УДК 004

В.А. Вишняков[1], И.В. Ся, Ч. Юй
[1]vish2002@mail.ru
Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь

ТЕХНОЛОГИЯ БЛОКЧЕЙН В СЕТИ ИНТЕРНЕТА ВЕЩЕЙ ДЛЯ ЗАЩИТЫ ДАННЫХ ОБУЧАЕМЫХ И ПАЦИЕНТОВ

В докладе предложено использовать технологию блокчейн для защиты конфиденциальных данных обучаемых и пациентов. Разработана архитектура интегрированной системы, которая объединяет сеть IoT, файловую структуру IPFS (InterPlanetary File System) с блокчейн Ethereum для создания надежной модели хранения данных. Эта система обеспечивает эффективную, безопасную и прозрачную обработку данных, оптимизируя процессы их регистрации, авторизации и проверки.

***Ключевые слова**: блокчейн, сеть IoT, безопасность данных, смарт контракт.*

Uladimir A. Vishniakou[1], I.W. Xia, C.Y. Yu
[1]vish2002@mail.ru;
Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus

BLOCKCHAIN TECHNOLOGY IN THE INTERNET OF THINGS NETWORK FOR DATA PROTECTION OF TRAINEES AND PATIENTS

The report suggests using blockchain technology to protect confidential data of trainees and patients. An integrated system architecture has been developed that combines the IoT network, the IPS (InterPlanetary File System) file structure with the Ethereum blockchain to create a reliable data storage model. This system ensures efficient, secure and transparent data processing, optimizing the processes of registration, authorization and verification.

***Keywords**: blockchain, IoT network, data security, smart contract.*

Введение

Технология интернета вещей (IoT) [1] включает сеть устройств и датчиков, соединенных между собой через интернет, способных собирать, обмениваться и обрабатывать данные для обеспечения эффективных и интеллектуальных операций. Однако технология IoT имеет проблемы в области безопасности данных, защиты конфиденциальности, которые варьируются от рисков утечки данных, уязвимостей в безопасности устройств и данных. Для обеспечения безопасности среды интернета вещей и эффективной защиты данных пользователей необходима стратегия безопасности, включающая усиление защиты устройств, шифрование данных, разработку и обеспечение соблюдения политик защиты конфиденциальности пользователей.

Технология блокчейн Ethereum [2] обеспечивает безопасность и неизменность данных благодаря хэшированию, шифрованию и децентрализации.

Ее применение в сетях IoT позволит обеспечить безопасность данных и конфиденциальность пользователей [3]. Ethereum – это платформа смарт-контрактов, основанная на технологии блокчейн, используемая для создания децентрализованных приложений (DApps).

Структура хранения данных IoT с использованием файловой системы и Ethereum

В системе интернета вещей IT-диагностики данные от датчиков, отправляются на локальный сервер. Сервер получает данные по протоколу HTTP и взаимодействует с веб-сервером с использованием WSGI (Web Server Gateway Interface). Сервер использует программу Flask для обработки данных, которые затем обрабатываются моделями нейронных сетей GRU, LSTM и RNN. Эти модели анализируют данные для генерации прогнозов. Сервер также включает базу данных для их хранения и извлечения.

На рис. 1 показана разработанная структура системы хранения данных IoT, использующая технологию блокчейн Ethereum и включающая процесс регистрации, авторизации и проверки данных через Ethereum и файловую систему (IPFS).

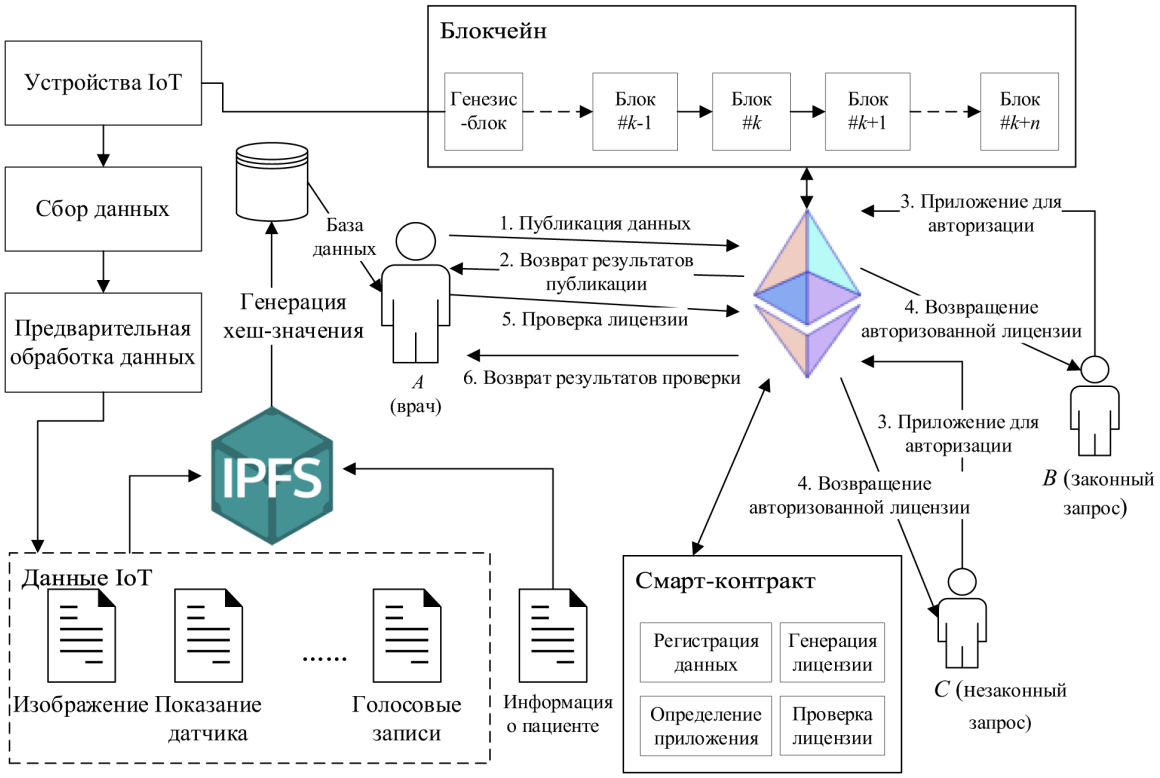

Рис. 1. Структура хранения данных с использованием Ethereum и IPFS

Ключевые компоненты, изображенные на рисунке 1, включают:

– сеть блокчейн: начинается с генезис-блока, за которым идет последовательность взаимосвязанных блоков (#*k*–1, #*k*, #*k*+1, #*k*+*n*). Это – структура данных блокчейна, где каждый блок содержит ряд транзакций, связанных через хэш-значения с предыдущим блоком.

– взаимодействие с пользователем: пользователь *A* отвечает за загрузку в систему данных, которые могут быть изображениями, показаниями датчиков, голосовыми записями или информацией о пациенте. Пользователи *B* и *C* запрашивают авторизацию для доступа к определенным данным или выполнения действий. Пользователь *B* получает разрешение на предоставление лицензии, в то время как заявка пользователя *C* завершается неудачей из-за незаконного запроса (например, из-за отсутствия лицензии);

– у смарт-контрактов – ключевая роль в системе, они выполняют регистрацию данных, генерацию лицензий, определение приложения и проверку лицензий.

Представим алгоритм работы системы IoT с блокчейн.

1. Ввод данных пациента и сбор данных с устройств IoT: пациенты используют смартфоны и различные устройства IoT для входа в систему и отправки своих личных данных. Эти устройства могут быть носимыми простыми датчиками, отслеживающими частоту сердечных сокращений и уровни активности, либо сложными датчиками, которые отслеживают уровень глюкозы в крови или кровяное давление.

2. Загрузка и хранение данных: данные загружаются на локальный сервер Flask с использованием протокола HTTP. Сервер Flask обрабатывает запрос и сохраняет полученные показатели в базе данных MongoDB, которая действует как центральное хранилище для этой информации.

3. Обработка прогнозирования: сервер Flask обрабатывает сохраненные данные, отправляя их агенту прогнозирования нейронной сети. Прогнозы, сделанные этим агентом, сохраняются обратно в базу данных MongoDB для ведения записей и дальнейшего использования.

4. Распространение результатов среди клиентов: пациенты получают результаты прогнозирования через HTTP-ответ. Кроме того, результаты распространяются среди врачей в режиме реального времени по протоколу MQTT, поддерживаемому брокером EMQX.

5. Резервное копирование данных через IPFS: в сеть IPFS экспортируется база данных MongoDB, которая включает как необработанные данные о пользователях, так и сгенерированные прогнозы.

6. Запись хэш-значений в блокчейн: всякий раз, когда резервная копия базы данных создается из MongoDB и сохраняется в IPFS, результирующие хэш-значения фиксируются в сети блокчейн. Пользователь *A*, который авторизован для обработки данных пациента, инициирует этот процесс. База данных MongoDB извлекает существующие данные из IPFS всякий раз, когда возникает необходимость записать новые данные для пользователя.

7. Контроль доступа к данным смарт-контрактов. Смарт-контракты на блокчейне запрограммированы для осуществления критически важных

функций в управлении корфиденциальными данными и доступе к ним. Они выполняют:

– регистрацию данных: когда пользователь *A* загружает новые данные в IPFS и записывает соответствующие хэш-значения в блокчейн, смарт-контракт регистрирует эти записи, гарантируя происхождение данных;

– генерацию лицензии: по запросу пользователя *B* смарт-контракт генерирует лицензию или токен, который предоставляет доступ к указанным данным. Этот процесс включает проверку учетных данных пользователя *B* и его намерений обеспечить соответствие политике доступа к данным;

– определение приложения: смарт-контракт автоматизирует оценку запросов на доступ. Когда пользователь *B* подает заявку на доступ к данным, смарт-контракт определяет законность запроса на основе предопределенных правил. И, наоборот, если пользователь *C* делает запрос, смарт-контракт идентифицирует его, как несанкционированный (из-за отсутствия предопределенных правил), и отказывает в доступе;

– проверку лицензии: при попытке доступа к данным смарт-контракт проверяет соответствие выданным лицензиям или токенам. Доступ к данным, хранящимся в IPFS, предоставляется только запросам, в которых указана лицензия, выданная пользователю *B*. Пользователю *C*, не имеющему такой лицензии, будет отказано, что гарантирует сохранность данных от несанкционированных изменений или взломов.

В контексте IT-диагностики пользователей работник (пользователь *A*) загружают информацию об обучаемом или пациенте, которая может включать записи или изображения. Смарт-контракты играют решающую роль в этой системе, управляя регистрацией данных в блокчейне, обеспечивая их подлинность с помощью уникальных значений хэша. Они также обрабатывают выдачу лицензий на доступ к данным, оценивая и подтверждая запросы пользователей на основе предопределенных критериев. Например, учитель, запрашивающий доступ к данным обучаемого, получит лицензию после выполнения необходимых условий. Файловая система IPFS [4] используется для децентрализованного хранения конфиденциальных файлов, что повышает безопасность и доступность данных. Система гарантирует, что только авторизованный персонал может получить доступ к конфиденциальным учебным или медицинским данным, тем самым сохраняя их конфиденциальность и целостность при управлении.

Смарт контракт

Смарт-контракт разработан с целью обеспечения безопасной структуры для хранения, управления и обмена медицинской информацией. В его состав входят:

– структуры данных: хранит хэш-значение учебных или медицинских записей, адрес владельца и статус доступности записи. Управляет правами доступа к записям для конкретных лиц (например, учителей, врачей);

– сопоставление хэшей данных с соответствующими записями: сопоставляет хэши данных и индивидуальные адреса с их правами доступа;

– события для регистрации записей обучаемого, предоставления, отзыва и проверки разрешений на доступ.

Интеграция IPFS с технологией блокчейн Ethereum поддерживает хранение больших данных, предлагая безопасное и эффективное решение, подходящее для управления данными в образовании и здравоохранении. Система повышает надежность и долговечность данных за счет снижения зависимости от централизованных серверов благодаря IPFS, децентрализованной системе хранения. Это обеспечивает целостность и неизменяемость данных. Изменения в данных изменяют их хэш-значение IPFS, что облегчает проверку. Хэш-значения, хранящиеся в блокчейне, обеспечивают постоянную запись, используя блокчейн.

Предложенный подход превосходит традиционное облачное хранилище по экономической эффективности, особенно для больших данных. Кроме того, он повышает безопасность данных, шифруя их в IPFS и сохраняя только хэш-значения в блокчейне, таким образом защищая конфиденциальную информацию. Эта технология применяется в управлении записями, обеспечивая неизменность и целостность данных как обучаемых так и пациентов.

Пользователь *A* публикует данные, которые затем отправляются в IPFS и регистрируются в блокчейне, создавая хэш-значение. Пользователи *B* и *C* обращаются к смарт-контракту для сбора или проверки данных, и смарт-контракт определяет, предоставлять ли авторизацию на основе встроенных правил. Для авторизованных запросов смарт-контракт генерирует лицензию и возвращает ее пользователю, для неавторизованных – возвращает результат сбоя.

Заключение

В докладе реализована интеграция блокчейна Ethereum и файловой системы IPFS с сетью IoT IT-диагностики для создания конфиденциальности хранения больших данных обучаемых и пациентов. Разработана система хранения данных IoT с использованием блокчейна Ethereum в сети IT-диагностики, позволяющая учителям или медицинским работникам безопасно загружать информацию о пациентах. Смарт-контракты управляют аутентичностью данных и контролем доступа.

Список литературы

1. Vishniakou U. A. Specialized IoT Systems: Models, Structures, Algorithms, Hardware, Software Tools. Minsk: Belarusian State University of Informatics and Radioelectronics. 2023:184.

2. Tikhomirov S. (2018) Ethereum: State of Knowledge and Research Perspectives. Foundations and Practice of Security: 10th International Symposium:206–221.

3. Bahga A., Madisetti V. K. (2016) Blockchain Platform for Industrial Internet of Things. Journal of Software Engineering and Applications. 9 (10):533–546.

4. Trautwein D., Raman A., Tyson G. (2022) Design and Evaluation of IPFS: A Storage Layer for the Decentralized Web. Proceedings of the ACM SIGCOMM:739–752.