ДОДАТОК А
ГРАФІЧНИЙ МАТЕРІАЛ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Харківський національний університет радіоелектроніки

Проєктування та дослідження програмних компонентів системи обміну персональними даними на основі блокчейн

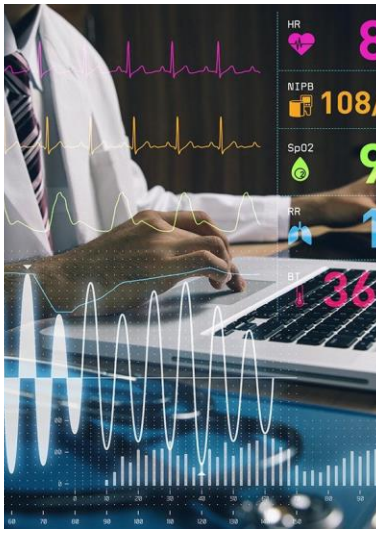
Виконав:
Студент групи СПм-22-3
Кулініч Д.В.

Науковий керівник:
Доц. каф. ЕОМ
Шматко О.В.

2024

Актуальність теми дослідження

- Ключові фактори:
  - Конфіденційність даних
  - Безпека
  - Інтероперабельність
  - Точність
  - Зниження витрат
- Інноваційні стартапи
  - Patientory
  - MedRec
  - SimplyVital Health



Об’єкт та предмет дослідження

- **Об'єктом дослідження** є система обміну персональними даними пацієнтів у сфері охорони здоров’я.

- **Предметом дослідження** є програмні компоненти, що базуються на блокчейн-технологіях, призначені для забезпечення безпеки, прозорості та ефективності обміну медичною інформацією.

Мета та задачі

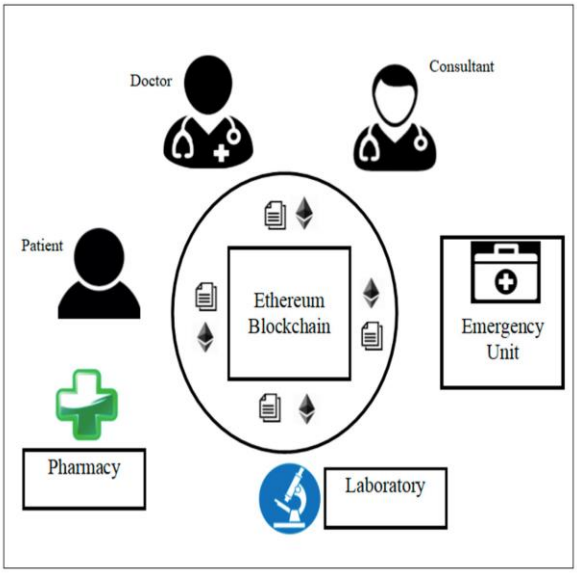
- **Метою даного дослідження** є забезпечення високого рівня безпеки та конфіденційності медичних даних, а також підвищення ефективності процесів у сфері охорони здоров'я за рахунок розробки програмних компонентів системи обміну персональними даними пацієнтів на основі блокчейн-технологій.

- Для досягнення поставленої мети необхідно вирішити такі **задачі**:
  - Дослідити існуючі підходи та рішення в галузі блокчейн-технологій для обміну медичними даними та виявити їх переваги та недоліки.
  - Виконати проєктування програмних компонентів системи обміну медичними даними на основі блокчейн, включаючи смарт-контракти та інтерфейс користувача.
  - Розробити програмні компоненти системи обміну медичними даними на основі блокчейн, включаючи смарт-контракти та інтерфейс користувача.
  - Провести дослідження та аналіз розроблених компонентів з метою визначення їх ефективності, надійності та безпеки.

Порівняння різних типів блокчейнів

Тип блокчейну	Децентралізація	Пропускна здатність	Витрати	Масштабованість
Державна мережа	Висока	Низька	Високі	Погана
Мережа консорціумів	Середня	Середня	Середні	Відмінна
Приватна мережа	Низька	Висока	Низькі	Відмінна
Гібридна мережа	-	-	Низькі	Велика

Смарт- контракти



Порівняння систем зберігання даних на основі блокчейн

Посилання	Тип блокчейну	Методи зберігання	Шифрування даних
[23]	публічний	мережеве сховище	ні
[24]	публічний	автономне сховище	так
[25]	приватний	автономне сховище	так
[26]	гібридне	автономне сховище	ні
[27]	публічний	автономне сховище	так
[28]	публічний	автономне сховище	ні
[29]	публічний	автономне сховище	так

23 Kuo T, Zavaleta Rojas H, Ohno-Machado L. Comparison of blockchain platforms: a systematic review and healthcare examples. J Am Med Inform Assoc. 2019 May 01;26(5):462–478.
24. McGhin T, Choo KR, Liu CZ, He D. Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications. 2019 Jun;135:62–75.
25. Vazirani AA, O'Donoghue O, Brindley D, Meinert E. Implementing Blockchains for Efficient Health Care: Systematic Review. J Med Internet Res. 2019 Feb 12;21(2):e12439.
26. Hussien HM, Yasin SM, Udzir SNI, Zaidan AA, Zaidan BB. A Systematic Review for Enabling of Develop a Blockchain Technology in Healthcare Application: Taxonomy, Substantially Analysis, Motivations, Challenges, Recommendations and Future Direction. J Med Syst. 2019 Sep 14;43(10):320.
27. 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); August 22-24; Vienna, Austria. 2016. pp. 25–30.
28. Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. J Med Syst. 2016 Oct;40(10):218.
29. Roehrs A, da Costa Cristiano André, da Rosa Righi Rodrigo. OmniPHR: A distributed architecture model to integrate personal health records. J Biomed Inform. 2017 Jul;71:70–81.

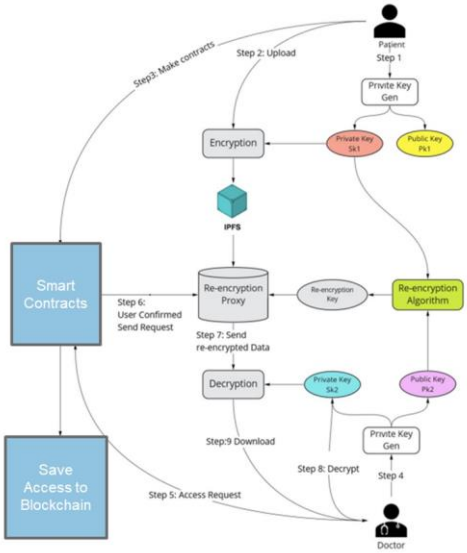
Функціональні вимоги

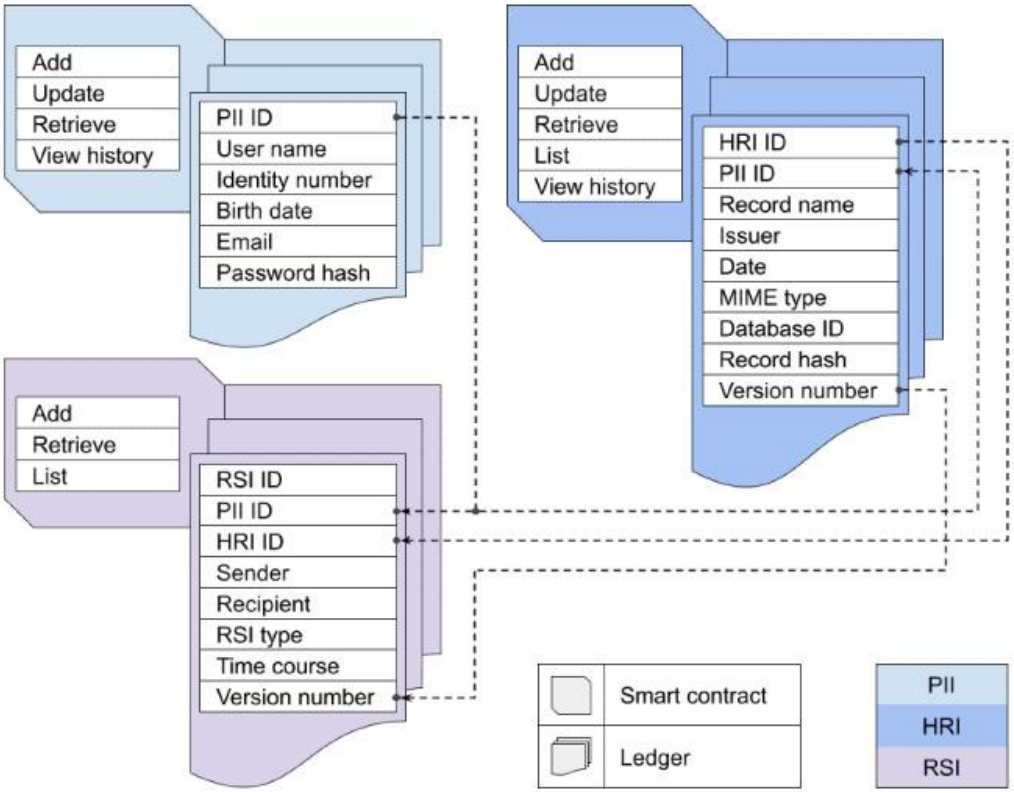
- **Функціональні вимоги:**
  - Пацієнти можуть зареєструватися та створити профіль із підтвердженням особи
  - Пацієнти можуть завантажувати медичні записи, такі як лабораторні аналізи, звіти про візуалізації і т.ін.
  - Пацієнти можуть надавати вибірковий доступ до записів конкретним постачальникам медичних послуг
  - Лікарі можуть запитувати доступ до історії хвороби пацієнта в дозволених цілях- Система забезпечує доступ до журналів і аудит всіх транзакцій
  - Пацієнти отримують повідомлення при доступі до їх даних або їх спільному використанні
  - Медичні організації можуть отримувати аналітичні дані

Нефункціональні вимоги

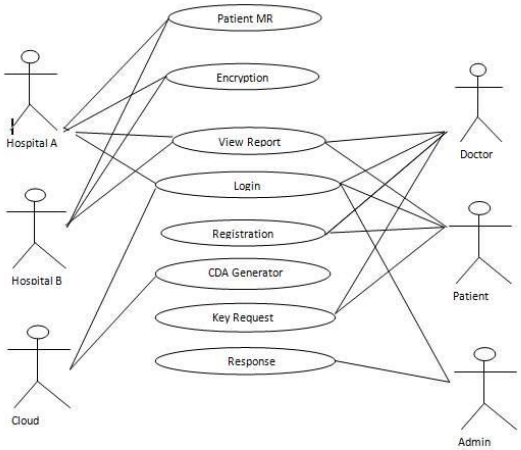
- **Нефункціональні вимоги:**
  - Система повинна підтримувати високу доступність - мінімальний час простою (не більше 40 хвилин)
  - Дані пацієнта повинні залишатися повністю конфіденційними та зашифрованими (використання проксі-шифрування)
  - Правила контролю доступу повинні суворо дотримуватися
  - Транзакції повинні оброблятися у встановлені терміни (не більше 5 с.)
  - Система повинна масштабуватися для підтримки декілька тисяч одночасних користувачів
  - Користувальницькі інтерфейси повинні бути інтуїтивно зрозумілими і зручними для користувача
  - Загальна затримка системи повинна становити менше 100 мс для більшості транзакцій
  - Рішення повинно інтегрувати такі стандарти, як HL7, fhir, ICD-10 і т. д.
  - Відповідність нормативним вимогам щодо конфіденційності медичних даних

Метод повторного шифрування через проксі (PRE)

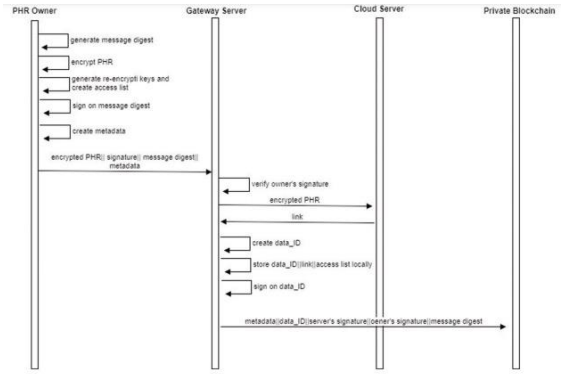




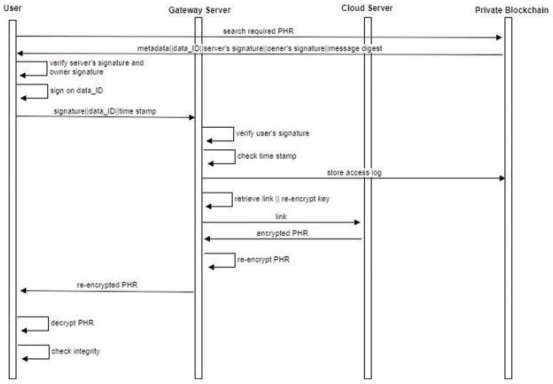
Діаграма варіантів використання



Діаграма послідовності

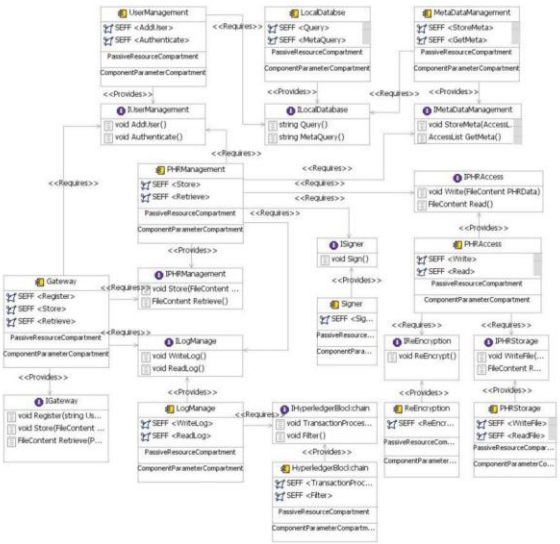


Діаграма послідовності для власника МД



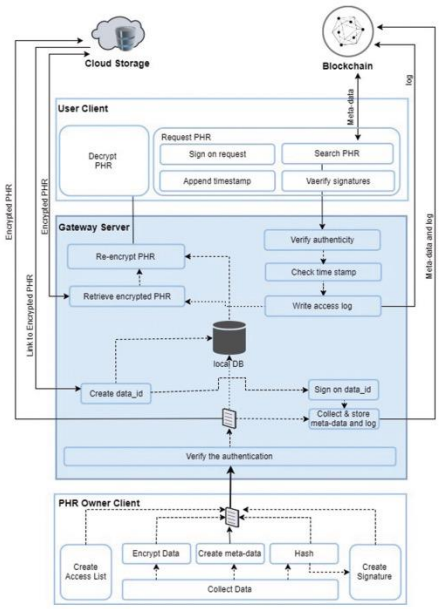
Діаграма послідовності запиту на отримання МД

Діаграма класів



Діаграма розгортання

Архітектурна модель системи (прототип)



Експериментальні дослідження

- **Параметри тестового середовища:**
  - процесор Intel Xeon E-2246g (12 МБ кеш-пам'яті, 3,60 ГГц, 6 ядер, 12 потоків)
  - графічний адаптер NVIDIA Quadro P1000
  - оперативна пам’ять об'ємом 16 ГБ
  - 64-розрядна операційна система Ubuntu 18.04.5 LTS.

- **Тестові данні:**
  - Пакети об’ємом 128Кб, 512 Кб;
  - Пакети об’ємом 2, 8, 32 і 128 МБ;

Аналіз отриманих результатів моделювання

Розмір даних	час хешування	час шифрування	Час генерації ключа повторного шифрування	Час підпису	Час відправки даних
128 КБ	10.29	91.18	24.16	1.16	152.73
512 КБ	18.24	94.01	24.66	1.15	173.87
2 МБ	40,63	101,19	26,15	1,18	268,95
8 МБ	65,60	142,03	26,88	1,16	421,67
32 МБ	241,80	303,79	27,00	1,31	645,70
128 МБ 1	946.10	1828.21	27.10	1.42	2200.36

Аналіз отриманих результатів моделювання

Розмір даних	Час перевірки підпису	Час завантаження	Час збереження локальної копії	Час входу на сервер	Час блокування
128 ГБ	0,07	157,41	31,57	1,24	3372,79
512 ГБ	0,07	221,65	24,66	1,15	3173,87
2 МБ	0,07	273,65	38,40	1,30	3365,34
8 МБ	0,08	457,51	33,82	1,49	3238,70
32 МБ	0.06	654.280	28.62	1.60	2935.02
128 МБ	0.07	2150.87	38.71	1.58	3381.05

Аналіз отриманих результатів моделювання

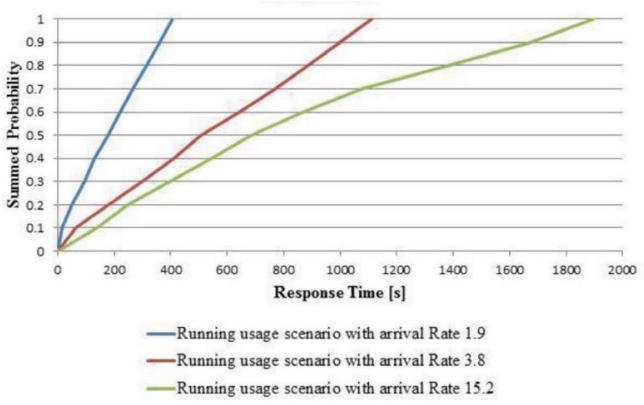
Розмір даних	Час пошуку МД по блокчейн	Час підтвердження підпису (власник, сервер)	Час підпису користувача	Час відправки запиту	Час розшифровки
128 КБ	785,69	0,07, 0,04	1,33	115,36	3,20
512 КБ	820,48	0,07, 0,04	1,29	124,30	6,04
2 МБ	751,15	0,07, 0,04	1,31	110,77	16,63
8 МБ	770,61	0,07, 0,04	1,23	136,25	59,41
32 МБ	823,37	0,07, 0,04	1,75	127,79	238,90
128 МБ	796,67	0,07, 0,04	1,39	128,77	1814,79

Аналіз отриманих результатів моделювання

Розмір даних	Час перевірки підпису користувача	Час збереження журналу в блокчейн	Час повторного шифрування	Час завантаження даних
128 КБ	0.11	3304.62	30.59	38.02
512 КБ	0.10	3288.55	31.50	78.27
2 МБ	0.10	3308.91	34.28	152.31
8 МБ	0.11	3398.48	58.75	214.84
32 МБ	0.13	3367.66	79.70	469.33
128 МБ	0.12	3372.62	80.65	1093.03

Аналіз отриманих результатів моделювання

$$= \frac{165000}{24} = \frac{165000}{3600 * 24} = \frac{165000}{86400} = 1 \text{ запи т/ с}$$



За темою роботи була опублікована наукова стаття

Висновки

- В роботі були сформульовані та вирішені наступні **задачі**:
  - Досліджено існуючі підходи та рішення в галузі блокчейн-технологій для обміну медичними даними та виявити їх переваги та недоліки.
  - Виконано проєктування програмних компонентів системи обміну медичними даними на основі блокчейн, включаючи смарт-контракти та інтерфейс користувача.
  - Розроблено програмні компоненти системи обміну медичними даними на основі блокчейн, включаючи смарт-контракти та інтерфейс користувача.
  - Проведено дослідження та виконано аналіз розроблених компонентів з метою визначення їх ефективності, надійності та безпеки.