МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ
имени Гумарбека Даукеева

Кафедра «Телекоммуникационные сети и системы»
Специальность: 6М071900 «Радиотехника, электроника и телекоммуникации»

ДОПУЩЕН К ЗАЩИТЕ
Зав. кафедрой
PhD, доцент Темырканова Э.К.
(ученая степень, звание, ФИО)
_____
(подпись)
«_____»_____2020 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ
пояснительная записка

на тему: «Алгоритмы децентрализованного хранения и обработки данных»

Магистрант: Нугманов Д.М. _____ группа МРЭТн 18-2
(Ф.И.О.) (подпись)

Руководитель: кт.н., проф. АУЭС _____ Лещинская Э.М
(ученая степень, звание) (подпись)

Рецензент:_____ _____ _____
(ученая степень, звание) (подпись)

Консультант по ВТ: кт.н., проф. АУЭС _____ Лещинская Э.М.
(ученая степень, звание) (подпись)

Нормоконтроль: кт.н., проф. АУЭС _____ Лещинская Э.М.
(ученая степень, звание) (подпись)

Алматы 2020

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ
имени Гумарбека Даукеева

Институт Космической Инженерии и Телекоммуникаций

Специальность: 6М071900 «Радиотехника, электроника и телекоммуникации»

Кафедра: «Телекоммуникационные сети и системы»

ЗАДАНИЕ
на выполнение магистерской диссертации

Магистранту Нугманову Дамиру Маратовичу
(фамилия, имя, отчество)

Тема диссертации «Алгоритмы децентрализованного хранения и обработки данных»

Утверждена Ученым советом университета №122 от «25» октября 2018 г.

Срок сдачи законченной диссертации «25» мая 2020 г.

Цель исследования состоит в обеспечении конфиденциальности и безопасности информации на основе применения алгоритмов распределенного хранения и обработки данных

Перечень подлежащих разработке в магистерской диссертации вопросов или краткое содержание магистерской диссертации:

1. Основные направления развития и проблемы алгоритмов децентрализованного хранения и обработки данных
2. Анализ моделей применений децентрализованного хранения и обработки данных
3. Моделирование архитектуры интеграции технологии блокчейн и IoT

Перечень графического материала (с точным указанием обязательных чертежей)

Рисунок 3.4 - Зависимость средней утилизации от размера блоков и интервала генерации в логарифмической шкале

Рисунок 3.5 - Зависимость процента устаревших блоков от размера блоков и интервала генерации в логарифмической шкале

Рисунок 3.7 - Зависимость процента устаревших блоков от сетевой задержки между узлами и интервала генерации в логарифмической шкале

Рисунок 3.10 – Зависимость процента устаревших блоков и средней утилизации от количества IoT устройств в логарифмической шкале

Рекомендуемая основная литература

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System // [bitcoin.org] - 2008. URL: https://bitcoin.org/bitcoin.pdf (дата обращения:23.05.2020).

2. Тихвинский В.О., Бочечка Г.С., Нургожин Б.И., Айтмагамбетов А.З. Сети IoT/M2M: технологии, приложения и регулирование. Изд. «АК-Шагыл».-Алматы, 2016.

Г Р А Ф И К
подготовки магистерской диссертации

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
1. Информационный обзор согласно темы	01.02.2019	
2. Основные направления развития и проблемы алгоритмов децентрализованного хранения и обработки данных	01.06.2019	
3. Анализ моделей применений децентрализованного хранения и обработки данных (исследовательская глава)	01.11.2019	
4. Моделирование архитектуры интеграции технологии блокчейн и IoT (расчетная часть)	01.03.2020	
5. Анализ полученных экспериментальных и расчетных данных	01.05.2020	

Дата выдачи задания_30 сентября 2018г._____

Заведующий кафедрой _____ (Темырканова Э.К.)
(подпись) (Ф.И.О.)

Научный
руководитель диссертации _____ (Лещинская Э.М..)
(подпись) (Ф.И.О.)

Задание принял к исполнению
магистрант _____ (Нугманов Д.М.)
(подпись) (Ф.И.О.)

Аңдатпа

Құпиялылық пен қауіпсіздікті қамтамасыз ету үшін әр түрлі салаларда деректердің таратылған сақтау алгоритмдерін пайдалануды талдау. IoT технологияларында, денсаулық сақтау және электрондық дауыс беру жүйелерінде таратылған сақтау технологияларын қолданудың жаңа әдістері қарастырылған.

IoT желісінде қауіпсіздік пен деректердің тұтастығы мәселелері қарастырылған, деректерді сақтау мен өңдеудің орталықтандырылмаған модельдерін қолдана отырып, оларды шешу әдістері ұсынылған, осы шешімдердің артықшылықтары мен кемшіліктері талданды. IoT желілерінде блокчейн интеграциясының архитектурасы ұсынылған, сонымен қатар модельдеу нәтижесінде алынған ұсыныстар берілген.

Аннотация

Выполнен анализ использования алгоритмов распределённого хранения данных в различных областях для обеспечения их конфиденциальности и безопасности. Рассмотрены методы применения технологии распределённого хранения в IoT технологиях, здравоохранении и системах электронного голосования.

Рассмотрены проблемы безопасности и целостности данных в сети IoT, предложены методы решения данных проблем с использованием децентрализованных моделей хранения и обработки данных, проанализированы преимущества и недостатки данных решений. Предложена архитектура интеграции технологии блокчейн и IoT, а также даны рекомендации, полученные в результате моделирования.

Abstract

Analysis of the use of distributed storage algorithms in various areas has been performed to ensure their confidentiality and security. New methods of using distributed storage technologies in IoT technologies, healthcare and electronic voting systems are considered.

The problems of security and data integrity in the IoT network are considered, methods for solving these problems using decentralized data storage and processing models are proposed, the advantages and disadvantages of these solutions are analyzed. The architecture of blockchain integration in IoT networks is proposed, as well as recommendations obtained as a result of modeling are given.

Содержание

Введение

По многим оценкам алгоритмы распределенного хранения и обработки данных одно из самых перспективных направлений в области технологий (вместе с машинным обучением (ML), интернетом вещей (IoT) и искусственным интеллектом (AI)), которое может иметь влияние на нашу жизнь, сопоставимое с развитием Интернета и мобильных устройств в начале 2000-х годов. По оценкам Всемирного экономического форума, к концу 2027-го года уже 10% мирового ВВП будет храниться в блокчейне.

На данный момент размер рынка распределённого хранения и обработки данных составляет около 230 млрд. долларов, большую часть, которого занимают финансовые операции.

Снижение издержек, повышение уровня безопасности и более высокая прозрачность транзакций – три главные сильные стороны блокчейна. В связи с потребностью банков, бизнеса и общества в этих трех аспектах, любая теоретическая работа или разработка в этой области становится достаточно актуальной.

Так же актуальность обоснована низкой изученностью данного научного направления в Республике Казахстан. Открыты возможности для формирования центра компетенций в области децентрализованных технологий с целью дальнейшего их применения на корпоративном рынке и государственных структурах в нашей стране.

Новизна работы состоит в поиске новых сценариев использования технологии в других отраслях с целью совершенствования систем обмена информацией, обеспечивая следующие свойства: прозрачность, необратимость, анонимность/псевдонимность, децентрализованность.

Практическая значимость работы заключается в возможности использования результатов исследования для задач, связанных с адаптацией блокчейна к IoT.

В работе исследуется технология блокчейна, анализируются проблемы на теоретического плана, возникающие в областях, в которых технология может быть применена. С использованием инструментов моделирования планируется исследование влияния интеграции блокчейна на характеристики IoT сети.

1 Анализ состояния вопроса и постановка задачи исследования

1.1 История создания и основные принципы технологии блокчейн

Блокчейн представляет собой децентрализованный реестр, который может надежно и безопасно хранить информацию, используя криптографическое шифрование и хеширование. Самая ранняя работа, в которой упоминается идея блокчейна, была опубликована Стюартом Хабером и В. Скотт Сторнеттом в 1991 году [1]. Эта работа посвящена технологии, которая, проверяет отметки времени (историю изменений) на документах. Исследователи пришли к выводу, что «в документ может быть добавлена информация об отметках времени (истории изменений) для повышения подлинности документов. Это класс документов, для которых изменения в будущем непредсказуемы. В 1992 году в концепт технологии было добавлено использование хэш деревьев, что сделало архитектуру более эффективной, позволяя собирать несколько документов в один блок, что станет особенно важным через 16 лет при создании технологий децентрализованного хранения и обработки данных.

Современный блокчейн был изобретен Сатоши Накамото в 2008 году. Целью блокчейна, по словам Накамото, было размещение публичного распределённого реестра (ledger) на блокчейне для криптовалюты Биткойн [2]. Идеей всего проекта было создание децентрализованной цифровой валюты, которая решала бы проблему двойных расходов. Двойные расходы — это недостаток технологии цифровой наличности (digital cash), при которой сторона может потратить один и тот же цифровой ресурс более одного раза, что ведет к инфляции, следовательно, для регулирования двойных расходов необходима третья сторона, в которой нет необходимости при использовании блокчейна. После запуска биткойна и технологии блокчейна, на которой он базировался, был заметен огромный рост пользователей криптовалюты в период с 2014 по 2017 год; размер блокчейна вырос с примерно 20 ГБ в 2014 году до почти 100 ГБ в 2017 году. Во время этого успеха многие компании следовали тем же принципам и выпустили на рынок приложения, использующие технологию блокчейна в самых разных областях. Блокчейн Ethereum - один из самых известных примеров. По определению CoinTelegraph, «смарт контакт» — это «специальный протокол, предназначенный для содействия, проверки или реализации переговоров либо выполнения контракта. Смарт контракты позволяют совершать доверительные транзакции без участия третьих лиц». Блокчейны даже начали использоваться для обеспечения юридических процессов при передаче недвижимости.

Известны различные определения технологии блокчейн. Дон и Алекс Тапскотт из «Blockchain Revolution» определяют блокчейн как «неподкупный цифровой реестр транзакций, который можно запрограммировать для записи не только финансовых транзакций, но и практически всего ценного» [3]. С точки зрения бизнеса блокчейн можно рассматривать как распределенный реестр, где

участники обмениваются активами, выполняя транзакции, которые хранятся в реестре. Отсутствует необходимость в центральной точке для обработки, проверки, защиты или даже хранения данных. Вместо этого данные хранятся у всех участниках сети.

Распределённый реестр (распределённый регистр, книга записей, distibuted ledger) — это синоним слова «блокчейн». Реестр хранится и обрабатывается на нескольких компьютерах или узлах, работающих независимо друг от друга. Перед тем как данные могут быть добавлены или изменены между узлами должен быть достигнут консенсус. Блокчейн не позволяет легко изменить (то есть подделать) хранящиеся данные внутри него, что делает блокчейн интересной технологией для конфиденциальных данных.

Блоки, составляющие блокчейн, содержат несколько фрагментов важной информации, а именно данные определенного типа, хэш текущего блока, хэш предыдущего блока и иногда временную метку (рис. 1.1). Данные, хранящиеся внутри блока, сильно зависят от типа блокчейна. В качестве данных могут быть любые данные - медицинские записи, налоговая информация, детали контракта и т. д.

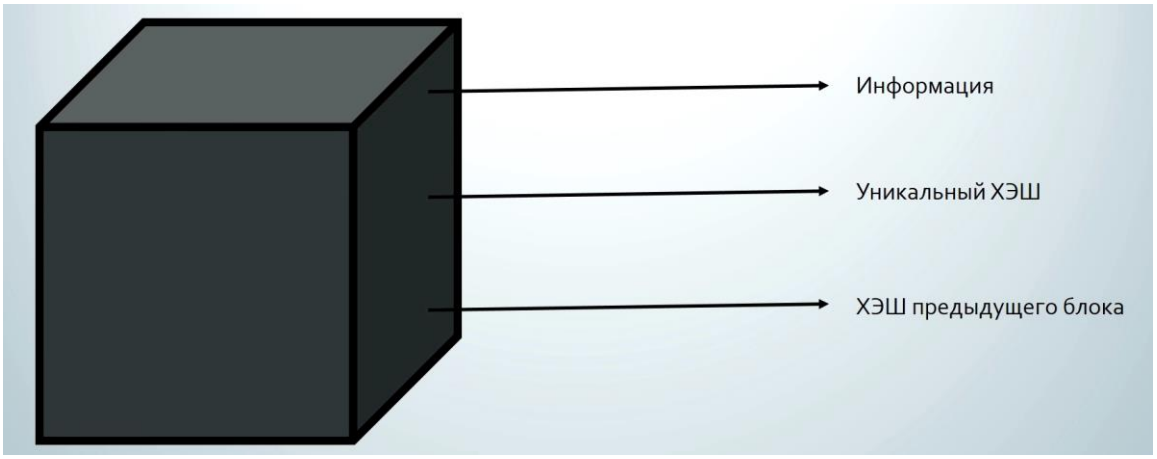

Рисунок 1.1 – Визуализация блоков в блокчейне

Хеш блока можно сравнить с цифровым отпечатком устройства (fingerprint), он всегда уникален и рассчитывается при создании блока. Если в блок будет внесено изменение после вычисления хеша, весь хеш изменится для этого блока. Это очень хороший способ обнаружить изменения в данных после того, как блок был добавлен в блокчейн, потому что, как только данные меняются, это уже другой блок данных, даже если изменить только всего один бит в данных. Такая же логика используется с хешем предыдущего блока. Все блоки в блокчейне будут содержать хэши самого блока плюс хэш его предыдущего блока. Поскольку первый блок в блокчейне не может содержать хэши из предыдущих блоков, значение обычно составляет только нули и называется блоком генезиса. Хеш блока генезиса будет, тем не менее, содержаться в следующих 15 блоках в цепочке. Этот блок, в свою очередь,

будет вычислять свой собственный хэш, который будет считан третьим блоком, чтобы определить его собственный хэш и т. д. (рис.1.2).

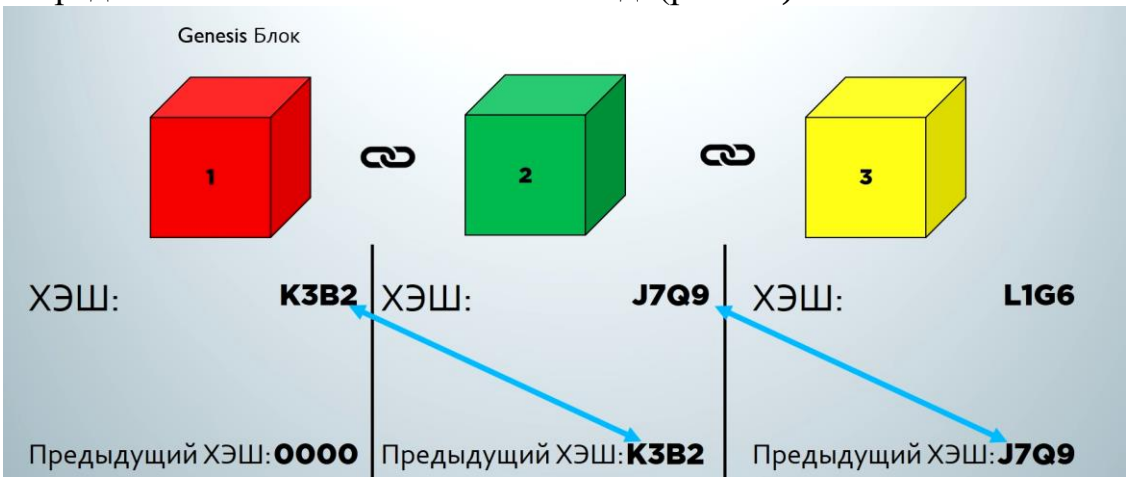

Рисунок 1.2 – Влияние хэша предыдущего блока на всю цепочку

Если хэш в блоке изменится, цепочка будет разорвана, и все последующие блоки должны будут также пересчитать свои хэши (рисунок 1.3). Поскольку заголовок каждого блока содержит часть или корень хэш-дерева (Merkle tree), изменение данных в блоке 2 сделает корень хэш-дерева в заголовке блока 3 недействительным. Если заголовок блока 3 изменится, изменится и заголовок блока 4, и так далее. Это создает цепочку блоков, основу которой составляет технология блокчейна.

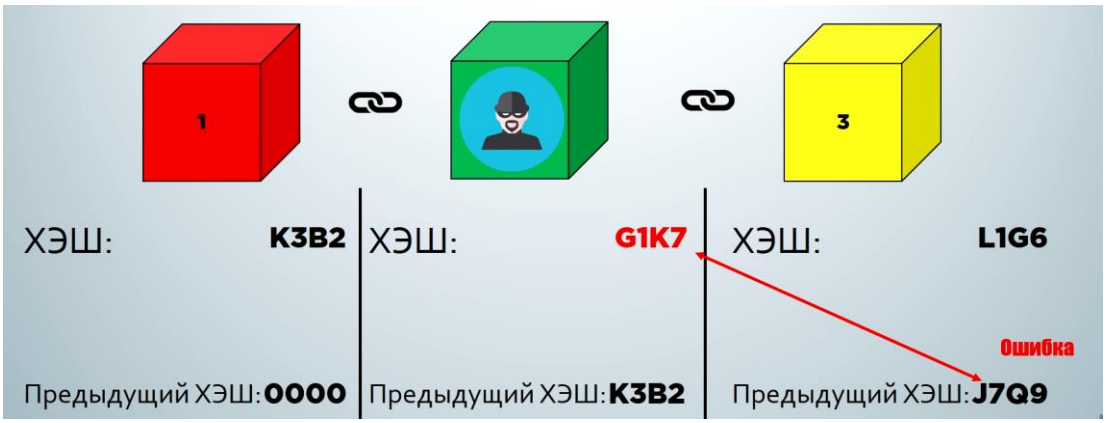

Рисунок 1.3 – Причины невалидности блоков

Каждый новый блок, содержащий транзакции, должен пройти процесс проверки для нахождения консенсуса о том, что блок является правильным блоком, а следующий блок может быть добавлен в цепочку. Этот процесс позволяет блокчейну расти (рисунок 1.4).

Блокчейн не обрабатывается из центральной точки. Вместо этого блокчейн управляется одноранговой сетью (P2P, peer-to-peer). Технология

позволяет каждому участнику обмениваться данными с кем-либо в сети, без необходимости привлечения стороннего посредника.

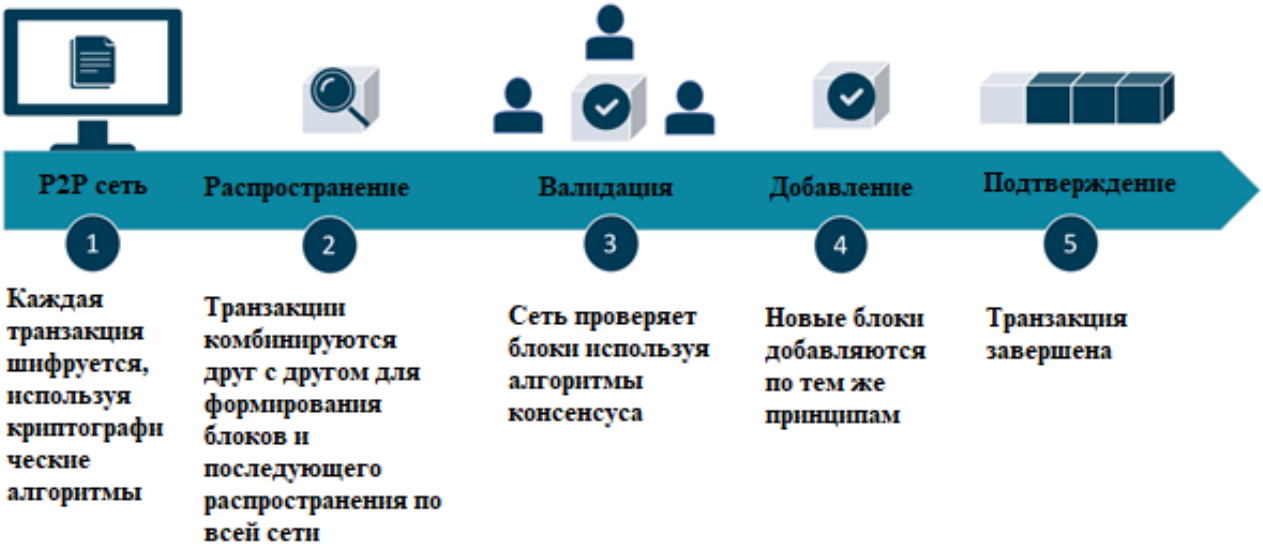

Рисунок 1.4 – Пошаговый процесс блокчейна

Существуют различные подходы, которые позволяют сети согласовывать обновление данных всего блокчейна. Внутренняя согласованность поддерживается благодаря тому, что все пользователи достигают консенсуса по текущему состоянию сети. Таким образом, разные копии одного блокчейна не существуют. Узлы проверяют транзакции, гарантируя, что это правильная информация, и затем добавляют их в блок. Затем сеть соглашается (достигает консенсуса) о том, какой блок должен быть добавлен в цепочку. Механизм консенсуса, который зависит от алгоритмического дизайна блокчейна, обеспечивает соблюдение правил. В общедоступном (инклюзивном) блокчейне (permissionless blockchain) все узлы могут предлагать дополнение к блокчейну, однако в частном (эксклюзивном) блокчейне (permissioned blockchain), только определенные узлы могут предлагать изменения. Процесс проверки позволяет осуществлять одноранговые транзакции, поскольку для проверки достоверности транзакций посредник не требуется.

Алгоритм цифрового отпечатка устройства (то есть криптографический хеш) используется для создания уникального кода, который указывает на исходный файл. Примером криптографической хеш-функции является «SHA256». Эта функция использует двоичный код и вычисляет новый хэш. Хэш состоит из 32 цифр или букв. Хеш-функция не обратима, следовательно, никто не может знать, что находится в цифровом файле, просто прочитав хеш. Каждый пользователь блокчейна имеет открытый ключ и закрытый ключ. Закрытый ключ используется для подписания транзакций, а открытый ключ используется для идентификации пользователей в системе. Открытый ключ указывает на данные пользователя, в то время как соответствующий закрытый ключ необходим для работы с этими данными. Следовательно, если пользователь контролирует как закрытый, так и открытый ключ, у него есть

подтверждение права собственности. Каждая транзакция в блокчейне подписывается цифровой подписью, для этого используется «криптография с открытым ключом». Отправитель может использовать закрытый ключ для шифрования хэша (называемого цифровой подписью), который может распространяться по всей сети. Открытый ключ отправителя может затем использоваться получателем для подтверждения того, что транзакция была подписана с помощью закрытого ключа отправителя [4].

Когда в системе имеется большое количество хэшей, может быть трудно управлять размером блокчейна. Хэш-дерево — это хеш, состоящий из нескольких хешей, структура дерева состоит из хешей, которые объединены на разных уровнях. Каждая комбинация хэшей создает новый уникальный хэш. Наконец, значение хеша, состоящее из двух последних хешей, является корнем хэш-дерева (рисунок 1.5). Чтобы убедиться, что в определённом блоке произошла определенная транзакция, достаточно использовать только заголовки блоков и корень хэш-дерева в заголовках блоков.

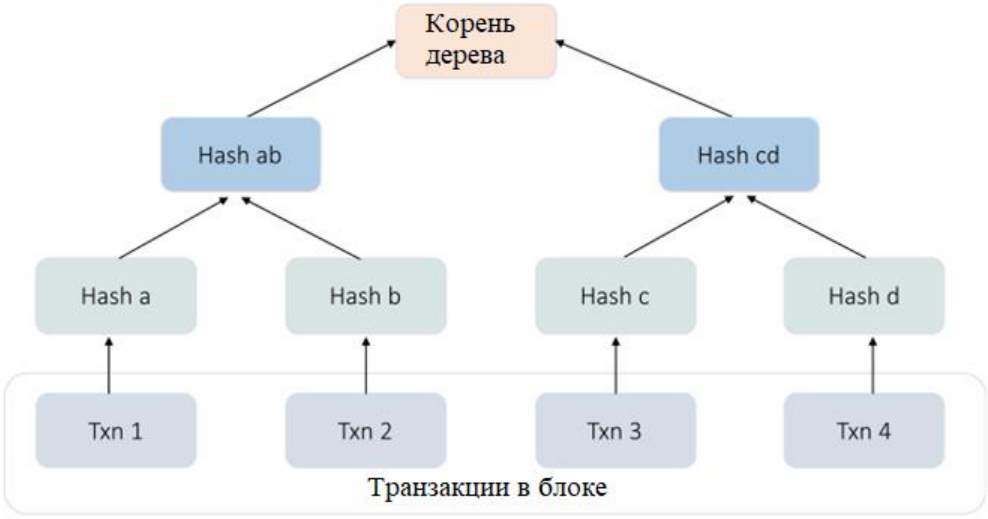

Рисунок 1.5 – Хэш-дерево

1.2 Основные преимущества и ограничения блокчейна

Блокчейн является развивающейся технологией, где все еще остается много работы для совершенствования и дальнейших исследований. Тем не менее Seebacher и его коллеги определили и проанализировали ключевые характеристики технологии блокчейна, которые отражены на рисунке 1.6 [5]. Технология блокчейна обеспечивает много преимуществ по сравнению с существующими. Две ее основные характеристики: доверие и децентрализация. Рассмотрим основные преимущества технологии распределённого хранения и обработки информации.

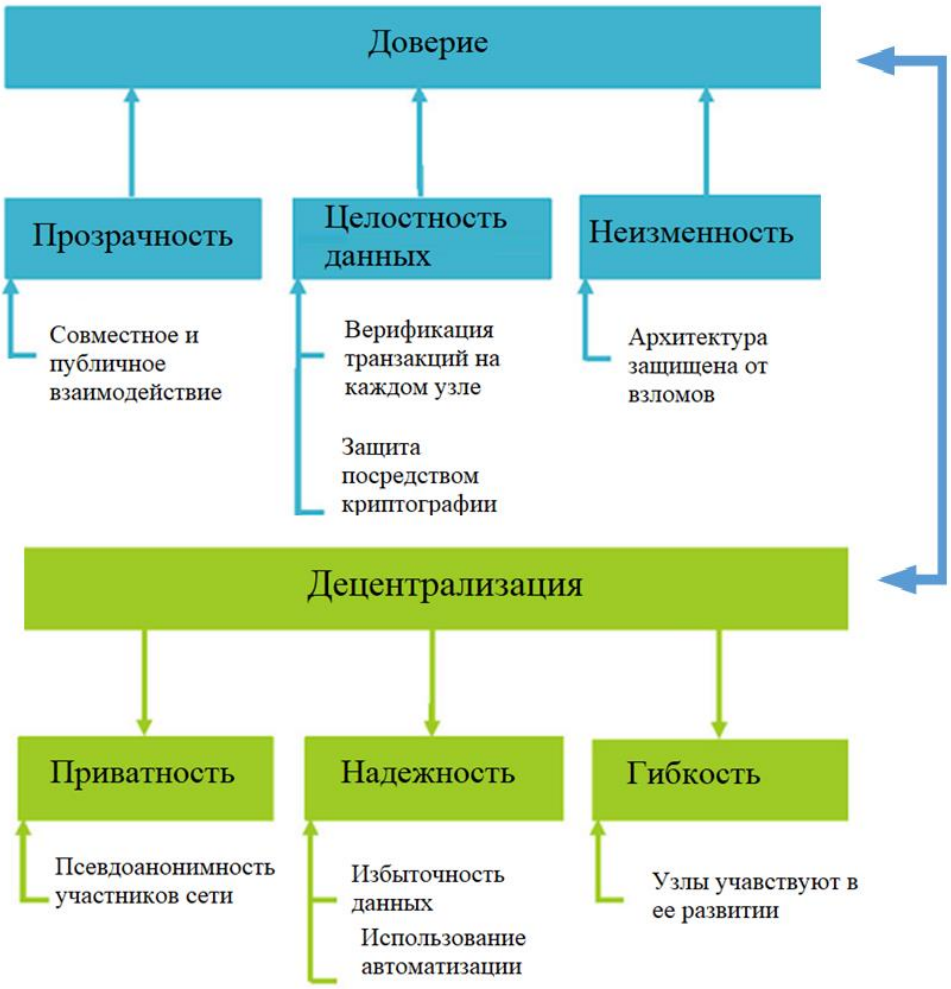

Рисунок 1.6 – Преимущества технологии блокчейн

В технологии блокчейн конфиденциальность участников — это преимущество и проблема технологии одновременно. С одной стороны, личности участников хранятся анонимно [5], что обеспечивает высокую степень конфиденциальности. Кроме того, все взаимодействия между сетевыми узлами защищены криптографией с открытым ключом. С другой стороны, стоит принимать во внимание, что в существующих системах детали транзакций хранятся и управляются третьими лицами.

Механизмы блокчейна гарантируют надежность и отказоустойчивость благодаря тому, что транзакции не добавляются в распределенный реестр, пока она не проверены и не подтверждены. После подтверждения транзакция реплицируется по сети через механизмы децентрализованного хранения блокчейна, поэтому данные становятся долговечными и устойчивыми к потере [6]. Не существует единой точки отказа или единой точки контроля над данными.

Технология блокчейна обеспечивает прозрачность для всех людей в сети, так как транзакции видимы для всех подключенных пользователей без контроля со стороны третьих лиц. Таким образом, система на основе блокчейна

предлагает улучшение в прозрачности передачи данных по сравнению с существующими централизованными системами хранения данных. Поскольку изменения видны всем в сети, и транзакции не могут быть изменены или удалены после записи в блокчейн [5].

Целостность данных достигается с помощью криптографии, которая является частью механизма консенсуса. Чтобы достичь консенсуса, сеть блокчейна использует разные механизмы. К примеру, алгоритмы доказательства работы (PoW) гарантируют, что изменение любой единицы информации в блокчейне будет означать использование огромного количества вычислительной мощности для изменений во всей сети.

Еще одним преимуществом является универсальность. Концепция блокчейн впервые возникла с применением биткойнов, однако технология применима в качестве распределённого реестра для любых типов транзакций, не только для цифровой валюты. Например, многие авторы и эксперты считают, что эта технология имеет большое влияние на энергетический сектор, поставки и логистику, музыкальную индустрию, здравоохранение и т.д.

Неизменность данных означает, что никто не может вернуться и переписать историю. Таким образом, после добавления транзакции в блок, который, в свою очередь, добавляется в блокчейн, эту транзакцию нельзя изменить. Эта степень неизменности возрастает с увеличением числа транзакций, совершаемых поверх блока, содержащего транзакцию [4].

Главное преимущество блокчейна состоит в том, что он поддерживает идею открытого, общедоступного и надежного хранилища данных. Таким образом, блокчейн предоставил первое решение проблемы установления доверия в небезопасной среде, не полагаясь на третьих лиц. Это известная проблема в распределенных вычислениях, также известная как проблема византийских генералов. Ее суть состоит в том, чтобы попытаться согласовать ход действий или состояние системы путем обмена информацией по ненадежной и потенциально скомпрометированной сети.

Характер проблем, связанных с технологией блокчейн, с технической точки зрения, будет основываться на систематическом обзоре Yli-Huumo [7]. Итоги этого анализа приведены на рисунке 1.7 в сокращенном варианте. Это исследование также выявило решения, предоставленные для каждой выявленной проблемы, и указало все еще не решенные.

Рассмотрим проблемы, связанные с безопасностью:

– атака на 51%: механизмы блокчейн разработаны с допущением, что 51% узлов контролируют сеть [7]. Если узлы злоумышленника коллективно контролируют большую вычислительную мощность, сеть уязвима для так называемой 51% атаки. Тем не менее, авторы исследований [8], показывают, что, хотя блокчейн спроектирован как полностью децентрализованная (распределенная) сеть, коэффициент децентрализации биткойнов постоянно увеличивается с 2011 года (0,26) к 2014 году (0,33). Коэффициент централизации 0 означает чисто децентрализованный, а 1 –централизованный

биткойн. Более того, есть исследования, утверждающие, что 50% контроля сети недостаточно для обеспечения безопасности [7];

– инциденты в области безопасности: С ростом использования криптовалюты, такой как Биткойн, в качестве способа осуществления платежей и переводов, инциденты в области безопасности увеличились и приводят к экономическим потерям. Используются все возможные типы взломов, включая DDoS-атаки, взлом личной учетной записи с использованием троянских программ или вирусов [7];

– проблемы гибкости данных (transaction malleability): целостность данных является существенной проблемой в среде блокчейна, поскольку данные должны отправляться всем сторонам в сети для проверки, поэтому важно не изменять их. Тем не менее, есть исследования, которые показывают, как атаки на гибкость происходят в блокчейне. При атаке на гибкость злоумышленник перехватывает, изменяет и ретранслирует транзакцию, заставляя эмитента транзакции полагать, что исходная транзакция не была подтверждена;

– проблемы аутентификации и криптографии: в блокчейне закрытый ключ является основным элементом аутентификации. Тем не менее, были некоторые инциденты с аутентификацией, такие как хорошо известный случай в Mt.Gox, когда компания была атакована, а личные ключи их клиентов были украдены [7]. Для решения этой проблемы предложены различные решения для усиления аутентификации в блокчейне.

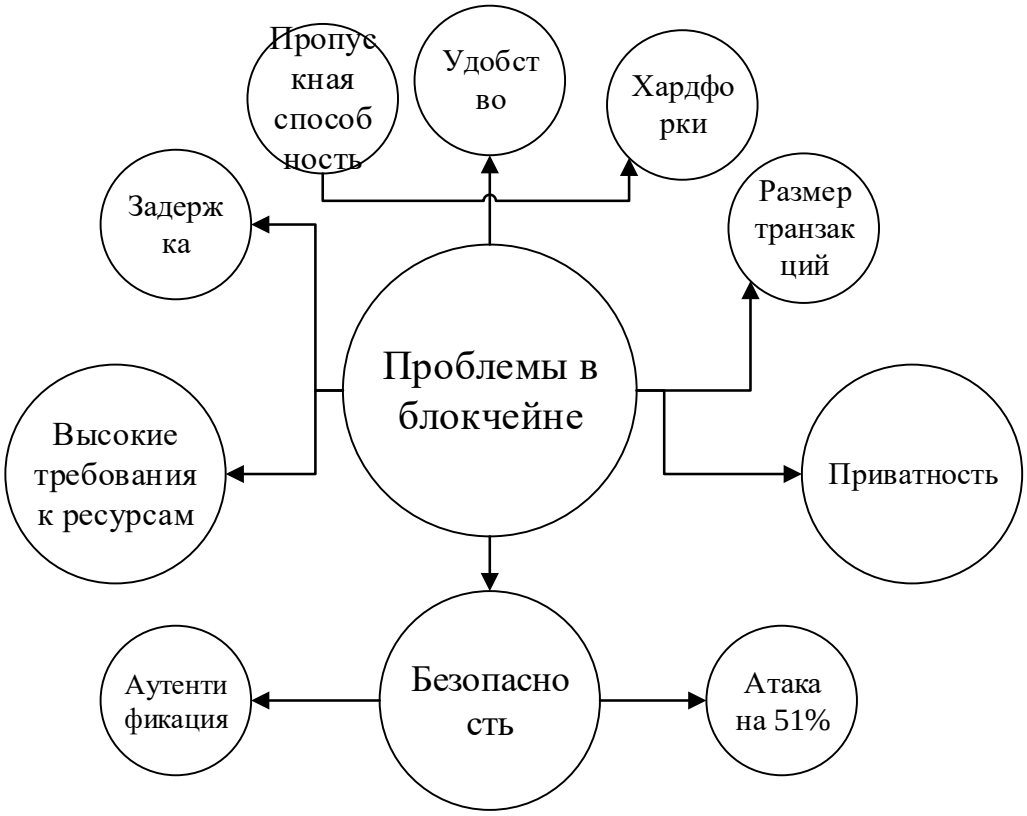

Рисунок 1.7 – Проблемы блокчейна

Майнинг – процесс записи и проверки транзакций. Это очень трудоемкий процесс, в следствии чего возникает проблема расходования ресурсов. Такое потребление энергоресурсов обусловлено усилиями в PoW. Существуют различные предлагаемые решения проблемы потребления. Однако проблема неэффективного использования ресурсов требует инновационных решений для более эффективного майнинга в блокчейне.

Как упоминалось ранее, конфиденциальность — это проблема и преимущество децентрализованного хранения, все участники могут видеть все транзакции, но без привязки транзакции к пользователю. В связи с проблемой конфиденциальности существует множество исследований, предлагающих различные типы контрмер и моделей конфиденциальности для повышения анонимности в блокчейне [7].

Блокчейн сталкивается со многими регуляторными проблемами. Например, проблема управления транснациональными сетями и обеспечения соблюдения законов, когда нет центрального посредника, который может нести юридическую ответственность [9]. Правовые вопросы могут возникать в областях юрисдикции, ответственности, интеллектуальной собственности, конфиденциальности данных, соблюдения правил регулирования финансовых услуг и управления данными. Узлы блокчейна могут быть расположены в любой точке мира. Следовательно, блокчейн может пересекать юрисдикционные границы, что требует тщательного рассмотрения договорных отношений между странами. Регулирование варьируется от страны к стране. К примеру, даже в ЕС могут быть различные правила в разных странах, особенно в энергетическом секторе. Поэтому важна координация между регулирующими органами [10]. К примеру, если срок действия контракта истекает или прекращается, возможно будет сложно гарантировать, что все данные клиента будут удалены. Однако существует несколько решений этой проблемы. Одним из решений является шифрование личной информации с использованием личного ключа. Когда личный ключ исчезает, он больше не имеет доступа к информации. Также возможно хранить только хэш транзакции в блокчейне, что позволяет стереть транзакции и оставить только след в блокчейне. Есть предположения, что блокчейн может помочь организациям достичь целей регулирования. Например, путем обеспечения большей прозрачности и упрощения нормативной отчетности [10].

В технологии блокчейн возникают такие проблемы, как стандартизация аппаратных средств, программного обеспечения и наличие квалифицированных специалистов. Масштабируемость и скорость транзакций так же является проблемой. Существует компромисс между масштабом и скоростью блокчейна. Общедоступные блокчейны часто имеют ограниченную скорость транзакций, но высокую масштабируемость, в то время как частные блокчейны могут иметь более высокую скорость транзакций, но им не хватает масштаба. Проблемы масштабируемости могут стать еще более серьезной проблемой в будущем, особенно если в сеть блокчейн будет включено большое

количество IoT-устройств. Они не могут хранить все данные из-за ограниченности ресурсов хранения и вычислительных ресурсов.

1.3 Классификация блокчейн-систем

Существуют различные типы блокчейнов, которые могут быть классифицированы по степени их открытости и децентрализации, от абсолютно общедоступных блокчейнов до полностью приватных (эксклюзивных) блокчейнов (рисунок 1.8) [9].

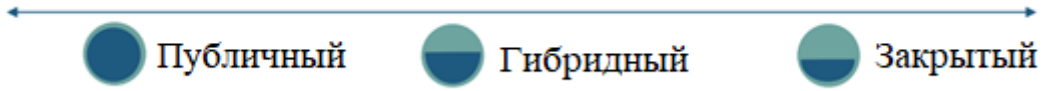

Рисунок 1.8 – Классификация блокчейн-систем

Биткойн был первым публичным блокчейном, разработанным без требований к контролю доступа [4]. Отдельные организации начали разрабатывать как частные, так и консорциумные (гибридные) блокчейны.

Различие между разными типами блокчейнов обусловлено тем, кому разрешено участвовать в сети и вносить изменения в реестр [11]. Точные характеристики зависят от базового протокола блокчейна [4]. Когда и какой тип блокчейна использовать, зависит даже от того, какие атрибуты сети являются наиболее важными [9]. В таблице 1.1 представлены сводные данные, а на рисунке 1.9 визуализация трех типов блокчейнов: частного, гибридного и публичного.

Таблица 1.1 – Сравнение разных типов блокчейн-систем

	Частный	Гибридный	Публичный
Управление	Одна организация	Несколько организаций	Сообщество
Механизм консенсуса	Алгоритм голосования Доказательство власти (Proof of Authority) Высокое доверие к валидаторам		Доказательство работы (PoW) Доказательство доли владения (PoS) Высокая анонимность валидаторов
Идентификация пользователей	Личности известны		Анонимность, псевдонимы
Токен	Токен не имеет значения		Токен для оплаты транзакций и стимулирования валидаторов

Продолжение таблицы 1.2

	Частный	Гибридный	Публичный
Преимущества	Низкое энергопотребление Быстрая масштабируемость Отсутствие юридических проблем		Неизменность данных Безопасность данных Низкие эксплуатационные расходы для пользователей
Недостатки	Более высокие затраты на разработку (для определенных приложений) Более высокие риски безопасности данных		Более низкая конфиденциальность данных Низкая скорость обработки данных и низкая масштабируемость Долгий процесс разработки
Примеры	MONAX, Multichain	Corda by R3, Energy Web Foundation, B3i	Bitcoin, Etherreum, Monero, Dash, Dodgecoin, Litecoint

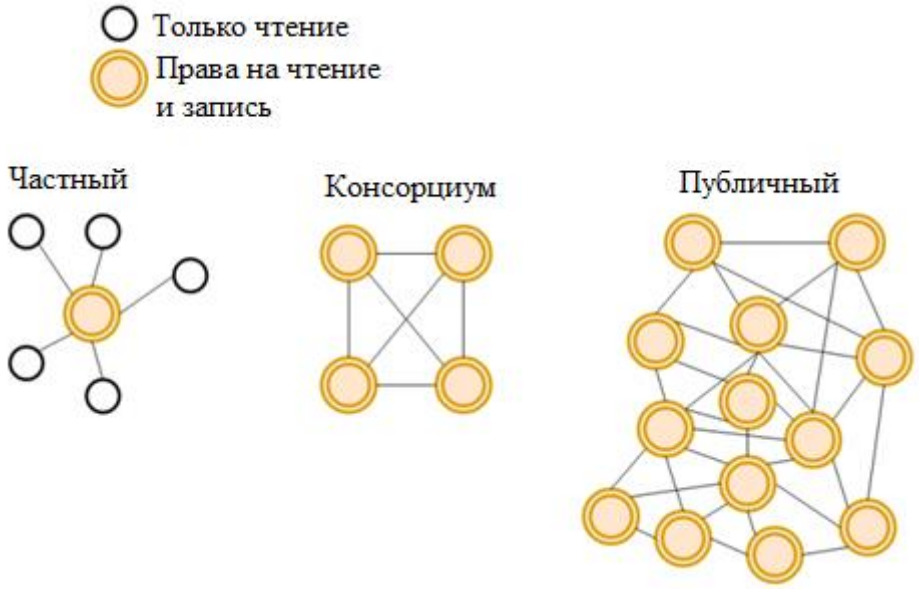

Рисунок 1.9 – Визуализация различных блокчейн-систем

Публичные блокчейны полностью открыты. Каждый может присоединиться к сети и участвовать в ней, поскольку предварительное разрешение на участие не требуется. Публичные блокчейны функционируют без центральной точки, выполняющей координирующую роль. Таким образом, отпадает необходимость сторон доверять центральной организации [4]. В

публичных блокчейнах доверие и координация создаются экономическими стимулами и публичный блокчейн не нуждается в традиционных юридических договорах. Нет ограничений на чтение или запись для публичных блокчейнов, а идентификаторы пользователей (узлов) не раскрываются, используются псевдонимы. Публичные блокчейны более безопасны, чем частные из-за того, что в них сложнее изменить информацию. Однако публичные хранилища зачастую дольше обрабатывают данные и обслуживание таких систем дороже, чем частные. Когда система общедоступна, уязвимость системы возрастает и скорость блокчейна снижается. Из-за большого количества узлов и предыдущих блоков в публичном блокчейне емкость хранилища также ограничена.

Частные блокчейны представляют собой закрытую сеть с предварительно известными участниками [12]. Владелец или администратор несет ответственность за доступ к сети и используемые алгоритмы распределённого хранения. В закрытых хранилищах число участников в сети меньше, чем в публичных, что упрощает настройку правил проверки и позволяет отменять транзакции. При использовании частных блокчейнов можно воспользоваться преимуществами блокчейнов, не открывая систему для общественности. Тем не менее, они могут иметь более высокие риски информационной безопасности, как и централизованная система, поскольку транзакции проверяются изнутри и не используют высокие вычислительные ресурсы. Частные блокчейны часто используются для управления базами данных [12].

Гибридный блокчейн — это нечто среднее между публичным и частным блокчейном в плане открытости и децентрализации. Гибриды разработаны для того, чтобы найти правильный баланс безопасности, возможности аудита и масштабируемости приложений, которые на них работают. Гибридные подходы часто представляют собой блокчейны консорциума, где уполномоченные участники, осуществляющие проверку и выполнение транзакций, являются членами консорциума [9]. Примером гибридного блокчейна (который является общедоступным) является Ripple. Все участники действуют как валидаторы, что делает его публичным блокчейном с точки зрения доступа, но не каждый может присоединиться и вносить изменения в сети [4].

Гибридные хранилища обычно не требуют высокой безопасности, которую обеспечивают основные консенсусные алгоритмы, такие как доказательство работы (PoW), поскольку членам доверяют по умолчанию. Это является недостатком по сравнению с общедоступными блокчейнами, потому что решение о том, кто может присоединиться к сети или, кто может передать данные в регистр, обычно делается централизованным способом [13]. Кроме того, из-за неравенства пользователей в сети, решение о том, как достичь консенсуса безопасным способом, является более трудным, особенно в условиях, где одни пользователи обладает значительно большей властью, чем другие. Тем не менее, юридические и нормативные требования к проектам блокчейна во многих отраслях (например, в сфере финансов, недвижимости,

банковского дела), скорее всего, потребуют, чтобы пользователь был известен в любом случае, и поэтому блокчейны консорциума в основном используют другие протоколы, такие как PBFT вместо PoW [13].

Подводя итог, можно выделить два основных типа моделей проектирования, которые определены ниже, между ними - гибридный вариант, который также может быть создан на основе двух основных типов, в зависимости от контроля доступа: какие операции и кому они разрешены.

– открытый (общедоступный, инклюзивный, без требований прав доступа): блокчейн, в котором нет ограничений на чтение данных блокчейна и отправку транзакций в хранилище;

– закрытый (приватный, эксклюзивный, с правами доступа): это блокчейн, в котором прямой доступ к данным блокчейна и отправка транзакций разрешены только для предварительно определенных пользователей (узлов).

1.4 Методы достижения консенсуса

В зависимости от типа блокчейн-системы используются разные алгоритмы достижения консенсуса. Цель алгоритма состоит в том, чтобы обеспечить существование единой истории транзакций, и чтобы эта история не содержала недопустимых или противоречивых транзакций. Например, ни одна учетная запись не должна потратить больше ресурсов, чем содержит, или дважды тратить один и тот же ресурс (двойные расходы). В таблице 1.2 приводится сопоставление основных алгоритмов.

Биткойн решил проблему консенсуса следующим образом: для каждого нового блока идет многократный пересчет с перебором различных вариаций параметра nonce (однократно используемое число), то есть блок будет принят, если хэш меньше определённого значения, задающего сложность вычисления. Поскольку выходные данные функции хеширования распределены равномерно, невозможно создать блок таким образом, чтобы было легко удовлетворить условию. Между майнинговыми компьютерами в сети идет гонка за поиском нужного параметра nonce. Как только цель достигается, компьютер майнинга передает этот блок в сеть, и другие участники проверяют транзакции. Эта процедура называется доказательством работы (PoW). Поскольку цель состоит в том, чтобы не предоставлять слишком много полномочий одному человеку или организации, необходимо выбрать ограниченный ресурс, который будет потрачен на проверку блока. В PoW этим ресурсом является вычислительная мощность. Поскольку вычислительная мощность становится все дешевле и доступнее благодаря законам Мура и облачным вычислениям, сложность проблемы хеширования регулируется в зависимости от того, как часто были решены предыдущие проблемы. Однако распространенная критика PoW заключается в том, что «потеря» вычислительной мощности также означает большие потери энергии. По сути, это означает, что майнеры вынуждены объединять ресурсы в то, что в конечном итоге может стать гигантскими биткойн-фермами, тем самым централизовав

децентрализованную сеть. Кроме того, PoW не обладает очень высокой пропускной способностью транзакций.

Недостатки PoW вызвали интерес к разработке алгоритмов, которые не требуют такого же высокого потребления электроэнергии в процессе добычи. PoS заменяет вычислительную работу в процессе майнинга на долю владения определенной криптовалютой. Вместо того чтобы тратить деньги на электроэнергию и оборудование для майнинга, валидаторы могут покупать криптовалюту и использовать ее, чтобы участвовать в процессе выборов, чтобы получать вознаграждения и поддерживать работу сети. Количество валюты, поставленной на карту валидатором, соответствует вероятности их выбора в качестве валидатора [14]. Однако алгоритмы PoS выбирают валидатора с помощью алгоритма рандомизации, чтобы гарантировать, что ни один валидатор не может быть выбран заранее. Безопасность достигается не за счет потребления электроэнергии, а за счет повышения экономической ценности в виде доли в криптовалюте, которая может быть утрачена если валидатор будет действовать нечестно. Таким образом, PoS более сфокусирован на штрафы по сравнению с PoW, который основан на наградах для обеспечения безопасности [15].

Round Robin (циклический перебор) - это алгоритм, который используется некоторыми частными блокчейнами. В рамках этой модели консенсуса узлы по очереди создают блоки. Для обработки ситуаций, когда узел недоступен, этот алгоритм включает ограничение по времени, позволяющее доступным узлам добавлять блоки, чтобы недоступные узлы не приводили к остановке. Эта модель гарантирует, что ни один узел не создаст большее количество блоков чем другие. Алгоритм выигрывает простотой идеи, не имеет криптографических головоломок и имеет низкие требования к энергопотреблению. Поскольку существует необходимость в доверии между узлами, циклический перебор не работает в общедоступных блокчейнах без требований прав доступа, используемых большинством криптовалют.

Алгоритм нахождения консенсуса «Доказательство полномочий» (также называемый «доказательством идентичности») опирается на частичное доверие к пользователям через их связь с личностями в реальном мире. Пользователи должны иметь свои удостоверения в сети блокчейна (например, идентифицирующие документы, которые были проверены и заверены нотариально, и загружены в блокчейн). Идея заключается в том, что узел использует свои персональные данные/репутацию для добавления новых блоков. Пользователи сети блокчейн напрямую влияют на репутацию валидирующего узла, основываясь на его поведении. Чем ниже репутация, тем меньше вероятность добавления блока. Следовательно, в интересах узла поддерживать высокую репутацию. Этот алгоритм применяется только к блокчейнам с правами доступа и высоким уровнем доверия.

Таблица 1.2 – Сравнение различных алгоритмов нахождения консенсуса

Алгоритм	Цель	Преимущества	Недостатки	Примеры внедрения
Доказательство работы (Proof of Work, PoW)	Обеспечение сложности в форме вычислительной задачи, чтобы предоставить возможность обмена данными между ненадежными участниками.	Тяжело достичь отказа в обслуживании (атака DDoS неэффективна) Открыт для всех, у кого есть оборудование, чтобы решить вычислительную задачу.	Высокая вычислительная нагрузка, высокое энергопотребление Потенциал для атаки на 51%, получив достаточную вычислительную мощность.	Bitcoin, Ethereum и многие другие криптовалюты
Доказательство доли владения (Proof of Stake, PoS)	Обеспечение менее сложного в вычислительном плане препятствия для добавления новых блоков, чем в PoW, чтобы предоставить возможность обмена данными между ненадежными участниками.	Менее требовательно в вычислениях, чем PoW. Открыто для всех, кто хочет учувствовать в блокчейне.	Заинтересованные стороны контролируют систему. Существует возможность формированию пула заинтересованных сторон для создания централизованной власти. Потенциал для 51% атаки	Ethereum, Casper, Krypton
Делегированный PoS (Delegated PoS)	Создание механизма консенсуса через «демократию», где участники голосуют (используя криптографически подписанные сообщения), чтобы выбрать и отозвать права делегатов	Избранные делегаты экономически мотивированы оставаться честными Менее требовательно в вычислениях, чем PoW	Меньшее разнообразие узлов, чем в PoW или в чистых реализациях PoS Поскольку все делегаты «известны», у производителей блоков может быть стимул сговариваться, ставя под угрозу безопасность	Bitshares, Steem, Cardano, EOS

Продолжение таблицы 1.2

Алгоритм	Цель	Преимущества	Недостатки	Примеры внедрения
Циклический (Round-robin)	Обеспечить систему для добавления блоков среди доверенных узлов	Низкая вычислительная мощность. Идея проста в понимании.	Требует большого доверия среди узлов.	MultiChain
Доказательство полномочий (Proof of Authority/Identity, PoA, PoI)	Создать централизованный процесс согласования, чтобы минимизировать время создание блоков и скорость подтверждения	Быстрое время подтверждения Позволяет увеличить темпы производства блоков Может использоваться в боковых цепях (sidechain), которые используют другую модель консенсуса	Полагается, что валидирующий узел не был скомпрометирован Существует центральная точка отказа	Ethereum Kovan testnet, POA Chain
Доказательство истекшего времени (Proof of Elapsed Time, PoET)	Обеспечение более экономичной модели консенсуса за счет гарантий безопасности, связанных с PoW.	Менее требовательно в вычислениях, чем PoW	Требование по аппаратному обеспечению для синхронизации времени, к примеру, Intel SGX	Hyperledger Sawtooth

1.5 Смарт контракты

Термин «смарт контракт» появился в 1994 году и был определен Ником Сабо как «протокол транзакций, который выполняет условия сделки. Общими целями заключения смарт контракта являются удовлетворение общих договорных условий (таких как условия оплаты, залоговое удержание, конфиденциальность и даже принудительное исполнение), минимизация злонамеренных и случайных действий, а также уменьшение потребности в доверенных посредниках» [16].

Смарт контракты расширяют и используют идею блокчейна. Смарт контракт — это набор кода и данных (иногда называемых функциями и состоянием), которые заключаются с использованием криптографически подписанных транзакций в сети блокчейна (например, смарт контракты Ethereum или Hyperledger Fabric). Смарт контракт выполняется узлами в сети блокчейна; все узлы, которые исполняют смарт контракт, должны получать одинаковые результаты от выполнения, эти результаты записываются в распределённое хранилище. Код, находящийся в блокчейне, защищен от несанкционированного доступа и, следовательно, может использоваться (среди прочих целей) в качестве доверенной третьей стороны (рисунок 1.10). Смарт контракт может выполнять вычисления, хранить информацию, изменять данные, и, при необходимости, автоматически отправлять данные другим пользователям. Это не обязательно могут быть финансовые операции. Важно отметить, что не каждый блокчейн может выполнять смарт контракты.

Код смарт контракта может представлять собой многостороннюю транзакцию, обычно в контексте бизнес-процесса. В случае, когда в контракте несколько сторон, преимущество смарт контрактов состоит в том, что это может гарантировать безопасность данных и их прозрачность.

Смарт контракты должны быть детерминированными, то есть при одинаковых входных данных они всегда будут давать один и тот же результат на выходе. Кроме того, все узлы, выполняющие смарт контракт, должны согласовывать состояние после выполнения. Чтобы достичь этого, смарт-контракты не могут работать с данными вне того, что непосредственно передается в них (например, смарт контракты не могут получать данные веб-сервисов - их нужно будет передавать в качестве параметра).

Для многих реализаций блокчейна узлы выполняют код смарт контракта одновременно при добавление новых блоков. Существуют некоторые реализации блокчейна, в которых есть узлы, которые не выполняют код смарт контракта, а вместо этого проверяют результаты пользователей, которые это делают. Для публичных хранилищ с поддержкой смарт контрактов (таких как Ethereum) пользователь, выполняющий транзакцию со смарт контрактом, должен будет оплатить стоимость выполнения кода. Существует ограничение на время выполнения, которое может потребоваться при вызове смарт контракта, в зависимости от сложности кода. Если этот лимит превышен, выполнение останавливается, и транзакция отбрасывается. Этот механизм не

только вознаграждает пользователей за выполнение кода смарт контракта, но также предотвращает выполнение злоумышленниками атаки на отказ в обслуживании (DDoS), потребляя все ресурсы сети (например, используя бесконечные циклы). В сетях с разрешенными смарт-контрактами, например Hyperledger Fabric, пользователи могут не требовать оплаты за выполнение кода смарт-контракта. Эти сети разработаны с учетом наличия известных участников. Могут быть использованы другие методы предотвращения злоумышленного поведения (например, аннулирование доступа).

Мерфи и Купер [17] утверждают, что смарт контракт имеет четыре ключевые характеристики. К ним относятся:

– цифровая форма смарт контракта — это код, данные (параметры);

– договорные положения и функциональные результаты описаны в коде ПО;

– выполнение контракта по умолчанию гарантируется технологией – выполнение условий и порядок действий определяется самой технологией и правилами, которые заложены в смарт контракт;

– после получения результатов, выполнение смарт контракта не может быть остановлено, если только результат не зависит от невыполненного условия.

Рисунок 1.10 – Пример работы смарт контракта

С юридической точки зрения использование смарт контрактов поднимает различные правовые вопросы. Исполнение смарт контракта не вписывается в традиционную основу территориальной юрисдикции, что затрудняет определение того, какие законы будут применяться для решения договорных

вопросов, связанных с конкретным смарт-контрактом. Более того, существует проблема определения того, какой суд обладает юрисдикцией для рассмотрения судебных исков, вытекающих из использования смарт контрактов. Трудно разрешать споры, возникающие в связи с выполнением смарт контрактов. Например, если одна из сторон оспаривает, является ли смарт-контракт юридически обязательным.

Существует множество платформ для создания смарт контрактов. Все они созданы для разных целей и разными организациями. Рассмотрим блокчейны Ethereum, Hyperledger Fabric и технологию DLT Corda. Причина, по которой они были выбраны, заключается в том, что первый является общедоступным, второй - частным блокчейном, а третий - не блокчейном, а технологией DLT, созданной консорциумом финансовых учреждений R3.

Целью платформы Ethereum является объединение предыдущей работы над технологией блокчейна с новыми функциональными возможностями для улучшения масштабируемости, стандартизации, простоты разработки и взаимодействия с другими платформами. Это децентрализованная платформа с функциональными возможностями смарт контрактов. Его криптовалютой является «Ether», используемый для оплаты транзакций, а язык программирования, используемый для создания смарт контрактов в Ethereum, называется Solidity. Для выполнения смарт контрактов используются достаточно высокие вычислительные затраты, что ведет к проблемам с производительностью. Будучи широко используемой платформой, Ethereum, возможно, не лучший выбор для смарт контрактов т. к. транзакции могут быть видны любому.

Hyperledger Fabric — это блокчейн, основанный на проекте Hyperledger, который дает возможность выполнять смарт контракты. Hyperledger Fabric позволяет создавать распределенные приложения на языках программирования общего назначения и не зависит от платформы криптовалюты. Однако языком программирования, используемым в смарт контрактах, является Go.

Corda является не блокчейном, а платформой распределенного хранения, разработанной для финансового сектора. Это платформа, которую можно использовать для разработки приложений для финансовых учреждений. Это также частная сеть, предназначенная для записи, управления и синхронизации финансовых соглашений или контрактов между регулируемыми финансовыми учреждениями. Corda позволяет создавать записи для финансовых событий, которые невозможно отозвать. Смарт контракты Corda могут быть написаны на Java. Corda имеет простую архитектуру, которая повышает ее производительность и безопасность по сравнению с другими средами корпоративного уровня.

Рассмотрим общую схему взаимодействия между блокчейном, смарт контрактами и пользователями.

Вся экосистема смарт контрактов представлена четырьмя основными компонентами системы: объектами, атрибутами, внутренними и внешними связями. Объекты в экосистеме и их отношения показаны на рисунке 1.11.

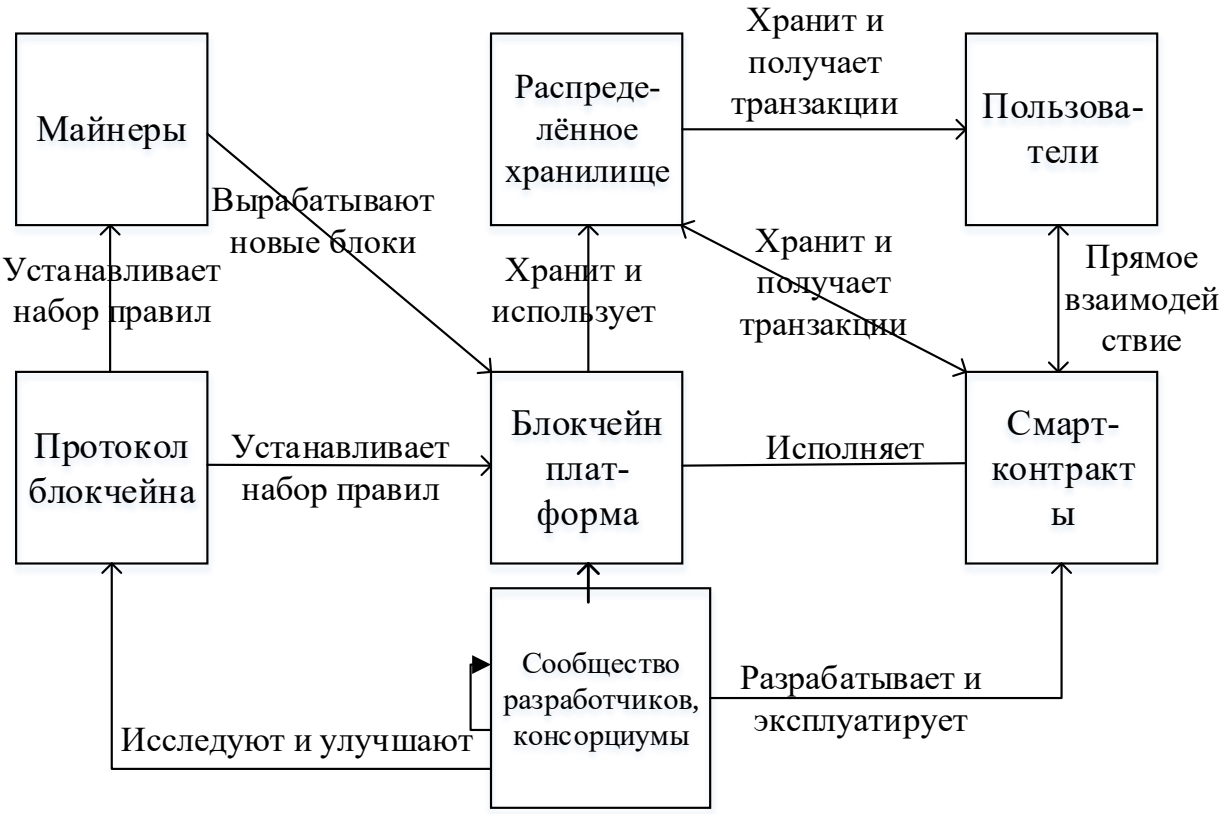

Рисунок 1.11 – Схема взаимодействия между блокчейном, смарт контрактами и пользователями

Ядро системы определяет блокчейн-платформа с возможностью осуществления смарт контрактов. Платформа блокчейна подчиняется протоколу блокчейна, который определяет реализации на техническом уровне. Это включает, например, используемый алгоритм консенсуса, криптографические хэш-функции или стимулы, предоставляемые майнерам (если таковые имеются). Кроме того, платформа блокчейна хранит и поддерживает распределенный реестр. Внутри распределенного реестра хранятся транзакции. Эти транзакции отправляются и принимаются пользователями и смарт-контрактами. Пользователи и смарт-контракты характеризуются наличием открытого ключа (то есть адреса) в блокчейне. Их взаимодействие достигается косвенно через транзакции, хранящиеся в распределенном реестре, или напрямую через вызовы функций смарт контрактов. Таким образом, любые взаимодействия по изменению состояния, такие как отправка данных, изменение переменных состояния в смарт-контракте или создание новых контрактов, должны проводиться посредством транзакции [2]. Смарт контракты могут взаимодействовать через вызовы функций API. Сообщество разработчиков внедряет платформу блокчейна, разрабатывает и поддерживает смарт контракты, а также исследует, определяет и улучшает протокол блокчейна. Это сообщество состоит из волонтеров, компаний, консорциума, некоммерческих организаций и других частных

организаций. Майнеры предоставляют вычислительную мощность и новые блоки, решая вычислительные головоломки, чтобы расширить распределенный реестр и поддерживать платформу блокчейна. Вышеупомянутые объекты изображают основу системы смарт контрактов.

1.6 Постановка задачи исследования

Блокчейн в последние годы демонстрирует быстрое развитие и рост популярности, однако на данный момент, единственным повсеместным применением технологий блокчейна являются криптовалюты.

По исследованиям Gartner [18], результаты которых представлены на рисунке 1.12, основным вектором развития децентрализованного хранения данных является поиск новых применений в самых различных областях цифровой экономики. В среднем для каждой технологии потребуется еще от 3 до 10 лет, чтобы перейти в стадию продуктивности. На данный момент больше всего прогрессируют обмен цифровыми активами и криптовалюты, как самые зрелые технологии на рынке. Многие технологии остаются на стадии эксперимента, это происходит из-за проблем, указанных в разделе 1.2.

Рисунок 1.12 – Цикл популярности

Исходя из вышеизложенного, была определена основная цель работы - обеспечение конфиденциальности и безопасности информации на основе применения алгоритмов распределенного хранения и обработки данных.

Для осуществления данной цели необходимо решить следующие задачи:

– анализ существующих алгоритмов распределенного хранения данных;

– поиск новых перспективных сфер применения технологии;

– анализ применения алгоритмов распределённого хранения данных для обеспечения безопасности в сетях IoT;

– моделирование архитектуры интеграции технологии блокчейн и IoT.

2 Анализ моделей применений децентрализованного хранения и обработки данных

2.1 Модели интеграции алгоритмов распределённого хранения и обработки и систем IoT

Большинство исследователей классифицируют приложения блокчейна на финансовые и нефинансовые, поскольку криптовалюты составляют значительную долю существующих сетей блокчейнов. Есть другие классификации в соответствии с версиями блокчейна (1.0, 2.0 и 3.0). В таблице 2.1 приводится прикладная классификация, как самая полная с точки зрения областей применения.

Таблица 2.1 – Классификация применений алгоритмов распределённого хранения

Сфера применения	Приложения
Бизнес и индустрия	Логистика, энергетический сектор
Управление данными	Распространение данных, управление человеческими ресурсами
Финансы	Криптовалюты, онлайн торговые площадки
Проверка целостности данных	Страхование, интеллектуальная собственность, проверка подделок
Государство	Голосование, закон и право, общественное администрирование, доказательство существования
IoT	Е-бизнес, распределённое управление данными
Здравоохранение	Электронные медицинские карты
Образование	Репутация образовательных заведений, управление сертификатами
Безопасность и приватность	Анонимность в хранение данных

Одним из самых развивающихся отраслей на сегодняшний день является Интернет вещей, рассмотрим перспективы объединения двух технологий – блокчейна и IoT [19].

Интернет вещей (IoT) — это повсеместное взаимодействие интеллектуальных устройств через сеть Интернет. IoT дает возможность любым устройствам соединяться и обмениваться данными, тем самым превращая физический мир в огромную информационную систему. Различные технологии, такие как облачные вычисления и машинное обучение для анализа

данных и информационного моделирования, быстро становятся неотъемлемой частью структуры IoT. Огромный прогресс в области IoT также способствует росту бизнеса в области инфокоммуникационных технологий (ИКТ). Степень, в которой IoT станет частью нашей повседневной жизни, можно понять из того, что 95% новых продуктов к 2022 году будут иметь поддержку IoT [20].

В условиях постоянно растущего количества устройств IoT и их доступности из Интернета, безопасность, т.е. законный доступ пользователей к данным, вызывает обеспокоенность. С одной стороны, вездесущий характер IoT стимулирует создание инновационных приложений для конечного пользователя, но, с другой стороны, отсутствие мер безопасности может привести к критическим проблемам, к примеру, таким как как кража со взломом в результате взлома умной сигнализации. Безопасность имеет еще один аспект, а именно «конфиденциальность». Компании, управляющие конфиденциальными пользовательскими данными, могут использовать их незаконно, что ведет к нарушению конфиденциальности.

Обострение ситуации связано с тем, что несколько лет назад были маловероятны сценарии развития IoT с миллиардами подключенных устройств, и по этой причине аспекты безопасности не всегда рассматривались на этапе проектирования продуктов. Фактически, согласно исследованиям, проведенным Gartner, в 2018 году расходы на безопасность IoT по всему миру достигли 1,5 млрд. долларов США, и к 2022 году половина всех бюджетов IoT будет направлена на устранение неисправностей, отзыв устройств с рынка и на устранение проблем безопасности, а не на защиту [21].

На данный момент IoT применяется в следующих областях: здравоохранение, промышленность, розничная торговля, строительство, развитие городской инфраструктуры, транспорт, энергетика и т.д. Согласно IHS Markit, прогнозируется, что на конец 2030 г. число подключенных устройств IoT достигнет 125 млрд. устройств [22].

Так как концепция IoT интегрируется в существующую архитектуру сетей, IoT использует IP-сети и облачную инфраструктуру для связи устройств и приложений, которые могут обмениваться информацией как между собой внутри частных сегментов, так и между сетями, оптимизируя процессы для увеличения эффективности и обеспечения безопасности.

Для реализации IoT наиболее важными вопросами являются безопасность данных, доверие к сети и изоляция соединения.

– безопасность данных;

Вирус, обнаруженный в 2010 году, нанес огромный ущерб промышленной и государственной инфраструктуре, такой как атомные электростанции, плотины и государственные сети связи (сети специального назначения). Надежная инфраструктура IoT гарантирует, что критически важные вычислительные сетевые ресурсы и ресурсы хранения работают, без незапланированных простоев оборудования. Безопасность означает, что данные не повреждены, не потеряны, не украдены и не подделаны.

– доверие к сети;

После случая с утечкой информации о нарушении закона «О защите персональных данных» в 2013 году в США, тем, кто внедряет IoT, трудно доверять партнерам и работникам, которые могут предоставлять доступ определенными структурам (например, правительствам, производителям или поставщикам услуг), позволяя им собирать и анализировать пользовательские данные. Таким образом, доверие и анонимность должны лежать в основе будущих решений IoT.

– контроль неизолированных соединений.

Взаимосвязанные устройства внутри локального сегмента IoT сети (к примеру, внутри дома или на территории промышленного здания) не работают изолированно, они должны взаимодействовать со всей экосистемой IoT. Глубина и ширина взаимосвязи определяют характер экосистемы IoT. Взаимодействие в сети Интернета вещей бывает нескольких типов: устройство к устройству, устройство к облачной платформе, устройство со шлюзом, облачная платформа к облачной платформе. Контроль неизолированных соединений является серьезной проблемой, которую необходимо решить.

В последние годы конфиденциальность и безопасность данных в области IoT была хороша исследована, и в результате были предложены различные подходы для решения разных аспектов конфиденциальности.

На данный момент одним из перспективных решений данных проблем является применение распределенных моделей хранения и обработки данных. Блокчейн — это многообещающая технология для достижения децентрализации, поскольку она позволяет достичь распределенного консенсуса между различными сторонами без необходимости доверять друг другу или центральному серверу / базе данных. То есть блокчейн, может обеспечить эффективное решение для конфиденциальности и безопасности данных IoT. Блокчейн обеспечивает высокий уровень конфиденциальности благодаря использованию изменяемого открытого ключа (public key) в качестве подтверждения личности пользователя. Эти особенности делают его привлекательным для обеспечения распределенной конфиденциальности и безопасности в IoT. Фактически, когда дело доходит до IoT, блокчейн можно использовать для хранения критически важных межмашинных сообщений, отправляемых в виде транзакций, обеспечивая подотчетность и безопасность хранимых данных. Распределённое хранение и обработка также может обеспечить идентификацию и подтверждение происхождения устройств IoT с его криптографическими функциями. Уже есть ряд применений блокчейна для ряда приложений, например, проверка местоположения, распределенные систем хранения медицинских данных.

Улучшения, которые может принести интеграция блокчейна в IoT сети:

– Децентрализация и масштабируемость: переход от централизованной архитектуры к распределенной P2P устранит единые точки сбоев и узкие места в топологиях IoT сетей. Это также поможет предотвращать сценарии, когда одна компания или человек контролируют обработку и хранение информации огромного количества людей. Другими преимуществами децентрализации

архитектуры являются улучшение отказоустойчивости и масштабируемости системы.

– идентификация (AAA): с помощью блокчейна участники могут идентифицировать каждое устройство. Данные, передаваемые в систему, являются неизменными, и они неразрывно связаны устройством/пользователем. Кроме того, блокчейн может обеспечить доверенную распределенную аутентификацию и авторизацию устройств для приложений IoT;

– автономность: технология блокчейна расширяет возможности приложений, делая возможным разработку интеллектуальных активов в качестве услуги. Благодаря блокчейну устройства могут взаимодействовать друг с другом без участия каких-либо централизованных серверов;

– надежность: информация в IoT сети всегда будет оставаться неизменной и связанной с временной отметкой в блокчейне. Участники системы способны проверять подлинность данных и могут быть уверены, что данные не были подделаны;

– безопасность: информация может быть защищены, если они хранятся как транзакции блокчейна. Блокчейн может рассматривать обмен сообщениями устройств как транзакции, проверенные смарт-контрактами, таким образом обеспечивая безопасность обмена данными между устройствами. Текущие протоколы, используемые в IoT, могут быть оптимизированы с помощью блокчейна;

– рынок услуг: блокчейн может ускорить создание экосистемы IoT услуг и рынков данных, где транзакции между партнерами возможны без установления прав. Микросервисы могут быть легко развернуты, а микроплатежи могут быть безопасными в условиях распределенного доверия. Это улучшило бы взаимосвязь IoT и доступ к данным IoT в блокчейне;

– безопасное развертывание кода: используя преимущества защищенного неизменяемого хранилища блокчейна, производители могут отслеживать состояния и обновления ПО с максимальной достоверностью.

Другой аспект, который следует принимать во внимание, относится к связи между базовой инфраструктурой IoT и блокчейном. При интеграции блокчейна необходимо решить, где будут происходить взаимодействия: внутри IoT, между IoT и блокчейном, или же исключительно через блокчейн. Туманные вычисления произвели революцию в IoT с добавлением нового уровня между облачными вычислениями и устройствами IoT и могли бы быть также использованы в целевой архитектуре интеграции.

– IoT – IoT: этот подход может быть самым быстрым с точки зрения задержки, поскольку он может работать в автономном режиме. Устройства IoT должны иметь возможность взаимодействовать друг с другом, что обычно включает механизмы обнаружения и маршрутизации данных. Только часть данных IoT хранится в блокчейне, тогда как взаимодействия IoT происходят без использования блокчейна (рис. 2.1а). Этот подход был бы полезен в

сценариях с данными IoT, где взаимодействия IoT происходят с низкой задержкой, однако в этом случае мы используем все преимущества распределенного хранения;

– IoT – блокчейн: в этом подходе все взаимодействия проходят через блокчейн, что позволяет фиксировать запись взаимодействий. Этот подход гарантирует, что все транзакции данных отслеживаются. Тем не менее, запись всех взаимодействий в блокчейне повлекла бы за собой увеличение пропускной способности и производительности конечных устройств, что является одной из хорошо известных проблем в блокчейне (рис. 2.1б);

– гибридный подход: гибридный дизайн, в котором только часть взаимодействий происходит в блокчейне, а остальные напрямую передаются между устройствами IoT. Одной из проблем этого подхода является выбор того, какие взаимодействия должны проходить через блокчейн. Идеальное сочетание этого подхода было бы наилучшим способом интеграции обеих технологий, поскольку он использует преимущества блокчейна и преимущества взаимодействия IoT в реальном времени. (Рис. 2.1в).

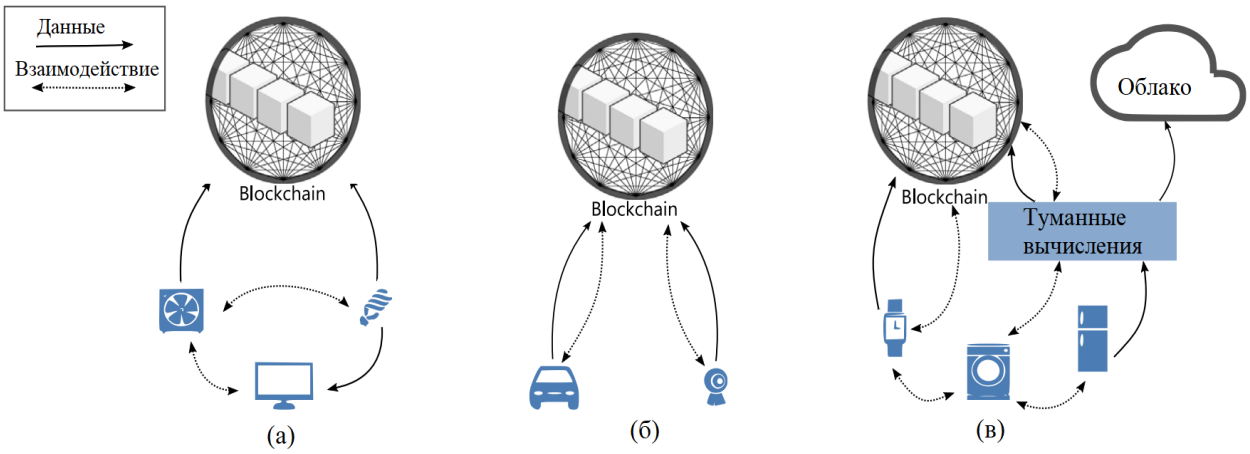

Рисунок 2.1 – Модели передачи данных в IoT сетях с блокчейном

Одним из применений IoT является платформа блокчейна для промышленного IoT (BPIIoT: A Light-Weighted Blockchain-Based Platform for Industrial IoT). BPIIoT использует смарт-контракты для разработки децентрализованных приложений облачного производства (cloud based manufacturing). При этом устройства IoT запускают сервисы распределённого хранения и используют кошельки для отправки транзакций в смарт контракты (умные контракты).

Так же смарт контракты можно использовать для управления данными, для обновления встроенного программного обеспечения устройств IoT, для управления доступом в качестве системы хранения данных в многоуровневой архитектуре IoT. Так же смарт контракты применяют для защиты авторизации к ресурсам IoT.

Вышеупомянутые модели используют либо выполнения смарт-контрактов, либо выполнения конкретных задач приложений, но не децентрализацию систем IoT и достижения автономного выполнения приложений.

Протокол Tangle реализует глобальный распределенный регистр для IoT, используя направленный ациклический граф, сгенерированный транзакциями. Tangle спроектирован для IoT для использования микроплатежей, однако он не предоставляет архитектуру или структуру данных для децентрализации IoT, также Tangle не является полным по Тьюрингу, чтобы поддерживать создание сценариев и смарт - контракты.

С целью разрешения / запрета доступа к данным, считываемым через устройства IoT используются различные политики. В целом, эти политики регулируются в соответствии с предварительно определенным набором правил. До настоящего времени в области IoT использовались различные модели управления доступом: управление доступом на основе ролей (RBAC), управление доступом на основе возможностей (CapBAC); управление доступом на основе атрибутов (ABAC) и модели управления доступом на основе семантических правил. Например, вводится основанная на блокчейне структура управления доступом под названием FairAccess для удовлетворения потребностей IoT в области безопасности и конфиденциальности. В FairAccess блокчейн используется для распределенного отслеживания и достоверности транзакций доступа между автономными организациями. С этой целью FairAccess вводит новые типы транзакций для предоставления, получения, делегирования и отзыва прав доступа к ресурсам.

Существует модель конфиденциальности и безопасности для «умных домов», где анализ рисков выполняется автоматизировано. Внешний объект, называемый провайдером управления безопасностью (SMP), может добавлять правила контроля доступа для защиты определенных устройств IoT или может применять динамические политики для изменения правил контроля доступа в зависимости от контекста, к примеру, в зависимости от местоположения.

Рассмотрим адаптивный подход с учетом контекста для устройств, которые обращаются к услугам на основе определения местоположения. Конфиденциальность обеспечивается агентом, который получает информацию о местоположении посредством анализа сетевых служб и реагирует на изменения местоположения. Кроме того, технология программно-определяемой сети (SDN) используется для блокировки / помещения в карантин устройств IoT в сети «умного дома» на основе их сетевой активности. Это предложение направлено на защиту конфиденциальности пользователя путем ограничения доступа к данным через внешний объект, то есть SMP, с использованием контекстной информации.

Одна из самых больших проблем при интеграции блокчейна в IoT — это масштабируемость. На самом деле, из-за огромного количества устройств и нехватки ресурсов для развертывания блокчейна в IoT является особенно сложной задачей. Оптимальная архитектура должна масштабироваться для

большого количества устройств IoT (они должны быть равноправными в сети), и сеть должна быть способна обрабатывать транзакции с высокой пропускной способностью.

2.2 Использование алгоритмов распределённого хранения в различных областях

2.2.1 Проверка функциональности и эффективности систем распределенного хранения данных в сфере здравоохранения.

Одним из наиболее важных применений технологии блокчейн является здравоохранение. Потенциал блокчейна в здравоохранении заключается в решение проблем, связанных с безопасностью данных, конфиденциальностью, совместным использованием и хранением данных.

Одним из требований для отрасли здравоохранения является способность двух сторон, будь то человек или машина, обмениваться информацией точно, эффективно и последовательно, так как цена ошибки при взаимодействии различных участников системы возрастает. Таким образом, целью применения блокчейна в здравоохранении является содействие обмену информацией, связанной со здоровьем, такой как электронная медицинская карта, между поставщиками медицинских услуг и пациентами. Более того, такое применение позволяет поставщикам безопасно обмениваться медицинскими записями пациентов (с учетом разрешений пациентов), независимо от местоположения поставщика и доверительных отношений между ними [23].

Технология распределенного хранения переопределяет моделирование данных и управление, развернутое во многих приложениях здравоохранения. Новые технологии здравоохранения, основанные на блокчейне, концептуально организованы в четыре уровня, включая источники данных, технологию блокчейна, приложения для здравоохранения и заинтересованные стороны. Рисунок 2.2 иллюстрирует представление основанного на блокчейне рабочего процесса для приложений здравоохранения.

Первоначально все данные из медицинских устройств, лабораторий, сетей и многих других источников объединяются и создают необработанные исходные данные. Эти данные являются неотъемлемым компонентом всей системы, основанной на блокчейне, и это основной компонент, который создает первый уровень стека. Технология блокчейна находится на уровень выше исходных данных. Каждая платформа блокчейна имеет разные особенности, такие как согласованные алгоритмы и протоколы. Платформы блокчейна облегчают пользователям создание и управление своими транзакциями.

Основными компонентами блокчейна являются смарт контракты, подписи, события, членство и цифровые активы. Исходя из ряда требований, которые необходимо выполнить, выбирается тип блокчейна – закрытый, открытый или гибридный. Следующим этапом является обеспечение интеграции приложений со всей системой. Основанные на блокчейне медицинские приложения можно разделить на три широких класса. Во-первых, управление данными, включая глобальный обмен научными данными для

исследований и разработок (НИОКР), управление и хранение данных (например, облачные приложения) и электронные медицинские карты. Второй класс представляет приложения управления поставками и логистикой, включая клинические испытания и фармацевтические препараты. Наконец, третий класс охватывает IoMT, включая слияние IoT и медицинских устройств. Наконец, на вершине иерархии находится уровень заинтересованных сторон, который состоит из сторон, пользующихся медицинскими приложениями, таких как бизнес-пользователи, исследователи и пациенты. Основными задачами пользователей на этом уровне является эффективный обмен, обработка и управление данными без ущерба для их безопасности и конфиденциальности.

Рисунок 2.2 – Модель применения блокчейна в здравоохранении

На рисунке 2.3 смоделируем схему движения медицинских данных при использовании блокчейна.

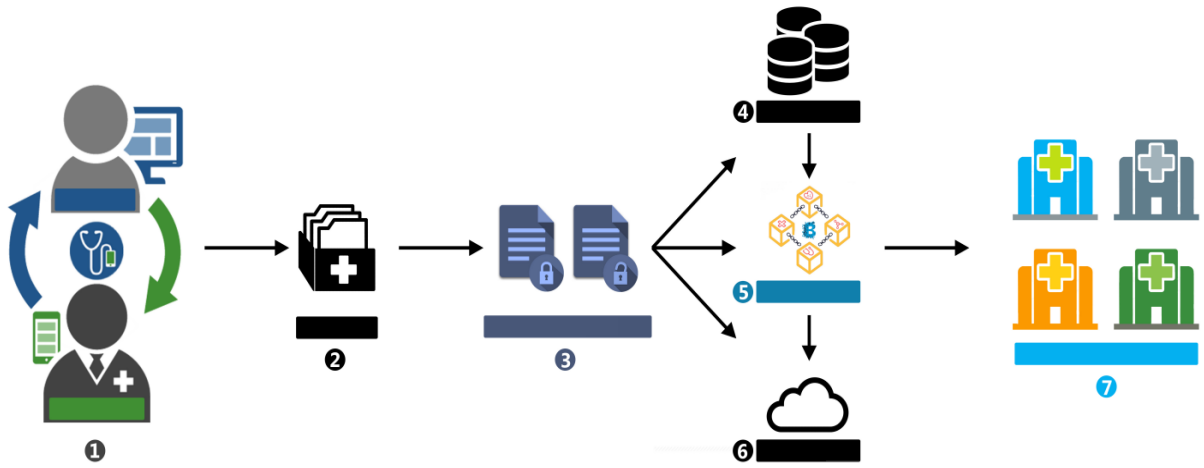

Рисунок 2.3 – Модель управления медицинскими данными в блокчейне

Шаг 1. Первичные данные генерируются взаимодействием пациента с его врачами и специалистами или такими устройствами как фитнес-трекерами, портативными пульсометрами, глюкометрами и так далее. Эти данные состоят из истории болезни, текущей проблемы и другой физиологической информации.

Шаг 2. Электронная медицинская карта (ЭМК) создается для каждого пациента с использованием первичных данных, собранных на первом этапе. Другая медицинская информация, например, полученная в результате лечения больных, истории болезни, также включена в ЭМК.

Шаг 3. Система контроля доступа к данным - пациент имеет индивидуальный контроль доступа к своей карте. Стороны, которые хотят получить доступ к этой информации, должны запросить разрешение, которое направлено владельцу медицинской карты, и владелец сам решает, кому будет предоставлен доступ.

Шаги 4,5,6. Эти три шага являются частью ядра всего процесса, включая базу данных, блокчейн и облачное хранилище. База данных и облачное хранилище хранят записи распределенным образом, а блокчейн обеспечивает максимальную конфиденциальность для обеспечения индивидуального доступа пользователей.

Шаг 7. Поставщики медицинских услуг, такие как специализированная клиника, общественный центр, больницы, являются конечными пользователями, которые хотят получить доступ к безопасной и надежной медицинской информации, доступ к которой будет санкционирован владельцем.

Технология блокчейна имеют популярность в секторе здравоохранения благодаря важности решения проблем безопасности ЭМК. ЭМК обладают потенциалом для улучшения оказания услуг медицинской помощи. Карточка изменяется, когда пациент поступает в больницу, или когда врач ставит диагноз пациенту или когда результаты диагностики, такие как сканирование МРТ, сохраняются в системе ЭМК. Таким образом, безопасность такой цифровой

информации имеет первостепенное значение, и в настоящее время должно использоваться распределённое хранение для надежных медицинских данных. Сохранение ценности данных и снижение стоимости хранения для управления данными в технологии блокчейна в здравоохранении играет важную роль. Благодаря своей уникальной возможности, технология блокчейна является единственным ответом для защиты цифровой информации, и она продолжает играть решающую роль в будущем управления корпоративными данными.

Управление поставками в здравоохранение на данный момент это сложный процесс, при комплектации заказов медикаментов, лекарств и других ресурсов существует наследственный риск нарушения процесса цепочки поставок, который может непосредственно повлиять на безопасность пациентов. Согласно исследованию, проведенному Всемирной организацией здравоохранения (ВОЗ), более 100 000 человек умирают в Африке из-за неправильного дозирования поддельных лекарств, заказанных у неизвестных или проверенных поставщиков. Подделка лекарств, отсутствие реестра и ошибки упаковки в медицинском учреждении могут нарушить работу всей цепочки поставок. Блокчейн является ключевой технологией мониторинга, позволяющей контролировать весь процесс перемещения лекарственных препаратов. Поскольку все изменения записаны, и каждый узел в блокчейне поддерживает чтение всех транзакций, легко проверить происхождение препарата, поставщика и дистрибьютора. Кроме того, распределенное хранение позволяет работникам здравоохранения и врачам проверять подлинность учетных данных поставщиков. Благодаря лучшему пониманию цепочки поставок благодаря надлежащему и своевременному процессу аутентификации, аптеки и поставщики медицинских услуг смогут гарантировать, что поток лекарств будет по-прежнему достигать тех пациентов, которые в нем нуждаются больше всего. В этом отношении технология блокчейн имеет большие перспективы для создания надежной сети поставщиков. Рисунок 2.4 иллюстрирует фармацевтический процесс управления поставками с использованием технологии блокчейн.

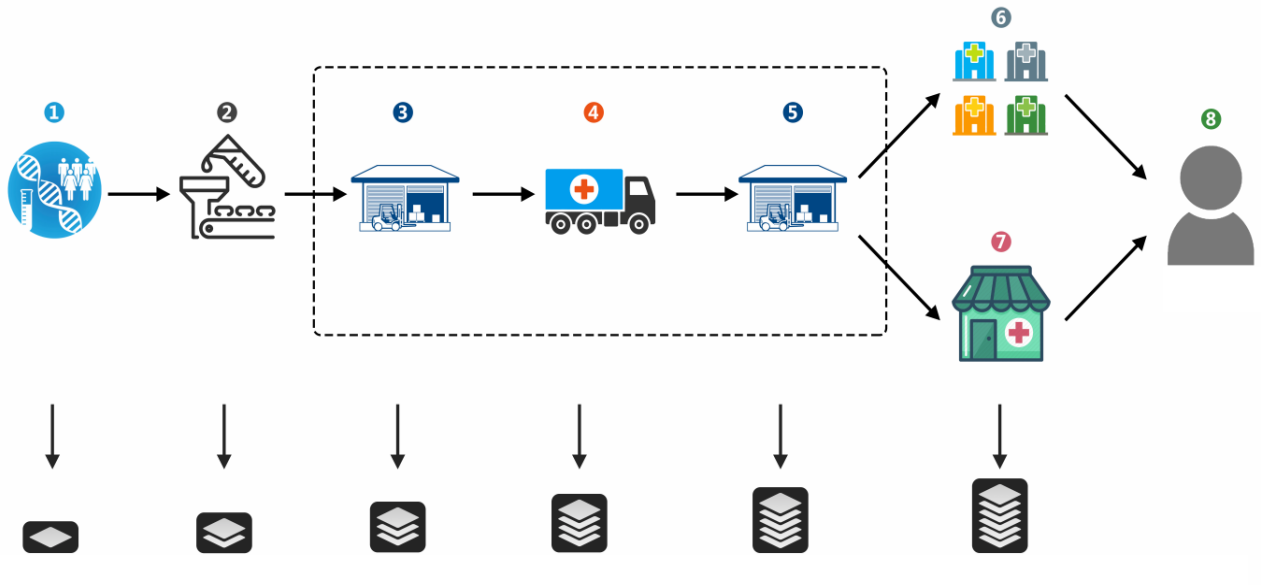

Рисунок 2.4 – Управление поставками лекарств

Шаг 1. Блок создается при изобретении нового лекарства или медицинской помощи, которая включает патентную защиту и длительный процесс клинических испытаний. Эта информация записывается в распределённый реестр.

Шаг 2. Как только клиническое испытание будет успешным, патент отправляется на завод-изготовитель для испытания опытного образца и серийного производства. Каждый продукт имеет свою уникальную идентификацию, включая другую соответствующую информацию.

Шаг 3. После завершения массового производства вместе с упаковкой лекарство собирается на складе для дальнейшей продажи. Такая информация, как, время, номер лота, штрих-код, дата истечения срока годности включены в блокчейн.

Шаг 4. Информация о транспортировке также включена в цепочку блоков, которая может включать в себя время ожидания, способ транспортировки, авторизованного агента и другую информацию.

Шаг 5. Независимая дистрибьюторская сеть, как правило, отвечает за распределение лекарств и медикаментов поставщикам медицинских услуг или розничным торговцам. Для этой цели используется склад для третьей стороны, откуда связаны все конечные точки распространения. Отдельная транзакция также интегрирована в блокчейн.

Шаг 6. Поставщики медицинских услуг, такие как больницы или клиники, должны предоставить информацию, например, номер партии, владельца продукта, дату истечения срока годности для проверки подлинности и предотвращения подделок. Это также входит в блокчейн.

Шаг 7. Действия, предпринимаемые продавцом, аналогичны Шагу 6.

Шаг 8. Пациентам рекомендуется определять подлинность на протяжении всего процесса, поскольку цепочка поставок блокчейн предлагает прозрачную информацию для проверки потенциальным покупателям.

Такой процесс обеспечивает недорогой контроль качества, регистрацию продукта, отслеживание движения лекарств и их происхождение через весь процесс поставок.

Системы IoMT играют жизненно важную роль в развитии систем здравоохранения [24]. Благодаря технологии IoMT медицинское оборудование, такое как кардиомонитор, сканеры тела и носимые устройства, могут собирать, обрабатывать и обмениваться данными через Интернет в режиме реального времени. Например, с развитием ИИ поставщики медицинских услуг, используя парадигму IoMT, могут захватывать изображения, идентифицировать злокачественные участки и делиться такими знаниями через глобальные сети (рисунок 2.5).

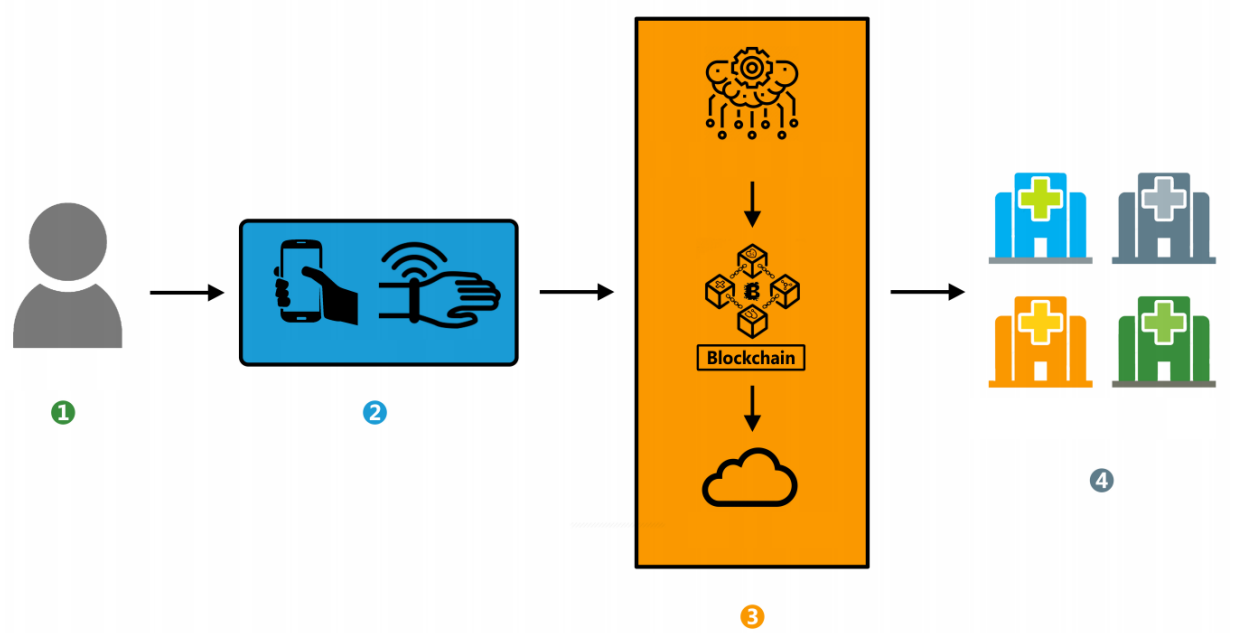

Рисунок 2.5 – Применение IoMT с блокчейном

Шаг 1. В сфере IoMT пациент является источником всех данных.

Шаг 2. Медицинские устройства IoT обычно либо прикреплены близко, либо дистанционно контролируют тело пациента, генерируя большой объем данных.

Шаг 3. Данные, созданные на шаге 2, хранятся в блоках или в облачном хранилище. В случае конфиденциальных медицинских данных, где безопасность является первоочередной задачей, децентрализованная система может помочь блокировать блоки данных для достижения максимальной безопасности.

Шаг 4. Поставщики медицинских услуг — это конечные пользователи, которые получают доступ к безопасной и надежной медицинской информации.

С помощью технологии блокчейна данные пациента будут действительно принадлежать и контролироваться законным владельцем данных, то есть пациентом. Тем не менее, есть еще несколько открытых проблем, которые требуют дальнейшего изучения. Например, способность блокчейна своевременно хранить и обрабатывать массивные транзакции доступа к данным. По мере увеличения объема транзакций задержка блоков будет увеличиваться в геометрической прогрессии. Следовательно, существует потребность в инновационных механизмах и алгоритмах для минимизации задержек при майнинге.

Кроме того, рассмотрена применимость блокчейна для решения проблемы доверия и повышения прозрачности данных в клинических испытаниях. Можно использовать блокчейн для повышения научной достоверности результатов клинических испытаний, которые могут быть подорваны такими проблемами, как отсутствие исходных данных и выборочная публикация. Очевидно, что технология блокчейн станет незаменимым инструментом для фармацевтов и медицинских работников для надлежащей и своевременной проверки подлинности потока законных лекарств и их доставки пациентам. Тем не менее, необходимы дальнейшие исследования надежных механизмов отслеживания, которые контролируют регистрацию продуктов.

Системы здравоохранения XXI века будут состоять из различных устройств, соединяющих пациентов (например, удаленные медицинские носимые устройства.) Эти системы генерируют данные непрерывно и могут подвергаться злонамеренным атакам во время передачи на различных уровнях сети связи. Основная проблема заключается в том, как блокчейн будет работать в сложных и разнообразных системах связи. Система IoMT будет использовать сети связи, принадлежащие разным поставщикам услуг с разными политиками контроля доступа к данным. Кроме того, поскольку сеть состоит из узлов и компьютеров, которые географически распределены, существует необходимость в механизмах синхронизации для определения порядка добавления блоков.

2.2.2 Использование алгоритмов распределенного хранения для гарантирования честности при проведении процессов голосования.

Одним из наиболее актуальных применений для блокчейна является голосование. Блокчейн распределяет индивидуальную информацию для голосования по тысячам компьютеров по всему миру, что делает невозможным изменение или удаление голосов после того, как они поданы. Такой подход способствует укреплению доверия между избирателями и правительствами, защищая их данные и конфиденциальность. Доверие создается благодаря тому, что пользователь контролирует свои данные. Подобные платформы позволяют гражданам голосовать на приложении для смартфонов, а не физически присутствовать на избирательных участках.

Архитектура блокчейна решает один из самых сложных факторов, влияющих на честность выборов - доверие. Блокчейн гарантирует, что доверие распределяется между множеством взаимно недоверчивых сторон, которые

потенциально могут соперничать друг с другом, которые участвуют в совместном управлении и поддержании криптографически безопасного цифрового следа выборов. Распределяя доверие таким образом, блокчейн сводит количество доверия, требуемого от тех, кто участвует в выборах, к минимуму. Основной недостаток блокчейна в предоставлении решения для большинства корпоративных применений заключается в том, что хранение больших файлов в блокчейне не является легкой задачей, так как он едва поддерживает небольшие текстовые строки, которые просто записывают передачу баланса между двумя сторонами. Однако Interplanetary File System (межпланетная файловая система - IPFS) представляет собой интересный проект, который может предоставить большую часть инфраструктуры, необходимой для хранения контента блокчейна, поскольку он обеспечивает постоянную децентрализованную сеть Web, где ни один объект не контролирует данные. Организации могут добавить к нему любые данные и в ответ получить уникальный идентификационный хеш (рисунок 2.6). Он обеспечивает децентрализованный способ хранения файлов в блокчейне, но дает больше контроля, надежно идентифицирует контент и обеспечивает программное взаимодействие.

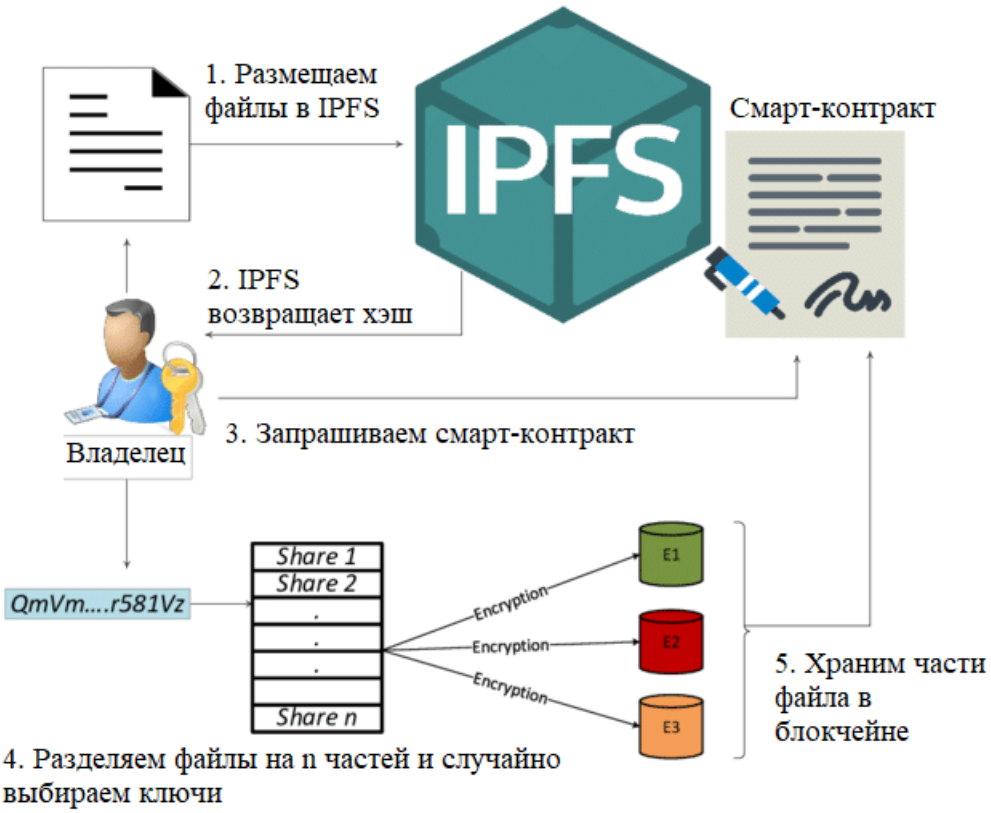

Рисунок 2.6 – Принцип работы IPFS и блокчейна

Некоторые проекты, которые в настоящее время разрабатывают или внедрили реализации электронного голосования в блокчейне:

Luxoft Holding, глобальный поставщик технологических решений для ИТ-услуг, стремится предоставить платформу для электронного голосования, которая дает возможность первого голосования на основе блокчейна. Являясь одним из основателей The Crypto Valley Association, которая стремится создать ведущую в мире экосистему блокчейнов и криптографических технологий, компания Luxoft сотрудничает с организациями, работающими над правительственными решениями сервисов блокчейнов, и предлагает им совместно создать блокчейн для правительственного альянса.

Компания утверждает, что использует инновационную технологию шифрования, которая анонимизирует голоса и обеспечивает защищенный учет и защищенный аудит. С помощью Университета прикладных наук и искусств Люцерна, Amazon AWS и n'cloud.swiss, платформа развернута в трех различных центрах обработки данных в облаке. Два из них находятся в Швейцарии и один в Ирландии. Распределяя данные по трем различным центрам обработки данных, риски безопасности и потери данных распределяются географически для обеспечения надежно

Fernado Lobato [25] разработал систему с открытым исходным кодом в виде умного контракта, работающего на Ethereum, в котором используются пороговые ключи и кольцевые подписи для обеспечения прозрачной и надежной системы, которая может быть реализована для выборов среднего размера. Каждый избиратель контролирует свой голос, оставаясь при этом анонимным среди множества пользователей. Протокол минимизирует централизацию, используя пороговую криптографию. Схема голосования разделена на следующие фазы после развертывания на блокчейне.

– настройка - избирательный орган загружает всю информацию о выборах. Продолжительность периодов голосования и регистрации, пороговый ключ для шифрования голосов избирателей и варианты голосования;

– регистрация - на этом этапе любой избиратель может обратиться в избирательный орган и потребовать, чтобы его открытый ключ был включен в набор открытых ключей, имеющих право голоса;

– голосование - на этом этапе любой ранее зарегистрированный избиратель подает зашифрованное голосование с пороговым ключом, опубликованным в контракте, с кольцевой подписью всех открытых ключей.

– завершено - после завершения этапа голосования все третьи стороны, обладающие секретами, могут передать их в блокчейн. Когда все секреты заключены в договоре, любой может загрузить и восстановить закрытый ключ;

– готов к подсчету - любой может подсчитать результат выборов;

– проанализировав текущую ситуацию в сфере электронного голосования на базе блокчейна, проверим насколько блокчейн может соответствовать всем требованиям, предъявляемых к системам голосования (Таблица 2.2).

Таблица 2.2 – Анализ применения блокчейна в электронном голосовании

Требования	Описание	Результат при применении блокчейна
Подлинность	Только пользователи с правом голоса должны иметь возможность голосовать	Каждый пользователь сети идентифицируется открытым ключом, доступ к которому возможен только через его собственный закрытый ключ. Если предположить, что каждый избиратель будет хранить свой собственный секретный ключ в безопасности, тогда требование подлинности будет выполнено
Уникальность голоса	Каждый избиратель должен иметь возможность проголосовать только один раз	Каждый поданный голос связан с открытым ключом избирателя на блокчейне. Позволяя каждому открытому ключу отдавать только один голос
Анонимность	Третье лицо не может сопоставить голос и избирателя	Поскольку каждый пользователь идентифицируется открытым ключом, а сохраненный голос зашифрован, невозможно связать избирателя с голосом
Целостность	Голоса не могут быть изменены или уничтожены	Так как хэш предоставляет блокчейну свойства, благодаря которым, голос нельзя фальсифицировать
Проверка результатов	Любой человек должен иметь возможность самостоятельно проверить, что все голоса были правильно подсчитаны	Поскольку блокчейн прозрачен для каждого узла сети, каждый может подтвердить, что количество отданных и подсчитанных голосов одинаково
Аудит и сертификация	Системы голосования должны быть проверены и сертифицированы независимыми агентами	Свойство прозрачности блокчейна позволяет любому узлу в сети проводить аудит блокчейна. Поскольку исходный код является открытым кодом и видим в блокчейне, это означает, что используемое приложение также может быть проверено

Продолжение таблицы 2.2

Требования	Описание	Результат при применении блокчейна
Мобильность	Возможность удаленного голосования	Единственными требованиями для доступа к сети является устройство с подключением к Интернету и адрес в платформе блокчейна, а это означает, что не требуется никакой специальной инфраструктуры или машин для голосования;
Прозрачность	Системы голосования должны быть четкими и предоставлять избирателям точность и безопасность.	Идентично требованию проверки результатов - прозрачность является одним из свойств блокчейна, и каждое приложение, реализованное в блокчейне, наследует это же свойство
Обнаружение ошибок и восстановлени е	Системы голосования должны выявлять ошибки, сбои и атаки и восстанавливать информацию для голосования	Если в цепочке блоков выполнено какое-либо вредоносное действие, оно будет обнаружено системой и признано недействительным, что соответствует требованию обнаружения. Как только некоторые данные сохраняются в блокчейне, они больше не могут быть удалены, а это означает, что данные всегда можно восстановить.

Исходя из вышеуказанных результатов на рисунке 2.7 приведем логическую архитектуру небольшого приложения для голосования.

Пользовательский интерфейс — это простая HTML-страница, которая позволяет пользователям получить доступ к функциям приложения.

API отвечает за реагирование на действия, выполняемые на интерфейсе, и взаимодействует с сервером шифрования и блокчейном. Для каждого запроса, сделанного в интерфейсе, он взаимодействует с сервером шифрования посредством вызовов сервера для шифрования, расшифрования или добавления голоса. Для взаимодействия с блокчейном используются транзакции.

Чтобы обеспечить конфиденциальность голосов, необходимо предотвратить несанкционированный доступ к голосам. Для этого каждый голос должен быть зашифрован перед передачей в блокчейн. Гомоморфное

шифрование — это схема шифрования с открытым ключом, свойства которой позволяют выполнять определенные типы вычислений на зашифрованном тексте, генерируя зашифрованный результат, когда при расшифровке результат будет равен выполнению той же операции с открытым текстом.

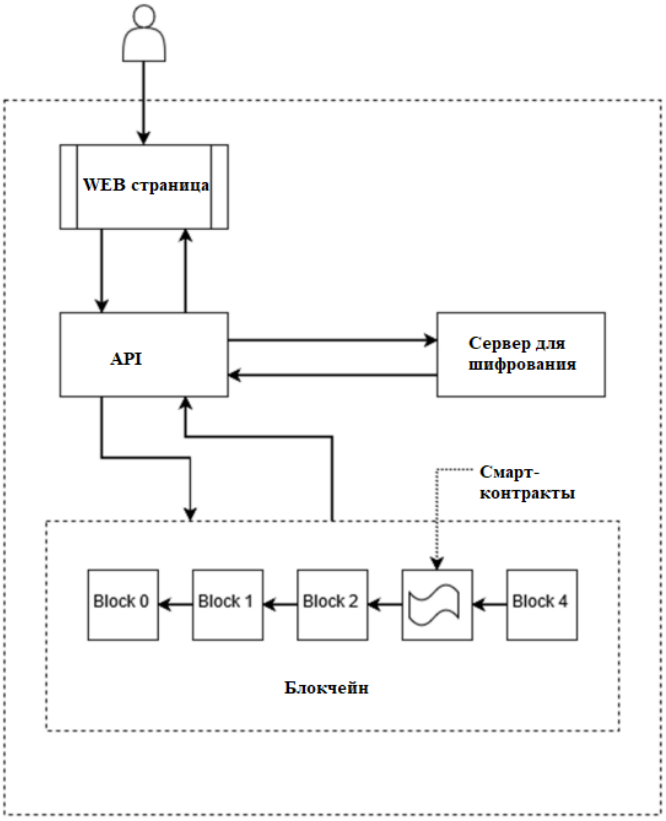

Рисунок 2.7 – Приложение для голосования, основанное на блокчейне

3 Моделирование архитектуры интеграции технологии блокчейн и IoT

3.1 Задачи моделирования блокчейна в IoT сетях

В данном разделе планируется провести моделирование и анализ интеграции распределенного хранения и обработки данных в IoT сетях. Как было отмечено ранее IoT сети имеют свои недостатки и ограничения, которые заключаются в следующем:

- низкая производительность оконечных устройств;
- низкая пропускная способность оконечных устройств;
- риски, связанные с передачей в нешифрованным виде важной информации (ранее были рассмотрены охранные доступы и медицинские данные).

Поэтому требуется выработать конкретные рекомендации по внедрению блокчейна, потому что интеграция без учета ограничений IoT сетей

нецелесообразна и технически неэффективна т.к. конечные узлы будут перегружены вычислительными операциями в случае PoW блокчейна.

Для решения этой задачи воспользуемся методами компьютерного моделирования.

3.2 Инструменты моделирования

3.2.1 Сетевой симулятор NS3.

Одной из самых больших проблем в исследованиях систем связи является высокая стоимость оборудования. Не все лаборатории могут приобрести несколько маршрутизаторов, точек беспроводного доступа и другого оборудования для тестирования новых протоколов, оптимизации архитектурных решений и выбора конкретных топологий для применения новых сетевых решений. Вот почему было создано программное обеспечение, которое может моделировать системы связи. С появлением этих программных продуктов стало возможным проводить необходимые исследования и эксперименты намного экономичнее и достичь практически тех же результатов, что и на реальном оборудование.

На сегодняшний день проблема компьютерного моделирования систем связи имеет самые разные методы решений.

Использование симулятора не только экономит деньги, но и позволяет проводить эксперименты без построения реальной сети, что дорого и трудоемко для проверки гипотез. Так же еще одно преимущество использования симулятора состоит в том, что в программных продуктах доступны любые модули оборудования.

На сегодняшний день известно множество сетевых симуляторов, и исследователи могут выбирать из широкого спектра продуктов таких как OPNET, OMNET, OMNET ++, NS2, NS3. Есть также узкоспециализированное ПО, созданное для моделирования конкретного оборудования. Как правило, такое программное обеспечение разрабатывается производителями телекоммуникационного оборудования, к примеру, Dynamips и Packet Tracer Simulator от Cisco, разработанные для эмуляции коммутаторов и маршрутизаторов.

Одним из наиболее распространенных является NS2, разработанный в 80-х годах. NS2 — это бесплатное программное обеспечение, оно имеет довольно большое и развитое сообщество, и в результате доступно огромное количество модулей, дополнений и фреймворков.

Широко используется сетевой симулятор NS3, один из самых передовых инструментов моделирования сетей передачи данных. NS3 распространяется под лицензией GNU GPLv2, программа передана в общественную собственность и распространяется бесплатно.

NS3 — это бесплатное программное обеспечение, распространяемое по лицензии GNU GPLv2 и предназначенное для исследований и обучения. Исходный код NS3 выпущен для исследования, модификации и использования

и доступен на веб-сайте проекта. NS3 - очень гибкий и мощный инструмент моделирования, использующий C ++ в качестве интегрированного языка описания моделей. В дополнение к C ++ также можно использовать Python [26].

С обширным и гибким API и полной документацией программного обеспечения, разработчики моделей не ограничены ни в чем, им предоставляется возможность построить модели любой сложности. Так же большинство распространённых моделей уже включены в пакет программного обеспечения. Благодаря используемой лицензии GNU GPLv2 исходный код NS3 может быть модифицирован. К примеру, разработчики NS3 создали модель беспроводных сетей, которая может моделировать движущиеся объекты в трехмерном пространстве. Модели были разработаны для создания различных сложных и смешанных топологий. Фреймворк под названием FlowMonitor предоставляет очень гибкий способ сбора различных показаний с моделируемых активных сетевых устройств и каналов связи. Проекты NetAnimator и PyViz используются визуализации моделей, так как у симулятора нет собственного графического интерфейса. Официальная документация содержит полный перечень всего функционала [27].

Разработка проекта NS3 продолжается на сегодняшний день. Об этом свидетельствует тот факт, что многие крупные компании опубликовали исследования, основанные на NS3. Некоторые компании и учреждения также объявили о разработке различных фреймворков для работы симулятора, разработчики ежедневно создают новые и более сложные модели. Симулятор может удовлетворить потребности в симуляции современных систем связи и является очень перспективным для развития, благодаря авторам проектов и сообществам, которые постоянно улучшают проект, разрабатывают новые модели и исправляют старые ошибки.

3.2.2 Bitcoin Simulator.

Bitcoin Simulator является фреймворком для симулятора NS3. Целью этого проекта является изучение того, как параметры, характеристики сети и модификации протоколов влияют на масштабируемость, безопасность и эффективность блокчейн сетей с поддержкой алгоритмов Proof of Work.

Цель симулятора - сделать его максимально реалистичным. Bitcoin Simulator способен симулировать любую повторную параметризацию блокчейн сети.

Во время разработки были использованы данные с blockchain.info, чтобы оценить время генерации блоков и распределение размера блоков, также использовался сканер (crawler) биткойнов, чтобы выяснить среднее число узлов в сети и их географическое распределение. Кроме того, использовались данные о подключения узлов, предоставленные Coinscope. Для облегчения процесса связи между узлами использовался quickjson.

Используя симулятор, и меняя входные параметры, указанные в таблице 3.1, можно оценить различные параметры блокчейна, такие как интервал генерации между блоками, размер блока, механизмы распространения, процент

устаревших блоков, пропускную способность и общее время распространения блоков.

Таблица 3.1 – Список основных входных параметров

Параметр	Описание	Стандартное значение
blockSize	Фиксированный размер блока (в байтах). Если используется значение по умолчанию, то blockSize используется согласно распределению размера биткойн-блока, оцененному путем сбора статистики из blockchain.info.	-1
noBlocks	Количество сгенерированных блоков	100
nodes	Общее количество узлов в сети. Количество узлов всегда должно быть больше или равно числу майнеров. Количество майнеров, скорости хэширования и их расположение можно изменять.	16
blockIntervalMinutes	Средний интервал генерации блока в минутах.	10
invTimeoutMins	Тайм-аут блока inv. Если используется значение по умолчанию, время ожидания в два раза больше, чем blockIntervalMinutes.	-1
litecoin	Использовать параметры сети litecoin.	false
dogecoin	Использовать параметры сети dogecoin.	false
blockTorrent	Включить протокол BlockTorrent.	false
spv	Включить механизм spv в blockTorrent. Используется только в сочетании с --blockTorrent.	false

У данного симулятора на текущий момент отсутствует графический интерфейс, все настройки производятся в терминальном окне на операционной системе Ubuntu.Рабочее окно программы со списком всех исходных параметров и примера работы приведено на рисунках 3.1 и 3.2.

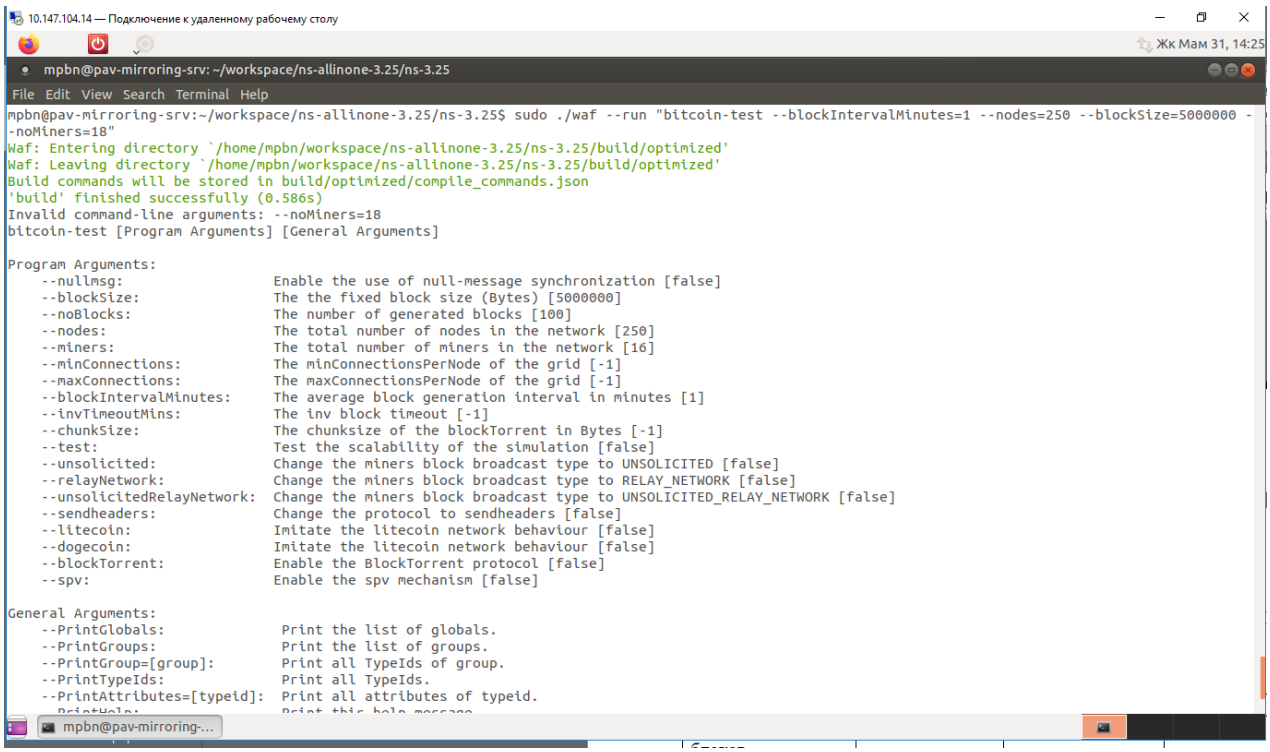

Рисунок 3.1 – Список всех исходных параметров Bitcoin Simulator

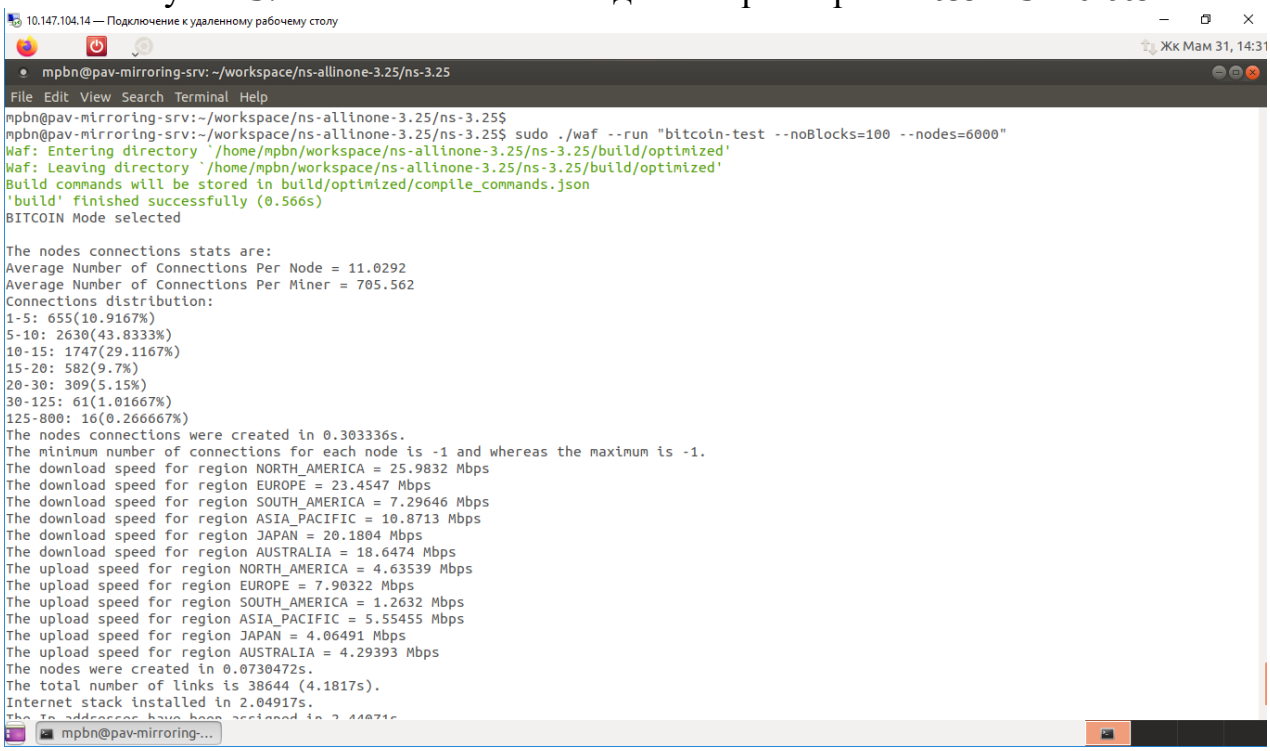

Рисунок 3.2 – Тестовый пример симуляции для 100 блоков и 6000 узлов со стандартными параметрами

3.2.3 Проверка симулятора.

С целью экспериментальной проверки симулятора сравниваются Bitcoin, LiteCoin и DogeCoin с симулированными аналогами.

Таблица 3.2 – Проверка достоверности симулятора

	Bitcoin	Litecoin	Dogecoin
Время генерации блоков, мин	10	2,5	1
Реальное значение – Среднее время распространения блока, сек	8,7	1,02	0,98
Симулированное значение– Среднее время распространения блока, сек	9,42	0,86	0,83
Реальное значение – Процент устаревших блоков, %	0,41	0,27	0,62
Симулированное значение – Процент устаревших блоков, %	0,15-1,85 (в зависимости от использования ретрансляции и незапрошенной отправки блоков)	0,24	0,79

Для каждого исследуемого блокчейна скорректированы входные параметры симулятора в соответствии с их реальными параметрами. Например, измерено распределение блоков биткойнов по размеру, а также скорость генерации блоков в реальной сети биткойнов в период с мая по ноябрь 2015 года [28]. Чтобы измерить процент устаревших блоков в реальных сетях блокчейнов, проверено 24 000 блоков биткойнов, 100 000 блоков Litecoin и 240 000 блоков Dogecoin[29].

Результаты показывают, что измеренное и смоделированное среднее время распространения блока близки, как и показатели устаревших блоков для Litecoin и Dogecoin. У Bitcoin скорость и время устаревания блоков падает в зависимости от использования ретрансляционной сети и незапрошенной отправке блоков (unsolicited block push). В случае, когда ретрансляционная сеть и незапрошенная отправка блоков не используются никем, скорость устаревания минимальна. Litecoin и Dogecoin не используют сети ретрансляции и не подвержены данной особенности.

3.3 Исследование характеристик блокчейна при интеграции в сетях IoT

3.3.1 Метрики и характеристики сети при интеграции блокчейна в сетях IoT.

Определим пять важных аспектов, которым должна подчиняться оптимальная реализация PoW для IoT: масштабируемость, безопасность, децентрализация, эффективность и пропускная способность сети. Далее проанализируем эти характеристики (Таблица 3.2).

Масштабируемость. Масштабируемость в IoT — это возможность изменения сети с точки зрения количества устройств, характеристик оборудования, а также функциональных требований при сохранении производительности. Для блокчейна это означает, что требуется одноранговая сеть, которая может масштабироваться в количестве узлов, пропускной способности, и в количестве транзакций за единицу времени.

Безопасность. Безопасность является критически важным аспектом в IoT. Хотя в этой работе не рассматривается несанкционированный доступ к IoT устройствам, проблема целостности данных для устройств IoT является важной проблемой, которую необходимо решить. В случае использования блокчейна целостность данных гарантируется по своей архитектуре.

Децентрализация. Децентрализация в IoT имеет решающее значение для повышения безопасности, конфиденциальности, и автономной работы. В одноранговых сетях, таких как блокчейны, децентрализация измеряется количеством правильно функционирующих узлов. В блокчейне, узел должен принять последний сгенерированный блок, прежде чем генерировать новый. Следовательно, определяем метрику для измерения децентрализации как количество функционирующих одноранговых узлов в сети. Также определяем нижнюю границу функционирующих одноранговых узлов, которая составляет 90% от общего объема, чтобы гарантировать надлежащую функциональность блокчейна для IoT.

Эффективность. Эффективность в IoT можно определить как оптимальное использование аппаратных ресурсов и энергии. Поэтому для достижения этого устройства IoT в блокчейне должны оптимально использоваться ресурсы и энергия для поддержания и развития блокчейна. Среди прочего, препятствием для этого является проблема устаревших блоков в PoW. В частности, устаревшие блоки ухудшают безопасность блокчейна, и транзакции в устаревших блоках рассматриваются сетью как необработанные, что требует дополнительных ресурсов для их обработки. Следовательно, определяем метрику для эффективности как коэффициент генерации устаревших блоков, верхняя граница которой равна 1%.

Пропускная способность сети. Пропускная способность сети будет равняться скорости сети IoT. Это определяется скоростями нисходящей линии связи и восходящей линии связи устройств IoT. Например, стандарты IEEE 802.15.4 и NarrowBand-IoT устанавливают пиковые скорости передачи данных 250 Кбит/с для связи между компьютерами, тогда как в стандартах LTE Cat M1

и LTE Cat 0 это 1 Мбит/с. Чтобы избежать перегрузок скорость принимаем равной 250 Кбит/с.

Таблица 3.3 – Оптимальные характеристики

Характеристика	Метрика
Масштабируемость	Максимальное количество IoT устройств, максимальное количество транзакций в секунду
Децентрализация	$\frac{\text{90\% времени распространения блока}}{\text{Время генерации блока}} \leq 1$
Эффективность	Процент устаревших блоков ~1%
Сетевая пропускная способность	250 Kbps

3.3.2 Настройка симулятора.

Чтобы использовать симулятор для наших оценок, классифицируем устройства IoT по двум ролям: майнеры и обычные устройства. Количество соединений на устройство майнера и обычное устройство соответствует распределению, как в работе [29]. Обычные устройства только проверяют и распространяют полученные блоки, тогда как майнеры также генерируют новые блоки. Соотношение майнеров к количеству узлов равно 7%, а остальные берут на себя роль обычных устройств, это подтверждается определенной статистикой [30].

Сетевая задержка играет критическую роль в производительности из-за природы однорангового распространения информации (то есть, блока и транзакции). Следовательно, чтобы оценить, как географическое расположение устройств влияет на задержку в сети, используем настройки симулятора для моделирования расположения устройств внутри одной страны, в Европе и во всем мире.

Пропускная способность устройств IoT, очевидно, влияет на время распространения информации в блокчейне. Чтобы получить реалистичную настройку пропускной способности, принимаем эталоны пропускной способности устройств Raspberry Pi. Это приводит к различной пропускной способности загрузки данных от 0,1 Мбит / с до 100 Мбит/с со средним значением 5 Мбит/с и различной пропускной способности отправки данных от 0,02 до 20 Мбит/с со средним значением 1 Мбит/с.

3.3.3 Размер блока и интервал генерации блоков.

Оценим влияние размеров блоков и интервалов генерации блоков с помощью симулятора с условием, что все устройства расположены внутри одной страны. Используем цикл генерации из шести блоков со следующими интервалами: 10 минут, 5 минут, 1 минута, 30 секунд, 10 секунд и 5 секунд. Для каждого поколения блоков в цикле варьируем размеры блоков: 10 КБ, 50 КБ, 100 КБ, 500 КБ, 1 МБ, 5 МБ, 10 МБ. Увеличим количество устройств IoT до 250 с 16 устройствами с ролями майнер. Результаты представлены в Таблице 3.4.

Данная задача выполняется путем выставления параметров:

– «--blockSize» в диапазоне от 10000 до 10000000;
– «--blockIntervalMinutes» в диапазоне от 0.0.8(3) до 10;
– «--nodes» статически равным 250;
– «--miners» статически равным 16.

Пример одного из экспериментов приведен на рисунке 3.3

Рисунок 3.3 - Процесс симуляции с интервалом 1 минуту и блоком равным 5MB

Исходя из требований, указанных в таблице 3.3, построим графики зависимости средней утилизации (рисунок 3.4), процента устаревших блоков (рисунок 3.5) и количества транзакций (рисунок 3.6) от размера блоков и интервала генерации и проведем дальнейший анализ.

Таблица 3.4 –Размер блока и интервал генерации блоков

Размер блока	Интервал генерации блоков	Суммарное количество блоков	Уста-ревшие блоки	Подлинные блоки	Процент устаревших блоков	Задержка распростра-нения	Средняя утилизация, kbps	Количество транзакций в секунду
10 MB	10 мин	10,8	0,43	10,4	3%	360	276	69,3
	5 мин	18,8	0,9	17,9	8,83%	755	723	119,5
	1 мин	45,6	16	26,93	35,07%	2162	21215	197,5
	30 сек	51,2	26,6	24,6	47,99%	2412	49520	164,1
	10 сек	57,7	41,2	16,5	71,38%	2560	151046	110,2
	5 сек	64,2	48,2	16	75,00%	2665	273777	107,1
5 MB	10 мин	10,2	0,26	9,9	2,6%	168	134	33,1
	5 мин	19,9	1	18,9	5,3%	180	288	63
	1 мин	67,3	12,1	55,2	17,99%	1888	8718	184
	30 сек	73,4	26,8	46,6	36,52%	2105	28528	155,5
	10 сек	84	56,5	27,5	67,18%	2472	100255	92
	5 сек	91,4	68,5	22,9	74,91%	2512	190671	76,4
1 MB	10 мин	12,3	0	12,3	0%	31	26	8,2
	5 мин	22,3	0	22,3	0%	32	53	14,9
	1 мин	92,4	3,4	89	3,71%	37	438	59,3
	30 сек	165,9	8,5	157,4	5,15%	818	3243	104,9
	10 сек	219,6	94,1	125,5	42,86%	1812	30259	83,7
	5 сек	232,5	128,7	103,8	55,37%	2183	69059	69,2
500 KB	10 мин	9,6	0	9,6	0%	15	13	3,2
	5 мин	18,6	0	18,6	0%	15	26	6,2
	1 мин	92,1	1,6	90,5	1,71%	17	136	30,1
	30 сек	165,2	9,2	156	5,56%	18	639	52
	10 сек	346,5	101,4	245,1	29,25%	1665	14762	81,7
	5 сек	350,6	161,1	189,5	45,96%	1972	41378	63,2

Продолжение таблицы 3.4

Размер блока	Интервал генерации блоков	Суммарное количество блоков	Уста-ревшие блоки	Подлинные блоки	Процент устаревших блоков	Задержка распростра-нения	Средняя утилизация, kbps	Количество транзакций в секунду
100 KB	10 мин	9,3	0	9,3	0%	3,2	2	0,6
	5 мин	23	0	23	0%	3,2	5	1,5
	1 мин	99	0	99	0%	3,2	27	6,6
	30 сек	186,4	4,4	182	2,35%	3,2	54	12,1
	10 сек	537,3	22,8	514,5	4,25%	3,4	447	34,3
	5 сек	954,5	124,5	830	13,04%	99	7249	55,3
50 KB	10 мин	11	0	11	0%	1,6	1	0,4
	5 мин	18,6	0	18,6	0%	1,6	2	0,6
	1 мин	96,3	0	96,3	0%	1,6	14	3,2
	30 сек	187,0	0,7	186,3	0,35%	1,6	28	6,2
	10 сек	562,0	10,2	551,8	1,82%	1,7	84	18,4
	5 сек	1120,4	43,4	1077	3,87%	1,8	931	35,9
10 KB	10 мин	10,3	0	10,3	0%	0,4	0,3	0,1
	5 мин	21,6	0	21,6	0%	0,4	0,7	0,2
	1 мин	101	0	101	0%	0,4	3,5	0,7
	30 сек	193,3	0	193,3	0%	0,4	7	1,3
	10 сек	598,6	0	598,6	0%	0,4	21	4
	5 сек	1166,3	19,9	1146,4	1,71%	0,4	42	7,6

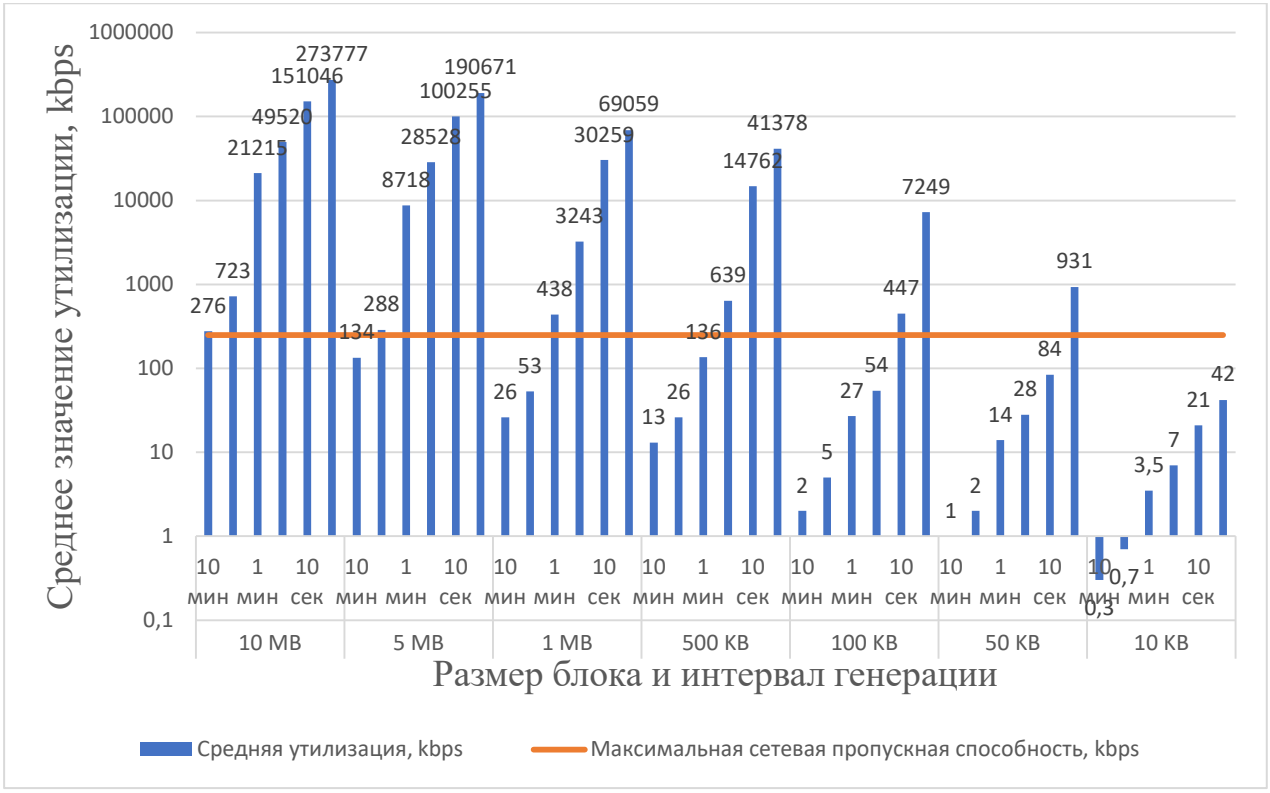

Рисунок 3.4 - Зависимость средней утилизации от размера блоков и интервала генерации в логарифмической шкале

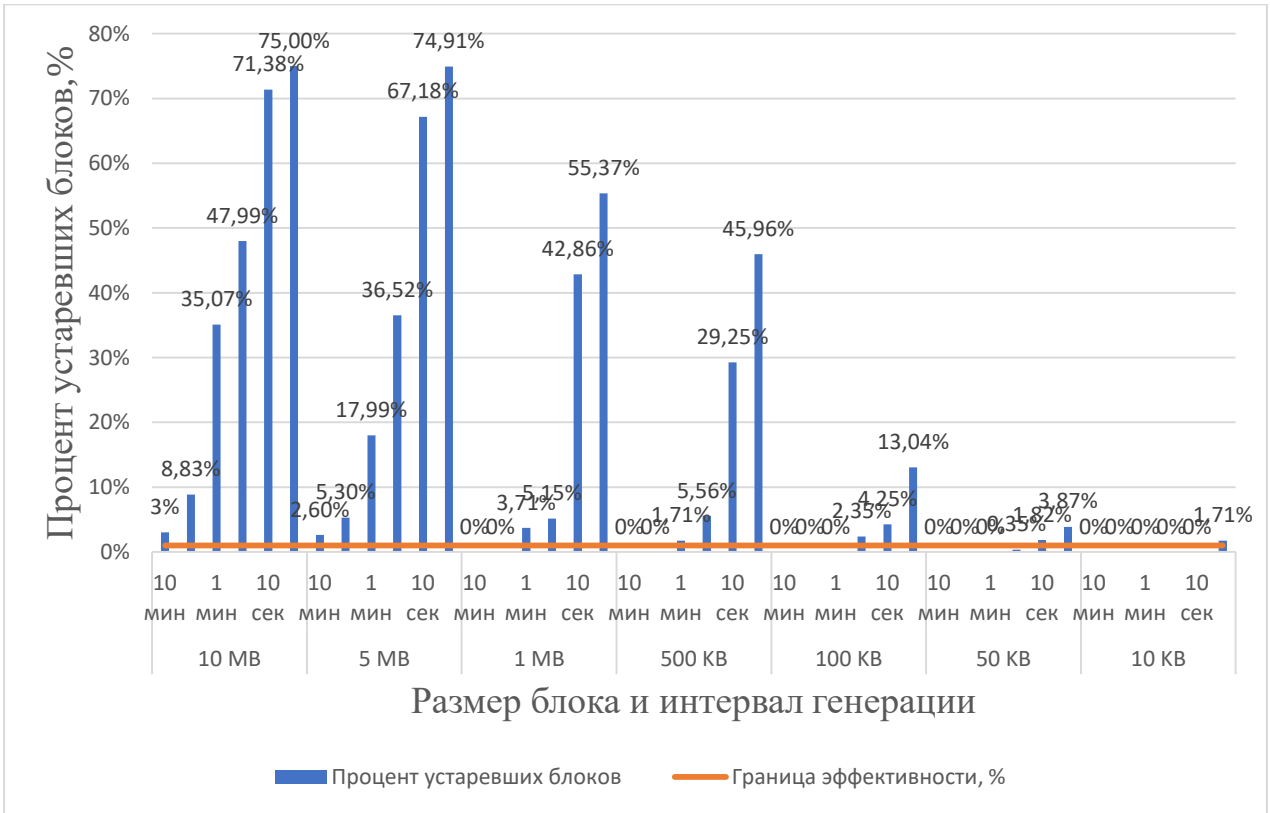

Рисунок 3.5 - Зависимость процента устаревших блоков от размера блоков и интервала генерации в логарифмической шкале

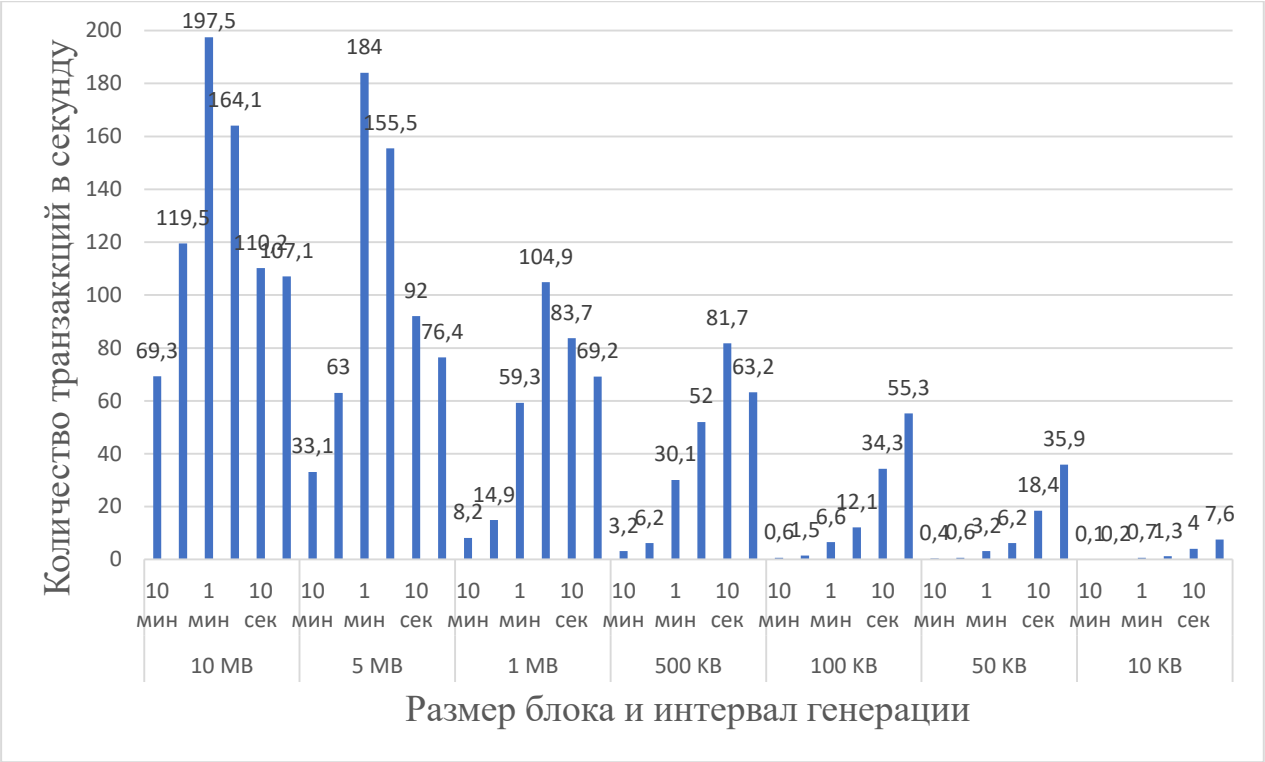

Рисунок 3.6 - Зависимость количества транзакций в секунду от размера блоков и интервала генерации

Пропускная способность сети. Очевидно, что использование больших блоков и/или короткие интервалы генерации блоков увеличивают среднее количество трафика сети. При этом большие блоки (например, 5 МБ) соответствуют ограничениям пропускной способности сети (250 kbps), когда интервал генерации блоков достаточно большой (например, 5 мин). Тогда как для небольших блоков (например, 10 КБ) подходят даже короткие интервалы генерации блоков (например, 5 с).

Безопасность. Очевидно, что использование более коротких интервалов генерации блоков увеличивает количество генерируемых блоков. Однако это не пропорционально, особенно когда размер блока больше 100 КБ. Точно так же в экспериментах с 1-минутной или более коротким интервалом генерации, увеличение размера блока уменьшает количество генерируемых блоков. Это связано с исчерпанием пропускной способности устройств. Следовательно, в соответствии с границами показателя безопасности использование небольших блоков (например, 10 КБ) с короткими интервалами генерации блоков (например, 5 с) является более подходящим для увеличения количества подлинных блоков.

Децентрализация. Согласно границам метрики децентрализации, время распространения блока на 90% узлов в сети должно быть меньше интервала генерации блока. Из-за ограниченных возможностей полосы пропускания устройствам IoT приходится тратить больше времени на распространение больших блоков, что, в свою очередь, нарушает ограничение времени

распространения блоков на 90%. Также можно заметить, что при использовании больших блоков (например, 10 МБ) интервал генерации блоков должен быть достаточно длинным (например, 10 м), чтобы удовлетворять нижней границе децентрализации. Например, когда используются небольшие блоки (например, 10 КБ), условие децентрализации может быть удовлетворено с более короткими интервалами генерации блоков (например, 5 с). Поэтому, чтобы добиться децентрализации, размеры блоков и интервалы генерации блоков должны быть тщательно подобраны.

Эффективность, масштабируемость. Короткие интервалы генерации блоков и/или использование больших блоков приводят к более высокому проценту устаревших блоков, поскольку полоса пропускания устройств IoT исчерпана при распространении блоков. Для достижения низкого процента устаревших блоков при установке короткого интервала генерации блоков можно использовать только небольшие блоки. Большие блоки (например, 1 МБ) могут использоваться с большими интервалами генерации блоков. Чем больше блок, тем длиннее интервал генерации блока должен использоваться для удовлетворения границы генерации блока с низким процентом устаревших блоков. Более того, размеры блоков больше 1 МБ не подходят для IoT. Достижение низкого процента устаревших блоков положительно влияет на пропускную способность транзакций. В экспериментах самая высокая достигнутая пропускная способность, с учетом заявленных требований, составляет 30,1 транзакции в секунду при использовании блоков по 500 КБ с настройкой интервала генерации блоков в 1 минуту с частотой устаревших блоков 1,71%.

Выводы: следует использовать блоки размером менее 1 МБ; интервалы генерации блоков должны быть как можно короче; размер блока и интервалы генерации блока должны быть установлены точно согласно расчётам, чтобы обеспечить низкий процент устаревших блоков и высокую децентрализацию.

3.3.4 Географическое расположение устройств.

Проведем оценку влияния расположения устройств, варьируя задержку в сети между устройствами IoT. Чтобы смоделировать это, используем симулятор с тремя настройками местоположения (внутри одной страны, Европа и Мир). Поскольку из оценки предыдущего моделирования оптимальный размер блока должен быть меньше или равен 1 МБ, размер блока в среднем составит 500 КБ. Используем цикл генерации из шести блоков со следующими интервалами: 10 минут, 5 минут, 1 минута, 30 секунд, 10 секунд и 5 секунд. Также увеличиваем количество устройств IoT до 250, где 16 из них являются майнерами. Результаты эксперимента представлены в таблице 3.5.

Для изменения топологии сети следует редактировать файл «src/applications/helper/bitcoin-topology-helper.cc», который содержит описание расположения всех элементов блокчейна.

Изменим топологию согласно задания:

std::array<double,7> nodesDistributionIntervals {KAZAKHSTAN, EUROPE, WORLD};

```
switch (m_cryptocurrency)
{
 case BITCOIN:
 {
  if (m_systemId == 0)
   std::cout << "BITCOIN Mode selected\n";
  std::array<double,6> nodesDistributionWeights {1, 0, 0};
```

Таким образом, меняя параметр nodesDistributionWeights, мы проведем несколько экспериментов.

Таблица 3.5 – Географическое расположение устройств

Интервал генерации блоков	Масштаб	Всего блоков	Устаревшие блоки	Подлинные блоки	Доля устаревших блоков, %	Задержка распространения	Ср. утилизация, kbps	Кол-во транзакций в сек.
10m	Страна	9,6	0	9,6	0	7	13	3,2
	Европа	9,9	0	9,9	0	16	13	3,3
	Мир	9,9	0	9,9	0	20	13	3,3
5m	Страна	18,6	0	18,6	0	6	26	6,2
	Европа	16,4	0	16,5	0	13	27	5,5
	Мир	15,5	0	15,5	0	17	27	5,2
1m	Страна	92,1	1,6	90,5	1,71	17	136	30,1
	Европа	93,6	4,8	88,8	5,14	18	140	29,6
	Мир	96,5	7,9	88,6	8,22	20	140	29,5
30s	Страна	165,2	9,2	156	5,56	18	639	52
	Европа	170,5	21,9	148,6	12,87	38	527	49,5
	Мир	169,5	23,9	145,6	14,11	52	592	48,5
10s	Страна	346,6	101,4	245,2	29,25	314	14762	81,7
	Европа	314	104,6	209,4	33,31	355	15237	69,8
	Мир	331	136,8	194,2	41,34	392	16777	64,7
5s	Страна	350,7	161,2	189,5	45,96	815	41378	63,2
	Европа	301,2	156	145,2	51,80	918	43931	48,4
	Мир	303,3	161,1	142,2	53,12	1000	45021	47,4

Исходя из требований, указанных в таблице 3.3, построим графики зависимости процента устаревших блоков (рисунок 3.7) и количества транзакций (рисунок 3.8) от размера блоков и интервала генерации и проведем дальнейший анализ.

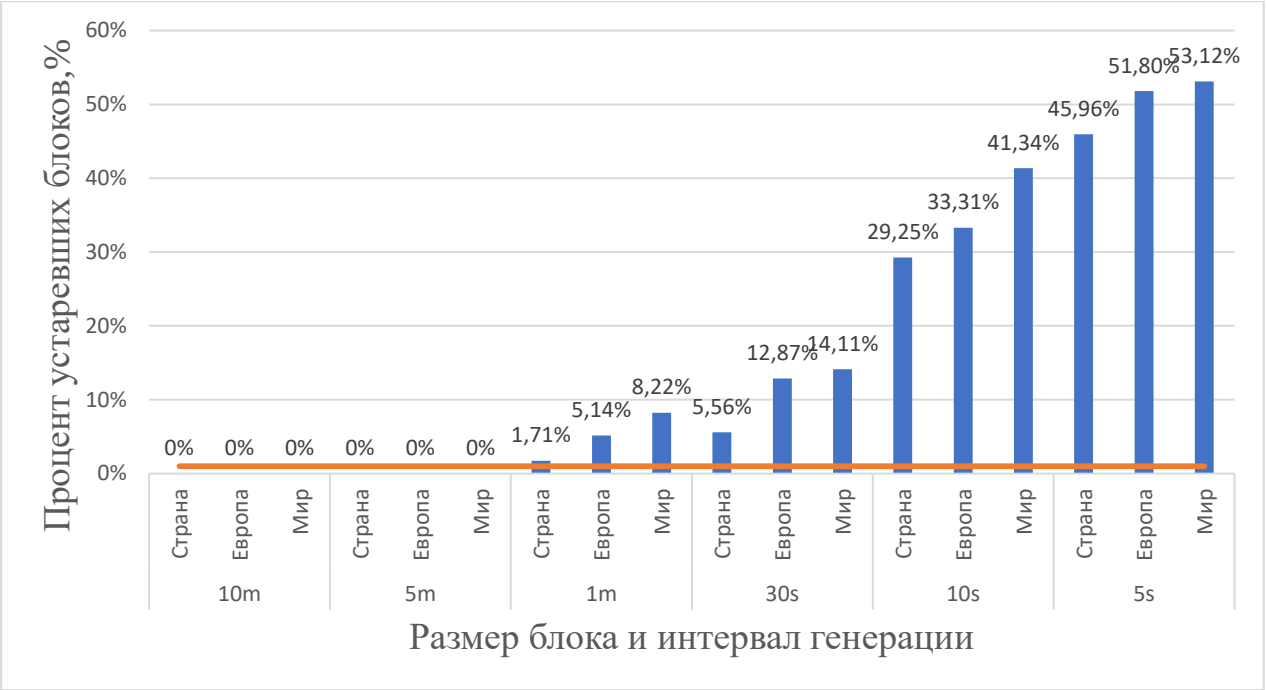

Рисунок 3.7 - Зависимость процента устаревших блоков от сетевой задержки между узлами и интервала генерации в логарифмической шкале

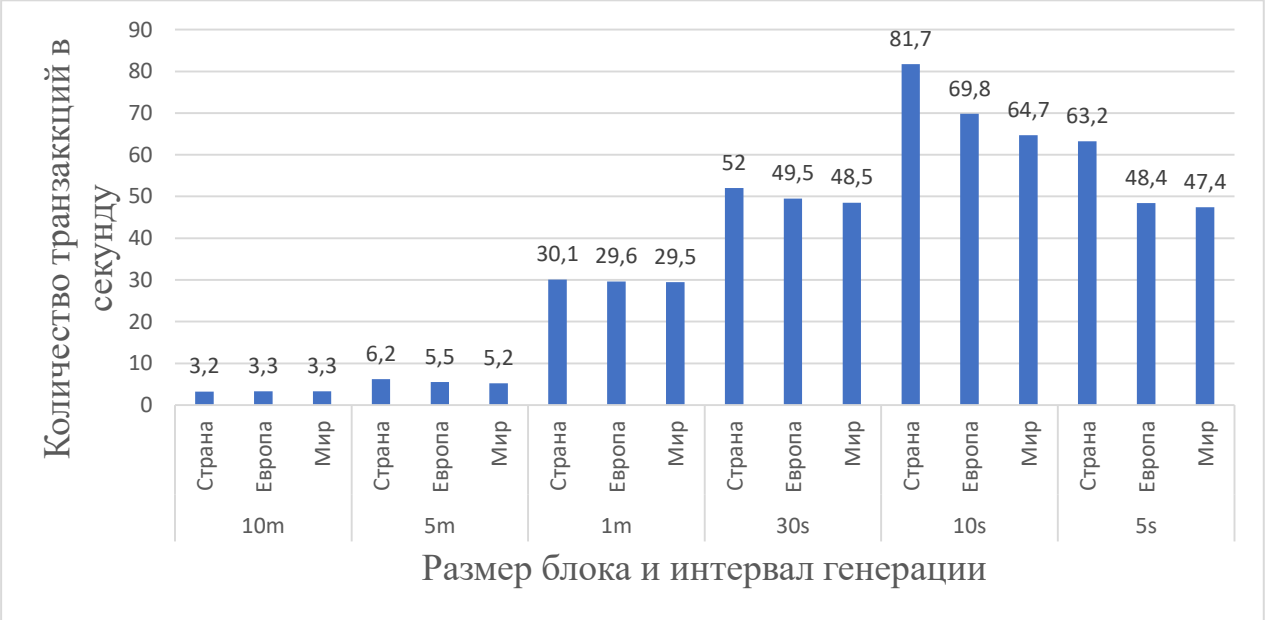

Рисунок 3.8 - Зависимость количества транзакций в секунду от сетевой задержки между узлами и интервала генерации в логарифмической шкале

Пропускная способность сети, безопасность. Для всех местоположений, в каждом интервале генерации блока утилизация пропускной способности на каждое устройство и количество сгенерированных подлинных блоков коррелируют между собой. В частности, только частота генерации блоков в 1 минуту или более может быть использована т.к. только эти интервалы

соответствуют ограничению для пропускной способности сети (250 Кбит/с) для всех вариаций местоположения. Следовательно, 1-минутный интервал генерации блока является наиболее подходящим с точки зрения безопасности, поскольку он имеет наибольшее количество подлинных блоков.

Масштабируемость, децентрализация, эффективность. Для любой симуляции, результат с самыми короткими задержками распространения блоков, самыми низкими процентами устаревших блоков и самыми высокими пропускными способностями транзакций будет получен при тесте внутри страны. Например, с интервалом генерации блока в 1 минуту блок-схема PoW с использованием настройки внутри страны достигает пропускной способности 30,1 в секунду и соответствует метрики эффективности (скорость устаревания блока составляет 1,71%) и метрики децентрализации (время распространения блока 90% составляет 17 секунд). Для сравнения в тестах Европы и Мира интервал генерации блока должен составлять не менее 5 минут, чтобы соответствовать тем же характеристикам.

Выводы: блокчейны, содержащие устройства IoT, которые географически близки друг к другу, обеспечивают более высокую пропускную способность при низкой скорости устаревания блоков.

3.3.5 Количество устройств IoT в одном блокчейне.

Проведем два измерения для оценки оптимального количества IoT устройств в одном блокчейне с переменными и фиксированным интервалом генерации блоков. В обоих тестах варьируем количество устройств IoT от 83 до 1250 и принимаем размер фиксированного блока 500 КБ. В блокчейне PoW интервал генерации блоков зависит от отношения сложности головоломки PoW к суммарной мощности майнинга системы [2]. Следовательно, с уменьшением сложности PoW задачи меняем интервалы генерации блоков обратно пропорционально количеству майнеров. В другом измерении, с фиксированным интервалом генерации блоков, равным 1 минуте, сложность головоломки PoW варьируется пропорционально количеству майнеров (сложность головоломки PoW составляет α для 6 майнеров и 15α для 90 майнеров).

Данная задача выполняется путем выставления параметров:

- «--blockSize» статически равным 500000;
- «--nodes» в диапазоне от 83 до 1250;
- «--blockIntervalMinutes» в диапазоне от 0,2 до 3;
- «--miners» в диапазоне от 6 до 90.

Пример симуляции данного эксперимента приведен на рисунке 3.9.

Эксперимент (A). Результаты приведены в таблице 3.6.

```
mpbn@pav-mirroring-srv:~/workspace/ns-allinone-3.25/ns-3.25$ sudo ./waf --run "bitcoin-test
--blockIntervalMinutes=1 --nodes=250 --blockSize=500000 --miners=16"
/////
Часть вывода удалена
////
Total Stats:
Average Connections/node = 10.6282
Average Connections/miner = 164.938
Mean Block Receive Time = 59.8417 or 0min and 59.8417s
Mean Block Propagation Time = 8.3892s
Median Block Propagation Time = 6.20544s
10% percentile of Block Propagation Time = 3.62249s
25% percentile of Block Propagation Time = 4.37992s
75% percentile of Block Propagation Time = 7.89761s
90% percentile of Block Propagation Time = 16.9018s
Miners Mean Block Propagation Time = 5.09388s
Miners Median Block Propagation Time = 5.61457s
Mean Block Size = 500000 Bytes
Total Blocks = 92.1
Stale Blocks = 1.6 (1.71%)
The size of the longest fork was 1 blocks
There were in total 5.984 blocks in forks
/////
Часть вывода удалена
////
Total average traffic/node = 1.03401e+08 Bytes (136.139 Kbps and 1036.04 KB/block)
2.44119s per generated block
```

Рисунок 3.9 – Пример отчета симулятора для эксперимента (А)

Таблица 3.6 – Количество устройств в одном блокчейне при переменном интервале генерации блоков

Кол-во майнеров/узлов	Интервал генерации блоков	Всего блоков	Устаревшие блоки	Подлинные блоки	Доля устаревших блоков, %	Задержка распространения	Ср, утилизация, kbps	Кол-во транзакций в сек,
6/83	3 мин	29,9	0	29,9	0	7	44	9,9
12/166	1,5 мин	76,7	1,3	75,4	1,9	8	88	25,1
16/250	1 мин	92,1	1,6	90,5	1,71	17	136	30,1
36/500	30 сек	177,7	15,6	162,1	8,8	41	1168	54
54/750	20 сек	237,2	32,9	204,3	13,87	147	3485	68,1
72/1000	15 сек	216,5	39,4	177,1	18,2	291	5791	59
90/1250	12 сек	212	47,5	164,5	22,43	498	8265	54,8

Наличие большего количества IoT-устройств с более короткими интервалами генерации блоков приводит к генерации большего количества блоков, что ведет к увеличению пропускной способности и количества сетевого трафика на устройство. Это приводит к значительному потреблению полосы пропускания, что приводит к длительным задержкам распространения блоков. Следовательно, экспериментальные варианты, содержащие 83, 166 и 250 устройств, удовлетворяют эффективности, пропускной способности сети и границам децентрализации. Когда речь заходит о масштабируемости и границах безопасности, сценарий, содержащий 250 устройств, является оптимальным, поскольку он генерирует высокий процент подлинных блоков,

достигает максимальной пропускной способности и масштабируется для большего количества устройств.

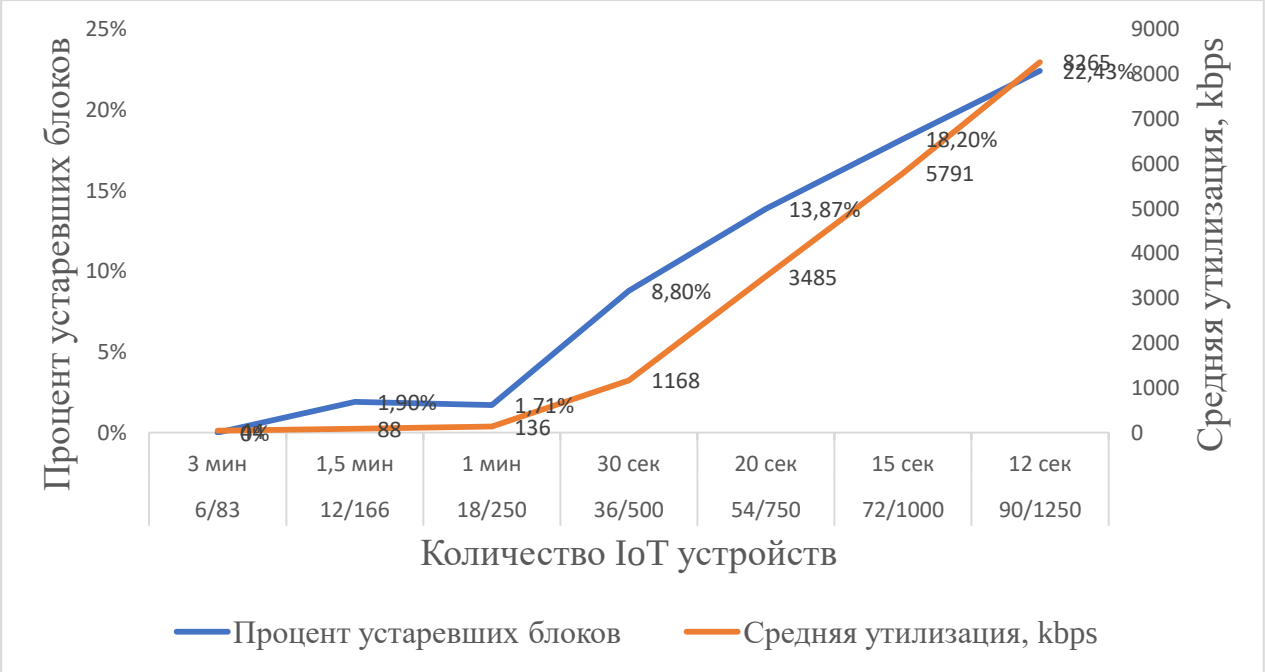

Рисунок 3.10 – Зависимость процента устаревших блоков и средней утилизации от количества IoT устройств в логарифмической шкале

Эксперимент (Б). Результаты приведены в таблице 3.7.

Таблица 3.7 – Количество устройств в одном блокчейне при постоянном интервале генерации блоков

Кол-во майнеров/узлов	Всего блоков	Сложность	Устаревшие блоки	Подлинные блоки	Доля устаревших блоков, %	Задержка распространения	Ср. утилизация, kbps	Кол-во транзакций в сек.
6/83	96,1	α	0,8	95,3	0,85	13	135,76	31,7
12/166	96,3	2α	1,8	94,5	1,19	14	133,37	31,1
18/250	92,1	3α	1,6	90,5	1,71	17	136	30,1
36/500	93,03	6α	3,99	89,04	4,29	26	122,99	32,86
54/750	93,41	9α	4,49	88,92	4,8	28	102,03	29,64
72/1000	93,03	12α	4,42	88,61	4,75	28	102,99	29,53
90/1250	92,77	15α	4,98	87,78	5,36	39	107,01	29,26

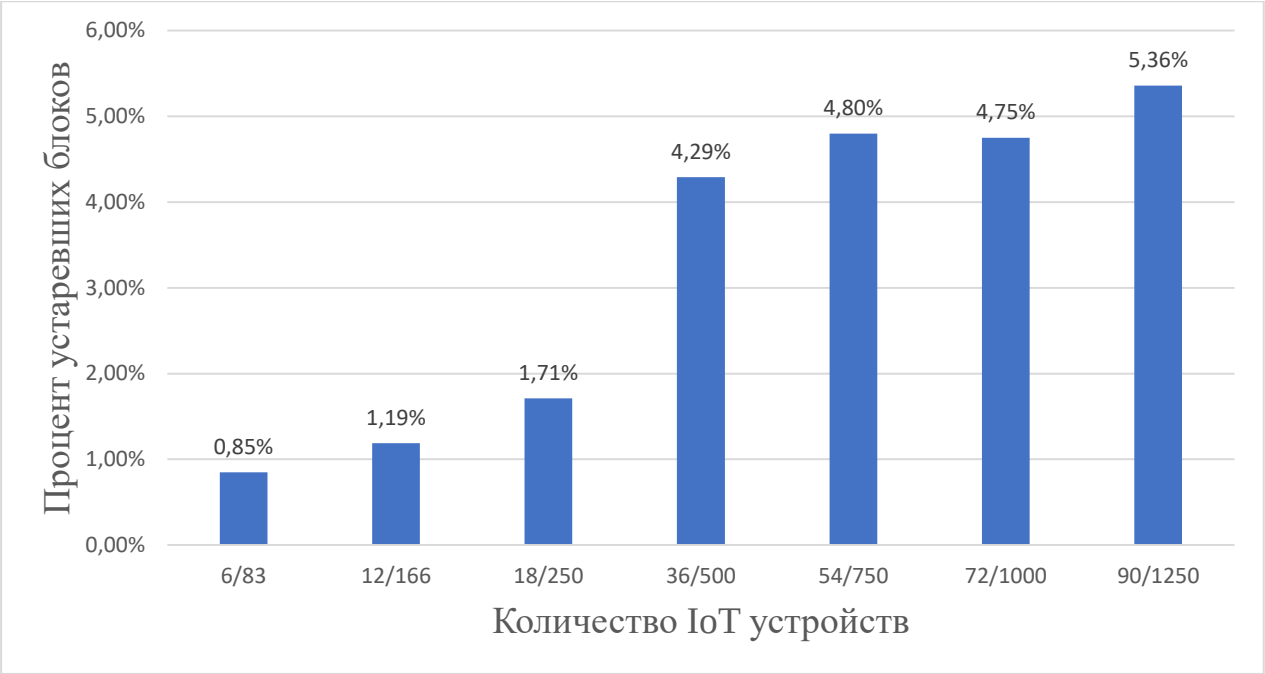

Рисунок 3.11 – Зависимость процента устаревших блоков от количества IoT устройств в логарифмической шкале

Во всех экспериментальных вариациях 90% времени распространения блока составляют интервал генерации блока менее 1 минуты, что соответствует границе децентрализации. Для всех вариантов соблюдается условие по ограничению пропускной способности в 250 кбит/с, однако только экспериментальные варианты, содержащие 83, 166 и 250 устройств, удовлетворяют эффективности, связанной с частотой устаревания блоков. Среди них эксперимент с 250 устройствами является оптимальным в соответствии с границами безопасности и масштабируемости, поскольку он обеспечивает максимальную пропускную способность и масштабируется на большее количество устройств.

Выводы: блокчейны PoW, содержащие несколько сотен IoT-устройств, обеспечивают более высокую пропускную способность транзакций; оптимальное количество IoT-устройств составляет около 250.

Заключение

В ходе выполнения исследования был проведен анализ современных алгоритмов распределённого хранения и обработки данных. Рассмотрены преимущества блокчейна перед существующими системами хранения данных, приведены основные технологии, используемые на данный момент и дана классификация систем. Также выделены основные ограничения технологии: проблемы безопасности, проблемы масштабирования и скорости обработки данных, высокие требования к ресурсам, поиск новых областей применения.

Рассматривая проблемы, как основные сферы для исследования и опираясь на рыночное состояние технологии в целом, был проведен анализ применения алгоритмов распределённого хранения в области IoT, здравоохранения и электронного голосования. Проведен анализ существующих концепций и протоколов использования блокчейна для гарантирования честности в проведении выборов.

Выделены основные риски, связанные с IoT и передачей конфиденциальных данных через сети передачи данных, в частности, Интернет. Основными проблемами считаются: безопасность данных, доверие к сети, контроль открытых подключений. Как следует из анализа большинство рисков можно снизить с применением алгоритмов распределенного хранения данных. Было проведено исследование влияния блокчейна на каждую из важнейших характеристики IoT сети: масштабируемость, безопасность, децентрализацию, эффективность, пропускную способность сети.

В качестве среды моделирования был выбран сетевой симулятор NS3 вместе с фреймворком Bitcoin Simulator. В результате произведенных измерений было выявлено, что блокчейны PoW, содержащие несколько сотен устройств IoT в непосредственной географической близости, достигают наивысшей производительности. Поэтому, чтобы спроектировать архитектуру блокчейна для IoT, предлагается развернуть множество субблокчейнов PoW для группы устройств IoT, включая следующие рекомендации:

– субблокчейны должны содержать несколько сотен IoT-устройств;

– субблокчейны должны содержать устройства IoT, которые географически близки и часто обмениваются данными друг с другом;

– размер блока и интервалы генерации блока должны быть установлены для обеспечения низкого процента устаревших блоков, а также высокой децентрализации;

– блоки должны быть меньше или равны 1 МБ;

– интервал генерации блока должен быть как можно короче.

Проведенное исследование показало высокую эффективность использования алгоритмов распределенного хранения и обработки данных в IoT.

Список литературы

1 Haber S., Stornetta W., How to Time-Stamp a Digital Document. -New Jersey: Bellcore South Street Morristown, 1991.

2 Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System // [bitcoin.org] -2008. URL: https://bitcoin.org/bitcoin.pdf (дата обращения:23.05.2020).

3 Tapscott D., Tapscott A. Blockchain revolution. - Portfolio, 2016.

4 World Bank Group Distributed Ledger Technology (DLT) and Blockchain, // Open knowledge World Bank Repository. - 2017. URL: https://openknowledge .worldbank.org/bitstream/handle/10986/29053/WP-PUBLIC-DistributedLedger-Technology-and-Blockchain-Fintech-Notes.pdf?sequence=1 (дата обращения: 23.05.2020).

5 Seebacher S., Schüritz R. Blockchain technology as an enabler of service systems: A structured literature review. // International Conference on Exploring Services Science: Springer. - 2017.

6 Antonopoulos M. Mastering Bitcoin: Programming the Open Blockchain. - O'Reilly Media, Inc., 2017.

7 Yli-Huumo J, Ko D., Choi S., Park S., Smolander K. Where Is Current Research on Blockchain Technology? — A Systematic Review. // PLoS ONE 11(10), 2016.

8 Beikverdi A., Song J. Trend of centralization in Bitcoin's distributed network. // Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 16th IEEE/ACIS International Conference on. 2015.

9 OECD Digital Economy Outlook. // OECD Publishing. - 2017. URL: http://dx.doi.org/10.1787/9789264276284-en. (дата обращения:23.05.2020).

10 World Energy Council The Developing Role of Blockchain. White Paper. Version 1.0. -Pwc, 2017.

11 Jayachandran P. The difference between public and private blockchain. // [IBM] - 2017. URL: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-privateblockchain/. (дата обращения:23.05.2020).

12 Blockchain Hub Blockchains & Distributed Ledger Technologies // [blockchainhub.net] - 2018. URL: https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/. (дата обращения:23.05.2020).

13 Vukoli´c M. The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. -English, 2017. -112–125 с.

14 Baliga A. Understanding blockchain consensus models. -Persistent, 2017.

15 V. Buterin A proof of stake design philosophy. // [medium.com] - 2017. URL: https://medium.com/@VitalikButerin/aproof-of-stake-design-philosophy-506585978d51. (дата обращения:23.05.2020).

16 Szabo N. Smart Contracts // fon.hum.uva.nl - Phonetic Science, Amsterdam – 1994. URL: www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/

Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (дата обращения: 23.05.2020).

17 Murphy S., Cooper C. Can Smart Contracts Be Legally Binding Contracts // Norton Rose Fulbright. - 2016. URL: http://www.nortonrosefulbright.com/files/r3-andnorton-rose-fulbright-white-paper-full-report-144581.pdf (дата обращения: 23.05.2020).

18 Gartner Hype Cycle Shows Most Blockchain Technologies Are Still Five to Years Away From Transformational Impact. // Gartner. - 2019. URL: https://www.gartner.com/en/newsroom/press-releases/2019-10-08-gartner-2019-hype-cycle-shows-most-blockchain-technologies-are-still-five-to-10-years-away-from-transformational-impact (дата обращения:23.05.2020).

19 Нугманов Д.М., Лещинская Э.М. Повышение конфиденциальности и безопасности данных в сети IoT с помощью алгоритмов децентрализованного хранения и обработки данных // Поиск.- 2019.- №3(1). С. 279-283.

20 Тихвинский В.О., Бочечка Г.С., Нургожин Б.И., Айтмагамбетов А.З. Сети IoT/M2M: технологии, приложения и регулирование. Изд. «АК-Шагыл».- Алматы, 2016.

21 Newsroom G. Gartner Says Worldwide IoT Security Spending Will Reach $1 Billion in 2018 // Gartner. - 2017. URL: https://www.gartner.com/newsroom/id/ (дата обращения:23.05.2020).

22 The Internet of Things: a movent, not a market // IHS Markit. - 2018. URL: http://cdn.ihs.com/www/pdf/IoT_ebook.pdf (дата обращения:23.05.2020).

23 Zhang P., Schmidt D., White J., Lenz G., Blockchain technology use cases in healthcare. In Advances in Computers. Amsterdam: -Elsevier, 2018. -1–41c.

24 Chiuchisan, I., Costin, H., Geman, O. Adopting the internet of things technologies in health care systems. // International Conference and Exposition on Electrical and Power Engineering, Iasi, Romania. 16 Октября 2014. – С -532 с.

25 Lobato F. Decentralized, Transparent, Trustless Voting on the Ethereum Blockchain. // International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056. - 2017.

26 Thomas R., Mathieu L., Riley G. Network simulations with the ns-simulator. // SIGCOMM. - 2008. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.415.6550&rep=rep1&type=pdf (дата обращения: 24.05.2020)

27 Балашов В. Обзор сетевого симулятора NS3 // Харьковский Исследовательский Институт Судебных Экспертиз им. заслуженного профессора Н. Бокариуса. - 2010. URL: https://lvee.org/ru/reports/LVEE_2010_31 (дата обращения:24.05.2020).

28 Karame G., Androulaki E., Capkun S. Double-spending fast payments in bitcoin. // ACM conference on Computer and communications security. - 2012. - С.906–917.

29 Blockchain Explorer. Search the tour Blockchain. // [blockchain.info]-2010. URL: blockchain.info (дата обращения:12.04.2020).

30 Miller A. Discovering bitcoin’s public topology and influential nodes // University of Maryland. - 2015. URL: https://www.cs.umd.edu/projects/coinscope/coinscope.pdf (дата обращения:12.04.2020).