Д. А. Коренев, А. А. Захаров
Тюменский государственный университет, г. Тюмень
УДК 004.056.2

ИСПОЛЬЗОВАНИЕ БЛОКЧЕЙН-ТЕХНОЛОГИИ ДЛЯ ДЕЦЕНТРАЛИЗОВАННОЙ ЗАЩИЩЕННОЙ СИСТЕМЫ IOT

Аннотация. *Интернет вещей — технология, использующаяся во всех сферах повседневной жизни, от здравоохранения до технологического производства. Однако безопасность Интернета вещей до сих пор остается открытым вопросом, так как в случае несанкционированного доступа данные с датчиков могут быть изменены, например, пользователем с авторизованными правами доступа, что может привести к непредвиденным последствиям.*

Ключевые слова: *информационная безопасность, блокчейн, Интернет вещей, децентрализация*.

Введение. На данный момент централизованные сервера используются для сбора данных с устройств Интернета вещей (IoT), которые являются дополнительным вектором атаки и также должны подлежать защищены, потому что, в случае если сервер будет недоступен, данные с устройств не попадут в базу данных. Некоторые из методов защиты могут быть довольно эффективными, но они не дают большой гарантии. В настоящее время наблюдается тенденция к децентрализации, которая постепенно приходит на смену более распространенной клиент-серверной архитектуре. В отличие от архитектуры клиент-сервер — децентрализованная архитектура блокчейна, которая обладает рядом преимуществ в области безопасности [1-3]:

- доверие основано на математической модели и поддерживается криптографическими методами;
- естественная невосприимчивость к единственной точке отказа;
- невосприимчивость к атаке повторного воспроизведения.

Однако существует несколько проблем, связанных с производительностью и масштабируемостью классических моделей блокчейна, таких как Bitcoin, Etherium и т. д. Альтернативы, предложенные

другими исследователями [4], не учитывают такие особенности области медицины, как:

- связь с другими данными, поскольку необходимо знать, к каким данным пациента относятся;
- более эффективные механизмы хранения данных.

Проблема исследования. Предложить архитектуру сети блокчейн для защищенного и эффективного хранения данных с устройств Интернета вещей.

Материалы и методы. Основной целью этой работы является создание более эффективной модели блокчейна, которая может решить вышеуказанные проблемы. Чтобы рассмотреть какие-либо варианты, необходимо выяснить, как работает блокчейн. Когда происходит каждая транзакция, она записывается как «блок» данных, эти транзакции показывают движение актива, который может быть материальным (продукт) или нематериальным (интеллектуальный). Блок данных может записывать информацию по вашему выбору: кто, что, когда, где, сколько и даже условия — например, температура доставки еды. Каждый блок связан с блоками до и после него, эти блоки образуют цепочку данных по мере того, как актив перемещается с места на место или переходит из рук в руки. Блоки подтверждают точное время и последовательность транзакций, и блоки надежно связаны друг с другом, чтобы предотвратить изменение любого блока или вставку блока между двумя существующими блоками. Каждый дополнительный блок усиливает проверку предыдущего блока и, следовательно, всего блокчейна. Это делает подделку блокчейна очевидной, обеспечивая ключевую силу неизменности. Это исключает возможность вмешательства злоумышленника и создает реестр транзакций, которому вы и другие участники сети можете доверять [5]. Пример блокчейн-схемы проиллюстрирован на рис. 1.

В базовой архитектуре блокчейна каждая транзакция должна быть проверена, тем самым выявляются блоки, которые были изменены тем или иным образом. Блокчейн представляет собой одноранговую сеть подключенных устройств, при добавлении транзакции она передается на все узлы, доступные в сети. После того, как все

узлы получили транзакцию, запускается проверка транзакции, зачастую в блокчейне используется алгоритм SHA-256 для генерации хэша. После успешной проверки, блок отправляется в цепочку регистров и добавляется в существующую цепочку блоков, этот процесс показан на рис. 2 а-в.

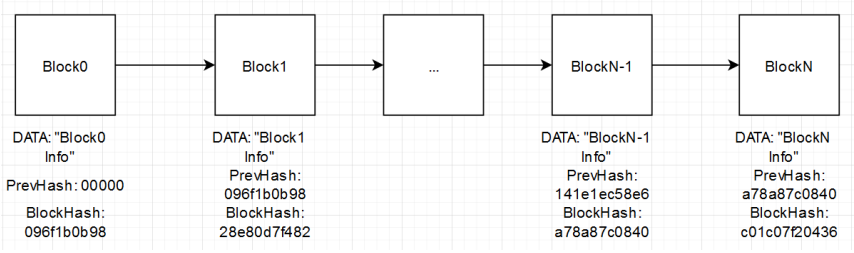

Рис. 1. Пример блокчейна

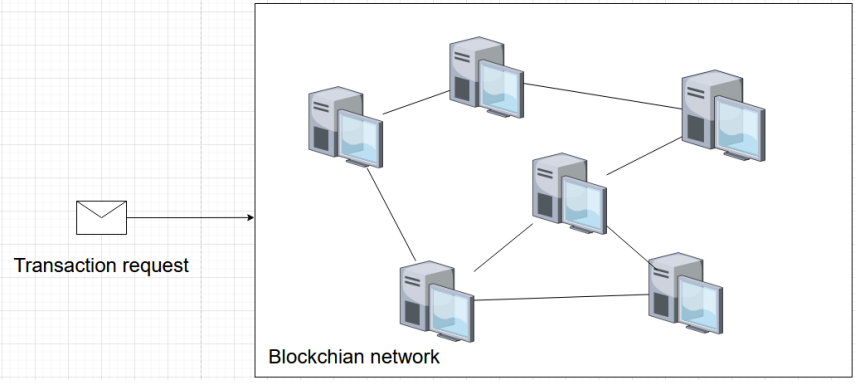

Рис. 2а. Пример запроса транзакции в блокчейн-сеть

Блокчейн подразделяется на несколько типов:

- публичный;
- частный;
- на основе разрешений.

В публичном блокчейне любой желающий может присоединиться к сети и внести свой вклад в нее. Любой желающий может читать, записывать и проверять текущую деятельность в публичной

сети, что помогает публичному блокчейну сохранять свой самоуправляемый характер. Но у этого подхода есть и обратная сторона, потому что этот тип блокчейна становится все более и более энергоемким, чем больше участников присоединяется к нему.

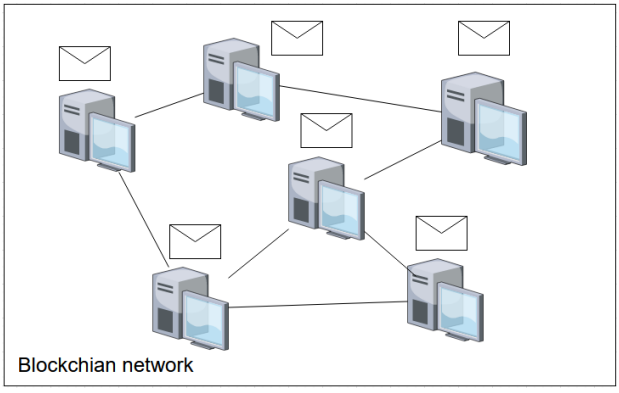

Рис. 2б. Передача тразакции в блокчейн-сети

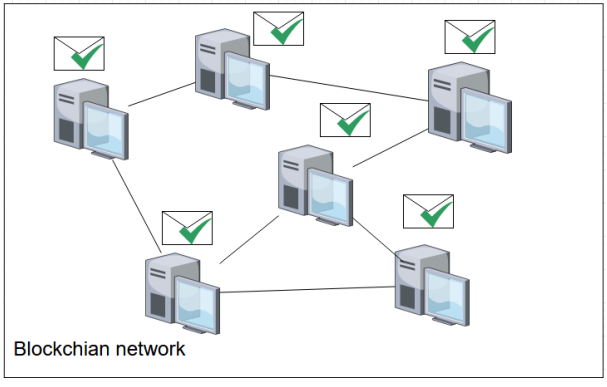

Рис. 2в. Подтверждение транзакции и синхронизация в блокчейна сети

Частный блокчейн допускает только проверенных участников путем аутентификации или подтвержденного приглашения. Это также позволяет выполнять консенсусный протокол, который определяет права на добычу новых блоков и вознаграждения, а также ведение общей «бухгалтерской книги».

Блокчейн на основе разрешений — это комбинация публичного и частного блокчейна с возможностью гибкой настройки позволяющей разграничить разрешенный функционал между членами сети. К примеру можно разрешить определенным нодам сети только просматривать блокчейн. Данный подход является самым оптимальным для нужд данного исследования, так как благодаря нему можно разрешить сторонним организациям безопасно собирать различную статистику.

Сущестует множество вариаций блокчейна которые используют различные виды подтверждения блока. В основном пременяются следущие методы:

• Proof of Work (PoW) — доказательство работы, который предполагает слжоное вычисление. это свидетельство затем принимается сетевыми узлами как созданное на основе вычисления хеш-функции.

• Proof of Stake (PoS) — доказательство владения, в котором узлы псевдослучайно выбираются для предложения следующего блока в цепочку в зависимости от количества «монет», которым владеет участник.

Вышеуказанные виды являются наиболее применяемыми и имеют свои преимущества и недостатки. PoW имеет более большее энергопотребление ввиду большого количества вычислений в сети, но и большую безопасность, в случае частного блокчейна или блокчейна на основе разрешений, эта проблема наиболее сильно смегчается. PoS же в свою очередь имеет более быструю архитектуру, но имеется проблема владения условных единиц ограниченным колвом людей, однако в случае частного или блокчейна на основе разрешений эта проблема решается. Но общая безопасность сети с алгоритмом PoS меньше чем у PoW ввиду свойств данных алгоритмов.

Важным фактором являются данные, для которых планируется взаимодействие, на данный момент рассматриваются такие данные, как: артериальное давление. уровень холестерина, уровень глюкозы. АСТ, АЛТ. Данные в блокчейне будут генерироваться на основе идентификатора устройства и данных, считываемых датчиком.

В случае применения обычной модели к устройствам Интернета вещей возникает несколько проблем:

• устройства Интернета вещей не имеют столько места для хранения всей цепочки блокчейн;

• вычислительная мощность устройств не позволяет выполнять более сложные вычислительные процессы, которые требуются при генерации блока.

В связи с этим предлагается перенести все формирование блокчейна на децентрализованные серверы в соответствии с моделью, описанной ниже на рис. 3. Это позволит решить проблему, связанную с необходимостью выполнения вычислений, а также хранения данных на устройстве Интернета вещей.

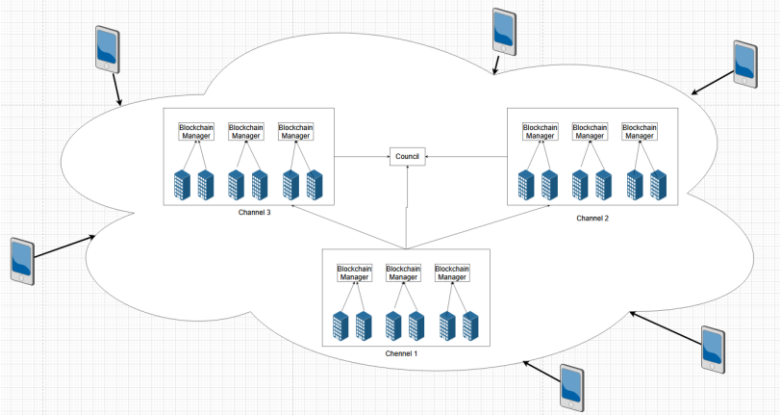

Рис. 3. Предлагаемая модель сети

Сеть частная, но в ней есть разрешения, то есть для каждого нового устройства требуется его регистрация в сети и установка для разрешений. Устройства Интернета вещей будут находиться на «внешнем» уровне, с которого запросы будут отправляться в облако, сервер выбирается в зависимости от его доступности, таким образом, все еще может быть обеспечена децентрализация и обеспечена защита от единой точки отказа. Единственным недостатком такого подхода является тот факт, что вам, возможно, придется выполнять дополнительные настройки, которые могут не поддерживаться некоторыми устройствами. Каналы — это точки, через которые устройства Интернета вещей будут передавать данные, а также

представляют собой соединения между больницами, которые могут быть расположены в другом облаке.

Блокчейн-менеджеры используются для генерации и сжатия данных в блокчейн, они также выступают в качестве источников для смарт-контрактов, поскольку в них хранится реплицированная копия блокчейн-сети.

Проверка сетевых блоков обрабатывается «советом», он содержит определенное колличество устройств, выполняющих проверку, тем самым обеспечивая защиту от единой точки отказа в случае, если один из узлов «совета» будет не доступен. «Совет» имеет взаимный доступ с «блокчейн-менеджерами», это показано на рис. 4.

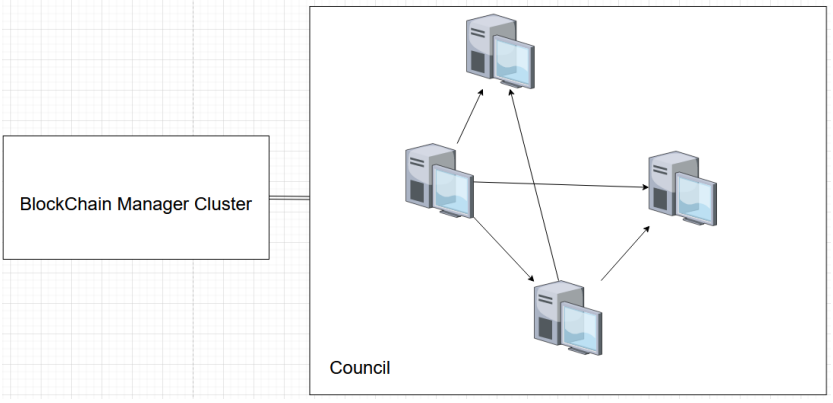

Рис. 4. Схема совета

Основываясь на схемах предствленных на рисунках 3 и 4, планируется следующее взаимодействие:

1) устройство Интернета вещей отправляет запрос на добавление к одному из каналов;

2) один из менеджеров блокчейна формирует запрос и отправляет его на проверку в «совет»;

3) после проверки блокчейн обновляется для всех, у кого есть разрешение на хранение блокчейна;

4) предоставление и анализ данных осуществляются при помощи смарт-контрактов.

Результаты. Результатом этой работы стала альтернативная модель децентрализованного и более безопасного хранения медицинских данных. Модель охватывает весь цикл передачи данных, начиная с отправки с устройств Интернета вещей и заканчивая безопасным получением данных третьей стороной с использованием смарт-контрактов.

Однако есть моменты, которые требуют дополнительного рассмотрения. Например, сколько блокчейн-менеджеров и членов «совета» необходимо для наилучшей производительности и как рассчитать их количество? Какую конфигурацию должны иметь эти устройства? А также как обеспечить более сильную связность данных и пациента, к которому они относятся.

Заключение. Эта работа предлагает альтернативную модель блокчейна, которая потенциально может быть более эффективной, чем другие модели. Был проведен обзор предлагаемой модели, описаны ее основные модули. В будущем планируется реализация блокчейн сети на основе предложенной модели.

СПИСОК ЛИТЕРАТУРЫ

1. Reyna A. On blockchain and its integration with IoT. Challenges and opportunities / A. Reyna, C. Martín. — Direct : text // Future Generation Computer Systems. — 2018. — Vol. 88. — P. 173-190.
2. Abbassi Y. IoT and Blockchain combined: for decentralized security / Y. Abbassi, H. Benlahmer. — Text : direct // Procedia Computer Science. — 2021. — Vol. 191. — P. 337-342.
3. Rathore S. BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network / S. Rathore, B. W. Kwon, J. H. Park. — Text : direct // Journal of Network and Computer Applications. — 2019. — Vol. 143. — P. 167-177.
4. Zeadally S. Lightweight Blockchain for Healthcare / S. Zedally, L. Ismail. — Text : direct // IEEE Access. — 2019. — Vol. 7. — P. 149935-149951.
5. Bodkhe U. Blockchain for Industry 4.0: A Comprehensive Review / U. Bodkhe, S. Tanwar. — Text : direct // IEEE Access. — 2020. — Vol. 8. — P. 79764-79800.