**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
**«Сибирский государственный университет науки и технологий  
имени академика М.Ф. Решетнева»**

**Институт информатики и телекоммуникаций  
Кафедра ИВТ**

**РЕФЕРАТ**

по информационным технологиям «Блокчейн»

Преподаватель ст. пр. кафедры ИВТ Кагиров Р. Р.   
 подпись, дата инициалы, фамилия

Обучающийся БПИ22-02, 221219040 Трифонов К.В.

Номер группы, зачетной книжки подпись, дата инициалы, фамилия

Красноярск 2023

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 3](#_Toc152533071)

[1 ИСТОРИЯ ПОЯВЛЕНИЯ И ПОНЯТИЕ БЛОКЧЕЙНА 4](#_Toc152533072)

[2 ПРИНЦИП РАБОТЫ ТЕХНОЛОГИИ БЛОКЧЕЙН 4](#_Toc152533073)

[3 ХАРАКТЕРНЫЕ ЭЛЕМЕНТЫ БЛОКЧЕЙН 5](#_Toc152533074)

[4 СУТЬ БЛОКОВ И ИХ МАЙНИНГА 6](#_Toc152533075)

[5 ПРИМЕНЕНИЕ В ЦЕНТРАХ ОБРАБОТКИ ДАННЫХ 7](#_Toc152533076)

[ЗАКЛЮЧЕНИЕ 9](#_Toc152533077)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 10](#_Toc152533078)

# ВВЕДЕНИЕ

Использование блокчейна в центрах обработки данных, colocation и IaaS предоставляет эффективные решения для майнинга и различных блокчейн-приложений. Проекты, такие как Storj, демонстрируют применение блокчейна в создании безопасных распределенных облачных хранилищ. Большие IT-компании, включая Microsoft, активно интегрируют технологию блокчейна в свои сервисы, предоставляя множественные средства разработки.

Цель данной работы исследование понятия блокчейна, истории и основных принципах технологии, а также применении в современном мире.

Для её достижения были поставлены следующие задачи:

- изучить историю появления и понятие блокчейна

- узнать принцип работы технологии

- обозначить характерные элементы

- исследовать суть блоков и их добычи

- определить применение в центрах обработки данных

Актуальность: блокчейн обеспечивает безопасность и прозрачность в цифровых транзакциях, что крайне важно в условиях растущей цифровой экономики. Его использование в финансовой сфере, управлении цифровыми активами, а также в обеспечении цифровой безопасности становится все более распространенным.

# 1 ИСТОРИЯ ПОЯВЛЕНИЯ И ПОНЯТИЕ БЛОКЧЕЙНА

В книге Блокчейн от А до Я [1, c. 26] автор Лоран Л. пишет про историю биткоина: **«**Первоначально биткойн являлся улучшением концепции b-money (придуманной Вэй Даем в 1999 году, в которой серверы должны были внести гарантийный взнос в нечетко раскрытый механизм) и технологии bitgold (описанной в 2005 году Ником Сабо и продвигавшей идею использования доказательств на основании расчетов).»

Также Генкин А., Михеев А. в книге Блокчейн: как это работает и что нас ждёт завтра [4, с. 18] пишут следующую историческую справку: «Основы криптовалюты были заложены в 1992 году киберпанками – неформальной группой людей, заинтересованных в сохранении анонимности и интересующихся криптографией. Об обеспечении конфиденциальности совершаемых в современном обществе платежных операций путем их многоэтапного шифрования одним из первых заявил в 1993 году американский программист Эрик Хьюз. В 1994-м американский ученый и инженер из корпорации Intel Тимоти Мэй в статье «Вопросы и ответы о криптопанке» (The Cyphernomicon) описал основные характеристики такой системы, в том числе безопасность неотслеживаемых транзакций через их шифрование, а также транзакции, проводимые без посредников. Для реализации этих идей надо было создать новый механизм расчетов, не затрагивающий банковский сектор.»

Лоран Л. [1, с. 31] приводит определение термина: «Термин «биткойн» происходит от сокращения двух английских слов: bit – единица информации в двоичном коде и coin – монета. Биткойн одновременно обозначает информационный протокол (биткойн) сети Интернет и единицу расчетов (биткойн), используемую в этой платежной системе.»

В свою очередь Федотова В.В. [2, с. 2] приводит определение: «Блокчейн (англ. «blockchain», «block» – блок, «chein» – цепь) – это распределенная база данных, состоящая из «цепочки блоков», устройства хранения блоков не подключены к общему серверу, база данных позволяет контролировать достоверность транзакций без надзора каких-либо финансовых регуляторов.»

# 2 ПРИНЦИП РАБОТЫ ТЕХНОЛОГИИ БЛОКЧЕЙН

О принципе работы блокчейн технологии пишет автор статьи Блокчейн и облака [3] Носов Н.: «Пользователь может выполнять роль как обычного участника, создающего записи, например о денежных переводах, так и майнера, который собирает записи пользователей, проверяет, формирует блоки и рассылает всем участникам сети. Участники сети проверяют созданный блок, после чего он становится подтвержденным, занимает свое место в цепочке, и следующий блок должен будет включать в себя его хеш (ключ).

Деление на майнеров и простых участников часто достаточно условно. Во многих случаях любой участник блокчейн-сети может быть майнером.

Как следует из названия технологии, в ее основе лежит цепочка последовательно связанных блоков. Новые блоки всегда добавляются строго в конец цепочки. Все блоки можно выстроить в одну цепочку, которая содержит информацию о всех совершенных когда-либо операциях. Блок состоит из заголовка и списка транзакций (тела). Заголовок блока включает в себя свой хеш, хеш предыдущего блока, хеши транзакций и дополнительную служебную информацию.»

К сведению Генкин А., Михеев А. пишут в своей книге [4, с. 37]: «Некоторые эксперты в описании блокчейна прибегают к красочным сравнениям: «Это технология хранения данных, прав и обязательств, защищенная математическими правилами так, что никто посторонний не может завладеть ими. Права на вашу собственность не смогут украсть, подделать или удалить. Иными словами, блокчейн – это как бы параллельная реальность типа SWIFT на международном уровне. Напомним, что SWIFT играет роль посредника: если я хочу сделать трансграничный перевод, я это сделаю через SWIFT, который гарантирует, что знает банк, который переводит, знает банк, которому переводят, и тем самым выступает в качестве посредника-гаранта. И в этом смысле блокчейн может также рассматриваться как своеобразный "СВИФТ"93».»

# 3 ХАРАКТЕРНЫЕ ЭЛЕМЕНТЫ БЛОКЧЕЙН

Основную структуру блокчейн технологии выделяют в своей книге Генкин А., Михеев А. [4, с.39]: «Итак, какие же элементы характерны для блокчейна в целом?

• Блокчейн в цифровой форме распределяется по множеству компьютеров практически в режиме реального времени: он децентрализован, и копия всей записи доступна всем пользователям и участникам одноранговой сети. Это избавляет от необходимости иметь централизованные уполномоченные органы, такие как банки, а также доверять посредникам, таким как брокерские фирмы.

• Для достижения консенсуса блокчейн использует множество участников сети: они задействуют свои компьютеры, чтобы аутентифицировать и проверить каждый новый блок – например, чтобы гарантировать, что какая-либо одна транзакция не пройдет несколько раз. Новые блоки принимаются сетью, как только большинство ее участников соглашаются, что они допустимы.

• Блокчейн использует криптографию и цифровые подписи для удостоверения личности: транзакции прослеживаются вплоть до криптографических идентификационных данных, которые теоретически анонимны, но могут быть прикреплены к реальным идентификационным данным после некоторого инженерного анализа.

• У блокчейна есть механизмы, благодаря которым сложно (но не невозможно) изменять хронологические записи: даже при том, что блокчейн позволяет считывать все данные и добавлять новые, те записи, которые уже существуют, теоретически не поддаются исправлению, кроме тех случаев, когда встроенные в протокол правила позволяют изменения – например, если более 50 % участников сети договорятся об этом.

• К транзакциям, основанным на блокчейне, добавляется метка времени, что делает удобным отслеживание и проверку информации.

• Блокчейн программируем: инструкции встроены в блоки, это позволяет выполнять транзакции или иные действия только при соблюдении определенных условий и может сопровождаться дополнительными цифровыми данными.»

# 4 СУТЬ БЛОКОВ И ИХ МАЙНИНГА

Автор Генкин А., Михеев А. в книге Блокчейн: как это работает и что нас ждёт завтра [4, с. 37] дают определяет применение блоков в блокчейне: «Блоки генерируются через общедоступное программное обеспечение и содержат информацию о том, когда и в какой последовательности совершались транзакции. Один блок в хронологическом порядке хранит информацию обо всех сделках, которые имели место в цепочке, отсюда и название blockchain. Другими словами, блокчейн – это база данных неизменной информации с меткой времени о каждой транзакции, которая растиражирована на серверах по всему миру. Эта технология лежит в основе криптовалюты биткоин.»

Также Носов. Н в своей статье [3] определяет задачи добытчиков биткоина: «Задача майнера – вычислить эту служебную информацию. Сложность вычисления специально заложена в алгоритм. При этом ищется компромисс между сложностью расчета, которая обеспечивает безопасность сети, и скоростью проведения транзакций. Например, в биткойне предусматривается, что вся сеть будет тратить на генерацию одного блока примерно 10 минут. И быстрее не получится, так как расчет производится перебором. По сути, майнер за подтверждение блока платит используемой им вычислительной мощностью.

Пусть требование к сложности таково, что хеш блока должен начинаться с десяти нулей. И вот, предположим, майнер рассчитал хеш нового блока – 9675346595423570985008687907853269984665640589182146373136543. Чтобы выполнить требование о десяти нулях, майнер методом перебора меняет специальное поле (nonce) в заголовке блока до тех пор, пока не получит результат типа 0000000000423570985008687907853269984665640589182146373136543.»

Помимо этого Лоран Л. в своей книге [1, с. 36] даёт определение майнингу: «Майнинг – это протокол распределенного и децентрализованного консенсуса, заключающийся в дешифровке данных или математических вычислений (именно поэтому и говорят о криптовалюте или криптодевизах, так как для того, чтобы их произвести, необходимо пройти процесс дешифровки).»

«Этот процесс предполагает, что отдельные люди будут вознаграждены сетью за свои услуги. Майнеры обрабатывают транзакции и обеспечивают безопасность сети с помощью специализированного оборудования, а в обмен получают новые биткойны.»

В дополнение к этому, Лоран Л. объясняет сложности добычи криптовалюты [1, с. 42]: «В теории все в мире могут быть майнерами, так было при запуске блокчейна. Но на практике при экспоненциальном увеличении числа транзакций майнинг – занятие для предприятий, в основном базирующихся в регионах, где стоимость электроэнергии ниже.

В блокчейне биткойн блок в настоящее время содержит 1000 транзакций с ограничением на размер в 1 мегабайт (средний размер блоков колеблется между 600 и 700 Кб), или около семи транзакций в секунду. Когда майнер собирается подтвердить блок транзакций, он получает 25 новых биткойнов, которые создаются каждые десять минут.

В блокчейне биткойн, существующем с января 2009 года, наградой за решение блока было от 50 биткойнов, но она автоматически уменьшалась в два раза каждые 210 тысяч блоков (около четырех лет): сегодня майнеры получают 12,5 биткойнов за блок с 2021 года 6,75 ВТС и т. д.»

# 5 ПРИМЕНЕНИЕ В ЦЕНТРАХ ОБРАБОТКИ ДАННЫХ

Носов Н. в своей статье [3] определяет следующее применение ЦОД для блокчейн: «Логично предположить, что сер­висы colocation и IaaS можно использовать для майнинга. Подтверждение вычислительной мощностью по-прежнему является самым популярным способом подтверждения правильности блоков. И не важно, для чего используется майнинг – для криптовалют, типа биткойна, для защищенного электронного документооборота или ведения реестров. Важно, что спрос на вычислительные мощности есть. И это, конечно, может быть интересным для ЦОДов.

В ЦОДах могут устанавливаться специализированные компьютеры для майнинга по модели colocation или же майнеры могут задействовать вычислительные мощности ЦОДа по модели IaaS. Сейчас половина мирового майнинга осуществляется в Китае. Однако в этой сфере у нас есть немалые конкурентные преимущества. Это низкая стоимость электроэнергии в восточных районах страны, которая в пять раз ниже китайской, и низкая среднегодовая температура, уменьшающая затраты на охлаждение. Если добавить к этому проблемы, вызванные «Великим китайским файрволом», то наши ЦОДы могут оказаться привлекательными даже для китайских майнеров.»

Также Генкин А., Михеев А в своей книге [4, с. 65] пишут о многочисленности облачных услуг в сфере блокчейн: «Компании Deloitte (с Rubix), Eris Industries и AlphaPoint (со StreamCore) продают готовые решения для приватных блокчейнов непосредственно бизнесу. Есть также Microsoft, которая начала предлагать «Блокчейн как услугу» (BaaS) и приватные блокчейн-узлы, сформированные как шаблоны быстрого запуска в облачном сервисе Azure. Развивать блокчейн-узлы, и публичные и приватные, с элементами Azure чрезвычайно просто, таким образом теперь становится возможным тестирование блокчейна и внедрение его «за час». Наконец, существует вариант приватного блокчейна, который просто разворачивается на рабочем столе компьютера посредством MultiChain. Все это позволяет быстро решать вопросы дизайна, установки и работы приватных блокчейнов с учетом пользовательской специфики бизнеса.

И это мы еще не говорим о больших проектах подающих надежды блокчейн-консорциумов и о собственном решении SWIFT. Однако вполне вероятно, что один из консорциумов в будущем сможет, используя свой приватный блокчейн, занять ведущее место на основных направлениях финансового рынка.

Одно можно сказать наверняка: чем шире распространяется частный блокчейн, тем более вероятно, что регулирующие его правила будут изменены.»

# ЗАКЛЮЧЕНИЕ

В заключение, блокчейн-технология представляет собой инновационное решение, находящее применение в различных областях, включая центры обработки данных, colocation и IaaS. Большие IT-компании, в том числе Microsoft, активно интегрируют блокчейн в свои сервисы, предоставляя разнообразные средства разработки. Преимущество блокчейн-технологии проявляется в ее способности обеспечивать безопасность и прозрачность в цифровых транзакциях, что является важным аспектом в условиях растущей цифровой экономики. В центрах обработки данных блокчейн может быть успешно использован для майнинга, а его применение в colocation и IaaS открывает новые перспективы для оптимизации бизнес-процессов.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Лоран Л. Блокчейн от А до Я. Все о технологии десятилетия / Groupe Eyrolles, Paris, France: Степанова А.Н., перевод на русский язык: Оформление. ООО «Издательство «Эксмо», 2018. – 175 с.
2. Федотова В.В. Понятие блокчейн и возможности его использования: научная статья / Федотова В.В., Емельянов Б.Г., Тинпер Л.М. – Екатеринбург: Уральский федеральный университет им. Б.Н. Ельцина, 2018. – 9 с.
3. Носов Н.В. Блокчейн и облака / ИКС-МЕДИА. 2016 [Электронный ресурс]. http://www.iksmedia.ru/articles/5291626-Blokchejn-i-oblaka.html (Дата обращения: 03.12.2023).
4. Генкин А., Михеев А. Блокчейн: как это работает и что нас ждёт завтра // «Издательство «Альпина», 2018. – 276 с.