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 _____

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: Особливості використання алгоритмів технології блокчейну в розподілених телекомунікаційних мережах.

Виконав: студент 2 курсу, групи ТМ-81мп

Власенко Владислав Володимирович _____
(прізвище, ім’я, по батькові) (підпис)

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

Рецензент_____ _____
(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)

Кафедра телекомунікацій
(повна назва)

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
Власенко Владислав Володимирович
(прізвище, ім'я, по батькові)

1. Тема дисертації Особливості використання алгоритмів технології блокчейну в розподілених телекомунікаційних мережах

науковий керівник дисертації Міночкін Дмитро Анатолійович, доц. каф. ТК, к.т.н., с.н.с.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «_07_» «_11_» 2019р. № _3840-с_

2. Строк подання студентом дисертації _____

3. Об'єкт дослідження Розподілені телекомунікаційні мережі_____
_____

4. Предмет дослідження Зменшення вразливостей мереж за допомогою технології блокчейну _____
_____

5. Перелік завдань, які потрібно розробити розглянути сучасний стандарт передачі даних для мобільних телефонів LTE, виявити його недоліки, розглянути технологію блокчейну та запропонувати способи вирішення недоліків LTE використовуючи блокчейн _____

_____

6. Орієнтовний перелік ілюстративного матеріалу _____
_____
_____
_____
_____

7. Орієнтовний перелік публікацій _____
_____
_____

8. Консультанти розділів дисертації

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

9. Дата видачі завдання 10.10.2018р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
1	Розгляд LTE	11.10.2018 – 01.03.2019	
2	Дослідення уразливостей LTE	02.03.2019 – 05.05.2019	
3	Дослідення технології блокчейну	06.05.2019 – 01.10.2019	
4	Способи використання блокчейну в телекомунікаційних мережах	02.10.2019-03.12.2019	

Студент _____ _____
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ _____
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Тема магістерської дисертації: Особливості використання алгоритмів технології блокчейну в розподілених телекомунікаційних мережах.

Текстова частина магістерської дисертації: с.78, рис. 19, табл.3, джерел 17.

Метою даної роботи є дослідження способів захисту розподілених телекомунікаційних мереж з використанням технології блокчейну від несанкціонованого доступу до службової інформації в мережах, інформації про абонентів, її видалення та заміни задля зловмисних цілей.

В результаті виконання даної роботи було описано сучасний стандарт високошвидкісної передачі даних для мобільних пристроїв та інших терміналів – LTE, досліджено деякі з основних уразливостей стандарту.

Задля уникнення цих уразливостей було обрано технологію блокчейну, яку також було описано, проаналізовано принцип роботи та її переваги над застарілими способами захисту та передачі даних, розроблено способи її використання в розподілених телекомунікаційних системах з ціллю вирішення їх уразливостей.

Дана робота є актуальною в наш час, оскільки сучасні стандарти високошвидкісної передачі даних для мобільних пристроїв мають низку значних недоліків і уразливостей, якими користуються зловмисники і важливим завданням є дослідити та знайти способи вирішення цієї проблеми.

Ключові слова: стандарти високошвидкісної передачі даних для мобільних пристроїв LTE, розподілена телекомунікаційна мережа, технологія blockchain, хешування, децентралізована мережа.

ABSTRACT

Master thesis: Features of using blockchain technology algorithms in distributed telecommunication networks.

Text part of the master's thesis: p.78, fig. 19, tables 3, sources 17.

The purpose of this paper is to investigate ways to protect distributed telecommunications networks using blockchain technology from unauthorized access to service information on networks, subscriber information, deletion and replacement for malicious purposes.

As a result of this work, a modern standard of high-speed data transmission for mobile devices and other terminals - LTE, was described, some of the main vulnerabilities of the standard were investigated.

In order to avoid these vulnerabilities, blockchain technology was chosen, which was also described, the principle of operation and its advantages over outdated methods of data protection and transmission were analyzed, and ways of its use in distributed telecommunication systems were developed in order to solve their vulnerabilities.

This work is relevant nowadays, as modern standards of high-speed data transmission for mobile devices have a number of significant disadvantages and vulnerabilities that malicious users use and an important task is to investigate and find ways to solve this problem.

Keywords: high-speed LTE mobile data standards, distributed telecommunications network, blockchain technology, hashing, decentralized network.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

LTE	Long-Term Evolution
UMTS	Universal Mobile Telecommunications System
GSM	Global System for Mobile
3GPP	3rd Generation Partnership Project
PLMN	Public Land Mobile Network
CS	Circuit Switched
PSTN	Public Switched Telephone Network
PS	Packet Switched
PDN	Packet Data Network
FDD	Frequency Division Duplex
TDD	Time Division Duplex
RNC	Radio Network Controller
BTS	Base Transceiver Station
BSC	Base Station Controller
MSC	Mobile Switching Centre
HLR	Home Location Register
AUC	Authentication Centre
PDU	Protocol Data Unit
SDU	Service Data Unit
VLR	Visitor Location Register
GPRS	General Packet Radio Service
MGW	Media GateWay
EPC	Evolved Packet Core
SAE	System Architecture Evolution
EPS	Evolved Packet System
WCDMA	Wideband Code Division Multiple Access
SS7	Signalling System No. 7
RADIUS	Remote Authentication Dial In User Service

AAA	Authentication, Authorization and Accounting
GUI	Graphical User Interface
IPFS	InterPlanetary File System
IoT	Internet of Things
AML	Anti-Money Laundering
KYC	Know Your Customer
VPMN	Visited Public Mobile Network
IRSF	International Revenue Sharing Fraud
EDR	Endpoint Detection and Response
CSP	Communication Service Providers
HPMN	Home Public Mobile Network
VAS	Value Added Services
OTT	Over the Top
DPI	Deep Packet Inspection
OSS	Operation Support System
BSS	Business Support System
AR	Augmented Reality
VR	Virtual Reality
M2M	Machine to Machine

ВСТУП

На протязі декількох останніх десятиліть, мобільні пристрої, такі як смартфони з'явилися повсюдно. Можливості мобільних систем зв'язку, починаючи з другого покоління (мережі 2G / GSM) і третього покоління (3G / UMTS), почали розширюватися. Наступним поколінням в цій еволюції, стало четверте покоління (4G / LTE). Четверте покоління "Long Term Evolution" в мережах мобільного зв'язку вже впроваджують по всьому світу. При розгляді LTE значно краще за своїх попередників не тільки в плані функціональності, але і по відношенню до безпеки та конфіденційності для абонентів. Однак проаналізувавши мережі LTE, специфікації протоколу, було виявлено декілька вразливостей, які дозволяють визначити місце розташування, управляти послугами і забезпечити витік даних. Мобільні системи зв'язку є важливою частиною життя. Використовуючи мобільні пристрої LTE в реальних мережах LTE, зловмисники проводять недорогі і практичні атаки, використовуючи ці вразливості.

Для вирішення цих недоліків може бути застосована сучасна революційна технологія блокчейну.

Акутальність роботи полягає в тому, що необхідно застосовувати нові і сучасні способи для усунення недоліків та вирішення проблем стандартів високошвидкісної передачі даних для мобільних пристроїв, що мають низку значних недоліків і уразливостей, якими користуються зловмисники. І саме технологія блокчейну пропонує багато можливостей для реалізації цих цілей.

Однак, для її ефективного застосування потрібно рішення низки особливих завдань, що пов’язані зі зміною структури мережі, організацією роботи користувачів і мереж, забезпеченням необхідного рівня захисту та безпеки даних і потрібних характеристик передачі та опрацювання даних.

Метою даної роботи є дослідження способів захисту розподілених телекомунікаційних мереж з використанням переваг технології блокчейну від

несанкціонованого доступу до службової інформації в мережах, інформації про абонентів, її видалення та заміни задля зловмисних цілей.

1 ТЕХНОЛОГІЯ LTE

1.1 Архітектурний огляд UMTS и GSM. Архітектура високого рівня

LTE був розроблений завдяки співпраці національних та регіональних органів телекомунікаційних стандартів, відомих як Проект партнерства третього покоління (3GPP) [1] і повністю відомий як 3GPP Long Term Evolution. LTE розвинувся з попередньої системи 3GPP, відомої як Універсальна система мобільного зв'язку (UMTS), яка, в свою чергу, розвинулася з Глобальної системи мобільного зв'язку (GSM). Щоб поставити LTE в контекст, ми почнемо з огляду архітектури UMTS та GSM та введення деяких важливих термінологій.

Мережа мобільних телефонів офіційно відома як загальнодоступна наземна мобільна мережа (PLMN), і керується оператором мережі, таким як Vodafone або Verizon. UMTS та GSM мають спільну мережеву архітектуру, що показано на рисунку 1.1. Є три основні компоненти, а саме: базова мережа, мережа радіодоступу та мобільний телефон.

Базова мережа містить два домени. Домен з комутованою схемою (CS) передає телефонні дзвінки через географічний регіон, який охоплює мережевий оператор, так само, як і традиційна система фіксованої лінії зв'язку. Він спілкується з телефонною мережею загального користування (PSTN), щоб користувачі могли телефонувати на наземні лінії та з комутованими доменами інших операторів мережі. Домен з комутацією пакетів (PS) транспортує потоки даних, такі як веб-сторінки та електронні листи, між користувачем та зовнішніми мережами пакетної передачі даних (PDN), такими як Інтернет.

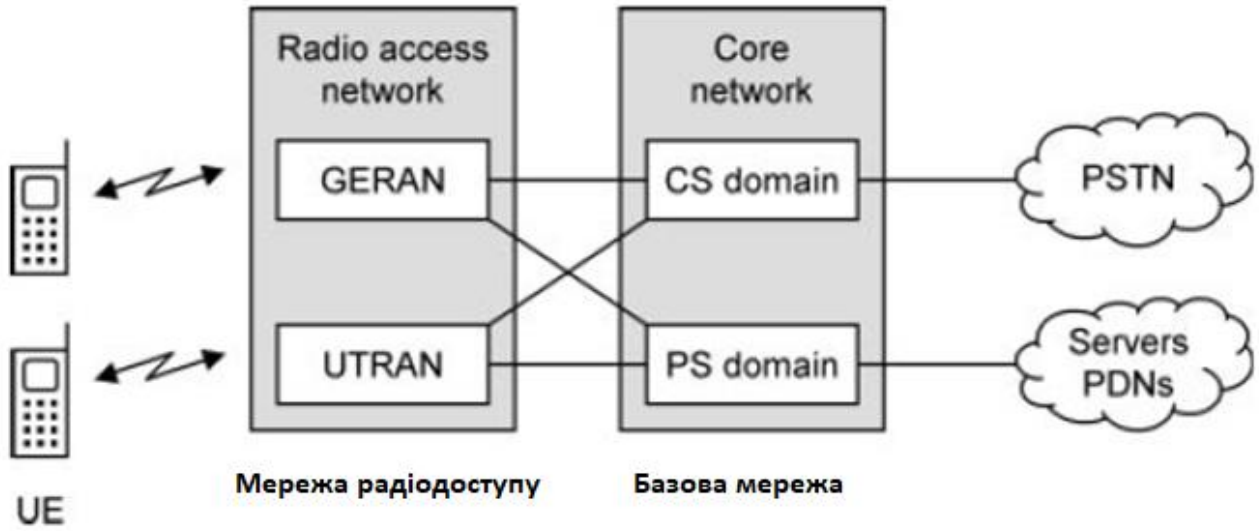


Рисунок 1.1 Архітектура високого рівня UMTS та GSM.

Ці два домена транспортують свою інформацію по-різному. Домен CS використовує метод, відомий як комутація каналів, в якому він виділяє виділене двостороннє з'єднання для кожного окремого телефонного виклику, щоб він міг передавати інформацію з постійною швидкістю передачі даних і мінімальною затримкою. Цей метод хороший, але досить неефективний: з'єднання має достатню пропускну здатність для обробки найгіршого сценарію, в якому обидва користувачі говорять одночасно, але зазвичай має занадто великий розмір. Крім того, він не підходить для передачі даних, при якій швидкість передачі даних може широко варіюватися.

Для вирішення цієї проблеми домен PS використовує інший метод, відомий як комутація пакетів. У цьому методі потік даних ділиться на пакети, кожний з яких позначається адресою необхідного пристрою призначення. Усередині мережі маршрутизатори зчитують адресні мітки вхідних пакетів даних і направляють їх у відповідні пункти призначення. Ресурси мережі розподіляються між усіма користувачами, тому цей метод більш ефективний, ніж комутація каналів. Однак можуть виникнути затримки, якщо занадто багато пристроїв будуть намагатися передавати дані одночасно, і це знайомо по роботі в Інтернеті.

Мережа радіодоступу здійснює радіозв'язок базової мережі з користувачем. На малюнку 1.1 фактично є дві окремі мережі радіодоступу, а саме мережа радіодоступу GSM EDGE (GERAN) і наземна мережа радіодоступу UMTS (UTRAN). Вони використовують різні методи радіозв'язку GSM і UMTS, але спільно використовують загальну базову мережу.

Телефонний пристрій користувача офіційно відомий як устаткування користувача (UE) і в розмовній мові називається мобільним. Він зв'язується з мережею радіодоступу за допомогою інтерфейсу, відомого як радиоинтерфейс. Напрямок від мережі до мобільного пристрою відомий як спадна лінія зв'язку (DL) або пряма лінія зв'язку, а напрямок від мобільного телефону до мережі відомо як висхідна лінія зв'язку (UL) або зворотна лінія зв'язку.

Мобільний пристрій може працювати за межами зони покриття вашого оператора мережі, використовуючи ресурси двох загальнодоступних наземних мобільних мереж: гостьовий мережі, в якій знаходиться мобільний пристрій, і домашньої мережі оператора. Ця ситуація відома як роумінг.

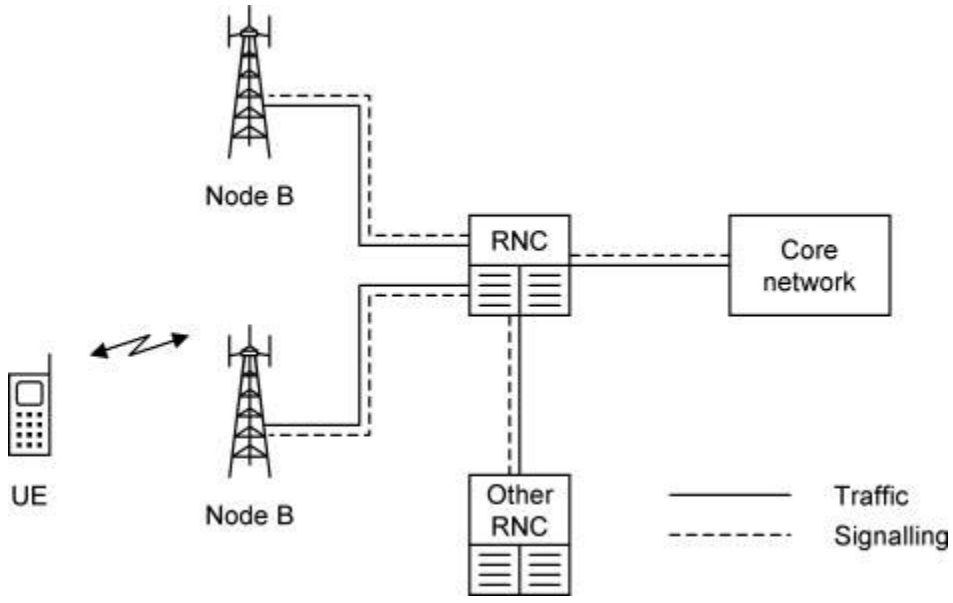


Рисунок 1.2. Архітектура наземної мережі радіодоступу UMTS.

На малюнку 1.2 показана мережа радіодоступу UMTS. Найбільш важливим компонентом є базова станція, яка в UMTS офіційно відома як вузол B. Кожна базова станція має один або кілька наборів антен, через які вона обмінюється даними з мобільними пристроями в одному або декількох секторах.

1.2 Архітектура мережі радіодоступу

Як показано на схемі, типова базова станція використовує три набори антен для управління трьома секторами, кожна з яких охоплює дугу 120 °. У такій країні середнього розміру, як Великобританія, типова мережа мобільного зв'язку може містити кілька тисяч базових станцій.

Слово сота може використовуватися двома різними способами [2]. В Європі сота, як правило, те ж саме, що і сектор, але в США це зазвичай означає групу сот, які контролює одна базова станція.

Кожна сота має обмежений розмір, який визначається максимальним діапазоном, на якому приймач може успішно чути передавач. Він також має обмежену пропускну здатність, яка є максимальною сумарною швидкістю передачі даних для всіх мобільних пристроїв в соті. Ці обмеження призводять до існування декількох типів сот. Макросоти забезпечують широке покриття в сільських районах або передмістях і мають розмір в кілька кілометрів. Мікросоти мають розмір в кілька сотень метрів і забезпечують більшу колективну ємність, яка підходить для густонаселених міських районів. Пікосоти використовуються у великих приміщеннях, таких як офіси або торгові центри, і мають ширину в кілька десятків метрів. Нарешті, абоненти можуть придбати домашні базові станції для установки в своїх будинках.

При більш уважному розгляді радіоінтерфейсу кожна мобільна і базова станції здійснюють передачу на певній радіочастоті, відомої як несуча частота. Навколо цієї несучої частоти вона займає певну кількість частотного

спектра, відомого як ширина смуги. Наприклад, мобільна станція може передавати з частотою 1960 МГц і шириною смуги 10 МГц, і в цьому випадку її передачі займатимуть діапазон частот від 1955 до 1965 МГц..

Радіоінтерфейс повинен відокремлювати передачі базових станцій від передач мобільних телефонів, щоб вони не заважали один одному. UMTS може зробити це двома способами. При використанні дуплексу з частотним поділом (FDD) базові станції здійснюють передачу на одній частоті, а мобільні станції - на інший. При використанні дуплексу з тимчасовим поділом (TDD) базові станції та мобільні станції здійснюють передачу на одній і тій же частоті, але в різний час. Радіоінтерфейс також повинен відокремлювати різні базові станції та мобільні телефони один від одного. Коли мобільний пристрій переміщається з однієї частини мережі в іншу, він повинен припинити зв'язок з однією сотою і почати зв'язок з наступною сотою. Залежно від обставин цей процес може бути виконаний з використанням двох різних методів, відомих як передача обслуговування і повторний вибір соти. В UMTS мобільний пристрій може фактично обмінюватися даними з більш ніж однією сотою одночасно в стані, відомому як м'який хендовер.

Базові станції згруповані по пристроях, відомим як контролери радіомережі (RNC). У них є дві основні задачі. По-перше, вони передають голосову інформацію користувача і пакети даних між базовими станціями і базової мережею. По-друге, вони управляють радіозв'язком мобільного телефону за допомогою сигналізації повідомлень, які невидимі для користувача, наприклад, повідомляючи мобільному телефону про перехід з однієї соти в іншу. Типова мережа може містити кілька десятків контролерів радіомережі, кожен з яких контролює кілька сотень базових станцій.

Мережа радіодоступу GSM має аналогічну конструкцію, хоча базова станція відома як базова приймальнопередаюча станція (BTS), а контролер відомий як контролер базової станції (BSC). Якщо мобільний телефон підтримує як GSM, так і UMTS, то мережа може передати його між двома

мережами радіодоступу в процесі, відомому як міжсистемна передача обслуговування.

На малюнку 1.2 ми показали трафік користувача суцільними лініями, а сигнальні повідомлення мережі - пунктирними лініями.

1.3 Архітектура базової мережі

На малюнку 1.3 показана внутрішня архітектура базової мережі. В домені з комутацією каналів медіашлюзи (MGW) маршрутизують телефонні дзвінки з однієї частини мережі в іншу, в той час як сервери мобільного комутаційного центру (MSC) обробляють сигнальні повідомлення, які встановлюють, керують і переривають телефонні дзвінки. Вони відповідно виконують функції трафіку і сигналізації двох попередніх пристроїв, відомих як центр комутації мобільного зв'язку і регістр місцеположення відвідувачів (VLR). Типова мережа може містити кілька пристроїв.

В домені з комутацією пакетів шлюзові вузли підтримки GPRS (GGSN) діють як інтерфейси для серверів і мереж пакетної передачі даних в зовнішньому світі. Обслуговуючі вузли підтримки GPRS (SGSN) маршрутизують дані між базовими станціями і GGSN і обробляють сигнальні повідомлення, які встановлюють, керують і розривають потоки даних. Ще раз, типова мережа може містити тільки кілька пристроїв.

Домашній абонентський сервер (HSS) є центральною базою даних, яка містить інформацію про всіх абонентів оператора мережі і розподіляється між двома мережевими доменами. Він об'єднує функції двох попередніх компонентів, які були відомі як регістр розташування дому (HLR) і центр аутентифікації (AuC).

1.4 Протоколи зв’язку

Як і інші системи зв'язку, UMTS і GSM передають інформацію з використанням апаратних і програмних протоколів.

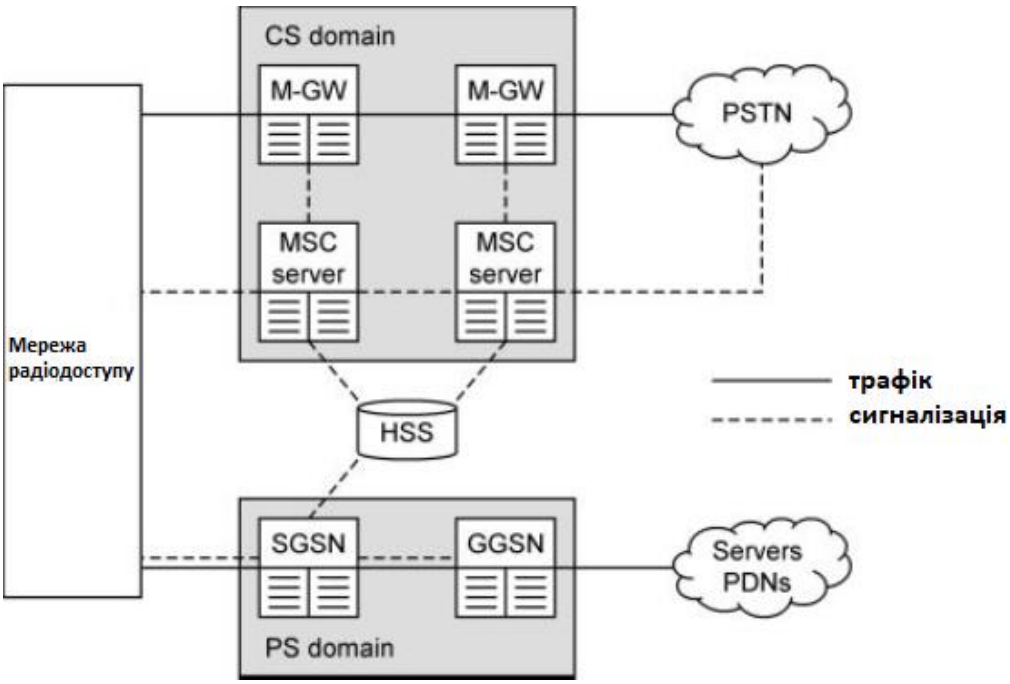


Рисунок 1.3 Архітектура основних мереж UMTS та GSM.

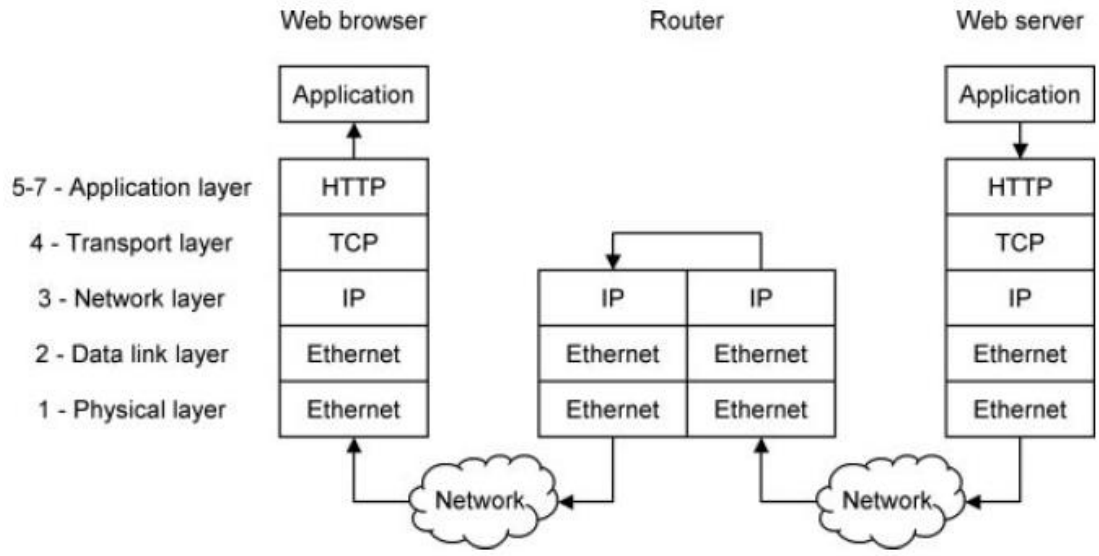


Рисунок 1.4 Приклади протоколів зв'язку, що використовуються в Інтернеті, з відображенням їх відображення на рівнях моделі OSI.

Кращий спосіб проілюструвати це насправді за допомогою протоколів, використовуваних в Інтернеті. Ці протоколи розроблені Інженерної робочою групою Інтернету (IETF) і згруповані в різні пронумеровані рівні, кожен з яких обробляє один аспект процесу передачі і прийому.

Як приклад (див. Рис. 1.4) припустимо, що веб-сервер відправляє інформацію в браузер користувача. На першому етапі протокол прикладного рівня, в даному випадку протокол передачі гіпертексту (HTTP), отримує інформацію від прикладного програмного забезпечення сервера і передає її на наступний рівень, представляючи її таким чином, що прикладний рівень користувача в кінцевому підсумку буде бути в змозі її зрозуміти. Інші протоколи прикладного рівня включають в себе простий протокол передачі пошти (SMTP) і протокол передачі файлів (FTP).

Транспортний рівень управляє наскрізною передачею даних. Є два основні протоколи. Протокол управління передачею (TCP) повторно передає пакет з кінця в кінець, якщо він надходить неправильно, і підходить для таких даних, як веб-сторінки і електронні листи, які повинні бути надійно отримані. Протокол UDP відправляє пакет без повторної передачі і підходить для таких даних, як голос або відео в реальному часі, для яких своєчасне надходження є більш важливим.

На мережевому рівні інтернет-протокол (IP) відправляє пакети по правильному маршруту від джерела до місця призначення, використовуючи IP-адреса пристрою призначення. Процес обробляється проміжними маршрутизаторами, які перевіряють IP-адреси призначення, реалізуючи тільки самі нижні три рівня стека протоколів. Канальний рівень управляє передачею пакетів від одного пристрою до наступного, наприклад, шляхом повторної передачі пакета по одному інтерфейсу, якщо він надходить неправильно. Нарешті, фізичний рівень має справу з фактичними деталями передачі; наприклад, встановивши напругу сигналу, що передається.

Інтернет може використовувати будь-які відповідні протоколи для каналу передачі даних і фізичних рівнів, такі як Ethernet.

На кожному рівні стека передавача протокол приймає пакет даних з вищевказаного протоколу в формі блоку службових даних (SDU). Він обробляє пакет, додає заголовок, щоб описати виконану ним обробку, і виводить результат у вигляді блоку даних протоколу (PDU). Процес триває до тих пір, поки пакет не досягне дна стека протоколів, після чого він буде переданий. Приймач повністю змінює процес, використовуючи заголовки, щоб допомогти йому скасувати ефект обробки передавачем.

Цей метод використовується у всіх радіодоступу та базових мережах UMTS і GSM.

1.5 Історія мобільних телекомунікаційних систем

1.5.1 Від 1G до 3G

Системи мобільного зв'язку були вперше впроваджені на початку 1980-х років. Системи першого покоління (1G) використовували методи аналогового зв'язку, які були аналогічні тим, які використовуються в традиційному аналоговому радіозв'язку. Окремі соти були великими, і системи не використовували ефективно доступний радіочастотний спектр, тому їхня пропускна здатність за сьогоднішніми стандартами була дуже мала. Мобільні пристрої були великими і дорогими і продавалися майже виключно для бізнес-користувачів.

Мобільний зв'язок став споживчим продуктом з впровадженням систем другого покоління (2G) на початку 1990-х років. Ці системи були першими, хто використав цифрову технологію, яка дозволила більш ефективно використовувати радіочастотний спектр і впровадити менші, дешевші пристрої. Спочатку вони були призначені тільки для голосового зв'язку, але згодом були вдосконалені для підтримки обміну миттєвими повідомленнями через службу коротких повідомлень (SMS). Найпопулярнішою системою 2G була Глобальна система мобільного зв'язку (GSM), яка спочатку була розроблена як загальноєвропейська технологія, але згодом стала популярною

у всьому світі. Також слід зазначити IS-95, також відомий як cdmaOne, який був розроблений Qualcomm і який став домінуючою системою 2G в США.

Успіх систем зв'язку 2G прийшов одночасно з раннім зростанням Інтернету. Для операторів мереж було природним об'єднати дві концепції, дозволяючи користувачам завантажувати дані на мобільні пристрої. Для цього, так звані системи 2.5G розширили шляхом введення домену базової мережі з комутацією пакетів і модифікації радіоінтерфейсу, щоб він міг обробляти як дані, так і голос. Служба пакетний радіозв'язок загального користування (GPRS) включила ці методи в GSM, а IS-95 була розроблена в систему, відому як IS-95B.

У той же час швидкість передачі даних через Інтернет поступово збільшувалася. Щоб відобразити це, розробники спочатку поліпшили продуктивність систем 2G, використовуючи такі методи, як Enhanced Data Rates for GSM Evolution (EDGE), а потім представили більш потужні системи третього покоління (3G) в роки після 2000 року. Системи 3G використовують різні методи для радіопередачі і прийому від їх попередників 2G, які збільшують пікові швидкості передачі даних, з якими вони можуть впоратися, і які ще ефективніше використовує доступний спектр радіочастот.

На жаль, ранні системи 3G були надмірно розкручені, і їх продуктивність спочатку не відповідала очікуванням. Через це 3G почав нормально працювати тільки після введення систем 3.5G в 2005 році. У цих системах радіоінтерфейс включає в себе додаткові оптимізації, призначені для додатків передачі даних, які збільшують середню швидкість, з якою користувач може завантажувати або закачувати інформацію за рахунок внесення більшої мінливості в швидкість передачі даних і час прибуття.

1.6 Потреба в LTE

1.6.1 Зростання мобільних даних

Протягом багатьох років голосові дзвінки домінували в трафіку мереж мобільного зв'язку. Спочатку ріст мобільної передачі даних був повільним, але в роки, що передували 2010 році, його використання стало різко збільшуватися. Щоб проілюструвати це, на малюнку 1.5 показані вимірювання Ericsson загального трафіку, що обробляється мережами в усьому світі, в петабайт (мільйон гігабайт) в місяць [3]. Ця цифра охоплює період з січня 2007 року по липень 2011 року, коли обсяг трафіку даних збільшився більш ніж в 100 разів.

Ця тенденція буде продовжуватися. Наприклад, на малюнку 1.6 показані прогнози Analysys Mason про зростання мобільного трафіку в період з 2011 по 2016 рік. Зверніть увагу на різницю в вертикальних масштабах двох діаграм.

Частково це зростання було обумовлене збільшенням доступності технологій зв'язку 3.5G. Однак більш важливим була поява Apple iPhone в 2007 році, за яким послідували пристрої на базі операційної системи Android від Google з 2008 року. Ці смартфони були більш привабливими і зручними у використанні, ніж їх попередники, і призначалися для підтримки створення додатків третіми сторонами. партія розробників. В результаті цих проблем мережі 2G і 3G почали перевантажуватися приблизно в 2010 році, що призвело до вимоги збільшити пропускну здатність мережі. У наступному пункті ми розглянемо обмеження на пропускну здатність системи мобільного зв'язку та покажемо, як можна домогтися такого збільшення пропускної здатності.

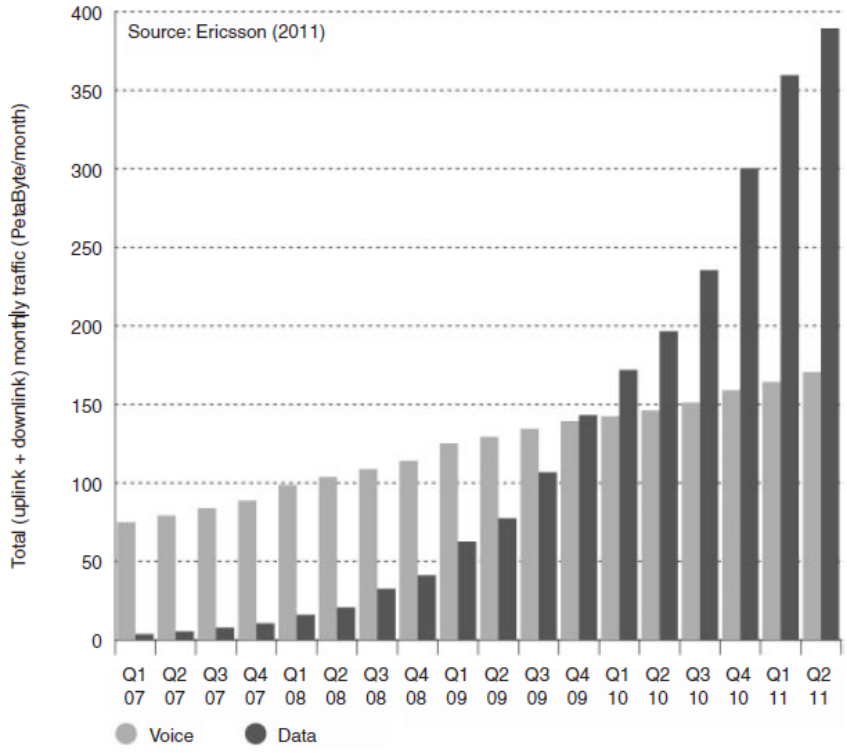


Рисунок 1.5 Вимірювання голосового трафіку і трафіку даних у всесвітніх мережах мобільного зв'язку в період з січня 2007 року по липень 2011 року

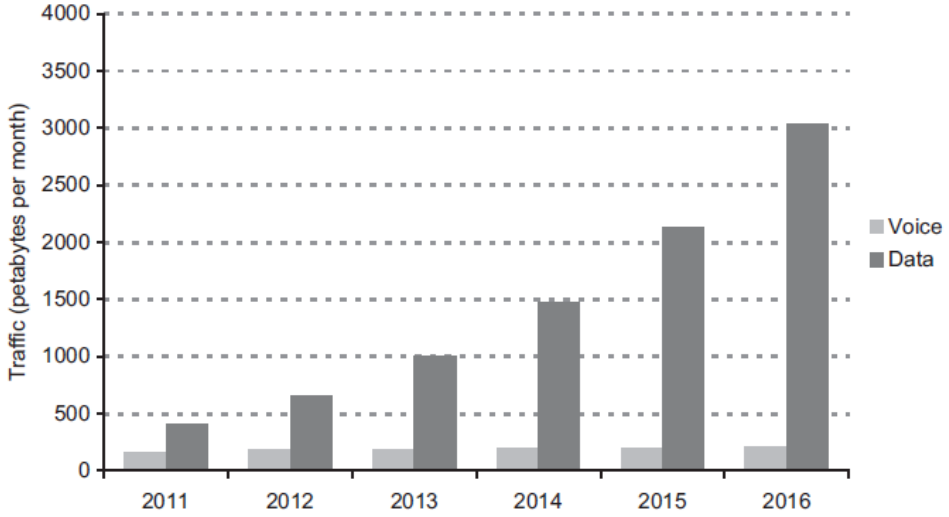


Рисунок 1.6. Прогнози голосового трафіку і трафіку даних у всесвітніх мережах мобільного зв'язку в період з 2011 по 2016 рр. Дані надані Analysys Mason

Результатом став вибух числа і використання мобільних додатків, що відображено на діаграмах. В якості допоміжного фактора оператори мереж раніше намагалися стимулювати зростання мобільних даних шляхом введення схем фіксованою тарифікації, які дозволяли необмежене завантаження даних. Це призвело до того, що ні розробники, ні користувачі не були мотивовані обмежувати споживання даних.

1.6.2 Збільшення пропускної здатності системи

Існує три основних способи збільшити пропускну здатність системи мобільного зв'язку, які ми можемо зрозуміти, вивчивши рівняння Шеннона і рисунок 1.7.

$$C = B \log_2 \left(1 + \frac{S}{N}\right)$$

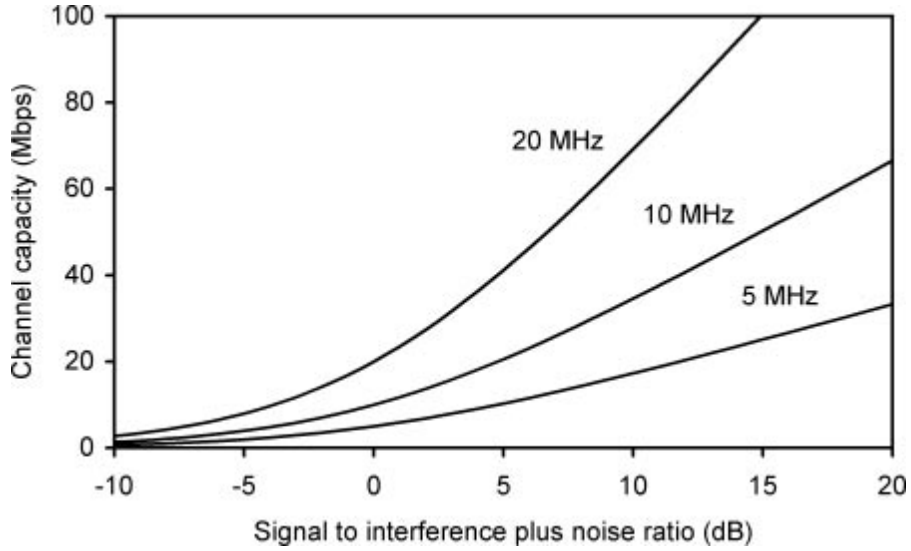


Рисунок 1.7 Пропускна здатність системи зв'язку Шеннона в смугах частот 5, 10 і 20 МГц

Перше і найважливіше - це використання менших сот. У мережі пропускна здатність каналу - це максимальна швидкість передачі даних, яку може обробляти одна сота. Створюючи додаткові базові станції та

зменшуючи розмір кожної соти, ми можемо збільшити пропускну здатність мережі.

Другий метод полягає в збільшенні пропускної спроможності. Радіочастотний спектр керується Міжнародним союзом електрозв'язку (МСЕ) і регіональними і національними регуляторними органами, і зростаюче використання рухомого електрозв'язку призвело до збільшення розподілу спектра для систем 2G і 3G. Проте, є тільки обмежена кількість доступного радіоспектра, і це також є необхідним для таких різноманітних додатків, як військовий зв'язок і радіоастрономія. Тому існують межі того, наскільки далеко може зайти цей процес.

Третій метод - поліпшити комунікаційні технології, які ми використовуємо. Це дає декілька переваг: це дозволяє нам наблизитися до теоретичної пропускної здатності каналу і використовувати більш високу SINR і велику пропускну здатність, які стали можливими завдяки іншим змінам, описаним вище. Це прогресивне вдосконалення комунікаційних технологій було постійною темою в розвитку мобільних телекомунікацій і є основною причиною введення LTE.

1.6.3 Додаткові причини

Три інші наслідки ведуть до переходу на LTE. По-перше, оператор 2G або 3G повинен підтримувати дві базові мережі: домен з комутацією каналів для голосу і домен з комутацією пакетів для даних. За умови, що мережа не занадто перевантажена, однак, також можливо передавати голосові виклики по мережах з комутацією пакетів, використовуючи такі методи, як передача голосу по IP (VoIP). Роблячи це, оператори можуть перемістити все в домен з комутацією пакетів і можуть зменшити свої капітальні та експлуатаційні витрати. В зв’язку з цим існує проблема в мережі 3G - вводяться затримки близько 100 мілісекунд для додатків даних при передачі пакетів даних між елементами мережі і за допомогою телефону. Це ледь прийнятно для голосу і

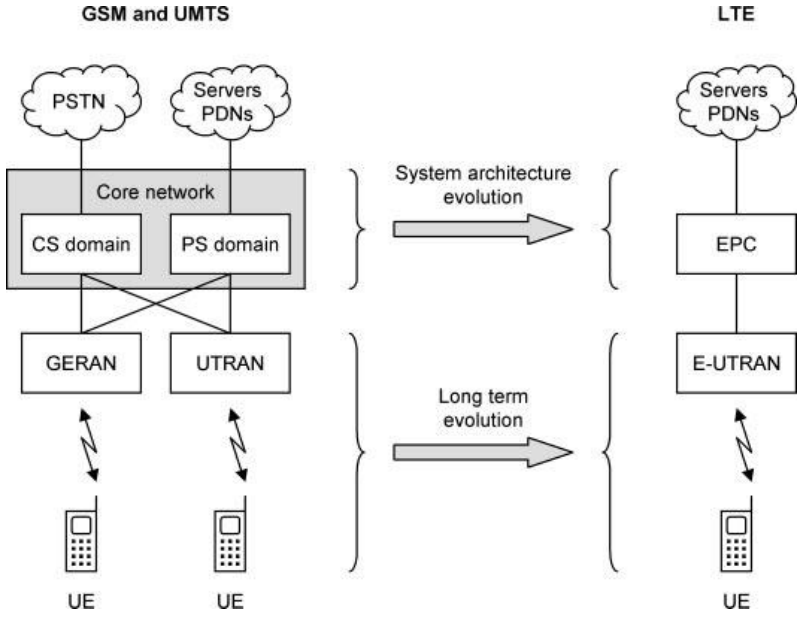
створює великі труднощі для більш вимогливих додатків, таких як інтерактивні ігри в реальному часі. Таким чином, другим драйвером є бажання зменшити наскрізну затримку або затримку в мережі.

По-третє, специфікації для UMTS і GSM з роками стають все більш складними через необхідність додавати нові функції в систему при збереженні зворотної сумісності з більш ранніми пристроями. Новий етап допомагає завданню дизайнерів, дозволяючи їм підвищити продуктивність системи без необхідності підтримки застарілих пристроїв.

1.7 Від UMTS до LTE

1.7.1 Архітектура високого рівня LTE

У 2004 році 3GPP почав вивчення довгострокової еволюції UMTS. Метою було зберегти конкурентоспроможність систем мобільного зв'язку 3GPP протягом 10 і більше років, забезпечуючи високі швидкості передачі даних і мінімальні затримки, які будуть потрібні майбутнім користувачам.



Рисунко 1.8 Ілюстрація підсумкової архітектури і того, як ця архітектура розвивалася в порівнянні з UMTS.

У новій архітектурі вдосконалене пакетне ядро (EPC) є прямою заміною домену з комутацією пакетів UMTS і GSM. Він поширює всі види інформації користувачеві, голосові і дані, використовуючи технології комутації пакетів, які традиційно використовувалися тільки для даних. Ве відсутній еквівалент домену з комутацією каналів: замість цього голосові виклики передаються з використанням голосу по IP. Розвинена наземна мережа радіодоступу UMTS (E-UTRAN) забезпечує радіозв'язок EPC з мобільною станцією, тому є прямою заміною UTRAN. Мобільний пристрій все ще представляється як устаткування користувача, хоча його внутрішня робота сильно відрізняється від попередньої.

Нова архітектура була розроблена як частина двох робочих елементів 3GPP, а саме: еволюція архітектури системи (SAE), яка охоплювала базову мережу, і довгострокова еволюція (LTE), яка охоплювала мережу радіодоступу, радіоінтерфейс і мобільний зв'язок. Офіційно вся система відома як розвинена пакетна система (EPS), тоді як абревіатура LTE відноситься тільки до розвитку радіоінтерфейсу. Незважаючи на це офіційне використання, LTE стало розмовною назвою для всієї системи і регулярно використовується таким чином 3GPP.

1.7.2 Long Term Evolution

Основним результатом дослідження довгострокової еволюції стала специфікація вимог до радіоінтерфейсу [4], в якій найбільш важливими були такі вимоги.

LTE потрібно забезпечити пікову швидкість передачі даних 100 Мбіт / с в низхідній лінії зв'язку і 50 Мбіт / с у висхідній лінії зв'язку. Ця вимога була перевищена в можливій системі, яка забезпечує пікові швидкості передачі даних 300 Мбіт / с і 75 Мбіт / с відповідно. Для порівняння, пікова швидкість передачі даних WCDMA в версії 6 специфікацій 3GPP становить 14 Мбіт / с в низхідній лінії зв'язку і 5,7 Мбіт / с в висхідній лінії зв'язку.

Однак не можна занадто сильно підкреслити, що ці пікові швидкості передачі даних можуть бути досягнуті тільки в ідеалізованих умовах і абсолютно недосяжні при будь-якому реалістичному сценарії. Кращою мірою є спектральна ефективність, яка виражає типову пропускну здатність однієї соти на одиницю смуги пропускання. LTE повинен був підтримувати спектральну ефективність в три-чотири рази більше, ніж у WCDMA версії 6 в низхідній лінії зв'язку і в два-три рази вище в висхідній лінії зв'язку.

Затримка - ще одна важлива проблема, особливо для критичних до часу додатків, таких як голосові та інтерактивні ігри. Тут є два аспекти. По-перше, вимоги свідчать, що час, необхідний для передачі даних між мобільним телефоном та фіксованого мережею, має бути менше п'яти мілісекунд за умови, що радіоінтерфейс не перевантажений. По-друге, в розділі 2 ми побачимо, що мобільні телефони можуть працювати в двох станах: в активному стані, в якому вони обмінюються даними з мережею, і в режимі очікування з низьким енергоспоживанням. Вимоги свідчать, що телефон повинен перемкнутися з режиму очікування в активний стан після втручання користувача менш ніж за 100 мілісекунд.

Є також вимоги щодо охоплення та мобільності. LTE оптимізований для осередків розміром до 5 км, працює з погіршеними характеристиками до 30 км і підтримує розміри сот до 100 км. Він також оптимізований для швидкостей до 15 км / год, працює з високою продуктивністю до 120 км / с і підтримує швидкість до 350 км / ч. Нарешті, LTE призначений для роботи з різними смугами пропускання, які варіюються від 1,4 МГц до максимум 20 МГц.

Специфікація вимог в кінцевому підсумку привела до детального проектування радіоінтерфейсу LTE. В інтересах тих, хто знайомий з іншими системами, в таблиці 1.1 узагальнені її основні технічні характеристики і порівняні з аналогічними характеристиками WCDMA. ,

1.7.3 Еволюція системної архітектури

Основним результатом дослідження еволюції архітектури системи була специфікація вимог для фіксованої мережі [5], в якій найбільш важливими були такі вимоги.

Таблиця 1.1 Основні характеристики радіоінтерфейсів WCDMA і LTE

Feature	WCDMA	LTE
Схема множинного доступу	WCDMA	OFDMA та SC-FDMA
Частота повт. використання	100%	Гнучка
Використання антен MIMO	З версії 7	Так
Смуга пропускання	5 MHz	1.4, 3, 5, 10, 15 чи 20 MHz
Тривалість кадру	10 ms	10 ms
Інтервал часу передачі	2 чи 10 ms	1 ms
Режими роботи	FDD та TDD	FDD та TDD

Розвинуте ядро пакетів маршрутизує пакети з використанням Інтернет-протоколу (IP) і підтримує пристрої, що використовують IP-версію 4, IP-версію 6 або IP-версію з двома стеками, версія 4 / версія 6. Крім того, EPC надає користувачам постійне підключення до зовнішнього світу, встановлюючи базове IP-з'єднання для пристрою при його включенні і підтримуючи цю сполуку до його виключення. Це відрізняється від поведінки UMTS і GSM, в якому мережу встановлює IP-з'єднання тільки за запитом і розриває це з'єднання, коли воно більше не потрібно.

EPC спроектований як канал передачі даних, який просто передає інформацію користувачеві і від нього: він не пов'язаний з інформаційним вмістом або з додатком. Це схоже на поведінку Інтернету, який транспортує пакети, які виходять із будь-якого прикладного програмного забезпечення, але відрізняється від такого в традиційній телекомунікаційній системі, в якій голосовий додаток є невід'ємною частиною системи. Через це голосові програми не утворюють частину LTE: замість цього голосові виклики

управляються деяким зовнішнім об'єктом, таким як IP-мультимедійна підсистема (IMS). EPC просто транспортує голосові пакети так само, як і будь-який інший потік даних.

На відміну від Інтернету, EPC містить механізми для вказівки і контролю швидкості передачі даних, частоти помилок і затримки, які отримає потік даних. Не існує явної вимоги щодо максимального часу, необхідного для проходження даних через EPC, але відповідна специфікація пропонує затримку площині користувача в 10 мілісекунд для мобільного телефону без роумінгу, збільшується до 50 мілісекунд в типовому сценарії роумінгу [6].

Таблиця 1.2 Основні характеристики мереж радіодоступу UMTS та LTE

Особливість	UMTS	LTE
Складові частини мережі радіодоступу	Node B, RNC	eNB
Стани протоколу RPC	CELL_DCH, CELL_FACH, CELL_PCH, URA_PCH, RRC_IDLE	RRC_CONNECTED, RRC_IDLE
Хендовери	М'який і жорсткий	Жорсткий
Список сусідів	Завжди потрібен	Не потрібен

Таблиця 1.3 Основні характеристики основних мереж UMTS та LTE

Особливість	UMTS	LTE
IP версії	IPv4 and IPv6	IPv4 and IPv6
USIM підтримка	Реліз 99 USIM і далі	Реліз 99 USIM і далі
Транспорті механізми	Комутація каналів і пакетів	Пакетна комутація
Компоненти домену CS	MSC сервер, MGW	-
Компоненти домену PS	SGSN, GGSN	MME, S-GW, P-GW
Підключення по IP	Після регістрації	Під час регістрації
Голос і СМС	Включені	Зовнішні

EPC також потрібно для підтримки міжсистемних передач обслуговування між LTE і більш ранніми технологіями 2G і 3G. Вони охоплюють не тільки UMTS і GSM, але і системи не 3GPP, такі як cdma2000 і WiMAX.

У таблицях 1.2 і 1.3 підсумовані ключові характеристики мережі радіодоступу і розвиненого ядра пакету і порівняні їх з відповідними функціями UMTS.

1.8 Від LTE до LTE-Advanced

1.8.1 Вимоги МСЕ до 4G

Проектування LTE відбулося одночасно з ініціативою Міжнародного союзу електрозв'язку. В кінці 1990-х років МСЕ посприяв у розвитку технологій 3G, опублікувавши набір вимог до системи мобільного зв'язку 3G під назвою International Mobile Telecommunications (IMT) 2000.

МСЕ запустив аналогічний процес в 2008 році, опублікувавши набір вимог для системи зв'язку четвертого покоління (4G) під назвою IMT-Advanced [7-9]. Згідно з цими вимогами, максимальна швидкість передачі даних сумісної системи повинна становити не менше 600 Мбіт / с в низхідній лінії зв'язку і 270 Мбіт / с в висхідній лінії в смузі пропускання 40 МГц. Відразу видно, що ці цифри перевищують можливості LTE.

1.8.2 Вимоги LTE-Advanced

Керуючись вимогами МСЕ до IMT-Advanced, 3GPP почав вивчати способи розширення можливостей LTE. Основним результатом дослідження була специфікація системи, відомої як LTE-Advanced [10], в якій основними вимогами були наступні.

LTE-Advanced повинен був забезпечити пікову швидкість передачі даних 1000 Мбіт / с в низхідній лінії зв'язку і 500 Мбіт / с в висхідній лінії

зв'язку. На практиці система була розроблена таким чином, щоб в кінцевому підсумку вона могла забезпечувати пікові швидкості передачі даних 3000 і 1500 Мбіт / с відповідно, використовуючи загальну смугу пропускання 100 МГц, яка складається з п'яти окремих компонентів по 20 МГц кожна. Зверніть увагу, як і раніше, ці цифри недосяжні при будь-якому реалістичному сценарії.

Специфікація також включає цілі для ефективності використання спектра в певних тестових сценаріях. Порівняння з відповідними показниками для WCDMA [11] має на увазі, що спектральна ефективність в 4,5-7 разів вище, ніж у версії 6 WCDMA в низхідній лінії зв'язку, і в 3,5-6 разів вище в висхідній лінії. Нарешті, LTE-Advanced розроблений для забезпечення сумісності з LTE в тому сенсі, що мобільний телефон LTE може зв'язуватися з базовою станцією, яка працює з LTE-Advanced, і навпаки.

1.8.3 Значення 4G

Спочатку MCE припускав, що термін 4G повинен використовуватися тільки для систем, які відповідають вимогам IMT-Advanced. LTE цього не зробив, як і мобільний WiMAX 1.0 (IEEE 802.16e). Через це, інженерне співтовариство прийшло, щоб описати ці системи як 3.9G. Ці міркування, однак, не завадили маркетинговый спільноті описати LTE і мобільний WiMAX 1.0 як технології 4G. Хоча цей опис було необгрунтованим з точки зору продуктивності, насправді в цьому була певна логічна логіка: існує чіткий технічний перехід при переході від UMTS до LTE, якого немає при переході від LTE до LTE-Advanced.

Незабаром MCE визнав свою поразку. У грудні 2010 року MCE благословив використання 4G для опису не тільки LTE і мобільного WiMAX 1.0, але також і будь-якої іншої технології з істотно кращою продуктивністю, ніж в ранніх системах 3G [12]. Вони не визначили слова «істотно краще», але нам просто потрібно знати, що LTE - це система мобільного зв'язку 4G.

1.8.4 Архітектура мереж LTE / LTE Advanced

Архітектура мережі LTE розроблена таким чином, щоб забезпечити підтримку пакетного трафіку з мобільністю, мінімальними затримками доставки пакетів і високими показниками якості обслуговування.

Мобільність як функція мережі забезпечується двома її видами: дискретною мобільністю (роумінгом) і безперервною мобільністю (хендовера). Оскільки мережі LTE повинні підтримувати процедури, роумінгу та хендовера з усіма існуючими мережами, для LTE-абонентів (терміналів) має забезпечуватися повсюдне покриття послуг бездротового широкосмугового доступу.

Пакетна передача дозволяє забезпечити всі послуги, включаючи передачу призначеного для користувача голосового трафіку. На відміну від більшості мереж попередніх поколінь, в яких спостерігається досить висока різнотипність і ієрархічність мережевих вузлів (так звана розподілена мережева відповідальність), архітектуру мереж LTE можна назвати «плоскою», оскільки практично вся мережеве взаємодія відбувається між двома вузлами: базовою станцією (БС), яка в технічних специфікаціях називається B-вузлом (Node-B, eNB) і блоком управління мобільністю БУМ (MME, Mobility Management Entity), як правило, включає і мережевий шлюз Ш (GW, Gateway), тобто мають місце комбіновані блоки MME / GW.

Відзначимо, що контролер радіомережі, який грав дуже значну роль в мережах попередніх поколінь, усунутий від управління потоком даних (фактично він навіть відсутній в структурних схемах), а його традиційні функції - управління радіоресурсами стиснення заголовків, шифрування, надійна доставка пакетів і ін. передані безпосередньо БС.

БУМ працює тільки зі службовою інформацією - так званою мережевою сигналізацією, так що IP-пакети, що містять інформацію користувача, через нього не проходять. Перевага наявності такого окремого блоку сигналізації в тому, що пропускну здатність мережі можна незалежно

нарощувати як для користувача трафіку, так і для службової інформації. Головною функцією БУМ є управління терміналами користувачів (КТ), що знаходяться в режимі очікування, включаючи перенаправлення і виконання викликів, авторизацію і аутентифікацію, роумінг та хендовер, встановлення службових і призначених для користувача каналів і ін.

Серед всіх мережевих шлюзів окремо виділені два: обслуговуючий шлюз ОШ (S-GW, Serving Gateway) і шлюз пакетної мережі (P-GW, Packet Data Network Gateway), або, коротше, пакетний шлюз (ПШ). ОШ функціонує як блок управління локальною мобільністю, приймаючи і пересилаючи пакети даних, що відносяться до БС і обслуговується їм ПВ. ПШ є інтерфейсом між набором БС і різними зовнішніми мережами, а також виконує деякі функції IP-мереж, такі, як розподіл адрес, забезпечення користувальницьких політик, маршрутизація, фільтрація пакетів і ін.

Як і в більшості мереж третього покоління, в основу принципів побудови мережі LTE покладено поділ двох аспектів: фізичного реалізації окремих мережевих блоків і формування функціональних зв'язків між ними. При цьому завдання фізичної реалізації вирішуються, виходячи з концепції області (domain), а функціональні зв’язки розглядаються в рамках прошарка (stratum). Первинним поділом на фізичному рівні є поділ архітектури мережі на область користувацького обладнання (UED, User Equipment Domain) і область мережевої інфраструктури (ID, Infrastructure Domain). Остання, в свою чергу, поділяється на (під) мережу радіодоступу (E-UTRAN, Evolved Universal Terrestrial Radio Access Network) і базову (пакетну) (під) мережу (EPC, Evolved Packet Core). Устаткування користувача - це сукупність КТ з різними рівнями функціональних можливостей, які використовуються мережевими абонентами для доступу до LTE-послуг. При цьому в якості призначеного для користувача терміналу може фігурувати як реальний («живий») абонент, який користується, наприклад, послугами голосового трафіку, так і знеособлений пристрій, призначений для передачі / прийому певних мережевих або призначених для користувача додатків.

На малюнку 1.9 показана узагальнена структура мережі LTE, з якої видно наявність двох шарів функціональних зв'язків: шару радіодоступу (AS, Access Stratum) і відсутність шару радіодоступу (NAS, Non-Access Stratum).

Показані на малюнку 1.9 овали зі стрілками позначають точки доступу до послуг.

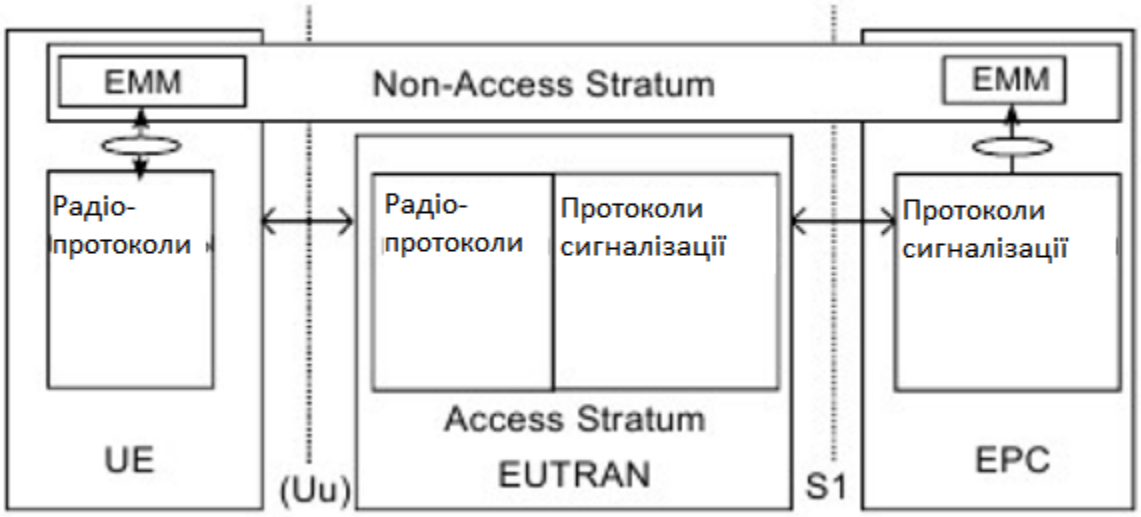


Рисунок 1.9 Узагальнена структура мережі LTE

Стик між областю UE користувацького обладнання і областю мережі радіодоступу UTRAN називається Uu-інтерфейсом; стик між областю мережі радіодоступу і областю базової мережі EPC - S1-інтерфейсом. Склад і функціонування різних протоколів, що відносяться до інтерфейсів Uu і S1, розділені на дві так звані площини: площину призначену для користувача (UP, User Plane) і площину управління (CP, Control Plane).

Поза рівнем доступу діють механізми управління мобільністю в базовій мережі (EMM, EPC Mobility Management).

У користувальницької площині реалізовані протоколи, що забезпечують передачу даних користувача по радіоканалу. До площини управління відносяться ті протоколи, які в різних аспектах забезпечують з'єднання між КТ та мережею. Також до цієї площини відносяться протоколи,

призначені для транспарентной (прозорою) передачі повідомлень, що відносяться до надання різних послуг.

Область мережі радіодоступу логічно розділена на два рівні: рівень радіомережі (RNL, Radio Network Layer) і рівень транспортної мережі (TNL, Transport Network Layer). Взаємодія входящих в область мережі радіодоступу БС здійснюється на основі X2-інтерфейсу (рисунок 1.10). Крім того, має місце транзитне сполучення між базовими станціями і базовою мережею через блок управління мобільністю (S1-MM-інтерфейс) або обслуговуючий вузол (S1-U-інтерфейс) - на малюнку 1.10 не показані. Таким чином, можна стверджувати, що S1-інтерфейс підтримує множинні відносини між набором БС і блоками БУМ / ОУ.

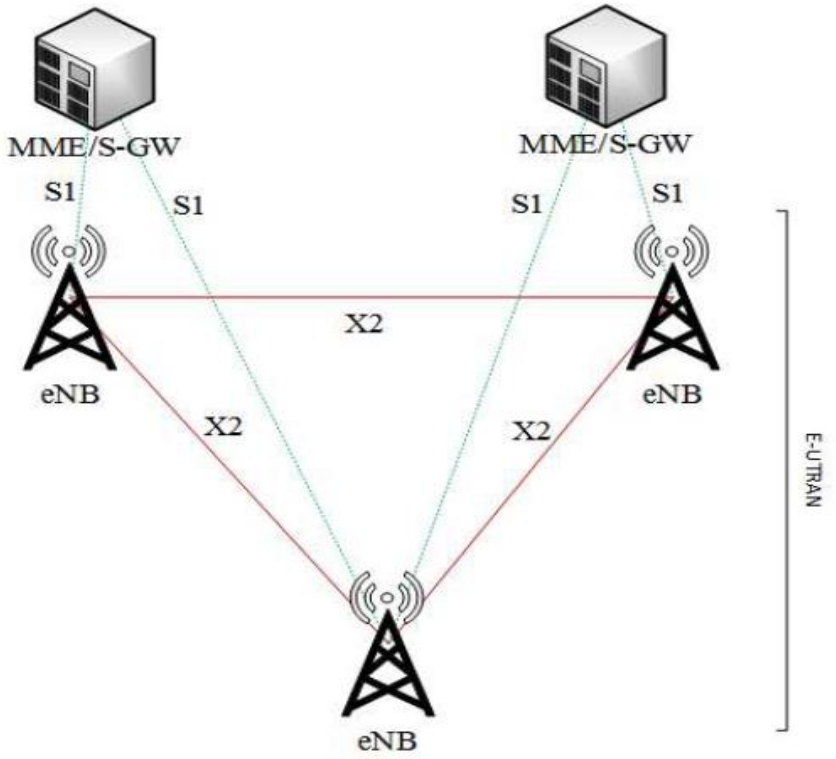


Рисунок 1.10 З'єднання функціональних вузлів мережі радіодоступу

Перш, ніж звернутися до вивчення протоколів мережі LTE, визначених у різних інтерфейсах і площинах, розглянемо призначення функціональних блоків мережі радіодоступу.

На БС в мережах LTE покладено виконання таких функцій:

- Управління радіоресурсами: розподіл радіоканалів, динамічний розподіл ресурсів в висхідних і низхідних напрямках - так звана диспетчеризація ресурсів (scheduling) і ін .;
- Стиснення заголовків IP-пакетів, шифрування потоку даних користувача;
- Вибір блоку управління мобільністю при включенні в мережу призначеного для користувача терміналу при відсутності у того інформації про минуле підключення;
- Маршрутизація в призначеній для користувача площині пакетів даних у напрямку до обслуговуючого шлюзу;
- Диспетчеризація та передача мовної інформації, отриманої від БУМ;
- Диспетчеризація та передача повідомлень PWS (Public Warning System, система тривожного сповіщення), отриманих від БУМ;
- Вимірювання і складання відповідних звітів для управління мобільністю та диспетчеризацією.

Блок управління мобільністю забезпечує виконання таких функцій:

- Передача захищеної інформації про точки доступу до послуг і захищене управління точками доступу;
- Передача інформації в базову мережу для управління мобільністю між різними мережами радіодоступу;
- Управління БС, що знаходяться в стані очікування, включаючи перенаправлення викликів;
- Управління списком зон відстеження КТ;
- Вибір обслуговуючого шлюзу і шлюзу пакетної мережі для мереж радіодоступу різних стандартів;
- Вибір нового блоку управління мобільністю при виконанні хендовера;
- Роумінг;
- Аутентифікація;

- Управління радіоканалом, включаючи установку виділеного каналу. Обслуговуючий вузол відповідає за виконання таких функцій:
- Вибір точки прив'язки локального місця розташування (Local Mobility Anchor) при хендовері;
- Буферизація пакетів даних в низхідному напрямку, призначених для КТ, що знаходяться в режимі очікування, і ініціалізація процедури запиту послуги;
- Санкціоноване перехоплення інформації користувачів;
- Маршрутизація і перенаправлення пакетів даних;
- Маркування пакетів транспортного рівня;
- Формування облікових записів користувачів і ідентифікатора класу якості обслуговування для тарифікації;
- Тарифікація абонентів.

Шлюз пакетної мережі забезпечує виконання таких функцій:

- Фільтрація користувальницьких пакетів;
- Санкціоноване перехоплення інформації користувачів;
- Розподіл IP-адрес для ПТ;
- Маркування пакетів транспортного рівня в низхідному напрямку;
- Тарифікація послуг, їх селекція.

Висновок до розділу 1

В результаті написання даного розділу була розлянута історія появи та розвитку такого стандарту передачі даних як LTE. Дізналися, що він має як деякі спільні принципи з попередніми стандартами, так і прогресивні відмінності. Пояснили, що перехід від UMTS до LTE є логічним та правильним кроком в розвитку мобільного зв’язку.

Оглянули та дали саме поняття архітектури LTE, короткий принцип роботи на певні переваги для сучасного користувача.

2 ВРАЗЛИВОСТІ LTE

2.1 Загальна оцінка недоліків LTE

LTE забезпечує теоретичну пікову швидкість передачі даних до 326,4 Мбіт / с від базової станції до користувача і до 172,8 Мбіт / с у зворотному напрямку. Для порівняння, мережі другого покоління (2G) теоретично здатні забезпечити пікову швидкість передачі даних за допомогою технології GPRS 56- 114 Кбіт / с. Мережі третього покоління (3G) забезпечують швидкість передачі даних до 3,6 Мбіт / с.

Системи 2G мали кілька вразливостей. Відсутність взаємної перевірки автентичності між пристроєм мобільного зв'язку та мережею має на увазі, що зловмисник має можливість встановити підроблені базові станції і переконати мобільні пристрої підключиться до нього. У 2G системах введений International Mobile Subscriber Identity (IMSI) - міжнародний ідентифікатор мобільного абонента (індивідуальний номер абонента). Однак при відсутності взаємної перевірки автентичності, фальшиві базові станції можуть бути використані в якості "IMSI - пасток" для збору інформації та відстеження поведінки користувачів. У специфікації 3G введені взаємні перевірки автентичності і використання більш міцних і добре проаналізованих криптографічних алгоритмів. Технічні характеристики LTE і далі зміцнюють сигнальні протоколи, вимагаючи перевірки автентичності та шифрування. Оскільки IMSI є постійним ідентифікатором абонента LTE, в специфікації необхідно звести до мінімуму його передачу по каналах радіозв'язку з міркувань безпеки і конфіденційності. Замість цього використовується глобальний унікальний тимчасовий ідентифікатор Globally Unique Temporary Identifier (GUTI), який дозволяє ідентифікувати абонентів в мережі радіозв'язку.

Компанія Positive Technologies, що спеціалізується на аналізі вразливостей інформаційних систем, в своєму дослідженні зазначила, що 4G

/ LTE мережі операторів схильні до перехоплення SMS повідомлень, розкриття місця розташування абонента, Dos-атак на абонентів і на обладнання операторів. Мережі 4G успадкували повний спектр загроз, актуальний для попередніх поколінь мереж зв'язку, говориться в дослідженні.

У минулому році експерти Positive Technologies провели дослідження вразливостей 3G-мереж в Європі і Азії. Під час його проведення в 80% випадків вдалося довести успішність проведення атак, спрямованих на збої в роботі, в 77% - можливість перехоплення SMS і голосових викликів, визначення місця розташування (при атаках з метою викликати витік інформації) і в 67% - успішність крадіжки грошей з рахунків абонентів і ін. при шахрайських атаках. Вибірка становила близько 50 світових операторів.

2.2 Різні види атак

2.2.1 SS7

Розроблена близько п’ятдесяти років тому система SS7 (ОКС-7) має певні недоліки в плані захищеності (наприклад, відсутність шифрування і перевірка справжності службових повідомлень). Мережа підтримує потреби мобільного зв'язку і надання додаткових послуг. На початку 2000-х була запропонована специфікація SIGTRAN, що дозволила передавати службову інформацію SS7 по IP-мережам. Сигнальна мережа перестала бути ізольованою.

Для доступу в сигнальну мережу потрібен SS7-шлюз. Але отримати до нього доступ непросто. Можна отримати операторську ліцензію, потрапити в мережу через зламане операторське обладнання, GGSN або фемтосоту.

Завдяки вразливостям можливо отримати баланс абонента, перехопити вхідне повідомлення, прослухати виклик, вкрасти інформацію про абонента, визначити його місцезнаходження, а також, здійснити шахрайство: перенаправлення вхідного дзвінка, перевести грошові кошти за допомогою

USSD, змінити профіль абонента, перенаправити вихідний дзвінок, здійснити Dos-атаки.

Більшість атак на мережі SS7 були можливі через відсутність перевірки реального місця розташування абонента. На другому і третьому місцях у списку причин - неможливість перевірки приналежності абонента мережі і відсутність фільтрації невикористовуваних сигнальних повідомлень. На четвертій позиції - помилки конфігурації SMS Home Routing.

2.2.2 Уразливість протоколу Diameter

Diameter - це протокол сімейства AAA, і є розвитком RADIUS. Призначений він, головним чином, для оцінки послуг в мережах зв'язку. Зокрема, в мережах 3G з його допомогою відбувається оцінка послуг передачі даних, а в IMS \ LTE протокол є одним з основних елементів, що управляють.

Важливою особливістю протоколу є його розширюваність і можливість створення не тільки власних атрибутів, але і додатків.

Базовий протокол реалізує вимоги до протоколів AAA, деталі яких відображені в RFC2989, і описує процес встановлення з'єднання, перевірку сумісності, правила відправки повідомлень і їх маршрутизації, розрив з'єднання.

В якості транспорту можуть використовуватися TCP і SCTP. Безпека протоколу повинна забезпечуватися на транспортному рівні, в рекомендаціях також зазначено, що протокол не повинен використовуватися без TLS, DTLS або IPsec. У довіреної мережі, зрозуміло, можна обійтися і без них, зокрема, якщо внутрішню мережу підприємства можна вважати надійною.

Специфікація визначає кілька типів вузлів Diameter. Для розуміння ролі вузлів необхідно ввести два терміна, які більш детально будуть розглянуті нижче.

Сесія - контролює стан абонента і включає в себе ті і тільки ті повідомлення, які відносяться до окремо взятого абоненту.

З'єднання - контролює стан зв'язку між вузлами Diameter.

Клієнт

Клієнтом зазвичай виступає мережевий пристрій, який безпосередньо обробляє трафік абонента.

Сервер

Роль сервера цілком зрозуміла, він повинен контролювати стан абонентських сесій.

Агент.

DIAMETER агенти є проміжними вузлами між клієнтом і сервером і виконують функції управління трафіком. Наприклад, вони можуть агрегувати повідомлення від пристроїв на одному майданчику, виконувати роль балансувальника навантаження, модифікувати пакети Diameter, виступати в ролі шлюзів безпеки при переході із довіреної мережі в публічну.

Мережа 4G на базі сигнального протоколу Diameter володіє уразливостями, що дозволяють реалізовувати атаки, пов'язані з визначенням місця розташування абонента, перехопленням sms-повідомлень і відмовою в обслуговуванні. Diameter - це протокол сімейства AAA. Одна з його функцій, наприклад, забезпечення роумінгу серед абонентів. Для перехоплення sms зловмисник зображує звичайну схему роботи операторів при переміщенні абонента в роумінгу. Він направляє домашній мережі оповіщення про те, що абонент-жертва знаходиться в зоні дії іншої (підробленої) мережі. У відповідь домашня мережа пересилає зловмисникові всі вхідні повідомлення і дзвінки. [13]

Висновок до розділу 2

В даному розділі було виявлено та описано деякі уразливості LTE, включаючи уразливість в системі SS7 та уразливості протоколів, уразливості

пов'язані з аутентифікацією, зміною інформації або взаємодією між стандартами всіх поколінь.

Оцінивши цю ситуацію зрозуміли, що цей стандарт має досить багато недоліків і їх використання задля нелегальних цілей не викликає значних складностей та бюджету.

Також дійшли до висновку, що вибір технології блокчейну для усунення та вирішення проблем є доцільним вибором і в наступному розділі вона буде розглянута.

3 ТЕХНОЛОГІЯ БЛОКЧЕЙНУ

3.1 Що таке блокчейн

Блокчейн в даний час є однією з найбільш обговорюваних і розкручених технологій. Існує не так багато галузей, які не повинні ні хвилюватися, ні турбуватися про його потенціал, так як прецеденти, перевірені концепції і повноцінні підприємства, засновані на технології блокчейна, з'являються все частіше.

Ця технологія може порушити бізнес-моделі в багатьох галузях, включаючи телекомунікації, і може підвищити прозорість і ефективність процесу. Проте, блокчейн-додатки є молодими, і країни, що розвиваються і доповнюють галузеві стандарти, швидше за все, будуть використовувати їх ще через кілька років. Проте, щоб уникнути руйнівних сюрпризів або втрачених можливостей, стратегам, фахівцям з планування та особам, які приймають рішення в телекомунікаційній екосистемі, необхідно приділити час для вивчення застосувань цієї технології як в основних, так і в суміжних операціях і бізнес-функціях. Раннє знайомство з відповідними можливостями та проблемами дозволить їм краще отримувати переваги в плані зростання доходів і скорочення витрат, коли технологія стане зрілою і готова до більш широкого впровадження.[14]

Сам же блокчейн - це тип розподіленого реєстру, захищеного від несанкціонованого розкриття, який зберігає інформацію про транзакції в приватній або публічній мережі у вигляді ланцюжка взаємопов'язаних блоків. Говорячи простою мовою, це система зберігання записів, доступ до якої є у будь-якого користувача мережі. Записи, потрапляючи в систему, формують так звані блоки, які, в свою чергу, зв'язуються в єдиний ланцюжок. Звідси пішла і назва blockchain - ланцюжок блоків. Блокчейн передбачає зв'язність, а значить, незмінність інформації. [15]

Дозволяючи цифровій інформації поширюватися, але не копіюватися, технологія блокчейн створила основу нового типу інтернету. Спочатку розроблена для цифрової валюти біткойнов (Buy Bitcoin), технологічне співтовариство знайшло інші потенційні можливості використання цієї технології.

У простому розумінні, блокчейн являє собою серію незмінних записів даних з мітками часу, якими управляє кластер комп'ютерів, які не належать до будь-якої однієї сутності. Кожен з цих блоків даних (тобто блок) захищений і пов'язаний один з одним з використанням криптографічних принципів (тобто ланцюжка).

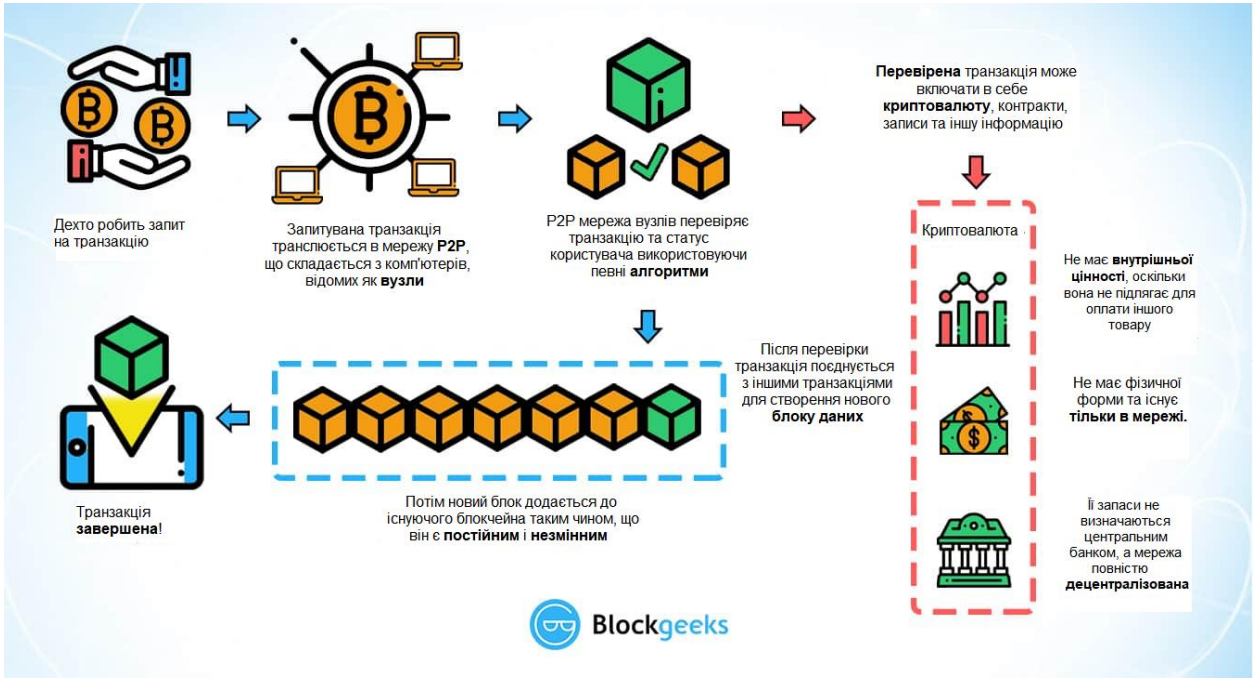


Рисунок 3.1 Короткий принцип роботи блокчейну

Отже, що ж такого особливого в цьому і чому ми говоримо, що у нього є руйнівні для промисловості можливості?

Мережа блокчейнів не має центральної влади - це саме визначення демократизованої системи. Оскільки це загальний і незмінний регістр, інформація в ньому відкрита для всіх і кожного. Отже, все, що побудовано на

блокчейні, за самою своєю природою прозоро, і всі учасники несуть відповідальність за свої дії.

3.1.1 Переваги блокчейну

Блокчейн не несе транзакційних витрат. (Вартість інфраструктури - так, але немає витрат на транзакції.) Блокчейн - це простий, але оригінальний спосіб передачі інформації від A до B повністю автоматизованим і безпечним способом. Одна сторона транзакції ініціює процес, створюючи блок. Цей блок перевірений тисячами, можливо, мільйонами комп'ютерів, розподілених по мережі. Перевірений блок додається в ланцюжок, який зберігається в мережі, створюючи не просто унікальний запис, а унікальний запис з унікальною історією. Фальсифікація запису означатиме фальсифікацію всього ланцюжка в мільйонах записах. Це практично неможливо. Біткойн використовує цю модель для грошових транзакцій, але її можна використовувати багатьма іншими способами.

Подумайте про залізничні компанії. Ми купуємо квитки в додатку або в Інтернеті. Компанія кредитної картки бере комісію для обробки транзакції. За допомогою блокчейна оператор залізниці не тільки може заощадити на оплаті обробки кредитних карт, але і може перемістити весь процес продажу квитків в блокчейн. Сторони угоди - залізнична компанія і пасажир. Квиток є блоком, який буде додано до блокчейн тікета. Так само, як грошова транзакція в блокчейні - це унікальний, піддається незалежній перевірці і не підлягає зміні запис (наприклад, біткойнів), таким може бути і ваш квиток. До речі, остаточний блокчейн квитка - це також запис всіх транзакцій, скажімо, для певного маршруту поїзда або навіть для всієї мережі поїздів, що включає кожен проданий квиток, кожну поїздку.

Але ключ тут полягає в наступному: це безкоштовно. Блокчейн може не тільки передавати і зберігати гроші, але також може замінити всі процеси і

бізнес-моделі, які покладаються на невелику комісію за транзакцію. Або будь-яка інша угода між двома сторонами.

Ось ще один приклад. Концентратор Gig Fivver стягує 0,5 долара за 5 транзакцій між приватними особами, які купують і продають послуги. З використанням технології блокчейн транзакція безкоштовна. Ergo, Fivver перестане існувати. Те ж саме будуть робити аукціонні будинки і будь-які інші господарюючі суб'єкти за принципом маркет-мейкера.

Навіть новачкам, таким як Uber і Airbnb, загрожують технології блокчейна. Все, що вам потрібно зробити, це зашифрувати транзакційну інформацію для поїздки на автомобілі або ночівлі, і знову у вас є абсолютно безпечний спосіб, який порушує бізнес-модель компаній, які тільки почали кидати виклик традиційній економіці. Ми не просто відмовляємося від посередників, які займаються збором платежів, ми також усуваємо необхідність в платформі для підбору гравців.

Оскільки операції з блокчейнами безкоштовні, ви можете стягувати незначні суми, скажімо 1/100 відсотка за перегляд відео або читання статті. Чому я повинен платити The Economist або National Geographic щорічну абонентську плату, якщо я можу платити за статтю в Facebook або в моєму улюбленому додатку чату? Знову ж таки, пам'ятайте, що транзакції блокчейна не несуть вартості транзакції. Ви можете стягувати плату за що завгодно в будь-якій сумі, не турбуючись про те, що треті сторони можуть скоротити вашу прибуток

Блокчейн може зробити продаж записаної музики знову вигідним для артистів, виключивши музичні компанії і таких дистриб'юторів, як Apple або Spotify. Музика, яку ви купуєте, може навіть бути закодована в самому блокчейні, що робить її хмарним архівом для будь-якої купленої пісні. Оскільки суми, що стягуються можуть бути такими маленькими, послуги підписки і потокової передачі стануть неактуальними.

Електронні книги можуть бути оснащені кодом блокчейна. Замість того, щоб Amazon заробляла гроші на продажу, а компанія, що випускає кредитні карти, заробила гроші на комісіях, книги будуть поширюватися в зашифрованому вигляді, а успішна транзакція блокчейна буде переводити гроші автору і відкривати книгу. Переведіть ВСІ гроші автору, а не тільки мізерні гонорари. Ви можете зробити це на веб-сайті рецензування книг, такому як Goodreads, або на своєму власному веб-сайті. Торговий майданчик Amazon тоді не потрібен. Успішні ітерації можуть навіть включати огляди та іншу сторонню інформацію про книгу.

У фінансовому світі додатки більш очевидні, а революційні зміни більш неминучі. Блокчейн змінить спосіб роботи фондових бірж, позики будуть об'єднані, а страхування буде укладено. Вони ліквідують банківські рахунки і практично всі послуги, пропоновані банками. Майже всі фінансові установи збанкрутують або будуть змушені кардинально змінитися, як тільки переваги використання блокчейну без комісійних за транзакції будуть широко зрозумілі і реалізовані. Зрештою, фінансова система побудована на тому, щоб брати невелику частину ваших грошей за привілегії та полегшення транзакції. Біржові маклери більше не зможуть заробляти комісійні, а спред покупки / продажу зникне.

3.2 Як працює блокчейн

Уявіть собі електронну таблицю, яка дублюється тисячі разів в мережі комп'ютерів. Потім уявіть, що ця мережа призначена для регулярного оновлення цієї електронної таблиці, і у вас є загальне уявлення про ланцюжок блоків.

Інформація, що зберігається в блокчейні, існує у вигляді загальної і постійно звіряє бази даних. Це спосіб використання мережі, який має очевидні переваги. База даних блокчейну не зберігається ні в одному місці, а це означає, що записи, які в ній зберігаються дійсно є загальнодоступними і

легко перевірятися. Ніякої централізованої версії цієї інформації для хакера не існує. Хостинг на мільйонах комп'ютерів одночасно, його дані доступні всім в Інтернеті.

Щоб заглибитися в аналогію з таблицями Google, я б хотів, щоб ви прочитали цю статтю від фахівця з блокчейну.

«Традиційний спосіб обміну документами за допомогою спільної роботи - це відправити документ Microsoft Word іншому одержувачу і попросити його внести зміни в нього. Проблема цього сценарію полягає в тому, що вам потрібно почекати, поки не буде отримана зворотна копія, перш ніж ви зможете побачити або внести інші зміни, тому що вам заборонено редагувати її, поки інша людина не закінчить з нею. Так працюють бази даних сьогодні. Два власника не можуть одночасно зв'язуватися з одним і тим же записом. Ось як банки підтримують грошові залишки і переклади; вони ненадовго блокують доступ (або зменшують баланс) під час передачі, потім оновлюють іншу сторону, потім знову відкривають доступ (або оновлюють знову). У Google Docs (або Google Sheets) обидві сторони мають доступ до одного і того ж документу в один і той же час, і одна версія цього документа завжди видно їм обом. Це як загальна книга, але це загальний документ. Розподілена частина вступає в гру, коли в обміні беруть участь кілька людей.

Уявіть кількість юридичних документів, які повинні використовуватися таким чином. Замість того, щоб передавати їх один одному, втрачати версії і не синхронізуватися з іншою версією, чому всі ділові документи не можуть бути передані в загальний доступ замість передачі туди і назад? Так багато типів юридичних контрактів були б ідеальними для такого типу робочого процесу. Вам не потрібен блокчейн для обміну документами, але аналогія з загальними документами є потужною». - Вільям Мугаяр, венчурний консультант, підприємець, маркетолог, стратег і фахівець з блокчейну.

Причина, по якій блокчейн придбав стільки захоплення, полягає в тому, що:

- Він не належить одній особі, отже, він децентралізований;
- Дані криптографічно зберігаються всередині;
- Блокчейн є незмінним, тому ніхто не може втручатися в дані, які знаходяться всередині блокчейна;
- Блокчейн прозорий, тому можна відстежувати дані.

3.3 Три опори для технології blockchain

Три основні властивості технології Blockchain, які допомогли їй отримати широке визнання, такі:

- Децентралізація;
- Прозорість;
- Незмінюваність.

3.3.1 Властивість №1 Децентралізація

До появи Bitcoin і BitTorrent ми більше звикли до централізованих сервісів. Ідея дуже проста. У вас є централізована сутність, в якій зберігаються всі дані, і вам доведеться взаємодіяти виключно з цією сутністю, щоб отримати будь-яку необхідну вам інформацію.

Інший приклад централізованої системи - банки. Вони зберігають всі ваші гроші, і єдиний спосіб, яким ви можете заплатити комусь, - це пройти через банк..

Традиційна модель клієнт-сервер є прекрасним прикладом цього:

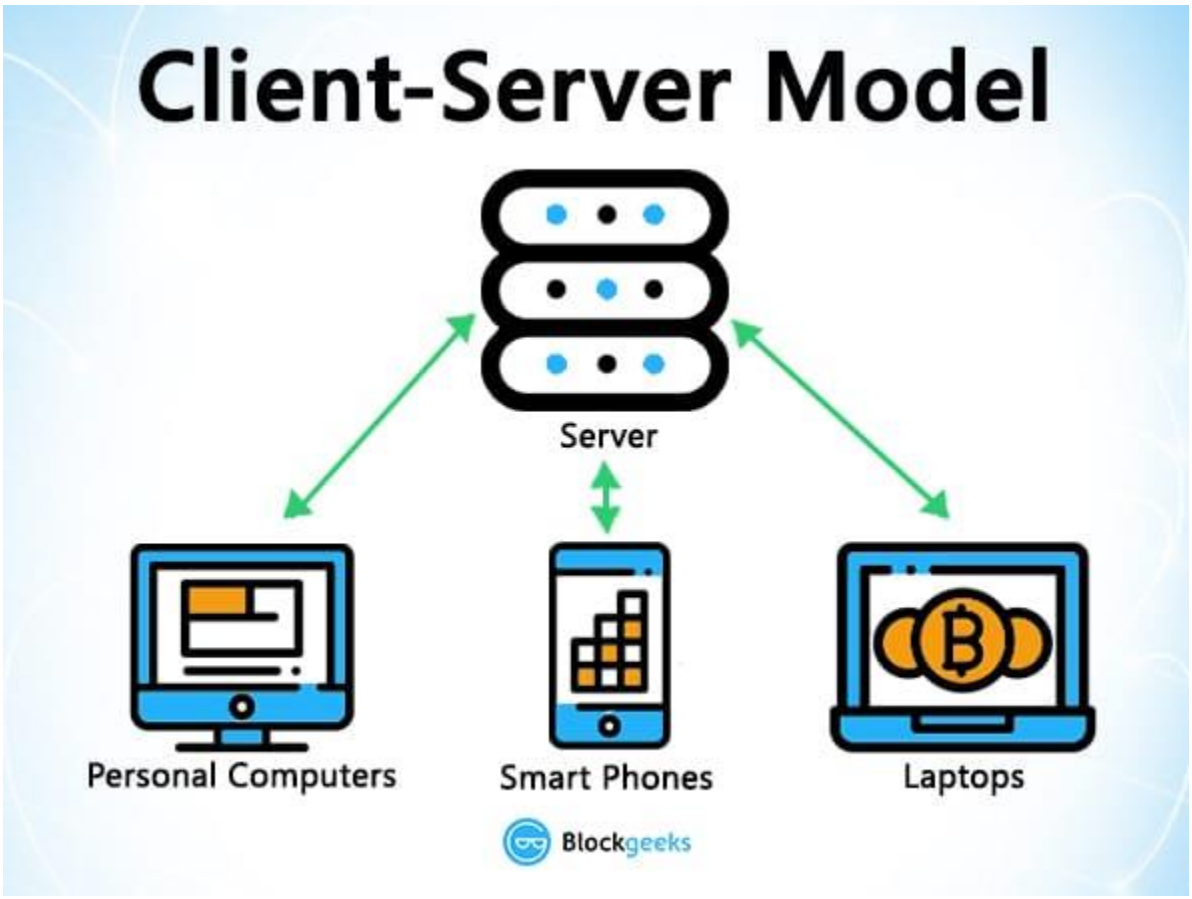


Рисунок 3.2 Традиційна модель клієнт-сервер

Коли ви щось шукаєте в Google, ви відправляєте запит на сервер, який потім повертає вам відповідну інформацію. Це простий клієнт-сервер.

Тепер централізовані системи вже багато років добре з нами поводяться, однак у них є декілька вразливостей.

По-перше, оскільки вони централізовані, всі дані зберігаються в одному місці. Це робить їх легкою ціллю для потенційних хакерів.

Якби централізована система пройшла оновлення програмного забезпечення, вона зупинила б всю систему.

Що якщо централізований об'єкт з яких-небудь причин відключиться? Таким чином, ніхто не зможе отримати доступ до інформації, якою він володіє.

У гіршому випадку, що, якщо цей об'єкт буде пошкоджений? Якщо це станеться, тоді всі дані, які знаходяться всередині блокчейна, будуть скомпрометовані.

Отже, що станеться, якщо ми просто заберемо цю централізовану сутність?

У децентралізованій системі інформація не зберігається одним об'єктом. Фактично, кожен в мережі володіє інформацією.

У децентралізованої мережі, якщо ви хочете взаємодіяти з вашим другом, ви можете зробити це прямо, без участі третьої сторони. Це було головною ідеологією біткойнов. Ви і тільки ви один відповідаєте за свої гроші. Ви можете відправити свої гроші кому завгодно без необхідності проходити через банк.

Рисунок 3.3 Приклад децентралізованої мережі для передачі грошей

Рисунок 3.4 Порівняння централізованої і децентралізованої мереж

3.3.2 Властивість №2 Прозорість

Одна з найцікавіших і неправильно зрозумілих концепцій в технології блокчейну - це «прозорість». Деякі люди кажуть, що блокчейн дає вам конфіденційність, а інші кажуть, що вона прозора. Як ви думаєте, чому це відбувається?

Ну ... особистість людини прихована за допомогою складної криптографії і представлена тільки публічним адресою. Таким чином, якщо ви подивитеся історію транзакцій людини, ви не побачите «Боб відправив 1 BTC», замість цього ви побачите «1MF1bhsFLkBzzz9vpFYEmvwT2TbyCt7NZJ відправлено 1 BTC».

Наступний знімок транзакцій Ethereum покаже вам, що мається на увазі:

TxHash	Block	Age	From		To	Value	[TxFee]
0x2d055e4585ae2a...	5629306	16 secs ago	0x003e3655090890...		0x2bdc9191de5c1b...	0.004741591554641 Ether	0.000294
0xb4d37c791ff4cde...	5629306	16 secs ago	0x6c3b4faf413e0e4...		0xf14cb3acac7b230...	0.744767225 Ether	0.000294
0x9979410dcb5f4c...	5629306	16 secs ago	0x99bcd75abbac05...		0x2d42ee86390c59...	0.016294 Ether	0.000294
0x189c4d4aae09be...	5629306	16 secs ago	0x175cd602b2a1e7...		0xd39681bb0586fb...	0.01 Ether	0.000294
0xda0e9bbb11fb77...	5629306	16 secs ago	0x73a065367d111c...		0x01995786f14357...	0 Ether	0.00150007
0x6be498fafad9acb...	5629306	16 secs ago	0xa3eb206871124a...		0x8a91cac422e55e...	0.029594 Ether	0.000294

Рисунок 3.5 Приклад транзакцій Ethereum

Таким чином, хоча справжня особистість цієї людини захищена, ви все одно побачите всі транзакції, які були зроблені за їх спільною адресою. Такий рівень прозорості ніколи не існував раніше в фінансовій системі. Він додає той додатковий і такий необхідний рівень підзвітності, який вимагається деяким з цих найбільших установ.

Говорячи чисто з точки зору криптовалюти, якщо ви знаєте публічний адресу однієї з цих великих компаній, ви можете просто вставити його в провідник і переглянути всі транзакції, в яких вони брали участь. Це змушує їх бути чесними, то, з чим їм ніколи не доводилося мати справу раніше.

Однак це не кращий варіант використання. Ми впевнені, що більшість з цих компаній не будуть здійснювати операції з використанням криптовалюти, і навіть якщо вони це зроблять, вони не будуть ВСІ свої транзакції використовувати за допомогою криптовалюти. Однак що, якщо технологія блокчейна була інтегрована ... скажімо, в їх ланцюжок поставок?

3.3.3 Властивіть №3: Незмінюваність

Незмінюваність в контексті блокчейна означає, що, як тільки щось було введено в блокчейн, воно не може бути підроблено.

Ви уявляєте, наскільки це буде цінно для фінансових інститутів?

Уявіть собі, скільки справ про розкрадання може бути припинено в зародку, якщо люди знають, що вони не можуть «працювати з книгами» і возитися з рахунками компанії.

Причиною, через яку блокчейн отримує цю властивість, є криптографічний хеш-функція.

Простіше кажучи, хешування означає взяття вхідного рядка будь-якої довжини і видачу вихідних даних фіксованої довжини. В контексті криптовалют, таких як біткойн, транзакції приймаються в якості вхідних даних і проходять через алгоритм хешування (біткойн використовує SHA-256), який видає фіксовану довжину.

Давайте подивимося, як працює процес хешування. Ми збираємося внести певні символи. Для цієї вправи ми будемо використовувати SHA-256 (алгоритм безпечного хешування 256).

INPUT	HASH
Hi	3639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8
Welcome to blockgeeks. Glad to have you here.	53A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8

Рисунок 3.6 Приклад хешування алгоритмом SHA-256

Як ви можете бачити, в випадку з SHA-256, незалежно від того, наскільки великий або маленький ваш вхід, вихід завжди буде мати фіксовану довжину в 256 біт. Це стає критичним, коли ви маєте справу з величезною кількістю даних і транзакцій. Таким чином, в основному, замість запам'ятовування вхідних даних, які можуть бути величезними, ви можете просто запам'ятати хеш і відстежувати.

Криптографічна хеш-функція - це особливий клас хеш-функцій, що володіють різними властивостями, що робить його ідеальним для криптографії. Є певні властивості, які повинна мати криптографічна хеш-функція, щоб вважатися захищеною.

Є тільки одна особливість, на яку ми хочемо звернути увагу. Це називається «ефект лавини».

Що це означає?

Навіть якщо ви внесете невелика зміна в свій введення, зміни, які будуть відображені в хеше, будуть величезними. Давайте перевіримо це за допомогою SHA-256:

INPUT	HASH
This is a test	C7BE1ED902FB8DD4D48997C6452F5D7E509FBCDBE2808B16BCF4EDCE4C07D14E
this is a test	2E99758548972A8E8822AD47FA1017FF72F06F3FF6A016851F45C398732BC50C

Рисунок 3.7 Приклад хешування алгоритмом SHA-256

Ви це бачите? Навіть якщо ви тільки що змінили регістр першого символу введення, подивіться, наскільки це вплинуло на вихідний хеш. Тепер давайте повернемося до нашого попереднього пункту, коли ми розглядали архітектуру блокчейна. Те, що ми сказали, було:

Блокчейн - це пов'язаний список, який містить дані і хеш-покажчик, який вказує на його попередній блок, і, отже, створює ланцюжок. Що таке

хеш-покажчик? Покажчик хешу схожий на покажчик, але замість того, щоб просто утримувати адресу попереднього блоку, він також містить хеш даних всередині попереднього блоку.

Цей невеликий твік робить блокчейни напрочуд надійними і новаторськими.

Уявіть собі на секунду, що хакер атакує блок 3 і намагається змінити дані. Через властивостей хеш-функцій невелика зміна даних різко змінить хеш. Це означає, що будь-які незначні зміни, зроблені в блоці 3, змінять хеш, який зберігається в блоці 2, тепер це, в свою чергу, змінить дані і хеш блоку 2, що призведе до змін в блоці 1 і т. Д і т . Д., Це повністю змінить ланцюжок, що неможливо. Саме так блокчейни досягають незмінності.

Якщо говорити про підтримку блокчейну, то блокчейн підтримується тимчасовою мережею. Мережа являє собою сукупність вузлів, які пов'язані між собою. Вузли - це окремі комп'ютери, які приймають вхідні дані, виконують на них функцію і видають вихідні дані. Блокчейн використовує особливу мережу, звану «однорангова мережа», яка розподіляє все робоче навантаження між учасниками, які мають однакові привілеї, і називається «рівноправними вузлами». Центрального сервера більше немає, тепер є кілька розподілених і децентралізованих.

3.4 Хто буде використовувати блокчейн?

Як веб-інфраструктури вам не потрібно знати про блокчейн, щоб він був корисний у вашому житті.

В даний час фінанси пропонують найефективніші варіанти використання технології. Міжнародні грошові перекази, наприклад. За оцінками Світового банку, в 2015 році було відправлено понад 430 мільярдів доларів США грошових переказів. І на даний момент існує високий попит на розробників блокчейнов.

Блокчейн потенційно виключає посередників для цих типів транзакцій. Персональні обчислення стали доступні широкому загалу з винаходом графічного інтерфейсу користувача (GUI), який прийняв форму «робочого столу». Точно так же найбільш поширений графічний інтерфейс, розроблений для блокчейна, - це так звані додатки «гаманця», які люди використовують для покупки речей за допомогою біткойнов і зберігання їх разом з іншими криптовалютами.

Транзакції онлайн тісно пов'язані з процесами перевірки особистості. Легко уявити, що додатки гаманця в найближчі роки перетворюються і будуть включати інші типи управління ідентифікацією.

3.5 Що таке блокчейн? І які нові додатки це принесе нам?

Блокчейн дає користувачам Інтернету можливість створювати цінності і аутентифікувати цифрову інформацію. Які нові бізнес-додатки будуть результатом цього?

3.5.1 Розумні контракти

Розподілені книги дозволяють кодувати прості контракти, які будуть виконуватися при дотриманні зазначених умов. Ethereum - це блокчейн-проект з відкритим вихідним кодом, створений спеціально для реалізації цієї можливості. Проте, на ранніх етапах Ethereum має потенціал для використання корисності блокчейнів і по-справжньому змінити світ.

На поточному рівні розвитку технології розумні контракти можуть бути запрограмовані для виконання простих функцій. Наприклад, певна сума може бути виплачена, коли певні умови, що були прописані в контракті виконались, з використанням технології блокчейна і біткойнов, що дозволяють автоматизувати виплату.

3.5.2 Економіка спільного споживання

Завдяки процвітанню таких компаній, як Uber і Airbnb, економіка спільного споживання вже довела свою успішність. В даний час, однак, користувачі, які хочуть використати сервіс спільного користування поїздкою, повинні покладатися на посередника, такого як Uber. Включаючи однорангові платежі, блокчейн відкриває двері для прямої взаємодії між сторонами - це призводить до дійсно децентралізованої економіки спільного використання.

У ранньому прикладі OpenBazaar використовує блокчейн для створення однорангового eBay. Завантажте програму на свій обчислювальний пристрій, і ви зможете здійснювати операції з постачальниками OpenBazzar без оплати транзакцій. Принцип «без правил» протоколу означає, що особиста репутація буде мати ще більше значення для ділової взаємодії, ніж в даний час на eBay.

3.5.3 Краудфандінг

Ініціативи по краудфандінгу, такі як Kickstarter і Gofundme, роблять передову роботу для розвитку тимчасової економіки. Популярність цих сайтів говорить про те, що люди хочуть безпосередньо впливати на розробку продукту. Блокчейни переносять цей інтерес на новий рівень, потенційно створюючи краудсорсінгові фонди венчурного капіталу.

У 2016 році один такий експеримент, який базується на Ethereum DAO (Децентралізована автономна організація), зібрав дивовижні 200 мільйонів доларів США всього за два місяці. Учасники придбали «токени DAO», що дозволило їм проголосувати за інтелектуальні контрактні венчурні інвестиції (право голосу було пропорційно кількості належних їм DAO). Подальший злом фондів проекту довів, що проект був запущений без належної обачності, з катастрофічними наслідками. Незважаючи на це, експеримент DAO

передбачає, що блокчейн може відкрити «нову парадигму економічного співробітництва».

3.2.4 Управління

Роблячи результати повністю прозорими і загальнодоступними, технологія розподілених баз даних може забезпечити повну прозорість виборів або будь-якого іншого виду голосування. Розумні контракти на основі Ethereum допомагають автоматизувати процес.

Додаток Boardroom дозволяє приймати організаційні рішення на блокчейні. На практиці це означає, що управління компанією стає повністю прозорим і піддається перевірці при управлінні цифровими активами, акціями або інформацією.

3.2.5 Аудит ланцюжка поставок

Споживачі все частіше хочуть знати, що етичні претензії компаній до їх продуктів реальні. Розподілені бухгалтерські книги надають простий спосіб підтвердити, що передісторія покупки нами речей є справжньою. Прозорість забезпечується за допомогою позначки часу на основі блокчейна дати і місця розташування - наприклад, на діамантах - що відповідає номеру продукту.

Британська компанія Provenance пропонує аудит ланцюжка поставок для ряду споживчих товарів. Пілотний проект Provenance, який використовує блокчейн Ethereum, забезпечує стабільний видобуток риби, що продається в суші-ресторанах в Японії, її постачальниками в Індонезії.

3.2.6 Файлове сховище

Децентралізація зберігання файлів в Інтернеті приносить явні переваги. Поширення даних по мережі захищає файли від злому або втрати.

Міжпланетна файлова система (IPFS) дозволяє легко зрозуміти, як може працювати розподілена мережа. Подібно до того, як BitTorrent переміщує дані по Інтернету, IPFS позбавляє від необхідності централізованих відносин клієнт-сервер (які є в даний час в Інтернеті). Інтернет, що складається з повністю децентралізованих веб-сайтів, може прискорити передачу файлів і час потокової передачі. Таке поліпшення не тільки зручно. Це необхідне оновлення для перевантажених в даний час систем доставки контенту в Інтернеті.

3.2.7 Прогнозні ринки

Краудсорсінг прогнозів по ймовірності події, як виявилося, має високу ступінь точності. Усереднення думок зводить нанівець недосліджені упередження, що спотворюють судження. Прогнозні ринки, які виплачуються відповідно до результатів подій, вже активні. Блокчейн - це технологія «мудрості натовпу», яка, без сумніву, знайде інші застосування в найближчі роки.

Додаток для прогнозування на ринку Augur робить пропозиції за результатами реальних подій. Учасники можуть заробляти гроші, купуючи в напрямку правильного прогнозу. Чим більше акцій куплено з правильним результатом, тим вище буде виплата. При невеликому виділення коштів (менше одного долара) кожен може поставити запитання, створити ринок на основі прогнозованого результату і отримати половину всіх комісійних зборів, які генерує ринок.

3.2.8 Захист інтелектуальної власності

Як відомо, цифрова інформація може нескінченно відтворюватися і широко розповсюджуватися завдяки Інтернету. Це дало веб-користувачам в усьому світі золоту жилу безкоштовного контенту. Проте, правовласникам не

так пощастило, вони втратили контроль над своєю інтелектуальною власністю і, як наслідок, постраждали в фінансовому відношенні. Інтелектуальні контракти можуть захищати авторські права і автоматизувати продаж творчих робіт в Інтернеті, усуваючи ризик копіювання та розповсюдження файлів.

Mycelia використовує блокчейн щоб створити тимчасову системи поширення музики. Компанія Mycelia, заснована британською співачкою і автором пісень Імоджен Хіп, дозволяє музикантам продавати пісні безпосередньо аудиторії, а також зразки ліцензій для продюсерів і розподіляти авторські відрахування авторам пісень і музикантам - всі ці функції автоматизуються за допомогою розумних контрактів. Здатність блокчейнов випускати платежі у вигляді дрібних сум криптовалюта (мікроплатежів) передбачає, що цей варіант використання для блокчейна має великі шанси на успіх.

3.2.9 Інтернет речей (IoT)

Що таке IoT? Кероване мережею управління певними типами електронних пристроїв, наприклад, моніторинг температури повітря в будинку. Розумні контракти уможливлюють автоматизацію віддаленого управління системами. Комбінація програмного забезпечення, датчиків і мережі полегшує обмін даними між об'єктами і механізмами. Результат підвищує ефективність системи і покращує моніторинг витрат.

Найбільші гравці в сфері виробництва, технологій і телекомунікацій борються за домінування в сфері Інтернету речей. Подумайте, Samsung, IBM і AT & T. Додатки IoT, природне розширення існуючої інфраструктури, контрольованої діючими операторами, забезпечать широкий спектр можливостей: від профілактичного обслуговування механічних частин до аналізу даних і масштабного управління автоматизованими системами.

3.2.10 Сусідні мікромережі

Технологія Blockchain дозволяє купувати і продавати поновлювану енергію, що генерується мікромережами по сусідству. Коли сонячні панелі виробляють надлишкову енергію, інтелектуальні контракти на основі Ethereum автоматично перерозподіляють її. Подібні типи автоматизації інтелектуальних контрактів матимуть багато інших додатків, оскільки IoT стає реальністю.

Consensys - одна з провідних світових компаній, розташована в Брукліні, яка розробляє ряд додатків для Ethereum. Одним з проектів, над яким вони співпрацюють, є Transactive Grid, що працює з розподіленою енергетичною компанією LO3. Прототип проекту, який в даний час запущений і працює, використовує розумні контракти Ethereum для автоматизації моніторингу та перерозподілу енергії мікросетей. Ця так звана «інтелектуальна мережа» є раннім прикладом функціональності IoT.

3.2.11 Управління ідентифікацією

Існує певна потреба в кращому управлінні ідентифікацією в мережі. Можливість підтвердити вашу особистість є стрижнем фінансових транзакцій, які відбуваються в Інтернеті. Проте, засоби захисту від ризиків безпеки, які пов'язані з веб-комерцією, в кращому випадку недосконалі. Розподілені книги пропонують розширені методи для підтвердження того, хто ви є, а також можливість оцифровки особистих документів. Наявність захищеної особистості також буде важливо для онлайн-взаємодії, наприклад, в економіці спільного використання. Зрештою, хороша репутація є найбільш важливою умовою для проведення транзакцій в Інтернеті.

Розробка стандартів цифрової ідентифікації виявляється дуже складним процесом. Крім технічних проблем, універсальне онлайн-рішення для ідентифікації вимагає співпраці між приватними особами і урядом.

Додайте до цього необхідність орієнтуватися в правових системах в різних країнах, і проблема стає експоненціально складною. Електронна комерція в Інтернеті в даний час використовує SSL-сертифікат (маленький зелений замок) для безпечних транзакцій в Інтернеті. Netki - це стартап, який прагне створити стандарт SSL для ланцюжка блоків. Нещодавно оголосивши стартовий раунд в 3,5 мільйона доларів, Netki очікує виходу продукту в найближчий час.

3.2.12 AML і KYC

Протидія відмиванню грошей (AML) і практика «Знай свого клієнта» (KYC) мають великий потенціал для адаптації до блокчейну. В даний час фінансові установи повинні виконувати трудомісткий багатоступінчастий процес для кожного нового клієнта. Витрати KYC можуть бути знижені за рахунок перевірки клієнтів між установами і в той же час підвищити ефективність моніторингу та аналізу.

Startup Polycoin пропонує рішення AML / KYC, яке включає аналіз транзакцій. Ті транзакції, які були визначені як підозрілі, передаються співробітникам по дотриманню. Ще один стартап, Tradle, розробляє додаток під назвою Trust in Motion (TiM). Програма TiM, яку називають «Instagram для KYC», дозволяє клієнтам робити знімки основних документів (паспорт, рахунок за комунальні послуги і т. Д). Після перевірки банком ці дані криптографічно зберігаються в блокчейні.

3.2.13 Управління даними

Сьогодні в обмін на свої особисті дані люди можуть безкоштовно користуватися соціальними мережами, такими як Facebook. У майбутньому користувачі матимуть можливість управляти і продавати дані, які генерує їх діяльність в Інтернеті. Оскільки він може бути легко розподілений

невеликими дробовими сумами, біткойнов - або щось в цьому роді - швидше за все буде тією валютою, яка використовується для транзакцій такого типу.

Проект MIT Enigma розуміє, що конфіденційність користувачів є ключовою умовою для створення ринку персональних даних. Enigma використовує криптографічні методи, що дозволяють розділяти окремі набори даних між вузлами і в той же час виконувати масові обчислення для всієї групи даних в цілому. Фрагментація даних також робить Enigma масштабованою (на відміну від тих рішень блокчейну, де дані реплікуються на кожному вузлі). Запуск бета-версії обіцяно протягом наступних шести місяців.

3.2.14 Реєстрація прав власності на землю

Як загальнодоступні книги, блокчейни можуть зробити всі види ведення записів більш ефективними. Назви власності є показовим прикладом. Вони, як правило, схильні до шахрайства, а також дороги і трудомісткі в управлінні.

Ряд країн здійснюють проекти з реєстрації землі на основі блокчейна. Гондурас був першим урядом, який оголосив про таку ініціативу в 2015 році, хоча нинішній статус цього проекту неясний. Також Республіка Грузія уклала угоду з групою Bitfury про розробку системи блокчейнов для прав власності. Як повідомляється, Ернандо де Сото, відомий економіст і захисник прав власності, буде консультувати проект. Зовсім недавно Швеція оголосила, що експериментує з блокчейн-заявкою на право власності.

3.2.15 Торгівля акціями

Потенціал для підвищення ефективності розрахунків по акціях дає вагомі підстави використовувати блокчейни в торгівлі акціями. При виконанні тимчасового зв'язку торговельні підтвердження стають практично

миттєвими (на відміну від трьох днів на оформлення). Потенційно це означає, що посередники - такі як розрахункова палата, аудитори та зберігачі - виключаються з процесу.

Численні фондові і товарні біржі створюють прототипи блокових додатків для пропонованих ними послуг, включаючи ASX (Австралійська фондова біржа), Deutsche Börse (Франкфуртська фондова біржа) і JPX (Японська біржова група). Найбільш помітним, тому що визнаним першопрохідником в цій області є Linq від Nasdaq, платформа для торгівлі на приватному ринку (зазвичай між стартапами до IPO і інвесторами). Партнерство з технологічною компанією Blockchain Chain, Linq, оголосило про завершення першої угоди з акціями в 2015 році. Зовсім недавно Nasdaq оголосив про розробку пробного проекту блокчейна для голосування за дорученням на естонській фондовій біржі[16].

Висновок до розділу 3

Блокчейн в даний час є однією з найбільш обговорюваних і розкручених технологій.

В даному розділі була розглянута технологія блокчейн. Було дане її визначення, а саме - блокчейн простими словами - це ланцюжок блоків, кожен з яких володіє міткою часу, посиланням на попередній блок і зберігається на різних комп'ютерах. Дізналися, що високий рівень безпеки є основою технології.

Основними властивостями технології є: децентралізація, прозорість та незмінюваність. Виявлено, що блокчейн може замінити традиційну схему клієнт-серверної передачі даних.

В кінці особливу увагу приділили особливостям та варіантами застосування технології в різних сферах людської діяльності, показані переваги технології.

4 ВИКОРИСТАННЯ БЛОКЧЕЙНУ В ТЕЛЕКОМУНІКАЦІЯХ

Як було сказано в розділі 1, сучасні способи надання телекомунікаційних послуг та мобільного зв’язку абонентам не є повністю захищеними від потенційних загроз та мають багато недоліків. Тому доцільно в даному розділі підвести результати нашої роботи та описати способи використання технології блокчейну в телекомунікаціяї задля зменшення чи повністю уникнення недоліків в сфері телекомунікацій.

4.1 Блокчейн в управлінні роумінгом

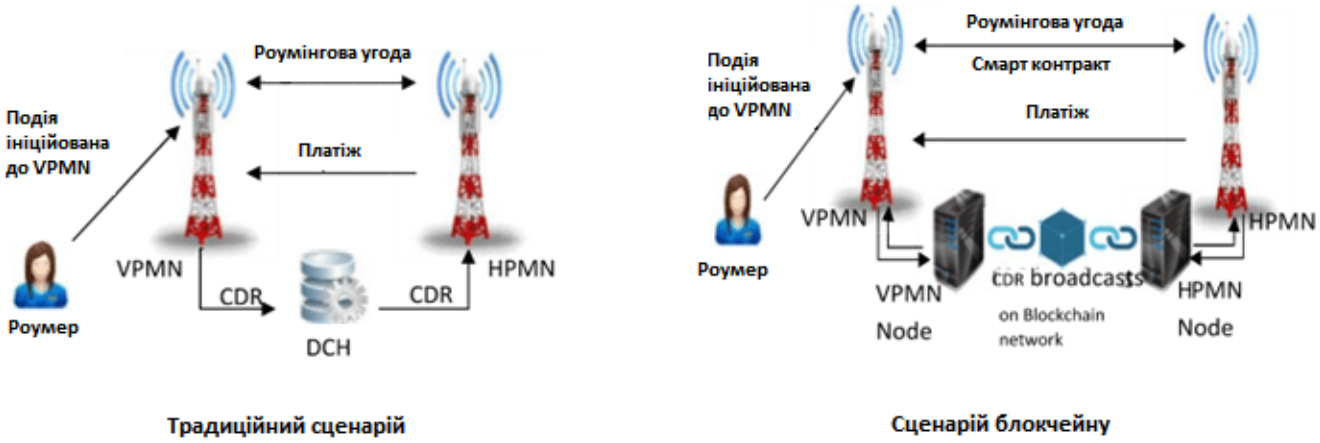


Рисунок 4.1 Порівняння сценаріїв отримання послуг роумінгу в традиційній мережі та з використанням блокчейну

Ці телекомунікаційні послуги надаються їх мережею віддалено, залишаючись далеко від домашньої мережі, шляхом вилучення їх через іншого постачальника послуг (VPMN). Оператори мобільного зв'язку несуть непрямі збитки від шахрайства через постійно зростаючі числа випадків телефонного шахрайства, пов'язаного з використанням технічних засобів для здійснення несанкціонованих дзвінків на платні номери (IRSF). Найчастіше телекомунікаційні компанії передають на аутсорсинг передачу файлів C / EDR і перетворюють їх в білінговий трафік відповідно до індивідуальної підписки третьої сторони, яка називається DCH (Data Clearing House).

Дозволений блокчейн може замінити традиційні способи відправки C / EDR. Усі постачальники послуг зв'язку (CSP), з якими укладено угоду про роумінг, можуть транслювати C / EDR в дозволеній мережі ланцюжка блоків.

Природа блокчейна дозволяє тільки авторизований доступ до мережі, тому ймовірність проникнення даних відсутня. Блокчейн Hyperledger обмежує передачу небажаних блоків блокчейна призначеними вузлами VPMN, а HPMN діють як Майнер для перевірки достовірності даних, що транслюються в мережі блокчейнів. Всякий раз, коли запит на запуск події ініціюється роумером, транзакція, що має всі подробиці про дані C / EDR, транслюється в мережі. Оскільки передача зв'язку відбувається під час виконання, HPMN може розрахувати суму рахунку для кожного абонента, а також оплату VPMN за саму середу виконання (в традиційній системі тривалий час, необхідний для HPMN, не дозволяє виявляти шахрайські дії в роумінгу до це відбувається, є більше технічних труднощів для запобігання, виявлення і автоматичного реагування на ініціювання дій проти шахрайства).

Блокчейн може вирішити давню проблему інтеграції дорогих систем традиційних операторів, і він забезпечує настройки доступу / аутентифікації для забезпечення дзвінків в роумінгу між мережами і операторами. Це допомагає без побоювань домогтися сертифікованого і плавного переходу між HPMN і VPMN. шахрайства.

Більш того, в сценарії з блокчейном, оскільки C / EDR передаються через мережу блокчейна за допомогою широкомовної передачі, це робить роль DCH неактуальною. Це допомагає телекомунікаційним компаніям заощадити ще більше коштів, оскільки для цього процесу не потрібно посередник.

Дозволений блокчейн може бути реалізований між кожною парою операторів, що мають угоду про роумінг. Призначені вузли від обох операторів діють як Майнер для перевірки недоторканності кожної транзакції, яка транслюється в мережі через Romaing Subscriber з домашньої мережі в мережу відвідувача, де угода про роумінг реалізована між

домашньою мережею та мережею відвідувачів в якості смарт-контракту, який ініціюється, коли транзакція, що містить дані CDR транслюються в мережі блокчейна через абонента, наприклад, голосовий виклик або пакет даних. Кожен раз, коли абонент ініціює подію в гостьовій мережі, VPMN передає інформацію CDR як транзакцію в HPMN. Ці дані запускають розумний контракт, і умови угоди виконуються. Таким чином, HPMN може автоматично підраховувати суму виставлення рахунків на основі наданих послуг і відправляти цю інформацію назад в VPMN. Це допомагає миттєво і перевірено авторизуватись, а також спросити виконання розрахунків відповідно до умов смарт-контрактів на основі ланцюжка блоків. CSP також можуть покінчити з DCH, що виступає в якості посередника, що призведе до додаткової економії коштів. Блокчейн дозволить створювати складні набори даних між декількома сторонами в режимі реального часу з високим рівнем довіри та безпеки, зокрема, встановлення особистості передплатника.

4.2 Блокчейн для переказу грошей та мікроплатежів

Рисунок 4.2 Блокчейн для переказу грошових коштів

Крім базових телекомунікаційних послуг, VAS і OTT є двома основними типами послуг, які споживачі отримують, користуючись.

- VAS - це неосновна послуга, що дозволяє підвищити цінність всіх пропозицій та послуг телекомунікаційних компаній. Вони надаються самим оператором або за допомогою третьої сторони.
- послуги OTT знаходяться поза контролем або відповідальністю операторів. Вони просто переносять IP-пакети з джерела в пункт призначення через свою мережу. Користувач може вільно користуватися послугами OTT, тому що кожен може самостійно користуватися Інтернетом так, як він хоче. Телекоми повинні інтегрувати VAS і SDP, щоб надавати такі послуги споживачам.

За зміст VAS або послуги OTT можна стягувати плату, а підписку можна пов'язувати з пропозиціями телекомунікаційних компаній. У всіх цих моделях спільної роботи телекомунікаційні компанії виставляють рахунки споживачам і повертають гроші постачальникам VAS або OTT за запропонований контент після збереження їх частки. IP-пакети послуг VAS або OTT передаються так само, як і базові послуги, пропоновані в мережі операторів.

Deep Packet Inspection (DPI) - це технологія, яка використовується телекомунікаційними компаніями для поділу цих пакетів. DPI дозволяє телекомунікаційним компаніям зчитувати і сканувати корисні дані кожного пакету, на відміну від тільки заголовків в старих методах, під час виконання, тому рішення про те, як класифікувати і контролювати трафік у своїй мережі, приймалося на основі додатків, контенту і передплатників, а також походження та призначення.

З впровадженням технології блокчейна в мережі мікроплатежів не тільки скоротяться витрати на транзакції, а й буде ефективний процес виставлення рахунків і перевірки правильності будь-якої транзакції.

Мікроплатежі можуть мати мережу блокчейнів, в якій використовується новітній масштабований протокол під назвою «Raiden Network». Цей протокол може обробляти більше мільйона передач в секунду, не стикаючись з такими проблемами, як затримка (яка зобов'язує операторів

платити постачальникам перед виставленням рахунків споживачам), втрати пакетів, неможливість ефективної обробки IP-пакетів, проблеми з’єднання, обхід OTT та інші. проблеми уразливості традиційних концепцій, які викликають величезний витік доходів для операторів.

Що стосується грошових переказів, Blockchain забезпечив економічно ефективні міжнародні грошові перекази по всьому світу з мінімальними комісійними за транзакції. Оператори зв'язку можуть стати глобальними провайдерами грошових переказів.

4.3 Блокчейн в біллінгу

Існуючі системи все ще повинні вирішити деякі основні проблеми через технічні обмеження, що виникають в результаті:

- Неправильної інтеграції мережевих елементів: синхронізація між HLR і BSS призводить до витоку доходів ...
- Впровадження нових продуктів: всякий раз, коли телекомунікаційні компанії анонсують новий продукт, система OSS / BSS разом з елементами базової мережі повинна добре інформувати про нові ціни....
- Неповна інформація про використання / споживання: через мінливі тенденцій в технологіях, завантаженості і складності використання даних ....
- Проблеми масштабованості.
- Швидкість обробки: обробка залишку балансу / виставлення рахунків за швидкість мережі / інтернету (4G);
- Уразливість витоку доходів білінгу для клієнтів з післяплатою.

З технологією блокчейна:

- У базовій мережі комутатори і різні регістри можуть бути розміщені в мережі блокчейна. Це допоможе комутаторам в режимі реального часу отримувати всю інформацію про споживачів. Вузол ланцюжка блоків

систем OSS / BSS, що забезпечує ідеальну синхронізацію з комутатором і регістрами.

- Всі вузли будуть працювати в якості Майнера в цій мережі блокчейна, і коли споживач подає будь-який запит щодо замовлення або відмови від будь-якої служби, цей запит буде переданий в мережу блокчейна BSS, і вузли комутаторів і регістрів оновляться відповідно через свої вузли. , Кожне оновлення статусу, пов'язане зі споживачем у будь-який з цих систем, транслюватиметься в мережі блокчейна під час виконання, а інші системи будуть підтримувати повну синхронізацію з цією інформацією під час виконання.
- Для сценаріїв як з передоплатою, так і з післяплатою, вбудована можливість обробки блокчейна під час виконання дозволяє телекомунікаційним компаніям надавати споживачам інформацію про їх статус споживання для будь-якої послуги, на яку вони підписані ... і це в будь-який час і з будь-якого місця ... Уникаючи перерахунків споживачів / обмежень кредитного ліміту, чеків рахунків ... і т. д

Значні поліпшення (в порівнянні з традиційними системами) розглядаються як одна і та ж інформація, яка автоматично оновлюється і синхронізується в BSS і регістрах, що виключає будь-яку можливість уразливості і витоку доходів. Таким чином, якщо BSS скасував підписку споживача на отримання рахунку за одну конкретну послугу, домашній регістр місця розташування також відмовиться від підписки того споживача, щоб скористатися цією конкретної послугою, і навпаки. Те ж саме обробляється для споживчої підписки на послугу. Основна проблема отримання доходу або витоку буде вирішена шляхом впровадження блокчейна, так як тепер споживачі отримують рахунки за кожну послугу, яку вони використовують. Це не тільки підвищує ефективність обслуговування операторів, але і покращує якість обслуговування клієнтів у всьому світі.

Очікується, що сегмент OSS / BSS буде займати найбільший розмір ринку, оскільки блокчейн буде вирішувати проблеми в галузі управління

запасами ресурсів, забезпечення обслуговування, управління мережею, управління продуктами, управління замовленнями, управління доходами і управління клієнтами.

4.4 Блокчейн замінює сім-карту?

SIM-карта, одна з основних моделей мобільних телефонів, застаріла, оскільки рішення Blockchain пропонують значні поліпшення. За допомогою нових концепцій, таких як блокчейн, смартфони завтрашнього дня можуть виглядати знайомими, але їхня технологія стане величезним стрибком вперед, який вже скоро настане.

У той час як інші апаратні засоби зберігання даних, модернізовані до цифрових технологій, так само, як відеоігри, перейшли від картриджів до цифрових завантажень, технологія SIM залишається практично такою ж, як і при створенні. Тепер його домінуюче становище заперечується технологією eSIM, яка вперше була розгорнута Google. За допомогою блокчейна він повинен вийти на більш широкий ринок і домогтися більшого успіху.

Громадянин з підтримкою блокчейну унікально і безпечно ідентифікується в будь-якій точці світу і використовує ідентифікатори для підписки на послуги Telco. Він може вибрати голосовий план з CSP-X, план передачі даних з CSP-Y і потокове відео з CSP-Z і так далі. Повна свобода вибору для вибору пакетів CSP і пропозицій по одному ID eSIM (в порівнянні з громіздким сценарієм з декількома SIM-картами в традиційних системах). І це на будь-який термін (одноразова передоплата, погодинна / щоденна / щомісячна підписка і т.д.). Технологія установки / надання та блокчейна eSig запропонує варіанти (різні послуги, пакети і т. Д.) Від будь-якого / кількох CSP за вибором / розташуванню користувача .... значний потік доходів, який все ще створює істотний прибуток для CSP [17].

Висновок до розділу 4

В останньому розділі були розгянуті способи використання технології блокчейну в розподілених телекомунікаційних мережах: блокчейн в управлінні роумінгом, блокчейн в біллінгу та блокчейн для платежів і переказів. Було доведено, що дана технологія має всі можливості для вирішення поставлених цілей.

ЗАГАЛЬНИЙ ВИСНОВОК

З огляду на важливість телекомунікаційної індустрії, потреба в технологіях розподіленого ланцюжка блоків стає актуальною на сьогоднішній день.

Блокчейн в даний час є лідером в області телекомунікаційних інновацій і змінює соціально-економічний ландшафт цифрових комунікацій у всьому світі. Це задовольняє найбільшу потребу телекомунікаційних компаній зробити свої послуги гнучкими відповідно до нових вимог ринку.

Технологія Blockchain дозволяє вирішити проблему високого тиску з боку телекомунікаційних компаній, щоб скоротити витрати, забезпечити нові потоки доходів, ефективність обслуговування, а також контролювати шахрайські дії, забезпечуючи при цьому чудову якість обслуговування клієнтів. Це усуває традиційну складний і довгий процес взаємопов'язаних операцій, які працюють спільно для надання послуг клієнтам.

Будучи децентралізованої технологією, блокчейн повністю виключає роль дорогої інфраструктури, а також необхідність в центральних органах влади або посередників. Це збільшує швидкість і ефективність цифрового обміну даними між людьми, відділами та забезпечує більш швидку, ефективну та безперебійну передачу інформації.

Блокчейн виглядає корисним для забезпечення взаємодії між внутрішніми, а також зовнішніми системами для телекомунікаційних компаній. Це може пошкодити інфраструктуру, а також дотримання нормативних вимог. Блокчейн може порушити бізнес-моделі за рахунок підвищення прозорості та ефективності телекомунікаційної мережі та її обробки. Децентралізований регістр блокчейна повністю документує кожну транзакцію, яка відбувається в розподіленої або тимчасової мережі, публічної, приватної або гібридної.

Крім того, блокчейн (визнаний довіреною технологією) грає важливу роль в багатьох областях, в яких традиційні системи технічно обмежені,

таких як конвергенція послуг, транзакції в реальному часі, галузева інтеграція, використання можливостей 5G, інтернет речей (IoT), доповненої реальності (AR), віртуальної реальності (VR), міжмашинної взаємодії (M2M), мобільність, безпека і багато інших, де пристрої, підключені до Інтернету, автоматично організовують свої взаємодії

Використання додатків, заснованих на блокчейні, телекомунікаційною галуззю набирає обертів і в кінцевому підсумку стане нормою.

ПЕРЕЛІК ПОСИЛАНЬ

1. Penttinen, J. (2011) *The LTE/SAE Deployment Handbook*, John Wiley & Sons, Ltd, Chichester.

2. Holma, H. and Toskala, A. (2011) *LTE for UMTS: Evolution to LTE-Advanced*, Ch. 10, John Wiley & Sons, Ltd, Chichester.

3. Salo, J., Nur-Alam, M. and Chang, K. (2010) *Practical Introduction to LTE Radio Planning*. Available at: http://www.eceltd.com/lte_rf_wp_02Nov2010.pdf (accessed 12 December, 2011).

4. 3GPP TR 36.814 (March 2010) *Further Advancements for E-UTRA Physical Layer Aspects*, Release 9,annex A.

5. Hata, M. (1980) Empirical formula for propagation loss in land mobile radio services, *IEEE Transactionson Vehicular Technology*, **29**, 317–325.

6. European Cooperation in Science and Technology (1999) *Digital Mobile Radio Towards Future Generation System*, COST 231 final report. Available at: http://www.lx.it.pt/cost231/final_report.htm (accessed 12 December, 2011).

7. Wireless World Initiative New Radio (2008) *WINNER II Channel Models*, WINNER II deliverable D1.1.2, version 1.2. Available at: http://www.ist-winner.org/WINNER2-Deliverables/D1.1.2.zip (accessed 12 December, 2011).

8. 3GPP TS 25.306 (October 2011) *UE Radio Access Capabilities*, Release 10, section 5.

9. 3GPP TS 36.306 (October 2011) *User Equipment (UE) Radio Access Capabilities*, Release 10, section 4.1.

10. 3GPP TS 36.101 (October 2011) *User Equipment (UE) Radio Transmission and Reception*, Release 10, section 5.6A.

11. 3GPP TR 25.912 (April 2011) *Feasibility Study for Evolved Universal Terrestrial Radio Access (UTRA) and Universal Terrestrial Radio Access Network (UTRAN)*, Release 10, section 13.5.

12. Department for Transport, UK (2008) *Road Statistics 2008: Traffic, Speeds and Congestion*. Available at: http://data.gov.uk/dataset/road_statistics_-_traffic_speeds_and_congestion (accessed 12 December, 2011).

13. «Исследование надежности шифрования данных в GSM сетях» [Електронний ресурс] – Режим доступу до ресурсу: https://sibsutis.ru/upload/65f/Ivanova_A_V_-_MG-162.pdf

14. Blockchain@Telco «How blockchain can impact the telecommunications industry and its relevance to the C-Suite» [Електронний ресурс] – Режим доступу до ресурсу: https://www2.deloitte.com/content/dam/Deloitte/za/Documents/technology-media-telecommunications/za_TMT_Blockchain_TelCo.pdf

15. Почему Blockchain является технологией будущего: итоги мастер-класса [Електронний ресурс] – Режим доступу до ресурсу: https://web-academy.com.ua/event/114-proshedshie-iventy/363-master-class-blockchain-itogi

16. What is Blockchain Technology? [Електронний ресурс] – Режим доступу до ресурсу: https://blockgeeks.com/guides/what-is-blockchain-technology/

17. Blockchain technology in the telecom industry: Part 3 [Електронний ресурс] – Режим доступу до ресурсу: https://www.rcrwireless.com/20180912/opinion/readerforum/blockchain-telecom-part3-reader-forum