid = blockchain.is_chain_valid(blockchain.chain)
    if valid:
        response = {'message': 'The Blockchain is valid.'}
    else:
        response = {'message': 'The Blockchain is NOT valid!'}
    return jsonify(response), 200

@app.route('/register_node', methods=['POST'])
def register_node():
    json_data = request.get_json()
    nodes = json_data.get('nodes')
    if nodes is None:
        return 'Error: Please supply a valid list of nodes', 400
    for node in nodes:
        blockchain.register_node(node)
    response = {
        'message': 'Nodes have been added',
        'total_nodes': list(blockchain.nodes)
    }
    return jsonify(response), 201

@app.route('/resolve_conflicts', methods=['GET'])
def resolve_conflicts():
    replaced = blockchain.resolve_conflicts()
    if replaced:
        response = {
            'message': 'Our chain was replaced',
```

```
            'new_chain': blockchain.chain
        }
    else:
        response = {
            'message': 'Our chain is authoritative',
            'chain': blockchain.chain
        }
    return jsonify(response), 200

@app.route('/search_transactions', methods=['POST'])
def search_transactions():
    json_data = request.get_json()
    sender = json_data.get('sender')
    recipient = json_data.get('recipient')
    min_amount = json_data.get('min_amount')
    transactions = blockchain.search_transactions(sender, recipient, min_amount)
    return jsonify({'transactions': transactions}), 200

if __name__ == '__main__':
    app.run(host='0.0.0.0', port=5000)
```