Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)

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

Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломної роботи

Магістр
(освітній ступінь)

на тему: Алгоритмічне та програмне забезпечення технології Blockchain при побудові мережевої ієрархічної структури

Виконав: студент (ка) 6 курсу, групи СІм-62
спеціальності
123 Комп'ютерна інженерія
(шифр і назва спеціальності)

(підпис) Дарморадський Л. О.
(прізвище та ініціали)

Керівник (підпис) Луцків А. М.
(прізвище та ініціали)

Нормоконтроль (підпис) Тима Є. В.
(прізвище та ініціали)

Рецензент (підпис) Сікорський О. Л.
(прізвище та ініціали)

м. Тернопіль – 2019

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)

Факультет комп'ютерно-інформаційних систем і програмної інженерії
Кафедра комп'ютерних систем та мереж
Освітній ступінь магістр
Напрям підготовки
(шифр і назва)
Спеціальність 123 Комп'ютерна інженерія
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри КС
Осухівська Г. М.
«30» 09 2019 р.

З А В Д А Н Н Я
НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ

Дармограй Василю Олеговичу
(прізвище, ім'я, по батькові)

1. Тема роботи Алгоритмічне та програмне забезпечення технології Blockchain при побудові мережевих IoT-інфраструктур

Керівник роботи Луцків Андрій Мирославович, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом по університету від «27» 09 2019 року № 4/7-857
2. Термін подання студентом роботи 27 грудня 2019 року
3. Вихідні дані до роботи Архітектура IoT-інфраструктури з використанням технології Blockchain та аналіз її ефективності та продуктивності

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1 Огляд предметної області
2 Аналіз технології Blockchain в контексті IoT
3 Опрацювання запропонованого підходу
4 Обґрунтування економічної ефективності
5 Охорона праці та безпека в надзвичайних ситуаціях
6 Екологія

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1 Алгоритмічне та програмне забезпечення технології Blockchain при побудові мережевих IoT-інфраструктур. 2 Архітектура програмного забезпечення. 3 Вузли майнерів. 4 Процес зберігання, доступу та моніторингу транзакцій. 5 Середній час обробки ОЗУ для зберігання нових блоків. 6 Оцінка впливу [illegible] та [illegible]. 7 Оцінка накладних витрат у LDM. 8 Оцінка впливу [illegible] ОЗУ на блоки та накладні витрати [illegible] на мережеві IoT-інфраструктури. 10 Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата завдання видав	Підпис, дата завдання прийняв
Економіка	Несторова Л.М., доц.	[illegible]	[illegible]
Структ. екон. сфери	Кирич Н.Б.	[illegible]	[illegible]
Безпека в НС	Стрілець В.Є., ст. викл. каф. ОХ	[illegible]	[illegible]
Охорона праці	Осухівська Г.М.	[illegible]	[illegible]

7. Дата видачі завдання 30.09.2019

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	30.09.19	виконав
2	Аналіз завдання	2.10.19	виконав
3	Огляд літератури щодо завдання	7.10.19	виконав
4	Сфери застосування технології IoT та Blockchain	9.10.19	виконав
5	Огляд вимог до [illegible]	13.10.19	виконав
6	Транзакції в Blockchain	16.10.19	виконав
7	Особливості використання Blockchain на [illegible]	18.10.19	виконав
8	Аналіз технології Blockchain в компанії IoT	20.10.19	виконав
9	Розробка розподіленого [illegible]	1.11.19	виконав
10	Налагодження транзакцій	2.11.19	виконав
11	Розробка застосованого підходу	4.11.19	виконав
12	Доступ до розумного [illegible] з налаштуванням	7.11.19	виконав
13	Обґрунтування економічної ефективності	15.11.19	виконав
14	Охорона праці та безпека в надзвичайних ситуаціях	19.11.19	виконав
15	Оформлення пояснювальної записки	21.11.19	виконав
16	Оформлення графічної частини	23.11.19	виконав
17	Захист роботи	22.11.19	

Студент ________ (підпис) Дармограй В. О. (прізвище та ініціали)

Керівник роботи ________ (підпис) [illegible] (прізвище та ініціали)

Зміст

ПЕРЕЛІК СКОРОЧЕНЬ

Access Control List (ACL)	Список контролю доступу
Block Managers (bm)	Менеджер блоків
Blockchain (BC)	Блокчейн
Certificate Authority (CA)	Орган з сертифікації
City Information Model (CIM)	Міська інформаційна модель
Cluster Head (CH)	Голова кластера
Distributed Throughput Management (DTM)	Управління розподіленою пропускною здатністю
Enterprise Resource Planning (ERP)	Планування ресурсів підприємства
Immutable Ledger (IL)	Локальний змінний кодекс
Internet of Things (IoT)	Інтернет речей
Lightweight scalable blockchain (LSB)	Легкий масштабований блокчейн
Local Block Managers (lbm)	Локальний менеджер блоків
Management of electronic health records (EHR)	Управління електронними медичними записами
Near Field Communications (NFC)	Полеві комунікації
Overlay Block Managers (OBM)	Менеджери накладених блоків
Peer to Peer (P2P)	Технологія рівний до рівного
Percentage of transactions to be verified (PTV)	Відсоток транзакцій, який потрібно підтвердити
Proof of Stake (PoS)	Доказ частини виконаної роботи
Proof of Work (PoW)	Доказ виконаної роботи
Public Key Infrastructure (PKI)	Інфраструктура відкритого ключа
Public Keys (PK)	Відкритий ключ
Radio Frequency IDentification (RFID)	Радіочастотна ідентифікація
Service Provider (SP)	Постачальник послуг
The Service Oriented Architecture (SOA)	Сервісно орієнтована архітектура
Cloud service provider (CSP)	Хмарний постачальник послуг

ВСТУП

Актуальність теми: IoT з кожним днем все збільшується та отримує все більш вагомі позиції в світі. Незважаючи на свій бурхливий розвиток IoT-мережі пристроїв можна характеризувати, як невпорядкованістю так і відсутністю чітких стандартів. Завдяки цьому безпека даних користувачів є під небезпекою. Тому Blockchain технологія, яка є ланцюжком блоків транзакцій, й, водночас, розподілена база даних, що зберігає впорядкований ланцюжок записів являє собою сильним доповненням до стабільності та захищеності постійно зростаючої IoT-системі.

Тому технології Blockchain для IoT-інфраструктур є актуальним напрямком досліджень саме на сьогоднішній день, у час, коли технології швидко розвиваються, а єдиних стандартів не існує.

Мета та задачі дослідження: Метою даної роботи є розроблення архітектури IoT-інфраструктури з використанням технології Blockchain та аналіз її ефективності та стресостійкості. Для досягнення вказаної мети в рамках дипломної роботи було сформульовано та розв’язано наступні задачі:

- Проаналізовано сучасний стан технологій IoT та Blockchain.
- Розглянути предметну область та проаналізовано спільне застосування технології Blockchain та IoT.
- Визначити проблематику та галузі їх можливого застосування. Визначити основні небезпеки несанкціонованого доступу до мережі та протидію йому.
- Оцінити та провести тестування ефективності, продуктивності та можливості масштабування мережі.
- Проаналізувати технології Blockchain в мережевій інфраструктурі IoT. Визначити ключові елементи керування мережею та її можливості.
- Оцінити стресостійкість мережі та її захист від атак зловмисника.

Предмет дослідження: Однорангові IoT-інфраструктури та методи передавання даних у них.

Об’єкт дослідження: Технологія Blockchain як засіб забезпечення захищеності IoT-інфраструктури.

Методи дослідження: Одним із методів тестування технології є програма Cooja яка добре підходить для оцінки низькоресурсних пристроїв і надає перевагу доступності впровадження різних протоколів, відомих IoT. Використання програми NS3 дозволить оцінки продуктивність накладення, оскільки вона широко застосовується для аналізу однорангових мереж.

Наукова новизна одержаних результатів

Проведено аналіз використання технології Blockchain в IoT-інфраструктурах і показано можливості їх сумісного використання.

Узагальнено та сформовано рекомендації, які дають змогу спростити процес масштабування інфраструктури.

Проведено експеримент в ході якого було проведено тестування сумісності технологій та їх продуктивність.

Практичне значення одержаних результатів

Розроблені рекомендації та здійснені тестування дають змогу спростити IoT-інфраструктуру при її масштабуванні.

Публікації

Результати дослідження апробовано на II міжнародні студентські науково-технічні конференції «Природничі та гуманітарні науки. Актуальні питання» м. Тернопіль 25-26 квітня 2019 року та VIII Міжнародній науково-технічній конференції молодих учених та студентів «Актуальні задачі сучасних технологій» м. Тернопіль 27-28 листопада 2019 року.

Структура роботи

Робота складається з пояснювальної записки та графічної частини. Пояснювальна записка складається із вступу, 3 розділів, висновків, список використаних джерел та додатку. Обсяг роботи: пояснювальна записка – 118 аркушів формату А4, графічна частина – 10 аркушів формату А1.

РОЗДІЛ 1
ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

1.1. Інтернет речей

Інтернет речей (IoT) - парадигма, яка швидко набирає позиції в сучасних бездротових телекомунікаціях. Основна ідея цієї концепції - всебічна присутність навколо нас різноманітних речей або предметів - таких, як RFID, різноманітні аксесуари та гаджети, тощо - які завдяки прописаним схемам адресації здатні взаємодіяти між собою та налагоджувати роботу із своїми сусідами для досягнення цілей їхніх власників.

Безперечно, головною концепцією IoT є сильний вплив, на різноманітні напрямки повсякденного життя власників. Найбільш явні ефекти впровадження IoT будуть помітні у робочих аспектах, та і у приватному житті IoT та все більше оточуватимуть нас. Допомога в житті людини, електронне здоров'я, всебічне навчання - лише декілька прикладів можливих варіантів застосування, коли нова стратегія відіграватиме основну роль у найближчому майбутньому. На сьогоднішній день, найбільш очевидні просування помітні в таких сферах, як, автоматизація на виробництві, логістика, управління бізнесом, GPS супровід як людей так і різноманітних товарів.

NIC передбачає, що «до 2025 року Інтернетвузли можуть міститись у повсякденних речах, прикрасах, одягу, паперових документах, та інше» [18]. NIC підкреслює майбутні можливості, які виникнуть, виходячи з ідеї, що «попит населення в поєднанні з прогресом технологій може призвести до широкого розповсюдження Інтернету речей (IoT), що може, як і нинішній Інтернет, неоціненно сприяти економічному розвитку». Підкреслюються також можливі загрози, що випливають із широкого впровадження такої технології. Особливо, підкреслюється, що «в тій мірі, коли повсякденні об'єкти стають ризиками інформаційної безпеки, IoT може поширювати ці ризики набагато ширше, ніж інтернет досі» [18].

Безліч складних рішень все ще потрібно прийняти і технологічні, і соціальні вузли повинні бути вирішені, перш ніж концепція IoT отримає широке прийняття. Методи позбавлені центрального управління дозволяють зробити повну сумісність взаємопов’язаних гаджетів, забезпечуючи їм завжди більш високий ступінь «розумності», їх адаптацію та автономну поведінку, гарантуючи при цьому довіру, конфіденційність та безпеку. Також ідея IoT нашому погляду кілька нових проблем, що стосуються комунікаційних аспектів. Насправді периферійні пристрої, що складають IoT, використовуватимуть малу кількість ресурсів як з точки зору розрахунків, так і з енергетичних виртат. Запропоновані рішення мають проявити пристальну увагу не тільки проблематиці масштабованості а й ефективності використання ресурсів.

На сьогоднішній день вирішенням розробки рішень для забезпечення виділених технологічних вимог, переймаються не тільки промислові а й дослідницькі організації.

1.2. Спільне застосування технології IoT та Blockchain

Потенціали, запропоновані IoT, дають можливість розробити величезну кількість застосувань, з яких на сьогодні нашому суспільству доступна лише дуже мала частина. Багато областей і середовищ, в яких нові програми, ймовірно, покращать якість нашого життя: вдома, під час подорожі, коли хворі, на роботі, і в тренажерному залі. Ці середовища тепер оснащені об'єктами лише примітивного інтелекту, більшість без будь-яких комунікаційних можливостей. Надання цим об'єктам можливості спілкуватися один з одним та обробку інформацію, сприйняту з навколишнього середовища, означає наявність різних середовищ, де можна розгорнути дуже широкий спектр програм. Вони можуть бути згруповані в наступні домени:

- транспортно-логістичний домен;
- домен охорони здоров'я;

- розумне середовище (будинок, офіс, підприємство);
- особиста та соціальна сфера.

Серед можливих застосувань можемо виділити ті, що безпосередньо застосовуються або наближаються до наших сучасних життєвих звичаїв, і ті футуристичні, про які ми можемо лише уявити на даний момент, оскільки технології та наші суспільства не готові до їх розгортання.

1.2.1. Транспортно-логістичний домен. Удосконалені автомобілі, поїзди, автобуси, велосипеди, а також дороги та/або рейки стають все більш оснащеними датчиками, приводами та потужністю обробки. Самі дороги та перевезені вантажі також обладнані мітками та датчиками, які надсилають важливу інформацію на сайти контролю руху та транспортні засоби для кращого маршрутного руху, допомагають в управлінні депо, надають туристу відповідну інформацію про перевезення та стежать за станом перевезений товар.

Технологія обробки інформації в реальному часі на основі RFID та NFC дозволяє реалізувати моніторинг у реальному часі майже кожної ланки ланцюга поставок, починаючи від товарного дизайну, закупівлі сировини, виробництва, транспортування, зберігання, дистрибуції та продажу напівфабрикатів і продуктів, уся ця інформація надходить на обробку та сервісне обслуговування. Також можна отримати інформацію, що стосується продукції, оперативно, своєчасно та точно, щоб підприємства чи навіть весь ланцюжок поставок могли реагувати на складні та мінливі ринки в найкоротші терміни. Результатом заявки є те, що час реакції традиційних підприємств становить 120 днів від вимог клієнтів на поставку товару, тоді як просунутим компаніям, які використовують ці технології (такі як Wal-mart та Metro), потрібно лише кілька днів, і вони можуть працювати в основному нульовий запас [18]. Крім того, доступ у режимі реального часу до програми «планування ресурсів підприємства» допомагає торговцям-помічникам краще інформувати покупців про наявність продуктів та надавати їм більше інформації про товар в цілому.

З точки зору Блокчейн технології. Управління ланцюгами поставок фізичних та цифрових товарів на блокчейні аналогічно застосуванню смарт-контракту. У цьому додатку товари позначаються цифровим значенням (наприклад, код, який можна сканувати для фізичних товарів, або трекер для цифрових товарів), і коли він переходить від однієї сутності до іншої, ця організація приймає її, а потім передає її іншій, використовуючи її публічно-приватний ключ. Ці транзакції додаються до блокчейн, тому різні учасники можуть відстежувати розпорядження товарами від створення через розподіл, роздрібну торгівлю та, можливо, до кінцевого споживача. Однак ця система дозволить лише бачити підзвітність того, яка сторона мала контроль над предмет в реальному світі, в який момент. Оскільки сам елемент не містить відстежуваного коду, його слід скріпити трекером, таким як код, який можна сканувати, або датчик, який дозволяє його відстежувати. Хтось із цього ланцюга може все-таки маніпулювати предметом, змінювати трекери чи іншим чином підробляти предмети в ланцюзі постачань, які можуть не входити в блокчейн. Прикладом управління ланцюгами поставок на блокчейн-платформі є відстеження корисних копалин Демократичної Республіки Конго, які будуть використовуватися для виготовлення акумуляторів.

1.2.2. Домен охорони здоров'я. Відстеження - це функція, спрямована на ідентифікацію людини чи предмета в русі. Це включає як відстеження положення в реальному часі, наприклад, моніторинг потоку пацієнтів для поліпшення робочого процесу в лікарнях, так і відстеження руху через задушні точки, наприклад, доступ до визначених місць. Щодо активів, відстеження найчастіше застосовується для постійного відстеження місця інвентаризації (наприклад, для технічного обслуговування, наявності або необхідності та моніторингу використання) та відстеження матеріалів для запобігання залишків під час операції, таких як препарати крові.

Ідентифікація та автентифікація включає в себе ідентифікацію пацієнта для зменшення випадків, шкідливих для пацієнтів (таких як неправильне

вживання лікарських засобів/дози/часу/процедури), всебічне та поточне ведення електронних медичних записів (як у стаціонарах, так і в амбулаторних умовах) та ідентифікація немовлят у лікарнях для запобігання невідповідності. По відношенню до персоналу, ідентифікація та автентифікація найчастіше використовуються для надання доступу та поліпшення моралі співробітників шляхом вирішення питань безпеки пацієнтів. Що стосується активів, то ідентифікації та автентифікації переважно застосовують, щоб уникнути крадіжок або втрат важливих інструментів та продуктів.

Було чи мало найрізноманітніших пропозицій щодо використання блокчейн у галузі охорони здоров’я, багато з яких стосуються управління електронними медичними записами (EHR). Однією з таких пропозицій є використання блокчейн для аутентифікації пацієнтів та медичних працівників на блокчейні для того, щоб дозволити спільний доступ до EHR. У цій пропозиції EHR проводиться в системі, на якій розміщений постачальник послуг, але існування запису публікується до блокчейн, і пацієнт може використовувати блокчейн для дозволу, хто може мати доступ до цього запису. Однак застосування блокчейн для охорони здоров’я позначає як юридичні закони та закони про конфіденційність у галузі охорони здоров'я, які можуть перешкоджати його використанню.

1.2.3. Домен розумних середовищ. Датчики та пускачі, що розповсюджуються в будинках та офісах, можуть зробити наше життя більш комфортним у кількох аспектах: опалення приміщень можна адаптувати до наших уподобань та у відповідності до погоди; освітлення кімнати може змінюватися залежно від часу доби; домашніх інцидентів можна уникнути відповідними системами моніторингу та сигналізації; а енергію можна заощадити, автоматично відключивши електрообладнання, коли це не потрібно. Логіка автоматизації може оптимізувати витрати споживання електроенергії протягом дня, спостерігаючи, коли ціни, що надаються зовнішньою веб-службою та встановлюються відповідно до поточного виробництва та

споживання енергії, дешеві та враховуючи конкретні вимоги кожної техніки на для дому (зарядний пристрій, холодильник).

1.2.4. Особиста та соціальна сфера. Соціальні мережі як додаток пов'язаний з автоматичним оновленням інформації про нашу соціальну діяльність на веб-порталах соціальних мереж, таких як Twitter та Facebook. Користувацькі інтерфейсні програми відображають канал подій, попередньо визначений їхніми друзями, і користувачі можуть контролювати свої списки друзів, а також те, які події розкриваються друзям.Ідея міської інформаційної моделі (CIM) заснована на концепції, що стан та ефективність кожної будівлі та міських елеменів - таких як пішохідні доріжки, велосипедні доріжки та більш важка інфраструктура, як каналізація, залізничні лінії та автобусні коридори - постійно контролюються. міська влада діє та надає третім повноваження особам через низку API, хоча деяка інформація є конфіденційною. Відповідно, нічого не можна будувати на не законних підставах, якщо воно не сумісне з CIM. Служби управління об'єктами спілкуються між собою та CIM, обмінюючись енергією найбільш рентабельно та ресурсоефективно. Вони автоматично торгують надлишки енергії між собою, а ціни розраховуються відповідно до попиту та пропозиції. У цьому сенсі планування та проектування - це постійний соціальний процес, в якому про результати роботи кожного елемента повідомляється в режимі реального часу та порівнюється з іншими. Відповідно до змін та скопичень людей в конкретних місцях CIM може зробити висновок, як змінити схеми руху громацького транспорту.

Використання блокчейну для соціальної та особистої сфери зводиться до управління ідентичністю яке сприймає асиметричне шифрування та незмінні транзакції як сильні сторони. У цьому використанні користувач має приватний ключ для перевірки транзакцій, зроблених з їх відкритим ключем, які потім публікуються (або дані про транзакцію публікуються) в блокчейн. Це гарантує, що лише користувач із приватним ключем може здійснювати транзакції та вирішує проблему подвійних витрат, оскільки транзакція публікується, щоб

інші користувачі могли перевірити розподіл ресурсів на цей відкритий ключ або адресу. Однак для цієї форми ідентичності потрібен як обчислювальний пристрій, так і Інтернет. Приватні особи мають можливість вимагати від користувачів підтримувати сумісний пристрій для своїх блокчейнів, і підключення до Інтернету, необхідне для здійснення транзакції на блокчейні, але інші організації (наприклад, державний сектор) можуть зіткнутися з труднощами при переході до ідентифікатора, що відповідає лише блокчейну. Оскільки деякі їх клієнтські бази не мають обчислювальних елементів, необхідних для проведення транзакції, створюючи проблему розподілу витрат.

1.2.5. Криптовалюти. Біткойн - найпопулярніша криптовалюта, яка займає найбільшу частку ринку і, певно, ініціює інтерес до технології blockchain. Криптовалюти, такі як і біткойн, створені для того, щоб дозволити обмін деяким цифровим активом вартості (криптовалютою) на товар або послугу. Вони часто не мають дозволу і використовують доказову модель роботи для додавання блоків. У цих системах кожен може створити гаманець, який включає приватний ключ, відкритий ключ та адресу, отриману з відкритого ключа. Потім вони набувають (шляхом майнінгу чи купівлі) криптовалюти і додають її як транзакцію до блокчейн, щоб їхня адреса була пов'язана з їх цінністю. Коли користувач щось придбає, він розблоковує доступ до криптовалюти своїм приватним ключем, передаючи її продавцю, який заблокує її своїм приватним ключем. Ця транзакція публікується в blockchain, тому всі користувачі можуть перевірити, якщо у покупця є набагато менше криптовалюти, а продаючий користувач має на стільки більше. Кожна криптовалюта має свій блокчейн.

1.3. Адресація та мережева проблематика

IoT буде включати несумірно велику кількість вузлів, кожен з яких створюватиме вміст, який повинен отримати будь-який користувач з

відповідними правами. В даний час протокол IPv4 ідентифікує кожен вузол через 4-байтну адресу. Добре відомо, що кількість доступних IPv4-адрес швидко зменшується і незабаром вичерпається. Отже, очевидно, що повинні використовуватись як і існуючі IPv4 політики адресації так і відміні від них.

Адреси IPv6 виражаються за допомогою 128 біт, а отже, можна визначити 1038 адрес, що повинно бути достатньо для ідентифікації будь-якого об'єкта, на який варто звернутись. Відповідно, можемо призначити адресу IPv6 всім речам, що входять у мережу. Однак, оскільки теги RFID використовують 64–96 бітові ідентифікатори, стандартизовані EPCglobal, потрібні рішення для включення їх індентифікації, до адреси тегів RFID в мережі IPv6. Останнім часом було досліджено інтеграцію тегів RFID в мережі IPv6 [19] та запропоновано методології інтеграції RFID-ідентифікаторів в IPv6-адрес. Наприклад, у [22] автори пропонують використовувати 64 біти ідентифікатора інтерфейсу адреси IPv6 для повідомлення про ідентифікатор тегу RFID, тоді як інші 64 біти префіксу мережі використовуються для адреси шлюзу між системою RFID та Інтернетом.

Відповідно, шлюз буде обробляти інформацію, створену тегами RFID, які повинні залишати систему RFID та входити в інтернет наступним чином. Буде створено новий пакет IPv6. Його корисне навантаження буде містити інформацію, породжену тегом, тоді як його основна адреса буде створена шляхом об'єднання ідентифікатора шлюзу (який копіюється в мережеву префіксну частину адреси IPv6) та ідентифікатора тегів RFID (який копіюється в ідентифікатор інтерфейсу частина адреси IPv6). Аналогічно, шлюз буде обробляти IPv6-пакети, що надходять з мережі і спрямовані на певний тег RFID, наступним чином. Специфічний тег RFID, який представляє призначення повідомлення, буде легко опрацьований, оскільки його ідентифікатор повідомляється в частині ідентифікатора інтерфейсу адреси IPv6; натомість сповіщення (яке в більшості випадків представляє запит певної операції) буде повідомлено відповідним RFID.

1.4. Проміжне програмне забезпечення

Проміжне програмне забезпечення - це програмний рівень або набір підшарів, розміщених між технологічним та прикладним рівнями. Його особливість згладжувати кути різних технологій, є основною беззаперечною метою для звільнення програміста від проблем, які безпосередньо не стосуються її/його напрямну роботи, а саме - розробка конкретного додатку, включеного інфраструктурами IoT. Проміжне програмне забезпечення набуває великомасштабного значення в наш час завдяки своїй вагомій позиції у спрощенні розвитку нових сервісів та інтеграції застарілих технологій. Це позбавляє програміста від необхідності точного знання різноманітного комплексу технологій, прийнятих нижніми шарами.

В контекстах інших, архітектур програмного забезпечення, пропонованих в останні роки для IoT, часто дотримуються сервісно орієнтованої архітектури (SOA). Прийняття принципів SOA впорядковує складні та монолітні системи в додатки, що складаються з системи більш простих і чітко визначених компонентів.

Технологія SOA підтримує розвиток циклу проектування робочих процесів узгоджених служб, які з часом пов'язані з діями об'єктів. Це в кращу сторону впливає на взаємодію між частинами підприємства та дозволяє скоротити час, необхідний для адаптації до змін, накладених стрімкою зміною ринку. Підхід SOA також сприяє до повторного використання застарілих програм та гаджетів, оскільки це не нав'язує конкретної технології для впровадження послуги.

Переваги підходу SOA використовуються в більшості досліджень щодо концепцій середнього програмного забезпечення для IoT. Незважаючи на те, що загальноприйнята шарова архітектура відсутня, запропоновані рішення впираються, по своїй структурі, з тими ж проблемами, як обмеження функціональності пристроїв та можливостей комунікацій, надання загального набору служб та середовища для складу послуг. Ці загальні цілі приводять нас

до визначення макету проміжного програмного забезпечення, показаного на рис. 1.1.

Рис 1.1. Цілі проміжного програмного забезпечення

1.4.1. Набір сервісів. Цей шар міститься поверх архітектури проміжного програмного забезпечення на основі SOA. Він наділяє функціональними можливостями для накладання одиночних послуг, пропонованих мережевими об'єктами для побудови конкретних додатків. На цьому шарі немає поняття пристроїв, і єдині видимі активи - це сервіси. Важливе розуміння підгрунтя обслуговування - це сховище всіх підключених в даний час службових елементів, які виконуються під час виконання для створення складених служб. Логіка створення та управління складними послугами може виражатися в робочих процесах, використовування мови. У цьому контексті частим вибором є прийняття стандартних мов, таких як Мова про виконання сервіс-процесів (BPEL) та Джолі [20,21]. Мови робочого процесу визначають сервіс-процеси, які взаємодіють із зовнішніми організаціями за допомогою операцій Веб-сервісу, визначених за допомогою мови визначення веб-служби. Робочі процеси можуть бути вкладені, тому можна викликати робочий процес всередині іншого. Створення складних процесів можна представити у вигляді послідовності узгоджених дій, що виконуються окремими компонентами.

1.4.2. Управління сервісами. Цей рівень надає основні функції, які, як очікується, бути доступні для кожного об'єкта і дозволяють керувати ними в

сценарії IoT. Основний набір послуг включає: динамічне виявлення об'єктів, моніторинг стану та конфігурацію послуги. На цьому рівні деякі пропозиції проміжного програмного забезпечення включають розширений набір функцій, пов'язаних з управлінням якістю обслуговування та управлінням блокуванням, а також деякі семантичні функції (наприклад, управління контекстом) [24]. Цей рівень може забезпечити віддалене розгортання нових служб під час виконання, щоб задовольнити потреби додатків. На цьому рівні створено сховище служб, щоб дізнатися, який каталог послуг, пов'язаних з кожним об'єктом в мережі. Потім верхній шар може складати складні послуги, приєднуючись до служб, що надаються на цьому рівні.

1.4.3. Абстрактний об'єкт. IoT покладається на величезний та неоднорідний набір об'єктів, кожен із яких забезпечує конкретні функції, доступні через власний діалект. Таким чином, існує потреба в шарі абстракції, який зможе гармонізувати доступ до різних пристроїв загальною мовою та процедурою. Відповідно, якщо пристрій не пропонує відкриті веб-сервіси в мережі IP, існує необхідність ввести обгортковий шар, що складається з двох основних підшарів: інтерфейсу та підшару зв'язку. Перший пропонує веб-інтерфейс, що розкриває методи, доступні через стандартний інтерфейс веб-служб, і відповідає за управління всіма вхідними/вихідними повідомленнями, що беруть участь у спілкуванні із зовнішнім світом. Другий підрівень реалізує логіку, що стоїть за методами веб-сервісу і переводить ці методи в набір команд, призначених для пристрою, для зв'язку з об'єктами реального світу.

У деяких роботах запропоновано вбудовувати стеки TCP/IP в такі пристрої, як TinyTCP, mIP та IwIP [23], які забезпечують інтерфейс, подібний до сокета для вбудованих додатків. Потім вбудовані веб-сервери можуть бути інтегровані в об'єкти, виконуючи функцію цього шару абстракції об'єкта. Однак частіше ця функція обгортання надається через проксі-сервер, який відповідає за відкриття комунікаційного гнізда за допомогою консолі пристрою та надсилання до нього всіх команд, використовуючи різні мови зв’язку. Після

чого відповідає за перетворення в стандартну мову веб-служб і, розробити запит на зменшення складності операцій, необхідних кінцевим пристроєм.

1.4.4. Управління: довірою, приватністю, безпекою. Розвиток розгортання автоматичного зв’язку об’єктів IoT представляє небезпеку для нашого майбутнього. Дійсно, небачені користувачами вбудовані RFID-теги в наші особисті пристрої, одяг та продуктові продукти можуть несвідомо викликати відповідь своїм посвідченням особи та іншою інформацією. Це потенційно дає можливість механізму спостереження, пронизувати велику частину нашого життя. Програмне забезпечення повинно включати функції, пов'язані з управлінням довірою, конфіденційністю та безпекою всіх обмінюваних даних. Пов'язані функції можуть бути або побудовані на одному конкретному шарі попередніх, або, розподіленим через весь стек, від абстракції об'єкта до сервісної композиції, таким чином, що не впливає на продуктивність системи або не вносить зайві накладні витрати.

1.5. Технологія блокчейн

Блокчейн - це цифрова книга, яка дозволяє сторонам здійснювати операції без використання центрального органу для перевірки цих транзакцій [1]. Використання центрального органу (тобто третьої сторони) можна уникнути, оскільки в блокчейн, коли транзакції додаються, особистість сторін, які проводять ці транзакції, перевіряються, а транзакції перевіряються по мірі їх додавання до книги як блок транзакцій. Ведення книги підлягає аудиту, оскільки кожен блок транзакцій залежить від попереднього блоку таким чином, що будь-яка зміна попередить інших користувачів про зміну історії транзакцій [2]. Міцні зв’язки між особами, транзакціями та великою книгою дозволяють сторонам, які можуть не довіряти один одному, домовлятися про обмін ресурсів, зареєстрованих у головній книзі. Домовляючись про цю транзакцію,

сторони можуть потім здійснити нову угоду із спільним розумінням того, хто має який ресурс та про їх здатність торгувати цим ресурсом.

Blockchain - це технологія яка поєднує в собі інноваційний спосіб використання існуючих технологій. Чотири конкретні технології використовуються для реалізації блокчейн-технологій: асиметричне шифрування ключа; хеші; дерево Меркла; однорангові мережі.

1.5.1. Розумні контракти. Цифрова природа blockchain призвела до того, що він асоціювався з розумними контрактами. Договір у фізичному світі - це домовленість сторін про те, що після виконання певних умов відбудеться передача активів. Розумний контакт кодифікує ці атрибути в коді, щоб машини могли перевірити, чи відповідають умови, і ініціювати передачу активів. Окрім сторін, які беруть участь у транзакції, інші користувачі платформи blockchain можуть надавати обчислювальні ресурси, необхідні для обробки або підтвердження договірної транзакції, тим самим отримуючи частку транзакції сприяючи перевірці транзакції в головній книзі.

1.6. Асиметричне шифрування ключа

Асиметричне шифрування ключів, відоме також як криптосистема публічно-приватного ключа, функціонує для створення ідентичності на блокчейн. Користувач створює два елементи, відкритий ключ, який допомагає ідентифікувати його транзакції в Blockchain, і приватний ключ, необхідний для проведення транзакції з відкритим ключем. Асиметричне шифрування дозволяє здійснити автентифікацію користувачів, оскільки лише ті, хто має приватний ключ, можуть розшифрувати дані, зашифровані відкритим ключем, або зашифрувати дані для розшифрування відкритого ключа, створивши таким чином підпис.

Відкритий ключ може транслюватися на самому блокчейні, або може бути прив'язаний до адреси, яка транслюється замість цього. У деяких

блокчейн-системах визначається реальна ідентифікація кожної адреси або відкритого ключа, щоб окремі користувачі могли його відслідковувати. В інших, користувач може мати змогу генерувати відкриті та приватні ключі незалежно та транслювати відкритий ключ чи адресу, не ідентифікуючи себе, створюючи псевдонімічну ідентичність на блокчейні.

У блокчейні відкритий ключ використовується для ідентифікації користувача в блокчейн та перевірки ресурсів, прив'язаних до публічного ключа або адреси цього користувача. Ресурс не можна використовувати, якщо власник відкритого ключа, до якого прив’язаний ресурс, розблоковує (або розшифровує) ресурс приватним ключем, що дозволяє перенести його до іншої ідентичності на блокчейн (відкритий ключ або адресу) та заблокувати приватним ключем другого користувача. Ця транзакція буде записана в блокчейн, щоб інші користувачі могли переконатися, що ресурс змінив власника.

Асиметричне шифрування ключів, окрім блокчейн, використовується щодня, коли користувач підключається до веб-сайту за допомогою протоколу захисту передачі гіпертексту (HTTPS). Щоб увімкнути безпечне з'єднання з веб-сайтом, користувач запускає процес, надсилаючи запит на сайт. Потім сайт надсилатиме свій відкритий ключ користувачеві, після чого на комп'ютері користувача генерується новий ключ (який буде використовуватися у HTTPS-з’єднанні), шифрується відкритим ключем веб-сайту та надсилається назад. Користувач знає, що тільки веб-сайт, який має приватний ключ, може розшифрувати інформацію, яку тільки що надіслав користувач. За допомогою нового, створеного користувачем, ключа веб-сайт створить захищене з'єднання з користувачем, позначеним піктограмою HTTPS у вікні браузера.

1.7. Хеш

Хеш використовує аналогічні математичні функції як метод шифрування для отримання рядка символів виводу з урахуванням деяких вхідних даних. Це

одностороння функція, тобто хеш-значення може бути створене з входу, але вхід неможливо відтворити з хешу. У блокчейнах ряд транзакцій здійснюють трансшифрування разом, щоб зробити єдиний блок, який потім хешують. Значення хешу використовуються для перевірки цілісності блоку. Будь-які зміни транзакцій, що складають блок, змінять хеш-значення блоку в цілому. Якщо хеш-значення блоку з часом залишається однаковим, користувачі можуть бути впевнені, що транзакції в цьому блоці не були підроблені. Це дозволяє користувачам на blockchain визначати, чи можуть вони довіряти історії в blockchain.

Бази даних та «велика книга» постійно редагуються, коли нові записи додаються, а дані змінюються, або видаляються. Якщо хтось хотів би мати хеш-значення для бази даних, потрібно було б постійно хешувати її та підтримувати спосіб забезпечення того, щоб вони мали правильне хеш-значення, щоб вирівнятись із поточним станом системи, та оцінити її цілісність. Крім того, чим більша стає база даних, тим більш обчислювальним стає хешування. Дерево Меркла - це криптографічна концепція, представлена Ральфом Меркле в 1980 році як спосіб вирішення цієї проблеми.

У дереві Меркла дані сегментуються окремо від одного цілого файлу даних. Існує кореневий блок даних із хеш-значенням, а потім наступні блоки даних (іноді їх називають дочірніми, гілками чи листовими блоками), які мають своє власне хеш-значення. Кожен наступний блок даних приймає хеш-значення їх попереднього блоку (іноді його називають батьківським блоком) як вхід при створенні хеш-значення нового блоку. Це створює ланцюжок, або дерево хеш-значень, криптографічно прив’язуючи нові блоки даних до попередніх таким чином забороняє змінювати попередні дані. Якби дані в попередньому блоці мали бути додані, змінені або видалені, хеш-значення наступних блоків даних не буде обчислюватися, попереджаючи користувачів про внесення змін. Це також дозволяє створювати хеш-значення для менших, більш дискретних блоків даних, щоб обчислювання було менш ресурсозатратним, ніж повторна перевірка всього набору даних щоразу коли робиться редагування.

Blockchains запозичують концепцію дерев Меркла для виготовлення хеш-ланцюгів. У blockchain створюється перший блок і для нього обчислюється хеш-значення. Це кореневий блок. Наступні блоки потім використовують хеш-значення попереднього блоку в ланцюзі як один із входів для створення наступного блоку. Це зв’язування хеш-значень створює міцний взаємозв'язок між блоками ланцюга ревізійним та незмінним записом транзакцій на блокчейні.

Мережа однорангових (P2P) дозволяє розрізненій системі комп’ютерів безпосередньо з'єднуватися один з одним без посилань, інструкцій чи маршрутизації центрального органу. Мережі P2P дозволяють обмінюватися файлами, обчислювальними ресурсами та пропускною здатністю мережі між мережами.

У blockchain мережа P2P дозволяє користувачам транслювати безпосередньо між собою поточний стан blockchain (щоб користувачі могли погодитись з історією транзакцій) та зміни коли буде доданий новий блок. Це також дозволяє резервувати дані в блокчейн, оскільки будь-який користувач може завантажити повну копію поточної книги транзакцій та додати новий блок, щоб не було жодної точки відмови для блокчейна, якщо вузол та мережа змінюються.

У деяких реалізаціях blockchain користувачі не розміщують копії книги між собою. Натомість користувачі використовують хмарного постачальника послуг (CSP) для підтримки активних та резервних копій блокчейна, а також обчислюють транзакції та блоки у міру того, як вони відбуваються. У цих випадках для запуску блокчейна необхідна мережа однорангових мереж. Хоча CSP не є центральним перевіряючим органом у цьому прикладі, він стає третьою стороною угоди.

1.8. Транзакції в Blockchain

Блокчейн складається з серії блоків транзакцій. Транзакція (угода) - це подія, при якій ресурс або актив змінюють володіння від однієї сторони до

іншої. Ці індивідуальні транзакції підписуються користувачами, які беруть участь у цих транзакціях за допомогою використання шифрування публічно-приватного ключа. Оскільки приватний ключ необхідний для звільнення та прийняття ресурсу в транзакції на блокчейні, користувачі, що здійснюють транзакцію на блокчейні, фактично підписують транзакцію для забезпечення її безпеки. Операції групуються разом і складаються в блок, який підтверджується при його створенні за допомогою акта майнінгу для створення блоків. Цілісність всієї книги забезпечується кожним блоком, що має хеш-значення, яке залежить від власного хеш-значення попереднього блоку. Кожен з цих трьох етапів спирається на сильну криптографію, яка забезпечує надійність книги.

Операції можуть не опублікуватись відразу в блокчейн. Якщо велика кількість транзакцій відбувається за короткий проміжок часу, блокчейн-платформа може створити пул відкладених транзакцій, які обробляються відповідно до правил цього блокчейна - що може надавати оплату, пріоритет користувача або інший метод розміщення певні транзакції в блок перед іншими.

1.9. Керування в Blockchain

Блокчейн може бути публічним або приватним. У загальнодоступному блокчейні кожен бажаючий може створити пару публічно-приватних ключів і завантажити копію блокчейна. Зазвичай це здійснюється за допомогою програмного пакету, який регулює транзакції на блокчейні. У приватному блокчейні контролюється членство користувачів на блокчейні. Користувачі, які мають право брати участь, можуть бути пов'язані договірними відносинами один з одним, їхні адреси блокчейна можуть бути тісно пов'язані з їхніми особами реального світу, або участь у цьому блокчейні може бути узгоджено з іншими учасниками. У будь-якому випадку, члени приватного блокчейна можуть більше довіряти один одному, ніж до публічного блокчейна

Блокчейн може бути з дозволом або без дозволу, що не залежить від того, чи є блокчейн публічним чи приватним. Дозволений блокчейн - це той, в якому призначений йому дозвіл користувача. Деякі користувачі можуть переглядати весь або частину блокчейна, інші можуть додавати нові блоки. У цій системі адміністратор (адміністратори) не виконують функції центрального органу, оскільки вони не регулюють створення блоків на блокчейні, а лише права користувачів на блокчейні. У без дозвільному блокчейні всі користувачі мають рівні права, при цьому будь-хто може завантажити повний блокчейн і мати можливість потенційно додати додаткові блоки.

Обговорення блокчейна як публічного або приватного стосується рівня свободи, який користувачі мають створити ідентичності в цьому блокчейн. Обговорення блокчейна як дозвільного або без дозвільного стосується рівня доступу, який користувач мав би на цей блокчейн. Користувачі в blockchain повинні досягти консенсусу щодо правил створення та публікації нових блоків та вирішення розбіжностей.

Blockchains має користувачів та вузли на своїй платформі. Користувачами в блокчейні можуть бути особи, підприємства чи інші особи, які мають пару публічно-приватних ключів і здійснюють транзакції. Вузол - це обчислювальна система цього блокчейна. У користувача може бути вузол (наприклад, комп'ютер фізичної особи чи обчислювальна мережа бізнесу), або група користувачів може об'єднати ресурси для створення єдиного вузла (наприклад, користувачі, які діляться своєю обчислювальною силою на майнінг для нових блоків у блокчейні) . У платформі blockchain, яка використовує CSP, CSP є вузлом на blockchain, але також може бути користувачем.

Створення та публікація нового блоку в blockchain називається майнінг. У блоках майнерів користувачі намагаються додати наступний блок до ланцюга. Майнінг стимулюється за рахунок поліпшення становища користувача в цьому блокчейні, або через грошову, репутаційну чи ставкову пропозицію за додавання нових блоків. Нові блоки можуть бути додані до блокчейн за

допомогою різних методів. Такими методами є – PoW [4], PoS [3], схема круглої роботи користувачів мережі по черзі.

В PoW, хто прагне додати блок до блокчейн, подається складна обчислювальна проблема. Вирішуючи проблему, вони виграють можливість опублікувати наступний блок і отримати винагороду за це. Їх рішення транслюється іншим користувачам, які можуть негайно його перевірити, не проходячи ті самі обчислювальні ресурси, необхідні для вирішення проблеми. У цій схемі проблема часто полягає в тому, що хеш-значення містить певні елементи (наприклад, значення починається з чотирьох нулів). Щоб створити хеш-значення з цими елементами, додаткова інформація додається як вхідна інформація (поряд із хеш-значенням попереднього блоку, транзакціями в блоці, інформацією про дані та час тощо). Ця додаткова інформація називається nonce, і може бути такою ж простою, як число, яке змінило б хеш-значення. Виявлення значення nonce, яке вирішує проблему, виграє для цього майнера право публікувати наступний блок.

У схемі PoS наступний блок може бути призначений користувачеві, який має відповідний пакет акцій у цьому блоці. Це може бути тому, що блок містить транзакції щодо цього користувача. Або користувач має *X* відсоток частки в цьому блокчейні, тому йому надається право публікувати *X* відсотків блоків у цьому блокчейні. Доказ схеми ставок обчислювально менш ресурсоємний, ніж доказ роботи. У схемі круглої роботи користувачі мережі по черзі додають нові блоки. Оскільки певний рівень довіри необхідний, щоб кругові схеми роботи працювали, вони використовуються в дозволених блокчейнах.

Якщо в blockchain є розбіжність, більшість користувачів вузла використовуватиме найдовший ланцюг у блоці як дійсну книгу і братиме її як основу для майбутніх транзакцій. У випадку, якщо два різних майнера публікують блоки одночасно, а ці блоки містять різну інформацію, блокчейн може дозволити опублікування обох блоків для цього раунду, а потім дозволити системі самостійно розв’язатись після публікації наступного блоку,

який потім створить найбільший ланцюжок транзакцій, а отже найбільш надійну книгу. Іншим способом вирішення розбіжностей є використання візантійської толерантності до помилок, при якій користувачі на блокчейн-платформі будуть голосувати, за який блок вони приймуть рішення, а кількість голосів визначає наступний блок, який повинен бути опублікований.

1.10. Проблематика використання Blockchain

Криптографічні атрибути blockchain є переконливою причиною його використання в порівнянні з іншими технологіями. Але існують стійкі підводні камені та невирішені умови, які можуть перешкоджати широкому використанню блокчейна.

1.10.1. Переносимість даних. Як і в інших системах обліку записів, коли дані реєструються в одній системі, перенесення цих даних у нову систему може бути проблематичним. Ця проблема зберігається у багатьох додатках blockchain. Після того як користувач вирішить використовувати один блокчейн, він не зможе видалити свої попередні записи транзакцій та перенести їх у нову систему, оскільки ці транзакції є частиною іншого блокчейна, і будь-яка зміна ланцюга призведе до того, що користувачі не зможуть генерувати хеш значення для нових блоків. Існування цих даних є постійним на блокчейні. Крім того, якщо користувач прагне скопіювати свої дані з одного блокчейна в інший, немає стандартів для побудови даних з одного блокчейна в інший, тому всі елементи даних з одного блокчейна можуть не вкладатися в інший, а також як вони оброблятимуть публічно-приватні ключі або хеш-значення. Відсутність стандартів у технологіях blockchain поширюється на межі того, як зберігаються дані, до того, як генеруються публічно-приватні ключі, як генеруються хеш-значення та як передаються дані між колегами. Відсутність стандартів фактично означає, що після того, як користувач вибере один блокчейн для їх використання, він може не зможе перейти на інший блокчейн. Хоча він,

можливо, зможе відтворити поточний розподіл ресурсів за новим ланцюжком та здійснювати транзакції з цього моменту, їх історія буде інкапсульована у попередньому ланцюжку.

1.10.2. Безпека ключів. Як і в інших формах шифрування, створення, зберігання та втрата контролю над приватним ключем створює проблеми, які не вирішені. Якщо у користувача буде порушено свій пристрій, який зберігає їх приватний ключ, зловмисник отримає доступ до їх приватного ключа та зможе перенести ресурси з цього відкритого ключа на інший відкритий ключ або адресу, контрольовану зловмисником. Якщо жорсткий диск користувача виходить з ладу, або він забуває чи іншим чином втрачає свій приватний ключ, модератори ефективно блокують ресурс, прив'язаний до їх відкритого ключа, назавжди, гальмуючи будь-яку іншу транзакцію з цим активом.

1.10.3. Управління блокчейн за допомогою більшості. Групи користувачів в blockchain можуть поєднувати обчислювальні ресурси та змову з майнерами блоків. У деяких реалізаціях blockchain це дозволяється та заохочується. Однак, у цій ситуації є можливість, коли групи користувачів можуть мати ненавмисний вплив на те, які транзакції перетворюють їх у блок, та блоки, які розміщуються. Крім того, користувач або група користувачів (зловмисник), що мають достатню обчислювальну потужність, можуть мати можливість відтворити блокчейн, тим самим змінивши попередні транзакції та трансляцію для користувачів блокчейн, що ланцюжок зловмисника дійсний. Оскільки це був би найдовший ланцюг, інші можуть автоматично прийняти його, навіть якщо він помилковий. Це називається атакою 51%. Хоча обчислювально це важко здійснити проте, це може дати можливість неохайним користувачам зіпсувати нову або запущену блокчейн-платформу, яка має більш короткі регістри, тим самим визнавши їх як контролерів створення блоків.

1.10.4. Ощадливість та безпека користувачів. Ще одне питання, яке стосується інших технологій, і те, що стосується блокчейн, - це рівень комфорту та знань, які повинен мати користувач із технологією, щоб правильно та безпечно ним користуватися. Наприклад, багато водіїв не знають, як працює машина, але все ще можуть безпечно керувати автомобілем. Багато користувачів не знають, як працюють комп'ютери та мережі, але все ж можуть набрати та надіслати електронний лист. Участь користувачів у програмі можлива, оскільки певні дизайнерські рішення приймалися керівництвом (наприклад, вимоги щодо безпеки, та потреба в посвідченні водія) та інженерами (наприклад, простими інтерфейсами користувача), які дозволяють користувачам використовувати ці технології. Оскільки технологія blockchain розробляється, приймається та використовується, подібні вимоги до дизайну можуть бути необхідними для забезпечення правильного використання та безпечного впровадження технології. Окрім використання самої технології blockchain, користувачі, також повинні знати про її підводні камені та компроміси, перш ніж прийняти її. Наприклад, розповсюджуються історії про те, що користувачі, які володіють Bitcoin, втратили доступ до своїх приватних ключів, тим самим заборонивши використовувати цей актив у майбутньому - вони фактично втратили актив, і без центрального органу керування не зможуть звернутися для відновлення цього активу.

1.11. Висновки до розділу

В даному розділі було розглянуто предметну область та проаналізовано спільне застосування технології Blockchain в IoT та можливості використання в різних сферах нашого життя. Визначено проблематику використання Blpckchain разом з IoT-пристроями, зокрема проблему безпеки. Проаналізовано галузі їх можливого застосування й проблеми.

РОЗДІЛ 2
АНАЛІЗ ТЕХНОЛОГІЇ BLOCKCHAIN В КОНТЕКСТІ IOT

У цьому розділі детально розглянемо основні концепції Blockchain, зокрема транзакції та менеджер блоків в деталях. Почнемо з визначення двох основних понять:

Транзакції (Угоди): Основні примітивні комунікації для обміну інформацією контролю між будь-якими об'єктами. Потік даних відрізняється від транзакцій.

BlockManager: - це базова одиниця, відповідальна за управління BC. Це включає генерацію, перевірку та зберігання окремих транзакцій та блоків транзакцій.

2.1. Вузли накладання

Як і в Bitcoin, припускаємо, що кожен вузол в накладанні відомий відкритим ключем. Вузли використовують свіжий РК для створення кожної нової транзакції для забезпечення анонімності. Накладення, як показано на рис.2.1, складається з різних об'єктів, відомих як вузли накладання, включаючи розумний дім, мобільні пристрої, Service Provider (SP), сервери та хмарне сховище.

Мережа накладення потенційно може складатися з великої кількості вузлів. Таким чином, щоб забезпечити масштабованість, припускаємо, що відкритий BC керується підмножиною вузлів накладання. Припускаємо, що алгоритм кластеризації, такий як у [5], використовується для групування вузлів у кластери, при цьому кожен кластер обирає голову кластера (CH). CH відповідають за управління BC і, таким чином, називаються управляючими блоками накладення (OBM). Крім того, CH обробляє вхідні та вихідні транзакції, що генеруються до, або від членів кластеру. Очікується, що вузол,

обраний як СН, буде залишатися в мережі протягом тривалого часу та мати достатні ресурси для обробки блоків та транзакцій. Припускаємо, що існують такі механізми, як ті, які використовуються в [6] для управління відмовами СН. Оскільки основні завдання виконуються СН, LSB не впливає на динаміку пристроїв IoT, тобто приєднання та вибуття пристроїв.

Операції, згенеровані вузлом накладання, захищаються за допомогою асиметричного шифрування, цифрових підписів та криптографічних хеш-функцій (наприклад, SHA256). Операції в накладенні можуть бути додатково класифіковані на (I) операції з єдиним підписом, які містять лише підпис генератора транзакцій, та (II) транзити з багатозначним сигналом, які підписуються як генератор транзакцій (запитувачем), так і одержувачем. Більшість транзакцій у LSB - багатозначні.

Структура транзакцій з багатозначним зображенням показана на рис.2.2. Перше поле є ідентифікатором транзакції, тоді як друге поле є вказівником на попередню транзакцію того ж вузла запитувача. Таким чином, усі транзакції, створені запитувачем, пов'язані між собою. Далі слідує РК та підпис запитувача та реквізитів. Останній підпис додається, коли транзакція отримана запитувачем. Сьоме поле є результатом транзакції і встановлюється запитувачем. Поле виводу містить такі 3 записи: (I) загальна кількість транзакцій згенерованих реквізитами, які були прийняті запитувачем (II) загальна кількість транзакцій, відхилених запитувачем (III) хеш РК, що запитувач буде використовувати для своєї наступної транзакції. Перші два поля містять історичну інформацію, необхідну для обчислення репутації запитувача, яка використовується в алгоритмі розподіленої довіри. Останнє поле виведення є необхідним для подальшої перевірки запитувача, оскільки вузли накладення змінюють РК, використовуваний для генерації кожної нової транзакції. Заключне поле транзакції з багатозначною ознакою, тобто метадані, надає інформацію про бажану дію та розумний домашній пристрій, який є ціллю цієї дії. Операція з єдиним підписом має схожу структуру, але виключає запитуваний РК та підписи, метадані та виходи «0» та «1», оскільки бере участь

лише один вузол накладання. Зауважимо, що транзакції з багатозначним сигналом та операціями з єдиним підписом організовані як окремі книги, оскільки відповідні результати відрізняються.

Ключові транзакції в накладанні:

- Генезис: кожен вузол накладання повинен спершу створити транзакцію генезису, яка служить вихідною точкою для ведення його книги у відкритому доступі.

- Запис: вузол накладення генерує транзакцію запису для зберігання даних у хмарному сховищі.

- Доступ: транзакція доступу створюється вузлом накладання для запиту збережених даних пристрою, наприклад, SP (запитувач) може запитувати всі дані, що зберігаються пристроєм (запитувачем) за останній тиждень.

- Моніторинг: транзакція моніторингу породжується вузлом накладання, наприклад, SP може захотіти отримати дані в режимі реального часу від пристрою.

У LBS потік даних зберігається окремо від потоку транзакцій. Таким чином, у відповідь на транзакцію доступу або моніторинг, запитуваний пристрій надсилає дані запитувачу в окремий пакет(и) даних після того, як буде підтверджено, що запитувач має право доступу до даних. Аналогічно, для транзакції запису, дані створені запитувачем, надсилаються чітко від транзакції. На відміну від транзакцій, які транслюються, пакети даних є одноадресними і можуть бути маршрутизовані по оптимальних шляхах через мережу накладання за допомогою протоколів маршрутизації, таких як OSPF [7].

Операції з накладенням зберігаються в загальнодоступних ВС, якими керують ОВМ. Кожен блок ВС складається з двох основних частин, а саме транзакцій та заголовка блоку. Заголовок блоку містить наступне: хеш попереднього блоку, ідентифікатор генератора блоків та підписи верифікаторів. Хеш попереднього блоку в загальнодоступному ВС забезпечує незмінність. Якщо зловмисник намагається змінити раніше збережену транзакцію, то хеш відповідного блоку, який зберігається в наступному блоці, більше не буде

послідовним і, таким чином, буде викривати цю атаку. Поля "ідентифікатор генератора блоків" та "підписи верифікаторів" будуть обговорені пізніше в цьому розділі. Подібно до Bitcoin, кілька транзакцій групуються разом і потім обробляються як один блок. Блок може зберігати не більше T-max транзакцій. Значення *T-max* впливає на пропускну здатність ВС таким чином, що при більшому *T-max* більше операцій може зберігатися в одному блоці.

Рис 2.1. Огляд LSB

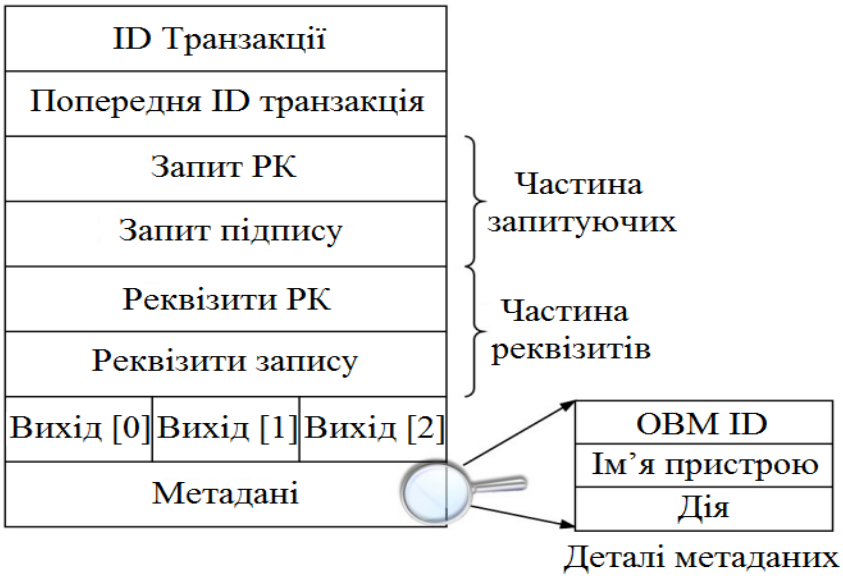


Рис 2.2. Структура транзакцій з великою кількістю

Таблиця 2.1

Таблиця довіри

Прямі докази	Кількість попередньо перевірених блоків	10	20	30	40	50
	Потрібно підтвердити	80%	20%	40%	30%	20%
Не прямі докази	Відсоток ОВМ підписаних блоків	20%	40%	60%	80%	100%
	Потрібно перевірити	80%	75%	70%	60%	40%

Коли ОВМ отримує транзакцію Y, він спочатку перевіряє, чи міститься запитувач цієї транзакції у своєму кластері. ОВМ підтримує список ключів (по суті спрощений список контролю доступу), що складається з запитуючих/реквізитів РК пар, який вказує реквізити, яким дозволено надсилати транзакції конкретним запитувачам. Цей список ключів оновлюється членом кластеру, щоб дати дозвіл іншим вузлам накладання надсилати транзакції. Запитувач може встановити значення реквізитів у списку ключів ОВМ як "трансляцію", що означає, що він отримає всі транзакції, що містять його РК як запитуючий РК. Якщо запитувач і реквізити вхідної транзакції Y збігаються з записом у списку ключів, ОВМ надсилає транзакцію запитувачеві (який знаходиться в межах його кластеру і, таким чином, безпосередньо пов'язаний з ОВМ). Якщо запитувач у Y не належить до кластеру ОВМ, транзакція транслюється на всі інші ОВМ. Усі очікувані транзакції зберігаються в пулі транзакцій на кожному ОВМ. Коли розмір запущеного пулу стає рівним *T-max*, ОВМ починає процес створення нового блоку, використовуючи алгоритм консенсусу.

2.1.1. Алгоритм консенсусу. В LSB пропонуємо алгоритм консенсусу на основі часу, замість більш ресурсомістких альтернатив, таких як PoW та PoS, які зазвичай використовуються в ВС. Алгоритм консенсусу повинен забезпечити вибір генератора блоків випадковим чином між вузлами, який обмежений у номерах блоків, які він може генерувати. Щоб запровадити випадковість між генераторами блоків, кожен ОВМ повинен дочекатися

випадкового часу, відомого як період очікування, до створення нового блоку. Оскільки період очікування відрізняється для кожної ОВМ, ОВМ може отримати новий блок, створений іншим ОВМ, який містить деякі або всі транзакції, які в даний час знаходяться в пулі транзакцій ОВМ. У цьому випадку цей ОВМ повинен видалити ці транзакції зі свого пулу, оскільки вони зберігаються в ВС іншим ОВМ. Вимога ОВМ чекати випадкового часу також зменшує кількість повторюваних блоків, які можна генерувати одночасно. Максимальний час очікування обмежується вдвічі більше максимальної затримки в кінці мережі. Коли генерується новий блок, він транслюється на всі інші вузли накладання, щоб він міг бути доданий до ВС.

Щоб захистити накладення від зловмисного ОВМ, який потенційно може генерувати велику кількість блоків з фальшивими транзакціями, періодичність, з якою ОВМ може генерувати блоки, обмежена таким чином, що лише один блок може бути згенерований через інтервал, позначений консенсус-періодом. Період консенсусу коригується розподіленим управлінням пропускною здатністю (DTM). Значення за замовчуванням (і максимальне) для консенсусного періоду - 10 хвилин, що аналогічно інтервалу видобутку в Bitcoin. Мінімальне значення періоду консенсусу дорівнює подвоєній максимальній затримці в кінці, щоб забезпечити достатній час для поширення нового блоку, генерованого іншими ОВМ. Кожен ОВМ контролює частоту, з якою інші ОВМ генерують блоки. Будь-які невідповідні блоки блокуються і довіра, пов’язана з відповідальним ОВМ, зменшується. Щоб попередня ОВМ не вимагали короткого періоду очікування, сусідні ОВМ відстежують частоту під час якої ОВМ генерує нові блоки в час початку очікування. Якщо кількість таких блоків перевищує поріг, визначений на основі застосування проектувальниками ВС, ОВМ скидає блок, сформований їх сусідом.

2.1.2. Перевірка. ОВМ повинен перевірити кожен новий блок, який він отримує від інших ОВМ, перед тим, як додати його до ВС. Для перевірки блоку ОВМ спочатку перевіряє підпис генератора блоків. Передбачається, що кожен

ОВМ використовує заздалегідь визначений ключ для генерації блоків, ці ключі відомі всім іншим ОВМ [8]. Дальше перевіряється кожна окрема транзакція в блоці. Блок вважається дійсним, якщо всі транзакції, що містяться в блоці, є дійсними.

Алгоритм перевірки транзакцій (рис. 2.3) окреслює процедуру перевірки окремої транзакції, X. Нагадаємо, що в загальнодоступному ВС всі транзакції з великим набором даних, що генеруються кожним запитувачем, організовані в окрему книгу. Вихід транзакцій з багатозначним сигналом створює метрику репутації для запитувача. Зв'язок між послідовними транзакціями встановлюється, включаючи хеш PK, який буде використаний запитувачем для наступної транзакції, у третьому полі виводу поточної транзакції. Таким чином, ОВМ спочатку підтверджує це, порівнюючи хеш запитувача PK в X з результатом [2] попередньої транзакції цього запитувача (Стрічки 1,2). Після цього підпис запитувача, який міститься в четвертому полі X, перевіряється (також називається викупленим), використовуючи його PK в X (Стрічки 4,5). Згадайте, що вихід (0) та вихід (1) використовуються для створення репутації вузла запитувача. Спочатку запитувач встановлює ці результати (виходячи з його історії транзакцій) у транзакції з великим набором даних. Якщо запитувач приймає транзакцію, то це збільшить вихід (0) на одиницю. В іншому випадку запитувач збільшує вихід (1). Щоб захистити ВС від вузлів, які претендують на помилкову репутацію, збільшуючи їх виводи, перш ніж надсилати їх до запитувача, на наступному етапі перевірки транзакцій ОВМ перевіряє, що тільки один з результатів X, тобто чи кількість успішних транзакцій (тобто вихід (0)) або кількість відхилених транзакцій (тобто вихід (10)) збільшується лише на одну (Стрічки 8,9). Після цього підпис запитувача перевіряється за допомогою PK у X (Стрічки 11,12). Якщо кроки виконані успішно, перевіряється X.

```
Input: Overlay Transaction (X)
Output: True or False Requester verification :
1: if (hash (X.Requester-PK) 6= X-1.output[2]) then
2: return False;
3: else
4: if (X.requester-PK redeem x.requester-signature) then
5: return False;
6: end if
7: end if Ouput validation :
8:   if   (X.output[0]   -   X-1.output[0])   +   (X.output[1]   -
X-1.output[1])> 1) then
9: return False;
10: end if Requestee verification :
11: if (X.requestee-PK redeem x.requestee-signature) then
12: return true; 13: end if
```

Рис. 2.3. Алгоритм перевірки транзакцій

Перевірка всіх транзакцій та блоків є обчислювальною, особливо коли кількість вузлів в мережі з накладанням збільшується. У контексті IoT можна очікувати серйозних проблем масштабування, оскільки очікується, що кількість вузлів буде дуже великою. Для вирішення цього питання LSB використовує алгоритм розподіленої довіри, який поступово зменшує кількість транзакцій, які необхідно перевірити в кожному новому блоці, оскільки OBM створюють довіру один до одного. Алгоритм вводить поняття прямих і непрямих доказів наступним чином:

– Прямі докази: OBM A має прямі докази щодо OBM B, якщо він попередньо перевіряв принаймні один блок, який генерується B.

– Непрямі докази: якщо OBM A не має прямих доказів щодо OBM B, але якщо одна з інших OBM підтвердила, що блок, що генерується B, є дійсним, то A має непрямі докази щодо B.

Кожен OBM підтримує список, який записує відповідну інформацію для встановлення прямих доказів. Для цього OBM записує кількість блоків, які він перевірив для всіх інших OBM. Згадайте, що OBM може створювати блоки, невідповідні алгоритму консенсусу. Інші OBM, які отримують невідповідний

блок, скинуть те саме і зменшать пряму довіру, пов’язану з відповідальним ОВМ. Якщо зловмисний ОВМ продовжить цю поведінку, його рейтинг довіри буде відповідно знижений. Це означає, що все більше та більше транзакцій доведеться перевіряти іншими ОВМ. Для непрямих доказів ОВМ перевіряє кількість інших ОВМ, які підтвердили отриманий блок, сформований ОВМ. Основна ідея алгоритму розподіленої довіри полягає в тому, що чим сильніші докази, зібрані ОВМ про ОВМ, що генерує новий блок, тим менше перевірок у цьому блоці потрібно перевірити, щоб перевірити блок. Таблиця довіри, приклад якої проілюстровано на табл. 2.1, підтримується ОВМ для реалізації цієї стратегії. Прямі докази мають перевагу над непрямими доказами. Якщо ОВМ має прямі дані про створення блоку, тоді частина транзакцій всередині блоку вибирається для перевірки, як показано на табл. 2.1. У разі відсутності прямих доказів ОВМ перевіряє, чи є непрямі докази, а потім вибирає іншу частку транзакцій, виходячи з того, скільки інших ОВМ вступили в силу для генератора блоків, як показано на табл. 2.1. Зауважте, що певна частка транзакцій завжди перевіряється, навіть якщо є вагомі докази для захисту від потенційно порушеного ОВМ. Якщо ніяких доказів не зафіксовано, то всі транзакції в блоці перевіряються.

2.1.3. Управління розподіленою пропускною здатністю (DTM). Класичні алгоритми консенсусу, що використовуються в BC, обмежують пропускну здатність BC, яка вимірюється як кількість транзакцій, що зберігаються в BC за секунду, оскільки рішення криптографічної загадки обчислювально вимагає, наприклад, Bitcoin BC обмежений 7 транзакціями в секунду через POW [2]. Для IoT такі обмеження були б неприйнятними, оскільки існували б численні взаємодії (та транзакції) між різними вузлами. У LSB запропоновано механізм управління розподіленою пропускною спроможністю (див. рис. 2.4) для активного моніторингу використання BC та внесення відповідних коригувань для того, щоб він залишався у прийнятному діапазоні. Наприкінці кожного періоду консенсусу кожен ОВМ обчислює використання (α) як відношення

загальної кількості нових транзакцій, що генеруються, до загальної кількості транзакцій, доданих до ВС. Зауважте, оскільки всі транзакції та блоки передаються всім ОВМ, використання, обчислення всіма ОВМ, повинно бути аналогічним. Мета DTM - забезпечити, щоб α залишався в певному бажаному діапазоні (α-*min,* α-*max*).

Якщо припустити мережу з N вузлами, з яких M є ОВМ та R, що представляють середню швидкість, з якою вузол генерує нові транзакції в секунду (R можна оцінити із загальної кількості транзакцій, що генеруються за консенсус-період), використання може бути представлено наступним чином:

$$a = \frac{N*R*Consensus-period}{T_{max}*M}.$$

Input: α
1: while true do
2: if (α > α_{max})
потім обчисліть консенсус-період$_{новий}$ з рівняння 1 с α = $\frac{a_{min}+a_{max}}{2}$
3: if (consensus-period$_{min}$ <= consensus-period$_{new}$)
потім оновити консенсус-період до консенсус-період$_{новий}$
4: else
скинути консенсус-період до значення за замовчуванням, обчислити M
з рівняння 1 з a= $\frac{a_{min}+a_{max}}{2}$
5: end if
6: end if
7: if (α < α_{min})
Потім обчисліть консенсус-періодновий з рівняння 1 з α = $\frac{a_{min}+a_{max}}{2}$
8: if (consensus-period$_{new}$ <= consensus-period$_{max}$)
потім оновити консенсус-період до консенсус-період$_{новий}$
9: else
скинути консенсус-період до значення за замовчуванням
обчислити M з рівняння 1 з α = $\frac{a_{min}+a_{max}}{2}$
10: end if
11: end if
12: end while

Рис. 2.4. Алгоритм управління розподіленою пропускною здатністю

Наведене рівняння дозволяє припустити, що має два способи коригування використання: (I) зміна консенсусного періоду, яке диктує частоту, з якою блокується додатак до ВС; або (II) зміна M, однаково ОВМ може генерувати один блок протягом періоду консенсусу. Останній підхід потребує значно більших накладних витрат, оскільки вимагає переналаштування всієї мережі накладання. Таким чином, якщо α перевищує α_{max}, в першу чергу DTM перевіряє, чи можна скоротити період консенсусу. Якщо так, то нове значення для консенсусперіоду обчислюється за допомогою рівняння 1 і припускаючи, що α дорівнює середині точки потрібного діапазону (α_{min}, α_{max}), що забезпечує стабільну робочу точку для мережі (Стрічка 2-3 , рис. 2.4). Навпаки, якщо термін консенсусу неможливо скоротити, то мережу потрібно переписати з новим значенням для M (Стрічка 4). Це нове значення обчислюється за допомогою рівняння 1, причому α знову встановлюється середньою точкою потрібного діапазону, а період консенсусу встановлюється за замовчуванням, яке є консенсус-періодом. Ця функція дозволяє LSB добре масштабувати, де збільшена кількість вузлів-учасників забезпечує більш високу пропускну здатність. Скидаємо консенсу-сперіод до значення за замовчуванням, оскільки воно в іншому випадку залишатиметься незмінним на мінімальному порозі, таким чином, завжди вимагає конфігурації мережі, якщо використання збільшиться вище порогового значення.

У випадку, коли використання знижується нижче α_{min}, застосовується зворотний підхід, тобто DTM спочатку намагається збільшити період консенсусу, інакше зменшує кількість ОВМ (Стрічки 7 - 9, рис. 2.4).

Щоб усі вузли відповідали дії, яку слід здійснити (будь то зміна періоду консенсусу), кожен ОВМ чекає довільну тривалість та передає повідомлення із зазначенням дії, яку слід здійснити для всіх інших ОВМ. ОВМ отримувач перевіряє, чи відповідає дія його рішенню. Якщо так, він підписує оригінальне повідомлення та передає його іншим ОВМ. Якщо ні, то воно створює свіже повідомлення із зазначенням його дії та передає його іншим ОВМ. Повідомлення про дію, яке отримує підписи від більшої половини кількості

ОВМ, передбачається узгодженим рішенням, яке повинні дотримуватися всі ОВМ. Зауважте, що в більшості випадків дії, які вживають усі вузли, будуть послідовними. Однак, іноді можуть спостерігатися незначні розбіжності в оцінці ОВМ щодо кількості сформованих транзакцій через проблеми з втратою пакету або затримки, що, в свою чергу, може призвести до незначних відмінностей у розрахунковому періоді консенсусу або М. У рідкісних випадках, коли існує відсутня чітка більшість, ОВМ використовують метод виборів, як у [9] для досягнення остаточної згоди щодо нового консенсусу.

2.2. Розумний дім

Розумний дім складається з безлічі пристроїв IoT, якими керує локальний ВМ (LBM). Оскільки пристрої IoT, як правило, обмежені ресурсами, локальні транзакції шифруються за допомогою симетричного шифрування, для якого встановлюється спільний ключ між двома сторонами, і використовують легку криптографічну хеш-функцію. У кожному розумному будинку LBM централізовано керує локальним змінним кодексом (IL), який за структурою схожий на BC, і обробляє локальні транзакції та накладення транзакцій, що генеруються в розумному будинку або з нього. LBM може бути інтегрований з Інтернет-шлюзом або окремим середнім ящиком, таким як F-secure [10], який виступає посередником між пристроями IoT та шлюзом. LBM використовує узагальнений метод розподілу ключів Діффі-Геллмана [11], щоб генерувати та розподіляти спільний ключ між двома локальними об'єктами, яким дозволено ділитися даними на основі заголовка політики в локальній IL.

Місцевий IP реєструє всі локальні транзакції та транзакції накладення, для яких запитувачем є LBM. Як показано на рис. 2.5, кожен блок локальної IL містить заголовок блоку та заголовок політики. Заголовок блоку підтримує хеш попереднього блоку, щоб забезпечити незмінність, аналогічну загальнодоступній BC. Заголовок політики складається у вигляді списку контролю доступу (ACL), який визначає правила для обробки локальних та

накладних транзакцій. Як показано в правому куті на рис. 2.3, заголовок політики має чотири параметри. "Заявник" позначає ідентифікатор особи, яка генерує транзакцію. Для вхідних накладних транзакцій, які є транзакціями, що перевозяться, це повинен бути PK запитувача. Для локальних транзакцій це стосується конкретного пристрою IoT. Другий параметр у заголовку політики вказує на дозволену дію (міститься у метаданих транзакції), яка може бути однією з таких: зберігати локально, зберігати у хмару, періодично зберігати доступ, контролювати та контролювати. Третій параметр вказує цільовий пристрій.

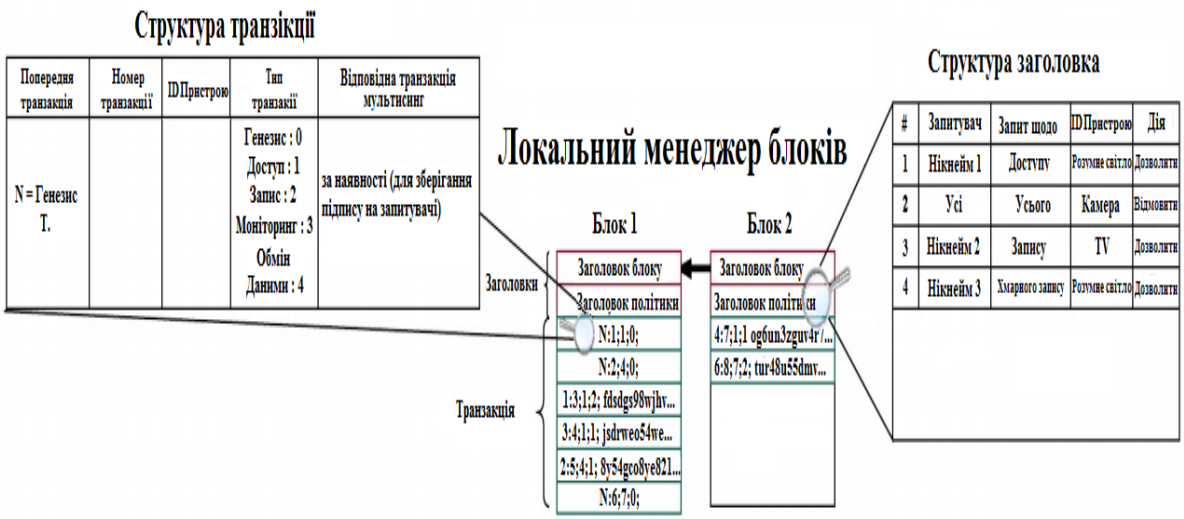


Рис. 2.5. Локальний менеджер блоків

Усі транзакції зберігаються в транзакційній частині IL для аудиту. Для кожної транзакції зберігається п’ять полів, як показано на лівій частині рис. 2.5. Перше поле - це вказівник на попередню транзакцію того ж пристрою, яка створює ланцюжок транзакцій для цього конкретного пристрою, що використовується LBM для аудиту та аутентифікації. Друге поле - ідентифікатор транзакції. Третє поле - ідентифікатор пристрою. Для місцевих транзакцій це ідентифікатор пристрою, який генерує транзакцію. Для транзакцій з накладенням - це ідентифікатор пристрою, дані якого запитуються (запитувачем) і витягуються з поля метаданих отриманої транзакції накладення. Якщо транзакція надсилається вузлом накладання, то хеш транзакції, тобто

ідентифікатор транзакції, зберігається у п’ятому полі, щоб його можна було використовувати для позначення транзакції в загальнодоступному ВС.

Кожен розумний дім оснащений локальним сховищем пам’яті, яке є таким пристроєм, як накопичувач резервного копіювання, який використовується розумними домашніми пристроями для локального зберігання даних. Це сховище може бути інтегровано до LBM або може бути окремим пристроєм. Передбачається, що локальне зберігання захищено. Припускаючи, що розумному пристрою дозволено зберігати дані до локальної пам’яті (що перевіряється за допомогою перевірки заголовка політики), LBM генерує загальний ключ, який використовується пристроєм для аутентифікації із сховищем даних.

2.3. Транзакції

Обговорюючи деталі кожного рівня, у цьому розділі обговоримо взаємодію між цими рівнями, що сприяє різним видам транзакцій.

2.3.1. Місцеві операції. Операції, що обмінюються між розумними пристроями, які належать до одного розумного будинку, називаються місцевими транзакціями. Локальні транзакції шифруються спільним ключем між двома суб'єктами, що беруть участь у транзакції. LBM генерує спільні ключі для пристроїв, використовуючи узагальнений протокол Діффі-Геллмана [11], після отримання дозволу власника будинку. Для відмови у дозволі LBM позначає раніше розподілений ключ недійсним, надсилаючи керуюче повідомлення тим суб'єктам, які використовують ключ для своїх транзакцій.

Місцеві транзакції:

− Генезисна транзакція: кожен пристрій спочатку вимагає транзакції генезису в локальній IP. LBM генерує загальний ключ для шифрування зв'язку між пристроєм та LBM та зберігає цей ключ в транзакції генезису.

− Зберігання локально: спочатку пристрій, який вимагає локального зберігання даних, надсилає свій запит до LBM. LBM генерує та розподіляє загальний ключ між пристроєм та локальним сховищем. Локальне зберігання використовує спільний ключ для аутентифікації. Для подальшого зв'язку пристрій та сховище спілкуються безпосередньо за допомогою спільного ключа.

− Обмін даними: кожен пристрій всередині розумного будинку може запитувати дані від іншого внутрішнього пристрою, щоб запропонувати певні послуги, наприклад датчик світла запитує дані датчика руху, щоб увімкнути світло, коли хтось заходить додому. Щоб досягти контролю за власним будинком над місцевими комунікаціями, спочатку LBM повинен надати спільний ключ пристроям, які вимагають обмін даними. Після отримання ключа пристрої спілкуються безпосередньо, поки ключ дійсний.

2.3.2. Накладення транзакцій. Операції, в яких генератор транзакцій та одержувач транзакцій є обома вузлами накладення, називаються транзакціями накладення. Нагадаємо, що асиметричне шифрування використовується для транзакцій із накладенням. Ключові операції з накладанням є наступними:

1. Генезис транзакції: кожен вузол накладання повинен спочатку створити генезисну транзакцію в загальнодоступному ВС. У ярусі накладення транзакція генезису ініціюється вузлом накладання, використовуючи один із наступних підходів:

− Органи сертифікації: при такому підході вузол спирається на широко розгорнуту інфраструктуру відкритих ключів (PKI) [12] в Інтернеті. Вузол накладання контактує з довіреним органом сертифікації (CA), який ратифікує РК вузла, додаючи підписаний сертифікат. Вузол включає сертифікат у транзакцію генезису. Для перевірки транзакції ОВМ перевіряє сертифікат. Передбачається, що ОВМ мають доступ до списку надійних кореневих сертифікатів CA для перевірки (аналогічно браузерам та ОС).

– Метод «Запишіть монету в Bitcoin»: альтернативно, якщо вузол не бажає покладатися на PKI, тоді він може приватно створити генезисну транзакцію, спалюючи біткойни [13]. Вузол створює постійну транзакцію в Bitcoin BC за рахунок знищення визначеної кількості, що позначається як "спалювання монет". Адреса операції запису використовується як вхід генезисної транзакції. Вузол накладання створює генезисну транзакцію з тим же PK, що і транзакція запису, і надсилає її до OBM, кластеру якого він належить. Якщо генератор транзакцій генезису є OBM, він передає транзакцію іншим OBM. Для перевірки прийнятої транзакції генезису OBM відповідає PK транзакції генезису PK транзакції запису в Bitcoin BC. Далі OBM перевіряє підпис у транзакції генезису.

В обох підходах після перевірки OBM транслював транзакцію генезису на інші OBM, які зберігаються в загальнодоступному BC.

2. Хмара зберігання: припускаємо, що користувач, який бажає зберігати свої дані, наприклад інтелектуальні дані термостата, у хмарі створено обліковий запис у постачальника послуг хмарного зберігання (наприклад, Dropbox, OneDrive тощо) поза межами діапазону (тобто незалежно від LSB). Припускаємо, що користувач створює пару публічних/приватних ключів для цього облікового запису хмарного сховища і що відповідний відкритий ключ використовується в наступних хмарних сховищах і транзакціях доступу. Нагадаємо, що LSB створює чітке розмежування між площиною управління та площиною даних для забезпечення ефективного маршрутизації пакетів даних через мережу. Щоб полегшити це, припускаємо, що LBM користувача надсилає запит під час початкового налаштування в хмарний сховище з вищезгаданим PK. Після аутентифікації хмарне сховище надсилає ідентифікатор свого OBM до цього LBM. Згодом усі дані, що збираються LBM, можуть бути безпосередньо перенаправлені до хмари. Потік подій для транзакцій у хмарному сховищі показаний на рис. 2.6. Пристрій, який бажає зберігати дані у хмарі, посилає транзакцію хмарного зберігання в LBM (S1 на рис. 2.6). Після авторизації (S2) LBM надсилає дані з ідентифікатором OBM хмари до власної

ОВМ. Потім ОВМ спрямовує дані безпосередньо до хмарного сховища за допомогою протоколу маршрутизації. Після зберігання даних хмарне сховище підписує отриману транзакцію від LBM та надсилає її до власної ОВМ для зберігання в ВС (S4).

3. Доступ та моніторинг: Потік транзакцій доступу та моніторингу показаний на рис 2.6. Для обох транзакцій запитувач генерує та надсилає транзакцію до ОВМ (A1, M1 на рис. 2.6). ОВМ перевіряє списки ключів, щоб знайти відповідність, а якщо не знаходить, то транслює транзакцію іншим ОВМ (A2, M2). Знайшовши відповідність, ОВМ пересилає транзакцію до LBM (A3, M3). Четвертий крок відрізняється щодо доступу або моніторингу транзакцій. Для транзакції доступу дані отримують з локального або хмарного сховища (A4), тоді як для транзакцій монітора дані реального часу запитуються з пристрою (M4).

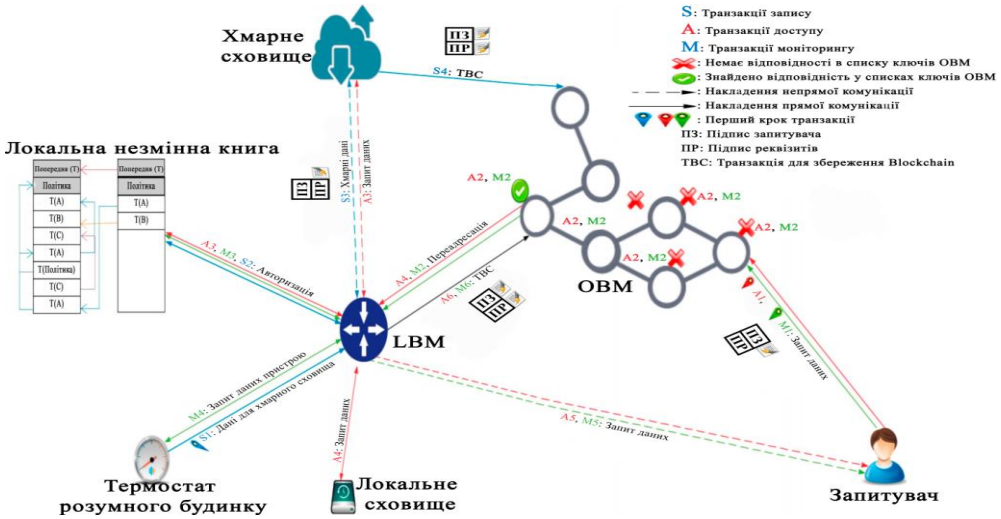


Рис. 2.6. Процес зберігання, доступу та моніторингу транзакцій

Після отримання даних LBM спрямовує його до запитувача (A5, M5). Нагадаємо, що потік даних направляється безпосередньо та окремо від потоку транзакцій. Нарешті, LBM підписує отриману транзакцію від запитувача та надсилає її в ОВМ для зберігання в загальнодоступному ВС (A6, M6).

2.3.3. Спільне накладення. У випадках, коли людина відповідає за декілька будинків (наприклад, коли він є власником кількох будинків),

управління кожним місцем проживання може примножити зусилля. LSB пропонує можливість створення спільного накладу для спрощення управління декількома розумними будинками. Менеджер вибирає один LBM в одному будинку як Спільний BM для всіх будинків. Інші будинки спільного накладання використовують з'єднання віртуальної приватної мережі (VPN) (між домашнім шлюзом Інтернету та ShBM) для безпечного з'єднання та обміну даними зі ShBM. ShBM виконує ті ж функції, що і LBM, але для всіх пристроїв у всіх будинках, які є частиною спільного накладання.

2.3.4. Репутація OBM. У класичних BC, наприклад Bitcoin або Ethereum, вузлам, що генерують нові блоки, пропонується грошова винагорода у вигляді монет як форма компенсації за витрачання своїх ресурсів на вирішення обчислювально-інтенсивної головоломки, пов'язаної зі створенням блоку. Ця плата сплачується за транзакцію користувачами. LSB використовує легкий алгоритм консенсусу, і таким чином ми усуваємо явні винагороди та плату за транзакції. Натомість OBM за генерування дійсного блоку здобуває репутацію з іншими OBM, що може розглядатися як неявна винагорода.

2.4. Висновки до розділу

В даному розділі було розроблено функціональну структуру та архітектуру IoT - інфраструктури з використанням ключових елементів, таких як LBM та OBM.

На основі ключових елементів LBM та OBM розроблено мережу накладення, яка потенційно може складатися з великої кількості вузлів.

Обґрунтовано використання алгоритму консенсусу на основі часу, замість більш ресурсомістких альтернатив, таких як PoW та PoS. Таким чином, завдяки алгоритму перевірки транзакцій кожен OBM перевіряє всі нові блоки, які отримує від пристроїв, та інших OBM.

РОЗДІЛ 3
АПРОБАЦІЯ ЗАПРОПОНОВАНОГО ПІДХОДУ

У цьому розділі надамо якісний аналіз безпеки та конфіденційності, а також кількісну оцінку ефективності.

3.1. Оцінка ефективності

У цьому розділі представлено широкі оцінки різних аспектів діяльності LSB. Вперше дослідили можливість використання екземплярів з відкритим кодом BC, таких як Ethereum. Однак ці платформи особливо підходять для розробки додатків поверх підкладки BC. LSB має суттєві відмінності у своїх основних операціях порівняно з цими даними BC. Як наслідок, не вдалося використати ці платформи для оцінок, і тому вирішено використовувати моделювання. Оцінюємо рівень інтелектуального будинку та накладку окремо, оскільки ці яруси працюють незалежно, особливо що стосується продуктивності. Таким чином, резюмуємо деталі одного рівня, вивчаючи ефективність другого рівня. Використовуємо наступні дві симуляції:

Cooja: Використовуємо Cooja [15] для вивчення ефективності рівня розумного будинку. Cooja добре підходить для оцінки низькоресурсних пристроїв і надає перевагу доступності впровадження різних протоколів, відомих IoT.

NS3: Використовуємо NS3 [16] для оцінки продуктивності накладення, оскільки вона широко застосовується для аналізу однорангових мереж.

Для моделювання NS3 розглядаємо мережу, що складається з 50 вузлів накладання. Вважаємо, що *T-max* дорівнює 10. Припускаємо, що п'ять запитувачів генерують чотири транзакції в секунду. Наведені вище параметри називаються конфігурацією за замовчуванням і використовуються в моделюванні, якщо прямо не зазначено інше.

3.1.1. Час обробки PoW. Маємо на меті оцінити час, який витрачається поза штатним пристроєм для вирішення стану PoW, одного з широко застосовуваних алгоритмів консенсусу в системах на базі BC [17]. Робимо це, щоб підкреслити неефективність використання класичних BC та PoW в контексті IoT. Кожен блок в Bitcoin BC має додаток до них. Майнер зобов'язаний шукати правильне поняття, щоб блок в цілому задовольняв певній умові. Зокрема, потрібно, щоб хеш SHA-256 блоку мав певну кількість провідних нулів. Єдиний спосіб знайти правильне поняття - це груба сила (майнинг). Кількість провідних нулів контролює труднощі розв'язання PoW. Чим більше тривалість цієї послідовності, тим більше ресурсів і часу на обробку потрібно для розгадування загадки. Реалізуэмо PoW за допомогою C++ на ПК (2,7 ГГц Intel Core i5 процесор, 8 ГБ пам'яті та графічна карта Intel Iris Graphics 6100), щоб вивчити час обробки рішення головоломки з двома труднощами. Типові пристрої IoT значно обмежені ресурсами, тому отримані результати - це консервативні верхні межі, яких можна очікувати на пристроях IoT. Розв'язання PoW з 6 ведучими нулями займає 2,2 секунди. Збільшення тривалості нулів до 7 збільшує час обробки до 28,59 хвилин. Наразі біткойн використовує блоки з 17 нулями, на вирішення яких на звичайному ПК знадобиться експоненціально більше часу. Результати, підтверджують, що розв'язання PoW, що використовуються в Bitcoin, спричиняє значні затримки на пристроях, тим самим підтверджуючи наш вибір дизайну щодо усунення PoW в LSB.

3.1.2. Виконання розумного дому. Проводимо моделювання за допомогою Cooja для оцінки споживання енергії та витрат часу на LBM. Це пояснюється тим, що LBM - це найбільш витратний ресурс у розумному будинку, оскільки він обробляє всі транзакції та виконує багато операцій хешування та шифрування (як симетричних, так і асиметричних). На відміну від цього, пристрої IoT повинні виконувати дуже прості завдання, найбільш обчислювально - симетричне шифрування. Більшість пристроїв IoT мають

достатні можливості для виконання цього завдання. Для порівняння накладних витрат LSB моделюємо інший метод, який має той самий потік транзакцій, що і LSB, але не використовує шифрування, хешування та локальний IL. Назвемо це "базовою лінією". Використовуємо IPv6 через бездротові персональні мережі (6LoWPAN) як базовий протокол зв'язку в нашому моделюванні, оскільки він добре підходить до обмежень ресурсів для налаштування розумного будинку. Симулюємо три датчики мота z1 (що імітують розумні пристрої для дому), які передають дані безпосередньо в LBM (також імітується як mo1 zte) кожні 10 секунд. Кожне моделювання триває 3 хвилини, а результати усереднюються за цю тривалість. Хмарне сховище безпосередньо підключено до LBM для зберігання даних. Щоб забезпечити комплексну оцінку, моделюємо транзакції збереження та доступу. Для транзакції збереження моделювали дві різні та реалістичні моделі потоку трафіку:

− Періодично: у цьому налаштуванні пристрої періодично зберігають дані на хмарне сховище (наприклад до розумного термостата, періодично зберігаючи показання температури в хмару).

− На основі запиту: тут пристрої зберігають дані, коли вони отримували запит від користувача (наприклад власник будинку запитує підключену камеру безпеки, щоб перевірити, чи хтось підходить до дверей).

Оцінюємо такі показники:

− Час накладних витрат: посилається на час обробки для кожної транзакції в LBM і вимірюється з моменту отримання транзакції в LBM до моменту надсилання відповідної відповіді запитувачу.

− Споживання енергії: посилається на енергію, яку споживає LBM на обробку операцій.

Час накладних витрат: рис. 3.1 показує результати для накладних витрат. LSB витрачає більше часу на обробку пакетів порівняно з базовою лінією, яку можна віднести до додаткових операцій шифрування та хешування. У гіршому випадку для транзакцій зберігання на основі запитів, додаткові накладні

витрати, введені LSB, становлять 20мс, що в абсолютних показниках ще невелике.

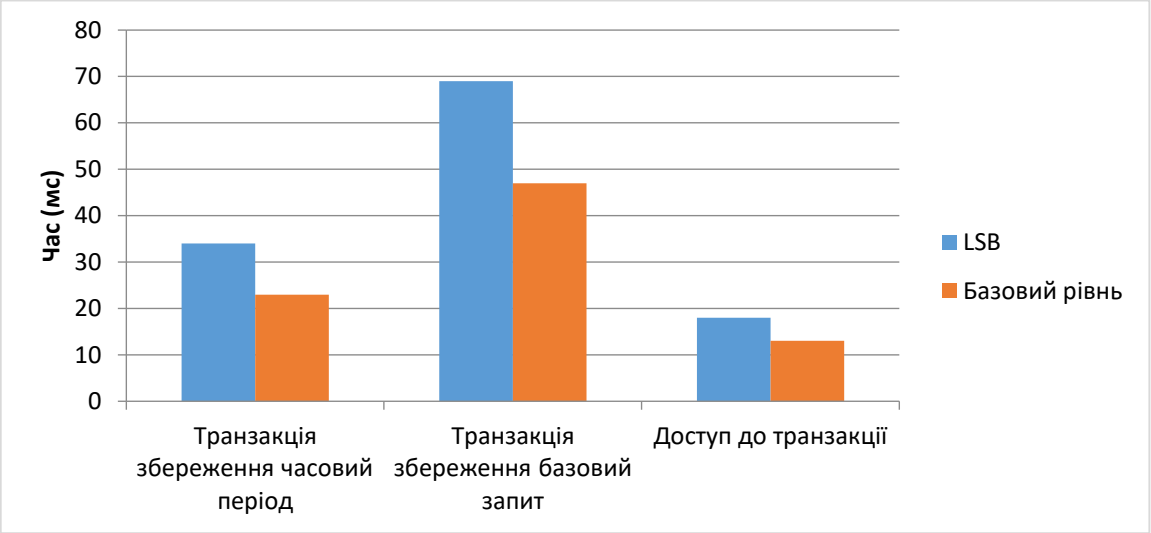
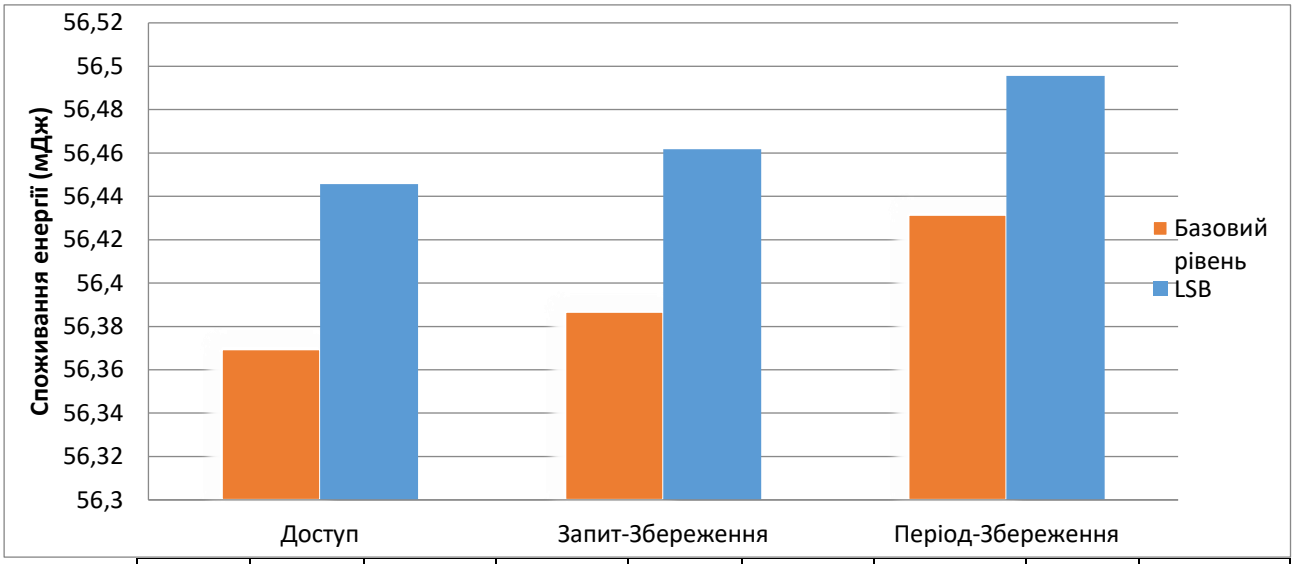


Рис. 3.1. Оцінка накладних витрат у LBM

Споживання енергії: На рис. 3.2 наведені результати споживання енергії. Як очевидно, LSB збільшує споживання енергії на 0,07 (мДж). У таблиці внизу на рис. 3.2 викладено споживання енергії для трьох основних завдань, що виконуються LBM, а саме: CPU, передача (Tx) та прослуховування (Lx). Споживання енергії процесором збільшується приблизно на 0,002 (мДж) в LSB за рахунок шифрування та хешування. LSB призводить до отримання більш довгих пакетів, що подвоює споживання енергії при передачі порівняно з базовою лінією. Слід зазначити, що припускається 100% радіо-робочий цикл в оцінках (тобто радіо завжди увімкнено). Якщо радіо сигнал з періодичністю вимикається, щоб зберегти енергію, то відносно накладні витрати на прослуховування лінії, в LSB, будуть вищими. Однак, навіть якщо припустити дуже агресивний робочий цикл у 1%, відносне збільшення енергії в прослуховування лінії все одно становитиме лише близько 60%.

3.1.3. Доступ до розумного домашнього пристрою з накладанням. У цьому розділі оцінюємо затримку, що виникає через накладений вузол для

доступу або контролю розумного домашнього пристрою (наприклад, коли власник будинку віддалено підключений до накладення та бажає контролювати свою камеру безпеки вдома).



	CPU	Tx	Lx	CPU	Tx	Lx	CPU	Tx	Lx
Базовий рівень	0.0103	0.0102	56.3489	0.0117	0.0357	56.3393	0.0121	0.0549	56.3645
LSB	0.0127	0.0834	56.3496	0.0132	0.1106	56.3379	0.0133	0.1166	56.3657

Рис. 3.2. Оцінка споживання енергії

Затримка вимірюється з моменту створення запиту до отримання відповіді. Проводимо моделювання за допомогою NS3 з конфігурацією за замовчуванням з 13 вузлами накладання, що діють як OBM. Порівнюємо LSB з базовим методом, який відповідає поточним пропозиціям інтелектуального будинку на ринку, де запитувач безпосередньо спілкується з LBM, не потребуючи жодної операції з обробки транзакцій, яка є частиною LSB. Затримка, що виникає з використанням базового методу, становить 17,62мс. При LSB затримка збільшується до 48,74мс. Більшу затримку можна пояснити тим, що транзакція повинна бути передана іншим OBM для перевірки. Кожна

ОВМ має затримку на 0,006мс для обробки транзакції. Однак ця затримка є відносно незначною.

LSB відокремлює потік даних від потоку транзакцій. У той час як транзакції транслюються між ОВМ в накладенні, пакети даних передаються до місця призначення по оптимальних шляхах, визначених протоколом маршрутизації, таким як OSPF. Для кількісної оцінки переваг цього дизайнерського рішення порівнюємо LSB з базовим методом, в якому і транзакції, і пакети даних транслюються в мережі накладання. Використовуємо конфігурацію за замовчуванням і припускаємо, що один запитувач надсилає реквізитам чотири операції доступу в секунду. Розглядаємо наступні два показники ефективності, які найкраще фіксують вплив поділу між транзакцією та потоками даних: (I) затримка в кінці - аналогічно вище (II) накладні витрати - це фіксує загальну кількість пакетів які передається ОВМ для доставки пакетів даних запитувачу. Оскільки розмір пакетів даних та транзакцій різний, вимірюємо останні як сукупну суму всіх розмірів пакетів у Кбайтах. Оскільки на ці дві метрики впливає кількість ОВМ в мережі, змінюємо кількість вузлів накладення, які виконують роль ОВМ, від 5 до 20. Результати представлені на рис 3.3.

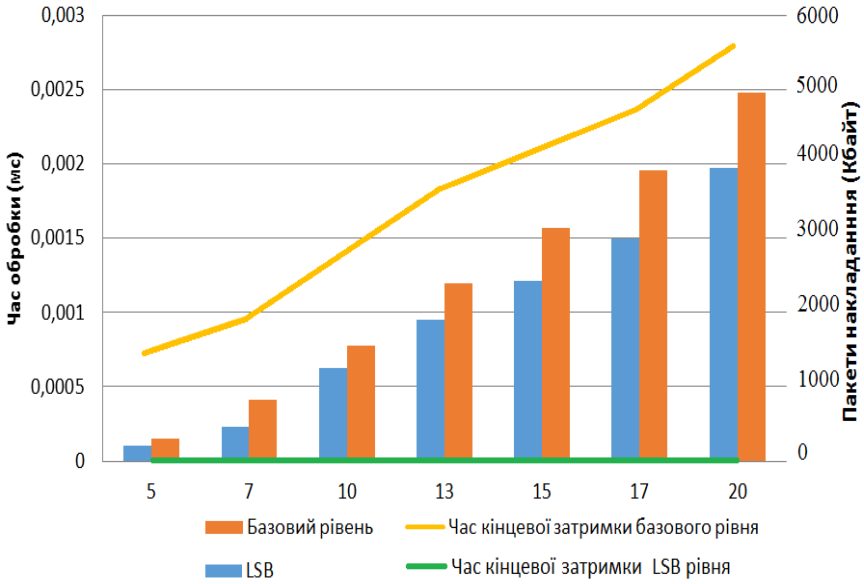


Рис. 3.3. Оцінка впливу розділення потоків даних та транзакцій

LSB включає в себе нижчі пакети накладних оскільки в останньому пакети даних транслюються між усіма ОВМ, порівняно з першими, де пакети даних маршрутизовані по оптимальних трасах. Для базової лінії обидва показники ростуть лінійно у міру збільшення кількості ОВМ. Кількість генерованого трафіку прямо пропорційна кількості ОВМ, що пояснює лінійне збільшення накладних витрат пакету.

Оскільки пакети даних зараз транслюються то сама затримка, що виникає при отриманні даних у запитувача, також лінійно збільшується. При LBS лише накладні витрати пакета збільшуються із кількістю ОВМ. Оскільки пакети даних перенаправляються безпосередньо до запитувача, кількість затримок не залежить від затримки в кінці.

3.1.4. Оцінка алгоритму розподіленої довіри. В класичному ВС всі транзакції всередині нового блоку повинні бути перевірені вузлом накладання. На відміну від ВС LSB використовує алгоритм розподіленої довіри, в якому кількість транзакцій, які необхідно перевірити, поступово зменшується, оскільки ОВМ створюють довіру один до одного. У цьому експерименті порівнюємо час обробки, для перевірки нового блоку в LSB з базовою стратегією, схожою на класичний ВС. Використовуємо конфігурацію мережі за замовчуванням та таблицю довіри, показану на табл. 2.1. Моделювання триває 180 секунд, а результати, показані на рис. 3.4, є середніми за 10-ма запусками. Показано також стандартне відхилення, за винятком базової лінії, де результати детерміновані. Вимірюємо час, необхідний кожному ОВМ для перевірки нового блоку та побудуємо середнє значення на рис. 3.4 (показано на лівій вертикальній осі). Зауважуємо, що нехтуючи всіма іншими завданнями (наприклад, перевірка списків ключів, генерування нових блоків тощо), крім перевірки нових блоків у цій оцінці, оскільки перші не впливають на алгоритм довіри. Рис. 3.4 зображує час обробки як функцію від кількості успішно перевірених (доданих до ВС) блоків, коли моделювання прогресує. Відсоток

транзакцій, який потрібно підтвердити (PTV), відображається на правій вертикальній осі. Можна зробити висновок з рис. 3.4, що при запуску час обробки однаковий для обох методів, оскільки ОВМ повинні ще довіряти один одному. Однак у міру прогресування часу та генерування і перевірки більшої кількості блоків ОВМ створюють пряму довіру один до одного. Отже, лише частину загальної кількості транзакцій у новому блоці потрібно перевірити в LSB, що скорочує час обробки порівняно з базовим рівнем, де всі транзакції всередині блоку перевірені. Більше того, у міру збільшення кількості перевірених блоків потрібно прогресивно зменшувати кількість транзакцій (також показано на рис. 3.4), оскільки довіра до інших ОВМ продовжує зростати. Після створення 50 блоків довіра серед ОВМ досягає найвищого рівня (табл. 2.1). З цього моменту кількість транзакцій, які потрібно перевірити, залишається фіксованою як і час обробки. У стаціонарному стані (тобто, коли мережа працює протягом значного періоду часу), LSB досягає понад 50% економії часу на обробку порівняно з базовою лінією.

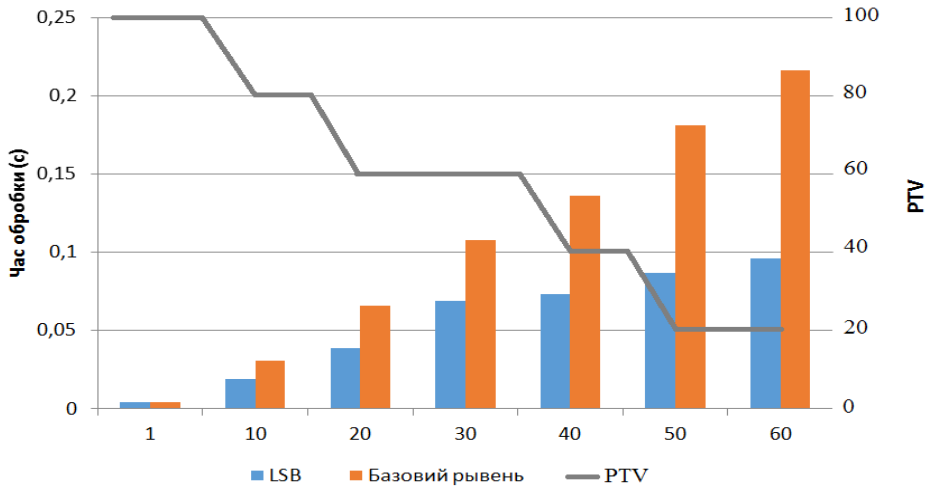


Рис 3.4. Середній час обробки ОВМ для перевірки нових блоків

У LSB, оскільки лише частина транзакцій всередині блоку перевірена, є ймовірність, що фальшива транзакція, створена зловмисним вузлом, не може бути перевірена і тим самим приєднана до ВС. Далі оцінюємо відсоток успішності такої атаки. Інтуїтивно зрозуміло, що чим більше ОВМ в мережі,

тим нижча ймовірність успішної атаки, оскільки зростає ймовірність того, що фальшива транзакція буде обрана для перевірки.

Однак накладні витрати пакетів також пропорційно збільшуються з кількістю ОВМ через збільшення трансляційного трафіку. Щоб вивчити цей компроміс, розглядаємо конфігурацію мережі за замовчуванням і змінюємо кількість вузлів накладення, що виступають в якості ОВМ, від 3 до 20. Показники оцінки - це рівень успішності атаки та кумулятивний накладний пакет. Для імітації атаки розглядаємо найгірший сценарій, коли високонадійний ОВМ, який генерував понад 50 блоків і таким чином накопичив високий рівень довіри, створює новий блок, що містить одну фальшиву транзакцію. Використовуємо таблицю довіри, показану на табл. 2.1. Виконуємо симуляцію 10 разів, а успіх атаки - це відсоток від кількості запусків, підроблений блок не виявляється жодним із чесних ОВМ. Порівнюємо накладні витрати пакетів, що виникають в LSB, з базовою лінією, в якій мережа накладення структурована аналогічно Bitcoin. Нагадаємо, що в Bitcoin всі вузли накладення (у нашому випадку 50) керують ВС розподілено на відміну від LSB, де управління ВС обмежено обраними вузлами накладання, тобто ОВМ. Базова лінія завжди точно визначатиме атаку, оскільки всі транзакції в блоці перевірені. Результати показані на рис. 3.5.

З збільшенням кількості ОВМ збільшується ймовірність успішної атаки. Як і очікувалося, накладні витрати пакетів збільшуються лінійно з кількістю ОВМ. З 13 ОВМ всі атаки виявляються успішно. Однак відповідні накладні витрати пакету (8497) значно нижчі, ніж у базової лінії (54177).

Процент успішності атаки безпосередньо впливає на PTV. Щоб вивчити цей вплив, оцінюємо відсоток успішності атаки для різних PTV в мережі з конфігурацією за замовчуванням з п'ятьма вузлами накладення, які діють як ОВМ. Причиною вибору п'яти ОВМ є показ впливу PTV на успіх атаки. Як видно з рис.3.5, наявність більшої кількості ОВМ значно покращує безпеку. Результати проілюстровані на рис. 3.6.

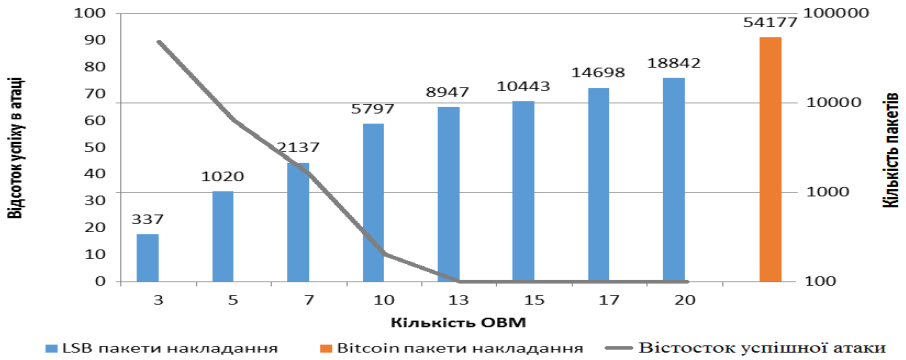


Рис 3.5. Оцінка впливу кількості ОВМ на безпеку та пакетні накладні витрати

Коли PTV дорівнює 100%, ОВМ перевіряють всі транзакції в блоці, що призводить до нульового відсотка успішності атаки (тобто атака завжди виявляється). Як показано на рис. 3.6, із зменшенням рівня PTV відсоток успішності атаки зростає.

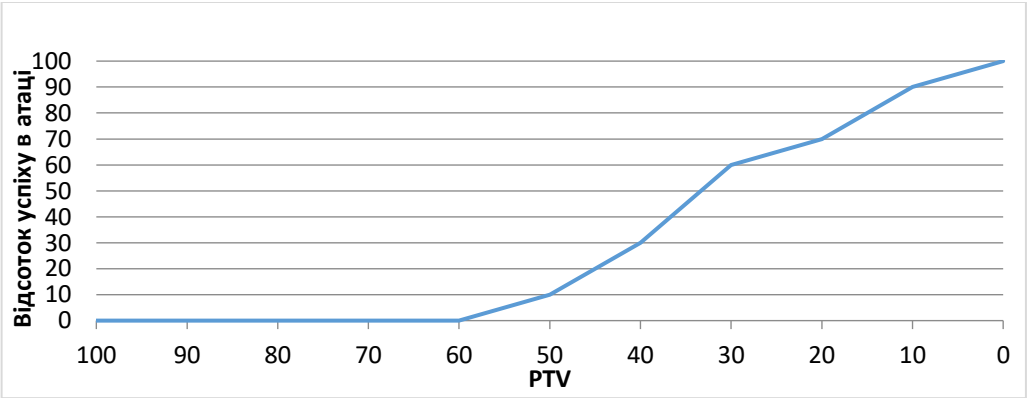


Рис. 3.6. Оцінка впливу PTV на здатність виявляти напади, що накладаються

Для мережевої конфігурації, використовуваної в цьому моделюванні, найменше значення PTV, яке може гарантувати безпеку, становить 60%. Повторюючи те саме моделювання для різної кількості ОВМ, щоб визначити найменше значення PTV, для якого завжди можна виявити атаку. У табл. 3.1 показані результати моделювання і їх можна використовувати як орієнтир для налаштування таблиці довіри. PTV, який нижчий за значення в табл. 3.1, зробить мережу вразливою до атак, що накопичуються.

Табл*иця 3.1*

Мінімальний PTV для виявлення приєднаних атак як функції кількості ОВМ

Кількість ОВМ	3	5	7	10	13	15	17	20
Мінімальний PTV	80	60	60	40	20	20	20	1

З іншого боку, більша величина збільшує час обробки нових блоків (оскільки потрібно перевірити більше транзакцій) та накладні витрати в мережі.

3.1.5. Аналіз продуктивності DTM. Механізм DTM, спрямований на динамічне регулювання використання мережі на основі загального навантаження, тобто кількості генерованих транзакцій. Щоб проілюструвати ефективність DTM, моделюємо мережу з конфігурацією за замовчуванням з 13 вузлами накладання, що виконують роль ОВМ. Оскільки класичні ВС мають фіксовану пропускну здатність (наприклад, ВС Bitcoin має фіксовану пропускну здатність 7 транзакцій в секунду), немає базової лінії, яку ми можемо використовувати для порівняння. Спочатку в мережі накладання за секунду генерується в цілому 10 кумулятивних транзакцій. Моделюємо ситуації, коли попит в мережі коливається. Кількість транзакцій в секунду збільшується до 32 за весь проміжок часу від 5 секунд до 40 секунд. За 40 секунд навантаження збільшується до 44 транзакцій за секунду. Зміни навантаження на мережу проілюстровані на рис. 3.7. DTM обчислює використання мережі α у кінці кожного консенсусного періоду як відношення між кількістю генерованих транзакцій та кількістю транзакцій, доданих до накладення ВС, з моменту останнього обчислення α. Інтервали часу, коли α обчислюється ОВМ, показані за допомогою сірих крапок на малюнку. Період консенсусу спочатку встановлюється на 10 секунд, що є значенням за замовчуванням. Будемо вважати, що α_{min} і α_{max} встановлені відповідно 0,24 та 1.

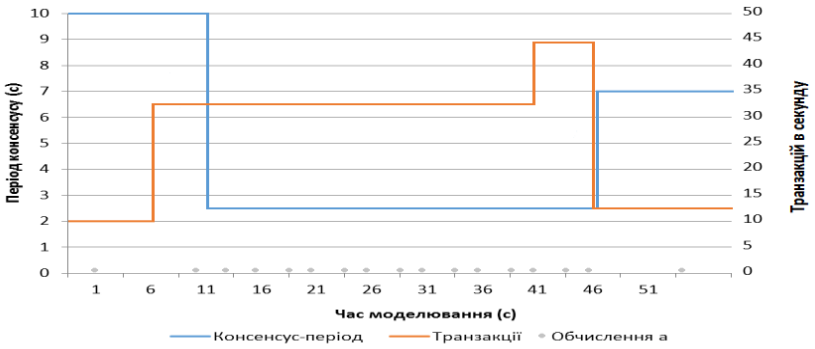


Рисунок 3.7 Оцінка DTM в накладанні

Наприкінці першого періоду консенсусу (тобто 10 секунд) α обчислюється рівним 2,4, що більше, ніж α_{max} (1). Це відбувається через різке збільшення навантаження на мережу за 5 секунд. Для зменшення використання мережі DTM скорочує консенсус-період до щойно обчисленого значення 2,5 секунди (стрічки 2-5 рис. 2.4), використовуючи рівняння 1, де α встановлений на 0,59, що є середньою точкою α_{min} і α_{max}. Період консенсусу також проілюстрований на рис. 3.7. Оскільки навантаження на мережу залишається стабільною до 40 секунд, період консенсусу також залишається незмінним. У цей час навантаження на мережу ще більше збільшується. Таким чином, наприкінці наступного періоду консенсусу (43 секунди) α обчислюється рівним 0,84. Оскільки обчислене значення все ще менше α_{max}, подальших дій не потрібно. Це підкреслює ефективність вибору середньої точки α_{min} та α_{max} для перерахунку α. Значення α падає до 0,2 за 48 секунд внаслідок різкого зменшення кількості транзакцій за 45 секунд. Оскільки це значення менше α_{min}, DTM збільшує період консенсусу (Стрічки 7- 9 алгоритму управління розподіленою пропускною здатністю) до нового значення, яке обчислюється як 7 секунд.

3.2. Аналіз безпеки та конфіденційності

У цьому розділі обговорюємо безпеку, конфіденційність та вірогідність LSB. Передбачається, що противником (або кооперативними супротивниками)

може бути ОВМ, пристрій у розумному будинку, вузол в мережі накладання або хмарне сховище. Супротивники здатні «перевіряти» комунікації, відкидати транзакції, створювати помилкові транзакції та блоки, змінювати або видаляти дані у сховищі, аналізувати декілька транзакцій у спробі деанонімізувати вузол та підписувати підроблені транзакції для легітимізації узгоджуючих вузлів. Припускаємо, що стандартні методи безпечного шифрування використовуються в інтелектуальному будинку та накладних ярусах, які не можуть бути порушені супротивниками.

Безпека: у обговореннях вимог безпеки узагальнено різні механізми, які дозволяють LSB виконувати ключові вимоги безпеки.

У переліку атак на Blockchain наведено 12 конкретних атак безпеки, до яких мережі IoT або BC є особливо вразливими, та окреслюємо, як LSB захищає від них. У при переліку атак аналізуємо, наскільки стійкий LSB проти кожної атаки та ймовірність того, що напад може статися, базуючись на критеріях аналізу ризиків Європейського інституту стандартів зв'язку (ETSI) [14]. Ці критерії оцінюють кожну атаку виходячи з наступних п'яти показників: I) час: сукупний час, коли зловмисник спочатку виявить вразливість, а згодом планує та розпочне успішну атаку; II) експертиза: загальна експертиза, якою повинен володіти нападник основні принципи для того, щоб організувати атаку; III) знання: конкретна інформація, яка доступна про цільову систему, наприклад, конфігурація безпеки, IV) можливість: тривалість і характер (наприклад, постійний або переривчастий) доступу до системи, необхідний у V) для запуску атаки; V) обладнання: програмне забезпечення та/або обладнання, необхідне для проведення атаки. LSB виявляє понад високу стійкість до семи атак і високу стійкість до трьох атак. Це говорить про те, що LSB є високо безпечним.

Конфіденційність: LSB використовує анонімність та контроль користувачів для захисту конфіденційності користувачів у накладеному, розумному будинку та хмарному сховищі. Використання змінних РК в якості ідентичності вузлів, що накладаються, вводить аналогічний рівень анонімності

та конфіденційності, як у інших ОС на базі ВС (наприклад, Bitcoin). У деяких додатках IoT, дві кінцеві точки, які передають один одному, можливо, повинні знати реальну ідентичність один одного. Наприклад, страхова компанія з дому повинна знати реальну особу власника розумного будинку, яку вона страхує. У цих випадках відповідний генератор транзакцій використовує унікальний РК для зв'язку з кожним вузлом накладання. Збережені транзакції в загальнодоступному ВС шифруються за допомогою запитуваного РК для захисту конфіденційності вузлів накладення проти зловмисників, які намагаються зчитувати дані в полі метаданих мультисигнальної транзакції (рис. 2.2).

У розумному будинку LBM застосовує політику власників будинків, щоб забезпечити свій контроль над обміном даними, тим самим захищаючи його конфіденційність.

Хмарне сховище здатне використовувати дані різних пристроїв накладеного вузла, щоб знайти його справжні ідентичні дані. Для захисту від цієї деанонімізації пристроїв вузол накладання використовує різні кредити для зберігання даних кожного свого пристрою. Це заважає хмарі ідентифікувати різні пристрої одного і того ж вузла накладання.

Толерантність до відмов: толерантність відмов - це міра того, наскільки еластичною є архітектура для вузла відмов. LBM та OBM реалізують різні ключові функції, і несправність цих вузлів може вплинути на нормальну роботу LSB. Вихід з ладу LBM відключить відповідний розумний дім та пов'язані з ним пристрої від накладання. Розумні пристрої могли б обмінюватися даними на місцях, але не зможуть зберігати дані у хмарному сховищі чи спілкуватися з іншими пристроями, що накладаються.

Якщо OBM залишає накладення, члени кластера, пов'язані з цим OBM, не отримають жодної послуги. Однак вони можуть легко вибрати новий OBM, з яким потрібно зв’язатись. Відхід OBM також може вплинути на пропускну здатність накладання, оскільки існує менше OBM для генерування блоків. Однак механізм DTM, може вирішити цю ситуацію. Відхід від декількох OBM

також може вплинути на безпеку завдяки відповідним діям механізму розподіленої довіри. Оскільки ОВМ-користувачі довіряють один одному, потрібно перевірити меншу кількість транзакцій всередині блоку. Таким чином, коли кілька ОВМ відходять, ймовірність виявлення фальшивої транзакції в новому блоці зменшується, оскільки менше мереж ОВМ залишається в мережі для перевірки нових блоків.

Обговорення вимог безпеки:

− Конфіденційність - шифрування (симетричне або асиметричне) використовується для всіх транзакцій.

− Цілісність - кожна транзакція включає хеш усіх інших полів, що містяться в транзакції.

− Доступність - 1) LBM обробляє всі вхідні транзакції та контролює доступ до всіх пристроїв розумного дому, тим самим захищаючи їх від зловмисних запитів; 2) ОВМ надсилає транзакцію членам кластеру лише у тому випадку, якщо ключ, що міститься в транзакції, відповідає одній із записів його келіста. Це гарантує, що члени кластера отримують транзакції лише від авторизованих вузлів.

− Аутентифікація - у розумному будинку LBM створює загальний ключ між двома комунікаційними пристроями, який також використовується для аутентифікації. У накладанні кожен вузол повинен мати збережену транзакцію генезису в БК, яку потрібно автентифікувати. Оскільки транзакції прикуті до транзакції генезису, вузол аутентифікується, коли він має приватний ключ, що відповідає виводу РК транзакції, що зберігається в ВС. У хмарному сховищі використовуються стандартні протоколи аутентифікації.

− Невідмовність - операції з накладенням підписуються генератором транзакцій для досягнення невідмовності. Крім того, усі транзакції, що накладаються, зберігаються в загальнодоступному ВС, тому ні запитувач, ні реквізити не можуть заперечувати свою співучасть у транзакції.

До ключових атак на Blockchain належать:

1. Зростаюча атака - зловмисник компрометує ОВМ і генерує блоки з фальшивими транзакціями, щоб створити помилкову репутацію. Захистом від атаки є інший ОВМ, який здатний виявити підроблений блок під час кроку перевірки, коли він перевіряє вихід і власника книги.

2. Атака відмови в службі (DOS) - зловмисник заспамлює накладений вузол (ціль) великою кількістю транзакцій, щоб перекрити вузол таким чином, що він не може виділити жодних ресурсів для обробки справжніх транзакцій з інших вузлів. Захистом від цієї атаки є такі методи: 1) ОВМ не надсилають транзакцію членам кластеру, якщо вони не знайдуть відповідність з об'єктом у своєму келісті; 2) Кожен вузол накладання має поріг максимальної швидкості транзакцій, отриманих від накладання. Якщо поріг буде перевищено, лист ключів оновлюється, щоб запобігти передачі вузлами транзакцій цільовому вузлу.

3. Розподілена атака DOS (DDOS) - це розподілена версія вищевказаної атаки, де зловмисник скомпрометовано кілька вузлів накладання чи розумних домашніх пристроїв. Методами захисту від атаки є: 1) Зараження пристроїв та накладених вузлів утруднене через використання списків ключів ОВМ та того, що до пристроїв немає прямої доступності 2) У розумному будинку LBM дає змогу здійснювати всі транзакції перед надсиланням накладення 3) Операції з накладенням не є дійсними в межах розумного будинку, оскільки в способі накладення та розумному будинку використовуються різні методи шифрування; 4) У розумному будинку пристрій може спілкуватися з іншим пристроєм лише в тому випадку, якщо LBM встановив спільний ключ між ними. Методи, що запобігають атакам DOS у вищевказаному рядку, також корисні для пом’якшення DDOS.

4. Пристрій ін'єкційного нападу - зловмисник вводить в розумний дім підроблені пристрої, щоб отримати доступ до приватної інформації в приміщенні. Протидією цьому є ізоляція введеного, оскільки місцеві комунікації вимагають, щоб LBM встановив загальний ключ, який повинен бути схвалений власником будинку.

5. Поєднання атаки - зловмисник (який може бути SP або хмарним сховищем) пов'язує декілька даних у хмарі або транзакції в BC з тим самим ідентифікатором, щоб знайти реальну ідентичність анонімного вузла. Захистом є вузли накладення, які використовують унікальний PK для кожної транзакції в накладанні. Кожен пристрій аутентифікується хмарою за допомогою окремих облікових записів. Це запобігає зловмиснику зв’язувати дані кількох пристроїв одного і того ж користувача.

6. Атака скидання - OBM скидає транзакції до або від своїх членів кластера, щоб ізолювати їх від накладання. Захистом від даної атаки є член кластера, який може змінити OBM, з яким він пов'язаний, якщо він зауважує, що його транзакції не обробляються.

7. Модифікаційна атака - зловмисне хмарне зберігання змінює або видаляє збережені дані. Для запобігання цього транзакція запису включає хеш збережених даних, як показано на рис. 2.6, який слугує доказом того,що коли дані були збережені або востаннє змінені, дані не підлягають відновленню.

8. Хибна репутація - вузол накладання збільшує свою репутацію за рахунок збільшення випуску (0) у кожній з транзакцій більш ніж на один. Захистом слугує OBM, який визначає помилкове збільшення під час перевірки транзакцій, обговореної на рис. 2.3.

9. Публічна модифікація BC - зловмисник підставляє помилкову книгу блоків і робить її найдовшою книгою. Таким чином, усі вузли приймають головну книгу нападника як справжню книгу. Протидія цьому є алгоритм консенсусу, який обмежує кількість блоків, котрі OBM може генерувати протягом часового інтервалу. Це обмежить кількість зловмисних блоків, які OBM може додати, і тим самим запобіжить зловмисникові генерувати більшу книгу, ніж справжня книга.

10. Порушення інтервалу часу - шкідливий OBM генерує більше одного блоку за кожен консенсус-період. Протидією атаці є інші OBM, котрі визначають це, оскільки отримують більше дозволеної кількості блоків за

період консенсусу. Отже, рейтинг довіри для цього ОВМ буде знижений, і він буде ізольований від решти накладення.

11. Напад консенсусу - зловмисник надсилає помилкові запити на оновлення консенсусу. Щоб запит вважався дійсним, він повинен бути підписаний щонайменше половиною кількості ОВМ. Ймовірність цього дуже низька.

12. 51% атака - зловмисник контролює понад 51% ОВМ і намагається скомпрометувати алгоритм консенсусу, генеруючи підроблені блоки або більше дозволеної кількості блоків. Атаку можна виявити під час перевірки блоку (див. рис. 2.3) або за допомогою інших ОВМ на основі алгоритму консенсусу.

3.3. Висновки до розділу

Проаналізовано ключові оцінки різних аспектів діяльності LSB.

Проаналізовано програми для визначення ефективності низькоресурсних пристроїв та оцінено продуктивність накладення за допомогою них.

Проведено моделювання роботи таких мереж з метою оцінювання накладних витрат у LBM та споживання енергії.

Проаналізовано вплив розподілу потоків даних і транзакцій на мережу, та середній час обробки ОВМ для перевірки нових блоків.

При аналізі безпеки та конфіденційності було проаналізовано вимоги безпеки та основні можливі атаки на Blockchain та способи їх уникнення.

Здійснено тестування й визначено вплив кількості ОВМ на безпеку та пакетні накладні витрати, а також визначено відсоток транзакцій, який потрібно підтвердити для забезпечення максимальної стійкості до атак.

РОЗДІЛ 4
ОБҐРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

4.1. Визначення стадій технологічного процесу та загальної тривалості проведення НДР

Економічне обґрунтування дипломної роботи магістра є суттю даного розділу, оскільки, дозволяє встановити доцільність проведення науководослідних робіт і економічно обґрунтувати доцільність застосування тих чи інших засобів.

Метою дипломної роботи магістра є дослідження методів та засобів реалізації сервісів для вивчення іноземних мов

Як відомо, розробка надійної і ефективної інформаційної системи вимагає значних затрат часу. Слід зауважити, що затрати часу залежать від кваліфікації розробника і його можливостей. Розробник повинен у достатній мірі володіти навиками програмування, вміти адекватно застосовувати математичний апарат, бути добре обізнаним з об'єктом дослідження.

Розробку даної інформаційної системи можна поділити на такі етапи:

1) постановка задачі;
2) збір потрібної інформації і наступне її опрацювання;
3) прийняття рішень щодо вибору оптимального шляху розв'язання поставленої задачі;
4) аналіз математичної моделі інформаційної системи;
5) розробка алгоритму програми інформаційної системи;
6) налаштування середовища розробки і роботи вже готової програми;
7) написання програми;
8) написання і оформлення документації (електронної і паперової).

Для оцінки тривалості виконання окремих робіт використовують нормативи часу або попередній досвід. До таких нормативів відносять тривалість написання операцій (команд), які в деяких підприємствах

становлять: для одної операції - 0,5-1,6 год та 8 годин для п'яти операцій (тривалість зміни).

У разі їх відсутності звертаються до експертних оцінок по встановленню тривалості кожного етапу (стадії):

при трьох оцінках:

$$Tвс=(tmin+4tн.й+tmax)/6,$$

при двох оцінках:

$$Tвс=(3tmin+2tmax)/5,$$

де $T_{вс}$ - очікуване (середнє) значення тривалості виконання етапу (стадії);

$t_{min.}$, $t_{н.й.}$, t_{max}- відповідно мінімальна, найбільш імовірна і максимальна оцінки тривалості виконання етапу (стадії).

Для визначення загальної тривалості проведення НДР (розробки програмного продукту) доцільно дані витрат часу на виконання окремих стадій (етапів) звести у табл. 4.1.

Витрати часу наукового керівника на виконання окремих стадій (етапів) при недостатній кількості інформації доцільно приймати в межах 5% сумарних витрат часу інженерів на виконання цих стадій (етапів).

Таблиця 4.1

Основні етапи і час їх виконання у НДР

№ з/п	Етап	Середній час виконання етапу, год	
		інженер	керівник
1	постановка задачі	3	10
2	отрібної інформації і наступне її опрацювання	10	5

Продовж. табл. 4.1

з/п	Етап	Середній час виконання етапу, год	
		інженер	керівник
3	прийняття рішень щодо вибору оптимального шляху розв'язання поставленої задачі	5	4
4	аналіз математичної моделі інформаційної системи	15	10
5	розробка алгоритму програми інформаційної системи	15	5
6	налаштування середовища розробки і роботи вже готової програми	2	1
7	написання програми	80	5
8	написання і оформлення документації (електронної і паперової)	20	10
Разом		150	50

4.2. Визначення витрат на оплату праці та відрахувань на соціальні заходи

Відповідно до Закону України “Про оплату праці” заробітна плата – це “винагорода, обчислена, як правило, у грошовому виразі, яку власник або уповноважений ним орган виплачує працівникові за виконану ним роботу”.

Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його праці та господарської діяльності підприємства. Заробітна плата складається з основної та додаткової оплати праці.

Основна заробітна плата нараховується на виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами і не залежить від результатів господарської діяльності підприємства.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов’язані з виплатами за фактично відпрацьований час. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, умов виробництва, кваліфікації виконавців. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

Основна з/п складається із прямої з/п і доплати, яка при укрупнених розрахунках становить 25% - 35% від прямої з/п. При розрахунку з/п кількість робочих днів в місяці слід приймати – 25,4 дні/міс., що відповідає 203,2 год./міс. Розмір місячних окладів керівника та інженерів слід приймати згідно існуючих на даний час норм. Основна заробітна плата розраховується за формулою:

$$З_{осн}=Т_{с} \text{ x } К_{г}, \quad (4.1)$$

де $Т_с$ – тарифна ставка, грн.;

$К_г$ - кількість відпрацьованих годин.

Посадові оклади (тарифні ставки) за розрядами Єдиної тарифної сітки визначаються шляхом множення окладу (ставки) працівника 1 тарифного розряду на відповідний тарифний коефіцієнт. У разі коли посадовий оклад (тарифна ставка) визначені у гривнях з копійками, цифри до 0,5 відкидаються, від 0,5 і вище - заокруглюються до однієї гривні. У 2019 році посадові оклади (тарифні ставки) розраховуються згідно з Законом України "Про Державний бюджет України на 2019 рік".

Мінімальна зарплата в 2019 р. прирівняна до прожиткового мінімуму для працездатних осіб (тобто з січня по грудень - 4173 гривень), в погодинному розмірі з 1 січня — 25,13 гривень, приймемо 118 грн. для інженера, для керівника — 178 грн.

Тарифні ставки: керівник проекту – 178 грн./год., інженер – 118 грн./год.

Основна заробітна плата становитиме:

$$Зосн=Тосн \text{ х } КГОД.$$

Керівник проекту

$$З_{осн}=178х50=8900грн.$$

Інженер

$$З_{осн}=118х150=17700грн.$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати:

$$Здод=ЗоснхКдопл\ , \qquad (4.2)$$

Керівник проекту

$$З_{дод}=8900х0.1=890\ грн.$$

Інженер

$$З_{дод}=17700х0.1=1770\ грн,$$

де $К_{допл.}$ – коефіцієнт додаткових виплат працівникам 0,1.

Звідси загальні витрати на оплату праці ($В_{О.П.}$) визначаються за формулою, і становлять:

$$ВОП=ЗОСН+З\ ДОД\ , \qquad (4.3)$$

Керівник проекту: $В_{ОП}=8900+890=9790\ грн.$

Інженер : $B_{ОП}$=17700+1770=19470 *грн*.

Таким чином загальна сума становить 29260 грн. Крім того, слід визначити відрахування на соціальні заходи:

− податок на доходи фізичних осіб: 18%;

− військовий збір 1,5%;

− єдиний соціальний внесок 22%.

У сумі зазначені відрахування становлять 41,5%.

Отже, сума відрахувань на соціальні заходи буде становити:

$$B_{с.з.} = ФОП \text{x} 0{,}415,\ B_{с.з.} = 29260 \text{x} 0{,}415 = 12143 \text{ грн},$$

де *ФОП* – фонд оплати праці, грн.

Проведені розрахунки витрат на оплату праці зведемо у наступну табл. 4.2.

Таблиця 4.2

Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Додаткова заробітна плата, грн.	Нарах. на ФОП, грн.	Всього витрати на оплату праці, грн. 6=3+4+5
		Тарифна ставка, грн.	К-сть від-працьов. год.	Фактично нарах. з/пл., грн.			
1.	Керівник проекту	178	50	8900	890	4063	13853
2.	Інженер	118	150	17700	1770	8080	27550
Разом				26600	2660	12143	41403

4.3. Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою:

$$З_е = W \text{x} T \text{x} S \,, \qquad (4.4)$$

де W – необхідна потужність, кВт;

T– кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Згідно з постановою НКРЕКП від 05 жовтня 2018 року № 1177 вартість електроенергії становить 182,28 коп./кВт.год.

Потужність комп'ютера – 300 Вт з підключеним маршрутизатором, кількість годин роботи обладнання згідно табл. 4.1 – 200 годин.

$$З_е = 0{,}3 \text{x} 200 \text{x} 1{,}8228 = 109{,}37 \text{ грн.}$$

4.4. Розрахунок витрат на матеріали

Результати розрахунку затрат на матеріали зводяться в табл. 4.3.

Таблиця 4.3

Визначення величини затрат на матеріали

Найменування матеріальних ресурсів	Одиниця виміру	Норма витрат	Ціна за одиницю грн	Затрати матеріалів грн	Транспортнозаготівельні витрати, грн	Загальна сума витрат на матеріали, грн
Папір А4-80	Пачка	1	115	115	-	115
Ватман	Штук	8	28	224	-	224
Коректор	Штук	1	20	20	-	20
Картки інтернет Київстару	Штук	1	500	500	-	500
Разом						859

4.5. Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення.

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Для цієї групи річна норма амортизації дорівнює 60 % (квартальна – 15 %).

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$A = \frac{Б_в \cdot Н_А}{100}, \quad (4.5)$$

де A – амортизаційні відрахування за звітний період, грн.

$Б_В$ – балансова вартість комп'ютера, на початок звітного періоду, грн.

$Н_А$ – норма амортизації, %.

$$\text{А} = \frac{34000 * 15\%}{100\%} = 5100.$$

4.6. Обчислення накладних витрат

Накладні витрати пов'язані з обслуговуванням виробництва, утриманням апарату управління підприємства (фірми) та створення необхідних умов праці.

Накладні витрати можуть становити 20% від суми основної та додаткової заробітної плати працівників:

$$Н_В = В_{О.П} \text{х.} 0.2, \quad (4.6)$$

$$Н_{в}=29260х0,2=5852 \text{ грн.}$$

4.7. Складання кошторису витрат та визначення собівартості НДР

Результати проведених вище розрахунків зведемо у табл. 4.3. Собівартість ($С_В$) НДР розрахуємо за формулою:

$$Св=Во.п.+Вс.з.+Зм.в.+Зе+Тв+А+Нв\ , \qquad (4.7)$$

$$С_{в}=29260+12143+109,37+859+5100+5852=53323,37 \text{ грн.}$$

Таблиця 4.4

Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці (основну і додаткову заробітну плату)	29260	54,87
Відрахування на соціальні заходи	12143	22,77
Матеріальні витрати	859	1,61
Витрати на електроенергію	109,37	0,21
Амортизаційні відрахування	5100	9,56
Накладні витрати	5852	10,97
Собівартість	53323,37	100

4.8. Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

$$Ц = \frac{C_B \cdot (1 + Р_{рен}) + К \cdot В_{н.і.}}{К} \cdot (1 + ПДВ), \quad (4.8)$$

де $P_{рен.}$ – рівень рентабельності, 30 %;

К – кількість замовлень, од. (встановлюється лише при розробці програмного продукту та мікропроцесорних систем);

$B_{н.і.}$ – вартість носія інформації, грн. (встановлюється лише при розробці програмного продукту);

ПДВ – ставка податку на додану вартість, (20 %).

Оскільки розробка є прикладною, і використовуватиметься тільки для одного підприємства, то для розрахунку ціни не потрібно вказувати коефіцієнти К та Ві.н , оскільки їх в даному випадку не потрібно.

Тоді, формула для обчислення ціни розробки буде мати вигляд:

$$Ц = C_B \cdot (1 + Р_{рен}) \cdot (1 + ПДВ),$$

$$Ц = 53323{,}37 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2).$$

Таким чином ціна рівна 83184,46 грн.

Визначимо величину прибутку:

$$П = Ц - Св . \quad (4.9)$$

Згідно даної формули отримаємо 29861, 09грн.

4.9. Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Економічна ефективність (E_p) полягає у відношенні результату виробництва до затрачених ресурсів:

$$E_P = П / C_в . \quad (4.10)$$

де $П$ – прибуток;

$C_В$ – собівартість.

$$E_P = 29861,09 / 53323,37 = 0,56.$$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень (T_p):

$$T_P = \frac{1}{E_P}, \quad (4.11)$$

$$T_P = 1 / 0,56 = 1,79 р.$$

Про доцільність розробки програми можна сказати при врахуванні наступних критеріїв (табл. 4.5).

Таблиця 4.5

Техніко-економічні показники НДР

№ п/п	Показник	Значення
1	Собівартість, грн.	53323,37
2	Плановий прибуток, грн.	29861,09

Продовж. табл. 4.5

3	Ціна, грн.	83184,46
4	Економічна ефективність	0,56
5	Термін окупності, рік	1,79 року

4.10. Висновок до розділу

В даному розділі завдяки результату проведених розрахунків отриманий результат показує, що розробка матиме оптимальну економічну ефективність 0,56 і термін окупності становитиме майже два роки (1,79 року). Варто зазначити, що дані розрахунки носять номінальний характер і основна їх мета оцінити приблизну вартість дослідження та створення даного продукту. Номінальний характер розрахунків зумовлений тим, що даний програмний продукт має дослідницьке призначення.

РОЗДІЛ 5
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

5.1. Охорона праці

При досліджені алгоритмічного та програмного забезпечення Blockchain при побудові мережевих IoT-інфраструктур було здійснено з дотриманням норм та правил з охорони праці та вимог техніки безпеки.

Згідно до санітарних правил і норм роботи з візуальними дисплеями електронно-обчислювальних машин ДСанПІН. 3.3.2.007-98. [33]. Температура повітря у приміщенні визначається температурою атмосферного повітря і джерелами виділення тепла. Ними є електрообладнання, сонячна радіація і теплота, яку виділяє організм людини. Суттєвого підвищення температури внаслідок дії сонячної радіації вдається уникнути, закривши вікна шторами. В даному випадку приміщення обладнане системою опалення та кондиціонером Panasonic. При низьких температурах у холодну пору року стабільність температури повітря підтримує опалювальна система. Як результат, протягом року температура повітря у приміщенні не виходить за встановлені межі. Тому по цим параметрам приміщення відповідає нормам викладених у ДСН 3.3.6.042-99 [29]. Температура приміщення становить $+22^0$С, що відповідає нормі [29].

Згідно ДБН В.2.5-28:2018 [30] приміщення, що розглядається, повинне мати природне і штучне освітлення. Природне освітлення приміщення відбувається за системою однобічного бічного освітлення. Природне світло проникає у приміщення через дві віконні отвори, які мають регулювальні пристрої для відкривання. Також наявні штори та жалюзі з можливістю захисту працюючих від прямого попадання сонячних променів і регулювання рівня освітленості в приміщенні. Вікна приміщення орієнтовані на північний схід. Оскільки будинок розташований у відносній віддаленості від прилеглих будівель, то які-небудь перешкоди природному освітленню розглянутого

приміщення відсутні. Всередині приміщення стіни обклеєні світлими шпалерами, стеля побілена (переважає білий колір), у якості підлогового покриття використаний паркет світлого кольору.

Під час дослідження в приміщенні використовується система загального рівномірного штучного освітлення. Люстра з трьома світлодіодними лампочками E1456Led. Люстра знаходиться точно по центру приміщення.

У приміщенні, що розглядається, відсутні ознаки підвищеної та особливої небезпеки ураження персоналу електрострумом. Через це приміщення за групою електронебезпечності відноситься до приміщень без підвищеної небезпеки ураження струмом.

Споживачі електроенергії у приміщенні – персональні комп'ютери, системні блоки, монітори та принтер приєднуються до електромережі окремо, згідно наказу про затвердження правил охорони праці під час експлуатації електронно-обчислювальних машин [31].

Усі електроприлади живляться від мережі змінного струму 220В/50Гц. Лінія електроживлення виконана шляхом прокладання фазового, нульового робочого та нульового захисного провідників (нульовий захисний провідник використовується для занулення). Усі електричні розетки, що використовуються для підключення апаратури, мають спеціальні контакти для підключення нульового захисного провідника. Нульовий робочий провідник не використовується як нульовий захисний.

Під час аналізу приміщення з улаштування електрообладнання з відповідним рівнем захисту, у просторі біля технологічних установок і комунікацій, було визначено, що приміщення відносяться до категорії В.

Ймовірними причинами виникнення пожару можуть бути несправність електрообладнання (кабелів, розеток), короткі замикання внаслідок виходу з ладу чи експлуатації несправного електроустаткування, порушення правил протипожежної безпеки тощо.

Експлуатація ліній електромережі практично повністю унеможливлює виникнення електричного джерела загоряння в наслідок короткого замикання

та перевантаження проводів. Застосовуються дроти з важкогорючою і негорючою ізоляцією.

Для гасіння пожежі приміщення обладнане ручними вуглекислотними вогнегасниками ВВК-1,4. У загальному коридорі встановлені пінні вогнегасники. Розглянуте приміщення обладнане датчиками централізованої системи пожежної сигналізації. Розроблено план евакуації персоналу і найбільш коштовного устаткування (майна), з урахуванням наказу міністерства внутрішніх справ України «Про затвердження правил пожежної безпеки в Україні» [32].

Внаслідок проведеного аналізу умов праці, умови електробезпеки і пожежної безпеки приміщення, де було проведення дослідження алгоритмічного та програмного забезпечення Blockchain при побудові мережевих IoT-інфраструктур. З урахуванням визначених умов можна зробити висновок, що приміщення відповідає дійсним нормативним вимогам.

5.2. Врахування шкідливих і небезпечних умов праці персоналу в ході провадження виробничої діяльності суб’єктами господарювання, що використовують об’єкти підвищеної небезпеки.

Важливим питанням є забезпечення належної діяльності, пов’язаної з експлуатацією об’єктів підвищеної небезпеки (далі - ОПН), захистом життя і здоров’я людей та довкілля від шкідливого впливу аварій на цих об’єктах шляхом запобігання їх виникненню, обмеження (локалізації) розвитку і ліквідації наслідків.

ОПН – це об’єкт, на якому використовуються, виготовляються, переробляються, зберігаються або транспортуються одна або кілька небезпечних речовин чи категорій речовин у кількості, що дорівнює або перевищує нормативно встановлені порогові маси, а також інші об’єкти як такі, що відповідно до закону є реальною загрозою виникнення надзвичайної ситуації техногенного та природного характеру [25].

На відміну від ОПН потенційно небезпечних об’єкт (далі - ПНО) – це об’єкт, на якому можуть теж використовуватися або виготовляються, переробляються, зберігаються чи транспортуються небезпечні речовини, біологічні препарати, а також інші об’єкти, що за певних обставин можуть створити реальну загрозу виникнення аварії.

Серед наявних на певній територій ПНО шляхом проведення ідентифікації визначають ОПН.

За суб’єктами господарської діяльності (далі - СГД), що використовують ОПН, здійснюється державний нагляд і контроль. Його здійснюють уповноважені законами органи влади, в тому числі спеціально уповноважені центральні органи виконавчої влади та їх відповідні територіальні органи, до відання яких віднесені питання охорони праці, забезпечення екологічної безпеки та охорони навколишнього природного середовища, захисту населення і територій від надзвичайних ситуацій техногенного та природного характеру, пожежної безпеки, санітарно-епідемічної безпеки, містобудування.

СГД, який експлуатує ОПН, зобов’язаний:

− Вживати заходів, направлених на запобігання аваріям, обмеження і ліквідацію їх наслідків та захист людей і довкілля від їх впливу;

− повідомляти про аварію, що сталася на ОПН, і заходи, вжиті для ліквідації її наслідків, органи виконавчої влади та органи місцевого самоврядування та населення;

− забезпечувати експлуатацію ОПН з додержанням мінімально можливого ризику.

СГД ідентифікує ОПН відповідно до кількості порогової маси небезпечних речовин. Нормативи порогової маси небезпечних речовин встановлюються КМ України [26].

Порогова маса небезпечних речовин – нормативно встановлена маса окремої небезпечної речовини або категорії небезпечних речовин чи сумарна маса небезпечних речовин різних категорій.

Під терміном «небезпечна речовина» розуміють хімічну, токсичну, вибухову, окислювальну, горючу речовину, біологічні агенти та речовини біологічного походження (біохімічні, мікробіологічні, біотехнологічні препарати, патогенні для людей і тварин мікроорганізми тощо), які становлять небезпеку для життя і здоров'я людей та довкілля, сукупність властивостей речовин і/або особливостей їх стану, внаслідок яких за певних обставин може створитися загроза життю і здоров'ю людей, довкіллю, матеріальним та культурним цінностям.

Для ідентифікації ОПН до небезпечних речовин за їх властивостями відносяться такі категорії речовин:

1) Горючі (займисті) гази – гази, які утворюють у повітрі при нормальному тиску суміші, що сприяють поширенню полум'я в детонаційному чи дефлаграційному режимі або можуть горіти в повітрі в дифузійному режимі при витіканні струменем (факельне горіння), у тому числі:

- Горючі (займисті) стиснуті гази – гази, які знаходяться в апаратах, резервуарах або трубопроводах під тиском, що перевищує 0,1 Мпа, і не можуть перебувати в рідкій фазі.
- Горючі (займисті) зріджені гази під тиском - гази, які знаходяться в апаратах, резервуарах або трубопроводах у рідкій фазі під тиском, що перевищує 0,1 Мпа, та при температурі, що дорівнює або перевищує температуру навколишнього середовища.
- Горючі (займисті) кріогенно зріджені гази – гази, які знаходяться в апаратах, резервуарах або трубопроводах у рідкій фазі під тиском, що перевищує 0,1 Мпа, та при температурі нижчій від температури навколишнього середовища.

2) Горючі рідини – рідини, які можуть самозайматися, а також займатися за наявності джерела горіння і самостійно горіти після його видалення. Горючі рідини з температурою спалаху, що дорівнює або менша 61 ^{0}C у закритому тиглі або температурою спалаху, що дорівнює або менша 66 ^{0}C у відкритому тиглі, належать до легкозаймистих. Особливо небезпечними є легкозаймисті

рідини, температура спалаху яких не перевищує 28 ^{0}С (згідно з ГОСТ 12.1.044-89).

3) Горючі рідини, перегріті під тиском – горючі рідини згідно з ГОСТ 12.1.044-89, які знаходяться в апаратах, резервуарах або трубопроводах під тиском при температурі, що перевищує температуру кипіння при атмосферному тиску в 1,25 і більше разів.

Якщо рідина являє собою суміш горючих рідин, за температуру кипіння при атмосферному тиску береться температура википання половини маси рідини. Якщо даних про таку температуру немає, за температуру кипіння береться температура на початку кипіння суміші (фракції).

За розрахункову береться максимальна температура за регламентом, робочими інструкціями або іншою технічною документацією. Якщо передбачено блокування за температурою, за розрахункову береться температура блокування;

4) Вибухові речовини – рідкі або тверді речовини чи суміші речовин, які під впливом зовнішніх факторів здатні швидко змінювати свій хімічний склад, а цей процес само розповсюджуватися з виділенням великої кількості тепла і газоподібних продуктів (клас 1 згідно з ГОСТ 19433-88), у тому числі:

− Речовини або суміші речовин, які, згораючи в режимі детонації, утворюють ударну хвилю в повітрі.

− Речовини або суміші речовин, екзотермічні реакції з якими у режимі детонації, дефлаграції або теплового вибуху в оболонці (апараті, резервуарі, трубопроводі або в спеціальному виробі) призводять до руйнування цієї оболонки з утворенням ударної хвилі в повітрі та розкиданням уламків.

Вибухові речовини поділяють на ініціюючі (первинні), бризантні (вторинні) та піротехнічні.

Ініціюючі (первинні) вибухові речовини – речовини, які під впливом теплових або механічних зовнішніх факторів (промінь вогню, тертя, слабкий удар тощо) здатні до швидкого хімічного перетворення з виділенням тепла і газоподібних продуктів.

Бризантні (вторинні) вибухові речовини – речовини, які під впливом ініціюючих вибухових речовин або значних теплових чи механічних зовнішніх факторів здатні до хімічного перетворення з виділенням тепла і газоподібних продуктів. Піротехнічні суміші – композиції на основі окислювача та горючої речовини з різними функціональними домішками, що здатні під впливом ініціюючих вибухових речовин або під значним впливом зовнішніх факторів до екзотермічних реакцій із світловим, тепловим, звуковим, реактивним або димовим (зокрема сльозогінним) ефектом;

5) Речовини-окисники – речовини 5 класу небезпеки (згідно з ГОСТ 19433-88), у тому числі:

- Речовини, які підтримують горіння, викликають та/або сприяють спалахуванню інших речовин у результаті екзотермічної окисно-відновної реакції, температура розкладання яких не перевищує 65 ^{0}С та/або час горіння суміші окисника яких з органічною речовиною (дубовою тирсою) не перевищує часу горіння еталонного окисника з дубовою тирсою (наприклад перманганат калію, бромат калію, перхлорат калію тощо).
- Органічні пероксиди (речовини з двовалентною структурою кисню, які можуть вважатися похідними пероксиду водню).

До цієї категорії відносяться речовини, які підтримують процес горіння (наприклад кисень, озон, оксиди азоту та інші речовини в зрідженому стані);

6) Високотоксичні та токсичні речовини (табл. 5.1) – речовини, які мають властивості, зазначені в таблиці (ГОСТ 12.1.007-76).

Токсичність речовин при пероральному впливі на тварин (дискримінуючи доза) визначено методом фіксованої дози за рекомендаціями Конвенції про трансграничний вплив промислових аварій (1992 рік).

До високотоксичних відносяться речовини, які за своїми біологічними властивостями та токсичністю належать до 1 класу небезпеки, а до токсичних – речовини, які за своїми біологічними властивостями та токсичністю належать до 2 класу небезпеки згідно з ГОСТ 12.1.007-76 і 12.1.005-88 та переліками граничнодопустимих концентрацій шкідливих речовин, затвердженими МОЗ.

7) Речовини, які становлять небезпеку для довкілля (високотоксичні для водних організмів) – речовини, які мають властивості, зазначені в таблиці, згідно з Конвенцією про трансграничний вплив промислових аварій (1992 рік); речовини, які можуть здійснювати тривалий негативний вплив на водне середовище (табл. 5.2).

Таблиця 5.1

Високотоксичні та токсичні речовини

Клас речовини	ГДК у повітрі робочої зони, міліграмів на 1 куб. метр	Середня смертельна доза (LD50) при потраплянні в шлунок, грамів на 1 кг ваги тіла	Середня смертельна доза (LD50) при впливі на шкіру, міліграмів на 1 кг ваги тіла	Середня смертельна концентрація (LD50) у повітрі міліграмів на 1 куб. метр	Дискримінуюча доза, міліграмів на 1 кг ваги тіла
Високотоксична	менш як 0,1	менш як 15	менш як 100	менш як 500	менш як 5
Токсична	0,1 - 1	15 - 150	100 - 500	500 - 5000	5

Таблиця 5.2

Речовини, які становлять небезпеку для довкілля

Смертельна концентрація (LC50), при впливі на рибу протягом 96 годин, міліграмів на літр	Ефективна концентрація (EC50) при впливі на дафнії протягом 48 годин, міліграмів на 1 літр	Інгібуюча концентрація (IC50) при впливі на водорості протягом 72 годин, міліграмів на 1 літр
не більш як 10	не більш як 10	не більш як 10

За видами аварій, що можуть статися виходячи з властивостей небезпечних речовин, та за впливом уражаючих факторів цих аварій категорії небезпечних речовин об’єднуються у наступні групи:

– Група 1 (вибух) – горючі (займисті) гази, горючі рідини, перегріті під тиском, ініціюючі (первинні), бризантні (вторинні) та піротехнічні вибухові

речовини, речовини-окислювачі, речовини, які вступають у бурхливу реакцію з водою з виділенням горючих та/або вибухонебезпечних чи токсичних газів.

− Група 2 (пожежа) – горючі (займисті) гази, горючі рідини, горючі рідини, перегріті під тиском, речовини-окисники, а також речовини, які вступають у бурхливу реакцію з водою з виділенням горючих та/або вибухонебезпечних чи токсичних газів.

− Група 3 (шкідливі для людей і довкілля) – високотоксичні речовини, токсичні речовини, речовини, які становлять небезпеку для довкілля (високотоксичні для водних організмів), речовини, які становлять небезпеку для довкілля (токсичні для водних організмів) та/або можуть здійснювати довгостроковий негативний вплив на водне середовище, а також речовини, які вступають у бурхливу реакцію з водою з виділенням горючих та/або вибухонебезпечних чи токсичних газів.

Індивідуальними небезпечними речовинами є речовини та суміші речовин, для яких встановлено значення нормативів порогових мас, що відрізняються від значень нормативів порогових мас тих категорій, до яких ці речовини можна віднести за їх властивостями (нормативи порогових мас деяких індивідуальних небезпечних речовин новедено у таблиці 5.3, а небезпечних речовин за категоріями – у табл. 5.4).

Таблиця 5.3

Нормативи порогових мас деяких індивідуальних небезпечних речовин

Найменування індивідуальної небезпечної речовини	Порогова маса, тонн		Категорії та групи, до яких може бути віднесена речовина	
	1 клас	2 клас	категорія	група
Алкіли свинцю	50	5	2, 3, 7, 9	1, 2, 3
Амонію нітрат*	2500	350	5	1
Амонію нітрат (добрива)**	5000	1250	5	1
Арсенатний ангідрид, арсенатна кислота та/або її солі	2	1	7, 8, 9	3

Продовж. табл.5.3

Арсенвмісний водень (арсін)	1	0,2	1, 7, 9	1, 2, 3
Ацетилен	50	5	1	1, 2
Берилій та його сполуки у перерахунку на берилій	0,01		3, 7	2, 3
Бром	50	20	6, 8, 9	1, 2, 3
Водень	50	5	1	1, 2
Вугільної кислоти дихлорангідрид (фосген)	0,75	0,3	8	3
Етилену оксид	50	5	1, 5, 8	1, 2
Кисень	2000	200	6	1, 2
Метанол	5000	500	2, 3, 9	1, 2, 3
Метилізоціанат	0,15		2, 3, 7	1, 2, 3
4,4-метилен-біс(2-хлоранілін) та/або солі в порошкоподібному стані	0,01		3, 7, 9	1, 2, 3
Поліхлоридні дибензофурани та поліхлоридні дибензодіоксини (включаючи ТХДД), розраховані із застосуванням коефіцієнта токсичного еквіваленту ТХДД***	0,001		7, 9	3
Пропілену оксид	50	5	2, 3, 8	1, 2
Сірководень	50	5	1, 8	1, 2
Толуїдиндиізоціонат	100	10	3, 7	1, 2, 3
Формальдегід (концентрація понад 90 відсотків)	50	5	1, 8, 9	1, 2, 3
Фосфористий водень (фосфін)	1	0,2	7, 9	3
Хлор	25	10	6, 8	1, 2

* Масовий вміст азоту в амонію нітраті та його сумішах становить понад 28 відсотків, а водяні розчини амонію нітрату містять понад 90 відсотків азоту.

** Масовий вміст азоту в простих добривах на основі амонію нітрату, а також у складних добривах на його основі (з фосфатом та/або поташем) становить понад 28 відсотків.

*** Коефіцієнти токсичного еквіваленту (ХДД – хлордибензодіоксин, ХДФ – хлордибензофуран, Т – тетра, П – пента, Гкс – гекса, Гпт – гепта, О - окта):

Таблиця 5.4

Нормативи порогових мас небезпечних речовин за категоріями

Номер категорії	Найменування категорії небезпечних речовин	Порогова маса, тонн		Групи, до яких може бути віднесена речовина відповідної категорії
		1 клас	2 клас	
1	Горючі (займисті) гази	200	50	1, 2
2	Горючі рідини	50000	5000	2
3	Горючі рідини, перегріті під тиском	200	50	1, 2
4	Ініціюючі вибухові речовини	50	10	1
5	Бризантні (вторинні) та піротехнічні вибухові речовини	200	50	1
6	Речовини-окисники	200	50	1, 2
7	Високотоксичні речовини	20	5	3
8	Токсичні речовини	200	50	3

5.3. Оцінка підготовки суб’єкта господарювання до відновлення порушеного виробництва

Визначення об’єктів підвищеної небезпеки 1 або 2 класу. Ідентифікації підлягають всі СГД, у власності або користуванні яких є об’єкти, де можуть використовуватися або виготовляються, переробляються, зберігаються чи транспортуються небезпечні речовини (далі - ПНО), а також на СГД, які мають намір розпочати будівництво ПНО.

Окремо ідентифікуються ПНО, у яких є радіоактивні речовини, об’єкти розвідки, видобутку та розробки корисних копалин, перевезення транспортом небезпечних речовин за межами СГД, гідротехнічні споруди, ПНО із наявністю на них відходів.

СГД, у власності або користуванні якого є хоча б один ПНО чи який має намір розпочати будівництво такого об’єкта, організовує проведення його ідентифікації.

ПНО вважається ОПН відповідного класу у разі, коли значення сумарної маси небезпечної або декількох небезпечних речовин, що використовуються або виготовляються, переробляються, зберігаються чи транспортуються на об’єкті, дорівнює або перевищує встановлений норматив порогової маси.

ПНО вважається апарат або сукупність пов’язаних між собою потоками в технологічний цикл апаратів, об’єднаних за адміністративною та/або територіальною ознакою. ПНО за адміністративною ознакою вважається структурний підрозділ (виробництво, цех, відділення, дільниця, тощо) СГД. У разі коли відстань між потенційно небезпечними об’єктами за адміністративною ознакою не досягає 500 метрів, вони вважаються одним ПНО. У разі коли до складу ПНО за адміністративною ознакою входять дільниці, відділення або окремі установки з небезпечними речовинами, що знаходяться на відстані понад 500 метрів одна від одної, вони вважаються окремими потенційно небезпечними об’єктами.

Під час проведення ідентифікації для кожного ПНО розраховується сумарна маса кожної небезпечної речовини із зазначених у нормативах порогових мас індивідуальних небезпечних речовин або кожної небезпечної речовини, яка за своїми властивостями може бути віднесена до будь-якої категорії або до декількох категорій небезпечних речовин згідно із зазначеними нормативами. У разі коли небезпечна речовина може бути віднесена одночасно до кількох категорій небезпечних речовин, використовується значення речовини у тій категорії, в якій її порогові маса найменша. У разі коли сумарна маса жодної індивідуально небезпечної речовини або небезпечної речовини будь-якої категорії не перевищує 1 відсотка порогової маси небезпечних речовин другого класу, об’єкт не відноситься до ОПН.

За сумарну масу небезпечної речовини береться:

1) Для сховищ (резервуарів) – сумарна маса небезпечної речовини, що може в них знаходитися при повному завантаженні відповідно до технологічного регламенту, проектної або іншої документації. При цьому обов'язково зазначається, для яких обсягів речовини виконувалися розрахунки. У разі зміни норм завантаження процедура ідентифікації виконується повторно згідно з вимогами.

2) Для технологічних установок – максимальна сумарна маса, що може знаходитися в апаратах і трубопроводах відповідно до технологічного регламенту, умов процесу та правил експлуатації.

3) Для обладнання колонного типу – сумарна маса небезпечної речовини при максимальному рівні рідини на тарілках. Для апаратів, у яких застосовуються наповнювачі з пористим інертним середовищем, сумарна маса небезпечної речовини визначається з урахуванням максимального обсягу вільного простору.

4) Для внутрішньозаводських, міжцехових, внутрішньоцехових, внутрішньо складських трубопроводів – сумарна маса небезпечної речовини у всьому трубопроводі.

ПНО відноситься до ОПН 1 класу, якщо сумарна маса хоча б однієї індивідуальної небезпечної речовини або небезпечної речовини однієї категорії на ПНО, що розрахована згідно вище зазначеного порядку, дорівнює пороговій масі небезпечних речовин 1 класу згідно з табл. 5.3 і 5.4 до нормативів або перевищує таку масу.

У разі коли сумарна маса жодної однієї індивідуальної небезпечної речовини або небезпечної речовини однієї категорії не перевищує порогову масу небезпечних речовин 1 класу, за її властивостями визначаються категорії, до яких вона може бути віднесена згідно нормативів і табл. 5.1. Якщо індивідуальна небезпечна речовина за своїми властивостями може бути віднесена до кількох категорій, її сумарна маса враховується під час визначення сумарної маси небезпечних речовин у кожній категорії, до якої вона може бути віднесена.

Порогову масу небезпечних речовин однієї групи або категорії визначають за формулою:

$$Q_{пгк} = \Sigma q_i : \Sigma(q_i / Q_i), \quad (5.1)$$

де $Q_{пгк}$ – порогова маса небезпечних речовин однієї групи або категорії;

q_i – сумарна маса небезпечної речовини або категорії і небезпечної речовини, що перебуває на об'єкті;

Q_i – норматив порогової маси небезпечної речовини або категорії небезпечної речовини відповідного класу;

і – змінюється від 1 до n, де n – загальна кількість індивідуальних небезпечних речовин та категорій небезпечних речовин.

Розрахунок значення порогової маси небезпечних речовин однієї категорії або групи для 1 класу проводиться з використанням значення Q для 1 класу і для 2 класу – з використанням значення Q_i для 2 класу згідно з таблицями 5.3 і 5.4 до нормативів.

Якщо речовина, зазначена у таблиці 1 до нормативів, належить за своїми властивостями також до однієї з категорій речовин, зазначених у таблиці 5.4 до нормативів, визначення $Q_{пгк}$ здійснюється з урахуванням порогової маси, наведеної у таблиці 5.3 до нормативів.

ПНО відноситься до ОПН 1 класу, якщо сумарна маса небезпечних речовин хоча б однієї категорії дорівнює пороговій масі небезпечних речовин 1 класу цієї категорії або перевищує таку масу.

У разі коли сумарна маса небезпечних речовин жодної категорії не перевищує порогову масу небезпечних речовин 1 класу для цієї категорії, за властивостями індивідуальних небезпечних речовин і категорій небезпечних речовин визначаються групи, до яких вони можуть бути віднесені. Порогова маса небезпечних речовин зазначених груп розраховується за формулою:

$$P_1 = \frac{P_t}{K_t} \ , \qquad (5.2)$$

де K_t – коефіцієнт перерахунку визначають за табл. 5.5

Таблиця 5.5

Коефіцієнти K_t для перерахування рівнів радіації на різний час t після вибуху

t,год	K_t	t,год	K_t	T,год	K_t	T,год	K_t
0.5	2.3	4.5	0.165	8.5	0.077	16	0.036
1	1	5	0.145	9	0,072	20	0.027
1.5	0.615	5.5	0.13	9.5	0.068	24	0.022
2	0.435	6	0.116	10	0.063	28	0.018
2.5	0.333	6.5	0.106	10.5	0.06	32	0.015

Якщо небезпечна речовина за своїми властивостями може бути віднесена до кількох груп, її сумарна маса враховується у кожній групі, до якої вона може бути віднесена.

У разі коли небезпечна речовина може бути віднесена одночасно до кількох груп небезпечних речовин, під час визначення класу небезпеки використовується зазначення речовини у тій групі, де її розрахована порогова маса найменша.

ПНО відноситься до ОПН 1 класу, якщо сумарна маса небезпечних речовин хоча б однієї групи дорівнює пороговій масі небезпечних речовин 1 класу для цієї групи, визначені за формулою 5.2, або перевищує таку масу.

Якщо сумарні маси всіх індивідуальних небезпечних речовин, категорій або груп небезпечних речовин, менші за нормативи порогової маси небезпечних речовин 1 класу, але хоча б одна з них дорівнює нормативу порогової маси небезпечних речовин 2 класу згідно з таблицями 5.3 і 5.4 до нормативів чи нормативу, розрахованому за формулою 5.2, або перевищує їх, ПНО відноситься до ОПН 2 класу.

Якщо сумарні маси всіх індивідуальних небезпечних речовин, категорій або груп небезпечних речовин менші за нормативи порогової маси небезпечних речовин 2 класу згідно з таблицями 5.3 і 5.4, до нормативів або нормативи, розраховані за формулою 5.2, ПНО не відноситься до ОПН.

У разі коли найменша відстань від елементів ПНО до елементів селитебної території або промислових об’єктів не перевищує 500 метрів для небезпечних речовин 1 і 2 групи і 1000 метрів для небезпечних речовин 3 групи, пороговою масою вважається маса небезпечних речовин, визначена за формулою:

$$Q_{ir} = Q_i \times (R_x/R_n)^2 . \qquad (5.3)$$

де Q_{ir} – порогова маса небезпечних речовин;

Q_i – встановлений або розрахований за формулою 5.2 норматив порогової маси 2 класу;

R_x – відстань від ПНО до межі найближчого елемента селитебної території або промислового об’єкта;

R_n – гранична відстань від ПНО до найближчого промислового об’єкта або елемента селитебної території, починаючи з якої проводиться перерахунок нормативу порогової маси (для речовин 1 і 2 групи R_n дорівнює 500 метрів, для речовин 3 групи R_n дорівнює 1000 метрів).

У разі коли Q_{ir} менше 1 відсотка встановленого або розрахованого за формулою 5.2 нормативу порогової маси 2 класу, порогова маса приймається рівною 1 відсотку незалежно від відстані ПНО до елементів селитебної території.

Селитебна територія – ділянки житлових будинків , громадських установ, будівель та споруд, зокрема навчальних, проектних, науково-дослідних та інших інститутів без дослідних виробництв, внутрішньоселитебна, вулично-дорожня і транспортна мережа, площі, парки, сади, сквери, бульвари, інші

об’єкти зеленого будівництва і місця загального користування (ДБН 360 – 92, пункт 2.2).

Коли найменша відстань від елементів ПНО до елементів селитебної території або промислових об’ктів не досягає 500 метрів для небезпечних об’єктів 1 і 2 групи та 1000 метрів для речовин 3 групи і сумарна маса хоча б однієї з усіх видів небезпечних речовин або хоча б однієї категорії чи групи небезпечних речовин дорівнює пороговій масі небезпечних речовин 2 класу або перевищує таку масу, ПНО відноситься до ОПН 2 класу, а якщо менша – не відноситься до ОПН.

Суб’єкт господарювання складає повідомлення про результати ідентифікації ОПН за формою ОПН-1 і надсилає його у двотижневий термін відповідним територіальним органам Держгірпромнагляду, Державної інспекції техногенної безпеки, Мінприроди, державної санітарно-епідеміологічної служби, Держархбудінспекції, а також відповідній місцевій держадміністрації або виконавчому органу місцевої ради (далі – уповноважені органи).

Місцеві держадміністрації або виконавчі органи місцевих рад публікують відомості про ОПН за відповідною формою в друкованих регіональних засобах масової інформації протягом 30 днів після отримання повідомлення.

Суб’єкт господарювання , у власності або користуванні якого є ОПН, проводить у шестимісячний строк їх повторну ідентифікацію у разі:

- Зміни умов виробництва, номенклатури небезпечних речовин або їх кількості.
- Внесення змін до законодавства у сфері діяльності, пов’язаної з ОПН.
- Будівництва в прилеглих районах нових об’єктів, якщо це впливає на зміст відомостей, наведених у повідомленні про результати ідентифікаціїю.
- Зміни власника об’єкта.

Держгірпромнагляд та його територіальні органи ведуть Державний реєстр ОПН на підставі повідомлень про результати ідентифікації та копій свідоцтв про їх державну реєстрацію.

Суб’єктом господарювання до територіального органу Держгірпромнагляду повідомлення про результати ідентифікації. Протягом 10 робочих днів після реєстрації територіальний орган видає суб’єкту господарювання свідоцтво про державну реєстрацію ОПН. В свою чергу суб’єкт господарювання надсилає уповноваженим органам копію свідоцтва про державну реєстрацію ОПН.

Держгірпромнагляд публікує до 1 березня поточного року в загальнодержавних друкованих засобах масової інформації дані про ОПН, включені до Державного реєстру ОПН станом на 31 грудня попереднього року.

Виключення ОПН з реєстру здійснюється за рішенням територіального органу Держгірпромнагляду на підставі звернення та усіх необхідних документів, які подаються суб’єктом господарювання до територіальних органів Держгірпромнагляду, у разі:

- Проведення змін, що призвели до зменшення на ОПН сумарної маси небезпечних речовин порівняно з найменшим нормативом порогової маси відповідно до нормативів порогових мас або розрахованої за формулами 5.1, 5.3.
- Ліквідації або виведення з експлуатації (списання з балансу) ОПН.

5.4. Висновки до розділу

В даному розділі було визначено, що технологія IoT дозволяють зібрати інформацію для оцінки шкідливості і небезпечності умов праці персоналу в ході провадження виробничої діяльності суб’єктами господарювання. Завдяки доповненню IoT-інфраструктури технологією Blockchsin, можна збирати, записувати та передавати необхідну інформацію, для своєчасної реакції на виникнення небезпечної ситуації. Симбіоз цих технологій дозволяє записувати зібрану інформацію в своєрідну базу даних для статистики та виявлення причинно-наслідкового зв’язку при виникненні небезпечної ситуації.

РОЗДІЛ 6
ЕКОЛОГІЯ

6.1. Методи визначення якості та обсягу забруднення

Для визначення рівня забрудненості довкілля та відповідного впливу забруднювальних речовин на екологічні системи і здоров'я людини, а також для проведення екологічних експертиз в усьому світі застосовують спеціальні поняття: гранично допустимі концентрації (ГДК), гранично допустимі екологічні навантаження (ГДЕН), максимально допустимий рівень (МДР), санітарно-захисна зона (СЗЗ) та ін[20]. Встановлюють також летальну (смертельну) концентрацію (ЛКзд і ЛДад) шкідливих речовин, за яких спостерігається загибель половини піддослідних тварин. Ці дані потрібні для визначення класу загрозливої дії речовини. У різних країнах встановлюються неоднакові нормативні показники.

Гранично допустима концентрація (ГДК) забруднювальних речовин означає максимально можливий вміст їх у тому чи іншому середовищі, який практично не шкідливий для живих організмів, у тому числі й для людини. За допомогою цього показника контролюють якість повітря і водного середовища. Для кожної забруднювальної речовини встановлюються два нормативи: ГДКмр — максимальна разова і ГДКСд — середньодобова. Перший норматив дає змогу запобігти рефлекторним реакціям людини на короткочасний (протягом 20 хв) вплив забруднювальних речовин атмосфери (органами чуття, зору та ін.), а другий — загальнотоксичному, канцерогенному та іншим впливам (у середньому протягом 24 год). Окремо нормують вміст шкідливих домішок у повітрі населених пунктів та їх промислових зонах.

Нормативи якості води — це показники ЇЇ складу і властивостей, які визначають рівень Її придатності для конкретних видів водокористування (питного, господарсько-побутового, промислового, рибогосподарського та ін.). Зрозуміло, що вимоги до питної води, водойм рибогосподарського призначення

більш жорсткі. Якщо, наприклад, у воді гос-подарсько-побутового призначення допускається вміст нафтопродуктів 0,3 мг/л, то рибогосподарського — лише 0,05 мг/л. Це пояснюється тим, що нафта надає рибі різкого неприємного смаку і є токсичною для риб'ячої ікри і мальків. Як бачимо, стосовно якості води водних об'єктів встановлюються нормативи, які лімітують показник шкідливості забруднювальних речовин і відображують пріоритетність вимог до якості води. Так, для води господарсько-побутового призначення важливими г санітарно-токсикологічний, загальносанітарний та органолептичний л і м і 111, для рибного господарства — рибогосподарський.

Незалежно від нормативних вимог до якості води встановлюються певні обмеження на скидання у водні об'єкти стічних вод. Забороняється скидати стічні води[27]:

1) Які при застосуванні раціональних технологій можна використати у системах повторного водокористування.

2) Що містять цінні домішки, які підлягають утилізації.

3) Із вмістом виробничої сировини, реагентів, який перевищує ГДК.

4) Що містять шкідливі речовини, ГДК яких не встановлено.

Для грунту (переважно для його орного шару) визначено ГДК пестицидів і важких металів. З урахуванням їх розроблені і впроваджуються у виробництво регламенти застосування пестицидів і мінеральних добрив з метою запобігання накопиченню шкідливих речовин у сільськогосподарській продукції . Тому у практиці часто використовують такий показник, як допустима залишкова кількість (ДЗК) пестицидів у грунті і продукції.

Проте значення ГДК якоїсь однієї забруднювальної речовини ще не дає повного уявлення про ступінь її шкідливості, оскільки вона, як правило, діє в сукупності з іншими шкідливими речовинами. При вмісті в середовищі кількох забрудників враховують їх спільну дію, так званий ефект підсумовування негативного впливу. За правилом ефекту підсумовування концентрація кількох шкідливих речовин у середовищі не повинна перевищувати одиниці.

Для всіх забрудників атмосфери встановлено гранично допустимі викиди (ГДВ). Це науково-технічний норматив викиду в повітря допустимої кількості забруднювальних речовий за одиницю часу.

Критеріями оцінки якості довкілля в цілому є стандарти — екологічні та виробничо-господарські; До перших належать ГДК та ГДР, до других — ГДВ. Контроль якості навколишнього середовища здійснюють відповідні державні установи.

Під час визначення ГДК враховують не лише ступінь впливу забруднювачів на здоров'я людини, але й їх дію на диких та свійських тварин, рослин, гриби, мікроорганізми і природні угрупування в цілому.

Результати найновіших досліджень свідчать, що нижніх безпечних меж впливів канцерогенних речовин і іонізуючої радіації не існує. Будь-які дози, що перевищують звичайний природний фон, є шкідливими.

6.2. Дисперсійний аналіз в екології

Дисперсійний аналіз (англ. analysis of variance (ANOVA) являє собою статистичний метод аналізу результатів, які залежать від якісних ознак. Кожен фактор може бути дискретною чи неперервною випадковою змінною, яку розділяють на декілька сталих рівнів (градацій, інтервалів). Якщо кількість вимірювань (проб, даних) на всіх рівнях кожного з факторів однакова, то дисперсійний аналіз називають рівномірним, інакше – нерівномірним[28].

Основною метою дисперсійного аналізу, фундаментальна концепція якого була запропонована Фішером у 1920 р., є дослідження значущості відмінності між середніми декількох груп даних або змінних. Якщо порівнюються середні двох груп, дисперсійний аналіз дасть той же результат, що і звичайний ґ-критерій для незалежних або залежних вибірок. Проте використання дисперсійного аналізу має переваги особливо для малих вибірок.

Суть цього методу полягає в статистичному вивченні вірогідності впливу одного або кількох факторів, а також їх взаємодії на результативну ознаку.

Відповідно до цього за допомогою дисперсійного аналізу вирішуються три основних завдання:

1) Загальна оцінка істотності відмінностей між груповими середніми.

2) Оцінка вірогідності взаємодії факторів.

3) Оцінка істотності відмінностей між парами середніх.

Найчастіше такі завдання доводиться вирішувати дослідникам при проведенні польових і зоотехнічних дослідів, коли вивчається вплив кількох факторів на результативну ознаку одночасно.

У дисперсійному аналізі перевірка статистичної значущості відмінності між середніми декількох груп здійснюється на основі вибіркових дисперсій. Ця перевірка проводиться за допомогою розбиття загальної дисперсії (варіації) на частини, одна з яких обумовлена випадковою помилкою (тобто внутрішньогруповою мінливістю), а друга пов'язана з відмінністю середніх значень. Якщо ця відмінність значуща, нульова гіпотеза щодо існування відмінності між середніми значеннями відкидається на певному рівні значущості. Дисперсійний аналіз полягає у виділенні й оцінюванні окремих факторів, що викликають зміну досліджуваної випадкової величини. При цьому проводиться розклад сумарної вибіркової дисперсії на складові, обумовлені незалежними факторами. Кожна з цих складових є оцінкою дисперсії генеральної сукупності. Щоб дати оцінку дієвості впливу даного фактору, необхідно оцінити значимість відповідної вибіркової дисперсії у порівнянні з дисперсією відтворення, обумовленою випадковими факторами. Перевірка значимості оцінок дисперсії проводять з допомогою критерію Фішера.

Коли розрахункове значення критерію Фішера виявиться меншим табличного, то вплив досліджуваного фактору немає підстав вважати значимим. Коли ж розрахункове значення критерію Фішера виявиться більшим табличного, то цей фактор впливає на зміни середніх[28].

В залежності від числа джерел дисперсії розрізняють однофакторний та багатофакторний дисперсійний аналіз. Дисперсійний аналіз особливо ефективний при вивченні кількох факторів. При класичному методі вивчення

змінюють тільки один фактор, а решту залишають постійними. При цьому для кожного фактору проводиться своя серія спостережень, що не використовується при вивченні інших факторів. Крім того, при такому методі досліджень не вдається визначити взаємодію факторів при одночасній їх зміні. При дисперсійному аналізі кожне спостереження служить для одночасної оцінки всіх факторів та їх взаємодії.

Дисперсійний однофакторний аналіз використовується у дослідженнях зміни результативної ознаки під впливом зміни умов або градацій фактора. Суть математичних перетворень дисперсійного методу полягає в тому, щоб зіставити дисперсії за факторами із дисперсією усіх значень, отриманих в експерименті. Однофакторний аналіз вимагає не менше трьох градацій фактора і не менше двох випробовувань у кожній градації. При проведенні дисперсійного аналізу необхідно перевірити нормальність розподілу досліджуваної випадкової величини і відсутність відмінності дисперсій сукупностей. Це можна виконати методами перевірки статистичних гіпотез

Дисперсійний двофакторний аналіз застосовується в тих випадках, коли досліджується одночасна дія двох факторів на різні вибірки об'єктів, тобто коли різні вибірки опиняються під впливом різних поєднань двох факторів. Може статися, що одна змінна значущо діє на досліджувану ознаку тільки при певних значеннях іншої змінної. Наприклад, посилення мотивації може підвищувати швидкість рішення завдань у високоінтелектуальних осіб і знижувати її у низькоінтелектуальних. Отже, дисперсійний двофакторний аналіз дозволяє оцінити не лише вплив кожного з факторів, але й їхню взаємодію.

Суть методу залишається тією самою, як і при однофакторній моделі, але у двофакторному дисперсійному аналізі можна перевірити більшу кількість гіпотез, проте розрахунки дещо складніші, ніж в однофакторних комплексах.

Дисперсійний двофакторний аналіз пред'являє особливі вимоги до формування комплексів. Для кожного фактора має бути не менше двох градацій; у кожному осередку комплексу повинно бути не менше двох спостережуваних значень для виявлення взаємодії градацій; комплекс має бути

симетричною системою: кожній градації фактора А повинна відповідати однакова кількість градацій фактора В; результативна ознака повинна мати нормальний розподіл; фактори мають бути незалежними, що може бути підтверджено відсутністю кореляційного зв'язку між змінними-чинниками.

6.3.Висновки до розділу

В даному розділі було проаналізовано методи визначення якості і обсягу забруднення. Визначено основну мету та методи дисперсійного аналізу в екології.

ВИСНОВКИ

В першому розділі було розглянуто предметну область та проаналізовано спільне застосування технології Blockchain в IoT та можливості використання в різних сферах нашого життя. Визначено проблематику використання Blpckchain разом з IoT-пристроями, зокрема проблему безпеки. Проаналізовано галузі їх можливого застосування й проблеми.

В другому розділі було розроблено функціональну структуру та архітектуру IoT - інфраструктури з використанням ключових елементів, таких як LBM та OBM.

На основі ключових елементів LBM та OBM розроблено мережу накладення, яка потенційно може складатися з великої кількості вузлів.

Обґрунтовано використання алгоритму консенсусу на основі часу, замість більш ресурсомістких альтернатив, таких як PoW та PoS. Таким чином, завдяки алгоритму перевірки транзакцій кожен OBM перевіряє всі нові блоки, які отримує від пристроїв, та інших OBM.

В третьому розділі проаналізовано ключові оцінки різних аспектів діяльності LSB.

Проаналізовано програми для визначення ефективності низькоресурсних пристроїв та оцінено продуктивність накладення за допомогою них.

Проведено моделювання роботи таких мереж з метою оцінювання накладних витрат у LBM та споживання енергії.

Проаналізовано вплив розподілу потоків даних і транзакцій на мережу, та середній час обробки OBM для перевірки нових блоків.

При аналізі безпеки та конфіденційності було проаналізовано вимоги безпеки та основні можливі атаки на Blockchain та способи їх уникнення.

Здійснено тестування й визначено вплив кількості OBM на безпеку та пакетні накладні витрати, а також визначено відсоток транзакцій, який потрібно підтвердити для забезпечення максимальної стійкості до атак.

В четвертому розділі завдяки результату проведених розрахунків отриманий результат показує, що розробка матиме оптимальну економічну ефективність 0,56 і термін окупності становитиме майже два роки (1,79 року). Варто зазначити, що дані розрахунки носять номінальний характер і основна їх мета оцінити приблизну вартість дослідження та створення даного продукту. Номінальний характер розрахунків зумовлений тим, що даний програмний продукт має дослідницьке призначення.

В розділі охорони праці та безпеки в надзвичайних ситуаціях було визначено, що технологія IoT дозволяють зібрати інформацію для оцінки шкідливості і небезпечності умов праці персоналу в ході провадження виробничої діяльності суб'єктами господарювання. Завдяки доповненню IoT-інфраструктури технологією Blockchsin, можна збирати, записувати та передавати необхідну інформацію, для своєчасної реакції на виникнення небезпечної ситуації. Симбіоз цих технологій дозволяє записувати зібрану інформацію в своєрідну базу даних для статистики та виявлення причинно-наслідкового зв'язку при виникненні небезпечної ситуації.

В розділі екології було проаналізовано методи визначення якості і обсягу забруднення. Визначено основну мету та методи дисперсійного аналізу в екології.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A.Kosba, A.Miller, E.Shi, Z.Wen Hawk:The blockchain model of cryptography and privacy-preserving smart contracts, 2016. 868p.

2. Bitcoin: A peer-to-peer electronic cash system. 2008. URL:https://git.dhimmel.com/bitcoin-whitepaper/ (дата звернення: 05.10.2019).

3. Ethereum: a secure decentralised generalised transaction ledger. 2017. URL: https://git.dhimmel.com/bitcoin-whitepaper/ (дата звернення: 12.10.2019).

4. The Quest for Scalable Blockchain Fabric:. 2015. URL: https://allquantor.at/blockchainbib/pdf/vukolic2015quest.pdf (дата звернення: 14.10.2019).

1. A. Kousaridas, S. Falangitis, P. Magdalinos, N. Alonistioti, and M. Dillinger, Systas: Density-based algorithm for clusters discovery in wireless networks, 2015. 991p.

2. I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, Chord: A scalable peer-to-peer lookup service for internet applications, 2001. 658p.

3. Shortest Path First (OSPF). 1998. URL: https://www.ietf.org/rfc/rfc2328.txt (дата звернення: 7.10.2019).

4. K. Lu, Y. Qian, M. Guizani, and H.-H. Chen, A framework for a distributed key management scheme in heterogeneous wireless sensor networks, 2008. 647p.

5. D. Ongaro and J. K. Ousterhout, In search of an understandable consensus algorithm, 2014. 320p.

6. F.-S.sense. 2016. URL: www.sense.f-secure.com (дата звернення: 15.10.2019).

7. H. Delfs, H. Knebl, and H. Knebl, Introduction to cryptography, 2002. 138p.

8. D. Cooper, Internet x. 509 public key infrastructure certificate and certificate revocation list (crl) profile, 2008. 147p.

9. F. Tschorsch and B. Scheuermann, Bitcoin and beyond: A technical survey on decentralized digital currencies, 2015. 2123p.

10. Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN). 2012. URL: https://www.etsi.org/deliver/etsi_ts/187000_187099/187005/03.01.01_60/ts_187005v030101p.pdf (дата звернення: 19.10.2019).

11. Cooja. 2016. URL: https://anrg.usc.edu/contiki/index.php/Cooja_Simulator (дата звернення: 18.10.2019).

12. NS3. 2017. URL: https://www.nsnam.org (дата звернення: 18.10.2019).

13. A. Gervais, G. O. Karame, K. Wust, V. Glykantzis, H. Ritzdorf, and S. Capkun, On the security and performance of proof of work blockchains, 2016. 16p.

14. Disruptive Civil Technologies: Six Technologies With Potential Impacts on US Interests Out to 2025. 2008. URL: https://www.hsdl.org/?view&did=485606 (дата звернення: 25.10.2019).

15. Y.-W. Ma, C.-F. Lai, Y.-M. Huang, J.-L. Chen, Mobile RFID with IPv6 for phone services, 2009. 1245p.

16. P. Spiess, S. Karnouskos, D. Guinard, D. Savio, O. Baecker, L. Souza, V. Trifa, SOA-based integration of the internet of things in enterprise services. Los Angeles, 2009. 975p.

17. C. Buckl, S. Sommer, A. Scholz, A. Knoll, A. Kemper, J. Heuer, A. Schmitt, Services to the field: an approach for resource constrained sensor/actor networks, 2009. 481p.

18. S.-D. Lee, M.-K. Shin, H.-J. Kim, EPC vs. IPv6 mapping mechanism, 2007. 862p.

19. S. Duquennoy, G. Grimaud, J.-J. Vandewalle, The web of things: interconnecting devices with high usability and performance, 2009. 330p.

20. J. Liu, Y. Xiao, C. L. P. Chen, Authentication and access control in the internet of things, 2012. 592p.

21. Закон про об'єкти підвищеної небезпеки. Київ, 2014. URL: https://zakon.rada.gov.ua/laws/show/2245-14 (дата звернення: 8.11.2019).

22. Закон про ідентифікацію та декларування безпеки об'єктів підвищеної небезпеки. Київ, 2015. URL: https://zakon.rada.gov.ua/laws/show/956-2002-п (дата звернення: 8.11.2019).

23. Аністратенко В. О, Федоров В. Г, Математичне планування експериментів в АПК, 1993. 376р.

24. Ф.А. Барбинов, А.Ф. Козьяков, Охрана окружающей среды, 1991. 264р.

25. Санітарні норми мікроклімату виробничих приміщень ДСН 3.3.6.042-99. Київ, 1999. URL: https://zakon.rada.gov.ua/rada/show/en/va042282-99 (дата звернення: 12.11.2019).

26. Природне та штучне освітлення. 2018. URL: https://ledeffect.com.ua/images/__branding/dbn2018.pdf (дата звернення: 12.11.2019).

27. Про затвердження Правил охорони праці під час експлуатації електронно-обчислювальних машин. 2018. URL: https://zakon.rada.gov.ua/laws/show/z0293-10 (дата звернення: 12.11.2019).

28. Наказ міністерства внутрішніх справ України «Про затвердження правил пожежної безпеки в Україні». Київ, 2017. URL: https://zakon.rada.gov.ua/laws/show/z0252-15#n2 (дата звернення: 12.11.2019).

29. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин. 1998. URL: https://zakon.rada.gov.ua/rada/show/v0007282-98 (дата звернення: 12.11.2019).

Додаток А

Тези конференції

II Міжнародна студентська науково - технічна конференція
"ПРИРОДНИЧІ ТА ГУМАНІТАРНІ НАУКИ. АКТУАЛЬНІ ПИТАННЯ"

Міністерство освіти і науки України,
Тернопільський національний технічний університет
імені Івана Пулюя
Маріборський університет (Словенія)
Технічний університет в Кошице (Словаччина)
Каунаський технологічний університет (Литва)
Львівський національний університет імені
Івана Франка,
Гірничо-металургійна академія ім. Станіслава Сташиця
(Польща)
Луцький національний технічний університет,
Чернівецький національний університет
імені Юрія Федьковича,
Вроцлавський економічний університет (Польща)
Донбаська державна машинобудівна академія

Студентське наукове товариство

СНТ ТНТУ

II МІЖНАРОДНА

студентська науково - технічна конференція

"ПРИРОДНИЧІ ТА ГУМАНІТАРНІ НАУКИ.

АКТУАЛЬНІ ПИТАННЯ"

25-26 квітня 2019 р.

(збірник тез конференції)

Тернопіль 2019

УДК 004.338
Дармограй В. – ст. гр. СІм-52
Тернопільський національний технічний університет імені Івана Пулюя

ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ BLOCKCHAIN В IOT

Науковий керівник: к.т.н., доц. Луцків А.М.

Darmohrarai V.
Ternopil Ivan Puluj National Technical University

APPLICATION OF BLOCKCHAIN TECHNOLOGY IN IOT

Ключові слова: блокчейн, інтернет речей;
Keywords: blockchain, internet of things.

Фахівці все більше розглядають технологію блокчейн (Blockchain) у контексті непов'язаному з криптовалютами, а як засіб підвищення надійності, захищеності та достовірності транзакцій та даних в мережі Інтернет.

Блокчейн (або деяке сховище транзакцій) є ланцюжком блоків транзакцій, й, водночас, розподіленою базою даних, що зберігає впорядкований ланцюжок записів (або блоків), який постійно стає довшим. Дані у блоках захищені від модифікації. Кожен блок містить часову мітку (timestamp), хеш попереднього блока та дані транзакцій, які представлені у вигляді хеш-дерева. Блок транзакцій є спеціальною структурою для запису нових транзакцій в системі. Блок зберігає інформацію про час та транзакцію, дерево їхніх хешів, а також заголовок із службовими даними, де наведено хеш попереднього, чи попередніх блоків. У результаті, кожен наступний блок є також підтвердженням попереднього. Остаточне підтвердження відбудеться лише після декількох блоків в яких буде підтвердження попередніх. Кожний наступний блок зсилається на попередній, тобто вони є в одному ланцюжку — історії транзакцій за ввесь час існування системи. Перший блок ланцюжка («первинний блок»), є унікальним за рахунок відсутності так званого материнського блоку.

Блокчейн є технологією, яка може гарантувати стабільність та захищеність постійно зростаючої IoT-інфраструктури, забезпечуючи при цьому безпеку та аунтентичність інформації. Оскільки транзакції проходять зразу через декілька елементів мережі, то вони можуть відслідковувати та аналізувати правильність та достовірність. При виявлені збоїв чи несанкціонованого втручання в якісь частини ланцюга система блокчейн допоможе їх виявити та прийняти коректуючі дії. Використання шифрування та децентралізації дозволяє перевіряти достовірність даних всім учасникам, залученим до мережі, та уникнути відмови сервера чи системи. В блокчейн відсутній елемент централізованості управління або будь-який інший спосіб втручання в його роботу. На відміну від типової бази даних, розміщеної на централізованому сервері, що є власністю якоїсь особи (компанії або конкретної людини), блокчейн розосереджений серед великої кількості користувачів мережі. Й визначальною особливістю мережі блокчейн є та, що ніхто з цих користувачів не може її контролювати. Кожен елемент транзакції який проходить через конкретний елемент записується та перевіряється без контролю з боку людини. Завдяки децентралізованій технології блокчейн ніхто не зможе перезаписати записи в ланцюжку блоків, оскільки при перевірці на цілісність даних всі інші учасники мережі одразу зреагують на недостовірність та виправлять її. Використання блокчейн-технології дає можливість швидкого і безпечного збереження протоколів обміну і результатів спільної роботи різних пристроїв в децентралізованій системі. При зломі одного чи декількох учасників мережі та спробі їх одночасного втручання в систему, це жодним чином не позначається на роботі всієї системи. Блокчейн дозволяє створювати транзакції, які будуть прийматися після виконання певних визначених умов. Блокчейн

працює як P2P-мережа, яка дає змогу надійно передавати дані по всій мережі. Чим більше пристроїв тим більше запротокольований результат їх взаємодії. Усі дані взаємодії одного пристрою з іншим заноситься у особистий блокчейн.

Однією із перших сфер застосування блокчейну в IoT є забезпечення захищеності та автентичності даних у мережі, зокрема підвищення стійкості мереж IoT-пристроїв до DNS-атак та ураження пристроїв зловмисним кодом, який дає змогу зловмиснику сформувати бот-нет мережу з підключених пристроїв.

Іншою важливою сферою застосування блокчейну в IoT є забезпечення надійності роботи великих розподілених мереж IoT-пристроїв при виході з ладу певних їх ланок: оскільки, сама мережа містить всю потрібну інформацію про інші пристрої та комунікаційні канали між ними, то завжди ця інформація буде доступною завдяки самій мережі.

Для імплементації технології блокчейн в IoT будь-яке вирішення має забезпечувати наступні функції:

- комунікація типу точка-точка;
- розподілене поширення файлів;
- автономна координація роботи пристроїв, які підключені до мережі.

Вдалим прикладом стеку технологій IoT-речей та блокчейну є наступний:

- IoT-пристрої – фізичні рівень підключених пристроїв, які отримують та передають дані в блокчейн й роблять ці дані доступними більшості програм.
- Комунікаційні засоби – дають змогу передавати дані від IoT-пристроїв у блокчейн, а пристрої, у свою чергу, підтримують різні типи комунікаційних засобів.
- Платформа блокчейн – середовище створення й виконання розподілених програм, яка включає інфраструктуру (обчислювальні засоби, сховища, мережеві ресурси), протоколи(консенсус, права доступу та інші правила розмежування ресурсів) та сервіси(утиліти та модулі розподілених програм).
- Децентралізовані програми - програмне забезпечення з яким працює користувач через блокчейн-інфраструктуру й забезпечує використання наявних даних, отримання даних введених користувачем та смарт-контракти.

З кожним днем з'являються, і будуть з'являтися нові рішення в найнесподіваніших сферах. І, безумовно, блокчейн-технологія ще далека від свого піку розвитку, а в сфері IoT вона і зовсім знаходиться на початковому етапі. Проте, поєднання цих технологій, у міру їх практичної реалізації, вже незабаром кардинально змінить архітектуру більшості діючих сьогодні IT-екосистем.

Література

1. Літошенко А. В. ТЕХНОЛОГІЯ BLOCKCHAIN: ПЕРЕВАГИ ТА НЕОЧЕВИДНІ МОЖЛИВОСТІ ВИКОРИСТАННЯ У РІЗНИХ ГАЛУЗЯХ [Електронний ресурс] / А. В. Літошенко // ЕКОНОМІЧНА НАУКА. – 2017. – Режим доступу до ресурсу: http://www.economy.in.ua/pdf/8_2017/20.pdf.

2. Данильчук Р. К. АНАЛІЗ ОСНОВНИХ ПРИНЦИПІВ ТЕХНОЛОГІЇ BLOCKCHAIN [Електронний ресурс] / Р. К. Данильчук, О. С. Жураковська // ЖУРНАЛ НАУКОВИЙ ОГЛЯД. – 2017. – Режим доступу до ресурсу: http://oaji.net/articles/2017/797-1513962644.pdf.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Національна академія наук України
Університет імені П'єра і Марії Кюрі (Франція)
Маріборский університет (Словения)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Шяуляйська державна колегія (Литва)
Жешувський політехнічний університет ім. Лукасевича (Польща)
Білоруський національний технічний університет (Республіка Білорусь)
Міжнародний університет цивільної авіації (Марокко)
Національний університет біоресурсів і природокористування України (Україна)
Наукове товариство ім. Шевченка
ГО «Асоціація випускників Тернопільського національного технічного університету імені Івана Пулюя»

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник

тез доповідей

Том ІІ

VIII Міжнародної науково-технічної конференції молодих учених та студентів

27-28 листопада 2019 року

УКРАЇНА
ТЕРНОПІЛЬ – 2019

УДК 004.338

В.О. Дармограй А. М. Луцків канд. техн. наук, доц.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

АНАЛІЗ БІБЛІОТЕК ДЛЯ РЕАЛІЗАЦІЇ BLOCKCHAIN-ІНФРАСТРУКТУРИ ДЛЯ СИСТЕМ IOT

V. O. Darmohrai, A. M. Lutskiv Ph.D., Assoc. Prof.

APPLICATION OF BLOCKCHAIN TECHNOLOGY IN IOT SYSTEMS

Інтернет речей (IoT) — це сфера, яка доволі швидко розвивається й є у нашому повсякденному житті. Є ціла низка безкоштовних та відкритих програмних засобів для побудови інфраструктур IoT мереж, зокрема Eclipse IOT. Для забезпечення кросплатформової взаємодії, як правило, використовується технологія Java, яка використовується й у Eclipse IOT проектах. Доволі актуальною технологією для забезпечення конфіденційності, ідентифікації користувачів та пристроїв, є Blockchain. Blockchain знайшла використання у різних сферах діяльності людини. Найвідомішими її застосуваннями є інфраструктури криптовалют, водночас, є багато спроб застосувань у наступних сферах: платежі та перекази коштів, розумні контракти “smart contracts”, нотаріальні послуги, розподілені хмарні сховища, засоби цифрової ідентифікації, децентралізовані комп’ютерні мережі, а також системи підтримки та забезпечення інтернету речей. Розглянемо спеціалізовані бібліотеки Java для реалізації Blochain-інфраструктури.

Bitcoinj - це бібліотека для роботи з протоколом Bitcoin. Він може підтримувати гаманець, відправляти/отримувати транзакції без необхідності локальної копії Bitcoin Core та має багато інших розширених функцій. Він реалізований на Java, але може використовуватися з будь-якої мови, сумісної з JVM, зокрема Python та JavaScript. На ньому побудовано багато великих, добре відомих додатків і служб Bitcoin. Особливостями bitcoinj є:

- високооптимізований легкий режим спрощеної перевірки платежів (SPV). У цьому режимі завантажується лише невелика частина ланцюга блоків, що робить bitcoinj придатним для використання на обмежених пристроях, таких як смартфони або дешеві віртуальні приватні сервери;
- повний режим перевірки, який виконує ту ж перевірку, що і Bitcoin Core. У цьому режимі обчислюється невикористаний набір вихідних транзакцій (набір UTXO) і, завдяки базі даних PostgreSQL, може бути збережений у базу даних, що забезпечує швидкий пошук за адресою;
- підтримка каналів мікроплатежів, які дозволяють встановити контракт з багатьма підписами між клієнтом і сервером, а потім вести переговори по каналу, дозволяючи швидкі мікроплатежі, що дозволяють уникати оплати майнерам;
- забезпечує як асинхронну передачу даних, так і синхронний потік з'єднання для мережевого вводу-виводу, що дозволяє вибирати між масштабованими не блокуючими та блокуючими функціями, такими як наближення SOCKS.
- клас гаманця з шифруванням, розрахунком гонорару, багатопідписанням, детермінованим виведенням ключів, підключенням вибору монети/контролем монет, підтримкою розширень для повідомлення про події.
- інструменти командного рядка для роботи з файлами гаманця та ланцюжка, протоколом платежів, мережею тощо.

Web3j - друга найбільш розвинута бібліотека, криптовалюта, заснована на цій передовій технології. бібліотека дозволяє працювати з блокчейном Ethereum, без

додаткових накладних витрат, необхідності писати власний інтеграційний код для платформи. Особливостями web3j є:

- підтримка особистих API-програм Parity та персональних клієнтів Geth
- повна реалізація клієнтського API JSON-RPC Ethereum через HTTP та IPC
- автогенерування обгортки смарт-контрактів Java для створення, розгортання, взаємодії з смарт-контрактами та виклику смарт-контрактів із власного коду Java (підтримуються формати Solidity та Truffle)
- додаткове управління через API JSON-RPC за допомогою Geth і Parity

Fabric Hyperledger - це платформа з відкритим кодом та дозволеною корпоративною технологією розподіленої книги (DLT), розроблена для використання в корпоративних контекстах, яка забезпечує ключові можливості для розмежування порівняно з іншими популярними платформами для ведення журналів або блокчейнів. Hyperledger має високомодульну та настроювану архітектуру, універсальності та оптимізації для широкого кола галузевих випадків використання, включаючи банківські справи, фінанси, страхування, охорону здоров'я, людські ресурси, ланцюжок поставок і навіть доставку цифрової музики. Hyperledger є першою платформою розподіленої книги для підтримки розумних контрактів, створених на мовах програмування загального призначення, таких як Java, Go і Node.js.

Fabric Hyperledger може використовувати протоколи консенсусу, які не потребують конкретної криптовалюти для того, щоб заробити видобуток та використати розумне виконання контрактів. Уникнення криптовалюти зменшує деякі значні вектори ризику/атаки, а відсутність операцій з видобутку криптовалют означає, що платформа може бути розгорнута приблизно з тими ж операційними витратами, що і будь-яка інша розподілена система. Поєднання цих відмінних особливостей робить hyperledger однією з найефективніших платформ, доступних сьогодні як з точки зору проведення транзакцій, а також забезпечує конфіденційність транзакцій та розумних контрактів.

Платформа Fabric є відкритою, це означає, що, на відміну від загальнодоступної закритої мережі, учасники відомі один одному, а не анонімні. Хоча учасники можуть не повністю довіряти один одному, мережа може функціонувати за моделлю управління, яка будується на основі того, що існує довіра між учасниками, наприклад юридична угода або рамки для вирішення спорів. Fabric Hyperledger була спеціально розроблена, щоб мати модульну архітектуру. Незалежно від консенсусу підключення, протоколів управління підключеними ідентифікаторами, таких як LDAP або OpenID Connect, протоколів управління ключами або криптографічних бібліотек, платформа розроблена таким чином, щоб відповідати різноманітним вимогам використання підприємств.

Література

1. A Blockchain Platform for the Enterprise [Електронний ресурс] – Режим доступу до ресурсу: https://hyperledger-fabric.readthedocs.io.

2. bitcoinj [Електронний ресурс] – Режим доступу до ресурсу: https://bitcoinj.github.io.

3. web3j [Електронний ресурс] – Режим доступу до ресурсу: docs.web3j.io.