Вестник Тверского государственного университета. Серия: Экономика и управление. 2018. №3. С. 106–112.
УДК 351.9

ОСОБЕННОСТИ ФОРМИРОВАНИЯ ДЕЦЕНТРАЛИЗОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ДАННЫМИ В МЕДИЦИНСКИХ УЧРЕЖДЕНИЯХ НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

И.А. Докукина

Среднерусский институт управления – филиал РАНХиГС, г. Орел

Цель статьи – рассмотреть особенности формирования децентрализованной системы управления данными в медицинских учреждениях. Показано, что в современном мире любой человек имеет потенциальную возможность быстро и качественно получить доступ к различным массивам данных и персональной информации. Существуют приложения, агрегирующие подобные информационные потоки в одном месте и предоставляющие удобный доступ к ней. Обозначенные тренды обходят стороной одну из наиболее важных сфер, от которой зависит качество и продолжительность жизни самого человека – это здравоохранение. Применение технологии блокчейн в данной сфере даст возможность повысить безопасность и сохранность медицинских данных пациента, а также поможет связать разрозненные базы в одно целое, сделав взаимодействие пациентов и врачей более простым и упорядоченным. Научная новизна заключается в построении работающего децентрализованного прототипа управления данными в медицинских учреждениях на основе последовательного применения технологии блокчейн.

Ключевые слова: *блокчейн, управление данными, децентрализованная система управления, медицинские учреждения, хранение данных.*

Хранение и управление данными в современном мире характеризуются следующими проблемами. Проблема целостности данных: медицинские данные хранятся разрозненно. Каждое медицинское учреждение имеет собственную базу данных, чаще всего ограниченную конкретным учреждением. Медицинские записи пациентов в государственных медицинских учреждениях и вовсе чаще всего хранятся на бумажных носителях в единственном экземпляре. Для того чтобы собрать все медицинские записи воедино, пациенту придется пройти долгий путь, и на определенных этапах пути с большой долей вероятности окажется, что часть данных утеряна и не подлежит восстановлению. Отсюда вытекает следующая проблема – проблема утраты данных. Нередки случаи, когда истории болезни были утеряны, либо утрачены в связи с форс-мажорными обстоятельствами, и это существенно влияло на качество лечения. Если человек часто переезжает с места на место и не проходит регулярных осмотров, вероятнее всего при следующем обращении в клинику на него будет заведена новая карта, без какой-либо информации о предыдущем отрезке его жизни. Проблема доступа к личным медицинским данным последняя в представленном списке, но не последняя по значимости – в существующей системе медицинские записи

хранятся открыто в рамках учреждения – будь то бумажные носители или базы данных, пациент не может регулировать доступ к ним.

В ходе изучения проблем хранения медицинских данных и вариантов их решения удалось выявить главные факторы, которым должны соответствовать разработки в области управления и хранения медицинских данных:

– обеспечение целостности данных. При обработке данных исследований или результатов испытаний, чья целостность может напрямую влиять на здоровье людей, необходима уверенность, что эти данные не были подделаны с момента их формирования;

– обеспечение безопасности данных;

– обеспечение мобильности данных, интеграция и функциональная совместимость.

Медицинские записи должны быть доступны для участников обмена медицинской информацией с минимальными затратами.

Таким образом, система управления данными должна отвечать следующим требованиям: возможность отслеживания изменений, децентрализация и работа с документами. Необходимо реализовать безопасную распределенную систему управления версиями, которая позволяет устанавливать режимы доступа, как для чтения, так и для записи. Запись должна быть безопасной и конфиденциальной. Наилучшим образом помогает преодолеть вышеописанные проблемы и наиболее соответствует выдвинутым требованиям, которым должна отвечать модель хранения медицинских данных, является блокчейн. Применение технологии блокчейн является новым научным направлением, что и обусловило актуальность проведенного исследования. Блокчейн представляет собой логически связанную последовательность информационных блоков, каждый из которых содержит данные о группе транзакций и ссылку на предыдущий блок [3, с. 117].

Важной особенностью журнала транзакций в блокчейне является его неизменность. Это свойство означает, что нельзя незаметно удалить транзакцию из журнала или добавить новую в его середину, что является ключевой особенностью безопасности сети.

Целостность и подлинность попадающих в блокчейн транзакций гарантируется с помощью криптографических техник, позволяющих эффективно выявлять любые некорректно добавленные в систему или искусственно измененные транзакции [6, с. 354].

Децентрализованный, открытый и криптографический характер блокчейн позволяет людям доверять друг другу и взаимодействовать друг с другом, что делает ненужным использование посредников. Это также обеспечивает беспрецедентные преимущества в плане безопасности.

Правильно созданная архитектура подобного рода дает пациенту доступ и контроль над своими полными медицинским записями, не налагая особой нагрузки на хранение или передачу данных. Среди типов блокчейн были выделены нами в ходе научного исследования публичные и приватные. Публичный блокчейн – это блокчейн, который может прочитать любой человек в мире. При этом он может отправлять транзакции и ожидать их включения, если они действительны, и он может участвовать в процессе

консенсуса – процессе для определения, какие блоки добавляются в цепочку и каково текущее состояние всей цепи. Приватные блокчейны характеризуются ограниченным уровнем допуска. В таких сетях подтверждение транзакций, проведение аудита, управление базами доступно четко определенному кругу лиц.

Блокчейн-сеть существует в состоянии консенсуса, автоматически проверяет сама себя каждый определенный промежуток времени, осуществляя своего рода самостоятельный аудит цифровой экосистемы. Сеть согласовывает каждую происходящую транзакцию с интервалом в десять минут [4, с. 50].

Любая технология, какой бы прогрессивной она не была, имеет свои плюсы и минусы. Среди плюсов технологии блокчейн важно отметить неизменяемость, прозрачность, децентрализванность, отказоустойчивость. Главными проблемами являются: избыточность – каждый полный узел это копия всей блочной цепи; масштабируемость; дороговизна транзакций – как в финансовом, так и во временном плане.

Данную технологию опробовали уже во многих сферах. В силу новизны данного инструментария большинство решений находятся в экспериментальной стадии или в процессе разработки. Попытки применения технологии блокчейн совершаются в сферах управления данными, управления авторскими правами и правами владения, проверки подлинности контента, электронного голосования, борьбы с контрафактом.

Поскольку разработанный нами прототип будет использовать для хранения данных публичный блокчейн, необходимо подумать о том, как защитить персональные данные. В качестве защиты было выбрано шифрование данных, при этом было принято решение применять как симметричный, так и асимметричный алгоритмы шифрования.

Среди требований к хранилищам данных для децентрализованных приложений мы выделили:

– распределенность;

– поддержку шардинга (если мы ожидаем, что приложение будет популярно и будет хранить огромные объемы данных, то хорошо бы воспользоваться мощностью сети, чтобы увеличить максимальные объемы хранения);

– скорость работы (для популярных приложений могут потребоваться сотни тысяч, если не миллионы транзакций по сохранению или чтению данных в секунду);

– структурированность;

– неизменяемость.

Для разработки использовались следующие технологии: JavaScript, Electron, Node.js, Express и MongoDB, React, Redux и Webpack, WebSoket, Ethereum Blockchain и BigchainDB. Блокчейн Ethereum стабильно существует уже более двух лет, и зарекомендовал себя в качестве надежной платформы для реализации децентрализованных приложений. BigchainDB – выбран для децентрализованного хранения большого объема данных и, кроме того, в настоящий момент его использование является бесплатным.

Оригинальность предлагаемой системы управления медицинскими данными в следующем:

1) при входе в систему пользователь должен иметь возможность авторизоваться или зарегистрироваться. Должно быть предоставлено два варианта регистрации: для пациента и поставщика медицинских услуг (врача);

2) в личном кабинете пользователя должна присутствовать возможность заполнения персональной информации;

3) в панели управления пациента должны отображаться: основная персональная информация, список запросов (четыре последних запроса) на доступ к личной медицинской карте, список врачей, которым доступны медицинские записи пациента (четыре последних врача), а также ссылки для перехода к личной медицинской карте и к полным спискам текущих врачей и запросов доступа.

В панели управления врача должны отображаться: основная персональная информация, список запросов со статусами, отправленных пациентам (четыре последних запроса), список пациентов с доступными медицинскими картами (четыре последних пациента), а также ссылки для перехода к списку запросов и списку пациентов;

4) пациент должен иметь возможность отклонить или принять запрос на доступ к своей медицинской карте. Пациент должен иметь возможность удалить врача из списка врачей, которым доступны его медицинские данные. При удалении пациентом врач должен терять любую возможность доступа к медицинской карте данного конкретного пациента, но сохранять возможность отправления запроса на доступ данному пациенту еще раз;

5) на странице медицинской карты пациент должен иметь возможность просматривать медицинские записи, начиная от самых новых, заканчивая самыми старыми записями. В записи должны отображаться информация о враче, который сделал запись, дата создания записи и непосредственно сама запись. Пациент не должен иметь возможность добавлять записи ни в собственную, ни в какую-либо иную медицинскую карту;

6) врач должен иметь возможность осуществить поиск пациента для отправки ему запроса на доступ. Кроме того, врач должен иметь возможность отправлять запросы на доступ к медицинским данным пациента и просматривать медицинские записи, если такой доступ был одобрен;

7) врач должен иметь возможность добавлять медицинские записи в карту пациента до тех пор, пока пациент не сочтет нужным удалить врача из списка текущих докторов, тем самым закрыв доступ к своей медицинской карте;

8) ни врач, ни пациент, ни владелец приложения или администратор не должны иметь возможности удалить ни одну из медицинских записей пациента.

Медицинские данные пациента не должны храниться в открытом виде и должны быть зашифрованы публичным ключом пациента. Приватный ключ пациента должен генерироваться и храниться на стороне клиента, и никогда не передаваться на сторону сервера, дабы избежать его кражи и компрометации, данных пациента.

Научная уникальность предлагаемого авторского прототипа заключается в том, что при регистрации каждому пользователю создается Ethereum адрес и криптографическая пара RSA ключей. Врач через

графический интерфейс добавляет новую медицинскую запись к карте пациента, данные шифруются публичным ключом пациента, и производится транзакция записи в блокчейн по Ethereum адресу пациента.

База данных авторского приложения состоит всего из пяти коллекций. В коллекцию User мы записываем пользователей, их персональные данные и публичные ключи. В коллекции Session хранятся сессии пользователей, коллекция Claim содержит запросы доступов с их текущими статусами. Коллекция Transaction включает массивы хешей транзакций каждого конкретного пользователя для более быстрого и удобного обращения к блокчейну Ethereum.

Создание распределенных приложений должно стать довольно востребованным направлением, так как они позволяют решать многие проблемы: отсутствие доверия к хранителю данных, уязвимые для атак серверы в централизованных системах, закрытость систем [5, с. 38].

Глобальное «общее состояние» Ethereum состоит из множества небольших объектов («учетных записей»), которые могут взаимодействовать друг с другом через инфраструктуру передачи сообщений. У каждой учетной записи есть связанное с ней состояние и 20-байтовый адрес. Адрес в Ethereum - это 160-битный идентификатор, который используется для идентификации любой учетной записи.

В ходе исследования были разработаны два типа учетных записей:

Внешние учетные записи, которые контролируются закрытыми ключами и не имеют никакого кода, связанного с ними. Контрактные учетные записи, которые контролируются кодом контракта, загруженным в него.

Внешняя учетная запись может отправлять сообщения другим внешним счетам или другим учетным записям, создавая и подписывая транзакцию с использованием своего закрытого ключа. Сообщение из внешней учетной записи на контрактную учетную запись активирует код учетной записи контракта, позволяя ему выполнять различные действия (например, создавать и переносить токены, записывать во внутреннее хранилище, выполнять некоторые вычисления, создавать новые контракты и так далее).

Медицинские записи, зашифрованные ключом пациента, хранятся в блокчейне, что обеспечивает невозможность прочтения данных никем, кроме владельца приватного ключа, а также защиту от изменения или удаления данных [2, с. 7].

Предполагается, что серверная часть разрабатываемого прототипа не должна выполнять сложных вычислений, нагружающих процессор, поскольку практически все энергозатратные операции, такие как генерация криптографических ключей, кодирование и декодирование данных, производятся на клиентской стороне.

Кроме всего прочего, благодаря тому, что данные реплицируются на несколько узлов, мы избавляемся от единой точки отказа системы, что также позволяет обеспечить целостность данных и агрегирование их в одном месте, а не во множестве разрозненных баз данных множества медицинских учреждений. В результате все публичные протоколы блокчейнов, которые работают на такой децентрализованной основе, реализуют компромисс между низкой пропускной способностью транзакций и высокой степенью

централизации. Другими словами, по мере роста размера блокчейна требования к хранению, пропускной способности и вычислительной мощности, необходимые для полного участия в сети, возрастают [1, с. 35].

Таким образом, универсальность данной разработки заключается в том, что предложенная архитектура не ограничивает возможности масштабирования приложения. Для медицинских учреждений возможно внедрение системы посредством API, что позволит избежать дополнительных временных затрат медицинских работников при записи данных. Медицинские записи, зашифрованные ключом пациента, хранятся в блокчейне, что обеспечивает невозможность прочтения данных никем, кроме владельца приватного ключа. А за счет того, что данные сохраняются в блокчейн – они защищены от изменения или удаления. Копия медицинской карты пациента, зашифрованная публичным ключом врача, сохраняется в базу данных приложения и при необходимости может быть бесследно удалена пациентом.

Список литературы

1. Бауэр В.П., Сильвестров С.Н., Барышников П.Ю. Блокчейн как основа формирования дополненной реальности в цифровой экономике // Информационное общество. 2017. № 3. С. 30–40.
2. Волошин И.П. Управление доступом на основе блокчейн // Информационная безопасность регионов. 2017. № 3–4 (28-29). С. 5–8.
3. Воробьева И.Г., Прокудина А.П. Преимущества и проблемы инвестирования в технологию блокчейн // Инновационные технологии в машиностроении, образовании и экономике. 2018. Т. 14. № 1–2 (7). С. 112–117.
4. Генкин А.С., Михеев А.Н Перспективы применения технологии блокчейн в государственном и муниципальном управлении // Самоуправление. 2017. № 4. С. 47–52.
5. Глухов В.В., Рожков Ю.В. Криптовалюты и блокчейн: подготовка специалистов // Вестник Хабаровского государственного университета экономики и права. 2017. № 4–5. С. 28–38.
6. Елистратова А.А. Проблемы внедрения технологии блокчейн в России // Актуальные проблемы авиации и космонавтики. 2017. Т. 2. № 13. С. 354–355.

FEATURES OF THE FORMATION OF A DECENTRALIZED DATA MANAGEMENT SYSTEM IN MEDICAL INSTITUTIONS BASED ON BLOCKCHAIN TECHNOLOGY

I.A. Dokukina

Central Russian Institute of Management, Branch of RANEPA

In today's world, anyone has the potential to quickly and efficiently access various data sets and personal information. There are applications that aggregate such information flows in one place and provide convenient access to it. These trends bypass one of the most important areas which closely connected with the quality and life expectancy of a person–it is health. One of the major challenges facing health systems worldwide is the provision of a large amount of health data to a range of stakeholders, while ensuring data

integrity and confidentiality. The use of blockchain technology in this area will make it possible to improve the safety and security of patient's medical data, as well as help to link disparate databases into one, making the interaction of patients and doctors more simple and orderly. The purpose of the article is to consider the features of the formation of a decentralized data management system in medical institutions. The scientific novelty of the article is obtained in the framework of achieving its goal and is to build a working decentralized prototype of data management in medical institutions based on the consistent use of blockchain technology.
Keywords: *blockchain, data management, decentralized management system, medical facilities, data storage.*

Об авторе:

ДОКУКИНА Ирина Александровна – кандидат экономических наук, доцент кафедры «Менеджмент и государственное управление», Среднерусский институт управления – филиал РАНХиГС, e-mail dokukina.orags@mail.ru

About the author:

DOKUKINA Irina Aleksandrovna – candidate of economics sciences, associate professor of department «Management and public administration», Central Russian Institute of Management, Branch of RANEPA, e-mail dokukina.orags@mail.ru

References

1. Bauehr V.P., Sil'vestrov S.N., Baryshnikov P.YU. Blokchejn kak osnova formirovaniya dopolnennoj real'nosti v cifrovoj ehkonomike // Informacionnoe obshchestvo. 2017. № 3. S. 30–40.
2. Voloshin I.P. Upravlenie dostupom na osnove blokchejn // Informacionnaya bezopasnost' regionov. 2017. № 3–4 (28-29). S. 5–8.
3. Vorob'eva I.G., Prokudina A.P. Preimushchestva i problemy investirovaniya v tekhnologiyu blokchejn // Innovacionnye tekhnologii v mashinostroenii, obrazovanii i ehkonomike. 2018. T. 14. № 1–2 (7). S. 112–117.
4. Genkin A.S., Miheev A.N Perspektivy primeneniya tekhnologii blokchejn v gosudarstvennom i municipal'nom upravlenii // Samoupravlenie. 2017. № 4. S. 47–52.
5. Gluhov V.V., Rozhkov YU.V. Kriptovalyuty i blokchejn: podgotovka specialistov // Vestnik Habarovskogo gosudarstvennogo universiteta ehkonomiki i prava. 2017. № 4–5. S. 28–38.
6. Elistratova A.A. Problemy vnedreniya tekhnologii blokchejn v Rossii // Aktual'nye problemy aviacii i kosmonavtiki. 2017. T. 2. № 13. S. 354–355.