Обзор интеграции блокчейна и Интернета вещей: исследование текущих проблем

М. Ал-Хуссеини
Санкт-Петербургский государственный Технологический институт (Технический университет)

Аннотация: Рассматривается применение технологии блокчейн для решения проблем безопасности и отслеживаемости в сфере Интернета вещей (IoT). Описываются особенности и преимущества использования блокчейна, а также отмечены проблемы, которые могут возникнуть при интеграции блокчейна с IoT. Статья предоставляет общий обзор и руководство по рассмотрению ключевых проблем внедрения и разработки современного проекта на основе Интернета вещей и блокчейна (IoTB).
Ключевые слова: блокчейн, интернет вещей, IoT, BIoT, безопасность Интернет вещей, децентрализованные сети IoT

1. Введение

Появление технологии блокчейн произвело революцию в том, как мы воспринимаем одноранговые сети. Технология позволяет участникам сети безопасно и прозрачно совершать транзакции и обмениваться информацией. Изначально блокчейны рассматривались как распределенные реестры или базы данных, но внедрение смарт-контрактов значительно расширило их возможности.

Этот технологический прогресс привлек внимание разработчиков и отраслевых гигантов, особенно, в области Интернета вещей (IoT). IoT — преобразующая технология, которая преобразует традиционные устройства в интеллектуальные за счет использования интернет-протоколов и сенсорных сетей. Интеграция блокчейна и IoT (IoTB) привела к значительному прогрессу и преимуществам для различных секторов промышленности, где они были реализованы.

Однако интеграция этих двух мощных технологий не обходится без проблем. В статье рассматриваются проблемы, связанные с интеграцией блокчейна (BC) и Интернета вещей (IoT). Цель статьи — выделить конкретные проблемы, возникающие при интеграции технологии блокчейна

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

с Интернетом вещей (IoT). Определяя ключевые вопросы, такие, как потребление энергии, масштабируемость, безопасность и конфиденциальность, обращаем внимание на сложности, с которыми можно столкнуться при разработке и внедрении проектов блокчейна IoT (BIoT).

2. Предыстория

2.1. Технология блокчейн

Блокчейн — инновационная технология, представляющая собой цепочку блоков, которые содержат информацию. Эта технология использует принципы криптографии для обеспечения безопасности и целостности данных, делая каждый блок в цепочке уникальным и неизменным. Ключевым элементом блокчейна является его способность к созданию децентрализованных и распределенных реестров, где данные хранятся на множестве компьютеров, а не в одном центральном месте, что обеспечивает высокий уровень безопасности и надежности, поскольку данные не могут быть легко изменены или уничтожены [1].

Одной из основных особенностей блокчейна является его прозрачность. Каждая транзакция в блокчейне проверяется и записывается в общедоступный реестр, что обеспечивает полную прозрачность и возможность отслеживания истории транзакций. Это делает блокчейн идеальным для приложений, где требуется четкая аудиторская трассировка и подотчетность.

В контексте кибербезопасности, блокчейн предлагает уникальные преимущества. Он может служить защитой от несанкционированного доступа, предоставляя надежные механизмы для аутентификации и защиты данных. Это особенно важно для устройств Интернета вещей (IoT), где безопасность является критическим аспектом [2]. Блокчейн находит применение во многих других областях, включая медицину, логистику и правоохранительные органы.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

Блокчейн представляет собой мощный инструмент, способный радикально изменить способы ведения бизнеса, управления данными и обеспечения безопасности в цифровом мире. Его интеграция с технологиями, такими как IoT, открывает новые возможности для создания более безопасных, эффективных и прозрачных систем (Рис.1) [2].

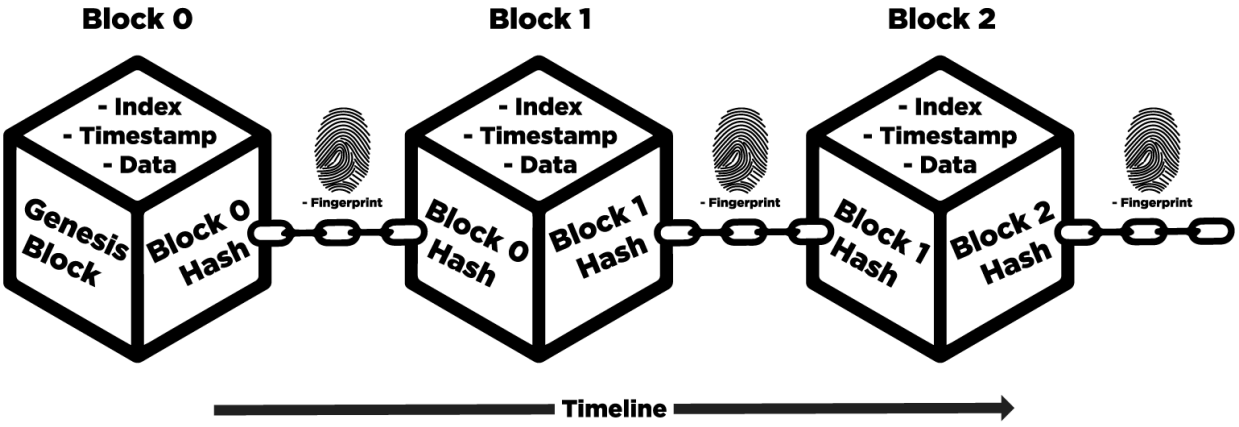

Рис. 1. – общая структура блокчейна

2.2. Интернет вещей (IoT)

Интернет вещей (IoT) представляет собой сеть физических устройств, от бытовых предметов до промышленного оборудования, подключенных к Интернету для сбора и обмена данными [3]. Развитие беспроводных технологий, MEMS и микросервисов позволило создать экосистему, где устройства взаимодействуют и общаются внутри глобальной информационной сети [4].

Основные характеристики IoT [3]:

- Связность: устройства IoT подключены к Интернету, обеспечивая удаленный мониторинг и контроль.
- Датчики: устройства IoT оснащены датчиками, собирающими данные из окружающей среды.
- Анализ данных: устройства IoT способны анализировать собранные данные, что позволяет им автоматически реагировать на изменения в

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

окружающей среде.

Индустриальный Интернет вещей (IIoT):

IIoT расширяет концепцию IoT в промышленной сфере, включая использование IoT-технологий для оптимизации производственных процессов и повышения эффективности. IoT и IIoT находят применение в различных секторах, включая умные дома, здравоохранение, сельское хозяйство и умные города, способствуя повышению уровня автоматизации и эффективности.

2.3. Интеграция блокчейна и IoT

Интеграция блокчейна и IoT — новая концепция, направленная на повышение функциональности и безопасности устройств и систем IoT. Сети IoT обычно полагаются на централизованные модели связи и управляются центральной системой управления сетью. Однако, по мере того, как количество устройств IoT продолжает расти в геометрической прогрессии, эта архитектура создает проблемы, связанные с масштабируемостью, безопасностью и едиными точками отказа. Блокчейн с его децентрализованной природой предлагает решение названных проблем, обеспечивая масштабируемую и безопасную структуру для взаимодействия и транзакций устройств IoT [5].

Преимущества интеграции: Интеграция блокчейна с IoT обеспечивает несколько ключевых преимуществ. Неизменность и прозрачность блокчейна затрудняют вмешательство третьих лиц в данные, которыми обмениваются устройства IoT, что повышает безопасность. Кроме того, блокчейн может хранить огромные объемы данных, генерируемых устройствами IoT, в децентрализованном виде, безопасном и с отметками времени, что обеспечивает лучшее управление данными и их проверку. Благодаря использованию смарт-контрактов, блокчейн также позволяет устройствам IoT

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

участвовать в автоматизированных микротранзакциях, представляющих собой транзакции, которые автоматически запускаются на основе определенных условий без необходимости стороннего вмешательства [5].

Примеры интегрированных систем: интеграция блокчейна и IoT ведется в нескольких секторах. Например, в управлении цепочками поставок устройства IoT отслеживают и записывают путь продукта от производителя к розничному продавцу на блокчейне, обеспечивая прозрачность и снижая риск мошенничества. В умных домах устройства IoT, такие, как счетчики энергии или умные холодильники, могут безопасно и автономно взаимодействовать, записывая свои данные и транзакции в блокчейн. Другой пример — в области сельского хозяйства, где датчики IoT могут записывать данные об окружающей среде в блокчейн для мониторинга и проверки условий ведения сельского хозяйства, повышая прослеживаемость сельскохозяйственной продукции [5].

В контексте систем IoT технология блокчейн приобретает все большую популярность в последнее десятилетие. Блокчейн, как распределенный и неизменяемый реестр, защищенный надежными алгоритмами криптографии, открывает новые перспективы для защиты систем IoT. Многие исследования были посвящены интеграции блокчейна в управление устройствами IoT, с целью обеспечения контроля доступа, целостности данных, безопасности и конфиденциальности. Инновационная сервисная платформа IoT, основанная на технологии блокчейна консорциума, абстрагирует межмашинные (M2M) и человеко-машинные (H2M) коммуникации в услуги, предоставляемые устройствами IoT. Затем материализует обмен данными сети IoT с помощью смарт-контрактов и транзакций блокчейна, демонстрируя потенциал блокчейна в децентрализации и обеспечении безопасности коммуникаций IoT [5].

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

3. Проблемы интеграции блокчейна и IoT

Несмотря на многообещающую синергию между технологией блокчейн и IoT, интеграция этих двух технологий - непростая задача. Необходимо решить многочисленные технические и нетехнические проблемы, прежде чем можно будет полностью реализовать потенциальные выгоды. Эти проблемы связаны с неотъемлемыми характеристиками технологий блокчейна и IoT, сложностями, ввиду их интеграции, а также с нормативными и правовыми ограничениями.

С точки зрения внутренних характеристик, системы IoT включают в себя множество устройств с ограниченной вычислительной мощностью и временем автономной работы, работающих в высокораспределенной и гетерогенной среде. Блокчейн, с другой стороны, является ресурсоемкой технологией, требующей значительных вычислительных мощностей для алгоритмов консенсуса, а также достаточной емкости хранилища для постоянно растущих реестров. Более того, существующие технологии блокчейна, разработанные в первую очередь для финансовых приложений, могут не подходить для контекстов IoT, которые требуют высокой масштабируемости, отклика в реальном времени и способности обрабатывать огромные объемы данных, генерируемых множеством устройств [6].

Кроме того, интеграция блокчейна и IoT порождает сложности, связанные с совместимостью систем, стандартизацией данных и общим дизайном системы. Например, фрагментация экосистем IoT из-за множества устройств, платформ и протоколов затрудняет создание единой системы блокчейна, которая может беспрепятственно работать на всех устройствах. Точно так же отсутствие универсальных стандартов для технологии блокчейн может привести к проблемам совместимости во время интеграции, тем самым делая процесс сложным и громоздким [6].

Нормативно-правовая среда представляет собой еще один спектр

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

проблем. Учитывая относительно недавно зарождающуюся стадию технологий IoT и блокчейна, многим юрисдикциям еще предстоит установить всеобъемлющие правила, касающиеся их развертывания, включая вопросы, связанные с конфиденциальностью данных, трансграничной передачей данных, законностью смарт-контрактов и т. д. [6].

Далее рассмотрим каждую из названых проблем, обсудим их последствия и возможные решения. Понимание этих проблем имеет решающее значение для успешного развертывания блокчейна в приложениях IoT и использования преимуществ этого тандема.

3.1. Масштабируемость

Масштабируемость является критическим вопросом, когда речь идет об интеграции блокчейна и IoT. Проблема возникает из-за того, что количество устройств IoT во всем мире исчисляется миллиардами и продолжает быстро расти. Каждое устройство генерирует данные, часто в режиме реального времени, и объем этих данных может быть огромным для блокчейна.

По своей сути блокчейн представляет собой распределенный реестр, в котором каждый узел сети хранит копию всей истории транзакций. По мере того, как устройства IoT продолжают генерировать данные, размер реестра растет, что делает его более ресурсоемким для обслуживания. В частности, хранение становится проблемой, поскольку каждый участвующий узел должен хранить каждую транзакцию с каждого устройства IoT в сети. Эта модель не является масштабируемой, учитывая огромное и растущее число устройств IoT.

Кроме того, блокчейн-сети обычно проверяют транзакции с помощью механизма консенсуса, что потребует много времени и вычислительных ресурсов. Это может существенно замедлить время обработки транзакции, и по мере увеличения количества транзакций (как это естественно будет в

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

контексте IoT) время, необходимое для обработки каждой транзакции, может стать узким местом, снижая производительность.

Хорошей иллюстрацией этой проблемы является сеть Bitcoin, которая может обрабатывать только 7 транзакций в секунду. Представим сценарий, в котором сеть IoT с миллионами устройств, каждое из которых выполняет несколько транзакций в секунду, построена на аналогичной модели блокчейна. Сеть будет быстро перегружена, что приведет к замедлению транзакций и сделает систему неэффективной.

Решение проблемы масштабируемости имеет решающее значение для интеграции блокчейна и IoT. Перспективным решением является архитектура Scalable and Trustworthy Blockchain (STB). STB использует сегментирование блокчейна и оракулы для установления доверия между ненадежными устройствами IoT полностью распределенным и заслуживающим доверия образом. Архитектура STB спроектирована так, чтобы быть масштабируемой и может обрабатывать большие объемы транзакций, типичные для сетей IoT. Масштабирование выполняется разделением блокчейн на более мелкие, более управляемые части (шарды), каждая из которых может обрабатывать транзакции независимо. Это позволяет STB быстрее обрабатывать больше транзакций, решая проблему масштабируемости [7]. Несмотря на эти возможные решения, проблема масштабируемости остается серьезным препятствием для широкого внедрения блокчейна в IoT.

3.2. Безопасность и конфиденциальность

Интеграция блокчейна и IoT создает серьезные проблемы безопасности и конфиденциальности. Одна из основных проблем - управление ключами. В блокчейне доступ к активам или данным контролируется криптографическими ключами. В контексте IoT каждое устройство должно управлять одним или несколькими наборами ключей для различных

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

операций. Безопасное создание, хранение и использование ключей — нетривиальная проблема. Например, если закрытый ключ утерян или украден, связанные с ним данные или активы могут стать навсегда недоступны или попасть в чужие руки. Такие решения, как аппаратные модули безопасности (HSM) или доверенные среды выполнения (TEE), могут обеспечить безопасное хранение ключей, но интеграция этих решений в потенциально миллионы или миллиарды устройств IoT может быть сложной и дорогостоящей.

Конфиденциальность — еще одна серьезная проблема. Устройства IoT часто собирают конфиденциальные данные, будь то данные о повседневной жизни пользователя с устройства умного дома или проприетарные операционные данные с промышленного датчика IoT. Когда эти данные хранятся в блокчейне, они фактически неизменны и могут быть прозрачными для всех участников сети, в зависимости от конструкции блокчейна. Это представляет потенциальный риск для личной или деловой конфиденциальности. Такие методы, как доказательства с нулевым разглашением или гомоморфное шифрование, могут позволить проверять и использовать данные без раскрытия фактических базовых данных, обеспечивая потенциальный путь к согласованию потребностей блокчейна и конфиденциальности.

Децентрализованная природа блокчейна также представляет собой обоюдоострый меч для безопасности. С одной стороны, децентрализация устраняет единые точки отказа, делая систему в целом более устойчивой к атакам. С другой стороны, децентрализация дает и новые векторы атаки. Например, в общедоступном блокчейне без разрешений объект с достаточными вычислительными ресурсами потенциально может взять на себя процесс консенсуса, что приведет к «атаке 51%». В контексте IoT аналогичная уязвимость может позволить злоумышленнику манипулировать

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

данными, поступающими с роя устройств, что приведет к постоянной записи неточной информации в блокчейне [8].

Таким образом, хотя блокчейн может обеспечить повышенную безопасность и доверие для приложений IoT, для эффективной реализации этих преимуществ необходимо тщательное рассмотрение управления ключами, конфиденциальности данных и последствий децентрализации для безопасности**.**

3.3. Функциональная совместимость

Функциональная совместимость является серьезной проблемой при интеграции блокчейна и IoT из-за разнообразия устройств, стандартов связи и протоколов. Устройства IoT часто сталкиваются с такими проблемами, как недостатки безопасности, проблемы конфиденциальности, неадекватная функциональная совместимость и отсутствие технических спецификаций [9]. Одним из решений для решения этих проблем является использование технологии блокчейн. Сегментирование блокчейна и оракулы используются для установления доверия между ненадежными устройствами IoT полностью распределенным и заслуживающим доверия образом. Введен новый облегченный алгоритм консенсуса, который резко масштабирует блокчейн, обеспечивая при этом функциональную совместимость между участниками блокчейна [4].

С технической стороны, различные устройства IoT могут использовать разные форматы данных или протоколы связи, что затрудняет обмен информацией друг с другом или с блокчейном. Эта проблема может быть решена с помощью промежуточного программного обеспечения или решений для преобразования протоколов, но это может усложнить систему и привести к потенциальным точкам отказа. Многообещающий отраслевой протокол IoT для глобальной совместимости, OMA Lightweight M2M

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

(LwM2M), был интегрирован с решением Blockchain для обеспечения надежности и возможности аудита.

С семантической стороны, обеспечение того, чтобы разные устройства «понимали» данные друг друга, также является проблемой. Например, датчик температуры может сообщать данные в градусах Цельсия, в то время как подключенная система отопления, вентиляции и кондиционирования воздуха может ожидать данных в градусах Фаренгейта. Семантическая интероперабельность может быть решена с помощью общих моделей данных и онтологий, но достижение консенсуса по ним на разных устройствах и производителях может быть сложной задачей.

Более того, выбор технологии блокчейн также может повлиять на функциональную совместимость. Например, устройство IoT, предназначенное для работы с определенным типом блокчейна (скажем, Ethereum), может не работать с другим блокчейном (например, Hyperledger Fabric) без существенных изменений. В качестве примера использования была предложена система управления идентификацией и доступом на основе блокчейна для IoT, в частности для интеллектуальных транспортных средств, демонстрирующая два совместимых блокчейна, Ethereum и Hyperledger Indy, а также модель автономной идентификации.

Последствия проблем с функциональной совместимостью могут быть серьезными. Если устройства не могут эффективно взаимодействовать с блокчейном или друг с другом, ценность системы блокчейн-IoT может быть значительно снижена. Например, решение для цепочки поставок с поддержкой IoT было бы малополезным, если бы датчики температуры и GPS-трекеры от разных поставщиков не смогли передавать данные в один и тот же блокчейн. Технология блокчейн хорошо взаимодействует с IoT, решая ключевые проблемы, такие, как конфиденциальность, проблемы с функциональной совместимостью и безопасностью.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

Таким образом, решение проблемы функциональной совместимости является важным шагом на пути к реализации всего потенциала интеграции блокчейна и IoT. Это требует не только технических решений, но и сотрудничества между производителями устройств, разработчиками блокчейна и отраслевыми органами по стандартизации.

3.4. Потребление энергии

Интеграция блокчейна с IoT приводит к серьезному набору проблем, одной из которых является высокое энергопотребление, связанное с определенными системами блокчейна, особенно с теми, которые используют алгоритм консенсуса Proof-of-Work (PoW). Proof-of-work, широко используемая в блокчейне Биткойна, требует, чтобы узлы (также известные, как майнеры) в сети решали сложные математические задачи для добавления новых транзакций в блокчейн. Решение этих задач требует значительных вычислительных мощностей и, следовательно, повышенного расхода электричества. Хотя эта функция хорошо зарекомендовала себя в обеспечении безопасности сети, она также вызвала критику из-за значительного энергопотребления. Было подсчитано, что майнинг биткойнов потребляет больше электроэнергии в год, чем некоторые страны. Этот вопрос становится особенно важным при рассмотрении контекста IoT. Устройства IoT обычно спроектированы так, чтобы быть энергоэффективными из-за их часто ограниченной мощности. Они могут работать от батарей или питаться от возобновляемых источников энергии, таких, как солнечные батареи в отдаленных местах, и, таким образом, не подходят для процессов, потребляющих большого количества энергии. Таким образом, использование блокчейна на основе PoW в сети IoT может быстро истощать энергетические ресурсы устройств или увеличивать потребление энергии сетью до неустойчивого уровня [10]. По мере того, как общества во всем мире

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

прилагают согласованные усилия по сокращению углеродного следа и переходу к более устойчивым практикам, энергоемкий характер блокчейнов PoW все чаще рассматривается как серьезный недостаток. Чтобы смягчить эту проблему, изучаются альтернативы PoW. Механизмы консенсуса, такие как proof-of-stake (PoS), proof-of-authority (PoA) или proof-of-elapsed-time (PoET), менее энергоемкие и могут быть более подходящими для сетей IoT. Эти альтернативные протоколы обеспечивают функции безопасности и неизменности блокчейна, будучи при этом более энергоэффективными, чем системы PoW. Кроме того, такие решения, как транзакции вне сети, когда несколько транзакций объединяются вместе перед добавлением в блокчейн, также могут снизить энергопотребление операций блокчейна. Тем не менее, каждая альтернатива имеет свой собственный набор компромиссов, которые необходимо тщательно рассмотреть.

В заключение отметим, что, хотя потребление энергии является серьезной проблемой при интеграции блокчейна и IoT, инновационные решения и альтернативные механизмы консенсуса предлагают многообещающие способы решения этой проблемы. Технология блокчейн, как распределенная и неизменная бухгалтерская книга, защищенная надежными алгоритмами криптографии, открывает новые перспективы для защиты систем IoT. Многие исследования были посвящены интеграции блокчейна в управление устройствами IoT, контроль доступа, целостность данных, безопасность и конфиденциальность. Потенциал блокчейна в децентрализации и обеспечении безопасности коммуникаций IoT виден в инновационной сервисной платформе IoT, основанной на технологии блокчейна консорциума, предложенной в статье Чжана, Сюй и Се. Эта платформа абстрагирует межмашинные (M2M) и человеко-машинные (H2M) коммуникации в сервисы, предоставляемые устройствами IoT, и материализует обмен данными сети IoT с помощью смарт-контрактов и

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

транзакций блокчейна [8].

4. Заключение

Отметим, что интеграция блокчейна с IoT представляет собой важный рубеж для технологического прогресса, способный произвести революцию в отраслях, обеспечив беспрецедентный уровень безопасности, конфиденциальности, эффективности и автоматизации. Однако важно признать, что процесс интеграции этих двух мощных технологий не лишен проблем.

Будущее IoT и интеграции блокчейна связано со многими возможностями. По мере развития технологий и углубления нашего понимания этих двух областей можно ожидать появления еще более инновационных подходов и решений. Что остается постоянным, так это потребность в постоянных исследованиях, экспериментах и сотрудничестве для реализации всего потенциала интеграции блокчейна и IoT.

По мере того, как движемся вперед, важно помнить, что, хотя технологии могут предоставить мощные инструменты, именно то, как используем эти инструменты, в конечном итоге определит их ценность. При тщательном рассмотрении, продуманном дизайне и глубоком понимании связанных с этих сложностей, интеграция блокчейна и IoT может быть использована для создания решений, которые не только технологически продвинуты, но и реагируют на реальные потребности и проблемы нашего взаимосвязанного мира.

Литература

1. Androulaki E. et al. Hyperledger fabric: a distributed operating system for permissioned blockchains //Proceedings of the thirteenth EuroSys conference. – 2018. URL: doi.org/10.1145/3190508.3190538
2. Пахаев Х. Х., Айгумов Т. Г., Абдулмукминова Ф. М. Роль технологии

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

блокчейн в реализации кибербезопасности // Инженерный вестник Дона. – 2022. №. 10. URL: ivdon.ru/ru/magazine/archive/n10y2022/7958

3. Менциев А. У., Айгумов Т. Г., Эмирова Г. А. Анализ характеристик и функциональных возможностей устройств IoT // Инженерный вестник Дона. 2023. №. 2. URL: ivdon.ru/ru/magazine/archive/n2y2023/8191
4. Atzori L., Iera A., Morabito G. The internet of things: A survey //Computer networks. – 2010. T. 54. №. 15. URL: doi.org/10.1016/j.comnet.2010.05.010
5. Moudoud H., Cherkaoui S., Khoukhi L. Towards a scalable and trustworthy blockchain: Iot use case //ICC 2021-IEEE International Conference on Communications. IEEE, 2021. URL: doi.org/10.1109/ICC42927.2021.9500535
6. Saberi S. et al. Blockchain technology and its relationships to sustainable supply chain management //International journal of production research. 2019. T. 57. №. 7. URL: doi.org/10.1080/00207543.2018.1533261
7. Zhang R., Xiu K., and Se M. (2022): "Secure Decentralized Service Platform for IoT Using Consortium Blockchain." Available at arxiv.org/abs/2209.12145v1 URL: doi.org/10.3390/s22218186
8. Panarello A. et al. Blockchain and iot integration: A systematic survey //Sensors. 2018. T. 18. №. 8. URL: doi.org/10.3390/s18082575
9. Gurnani B., Kaur K., Morya A. K. Adoption, implementation, definitions, and future of blockchain technology in ophthalmology //Indian Journal of Ophthalmology. 2023. T. 71. №. 3. URL: doi.org/10.4103%2Fijo.IJO_1802_22
10. Khan M. A., Salah K. IoT security: Review, blockchain solutions, and open challenges //Future generation computer systems. 2018. T. 82. .URL: doi.org/10.1016/j.future.2017.11.022

References

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

1. Androulaki E. et al. Proceedings of the thirteenth EuroSys conference. 2018. URL : doi.org/10.1145/3190508.3190538
2. Khapaev H. H., Aigumov T. G., Abdulmukminova F. M. Inzhenernyj vestnik Dona. 2022. №. 10. URL: ivdon.ru/ru/magazine/archive/n10y2022/7958
3. Menziev A. U., Aigumov T. G., Emirova G. A. Inzhenernyj vestnik Dona. 2023. №. 2. URL: ivdon.ru/ru/magazine/archive/n2y2023/8191
4. Atzori L., Iera A., Morabito G. Computer networks. 2010. №.15. URL: doi.org/10.1016/j.comnet.2010.05.010
5. Moudoud H., Cherkaoui S., Khoukhi L. IEEE International Conference on Communications. IEEE2021. URL: doi.org/10.1109/ICC42927.2021.9500535
6. Saberi S. et al. International journal of production research. 2019. №. 7. URL: doi.org/10.1080/00207543.2018.1533261
7. Zhang R., Xu C., Xie M. Sensors. 2022. №. 21. URL: doi.org/10.3390/s22218186
8. Panarello A. et al.Sensors. 2018. №. 8. URL: doi.org/10.3390/s18082575
9. Gurnani B., Kaur K., Morya A. K. Indian Journal of Ophthalmology. 2023. №.3. URL: doi.org/10.4103%2Fijo.IJO_1802_22
10. Khan M. A., Salah K. Future generation computer systems. 2018. T. 82. URL: doi.org/10.1016/j.future.2017.11.022

Дата поступления: 24.10.2023

Дата публикации : 10.02.2024

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024