|  |  |
| --- | --- |
|  | **Российский государственный социальный университет** |

**Итоговое практическое задание № 3.**

**по дисциплине «Информационная безопасность»**

**на тему «Создание блоков в сети Биткоин»**

|  |  |
| --- | --- |
| **ФИО студента** | Салов Артём Владимирович |
| **Направление подготовки** | Программная инженерия |
| **Группа** | ПИН-Б-О-Д-2021-1 |

**Москва 2023**

Оглавление

[Введение. 3](#_Toc153737419)

[1. Основные принципы работы сети Биткоин. 4](#_Toc153737420)

[1.1. Понятие блокчейна и его роль в сети Биткоин. 4](#_Toc153737421)

[1.2. Децентрализованная природа криптовалюты и блокчейна. 4](#_Toc153737422)

[1.3. Концепция децентрализованных транзакций и хранения данных. 4](#_Toc153737423)

[2. Майнинг и майнеры в сети Биткоин. 4](#_Toc153737424)

[2.1. Роль майнинга в создании новых блоков. 4](#_Toc153737425)

[2.2. Как майнеры конкурируют за право добавить блок в блокчейн. 4](#_Toc153737426)

[2.3. Вознаграждение майнеров и стимулы для участия в майнинге. 4](#_Toc153737427)

[3. Структура блока в сети Биткоин. 4](#_Toc153737428)

[3.1. Как формируются транзакции внутри блока. 5](#_Toc153737429)

[3.2. Размер блока и проблемы масштабируемости. 5](#_Toc153737430)

[3.3. Мерклевские деревья и их роль в обеспечении целостности блока. 5](#_Toc153737431)

[4. Криптографические аспекты создания блоков в сети Биткоин. 5](#_Toc153737432)

[4.1. Применение хэш-функций в блокчейне. 5](#_Toc153737433)

[4.2. Роль нулевых битов (Proof-of-Work) в процессе майнинга. 5](#_Toc153737434)

[4.3. Обеспечение безопасности блокчейна через криптографию. 5](#_Toc153737435)

[5. Транзакции в сети Биткоин: 5](#_Toc153737436)

[5.1. Структура транзакции. 6](#_Toc153737437)

[5.2. Входы и выходы транзакции: 6](#_Toc153737438)

[5.3. Подписи и удостоверения подлинности в транзакциях: 6](#_Toc153737439)

[6. Проблемы и вызовы при создании блоков в сети Биткоин: 6](#_Toc153737440)

[6.1. Проблемы масштабируемости и способы их решения: 6](#_Toc153737441)

[6.2. Экологические и энергетические аспекты майнинга: 6](#_Toc153737442)

[6.3. Влияние высоких комиссий на процесс создания блоков: 6](#_Toc153737443)

[7. Будущее создания блоков в сети Биткоин: 6](#_Toc153737444)

[7.1. Тенденции и направления развития технологии: 7](#_Toc153737445)

[7.2. Исследования и предложения по улучшению процесса создания блоков: 7](#_Toc153737446)

[7.3. Возможные изменения и обновления протокола Биткоин: 7](#_Toc153737447)

[Заключение. 8](#_Toc153737448)

# Введение.

В современном мире криптовалюты стали одним из наиболее обсуждаемых и активно развивающихся направлений в финансовой сфере. Среди них особое место занимает биткоин – первая и наиболее известная криптовалюта, которая стала непрерывным объектом внимания исследователей, инвесторов и обычных пользователей.

Одним из фундаментальных аспектов функционирования биткоин-сети является процесс создания блоков, который является неотъемлемой частью механизма децентрализованной криптовалютной системы. Создание блоков в сети биткоин обеспечивает не только осуществление транзакций, но и обеспечивает безопасность и устойчивость всей сети.

В данном докладе мы рассмотрим ключевые аспекты создания блоков в сети биткоин, начиная от базовых принципов и заканчивая более сложными технологическими процессами. Мы рассмотрим, как майнеры соревнуются за право добавить новый блок в блокчейн, как формируются транзакции в блоках, и какие механизмы обеспечивают целостность и надежность всей системы.

Погружение в процесс создания блоков в сети биткоин позволит нам лучше понять не только технические аспекты функционирования криптовалют, но и их влияние на современную финансовую и технологическую парадигму. Давайте вместе пройдем через ключевые шаги и механизмы, сделавшие биткоин настоящим веховым событием в мире децентрализованных финансов.

# Основные принципы работы сети Биткоин.

*Битко́йн* — пиринговая платёжная система, использующая одноимённую единицу для учёта операций.

Сеть Биткоин представляет собой децентрализованный механизм обмена цифровыми активами, основанный на инновационной технологии блокчейн.

## Понятие блокчейна и его роль в сети Биткоин.

*Блокчейн* представляет собой цепочку блоков, каждый из которых содержит информацию о транзакциях. Эта цепочка хранится на распределенной сети компьютеров, что обеспечивает прозрачность и надежность. Блокчейн является основой для регистрации всех транзакций в сети Биткоин.

## Децентрализованная природа криптовалюты и блокчейна.

Биткоин работает без центрального контроля, что отличает его от традиционных финансовых систем. Блокчейн распределен по всей сети узлов, каждый из которых хранит полную историю транзакций. Это исключает необходимость доверия к центральному органу и обеспечивает устойчивость к внешним атакам.

## Концепция децентрализованных транзакций и хранения данных.

Транзакции в сети Биткоин проводятся напрямую между участниками, обходя посредников. Эти транзакции затем собираются в блоки и добавляются к общей цепочке. Этот процесс обеспечивает децентрализованный и открытый характер сети, снижая вероятность мошенничества и обеспечивая непрерывность операций.

# Майнинг и майнеры в сети Биткоин.

Майнинг в сети Биткоин представляет собой ключевой механизм, обеспечивающий безопасность и эффективную работу блокчейна. Майнеры играют решающую роль в создании новых блоков и поддержании устойчивости криптовалютной системы.

## Роль майнинга в создании новых блоков.

*Майнинг* – это процесс решения математически сложных задач, известных как "Proof-of-Work" (доказательство выполнения работы), с целью добавления нового блока в блокчейн. Этот процесс требует вычислительной мощности, и успешное решение проблемы позволяет майнеру создать новый блок и добавить его к цепочке.

## Как майнеры конкурируют за право добавить блок в блокчейн.

Майнеры соревнуются между собой за возможность добавить следующий блок. Это достигается путем решения криптографической задачи, что делает процесс не только конкурентоспособным, но и децентрализованным. Успешный майнер получает право добавить блок и получает вознаграждение в виде новых биткоинов и комиссий от транзакций.

## Вознаграждение майнеров и стимулы для участия в майнинге.

Майнеры получают как новые биткоины, так и комиссии от транзакций в блоке в качестве вознаграждения за свою работу. Это служит стимулом для участия в майнинге и обеспечивает долгосрочную устойчивость сети. Система также предусматривает уменьшение вознаграждения с течением времени, что создает дефицитность биткоинов и повышает их ценность.

# 3. Структура блока в сети Биткоин.

Структура блока в сети Биткоин представляет собой сложный организованный формат, в котором информация о транзакциях и других ключевых элементах сохраняется и обеспечивает ее интегритет. Рассмотрим основные компоненты и принципы формирования блока в блокчейне Биткоин.

## 3.1. Как формируются транзакции внутри блока.

Каждый блок содержит информацию о проведенных транзакциях. Эти транзакции группируются в блок в хронологическом порядке и представляют собой записи об обмене биткоинами между участниками сети. Каждая транзакция содержит входы (inputs) и выходы (outputs), определяя, откуда берутся средства и куда они направляются.

## 3.2. Размер блока и проблемы масштабируемости.

Размер блока влияет на количество транзакций, которые он может содержать. Проблемы масштабируемости в сети Биткоин связаны с ограниченным размером блока, что приводит к задержкам в обработке транзакций и увеличению комиссий. Сообщество активно исследует способы решения этих проблем, такие как внедрение второго уровня (Layer 2) или увеличение размера блока.

## 3.3. Мерклевские деревья и их роль в обеспечении целостности блока.

Мерклевские деревья представляют собой структуру данных, позволяющую эффективно и безопасно хранить хеш-суммы транзакций в блоке. Это обеспечивает быструю проверку целостности блока: изменение любой транзакции потребует изменения соответствующей хеш-суммы, что сразу становится заметным.

# Криптографические аспекты создания блоков в сети Биткоин.

Криптография играет фундаментальную роль в обеспечении безопасности и целостности блокчейна Биткоин. Рассмотрим ключевые криптографические аспекты, которые лежат в основе создания блоков и обеспечивают надежность этой инновационной криптовалютной системы.

## Применение хэш-функций в блокчейне.

Хэш-функции играют центральную роль в создании блоков. Каждый блок содержит уникальный хеш, который зависит от данных в блоке. Эта хеш-функция служит не только для идентификации блока, но и для обеспечения целостности данных: даже небольшие изменения в блоке вызовут существенное изменение его хеша.

## Роль нулевых битов (Proof-of-Work) в процессе майнинга.

Алгоритм Proof-of-Work требует, чтобы майнеры находили хеш для блока, начинающийся с определенного количества нулевых битов. Этот процесс трудоемок и требует значительной вычислительной мощности. Таким образом, майнеры фактически доказывают, что они выполнили определенный объем работы для создания нового блока.

## Обеспечение безопасности блокчейна через криптографию.

Эллиптическая криптография используется для создания криптографических подписей, которые подтверждают подлинность транзакций в блоке. Приватные и публичные ключи используются для безопасной передачи средств, а смарт-контракты предоставляют дополнительные возможности для программных соглашений в блокчейне.

# Транзакции в сети Биткоин:

Транзакции представляют собой основной строительный блок блокчейна Биткоин, определяя перемещение цифровых активов между участниками сети. Рассмотрим ключевые аспекты транзакций в сети Биткоин, начиная от их структуры и заканчивая важными элементами, обеспечивающими безопасность и прозрачность операций.

## Структура транзакции.

Транзакция включает в себя несколько обязательных элементов. Это входы, которые указывают, откуда берутся средства, и выходы, которые определяют, куда направляются эти средства. Также присутствует поле с данными и подписи для обеспечения подлинности.

## Входы и выходы транзакции:

Входы транзакции представляют собой ссылки на выходы предыдущих транзакций, которые становятся входами для новой операции. Выходы определяют, какие адреса и с какими суммами получат средства. Эта структура обеспечивает прозрачность владения и передачи биткоинов.

## Подписи и удостоверения подлинности в транзакциях:

Для подтверждения того, что отправитель имеет право распоряжаться средствами, используется цифровая подпись. Она создается приватным ключом отправителя и проверяется публичным ключом, что обеспечивает надежную аутентификацию и предотвращает манипуляции с транзакциями.

# Проблемы и вызовы при создании блоков в сети Биткоин:

Несмотря на инновационность и успехи сети Биткоин, существуют определенные вызовы и проблемы, которые необходимо решать для дальнейшего развития и улучшения функциональности блокчейна. Рассмотрим некоторые из ключевых проблем и вызовов, с которыми сталкивается сеть Биткоин.

## Проблемы масштабируемости и способы их решения:

С увеличением числа транзакций возникают проблемы масштабируемости. Ограниченный размер блока приводит к задержкам в обработке транзакций и увеличению комиссий. Разработка технологий второго уровня, таких как Lightning Network, и обновлений протокола направлена на решение этих проблем.

## Экологические и энергетические аспекты майнинга:

Майнинг Биткоина требует значительных вычислительных ресурсов, что приводит к высокому энергопотреблению. Эта проблема привлекает внимание из-за своего воздействия на окружающую среду. Исследования направлены на разработку более эффективных и экологически устойчивых методов майнинга.

## Влияние высоких комиссий на процесс создания блоков:

В условиях ограниченной вместимости блоков, конкуренция за включение транзакций становится более яркой, что приводит к увеличению комиссий. Это может сделать мелкие транзакции менее конкурентоспособными и повлиять на пользователей с небольшими суммами.

# Будущее создания блоков в сети Биткоин:

Будущее сети Биткоин предвещает внедрение новых технологий и изменения в протоколе с целью повышения эффективности, безопасности и устойчивости системы. Рассмотрим направления развития, которые могут оказать влияние на процесс создания блоков в блокчейне Биткоин.

## Тенденции и направления развития технологии:

С появлением новых технологий, таких как смарт-контракты и алгоритмы консенсуса, сеть Биткоин может расширить свои возможности. Исследования в области масштабируемости, приватности и интероперабельности также будут влиять на будущую архитектуру создания блоков.

## Исследования и предложения по улучшению процесса создания блоков:

Активное научное исследование направлено на выявление потенциальных улучшений в протоколе Биткоина. Вопросы, связанные с масштабируемостью, снижением энергопотребления и улучшением алгоритмов консенсуса, занимают центральное место в этих исследованиях.

## Возможные изменения и обновления протокола Биткоин:

Сообщество Биткоин активно обсуждает различные предложения по улучшению протокола, такие как BIP (Bitcoin Improvement Proposals). Эти изменения могут включать в себя улучшенные методы масштабирования, новые функциональности и изменения в правилах создания блоков.

# Заключение.

В заключение можно отметить, что блокчейн Биткоин стал неотъемлемой частью современного финансового мира, предоставляя инновационный и эффективный механизм обмена цифровыми активами. Процесс создания блоков в сети Биткоин, основанный на принципах децентрализации, безопасности и прозрачности, стал фундаментом для развития криптовалют и блокчейн-технологии в целом.

Несмотря на свои достижения, сеть Биткоин сталкивается с вызовами, такими как проблемы масштабируемости и вопросы, связанные с энергопотреблением майнинга. Однако активное исследование и обсуждение в сообществе намечают пути решения этих проблем, что говорит о готовности к долгосрочному развитию.

Роль Биткоина как средства хранения стоимости и инструмента для достижения финансовой инклюзивности подчеркивает его значение в глобальной экономике. Будущее блокчейна Биткоин наполнено инновациями, исследованиями и постоянным стремлением к улучшению, что делает его ключевым участником в мировой финансовой революции.

*Список источников:*

1. Bitcoin. Как это работает – URL: <https://habr.com/ru/articles/114642/>
2. Блокчейн изнутри: как устроен биткоин. Разбираемся раз и навсегда человеческим языком. – URL: <https://pikabu.ru/story/blokcheyn_iznutri_kak_ustroen_bitkoin_razbiraemsya_raz_i_navsegda_chelovecheskim_yazyikom_dlinnopost_8857566>
3. Биткойн – URL: <https://ru.wikipedia.org/wiki/Биткойн>
4. Блок Биткоина - что это такое и как он устроен? – URL: <https://tehnoobzor.com/cryptolife/bitcoin/2006-blok-bitkoina-chto-eto-takoe-i-kak-on-ustroen.html>
5. Технология блокчейн и Биткоин: Информация – URL: <https://intuit.ru/studies/courses/3520/762/info>