Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра мережевих та інтернет технологій

ЗАТВЕРДЖУЮ
завідувач кафедри
мережевих та інтернет технологій
_____ Юрій КРАВЧЕНКО
«_____»_____2022 року

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

галузі знань 17 «Електроніка та телекомунікації»
за спеціальністю 172 «Телекомунікації та радіотехніка»
освітньо-професійна програма «Мережеві та інтернет технологій»

на тему:

Організація телекомунікаційної системи з використанням технології «Blockchain»

Виконав: студент групи МІТ -41
Ярослав ТРИКОЗ _____
(ім'я та ПРІЗВИЩЕ) (підпис)

Керівник: доцент кафедри мережевих та інтернет технологій
(посада)
к.т.н., доцент Ольга ЛЕЩЕНКО _____
(науковий ступень, вчене звання, ім'я та ПРІЗВИЩЕ) (підпис)

Київ 2022

Міністерство освіти і науки України
«Київський Національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра мережевих та інтернет технологій

ЗАТВЕРДЖУЮ
завідувач кафедри
мережевих та інтернет технологій
_____ Ю.В. Кравченко
«_____»_____2022 року

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ

Здобувачу вищої освіти Трикозу Ярославу Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи:
Організація телекомунікаційної системи з використанням технології «блокчейн»
затверджена на засіданні кафедри МІТ «24» грудня 2021 р. протокол №8
2. Термін здачі закінченої роботи «30» травня 2020р
3. Вихідні дані до проекту (роботи)
Мова програмування – C, C#.
Технологія Arduino: контролер, датчики, bluetooth-модуль. Програмне забезпечення XCSoar.
4. Зміст пояснювальної записки (перелік питань, що їх потрібно розробити, обсяг – 35-40 стор.)
Вступ
1. Що таке blockchain. Історія виникнення
1.1. Історія розвитку технології Blockchain.
1.2. Основні поняття технології Blockchain. Алгоритми шифрування. Смарт-контракти
1.3. Переваги та недоліки Blockchain
1.4. Постановка задачі

2. Принципи та функції blockchain
2.1. Мережа P2P та її роль для blockchain
2.2. Класифікація blockchain мереж. Властивості технології blockchain
2.3. Структура та принципи функціонування блокчейн
3. Можливості застосування blockchain у телекомунікаційних системах
3.1. Використання blockchain для IoT
3.2. Розумний будинок на базі технології Blockchain.
3.3 Основні компоненти. Компоненти Розумного Будинку. Керування транзакціями
Висновки
5. Перелік графічного матеріалу 8-10 слайдів
Дата видачі завдання
Керівник роботи Ольга ЛЕЩЕНКО
(підпис) (посада, прізвище, ім'я, по батькові)

Завдання прийняв до виконання
Ярослав ТРИКОЗ
(підпис)

Дата видачі завдання

КАЛЕНДАРНИЙ ПЛАН ВИКОНАННЯ РОБОТИ

Номер	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Підготовчий	02.05.2022	
2	Розділ 1	10.05.2022	
3	Розділ 2	15.05.2022	
4	Розділ 3	20.05.2022	
5	Доповідь та слайди	25.05.2022	
6	Пояснювальна записка	30.05.2022	

Здобувач вищої освіти _____ Ярослав ТРИКОЗ
(підпис)

Керівник _____ Ольга ЛЕЩЕНКО
(підпис)

Реферат

Дипломна робота містить 51 сторінка, 15 рисунків. Було використано 12 джерел інформації.

Мета роботи полягає у вивченні основних принципів роботи блокчейну. Дослідження можливості використання технології blockchain у телекомунікаційних системах та розгляд уже існуючих рішень на базі blockchain.

Технологія Blockchain дуже стрімко розвивається. Вона надає можливість створення нових бізнес-моделей в різних галузях, зокрема, і в телекомунікаціях. Послуги, які надають телекомунікаційні компанії, можна розглядати як складну екосистему, вимагає великої кількісті взаємозалежних груп операторів, як внутрішніх так і зовнішніх, які хочуть і можуть працювати над спільними проектами. По факту, блокчейн уже використовується для того, щоб позбутися посередників між операторами, запобігання шахрайству у роумінгу і для ефективної мобільності телефонних номерів.

Ключові слова: blockchain, телекомунікаційна система, смарт-контракт, шифрування, децентралізація, база даних, криптосистема.

ABSTRACT

The work contains 51 pages, 15 illustrations, 12 sources of used information.

The purpose of the work is to study the basic principles of blockchain. Research of the possibility of using blockchain technology in telecommunication systems and consideration of already existing solutions based on blockchain.

Blockchain technology is evolving very rapidly. It provides an opportunity to create new business models in various industries, including telecommunications. The services provided by telecommunications companies can be considered as a complex ecosystem, requiring a large number of interdependent groups of operators, both internal and external, who want and can work on joint projects. In fact, the blockchain is already being used to get rid of intermediaries between operators, to prevent roaming fraud and for the effective mobility of telephone numbers.

Keywords: blockchain, telecommunication system, smart contract, encryption, decentralization, database, cryptosystem.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

eSim – an embedded-SIM

IoT (Internet of things) – Інтернет речей

P2P – Peer-to-Peer

PoC (Proof of Consept) – доказ існування певного методу

PoS (Proof of Stake) – метод захисту в криптовалютах, заснований на необхідності доказу зберігання певної кількості коштів на рахунку

PoW (Proof of Work) – Доказ виконаної роботи

CSP (Crypto Service Provider) – криптопровайдер

WLAN (Wireless Local Area Network) – безпровідна локальна мережа

BC – Blockchain

CH (Cluster Head) – кластер-керівник

PK (Public Key) – публічний ключ

SHA – Secure Hash Algorithm

ВСТУП

Сфера телекомунікацій бере свій початок зі створення у 1876 році американським винахідником Александром Беллом першого прототипу сучасного телефону. З моменту винаходу минуло вже більше століття, і технології докорінно змінили те, як ми спілкуємося та обмінюємося інформацією. Найвагоміший винахід сьогодення є, безумовно, Інтернет. Проте і на цьому людство не зупинилося, і те що вчора здавалося «проривом» вже сьогодні втрачає свою актуальність. Так було, наприклад, зі першими мобільними телефонами ще 20-30 років тому. Вони мали великі габарити та доволі обмежений функціонал у порівнянні зі сучасними смартфонами, також була під питанням доступність, коли лише обмежене коло осіб мало змогу користуватися пристроями.

Нині щороку крупні корпорації та виробники змагаються одне з одним у спроможності створити більш потужний пристрій, шляхом підвищення ємності оперативної пам’яті, об’єму батареї та інше. Все це призводить до недостачі місця у корпусі телефону, тому віднедавна впровадили технологію eSIM. Мета технології – заміна пластикової USIM-картки, що надає змогу користуватися декількома телефонними номерами. Зважаючи на подібні новинки, варто також попіклуватися про безпеку даних у смартфоні. Задля вирішення цієї проблеми необхідно звернути увагу на технологію під назвою Blockchain.

Blockchain (англ. Block chain від block – блок, chain - ланцюг) – це розподілена база даних, яка складається з впорядкованих ланцюжкових записів, які називаються блоками. Захист від підробок забезпечується тим, що кожен блок має часову позначку та посилання на попередній блок хеш дерева. Хоч технологія вважається загальнодоступною, це аж ніяк не означає, що будь-хто може отримати доступ до конкретних транзакцій. До технології входить створення приватного ключа, до якого має доступ лише певний користувач і за допомогою ключа можна отримати доступ до конкретних даних.

Зараз Blockchain – одна з найбільш обговорюваних та відкритих технологій. Ця технологія має можливість змінити підхід до створення бізнес-моделей в

багатьох галузях, включаючи телекомунікації. На даний момент, технологія вже використовується для того щоб, позбутись посередників між операторами, запобігання шахрайству, та мобільності телефонних номерів.

Перспективним напрямком використання блокчейну є активне впровадження технології у системи IoT. Світові компанії наразі працюють над розробкою протоколу на базі технології блокчейн, що дозволить безпечно обмінюватись інформацією між різними IoT- пристроями. Зважаючи на те, що з кожним днем все більше і більше пристроїв під’єднуються до мережі Інтернет, то відповідно підвищується і ризик злому або ж іншого неналежного втручання у роботу пристроїв, що може призвести до небажаних наслідків. Тому можливість використання нової та безпечної технології є досить актуальним.

1. ЩО ТАКЕ BLOCKCHAIN. ІСТОРІЯ ВИНИКНЕННЯ

Мета розділу – розглянути основні поняття технології Blockchain та історію його створення. В рамках розділу пропонується визначити основне призначення blockchain у світі інформаційних технологій. Розгляд технології наддасть гарний фундамент задля подальшого аналізу шляхів використання у телекомунікаційній сфері.

1.1 Історія розвитку технології Blockchain.

Blockchain – це технологія, яка представлена як розподілена структура даних, що складається з послідовності блоків, де кожен блок містить хеш із попереднього блоку, тим самим утворюючи ланцюг блоків (рис. 1.1). Перший блок у ланцюжку (батьківський блок, genesis block) розглядають як окремий випадок, оскільки в нього відсутній попередній блок. Blockchain функціонує у вигляді розподіленої бази даних, яка здійснює облік усіх транзакцій у мережі. Транзакції мають помітки часу та зберігаються у блоках, де кожен блок ідентифікується своїм криптографічним хешем. Blockchain зберігається повністю у кожному вузлі мережі. Blockchain для роботи не потрібна довіра між вузлами мережі, адже будь-який вузол може самостійно перевірити, чи збігається його копія бази з копіями, які зберігаються в інших вузлах.

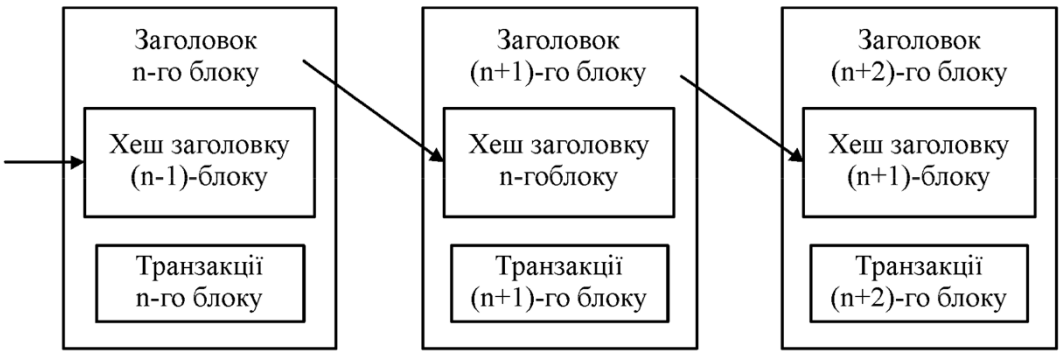

Рис 1.1 Спрощена послідовність блоків.

За останні роки технологія набула великої популярності, однак її історія розпочалася набагато раніше. У 1991 році за авторством С.Хабера та У.Скотта була опублікована перша наукова робота, котра описувала криптографічний захист ланцюжків блоків. Автори ставили за мету створити систему, в якій неможливо було б підробити часові позначки. Система використовувала криптографічно закріплений ланцюжок блоків, для зберігання документів з позначкою часу, а 1992 року дерева Меркла були введені у розробку, що зробило її ефективнішою, дозволивши збирати кілька документів в один блок.

Згодом, у 2008 році, людина або ж група людей під псевдонімом Satoshi Nakamoto, опублікували статтю «Bitcoin: A Peer-to-Peer Electronic Cash System», яка описувала концепцію та принципи роботи платіжної системи у вигляді одноранговой мережі. У 2009 р. Було представлено протокол криптовалюти Bitcoin та опубліковано код програми-клієнта. Ключова особливість концепції полягала в тому, що онлайн платежі між учасниками здійснюються без центральної фінансової установи, котра виконує роль довіреної структури, з використанням криптографічних методів та публічної розподіленої бази даних, яка складається з ланцюжка блоків (Blockchain). Першим одержувачем Біткойна був Хел Фінні, він отримав 10 біткойнів від Сатоші Накамото, в першій Bitcoin транзакції у світі, 12 січня 2009 року.

У 2013 році, Віталік Бутерін, програміст та один із засновників журналу «Bitcoin», заявив, що Біткойн потрібна скриптова мова для створення децентралізованих додатків. Віталік розпочав розробку нової, розподіленої, обчислювальної платформи на основі блокчейн, Ethereum, який показав скриптову функціональність, яку називають смарт-контрактами. «Розумні» контракти – це програми або скрипти, які застосовуються та виконуються в блокчейні Ethereum, їх можна використовувати, наприклад, для здійснення транзакції, якщо виконуються певні умови.

На сучасному етапі блокчейн продовжує свій розвиток та все більше передових компаній знаходять нові шляхи з метою використання технології. Компанія Microsoft активно інвестує кошти в спеціалістів в області Blockchain,

результатом чого були створені приватні та гібридні блокчейни. Samsung та IBM на даний момент працюють над перспективним проектом Adept, котрий дозволить створити децентралізовані мережі із великої кількості пристроїв Інтернету Речей (IoT) використовуючи блокчейноподібні технології.

1.2 Основні поняття технології Blockchain

Технологія Blockchain уособлює новий підхід до побудови розподілених баз даних з метою спільного збереження інформації. Блокчейн складається з двох ключових елементів: блок та операції.

Блок – це файл, в якому зберігається інформація про проведені транзакції, до моменту створення блоку. При створенні блоку, в нього додаються всі недавні транзакції, що не входили у попередні блоки. Щойно створений блок додається у кінець ланцюга і його вже буде неможливо змінити у майбутньому.

Транзакція або операція – передача даних від одного адресу на інший. Подібним чином функціонують фінансові транзакції, де пересилаються кошти між відправником та одержувачем.

Основа технології blockchain – використання різних технологій та методів роботи і шифрування даних.

- Асиметричні алгоритми шифрування, або «асиметричні криптосистеми»
- Смарт-контракти – протокол, що використовується, як інструмент заключення договорів.
- Хеш-функції або «хешування» даних
- Хеш-таблиці – асоційований масив, використовуються для запису результатів хешування у вигляді ключ-значення.
- Proof of Concept (PoC) та алгоритми консенсусу – доказ концепції, як метод підтвердження події (верифікація угоди) в системі.

Розглянемо ці поняття більш детально.

1.2.1 Асиметричні алгоритми шифрування

Асиметричні алгоритми шифрування – це набір методів, для захисту даних користувача, що передаються у систему Blockchain. Алгоритми використовують два ключі. Перший ключ є відкритим, він використовується для зашифровування даних. Другий ключ – таємний, відповідно він потрібен для розшифровування. Таким чином ключі є унікальними і вони не здатні замінити одне одного.

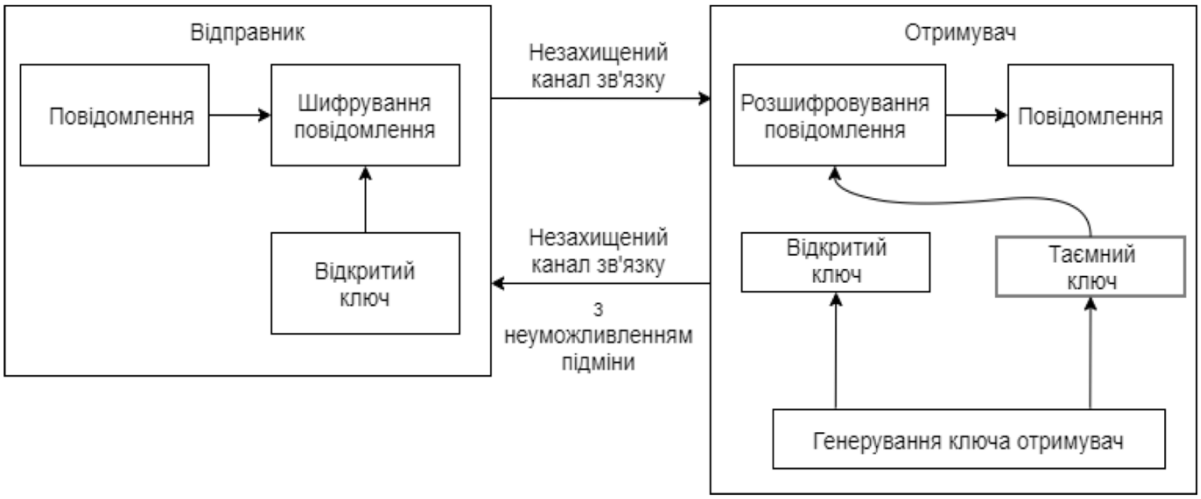

Рис 1.2.1.1 – Схема передачі даних у асиметричних криптосистемах

Ідея криптографії з відкритим ключем тісно пов’язана з ідеєю односторонніх функцій, або таких функцій f(x), що знаючи значення аргументу ‘x’ достатньо легко знайти значення функції, тоді як визначення аргументу з функції досить складне в сенсі теорії.

В цілому, всі сучасні криптосистеми з відкритим ключем використовують один з даних типів незворотних перетворень:

1. Розбиття великих чисел на прості множники;

2. Розрахунок логарифмічних функцій у скінченному просторі;

3. Розрахунок коренів алгебраїчних рівнянь.

Одні з найпопулярніших криптосистем є RSA, Діффі-Геллмана або Ель Гамеля.

Електронний підпис – це ряд символів, який водночас залежить і від відправника та змісту повідомлення. Використовується задля перевірки повідомлення, чи дійсно воно належить користувачу в мережі. Жоден, включно із користувачем, не здатен змінити зміст повідомлення так, щоб підпис залишався без змін.

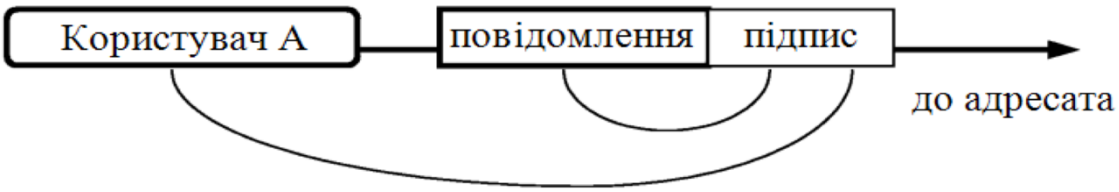

Рис 1.2.1.2 – Підпис як частина повідомлення

1.2.2 Хеш-функція

Хеш-функція або функція згортки – це функція, яка займається перетворенням вхідного масиву даних довільної довжини у вихідний бітовий рядок фіксованої довжини. Хеш-функція фактично бере будь-які дані (повідомлення), та перетворює їх у рядок з букв та цифр (хеш). Незважаючи на те що одні і ті ж дані повертають однаковий хеш – відтворити початкові дані за хешем майже неможливо.

Наразі існують доволі багато криптографічних функцій, проте розглянемо найбільш популярні.

Алгоритм MD5 перетворює текст будь-якої довжини у 128-бітний криптографічний рядок. Алгоритм отримав широке поширення в сучасних мережах як спосіб перевірки цілісності файлу шляхом порівняння даних з попередньо розрахованим хешем.

Алгоритм SHA-256 – розроблений Агентством національної безпеки США. Алгоритм працює з даними, що розподілені на блоки по 512 біт (64 байти). Виконує криптографічне «змішування» та видає в результаті 256-бітний хеш-код.

Цей алгоритм робить розшифрування дуже складним процесом, через завелику кількість варіантів.

1.2.3 Хеш-таблиця

Хеш-таблиця – структура даних, що являє собою асоційований масив даних, який зберігає пари ключ-значення. В таблиці положення елементів залежить від значення елементу. Також таблиця дозволяє реалізувати три операції: додавання нової пари, операція пошуку по ключу, операція видалення по ключу.

Хеш-таблиці поділяються на декілька видів:

- З лінійним розміщенням (метод ланцюжків) – в таблицях виконується пошук вільної комірки до тих пір, поки не буде знайдена вільна.
- З відкритою адресацією – таблиці використовують в якості сховища даних неперервний масив.

Колізією називається ситуація, коли для різних ключів отримується одне й те саме хеш-значення. Подібна ситуація відбувається нерідко, якщо наприклад, при додаванні в хеш-таблицю розмірністю 365 комірок лише 23-х елементів ймовірність виникнення колізії перевищує 50 відсотків (за умови якщо кожен елемент з однаковою ймовірністю має шанс потрапити в будь-яку комірку) Враховуючи цю проблему, механізм розв'язання колізій — це важлива складова при роботі з будь-якою хеш-таблицею.

У методі ланцюжків кожна комірка масиву є вказівником на зв’язаний список (ланцюжок) пар ключ-значення, відповідних одному і тому самому хеш-значенню. Колізії у свою чергу призводять до того, що з'являються ланцюжки більше одного елемента у довжину. Операції пошуку або видалення елемента потребують перегляд усіх елементів ланцюжка, задля знаходження в ньому елементу зі заданим ключем. Щоб додати новий елемент необхідно додати його в кінець або в початок списку, і, якщо коефіцієнт заповнення стане занадто великим, потрібно збільшити розмір масиву та перебудувати таблицю.

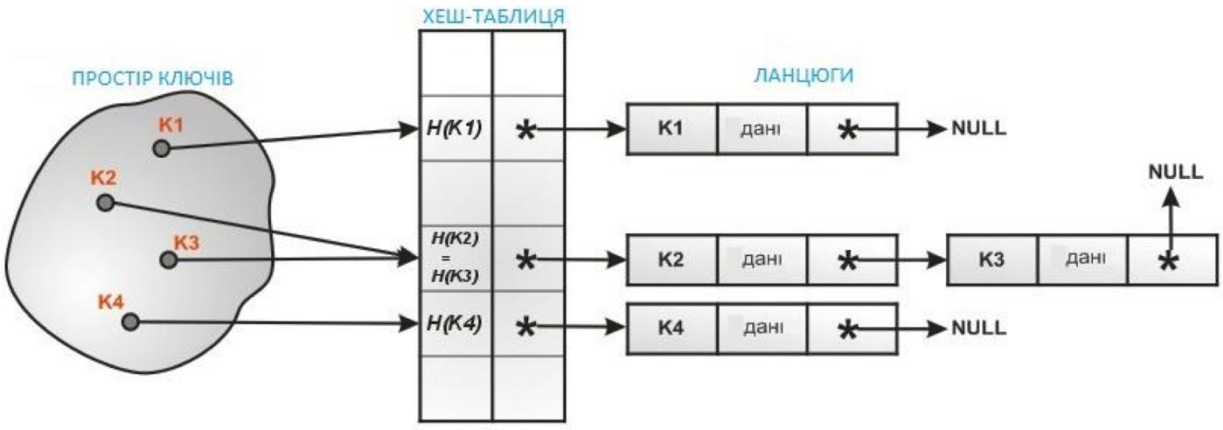

Рис 1.2.3.1 Розв’язання колізій (метод ланцюжків)

У випадку методу з відкритою адресацією (замкнуте хешування) всі елементи зберігаються безпосередньо в хеш-таблиці без використання пов’язаних списків. У хеш- таблицях з замкнутим хешуванням може скластися ситуація, коли вся таблиця буде повністю заповненою так, що неможливо буде додавати нові елементи. Розв’язанням такої проблеми є динамічне збільшення розміру хеш-таблиці з її одночасною зміною структури.

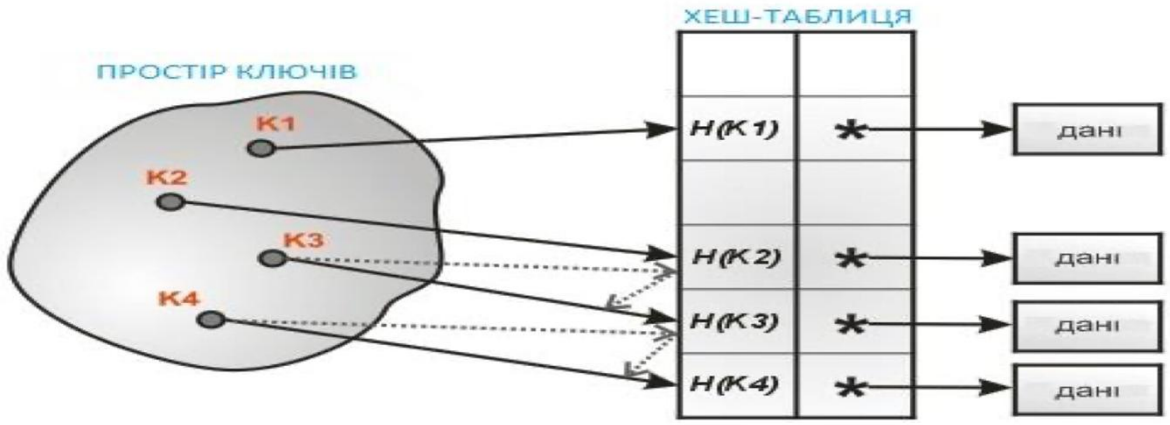

Рис 1.2.3.2 Метод відкритої адресації

1.2.4 Смарт-контракти

Смарт-контракт – це програмний код, який містить інформацію про транзакцію (угода) у форматі «якщо…. тоді…». Наведемо приклад використання на базі блокчейну Ethereum. Якщо користувач А занесе у систему 100 ETH, тоді користувач В відправить 10 токенів N користувачу А. Таким чином, якщо користувачі дотримуються умов контракту, тоді кожен отримає попередньо визначений ресурс. Якщо хтось зі сторін спробує уникнути виконання контракту, тоді угода буде вважатися недійсною, і кожен залишиться при своєму.

Смарт-контракт містить у собі три основні атрибути:

- Цифрові підписи зацікавлених сторін.
- Певний предмет по якому проводиться угода.
- Математично підтверджений опис умов, за яких контракт буде вважатися можливим для виконання.

До переваг смарт-контрактів можна віднести: Перше – Захист від втручання – жодна третя сторона не здатна втрутитися у договір, також це є і фінансовим плюсом, адже не потрібно платити за посередництво. Друге – Безпека – шляхом кодування контракту з високим рівнем, стає майже неможливо його зламати. Третє – Швидкість – обробка документів проходить значно швидше, ніж у реальному житті.

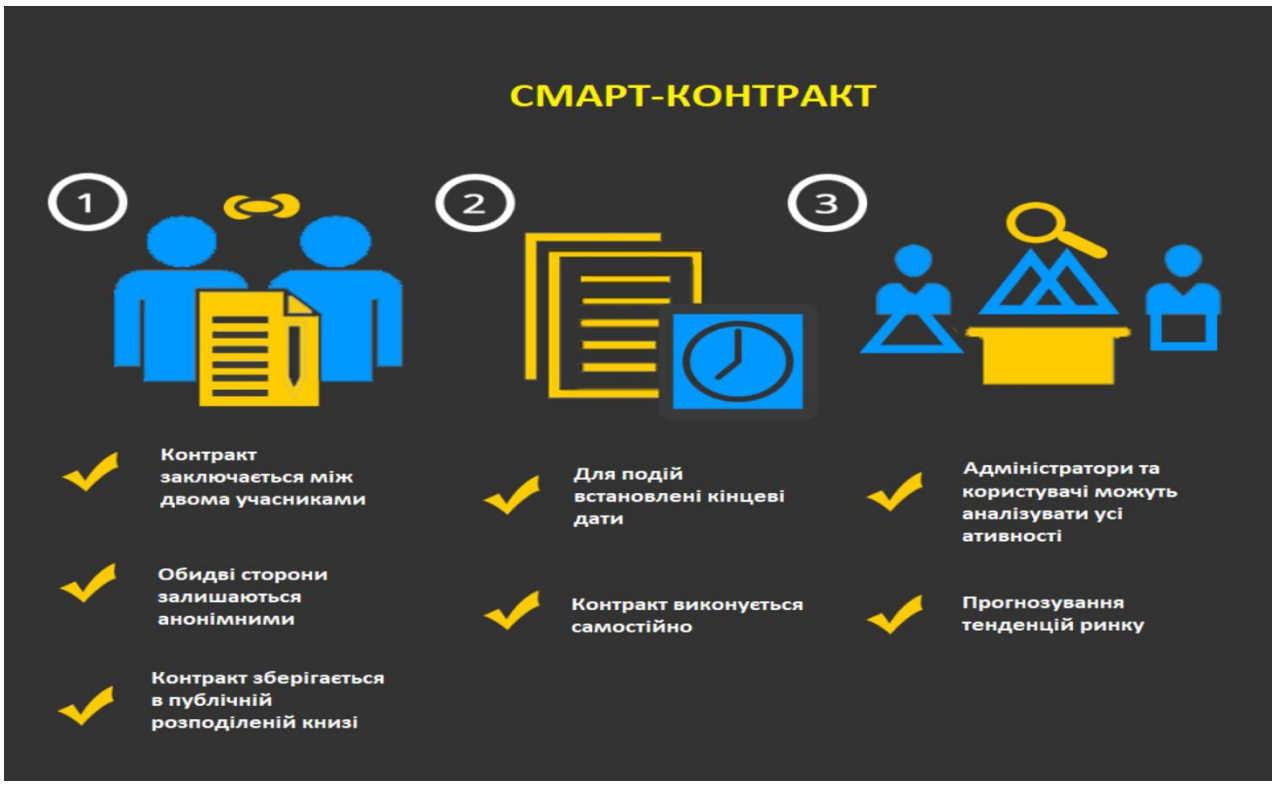

Рис 1.2.4.1 Графічне пояснення сутності смарт-контракту

1.2.5 Алгоритм консенсусу

Враховуючи те, що блокчейн являє собою розподілену систему, тобто в ній відсутні центри прийняття рішень, то їй потрібно ці рішення приймати самостійно. Саме тому були розроблені алгоритми консенсусу, котрі покликані забезпечувати цілісність та безпеку розподілених систем. Алгоритми гарантують достовірність усіх транзакцій, а також забезпечують виконання наявних протоколів, або ж дій та правил котрих потрібно дотримуватися. Нині існують доволі багато різних алгоритмів, проте найбільшу популярність отримали PoW та PoS.

Proof of Work (PoW) – перший алгоритм, який широко використовується в технології Bitcoin а також інших криптовалютах. Основна думка полягає в тому, щоб вузли блокчейн мережі, що підтверджують транзакції, проробляли досить складну обчислювальну роботу (прорахунок алгоритму), результат роботи якого легко та швидко перевірявся іншими вузлами мережі. PoW гарантує, що деякий вузол (майнер) має змогу додавати новостворений блок до блокчейну, якщо інші

вузли досягли консенсусу щодо валідності блоку. Перший вузол, який повністю провів всі необхідні обчислення, отримує винагороду від блокчейн мережі. Всі вузли борються між собою, нарощуючи ємність обчислювальних ресурсів, щоб виявитися тим самим першим вузлом, який отримав винагороду.

Proof of Stake (PoS) – є наслідувачем алгоритму PoW. В даному алгоритмі творцем наступного блоку в ланцюжку блоків вибирається вузол, який має більший баланс — кількість ресурсів, наприклад, монет у криптовалюті. За створення блоку вузол винагороду не отримує. Винагорода виплачується за транзакції. Алгоритм має як переваги так і недоліки. На противагу алгоритму PoW, що PoS потребує суттєво менше споживання електроенергії, проте мотивація концентрувати якомога більше ресурсів або коштів призводить до централізації системи.

1.3 Переваги та недоліки Blockchain

Головна перевага blockchain, втілюється у відсутності третьої сторони в операціях. Одна із сторін ініціює процес передачі даних, який є абсолютно безпечним, в результаті чого створюється блок. Блок проходить перевірку через велику кількість комп’ютерів, що розподілені в мережі. Щойно перевірка завершується такий блок додається в ланцюг, створюючи унікальний запис з унікальними ідентифікаторами. Підробка такого запису призводить до підробки всього ланцюга в мільйонах записах, що є практично неможливим.

В сучасному світі будь-яка паперова угода, може бути сфальсифікована. Blockchain пропонує використовувати електронні договори. В такому разі не потрібні посередники, усе виконується в автономному децентралізованому режимі і саме це забезпечує максимальну прозорість. Учасники такої угоди є анонімними рівноправними користувачами і у разі порушення умов угоди система автоматично анулює її та поверне учасникам їх власні ресурси.

Блокчейн функціонує до тих пір поки є хоча б один комп’ютер, котрий під'єднаний до світової мережі. Усі дані транзакцій зберігаються на різних пристроях, не тільки на одному, - це і є розподільність блокчейну. Таким чином,

подібна система є системою з високим показником стійкості, що не піддається технічним проблемам та різним хакерським атакам. Адже, не існує єдиної точки входу в таку систему.

Один із найвідоміших недоліків технології вважається так звана «атака 51%». Існує гіпотеза, якщо один вузол бере під контроль понад 50% потужності хешування мережі, то це може призвести до порушень роботи в системі. Проте, на даний момент подібна спроба не досягла успіху.

Використання двох ключів шифрування: публічного та приватного, теж несе в собі недоліки. Перший використовується для проведення транзакцій. Приватний потрібен для доступу до ресурсів власника ключа. Але, якщо ключ десь загубіться, це зробить неможливим отримати доступ до коштів і таким чином вони безповоротно втрачаються.

Головним недоліком технології вважають замалу кількість транзакцій за певний час. Якщо взяти за приклад відомі платіжні системи, як Visa та Mastercard, то вони здатні підтримувати до 40 тис. операцій за секунду, відповідно блокчейн може розраховувати лише на у декілька тисяч разів менші об’єми.

1.4 Постановка задачі

Метою даної роботи є розгляд технології blockchain, особливостей його функціонування, огляд основних blockchain-рішень в різноманітних сферах телекомунікаційних систем, а також дослідження основних технологій та засобів впровадження технології blockchain в систему «Розумного будинку»;

Для досягнення мети роботи було поставлено та вирішено такі задачі:

1. Вивчення основних компонентів технології blockchain;
2. Аналіз принципів функціонування blockchain;
3. Розгляд вже існуючих рішень на базі технології blockchain;
4. Розробка варіанту впровадження технології blockchain в систему «Розумного будинку»

Висновки до розділу:

1. Blockchain – технологія, що змінила уявлення про те, як сприймаються бази даних, оформлення та збереження даних. На даний час технологія набирає обертів і у досяжній перспективі здатна створити нові рішення у багатьох галузях, включно із телекомунікаціями, шляхом підвищення прозорості та ефективності процесів у галузі.
2. Загальнодоступність та розподільність надає впевненість у захищеності технології. Подібний підхід разом з використанням надскладних алгоритмів шифрування унеможливлює підробку транзакцій.
3. Blockchain – це універсальна технологія, хоч вона знайшла найбільшої популярності у фінансах (переводи грошових транзакцій), можливості її не вичерпуються цим.

2. ПРИНЦИПИ ТА ФУНКЦІЇ BLOCKCHAIN

Мета розділу – розгляд основних архітектур технології blockchain, опис принципів та особливостей роботи blockchain враховуючи всі переваги та недоліки. Також розділ зосередиться на розгляді P2P мережі та її роль у blockchain. Будуть розглянуті основні властивості blockchain систем.

2.1 Мережа P2P та її роль для blockchain

У галузі інформаційних технологій, однорангова чи пірингова (англ. peer-to-peer) мережа складається з групи взаємозалежних пристроїв (вузлів), які проводять обмін між собою файлами між собою та зберігають один ідентичний набір даних. Усі вузли є рівні, і обмін даними відбувається без центрального сервера, тобто кожен комп’ютер або вузол може виступати і як файловий сервер, і як клієнт. Наприклад, виконуючи роль клієнта, вузол завантажує дані від інших

учасників; і коли він діє як сервер, він може бути джерелом завантаження.

Оскільки кожен вузол зберігає, передає і отримує файли, P2P-мережі мають тенденцію працювати швидше і ефективніше, оскільки їх база користувача збільшується. Окрім того, розподілена архітектура сприяє стійкості подібних систем до різних кібератак. На противагу традиційним моделям, у P2P-мереж відсутня єдина точка відмови.

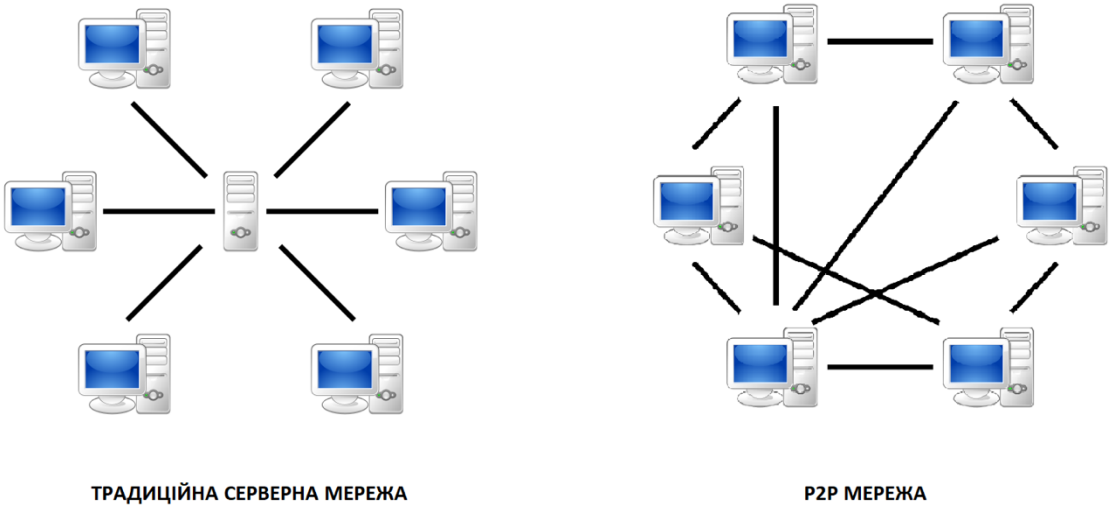

Рис 2.1 Порівняння серверної та однорангової мереж

Ми можемо класифікувати однорангові системи відповідно до їхньої архітектури. Існує три основні види: неструктурована, структурована та гібридна P2P-мережа.

Неструктуровані мережі є найпростішим типом P2P для налаштування та є більш поширеними. Вузли випадково контактують один з одним, і у зв'язку з цим, подібні системи вважаються стійкими до високої активності текучці вузлів (тобто одні вузли приєднуються до мережі, тоді як інші полишають її). Неструктуровані мережі, попри простоту побудови, можуть вимагати більш високого завантаження центрального процесора та оперативної пам'яті, адже пошукові запити будуть відправлятися максимально можливій кількості вузлів. Подібна архітектура може бути здатною переповнювати мережу запитами, за умови якщо деякі вузли пропонують бажану інформацію.

Структуровані мережі P2P організовані таким чином, що кожен вузол може шукати та знаходити ресурси, навіть у випадку, коли ці дані не є широкодоступними. У більшості випадків використовуються хеш-функції, які полегшують пошук бази даних. У той момент як структуровані мережі володіють високою працездатністю та продуктивністю, вони як правило, є більш централізовані і вимогливими з точки зору встановлення та обслуговування. За умови тимчасового випадання великої групи вузлів, робота всієї системи порушується.

Гібридні моделі P2P поєднують традиційні моделі клієнт/сервер і однорангові моделі. Як правило, гібридна модель складається з центрального сервера, який забезпечує централізовану структуровану функціональність сервера/клієнта, наприклад, допомагає вузлам знаходити один одного, а також децентралізовану агрегацію, яка забезпечується рівністю вузлів чистої, неструктурованої однорангової мережі. У порівнянні з двома іншими видами, гібридні моделі, як правило, демонструють більш високу загальну продуктивність. Вони зазвичай поєднують у собі деякі з основних переваг кожного з підходів і завдяки цьому досягають високого рівня ефективності та децентралізації одночасно.

Таким чином, у мережі біткоїн відсутні банки, що займаються обробкою чи реєстрацією всіх транзакцій. Замість цього, блокчейн працює як цифровий регістр, який публічно фіксує всю активність. На практиці кожен вузол зберігає копію блокчейна і порівнює її з копіями інших вузлів, щоб переконатися в точності даних. Таким чином, мережа швидко реагує на усі шкідливі дії чи неточності. Попри те, що мережа однорангова, різні вузли здатні виконувати різні функції. Наприклад, так звані «повні ноди» існують для виконання основного завдання – перевірка транзакцій у системі з приводу відповідності алгоритмам консенсусу, що діють у системі. Також є й інші вузли – майнери, основним завданням котрих – створення нового блоку збереження інформації.

Попри численні переваги, однорангові мережі також мають певні недоліки. Оскільки розподілені регістри повинні оновлюватися на кожному вузлі, а не на

центральному сервері, додавання транзакцій у блокчейн потребує великої кількості обчислювальних ресурсів. Хоча це і забезпечує підвищену безпеку, у свою чергу значно знижується оперативність роботи, що є однією з основних перешкод, коли йдеться про масштабованість та широкомасштабну адаптацію. Тим не менш, криптографи та блокчейн-розробники вивчають альтернативні варіанти, які можуть бути використані як рішення для збільшення масштабованості.

2.2. Класифікація blockchain мереж

По суті блокчейн є розподіленою базою, у якій запис всіх змін здійснюється як ланцюжок блоків. При цьому сама структура блокчейна передбачає різні рівні доступу до інформації. Цей параметр використовується як критерій для класифікації блокчейнів, яка має умовний характер, оскільки принцип технології блокчейн є при цьому єдиним. Існує три основних типи blockchain: публічний, приватний та гібридний.

Публічний блокчейн - це ланцюжок блоків, який може "прочитати" будь-яка людина у світі. Також будь-яка людина може відправляти транзакції, очікувати їх включення, якщо вони дійсні, і брати участь у процесі консенсусу (процес для визначення, які блоки додаються в ланцюжок і який стан мережі). Попри публічність блокчейну – він не є менш захищеним. Тут так само ніхто не може отримати доступ до інформації про користувачів, є лише доступ до публічного рахунку, дати чи суми транзакції.

На додачу, ще вагомою перевагою публічного блокчейну, попри надійність і безпеку є його відкритість і прозорість. Копія записів цифрової «книги» міститься на кожному авторизованому вузлі, що робить цю систему відкритою і прозорою таким чином це запобігає шахрайству. Оскільки, суттєва кількість вузлів спостерігає за тими чи іншими операціями.

Головним недоліком такої архітектури є низький показник транзакцій за секунду (TPS). Оскільки мережа має у складі велику кількість вузлів, кожен вузол проводить операцію перевірки транзакції, яка забирає доволі багато часу.

Приватний блокчейн – це блокчейн, що характеризується обмеженим рівнем доступу до даних. Підтвердження транзакцій у таких мережах, проведення аудиту, управління базами керується чітко визначеним колом осіб. Якщо говорити про право на читання даних, воно може бути як загальнодоступним, так і повністю обмеженим. Подібна мережа дозволяє змінювати записи в регістрі, що є головною відмінністю систем з публічним блокчейном, де дані не можуть бути змінені чи видалені. Приватний блокчейн знайшов своє місце у допомозі підприємствам, а саме коли необхідно підвищити ефективність без надання публічного доступу до своїх транзакцій.

Головною перевагою систем з приватним блокчейном у порівнянні з публічним є швидкість транзакцій за секунду, адже мережа має обмежену кількість вузлів. Це загалом прискорює консенсус та процес перевірки транзакцій і така система здатна обробляти транзакції зі швидкістю до декількох тисяч одночасно.

Нижча безпека є найбільшим недоліком приватного блокчейну. Враховуючи, що система має обмежену кількість вузлів, які підпадають під регулювання певного центрального органу, то у випадку, якщо якийсь вузол отримає доступ до центральної системи,- він може мати доступ до усієї мережі.

Гібридний блокчейн – це поєднання централізованої та децентралізованої системи, що надає дозвіл керувати загальною кількістю користувачів, які здатні перевіряти транзакції. Мережа керується певними вузлами, які заздалегідь обираються. Подібно приватним системам, у випадку хакерської атаки, подібна мережа має єдину точку відмови, проте у таких блокчейн системах використовується підвищена ступінь криптографії з метою збільшення безпеки аудиту. Контроль відбувається не єдиним центральним органом, а декількома затвердженими користувачами.

2.3. Структура та принципи функціонування блокчейн

Принцип функціонування технології Blockchain, для прикладу, розглянемо на базі криптовалюти Bitcoin. Криптовалюта Bitcoin використовує криптографічну

хеш-функцію SHA-256. Деревоподібне хешування (дерево Меркле) уособлює особливу структуру даних, яка зберігає інформацію про завершені транзакції. Це «дерево» необхідне для перевірки даних та їх цілісності у блоці. Щоб цього досягти, з кожної транзакції необхідно обчислити хеш, а вже потім з кожної пари хешів обчислити нові хеш пари. Процес триває доти, поки не залишиться лише один хеш.

Групу транзакцій після перевірки записують у спеціальний блок (рис. 2.3.1). Блок має у складі заголовок та список транзакцій (Tr A, Tr B, ...). Заголовок блоку включає: хеш минулого блоку (Previous Hash), хеш транзакцій (Merkle Root), деяку додаткову інформацію (Nonce, Timestamp) і наостанок загальний хеш даного блоку. Timestamp (часова помітка) вказує, коли блок був створенний, і надає докази того, що дані блоцу існували в певний момент часу. Nonce – одноразовий код вибраний псевдовипадковим чином.

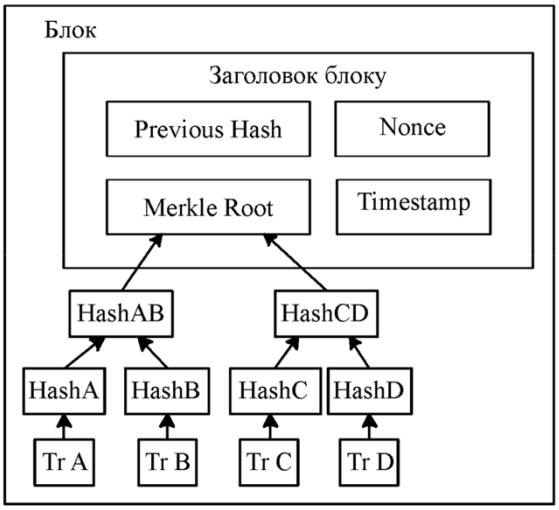

Рис. 2.3.1 Структура блоку

Щоб підтвердити коректність блоку, необхідно обчислити хеш заголовку нового блоку, який має починатися із заданої заздалегідь кількості нулів. Ця задача більш відома, як доказ правильності роботи (proof-of-work), що базується на декількох принципах: 1) підтвердження транзакцій необхідно зробити затратними для користувачів мережі шляхом комп'ютерних обчислень; 2) надати деяку винагороду за поміч у перевірці транзакцій.

Сенс задачі "доказ правильності роботи" полягає в тому, щоб знайти таке

число x, яке додавши до повідомлення (набір транзакцій) S, забезпечить результат хешування. Складність же задачі залежить від певної кількості нулів на початку значення хеш-функції. Розглянемо на прикладі складність задачі. Позначимо через h – фіксовану хеш-функцію, S – черга незавершених транзакцій. Нехай S = "Internet of Things", одноразовий код x = 47304. Обчислюємо хеш-функцію із комбінації ("Internet of Things 47304"):

Якщо x=47304, початок хеш-функції складається з чотирьох нулів:
h = sha256 ("Internet of Things 47304").
h= '0000c75f1b2ba0cbc69068dee203907dd4b5ae6fe12aed0261052d25036d174a'.

Новий блок сприймається усіма вузлами мережі, тільки у випадку, коли хеш заголовку дорівнює або ж є меншим від заданого числа. Необхідно додати, що величина цього числа періодично змінюється. Коли знайдено результат, готовий блок починає розсилатися всім іншим вузлам, на перевірку. Якщо перевірка успішна - блок додають в ланцюжок і наступний блок вже повинен включати в себе хеш новоствореного блоку.

Ланцюг блоків – є базою транзакцій, яка обробляється всіма учасниками мережі. Повна копія такого ланцюга містить абсолютно усі транзакції, які були здійснені в системі. Від кожного блоку в ланцюгу є лише один шлях до нульового блоку.

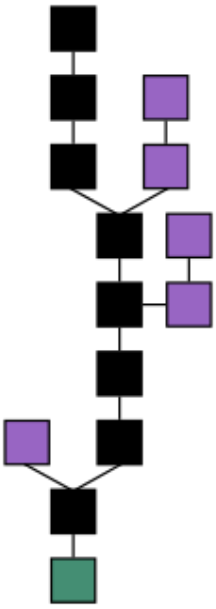

Рис. 2.3.2. Основна послідовність блоків (чорний ланцюг є найдовшою гілкою від нульового блоку)

Робота, яку необхідно виконати вузлам з метою створення нового блоку, потребує багато часу та обчислювальних потужностей. Таким чином знижується ймовірність того, що два блоки будуть одночасно винайдені, проте така ситуація не є винятковою. Коли подібне відбувається, то створюється розгалуження в Blockchain. За таких обставин вузли почнуть будувати ланцюг на двох різних гілках. Кожна гілка рівноправна до тих пір, поки одна з них не стане коротшою за іншу. Задля запобігання такої ситуації, кожен вузол має відстежувати всі гілки, проте вузли намагатимуться працювати над розширенням тільки найдовшої гілки. Транзакції, які увійшли в коротшу гілку – втрачають статус підтверджених. Такі зайві операції не отримують підтвердження і втрачаються.

Варто наголосити, що довжину визначають не кількістю блоків, а загальним обсягом роботи, яка затрачена на створення гілки, і визначається кількістю нулів на початку хешу блоку.

Мережа блокчейна складається з «повних вузлів». Їх можна представити у вигляді комп’ютерів, на яких виконуються програми, алгоритм яких забезпечує

захист усієї системи. Кожен вузол містить у собі копію всіх операцій (транзакцій), які коли-небудь були записані в ланцюг блокчейну.

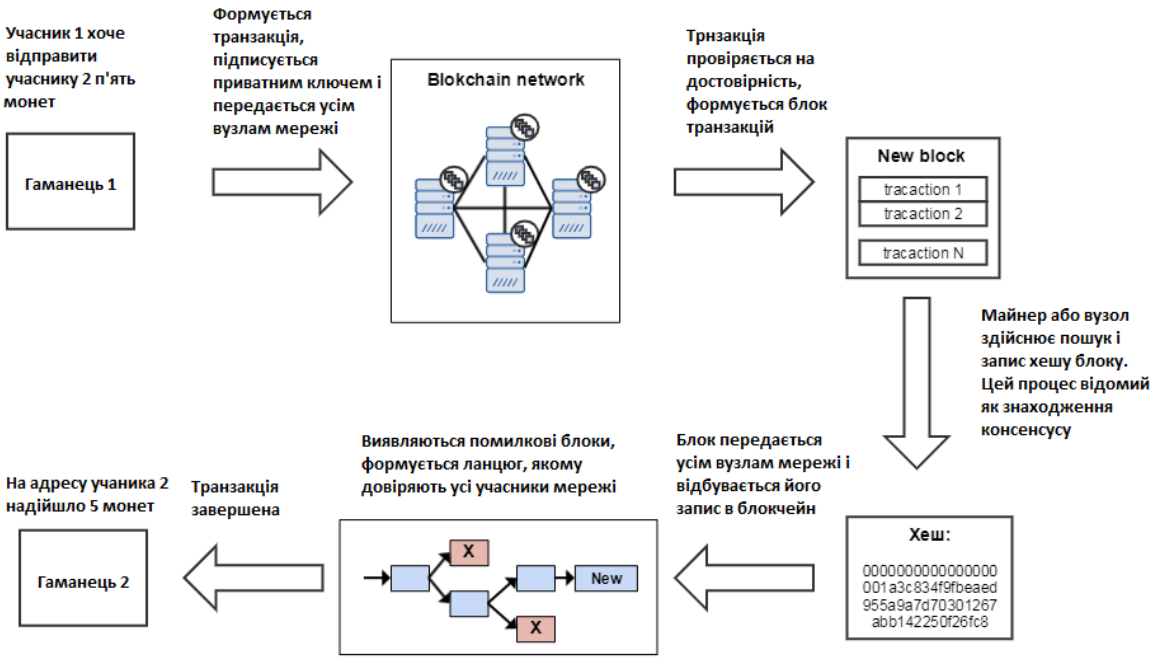

Рис. 2.3.3. Принцип роботи блокчейн мережі

2.4. Властивості технології blockchain

Незмінність - будь-які записи, зроблені в блокчейні, не можна змінювати або видаляти. Хеш-функція гарантує незмінність блокчейн-ланцюга. Вона використовує вхідний рядок необмеженої довжини та здійснює перетворення його у рядок фіксованої довжини. В контексті криптовалюти Bitcoin використовується алгоритм хешування SHA-256.

Децентралізація - інформація про всі транзакції знаходиться у всіх користувачів і транзакції мають підтверджуватися незалежними вузлами, отже подібну систему неможливо змінити. Децентралізоване управління можна побачити на прикладі криптовалютних біржах. Подібні біржі впроваджують технології блокчейн і зосереджують кошти користувача в його управлінні. Децентралізовані електронні валюти повністю закріплені саме за їх власником і тільки він може здійснювати транзакції та отримувати доступ до свого сховища. Децентралізована криптовалюта Bitcoin – є першопрохідцем та наразі найпопулярніша електронна валюта у світі. В блокчейні Bitcoin відслідковується

вся історія платежів, проте учасники мережі зберігають анонімними. Сьогодні триває подальше вдосконалення цієї технології.

Анонімність - кожен учасник мережі Blockchain має згенеровану адресу, а не ідентифікаційний номер користувача. Таким чином зберігається анонімність для користувачів, особливо зважаючи на загальнодоступність структури blockchain

Прозорість - систему blockchain неможливо пошкодити. В цій технології особистість людини представлена у вигляді публічного криптографічного ключа. Тобто, якщо досліджувати історію транзакцій, то ви не побачите імена, а лише, що «21Mf82gf023Kf92dfasfk291kdds822ksdf2FJK5l відправив 3 Bitcoin». Таким чином, можна дослідити усі транзакції, які були зроблені за цією адресою, однак, не можна отримати інформацію про особистість. Загалом технологія корисна, коли потрібно дослідити весь рух фінансів.

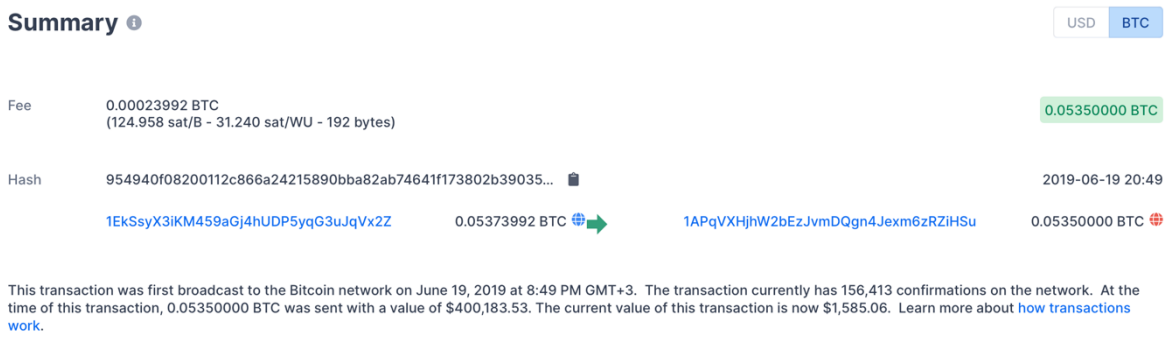

Рис. 2.4.1. Приклад транзакції Bitcoin

На рис. 2.4.1 зображено приклад транзакції в мережі Bitcoin. Дані хеш операції, публічні адреси відправника та отримувача, сума транзакції, час та дата, статус операції (підтверджена), та винагорода майнеру за цю операцію (0.00023992 BTC). Сума транзакції на момент її здійснення дорівнює 1,587.56$, а винагорода майнеру становить 7.12$.

Висновки до другого розділу

1. Блокчейн – децентралізована технологія, в основі якої лежить мережа P2P. Мережа складається з багатьох комп’ютерів, котрі займаються перевіркою

транзакціій та роблять потенційну фальсифікацію неможливою.

2. В ході цього розділу було досліджено основні архітектури технології blockchain з переліком їх переваг та недоліків. Було розглянуто основні компоненти блокчейн-системи.
3. Блокчейн є технологією, яка не піддається змінам і є цілком прозорою.

3. МОЖЛИВОСТІ ЗАСТОСУВАННЯ BLOCKCHAIN У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Метою даного розділу є опис застосування технології blockchain та дослідження можливості застосування технології у різних телекомунікаційних системах. В рамках цього розділу розглянемо технологічні рішення на базі blockchain та ознайомимося з реалізацією архітектури “Розумного будинку” з використанням технології blockchain.

3.1 Телекомунікації та blockchain

Телекомунікації – це неймовірно складна галузь, яка вимагає величезної фізичної інфраструктури, складних мереж з багатьма учасниками, складних систем виставлення рахунків, роумінгових угод та інших аспектів. Телекомунікаційний ланцюжок створення вартості складається із забезпечення необхідної мережевої інфраструктури та підключення для передачі голосу, даних, мультимедіа та інших супутніх послуг. Обмін даними відбувається між мережами, що вимагає захисту, цілісності та перевірки даних та запобігання шахрайству.

Технологія Blockchain пропонує телекомунікаційній галузі ідеальне рішення для однієї з основних вимог. Завдяки надійному безпечному доступу до даних блокчейн вже використовується в багатьох додатках у телекомунікаційній галузі. Можливість зберігати історичні записи користувачів без можливості втручання в ці записи дозволяє контролювати різні аспекти облікових записів користувачів. Деякі блокчейн-додатки в телекомунікаційній галузі включають автоматизацію багатьох внутрішніх операцій, таких як системи виставлення рахунків, роумінг та управління ланцюгами поставок.

Автоматизація білінгових систем за допомогою смарт-контрактів, що надаються за допомогою технології блокчейн, економить компанії багато часу та грошей та запобігає будь-якій можливості шахрайства. Як результат, весь процес бухгалтерського обліку та аудиту буде автоматизований, що дозволить заощадити телекомунікаційним компаніям більше грошей.

Низька вартість використання блокчейн для дешевих платежів може дозволити телекомунікаційним компаніям надавати мікроплатежі, які зазвичай використовуються для купівлі мобільних онлайн ігор, музики тощо. У результаті розгортання цієї послуги стороннім додаткам не потрібно надавати реквізити банківського рахунку, дані кредитної картки чи будь-яку іншу конфіденційну чи конфіденційну інформацію.

3.2. Блокчейн-рішення від IBM для роумінгу

Компанія IBM розробила рішення для роумінгу на базі технології blockchain з відкритим кодом. Розробка покликана забезпечити координацію та виконання смарт-контрактів між мобільними операторами. Смарт-контракти надають можливість визначати правила та процеси й контролювати транзакції між сторонами, таким чином контракти допомагають підвищити ефективність роботи клієнтів та спростити вирішення суперечливих бізнес питань.

Постачальники послуг зв’язку (CSP) часто стикаються з проблемами, пов’язаними з абонентами в роумінгових мережах CSP, і вони не завжди чітко бачать діяльність своїх абонентів у цих мережах. Звірка платежів для клієнтів у

роумінгу займає час і вимагає посередництва сторонніх розрахункових центрів із відповідними витратами.

Виявлення та запобігання шахрайству продовжують залишатися актуальними проблемами для більшості CSP, які коштують понад 38 мільярдів доларів на рік. Шахраї можуть отримати доступ до домашньої мережі CSP під час клонування особи роумінгового абонента. Blockchain об'єднує ці CSP в єдину мережу, що забезпечує прямий обмін інформацією з незмінними транзакціями, які виконуються на основі консенсусної моделі, яка використовує правила смарт-контрактів. Це покращує видимість CSP для платника, забезпечує швидку звірку платежів та зменшує кількість шахрайських транзакцій.

Ця бізнес-модель включає:

– SubscriberSims, які представляють єдиний міжнародний каталожний номер мобільної станції (MSISDN). Іншими словами, кожен SubscriberSim представляє собою номер мобільного телефону.
– Постачальники послуг зв'язку, які діють або як домашній оператор, або як роумінг-партнер SubscriberSim.

Рис. 3.2.1 Бізнес-модель використання blockchain компанії IBM

Таке рішення передбачає чотири сценарії використання:

- **Ідентифікація абонента в роумінгу** – SubscriberSim переміщується в нове місце, яке не є частиною його домашньої мережі. Якщо виявлено, що абонент присутній у мережі роумінгового партнера за допомогою функції виявлення, аутентифікований як дійсний користувач за допомогою функції аутентифікації, то його тарифи оновлюються використовуючи функцію updateRate.
- **Рахунки абонента в роумінгу**. Після авторизації SubscriberSim він може використовувати мережу роумінгового партнера для ініціалізації дзвінка. Функції callOut і callEnd можна використовувати для ініціалізації та завершення виклику. Плата за використання мережі миттєво записується між домашнім оператором і роумінг-партнером на основі їхньої угоди, яка визначена в смарт-контракті. Функція callPay виконується для розрахунку вартості дзвінка.
- **Ідентифікація шахрайства** – додається шахрайський SubscriberSim (з тим же MSISDN, що й існуючий SubscriberSim). Функція аутентифікації ідентифікує користувача як шахрайського та позначає SubscriberSim як isValid = Fraud у книзі. Це запобігає шахрайському SubscriberSim від ініціювання будь-яких дзвінків.
- **Управління надлишком** — абонент у роумінгу ініціює виклик, і виконується функція callOut. Розумний контракт визначає, що абонент потенційно досягає межі ресурсів, які були виділені йому згідно тарифу. Оператор сповіщає абонента про досягнення межі та вказує можливі зміни тарифу. Абонента просять прийняти або відхилити нові платежі, відповідь абонента записується в книгу, а майбутні дзвінки (включаючи цей) ініціюються або відхиляються залежно від того, прийняв або відхилив абонент плату за перевищення. Якщо абонент у роумінгу прийняв тарифи, для всіх майбутніх дзвінків (включаючи цей) буде використовуватися OverageRate для розрахунку вартості дзвінків замість тарифу роумінгу.

Переваги blockchain-рішення від IBM:

- Автоматичне запуск контракту між домашнім оператором і роумінг-партнерами, автоматично примусове виконання контрактів.
- Майже миттєва обробка платежів, виключаючи дорогі сторонні процеси, як-от розрахункові палати.
- Ефективне керування ідентифікаційними даними через CSP для запобігання шахрайству в роумінгу та підписках.
- Попередження в режимі реального часу про проблеми з перевищенням даних.

3.3 Управління та підтвердження цифрової ідентифікації

Перевірка посвідчення особи щорічно коштує корпораціям і урядам сотні мільярдів доларів. Наразі такі стартапи, як Civic, розробляють нові системи перевірки ідентичності на основі блокчейну. Телекомунікаційні компанії працюють з величезними обсягами даних клієнтів, їм вигідно виступати в якості джерела аутентифікації. Компанії можуть розробляти нові системи, більш прозорі, безпечні та зручні як для клієнтів, так і для бізнесу, щоб отримувати додаткові джерела доходу.

Оператори можуть надати своїм абонентам вбудовану SIM-карту (eSIM) або програму, яка створює унікальні віртуальні ідентифікатори для кожного абонента, які шифруються та зберігаються в Blockchain. Система управління ідентифікацією блокчейн дозволить користувачам керувати своїми ідентифікаторами в різних програмах, пристроях і організаціях за допомогою лише одного пароля. Кожен абонент отримує головний ключ, за допомогою якого він зможе підтвердити свою особу в будь-якій цифровій присутності.

Підписники можуть використовувати цю особистість для автоматичної автентифікації під час відвідування веб-сайтів електронної комерції, охоронних будівель, розумних транспортних засобів, квитків на літак тощо, а також для

перевірки особистих документів, таких як паспорти, водійські права, свідоцтва про народження та шлюб, а також освітні градуси. Наприклад, віртуальний ідентифікатор, що зберігається в блокчейні за допомогою програми оператора, може використовуватися абонентом для входу в Facebook або Google на мобільному пристрої. Перевага такої послуги полягає в тому, що абоненту не потрібно надавати свої особисті дані різним постачальникам послуг для створення нових облікових записів і складних паролів. Віртуальний ідентифікатор, що зберігається через додаток оператора, може надаватися численним партнерським веб-сайтам, постачальникам комунальних послуг і додаткам як унікальний ідентифікатор. Людям буде набагато легше пробувати нові послуги, якщо їм не доведеться підписуватися з нуля – найкращим прикладом цього є вхід за допомогою свого облікового запису Google/Facebook.

Це може стати чудовою можливістю для телекомунікаційних організацій розвивати та поширювати свій бізнес-сегмент. На даний момент такий проект управління ID вже розгортається в Європі. Проект ID2020 має намір надати 1,1 мільярда людей безпечну та надійну систему управління ідентифікацією в найближчому майбутньому.

3.4 Використання blockchain для 5G включення

Попит на послуги зв'язку зростає, і незабаром світ перейде на мережу 5G, яка буде в десять разів швидша за 4G, матиме набагато менші затримки та більшу пропускну здатність, але управління такою складною мережею потребуватиме більшої обчислювальної потужності та ємність зберігання.

5G – це ще одна технологія, яка може отримати вигоду від блокчейна. 5G обіцяє поширений доступ до різних мереж, і телекомунікаційним компаніям доведеться мати справу з універсальними вузлами доступу та різноманітними механізмами доступу. Вибір вузла для найшвидшого доступу для всіх користувачів незабаром стане головною проблемою для телекомунікаційних компаній. Блокчейн має потенціал, щоб увімкнути такі механізми вибору доступу.

Сьогодні комунікаційні системи централізовані в моделі клієнт-сервер, де

правила, що зберігаються на сервері, передаються клієнту. Це спричиняє затримки та не дозволяє безперебійно забезпечувати пристрій мережею. Крім того, надання правил не є процесом у реальному часі, а це означає, що їх не можна змінювати.

3GPP (LTE, GPRS) і мережі доступу, які не є 3GPP (WiMax, WLAN, WiFi) у певній зоні можуть бути об'єднані в мережу через блокчейн, де кожна точка доступу (маршрутизатор Wi-Fi, вежа стільникового зв'язку тощо) може служити вузлом у мережі, що контролює пристрої. Правила та угоди між різними мережами, що надають доступ, можуть бути закодовані як смарт-контракти. Ці контракти можуть мати динамічний характер, якщо потрібно коли-небудь змінити політику, потрібно змінити лише код договору.

Коли пристрій передає свою особу, він приймається в мережу відповідною коміркою CSP (постачальник послуг зв'язку). Після того, як пристрій передає своє місцезнаходження, вузол доступу, який найкраще може надати послугу пристрою, спрацьовує. Це також дозволяє безперебійно оцінювати та оплачувати всі послуги між різними вузлами доступу. Якщо, наприклад, WLAN з офісної або домашньої мережі надала доступ до пристрою, то CSP може, ймовірно, зменшити суму рахунка відповідно до рахунка компанії, що здійснює розміщення, або будинку. Служби на основі місцезнаходження також можна ввімкнути, якщо ви є частиною цієї мережі блокчейнів і, отже, завжди знаєте, які пристрої знаходяться поблизу.

Blockchain забезпечує підвищення ефективності обміну даними в мережі 5G, є прозорим, незмінюваним та стійким до зовнішнього впливу. Децентралізована архітектура отримує оброблені запити клієнтів через розподілені вузли, таким чином значно зменшуються будь-які затримки. Архітектура подібного рішення називається мета-ключем, де ці ключи зберігаються в децентралізованому сховищі у вигляді метаданих, захищених приватним ключем.

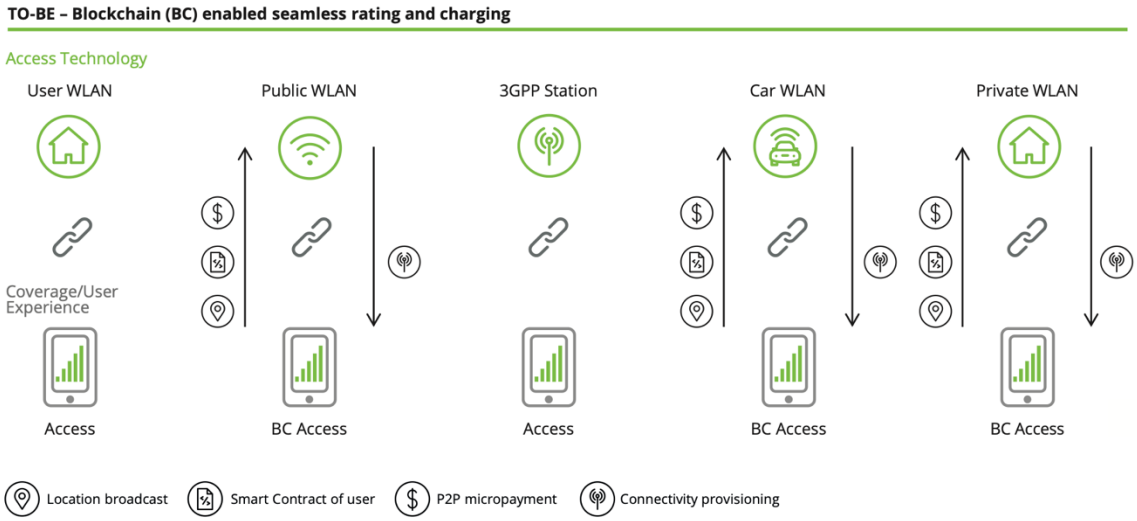

Рис. 3.4.1 Використання blockhain сумісно з 5G

3.5 Використання blockchain для IoT

До наступного десятиліття кількість стільникових з’єднань IoT досягне мільярдів. Головна проблема полягає в тому, що зростання Інтернету речей і зростання незахищеності даних прямо пропорційні. Підключення до Інтернету речей створює серйозні проблеми, як-от необхідність захисту мільярдів взаємодій між машинами та датчиками, а також необхідність захисту конфіденційної інформації, яка збирається та передається через пристрої. Як наслідок, вимоги щодо безпеки даних та мережі можуть стати дорогими, оскільки ці мережі IoT продовжують зростати.

Децентралізований контроль на основі блокчейну дозволяє зробити безпеку Інтернету речей більш масштабованою, а безпечна верифікація та валідація не дозволять шахрайському пристрою втручатися в домашню або заводську систему, надаючи неправдиву інформацію.

Blockchain може створювати високозахищені однорангові самокеровані сітчасті мережі, які використовують велику кількість вузлів. Ці вузли можуть бути представлені датчиками IoT з можливістю перевірки кожного блоку, який змінюється в блокчейні. Такі мережі можуть бути введені в приватне середовище на базі веж стільникового зв'язку. Постачальники комунікаційних послуг могли б

забезпечити безпеку приватних/відкритих ключів і широке підключення, щоб забезпечити таку мережу блокчейну з глобальним охопленням.

Наступні характерні особливості ВС роблять його привабливою технологією для вирішення вищезгаданих проблем безпеки та конфіденційності в IoT:

- Децентралізація: відсутність центрального контролю забезпечує масштабованість та надійність за рахунок використання ресурсів усіх вузлів-учасників та виключення потоків трафіку багато-в-одному, що, у свою чергу, зменшує затримку та долає проблему єдиної точки збою.
- Анонімність: притаманна анонімність добре підходить для більшості випадків використання Інтернету речей, коли особистість користувачів має бути конфіденційною.
- Безпека: ВС реалізує захищену мережу через ненадійні сторони, що є бажаним для IoT з численними і гетерогенними пристроями.

Однак впровадження ВС в IoT не є простим і вимагає вирішення наступних критичних проблем:

- Майнінг є особливо інтенсивним з точки зору обчислень, тоді як більшість пристроїв IoT мають обмежені ресурси.
- Майнінг блоків займає багато часу, тоді як у більшості додатків IoT бажана низька затримка.
- ВС погано масштабується, оскільки кількість вузлів у мережі збільшується. Очікується, що мережі IoT міститимуть велику кількість вузлів.
- Базові протоколи ВС створюють значний накладний трафік, що може бути небажаним для деяких пристроїв IoT з обмеженою пропускною здатністю.

3.6 Розумний будинок на базі технології Blockchain

Сьогодні більшість існуючих великомасштабних промислових IoT-інфраструктур розробляються, розгортаються і обслуговуються окремими сторонами. Як правило, вони засновані на clouds і на моделях централізованого зв'язку, у яких всі пристрої ідентифікуються, проходять перевірку автентичності і підключаються через хмарні сервери, які забезпечують великі можливості

обчислень та зберігання. В той час, як відбувається швидке зростання розмірів та складності IoT мережі, централізовані рішення IoT, через високу вартість розгортання і обслуговування стають все більш дорогими, пов'язаної з мережевою та хмарною інфраструктурою. У традиційних мережах IoT дані, які забезпечуються деякими промисловими організаціями, можуть бути скомплементовані або змінені зловмисниками або власником даних, таким чином вони ненадійні. Необхідно мати процедури для перевірки на достовірність даних в мережах IoT. Враховуючи ці вимоги до мереж IoT, технологія blockchain може служити потенційним кандидатом на надання даних послуг.

Безпека та конфіденційність Інтернету речей (IoT) залишаються серйозною проблемою, в основному через масовий масштаб і розподілену природу мереж IoT. Підходи, засновані на блокчейні, забезпечують децентралізовану безпеку та конфіденційність, але впровадження BC в контексті IoT не є простим і тягне за собою кілька значних проблем, таких як: високий попит на ресурси для вирішення POW, велика затримка для підтвердження транзакцій і низька масштабованість. Запропонована схема спирається на ієрархічну структуру та розподілену довіру для підтримки безпеки та конфіденційності Blockchain, водночас роблячи її більш придатною для конкретних вимог IoT. Ідея представлена в вигляді розумного будинку.

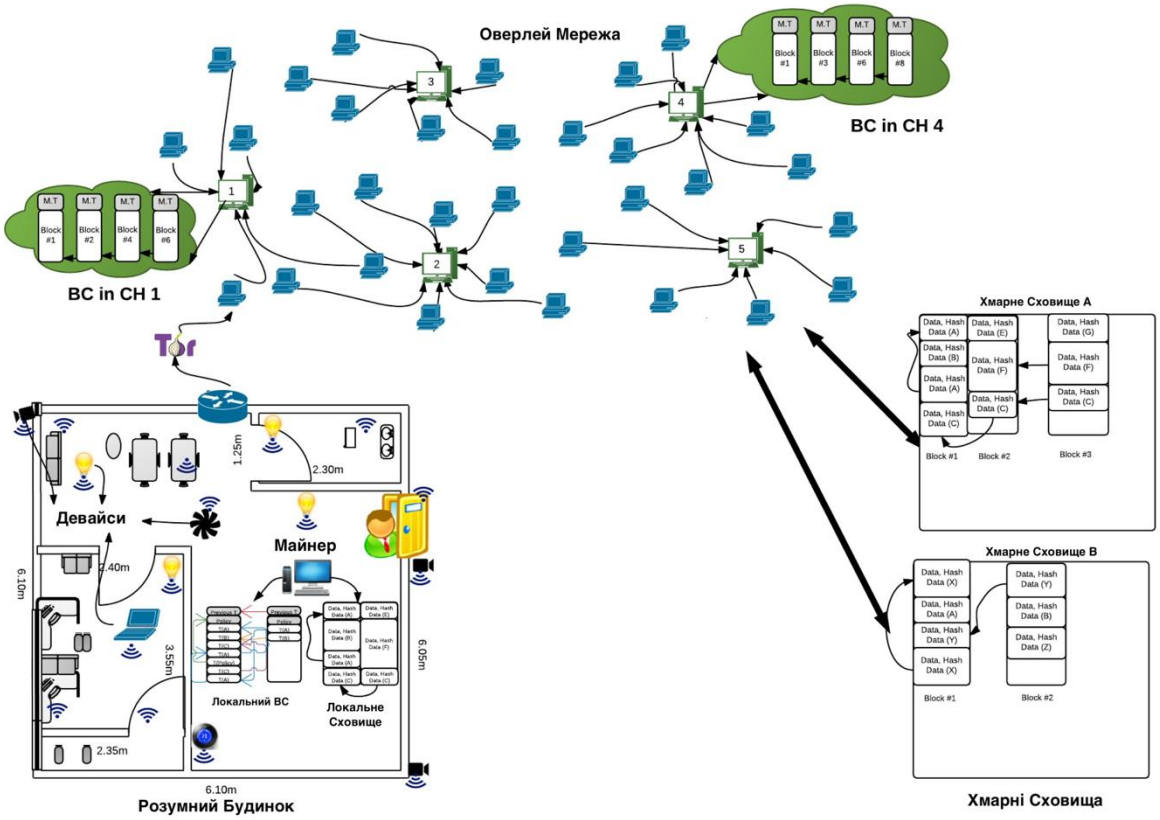

Рис 3.6 Загальний вигляд архітектури на базі Blockchain

3.6.1 Основні компоненти

Архітектура складається з трьох основних рівнів: розумний дім, хмарне сховище та оверлей. Смарт пристрої розташовані всередині рівня розумного будинку і централізовано керуються Майнером. Розумні будинки утворюють оверлейну мережу разом з постачальниками послуг (ПП), хмарними сховищами і смартфонами або персональними комп'ютерами користувачів.

Оверлей мережа схожа на однорангову мережу в Bitcoin і привносить розподілену функцію в архітектуру. Щоб зменшити накладні витрати та затримку мережі, вузли в мережі оверлей групуються в кластери, і кожен кластер обирає кластера-керівника (CH). Кластери-керівники підтримують загальнодоступний BC у поєднанні з двома списками ключів. Такими списками ключів є: списки ключів запитувача, тобто список оверлей PK (публічний ключ) користувачів, яким дозволено доступ до даних розумних будинків, підключених до цього кластера; списки запитуваних ключів – це список PK (публічних ключів)

розумних будинків, підключених до цього кластера, до яких дозволений доступ. Хмарне сховище необхідне пристроям розумного будинку для зберігання та обміну даними.

3.6.2 Компоненти Розумного Будинку

Транзакції. Зв'язок між локальними пристроями або вузлами оверлей відомі як транзакції. У розумному будинку на базі Blockchain існують різні транзакції, кожна з яких призначена для певної функції. Транзакції зберігання генеруються пристроями для зберігання даних. Транзакція доступу генерується SP (постачальник послуг) або власником будинку для доступу до хмарного сховища. Транзакція моніторингу генерується власником будинку або постачальниками послуг для періодичного моніторингу інформації про пристрої. Додавання нового пристрою до розумного будинку здійснюється за допомогою транзакції Genesis, а пристрій видаляється за допомогою транзакції видалення. Усі транзакції до або з розумного будинку зберігаються в локальному приватному Blockchain.

Локальний Blockchain. У кожному розумному будинку є локальний приватний блокчейн, який відстежує транзакції та має заголовок політики, щоб забезпечити дотримання політики користувачів щодо вхідних та вихідних транзакцій. Починаючи з транзакції Genesis, транзакції кожного пристрою з’єднуються разом як незмінна книга в блокчейн. Кожен блок у локальному блокчейн містить два заголовки, які є заголовком блоку та заголовком політики. Заголовок блоку містить хеш попереднього блоку, з метою зберегти блокчейн незмінним. Заголовок політики використовується для авторизації пристроїв і застосування політики контролю власника над його будинком. Заголовок політики має чотири параметри. Параметр ”Requester” відноситься до публічного ключа запитувача в отриманій оверлейній транзакції. Параметр «Device ID» використовується для локальних пристроїв. Друга колонка у заголовку політики визначає бажану дію в транзакції: store зберігати дані локально, store cloud зберігати дані в хмарному сховищі, access доступ до збережених даних пристрою, monitor для доступу до даних конкретного пристрою в реальному часі. Третя

колонка у заголовку політики позначає ідентифікатор пристрою в розумному домі. І остання колонка відображає дію, котру треба виконати для транзакції.

Окрім заголовків кожен блок містить цілий ряд транзакцій. У кожній транзакції існують п’ять параметрів. Перші два параметри використовуються для створення ланцюжка транзакцій одного і того ж пристрою одне з одним та служать для ідентифікації кожної унікальної транзакції в Blockchain. Відповідний ідентифікатор пристрою транзакції вставляється в третє поле. «Transaction type» - тип транзакції: genesis, access, store, monitor. Сама транзакція зберігається у п’ятому стовпчику, за умови якщо вона надходить з оверлей мережі, в іншому випадку поле залишається порожнім. Локальний Blockchain утримується та керується локальним Майнером.

Майнер розумного будинку. Це пристрій, який централізовано обробляє вхідні та вихідні транзакції в розумний будинок та із нього. На подобі до центральних пристроїв безпеки, майнер аутентифікує, авторизує та перевіряє транзакції. Також, майнеру властиві інші додаткові функції: генерування транзакції генезису, розповсюдження та оновлення ключів, змінювання структури транзакцій, формування кластеру і керування ним. Майнер збирає всі транзакції в блок і додає готовий блок до Blockchain.

Локальне сховище. У кожному будинку може бути додаткове локальне сховище для локального зберігання даних. Це може бути локальний резервний диск. Це сховище можна інтегрувати з майнером або бути окремим пристроєм.

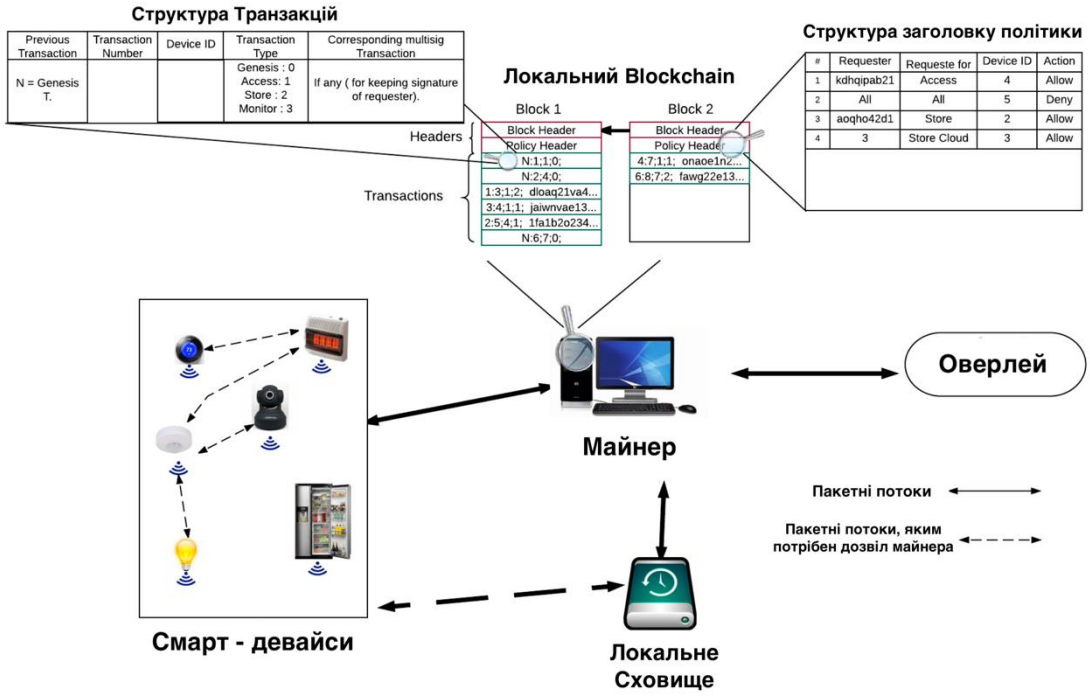

Рис 3.6.2.1 Загальний вигляд схеми «Розумний Будинок»

3.6.3 Оверлей Мережа

Оверлей мережа схожа на однорангову мережу в Bitcoin. Складовими вузлами можуть бути розумні домашні майнери, інші домашні пристрої з високими ресурсами, смартфон або персональний комп'ютер користувача. Кожен вузол використовує Tor для підключення до оверлей мережі для додаткової анонімності на IP-рівні. Конкретний користувач може мати більше одного вузла в мережі. Щоб зменшити накладні витрати та затримку, вузли в мережі групуються в кластери, і кожен кластер обирає кластера-керівника (CH). Кожен вузол може змінити свій кластер, якщо він відчуває надмірні затримки. Більше того, вузли в кластері можуть обрати новий CH в будь-який момент.

Оверлейний Blockchain зберігається всіма кластерами-керівниками в оверлей мережі, який містить транзакції з кількома підписами, надіслані хмарним сховищем та транзакціями доступу. На відміну від майнінгу біткойн, кожен CH самостійно вирішує, зберігати новий блок чи відкидати його, на основі свого спілкування з учасниками отриманої транзакції. Це може призвести до різних

версій ВС в кожній СН. Наприклад СН1 має блоки 1, 2, 4 і 6, а СН4 має блоки 1, 3, 6 і 8. Оскільки немає вимоги до узгодження ВС, накладні витрати на синхронізацію зменшуються.

3.6.4 Хмарне сховище

У деяких випадках пристрої в розумному домі (наприклад, розумний термостат) можуть захотіти зберігати свої дані в хмарному сховищі, щоб сторонній постачальник послуг (SP) міг отримати доступ до збережених даних і надати певні розумні послуги (наприклад, інтелектуальне регулювання температури). Хмарне сховище групує дані користувача в ідентичні блоки, пов’язані з унікальним номером блоку. Номер блоку та хеш збережених даних використовуються користувачем для аутентифікації. Якщо сховище може успішно знайти дані з заданим номером блоку та хешем, тоді користувач проходить автентифікацію. Пакети даних, отримані від користувачів, зберігаються в блоках у порядку «перший прийшов – перший вийшов» разом із хешем збережених даних. Після збереження даних новий номер блоку шифрується за допомогою спільного ключа, отриманого з узагальненого алгоритму Діффі-Хеллмана. Це гарантує, що той, хто володіє ключем, є єдиним, хто знає номер блоку. Оскільки хеші стійкі до колізій і лише справжній користувач знає номер блоку, ми можемо гарантувати, що ніхто, крім справжнього користувача, не зможе отримати доступ до її даних, а також приєднати свіжі дані до існуючої книги. Варто зазначити, що кожен користувач може створити різні реєстри даних у сховищі для кожного зі своїх пристроїв або єдину загальну книгу для всіх своїх пристроїв.

3.6.5 Керування транзакціями

Щоб додати пристрій до розумного дому, майнер генерує genesis транзакцію, ділиться ключем із пристроєм. Спільний ключ між Майнером і пристроєм зберігається в genesis транзакції. Власник будинку створює власні політики відповідно до запропонованої структури політики та додає заголовок політики до

першого блоку. Майнер використовує заголовок політики в останньому блоці в Blockchain; отже, щоб оновити політику, власник має оновити заголовок політики останнього блоку.

Розумні пристрої можуть спілкуватися безпосередньо один з одним або з об’єктами, які знаходяться ззовні розумного будинку. Пристрій всередині будинку здатен запитувати дані від іншого внутрішнього пристрою, з метою запропонувати деякі послуги: лампочка запитує дані від датчика руху, щоб автоматично вмикати світло, якщо помічено рух у приміщенні. Для отримування контролю користувачем над транзакціями розумного будинку, майнер повинен розподілити спільний ключ для пристроїв. Щоб згенерувати ключ, майнер перевіряє заголовок політики або запитує дозвіл у власника, а вже потім розподіляє спільний ключ між пристроями. Щойно отримавши ключа пристрої спілкуються безпосередньо, до тих пір поки їх ключ є дійсним. Щоб відмовити у дозволі, майнер визначає ключ як недійсний, надсилаючи відповідне повідомлення до пристроїв. Цей метод має подвійні переваги: майнер (власник) має список пристроїв, які обмінюються даними, а також зв’язок між пристроями гарантується спільним ключем.

Зберігання даних на локальному сховищі за допомогою пристроїв є іншим можливим шляхом для транзакцій всередині будинку. Для локального зберігання даних, кожному пристрою необхідно пройти автентифікацію в сховищі, що виконується з допомогою спільного ключа. Пристрій надсилає запит для майнера, з метою отримати ключа і якщо він має дозвіл на зберігання, майнер генерує ключ і надсилає його для пристрою та сховища. Отримавши ключ, локальне сховище створює початкову точку, яка містить спільний ключ. Якщо пристрій має спільний ключ, він може зберігати дані безпосередньо в локальному сховищі.

Пристрої можуть вимагати збереження даних у хмарному сховищі, що називається store transaction. Припустимо, що користувач створив обліковий запис у хмарному сховищі та налаштував дозволи для свого термостата на завантаження даних до цього сховища. Під час процесу завантаження хмарне сховище повертає вказівник на перший блок даних. Коли розумному термостату потрібно зберегти

дані в хмарному сховищі, він надсилає свої дані майнеру. Після перевірки дозволів і вилучення попереднього номера блоку та хешу, майнер створює випадковий ідентифікатор і надсилає дані в сховище з цим ідентифікатором. Передбачається, що в будь-який момент часу два вузли не можуть мати однаковий ідентифікатор. Сховище перевіряє дійсність транзакції, а також підтверджує наявність вільного місця в хмарному сховищі. Якщо все вийшло, він обчислює хеш отриманих пакетів даних і порівнює його з отриманим хешем. Якщо два хеші збігаються, то пакети даних зберігаються в сховищі, а новий номер блоку шифрується за допомогою спільного ключа та надсилається майнеру. Далі підписаний хеш даних підписується сховищем і відправляється в оверлей мережу для майнінгу в оверлейному Blockchain. Це гарантує, що будь-які зміни в даних користувача будуть видимі для всіх.

У випадку з локальним сховищем дії аналогічні, різниця лише в тому, що немає необхідності використовувати ідентифікатори, оскільки всі комунікації виконуються локально в розумному будинку.

Інші можливі транзакції – це access та monitor транзакції. Ці транзакції в основному генеруються або власником будинку для моніторингу житла, коли він знаходиться на вулиці, або постачальниками послуг для обробки даних пристроїв для персоналізованих послуг. Постачальнику послуг може знадобитися отримати доступ до збережених даних протягом певного періоду часу (наприклад, за останні 24 години) або до всього ланцюжка даних для певного пристрою, щоб реалізувати певні послуги. Для доступу до інформації ПП створює та підписує транзакцію з кількома підписами, яку потрібно підписати запитувачу (ПП) і отримувачу (майнер розумного будинку) і надіслати її на свій власний СН. СН перевіряє обидва списки РК. Якщо ініціатор транзакції з мультипідписом знаходиться у списку РК запитувача СН або його одержувач знаходиться у списку РК одержувачів, він передає транзакцію у свій власний кластер. В іншому випадку транзакція транслюється на інші кластери, і РК запитувача поміщається в список пересилання. Коли майнер розумного будинку отримує транзакцію з кількома підписами, він повинен перевірити політики в своєму локальному

Blockchain, щоб перевірити, чи має ПП дозвіл на доступ до даних, який повинен був надати користувач раніше. Якщо так, майнер запитує пакети зі сховища, шифрує їх за допомогою РК запитувача і відправляє їх запитувачу. Після відправки даних для запитувача майнер повинен зберігати транзакцію з мультипідписом в локальному Blockchain. Крім того, майнер надсилає транзакцію з мультипідписом до випадкового набору кластерів для збереження в оверлей мережі. Ці збережені транзакції з мультипідписом можуть розглядатися як доказ того, що дані були надіслані користувачем, а також можуть бути використані для того, щоб інші вузли повідомили про неправильну поведінку (наприклад, вузол запитує дані, доступ до яких йому не дозволено).

Отримуючи транзакцію access від вузлів оверлею, майнер проводить перевірку, чи знаходяться необхідні дані в локальному або ж хмарному сховищі. Якщо дані зберігаються в локальному сховищі, майнер запитує дані з нього та надсилає їх запитувачу. Якщо ж дані зберігаються в хмарному сховищі, майнер або запитує дані з хмари і відправляє їх запитувачу, або надсилає останній номер блоку та хеш запитувачу.

Отримуючи транзакцію monitor, майнер надсилає запитувачу дійсні дані бажаного пристрою. Якщо запитувачу дозволено отримувати дані протягом певного періоду часу, майнер надсилає дані періодично, доки запитувач не надішле запит на закриття майнеру та не скасує транзакцію. Транзакція monitor дозволяє власникам будинків дивитися камери або інші пристрої, на які періодично надсилаються дані. Якщо час, протягом якого майнер надсилає дані для запитувача, вичерпується, то з’єднання розривається майнером.

Результати дослідження. В даній роботі було розглянуто концепцію інтегрування технології blockchain до "Розумного будинку" на базі Інтернету Речей. Blockchain обіцяє конфіденційність та безпеку в Інтернеті речей. Однак застосування ВС в IoT не є простим через різні пов’язані з цим проблеми, зокрема: високе споживання ресурсів, масштабованість та час обробки. У роботі було запропоновано оптимізований Blockchain, який усуває накладні витрати, пов’язані з класичним Blockchain, зберігаючи при цьому його переваги безпеки та

конфіденційності. Запропонований Blockchain не вимагає майнінгу , таким чином, не зазнає додаткових затримок в обробці згенерованих транзакцій. Ієрархічна архітектура, складається з приватного та централізованого Blockchain на рівні локальної мережі IoT для зменшення накладних витрат, децентралізованого публічного Blockchain на пристроях вищого класу.

ВИСНОВОК

В ході дипломної роботи було досліджено актуальність вибраної теми. В роботі було представлено ознайомлення з історією розвитку технології Blockchain. Досліджені основні принци роботи мережі Blockchain, розглянуті основні компоненти: хеш функція, хеш таблиця, асиметричні алгоритми шифрування, смарт-контракти. Використання згаданих компонентів надає цілий ряд переваг: доступність та ідентичність даних, уникнення доступу до даних небажаних сторін та надійність їх збереження, прозорий механізм передачі, усунення потреби в посередниках, можливість перевірки інформації, надійність роботи мережі. Недоліками подібного рішення можуть стати складність реалізації стабільної роботи на етапах розвитку мережі, відносна проблема з масштабованістю мережі, оскільки, Blockchain – нова технологія, яка все ще розвивається.

Було встановлено, що блокчейн – це децентралізована база даних, яка організована на основі мережі P2P. Вона складається з великої кількості комп’ютерів, які розташовані у різних місцях та взаємодіють на основі консенсусу. Також було досліджено мережу P2P та її роль для технології blockchain. Відбувся опис класифікації блокчейн-мереж та дослідження структури та принципів роботи блокчейн-ланцюга. Були досліджені основні властивості blockchain: децентралізація, прозорість та незмінюваність.

В останньому розділі було описана можливість застосування технології блокчейн в сучасних компаніях та приклади основних ідей застосування технології blockchain у різних телекомунікаційних системах. Розглянуто технологічні рішення на базі blockchain та доцільність її використання в різних телекомунікаційних системах. Розглянуто блокчейн-рішення компанії IBM, досліджені переваги застосування blockhain для вирішення тої чи іншої задачі: автентифікацію користувача у роумінгу, узгодження взаємодії операторів у роумінгу, конфіденційність даних та їх монетизацію, використання blochchain для

5G включень та для IoT.

Було створено структурний опис та схему роботи телекомунікаційної мережі використовуючи технологію “Розумний Будинок” та інтеграція технології в Blockchain, описані основні процеси обміну даними між пристроями та рівнями мережі. Даний матеріал повинен допомогти в розгортанні механізмів комунікації та роботи усіх клієнтів в рамках зазначеної структури.

Отже, можемо сказати, що використання Blockchain може вирішити сучасні проблеми комунікації та проблеми збереження та доступу до даних. Основною перешкодою на шляху до цього є відносна новизна технології.

ПЕРЕЛІК ПОСИЛАНЬ

1. How blockchain can impact the telecommunications industry and its relevance to the C-Suite // Deloitte. [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www2.deloitte.com/content/dam/Deloitte/za/Documents/technology-mediatelecommunications/ za_TMT_Blockchain_TelCo.pdf.
2. 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
3. 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/
4. The History of Blockchain Technology [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://101blockchains.com/history-of-blockchain-timeline/
5. Что такое Алгоритм Консенсуса в Blockchain? [Електронний ресурс]. Режим доступу до ресурсу: https://academy.binance.com/ru/blockchain/what-is- a-blockchain-consensus-algorithm
6. Григорчук К. Обзор 9 алгоритмов блокчейн консенсуса [Електронний ресурс] / Кирилл Григорчук // DigitalForest. – 2018. – Режим доступу до ресурсу: https://digiforest.io/blog/blockchain-consensus-algorithms.
7. Blockchain Use Cases in the Telecom Industry [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.infopulse.com/blog/blockchain-use-cases-in-the-telecom-industry
8. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. [Електронний ресурс]. – Режим доступу до ресурсу: https://bitcoin.org/bitcoin.pdf.
9. Перспективи використання технології блокчейн у мережі інтернет речей [Електронний ресурс] / Н.Г. Яцків, С.В. Яцків. . – 2016. – Режим доступу до ресурсу: https://nv.nltu.edu.ua/Archive/2016/26_8/59.pdf
10. A.Dorri, S.S.Kanhere, and R.Jurdak,“Blockchain in internet of things: Challenges and solutions,” [Електронний ресурс] arXiv preprint arXiv:1608.05187, 2016.
11. K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” [Електронний ресурс]. – 2016. – IEEE Access, vol. 4, pp. 2292–2303, 2016.

12. Reyna, Ana, et al. "On blockchain and its integration with IoT. Challenges and opportunities." Future Generation Computer Systems [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://doi.org/10.1016/j.future.2018.05.046