**ОТЧЕТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ**

**1. Цель работы**

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

**2. Краткие теоретические сведения**

**2.1. Общие сведения о блокчейн**

Блокчейн (blockchain) — распределённая защищенная от изменений база данных, у которой устройства хранения данных не подключены к общему серверу. Блокчейн является примером синхронной репликации - полного дублирования всей информации во всех распределенных копиях. База данных блокчейн организована в виде цепочки блоков информации. Блок - это подборка транзакций, объединенных в пакет. Транзакция - это регистрация события: финансовая транзакция, аудит событий аутентификации и авторизации, документы, история болезней, программный код (умные контракты) и т.д.

**2.2. Хэш-функции**

Безопасность блокчейн основывается на стойкости криптографических хэш-функций. Хэширование (hashing) - преобразование по определённому алгоритму входного массива данных произвольной длины в выходную битовую строку фиксированной длины. В блокчейн используются криптографические хэш-функции, что гарантирует защиту от изменений в базе данных. В блокчейн криптовалюты биткоин используется алгоритм криптографической хэш-функции SHA-256.

**2.3. Алгоритм «дерево Меркла» подсчета хэш-функции в блокчейн биткоин**

Подсчет значения хэш блока в блокчейн осуществляется с помощью алгоритма «дерево Меркла», который упрощает подсчет хэш-значения при добавлении в блок новой транзакции и проверки подлинности. Дерево Меркла позволяет быстро вычислять хэш от всех транзакций в блоке при добавлении новой транзакции, а также эффективно верифицировать транзакции.

**2.4. Алгоритмы консенсуса публичных блокчейн**

Консенсус - это процесс согласования финального состояния данных в блокчейн между узлами, не доверяющими друг другу. Алгоритм консенсуса должен обеспечивать принятие общего соглашения всеми «честными» узлами и сохранять работоспособность при наличии неисправных и вредоносных узлов. Основные алгоритмы консенсуса включают Proof of Work (PoW) и Proof-of-Stake (PoS).

**2.5. Общие сведения о блокчейн криптовалют**

Криптовалюта (криптографическая валюта) это цифровая валюта, предназначенная для работы в качестве средства обмена через компьютерную сеть, которая не зависит от какого-либо центрального органа. Монеты (сама криптовалюта) хранятся в блокчейн в виде транзакций, подписанных секретным ключом узла, создавшим транзакцию.

**2.6. Состав блока блокчейн биткоин**

Блок в блокчейн биткоин состоит из полей: размер блока, заголовок блока, счетчик транзакций и сами транзакции. Заголовок блока включает: версию блока, хэш заголовка предыдущего блока, хэш корня Меркла, метку времени, target и nonce.

**2.7. Алгоритм создания блоков в сети криптовалюты Bitcoin (майнинг)**

Майнинг биткоина использует функцию доказательства работы HashCash, которая заключается в поиске хэш с заданной целью сложности. Алгоритм HashCash многократно хэширует заголовок блока, увеличивая поля Nonce и extraNonce, до тех пор, пока не будет найден хэш с требуемой целью сложности.

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

Майнер-злоумышленник создает побочную цепочку блокчейн, скрытую от остальной части сети, и пытается добавить блоки в свою цепочку быстрее, чем другие майнеры добавляют блоки в истинный блокчейн. Для успешной атаки злоумышленнику потребуются мощности, превосходящие мощности всей остальной сети, что практически нереально.

**3. Описание программной реализации**

**3.1. Используемый язык программирования и среда разработки**

Программная реализация выполнена на языке Python. Для хэширования используется библиотека `hashlib`.

**3.2. Описание работы программы**

1. Программа считывает данные из файлов с транзакциями и вычисляет их хэш.

2. Хэши транзакций используются для вычисления корня дерева Меркла.

3. Программа считывает хэш заголовка предыдущего блока из файла.

4. Создается заголовок блока, включающий версию блока, хэш заголовка предыдущего блока, хэш корня Меркла, метку времени и nonce.

5. Программа последовательно изменяет значение nonce, пока не найдет хэш заголовка блока, начинающийся с четырёх нулей.

6. Найденный заголовок блока сохраняется в файл.

**4. Результаты работы программы**

Программа была успешно выполнена, и результаты представлены ниже:

**Корневой хеш Меркла:** 1ac604e4a4c0a56329082edc30fb73e8c1d830866587742b2c4dda92523d4f46

**Block Hash:** 00008e0b6ccf6ff23e1839327f6617006379152a866dd80c5c7f32e218d82e74

**Nonce:** 7537

Заголовок блока был сохранен в файл **block.bin**.

**5. Выводы**

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.