МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ КОМП'ЮТЕРНОЇ ТА ПРОГРАМНОЇ ІНЖЕНЕРІЇ
Кафедра комп'ютеризованих систем управління

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
Олександр ЛИТВЕНЕНКО

"_____" _____ 2022 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ЗДОБУВАЧА ОСВІТНЬОГО СТУПЕНЯ "МАГІСТР"

Тема: Засоби децентралізованого зберігання даних в технологіях *IoT*.

Виконавець: Ворона Владислав Богданович
Керівник: Вавіленкова Анастасія Ігорівна
Нормоконтролер: Вавіленкова Анастасія Ігорівна

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Київ 2022

Факультет кібербезпеки комп'ютерної та програмної інженерії

Кафедра комп'ютеризованих систем управління

Спеціальність 123 «Комп'ютерна інженерія»
(шифр, найменування)

Освітньо-професійна програма «Системне програмування»

ЗАТВЕРДЖУЮ
Завідувач кафедри
Олександр ЛИТВЕНЕНКО
«_____»_____ 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи
Ворони Владислава Богдановича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Засоби децентралізованого зберігання даних в технологіях *IoT*»

затверджена наказом ректора від «16» вересня 2022 р. № 1530/ст.

2. Термін виконання роботи: з 05.09.2022 р. по 30.11.2022 р.

3. Вхідні дані до роботи: технічна документація, тестові дані, програмні продукти, *Bitcoin Simulator, blockchain.info*

4. Зміст пояснювальної записки:

Розділ 1. Основні принципи технології блокчейн;

Розділ 2. Аналіз моделей децентралізованого зберігання та обробки даних;

Розділ 3. Моделювання архітектури інтеграції технології блокчейн та *IoT*.

5. Перелік обов'язкового графічного (ілюстрованого) матеріалу:

1) Моделі передавання даних в *IoT* мережах із блокчейном;

2) Модель управління поставками ліків;

3) Залежність кількості транзакцій на секунду від розміру блоків та інтервалу генерації;

4) Залежність відсотка застарілих блоків від мережевої затримки між вузлами та інтервалу генерації в логарифмічній шкалі;

5) Залежність відсотка застарілих блоків від кількості IoT пристроїв в логарифмічной шкалі.

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Постановка задачі та узгодження з керівником кваліфікаційної роботи.	05.09.2022	Виконано
2	Формування структури розділів кваліфікаційної роботи.	06.09.2022 – 09.09.2022	Виконано
3	Формування та оформлення першої частини кваліфікаційної роботи.	10.09.2022 – 25.09.2022	Виконано
4	Збір науково-технічного матеріалу до другої частини кваліфікаційної роботи. Написання другого розділу роботи.	26.09.2022 – 13.10.2022	Виконано
5	Проведення тестів практичної частини завдання для третього розділу.	14.10.2022 – 18.10.2022	Виконано
6	Формування та оформлення третьої частини кваліфікаційної роботи.	19.10.2022 – 26.10.2022	Виконано
7	Оформлення пояснювальної записки, підписання необхідних документів.	27.10.2022 – 03.11.2022	Виконано
8	Оформлення графічного матеріалу, підготовка до захисту роботи.	04.11.2022 – 10.11.2022	Виконано

7. Дата видачі завдання: «05» вересня 2022 р.

Керівник кваліфікаційної роботи _____ Вавіленкова Анастасія Ігорівна
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Ворона Владислав Богданович
(підпис здобувача освіти) (П.І.Б.)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Засоби децентралізованого зберігання даних в технологіях IoT»: сторінок 86, рисунки 24, таблиць 9, використаних джерел 30.

Об’єкт дослідження – процес симуляції IoT мережі з використанням технології блокчейн.

Мета роботи – проведення тестування для забезпечення подальшої конфіденційності та безпеки інформації на основі застосування розподіленого зберігання та обробки даних в системах IoT.

Предмет – сучасні системи розподіленого зберігання та обробки даних та способи передачі даних серед IoT мережі.

Методи дослідження – технології систем управління проектами, порівняльний аналіз, методи симуляції розподілених систем.

Практичне значення отриманих результатів – надання можливості захисту збереження даних клієнтів страхової компанії в банківській сфері.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

IoT (*internet of things*) – концепція мережі передавання даних між фізичними об'єктами, оснащеними вбудованими засобами і технологіями для взаємодії один з одним або із зовнішнім середовищем;

PoW (Proof-of-work) – система захисту систем від *DoS*-атак або зловживання послугами;

DoS (Denial of Service) – хакерська атака на обчислювальну систему з метою довести її до відмови, тобто створення таких умов, за яких сумлінні користувачі системи не зможуть отримати доступ до системних ресурсів, що надаються, або цей доступ буде утруднено;

PoS (Proof-of-Stake) – метод захисту в криптовалютах, за якого ймовірність формування учасником чергового блоку в блокчейні пропорційна частці, яку становлять належні цьому учаснику розрахункові одиниці цієї криптовалюти від їхньої загальної кількості;

AI (Artificial intelligence) – штучний інтелект.

ML (Machine learning) – машинне навчання.

P2P (Peer to Peer) – однорангова, децентралізована або пірингова мережа.

Вступ.

Актуальність. За багатьма оцінками алгоритми розподіленого зберігання й обробки даних - один із найперспективніших напрямів у сфері технологій (разом із машинним навчанням (*ML*), інтернетом речей (*IoT*) і штучним інтелектом (*AI*)), що може мати вплив на наше життя, який можна порівняти з розвитком Інтернету та мобільних пристроїв на початку 2000-х років. За оцінками Всесвітнього економічного форуму, до кінця 2027-го року вже 10% світового ВВП зберігатиметься в блокчейні.

Наразі розмір ринку розподіленого зберігання і обробки даних становить близько 230 млрд доларів, більшу частину якого займають фінансові операції.
Зниження витрат, підвищення рівня безпеки та вища прозорість транзакцій - три головні сильні сторони блокчейна. У зв'язку з потребою банків, бізнесу і суспільства в цих трьох аспектах, будь-яка теоретична робота або розробка в цій галузі стає досить актуальною.

Так само актуальність обґрунтована низькою вивченістю цього наукового напряму в Україні. Відкрито можливості для формування центру компетенцій у сфері децентралізованих технологій з метою подальшого їх застосування на корпоративному ринку і державних структурах у нашій країні.

Об’єкт дослідження – процес симуляції IoT мережі з використанням технології блокчейн.

Мета роботи – проведення тестування для забезпечення подальшої конфіденційності та безпеки інформації на основі застосування розподіленого зберігання та обробки даних в системах *IoT*.

Предмет – сучасні системи розподіленого зберігання та обробки даних та способи передачі даних серед *IoT* мережі.

Методи дослідження – технології систем управління проектами, порівняльний аналіз, методи симуляції розподілених систем.

Здійснено дослідження моделювання роботи мережі *IoT* з використанням технології блокчейн на основі *Proof of Wor*k консенсусу. Також був проведений

порівняльний аналіз різних конфігурацій мереж та налаштувань систем для отримання ефективних результатів роботи.

Новизна роботи полягає в пошуку нових сценаріїв використання технології в інших галузях з метою вдосконалення систем обміну інформацією, забезпечуючи такі властивості: прозорість, незворотність, анонімність, децентралізованість. Практична значущість роботи полягає в можливості використання результатів дослідження для задач, пов'язаних з адаптацією блокчейна до *IoT*.

Практичні значення отриманих результатів – просунення та популяризація технології блокчейн в повсякденне життя. Отримання ефективної конфігурації проектування мереж *IoT*.

Апробація отриманих результатів. Симуляція проводилась на основі вже існуючої технології зі збереженням особливостей побудови мереж та характеристик пристроїв-учасників, що надає можливі видворити змодельовані дані в реальному житті.

Прогнозні припущення про розвиток об’єкту та предмету дослідження – застосування напрацювань у створенні реальних мереж *IoT* з децентралізованим збереженням даних. Також технології зв’язку будуть розвиватися, становитися більш надійними, енергоефективними та доступнішими. Прикладом стає нові розробки *RadioDoge* з використанням *HF*/*LoRaWAN*.

Розділ 1. Основні принципи технології блокчейн.

1.1. Історія створення та основні принципи технології блокчейн.

Блокчейн являє собою децентралізований реєстр, який може надійно і безпечно зберігати інформацію, використовуючи криптографічне шифрування і хешування. Найранішу роботу, в якій згадується ідея блокчейна, було опубліковано Стюартом Хабером і В. Скотт Сторнеттом у 1991 році [1]. Ця робота присвячена технології, яка перевіряє позначки часу (історію змін) на документах. Дослідники дійшли висновку, що "у документ може бути додана інформація про позначки часу (історію змін) для підвищення автентичності документів". Це клас документів, для яких зміни в майбутньому непередбачувані. У 1992 році до концепту технології додали використання хеш-дерев, що зробило архітектуру ефективнішою, даючи змогу збирати кілька документів в один блок, що стане особливо важливим за 16 років при створенні технологій децентралізованого зберігання й опрацювання даних.

Сучасний блокчейн був описаний Сатоші Накамото у 2008 році. Метою блокчейна, за словами Накамото, було розміщення публічного розподіленого реєстру (*ledger*) на блокчейні для криптовалюти *Bitcoin* [2]. Ідеєю всього проєкту було створення децентралізованої цифрової валюти, яка вирішувала б проблему подвійних витрат. Подвійні витрати - це недолік технології цифрової готівки (*digital cash*), за якої сторона може витратити один і той самий цифровий ресурс більш ніж один раз, що призводить до інфляції, отже, для регулювання подвійних витрат необхідна третя сторона, в якій немає необхідності за використання технології блокчейн. Після запуску біткойна і технології блокчейна, на якій він базувався, було помітно величезне зростання користувачів криптовалюти в період із 2014 до 2017 року; розмір блокчейна зріс із приблизно із 20 ГБ у 2014 році до майже 100 ГБ у 2017 році. Під час цього успіху багато компаній слідували тим самим принципам і випустили на ринок додатки, що використовують технологію блокчейна в найрізноманітніших сферах. Блокчейн *Ethereum* - один із найвідоміших прикладів.

За визначенням *CoinTelegraph*, "смартконтакт" – це "спеціальний протокол, призначений для сприяння, перевірки або реалізації переговорів чи виконання контракту. Смартконтракти дають змогу здійснювати довірчі транзакції без участі третіх осіб". Блокчейни навіть почали використовуватися для забезпечення юридичних процесів під час передачі нерухомості.

Відомі різні визначення технології блокчейн. Дон і Алекс Тапскотт з "*Blockchain Revolution*" визначають блокчейн як "непідкупний цифровий реєстр транзакцій, який можна запрограмувати для запису не тільки фінансових транзакцій, а й практично всього цінного" [3]. З точки зору бізнесу блокчейн можна розглядати як розподілений реєстр, де учасники обмінюються активами, виконуючи транзакції, які зберігаються в реєстрі. Відсутня необхідність у центральній точці для обробки, перевірки, захисту або навіть зберігання даних. Замість цього дані зберігаються у всіх учасників мережі.

Розподілений реєстр (розподілений регістр, книга записів, *distibuted ledger*) – це синонім слова "блокчейн". Реєстр зберігається й обробляється на кількох комп'ютерах або вузлах, що працюють незалежно один від одного. Перед тим як дані можуть бути додані або змінені, між вузлами має бути досягнутий консенсус. Блокчейн не дозволяє легко змінити (тобто підробити) дані, що зберігаються всередині нього, що робить блокчейн корисною технологією для конфіденційних даних.

Блоки, що складають блокчейн, містять кілька фрагментів важливої інформації, а саме: дані певного типу, хеш поточного блоку, хеш попереднього блоку та іноді часову мітку (рис. 1.1). Дані, що зберігаються всередині блоку, сильно залежать від типу блокчейна. Як дані можуть бути будь-які дані: медичні записи, податкова інформація, деталі контракту тощо.

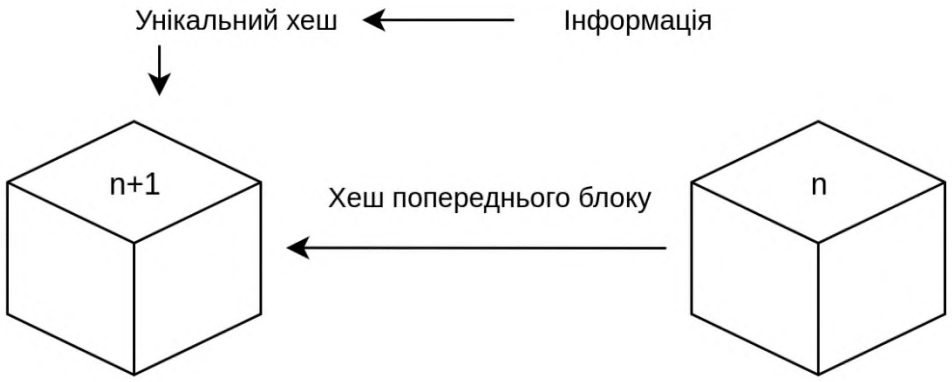

Рис. 1.1. Візуалізація блоків у блокчейні.

Хеш блоку можна порівняти з цифровим відбитком пристрою (*fingerprint*), він завжди унікальний і розраховується під час створення блоку. Якщо в блок буде внесено зміну після обчислення хешу, весь хеш зміниться для цього блоку. Це дуже хороший спосіб виявити зміни в даних після того, як блок було додано в блокчейн, тому що, як тільки дані змінюються, то хеш змінюється, навіть якщо змінити лише всього один біт у даних. Така ж логіка використовується з хешем попереднього блоку. Усі блоки в блокчейні міститимуть хеші самого блоку плюс хеш його попереднього блоку. Оскільки перший блок у блокчейні не може містити хеші з попередніх блоків, значення зазвичай становить лише нулі та називається блоком генезису. Хеш блоку генезису буде, тим не менш, міститися в наступному блоці. Цей блок, у свою чергу,обчислюватиме свій власний хеш, який буде зчитаний третім блоком, щоб визначити його власний хеш тощо, рис. 1.2.

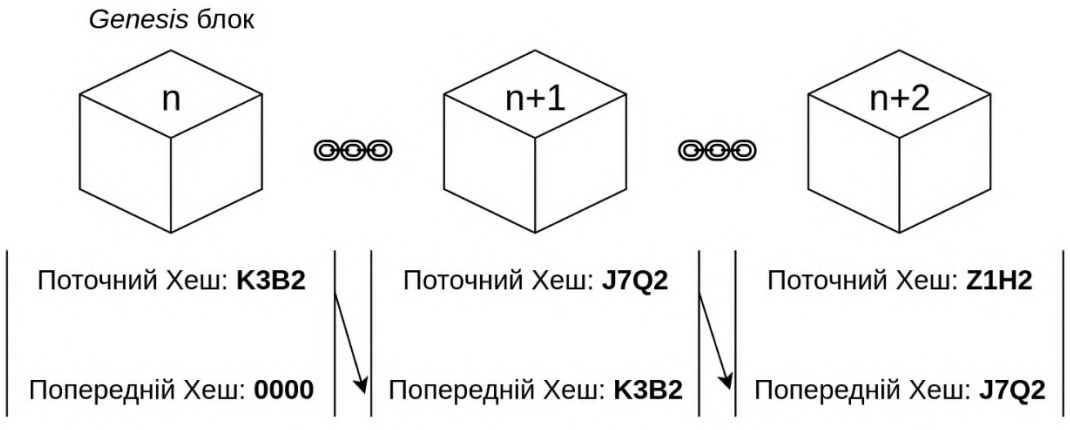

Рис. 1.2. Вплив хешу попереднього блоку на весь ланцюжок.

Якщо хеш у блоці зміниться, ланцюжок буде розірвано, і всі наступні блоки повинні будуть також перерахувати свої хеші, рис. 1.3. Оскільки заголовок кожного блоку містить частину або корінь хеш-дерева (*Merkle tree*), зміна даних у блоці 2 зробить корінь хеш-дерева в заголовку блоку 3 недійсним. Якщо заголовок блоку 3 зміниться, зміниться і заголовок блоку 4, і так далі. Це створює ланцюжок блоків, основу якого становить технологія блокчейна.

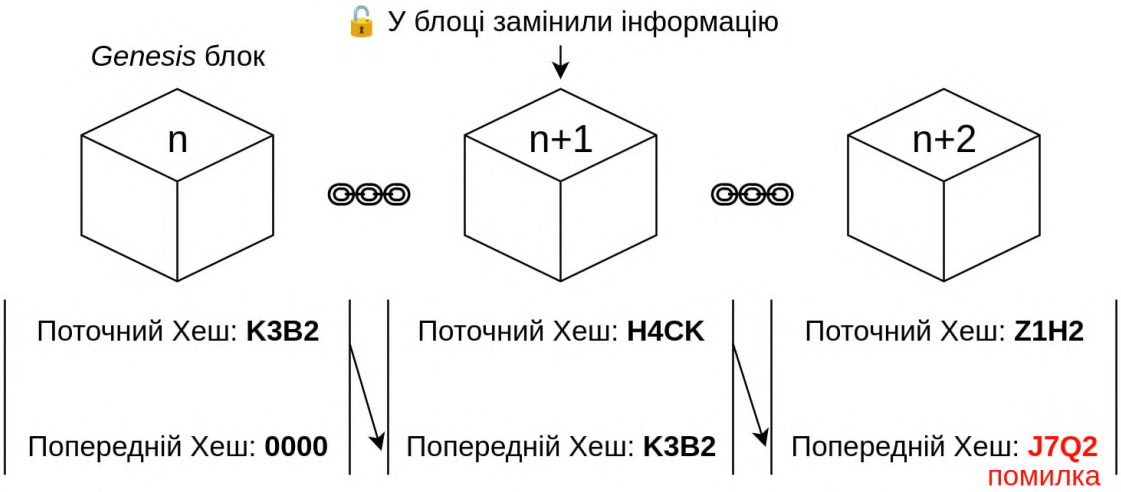

Рис. 1.3. Захищеність блоків.

Кожен новий блок, що містить транзакції, має пройти процес перевірки для знаходження консенсусу про те, що блок є правильним блоком, а вже потім блок може бути доданий у ланцюжок. Цей процес дає змогу блокчейну зростати, рис. 1.4.

Блокчейн не обробляється центральним комп'ютером. Замість цього блокчейн управляється одноранговою мережею (*P2P, peer-to-peer*). Технологія дає змогу кожному учаснику обмінюватися даними з будь-ким у мережі, без необхідності залучення стороннього посередника.

Рис. 1.4. Покроковий процес створення блоку.

Існують різні підходи, які дають змогу мережі узгоджувати оновлення даних усього блокчейна. Внутрішня узгодженість підтримується завдяки тому, що всі користувачі досягають консенсусу щодо поточного стану мережі. Таким чином, різні копії одного блокчейна не існують. Вузли перевіряють транзакції, гарантуючи, що це правильна інформація, і потім додають їх у блок. Потім мережа погоджується (досягає консенсусу) щодо того, який блок має бути доданий у ланцюжок. Механізм консенсусу, який залежить від алгоритмічного дизайну блокчейна, забезпечує дотримання правил. У загальнодоступному (інклюзивному) блокчейні (*permissionless blockchain*) усі вузли можуть пропонувати доповнення до блокчейну, однак у приватному (ексклюзивному) блокчейні (*permissioned blockchain*), лише певні вузли можуть пропонувати зміни. Процес перевірки дає змогу здійснювати однорангові транзакції, оскільки для перевірки достовірності транзакцій посередник не потрібен.

Алгоритм цифрового відбитка пристрою (тобто криптографічний хеш) використовується для створення унікального коду, який вказує на вихідний файл. Прикладом криптографічної хеш-функції є "*SHA256*". Ця функція використовує двійковий код і обчислює новий хеш. Хеш складається з 32 цифр або букв. Хеш-функція не оборотна, отже, ніхто не може знати, що знаходиться в цифровому файлі, просто прочитавши хеш. Кожен користувач блокчейна має відкритий ключ і закритий ключ. Закритий ключ використовується для підписання транзакцій, а

відкритий ключ використовується для ідентифікації користувачів у системі. Відкритий ключ вказує на дані користувача, тоді як відповідний закритий ключ необхідний для роботи з цими даними. Отже, якщо користувач контролює як закритий, так і відкритий ключ, у нього є підтвердження права власності. Кожна транзакція в блокчейні підписується цифровим підписом, для цього використовується "криптографія з відкритим ключем". Відправник може використовувати закритий ключ для шифрування хешу (званого цифровим підписом), який може поширюватися всією мережею. Відкритий ключ відправника може потім використовуватися одержувачем для підтвердження того, що транзакція була підписана за допомогою закритого ключа відправника [4].

Коли в системі є велика кількість хешів, може бути важко керувати розміром блокчейна. Хеш-дерево -- це хеш, що складається з декількох хешів, структура дерева складається з хешів, які об'єднані на різних рівнях. Кожна комбінація хешів створює новий унікальний хеш. Нарешті, значення хеша, що складається з двох останніх хешів, є коренем хеш-дерева, рис. 1.5. Щоб переконатися, що в певному блоці відбулася певна транзакція, достатньо використовувати тільки заголовки блоків і корінь хеш-дерева в заголовках блоків.

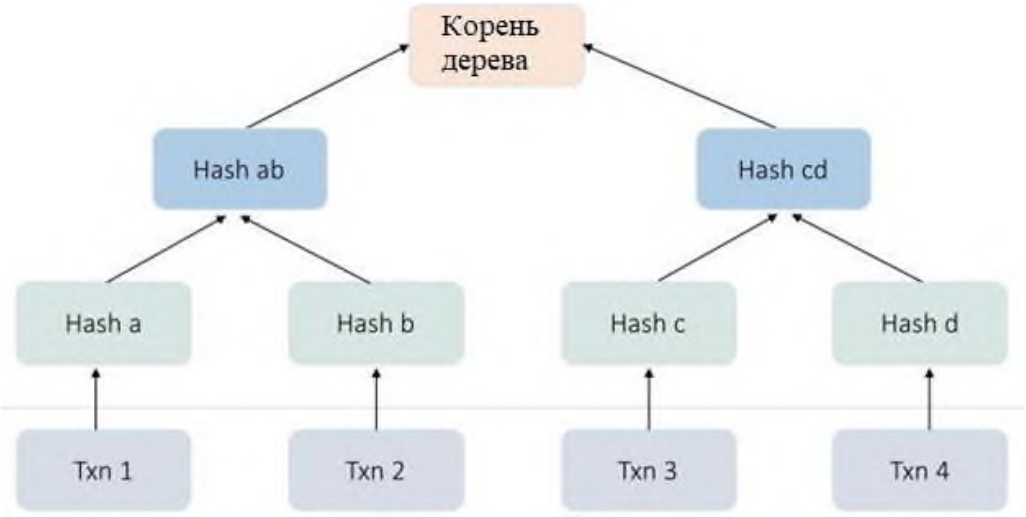

Рис. 1.5. Хеш-дерево.

1.2. Основні переваги та обмеження блокчейну.

Блокчейн є технологією, що розвивається, де все ще залишається багато роботи для вдосконалення та подальших досліджень. Проте проаналізувавши ключові характеристики технології блокчейну, які відображені на рисунку 1.6 [5]. Технологія блокчейна забезпечує багато переваг порівняно з наявними. Дві її основні характеристики: довіра та децентралізація. Розглянемо основні переваги технології розподіленого зберігання та обробки інформації.

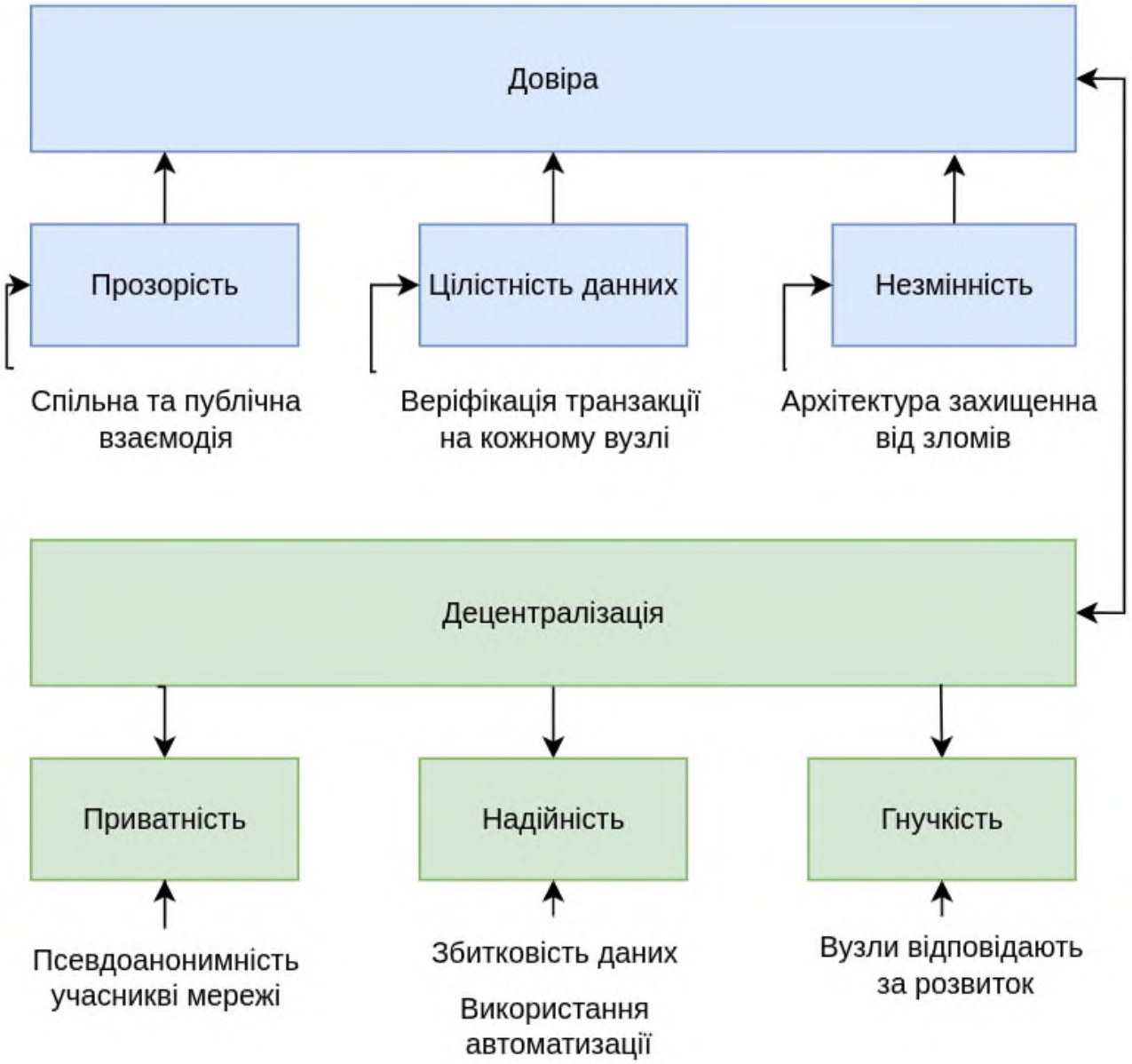

Рис. 1.6. Переваги технології блокчейн.

У технології блокчейн конфіденційність учасників - це перевага і проблема технології одночасно. З одного боку, особистості учасників зберігаються анонімно [5], що забезпечує високий ступінь конфіденційності. Крім того, всі взаємодії між мережевими вузлами захищені криптографією з відкритим ключем. З іншого боку, варто брати до уваги, що в наявних системах деталі транзакцій зберігаються і управляються третіми особами.

Механізми блокчейна гарантують надійність і відмовостійкість завдяки тому, що транзакції не додаються до розподіленого реєстру, доки вони не перевірені та не підтверджені. Після підтвердження транзакція реплікується мережею через механізми децентралізованого зберігання блокчейна, тож дані стають довговічними та стійкими до втрати [6]. Не існує єдиної точки відмови або єдиної точки контролю над даними.

Технологія блокчейна забезпечує прозорість для всіх людей у мережі, оскільки транзакції видимі для всіх підключених користувачів без контролю з боку третіх осіб. Таким чином, система на основі блокчейна пропонує поліпшення в прозорості передачі даних порівняно з наявними централізованими системами зберігання даних. Оскільки зміни видно всім у мережі, і транзакції не можуть бути змінені або видалені після запису в блокчейне [5].

Цілісність даних досягається за допомогою криптографії, яка є частиною механізму консенсусу. Щоб досягти консенсусу, мережа блокчейна використовує різні механізми. Наприклад, алгоритми доказу роботи (*PoW*) гарантують, що зміна будь-якої одиниці інформації в блокчейні означатиме використання величезної кількості обчислювальної потужності для змін у всій мережі.

Ще однією перевагою є універсальність. Концепція блокчейн уперше виникла із застосуванням біткойнів, проте технологія може бути застосована як розподілений реєстр для будь-яких типів транзакцій, не лише для цифрової валюти. Наприклад, багато авторів та експертів вважають, що ця технологія має великий вплив на енергетичний сектор, постачання та логістику, музичну індустрію, охорону здоров'я тощо.

Незмінність даних означає, що ніхто не може повернутися і переписати історію. Таким чином, після додавання транзакції в блок, який, у свою чергу, додається в блокчейн, цю транзакцію не можна змінити. Цей ступінь незмінності зростає зі збільшенням кількості транзакцій, що здійснюються поверх блоку, який містить транзакцію [4].

Головна перевага блокчейна полягає в тому, що він підтримує ідею відкритого, загальнодоступного і надійного сховища даних. Таким чином, блокчейн надав перше рішення проблеми встановлення довіри в небезпечному середовищі, не покладаючись на третіх осіб. Це відома проблема в розподілених обчисленнях, також відома як проблема візантійських генералів. Її суть полягає в тому, щоб спробувати узгодити хід дій або стан системи шляхом обміну інформацією через ненадійну і потенційно скомпрометовану мережу.

Характер проблем, пов'язаних із технологією блокчейн, з технічного погляду, ґрунтуватиметься на систематичному огляді *Yli-Huumo* [7]. Це дослідження виявило рішення, надані для кожної виявленої проблеми, і вказало все ще не вирішені.
Розглянемо проблеми, пов'язані з безпекою:

— **атака на 51%:** механізми блокчейн розроблені з припущенням, що 51% вузлів контролюють мережу [7]. Якщо вузли зловмисника колективно контролюють велику обчислювальну потужність, мережа вразлива для так званої 51% атаки. Тим не менш, автори досліджень [8], показують, що, хоча блокчейн спроектований як повністю децентралізована (розподілена) мережа, коефіцієнт децентралізації біткойнів постійно збільшується з 2011 року (0,26) до 2014 року (0,33). Коефіцієнт централізації 0 означає суто децентралізований, а 1 - централізований біткойн. Більше того, є дослідження, які стверджують, що 50% контролю мережі недостатньо для забезпечення безпеки [7];

— **інциденти в галузі безпеки:** Зі зростанням використання криптовалюти, такої як Біткойн, як способу здійснення платежів і переказів, інциденти в галузі безпеки збільшилися і призводять до економічних втрат. Використовуються всі можливі типи зломів, включно з *DDoS*-атаками, зломом особистого облікового запису з використанням троянських програм або вірусів [7];

— **проблеми гнучкості даних (*transaction malleability*)**: цілісність даних є істотною проблемою в середовищі блокчейна, оскільки дані мають надсилатися всім сторонам у мережі для перевірки, тому важливо не змінювати їх. Проте є дослідження, які показують, як атаки на гнучкість відбуваються в блокчейні. Під час атаки на гнучкість зловмисник перехоплює, змінює і ретранслює транзакцію, змушуючи емітента транзакції вважати, що початкову транзакцію не було підтверджено;

— **проблеми аутентифікації та криптографії:** у блокчейні закритий ключ є основним елементом аутентифікації. Проте, були деякі інциденти з автентифікацією, як-от добре відомий випадок у *Mt.Gox*, коли компанію атакували, а особисті ключі їхніх клієнтів було вкрадено [7]. Для розв'язання цієї проблеми запропоновано різні рішення для посилення автентифікації в блокчейні.

Як згадувалося раніше, конфіденційність — це проблема і перевага децентралізованого зберігання, всі учасники можуть бачити всі транзакції, але без прив'язки транзакції до користувача. У зв'язку з проблемою конфіденційності існує безліч досліджень, що пропонують різні типи контрзаходів і моделей конфіденційності для підвищення анонімності в блокчейні [7].

Блокчейн стикається з багатьма регуляторними проблемами. Наприклад, проблема управління транснаціональними мережами та забезпечення дотримання законів, коли немає центрального посередника, який може нести юридичну відповідальність. Правові питання можуть виникати в галузях юрисдикції, відповідальності, інтелектуальної власності, конфіденційності даних, дотримання правил регулювання фінансових послуг та управління даними. Вузли блокчейна можуть бути розташовані в будь-якій точці світу. Отже, блокчейн може перетинати юрисдикційні кордони, що вимагає ретельного розгляду договірних відносин між країнами. Регулювання варіюється від країни до країни. Наприклад, навіть у ЄС можуть бути різні правила в різних країнах, особливо в енергетичному секторі. Тому важлива координація між регулюючими органами [10]. Наприклад, якщо термін дії контракту закінчується або припиняється, можливо, буде складно гарантувати, що всі дані клієнта будуть видалені. Однак існує кілька рішень цієї проблеми. Одним із

рішень є шифрування особистої інформації з використанням особистого ключа. Коли особистий ключ зникає, він більше не має доступу до інформації. Також можливо зберігати лише хеш транзакції в блокчейні, що дає змогу стерти транзакції та залишити лише слід у блокчейні. Є припущення, що блокчейн може допомогти організаціям досягти цілей регулювання. Наприклад, шляхом забезпечення більшої прозорості та спрощення нормативної звітності [10].

У технології блокчейн виникають такі проблеми, як стандартизація апаратних засобів, програмного забезпечення та наявність кваліфікованих фахівців. Масштабованість і швидкість транзакцій так само є проблемою. Існує компроміс між масштабом і швидкістю блокчейна. Загальнодоступні блокчейни часто мають обмежену швидкість транзакцій, але високу масштабованість, тоді як приватні блокчейни можуть мати вищу швидкість транзакцій, але їм не вистачає масштабу. Проблеми масштабованості можуть стати ще більш серйозною проблемою в майбутньому, особливо якщо в мережу блокчейн буде включено велику кількість *IoT*-пристроїв. Вони не можуть зберігати всі дані через обмеженість ресурсів зберігання та обчислювальних ресурсів.

1.3. Класифікація блокчейн-систем.

Існують різні типи блокчейнів, які можна класифікувати за ступенем їхньої відкритості та децентралізації, від абсолютно загальнодоступних блокчейнів до повністю приватних (ексклюзивних) блокчейнів.

Біткойн був першим публічним блокчейном, розробленим без вимог до контролю доступу [4]. Окремі організації почали розробляти як приватні, так і консорціумні (гібридні) блокчейни.

Відмінність між різними типами блокчейнів зумовлена тим, кому дозволено брати участь у мережі та вносити зміни до реєстру [11]. Точні характеристики залежать від базового протоколу блокчейна [4]. Коли і який тип блокчейна використовувати, залежить навіть від того, які атрибути мережі є найбільш важливими [9]. У таблиці 1.1 наведено зведені дані.

Таблиця 1.1. Порівняння різних типів блокчейн-систем.

	Приватний	**Гібридний**	**Публічний**
Управління	Одна організація	Кілька організацій	Спільнота
Механізм консенсусу	Алгоритм голосування Доказ влади (*Proof of Authority*) Висока довіра до валідаторів		Доказ роботи (*PoW*) Доказ частки володіння (*PoS*) Висока анонімність валідаторів
Ідентифікація користувачів	Особистості відомі		Анонімність, псевдоніми
Токен	Токен не має значення		Токен для оплати транзакцій і стимулювання валідаторів

Продовження таблиці 1.1.

	Приватний	**Гібридний**	**Публічний**
Переваги	Низьке енергоспоживання Швидка масштабованість Відсутність юридичних проблем		Незмінність даних Безпека даних Низькі експлуатаційні витрати Низькі експлуатаційні витрати для користувачів
Недоліки	Більш високі витрати на розробку (для певних додатків) Більш високі ризики безпеки даних		Більш низька конфіденційність даних Низька швидкість обробки даних і низька масштабованість Довгий процес розробки
Приклади	*MONAX, Multichain*	*Corda by R3, EnergyWeb Foundation, B3i*	*Bitcoin, Etherreum, Monero, Dash, Dogecoin, Litecoint*

Публічні блокчейни повністю відкриті. Кожен може приєднатися до мережі та брати участь у ній, оскільки попередній дозвіл на участь не потрібен. Публічні блокчейни функціонують без центральної точки, що виконує координуючу роль. Таким чином, відпадає необхідність сторін довіряти центральній організації [4]. В публічних блокчейнах довіру та координацію створюють економічні стимули і публічний блокчейн не потребує традиційних юридичних договорів. Немає обмежень на читання або запис для публічних блокчейнів, а ідентифікатори користувачів (вузлів) не розкриваються, використовуються псевдоніми. Публічні блокчейни безпечніші, ніж приватні через те, що в них складніше змінити інформацію. Однак публічні сховища часто довше обробляють дані й обслуговування таких систем дорожче, ніж приватні. Коли система загальнодоступна, вразливість системи зростає і швидкість блокчейна знижується.

Через велику кількість вузлів і попередніх блоків у публічному блокчейні ємність сховища також обмежена.

Приватні блокчейни являють собою закриту мережу з попередньо відомими учасниками [12]. Власник або адміністратор несе відповідальність за доступ до мережі та використовувані алгоритми розподіленого зберігання. У закритих мережах кількість учасників менша, ніж у публічних, що спрощує налаштування правил перевірки і дає змогу скасовувати транзакції. При використанні приватних блокчейнів можна скористатися перевагами блокчейнів, не відкриваючи систему для публіки. Проте вони можуть мати вищі ризики інформаційної безпеки, як і централізована система, оскільки транзакції перевіряються зсередини і не використовують високі обчислювальні ресурси. Приватні блокчейни часто використовують для управління базами даних [12].

Гібридний блокчейн — це щось середнє між публічним і приватним блокчейном у плані відкритості та децентралізації. Гібриди розроблені для того, щоб знайти правильний баланс безпеки, можливості аудиту і масштабованості додатків, які на них працюють. Гібридні підходи часто являють собою блокчейни консорціуму, де уповноважені учасники, які здійснюють перевірку і виконання транзакцій, є членами консорціуму [9]. Прикладом гібридного блокчейна (який є загальнодоступним) є *Ripple*. Усі учасники діють як валідатори, що робить його публічним блокчейном з погляду доступу, але не кожен може приєднатися та вносити зміни до мережі [4].

Гібридні сховища зазвичай не вимагають високої безпеки, яку забезпечують основні консенсусні алгоритми, такі як доказ роботи (*PoW*), оскільки членам довіряють за замовчуванням. Це є недоліком порівняно із загальнодоступними блокчейнами, тому що рішення про те, хто може приєднатися до мережі або, хто може передати дані до реєстру, зазвичай робиться централізованим способом [13]. Крім того, через нерівність користувачів у мережі, рішення про те, як досягти консенсусу в безпечний спосіб, є більш важким, особливо в умовах, коли одні користувачі мають значно більшу владу, ніж інші. Проте, юридичні та нормативні вимоги до проєктів блокчейну в багатьох галузях (наприклад, у сфері фінансів,

нерухомості, банківської справи), найімовірніше, вимагатимуть, щоб користувач був відомий у будь-якому разі, і тому блокчейни консорціуму в основному використовують інші протоколи, такі як *PBFT* замість *PoW* [13].

Підбиваючи підсумок, можна виділити два основні типи моделей проєктування, які визначено нижче, між ними - гібридний варіант, який також може бути створений на основі двох основних типів, залежно від контролю доступу: які операції і кому вони дозволені.

– **відкритий** (загальнодоступний, інклюзивний, без вимог прав доступу): блокчейн, у якому немає обмежень на читання даних блокчейна і надсилання транзакцій у сховище;

– **закритий** (приватний, ексклюзивний, з правами доступу): це блокчейн, у якому прямий доступ до даних блокчейна і надсилання транзакцій дозволено тільки для попередньо визначених користувачів (вузлів).

1.4. Методи досягнення консенсусу.

Залежно від типу блокчейн-системи використовуються різні алгоритми досягнення консенсусу. Мета алгоритму полягає в тому, щоб забезпечити існування єдиної історії транзакцій, і щоб ця історія не містила неприпустимих або суперечливих транзакцій. Наприклад, жоден обліковий запис не повинен витратити більше ресурсів, ніж містить, або двічі витрачати один і той самий ресурс (подвійні витрати).

Біткойн розв'язав проблему консенсусу в такий спосіб: для кожного нового блоку йде багаторазовий перерахунок із перебором різних варіацій параметра *nonce* (одноразово використовуване число), тобто блок буде прийнято, якщо хеш менший за певне значення, яке задає складність обчислення. Оскільки вихідні дані функції хешування розподілені рівномірно, неможливо створити блок таким чином, щоб було легко задовольнити умову. Між майнінговими комп'ютерами в мережі йде гонка за пошуком потрібного параметра *nonce*. Щойно мета досягається, комп'ютер майнінгу передає цей блок у мережу, й інші учасники перевіряють транзакції. Ця процедура називається доказом роботою (*PoW*). Оскільки мета полягає в тому, щоб не надавати занадто багато повноважень одній людині або організації, необхідно вибрати обмежений ресурс, який буде витрачено на перевірку блоку. У *PoW* цим ресурсом є обчислювальна потужність. Оскільки обчислювальна потужність стає дедалі дешевшою та доступнішою завдяки законам Мура та хмарним обчисленням, складність проблеми хешування регулюється залежно від того, як часто були вирішені попередні проблеми. Однак поширена критика *PoW* полягає в тому, що "втрата" обчислювальної потужності також означає великі втрати енергії. По суті, це означає, що майнери змушені об'єднувати ресурси в те, що в кінцевому підсумку може стати гігантськими біткойн-фермами, тим самим централізувавши децентралізовану мережу. Крім того, *PoW* не має дуже високої пропускної здатності транзакцій.

Недоліки *PoW* викликали інтерес до розроблення алгоритмів, які не потребують такого ж високого споживання електроенергії в процесі видобутку. *PoS*

замінює обчислювальну роботу в процесі майнінгу на частку володіння певною криптовалютою. Замість того щоб витрачати гроші на електроенергію та обладнання для майнінгу, валідатори можуть купувати криптовалюту і використовувати її, щоб брати участь у процесі виборів, щоб отримувати винагороди і підтримувати роботу мережі. Кількість валюти, поставленої на карту валідатором, відповідає ймовірності їхнього вибору як валідатора [14]. Однак алгоритми *PoS* вибирають валідатора за допомогою алгоритму рандомізації, щоб гарантувати, що жоден валідатор не може бути обраний заздалегідь. Безпека досягається не за рахунок споживання електроенергії, а за рахунок підвищення економічної цінності у вигляді частки в криптовалюті, яка може бути втрачена, якщо валідатор діятиме нечесно. Таким чином, *PoS* більш сфокусований на штрафи порівняно з *PoW*, який заснований на нагородах для забезпечення безпеки [15].

Round Robin (циклічний перебір) – це алгоритм, який використовується деякими приватними блокчейнами. У рамках цієї моделі консенсусу вузли по черзі створюють блоки. Для опрацювання ситуацій, коли вузол недоступний, цей алгоритм включає обмеження за часом, що дозволяє доступним вузлам додавати блоки, щоб недоступні вузли не призводили до зупинки. Ця модель гарантує, що жоден вузол не створить більшу кількість блоків, ніж інші. Алгоритм виграє простотою ідеї, не має криптографічних головоломок і має низькі вимоги до енергоспоживання. Оскільки існує необхідність у довірі між вузлами, циклічний перебір не працює в загальнодоступних блокчейнах без вимог прав доступу, що використовуються більшістю криптовалют.

Алгоритм знаходження консенсусу "Доказ повноважень" (також званий "доказом ідентичності") спирається на часткову довіру до користувачів через їхній зв'язок з особистостями в реальному світі. Користувачі повинні мати свої посвідчення в мережі блокчейна (наприклад, ідентифікуючі документи, що були перевірені та завірені нотаріально, і завантажені в блокчейн). Ідея полягає в тому, що вузол використовує свої персональні дані/репутацію для додавання нових блоків. Користувачі мережі блокчейн безпосередньо впливають на репутацію вузла, що валідує, ґрунтуючись на його поведінці. Що нижча репутація, то менша ймовірність

додавання блоку. Отже, в інтересах вузла підтримувати високу репутацію. Цей алгоритм застосовується тільки до блокчейнів із правами доступу та високим рівнем довіри.

1.5. Смартконтракти.

Термін “смартконтракт” з'явився 1994 року і був визначений Ніком Сабо як “протокол транзакцій, який виконує умови угоди. Загальними цілями укладення смартконтракту є задоволення загальних договірних умов (таких як умови оплати, заставне утримання, конфіденційність і навіть примусове виконання), мінімізація зловмисних і випадкових дій, а також зменшення потреби в довірених посередниках” [16].

Смартконтракти розширюють і використовують ідею блокчейна. Смартконтракт — це набір коду і даних (іноді званих функціями і станом), які укладаються з використанням криптографічно підписаних транзакцій у мережі блокчейна (наприклад, смартконтракти *Ethereum* або *Hyperledger Fabric*). Смартконтракт виконують вузли в мережі блокчейна; усі вузли, які виконують смартконтракт, мають отримувати однакові результати від виконання, ці результати записуються в розподілене сховище. Код, що міститься в блокчейні, захищений від несанкціонованого доступу і, отже, може використовуватися (серед інших цілей) в якості довіреної третьої сторони. Смартконтракт може виконувати обчислення, зберігати інформацію, змінювати дані, і за необхідності, автоматично надсилати дані іншим користувачам. Це не обов'язково можуть бути фінансові операції. Важливо зазначити, що не кожен блокчейн може виконувати смартконтракти.

Код смартконтракту може являти собою багатосторонню транзакцію, зазвичай у контексті бізнес-процесу. У разі, коли в контракті кілька сторін, перевага смарт-контрактів полягає в тому, що це може гарантувати безпеку даних та їхню прозорість.

Смартконтракти мають бути детермінованими, тобто за однакових вхідних даних вони завжди даватимуть один і той самий результат на виході. Крім того, всі вузли, що виконують смартконтракт, повинні узгоджувати стан після виконання. Щоб досягти цього, смартконтракти не можуть працювати з даними поза тим, що безпосередньо передається в них (наприклад, смартконтракти не

можуть отримувати дані веб-сервісів – їх потрібно буде передавати як параметр) [17].

Для багатьох реалізацій блокчейна вузли виконують код смартконтракту одночасно під час додавання нових блоків. Існують деякі реалізації блокчейна, в яких є вузли, що не виконують код смартконтракту, а замість цього перевіряють результати користувачів, які це роблять [18]. Для публічних сховищ із підтримкою смартконтрактів (таких як *Ethereum*) користувач, який виконує транзакцію зі смартконтрактом, повинен буде сплатити вартість виконання коду. Існує обмеження на час виконання, який може знадобитися при виклику смартконтракту, залежно від складності коду. Якщо цей ліміт перевищено, виконання зупиняється, і транзакція відкидається. Цей механізм не тільки винагороджує користувачів за виконання коду смартконтракту, але також запобігає виконанню зловмисниками атаки на відмову в обслуговуванні (*DDoS*), споживаючи всі ресурси мережі (наприклад, використовуючи нескінченні цикли). У мережах із дозволеними смартконтрактами, наприклад *Hyperledger Fabric*, користувачі можуть не вимагати оплати за виконання коду смартконтракту. Ці мережі розроблені з урахуванням наявності відомих учасників. Можуть бути використані інші методи запобігання зловмисній поведінці (наприклад, анулювання доступу).

З юридичного погляду використання смарт контрактів порушує різні правові питання. Виконання смарт контракту не вписується в традиційну основу територіальної юрисдикції, що ускладнює визначення того, які закони застосовуватимуться для вирішення договірних питань, пов'язаних із конкретним смартконтрактом. Бо існує проблема визначення того, який суд має юрисдикцію для розгляду судових позовів, що випливають із використання смартконтрактів. Важко вирішувати спори, що виникають у зв'язку з виконанням смартконтрактів. Наприклад, якщо одна зі сторін оскаржує, чи є смартконтракт юридично обов'язковим.

Існує безліч платформ для створення смартконтрактів. Усі вони створені для різних цілей і різними організаціями. Розглянемо блокчейни *Ethereum,*

Hyperledger Fabric і технологію *DLT Corda*. Причина, з якої їх було обрано, полягає в тому, що перший є загальнодоступним, другий - приватним блокчейном, а третій - не блокчейном, а технологією *DLT*, створеною консорціумом фінансових установ *R3*.

Метою платформи *Ethereum* є об'єднання попередньої роботи над технологією блокчейна з новими функціональними можливостями для поліпшення масштабованості, стандартизації, простоти розробки та взаємодії з іншими платформами. Це децентралізована платформа з функціональними можливостями смартконтрактів. Його криптовалютою є "*Ether*", що використовується для оплати транзакцій, а мова програмування, яка використовується для створення смартконтрактів в *Ethereum*, називається *Solidity*. Для виконання смартконтрактів використовуються досить високі обчислювальні витрати, що веде до проблем із продуктивністю. Будучи широко використовуваною платформою, *Ethereum*, можливо, не найкращий вибір для смарт-контрактів, оскільки транзакції може побачити будь-хто.

Hyperledger Fabric - це блокчейн, заснований на проєкті *Hyperledger*, який дає змогу виконувати смартконтракти. *Hyperledger Fabric* дає змогу створювати розподілені додатки на мовах програмування загального призначення і не залежить від платформи криптовалюти. Однак мовою програмування, що використовується в смарт контрактах, є *Go*.

Corda є не блокчейном, а платформою розподіленого зберігання, розробленою для фінансового сектору. Це платформа, яку можна використовувати для розробки додатків для фінансових установ. Це також приватна мережа, призначена для запису, управління та синхронізації фінансових угод або контрактів між регульованими фінансовими установами. *Corda* дозволяє створювати записи для фінансових подій, які неможливо відкликати. Смартконтракти *Corda* можуть бути написані на *Java*. *Corda* має просту архітектуру, яка підвищує її продуктивність і безпеку порівняно з іншими середовищами корпоративного рівня.

1.6. Висновки до розділу.

У технології блокчейн чітко вираженні переваги та недоліки та освітлення обмежень типів цієї технології. Подальше порівняння кожного з них допомогло дізнатися можливість використання цієї системи, як основи для побудови засобів децентралізованого зберігання даних в технологіях IoT. Необхідно надати увагу безпеці, через високу вірогідність використання IoT разом з конфіденційною інформацією, та підтриманням контролю над самими комп'ютерами. Для цього розглянуті можливості втручання та впливу на роботу мережі на основі технології Blockchain та розглянуто варіанти створення довірених вузлів, які будуть підтримувати та перевіряти транзакції в мережі.

Останнім етапом пошук варіантів відтворення ідеї автоматизації роботи IoT в мережі. Цим інструментом виступлять смартконтракти. Було розглянуто основні принципи роботи та вже створенні та популярні рішення на різних типах блокчейнів.

2. Аналіз моделей застосувань децентралізованого зберігання та обробки даних.

2.1. Моделі інтеграції алгоритмів розподіленого зберігання й оброблення та систем *IoT*.

Більшість дослідників класифікують додатки блокчейна на фінансові та нефінансові, оскільки криптовалюти становлять значну частку наявних мереж блокчейнів. Є інші класифікації відповідно до версій блокчейна (1.0, 2.0 і 3.0). У таблиці 2. 1 наведено прикладну класифікацію, як найповнішу з погляду галузей застосування.

Таблиця 2.1. Класифікація застосувань алгоритмів розподіленого зберігання.

Сфера застосування	**Додатки**
Бізнес та індустрія	Логістика, енергетичний сектор
Управління даними	Поширення даних, управління людськими ресурсами
Фінанси	Криптовалюти, онлайн торгові майданчики
Перевірка цілісності дані	Страхування, інтелектуальна власність, перевірка підробок
Держава	Голосування, закон і право, громадське закон і право, громадське адміністрування, доказ існування
IoT	Е-бізнес, розподілене управління даними
Охорона здоров'я	Електронні медичні картки
Освіта	Репутація освітніх закладів, управління сертифікатами
Безпека та приватність	Анонімність у зберіганні даних

Однією з галузей, що розвивається найбільше, на сьогоднішній день є

Інтернет речей, розглянемо перспективи об'єднання двох технологій - блокчейну та *IoT* [19].

Інтернет речей (*IoT*) - це повсюдна взаємодія інтелектуальних пристроїв через мережу Інтернет. *IoT* дає можливість будь-яким пристроям з'єднуватися і обмінюватися даними, тим самим перетворюючи фізичний світ на величезну інформаційну систему. Різні технології, такі як хмарні обчислення і машинне навчання для аналізу даних та інформаційного моделювання, швидко стають невід'ємною частиною структури *IoT*. Величезний прогрес у сфері *IoT* також сприяє зростанню бізнесу в галузі інфо-комунікаційних технологій (ІКТ). Момент, у якій *IoT* стане частиною нашого повсякденного життя, можна предсказати з того, що 95% нових продуктів до 2022 року матимуть підтримку *IoT* [20].

В умовах постійно зростаючої кількості пристроїв *IoT* і їхньої доступності до Інтернету, викликає стурбованість про безпеку, тобто законний доступ користувачів до даних. З одного боку, всюдисущий характер *IoT* стимулює створення інноваційних додатків для кінцевого користувача, але, з іншого боку, відсутність заходів безпеки може призвести до критичних проблем, приміром, таких як крадіжка зі зломом унаслідок слабкого місця в розумнії сигналізації. Безпека має ще один аспект, а саме "конфіденційність". Компанії, які керують конфіденційними даними користувача, можуть використовувати їх незаконно, що веде до порушення конфіденційності.

Загострення ситуації пов'язане з тим, що кілька років тому були малоймовірні сценарії розвитку *IoT* з мільярдами підключених пристроїв, і з цієї причини аспекти безпеки не завжди розглядалися на етапі проектування продуктів. Фактично, згідно з дослідженнями, проведеними *Gartner*, у 2018 році витрати на безпеку *IoT* в усьому світі сягнули 1,5 млрд. доларів США, і до 2022 року половину всіх бюджетів *IoT* буде спрямовано на усунення несправностей, відкликання пристроїв з ринку та на усунення проблем безпеки, а не на захист [21].

Наразі *IoT* застосовується в таких галузях: охорона здоров'я, промисловість,

роздрібна торгівля, будівництво, розвиток міської інфраструктури, транспорт, енергетика тощо. Згідно з *IHS Markit*, прогнозується, що на кінець 2030 р. кількість під'єднаних пристроїв *IoT* досягне 125 млрд. пристроїв [22].

Оскільки концепція *IoT* інтегрується в наявну архітектуру мереж, *IoT* використовує *IP*-мережі та хмарну інфраструктуру для зв'язку пристроїв і застосунків, які можуть обмінюватися інформацією як між собою всередині приватних сегментів, так і між мережами, оптимізуючи процеси для збільшення ефективності та забезпечення безпеки.

Для реалізації *IoT* найважливішими питаннями є безпека даних, довіра до мережі та ізоляція з'єднання.

Безпека даних. Вірус, виявлений 2010 року, завдав величезної шкоди промисловій і державній інфраструктурі, такій як атомні електростанції, греблі та державні мережі зв'язку (мережі спеціального призначення). Надійна інфраструктура *IoT* гарантує, що критично важливі обчислювальні мережеві ресурси та ресурси зберігання працюють, без незапланованих простоїв обладнання. Безпека означає, що дані не пошкоджені, не загублені, не вкрадені та не підроблені.

Довіру до мережі. Після випадку з витоком інформації про порушення закону "Про захист персональних даних" у 2013 році у США, тим, хто впроваджує *IoT*, важко довіряти партнерам та працівникам, які можуть надавати доступ певними структурам (наприклад, урядам, виробникам або постачальникам послуг), дозволяючи їм збирати та аналізувати користувацькі дані. Таким чином, довіра та анонімність повинні лежати в основі майбутніх рішень *IoT*.

Контроль неізольованих з'єднань. Взаємопов'язані пристрої всередині локального сегмента *IoT* мережі (наприклад, усередині будинку або на території промислової будівлі) не працюють ізольовано, вони повинні взаємодіяти з усією екосистемою *IoT*. Глибина і ширина взаємозв'язку визначають характер екосистеми *IoT*. Взаємодія в мережі Інтернету речей буває декількох типів:

пристрій до пристрою, пристрій до хмарної платформи, пристрій зі шлюзом, хмарна платформа до хмарної платформи. Контроль неізольованих з'єднань є серйозною проблемою, яку необхідно вирішити.

Останніми роками конфіденційність і безпеку даних у сфері *IoT* було добре досліджено, і в результаті було запропоновано різні підходи для вирішення різних аспектів конфіденційності.

Наразі одним із перспективних рішень цих проблем є застосування розподілених моделей зберігання та обробки даних. Блокчейн - це багатообіцяюча технологія для досягнення децентралізації, оскільки вона дає змогу досягти розподіленого консенсусу між різними сторонами без необхідності довіряти одна одній або центральному серверу / базі даних. Тобто блокчейн, може забезпечити ефективне рішення для конфіденційності та безпеки даних *IoT*. Блокчейн забезпечує високий рівень конфіденційності завдяки використанню змінюваного відкритого ключа (*public key*) як підтвердження особи користувача. Ці особливості роблять його привабливим для забезпечення розподіленої конфіденційності та безпеки в *IoT*. Фактично, коли справа доходить до *IoT*, блокчейн можна використовувати для зберігання критично важливих міжмашинних повідомлень, що надсилаються у вигляді транзакцій, забезпечуючи підзвітність і безпеку даних, що зберігаються. Розподілене зберігання і обробка також може забезпечити ідентифікацію і підтвердження походження пристроїв *IoT* з його криптографічними функціями. Уже є низка застосувань блокчейна наприклад, перевірка місця розташування, розподілені системи зберігання медичних даних.

Покращення, які може принести інтеграція блокчейна в *IoT* мережі:

- **Децентралізація і масштабованість:** перехід від централізованої архітектури до розподіленої *P2P* усуне єдині точки збоїв і вузькі місця в топологіях *IoT* мереж. Це також допоможе запобігати сценаріям, коли одна компанія або людина контролюють обробку і зберігання інформації

величезної кількості людей. Іншими перевагами децентралізації є архітектури є поліпшення відмовостійкості та масштабованості системи.

- **Ідентифікація:** за допомогою блокчейна учасники можуть ідентифікувати кожен пристрій. Дані, що передаються в систему, є незмінними, і вони нерозривно пов'язані пристроєм/користувачем. Крім того, блокчейн може забезпечити довірену розподілену розподілену автентифікацію та авторизацію пристроїв для додатків *IoT*;
- **Автономність:** технологія блокчейна розширює можливості додатків, уможливлюючи розробку інтелектуальних активів як послуги. Завдяки блокчейну пристрої можуть взаємодіяти один з одним без участі будь-яких централізованих серверів;
- **Надійність:** інформація в *IoT*-мережі завжди залишатиметься незмінною і пов'язаною з часовою відміткою в блокчейні. Учасники системи здатні перевіряти справжність даних і можуть бути впевненими, що дані не були підроблені;
- **Безпека:** інформація може бути захищеною, якщо вони зберігаються як транзакції блокчейна. Блокчейн може розглядати обмін повідомленнями пристроїв як транзакції, перевірені смарт-контрактами, таким чином забезпечуючи безпеку обміну даними між пристроями. Поточні протоколи, що використовуються в *IoT*, можуть бути оптимізовані за допомогою блокчейна;
- **Ринок послуг:** блокчейн може прискорити створення екосистеми *IoT* послуг і ринків даних, де транзакції між партнерами можливі без встановлення прав. Мікросервіси можуть бути легко розгорнуті, а мікротранзакції можуть бути безпечними в умовах розподіленої довіри. Це поліпшило б взаємозв'язок *IoT* і доступ до даних *IoT* у блокчейні;
- **Безпечне розгортання коду:** використовуючи переваги захищеного незмінюваного сховища блокчейна, виробники можуть відстежувати стани та оновлення ПЗ з максимальною достовірністю.

Інший аспект, який слід брати до уваги, стосується зв'язку між базовою

інфраструктурою *IoT* і блокчейном. Під час інтеграції блокчейна необхідно вирішити, де відбуватимуться взаємодії: усередині *IoT*, між *IoT* і блокчейном, або ж виключно через блокчейн. Туманні обчислення зробили революцію в *IoT* з додаванням нового рівня між хмарними обчисленнями і пристроями *IoT* і могли б бути також використані в цільовій архітектурі інтеграції.

- *IoT - IoT* : цей підхід може бути найшвидшим з точки зору затримки, оскільки він може працювати в автономному режимі. Пристрої *IoT* повинні мати можливість взаємодіяти один з одним, що зазвичай включає механізми виявлення і маршрутизації даних. Тільки частина даних *IoT* зберігається в блокчейні, тоді як взаємодії *IoT* відбуваються без використання блокчейна (рис. 2.1а). Цей підхід був би корисним у сценаріях з даними *IoT*, де взаємодії *IoT* відбуваються з низькою затримкою, проте в цьому випадку ми використовуємо всі переваги розподіленого зберігання;
- *IoT* - блокчейн: у цьому підході всі взаємодії проходять через блокчейн, що дає змогу фіксувати запис взаємодій. Цей підхід гарантує, що всі транзакції даних відстежуються. Проте запис усіх взаємодій у блокчейні призвів би до збільшення пропускної спроможності та продуктивності кінцевих пристроїв, що є однією з добре відомих проблем у блокчейні (рис. 2.1б);
- гібридний підхід: гібридний дизайн, у якому тільки частина взаємодій відбувається в блокчейні, а решта безпосередньо передаються між пристроями *IoT*. Однією з проблем цього підходу є вибір того, які взаємодії повинні проходити через блокчейн. Ідеальне поєднання цього підходу було б найкращим способом інтеграції обох технологій, оскільки він використовує переваги блокчейна і переваги взаємодії *IoT* в реальному часі. (Рис. 2.1в).

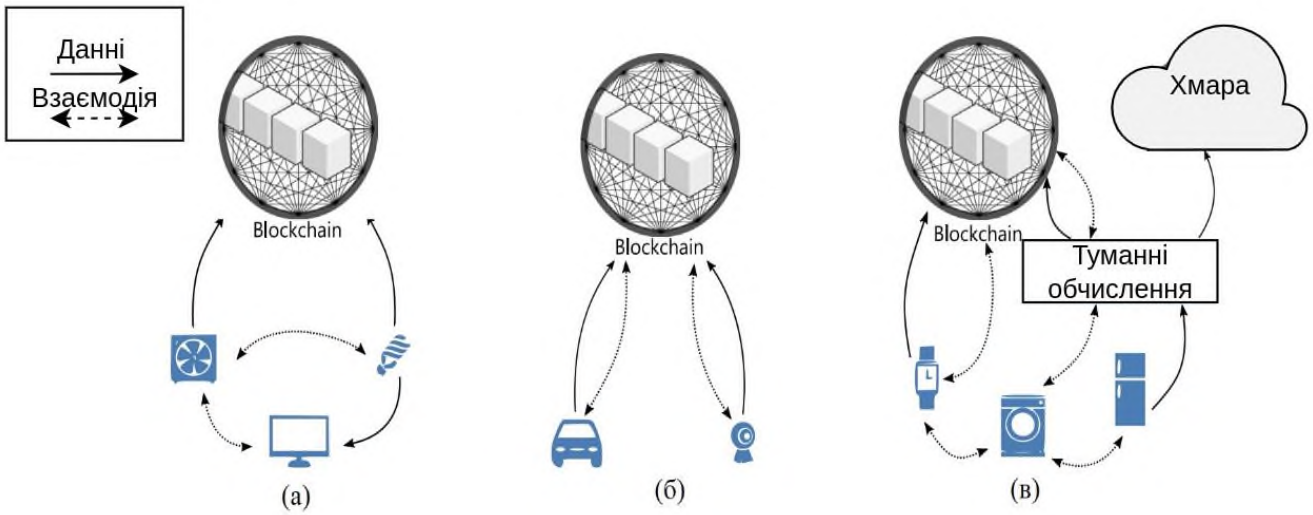

Рис. 2.1. Моделі передавання даних в *IoT* мережах із блокчейном.

Одним із застосувань *IoT* є платформа блокчейну для промислового *IoT* (*BPIIoT: A Light-Weighted Blockchain-Based Platform for Industrial IoT*). *BPIIoT* використовує смарт-контракти для розробки децентралізованих додатків хмарного виробництва (*cloud based manufacturing*). При цьому пристрої *IoT* запускають сервіси розподіленого зберігання і використовують гаманці для надсилання транзакцій у смарт-контракти (розумні контракти).

Так само смарт-контракти можна використовувати для управління даними, для оновлення вбудованого програмного забезпечення пристроїв *IoT*, для управління доступом, як систему зберігання даних у багаторівневій архітектурі *IoT*. Так само смарт-контракти застосовують для захисту авторизації до ресурсів *IoT*.

Вищезазначені моделі використовують або виконання смарт-контрактів, або виконання конкретних завдань додатків, але не децентралізацію систем *IoT* і досягнення автономного виконання додатків.

Протокол *Tangle* реалізує глобальний розподілений регістр для *IoT*, використовуючи спрямований ациклічний граф, згенерований транзакціями. *Tangle* спроектований для *IoT* для використання мікротранзакцій, однак він не надає архітектуру або структуру даних для децентралізації *IoT*, також *Tangle* не є повним за Тюрингом, щоб підтримувати створення сценаріїв і смарт-контракти.

З метою дозволу / заборони доступу до даних, що зчитуються через

пристрої *IoT*, використовуються різні політики. Загалом, ці політики регулюються відповідно до попередньо визначеного набору правил. До теперішнього часу в галузі *IoT* використовувалися різні моделі управління доступом: управління доступом на основі ролей (*RBAC*), управління доступом на основі можливостей (*CapBAC*); управління доступом на основі атрибутів (*ABAC*) і моделі управління доступом на основі семантичних правил. Наприклад, запроваджується заснована на блокчейні структура управління доступом під назвою *FairAccess* для задоволення потреб *IoT* у сфері безпеки та конфіденційності. У *FairAccess* блокчейн використовується для розподіленого відстеження і достовірності транзакцій доступу між автономними організаціями. З цією метою *FairAccess* вводить нові типи транзакцій для надання, отримання, делегування та відкликання прав доступу до ресурсів.

Існує модель конфіденційності та безпеки для "розумних будинків", де аналіз ризиків виконується автоматизовано. Зовнішній об'єкт, званий провайдером управління безпекою (*SMP*), може додавати правила контролю доступу для захисту певних пристроїв *IoT* або може застосовувати динамічні політики для зміни правил контролю доступу залежно від контексту, наприклад, залежно від місця розташування.

Розглянемо адаптивний підхід з урахуванням контексту для пристроїв, які звертаються до послуг на основі визначення місця розташування. Конфіденційність забезпечується агентом, який отримує інформацію про місцезнаходження за допомогою аналізу мережевих служб і реагує на зміни місця розташування. Крім того, технологію програмно-визначуваної мережі (*SDN*) використовують для блокування/поміщення в карантин пристроїв IoT у мережі "розумного будинку" на основі їхньої мережевої активності. Ця пропозиція спрямована на захист конфіденційності користувача шляхом обмеження доступу до даних через зовнішній об'єкт, тобто *SMP*, з використанням контекстної інформації.

Одна з найбільших проблем під час інтеграції блокчейну в *IoT* - це масштабованість. Насправді, через величезну кількість пристроїв і брак ресурсів

для розгортання блокчейну в *IoT* є особливо складним завданням. Оптимальна архітектура повинна масштабуватися для великої кількості пристроїв *IoT* (вони мають бути рівноправними в мережі), і мережа має бути здатна обробляти транзакції з високою пропускною здатністю.

2.2. Використання алгоритмів розподіленого зберігання в різних галузях.

2.2.1. Перевірка функціональності та ефективності систем розподіленого зберігання даних у сфері охорони здоров'я.

Одним із найважливіших застосувань технології блокчейн є охорона здоров'я. Потенціал блокчейна в охороні здоров'я полягає у розв'язанні проблем, пов'язаних із безпекою даних, конфіденційністю, спільним використанням і зберіганням даних.

Однією з вимог для галузі охорони здоров'я є здатність двох сторін, чи то людина, чи то машина, обмінюватися інформацією точно, ефективно та послідовно, оскільки ціна помилки під час взаємодії різних учасників системи зростає. Таким чином, метою застосування блокчейна в охороні здоров'я є сприяння обміну інформацією, пов'язаною зі здоров'ям, такою як електронна медична картка, між постачальниками медичних послуг і пацієнтами. Більше того, таке застосування дає змогу постачальникам безпечно обмінюватися медичними записами пацієнтів (з урахуванням дозволів пацієнтів), незалежно від місця розташування постачальника та довірчих відносин між ними [23].

Технологія розподіленого зберігання перевизначає моделювання даних і управління, розгорнуте в багатьох додатках охорони здоров'я. Нові технології охорони здоров'я, засновані на блокчейні, концептуально організовані в чотири рівні, включно з джерелами даних, технологією блокчейна, застосунками для охорони здоров'я та зацікавленими сторонами. Рисунок 2.2 ілюструє уявлення заснованого на блокчейні робочого процесу для додатків охорони здоров'я.

Спочатку всі дані з медичних пристроїв, лабораторій, мереж і багатьох інших джерел об'єднуються і створюють необроблені вихідні дані. Ці дані є невід'ємним компонентом всієї системи, заснованої на блокчейні, і це основний компонент, який створює перший рівень стека. Технологія блокчейна знаходиться на рівень вище вихідних даних. Кожна платформа блокчейна має різні особливості, такі як узгоджені алгоритми і протоколи. Платформи блокчейна полегшують користувачам створення та управління своїми транзакціями.

Основними компонентами блокчейна є смарт-контракти, підписи, події,

членство і цифрові активи. Виходячи з низки вимог, які необхідно виконати, обирається тип блокчейна - закритий, відкритий або гібридний. Наступним етапом є забезпечення інтеграції додатків з усією системою. Засновані на блокчейні медичні застосунки можна розділити на три широкі класи. По-перше, управління даними, включно з глобальним обміном науковими даними для досліджень і розробок, управління і зберігання даних (наприклад, хмарні додатки) та електронні медичні картки. Другий клас представляє додатки управління поставками і логістикою, включно з клінічними випробуваннями і фармацевтичними препаратами. Нарешті, третій клас охоплює *IoMT*, включно зі злиттям *IoT* і медичних пристроїв. Нарешті, на вершині ієрархії знаходиться рівень зацікавлених сторін, який складається зі сторін, що користуються медичними застосунками, таких як бізнес-користувачі, дослідники та пацієнти. Основними завданнями користувачів на цьому рівні є ефективний обмін, обробка та управління даними без шкоди для їхньої безпеки та конфіденційності.

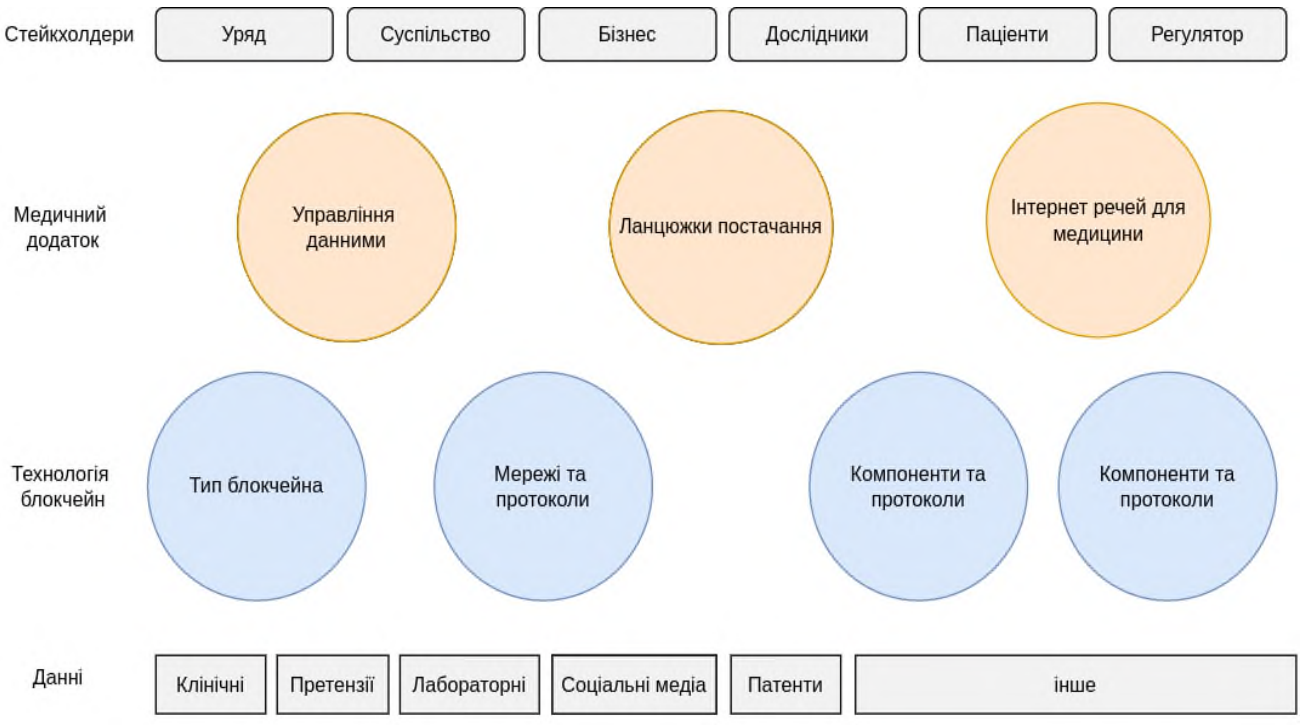

Рис. 2.2. Модель застосування блокчейна в охороні здоров'я.

На рисунку 2.3 змоделюємо схему руху медичних даних при використанні

блокчейна.

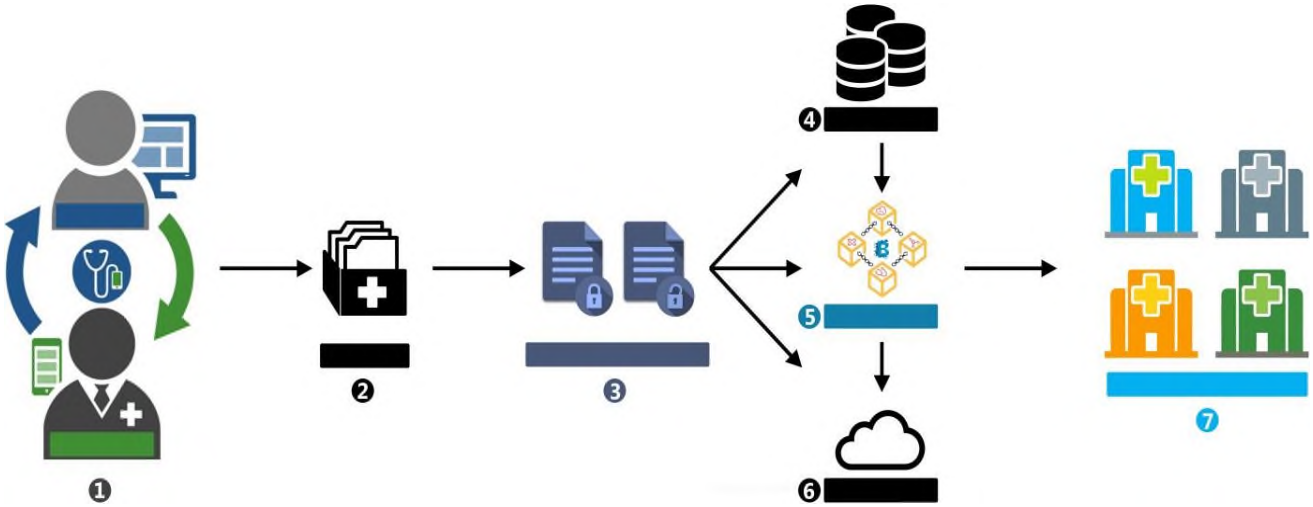

Рис. 2.3. Модель управління медичними даними в блокчейні.

Крок 1: Первинні дані генеруються взаємодією пацієнта з його лікарями та фахівцями або такими пристроями, як фітнес-трекери, портативні пульсометри, глюкометри тощо. Ці дані складаються з історії хвороби, поточної проблеми та іншої фізіологічної інформації.

Крок 2. Електронна медична карта (ЕМК) створюється для кожного пацієнта з використанням первинних даних, зібраних на першому етапі. Інша медична інформація, наприклад, отримана в результаті лікування хворих, історії хвороби, також включена в ЕМК.

Крок 3. Система контролю доступу до даних - пацієнт має індивідуальний контроль доступу до своєї картки. Сторони, які хочуть отримати доступ до цієї інформації, мають запросити дозвіл, який надіслано власнику медичної картки, і власник сам вирішує, кому буде надано доступ.

Кроки 4,5,6. Ці три кроки є частиною ядра всього процесу, включно з базою даних, блокчейном і хмарним сховищем. База даних і хмарне сховище зберігають записи розподіленим чином, а блокчейн забезпечує максимальну конфіденційність для забезпечення індивідуального доступу користувачів.

Крок 7. Постачальники медичних послуг, такі як спеціалізована клініка, громадський центр, лікарні, є кінцевими користувачами, які хочуть отримати доступ до безпечної та надійної медичної інформації, доступ до якої буде

санкціоновано власником.

Технологія блокчейну мають популярність у секторі охорони здоров'я завдяки важливості вирішення проблем безпеки ЕМК. ЕМК мають потенціал для поліпшення надання послуг медичної допомоги. Картка змінюється, коли пацієнт надходить до лікарні, або коли лікар ставить діагноз пацієнту, або коли результати діагностики, такі як сканування МРТ, зберігаються в системі ЕМК.

Таким чином, безпека такої цифрової інформації має першорядне значення, і в даний час має використовуватися розподілене зберігання для надійних медичних даних. Збереження цінності даних і зниження вартості зберігання для управління даними в технології блокчейна в охороні здоров'я відіграє важливу роль. Завдяки своїй унікальній можливості, технологія блокчейна є єдиною відповіддю для захисту цифрової інформації, і вона продовжує відігравати вирішальну роль у майбутньому управління корпоративними даними.

Управління поставками в охорону здоров'я на даний момент це складний процес, під час комплектації замовлень медикаментів, ліків та інших ресурсів існує спадковий ризик порушення процесу ланцюжка поставок, який може безпосередньо вплинути на безпеку пацієнтів. Згідно з дослідженням, проведеним Всесвітньою організацією охорони здоров'я (ВООЗ), понад 100 000 людей помирають в Африці через неправильне дозування підроблених ліків, замовлених у невідомих або перевірених постачальників. Підробка ліків, відсутність реєстру та помилки пакування в медичному закладі можуть порушити роботу всього ланцюжка поставок. Блокчейн є ключовою технологією моніторингу, що дає змогу контролювати весь процес переміщення лікарських препаратів. Оскільки всі зміни записані, і кожен вузол у блокчейні підтримує читання всіх транзакцій, легко перевірити походження препарату, постачальника і дистриб'ютора. Крім того, розподілене зберігання дає змогу працівникам охорони здоров'я та лікарям перевіряти справжність облікових даних постачальників. Завдяки кращому розумінню ланцюжка поставок завдяки належному і своєчасному процесу автентифікації, аптеки і постачальники медичних послуг зможуть гарантувати, що потік ліків, як і раніше, досягатиме тих пацієнтів, які його потребують найбільше.

У цьому відношенні технологія блокчейн має великі перспективи для створення надійної мережі постачальників. Рисунок 2.4 ілюструє фармацевтичний процес управління поставками з використанням технології блокчейн.

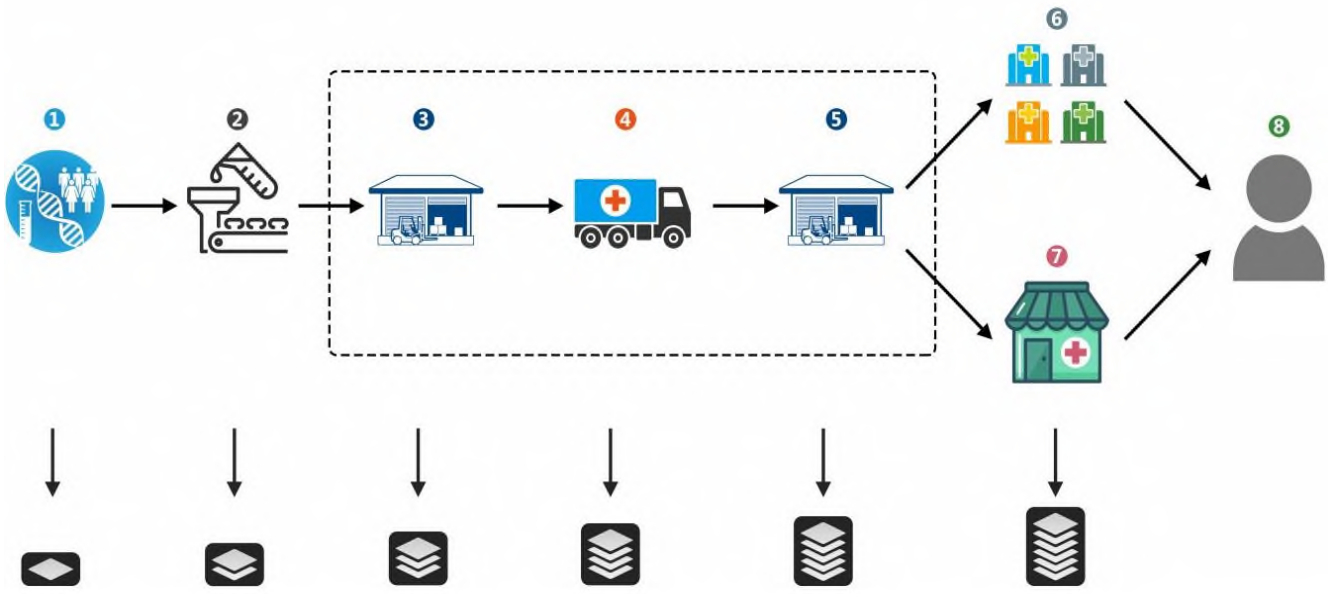

Рис. 2.4. Модель управління поставками ліків.

Крок 1. Блок створюється під час винаходу нових ліків або медичної допомоги, яка включає патентний захист і тривалий процес клінічних випробувань. Ця інформація записується в розподілений реєстр.

Крок 2. Щойно клінічне випробування буде успішним, патент відправляють на завод-виробник для випробування дослідного зразка та серійного виробництва. Кожен продукт має свою унікальну ідентифікацію, включно з іншою відповідною інформацією.

Крок 3. Після завершення масового виробництва разом з упаковкою ліки збираються на складі для подальшого продажу. Така інформація, як, час, номер лота, штрих-код, дата закінчення терміну придатності включені в блокчейн.

Крок 4. Інформацію про транспортування також включено в ланцюжок блоків, який може містити час очікування, спосіб транспортування, авторизованого агента та іншу інформацію.

Крок 5. Незалежна дистриб'юторська мережа, як правило, відповідає за

розподіл ліків і медикаментів постачальникам медичних послуг або роздрібним торговцям. Для цієї мети використовується склад для третьої сторони, звідки пов'язані всі кінцеві точки розповсюдження. Окрема транзакція також інтегрована в блокчейн.

Крок 6. Постачальники медичних послуг, як-от лікарні або клініки, повинні надати інформацію, наприклад, номер партії, власника продукту, дату закінчення терміну придатності для перевірки достовірності та запобігання підробкам. Це також входить у блокчейн.

Крок 7. Дії, яких вживає продавець, аналогічні Кроку 6.

Крок 8. Пацієнтам рекомендується визначати справжність упродовж усього процесу, оскільки ланцюжок поставок блокчейн пропонує прозору інформацію для перевірки потенційним покупцям.

Такий процес забезпечує недорогий контроль якості, реєстрацію продукту, відстеження руху ліків та їхнього походження через весь процес постачання.

Системи *IoMT* відіграють життєво важливу роль у розвитку систем охорони здоров'я [24]. Завдяки технології *IoMT* медичне обладнання, таке як кардіомонітор, сканери тіла і носяться пристрої, можуть збирати, обробляти і обмінюватися даними через Інтернет в режимі реального часу. Наприклад, із розвитком ШІ постачальники медичних послуг, використовуючи парадигму *IoMT*, можуть захоплювати зображення, ідентифікувати злоякісні ділянки та ділитися такими знаннями через глобальні мережі (рисунок 2.5).

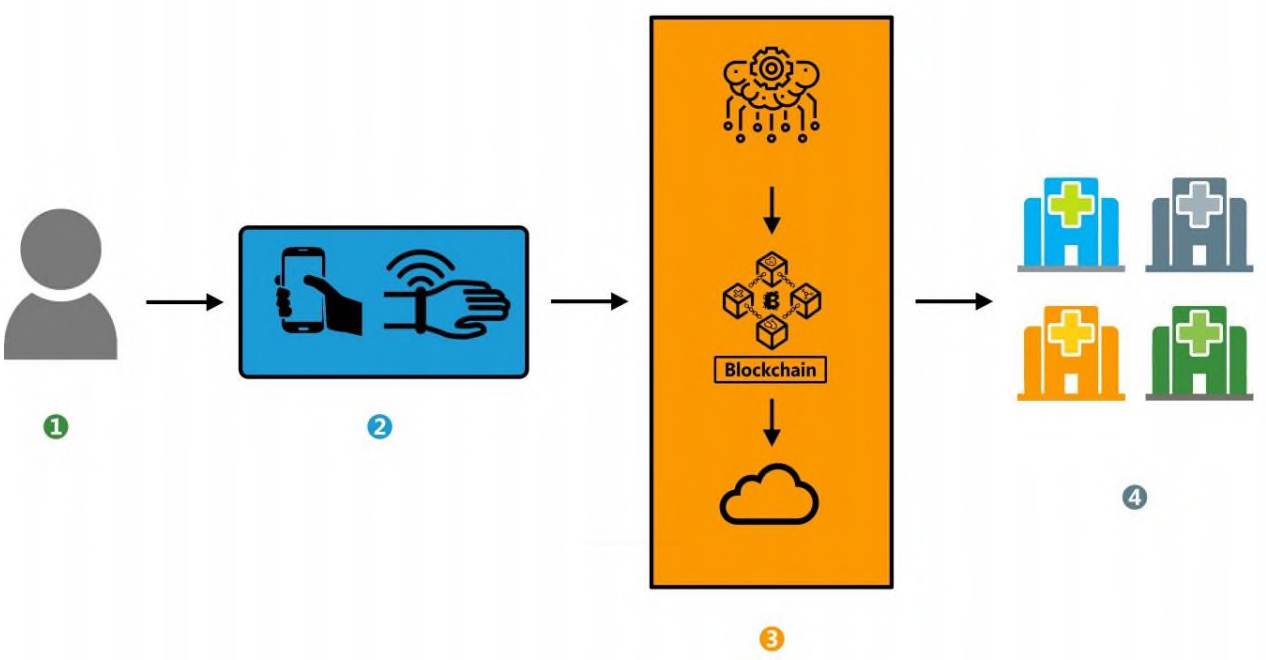

Рис 2.5. Схема застосування *IoMT* із блокчейном.

Крок 1. У сфері *IoMT* пацієнт є джерелом усіх даних.

Крок 2. Медичні пристрої *IoT* зазвичай або прикріплені близько, або дистанційно контролюють тіло пацієнта, генеруючи великий обсяг даних.

Крок 3. Дані, створені на кроці 2, зберігаються в блоках або в хмарному сховищі. У разі конфіденційних медичних даних, де безпека є першочерговим завданням, децентралізована система може допомогти блокувати блоки даних для досягнення максимальної безпеки.

Крок 4. Постачальники медичних послуг – це кінцеві користувачі, які отримують доступ до безпечної та надійної медичної інформації.

За допомогою технології блокчейна дані пацієнта будуть дійсно належати і контролюватися законним власником даних, тобто пацієнтом. Проте є ще кілька відкритих проблем, які потребують подальшого вивчення. Наприклад, здатність блокчейна своєчасно зберігати і обробляти масивні транзакції доступу до даних. У міру збільшення обсягу транзакцій затримка блоків збільшуватиметься в геометричній прогресії. Отже, існує потреба в інноваційних механізмах і алгоритмах для мінімізації затримок під час майнінгу.

Крім того, розглянуто застосовність блокчейна для розв'язання проблеми довіри та підвищення прозорості даних у клінічних випробуваннях. Можна використовувати блокчейн для підвищення наукової достовірності результатів клінічних випробувань, які можуть бути підірвані такими проблемами, як відсутність вихідних даних і вибіркова публікація. Очевидно, що технологія блокчейн стане незамінним інструментом для фармацевтів і медичних працівників для належної та своєчасної перевірки достовірності потоку законних ліків і їх доставки пацієнтам. Проте, необхідні подальші дослідження надійних механізмів відстеження, які контролюють реєстрацію продуктів.

Системи охорони здоров'я XXI століття складатимуться з різних пристроїв, що з'єднують пацієнтів (наприклад, віддалені медичні переносні пристрої.) Ці системи генерують дані безперервно та можуть зазнавати зловмисних атак під час передачі на різних рівнях мережі зв'язку. Основна проблема полягає в тому, як блокчейн працюватиме в складних і різноманітних системах зв'язку. Система *IoMT* буде використовувати мережі зв'язку, що належать різним постачальникам послуг з різними політиками контролю доступу до даних. Крім того, оскільки мережа складається з вузлів і комп'ютерів, які географічно розподілені, існує потреба в механізмах синхронізації для визначення порядку додавання блоків.

2.2.2. Використання алгоритмів розподіленого зберігання для гарантування чесності під час проведення процесів голосування.

Одним із найактуальніших застосувань для блокчейна є голосування. Блокчейн розподіляє індивідуальну інформацію для голосування між тисячами комп'ютерів по всьому світу, що унеможливлює зміну або видалення голосів після того, як вони подані. Такий підхід сприяє зміцненню довіри між виборцями та урядами, захищаючи їхні дані та конфіденційність. Довіра створюється завдяки тому, що користувач контролює свої дані. Подібні платформи дають змогу громадянам голосувати, використовуючи додаток для смартфонів, а не фізично бути присутніми на виборчих дільницях.

Архітектура блокчейну вирішує один із найскладніших чинників, що впливають на чесність виборів -- довіру. Блокчейн гарантує, що довіра розподіляється між безліччю взаємно недовірливих сторін, які потенційно можуть змагатися один з одним, які беруть участь у спільному управлінні та підтримці криптографічно безпечного цифрового сліду виборів. Розподіляючи довіру таким чином, блокчейн зводить кількість довіри, необхідної від тих, хто бере участь у виборах, до мінімуму. Основний недолік блокчейна в наданні рішення для більшості корпоративних застосувань полягає в тому, що зберігання великих файлів у блокчейні не є легким завданням, оскільки він ледь підтримує невеликі текстові рядки, які просто записують передачу балансу між двома сторонами. Однак *Interplanetary File System* (міжпланетна файлова система - *IPFS*) являє собою цікавий проєкт, який може надати більшу частину інфраструктури, необхідної для зберігання контенту блокчейна, оскільки він забезпечує постійну децентралізовану мережу *Web*, де жоден об'єкт не контролює дані. Організації можуть додати до нього будь-які дані і у відповідь отримати унікальний ідентифікаційний хеш (рисунок 2.6). Він забезпечує децентралізований спосіб зберігання файлів у блокчейні, але дає більше контролю, надійно ідентифікує контент і забезпечує програмну взаємодію.

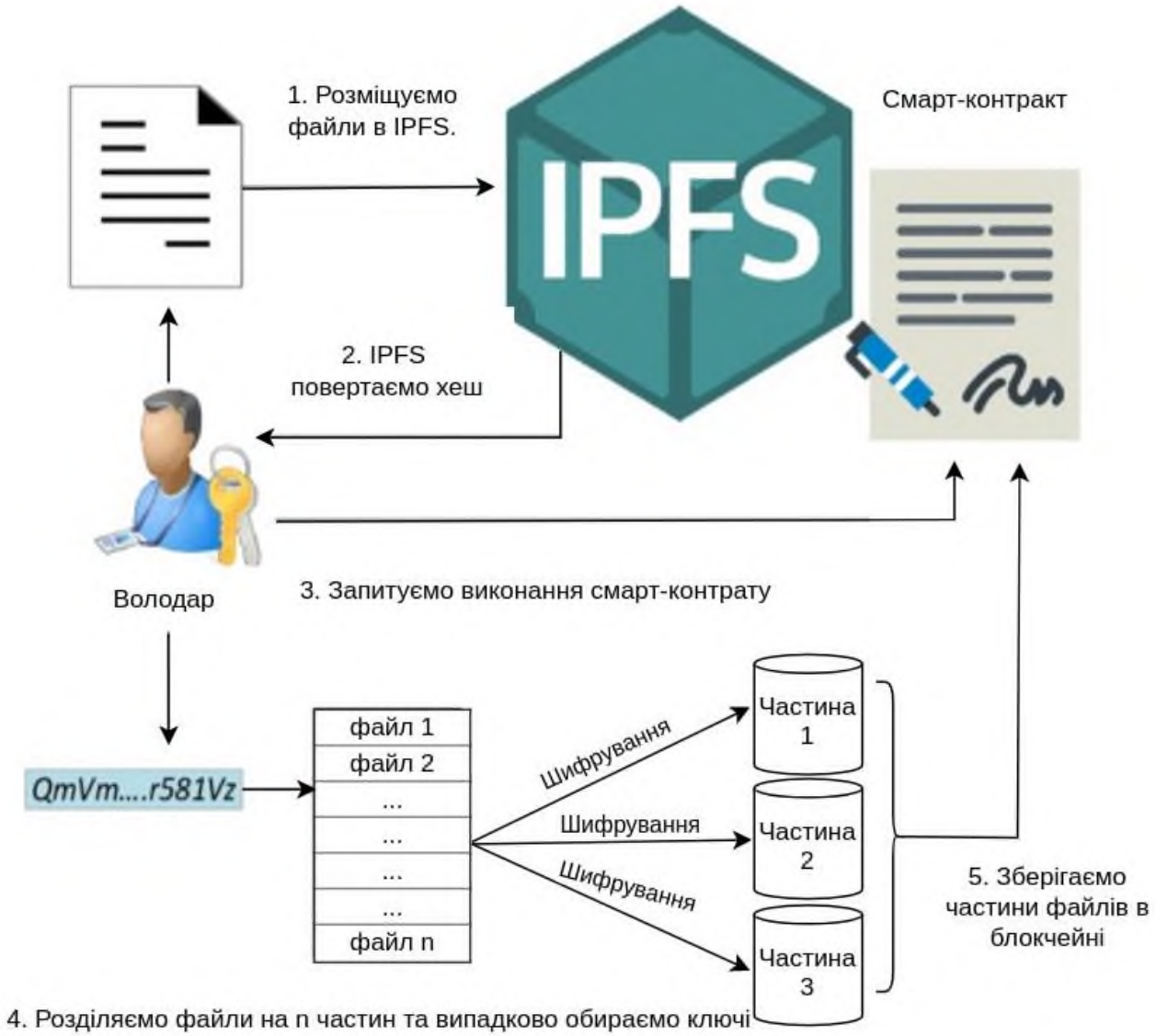

Рис. 2.6. Принцип роботи *IPFS* та блокчейна.

Деякі проєкти, які наразі розробляють або впровадили реалізації електронного голосування в блокчейні: *Luxoft Holding*, глобальний постачальник технологічних рішень для *IT*-послуг, прагне надати платформу для електронного голосування, що дає можливість першого голосування на основі блокчейну. Будучи одним із засновників *The Crypto Valley Association*, яка прагне створити провідну в світі екосистему блокчейнів і криптографічних технологій, компанія *Luxoft* співпрацює з організаціями, що працюють над урядовими рішеннями сервісів блокчейнів, і пропонує їм спільно створити блокчейн для урядового альянсу.

Компанія стверджує, що використовує інноваційну технологію шифрування, яка анонімізує голоси та забезпечує захищений облік і захищений аудит. За допомогою Університету прикладних наук і мистецтв Люцерна, *Amazon AWS* і *n'cloud.swiss*, платформа розгорнута в трьох різних центрах обробки даних у хмарі. Два з них розташовані у Швейцарії та один в Ірландії. Розподіляючи дані за трьома різними центрами обробки. *Fernado Lobato* [25] розробив систему з відкритим вихідним кодом у вигляді розумного контракту, що працює на *Ethereum*, у якому використовуються порогові ключі та кільцеві підписи для забезпечення прозорої та надійної системи, яка може бути реалізована для виборів середнього розміру. Кожен виборець контролює свій голос, залишаючись при цьому анонімним серед безлічі користувачів. Протокол мінімізує централізацію, використовуючи порогову криптографію. Схему голосування розділено на наступні фази після розгортання на блокчейні.

1. Налаштування - виборчий орган завантажує всю інформацію про вибори. Тривалість періодів голосування та реєстрації, пороговий ключ для шифрування голосів виборців і варіанти голосування;
2. Реєстрація - на цьому етапі будь-який виборець може звернутися до виборчого органу і вимагати, щоб його відкритий ключ було включено до набору відкритих ключів тих, хто має право голосу;
3. Голосування - на цьому етапі будь-який раніше зареєстрований виборець подає зашифроване голосування з пороговим ключем, опублікованим у контракті, з кільцевим підписом усіх відкритих ключів.
4. Завершено - після завершення етапу голосування всі треті сторони, що володіють секретами, можуть передати їх у блокчейн. Коли всі секрети укладені в договорі, будь-хто може завантажити і відновити закритий ключ;
5. Готовий до підрахунку - будь-хто може підрахувати результат виборів;
6. Проаналізувавши поточну ситуацію у сфері електронного голосування на базі блокчейна, перевіримо, наскільки блокчейн може відповідати всім вимогам, що висуваються до систем голосування (Таблиця 2.2).

Таблиця 2.2. Аналіз застосування блокчейна в електронному голосуванні.

Вимоги	**Опис**	**Результат при застосуванні блокчейна**
Справжність	Тільки користувачі з правом голосу повинні мати можливість голосувати	Кожен користувач мережі ідентифікується відкритим ключем, доступ до якого можливий тільки через його власний закритий ключ. Якщо припустити, що кожен виборець зберігатиме свій власний секретний ключ у безпеки, тоді вимогу автентичності буде виконано
Унікальність голосу	Кожен виборець повинен мати можливість проголосувати тільки один раз	Кожен поданий голос пов'язаний з відкритим ключем виборця на блокчейні. Дозволяючи кожному відкритому ключу віддавати тільки один голос
Анонімність	Третя особа не може зіставити голос і виборця	Оскільки кожен користувач ідентифікується відкритим ключем, а збережений голос зашифрований, неможливо пов'язати виборця з голосом
Цілісність	Голоси не можуть бути змінені або знищені	Через те, що хеш надає блокчейну властивості, завдяки яким, голос не можна фальсифікувати

Продовження таблиці 2.2.

Вимоги	**Опис**	**Результат при застосуванні блокчейна**
Перевірка результатів	Будь-яка людина повинна мати можливість самостійно перевірити, що всі голоси були правильно підраховані	Оскільки блокчейн прозорий для кожного вузла мережі, кожен може підтвердити, що кількість відданих і підрахованих голосів однаково
Аудит і сертифікація	Системи голосування мають бути перевірені та сертифіковані незалежними агентами	Властивість прозорості блокчейна дозволяє будь-якому вузлу в мережі проводити аудит блокчейна. Оскільки вихідний код є відкритим кодом і видимий у блокчейні, це означає, що застосунок, який використовується, також може бути перевірено
Мобільність	Можливість віддаленого голосування	Єдиними вимогами для доступу до мережі є пристрій з підключенням до Інтернету та адреса в платформі блокчейна, а це означає, що не потрібно жодної спеціальної інфраструктури або машин для голосування;

Продовження таблиці 2.2.

Вимоги	**Опис**	**Результат при застосуванні блокчейна**
Прозорість	Системи голосування мають бути чіткими та надавати виборцям точність і безпеку.	Ідентично вимозі перевірки результатів - прозорість є однією з властивостей блокчейна, і кожен застосунок, реалізований у блокчейні, успадковує це саме властивість
Виявлення помилок і відновлення	Системи голосування повинні виявляти помилки, збої та атаки і відновлювати інформацію для голосування	Якщо в ланцюжку блоків виконано будь-яку шкідливу дію, вона буде виявлена системою і визнана недійсною, що відповідає вимозі виявлення. Щойно деякі дані зберігаються в блокчейні, вони більше не можуть бути видалені, а це означає, що дані завжди можна відновити.

Виходячи з вищевказаних результатів, на рисунку 2.7 наведемо логічну архітектуру невеликого додатка для голосування.

Користувацький інтерфейс — це проста *HTML*-сторінка, яка дає змогу користувачам отримати доступ до функцій програми.

API відповідає за реагування на дії, що виконуються на інтерфейсі, і взаємодіє із сервером шифрування і блокчейном. Для кожного запиту, зробленого в інтерфейсі, він взаємодіє із сервером шифрування за допомогою викликів сервера для шифрування, розшифрування або додавання голосу. Для взаємодії з блокчейном використовуються транзакції.

Щоб забезпечити конфіденційність голосів, необхідно запобігти несанкціонованому доступу до голосів. Для цього кожен голос має бути

зашифрований перед передачею в блокчейн. Гомоморфне шифрування — це схема шифрування з відкритим ключем, властивості якої дають змогу виконувати певні типи обчислень на зашифрованому тексті, генеруючи зашифрований результат, коли під час розшифрування результат дорівнюватиме виконанню тієї самої операції з відкритим текстом.

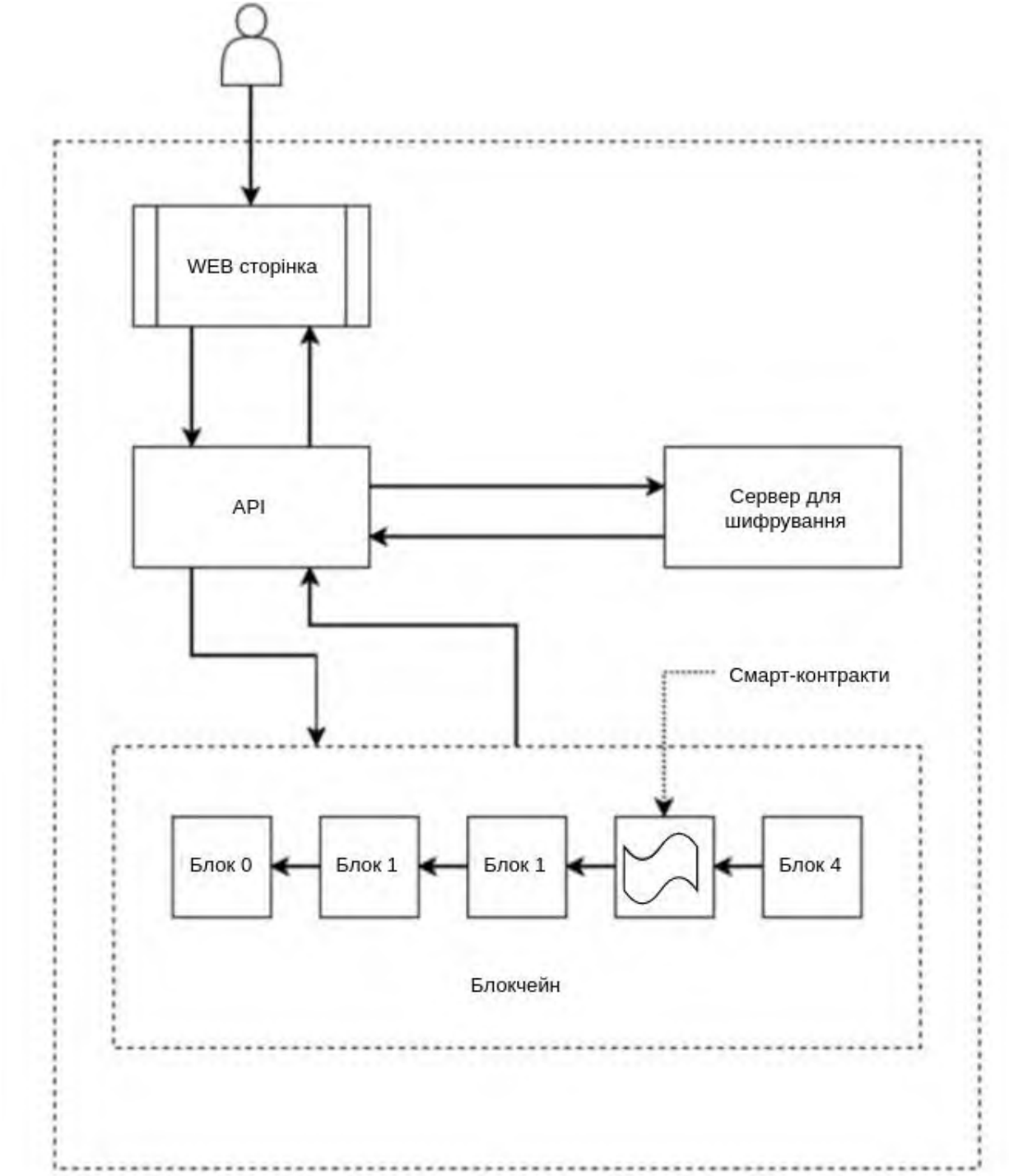

Рис. 2.7. Модель роботи додатку для голосування, заснованого на блокчейні.

3. Моделювання архітектури інтеграції технології блокчейн та IoT.

3.1 Завдання моделювання блокчейну в *IoT* мережах.

У даному розділі планується провести моделювання та аналіз інтеграції розподіленого зберігання та обробки даних в *IoT* мережах. Як було зазначено раніше, *IoT* мережі мають свої недоліки та обмеження, які полягають у такому:

- низька продуктивність кінцевих пристроїв;
- низька пропускна здатність кінцевих пристроїв;
- ризики, пов'язані з передачею в нешифрованому вигляді важливої інформації (раніше було розглянуто охоронні доступи та медичні дані).

Тому потрібно виробити конкретні рекомендації щодо впровадження блокчейна, тому що інтеграція без урахування обмежень *IoT* мереж недоцільна і технічно неефективна тому що кінцеві вузли будуть перевантажені обчислювальними операціями в разі використання *PoW* блокчейна.

Для вирішення цього завдання скористаємося методами комп'ютерного моделювання.

3.2 Інструменти моделювання.

3.2.1 Мережевий симулятор *NS3*.

Однією з найбільших проблем у дослідженнях систем зв'язку є висока вартість обладнання. Не всі лабораторії можуть придбати кілька маршрутизаторів, точок бездротового доступу та іншого обладнання для тестування нових протоколів, оптимізації архітектурних рішень і вибору конкретних топологій для застосування нових мережевих рішень. Ось чому було створено програмне забезпечення, яке може моделювати системи зв'язку. З появою цих програмних продуктів стало можливим проводити необхідні дослідження та експерименти набагато економічніше і досягти практично тих самих результатів, що й на реальному обладнанні.

На сьогоднішній день проблема комп'ютерного моделювання систем зв'язку має найрізноманітніші методи рішень.

Використання симулятора не тільки економить гроші, а й дає змогу проводити експерименти без побудови реальної мережі, що дорого в часі і трудомістко для перевірки гіпотез. Так само ще одна перевага використання симулятора полягає в тому, що в програмних продуктах доступні будь-які модулі обладнання.

На сьогодні відомо безліч мережевих симуляторів, і дослідники можуть обирати з широкого спектра продуктів, таких як *OPNET, OMNET, OMNET++, NS2, NS3*. Є також вузькоспеціалізоване ПЗ, створене для моделювання конкретного обладнання. Як правило, таке програмне забезпечення розробляється виробниками телекомунікаційного обладнання, наприклад, *Dynamips* і *Packet Tracer Simulator* від *Cisco*, розроблені для емуляції комутаторів і маршрутизаторів.

Одним із найпоширеніших є *NS2*, розроблений у 80-х роках. *NS2* - це безоплатне програмне забезпечення, воно має доволі велику та розвинену спільноту, і внаслідок цього доступна величезна кількість модулів, доповнень та

фреймворків.

Широко використовується мережевий симулятор *NS3*, один із найпередовіших інструментів моделювання мереж передавання даних. *NS3* поширюється під ліцензією *GNU GPLv2*, програма передана в суспільну власність і поширюється безкоштовно.

NS3 — це безоплатне програмне забезпечення, що поширюється за ліцензією *GNU GPLv2* і призначене для досліджень і навчання. Вихідний код *NS3* випущено для дослідження, модифікації та використанняі доступний на веб-сайті проекту. *NS3* дуже гнучкий і потужний інструмент моделювання, що використовує *C++* як інтегровану мову опису моделей. На додаток до *C++* також можна використовувати *Python* [26]. З широким і гнучким *API* та повною документацією програмного забезпечення, розробники моделей не обмежені ні в чому, їм надається можливість побудувати моделі будь-якої складності. Так само більшість поширених моделей уже включені в пакет програмного забезпечення. Завдяки використовуваній ліцензії *GNU GPLv2* вихідний код *NS3* може бути модифікований. Наприклад, розробники *NS3* створили модель бездротових мереж, яка може моделювати рухомі об'єкти в тривимірному просторі. Моделі були розроблені для створення різних складних і змішаних топологій під назвою *FlowMonitor* надає дуже гнучкий спосіб збору різних свідчень з модельованих активних мережевихпристроїв і каналів зв'язку. Проєкти *NetAnimator* і *PyViz* використовуються для візуалізації моделей, так як у симулятора немає власного графічногоінтерфейсу. Офіційна документація містить повний перелік усього функціоналу [27].

Розробка проєкту *NS3* триває на сьогоднішній день. Про це свідчить той факт, що багато великих компаній опублікували дослідження, засновані на *NS3*. Деякі компанії та установи також оголосили про розробку різних фреймворків для роботи симулятора, розробники щодня створюють нові та складніші моделі. Симулятор може задовольнити потреби в симуляції сучасних систем зв'язку і є дуже перспективним для розвитку, завдяки авторам проєктів і спільнотам, які постійно покращують проєкт, розробляють нові моделі та виправляють старі

помилки.

3.2.2 *Bitcoin Simulator*.

Bitcoin Simulator є фреймворком для симулятора *NS3*. Метою цього проєкту є вивчення того, як параметри, характеристики мережі та модифікації протоколів впливають на масштабованість, безпеку та ефективність блокчейн-мереж із підтримкою алгоритмів *Proof of Work*.

Мета симулятора — зробити його максимально реалістичним. *Bitcoin Simulator* здатний симулювати будь-яку повторну параметризацію блокчейн мережі.

Під час розробки було використано дані з *blockchain.info*, щоб оцінити час генерації блоків і розподіл розміру блоків, також використовували сканер (*crawler*) біткойнів, щоб з'ясувати середню кількість вузлів у мережі та їхній географічний розподіл. Крім того, використовувалися дані про підключення вузлів, надані *Coinscope*. Для полегшення процесу зв'язку між вузлами використовувався *quickjson*.

Використовуючи симулятор і змінюючи вхідні параметри, зазначені в таблиці 3.1, можна оцінити різні параметри блокчейна, такі як інтервал генерації між блоками, розмір блоку, механізми розповсюдження, відсоток застарілих блоків, пропускну здатність і загальний час поширення блоків.

Таблиця 3.1. Список основних вхідних параметрів.

Параметр	**Опис**	**Стандатне значення**
blockSize	Фіксований розмір блоку (у байтах). Якщо використовується значення за замовчуванням, то *blockSize* використовується згідно з розподілом розміру біткойн-блока, оціненому шляхом збору статистики з *blockchain.info*.	-1
noBlocks	Кількість згенерованих блоків	100
nodes	Загальна кількість вузлів у мережі. Кількість вузлів завжди має бути більшою або дорівнювати числу майнерів. Кількість майнерів, швидкості хешування та їхнє розташування можна змінювати.	16
blockIntervalMinutes	Середній інтервал генерації блоку в хвилинах.	10
invTimeoutMins	Тайм-аут блоку inv. Якщо використовується значення за замовчуванням, час очікування вдвічі більший, ніж *blockIntervalMinutes*.	-1
litecoin	Використовувати параметри мережі *litecoin*.	*false*
dogecoin	Використовувати параметри мережі *dogecoin*.	*false*
blockTorrent	Увімкнути протокол *BlockTorrent*.	*false*
spv	Увімкнути механізм *spv* у *blockTorrent*. Використовується тільки у поєднанні з — *blockTorrent*.	*false*

У цього симулятора на поточний момент немає графічного інтерфейсу, всі налаштування проводяться в термінальному вікні на операційній системі *Ubuntu*. Робоче вікно програми зі списком усіх вихідних параметрів і прикладу роботи

наведено на малюнках 3.1 і 3.2.

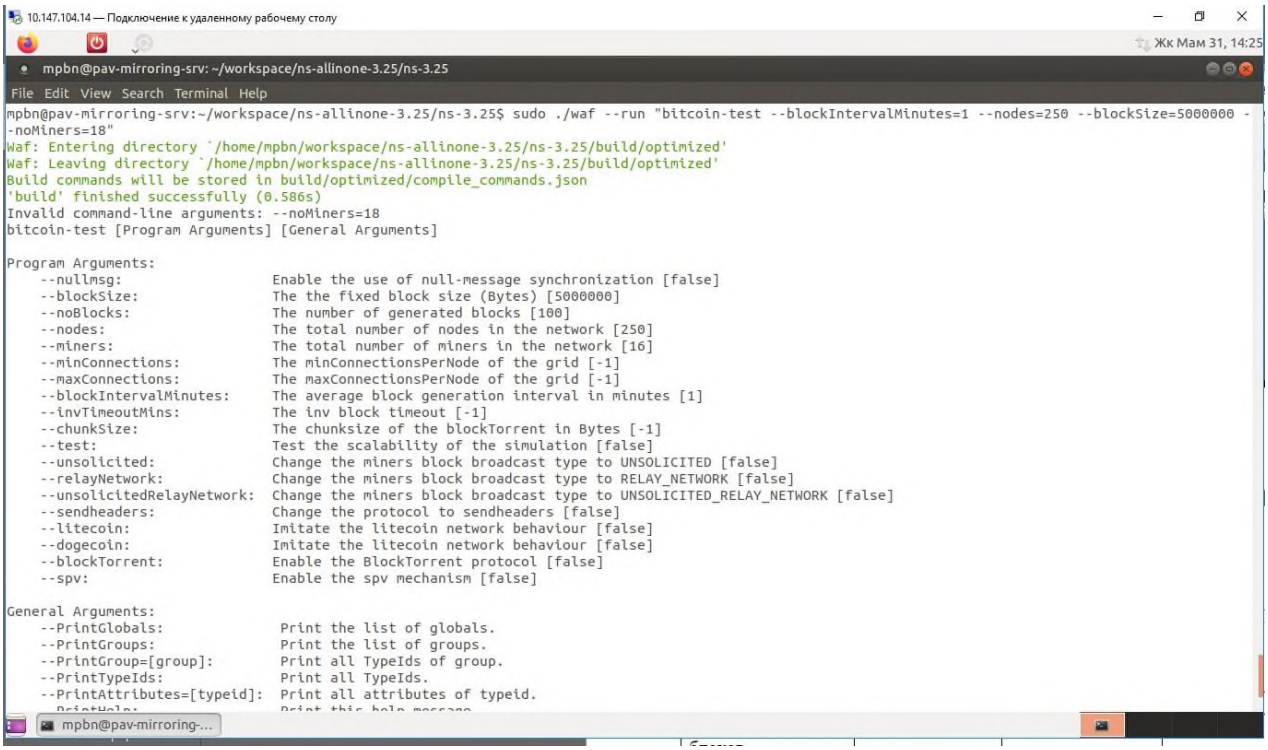

Рис. 3.1. Список усіх вихідних параметрів *Bitcoin Simulator*.

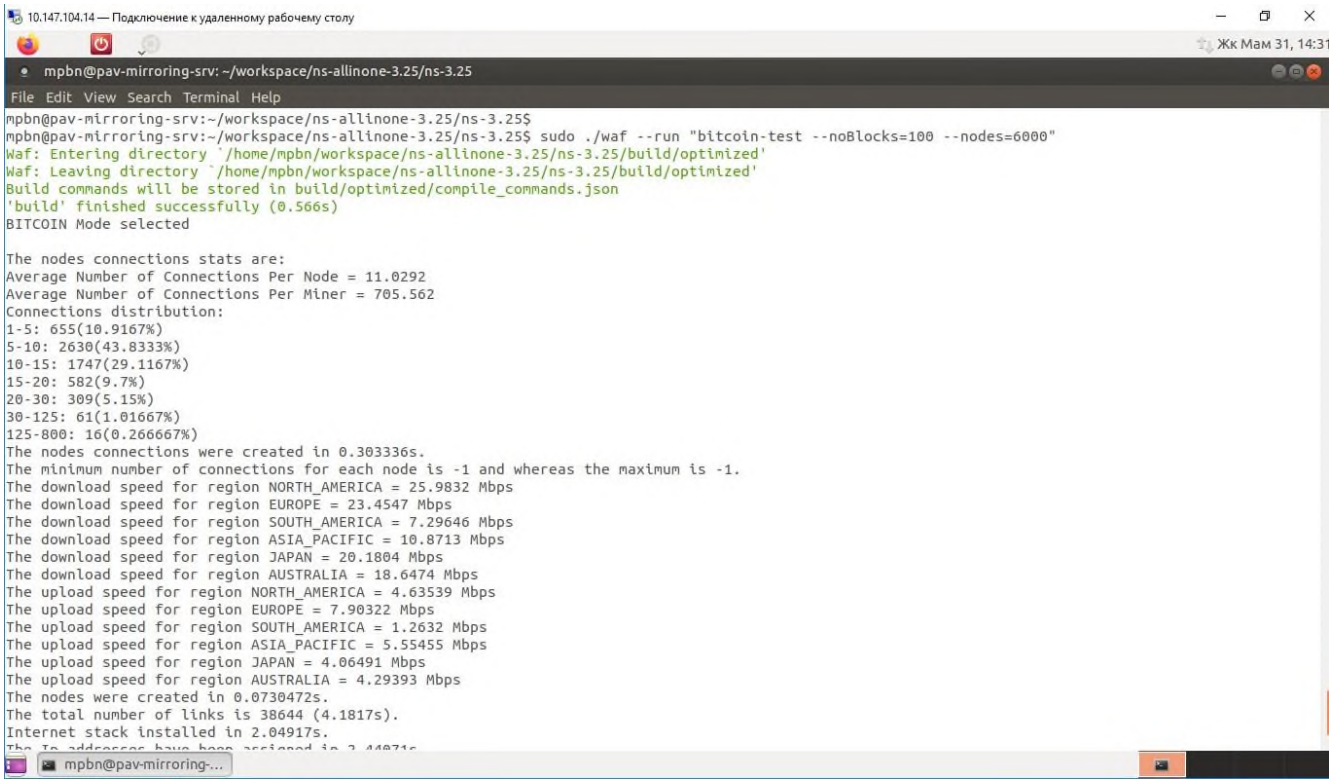

Рис. 3.2. Тестовий приклад симуляції для 100 блоків і 6000 вузлів зі стандартними параметрами

3.2.3. Перевірка симулятора.

З метою експериментальної перевірки симулятора порівнюються *Bitcoin*, *LiteCoin* і *DogeCoin* із симульованими аналогами.

Таблиця 3.2. Перевірка достовірності симулятора.

	Bitcoin	***Litecoin***	***Dogecoin***
Час генерації блоків, хв	10	2,5	1
Реальне значення — Середній час поширення блоку, сек	8,7	1,02	0,98
Симульоване значення. Середній час поширення блоку, сек	9,42	0,86	0,83
Реальне значення. Відсоток застарілих блоків, %	0,41	0,27	0,62
Симульоване значення. Відсоток застарілих блоків, %	0,15-1,85 (в залежно від використання ретрансляції та незапрошеного надсилання блоків)	0,24	0,79

Для кожного досліджуваного блокчейна скориговано вхідні параметри симулятора відповідно до їхніх реальних параметрів. Наприклад, виміряно розподіл блоків біткойнів за розміром, а також швидкість генерації блоків у реальній мережі біткойнів у період з травня по листопад 2015 року [28]. Щоб виміряти відсоток застарілих блоків у реальних мережах блокчейнів, перевірено 24 000 блоків біткойнів, 100 000 блоків *Litecoin* і 240 000 блоків *Dogecoin*[29].

Результати показують, що виміряний і змодельований середній час розповсюдження блоку близькі, як і показники застарілих блоків для *Litecoin* і

Dogecoin. У *Bitcoin* швидкість і час старіння блоків падає залежно від використання ретрансляційної мережі та незапрошеного надсилання блоків (*unsolicited block push*). У разі, коли ретрансляційна мережа і незапрошене надсилання блоків не використовуються ніким, швидкість старіння мінімальна. *Litecoin* і *Dogecoin* не використовують мережі ретрансляції і не схильні до цієї особливості.

3.3. Дослідження характеристик блокчейна під час інтеграції в мережах IoT.

3.3.1 Метрики та характеристики мережі під час інтеграції блокчейна в мережах *IoT*.

Визначимо п'ять важливих аспектів, яким повинна підкорятися оптимальна реалізація *PoW* для *IoT*: масштабованість, безпека, децентралізація, ефективність і пропускна здатність мережі. Далі проаналізуємо ці характеристики (Таблиця 3.3).

Масштабованість. Масштабованість в *IoT* — це можливість зміни мережі з точки зору кількості пристроїв, характеристик обладнання, а також функціональних вимог при збереженні продуктивності. Для блокчейна це означає, що потрібна однорангова мережа, яка може масштабуватися в кількості вузлів, пропускної спроможності, і в кількості транзакцій за одиницю часу.

Безпека. Безпека є критично важливим аспектом в *IoT*. Хоча в цій роботі не розглядається несанкціонований доступ до *IoT* пристроїв, проблема цілісності даних для пристроїв *IoT* є важливою проблемою, яку необхідно вирішити. У разі використання блокчейна цілісність даних гарантується за своєю архітектурою.

Децентралізація. Децентралізація в *IoT* має вирішальне значення для підвищення безпеки, конфіденційності та автономної роботи. В однорангових мережах, таких як блокчейни, децентралізація вимірюється кількістю правильно функціонуючих вузлів. У блокчейні, вузол повинен прийняти останній згенерований блок, перш ніж генерувати новий. Отже, визначаємо метрику для вимірювання децентралізації як кількість функціонуючих однорангових вузлів у мережі. Також визначаємо нижню межу функціонуючих однорангових вузлів, яка становить 90% від загального обсягу, щоб гарантувати належну функціональність блокчейна для *IoT*.

Ефективність. Ефективність в *IoT* можна визначити як оптимальне використання апаратних ресурсів та енергії. Тож для досягнення цього пристрою *IoT* у блокчейні мають оптимально використовуватися ресурси та енергія для підтримання та розвитку блокчейну. Серед іншого, перешкодою для цього є

проблема застарілих блоків у *PoW*. Зокрема, застарілі блоки погіршують безпеку блокчейна, і транзакції в застарілих блоках розглядаються мережею як необроблені, що потребує додаткових ресурсів для їхнього опрацювання. Отже, визначаємо метрику для ефективності як коефіцієнт генерації застарілих блоків, верхня межа якої дорівнює 1%.

Пропускна здатність мережі. Пропускна здатність мережі буде дорівнювати швидкості мережі *IoT*. Це визначається швидкостями низхідної лінії зв'язку і висхідної лінії зв'язку пристроїв *IoT*. Наприклад, стандарти *IEEE* 802.15.4 і *NarrowBand-IoT* встановлюють пікові швидкості передачі даних 250 Кбіт/с для зв'язку між комп'ютерами, тоді як у стандартах *LTE Cat M1* і *LTE Cat 0* це 1 Мбіт/с. Щоб уникнути перевантажень швидкість приймаємо рівною 250 Кбіт/с.

Таблиця 3.3 - Оптимальні характеристики

Характеристика	**Метрика**
Масштабованість	Максимальна кількість *IoT* пристроїв, максимальна кількість транзакцій на секунду
Децентралізація	$\frac{\text{90\% часу поширення блоку}}{\text{Час генерації блоку}} \leq 1$
Ефективність	Відсоток застарілих блоків ~1%
Мережева пропускна здатність	250 Кбіт/с

3.3.2. Налаштування симулятора.

Щоб використовувати симулятор для наших оцінок, класифікуємо пристрої *IoT* за двома ролями: майнери та звичайні пристрої. Кількість з'єднань на пристрій майнера та звичайний пристрій відповідає розподілу, як у роботі [29]. Звичайні пристрої лише перевіряють і поширюють отримані блоки, тоді як майнери також генерують нові блоки. Співвідношення майнерів до кількості вузлів дорівнює 7%, а решта беруть на себе роль звичайних пристроїв, це підтверджується певною

статистикою [30].

Мережева затримка відіграє критичну роль у продуктивності через природу однорангового розповсюдження інформації (тобто, блоку та транзакції). Отже, щоб оцінити, як географічне розташування пристроїв впливає на затримку в мережі, використовуємо налаштування симулятора для моделювання розташування пристроїв усередині однієї країни, у Європі та в усьому світі.

Пропускна здатність пристроїв *IoT*, очевидно, впливає на час поширення інформації в блокчейні. Щоб отримати реалістичне налаштування пропускної здатності, приймаємо еталони пропускної здатності пристроїв *Raspberry Pi*. Це призводить до різної пропускної здатності завантаження даних від 0,1 Мбіт/с до 100 Мбіт/с із середнім значенням 5 Мбіт/с і різної пропускної здатності надсилання даних від 0,02 до 20 Мбіт/с із середнім значенням 1 Мбіт/с.

3.3.3. Розмір блоку та інтервал генерації блоків.

Оцінимо вплив розмірів блоків та інтервалів генерації блоків за допомогою симулятора з умовою, що всі пристрої розташовані всередині однієї країни. Використовуємо цикл генерації з шести блоків з такими інтервалами: 10 хвилин, 5 хвилин, 1 хвилина, 30 секунд, 10 секунд і 5 секунд. Для кожного покоління блоків у циклі варіюємо розміри блоків: 10 КБ, 50 КБ, 100 КБ, 500 КБ, 1 МБ, 5 МБ, 10 МБ. Збільшимо кількість пристроїв IoT до 250 з 16 пристроями з ролями майнер. Результати представлені в Таблиці 3.4.

Це завдання виконується шляхом виставлення параметрів:

- "--*blockSize*" у діапазоні від 10000 до 10000000;
- "--*blockIntervalMinutes*" у діапазоні від 0.0.8(3) до 10;
- "--*nodes*" статично рівним 250;
- "--*miners*" статично рівним 16.

Приклад одного з експериментів наведено на рисунку 3.3.

```
mpbn@pav-mirroring-srv:~/workspace/ns-allinone-3.25/ns-3.25$ sudo ./waf --run "bitcoin-test --blockIntervalMinutes=1 --nodes=250 --blockSize=5000000 -
-miners=16"
Waf: Entering directory `/home/mpbn/workspace/ns-allinone-3.25/ns-3.25/build/optimized'



Waf: Leaving directory `/home/mpbn/workspace/ns-allinone-3.25/ns-3.25/build/optimized'
Build commands will be stored in build/optimized/compile_commands.json
'build' finished successfully (0.571s)
```

Рис. 3.3. Процес симуляції з інтервалом 1 хвилину і блоком, що дорівнює 5 *MB*.

Виходячи з вимог, зазначених у таблиці 3.3, побудуємо графіки залежності середньої утилізації (рис. 3.4), відсотка застарілих блоків (рис. 3.5) і кількості транзакцій (рис. 3.6) від розміру блоків та інтервалу генерації і проведемо подальший аналіз.

Таблиця 3.4. Розмір блоку та інтервал генерації блоків.

Розмір блоку	**Інтервал генерації блоків**	**Сумарне кількість блоків**	**Заста-рівші блоки**	**Справжні блоки**	**Відсоток застарілих блоків**	**Затримка розповсюд-ження**	**Швид-кість утилізації, *kbps***	**Кількість транзакцій на секунду**
10 МБ	10 хв	10,8	0,43	10,4	3%	360	276	69,3
	5 хв	18,8	0,9	17,9	8,83%	755	723	119,5
	1 хв	45,6	16	26,93	35,07%	2162	21215	197,5
	30 сек	51,2	26,6	24,6	47,99%	2412	49520	164,1
	10 сек	57,7	41,2	16,5	71,38%	2560	151046	110,2
	5 сек	64,2	48,2	16	75,00%	2665	273777	107,1
5 МБ	10 хв	10,2	0,26	9,9	2,6%	168	134	33,1
	5 хв	19,9	1	18,9	5,3%	180	288	63
	1 хв	67,3	12,1	55,2	17,99%	1888	8718	184
	30 сек	73,4	26,8	46,6	36,52%	2105	28528	155,5
	10 сек	84	56,5	27,5	67,18%	2472	100255	92
	5 сек	91,4	68,5	22,9	74,91%	2512	190671	76,4

Продовження таблиці 3.4.

Розмір блоку	**Інтервал генерації блоків**	**Сумарне кількість блоків**	**Заста-рівші блоки**	**Справжні блоки**	**Відсоток застарілих блоків**	**Затримка розповсюд-ження**	**Швидкість утилізації, kbps**	**Кількість транзакцій на секунду**
1 МБ	10 хв	12,3	0	12,3	0%	31	26	8,2
	5 хв	22,3	0	22,3	0%	32	53	14,9
	1 хв	92,4	3,4	89	3,71%	37	438	59,3
	30 сек	165,9	8,5	157,4	5,15%	818	3243	104,9
	10 сек	219,6	94,1	125,5	42,86%	1812	30259	83,7
	5 сек	232,5	128,7	103,8	55,37%	2183	69059	69,2
500 КВ	10 хв	9,6	0	9,6	0%	15	13	3,2
	5 хв	18,6	0	18,6	0%	15	26	6,2
	1 хв	92,1	1,6	90,5	1,71%	17	136	30,1
	30 сек	165,2	9,2	156	5,56%	18	639	52
	10 сек	346,5	101,4	245,1	29,25%	1665	14762	81,7
	5 сек	350,6	161,1	189,5	45,96%	1972	41378	63,2

Продовження таблиці 3.4.

Розмір блоку	**Інтервал генерації блоків**	**Сумарне кількість блоків**	**Застарівші блоки**	**Справжні блоки**	**Відсоток застарілих блоків**	**Затримка розповсюдження**	**Швидкість утилізації, kbps**	**Кількість транзакцій на секунду**
100 КВ	10 хв	9,3	0	9,3	0%	3,2	2	0,6
	5 хв	23	0	23	0%	3,2	5	1,5
	1 хв	99	0	99	0%	3,2	27	6,6
	30 сек	186,4	4,4	182	2,35%	3,2	54	12,1
	10 сек	537,3	22,8	514,5	4,25%	3,4	447	34,3
	5 сек	954,5	124,5	830	13,04%	99	7249	55,3
50 КБ	10 хв	11	0	11	0%	1,6	1	0,4
	5 хв	18,6	0	18,6	0%	1,6	2	0,6
	1 хв	96,3	0	96,3	0%	1,6	14	3,2
	30 сек	187,0	0,7	186,3	0,35%	1,6	28	6,2
	10 сек	562,0	10,2	551,8	1,82%	1,7	84	18,4
	5 сек	1120,4	43,4	1077	3,87%	1,8	931	35,9
10 КВ	10 хв	10,3	0	10,3	0%	0,4	0,3	0,1
	5 хв	21,6	0	21,6	0%	0,4	0,7	0,2
	1 хв	101	0	101	0%	0,4	3,5	0,7
	30 сек	193,3	0	193,3	0%	0,4	7	1,3
	10 сек	598,6	0	598,6	0%	0,4	21	4
	5 сек	1166,3	19,9	1146,4	1,71%	0,4	42	7,6

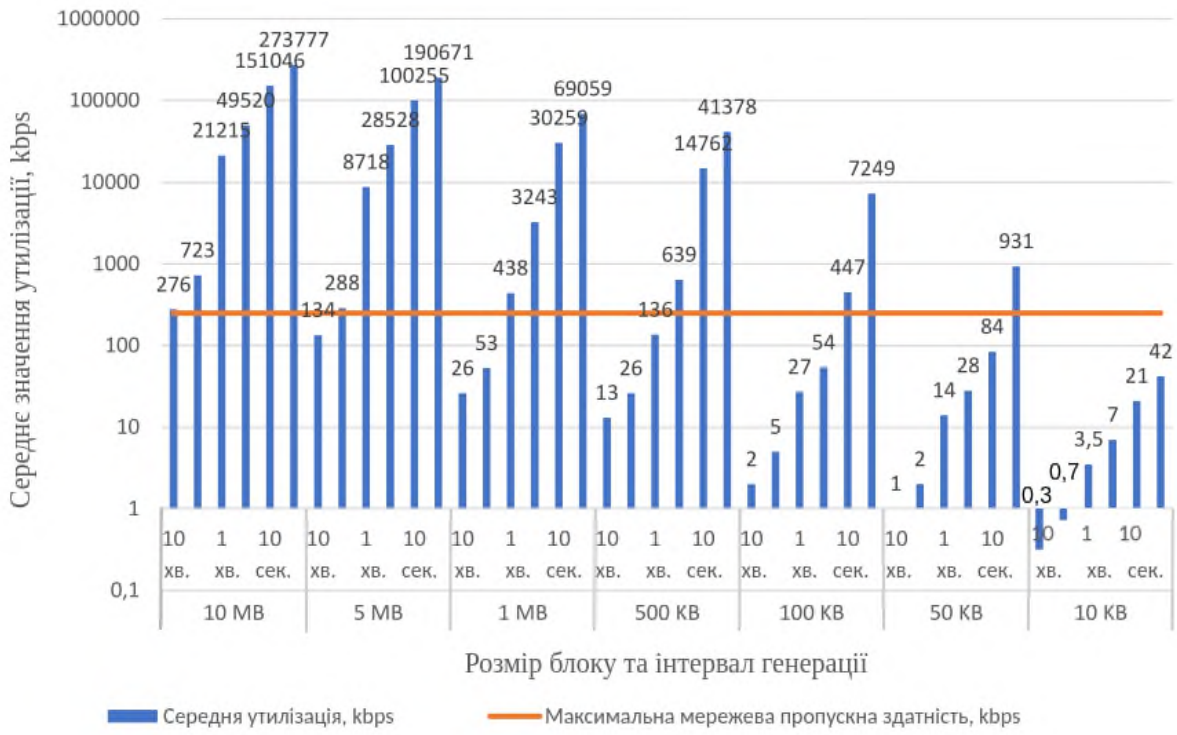

Рис. 3.4. Залежність середньої утилізації від розміру блоків та інтервалу генерації в логарифмічній шкалі.

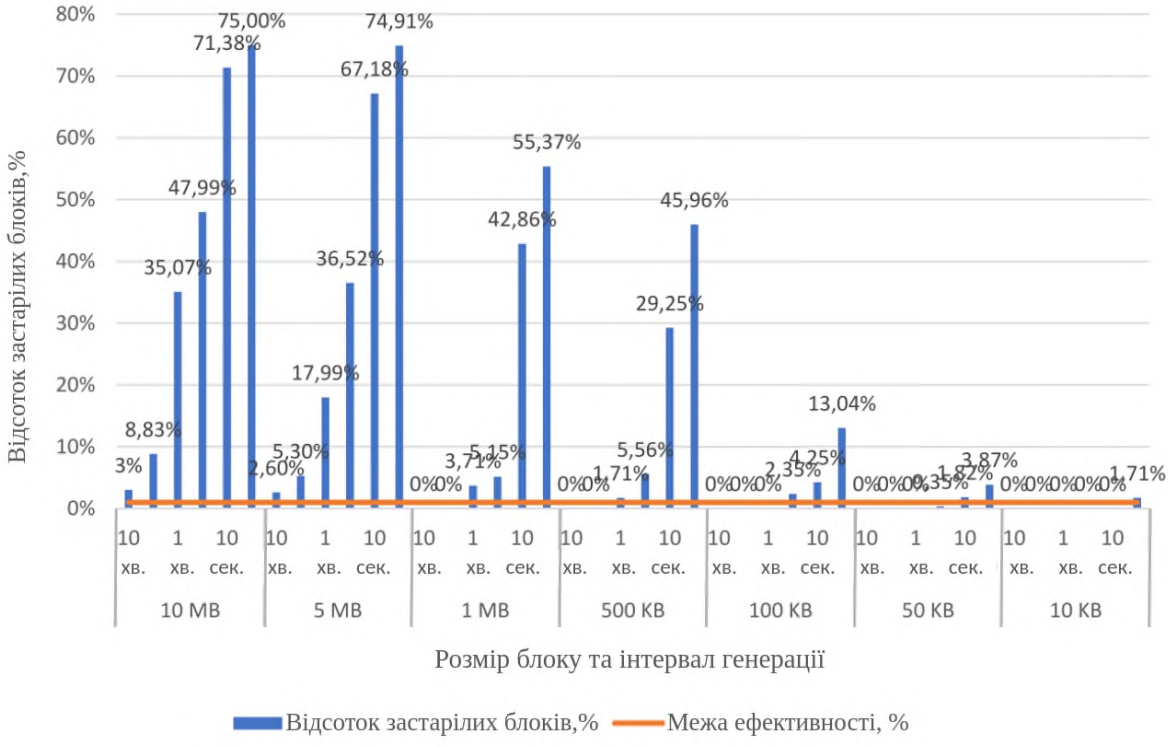

Рис. 3.5. Залежність відсотка застарілих блоків від розміру блоків та інтервалу генерації в логарифмічній шкалі.

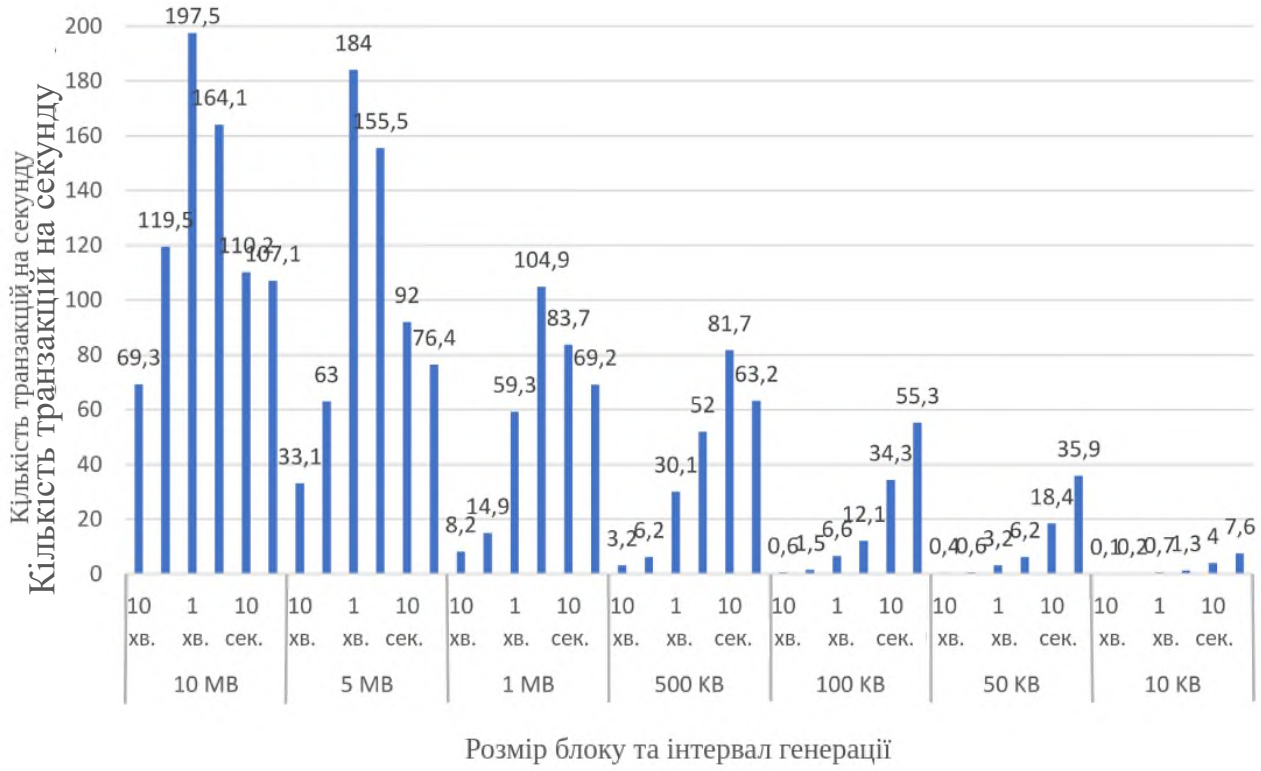

Рис. 3.6. Залежність кількості транзакцій на секунду від розміру блоків та інтервалу генерації.

Пропускна здатність мережі. Очевидно, що використання великих блоків та/або короткі інтервали генерації блоків збільшують середню кількість трафіку мережі. При цьому великі блоки (наприклад, 5 МБ) відповідають обмеженням пропускної здатності мережі (250 *kbps*), коли інтервал генерації блоків досить великий (наприклад, 5 хв.). Тоді як для невеликих блоків (наприклад, 10 КБ) підходять навіть короткі інтервали генерації блоків (наприклад, 5 с.).

Безпека. Очевидно, що використання коротших інтервалів генерації блоків збільшує кількість генерованих блоків. Однак це не пропорційно, особливо коли розмір блоку більший за 100 КБ. Так само в експериментах з 1-хвилинним або коротшим інтервалом генерації, збільшення розміру блоку зменшує кількість генерованих блоків. Це пов'язано з вичерпанням пропускної здатності пристроїв. Отже, відповідно до меж показника безпеки використання невеликих блоків (наприклад, 10 КБ) з короткими інтервалами генерації блоків (наприклад, 5 с) є більш придатним для збільшення кількості справжніх блоків.

Децентралізація. Згідно з межами метрики децентралізації, час поширення

блоку на 90% вузлів у мережі має бути меншим за інтервал генерації блоку. Через обмежені можливості смуги пропускання пристроям *IoT* доводиться витрачати більше часу на поширення великих блоків, що, своєю чергою, порушує обмеження часу поширення блоків на 90%. Також можна помітити, що під час використання великих блоків (наприклад, 10 МБ) інтервал генерації блоків має бути досить довгим (наприклад, 10 хв.), щоб задовольняти нижню межу децентралізації. Наприклад, коли використовуються невеликі блоки (наприклад, 10 КБ), умову децентралізації можна задовольнити з коротшими інтервалами генерації блоків (наприклад, 5 с). Тому, щоб домогтися децентралізації, розміри блоків та інтервали генерації блоків мають бути ретельно підібрані.

Ефективність, масштабованість. Короткі інтервали генерації блоків та/або використання великих блоків призводять до вищого відсотка застарілих блоків, оскільки смуга пропускання пристроїв IoT вичерпана під час поширення блоків. Для досягнення низького відсотка застарілих блоків під час встановлення короткого інтервалу генерації блоків можна використовувати тільки невеликі блоки. Великі блоки (наприклад, 1 МБ) можуть використовуватися з великими інтервалами генерації блоків. Що більший блок, то довший інтервал генерації блоку має використовуватися для задоволення межі генерації блоку з низьким відсотком застарілих блоків. Оскільки більше, розміри блоків понад 1 МБ не підходять для *IoT*. Досягнення низького відсотка застарілих блоків позитивно впливає на пропускну здатність транзакцій. В експериментах найвища досягнута пропускна спроможність, з урахуванням заявлених вимог, становить 30,1 транзакції за секунду за використання блоків по 500 КБ з налаштуванням інтервалу генерації блоків в 1 хвилину з частотою застарілих блоків 1,71%.

Висновки: слід використовувати блоки розміром менше ніж 1 МБ; інтервали генерації блоків мають бути якомога коротшими; розмір блоку та інтервали генерації блоку мають бути встановлені точно згідно з розрахунками, щоб забезпечити низький відсоток застарілих блоків і високу децентралізацію.

3.3.4. Географічне розташування пристроїв.

Проведемо оцінку впливу розташування пристроїв, варіюючи затримку в мережі між пристроями *IoT*. Щоб змоделювати це, використовуємо симулятор із трьома налаштуваннями місця розташування (всередині однієї країни, Європа і Світ). Оскільки з оцінки попереднього моделювання оптимальний розмір блоку має бути меншим або дорівнювати 1 МБ, розмір блоку в середньому становитиме 500 КБ. Використовуємо цикл генерації з шести блоків з такими інтервалами: 10 хвилин, 5 хвилин, 1 хвилина, 30 секунд, 10 секунд і 5 секунд. Також збільшуємо кількість пристроїв IoT до 250, де 16 із них є майнерами. Результати експерименту представлені в таблиці 3.5.

Для зміни топології мережі слід редагувати файл "*src/applications/helper/bitcoin-topology-helper.cc*", який містить опис розташування всіх елементів блокчейна.

Змінимо топологію згідно із завданням:

```
std::array<double,7> nodesDistributionIntervals {UKRAINE, EUROPE, WORLD};
 switch (m_cryptocurrency)
  {
    case BITCOIN:
     {
       if (m_systemId == 0)
      std::cout << "BITCOIN Mode selected\n";
      std::array<double,6> nodesDistributionWeights {1, 0, 0};
```

Таким чином, змінюючи параметр *nodesDistributionWeights*, ми проведемо кілька експериментів.

Таблиця 3.5. Географічне розташування пристроїв.

Інтервал генерації блоків	**Масштаб**	**Усього блоків**	**Застарілі блоки**	**Справжні блоки**	**Частка застарілих блоків, %**	**Затримка розповсюдження**	**Швидкість утилізації, *kbps***	**Кількість транзакцій за сек.**
10m	Країна	9,6	0	9,6	0	7	13	3,2
	Європа	9,9	0	9,9	0	16	13	3,3
	Світ	9,9	0	9,9	0	20	13	3,3
5m	Країна	18,6	0	18,6	0	6	26	6,2
	Європа	16,4	0	16,5	0	13	27	5,5
	Світ	15,5	0	15,5	0	17	27	5,2
1m	Країна	92,1	1,6	90,5	1,71	17	136	30,1
	Європа	93,6	4,8	88,8	5,14	18	140	29,6
	Світ	96,5	7,9	88,6	8,22	20	140	29,5
30s	Країна	165,2	9,2	156	5,56	18	639	52
	Європа	170,5	21,9	148,6	12,87	38	527	49,5
	Світ	169,5	23,9	145,6	14,11	52	592	48,5
10s	Країна	346,6	101,4	245,2	29,25	314	14762	81,7
	Європа	314	104,6	209,4	33,31	355	15237	69,8
	Світ	331	136,8	194,2	41,34	392	16777	64,7
5s	Країна	350,7	161,2	189,5	45,96	815	41378	63,2
	Європа	301,2	156	145,2	51,80	918	43931	48,4
	Світ	303,3	161,1	142,2	53,12	1000	45021	47,4

Виходячи з вимог, зазначених у таблиці 3.3, побудуємо графіки залежності відсотка застарілих блоків (рисунок 3.7) і кількості транзакцій (рисунок 3.8) від розміру блоків та інтервалу генерації і проведемо подальший аналіз.

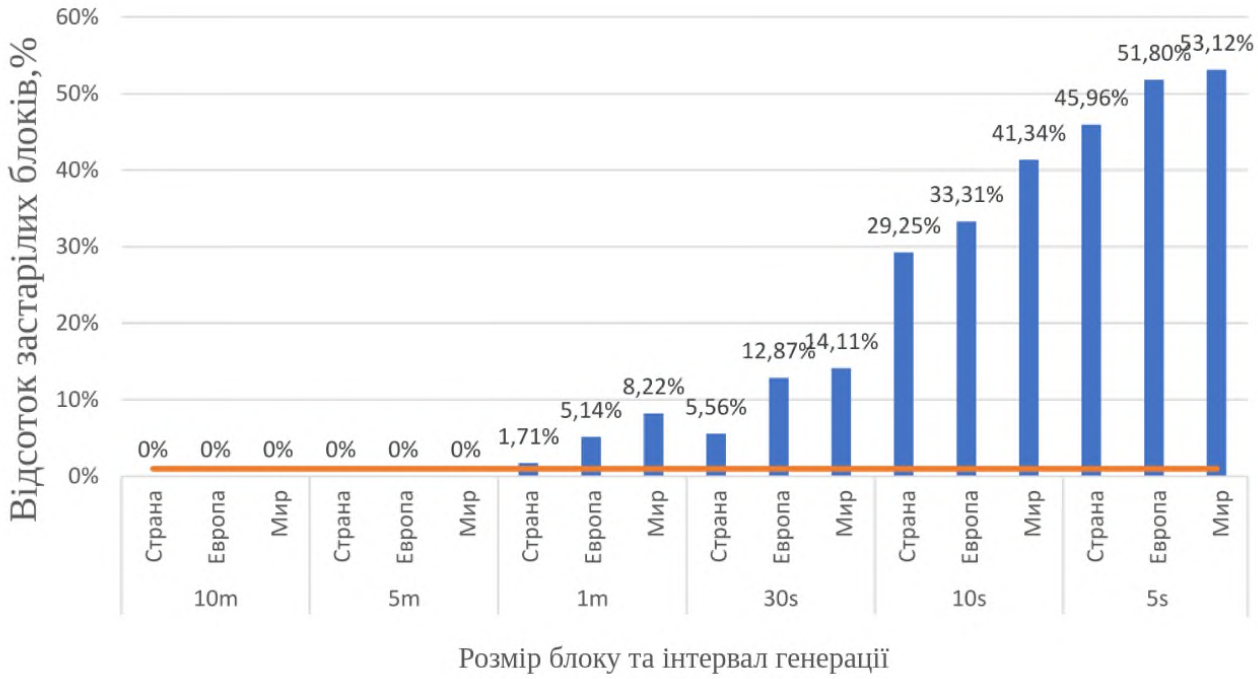

Рис. 3.7. Залежність відсотка застарілих блоків від мережевої затримки між вузлами та інтервалу генерації в логарифмічній шкалі.

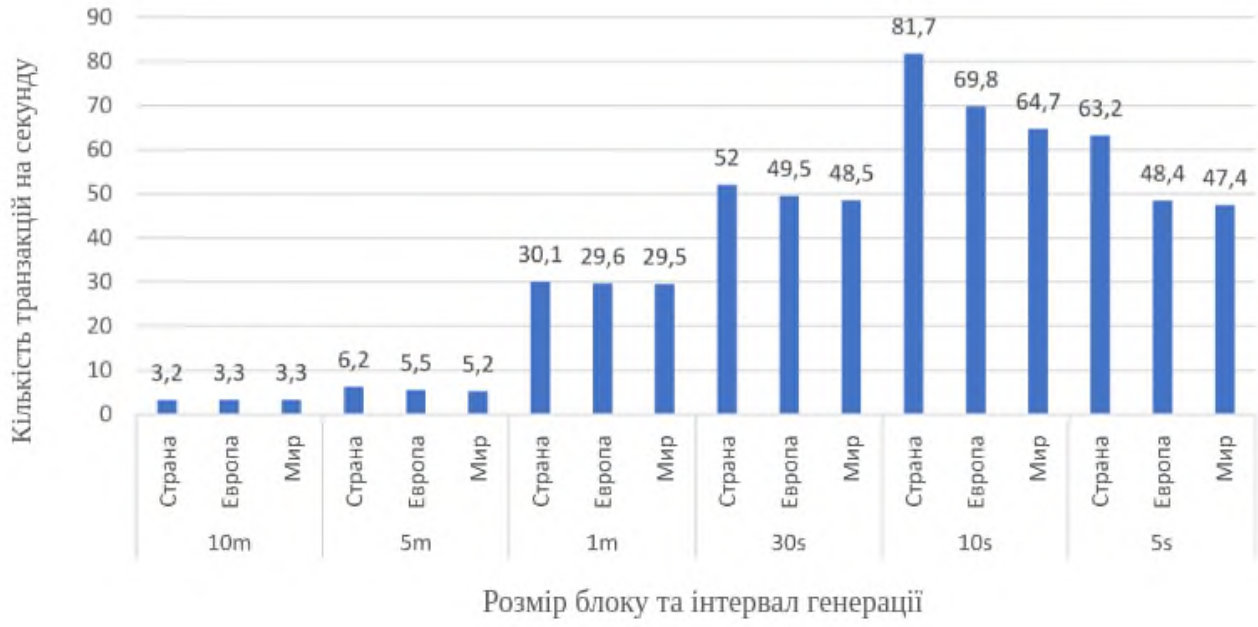

Рис. 3.8. Залежність кількості транзакцій на секунду від мережевої затримки між вузлами та інтервалу генерації в логарифмічній шкалі.

Пропускна здатність мережі, безпека. Для всіх місць розташування, у кожному інтервалі генерації блоку утилізація пропускної спроможності на кожен пристрій і кількість згенерованих справжніх блоків корелюють між собою. Зокрема, тільки

частота генерації блоків в 1 хвилину або більше може бути використана, оскільки тільки ці інтервали відповідають обмеженню для пропускної спроможності мережі (250 Кбіт/с) для всіх варіацій місця розташування. Отже, 1-хвилинний інтервал генерації блоку є найбільш підходящим з точки зору безпеки, оскільки він має найбільшу кількість справжніх блоків.

Масштабованість, децентралізація, ефективність. Для будь-якої симуляції, результат із найкоротшими затримками поширення блоків, найнижчими відсотками застарілих блоків і найвищими пропускними здібностями транзакцій буде отримано під час тесту всередині країни. Наприклад, з інтервалом генерації блоку в 1 хвилину блок-схема *PoW* з використанням налаштування всередині країни досягає пропускної спроможності 30,1 за секунду і відповідає метриці ефективності (швидкість застарівання блоку становить 1,71%) і метриці децентралізації (час поширення блоку 90% становить 17 секунд). Для порівняння в тестах Європи та Світу інтервал генерації блоку має становити щонайменше 5 хвилин, щоб відповідати тим самим характеристикам.

Висновки: блокчейни, що містять пристрої *IoT*, які географічно близькі один до одного, забезпечують вищу пропускну здатність за низької швидкості застарівання блоків.

3.3.5. Кількість пристроїв *IoT* в одному блокчейні.

Проведемо два виміри для оцінки оптимальної кількості *IoT* пристроїв в одному блокчейні зі змінними та фіксованим інтервалом генерації блоків. В обох тестах варіюємо кількість пристроїв *IoT* від 83 до 1250 і приймаємо розмір фіксованого блоку 500 КБ. У блокчейні *PoW* інтервал генерації блоків залежить від відношення складності головоломки *PoW* до сумарної потужності майнінгу системи [2]. Отже, зі зменшенням складності *PoW* задачі міняємо інтервали генерації блоків обернено пропорційно до кількості майнерів. В іншому вимірі, з фіксованим інтервалом генерації блоків, що дорівнює 1 хвилині, складність головоломки *PoW* варіюється пропорційно до кількості майнерів (складність головоломки *PoW*

становить α для 6 майнерів і 15α для 90 майнерів).

Це завдання виконується шляхом виставлення параметрів:

- "*--blockSize*" статично рівним 500000;
- "*--nodes*" у діапазоні від 83 до 1250;
- "*--blockIntervalMinutes*" у діапазоні від 0,2 до 3;
- "*--miners*" у діапазоні від 6 до 90.

Приклад симуляції цього експерименту наведено на рисунку 3.9. Експеримент (А). Результати наведено в таблиці 3.6.

```
mpbn@pav-mirroring-srv:~/workspace/ns-allinone-3.25/ns-3.25$ sudo ./waf --run "bitcoin-test
--blockIntervalMinutes=1 --nodes=250 --blockSize=500000 --miners=16"
/////
Часть вывода удалена
////
Total Stats:
Average Connections/node = 10.6282
Average Connections/miner = 164.938
Mean Block Receive Time = 59.8417 or 0min and 59.8417s
Mean Block Propagation Time = 8.3892s
Median Block Propagation Time = 6.20544s
10% percentile of Block Propagation Time = 3.62249s
25% percentile of Block Propagation Time = 4.37992s
75% percentile of Block Propagation Time = 7.89761s
90% percentile of Block Propagation Time = 16.9018s
Miners Mean Block Propagation Time = 5.09388s
Miners Median Block Propagation Time = 5.61457s
Mean Block Size = 500000 Bytes
Total Blocks = 92.1
Stale Blocks = 1.6 (1.71%)
The size of the longest fork was 1 blocks
There were in total 5.984 blocks in forks
/////
Часть вывода удалена
////
Total average traffic/node = 1.03401e+08 Bytes (136.139 Kbps and 1036.04 KB/block)
2.44119s per generated block
```

Рис. 3.9. Приклад звіту симулятора для експерименту (А).

Таблиця 3.6. Кількість пристроїв в одному блокчейні за змінного інтервалу генерації блоків.

Кіль-кість майнерів /вузлів	**Інтервал генерації блоків**	**Усього блоків**	**Заста-рілі блоки**	**Спра-вжні блоки**	**Частка заста-рілих блоків, %**	**Затри-мка розпо-всю-дження**	**Швид-кість утилі-зації, kbps**	**Кількість транзакцій на сек.**
6/83	3 хв	29,9	0	29,9	0	7	44	9,9
12/166	1,5 хв	76,7	1,3	75,4	1,9	8	88	25,1
16/250	1 хв	92,1	1,6	90,5	1,71	17	136	30,1
36/500	30 сек	177,7	15,6	162,1	8,8	41	1168	54
54/750	20 сек	237,2	32,9	204,3	13,87	147	3485	68,1
72/1000	15 сек	216,5	39,4	177,1	18,2	291	5791	59
90/1250	12 сек	212	47,5	164,5	22,43	498	8265	54,8

Наявність більшої кількості *IoT*-пристроїв з більш короткими інтервалами генерації блоків призводить до генерації більшої кількості блоків, що веде до збільшення пропускної здатності та кількості мережевого трафіку на пристрій. Це призводить до значного споживання смуги пропускання, що призводить до тривалих затримок поширення блоків. Отже, експериментальні варіанти, що містять 83, 166 і 250 пристроїв, задовольняють ефективності, пропускній здатності мережі та межам децентралізації. Коли мова заходить про масштабованість і межі безпеки, сценарій, що містить 250 пристроїв, є оптимальним, оскільки він генерує високий відсоток справжніх блоків, досягає максимальної пропускної здатності та масштабується для більшої кількості пристроїв.

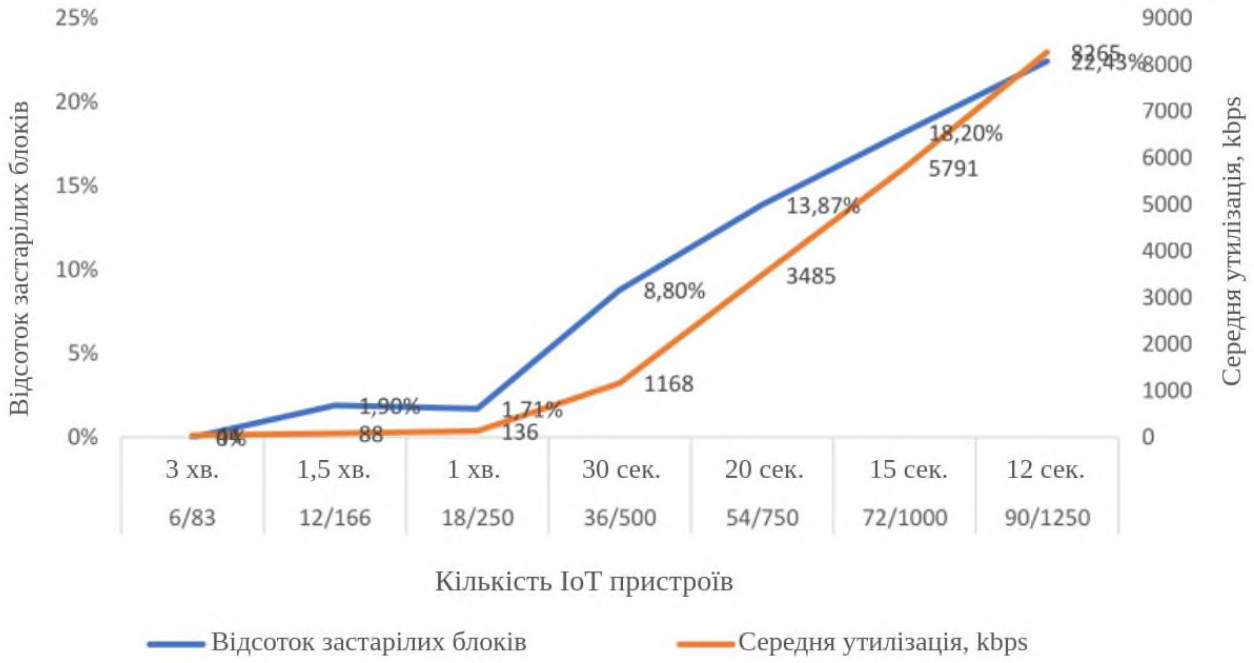

Рис. 3.10. Залежність відсотка застарілих блоків і середньої утилізації від кількості *IoT* пристроїв у логарифмічній шкалі.

Експеримент (Б). Результати наведено в таблиці 3.7.

Таблиця 3.7. Кількість пристроїв в одному блокчейні за постійного інтервалу генерації блоків.

Кількість майнерів/ вузлів	**Усього блоків**	**Складність**	**Застарілі блоки**	**Справжні блоки**	**Частка застарілих блоків, %**	**Затримка розповсюдження**	**Швидкість утилізації, kbps**	**Кількість транзакцій на сек.**
6/83	96,1	α	0,8	95,3	0,85	13	135,76	31,7
12/166	96,3	2α	1,8	94,5	1,19	14	133,37	31,1
18/250	92,1	3α	1,6	90,5	1,71	17	136	30,1
36/500	93,03	6α	3,99	89,04	4,29	26	122,99	32,86
54/750	93,41	9α	4,49	88,92	4,8	28	102,03	29,64
72/1000	93,03	12α	4,42	88,61	4,75	28	102,99	29,53
90/1250	92,77	15α	4,98	87,78	5,36	39	107,01	29,26

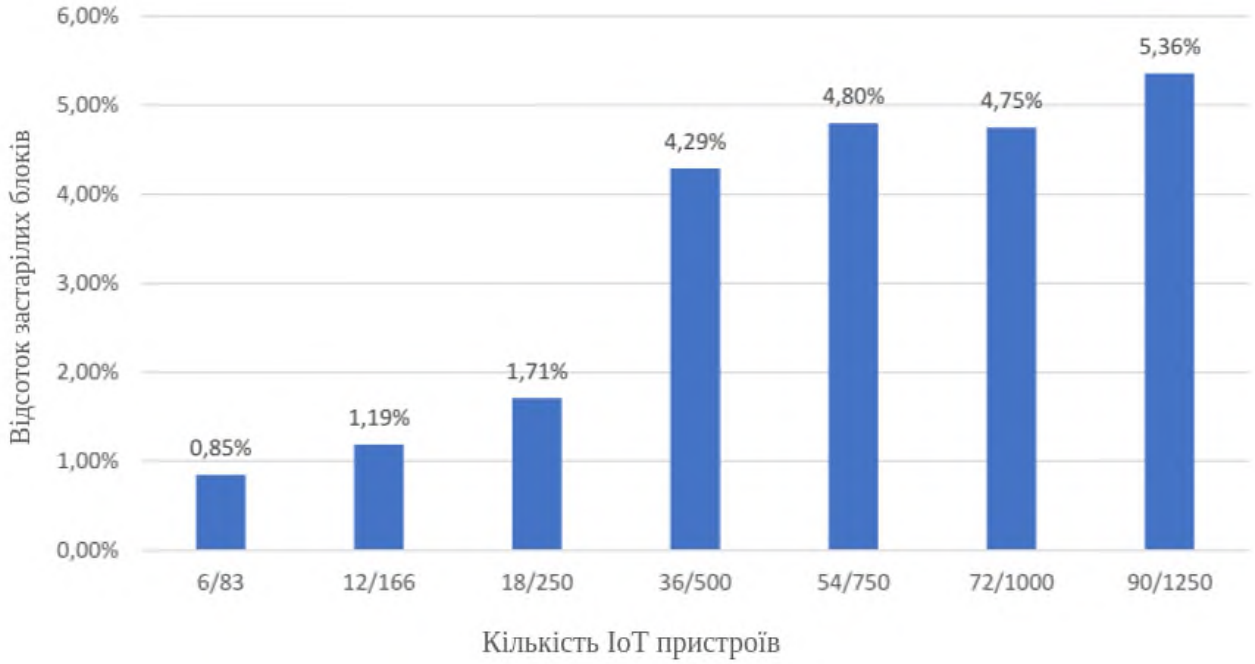

Рис. 3.11. Залежність відсотка застарілих блоків від кількості *IoT* пристроїв в логарифмічной шкалі.

У всіх експериментальних варіаціях 90% часу розповсюдження блоку становлять інтервал генерації блоку менше 1 хвилини, що відповідає межі децентралізації Для усіх варіантів дотримується умова щодообмеження пропускної спроможності у 250 кбіт/с, проте тільки експериментальні варіанти, які містять 83, 166 і 250 пристроїв, задовольняють ефективності, пов'язаній із частотою застарівання блоків. Серед них експеримент з 250 пристроями є оптимальним згідно з межами безпеки та масштабованості, оскільки він забезпечує максимальну пропускну здатність і масштабується на більшу кількість пристроїв.

Висновки: блокчейни *PoW*, що містять кілька сотень *IoT*-пристроїв, забезпечують вищу пропускну здатність транзакцій; оптимальна кількість *IoT*-пристроїв становить близько 250.

Висновки.

Під час виконання дослідження було проведено аналіз сучасних алгоритмів розподіленого зберігання та обробки даних. Розглянуто переваги блокчейна перед наявними системами зберігання даних, наведено основні технології, які використовуються на даний момент, і дано класифікацію систем. Також виокремлено основні обмеження технології: проблеми безпеки, проблеми масштабування і швидкості обробки даних, високі вимоги до ресурсів, пошук нових сфер застосування.

Розглядаючи проблеми, як основні сфери для дослідження і спираючись на ринковий стан технології загалом, був проведений аналіз застосування алгоритмів розподіленого зберігання в галузі *IoT*, охорони здоров'я та електронного голосування. Проведено аналіз наявних концепцій і протоколів використання блокчейна для гарантування чесності в проведенні виборів.

Відокремлено основні ризики, пов'язані з *IoT* і передачею конфіденційних даних через мережі передавання даних, зокрема, Інтернет. Основними проблемами вважаються: безпека даних, довіра до мережі, контроль відкритих підключень. Як випливає з аналізу, більшість ризиків можна знизити із застосуванням алгоритмів розподіленого зберігання даних. Було проведено дослідження впливу блокчейна на кожну з найважливіших характеристики *IoT* мережі: масштабованість, безпеку, децентралізацію, ефективність, пропускну здатність мережі.

Як середовище моделювання було обрано мережевий симулятор *NS3* разом із фреймворком *Bitcoin Simulator*. У результаті проведених вимірювань було виявлено, що блокчейни *PoW*, що містять кілька сотень пристроїв *IoT* у безпосередній географічній близькості, досягають найвищої продуктивності. Тому, щоб спроектувати архітектуру блокчейна для *IoT*, пропонується розгорнути безліч субблокчейнів *PoW* для групи пристроїв *IoT*, включно з такими рекомендаціями:

- субблокчейни мають містити кілька сотень *IoT*-пристроїв;
- субблокчейни повинні містити пристрої *IoT*, які географічно близькі і часто обмінюються даними один з одним;

- розмір блоку та інтервали генерації блоку мають бути встановлені для забезпечення низького відсотка застарілих блоків, а також високої децентралізації;
- блоки мають бути меншими або дорівнювати 1 МБ;
- інтервал генерації блоку має бути якомога коротшим.

Проведене дослідження засвідчило високу ефективність використання алгоритмів розподіленого зберігання та оброблення даних в *IoT*.

Список літератури.

1. Haber S., Stornetta W., How to Time-Stamp a Digital Document. -NewJersey: Bellcore South Street Morristown, 1991.
2. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System // [bitcoin.org] - 2008. URL: https://bitcoin.org/bitcoin.pdf
3. Tapscott D., Tapscott A. Blockchain revolution. - Portfolio, 2016. World Bank Group Distributed Ledger Technology (DLT) and Blockchain, // Open knowledge
4. World Bank Repository. - 2017. URL: https://openknowledge.worldbank.org/bitstream/handle/10986/29053/WP-PUBLIC-DistributedLedger-Technology-and-Blockchain-Fintech-Notes.pdf?sequence=1 .
5. Seebacher S., Schüritz R. Blockchain technology as an enabler of service systems: A structured literature review. // International Conference on Exploring Services Science: Springer. - 2017.
6. Antonopoulos M. Mastering Bitcoin: Programming the Open Blockchain. - O'Reilly Media, Inc., 2017.
7. Yli-Huumo J, Ko D., Choi S., Park S., Smolander K. Where Is Current Research on Blockchain Technology? — A Systematic Review. // PLoS ONE 11(10),2016.
8. Beikverdi A., Song J. Trend of centralization in Bitcoin's distributed network. // Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 16th IEEE/ACIS International Conference on. 2015.
9. OECD Digital Economy Outlook. // OECD Publishing. - 2017. URL: http://dx.doi.org/10.1787/9789264276284-en.
10. World Energy Council The Developing Role of Blockchain. White Paper. Version 1.0. -Pwc, 2017.
11. Jayachandran P. The difference between public and private blockchain. // [IBM] - 2017. URL: https://www.ibm.com/blogs/blockchain/2017/05/the-difference- between-public-and-privateblockchain/.
12. Blockchain Hub Blockchains & Distributed Ledger Technologies // [blockchainhub.net] - 2018. URL: https://blockchainhub.net/blockchains-and-

distributed-ledger-technologies-in-general/.

13. Vukoli´c M. The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. -English, 2017. -112–125 c.

14. Baliga A. Understanding blockchain consensus models. -Persistent, 2017. 15 V. Buterin A proof of stake design philosophy. // [medium.com] - 2017.

15. URL: https://medium.com/@VitalikButerin/aproof-of-stake-design-philosophy-506585978d51.

16. Szabo N. Smart Contracts // fon.hum.uva.nl - Phonetic Science, Amsterdam 1994. URL:www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

17. Murphy S., Cooper C. Can Smart Contracts Be Legally Binding Contracts // Norton Rose Fulbright. - 2016. URL: http://www.nortonrosefulbright.com/files/r3-andnorton-rose-fulbright-white-paper-full-report-144581.pdf

18. Gartner Hype Cycle Shows Most Blockchain Technologies Are Still Fiveto Years Away From Transformational Impact. // Gartner. - 2019. URL: https://www.gartner.com/en/newsroom/press-releases/2019-10-08-gartner-2019-hype-cycle-shows-most-blockchain-technologies-are-still-five-to-10-years-away-from-transformational-impact

19. Нугманов Д.М., Лещинская Э.М. Повышение конфиденциальности и безопасности данных в сети IoT с помощью алгоритмов децентрализованного хранения и обработки данных // Поиск.- 2019.- №3(1). С. 279-283.

20. Тихвинский В.О., Бочечка Г.С., Нургожин Б.И., Айтмагамбетов А.З. Сети IoT/M2M: технологии, приложения и регулирование. 2016.

21. Newsroom G. Gartner Says Worldwide IoT Security Spending Will Reach $1 Billion in 2018 // Gartner. - 2017. URL: https://www.gartner.com/newsroom/id/

22. The Internet of Things: a movent, not a market // IHS Markit. - 2018. URL: http://cdn.ihs.com/www/pdf/IoT_ebook.pdf

23. Zhang P., Schmidt D., White J., Lenz G., Blockchain technology use cases in healthcare. In Advances in Computers. Amsterdam: -Elsevier, 2018. -1–41c.

24. Chiuchisan, I., Costin, H., Geman, O. Adopting the internet of things technologies

in health care systems. // International Conference and Exposition on Electrical and Power Engineering, Iasi, Romania. 16 Октября 2014. – С -532 с.

25. Lobato F. Decentralized, Transparent, Trustless Voting on the Ethereum Blockchain. // International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056. - 2017.

26. Thomas R., Mathieu L., Riley G. Network simulations with the ns-simulator. // SIGCOMM. - 2008. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.415.6550&rep=rep1&type=pdf

27. Балашов В. Обзор сетевого симулятора NS3 // Харьковский Исследовательский Институт Судебных Экспертиз им. заслуженного профессора Н. Бокариуса. - 2010. URL: https://lvee.org/ru/reports/LVEE_2010_31

28. Karame G., Androulaki E., Capkun S. Double-spending fast payments in bitcoin. // ACM conference on Computer and communications security. - 2012. - С.906–917.

29. Blockchain Explorer. Search the tour Blockchain. // [blockchain.info]- 2010. URL: blockchain.info

30. Miller A. Discovering bitcoin’s public topology and influential nodes // University of Maryland. - 2015. URL: https://www.cs.umd.edu/projects/coinscope/coinscope.pdf