Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
(повна назва інституту/факультету)

Кафедра телекомунікацій
(повна назва кафедри)

«На правах рукопису»
УДК 004.056.5

До захисту допущено
В.о. завідувача кафедри

_____ Явіся В.С.
(підпис) (ініціали, прізвище)
“___”_____2019_р.

Магістерська дисертація

на здобуття освітнього ступеня «магістр»

Спеціальність 172 Телекомунікації та радіотехніка,
(код і назва)

За освітньо-професійною програмою Інженерія та програмування інфокомунікацій.

на тему: Дослідження можливості використання технології blockchain в телекомунікаційних системах

Виконав: студент 2 курсу, групи ТМ - 81мп

Іванов Іван Іванович
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник доцент, к.т.н. с.н.с. Міночкін Д.А.
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

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

Рецензент доцент каф. ТС, к.т.н Созонник Г.Д. _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.

Студент _____
(підпис)

Київ – 2019 рік

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
(повна назва інституту/факультету)

Кафедра телекомунікацій
(повна назва кафедри)

Спеціальність 172 Телекомунікації та радіотехніка
(код і назва)

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою Інженерія та програмування інфокомунікацій.

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Явіся В.С.
(підпис) (ініціали, прізвище)
«___»_____2019 р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Іванову Івану Івановичу

1. Тема дисертації Дослідження можливості використання технології blockchain в телекомунікаційних системах
науковий керівник дисертації доцент кафедри ТК Міночкін Д.А.,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету від «_07_» «_11_» 2019р. № 3840-с

2. Строк подання студентом дисертації 1 грудня 2019 р.

3. Об'єкт дослідження технологія Blockchain, як база даних в телекомунікаційних системах
4. Предмет дослідження можливість використання технології blockchain в телекомунікаціях
5. Перелік завдань, які потрібно розробити:
   1) Визначення технології blockchain, його принципи та функції.
   2) Аналіз сфер використання blockchain, його доцільність в цих сферах.
   3) Аналіз можливості реалізації blockchain в телекомунікаційних системах, розгляд варіантів впровадження blockchain.

6. Орієнтовний перелік ілюстративного матеріалу 14 рисунків

7. Орієнтовний перелік публікацій -

8. Консультанти розділів дисертації

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

9. Дата видачі завдання 20 вересня 2018

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
1	Написання першого розділу, постановка завдання на магістерську дисертацію.	20 вересня 2018р.	
2	Розгляд технології Blockchain, визначення її складових. Перший розділ.	1 грудня 2018р.	
3	Опис складових, на яких базується Blockchain. Другий розділ.	17 березня 2019р.	
4	Огляд компаній та розділів в них, де застосовується технологія blockchain. Третій розділ.	10 вересня 2019р.	
5	Огляд сфер, де можна застосувати blockchain в телекомунікаційних системах. Четвертий розділ.	1 листопада 2019р.	
6	Оформлення роботи. Підготовка ілюстративного матеріалу та доповіді.	1 грудня 2019р.	

Студент _____ _____

Науковий керівник дисертації _____ _____

УДК 004.056.5

РЕФЕРАТ

Робота містить 79 с, 14 рис., 11 джерел.

API, BLOCKCHAIN, IOT, БАЗА ДАНИХ, ХЕШ-ФУНКЦІЇ, СМАРТ-КОНТРАКТ, ХЕШУВАННЯ ДАНИХ, РОУМІНГ, КРИПТОСИСТЕМА

Об’єктом дослідження є технологія Blockchain, як технологія бази даних в телекомунікаційних системах.

Мета роботи: Вивчення основних компонентів технології blockchain. Аналіз принципів функціонування blockchain, способів передачі, обробки та зберігання даних. В ході роботи були розглянуті вже існуючі рішення на базі технології blockchain, а також розроблені варіанти впровадження технології blockchain в різних телекомунікаційних системах. В результаті, було розглянуто декілька варіантів в сфері телекомунікацій, де доцільно користуватись технологією blockchain. Результати роботи можуть бути використані для подальшого розгортання телекомунікаційних систем.

ABSTRACT

The work contains 79 pages, 14 figures, 11 sources.

API, BLOCKCHAIN, IOT, DATABASE, HASH FUNCTIONS, SMART CONTRACT, DATA HASHING, ROAMING, CRYPTOSYSTEM

The object of the study is Blockchain technology, as a database technology in telecommunications systems.

The purpose of the work: To study the main components of blockchain technology. Analysis of the principles of blockchain operation, methods of data transmission, processing and storage. In the course of the work, existing solutions based on blockchain technology were considered, as well as variants of implementation of blockchain technology in various telecommunication systems were developed. As a result, several options for telecommunications have been considered, where it is advisable to use blockchain technology. The results can be used to further deploy telecommunication systems.

Пояснювальна записка
до магістерської дисертації

на тему: Дослідження можливості використання технології blockchain в телекомунікаційних системах

Київ – 2019 року

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

API – Application Programming Interface (інтерфейс або протокол зв'язку між клієнтом і сервером)

ATM – Asynchronous transfer mode (Асинхронний режим передачі даних)

CLI – Command-line interface (Інтерфейс командного рядка)

CSP – Communications Service Provider (додатковий рівень безпеки, який допомагає виявляти та пом’якшувати певні типи атак, включаючи міжсайтові сценарії (XSS) та атаки введення даних)

EEA – Enterprise Ethereum Alliance (галузева організація під керівництвом членів, мета якої - використовувати технологію блокчейн Ethereum як відкритого стандарту для розширення можливостей BCIX підприємств)

ESP – Encapsulating Security Payload (шифрування даних)

ETH – Ether (відкрита, публічна, розподілена обчислювальна платформа на основі блокчейна та операційна система, що має функціональні можливості смарт-контрактів (сценаріїв).)

EVM – Ethereum Virtual Machine (Віртуальна машина Ethereum)

HTTP – Hyper Text Transfer Protocol (протокол передачі гіпертексту)

IP – Internet Protocol address (Інтернет протокол)

IoT – Internet of Things (система взаємопов’язаних обчислювальних пристроїв, механічних і цифрових машин, предметів, тварин або людей, яким надаються унікальні ідентифікатори та можливість передачі даних по мережі без необхідності використання людиною людиною або людиною до комп'ютера)

NEXT – відкрита, публічна, розподілена обчислювальна платформа на основі блокчейна та операційна система, що має функціональні можливості смарт-контрактів (сценаріїв).

IPSec – Internet Protocol Security (Безпека інтернет протоколу)

IMSI – International Mobile Subscriber Identity (міжнародна ідентифікація мобільного абонента)

LLN – Low power and Lossy Networks (мережа малої потужності та втрати)

LTE – Long-Term Evolution (стандарт бездротового широкосмугового зв'язку для мобільних пристроїв та терміналів передачі даних, заснований на технологіях GSM / EDGE та UMTS / HSPA)

ВСТУП

Актуальність. Телекомунікаційні компанії пов'язують людей один з одним через телефони і інтернет по кабелю або по бездротовому зв'язку. Індустрія телекомунікацій виявляється застарілою, оскільки вона заснована на картах модулю ідентифікації абонента (SIM), які були розроблені ще в 1991 році. Доброю новиною є те, що SIM-карти поступово замінюються картами eSIM, які являють собою цифровий чіп, який робить ту ж роботу. Але недостатньо просто задовольнятися зручною і швидкою установкою плат нового покоління, і тому оператори звертаються до блокчейну, який знає, як правильно обробляти дані.

Blockchain - це база даних, яка підтримує постійно зростаючий набір даних. Зараз Blockchain - одна з найбільш широко обговорюваних та відкритих технологій. Ця технологія несе в собі можливість зруйнувати бізнес-моделі в багатьох галузях, включаючи телекомунікації, і може підвищити прозорість та ефективність процесу.

Великою перевагою blockchain є те, що він є загальнодоступним. Усі учасники можуть бачити блоки та транзакції, що зберігаються в них. Це не означає, що кожен може бачити фактичний вміст транзакції; він захищений вашим приватним ключем.

Мета роботи.

Для досягнення мети роботи було поставлено та вирішено такі задачі:

1) Вивчення основних компонентів технології blockchain;
2) Аналіз принципів функціонування blockchain, способів передачі, обробки та зберігання даних;
3) Аналіз вже існуючих рішень на базі технології blockchain;
4) Розробка варіантів впровадження технології blockchain в різних телекомунікаційних системах.

1. ЩО ТАКЕ BLOCKCHAIN, ІСТОРІЯ ЙОГО ВИНИКНЕННЯ

Метою даного розділу є розгляд технології blockchain та основних сфер його призначення. В рамках даного розділу сформулюємо визначення основної мети та завдання blockchain у сучасному світі інформаційних технологій. Розгляд технології blockchain та його цілей має стати гарним підґрунтям знань, що необхідні для повноцінного аналізу функціональності та вимог до сучасних рішень у даній сфері.

1.1 Історія виникнення blockchain

Blockchain - це розподілена база даних, яка підтримує постійно зростаючий набір даних. Це зростаючий список записів, званих блоками, які пов'язані за допомогою криптографії. База захищена від підробки та переробки. Кожен блок містить криптографічний хеш попереднього блоку, часову позначку та дані транзакцій. Блокчейн поширений у природі, тобто це означає, що не існує одного головного комп'ютера, який би тримав всі дані в одному порядку.

За задумом, блокчейн стійкий до модифікації даних. Це "відкрита, розподілена книга, яка може ефективно і оперативно фіксувати транзакції між двома сторонами". Для використання в якості розподіленої книги, блокчейн, як правило, керується одноранговою мережею, яка колективно дотримується протоколу для міжвузлового зв'язку та перевірки нових блоків. Після запису дані в будь-якому даному блоці не можуть бути змінені заднім числом без зміни всіх наступних блоків.

Перша робота над криптографічно захищеним ланцюжком блоків була описана в 1991 році Стюартом Хабер та У. Скотт Сторнеттом. Вони хотіли запровадити систему, в якій не можна було б підробити часові позначки документів.

Блокчейн був винайдений людиною (або групою людей), що використовували прізвище Сатоші Накамото в 2008 році, для того щоб служити головним журналом транзакцій для крипловалюти Bitcoin. Особа Сатоші Накамото невідома. Винахід блокчейна для біткойна зробив його першою цифровою валютою, яка вирішила проблему подвійних витрат без необхідності довіреного органу чи центрального сервера. З моменту винайдення та формулювання принципів роботи мережі ця технологія зазнала чималих змін та популярності в світі.

2011 рік

- У лютому запускається інтернет-ринок Silk Road. Анонімні користувачі купують і продають (в основному нелегальні) товари в Bitcoin. Криптовалюта бере на себе основну увагу поганої преси.
- У той же час ціна 1 біткойна досягає 1 долара, стимулюючи інтерес. Більше людей починають видобувати біткойн.Сатоші передає підтримку коду Bitcoin. Він або вона залишає щонайменше 50 біткоінів у гаманці (які існують і донині) і зникає.
- Перші пошуки терміна "blockchain" починають з'являтися в Google.
- Оскільки код Bitcoin є відкритим кодом (доступний для населення), люди починають робити власні монети. На сцену з’являються Namecoin, Litecoin і Swiftcoin. Всі вони мають свій погляд на глобальну валюту.

2013 рік

- ФБР припиняє Шовковий шлях та заарештовує свого власника, звинувачуючи його у в'язниці.
- У Флориді, США, притулок для бездомних людей починає приймати біткойни.
- Зростає інтерес до інших підприємств, пов'язаних з блокчейном. Pantera Capital, перша американська інвестиційна фірма Bitcoin інвестує в обмін

криптовалют Coinbase, Circle і Bitstamp.

- Віталік Бутерин, 19-річний розробник, який був співавтором журналу Bitcoin, має бачення нового виду криптовалют. Той, який може зробити більше, ніж просто здійснити платежі. Він пропонує це у газеті під назвою "Ethereum: Смарт контракт нового покоління та децентралізована платформа додатків".
- Після величезного зростання цін Bitcoin досягає 1000 доларів, але одразу впаде знову і не досягає такої ж висоти до 2017 року.
- Китай забороняє своїм банкам торгувати біткойнами.

2015 рік

- NASDAQ розпочинає випробування блокчейну для підвищення швидкості, ефективності та зниження вартості.
- Barclays, Credit Suisse, Goldman Sachs, JP Morgan та RBS утворюють новий блокчейн-консорціум під назвою R3.
- Ethereum запускає власний блокчейн.
- Capital One, Visa, Citi Ventures та NASDAQ інвестують у Chain, компанію, що будує приватні блокчейн для бізнесу.
- Американське фінансове агентство FinCEN Ripple Labs оштрафує на 700 000 доларів США за продаж своїх криптовалют XRP без попередньої реєстрації у них.
- Найбільша у світі некомерційна організація з відкритим кодом, Linux Foundation, запускає Hyperledger - набір інструментів, які допомагають людям створювати блокчейн-проекти.

2018 рік

- Американський штат Арізона та Швейцарія приймають податки в біткойн.
- Камерна компанія Kodak оголошує про плани створення власного KodakCoin. Акції піднімаються на 60%.

- Криптовалюта EOS збирає $ 4 млрд на найбільшому ICO коли-небудь. Багато хто вважає, що одного разу замінить Ethereum.
- Консенсус, найбільша щорічна конференція блокчейнів у світі, досягає 4000 відвідувачів. У 2015 році їх було всього 400.
- МВФ (Міжнародний валютний фонд) заявляє, що "криптовалюти становлять обмежену загрозу для фінансової стабільності".
- Іспанська банківська група BBVA, швейцарський багатонаціональний інвестиційний банк UBS та Microsoft виявляють інтерес до смарт-контрактів на основі блокчейна.
- За даними Forbes.com, майже 15% фінансових компаній сьогодні використовують блокчейн.

Великою перевагою blockchain є те, що він є загальнодоступним. Усі учасники можуть бачити блоки та транзакції, що зберігаються в них. Це не означає, що кожен може бачити фактичний вміст транзакції.

Можливість поширювати інформацію по мережі без її копіювання між учасниками мережі – саме так Блокчейн створив основу для нового типу даних у всесвітньому інтернеті. Оригінальна розробка технології була спрямована на винайдення нового слова в сфері цифрових валют – криптовалют, таких як Bitcoin (укр. (дослівно) Цифрова бітова монета), ETH (Ethereum), Bitcoin Cash та інших. Але, з часом, спеціалісти в технічній сфері почали винаходити нові варіації і потенціали блокчейну та його похідних.

Блокчейн це незламний цифровий кластер для запису змін в мережі, що може бути запрограмовано не тільки на запис грошових і фінансових транзакцій, але й будь яких інших існуючих значень – будь-якого типу інформації в світі.

1.2 Основні поняття в технології blockchain

Блокчейн складається з двох типів елементів:

Операції - це дії, створені учасниками системи.

Блоки записують ці транзакції і переконуються, що вони в правильній послідовності та не були підроблені. Блоки також записують позначку часу, коли транзакції додаються.

В основу технології блокчейн – роботу всіх механізмів закладено використання таких технологій та методів роботи і шифрування даних:

- *Асиметричні алгоритми шифрування* або «асиметричні криптосистеми» (пари "приватних" та "публічних" ключів);

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

- *Хеш-таблиці* для запису результатів хешування – операцій в блоках транзакцій (використання хеш-дерева типу "Дерево Меркла");

- *Смарт-контракти* (англ. Smart Contracts) – метод передачі даних (цифрових цінностей) від однієї особи до іншої;

- *Токени* та реалізація механізму Proof of concept (POC) – доказ концепції, як методу верифікації події (затвердженняугоди) в системі.

Визначимо поняття кожного вище зазначеного терміну з переліку.

Асиметричні алгоритми шифрування – захист даних в мережі Blockchain, що передаються від користувача.

Хеш - це як відбиток пальця (довгий запис, що складається з деяких цифр і літер). Кожен блок-хеш генерується за допомогою алгоритму криптографічного хешу (SHA 256 наприклад). Отже, це допомагає легко ідентифікувати кожен блок у структурі blockchain. З моменту створення блоку він автоматично приєднує хеш, тоді як будь-які зміни, внесені в блок, впливають і на зміну хеша. Простіше сказано, хеші допомагають виявити будь-які зміни в блоках.

Асиметричні криптосистеми – ефективні системи криптографічного захисту даних, які також називають криптосистемами з відкритим ключем. В таких системах для зашифровування даних використовують один ключ, а для розшифровування – інший (звідси і назва – асиметричні). Перший ключ є відкритим і може бути опублікованим для використання усіма користувачами системи, які шифрують дані.

Розшифровування даних за допомогою відкритого ключа неможливе. Для розшифровування даних отримувач зашифрованої інформації використовує другий ключ, який є секретним (закритим). Ключ розшифровування не може бути визначеним з ключа зашифровування.

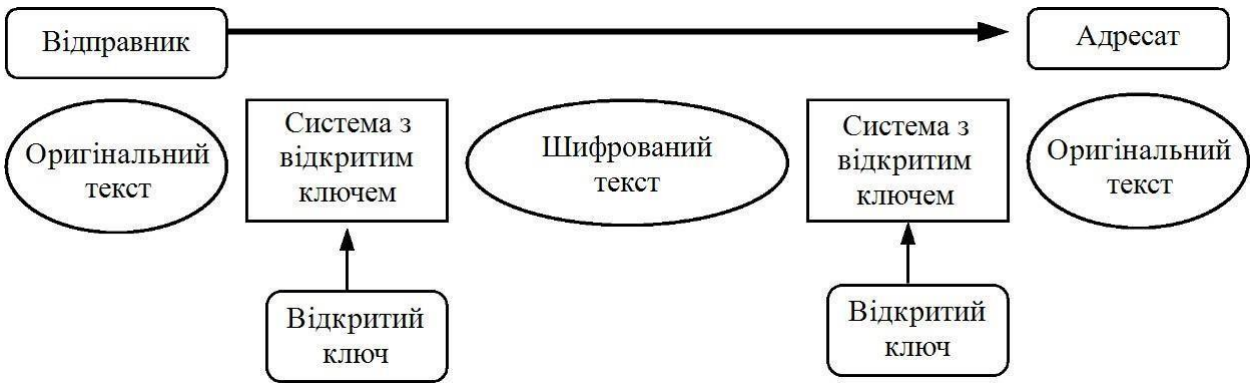

Рис. 1 Схема передачі даних в асиметричних криптосистемах

Блокчейн децентралізований, тому не існує єдиного органу, який може затвердити транзакції або встановити конкретні правила для прийняття транзакцій. Це означає, що існує велика довіра, оскільки всі учасники мережі повинні досягти консенсусу для прийняття транзакцій.

Цифрова сигнатура або електронний підпис (англ. signature – підпис) – це рядок символів, що залежить як від відправника так і від змісту повідомлення (рис. 1.2).

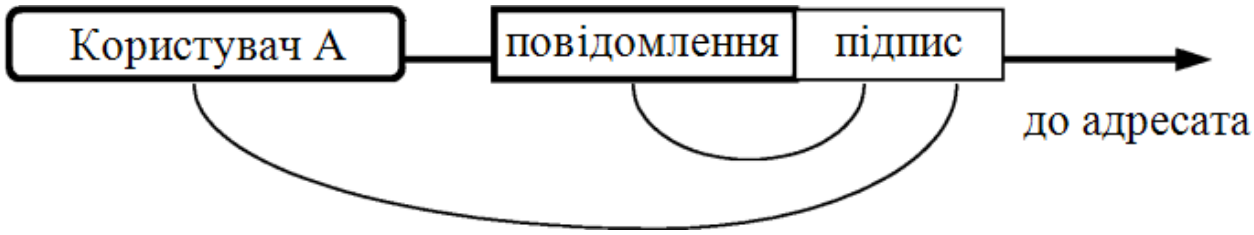

Рис. 2 Цифрова сигнатура як частина самого повідомлення

Жоден учасник мережі крім користувача А (відправника) не може визначити формат підпису для кожного конкретного повідомлення. Жоден, включаючи самого користувача, не може змінити змісту повідомлення так, щоби підпис залишався незмінним. Хоч і отримувач повідомлення мусить мати змогу перевірки підпису на належність до відправника. Для перевірки валідності цифрового підпису користувач В (отримувач), має надати інформацію третій особі С (мережа або сервер верифікації підписів) про те, які самі дані було використано для перевірки сигнатури. Якщо повідомлення передається безпосередньо від відправника до адресата, виключаючи третю сторону, то в такому випадку мова йде про “самобутній цифровий підпис”.

Тим не менш, навіть така схема цифрового підпису успішно використовується в цифрових системах, де має виконуватися два простих правила: необхідність аутентифікації / інформаційного впізнання та обов'язкове шифрування повідомлень, що передаються в мережі.

Блокчейн може забезпечити захищені, доступні цифрові версії для всіх сторін угоди, а розумні контракти можна використовувати для управління робочим процесом схвалень та автоматичного переказу платежу за всі зібрані підписи.Blockchain дозволяє різним сторонам, які не знають і не довіряють одна одній, підтримувати консенсус щодо стану змін, внесених до загальної книги. Обсяг потенційних застосувань широкий і стосується майже кожної галузі, що викликає широкий інтерес та інвестиції в блокчейн-інтеграцію за останні кілька років.

1.3 Постановка завдань на магістерську дисертацію

Можливість поширювати інформацію по мережі без її копіювання між учасниками мережі – саме так blockchain створив основу для нового типу даних у всесвітньому інтернеті. Метою даної роботи є розгляд технології blockchain, особливостей його функціонування, а також огляд основних blockchain-рішень в різноманітних сферах телекомунікаційних систем.

Для досягнення мети роботи було поставлено та вирішено такі задачі:

1) Вивчення основних компонентів технології blockchain;

2) Аналіз принципів функціонування blockchain, способів передачі, обробки та зберігання даних;

3) Аналіз вже існуючих рішень на базі технології blockchain;

4) Розробка варіантів впровадження технології blockchain в різних телекомунікаційних системах.

Висновки до розділу

1. Blockchain - це принципово нова надійна технологія зберігання записів, яка може кардинально змінити підхід до формування і зберігання баз даних. Зараз це одна з найбільш широко обговорюваних та відкритих технологій. Ця технологія несе в собі можливість зруйнувати бізнес-моделі в багатьох галузях, включаючи телекомунікації, і може підвищити прозорість та ефективність процесу.

2. Оригінальна розробка технології була спрямована на винайдення нового слова в сфері цифрових валют – криптовалют, таких як Bitcoin, ETH (Ethereum), Bitcoin Cash та інших.

3. Великою перевагою blockchain є те, що він є загальнодоступним. Усі учасники можуть бачити блоки та транзакції, що зберігаються в них. Це не означає, що кожен може бачити фактичний вміст трансакції; захищений вашим приватним ключем.

4. Блокчейн це незламний цифровий кластер для запису змін в мережі, що може бути запрограмовано не тільки на запис грошових і фінансових транзакцій, але й будь яких інших існуючих значень – будь-якого типу інформації в світі.

2. ПРИНЦИПИ ТА ФУНКЦІЇ BLOCKCHAIN

Завданням другого розділу є огляд основних архітектур blockchain, опис принципів їх роботи. Ця інформація має вказати на основні особливості роботи цієї технології, вказати на основні переваги та недоліки. Другий розділ дає уявлення про роботу технології. В третьому розділі буде зосереджено основну увагу, показано які завдання вирішує blockchain в телекомунікаційних системах вже зараз.

2.1 Принципи побудови blockchain

Технологія blockchain дозволяє поширювати цифрову інформацію, а не копіювати її. Ця розподілена книга забезпечує прозорість, довіру та безпеку даних.

Blockchain архітектура використовується дуже широко у фінансовій галузі. Проте в наші дні ця технологія використовується не тільки для криптовалют, але і для ведення діловодства, цифрового нотаріусу та розумних контрактів.

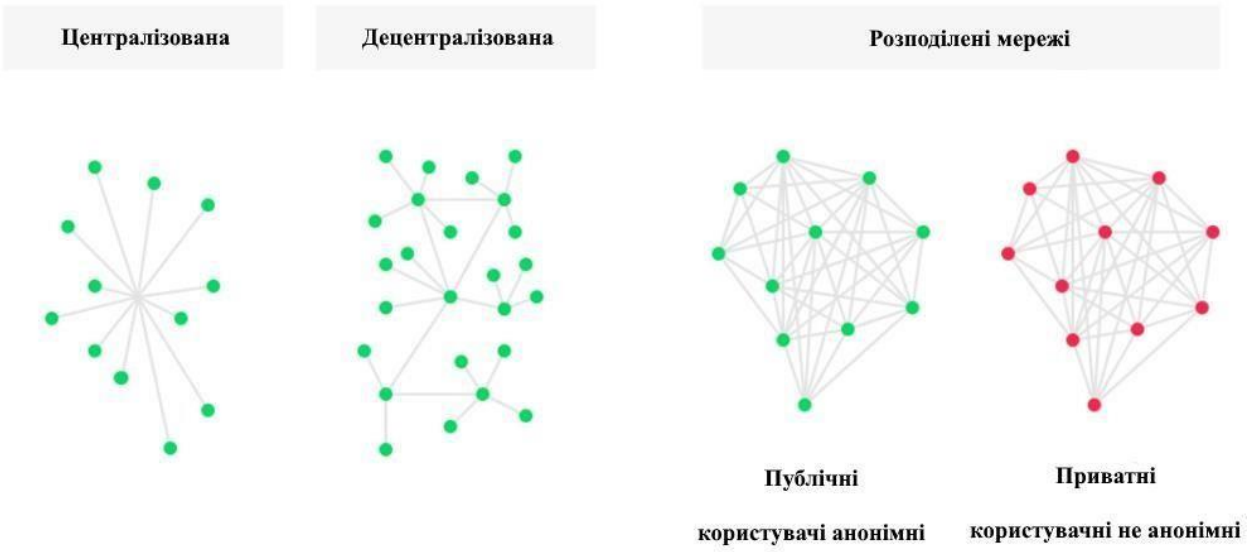

Рис.3 Архітектура блокчейн мережі

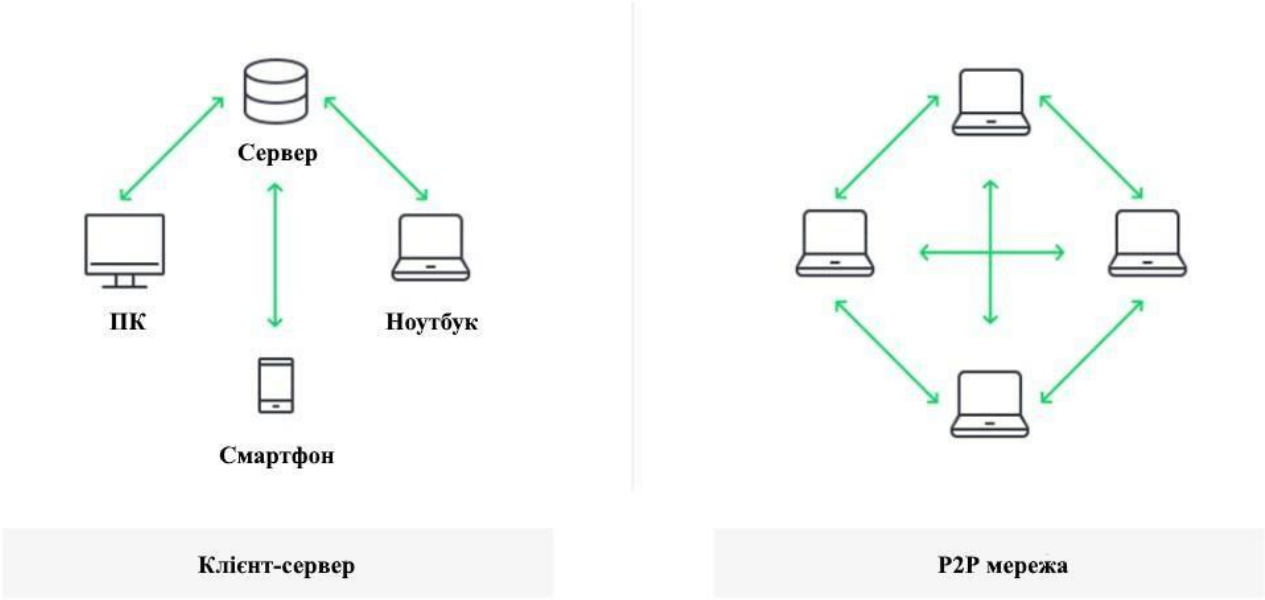

Рис.4 Порівняння архітектури “Клієнт-сервер” “P2P”

Традиційна архітектура всесвітньої павутини використовує мережу клієнт-сервер. У цьому випадку сервер зберігає всю необхідну інформацію в одному місці, щоб його було легко оновлювати, оскільки сервер є централізованою базою даних, керованою низкою адміністраторів з дозволами.

Що стосується розподіленої мережі архітектури blockchain, кожен учасник мережі підтримує, затверджує та оновлює нові записи. Системою керують не лише окремі люди, а й усі в межах блокчейн-мережі. Кожен член забезпечує, щоб усі записи та процедури були в порядку, що призводить до достовірності даних та безпеки. Таким чином, сторони, які не обов’язково довіряють одна одній, здатні досягти спільного консенсусу.

Кожен блок блокчейн складається з:

- певні дані
- хеш блоку
- хеш із попереднього блоку

Дані, що зберігаються всередині кожного блоку, залежать від типу блокчейна. Наприклад, у структурі блокчейн Bitcoin блок підтримує дані про приймача, відправника та кількість монет.

Підсумовуючи, блокчейн – це децентралізована, розподілена книга (державна чи приватна) різного роду транзакцій, організованих у мережу P2P.

Ця мережа складається з багатьох комп’ютерів, але таким чином, що дані не можуть бути змінені без консенсусу всієї мережі (кожного окремого комп’ютера).

2.2 Архітектура і класифікація blockchain мереж

Усі структури блокчейну поділяються на три категорії:

Публічна архітектура блокчейна

Загальнодоступна архітектура блокчейна означає, що дані та доступ до системи доступні всім, хто бажає брати участь (наприклад, системи блокчейн Bitcoin, Ethereum та Litecoin є загальнодоступними).

Приватна блокчейн-архітектура

На відміну від публічної архітектури blockchain, приватна система контролюється лише користувачами певної організації або авторизованими користувачами, які мають запрошення на участь.

Архітектура блокчейна консорціуму

Ця структура blockchain може складатися з декількох організацій. У консорціумі процедури встановлюються та контролюються попередньо призначеними користувачами.

Важливим фактором успіху для blockchain в архітектурі підприємства є проміжне програмне забезпечення. Їх необхідно інтегрувати між собою та кількома іншими системами, протоколами зв’язку та технологіями в режимі реального часу.

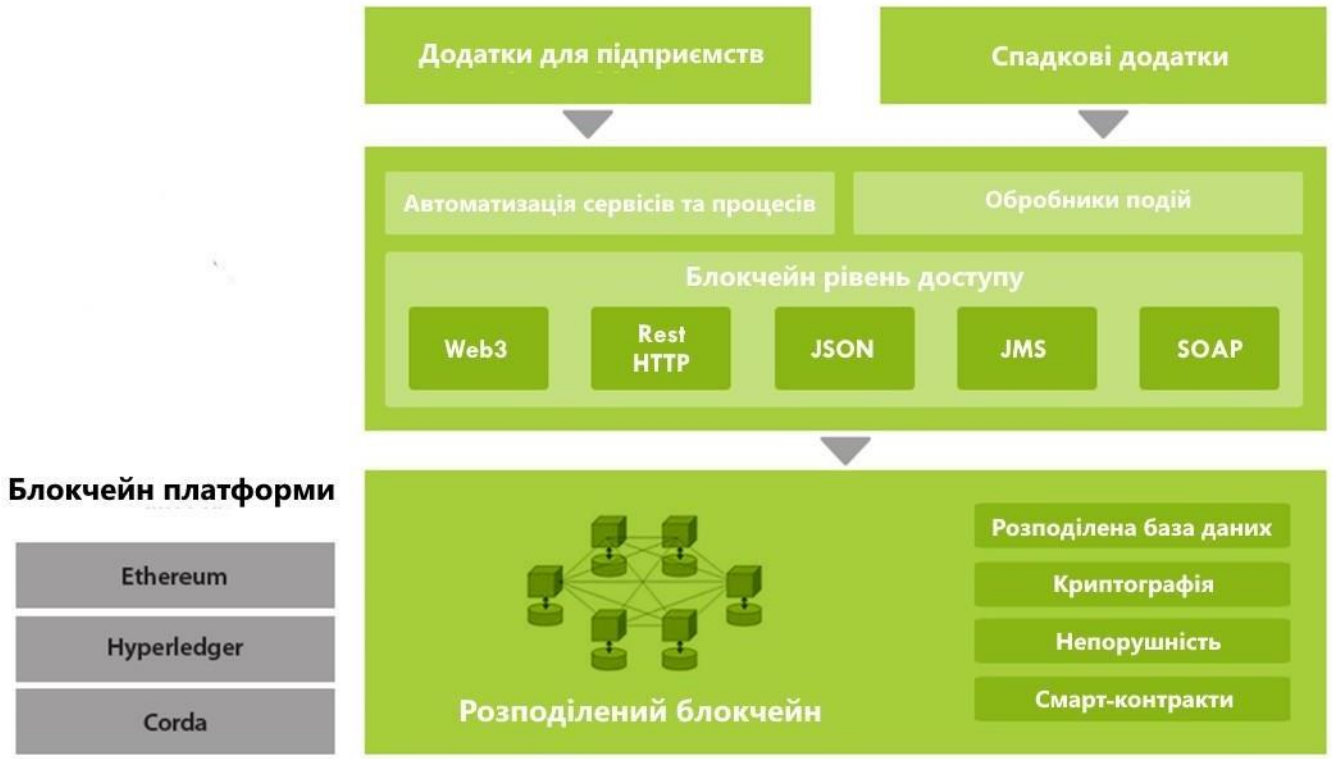

Рис.5 Рівні архітектури в blockchain

Blockchain проксі-рівень

Проксі-рівень blockchain вводиться для створення рівня абстракції між базовим стеком базових технологій blockchain та інтегрованими додатками чи послугами. Під час спілкування за допомогою цього рівня всі блокчейни виглядають однаково, знижуючи рівень залежності від обраної технології та дозволяючи розв'язати архітектуру рішень. Зауважимо, що, враховуючи стан сучасних стеків технологій blockchain, досягти повністю загального проксі-рівня може бути важко, оскільки можливості та підходи часто сильно різняться між рішеннями.

Однак використання мікропослуг системного рівня, що поєднують загальновживані функції блокчейна, може полегшити створення такого проксі-рівня.Щоб існуючі програми безперебійно працювали з blockchain, потрібен шар доступу :

1) Впоратися зі складнощами інтеграції блокчейн-системи та смарт-контрактів;

2) Інтерфейс з функціональними можливостями програми blockchain та передавання їх застарілим програмам;

3) Мати повну видимість кожної події в мережі блокчейн;

4) Дозволить блокчейн-події запускати процеси в позаланцюгових та мережевих додатках.

5) Забезпечити управління та зменшити ризики мережі блокчейн.

Смарт контракти

Blockchain програми виходять далеко за межі своїх перших областей додатків у віртуальній валюті, що дозволяє не тільки виконувати прості транзакції, але й проводити обчислення в мережі, де, наприклад, виплати стають умовними станом деяких внутрішніх чи зовнішніх змінних, виконання яких не потребує втручання людини.

Смарт контракти - самовиконання коду на блокчейні, який автоматично реалізує умови угоди між сторонами - є важливим кроком вперед, впорядковуючи процеси, що в даний час поширюються в декількох базах даних та застарілих системах. Замість статичних об'єктів даних, які вставляються в розподілену книгу, смарт-контракт - це програма, яка може виконувати генерацію подальших дій при дотриманні відповідних умов. Вони стають непорушними лише після того, як їх приймають до книги. Правила ведення бізнесу закладені в контракт, який може автоматично запускатися на основі певних умов. Наприклад попередня кваліфікація кредиту або активи, передані після здійснення платежу або після надання законного затвердження тощо.

Це не контракти в юридичному розумінні, а компоненти програмного забезпечення, що розширюють корисність блокчейну від простого ведення обліку записів фінансових транзакцій до автоматичного виконання умов багатопартійних угод. Смарт контракти виконуються мережею вузлів за допомогою протоколів консенсусу і після їх розгортання в блокчейні смарт-контракт завжди працює і відповідає на запити. По суті, це знижує потребу в сторонніх наглядах, оскільки саме програмне забезпечення є контрольованою та відкритою основою, видимою для всіх учасників трансакції, що дозволяє сторонам домовлятися про умови, знижуючи ризик помилок чи маніпуляцій.

Як уже згадувалося, blockchain - це розповсюджений журнал, де всі учасники мають місцевий примірник. Однак, виходячи з типу структури блокчейна та його контексту, система може бути більш централізованою або децентралізованою. Це просто стосується дизайну архітектури блокчейну та того, хто контролює головну книгу.

Приватний блокчейн вважається більш централізованим, оскільки він контролюється певною групою з підвищеною конфіденційністю. Навпаки, публічний блокчейн є відкритим і таким чином децентралізованим.

У загальнодоступному блокчейні всі записи видимі громадськості, і кожен бажаючий може взяти участь у процесі узгодження. З іншого боку, це менш ефективно, оскільки потрібно багато часу, щоб прийняти кожен новий запис в архітектуру блокчейна.

Основні компоненти архітектури Blockchain:

Вузол - користувач або комп'ютер в архітектурі блокчейна (кожен має незалежну копію всієї книги блокчейн)

Транзакція - найменший будівельний блок блокчейн-системи (записи, інформація тощо), який служить метою блокчейн

Блок - структура даних, що використовується для зберігання набору транзакцій, який розподіляється на всі вузли мережі

Ланцюг - послідовність блоків у визначеному порядку

Майнери - конкретні вузли, які виконують процес перевірки блоку, перш ніж щось додати до структури блокчейн

Consensus (консенсус-протокол) - сукупність правил та домовленостей щодо здійснення блокчейн-операцій

Будь-який новий запис або транзакція всередині блокчейна передбачає побудову нового блоку. Кожен запис потім перевіряється та цифровим підписом, щоб забезпечити його справжність. Перед тим, як цей блок буде доданий до мережі, його слід перевірити більшістю вузлів у системі.

2.3 Основні функції blockchain

Кожен новий користувач (вузол), який приєднується до однорангової мережі blockchain, отримує повну копію системи. Після створення нового блоку він надсилається кожному вузлу в системі blockchain. Потім кожен вузол перевіряє блок і перевіряє, чи вказана там інформація є правильною. Якщо все в порядку, блок додається в локальний блокчейн у кожному вузлі.

Усі вузли всередині архітектури blockchain створюють консенсус-протокол. Система консенсусу - це сукупність мережевих правил, і якщо всі дотримуються їх, вони стають самозабезпеченими всередині блокчейна.

Blockchain архітектура має багато переваг для бізнесу. Ось кілька вбудованих функцій:

Криптографія - блокчейн-транзакції підтверджені та заслуговують на довіру завдяки складним обчисленням та криптографічним підтвердженням між залученими сторонами

Незмінність - будь-які записи, зроблені в блокчейні, не можна змінювати або видаляти

Походження - стосується того, що можна відстежити походження кожної транзакції всередині книги блокчейн

Децентралізація - кожен член структури блокчейн має доступ до всієї розподіленої бази даних. На відміну від центральної системи алгоритм консенсусу дозволяє контролювати мережу

Анонімність - кожен учасник блокчейн-мережі має згенеровану адресу, а не ідентифікацію користувача. Це зберігає анонімність користувачів, особливо в загальнодоступній структурі blockchain

Прозорість - система blockchain не може бути пошкоджена. Це навряд чи станеться, оскільки для повного перезапису блокчейн-мережі потрібно величезна обчислювальна потужність

Blockchain архітектура може слугувати наступним цілям для організацій та підприємств:

Скорочення витрат - багато грошей витрачається на підтримку централізованих баз даних (наприклад, банків, урядових установ), забезпечуючи безпеку даних від кібер-злочинів та інших корупційних намірів.

Історія даних - всередині структури blockchain можна перевірити історію будь-якої транзакції в будь-який момент часу. Це постійно зростаючий архів, в той час як централізована база даних є більш швидким знімком інформації в певний момент.

Дійсність та безпека даних - щойно введені, дані важко підробити через характер блокчейна. Щоб перевірити запис, потрібен час, оскільки процес відбувається в кожній незалежній мережі, а не через з'єднувальну потужність обробки. Це означає, що система жертвує швидкістю роботи, але натомість гарантує високу безпеку та надійність даних.

Рішення Blockchain призведуть до істотних змін у способі розробки та розгортання програм. Важливо, що технологія Blockchain здатна підключатися до різних систем основних застосувань, таких як ERP, CRM тощо, що дозволяє клієнтам досягти успіху в бізнесі. Однак, як обговорювалося раніше, блокчейн - це не завжди відповідь. Необхідно враховувати різні чинники, щоб визначити, чи він підходить.

З точки зору IT, блокчейн є важливою частиною основної діяльності підприємства, тому його мета безперешкодно інтегруватись з іншими застарілими системами.

Надалі рішення для інтеграції блокчейнів різних компаній або навітьгалузей зможуть безперебійно спілкуватися та ділитися цифровими активами.

Для підприємств, випадки використання яких залежать від блокчейн, потенційні переваги інтеграції є цілком зрозумілими: більше партнерських відносин в екосистемі, які можуть сприяти підвищенню вартості та рентабельності інвестицій.

Рис.6 Механізм роботи blockchain

Організації можуть використовувати інновації щодо можливостей блокчейну, які трансформують існуючі бізнес-процеси та з'єднують ці можливості в основні процеси.

Щоб дозволити організаціям брати участь у декількох блокчейнах, окремої інтеграції можна уникнути, маючи рівень доступу, інтегрований із системами запису, що полегшують участь у кількох блокчейнах.

Своєрідний Q&A про blockchain

Blockchain масштабується?

Щоб блокчейн працював, багатьом учасникам потрібно зберігати актуальні копії. Це означає, що однакова база даних утримується тисячами вузлів. Це досить неефективно.

Якби ми подивилися на те, як розвивалися технології за останні п’ятнадцять років, blockchain суперечить логіці, що стоїть за хмарними обчисленнями. Тенденції хмарних обчислень до єдиної бази даних, до якої можуть отримати доступ кілька вузлів. Ці вузли не повинні зберігати власну приватну копію цієї бази даних.

Крім того, вузли, що зберігають копії блокчейна, отримують постійні оновлення. Ці вузли поширені по всьому світу. Через це блокові ланцюги мають високу затримку (затримка - це кількість часу, необхідного для переміщення даних по мережі).Як результат, технологія blockchain стикається з масштабуючими проблемами. Біткойн може обробити близько 4-5 транзакцій в секунду. Ethereum максимумує близько 25 транзакцій в секунду. Visa може обробити понад 24 000 транзакцій за секунду.

Blockchain анонімний?

У перші дні Bitcoin технологія blockchain - як і багато технологій, що народжуються - в народі асоціювалася з незаконною діяльністю.Чому технологія blockchain на зразок Bitcoin була ефективною для такого типу підприємств? Незважаючи на те, що облік трансакцій Bitcoin є загальнодоступним, глобальний, децентралізований характер мережі означає, що жодна організація - як уряд США чи Visa - не може закрити її, заморозити кошти чи обернути транзакції. І в ті перші дні було дуже важко пов’язати гаманець Bitcoin з певною особою, навіть якщо були докази того, що гаманець використовувався в незаконній діяльності.

Однією з причин того, що Bitcoin набув більшої популярності як магазину цінних та фінансових інструментів, є те, що він вже не такий анонімний, як це було в перші дні. Більшість основних сервісів, які дозволяють купувати та продавати біткойн, використовують стандарти "знайте свого клієнта" (KYC), а правоохоронні органи стали більш досконалими у зв'язку з транзакціями Bitcoin з конкретними людьми. Є й інші проекти, які з'явилися у спробах використовувати технологію blockchain для захисту анонімності користувачів (наприклад, Monero та ZCash), але вони значно менші.

Blockchain економічний?

Одним із ключових моментів, щоб довгострокова технологія blockchain була життєздатною, - це гарантувати, що транзакції, на зразок Аліси та Боба, можуть здійснюватися з мінімальними комісіями. Гонорари важливі, оскільки вони стимулюють майнерів своєчасно додавати ваші транзакції до блокчейну - але високі збори ускладнюють переконання потенційних користувачів взяти участь у роботі.

У грудні 2017 року середня плата за транзакції в мережі Bitcoin досягла 34 доларів за транзакцію. Такі компанії, як Stripe і Valve, оголосили, що більше не прийматимуть оплату за біткойн через високі комісії.

Сьогодні середній розмір транзакцій у мережі Bitcoin становить близько 300 доларів, тоді як медіанна плата за транзакції коливається в межах 0,10 долара - це 0,03% медіанна плата за транзакції, що набагато краще, ніж 0,7% комісійних витрат.

Хоча збори знизилися, Bitcoin все ще не здатний до повсякденної комерції - платформа повинна вирішувати проблеми зі масштабуванням, часом блокування транзакцій тощо, перш ніж вона буде готова до великих ліг.

Висновки до розділу

1. Підсумовуюч, блокчейн - це децентралізована, розподілена книга (державна чи приватна) різного роду транзакцій, організованих у мережу P2P. Ця мережа складається з багатьох комп'ютерів, але таким чином, що дані не можуть бути змінені без консенсусу всієї мережі (кожного окремого комп'ютера).

2. Будь-які корупційні спроби провокують зміни блоків. Після цього всі наступні блоки несуть невірну інформацію та роблять всю блокчейн-систему недійсною.

3. Для резюме це робить технологію blockchain незмінною та криптографічно захищеною, усуваючи будь-яких сторонніх сторін. Не можна підробляти систему блокчейн; як це було б необхідним для вторгнення в усі його блоки, перерахуйте перевірку роботи кожного блоку, а також контролюйте понад 50% усіх вузлів в одноранговій мережі.

3. ДЕ ВИКОРИСТОВУЮТЬ BLOCKCHAIN ЗАРАЗ

Метою даного розділу є огляд компаній, що користуються технологією blockchain вже зараз, описом процесів, що мають відбуватися при передачі даних та їх реалізації, встановленні діалогів та сервіс-сесій в рамках даної концепції.

В рамках даного розділу розглянемо такі компанії, як BubbleTone, IBM та Cisco. В результаті матимемо картину доцільності blockchain в цих компаніях, визначимо його переваги та недоліки.

3.1 BUBBLETONE - блокчейн-рішення для управління тарифами на роумінг

Рис. 7 Логотипи роумінг компаній

Bubbletone - це телекомунікаційне рішення на основі приватної блокчейн мережі, яке забезпечує автономне регулювання платежів за міжнародний роумінг. Компанія надає більше 10 варіантів використання свого рішення.

Вибір “двигуна” блокчейн BubbleTone став Graphene, системою з відкритим кодом з перевіреним досвідом. Це платформа, яка дозволяє торгувати цифровими активами за допомогою смарт-контрактів, це спеціальні автоматизовані алгоритми, які гарантують прозорість та незмінність транзакцій.

Відповідно до децентралізованої філософії BubbleTone, вихідний код Graphene відкритий і керується спільнотою програмістів, яка вже кілька років переглядає його. Блокчейн телекомунікацій здатний безперешкодно інтегруватися з операторами через API, які вже працюють.

Швидкість - одна з найважливіших показників у галузі, що стоїть перед клієнтом, як телекомунікації. А мова програмування, на якій ґрунтується Graphene, C ++, забезпечує операції, при яких смарт контракти оброблятись за лічені секунди. Тести на блокчейн-платформі BubbleTone показали, що вона тепер може обробляти понад 10 тисяч транзакцій в секунду.

В оперативному режимі блокчейн BubbleTone потребує лише обмеженої кількості обчислювальної потужності та електроенергії завдяки делегованому консенсусу Graphene Proof of-Stake. Також блокчейн підтримується децентралізовано, при цьому нові учасники підлягають підтвердженню шляхом голосування всіма існуючими членами.

Каліфорнійська компанія ShoCard стала ключовим партнером BubbleTone для надання аутентифікації користувача. ShoCard - це провідна платформа управління цифровими ідентифікаторами на основі блокчейна, здатна перевіряти ідентичність користувачів без обробки будь-яких особистих даних.

Забезпечуючи найвищий рівень безпеки для інноваційних платформ, ShoCard вже керує ідентифікацією користувачів для галузей, де безпечна аутентифікація є критичною, включаючи операторів мережі кредитних карт, фінансових установ та авіакомпаній.

Оскільки багатонаціональні оператори телекомунікацій виявляють зацікавленість і набирають більше нових угод про партнерство, BubbleTone вже запустив ICO з 20 квітня 2018 року, щоб мати можливість додатково розширити та розширити платформу.

Інженери BubbleTone об'єднуються з вченими у сфері блокчейну у провідних університетах та академічних центрах у всьому світі, щоб зробити додаткові тести та огляди цієї унікальної реалізації Graphene. Код блокчейна BubbleTone доступний на GitHub.

Однією з основних цілей компанії є створення глобальної блокчейн-екосистеми в області телекомунікацій, яка дозволить забезпечити глобальний роумінг без спеціальних угод між постачальниками послуг.

3.2 PoC блокчейн-рішення від IBM для роумінгу

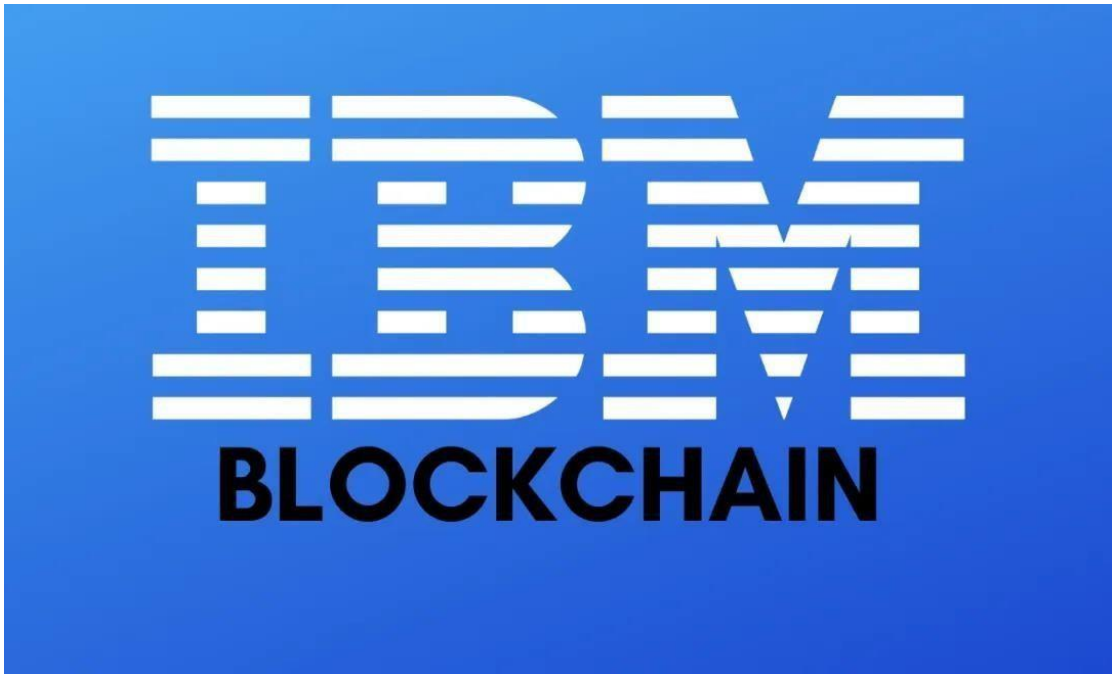

Рис. 8 Логотип блокчейн-рішення компанії IBM

IBM розробила рішення для багатьох телекомунікаційних компаній для управління роумінгом, запобігання шахрайства в мережах та стеження за перевитратою коштів компаній. PoC розроблений за допомогою Hyperledger Fabric і Hyperledger Composer.

Він демонструє прямий обмін інформацією через транзакції, які є незмінними і виконуються на основі консенсусної моделі з використанням правил, прописаних в смарт-контрактах.

Смарт-контракт – це програмний код, який містить інформацію про транзакцію (або, простіше, угоду) у форматі “якщо … тоді …”. Наприклад, “Якщо користувачем X буде занесено в систему 100 ETH, тоді він отримає 10 токенів N від користувача Y”.

Постачальники послуг зв'язку (CSP) часто стикаються із проблемами, пов’язаними з абонентами в роумінгових мережах CSP, і вони не завжди мають чітку видимість діяльності своїх абонентів у цих мережах. Узгодження платежів для роумінгових клієнтів потребує часу та вимагає посередництва сторонніх клірингових будинків із пов'язаними з цим витратами. Виявлення та запобігання шахрайству продовжують залишатися актуальними питаннями для більшості CSP , коштуючи понад 38 мільярдів доларів щорічно.

Шахрайські абоненти можуть отримати доступ до домашньої мережі CSP, клонуючи особу одного із роумінгових абонентів. Blockchain об'єднує ці CSP на єдину блокчейн мережу Hyperledger Fabric, що дозволяє безпосередньо обмінюватися інформацією з транзакціями, які незмінні та виконуються на основі модельного консенсусу, який використовує правила смарт-контракту. Це покращує видимість CSP перед платником, дозволяє швидке узгодження платежів та зменшує шахрайські транзакції до мінімуму.

Цей шаблон розробника показує, як налаштувати додаток для телекомунікаційного роумінгу за допомогою смарт-контрактів, які керують транзакціями, які виконуються SubscriberSims, які можуть переміщуватися через зони покриття різних CSP. Ці CSP можуть виступати або домашніми операторами, або роумінговими партнерами SubscriberSims для відстеження діяльності мобільних користувачів у мережі.

Ця бізнес-мережа включає:

SubscriberSims, які представляють єдиний номер міжнародного каталогу абонентів мобільної станції. Іншими словами, кожен SubscriberSim являє собою мобільний номер.

CSP, які виступають або домашнім оператором, або роумінговим партнером SubscriberSim.

Рис. 9 Шаблон екосистеми

У цьому кодовому шаблоні існує чотири сценарії:

1) Ідентифікація абонентів у роумінгу - SubscriberSim переміщується на нове місце, яке не є частиною його домашньої мережі. Якщо виявлено, що він присутній у мережі роумінгових партнерів за допомогою спеціальної функції і аутентифікований як дійсний користувач, то тарифи його викликів оновлюються за допомогою функції updateRate.

2) Розміщення абонентів у роумінгу - після авторизації SubscriberSim він може використовувати мережу партнера роумінгу для ініціювання свого дзвінка. Функції callOut та callEnd можна використовувати для ініціювання та завершення виклику. Збори за користування мережею миттєво фіксуються між оператором дому та роумінговим партнером на основі їхньої згоди, визначеної у смарт-контракті. Функція callPay обчислює витрати за дзвінок.

3) Ідентифікація шахрайства - додається шахрайський SubscriberSim (з тим самим MSISDN, що і існуючий SubscriberSim). Функція аутентифікації ідентифікує користувача як шахрайського та позначає SubscriberSim за допомогою isValid = шахрайство в регістрі. Це заважає шахрайському SubscriberSim ініціювати будь-які дзвінки і виконувати будь-які дії в мережі.

4) Управління Overage - абонент роумінгу активізує дзвінок і виконується функція callOut. Смарт-контракт визнає, що абонент потенційно досягає граничного значення. Оператор сповіщає абонента про перевищення порогу та вказує на можливі зміни тарифу (відповідно і коштів). Абонент може прийняти або відмовитись від нових платежів, відповідь абонента записується в головну книгу, а майбутні дзвінки (включаючи цей) або ініціюються, або відмовляються, виходячи з того, прийняв або відхилив абонент плату за надмірну вартість. Якщо абонент роумінгу прийняв плату, усі майбутні дзвінки (включаючи цей) використовуватимуть OverrageRate для обчислення тарифів на дзвінки замість роумінгу.

Цінність бізнесу для клієнтів така:

- Автоматичне завершення дії контракту між оператором дому та роумінговими партнерами, автоматично примусове виконання контрактів

- Майже миттєве вирішення зборів, усуваючи дорогі сторонні процеси, такіяк клірингові будинки

- Оснащення сховища перевіряються транзакціями між операторами для вирішення суперечок

- Ефективне управління ідентифікацією через CSP для пом’якшення роумінгу та шахрайства підписки

- Повідомлення в режимі реального часу щодо проблем із сукупністю даних та дзвінків між сторонами, що призводить до підвищення задоволеності клієнтів

3.3 Cisco блокчейн-платформа

Рис. 10 Промо-картинка впровадження blockchain в платформу Cisco

В даний час Cisco розробляє блокчейн-платформу, спрямовану на задоволення бажаних вимог використання у різних галузях. Ядро платформи складається з декількох шарів, кожен з яких включає в себе декілька підслугових служб, причому багато настроюються за допомогою підключаються інтерфейсів.

Взаємодія операцій Blockchain має важливе значення для визначення ефективності блокчейна Cisco в довгостроковій перспективі. Висока сумісність полегшує обмін даними між блокчейнами з найнижчою затримкою. Розвиток інтероперабельності блокчейну ще на ранній стадії, і Європейський Союз нещодавно почав закликати до стандартів інтероперабельності blockchain. Для полегшення сумісності блокчейну Cisco створює загальну модель даних для оцифрованих фізичних активів, які можуть бути розгорнуті в будь-якій існуючій мережі блокчейн, включаючи своїх партнерів, таких як Hyperledger та Enterprise Ethereum Alliance (EEA). Cisco також може інтегрувати блокчейн у існуючу мережу IoT, що дозволяє мільйонам пристроїв Cisco, підключених до блокчейна. Як тільки блокчейн стане взаємодіючим, мережа послуг зберігання в ланцюзі поставок стане основним додатком серед підприємств.

Він містить комунікаційний рівень та розподілену книгу, підключається смарт контрактний механізм, який підтримує звичні мови розробника, такі як JavaScript, GoLang та Python, ідентифікаційний та політичний рівень, відповідальний за такі завдання, як аутентифікація, авторизація та управління ідентифікацією, та рівень оркестрації, який пов'язаний всі інші рівні обслуговування разом як частина "сервісної сітки".

Структура блокчейн має “END-END” захист і аналітику, що охоплює інфраструктурний рівень через інтерфейсний рівень.

Рис. 11 Суть Cisco фреймфорк-платофрми

Крім своєї платформи blockchain, Cisco каже, що будує екосистему, яка об'єднає постачальників послуг, незалежних постачальників програмного забезпечення (ISV) та стартапів, а також ключових консультаційних партнерів для створення цілих галузевих рішень для підприємства.

Основним напрямком цієї "справжньої мережі довіри в Інтернеті" є взаємодія. Cisco каже, що створює загальну модель даних для оцифрованих фізичних активів, які можуть бути розгорнуті в будь-якій існуючій блокчейн-мережі, включаючи відомі платформи в проекті Hyperledger та Enterprise Ethereum.

Фірма співпрацює з кількома галузевими партнерами, включаючи Trusted IoT Alliance, проект Hyperledger, Enterprise Ethereum Alliance та Палату цифрової торгівлі, щоб розробити стандарти та інструменти.

12 вересня 2017 компанія Intel спільно з китайським гігантом у сфері телекомунікацій Tencent підписали договір про наміри щодо спільної розробки рішень на базі технології blockchain для інфраструктури Інтернету речей.

Спільну заяву двох компаній було зроблено в Китаї на щорічному заході World Internet of Things.

Розробники мають намір сконцентрувати зусилля на розвитку проекту компанії Tencent - TUSI Internet of Things laboratory. Проект покликаний підвищити безпеку рішень для корпоративних клієнтів в обчислювальній мережі фізичних предметів Інтернету речей.

У свою чергу, Intel надасть Tencent свою хмарну блокчейн-технологію. Лабораторія TUSI IoT є дослідний центр, що спеціалізується на випробуваннях перспективних промислових технологій, їх сертифікації, спільну розробку та інших технічних послугах.

Проект TUSI Internet of Things laboratory ставить перед собою амбітне завдання створити "розумне місто", де основні служби функціонуватимуть відповідно до принципу децентралізації. Учасники проекту впевнені, що концепцію "розумного міста" можливо реалізувати застосувавши blockchain, хмарні технології, а також Інтернет речей.

Інтернет речей - це широка мережа пристроїв, підключених до інтернету, в тому числі смартфони, планшети і практично будь-які "речі", які мають датчики: автомобілі, промислове обладнання, реактивні двигуни, нафтові вишки та багато іншого. Всі ці "речі" збирають дані і обмінюються ними між собою.

Для цього Cisco розробляє блокчейн-платформу для відстеження інтернет-пристроїв, їх активності і рівня надійності при підключенні до мережі. Система також буде самостійно реєструвати і оцінювати додані пристрої на основі інформації про існуючі пристрої.

У заяві компанії йдеться "про мережі з низьким енергоспоживанням", на яких базуються smart grid - розумні мережі електропостачання. Відзначається, що такі мережі можуть складатися з десятків, тисяч або навіть мільйонів LLN-роутерів.

Кількість LLN-мереж стає дедалі більше, проте, враховуючи середовище і конструкцію таких пристроїв, вони схильні до різних вразливостей. У контексті IoT і подібних систем ідентифікація і управління пристроями є ключовою умовою для вироблення життєздатного комплексного вирішення. В залежності від кожного конкретного випадку, "пристрій" має пройти ідентифікацію і реєстрацію за допомогою різних механізмів і процедур, і стати одним із пристроїв в загальній IoT системі.

До випуску посібника Cisco Cisco співпрацював зі своїми партнерами в дослідженні сумісності блокчейна. Наприклад, Cisco спонсорував та брав участь у пісочниці, ініційованій Trusted IoT Alliance, що відкрите джерело тестування дозволило дослідити взаємодію блокчейн для випадків використання IoT у масштабах планети. Тестова мережа також дозволяла взаємодія між загальнодоступними протоколами протоколів блокчейн і підприємства. Співпраця з Trusted IoT Alliance забезпечила міцну основу для Cisco для сприяння подальшій сумісності блокчейнів.

Помітно, що поточне застосування блокчейн у галузі ланцюгів поставок здебільшого пов'язане з відстеженням продукції та виявленням підробленого імпорту. Ми вважаємо, що коли блокчейн взаємодіє один з одним, це означає, що значення розблоковано, оскільки дані можна вільно переносити через один блокчейн в інший.

Значення розблокування включає не лише дані, але й притаманні їм валюти, такі як біткойн та маркери безпеки. З більш широкої точки зору, ці міжсерійні дані в цілому є більш цінними для підприємств, оскільки полегшують передачу даних між різними підприємствами на блокчейні. Крім того, монетизація даних може стати новим потоком доходів для підприємств, коли блокчейн є взаємодіючим. Підприємства зможуть монетизувати використання непрацюючих активів та даних через ринок, щоб підвищити операційну ефективність.

Висновки до розділу

1. Як бачимо, перспектив для впровадження технології blockchain достатньо. Було сформовано основні принципи та переваги використання технології блокчейн в нових мережах. За результатами огляду можливо зробити висновок, що існуючі технології поступаються технології blockchain в сферах роумінгу, монетизації та конфіденційності даних.

2. Аналіз перспектив розвитку технології блокчейн та особливостей її розвитку вказує на такі основні її переваги: доступність та ідентичність даних у мережі, уникнення небажаного контролю за даними третьою стороною, безпека та підвищена продуктивність груп користувачів, використання сучасних методів збереження конфіденційності. Недоліками подібного рішення можуть стати складність реалізації стабільної роботи на етапах розвитку засобу, відносна проблема з масштабованістю мережі та прийняття нового принципу комунікації усіма структурами й учасниками світової спільноти глобальної мережі.

4. МОЖЛИВОСТІ ВИКОРИСТАННЯ BLOCKCHAIN В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Метою даного розділу є розгляд сфер телекомунікацій, де можна застосувати технологію blockchain. Деякі компанії вже користуються перевагами blockchain, створюють нові проекти на базі цієї технології, але існує ще декілька перспективних варіантів, які я розгляну в даному розділі.

В рамках даного розділу буде розглянуто аутентифікацію користувачів на роумінгу за допомогою blockchain-аутентифікації, роумінгові дзвінки на базі технології blockchain, конфіденційність даних, а також монетизацію телекомунікаційних послуг. Саме ці напрямки я вважаю перспективними для впровадження технології blockchain.

4.1 Аутентифікація користувача на роумінгу на основі blockchain-аутентифікації

Сучасна технологія сигналізації, яка використовується операторами зв'язку для передачі даних про аутентифікацію користувачів роумінгу, вже не настільки ефективна, як раніше. Для цього є кілька причин, включаючи затримку аутентифікації, проблеми безпеки та вартість. Що стосується затримок аутентифікації, користувачам іноді доведеться чекати періоди від 5 до 15 хвилин, поки вони не отримають дозвіл на роумінгову послугу. У епоху майже очікуваних реакцій у реальному часі ця затримка занадто довга.

Крім того, все більш критичним є той факт, що існуючий метод шифрування, який використовує галузь для цілей роумінгу - шифрування SS7, був поставлений під загрозу. Насправді, було показано, що він руйнується за допомогою грубої сили більше десяти років тому. Очевидно, що потрібен новий і більш безпечний підхід. Третя причина вдосконалення аутентифікації в роумінгу - це вартість.

Телекомунікаційні компанії сплачують велику щомісячну плату за існуючі послуги аутентифікації, але ці послуги не є рентабельними, а також не відповідають вимогам, для яких вони були розроблені.

Рішення

Запропоноване рішення полягає у використанні мережі зв'язку з підтримкою блокчейн, щоб полегшити надання послуг операторами телекомунікацій для користувачів, які роумують між мережами. Цей об'єкт, заснований на блокчейн, був би захищений за допомогою сучасних методів шифрування (наприклад, SHA-3) з кожним оператором, який має пару відкритих / приватних ключів.

Ідея полягає у створенні реєстру відкритих ключів для кожного оператора на дозволеній основі, щоб кожен оператор мав доступ до інших операторів. Таким чином, цей реєстр сприяв би прямому / зашифрованому повідомленню авторизованих служб для роумінгових запитів - дозволяючи спільне, безпечне та простежуване покращення від поточного методу.

Зацікавлені сторони

Основними зацікавленими сторонами є оператори зв'язку, тоді як бенефіціарами є як оператори, так і їх клієнти. GSMA (Глобальна система мобільного зв’язку) - це глобальна організація торгівлі, яка представляє інтереси операторів мобільної мережі по всьому світу і, ймовірно, буде однією з організацій, яка виступає основним драйвером мобільних операторів зв'язку.

Архітектура

Щоб додати до робочого процесу вище, тут представлена схема високого рівня, яка описує інтерфейси та деякі основні компоненти. Використовуючи рішення на основі блокчейна, оператори отримують перевагу від спільних схем та стандартизованої обробки транзакцій (за допомогою смарт-контрактів), які забезпечують кращу безпеку та швидший час реакції, ніж поточне рішення.

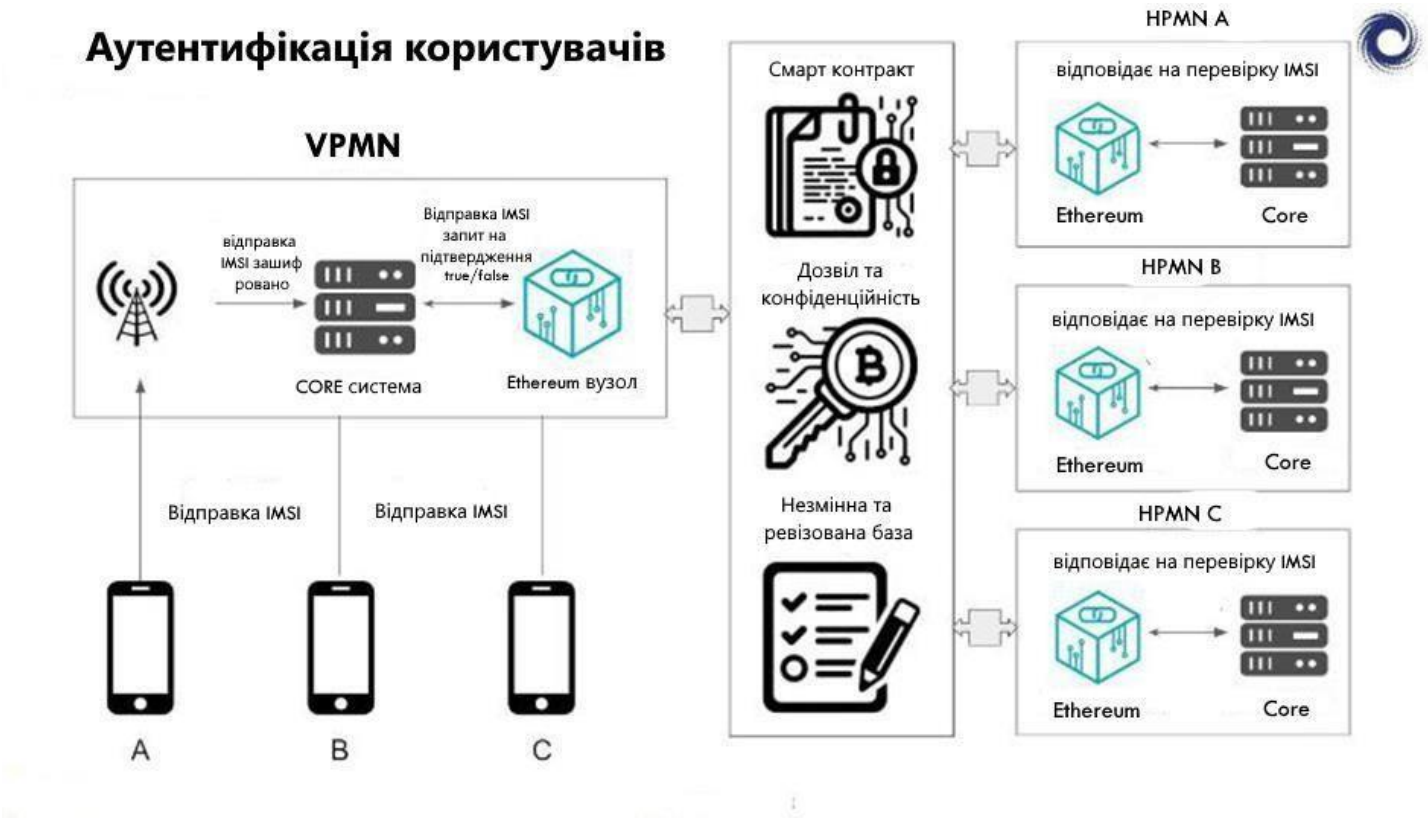

Рис. 12 Аутентифікація користувачів

4.2 Примирення роумінгових дзвінків на основі блокчейна

Пропозиція та підтримка роумінгових телекомунікаційних можливостей є важливою складовою сервісу для телекомунікаційних компаній, але вона повинна бути вигідною для операторів для управління та обслуговування таких послуг.

Будь-яке подібне резервування також повинно забезпечити безперебійний та недорогий досвід / без витрат на користування мобільними користувачами.

Однак політика між операторами, разом з транзакціями та накладними платежами, пов'язаними з роумінгом, стали досить складними. Ця комбінація представляє складні виклики для перевізників, особливо якщо мова йде про узгодження плати за роумінгові послуги між операторами. Вимоги до глобального рішення, яке може покращитись при поточному підході, не дивно, досить жорсткі. Будь-яке рішення щодо забезпечення та примирення повинно не лише керувати кількома відносинами, але й керувати складними фінансовими відносинами із різними законами та нормативними актами в різних країнах та регіонах світу. для цих складних фінансових та ділових процесів це особливо актуально в поєднанні з очікуванням користувачів щодо сумісності послуг.

Переглядаючи нову систему примирення роумінгу, виникає ряд проблем. Деякі з більш важливих проблем включають:

1.Поширення чутливих бізнес-даних з іншими компаніями
2.Захист від підробки та шахрайства користувачів
3. Обробка великих обсягів даних

Рішення

Для вирішення проблеми різні компанії, що займаються мобільним роумінгом, створили консорціум, який пропонує вказати рішення для телекомунікаційного роумінгу, яке може передавати та обмінюватися чутливими даними безпосередньо в мережі блокчейн. Зокрема, рішення стосується використання як компонентів рівня 1 (децентралізована книга), так і рівня 2 (державні канали), щоб забезпечити як незмінність, так і ведення обліку, а також розширену пропускну здатність і масштаб, необхідний для підтримки глобальної телекомунікації в реальному часі.

Цей консорціум, роумінг-контракти та бізнес-потоки можуть розроблятися, розповсюджуватися, перевірятися та застосовуватися.

Ці бізнес-потоки та контракти виражаються за допомогою смарт контрактів у рамках blockchain рішення.

Серед інших транзакційних потреб, пропоновані смарт-контракти стосуються таких напрямків:

• Узгодження журналу дзвінків в роумінгу зі списком плати разом із розрахунком плати за послуги

• Переадресація журналу дзвінків користувача до домашнього оператора від відвідуваного оператора

• Створення та відправлення рахунку за плату за послуги та відправка на домашнього оператора від відвідуваного оператора

• Підтвердження отримання рахунків-фактур та журналів викликів домашнім оператором

• Узгодження відправлених та отриманих рахунків та створення рахунку платіжного балансу з іншими операторами

• Оплата відкритих залишків, перенесення залишків вперед та / або оспорювання будь-яких транзакційних елементів

Переваги дизайну

Завдяки вдосконаленому роумінговому рішенню, телекомунікаційні компанії зможуть краще співвіднести використання непримітного оператора користувача з договором користувача, щоб забезпечити більшу прозорість та швидше реагування на послуги та проживання.

Переваги для користувачів полягають у тому, що вони отримують велику гнучкість обслуговування та зменшують плату за послуги, що, в свою чергу, збільшить їх використання. Для телекомунікаційних компаній переваги включають зменшення витрат, підвищення лояльності клієнтів та покращення запобігання шахрайству.

Технічні примітки

• Дані, пов’язані з мережею, і дані реєстру можуть бути відкриті на дозволеній основі в мережі блокчейн, тоді як приватні транзакції та дані можуть бути зашифровані та оброблені за допомогою алгоритмів підтвердження нульових знань.

• Використовуваний алгоритм консенсусу може бути оптимізований для відображення дозволеного характеру мережі, а також для задоволення потреб передбачуваної пропускної здатності. Запропонований алгоритм в даний час базується на консенсусі підтвердження авторитету, який дозволяє лише довіреним сторонам грати роль у валідації та верифікації транзакцій.

• Обробку даних можна звести до мінімуму, передаючи лише відповідні дані до вузла оператора роумінгу.

Переваги

• Прозорість та довіра: довіра між роумінговими партнерами буде забезпечена як принципом «взаємного моніторингу», так і «стійкості до несанкціонованого» рішення блокчейна. Оператори можуть запускати та підтримувати вузли в одній мережі і, отже, відіграють роль у створенні консенсусу для записів транзакцій, а також у валідації та верифікації кожного блоку транзакцій. Можливі також багатосторонні угоди, які включають та покращують прозорість та довіру.

• Розумна видимість контрактів: багатосторонні договори можна виконувати та керувати більш прозорим та вірним способом.

Первинні потоки між сторонами будуть автоматизовані та полегшені розумними контрактами.

-> В*изитний оператор*: Отримання інформації про користувача для надання послуг → послуга мережі постачань → записуйте журнал викликів до blockchain

-> *Домашній оператор*: підтвердьте журнал викликів та рахунок-фактуру від відвідувача оператора → розрахунок рахунків та оплата / отримання платежів

• Обробка в режимі реального часу: Ще однією вагомою перевагою переходу до блокчейн-рішення є можливість обробляти транзакції в режимі реального часу та підтримувати більш поточні баланси роумінгу між операторами. (Хоча продуктивність мереж blockchain часто піддається критиці, дозволена / приватна мережа у поєднанні з використанням державних каналів розроблена для управління типом пропускної здатності, що розглядається тут.) Ця можливість в реальному часі дозволяє операторам більш легко знати, що відбувається з кросом - перевезення перевізників, а також залишаються на вершині своїх бізнес-прогнозів доходів і витрат та фактичних даних.

• Скорочення витрат: Усі перераховані вище переваги дозволять перевізникам зменшити витрати, пов’язані з часом підтвердження, процесом коригування та іншим узгодженням після транзакцій, що зараз відбувається. Здійснення коригування витрат одночасно з наданням послуг усуне значну кількість накладних та післяобслуговувальних заходів. Спільність рішення та важелі, отримані завдяки видимим контрактам, вираженим виконуваним кодом, також виявляться значною економією для перевізників.

4.3 Конфіденційність даних та монетизація

Телекомунікаційні оператори в усьому світі стикаються з дедалі більшими труднощами перед традиційними бізнес-моделями. Ці виклики включають збільшення витрат на інфраструктуру та спектр даних внаслідок експоненціально зростаючих потреб споживачів на більшу кількість даних та жорсткої конкуренції серед телекомунікацій із посиленням уваги як громадськості, так і влади щодо ділових практик телекомунікацій. Один з останніх викликів пов'язаний зі зростанням поінформованість громадськості, а також суворіші регуляторні позиції органів влади щодо конфіденційності та права власності на дані, які належать абонентам, або можуть походити від передплатників.

Кілька прикладів цього:

• Дані, якими володіють абоненти, можуть включати документи, зображення, відео абонентів абонентів, а також інформацію про особи абонентів, всі або частина яких абоненти можуть вибрати для зберігання в хмарних службах, що управляються телекомунікаційними службами.

• Дані, де абоненти є джерелами генерації, можуть включати текстові повідомлення SMS, місцеположення, час та зміст діяльності, вказані лайки, уподобання, інтереси та / або думки, схеми використання послуг, історіїпридбання та / або платежів тощо. Майже у всіх випадках телекомунікаційні компанії могли використовувати лише ті дані, які їм було надано явну згоду на використання від абонентів.

Ситуація складніша, однак, якщо врахувати, що багато телекомунікацій все частіше застосовують розширену аналітику даних, часто підкріплену масштабними та централізованими інфраструктурами великих даних та використанням передових методів машинного навчання (ML), що дозволяє глибокому навчанню та іншим подібним методам витягнути все більше «розуміння» про своїх підписників.

Це профілювання часто проводиться індивідуально, але також проводиться в різних «групуваннях» або «категоріях». Такі аналізовані уявлення можуть включати в себе високоточні оцінки характерів, уподобань людей, емоцій, захоплень, політичних та інших соціальних схильностей, сімейних та інших соціальних відносин та мереж, а також поведінкові та трансакційні прогнози. Багато телекомунікацій сьогодні здатні аналізувати кожного абонента, який він обслуговує. сотні "категорій" і формують інтегровані, всебічні "профілі.

У багатьох випадках телекомунікаційні компанії можуть використовувати таку інформацію для оптимізації своєї ділової практики та процесів, включаючи оптимізацію побудови її інфраструктури та адаптивного використання, а також забезпечення високоцільових цифрових маркетингових кампаній щодо осіб та груп людей.

Проблема

Реальність ситуації полягає в тому, що навіть якщо передплатники дали прямі та всебічні згоди на використання даних своїм телекомунікаційним апаратам, вони можуть бути не дуже чітко проінформовані про ширину та глибину розуміння, яке компанії можуть отримати з погоджених даних.

Крім того, у більшості випадків абоненти жодним чином не отримують прямих грошових вигод від такої інформації, хоча вони часто надають більшість потоків даних, які потрібні та використовуються при створенні такої інформації.

Тим часом у зовнішньому світі обізнаність споживачів про «цінність даних» та «важливість конфіденційності даних» стає все більш посиленою. Нещодавні виклики щодо практики обробки даних та конфіденційності з боку глобальних служб OTT, таких як Facebook, Google та YouTube, дозволяють припустити, що телекомунікаційні компанії, які є аналогічними обробниками величезної кількості даних про своїх абонентів, можуть піддаватись рівномірному ризику публічного знущання. Крім того, в регуляторному середовищі передбачається, що прийняття GDPR в ЄС спричинить зростання рівнів досі небачених викликів організаціям, що займаються обробкою даних. Режим GDPR містить значні заходи щодо згоди чи інших законних підстав для законного опрацювання, щодо прав суб'єктів даних, конфіденційності та повернення контролю над особистими даними в руки людей.

Тому будь-яка відповідність, очевидно, вимагає перспективи, яка стосується впливу та ризику в широкому діапазоні обробки даних, зберігання та передачі даних. Голоси від НУО та навіть юридичних фірм, які виступають за "MyData", посилаючись на права власників даних на не лише похідні похідні вигоди, але і а також прямі вигоди від ланцюга створення цінності даних, все більше лунають у публічних просторах.

Очевидно, що телекомунікаційні компанії рекомендують уважно вивчити, як вони можуть найкраще виправити ситуацію, сприяючи полегшенню проблем з боку споживачів, а також органів влади, одночасно надаючи інноваційні послуги абонентам, а також допомагаючи покращити бізнес-результати корпорацій.

Технологія SolutionBlockchain обіцяє включити різноманітні децентралізовані сервіси, коли учасникам не потрібно створювати або встановлювати попередню довіру до інших учасників. Зокрема, Ethereum, завдяки підтримці смарт-контрактів, що займаються Тьюрінгом, може бути цілком придатний для вирішення проблем, пов'язаних з даними, що стоять перед телекомунікаційними провайдерами.

Оскільки будь-які дані, що зберігаються на blockchain, можуть становити персональні дані, розробники та компанії, які, ймовірно, підпадають під дію GDPR, повинні обмежувати вид або кількість особистих даних, що зберігаються в blockchain, і придумувати нові методи анонімності даних, використовуючи деякий стан -Технічні технології, такі як Zero Knowledge Proofs для мінімізації можливого конфлікту з GDPR.

З точки зору "права бути забутим", особисті дані, що стосуються передплатників, повинні зберігатися окремо від блокчейна в "поза ланцюгових" даних зберігання через незмінність, характерну для blockchain, лише з його криптографічним хеш-значенням або свідченням на платформі blockchain. Роблячи це, особисті дані можуть бути стерті у випадку запиту абонентів або вказаних підстав для видалення їх інформації без порушення цілісності блокчейна.

Користувальницькі мережі StoriesBlockchain можуть бути використані для встановлення запису даних про події та транзакції. Хоча дані самої події (тобто користувача, конкретного використання або сповіщення) можуть не включатися до запису транзакцій, позначення щодо їївиникнення може встановити незмінний запис про його існування.

Наприклад, постачальник послуг телекомунікацій може генерувати і зберігати "уявлення клієнтів" про індивідуальні та / або групи своїх абонентів - після збору, обробки та аналізу даних, що надаються абонентами.

У ході цієї пропозиції вони сповіщатимуть окремих або груп клієнтів про доступність нової інформації та пропонують "повернути" або "надіслати" таку інформацію клієнтам.

Ці сповіщення можуть бути записані в блокчейн Ethereum як такі, що відбулися за часом - з посиланням на дозволені записи, які забезпечують конкретні деталі повідомлень та їх отримання.

Підписники можуть або прийняти, або відхилити таку пропозицію, де така ознака також може бути записані на блокчейні як подія. Якщо пропозиція буде прийнята, постачальник послуг телекомунікацій надішле інформацію, а також метадані транзакцій, відповідному клієнту.

Механізм надсилання може використовуватися за допомогою текстових повідомлень мобільних телефонів у текстових або файлових форматах, електронних листах клієнта, облікових записах послуг на основі хмарних даних або інших механізмах. Потім інформація про інформацію зберігається в зашифрованому форматі у сховищі - як мобільний телефон, SIM-карта, будь-який інший онлайн-чи офлайн-пристрій або хмарне сховище - використовуючи відкритий ключ абонента як ключ пошуку.

Будь-яка особа, можливо, захоче продати або торгувати цілою або частиною інформації про інформування третій стороні або бажає просто поділитися нею з другом або іншою стороною.

Вказівка індивіда про своє бажання ділитися, продавати чи торгувати своєю інформаційною інформацією, а також деякі метадані, що описують її з метою виявлення третьою стороною, також буде записано як подію.

Таке вказівка також може транслюватися або поділятися подібним чином на «базарі», що базується на блокчейні, як система.

Якщо будь-яка особа чи сторона, яка бере участь у «базарі даних на основі блокчейна», знайде опис інформації про те, що це може бути зацікавлений, запит на обмін, сигнал покупки або сигнал торгівлі може виходити і проходити через ринок.

Вся така сигналізація також може бути записана за допомогою запису блокчейн. Може бути сторонній агрегатор або брокер, який може об'єднувати інформацію про представлення безлічі підписників і продавати або торгувати агрегованою такою інформацією від імені абонентів, які запропонували свою просвітницьку інформацію, а також будь-яка третя сторона, яка вимагає такої інформації.

Постачальник послуг телекомунікацій може виступати таким агрегатором або брокером. Будь-яка акція, продаж або торгова діяльність реєструються вблокчейн. Постачальник послуг телекомунікацій не може безпосередньо продавати інформацію про інформацію в розшифрованому форматі.

Він може лише спрямовувати потенційного замовника на посилання, завдяки якому замовник зможе отримати збережену інформацію.

Переваги

У вищеописаному сценарії індивідуальний абонент може отримати вигоду, отримавши:

1) краще інформування про власну власну власні сили (характеристики, вподобання, поведінкові тенденції, фактичну діяльність тощо);

2) можливість вільно ділитися такою інформацією з обраними сторонами або ataprofit сторонам, які вимагають такої інформації.

Технологія blockchain може використовуватися як спосіб повернення права власності на дані або значення, що випливають з них назад, абонентам або користувачам, що неможливо в централізованій архітектурі, що домінувала в Інтернет-сервісах протягом останніх десятиліть.

Постачальник послуг телекомунікацій може виграти, налагоджуючи нові відносини зі своїм абонентом, якщо абонент може почувати себе краще; тим самим розраховуючи ефективніше конкурувати зі своїми конкурентами; безпосередньо отримувати нові доходи від плати за транзакції, стягуваної з клієнтів інформації про інформаційний ринок.

Влада може отримати вигоду, гарантуючи, що конфіденційність даних та права власності на абоненти послуги telco може підтримуватися більш прозорими та незмінними способами, ніж раніше.

4.4 Покращення операцій у сфері телекомунікацій

Блокчейн та смарт контракти можуть створити багато автоматизованих процесів у внутрішніх процесах, таких як виставлення рахунків, роумінг та управління ланцюгами постачань. Наразі транзакції з телекомунікаційними книгами повинні пройти через клірингову палату, яка має бути затверджена.

Розумні контракти можуть автоматизувати цей процес та гарантувати розрахунки між учасниками, шляхом маршрутизації від блокчейна одного оператора до іншого оператора та підвищити прозорість для кінцевого клієнта. Абонент роумінгу ініціює голосовий дзвінок у телекомунікаційній мережі.

Потім транзакція записується в мережу blockchain, і коли виклик закінчується, тривалість дзвінка зберігається на платформі blockchain. На основі правил розумного контракту встановлюються збори, а оплата реєструється від оператора дому до віддаленого партнера.

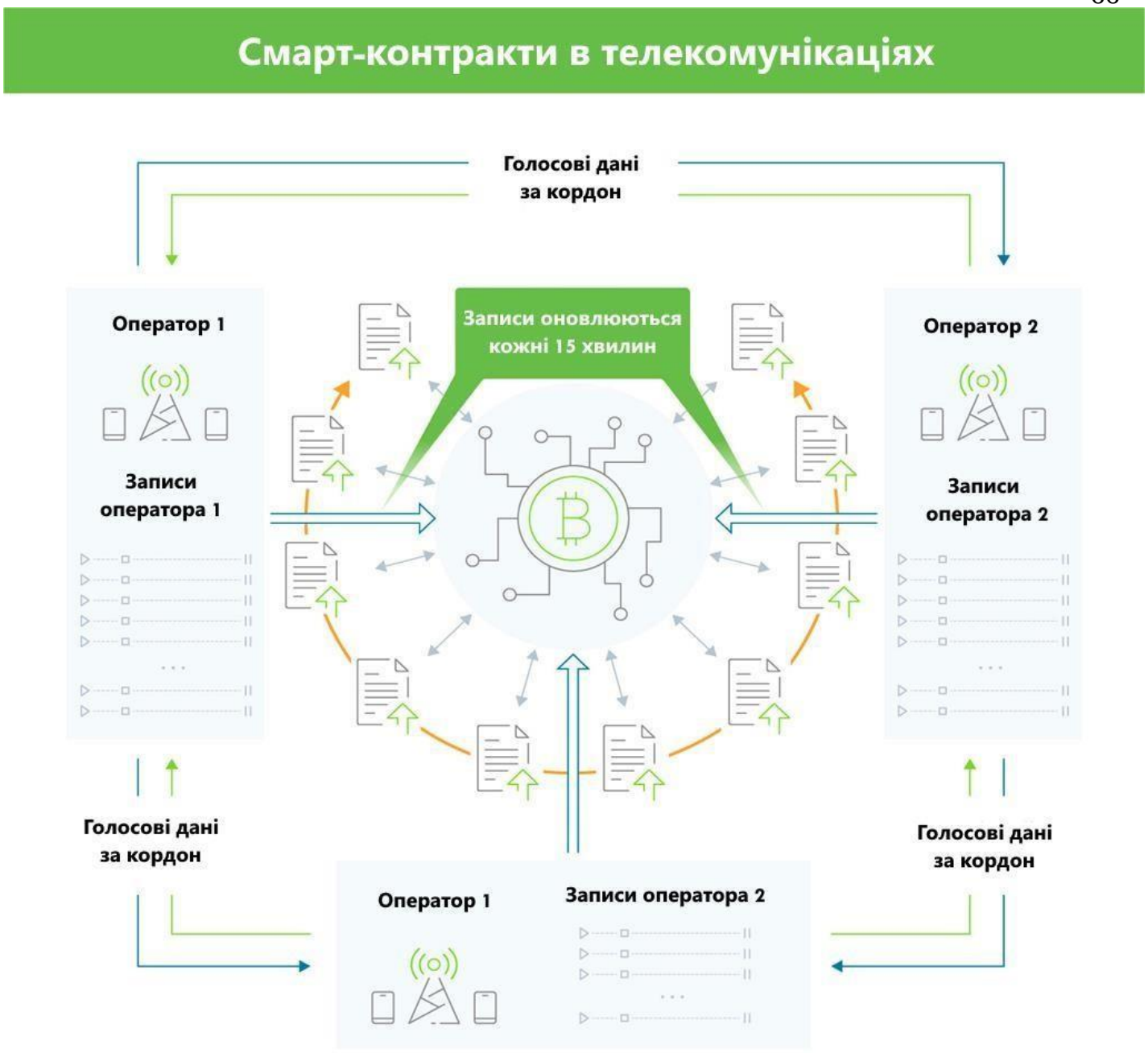

Рис.13 Смарт-контракти в телекомунікаціях

Процес базується на консенсусній моделі та технології спільної книги, яка не передбачає жодних клірингових бюро. Це допомагає уникнути суперечок між залученими учасниками; це менш трудомістко і затримує витрати, витрачені на аудит та облік, а головне, виключає дороге посередництво послуг клірингових будинків. Операції з цифровими активами.

Підприємства телекомунікацій можуть використовувати блокчейн для включення мікроплати за музику, мобільні ігри та інші види таких послуг. Більше того, блокчейн може бути реалізований для послуг з переказу грошей клієнту на замовника. Airtel, провідна телекомунікаційна компанія Індії, пропонує цифрові гаманці, що дозволяють здійснювати оплату від клієнта до замовника.

Використовуючи блокчейн для обробки транзакцій, Airtel робить свої гаманці більш захищеними від перевірки ідентифікаторів. Крім того, такий підхід призводить до дешевших міжнародних грошових переказів, більш швидких та зручних переказів, що, як результат, позитивно впливає на доходи компанії.

Смарт контракти та управління ланцюгами поставок

Підприємства телекомунікацій можуть покращити управління ланцюгами поставок за допомогою блокчейн. Розумні контракти дозволяють автоматизувати співпрацю між підприємством та партнерами в межах ланцюга і можуть автоматизувати процес управління запасами. Розумні контракти мають попередньо встановлені умови, і договір самостійно виконується лише тоді, коли умови виконуються повністю.

Використання розумних контрактів пропонує остаточне зниження витрат для телекомунікаційних підприємців. Він усуває посередників, полегшує розрахунки з постачальниками та постачальниками, а також веде облік, хоча весь цикл поставок простий та прозорий, що зменшує витрати на облік та аудит.

Управління та перевірка цифрових ідентифікацій

Підтвердження посвідчення особи щорічно коштує корпораціям та урядам сотні мільярдів доларів. В даний час стартапи, як Civic, розробляють нові системи підтвердження ідентичності на основі блокчейна.

Телекомунікаційні підприємства працюють з величезною кількістю даних клієнтів, їм вигідно виступати джерелом аутентифікації особи. Вони можуть спроектувати нові системи, які є більш прозорими, безпечними та зручними, як для клієнтів, так і для підприємств для отримання додаткових джерел доходу.

Коли абонент потрапляє в мережу партнера роумінгу, роумінговий партнер визначає, що це відвідувач від домашнього оператора. Це реалізується за допомогою транзакцій з обміну інформацією абонентів у мережі на основі блокчейна. Потім абонент затверджується та реєструється на смарт-контракті. Система управління ідентифікацією Blockchain дозволить користувачам керувати своїм ідентифікатором через різні програми, пристрої та організації лише одним єдиним паролем. Кожен абонент отримує головний ключ, за допомогою якого він зможе підтвердити свою особу в будь-якій цифровій присутності.

Це може бути чудовою можливістю для телекомунікаційних організацій розростати та розширювати свій бізнес-сегмент. Кілька прикладів - це посвідчення водія абонента, паспорти, посвідчення шлюбу тощо. Наразі такий проект управління посвідченням особи вже розгортається в Європі. Проект ID2020 має намір найближчим часом забезпечити 1,1 мільярда людей надійною та надійною системою управління ідентифікацією.

4.5 Blockchain та 5G включення

Попит на послуги зв’язку зростає, і незабаром світ перейде в мережу 5G, яка буде в десять разів швидше, ніж 4G, матиме значно менші затримки та більшу потужність, але управління такою складною мережею вимагатиме більшої потужності розрахунку та ємність зберігання.

5G - це ще одна технологія, яка може отримати користь від блокчейн. 5G обіцяє переважаючий доступ до різних мереж, і телекомунікаційним підприємцям потрібно буде працювати з універсальними вузлами доступу та різноманітними механізмами доступу. Вибір найшвидшого вузла доступу для кожного користувача незабаром стане головним завданням для телекомунікаційних компаній. Blockchain має можливість ввімкнути такі механізми вибору доступу при розробці 5G.

Сьогодні системи зв'язку централізовані за моделлю клієнт-сервер, де правила, що зберігаються на сервері, висуваються до замовника. Це спричиняє затримки і не дозволяє безперешкодно забезпечувати пристрій між мережами доступу для пристрою. Крім того, надання правил - це не процес реального часу, що означає, що вони не можуть бути змінені.

Мережі доступу GPRS, WiMAX, WLAN та Wi-Fi у певній області можуть бути об'єднані в блокчейн, де кожна точка доступу, як маршрутизатор Wi-Fi або башта стільникового зв'язку, може служити вузлом у мережі. Правила та угоди між різними мережами забезпечення доступу можуть бути встановлені у смарт-договорі. Ці договори можуть мати динамічний характер, коли в будь-який час потрібно змінювати політику, змінювати лише код договору.

Коли пристрій транслює свою особу, його приймає в мережу відповідний постачальник послуг зв'язку. Як тільки пристрій транслює своє місцезнаходження, вузол доступу, який найкраще може надавати послугу пристрою.

Це призводить до безперебійного оцінювання та оплати всіх послуг між різними вузлами доступу.

Blockchain та IoT у телекомунікаційній індустрії

Стільникові зв'язки IoT досягають мільярдів до наступного десятиліття. Основне питання полягає в тому, що зростання IoT та зростаюча незахищеність даних прямо пропорційні.

Підключення IoT створює серйозні проблеми, наприклад, необхідність забезпечення мільярдів взаємодій між машинами та датчиками, а також необхідність захищати конфіденційну інформацію, яка захоплюється та передається через пристрої.

Як результат, вимоги до даних та безпеки мережі можуть стати дорогими, оскільки ці мережі IoT продовжують зростати. Децентралізоване управління на основі блокчейн дозволяє забезпечити більш масштабовану безпеку IoT, а безпечна перевірка та перевірка не дозволять пристрою шахраїв втручатися в будинок або на заводську систему шляхом надання недостовірної інформації.

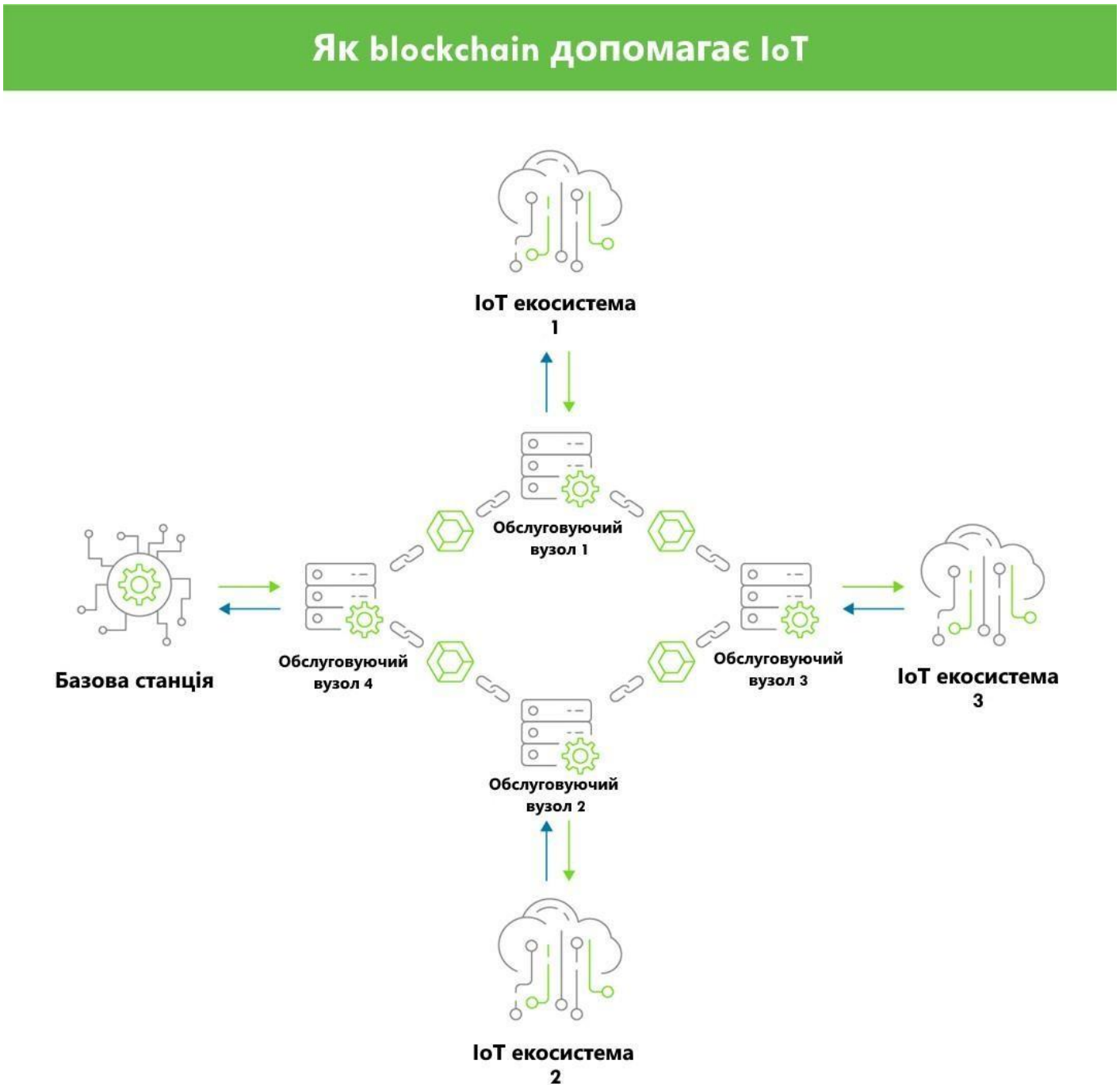

Рис. 14 Як blockchain допомагає IoT

Blockchain може створювати високозахищені однорангові мережеві мережі, що управляються одноранговими, які використовують велику кількість вузлів. Ці вузли можуть бути представлені датчиками IoT з можливістю перевірити кожен блок, що змінюється. Такі мережі можуть бути впроваджені в приватне середовище на базі стільникових веж.

Тоді постачальники послуг зв'язку можуть забезпечити безпеку приватного / відкритого ключа та широке підключення для того, щоб таку блокчейн-мережу мали глобальний доступ.

Висновок

Блокчейн - це передова технологія, яка може внести величезний внесок у телекомунікаційну галузь. Він має потенціал для підвищення безпеки та створення додаткових джерел доходу для підприємств телекомунікацій. Хоча прийняття блокчейна може спричинити низку проблем, наприклад, перешкода може відповідати існуючим стандартам даних щодо структури та транспорту інформації. Крім того, телекомунікаційним компаніям необхідно визначити нормативні рамки для впровадження розумних контрактів у свою ділову практику.

Тим не менш, прийняття blockchain коштує великих витрат. Розумні контракти виключають необхідність посередників клірингових будинків і різко зменшують бухгалтерські витрати.

За допомогою blockchain підприємці з телекомунікацій можуть запобігти роумінгу та шахрайству з ідентичністю, що є основним джерелом фінансових втрат у галузі. Найголовніше, що блокчейн стане невід'ємною частиною майбутніх комунікацій, поряд із мережею 5G та IoT.

Де ще blockchain має сенс?

Коротка відповідь: в унікальних екземплярах.

Щоб побачити, які можуть бути ці екземпляри, давайте поміркуємо, чому для біткойна потрібна технологія блокчейн. Є три основні причини. Біткойн - це публічна книга операцій з біткойнами(криптовалютою). Існують ненадійні вузли, що записують транзакції в регістрі Bitcoin. Біткойн не хоче довіряти третій стороні для адміністрування книги, він хоче мати власну книгу.

Ефективно, Bitcoin використовує блокчейн для децентралізації платежів. Де ще ми могли використовувати цю унікальну архітектуру баз даних, щоб позбутися посередника? Чи є інші речі, які були б більш цінними, якби вони були децентралізованими? Візьмемо це крок за кроком. Який ще сценарій, коли кожному потрібен запис права власності, і коли довірена третя сторона не бажана?

Пам'ятають про декілька випадків негайного використання. Право власності на землю - одне. Для всіх може бути корисним доступ до децентралізованого джерела запису, який говорить, хто є власником даної земельної ділянки.

Враховуючи, що державні перевороти та війни часто перерозподіляють землю несправедливо та / або неправильно, це може не тільки виявитись корисним: воно може мати і гуманітарний вплив. Після узгодження розподілу земельних ділянок він може бути записаний у розподіленій книзі і більше не підлягає дискусії.

Ряд компаній працюють над цим, включаючи Velox.RE .У цьому ж ключі блокчейн може бути використаний для встановлення права власності на будь-яку кількість фізичних цінностей - автомобілів, мистецтва, музичних інструментів тощо. Заголовок паперового напису схильний до підробки та / або фізичної деградації. Централізовані бази даних схильні до злому, людських помилок та / або підробки. Блокчейн означає, що не існує жодної сутності, яка контролює велику книгу.

Таким чином, запис фізичних активів на блокчейні - це яскравий приклад того, де ця технологія може стати в нагоді для відстеження права власності на захист від несанкціонованої, нейтральної та стійкої системи. Зробивши цей крок далі, технологія blockchain може навіть виявитися застосовною у віртуальній реальності. Якщо створений віртуальний світ - для ігор або з будь-якої кількості інших причин - блокчейн-технологія може дозволити користувачам купувати та володіти шматочками цього віртуального світу, подібно до того, як вони можуть придбати земельну ділянку.

.

Це, звичайно, трохи далеко, але Decentraland - це один із проектів, який вже працює над цим. У серпні 2017 року команда зібрала 25 млн доларів за свій жетон MANA та пообіцяла побудувати «першу віртуальну платформу, що належить її користувачам». Ідентичність може бути також низько висячим фруктом. Зловмисник 2017 року «Ecifax» викрив суму соціального страхування 143 мільйонів американців. Номери соціального страхування ніколи не мали використовуватись для ідентифікації - зауважте, як ця стара карта соціального страхування зазнає ударів від взломів.

Технологія blockchain може бути кращим засобом встановлення ідентичності. Замість того, щоб держава чи уряд видавали її, ідентичність можна було б перевірити на відкритій, глобальній блокчейні - контролювати її ніхто і довіряти всім. Таким чином, користувачі могли контролювати власну ідентичність. На цій арені працює ряд компаній, серед яких ID2020 та Civic.

Аналогічно, Blockstack сподівається створити новий децентралізований Інтернет, "де користувачі володіють своїми даними, а додатки працюють локально". Технічно кажучи, Blockstack є одним з перших прикладів децентралізованої системи DNS (сервера доменних імен), побудованої за допомогою технології blockchain. Компанія зібрала 52 млн доларів у грудні 2017 року та сподівається, що її новий Інтернет допоможе користувачам "володіти своїми даними та підтримувати їх конфіденційність, безпеку та свободу". Якщо це спрацює, Blockstack може зірвати багатьох інтернет-гігантів, які діють як посередники сьогодні - подумайте про Google і Facebook. Звичайно, це здорово, якщо вийде.

Існує також широкий спектр потенційних децентралізованих інтернет-послуг, як-от децентралізована реклама. Основна увага Token останнім часом набирає позиції як протокол на основі блокчейна, який обіцяє зробити рекламу більш ефективною, розподіляючи значення між користувачами, рекламодавцями та видавцями.

Проект, заснований Бренданом Ейхом, творцем JavaScript і співзасновником Firefox і Mozilla, використовує маркер на основі блокчейна у спеціально створеному браузері для відстеження та винагородження зосередженої уваги користувачів на рекламі, захищаючи конфіденційність користувачів.

Інші потенційні програми включають платформу, де традиційно неліквідні активи представлені та торгуються через блокчейн-жетони. Уявіть собі децентралізований ринок активів, де ви можете купувати, продавати та торгувати частковою власністю на високоцінні картини, нерухомість та компанії через сумісні бази даних без будь-якого посередника. Це такий тип ліквідності, який працює 0x Project, щоб зробити можливим завдяки своєму протоколу децентралізованої біржі активів.

Висновки до розділу

1. Будь-які корупційні спроби провокують зміни блоків. Після цього всі наступні блоки несуть невірну інформацію та роблять всю блокчейн-систему недійсною.

2. Як бачимо, перспектив для впровадження технології blockchain достатньо. Було сформовано основні принципи та переваги використання технології блокчейн в нових мережах. За результатами огляду можливо зробити висновок, що існуючі технології поступаються технології blockchain в сферах роумінгу, монетизації та конфіденційності даних.

3. Аналіз перспектив розвитку технології блокчейн вказує на такі основні її переваги: доступність та ідентичність даних у мережі, уникнення небажаного контролю за даними третьою стороною, безпека та підвищена продуктивність груп користувачів, використання сучасних методів збереження конфіденційності. Недоліками подібного рішення можуть стати складність реалізації стабільної роботи на етапах розвитку засобу, відносна проблема з масштабованістю мережі та прийняття нового принципу комунікації усіма структурами й учасниками світової спільноти глобальної мережі.

4. Принципи цієї технології роблять blockchain незмінною та криптографічно захищеною, усуваючи будь-які сторонні дані. Підробити дані в системі blockchain практично неможливо: щоб змінити дані в ланцюгах та транзакціях, необхідно мати підтвердження більшої сторони ланцюга, тобто так званого “51%”. Основною перешкодою на шляху до цього стає відносне неповноліття даної технології та відсутність чітких стандартів роботи подібних мереж.

ВИСНОВКИ

1. Підсумовуючи, блокчейн - це децентралізована, розподілена книга (державна чи приватна) різного роду транзакцій, організованих у мережу P2P. Ця мережа складається з багатьох комп'ютерів, але таким чином, що дані не можуть бути змінені без консенсусу всієї мережі (кожного окремого комп'ютера).

2. Визначено принципи роботи мережі Blockchain, розглянуто компоненти в її складі: хеш функція, хеш таблиця, асиметричні алгоритми шифрування, смарт-контракт. Основними перевагами використання цих механізмів визначено: неможливість підробки даних, прозорий механізм передачі даних, можливість перевірки інформації, що передається, надійність роботи мережі та розподілені зв’язки в системі. Ці особливості як найкраще можуть слугувати для функціонування нового покоління VPN та передачі трафіку в цілому.

3. Було створено структурний опис та схему роботи і комунікації клієнтів в мережах блокчейн, виділено основні етапи обміну даними, встановлення діалогів та сервіс-сесій. Даний матеріал повинен допомогти в розгортанні механізмів комунікації та роботи усіх клієнтів в рамках зазначеної структури.

4. За підсумками третього та четвертого розділу можемо зазначити, що використання Blockchain для вирішення сучасних проблем комунікації та доступу до даних може вирішити усі насущні проблеми Інтернет зв’язку і створити паралельну та альтернативну гілку розвитку з власними принципами роботи мережі. Основною перешкодою на шляху до цього стає відносне неповноліття даної технології та відсутність чітких стандартів роботи подібних мереж. Це завдання є основним на шляху до винайдення нових застосувань даного рішення.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Blockchain architecture basics: components, structure, benefits & creation // https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture (дата звернення: 05.11.2019).

2. Кукліна, А.С. Побудова VPN мереж на базі технології Blockchain: магістерська дис.: 172 Телекомунікації та радіотехніка / Кукліна Анна Сергіївна. Київ, 2018. - 106 с. (дата звернення 10.11.2019)

3. Report: Cisco is building a blockchain ecosystem and platform // URL: https://fintechnews.ch/blockchain_bitcoin/report-cisco-is-building-a-blockchain-ecosystem-and-platform/24661/ (дата звернення: 17.11.2019).

4. How blockchain can impact the telecommunications industry and its relevance to the C-Suite // Deloitte URL: https://www2.deloitte.com/content/dam/Deloitte/za/Documents/technology-media-telecommunications/za_TMT_Blockchain_TelCo.pdf (дата звернення: 20.11.2019)

5. Блокчейн у телекомунікації: як Nexign та Bubbletone модернізують галузь // URL: https://nexign.com/en/blog/Blockchain-in-telecom (дата звернення: 27.11.2019р).

6. The WIRED Guide to the Blockchain // URL: https://www.wired.com/story/guide-blockchain/ (дата звернення 10.10.2019).

7. Блокчейн // Вікіпедія. URL: https://uk.wikipedia.org/wiki/Блокчейн (дата звернення: 03.11.2019).

8. Асиметричні алгоритми шифрування // Вікіпедія. URL: https://uk.wikipedia.org/wiki/Асиметричні_алгоритми_шифрування (дата звернення: 17.11.2019).

9. Blockchain Unleashed // IBM Blockchain Blog. URL: https://www.ibm.com/blogs/blockchain/ (дата звернення: 25.11.2019)

10. Whait is Blockchain Technology ? // URL : https://www.cbinsights.com/research/what-is-blockchain-technology/ (дата звернення 28.11.2019)

11. A brief history of blockchain // URL: https://medium.com/coinmonks/a-brief-history-of-blockchain-70c519d3053 (дата звернення 27.11.2019)