НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

ФАКУЛЬТЕТ БІОМЕДИЧНОЇ ІНЖЕНЕРІЇ
(повна назва інституту/факультету)

кафедра БІОМЕДИЧНОЇ КІБЕРНЕТИКИ
(повна назва кафедри)

«На правах рукопису»

УДК 004.891.3 + 612.171

«До захисту допущено»
Завідувач кафедри БМК

_____ Євген. НАСТЕНКО
(підпис) (ініціали, ПРІЗВИЩЕ

"___" __*грудня*_____2021р.

Магістерська дисертація

на здобуття ступеня магістра
за освітньо-професійною програмою *«Комп'ютерні технології в біології та медицині»*
зі спеціальності *122 «Комп'ютерні науки»*

на тему: ***Електронна медична карта пацієнта на основі блокчейн технологій***

Виконав (-ла): студент (-ка) **II** курсу, групи _БС-01мп__

ШЕРБЕРГ ОЛЕКСАНДР ВОЛОДИМИРОВИЧ
(прізвище, ім'я, по батькові) (підпис)

Науковий керівник: *доцент каф. біомедичної інженерії (БМІ) доц., к.ф.-м.н., Соломін Андрій В'ячеславович*
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по ініціали) (підпис)

Консультант з розділів магістерської дисертації:

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

Рецензент: *доцент каф. біомедичної інженерії, доцент, к.т.н. Зубчук Віктор Іванович*
(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 – 2021 року

Нормо контролер _____ Галина КОРНІЄНКО

_____

Шерберг, О. В. Електронна медична карта пацієнта на основі блокчейн: магістерська дис. : 122 Комп'ютері науки / Шерберг Олександр Володимирович. – Київ, 2021. – 100 с.

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет біомедичної інженерії

Кафедра біомедичної кібернетики

Рівень вищої освіти – другий (магістерський)

Спеціальність – 122 «Комп'ютерні науки»

Освітньо-професійна програма «Комп'ютерні технології в біології та медицині»

ЗАТВЕРДЖУЮ

Завідувач кафедри БМК

_____ Євген НАСТЕНКО

«_*31*_»__*серпня*___2021 р.

ЗАВДАННЯ
на магістерську дисертацію студенту

ШЕРБЕРГУ ОЛЕКСАНДРУ ВОЛОДИМИРОВИЧУ

(прізвище, ім'я, по батькові)

1. Тема дисертації ***Електронна медична карта пацієнта на основі блокчейн технологій***

науковий керівник дисертації
Соломін Андрій В'ячеславович, к.ф.-м.н., доцент

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «*09*» *листопада* 2021 р. №***3703-с***

2. Термін подання студентом дисертації ***01-04 грудня 2021 року***

3. Об'єкт дослідження: ***алгоритми реконструкції зображень.***

4. Вихідні дані: ***результати дипломної роботи бакалавра; потоки відеоданих ехокардіографії, отриманих за технологією спекл-трекінг; результати колег по цеху з кафедри біомедичної кібернетики.***

5. Перелік завдань, які потрібно розробити: ***1. Проаналізувати існуючі електронні медичні системи 2. Описати існуючі версії блокчейну та консенсусів. 3. Створення веб застосунку електронної медичної карти пацієнта. 4. Впровадити блокчейн у створений веб додаток. 5. Проробити стартап-проект для виведення результатів роботи на ринок. 6. Розробити концептуальні висновки за результатами магістерської дисертації.***

6. Орієнтовний перелік графічного (ілюстративного) матеріалу: ***29 рисунків, 9 таблиць, презентація на 12 слайдів.***

7. Орієнтовний перелік публікацій: ***1 публікація у фаховому виданні.***

8. Консультанти розділів дисертації*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Магістерської дисертації		31.08.2021р	01.12.2021р

9. Дата видачі завдання ***31 серпня 2021 р.***

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Отримання завдання на МД	31 серпня 2021р.	
2	Практика	з 01.09.2021р. по 26.10.2021р.	
3	Вставлення результатів практики в розділи МД	4 листопада 2021р.	
4	Аналіз предметної області	4 листопада 2021р.	
5	Проектування схеми бази даних	5-11 листопада 2021р.	
6	Розробка веб додатку електронної медичної карти пацієнта	12-18 листопада 2021р.	
7	Введення компоненти блокчейн в готовий веб додаток електронної медичної карти пацієнта	19-25 листопада 2021р.	
8	Стартап аналіз проекту магістерської дисертації	26-29 листопада 2021р.	
9	Складання висновків до результатів виконання магістерської дисертації	30 листопада 2021р.	
10	Подання в електронному вигляді МД та анотації до неї на перевірку нормоконтролера та UNICHECK .	1-3 грудня 2021р	
11	Передзахист МД та допуск до захисту дисертації	4-6 грудня 2021р.	
12	Подання МД рецензенту. Отримання рецензії.	7-15 грудня 2021р.	

Студент _____ **Олександр ШЕРБЕРГ**
(підпис) (ім'я, ПРІЗВИЩЕ)

Науковий керівник _____ **Андрій СОЛОМІН**
(підпис) (ім'я, ПРІЗВИЩЕ)

* Якщо визначені консультанти. Консультантом не може бути зазначено наукового керівника магістерської дисертації.

РЕФЕРАТ

Магістерська дисертація за темою «Електронна медична карта пацієнта на основі блокчейн» виконана студентом кафедри біомедичної кібернетики ФБМІ *Шербергом Олександром Володимировичем зі спеціальності 122 «Комп'ютерні науки» за освітньо-професійною програмою «Комп'ютерні технології в біології та медицині» та* складається зі: вступу; 4 розділів («Аналіз предметної області», «Теоретична частина», «Аналітична частина», «Практична частина»), розділу зі стартап проекту, висновків до кожного з цих розділів; загальних висновків; списку використаних джерел, який налічує 21 джерело. Загальний обсяг роботи 96 сторінок

Обсяг роботи: 96 сторінок, 29 ілюстрацій, 21 джерела посилань.

Актуальність теми. Актуальність роботи пов'язана з діджиталізацією охорони здоров'я, персоніфікацією медичної інформації, надійністю її зберігання на протязі десятків років, розділенням прав доступу.

Мета дослідження. Проектування системи електронних медичних карток пацієнтів на основі блокчейн технологій та сучасних алгоритмів збереження та захисту інформації.

Об'єкт дослідження. Блокчейн технології та розподілені бази даних.

Предмет дослідження. Впровадження блокчейну до електронної медичної карти пацієнта.

Методи дослідження. Проектування та створення веб додатку медичної карти пацієнта.

Інструменти дослідження. Ruby, Ruby on Rails.

Ключові слова: *блокчейн, діджиталізація, електронні медичні картки, хеш-функція, алгоритм, Ruby*.

Публікації. За результатами виконаної роботи було опубліковано 1 наукову статтю:

Sheberh O.V. *Electronic medical card of patient on the basis of blockchain technologies / Sheberh O.V., Solomin A.V. // Modern engineering and innovative technologies. – Germany, 2021.– Issue №17, Part 3, p. 23-28*

Конференції. Прийнято участь в роботі двох конференцій:

1. ***Sheberh O.V.*** *Blockchain technologies in the digitalization of the health care system / / Sheberh O.V., Solomin A.V. // Technique and technology of the future '2021'. – Karlsruhe, Germany, 2021*

2. *Шерберг О.В. Блокчейн технології в діджиталізації системи охорони здоров'я // Шерберг О.В., Соломін А.В. // IV Міжнародна науково-практична конференція «Інформаційні системи та технології в медицині» (ІСМ–2021) [Текст] : зб. наук. пр. – Харків : Нац. аерокосм. ун-т ім. М. Є. Жуковського «Харків. авіац. ін-т», 2021. – с. 54-55*

Abstract

Master's thesis on "Electronic medical card of a patient based on blockchain" is executed by a student of the Department of Biomedical Cybernetics *Sherberh Oleksander Vladimirovich* in the specialty 122 "Computer Science" in the educational-professional program "Computer Technology in Biology and Medicine" and consists of: introduction ; 4 sections ("Subject area analysis", "Theoretical part", "Analytical part", "Practical part"), sections on the startup project, conclusions to each of these sections; general conclusions; a list of used sources, which includes 21 sources. The total volume of the work is 96 pages

Paper size: 96 pages, 29 illustrations, 21 references.

Key words: blockchain, digitalization, electronic medical cards, hash function, algorithm, Ruby.

Relevance of the topic. The urgency of the work is primarily in the introduction of blockchain technology because this approach allows better control of doctors. Because all changes to patient data will be recorded in the database, listed as changes, or deletion will not be possible.

Objective of the study. Analysis and development of electronic medical records based on blockchain technologies.

Object of study. Blockchain technology and distributed databases.

Subject of study. Introduction of a blockchain to the electronic medical card of patients.

Research methods. Design and creation of a web application for medical records of patients.

Research tools. Ruby, Ruby on Rails.

Publications. According to the results of the work performed, 1 scientific statistic was published:

Sheberh O.V. *Electronic medical card of patient on the basis of blockchain technologies / Sheberh O.V., Solomin A.V. // Modern engineering and innovative technologies. – Germany, 2021.– Issue №17, Part 3, p. 23-28*

Conferences. Two conferences were attended:

1. ***Sheberh O.V.*** *Blockchain technologies in the digitalization of the health care system / / Sheberh O.V., Solomin A.V. // Technique and technology of the future '2021'. – Karlsruhe, Germany, 2021*

2. **Шерберг О.В.** Блокчейн технології в діджиталізації системи охорони здоров'я // Шерберг О.В., Соломін А.В. // IV Міжнародна науково-практична конференція «Інформаційні системи та технології в медицині» (ІСМ–2021) [Текст] : зб. наук. пр. – Харків : Нац. аерокосм. ун-т ім. М. Є. Жуковського «Харків. авіац. ін-т», 2021. – с. 54-55

Зміст

ВСТУП

Цифрові технології поступово охоплюють всі сфери життєдіяльності. У сфері охорони здоров’я актуальною задачею є створення та удосконалення електронної системи медичних карток пацієнтів. Переваги такої системи очевидні, але до неї висуваються досить жорсткі вимоги. Це і надійність, і доступність для профільних лікарів, і захищеність, і збереження персональних даних, тощо. У зв’язку з розвитком технологій блокчєйн з’явилась можливість використати їх переваги і в цій галузі охорони здоров’я, що дозволить задовольнити багато з висунутих вимог.

Блокчєйн дозволяє підвищити довіру та ефективність в обміні практично будь-чим.

Будь-які транзакції можна подати для блокчєйну. Це забезпечить надійність збереження інформації та захистить від можливості її несанкціонованої або випадкової зміни навіть з правами адміністратора. Що-до бази даних, у ній взагалі буде відсутня роль адміністратора, це забезпечує подвійну надійність.

Наразі блокчєйн являє собою потужний інструмент для проведення транзакцій не переймаючись через можливі перехоплення вузлів баз даних хакерами, тому що децентралізована система спроможна повернути усі вузли баз даних у початковий стан, зберігаючи при цьому всю інформацію що була у базі, до її зміни зловмисником.

На даний момент часу одним з найвідоміший блокчєйнів Єфір являє собою криптовалюту. Це одна з найстарших платформ, вона пропонує децентралізований блокчєйн, який можна порівняти з біткоїном. Засновник стверджує що справжня сила полягає у децентралізованості з підтримкою смарт контрактів. Однак у такого підходу є і мінуси, такі як повільне виконання та великі затрати на виконання, порівняно з іншими платформами.

Ще одним прикладом блокчєйну є IBM блокчєйн, це приватна децентралізована мережа, з найбільш успішною клієнтською базою, не

схильною до ризику. У ній найбільші можливості у використанні його для підключення до корпоративної хмари та застарілих технологій легше ніж в інших децентралізованих мережах.

Також існує така платформа Тезос це старіша платформа, яка розробляється з 2014 року, яка підтримує децентралізовані програми, смарт-контракти та нові фінансові інструменти, такі як NFT, які можна розглядати як сучасну варіацію торгових карток, пов'язаних із цифровими активами. Платформа підтримує протокол, що динамічно оновлюється, і модульні програмні клієнти, які дозволяють їй адаптуватися до нових видів використання. Спільнота Тезос швидко оновлює платформу з останніми вдосконаленнями, які покращили продуктивність і збільшили обмеження розміру для смарт-контрактів.

Дана робота являє собою розробку програмного додатку який відображає електронну медичну карту пацієнта реалізованого для роботи з децентралізованими базами даних.

Актуальність роботи пов'язана з діджиталізацією охорони здоров'я, персоніфікацією медичної інформації, надійністю її зберігання на протязі десятків років, розділенням прав доступу.

Першочерговою задачею буде аналіз та проектування схеми бази даних, тобто детальна розробка таблиць та полів що їм належать, а також усі взаємозв'язки між цими таблицями. Якісний аналіз та проектування дозволять уникнути багатьох проблем при розробці самого додатку.

Метою роботи є проектування системи електронних медичних карток пацієнтів на основі блокчейн технологій та сучасних алгоритмів збереження та захисту інформації.

Для досягнення мети були поставлені наступні задачі:

1. Проаналізувати джерела, які стосуються впровадження та роботи з децентралізованими базами даних.

2. Дослідити роботу відомих систем, які працюють на основі блокчейн технологій.

3. Реалізувати програмно схему змодельованої бази даних електронної медичної карти пацієнта.

4. Застосувати розроблену схему бази даних у програмному додатку та розробити інтерфейс взаємодії з цією базою.

5. Реалізувати блокчєйн технологію на розробленому додатку.

Мета і завдання дослідження

Метою роботи є розробка та реалізація веб застосунку електронної медичної карти пацієнта на основі блокчєйн технологій, та реалізація у ньому графічного інтуїтивно зрозумілого інтерфейсу користувача.

Об'єктом дослідження є блокчєйн технології та розподілені бази даних.

Предметом дослідження є впровадження блокчєйну до електронної медичної карти пацієнта.

Методи дослідження. Проектування та створення веб додатку медичної карти пацієнта.

Наукова новизна одержаних результатів

Результатом даної роботи стало перше застосування блокчєйн технологій для електронної медичної карти пацієнта.

Практичне значення одержаних результатів

Розроблений веб застосунок під назвою «MedicalCard» містить в собі блокчєйн, та протестований на тимчасових даних. Основні вузли програми вдало налаштовані і працюють без перебоїв.

Даний веб застосунок можна використовувати для роботи лікарів, замість стандартної медичної карти пацієнта. Це полегшить як роботу лікаря так і допоможе пацієнту швидко переглянути свої дані.

Особистий внесок здобувача

Для виконання поставлених задач здобувачем було проаналізовано поставлену задачу та обрано найліпший метод та технології для її вирішення. Мовою програмування Ruby було створено веб додаток, в якому реалізовано блокчєйн технологія.

За допомогою фреймворку Ruby on rails веб додаток було успішно оформлено та спроектовано здобувачем. Були використані останні версії застосованих бібліотек для полегшення написання веб застосунку.

Для побудови графічного інтерфейсу були використані можливості мови програмування JavaScript та каскадні таблиці стилів. Окрім цього

Апробація результатів дисертації

Sheberh O.V. *Blockchain technologies in the digitalization of the health care system / / Sheberh O.V., Solomin A.V. // Technique and technology of the future '2021'. – Karlsruhe, Germany, 2021*

Шерберг О.В. Блокчейн технології в діджиталізації системи охорони здоров'я // Шерберг О.В., Соломін А.В. // IV Міжнародна науково-практична конференція «Інформаційні системи та технології в медицині» (ІСМ–2021) [Текст] : зб. наук. пр. – Харків : Нац. аерокосм. ун-т ім. М. Є. Жуковського «Харків. авіац. ін-т», 2021. – с. 54-55

Публікації

За результатами досліджень опубліковано 1 наукова праця у науковому фаховому виданні України.

Sheberh O.V. *Electronic medical card of patient on the basis of blockchain technologies / Sheberh O.V., Solomin A.V. // Modern engineering and innovative technologies. – Germany, 2021.– Issue №17, Part 3, p. 23-28*

Структура дисертації

Магістерська дисертація за темою «Електронна медична карта пацієнта на основі блокчєйн» виконана студентом кафедри біомедичної кібернетики *Шербергом Олександром Володимировичем зі спеціальності 122 «Комп'ютерні науки» за освітньо-професійною програмою «Комп'ютерні технології в біології та медицині» та* складається зі: вступу; 4 розділів («Аналіз предметної області», «Теоретична частина», «Аналітична частина», «Практична частина»), розділу зі стартап проекту, висновків до кожного з цих розділів; загальних висновків; списку використаних джерел, який налічує 21 джерело, 29 ілюстрацій. Загальний обсяг роботи 96 сторінок.

РОЗДІЛ 1
АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

Для проведення аналізу предметної області, пов’язаної з блокчєйн технологією та використанням децентралізованих баз даних, було використано 7 джерел.

1.1 Розуміння проблематики

З розвитком цифрових технологій черга дійшла до оцифрування медичних карт пацієнта і перетворення їх з паперових книжок, які можна легко загубити або забути, на онлайн кабінети користувачів, де пацієнт може онлайн подивитись інформацію про свій діагноз.

Але навіть у цифрових технологій є свої недоліки, такі як недостовірність інформації. Це пов’язано з можливістю несанкціонованої зміни записів, у тому числі виправленні раніше поставлених помилкових діагнозів або помилково призначених протоколів лікування.

1.2 Розуміння технології блокчєйн

Технологія блокчєйн, як деякий аналог загальної незмінної бухгалтерської книг, може стати гарантом збереження всієї історії записів.

Блокчєйн — це загальна розподілена система, яка полегшує процес реєстрації транзакцій та відстеження активів у бізнес мережі. Актив може бути матеріальним — будинок, автомобіль, готівка, земля — або нематеріальні, як інтелектуальна власність, наприклад патенти, авторські права або брендинг. Практично будь-що цінне може відстежуються та продаватись або покупатись у мережі блокчєйн, що знижує ризик і скорочує витрати для всіх учасників торгів.

Блокчейн, по суті, є розподіленою базою даних записів або публічної книги всіх транзакцій або цифрових подій, які були виконані та спільні між сторонами-учасниками. Кожна операція в публічній книзі перевіряється консенсусом більшості учасників системи. І після введення інформація ніколи не може бути стерта.

Блокчейн містить певний і підданий перевірці запис кожної окремої транзакції. Найпопулярнішим прикладом використання технології блокчейн є біткоїн, децентралізована цифрова валюта. Сама по собі цифрова валюта біткоїн дуже суперечлива, але базова технологія блокчейн працювала бездоганно і знайшла широкий спектр застосувань як у фінансовому, так і в нефінансовому світі.

Але найголовнішим досягненням була розробка консенсусу. Це програмне забезпечення, яке дозволяє цифровій валюті функціонувати, слід розглядати цей винахід, як паровий двигун або двигун внутрішнього згоряння, який має потенціал змінити світ фінансів і не тільки.

Сучасна цифрова економіка базується на певному авторитеті якому можна довіряти. Усі наші онлайн-транзакції покладаються на те, щоб довіряти комусь, хто скаже нам правду — це може бути постачальник послуг електронної пошти, який повідомляє нам, що наш електронний лист доставлено; це може бути центр сертифікації, який повідомляє нам, що певний цифровий сертифікат заслуговує на довіру; або це може бути соціальна мережа, як-от Facebook, яка повідомляє нам, що нашими повідомленнями про події нашого життя ділиться лише з нашими друзями, або це може бути банк, який повідомляє нам, що наші гроші надійно доставлені нашим дорогим людям у віддаленій країні.

Справа в тому, що ми живемо нестабільно в цифровому світі, покладаючись на третю особу для безпеки та конфіденційності наших цифрових активів. Факт залишається фактом, що ці сторонні джерела можна зламати, маніпулювати або зламати. Ось тут і стає в нагоді технологія блокчейн. Він має потенціал революціонізувати цифровий світ, забезпечуючи

розподілений консенсус, де кожну онлайн-транзакцію, минулу й теперішню, що стосується цифрових активів, можна перевірити в будь-який час у майбутньому. Це робиться без шкоди для конфіденційності цифрових активів і залучених сторін. Розподілений консенсус та анонімність — це дві важливі характеристики технології блокчейн.

Переваги технології блокчейн переважають над регуляторними питаннями та технічними проблемами. Одним з ключових нових випадків використання технології блокчейн є «розумні контракти». Смарт-контракти – це в основному комп'ютерні програми, які можуть автоматично виконувати умови контракту. Коли попередньо налаштована умова смарт-контракту між суб'єктами-учасниками виконується, тоді сторони, які беруть участь у контрактній угоді, можуть автоматично здійснювати платежі відповідно до контракту прозорим способом.

Розумна власність — це ще одна пов'язана концепція, яка стосується контролю власності на майно або актив через блокчейн за допомогою смарт-контрактів. Власність може бути фізичною, як-от автомобіль, будинок, смартфон тощо, або нефізичною, як-от акції компанії. Тут слід зазначити, що навіть біткоїн насправді не є валютою – біткоїн – пов'язаний з контролем власності на гроші.

Технологія блокчейн знайшла застосування в широкому діапазоні сфер — як фінансових, так і нефінансових.

Фінансові установи та банки більше не розглядають технологію блокчейн як загрозу традиційним бізнес-моделям. Найбільші банки світу насправді шукають можливості в цій сфері, проводячи дослідження інноваційних блокчейн-додатків. В недавньому інтерв'ю Рейн Ломус з естонського банку LHV розповів, що вони вважають блокчейн найбільш перевіреним і безпечним для деяких програм, пов'язаних із банківськими та фінансовими послугами.

Можливості нефінансових додатків також нескінченні. Ми можемо передбачити розміщення в блокчейні доказів існування всіх юридичних

документів, медичних карт та платежів лояльності в музичній індустрії, нотаріуса, приватних цінних паперів та шлюбних ліцензій. Зберігаючи відбиток цифрового активу замість того, щоб зберігати сам цифровий актив, можна досягти цілі анонімності або конфіденційності.

Існує багато різних типів блокчейнів.

1. Публічні блокчейн: публічні блокчейн, такі як біткоїн, є великими розподіленими мережами, які запускаються через рідний токен. Вони відкриті, тобто будь-хто може брати участь на будь-якому рівні та мати відкритий вихідний код, який підтримує громада.

2. Блокчейн з обмеженим доступом: такі як Ripple, контрольні ролі, які окремі особи можуть грати в мережі. Вони досить великі й розподілені системи, які використовують рідний маркер. Їх основний код може бути не з відкритим кодом.

3. Приватні блокчейн: приватні блокчейн, як правило, менші і не використовують токен. Їхнє членство суворо контролюється. Ці види блокчейн віддають перевагу консорціумам, які мають довірених членів і торговельну конфіденційну інформацію.

1.3 Необхідність впровадження блокчейну

Протягом історії створювались різні інструменти довіри, такі як карбовані монети, паперові гроші, акредитиви та банківські системи для полегшення обміну та захисту покупців і продавців.

Важливі нововведення, зокрема телефонні лінії, кредитні карткові системи, Інтернет та мобільні технології покращили зручність, швидкість та ефективність транзакцій скорочуючи а іноді й практично усуваючи дистанцію між покупцями і продавцями.

Проте багато ділових операцій залишаються неефективними, дорогими, і вразливими, страждають від таких обмежень:

1. Готівка корисна лише в місцевих транзакціях і у відносно невеликих сумах.

2. Час між транзакцією та розрахунком може тривати довго.

3. Дублювання зусиль і необхідність перевірки третьою стороною та/або наявність посередників додають незручностей.

4. Шахрайство, кібератаки і навіть прості помилки підвищують вартість і складність ведення бізнесу, і всі учасники мережі ризикують, якщо центральна система, наприклад банк, скомпрометований.

5. Половина людей у світі не мають доступу до банківського рахунку і довелося розробити паралельні платіжні системи що дозволяють проводити операції.

Обсяги транзакцій у всьому світі зростають в геометричній прогресії безсумнівно це збільшить складність, вразливість, неефективність і витрати поточних трансакційних систем. Зростання електронної комерції, онлайн-банкінг, покупки в додатку та збільшення мобільності людей у всьому світі сприяло розвитку зростання обсягів транзакцій. І обсяги транзакцій будуть вибухати із розвитком Інтернету речей.

Щоб вирішити ці та інші проблеми, світ потребує платіжні мережі, які є швидкими та забезпечують механізм, який встановлює довіру, не потребує спеціалізованого обладнання, не має повернення платежів або щомісячних платежів, а також надає колективне бухгалтерське рішення для забезпечення прозорості та довіри.

1.4 Перше введення блокчєйну

У 2008 році окрема особа або група, яка пишеться під ім’ям Сатоші Накамото, опублікувала статтю під назвою «Біткоїн: однорангова електронна готівкова система». У цій статті описується однорангова версія електронної готівки, яка дозволить пересилати онлайн-платежі безпосередньо від однієї сторони до іншої, не проходячи через фінансову установу. Біткоїн був першою

реалізацією цієї концепції. Тепер слово «криптовалюти» — це ярлик, який використовується для опису всіх мереж і засобів обміну, які використовують криптографію для захисту транзакцій — на відміну від тих систем, де трансакції здійснюються через централізовану довірену структуру.

Автор першої статті хотів залишитися анонімним, тому Сатоші Накамото ніхто не знає донині. Через кілька місяців була випущена програма з відкритим вихідним кодом, що реалізує новий протокол, яка почалася з блоку Genesis з 50 монет. Будь-хто може встановити цю програму з відкритим кодом і стати частиною однорангової мережі біткойн. Відтоді популярність її зростала.

Одне рішення, яке було розроблено для вирішення складнощів, вразливості, неефективності та витрат поточної системи транзакцій — це біткоїн — цифрова валюта, яка була запущена в 2009 році.

На відміну від традиційних валют, які випускаються центральними банками, біткоїн не має центрального монетарного органу. Це ніхто не контролює. Біткоїни друкуються не так, як долари чи євро; їх добувають люди і все частіше підприємства, запущені комп’ютери у всьому світі, використовуючи програмне забезпечення, яке розв’язує математичні головоломки. Замість того, щоб покладатися на моніторинг центрального монетарного органу, перевіряти та затверджувати операції та керувати грошовою масою, біткоїн підтримується одноранговою комп’ютерною мережею своїх користувачів, подібно до мереж, які лежать в основі.

Біткоїн має ряд переваг перед іншими поточними системами транзакцій, включаючи такі:

1. Економічна ефективність: біткоїн усуває потребу в посередниках.
2. Алгоритмічна ефективність: інформація про транзакції записується один раз і залишається доступною для всіх сторін через розподілену мережу.

3. Надійність та захищеність: Транзакцію не можна змінити, її можна повернути тільки за допомогою іншої транзакції, у цьому випадку обидві операції стають видимими.

Насправді біткоїн побудований на основі блокчейну, який служить спільною книгою біткоїн. Блокчейн краще розглядати як операційну систему, таку як Microsoft Windows або MacOS, і біткоїн як лише одна з багатьох програм, які можна запускати в цій операційній системі.

Блокчейн надає засоби для запису транзакцій — загальна бухгалтерська книга, але ця книга може використовуватися для запису будь-якої транзакції та відстеження руху будь-го активу: матеріального, нематеріального чи цифрового. Наприклад, блокчейн дозволяє проводити розрахунки цінними паперами здійснювати за хвилини, а не за дні. Це також може використовуватися, щоб допомогти компаніям керувати потоком товарів і пов'язаними платежами або дозволити виробникам ділитися журналами оригінального виробництва.

Біткоїн і блокчейн – це не одне й те саме. Блокчейн надає засоби для запису та зберігання біткоїн-транзакцій, але блокчейн має багато застосувань, крім біткоїнів. Біткоїн є лише перший варіант використання блокчейну і перше застосування у фінансових цілях. В наші дні біткоїн має дуже великий курс.

1.5 Принцип роботи блокчейну

Інтернет-комерція пов’язана виключно з фінансовими установами, які виступають довіреною третьою стороною, яка обробляє будь-які електронні транзакції та є посередником. Роль довіреної третьої сторони полягає в тому, щоб перевіряти, захищати та зберігати транзакції.

Певний відсоток шахрайства неминучий в онлайн-транзакціях, і це потребує посередництва у фінансових операціях. Це призводить до високих трансакційних витрат.

Біткойн використовує криптографічне підтвердження замість довіри до третьої сторони для двох сторін, які бажають виконати онлайн-транзакцію через Інтернет. Кожна транзакція захищена цифровим підписом. Кожна транзакція надсилається на «відкритий ключ» одержувача з цифровим підписом за допомогою «приватного ключа» відправника.

Щоб витрачати гроші, власнику криптовалюти необхідно підтвердити право власності на «приватний ключ». Суб'єкт, який отримує цифрову валюту, перевіряє цифровий підпис – таким чином право власності на відповідний «приватний ключ» – у транзакції, використовуючи «відкритий ключ» відправника.

За допомогою традиційних методів запису транзакцій та відстеження активів, учасники мережі ведуть власні облікові книги та інші записи (рис 1.1). Цей традиційний метод може бути дорогим, частково через це залучають посередників, які стягують плату за свої послуги. Він явно неефективний через затримки у виконанні угод та дублювання зусиль, необхідних для ведення численних бухгалтерських книг. Він також вразливий, оскільки якщо центральна система (наприклад, банк) скомпрометовано через шахрайство, кібератаку або просту помилку, постраждає вся мережа бізнесу.

Кожна транзакція транслюється на кожен вузол мережі біткоїн, а потім після перевірки записується в публічну книгу. Кожна транзакція повинна бути перевірена на дійсність, перш ніж вона буде записана в публічну книгу. Перевіряючий вузол повинен забезпечити дві речі перед записом будь-якої транзакції:

1. Користувачеві належить криптовалюта — перевірка цифрового підпису на транзакції.

2. Користувач має достатню кількість криптовалюти на своєму рахунку: перевіряючи кожну транзакцію з «відкритим ключем» облікового запису споживача в книзі, щоб переконатися, що у нього/неї є достатній баланс на його/її рахунку.

Однак виникає питання підтримки порядку цих транзакцій, які транслюються на кожен інший вузол однорангової мережі біткоїн. Транзакції відбуваються не в тому порядку, в якому вони генеруються, і, отже, потрібна система, щоб переконатися, що подвійне витрачання криптовалюти не відбувається.

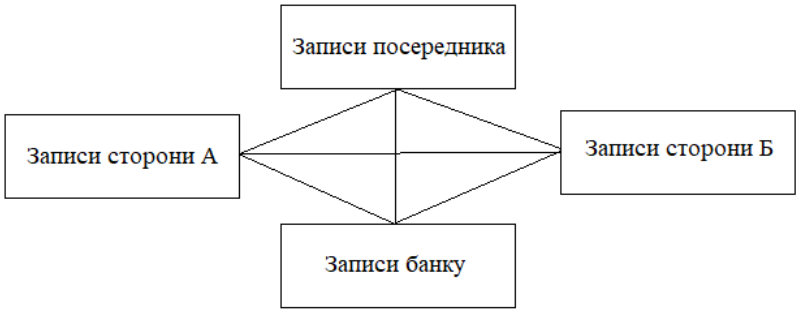

Рисунок. 1.1. Транзакція без застосування блокчейну

Бізнес мережі, які використовують блокчейн (рис 1.2). Архітектура блокчейн дає можливість учасникам поділитися реєстром, який оновлюється через однорангову реплікацію, щоразу, коли відбувається транзакція. Однорангова реплікація означає, що кожен учасник (вузол) в мережі виступає і як видавець, і як передплатник. Кожен вузол може отримати або надсилати транзакції іншим вузлам, і дані синхронізуються через мережу під час передачі.

Рисунок. 1.2. Транзакція з застосуванням блокчейну

Враховуючи, що транзакції передаються вузол за вузлом через мережу біткоїн, немає гарантії, що замовлення, в яких вони отримані на вузлі, є тим самим порядком, в якому ці транзакції були згенеровані.

Мережа блокчєйн економічна та ефективна, оскільки виключає дублювання зусиль і зменшує потребу в посередниках. Також блокчєйн менш вразливий, оскільки використовує моделі консенсусу для перевірки інформації. Транзакції є безпечними, аутентифікованими та легкими для перевірки.

Учасники обох транзакційних систем однакові. Якщо змінилась інформація в одному вузлі, то вона також зміниться в усіх інших одночасно.

Мережа блокчєйн має такі ключові характеристики:

1. Консенсус: щоб транзакція була дійсною, всім учасники необхідно домовитися про її дійсність.
2. Походження: учасники знають, звідки взявся актив і як його належність змінювалася з часом.
3. Незмінність: жоден учасник не може змінювати транзакцію після запису її до бази даних. Якщо в транзакції помилка, нова транзакція повинна бути використана для виправлення цієї помилки, і тоді обидві транзакції будуть записані до бази даних.
4. Остаточність: єдиний загальний реєстр надає одне місце, куди можна перейти, щоб визначити право власності на актив або завершення транзакції.

1.6 Ризики для впровадження

Блокчєйн – перспективна проривна технологія. Існує величезна кількість додатків або проблем, які можна вирішити за допомогою технології на основі Блокчєйн. Від фінансових (переказів до інвестиційно-банківських) до нефінансових програм, таких як послуги нотаріуса. Більшість із них –

радикальні інновації. Як це відбувається з впровадженням радикальних інновацій, існують значні ризики впровадження.

Зміна поведінки: зміни є постійними, але є опір змінам. У світі нематеріальної довіреної третьої сторони, яку представляє Блокчєйн, клієнтам потрібно звикнути до того, що електронні транзакції є безпечними, захищеними та повними. Сучасні посередники, такі як Віза або Мастеркард (у випадку кредитних карток), також змінять ролі та відповідальність. Ми передбачаємо, що вони також інвестують та перенесуть свої платформи на базу Блокчєйн. Вони й надалі надаватимуть послуги у відносинах із клієнтами.

Масштабування: масштабування поточних служб, що зароджуються на основі Блокчєйн, є проблемою. При виконанні транзакції Блокчєйн вперше потрібно буде завантажити весь набір існуючих блокчєйнів і перевірити, перш ніж виконати першу транзакцію. Це може зайняти години або більше, оскільки кількість блоків збільшується в геометричній прогресії.

Завантаження: переміщення існуючих контрактів, бізнес-документів чи фреймворків до нової методології на основі Блокчєйн представляє значний набір завдань міграції, які необхідно виконати. Наприклад, у випадку володіння нерухомістю або права застави, наявні документи, що лежать в компаніях округу або Escrow, необхідно перенести до еквівалентної форми Блокчєйн. Це може включати час і витрати.

Державні нормативні акти: у новому світі транзакцій на основі Блокчєйн урядові установи, можуть уповільнити прийняття, вводячи нові закони для моніторингу та регулювання галузі на предмет відповідності. У США це може певним чином сприяти усиновленню, оскільки ці агентства викликають довіру клієнтів. У країнах з більш контрольованою економікою, як-от у Китаї, прийняття може зіткнутися зі значним супротивом.

Шахрайська діяльність: враховуючи псевдонімний характер транзакцій Блокчєйн, у поєднанні з легкістю переміщення цінних речей, хакери можуть використовувати це для шахрайських дій, таких як торгівля грошима. Тим не менш, за наявності достатньої кількості нормативно-правових актів та

технологічної підтримки правоохоронні органи зможуть контролювати та переслідувати їх.

Квантові обчислення: Основа технології Блокчєйн покладається на той факт, що одна сторона математично не може обробити можливі варіанти через відсутність необхідної обчислювальної потужності. Але з появою квантових комп'ютерів (у майбутньому) криптографічні ключі можна буде легко зламати за допомогою грубої сили протягом розумного часу. Це поставить всю систему під загрозу.

Контр-аргументом було б, щоб ключі стали ще міцнішими, щоб їх було нелегко зламати.

Висновки до розділу 1

Отже у першому розділі було розглянуто літературні джерела які дали опис технології блокчєйн. Були приведені різні типи технологій блокчєйн, та їх стислий опис. Також коротко описана історія застосування блокчєйну та приведені переваги децентралізованої бази даних над централізованою.

Існує величезний інтерес до бізнес-додатків на основі блокчєйн, а отже, численні стартапи, які працюють над ними. Прийняття, безумовно, стикається з сильним супротивом, як описано раніше. Великі фінансові установи, такі як Visa, Mastercard, Banks, тощо, інвестують у вивчення застосування сучасних бізнес-моделей на блокчєйн. Фактично, деякі з них шукають нові бізнес-моделі у світі блокчєйн. Деякі хотіли б залишатися попереду з точки зору трансформованого регуляторного середовища блокчєйн

Функціональність розподіленої бази даних в поєднанні з безпекою блокчєйну робить її дуже привабливою технологією для вирішення поточних фінансових, а також нефінансових проблем бізнесу.

Блокчєйн створює довіру до цифрових даних. Коли інформація була записано в базу даних блокчєйну, її майже неможливо видалити чи змінити.

Якщо дані є постійними та надійними в цифровому форматі, то можна здійснювати різні бізнес транзакції в Інтернеті способами, які раніше були можливими лише офлайн. Все, що було аналоговим, включаючи права власності та особистість, може тепер створюватися та підтримуватися в режимі онлайн. Повільні ділові та банківські процеси, такі як грошові перекази та розрахунки з фондами, тепер можна зробити майже миттєво. Наслідки для безпечних цифрових записів є величезними для глобальної економіки.

Також після ознайомлення з технологією блокчейн відкриваються можливості застосування блокчейну в медицині. Перш за все можна позбутись паперових медичних карт, якщо перевести їх у цифровий формат. В такому форматі буде доступна швидка передача без втрати даних до тих лікарень в яких дані буде потрібно переглянути або додати інформацію до них.

РОЗДІЛ 2
ТЕОРЕТИЧНА ЧАСТИНА

Блокчєйн — це однорангова система без центрального управління потоку даних. Один з ключових способів зняття центрального керування при збереженні цілісності даних полягає у наявності великої розподіленої мережі незалежних користувачів. Це означає, що комп’ютери, які утворюють мережу, знаходяться в кількох Розташування. Ці комп’ютери часто називають повними вузлами.

Блокчєйни складаються з трьох основних частин:

Блок: список транзакцій, записаних за певний період. Їх розмір, період і ініціююча подія для блоків різні. Не для всіх блокчєйн збереження та захищення блоку даних є головною метою. Але всі блокчейни забезпечують зміну своєї криптовалюти або токена. Можна вважати транзакцію як простий запис у базі даних.

Ланцюжок: хеш, який зв'язує один блок з іншим називають ланцюжок. Це одна з найскладніших концепцій в блокчейні для розуміння. Хеш в блокчейні створюється з даних, які були в попередньому ланцюгу. Хеш є унікальним для будь-якого набору даних і блокує порядок блоків даних.

Хоча блокчейни є відносно новою інновацією, хешування не є таким. Хешування було винайдено більше 30 років тому. Це старе нововведення використовується, оскільки створює односторонню функцію, яку неможливо розшифрувати. А функція хешування створює математичний алгоритм, який відображає дані будь-якого розміру до бітового рядка фіксованого розміру. Довжина бітового рядка зазвичай становить 32 символи, який потім представляє дані, які були хешовані. Алгоритм безпечного хешування (SHA) є однією з деяких криптографічних хеш-функцій, що використовуються в блокчейнах. SHA-256 – це звичайний алгоритм, який генерує майже унікальний 256-бітний (32-байтний) хеш фіксованого розміру. Для

практичних цілей можна уявити хеш як цифровий відбиток даних, який використовується, щоб зафіксувати їх усередині блокчейн.

Мережа: мережа складається з «повних вузлів». Можна думати про них як про комп'ютер, на якому запущено алгоритм, який захищає мережу. Кожен вузол містить повний запис усіх транзакцій, які коли-небудь були записані в блокчейн. Вузли розташовані по всьому світу, і ними може керувати будь-хто. Їх стимулюють до керування вузлом, винагороджуючи їх за це криптовалютою. Базовий алгоритм блокчейну винагороджує їх за службу. Нагородою зазвичай є токен або криптовалюта, наприклад біткоїн.

2.1 Життєвий цикл блокчейну

Блокчейн виник зі створенням біткоїну. Це продемонструвало, що група людей, які ніколи не зустрічалися, могли працювати онлайн в системі, яка була нечутлива до обману інших, які співпрацювали в мережі. Оригінальна мережа біткоїн була побудована для захисту цієї криптовалюти. Він має близько 5000 повних вузлів і поширюється по всьому світу. В основному використовується для торгівлі біткоїнами, але спільнота побачила потенціал робити набагато більше з мережею. Через свій розмір і перевірений часом безпеки, він також використовується для захисту інших невеликих блокчейнів і блокчейн-додатків. Мережа Ефір є другою еволюцією концепції блокчейну. Це бере традиційну структуру блокчейну та додає мову програмування яка вбудована всередині нього. Як і біткоїн, він має понад 5000 повних вузлів які глобально поширені. Ефір в основному використовується для торгівлі ефіром, створення контрактів та створення децентралізованих автономних організацій. Він також використовується для захисту блокчейн-додатків і невеликих блокчейнів.

Мережа Фатком – це третя еволюція в технології блокчейн. Вона використовує більш легку систему консенсусу, включає голосування та зберігає набагато більше інформації. Він був створений в першу чергу для захисту даних і системи. Фатком працює з об'єднаними вузлами та

необмеженою кількістю вузлів аудиту. Його мережа невелика, тому він приєднується до інших розподілених мереж, будуючи мости через блокчейни.

2.2 Консенсус як двигун для блокчейнів

Блокчейни є потужними інструментами, оскільки вони створюють надійні системи, які самовправляються без потреби третьої сторони для дотримання правил (рис.2.1). Вони досягають забезпечення виконання правил за допомогою їхнього консенсусного алгоритму.

У світі блокчейну консенсус — це процес розробки угоди серед групи акціонерів, які зазвичай не довіряють. Ці повні вузли в мережі. Повні вузли перевіряють транзакції, які є введені в мережу для запису як частина реєстру.

Рисунок. 2.1. Схема роботи блокчейну

Кожен блокчейн має власні алгоритми створення угоди в межах своєї мережі на записах, що додаються. Існує багато різних моделей для створення консенсусу, оскільки кожен блокчейн створює різні види записів. Деякі блокчейни є цінними для торгівлі, інші зберігають дані та інші забезпечують системи та контракти.

Наприклад, біткоїн торгує вартістю свого токена між учасниками мережі. Жетони мають ринкову вартість, тому вимоги пов'язані з продуктивністю, масштабованістю, узгодженістю, моделлю загрози та моделлю відмови вище.

Біткойн працює на основі припущення, що зловмисники хочуть зіпсувати історію торгів, щоб вкрасти токени.

Біткойн заважає це зробити за допомогою консенсусної моделі, яка називається «доказ роботи». вирішує проблему візантійського полководця: «Звідки ти знаєш, що інформація, яку ви переглядаєте, не була внутрішньо змінена або зовні?» Тому що зміна або маніпулювання даними – це майже завжди можливо, надійність даних є великою проблемою для інформатики.

Більшість блокчейнів працюють за умови, що вони будуть атаковані сторонніми силами або користувачами системи. Очікувана загроза і ступінь довіри, яку мережа має до вузлів, які керують блокчейном визначають тип алгоритму консенсусу, який вони використовують для розрахунку своєї книги.

Наприклад, Bitcoin і Ethereum очікують дуже високий ступінь загрози і використовують міцний алгоритм консенсусу, який називається доказом роботи. Немає довіри до мережі.

На іншому кінці спектру — блокчейни, які використовуються для запису фінансових операцій між відомими сторонами можна використовувати легше і швидше консенсус.

Їхня потреба у високошвидкісних транзакціях важливіша. Доказ роботи надто повільний і дорогий для них через порівняно невелику кількість учасників у мережі та потребу терміновості для кожного транзакції.

2.2 Архітектура Блокчєйну

Технологія блокчейни працює за децентралізованої бази даних, де ці бази даних існують на кількох комп’ютерах і кожна копія цих баз даних ідентична.

Організації зберігають свої дані в централізованій базі даних, що робить їх легкою мішенню для хакерів, тоді як завдяки децентралізованій структурі блокчейну забезпечується захищеність. Блокчейни можна розглядати як однорангову мережу, яка працює на вершині Інтернету. Архітектуру блокчейну можна в основному розділити на три рівні: додатки, децентралізована книга та однорангова мережа. Програми – це верхній рівень мережі, за яким слідує децентралізована книга, а нижній рівень – однорангова мережа. Прикладний рівень містить прикладне програмне забезпечення блокчейн. Наприклад, програмне забезпечення для біткоїн-гаманця створює і зберігає приватні та відкриті ключі, що дозволяє користувачам контролювати невитрачені біткоїни. Прикладний рівень забезпечує зручний для читання інтерфейс, де користувачі можуть відстежувати свої транзакції.

Децентралізований блок — це середній рівень в архітектурі блокчейну, який підтверджує послідовний і стійкий глобальний реєстр. На цьому рівні транзакції можуть бути згруповані в блоки, які криптографічно пов’язані один з одним. Транзакції можна визначити як обмін токенами між двома учасниками, і кожна транзакція проходить процес перевірки, перш ніж вважатися законною транзакцією. Майнінг — це процес групування транзакцій у блок, який додається в кінець поточного блокчейну. Блокчейн використовує спеціальний алгоритм підтвердження роботи, щоб прийняти рішення. Ланцюг, вимагає найбільших кумулятивних зусиль для побудови та забезпечення консенсусу між усіма вузлами для визначення законності блокчейну. Нижній рівень в архітектурі блокчейну — це однорангова мережа, де типи нодів грають різні ролі та обмінюються різними повідомленнями в головний децентралізований вузол.

2.2.1 Прикладний рівень

Він надає інтерфейси додатків поверх блокчейну і використовується для забезпечення безпеки криптовалют. Це програмне забезпечення можна встановити на комп’ютер або мобільний телефон пристроїв або також можуть бути розміщені на сторонній платформі.

2.2.2 Децентралізований вузол

Децентралізований вузол — це спільна та реплікована база даних яка синхронізується між учасниками мережі. Це веде облік операцій між учасниками в мережі. Головна книга відповідає за ведення записів операцій між учасниками. Блокчєйн має властивість бази даних, за винятком того факту, що вона зберігає інформація в заголовку і дані зберігаються у вигляді токена або криптовалюти. Необхідно згрупувати щойно підтверджені транзакції в блок як перший крок запису транзакцій у бухгалтерську книгу. Будь-який учасник блокчєйну може збирати нові транзакції, що створюють створюють блоки, які можна додати до блокчєйн. Блок в основному складається з транзакцій і має покажчик, часові позначки та одноразовий термін. Вузли виконують різні функції залежно від своєї ролі в мережа блокчєйн. Вузол можна назвати майнером, коли він пропонує та перевіряє транзакції та виконує майнінг щоб забезпечити консенсус для захисту блокчєйну. Це може виконувати такі функції, як проста перевірка платежу тощо, і функціонує залежно від використовуваного блокчєйну. Підтвердження роботи визначається як консенсусний алгоритм, який перевіряє точність даних. Наприклад, біткоїн використовує хеш-кеш як доказ роботи для транзакцій з біткоїнами. Майнери повинні заповнити підтвердження роботи, щоб перевірити транзакцій у блоці, щоб його можна було прийняти мережі.

Підтвердження роботи гарантує безпеку та консенсус у мережі блокчєйн. Під час перевірки блок отримує хеш (ідентифікатор). Щоб перевірити наступний блок, цей хеш додається до поточного блоку транзакцій. На наступному кроці додається нонс, яке визначається як випадкове число, яке можна використовувати лише один раз, до кінця наступного блоку. Хеш-функція використовується для змін цього випадкового числа, щоб створити рядок, який містить кількість нулів перед ним.

Підтвердження роботи коштує дорого, і воно може мати майбутні проблеми масштабованості та безпеки, оскільки це завжди залежить від

заохочення майнерів. Існує розширене рішення, яке називається як доказ володіння, який є прибутковим для виконання, і це визначає, хто має право оновлювати консенсус, і відкладає небажане розгалуження базового блокчейну. У блокчейні не передається конфіденційна інформація мережі, і всі транзакції видимі кожному вузлу в мережі. Ця однорангова мережа не вимагає додаткового захисту і може бути побудована на будь-якій фізичній інфраструктурі.

2.3 Версії блокчейну

Блокчейн 1.0. Цей блокчейн в основному використовується для криптовалют і був представлений з винаходом біткоїна. Він також включає основні програми.

Блокчейн 2.0. Блокчейн 2.0 використовується у фінансових послугах та галузях, які включають фінансові активи, опціони, болота та облігації тощо. Смарт-контракти вперше були представлені в Блокчейн 2.0, який можна визначити як спосіб перевірити, чи надсилаються продукти та послуги постачальником під час процесу транзакції між двома сторонами.

Блокчейн 3.0. Блокчейн 3.0 пропонує більшу безпеку в порівнянні з Блокчейн 1.0 і 2.0, він має високу масштабованість і адаптацію та забезпечує стійкість. Він використовується в різних галузях, таких як мистецтво, охорона здоров’я, правосуддя, засоби масової інформації та в багатьох державних установах. Покоління X. Це бачення концепції сингулярності, де послуга блокчейн буде доступна для всіх. Цей блокчейн буде відкритим для всіх і буде управлятися автономними агентами.

2.4 Типи блокчейнів

Блокчейн значно розвинувся за останні кілька років, і на основі його різних атрибутів їх можна розділити на кілька типів.

Публічні блокчейни. Публічні блокчейни відкриті для громадськості, і будь-яка особа може брати участь у процесі прийняття рішень, ставши вузлом, але користувачі можуть отримати або не отримати вигоду для їх залучення до процесу прийняття рішень. Ніхто в мережі не має права власності на реєстри і відкриті для всіх, хто бере участь у мережі. Користувачі в блокчєйн використовують розподілений механізм консенсусу для прийняття рішення та збереження копії вузла бази даних на своїх локальних вузлах.

Приватні блокчейни. Ці типи блокчєйнів не відкриті для громадськості та відкриті лише для групи людей або організацій, а реєстр доступний лише для його учасників.

Напівприватні блокчейни. У напівприватному блокчєйні деяка частина блокчєйну є приватною і контролюється групою або організаціями, а решта відкрита для всіх для участі.

Бічні ланцюги. Ці блокчейни також відомі як прив’язані бічні ланцюги, де монети можна переміщати з блокчєйну в інший блокчєйн. Існує два типи бічних ланцюжків, які називають одностороннім прив’язаним бічним ланцюгом і двостороннім прив’язаним бічним ланцюгом. Односторонній прив’язаний бічний ланцюг дозволяє переміщатися від одного бічного ланцюга до іншого, тоді як двосторонній прив’язаний бічний ланцюг дозволяє переміщатися по обидва боки двох бічних ланцюгів.

Дозволена книга. У цьому типі блокчєйну учасники відомі і вже довіряють. У реєстрі дозволів протокол угоди використовується для підтримки спільної версії правди, а не механізму консенсусу.

Розподілена книга. У блокчейни розподіленої книги реєстр розподіляється між усіма учасниками блокчєйну і може поширюватися між кількома організаціями. У розподіленій книзі записи зберігаються безперервно замість відсортованого блоку, і вони можуть бути як приватними, так і загальнодоступними.

Спільна книга. Спільна книга може бути програмою або базою даних, які спільно використовують публічно або організація.

Повністю приватні блокчейни. Ці типи блокчєйнів не є частиною жодного з основних додатків і відрізняються ідеєю децентралізації Цей тип блокчєйнів стане в нагоді, коли потрібно поділитися даними в організації та забезпечити достовірність даних. Державні організації можуть використовувати приватні запатентовані блокчейни для обміну даними між різними відділами.

Токенізовані блокчейни. Це стандартні блокчейни, які генерують криптовалюти шляхом консенсусного процесу за допомогою майнінгу або початкового розподілу

Блокчєйни без маркерів. Ці блокчейни не є справжніми блокчєйнами, оскільки вони не мають можливості передавати значення, але вони можуть бути корисними, коли не потрібно передавати значення між вузлами, а є лише потреба в передачі даних між вже довіреними сторонами.

2.5 Переваги блокчєйнів

Однією з найбільших переваг блокчєйну є розповсюдження, яке дозволяє використовувати базу даних без центрального органу чи організації. Через децентралізовану природу блокчєйну практично неможливо обмежити дані в порівнянні зі звичайною базою даних.

Користувачі мають право контролювати свою інформацію та транзакції. Блокчейни надають повні, послідовні та актуальні дані.

Оскільки блокчєйн не має центральної точки збою через свою децентралізовану мережу, він може протистояти будь-якій атаці безпеки. Оскільки центральний орган не потрібен, користувачі можуть бути впевнені, що транзакція буде виконана як протокольні команди. Блокчєйн забезпечує прозорість і незмінність транзакцій, оскільки всі транзакції не можуть бути змінені або видалені. Однорангові зв’язки Блокчєйн допомагають виявити шахрайство в мережі та розподілений консенсус. Майже неможливо

вторгнутися в мережу, оскільки зловмисник може вплинути на мережу лише тоді, коли він отримає контроль над 51% вузлів.

Використовуючи блокчейн, конфіденційні бізнес-дані можна захистити за допомогою наскрізного шифрування. Користувачі в блокчейні можуть легко простежити історію будь-якої транзакції, оскільки всі транзакції в блокчейні мають цифровий штамп. Блокчейн стійкий до кібератак завдяки одноранговому характеру і мережі будуть працювати, навіть якщо деякі вузли знаходяться в автономному режимі або піддаються атаці безпеки.

Кілька копій даних можна зберігати в блокчейні, і, отже, користувачі можуть уникнути зберігання конфіденційних даних в одному місці. Клієнти, як правило, більше довіряють системі блокчейн через її підвищену безпеку.

2.6 Недоліки блокчейнів

Блокчейни є дорогими та ресурсомісткими, оскільки кожен вузол у блокчейні повторює завдання для досягнення консенсусу.

У блокчейні користувачі перевіряють транзакцію на основі аутентифікації сертифікатів, прав власності на землю, криптовалюти тощо. Але немає способу скасувати транзакцію, навіть якщо обидві сторони, які беруть участь у транзакції, готові до цього.

Транзакція в блокчейні виконується лише тоді, коли всі вузли в блокчейні успішно перевіряють транзакцію. Це може бути дуже повільним процесом, оскільки вставлений блок повинен бути перевірений, щоб позначити транзакцію як автентичну всіма вузлами. Нова концепція, яка називається освітлювальною мережею, де транзакцію можна перевірити негайно, може бути хорошим рішенням цієї проблеми.

Розмір блокчейну зростає з додаванням блоку. Вузол повинен зберігати всю історію блокчейну, щоб брати участь у перевірці транзакцій, що призводить до постійного зростання блокчейну. Блокчейн буде рости швидше, якщо він має великі блоки, і таким чином відокремить майнерів, і це вплине

на здоров’я блокчейну, оскільки здоров’я залежить від кількості вузлів у мережі.

Одним з недоліків блокчейну є його складність і складність для розуміння людиною. Блокчейн сповнений складних концепцій і процесів, які ще не вдосконалені, щоб звичайна людина могла легко засвоїти та спожити інформацію про те, як ним користуватися, саме через це він ще не готовий до масового використання.

У блокчейні вся інформація, пов’язана з транзакціями, є загальнодоступною, що може стати великою проблемою, коли розподілені реєстри використовуються в чутливих середовищах, таких як робота з державними даними або медичними даними пацієнтів. Книги потрібно змінити і доступ має бути обмежений лише за наявності відповідного дозволу.

2.7 Блокчейни в індустрії

Прозора та децентралізована платформа блокчейн залучила різні галузі, і організації все більше і більше схиляються до її використання для різних бізнес-цілей. Банківські та платіжні системи почали використовувати блокчейн, щоб зробити свої операції більш гладкими, ефективними та безпечними.

Кошти можна ефективно та безпечно передавати за допомогою технології децентралізації.

Блокчейн стає все більш популярним в галузі охорони здоров’я, оскільки він здатний відновити втрачену довіру між клієнтами та медичними закладами.

За допомогою блокчейну здійснюється авторизація та ідентифікація людей. Шахрайства та втрати записів можна уникнути завдяки здатності блокчейну ефективно зберігати та перевіряти документи, юридичні галузі почали використовувати блокчейн для надійної перевірки записів і документів.

Блокчєйн може значно зменшити кількість судових справ і баталій, надаючи автентичний засіб для перевірки та підтвердження правдивості юридичних документів.

Підтасовки результатів виборів можна уникнути за допомогою ефективного використання блокчєйну. Реєстрацію та перевірку виборців можна здійснити за допомогою блокчєйну та забезпечити легітимність голосів шляхом створення загальнодоступної книги записів голосів.

Такі галузі, як страхування, освіта, приватний транспорт і обмін поїздками, державні та суспільні послуги, роздрібна торгівля, нерухомість тощо, почали впроваджувати блокчєйн, щоб зменшити витрати, щоб підвищити прозорість і зміцнити довіру.

Провідні ринкові аналітики прогнозують, що такі галузі, як банківська справа та ринки капіталу, уряд, страхування, споживачі будуть швидко розвиватися до 2020 року, а також різні інші галузі, такі як роздрібна торгівля, охорона здоров'я, фармацевтика, подорожі та транспорт також почне активно використовувати блокчейни у своїх відповідних доменах.

2.8 Практичне впровадження блокчєйну в організаціях

Для організації найкращою областю для початку впровадження блокчєйн є одноразовий незалежний додаток, де не потрібна координація між різними додатками та третіми сторонами.

Простим підходом до впровадження блокчєйну було б представити біткоїн як платіжну систему, оскільки біткоїн вже має надійну і перевірену архітектуру, а також має зростаючий ринок.

Іншим безпечним та ефективним підходом було б впровадження блокчєйну як технології баз даних для управління та ведення цифрових записів транзакцій. Тестування цих одноразових незалежних програм дають організаціям ідею реалізувати блокчєйн як масштабований проект.

Як наступний крок, організації можуть зосередитися на локалізованих додатках, такі як компанії з фінансових послуг, де створення приватних мереж для транзакцій між аналогами допомогли б організаціям заощадити величезні трансакційні витрати. Зміни - це завжди виклик існуючим рішенням, а реалізувати нове та краще рішення вимагає ретельного планування та виконання. Добрий підхід був би без впливу на кінцевих користувачів надати економічно ефективні рішення, які повинні бути легко адаптованими.

Висновки до розділу 2

В даному розділі були розглянуті теоретичні аспекти роботи технології блокчейн в загальному вигляді, також можливості її використання, плюси та мінуси використання розподіленої бази даних, а також були приведені приклади різних типів блокчейнів.

Блокчейн є революційною концепцією, оскільки він успішно зміг забезпечити прозорість серед користувачів і змінив гру для багатьох галузей.

Блокчейн заохочує підприємництво, руйнуючи корупцію бюрократії та встановлення власності загальної маси. Ця технологія «рівний-рівному» відкрила двері для нових можливостей і створила особисту основу для розширення економічних можливостей. Поки що рано говорити, що попереду, але майбутнє блокчейну виглядає багатообіцяючим, і можна зробити висновок, що технологія блокчейн залишиться.

РОЗДІЛ 3
АНАЛІТИЧНА ЧАСТИНА

Будь-який додаток починається з проектування бази даних. У цьому розділі розглянуто і змодельовано основний вузол бази даних електронної медичної карти пацієнта. Використовуючи інструменти для проектування баз даних описана схема бази даних, тобто усі таблиці та їх взаємозв'язки.

3.1 Постановка задачі

Треба змоделювати медичну картку пацієнта лікарні в цифровому форматі. Отже для цього знадобиться основна таблиця під назвою «пацієнт» і вона буде підтримувати взаємозв'язки з іншими таблицями які від неї залежать. Наприклад таблиця «контакти» буде зв'язана з нею по типу один до багатьох. Також в процесі цього розділу буде повністю змодельована схема таблиць.

3.2 Аналіз та проектування електронної карті пацієнта

Почнемо з проектування моделі бази даних. Це буде складна система з багатьма компонентами що взаємодіють один з одним. Перш за все розділимо медичну карту на розділи, щоб було зручніше з ними працювати. Всього буде три розділи.

В першому розділі будуть зазначатись персональні дані про пацієнта, такі як: код хворого, прізвище, ім'я, по батькові, також стать, дата народження, телефон, місце проживання і тому подібне. Вся ця інформація зазначена на першій сторінці медичної карти, але також там зазначається назва міністерства, іншого органу виконавчої влади, підприємства, установа або організації до сфери управління якого належить заклад охорони здоров'я. Окрім цього ще й найменування та місцезнаходження закладу охорони

здоров’я де заповнюється форма. Таку інформацію краще зберігати у відокремленій таблиці, тому перший розділ розіб’ємо ще на два підрозділи, які будуть самостійними таблицями в базі даних.

У другому розділі вже зазначені діагнози, він так і буде називатись: листок запису заключних уточнених діагнозів. До цього розділу входять: дата звернення (число, місяць, рік), заключні діагнози, вперше встановлений діагноз, встановлений вперше при профогляді та підпис лікаря. Якщо з першими полями все доволі зрозуміло, тобто буде використовуватись звичайне поле типу date та інші типу varchar, то з підписом лікаря не все так легко. У цьому полі буде зберігатись ЕЦП лікаря, у зашифрованому вигляді. Для реалізації цього вже існують готові інструменти.

Третій розділ включатиме в себе спеціальні позначки, такі як: група крові, резус фактор, переливання крові (коли, скільки), цукровий діабет, інфекційні захворювання, хірургічні втручання, алергічний анамнез та непереносимість до лікарських препаратів. Тут все зрозуміло з даними про групу крові, резус фактор та цукровий діабет. Це будуть дані типів varchar та bool. Але для того щоб дотриматись першої нормальної форми бази даних, усі інші поля винесемо до окремих таблиць, які будуть зв’язані з цією через foreign key. Наприклад нова таблиця «хірургічні втручання» буде включати в себе: назву втручання та дату проведення. Переливання крові також дату та об’єм. І таким чином наша база набуває атомарності, що і вимагає перша нормальна форма.

Перший розділ бази даних медичної картки (рис 3.1), але як завжди буває, на практиці доведеться вносити зміни. Як видно, до окремої таблиці було винесено організацію, а також телефони, тому що телефонів може бути декілька(мобільний, робочий, домашній і тд.)

Слід зазначити що так як для проектування використовується безкоштовна версія середовища, то відповідні стрілки не вказують тип зв’язку між таблицями, отже зв’язок між таблицею персональних даних та таблицею телефонів «один до багатьох», а зв’язок з таблицею організації «один до

одного». Взагалі існує можливість об’єднати таблицю організації та персональних даних, але зараз вони розділені логічним чином, якщо подумати, то інформація про установу не повинна належати до персональних даних пацієнта, саме тому вона була винесена у іншу таблицю.

Також слід зазначити що в подальшому таблиця «телефон» може бути замінена на таблицю «контакти». Це не дуже критична зміна у проекті і вона легко піддається міграції. В даному випадку було обрано саме таблицю «телефон» через те що в паперовій медичній карті пацієнта контактами зазначаються саме домашні та робочі телефони. В цифровій же системі буде справедливо вказувати і інші контактні зв’язки, наприклад електронну пошту або мессенджер.

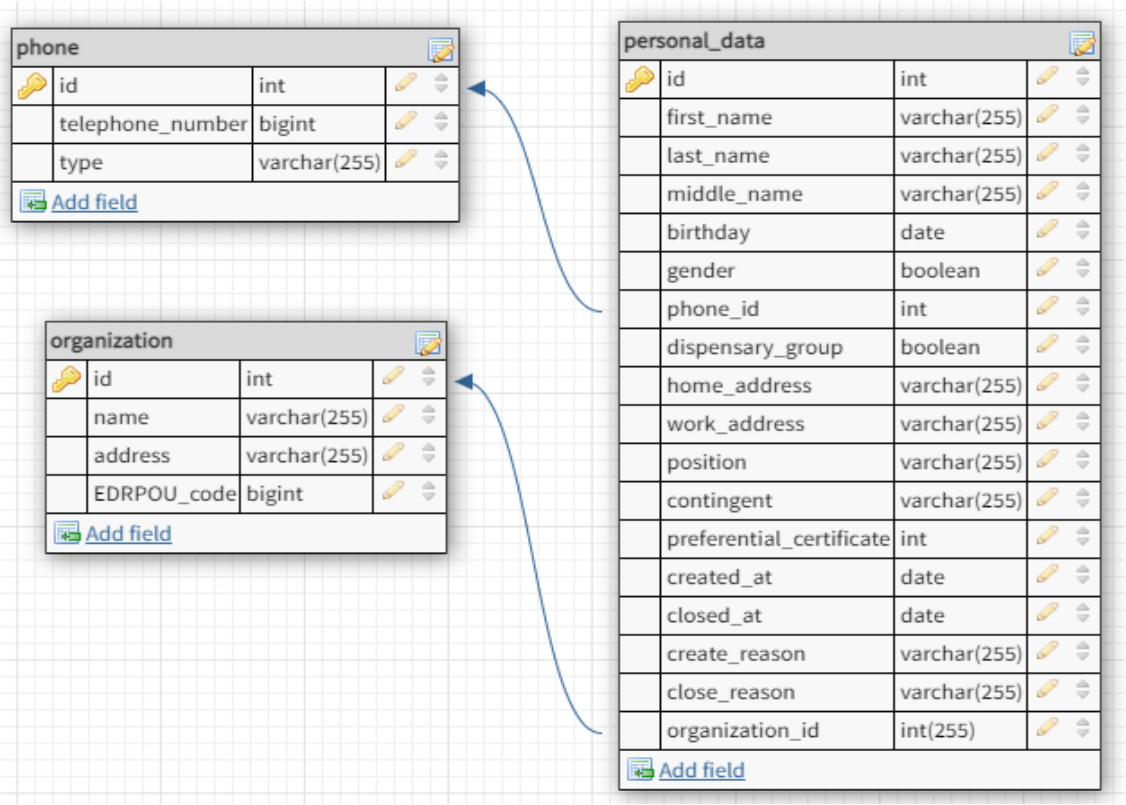

Рисунок 3.1. Перша частина бази даних електронної медичної карти пацієнта

Наступним кроком спроектуємо другий розділ бази даних, у якому буде зазначена інформація щодо діагнозів поставлених різними лікарями. Це одна

з ключових таблиць яка має бути ретельно змодельована тому що на неї буде головний опір в блокчейні.

Оновлена структура бази даних, (рис 3.2) до неї додана таблиця «діагнози». Зв'язок таблиці персональних даних з діагнозами «один до багатьох»

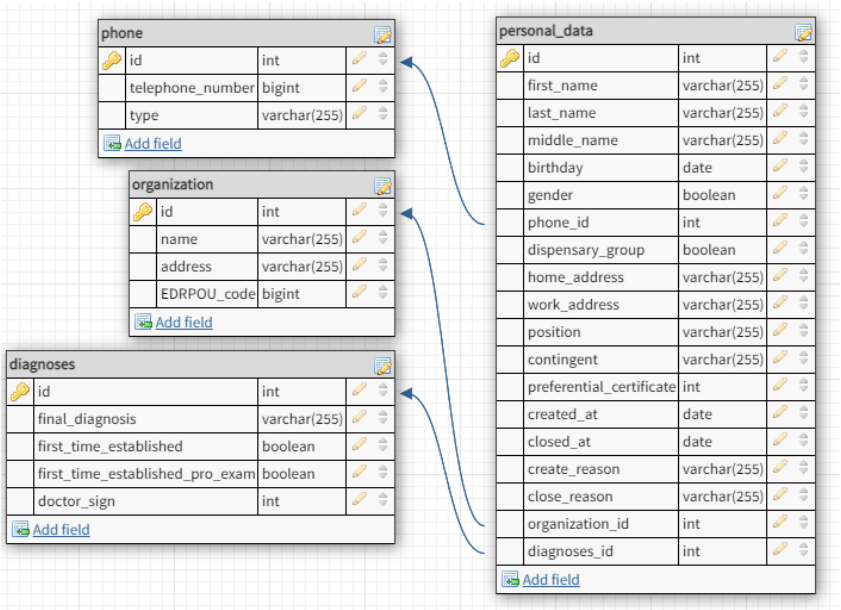

Рисунок 3.2. Друга частина бази даних електронної медичної карти пацієнта

Остаточна схема бази даних (рис 3.3), розписані усі таблиці та зв'язки між ними. Щодо останньої таблиці «сигнальні позначки» то вона має декілька дочірніх таблиць зі зв'язками «один до багатьох».

Таблиці про переливання крові, хірургічні втручання та інфекційні захворювання мають спільне поле дата, в якому вказується коли саме було проведена дана операція або щодо інфекційних захворювань – коли саме пацієнту був встановлений цей діагноз. Ці таблиці були спроектовані таким чином, щоб їх було легко доповнювати, або корегувати при необхідності.

Змодельована схема бази даних буде використовуватись як блок в системі блокчейну, а саме як його частина. Далі через спеціалізовані функції будуть вийматись усі дані з цих таблиць та направлятись в хеш функцію. Після

цього ми отримаємо хеш даних пацієнта і цей хеш буде виступати в ролі гаранту надійності блокчейну, так як наступний блок запам'ятає цей хеш та буде працювати лише з ним, а зміни в попередньому блоці призведуть до зміни хешу попереднього блоку.

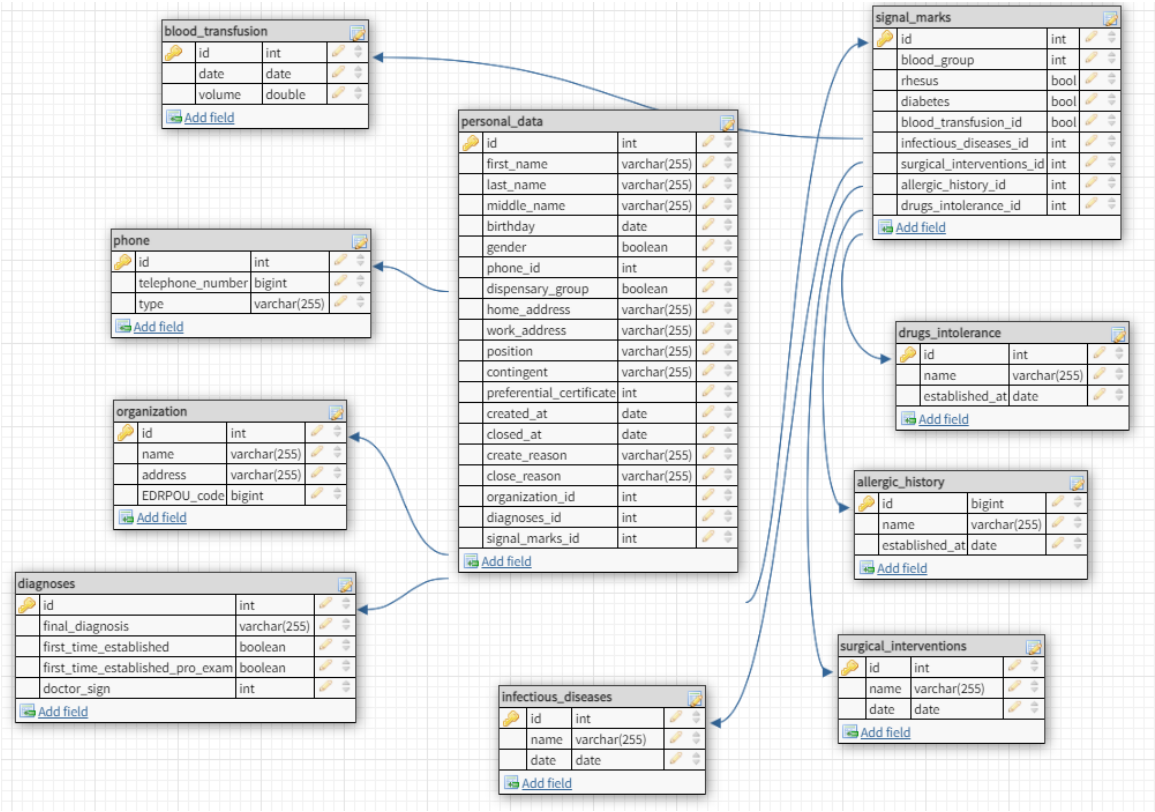

Рисунок 3.3. Повна схема бази даних електронної медичної карти пацієнта

3.3 Опис алгоритму взаємодії блоків

Отже в попередньому розділі було спроектовано схему бази даних, і тепер можна переходити до теоретичного опису алгоритму роботи блоків. Перш за все що таке блокчейн і як він працює. Блокчейн складається з трьох важливих понять: блоки, вузли та майнери.

Кожен ланцюжок складається з декількох блоків, і кожен блок має три основні елементи:

- Дані в блоці.

- 32-розрядне ціле число, яке називається «nonce». Nonce генерується випадковим чином при створенні блоку, який потім генерує хеш заголовка блоку.
- Хеш-це 256-розрядне число, прив'язане до нонс. Він повинен починатися з величезної кількості нулів (тобто бути надзвичайно малим).

Коли створюється перший блок ланцюга, nonce генерує криптографічний хеш. Дані в блоці вважаються підписаними і назавжди прив'язаними до nonce та hash, якщо вони не видобуті.

Майнери створюють нові блоки в ланцюжку за допомогою процесу, який називається майнінгом.

У блокчейні кожен блок має свій унікальний номер, так званий нонс та хеш, але також посилається на хеш попереднього блоку в ланцюжку, тому видобуток блоку непростий, особливо у великих ланцюгах.

Майнери використовують спеціальне програмне забезпечення для вирішення неймовірно складної математичної проблеми пошуку нонса, який генерує прийнятий хеш. Оскільки нонс становить лише 32 біта, а хеш-256, існує приблизно чотири мільярди можливих комбінацій нонс-хеш, які необхідно добути, перш ніж знайти правильну. Коли це відбувається, кажуть, що майнери знайшли "золотий нонс", і їх блок додається до ланцюга.

Внесення змін до будь-якого блоку раніше в ланцюжку вимагає повторного видобутку не тільки блоку зі зміною, але і всіх блоків, які приходять після. Ось чому надзвичайно важко маніпулювати технологією блокчейн. Знаходження золотих нонс потребує величезної кількості часу та обчислювальної потужності.

Коли блок успішно добувається, зміна приймається усіма вузлами мережі, а майнер винагороджується фінансово.

Саме так блокчейн працює на прикладі криптовалюти. Ми будемо застосовувати трохи змінений алгоритм, в якості транзакцій будуть виступати

внесені лікарем зміни до карти пацієнта, а при підтвердженні цих змін буде створюватись новий блок.

Схема роботи блоків у ланцюгу (рис 3.4). Це забезпечує надійне збереження даних. Транзакції може здійснювати тільки лікар, за допомогою власного ЕЦП.

При спробі якось змінити інформацію щодо транзакцій з попередніх блоків, весь наступний ланцюжок блоків стане недійсним, саме завдяки цьому забезпечується цілісність даних.

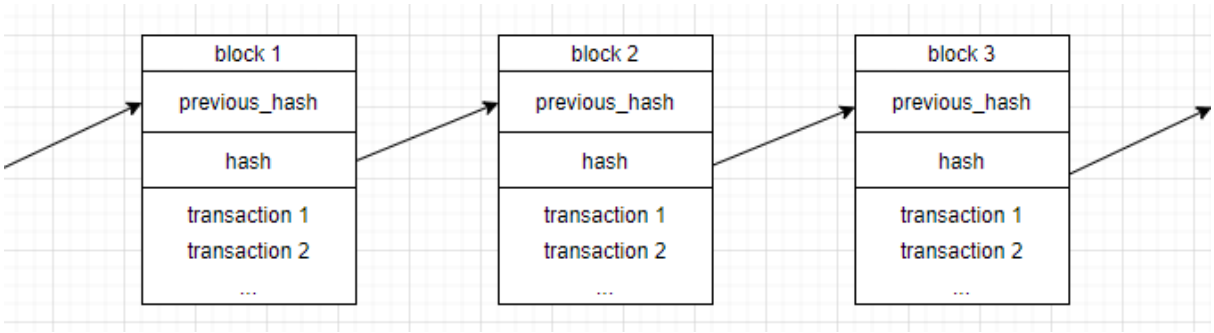

Рисунок 3.4. Схема блоків

Отже перейдемо до проектування алгоритму на основі класів. Спочатку спроектуємо клас Blockchain. У конструкторі буде знаходитись поле chain та current_transaction, також створимо декілька методів, що дозволять працювати з цим блокчейном.

Першим додаємо метод який буде створювати новий блок та додавати його до ланцюжка. Наступним створимо метод, що додає нову транзакцію до списку транзакцій. Взагалі цей метод буде порівнювати як змінились дані в порівнянні з попередніми останніми захешованими їх значеннями.

Також нам знадобляться методи для хешування блоків та повернення останнього блоку у ланцюжку.

Метод хешування буде поєднувати усю інформацію з таблиць, та хешувати. Таким чином ми будемо отримувати хеш блока.

Після додавання нового блоку у ланцюг, ця інформація відправлятиметься до усіх інших користувачів цієї мережі і в усіх оновиться інформація щодо стану пацієнта. Додавати новий блок, тобто підтверджувати зміни у медичній картці пацієнта зможе тільки лікар, при наявності у нього власного ЕЦП.

Безпосередньо пацієнт, також може бути учасником цієї мережі, але тільки в якості глядача. Пацієнт у будь-який час зможе переглянути усі заключення лікарів. На рис.3.5 зображена діаграма класів блокчейну. Це лише теоретична схема взаємодії класів, на практиці можливо знадобиться додаткова їх модифікація.

Клас блок має поле «data», який в свою чергу зберігає в собі повну структуру бази даних, яка була спроектована в попередньому розділі.

В цілому сервіс буде працювати наступним чином. Спочатку йде реєстрація організації або установи, яка буде надавати медичні послуги пацієнтам.

Разом з цим проходить реєстрація лікарів з їх персональними ЕЦП. Далі коли до цієї установи звертається пацієнт, то проходить реєстрація, заповнюється база персональними даними цього пацієнта, при цьому створюється перший блок, і йому надається його хеш значення.

Надалі по мірі звернення пацієнта до лікарів, нові лікарі будуть, підтверджуючи зміни у медичній карті пацієнта, створювати нові блоки.

При створенні нового блоку буде відправлятись запит на всі клієнти цієї мережі для оновлення ланцюга блоків.

Якщо була спроба несанкціоновано змінити який-небудь з блоків цього ланцюжка, то весь ланцюжок на клієнті стане недійсний, та спробує оновитись з будь-якого іншого клієнта цієї мережі на валідний блокчейн.

У мережі клієнтами виступають саме медичні установи та організації і чим більше буде таких клієнтів, тим надійніше буде блокчейн.

У даному випадку буде тільки два вузли децентралізованої бази даних, та при необхідності можуть бути введені додаткові вузли, які будуть виступати в якості перевірочних.

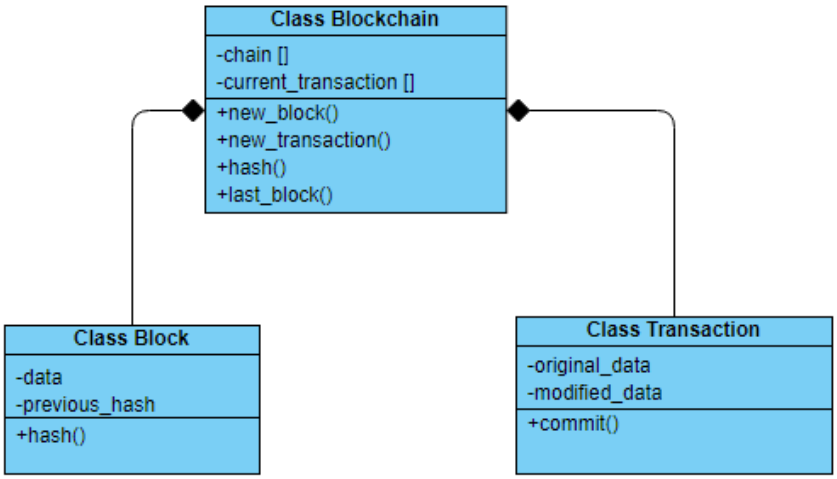

Рисунок 3.5. Діаграма класів блокчейн

3.4 Популярні протоколи консенсусу

Протоколи консенсусу можна вважати основою мережі блокчейн, оскільки вони забезпечують узгодженість і цілісність, що веде до захисту від несанкціонованого доступу та незмінних властивостей. У цьому розділі ми розглянемо деякі добре відомі протоколи консенсусу на користь нових дослідників у просторі блокчейну.

Ці протоколи поділяються на дві широко визначені групи: протоколи, засновані на доказах і на основі голосування. Протоколи на основі підтвердження включають підтвердження роботи (ПР), відкладене підтвердження роботи (ВПР), підтвердження важливості (ПВ), підтвердження минулого часу (ПМЧ), підтвердження ємності (ПЄ), підтвердження повноважень (ПП) і доказ опіку (ДО), тоді як протоколи на основі голосування включають доказ власності (ДВ), делегований доказ власності (ДДВ), протокол Ріпл (ПРІ), практична візантійська відмовостійкість (ПВВ),

делеговану Візантійську відмовостійкість (ДВВ) та Федеративну Візантійську угоду (ФВУ).

3.4.1 Протокол доказ роботи

Одним з найбільш поширених протоколів консенсусу з моменту впровадження біткоїна в 2009 році є ДР. У ДР суб'єкти або учасники мережі використовують обчислювальну потужність, щоб отримати право додавати нові блоки в блокчейн. У разі виявлення нового блоку та його додавання в мережу вузол, який виявив блок, має право отримати попередньо визначену винагороду або комісію за транзакцію. Обчислювальна потужність витрачається на розв'язання хеш-головоломки, розв'язання якої входить в отриманий блок. Процес розв'язування головоломки носить інтенсивний і стохастичний характер. Пошук рішення порівнюється з видобутком золота; отже, процес хешування називають майнінгом, а вузол, який його виконує, — майнером. Будь-який бажаючий і зацікавлений суб'єкт може брати участь у майнінгу, використовуючи власні обчислювальні потужності, що призводить до того, що ДР споживає величезну кількість енергії. Наприклад, енергія, необхідна для роботи мереж біткоїн та ефір, еквівалентна забезпеченню електроенергією 3,5 мільйонів та 1 мільйона домогосподарств відповідно. Крім споживання енергії, інші недоліки ДР включають низьку пропускну здатність і децентралізацію. Щоб супротивник обійшов протокол ДР і порушив консенсус, він повинен перевищити накопичені вищі обчислювальні активи в порівнянні з комбінованими обчислювальними активами всіх чесних компаній, що займаються майнінгом. Це називається атакою 51%. Багато хто вважає, що здійснити цю атаку через мережу блокчейн економічно недоцільно; однак поява пулів для майнінгу та використання інтегральних мікросхем (ASIC) для конкретних додатків показали інше. Біткоїн, ефір, лайткоїн і догкоїн - це криптовалюти, засновані на ДР.

3.4.2 Протокол відкладений доказ роботи

Консенсусний протокол В ДР використовується комодо, багато ланцюговою платформою. Як випливає з назви, багато ланцюгова платформа використовує безпеку, надану вторинним блокчейном (у даному випадку, захист від вирішення хеш-головоломок у ДР) для захисту блоків у основний блокчейн. Цьому процесу сприяють 64 нотаріальних вузла, які обираються щорічно, метою яких є запис у блокчейн ДР. Завдяки цьому В ДР дозволяє уникнути додаткового споживання енергії та накладних витрат. Протокол консенсусу В ДР використовує призначений ДР блокчейн для збереження транзакцій комодо. Окрім економічної ефективності, В ДР також стійкий до атаки 51%, оскільки для успіху противник повинен атакувати як основний, так і вторинний ланцюги.

3.4.3 Протокол доказ власності

ДВ — це альтернативний протокол консенсусу, який зберігає переваги ДР, долаючи деякі його слабкі сторони. У ДВ суб’єкт-учасник повинен мати певну частку (криптовалюта) в системі, щоб майнити або перевіряти транзакції блокування. Якщо учасник володіє 10% частки (монет), то ймовірність майнити наступного блоку таким учасником становить 10%. Механізм пропозиції блоку в протоколі консенсусу ДВ полягає в наступному: блоки створюються вузлами власності, які також називаються валідаторами, яким потім дозволяється брати участь у процесі створення блоку шляхом розміщення певної кількості валюти. Потім протокол вибирає сутність або вузол, які будуть видобувати наступний блок на основі їхньої ставки. Усі вузли, які беруть участь у мережі консенсусного протоколу ДВ, повинні підтвердити право власності на певну кількість акцій, заблокованих у мережі. Згодом псевдовипадковий механізм використовується для вибору лідера або автора блоку. Комітет, сформований шляхом відбору вузлів на основі їхньої частки, заблокованої в мережі, приймає рішення про дійсність блоку, запропонованого лідером. Вибрані валідатори проголосували, щоб схвалити або відхилити запропонований блок. Запропонований блок приймається та

додається до блокчейну лише в тому випадку, якщо більшість членів комітету проголосували за схвалення, як правило, дві третини голосів розміру комітету.

3.4.4 Протокол делегований доказ власності

ДДВ — це ще один протокол консенсусу на основі голосування, який є похідним від ДВ. ДДВ передбачає виборчий процес, аналогічний раді директорів, коли кількість членів правління обмежена і обирається населенням. Крім того, вони мають мандат своїх виборців на здійснення своїх прав. Крім суми криптовалюти, що ставиться, члени з правом голосу обираються шляхом обрання та заміни. Статки, які ставляться в протокол під час раундів голосування, заблоковані в смарт-контрактах. Перевірка транзакцій, створення нового блоку, мережеві операції та обслуговування виконується групою обраних делегатів. Ці делегати є виробниками блоків (ВР), які відповідно винагороджуються за виконану роботу. Існує також група резервних ВР, які також отримують менші винагороди. За будь-яку негативну дію (наприклад, змову) або пропущений хід ВР може бути виключена зі списку. Ставку або монету в смарт-контракті учасника заморожують або конфіскують як штраф. Механізм ДДВ усуває фундаментальні недоліки, такі як проблема «нічого на карті», атака на великі відстані та слабка суб’єктивність базової системи ДВ. ДДВ є більш енергоефективним і має високу пропускну здатність. Одним з основних недоліків ДДВ є те, що він прагне до централізації, і учасники з великими частками в мережі можуть самостійно голосувати за те, щоб стати валідаторами. Біт шейрс, Стіміт, Іос, Ліск та Арк засновані на ДДВ.

3.4.5 Протокол підтвердження повноважності

ПП є варіантом протоколу ДВ. У ПП для перевірки транзакцій і блоків вибираються довірені вузли, відомі як валідатори. Через обмежену кількість необхідних валідаторів мережа має високу пропускну здатність, високу масштабованість і майже нульову плату за обробку. Валідатор також не повинен ставити на ставку будь-які свої активи, як у випадку з ДВ, а скоріше власну репутацію. Здійснюючи ставку на репутацію (щось, що потрібно

заробити з часом, беручи участь у мережі), це долає головну проблему ДВ, де ставка багатства призводить до того, що багаті учасники отримують більшість стимулів у мережі. Однак ПП має тенденцію до сильної централізації, оскільки вся мережа знаходиться в руках невеликої кількості нодів.

3.4.6 Протокол підтвердження важливості

ПВ був введений організацією NEM для надання вузлам дозволу на створення нових блоків, процес, який називається збиранням. Лише вузли з вказаною сумою балансу криптовалюти мають право на збір. Вузли з меншою сумою балансу мають нульову оцінку важливості. Вузли з нульовою оцінкою важливості не мають шансів бути обраними для створення блоків. Це гарантує, що вибрані вузли є лише тими, у яких є заблокований у мережі розумний обсяг багатства, і, таким чином, вони отримають вигоду від захисту мережі через свої власні інтереси. Важливість враховується в процесі збору, коли вузли з вищими оцінками важливості, швидше за все, будуть обрані для створення нових блоків і отримання комісії за транзакції. Важливість розраховується на основі вихідних транзакцій із зазначеним мінімальним значенням, здійснених вузлом протягом певного періоду часу. Процес вибору виробника блоку, по суті, випадковий і заснований на часі, де вузли повинні визначити, чи не падає їхнє поточне значення звернення (розраховане на основі хешу попереднього блоку та відкритого ключа вузла) нижче цільового значення (розрахованого з часу останнього блоку, важливості вузла та поточного рівня складності).

3.4.7 Протокол практична візантійська відмовостійкість

ПВВ — це протокол консенсусу, заснований на тиражуванні між відомими сторонами, який може терпіти відмову до однієї третини сторін.

Це алгоритм для вирішення візантійської помилки, що виникла в результаті невдачі в досягненні консенсусу, викликаної проблемою візантійських генералів (ПВГ). Загалом, обраний лідер (первинний вузол) створює впорядкований список транзакцій, який передається іншим вузлам перевірки, які потім виконують їх.

Після виконання транзакцій вузли перевірки обчислюють хеш-код для нового блоку, який потім транслюється своїм аналогам. Якщо дві третини отриманих хеш-кодів однакові, блок передається в локальну копію блокчейну вузла. ПВВ забезпечує відмовостійкість мережі і дозволяє виконувати тисячі операцій в секунду з незначним збільшенням часу очікування.

Однак одним із основних недоліків ПВВ є можливість практичної реалізації алгоритму через величезну кількість необхідних обчислень. Тендермінт, блокчейн Дієм, Хешграф і Гіперледжер фабрік досягли консенсусу на основі ПВВ.

3.4.8 Протокол Ріпл

Протокол консенсусу Ріпл або ПРі є візантійським відмовостійким протоколом консенсусу. Набір валідаторів (також відомий як унікальний список вузлів), обраний учасниками мережі, оцінює транзакції. Ці валідатори мають бути чесними вузлами, які навряд чи вступлять у змову один з одним. Коли великий відсоток цих валідаторів погоджується на певний набір транзакцій, він включається в наступну версію вузла бази даних. Якщо ні, ці валідатори змінюють свої пропозиції транзакцій, щоб узгодити їх з іншими довіреними валідаторами. Це може включати включення або видалення нових трансакцій. Це ітераційний процес, який виконується до досягнення консенсусу. Консенсус можна досягти, якщо є принаймні 80% валідаторів, які не є несправними. Однак, якщо ця вимога не виконується, вся мережа просто зупиняється та стає невразливою до атак.

3.4.9 Протокол делегована візантійська відмовостійкість

Делегована візантійська відмовостійкість ДВВ – це протокол консенсусу, аналогічний системі управління країною, де є громадяни, делегати та доповідачі, які забезпечують управління країною (мережею).

Цей протокол спирається на систему голосування для вибору делегатів та доповідачів, схожі на ДВ. Громадяни (звичайні вузли) в ДВВ голосують за делегатів (вузли бухгалтерії), де кожен звичайний вузол має право голосу, незалежно від їх цінності. Потім доповідачі обираються випадковим чином з

цих делегатів. Відповідальність несуть делегати для відстеження та запису запитів громадян тобто мережевих транзакцій у вузлі бази даних. Щоб перевірити блок, випадково обраний доповідач пропонує свій останній блок з послідовності блокчейну і транслює його іншим делегатам, які потім порівнюють блок мовця зі своїм, щоб перевірити його дійсність.

Перед запропонованим блок може бути прийнятий і доданий до мережі, принаймні дві третини делегатів повинні погодьтеся з цим.

Однак, якщо менш ніж дві третини делегатів згодні, тоді новий доповідач буде вибиратися випадковим чином, і весь процес цей починається з самого початку.

3.4.10 Протокол федеративна візантійська угода

Призначений для полегшення транзакцій між токенами від різних емітентів. Його основний протокол консенсусу, Протокол згоди Stellar Consensus Protocol (SCP), заснований на Федеративній Візантійській угоді (ФВУ), яка є узагальненням Візантійської угоди (ВУ), яка підтримує відкрите членство. Емітенти токенів можуть призначати валідаторів, щоб забезпечити остаточність транзакції, при цьому валідитори від різних емітентів токенів повинні прийти до консенсусу, перш ніж хтось зможе взяти участь у історії транзакцій. Щоб полегшити процес консенсусу, SCP вводить поняття кворуму.

Кворуми — це підмножини вузлів, де кожна пара кворумів має непорожні перетини.

Іншими словами, кожна пара кворуму має принаймні один вузол, що перекривається. Кворуми відіграють життєво важливу роль у досягненні угоди в розподіленій системі, при якій оновлення стану виконуються лише тоді, коли є кворум згодних вузлів.

Традиційно кворуми є фіксованими та однорідними, але в SCP традиційні кворуми не можуть застосовуватися, оскільки можуть бути випадки, коли вузли не знають про існування один одного. Замість цього

кожен вузол v може оголосити власні фрагменти кворуму (набори вузлів) з такими вимогами:

• Якщо всі вузли в зрізі узгоджені щодо стану системи, v припускає, що вони мають рацію.

• Системну інформацію може отримати v своєчасно з одного з кворуму скибочки в будь-який момент часу.

Зрізи вузла X можуть містити вузли, з якими X має бути узгоджено. Вузли в цих сегментах також мають власні фрагменти кворуму. Угода між вузлами з різних фрагментів кворуму (які не знають про існування один одного) потім виводиться через спільні вузли, які потім утворюють кворум. Протокол SCP складається з двох етапів: висунення та голосування. Під час фази номінації вузли призначають значення-кандидати для фіксації до книги. Повторюючи номінацію своїх однолітків, усі вузли в кінцевому підсумку сходяться до певного значення, відомого як кандидат.

Потім цей кандидат прив’язується до бюлетеня, за який голосують вузли. За кілька кандидатів, які голосують одночасно, може бути кілька бюлетенів. Консенсус досягається, коли вузли можуть знайти кворум, який приймає певний бюлетень.

3.4.11 Протокол підтвердження минулого часу

У 2016 році Intel представила ПМЧ як альтернативу ПР. Наразі проект Sawtooth від Hyperledger працює за протоколом ПМЧ. Замість того, щоб конкурувати на основі обчислювальних ресурсів або власності криптовалюти, ПМЧ реалізує конкуруючу схему, побудовану на механізмі випадкового відступу, який раніше був прийнятий в локальних мережах, спеціально для процедур контролю доступу до середовища. Загалом, вузли-учасники запитують випадково розподілений час очікування, в результаті чого вузол, якому було призначено найкоротший період очікування, вибирається лідером блоку.

Окрім публікації нового блоку, лідер блоку також повинен надати докази свого найкоротшого часу очікування та того, що він не транслював свій

блок до закінчення часу очікування. ПМЧ є більш децентралізованим через низьку вартість участі, що дозволяє більшій кількості організацій легко брати участь. Крім того, організаціям-учасникам набагато легше перевірити, чи був лідер законним обраний і що вартість виборів лідера пропорційна вартості, отриманій від цього.

Однак він не підходить для публічних блокчейнів і не може бути масовим, оскільки він вимагає використання спеціалізованого обладнання Intel. Крім того, це також вимагає довіри у самому апаратному забезпеченні сторонніх розробників, що суперечить одній з фундаментальних ідей блокчейн, тобто він повинен бути надійним.

3.4.12 Протокол доказ опіку

Замість того, щоб інвестувати у фізичні ресурси для виконання операцій з майнінгу, таких як ПР, ДР навмисно спалює криптовалюту як засіб вибору лідерів блоків. Потужні обчислювальні ресурси не потрібні для процесу перевірки блоків у мережах на основі ДР, отже, потужне обладнання для майнінгу, не потрібно. Акт спалювання валюти можна розглядати як акт купівлі віртуальної майнінгової установки. Це дозволяє вузлу продемонструвати прихильність до мережі, беручи короткострокові втрати заради довгострокового виграшу. Монети можна спалити, відправивши їх на заздалегідь визначену адресу запису, і вони не можуть бути відновлені. Ці транзакції запису призводять до хешів запису, які аналогічні хеш-значенням, які використовуються для визначення лідерів блоків у ПР. Slimcoin є одним із прикладів криптовалюти, яка використовує ДР як механізм консенсусу.

3.4.13 Протокол доказ ємності

ДЄ — це протокол, який передбачає виділення нетривіального обсягу пам'яті або дискового простору для вирішення проблеми, представленої постачальником послуг. ДЄ — це частина даних, які перевіряючий надсилає верифікатору, щоб показати, що він зарезервував певний обсяг місця. Наприклад, учасник, який запитує певну послугу, повинен зарезервувати або виділити певний обсяг дискового простору, який потім перевіряється

процесом перевірки. Процес перевірки має бути своєчасним, ефективним і займати достатню кількість дискового простору. Зарезервований простір пам’яті демонструє прихильність вузла до мережі, що гарантує, що вузол, який запитує послугу, є справжнім. На практиці вузлу, що запитує послугу, важко пройти процес перевірки, якщо він не зарезервував простір пам'яті, як заявлено. ДЄ часто реалізується з використанням важкодоступних графіків. Верифікуючий вузол просить запитуючий вузол виконати позначення труднодоступного графа, до якого запитуючий вузол повинен приєднатися. Перевіряючий вузол запрошує запитувача як доказ випадково відкрити кілька місць у зарезервованому дисковому просторі. Burstcoin, Chia і SpaceMint засновані на ДЄ.

3.5 Фінансова сторона застосування блокчєйну

Зазвичай такий посередник, як банк, перевіряє та обробляє фінансові операції. Наявність такої централізованої системи покладає величезну роботу на посередників, в той час як транзакції схильні до помилок, оскільки кільком некоординованим сторонам потрібно вести облік і коригувати їх. Таким чином, весь процес трудомісткий і витратний. Блокчєйн спрощує такі ускладнення, пов’язані з фінансовими послугами, запроваджуючи розподілену публічну книгу, де транзакції перевіряються майнерами за допомогою «підтвердження роботи».

Оскільки кожен вузол в мережі Блокчєйн має копію оновленого Блокчєйн, існує прозорість щодо транзакцій. Оскільки блоки впорядковані в хронологічному порядку, після того, як блок додається до Блокчєйн з підтвердженою транзакцією, весь Блокчєйн стає незмінним.

Таким чином, зловмисники не можуть маніпулювати транзакціями, коли вони зареєстровані в системі. У разі конфліктного блокчєйну, де може виникнути розгалуження, майнери завжди вибирають найдовший ланцюжок, оскільки найдовший ланцюг є надійнішим. Завдяки такому захищеному

протоколу зв’язку та надійному методу перевірки він створює ефективну систему для покращення наших існуючих фінансових послуг.

3.5.1 Криптовалюта

Криптовалюта, ринкова капіталізація якої складає мільярди доларів, стала можливою за допомогою блокчейна. Зокрема, біткоїн, запропонований програмістом, відомим як Сатоші Накамото, заснований на криптографічних методах, які дозволяють одержувачу отримувати гроші безпечно або справді, не вимагаючи довіреної третьої сторони, наприклад, банку або компанії, як-от PayPal.

Мережа біткоїн спирається на блокчейн — розподілену публічну книгу транзакцій — де новий блок генерується шляхом виконання консенсусного алгоритму, такого як доказ роботи.

Практично неможливо отримати чийсь закритий ключ з його чи її відкритого ключа, що не дозволяє користувачам видавати себе за атаки. Щоб здійснити транзакцію, клієнтське програмне забезпечення біткоїн виконує математичну операцію, щоб поєднати відкритий ключ одержувача і закритий ключ відправника разом із кількістю біткоїнів, які ви хочете заплатити або надіслати. Потім транзакція надсилається в розподілену мережу біткоїн для перевірки клієнтами програмного забезпечення біткоїн або користувачами, які не є відправником і одержувачем. Усі користувачі біткоїн, які перебувають у режимі онлайн, окрім відправника та одержувача, перевіряють, чи це правда власник надсилав гроші, використовуючи математичний зв'язок між його відкритим і закритим ключами; публічний журнал транзакцій, що зберігається на комп’ютері кожного користувача біткоїн, щоб переконатися, що відправник має біткоїни на витрати.

3.5.2 Глобальні платежі

Глобальні платежі стають складними та забирають багато часу, оскільки для перевірки транзакцій залучено багато посередників.

Весь процес може бути схильним до помилок і дорого коштувати. Ці проблеми виникають в основному через централізацію грошових операцій,

коли такі установи, як банки та інші фінансові фірми, диктують процеси, і вони відповідають за перевірку операцій. Технологія блокчейн зменшує такі складності, вводячи децентралізовану публічну книгу та надійний метод перевірки для перевірки транзакцій. У цій одноранговій мережі глобальні платежі швидші, піддаються перевірці, незмінні та безпечніші. Є кілька компаній, які здійснюють грошові перекази, такі як Abra і Bitspark, які вже використовують технологію блокчейн для послуг грошових переказів.

3.5.3 Страхові претензії та обробка

Страхові виплати розглядали декілька випадків шахрайства. Крім того, повинні бути оновлені правила та дані, пов’язані з кожною претензією, щоб належним чином обробити страхову претензію, яку важко обробити за традиційних підходів. Завдяки технології блокчейн процес можна ефективно безпечно обробляти за допомогою блокчейн (технологія розподіленої книги). Аналогічно, будь-які шахрайські претензії/транзакції можуть бути виявлені та відкинуті з хорошою впевненістю, оскільки кільком учасникам або майнерам необхідно домовитися про дійсність кожної транзакції. Це гарантує, що страховики швидко та ефективно врегулюють свої вимоги, на які вони заслуговують.

3.6 Застосування блокчейн для уряду

Щоб побудувати надійні та ефективні урядові операції через спільні та прозорі мережі, різні державні організації та підрозділи можуть використовувати технологію блокчейн. Технологія блокчейн з її помітними функціями допоможе забезпечити підзвітність, прозорість і довіру серед зацікавлених сторін, таких як громадяни, лідери, урядовці та їхні різні операції. Уряд зобов’язаний зробити свої справи прозорими, щоб забезпечити підзвітність своїх органів.

Для цього уряду, можливо, доведеться відкрити велику кількість даних для громадськості. Кілька організацій можуть використовувати відкриті дані,

щоб викрити незаконні дії. Громадськість може поставити під сумнів якість медичної допомоги та постачання продуктів харчування з наданими відкритими даними, що в кінцевому підсумку робить систему більш справедливою і довірою.

Отже, оприлюднення даних є корисним для економіки, але воно також має свої проблеми з оприлюдненням даних. Коли дані оприлюднюються лише раз на рік, вони в основному залишаються непоміченими громадськістю.

Таким чином, альтернативою цьому може бути блокчейн-уряд, де дані розподіляються в загальнодоступній книзі і весь час відкриті для громадськості. Крім того, розумні контракти можна використовувати для забезпечення роботи виборців на користь виборців. Контракти можуть бути засновані на маніфесті виборців, і вони отримують гроші лише тоді, коли задовольнить попит виборців за допомогою смарт-контрактів. Така технологія може поставити під контроль електорат і, можливо, змусити їх виконати свої обіцянки.

3.7 Інтернет речей

Кількість електронних пристроїв, які підключаються до Інтернету, з кожним роком стрімко зростає. Завдяки величезній кількості пристроїв, взаємопов’язаних один з одним, створюється Інтернет речей. Очікується, що Інтернет речей змінить спосіб життя, де можливі ідеї, як розумні будинки.

Хоча це нове явище, ймовірно, полегшить життя, маючи величезну кількість неоднорідних пристроїв, підключених до Інтернету, це створює серйозні проблеми з кібербезпекою та конфіденційністю. Блокчейн може бути важливою технологією для захисту інтернету речей. Маючи мільйони пристроїв, підключених один до одного та спілкуючись, важливо забезпечити, щоб інформація, що протікає через Інтернет речей, залишалася захищеною та робила учасниками відповідальними.

3.7.1 Енергетична кіберфізична система

Розумні енергетичні системи стають складними кібер-фізичними системами, де складні взаємодії між виробництвом, розподілом, комунальними службами та користувачами відбуваються двосторонньо. Характерні особливості технології Блокчейн забезпечують безпечне та перевірене середовище для підтримки взаємодії в енергетичній кібер-фізичній системі.

3.7.2 Автомобільна кіберфізична система

Фізична кібернетична система транспортних засобів вважається основою для інтелектуальних транспортних систем, мереж безпілотних літальних апаратів та автономного водіння для підвищення безпеки дорожнього руху та ефективності руху. Безпека та конфіденційність у кіберфізичній системі транспортних засобів завжди є центральними питаннями, оскільки транспортні засоби пов’язані з приватною інформацією їх власника, водія чи орендаря.

Блокчейн з його функціями, такими як децентралізація, незмінність, цілісність та анонімність за допомогою пари відкритих і закритих ключів, можна використовувати для створення розумної та безпечної автономної інтелектуальної транспортної системи.

3.7.2 Блокчейн в авіаційних системах

Блокчейн в авіаційній галузі може запропонувати надійне спільне партнерство між постачальниками послуг і продуктів, щоб пропонувати туристичні послуги, а також продукти розподіленим безпечним способом. Смарт-контракти можуть спростити взаємодію між підприємствами та різними підрозділами всередині бізнесу.

3.7.3 Підтримка блокчейну в системах датчиків

Розумні датчики можуть бути корисними для компаній, щоб збирати інформацію про ланцюжок поставок, коли вони транспортуються по всьому світу. Повідомляється, що кілька провідних компаній ланцюга поставок використовують розумні датчики для відстеження поставок. Тому очікується,

що найближчим часом кількість таких датчиків буде швидко зростати. Маючи такий масовий розподіл датчиків, буде потрібно зібрати та проаналізувати величезну кількість даних. Технологію блокчєйн можна використовувати для руйнівної трансформації для ефективних і безпечних підтримок ланцюгів у мережі.

3.7.4 Блокчєйн для розумного дому

Блокчєйн у контексті розумних будинків із пристроями інтернету речей може допомогти забезпечити безпечні та надійні операції для операцій розумного дому.

Однак впровадження Блокчєйн в таких системах інтернету речей з обмеженими ресурсами не є простим через високий попит на ресурси, необхідні для підтвердження роботи, обмежену ємність зберігання, низьку затримку та низьку масштабованість.

3.7.5 Кібербезпека

Іншим застосуванням блокчєйн є кібербезпека для боротьби з можливими атаками, коли інформація про загрози може передаватися за допомогою блокчєйн між учасниками/організаціями для боротьби з можливими кібератаками. Наприклад, різні організації або країни не вагаються поділитися інформацією про кібератаки або загрози іншим, оскільки конкуренти можуть зловживати інформацією, щоб отримати переваги в односторонньому порядку, коли інформація надається разом із ідентифікаційною інформацією.

Однак, використовуючи блокчєйн за допомогою пари відкритих і закритих ключів, можна поділитися інформацією, не розкриваючи ідентифікаційної інформації, крім відкритого ключа. Це гарантує, що організації або країни можуть обмінюватися інформацією про загрози, не турбуючись про те, що конкуренти зловживають спільною інформацією, щоб скористатися перевагами в односторонньому порядку. Однак блокчєйн не зможе виправити все, але його функції можна використовувати для зміцнення систем проти безлічі кіберзагроз.

3.8 Розумна власність та публічні цінності

Усі об’єкти або майно, такі як будинок, земля, автомобілі, акції тощо, можуть бути представлені в технології реєстру, а блокчейн може використовуватися для відстеження всіх операцій та обліку майна.

Після того, як записи зберігаються в блокчейні, вони надсилаються всім зацікавленим сторонам або учасникам, що можна легко використовувати для укладення контрактів та їх перевірки. Таким чином, за допомогою децентралізованої книги будь-який втрачений запис може бути продубльований з мережі та негайно використаний для відновлення втрати.

3.8.1 Кредитування

Грошове кредитування служить людям для пом’якшення фінансового тягаря в короткостроковій перспективі. Він вимагає від позичальника мати в якості застави таке майно, як нерухомість.

Тому важливо, щоб застава була законною та надійною. Кредитори можуть втратити гроші, якщо заставу не можна викупити. Аналогічно, позичальник може втратити своє майно, якщо кредитор використовує шахрайську політику як частину угоди. За допомогою блокчейн і власність, і політики можна закодувати в реєстрі та розподілити між користувачами. Це створить здорове середовище, де люди зможуть торгувати з абсолютно незнайомими людьми завдяки прозорості та безпеці блокчейн. Смарт-контракти можна розгорнути за допомогою блокчейн для таких сценаріїв.

3.8.2 Розумні прилади

Розумні прилади, по суті, є електронними пристроями, доповненими кібер-системою, так що кібер-частина може передавати інформацію про середовище навколо пристрою та самого пристрою.

По суті, йдеться про ідею «розмовляючого тостера», де тостер може надавати користувачам інформацію, що стосується його використання.

Дім, підключений до розумної техніки, можна вважати розумним будинком, де кіберфізична система намагається оптимізувати функціональні можливості смарт-пристроїв, надаючи максимальну корисність своїм користувачам.

Оскільки так багато пристроїв, залучених до розумних пристроїв, ми можемо закодувати їх у блокчейн як розумну власність.

Така практика може легко забезпечити право власності користувача на ці пристрої.

3.8.3 Управління активами

Управління активами включає в себе кілька сторін, і кожна сторона зобов'язана зберігати операції. Збереження однієї транзакції в різних місцях може зробити весь процес неефективним і схильним до помилок. Що ще гірше, управління активами може також включати транскордонні транзакції, додаючи більшої складності для перевірки транзакцій.

Такі питання можна вирішувати за допомогою розподіленої книги де кожна сторона може мати копію всієї транзакції та отримувати оновлення про кожну транзакцію за допомогою криптографічного зв'язку. Це підвищує ефективність і знижує витрати, оскільки не буде посередника для перевірки транзакцій.

3.8 Хмарні сховища

Метадані, які записують історію створення та всі операції, включаючи дії з доступу до файлів або даних, можуть зберігатися в блокчейні, а потім надаватися всім зацікавленим сторонам. Походження даних через блокчейн важливе для таких додатків, як підзвітність і криміналістична експертиза. Наприклад, коли різні користувачі отримують доступ і вносять зміни до спільних документів, таких як файли, якими ділиться через документ, користувачі можуть вносити зміни, і ці зміни зберігаються в блокчейні. Зберігаючи всі внесені правки та зміни, зберігаються в блокчейні.

Знову ж таки, використовуючи особливості блокчейну та походження, можна підтримувати цілісність та підзвітність у хмарному сховищі та обробці.

Аналогічно, у хмарному сховищі, коли кілька користувачів отримують доступ до вмісту та змінюють його, буде легко відстежувати зміни чи зміни в хмарі для цілісності та підзвітності.

3.9 Інтелектуальна власність

Система управління інтелектуальною власністю може використовувати технологію блокчейн для забезпечення захисту прав інтелектуальної власності, що підтверджуються, коли перевірені, незмінні та безпечні операції в блокчейн можуть допомогти в будь-яких суперечках.

3.10 Нотаріус на основі блокчейн

Блокчейн, що використовує технологію розподіленої книги з криптографією, замінює довірені треті сторони, такі як нотаріус (довірена третя сторона в традиційних системах). Блокчейн допомагає всьому нотаріальному процесу, автоматично виконуючи процес економічно ефективним, прозорим і безпечним способом

3.11 Медицина на основі блокчейн

Особисті медичні записи є конфіденційною інформацією, і з ними потрібно працювати з високим рівнем безпеки.

Такі особисті записи можна кодувати та зберігати за допомогою блокчейн і надавати приватний ключ, який дозволить лише окремим особам отримати доступ до записів.

Подібним чином, той самий протокол може бути застосований для проведення досліджень, коли персональні записи використовуються

відповідно до законів про медичне страхування та про відповідальність, щоб забезпечити конфіденційність даних.

Записи пацієнтів у блокчейні можуть автоматично надсилатися постачальникам страхових послуг, або лікар може безпечно надіслати медичні картки зацікавленим сторонам.

3.12 Збір коштів та прозорість

Прозорість є одним із питань, які необхідно вирішувати в діяльності зі збору коштів, щоб зробити процес надійним. Блокчейн як технологія розподіленої книги може забезпечити прозорість, безпеку та цілісність у діяльності зі збору коштів, використовуючи такі функції блокчейна, як незмінність, перевірка та безпека.

3.13 Бездротові мережі та віртуалізація

Бездротова мережа страждає від стрімкого зростання додатків інтернету речей і кіберфізичних систем. Були вивчені різні підходи для збільшення пропускної здатності мережі та покриття. операторів у спосіб, який можна перевірити, щоб якість обслуговування користувачів була забезпечена шляхом запобігання подвійним витратам/суборенди одного і того ж бездротового ресурсу кільком сторонам у розподілений спосіб.

3.14 Нерухомість

Технологія блокчейн як система баз даних розподіленої книги може принести користь індустрії нерухомості. Запис прав власності можна зробити за допомогою блоків із транзакціями в блокчейн, а не за допомогою традиційної/поточної системи обліку.

3.15 Смарт контракти

Цифровий об’єкт смарт-контрактів, написаний на мові байтів Тьюринга, який називається байт-кодом віртуальної машини Ethereum. По суті, це набір функцій, де кожна функція є послідовністю інструкцій. Такі контракти вбудовані з умовними операторами, які дають змогу виконувати їх самостійно. Смарт-контракти можуть бути заміною посередникам, які гарантують, що всі сторони зобов'язуються за погодженими умовами. Таким чином, з блокчєйн такі регулюючі органи стають зайвими.

Смарт-контракти, засновані на блокчєйн, гарантують, що учасники знають деталі контракту, і угода автоматично виконується після виконання умов. Для того, щоб розумні контракти працювали, існує група взаємно «недовірених» однолітків, які називаються майнерами, які перевіряють транзакції, пов’язані з контрактом. Кожна трансакція, що транслюється в мережу блокчєйн, збирається майнерами та перевіряється, перш ніж вони будуть закодовані в новий блок і додані до блокчєйн.

Будь-який потенційний конфлікт вирішується за допомогою протоколу консенсусу, який базується на «доказі роботи». Таким чином, смарт-контракт працює лише за умови відсутності упередження або більшості обчислювальної потужності мережі, що забезпечує децентралізацію мережі. Майнери отримують винагороду за створення нових блоків згідно з протоколом, якого повинні дотримуватися всі майнери.

Робота будь-якого майнера дискредитується іншими майнерами, якщо він/вона не дотримується протоколу, тому кожен майнер має стимул дотримуватися правил.

Смарт контракти ще один інструмент, за допомогою якого вирішується багато актуальних задач короткий огляд різних додатків, що базуються на управлінні ідентифікацією, і те, як вони можуть отримати користь від технології блокчєйн.

Вони засновані на основі блокчєйн та можуть гарантувати усім учасникам мережі те, що вони знають деталі контракту та угода буде автоматично виконуватись.

3.16.1 Музика на основі блокчєйн

У музичній індустрії є величезним викликом володіти продукцією через права власності та отримати вигоду від розподілу роялті. Щоб монетизувати цифрові музичні продукти, потрібні права власності.

Технологію блокчєйн і смарт-контрактів можна використовувати для створення повної та точної децентралізованої бази даних прав на музику. Тим часом, реєстр можна використовувати для надання прозорої інформації щодо гонорарів виконавця та розподілу в режимі реального часу для всіх залучених лейблів. Цифрову валюту можна використовувати для здійснення платежів згідно з умовами контрактів.

3.16.2 Свідоцтва про народження, шлюб та смерть

Записи про народження, шлюб і смерть є важливими записами громадянина, оскільки вони використовуються для підтвердження громадянства громадян та надання прав відповідно до їх статусу, таких як право голосу та дозвіл на роботу.

Хоча ведення таких записів звичайним методом може бути повільним і схильним до помилок, такі проблеми можна виправити за допомогою публічної книги, такого як блокчєйн. Блокчєйн може зробити такі записи більш надійними, шифруючи записи.

3.16.3 Паспорт

Перший цифровий паспорт був запущений у 2014 році, який міг допомогти власникам ідентифікувати себе в Інтернеті та офлайн. За допомогою цієї технології блокчєйн користувач може зробити знімок і поділитися ним за допомогою криптографічного зв’язку, який можна використовувати для обміну зображенням і перевірки серед користувачів за допомогою цифрових підписів. У системі паспортів на основі блокчєйну

паспорти зберігаються в розподіленій книзі, яка підтверджується або перевіряється як користувачами, так і урядом.

3.16.4 Голосування

Блокчейн може запропонувати багато відчутних переваг для перевіреної безпечної системи голосування в найближчі роки. Поточна система голосування має недоліки і важко перевірити голоси та результати. Таким чином, блокчейн зі своїми функціями може забезпечити незмінну, перевірену та безпечну систему голосування, де виборці можуть віддати свої голоси з найвищою впевненістю з будь-якої точки світу.

3.17 Система репутацій

Система репутації є важливим показником того, наскільки громада довіряє людині. Така система відіграє важливу роль для оцінки людини через її репутацію, яка оцінюється на основі її минулих операцій та взаємодії з громадою.

Кредитну систему можна розглядати як систему репутації, де користувачам надаються кредитні бали на основі їх фінансової діяльності, а пізніше вони використовуються для прийняття рішень щодо інших фінансових операцій. У разі порушення цілісності даних така система може бути фальсифікована.

Таким чином, важливо безпечно зберігати записи минулих транзакцій і справедливо оцінювати репутацію користувачів. Тут блокчейн може бути дійсно важливою технологією, оскільки він веде розподілену публічну книгу, яка ретельно перевіряється консенсусом користувачів у мережі.

3.18 Інші програми та варіанти використання

Технологія блокчейн може використовуватися в будь-яких сценаріях, коли довірена третя сторона не потрібна або однорангова система потрібна для

управління транзакціями, з такими функціями, як прозорість, децентралізація, цілісність, незмінність, безпека та конфіденційність. Однак блокчейн має деякі обмеження, такі як висока затримка, яка вноситься шляхом консенсусу, великий розмір блоків у блокчейні тощо.

Висновки до розділу 3

В даному розділі було спроектовано та змодельовано схему бази даних із взаємодією всіх таблиць. Окрім цього було запропоновано невелике відхилення від повного моделювання паперової медичної картки пацієнта в силу зростання та еволюції цифрових технологій.

У даному розділі було підсумовано не тільки те, як працює блокчейн, але й різні його нові програми та варіанти використання. Ми також представили типи блокчейну та структуру типового ланцюжка блоків у блокчейні. Ми представили кілька відкритих завдань, які необхідно вирішити, щоб повністю використовувати основні функції блокчейну в різних програмах.

Також у даному розділі були розглянуті різні протоколи консенсусу для блокчейну. Були розглянуті їх переваги та недоліки при застосуванні у децентралізованій мережі бази даних. Для додатку був обраний протокол делегована візантійська відмовостійкість. По-перше через те, що йому не важливі цінність вузлів для консенсусу, і в проектованій системі саме цей випадок буде найоптимальнішим серед усіх інших.

Також окрім бази даних було змодельовано невелику систему класів для керування блокчейном

РОЗДІЛ 4
ПРАКТИЧНА ЧАСТИНА

Для переходу до практичної частини роботи було підготовлено середовище розробки від фреймворку Ruby on Rails. Були встановлені всі необхідні для цього бібліотеки, включаючи бібліотеки для аутентифікації користувачів.

Планується розробити два типи користувачів лікар та пацієнт. У цьому розділі здійснюється розробка системи для лікаря, таким чином можна наглядно продемонструвати технологію блокчейн в роботі. Адже лікар вносячи зміни до медичної карти пацієнта створює новий блок електронної карти пацієнта, який зв'язаний з попереднім через хеш. А попередній блок являє собою ту саму електронну карту але до внесених змін.

4.1 Підготовчі роботи

Підготовка проекту включає в себе ретельний підбір потрібних бібліотек та встановлення на комп'ютері необхідного програмного забезпечення для коректної роботи цих бібліотек. Перш за все знадобиться встановлена локальна СУБД, для роботи було обрано PostgreSQL, через її швидкість та надійність. Також цю СУБД використовують більшість ентерпрайзів.

Окрім СУБД також знадобиться середа розробки мови програмування Ruby. Для Рубі знадобиться віртуальний менеджер пакетів, для того щоб встановлювати необхідні бібліотеки до віртуального середовища. Також для коректного відображення зовнішньої частини сервісу, потрібно встановити менеджер пакетів та NodeJS.

Також були введені певні зміни до схеми бази даних. Перш за все в порівнянні з першою версією схеми було прийнято рішення замінити таблицю з номерами телефонів пацієнта на таблицю контактів, яка може зберігати в собі

будь-який тип контакту з пацієнтом, наприклад електронну пошту, скайп, телеграм або той самий номер телефону.

Зараз видозмінена схема бази даних виглядає інакше (рис. 4.1). Також була видалена таблиця спеціальних показників і замість неї усі спеціальні показники тепер з’єднані з таблицею пацієнта.

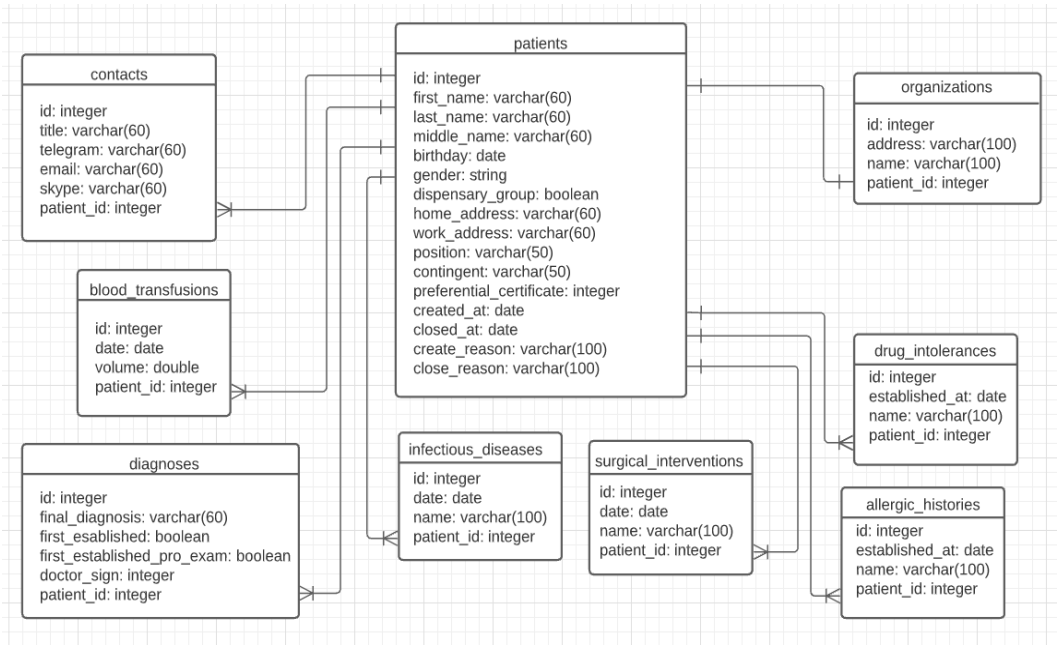

Рисунок. 4.1. Оновлена схема бази даних

4.2 Перша сторінка веб додатку

Після того як були проведені підготовчі роботи, потрібно належним чином оформити першу сторінку додатку. Так як демо проект буде керуватись поки що тільки користувачем лікаря, то перша сторінка буде вести на список пацієнтів та функції маніпуляції з нею. Перша сторінка була введена в роботу і відображена на рис. 4.2.

Поки це демонстраційний проект то були налаштовані базові стилі та оформлення. Перш за все нас цікавить функціонал веб додатку і після того як функціонал буде доведено до належного стану, тоді можна буде додати інші стилі.

В останній версії веб додатку також були додані можливості сортування інформації, це надає лікарю можливість швидше обробляти потрібні запити та полегшує пошук необхідних пацієнтів, або записів у базі даних.

Для наочності в базу були внесені несправжні дані, щоб продемонструвати можливості веб застосунку, та заодно перевірити чи справно працюють увесь запланований функціонал.

Рисунок. 4.2. Головна сторінка додатку

Як можна побачити з рис. 4.2, присутня таблиця з основними даними пацієнта, судячи з яких лікар може визначити з яким саме пацієнтом йому потрібно працювати. Також з права присутня кнопка для внесення змін до даних пацієнта.

4.3 Детальний огляд пацієнта

Після оформлення загальної сторінки всіх наявних пацієнтів можна перейти до більш детального огляду. Натиснувши на кнопку зміни даних пацієнта – переходимо до меню персональних даних. Персональні дані, доступні для редагування можна побачити на рис. 4.3.

Після переходу до детального огляду певного пацієнта користувач переходить в спеціальне меню, де він одразу може побачити підменю для керування даними цього пацієнта, а саме: контакти, діагнози, переливання крові, алергії, алергії на ліки, інфекційні захворювання та хірургічні втручання.

Такі пункти підменю були спроектовані з форми 025 і перехід по ним може полегшити та прискорити як роботу лікаря при встановленні певного діагнозу або при внесенні змін щодо останніх хірургічних втручаннь, або переливання крові, так і для пацієнта буде можливість зручно переглянути які зміни були внесені, коли та ким.

Перейдемо до більш детального перегляду персональних даних (рис. 4.3).

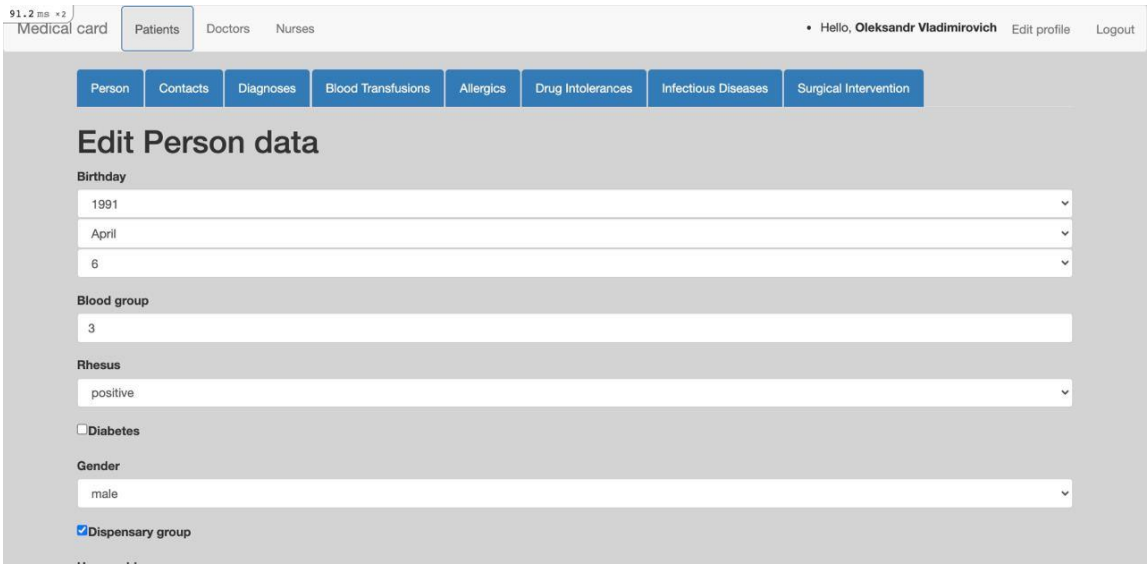

Рисунок. 4.3. Персональні дані пацієнта

Як це видно з рис. 4.3 видно більше детальне відображення персональних даних пацієнта. Не всі з цих даних відображені на рисунку перш за все через доволі довгий писок цих параметрів. Інші параметри можна побачити в третьому розділі на схемі бази даних.

Для більш зручного користування в окремі вкладки були винесені контакти пацієнта ти діагнози (рис 4.4).

Слід зазначити що у поточній версії веб застосунку електронної медичної карти пацієнта наявні лише номер телефону пацієнта, його скайп та найголовніше це електронна пошта. Адже саме через електронну пошту здійснюється найбільша кількість дій, включаючи навіть реєстрацію пацієнта у веб застосунку.

В системі електронна пошта виступає унікальним ідентифікатором користувача.

Рисунок 4.4. Сторінка контактів пацієнта

Як це видно з рис. 4.4, форми контактів дана версія веб додатку розширює можливості паперової медичної карти пацієнта, оскільки в ній під способами зв’язку існують тільки телефони, а у цифровій версії контакти поширюються на месенджери та електронну пошту.

Як це видно з рис. 4.5 вперше можна побачити невеликі зелені круги, які відображають блоки блокчейну. Зараз вони знаходяться у звернутому вигляді, тоді як буде потрібно детальніше передивитись транзакції цих блоків, їх можна окремо один від одного розгортати, дану можливість буде продемонстровано після ознайомлення з усіма підпунктами меню пацієнта.

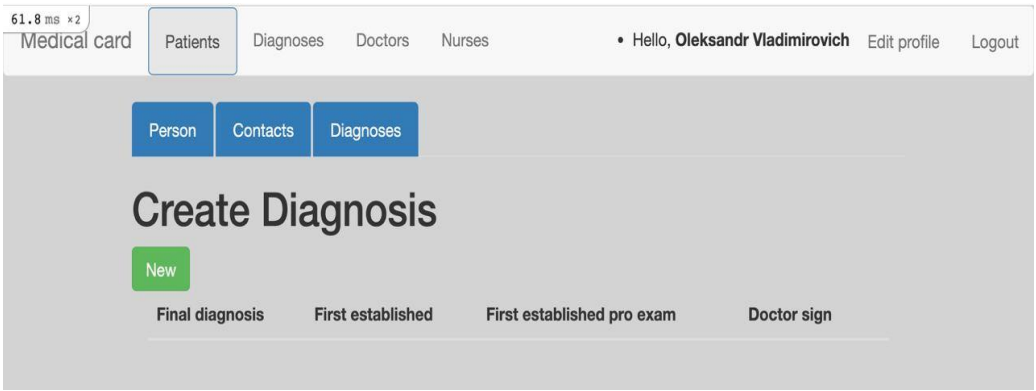

Рисунок. 4.5. Сторінка діагнозів пацієнта

Вкладка діагнози, яка була останньою вкладкою продемонстрованою в попередній версії додатку електронної медичної картки, як це видно з рис. 4.5, до того як в неї були внесені зміни.

Вкладка діагнозів включє в себе назву діагнозу, інформацію про те чи вперше цей діагноз був встановлений та підпис лікаря.

У демонстраційній версії додатку підпис лікаря являє собою звичайне ціле число, цього буде достатньо для демонстрації роботи блокчейну.

Наразі вкладка діагнозів виглядає інакше, до неї були додані функції сортування інформації в алфавітному порядку для будь якої колонки, що полегшити роботу лікаря, якщо йому необхідно знайти певну інформацію щодо діагнозів, або переглянути хто саме вносив зміни.

Окрім цього було додано колонку з датою, яка показує коли саме було поставлено діагноз. По даній колонці теж можна відсортувати по даті створення.

Оновлена версія сторінки діагнозів (рис. 4.6).

Рисунок. 4.6. Оновлена форма діагнозів пацієнта

Форма заповнення діагнозів не понесла значних змін порівняно з попередньою версією додатку, вона зображена на рисунку 4.7, на цій формі відображені поля для заповнення та унікального підпису лікаря.

Також додана функція сортування по різним типам даних, як по назві діагнозу, так і по даті встановлення діагнозу лікарем. Ця функція не несе високої нагрузки на систему.

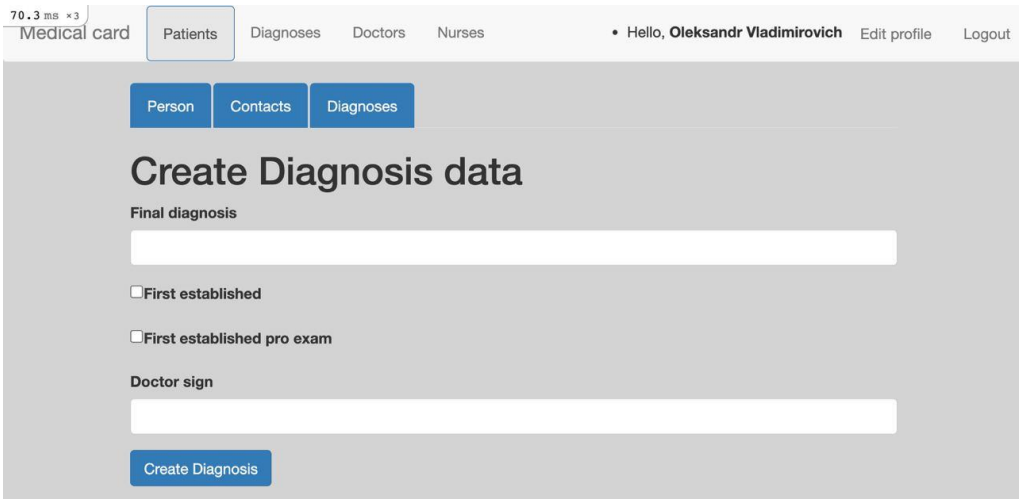

Рисунок. 4.7. Форма діагнозів пацієнта

Після заповнення форми інформацією і натиснення лікарем кнопки створення, веб додаток створює запис у базі даних та повертає на сторінку всіх діагнозів з оновленою інформацією, що зображено на рисунку 4.7. Також створюється новий блок з транзакціями створення нового діагнозу, на рис. 4.8 не відображено створення нового блоку, тому що в попередній версії веб додатку ще не було введено блокчейн компоненту.

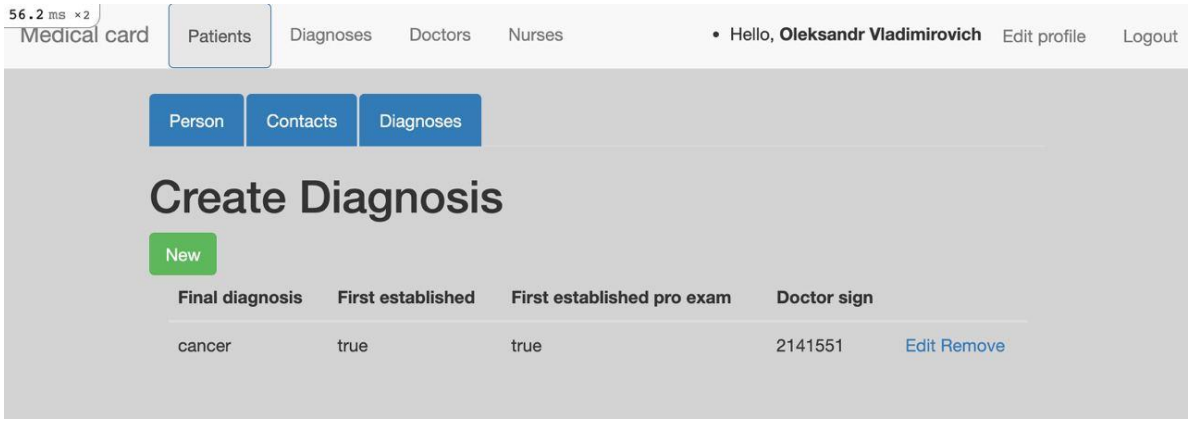

Рисунок. 4.8. Оновлена сторінка діагнозів

Наступним пунктом розглянемо одну з нових сторінок веб застосунку – це меню історії переливань крові. Наразі це меню містить в собі два поля: дату коли саме було переливання крові та кількість крові що було перелите пацієнту. Меню переливання крові зображено на рис. 4.9.

Рисунок. 4.9. Сторінка переливання крові

Така форма буде зручна як для лікаря так і для пацієнта при перегляді.

На цій сторінці також можна побачити відображення нодів блокчейну. Це ті ж самі блоки, що і у попередньому меню, так було впроваджено для зручного перегляду транзакцій блоків.

На рис. 4.10 зображено меню алергій. Діагностуючи будь-яку алергію у пацієнта на зовнішній подразник, лікар може занести ці данні в базу даних. Ці зміни також будуть відображені в блокчейні.

Наразі для наочності в таблицю алергій були занесені тестові дані, які не являють собою нічого правдивого.

Можна побачити що ця таблиця зберігає в собі назву алергії та дату встановлення.

На даний момент часу поки що не були введені функції сортування для цих колонок, так як навряд чи у одного пацієнта буде багато різних алергій, для необхідності їх сортувати по назві або даті встановлення.

При проектуванні виникала ідея замість розподілення таблиць окремо на алергії та діагнози можна було зробити одну таблицю в базі даних, яка б вміщувала в собі і діагнози і алергії, але було прийнято рішення слідувати

канонічній формі 025 та розподілити ці таблиці, адже лікарю слід окремо бачити алергії.

Також вони можуть існувати на протязі всього життя і замість закриття як з діагнозами їх буде швидше просто видалити, адже транзакція все одно збережеться.

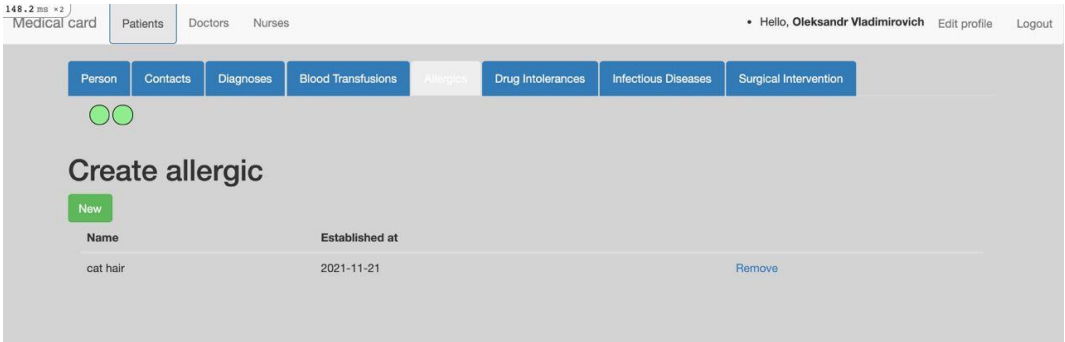

Рисунок. 4.10. Сторінка алергій

Як видно з рис. 4.11 зображено схожу з попередньою таблицю, алергії на препарати.

Згідно форми 025 алергії на зовнішні подразники та препарати розділяють на різні категорії, у веб застосунку було також розділено ці два типи.

Як видно з рис. 4.11 що інтерфейс оформлено для того щоб лікарю було зручно керувати даними пацієнта. А пацієнту було зручно передивлятись маніпуляції лікаря зі своїми даними та відслідковувати останні зміни.

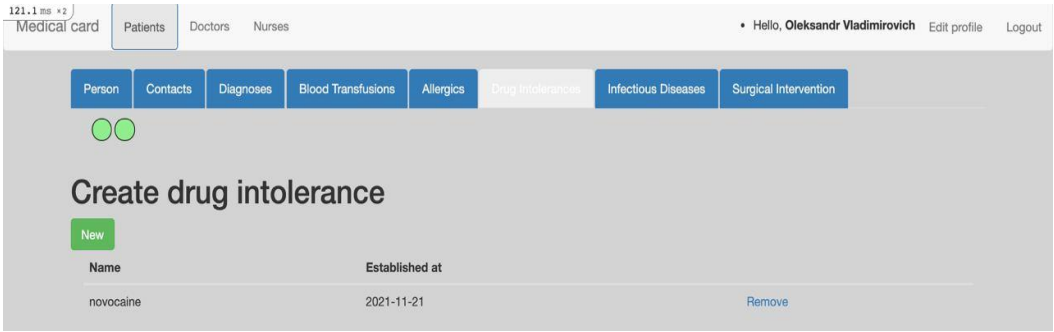

Рисунок. 4.11. Сторінка алергій на препарати

Сторінка алергій на препарати також містить в собі колонки з назвою препарату та датою встановлення алергії. Можливо можна оптимізувати, замість розділення цих двох таблиць ввести одну, але для покращення розуміння все ж таки було прийнято рішення залишити так.

Як видно з рис. 4.12 зображено створення інфекційної хвороби. Насправді це продемонстровано процес діагностування та внесення лікарем в базу даних хворого нового захворювання.

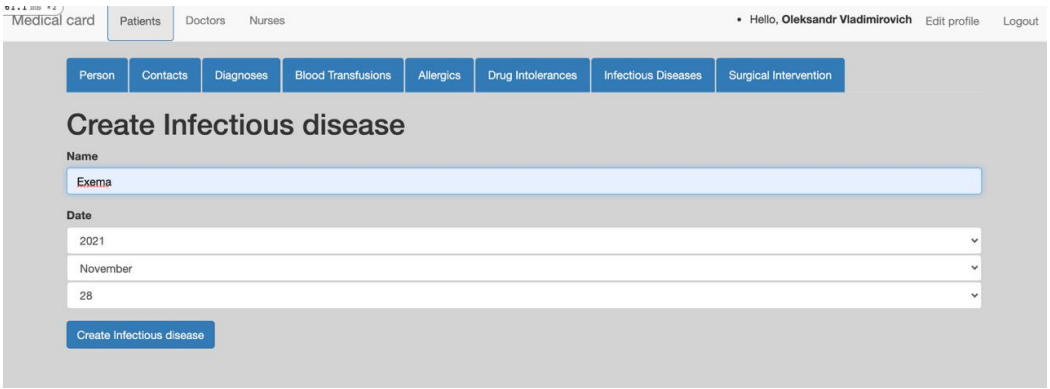

Рисунок. 4.12. Сторінка створення інфекційних захворювань

Як видно з рис. 4.12, або сторінці створення інфекційних захворювань можна побачити такі поля як назва захворювання та дата встановлення цього захворювання.

Після підтвердження створення нового інфекційного захворювання веб застосунок переадресовує користувача на оновлену сторінку усіх захворювань даного пацієнта. Також створюється новий блок у послідовності блоків, до нього записуються ті транзакції створення інфекційної хвороби.

На рис. 4.13 зображена оновлена сторінка інфекційних захворювань пацієнта.

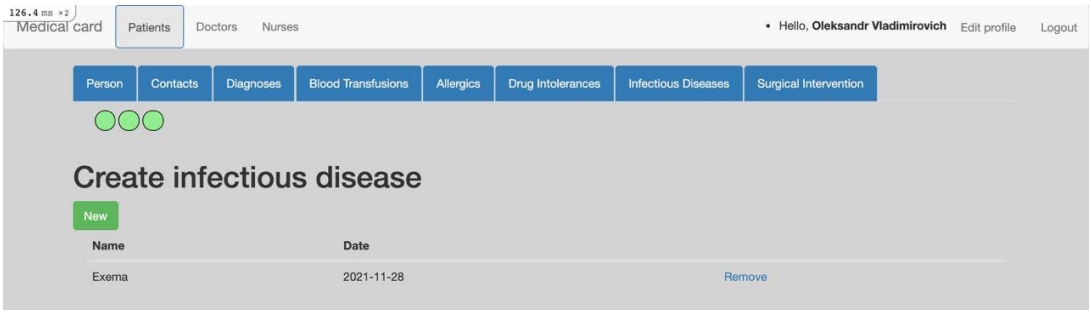

Рисунок. 4.13. Оновлена сторінка інфекційних захворювань

Як видно з рис. 4.13, дійсно було створено новий запис в базі даних щодо інфекційних захворювань, а також новий блок, який зверху зберігається у вигляді зеленого кругу.

Останній та не менш важливий пункт підменю пацієнта, це хірургічні втручання. Сторінка хірургічних втручаннь (рис. 4.14).

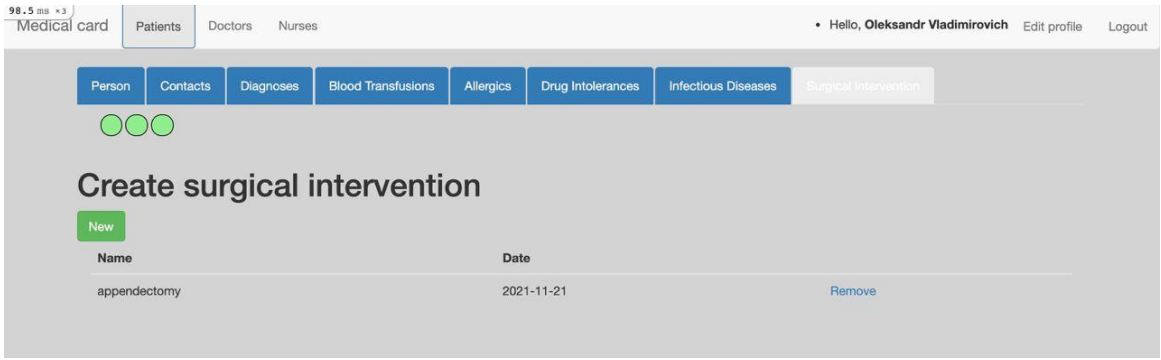

Рисунок. 4.14. Сторінка хірургічних втручаннь

Як видно з рис. 4.15 зображений розгорнутий блок з усією інформацією по ньому. Там зберігаються хеш даного блоку, та проведені транзакції.

Також можна побачити те що, останнє коло виділено жирною лінією, це свідчить про те що розгорнутий саме цей блок. Цей елемент користувацького інтерфейсу був розроблений спеціально для зручного використання як пацієнтом, який переглядає зміни, які були проведені над його персональними даними лікарем. Так і для лікаря це зручний спосіб ще раз переконатись що він не помилився з користуванням системою, та виконав саме ті дії які й планував.

Розгорнутий блок можна з легкістю згорнути лівою кнопкою миші, так само він і розгортається.

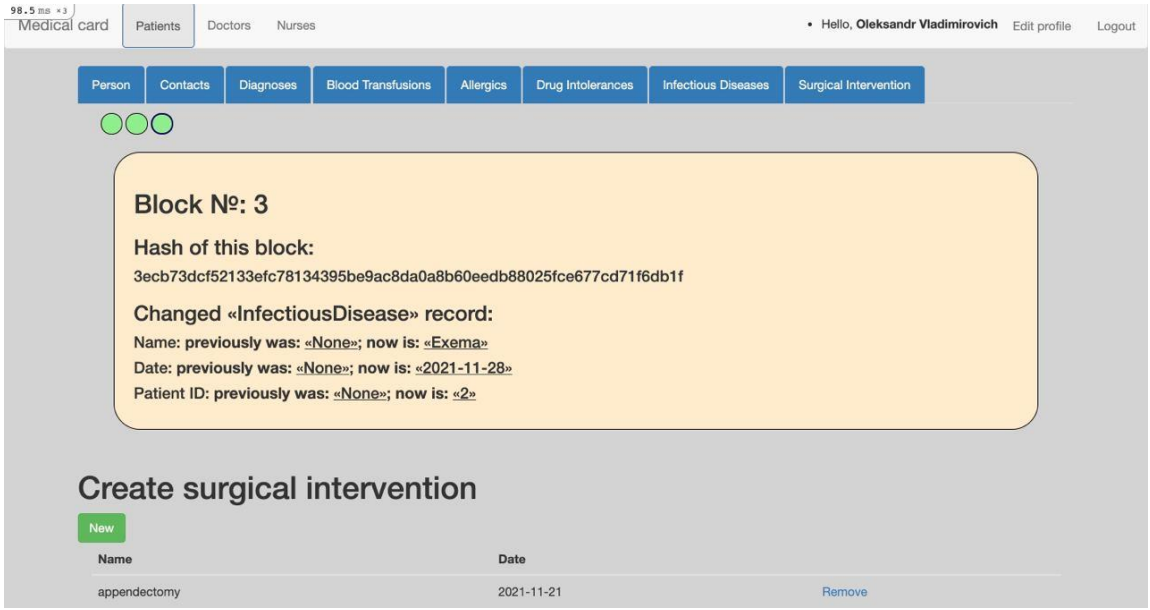

Рисунок. 4.15. Розгорнутий блок

Як видно з рис. 4.15, розгорнутий останній блок транзакцій, також для полегшення сприйняття, шляхом додавання спеціальних стилів, розгорнутий блок обмальовується розширеною границею.

Окрім цього був створений новий запис у базі даних, тому що попередні значення цього запису відсутні.

Якщо лікар змінює дані в базі щодо пацієнта, то в новому блоці в транзакціях будуть відображені ці зміни, а саме будуть присутні попередні значення запису.

Як видно з рис. 4.16 показано як в інтерфейсі користувача виглядають декілька окремо розгорнутих блоків.

Як було сказано раніше, активні або розгорнуті блоки підсвічуються виділеною жирною лінією навколо круга, це свідчить про те що блок знаходиться у розгорнутому вигляді.

Видно що блоки знаходяться у валідному стані, тобто не було застосовано до них жодних несанкціонованих змін.

Якщо ж застосувати несанкціоновану зміну для будь-якого блоку, то він перестане валідуватись в системі і змінить колір кругу на червоний.

Його також можна відкрити та передивитись усі наявні в блоці транзакції.

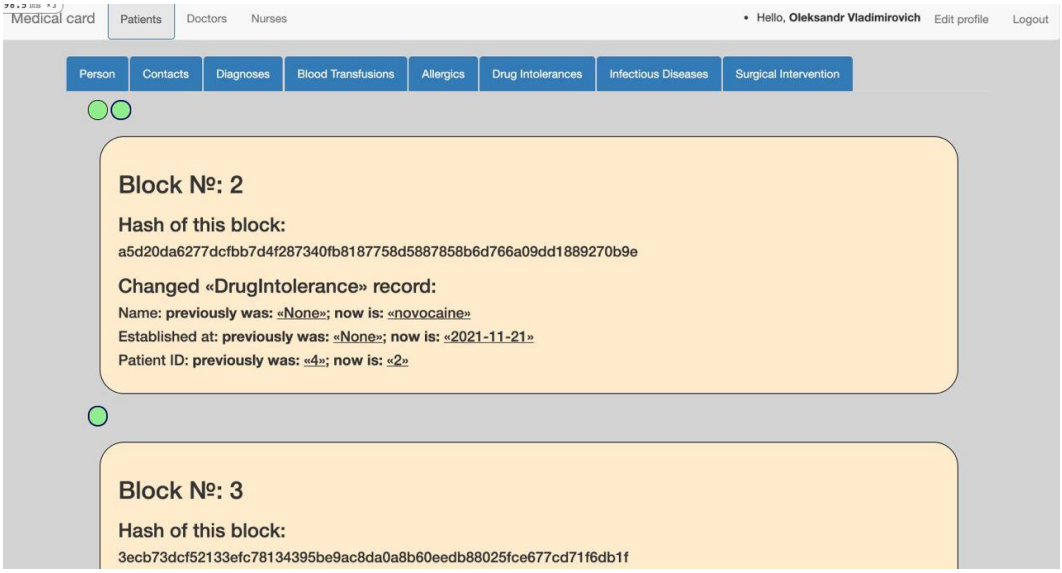

Рисунок. 4.16. Декілька розгорнутих блоків

Як видно з рис. 4.16, є можливість розгорнути декілька блоків одночасно щоб передивитись які зміни були у всіх блоках одночасно.

Продемонстровано несанкціоновану зміну транзакцій блоку через термінал з правами адміністратора (рис. 4.17).

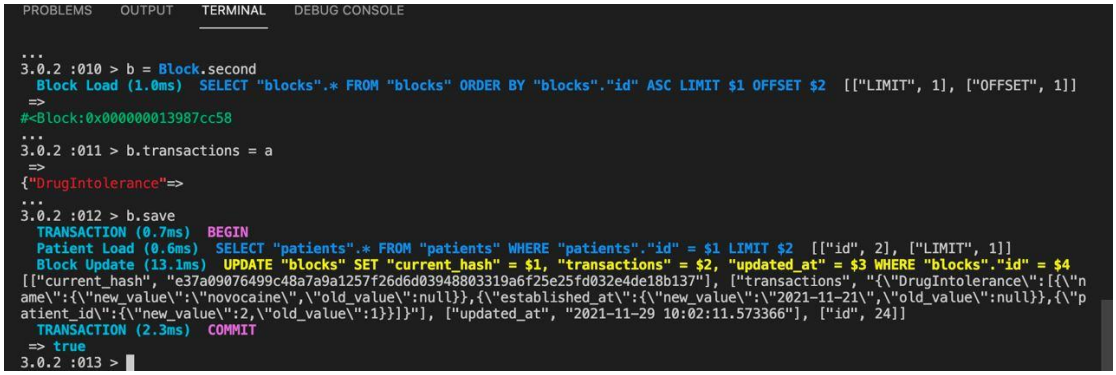

Рисунок. 4.17. Термінал веб застосунку

Спочатку обираємо певний блок, потім змінюємо його поле з транзакціям.

В результаті при оновленні сторінки в веб застосунку маємо невалідний блокчєйн, та червону позначку кола про те, який саме блок перестав валідуватись в системі. Як видно з рис. 4.18 меню веб додатку з невалідним блоком.

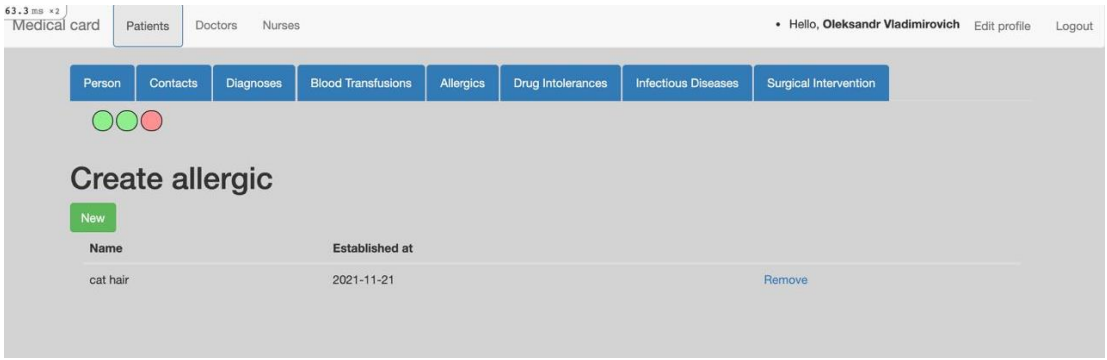

Рисунок. 4.18. Невалідний блок

Як видно з рис. 4.18 останній круг став червоним, це свідчить про невалідність як певного блоку, так і усієї послідовності. В такому вигляді система не зможе прийти до консенсусу і їй потрібно оновитись з будь-якого іншого вузла децентралізованої бази даних, де послідовність блоків повністю проходить валідацію.

Висновки до розділу 4

В даному розділі було створено програмний додаток який відображає взаємодію між лікарем та медичною картою пацієнта. Були впроваджені останні версії існуючих технологій для низькорівневої взаємодії між компонентами веб додатку.

Були продемонстровані можливості використання блокчєйн технологій та перевірка валідності проведених транзакцій. Було доведено, що при будь-

якій незначній зміні даних, стосовно проведених транзакцій, блокчєйн перестає валідуватись у даному вузлі децентралізованої бази даних.

РОЗДІЛ 5
СТАРТАП АНАЛІЗ ПРОЕКТУ

Стартап-проект за темою магістерської дисертації є введенням блокчєйн технологій в сферу медицини, для полегшення роботи з даними лікарів та забезпечення надійності збереження даних. Під керівництвом та з допомогою доценту кафедри біомедичної інженерії Соломіна Андрія В'ячеславовича. Нинішній стартап проект розрахований як для полегшення користування так і надійності даних без додаткової їх перевірки, окрім цього зручний та інтуїтивно зрозумілий інтерфейс було спроектовано для швидкого розуміння про призначення будь-яких пунктів меню веб-застосунку.

Це розділ створений задля аналізу стартап-проекту для можливості впровадження його на ринку нових технологій, так як в нього наразі ще немає конкуренції.

5.1 Резюме бізнес-плану

5.1.1 Найменування проекту

MedicalCard (середа керування даними пацієнта для лікаря та перегляд змін, внесених лікарем пацієнтом).

5.1.2 Характеристика стартапу

В роботі запропоновано варіант проектування сервісу електронних медичних карток пацієнта на основі блокчєйн технологій.

Обґрунтована організація структури бази даних для пацієнта та алгоритм взаємодії блоків з використанням блокчєйн. В цілому система являє собою список блокчєйнів, де кожному пацієнту цієї системи відведено окремий ланцюжок блоків.

5.1.3 Персонал проекту

1. Шерберг Олександр Володимирович (рис. 5.1) – виконавець, магістр кафедри біомедичної кібернетики.

Рисунок 5.1. Виконавець стартап-проекту

2. Соломін Андрій В’ячеславович (рис. 5.2) – науковий керівник, доцент кафедри біомедичної інженерії.

Рисунок 5.2. Науковий керівник стартап-проекту

5.1.4 Переваги нового продукту

Переваги запропонованої системи пов’язані з корисними властивостями технології блокчейн та дозволяють задовольнити вимоги персоніфікації

медичної інформації, надійності тривалого зберігання, розділення прав доступу. Окрім цього це забезпечує довіру до даних, які не можуть бути приховано змінені сторонньою особою, яка має несанкціонований доступ до бази даних, ані лікарем. Головне меню додатку зображено на рис. 5.3.

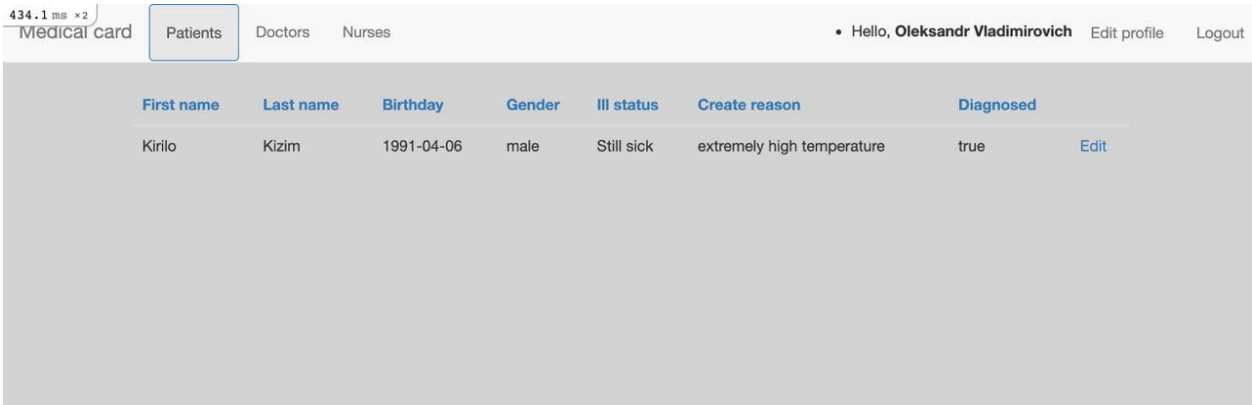

Рисунок 5.3. Головне меню MedicalCard

5.2 Опис ідеї стартап-проекту

Було послідовно проаналізовано:

· зміст ідеї;

· найкращі варіанти застосування;

· користь, яку може принести веб застосунок своїм користувачам;

· наявність на ринку продуктів аналогів.

В табл. 5.1 представлені зміст ідеї, напрямки застосування та яку вигоду може отримати користувач від даного продукту.

Таблиця 5.1

Ідея стартап-проекту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Створення додатку медична карта пацієнта на основі блокчейн технологій	Медицина	Користувачами даної програми будуть як лікарі так і пацієнти. Лікарі зможуть зручно керувати даними пацієнта, а пацієнт переглядати ці зміни.

В табл. 5.2 наведені сильні, слабкі та нейтральні сторони ідеї стартап-проекту.

При аналізі теми, перед проектуванням була наявна проблема щодо швидкодії додатку. У децентралізованих базах даних є період коли їм необхідно прийти до консенсусу. Це доволі затратний по часу процес, але в даному випадку, будуть активні лише дві ноди, одна з яких зберігатиме в собі базу даних на стороні лікарні, а інша на стороні пацієнта. Тому час за який два вузли баз даних зможуть прийти до консенсусу відносно малий і майже не помітний як для лікаря так і для пацієнта.

Але все ж таки є дійсно слабкі сторони, це перехід лікарень на дану систему. Перш за все це буде затратно по часу та ресурсам встановлення та налаштування роботи вузлів веб застосунку. Також складним, але передбачуваним фактором стало те, що пацієнту потрібно буде застосовувати сторонній веб сервіс з базою даних, або тримати активним вузол бази даних у себе на комп’ютері.

Таблиця 5.2

Визначення характеристик ідеї стартап-проекту

№ п/п	Техніко-економічні характеристики ідеї	W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
1	Встановлення та підтримка	+		
2	Конфіденційність для пацієнтів			+
3	Швидкість проходження процесів			+
4	Коефіцієнт довіри користувача до даних			+
5	Надійність збереження даних			+

Висновки до розділу 5

Після проведення стартап-аналізу спроектованого додатку для магістерської дисертації були виявлені сильні та слабкі сторони проекту. В цілому аналіз показав що ідея на даний момент є дуже перспективною і не має аналогів на ринку медицини. Однак на даний момент часу веб застосунок потребує ще багатьох доповнень та оновлень, оскільки проект покриває дуже велику кількість потреб, то звісно і сам потребує багато функціоналу.

Також як можна побачити з характеристик стартап-проекту, він має більше переваг аніж недоліків і уся складність саме у підтримці та встановленні системи для користувачів. Але ця проблема вирішується автоматичним налаштуванням потрібних сервісів, та введення адміністраторської панелі, з якої буде можливо керувати саме підключенням до баз даних.

ЗАГАЛЬНІ ВИСНОВКИ

Поставлена мета в роботі досягнута. Спроектована та реалізована система електронних медичних карток пацієнтів на основі блокчєйн технологій та сучасних алгоритмів збереження та захисту інформації.

В ході роботи магістерської дисертації було проаналізовано можливості застосування блокчєйн технологій, існуючі системи, які працюють на основі блокчєйн. Було виявлено ряд переваг та недоліків при застосуванні блокчєйну. Було вивчено теоретичні відомості стосовно усіх нюансів блокчєйну, розглянуті алгоритми роботи консенсусів та протоколи.

Були приведені різні типи технологій блокчєйн, та їх стислий опис. Також коротко описана історія застосування блокчєйну та приведені переваги децентралізованої бази даних над централізованою.

В роботі запропоновано схему використання переваг технології блокчєйн для забезпечення актуальних вимог сфери діджиталізації медичного документообігу, головним чином обігу електронних медичних карток.

Обґрунтовано будову класів для реалізації технології блокчєйн та структуру бази даних електронних медичних карток, описано схему функціонування сервісу

Окрім цього було спроектовано схему бази даних на основі існуючої паперової версії медичної карти пацієнта, та після цього вдосконалено та оптимізовано цю схему під роботу у цифровому режимі.

Також було створено веб застосунок, який демонструє можливості використання електронної медичної карти на основі блокчєйн та впроваджено графічний інтерфейс користувача, який запроектовано інтуїтивно зрозумілим для користувача. Були впроваджені функції сортування інформації по колонкам.

Було проаналізовано стартап проект, на основі даної дисертації. Проаналізовано сучасний ринок технологій і виявлено що аналогів даний проект не має.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бабенко М. «Введення в теорію алгоритмів та структур даних» // Алгоритми та структури даних. 2019. С. 69-80

2. Вендров А.М. Проектування програмного забезпечення економічних інформаційних систем М.: Фінанси та статистика, 2005. – 544 с

3. Вороновский Г.К. Генетичні алгоритми, штучні нейронні мережі та проблеми виртуальної реальності – Х.: ОСНОВА, 1997 – 112.

4. Заенцев И. В. Нейронные сети: основные модели. Учебное пособие – Воронеж: ВГУ, 1998 – 76.

5. Осовський С. Нейронні мережі для обробки інформації – М.: «Фінанси та статистика», 2002 – 344.

6. Курейчик В.М. Генетичні алгоритми та їх застосування, 2002 – 244.

7. Фултон Хел. Програмування мовою Ruby, 28 серпня 2013. 16 – 364 с

8. Хайкин С. Нейронні мережі: повний курс – СПб. : Вільямс, 2008 – 1104.

9. Єжов А., Чечьоткин В. Блокчєйн технології в медицині– Троїцьк, 2003 – 117.

10. Branke, J. Evolutionary Algorithms for Neural Network Design and Training. Technical Report No.322 – University of Karlsruhe, Institute AIFB, 1995 – 21.

11. Ctistensen D. Blockchain usage in medical structures // Computer science for medicine. 2019. T. 111.

12. Darrel Whitley. A Genetic Algorithm Tutorial – International Workshop on Combinations of Genetic Algorithms and Neural Networks COGANN, 1993 – 40.

13. David A. Black. The Well-Grounded Rubyist. Third edition 2019. 30 – 122 с

14. Delavery L. Fundamental blockchain principles: Discovery, Value Attribution and Exhange 1991–2020 // Computers in Biology and Medicine. 2021. T. 128.

15. Fawcett T. ROC Graphs: Notes and Practical Considerations for Researchers – Kluwer Academic Publishers, 2004 – 38.7. Bansal M., Kasliwal R. R. How do i do it? Speckle-tracking echocardiography // Indian Heart Journal. 2013. T. 65. № 1.

16. Philipp Koehn. Combining Genetic Algorithms and Neural Networks: The Encoding Problem – The University of Tennessee, Knoxville, 1994 – 67.

17. Raval C. Децентралізовані бази даних, та додатки 2017.

18. Rubber O. Databases and design patterns of developing wide used applications 2020.

19. Schaffer, J.D., Whitley, D. and Eshelman, L.J. Combinations of Genetic Algorithms And Neural Networks: A Survey of The State of The Art – International Workshop on Combinations of Genetic Algorithms and Neural Networks COGANN, 1992 – 92.

20. Shifei Ding, Xinzheng Xu, Hong Zhu. Studies on Optimization Algorithms for Some Artificial Neural Networks Based on Genetic Algorithm (GA) – JOURNAL OF COMPUTERS, 2011 – 939-946.

21. Spears W.M., De Jong K.A., Back, T., Fogel D.B. and Garis H.d. An Overview of Evolutionary Computation – Proceedings