Правительство Российской Федерации ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ» (НИУ ВШЭ)

Московский институт электроники и математики им. А. Н. Тихонова

ОТЧЕТ

О ПРАКТИЧЕСКОЙ РАБОТЕ № 6

по дисциплине «Криптографические методы защиты информации»

Программа алгоритма консенсуса блокчейн «Доказательство выполнения работы»

(Proof of Work, PoW)

|  |
| --- |
| Студент гр. БИБ222  Малыгин Данила Дмитриевич  «02» июня 2024 г. |
| Старший преподаватель  Доктор технических наук  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ И. Г. Шапошников  «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2024 г. |

Москва 2024

**СОДЕРЖАНИЕ**

[1. Цель работы 3](#_Toc168402322)

[2. Задание 4](#_Toc168402323)

[3. Краткая теоретическая часть 5](#_Toc168402324)

[3.1. Общие сведения о блокчейн 5](#_Toc168402325)

[3.2. Хэш-функции 6](#_Toc168402326)

[3.3. Алгоритм «дерево Меркла» подсчёта хэш-функции в блокчейн биткоин 6](#_Toc168402327)

[3.4. Алгоритмы консенсуса публичных блокчейн 7](#_Toc168402328)

[3.5. Общие сведения о блокчейн криптовалют 8](#_Toc168402329)

[3.6. Состав блока блокчейн биткоин 8](#_Toc168402330)

[3.7. Алгоритм создания блоков в сети криптовалюты Bitcoin (майнинга) 9](#_Toc168402331)

[3.8. Атака двойной траты (двойного расходования) или атака 51% 10](#_Toc168402332)

[4. Хэш-функция SHA-256 11](#_Toc168402333)

[4.1. Достоинства 12](#_Toc168402334)

[4.2. Недостатки 12](#_Toc168402335)

[7. Описание программной реализации 14](#_Toc168402336)

[8. Пример работы программы 17](#_Toc168402337)

[9. Выводы о проделанной работе 18](#_Toc168402338)

[10. Список использованных источников 19](#_Toc168402339)

[11. Ссылка на репозиторий с программой 20](#_Toc168402340)

# Цель работы

Целью данной работы является приобретение навыков программной реализации алгоритма консенсуса PoW, аналогичного алгоритму PoW в Bitcoin (майнинга).

# Задание

1. Написать программную реализацию алгоритмов хэш-функции SHA-256;
2. Для четырёх транзакций (файлов размера 226 байт каждый) подсчитать хэш корня Меркла с помощью алгоритма SHA-256;

3. Создать заголовок блока, состоящий из следующих полей: размер блока (4 байта); хэш заголовка предыдущего блока (берётся случайное 256 битное число); хэш корня Меркла транзакций (256 бит); метка времени (4 байта); nonce (32 бита);

4. Последовательно изменяя значение nonce, найти хэш заголовка блока с четырьмя первыми нулями.

5. Подготовить отчет о выполнении работы.\

Программа должна обладать следующей функциональностью:

1. Принимать на вход файлы, содержащие транзакции;

2. Принимать на вход файл, содержащий хэш заголовка предыдущего блока;

3. Осуществлять вычисление корня Меркла для транзакций;

4. Осуществлять вычисления хэш заголовка до получения требуемого результата, последовательно изменяя nonce;

5. Сохранять созданный блок в файле.

Отчет должен содержать следующие составные части:

1. Раздел с заданием;

2. Раздел с краткой теоретической частью;

3. Раздел с описанием программной реализации с учетом особенностей выбранной среды разработки и языка программирования;

4. Раздел с результатами работы программы;

5. Раздел с выводами о проделанной работе.

# Краткая теоретическая часть

**3.1. Общие сведения о блокчейн**

Блокчейн (blockchain) — это распределённая база данных, защищённая от изменений, где устройства хранения не подключены к общему серверу. Блокчейн представляет собой цепочку блоков информации, каждый из которых содержит транзакции и ссылку на предыдущий блок. Благодаря хэш-суммам, блокчейн защищён от изменений.

Концепцию цепочек блоков предложил Сатоши Накамото в 2008 году и впервые реализовал в 2009 году как часть биткоина. Однако идеи, подобные блокчейну, обсуждались ещё с 1982 года в работах криптографа Дэвида Чаума и других учёных.

Основные характеристики блокчейна:

– Пиринговый: все участники сети равноправны, без центрального контроля.

– Распределённый реестр: каждый участник имеет полную копию базы данных.

– Только добавление: блоки можно только добавлять, изменение данных практически невозможно.

– Обновляемый по соглашению: обновления происходят через консенсус участников.

Существует три основных типа блокчейна:

1. Публичный: доступен всем, любой может участвовать в его работе.
2. Приватный: доступ ограничен, только по приглашению администраторов.
3. Консорциум: управляется группой равноправных узлов, члены консорциума совместно валидируют транзакции.

Блокчейн используется для передачи информации без участия третьей стороны, что делает его важным для финансовых транзакций, прав собственности, умных контрактов и других сфер. Он также применяется в банковском секторе, земельных реестрах, медицине и других областях.

Основные требования к криптографическим хэш-функциям включают:

1. Необратимость – невозможно вычислить исходный блок данных по заданному значению хэш-функции.
2. Стойкость к коллизиям первого рода – невозможно подобрать другое сообщение с тем же хэш-значением.
3. Стойкость к коллизиям второго рода – невозможно найти пару сообщений с одинаковым хэш-значением.

**3.2. Хэш-функции**

Безопасность блокчейна основывается на криптографических хэш-функциях. Хэширование преобразует входные данные произвольной длины в фиксированную битовую строку. Хэш-функция называется криптографической, если она необратима и устойчиво к нахождению коллизий — сообщений с одинаковыми хэш-значениями.

Хэш-функции в блокчейне защищают данные от изменений. Сложность нахождения коллизий называется стойкостью хэш-функции. Наиболее известный метод нахождения коллизий — атака "дней рождения", где вероятность успеха поиска коллизии связана с числом возможных хэш-значений.

В блокчейне биткоина используется алгоритм SHA-256, который генерирует 256-битные хэши. Алгоритм обрабатывает данные блоками по 512 бит через 64 цикла, используя 32-битные слова и константы. В результате обработки всех блоков получается итоговый 256-битный хэш.

Для корректной работы исходное сообщение дополняется до длины, кратной 512 битам, добавлением единицы, нулей и длины сообщения в последние 64 бита. Начальное значение хэша заполняется константами.

Изображение выглядит как текст, диаграмма, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 1 - Схема работы SHA-256

**3.3. Алгоритм «дерево Меркла» подсчёта хэш-функции в блокчейн биткоин**

Подсчет хэша блока в блокчейне обычно выполняется с помощью алгоритма «дерево Меркла». Это двоичное дерево, где листовые вершины содержат хэши данных, а внутренние вершины — хэши дочерних вершин. Корневой узел дерева содержит хэш всего набора данных.

Дерево Меркла упрощает вычисление хэша блока при добавлении новой транзакции и позволяет эффективно проверять подлинность транзакций. Если количество транзакций нечетное, последняя транзакция дублируется.

Использование хэш-дерева позволяет быстро доказать принадлежность блока данных к множеству, проверяя только один блок, без пересчета хэшей остальных узлов дерева.

Изображение выглядит как снимок экрана, Прямоугольник, прямоугольный, клавиатура

Автоматически созданное описание

Рисунок 2 - Дерево Меркла

**3.4. Алгоритмы консенсуса публичных блокчейн**

Консенсус — это процесс согласования данных в блокчейне между узлами. Алгоритм консенсуса должен обеспечивать согласие всех «честных» узлов и работать при наличии неисправных или вредоносных узлов. Он также должен защищать от атак, таких как атака Сивиллы, где один пользователь создает множество ложных узлов для захвата сети.

В блокчейне существуют два основных алгоритма консенсуса: Proof of Work (PoW) и Proof of Stake (PoS).

Proof of Work (PoW) – участники (майнеры) решают сложные вычислительные задачи, чтобы предложить блок для сети. Первый, кто решает задачу, получает вознаграждение. Пример: алгоритм HashCash в биткоине. Сложность задач регулируется для поддержания средней скорости создания блоков.

Proof of Stake (PoS) – участники (валидаторы) показывают, что у них есть доля в системе (например, фиксированное количество криптовалюты). Валидаторы выбираются случайным образом для создания и подтверждения блоков. Пример: Ethereum перешел на PoS в 2022 году, сократив потребление энергии на 99%. Валидаторы должны заморозить 32 ETH для участия.

PoS не требует майнеров и специального оборудования, что делает его более энергоэффективным. Стейкинг (заморозка криптовалюты) используется для обеспечения участия в консенсусе PoS.

**3.5. Общие сведения о блокчейн криптовалют**

Криптовалюта — это цифровая валюта, работающая через компьютерную сеть без центрального органа, такого как правительство или банк. Монеты (например, Bitcoin, BTC) хранятся в блокчейне как транзакции, подписанные секретным ключом. Транзакции включают открытый ключ для проверки подписи и адреса отправителя и получателя. Адреса, часто представляющие собой хэшированный открытый ключ, могут изменяться для повышения анонимности.

Баланс пользователя проверяется через программное обеспечение, используя закрытые ключи, которые хранятся в кошельке. Кошелек — это программа (например, Bitcoin Core), позволяющая пользователю отправлять и получать монеты.

Сеть криптовалюты является пиринговой (P2P), узлы обмениваются информацией о транзакциях и блоках. Полные узлы хранят блокчейн и проверяют новые блоки, а легковесные узлы выполняют только функции кошелька и сетевой маршрутизации.

Биткоин, первая криптовалюта, был выпущен в 2009 году. К июню 2023 года существовало более 25 000 криптовалют, из которых более 40 имели рыночную капитализацию свыше 1 миллиарда долларов. Среди них крупнейшие — Bitcoin и Ethereum.

**3.6. Состав блока блокчейн биткоин**

Блок в блокчейне биткоина состоит из следующих полей: размер блока (4 байта), заголовок блока (80 байт), счётчик транзакций (переменной длины) и сами транзакции (переменной длины). Размер блока не должен превышать 1 МБ.

Транзакции представляют собой криптографически защищенный обмен активами между участниками сети. Первая транзакция в любом блоке — coinbase транзакция — создаётся майнером для получения вознаграждения за найденный блок.

Заголовок блока включает: версию блока (4 байта), хэш предыдущего блока (32 байта), хэш корня Меркла (32 байта), метку времени (4 байта), текущую цель сложности сети (4 байта) и nonce (4 байта).

Изображение выглядит как текст, снимок экрана, программное обеспечение, мультимедиа

Автоматически созданное описание

Рисунок 3 - Цепочка блоков

Цель сложности сети — это число, меньше которого должен быть хэш заголовка. Если 32-битного nonce недостаточно для нахождения нужного хэша, используется extraNonce в транзакции coinbase. При этом пересчитывается только одна "ветка" дерева Меркла.

**3.7. Алгоритм создания блоков в сети криптовалюты Bitcoin (майнинга)**

После подписания владельцем биткойнов транзакция передается в сеть, где каждый узел проверяет подпись и историю транзакций, чтобы подтвердить наличие средств. После подтверждения транзакция попадает в мемпул (локальный пул неподтвержденных транзакций). Майнеры выбирают транзакции из мемпула для формирования блока.

Майнеры получают вознаграждение за создание блока, включающее субсидию и комиссии за транзакции. Субсидия — это фиксированное количество новых биткойнов за каждый добавленный блок, которое уменьшается вдвое каждые 210,000 блоков (процесс халвинга). Комиссии за транзакции добавляются майнерами в блок, причем приоритет отдается транзакциям с более высокими комиссиями.

Сеть биткойн использует алгоритм Proof of Work (PoW), при котором майнеры решают сложные вычислительные задачи, чтобы найти хэш, удовлетворяющий текущей цели сложности. Если 32-битного nonce недостаточно, используется поле extraNonce, что требует пересчета корня дерева Меркла.

По мере роста хэшрейта сети, сложность задач автоматически регулируется. Первоначальная субсидия за блок составляла 50 BTC, и она уменьшалась в 2012, 2016 и 2020 годах. Ожидается, что последний биткойн будет добыт около 2140 года. После этого майнеры будут получать вознаграждение только за счет комиссий за транзакции.

**3.8. Атака двойной траты (двойного расходования) или атака 51%**

Злоумышленник-майнер создает скрытую от сети побочную цепочку блокчейна и тратит свои биткойны в основной цепочке, не включая эти транзакции в изолированную версию. Затем он пытается добавлять блоки в свою цепочку быстрее, чем другие майнеры в основной цепочке. Когда его цепочка становится длиннее, он транслирует ее в сеть, заставляя всех переключиться на подменную версию, возвращая себе потраченные биткойны.

Для успешной атаки злоумышленнику нужны мощности, превышающие мощность всей сети, что практически невозможно. Однако такие атаки возможны при ошибках в протоколе блокчейна.

# Хэш-функция SHA-256

SHA-256 (Secure Hash Algorithm 256-bit) — это криптографическая хэш-функция, разработанная Национальным институтом стандартов и технологий США (NIST), и является частью семейства SHA-2. Она широко используется для обеспечения целостности и безопасности данных в различных областях, включая блокчейн-технологии.

Принципы работы:

1. Входные данные:

– Принимает данные произвольной длины.

– Обрабатывает данные по блокам размером 512 бит.

1. Подготовка данных:

– Дополняет данные до длины, кратной 512 битам.

– К исходным данным добавляется бит "1", за которым следует набор битов "0".

– В последние 64 бита добавляется длина исходного сообщения.

1. Инициализация:

– Инициализация восьми 32-битных слов начальных значений, которые используются для хранения промежуточных хэш-значений.

1. Основной процесс:

– Сообщение разбивается на блоки по 512 бит.

– Каждый блок обрабатывается функцией сжатия, состоящей из 64 раундов, в которых используются побитовые операции, сдвиги и логические функции.

– В каждом раунде используются разные константы и изменяемые данные, основанные на текущем состоянии хэша и обрабатываемом блоке.

1. Итерации:

– Промежуточные хэш-значения обновляются после обработки каждого блока.

– Итоговый хэш получается после обработки всех блоков сообщения.

1. Выходные данные:

– Результатом является 256-битный (32-байтовый) хэш, уникальный для каждого набора входных данных.

Связь с блокчейном:

– В блокчейне биткоина SHA-256 используется для создания хэшей транзакций и блоков, что обеспечивает целостность данных.

– Хэш каждого блока содержит хэш предыдущего блока, создавая непрерывную цепочку.

– Майнеры решают задачи поиска хэша, который соответствует определенным условиям (целевой сложности).

– Для нахождения подходящего хэша майнеры изменяют параметр nonce и вычисляют новый хэш блока.

– Процесс требует значительных вычислительных ресурсов, обеспечивая безопасность сети.

* 1. **Достоинства**

– Хэш-функция SHA-256 является односторонней, что означает, что из хэша невозможно восстановить исходные данные. Это обеспечивает высокий уровень безопасности данных.

– Вероятность того, что две разные последовательности данных дадут одинаковый хэш (коллизия), крайне мала. Это делает SHA-256 надежным для проверки целостности данных.

– SHA-256 разработан с учетом защиты от различных криптографических атак, таких как атаки на коллизии и атаки на прообраз.

– Алгоритм SHA-256 достаточно быстрый и может обрабатываться эффективно как программными, так и аппаратными средствами.

– Благодаря своей структуре, SHA-256 может быть оптимизирован для выполнения на различных платформах и устройствах.

– SHA-256 является частью криптографического стандарта SHA-2 и широко используется в различных индустриях, включая блокчейн, цифровую подпись, SSL/TLS и другие криптографические протоколы.

– Использование SHA-256 гарантирует совместимость с большинством современных систем безопасности и криптографических приложений.

* 1. **Недостатки**

– В контексте блокчейна, особенно в случае биткоина, процесс майнинга с использованием SHA-256 требует значительных вычислительных ресурсов и, следовательно, большой затраты энергии. Это приводит к экологическим и экономическим проблемам.

– Размер хэша в 256 бит может быть избыточным для некоторых приложений, где требуется меньший размер хэша. Это увеличивает объем данных, которые нужно хранить и передавать.

– С развитием квантовых компьютеров алгоритмы, основанные на традиционной криптографии, такие как SHA-256, могут стать уязвимыми к квантовым атакам. Хотя на данный момент это не является непосредственной угрозой, будущее развитие квантовых технологий может потребовать новых хэш-функций, устойчивых к квантовым атакам.

– Хотя SHA-256 эффективен на современных платформах, его производительность может значительно варьироваться в зависимости от аппаратного обеспечения. Некоторые устройства могут испытывать трудности с выполнением вычислений на приемлемой скорости.

# Описание программной реализации

Программа написана на языке Python с использованием стандартных библиотек struct и time. Я использовал текстовый редактор Spyder и Python версии 3.10 для разработки программы. Программа реализует алгоритм хэширования на основе Keccak. Она считывает данные из файла, преобразует их в битовую строку, выполняет необходимые математические преобразования (Theta, Rho, Pi, Chi, Iota) над массивом состояния, и генерирует хэш-значение. Полученное хэш-значение сохраняется в указанный выходной файл и выводится сообщение о его сохранении.

Подробное описание работы программы

1. **Импорт библиотек:**

– struct используется для работы с бинарными данными.

– time используется для получения текущего времени.

1. **Определение констант:**

– K – список констант, используемых в алгоритме SHA-256.

1. **Функция sha256(data: bytes) -> str:**

– Принимает данные в виде байтов и возвращает их SHA-256 хеш в шестнадцатеричном формате.

1. **Функция generate\_hash(message: bytearray) -> bytearray:**

– Основная функция для генерации SHA-256 хеша.

– Принимает сообщение и преобразует его в формат bytearray.

– Дополняет сообщение битом '1' и затем нулями, чтобы его длина была кратной 512 минус 64 бита.

– Добавляет длину сообщения в конце.

– Разделяет сообщение на блоки по 512 бит.

– Инициализирует переменные состояния.

– Для каждого блока сообщения создает расписание сообщений.

– Обрабатывает каждый блок, обновляя значения переменных состояния.

– Возвращает итоговый хеш в виде байтов.

1. **Вспомогательные функции:**

– \_sigma0(num: int): выполняет побитовые вращения и сдвиги.

– \_sigma1(num: int): выполняет побитовые вращения и сдвиги.

– \_capsigma0(num: int): выполняет побитовые вращения.

– \_capsigma1(num: int): выполняет побитовые вращения.

– \_ch(x: int, y: int, z: int): выполняет функцию выбора (ch).

– \_maj(x: int, y: int, z: int): выполняет функцию большинства (maj).

– \_rotate\_right(num: int, shift: int, size: int = 32): выполняет побитовый циклический сдвиг вправо.

1. **Функция merkle\_root(transactions):**

– Принимает список транзакций.

– Вычисляет корень дерева Меркла, объединяя пары хешей и применяя к ним SHA-256.

– Возвращает корень дерева Меркла.

1. **Функция create\_block\_header(prev\_hash, merkle\_root\_hash, nonce):**

– Создает заголовок блока, объединяя:

– Версию блока.

– Хеш предыдущего блока.

– Корневой хеш дерева Меркла.

– Текущее время.

– Цель сложности сети.

– Значение nonce.

– Возвращает заголовок блока в виде байтов.

1. **Функция mine\_block(prev\_hash, merkle\_root\_hash):**

– Выполняет майнинг блока, изменяя значение nonce и проверяя, начинается ли хеш блока с определенного количества нулей.

– Возвращает хеш блока и значение nonce, если найдено подходящее значение.

1. **Основная функция main():**

– Читает транзакции из файлов и вычисляет их хеши.

– Вычисляет корневой хеш дерева Меркла.

– Читает хеш предыдущего блока из файла.

– Выполняет майнинг блока, чтобы найти подходящий хеш.

– Выводит хеш блока и значение nonce.

– Сохраняет заголовок блока в бинарный файл.

1. **Запуск программы:**

– При запуске файла, функция main() выполняется, инициируя процесс майнинга блока и вычисления SHA-256 хеша для транзакций.

# Пример работы программы

Запускаем программу, имеем 4 транзакции.

Изображение выглядит как текст, программное обеспечение, Шрифт, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 4 - Файл с текстом, которых хотим зашифровать

Результат выполнения программы. Заголовок блока был сохранен в файл **block.bin.**

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 5 - Результат выполнения программы

**Корневой хеш Меркла:** 1ac604e4a4c0a56329082edc30fb73e8c1d830866587742b2c4dda92523d4f46

**Block Hash:** 0000f69f05c39d7fb9b85fc8d765e4be2b84fca036b2116653c0e7e95da07be5

**Nonce:** 261681

Повторный результат выполнения программы. Заголовок блока был сохранен в файл block.bin

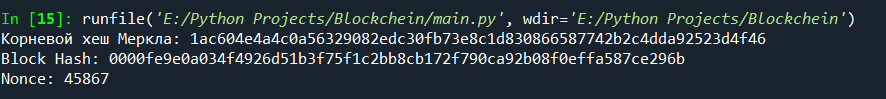


Рисунок 6 - Результат выполнения программы

**Корневой хеш Меркла:** 1ac604e4a4c0a56329082edc30fb73e8c1d830866587742b2c4dda92523d4f46

**Block Hash:** 0000fe9e0a034f4926d51b3f75f1c2bb8cb172f790ca92b08f0effa587ce296b

**Nonce:** 45867

Программа, вычисляющая корневой хэш дерева Меркла и майнит блоки, может принимать на вход данные не только из файлов формата .txt, но и из других типов файлов, таких как .jpg, поскольку код может считывать любые бинарные данные из файлов.

Входные данные – transaction1.jpg – transaction4.jpg

Изображение выглядит как снимок экрана

Автоматически созданное описание

Рисунок 7 – Транзакции формата .jpg

В итоге получаем:

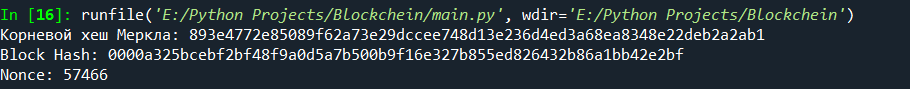


Рисунок 8 - Результат выполнения программы

Аналогично с форматом .pdf:

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

Рисунок 9 - Транзакции формата .pdf

Получаем:

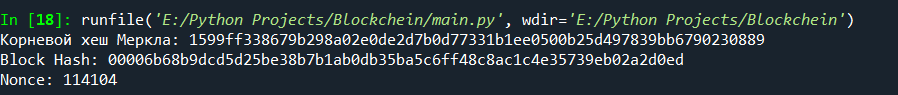


Рисунок 10 - Результат выполнения программы

# Выводы о проделанной работе

В результате выполнения практической работы была создана программа, реализующая основные аспекты алгоритма консенсуса Proof of Work (PoW), аналогичного используемому в блокчейн сети Bitcoin. Программа включает в себя создание хэшей транзакций, вычисление корня дерева Меркла, создание заголовка блока и майнинг блока с заданным условием сложности.

Таким образом, цели работы были достигнуты, и необходимые навыки программной реализации алгоритма консенсуса PoW были успешно приобретены.

# Список использованных источников

1. Как это работает: Деревья Меркла в биткойн сети – URL: [https://habr.com/ru/companies/bitfury/articles/346398/](https://en.wikipedia.org/wiki/Modular_exponentiation).

2. Что такое SHA-256 – URL: [https://crypto.ru/algoritm-heshirovaniya-sha-256/](https://en.wikipedia.org/wiki/Modular_exponentiation).

3. Block Headers – <https://developer.bitcoin.org/reference/block_chain.html>.

# Ссылка на репозиторий с программой

https://github.com/fedyarays/SHA-256