Аннотация – В документе представлен анализ системы транзакций медицинского Интернета вещей (IoMT), основанной на блокчейн-технологии (китайский патент CN111913833A). В ходе анализа рассматриваются различные аспекты системы, включая её архитектуру, функции безопасности, вопросы безопасности и конфиденциальности и потенциальное применение в секторе здравоохранения.

Приводится качественное изложение содержательной части патента в интересах специалистов в области безопасности и других отраслей промышленности. Этот анализ особенно полезен экспертам по кибербезопасности, инженерам DevOps, ИТ-специалистам, forensics-аналитикам и производителям медицинского оборудования для понимания последствий объединения технологии блокчейн с IoMT. Он даёт представление каким образом интеграция решает проблемы в отрасли здравоохранения, в т.ч несанкционированный доступ, утечку данных и отсутствие стандартизированного протокола для безопасного обмена данными.

I. Основная идея

Патент CN111913833A предлагает систему транзакций на основе блокчейна, специально разработанную для медицинского Интернета вещей (IoT). Эта система предназначена для решения проблем безопасности данных, конфиденциальности и функциональной совместимости в здравоохранении. Предлагаемое решение повышает безопасность и конфиденциальность данных пациентов за счёт использования двойных блокчейнов, аутентификации на основе атрибутов и интеграции искусственного интеллекта.

Основная идея патента заключается в обеспечении конфиденциальности и безопасности медицинских данных при одновременном облегчении обмена этими данными между различными заинтересованными сторонами в экосистеме здравоохранения.

Представлено несколько ключевых моментов и выводов:

- **Архитектура с двойным блокчейном**: система включает в себя две цепочки блоков: публичный блокчейн для публикации пользовательских данных и частный блокчейн для безопасного хранения медицинских данных.
- **Шифрование на основе атрибутов**: доступ к медицинским данным контролируется с помощью шифрования на основе атрибутов, которое позволяет только авторизованным пользователям с определёнными атрибутами получать доступ к данным или изменять их.
- **Конфиденциальность и безопасность**: система предназначена для повышения конфиденциальности и защищённости медицинских данных, что имеет решающее значение в отрасли здравоохранения.
- **Интероперабельность**: используя технологию блокчейн, система облегчает безопасный обмен данными между различными субъектами экосистемы здравоохранения, способствуя интероперабельности.
- **Смарт-контракты**: система использует смарт-контракты для автоматизации и обеспечения соблюдения правил доступа к данным и транзакций, уменьшая потребность в посредниках и повышая эффективность.
- **Интеграция искусственного интеллекта**: патент предполагает потенциальную интеграцию искусственного интеллекта с блокчейном для улучшения медицинских услуг в т.ч. модели прогнозирования заболеваний.
- **Мониторинг в режиме реального времени**: предлагаемая система может обеспечивать мониторинг состояния пациентов в режиме реального времени с помощью устройств Интернета вещей, предоставляя своевременные и точные данные о состоянии здоровья.
- **Децентрализация**: децентрализованный характер блокчейна обеспечивает эффективное решение для защиты от единичных сбоев и несанкционированного изменения данных.

II. Область применения

Технология обладает потенциалом улучшить способы управления медицинскими данными и их совместного использования в различных секторах индустрии здравоохранения. Ее акцент на безопасность, конфиденциальность и функциональную совместимость соответствует важнейшим потребностям этих отраслей, обещая повысить эффективность, снизить затраты и улучшить результаты лечения пациентов.

A. Здравоохранение:

Отрасль здравоохранения получит значительную выгоду от этого патента, включая больницы, диспансеры и другие медицинские учреждения, которым требуется

безопасное управление данными о пациентах и обмен ими. Предлагаемое решение может повысить безопасность и конфиденциальность медицинских данных, что имеет решающее значение для доверия пациентов и соблюдения нормативных требований. Используя блокчейн, поставщики медицинских услуг могут гарантировать неизменяемость и отслеживаемость медицинских записей

B. Медицинские устройства:

Производители и дистрибьюторы медицинских устройств Интернета вещей, таких как носимые медицинские мониторы и подключённое медицинское оборудование, непосредственно участвуют в экосистеме, о которой говорится в патенте. Система будет управлять данными, генерируемыми этими устройствами, гарантируя, что они надёжно хранятся и передаются только авторизованным сторонам. Это может улучшить мониторинг и надёжность устройств.

C. Информационные технологии в области здравоохранения:

Компании, специализирующиеся на ИТ-решениях для здравоохранения, электронных медицинских картах и системах управления медицинскими данными заинтересованы в системе повышающей потенциал безопасности данных и интероперабельности. Патент может стать новой моделью обмена медицинской информацией, сделав электронные медицинские записи более безопасными и легко доступными для обмена между различными системами здравоохранения.

D. Фармацевтические препараты:

В фармацевтической промышленности система может найти решение для безопасного обмена данными в ходе клинических испытаний и процессов разработки лекарств. Способность блокчейна обеспечивать прозрачную и неизменяемую запись транзакций может помочь в отслеживании происхождения лекарств, обеспечении их подлинности и оптимизации цепочки поставок.

E. Страхование:

Медицинские страховые компании могут использовать эту систему для безопасного доступа к данным пациентов в целях обработки претензий и предотвращения мошенничества. Неизменяемый характер записей блокчейна также может помочь страховщикам проверить точность претензий и сократить мошеннические действия.

F. Исследования и разработки:

Исследовательские учреждения, которым требуется доступ к медицинским данным для проведения исследований, могли бы воспользоваться возможностями системы безопасного и контролируемого обмена данными. Блокчейн может облегчить сотрудничество между исследователями, предоставив безопасную платформу для обмена данными при сохранении конфиденциальности пациентов.

G. Регулирующие органы:

Государственные учреждения здравоохранения и регулирующие органы могут быть заинтересованы в системе контроля за соблюдением правил конфиденциальности медицинских данных. Присущие блокчейну функции могут помочь гарантировать, что поставщики медицинских услуг и другие заинтересованные стороны придерживаются необходимых стандартов.

H. Кибербезопасность:

Компании, специализирующиеся на решениях в области кибербезопасности для отрасли здравоохранения, найдут патент актуальным в плоскости безопасности транзакций медицинских данных. Предлагаемая блокчейн-система может предложить новые способы защиты от утечек данных и киберугроз.

III. Предлагаемое решение

Ключевыми компонентами предлагаемого решения являются архитектура с двумя блокчейнами, шифрование на основе атрибутов для контроля доступа к данным, алгоритм консенсуса, оптимизированный для пропускной способности транзакций, контроль доступа к данным пациентов и различные функции для удалённой диагностики, обмена данными и транзакций в контексте медицинского Интернета вещей:

Архитектура с двумя блокчейнами:

- Публичный блокчейн для публикации пользовательских данных
- Частный блокчейн для безопасного хранения медицинских данных.

Шифрование на основе атрибутов (ABE):

- Доступ к медицинским данным контролируется с помощью шифрования на основе атрибутов, которое позволяет только авторизованным пользователям с определёнными атрибутами получать доступ к данным или изменять их.
- Обеспечение конфиденциальности и безопасности конфиденциальной медицинской информации.

Пропускная способность:

- Предлагается алгоритм консенсуса, основанный на доказательстве объёма транзакции для оптимизации пропускной способности.
- Решение проблемы низкой пропускной способности транзакций в существующих общедоступных решениях для обработки медицинских данных на основе блокчейна.

Контроль доступа к данным пациента:

- Пациенты имеют разрешения на управление своими медицинскими данными.
- Решение проблемы игнорирования контроля доступа к данным пациентов в текущих решениях для медицинских данных на основе блокчейна.

Функции удалённой диагностики, обмена данными и транзакций данных:

- Предоставление функций для удалённой диагностики, обмена данными и транзакции данных.
- Функции позволяют использовать различные приложения и сервисы в медицинской экосистеме Интернета вещей.

A. Архитектура с двумя блокчейнами

Предлагаемое решение использует архитектуру с двумя блокчейнами, состоящую из публичного блокчейна для публикации пользовательских данных и частного блокчейна для безопасного хранения медицинских данных. Такой подход направлен на решение проблем безопасности данных, конфиденциальности и функциональной совместимости в экосистеме медицинского ввода-вывода.

Комбинация публичных и частных блокчейнов:

- Публичный блокчейн — это блокчейн без разрешений, который позволяет любому присоединиться и участвовать в прозрачной публикации и проверке пользовательских данных.
- Частный блокчейн — это разрешённый блокчейн с ограниченным доступом для безопасного хранения конфиденциальных медицинских данных.

Дифференцированные роли и контроль доступа:

- Публичный блокчейн позволяет пользователям контролировать свои данные и обеспечивает прозрачность при публикации данных.
- Частный блокчейн обеспечивает безопасную частную среду для хранения медицинских данных и обмена ими только между авторизованными участниками.

Обеспечение баланса между прозрачностью, безопасностью и конфиденциальностью:

- Подход с двойным блокчейном направлен на использование сильных сторон блокчейнов.
- Направленность на достижение баланса между прозрачностью и децентрализацией публичных блокчейнов и повышением конфиденциальности и эффективности частных блокчейнов.

Устранение ограничений отдельных типов блокчейнов:

- Публичные блокчейны могут столкнуться с проблемами масштабируемости и конфиденциальности.
- Частные блокчейны «могут принести в жертву» некоторый уровень децентрализации и прозрачности.
- Сочетание обоих типов смягчает их индивидуальные недостатки.

Обеспечение безопасного обмена данными и совместной работы:

- Архитектура облегчает безопасный обмен медицинскими данными между уполномоченными организациями на частном блокчейне.
- Это способствует сотрудничеству между заинтересованными сторонами в сфере здравоохранения при сохранении конфиденциальности пациентов.

Повышение доверия и целостности данных:

- Неизменяемость и прозрачность публичного блокчейна помогают установить доверие ко всей системе.
- Частный блокчейн обеспечивает целостность и конфиденциальность медицинских данных.

Потенциал для повышения эффективности и эксплуатационных характеристик:

- Ограниченное участие в частном блокчейне может привести к более быстрой обработке транзакций и достижению консенсуса по сравнению с публичными блокчейнами.
- Структура с двумя блокчейнами позволяет оптимизировать систему на основе конкретных требований каждого компонента.

B. Шифрование на основе атрибутов (ABE)

ABE — это обобщение шифрования с открытым ключом, которое позволяет использовать политики контроля доступа. При традиционном шифровании с открытым ключом сообщение шифруется для конкретного получателя с использованием его открытого ключа. Напротив, ABE шифрует данные на основе атрибутов или политик, позволяя осуществлять контроль доступа на основе атрибутов, которыми обладают пользователи.

Существует два основных типа ABE:

- •**Key-Policy ABE (KP-ABE)**: в KP-ABE закрытый ключ каждого пользователя связан с политикой доступа или структурой, которая определяет, какие зашифрованные тексты может расшифровывать ключ. Зашифрованные тексты помечены наборами атрибутов.
- **Ciphertext-Policy ABE (CP-ABE)**: в CP-ABE политика доступа встроена в зашифрованный текст, и закрытый ключ каждого пользователя связан с набором атрибутов. Пользователь может расшифровать текст только в том случае, если его атрибуты удовлетворяют политике доступа.

Основные характеристики ABE:

- **Детальный контроль доступа**: ABE обеспечивает детальный контроль доступа к зашифрованным данным, позволяя определять политики доступа на основе атрибутов. Это особенно полезно в здравоохранении, где разным заинтересованным сторонам (например, врачам, медсёстрам,

исследователям) требуются разные уровни доступа к данным о пациентах.

- **Устойчивость к сговору**: схемы ABE разработаны таким образом, чтобы быть устойчивыми к атакам с целью сговора. Даже если несколько пользователей вступают в сговор и объединяют свои атрибуты, они не должны иметь возможности расшифровать текст, если хотя бы один из них по отдельности не удовлетворяет политике доступа.
- **Гибкость**: ABE позволяет создавать политики доступа и применять сложные требования к контролю доступа.
- **Отзыв атрибута**: некоторые схемы ABE поддерживают отзыв атрибута, затрагивая других пользователей, которые используют те же атрибуты. Это важно в динамичных средах, таких как здравоохранение, где роли пользователей и разрешения могут меняться с течением времени.
- **Обновление политики**: некоторые конструкции ABE допускают обновления, позволяя изменять политики доступа, связанные с зашифрованными текстами, без повторного шифрования данных. Это обеспечивает гибкость в управлении контролем доступа по мере изменения требований.
- **Отслеживаемость**: схемы ABE позволяют отследить личность пользователя, который слил свой ключ дешифрования. Это помогает поддерживать подотчётность и предотвращать несанкционированный обмен данными.

ABE в здравоохранении

ABE обладает значительным потенциалом в обеспечении безопасности медицинских данных, особенно в облачных системах электронного здравоохранения. Используя ABE, данные пациента могут быть зашифрованы с помощью детализированных политик доступа, гарантирующих, что расшифровать данные и получить к ним доступ смогут только авторизованные пользователи (например, поставщики медицинских услуг с определёнными ролями или атрибутами). Это помогает защитить конфиденциальность пациентов и соответствовать нормативным требованиям, таким как HIPAA.

Более того, такие функции, как отзыв атрибута и обновление политики, имеют решающее значение в здравоохранении, поскольку роли пользователей и требования к доступу к данным могут часто меняться. Отслеживание также важно для предотвращения утечки данных и обеспечения соответствия требованиям.

C. Алгоритм консенсуса, основанный на доказательстве объёма транзакции

В системах блокчейна консенсусные алгоритмы используются для достижения соглашения между участвующими узлами о состоянии леджеров. Они гарантируют, что все узлы имеют согласованное представление о блокчейне, и предотвращают двойные расходы или другие вредоносные действия. Однако традиционные консенсусные алгоритмы, такие как Proof-of-Work (PoW) и Proof-of-Stake (PoS), часто сталкиваются с проблемами масштабируемости, что приводит к низкой пропускной способности транзакций.

Предложенный в патенте алгоритм консенсуса, основанный на доказательстве объёма транзакций, направлен на оптимизацию их пропускной способности специально для медицинского сценария Интернета вещей.:

- **Объём транзакций как показатель**: алгоритм, использует объём или количество транзакций, обработанных узлом, в качестве показателя для определения его права создавать новые блоки. Узлам, обрабатывающим больший объём транзакций, может быть присвоен приоритет или больший вес в процессе согласования.
- **Поощрение активного участия**: основываясь на консенсусе по объёму транзакций, алгоритм стимулирует узлы к активному участию в сети и обработке транзакций. Узлы, которые вносят больший вклад в пропускную способность сети, получают более высокую вероятность создания новых блоков и получения вознаграждения.
- **Оптимизация пропускной способности**: за счёт приоритизации узлов с более высокими объёмами транзакций алгоритм направлен на оптимизацию общей пропускной способности сети. Узлам, которые могут эффективно обрабатывать транзакции, предоставляется больше возможностей для добавления новых блоков, тем самым увеличивая пропускную способность блокчейна.
- **Решение проблемы масштабируемости**: алгоритм разработан для устранения ограничений масштабируемости существующих общедоступных решений для обработки медицинских данных на основе блокчейна. Уделяя особое внимание объёму транзакций в качестве ключевого показателя, он направлен на улучшение способности сети обрабатывать большое количество транзакций, что имеет решающее значение в контексте медицинского Интернета вещей.

Ключевые особенности алгоритма консенсуса

- **Оптимизация пропускной способности**: основная цель алгоритма – оптимизировать пропускную способность транзакций, позволяя сети блокчейн эффективно обрабатывать больший объём транзакций.
- **Масштабируемость**: решая проблему низкой пропускной способности транзакций, алгоритм направлен на повышение масштабируемости блокчейн-системы, делая её пригодной для обработки крупномасштабных данных.
- **Стимулирование активного участия**: алгоритм вознаграждает узлы, которые активно участвуют в сети и обрабатывают большой объём транзакций.

Это побуждает узлы вносить свой вклад в пропускную способность сети и поддерживать здоровую экосистему.

- **Настройка для медицинского Интернета вещей**: алгоритм разработан специально для медицинской системы транзакций Интернета вещей с учётом уникальных требований и задач этой области, таких как необходимость высокоскоростной обработки больших объёмов медицинских данных.
- **Интеграция с архитектурой с двумя блокчейнами**: алгоритм консенсуса, основанный на доказательстве объёма транзакции интегрирован с архитектурой с двумя блокчейнами, предложенной в патенте, оптимизируя производительность компонентов публичного блокчейна и частного блокчейна.

D. Контроль доступа к данным пациента

Контроль доступа к данным пациентов является важнейшим компонентом предлагаемой системы транзакций медицинского Интернета вещей (IoT), основанной на блокчейне.

Система позволяет пациентам контролировать их конфиденциальную медицинскую информацию, использует шифрование на основе атрибутов и смарт-контракты для обеспечения детализированных и автоматизированных политик доступа, предоставляет проверяемые и прозрачные записи, допускает динамические изменения разрешений и интегрируется с более широкой экосистемой Интернета вещей. Такой комплексный подход к контролю доступа повышает безопасность и конфиденциальность данных пациентов.

Ключевыми функциями механизма контроля доступа к данным пациента в этой системе являются:

Контроль, ориентированный на пациента:

- Система предназначена для предоставления пациентам первичных прав контроля и управления их собственными медицинскими данными.
- Подход, ориентированный на пациента, гарантирует защиту его прав и интересов в отношении конфиденциальной медицинской информации.
- Пациенты могут решать, кто имеет доступ к их данным и при каких обстоятельствах.

Управление доступом на основе атрибутов:

- Доступ к медицинским данным контролируется с помощью шифрования на основе атрибутов (ABE).
- ABE разрешает доступ к данным или их изменение только авторизованным пользователям с определёнными атрибутами.
- Атрибуты могут относиться к роли пользователя (например, врача, медсестры, исследователя), специальности, местоположению или другим значимым факторам.
- Детализированный контроль доступа гарантирует, что конфиденциальные данные будут доступны только тем, у кого есть законная потребность и разрешение.

Автоматизация на основе интеллектуальных контрактов:

- Политики контроля доступа и разрешения закодированы в смарт-контрактах на блокчейне.
- Смарт-контракты позволяют автоматически выполнять и обеспечивать соблюдение правил доступа без ручного вмешательства.
- Автоматизация упрощает процесс контроля доступа и снижает риск несанкционированного доступа из-за человеческой ошибки или манипуляций.

Прозрачность и отслеживаемость:

- Все попытки доступа и транзакции с данными неизменно регистрируются в блокчейне.
- Это позволяет отслеживать, кто к каким данным обращался и когда.
- Прозрачность и отслеживаемость, обеспечиваемые блокчейном, помогают обеспечить соблюдение правил защиты данных и предотвращают попытки несанкционированного доступа.

Динамический и отзываемый доступ:

- Разрешения на доступ к пациенту могут предоставляться, изменяться или отзываться по мере необходимости.
- Например, пациент может предоставить временный доступ к специалисту для проведения определённого лечения, а затем отозвать этот доступ после завершения лечения.
- Гибкость позволяет системе контроля доступа адаптироваться к динамичным потребностям медицинского обслуживания при сохранении безопасности.

Интеграция с медицинской экосистемой Интернета вещей:

- Система контроля доступа интегрирована с более широкой медицинской системой транзакций Интернета вещей, предложенной в патенте.
- Это обеспечивает безопасный и контролируемый доступ к данным, генерируемым различными медицинскими устройствами Интернета вещей и носимыми устройствами.
- Авторизованные поставщики медицинских услуг могут получить доступ к этим данным Интернета вещей для удалённого мониторинга, диагностики и лечения пациентов.

IV. Технологический процесс

Предлагаемое решение использует архитектуру с двумя блокчейнами: публичный блокчейн для публикации данных и частный блокчейн для безопасного хранения данных. ABE используется для детального контроля доступа, в то время как согласованный алгоритм обеспечивает эффективную проверку транзакций. Пациенты сохраняют контроль над своими данными с помощью механизмов контроля доступа. Система призвана обеспечить безопасный, эффективный и ориентированный на пациента подход к управлению медицинскими данными и обмену ими в среде Интернета вещей.

graph TD
A[Владелец данных] - Шифрует данные с помощью ABE -> B (Публичный блокчейн - блокчейн)
A - Устанавливает политики доступа -> B
B - Хранит зашифрованные данные -> C (Частный блокчейн - блокчейн)
C - Безопасное хранение медицинских данных -> D [Облачное хранилище]
E[Пользователь] -- Запрашивает доступ к данным --> F(Полномочия атрибута)
F -- Проверяет атрибуты пользователя --> F
F -- Выдаёт ключ дешифрования --> E
E - Извлекает зашифрованные данные -> D
E -- Расшифровывает данные с помощью ключа --> E
G[Согласованные узлы] - Проверка транзакций с помощью алгоритма консенсуса -> C
H[Пациент] -- Предоставляет / отменяет права доступа --> C

Настройка политики шифрования данных и доступа:

- Владелец данных (например, пациент или поставщик медицинских услуг) шифрует медицинские данные на основе атрибутов (ABE).
- Владелец данных определяет политики доступа, решающие, какие атрибуты требуются для расшифровки данных.
- Зашифрованные данные и политики доступа публикуются в общедоступной блокчейн-цепочке.

Безопасное хранение данных:

- Зашифрованные медицинские данные из блокчейна надёжно хранятся в частной блокчейне.
- Блокчейн действует как безопасный уровень хранения конфиденциальных медицинских данных с контролируемым доступом.
- Зашифрованные данные также могут храниться в облачном хранилище для обеспечения масштабируемости и доступности.

Аутентификация пользователя и выдача ключа:

- Пользователь (например, врач), который хочет получить доступ к зашифрованным данным, отправляет запрос в Центр управления атрибутами.
- Центр управления проверяет атрибуты пользователя на соответствие политикам доступа.
- Если пользователь обладаёт требуемыми атрибутами, Центр управления выдаёт пользователю ключ дешифрования.

Доступ к данным и их расшифровка:

- Авторизованный пользователь извлекает зашифрованные данные из блокчейна или облачного хранилища.
- Используя ключ дешифрования, полученный от Администратора атрибута, пользователь расшифровывает данные.
- Пользователь может получить доступ к открытым медицинским данным в соответствии с предоставленными правами доступа.

Проверка транзакции и достижение консенсуса:

- Узлы в сети блокчейн проверяют транзакции с использованием алгоритма консенсуса, основанного на доказательстве объёма транзакции.
- Этот механизм консенсуса оптимизирует пропускную способность транзакций и обеспечивает целостность и безопасность блокчейна.

Контроль доступа пациентов:

- Пациенты имеют контроль над своими медицинскими данными и могут предоставлять или отзывать разрешения на доступ определённым пользователям или организациям.
- Политика контроля доступа обеспечивается с помощью смарт-контрактов на блокчейне.

Дополнительные функции:

- Система поддерживает удалённую диагностику, позволяя авторизованным поставщикам медицинских услуг получать доступ к данным пациента в целях телемедицины.
- Функции обмена и транзакций обеспечивают безопасный обмен медицинскими данными между уполномоченными сторонами, такими как поставщики медицинских услуг, исследователи или страховщики.

V. Преимущества, недостатки и значимость предлагаемого решения

Предлагаемая система медицинских транзакций Интернета вещей, основанная на блокчейне, предлагает значительные преимущества с точки зрения повышения безопасности, конфиденциальности, контроля за пациентами и обмена данными. Однако она также сталкивается с ограничениями, связанными со сложностью, масштабируемостью, соблюдением нормативных требований, и зависимостью от технологии блокчейн.

Преимущества:

- **Повышенная безопасность и конфиденциальность**: архитектура с двумя блокчейнами,наряду с шифрованием на основе атрибутов (ABE) для детального контроля доступа, значительно повышает безопасность и приватность конфиденциальных медицинских данных.
- **Контроль, ориентированный на пациента**: система предоставляет пациентам разрешения на управление своими медицинскими данными, гарантируя защиту их прав и интересов.
- **Улучшенный обмен данными и совместная работа**: безопасный и эффективный обмен данными, обеспечиваемый системой, способствует сотрудничеству между заинтересованными сторонами в сфере здравоохранения при сохранении конфиденциальности пациентов.
- **Повышение доверия и целостности данных**: неизменность и прозрачность транзакций на блокчейне устанавливают доверие к системе и обеспечивают целостность данных.
- **Потенциал повышения эффективности**: алгоритм консенсуса, основанный на доказательстве объёма транзакции, направлен на оптимизацию пропускной способности транзакций, решая проблемы масштабируемости в существующих решениях.

Ограничения:

- **Сложность и проблемы с внедрением**: предлагаемая система включает в себя множество компонентов и технологий, которые могут создавать проблемы с точки зрения сложности, совместимости и внедрения организациями здравоохранения.
- **Соблюдение нормативных требований**: обеспечение соблюдения правил и стандартов конфиденциальности медицинских данных может быть сложной задачей и потребовать дополнительных мер.
- **Масштабируемость и производительность**: хотя предлагаемый согласованный алгоритм направлен на повышение пропускной способности транзакций, масштабируемость и производительность системы при обработке больших объёмов медицинских данных в реальных сценариях нуждаются в дальнейшей проверке.
- **Управление ключами и контроль доступа**: внедрение безопасного и эффективного управления ключами для ABE и управление динамическими политиками контроля доступа могут быть сложными, особенно в чрезвычайных ситуациях.
- **Зависимость от технологии блокчейн**: система в значительной степени зависит от технологии блокчейн, которая все ещё развивается и может столкнуться с проблемами, связанными с потреблением энергии, функциональной совместимостью и юридическим признанием.

Значимость:

- **Обеспечение безопасного управления медицинскими данными**: Предлагаемое решение решает важнейшие проблемы безопасности, конфиденциальности и совместного использования медицинских данных, способствуя разработке более безопасных и ориентированных на пациента систем управления медицинской информацией.
- **Стимулирование инноваций в здравоохранении**: используя передовые технологии, такие как блокчейн, ABE и IoT, патент поощряет инновации в области здравоохранения, что потенциально ведёт к улучшению ухода за пациентами, научных исследований и общей эффективности.
- **Расширение прав и возможностей пациентов**: акцент на контроле пациентами своих данных соответствует растущей тенденции развития здравоохранения, ориентированного на пациента, и может вдохновить на дальнейшие инновации в этом направлении.
- **Поощрение сотрудничества и обмена данными**: возможности системы безопасного обмена данными способствуют беспрецедентному уровню сотрудничества между поставщиками медицинских услуг, исследователями и другими заинтересованными сторонами, ускоряя прогресс в медицине.
- **Вклад в развивающийся ландшафт блокчейна в здравоохранении**: патент дополняет растущий объём исследований и инноваций, изучающих применение технологии блокчейн в секторе здравоохранения, помогая определить её будущее направление и потенциальное влияние.

A. Архитектура с двумя блокчейнами

Архитектура с двумя блокчейнами предлагает значительные преимущества в повышении безопасности, конфиденциальности, интеграции Интернета вещей, масштабируемости и контроле доступа к данным пациентов

1) Преимущества

Интеграция с устройствами Интернета вещей:

- Архитектура обеспечивает безопасный обмен медицинскими данными, собранными с различных медицинских устройств Интернета вещей и носимых устройств.
- Авторизованные поставщики медицинских услуг могут получить доступ к этим данным Интернета вещей для удалённого мониторинга, диагностики и лечения пациентов.
- Децентрализованный характер блокчейна повышает целостность и безопасность данных, генерируемых устройствами Интернета вещей.

Масштабируемость и производительность:

- Структура с двумя блокчейнами позволяет оптимизировать систему на основе конкретных требований каждого компонента блокчейна.
- Ограниченное участие в частном блокчейне может привести к более быстрой обработке транзакций и достижению консенсуса по сравнению с публичными блокчейнами.
- Методы распараллеливания могут быть использованы для увеличения пропускной способности системы и сокращения сетевого трафика.

Контроль доступа к данным пациента:

- Пациенты имеют контроль над своими медицинскими данными и могут предоставлять или отзывать разрешения на доступ определённым пользователям или организациям.
- Политика контроля доступа обеспечивается с помощью смарт-контрактов на блокчейне.
- Детальный контроль доступа осуществляется с помощью шифрования на основе атрибутов, гарантирующего доступ к данным пациента только авторизованным сторонам.

2) Ограничения:

Сложность и проблемы с внедрением:

- Архитектура с двойным блокчейном включает в себя множество компонентов и технологий, которые могут создавать проблемы с точки зрения сложности, функциональной совместимости и внедрения организациями здравоохранения.
- Интеграция системы с существующей инфраструктурой здравоохранения и обеспечение совместимости могут оказаться сложными задачами.

Соответствие нормативным требованиям:

- Обеспечение соблюдения правил и стандартов конфиденциальности медицинских данных может быть сложной задачей и потребовать дополнительных мер.
- Ориентироваться в нормативно-правовом ландшафте различных юрисдикций может быть сложно.

Ограничения на масштабируемость и производительность:

- Хотя архитектура с двумя блокчейнами направлена на повышение масштабируемости и производительности, способность системы обрабатывать большие объёмы медицинских данных в реальных сценариях нуждаётся в дальнейшей проверке.
- Механизм консенсуса и синхронизация данных по-прежнему могут сталкиваться с проблемами масштабируемости.

3) Влияние:

Повышение безопасности управления медицинскими данными:

- Архитектура с двумя блокчейнами решает важнейшие задачи в области безопасности, конфиденциальности и совместного использования медицинских данных.
- Это способствует разработке более безопасных и ориентированных на пациента систем управления медицинской информацией.

Обеспечение безопасного обмена данными и совместной работы:

- Архитектура облегчает безопасный обмен медицинскими данными между уполномоченными организациями, способствуя сотрудничеству между поставщиками медицинских услуг, исследователями и другими заинтересованными сторонами.
- Это обеспечивает беспрецедентный уровень обмена данными при сохранении конфиденциальности пациентов.

Расширение прав и возможностей пациентов:

- Предоставляя пациентам контроль над их правами доступа к медицинским данным, система расширяет возможности пациентов и соответствует тенденции развития здравоохранения, ориентированного на пациента.
- Это позволяет пациентам выборочно делиться своими данными для улучшения обслуживания и исследовательских целей.

B. Шифрование на основе атрибутов (ABE)

ABE предлагает значительные преимущества в повышении безопасности, конфиденциальности и детальном контроле доступа к медицинским данным, обеспечивая при этом их безопасный обмен и расширение прав и возможностей пациентов. Однако масштабируемость, производительность и соблюдение нормативных требований остаются ключевыми проблемами, требующими решения.

1) Преимущества:

Повышенная безопасность и конфиденциальность:

- ABE позволяет шифровать данные таким образом, что только пользователи, обладающие определёнными атрибутами, могут расшифровывать данные и получать к ним доступ, обеспечивая детальный контроль доступа
- Это позволяет пациентам хранить свои медицинские записи в зашифрованном виде и

криптографически обеспечивает соблюдение политик доступа пациентов или организаций.

- ABE защищает конфиденциальную медицинскую информацию от несанкционированного доступа, повышая конфиденциальность.

Интеграция с блокчейном и Интернетом вещей:

- ABE можно эффективно комбинировать с технологией блокчейн для обеспечения безопасного и децентрализованного контроля доступа в средах Интернета вещей, включая здравоохранение.
- Это позволяет безопасно обмениваться данными, собранными с различных медицинских устройств Интернета вещей и носимых устройств, между авторизованными сторонами.
- Интеграция ABE и блокчейна обеспечивает целостность, конфиденциальность и возможность проверки данных Интернета вещей.

Детальный контроль доступа:

- ABE обеспечивает детальный контроль доступа к зашифрованным данным, позволяя определять политики доступа на основе атрибутов.
- Он поддерживает политики доступа, которые могут быть представлены в виде логических формул или древовидных структур, что позволяет применять сложные требования к контролю доступа.
- Различным заинтересованным сторонам в сфере здравоохранения, таким как врачи, медсестры и исследователи, могут быть предоставлены разные уровни доступа к данным о пациентах в зависимости от их характеристик.

2) Ограничения:

Масштабируемость и производительность:

- Схемы ABE могут сталкиваться с проблемами масштабируемости, особенно при работе с большим количеством атрибутов или сложными политиками доступа.
- Вычислительные затраты на операции шифрования и дешифрования в ABE растут со сложностью политик доступа и количеством задействованных атрибутов.
- Эффективные механизмы управления ключами и отзыва атрибутов имеют решающее значение для практического внедрения ABE в крупномасштабных системах.

Соответствие нормативным требованиям:

- Внедрение ABE в системах здравоохранения должно обеспечивать соблюдение правил и стандартов конфиденциальности данных, может быть непростой задачей.
- Обеспечение баланса между необходимостью детального контроля доступа и требованиями экстренного доступа к данным пациента в критических ситуациях является сложной проблемой.

3) Влияние:

Обеспечение безопасного обмена данными и совместной работы:

- ABE облегчает безопасный обмен конфиденциальными медицинскими данными между уполномоченными сторонами
- Это позволяет осуществлять детальный контроль доступа, гарантируя, что разные пользователи могут получать доступ только к определённым данным.

Расширение прав и возможностей пациентов:

- Интегрируя ABE в системы здравоохранения, пациенты могут иметь больший контроль над тем, кто может получить доступ к их медицинским записям и при каких условиях.
- Такой подход, ориентированный на пациента, соответствует растущей тенденции предоставления пациентам возможности самостоятельно управлять своими медицинскими данными.

Развитие здравоохранения с сохранением конфиденциальности:

- ABE вносит свой вклад в разработку решений для здравоохранения, обеспечивающих конфиденциальность, безопасное хранение медицинских данных и обмен ими в облачных средах.
- Он решает важнейшие проблемы безопасности данных и конфиденциальности в эпоху цифрового здравоохранения и Интернета вещей.

C. Алгоритм консенсуса, основанный на доказательстве объёма транзакции

Алгоритм консенсуса, основанный на доказательстве объёма транзакции, предлагает преимущества с точки зрения оптимизации пропускной способности транзакций, стимулирования активного участия и решения проблем масштабируемости. Однако у него также есть ограничения, связанные с потенциальной централизацией, уязвимостью к атакам и проблемами с внедрением.

1) Преимущества:

Оптимизированная пропускная способность транзакций:

- Основная цель алгоритма - оптимизировать пропускную способность транзакций, позволяя сети блокчейн эффективно обрабатывать больший объём транзакций.

- За счёт приоритизации узлов с более высокими объёмами транзакций алгоритм направлен на повышение общей пропускной способности сети и способности обрабатывать большое количество транзакций.

Решение проблем масштабируемости:

- Алгоритм направлен на устранение низкой пропускной способности транзакций и ограничений масштабируемости существующих общедоступных решений для обработки медицинских данных на основе блокчейна.
- Уделяя особое внимание объёму транзакций как ключевому показателю, алгоритм стремится повысить способность сети обрабатывать крупномасштабные данные, генерируемые в медицинских сценариях Интернета вещей.

2) Ограничения:

Потенциальная централизация:

- Если небольшое количество узлов последовательно обрабатывает значительно больший объём транзакций, они могут получить непропорционально большое влияние на процесс согласования.
- Это может привести к некоторой централизации, подрывающей децентрализованный характер сети блокчейнов.

Уязвимость к атакам:

- Узлы с большими объёмами транзакций могут стать объектами атак, поскольку их компрометация позволит злоумышленнику нарушить процесс согласования.
- Алгоритму могут потребоваться дополнительные меры безопасности для снижения риска таких атак.

Сложность и проблемы с внедрением:

- Внедрение и интеграция алгоритма с существующими системами могут создавать проблемы с точки зрения сложности и внедрения.
- Эффективность алгоритма в реальных медицинских сценариях Интернета вещей требует дальнейшей проверки и тестирования.

3) Влияние:

Продвижение масштабируемых блокчейн-решений:

- Алгоритм способствует разработке более масштабируемых и эффективных блокчейн-решений для обработки больших объёмов транзакций.
- Это решает важнейшую проблему применения технологии блокчейн в областях с большим объёмом данных

Продвижение внедрения блокчейна в здравоохранении:

- Оптимизируя пропускную способность транзакций, алгоритм может сделать блокчейн более жизнеспособным для управления большими объёмами медицинских данных и обмена ими.
- Это может способствовать внедрению технологии блокчейн в отрасли здравоохранения, обеспечивая безопасное и эффективное управление данными и совместную работу.

Поощрение инноваций в алгоритмах достижения консенсуса:

- Алгоритм представляет собой инновационный подход к достижению консенсуса, ориентированный на объём транзакций как ключевой показатель.
- Это способствует текущим исследованиям и разработке новых согласованных алгоритмов, адаптированных к конкретным случаям использования и требованиям.

D. Контроль доступа к данным пациента

Механизм контроля доступа к данным пациента предлагает значительные преимущества с точки зрения повышения безопасности, конфиденциальности, детального контроля и расширения возможностей пациента.

1) Преимущества:

Повышенная безопасность и конфиденциальность:

- Система гарантирует, что пациенты имеют разрешения на управление своими медицинскими данными, защищая их права и интересы.
- Детальный контроль доступа с помощью шифрования на основе атрибутов (ABE) позволяет только авторизованным пользователям с определёнными атрибутами получать доступ к данным или изменять их.
- Политики контроля доступа применяются с помощью смарт-контрактов на блокчейне, обеспечивая автоматизированный и безопасный способ управления разрешениями.

Интеграция с блокчейном и Интернетом вещей:

- Механизм контроля доступа к данным пациента интегрирован с более широкой медицинской системой IoT-транзакций на основе блокчейна, предложенной в патенте.
- Эта интеграция обеспечивает безопасный и контролируемый доступ к данным, генерируемым различными медицинскими устройствами Интернета вещей и носимыми устройствами.
- Неизменяемость и прозрачность блокчейна устанавливают доверие к системе и обеспечивают целостность данных.

Детальный контроль доступа:

- Система использует шифрование на основе атрибутов (ABE) для обеспечения детального контроля доступа к данным.
- Политики доступа могут определяться на основе различных атрибутов, таких как роли пользователей, местоположения или другие соответствующие факторы, что обеспечивает детальный и гибкий контроль доступа.

2) Ограничения:

Сложность и проблемы с внедрением:

- Внедрение детального контроля доступа и интеграция его с системами блокчейна и интернета вещей могут быть сложными, требующими значительных технических знаний и ресурсов.
- Проблемы с внедрением могут возникнуть из-за необходимости для организаций здравоохранения адаптировать свои существующие системы и процессы для включения новых механизмов контроля доступа.

Проблемы с масштабируемостью и производительностью:

- По мере роста объёма данных о пациентах и числа пользователей могут быть протестированы масштабируемость и производительность системы контроля доступа.
- Эффективное управление ключами, отзыв атрибутов и обновления политик становятся решающими для поддержания оперативности и эффективности системы.

3) Влияние:

Обеспечение безопасного обмена данными и совместной работы:

- Отлаженная система контроля доступа облегчает безопасный обмен данными о пациентах между уполномоченными заинтересованными сторонами в сфере здравоохранения, способствуя сотрудничеству и улучшая координацию медицинской помощи.
- Это позволяет исследователям получать доступ к анонимизированным данным пациентов для медицинских исследований, сохраняя при этом конфиденциальность пациента.

Стимулирование инноваций в сфере безопасности здравоохранения:

- Интеграция блокчейна, Интернета вещей и шифрования на основе атрибутов для контроля доступа к данным пациентов представляет собой инновационный подход к безопасности медицинских данных.
- Он демонстрирует потенциал использования новейших технологий для решения важнейших проблем конфиденциальности данных, безопасности и расширения прав и возможностей пациентов в эпоху цифрового здравоохранения.

E. Функции удалённой диагностики, обмена данными и транзакций данных

Функции удалённой диагностики, обмена данными и транзакций данных предлагают значительные преимущества с точки зрения улучшения доступа к медицинскому обслуживанию, расширения обмена данными и совместной работы. Однако существуют ограничения, связанные с техническими проблемами, соображениями безопасности данных и конфиденциальности, а также проблемами внедрения и интеграции.

1) Преимущества:

Улучшение доступа к медицинскому обслуживанию:

- Дистанционная диагностика позволяет пациентам получать медицинские консультации и диагнозы, не выходя из дома.
- Это особенно полезно для пациентов в сельской местности, пожилых пациентов или лиц с ограниченными физическими возможностями, которым может быть трудно получить доступ к традиционным медицинским учреждениям.
- Удалённый мониторинг позволяет непрерывно отслеживать данные о состоянии здоровья пациентов, обеспечивая раннее выявление потенциальных проблем со здоровьем и вмешательство в них.

Улучшенный обмен данными и совместная работа:

- Система облегчает безопасный обмен медицинскими данными между уполномоченными сторонами, такими как поставщики медицинских услуг, исследователи и страховщики.
- Технология блокчейн обеспечивает целостность, конфиденциальность и возможность проверки совместно используемых данных.
- Улучшенный обмен данными способствует сотрудничеству и позволяет принимать более обоснованные решения при уходе за пациентами.

Эффективные операции с данными:

- Система обеспечивает эффективные и безопасные транзакции данных между различными заинтересованными сторонами в экосистеме здравоохранения.
- Смарт-контракты могут автоматизировать процессы доступа к данным и совместного использования, снижая административные издержки и повышая эффективность.
- Безопасные транзакции с данными помогают сохранить конфиденциальность пациентов, обеспечивая при этом авторизованный доступ для законных целей.

2) Ограничения:

Технические проблемы:

- Для реализации удалённой диагностики и мониторинга может потребоваться специализированное оборудование и надёжное подключение к Интернету, что может быть сложной задачей в определённых областях.
- Обработка больших объёмов данных, генерируемых устройствами Интернета вещей, и обеспечение обработки и анализа в режиме реального времени могут быть технически сложными.

Вопросы безопасности и конфиденциальности данных:

- Обмен конфиденциальными медицинскими данными вызывает опасения по поводу безопасности данных и конфиденциальности пациентов.
- Для предотвращения несанкционированного доступа и утечки данных необходимо внедрить надёжные меры безопасности, такие как шифрование и механизмы контроля доступа.
- Соблюдение правил защиты данных, таких как HIPAA, усложняет проектирование и внедрение системы.

Проблемы внедрения и интеграции:

- Внедрение технологий дистанционной диагностики и мониторинга может потребовать значительных изменений в существующих рабочих процессах здравоохранения.
- Поставщикам медицинских услуг может потребоваться обучение и поддержка для эффективного использования новых технологий и интерпретации полученных данных.
- Интеграция с существующими системами электронной медицинской карты (EHR) и обеспечение бесперебойного обмена данными могут оказаться сложной задачей.

3) Влияние:

Трансформация системы оказания медицинской помощи:

Функции удалённой диагностики, обмена и транзакций данных потенциально могут преобразовать оказание медицинской помощи, сделав его более доступным, эффективным и ориентированным на пациента.

Эти технологии позволяют перейти к проактивной и профилактической помощи, снижая нагрузку на медицинские учреждения и улучшая результаты лечения пациентов.

Продвижение персонализированной медицины:

- Постоянный мониторинг и анализ данных о пациентах с помощью дистанционного мониторинга позволяет проводить персонализированные и целевые вмешательства.
- Медицинские работники могут разрабатывать планы лечения на основе индивидуальных потребностей пациента и его реакции, что приводит к более эффективному уходу.

Внедрение системы здравоохранения, основанной на данных:

- Система генерирует огромное количество медицинских данных, которые могут быть использованы для исследований, аналитики и поддержки принятия решений.
- Анализ агрегированных и анонимизированных данных о пациентах может привести к пониманию характера заболеваний, эффективности лечения и тенденций в области здоровья населения.
- Подходы, ориентированные на данные, могут служить основой для политики здравоохранения, распределения ресурсов и разработки новых методов лечения и вмешательств.