Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем
(повне найменування інституту, факультету)

Кафедра телекомунікацій
(повна назва кафедри)

До захисту допущено
В.о. завідувача кафедри
_____ Валерій ЯВІСЯ
(підпис) (Ім'я, прізвище)
"_04_" _червня_____ 2020_р.

Дипломна робота

на здобуття освітнього ступеня "бакалавр"
(назва ОС)

Спеціальність 172 Телекомунікації та радіотехніка,
(код і назва)

на тему: Можливість застосування технології блокчейн в телекомунікаційних системах

Виконав: студент IV курсу, групи ТМ-61
(шифр групи)

Денисюк Владислав Вікторович _____ _____
(прізвище, ім'я, по батькові) (підпис)

Керівник доцент каф. ТК, к. т. н., с. н.с. Міночкін Д. А. _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент доцент каф. ІТМ, д.т.н, с.н.с. Скулиш М.А._____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____
(підпис)

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем
(повна назва)

Кафедра телекомунікацій
(повна назва)

Освітній ступінь бакалавр

Спеціальність 172 Телекомунікації та радіотехніка
(код і назва)

ЗАТВЕРДЖУЮ

В.о. завідувача кафедри

_____ Валерій_ЯВІСЯ
(підпис) (ім'я, прізвище)

"_22_" _січня_2020 р.

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

Денисюк Владислав Вікторович
(прізвище, ім'я, по батькові)

1. Тема роботи: Можливість застосування технології блокчейн в телекомунікаційних системах

Керівник роботи доцент каф. ТК, к. т. н., с. н. с. Міночкін Д.А.,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від 30 березня 2020 р. №_924_-с

2. Термін подання студентом роботи____04.06.2020_____

3. Вихідні дані до роботи: технологія blockchain, розподільна мережа, децентралізована система, теоретичні відомості_____

_____

4.Зміст роботи:

_1) Дослідження основних складових технології blockchain та ознайомлення з історією її виникнення. Аналізування основних переваг та недоліків використання блокчейну.

_2) Дослідження основних принципів та функцій технології blockchain

_3) Проведення аналізу існуючого застосування blockchain та можливості його використання у телекомунікаційних системах.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

1) Тема та предмет дослідження. Мета роботи
2) Історія виникнення технології blockchain та її основні складові
3) Переваги та недоліки використання blockchain

4) Принципи та функції технології blockchain, властивості блокчейну
5) Застосування blockchain у телекомунікаційних системах. BubbleTone – блокчейн рішення для управління тарифами у роумінгу
6) PoC і IRBIS блокчейн рішення
7) Можливості використання технології blockchain у телекомунікаційних системах. Автентифікація користувача у роумінгу.
8) Узгодження взаємодії операторів у роумінгу. Конфіденційність даних
9) Використання blockchain для 5G та IoT
10) Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання _____12.12.2019_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Дослідження джерел по темі дослідження	15.12.19 – 27.01.20	
2	Дослідження основних складових технології blockchain, ознайомлення з історією його виникнення	30.01.20 – 05.03.20	
3	Дослідження переваг та недоліків використання технології blockchain	06.03.20 – 13.03.20	
4	Дослідження принципів та функцій технології blockchain	15.03.20 – 05.04.20	
5	Аналіз існуючих застосувань технології blockchain у телекомунікаційних системах	08.04.20 – 05.05.20	
6	Пошук прикладів можливості застосування технології blockchain у телекомунікаційних системах	06.05.20 – 25.05.20	
7	Підведення підсумків та оформлення пояснювальної записки	27.05.20 – 02.06.20	

Студент _____ _____Денисюк В.В._____
(підпис) (прізвище та ініціали)

Керівник роботи _____ _____Міночкін Д.А._____
(підпис) (прізвище та ініціали)

Реферат

Дипломна робота містить 66 сторінок, 20 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 66 pages, 20 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 ТА СКОРОЧЕНЬ

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

MD - Message Digest

SHA - Secure Hash Algorithm

HTTPS - Hyper Text Transfer Protocol Secure

SSL (Secure Sockets Layer) – Рівень захищених сокетів

MSISDN (Mobile Subscriber Integrated Services Digital Number) - номер мобільного абонента цифрової мережі з інтеграцією служб

CSP (Cryptography Service Provider) – криптопровайдер

HLR - Home Location Register

VLR - Visitors Location Register

LTE – Long-Term Evolution

GPRS - General Packet Radio Service

WiMAX - Worldwide Interoperability for Microwave Access

WLAN (Wireless Local Area Network) – безпровідна локальна мережа

ВСТУП

Сфера телекомунікацій розпочала свій стрімкий розвиток з моменту запатентування першого прототипу сучасного телефону. Це було зроблено у 1876 році американським винахідником Александром Беллом. З цього часу розпочинається більш, ніж столітня історія телекомунікацій. Цей період багатий на різні відкриття, одним з найважливіших, на мою думку, є Інтернет. Однак, нічого немає вічного, сучасний світ стрімко розвивається, наука крокує вперед і на заміну старим технологіям приходять нові. Ми це бачили на прикладі мобільного зв'язку, та, зокрема, на прикладі мобільного телефону, який лише близько 20 тому був доступний лише певному колу осіб, мав величезні розміри та не мав таких функцій, які мають сучасні смартфони.

Сучасні мобільні телефони стають все потужнішими з кожним роком. Виробники збільшують об'єми оперативної пам'яті, покращують камеру, збільшують об'єми батареї,- усе це потребує додаткового місця. Одним із розв'язань такої проблеми є створення технології eSIM, яка уже реалізована на нових смартфонах, та впроваджена в Україні мобільним оператором Lifecell та ТриМоб. Ця технологія передбачає використання замість звичайної пластикової USIM-карти різних розмірів та являє собою чип, який уже вбудовано у смартфон. Користувач лише сканує QR-код і може використовувати на своєму пристрої та використовувати не один телефонний номер, а навіть два. Усе це потребує додаткового захисту, щоб ніхто, окрім нас не міг отримати доступ до наших контактів, та взагалі, до усіх наших додатків. Для вирішення цієї проблеми можна використати технологію під назвою Blockchain.

Blockchain (англ. Block chain від block – блок, chain – ланцюг) – являє собою розподілену базу даних, яка складається з впорядкованих ланцюжкових записів, які називаються блоками. Ця база може постійно зростати. Вона захищена від підробки тим, що кожен блок має часову позначку та посилання на попередній блок хеш дерева. Ця технологія є загальнодоступною, але це не

означає, що будь-хто може отримати доступ до конкретних транзакцій. Навпаки, ця технологія створює приватний ключ, до якого має доступ лише певний користувач і за допомогою цього ключа можна отримати доступ до конкретних даних. На прикладі eSIM – створюється приватний зашифрований ключ, який прив'язаний лише до одного пристрою. Цей ключ використовується для авторизації користувача в мережі. Кожен ключ є унікальним.

Сьогодні, технологія Blockchain є дуже перспективною, та дуже стрімко розвивається. Вона несе в собі можливість на створення нових бізнес-моделей в різних галузях, зокрема, і в телекомунікаціях. Послуги, які надають телекомунікаційні компанії, можна розглядати як складну екосистему. Вона вимагає велику кількість взаємозалежних груп операторів, як внутрішніх так і зовнішніх, які хочуть і можуть працювати над спільними проектами. По факту, сценарії впровадження блокчейну уже використовуються для того, щоб позбутись посередників між операторами, запобігання шахрайству в роумінгу і для ефективної мобільності телефонних номерів.

В кінці січня 2017 року було створено новий блокчейн-консорціум, завданням якого є підвищення безпеки та поліпшення використання IoT. Спільними зусиллями компанії розробляють на основі технології блокчейн протокол безпечного обміну інформацією між різними IoT-пристроями. Оскільки, щодня все більше і більше пристроїв отримує доступ до Всесвітньої павутини, то підвищується ризик злому такого обладнання для власної вигоди хакерів. Учасники нового консорціуму об'єдналися для того, щоб підвищити стійкість та ефективність інтернет-взаємодії IoT-продуктів.

1. ЩО ТАКЕ BLOCKCHAIN ТА ІСТОРІЯ ЙОГО ВИНИКНЕННЯ

Метою цього розділу є розгляд основних понять технології blockchain, історії його створення. В цьому розділі сформулюємо визначення основної мети та завдання blockchain у сучасному технологічному світі. Цей розділ має закласти фундамент для подальшого аналізу функціонування та вимог до рішень у телекомунікаційній сфері.

1.1. Історія розвитку технології Blockchain

Blockchain - це технологія, на основі якої засновані такі криптовалюти, як: Bitcoin, Litecoin, Ethereum, тощо. Технологія дозволяє передавати цифрову інформацію, але в жодному разі не копіювати її. Це означає, що кожна окрема частина даних може мати лише одного власника. Іншими словами, blockchain – це система облікової книги, яка сприяє децентралізації, прозорості та цілісності даних. Зазвичай цифрові фрагменти інформації являють собою «блоки» в регістрі. Цей «блок» зберігає інформацію про транзакцію, а саме: час, дату, суму, тощо. Зараз такі блоки можуть зберігати різні типи даних, такі як документи, зображення, посвідчення особи, тощо. Однак, замість того, щоб використовувати ваше справжнє ім’я, ви отримуєте унікальний «цифровий ключ» який ідентифікує вас як користувача. Крім того, блок містить лице це ім’я користувача. Ще один важливий факт полягає в тому, що кожен блок відрізняється від інших блоків. Таким чином, блок зберігає «хеш», який є унікальним кодом, який допомагає розрізнити системі два блоки. Щось схоже на унікальний ідентифікатор, наприклад, як номер студентського квитка, який є в одному варіанті для певного студента.

Технологія blockchain набула неабиякої популярності за останні десять років. Однак, її історія розпочалась значно раніше. У 1991 році була опублікована перша наукова робота, яка описувала криптографічний захист ланцюгів блоків. Її авторами стали С.Хабер та У.Скотт. Метою цієї роботи було знаходження рішення про неможливість спотворення чи пошкодження часових позначок. У 1992 році Хабер разом зі своїми колегами використав свої

напрацювання, які значно покращили ефективність і дозволили включати в один блок уже не один, а декілька документів, у проекті по створенню хеш-дерева. Хеш-дерево являє собою певну систему для контролю даних, які зберігаються, обробляються і передаються між комп'ютерами. Ця перевірка забезпечує унікальність та достовірність блоків та даних в цілому, при обміні між вузлами P2P мережі.

Пізніше, у 2008 році, людина чи група людей під псевдонімом Сатосі Накамото, опублікували нову ідею для використання технології blockchain. Ідея була в тому, щоб використовувати цю технологію як ядро для криптовалюти під назвою Bitcoin. Ця валюта змінила уявлення людей про використання цифрової форми оплати. Багато людей вважають, що Bitcoin і Blockchain – це одне і те саме. Однак, це не так, оскільки, остання забезпечує роботу більшості додатків, одним із яких є криптовалюта.

Після презентації альтернативного використання blockchain, у 2009 році Сатосі Накамото нарешті представили статтю про Bitcoin. У ній були описані усі відомості про роботу мережі та були описані тезиси про можливість підвищення цифрової довіри. Насправді, у цій мережі ніхто нікого не контролює, тому ніхто не може зламати довіру інших. Після цього Сатосі Накамото передали права на розробку платформи іншим розробникам і зникли з поля зору. Інші розробники почали створювати різні blockchain платформи, однак, відбувалось це дуже повільно. Увагу великої кількості людей привернули після оприлюднення можливості використання blockchain як децентралізованого додатку. [1] Так чи інакше, у 2010 році відбулась перша онлайн-купівля криптовалюти Bitcoin. Користувач придбав 10 000 «біткоїнів» по ціні 20 доларів. У 2018 році він міг би продати їх уже за 20000$ за одиницю.

Період 2012-2014 років був найбільш значущим у історії розвитку blockchain. Розробники розуміли, що ця технологія дуже перспективна і ще не досліджені всі її можливості. Серед них був і В.Бутерін, який додав нові напрацювання в базу блокчейну. Він працював над новим продуктом на базі блокчейну, який міг мати більшу кількість функцій та все ще підтримував би

peer-to-peer зв’язок. В цей час Bitcoin стає все популярнішим і його вартість перевищила 1 млрд доларів на ринку і ціна за одиницю була вище 1000$. У 2013 році Бутерін створює статтю про нове бачення використання блокчейну, не тільки для криптовалют, а використовувати його в різних сферах і публікує її під назвою «Ethereum: Смарт-контракт нового покоління та децентралізована платформа додатків». Він запропонував ідею універсальної децентралізованої блокчейн-платформи, в якій кожен користувач може програмно реалізувати різні системи зберігання і обробки інформації. Головна вимога полягла в тому, що дії мають бути описані в якості математичних правил. [1]

У 2015 році Linux Foundation, яка є найбільшою комерційною організацією з відкритим кодом, запускає розробку Hyperledger – платформа для допомоги людям у створенні блокчейн-проектів. У цей же час, Ethereum офіційно запустив і представив нову функцію під назвою «смарт-контракт». «Розумні» контракти – це звичайні контракти, які дозволяють обмінювати вашу власність, гроші, акції та інші цінності, але з одною відмінністю: зі смарт-контрактами вам не потрібен посередник.

Історія і розвиток блокчейну не закінчується на Ethereum і Bitcoin. За останні роки були створені десятки нових криптовалют. Передові країни почали приймати податки такими валютами. З прискореним розвитком Інтернету Речей була оптимізована платформа криптовалюти, оскільки її метою є забезпечення нульової комісії за транзакції. Сьогодні, мільярдні компанії взяли на себе ініціативо по вивченню і створенню додатків на базі цієї технології. Наприклад, Microsoft вкладає великі кошти в спеціалістів в області Blockchain, в результаті чого були створені приватні, гібридні і федеративні блокчейни. IBM та Samsung працюють над проектом Adept, який дозволить використовувати блокчейноподібні технології для створення децентралізованої мережі із великої кількості різних пристроїв сімейства Інтернету Речей (IoT), які можуть взаємодіяти один з одним. У цієї технології

великі перспективи, що признали на Всесвітньому економічному форумі, де блокчейн назвали одним з перспективних напрямків для інвестицій.

1.2. Основні складові технології Blockchain

По своїй суті blockchain – це лише термін з області комп'ютерних наук, який пояснює як в системі відбувається структурування та обмін даними. Ця технологія – це новий підхід до побудови розподілених баз даних, які контролює певна група людей з метою спільного збереження інформації і сумісної взаємодії. Всі дані представлені у вигляді списку, який є неперервним послідовним ланцюгом блоків.

Блок – це файли, які записуються без можливості змінити в майбутньому у мережі. В ньому зберігається інформація про проведених транзакціях до моменту створення даного файлу. Крім того, в блок записуються всі недавні транзакції, які не входили в попередні блоки. При створенні нового блоку, він завжди додається в кінець ланцюга блокчейну.

Транзакція або операція – передача даних від одного адресу до іншого. Вона подібна фінансовим транзакціям, де відбувається пересилання коштів від одного клієнта до іншого. В мережі ви робите все те саме, пересилаючи дані один одному.

В основу технології blockchain – закладено використання різних технологій та різних методів обробки і шифрування даних, а саме :

- *Асиметричні алгоритми шифрування*, інша назва яких: «*Асиметричні криптосистеми*»;

- *Смарт-контракти* – віртуальний протокол, написаний мовою програмування і використовується як інструмент обміну товарами й заключення договорів.

- *Хеш-функції* або «*хешування*» даних (функції MD та SHA);

- *Хеш-таблиці* – структура даних у вигляді асоціативного масиву, яка дозволяє зберігати пари (ключ, значення) і виконує три операції: додавання нової пари, видалення і пошук пари по ключу;

- *Майнінг* - процес який дозволяє усім криптовалютам працювати в якості децентралізованої однорангової мережі без посередників.

- Алгоритм консенсусу та реалізація механізму Proof of concept (PoC) – демонстрація практичної працездатності якогось методу, ідеї чи технології, з метою доведення, що метод, ідея чи технологія працюють.

Розглянемо детальніше вищезгадані терміни.

1.2.1. Асиметричні алгоритми шифрування

Асиметричні алгоритми шифрування – набір методів захисту даних в криптографії, які використовують два ключі. Перший ключ використовується для зашифровування даних. Цей ключ є відкритим і не може бути використаним для розшифровування. Другий ключ – таємний і використовується для розшифровування, не можливе за допомогою відкритого ключа. Тобто, ключ зашифровування і ключ розшифровування не можуть замінити один одного і є абсолютно унікальними.

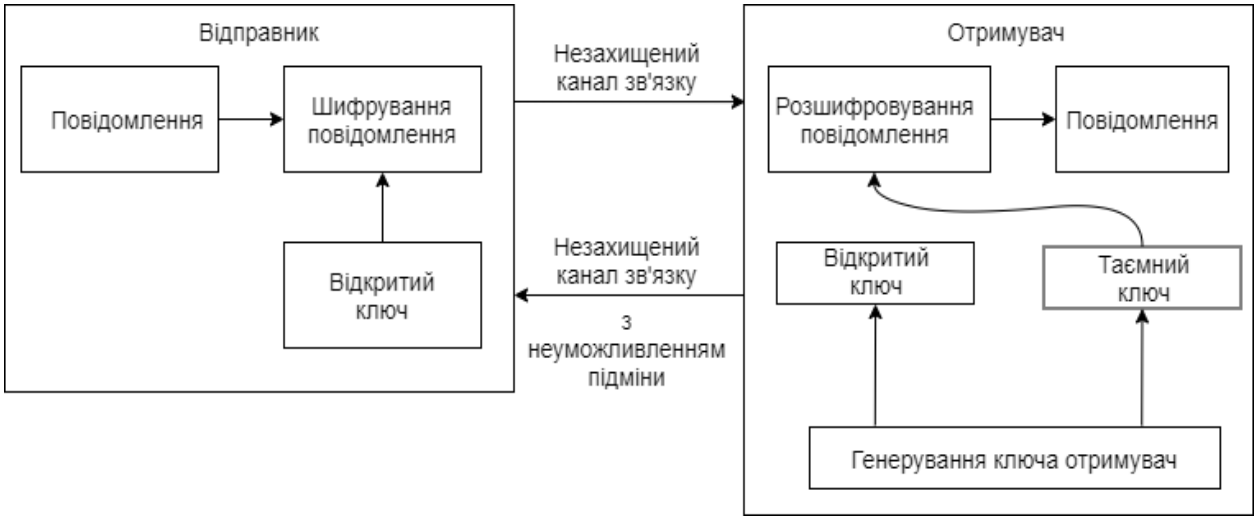

Рис. 1.1. Схема передачі даних у асиметричних криптосистемах.

1.2.2. Хеш-функція

Хеш-функція або функція згортки (англ. Hash – «мішанина») – функція, яка здійснює перетворення масиву вхідних даних довільної довжини в вихідний бітовий рядок встановленої довжини. Це перетворення здійснюється певним алгоритмом. Вхідні дані називаються вхідним масивом, «ключем», або «повідомленням». Вихідні дані (результат перетворення) називаються «хеш» або «хеш-код».

Криптографічна хеш-функція бере будь-які дані (довгі чи короткі) і, по суті, перетворює їх в рядок букв і цифр. Ці функції, які застосовуються в технології blockchain, діють лише в одному напрямку. Хоча одні і ті ж дані завжди дають один і той же хеш – відтворити початкові дані по отриманому хеші неможливо. У випадку технології Bitcoin – хеш складається з 256 біт, або ж з 64-х символів. Може показатись неможливим, що майже безкінечне число даних може послідовно перетворитись в унікальний рядок з 64-х символів, але саме таким чином працюють криптографічні функції. [2] Так функція маж мати як найменшу ймовірність виникнення колізій, адже, недопустимо, щоб для різних масивів даних часто будуть отримуватись одні й ті самі значення хешу.

Існують різні види криптографічних хеш-функцій, і кожна з них працює по-різному. Розглянемо найпопулярніші з них.

MD5 – алгоритм, який використовується для створення 128-бітного криптографічного рядка будь-якої довжини, який є унікальним для будь-яких даних. По своїй суті нагадує унікальний ідентифікатор людини, наприклад, єдиний цифровий підпис. Цей алгоритм призначений для використання додатками цифрових підписів, які вимагають, щоб великі об’єми даних були стиснуті безпечним шляхом перед своїм шифруванням за допомогою ключа в криптосистемі.

SHA-256 – алгоритм криптографічної хеш-функції, вхідний хеш, якого складає 256 біт. Цей алгоритм робить злом і розшифровування дуже складним процесом, оскільки чисельність варіантів є дуже великою. Цей алгоритм працює з розподіленими на 512-бітні блоки даних. Після криптографічного «змішування» на виході отримуємо 256-бітний хеш-код.

1.2.3. Хеш-таблиця

Хеш-таблиця – масив даних для зберігання пар значення-ключ, де положення елементів залежать від значення цього самого елемента. В таких таблицях реалізовано 3 типи операцій. Додавання нової пари по типу ключ-значення; операція пошуку по ключу; операція видалення по ключу.

Існує два основних види хеш-таблиць:

- Хеш-таблиці з лінійним розміщенням (метод ланцюжків) – в таких таблицях виконується пошук вільної комірки до тих пір, поки не знайдеться вільна. Тобто, якщо ви намагаєтесь вставити дані, а комірка зайнята, то ви переходите до наступної комірки й так до тих пір, поки не знайдеться вільна.
- Хеш-таблиці з відкритою адресацією – такі таблиці використовують в якості сховища даних неперервний масив.

Головною проблемою хеш-таблиць є те, що при меншому значенні розміру хеш-таблиці до кількості ключів, або при поганій хеш-функції можуть відбуватись колізії. Це означає, що одна комірка може містити два ключі.

У випадку додавання в хеш-таблицю в певну комірку ми зустрічаємо посилання на елемент пов’язаного списку, то відбувається колізія. Тоді, ми просто додаємо наш елемент в список. При пошуку ми проходимо по ланцюгам, порівнюючи ключи між собою на еквівалентність, доки не знайдемо потрібний. Головним недоліком такої таблиці є те, що при створенні досить довгих послідовностей заповнених комірок – збільшується середній час пошуку елементів в таблиці. Розв’язанням такої проблеми є використання

подвійного хешування. Головна ідея полягає в тому, що для визначення кроку зміщення при колізії в комірці використовується інша хеш-функція, яка не лінійно зміщує на один крок, а шукає вільне місце. [2]

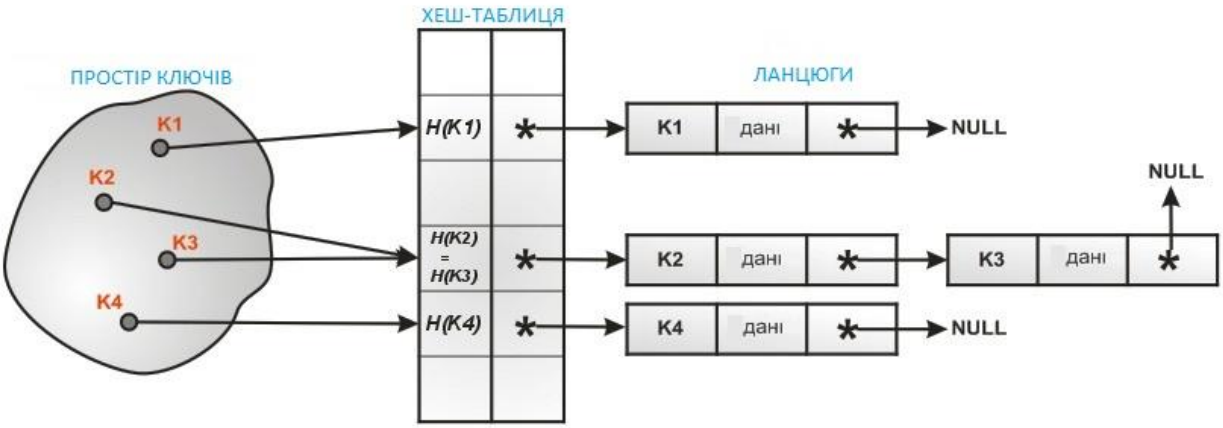

Рис. 1.2. Розв'язання колізій за допомогою ланцюжків.

У випадку методу з відкритою адресацією (замкнуте хешування) всі елементи зберігаються безпосередньо в хеш-таблиці без використання пов'язаних списків. На відміну від методу лінійного розміщення, 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. Найбільшою складністю при побудові таких таблиць є досить складна функціональність видалення елементу. Після видалення даних із хеш-таблиці ми робимо неможливим пошук ключа, в процесі вставки якого комірка стала заповненою. Нам доведеться певним чином помічати пусті клітки.

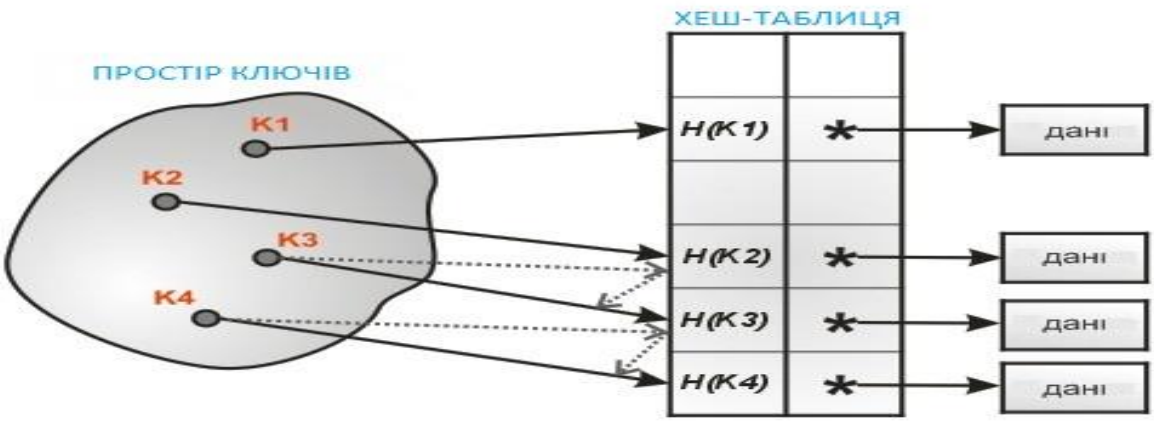

Рис.1.3. Приклад розв'язання колізій в хеш-таблиці з відкритою адресацією.

1.2.4. Смарт-контракти

Смарт-контракти (розумні контракти) – те саме, що і звичайні контракти, які дозволяються купувати та продавати різні речі, наприклад, нерухомість, акції, гроші, але такі контракти працюють без посередника.

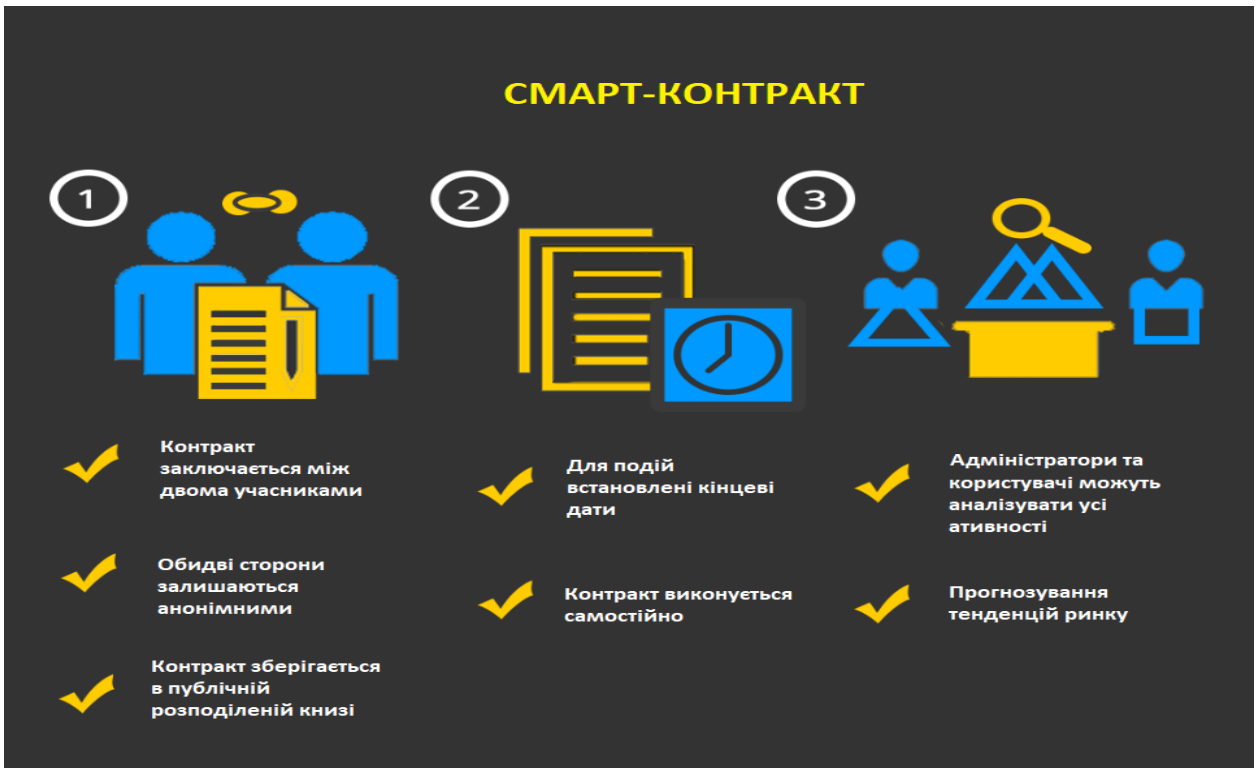

Рис. 1.4. Графічне пояснення смарт-контракту

Допустимо, що громадянин «А» хоче купити квартиру у громадянина «Б». Перший може легко перерахувати кошти, використовуючи технологію блокчейн та криптовалюту. Громадянин «А» отримає віртуальну квитанцію, яка буде включена у смарт-контракт. Після того, як «Б» віддасть ключі протягом певного терміну, то «А» здійснює платіж. Якщо ключі не були передані, тоді система буде вимагати повернення коштів. Тобто, лише коли будуть виконані умови із двох сторін: оплата і передача ключів – тоді система видає «А» ключ, а «Б» його кошти.

Переваги смарт-контрактів:

- Захист від втручання – жодна третя сторона не може втрутитися у ваш договір, лише ви самостійно приймаєте рішення по тій чи іншій угоді. Вам не потрібно чекати підтвердження нотаріуса, адвоката чи іншої особи.
- Безпека – смарт-контракти захистять ваші документи від хакерів процесом кодування з високим рівнем, яке майже неможливо підробити.
- Захист від помилок – при заповненні договору вручну – є велика ймовірність створення тої чи іншої помилки. Автоматизовані смарт-контракти автоматично закінчать увесь процес без єдиної помилки.
- Вигода – не потрібно платити третій стороні чи посередникам певну комісію.
- Швидкість – обробка усіх документів відбувається значно швидше, ніж у реальному житті.

Звичайний смарт-контракт містить в собі три окремі частини. Перша – цифрові підписи зацікавлених сторін. Друга – це певний предмет по якому проводиться угода. Третя - математично-описані умови угоди, за допомогою яких мови програмування записують ці дані в договір [3].

Усі дані контрактів мають отримуватись від надійного джерела. Щоб це гарантувати – використовуються різні програмні додатки та протоколи, наприклад, HTTPS і сертифікати безпеки SSL.

1.2.5. Поняття майнінгу

Головним учасником процесу майнінгу є майнер. Він являє собою вузол мережі, який збирає транзакції для подальшого додання їх в блок. Після того, як відбулась певна операція ці вузли отримують транзакції для подальшої їх перевірки. Після чого вони додають їх в певний «пул» пам'яті і починають збирати декілька транзакцій в один блок. Перед тим, як запустити процес, майнер додає транзакцію, в якій прописана нагорода за його роботу. Після хешування всіх функцій – вони об'єднуються в хеш-дерево, де вони сполучаються в пари до тих пір, доки не буде досягнута «вершина дерева». Ідентифікатор кожного блока утворюється в результаті додання поточного хешу з хешем попереднього блоку і певним випадковим числом. Тобто, він утворюється за певним протоколом. Іноді буває, що два вузли додають підтверджений блок і користувачі починають майнити блоки уже на основі цих даних, що є неправильним. В результаті чого конкуренція буде продовжуватись до тих пір, поки не буде створений один блок на основі одного із двох попередніх блоків. [4]

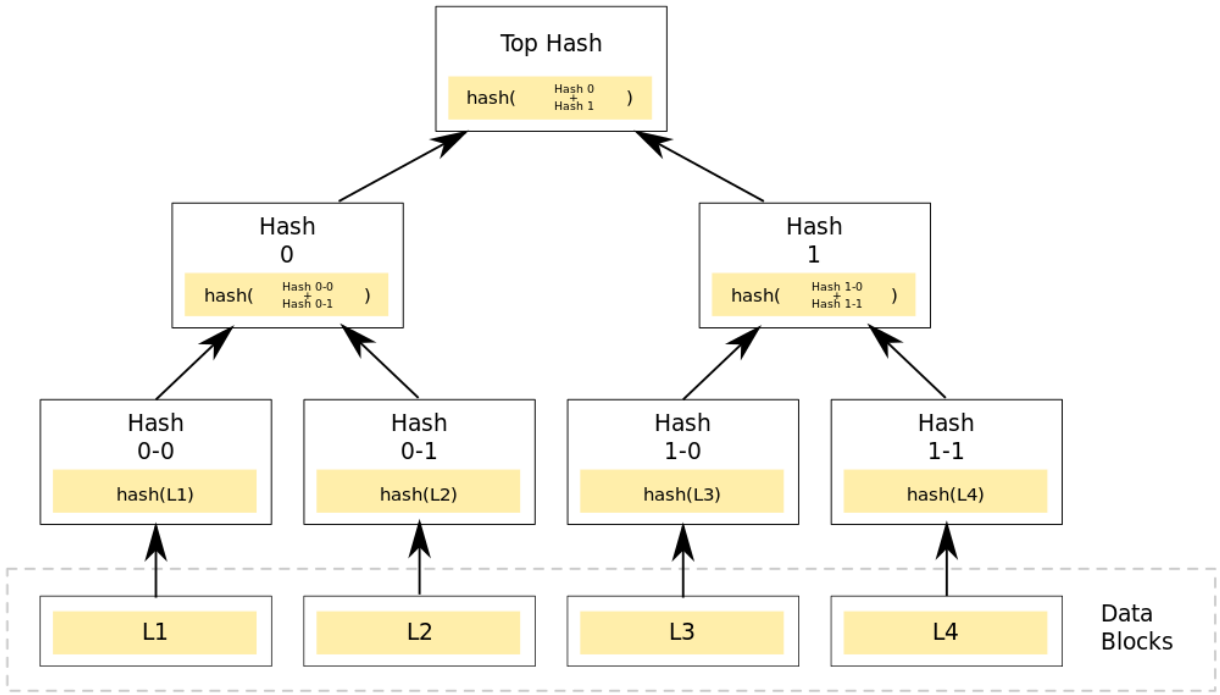

Рис. 1.5. Приклад хеш-дерава або дерева Меркла

1.2.6. Алгоритм консенсусу

Алгоритм консенсусу являє собою елемент технології blockchain, який забезпечує підтримку цілісності і безпеки цих розподілених систем. Оскільки блокчейн – це децентралізована система, тобто, у ній відсутні центральні органи, які виносять рішення, то цій мережі потрібно приймати рішення самостійно. Алгоритми консенсусу забезпечують виконання протоколу, гарантуються достовірність усіх транзакцій. Відмінність протоколу і алгоритму полягає в тому, що перший – це правила та дії, які необхідно дотримуватись системі для досягнення певної мети. Алгоритм – це механізм, який забезпечує виконання протоколів. Існує декілька алгоритмів консенсусу, але найбільш популярними є PoS та PoW.

Proof of Work (PoW) – це перший алгоритм консенсусу, який використовується в технології Bitcoin та в багатьох інших криптовалютах. Цей алгоритм представляє певну кількість спроб хешування, ця кількість прямо пропорційно залежить від обчислювальної потужності. PoW гарантує, що майнери можуть підтверджувати новий блок транзакцій та додавати його в блокчейн, якщо розподілені вузли досягають консенсусу щодо валідності (правильності) представленого блоку. Блокчейн Ethereum заснований на цьому алгоритмі. [5]

Proof of Stake (PoS) – алгоритм, який появився на заміну PoW. Головна його відмінність полягає в тому, що блоки провіряються відповідно до часток учасників. Тобто, враховується певна сума криптовалюти, яка додана тим чи іншим учасником. [5]

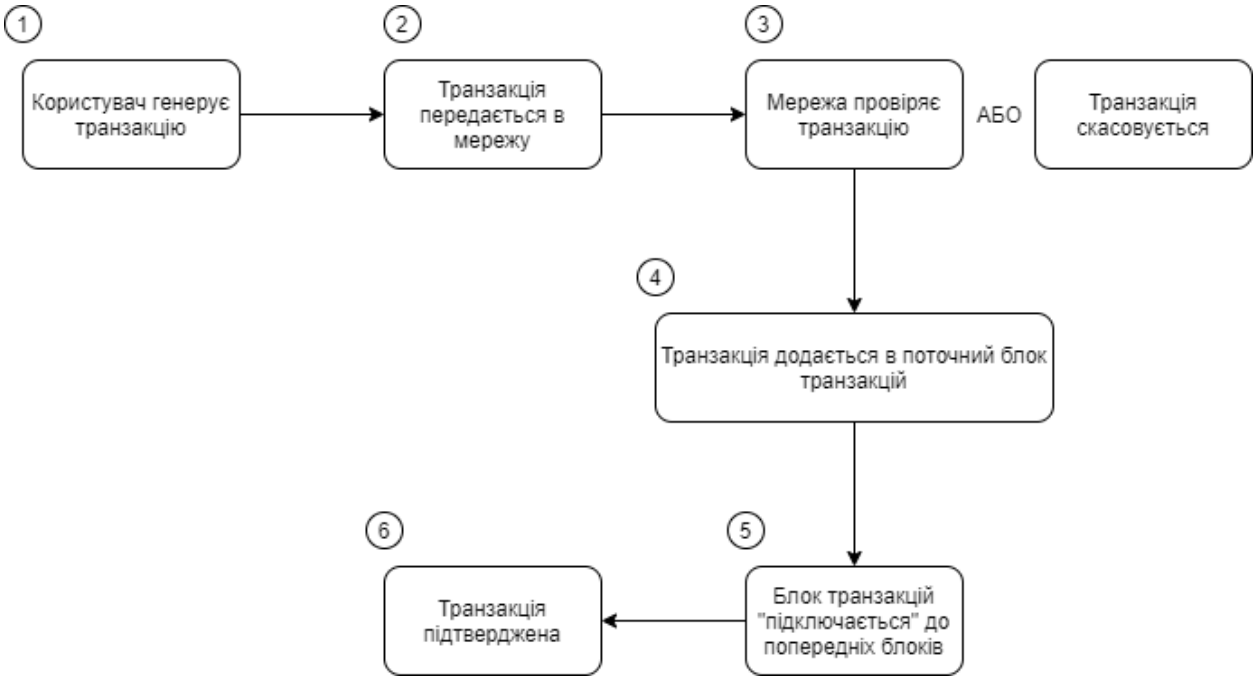

Рис. 1.6. Як в мережі blockchain досягається консенсус

1.3. Переваги та недоліки технології Blockchain

Головною перевагою blockchain, як уже було згадано вище, є відсутність додаткової плати, тобто, комісії чи оплати роботи третіх сторін. Одна сторона ініціює будь-який процес передачі даних, який є абсолютно безпечним, в результаті чого створюється блок. Він перевіряється великою кількістю комп'ютерів, розподілених в мережі. Після перевірки 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.

Наприклад, ви оплачуєте комунальні платежі дистанційно, тобто, використовуючи ваш комп'ютер чи мобільний телефон. Банківська компанія стягує додаткову комісію за оплату цих платежів. Якщо комунальні компанії будуть використовувати blockchain технологію, то це допоможе користувачам зекономити власні кошти, а також всі операції стануть значно захищеними. В даному випадку, сторонами договору є споживач та комунальна компанія. Квитанція за комунальні платежі є, по факту, смарт-контрактом, в якому

описано, що за ті чи інші послуги споживач зобов'язаний заплатити певну суму коштів. Така квитанція, так само як і грошовий переказ в мережі блокчейн, є унікальною, піддається незалежній перевірці без доступу до інформації транзакції, до ваших персональних даних і не піддається жодним змінам. І все це є абсолютно безкоштовним, blockchain може передавати, зберігати та контролювати будь-які грошові та не тільки процеси й може суттєво змінити укладене уявлення про певну оплату. [6]

Блокчейн існує до поки у світі є хоча б один комп'ютер, який підключений до мережі, адже, будь-хто може спостерігати за транзакціями, але без доступу до їх змісту. Усі дані транзакцій зберігаються на різних пристроях, а не лише на одному,- це і є розподільність блокчейна. Тобто, така система є системою з високим показником стійкості, тобто не піддається технічним проблемам та різним хакерським атакам. Адже, не існує єдиної точки входу в таку систему, що є набагато ефективнішим, ніж використовувати один сервер. Також з розвитком криптографії, створюються різні методи шифрування, що робить блокчейн з однієї сторони відкритим, а з іншою – надійно захищеним.

Однією із переваг блокчейну є його захищеність. Будь-яка паперова угода, може бути сфальсифікована певними «спеціалістами». Blockchain дозволяє використовувати електронні договори. У такому випадку не потрібні посередники, усе виконується в автономному децентралізованому режимі і саме це забезпечує прозорістю цієї технології. Учасники такої угоди є анонімними рівноправними користувачами і можуть як виконувати свої обов'язки так і порушувати їх, однак, у разі порушення система автоматично анулює контракт і поверне усім учасникам їх ресурси.

Після того, як ви зареєстрували дані в мережі blockchain – практично неможливо видалити чи змінити. Таке рішення робить цю технологію ідеальною для використання у різних фінансових структурах, для збереження інформації про транзакції та інші дані. Blockchain не дозволить жодному співробітнику завдати навмисних збитків. Ця технологія є абсолютно

довіреною системою, адже усі операції перевіряються тисячами комп'ютерів і такий процес називається майнінг. [6]

Одним із недоліків системи на базі технології blockchain є так звана «атака 51%». Існує припущення, що у разі отримання контролю одним об'єктом контролю понад 50% потужності хешування мережі, то це може порушити роботу системи. Однак, не зважаючи на те, що теоретично така можливість існує, але така маніпуляція над blockchain не досягнула успіху.

Головним недоліком технології блокчейн є її неможливість підтримувати велику кількість транзакцій за певний час. Наприклад, MasterCard і Visa підтримують понад 40 тисяч операцій в секунду, при цьому у blockchain технології цей показник є у тисячі разів нижче. Хоча з кожним днем бази даних розширюються і об'єм даних значно зростає. Внаслідок цього мережа ризикує втратити вузли, якщо регістр стане значно великим і користувачі не зможуть завантажити дані для їх зберігання. З усього цього виникає наступний недолік – збільшення навантаження на електричну мережу, адже, складні обрахунки спонукають комп'ютери використовувати велику кількість електроенергії. Прикладом цього є те, що спожиті ресурси, мережею Bitcoin є значно більшими, ніж у таких країн як Данія й Ірландія.

Великою проблемою технології блокчейн є використання двох типів ключів: публічний і приватний. Перший використовується для того, щоб ним можна було поділитися для проведення транзакції. Приватний ключ використовується для доступу до ваших коштів, по факту, до банку. Однак, у разі втрати цього ключа стає неможливо отримати доступ до своїх коштів і вони втрачаються. І з цим неможливо нічого зробити. [6]

Висновки до першого розділу

1. Blockchain – революційна технологія зберігання даних, яка кардинально змінює підхід до звичайних баз даних. Ця технологія є дуже перспективною та має можливість створити нові рішення у багатьох галузях,

включаючи телекомунікації. Blockchain підвищить надійність та ефективність поряд із прозорістю процесу.

2. Загальнодоступність і розподільність blockchain унеможливлює фальсифікацію транзакцій, які захищені вашим приватним ключем. Надскладні алгоритми шифрування інформації у цій технології роблять неможливим підробки інформації, а використання смарт-контрактів забезпечує кошти користувачів, шляхом вилучення з процесу третіх сторін.

3. Винайдення blockchain знайшло своє застосування у криптовалютах, таких як Bitcoin, Ethereum та інші, однак має перспективу застосування у різних галузях.

2. ПРИНЦИПИ ТА ФУНКЦІЇ ТЕХНОЛОГІЇ BLOCKCAIN

Завданням цього розділу є розгляд основних архітектур технології blockchain, особливості їх роботи, враховуючи усі переваги та недоліки. Також буде розлянуто P2P мережу і її роль в технології блокчейн. Цей розділ пояснить основні властивості blockchain мережі. Буде розглянуто головні принципи блокчейн систем та проведене базове ознайомлення з криптовалютами та їх видами.

2.1. Мережа P2P і її роль для технології blockchain

Peer-to-peer (P2P) – мережа, яка складається з певної групи взаємопов'язаних пристроїв, які обмінюються між собою файлами та зберігають однаковий набір даних. Кожен учасник (вузол) є рівноправним учасником, на відміну від традиційної архітектури, коли сервер надає певні послуги іншим.

Вузол – комп'ютер в архітектурі блокчейна, який має незалежну копію всієї книги реєстру.

Як правило, в мережі P2P усі учасники мають однакову потужність і виконують однакові задачі. У мережі blockchain P2P-платформа дозволяє учасникам здійснювати транзакції (обмін криптовалютами чи цифровими активами) через розподільну мережу та без третіх сторін, тобто, без посередників. Сьогодні P2P архітектура є невід'ємною складовою технології blockchain.

P2P-система складається з мережі розподілених користувачів, які знаходяться в різних куточках світу. Зазвичай, у цієї системи відсутній сервер, оскільки, кожен вузол зберігає копію всіх файлів і виступає джерелом для інших вузлів. Звідси, кожен пристрій може завантажувати файли з інших пристроїв, а також, може виступати у ролі сервера для завантаження даних на інший девайс. [7]

В таких мережах існує безліч програмних додатків для завантаження даних. Наприклад, один вузол ініціює процес завантаження з іншого, після успішної передачі такий вузол стає джерелом, по факту, сервером. Тобто, якщо вузол завантажує файли – він є клієнтом, у разі зворотної операції – він виступає у ролі серверу. На практиці можливе одночасне виконання цих двох операцій (наприклад, завантаження файлу «А» і передача файлу «В»).

В залежності від архітектури, існує три основних види P2P-мереж: структурована, неструктурована та гібридна.

Структурована P2P мережа представляє організовану архітектуру, яка за допомогою хеш-функцій дозволяє вузлам ефективно і значно швидше здійснювати пошук файлів, навіть у випадку, коли ці дані не є широкодоступними. Такий вид мережі є складнішим під час розгортання та підтримки життєдіяльності. [7]

Неструктурована P2P мережа не має конкретної організації вузлів: усі учасники випадковим чином взаємодіють один з одним. Враховуючи це, такі мережі є стійкішими до зміни активності вузлів, тобто при підключенні і відключенні тих чи інших пристроїв. Такий вид мережі є не дуже ефективним при пошуку даних, адже, відбувається велике навантаження на центральний процесор та оперативну пам’ять внаслідок того, що запити відсилаються максимально можливій кількості вузлів. [7]

Гібридні P2P мережі поєднують традиційну модель з одноранговою моделлю. Наприклад, можливо створити центральний сервер, який містить інформацію про усі вузли та спростить процес з’єднання вузлів між собою. Такий вид мережі є більш продуктивним. Оскільки, технологія blockchain є децентралізованою системою, то використання різних архітектур P2P мереж може мати різний рівень децентралізації. [7]

Технологія Bitcoin використовує P2P мережу для обміну криптовалютою між різними учасниками системи без посередників. Таким чином, в мережі відсутні банки, які обробляють та реєструють усі транзакції, однак, присутній публічний цифровий регістр, який перевіряється великою кількістю учасників.

Використання однорангової мережі унеможливлює блокування криптовалютних активів зі сторони центральних органів влади. Тобто, такі кошти не можуть бути вилучені чи заморожені будь-якою третьою стороною.

Головним недоліком P2P мереж є те, що регістри повинні постійно оновлюватись, що спричиняє необхідність у великій кількості обчислювальної потужності. Тобто, приходиться жертвувати часом задля підвищеної безпеки, однак, уже є деякі варіанти, які допомагають масштабувати систему.

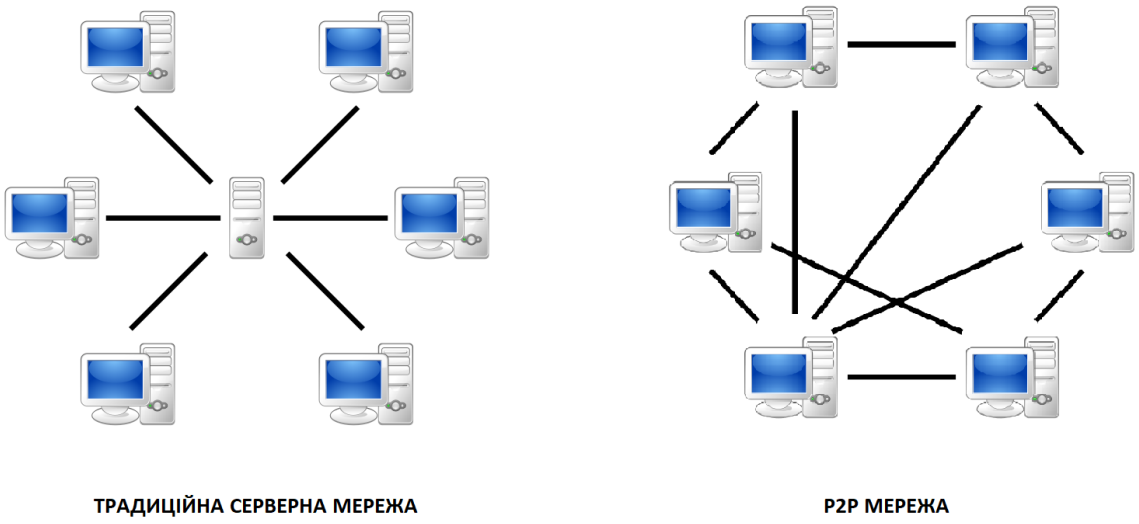

Рис. 2.1. Порівняння серверної та P2P мереж

Мережевий вузол – це точка, у якій повідомлення можуть бути створені, передані чи отримані. Повні вузли – ті пристрої, які підтримують і забезпечують безпеку блокчейн мережі. Вони приймають участь в процесі перевірки транзакцій і блоків, не зважаючи на консенсус правила системи. Повний вузол Bitcoin системи завантажує копію бази даних з кожним блоком і транзакцією. Такий вузол має мінімальні системні вимоги:

- портативний комп’ютер, або ноутбук з останньою версією Windows, Mac OS X чи Linux
- 200 GB вільного місця на жорсткому диску
- 2 GB оперативної пам’яті
- Високошвидкісне підключення до мережі Інтернет зі швидкістю передачі не менше 50 кБ/с

- Можливість безлімітного завантаження
- Можливість працювати не менше 6 годин на добу, а краще взагалі цілодобово

На сьогодні в мережі Bitcoin працює близько 10 тисяч загальнодоступних вузлів. Це число включає в себе лише загальнодоступні вузли, які є доступними і публічними.

Публічний вузол (супер вузол) підключається і передає інформацію будь-якому іншому вузлу, який вирішує встановити з ним з'єднання. Супер вузол є точкою розподілення, яка може діяти як джерело даних так і міст зв'язку. Він працює 24/7 та має декілька встановлених з'єднань з вузлами по всьому світі. Такий вузол потребує більшої обчислювальної потужності і кращого інтернет-з'єднання.

Водночас, майнери можуть вибирати: працювати самостійно (solo miner) чи в групі (pool miner). Перші використовують власну копію блокчейну, а групові майнери працюють разом, де кожен вносить свої власні обчислювальні потужності (хеш потужність). Для групових користувачів потрібен адміністратор для запуску повного вузла.

2.2. Класифікація blockchain мереж

Блокчейн являє собою таку структуру даних, яка додає нові записи в розподільну базу з публічним доступом до неї різних незалежних учасників. Існує три основних типи blockchain: публічний, приватний та гібридний.

Публічний блокчейн – відкритий ресурс, до якого може приєднатися будь-який охочий. Такі мережі деколи називаються «безправними» тому, що ніхто не надає права користувачам для взаємодії з цією технологією. Можливо виникає думка, що у разі публічності блокчейну – він менш захищений. Однак, це не так. Тут так само ніхто не може отримати доступ до інформації про користувачів, є лише доступ до публічного рахунку, дати чи суми транзакції.

Можливість будь-якого користувача перевіряти код блокчейну забезпечує його самоуправління та високий рівень безпеки, а велика кількість вузлів унеможливлює фальсифікацію даних. Адже, щоб виправити ті чи інші дані – потрібно їх виправляти у всіх базах, а вони розподілені на сотнях різних вузлах. Публічний blockchain – це децентралізована мережа, у якій неможливо підрахувати кількість вузлів, оскільки деякі з них є вузлами з закритим портом. Однак, будь-хто може приєднатися до мережі Bitcoin, не зважаючи на вік, географічне положення та рівень забезпеченості. Ще однією 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 і це одна із характеристик, яка виключає шахрайство. Адже, велика кількість вузлів спостерігає за тими чи іншими операціями.

Головним недоліком такої архітектури є низький показник транзакцій за секунду (TPS). Це пояснюється тим, що мережа складається з великої кількості вузлів, кожен з яких виконує операцію перевірки транзакції, яка потребує дуже багато часу. Саме тому публічна технологія Bitcoin має значну менший показник виконаних операцій за секунду, ніж Visa та Mastercard. Одним із недоліків публічного блокчейну є його масштабованість. Адже, вузли мають технічну обмеженість у збільшені продуктивності. Неможливо додати величезну кількість оперативної пам’яті чи використовувати процесор з надвисокою частотою,- усе це має функціональні обмеження. А зі збільшенням кількості вузлів виникає проблема великого використання електроенергії.

Приватний блокчейн – система з суворо фіксованими учасниками і часто використовується компаніями для внутрішнього аудиту. Тому таким підприємствам необхідно надавати доступ лише певним користувачам. В такій системі центральний орган (підприємство) відповідає за створення і перевірку транзакцій, а також за список тих учасників, які можуть читати ці операції. Така мережа дозволяє змінювати записи в регістрі, що є головною відмінністю

систем з публічним блокчейном, де дані не можуть бути змінені чи видалені. В такій мережі учасники відомі один одному, але деталі транзакцій приватні. Тому система приватного блокчейну знайшла своє застосування, коли підприємствам необхідно підвищити ефективність без надання публічного доступу до своїх транзакцій та є необхідність у створенні певних обмежень, які контролюють учасників мережі.

Головною перевагою систем з приватним блокчейном є швидкість транзакцій за секунду. Така можливість досягається через те, що мережа має обмежену кількість вузлів, на відміну від публічного блокчейну. Це все прискорює консенсус та процес перевірки транзакцій і така система обробляє транзакцій зі швидкістю до тисяч одночасно. Також приватний блокчейн мережі є досить масштабованими, ви можете вибрати розмір системи відповідно до ваших потреб. У разі необхідності у нових вузлах, компанії можуть легко додати нові, чи навпаки, зупинити непотрібні.

Головним недоліком приватного блокчейну є нижча безпека, у порівнянні з публічним. Оскільки, така система має обмежену кількість вузлів, які регулюються певним центральним органом, то у разі, якщо якийсь вузол отримає доступ до центральної системи,- він може отримати доступ до усієї мережі. Тому, системи з центральним органом керування є менш захищеними, оскільки вся ця система суперечить ідеї децентралізації, яка є одним із правил технології blockchain.

Гібридний блокчейн – являє собою розподільну мережу, яка керується певними вузлами, які заздалегідь обираються. Такі системи є поєднанням публічного і приватного блокчейну. Як і приватні системи, у випадку хакерської атаки, така мережа має єдину точку відмови, але такі блокчейн системи використовують підвищену ступінь криптографії для збільшення безпеки аудиту. Контроль у такій мережі відбувається не єдиним центральним органом, а декількома затвердженими користувачами. Гібридний блокчейн – це поєднання централізованої та децентралізованої системи, що дозволяє керувати кількістю користувачів, які можуть перевіряти транзакції. [8]

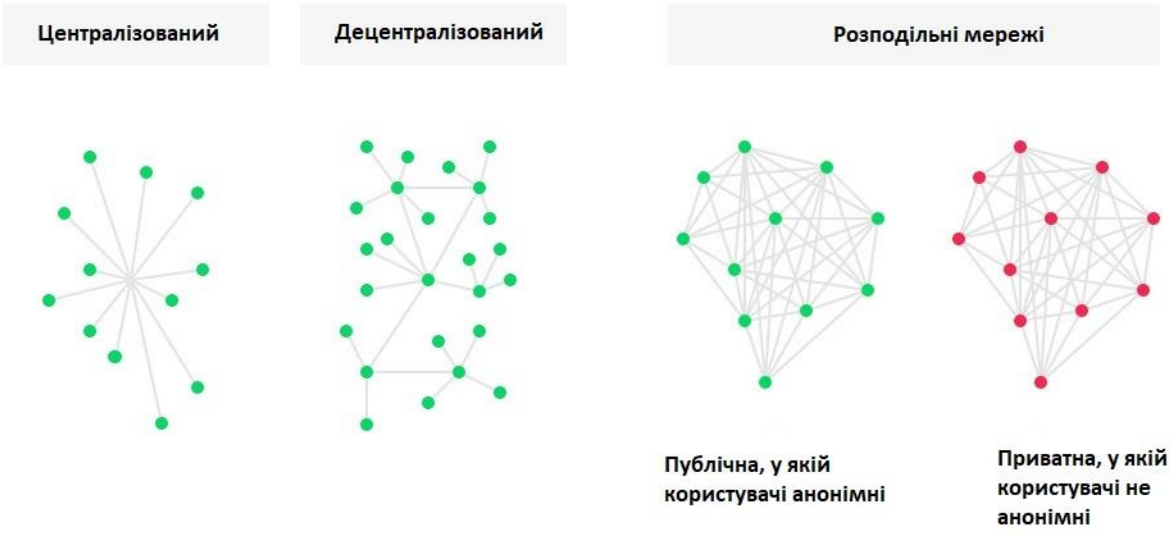

Рис. 2.2. Архітектура мережі blockchain

2.3. Структура та принцип роботи блокчейн ланцюга

Блокчейн ланцюг складається з трьох основних частин: блок, ланцюг блоків та мережа.

Блок – структура даних, яка має на меті об'єднання транзакцій і їх розподілення на всі вузли мережі. В blockchain мережі блоки містять інформацію про рух транзакцій в системі. Блок складається з двох частин: з заголовка та тіла. Останній містить список усіх транзакцій, які повинні міститись в поточному блоці для подальшої передачі в мережу blockchain. Заголовок містить інформацію, яка відповідає за стабільність мережі. Класичний заголовок blockchain мережі містить такі поля:

- Номер версії (version) – поточна версія блоку
- Хеш попереднього блоку (p_block)
- Хеш всіх транзакцій поточного блоку (tr_hash)
- Мітку часу, яка вказує, коли блок був створений (time)
- Nonce – числовий параметр, який обраховується в процесі майнінгу, для того, щоб хеш блоку був меншим деякого заданого числа.
- Bits – максимальне число, яке не повинен перевищувати хеш блоку

Ці 6 полів складають заголовок блоку. Решту блоку складають транзакції, які майнер вибрав, щоб додати в створений блок. Для отримання хешу всіх транзакцій в блоці використовується алгоритм Меркла, який обраховує 256-бітний хеш. Він використовується для подальшого обчислення хешу всього блоку. В кожній реалізації блокчейн-мережі розмір блоку, кількість можливих транзакцій можуть відрізнятись. [8]

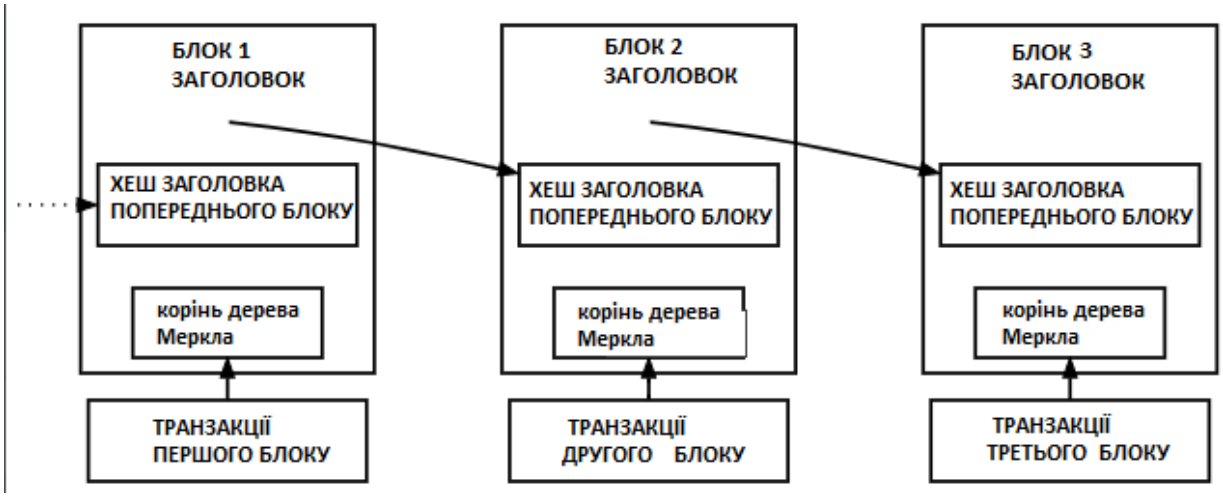

Рис. 2.3. Зв'язний список блоків

Хеш використовується для того, щоб якнайшвидше відрізнити одні дані від інших без необхідності порівняння кожного біту. Такий процес значно пришвидшує перевірку транзакцій. Кожен блок складається із заголовку, хешу попереднього блоку, кореню дерева Меркла та власних транзакцій. Кожен блок має містити одну, або декілька транзакцій. Перша з яких має бути транзакцією на базі монети, яка повинна збирати нагороду за операції. На рис. 1.5. зображено приклад хешування блоків. Кожен блок хешується з партнером, у разі його відсутності, хешується сам з собою. Такі операції проводяться до тих пір, доки не буде отриманий єдиний хеш – корінь дерева Меркла. Він є доказом того, що блок є достовірним і всі транзакції знаходяться у необхідному порядку.

Ланцюг блоків – являє собою базу транзакцій, яка обробляється кожним учасником мережі. Повна копія такого ланцюга містить абсолютно усі транзакції, які були здійснені в системі. Така інформація містить кількість дані

про те, яка кількість валюти була на певній біткоїн адресі в певний проміжок часу. Транзакція є непідтвердженою до тих пір, поки дані про транзакцію не будуть згруповані в спеціальні вигляд – блоки. Від кожного блоку в ланцюгу є лише один шлях до нульового блоку. Якщо відслідковувати блоки від нього, то ми будемо бачити розгалуження від кожного наступного блоку. Оскільки, блоки одночасно створюються різними майнерами, то нерідко виникали ситуації, коли один і той самий блок є попереднім для двох попередніх блоків. Кожен блок може містити як однакову інформацію про транзакції так і дані про транзакції лише цього блоку. Кожна гілка рівноправна до тих пір, поки одна з них не стане коротшою за іншу. Система автоматично рахує довший ланцюг, не звертаючи уваги на коротші гілки. Транзакції, які увійшли в коротшу гілку – втрачають статус підтверджених. Такі зайві операції не отримують підтвердження і втрачаються. [8]

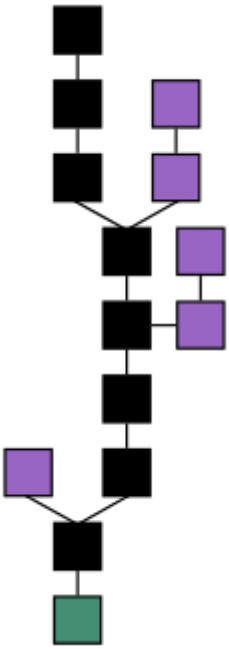

Рис. 2.4. Основна послідовність блоків (чорний ланцюг є найдовшою гілкою від нульового блоку)

База публічно зберігає в незашифрованому вигляді інформацію про всі транзакції. Для запобігання багатократної витрати одної і тої самої суми – використовуються мітки часу. Вони реалізовані шляхом розбиття ланцюга на

блоки. Кожен новий блок здійснює підтвердження транзакцій, інформація про які міститься у всіх попередніх блоках.

Ланцюг блокчейна представляє собою однорангову систему, яка не має центрального вузла і керується потоком даних. Централізований контроль здійснюється за рахунок організації великої кількості незалежних користувачів. Для запобігання загрозам мережі, окрім децентралізованої структури, використовується криптовалюта – цифровий токен, який має ринкову вартість. З нею здійснюються біржові операції, які аналогічні операціям з акціями. Криптовалюта кожного блокчейну функціонує за власними правилами. В основному, програмне забезпечення передбачає оплату роботи комп'ютерного обладнання, яке включає в себе повні вузли. Повні вузли – комп'ютери, які забезпечують роботу мережі і фізично знаходяться більше, ніж в одному місці.

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 повну копію всіх транзакцій, які колись були записані в блокчейн-ланцюг. Оскільки обслуговування вузлів – складна справа, яка потребує немалих вкладень, то контроль транзакцій – не безкоштовна справа. Сам алгоритм блокчейна передбачає винагороду вузлам у вигляді криптовалюти, наприклад, біткоїн.

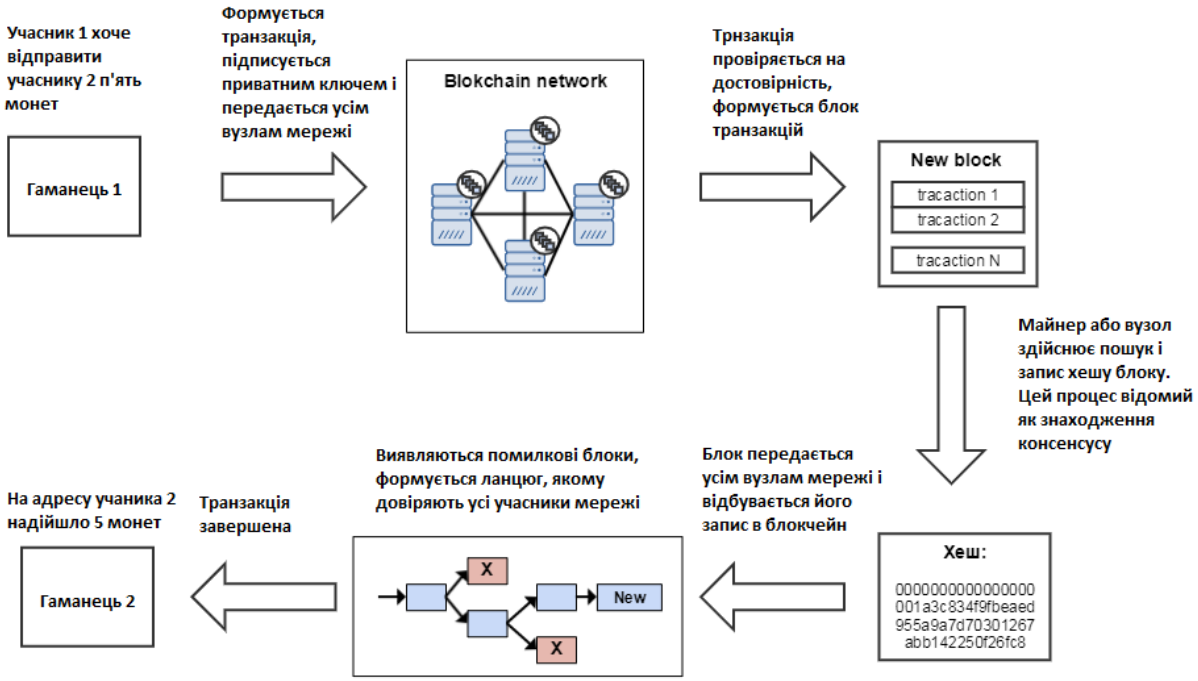

Рис. 2.5. Принцип роботи блокчейн мережі

2.4. Властивості технології blockchain

2.4.1. Децентралізація мережі blockchain

Децентралізація – процес розподілення влади чи фінансів без контролю глобального органу управління. Такі системи управління давно існують в багатьох компаніях. Однак, система децентралізованого управління фінансами з'явилася лише після створення блокчейн-ланцюга. В мережі блокчейн децентралізація здійснюється завдяки тому, що відсутній локальний сервер, а всі учасники ланцюга є рівноправними. У такій системі підтвердження транзакцій здійснюється самими учасниками. Технологія передбачає розподілення обчислювальних потужностей і даних по всій земній кулі при багаторазовому дублюванні інформації. Така можливість запобігає втратам, а DDOS-атаки на таку систему мають мінімальний чи зовсім нульовий ефект.

Навіщо потрібна децентралізація для криптовалюти? Вона забезпечує високий рівень безпеки транзакцій і зберігання коштів. Оскільки, інформація

про всі транзакції зберігається у кожного користувача і операції підтверджуються декількома незалежними вузлами, то таку систему неможливо змінити. В банківських структурах використовуються локальні системи, які є менш захищеними і швидкість транзакцій тут на пряму залежить від завантаженості і потужності локального серверу. Велика кількість учасників блокчейн-мережі, які розкидані по всьому світу, збільшують потужність і, відповідно, швидкість.

Найбільшою перевагою децентралізованої системи є відсутність зовнішнього регулювання. Наприклад, якщо правоохоронні органи вирішують вилучити пристрої і розробки власника. З децентралізованою системою це неможливо, оскільки потужності належать великій кількості учасників, а сама технологія знаходиться у відкритому доступі. Тому криптовалюта не піддається регулюванню зі сторони влади і ціна на неї залежить лише від попиту і пропозицій користувачів.

Приклад децентралізованого управління можна побачити на криптовалютних біржах. Вони розроблені на базі технології блокчейн і зосереджують кошти користувача в його управлінні. В той час як централізовані біржі лише надають можливість обмінювати, купувати валюту на їх серверах, при цьому, зашифровані приватні ключі зберігаються на сервері біржі. Децентралізовані електронні валюти повністю закріплені саме за їх власником і тільки він може здійснювати транзакції та отримувати доступ до свого сховища. У випадку централізованої системи, кошти зберігаються на банківському рахунку фінансового закладу, який залишає за собою право на блокування і зняття коштів. [9]

Одним із прикладів децентралізованої криптовалюти є Bitcoin – перша і найпопулярніша електронна валюта. В блокчейні біткоїна можна відслідкувати всю історію платежів, але учасники залишаються анонімними. Сьогодні продовжується розробка і вдосконалення цієї блокчейн-системи

розробниками, однак, ніхто з них не може керувати цією мережею для власних цілей.

Друга відома децентралізована криптовалюта – Ethereum. Вона має власну платформу, на якій розробники можуть запускати власні криптовалютні проекти. Ethereum є популярною валютою і займає друге місце, після Bitcoin по капіталізації. Основна її задача – виконувати роль коштів для обміну ресурсами. Ще одна популярна децентралізована криптовалюта, яка почала своє функціонування у 2012 році – Ripple. Вона активно співпрацює з фінансовими закладами і урядом з метою спрощення глобальної системи транзакцій. Централізація Ripple полягає в тому, що кожен вузол мережі вибирається компанією. [9]

2.4.2. Прозорість мережі blockchain

Прозорість блокчейн мережі обмежує властивість конфіденційності цієї самої системи. В цій технології особистість людини представлена у вигляді публічного криптографічного ключа. Тобто, якщо досліджувати історію транзакцій, то ви не побачите імена, а лише, що «21Mf82jf023Kf92dfasfk291kfds821ksdf2FJK2l відправив 1 Bitcoin». Таким чином, можна дослідити усі транзакції, які були зроблені за цією адресою, однак, не отримаєте інформацію про особистість. Така можливість є дуже перспективною. Наприклад, якщо перевести фінансовий облік компаній у систему блокчейн і знати публічну адресу, то можна дослідити весь рух фінансів. Тобто, така можливість є дуже перспективною, оскільки, існують компанії, які приховують свої фінанси.

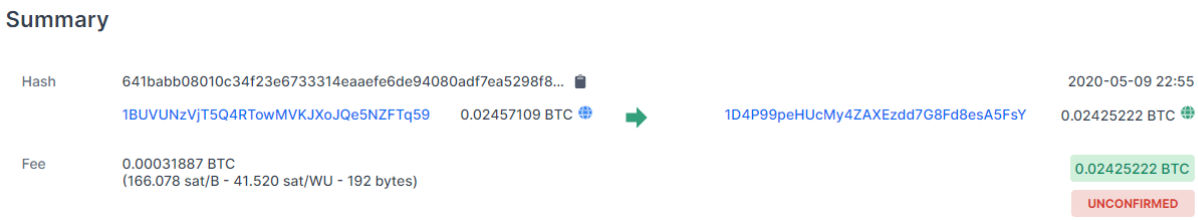

Рис. 2.6. Приклад транзакції Bitcoin

На рис. 2.6. представлений приклад транзакції в мережі Bitcoin. Показаний хеш операції, публічна адреса відправника та отримувача, сума переводу, час та дата, статус операції (не підтверджена), та винагорода майнеру за цю операцію (0.00031887 BTC). Сума транзакції на момент її здійснення дорівнює 239.53$, а винагорода майнеру становить 3.11$.

2.4.3. Незмінюваність blockchain

Криптографічна хеш-функція забезпечує незмінність блокчейну. Вона використовує вхідний рядок будь-якої довжини і перетворює його у вихідні дані фіксованої довжини. В контексті криптовалюти Bitcoin використовується алгоритм хешування SHA-256.

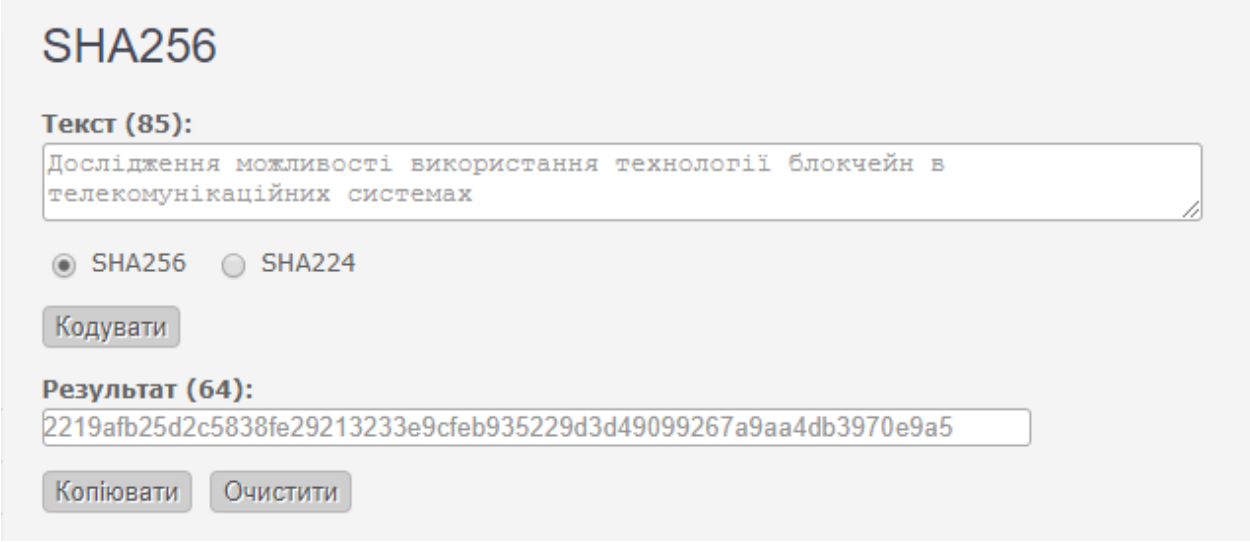

Рис. 2.7. Приклад кодування алгоритмом SHA-256

Отже, незалежно від довжини вхідного рядку, результат кодування буде фіксованої довжини – 256 біт. Така можливість допомагає, коли ви працюєте

з великими об’ємами даних. Тобто, замість запам’ятовування великих об’ємів даних, достатньо лише записувати хеші і відслідковувати цю інформацію. Криптографічна хеш-функція змінюється при найменших модифікаціях вхідного рядку. Тобто, функція буде змінюватись, навіть при заміні регістру букви.

Висновки до другого розділу

1. Блокчейн – децентралізована технологія, в основі якої лежить мережа P2P. Вона являє собою систему багатьох комп’ютерів, які провіряють транзакції та унеможливлюють їх фальсифікацію.
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. ЗАСТОСУВАННЯ BLOCKCHAIN ТА МОЖЛИВІСТЬ ЙОГО ВИКОРИСТАННЯ У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Метою даного розділу є опис застосування технології блокчейну в сучасних компаніях та дослідження можливості застосування технології blockchain у різних телекомунікаційних системах. В рамках цього розділу розглянемо технологічні рішення на базі blockchain та доцільність її використання в різних телекомунікаційних системах, будуть досліджені переваги застосування blockhain для вирішення тої чи іншої задачі. Буде розглянуто блокчейн-рішення компанії IBM, блокчейн-платформу компанії Cisco, концепцію мережі IRBIS та блокчейн-рішення BubbleTone.

В цьому розділі розглянемо можливі телекомунікаційні рішення на основі blockchain: автентифікацію користувача у роумінгу, узгодження взаємодії операторів у роумінгу, конфіденційність даних та їх монетизацію, використання blochchain для 5G включень та для IoT.

3.1. Застосування blockchain у телекомунікаційних системах

3.1.1. BubbleTone - блокчейн-рішення для управління тарифами на роумінг

Проблема: міжнародний роумінг – це великі витрати як для операторів, так і для абонентів по всьому світі.

Рішення

BubbleTone – інновація у сфері телекомунікацій, яка розроблена на базі технології blockchain. Це рішення створене на базі приватної блокчейн-мережі, яка забезпечує автономне регулювання плати за міжнародний роумінг. BubbleTone – перша децентралізована екосистема, яка дозволяє операторам мобільного зв’язку, користувачам телефонів і постачальникам послуг взаємодіяти напряму. Така система підключає операторів і кінцевих користувачів по всьому світу на блочно-орієнтованому ринці. [10] Якщо ви

подорожуєте світом і у вас виникла необхідність у використанні мобільного зв'язку чи інтернету закордоном, то вам не потрібно купувати SIM-карту місцевого оператора чи використовувати дорогий тариф вашого провайдера. Щоб розпочати використовувати такий підхід, достатньо завантажити безкоштовний додаток BubbleTone і система автоматично визначить ваше положення: чи знаходитесь ви у країні вашого оператора, чи ні. У разі використання цієї послуги закордоном – система автоматично підбере вам тариф місцевого оператора по місцевому тарифу, тобто, без роумінгу. Також доступна можливість вибору більш привабливого тарифу. Тому, більше не потрібно витрачати зайві кошти на покупки SIM-карт, адже, ви будете телефонувати за допомогою своєї власної. Така можливість доступна більше, ніж у 80-ти країнах світу.

Пряме підключення, яке застосовується у цьому додатку надає можливість використовувати LTE високої якості за доступними цінами. BubbleTone заснований на консенсусі PoS, який використовується для обробки великої кількості інтелектуальних даних. Цей додаток є повністю безкоштовним, ви платите лише за послуги оператора. Така можливість доступна через те, що BubbleTone бере комісію з провайдерів послуг за те, що залучили нового користувача.

Як це працює для операторів? Вони публікують власні пропозиції у вигляді смарт-контрактів на ринок. Ці пропозиції доступні для всіх інших операторів. Домашні оператори вибирають пропозиції, які вони бажають надати своїм абонентам. Вони мають повний контроль над цими пропозиціями та визначають ціни для абонентів у місцевій валюті. Після цього абонент вибирає бажану пропозицію і оплачує її. Створюється смарт-контракт, тобто, запит з цифровою ідентифікацією абонента та з транзакцією. Кошти перераховуються домашньому оператору та тому, чиї послуги використовуються. Завдяки технології blockchain оператори можуть взаємодіяти як рівноправні партнери і процедура узгодження значно спрощується. [10]

Переваги BubbleTone для користувачів:

- тепер у нас є можливість здійснювати дзвінки по вигідним тарифам в кожному куточку світу без складнощів підключення до місцевих операторів

- не потрібно змінювати свій мобільний номер

Переваги BubbleTone для операторів:

- кожен оператор отримає додаткову рекламу
- будь-який оператор отримає прямий доступ до міжнародного ринку з можливістю залучення додаткових клієнтів

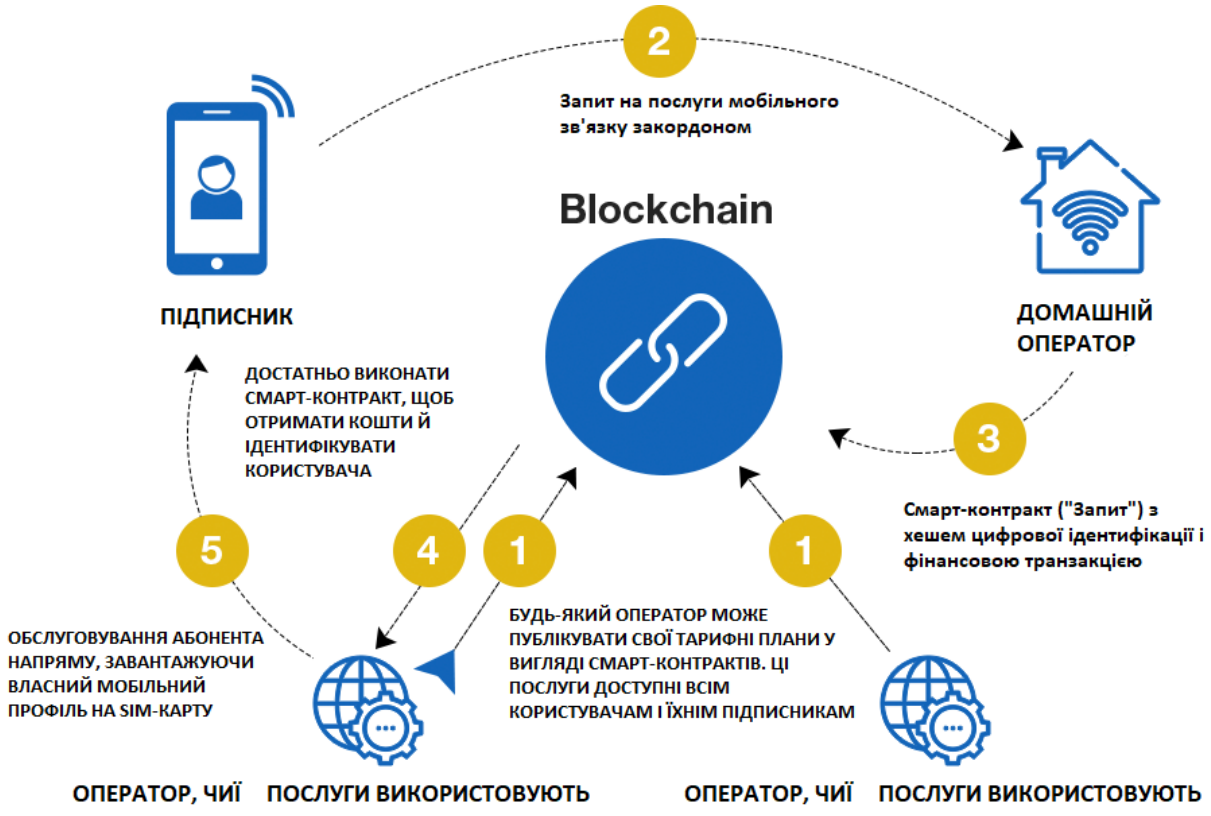

Рис. 3.1. BubbleTone і принцип його роботи

3.1.2. PoC блокчейн-рішення від IBM для роумінгу

Дві провідні компанії Syniverse та IBM об’єднали зусилля для створення рішення наступного покоління для роумінгу на базі технології blockchain з відкритим кодом. Ця розробка створена для того, щоб забезпечити

координацію та виконання смарт-контрактів між мобільними операторами. Розумні контракти дають можливість визначати правила та процеси й регулювати транзакції між сторонами. Така можливість допоможе підвищити ефективність роботи клієнтів та спростить вирішення суперечливих питань у бізнесі.

Проблема: провайдери послуг зв'язку (CSP) часто зустрічають проблеми, які пов'язані з абонентами роумінгових CSP мереж. Вони не завжди мають чітке бачення діяльності своїх абонентів у таких системах. Надання платежів для роумінгових клієнтів вимагає як більшого часу так і посередництва третіх сторін. Також залишається актуальною проблема, яка коштує провайдерам понад 40 мільярдів доларів щорічно: виявлення та запобігання шахрайства. Зловмисники можуть отримати доступ до домашньої мережі абонента, клонуючи його особу роумінгового користувача. Blockchain об'єднує ці CSP в єдину мережу, що дозволяє безпосередньо обмінюватися інформацією з транзакціями, які незмінні та виконуються на базі смарт-контрактів.

Рішення

Бізнес-модель на рис. 3.2. включає:

- SubscriberSims, які представляють собою MSISDN – присвоєний SIM-картці телефонний номер користувача, який використовується для здійснення і отримання дзвінків.
- CSPs, які діють як домашній оператор чи роумінговий партнер SubscriberSims

Рис. 3.2. Бізнес-модель використання blockchain компанії IBM

Таке рішення передбачає чотири сценарії використання:

- Ідентифікація абонентів у роумінгу – SubscriberSim подорожує у інше місце, яке не є частиною домашньої мережі. Якщо визначається, що він присутній у мережі роумінгового партнера за допомогою функції виявлення і автентифікований як користувач, то його тарифи оновлюються за допомогою функції updateRate.
- Виставлення рахунків абонентам у роумінгу. Після того, як SubscriberSim авторизується – він може використовувати мережу роумінгового партнера для дзвінків. Функції callOut та callEnd використовуються для початку дзвінка та його завершення. Кошти за користування мережею розподіляються між домашнім оператором та роумінговим партнером на основі згори, зазначеною у смарт-контракті. Функція callPay обчислює витрати за кожен дзвінок. [12]
- Ідентифікація шахрайства – додається шахрайський SubscriberSim з таким же MSISDN як і існуючий. Функція автентифікації ідентифікує цього користувача як зловмисника та позначає його SubscriberSim певною позначкою у базі. Це не дає змогу створювати будь-які дзвінки таким шляхом.

- Управління ресурсами – абонент у роумінгу здійснює дзвінок, одразу виконується функція callOut. Смарт-контракт визначає той момент, коли абонент досягає граничного значення ресурсів, які доступні йому за певним тарифним планом. Оператор сповіщає користувача про цю ситуацію та визначає можливі зміни тарифу. Абонент має два шляхи: прийняти чи відмовитися від нових платежів. Відповідь абонента записується у базу, а наступні дзвінки (включаючи поточний) або відбуваються за новим тарифом, або відхиляються. Ситуація залежить від прийнятого абонентом рішення. [12]

Переваги blockchain рішення компанії IBM:

- Автоматичне регулювання контрактів між домашнім та роумінговим оператором
- Миттєва обробка операцій без залучення третіх сторін, що призводить до економії коштів як операторів так і користувачів
- Надійне управління ідентифікацією користувачів для унеможливлення шахрайства
- Сповіщення у режимі реального часу про проблеми, пов’язані з тарифним планом

3.1.3. Концепція мережі IRBIS на базі технології blockchain

Проблема: сучасні мобільні технології потребують додаткового захисту користувачів від можливих кібератак. В результаті зловмисник може керувати параметрами профілю користувача, адресою HLR, в якому зберігаються дані параметри, а також адресу VLR, де зберігається інформація про те, в якому регіоні знаходиться абонент. Також зловмисники можуть займатися перехопленням SMS чи прослуховування телефонних розмов.

Рішення

Компанія SC Telecom розробляє новий продукт IRBIS, задача якого – підвищити конфіденційність телефонних дзвінків по всьому світу. Вся економіка проекту поділена на дві частини: фіатну і криптовалютну.

Функціональність фіатної частини забезпечує можливість користувачам вносити кошти на баланс, щоб здійснювати дзвінки та відправляти повідомлення. SafeCalls Telecom – канал, який виконує функції абонентського білінгу, тобто знімає кошти з рахунків і здійснює платежі операторам зв'язку за використані канали зв'язку.

Фіатна частина має форму централізованої бази даних в доларах США з балансами і абонентськими операціями, що необхідно для правильного розрахунку платежів користувачів, а також для розрахунку комісій, які відправляються в децентралізовану частину системи SafeCalls Telecom.

Децентралізована частина SafeCalls Telecom складається з маршрутизаторів – вузлів мережі, а також блокчейна, який виконує декілька функцій: зберігання тарифів зв'язку різних операторів, реєстраціє маршрутизаторів в мережі, передача платежів, а також виконання смарт-контрактів, згідно яким виконується розрахунок плати за використання роутерів мережі. [12]

Фіатна частина використовується для здійснення дзвінків, мобільного трафіку, зберігання анонімності: зміна чи приховування номеру телефону, зміна тембру голосу.

Рис. 3.3. Принцип роботи мережі IRBIS

Перевагами такого блокчейн-рішення є підвищена захищеність персональних даних користувача, яка передбачає унеможливлення відслідковування його дій, та без можливості прослуховування його розмов.

3.1.4. Cisco блокчейн-платформа

Cisco тривалий час займається розробкою блокчейн-платформи, яка спрямована на вирішення вимог використання у різних галузях. Саме ядро платформи складається з декількох рівнів, кожен з яких містить декілька служб, які налаштовуються за допомогою певних інтерфейсів. Платформа містить рівень комунікацій та базу даних, до них підключається механізм на базі штучного інтелекту. Також платформа містить ідентифікаційний рівень та рівень захисту інтересів користувачів. Останній відповідає за ідентифікацію, дотримання користувацьких правил. Інфраструктурний рівень платформи відповідає за захист та аналітику. Окрім, своєї блокчейн-платформи Cisco

створює «екосистему», яка має на меті об’єднання провайдерів, розробників програмного забезпечення та консультаційних партнерів з метою створення галузевих рішень для підприємств.

Платформа заснована на використанні смарт-контрактів. Рівень комунікації і розподілення відповідає за можливість блокчейн-вузлів взаємодіяти один з одним в умовах консенсусу. Оцінюючи будь-яку нову технологію блокчейн для підприємства, важливо враховувати простоту розгортання та управління мережею. Також важливою є можливість інтеграції з уже існуючими системами організації. На допомого приходять інтерфейси, які виконують необхідну функціональність для виконання цілей, метою яких є підвищення простоти використання.

Платформа надає можливу підтримку вибору інфраструктурних технологій, включаючи апаратні модулі. Апаратно-незалежний блок визначає набір стандартів для уникненню ризиків безпеки на рівні інфраструктури.

Одним із варіантів використання блокчейн-платформи Cisco є відслідковування пристроїв, які підключені до мережі Інтернет. З метою забезпечення надійного підключення до мережі та спостерігання за активністю. Стрімкий розвиток IoT дозволяє спрогнозувати кількість підключених девайсів до мережі Інтернет станом на 2023 рік,- ця кількість буде в районі 20 мільярдів пристроїв. У сенсі IoT ідентифікація і управління пристроями є основною задачею для підтримки життєдіяльності усієї мережі. Тому Cisco блокчейн-платформа знайде своє застосування у майбутньому.

Рис. 3.4. Архітектура Cisco-блокчейн-платформи

3.2. Можливості застосування blockchain у телекомунікаційних системах

3.2.1. Автентифікація користувача в роумінгу на базі технології blockchain

Сфера телекомунікацій стрімко розвивається у наш час. Однак, сьогодні оператори зв'язку використовують застарілу технологію сигналізації, яка використовується для автентифікації роумінгових користувачів. Основною характеристикою є велика затримка розпізнавання користувачів. Іноді вони змушені чекати до 15-ти хвилин для того, щоб отримати авторизацію послуг роумінгу. Оскільки, ми звикли до миттєвого відгуку програм, звикли до швидкостей сучасного світу, то ця затримка є занадто довгою.

Другим недоліком сучасної системи є використання системи сигналізації SS7. ЇЇ незахищеність було показано ще більше, ніж 10 років тому, однак він все ще залишається у використанні. Було досліджено, що зловмисник має можливість відправляти в мережу запити протоколів рівня додатків, які можуть призвести до реалізації різних загроз. Використовуючи недоліки захищеності мереж операторів мобільного зв'язку, зловмисник може отримати доступ до інформації про абонента (IMSI, місцеположення, поточний баланс

чи деталі профілю) та інформації про оператора. Також він може здійснити перехоплення абонентського трафіку, здійснювати різного роду маніпуляції з платіжною системою.

Поряд з вищезгаданими недоліками розташована вартість послуг. Телекомунікаційні оператори витрачають великі кошти для автентифікації користувачів. Вони платять за систему, яка не відповідає вимогам.

Рішення

Розв'язанням вищезгаданих проблем є використання мережі зв'язку на базі технології blockchain. Вона полегшить процес надання послуг від операторів до користувачів. Це рішення буде засновано на базі сучасних методів шифрування, наприклад, SHA-3. За допомогою нього кожен оператор отримає пару відкритих та приватних ключів. Ідея полягає в тому, щоб створити реєстр відкритих ключів для кожного постачальника для подальшої взаємодії з іншими операторами. Цей реєстр сприяв би прямому зашифрованому зв'язку авторизованих служб для роумінгових запитів, що дозволяє досягти спільного покращення у необхідній сфері.

Зацікавленими сторонами такого рішення є оператори зв'язку, тоді, як отримувачами послуг є як постачальники та і їх користувачі. GSMA представляє інтереси операторів мобільної мережі у всьому світі і, ймовірно, буде однією з організацій, яка дасть поштовх мобільним операторам.

Архітектура

На рис. 3.5. схематично зображено інтерфейси та деякі основні компоненти. Використовуючи рішення на базі технології blockchain, оператори отримують перевагу у вигляді спільних стандартизованих схем на обробку транзакцій. Таке рішення має високу захищеність, оскільки використовує сучасні методи шифрування та має менший час відгуку. VPMN – відвідана загальнодоступна мережа, яку використовує абонент під час

роумінгу. Цей термін використовується на відміну від домашньої суспільної мережі – HPMN.

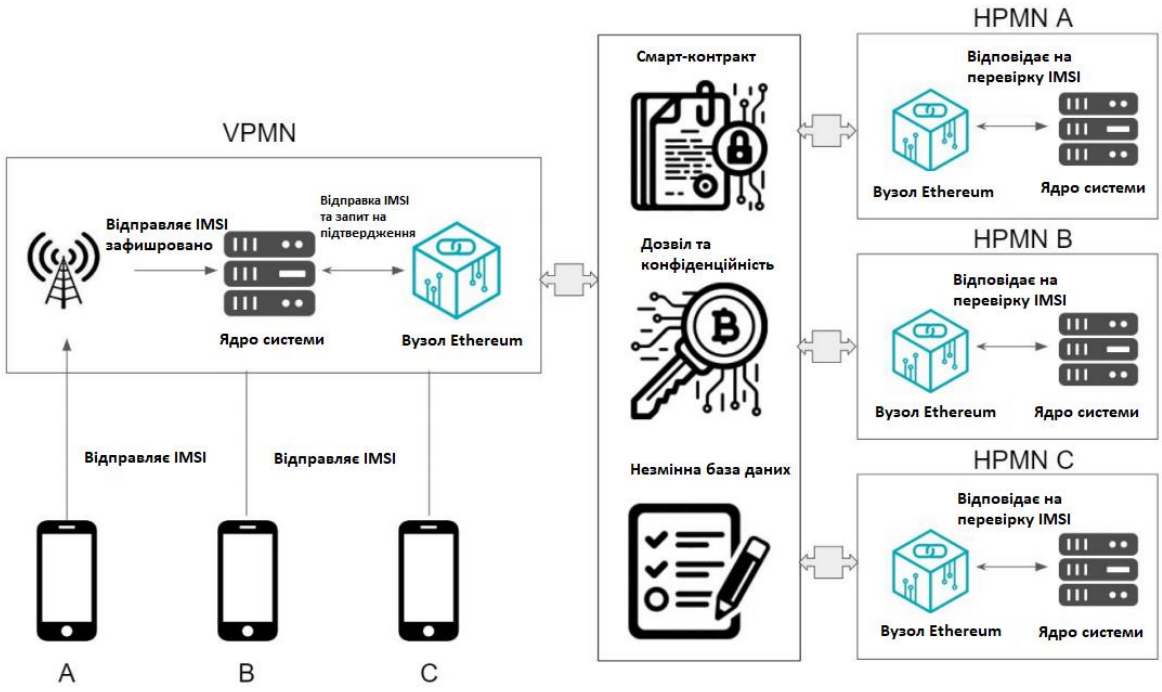

Рис. 3.5. Архітектура системи автентифікації користувача у роумінгу на базі технології blockchain

3.2.2. Узгодження взаємодії операторів у ромінгу на основі blockchain

Створення та підтримка роумінгових сервісів – важлива частина роботи телекомунікаційних компаній. Однак, це має бути зручним для операторів при управлінні сервісів. Оскільки, зменшення затрат на ці роботи для провайдерів призведе до зниження вартості послуг для користувачів.

Взаємодія операторів щодо транзакцій, які пов’язані з роумінгом є досить складною процедурою. Вона представляє собою великі затрати на компанії, які займаються передачею оплати від одного провайдера до іншого. Сумісне використання послуг – необхідне та складне і повинне включати фінансові відносини з урахуванням законів певних країн. Розглядаючи нову систему узгодження дзвінків у роумінгу виникають проблеми зі захистом

персональних даних та захистом від шахрайства; обробка великих об’ємів даних; захищеність обміну даними між компаніями.

Рішення

Для вирішення цієї проблеми різні компанії, які займаються мобільним роумінгом, створили консорціум. За допомогою нього оператори можуть обмінюватись даними напряму через блокчейн-мережу. Таке рішення використовує децентралізовану базу даних та P2P мережу для підтримки незмінюваності даних та забезпечення можливості розширення системи. За допомогою цього консорціуму роумінг-контракти можуть створюватися, поширюватися, перевірятися та підтверджуватися. Вони засновані на основі смарт-контрактів в рамках блокчейн-мережі. Серед інших можливих видів застосування роумінг-контрактів є:

- Створення журналу дзвінків у роумінгу зі списком оплати за послуги та розрахунок вартості самих послуг
- Переадресація журналу викликів користувача на домашнього оператора
- Створення та відправка запиту на оплату послуг від домашнього оператора до роумінгового
- Підтвердження виставлених рахунків та реєстрація журналу викликів домашнім оператором
- Узгодження платіжного балансу між операторами без застосування третіх сторін
- Простий аналіз руху коштів та можливість дослідження сумнівних операцій

Переваги архітектури

За допомогою вдосконаленого роумінгового рішення телекомунікаційні компанії зможуть швидше обробляти інформацію про використання послуг і співвідносити це з договором користувача. Така можливість забезпечить більшу прозорість та швидше оброблення послуг із зменшенням сервісних

зборів. Для телекомунікаційних компаній переваги таких рішень є в зменшенні витрат на обслуговування, покращення безпеки системи та збільшення кількості клієнтів.

Технічні примітки

- Дані мережі і реєстру можуть бути представлені у відкритому доступі на основі технології blockchain, в той час як приватні транзакції та дані можуть шифруватися та оброблятися надскладними алгоритмами
- Використання алгоритму консенсусу забезпечить відображення потреби пропускної здатності. Довірені сторони можуть валідувати та верифікувати транзакції
- Обробка даних може бути зведена до мінімуму шляхом передачі лише відповідних даних у роумінговий вузол оператора

Переваги

1) Прозорість операцій між роумінговими партнерами забезпечена як взаємним спостереженням так і за допомогою технології blockhain. Можливість створення багатосторонніх договорів на основі консенсусу з перевіркою усіх транзакційних записів.

2) Смарт-контракти забезпечать автоматичне виконання договорів між усіма сторонами. Роумінговий оператор може отримувати інформацію про користувача, надавати йому послуги та записувати журнал викликів до сумісної blockhain мережі. Домашній оператор може підтверджувати журнал викликів з журналу роумінгового оператору та виставляти і отримувати оплату за послуги.

3) Обробка в реальному режимі часу допоможе миттєво обробляти транзакції та підтримувати баланс між операторами. Ця можливість допоможе провайдерам знати фактичні витрати в кожен момент часу для підтримки бізнес-прогнозів.

4) Зменшення витрат усуне значну кількість паперових документів та зменшить витрати на обмін коштів між операторами. Завдяки смарт-контрактам, провайдери мають спільні важелі рішень.

3.2.3. Конфіденційність даних та монетизація

Телекомунікаційні оператори по всьому світу стикаються з проблемами збільшення витрат на підтримку інфраструктури та зі збільшенням попиту користувачів на отримання все більших об’ємів даних. Все це спричиняє жорстку конкуренцію серед телекомунікаційних компаній. Одним із головних викликів, які постали перед операторами – збереження конфіденційності інформації. Оскільки, у сучасному світі стрімко розвивається політика конфіденційності інформації, тому цей процес передбачає захищення даних, якими володіють абоненти: різні документи, зображення, інформацію про особу абонента, інформацію про вибір хмарного сховища. Також він передбачає захищеність даних, які створили самі користувачі: текстові повідомлення SMS, місцеположення, вказані інтереси, придбані послуги, платежі. Телекомунікаційні компанії використовують лише ті дані для обробки, на які користувачі надали дозвіл. Однак, все частіше застосовується розширена аналітика, яка використовує масивні централізовані дані поряд з передовими методами машинного навчання. Все це дозволяє дослідити все більше про своїх користувачів.

Таке профілювання часто проводиться в різних групах чи категоріях. Проаналізовані дані можуть містити високоточні оцінки інтересів користувачів та дослідження їх активності. За допомогою цієї інформації телекомунікаційні компанії можуть оптимізувати ділову практику та процеси, включаючи оптимізацію створення інфраструктури.

Проблема

Реальність ситуації полягає в тому, що навіть, якщо користувачі представлять пряму всебічну згоду на використання даних, вони можуть бути

не чітко проінформовані про обсяг аналізу цих даних та не зовсім розуміти для чого компанії будуть використовувати цю інформацію. У більшості випадків абоненти не отримують грошової винагороди від такої інформації. Тим часом у світі поширюється обізнаність користувачів про «важливість» та «цінність» даних посилюється. Прийняття GDPR в ЄС причинить зростання рівнів викликів організаціям, які займаються обробкою великих об'ємів даних. Режим GDPR містить заходи щодо згоди чи інших законних підстав для обробки даних та повернення контролю над особистими даними користувачам.

General Data Protection Regulations (GDPR) – загальні положення про захист даних стосуються три основні питання. Вони включають як відстеження даних, конфіденційність та право бути забутим. Розглянемо три основні питання GDPR.

1) Як відслідковувати персональні дані – персональні дані містяться у багатьох програмах, які охоплюють велику кількість серверів, центрів обробки даних, постачальників послуг, тобто, усі місця де вони зберігаються. GDPR вимагає, щоб була можливість отримувати доступ, повідомляти та видаляти особисту інформацію, коли цього вимагає користувач, або певний регулятивний орган. Відстеження цього потоку даних є складним процесом, який вимагає певного рівня захищеності.

2) Конфіденційність архітектури – це питання вирішує різні підходи до побудови архітектури системи, враховуючи ризики конфіденційності та відповідність захищеності даних. Такі проекти включають розробку нових IT-систем, розробку нових фінансових продуктів та створення нової політики обміну даними з третіми сторонами.

3) Право бути забутим – дозволяє фізичним особам отримати від контролюючого органу видалення усіх особистих даних без найменших затримок. Ця особа просто відкликає згоду, на основі якої відбувалася обробка даних.

Рішення

Технологія blockchain може забезпечити різноманітність децентралізованих сервісів там, де це роблять учасники. Тобто, не потрібно створювати чи встановлювати попередню довіру до інших учасників. Смарт-контракти можуть бути цілком придатними для вирішення проблеми, з якими стикаються телекомунікаційні провайдери. Оскільки, будь-які дані, які зберігаються в системі blockchain можуть становити як персональні дані, так і дані розробки компанії і вони можуть цілком надійно шифруватися на основі цією ж системою. З точки зору права на забуття, особисті дані повинні зберігатися окремо в сховищі з криптографічним хеш-значенням, що може забезпечити мережа blockchain, до якої легко може звернутися абонент зі запитом на видалення особистих даних.

Переваги

Перевагою такого рішення для абонентів є покращення збереження особистої інформації, можливістю обміну її з вибраними сторонами. Технологія blockchain може використовуватися як спосіб надання права власності на дані, або позначки тої інформації, на яку надійшов запит на видалення від абонентів.

Постачальник послуг може отримати вигоду за рахунок встановлення нових відносин зі своїм абонентом, де він може дослідити потреби свого користувача та надати йому сервіси на основі аналізу даних. Конфіденційність даних та прав власності абонентів можуть підтримуватися більш прозорими та незмінними методами, ніж це використовується зараз.

3.2.4. Використання blockchain для 5G включення

5G - революційна технологія в мобільних телекомунікаціях, яка обіцяє стати швидшою в 20 разів, ніж сучасна 4G технологія. 5G може використовуватися для нових бізнес-моделей, які потребують взаємодії з

різними сторонами, включаючи операторів мобільного зв'язку, державних регуляторів та керівників інфраструктури. В той час як blockhain показав себе як сприятливу технологію з необмеженим потенціалом для використання у різних сферах. Ця технологія все частіше використовується для ідентифікації, реєстрації та валідації активів та транзакцій, регулювання взаємодії, запису даних між декількома сторонами. Вибір найшвидшого і найближчого вузла незабаром стане головним завданням телекомунікаційних компаній. Blockchain дозволяє увімкнути такі механізми вибору.

Сьогодні системи зв'язку централізовані й організовані на базі моделі клієнт-сервер, де усі правила, що зберігаються на сервері – застосовуються щодо користувача. Така модель спричиняє затримки і не дозволяє безперешкодно забезпечувати пристрій мережею. Мережі доступу до GPRS, WiMAX, WLAN та Wi-Fi у певній області можуть бути об'єднані в блокчейн мережу, де кожна точка доступу, наприклад, маршрутизатор Wi-Fi чи стільникова базова станція можуть слугувати вузлом мережі. Правила взаємодії між різними мережами встановлені у смарт-контрактах, які мають динамічний характер, тому, у разі зміни політики необхідно лише змінити код договору. Коли пристрій транслює своє місцеположення, вузол доступу, який має найкращу швидкість може надавати послугу користувачу. Це призводить до безперебійної взаємодії між мережею та користувачем та простої оплати всіх послуг між різними вузлами. Наприклад, якщо WLAN з офісу чи домашньої мережі забезпечив доступ до пристрою, то криптографічний провайдер у свою чергу зменшить рахунок відповідно до положення компанії.

Швидке зростання об'ємів даних в мобільної мережі 5G виявили необхідність рішення інноваційних рішень для захисту та забезпечення ефективного обміну даними через ненадійне середовище. Абоненти не задумуються де знаходиться їх персональна інформація та як вона захищена і вони мають дуже обмежену можливість контролю цих даних. Blockchain може вирішити цю проблему, оскільки він забезпечує підвищення ефективності

обміну даними в мережі 5G, є прозорим, незмінюваним та стійким до зовнішнього впливу. Децентралізована архітектура дозволяє отримувати оброблені запити користувачів через розподілені вузли, що значно зменшує будь-які затримки.

Архітектура такого рішення називається мета-ключем, де ці ключі зберігаються в децентралізованому сховищі у вигляді метаданих, захищених приватним ключем. Спільні дані можуть зберігатися у хмарному сховищі. Blockchain може захищати мобільні мережі, проводити транзакції на дуже детальному рівні, тоді як 5G буде відповідати за навантаження мережі.

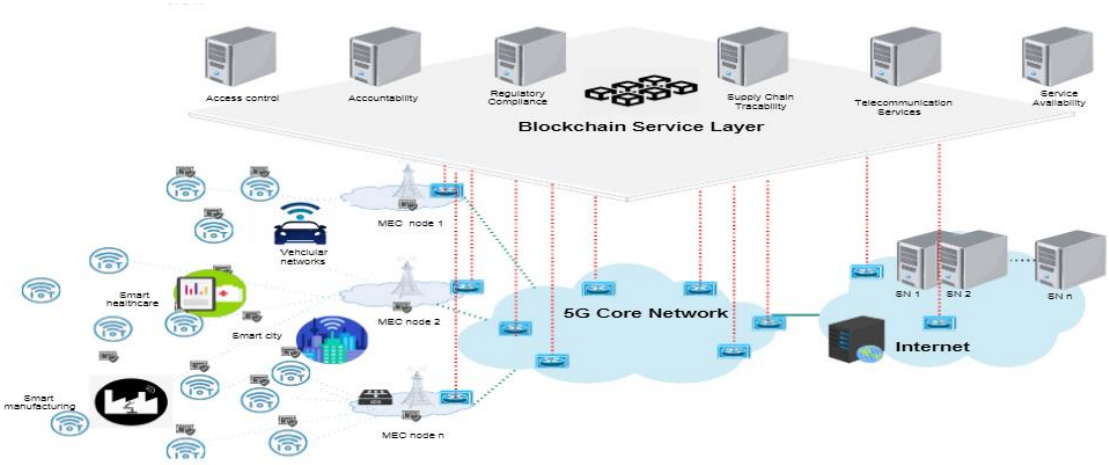

Рис. 3.6. Використання blockhain сумісно з 5G

3.2.5. Використання blockchain для IoT

Сьогодні дуже стрімко розвивається сфера Інтернету Речей, підключення якої досягнуть мільярдів уже незабаром. Основна проблема полягає в тому, що зростання IoT прямо пропорційно збільшує незахищеність даних. Підключення Інтернету Речей створюють серйозні проблеми: потреба забезпечення мільярдів взаємодій між різними машинами та потреба захисту приватної інформації, яка передається через пристрої. Як результат, усе це потребує неймовірних коштів на обслуговування та розвиток. Децентралізоване управління на основі блокчейн дозволяє забезпечити більш

масштабовану безпеку IoT та забезпечує прозору перевірку і захист від втручання.

Blockchain дозволяє використовувати безпечні однорангові мережеві вузли, які працюють одночасно і можуть бути представлені через одиничні вбудовані сенсори IoT з можливістю перевірки кожного блоку в мережі блокчейн.

В сфері Інтернету Речей blockchain може застосовуватися для збереження інформації сенсорів, забезпечення безпеки шляхом ідентифікації окремого IoT пристрою та його захисту від злому, спрощення налаштування мережі та здійснення оплати за послуги.

По-перше, blockchain – це та технологія, яка забезпечує безпеку. У контексті Інтернету Речей, де безпека є дуже головним аспектом – ця технологія дуже перспективна.

По-друге, масштабованість – блокчейн-мережі можуть впоратися з дуже великими об’ємами даних. За допомогою цієї технології можливо значно швидше отримувати та передавати інформацію, що дуже важливо у сучасному світі.

По-третє, необхідно розподілити права та обов’язки користувачів та виробників. Наприклад, якщо пристрій, встановлений пацієнту, завдає шкоди пацієнту, то хто в цьому випадку має понести покарання.

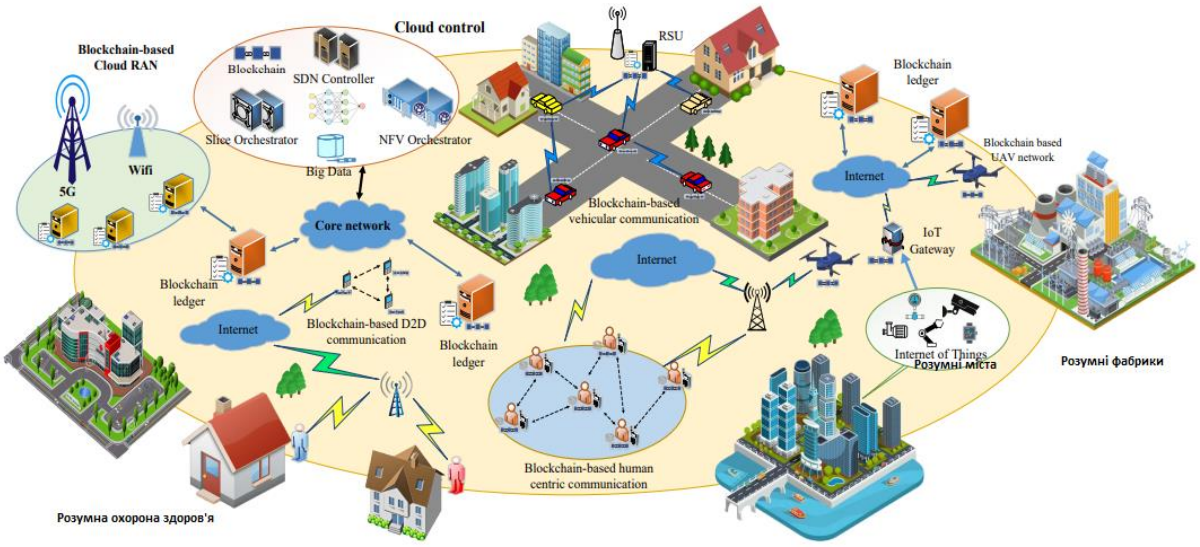

Рис. 3.7. Співіснування IoT та blockchain

Технологія blockchain може забезпечити просту інфраструктуру для двох пристроїв, щоб безпосередньо передавати дані між собою, чи передавати кошти за допомогою захищеного та надійного контрактного сеансу зв'язку. Для обміну використовуються уже відомі смарт-контракти, які моделюють угоду між двома сторонами.

Переваги використання тандему IoT-blockchain:

1) Відстежування активів в режимі реального часу під час переміщення по багаточисельному ланцюгу
2) Проста перевірка дотримання договорів
3) Незмінюваність записів, що дозволяє уникнути зайвих суперечок
4) Надійність збереження даних, які обробляються і записуються за певними галузевими стандартами з дотриманням законодавств.

Висновки до третього розділу

По-перше, в цьому розділі були досліджені та наведені приклади основних ідей застосування технології blockchain у телекомунікаційних системах. Були розглянуті рішення провідних компаній. Також було

проаналізовано основні сфери застосування цієї технології у сучасних телекомунікаційних системах.

Як бачимо, певні компанії дослідили перспективи використання технології blockchain та розробляють свої блокчейн-рішення для тих чи інших ситуацій. Було досліджено переваги використання блокчейну у цих системах. Тому ми бачимо, що blockchain перспективний у використанні для роумінгу.

Перевагами блокчейну у вищезгаданих системах є надійність збереження персональних даних, захищеність голосових дзвінків та текстових повідомлень. Відсутність посередників, тобто, третіх сторін. Підвищена продуктивність систем при використанні сучасних методів конфіденційності. Недоліком на даний час є складність реалізації стабільної роботи, та відсутність великої кількості підготовлених кадрів, оскільки, ця технологія є достатньо новою.

По-друге, були досліджені переваги застосування blockchin. Перед усім, сфери які працюють з даними користувачів, мають детально захистити їх від шахраїв. На вирішення цієї проблеми приходить блокчейн, оскільки зміна одного блоку призводить до недостовірності усього ланцюга.

По-третє, аналіз перспектив застосування blobckchain у телекомунікаційних системах показав такі переваги: уникнення доступу до даних небажаних сторін та надійність їх збереження; вища продуктивність системи при роботі з великими об’ємами даних; використання сучасних криптографічних методів шифрування. Серед недоліків може стати складність реалізації системи на різних етапах, оскільки, blockchain – нова технологія, яка все ще розвивається.

ВИСНОВКИ

В ході дипломної роботи було досліджено актуальність вибраної теми. Було ознайомлення з історією розвитку технології blockchain. Було досліджено основні принци роботи мережі blockchain, та розглянуто основні компоненти: асиметричні алгоритми шифрування, смарт-контракти, хеш-функції, хеш-таблиці, алгоритми консенсусу, поняття «майнінгу».

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 дослідження можливості застосування технології blockchain у різних телекомунікаційних системах. Розглянуто технологічні рішення на базі blockchain та доцільність її використання в різних телекомунікаційних системах, досліджені переваги застосування blockhain для вирішення тої чи іншої задачі. Розглянуто блокчейн-рішення компанії IBM, блокчейн-платформу компанії Cisco, концепцію мережі IRBIS та блокчейн-рішення BubbleTone.

Було розглянуто розглянемо можливі телекомунікаційні рішення на основі blockchain: автентифікацію користувача у роумінгу, узгодження взаємодії операторів у роумінгу, конфіденційність даних та їх монетизацію, використання blochchain для 5G включень та для IoT

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

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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

2. Cryptography Hash functions [Електронний ресурс]. Режим доступу до ресурсу: https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm

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

4. Майнинг [Електронний ресурс]. Режим доступу до ресурсу: https://ru.bitcoinwiki.org/wiki/%D0%9C%D0%B0%D0%B9%D0%BD%D0%B8%D0%BD%D0%B3

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

7. What’s a Peer-to-Peer (P2P) Network? [Електронний ресурс]. – 2002. - Режим доступу до ресурсу: https://www.computerworld.com/article/2588287/networking-peer-to-peer-network.html

8. 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

9. Что такое децентрализация биткоин и криптовалют [Електронний ресурс]. – 2019. - Режим доступу до ресурсу: https://prostocoin.com/blog/decentralization

10. BubbleTone - первая децентрализованная телекоммуникационная экосистема. [Електронний ресурс]. – 2018. - Режим доступу до ресурсу: https://cyberway.golos.io/@ambicia/5blgxw-bubbletone-pervaya-decentralizovannaya-telekommunikacionnaya-ekosistema

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

12. 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/