Інше

УДК 004.9:61

Коваленко Олександр Сергійович
доктор медичних наук, професор,
професор кафедри біомедичної кібернетики
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Kovalenko Oleksandr
Doctor of Medical Sciences, Professor,
Professor of the Department of Biomedical Cybernetics
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
ORCID: 0000-0001-6635-0124

Кононов Антон Вікторович
студент кафедри біомедичної кібернетики
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
Kononov Anton
Student of the Department of biomedical cybernetics
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"

Авер'янова Ольга Анатоліївна
викладач кафедри біомедичної кібернетики
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Averyanova Olga
Assistant of the Department of Biomedical Cybernetics
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"

ВИКОРИСТАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЇ ДЛЯ ДЕЦЕНТРАЛІЗОВАНОГО ТА НАДІЙНОГО ЗБЕРІГАННЯ МЕДИЧНИХ ДАНИХ

BLOCKCHAIN TECHNOLOGY USAGE FOR DECENTRALIZED AND RELIABLE STORAGE OF MEDICAL DATA

Анотація. *Вступ. В епоху, що характеризується швидким оцифруванням майже кожного аспекту нашого життя, сфера охорони здоров'я стала свідком безпрецедентного прогресу. Цей прогрес, однак, породив унікальні виклики, особливо щодо безпечного, надійного та ефективного зберігання та управління великими обсягами конфіденційних медичних даних. Саме тут розкривається потенціал технології блокчейн, яка пропонує багатообіцяючі рішення для вирішення проблеми медичних даних. Саме в цьому контексті ця дана робота досліджує використання технології блокчейн для децентралізованого та надійного зберігання медичних даних.*

Технологія блокчейн, що базується на децентралізації, безпеці та незмінності, має потенціал для революції в галузі охорони здоров'я. Її здатність забезпечувати безпечні, перевірені та постійні методи запису даних має вирішальне значення для покращення цілісності та доступності медичних даних, зберігаючи при цьому конфіденційність пацієнтів. Крім того, децентралізований характер технології блокчейн знижує ризик втрати, крадіжки або корупції даних, які часто асоціюються з централізованими базами даних.

Мета. Метою дослідження є розкриття концептуальних підходів до реалізації інформаційної системи на основі блокчейну, що забезпечує децентралізоване та надійне зберігання медичних даних пацієнтів.

Результати. У науковій статті розкрито алгоритми, що сприятимуть послідовному та надійному децентралізованому зберіганню

медичних даних на багатьох вузлах, забезпечуючи цілісність та доступність даних. Забезпечено віддалену взаємодію між пацієнтами, медичними працівниками та сховищами медичних даних у безпечний спосіб із збереженням конфіденційності. Перераховано функціональні можливості смарт контракту, які регулюють доступ та модифікацію медичних даних у блокчейні, забезпечуючи дотримання вимог законодавства у сфері охорони здоров'я та прав пацієнтів на конфіденційність.

Перспективи. Впровадження запропонованої системи блокчейн в медичні заклади для забезпечення децентралізованого та надійного зберігання медичних даних пацієнтів, дозволивши здійснювати надійний моніторинг цих записів, зберігаючи конфіденційність та автентичність.

Ключові слова: *блокчейн, зберігання медичних даних, децентралізація, безпека даних, криптографія, приватні та публічні ключі.*

Summary. *Introduction. In an era characterized by the rapid digitization of almost every aspect of our lives, the healthcare industry has witnessed unprecedented progress. This progress, however, has given rise to unique challenges, especially with regard to the safe, secure, and efficient storage and management of large volumes of sensitive healthcare data. This is where the potential of blockchain technology comes into play, offering promising solutions to the healthcare data challenge. It is in this context that this paper explores the use of blockchain technology for decentralized and secure storage of medical data.*

Based on decentralization, security, and immutability, blockchain technology has the potential to revolutionize the healthcare industry. Its ability to provide secure, verifiable, and permanent methods of recording data is crucial to improving the integrity and accessibility of medical data while maintaining patient privacy. In addition, the decentralized nature of blockchain technology

reduces the risk of data loss, theft, or corruption often associated with centralized databases.

Purpose. The purpose of the study is to reveal conceptual approaches to the implementation of a blockchain-based information system that provides decentralized and reliable storage of patient medical data.

Results. The scientific article reveals algorithms that will facilitate consistent and reliable decentralized storage of medical data on many nodes, ensuring data integrity and availability. Remote interaction between patients, healthcare providers, and medical data stores is ensured in a secure manner while maintaining confidentiality. We list the functionalities of a smart contract that regulate access to and modification of medical data in the blockchain, ensuring compliance with healthcare legislation and patients' privacy rights.

Discussion. Implementation of the proposed blockchain system in medical institutions to ensure decentralized and secure storage of patients' medical data, allowing for reliable monitoring of these records while maintaining confidentiality and authenticity.

Key words: *Blockchain, medical data storage, decentralization, data security, cryptography, private and public keys.*

Постановка проблеми. Революційна інновація, що народилася у 2008 році під загадковим псевдонімом Сатоші Накамото, технологія блокчейн обіцяє змінити такі галузі, як фінанси, охорона здоров'я та логістика. Її назва влучно відображає її основну структуру: окремі пакети даних ("блоки"), з'єднані ланцюжком, забезпечують незмінну цілісність даних і прозоре ведення обліку. Це робить блокчейн наріжним каменем безпечних та ефективних цифрових транзакцій.

За своєю суттю, блокчейн – це розподілений, децентралізований реєстр, який реплікує записи про транзакції на численних комп'ютерах. Це робить дані незмінними, гарантуючи автентичність цифрових активів.

Уявіть собі спільний блокнот, який не належить одній людині, а ретельно підтримується всією мережею. Кожна "сторінка" (блок) містить набір транзакцій, і з кожним новим записом копія кожного учасника оновлюється одночасно. Таке колективне управління реєстром відоме як технологія розподіленого реєстру (DLT) [1].

Постановка проблеми полягає в необхідності створення децентралізованої та надійної системи зберігання медичних даних. У сучасному ландшафті охорони здоров'я існує кілька викликів, які роблять це питання нагальним:

- **Відсутність децентралізації**. Традиційні системи охорони здоров'я зазвичай зберігають дані про пацієнтів у централізованих базах даних. Така централізація створює кілька проблем. По-перше, вона створює єдину точку відмови; якщо центральна база даних буде скомпрометована, всі дані в ній опиняться під загрозою. По-друге, це часто призводить до ізоляції даних, коли цінні дані про пацієнтів ізольовані в системі одного медичного закладу і не можуть бути легко поширені або доступні для інших.
- **Інтероперабельність**. Деяким системам бракує інтероперабельності, оскільки існують випадки в яких різні відділень однієї лікарні не можуть взаємодіяти одна з одною. Тож ви можете собі уявити рівень складності, коли системи різних постачальників медичних послуг повинні взаємодіяти одна з одною.
- **Історії хвороби**. У випадку невідкладних станів або якщо пацієнт хоче змінити постачальника медичних послуг, для нього стає складним завданням отримати свою історію хвороби та надати її новому постачальнику послуг. Всі діагностичні тести доводиться проводити заново, щоб точно визначити проблему, що призводить до затримки лікування та подальшого поглиблення проблеми.
- **Ефективне використання телемедицини**. Телемедицина - це надання медичної допомоги пацієнтам на відстані за допомогою телефонів,

комп'ютерів тощо. Вона дозволяє медичним працівникам оцінювати, діагностувати та лікувати пацієнтів без необхідності особистого візиту. Однак щоразу, коли пацієнт звертається до лікаря онлайн, він повинен заповнити всі дані своєї історії хвороби. Для пацієнтів не існує ефективного способу ефективно ділитися своїми медичними даними з лікарем за допомогою дистанційних технологій [2].

Однак технологія блокчейн може забезпечити безпечний і стійкий спосіб обміну медичними даними пацієнтів, зберігаючи при цьому контроль пацієнтів над своїми даними. Вона стоїть порозі революції в секторі охорони здоров'я, запроваджуючи безпечну, децентралізовану і незмінну основу для зберігання та обміну медичними даними, вирішуючи кілька основних проблем, включаючи безпеку, інтероперабельність, управління згодою та цілісність даних [3].

Аналіз останніх досліджень і публікацій. Досліджуючи різні застосування технологій у сфері охорони здоров'я, ми помітили прогалину у зручних, інтегрованих з веб-сайтами блокчейн-рішеннях, орієнтованих на сектор охорони здоров'я. Існуючі системи, як, наприклад, додаток Інтернету речей для зберігання і передачі мультимедійних даних Rathee та ін. [4], часто зосереджуються на конкретних функціональних можливостях без урахування загального користувацького досвіду і безперешкодної інтеграції з існуючою інфраструктурою. Це може призвести до перешкод у впровадженні та обмежити трансформаційний потенціал цих технологій.

Запропонована нами система має на меті подолати цю прогалину, пропонуючи нову архітектуру, яка використовує притаманні блокчейну сильні сторони, такі як незмінність та прозорість даних, надаючи при цьому пріоритет зручності для користувача та інтеграції з веб-сайтами. Цей підхід черпає натхнення в поєднанні потенціалу децентралізації та смарт-контрактів, як це досліджували Шарма та ін. [5] в своїй архітектурі електронної охорони здоров'я. Їх робота підкреслює переваги такого

підходу з точки зору підвищення ефективності та безпеки в порівнянні з традиційними методами.

Крім того, ми вирішуємо проблеми, пов'язані з конфіденційністю та безпекою даних, використовуючи такі механізми, як концепція сертифікатів на основі блокчейну Poorni та ін. [6] для посиленої автентифікації та хмарна стратегія Pariselvam і Swarnamukhi для багаторівневого шифрування та контролю доступу [7]. Ці стратегії ґрунтуються на фундаментальних аспектах безпеки блокчейну, які обговорюються Агбо та ін. в їхньому аналізі додатків для охорони здоров'я [8].

Орієнтація нашої системи на зручність для користувача і доступ до даних в режимі реального часу відповідає цілям кібер-фізичної системи Шарми і Раджіва для передачі даних в критично важливих сферах охорони здоров'я [9]. Забезпечуючи віддалений моніторинг пацієнтів і своєчасне втручання, ми прагнемо поліпшити результати охорони здоров'я, подібно до бачення Ламбая і Паккіра Мохідіна щодо використання великих обсягів медичних даних [10].

Крім того, вирішуючи проблеми конфіденційності та безпеки за допомогою наскрізної архітектури та надійних механізмів захисту даних, ми прагнемо подолати обмеження, визначені Zalloum і Alamleh в їхньому аналізі існуючих платформ електронної охорони здоров'я [11]. Наш підхід також включає ефективні протоколи автентифікації, натхненний роботою Хоссейна та ін. з розробки блокчейну для систем електронної охорони здоров'я [12].

Таким чином, запропонована нами система заповнює критичну прогалину в секторі охорони здоров'я, пропонуючи зручне, інтегроване з веб-сайтом блокчейн-рішення, яке ставить на перше місце ефективність, безпеку та зручність для пацієнтів. Спираючись на ідеї та досягнення, представлені в попередніх дослідженнях, ми прагнемо революціонізувати

систему охорони здоров'я та покращити результати лікування пацієнтів завдяки трансформаційній силі технології блокчейн.

Метою статті є розкриття концептуальних підходів до реалізації інформаційної системи на основі блокчейну, що забезпечує децентралізоване та надійне зберігання медичних даних пацієнтів.

Виклад основного матеріалу. У зв'язку з тим, що зберігання великих обсягів даних у блокчейні є дуже дорогим та енергоємним, для зберігання даних буде використано одноранговий децентралізований протокол для зберігання даних на основі блокчейну – IPFS. На відміну від звичайних систем, де ресурси розміщуються за їхніми адресами, IPFS ідентифікує дані на основі їхнього вмісту. Вона використовує унікальний підхід, коли кожен тип контенту, будь то відео, зображення або статті, ідентифікується криптографічним хешем, подібним до цифрового відбитка пальця. Цей хеш слугує унікальним ідентифікатором для кожного файлу. На практиці, шукаючи певний файл, користувачі звертаються до мережі IPFS із запитом на файл, пов'язаний з певним хешем. Одноранговий партнер, який володіє цим файлом, відповідає, полегшуючи передачу файлу. Винахідливість IPFS полягає у функції хешування, яка забезпечує цілісність даних. Отримавши файл, користувачі можуть перевірити його автентичність, порівнявши оригінальний запитуваний хеш з хешем отриманого файлу. Збіг підтверджує, що файл є точним і незмінним [13].

Крім того, механізм хешування IPFS суттєво сприяє дедуплікації даних. Це означає, що будь-який файл, незалежно від його природи, при завантаженні генерує унікальний хеш. Якщо завантажується інший файл з ідентичним вмістом, він генерує такий самий хеш, таким чином запобігаючи надмірності. Цей аспект не лише економить місце в сховищі, але й підвищує ефективність мережі. Крім того, фреймворк IPFS підтримує більш стійкий та ефективний метод обробки даних, що сприяє загальній стійкості та надійності екосистеми блокчейну

Для взаємодії з блокчейном будуть використання самодостатні контракти, умови яких закодовані безпосередньо в програмному забезпеченні. Працюючи на розподіленій і децентралізованій платформі блокчейн, вони уможливлюють довірчі угоди та контракти між різними невідомими сторонами, оминаючи потребу в центральному нагляді, традиційних правових системах або зовнішніх методах реалізації. Вони роблять транзакції відстежуваними, прозорими та незворотними.

Дані про здоров'я пацієнтів, які вирішили взяти участь у блокчейні, будуть зашифровані та зберігатися в захищеній розподіленій файловій системі IPFS, що не належить до блокчейну. В той час як всі транзакції, що стосуються запитів ЕМК, обмінів та посилань на дані ЕМК зберігатимуться в головному блокчейні.

У контексті технології блокчейн для децентралізованого та надійного зберігання медичних даних смарт-контракти відіграють вирішальну роль в автоматизації процесів, зберіганням метаданих для доступу до даних ЕМК, що зберігаються в IPFS та надання, анулювання або відмову надавачам медичних послуг у доступі до отримання даних пацієнтів.

Всі користувачі, такі як пацієнти та медичні працівники, можуть стати частиною мережі блокчейну, створивши крипто гаманець, який буде використовуватись для ідентифікації та підтвердження транзакцій. Таким чином, кожному користувачеві присвоюється унікальний ідентифікатор, представлений хеш-значенням, яке також називається адресою облікового запису. Генеруються два ключі: приватний і публічний. Користувач зберігає приватний ключ у таємниці, а публічний ключ - це адреса облікового запису, якою можна ділитися. Закритий ключ повинен підписувати будь-яку транзакцію, пов'язану з адресою акаунта. Транзакцію можна визначити як процес завантаження, оновлення, видалення або обміну даними ЕМК. Усі транзакції повинні забезпечувати відповідність публічного та приватного ключів до того, як транзакції будуть записані в блокчейні [14].

Після реєстрації в системі яка розробляється лікарі або пацієнти можуть завантажувати свої медичні записи в систему (рис.1). Електронні медичні картки пацієнтів, а також дані про їхні візити, рецепти, рахунки тощо будуть зашифровані та зберігатися в IPFS. Після того, як документи завантажуються в IPFS, адреса збережених документів зберігається в смарт-контрактах. Таким чином, кожного разу, коли завантажується новий документ, в блокчейні зберігатиметься хеш запису IPFS, а не самі дані, що в кінцевому підсумку знижує вартість кожної транзакції.

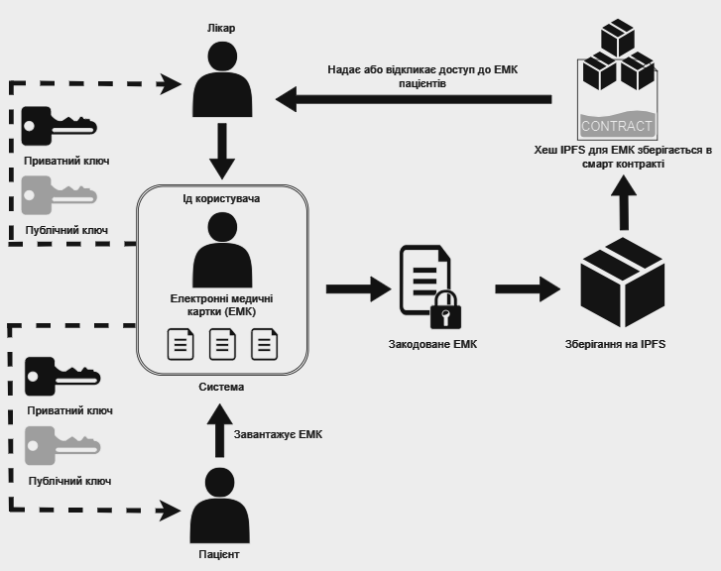

Рис. 1. Діаграма варіантів використання системи ЕМК

Джерело: авторська розробка

Результати роботи. Застосовуючи наведену вище концепцію створення медичної інформаційної системи на платформі блокчейн, були розроблені програмні засоби, які підтримують обмін та зберігання медичної інформації та даних в закладах охорони здоров'я та між ними. Їх апробація показала значну ефективність реалізованих процесів, як при захисті персональних даних, так і для реалізації принципів інтероперабельності.

Нижче наведені приклади реалізації системи.

- **Домашня сторінка**

Нижче показано домашню сторінку системи (рис. 2). Лікарі та пацієнти потребують під'єднання крипто гаманця, щоб отримати доступ до всіх сторінок системи.

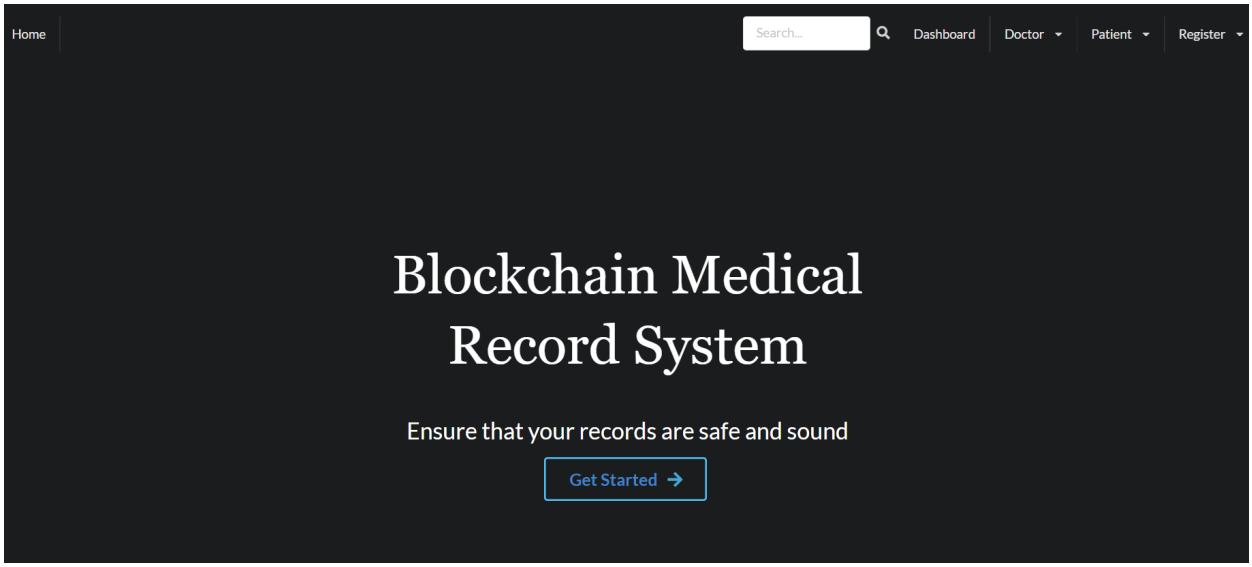

Рис. 2. Домашня сторінка системи

Джерело: авторська розробка

- **Дошка**

Сторінка з інформацією про систему (рис. 3), на якій можемо побачити скільки пацієнтів долучилися до платформи цього місяця, загальну кількість пацієнтів, лікарів та наданання доступу на використання даних користувачів.

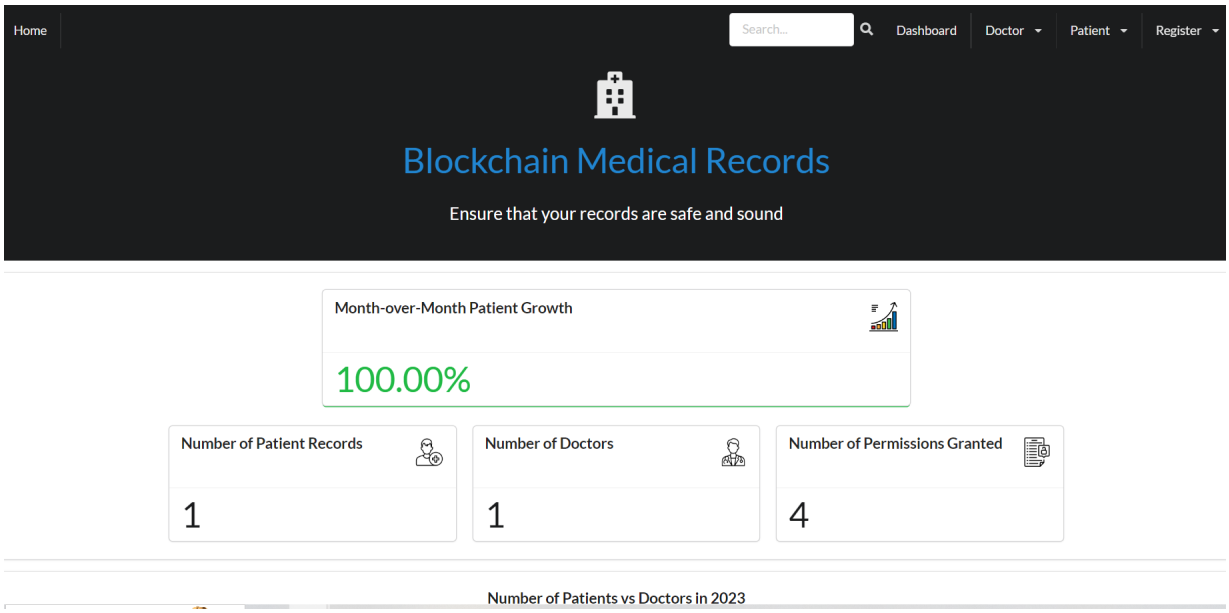

Рис. 3. Сторінка з статистикою системи

Джерело: авторська розробка

- **Реєстрація лікаря**

На рис. 4 показано процес реєстрації лікаря. Форма для заповнення даних про лікаря, як ім'я, дата народження, стать, номер мобільного телефону та спеціальність.

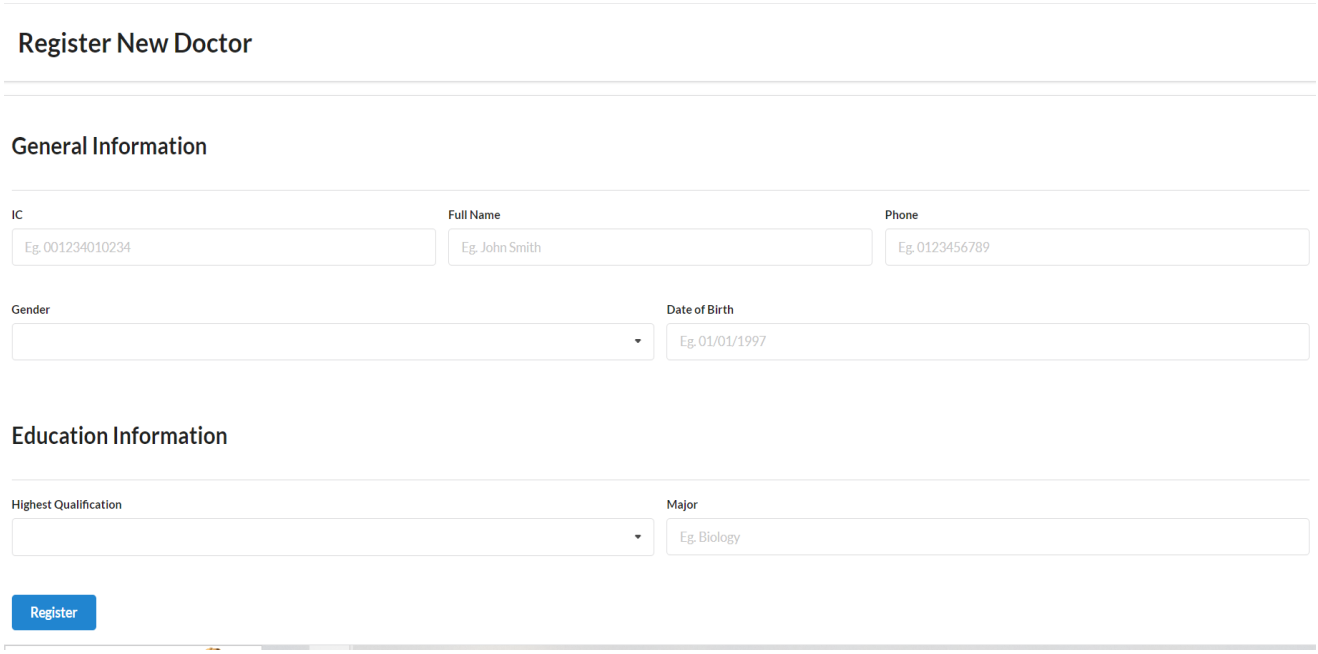

Рис. 4. Форма реєстрації лікаря

Джерело: авторська розробка

Через крипто гаманець MetaMask система отримуватиме повідомлення з підтвердженням аутентифікації. Для подальшого кодування та декодування даних, користувач повинен надати доступ на використання публічного ключа шифрування.

- **Реєстрація пацієнта**

Нижче зображено модуль реєстрації пацієнта (рис. 5), який вимагає введення інформації про пацієнта, такої як ім'я, номери телефонів пацієнта та контакту на випадок надзвичайних ситуацій, стать, дата народження, ріст та вага. Після заповнення всіх полів необхідною інформацією користувач повинен натиснути кнопку "Зареєструватися", щоб зберегти дані.

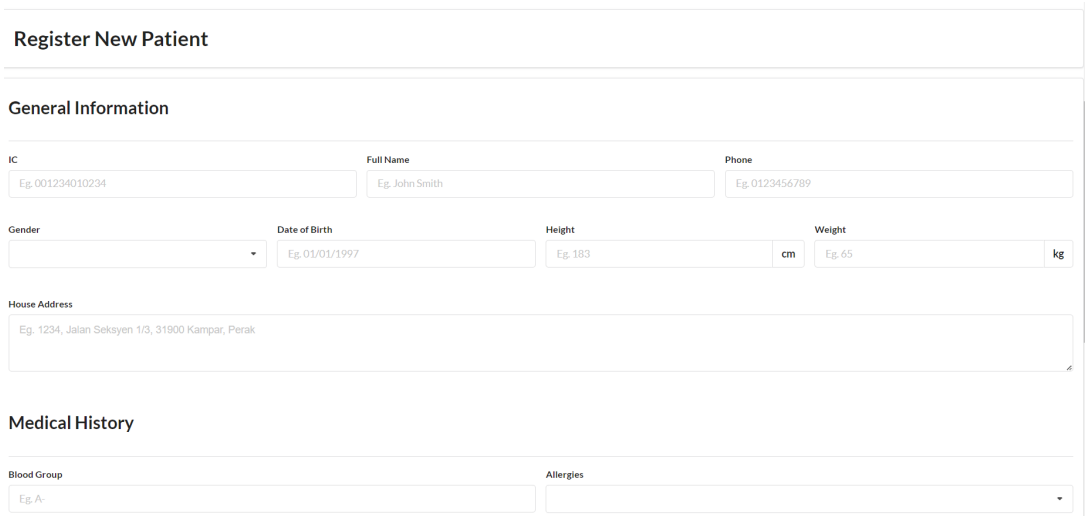

Рис. 5. Форма реєстрації пацієнта

Джерело: авторська розробка

- **Панель лікаря**

Перегляд та редагування інформації лікарем. Для перегляду інформації лікар повинен підтвердити запит на декодування даних, які були закодовані при реєстрації. Після підтвердження декодування, лікар може переглядати інформацію про себе, таку як ім'я, область спеціалізації та кваліфікація (рис. 3).

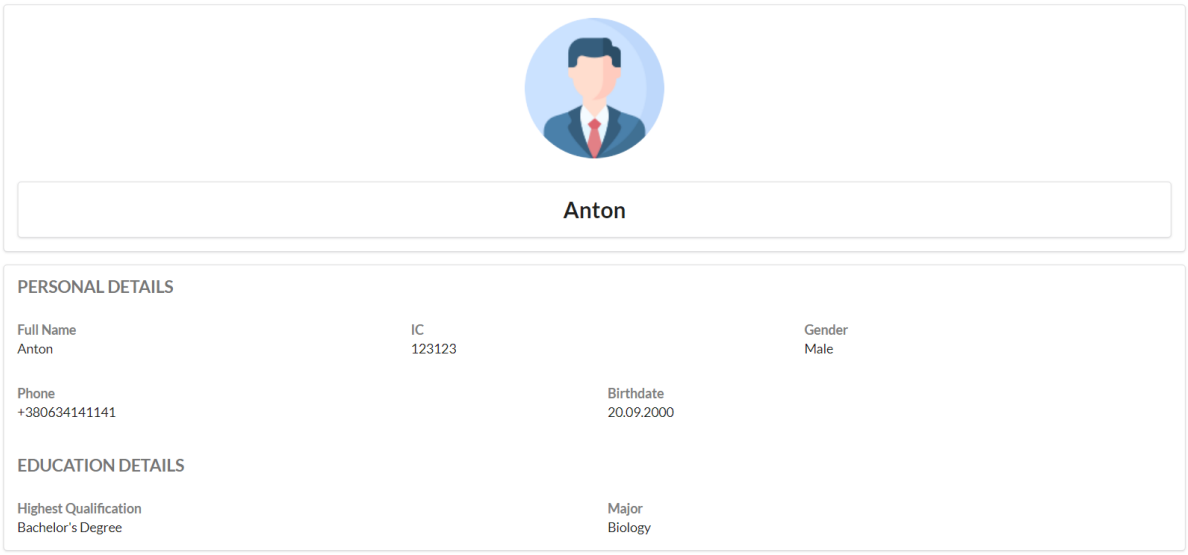

Рис. 6. Картка з інформацією лікаря

Джерело: авторська розробка

- **Панель пацієнта**

Для перегляду інформації пацієнт повинен підтвердити запит на декодування даних, які були закодовані при реєстрації, таким самим чином як лікар. Нижче показано медичну карту пацієнта (рис. 7), яку може бачити пацієнт та тільки ті користувачі, яким пацієнт надав доступ до своїх даних.

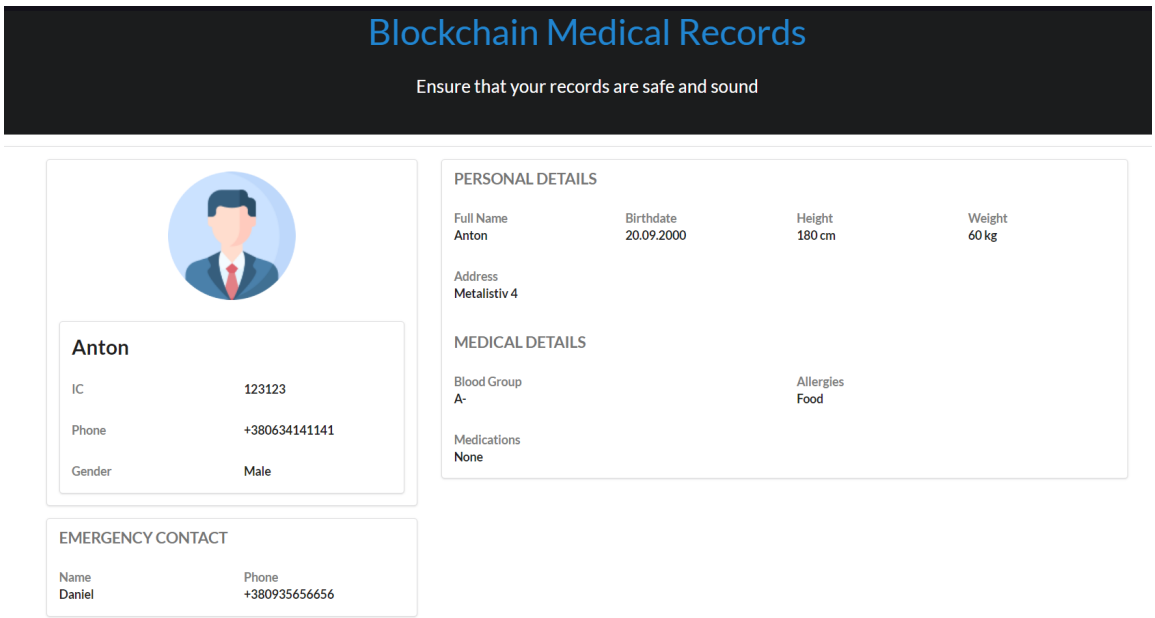

Рис. 7. Картка з інформацією пацієнта

Джерело: авторська розробка

- **Надання доступу до даних пацієнта**

Процес надання доступу до даних пацієнта іншому користувачу (рис. 8), для цього користувач повинен бути зареєстрований у системі, що б при введенні адреси гаманця система могла розпізнати кому буде надано доступ.

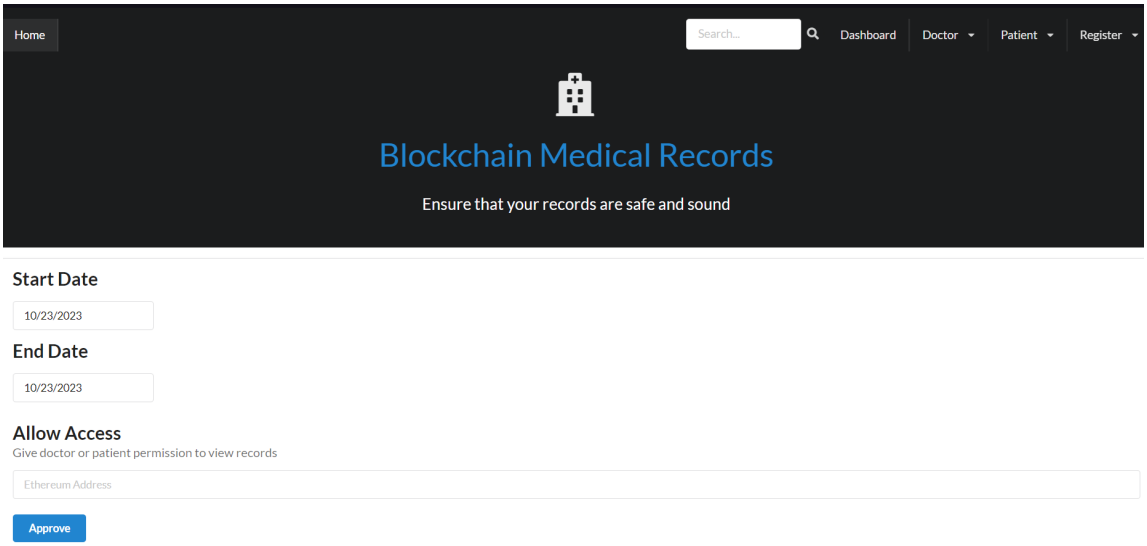

Рис. 8. Форма надання доступу до даних пацієнта

Джерело: авторська розробка

- **Відклик доступу до даних пацієнта**

Метод відклику доступу до даних пацієнта (рис. 9), для цього пацієнт повинен надати адресу гаманця користувача, якому у подальшому доступ до даних пацієнта буде відмовлено.

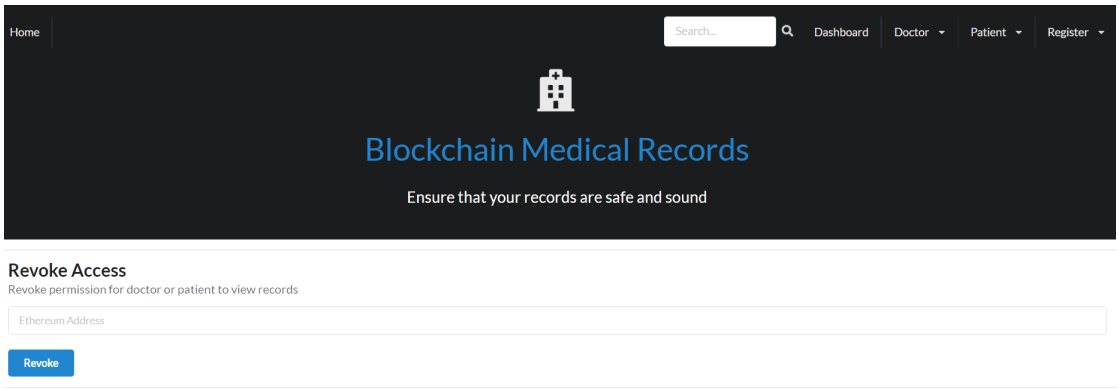

Рис. 9. Форма відклику доступу до даних пацієнта

Джерело: авторська розробка

Висновки. Теоретичне дослідження цієї роботи підкреслило революційний потенціал технології блокчейн в управлінні медичними

даними. Її здатність децентралізувати, захистити та впорядкувати зберігання та обмін медичними даними може вирішити багато існуючих проблем у секторі охорони здоров'я.

В основі цієї потенційної трансформації лежить унікальний набір характеристик блокчейну, який включає децентралізацію, незмінність, прозорість і криптографічну безпеку. Ці характеристики були детально розглянуті, збагативши наше розуміння того, наскільки вони є фундаментальними для застосування блокчейну в охороні здоров'я.

Смарт-контракти, ключові компоненти блокчейну, мають потенціал для революційної зміни різних процесів у сфері охорони здоров'я. Від управління згодою пацієнта до автоматизації виставлення рахунків і обробки претензій, ці самодостатні контракти можуть відкрити еру підвищеної ефективності та безпеки в охороні здоров'я, що призведе до економії коштів і підвищення рівня задоволеності пацієнтів.

Запропонована система дозволяє пацієнту надавати та відкликати будь-який дозвіл на доступ до даних одним дотиком. Завдяки смарт-контрактам цю автоматизацію стало набагато простіше впровадити. Криптографічні методи шифрування системи, які неможливо зламати, забезпечать безпеку і надійність Таким чином, технологія блокчейн, досліджена в цій статті, демонструє значний потенціал для революції в зберіганні та обміні медичними даними, забезпечуючи децентралізовану, безпечну та надійну систему, яка дозволяє пацієнтам контролювати свої власні дані. Проте, залишаються значні виклики, включаючи гарантування конфіденційності, досягнення сумісності з існуючими системами та подолання обмежень масштабованості існуючих блокчейн-платформ. Прототип, запропонований в цій статті, означає рух до майбутнього, де технологія блокчейн є фундаментальною для охорони здоров'я. Однак подальші дослідження і розробки мають вирішальне значення для повного розкриття цього потенціалу. Закладаючи основу для таких майбутніх

досліджень, ми сподіваємося, що ця стаття стане трампліном для подальших досліджень у цій повній надій і життєво важливій сфері.

Література

1. Shuchih Ernest Chang, Yi Chian Chen Blockchain in Health Care Innovation: Literature Review and Case Study from a Business Ecosystem Perspective. *J Med Internet Res.* 2020. 22(8). e19480. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7490679/ (дата звернення: 20.10.2023).
2. Zhijie Sun, Dezhi Han, Dun Li, Xiangsheng Wang, Chin-Chen Chang, Zhongdai Wu A blockchain-based secure storage scheme for medical information. *EURASIP Journal on Wireless Communications and Networking.* 2022. URL: https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-022-02122-6 (дата звернення: 20.10.2023).
3. Gupta M. PR wallet based blockchain access protocol to secure EHRs. *Blockchain and IoT Integration, Auerbach Publications*. 2021. P. 65–76. URL: https://wvvw.easychair.org/publications/preprint_download/3Lwj (дата звернення: 20.10.2023).
4. Rathee G., Sharma A., Saini H., Kumar R., Iqbal R. A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. *Multimedia Tools and Applications*. 2020. Vol. 79, No. 15-16. P. 9711–9733. URL: https://link.springer.com/article/10.1007/s11042-019-07835-3 (дата звернення: 20.10.2023).
5. Sharma Ashutosh, Sarishma Dangi, Ravi Tomar, Naveen Chilamkurti, Byung-Gyu Kim Blockchain based smart contracts for internet of medical things in e-Healthcare. *Electronics.* 2020. Vol. 9, No. 10. P. 1609. URL: https://www.mdpi.com/2079-9292/9/10/1609 (дата звернення: 20.10.2023).

6. Poorni R., Lakshmanan M., Bhuvaneswari S. DIGICERT: a secured digital certificate application using blockchain through smart contracts. *International Conference on Communication and Electronics Systems*. Coimbatore, India, 2019. P. 215–219. URL: https://ieeexplore.ieee.org/abstract/document/9002576 (дата звернення: 20.10.2023).
7. Pariselvam S., Swarnamukhi M. Encrypted cloud based personal health record management using DES scheme. *International Conference on System, Computation, Automation and Networking (ICSCAN)*. Pondicherry, India, 2019. P. 1–6, URL: https://ieeexplore.ieee.org/abstract/document/8878773 (дата звернення: 20.10.2023).
8. Agbo C. C., Mahmoud Q. H., Eklund J. M. Blockchain technology in healthcare: a systematic review. *Multidisciplinary Digital Publishing Institute, In Healthcare.* 2019. Vol. 7, No. 2. P. 56. URL: https://www.mdpi.com/2227-9032/7/2/56 (дата звернення: 20.10.2023).
9. Sharma Ashutosh, Kumar Rajiv Service level agreement and energy cooperative cyber physical system for quickest healthcare services. *Journal of Intelligent & Fuzzy System.* 2019. Vol. 36, No. 5. P. 4077–4089. URL: https://content.iospress.com/articles/journal-of-intelligent-and-fuzzy-systems/ifs169968 (дата звернення: 20.10.2023).
10. Lambay M. A., Pakkir Mohideen S. Big data analytics for healthcare recommendation systems. *International Conference on System, Computation, Automation and Networking (ICSCAN).* Pondicherry, India, 2020. P. 1–6. URL: https://ieeexplore.ieee.org/abstract/document/9262304 (дата звернення: 20.10.2023).
11. Zalloum M., Alamleh H. Privacy preserving architecture for healthcare information systems. *International Conference on Communication, Networks and Satellite (Comnetsat).* Batam, Indonesia, 2020. P. 429–432.

URL: https://ieeexplore.ieee.org/abstract/document/9328985 (дата звернення: 20.10.2023).

12. Hossein K. M., Esmaeili M. E., Dargahi T., Khonsari A. Blockchain-based privacy-preserving healthcare architecture. *Canadian Conference of Electrical and Computer Engineering (CCECE).* Edmonton, AB, Canada, 2019. P. 1–4. URL: https://ieeexplore.ieee.org/abstract/document/8861857 (дата звернення: 20.10.2023).
13. Jin Sun, Xiaomin Yao, Shangping Wang, Ying Wu. Blockchain-Based Secure Storage and Access Scheme for Electronic Medical Records in IPFS. 2020. URL: https://www.researchgate.net/publication/340155316_Blockchain-Based_Secure_Storage_and_Access_Scheme_For_Electronic_Medical_Records_in_IPFS (дата звернення: 20.10.2023).
14. Hong-Bing Shu, Ping Qi, Yongqing Huang, Fulong Chen, Dong Xie, Liping Sun. An Efficient Certificateless Aggregate Signature Scheme for Blockchain-Based Medical Cyber Physical Systems. 2020. URL: https://www.mdpi.com/1424-8220/20/5/1521/pdf?version=1583841418 (дата звернення: 20.10.2023).

References

1. Shuchih Ernest Chang, Yi Chian Chen Blockchain in Health Care Innovation: Literature Review and Case Study from a Business Ecosystem Perspective. J Med Internet Res. 2020. 22(8). e19480. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7490679/ (date of access: 20.10.2023).
2. Zhijie Sun, Dezhi Han, Dun Li, Xiangsheng Wang, Chin-Chen Chang, Zhongdai Wu A blockchain-based secure storage scheme for medical information. EURASIP Journal on Wireless Communications and Networking. 2022. URL: https://jwcn-

eurasipjournals.springeropen.com/articles/10.1186/s13638-022-02122-6 (date of access: 20.10.2023).

3. Gupta M. PR wallet based blockchain access protocol to secure EHRs. Blockchain and IoT Integration, Auerbach Publications. 2021. P. 65–76. URL: https://wvvw.easychair.org/publications/preprint_download/3Lwj (date of access: 20.10.2023).
4. Rathee G., Sharma A., Saini H., Kumar R., Iqbal R. A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. Multimedia Tools and Applications. 2020. Vol. 79, No. 15-16. P. 9711–9733. URL: https://link.springer.com/article/10.1007/s11042-019-07835-3 (date of access: 20.10.2023).
5. Sharma Ashutosh, Sarishma Dangi, Ravi Tomar, Naveen Chilamkurti, Byung-Gyu Kim Blockchain based smart contracts for internet of medical things in e-Healthcare. Electronics. 2020. Vol. 9, No. 10. P. 1609. URL: https://www.mdpi.com/2079-9292/9/10/1609 (date of access: 20.10.2023).
6. Poorni R., Lakshmanan M., Bhuvaneswari S. DIGICERT: a secured digital certificate application using blockchain through smart contracts. International Conference on Communication and Electronics Systems. Coimbatore, India, 2019. P. 215–219. URL: https://ieeexplore.ieee.org/abstract/document/9002576 (date of access: 20.10.2023).
7. Pariselvam S., Swarnamukhi M. Encrypted cloud based personal health record management using DES scheme. International Conference on System, Computation, Automation and Networking (ICSCAN). Pondicherry, India, 2019. P. 1–6, URL: https://ieeexplore.ieee.org/abstract/document/8878773 (date of access: 20.10.2023).
8. Agbo C. C., Mahmoud Q. H., Eklund J. M. Blockchain technology in healthcare: a systematic review. Multidisciplinary Digital Publishing

Institute, In Healthcare. 2019. Vol. 7, No. 2. P. 56. URL: https://www.mdpi.com/2227-9032/7/2/56 (date of access: 20.10.2023).

9. Sharma Ashutosh, Kumar Rajiv Service level agreement and energy cooperative cyber physical system for quickest healthcare services. Journal of Intelligent & Fuzzy System. 2019. Vol. 36, No. 5. P. 4077–4089. URL: https://content.iospress.com/articles/journal-of-intelligent-and-fuzzy-systems/ifs169968 (date of access: 20.10.2023).
10. Lambay M. A., Pakkir Mohideen S. Big data analytics for healthcare recommendation systems. International Conference on System, Computation, Automation and Networking (ICSCAN). Pondicherry, India, 2020. P. 1–6. URL: https://ieeexplore.ieee.org/abstract/document/9262304 (date of access: 20.10.2023).
11. Zalloum M., Alamleh H. Privacy preserving architecture for healthcare information systems. International Conference on Communication, Networks and Satellite (Comnetsat). Batam, Indonesia, 2020. P. 429–432. URL: https://ieeexplore.ieee.org/abstract/document/9328985 (date of access: 20.10.2023).
12. Hossein K. M., Esmaeili M. E., Dargahi T., Khonsari A. Blockchain-based privacy-preserving healthcare architecture. Canadian Conference of Electrical and Computer Engineering (CCECE). Edmonton, AB, Canada, 2019. P. 1–4. URL: https://ieeexplore.ieee.org/abstract/document/8861857 (date of access: 20.10.2023).
13. Jin Sun, Xiaomin Yao, Shangping Wang, Ying Wu. Blockchain-Based Secure Storage and Access Scheme for Electronic Medical Records in IPFS. 2020. URL: https://www.researchgate.net/publication/340155316_Blockchain-Based_Secure_Storage_and_Access_Scheme_For_Electronic_Medical_Records_in_IPFS (date of access: 20.10.2023).

14. Hong-Bing Shu, Ping Qi, Yongqing Huang, Fulong Chen, Dong Xie, Liping Sun. An Efficient Certificateless Aggregate Signature Scheme for Blockchain-Based Medical Cyber Physical Systems. 2020. URL: https://www.mdpi.com/1424-8220/20/5/1521/pdf?version=1583841418 (date of access: 20.10.2023).