МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КубГУ»)**

**Кафедра прикладной математики**

**КУРСОВАЯ РАБОТА**

**РАЗРАБОТКА ПРИЛОЖЕНИЯ К ТЕХНОЛОГИИ BLOCKCHAIN**

Работу выполнил \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_В.В.Меликян

(подпись, дата) (инициалы,фамилия)

Факультет компьютерных технологий и прикладной математики курс 3

Направление 02.03.03. Математическое обеспечение и администрирование информационных систем

Научный руководитель, д.т.н.

профессор \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_А.А.Халафян

(подпись, дата) (инициалы, фамилия)

Нормоконтролер,

к.ф.м.н.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Г.В. Калайдина

(подпись, дата) (инициалы, фамилия)

Краснодар 2018

СОДЕРЖАНИЕ

Введение 3

1 Технология blockchain 4

* 1. Принципы работы 4
  2. Хеширование…………………………………………………………..6
  3. Цифровая подпись……………………………………………………..9

2 Достоинства технологии blockchain 11

2.1 Основные принципы обеспечения безопасности 11

2.2 Сферы применения технологии в реальной жизни 13

### 2.2.1Блокчейн в медицине.………………………………………...13

### 2.2.2 Энергетика…………………...………………………………..14

### 2.2.3 Недвижимость…...……………………………………………15

### 2.2.4 Интернет вещей…………………………...…………………..15

### 2.2.5 Видеоигры...…………………………………………………..15

2.2.6 Блокчейн в России………………………………...………….16

3 Разработка технологии blockchain…………………………………………….17

Заключение 26

Список использованных источников 27

ВВЕДЕНИЕ

Настоящая работа посвящена изучению технологии blockchain и разработке приложения для работы с данной технологией на языке программирования Python.

В настоящий момент криптовалюты повсеместно привлекают к себе высокий интерес, помимо коммерческого вопроса и желания заработать крупный бизнес и обычные люди обратили свое внимание и на технологию, на которой все основано – блокчейн.

Блокчейн – это именно та цифровая платформа, которая даёт концептуальные возможности для безопасного, быстрого и недорогого в обслуживании обращения новой формы денежных средств.

Благодаря этому изучение технологии Блокчейн приобретают особую актуальность.

Исходной точкой к созданию альтернативных систем для поддержания цифровых транзакций стали банковские услуги, но на сегодняшний день современные технологии используются не только в банковской сфере, а во многих отраслях жизнедеятельности.

Данная технология хорошо себя зарекомендовала в сферах, где нужно обрабатывать большое количество данных, так же данная технология позволяет не беспокоиться о сохранении своих персональных данных, так как внутри технологии реализована современная система защита, которую практически невозможно взломать.

Цель: разработать программное обеспечение, которое будет выполнять все основные операции, соответствующие технологии Блокчейн.

Задача:

– изучить технологию blockchain;

– изучить язык программирования Python.

1 Технология blockchain

Блокчейн (blockchain) – это распределенная база данных, хранящая данные о совершенных транзакциях (действиях), которые записываются в определенном порядке и формируют неизменную последовательность связанных блоков.Блок – своего рода папка, в которую вложена закодированная информация о контрактах и сделках внутри системы. У этой папки есть свои атрибуты, которые невозможно подделать и которые содержат информацию о предыдущей папке в цепи. У такого атрибута есть специальное название – хеш. Создание блоков получило название майнинг, вознаграждение за успешную работу – специальная криптовалюта - биткоин.

Биткоин (bitcoin) – децентрализованная платёжная система, использующая одноимённую единицу для учёта операций и одноимённый протокол передачи данных. Для обеспечения функционирования и защиты системы используются криптографические методы.

Майнинг (mining) – деятельность по созданию новых структур для обеспечения функционирования криптовалютных платформ. За создание очередной структурной единицы обычно предусмотрено вознаграждение за счёт новых (эмитированных) единиц криптовалюты и/или комиссионных сборов. Зачастую майнинг сводится к серии вычислений с перебором параметров для нахождения хеша с заданными свойствами.

## 1.1 Принцип работы blockchain

Цифровые записи объединяются в «блоки», которые потом связываются криптографически и хронологически в «цепочку» с помощью сложных математических алгоритмов. Каждый блок связан с предыдущим и содержит в себе набор записей. Новые блоки всегда добавляются строго в конец цепочки. Процесс шифрования, известный как хеширование, выполняется большим количеством разных компьютеров, работающих в одной сети. Если в результате их расчетов все они получают одинаковый результат, то блоку присваивается уникальная цифровая сигнатура (подпись). Как только реестр будет обновлён и образован новый блок, он уже больше не может быть изменён. Таким образом подделать его невозможно. К нему можно только добавлять новые записи. Важно учесть то, что реестр обновляется на всех компьютерах в сети одновременно.

Одна из классических задач криптологии «задача византийских генералов» формулируется следующим образом – «Византийская армия осаждает город. Генералам необходимо выработать единую стратегию действий, которая приведет к победе, даже если среди них будут предатели, намеренно искажающие информацию о численности своих отрядов и времени наступления».

Основная цель задачи выяснить, как согласовать действия участников системы, объединенных одной целью, но лишенных доверия друг к другу.

Если не пользоваться инструментами математики, то очевидным решением кажется создание единого контролирующего и проверяющего органа, который будет гарантировать участникам системы достоверность получаемой информации.

Благодаря блокчейн-технологии необходимость в посредниках отпадает. Это достигается благодаря особой форме хранения информации о транзакциях сразу на всех компьютерах системы – в распределенных реестрах или базах данных.

В 2008 году Сатоси Накамото изобрел новый способ достижения социального консенсуса, позволяющий подтверждать истинность всех транзакций без участия третьей стороны. Проще всего продемонстрировать это, вкратце объяснив суть работы блокчейн-технологий на примере переводов в биткоинах.

Каждая транзакция происходит онлайн и представляет собой лишь сообщение о том, что некий пользователь переводит другому пользователю известное количество биткоинов. Как только транзакция проведена, она становится видна майнерам.

Ни одна из транзакций не будет считаться завершенной, пока ее не включат в так называемый блок – именно этим и занимаются майнеры. Каждый блок содержит информацию о тысячах обрабатываемых транзакций. Чтобы он считался сформированным, майнер должен вычислить хеш-функцию – цифробуквенную строку, в которую преобразован входящий массив данных.

Хеш-функция содержит информацию о предыдущем блоке, а значит – обо всех транзакциях, совершенных с момента возникновения биткоина как валюты. Если изменить хотя бы бит информации в предыдущей цепочке, до неузнаваемости изменится и хеш-функция. Получается, что распределенная база данных в блокчейне – это цепочка из блоков, каждый из которых ссылается на предыдущий.

Сохранение истории операций с биткоинами гарантирует, что пользователь не переведет кому-то сумму, которой у него нет. Блокчейн-технология позволяет избежать и двойного расходования – ситуации, когда человек дважды пытается потратить одну и ту же сумму. Залогом этого служит большое количество пользователей и майнеров.

Разберем подробнее понятие хеш-функции, на котором строится безопасность блокчейна.

1.2 Хеширование

Хеширование – это процесс преобразования массива входных данных произвольной длины в (выходную) битовую строку фиксированной длины. Например, хеш-функция может принимать строку с любым количеством знаков (одна буква или целое литературное произведение), а на выходе получать строку со строго определенным числом символов (дайджест).

Хеш используется для того, чтобы быстрее отличать одни данные от других без необходимости сравнивать каждый бит этих данных. Достаточно обработать эти данные один раз (вычислить их хеши) и можно сравнивать только их, а это гораздо быстрее. Идея заключается в том, что, если хеши различаются, значит, это совершенно точно разные данные. Если хеши одинаковы, значит, с вероятностью в 99,9% это одинаковые данные. Хотя всегда существует маленький шанс, что данные всё-таки разные, несмотря на одинаковые хеши.

Требования, которые выдвигаются для хеширующего алгоритма (хеш-функции):

1) Одни и те же данные должны давать всегда один и тот же хеш. Это обязательное условие.

2) Разные данные должны давать разный хеш.

Хорошая хеш-функция ведёт себя следующим образом:

1) Весь доступный диапазон хешей используется по максимуму. То есть, если на хеш отведено 32 байта, то разные данные дают максимально разнообразный хеш, который может являться совершенно любой комбинацией битов.

2) Любое, даже самое незначительное, изменение входных данных должно давать другой хеш. Не должно быть такого, что небольшие изменения дают тот же самый хеш. Тот же самый хеш должен возникать в результате какого-то совершенно другого набора данных, чтобы вероятность случайного присутствия двух таких данных (дающих одинаковый хеш) была минимальной.  
 Хеш-функции имеются практически в любом языке программирования. Например, они используются для реализации хеш-таблиц и множеств (HashMap/HashSet в Java, dict и set в Python, Map, Set и объекты в JavaScript и так далее). Отдельная категория хеш-функций – криптографические хеш-функции. К ним предъявляются существенно более строгие требования, чем к функциям, обычно используемым в хеш-таблицах. Поэтому и применяются они в более «серьезных» случаях, например, для хранения паролей. Криптографические хеш-функции вырабатываются и тщательно проверяются исследователями по всему миру.

Для чего нужен хеш. Предположим, есть массив из миллиона разных строк. В каждой строке миллион символов (то есть, всего 1 терабайт = 1000 гигабайт данных). Вам приходит такое указание: добавьте строку, содержащую какую-либо информацию в ваш массив, но только в том случае, если такой строки там ещё нет.

В итоге, задача превращается в посимвольное сравнение миллиона символов в миллионах строк. Очевидно, что данная работа потребует огромное количество ресурсов и времени.

Но если перед записью имеются вычисленные заранее хеши эти строк, то задача превращается в сравнение 32 символов вместо миллиона символов (32 мегабайта данных на весь массив). Если будет обнаружено, что в списке есть точно такой же хеш, то для полной надёжности, можно сравнить посимвольно лишь эту строку.

Хеш-функции в блокчейнах гарантируют «необратимость» всей цепочки транзакций. Дело в том, что каждый новый блок транзакций ссылается на хеш предыдущего блока в реестре. Хеш самого блока зависит от всех транзакций в блоке, но вместо того, чтобы последовательно передавать транзакции хеш-функции, они собираются в одно хеш-значение при помощи двоичного дерева с хешами (дерево Меркла). Таким образом, хеш используются как замена указателям в обычных структурах данных: связанных списках и двоичных деревьях. За счет использования хешей общее состояние блокчейна – все когда-либо выполненные транзакции и их последовательность – можно выразить одним-единственным числом: хешем самого нового блока. Поэтому свойство неизменности хеша одного блока гарантирует неизменность всего блокчейна.

Хеш-деревья имеют много применений помимо блокчейнов. Они используются в файловых системах для проверки целостности файлов, распределенных базах данных для быстрой синхронизации копий и в управлении ключами для надежного журналирования выдачи сертификатов. Git использует обобщение хеш-деревьев – направленные ациклические графы на основе хешей. В блокчейне использование хеш-деревьев продиктовано соображениями производительности, так как они делают возможным существование «легких клиентов», которые обрабатывают лишь малую часть транзакций из блокчейна.

## 1.3 Цифровая подпись

## Цифровая подпись – это последовательность байтов, формируемая путем преобразования подписываемой информации по криптографическому алгоритму и предназначенная для проверки авторства электронного документа.

Цифровые подписи, так же, как и настоящие подписи, – это один из способов доказать, что кто-то является тем, за кого он себя выдает. С учетом того, что в этой ситуации используется криптография и математика, это значительно безопаснее, чем обычные рукописные подписи, которые можно легко подделать.

В асимметричных системах шифрования пользователи генерируют по определенному алгоритму так называемые пары ключей, каждая из которых является открытым ключом (public key) и закрытым ключом (private key).

Открытый и закрытый ключи связаны друг с другом при помощи некоторых математических отношений. Открытый ключ предназначен для распространения публично. Он служит в качестве адреса для приема сообщений от других пользователей, таких как IP-адрес или домашний адрес.

Закрытый ключ хранят в секрете. Он используется в качестве цифровой подписи для сообщений, отправленных другим пользователям. Подпись включается в сообщение, таким образом, получатель может идентифицировать отправителя с помощью его открытого ключа.  
 Цифровые подписи в блокчейне базируются на криптографии с открытым ключом. В ней используются два ключа. Первый – закрытый ключ – нужен для формирования цифровых подписей. Второй – открытый ключ – используется для проверки электронной подписи. Открытый ключ реально вычислить на основе закрытого ключа, а вот обратное преобразование требует невозможного на практике объема вычислений.

Поскольку в блокчейне нет центрального узла, который может авторизовать произвольные транзакции, безопасность системы становится децентрализованной, а вероятность успешного вмешательства в работу блокчейна снижается практически до нуля.

Таким образом, блокчейн использует цифровые подписи для аутентификации и обеспечения целостности транзакций (и иногда блоков). В случае криптовалюты процесс аутентификации означает, что потратить средства может только тот человек, которому они были посланы другой, более ранней, транзакцией. Особенность блокчейна состоит в том, что информация об аутентификации «вшита» в каждую транзакцию, а не отделена от бизнес-логики, поэтому блокчейн считается более защищенным. В обычной системе можно взломать или административно обойти механизм аутентификации и провести манипуляции с бэкэндом, а в блокчейне сделать этого не получится по определению.

## **2 Достоинства технологии блокчейн**

Именно в отсутствии посредников и заключается главное преимущество блокчейна перед обычными банковскими транзакциями. Известно, что сейчас все операции с документами, деньгами или иными данными обязательно проходят через посредников. Государственные органы, банки или нотариусы постоянно следят за подлинностью проделанных операций. Здесь же не имеется центрального органа, поэтому транзакции проверяют все участники системы. Это значительно упрощает процедуру и избавляет от посредников.

Программный код сети доступен любому желающему обратиться к нему, однако личность пользователя и иная персональная информация не раскрывается. Создателям блоков видны только необходимые данные по конкретной операции.

Блокчейн децентрализован, нет какого-то одного общего командного центра, взломав который получится уничтожить все данные о сделке и ее участниках или подменить их.

Например, если проводилась транзакция, в которой участвовали 100 человек, то эта блокчейн-цепочка останется рабочей и доступной для просмотра даже в том случае, если 99 компьютеров других участников будут испорчены. Ведь, по сути, каждое звено блокчейн-цепи – это своеобразный полный бекап данных всех транзакций всех остальных участников на это звено.  
 Взлом одного из таких компьютеров никак не скажется на сохранности данных на остальных (как и на их изменении).

2.1 Основные принципы обеспечения безопасности

Применение шифрования гарантирует, что пользователи могут изменять только те части цепочки блоков, которыми они «владеют» в том смысле, что у них есть закрытые ключи, без которых запись в файл невозможна. Кроме того, шифрование гарантирует синхронизацию копий распределенной цепочки блоков у всех пользователей. В технологию блокчейн изначально заложена безопасность на уровне базы данных. Концепцию цепочек блоков предложил в 2008 г. Сатоши Накамото (Satoshi Nakamoto). Впервые реализована она была в 2009 г. как компонент цифровой валюты – биткоина, где блокчейн играет роль главного общего реестра для всех операций с биткоинами. Благодаря технологии блокчейна биткоин стал первой цифровой валютой, которая решает проблему двойных расходов (в отличие от физических монет или жетонов, электронные файлы могут дублироваться и тратиться дважды) без использования какого-либо авторитетного органа или центрального сервера.  
 Безопасность в технологии блокчейн обеспечивается через децентрализованный сервер, проставляющий метки времени, и одноранговые сетевые соединения. В результате формируется база данных, которая управляется автономно, без единого центра. Это делает цепочки блоков очень удобными для регистрации событий (например, внесения медицинских записей) и операций с данными, управления идентификацией и подтверждения подлинности источника.

Блокчейн-технология имеет встроенную устойчивость к ошибкам. Это служит хорошим предзнаменованием для блокчейн-технологии, которая продолжает развиваться. Как бы революционно это ни звучало, блокчейн действительно представляет собой механизм, обеспечивающий высшую степень учета и идентификации. Больше не будет пропущенных транзакций, ошибок человека или машины, или даже изменений, сделанных без согласия вовлеченных сторон. А наиболее важно то, что блокчейн помогает гарантировать законность транзакции путем записи её не только в главном реестре, а в распределённой системе реестров, связанных через защищенный механизм проверки.

2.2 Сферы применение технологии в реальной жизни

Неизменные и верифицированные данные, прозрачность правоотношений, быстрота и удобство сервиса – все эти причины стали поводом для того, чтобы крупный бизнес обратил внимание на эту перспективную технологию. Как прогнозирует J’son & Partners Consulting, первые кандидаты на внедрение блокчейна – финансовая сфера, телеком, транспорт, промышленность и агропромышленный комплекс.

Кстати, банки понимают все перспективы блокчейн и активно начинают использовать его. Например, в России создание блокчейн-платформ тестируют Сбербанк, банки Тинькофф, Открытие, Альфа и платежная система Qiwi. Технические решения на основе блокчейн разрабатывает ЦБ. Есть первые тестовые транзакции.

Несмотря на то, что интерес к Блокчейн-технологии в большей степени связан скорее с областью финансов, сферы применения технологии распределенных реестров не ограничиваются только ей. Наряду с банками, игроки других, не связанных с финансовой отраслью рынков, также обратили внимание на технологию и ищут способы извлечения пользы из возможностей, которые она предоставляет. Рассмотрим некоторые примеры практических применений технологии блокчейн, существующие за рамками сферы финансовых услуг.

## 2.2.1 Блокчейн в медицине

Практически во всех сферах, где можно использовать блокчейн, он выполняет роль универсального хранилища данных, которое практически невозможно взломать и изменить. Кроме того, доступ к этим данным может получить любой пользователь, обладающий соответствующими правами.

Медицина является одной из сфер, где хранение и обработка данных является одним из ключевых факторов. От того насколько быстро врачи получат результаты обследования или историю болезни, может зависеть здоровье, и даже жизнь пациента. Блокчейн-технологии позволяют заносить в карту пациента все данные, а доступ к ним смогут получить, при необходимости, даже врачи другого города или страны (например, если пациент был вынужден обратиться в медучреждение во время отдыха или командировки).

В медицине и ранее использовались механизмы хранения данных в электронном виде, но они были ограничены одной системой. Врачи одной страны могли зайти на внутренний интернет ресурс и получить нужные сведения, или добавить новые данные, однако иностранные коллеги не имели доступа к этой базе. С применением блокчейна специалистов из других стран можно без всяких опасений допустить на внутренний ресурс, предварительно ограничив доступы рамками необходимого.

### 2.2.2 Энергетика

Основатели “Energy Blockchain Labs” утверждают, что компания представляет собой единственное в мире предприятие, деятельность которого целиком посвящена полному циклу создания добавленной стоимости в энергетической отрасли. Будучи основанной в 2016 году тремя опытными специалистами в области энергетики, финансов и информационных технологии, лаборатория работает над революционными решениями, в числе которых есть совместные с другими компаниями проекты, нацеленные на разработку ряда энергетических интернет-технологий на базе Блокчейн и решение задач в области выработки и потребления энергии, торговли, управления ей и других.

### 2.2.3 Недвижимость

“UBITQUITY” предлагает риелторским, ипотечным и проверяющим компаниям услуги собственной блокчейн-платформы для ведения записей об имуществе и связанных с ним правах собственности. Платформа позиционируется как параллельная альтернатива унаследованной бумажной системе ведения сделок, позволяющая ускорить процесс юридического аудита недвижимости, повышения прозрачности сделок и доверия с помощью полной децентрализации.  
 “Silvertown” помогает жилищно-строительным ассоциациям и крупным управляющим компаниям следить за физическим состоянием имущества с помощью технологий умного дома. Полученная от умных маячков и датчиков информация передается и хранится в блокчейн, что позволяет гарантировать целостность данных и неприкосновенность частной жизни съемщиков.

### 2.2.4 Интернет вещей

“Chronicled” – компания из Сан-Франциско, запустившая в августе перспективную блокчейн-платформу для Интернета вещей, нацеленную на улучшение потребительского опыта. В рамках проекта Ethereum-блокчейн хранит идентификационные данные физических предметов, таких, как потребительские товары и предметы коллекционирования. Это позволяет создавать безопасные и совместимые со множеством других систем цифровые идентификаторы, что открывает возможности для новых механизмов взаимодействия с потребителем, основанные на отслеживании его близости к предмету.

### 2.2.5 Видеоигры

Блокчейн нашел своих поклонников даже в индустрии видеоигр.  
 “Etheria” – виртуальный мир, где игроки стараются завладеть ячейками игрового поля, добывая их за блоки, и что-нибудь на них построить. Все данные, описывающие мир и его состояние, равно как и все действия игроков хранятся в децентрализованном Ethereum-блокчейне.

“First Blood” – платформа, позволяющая киберспортсменам бросать друг другу вызов в различных игровых дисциплинах, фанатам – делать ставки или судить игры, а также организовывать турниры и получать вознаграждение от любой подобной деятельности. First Blood работает на базе Ethereum-блокчейна с собственным токеном 1ST, активно применяя умные контракты для обработки результатов и оракулов в качестве источника информации о результатах матчей.

2.2.6 Блокчейн в России

В настоящее время в России тестируется и функционирует большое количество проектов, основанных на технологии Блокчейн, вот лишь некоторые примеры:

Национальный расчетный депозитарий России использует блокчейн-технологии в процедуре электронного голосования держателей ценных бумаг.

В компании «33 слона» такие цепочки обеспечивают документооборот между участниками купли-продажи недвижимости.

Агрегатор предложений от страховых компаний Prosto.Insure записывает в блокчейн-базу данные о проданных страховках.

«Альфа-банк» и авиакомпания S7 Airlines продают авиабилеты при помощи Ethereum, сократив время проведения транзакции с 14 дней до 23 секунд.

С начала 2017 года «Сбербанк» и «М. Видео» используют блокчейн-технологии в факторинговых операциях: если раньше обмен информацией в рамках каждой сделки осуществлялся через письма и телефонные звонки и занимал до трех дней, то теперь этот срок сократился до нескольких часов.

3. Разработка приложения blockchain

Перейдем к разработке собственного blockchain, для этого будет использоваться язык программирование Python 3.6.

Разобьем процесс разработки ПО на несколько этапов:

1. Создание блокчейна.
2. Свой блокчейн в качестве API
3. Взаимодействие с созданным блокчейном

Этап 1: Создание блокчейна.

Создадим класс Blockchain, конструктор которого будет создавать изначально пустой список (для хранения нашего блокчейна), и еще один для хранения транзакций. Ниже приведен код создания класса:



Рисунок 1 – Создание класса blockchain

Класс blockchain отвечает за управление цепочкой. В нем будут храниться транзакции и некоторые вспомогательные методы для добавления блоков в цепочку.

Что из себя представляет блок?

Каждый блок содержит в себе индекс(index), временную метку (timestamp), список транзакций (sender – отправитель, recipient – получатель, amount - количество), доказательность (proof) и хэш предыдущего блока(previous\_hash).

Далее приведен пример того, как выглядит отдельный блок:

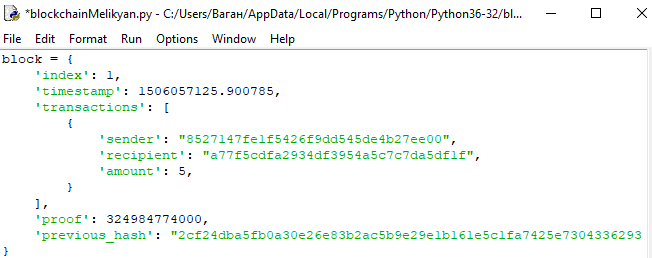


Рисунок 2 – Создание блока внутри blockchain

На данном этапе идея цепочки следующая – каждый новый блок внутри себя содержит хэш предыдущего блока. Именно **наличие предыдущего хэша** является решающим фактором, который делает **блокчейн неизменяемым**.

# Добавление транзакций в блок.

Нам необходим способ добавлений транзакций в блок. За это будет отвечать метод new\_transaction():

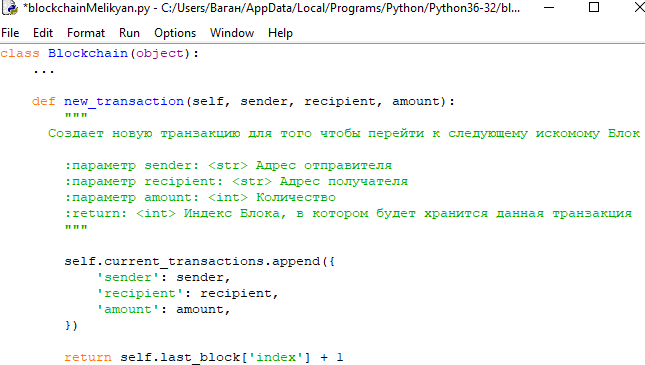


Рисунок 3 – Создание метода new\_transaction

После того, как метод добавил транзакцию в список, он возвращает индекс блока, в который будет добавлена транзакция – следующий искомый блок.

Созданный блокчейн необходимо заполнить исходным блоком – блок у которого нет предшественников. Также необходимо добавить «proof» в исходный блок, который является результатом анализа (или алгоритма «доказательство выполнения работы»).

Кроме этого, для создания исходного блока в конструкторе, необходимо добавить следующие методы: new\_block(), new\_transaction() и hash():

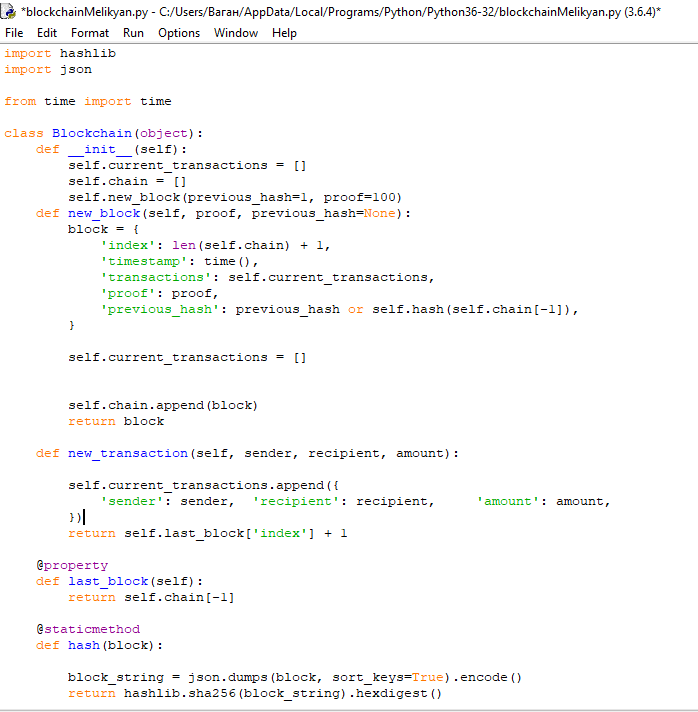


Рисунок 4 – создание исходного блока

# Что такое алгоритм «Доказательство выполнения работы?

Алгоритм «Доказательство выполнения работы» (Proof of work или сокращенно PoW) – это процесс создания новых блоков в блокчейне. Целью алгоритма PoW является нахождение такого числа (метки), которое будет решать проблему. Число должно быть таким, чтобы его было **сложно найти и легко проверить**. Основная идея данного алгоритма в том, что не важно кем в сети это может быть сделано.

# Этап 2: Свой блокчейн в качестве API.

Для последующей работы понадобится фреймворк Flask он позволяет обращаться к нашему блокчейну за счет веб-соединения с помощью HTTP-запросов.

Настраиваем Flask для того, чтобы реализовать свой блокчейн.

Наш «сервер» будет формировать одиночный узел в нашей блокчейн-сети.



Рисунок 5 – Настройка фреймворка Flask

Endpoint для транзакций.

Ранее были созданы методы для класса, отвечающие за добавление транзакции в блок, сейчас нужно создать функцию, которая будет добавлять транзакции:

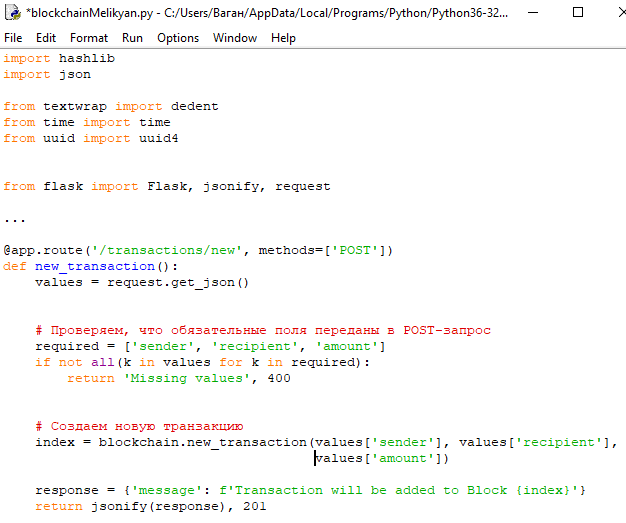
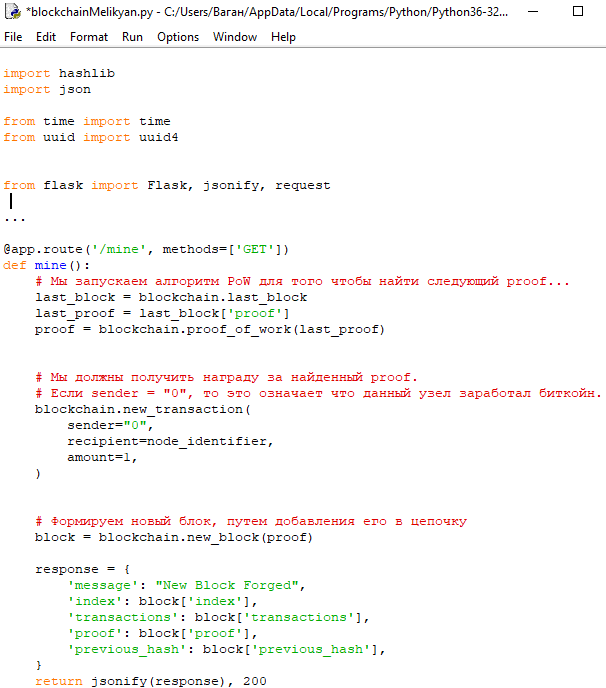


Рисунок 6 – Endpoint для транзакций

## Endpoint для майнинга.

## Endpoint майнинга отвечает за три следующих задачи:

1. Расчет алгоритма PoW.
2. Майнер(ы) получают награду в виде транзакции, которая гарантируем им 1 биткойн.
3. Формирование нового блока, путем его добавления в цепочку.



## Рисунок 7 – Endpoint для майнинга

На данном этапе была закончена подготовка нашего блокчейна и теперь можно начать взаимодействовать с ним.

Этап 3: для взаимодействия с нашим Blockchain через сеть воспользуемся программой Postman, для начала работы запустим сервер



Рисунок 8 – запуск сервера

Для того, чтобы смайнить новый блок необходимо воспользоваться запросом типа GET на http://localhost:5000/mine:

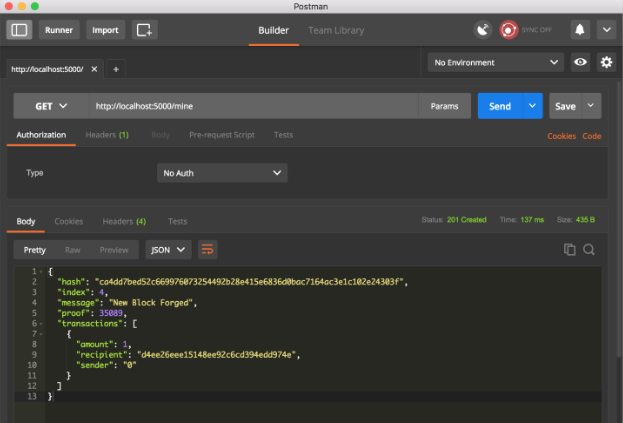


Рисунок 9 – Get-запрос

Далее создадим новую транзакцию с помощью POST-запроса на http://localhost:5000/transactions/new с телом, содержащим структуру нашей транзакции:

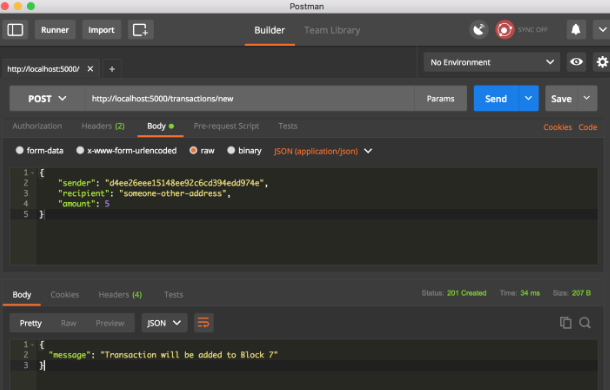


Рисунок 10 – Post-запрос

На экране появилось сообщение «Transaction will be added to Block 7», которое подтверждает успешное добавление транзакции.

Созданный Блокчейн, позволяет принимать транзакции, тем самым позволяя нам майнить новые Блоки, выполняя основную задачу базового блокчейна.

ЗАКЛЮЧЕНИЕ

«Блокчейн – это та технология, которая имеет шанс перевернуть сферу государственного регулирования, сферу государства в целом, финансы – все до одной сферы», – заявил в конце января 2016 г. на совещании у Владимира Путина президент и председатель правления Сбербанка Герман Греф.

Именно в данной высказывании заключается основной результат изучения технологии blockchain.

Вполне возможно, что сейчас наступил тот момент, когда блокчейн обкатывается на дорогах общего пользования, и внедряется в наиболее важные отрасли жизни.

Новые проекты на блокчейне будут основываться на его главных преимуществах – открытости, защищенности, безопасности.

Именно поэтому блокчейн станет хорошим подспорьем для любых сервисов, где пользователи могли переживать о возможном мошенничестве или о сохранности данных.

В курсовой работе были рассмотрены различные сферы применения и способы использования данной технологии, помимо банковского дела.

В разработанном, на языке программирования Python, программном обеспечении созданы различные методы и классы, для работы с блокчейном. Реализована возможность добавления транзакций, добавление алгоритм “Pow” (алгоритм «Доказательство выполнения работы»).

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Натаниэль Поппер. Цифровое золото. Невероятная история биткойна, или О том, как идеалисты и бизнесмены изобретают деньги заново, Вильямс, 2016, 386с.
2. Мелани Свон. Блокчейн. Схема новой экономики, Олимп- Бизнес, 2017, 240с.
3. Дон Тапскотт, Алекс Тапскотт. Блокчейн-революция. Как технология, стоящая за биткойном, меняет деньги, бизнес и мир, Эксмо, 2017, 448с.
4. Артем Генкин, Алексей Михеев, Блокчейн. Как это работает и что ждет нас завтра, Альпина Паблишер, 2018, 592с.
5. Уильям Могайар. Блокчейн для бизнеса, Эксмо, 2017, 349с.