МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«**КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**»
(**ФГБОУ ВО «КубГУ»**)

Кафедра информационных технологий

КУРСОВАЯ РАБОТА

РАЗРАБОТКА ПРИЛОЖЕНИЯ НА ОСНОВЕ ТЕХНОЛОГИИ BLOCKCHAIN

Работу выполнил_____ А. С. Горенко
(подпись, дата)

Факультет компьютерных технологий и прикладной математики курс 3

Специальность 02.03.03 - «Математическое обеспечение и администрирование информационных систем»

Научный руководитель
доц., канд. физ-мат. наук. _____В. В. Подколзин
(подпись, дата)

Нормоконтроллер
ст. преп. _____ А. В. Харченко
(подпись, дата)

Краснодар 2017

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Данная курсовая работа посвящена изучению технологии Blockchain и разработке данной технологии на языке программирования Java.

В настоящий момент криптовалюты и технология блокчейн, на которой они основаны повсеместно привлекают к себе много внимания.

Несмотря на то, что интерес к Блокчейн-технологии в большей степени связан 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.

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 система защиты, которую практически невозможно взломать.

Благодаря этому изучение технологии Blockchain приобретают особую актуальность.

Цель: изучить технологию Blockchain и разработать программное обеспечение.

Задача: разработать программное обеспечение на языке программирования Java, которое будет выполнять все основные операции, соответствующие технологии Блокчейн.

1 История создания технологии Блокчейн

Последние 50 лет мировой истории были ознаменованы бурным развитием финансово-банковской сферы, предопределившим возникновение электронных денег.

В 1983 Стефан Брэндс и Дэвид Чаум первыми предложили идею использования электронной валюты и даже описали её концепцию.

Следующий существенный взнос в формирование концепции цифровых валют был сделан только в 1997 году Адамом Баков. Именно он предложил использовать систему Hashcash, которая должна была справляться с DoS-атаками и противодействовать отправке спама. Именно эта система стала основой в создании блоков в цепочке блокчейна, а значит, позволила работать с первой криптовалютой в мире.

Первая успешная реализация цифровой цифровой валюты была создана Вэй Дай в 1998 году и получила название b-money. Следующей попыткой стал Bit Gold, разработанный Ником Сабо в 2000 году. Обе валюты обладали большим недостатком — несовершенством системы принятия решения среди удаленных абонентов.

В 2008 году Сатоши Накамото, собрав воедино наработки единомышленников, выложил в открытый доступ научную работу с описанием основных элементов блокчейна, принципов работы и математической модели сети. Нововведения этой технологии решают проблему принятия решений и обеспечивают безопасность и работоспособность сети. Это позволило в 2009 году создать первую полноценную криптовалюту — Bitcoin.

2 Устройство работы технологии Blockchain

Блокчейн (от англ. «Blockchain» - цепочка блоков) – это выстроенная по определённым правилам непрерывная последовательная цепочка блоков, хранящих некоторые данные, которая реплицируется на каждый из компьютеров, объединенных в одноранговую(пиринговую) сеть[2]. Данными могут быть денежные транзакции, умные контракты либо любая другая информация нуждающаяся в независимой записи и проверке.

Члены данной одноранговой сети — это анонимные лица, называемые узлами. Все коммуникации внутри сети используют асимметричную систему шифрования и хеширование, чтобы надежно идентифицировать отправителя и получателя. Когда один из узлов хочет добавить данные в блокчейн, в сети формируется новый блок и при помощи алгоритма консенсуса добавляется в цепь.

2.1 Одноранговые(пиринговые сети) сети.

На современном рынке IT-систем существует два типа архитектур компьютерных сетей: клиент-серверная сеть (рисунок 1) и одноранговая (пиринговая) сеть (рисунок 2).

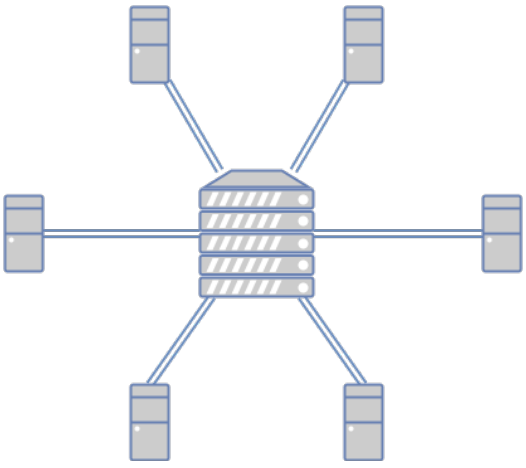


Рисунок 1 – Сеть с клиент-серверной архитектурой.

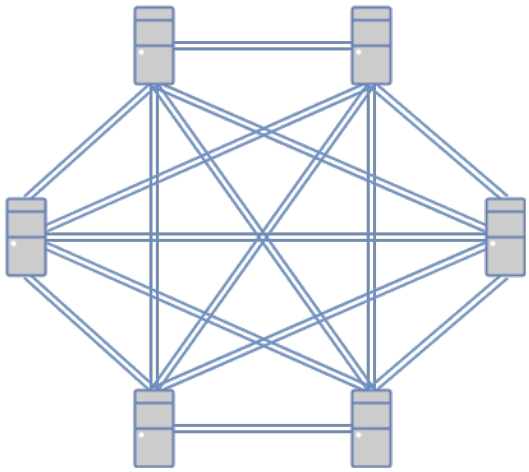


Рисунок 2 – Одноранговая сеть

Сеть с клиент-серверной архитектурой подразумевает централизованный контроль данных и доступа. Вся системная логика и информация скрыты внутри сервера, что позволяет снизить требования к производительности клиентских устройств и обеспечить высокую скорость обработки данных, но такая сеть обладает низкой отказоустойчивостью.

В основе технологии блокчейн лежат одноранговые или децентрализованные сети. Такая сеть не имеет главного устройства, и все участники имеют равные права. В такой модели каждый пользователь является не только потребителем, но и сам становится поставщиком сервиса.

Преимуществом такой системы является доступность данных: нет единой точки точки отказа, как в случае с базой данных, расположенной на одном сервере и высокая отказоустойчивость: при прекращении функционирования одного или нескольких узлов работоспособность сети не нарушается.

2.2 Структура блока

Технология блокчейн предполагает использование распределенной базы данных состоящей из цепочки блоков, представляющей собой связный список, в котором каждый блок содержит идентификатор предыдущего.

Для идентификации каждого блока используется хеш, создаваемый при помощи криптографической функции.

Хеширование — это преобразование массива входных данных произвольной длинны в (выходную) битовую строку установленной длины, выполняемое определённым алгоритмом. Криптографическая функция, воплощающая алгоритм и выполняющая преобразование, называется хеш-функцией. В качестве параметра хеш-функции может быть передана строка любой длинны (одна буква или целое литературное произведение), а результатом её работы всегда будет битовая строка строго фиксированной длины.

Все хеширующие функции должны отвечать следующим требованиям:

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.

На практике возможны случаи, при котором хеш-функция преобразует несколько разных сообщений в одинаковые сводки - это называется коллизией. Вероятность возникновения коллизий используется для оценки качества хеш-функций и должна стремиться к минимуму.

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.

Каждый блок состоит из заголовка и списка транзакций представленных, корнем хеш-дерева Меркла. Заголовок блока включает в себя свой хеш, хеш предыдущего блока и дополнительную служебную информацию (рисунок 3).

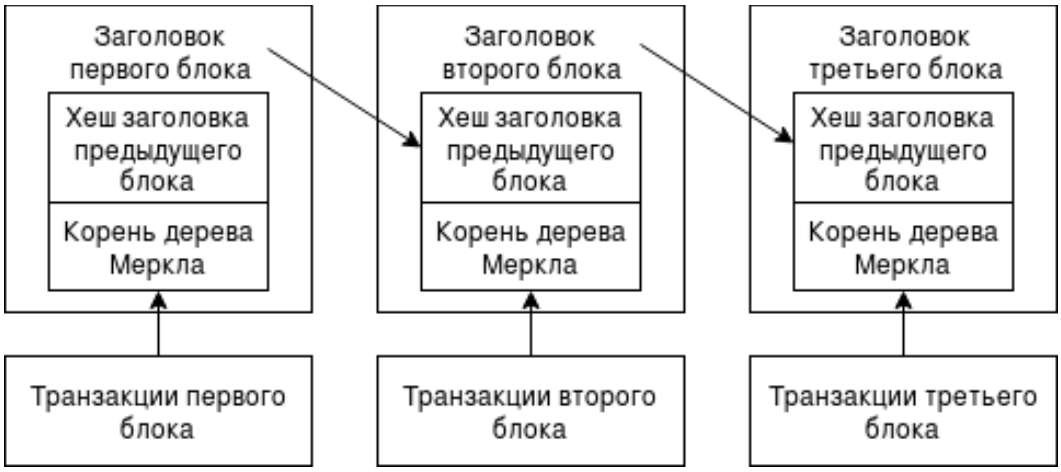


Рисунок 3 — Связный список блоков

Дерево Меркла (Merkle tree) или бинарное дерево хэшей — это двоичное дерево, конечные узлы которого — это хеши транзакций, а внутренние

вершины — результаты сложения значений связанных вершин[3] (Рис. 4).

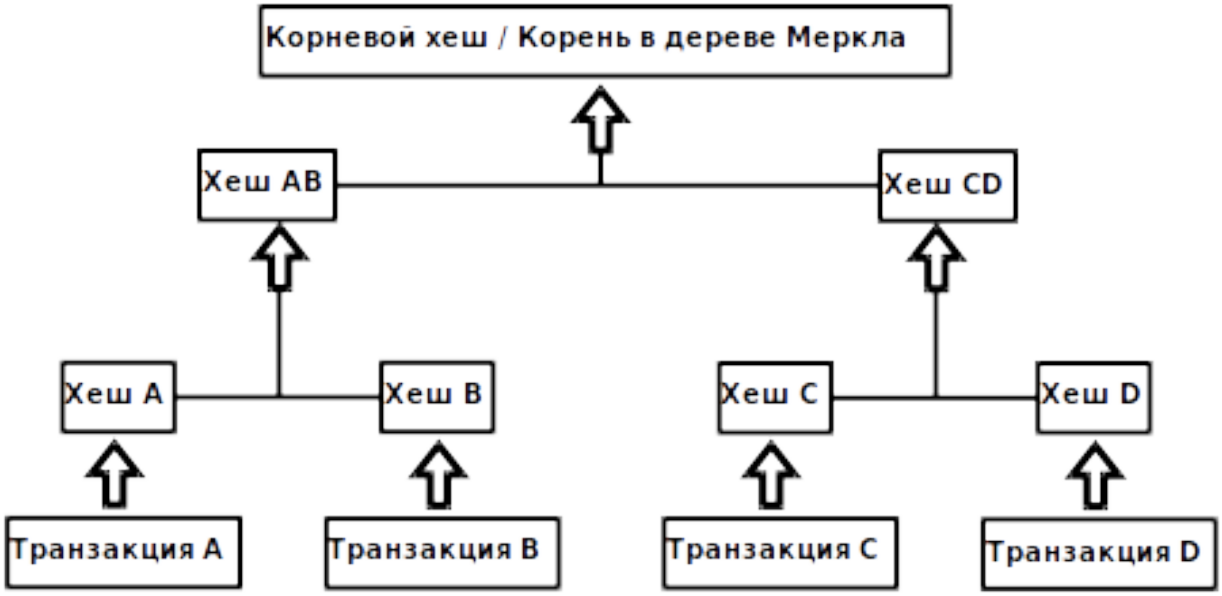


Рисунок 4 - хеш-дерево Меркла

Следует отметить, что поскольку дерево бинарное, то на каждом шаге должно быть четное число элементов. Поэтому если, на каком-то этапе количество хешей нечетное, то последний хеш дублируется для получения пары.

Преимущества такого алгоритма хеширования перед хешированием всех транзакций разом, объединённых в один большой блок данных, состоит в том, что он обеспечивает не только доказательство подлинности каждой отдельной транзакции, но и делает невозможным внесение изменения в порядок транзакций. Так как при перемещении транзакции с её законного места изменится вся ветвь хешей и корень в дереве Меркла.

Список транзакций для внесения в новый блок, формируется участниками сети из очереди необработанных транзакций, ещё не записанных в предыдущие блоки.

2.3 Структура транзакции

Идентификатором транзакции является её хеш (TXID), который строится на основе состава транзакции. Каждая транзакция включает в себя таблицу входов, таблицу выходов, цифровую подпись отправителя, публичный ключ

получателя и количество средств для перевода (рисунок 5).

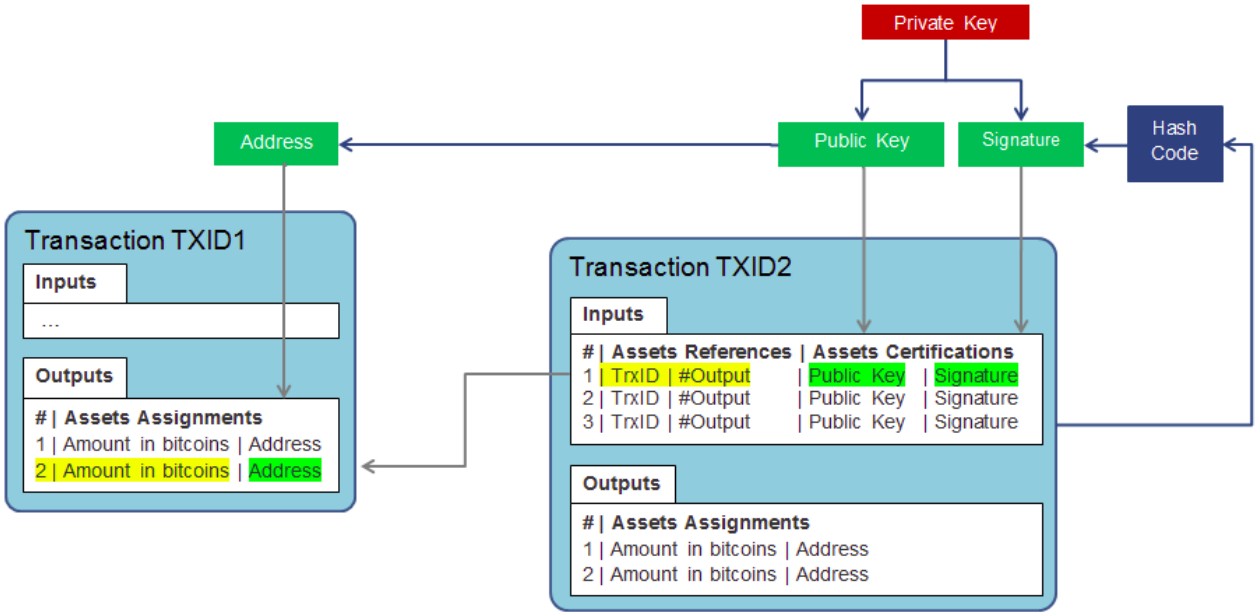


Рисунок 5 — структура транзакции

2.3.1 Цифровые подписи

Цифровая подпись является альтернативой рукописной подписи и предназначена для проверки авторства электронных документов. Такая подпись представляет собой последовательность байтов, формируемую путем преобразования подписываемой информации по криптографическому алгоритму.

Цифровые подписи в блокчейне формируются на основе асимметричной системы шифрования, в которой для каждого пользователя по определенному алгоритму генерируется так называемые пары ключей, состоящие из открытого (публичного) и закрытого (частного) ключей[1].

Открытый ключ предназначен для распространения публично. Он служит в качестве адреса для приема сообщений от других пользователей.

Закрытый ключ хранят в секрете. Он используется в качестве цифровой подписи для сообщений, отправленных другим пользователям.

При отправке сообщения отправитель шифрует информацию с помощью

открытого ключа адресата. Расшифровать это секретное сообщение получатель может только, используя закрытый ключ из пары с открытым, которым оно было зашифровано. В то же время сообщение зашифрованное закрытым ключом отправителя, может быть расшифровано только при помощи соответствующего открытого ключа из пары с закрытым.

Открытый и закрытый ключи связаны друг с другом при помощи некоторых математических отношений. Открытый ключ реально вычислить на основе закрытого ключа, а вот обратное преобразование требует невозможного на практике объема вычислений.

Таким образом, асимметричное шифрование используется в блокчейне для аутентификации отправителей и обеспечения целостности транзакций.

2.3.2 Входы и выходы транзакций

В существующих банковских системах, транзакции представляют собой редактирование единой таблицы балансов вида <адрес, баланс> с помощью некоторого центрального регулятора.

В системе на основе блокчейна процесс перевода средств выглядит совершенно иначе - не существует никакой единой структуры, в которой каждому адресу был бы сопоставлен его текущий баланс. Вместо этого вся информация о транзакциях хранится в цепочке блоков. Это означает, что если пройти по всему блокчейну, то можно вычислить количество средств принадлежащих конкретному адресу.

Перевод средств от получателя к отправителю осуществляется за счёт таблиц входов и выходов.

Каждый вход в таблице входов представляет собой ссылку на выход другой транзакции, которая когда-либо была отправлена адресанту перевода.

Выход транзакции представляет собой идентификатор адресата перевода и количество переведённых средств.

Выходов может быть несколько, это позволяет разделить сумму входов,

между несколькими получателями. Это очень важное свойство т.к. использовать каждую транзакцию в качестве входа можно только один раз.

В том случае когда сумма входов транзакции больше чем сумма выходов разница либо помещается в отдельный выход, адресуемый отправителю средств, либо становится комиссией за транзакцию (transaction fee).

Рассмотрим пример транзакции с двумя входами и двумя выходами изображённой на рисунке 6.

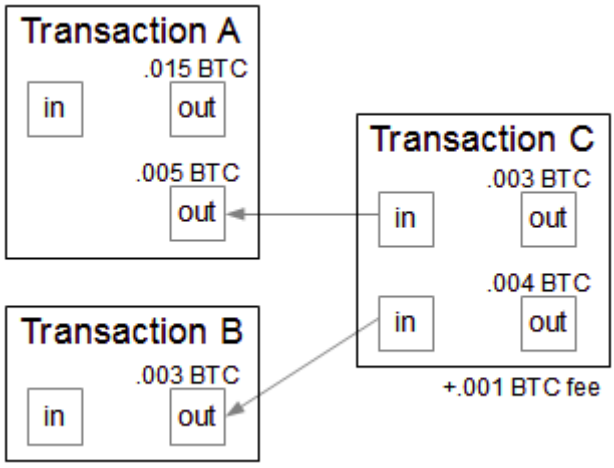


Рисунок 6 — транзакция с двумя входами и двумя выходами

В данном примере создается новая транзакция C, которая ссылается на два выхода — A и B. В результате на входе у транзакции получается 0.008 BTC, которые потом разделяются на два выхода — на первый адрес отправляется 0.003 BTC, а на второй 0.004 BTC. Разница в 0.001 BTC помещается в комиссию за транзакцию.

Транзакция считается исполненной, как только она будет занесена в блокчейн. Для этого она должна пройти верификацию при добавлении в очередной блок, а блок должен быть добавлен в цепочку. Выходы исполненной транзакции могут быть использованы в качестве входов новых транзакций, тем самым создавая цепочку передачи прав собственности, по мере того, как ценность перемещается от адреса к адресу. Такие, пока еще непотраченные выходы, имеют специальное название — UTXO (unspent transaction output).

Добавление транзакциий в очередной блок осуществляется майнерами.

2.4 Добавление блоков в цепочку. Майнинг.

При создании транзакции пользователем, перед добавлением в блок, она помещается в список необработанных транзакций (рисунок 7).

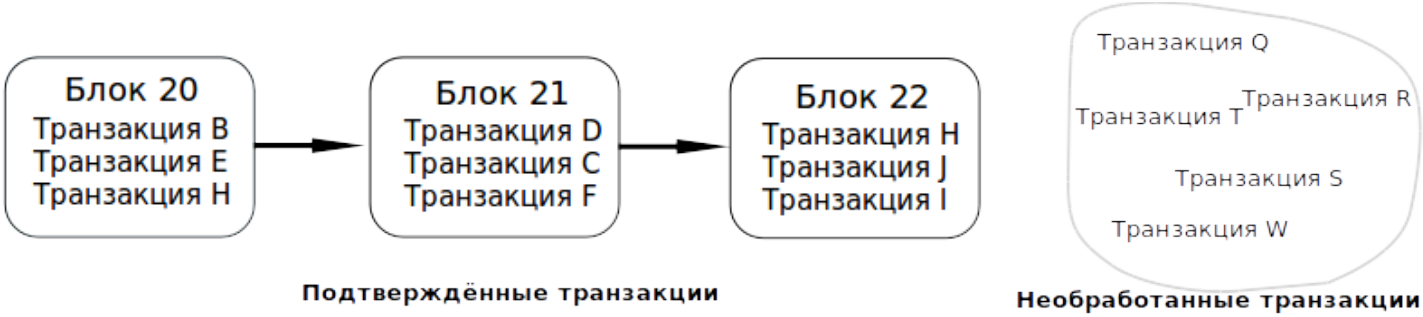


Рисунок 7 — необработанные транзакции

Затем некоторые узлы сети создают новые локальные блоки включающие в себя необработанные транзакции. Такие узлы называются майнерами.

Блок будет сформирован, когда в него будет добавлен достаточный объём транзакций. Объём транзакций для блока регламентируется не количеством транзакций, а их объёмом, который зависит от количества входов и выходов в транзакции.

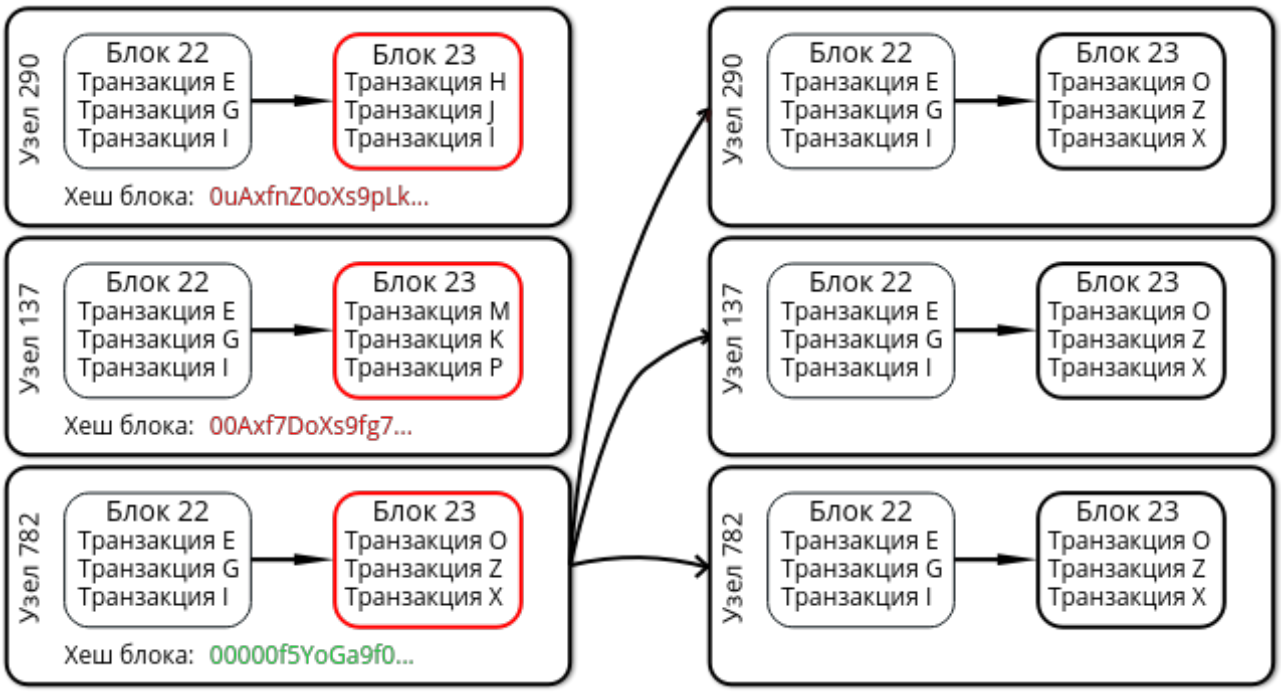
После завершения формирования блока майнер начинает майнинг блока.

Процесс майнинга заключается в повторении хеширования исходных данных блока до тех пор, пока полученный хеш не будет содержать определённое количество ведущих нулей.

Так как результатом работы хеш-функции на одних и тех же данных будет всегда один и тот же хеш, в каждый блок включают ничего не значащее поле «Nonce», которое содержит ничего не значащее число. После каждой неудачной попытки хеширования параметр «Nonce» увеличивается на единицу, либо подбирается случайным образом.

Множество майнеров каждую секунду, перебирают тысячи случайных хешей, чтобы сформировать новый блок (рисунок 8).

Рисунок 8 — майнинг блоков со сложностью, равной 5



Когда один из майнеров подбирает хеш, новый блок отсылается всем узлам сети, которые проверят действителен ли блок, проверив все содержащиеся в нём транзакции, и добавят его в свою копию блокчейна. В качестве награды за майнинг на адрес майнера, подобравшего хеш автоматически формируется, транзакция, с вознаграждением.

Награда за майнинг состоит из вознаграждения за «добычу» блока, которое определённого в системе и суммы комиссий всех транзакций входящих в блок. Время появления нового блока регулируется сложностью хеширования — необходимым количеством ведущих нулей в хеше. Сложность подбирается системой так, чтобы новый блок появлялся примерно раз в 10 минут и увеличивается пропорционально суммарной вычислительной мощности всех майнеров сети.

2.4.1. Непреднамеренное разветвление цепи

Не смотря на высокую сложность хеширования возможна ситуация, когда два майнера одновременно добавляют действительные блоки в блокчейн. В таком случае часть узлов может принять один действительный блок, а другая

часть другой действительный блок и возникнет два разных состояния блокчейна (рисунок 9) в одно и то же время. Такая ситуация называется непреднамеренной развилкой.

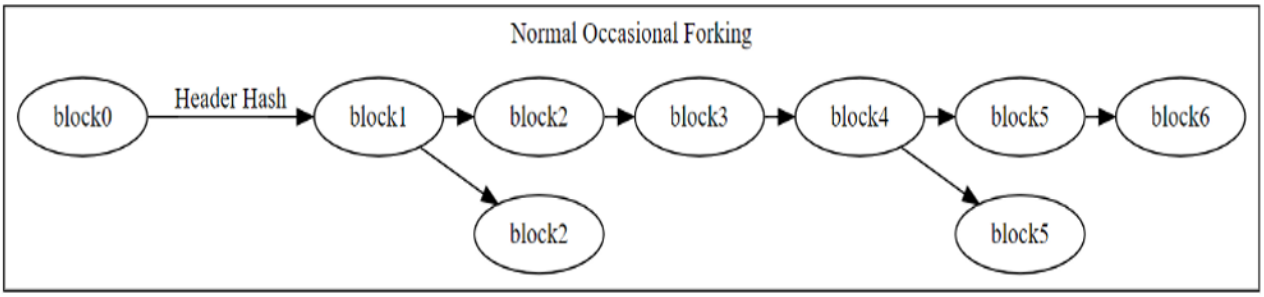


Рисунок 9 — непреднамеренная развилка

Подобную проблему все консенсусные протоколы решают с помощью простого правила: выигрывают самые длинные цепочки.

Когда случается непреднамеренное разветвление, некоторые майнеры начнут добывать новые блоки в одной цепочке, а другие начнут добычу в другой цепочке. Неизбежно, одна из цепочек будет иметь больше майнеров, чем другая, и соответственно будет быстрее добавлять новые блоки в свою цепочку. Остальные майнеры перейдут к более длинной цепи, и рост ответвленной цепи прекратится. При этом основной цепочке не будет нанесен ущерб.

В редких случаях, ответвлённая цепь может обладать значительным количеством ресурсов для добычи (рисунок 10).

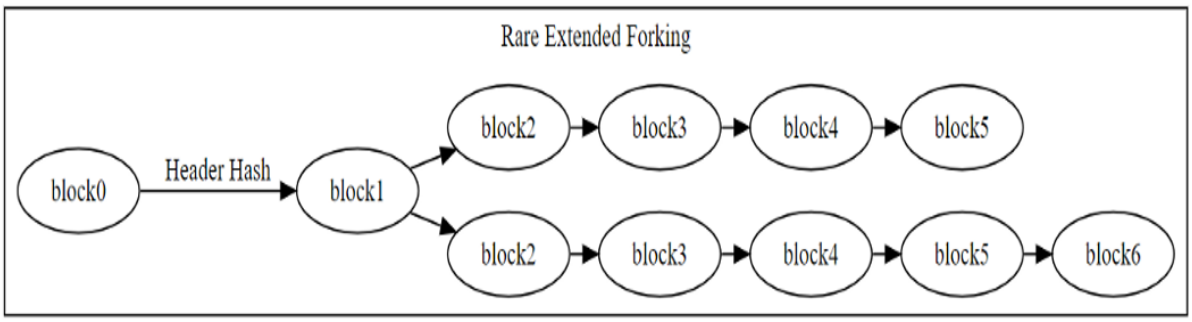


Рисунок 10 — редкий случай непреднамеренного разветвления

В этом случае может потребоваться некоторое время, прежде чем станет ясно, какая из ответвленных цепей является основной цепью.

Из-за возможности возникновения подобной ситуации, в блокчейне определён параметр, называемый необходимой глубиной блока. Этот параметр определяет необходимое количество блоков, которые должны быть добавлены после текущего, чтобы транзакции в этом блоке считались исполненными.

Правило, согласно которому побеждает самая длинная цепь, в сочетании с тем фактом, что требуется огромная вычислительная мощность для добавления блоков в цепочку, делает блокчейн невероятно безопасным. Практически единственный способ атаковать сеть — это вернуться к какому-либо блоку в блокчейне, и начать формировать с него новую цепочку блоков. Однако, для этого злоумышленнику понадобится вычислительная мощность, большая чем вся объединенная сеть майнеров.

3 Реализация технологии блокчейн

3.1. Обзор аналогичных продуктов

На данный момент самой популярной пиринговой платёжной системой, основанной на технологии блокчейн является Биткойн. Данная система очень безопасна и обеспечивает надёжное исполнение транзакций, но она обладает рядом недостатков, как со стороны обычных пользователей, желающих использовать Биткойн только для передачи транзакций, так и со стороный майнеров.

Одним из основных недостатков данной системы является длительное время ожидания исполнения транзакции. Это связано с маленькой скоростью добавления блоков в цепочку - 1 блок в 10 минут. Так как для подтверждения транзакции находящейся в опредённом блоке необходимо, чтобы глубина этого блока была равна, как минимум 2, то транзакция в сети биткоин подтверждается в срок от 15-20 минут до часа.

Ещё одним недостатком системы биткойн является использование в качестве криптографической хеш-функциии, функции SHA-256, разработанной в 2009 году агентством национальной безопасности США. Простота функции SHA-256 позволяет создать аппаратные решения, которые будут выполнять вычисления хеша гораздо эффективнее, чем на обычном компьютерном процессоре (CPU). Это привело к появлению специального дорогостоящего оборудования для майнинга, основанного на микросхемах ASIC - интегральных схемах специального назначения (англ.: «ASIC - Application Specific Integrated Circuit»). Использование такого оборудования для майнинга привело к концентрации больших вычислительных ASIC-мощностей в отдельных узлах сети Биткойн и сделало невозможным майнинг для простых пользователей. Это приводит уменьшению децентрализации сети, что противоречит философии технологии блокчейн.

3.2. Описание концепции разрабатываемого программного обеспечения

Концепция Ставится задача разрабатываемого программного продукта представляет собой настольное приложение, реализующее технологию блокчейн и уменьшающее выявленные недостатки аналогичных продуктов.

Для решения проблемы связанной с уменьшением децентрализации сети из-за большой концентрации вычислительной ASIC-мощности у отдельных узлов цепи было решено использовать в качестве криптографиччеcкой функции адаптивную хеш-функцию SCrypt, разработанную в 2012 году Колином Персивалем. Функция хэшинга SCrypt специально разрабатывалась с целью усложнить аппаратные реализации путем использования значительных объёмов пямяти со случайным доступом, например ОЗУ компьютеров. По причине высоких требований к памяти ASIC-оборудование не будет так же эффективно для майнинга. Вычислительная мощность в такой сети будет распределена более равномерно, среди её узлов, благодаря чему система останется децентрализованной.

Для сокращения времени исполнения транзакций скорость добавления нового блока в систему была уменьшена до 2 минут, но для предотвращения ошибки двойных трат и сохранения безопасности цепи минимальная глубина блока для исполнения транзакции, находящейся в этом блоке будет равна 5. Это позволит сократить минимальное время подтверждения транзакции до 10-12 минут.

3.2.1 Выбор архитектуры сети

Сеть в системе блокчейн может насчитывать тысячи компьютеров. Полная децентрализация такой сети приведёт к сложностям в управлении ими. Поэтому для разрабатываемого приложения предлагается гибридная архитектура сети (рисунок 11).

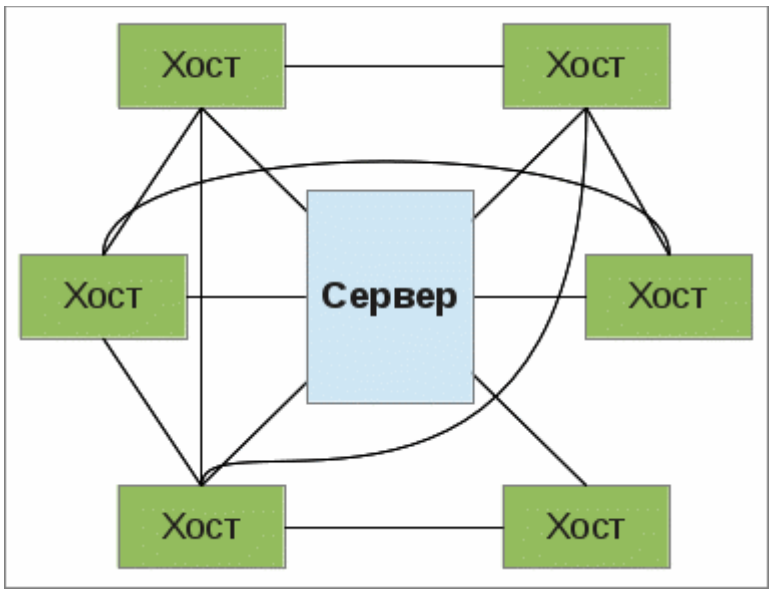


Рисунок 11 –

Гибридная сеть

Координационный сервер выполняет задачи контроля за состоянием сети и предоставления списка активных участников сети.

3.2.2 Описание основных модулей программы

Функционал разрабатываемого приложения состоит из следующих модулей:

- Модуль User interface обеспечивает передачу информации между пользователем и программными компонентами приложения.

- Модуль Blockchain core отвечает за выполнение всех основных операций, описанной во 2й главе технологии блокчейн.

- Модуль Serialization отвечает за сериализацию данных для передачи и приёма данных в сети.

- Модуль P2PServer выполняет основные функции по обработке и приёму данных от других узлов сети.

- Модуль P2PClient отвечает за отправку данных всем активным участникам сети.

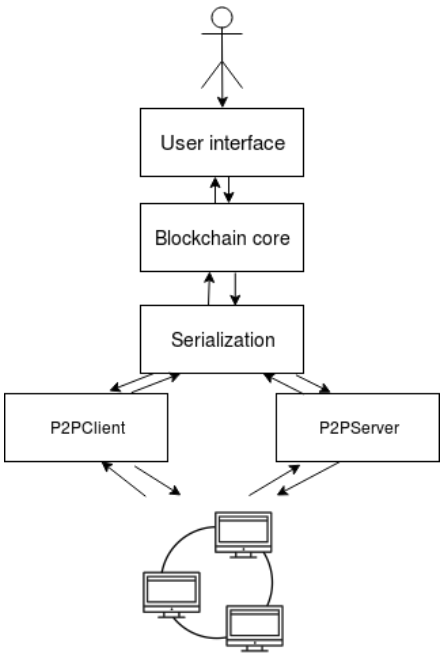


Рисунок 12 — Модули приложения и связи между ними

3.3 Описание технологий, выбранных для разработки

В качестве языка программирования был выбран язык Java. Одно из главных преимуществ данного языка - его независимость от платформы, на которой выполняются программы. Таким образом, один и тот же код можно запускать под управлением разных операционных систем. Благодаря наличию в Java JIT(just in time) компилятора программы написанные на этом языке обладают хорошим быстродействием и высокой вычислительной производительностью. Вследствие чего выбор и пал на данный язык программирования.

Для реализации пользовательского интерфейса была выбрана платформа JavaFx. JavaFx – это платформа на основе Java для создания приложений с насыщенным графическим интерфейсом. Может использоваться как для создания настольных приложений, запускаемых непосредственно из-под операционных систем, так и для интернет-приложений, работающих в браузерах, и для приложений на мобильных устройствах.

Для всех криптографических аспектов приложения была использована

популярная библиотека BouncyCastle, включающая функции генерации пар ключей и цифровых подписей на их основе, а так же включающая реализацию хеш-функции Scrypt.

Сериализация данных для последующей отправки через сеть осуществляется в приложении с помощью библиотеки ApacheSerializationUtils.

3.4 Описание интерфейса и работы компонентов приложения

3.4.1 Стартовое окно приложения

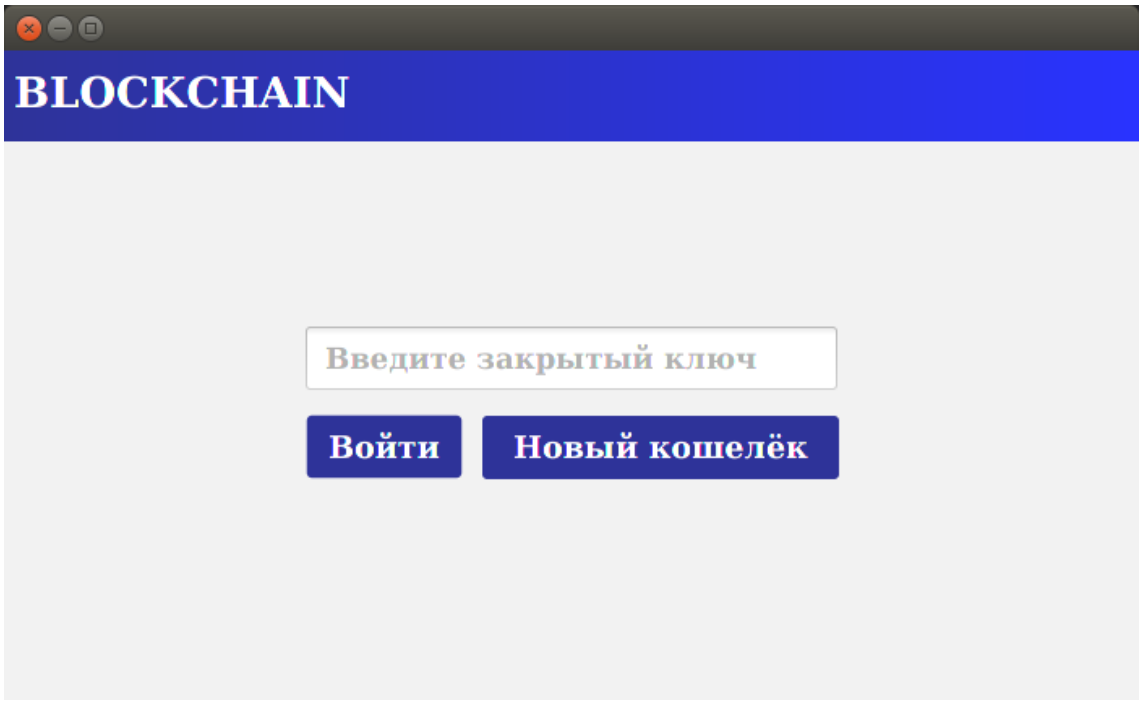


Рисунок 13 – Стартовое окно приложения

При запуске программы открывается стартовое окно приложения(рисунок 13). Пользователю предлагается ввести свой секретный идентификатор и войти в сеть, либо создать новый кошелёк. При создании нового кошелька для пользователя случайным образом генерируется уникальный закрытый ключ, который будет являться его личным идентификатором для входа.

При входе в приложение открывается главное окно, и на основе закрытого ключа генерируется открытый адрес кошелька пользователя, с

помощью которого он может совершать транзакции и отслеживать изменения баланса.

Главное окно приложения содержит основные элементы управления, сгруппированные по вкладкам: Обзор, Мой кошелёк, Новая транзакция и Майнинг.

3.4.2 Обозреватель блоков

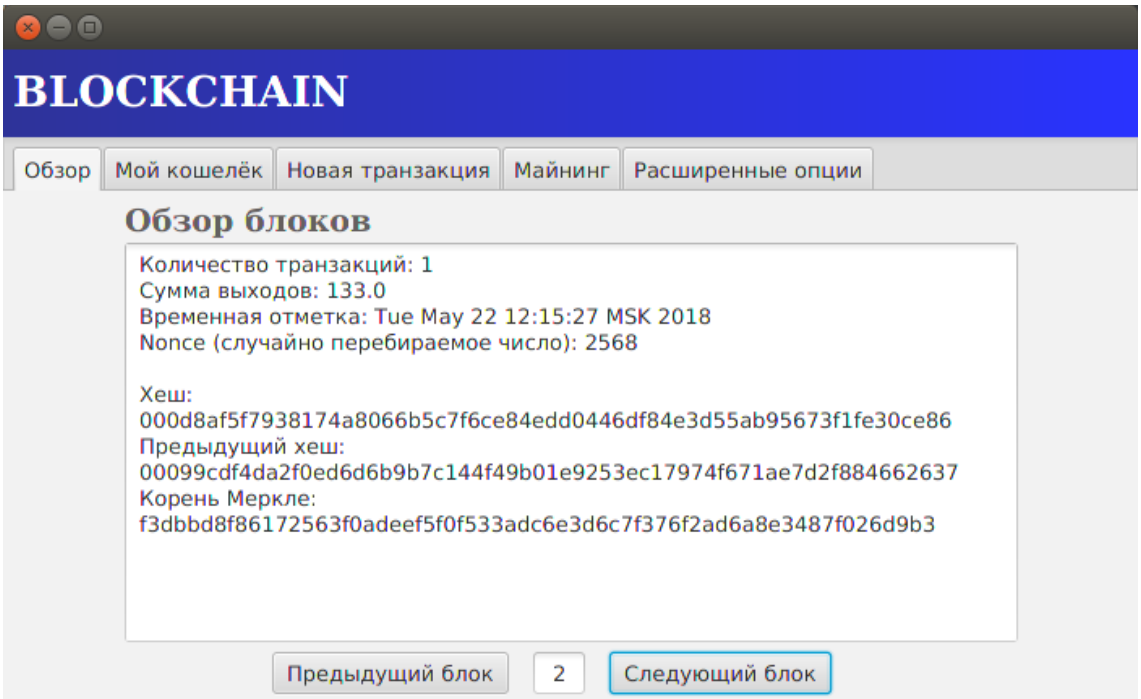


Рисунок 14 – Вкладка Обзор блоков

На вкладке обзор(рисунок 14) пользователь может просмотреть всю необходимую информацию о любом существующем блоке цепочки. Навигацию между блоками осуществляется посредством нажатия кнопок Предыдущий блок и Следующий блок, либо посредством указания номера блока в текстовом поле.

3.4.2 Вкладка Мой кошелёк

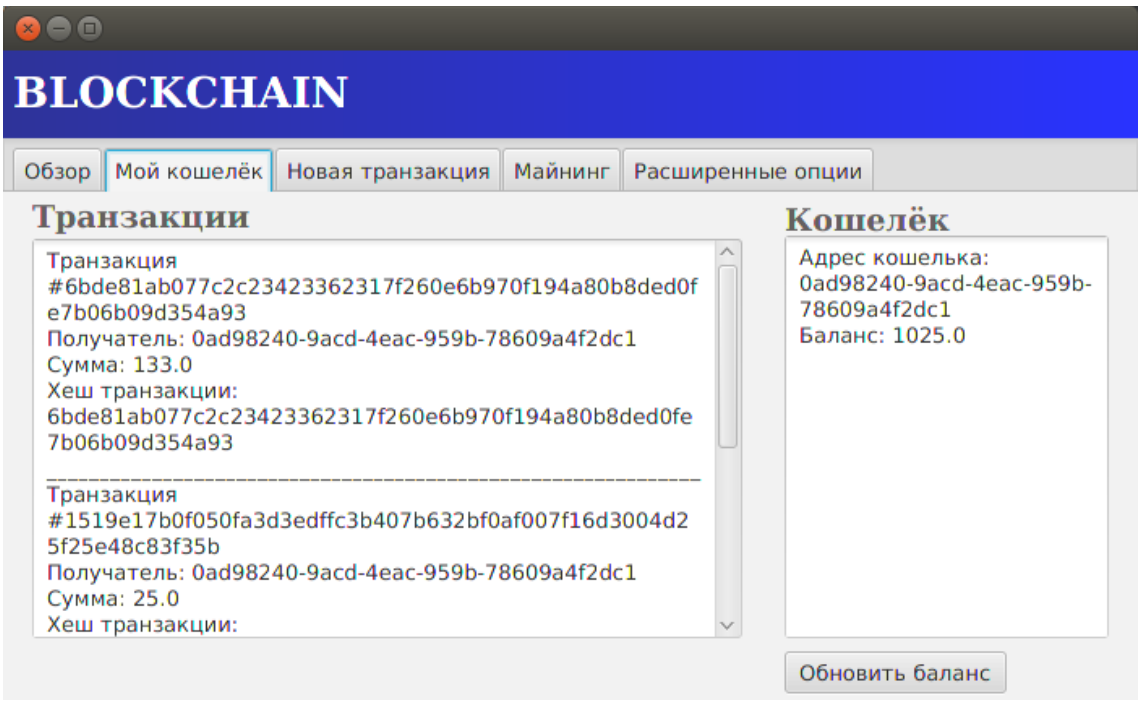


Рисунок 15 – Вкладка Мой кошелёк

Вкладка мой кошелёк(рисунок 15) предоставляет пользователю возможность просмотреть историю всех исходящих и входящих транзакций его кошелька, узнать свой баланс и идентификатор кошелька. Идентификатор кошелька служит адресом для получения и перевода средств при создании транзакции.

3.4.3 Создание новой транзакции

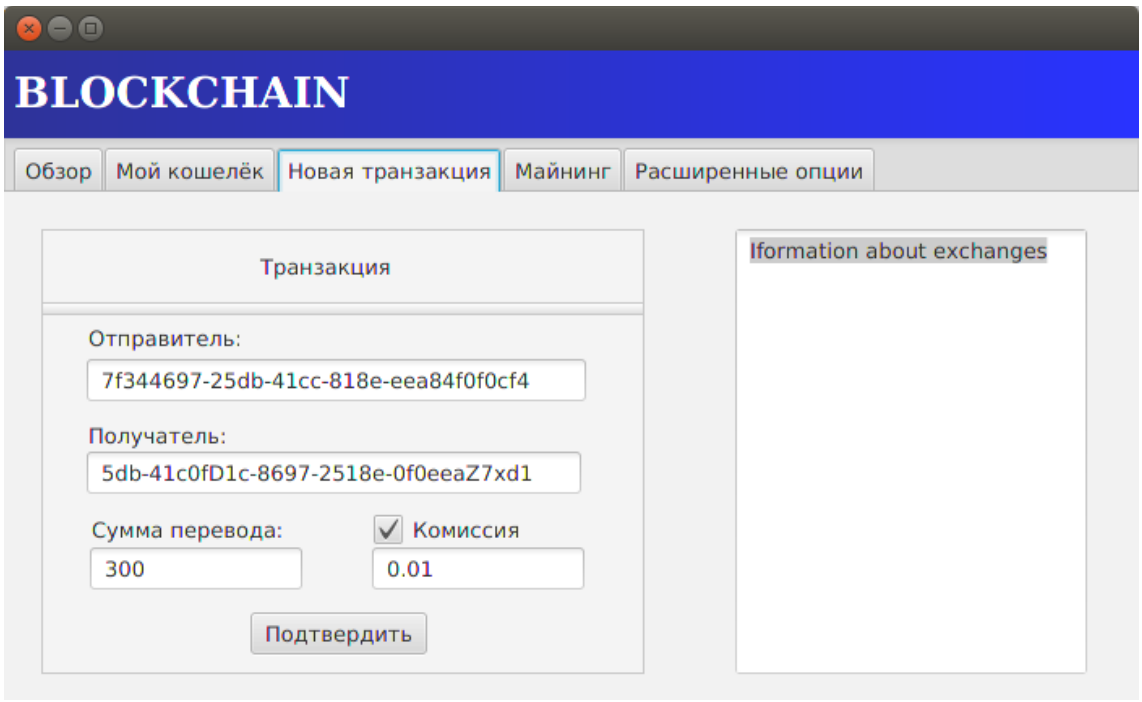


Рисунок 16 – Вкладка Новая транзакция

Элементы управления для создания транзакции находятся на вкладке новая транзакция (рисунок 16). Для создания новой транзакции пользователь должен заполнить форму составления транзакции, в соответствии с указанными на странице правилами. По нажатию на кнопку подтвердить будет выведено диалоговое окно предлагающее пользователю проверить и подтвердить введённые данные, либо диалоговое окно сообщающее о ошибке в составлении транзакции. Ошибкой в составлении транзакции может являться как неправильное заполнение полей, так и нехватка средств.

При выборе отправки транзакции с комиссией, можно указать размер комиссии включённой в транзакцию. В этом случае средства для оплаты комиссии будут сняты со счёта пользователя сверх суммы перевода. Если оставить поле пустым то, размер комиссии будет составлять 0.5% от суммы перевода.

После подтверждения транзакции она отправляется в список необработанных транзакций и ожидает включения в следующий блок.

3.4.4 Управление майнингом

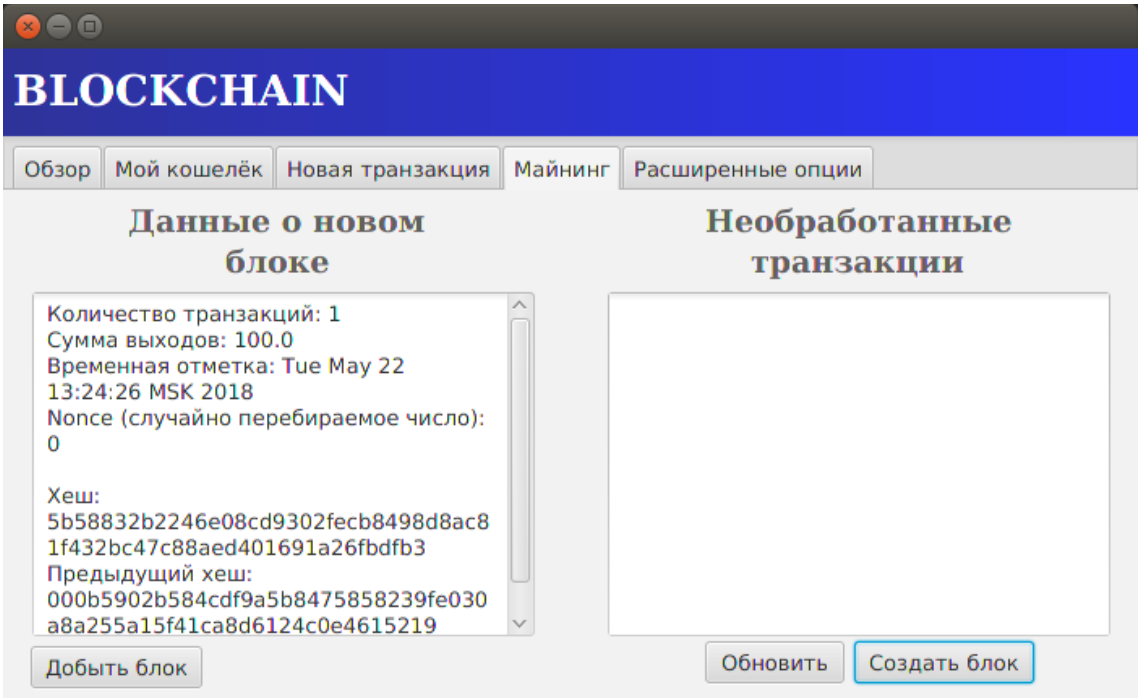


Рисунок 17– Вкладка Майнинг

Вкладка майнинг(рисунок 17) включает в себя элементы управления для создания и майнинга блоков. В текстовом поле «Необработанные транзакции» отображаются транзакции, которые ещё не были включены в блокчейн.

Нажатие на кнопку Обновить посылает в пул запрос об обновлении списка необработанных транзакций. Кнопка создать блок отвечает за конфигурирование нового блока. При её нажатии создаётся новый блок, в который помещается 10 необработанных транзакций из списка, а в текстовое поле «Данные о новом блоке» помещается информации о данном блоке.

При нажатии кнопки Добыть блок в отдельном потоке начинается процесс майнинга сконфигурированного блока. При успешной добыче блока, новый блок рассылается всем активным узлам цепи, а в клиентском окне появляется уведомление о успешном создании нового блока.

ЗАКЛЮЧЕНИЕ

В связи с возрастающим влиянием электронных денег в мировой экономике и постепенным внедрением технологий распределённого реестра во многие сферы жизни общества, нельзя не сказать об актуальности детального изучения технологии блокчейн.

В рамках данной курсовой работы были достигнуты следующие результаты:

- Изучены основные понятия и принципы, заложенные в технологии блокчейн.

- Проведён анализ аналогичных продуктов и выявлены их недостатки.

- Разработано настольное приложение на языке программирования Java, представляющее собой пиринговую платёжную систему и реализующее все основные функции рассмотренной технологии блокчейн.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Алекс Тапскотт. Революция блокчейна. , 2016. – 416с.

2 Роджер Воттенхофер. Наука о блокчейне. , 2014 – 730с.

3 Информационно-аналитический ресурс, посвященный технологии блокчейн – URL: http://www.machinelearning.ru [17 Мая 2018].