Муниципальное бюджетное общеобразовательное учреждение

гимназия им. академика Н.Г.Басова

Блокчейн. Иллюстрация работыблокчейна.

Выполнил

ученик 11 “Е” класса

Орлов Ярослав

Научный руководитель:

Татьянкина Ю.Г

Воронеж 2017

СОДЕРЖАНИЕ.

1. Введение. Описание и цель работы

2. Теоретическая часть

2.1 Определение блокчейна и его свойства

2.2 Практическое использование блокчейна

2.3 Определения, которые помогут разобраться в работе блокчейна и майнинга.

2.4 Проблемы изучения основ блокчейна и криптовалют

3. Практическая часть

4. Заключение

5. Литература.

**1. Введение**

**Цель работы** – создать сайт, иллюстрирующий работу блокчейна и его компонентов.

**Задачи:**

-Выяснить, что такое блокчейн и как работает эта система.

- Предоставить людям возможность создавать блоки и исследовать информацию в них.

- Показать возможности блокчейна и его применение в повседневной жизни.

**2. Теоретическая часть.**

**2.1 Что такое блокчейн?**

Блокчейн - выстроенная по определённым правилам открытая децентрализованная криптозащищенная непрерывная последовательная цепочка блоков, содержащих информацию. Каждый узел имеет полную или укороченную версию блокчейна для поддержания работы системы.

Теперь стоит разобрать каждое слово в определении.

1) Децентрализованная – значит не имеющая единого контролирующего центра. Ноды в блокчейне не разделены на ранги, которые могли бы влиять на систему “сильнее” или “слабее”.

2) Криптозащищённая – значит защищенная криптографией. Биткоин (Самая известная криптовалюта, созданная на блокчейне) защищен криптографической функцией sha-256, которая способна из строки любой длины (Хоть в миллиард символов) сделать строку длинной в 64 символа.

3) Узлы, содержащие полные версии блокчейна, поддерживают его работоспособность. Если недобросовестный пользователь захочет изменить цепочку блоков у себя на компьютере, то другие участники сети не будут принимать от него транзакции, тем самым ограничив ноду в работе. Так же существуют light версии блокчейна, которые обычно используют мобильные телефоны. У смартфонов обычно немного физической памяти, поэтому они хранят только несколько сотен последних блоков, при этом сохраняют возможность подписывать и отправлять транзакции.

4) Открытость – неотъемлемое свойство блокчейна, позволяющее каждому человеку посмотреть все транзакции и вообще действия, которые были совершены другими пользователями в рамках системы. Например, если я знаю биткоин адрес друга, то я могу посмотреть, кому и сколько он отправил криптовалюты в прошлом.

**2.2 Практическое использование блокчейна**

Чаще всего блокчейн используют для создания новых криптовалют. Блокчейн способен делать транзакции быстрыми и безопасными, что делает эту систему незаменимой в криптовалютах.

Но цепочку блоков используют не только для отправления денег другим пользователям. Блокчейн очень востребован в сфере хранения информации. Например, компании нужно найти способ безопасно содержать у себя ценные документы. И в этой проблеме как никто другой поможет блокчейн, который будет хранить информацию на всех компьютерах компании, при этом каждый сможет посмотреть в нем информацию добавленных документов.

Так же блокчейн можно использовать для вполне конкретных целей. Возьмем ситуацию, когда врач выписывает рецепт пациенту, а тот продает это лекарство другим людям. Проблему этой контрабанды поможет решить блокчейн. При выпуске препарата достаточно давать ему электронно-цифровую подпись, которой врач сможет дать конкретное указание на больного человека. Позже, покупая препарат в магазине, другой человек сможет посмотреть его историю, в которой может быть предназначение совсем другому больному. Таким образом, блокчейн сможет решить проблему контрабанды, которая приносит миллионы долларов мошенникам, а так же устранить ситуацию, когда покупатель приобретает уже просроченный и опасный для применения препарат.

**2.3 Определения, которые помогут разобраться в работе блокчейна и майнинга**

**Хэш-функция -**  преобразование массива входных данных произвольной длины в выходную строку фиксированной длины, выполняемое определённым алгоритмом.

**Блок** – единица в блокчейне, в которой записывается вся информация. Разделен на блок со служебной (Head) и необязательной информацией.

**Head блок** содержит информацию о создании блока, его ID, его хэш, а так же хэшпредыдущего блока.

**Майнинг** – перебор хэшей.

**Валидность/Невалидность** – свойство блока, определяющее соответствие и правильность информации в нем.

**Майнинг** – перебор хешей. Используется для нахождения новых блоков и поддержания работы криптовалют.

Все эти определения помогут понять принцип работы блокчейна, представленный на моем сайте.

**2.4 Проблемы изучения основ блокчейна и криптовалют**

Нынешняя ситуация показывает, что подавляющее большинство не понимает ни что такое блокчейн, ни что такое криптовалюты, ни как они работают.

Связано это с тем, что сама по себе система очень сложная. Я пытался объяснить одноклассникам все про криптовалюты и блокчейн, однако только трое из них запомнили основные понятия, так и не поняв полностью его внутреннее устройство.

Сейчас не существует единого реестра, в котором была бы вся информация о блокчейне, поэтому для его изучения приходится искать отдельную информацию на десятках сайтов, в том числе и на англоязычных. Это значит, что не каждый мотивированный изучением человек сможет понять технологию полностью.

**3. Практическая часть**

Я решил создать сайт, который бы смог решить эту проблему. Расположен он на домене **blockeducation.ru**

Изучая статьи, посвящённые блокчейну и криптовалютам, я понял, что нет ресурсов, которые позволили бы мне поэкспериментировать с полученными знаниями. Тогда у меня и появилась идея создать сайт, который решил бы эту проблему. Когда я делал сайт, то получал новые знания не только о технической работе блокчейне, но и о новых библиотеках js. Спустя пару недель мной был создан первый прототип сайта, на котором можно было просто создавать блоки. Но этого функционала мне не хватало, поэтому я сделал много уникальных возможностей, например:  
 - Возможность регулировать сложность создания блока (Поле Target)  
 - Возможность генерировать в блоке не рандомную информацию, а ту, которую захочет там видеть сам пользователь (Режим “Блокнот”)  
 - Режим проверки блоков, который может проверить информацию в каждом блоке на валидность и покрасить невалидные блоки в красный цвет.

- Возможность создавать сразу несколько блоков.

На сайте можно - Создавать блоки - изучать информацию в каждом поле блока - понять принцип майнинга и создания блоков

А так же найти на нем новые определения для дальнейшего изучения блокчейна.  
Полное описание работы алгоритма, который создает блок:

1) Создание основы блока (HTML5) и его стилизация css3.

2) Заполнение полей "Номер блока", "Время создания блока", "Транзакции" и "Хэш предыдущего блока" (Не изменяются в последствии).

3) Перебор значения nonce до нужного значения (меньше target):

3.1) Значение полей "Номер блока", "Время создания блока", "Транзакции", "Хэш предыдущего блока" и "nonce" складываются (без разделений) и хэшируются хэш-функцией sha256.

3.2) На выходе получается строка длиной 64 символа в 16-ричной системе счисления (символы от 0 до F).

3.3) Далее происходит укорачивание хэша до 6 символов. Делается это для того, чтобы не сравнивать все 64 символа, так как это очень долго и не практично с точки зрения проекта. Если бы js перебирал все символы, то время создания блоков увеличилось бы в десятки раз, что не нужно для учебного сайта.

3.4) 6 символов от хэша переводятся в 10-ричную систему счисления.

3.4) И, наконец, происходит сравнение значений Target и хэша (точнее их 6 символов).

3.5) Если хэш удовлетворяет условию, то есть он <target, то создается блок (PoW консенсус в блокчейне).

4) Заполняется поле nonce, которое подошло для хэша. (для target 2500 - примерно 5000 переборов), и значение “Хэш”, которое подходит по условию.

5) Все последующие блоки создаются точно так же.

6) Режим проверки блоков анализирует все созданные блоки на их валидность. То есть проверяет их хешированием уже полученных данных (Поле nonce искать не надо, оно уже было найдено) и сравнивая этот хэш со значением target.

6) Режим "Блокнот" позволит создать блок с произвольной информацией в поле "транзакции".

7) Пользователь в любой момент может изменить зачение поля target, тем самым изменив сложность создания блоков. Уменьшение этого числа ведет к усложнению создания блока, и наоборот.

Сайт был создан с помощью HTML5,CSS3, Js + jquery и с помощью библиотеки, которая умеет хешировать информацию.

**4. Заключение**

Цель работы выполнена. Был разработан сайт**«**Blockeducation.ru», который поможет новичкам в сфере блокчейна изучить основы технологии, а так же поэкспериментировать с его функционалом.

Блокчейн – технология, уже сейчас оказывающая колоссальное влияние на будущее. На ее основе создана виртуальная машина Ethereum, способная принимать, обрабатывать и выполнять смарт-контракты, были сделаны сотни других криптовалют, со своими функциями и особенностями, которые можно применять в разных сферах жизни.

**5. Литература**

1)Masteringbitcoin (AndreasAntonopoulos)- полное описание работы блокчейна и биткойна.

2)Blockchain: BlueprintforaNewEconomy (МеланиСуон) – всеоблокчейне

3) BlockchainRevolution: HowtheTechnologyBehindBitcoinIsChangingMoney(АлексТапскотт) – книгаотом, почемублокчейнизменитжизньчеловека.

4) Статьи о Ethereum и смарт-контрактах на golos.io