МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Чорноморський національний університет
імені Петра Могили
Факультет комп'ютерних наук
Кафедра інтелектуальних інформаційних систем

ДОПУЩЕНО ДО ЗАХИСТУ
Завідувач кафедри інтелектуальних
інформаційних систем, д-р техн. наук, проф.
_____Ю. П. Кондратенко
«____»_____2022 р.

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

СИСТЕМА НА ОСНОВІ БЛОКЧЕЙНУ ДЛЯ ЗАХИСТУ НАБОРІВ ДАНИХ ЩОДО СТАНУ ПОСТ-ІНСУЛЬТНИХ ПАЦІЄНТІВ НА ВІДДАЛЕНІЙ РЕАБІЛІТАЦІЇ

Спеціальність 124 «Системний аналіз»

124 – МКР – 607.21830804

Студент _____ В. О. Шурбін
«__» _____ 2022 р.

Керівник _____ І. М. Журавська
д-р техн. наук, проф.
«__» _____ 2022 р.

Миколаїв – 2022

Чорноморський національний університет ім. Петра Могили
Факультет комп'ютерних наук
Кафедра інтелектуальних інформаційних систем

Освітньо-кваліфікаційний рівень **магістр**
Галузь знань **12 «Інформаційні технології»**
(шифр і назва)
Спеціальність **124 «Системний аналіз»**
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри інтелектуальних інформаційних систем, д-р техн. наук, проф.
_____ Ю. П. Кондратенко
«____» _____20__р.

ЗАВДАННЯ
на магістерську кваліфікаційну роботу

Шурбін Владислав Олегович
(прізвище, ім'я, по батькові)

1. Тема магістерської кваліфікаційної роботи _
Система на основі блокчейну для захисту наборів даних щодо стану пост-інсультних пацієнтів на віддаленій реабілітації.

Керівник роботи д-р техн. наук, проф Журавська Ірина Миколаївна.
Затв. наказом Ректора ЧНУ ім. Петра Могили від «___» ____20__р. № _____
2. Строк подання студентом роботи «___» ___ 20__р.
3. Вхідні (початкові) дані до роботи: набори даних щодо стану пост-інсультних пацієнтів.
Очікуваний результат роботи: програмний комплекс для захисту наборів даних щодо стану пост-інсультних пацієнтів.

4. Зміст пояснювальної записки (перелік питань, які потрібно розглянути): Титульний аркуш, завдання на МР, анотація українською та англійською мовами,
зміст, перелік скорочень. Вступ. Аналіз медичних систем зберігання та обробки даних на основі технології блокчейн. Огляд та вибір апаратних компонентів. Розробка програмного забезпечення для системи зберігання даних на технології блокчейн. Висновки. Перелік джерел посилання. Додатки.

5. Перелік графічних матеріалів
Загальна діаграма компонентів системи. Діаграма розроблемніх смартк-контрактів та їх взаємодії.

6. Завдання до спеціальної частини
Охорона праці ІТ-працівників в медичних установах.

7. Консультанти:

Розділ	**Прізвище, ініціали та посада консультанта**	**Підпис**
Спеціальна частина з охорони праці	зав. кафедри екології д-р біол. наук, проф. Григор'єва Л. І.	
Методична частина	д-р техн. наук, проф Журавська І. М.	

Керівник роботи д-р техн. наук, проф Журавська Ірина Миколаївна.
(наук. ступінь, вчене звання, прізвище та ініціали)

_____
(підпис)

Завдання прийнято до виконання Шурбін Владислав Олегович
(прізвище та ініціали)

_____
(підпис)

Дата видачі завдання «____» _____ 20__ р.

КАЛЕНДАРНИЙ ПЛАН

Виконання магістерської кваліфікаційної роботи

Тема: Система на основі блокчейну для захисту наборів даних щодо стану пост-інсультних пацієнтів на віддаленій реабілітації.

№	Найменування роботи	Початок	Закінчення	Примітки
1	Визначення керівника і теми МКР. Подання заяви на затвердження теми МКР	01.09.2021	10.10.2021	Виконано
2	Отримання завдання на виконання МКР	19.10.2021	22.10.2021	Виконано
3	Складання календарного плану на період виконання МКР	23.10.2021	26.10.2021	Виконано
4	Огляд літератури за темою дослідження	27.10.2021	10.11.2021	Виконано
5	Проходження переддипломної практики, збір та аналіз матеріалів до МКР	29.11.2021	18.12.2021	Виконано
6	Аналіз предметної області та розробка технічного завдання. Моделювання результатів	23.12.2021	02.01.2022	Виконано
7	Опис фахової частини МКР.	03.01.2022	25.01.2022	Виконано
8	Розробка спеціальної частини з охорони праці та методичної частини	26.01.2022	30.01.2022	Виконано
9	Попередній захист МКР на засіданні комісії кафедри	31.01.2022	31.01.2022	Виконано
10	Корегування роботи за результатами попереднього захисту	01.02.2022	03.02.2022	Виконано
11	Остаточне оформлення пояснювальної записки та слайдів доповіді для захисту	04.02.2022	08.02.2022	Виконано
12	Подання МКР рецензенту	11.02.2022	12.02.2022	Виконано
13	Рецензування МКР	13.02.2022	14.02.2022	Виконано
14	Подання МКР, її електронної копії та інших документів (відгуку, рецензії) до захисту	16.02.2022	17.02.2022	Виконано
15	Захист МКР перед екзаменаційною комісією (ЕК)	23.02.2022	24.02.2022	

Розробив студент Шурбін Владислав Олегович _____
(прізвище та ініціали) (*підпис*)

Керівник роботи д-р техн. наук, проф Журавська Ірина Миколаївна _____
(*наук. ступінь, вчене звання, прізвище та ініціали)* *(підпис)*

«25» жовтня 2021 р.

АНОТАЦІЯ

до магістерської кваліфікаційної роботи
студента групи 607 ЧНУ ім. Петра Могили

Шурбіна Владислава Олеговича

на тему: **“ СИСТЕМА НА ОСНОВІ БЛОКЧЕЙНУ ДЛЯ ЗАХИСТУ НАБОРІВ ДАНИХ ЩОДО СТАНУ ПОСТ-ІНСУЛЬТНИХ ПАЦІЄНТІВ НА ВІДДАЛЕНІЙ РЕАБІЛІТАЦІЇ”**

На сьогодні захист медичної облікової інформації представляє комплекс заходів, спрямованих на обмеження доступу до конфіденційної інформації, та включає засоби перевірки достовірності та цілісності інформації. Конфіденційною інформацією вважається інформація про стан пацієнта, яка дозволяю прямим способом або опосередковано ідентифікувати пацієнта, до якого ця інформація відноситься, тобто, його персональні дані. В той же час, для проведення медичних заходив та аналізу стану пацієнта необхідне підтвердження цілісності та достовірності облікової інформації щодо пацієнта.

Метою роботи є створення системи, яка дозволить пацієнту контролювати доступ до своєї облікової інформації, надавати доступ до інформації обмеженому колу осіб – постачальників медичних послуг.

У світі спостерігається тенденція використання для захисту цифрових медичних карт технології блокчейн (сервіси MedRec ц США, Medicalchain у Великобританії, Guardtime в Естонії, тощо). Використання блокчейну може вивести облік медичних послуг на новий рівень, забезпечивши своєчасне оновлення даних і гарантію доступу тільки авторизованих лікарів. Блокчейн (англ. Blockchain) – це технологія розподіленого реєстру, яка використовується для запису транзакцій. Транзакції згруповані у блоки, та кожен наступний блок містить контрольну суму попереднього блоку. Такий підхід забезпечує цілісність реєстру та значно знижує можливість підробки транзакцій. При цьому, повна копія реєстру зберігається на багатьох комп’ютерах одночасно.

В роботі використовується публічна платформа Ethereum для створення децентралізованих онлайн-сервісів на базі блокчейну; вона застосована для зберігання інформації щодо факту надання доступу до інформації пацієнта. Зазначений доступ надається через смарт-контракт між пацієнтом та сертифікованим постачальником медичних послуг. Розроблено додаткове програмне забезпечення для взаємодії пацієнта та постачальника послуг з обліковими даними пацієнта на основі метаданих, що зберігаються у блокчейні Ethereum. Для зберігання облікових даних пацієнта використовується система на основі технології IPFS для розподіленого зберігання інформації з додатковим шифруванням для забезпечення контролю доступу до облікових даних. IPFS (Inter-Planetary File System) – система розподіленого зберігання даних, яка використовує систему ідентифікації за вмістом та зберігає копію даних на кількох вузлах мережі однозначно. Це забезпечує захист даних від підробки та доступність у будь-якій момент часу.

Запропонований підхід та програмне забезпечення доцільно використовувати для захисту наборів даних щодо стану пост-інсультних пацієнтів на віддаленій реабілітації, коли конфіденційні дані передаються від пацієнта до медичного працівника відкритими каналами зв’язку.

ABSTRACT

to the master's qualification work by the student of the group 607
of Petro Mohyla Black Sea National University

Shurbin Vladyslav

"BLOCKHAIN-BASED SYSTEM FOR PROTECTION OF DATA SETS ON THE CONDITION OF POST-STROKE PATIENTS IN REMOTE REHABILITATION "

Today, the protection of medical records is a set of measures aimed at restricting access to confidential information, and includes means of verifying the accuracy and integrity of information. Confidential information is information about the patient's condition that allows you to directly or indirectly identify the patient to whom this information relates, ie his personal data. At the same time, to conduct medical interventions and analyze the patient's condition, it is necessary to confirm the integrity and accuracy of accounting information about the patient.

The aim of the work is to create a system that will allow the patient to control access to their credentials, provide access to information to a limited number of people - health care providers.

There is a tendency in the world to use blockchain technology to protect digital medical cards (MedRec services in the USA, Medicalchain in the UK, Guardtime in Estonia, etc.). The use of the blockchain can take the accounting of medical services to a new level, ensuring timely updating of data and guaranteeing access only to authorized doctors. Blockchain is a distributed registry technology used to record transactions. Transactions are grouped into blocks, and each subsequent block contains the checksum of the previous block. This approach ensures the integrity of the registry and significantly reduces the possibility of forgery of transactions. However, a complete copy of the registry is stored on many computers at the same time.

The work uses the public platform Ethereum to create decentralized online services based on blockchain; it is used to store information about the fact of access to patient information. This access is provided through a smart contract between the patient and a certified health care provider. Additional software has been developed for patient and service provider interaction with patient credentials based on metadata stored in the Ethereum blockchain. IPFS-based distributed storage system with additional encryption is used to store patient credentials to control access to credentials. IPFS (Inter-Planetary File System) is a distributed storage system that uses a content identification system and stores a copy of data on multiple network nodes uniquely. This protects data from forgery and availability at any time.

The proposed approach and software should be used to protect data sets on the status of post-stroke patients in remote rehabilitation, when confidential data is transmitted from patient to health care provider through open communication channels

Пояснювальна записка

до магістерської кваліфікаційної роботи

на тему:

«СИСТЕМА НА ОСНОВІ БЛОКЧЕЙНУ ДЛЯ ЗАХИСТУ НАБОРІВ ДАНИХ ЩОДО СТАНУ ПОСТ-ІНСУЛЬТНИХ ПАЦІЄНТІВ НА ВІДДАЛЕНІЙ РЕАБІЛІТАЦІЇ»

Спеціальність 124 «Системний аналіз»

124 – МКР – 607.21830804

Студент _____ В. О. Шурбін
«__» _____ 2022 р.

Консультант _____ І. М. Журавська
д-р техн. наук, професор
«__» _____ 2022 р.

Миколаїв – 2022

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АІС – архітектура інформаційних систем

БД – база даних

ЗВО – заклад вищої освіти

МІС – медична інформаційна система

ПЗ – програмне забезпечення

ЧНУ – Чорноморський національний університет

ETH - Ethereum

HTTP – HyperText Transfer Protocol

IDE – Integrated Development Environment

IEEE – Institute of Electrical and Electronics Engineers

JCP – Java Community Process

JS – Java Script

MCP - Medical Service Provider

MVC – Model-View-Controller

OMG – Object Management Group

SEI – Software Engineering Institute

SEO – Search Engine Optimization

UI/UX – User Interface/User Experience

WWW – World Wide Web

ВСТУП

Інсульт (у перекладі з латинського «удар») – одна з найтяжчих форм судинних уражень головного мозку. В економічно розвинених країнах інсульт займає друге або третє місце в списках по захворюваності й смертності. У результаті інвалідизації працездатного населення, витрат на тривале лікування й реабілітацію, інсульт наносить суспільству величезний економічний збиток.

З 2017 року розроблено нові глобальні стратегії щодо основ реабілітації пацієнтів та їхніх родичів. Протокол «Реабілітація 2030», підготований Всесвітньою організацією охорони здоров'я (ВООЗ), «Білль про права людини після інсульту» (ВООЗ), «Звіт про інсульт у Європі» (SAFE), а також Програма дій 2018–2030 рр. [1], створена сумісно Європейською асоціацією з боротьби з інсультом (ESO) та Європейського альянсу боротьби з інсультом (SAFE), були створені з метою визначення необхідності та важливості нейрореабілітації після інсульту [2].

В Україні склалася вкрай небезпечна ситуація, пов'язана з наслідками інсульту. На відміну від багатьох інших країн, де ця хвороба займає серед причин смертності третє місце, у нас вона значно випередила злоякісні новоутворення й упевнено займає друге місце. Смертність від інсульту серед чоловіків віком 47–74 років становить 606, а серед жінок – 408 осіб на 100 тис. населення. Це, відповідно, в 11,2 і 12,75 рази вище, порівняно зі Швейцарією, і в декілька разів, порівняно з іншими країнами Європи [3].

Тому в Україні велика увага приділяється організації віддаленої реабілітації пост-інсультних хворих в індивідуальних умовах. У такому разі здійснюється збір повідомлених пацієнтами результатів лікування (наприклад, через шість місяців і один рік), які передаються відкритими каналами зв'язку й тому є уразливими до крадіжки або спотворення. Заходи щодо пост-інсультної віддаленої реабілітації пацієнтів передбачають так звану «роботизовану

терапію» [4]. При цьому різко збільшується обсяг наборів медичних даних, що потребують інтелектуального аналізу з наступним коригуванням індивідуальних реабілітаційних програм.

За даними Всесвітньої організації охорони здоров'я, протягом останніх 15 років спостерігається стабільне зростання у впровадженні національних систем ведення ЕМК. В період з 2011-го по 2016-й показник такого зростання склав 46%. Звісно, їх прийняття стосується в першу чергу країн із середнім та високим рівнем доходу, які щонайменше можуть створити ефективний цифровий реєстр та забезпечити лікарів інструментами для його заповнення [5].

Медичні дані в Україні з 2018 р. передбачають облік в електронних медичних картках (ЕМК) [6]. Сімейні лікарі, терапевти та педіатри медзакладів, що підключені до Електронної системи охорони здоров'я (ЕСОЗ), отримали змогу вносити інформацію про пацієнтів, створюючи для них ЕМК. Пацієнтам, своєю чергою, стала доступною інформація про їх звернення до спеціалістів, діагнози, призначене лікування, направлення на додаткове обстеження тощо. Збереження та поповнювання ЕМК контентом, що містить персональні дані пацієнтів, потребує супроводження та забезпечення захисту великих обсягів даних у цифрових сховищах.

У результаті одного з наймасштабніших на сьогодні зломів даних у сфері охорони здоров'я медичні записи приблизно 4,5 мільйонами пацієнтів системи UCLA скомпрометовано після того, як хакери отримали доступ до мережі [7]. Внаслідок інциденту зловмисники отримали доступ до конфіденційних клінічних та фінансових даних, таких як медичні діагнози та захворювання, клінічні процедури, результати тестів, номери соціального страхування, адреси та дати народження. Ця подія привернула увагу не лише своїм масштабом і розміром, а й тим, що, як і в багатьох інших порушеннях у сфері охорони здоров'я тоді й зараз, дані були переважно незашифрованими.

Понад 40 мільйонів записів пацієнтів були скомпрометовані через інциденти у минулому році, на тлі попереджень про хакерські групи та новини пов’язані з програмним забезпеченням-вимагачем. 2021 рік став особливо жахливим роком з точки зору зловживання медичними даними та інцидентів, які виводять з ладу мережі на кілька тижнів, і потенційно призводять до збоїв у наданні медичної допомоги по всій країні [8, 9].

Об'єкт дослідження – проєктування системи електронного обліку медичних даних на основі блокчейну та смарт-контрактів.

Предмет дослідження – система для захисту наборів даних щодо стану пост-інсультних пацієнтів на віддаленій реабілітації.

Метою магістерської кваліфікаційної роботи (МКР) є створення системи, яка дозволить пацієнту контролювати віддалений доступ до своєї облікової інформації, надавати доступ до інформації обмеженому колу осіб-постачальників медичних послуг.

Досягнення цієї мети буде відбуватися завдяки виконанню наступних завдань:

- аналіз існуючих сервісів-аналогів для контролю ідентифікації та розподілення персональної медичної інформації, розроблених у інших країнах світу;
- дослідження технологій для створення захищеної системи від несанкціонованого доступу;
- розробка моделі створюваної системи з використанням обраних інформаційних технологій;
- розробка системи для захисту наборів даних щодо стану пост-інсультних пацієнтів на віддаленій реабілітації;

- тестування розробленої системи на відкритих спеціалізованих наборах даних великого обсягу, зібраних медичними фахівцями, що працюють з пост-інсультними пацієнтами.

Практичне значення роботи полягає в тому, що дана МКР є складовою частиною науково-дослідної роботи ЧНУ ім. Петра Могили «Розробка модулів автоматизації бездротових приладів відновлення пост-інфарктних, пост-інсультних пацієнтів в індивідуальних умовах віддаленої реабілітації» № держреєстрації 0121U109898 (наук. кер. проф. Трунов О. М.).

Робота пройшла **апробацію** під час XXIV Всеукраїнської науково-практичної конференції «Могилянські читання» (Миколаїв, 08–12 листопада 2021 р.).

Публікації. Основні положення та результати магістерської роботи опубліковані у збірнику матеріалів Всеукраїнської науково-практичної конференції «Могилянські читання–2021» [26].

Структура та обсяг роботи. Магістерська робота складається з анотації на 2 сторінках, вступу, шести розділів, висновків, списку використаних джерел з 40 найменувань, двох додатків, методичної частини та спеціальної частини з охорони праці та безпеки життєдіяльності. Основна частина роботи становить 58 с., серед яких 22 рис., 3 табл.

1 АНАЛІЗ ПРОБЛЕМИ ОБРОБКИ НАБОРІВ ДАНИХ ЩОДО СТАНУ ПОСТ-ІНСУЛЬТНИХ ПАЦІЄНТІВ НА ВІДДАЛЕНІЙ РЕАБІЛІТАЦІЇ

1.1 Обґрунтування вибору технології для захищеної обробки системи обліку пацієнтів

Через використання великого обсягу медичних даних у сфері охорони здоров'я, питання забезпечення конфіденційності та цілісності набуває все більшої актуальності. У 2022 році передбачають особливо великим вплив двох технологій, гомоморфного шифрування та блокчейну на безпеку галузі охорони здоров'я [10].

Зберігання та захист медичної документації вже давно є пріоритетом і проблемою для організацій охорони здоров'я. Технологія блокчейн може полегшити досягнення цієї мети, мінімізуючи шахрайство та пов'язані з ним витрати. Досвід використання цієї технології для захисту медичних даних вже активно накопичується в Естонії та інших країнах [11].

Завдяки технології блокчейн пацієнти можуть отримати доступ до своєї медичної інформації через колективну мережу. Ця технологія забезпечує більшу безпеку та конфіденційність. Крім того, інформація буде розміщена на єдиній надійній платформі, де лікарі та інший медичний персонал зможуть отримати доступ до тих самих даних. Оновлення будуть доступні відразу для всіх, що потенційно змінить догляд за пацієнтами [12].

Отже, блокчейн можна використовувати для вирішення низки галузевих проблем, включаючи сприяння ефективній обробці претензій і платежів, щоб забезпечити надійний і безперешкодний обмін інформацією про медичне обслуговування, а також підтримувати поточні та точні каталоги постачальників. Унікальні властивості блокчейну роблять його придатним для

впровадження у великі мережі для швидкого обміну конфіденційними даними у дозволений, контрольований та прозорий спосіб [13].

1.2 Огляд та аналіз наявних аналогів медичних систем обліку

1.2.1 MedRec

MedRec – це проста, розподілена система для особистого контролю ідентифікації та розподілення персональної інформації [22]. Система MedRec побудована на основі блокчейну Ethereum з використанням смарт-контрактів – скриптів, які дозволяють виконувати більш складні транзакції на блокчейні. Смарт-контракти не є заміною контрактів у традиційному розумінні, це скоріше угоди щодо виконання певної дії чи коду за допомогою набору умови [23].

Перша реалізація MedRec, розроблена Аріелем Екблау та Асафом Азарією, детально описана в білій книзі «Приклад для блокчейна в охороні здоров'я». Це було пілотне впровадження у серпні 2016 року в медичному центрі Beth Israel Deaconess. Ця реалізація формує архітектурну основу для сучасної версії зі значними змінами MedRec 2.0, яка розробляється у MIT (США).

Зокрема, MedRec 2.0 розроблено з використанням Go-ethereum (Geth) і Solidity – на відміну від бібліотек Pyethereum і Serpent, в яких був розроблений оригінал і внесено зміни до обсягу інформації, що зберігається в блокчейні, з метою покращення як масштабування, так і властивості конфіденційності транзакції (рис. 1.1).

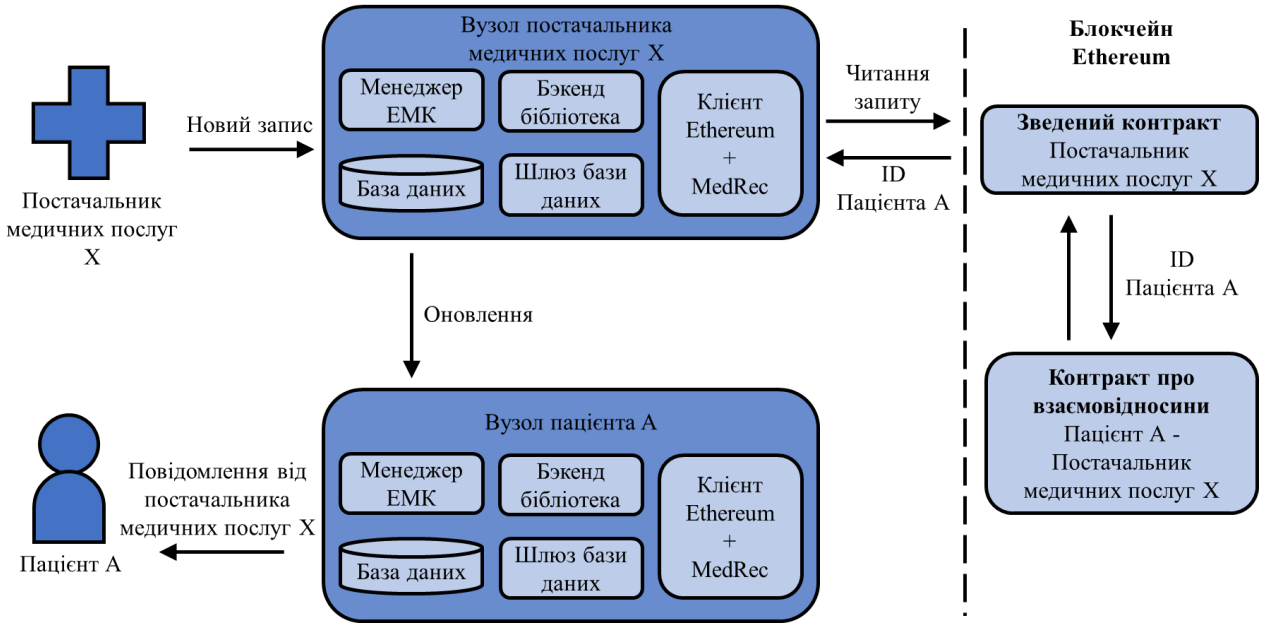


Рис. 1.1. Потоки даних у системі MedRec

MedRec не зберігає ЕМК безпосередньо в блокчейні Ethereum, замість цього використовує реляційний набір смарт-контрактів для кодування покажчиків, які можуть використовуватися для визначення місцезнаходження та аутентифікації для запису місць. MedRec визначає три основні види смарт-контрактів, у рамках яких існують певні відмінності між контрактами, що належать пацієнтам, постачальникам та іншим формам користувачів [24].

Контракт з реєстратором зіставляє ідентифікатори учасників (пацієнтів, постачальників, страховиків) з їх ідентифікаторами адреси в Ethereum (еквівалентно відкритому ключу). Регулювання нових ідентифікаційних даних може бути закодовано в контракті, гарантуючи, що тільки сертифіковані установи можуть додавати нову інформацію в блокчейн. У свою чергу, нова інформація про пацієнта (наприклад, нові стосунки) додається лише зі схвалення цього пацієнта. Кожен рядок ідентифікації знаходиться за адресою в блокчейні, де на неї посилається зведений контракт.

Контракт про взаємовідносини з постачальником пацієнта пов’язує два вузли в системі, де один вузол зберігає та керує медичними записами іншого. Цей зв’язок може існувати між конкретним постачальником послуг і пацієнтом, але поширюється на будь-яку попарну взаємодію з управління даними.

Зведений контракт слугує сполучною ланкою, де кожен учасник системи може знайти резюме своїх стосунків один з одним учасником. Зведений контракт кодує список посилань на контракти про взаємовідносини між пацієнтом і постачальником, вказуючи як поточні, так і попередні взаємодії з іншими вузлами системи. Кожен зв’язок також зберігає змінну «статус», яка вказує, коли зв’язок було встановлено, і чи було воно схвалено пацієнтом. Прийняття, відмова чи видалення стосунків контролюється пацієнтом, надаючи повний контроль над тим, які записи в своїй історії вони хочуть підтвердити.

1.2.2 Guardtime/Gravitate-Healthis

Система Guardtime/Gravitate-Healthis розроблюється у теперішній час в Естонії у числі міжнародних дослідницьких та інноваційних проєктів, що фінансуються Європейською комісією (Horizon 2020). Критичні ланцюги підсистеми спрямовані на боротьбу з незаконними транзакціями та підміною даних шляхом створення цілісної та адаптивної структури, включаючи кінцевих віддалених користувачів (пацієнтів та медичних працівників) в інноваційній трикутній моделі підзвітності.

Ця модель інтегрує базові технології та представляє нову платформу «як послуга» (XaaS), яка має на меті захистити медичну інфраструктуру, що має включені віддалені сегменти амбулаторій та пацієнтів на реабілітації, від несанкціонованого доступу. Мета – реалізувати апаратну схему кібер-фізичної безпеки через семантичне моделювання контекстів безпеки та конфіденційності.

Кінцевим продуктом буде фреймворк Critical-Chains, який працює в хмарі та включає такі основні блоки:

- посилені послуги аутентифікації та авторизації за допомогою безпечних пристроїв IoT на основі апаратного забезпечення та біометричної аутентифікації;
- криптографічний сервер, що забезпечує симетричну криптографію, хешування, генерацію справді випадкових чисел, генерацію простих чисел і ключів;
- система підписання та верифікації, яка створює основні рівні цілісності даних. У проєкті Guardtime займається аналізом вимог і визначенням пріоритетів.

Guardtime пропонує підтримку архітектури щодо інтеграції компонентів блокчейну. Крім того, перевірка цілісності Blockchain-as-a-Service (BCaaS) є одним з пріоритетів, щоб довести життєздатність віддалених сервісів.

Gravitate-Healthis розробляє цифрові медичні інструменти для пацієнтів і медичних працівників, щоб покращити доступ до надійної інформації про ліки, реабілітаційні програми та плани догляду, у т. ч. пацієнтів на віддаленій реабілітації.

Gravitate-Health розробить і випробує інтегроване, цифрове, орієнтоване на користувача інформаційне рішення про здоров’я, яке прагне продемонструвати відчутні покращення доступності та розуміння медичної інформації з набору надійних джерел, починаючи електронної медичної картки (рис. 1.2).

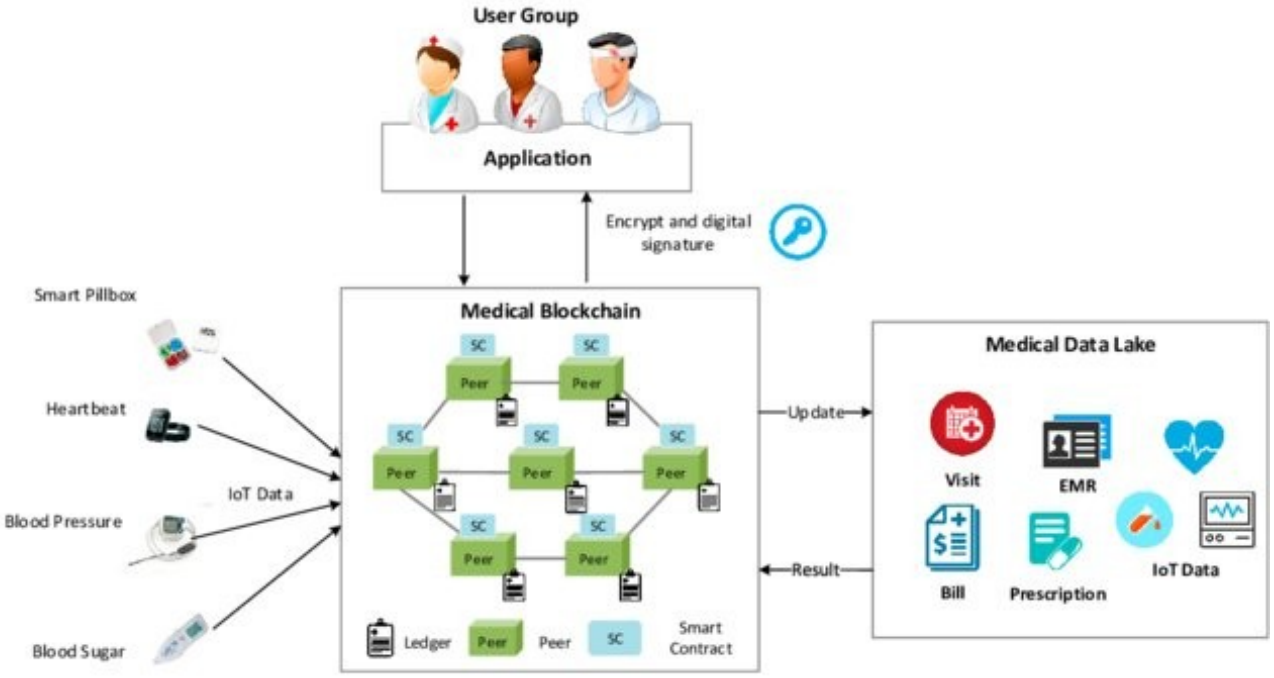


Рис. 1.2. Структура системи Gravitate-Health [31]

Основними результатами стануть цифрова платформа з відкритим вихідним кодом, що підтримує функціональну підтримку G-Lens, і «Біла книга» з рекомендаціями щодо реалістичних стратегій для покращення доступу, розуміння та майбутнього використання цифрових послуг, таких як електронна інформація про продукти (ePI), як інструменту мінімізації ризиків.

Guardtime забезпечить механізм аудиту даних для основних компонентів та джерел інформації Gravitate-Health, що дозволить довести цілісність даних та їх походження.

1.2.3 Medicalchain

Medicalchain використовує технологію блокчейн для створення орієнтованої на користувача електронної медичної картки, зберігаючи при цьому єдину правдиву версію даних користувача [18].

Система Medicalchain використовує механізм подвійного шифрування на закритому блокчейні на основі дозволів. Безпека медичних записів забезпечується за межами будь-якої централізованої системи даних, яка зараз використовується. Дані пацієнтів недоступні безпосередньо в блокчейні [19].

Блокчейн діє як вказівник на те, де дані пацієнта зберігаються в зашифрованому форматі, а це означає, що будь-хто, хто намагається перехопити дані пацієнта, не зможе з легкістю, яка потрібна для доступу до даних, існуючих у будь-якому центральному місці.

Перший блокчейн контролює доступ до медичних записів і створений за допомогою Hyperledger Fabric. Другий блокчейн працює на основі токена ERC20 на Ethereum і лежить в основі всіх застосунків і сервісів для обраної платформи [20].

Мережа блокчейн Hyperledger базується на дозволах і вимагає від користувачів зареєструватися, щоб використовувати її. Дозволи в мережі контролюються за допомогою мов моделювання Hyperledger і керування доступом. Hyperledger Fabric – це платформа для рішень розподіленого реєстру, що базується на модульній архітектурі, що забезпечує високий рівень конфіденційності, стійкості, гнучкості та масштабованості.

Медична інформація часто є приватною, тому закритий блокчейн, такий як Hyperledger Fabric, допомагає зберегти конфіденційність, необхідну для медичної системи. Hyperledger Fabric є кращим рішенням для керування доступом до медичних записів, оскільки він підтримує кілька рівнів дозволів, тобто власник набору даних може контролювати, до яких частин його даних можна отримати доступ [21].

Рис. 1.3. Структура системи Medicalchain із використанням закритого блокчейну Hyperledger Fabric

Ethereum – це цифрова платформа, на якій тисячі потужних комп'ютерів по всьому світу гармонійно працюють для розміщення мережі Ethereum. Блокчейн Ethereum представляє всі облікові записи та транзакції, здійснювані його користувачами. Смарт-контракти – це код, який зберігається та виконується на блокчейні Ethereum. Процеси, які зазвичай вимагають професіонала або нотаріуса, можуть бути автоматизовані та підтверджені смарт-контрактом повністю прозорим і безпечним способом.

Використовуючи технологію блокчейн, смарт-контракти та нашу криптовалюту, Medicalchain надає інфраструктуру для створення цифрових медичних програм і послуг. Ці програми та послуги будуть безперешкодно працювати на основі даних про здоров'я користувачів.

Шахрайство з ідентифікаційними даними є масовою проблемою у світі. Хакери крадуть особисті дані та видають себе за користувачів, щоб понести

величезні витрати як для користувачів, так і для бізнесу. Щоб боротися з шахрайством, Medicalchain співпрацює з Civic і використовуватиме послуги аутентифікації користувачів Civic для легкого та безпечного керування ідентифікаторами користувачів децентралізованим способом. Civic ідентифікує та перевіряє користувачів за допомогою біометричних даних, що забезпечує простий і безпечний спосіб забезпечення конфіденційності користувачів.

1.3 Постановка задачі

Доцільно розробити додаткове програмне забезпечення для взаємодії пацієнта та постачальника послуг з обліковими даними пацієнта на основі метаданих, що зберігаються у блокчейні Ethereum.

Публічна платформа Ethereum, що обрана для використання в роботі, має доведену надійну репутацію для створення децентралізованих онлайн-сервісів на базі блокчейну. Платформа Ethereum пристосована для зберігання інформації щодо факту надання доступу до інформації пацієнта.

Доступ до інформації пацієнта доцільно надавати через смарт-контракт між пацієнтом та сертифікованим постачальником медичних послуг.

Висновки до розділу 1

Аналіз існуючих сервісів-аналогів для контролю ідентифікації та розподілення персональної медичної інформації, розроблених у інших країнах світу, підтвердив стрімке впровадження діджиталізації в облік даних про пацієнтів.

Зважаючи, що такі пацієнти, як пост-інсультні, потребують дуже довготривалого супроводження під час реабілітації та надання медичних послуг віддаленим шляхом, актуальним є захист безперервно зростаючого обсягу інформації про пост-інсультних пацієнтів у медичних базах від

несанкціонованого доступу, незаконного поширення та спотворення даних про пацієнтів.

Використання технології блокчейн для захисту наборів даних щодо стану пост-інсультних пацієнтів на віддаленій реабілітації дозволяє:

- забезпечити цілісність даних у медичних базах, що зберігаються централізовано;
- значно знизити можливість підробки транзакцій;
- зберігати повну копію медичного реєстру на багатьох комп'ютерах одночасно.

Серед невирішених задач медичної галузі є організація віддаленої взаємодії пацієнта та постачальника послуг з обліковими даними пацієнта. Тому у магістерській роботі передбачено розробити додаткове програмне забезпечення зазначеної тематики на основі метаданих, що зберігаються у блокчейні Ethereum.

2 МАТЕМАТИЧНІ МОДЕЛІ, МЕТОДИ, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ДЛЯ МЕДИЧНОЇ СИСТЕМИ НА ОСНОВІ БЛОКЧЕЙНУ

2.1 Технологія блокчейну та смарт-контракти

Блокчейн – це розподілена цифрова база даних, яка підтримується та синхронізується за допомогою криптографічного алгоритму та зберігається на кількох вузлах (тих комп'ютерах, які зберігають копію бази даних). Блокчейни можна розглядати як однорангову мережу, де кожен вузол сам по собі зберігає, верифікує та поширює повну або часткову копію даних.

Блокчейн представляють як нову технологію для зберігання даних, так і нову програмовану платформу, яка дозволяє створювати нові застосунки, такі як смарт-контракти. Важливо відзначити, що блокчейн-екосистема багатошарова (рис. 2.1).

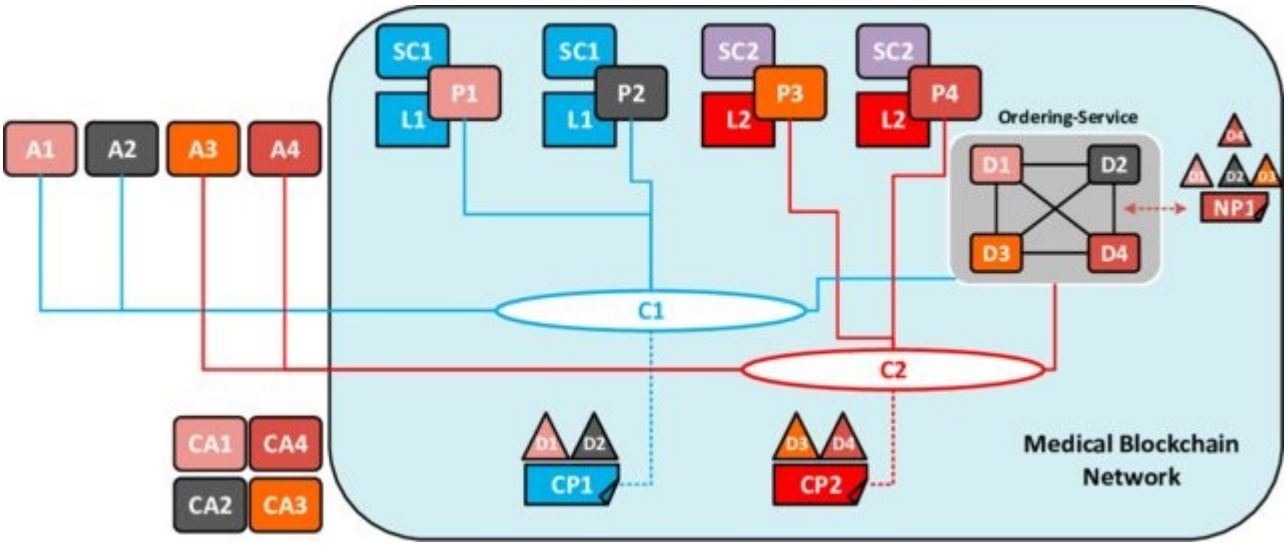


Рис. 2.1. Зразок топології медичної мережі блокчейн [31]

На рис. 2.1 представлено зразок топології багатошарової мережі для медичного блокчейну.

Топологія мережі включає чотири відділи: неврологічне відділення (для стаціонарного лікування інсультних хворих), реабілітаційне відділення (для стаціонарного лікування пост-інсультних хворих), сімейна амбулаторія (для амбулаторного лікування пост-інсультних хворих) і безпосередньо пост-інсультні хворі на віддаленій реабілітації (представлено як D1, D2, D3 і D4) у двох каналах телекомунікаційного зв’язку. Ці чотири відділи мають спільну політику мережі, яка полягає у тому, що вони створюють та ініціалізують блокчейн мережі. Стаціонарні відділення D1 і D2 здійснюють приватне спілкування в каналі C1, що керується відповідно до правил політики CP1, а також D3 і D4.

Канал C1 знаходиться під контролем однорангового партнера P1 і однорангового партнера P2, де діє смарт-контракт SC1, розміщений у книзі L1. Аналогічно, канал C2 регулюється політикою каналу CP2 для учасників протоколу D3 і D4. Каналом C2 керують одноранговий партнер P3 і одноранговий партнер P4, за правилами смарт-контракту SC2, розміщеного у книзі L2.

Служба замовлень виконує роль менеджера однорангового мережі та може дозволити іншим користувачам приєднатися до певного каналу. Вона також підтримує зв'язок з каналами C1 і C2, щоб упорядкувати транзакції по блоках на канал.

Клієнтські програми A1, A2 можуть використовувати канал C1 для підключення до інших мережевих об’єктів, тоді як A3, A4 можуть зробити це через канал C2. Кожен із відділів пов’язаний з постійним центром сертифікації (CA), наприклад, клієнтська програма A1, що належить відділу D1, видається центром сертифікації CA1. CA видає сертифікати на основі інфраструктури відкритих ключів (PKI) відділам-членам мережі та їх користувачам.

Доцільність застосування технології блокчейн для обліку медичних даних підтверджується, по-перше, тим, що самі блокчейни покладаються на Інтернет і протокол TCP/IP, і в цьому відношенні їх можна розглядати як нові протоколи застосунків, які знаходяться на цьому транспортному рівні. По-друге, на застосунок до інфраструктури управління даними, блокчейни також забезпечують програмовану платформу, на якій можуть бути закріплені різні інші програми. З цієї причини сам блокчейн також служить основою, на якій працюють децентралізовані програми, такі як смарт-контракти.

Термін «смарт-контракт» бере свій початок з 1996 року, коли Нік Сабо визначив його як набір цифрових умов, включаючи протоколи, за якими сторони дотримуються їх, і можуть бути реалізовані без залучення посередників. Він мав на меті розробити комп’ютерне програмне забезпечення, яке нагадує договірні положення і водночас здатне зв’язати сторони разом таким чином, що будь-якій зі сторін було б важко в односторонньому порядку розірвати угоду. І хоча багатьох зацікавила ідея створення контрактів, які могли б читати та використовувати як люди, так і машини, смарт-контракти не було реалізовано технічно. Лише з розвитком технології блокчейн в останні роки цей термін відродився [14].

Таким чином, блокчейн дає змогу реалізувати контракт, яким може повністю керувати комп’ютер та реалізовувати без залучення посередників. Як програми другого рівня (закріплені у відповідному блокчейні), смарт-контракти отримують захищеності від несанкціонованого доступу, яку реалізує базова інфраструктура блокчейну. Це означає, що їх виконання не може бути зупинено окремими особами або групами, якщо це спеціально не вбудовано в код. Враховуючи, що кілька вузлів блокчейну виконують код смарт-контракту, він не контролюється і не може бути зупинений однією стороною.

Після того, як було опубліковано ідею смарт-контракту понад двадцять років тому Ethereum знову підхопили цю ідею [15, 16]. Блокчейн Ethereum розглядає смарт-контракти як «криптографічні коробки», які містять цінність і розблокують її лише при виконанні певних умов». Відповідно до цієї точки зору, смарт-контракти – це програми, що виконуються комп'ютерами, які беруть участь у мережі блокчейну та запускають транзакцію, коли виникають раніше визначені умови.

Отже, «смарт-контракт» – це програмний код, який працює на блокчейні та обробляє інформацію про цифрові активи або представлення фізичних об'єктів чи права на них на основі інших (зовнішніх) даних, які ще не були відомі на момент програмування коду, перепризначених між двома або більше сторонами у формі правочинів.

Смарт-контракт, побудований на технології блокчейн, має загалом чотири життєві цикли: створення, заморожування, виконання та завершення [17].

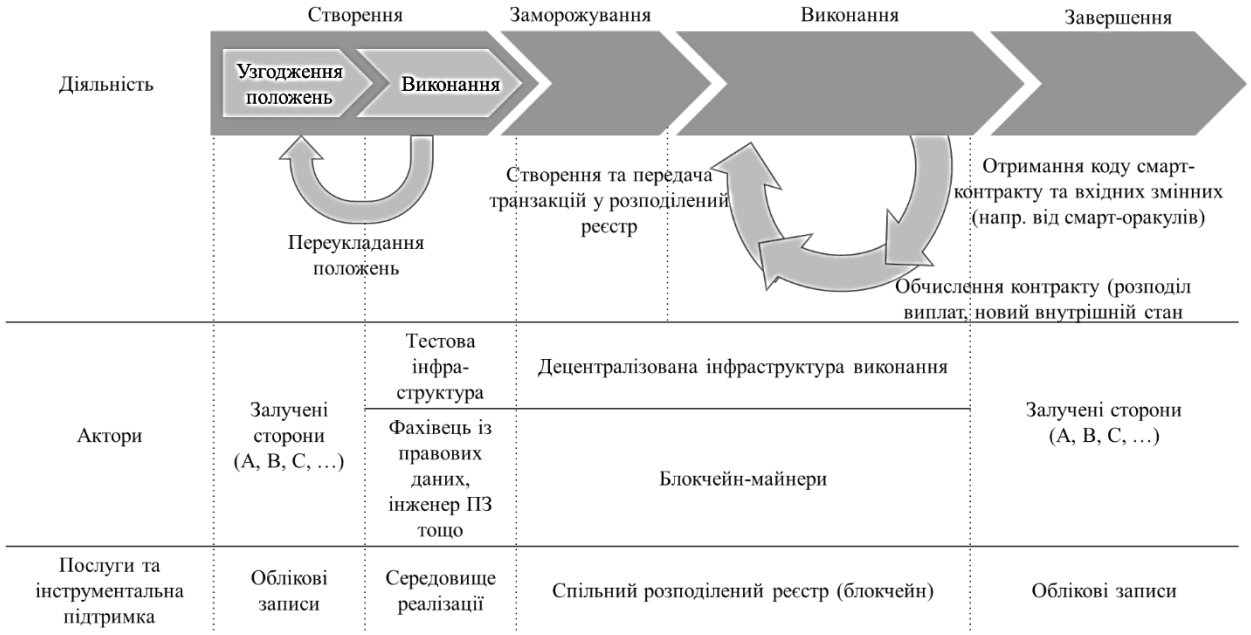


Рис. 2.1. Життєвий цикл смарт-контракту

Під час фази створення смарт-контракт визначається і перетворюється на код. Потім програмне забезпечення заморожується, поки воно додається до ланцюжка за допомогою відповідного процесу консенсусу, перш ніж воно буде виконано, тобто зчитується та реалізується різними вузлами. Нарешті, смарт-контракт завершується збереженням нової інформації про стан і транзакцій у блокчейні та підтвердженням їх відповідно до протоколу консенсусу.

2.2 Механізм створення смарт-контракту між сторонами

Для створення системи буде використано смарт-контракти на блокчейні Ethereum для створення представлень наявних медичних записів, які зберігаються в мережі в окремих вузлах. Контракти містять метадані власності на записи, дозволи та цілісність даних. Транзакції блокчейну системи містять криптографічно підписані інструкції для керування цими властивостями. Перехідні функції контракту здійснюють політику лише шляхом законних транзакцій, що забезпечують чергування даних.

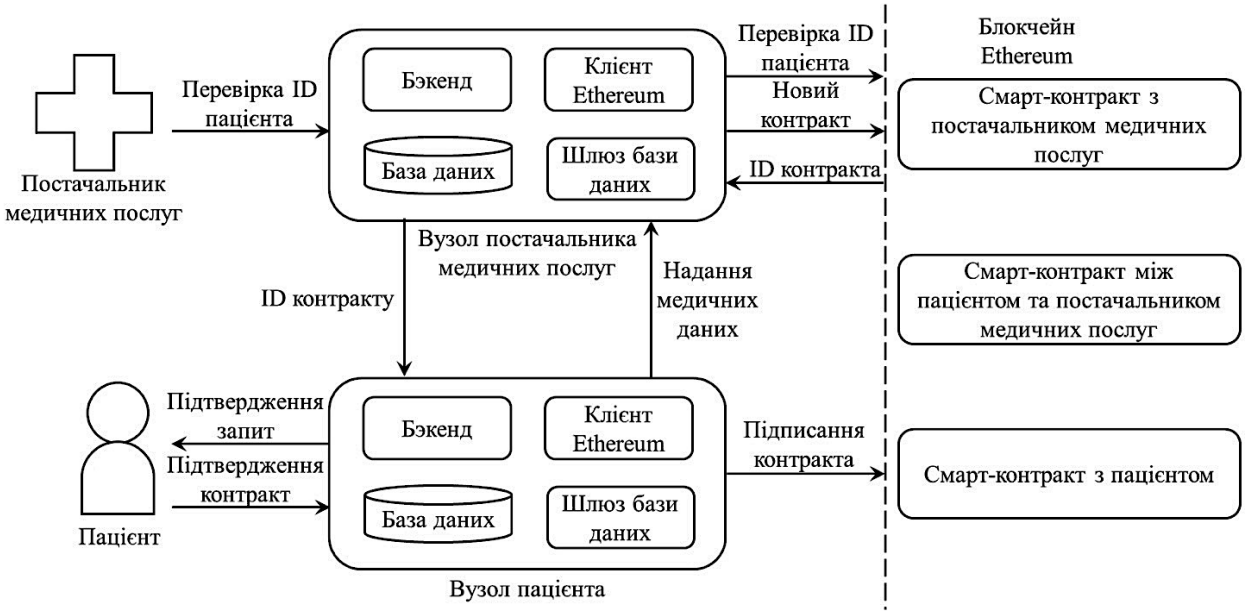


Рис. 2.2. Діаграма створення смарт-контракту між сторонами

Ці правила можуть бути структуровані так, щоб забезпечити виконання будь-якого набору правил, що регулюють конкретну медичну карту. Наприклад, може бути передбачено надсилання окремих транзакцій згоди як пацієнтів, так і медичних працівників, перш ніж надавати третій стороні дозвіл на перегляд. Смарт-контракти можна використовувати для різних медичних робочих процесів, а також для керування дозволом на доступ до даних між різними організаціями в екосистемі охорони здоров'я.

Смарт-контракт може мати всі умови: від керування різними дозволами до доступу до даних для зацікавлених сторін. Це допоможе покращити взаємодію між лікарями та пацієнтами. Правила авторизації даних вбудовані в такі смарт-контракти. Вони також можуть допомогти відстежувати всі дії з унікальним ідентифікатором – від їх походження до здачі. Не буде необхідності мати централізований орган для управління та схвалення операції, оскільки нею можна безпосередньо керувати за допомогою смарт-контракту, що значно зменшить адміністративні витрати на управління процесом. Усі дані медичної картки зберігаються в локальному сховищі бази даних для підтримки продуктивності та економічної життєздатності, а хеш даних є елементом даних блоку, переданого в ланцюжок (рис. 2.3).

Транзакції даних підписуються закритим ключем власника (пацієнта або лікаря). Блоковий вміст для системи являє собою право власності на дані та права перегляду, якими користуються учасники одноранговой приватної мережі. Технологія блокчейн підтримує використання смарт-контрактів, які дозволяють нам автоматизувати та відстежувати певні переходи стану (наприклад, зміна прав перегляду або створення нового системного запису).

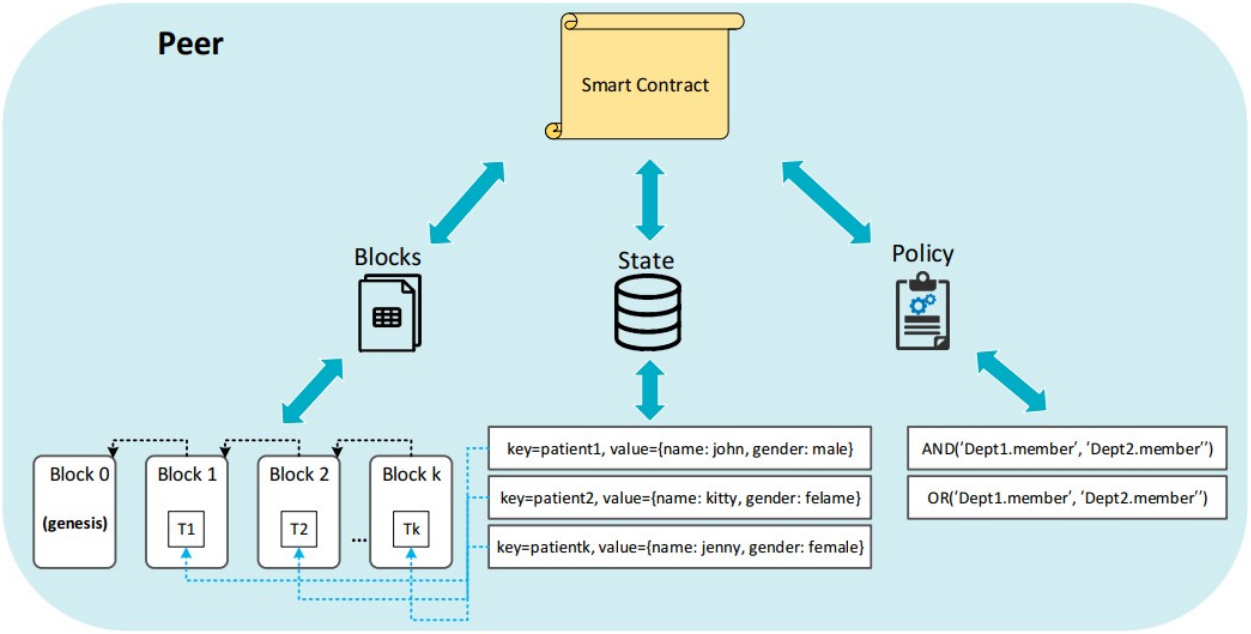


Рис. 2.3. Внутрішня структура смарт-контракту на платформі медичного блокчейну [31]

Відносини між пацієнтом і постачальником медичних послуг будуть реєструватись за допомогою смарт-контрактів на блокчейні Ethereum, які пов'язують медичну карту з дозволами на перегляд та інструкціями щодо отримання даних (по суті, вказівниками інформації) для виконання зовнішнього сервера. Щоб захистити дані від підробок, включається криптографічний хеш запису в блокчейні, що забезпечує цілісність.

Постачальники медичних послуг можуть додати новий запис, пов'язаний з конкретним пацієнтом, а пацієнти можуть дозволити обмін записами між постачальниками. Сторона, яка отримує нову інформацію, отримує автоматичне повідомлення в обох випадках і може перевірити запропонований запис до того, як дані будуть прийняті або відхилені. Завдяки цьому учасники будуть інформованими та зацікавленими в розвитку їхніх записів.

Така система надає перевагу зручності використання, також пропонуючи призначений контракт, який об’єднує посилання на всі відносини користувача та постачальника, таким чином забезпечуючи єдину точку відліку для перевірки будь-яких оновлень історії хвороби. Буде використано криптографію з відкритим ключем для керування перевіркою ідентичності та реалізацію, яка зіставляє прийняту форму ідентифікатора, наприклад ім’я чи номер соціального страхування, на адресу користувача Ethereum. Після перенаправлення блокчейну на підтвердження дозволів через сервер аутентифікації бази даних, алгоритм синхронізації обробляє обмін даними між базою даних пацієнтів і базою даних постачальника медичних послуг.

2.3 Дерева Меркла та їх альтернативи

Вузли в блокчейн-мережі анонімні та працюють в умовах відсутності довіри. Для оцінки коректності транзакцій кожного блоку знадобиться велика кількість часу та обчислювальних ресурсів. Спростити цей процес допомагають дерева Меркла.

Блоки в блокчейні – це файли, які містять інформацію про транзакції проведені користувачами. Додатково кожен блок містить Generation Transaction – транзакція з інформацією про адресу з нагородою за рішення блоку, яка завжди стоїть першою у списку.

Усі транзакції у блоці представлені як рядки у шістнадцятковому форматі (raw transaction format), які хешуються для отримання ідентифікаторів транзакцій (txid). На основі будується хеш блоку, який враховується наступним блоком, забезпечуючи незмінність і зв'язність реєстру. Єдине хеш-значення блоку збирається за допомогою дерева Меркла, концепція якого була запатентована Ральф Меркло (Ralph Charles Merkle) в 1979 році.

Дерево Меркла (або хеш-дерево) – це двійкове дерево, кінцеві вузли якого – це хеші транзакцій, а внутрішні вершини – результати складання значень пов'язаних вершин [27]. Приклад хеш-дерева з трьома транзакціями-листами наведено на рис. 2.4.

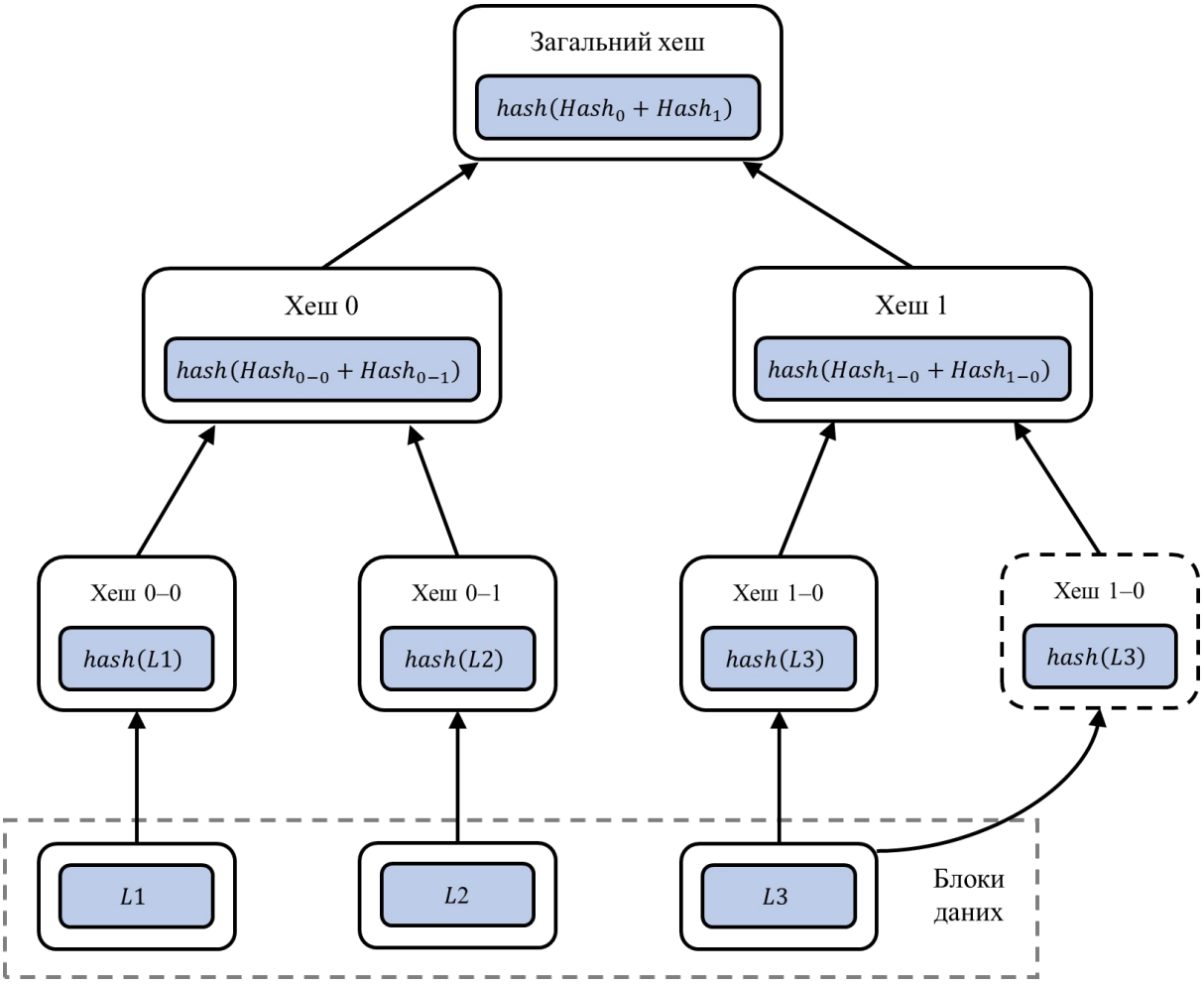


Рис. 2.4. Хеш-дерево з трьома транзакціями-листами

Дерево Меркла підсумовує всі транзакції в блоці і генерує цифровий відбиток всього набору операцій, що дозволяє користувачеві перевірити, чи містить воно транзакцію в блоці.

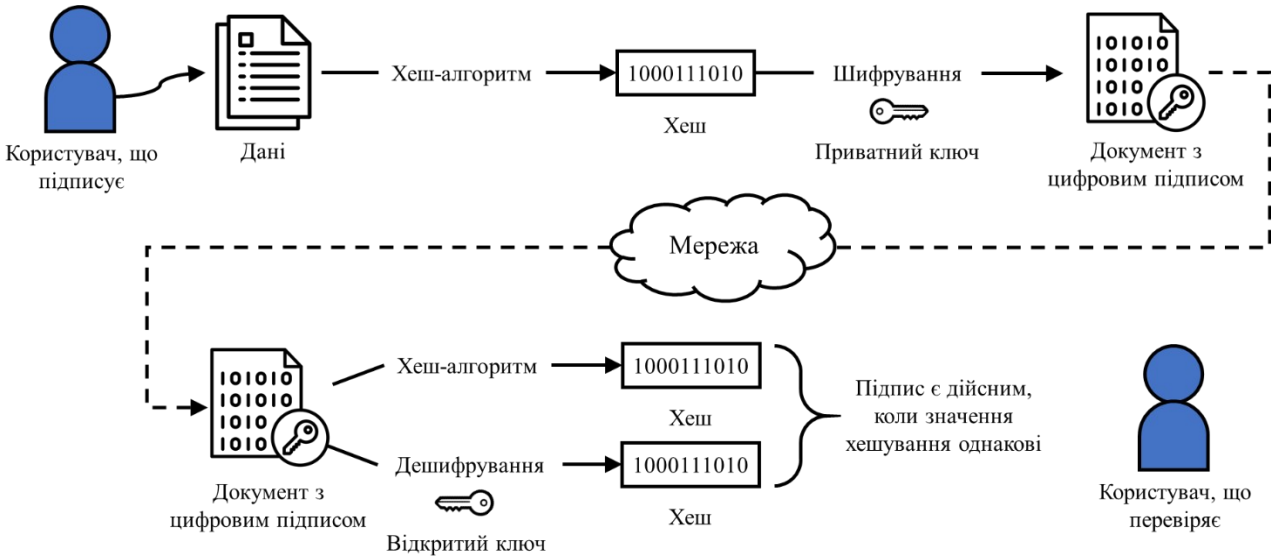


Рис. 2.5. Алгоритм роботи дерева Меркла у блокчейні

Дерева Меркла створюються шляхом багаторазового хешування пар вузлів, поки не залишиться лише один хеш. Цей хеш відомий як корінь Меркла або кореневий хеш. Такі дерева будуються знизу, використовуючи ідентифікатори транзакцій, які є хешами окремих транзакцій. Кожен нелістовий вузол є хешем свого попереднього хеша, а кожен листовий вузол є хешем транзакційних даних [28].

Алгоритм побудови дерева Меркла у блокчейні (рис. 2.4):

1) L1, L2 та L3 – це три транзакції, які виконуються в одному блоці. Кожна транзакція хешується, утворюючи hash(L1), hash(L2) та hash(L3).

2) Далі хеші об’єднуються разом, в результаті чого отримуємо hash(hash(L1) + hash(L2)) та hash(hash(L3) + hash(L3)). Оскільки дерево Меркла є бінарним, число елементів кожної ітерації має бути парним. Тому, якщо блок містить непарну кількість транзакцій, то остання дублюється і складається сама з собою.

3) Процес об’єднання повторюється стільки разів, доки не буде отримано єдиний хеш, а саме корінь дерева Меркла. Він є криптографічним доказом цілісності блоку (тобто те, що всі транзакції перебувають у заявленому порядку). Значення кореня фіксується у заголовку блоку.

Дерева Меркла у блокчейні мають чотири значущі переваги:

- перевірка цілісності даних: його можна використовувати для ефективної перевірки цілісності даних;
- займає мало дискового простору: у порівнянні з іншими структурами даних дерево Меркла займає дуже мало місця на диску;
- своєчасне інформування по мережах: дерева Меркла можна розбити на невеликі фрагменти даних для перевірки;
- ефективна перевірка: формат даних ефективний, і перевірка цілісності даних займає лише кілька хвилин.

У блокчейні дерева Меркла будуються за допомогою подвійного хешування SHA-256. Ось приклад хешування рядка hello:

Перший раунд SHA-256:

2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824

Другий раунд:

9595c9df90075148eb06860365df33584b75bff782a510c6cd4883a419833d50

Двійкові дерева Меркла добре підходять для верифікації послідовності елементів, тому справляються із завданням збереження структури транзакцій. Однак вони обмежують можливості легких клієнтів, які не отримують інформації про стан системи. Наприклад, дізнатися, яка кількість монет є за вказаною адресою, неможливо.

Для обходу обмеження дослідники та розробники модернізують вже існуючі алгоритми та розробляють нові. У блокчейн-платформі Ethereum

використовується так зване префіксне дерево Меркла (Trie). Це структура даних, що зберігає асоціативний масив із ключами [29].

На відміну від бінарних дерев Меркла, ключ, що ідентифікує конкретний вузол дерева, є динамічним. Його значення визначається місцем розташування на дереві і формується шляхом з'єднання символів, привласнених ребрам графа, що проходять від кореня до заданого вузла.

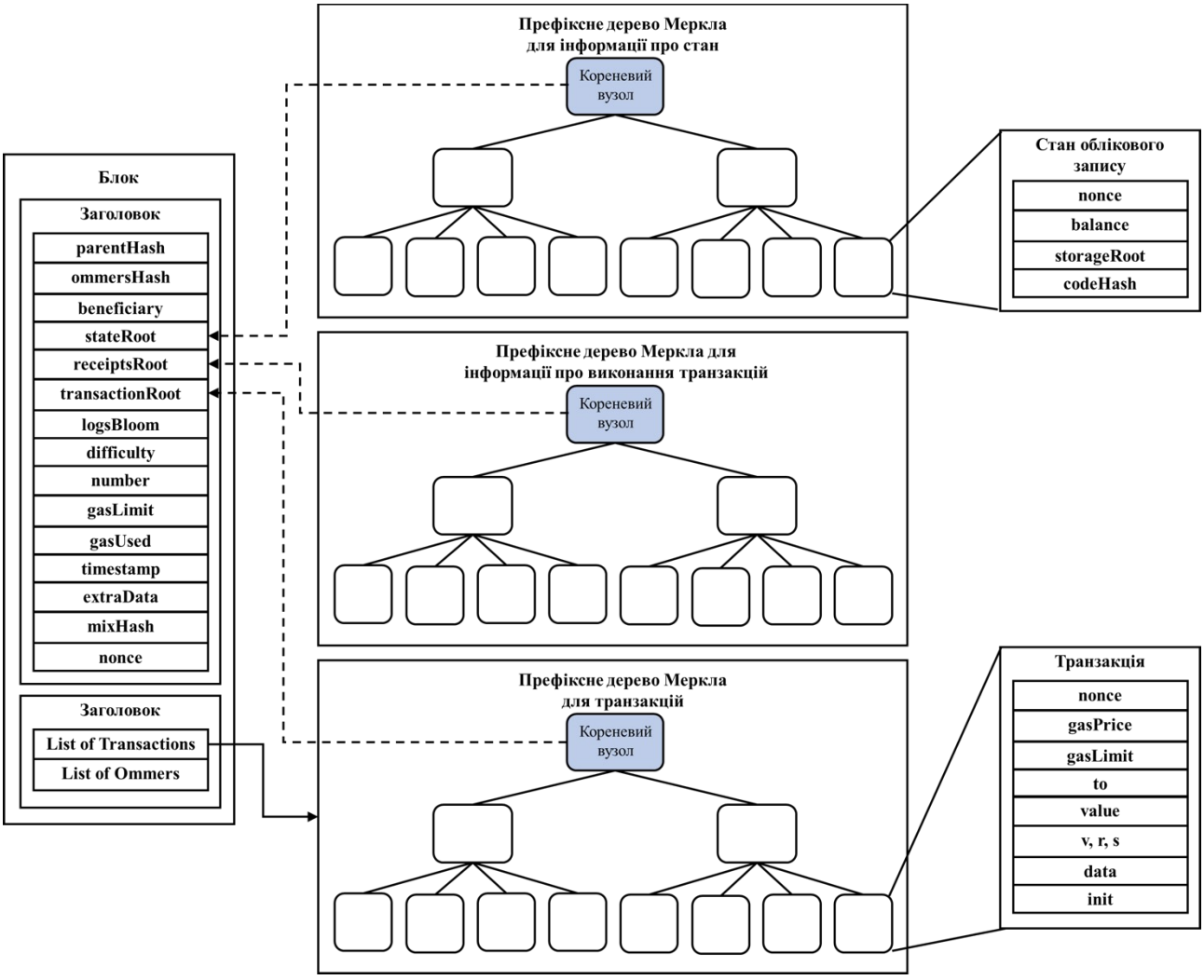


Рис. 2.6. Структура префіксного дерева Меркла у блокчейн-проєкті Ethereum

В Ethereum заголовок блоку містить відразу три префіксних дерева Меркла: для транзакцій, інформації про їх виконання та стан (рис. 2.6). Такий

підхід дозволяє клієнтам отримувати від системи відповіді на запитання: «Чи є транзакція у вказаному блоці?», «Скільки монет на рахунку?» та «Яким буде стан системи після виконання цієї транзакції?».

Префіксне дерево Меркла для інформації про стан – це зіставлення між адресами та станами облікового запису. Його можна розглядати як глобальний стан, який постійно оновлюється виконанням транзакцій. Мережа Ethereum – це децентралізований комп'ютер, і стан спроби вважається жорстким диском. Вся інформація про облікові записи зберігається в дереві, і її можна отримати, зробивши запит.

Префіксне дерево Меркла для транзакцій записує транзакції в Ethereum. Транзакції відіграють основну роль у зміні станів, оскільки Ethereum – це «стан» на основі транзакцій. Після запису транзакції в блоці її неможливо змінити, щоб підтвердити баланс рахунків (стан). Оскільки транзакційне дерево створено за допомогою модифікованого дерева Меркла, єдиний кореневий вузол зберігається в блоці

Префіксне дерево Меркла для інформації про виконання транзакцій записує надходження (результати) транзакцій. Квитанція є результатом транзакції, яка успішно виконана. Квитанція містить хеш транзакції, номер блоку, кількість використаного газу та адресу контракту тощо.

Іншою альтернативою класичним деревам Меркла виступає метод комбінування хеш-значень HashFusion, запропонований Hewlett Packard Labs. Як зазначають у компанії, новий підхід дозволяє розраховувати значення хешів поетапно. Компоненти хешу обчислюються відразу, як дані стають доступні, та був об'єднуються друг з одним за необхідності [30].

HashFusion передбачає побудову елементів хешу з допомогою бінарної функції об'єднання (рис. 2.7). Вона є асоціативною та некомутативною, тому її

можна використовувати для об'єднання хешей у момент формування. Це дозволяє зменшити обсяги пам'яті, необхідних їх зберігання.

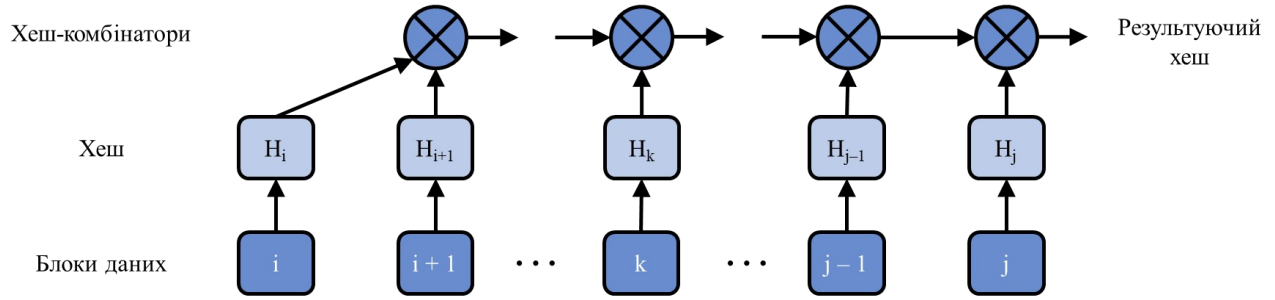


Рис. 2.7. Об’єднання суміжних блоків хешів
за допомогою бінарної функції об'єднання

Робота бінарної функції будується так: вона приймає на вхід значення хешей (генерованих класичними хешуючими функціями) і конвертує в матриці цілих чисел. Після чого матриці перемножуються, а результат перетворюється назад на байтовий масив фіксованої довжини. HashFusion реалізує більш гнучкі структури порівняно з деревами Меркла, які дозволяють оновлювати існуючі хеші та вибірково видаляти/вставляти нові значення.

2.4 Інформаційні технології для медичної системи на основі блокчейну

Як і всі ініціативи цифрових технологій, блокчейн – це не тільки програмне забезпечення. Це також апаратне забезпечення. Щоб належним чином запустити систему, що засновану на блокчейні, необхідно надати апаратні ресурси для підтримки цього проєкту (табл. 2.1 – 2.2).

Таблиця 2.1

Апаратне забезпечення та середовище розробки медичної блокчейн-мережі

Компоненти	Характеристики
Процесор	Intel Core i5-8500 @ 3.00 GHz
Оперативна пам’ять	8 Гбайт
Операційна система	Ubuntu Linux 18.04.1 LTS
Docker Engine	Version 18.06.1-ce
Docker-Compose	Version 1.13.0
Node	v8.11.4
Python	v2.7.15
Hyperledger Fabric	v1.2
IDE	Remix, VS Code
CLI Tool	composer-playgroundcomposer-cli, composer-rest-server, geth

Таблиця 2.2

Апаратне забезпечення та середовище розробки вебзастосунку доступу до медичної блокчейн-мережі

Компоненти	Характеристики
Операційна система	Windows 10 Pro 64 bit
IDE	VS Code
Browser	Firefox, Google Chrome
Library and Framework	React
Programming Language	HTML, CSS, JavaScript

Висновки до розділу 2

У світі спостерігається тенденція використання для захисту цифрових медичних карт технології блокчейн (сервіси MedRec ц США, Medicalchain у Великобританії, Guardtime в Естонії, тощо). Використання блокчейну може вивести облік медичних послуг на новий рівень, забезпечивши своєчасне оновлення даних і гарантію доступу тільки авторизованих лікарів. Технологія блокчейн використовується для запису транзакцій. А вони у свою чергу згруповані у блоки, та кожен наступний блок містить контрольну суму попереднього блоку. Такий підхід забезпечує цілісність реєстру та значно знижує можливість підробки транзакцій. При цьому, повна копія реєстру зберігається на багатьох комп'ютерах одночасно.

Блокчейн можна використовувати для вирішення низки галузевих проблем, включаючи сприяння ефективній обробці претензій і платежів, щоб забезпечити надійний і безперешкодний обмін інформацією про медичне обслуговування, а також підтримувати поточні та точні каталоги постачальників. Унікальні властивості блокчейну роблять його придатним для впровадження у великі мережі для швидкого обміну конфіденційними даними у дозволений, контрольований та прозорий спосіб.

Отже, було вирішено використовувати в роботі публічну платформу Ethereum для створення децентралізованих онлайн-сервісів на базі блокчейну; вона застосована для зберігання інформації щодо факту надання доступу до інформації пацієнта. Зазначений доступ надається через смарт-контракт між пацієнтом та сертифікованим постачальником медичних послуг. Для зберігання облікових даних пацієнта буде створено систему на основі технології IPFS для розподіленого зберігання інформації з додатковим шифруванням для забезпечення контролю доступу до облікових даних.

3 МОДЕЛЮВАННЯ ТА ДОСЛІДЖЕННЯ ОТРИМАНИХ РЕЗУЛЬТАТІВ

3.1 Приватна блокчейн мережа

Система розроблена як додаток до блокчейну Ethereum, але такий підхід має переваги та недоліки. Хоча технологія блокчейн загалом на сьогодні є експериментальною, саме Ethereum є найбільш стабільним та повнофункціональним блокчейном. Але публічна мережа також містить кілька недоліків, а саме:

- високу ціну комісії за транзакцію;
- високу волотильність цінності основного токену платформи

Для вирішення цих недоліків оптимальним рішенням буде провести запуск приватної мережі, повністю ідентичної платформі Ethereum. Також вирішено провести налаштування деяких параметрів для запобігання зайвих витрат з боку пацієнтів. Таке рішення також дозволить у майбутньому у разі необхідності клонувати систему на публічний блокчейн Ethereum. Також для приватного блокчейну бажано замінити алгоритм консесусу мережі та використовувати Proof-of-Authority замість Proof-of-Work. Це дозволить зменшити витрати на обчислювальне обладнання.

Для запуску приватної мережі необхідно створити першій блок у блокчейні (так званий Генезис блок). У цьому блоці вказані деякій налаштування мережі основним з яких є час створення нових у блоків у мережі (У нашому випадку 2 секунди). Для підключення вузлів мережі між собою необхідно розгорнути стартовий вузол (bootnode) у мережі інтернет. Через якій нові вузли мережі можуть знайти один одного у мережі інтернет (peer discovery). Для цього використано інструменти що входить до пакету програмного забезпечення Go-Ethereum. Для забезпечення відмово стійкості та

децентралізації таких вузлів має буті декілька та вони мають фізично знаходитись у різних місцях. Використовуючи той же набір інструментів створено конфігураційні файли які необідні для запуску вузлів мережи.

Для моніторингу мережі була розгорнута програма Ethstats, що містить у собі вебзастосунок, у якому відображаються підключені вузли та інші деталі щодо поточного стану мережі.

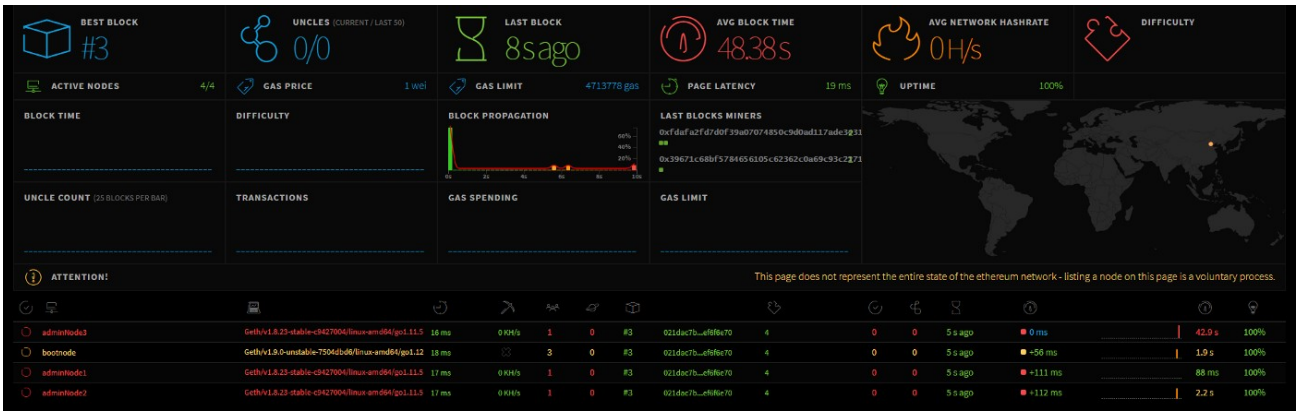


Рис. 3.1. Скріншот програми Ethstats для моніторингу активних вузлів мережі

Запущена приватна мережа є повною копією блокчейн платформи Ethereum, оскільки фактично використовує ті ж самі програми, але налаштовані для роботи в рамках окремої мережі замість підключення до основної платформи.

3.2 Смарт-контракти

Блокчейн-мережа Ethereum має деякі обмеження щодо смарт-контрактів а саме розмір байт-коду (скомпільованого смарт-контракту) не має перевищувати 24 кбайт. Тому для забезпечення можливості розширення функцій система складається з 3 смарт-контрактів:

1) смарт-контракт пацієнта – реалізує зберігання та керування даними пацієнта, існує в єдиному екземплярі для пацієнта;

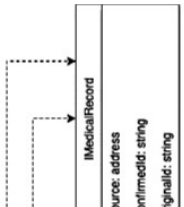
2) смарт-контракт надавача медичних послуг (лікаря або медичного приладу) – реалізує керування даними щодо надавача послуг, існує в єдиному екземплярі для надавача медичних послуг;

3) смарт-контракт відносин (між пацієнтом та надавачем медичних послуг) – має бути погоджений між сторонами та надає доступ до створення або зчитування медичних облікових даних пацієнта. Після створення не може буті змінений, але може бути розірваним.

На рис. 3.2 наведено смарт-контракти та використовувані структури даних у вигляді UML-диграми класів.

3.3 Створення смарт-контракту між сторонами

Створення нового договору (смарт-контракту) між пацієнтом та надавачем медичних послуг. Пацієнту та надавачу необхідно сканувати QR-код відповідної сторони, застосунок з боку надавача медичних послуг заповнює дані у смарт-контракт створює та підписує транзакцію для завантаження смарт-контракту у блокчейн мережу. Після чого через QR-код транзакція передається у застосунок пацієнта. Пацієнт перевіряє усі дані та підтверджує створення смарт-контракту підписуючи транзакцію своїм криптографічним ключем. При цьому застосунок пацієнта верифікує байт-код смарт-контракту для якого завчасно створено криптографічнім підписом розробника смарт-контракту, а ключі для верифікації вбудовані у застосунки для обох сторін. Такий механізм забезпечує захист сторін від можливої атаки через модифікацію байт-коду смарт-контракту однією із сторін. UML-діаграма цього процесу наведена на рис. 3.3.



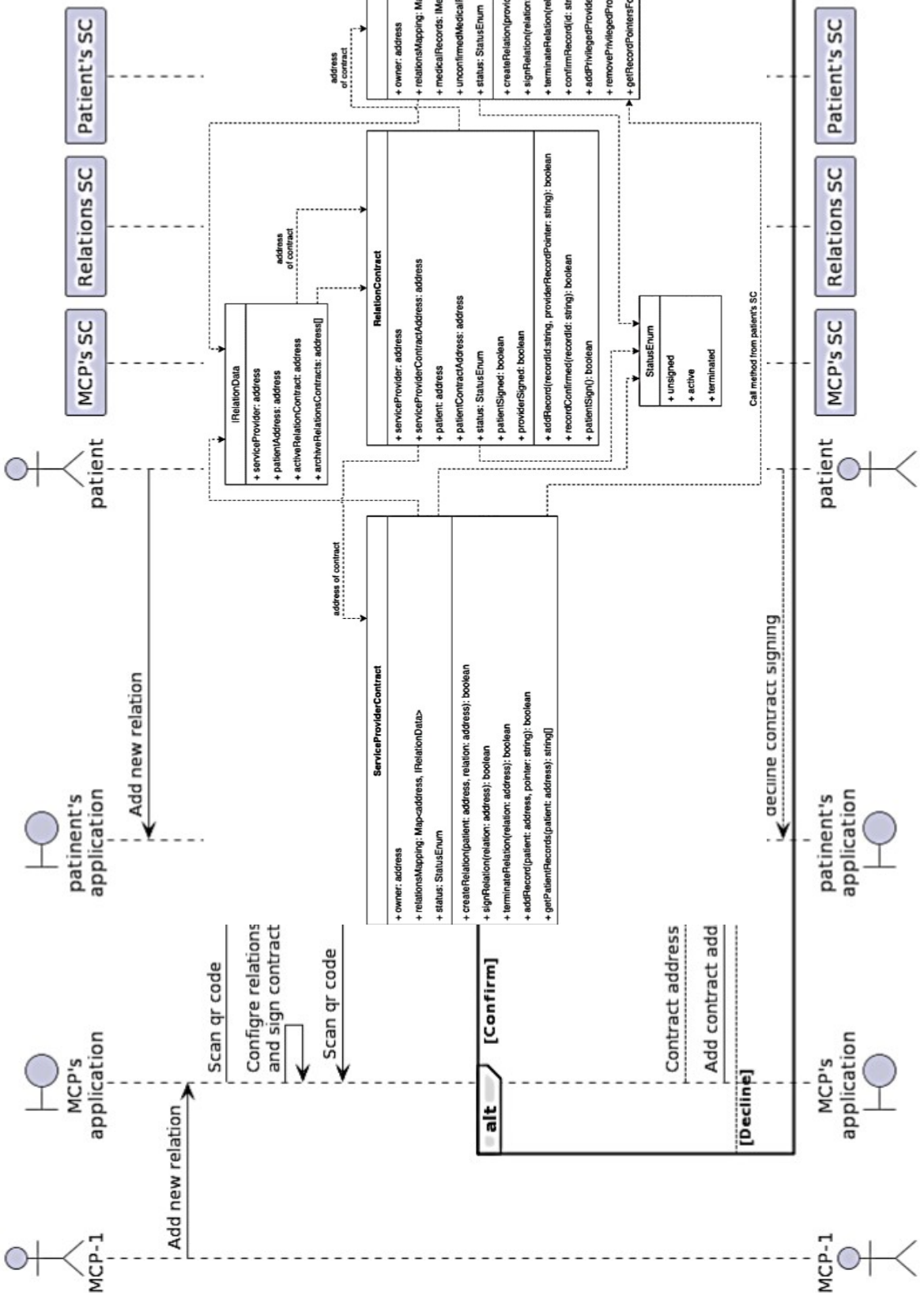


Рис. 3.3. UML-діаграма послідовності створення смарт-контракту відносин між сторонами

3.4 Створення медичних записів

Запис даних шифрується декількома ключами для оптимізації обсягу даних. Використовується шифрування розроблене на основі програми GPG. Застосунок генерує випадковий ключ який використовується для шифрування даних симетричним алгоритмом AES256 та шифрує ключ асиметричним алгоритмом ED25519, використовуючи ті ж ключі, що використовуються сторонами для операцій у блокчейні. Таким чином забезпечується захист даних від неавторизованого доступу та виключаються необхідність окремого зберігання ключів шифрування.

Зашифровані записи зберігаються у публічну децентралізовану мережу IPFS, яка гарантує доступність даних у будь-якій момент часу та реалізує ідентифікацію за вмістом. Як наслідок після завантаження дані з IPFS не можуть бути видалені та є фактично публічними. Але, оскільки приватні дані зашифровані досить надійним способом, то неавторизований користувач не зможе ними скористатись.

Після завантаження даних у IPFS отриманий ідентифікатор записуєтеся у смарт-контракт пацієнта. Далі існує 2 можливих сценарії:

1) медичний запис створює лікар у відповідному застосунку – пацієнт має перевірити та підтвердити і такім чином погодись, що створений запис є правдивим;

2) медичний запис створює автоматичний пристрій наприклад прилад для цілодобового моніторингу пульсу та тиску. У такому випадку пацієнт завчасно відмічає у своєму смарт-контракті ідентифікатор цього приладу як довірений. Дані, отримані від такого приладу, будуть підтверджені смарт-контрактом пацієнта автоматично.

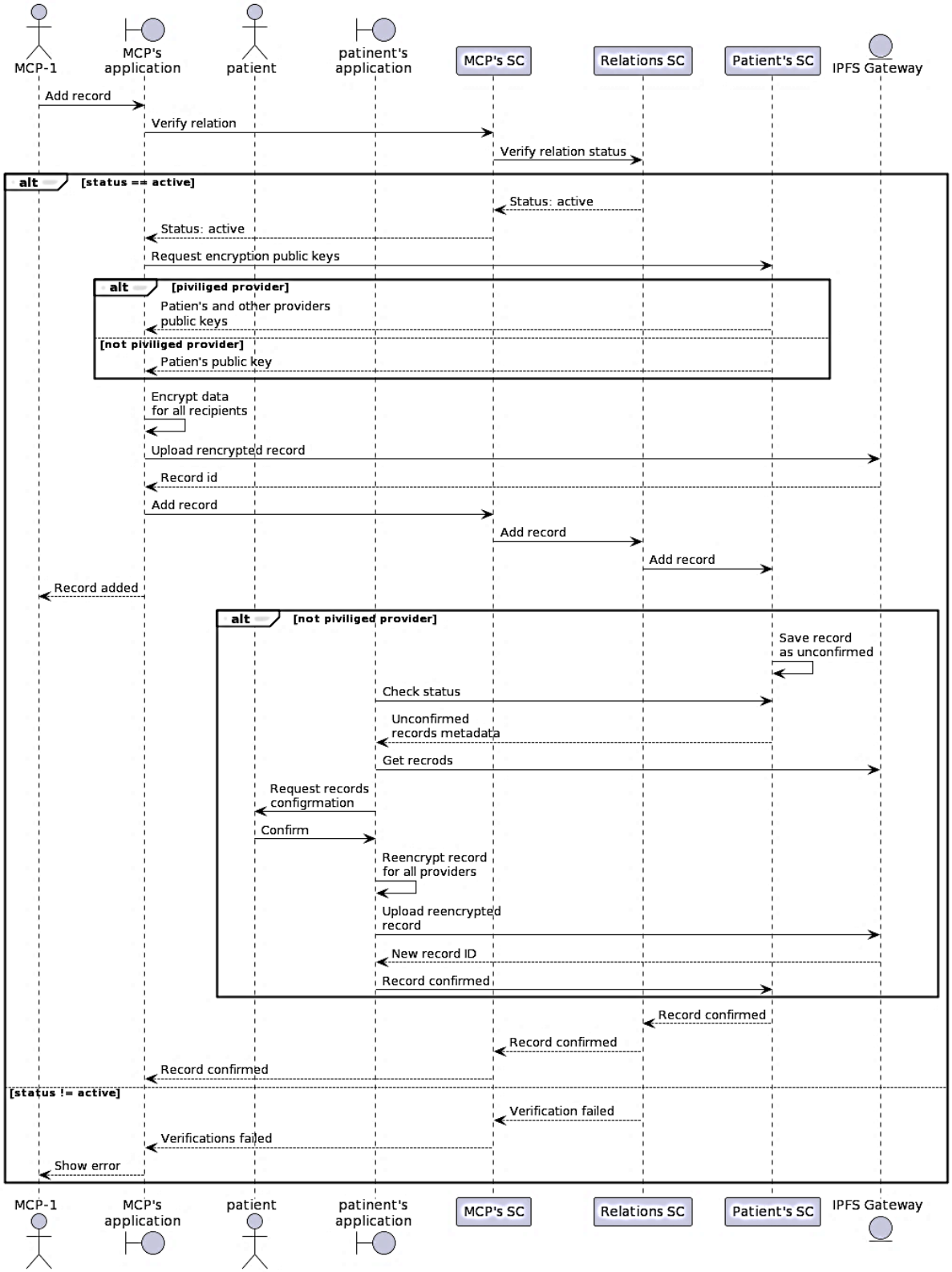

MCP-1
MCP's application
patient
patinent's application
MCP's SC
Relations SC
Patient's SC
IPFS Gateway
Add record
Verify relation
Verify relation status
alt
[status == active]
Status: active
Status: active
Request encryption public keys
alt
[piviliged provider]
Patien's and other providers public keys
[not piviliged provider]
Patien's public key
Encrypt data for all recipients
Upload rencrypted record
Record id
Add record
Add record
Add record
Record added
alt
[not piviliged provider]
Save record as unconfirmed
Check status
Unconfirmed records metadata
Get recrods
Request records configrmation
Confirm
Reencrypt record for all providers
Upload reencrypted record
New record ID
Record confirmed
Record confirmed
Record confirmed
Record confirmed
[status != active]
Verification failed
Verifications failed
Show error
MCP-1
MCP's application
patient
patinent's application
MCP's SC
Relations SC
Patient's SC
IPFS Gateway

Рис. 3.2. UML-діаграма послідовності процесу створення нового медичного запису

Висновки до розділу 3

В результаті проведених досліджень прийнято рішення провести запуск приватної мережі, повністю ідентичної платформі Ethereum. Також вирішено провести налаштування деяких параметрів для запобігання зайвих витрат з боку пацієнтів. Таке рішення також дозволить у майбутньому у разі необхідності клонувати систему на публічний блокчейн Ethereum. Також для приватного блокчейну бажано замінити алгоритм консесусу мережі та використовувати Proof-of-Authority замість Proof-of-Work. Це дозволить зменшити витрати на обчислювальне обладнання.

Для моніторингу мережі була розгорнута програма Ethstats, що містить у собі вебзастосунок, у якому відображаються підключені вузли та інші деталі щодо поточного стану мережі.

Розроблений застосунок генерує випадковий ключ який використовується для шифрування даних симетричним алгоритмом AES256 та шифрує ключ асиметричним алгоритмом ED25519, використовуючи ті ж ключі, що використовуються сторонами для операцій у блокчейні. Таким чином забезпечується захист даних від неавторизованого доступу та виключаються необхідність окремого зберігання ключів шифрування.

Зашифровані записи зберігаються у публічну децентралізовану мережу IPFS, яка гарантує доступність даних у будь-якій момент часу та реалізує ідентифікацію за вмістом. Як наслідок після завантаження дані з IPFS не можуть бути видалені та є фактично публічними. Але, оскільки приватні дані зашифровані досить надійним способом, то неавторизований користувач не зможе ними скористатись.

4 ПРОГРАМНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ

4.1 Застосунок для пацієнта

При першому запуску застосунку пацієнту необхідно згенерувати приватний ключ для взаємодії з системою. Макет екрану першого запуску мобільного застосунку пацієнта наведено на рис. 4.1. Застосунок відобразіть попередження пацієнту про необхідність створення резервної копії ключової (рис. 4.2–4.3) фрази, використовуючи яку він зможе відновити свій приватний ключ на іншому приладі. Таку резервну копію можна створити на паперовому або іншому аналоговому носії інформації. Ключова фраза складається з 24 англійських слів зі словника BIP39 (Bitcoin Improvement Proposal 39). Або якщо пацієнт вже використовував застосунок при першому запуску застосунку на новому пристрої він зможе відновити свій приватний ключ за допомогою резервної копії ключової фрази.

Додатково застосунок запропонує пацієнту встановити пароль, який буде використано для генерації приватного ключа. Алгоритм генерацій приватних ключів розроблено на основі специфікації BIP39, тому не може існувати неправильного паролю при відновленні ключів на новому пристрої. У випадку невірно введеного паролю застосунок згенерує новий приватний ключ замість того, яким раніше користувався пацієнт.

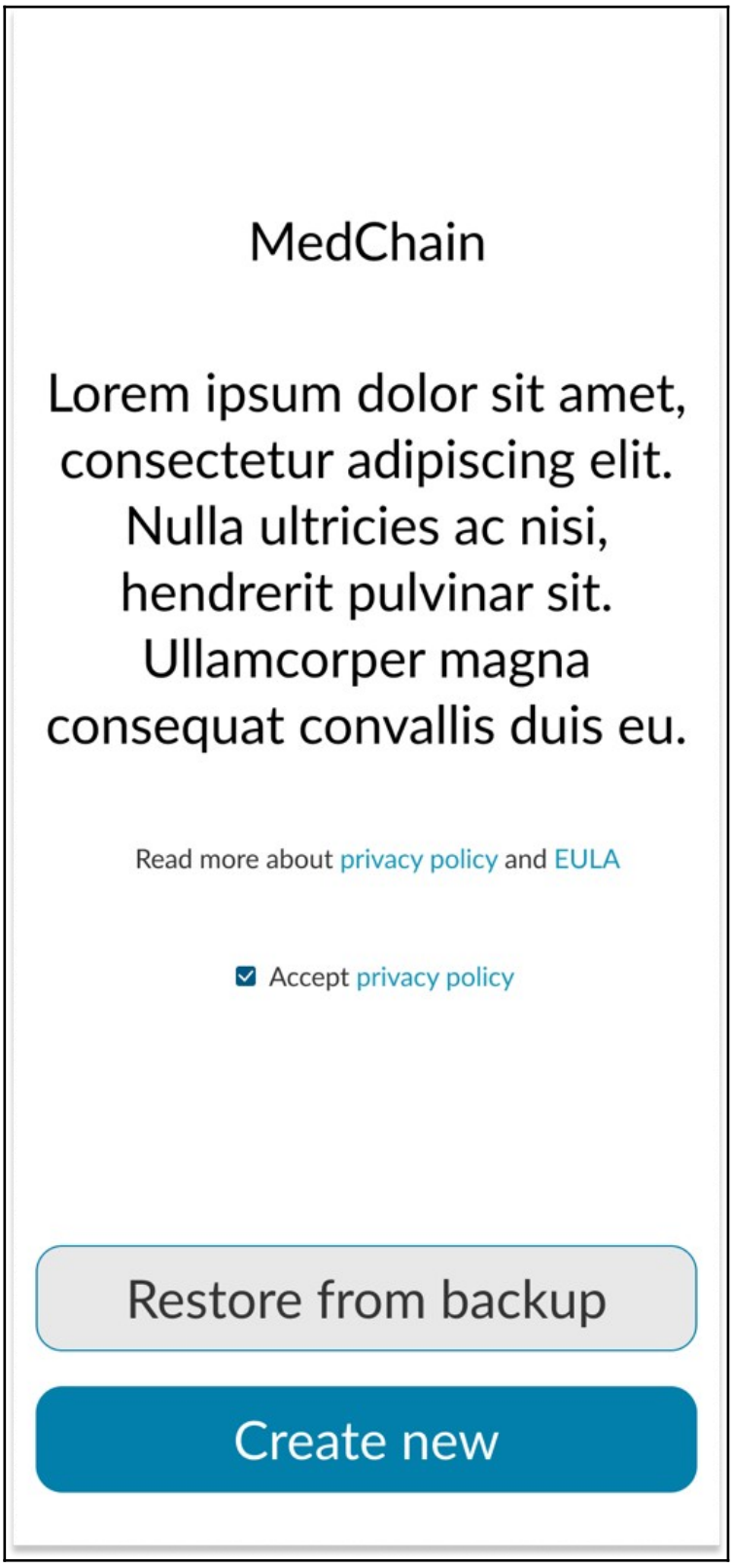


Рис. 4.1. Макет екрану першого запуску застосунку пацієнта

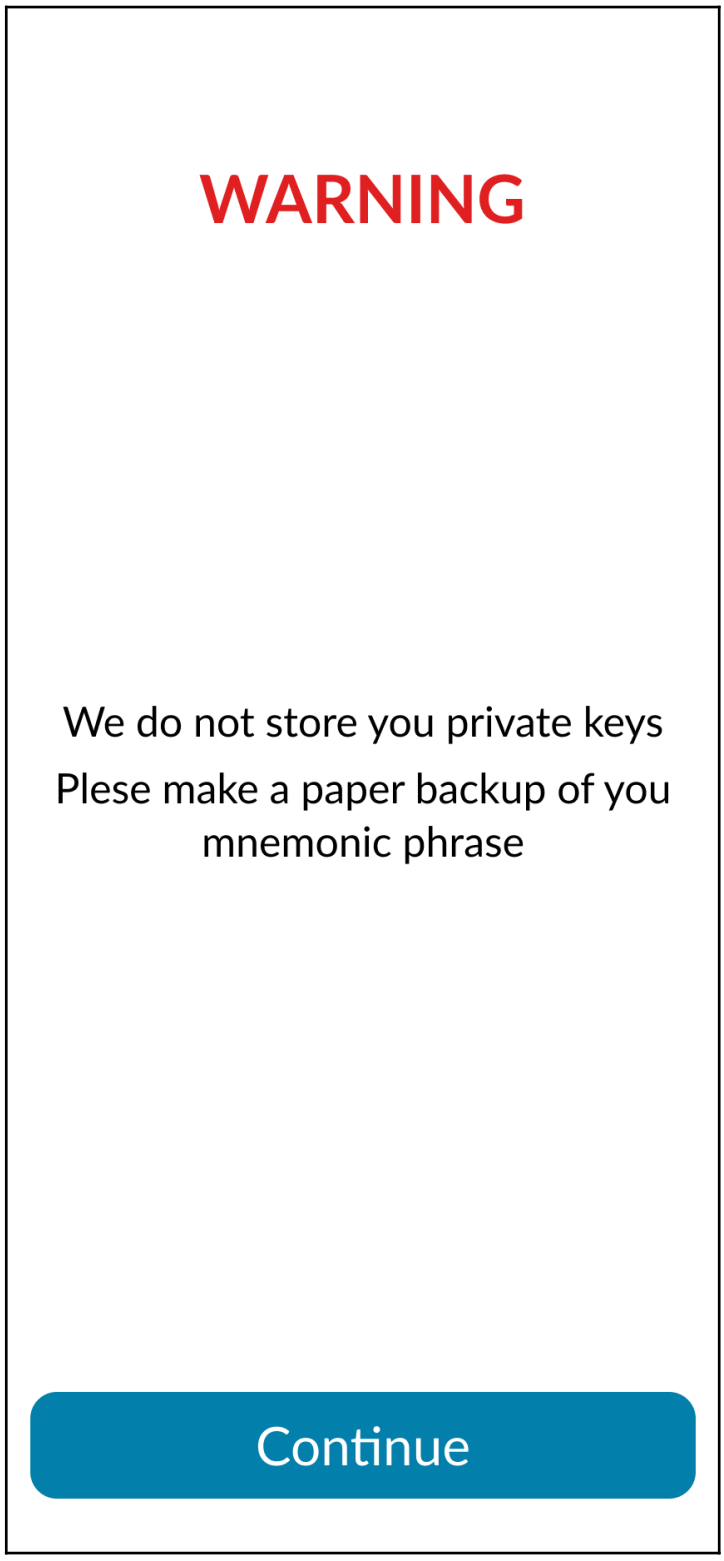


Рис. 4.2. Макет попередження про створення резервної копії ключової фрази

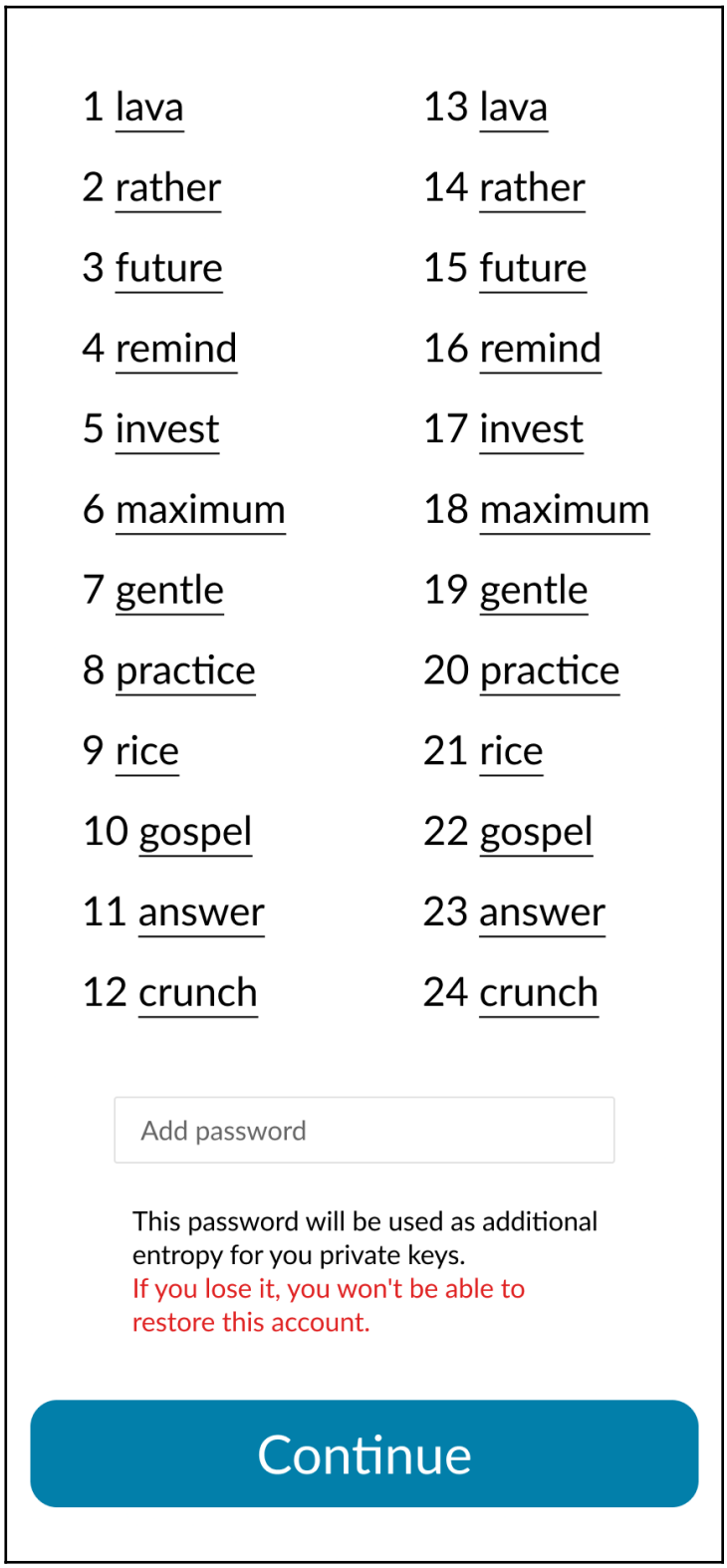


Рис. 4.3. Скріншот генерації ключової фрази та приватних ключів у мобільному застосунку пацієнта

Після створення приватних ключів застосунок відобразіть головне меню, в якому доступні функції створення нових смарт-контрактів з надавачами медичних послуг, перегляд існуючих смарт-контрактів в яких зазначено пацієнта, припинення дії активних смарт-контрактів та перегляд медичних записів (рис. 4.4).

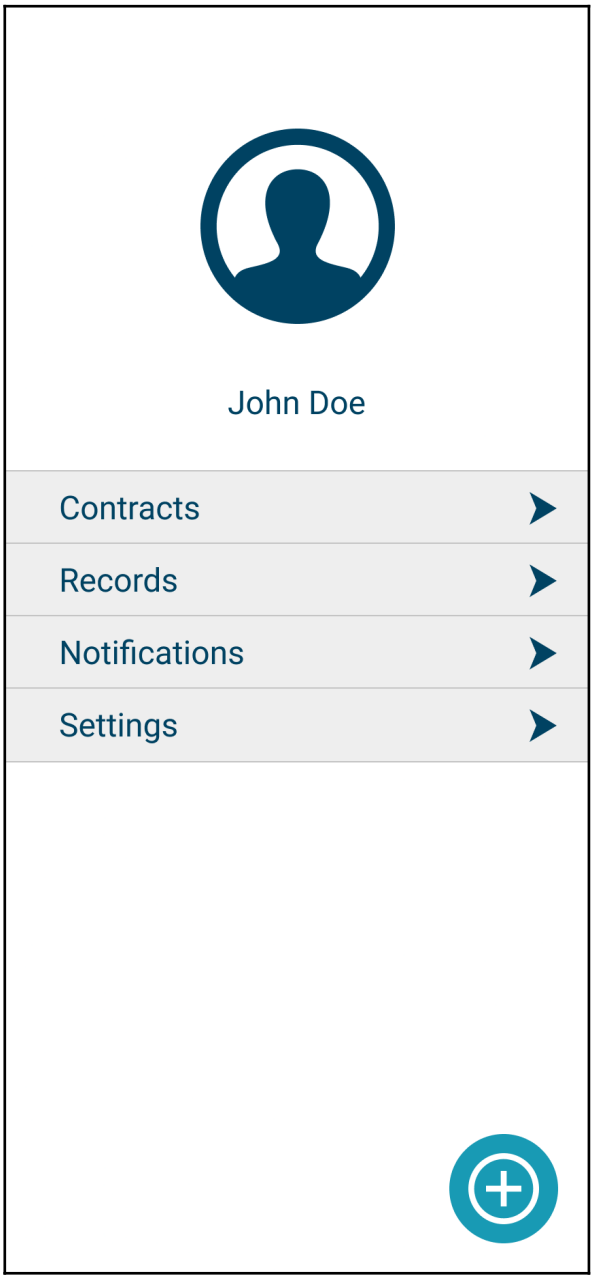


Рис. 4.4. Скріншот головного меню застосунку пацієнта

4.2 Створення нового смарт-контракту між сторонами

Технічні деталі процесу створення смарт-контракту між сторонами наведені у розділі 3.3. А для користувачів системо необхідно лише сканувати QR-код іншої сторони у відповідному застосунку. Скріншоти створення смарт-контракту у застосунку пацієнта наведені на рис. 4.5, рис 4.6. У вебзастосунку для лікаря подібним чином відображається QR-код та його можна сканувати вебкамерою, приєднаною до комп’ютера. У випадку автоматизованих пристроїв моніторингу вони мають бути оснащені спеціальнім сканером QR-коду та невеликим екраном для відображення інформації.

4.3 Вебзастосунок для співробітників медичних закладів

Для співробітників медичних закладів розроблено функціонально схожій з застосунком пацієнта, але оптимізованій з урахуванням потреб співробітників медичних закладів. Для зручного пошуку та перегляду даних, списків пацієнтів та медичних записів створені таблиці, та сторінки для перегляду детальної інформації про пацієнта та окремі медичні записи.

Рис 4.5. Відображення QR-коду у застосунку пацієнта

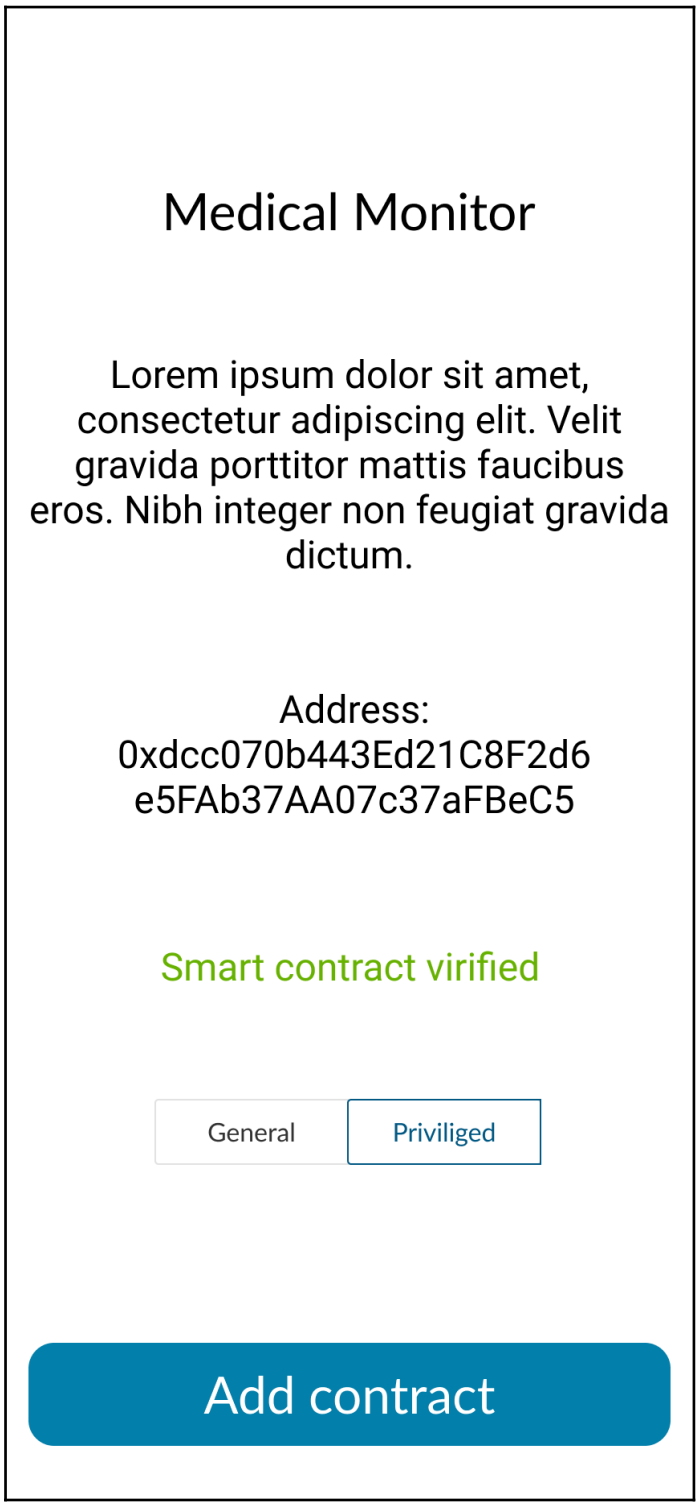


Рис 4.6. Скріншот екрану, на якому пацієнт може перевірити дані смарт-контракту та підтвердити або відмінити його створення

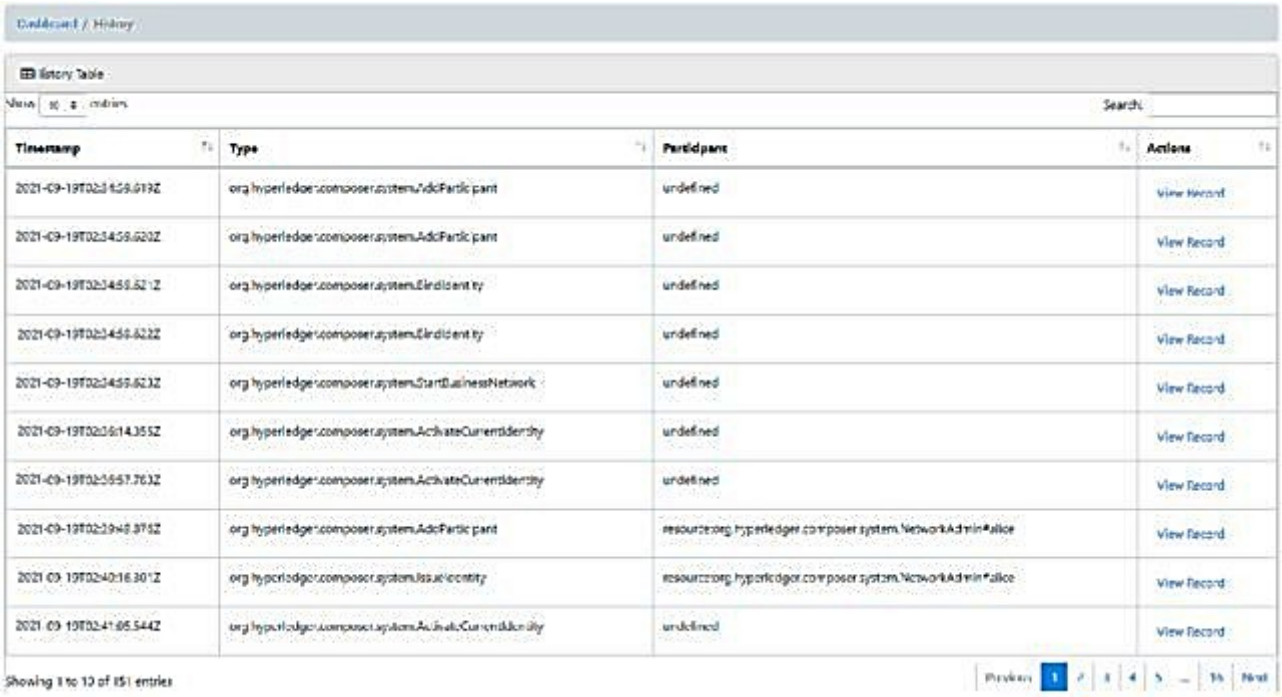


Рис. 4.7. Скріншот інформаційної панелі історії транзакцій у вебзастосунку для лікарів

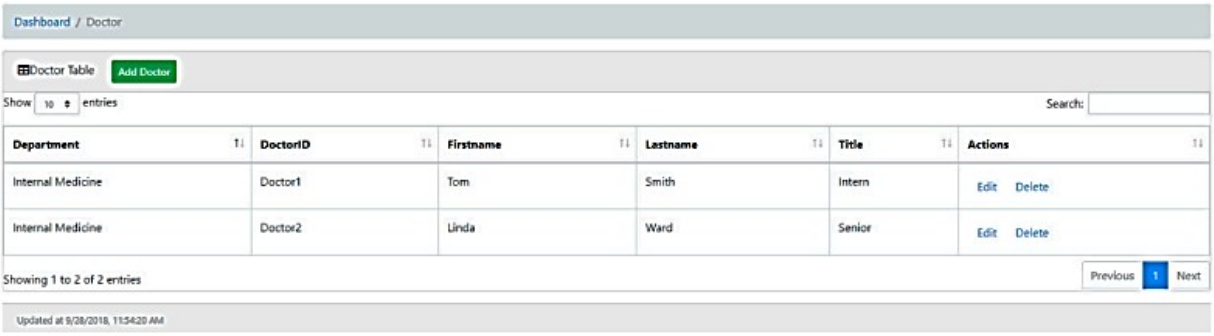


Рис. 4.8. Скріншот вебзастосунку для лікарів з таблиці лікарів, які надавали послуги пацієнту

Таким чином, система є досить простою для використання і при цьому забезпечує доступність даних у будь-якій момент часу та незалежно від місцезнаходження лікаря та пацієнта. Дані, які зберігаються у IPFS, зашифровані надійними криптографічними алгоритмами, тому неавторизований користувач не має змогу отримати до них доступ.

Висновки до розділу 4

В результаті програмної реалізації розроблений застосунок для пост-інсультного пацієнта, що знаходиться на віддаленій реабілітації.

При першому запуску застосунку пацієнту необхідно згенерувати приватний ключ для взаємодії з системою. Застосунок відобразіть попередження пацієнту про необхідність створення резервної копії ключової фрази використовуючи яку він зможе відновити свій приватний ключ на іншому приладі. Таку резервну копію можна створити на паперовому або іншому аналоговому носії інформації.

Алгоритм генерацій приватних ключів розроблено на основі специфікації BIP39, тому не може існувати неправильного паролю при відновленні ключів на новому пристрої. У випадку невірно введеного паролю застосунок згенерує новий приватний ключ замість того, яким раніше користувався пацієнт.

У роз робленому меню доступні функції створення нових смарт-контрактів з надавачами медичних послуг, перегляд існуючих смарт-контрактів, в яких зазначено пацієнта, припинення дії активних смарт-контрактів та перегляд медичних записів.

В результаті тестування підтверджено, що розроблена система на основі блокчейну забезпечує захист наборів даних щодо стану пост-інсультних пацієнтів на віддаленій реабілітації та придатна для практичного використання.

ВИСНОВКИ

За результатами МНР було створено систему, яка дозволяє пацієнту контролювати віддалений доступ до своєї облікової інформації, надавати доступ до інформації обмеженому колу осіб-постачальників медичних послуг.

Досягнення цієї мети відбулося завдяки виконанню наступних завдань::

- проведено аналіз існуючих сервісів-аналогів для контролю ідентифікації та розподілення персональної медичної інформації, розроблених у інших країнах світу;
- досліджено технології для створення захищеної системи від несанкціонованого доступу;
- розроблено модель створюваної системи з використанням обраних інформаційних технологій;
- розроблено систему для захисту наборів даних щодо стану пост-інсультних пацієнтів на віддаленій реабілітації;
- проведено тестування розробленої системи на відкритих спеціалізованих наборах даних великого обсягу, зібраних медичними фахівцями, що працюють з пост-інсультними пацієнтами.

В роботі використовується публічна блокчейн платформа Ethereum для створення децентралізованих онлайн-сервісів на базі блокчейну. Вона застосована для зберігання інформації щодо факту надання доступу до інформації пацієнта. Зазначений доступ надається через смарт-контракт між пацієнтом та сертифікованим постачальником медичних послуг. Розроблено додаткове програмне забезпечення для взаємодії пацієнта та постачальника послуг з обліковими даними пацієнта на основі метаданих, що зберігаються у блокчейні Ethereum. Для зберігання облікових даних пацієнта використовується система на основі технології IPFS для розподіленого зберігання інформації з додатковим шифруванням для забезпечення контролю доступу до облікових

даних. IPFS (Inter-Planetary File System) – система розподіленого зберігання даних, яка використовує систему ідентифікації за вмістом та зберігає копію даних на кількох вузлах мережі однозначно. Це забезпечує захист даних від підробки та доступність у будь-якій момент часу.

Розроблену систему протестовано на відкритих спеціалізованих наборах даних великого обсягу (data set) щодо пост-інсультних пацієнтів (з ресурсів Медичного університету Південної Кароліни, США).

Запропонований підхід та програмне забезпечення має перспективу використання для захисту наборів даних щодо стану пост-інсультних пацієнтів на віддаленій реабілітації, коли конфіденційні дані передаються від пацієнта до медичного працівника відкритими каналами зв’язку.

Практичне значення роботи полягає в тому, що дана МКР є складовою частиною науково-дослідної роботи ЧНУ ім. Петра Могили «Розробка модулів автоматизації бездротових приладів відновлення пост-інфарктних, пост-інсультних пацієнтів в індивідуальних умовах віддаленої реабілітації» № держреєстрації 0121U109898 (наук. кер. проф. Трунов О. М.).

Робота пройшла апробацію під час XXIV Всеукраїнської науково-практичної конференції «Могилянські читання» (Миколаїв, 08–12 листопада 2021 р.), за якою опубліковано тези доповіді у збірнику матеріалів конференції

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. План дій боротьби з інсультом у Європі на 2018–2030 рр, Брюсель, 2018. URL: https://www.safestroke.eu/wp-content/uploads/2019/05/sap-ukraine-s.pdf (дата звернення: 15.01.2022).

2. Рекомендації щодо нейрореабілітації пацієнтів після інсульту. URL: https://health-ua.com/article/41706-rekomendatc-shodo-nejroreabltatc-patcntvpslya-nsultu (дата звернення: 15.01.2022).

3. Х. Юхимчук, «Реабілітацію хворих з інсультом». *Медсестринство*. 2018. № 3. С 23–26. ISSN 2411-1597. URL: http://www.cs.binghamton.edu/~zhangy/paper/hotpower13.pdf (дата звернення: 15.01.2022).

4. Сучасні тенденції у постінсультній реабілітації в Україні. URL: http://health-ua.com/article/5201-suchasn-tendentc-upostnsultnj-reabltatc-vukran (дата звернення: 15.01.2022).

5. Цифровий лікар: як електронні медичні картки трансформують систему охорони здоров'я в Україні. URL: https://biz.nv.ua/ukr/markets/elektronna-medichna-karta-yak-emk-dopomozhut-paciyentam-i-likaryam-novini-ukrajini-50126517.html (дата звернення: 15.01.2022).

6. В Україні введуть електронні медкартки: що це значить. URL: https://nv.ua/ukr/ukraine/events/v-ukrajini-vvedut-elektronni-medkartki-shcho-tse-znachit-2512710.html (дата звернення: 15.01.2022).

7. UCLA will pay $7.5 million in claims, cyber enhancements to settle 2015 breach. URL: https://www.healthcareitnews.com/news/ucla-will-pay-75-million-claims-cyber-enhancements-settle-2015-breach

8. The biggest healthcare data breaches of 2021. URL: https://www.healthcareitnews.com/news/biggest-healthcare-data-breaches-2021 (last acsessed: 16.01.2022).

9. Scripps Health network still down, 2 weeks after cyberattack. URL: https://www.healthcareitnews.com/news/scripps-health-network-still-down-2-weeks-after-cyberattack (last acsessed: 16.01.2022).

10. Cybersecurity in 2022: password-less authentication, zero trust, blockchain and morehttps://www.healthcareitnews.com/news/cybersecurity-2022-password-less-authentication-zero-trust-blockchain-and-more (last acsessed: 16.01.2022).

11. Блокчейн для медицини. URL: https://www.livemd.ru/tags/blokchejn_dlja_mediciny/ (дата звернення: 16.01.2022).

12. Aetna, Anthem, Health Care Service Corporation, PNC Bank and IBM announce collaboration to establish blockchain-based ecosystem for the healthcare industry. URL: https://newsroom.ibm.com/2019-01-24-Aetna-Anthem-Health-Care-Service-Corporation-PNC-Bank-and-IBM-announce-collaboration-to-establish-blockchain-based-ecosystem-for-the-healthcare-industry (last acsessed: 16.01.2022).

13. Khatoon A. A Blockchain-Based Smart Contract System for Healthcare Management. *Electronics*, 2020, vol. 9, doi:10.3390/electronics9010094.

14. Fries M., Paal B. P. Smart Contracts. Mohr Siebeck GmbH and Co. KG, 2019. 142 p. URL: https://www.jstor.org/stable/j.ctvn96h9r (last acsessed: 18.01.2022).

15. A gentle introduction to Ethereum. URL: https://bitsonblocks.net/2016/10/02/gentle-introduction-ethereum/ (last acsessed: 18.01.2022).

16. Ethereum Whitepaper. URL: https://ethereum.org/en/whitepaper/ (last acsessed: 18.01.2022).

17. Sillaber C., Waltl B. Life Cycle of Smart Contracts in Blockchain Ecosystems. *Datenschutz und Datensicherheit*, 2017, vol. 41, pp. 497–500. https://doi.org/10.1007/s11623-017-0819-7.

18. Medicalchain. URL: https://knowledge4policy.ec.europa.eu/foresight/tool/dlt4good/medicalchain_en (last acsessed: 25.01.2022).

19. Blockchain In Healthcare Use Case #23: Medicalchainhttps://www.disruptordaily.com/blockchain-in-healthcare-use-case-medicalchain/ (last acsessed: 25.01.2022).

20. Medicalchain. Whitepaper 2.1. URL: https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf (last acsessed: 25.01.2022).

21. Rouhani S., Butterworth L., Simmons A. D., Humphery D. G., Deters R. MediChainTM: A Secure Decentralized Medical Data Asset Management System. *2018 IEEE Confs on Internet of Things*, 2018. DOI: 10.1109/ Cybermatics_2018.2018.00258. URL: https://arxiv.org/ftp/arxiv/papers/ 1901/1901.10645.pdf (last acsessed: 25.01.2022).

22. Azaria A., Ekblaw A., Vieira T., Lippman A. MedRec: Using Blockchain for Medical Data Access and Permission Management. *2016 2nd International Conference on Open and Big Data (OBD)*, 2016. https:// www.researchgate.net/publication/ 308570159_MedRec_Using_Blockchain_for_Medical_Data_Access_and_Permission _Management (last acsessed: 25.01.2022).

23. MedRec: Medical Data Management on the Blockchain. URL: https://v3.pubpub.org/pub/medrec (last acsessed: 25.01.2022).

24. MedRec technical documentation. URL: https://medrec.media.mit.edu/technical/ (last acsessed: 25.01.2022).

25. How Using Blockchain in Healthcare Is Reviving the Industry's Capabilities. URL: https://builtin.com/blockchain/blockchain-healthcare-applications-companies (last acsessed: 25.01.2022).

26. Шурбін В. О., Журавська І. М. Використання технології блокчейн для системи обліку пост-інсультних пацієнтів. *Могилянські читання – 2021* : тези доп. XXIV Всеукр. наук.-метод. конф. Миколаїв, 8–12 листоп. 2021 р. Миколаїв : Чорном. нац. ун-т ім. Петра Могили, 2021. С. 45–46.

27. Features of using the Merkle tree in blockchain and Bitcoin. URL: https://changelly.com/blog/merkle-tree-explain/ (last acsessed: 09.02.2022).

28. Merkle Tree in Blockchain: What is it, How does it work and Benefits. URL: https://www.simplilearn.com/tutorials/blockchain-tutorial/merkle-tree-in-blockchain (last acsessed: 09.02.2022).

29. Ethereum State Trie Architecture Explained. URL: https://medium.com/@eiki1212/ethereum-state-trie-architecture-explained-a30237009d4e (last acsessed: 09.02.2022).

30. Monahan B., Chen L., Haber S. HashFusion – a method for combining cryptographic hash values. 2017. URL: https://www.labs.hpe.com/techreports/2017/HPE-2017-08.pdf (last acsessed: 09.02.2022).

31. Hang L., Choi E., Kim D.-H. A Novel EMR Integrity Management Based on a Medical Blockchain Platform in Hospital. *Electronics.* 2019. Is. 8(4):467. 29 p. DOI: 10.3390/electronics8040467.

32. Охорона праці в медичних установах. URL: https://www.ohrana-truda.in.ua/uk/materyalu/ot-v-otraslyah/medicine/ (дата звернення: 24.01.2022).

33. ГОСТ 12.1.002-84. ССБТ. Электрические поля промышленной частоты. Допустимые урони напряженности и требования к проведению контроля на робочих местах. [На замену ГОСТ 12.1.002-75; действителен от 2019-02-28]. Вид. офиц. Москва, 1984. Межгосударственный стандарт, 1984.

34. ДБН В.2.5-28:2018. Природне і штучне освітлення. [На заміну ДБН В.2.5-28:2006; чинний від 2019-02-28]. Вид. офіц. Київ, 2018. Державні Будівельні Норми України, 2018. 133 с.

35. Джигирей В. С., Сторожук В. М., Лико Х. І., Туряб Л. В. Практикум з охорони праці: навч. посіб. / за ред. В. Ц. Жидецького. Львів : Афіша, 2000. 352 с.

36. ДСанПІН 3.3.2.007-98. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин. [Чинний від 1998-12-10]. Вид. офіц. Київ, 1998. Міністерство охорони здоров'я України, 1998. 27 с.

37. ДСН 3.3.6.042-99. Санітарні норми мікроклімату виробничих приміщень. [Чинний від 1999-12-01]. Вид. офіц. Київ, 1999. Міністерство охорони здоров'я України, 1999. 16 с.

38. Жидецький В. Ц., Джигирей В. С., Мельников О. В. Основи охорони праці: навч. посіб. Вид.4-те, допов. Львів, 2000. 350 с.

39. Жидецький В. Ц. Охорона праці користувачів комп'ютерів. Львів, 2000. 176 с.

40. Запобігання пожежі з причин короткого замикання. *Луганське енергетичне об'єднання* : вебсайт. URL: https://www.en.lg.ua/

potrebitelu/electrobezopasnost/item/911-zapobihannia-pozhezhi-z-prychyn-korotkoho-zamykannia (дата звернення: 17.12.2021).

ДОДАТОК А

Фрагменти програмного коду

А.1 Код смарт-контракту відносин між сторонами

```
import "@openzeppelin/contracts/access/Ownable.sol";
import "@openzeppelin/contracts/access/AccessControl.sol";

import "./utils.sol";

contract RelationContract {
   address public serviceProvider;
   address public serviceProviderContract;
   address public patient;
   address public patientContract;
   StatusEnum public status;

   constructor(address _serviceProvider, address _serviceProviderContract, address _patient, address
_patientContract) {
      serviceProviderContract = _serviceProvider;
      serviceProviderContract = _serviceProviderContract;
      patient = _patient;
      patientContract = _patientContract;
      status = StatusEnum.ACTIVE;
   }

   function terminate() public {
      require(msg.sender == serviceProviderContract || msg.sender == patientContract, "Can be called only by
members");
      status = StatusEnum.TERMINATED;
   }
}
```

А.2 Код смарт-контракту пацієнта

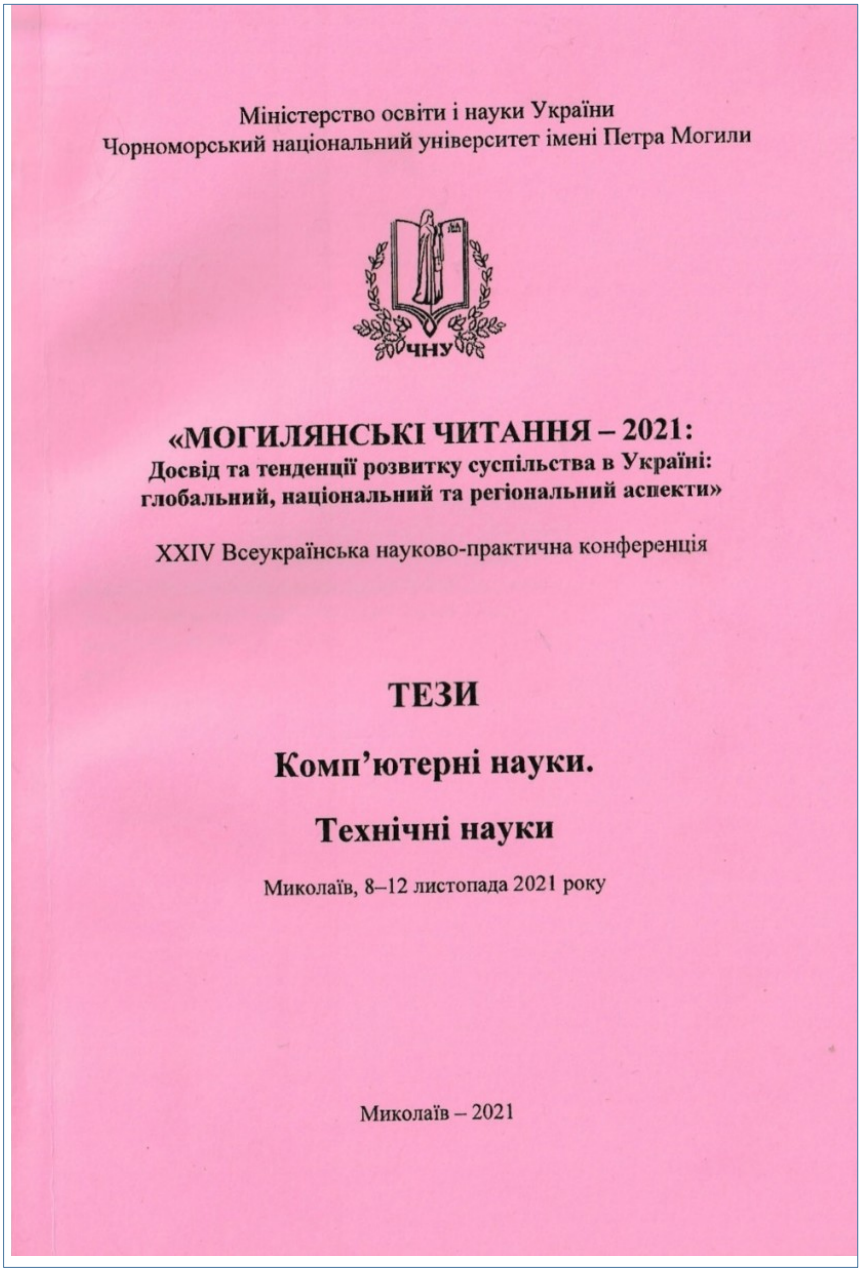
```
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/access/Ownable.sol";
import "@openzeppelin/contracts/access/AccessControl.sol";

import "./utils.sol";
import "./0_Relation.sol";

struct IRelationData {
    uint256 id;
    address serviceProvider;
    address scAddress;
}

contract PatientSummary is Ownable, AccessControl {
    // RBAC
    bytes32 public constant PROVIDER = keccak256("PROVIDER");
    bytes32 public constant PRIVILEGED_PROVIDER = keccak256("PRIVILEGED_PROVIDER");

    uint256 relationsCounter;
    uint256 recordsCounter;
    mapping(address => IRelationData) public relationsByProvider;
    mapping(address => IRelationData) public relations;
    mapping(string => IMedicalRecord) public records;
    StatusEnum public status;

    constructor() Ownable() AccessControl() {
        status = StatusEnum.ACTIVE;
        relationsCounter = 0;
        _setupRole(DEFAULT_ADMIN_ROLE, msg.sender);
    }

    function setPrivilegedProvider(address provider) public onlyOwner returns (bool) {
        IRelationData storage relationData = relationsByProvider[provider];
        bool isContractActive = relationData.id > 0 && RelationContract(relationData.scAddress).status() ==
StatusEnum.ACTIVE;
        require(isContractActive, "Relations contract not exists or not active");
        grantRole(PRIVILEGED_PROVIDER, provider);
    }

    function revokePrivilegedProvider(address provider) public onlyOwner {
        IRelationData storage relationData = relationsByProvider[provider];
        bool isContractActive = relationData.id > 0 && RelationContract(relationData.scAddress).status() ==
StatusEnum.ACTIVE;
        require(isContractActive, "Relations contract not exists or not active");
```

```
    require(hasRole(PRIVILEGED_PROVIDER, provider), "Provider is not privileged");
    revokeRole(PRIVILEGED_PROVIDER, provider);
  }

  function addRecord(string memory recordId) public onlyRole(PROVIDER) {
    bool isPriviliged = hasRole(PRIVILEGED_PROVIDER, msg.sender);
    recordsCounter++;
    records[recordId] = IMedicalRecord(recordsCounter, recordId, msg.sender, isPriviliged);
  }

  function confirmRecord(string calldata recordId) public onlyOwner {
    require(records[recordId].id > 0, "Record does not exists");
    records[recordId].confirmed = true;
  }

  function createRelation(address provider, address relation, bool isPriviliged) public onlyOwner {
    // grant roles to provider
    _setupRole(PROVIDER, provider);
    relationsCounter++;
    IRelationData memory relationData = IRelationData(relationsCounter, provider, relation);
    relationsByProvider[provider] = relationData;
    relations[relation] = relationData;
  }

  function terminateRelation(address relation) public onlyOwner {
    RelationContract(relation).terminate();
  }
}
```

ДОДАТОК Б

Публікації за темою диплому

Б.1 Тези доповіді на XXIV Всеукраїнській науково-практичній конференції «Могилянські читання – 2021»


Міністерство освіти і науки України
Чорноморський національний університет імені Петра Могили

ЧНУ

«МОГИЛЯНСЬКІ ЧИТАННЯ – 2021:
Досвід та тенденції розвитку суспільства в Україні:
глобальний, національний та регіональний аспекти»

XXIV Всеукраїнська науково-практична конференція

ТЕЗИ

Комп'ютерні науки.

Технічні науки

Миколаїв, 8–12 листопада 2021 року

Миколаїв – 2021

ЗМІСТ

Секція: КОМП'ЮТЕРНІ НАУКИ

ПІДСЕКЦІЯ: Інтелектуальні інформаційні системи

ПІДСЕКЦІЯ: Комп'ютерна інженерія

Важливою ознакою стандартної моделі ССЕ є те, що кількість параметрів інтерполянту співпідає з кількістю вузлів.

Варто зазначити, що в деяких джерелах серендипові скінченні елементи називають ізопараметричними.

УДК 004.415.2: 004.67

Шурбін В. О.,
магістрант,
Журавська І. М.,
д-р техн. наук, професор,
ЧНУ ім. Петра Могили, м. Миколаїв

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ СИСТЕМИ ОБЛІКУ ПОСТ-ІНСУЛЬТНИХ ПАЦІЄНТІВ

На сьогодні захист медичної облікової інформації представляє комплекс заходів, спрямованих на обмеження доступу до конфіденційної інформації, та включає засоби перевірки достовірності та цілісності інформації. Конфіденційною інформацією вважається інформація про стан пацієнта, яка дозволяє прямим способом або опосередковано ідентифікувати пацієнта, до якого ця інформація відноситься, тобто, його персональні дані. У той же час, для проведення медичних заходів та аналізу стану пацієнта необхідне підтвердження цілісності та достовірності облікової інформації щодо пацієнта.

Метою роботи є створення системи, яка дозволить пацієнту контролювати доступ до своєї облікової інформації, надавати доступ до інформації обмеженому колу осіб – постачальників медичних послуг.

У світі спостерігається тенденція використання для захисту цифрових медичних карт технології блокчейн (сервіси MedRec у США, Medicalchain у Великобританії, Guardtime в Естонії, тощо). Використання блокчейну може вивести облік медичних послуг на новий рівень, забезпечивши своєчасне оновлення даних і гарантію доступу тільки авторизованих лікарів. Блокчейн (англ. Blockchain) – це технологія розподіленого реєстру, яка використовується для запису транзакцій. Транзакції згруповані у блоки, та кожен наступний блок містить контрольну суму попереднього блоку. Такий підхід забезпечує цілісність реєстру та значно знижує можливість підробки транзакцій.

При цьому, повна копія реєстру зберігається на багатьох комп'ютерах одночасно.

Рис. 1. Діаграма створення смарт-контракту між сторонами

У роботі використовується публічна платформа Ethereum для створення децентралізованих онлайн-сервісів на базі блокчейну; вона застосована для зберігання інформації щодо факту надання доступу до інформації пацієнта. Зазначений доступ надається через смарт-контракт між пацієнтом та сертифікованим постачальником медичних послуг. Розроблено додаткове програмне забезпечення для взаємодії пацієнта та постачальника послуг з обліковими даними пацієнта на основі метаданих, що зберігаються у блокчейні Ethereum. Для зберігання облікових даних пацієнта використовується система на основі технології IPFS для розподіленого зберігання інформації з додатковим шифруванням для забезпечення контролю доступу до облікових даних. IPFS (Inter-Planetary File System) – система розподіленого зберігання даних, яка використовує систему ідентифікації за вмістом та зберігає копію даних на кількох вузлах мережі однозначно. Це забезпечує захист даних від підробки та доступність у будь-який момент часу.

Розроблену систему протестовано на відкритих спеціалізованих наборах даних великого обсягу (data set) щодо пост-інсультних пацієнтів

Запропонований підхід та програмне забезпечення доцільно використовувати для захисту наборів даних щодо стану пост-інсультних пацієнтів на віддаленій реабілітації, коли конфіденційні дані передаються від пацієнта до медичного працівника відкритими каналами зв'язку.

ДОДАТОК В

Акт впровадження у науково-дослідну роботу

АКТ

впровадження результатів магістерської кваліфікаційної роботи

студента групи 607м Шурбіна В. О. на тему: «**Система на основі блокчейну для захисту наборів даних щодо стану пост-інсультних пацієнтів на віддаленій реабілітації**» при виконанні держбюджетної НДР «РОЗРОБКА МОДУЛІВ АВТОМАТИЗАЦІЇ БЕЗДРОТОВИХ ПРИЛАДІВ ВІДНОВЛЕННЯ ПОСТ-ІНФАРКТНИХ, ПОСТ-ІНСУЛЬТНИХ ПАЦІЄНТІВ В ІНДИВІДУАЛЬНИХ УМОВАХ ВІДДАЛЕНОЇ РЕАБІЛІТАЦІЇ»;

№ держ. реєстрації 0121U109898;

керівник НДР д-р техн. наук, проф. Трунов О. М.,

термін виконання роботи 01.01.2021–31.12.2022

Держбюджетна НДР № держ. реєстрації 0121U109898 виконується в Чорноморському національному університеті ім. Петра Могили. При виконанні першого етапу НДР в період з 01.01.2021 по 31.12.2021, а також при підготовці проміжного звіту з НДР є прийнята для впровадження розроблена інформаційна система, яка дозволяє пацієнту контролювати віддалений доступ до своєї облікової інформації, надавати доступ до інформації обмеженому колу осіб-постачальників медичних послуг. В процесі виконання НДР також використані такі наукові й практичні результати розробленої інформаційної системи:

– застосування для захисту персональних даних пост-інсультних пацієнтів на віддаленій реабілітації технології блокчейну та смарт-контрактів;

– використання «Дерева Меркла» у блокчейні для багаторазового хешування пар вузлів, поки не залишиться лише один хеш, що використовується для захисту цілісності даних пацієнтів;

– тестування на відкритих спеціалізованих наборах даних великого обсягу (DataSet пост-інсультних пацієнтів Center for Machine Learning and Intelligent Systems at University of California, Irvine, USA).

Магістрант Шурбін В. О. виконував роботу під керівництвом відповідального виконавця НДР, д-ра техн. наук, проф. Журавської І. М.

Керівник НДР,
професор кафедри автоматизації та
комп'ютерно-інтегрованих технологій,
д-р техн. наук, проф. О. М. Трунов

«10» 02 2022 р.

Підпис О.М. Трунова засвідчую
Начальник ВК О.А. Сасенко