НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ФАХОВИЙ КОЛЕДЖ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломної роботи
фахового молодшого бакалавра

на тему: **Перспективи впровадження технології Blockchain у сучасні телекомунікаційні системи**

Виконав студент IV курсу, групи ТК-41
спеціальності 172 Телекомунікації та радіотехніка
ОПП «Телекомунікації та комп'ютерні технології»
Проць Максим Андрійович

Керівник _____ Олександра ЗАГОРЯНСЬКА
(підпис)

Нормоконтролер _____ Володимир ПЛІШ
(підпис)

Рецензент _____ Олег ЛЕЩАК
(підпис)

Голова ЕК _____ Андрій ВАХ
(підпис)

Члени ЕК _____ Ігор ТИБЕЛЬ
(підпис)

_____ Володимир ПЛІШ
(підпис)

Дипломна робота захищена в ЕК «__» _____ 2025 р.

з оцінкою «_____»

Львів 2025

ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ФАХОВИЙ КОЛЕДЖ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

Циклова комісія ***Телекомунікації***
Освітньо-професійний ступінь ***Фаховий молодший бакалавр***
Освітньо-професійна програма ***Телекомунікації та комп'ютерні технології***
Спеціальність ***172 Телекомунікації та радіотехніка***

ЗАТВЕРДЖУЮ
Завідувач відділення
«Телекомунікацій та
комп'ютерних технологій»
_____ Ігор ТИБЕЛЬ
« 25 » квітня 2025 року

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ ЗДОБУВАЧУ

Процю Максиму Андрійовичу
(прізвище, ім'я та по батькові)

1.Тема роботи *Перспективи впровадження технології Blockchain у сучасні телекомунікаційні системи*

Керівник роботи *Олександра ЗАГОРЯНСЬКА*
викладач вищої категорії,
(ім'я, прізвище, науковий ступінь, вчене звання)

затверджені наказом директора від " 20 " березня 2025 року № 20-СТ

2. Строк подання студентом роботи "10" червня 2025 року

3. Вихідні дані до роботи *3.1 Пронанлізувати ключові компоненти технології Blockchain*

3.2 Використати технологію P2P в контексті Blockchain мережі;

3.3 Використати ключові аспекти технології Blockchain;

3.4 Застосувати технологію Blockchain у телекомунікаційних системах.

4. Зміст розрахунково-пояснювальної записки

4.1 Сутність технології Blockchain та її еволюція

4.2 Основні принципи та функції технології Blockchain

4.3 Потенціал використання технології Blockchain у телекомунікаційних системах

4.4 Техніко-економічне обгрунтування.

4.5 Охорона праці та безпека життедіяльності

5. Перелік графічного матеріалу

5.1.	*Принцип передачі даних у системах з асиметричним шифруванням*
5.2.	*Візуальне зображення роботи смарт-контракту*
5.3.	*Основні відмінності між серверною та P2P мережами*
5.4.	*Структура мереж Blockchain*
5.5	*Принципи функціонування Blockchain мережі*

6. Консультанти розділів дипломної роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	Завдання отримав
Техніко-економічне обґрунтовування	*Мар'яна СМУК викладач вищої категорії*	*25.04.2025р.*	*25.04.2025р*
Охорона праці та безпека життєдіяльності	*Олена МЕЛЬНИКОВА викладач першої категорії*	*25.04.2025р.*	*25.04.2025р.*

7. Дата видачі завдання « 25» квітня 2025 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання	Примітка
1	*Вступ.*	*25.04-01.05*	
2	*Сутність технології Blockchain та її еволюція*	*02.05-08.05*	
3	*Основні принципи та функції технології Blockchain*	*09.05-15.05*	
4	*Потенціал використання технології Blockchain у телекомунікаційних системах*	*16.05-22.05*	
5	*Техніко – економічне обґрунтування*	*23.05-29.05*	
6	*Охорона праці та безпека життєдіяльності*	*30.05-03.06*	
7	*Висновки*	*04.06-05.06*	
8	*Підготовка графічного матеріалу.*	*06.06-09.06*	

Здобувач _____ *Максим ПРОЦЬ*
(підпис) (ім'я, прізвище)

Керівник роботи _____ *Олександра ЗАГОРЯНСЬКА*
(підпис) (ім'я, прізвище)

РЕФЕРАТ

Текстова частина дипломної роботи: 68 с., 20 рис., 1табл., 8 джерел.

Об’єкт дослідження – технологія Blockchain

Мета роботи – є оцінити потенціал технології blockchain для вдосконалення комунікаційних процесів у телекомунікаційних системах

Метод дослідження – є аналіз літературних джерел, новітніх публікацій за темою дослідження.

Перш за все, робота розглядає принципи та принципи роботи технології блокчейн, а також її історичний контекст. Досліджується, як технологія блокчейн може бути застосована в телекомунікаційній галузі для підвищення ефективності, забезпечення безпеки та надійності мережі.

У роботі аналізуються переваги використання технології блокчейн в телекомунікаційних системах, такі як децентралізація, прозорість, незмінюваність даних та підвищена безпека. Досліджуються можливості використання технології блокчейн у різних аспектах телекомунікаційного бізнесу, включаючи автентифікацію користувачів, управління даними та рахунками, вирішення проблем роумінгу та інші.

BLOCKCHAIN, ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, СМАРТ-КОНТРАКТ, ШИФРУВАННЯ, ДЕЦЕНТРАЛІЗАЦІЯ, БАЗА ДАНИХ, КРИПТОСИСТЕМА.

ЗМІСТ

ВСТУП

З кожним роком мобільні телефони стають все більш продуктивними та функціональними. За останні кілька років ми спостерігаємо зростання обсягів оперативної пам'яті, покращення камер, а також збільшення ємності батареї. Однак ці інновації потребують додаткового простору в смартфонах. Одним із рішень для вирішення цієї проблеми є впровадження технології eSIM, яка вже існує в новітніх смартфонах та доступна українським абонентам завдяки мобільним операторам Lifecell та ТриМоб. Ця інновація передбачає використання чіпа, вбудованого безпосередньо в смартфон, замість традиційної пластикової USIM-карти. Користувачам достатньо лише сканувати QR-код для активації, щоб користуватися не лише одним, але й навіть декількома телефонними номерами на одному пристрої. Проте, така інновація потребує надійного захисту, щоб гарантувати конфіденційність особистих даних і доступу до додатків. У цьому контексті технологія Blockchain може стати ефективним рішенням для забезпечення безпеки та конфіденційності.

Blockchain – це технологія розподіленої бази даних, що складається з послідовно впорядкованих блоків. Кожен блок містить часову мітку та посилання на попередній блок, що забезпечує недоступність підробки. Однак, відмінною рисою є те, що доступ до конкретних транзакцій може мати лише особа з відповідним приватним ключем.

Сучасна технологія Blockchain має великий потенціал і швидко розвивається, відкриваючи нові можливості для різних галузей, зокрема для телекомунікацій. Телекомунікаційна галузь є складною екосистемою, що потребує співпраці між внутрішніми та зовнішніми операторами для успішної реалізації проєктів. Застосування технології Blockchain вже використовується для усунення посередників між операторами, запобігання шахрайству в роумінгу та покращення ефективності мобільності телефонних номерів.

1 СУТНІСТЬ ТЕХНОЛОГІЇ BLOCKCHAIN ТА ЇЇ ЕВОЛЮЦІЯ

1.1 Еволюція та історія розвитку технології blockchain

Технологія blockchain є основою для багатьох криптовалют, таких як Bitcoin, Litecoin, Ethereum та інші. Ця інноваційна технологія дозволяє передавати цифрові дані без можливості їхнього подвоєння чи зміни. Кожен фрагмент інформації в Blockchain є унікальним блоком, який зберігає дані про конкретну транзакцію, включаючи час, дату, суму та інші параметри. Зазвичай ці блоки можуть містити різноманітні дані, такі як документи, зображення, посвідчення особи та інше. Кожен користувач отримує унікальний цифровий ключ для ідентифікації, а блоки містять інформацію про імена користувачів. Кожен блок також містить унікальний код, що допомагає розрізнити його від інших блоків, що подібно до унікального номера студентського квитка.

Хоча технологія blockchain здобула широку популярність протягом останніх десяти років, її історія сягає глибоко в минуле. Вже у 1991 році була опублікована перша наукова робота про криптографічний захист ланцюгів блоків, авторами якої були С. Хабер та У. Скотт. Метою цієї роботи було знайти рішення для неможливості спотворення чи пошкодження часових позначок. У 1992 році Хабер разом з колегами використав свої наукові дослідження для значного покращення ефективності технології. Вони розробили хеш-дерево, що є системою для контролю даних між комп'ютерами, забезпечуючи унікальність та достовірність блоків та даних при обміні між вузлами P2P мережі.

Історія розвитку технології blockchain налічує багато важливих моментів. У 2008 році під псевдонімом Сатосі Накамото була опублікована ідея використання blockchain як основи для криптовалюти Bitcoin, що революціонізувала світ цифрових платежів. Після цього було запропоновано кілька інших blockchain-платформ, що сприяло зростанню інтересу до цієї технології. В 2010 році відбулась перша онлайн-купівля Bitcoin, а в 2018 році вартість цієї криптовалюти стрімко зросла, що свідчить про її значний потенціал. Однак період між 2012 і

2014 роками був найбільш значущим у розвитку blockchain. Розробники, у тому числі Віталік Бутерін, розуміли потенціал цієї технології і додавали нові можливості до бази блокчейну. Бутерін спроектував Ethereum - універсальну децентралізовану платформу, яка може використовуватися в різних галузях та підтримує peer-to-peer зв'язок. Ці інновації відкрили широкі перспективи для застосування blockchain в різних сферах та підкреслили його значення як ключового елементу технологічного прогресу. [1]

У 2015 році відбулися два значущі події в історії розвитку blockchain технології. По-перше, Linux Foundation, одна з провідних комерційних організацій з відкритим кодом, розпочала розробку Hyperledger - платформи, спрямованої на полегшення створення блокчейн-проектів. Цей крок відкривав нові можливості для розробників та підтримував поширення блокчейн-технології у різних секторах. Паралельно з цим, Ethereum офіційно представив нову функцію, відому як "смарт-контракти". Ці "розумні" контракти дозволяли обмінювати різні цінності без посередників, відкриваючи шлях до більш ефективних та прозорих угод для всіх учасників.

Історія та розвиток блокчейну розширюється далеко за межі Ethereum і Bitcoin. Останніми роками було створено безліч нових криптовалют, які отримали визнання й почали використовуватися в передових країнах для оплати податків та інших послуг. З розвитком Інтернету речей стала актуальною оптимізація платформи криптовалют для забезпечення нульової комісії за транзакції. Зараз великі корпорації, такі як Microsoft, активно інвестують у розвиток технології блокчейн, що призвело до створення приватних, гібридних і федеративних блокчейнів. Крім того, компанії, такі як IBM та Samsung, спільно працюють над проектом Adept, який має на меті створення децентралізованої мережі з великою кількістю різноманітних пристроїв Інтернету речей (IoT), які можуть взаємодіяти між собою. Ця технологія відкриває широкі перспективи, які були визнані на Всесвітньому економічному форумі, де блокчейн був названий одним з перспективних напрямків для інвестицій.

1.2 Ключові компоненти технології blockchain

Основна ідея технології blockchain полягає в структуруванні та обміні даними в системі. Вона представляє собою новий підхід до створення розподілених баз даних, які контролюються групою людей з метою спільного збереження та взаємодії. У цій технології дані організовані у вигляді послідовних блоків, що утворюють неперервний ланцюг.

Кожен блок є файлом, який записується в мережі без можливості майбутньої зміни. Він містить інформацію про проведені транзакції до моменту свого створення та всі останні транзакції, які не включалися в попередні блоки. При створенні нового блоку він автоматично додається до кінця ланцюга блокчейну.

Транзакція або операція в контексті blockchain – це передача даних від одного вузла до іншого. Це подібно до фінансових транзакцій, де кошти переказуються від одного клієнта до іншого. В мережі blockchain ви виконуєте аналогічні дії, передаючи дані один одному.

В основі технології blockchain лежать різні інноваційні методи і технології для обробки та захисту даних, включаючи:

– Системи асиметричного шифрування, що також відомі як асиметричні криптосистеми, які забезпечують безпеку даних за допомогою публічних та приватних ключів.

– Смарт-контракти, що є віртуальними протоколами, написаними мовою програмування, і використовуються для автоматизації обміну товарами та укладення договорів.

– Хеш-функції, такі як функції MD та SHA, що використовуються для шифрування даних та забезпечення їх цілісності.

– Хеш-таблиці, що є структурою даних у вигляді асоціативного масиву для зберігання пар ключ-значення та виконання операцій додавання, видалення та пошуку даних.

– Процес майнінгу, який дозволяє криптовалютам працювати в якості децентралізованої мережі без посередників.

– Алгоритми консенсусу та механізми Proof of Concept (PoC), що демонструють практичну працездатність методу, ідеї або технології.

Асиметричні алгоритми шифрування в криптографії використовують два ключі: публічний і приватний. Публічний ключ використовується для зашифрування даних і доступний для всіх, тоді як приватний ключ використовується для розшифрування та є конфіденційним. Ці ключі взаємодіють унікальним чином, забезпечуючи безпеку та конфіденційність передачі даних.

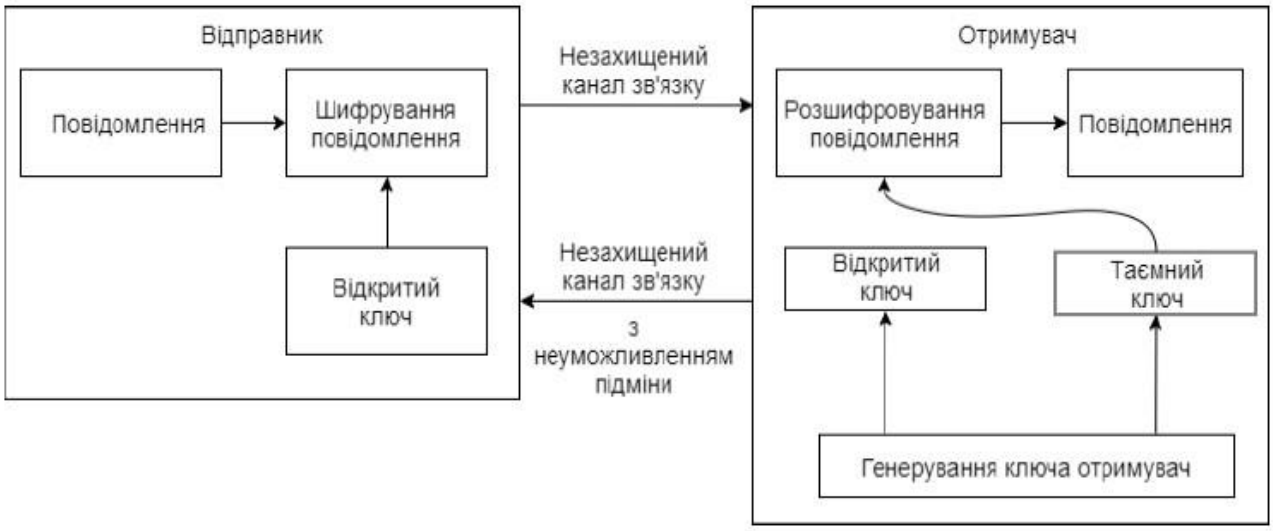

Рисунок 1.1 – Принцип передачі даних у системах з асиметричним шифруванням

Хеш-функція, відома також як функція згортки, виконує перетворення вхідних даних будь-якої довжини у вихідний рядок фіксованої довжини за допомогою певного алгоритму. Цей процес надає унікальний код, відомий як хеш-код, який ідентифікує вхідні дані. У контексті технології blockchain, криптографічні хеш-функції використовуються для забезпечення безпеки та недоступності початкових даних, що піддаються хешуванню. Хоча може здатися, що неможливо отримати початкові дані з хеш-коду, функції згортки гарантують однаковий хеш для одних і тих самих даних. Важливо, щоб хеш-функції мали

мінімальну ймовірність колізій, тобто ситуацій, коли різні вхідні дані в результаті дають один і той же хеш-код.

Існує різноманіття криптографічних хеш-функцій, кожна з яких має свої особливості та застосування. Однією з найпоширеніших є MD5, що генерує 128-бітний унікальний криптографічний рядок для будь-яких вхідних даних. Цей алгоритм часто використовується для цифрових підписів, які вимагають стиснення та шифрування об'ємних даних для забезпечення їх безпеки.

Ще одним популярним алгоритмом є SHA-256, який генерує хеш довжиною 256 бітів. Цей алгоритм важко піддати злому через велику кількість можливих комбінацій. Він опрацьовує дані блоками по 512 бітів і видає 256-бітний хеш-код, що забезпечує високий рівень безпеки для переданих даних.

Хеш-таблиці – це структури даних, призначені для зберігання пар ключ-значення, де розташування елементів залежить від значень ключів. У таких таблицях реалізовано три основні операції: додавання нової пари ключ-значення, пошук за ключем і видалення за ключем.

Існують два основних типи хеш-таблиць:

– Хеш-таблиці з лінійним розташуванням (метод ланцюжків) – в цих таблицях пошук вільної комірки виконується до тих пір, поки не буде знайдена вільна комірка. Якщо комірка вже зайнята, відбувається перехід до наступної комірки, і цей процес повторюється до тих пір, поки не буде знайдена вільна комірка для вставки даних.

– Хеш-таблиці з відкритою адресацією – ці таблиці використовують неперервний масив як сховище даних. Якщо вставка вказує на вже зайняту комірку, використовується спеціальний метод для пошуку нового місця для зберігання даних, часто за допомогою хеш-функцій та розроблених алгоритмів розподілення.

Однією з основних проблем хеш-таблиць є можливість колізій, які виникають при вставці ключів в ті самі комірки таблиці. Колізія виникає, коли два або більше ключі вказують на одну і ту саму комірку. У такому випадку, використовуючи метод ланцюжків, ми створюємо зв'язаний список елементів, які

зберігаються в цій комірці. При пошуку ключа ми пройдемо по цьому списку, порівнюючи ключі між собою, поки не знайдемо потрібний.

Недоліком такої хеш-таблиці є те, що при додаванні багато елементів, які вказують на одну комірку, утворюється довгий зв'язаний список, що збільшує середній час пошуку елементів у таблиці. Для вирішення цієї проблеми використовується метод подвійного хешування. Головна ідея полягає в тому, що для визначення кроку зміщення при колізії використовується інша хеш-функція, яка встановлює зміщення більш ефективно, що дозволяє знаходити вільні місця швидше.

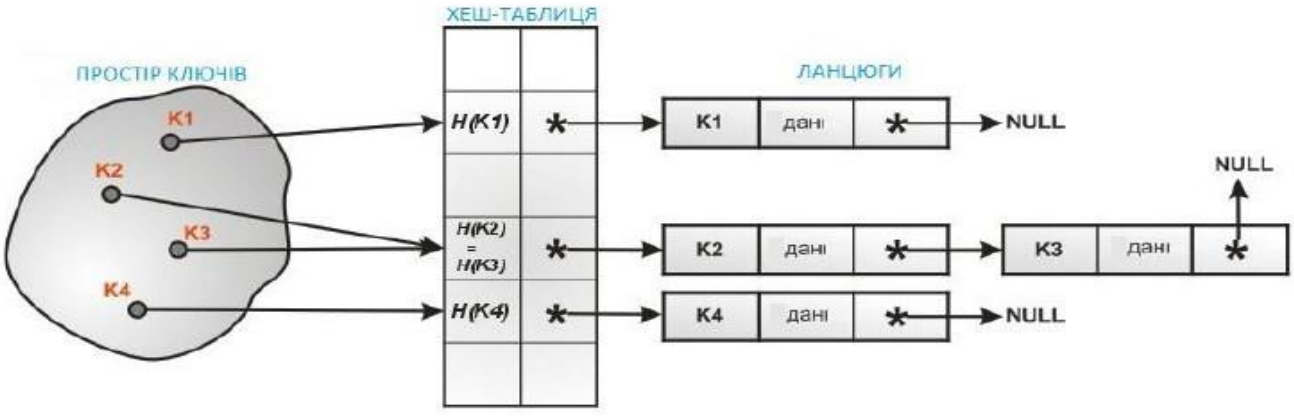

Рисунок 1.2 – Методи рішення колізій у хеш-таблицях

В методі з відкритою адресацією (замкнуте хешування) всі елементи зберігаються безпосередньо в хеш-таблиці без використання пов’язаних списків. Відмінною особливістю цього методу порівняно з методом лінійного розміщення є те, що таблиця може стати повністю заповненою, що ускладнює додавання нових елементів. Розв’язанням цієї проблеми є динамічне збільшення розміру хеш-таблиці з одночасною зміною її структури. Однак, видалення елементів є складнішим завданням у порівнянні з методом лінійного розміщення. Після видалення даних з хеш-таблиці ми робимо неможливим пошук ключа, який може займати ту саму комірку. Це вимагає впровадження спеціальних механізмів для ефективного використання вільного місця.

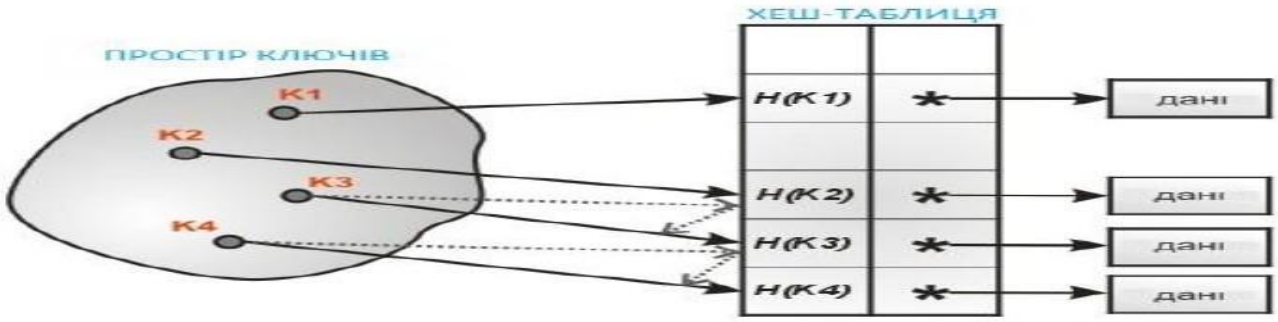

Рисунок 1.3 – Механізм вирішення колізій в хеш-таблиці з відкритою адресацією

Смарт-контракти (розумні контракти) – це програми, що автоматизують виконання угод між сторонами без необхідності посередника. Вони дозволяють встановлювати умови та виконувати операції автоматично при виконанні цих умов, наприклад, при отриманні певної суми коштів або визначеній даті.

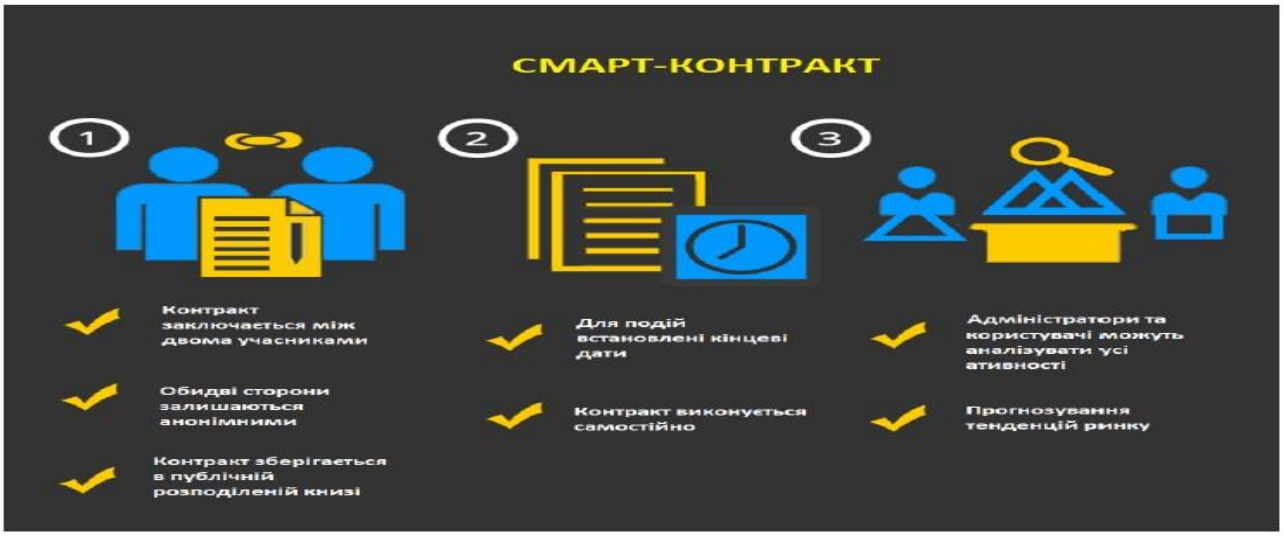

Рисунок 1.4 – Візуальне зображення роботи смарт-контракту

Припустимо, що громадянин А бажає придбати квартиру у громадянина Б. Використовуючи технологію блокчейн та криптовалюту, громадянин А може легко перерахувати кошти. Після цього він отримає віртуальний документ, який буде включений у смарт-контракт. Коли громадянин Б передасть ключі протягом певного терміну, система автоматично здійснить оплату громадянинові Б. У разі невиконання умов з обох сторін, наприклад, якщо ключі не будуть передані,

система поверне кошти громадянину А. Таким чином, система гарантує виконання умов угоди та забезпечує безпеку обох сторін.

Переваги смарт-контрактів:

– Гарантований захист від зовнішніх втручань. Ваш договір залишається безпечним і недоступним для будь-яких третіх осіб. Ви самостійно контролюєте умови угоди, не потребуючи підтвердження від нотаріуса чи інших посередників.

– Високий рівень безпеки. Смарт-контракти застосовують надійні методи кодування, які майже неможливо взламати, що гарантує захист ваших даних від хакерських атак.

– Уникнення помилок. Автоматизовані смарт-контракти усувають ризик людських помилок під час укладання угоди, запобігаючи можливим недорозумінням і помилкам у документах.

– Економія витрат. Вам не доведеться платити комісію третім сторонам або посередникам за проведення угоди, що дозволяє ефективно економити ваші кошти.

– Швидкість та ефективність. Обробка усіх документів здійснюється автоматично і швидко, що значно прискорює процес укладання угоди порівняно з традиційними методами.

Звичайний смарт-контракт має три ключові складові. По-перше, цифрові підписи усіх учасників угоди, які забезпечують їхню автентичність і зобов'язання. По-друге, визначення об'єкту угоди, який може бути будь-яким активом або послугою. По-третє, математично сформульовані умови угоди, які програмуються для автоматичного виконання [3].

Всі дані, використовувані в контракті, повинні бути отримані з надійних джерел. Для забезпечення цієї достовірності застосовуються різні програмні засоби і протоколи безпеки, такі як HTTPS і сертифікати SSL.

Головною фігурою у процесі майнінгу є майнер, що виступає як вузол мережі. Його завданням є збір транзакцій для їх подальшого включення у блок. Після отримання транзакцій вузли починають їх перевірку і додають у

відповідний "пул" пам'яті. Потім майнери об'єднують кілька таких транзакцій у новий блок, додаючи до нього також транзакцію з нагородою за їхню працю.

Перед початком майнінгу майнери додають спеціальну транзакцію, яка містить нагороду за їхню роботу. Після хешування всіх функцій дані об'єднуються у хеш-дерево, де вони сполучаються в пари, поки не буде досягнута "вершина дерева". Ідентифікатор кожного блоку формується шляхом додавання поточного хешу до хешу попереднього блоку та певного випадкового числа, згенерованого за певним протоколом.

У деяких випадках може виникати ситуація, коли два вузли додають підтверджений блок одночасно, що призводить до конфлікту. В таких випадках конкуренція продовжується, поки не буде створений блок на основі одного з двох попередніх блоків [4].

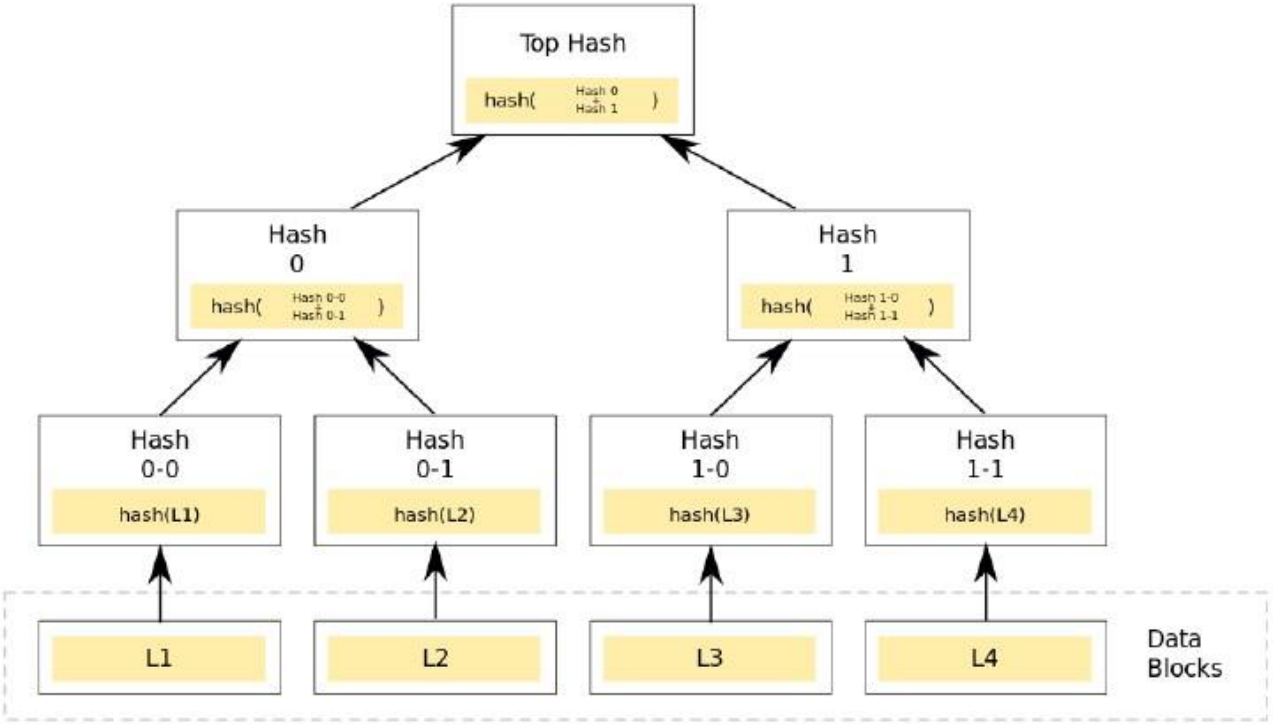

Рисунок 1.5 – Приклад структури дерева Меркла

Алгоритм консенсусу – це ключовий елемент у технології blockchain, що забезпечує згоду всіх учасників мережі та забезпечує безпеку та цілісність даних у розподіленій системі. У зв'язку з децентралізацією блокчейну, де відсутні

централізовані органи прийняття рішень, алгоритм консенсусу відіграє важливу роль у прийнятті рішень мережею самостійно. Він забезпечує виконання протоколу та гарантує достовірність всіх транзакцій. Відмінність між протоколом та алгоритмом полягає в тому, що протокол визначає правила та дії, які має дотримуватись система для досягнення певної мети, тоді як алгоритм забезпечує виконання цих правил. Існують різні алгоритми консенсусу, серед яких найбільш популярні PoS (Proof of Stake) та PoW (Proof of Work).

Proof of Work (PoW) – це перший алгоритм консенсусу, що використовується у технології Bitcoin та багатьох інших криптовалют. В основі PoW лежить ідея вирішення складної обчислювальної задачі, щоб довести свою працездатність. Майнери змагаються між собою за право створити новий блок транзакцій, розв'язуючи цю задачу. Тільки блоки, що успішно вирішують задачу, приймаються і додаються до блокчейну. Цей метод дозволяє гарантувати безпеку мережі і запобігає подвійному витрачанню. Ethereum також використовує PoW, хоча планує перейти на інший алгоритм, Proof of Stake (PoS), у майбутньому.

Proof of Stake (PoS) – це алгоритм консенсусу, що з'явився як альтернатива PoW. Основна його особливість полягає в тому, що блоки перевіряються відповідно до частки криптовалюти, утримуваної учасником мережі. Іншими словами, право на генерацію нових блоків та підтвердження транзакцій надається учасникам в залежності від їхнього володіння та участі в мережі, а не від обчислювальної потужності, як у PoW.

Рисунок 1.6 – Приклад як досягається згода в мережі блокчейн

Однією з ключових переваг технології блокчейн є його безпека та відсутність необхідності у додаткових оплатах чи комісіях для третіх сторін. Коли одна сторона ініціює передачу даних, що є абсолютно безпечною, створюється новий блок. Цей блок перевіряється великою кількістю комп'ютерів, що розподілені в мережі. Після успішної перевірки блок додається до ланцюга, створюючи унікальний запис з унікальним ідентифікатором. Підробка такого запису стає практично неможливою, оскільки вимагає модифікації всього ланцюга в мільйонах записів.

Припустимо, ви оплачуєте комунальні послуги через Інтернет, використовуючи ваш комп’ютер або мобільний телефон. Зазвичай банківські компанії стягують додаткові витрати за оплату цих послуг. Але якщо комунальні компанії перейдуть на технологію блокчейн, це допоможе користувачам заощадити власні кошти та забезпечить безпеку операцій. У цьому випадку, сторонами угоди є споживач та комунальна компанія. Квитанція за комунальні послуги, по суті, стає смарт-контрактом, в якому описано обов’язок споживача оплатити певну суму за послуги. Ця квитанція, так само як і грошовий переказ через мережу блокчейн, є унікальною та піддається незалежній перевірці без доступу до інформації про транзакцію або ваші особисті дані, та не підлягає жодним змінам. І найголовніше, це все безкоштовно. Технологія блокчейн може ефективно керувати процесами оплати, зберігання та передачі будь-яких фінансових та інших даних, вносячи значні зміни у наше уявлення про платіжні процеси.

Блокчейн існує, поки є хоча б один комп’ютер підключений до мережі. Кожен учасник може спостерігати за транзакціями, але не має доступу до їх змісту. Дані про транзакції зберігаються на різних пристроях, що є основною перевагою блокчейну. Ця розподіленість забезпечує високий рівень стійкості системи, оскільки вона не залежить від одного централізованого сервера і, отже, не піддається технічним проблемам або хакерським атакам на централізовану точку входу. Крім того, завдяки розвитку криптографії, виникають нові методи

шифрування, які роблять блокчейн відкритим для однієї сторони, а для іншої – надійно захищеним.

Однією з переваг блокчейну є його висока захищеність. У порівнянні з паперовими угодами, які можуть бути сфальсифіковані, електронні договори, що базуються на блокчейні, забезпечують вищий рівень безпеки. Вони дозволяють укладати угоди без посередників в автономному децентралізованому середовищі, що забезпечує прозорість та надійність транзакцій. Учасники таких угод залишаються анонімними, але рівноправними користувачами. В разі порушення угоди система автоматично анулює контракт і повертає ресурси усім учасникам, що забезпечує справедливість та надійність в угодах.

Після реєстрації даних в мережі блокчейн видалення чи зміни цих даних практично неможливе. Ця особливість робить технологію блокчейн ідеальною для використання в різних фінансових структурах та для збереження інформації про транзакції та інші дані. Завдяки блокчейну неможливо нанести шкоду чи вчинити будь-які недобросовісні дії. Ця технологія є довіреною, оскільки всі операції перевіряються тисячами комп’ютерів у процесі майнінгу [6].

Одним з недоліків технології блокчейн є так звана «атака 51%». Це можливість для одного суб'єкта контролювати понад 50% потужності хешування мережі, що може порушити роботу системи. Однак, на практиці такі спроби маніпуляцій над блокчейном не були успішними.

Іншим недоліком технології блокчейн є обмежена пропускна здатність для обробки транзакцій. Наприклад, платіжні системи, такі як MasterCard і Visa, здатні обробляти понад 40 тисяч операцій в секунду, в той час як технологія блокчейн значно обмежена цим показником. Щоразу, коли база даних розширюється, обсяг даних зростає, що може призвести до втрати вузлів мережі і недоступності для користувачів. Це також призводить до збільшення навантаження на електричну мережу, оскільки складні обчислення вимагають значних енергетичних витрат. Наприклад, споживання ресурсів мережею Bitcoin перевищує витрати на енергію цілих країн, таких як Данія та Ірландія.

2 ОСНОВНІ ПРИНЦИПИ ТА ФУНКЦІЇ ТЕХНОЛОГІЇ BLOCKCHAIN

2.1 Роль технології P2P в контексті blockchain мережі

Peer-to-peer (P2P) – це мережа, що складається з групи взаємопов'язаних пристроїв, які обмінюються файлами та зберігають однаковий набір даних. Кожен учасник, або вузол, має рівноправне становище, у відміну від централізованих архітектур, де сервер надає послуги іншим. У мережі P2P кожен учасник має можливість виконувати однакові завдання та мати однакову потужність. У мережі blockchain P2P-платформа дозволяє учасникам здійснювати транзакції через розподілену мережу без посередників. Сьогодні P2P архітектура є важливою складовою технології блокчейн. P2P-система складається з мережі розподілених користувачів, які розташовані в різних частинах світу. Зазвичай, в цій системі відсутній центральний сервер, оскільки кожен вузол зберігає копію всіх файлів і служить джерелом для інших вузлів. Таким чином, кожен пристрій може завантажувати файли з інших пристроїв та виконувати роль сервера для надання даних іншим пристроям [7].

У таких мережах існує безліч програмних додатків для обміну даними. Наприклад, один вузол може ініціювати процес завантаження даних з іншого вузла. Після успішної передачі даних цей вузол стає джерелом, фактично виступаючи сервером. Таким чином, учасник, який завантажує дані, діє як клієнт, а у випадку обміну зворотніми даними він виступає у ролі сервера. На практиці можливе одночасне виконання обох операцій - як завантаження даних, так і їх передача іншим учасникам мережі.

Залежно від структури і організації взаємодії, існують три основних типи P2P-мереж: структуровані, неструктуровані та гібридні.

У структурованих P2P мережах вузли організовані за допомогою хеш-функцій, що сприяє ефективному пошуку файлів, навіть якщо ці дані не є загальнодоступними. Такі мережі вимагають складнішої реалізації та підтримки.

У неструктурованих P2P мережах відсутня конкретна організація вузлів, тому учасники взаємодіють випадковим чином. Це забезпечує стійкість до змін активності вузлів, але призводить до значного навантаження на процесор та оперативну пам'ять.

Гібридні P2P мережі комбінують традиційну та однорангову моделі. Наприклад, можливе створення центрального сервера, що спрощує процес з'єднання вузлів. Такий підхід може покращити продуктивність мережі. З огляду на децентралізовану природу технології блокчейн, використання різних типів архітектур P2P мереж може впливати на рівень децентралізації.

Технологія Bitcoin використовує P2P мережу для безпосереднього обміну криптовалютою між користувачами без участі посередників. Ця система дозволяє уникнути втручання банків або інших централізованих установ у обробці та реєстрації транзакцій. Натомість, існує публічний цифровий реєстр, який перевіряється та підтримується великою кількістю учасників мережі.

Використання однорангової мережі недопущає можливість блокування або заморожування криптовалютних активів з боку центральних органів влади. Це означає, що кошти, збережені в цій системі, залишаються під повним контролем власника і не піддаються втручанню третіх сторін.

Однак, головним недоліком такої P2P мережі є необхідність постійного оновлення реєстрів, що вимагає значних обчислювальних ресурсів. Це може призвести до затримок у проведенні операцій та збільшення часу на обробку транзакцій. Тим не менш, розробники постійно працюють над вдосконаленням системи та пошуку способів оптимізації масштабування для забезпечення безпеки та ефективності мережі.

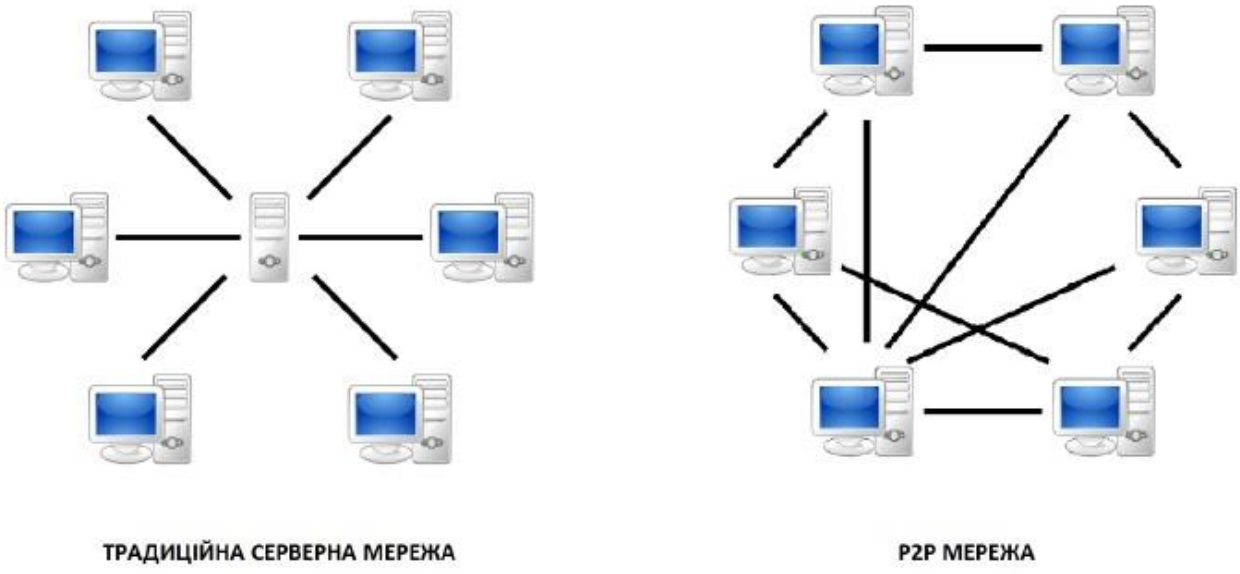

Рисунок 2.1 – Основні відмінності між серверною та P2P мережами

Мережевий вузол – це вузол, який може бути використаний для передачі або отримання повідомлень у мережі. Повні вузли в контексті блокчейн технології відіграють важливу роль у підтримці та безпеці мережі. Вони беруть участь у верифікації транзакцій та блоків згідно з правилами консенсусу системи.

Повний вузол в мережі Bitcoin - це вузол, який зберігає копію всієї блокчейн бази даних, включаючи всі транзакції та блоки. Щоб стати повним вузлом, потрібні наступні системні вимоги:

– потужний комп'ютер або сервер з підтримкою операційних систем Windows, Mac OS X або Linux;

– достатньо вільного місця на жорсткому диску для зберігання повної копії блокчейн бази даних;

– достатньо оперативної пам'яті для оптимальної роботи програмного забезпечення;

– швидке та стабільне підключення до Інтернету з швидкістю передачі даних не менше 50 кБ/с;

– здатність працювати безперервно протягом тривалого часу.

На сьогоднішній день в мережі Bitcoin існує приблизно 10 тисяч загальнодоступних вузлів. Ця кількість включає лише ті вузли, які є публічними та доступними для всіх користувачів.

Публічний вузол, також відомий як супервузол, може передавати інформацію будь-якому іншому вузлу, який вирішить з'єднатися з ним. Супервузол виступає як центральна точка передачі даних і зв'язку, працюючи без перерви та підтримуючи кілька з'єднань з вузлами по всьому світу. Для ефективної роботи такий вузол вимагає значних обчислювальних ресурсів та стабільного інтернет-з'єднання.

Майнери мають можливість вибирати між працюванням самостійно (соло майнінг) або у групі (пул майнінг). Соло майнери використовують свою власну копію блокчейну, тоді як у пулі майнери працюють разом, спільно внести свої обчислювальні потужності (хешрейт). Для участі у пулі майнерів потрібний адміністратор для налагодження та управління повним вузлом.

2.2 Різновиди мереж на основі технології blockchain

Блокчейн – це форма децентралізованої бази даних, яка дозволяє додавати нові записи в розподільну систему, доступну для різних учасників. Технологія блокчейн може бути класифікована за різними параметрами, включаючи тип доступу, спосіб контролю, та характер використання.

Публічний блокчейн – це відкрита мережа, до якої може приєднатися будь-хто. У таких мережах немає централізованої влади, тому їх іноді називають «безвласними». Жоден конкретний суб'єкт не має привілеїв або контролю над мережею. Це не означає, що публічний блокчейн менш захищений. Він пропонує високий рівень безпеки завдяки тому, що будь-який користувач може перевірити код мережі та брати участь у її самоуправлінні.

Масштабність публічних блокчейнів полягає в тому, що вони розподілені між безліччю вузлів. Це ускладнює можливість фальсифікації даних, оскільки

будь-які зміни в поточному стані мережі потребують змін у всіх копіях бази даних, що розподілені по різних вузлах.

Наприклад, публічний блокчейн Bitcoin є одним з найбільш відомих прикладів. Він базується на концепції децентралізації, де кожен користувач може перевіряти та долучатися до обробки транзакцій, забезпечуючи високий рівень безпеки та незалежність від централізованих структур.

Будь-хто може приєднатися до мережі Bitcoin, незалежно від свого віку, місця проживання чи матеріального стану. Ця відкритість є однією з ключових переваг публічного блокчейну, що забезпечується його прозорістю та відкритістю. Кожен авторизований вузол мережі містить копію цифрового журналу, що робить систему відкритою і прозорою, а також допомагає у запобіганні шахрайству, оскільки велика кількість вузлів слідкує за всіма операціями.

Одним із недоліків публічних блокчейнів є обмежена швидкість обробки транзакцій на секунду (TPS). Це відбувається через велику кількість вузлів, кожен з яких виконує процес перевірки та підтвердження транзакцій, що потребує значної кількості часу. Таким чином, публічні блокчейни, такі як Bitcoin, мають обмежену продуктивність порівняно з традиційними платіжними системами, наприклад, Visa та Mastercard.

Крім того, масштабування публічних блокчейнів також є проблемою, оскільки вузли мають обмежену можливість збільшення продуктивності. Неможливо просто додати додаткову оперативну пам'ять або використати процесор з високою частотою, оскільки це може призвести до функціональних обмежень. Крім того, зі збільшенням кількості вузлів виникає проблема з великим споживанням електроенергії, що також є серйозною проблемою.

Приватний блокчейн – це система з фіксованим списком учасників, яка часто використовується компаніями для внутрішнього аудиту та обміну даними. У такій системі доступ до блокчейну надається лише визначеним користувачам, які мають відповідні дозволи.

У приватному блокчейні централізований орган, такий як компанія, відповідає за створення та верифікацію транзакцій, а також за управління списком учасників, які мають право доступу до інформації. На відміну від публічного блокчейну, де дані є неизменними, в приватному блокчейні можливість зміни записів є можливою.

Учасники приватного блокчейну відомі один одному, але деталі транзакцій залишаються приватними. Ця модель знаходить своє застосування в ситуаціях, коли підприємствам потрібно підвищити ефективність обміну даними без публічного розголошення інформації про транзакції та контролювати доступ до них.

Однією з ключових переваг приватних блокчейнів є їхня висока швидкість обробки транзакцій. Це досягається завдяки обмеженій кількості вузлів у мережі, що робить процес консенсусу та перевірки транзакцій швидшим та ефективнішим. Приватні блокчейни можуть обробляти транзакції зі значною швидкістю, навіть до тисяч операцій одночасно.

Крім того, приватні блокчейни є дуже масштабованими, оскільки їхні розміри можуть бути легко адаптовані до потреб користувачів. У разі потреби у нових вузлах, компанії можуть швидко додати їх до мережі, або навпаки, відключити непотрібні вузли, що забезпечує гнучкість та ефективність управління системою.

Одним з основних недоліків приватних блокчейнів є їхня менша стійкість до атак порівняно з публічними системами. Це відбувається через обмежену кількість вузлів, які контролюються централізованим органом управління. Якщо один з цих вузлів стане жертвою атаки або буде компрометований, це може призвести до порушення безпеки всієї мережі. Таким чином, системи з централізованим управлінням є менш стійкими, оскільки суперечать ідеї децентралізації, яка є одним з ключових принципів технології блокчейн.

Гібридний блокчейн представляє собою розподілену мережу, керовану визначеними вузлами, які попередньо обираються. Ці системи поєднують в собі елементи як публічних, так і приватних блокчейнів. На відміну від чисто

приватних систем, гібридні мережі використовують підвищену криптографію для підвищення безпеки та аудиту.

У таких мережах контроль не зосереджується в одному центральному органі, але розподілений між кількома авторизованими користувачами. Гібридний блокчейн поєднує в собі як централізовані, так і децентралізовані аспекти, що дозволяє регулювати кількість користувачів, які можуть здійснювати перевірку транзакцій.

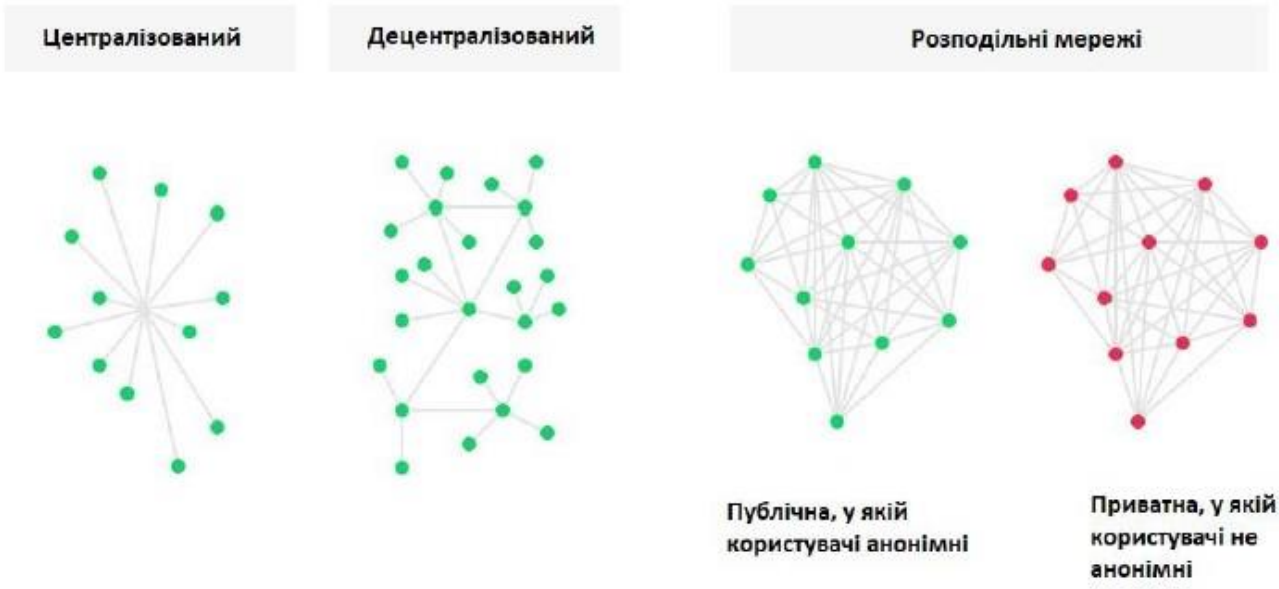

Рисунок 2.2 – Структура мереж blockchain

2.3 Організація та функціонування технології blockchain

Основні компоненти технології блокчейн включають блоки, ланцюг блоків та мережу. Кожен блок у блокчейні представляє собою структуру даних, що об'єднує транзакції та розподіляє їх між всіма вузлами мережі. Вміст кожного блоку містить інформацію про транзакції, що відбулися в системі. Блок складається з двох ключових частин: заголовка та тіла. Останнє включає список усіх транзакцій, які мають бути включені до поточного блоку для передачі в мережу блокчейн. Заголовок містить інформацію, що забезпечує стабільність та цілісність мережі.

Класичний заголовок в мережі блокчейн містить ряд обов'язкових полів:

– Версія (version) – це вказує на поточну версію блоку.

– Хеш попереднього блоку (p_block) –це хеш-значення попереднього блоку в ланцюжку.

– Хеш всіх транзакцій поточного блоку (tr_hash) – це хеш-значення, яке представляє унікальний ідентифікатор всіх транзакцій в поточному блоку.

– Мітка часу (time) – це вказує на час створення блоку.

– Nonce – це числовий параметр, який обчислюється в процесі майнінгу для досягнення заданого рівня важкості хешу блоку.

– Bits – це максимальне число, яке не повинно бути перевищено для хешу блоку.

Ці поля складають заголовок блоку. Окрім них, блок містить іншу інформацію, таку як транзакції, які вибирає майнер для включення в блок. Для обчислення хешу всіх транзакцій в блоку застосовується алгоритм Меркла, який генерує 256-бітний хеш. Це значення використовується для обчислення кінцевого хешу всього блоку. Розмір блоку та кількість транзакцій можуть відрізнятись в залежності від конкретної реалізації мережі блокчейн.

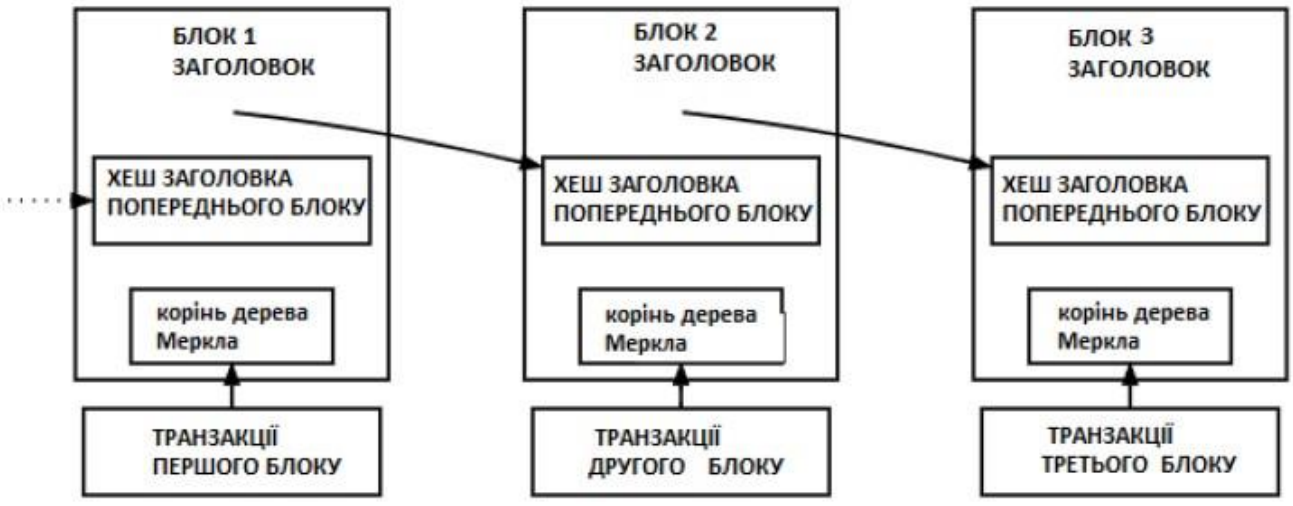

Рисунок 2.3 – Послідовний ланцюг блоків

Хеші використовуються для швидкого відрізнення даних одного блоку від іншого без необхідності порівняння кожного біту, що значно прискорює процес перевірки транзакцій. Кожен блок має свій заголовок, включаючи хеш попереднього блоку, корінь дерева Меркла та список транзакцій, з яких перша зазвичай є транзакцією винагороди за блок. Нижче подано приклад процесу хешування блоків. Кожен блок хешується разом з попереднім блоком, а в разі відсутності попереднього блоку, блок хешується сам з собою. Ці операції повторюються до отримання єдиного хешу - кореня дерева Меркла, який слугує підтвердженням достовірності блоку та правильності розташування транзакцій в ньому.

Ланцюг блоків є центральною частиною блокчейн системи, що містить історію всіх проведених транзакцій у мережі. Кожен учасник мережі має повну копію цього ланцюга, що забезпечує децентралізовану природу блокчейну. Така інформація дозволяє відстежувати кількість криптовалюти на будь-якій адресі протягом певного періоду часу. Транзакція залишається непідтвердженою, поки дані про неї не будуть згруповані у блок. Кожен блок в ланцюгу має лише одну точку відходу – блок, який не має попередника. Спостерігаючи за блоками від одного до іншого, ми можемо помітити гілкування, де кожен наступний блок може мати різних попередників. Через те, що блоки створюються різними майнерами одночасно, можуть виникати ситуації, коли один і той самий блок є попереднім для двох або більше наступних блоків. Кожен блок може містити інформацію про транзакції не лише свого блоку, а й попередніх. Кожна гілка в ланцюгу рівноправна, поки одна з них не стає коротшою за іншу. Система автоматично вибирає довший ланцюг, ігноруючи коротші гілки. Транзакції, що увійшли до коротшої гілки, стають непідтвердженими і втрачаються.

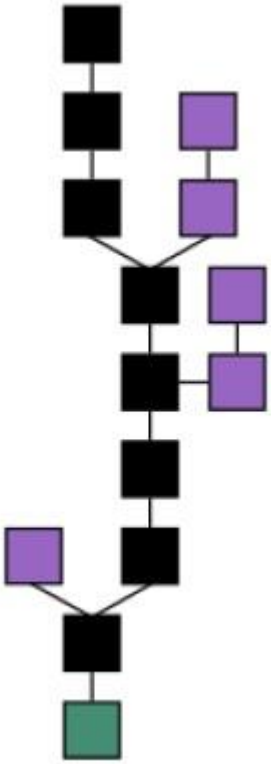

Рисунок 2.4 – Послідовна структура блоків

Публічна база зберігає інформацію про всі транзакції у незашифрованому вигляді. Для уникнення подвійного використання однієї суми, застосовуються мітки часу шляхом розбиття ланцюга на блоки. Кожен новий блок підтверджує транзакції, і дані про них містяться у всіх попередніх блоках.

Ланцюг блокчейну відображає децентралізовану систему, що не оперує центральним вузлом, а керується розподілом даних. Контроль над мережею забезпечується завдяки участь великої кількості незалежних учасників. Для забезпечення безпеки мережі, крім децентралізованої структури, використовується криптовалюта – цифровий актив з ринковою цінністю. Ця валюта використовується для проведення торгівельних операцій, подібних до операцій зі звичайними активами. Правила функціонування криптовалют для кожного блокчейну встановлюються його власними правилами. Загалом, програмне забезпечення передбачає компенсацію за роботу комп'ютерного обладнання, яке виконує функції повних вузлів. Повні вузли - це комп'ютери, які забезпечують функціонування мережі і можуть фізично знаходитися в різних місцях.

Мережа блокчейна складається з повних вузлів, які можна уявити як комп'ютери, що виконують програми з алгоритмами для захисту всієї системи. Кожен такий вузол зберігає повну копію всіх транзакцій, що колись були зареєстровані в ланцюгу блокчейну. Оскільки обслуговування вузлів вимагає значних витрат, контроль над транзакціями не є безкоштовним. Сам алгоритм блокчейну передбачає винагороду для вузлів у вигляді криптовалюти, такої як біткоїн.

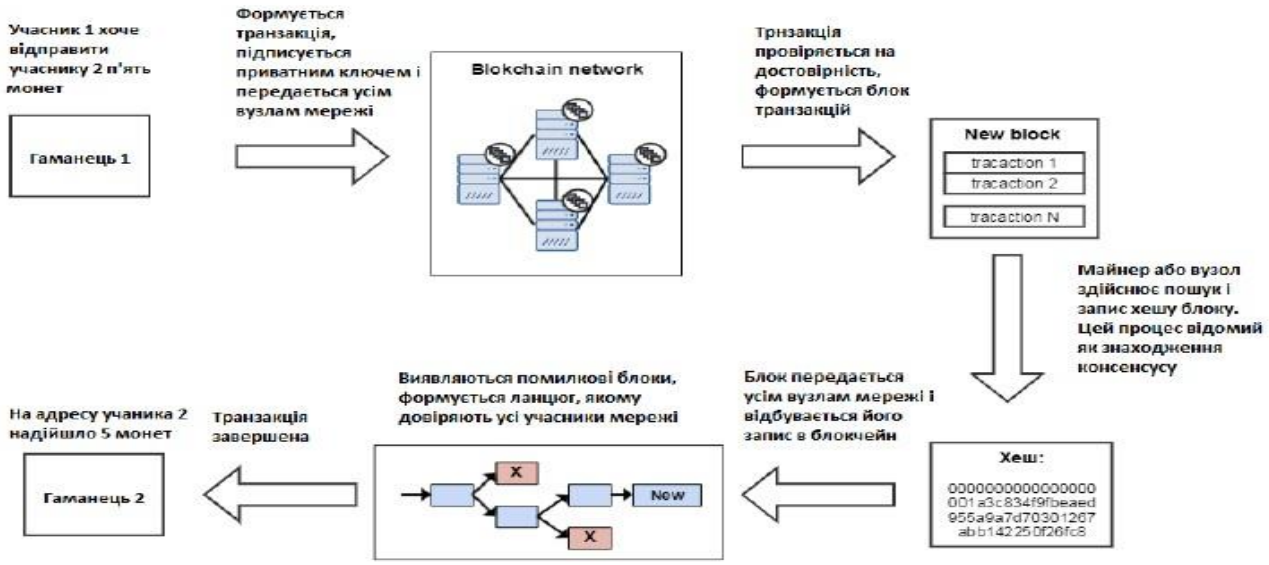

Рисунок 2.5 – Принципи функціонування blockchain мережі

2.4 Ключові аспекти технології blockchain

2.4.1 Основи децентралізації у технології blockchain

Децентралізація у технології блокчейн: перехід до розподіленого управління та фінансами без централізованого контролю. Ця концепція виникла з впровадженням блокчейн-технології, де всі учасники мережі мають однакові права. У децентралізованій системі блокчейн транзакції підтверджуються спільнотою, а не централізованим органом. Це досягається шляхом розподілу

обчислювальних ресурсів та даних по всьому світу з дублюванням інформації, що запобігає втратам та мінімізує ефективність DDOS-атак.

Децентралізація у криптовалюті відіграє ключову роль у забезпеченні безпеки та надійності транзакцій, а також збереженні коштів користувачів. Інформація про усі транзакції розподіляється між усіма користувачами мережі і підтверджується декількома незалежними вузлами, що робить цю систему невразливою до маніпуляцій. Навпаки, у банківських структурах використовуються централізовані системи, які є менш безпечними, а швидкість транзакцій залежить від завантаження та потужності локальних серверів. Велика кількість учасників у блокчейн-мережі, розподілених по всьому світу, сприяє підвищенню потужності та швидкості операцій.

Децентралізована система має важливу перевагу у відсутності залежності від зовнішнього регулювання. Наприклад, якщо правоохоронні органи вирішать втрутитись та конфіскують пристрої та розробки власника, в децентралізованій системі це неможливо. Технологія блокчейн має відкритий доступ, а потужності розподілені між великою кількістю учасників. Таким чином, криптовалюта залишається поза контролем влади, а її вартість визначається виключно попитом та пропозицією користувачів.

Приклад децентралізованого управління можна спостерігати на криптовалютних біржах. Ці біржі, побудовані на технології блокчейн, дозволяють користувачам мацювати контроль над своїми коштами. У порівнянні з централізованими біржами, де приватні ключі зберігаються на серверах біржі, децентралізовані електронні валюти повністю управляються їх власниками. Власник має можливість здійснювати транзакції та отримувати доступ до свого гаманця. У випадку централізованої системи, кошти зберігаються на банківському рахунку фінансового закладу, який має право на блокування та зняття цих коштів.

Bitcoin є одним з найвідоміших прикладів децентралізованої криптовалюти. Ця електронна валюта відома своєю відкритою та прозорою системою блокчейн, яка дозволяє відслідковувати всю історію транзакцій. Однак учасники мережі

залишаються анонімними. Розробники продовжують працювати над розвитком та вдосконаленням цієї блокчейн-системи.

Ще однією з відомих децентралізованих криптовалют є Ethereum. Ця криптовалюта володіє власною платформою, на якій розробники можуть запускати свої власні криптовалютні проекти. Ethereum є популярною валютою і займає друге місце за капіталізацією, після Bitcoin. Основна мета Ethereum полягає у здійсненні ролі для обміну ресурсами.

Ще однією відомою децентралізованою криптовалютою, яка з'явилася у 2012 році, є Ripple. Ця криптовалюта активно співпрацює з фінансовими установами та урядами з метою спрощення глобальної системи транзакцій. Хоча варто відзначити, що в централізованій мережі Ripple кожен вузол обирається компанією.

2.4.2 Принцип відкритості в мережі blockchain

Принцип прозорості в мережі блокчейн обмежує можливість збереження конфіденційності у цій системі. В цій технології особистість користувача відображається у вигляді унікального криптографічного ключа. При аналізі історії транзакцій ви побачите лише записи у вигляді «21Mf82jf023Kf92dfasfk291kfds821ksdf2FJK2l відправив 1 Bitcoin», не знаючи конкретної особи за цим ключем. Це відкриває можливість аналізувати всі фінансові операції, які були здійснені через цю адресу, не розкриваючи особистої інформації. Це може бути корисним, наприклад, для проведення аудиту фінансової діяльності компаній, які прагнуть зберігати конфіденційність своїх фінансових операцій.

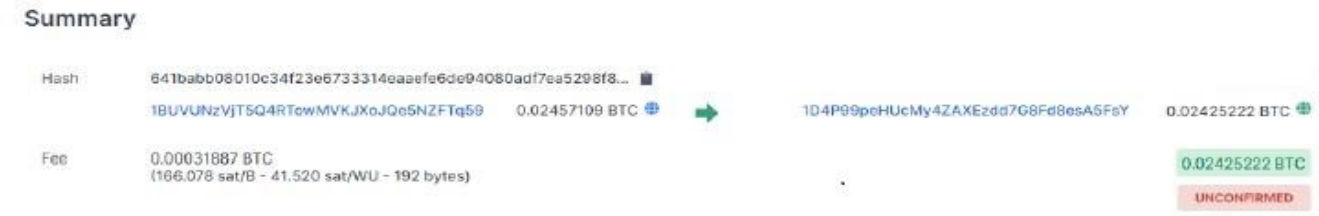

Рисунок 2.6 – Процес транзакції Bitcoin

Приклад транзакції у мережі Bitcoin. Включає хеш операції, публічні адреси відправника та отримувача, суму переводу, час та дату проведення операції, статус (не підтверджена), та винагороду майнеру (0.00031887 BTC). Сума транзакції на момент виконання складає 239.53$, а винагорода майнеру становить 3.11$.

2.4.3 Стійкість blockchain до змін

Незмінність блокчейну забезпечується за допомогою криптографічних хеш-функцій. Ці функції беруть на вхід будь-який рядок даних та перетворюють його в фіксовану довжину вихідних даних. Наприклад, для криптовалюти Bitcoin використовується алгоритм хешування SHA-256.

Рисунок 2.7 – Приклад використання алгоритму SHA-256 для шифрування даних

Криптографічна хеш-функція SHA-256 гарантує, що будь-який вхідний рядок буде перетворений в результат фіксованої довжини - 256 біт. Ця особливість особливо корисна при обробці великих обсягів даних, оскільки для збереження і відслідковування цих даних достатньо лише записувати їх хеш-коди. Навіть найменші зміни в вхідному рядку призводять до істотних змін у вихідному хеші, що робить хеш-функцію надійним інструментом для перевірки цілісності даних.

3 ПОТЕНЦІАЛ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ BLOCKCHAIN У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

3.1 Blockchain в телекомунікація

3.1.1 Платформа BubbleTone

Проблема міжнародного роумінгу вимагає значних витрат як для операторів мобільного зв'язку, так і для абонентів у всьому світі.

BubbleTone – це інноваційне телекомунікаційне рішення, що базується на технології Blockchain. Це рішення створене на основі приватної блокчейн-мережі, яка забезпечує автономне регулювання тарифів за міжнародний роумінг. BubbleTone є першою децентралізованою екосистемою, яка дозволяє операторам мобільного зв'язку, користувачам телефонів та постачальникам послуг взаємодіяти безпосередньо. Ця система з'єднує операторів і кінцевих користувачів у всьому світі за допомогою блокчейн-технологій.

Завантаживши безкоштовний додаток BubbleTone, користувачі можуть отримати доступ до роумінгових послуг без необхідності купувати SIM-карти місцевих операторів чи використовувати дорогі тарифи від свого провайдера. Система автоматично визначає місцезнаходження користувача та надає можливість вибору місцевих тарифів операторів замість роумінгу. Це дозволяє зекономити кошти та отримати зручний доступ до мобільного зв'язку у більш ніж 80 країнах світу.

Пряме підключення, яке впроваджується в цьому додатку, дозволяє користувачам отримувати доступ до високоякісного LTE зв'язку за доступними цінами. BubbleTone використовує консенсус PoS для ефективної обробки великих обсягів інтелектуальних даних. Цей додаток є абсолютно безкоштовним для завантаження, ви оплачуєте лише за послуги оператора. Ця можливість стає можливою завдяки тому, що BubbleTone отримує комісію від постачальників послуг за кожного нового користувача, якого вони привернули.

Ця система створює механізм для операторів зв'язку, де вони можуть пропонувати свої пакети послуг через смарт-контракти на ринку. Вони можуть створювати, публікувати та управляти своїми пропозиціями, які будуть доступні для інших операторів. Користувачі операторів можуть вибирати бажані пропозиції та оплачувати їх. Це активує смарт-контракт, який автоматично передає кошти та інші деталі угоди між операторами. Використання технології блокчейн дозволяє операторам взаємодіяти між собою ефективно та безпечно, спрощуючи процес узгодження угод [10].

Переваги системи BubbleTone для користувачів:

– забезпечення можливості здійснювати дзвінки за вигідними тарифами у будь-якій точці світу без необхідності підключення до місцевих операторів;

– збереження мобільного номера без необхідності змінювати його.

Переваги системи BubbleTone для операторів:

– забезпечення кожному оператору додаткової реклами;

– надання можливості кожному оператору отримати безпосередній доступ до міжнародного ринку з можливістю залучення нових клієнтів.

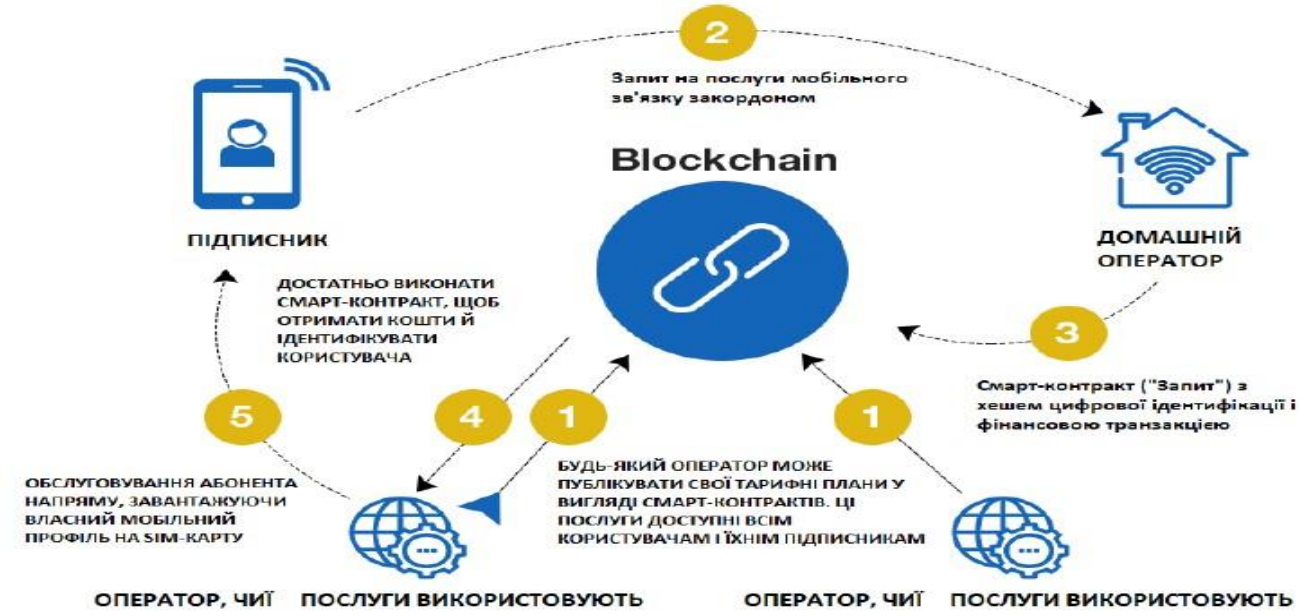

Рисунок 3.1 – Принцип функціонування платформи BubbleTone

3.1.2 Прототип роумінгового blockchain -рішення від компанії IBM

Спільний проєкт двох відомих компаній Syniverse і IBM спрямований на розробку передового рішення для роумінгу, використовуючи технологію блокчейн з відкритим вихідним кодом. Ця ініціатива створена з метою полегшення координації та автоматизації виконання угод між мобільними операторами. Завдяки використанню розумних контрактів, можна стандартизувати правила та процеси, а також регулювати транзакції між учасниками. Це сприятиме підвищенню ефективності роботи клієнтів та спростить вирішення потенційних конфліктних ситуацій в бізнесі.

Проблема. Постачальники послуг зв'язку (CSP) часто мають труднощі з управлінням абонентами, що користуються послугами роумінгу в мережах інших CSP. Часто вони не мають повної картини діяльності своїх абонентів у таких системах. Обробка платежів для клієнтів, що подорожують, вимагає значного часу через участь третіх сторін. Також актуальною залишається проблема виявлення та запобігання шахрайству, яка призводить до втрат провайдерів у розмірі понад 40 мільярдів доларів щорічно. Зловмисники можуть отримати доступ до мережі абонента, клонуючи його роумінговий профіль.

Рішення: В розробленій бізнес-моделі рис.3.2, враховано:

– абонентські SIM-карти, які ідентифікуються за номерами MSISDN і використовуються для здійснення та отримання дзвінків;

– CSP, які діють як домашні оператори або роумінгові партнери абонентських SIM-карт.

Рисунок 3.2 – Стратегія використання технології blockchain компанією IBM

Рішення передбачає чотири сценарії використання:

– Автоматична ідентифікація абонентів у роумінгу. Коли абонентна SIM-картці переходить до мережі роумінгового партнера, система автоматично визначає його присутність та автентифікує як користувача. Після цього тарифи оновлюються з використанням функції оновлення тарифів.

– Виставлення рахунків абонентам у роумінгу. Після авторизації абонента, він може здійснювати дзвінки через мережу роумінгового партнера. Функції "виклик" та "завершення виклику" використовуються для управління дзвінками, і кошти за них розподіляються між оператором та партнером на основі зазначених у смарт-контракті відсотків.

– Виявлення шахрайства. Система виявляє шахрайські SIM-картки, що намагаються використовувати той самий номер MSISDN, що й існуючі користувачі. Ці спроби ідентифікуються, а зловмисникам блокується можливість здійснювати дзвінки.

– Управління ресурсами. Система встановлює граничне значення ресурсів, доступних абоненту за його тарифним планом. Коли абонент наближається до цього ліміту, він сповіщається про це, і йому пропонується можливість зміни тарифу. Зміни можуть бути прийняті або відхилені абонентом, і подальші дзвінки обробляються відповідно до прийнятого рішення.

Переваги блокчейн-рішення від компанії IBM:

– автоматизоване управління контрактами між домашнім та роумінговим операторами;

– швидка обробка транзакцій без необхідності залучення посередників, що призводить до економії як для операторів, так і для користувачів;

– надійна система ідентифікації користувачів для запобігання шахрайству;

– надсилання миттєвих сповіщень про проблеми з тарифним планом в реальному часі.

3.1.3 Створення мережі IRBIS з використанням blockchain технологій

Проблема. В контексті сучасних мобільних технологій існує висока потреба у забезпеченні додаткового рівня безпеки для користувачів, щоб запобігти можливим кібератакам. Зловмисники можуть отримувати доступ до параметрів профілю користувача, адреси HLR (Home Location Register), де зберігаються ці параметри, а також адреси VLR (Visitor Location Register), де зберігається інформація про місцезнаходження абонента. Крім того, зловмисники можуть використовувати методи перехоплення SMS або прослуховування телефонних розмов.

Рішення. Компанія SC Telecom пропонує новий продукт під назвою IRBIS, який спрямований на підвищення конфіденційності телефонних дзвінків по всьому світу. Проект економічно розділяється на дві частини: фіатну і криптовалютну.

Функціонал фіатної частини дозволяє користувачам поповнювати баланс для здійснення дзвінків та надсилання повідомлень. SafeCalls Telecom є каналом, що виконує функції абонентського білінгу, тобто знімає кошти з рахунків користувачів і проводить платежі операторам зв'язку за використані канали зв'язку.

SafeCalls Telecom не оперує централізованою базою даних у доларах США для балансів і транзакцій, необхідних для коректного розрахунку користувальницьких платежів та комісій. Замість цього, система використовує децентралізовану структуру, яка складається з маршрутизаторів та блокчейну. Блокчейн зберігає тарифи різних операторів зв'язку, реєструє маршрутизатори в мережі, виконує платежі та запускає смарт-контракти для розрахунку плати за використання мережевих роутерів.

Фіатна частина системи використовується для обробки телефонних дзвінків, передачі мобільного трафіку та забезпечення приватності користувачів через функції, такі як анонімізація номерів телефонів та зміна тембру голосу.

Рисунок 3.3 – Принципи функціонування мережі IRBIS

Це блокчейн-рішення має важливу перевагу в захисті приватності користувачів, що забезпечує недосяжність для відстеження їхніх дій та неможливість прослуховування їхніх розмов.

3.1.4 Платформа для blockchain розробки від Cisco

Cisco інвестує значні зусилля у створення власної блокчейн-платформи, спрямованої на відповідь на потреби різних секторів промисловості. Ця платформа складається з різних рівнів, кожен з яких включає набір служб, доступних через спеціальні інтерфейси. Серед основних компонентів платформи - рівень комунікацій та база даних, які доповнюються механізмами штучного інтелекту для покращення функціональності. Також важливими є ідентифікаційний та захист користувачів. Ця платформа Cisco спрямована на створення екосистеми, яка об'єднує провайдерів, розробників програмного

забезпечення та консультантів для спільної розробки галузевих рішень для підприємств.

Центральною особливістю платформи є використання смарт-контрактів, які дозволяють автоматизувати та управляти угодами. Рівень комунікації та розподілу відповідає за взаємодію між вузлами блокчейну в умовах консенсусу. При оцінці нових блокчейн технологій для підприємства, важливо враховувати легкість впровадження та управління мережею, а також можливість інтеграції з існуючими системами. Платформа надає зручні інтерфейси для досягнення цих цілей та спрощення використання.

Платформа Cisco відкриває можливості для використання різних інфраструктурних технологій, включаючи апаратні модулі. Апаратно-незалежний блок визначає стандарти для забезпечення безпеки на рівні інфраструктури.

Однією з перспектив використання блокчейн-платформи Cisco є відслідковування пристроїв, підключених до Інтернету, для забезпечення надійності підключення та моніторингу їхньої активності. З розвитком Інтернету речей (IoT) передбачається значний приріст кількості підключених пристроїв, досягаючи близько 20 мільярдів пристроїв до 2023 року. У цьому контексті ідентифікація та управління пристроями стають ключовим завданням для забезпечення функціональності мережі. Тому платформа Cisco блокчейн має потенціал знайти широке застосування в майбутньому.

Рисунок 3.4 – Структура технологічної платформи від Cisco з використанням блокчейн технологій

3.2 Використання технології blockchain у телекомунікаційних системах

3.2.1 Використання технології blockchain для ідентифікації користувачів під час роумінгу

У сучасному світі телекомунікацій розвиваються величезними темпами. Проте, багато операторів зв'язку все ще користуються застарілими технологіями сигналізації для реєстрації користувачів у роумінгу. Це призводить до значних затримок у процесі автентифікації, часто до 15 хвилин чекання. В епоху швидких і миттєвих відгуків від програм та сервісів, такі затримки стають неприйнятними для користувачів.

Ще одним серйозним недоліком сучасних телекомунікацій є використання застарілої системи сигналізації SS7, яка демонструє свою незахищеність вже протягом більш ніж 10 років. Ця вразливість дозволяє зловмисникам використовувати різні методи атак для отримання конфіденційної інформації про абонентів та маніпулювання платіжними системами. Це може стати загрозою як для приватності користувачів, так і для безпеки їхніх фінансових даних.

Окрім зазначених недоліків, існує ще одна проблема, пов'язана з вартістю послуг. Телекомунікаційні компанії витрачають значні фінансові ресурси на процес автентифікації користувачів, проте отримують незадовільні результати від використаної системи, що не відповідає сучасним вимогам.

Щоб вирішити вищезгадані проблеми, пропонується використання технології блокчейн у телекомунікаційних мережах. Це дозволить оптимізувати процес надання послуг від операторів до користувачів шляхом використання сучасних методів шифрування, таких як SHA-3. Кожен оператор отримає свою пару відкритих та приватних ключів для забезпечення безпеки. Ідея полягає в створенні реєстру відкритих ключів для кожного постачальника, що сприятиме захищеному зв'язку між ними та покращить роботу відповідних служб. Зацікавлені сторони включають операторів мережі зв'язку та постачальників послуг, а GSMA може відігравати ключову роль у впровадженні цієї ініціативи.

Рис. 3.5 надає схематичне зображення інтерфейсів та основних компонентів. Застосування технології блокчейн дозволяє операторам скористатися перевагами спільних стандартизованих схем обробки транзакцій. Це рішення гарантує високий рівень безпеки за рахунок сучасних методів шифрування та забезпечує швидкий час реакції. Термін VPMN (відвідувана загальнодоступна мережа) використовується для позначення мережі, яку абонент використовує під час роумінгу, відмінної від його домашньої суспільної мережі (HPMN).

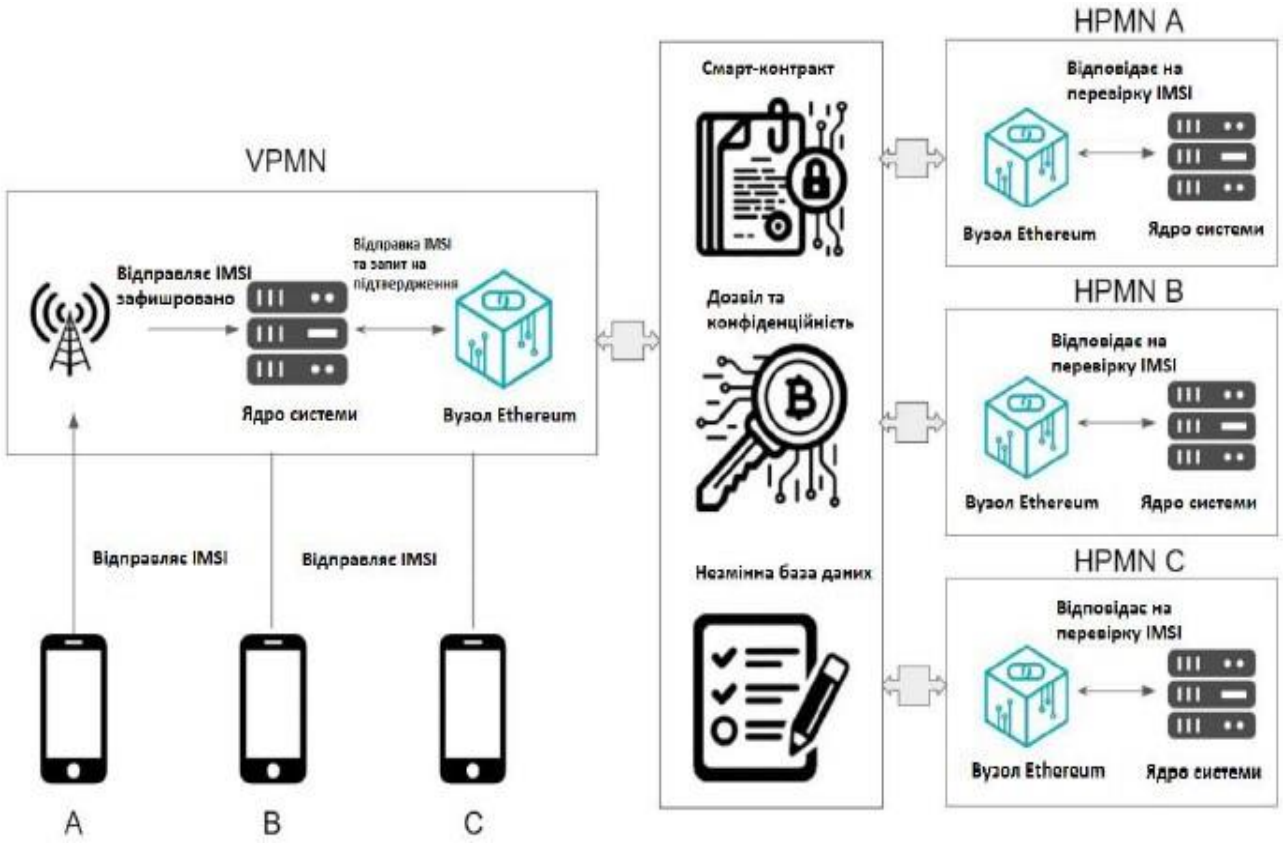

Рисунок 3.5 – Структура системи авторизації користувача у роумінгу з використанням технології blockchain

3.2.2 Оптимізація співпраці між операторами роумінгу за допомогою технології blockchain

Розвиток та підтримка роумінгових сервісів є важливою частиною діяльності телекомунікаційних компаній, але управління цими сервісами може бути викликом для операторів. Зниження витрат на надання послуг може призвести до зменшення їх вартості для користувачів.

Взаємодія між операторами щодо роумінгових транзакцій є складним процесом, який потребує значних зусиль і ресурсів. Це включає великі витрати на обробку платежів між провайдерами та вирішення фінансових питань відповідно до законодавства різних країн.

Впровадження нової системи узгодження дзвінків у роумінгу постає перед рядом викликів, таких як захист особистих даних, обробка великих обсягів інформації та забезпечення безпеки обміну даними між компаніями.

Для вирішення цієї проблеми різні компанії, що діють у сфері фінансів, об'єдналися в консорціум. Цей консорціум використовує блокчейн-технологію для прямого обміну даними між операторами. Такий підхід забезпечує децентралізовану базу даних та можливість розширення системи. За допомогою цього консорціуму можна створювати, розповсюджувати, перевіряти та підтверджувати фінансові угоди. Ці угоди ґрунтуються на смарт-контрактах в рамках блокчейн-мережі. Серед можливих застосувань фінансових угод є:

– створення та управління журналом транзакцій зі списком операцій і розрахунків вартості послуг;

– переадресація транзакцій користувачів між різними фінансовими операторами;

– запит на оплату послуг від клієнта одного оператора до іншого;

– підтвердження виставлених рахунків та реєстрація транзакцій в системі;

– узгодження платіжних балансів між фінансовими установами без посередництва третіх сторін;

– аналіз потоків коштів та виявлення сумнівних операцій для подальшого дослідження.

Завдяки вдосконаленому телекомунікаційному рішенню, компанії отримають змогу ефективніше аналізувати дані про використання послуг і порівнювати їх з умовами угоди з клієнтами. Це сприятиме більшій прозорості та швидкішому реагуванню на потреби користувачів, що в свою чергу призведе до зниження сервісних комісій. Для телекомунікаційних компаній такі рішення

також означають менші витрати на обслуговування, покращення безпеки системи та приваблення більшої кількості клієнтів.

Технічні зауваження:

– Доступ до мережі та реєстру може бути реалізований через відкриті механізми на основі технології blockchain, при цьому приватні дані та транзакції можуть бути зашифровані й оброблені за допомогою складних алгоритмів.

– Застосування алгоритмів консенсусу гарантує врахування потреб у пропускній здатності. Довірені сторони можуть валідувати та перевіряти транзакції.

– Мінімізація обробки даних можлива через передачу лише необхідної інформації до роумінгового вузла оператора.

Переваги:

– Забезпечена прозорість операцій між роумінговими партнерами за допомогою взаємного спостереження та застосування технології blockchain. Можливість укладання багатосторонніх угод на основі консенсусу з перевіркою всіх транзакційних записів.

– Смарт-контракти забезпечать автоматизоване виконання угод між усіма сторонами. Роумінговий оператор може отримувати інформацію про користувача, надавати послуги та реєструвати журнал викликів у спільній blockchain мережі. Домашній оператор може підтверджувати журнал викликів з реєстру роумінгового оператора та виставляти рахунки за послуги.

– Можливість обробки в реальному часі допомагатиме негайно обробляти транзакції та підтримувати баланс між операторами. Це сприятиме забезпеченню провайдерів інформацією про фактичні витрати в кожний момент часу для підтримки бізнес-прогнозів.

– Зменшення витрат усуне значну кількість паперових документів та знизить витрати на обмін коштів між операторами. Завдяки смарт-контрактам, провайдери матимуть спільні рушії рішень.

3.2.3 Захист приватності та можливості заробітку

Телекомунікаційні компанії по всьому світу стикаються з викликом збільшення витрат на розвиток інфраструктури та зрослою потребою користувачів у передачі великих обсягів даних. Це породжує загострену конкуренцію серед операторів зв'язку. Однією з ключових проблем, що виникають перед ними, є збереження приватності інформації. У зв'язку зі стрімким розвитком політики конфіденційності даних сучасного світу, цей процес вимагає захисту інформації, що належить абонентам: від різних документів та зображень до особистих даних та вибору хмарного сховища. Також важливо забезпечити захищеність даних, створених самими користувачами, таких як текстові повідомлення SMS, місцеположення, інтереси, придбані послуги та платежі. Компанії зв'язку використовують лише ті дані, на які отримали згоду від користувачів. Проте все частіше використовується розширена аналітика, що оперує великими централізованими даними поряд із передовими методами машинного навчання. Це дозволяє досліджувати більше інформації про користувачів.

Часте профілювання зазвичай виконується в різних групах або категоріях. Аналіз отриманих даних може включати детальні оцінки інтересів користувачів та вивчення їх активності. З цією інформацією телекомунікаційні компанії можуть оптимізувати свою бізнес-практику та процеси, включаючи раціоналізацію створення інфраструктури.

У реальності ситуація полягає в тому, що навіть якщо користувачі надають пряму та всебічну згоду на використання своїх даних, вони можуть бути недостатньо інформовані про те, як саме ці дані будуть аналізуватися та для яких цілей компанії будуть використовувати цю інформацію. Більшість випадків не передбачають отримання абонентами фінансової винагороди за таку інформацію. У той же час, світова обізнаність користувачів про важливість та цінність їх даних посилюється. Прийняття Загального регламенту з захисту даних (GDPR) в Європейському Союзі призводить до зростання вимог до організацій, які займаються обробкою великих обсягів інформації. GDPR встановлює вимоги

щодо згоди або інших законних підстав для обробки даних та повертає контроль над особистими даними користувачам. Положення GDPR стосуються трьох основних аспектів: відстеження даних, конфіденційність та право на забуття.

Розглянемо три основні аспекти GDPR:

– Управління персональними даними – персональні дані розповсюджені по різних програмах і системах, які зазвичай розміщуються на багатьох серверах та центрах обробки даних. GDPR вимагає, щоб було можливо отримувати доступ, повідомляти та видаляти особисту інформацію за запитом користувача або регулятивного органу. Відслідковування такого потоку даних є складним завданням, яке потребує високого рівня захисту.

– Забезпечення конфіденційності архітектури – це включає в себе розгляд різних підходів до побудови системної архітектури з урахуванням ризиків конфіденційності та відповідності захисту даних. Ці проекти охоплюють розробку нових IT-систем, створення нових фінансових продуктів та формування політики обміну даними з третіми сторонами.

– Право на забуття - це право фізичних осіб вимагати видалення всіх своїх особистих даних без затримок. Ця можливість просто здійснюється шляхом відкликання згоди на обробку своїх даних.

Технологія блокчейн може створити різноманіття децентралізованих сервісів, де взаємодіють учасники без потреби попередньої взаємної довіри. Смарт-контракти можуть використовуватися для вирішення проблем, з якими зіштовхуються телекомунікаційні провайдери. У системі блокчейн дані, що зберігаються, можуть бути як особистими, так і корпоративними, і вони можуть бути надійно зашифровані з використанням цієї технології. З точки зору права на забуття, особисті дані можуть бути збережені в окремому сховищі з криптографічним хешем, доступ до якого може бути забезпечений через мережу блокчейн, щоб абонент міг легко вимагати видалення своїх особистих даних.

Це рішення вносить значні покращення для абонентів, оскільки забезпечує покращену захищеність особистих даних та можливість обміну їх з вибраними сторонами. Використання технології блокчейн може виступати як засіб для

надання права власності на дані або позначки на інформацію, за яку абоненти подали запит на видалення.

Постачальнику послуг може бути вигідно встановлення нових відносин зі своїми абонентами, де він може краще вивчити їхні потреби та надавати їм сервіси на основі аналізу даних. Конфіденційність даних та право власності абонентів можуть бути забезпечені більш прозорими та стійкими методами, ніж це здійснюється зараз.

3.2.4 Впровадження технології blockchain у системи підтримки мереж 5G

Розгляд нових підходів до використання технології 5G у сфері мобільних телекомунікацій, яка обіцяє значно підвищити швидкість передачі даних у порівнянні з 4G. Впровадження цієї технології може створити нові можливості для бізнесу, що вимагають взаємодії з різними учасниками, включаючи операторів мобільного зв'язку, регуляторів та інфраструктурних постачальників. У той же час, технологія блокчейн активно використовується для ідентифікації, реєстрації та валідації активів і транзакцій, а також для регулювання взаємодії та обміну даними між різними сторонами. Вирішення завдання вибору найшвидшого і найближчого вузла вже стає ключовим аспектом діяльності телекомунікаційних компаній, і технологія блокчейн може допомогти впровадити відповідні механізми для цього.

На сьогоднішній день комунікаційні системи зазвичай базуються на централізованій моделі клієнт-сервер, де всі правила, що зберігаються на сервері, застосовуються до кожного користувача. Однак така модель може призводити до затримок і не завжди забезпечувати безперешкодне підключення пристроїв до мережі. У замість цього, можна розглядати об'єднання мереж доступу GPRS, WiMAX, WLAN та Wi-Fi в блокчейн мережу, де кожна точка доступу, наприклад, маршрутизатор Wi-Fi чи стільникова базова станція, може виступати як вузол мережі. Правила взаємодії між різними мережами можуть бути встановлені у смарт-контрактах, які мають динамічний характер, тому при зміні політики

потрібно лише внести зміни в код контракту. Коли пристрій передає своє місцезнаходження, вузол доступу, який може забезпечити найкращу швидкість, надає послугу користувачу. Це забезпечує безперебійну взаємодію між мережею та користувачем, а також просте розрахування за послуги між різними вузлами. Наприклад, якщо доступ до пристрою забезпечується через мережу WLAN офісу чи домашньої мережі, криптографічний провайдер автоматично зменшує рахунок відповідно до умов компанії.

Швидкий розвиток обсягів даних у мобільній мережі 5G підкреслив потребу в інноваційних рішеннях для забезпечення захисту та ефективного обміну інформацією в ненадійному середовищі. Багато абонентів не мають належного усвідомлення про те, де знаходиться та як захищена їх персональна інформація, і вони мають обмежені можливості контролю над своїми даними. Використання технології блокчейн може допомогти вирішити цю проблему, забезпечуючи підвищення ефективності обміну даними в мережі 5G, забезпечуючи прозорість, незмінність та стійкість до впливу зовнішніх факторів. Децентралізована архітектура дозволяє отримувати оброблені запити користувачів через розподілені вузли, що значно зменшує будь-які затримки.

В архітектурі такого рішення використовується концепція мета-ключів, де ці ключі зберігаються в децентралізованому сховищі у вигляді метаданих, захищених приватним ключем. Спільні дані можуть бути збережені у хмарному сховищі. Застосування блокчейну дозволяє захищати мобільні мережі, проводити транзакції на дуже детальному рівні, тоді як технологія 5G буде відповідати за навантаження мережі.

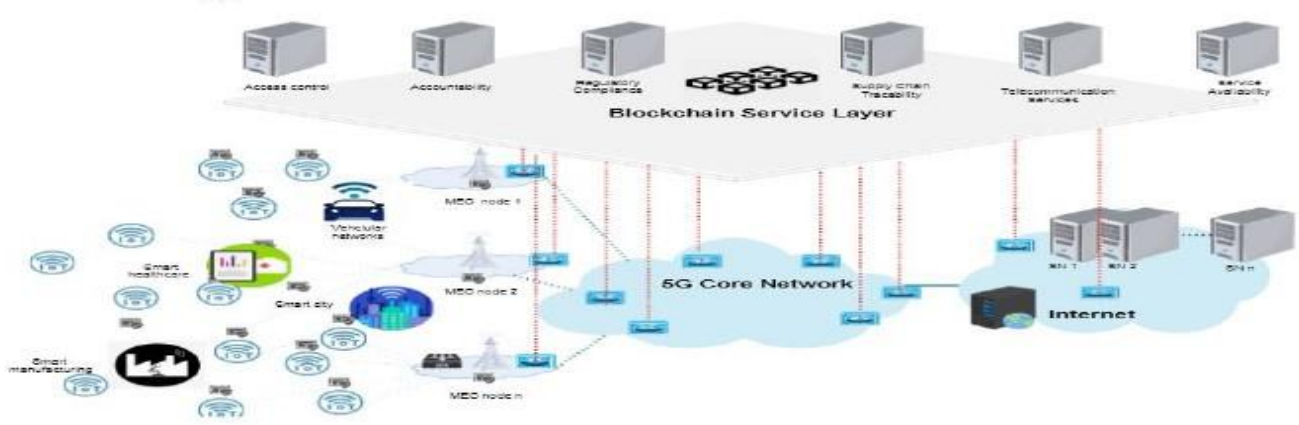

Рисунок 3.6 – Інтеграція технології блокчейн у контексті мобільних мереж 5G

3.2.5 Впровадження технології blockchain у сегменті Інтернету речей (IoT)

Розвиток інтернету речей швидко набирає обертів, очікується підключення мільярдів пристроїв у найближчому майбутньому. Збільшення кількості пристроїв IoT створює великі виклики, зокрема потребу в захисті персональних даних та забезпеченні безпеки взаємодії між ними. Це призводить до значних витрат на підтримку та розвиток інфраструктури. Використання децентралізованого управління на базі технології блокчейн дозволяє забезпечити масштабовану безпеку IoT та забезпечує прозору перевірку та захист від потенційних втручань.

Використання технології блокчейн у сфері Інтернету Речей відкриває можливість створення безпечних інтегрованих мережевих вузлів, що працюють синхронно і можуть бути реалізовані через вбудовані сенсори IoT з можливістю перевірки кожного блоку в мережі блокчейн.

Блокчейн у сфері IoT може забезпечити збереження інформації від сенсорів, забезпечуючи безпеку шляхом ідентифікації кожного пристрою IoT та захисту його від несанкціонованого доступу, спрощення процесу налаштування мережі та проведення оплати за послуги.

По-перше, технологія блокчейн забезпечує надійну безпеку, що є критичним в аспекті Інтернету Речей, де безпека дуже важлива.

По-друге, блокчейн-мережі можуть легко масштабуватися для впорядкування великих обсягів даних, що дозволяє швидко отримувати та передавати інформацію, що має велике значення в сучасному світі.

По-третє, важливо чітко розподілити права та обов'язки між користувачами та виробниками. Наприклад, у випадку, коли пристрій, встановлений пацієнту, завдає йому шкоди, потрібно визначити відповідальність за такі події.

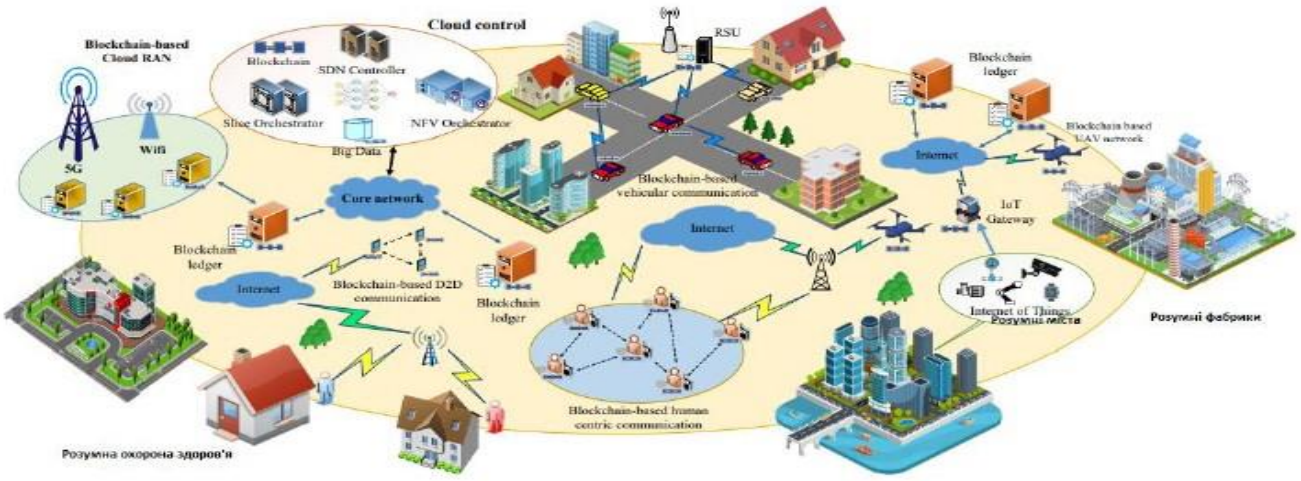

Рисунок 3.7 – Взаємодія мереж інтернету речей і технології blockchain

Використання технології блокчейн у поєднанні з IoT відкриває широкі можливості для надійного та безпечного обміну даними та коштами між пристроями. Ось кілька переваг цього підходу:

– забезпечення відстеження активів у реальному часі під час переміщення через складний ланцюг;

– спрощена перевірка виконання угод;

– гарантована незмінність записів, що дозволяє уникнути спірних ситуацій;

– надійне збереження та обробка даних відповідно до визнаних галузевих стандартів та вимог законодавства;

Ця комбінація забезпечує ефективний та безпечний обмін даними та коштами між пристроями, що є важливим для розвитку сучасних технологій зв'язку та інтернету речей.

4 ТЕХНІКО – ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ

4.1 Розрахунок капітальних витрат на розробку

Капітальні витрати на розробку становлять:

$$К=К1+К2 \quad (4.1)$$

де: К1– витрати на розробку, грн.;

К2– витрати на налагодження і дослідну експлуатацію програмного засобу на ПК, грн.;

4.2 Складові структури витрат на розробку

Складові структури витрат на розробку та реалізацію розробки розраховуються за формулою:

$$К1=Зз+Нз+Ві, \quad (4.2)$$

де: Зз – загальна зарплата розробників, грн;

Нз – нарахування на зарплату, грн;

Ві – інші витрати, грн;

Для проведення розрахунків зарплати (Зз) необхідно визначити спеціальність робітників, чисельність робітників і трудомісткість цих робіт. Для розробки проектного рішення потрібно чотири спеціалісти розробники:

– Керівник проекту(К);

–Студент-дипломник(СД);

– Консультант з економічне ї частини(КЕ);

– Консультант з охорони праці(КОП);

Згідно з штатним розписом сума витрат на оплату праці робітників, з 01.01.2025р. складає:

– Керівник (викладач вищої категорії) – 107,93 грн/год;

– Консультант з економічної частини (викладач вищої категорії) – 107,93 грн/год;

– Консультант з охорони праці(викладач першої категорії) 93,70 грн/год;

– Час витрачений керівником – tk = 14 годин.

– Час витрачений консультантом з охорони праці – tko= 1 година.

– Час витрачений консультантом з економічної частини–tke = 1 година.

– Час витрачений студентом дипломником tc = 3×50= 150 годин.

Витрати на оплату праці керівника проекту:

Ск = 14 роб.год.× 107,93 грн.год.=1511,02 грн.

Витрати на оплату праці консультанта з економічної частини:

Ске = 1 роб.год.×107,93грн.год.= 107,93 грн.

Витрати на оплату праці консультанта з охорони праці :

Ско = 1 роб.год×93,70грн.год.= 93,70грн.

Денна оплата студента дипломника :

1510/173=8,73 грн.

1510 – стипендія

173 – місячний фонд робочого часу, годин.

Витрати на оплату праці студента дипломника

Сс = 8,73×150= 1310 грн.

Витрати на оплату праці робітників проектустановлять

Зз= Ск+Ске+Ско+Сс= 1511,02 +107,93 +93,70 +1310= 3022,65 грн.

Нарахування на зарплату визначаються в розмірі 22% від фонду оплати праці

Нз = Зз×22% = (3022,65 ×22)/100 = 664,98 грн.

де 22 – норматив нарахування на зарплату, %

Інші витрати Ві відображають витрати які, не враховані в попередніх статтях витрат. Ці витрати розраховуються згідно структури витрат(5%)

Ві = 0.05×(Зз+Нз)= 0.05×(3022,65 +664,98)=1843,93 грн.

К1 = Зз+Нз+Ві= 3022,65 +664,98 +1843,93 =5578,56 грн.

4.3 Витрати на відлагодження розробки

Витрати на від лагодження та дослідну експлуатацію розробки

$$К2 = Sм\text{-}г. \times t \quad (4.3)$$

де Sм-г. – вартість однієї машино-години роботи конкретно ПК, грн./год.;

t–машинний час, витрачений на накладку та дослідну експлуатацію програмного засобу, год.

Вартісь 1 машинно-години роботи ПК розраховуємо за складовими витрат на таку роботу:

$$Sм\text{-}г =(А+Ен)/Фд \quad (4.4)$$

де А – амортизація використаного ПК, грн;

Ен – вартість електроенергії, яку споживає ПК, грн.;

Фд – дійсний час від лагодження програми, год.;

Розрахунок складових вартості 1 машино-години роботи ПК:

а) амортизація ПК становить

А= (Кт×На)/100 = (670,31 ×15%)/100= 100,55 грн.

Де Кт – вартість використання ПК, грн..

На – норма амортизації (На=15%)

Кт = (Кс×Тексп)/Твик = (14625×2,2)/48= 670,31 грн.

де Кс – вартість компютероної системи,грн.

Тексп – період експлуатації системи 2.2 місяців(50 робочих днів)

Твик – термін корисного використання 4 роки (48 місяців):

Кс= Ркомп×Р$ = 500×41,00=14625 грн.

де Ркомп –вартість комп'ютерної системи у доларах США;

Р$ – курс долара США по курсу НБУ на момент купівлі системи.

б) вартість використання електроенергії розраховується за формулою:

Ен = (Р×Тф)×Фд×Квик=(0,25 ×5,60)×150×0,8=154,8грн.

де Р – потужність обчислювальної системи, кВт (Р=0,25)

Квик – коефіцієнт використання ПК

Тф – ціна за 1кВт/год.,грн..(Тф = 5,16 грн.)

Фд – дійсний час від лагодження програми

Фд = пр.д.×Тсер= 50р.дн.×3год. = 150год.

Де пр.д. – кількість робочих днів ПК

Тсер = 3 год – середній щоденний час роботи ПК

Отже вартість 1 машино-години роботи і від лагодження на ПК становить

Sм-г=(100,55+154,8)/150= 1,70 грн.

Таким чином сумарні витрати на від лагодження і дослідну експлуатацію проектного рішення становлять:

К2=Sм-г×Фд= 1.70×150=255 грн.

Отже, капітальні витрати на розробку проектного рішення за формулою становлять:

К=К1+К2 = 5578,56 + 255 = 5833,56 грн.

Загальний кошторис витрат на розробку проектного рішення приведений в таблиці 4.1

Таблиця 4.1 – Кошторис витрат на розробку проектного рішення

Складові елементи витрат	Умовне позначення	Сума витрат, грн
Витрати на оплату праці	Зз	3022,65
Нарахування на зарплату	Нз	664,98
Інші витрати	Ві	1843,93
Разом	К1	5578,56
Витрати на відлагодження	К2	255
Разом К=К1+К2	К	5833,56

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЕДІЯЛЬНОСТІ

5.1 Загальні положення

Визначення поняття охорони праці дається в ст. 1 Закону України від 14 жовтня 1992 р. «Про охорону праці». Охорона праці – це система правових, соціально-економічних, організаційно-технічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження здоров'я і працездатності людини в процесі праці. В поняття охорони праці входять і всі ті заходи, що спеціально призначені для створення особливих полегшених умов праці для жінок і неповнолітніх, а також працівників зі зниженою працездатністю. Охорону праці і здоров'я громадян віднесено до пріоритетних напрямків соціальної політики України. Так, Конституція України одним з основних соціальних прав громадян визначає право кожного на належні, безпечні й здорові умови праці, встановлює, що використання праці жінок і неповнолітніх на небезпечних для їхнього здоров'я роботах забороняється. Завдання охорони праці:

– проектування підприємств, технологічних процесів і конструювання обладнання з обов'язковим виконанням вимог охорони праці;

– знаходження оптимальних співвідношень між різними факторами виробничого середовища, що дозволяє забезпечити мінімум несприятливого впливу їх на здоров'я працівників;

– розробка конкретних заходів щодо покращення умов праці та забезпечення її безпеки на основі застосування у виробництві новітніх досягнень науки і техніки;

– застосування раціональних засобів захисту працівників від впливу несприятливих факторів виробничого середовища, а також втілення організаційних заходів, які нейтралізують або послаблюють ступінь їх впливу на організм людини;

– розробка та застосування методів і засобів оцінки ефективності заходів з охорони праці, що плануються і здійснюються.

5.2 Організація охорони праці на підприємстві

На сучасному етапі науково-технічного розвитку нашої держави питання охорони праці на підприємствах є одним із найактуальніших.

Належна організація охорони праці, яка відповідає вимогам нормативно-правових актів, є основним заходом профілактики та запобігання виробничому травматизму й професійній захворюваності. Крім того, кожним трудовим договором передбачаються зобов’язання роботодавця щодо забезпечення найманих працівників безпечними умовами праці.

Законодавство України покладає на всіх роботодавців обов'язок щодо забезпечення безпечних і нешкідливих умов праці. Витрати на охорону праці на підприємстві згідно зі ст. 19 Закону повинні становити не менше 0,5% від фонду оплати праці за попередній рік, а за невиконання законодавства про охорону праці до підприємства можуть бути застосовані санкції аж до заборони його експлуатації.

Для того щоб не поставити під загрозу існування підприємства, роботодавцю необхідно:

– створити службу охорони праці.

Згідно зі ст. 15 Закону така служба обов'язково повинна бути створена на підприємстві з кількістю працюючих 50 і більше осіб відповідно до Типового положення про службу охорони праці, затвердженого наказом Держкомітету з нагляду за охороною праці від 15.11.2004 № 255. На підставі цього документа також має бути розроблено Положення про службу охорони праці цього підприємства, визначено структуру такої служби, її чисельність, основні завдання, функції та права її працівників. На підприємствах із кількістю працівників менше 50 осіб функції служби охорони праці можуть виконувати в порядку сумісництва особи, які мають відповідну підготовку.

– Розробити та затвердити на підприємстві положення, інструкції та інші акти з охорони праці.

Обов'язок роботодавця стосовно розробки та затвердження документів, які повинні встановлювати правила виконання робіт і поведінки працівників на території підприємства, у виробничих приміщеннях, на будівельних майдан-чиках і робочих місцях, передбачений ст. 13 Закону про охорону праці.

– Організувати проведення інструктажів з питань охорони праці.

Перед початком роботи нового працівника роботодавець згідно зі ст. 29 КЗпП зобов'язаний проінформувати його під розпис про умови праці, наявні на його робочому місці, у тому числі про всі небезпечні чи шкідливі виробничі фактори, які ще не усунуто, та про можливі наслідки їх впливу на здоров'я працівника, а також про можливі пільги та компенсації за роботу в таких умовах.

– Забезпечити навчання і перевірку знань з питань охорони праці.

Згідно зі ст. 18 Закону працівники, зайняті на роботах з підвищеною небезпекою або там, де є потреба у професійному доборі, проходять спеціальне навчання і перевірку знань відповідних нормативно-правових актів з охорони праці. Таке навчання з питань охорони праці може проводитись як безпосередньо на підприємстві, так і навчальним центром.

– Подбати про проведення медичних оглядів.

Згідно зі ст. 169 КЗпП роботодавець зобов'язаний за свої кошти організувати проведення попереднього (при прийнятті на роботу) та періодичних (протягом трудової діяльності) медоглядів працівників, зайнятих на важких роботах, роботах із шкідливими чи небезпечними умовами праці або таких, де є потреба у професійному доборі. Також він зобов'язаний проводити щорічний обов'язковий медогляд осіб віком до 21 року.

– Забезпечити працівників засобами індивідуального захисту.

На роботах із шкідливими й небезпечними умовами праці, а також на роботах, пов'язаних із забрудненням або несприятливими температурними умовами, працівникам згідно зі ст. 164 КЗпП необхідно безкоштовно видавати спеціальний одяг, взуття та інші ЗІЗ.

– Провести атестацію робочих місць.

На підприємствах, де технологічний процес, використовуване обладнання, сировина, матеріали є потенційними джерелами шкідливих і небезпечних виробничих факторів, які можуть негативно впливати на стан здоров'я працюючих, повинна проводитись атестація робочих місць за умовами праці. Така атестація повинна проводитися атестаційною комісією, склад і повноваження якої визначаються наказом по підприємству в строки, передбачені колективним договором, але не рідше одного разу на 5 років. Порядок проведення такої атестації передбачений постановою КМУ від 01.08.1992 № 442. Відомості про результати атестації заносяться в картку умов праці.

– Налагодити облік нещасних випадків.

Згідно зі ст. 22 Закону «Про охорону праці» роботодавець зобов'язаний організувати розслідування та вести облік нещасних випадків, професійних захворювань і аварій у порядку, встановленому постановою КМУ від 30.11.2011 № 1232. За результатами такого розслідування роботодавець повинен складати акт за формою Н-5 (якщо нещасний випадок визнано таким, що не пов'язаний з виробництвом) або Н-1 (якщо він визнаний пов'язаним з виробництвом). Один із примірників повинен видатися потерпілому або іншій зацікавленій особі не пізніше трьох днів з моменту закінчення розслідування.

5.3 Заходи безпеки на робочому місці

Конструкція робочого місця, його розміри та взаємне розташування його елементів повинні відповідати антропометричним, фізіологічним І психофізіологічним характеристикам людини, а також характеру роботи.

Організація робочих місць повинна забезпечувати стійке положення та вільність рухів працівника, безпеку виконання трудових операції виключати або допускати лише в деяких випадках роботу в незручну позиціях, котрі зумовлюють підвищену втомлюваність.

Загальні принципи організації робочого місця:

– на робочому місці не повинно бути нічого зайвого; всі необхідні для роботи предмети повинні знаходитись поряд з працівником, але не заважати йому;

– ті предмети, котрими користуються частіше, розташовуються ближче, ніж ті предмети, котрими користуються рідше;

– предмети, котрі беруть лівою рукою, повинні знаходитись зліва а ті предмети, котрі беруть правою рукою, повинні знаходитись справа;

– якщо використовують обидві руки, то місце розташування інструментів вибирається з врахуванням зручності захоплювання його двома руками;

– небезпечніше, з точки зору можливості травмування обладнання повинне розташовуватись вище, ніж менш небезпечне. Однак слід враховувати, що важкі предмети під час роботи зручніше опускати, ніж піднімати.

5.4 Санітарно-гігієнічні вимоги

Санітарно-гігієнічні вимоги до умов праці під час виконання роботи мають відповідати визначеним нормативам:

– параметри мікроклімату у приміщенні забезпечували комфортне самопочуття організму. Параметри мікроклімату закритих приміщень унормовані за санітарні норми ДСН 3.3.6.042-99.

– освітлення приміщень та робочих місць забезпечене відповідно до встановлених вимог. Відносно вікна робоче місце розміщено так, що природне світло збоку, переважно з лівого та забезпечувало коефіцієнт природної освітленості не нижче 1,5 %. Освітленість за штучного освітлення в площині робочої поверхні становила 300 – 500 Лк. Відношення яскравості робочих поверхонь було 3:1, а яскравість робочих поверхонь і стін (іншого обладнання) – 5:1. Використана система вимикачів, що дозволяє регулювати інтенсивність штучного освітлення залежно від інтенсивності природного, а також дозволяє освітлювати тільки потрібні для роботи зони приміщення.

– Дотримані вимоги до рівнів шуму та вібрації. Було дотримано допустимих рівнів звукового тиску в октавних смугах частот, еквівалентні рівні звуку на робочих місцях встановлені санітарними нормами виробничого 17 шуму, ультразвуку та інфразвуку ДСН 3.3.6.037-99.

– Надходження свіжого повітря регульоване, виходячи із відповідних нормативних.

– Передбачений захист від шуму та вібрацій.

Дотримані заходи особистої гігієни на робочому місці (підтримання чистоти, миття рук тощо). Заходи особистої гігієни на робочому місці передбачають щоденне вологе прибирання, утримання у чистоті робочого місця, наявність на робочому місці тільки необхідних для роботи засобів. На робочому місці необхідно дотримуватись вимог правил внутрішнього трудового розпорядку.

ВИСНОВКИ

Під час дослідження було виявлено, що технологія blockchain може стати ключовим інструментом для вирішення сучасних проблем у сфері телекомунікацій. Використання blockchain дозволяє покращити ефективність комунікаційних процесів, забезпечити безпеку та конфіденційність даних, а також реалізувати нові можливості, такі як автентифікація користувачів у роумінгу, оптимізація роботи операторів у роумінгу, монетизація даних та впровадження технологій 5G та IoT.

Технологічні рішення на основі blockchain, такі як ті, що запропоновані компаніями IBM, Cisco та іншими, вже показали свою ефективність у реальних умовах. Використання blockchain може допомогти вирішити проблеми збереження, доступу та безпеки даних, що є важливими для сучасного телекомунікаційного сектору. Хоча існують технічні та організаційні виклики, пов'язані з впровадженням цієї технології, але перспективи її використання в цій галузі дуже обіцяючі.

ПЕРЕЛІК ПОСИЛАНЬ

1. The History of Blockchain Technology [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://101blockchains.com/history-of-blockchain-timeline/.

2. Cryptography Hash functions[Електроннийресурс].Режим доступ удо ресурсу:https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm

3. Smart Contracts: The Ultimate Guide for the Beginners [Електронний ресурс]. – 2018. - Режим доступудо ресурсу: https://101blockchains.com/smart-contracts/

4. J. Golosova, A. Romanovs, “The Advantages and Disadvantagesof the Blockchain Technology”, Riga, 2018

5. What’sa Peer-to-Peer(P2P)Network?[Електроннийресурс].–2002.- Режим доступу до ресурсу: https://www.computerworld.com/article/2588287/networking-peer-to-peer-network.html

6. Blockchain Architecture Basics: Components,Structure,Benefits&Creation [Електронний ресурс]. – 2019. - Режим доступу до ресурсу: https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture

7. SCTelecom. IRBIS Network Decentralized telecommunications network [Електронний ресурс]. – 2019. - Режим доступу до ресурсу: https://safecalls.io/ieo/docs/SCTelecomWPv1.2.pdf?

8. Blockchain for telecom roaming, fraud user identification, and overage management. [Електронний ресурс].–2018.- Режим доступу до ресурсу:

https://developer.ibm.com/technologies/blockchain/patterns/blockchain-for-telecom-roaming-fraud-and-overage-management/

КОПІЇ ОБОВ’ЯЗКОВИХ КРЕСЛЕНЬ