Электронный научный журнал «Век качества» ISSN 2500-1841 https://www.agequal.ru

2025, №2 https://www.agequal.ru/pdf/2025/AGE_QUALITY_2_2025.pdf

Ссылка для цитирования этой статьи:

Слядников П. Е., Тутова Н.В., Ерохин А. Г. Анализ проблем и перспектив интеграции блокчейна в системы Интернета вещей // Электронный научный журнал «Век качества». 2025. №2. С. 313-328. Режим доступа: https://www.agequal.ru/pdf/2025/225015.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

УДК 004.7

Анализ проблем и перспектив интеграции блокчейна в системы Интернета вещей

Слядников Павел Евгеньевич,
аспирант,
Московский технический университет связи и информатики,
111024, Россия, Москва, ул. Авиамоторная, 8А
p.e.slyadnikov@mtuci.ru

Тутова Наталья Владимировна,
заведующий кафедрой «Бизнес-информатика»,
кандидат технических наук, доцент,
Московский технический университет связи и информатики,
111024, Россия, Москва, ул. Авиамоторная, 8А
n.v.tutova@mtuci.ru

Ерохин Андрей Густавович,
доцент, кандидат технических наук, доцент,
Московский технический университет связи и информатики,
111024, Россия, Москва, ул. Авиамоторная, 8А
a.g.erokhin@mtuci.ru

Современные системы Интернета вещей представляют собой масштабные распределённые структуры, с огромным количеством взаимосвязанных устройств, между которыми идет систематический обмен данными. Область применения таких сетей постоянно расширяется: от управления инфраструктурой умных городов до промышленного Интернета вещей и современной телемедицины.

Однако, по мере увеличения количества подключённых устройств и объёмов передаваемой информации, приобретают всё большую выраженность фундаментальные ограничения традиционных централизованных решений. Существующие архитектуры демонстрируют ряд существенных недостатков: уязвимость к кибератакам, недостаточную пропускную способность центральных узлов, отсутствие механизмов для обеспечения прозрачности и отслеживаемости операций. Кроме того, сети Интернета должны обладать высокой отказоустойчивостью, а информация должна в них обрабатываться в режиме

реального времени. Эти проблемы ограничивают потенциал Интернета вещей и создают серьёзные риски при внедрении в критически важные инфраструктуры.

Блокчейн-технологии, предлагаемые для интеграции в сети Интернета вещей, обладают полезными свойствами, которые могут значительно улучшить работу таких сетей. Децентрализованность блокчейна, невозможность несанкционированного изменения информации и надежная криптографическая защита позволят предложить подходящую основу для построения безопасных и более прозрачных систем обмена данными.

В статье рассмотрены распространенные архитектуры сетей Интернета вещей и отмечены их особенности, проанализированы проблемы и перспективы использования блокчейна для хранения данных систем Интернета вещей, сделан вывод о целесообразности его применения. Рассмотрены основные методы моделирования для оценки вероятностно-временных характеристик блокчейн-систем в интеграции с сетями Интернета вещей.

Ключевые слова: блокчейн; Интернет вещей; безопасность; масштабируемость; децентрализация; моделирование.

Введение

Интернет вещей (IoT) представляют собой системы взаимосвязанных устройств и датчиков, обменивающихся данными посредством сети Интернет и локальных вычислительных сетей, целью которых является автоматизация процессов и повышение эффективности различных операций. Рост распространения IoT в настоящее время сопряжен с серьёзными рисками, связанными с безопасностью данных и защитой конфиденциальности пользователей. Среди ключевых вызовов можно выделить: уязвимости в программном обеспечении устройств в таких сетях, недостаточность защиты данных при их передаче, опасность их копирования или подмены злоумышленниками.

Для снижения рисков таких событий потребуется комплексный подход, предполагающий повышение безопасности устройств, в том числе с помощью криптографических методов защиты и настройки строгих политик конфиденциальности. Одним из перспективных решений может стать интеграция технологии блокчейн в сети Интернета вещей, которая обеспечит защиту данных за счёт децентрализации, криптографической устойчивости и неизменяемости хранящейся информации. Анализ предметной области демонстрируют интерес к

применению блокчейна в IoT-сетях и то, что его применение способно существенно повысить уровень безопасности и гарантировать сохранность пользовательских данных [1, 2, 3].

При этом внедрение блокчейна в сетях Интернета вещей сталкивается с существенными техническими барьерами: большинство вычислительных устройств в таких сетях обладают ограниченной производительностью, в то время как сами сети генерируют значительные объемы данных для передачи, требующие мгновенной обработки. Кроме того, для многих IoT-приложений задержки при передаче данных критически важны. Эти проблемы требуют создания адаптированных архитектур и новых подходов, которые смогут предложить преимущества блокчейна для работы в сетях Интернета вещей с учетом их особенностей и ограничений.

Типовые архитектуры Интернета вещей и их особенности

Современные системы Интернета вещей строятся на основе нескольких распространённых архитектурных моделей, каждая из которых имеет свои преимущества и недостатки. Принято выделять централизованные, децентрализованные и гибридные подходы к построению таких сетей [4, 5, 6].

1. *Централизованная архитектура*

Особенностью такой архитектуры является то, что все данные с устройств передаются на центральный сервер (в облако или дата-центр), где происходит их обработка, хранение и управление. К примерам реализации такой архитектуры можно отнести сервисы умных домов Google Home, Amazon Alexa и некоторые из простых систем промышленного Интернета вещей. При всей своей простоте развертывания и удобстве управления они обладают существенными недостатками: единой точкой отказа, уязвимостью центрального узла к DoS-атакам (англ. denial-of-service attack – «отказ в обслуживании») и задержками при передаче данных. Конфиденциальность данных потребителей в этом случае определяется надежностью и безопасностью центрального сервера.

2. *Децентрализованная (распределённая) архитектура*

В ней поступающие данные обрабатываются на нескольких узлах (например, шлюзах или нескольких отдельных серверах), что снижает общую нагрузку. На основе такой архитектуры построено большинство существующих систем промышленного Интернета вещей и проекты умных городов [7]. Применение подобных систем обеспечивает повышенную отказоустойчивость, по сравнению с централизованными вариантами, и уменьшает задержки при передаче и обработке информации. К недостаткам такой архитектуры можно отнести сложности, связанные с синхронизацией данных в сети, риски несогласованности версий и возможности манипуляций, например, если такая сеть управляется одной организацией.

3. *Гибридная архитектура граничных/туманных вычислений (Fog/Edge Computing)*

Такая архитектура предполагает комбинацию облачных и локальных вычислений. Данные частично обрабатываются на граничных устройствах (edge) или промежуточных туманных узлах (fog), а критически важная информация отправляется в облако. К примерам таких систем можно отнести современные автономные автомобили с возможностью обработки данных на борту и анализом данных в облаке, различные телемедицинские системы с локальной обработкой данных датчиков и облачным безопасным хранением важной информации.

Использование граничных и туманных вычислений позволяет снизить нагрузку на общие ресурсы, перенося вычисления ближе к конечным пользовательским устройствам, при этом задержки обработки минимизируются. Среди недостатков такого подхода следует отметить сложность согласования работы граничных и туманных вычислений и облачной инфраструктуры, ограниченность производительности граничных устройств и риски потери данных на различных уровнях обработки и при передаче.

4. Одноранговая (Peer-to-Peer – P2P) архитектура

Устройства взаимодействуют напрямую без центрального сервера, образуя одноранговую сеть. Примерами реализации такой архитектуры являются Mesh-сети (Helium IoT) и децентрализованные системы умного дома. Mesh-сеть – это распределенная, одноранговая, ячеистая сеть. Каждый узел в ней обладает такими же полномочиями, как и все остальные.

К преимуществам таких сетей относят высочайшую отказоустойчивость и отсутствие уязвимости в виде единой точки атаки. С другой стороны, при росте числа устройств такая сеть может становиться медленнее, что ведет к сложностям при масштабировании и проблемам с безопасностью на отдельных устройствах. Также каждое устройство в таких сетях участвует в маршрутизации, что влечет повышенные требования к производительности.

5. Блокчейн-ориентированная архитектура

В этой современной архитектуре данные записываются в распределённый реестр, а управление устройствами происходит через смарт-контракты. Примерами реализации стали сети IOTA (для IoT-устройств) и VeChain (для управления логистикой и цепочками поставок) [8]. Как и в P2P-архитектуре к ее преимуществам относятся повышенная безопасность и отсутствие единого управляющего центра. При этом недостатками такой реализации являются: относительно медленная скорость работы, так как транзакции данных в IoT происходят регулярно и в больших объемах, повышенное энергопотребление (в случае использования алгоритма консенсуса Proof of Work), а так же сложность интеграции, потому что не все устройства Интернета вещей поддерживают криптографические операции.

У каждой из представленных выше архитектур Интернета вещей имеются свои сильные и слабые стороны, но наиболее перспективными в будущих сетях Интернета вещей являются гибридные модели с элементами блокчейна и граничных и туманных вычислений, которые смогут обеспечивать как повышенную безопасность, так и производительность [9, 10, 11].

Технология блокчейна

Рассмотрим классическую технологию устройства сети блокчейн. Она представляет собой распределенную децентрализованную систему, функционирующую на основе алгоритма консенсуса Proof-of-Work (PoW), который является наиболее распространенным и популярным алгоритмом консенсуса [12, 13]. Данная архитектура обеспечивает создание неизменяемой цепочки блоков, содержащих информацию о транзакциях, где каждый участник сети обладает полной копией реестра [14].

Процесс обработки транзакций начинается с их создания и подписания отправителем с использованием криптографических ключей. Сформированные транзакции проходят первоначальную валидацию, в ходе которой проверяется их корректность, наличие достаточного баланса и соответствие установленным протоколом требованиям. Неподтвержденные транзакции временно сохраняются в мемпуле – специальном буфере ожидания, где они находятся до включения в блок.

Пользователи сети, обычно называемые майнерами, выполняющие ключевую роль в поддержании работы сети, осуществляют сбор транзакций из мемпула и их компоновку в блоки-кандидаты. Для обеспечения целостности данных применяется древовидная хеш-структура Меркла. Основной вычислительный процесс заключается в решении криптографической задачи PoW, требующей нахождения значения nonce, удовлетворяющего заданным условиям сложности. Данный процесс характеризуется высокой ресурсоемкостью и носит вероятностный характер.

Успешное нахождение корректного nonce приводит к созданию нового блока, который затем распространяется по сети для верификации другими узлами. Проверка включает анализ связности с предыдущим блоком, валидацию транзакций и подтверждение соответствия всех параметров установленным протоколом требованиям. После успешной верификации блок добавляется в цепочку, а майнер получает предусмотренное вознаграждение.

Структурно каждый блок содержит заголовок с метаданными (включая хеш-ссылки на предыдущий блок) и список транзакций. Криптографическая связность блоков обеспечивает устойчивость системы к модификации данных, то есть попытка изменения информации в каком-либо блоке потребует пересчета всех последующих блоков, что делает подобные действия вычислительно нецелесообразными.

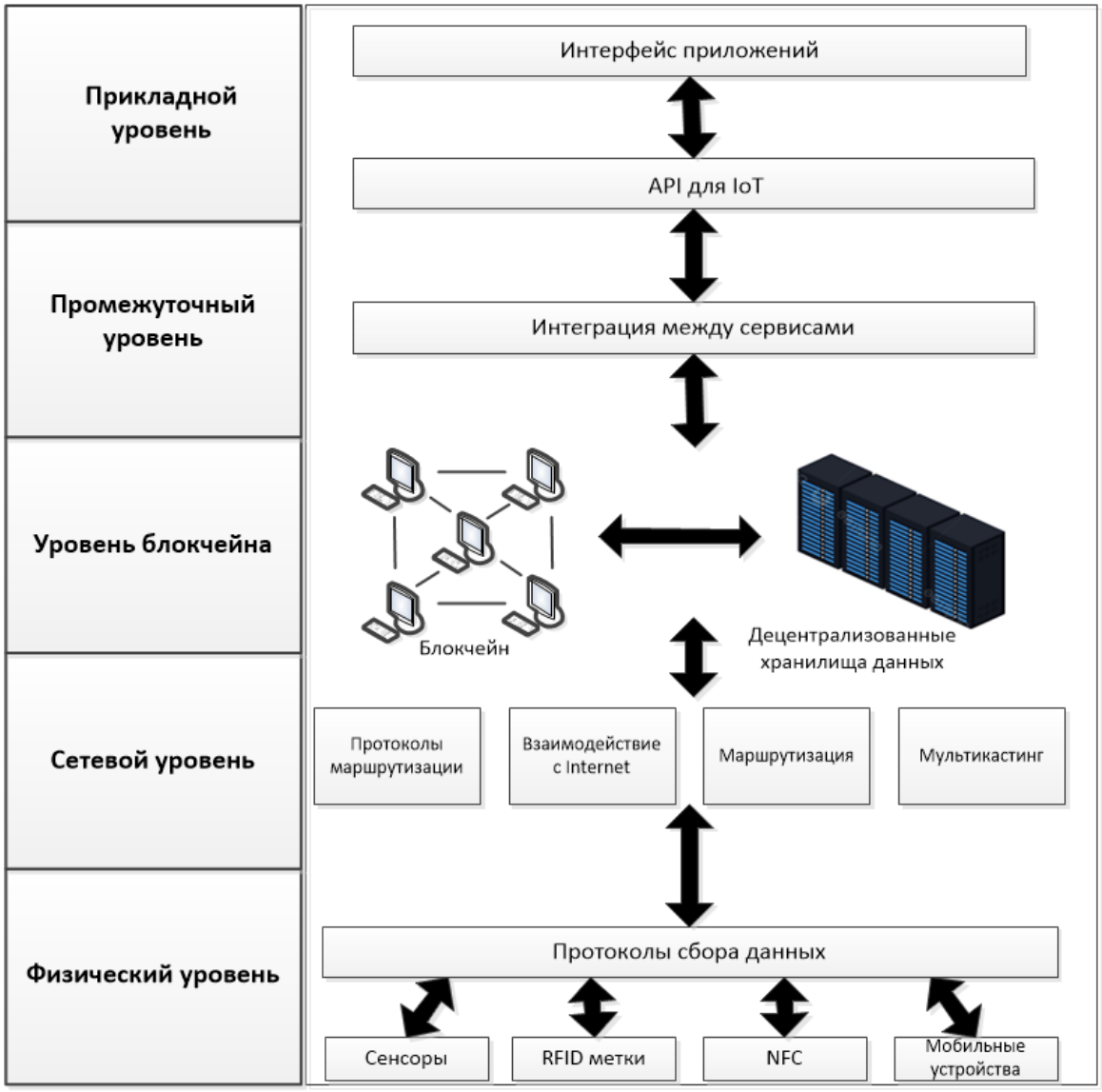
Примером реализации такой сети является сеть Bitcoin, которая предусматривает формирование нового блока приблизительно каждые 10 минут при ограничении размера блока 1 МБ. По состоянию на 2025 г. общий объем блокчейна составляет около 630 ГБ. Транзакция считается окончательно подтвержденной после включения в блок и получения нескольких последующих подтверждений, что гарантирует ее необратимость и достоверность.

Пакетная обработка транзакций и периодическое создание блоков обусловлены как вычислительной сложностью процесса майнинга, так и необходимостью обеспечения надежной синхронизации данных в распределенной сети. В среднем каждый блок содержит от 1000 до 2500 транзакций, что определяет пропускную способность системы и влияет на время обработки операций.

Архитектура Интернета вещей с использованием блокчейна

Пятиуровневая архитектура сети IoT с применением технологии блокчейн представлена на рис. 1.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru



Источник: составлено авторами на основе данных [15]

Рис. 1. Архитектура сети Интернета вещей с применением блокчейн

Данная архитектура сочетает в себе особенности традиционных IoT-систем и блокчейн.

На Физическом уровне представлены различные устройства, взаимодействующие с приложениями, собирающие и передающие данные (датчики, элементы умного дома, радиочастотные RFID-метки и мобильные телефоны).

На Сетевом уровне обеспечивается связь между IoT-устройствами, происходит маршрутизация и многоадресная передача информации.

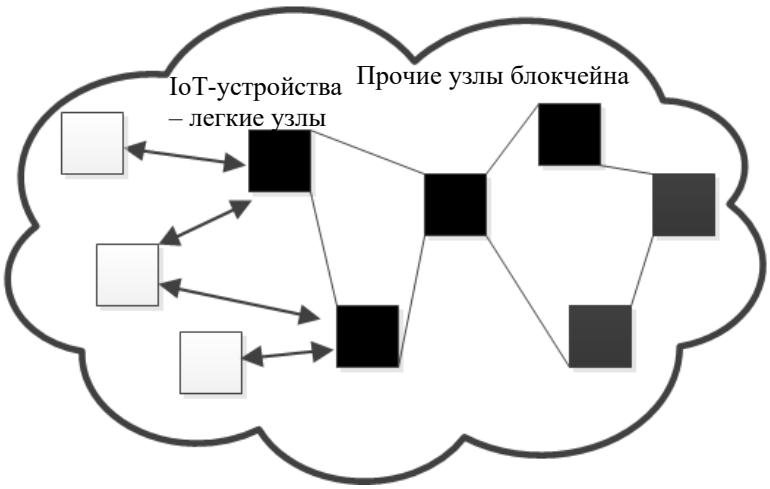
Блокчейн-уровень привносит в модель распределенную систему хранения и обработки данных, в которой используются механизмы консенсуса для безопасности и неизменности транзакций. При создании сети Интернета вещей возможен выбор между приватными или публичными блокчейн-решениями, в зависимости от поставленных перед разработчиками задач.

На Промежуточном уровне происходит интеграция сервисов, и принимаются дополнительные меры безопасности за счет дополнительных протоколов.

Наконец, на Прикладном уровне пользователи получают доступ к управлению IoT-приложениями через интерфейс прикладного программирования (API), что обеспечивает удобное взаимодействие с системой.

Блокчейн же в данной архитектуре выступает в качестве надежной распределенной базы данных, гарантирующей целостность и защиту данных от несанкционированных изменений – после подтверждения и добавления блока все содержащиеся в нем транзакции, а также предыдущие записи, становятся необратимыми и защищенными от злоупотреблений. Кроме того, все совершенные записи могут быть легко извлечены без потери информации. Авторизованный пользователь может просматривать все транзакции и проверять подлинность каждой из них.

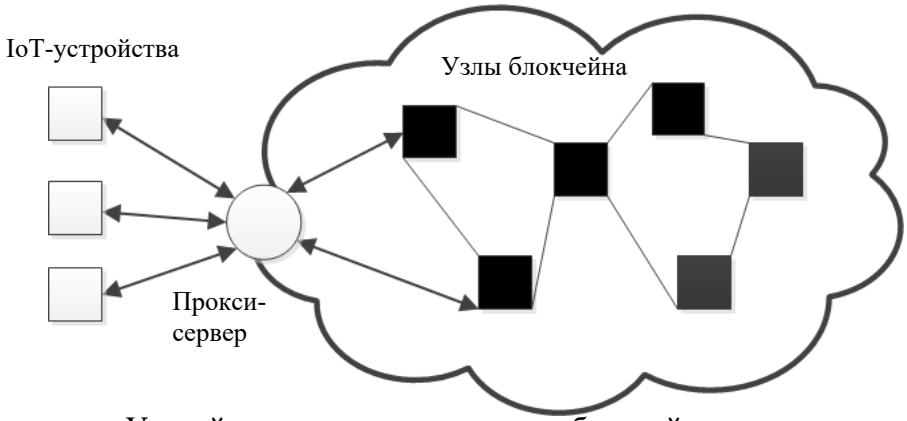
IoT-устройства могут являться как самостоятельными узлами в блокчейн-сети, так и осуществлять взаимодействие через прокси-сервер, выступающий в роли узла блокчейна. Данные варианты взаимодействия представлены на рис. 2 и 3 соответственно. В первой ситуации такие узлы из-за ограниченности ресурсов будут так называемыми «легкими» узлами, которые не участвуют в генерации блоков и хранят данные только о последнем блоке.



Устройства являются частью блокчейн-сети

Источник: составлено авторами на основе данных [15]

Рис. 2. IoT устройства, являющиеся узлами сети блокчейн



Устройства не являются частью блокчейн-сети,
прокси-сервер – узел блокчейна

Источник: составлено авторами на основе данных [15]

Рис. 3. Доступ к блокчейн сети через прокси-сервер

В случае если IoT-устройства не подключены напрямую к блокчейн-сети, а взаимодействуют с ней через прокси-сервер, это позволяет повысить эффективность передачи данных. Прокси-сервер кэширует информацию, ускоряя обработку транзакций и предотвращая перегрузку сети.

В отличие от архитектуры, где IoT-устройства напрямую участвуют в блокчейн-консенсусе, такой подход дает возможность использовать преимущества

распределенного реестра без необходимости поддерживать полноценные узлы, что снижает затраты на вычислительные ресурсы и упрощает развертывание системы.

Основные методы моделирования в сетях блокчейна

Развертывание приложений IoT на блокчейн-системах остается сложной задачей в связи с ограниченным хранилищем и вычислительными возможностями устройств IoT, их огромным разнообразием и количеством. Для успешной реализации оптимизированных и производительных систем необходимо предварительно производить их моделирование. Наибольшее распространение в настоящее время получили аналитические, дискретно-событийные и агентные методы моделирования блокчейна.

Аналитические методы, основанные на математическом аппарате теории массового обслуживания, вероятностных моделях и теории игр, позволяют оперативно оценивать базовые параметры сети, такие как пропускная способность и надежность алгоритма консенсуса, однако упрощают реальные условия функционирования системы. С помощью математического аппарата, применяемого в данном методе, делается оценка ключевых параметров блокчейна. Например, теория очередей используется для анализа задержек обработки транзакций, вероятностные модели, в свою очередь, для оценки надежности консенсусных алгоритмов (PoW/PoS), а теория игр применяется для изучения мотивации участников – пользователей сети.

Во многих работах для моделирования потоков в блокчейн используются модели однорангового трафика [16], в которых для расчета вероятности доступа к ресурсу используется распределение Мандельброта-Ципфа. Распределение показывает, что вероятность $p(i)$ доступа пользователя к ресурсу i, отсортированном в порядке убывания популярности из N доступных ресурсов, равна

$$p(i) = \frac{K}{(1+q)^{\alpha}}, \quad (1)$$

где $K = 1/(\sum_{i=1}^{N} 1/(i+q)^{\alpha})$ с фактором плато q, определяющим степень сглаживания пика распределения, и фактором асимметрии α.

Для генерации блока в алгоритме консенсуса PoW используется распределение Пуассона [14, 15]. Вероятность генерации N блоков за время t с интенсивностью λ имеет следующий вид:

$$P = \int_0^{\infty} \frac{(\lambda t)^N}{N!} e^{-\lambda t} dt. \quad (2)$$

Средствами *дискретно-событийного имитационного моделирования* может достигаться более детализированное исследование временных характеристик, где функционирование сети блокчейн представляется в качестве последовательности синхронизированных по времени событий генерации, распространения и валидации блоков. Для генерации событий используются формулы 1 и 2.

Среди методов моделирования наиболее детализованным является *агентное моделирование*, которое рассматривает каждого участника сети – пользователя как автономный субъект с индивидуальным поведением. Его главное преимущество – возможность выявления эмерджентных свойств сети, неочевидных при других подходах [17].

Выбор конкретного метода моделирования зависит от потребностей при построении моделей и целей исследования.

Заключение

Интеграция блокчейн-технологий в системы Интернета вещей в настоящее время является перспективным направлением, предлагающим решение актуальных проблем IoT. Несмотря на существующие технические барьеры, сочетание этих двух инновационных направлений способно создать устойчивую основу для следующего поколения распределенных систем.

Архитектура сети Интернета вещей с применением блокчейна решает некоторые из проблем безопасности и масштабируемости традиционных сетей IoT, но в связи с недостатком ресурсов устройств IoT и большой их численностью имеет ограничения.

Наиболее вероятным путем развития представляется создание гибридных архитектур, сочетающих преимущества распределенных реестров с граничными вычислениями и оптимизированными протоколами консенсуса. При разработке таких решений должны обязательно учитываться существующие ограничения IoT-устройств. Для этого целесообразно разработать новые модели и методы для проектирования и оптимизации таких систем.

Список литературы

1. Ал-Хуссеини, М. Обзор интеграции блокчейна и Интернета вещей: исследование текущих проблем / М. Ал-Хуссеини // Инженерный вестник Дона. – 2024. – № 2(110). – С. 9-24.
2. Вишняков, В.А. Использование блокчейна Ethereum в сети интернета вещей для IT-диагностики / В.А. Вишняков, И. Ся, Ч. Юй // Цифровая трансформация. – 2024. – Т. 30. – № 3. – С. 61-68.
3. Phionah, Mukantabana & Extension, Kiu Publication. The Role of Blockchain in Securing IoT Devices // Research Output Journal of Engineering and Scientific Research. – 2024. – Vol. 3. – Issue 2. – Pp. 26-29.
4. Paolone, Gaetanino et al. Conceptualization of IoT architectures // International Journal of Informatics and Communication Technology (IJ-ICT). – 2025. – Vol. 14. – Issue 1. – Pp. 334-346.
5. Elzaghmouri, B.M. et al. A Novel Hybrid Architecture for Superior IoT Threat Detection through Real IoT Environments // Computers, Materials & Continua. – 2024. – Vol. 81. – №. 2. – Pp. 2299-2316.

6. Slyadnikov, P. et al. Modeling of Blockchain Systems in Internet of Things Networks // 2025 Systems of Signals Generating and Processing in the Field of on Board Communications. – IEEE, 2025. – Pp. 1-4.
7. Hassija, V. et al. A survey on IoT security: application areas, security threats, and solution architectures // IEEe Access. – 2019. – Vol. 7. – Pp. 82721-82743.
8. Гузаеров, В.В. Сеть IOTA как способ реализации систем распределенного реестра в умных городах / В.В. Гузаеров, К.Н. Панков, А.В. Власов // REDS: Телекоммуникационные устройства и системы. – 2023. – Т. 13. – № 3. – С. 9-13.
9. Dlimi Z., Ezzati A., Alla S. B. A Lightweight Blockchain for IoT in Smart City (IoT-Smart Chain) // Computers, Materials & Continua. – 2021. – Vol. 69. – № 2. – Pp. 2687–2703.
10. Solomon G. et al. A secure and cost-efficient blockchain facilitated IoT software update framework // IEEE Access. – 2023. – Vol. 11. – Pp. 44879-44894.
11. Potgantwar A.D., Rajawat A., Muqeem M. Unlocking the Potential of Smart Devices: The Synergy Between Blockchain and IoT using RBM. – 2023. – Vol. 1. – Issue 1. – Pp. 126-134.
12. Alam T. Blockchain and its Role in the Internet of Things (IoT) // arXiv preprint arXiv:1902.09779. – 26 Feb. 2019. – URL: https://arxiv.org/abs/1902.09779.
13. Wilhelmi F., Barrachina-Muñoz S., Dini P. End-to-end latency analysis and optimal block size of proof-of-work blockchain applications // IEEE Communications Letters. – 2022. – Vol. 26. – №. 10. – Pp. 2332-2335.
14. Спиркина, А.В. Научные аспекты структурно-параметрического моделирования блокчейн-систем / А.В. Спиркина // Труды учебных заведений связи. – 2021. – Т. 7. – № 1. – С. 122-131. – DOI 10.31854/1813-324X-2021-7-1-122-131.
15. Lao L. et al. A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling // ACM Computing Surveys (CSUR). – 2020. – Vol. 53. – №. 1. – Pp. 1-32.

16. Hefeeda M., Saleh O. Traffic modeling and proportional partial caching for peer-to-peer systems // IEEE/ACM Transactions on networking. – 2008. – Vol. 16. – № 6. – Pp. 1447-1460.
17. Rosa E., D'Angelo G., Ferretti S. Agent-based simulation of blockchains // Asian Simulation Conference. – Singapore: Springer Singapore, 2019. – Pp. 115-126.

Analysis of the problems and prospects of integrating blockchain in Internet of Things systems

Slyadnikov Pavel Evgenievich,
postgraduate student,
Moscow Technical University of Communications and Informatics,
111024, Russia, Moscow, Aviamotornaya Street, 8A,
p.e.slyadnikov@mtuci.ru

Toutova Natalia Vladimirovna,
Candidate of Technical Sciences, Associate Professor,
Moscow Technical University of Communications and Informatics,
111024, Russia, Moscow, Aviamotornaya str., 8A
n.v.tutova@mtuci.ru

Erokhin Andrey Gustavovich,
Candidate of Technical Sciences, Associate Professor,
Moscow Technical University of Communications and Informatics,
111024, Russia, Moscow, Aviamotornaya str., 8A
a.g.erokhin@mtuci.ru

Modern Internet of Things systems are large-scale distributed structures with a vast number of interconnected devices that systematically exchange data. The scope of such networks is constantly expanding – from managing smart city infrastructure to industrial IoT and modern telemedicine.

However, as the number of connected devices and the volume of transmitted data grow, the fundamental limitations of traditional centralized solutions become evident. Existing architectures exhibit several significant drawbacks: vulnerability to cyberattacks, insufficient bandwidth of central nodes, and the lack of mechanisms to ensure transparency and traceability of operations. These issues constrain the potential of the Internet of Things and create serious risks when deploying it in critical infrastructures. These challenges become especially relevant in the context of the need for real-time data processing in Internet of Things networks and the demand for high fault tolerance in such systems.

Blockchain technologies, proposed for integration into Internet of Things networks, offer capabilities that could significantly enhance their performance. Their decentralized nature, resistance to unauthorized data modification, and robust cryptographic protection provide a suitable foundation for building secure and more transparent data exchange systems.

The article considers methods of blockchain modeling for assessing the probabilistic and temporal characteristics of blockchain systems in integration with Internet of Things systems.

Keywords: blockchain; Internet of Things; security; scalability; decentralization; modeling.