Технічні науки

УДК 004.62:006.86

Коваленко Олександр Сергійович
доктор медичних наук, завідувач відділу
Міжнародний науково-навчальний центр
інформаційних технологій та систем НАН України

Гулін Іван Леонідович
студент
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»

Завражний Дмитро Костянтинович
студент
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»

Романюк Оксана Олександрівна
молодший науковий співробітник
Міжнародний науково-навчальний центр
інформаційних технологій та систем НАН України

ЗАСТОСУВАННЯ СУЧАСНИХ МЕТОДІВ ЗБЕРІГАННЯ ДАНИХ В ЕЛЕКТРОННІЙ ОХОРОНІ ЗДОРОВ'Я

Анотація. *В статті розглянуті приклади використання децентралізованих баз даних в медицині, проблеми та рішення використання блокчейну для передачі та управління медичної інформації та даних, що пов'язані з охороною здоров'я у програмному забезпеченні.*

Ключові слова: *блокчейн, система охорони здоров'я, безпека, self-sovereign identity.*

Вступ. Цифрова революція продовжує набирати оберти. Багато аспектів та процесів життя людини вже в якійсь мірі успішно пройшли цифрову трансформацію. Доставка речей, продаж послуг та речей, спілкування, новини, всі можливі редактори будь чого, та багато іншого вже реалізовано та використовується, з метою зробити життя людини простіше. Але і виклики існують досі. Багато інформаційних систем, що активно використовуються не відповідають принципам анонімності та контрольованості розповсюдження даних, що є важливими для користувачів. Рішення апелюють на те, що потрібна довіра для обміну ресурсами між учасниками процесів. Без контролю супервізорів постраждають усі – і користувачі, і організації.

Особиста інформація людей зберігається на централізованих серверах, що належать організаціям, і користувачі повинні підтримувати велику кількість особистих облікових записів, якими насправді не володіють, для взаємодії з різними платформами. Проблема полягає в тому, що ці організації мають доступ до інформації, яку можуть видаляти, змінювати, або розповсюджувати як вважають за потрібне.

З набуттям чинності нових суворих норм, організації зобов'язані докласти зусиль для реструктуризації своєї діяльності з обробки даних та зробити процеси ідентичності більш орієнтованими на користувачів; вони повинні бути в змозі довести, що вони досягли явної згоди перед тим, як збирати та використовувати особисту інформацію або ділитися нею з третьою стороною.

Це ставить людей, на відміну від централізованих постачальників послуг, посеред процесу ідентифікації та надає їм більше контролю. Але це жодним чином не забезпечує анонімність.

Крім того, особиста інформація досі зберігаються у вразливих централізованих базах даних - які мають достатню економічну цінність для зловмисників, щоб здійснити напади на них.

Саме з цих причин з'явилася і поширилась концепція self-sovereign identity (SSI). Системи SSI, як правило, розміщуються на блокчейнах, та мають на меті надати користувачам не лише адміністративні права, а й ексклюзивне право власності та контроль над їх особистими даними.

Інша мета SSI – електронний документообіг, який випливає з тверджень про повну власність своєї інформації користувачами. В системі довірені особи видають документи користувачам, а користувачі, можуть надати іншим довіреним особам, які в свою чергу, зможуть упевнитися, що цим даним можна довіряти завдяки криптографічним алгоритмам системи за принципом Zero-Knowledge Proof.

Поєднання таких особливостей надає багато можливостей покращення багатьох цифрових процесів, таких як медичний документообіг.

Блокчейн в медицині. Новітні технології розповсюджуються і на системи охорони здоров'я, що сприяє більш комфортній комунікації користувачів з усіма суб'єктами медичної галузі. Однак залишається багато викликів, зокрема тих, що стосуються єдиного управління записами електронної охорони здоров'я (EHR), які могли б дати змогу багатьом лікарям отримати доступ до повної історії хвороби свого пацієнта. Блокчейн може підтримувати уніфіковані записи, забезпечити поліпшення безпеки та конфіденційності.

Дані про здоров'я - найцінніший актив будь-якої системи охорони здоров'я. Ці дані розкидані по різних системах, а забезпечення обміну ними - це важливе питання для створення ефективної системи електронної охорони здоров'я. Для прикладу, пацієнт може відвідувати різних лікарів у різних медичних мережах з різними скаргами, і було б корисно кожному лікареві переглянути всю історію пацієнта. Крім того, централізоване розташування даних (наприклад, дані зберігаються на хмарі) може бути вразливим до нападу з ціллю викрадання даних. Окремі докази останніх

років показують, що дані про здоров'я продовжують залишатися прибутковою ціллю [1]. Загальнодержавний спільний доступ до медичної інформації також є складним, оскільки вимагає високого рівня сумісності.

В ідеальному світі пацієнти повинні не тільки володіти власними медичними записами, а й контролювати та обмінюватися власними даними без шкоди для безпеки та конфіденційності. Через децентралізований характер медичних записів, технологія блокчейн досить скоро отримала визнання в медицині. Починаючи з літа 2017 року, гіганти охорони здоров'я беруть участь у розробці блокчейну, будь то в об'єднанні зусиль консорціуму на кшталт Hyperledger, чи розробки власних продуктів. Паралельно, кількість публікацій у наукових базах даних зросла, що підкреслює потенціал блокчейну для покращення прозорості та безпеки при обміні медичними записами [2].

Платформи варіюються від загальних, до більш спеціалізованих, що визначають конкретні групи пацієнтів або медичних сфер. Наприклад, «Healthcoin» - це спеціалізована платформа на основі блокчейну для управління та забезпечення профілактики діабету другого типу. Користувачі взаємодіють із системою, подаючи свої біомаркери у блокчейн. Якщо біомаркер демонструє поліпшення, система нагороджує пацієнта так званими «Healthcoins», які можна використовувати для отримання державних податкових пільг та знижок до багатьох фітнес брендів [3].

Інший приклад використання блокчейну для конкретного лікування був представлений у статті [4] – стаття описує структуру даних, яка дозволить пацієнтам мати вільний та захищений доступ до медичних зображень без необхідності стороннього адміністратора. Рентгенологічні зображення не зберігаються всередині блокчейна через великий розмір; блок-транзакція пов'язує відкритий ключ з посиланням (URL) для встановлення джерела зображення. В статті [5] представлено аналогічну

спеціалізовану блокчейн-систему для дерматології, для зберігання зображень, що пов'язані з дерматологією, хоча тут все ж зберігаються зашифровані зображення в блокчейні.

У статті [6] розробили фреймфорк для управління та обміну електронними медичними записами, пов'язаних з онкологією. Оскільки блокчейн усуває посередника, фреймфорк має зменшити витрати, скоротити час роботи для обміну записів хворих на рак та покращити прийняття рішень щодо медичної допомоги.

Найбільший аспект системи охорони здоров'я – документообіг, втім, ще не має більш менш робочого прототипу додатку з блокчейном, хоча багато ідей вже обговорюються спільнотою.

Архітектура. Self-sovereign identity - рішення досить ефективно може бути використане для вдосконалення документообігу. Найбільш відома імплементація рішення – Hyperledger Indy, надає інструменти для забезпечення цифрових ідентичностей, що засновані на блокчейні. Важливою особливістю Hyperledger Indy є те, що це публічний блокчейн, який схвалений державами, де розробляються рішення на основі нього; на відміну від Corda або Fabric, які є приватними, хоч і схваленими.

Indy забезпечує екосистему програмного забезпечення для приватної, захищеної та потужної ідентичності. Indy дозволяє людям відповідати за рішення про власну конфіденційність та розголошення інформації, на відміну організаціям, які зберігають інформацію централізовано. Це дозволяє використовувати багато інновацій: договори про створення зв'язку між користувачами, нові процеси оплати послуг, функції управління активами та документами, відслідковування репутації, інтеграція з іншими технологіями тощо.

Indy використовує технологію розподіленої «книги» з відкритим кодом. Ці «книги» є формою бази даних, яка утворюється спільно всіма учасниками, а не гігантською базою даних з адміністратором. Результат -

надійне, публічне джерело веріфікованих даних, яке не контролюється жодним суб'єктом господарювання, надійне до збоїв у системі, стійке до злому і дуже несприйнятливе до диверсій ворожих суб'єктів [7].

В блокчейні зберігаються записи, що описують сутність об'єкта. Ці записи можуть включати: публічні ключи, схеми та їх визначення. Об'єкт асоціюється з DID (Decentralized Identifier), який є унікальним. Щоб підтримувати приватність об'єкт може мати багато DID.

Є два види DID – verinym та pseudonym. Перший асоціюється з об'єктом з точки зору системи. Це потрібно, щоб будь-які об'єкти могли впевнитись, що джерелом інформації, що надав користувач, є сторона, якій можна довіряти. По термінології цю сторону називають Trust Anchor. Як і в реальному житті, всі документи, що користувач отримав від довіреної сторони будуть дійсними для інших сторін. З цього виходить, що тільки trust anchor мають verinym, щоб бути розпізнаними іншими сторонами. Pseudonym з іншого боку – це ідентифікатор, що асоціюється з об'єктом для лише одного користувача. Тобто користувачі мають унікальні псевдоніми для кожного зв'язку. Це необхідно, щоб підтримувати приватність.

Кожен trust anchor може публікувати схеми. Схема – це опис, деякий шаблон документу, що може бути заповнений і виданий користувачам. Для того, щоб заповнити документ, trust anchor публікує своє визначення цієї схеми – саме визначення просто повідомляє, що цей trust anchor буде заповняти цю схему, так як заповняти можна будь які схеми, опубліковані в блокчейні (рис.1).

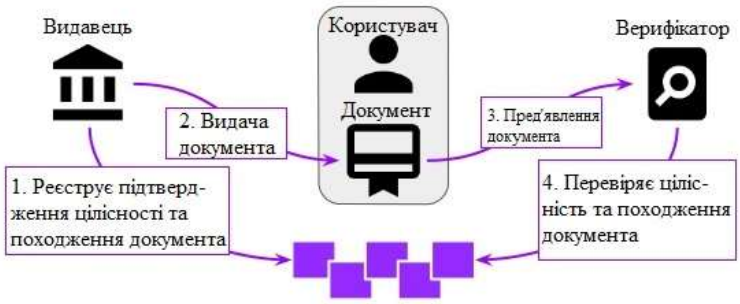

Рис. 1. Процес видачі та перевірки документів в системі

Hyperledger Indy надає клієнту, які використовують для підтримки обміну peer-to-peer, назву agent. Клієнти містять в собі гаманець з даними та псевдоніми (та verinym для trust anchor).

Виходячи з зазначеного вище, можна побудувати систему для обміну медичних документів. Є кілька нюансів, які треба дослідити:

1) Пацієнти мають отримати документи, що засвідчують особу.
2) Ці документи має видати якась довірена особа.
3) Лікарі мають створювати та видавати документи.

Вірогідним виглядає процес автентифікації, коли користувач при першому користуванні створює гаманець, встановлює контакт з державою (що є довіреною особою), висилає деяку унікальну інформацію про себе, після перевірки якої держава видає документи користувачу. Це може бути паспорт, ідентифікаційний код. Якщо держава розпізнала в цих даних лікаря, то ще може видати диплом та сертифікати. Лікар має видавати документи також, тому держава реєструє роль лікаря як trust anchor в блокчейні. Так як держава є trust anchor, вона може це зробити.

Лікар будь-яким чином пропонує встановити зв'язок з користувачами, після якого можна починати процес обміну документів та запитів на підтвердження особистості. Hyperledger Indy дозволяє створити запит на видачу часткової чи повної інформації, яка прописана в схемі. Держава заздалегідь створила схеми паспорту, ідентифікаційного коду,

диплому чи сертифікатів, де чітко приписала, які атрибути в неї входять. Тому лікар може запитати, наприклад, повне ім'я та ідентифікаційний код пацієнта, який, при згоді, видає лише частину інформації з документів, що необхідна лікарю. Лікар, завдяки криптографічним алгоритмам Indy зможе прослідкувати, що ці дані були видані державою, а не кимось іншим. Так само процес може відбуватися в зворотному напрямку, пацієнт зробить запит на видачу часткової інформації з диплому чи сертифікатів лікаря, щоб впевнитись, чи справжній це лікар, або чи є в нього кваліфікація тощо. При будь яких порушеннях не є проблемою видалити підозрілий контакт.

Якщо все вдало, пацієнт може збирати медичну інформацію про себе, яку при запиті лікаря, він може видавати чи не видавати. Таким чином буде досягнуто повне володіння своєї інформації пацієнтом (рис.2).

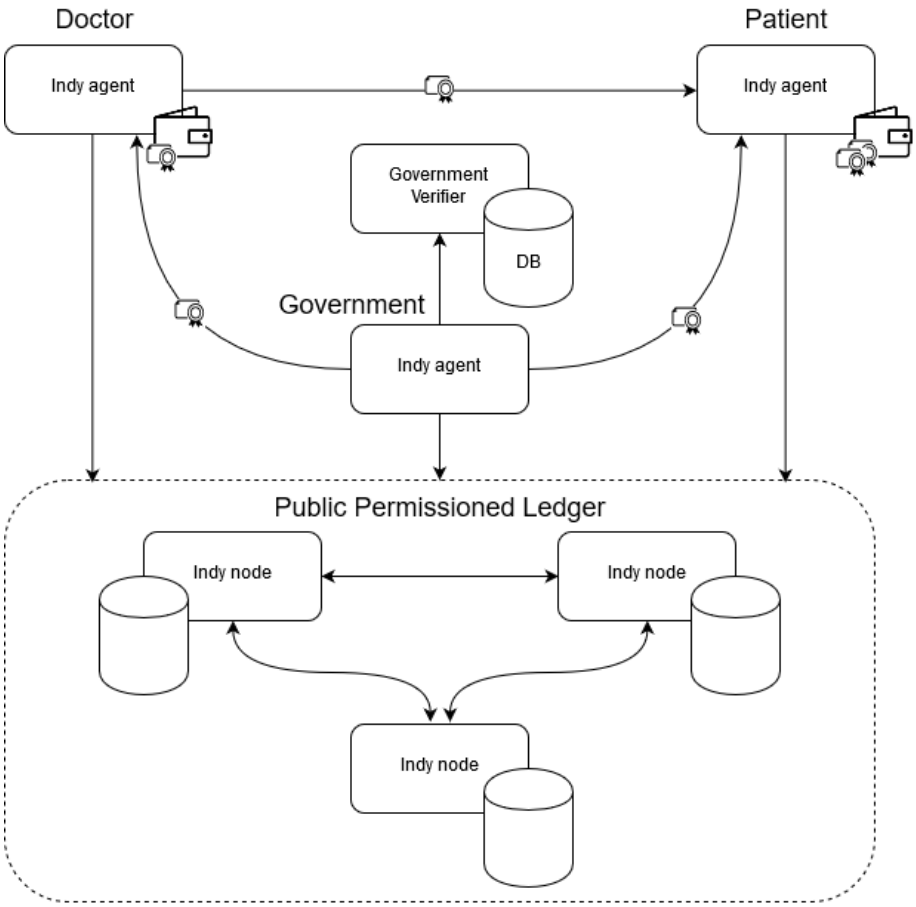

Рис. 2. Прототип архітектури

По цьому концепту було розроблено додаток, з деякими

доповненнями. В додатку доданий функціонал чату та медичних записів на кшталт додатку Health від Apple, де пристрої, чи сама людина, заповнюють дані щодо роботи серця, кровоносної системи чи просто вимірів тіла. Back-end частина додатку розроблена на мові програмування Java, front-end – javascript з підтримкою фреймфорку React Native. Архітектура back-end частини є мікро-сервісною.

Уявно всі сервіси можна поділити на 2 групи:

1. Структурна логіка – сюди входять процеси автентифікації, авторизації, управління роботою сервісів, побудови маршруту запитів, генерування документації запитів, зв'язування сервісів тощо.
2. Бізнес логіка – процеси, що відносяться саме до головної логіки: управління леджером, прийом запитів, обробка та вивід результатів.

Структурна логіка описує структуру проекту, кожен сервіс виконує свої обов'язки для підтримання системи у безпеці та робочому стані. Складається з 4 сервісів:

1. Service Discovery Server – це сервер імен або реєстр сервісів, що забезпечує зв'язність сервісів.
2. Gateway service – це шлюз та маршрутизатор, що спілкується з відкритим світом, ховаючи інші сервіси під собою.
3. Auth service – сервіс, що регулює роботу з безпекою, видає та перевіряє токени доступу.
4. Documentation service – сервіс, що генерує API документацію сервісів, що взаємодіють зі шлюзом (user service, government service).

Бізнес логіка це ядро проекту, саме тут відбуваються усі процеси, які можна зробити в системі. Складається з 3 сервісів:

1. User service – сервіс, що приймає запити від додатку і виконує роботу, що непов'язана безпосередньо з леджером.
2. Self-sovereign identity service – сервіс, що виконує логіку, пов'язану з леджером.

3. Government service – сервіс, що імітує роботу держави для верифікації користувачів, при реєстрації, та видачі документів, які будуть служити як базові для користувачів (рис.3).

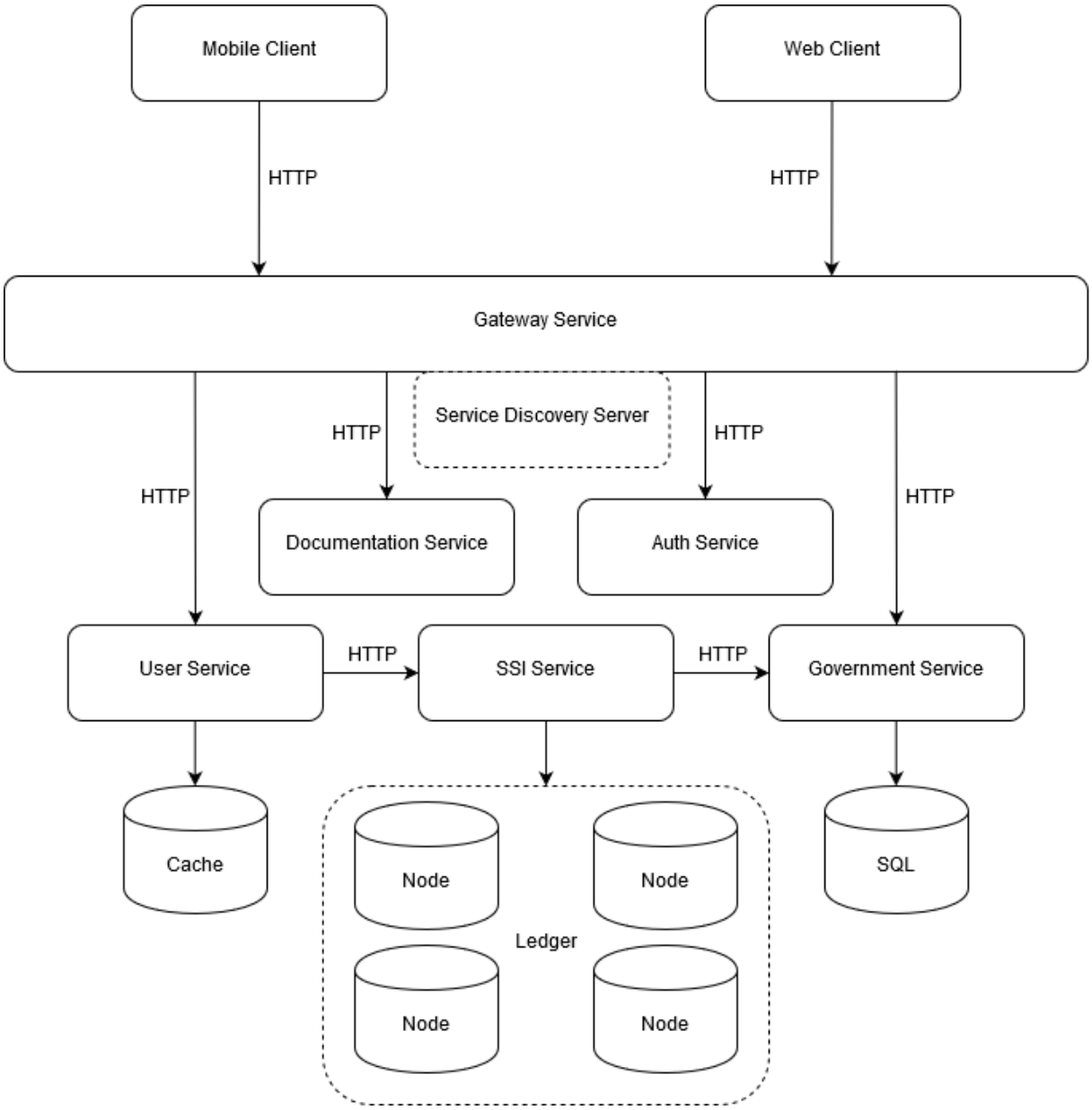

Рис. 3. Мікро-сервісна архітектура back-end

Висновок. Хоча вже існують багато прикладів використання блокчейну в медицині, до недавніх пір було досить нетривіально розробити систему, що дозволила б повністю перевести керуючі процеси, на блокчейн. Не було відповідної архітектури, здатної задовольнити усіх: пацієнтів з приватністю, держустанов з доступом до даних, та безпеки для

усіх. Застосування структури Hyperledger Indy, яка створена для проекції документообігу у реальному житті, дає можливість досить ефективно використовувати її в електронній охороні здоров'я .

Література

1. Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. Journal of Medical Systems, 40(10). doi: 10.1007/s10916-016-0574-6.
2. Kassab, M., Defranco, J., Malas, T., Neto, V. V. G., & Destefanis, G. (2019). Blockchain: A Panacea for Electronic Health Records? 2019 IEEE/ACM 1st International Workshop on Software Engineering for Healthcare (SEH). doi: 10.1109/seh.2019.00011.
3. Healthcoin. (n.d.). URL: https://www.crunchbase.com/organization/healthcoin
4. Patel, V. (2018). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health Informatics Journal, 25(4), 1398–1411. doi: 10.1177/1460458218769699.
5. Tung, J., & Nambudiri, V. (2018). Beyond Bitcoin: potential applications of blockchain technology in dermatology. British Journal of Dermatology, 179(4), 1013–1014. doi: 10.1111/bjd.16922.
6. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., and Wang, F. (2017). "Secure and Trustable Electronic Medical Records Sharing Using Blockchain," in AMIA (American Medical Informatics Association) Annual Symposium Proceedings.
7. Hyperledger. (n.d.). hyperledger/indy-sdk. URL: https://github.com/hyperledger/indy-sdk.