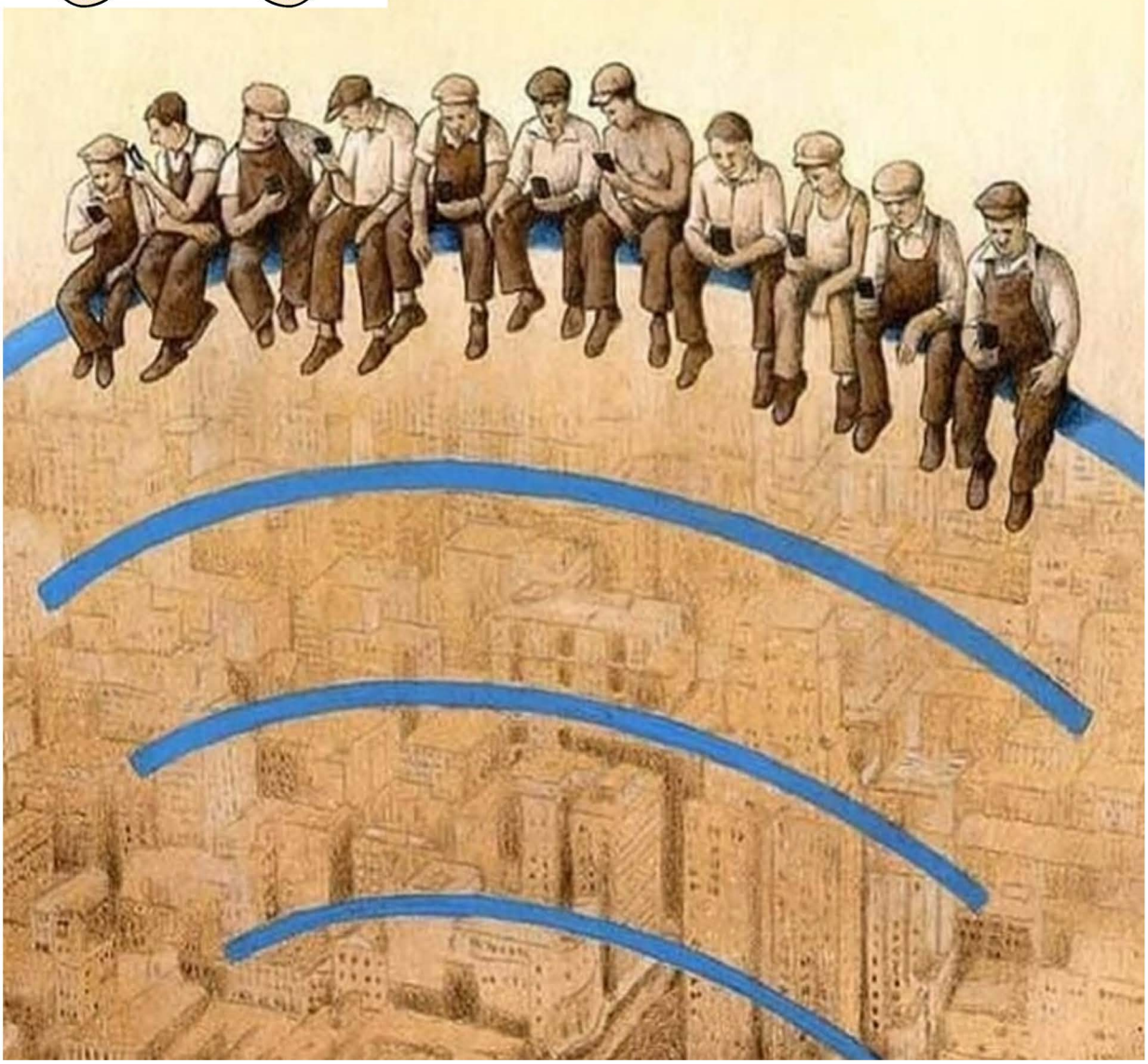
Экономика знаний & Блокчейн и умные контракты

А.В. Солодов
В. Д. Мунистер



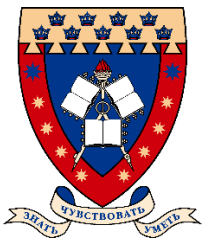
Учебное издание

«Экономика знаний. Блокчейн и умные контракты»

Солодов А.В, Мунистер В.Д.

2021 г.

GLÜCKSRITTER MUNISTER



INSCRIPTUM

Объект исследования — образование и наука в их широком аспекте; подходы к организации образовательного и научного процесса и непосредственно сам процесс обучения.

Предмет исследования — применение технологии блокчейн в образовании и науке.

Цель исследования — выявить подходы к применению технологии блокчейн в образовании и науке.

На основе выдвинутой гипотезы и поставленной цели были сформулированы следующие **задачи исследования**:

1. Провести анализ источников по теме устройства работы технологии блокчейн, ее правового положения и принципов работы технологий, связанных с ней.
2. Провести анализ источников в области применения технологии блокчейн в различных сферах деятельности с целью ее применения в образовании и науке.
3. Выделить основные направления применения технологии блокчейн в образовании и науке.
4. Описать подходы к применению технологии блокчейн в образовании и науке.
5. Инкапсулировать практический модуль по введению в технологию блокчейн и смарт-контракты.

ве опоры для разработок реальных проектов;

- выявлены возможности для решения ряда проблем в образовании и науке на основании отраженных в описанных моделях преимуществ технологии блокчейн.

Теоретическая значимость исследования заключается в следующем:

- описано текущее правовое положение криптовалют, во многом определяющих правовое положение как самой технологии блокчейн, так и других технологий, тесно связанных с блокчейном;
- описано устройство работы технологии блокчейн и принципов работы технологий смарт-контрактов и Initial coin offering (ICO), использующих блокчейн в основе своей работы;
- выявлены возможности применения технологии блокчейн в образовании и науке, которые могли бы решить ряд проблем в этих сферах.

Практическая значимость исследования заключается в том, что основе описанных моделей выявлены подходы к применению технологии блокчейн в образовании и науке и предпринята попытка определить, насколько возможны реализации таких моделей. Данные наработки могут оказаться полезными для практических разработок, использующих их в своей основе.

ВВЕДЕНИЕ

Сегодня развитие технологий происходит настолько быстро, что порой законодательства тех или иных стран не успевают за их стремительным развитием и ростом популярности.

В связи с этим есть вероятность ситуаций, при которых могут возникнуть некоторые трудности, связанные с официальной стороной вопроса. Например, с допустимостью занятия данного рода деятельностью. Ведь в тех же вузах этому не обучают, работу, где бы можно было получить опыт, как следствие, тоже не так просто найти. Приходится получать информацию в Интернете.

Происходит это в некоторых случаях из-за сложности технологии, которая, к тому же еще и может модернизироваться, в других — из-за недостатков бюрократической системы, а иногда даже из-за опасности нанести ущерб человеку. Но это уже относится скорее к вопросам этики. Таким образом, государство занимает выжидательную позицию в отношении распространяемых новшеств, оценивая, как пользу, так и вред от их введения.

В подобной ситуации, когда до сих пор нет чёткого регулирования, сейчас находятся криптовалюты и технология блокчейн, на которой они основаны, и о которой, собственно, пойдет речь.

Актуальность

На *социально-педагогическом уровне* связана с необходимостью перехода к цифровым технологиям.

На *научно-теоретическом уровне* обусловлена стремлением государства к высокому уровню технологичности образования и науки, что является важным аспектом повышения качества жизни граждан, обеспечения экономического роста и национального суверенитета и отражено в программе «Цифровая экономика России» [18].

На *научно-методическом уровне* заключается в дефиците теоретических описаний сценариев применения технологии блокчейн в образовании и науке, в которых этот процесс рассматривался бы с разных сторон и на которые можно было бы опереться при разработке реальных продуктов. Данная проблема связана с тем, что технология является ещё новой, недостаточно изученной и протестированной в современных реалиях и, как следствие, находится в состоянии неопределенности с правовой точки зрения.

Отсюда возникает ряд **противоречий**.

На *социально-педагогическом уровне*: между необходимостью перехода к цифровым технологиям и незнанием этих технологий широкими слоями населения.

На *научно-теоретическом уровне*: между важностью перехода на цифровую экономику и недостаточной изученностью технологии блокчейн, которая могла бы способствовать этому скорейшему переходу.

На *научно-методическом уровне*: с одной стороны, заинтересованность общества в технологии блокчейн, а с другой — дефицит подробно описанных теоретических моделей, в которых были бы отражены способы и аспекты применения технологии в образовании и науке и которые помогли бы в понимании её устройства и дальнейшего развития.

Проблема исследования заключается в дефиците теоретических описаний подходов к применению технологии блокчейн в образовании и науке.

Ключевые понятия исследования

Биткойн (англ. Bitcoin, от bit — «бит» и coin — «монета») — пиринговая платёжная система, использующая одноимённую единицу для учёта операций и одноимённый протокол передачи данных [3].

Блокчейн (англ. blockchain или block chain) — выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию [4].

Криптовалюта — разновидность цифровой валюты, создание и контроль за которой базируются на криптографических методах [13].

Майнинг (с англ. mining — добыча полезных ископаемых) — деятельность по созданию новых структур (обычно речь идёт о новых блоках в блокчейне) для обеспечения функционирования криптовалютных платформ [16].

Смарт-контракт (с англ. Smart contract — умный контракт) — компьютерный алгоритм, предназначенный для заключения и поддержания коммерческих контрактов в технологии блокчейн [29].

Токен (с англ. Token — знак, символ; опознавательный знак; жетон) — это единица стоимости, выпущенная частной организацией в системе блокчейн [41].

Хэширование (англ. hashing) — преобразование массива входных данных произвольной длины в (выходную) битовую строку установленной длины, выполняемое определённым алгоритмом [42].

ICO, Initial coin offering (с англ. — «первичное предложение монет, первичное размещение монет») — форма привлечения инвестиций в виде продажи инвесторам фиксированного количества новых единиц криптовалют (токенов), полученных разовой или ускоренной эмиссией [71].

Объект исследования — образование и наука в их широком аспекте; подходы к организации образовательного и научного процесса и непосредственно сам процесс обучения.

Предмет исследования — применение технологии блокчейн в образовании и науке.

Гипотеза исследования заключается в том, что принципы, заложенные в технологии блокчейн, имеют подходы к применению в образовании и науке с целью решения ряда проблем в этих сферах.

Цель исследования — выявить подходы к применению технологии блокчейн в образовании и науке.

На основе выдвинутой гипотезы и поставленной цели были сформулированы следующие **задачи исследования**:

1. Провести анализ источников по теме устройства работы технологии блокчейн, ее правового положения и принципов работы технологий, связанных с ней.
2. Провести анализ источников в области применения технологии блокчейн в различных сферах деятельности с целью ее применения в образовании и науке.
3. Выделить основные направления применения технологии блокчейн в образовании и науке.
4. Описать подходы к применению технологии блокчейн в образовании и науке.

Научная новизна исследования заключается в следующем:

- описаны теоретические модели реализации сценариев применения технологии блокчейн в образовании и науке, которые могут быть использованы в качестве опоры для разработок реальных проектов;
- выявлены возможности для решения ряда проблем в образовании и науке на основании отраженных в описанных моделях преимуществ технологии блокчейн.

Теоретическая значимость исследования заключается в следующем:

- описано текущее правовое положение криптовалют, во многом определяющих правовое положение как самой технологии блокчейн, так и других технологий, тесно связанных с блокчейном;
- описано устройство работы технологии блокчейн и принципов работы технологий смарт-контрактов и ICO, использующих блокчейн в основе своей работы;
- выявлены возможности применения технологии блокчейн в образовании и науке, которые могли бы решить ряд проблем в этих сферах.

1 ТЕОРЕТИЧЕСКИЕ ПОДХОДЫ К ИССЛЕДОВАНИЮ СПОСОБОВ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН В ОБРАЗОВАНИИ И НАУКЕ

1.1 Описание блокчейна и технологий, использующих блокчейн в основе своей работы

1.1.1 Описание истории развития и устройства работы технологии блокчейн

В 2014 году на сайте Bitcoin Magazine автором Кеном Гриффитом, являющимся соучредителем компании Dinero Limited, которая представляет из себя платформу с богатым инструментарием для обмена цифровыми валютами, размещена статья [48], где история блокчейна рассматривается с периодов до появления первой криптовалюты, начиная с идей, отдаленно напоминающих то, что мы видим сейчас.

Эта же статья в дальнейшем была переведена и использована Артемом Генкиным и Алексеем Михеевым в книге «Блокчейн: Как это работает и что ждет нас завтра» [8, с. 24–25].

Основы криптовалют были разработаны в 1992 году киберпанками — неформальной группой людей, заинтересованных в сохранении анонимности и интересующихся криптографией. В 1993 году американский программист Эрик Хьюз заявил о возможности обеспечения конфиденциальности совершаемых платежных операций путем многоэтапного шифрования. Затем в 1994 году американский ученый и инженер из корпорации Intel Тимоти Мэй в статье «Вопросы и ответы о криптопанке» (The Cyphernomicon) описал основные характеристики такой системы, в том числе безопасность неотслеживаемых транзакций через их шифрование, а также транзакции, проводимые без посредников. Для реализации этих идей надо было создать новый

механизм расчетов, не затрагивающий банковский сектор. Вай Дай, описавший концепцию криптовалюты b-money в 1998 году, предложил, по сути, реальный способ исполнения условий договора между анонимными участниками. А Девид Чауму изобрел «слепую подпись». И лишь спустя 10 лет, доселе неизвестный человек (или группа людей) под псевдонимом Сатоши Накамото вывел в публичное пространство цифровую валюту Биткойн, опубликовав статью «Bitcoin: A Peer-to-Peer Electronic Cash System» [75] в списке рассылки о криптографии (The Cryptography Mailing list) metzdowd.com. В статье описывается децентрализованное решение с использованием идей пиринговой системы, криптографии, математических правил, таких, как например, доказательство работы (Proof-of-Work) и общих правил проведения транзакций между участниками системы. Данное решение получило название блокчейн биткойна. Это событие и стало отправной точкой в развитии технологии [48], [8, с. 24], [26], [24].

На текущий момент на свет появилось огромное количество других криптовалют, альтернатив биткойна, называемых *альткойнами*, что свидетельствует об огромной популярности данного способа обмена средствами [8, с. 25].

Так, например, по состоянию на 18 декабря 2017 года капитализация валюты биткойн составляла 320 млрд долларов (по данным биржи CoinMarketCap) [59]. Для сравнения капитализация ExxonMobil, крупнейшей американской компании, по состоянию на 4 квартал 2017 года равна 350,6 млрд долларов [2].

Поскольку блокчейн — это достаточно новая и еще развивающаяся технология, официального и исчерпывающего определения ей нет.

В своей книге А. С. Генкин и А. А. Михеев касаются вопроса формулировки и приводят несколько трактовок понятия, дающие ряд деятелей, изучающих данную технологию [8, с. 88–92].

Блокчейн (англ. *blockchain* или *block chain*) — выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию [4].

Технология надежного распределенного хранения записей обо всех когда-либо совершенных транзакциях. Блокчейн представляет собой цепочку блоков данных, объем которой постоянно растет по мере добавления новых блоков с записями самых последних транзакций. Это хронологическая база данных, т.е. такая база данных, в которой время, когда была сделана запись, неразрывно связано с самими данными, что делает ее некоммутативной [24].

Данные представлены последовательностью записей, которую можно дополнять. Записи вместе с вспомогательной информацией хранятся в блоках. Блоки хранятся в виде односвязного списка. Каждый участник представлен узлом (node), который хранит весь актуальный массив данных и контактирует с другими узлами. Узлы могут добавлять новые записи в конец списка, а также сообщают друг другу об изменениях списка [24].

Теперь рассмотрим механизмы, с помощью которых осуществляется данная деятельность, и те характеристики, которые обеспечены данными механизмами.

В своём сайте Андерс Браунворт реализовал демоверсию блокчейна, которую можно «пощупать» и понять, как эта технология работает [56].

В видео он рассказывает об ее устройстве, начиная с такого понятия как хэширование на примере хэш-функции SHA256.

Не будем углубляться в процесс работы этой функции, а лишь рассмотрим основные ее компоненты, обозначенные на рисунке 1.

Хэширование или **хеширование** (англ. *hashing*) — преобразование массива входных данных произвольной длины в (выходную) битовую строку установленной длины, выполняемое определённым алгоритмом [42].

Функция, воплощающая алгоритм и выполняющая преобразование, называется «**хэш-функцией**» или «**функцией свёртки**» [42].

Исходные данные называются входным массивом, «**ключом**» или «**сообщением**».

Результат преобразования (выходные данные) называется «**хэшем**», «**хэш-кодом**», «**хэш-суммой**», «**сводкой сообщения**» [42].

Рисунок 1 — Компоненты хэширования

Представленный ниже набор символов в поле «Hash» является уникальным для заданного набора входных данных поля «Data». Он также может быть получен для любого другого набора входных данных.

Однако процесс обратного извлечения входных данных с помощью имеющегося хэш-кода является задачей, требующей больших вычислительных мощностей [24], [21].

В блоке используется тот же процесс хэширования, однако входные данные разделены на четыре секции (рисунок 2):

- «Block» — номер блока в цепи;
- «Nonce» — случайное число, которое генерируется для получения такого хэша, который удовлетворял бы заложенным разработчиками условиям;
- «Data» — набор данных;
- «Prev» — хэш предыдущего блока в цепи.

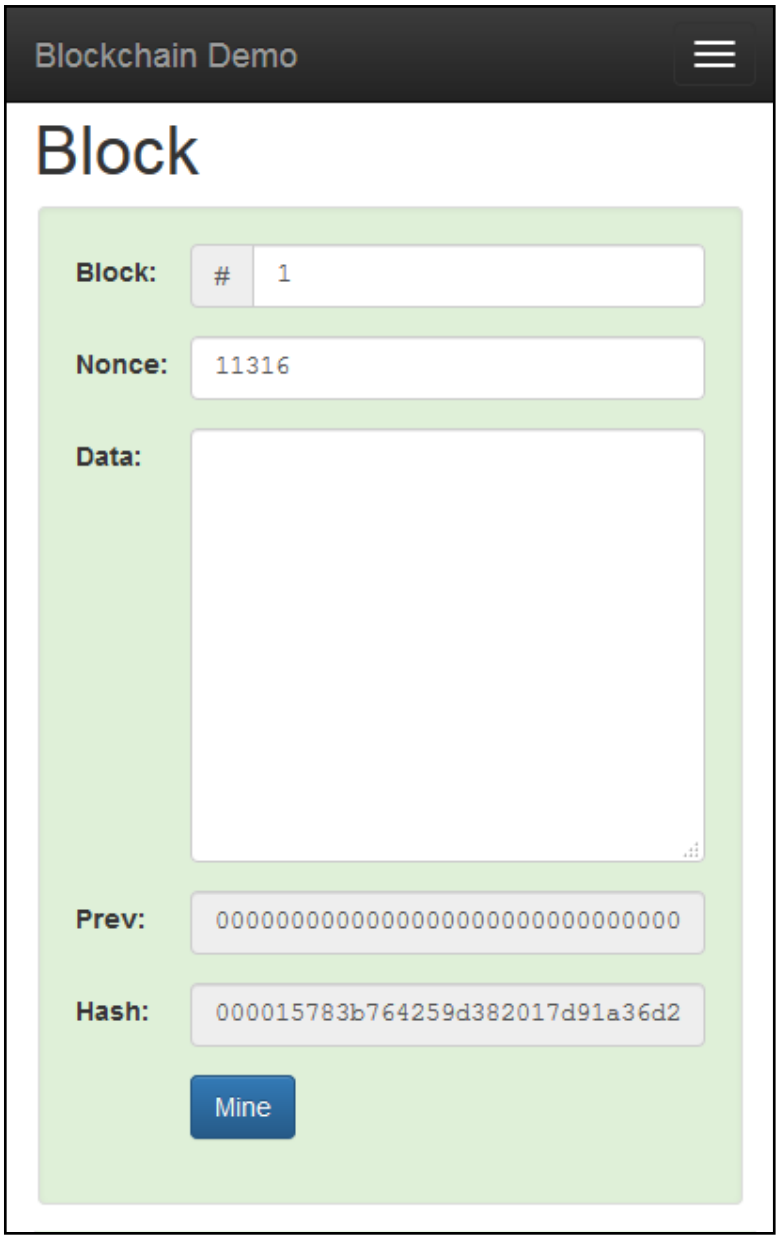


Рисунок 2 — Схема блока цепи

Базовую модель распределения данных в системе, построенной на блокчейне, можно представить в виде следующей последовательности действий:

1. Новая транзакция отсылается всем узлам сети, сеть построена по принципу пиринговой сети, транзакция попадает в пул необработанных данных на этих узлах (рисунок 3).

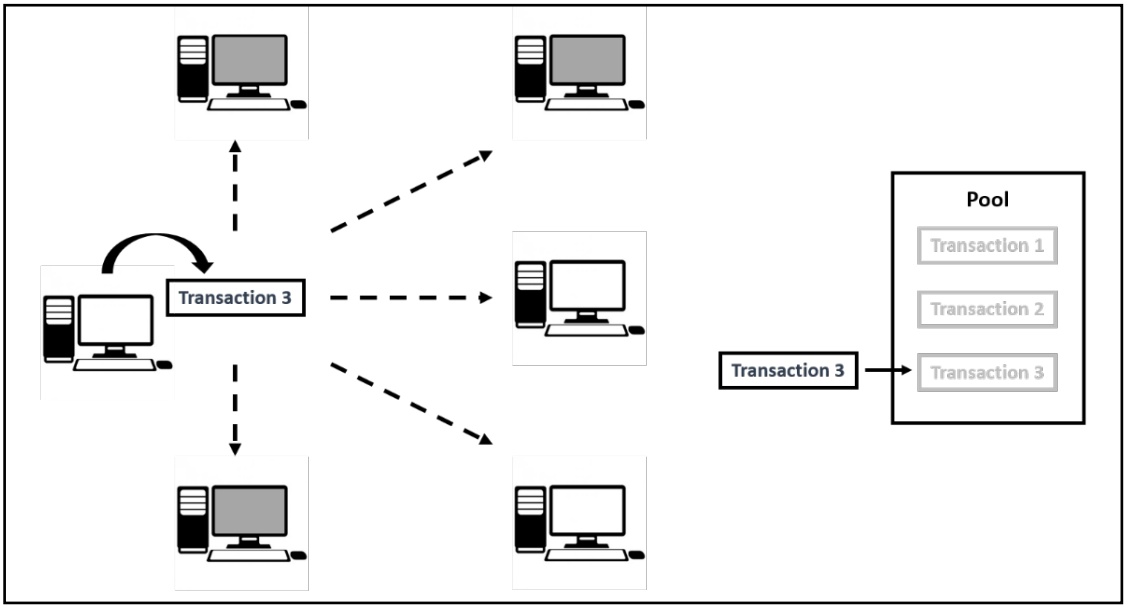


Рисунок 3 — Добавление транзакции в пул необработанных транзакций

2. Определенные узлы, занимающиеся **майнингом** (деятельность по созданию новых структур (обычно речь идёт о новых блоках в блокчейне) для обеспечения функционирования криптовалютных платформ) (на рисунке 3 отмечены серым цветом), добавляют транзакции, расположенные в пуле необработанных данных в блок (рисунок 4).

3. Каждый майнер ищет такое значение поля «Nonce», при котором хэш блока удовлетворял бы заданным разработчиками условиям (в блокчейне биткойна условием было наличие в начале хэша блока определенного количества нулей), данная операция называется подтверждением работы (Proof-of-work). Так же на данный момент появился другой способ подтверждения права на осуществление операции по внесению блока — метод подтверждения доли (Proof-of-stake). Оба метода будут рассмотрены позже.

4. Первый майнер, получивший удовлетворяющий условию хэш блока, отправляет блок данных всем участникам сети, а сам майнер получает вознаграждение за добавление блока (рисунок 5). Не критично, если блок получат не все узлы, как только узел, пропустивший один из блоков, получит уже следующий за ним, он запросит недостающую информацию, чтобы заполнить очевидный пропуск.

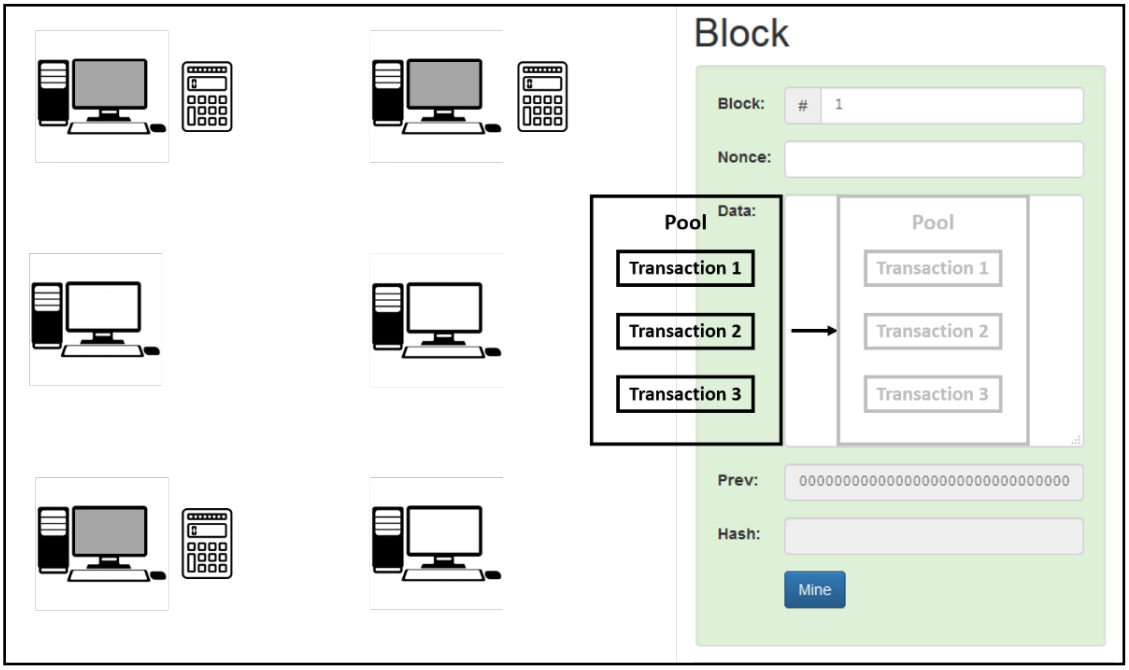


Рисунок 4 — Добавление пула необработанных транзакций в блок

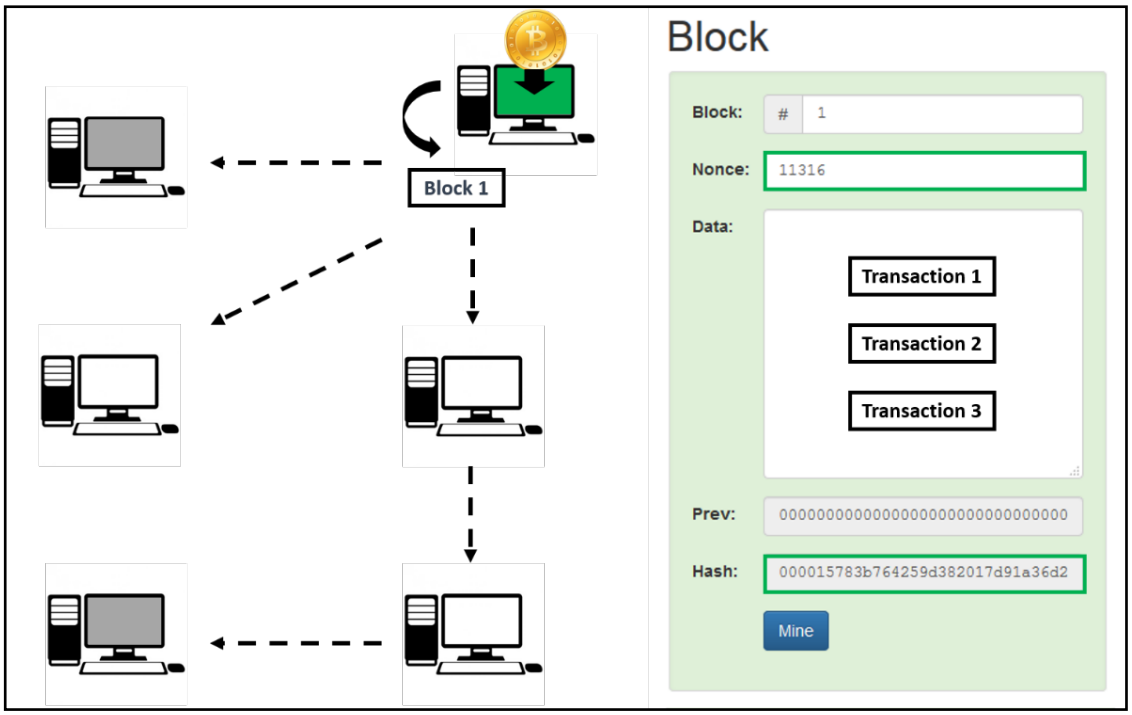


Рисунок 5 — Вычисление хэша и отправка его другим узлам на проверку

5. Узлы, получившие данный блок производят проверку на корректность транзакций и отсутствие так называемой двойной траты (рисунок 6). Если блок не проходит проверку, он отбрасывается.

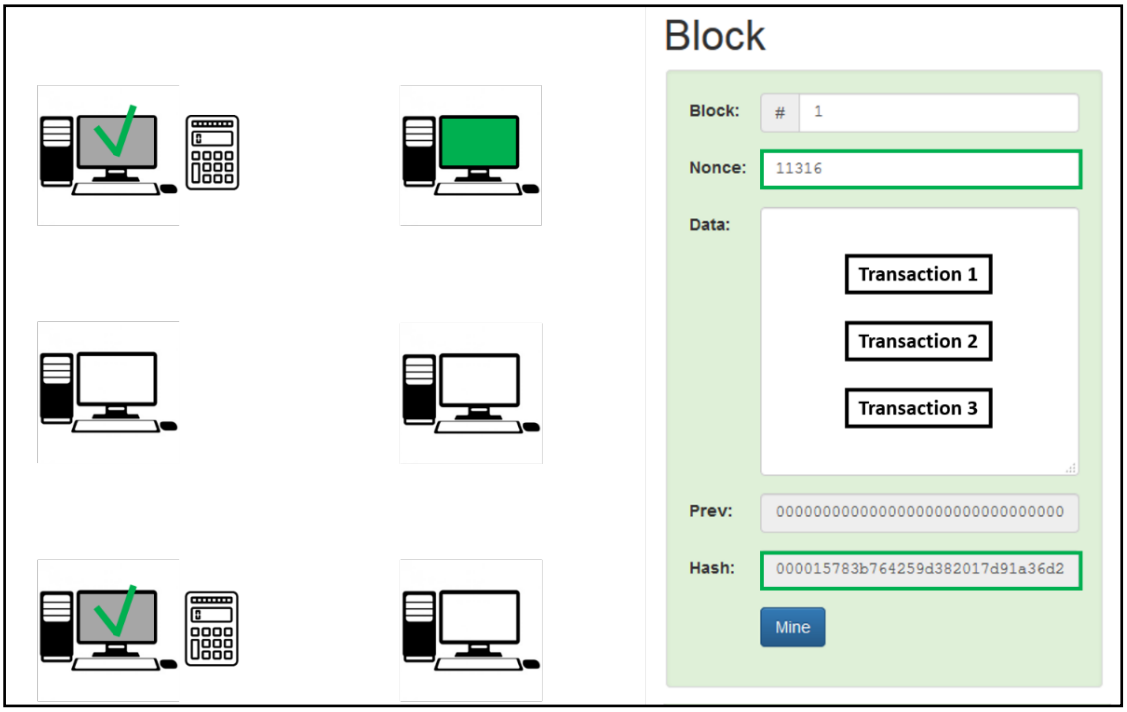


Рисунок 6 — Проверка блока

6. Если достигается согласие по корректности блока, майнеры добавляют его в цепочку и начинают работать над новым блоком данных, основанном на хэше только что добавленного блока (рисунок 7).

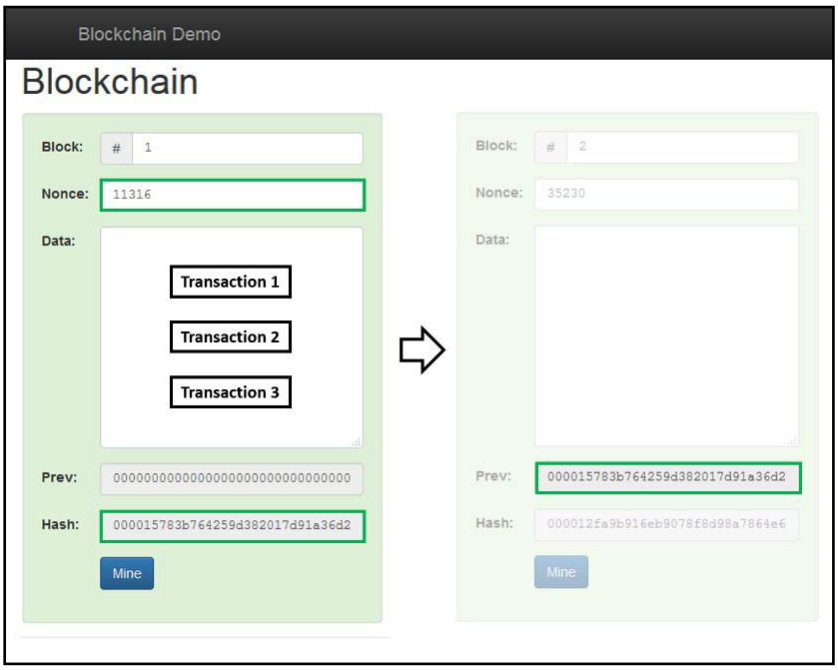


Рисунок 7 — Добавление блока в цепочку

Поскольку в формировании хэша текущего блока, помимо других входных данных, участвует, в том числе, и хэш предыдущего блока, любое изменение любых входных данных предыдущего блока приведет к изменению как предыдущего хэша, так и хэша блока, следующего за ним, который из-за этого перестанет соответствовать заданному условию, а следом за ним некорректной станет и вся последующая цепь. Более того, чем старее блок в цепи, тем сложнее его изменить.

Информация о транзакциях не передается в открытом виде, иначе каждый бы смог создать транзакцию, «представившись» в системе другим человеком, и таким образом отправить все средства самому себе. Данные об отправителях и получателях преобразуются в нечитаемый набор символов. И вот как это происходит.

Каждый участник сети при регистрации в ней и установке необходимого программного обеспечения на рабочую станцию генерирует случайный набор чисел (приватный ключ), с помощью которого формируется другой, более сложный набор символов (публичный ключ) (рисунок 8). Получить приватный ключ из публичного невозможно, поскольку его длина очень велика и требует огромных вычислительных мощностей.

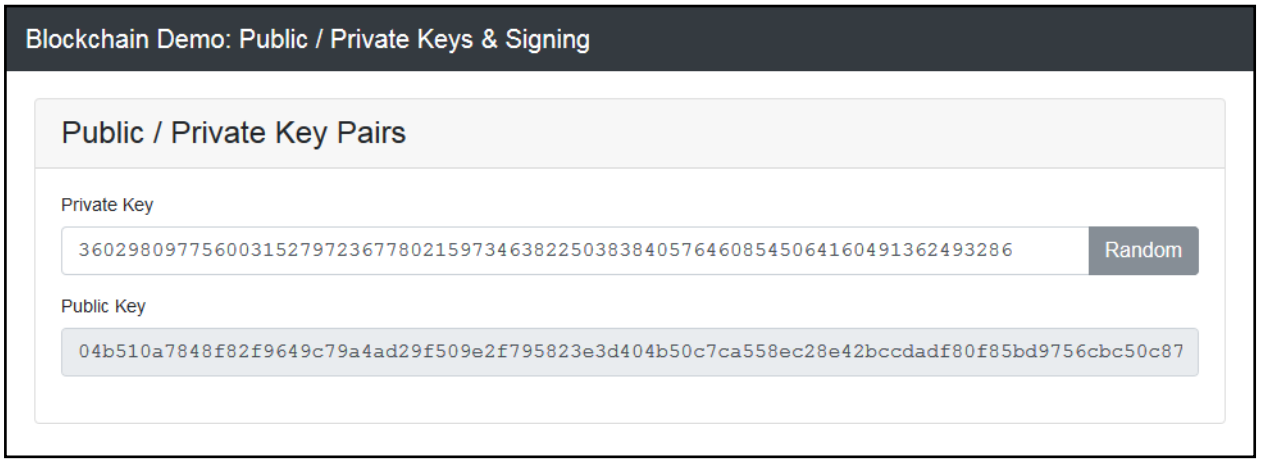


Рисунок 8 — Приватный и публичный ключи

Приватный ключ принадлежит только тому пользователю, который сгенерировал его. Он не участвует в транзакциях, и его не следует разгла-

шать никому. Он служит для осуществления подписи транзакции, однако в открытом виде не передается [21].

Для того, чтобы отправить транзакцию, каждый пользователь осуществляет подпись. В отправителях он вводит свой публичный ключ для обозначения своего кошелька, в получателях публичный ключ того кошелька, на который требуется перевести средства, и сумму, которую желает перевести (рисунок 9).

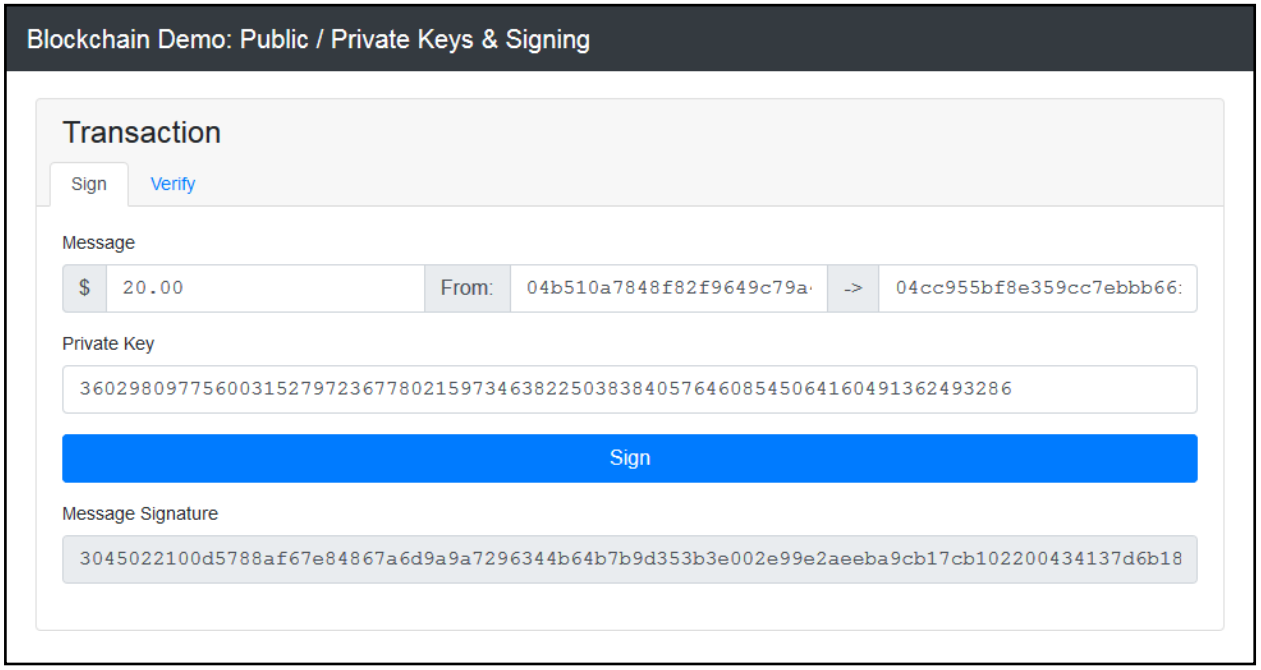


Рисунок 9 — Подпись транзакции

На основе этих входных данных и приватного ключа формируется подпись, а затем отправляется другим участникам для проверки и внесения транзакции в блок.

Имея подпись и все входные данные, каждый пользователь системы может проверить, что транзакция, которую пытаются внести в блок, подписана пользователем, имеющим доступ к реальному приватному ключу (рисунок 10).

Таким образом, блокчейн уже не имеет персональных данных о лицах, передающих средства тому или иному лицу, а имеет лишь некие ключи, представляющие собой кошельки, за которыми находятся те или иные лица и подписи к каждой транзакции (рисунок 11).

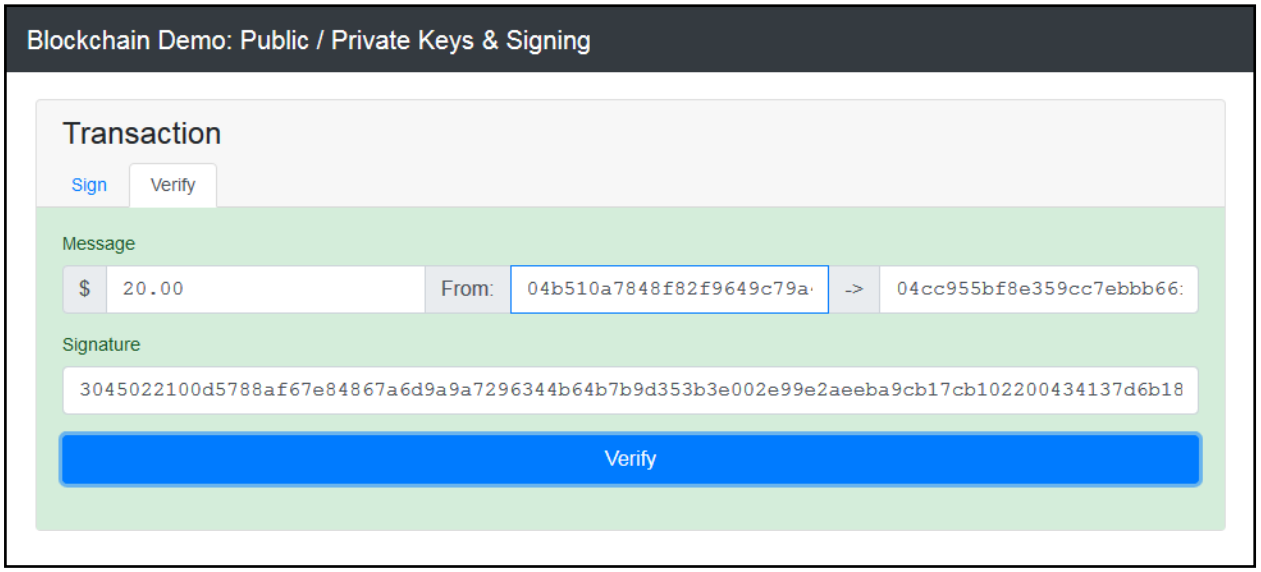


Рисунок 10 — Подтверждение подписи транзакции

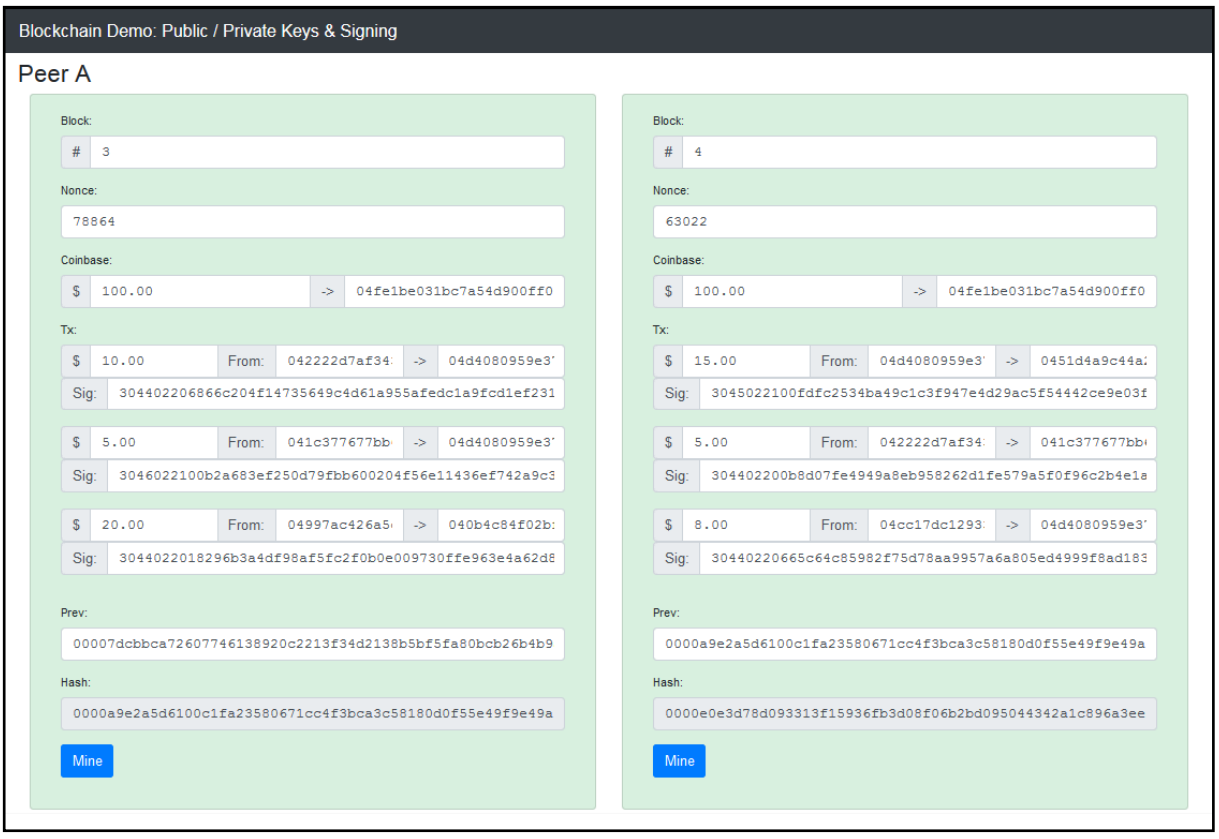


Рисунок 11 — Схема цепи блоков с публичными ключами и подписями в транзакциях

Как уже было сказано выше, любое малейшее изменение входных данных, будь то номер кошелька отправителя или получателя, передаваемые средства или подпись, мгновенно приведет к изменению конечного хэша и некорректности всей цепи.

Хэш в этой схеме — это преобразованный с помощью хэш-функции массив данных. В случае криптовалют — это информация о транзакции, в более сложных системах — это информация об умных контрактах и актуальное состояние программного кода, внесенного в блокчейн. В результате преобразования мы получаем практически уникальную, кроме случаев коллизий хэширования, буквенно-числовую строку, которая характеризует начальный элемент, но не может быть преобразована в обратную сторону. Сочетание использования открытых и закрытых ключей совместно с хэшированием дает технологии блокчейна высокий уровень безопасности хранения данных [24].

Если один из майнеров пытается добавить блок, не соответствующий данному правилу, то такой блок автоматически отклоняется другими участниками сети блокчейна. Чтобы майнер смог добавить не валидный блок, необходимо изменить хэш всех предыдущих блоков, вплоть до так называемого «генезис-блока» — первого блока в системе. Данный блок обычно задается разработчиками системы. Из этого возникает одно из существенных свойств технологии распределенного реестра — попавшая в цепочку блоков информация не может быть изменена постфактум [24].

Ввиду того, что в процессе майнинга пользователи стали объединяться в группы, называемые *пулами*, появилась возможность переписать недавно добавленный блок, однако это также является трудновыполнимой задачей, поскольку в таком случае всё равно приходится бороться с вычислительными мощностями всей остальной сети [21].

Необходимо сказать, что добавление новых блоков майнерами происходит по определенным принципам. Данные принципы были введены в систему для увеличения безопасности блокчейна и в то же время обеспечения децентрализации системы [24].

На данный момент существуют два основных принципа, по которым в системе достигается консенсус по добавлению нового блока в блокчейн — это доказательство проделанной работы (Proof-of-work, или PoW) и доказательство доли владения (Proof-of-stake, или PoS) [24], [44].

Существуют также и другие алгоритмы, по которым происходит добавление нового блока, но описанные выше являются основными и наиболее используемыми [44].

В связи с тем, что безопасность блокчейна не полагается на единый удостоверяющий центр, такой, например, как банк, с его инфраструктурой безопасности, то каждый из узлов данной системы не знает априори, какая версия базы данных является действительной [24]. Важно учесть то, что реестр обновляется на всех компьютерах в сети одновременно с определенным интервалом времени [21].

В блокчейне биткойна безопасность сети полагается на алгоритм доказательства работы (PoW) в процессе майнинга блоков. Каждый узел, желающий принимать участие в процессе майнинга, должен решить вычислительно сложную задачу, чтобы гарантировать действительность блока. Награда за решение автоматически начисляется майнеру новыми биткойнами [24].

Если будет происходить атака на базу данных блокчейна, атакующий должен решить ту же задачу, что и оставшаяся часть сети, т.е. атака будет успешной, только если атакующий сможет привлечь значительные вычислительные ресурсы [24], [21].

Функционирование протокола биткойна таково, что безопасность сети поддерживается следующими ресурсами [24]:

- специализированное оборудование для проведения вычислений;
- электричество, необходимое для работы оборудования.

Это делает биткойн неэффективным с точки зрения потребления ресурсов. Для увеличения своей доли вознаграждения, майнеры в сети биткойн вынуждены участвовать в «гонке вооружений», то есть использовать всё больше ресурсов для майнинга. С одной стороны, это делает стоимость атаки на биткойн непомерно высокой. С другой, экологическое недружелюбие биткойна привело к возникновению предложений построить подобные системы, которые требуют намного меньше ресурсов [24].

Решением данной проблемы стал метод, основанный на алгоритме подтверждения доли (PoS). Идея подтверждения доли такова: вместо вычисли-

тельной мощности, вероятность создать новый блок и получить соответствующее вознаграждение пропорциональное доле владения пользователя в системе [24].

Логическое обоснование состоятельности алгоритма подтверждения доли заключается в следующем: пользователи с наибольшими долями в системе имеют наибольший интерес в поддержании безопасности сети, так как они больше всего пострадают в случае, если репутация и стоимость криптовалюты упадет в результате атак. Чтобы провести успешную атаку, злоумышленник должен приобрести большую часть валюты, а это будет непомерно дорого, если система будет достаточно популярной [24].

Распределённая природа баз данных делает взлом хакерами практически невозможным, поскольку для этого им нужно одновременно получить доступ к копиям базы данных на огромном количестве компьютеров в сети. DoS-атаки также становятся бессмысленными, поскольку нет единого центра, который был бы подвержен отказу в обслуживании [21].

Кроме того, в блокчейн существует возможность доработки алгоритма его работы и включения изменений в работу при условии, если они будут приняты большинством участников системы [21].

Таким образом, технология распре деленного реестра обладает следующими характеристиками [24]:

- децентрализация;
- открытость внесенных данных;
- математико-криптографическая защита информации;
- невозможность изменить единожды внесенные в систему данные.

В различных источниках часто выделяют следующие особенности [12], [21], [8, с. 96–97]:

- прозрачность: доступ ко всей истории событий — денежным переводам, соглашениям и другим записям — всегда открыт всем участникам системы;
- децентрализованность: история транзакций хранится у каждого участника на жестком диске, а не на каком-то главном сервере;

- анонимность: для работы в блокчейне не нужно раскрывать свою личность;
- равноправие: в блокчейне нет администраторов или хранителей информации, а у всех участников одинаковый статус и возможности;
- безопасность: никто не подделает и не подменит зафиксированную в блокчейне информацию, можно быть уверенным, что она достоверна.

Достоинства криптовалют, согласно Т. Г. Ильиной, таковы:

- высокая скорость операций и мобильность;
- очень низкая стоимость эмиссии;
- безопасность;
- идеальная сохраняемость;
- возможность полноценного контроля;
- децентрализация;
- многофункциональность;
- универсальность;
- независимость;
- отсутствие инфляции;
- открытость и публичность;
- делимость;
- отсутствие запретов;
- анонимность;
- отсутствие подделок;
- простота, удобство и доступность;
- возможность зарабатывать;
- ликвидность и конвертируемость.

Недостатки же у них следующие:

- необходимость в стойкой криптографической защите;
- необходимость в инструментах передачи, пользования и хранения;
- отсутствие должного юридического урегулирования и гарантий;

- недостаточная распространенность;
- нестабильный курс;
- вирусы и киберпреступность;
- ограниченная эмиссия;
- отсутствие идентификации клиента;
- необеспеченность;
- повышенные риски при инвестировании;
- недостаточная изученность и отсутствие необходимой информации;
- постоянно меняющаяся технология;
- высокие затраты на электричество;
- отсутствие немонетарного спроса;
- ограниченность использования;
- неготовность среды и потребителей для внедрения.

По мнению Т. Ильиной, доверие к криптовалюте в первую очередь связано с действиями органов денежного регулирования, лимитированностью эмиссии, уникальностью и узнаваемостью бренда, популярностью и расширением сферы использования, уровнем кибермошенничества, а также с внешними политическими, экономическими и другими факторами.

О. А. Николайчук к достоинствам криптовалют также относит открытость, надежность, невозможность фальшивомонетничества. При этом надежность достигается не путем закрытости информации для остальных субъектов рынка и контроля доступа, а за счет обеспечения каждому клиенту возможности вычислить правильность транзакции.

Кроме того, к достоинствам криптовалют можно отнести и плюсы, свойственные развитию безналичных платежей в целом, такие как:

- отсутствие накоплений вне банковского сектора и привлечение инвестиций в экономику;
- сокращение затрат общества на обработку и хранение банкнот, монет, на инкассацию;

- повышение прозрачности и безопасности платежей для всех агентов этого рынка;
- достижение определенной собираемости налогов.

Что касается анонимности, которую часто ставят в упрек криптовалютам, то хочется привести цитату из заключения организации экономического сотрудничества и развития (ОЭСР): «Определение криптовалюты как средства для совершения мошеннических операций является результатом очевидного (наличия) анонимности, встроенной в систему. На самом деле наличные деньги являются еще более анонимным средством платежа, чем виртуальные валюты… Если имя и адрес (владельца) однажды будут идентифицированы законодательными органами, то они включат мощный механизм, позволяющий отследить все цепочки передачи ценности, что никогда не позволили бы сделать наличные деньги. Аргументы, используемые против анонимности криптовалют, намного слабее, чем против наличных средств».

Как далее отмечает ОЭСР, в отличие от национальной валюты, криптовалюта не обеспечена полным признанием и доверием национального правительства, при этом она не регулируется его постановлениями, ограничивающими какие-либо действия (например, внезапную гиперэмиссию этой валюты). Однако поскольку покупатель ожидает, что другие участники примут ту же криптовалюту в качестве средства сбережения, он будет готов купить ее.

По мнению ОЭСР, есть другой риск: что определенные правительства попытаются принять меры, эффективно исключающие использование виртуальной валюты в качестве валюты как таковой. Это подразумевает вероятность того, что криптовалюта будет объявлена вне закона. В докладе ОЭСР есть такие слова: «Даже если виртуальная валюта не объявлена незаконной, само обсуждение этой возможности наносит убытки взаимному доверию к будущей покупательной силе виртуальной валюты, которая необходима для обеих сторон сделки, чтобы рассматривать ее в качестве средства сбережения». Ниже в главах о российском регулировании мы увидим всю горькую справедливость этих слов [8, с. 81–84].

1.1.2 Описание принципа работы смарт-контрактов

Умные контракты (или смарт-контракты) — одно из приложений блокчейн, вызывающее особый интерес.

Процесс заключения любой сделки — это, прежде всего, составление контракта, в котором прописаны все условия, права и обязательства принимающих участие сторон. Однако в большей части договоров присутствуют не только стороны, заключающие соглашение, но и посредники — банки, нотариусы, регистраторы, регуляторы. Благодаря активному развитию технологии блочных цепей (блокчейн) эта необходимость остаётся в прошлом — на смену обыкновенным контрактам пришли так называемые «умные» контракты, с английского языка — смарт-контракт [20].

Технология смарт-контрактов сама по себе также является перспективной технологией для многих отраслей, в том числе и для образования.

И несмотря на то, что первые идеи появились еще в 1994 году, практические реализации стали возможными благодаря появлению технологии блокчейн, а в особенности — проекта канадско-российского программиста Виталика Бутерина Ethereum, также использующего блокчейн в основе своей работы [29].

Спустя 20 с лишним лет понятие «смарт-контракта» расширилось.

Вот как его определяет Георгий Прокопчук (Российский IoT-центр): «Под смарт-контрактом понимается компьютерная программа, которая позволяет облегчить и автоматизировать соблюдение различных видов контрактов или сделок. Смарт-контракт и блокчейн в силу своей децентрализованной архитектуры и открытости интерфейса дают возможность для образования так называемых распределенных автономных организаций, которые представляют собой прообраз искусственного интеллекта» [8, с. 108].

Определение консалтинговой фирмы Oliver Wyman: «Смарт-контракт — снабженное цифровой подписью, вычислительное соглашение между двумя или более сторонами. Третья виртуальная сторона — про-

граммный агент — может выполнить и осуществить по крайней мере некоторые условия таких соглашений» [8, с. 108].

Мелани Свон определяет смарт-контракт как способ использования криптовалюты для формирования соглашения посредством блокчейна. Эта технология устраняет необходимость доверия между сторонами за счет автоматического определения и исполнения на основе работающего на блокчейне кода, который, в свою очередь, исключает риски, связанные с человеческим фактором [8, с. 108].

Определим понятия смарт-контракта следующим образом.

Смарт-контракт (англ. *Smart contract* — умный контракт) — компьютерный алгоритм, предназначенный для заключения и поддержания коммерческих контрактов в технологии блокчейн [29].

Такие соглашения могут заключаться между двумя людьми, другими словами, peer-to-peer (P2P), человеком и организацией (P2O) или человеком и машиной (P2M).

Смарт-контракты позволяют автоматизировать платежи и перевод валюты или других активов в качестве согласованных условий. Как только будет выполнено заданное в умном контракте условие (например, продажа товаров «1» на бирже «2»), договор выполняется автоматически и активы (например, денежные средства, цифровая валюта, право собственности, данные) обмениваются между договаривающимися сторонами. Затем транзакция реплицируется и проверяется на блочной цепочке.

Смарт-контракты позволяют обменять актив, если третьи стороны не знают о передаче. Это открывает возможность дезинтегрировать всю правовую систему и создать новую форму виртуальных соглашений. На деле, являясь фрагментами кода, которые автоматически выполняют действия, когда соблюдаются заданные условия, умные контракты пока не могут рассматриваться как обычные контракты с юридической точки зрения. Тем не менее, они могут использоваться в качестве доказательства решения той или иной задачи и многочисленные отрасли изучают потенциальные возможности применения таких контрактов. Однако эксперты видят широкое применение

умных контрактов лишь в далекой перспективе, поскольку, несмотря на некоторые попытки их реализации, эта технология находится на стадии экспериментов и пока не созрела для появления первых рыночных продуктов [43].

Для создания смарт-контракта нужны следующие компоненты [20], [29]:

- предмет договора — программа должна иметь доступ к товарам или услугам, по поводу которых заключается контракт, и иметь возможность автоматически дать или закрыть к ним доступ;
- цифровые подписи — все участники инициируют соглашение, подписывая договор своими секретными ключами;
- условия договора — условия смарт-контракта в форме точной последовательности операций, которые должны подписать все участники;
- участники договора — описанные выше модели между двумя людьми (P2P), человеком и организацией (P2O) или человеком и машиной (P2M);
- децентрализованная платформа — смарт-контракт записывается в блокчейн этой платформы и распределённо хранится на ее узлах.

В блокчейне как раз присутствуют вышеперечисленные компоненты.

1.1.3 Описание принципа работы Initial coin offering и понятия токен

ICO, **Initial coin offering**, (с англ. — «первичное предложение монет, первичное размещение монет») — форма привлечения инвестиций в виде продажи инвесторам фиксированного количества новых единиц криптовалют, полученных разовой или ускоренной эмиссией [71].

Встречается также форма «первичного предложения токенов». Помимо этого, термин ICO часто заменяется словом «краудсейл» [71].

Токен (перевод с англ. *Token* — знак, символ; опознавательный знак; жетон) — это единица стоимости, выпущенная частной организацией в системе блокчейн [41].

Согласно Д. Бренеру, последовательность действий в предварительной продаже токенов обычно такова [8, с. 114]:

1. Публикация описания сети и планов на дальнейшее развитие (так называемая *белая книга* (англ. *white paper*).

2. Объявление о предстоящей ICO и публикация исходного кода до генерации первого токена.

3. Развертывание сети и генерация токенов с помощью майнинга; возможно резервирование части токенов для основателей, в качестве вознаграждения за идею и развитие сети.

4. Реклама ICO и продажа токенов всем желающим.

5. Работа по созданию сетевого эффекта, создание приложений и поддержка сети; по мере роста сети возрастает спрос на токены, что ведет к увеличению стоимости пользовательских токенов.

Структура white paper обычно включает в себя следующие структурные элементы [11]:

1. Титульная страница. Включает в себя: логотип, название, краткую суть в одном предложении.

2. Содержание документа.

3. Аннотация. Представляет из себя описанную в нескольких абзацах суть проекта (как правило, размещается на одной странице).

4. Введение. Отражает текущее положение дел в той нише, в которой организация предполагает вести свою деятельность; тенденции, формирующие тот или иной рынок; факторы, влияющие на изменения.

5. Предпосылки. В этом разделе описывается проблема, послужившая толчком к созданию проекта, а также опасность, к которой может привести развитие этой проблемы.

6. Описание проекта. Включает в себя: цели, задачи, миссию, социальную значимость, коммерческую значимость, механику работы, описание прототипа, примеры использования проекта и роли пользователей в нём. Каждый из перечисленных выше пунктов может быть как составной частью общего описания, так и самостоятельными, независимыми подразделами.

7. Маркетинговый анализ. Описание реалий рынка, востребованность проекта.

8. Техническая часть. Описаний технологий, тонкостей реализации.

9. Описание токена и финансовая модель. Подробное описание выпускаемой криптовалюты и ее экономической целесообразности для ее владельцев.

10. Путевая карта разработки. Указание ключевых этапов разработки проекта с датами.

11. Команда проекта. Описание лиц, которые будут работать над проектом, и их должности. Чем авторитетнее люди в команде, тем больше доверия к проекту.

12. Заключение. Подведение итогов, резюмирование, акцентирование внимание на ключевых моментах проекта.

Токены можно заработать, занимаясь майнингом (в сетях биткоина, Etherium или Sia), а также, например, публикуя контент (в сети Steemit). Записанные в блокчейне токены-жетоны могут свободно покупаться и продаваться за любую криптовалюту или за фиатные деньги.

Токены-акции (криптоакции) дают своим держателям право в обмен на инвестиции получать дивиденды в части дохода сети или комиссий за транзакции в ней. Например, в сети Sia 3,9 % от дохода за хранение информации выплачиваются держателям Siafund — токенов-акций сети. Зачастую токены-акции являются долями в децентрализованных автономных организациях: там программным образом эмитируются токены, собираются деньги от их продажи и заключаются контракты с разработчиками. Кроме того, держатели токенов-акций Decentralized autonomous organization (DAO) имеют право

вносить бизнес-предложения и голосовать по существующим предложениям пропорционально пакету токенов-акций. Пример: Digix — компания типа DAO, построенная на платформе Etherium, Golem, SingularDTV, та же Sia [8, с. 113–114].

По мнению уже упомянутого Степана Гершуни, можно выделить три преимущества проведения ICO для предпринимателей и основателей проектов [8, с. 114–115]:

- «возможность получить больший раунд финансирования за более короткий срок по сравнению с традиционным венчурным, оставляя при этом полный контроль у проекта над тем, каким образом распределяются доли;
- мгновенный Public Relations (PR) и строительство экосистемы вокруг проекта. Тот факт, что в ICO принимает участие не дюжина фондов и андеррайтеров, а тысячи и иногда десятки тысяч людей, позволяет еще даже до начала этапа разработки собрать сильное сообщество, заинтересованное в успехе проекта и способствующее его развитию. Можно сказать, что smart money в случае краудсейлов заменяется на crowd wisdom;
- отклик от рынка и ранние клиенты (early adopters). Подобно Kickstater, на котором производители товара собирают заказы на годы вперед еще до начала производства, для блокчейн-проекта интерес на этапе ICO сигнализирует о реакции потенциального рынка на предлагаемый продукт. По сути, инвесторы этапа краудсейла — это своего рода рынок предсказаний, зачастую гораздо более точный, чем дорогостоящие аналитики и консультанты».

1.2 Правовой статус технологии блокчейн

Любые позитивные изменения в правовом положении любой из рассмотренных технологий будет позитивно сказываться и на остальные.

Разрешение ICO как средства финансирования стартапа фактически будет означать разрешение на выпуск собственной криптовалюты компа-

нии — токенов, что, в свою очередь, будет означать признание технологии блокчейн как новой законной формы организации безопасной деятельности в сети Интернет, ведь работа криптовалют и токенов, как уже было сказано выше, неразрывно связана с технологией блокчейн, и даст «зелёный свет» на массовую разработку собственных проектов с использованем ICO, которые будут заключать так называемые смарт-контракты со своими инвесторами и другими заинтересованными лицами.

При дальнейшем развитии данной идеи, блокчейн был выделен как обособленная технология, которая может использоваться за рамками криптовалют. В России она получила название «Технологии распределенного реестра» (англ. *Distributed ledger technology — DLT*) [24].

Правовой режим криптовалют, в частности системы «Биткойн», значительно различается в разных странах. В ряде стран официально разрешены операции с криптовалютами. Обычно они рассматриваются как товар или инвестиционный актив и для целей налогообложения подчинены соответствующему законодательству. Иногда биткойны признают в качестве расчётной денежной единицы (например, в Германии), в других странах (например, в Японии) Bitcoin является законным платёжным средством с налогом на покупку. В других странах (например, в Китае) операции с биткойнами запрещены для банков, но разрешены для физических лиц, при этом Китай является лидером в области майнинга по причине наличия наибольших производственных мощностей. В Швейцарии на криптовалюты действуют такие же правила, как и на иностранные валюты, и эта страна является одной из самой благоприятной юрисдикций для Bitcoin-стартапов и общественных блокчейнов. В России на 2017 год никаких ограничений на использование биткойнов нет. Необходимость регулирования в цифровых децентрализованных активов в позитивном ключе предлагали Президент России Владимир Путин, зампред Центробанка Ольга Скоробогатова, глава Сбербанка Герман Греф, первый вице-премьер Игорь Шувалов. Мнение заместителя министра финансов

Алексея Моисеева существенно смягчилось к 2017 году — от предложения ввести наказание за использование криптовалюты до заявлений о том, что стоит считать криптовалюту финансовым активом. Негативное отношение к биткойну высказывал представитель следственного комитета Георгий Смирнов, однако депутат Либерально-демократической партии России Андрей Луговой категорически не согласен с его позицией. Правовой режим криптовалют в Российской Федерации обсуждается [22].

Несмотря на неопределенный статус рассмотренных технологий в России, государство имеет к ней высокий интерес, что отражено в программе «Цифровая экономика Российской Федерации» из распоряжения Правительства Российской Федерации от 28 июля 2017 года № 1632-р [18].

В документе сказано: «В целях реализации Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы" (далее — Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы), настоящая Программа направлена на создание условий для развития общества знаний в Российской Федерации, повышение благосостояния и качества жизни граждан нашей страны путем повышения доступности и качества товаров и услуг, произведенных в цифровой экономике с использованием современных цифровых технологий, повышения степени информированности и цифровой грамотности, улучшения доступности и качества государственных услуг для граждан, а также безопасности как внутри страны, так и за ее пределами» [18].

Одной из основных сквозных цифровых технологий, которые входят в рамки программы, являются системы распределенного реестра, к которым причисляют и блокчейн.

Кроме того, существуют подходы к применению блокчейна, смарт-контрактов и криптоактивов через уже работающие законы, касающиеся различных информационных технологий, частично относящихся к блокчейну.

К примеру, запись в блокчейне фиксируется хэш-кодом. Хэш — это техническая запись в блоках базы данных блокчейн, содержащая сведения о проведенных транзакциях. С юридической точки зрения хэш — это электронный документ, который может являться письменным доказательством в суде [47].

Характеристики электронного документа [47]:

- документированная информация (на материальном носителе с реквизитами);
- в электронной форме (в пригодном для восприятия с помощью электронно-вычислительной машины (ЭВМ) виде);
- передается по ИТ-сетям и обрабатывается в информационных системах (п. 11.1 ст. 2 ФЗ от 27.07. 2016 № 149 ФЗ);
- подписан простой электронной подписью (ЭП) или неквалифицированной ЭП во исполнение соглашения между участниками электронного взаимодействия (ч.1 ст. 6 ФЗ от 06.04.2011 №63-ФЗ).

Электронная же подпись уже вполне может использоваться как легитимный способ доказательства в суде, но при соблюдении ряда условий [47].

Электронная подпись — это информация в электронной форме, которая присоединена к подписываемой информации и используется для определения лица, подписывающего информацию [19].

Таким образом, к юридическим аспектам блокчейна можно подобраться с помощью юридических аспектов близких к нему технологий, однако нужно понимать, что и несоблюдение определенных законов, также не напрямую относящихся к блокчейну, несёт в себе риски быть объектом интереса со стороны правопорядка и навлечь на себя судебные иски.

1.3 Примеры применения блокчейна в различных сферах

Вопреки отсутствию чёткого регулирования, технология продолжает развиваться, уже завоевав внимание всего мира, и теперь ей пытаются найти применение в очень многих сферах человеческой жизнедеятельности [43], [21].

О многих из них написано в статье «Перспективы развития технологии блокчейн в России: конкурентные преимущества и барьеры» ведущим сотрудником Центра научно-технической экспертизы Института прикладных экономических исследований Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации Л. А. Цветковой [43] и книге А. Генкина и А. Михеева «Блокчейн: Как это работает и что ждет нас завтра» [8, с. 89–94].

В книге «Блокчейн. Схема новой экономики» (Blockchain. Blueprint for a New Economy), исследователь и основатель института блокчейн-исследований, Мелани Свон (Melanie Swan), выделяет три условные области применения данной технологии [28]:

- Blockchain 1.0 — это валюта (криптовалюты применяются в различных приложениях, имеющих отношение к финансовым транзакциям, например системы переводов и цифровых платежей);
- Blockchain 2.0 — это контракты (приложения в области экономики, рынков и финансов, работающие с различными типами инструментов — акциями, облигациями, фьючерсами, закладными, правовыми титулами, активами и контрактами);
- Blockchain 3.0 — приложения, область которых выходит за рамки финансовых транзакций и рынков (распространяются на сферы государственного управления, здравоохранения, науки, образования и др.).

В 2014 году 9 крупных финансовых организаций (Barclays, BBVA, Commonwealth Bank of Australia, Crédit Suisse, Goldman Sachs, J.P. Morgan & Co., Королевский банк Шотландии, State Street Corporation и UBS) создали

финансово-технологическую исследовательскую компанию R3 CEV LLC, известную в России под именем R3 консорциум. Основной целью была заявлена исследовательская деятельность в области возможности применения технологии блокчейн в финансовом и банковском секторе. К концу 2016 году в состав данной организации вошли уже более 50 крупнейших банков и финансовых организаций со всего мира [24].

Целесообразность применения технологий распределенного реестра начали прорабатывать и разработчики различных комплексных информационных систем, в частности развивающие методологию создания решений в рамках концепции «Smart City». Различные примеры первых проработок использования приложений блокчейн-технологий с группировкой по классам, представлены в таблице 1 [24].

Примечание: таблица составлена авторами с учетом данных, представленных на сайте «Ledra Capital» в одной из серии статей блога под названием «Bitcoin Series 24: The Mega-Master Blockchain List» [51].

Таблица 1 — Применение технологии распределенного реестра в приложениях Blockchain

Класс приложений	**Области применения приложений**
Blockchain 1.0	
Информация о конкретной транзакции и ее ценности, назначенной в системе	Криптовалюты в различных приложениях, имеющих отношение к финансовым транзакциям, например системы переводов и цифровых платежей
Blockchain 2.0	
Гарантийные обязательства	Оформление гарантийных обязательств, трехсторонний арбитраж, многосторонняя подпись, сделки с использованием счетов Escrow
Финансовые транзакции	Ценные бумаги, акции компаний, краудфайдинг, облигации, взаимные фонды, производные финансовые инструменты, аннуитеты, пенсии
Частные документы	Долговые расписки, договоры, пари, подписи, завещания, доверенности
Документы, требующие засвидетельствования	Страховые свидетельства, свидетельства о собственности, нотариальное заверение документов
Регистрация нематериальных активов	Патенты, торговые марки, авторские права, бронирование и т.д.

Окончание таблицы 1

Blockchain 3.0	
Свидетельства и лицензии, заверяемые государством	Свидетельства о праве собственности на земельные участки и недвижимость, свидетельства о регистрации транспортных средств, лицензии на право занятия определенными видами деятельности
Удостоверения, заверяемые государством	Удостоверения личности, паспорта, свидетельство о регистрации избирателя, водительские удостоверения, свидетельства о рождении, браке и смерти
Информация и документация, относящаяся к медицине	Данные истории болезни пациентов медицинских учреждений, информация о результатах обследований, регистрация прав доступа медицинского персонала к определенным данным и конкретным пациентам
Информация и документация в сфере образования, науки, культуры	Данные и информация об обучающихся и преподавателях, научных работниках, работниках культуры и искусства, различных транзакциях в сфере образования, науки, культуры (в т.ч. показателях работы учреждений и отдельных лиц)
Информация и документация в сфере ЖКХ	Данные и информация о различных транзакциях в сфере жилищно-коммунального хозяйства: показатели потребления электроэнергии, воды, телекоммуникационных услуг, функционирования систем «умного дома» и т.п.

Основные сферы применения блокчейна — это, прежде всего, финансовая и банковская сферы, для которых пока разрабатывается большинство приложений блокчейн. Перечень технологических решений на основе блокчейн, которые способны революционизировать финансовую систему, довольно обширен. Это — межбанковские расчеты, расчеты между юридическим и физическим лицами, платежи, ценные бумаги, кредитные истории [43].

Микроплатежи — одно из самых перспективных направлений финансовой сферы и бизнеса. Например, до недавнего времени платежи размером в доли цента были слишком затруднительными для пользователей Интернета. Разработка соответствующих приложений на основе блокчейн сделает такие платежи возможными и практичными. Это позволит эффективно монетизировать социальные сети, а также сделать их альтернативным способом оплаты за небольшие работы, такие, например, как заполнение опросов или внештатная редактура для разных клиентов [43].

Перспективой использования блокчейна в торговле является отслеживание цепочки продвижения товаров. В истории не раз встречались ситуации, когда целым индустриям приходилось останавливать производство из-за случаев отравления продуктами одного производителя. Только быстрое реагирование поможет справиться с подобными ситуациями. Для подобных операций блокчейн идеально подходит. С его помощью все поставщики надежно и автономно друг от друга могут идентифицировать свои продукты, а сети магазинов могут точно сообщать потребителям, откуда и какой ингредиент продукта, который они покупают, был доставлен. Например, компания Provenance успешно внедряет технологию блокчейн в супермаркетах. В масштабах глобальных компаний эта задача решается гораздо сложнее, и над ее решением работают все крупные торговые сети [15].

Несмотря на то, что ажиотаж вокруг индустрии потребительских товаров на основе биткойна несколько остыл, технология блокчейн, являющаяся для него основой, остается привлекательной благодаря более низким издержкам, которые она может предложить сторонам в глобальных одноранговых транзакциях [43].

Сбербанк и Федеральная антимонопольная служба (ФАС) России, в свою очередь, уже запустили проект Digital Ecosystem, работающего на основе технологии блокчейн, с помощью которого документами можно будет безопасно обмениваться и хранить в зашифрованном виде без участия операторов связи и посредников, а также использовать электронную подпись. Проект находится в пилотной стадии, однако в нем уже принимают участие другие российские компании, в их числе — «Аэрофлот», «Русский Уголь», «ФортеИнвест» [27].

Находят применение блокчейну и в области авторского права. Американская компания с богатой историей Kodak планирует использовать его для защиты авторских прав на зарегистрированные на платформе изображения и фотографии, что в эпоху либерального Интернета сделать проблематично, и уже собирает средства на инвестиции в проект [72]. Помимо изображений и

фотографий большой спрос есть в музыкальной индустрии. Авторы музыкальных произведений сейчас также сталкиваются с несоблюдением авторских прав и диктатурой музыкальных площадок, из-за чего они недополучают награду за свои труды. За изменение этой ситуации взялись блокчейн-проекты PeerTracks, MUSE, Bittunes и Ujo Music [6]. Также, японский технологический гигант Sony подал патент в Бюро по патентным и товарным знакам Соединенных Штатов Америки по использованию блокчейна в области защиты авторских прав, объясняя это тем, что нынешние технические средства для защиты авторских прав (DRM), нацеленные на оперативную совместимость, «могут быть не очень надежными и полагаются на одну уникальную точку отказа. Если система или поставщик услуг по защите прав уйдут из бизнеса или каким-то другим образом выйдут из строя, пользователь потеряет весь приобретенный контент». Их система может работать для разных видов контента и данных, таких как фильмы, телевидение, видео, музыка, аудио, игры, научные данные, медицинские данные и т.д. [79].

Кроме того, Sony подал еще патент, связанный с использованием блокчейна в сфере образования, для хранения информации, например, об опыте обучения, сертификатах и прочих данных пользователя, а также в концепции, не связанной с образованием напрямую — Интернете транспортных средств, при помощь которой автомобилисты смогут передавать друг другу информацию о дорожных условиях в реальном времени в условиях децентрализованной сети [78].

Эта концепция частично соотносится с другим перспективным направлением — Интернетом вещей, где также не обошлось без блокчейна из-за его децентрализованной природы. Об этом есть статьи, написанные авторами из Латвии, Финляндии [70] и Румынии, Италии [74], а также упоминается и в статье Л. А. Цветковой [43].

Интернет вещей (англ. *Internet of Things*, *IoT*) — концепция вычислительной сети физических предметов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой, рас-

сматривающая организацию таких сетей как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека [9].

Блокчейн станет основой для более легкого взаимодействия между устройствами, когда каждый управляет своими собственными ролями и поведением, облегчит различные виды транзакций между устройствами, такие как регистрация нового устройства, аутентификация удаленных пользователей и контакт для обмена с другими устройствами. Всё это должно быть осуществимо с должным уровнем конфиденциальности и безопасности от несанкционированного доступа [43]. Применений сочетания блокчейна и IoT также огромное количество: на производственных предприятиях, в концепции умного города, в уходе за престарелыми и нуждающимися людьми и многое другое [74], [5].

Другим направлением, в которое хорошо вписывается технология, является здравоохранение. Здесь блокчейн может быть использован, например, как карточка, где будет надёжно и безопасно хранится история лечения пациента или иным способом, о чём написано такими зарубежными авторами как, например, A. Azaria, A. Ekblaw, J. Halamka, A. Lippman из Массачусетского технологического института и Гарвардской медицинской школы в их совместной работе «Case Study for Blockchain in Healthcare: «MedRec» prototype for electronic health records and medical research data» [64], а также в теоретическом исследовании на сайте Европейского координационного комитета [50]. В статье Л. А. Цветковой приводятся примеры реального использования для медицинских записей в Эстонии и исследований в этой же области компаниями Novartis и Pfizer, где пользователи могут разрешать врачам и другим лицам просматривать их медицинские записи по мере необходимости с помощью своего секретного ключа. Записи могут содержать информацию от фитнес-трекера, статус вакцинации, рецепты, предыдущие процедуры, рекомендации врачей и доказательства страховки. Эти анонимные данные о

здоровье откроют новые перспективы для разработки лекарств для фармацевтических компаний [43].

Также перспективной сферой, где бы мог пригодиться блокчейн, является недвижимость. Здесь, например, он может помочь в организации новых форм реестров, титулов собственности и оформления сделок. Записанные в блокчейн-систему блоки будут удостоверять процесс перехода права собственности на собственность — будут подтверждаться денежные переводы, договоры и данные собственника. Это позволит исключить посредников, которые забирают часть суммы в виде комиссии в процессе сделок. Иногда эти проценты выливаются в крупную сумму, особенно если учесть, что жильё, как правило, стоит не дёшево. Вдобавок сократятся риски мошенничества (например, при аренде или продаже квартир) и время для подготовки сделок и справок. Специализированные блокчейн-платформы позволят предотвратить подделку данных, упростят процессы проверки объектов недвижимости перед продажей, клиенты получат доступ к платформам в режиме 24/7. Уже запущены первые проекты — iNation и Международная ассоциация биткойн недвижимости создают распределенный реестр собственников, блокчейн-сервисы для ведения сделок с недвижимостью строят ABN Amro и IBM. Отличился также и уже упоминавшийся ранее российский Сбербанк и Внешэкономбанк в своих блокчейн-проектах по быстрому оформлению сделок с недвижимостью [17].

Коснулся блокчейн и государственного сектора.

Особенно насущным вопросом является проведение голосований. Функционирующие в наше время системы электронного голосования (СЭГ) обладают рядом недостатков. Главный из них — это наличие единого центра, где происходит формирование баз кодов и результатов, откуда производится управление ими и где устанавливаются методы и формы контроля над сбором данных. Проверить корректность результатов извне почти невозможно. Это не позволяет получить ожидаемый обществом уровень доверия к итогам голосования. Кроме того, большинство людей уверенно, что такие системы

слабо защищены от кибератак, а значит, результаты могут быть подтасованы. Благодаря стойкой к изменениям технологии блокчейн, каждый отданный голос будет корректно учтён при принятии важных решений, а референдумы можно будет проводить гораздо чаще из-за простоты организации такого рода формата голосования [8, с. 134].

В России электронное голосование на основе блокчейна уже использует Национальный расчетный депозитарий (НРД). Запуск разработанной для НРД платформы электронного голосования e-voting был анонсирован на первое полугодие 2017 года. Новый сервис позволит владельцам ценных бумаг удаленно принимать участие в голосованиях [8, с. 135].

Помимо голосования блокчейн рассматривают также и в других направлениях, в которых технология распределенного реестра потенциально могла бы помочь государству [8, с. 138]:

- нотариат;
- сбор налогов;
- распределение пособий;
- выдача паспортов;
- работа с земельными кадастрами;
- обеспечение каналов поставок товаров;
- поддержание государственных записей и услуг в целостном виде.

Этот список с примерами применения блокчейна можно продолжать еще долго, но уже ясно, что с каждым годом всё больше человек и организаций находят потенциал в этой технологии.

Более того, в 2018 году по инициативе Германии и Франции на саммит G20, который пройдет в Аргентине, в список вопросов для обсуждения было предложено внести эффективность криптовалют как вид актива [66], [81].

По итогам первых переговоров министрами финансов и главами центробанков стран G20 было принято нейтральное решение. Участники саммита выразили мнение, что пока криптоактивы не угрожают мировой финансо-

вой стабильности, поскольку даже на пике их совокупная рыночная стоимость составляла менее одного процента от мировой экономики, однако они могут служить для уклонения от уплаты налогов, отмывания денег и финансирования терроризма, а у инвестирующих в них граждан могут возникнуть проблемы с получением своих средств. В какой-то момент это может иметь последствия в том числе и для финансовой стабильности. Страны G20 согласились, что ситуация с криптоактивами требует мониторинга и более подробного изучения перед конкретными действиями по регулированию. Конкретные предложения по регулированию было решено представить и обсудить на следующей встрече в рамках саммита G20 в июле [67], [68].

В итоговой декларации [60] также содержатся призывы к международным органам по стандартизации (SSB) по мониторингу криптоактивов и оценке их рисков и к межправительственной организацией по выработке мировых стандартов в сфере противодействия отмывания преступных доходов и финансирования терроризма (FATF) по рассмотрению существующих стандартов FATF в отношении криптоактивов.

1.4 Анализ источников по теме применения блокчейна в образовании и науке

Технология блокчейн не обошла стороной и так или иначе затронула и такие сферы жизнедеятельности как образование и наука.

Поскольку изначально блокчейн и криптовалюты зародились в Интернете, и, по сути, без него функционировать в полной мере не могут, логичным будет то, что большая часть информации о них находится именно во Всемирной сети, в особенности в иностранных ее сегментах.

Способствует этому еще и то, о чём уже было сказано выше — это отсутствие чёткого регулирования со стороны государства, из-за чего и получается, что преобладающим источником для получения информации о феномене является Интернет.

Однако это не говорит о том, что технологию нельзя рассматривать с научной точки зрения, как предмет исследования, и в этом плане можно воспользоваться наработками и перспективными идеями различных деятелей науки в данной области.

Более того, по данной тематике уже написаны книги, являющиеся бестселлерами.

О тех или иных событиях, разработках, анонсах инновационных проектов в сфере криптоиндустрии сообщается в новостных и тематических интернет-ресурсах.

Теперь рассмотрим источники поподробнее.

Впервые принципы распределенной базы данных блокчейн были описаны неизвестным человеком или группой лиц под псевдонимом Сатоси Накамото. В опубликованной 31 октября 2008 года статье «Bitcoin: A Peer-to-Peer Electronic Cash System» [75] был описан Биткойн — полностью децентрализованная система электронной наличности, не требующая доверия третьим сторонам, а в начале 2009 года выпущена первая версия биткойн-кошелька и запущена сеть Биткойн [26].

Поскольку технология является достаточно новой и всё еще развивается, исследований по ней не так много, однако определенные наработки и идеи всё же есть.

Важным источником является книга-бестселлер «Революция блокчейн. Как технология, стоящая за биткойн, меняет деньги, бизнес и Мир», написанная авторами Доном и Алексом Тапскоттами, а затем переведенная на русский язык К. Шашковой и Е. Ряхиной под названием «Технология блокчейн. То, что движет финансовой революцией сегодня» [39].

Дон — известный канадский публицист, бизнес-консультант, государственный советник, учёный. Мировой авторитет в области бизнес-стратегии, организационных преобразований, влияния технологии на бизнес и общество. Профессор менеджмента Университета Торонто, почетный доктор юридических наук трех канадских университетов. В 1993 году основал Меж-

дународный научно-исследовательский центр New Paradigm (сейчас nGenera Insight). Является главным исполнительных директором (CEO) Tapscott Group, известен как автор книг «Wikinomics: How Mass Collaboration Changes Everything», «The Digital Economy: Promise and Peril in the Age of Networked Intelligence» описывающих новую экономическую реальность, и десятка других популярных трудов о технологиях, бизнесе и обществе [40].

Алекс Тапскотт — сын Дона Тапскотта, CEO и основатель венчурного фонда Northwest Passage Ventures, специализирующегося на инвестициях в рынок блокчейн-проектов, также он основал фонд NextBlock Global, специализирующийся на инвестициях в цифровые активы [49].

Кроме того, Алекс вместе со своим отцом основали Институт исследований блокчейна (Blockchain Research Institute) [63]. В нём группа узкоспециализированных исследователей планирует проводить академический анализ влияния блокчейна на широкий круг отраслей, включая финансовые услуги, розничную торговлю и производство, а также влияние технологии на ряд руководящих должностей. Помимо этого, новый исследовательский институт планирует изучать вопрос того, как блокчейн повлияет на ситуацию на рынке труда. Отличительной особенностью института, дистанцирующей его от других аналогичных проектов, станет привлечение «умнейших людей в мире» для проведения исследований за счет хорошей оплаты их труда. Тапскотт отметил, что институт, созданный для того, чтобы предоставить инвесторам моментальный доступ к специализированным исследованиям, проведенным широким кругом лидеров отрасли, в конечном счете отдает большую часть своих знаний. Группа учредителей включает как уже состоявшиеся компании: Accenture, IBM, SAP, Digital Asset, NASDAQ, PepsiCo, Centrica, Liberty Global, the Government of Ontario, University Health Network, так и те, которые являются еще только пионерами в этой области: Nuco, Paycase, Artlery, Votem, Cosmos, YouBase и WISeKey. Ожидается, что этот первоначальный список будет расти и включать членов правительств, компаний и организаций со всего мира. В первый год институт планирует заниматься изучением влияния блокчейна по десяти направлениям: финансовые услуги, розничный

товарооборот, влияние на государства и политический строй, энергетика, высшее образование, логистика, промышленность, медиапространство и телекоммуникации, технологии, здравоохранение и ресурсооборот. Аффилированные организации, среди которых Hyperledger, Палата цифровой коммерции (Chamber of Digital Commerce) и Enterprise Ethereum Alliance помогут свести к минимуму объем ненужной работы [63].

И хотя в проектах Алекса находили несостыковки [14], основываясь на вышеизложенном, можно сделать вывод, что авторы исследовали технологию в течение длительного времени и определенно располагают огромным багажом знаний в области криптовалют и блокчейна, что они и демонстрируют в своей книге.

В этой книге рассказывается об истории возникновения и развития технологии, начиная от создания криптовалюты Биткойн, раскрывается суть алгоритма ее работы (так называемых цепочек блоков транзакций), выведены принципы для решений, создающихся на основе данной технологии. Помимо важности технологии в финансовой сфере, авторы отмечают также ее революционный характер и применение во множестве других сферах жизни, опыт которых можно переложить в том числе и на образование.

Кроме того, у Тапскоттов вышла статья в журнале «Educase» под названием «The Blockchain Revolution and Higher Education» [80]. В ней блокчейн выступает как основа для новой эры Интернета — Интернета ценностей, а его роль в высшем образовании подразделяется на четыре категории:

- идентификация и студенческий учёт: как идентифицировать студентов, защищать их конфиденциальность, оценивать, вести учёт, проверять достижения, сохраняя эти данные в безопасности;
- новая педагогика: как настроить преподавание под каждого ученика и создавать новые модели обучения;
- расходы (студенческие задолженности): как оценивать и финансировать образование, как вознаграждать студентов за качество их работы;

- мета-университет: как разрабатывать совершенно новые модели высшего образования, чтобы мечта бывшего президента Массачусетского технологического института Чака Веста могла стать реальностью.

Сооснователем проекта Teachur (рисунок 12) Беном Блэйром на платформе для социальной журналистики «Medium» размещены ряд полезных для темы исследования статей, в частности, приводятся особенности самого проекта Teachur, реализованного на технологии блокчейн:

1. «Using blockchain to re-imagine learning» [54] — сообщает о тех проблемах в образовании начальной и средней школы, который может решить проект Teachur. Его суть заключается в новом подходе для оценивания учащихся по тем или иным стандартам, строгой и безопасной системе хранения этих данных и в легкости ее переноса. Особенность инновационной системы оценивания заключается в том, что оценка связывается с теми знаниями и целями, которые были поставлены с тот или иной момент времени, и путь которых основывается на предыдущих знаниях, целях и оценках, подобно тому, как связываются в цепочки блоки в блокчейне, гарантируя безопасность и лёгкость их переноса, при этом позволяя производить оценку более творчески и экспериментально, в отличие, например, от тестирования.

2. «4 Use Cases for Blockchain for Higher Ed» [52] — рассказывается о четырёх способах применения технологии блокчейн в высшем образовании, реализованных в проекте Teachur: учёт процесса обучения, смарт-контракты для получения диплома, смарт-контракты для двустороннего рынка, токены платформы Teachur. Цели, достигнутые в процессе обучения, представляют из себя надежный и полный отчёт о деятельности обучаемого, которым они могут в любой момент поделиться, если пожелают, что позволяет легко находить сотрудников и партнёров с необходимыми навыками. А получение диплома представляет из себя смарт-контракт, исполняемый автоматически при выполнении необходимого условия, что сразу становится достоверным подтверждением способностей обучаемого. Преподаватели могут получать отчисления за долю или целую часть от разработки и последующего исполь-

зования курсовых работ, учебных материалов и т.д. В системе реализованы собственные токены, которые можно получить как раз в виде отчислений или за иной вид работы. Таким образом, работа с системой становится экономически выгодной.

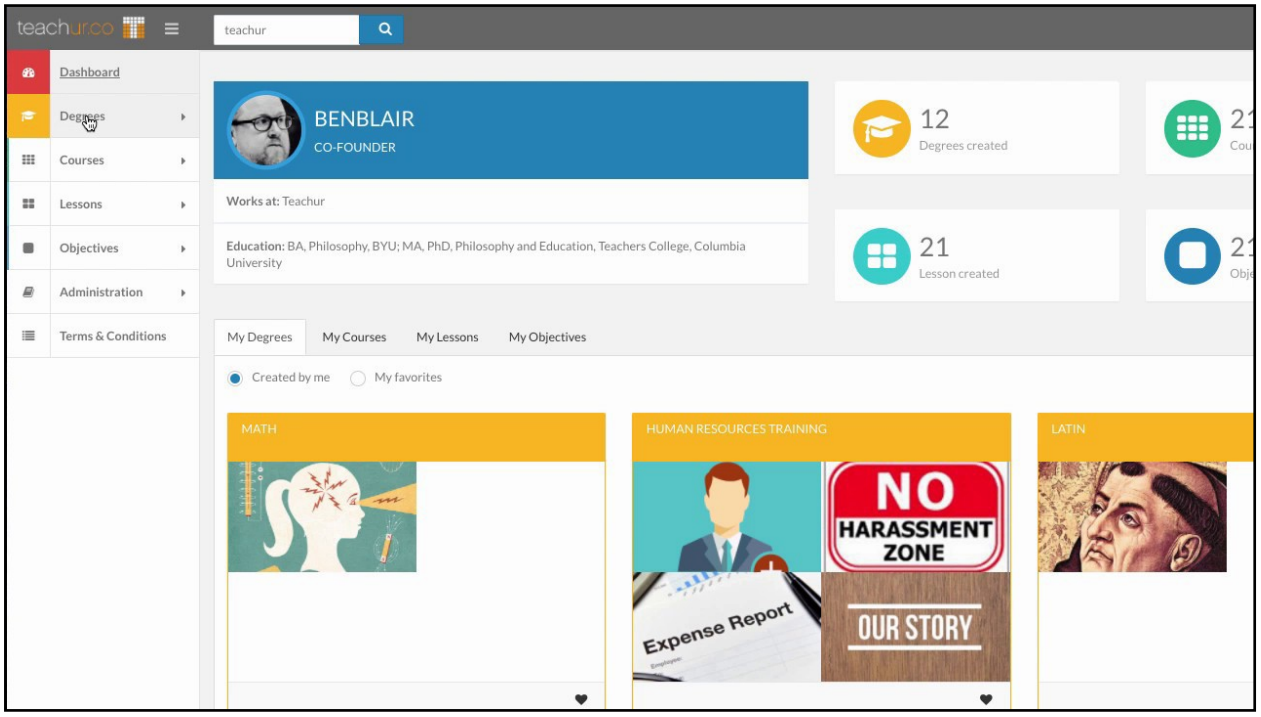


Рисунок 12 — Интерфейс Teachur

3. Исследованиями в области применения смарт-контрактов в процессе обучения поделился Бен Блейр в статье «Smart Contracts for Effective Curriculum» [53], где смарт-контракты используются для всего учебного плана, когда достижение определенной контрольной точки учебного плана связано с определенным жестко прописанным условием, а все учебные материалы являются интеллектуальной собственностью их создателя, за использование которых он получает отчисления. Успешная работа по учебным материалам определенных преподавателей увеличивает спрос на них, что стимулирует их к созданию высококачественных материалов.

О том, чтобы стать первыми, кто внедрит блокчейн для подтверждения действительности аттестатов и сертификатов кандидата на его соответствие требуемым компетенциям, написал Люк Паркер в статье «Authenticating

academic certificates on the Bitcoin blockchain» [76], которая, по сути, является кратким обзором применения технологии таким образом.

Вопросами защиты и подтверждения действительности сертификатов [83], [55], а также системой репутации [58] с помощью блокчейна особенно занимаются в Массачусетском технологическом институте. Ими были выпущено несколько версий программы Blockcerts с открытым исходным кодом, реализующей учёт и выдачу сертификатов с возможностью делиться ими с работодателями. На рисунке 13 представлена архитектура их программы. В статье «What we learned from designing an academic certificates system on the blockchain» говорится также и о проблемах, с которыми они сталкиваются в своей работе: например, обеспечение возможности делиться своими академическими достижениями с одними, но при этом держать их в тайне от других.

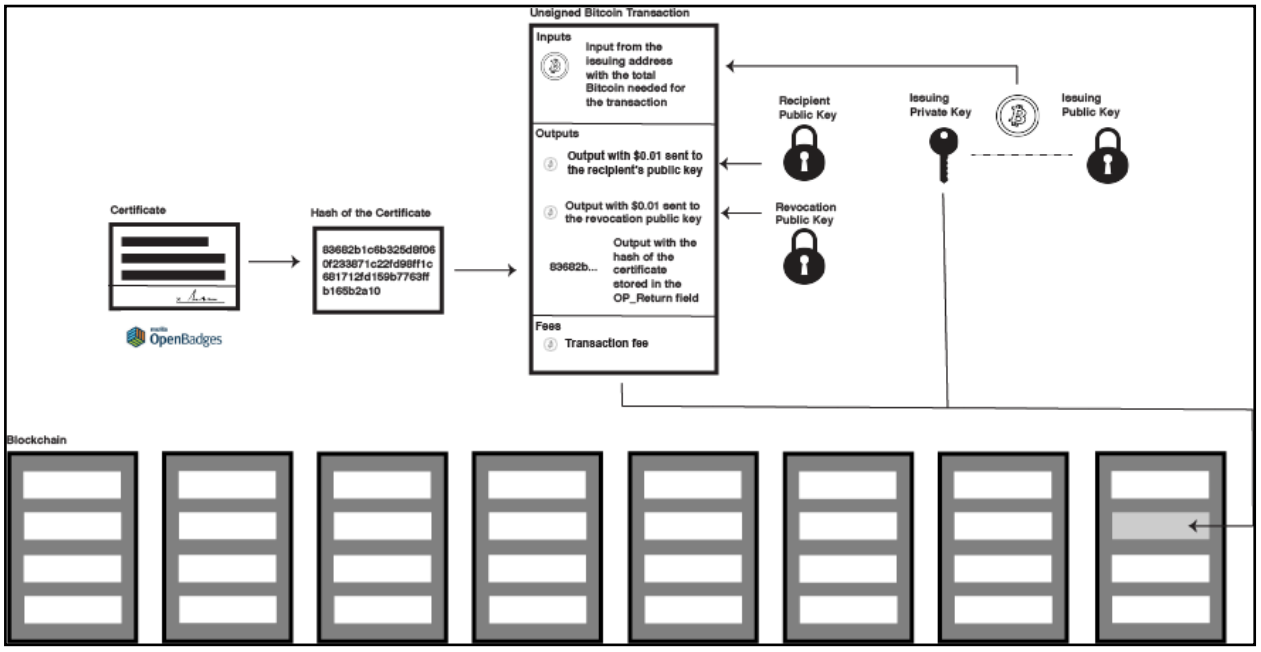


Рисунок 13 — Архитектура программы цифровых сертификатов Массачусетского технологического института

Более того, Массачусетский технологический университет в этом году предоставляет возможность студентам получить цифровую версию их дипломов на блокчейне в рамках экспериментальной программы, позволяющей сделать академические данные безопасными и переносимыми [62].

Также на платформе «Medium» опубликована еще одна статья, касающаяся технологии блокчейна в образовании, «Blockchain Technology Needs to Be Changing Education» [57]. В ней блокчейн выступает в роли защиты учебных данных учеников, которые формируются и подстраиваются под ученика адаптивными системами диагностики (например, i-Ready, Edulastic).

В личном блоге Одри Уоттерса Hack Education под заголовком «The Blockchain for Education: An Introduction» [82] был проведен разбор сначала истории и работы технологии блокчейн, а затем рассмотрены возможности ее применения в образовании.

На сайте Hackernoon, где размещаются статьи, касающиеся хакинга, разработки, искусственного интеллекта и криптовалют, размещена статья «How Can Blockchain Technology Innovate Your Education» [65], в которой рассматриваются инновационные идеи для образования с применением блокчейна, платформа для обучения LiveEDU, проводятся некоторые параллели с дистанционным обучением, понятием массовых открытых онлайн-курсов (MOOC).

Подобный пример уже случался, когда на фоне развития Интернета многие процессы стали переноситься электронный вид, в том числе это коснулось и образования. Так появилось *электронное обучение (e-learning)*, а затем и *массовые открытые онлайн-курсы (MOOC)*, завязанные на обучении дистанционно [33], [34]. Ярким примером такой формы обучения стал проект Codecademy, представляющий из себя площадку для изучения программирования в режиме онлайн [36].

Возможность получить знания из любой точки мира, а также более низкую стоимость или вовсе бесплатное обучение не могла оставить людей равнодушными. Комбинирование различных курсов позволяет предлагать обучаемым различные стратегии обучения [33], [34].

Внедрение технологии блокчейн, позволит стандартизировать выдаваемые документы, что в свою очередь может стандартизировать образование во всем мире [21].

Подтвержденные знания и навыки кандидатов могут храниться в единой базе данных, что позволит выбирать кандидатов по динамическому отбору исходя из их набора умений и требуемых навыков для выбранной должности [21].

Итогом создания данной базы данных будет наличие открытого рынка кандидатов с подтвержденными знаниями. А это в свою очередь позволит создать спрос на конкретные компетенции и создаст тенденции на изучение определенных образовательных программ, в результате которых и формируются эти компетенции [21].

Образовательные организации будут в реальном времени видеть картину требуемых кандидатов и выпускать соответствующие образовательные программы или обучающие курсы [21].

В результате это позволит сократить разрыв между рынком труда и рынком образования, а также решить проблему стремительной деактуализации учебных программ, резвившейся в ходе стремительного роста информационных технологий [21].

Сегодня обучение и подтверждение действительности аттестатов и сертификатов кандидата на его соответствие требуемым компетенциям является дорогостоящим и длительным процессом как для образовательного учреждения, так и для предприятия [21].

Предприятие, в случае несоответствия кандидата определенным требованиям, в будущем может понести убытки.

Некоторые школы обратились за помощью к технологии блокчейн, как к недорогому и надежному способу записи академических успехов ученика, представляющий из себя децентрализованный регистр, надежно хранящий данные в Интернете с открытым доступом для публики [21].

Один из таких примеров — Holberton School of software engineering (школа разработчиков программного обеспечения), которая была создана как проект-альтернатива колледжам. В октябре 2015 года школа объявила о

намерении сохранять аттестаты студентов на блокчейн, начиная с 2017 года [21].

Японская компания Sony, создавшая сервис Sony Global Education, в конце 2017 года уже использует технологию блокчейн при выдаче сертификатов. Своим примером они собираются показать, как данная технология станет будущим в области обеспечения достоверности знаний, обучающихся в образовании. Так же планируется показать возможности технологии на примере «следующего поколения ИТ-школы» для Министерства внутренних дел Японии [77], [61], [21].

Sony Global Education считают, что индивидуальные данные о производительности обучаемого в образовании так же ценны, как, например, персональная кредитная история. При использовании технологии блокчейн данные будут защищены цифровой подписью и могут быть безопасно переданы другим заинтересованным лицам. Сохранение достоверных данных позволит получить полную историю обучаемого (например, компьютерный тест) на полностью защищенной платформе [77], [61], [21].

Таким образом, реализация технологии блокчейн в образовании уже сейчас находит свое применение. Конечно, основной упор сделан на реализацию возможности безопасного хранения сертификатов, аттестатов, дипломов и успеваемости обучаемых, что может решить следующие задачи:

- стандартизация и глобализация образования (возможна стандартизация без глобализации);
- наличие достоверного, открытого и единого рынка кандидатов с подтвержденными знаниями;
- актуальность образовательным программ, а следовательно, сокращение разрыва между рынком труда и рынком образования.

В Объединенном научно-исследовательском центре Европейской комиссии опубликовано большое исследование «Blockchain in Education» [69], затрагивающие многие аспекты тех или иных способов применения блокчей-

на в сфере образования. На основе проведенного исследования выводятся восемь сценариев применения технологии в образовании:

1. Обеспечение постоянной защиты сертификатов обучаемых.
2. Использование блокчейна для многоступенчатой аккредитации.
3. Автораспознавание и передача средств с помощью блокчейна.
4. Использование блокчейна в качестве паспорта по обучению на всю жизнь.
5. Блокчейн для отслеживания интеллектуальной собственности и поощрения как первичного, так и повторного ее использования.
6. Получение платежей от студентов через блокчейн.
7. Предоставление студентам финансирования через блокчейн в форме ваучеров.
8. Последующая идентификация уже прошедших проверку студентов в образовательных организациях.

1.5 Анализ источников по теме проблем и уязвимостей в Российской системе образования и науки

Современная система образования переживает достаточно тяжёлые времена. Советская школа разрушается, на смену приходят европейские тенденции. Порой внедрение новшеств происходит на неподготовленную почву, или инновации не адаптированы под российский менталитет. Проблем в современном российском образовании достаточно [37]. Попробуем в них разобраться.

Во-первых, всё чаще приходится слышать о кризисе старой системы образования. В высшей школе выход был найден в переходе на систему бакалавриат и магистратура. Но остались не охваченными средняя школа и профессиональные училища. Недавно изданный закон об образовании призван решить и эту проблему. А насколько он будет действенным, покажет практика. Сейчас же стала очевидной необходимость изменения подхода к

процессу обучения. Современное общество находится на таком уровне развития, когда пора уже отойти от обучения как заучивания фактов. Нужно учить детей самостоятельно добывать информацию, понимать её и применять на практике. Этому способствует развитие критического мышления [46]. Одним из способов такого развития является технология развития критического мышления через чтение и письмо, разработанная американскими педагогами К. Мередитом, Д. Стилом, Ч. Темплом, С. Уорреном и описанная отечественными учёными И. О. Загашевым, С. И. Заир-Беком и др. [46]. Требуется колоссальный труд по подготовке не только новых учебников для учеников и пособий для учителей, но и самих педагогических работников [23].

Другой проблемой образования в России называют излишнюю его теоретическую направленность. Воспитывая учёного-теоретика, мы создаем огромную нехватку узких специалистов. Получив хорошую теоретическую подготовку, мало кто может применить знания на практике. Поэтому, устроившись на работу, новые сотрудники переживают серьёзную адаптацию, связанную с невозможностью сопоставить свои знания с практической деятельностью [23].

Одной из фундаментальных проблем, порождающей другие, является недостаточность финансирования [37].

Напомним, что при этом расходы на высшее образование в федеральном бюджете снижаются четыре года подряд, и их планируется снижать и дальше [7].

Неудовлетворительное финансирование является одной из основных причин возникновения кризисных ситуаций в системе образования. В целом потребность образовательных учреждений в финансовых средствах обеспечивается за счет средств бюджетов всех уровней менее чем на четверть. Сохраняется тенденция сокращения реального объема ассигнований на нужды образования. В текущих ценах они сократились примерно в пять раз, что в сопоставимых ценах составляет более чем двадцатикратное уменьшение.

Острейший дефицит финансовых ресурсов породил опасность потери лучшего из того, что имелось и еще имеется в системе образования Российской Федерации. Сохраняют угрозу углубления в системе образования, способные нанести серьезный ущерб состоянию безопасности государства [37].

В то же время необходимо понимать, что сама по себе финансовая поддержка образования не приведет к резкому повышению его качества. В российском образовании мало профессиональных менеджеров, умеющих эффективно расходовать деньги [10].

Определенные сложности характерны для деятельности преподавательских кадров. С одной стороны, можно отметить старение кадрового состава преподавателей вузов. С другой стороны, отмечается неразвитость системы повышения квалификации и переподготовки педагогических кадров. Отсутствует организованная, систематическая кадровая работа по направлению преподавателей в учебные центры повышения квалификации [10].

Недостаток в России высококвалифицированного кадрового потенциала, в первую очередь в сфере научно-инновационной деятельности, является одним из сдерживающих факторов при разработке крупных инвестиционных проектов национального и международного масштабов, тормозом успешного развития инновационных секторов российской экономики [10].

Сегодня будущие абитуриенты не выбирают профессию педагога, поскольку она низкооплачиваема, что приводит к необходимости поиска преподавателями дополнительных заработков [10]. Работа преподавателем предполагает стрессы, перенапряжение, проверка домашнего задания внерабочее время — и это за небольшую зарплату. Выпускники отдают предпочтение экономическим, юридическим специальностям [45].

Доклад «Образование в России, 2016» [73] Ивана Куриллы, профессора Европейского Университета в Санкт-Петербурге, был опубликован в Russian Analytical Digest No. 191. Начинается он с цитаты президента России, назвавшего образование «самым главным, на что мы должны обратить внимание в ближайшие годы». Несмотря на заявленную принципиальную важ-

ность этой сферы, ситуация в ней остаётся тяжёлой, констатирует И. Курилла [7].

Для действующей образовательной политики является наличие острых противоречий между академией и бюрократией.

Первое из них — в том, как педагогический процесс оказался задавлен несметным количеством различной документации, которую педагоги должны заполнять [7].

Второе противоречие, которое отмечает профессор в докладе, также связано с бюрократическим подходом к решению проблем, но касается оно оценки компетентности преподавателей. Чтобы продолжать работу, они должны соответствовать выставленным им количественным показателям — иметь высокиий индекс Хирша, нужное число публикаций в международных рецензируемых журналах [7].

«Новые требования Минобра подтолкнули российских учёных к тому, чтобы печататься за рубежом, но одновременно с этим новые стандарты привели к отчуждению нескольких больших групп педагогов, включая тех, кто не пишет по-английски, и тех, кто считает эти требования искусственными и даже вредными для российской науки» [7].

Эти и другие инициативы по укреплению международного сотрудничества (финансирование крупных грантов для привлечения зарубежных ученых и создания интернациональных исследовательских групп) входят в противоречия с антизападной риторикой и изоляционной политикой России в других областях, отмечает И. Курилла [7].

Таким образом, в сфере образования в России сейчас есть много разобщённых групп, которые не могут объединиться для улучшения существующей системы, поскольку не поддерживают требования друг друга [7].

По мнению И. Куриллы, для улучшения системы образования министерство в первую очередь должно отказаться от бюрократизации [7].

По его словам, это предложение не потребует дополнительного финансирования.

«А если уменьшить бюрократическое давление и распустить все соответствующие подразделения Минобрнауки, Рособрнадзора и всяких облоно, гороно и районо, — можно еще и сэкономить и поднять зарплату учителям», — добавляет И. Курилла [7].

Вопрос поднятия зарплаты работникам образования так и остаётся нерешённым — мы «до сих пор где-то на позорном месте в мире по этому уровню», указывает профессор. Улучшить положение университетских преподавателей также помогло бы инвестирование в рынок академического труда [7].

Особо остро выпускники школ и студенты-первокурсники начинают ощущать низкий уровень связи между этапами образования. Так, теперь, чтобы поступить в вуз, часто родители нанимают репетитора для сдачи Единого государственного экзамена (ЕГЭ), т.к. школа не может дать соответствующий уровень подготовки. Особенно если вуз престижный и конкурс на выбранное направление подготовки будет большой. Отличается и уровень требований, который предъявляли в школе, от уровня, необходимого для обучения в вузе. Поэтому первый год обучения — самый тяжёлый для студентов и отличается наибольшим количеством отчисленных ребят, не выдержавших нового ритма учёбы [23].

Следующая проблема вытекает из, казалось бы, положительной тенденции на увеличение спроса на вузы. Всё большее число вчерашних школьников стремится получить документ о высшем образовании. Но эта тенденция имеет свой недостаток, т.к. увеличилось число негосударственных вузов, с которыми нужно быть очень осторожными и внимательными [23].

Конечно, нельзя пройти мимо такой проблемы, как коррупция. Одних объявлений о продаже дипломов о высшем образовании в сети Интернет можно найти множество. К коррупции можно отнести и денежные поборы в школе, взятки за экзамены (зачёты), хищение средств из бюджета [23].

Наблюдается также падение престижа профессионально-технических училищ (ПТУ) и техникумов. Это ведёт к нехватке рабочих кадров на предприятиях, в обслуживающей сфере и т.д. [23].

Закон об образовании — попытка решить ряд назревших проблем. Но для полноценного развития нации необходимо принятие ещё ряда мер в сфере образования. Государство должно не только стремиться сделать так, чтобы образование соответствовало международным стандартам, но и полностью удовлетворяло нужды страны в квалифицированных специалистах и высокообразованных гражданах [23].

Много говорят в последнее время о доступности образования для лиц с ограниченными возможностями здоровья (ОВЗ). Из-за недостаточно развитого в некоторых случаях уровня обеспеченности условиями для комфортного получения образования для данных категорий лиц (отсутствие лифтов, пандусов, необходимой инфраструктуры, неразвитость инклюзивного образования), иногда приходится переходить на самостоятельное обучение. Также это касается и других граждан, которые по тем или иным причинам были вынуждены перейти на самостоятельное обучение [38].

Самостоятельное обучение часто сопровождается проблемой поиска информации. Интернет наполнен множеством информации, но не вся она полезна. Также требуется жёсткая самодисциплина, которая ослабевает с появлением каждого нового препятствия и каждый новой проблемы на пути к обучению. А без постоянного контроля желание может и вовсе пропасть [33], [34].

Остро строит проблема патентования в России. Если сравнить с Соединенными Штатами Америки в России подаётся значительно меньше заявок на патентные разработки (578802 против 40308 соответственно). Значительная доля заявок иностранных патентных разработок приходится на страны, где патентование развитие намного хуже, чем в России [1].

А. Р. Аюпова и Н. Г. Хабиров утверждают, что это связано с множеством недоработок и слабых мест в российском законодательстве и устройстве процедур патентования, а именно [1]:

- схожесть процедуры получения патента и изобретения на полезную модель даёт возможность подавать заявки одновременно и на изобретение, и на полезную модель, а это создает неточности в формуле объектов патентования, допуская их разное толкование. А любую неоднозначность в описании нарушитель сможет использовать для ухода от ответственности за нарушение исключительных прав;
- внесение небольших изменений в уже известные технические решения и модели и использование несовершенства процедуры получения патента для патентования данной модификации как нового технического решения или модели.

Используется также промышленный шпионаж, обратный инжиниринг или обратное проектирование с целью получить доступ к коммерческой тайне любыми способами, а затем оформить её на себя [1].

Всё это является факторами, тормозящими научно-технический и экономический прогресс [1].

Распоряжением Правительства Российской Федерации от 17 ноября 2008 г. утверждена Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 г., в которой отмечается, что модернизация системы образования является необходимым условием формирования инновационной экономики страны, основой динамичного экономического роста и социального развития общества, а также фактором благополучия граждан и безопасности страны. В концепции задан стратегический подход к развитию российского образования и определены следующие задачи: обеспечение инновационного характера базового образования; модернизация институтов системы образования как инструментов социального развития; создание современной системы непрерывного образования, подготовки и переподготовки профессиональных кадров; формирование ме-

ханизмов оценки качества и востребованности образовательных услуг с участием потребителей, участие в международных сопоставительных исследованиях. Функционирование системы непрерывного образования обеспечивается преемственностью образовательных программ различного уровня, направленности, образовательных структур и механизмов регулирования деятельности [35].

Технологичность образования и науки будут достигаться с помощью уже отмеченной программы «Цифровая экономика России» [18].

В итоге и получается, что из-за совокупности как описанных проблем, так и множества других Россия на сегодня по уровню образования находится на 34 месте [25].

Выводы по первой главе

На основе проведенного анализа было выявлено, что технология блокчейн обладает следующими особенностями:

- прозрачность;
- децентрализованность;
- анонимность;
- равноправие;
- безопасность.

В зависимости от реализации технологии распределенного реестра в том или ином проекте блокчейна выделяют различные преимущества и недостатки технологии.

Согласно Т. Г. Ильиной, преимущества таковы:

- высокая скорость операций и мобильность;
- очень низкая стоимость эмиссии;
- безопасность;
- идеальная сохраняемость;
- возможность полноценного контроля;

- децентрализация;
- многофункциональность;
- универсальность;
- независимость;
- отсутствие инфляции;
- открытость и публичность;
- делимость;
- отсутствие запретов;
- анонимность;
- отсутствие подделок;
- простота, удобство и доступность;
- возможность зарабатывать;
- ликвидность и конвертируемость.

Недостатки же у них следующие:

- необходимость в стойкой криптографической защите;
- необходимость в инструментах передачи, пользования и хранения;
- отсутствие должного юридического урегулирования и гарантий;
- недостаточная распространенность;
- нестабильный курс;
- вирусы и киберпреступность;
- ограниченная эмиссия.

Данные преимущества и особенности позволили развиться следующим технологиям:

1. Смарт-контракты — описанные с помощью программного кода, алгоритмы, позволяющие автоматически при выполнении необходимых условий исполнять соглашение, заключенное в контракте. Такие соглашения могут заключаться между двумя людьми (P2P), человеком и организацией (P2O) или человеком и машиной (P2M) Для создания смарт-контракта необходимы следующие компоненты: предмет договора, цифровые подписи, условия договора, участники договора и децентрализованная платформа.

2. Initial coin offering (ICO) и токены. ICO — это форма привлечения инвестиций в виде продажи инвесторам фиксированного количества новых единиц криптовалют, полученных разовой или ускоренной эмиссией. Токены — это, по сути и есть, эта криптовалюта, имеющая разные виды и функции в зависимости от системы, в которой они созданы. Благодаря особенностям блокчейна, ICO имеет следующие преимущества по сравнению с традиционными способами привлечения инвестиций: большее количество привлеченных средств за меньший срок, большее количество заинтересованных лиц для пиара и строительства экосистемы вокруг проекта, быстрый отклик рынка и раннее появление клиентов и инвесторов.

Правовые положения криптовалют, блокчейна, смарт-контрактов, ICO и токенов так или иначе взаимосвязаны между собой и формируют общее юридическую обстановку, которую на сегодняшний день можно охарактеризовать следующим образом.

Как такового запрета на вышеперечисленные технологии нет, за исключением случаев, когда деятельность, связанная с ними, противоречит законодательству Российской Федерации. Однако все риски граждане, пользующиеся услугами организаций, использующих эти технологии, берут на себя.

Вышеописанные технологии нашли своё применение во многих сферах жизнедеятельности. Среди них:

- финансовая и банковская сферы (межбанковские расчеты, расчеты между юридическим и физическим лицами, платежи, ценные бумаги, кредитные истории);
- микроплатежи (оплата за небольшие работы);
- торговля (отслеживание цепочки продвижения товаров);
- документооборот; авторское право (на изображения и фотографии, музыку, универсальные решения на разные виды контента и данных);
- Интернет транспортных средств;
- Интернет вещей;
- здравоохранение (история лечения пациента);

- недвижимость (новые формы реестров, титулов собственности и оформления сделок);
- госсектор (голосование, нотариат, сбор налогов, распределение пособий, выдача паспортов, работа с земельными кадастрами, обеспечение каналов поставок товаров, поддержание государственных записей и услуг);
- и многое другое.

Нашла своё применение технология в таких сферах как образование и наука.

Исходя из проведенного анализа были выведены следующие подходы к её применению в этих сферах:

1. Идентификация студента.
2. Учёт успеваемости студента.
3. Оплата обучения.
4. Стипендии и поощрения.
5. Мета-университет.
6. Связывание каждых новых полученных оценок с целями и знаниями, которые, в свою очередь, связываются с полученными ранее целями и знаниями, на которых они основаны и уровень которых также был оценен.
7. Автоматическая выдача дипломов, аттестатов и сертификатов при достижении определенного результата.
8. Подтверждение действительности дипломов, аттестатов и сертификатов.
9. Безопасное хранение и передача информации.
10. Проведение тестирований, опросов и голосований.
11. Привлечение инвестиций.
12. Аккредитация и контроль за образовательным учреждением.
13. Система репутации и портфолио.

Объединенный научно-исследовательский центр Европейской комиссии, в свою очередь, выделяет следующие сценарии применения:

1. Обеспечение постоянной защиты сертификатов обучаемых.
2. Использование блокчейна для многоступенчатой аккредитации.

3. Автораспознавание и передача средств с помощью блокчейна.

4. Использование блокчейна в качестве паспорта по обучению на всю жизнь.

5. Блокчейн для отслеживания интеллектуальной собственности и поощрения как первичного, так и повторного ее использования.

6. Получение платежей от студентов через блокчейн.

7. Предоставление студентам финансирования через блокчейн в форме ваучеров.

8. Последующая идентификация уже прошедших проверку студентов в образовательных организациях.

Для выявления подходов, через которые возможно было бы применить технологии, основанные на блокчейне, был также проведён анализ проблем и уязвимостей, присутствующих в образовании и науке России. Были получены следующие подходы, улучшение положения которых предполагается возможным с помощью блокчейна:

- финансирование;
- внутренние выплаты образовательного учреждения;
- снижение бюрократической составляющей и упрощение документооборота;
- повышение доступности образования;
- структурирование научных исследований;
- сохранность и неизменность академических успехов;
- упрощение процесса патентования;
- обеспечение непрерывности образования.

2 ОПИСАНИЕ ПОДХОДОВ К ПРИМЕНЕНИЮ ТЕХНОЛОГИИ БЛОКЧЕЙН В ОБРАЗОВАНИИ И НАУКЕ

2.1 Модель реализации сценария использования технологии блокчейн для отслеживания успеваемости обучающегося

2.1.1 Регистрация пользователей

В процессе обучения бывают случаи, когда обучающийся начинает отставать от других по определенной дисциплине или даже ряду дисциплин, и, если не отреагировать сразу же, на последующих этапах отставание будет увеличиваться, а проблемы будут нарастать как снежный ком.

Найти момент, где именно начались проблемы, не всегда удаётся найти, ввиду того, что информация о пройденных этапах не имеет лёгкого доступа ни со стороны преподавателей, ни со стороны обучающихся. В области быстрого доступа находятся, как правило, лишь конечные результаты (оценки, сертификаты об успешном завершении и т.д.), и то зачастую это будут лишь самые свежие данные, и откатиться на более ранний этап становится практически невыполнимой задачей.

В описанной модели эту задачу предлагается решить с помощью блокчейна.

При создании наглядного изображения модели брались во внимание принципы представления информации на экране [30], [31].

Перед началом работы с системой необходимо пройти процесс регистрации (рисунок 14).

На первом этапе регистрации пользователь (будь то обучающийся или преподаватель) должен сгенерировать для себя приватный ключ на основе каких-либо персональных данных или их комбинации. Желательно, чтобы это была такая информация, которая всегда будет доступна, восстанавливае-

ма в случае утери и неизменна в течение долгого времени. В качестве примера был взят страховой номер индивидуального лицевого счёта (СНИЛС) (рисунок 15).

Приватный ключ принадлежит только пользователю.

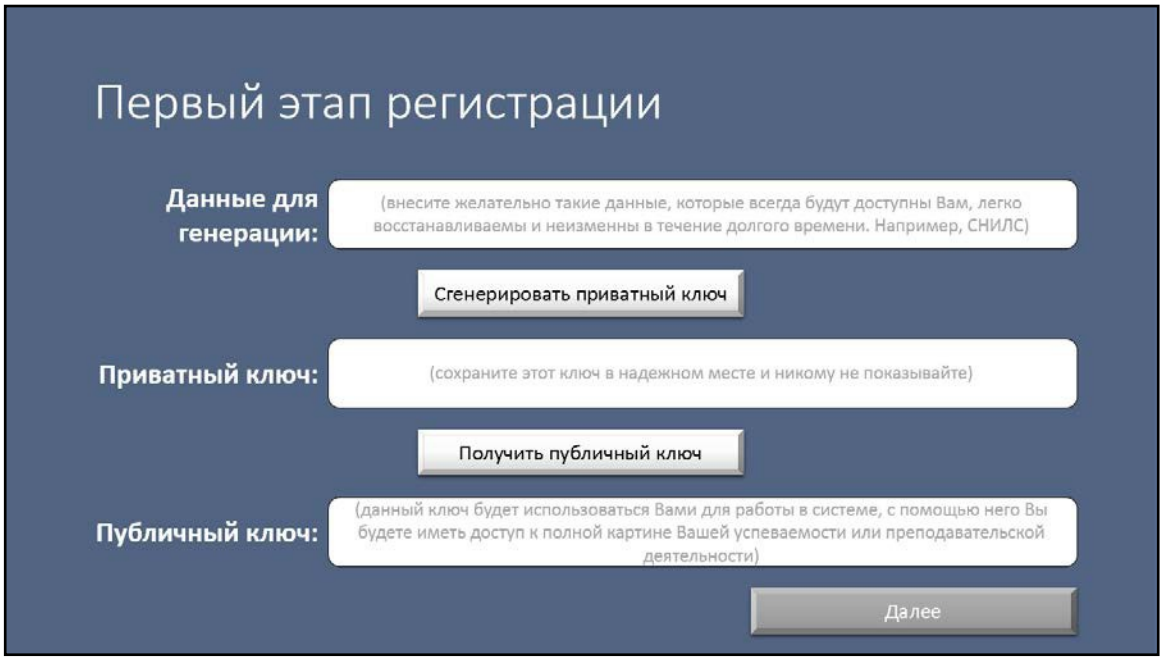


Рисунок 14 — Первый этап регистрации

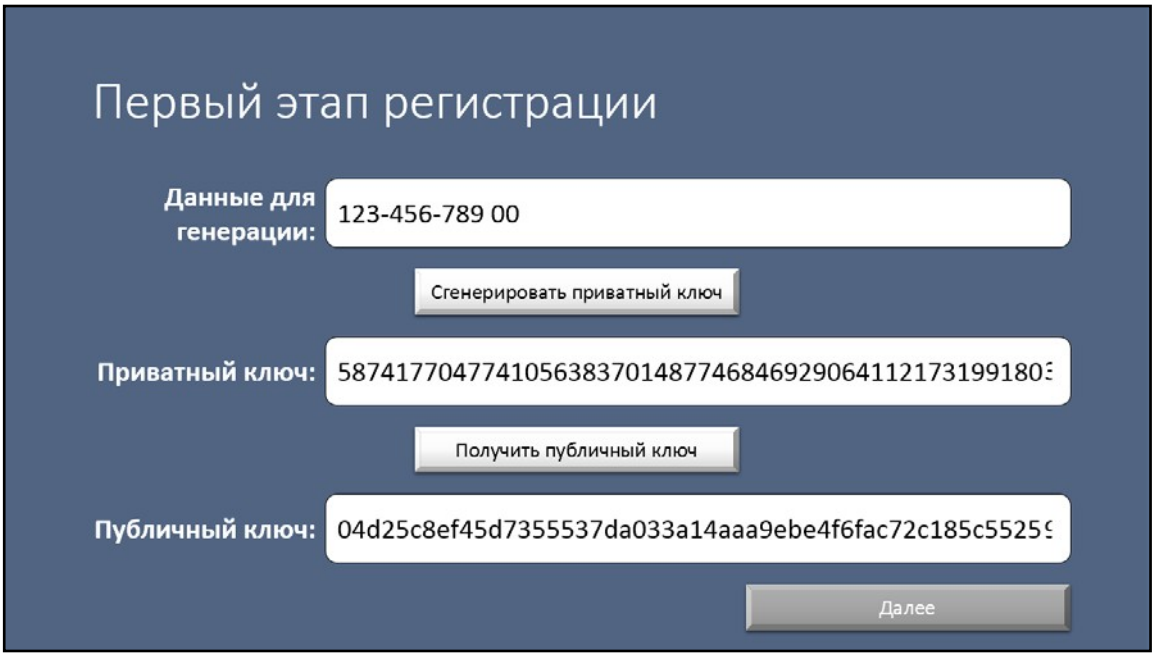


Рисунок 15 — Первый этап регистрации с заполненными данными

На основе него с помощью алгоритма шифрования создаётся публичный ключ, к которому привязывается вся персональная информация (фами-

лия, имя, отчество (ФИО), паспортные данные, фото, роль пользователя в системе и т.д.), а затем подтверждается в образовательной организации. Внесение персональных данных является вторым этапом регистрации (рисунок 16). Информация о персональных данных доступна только образовательной организации и лицу ее предоставившему.

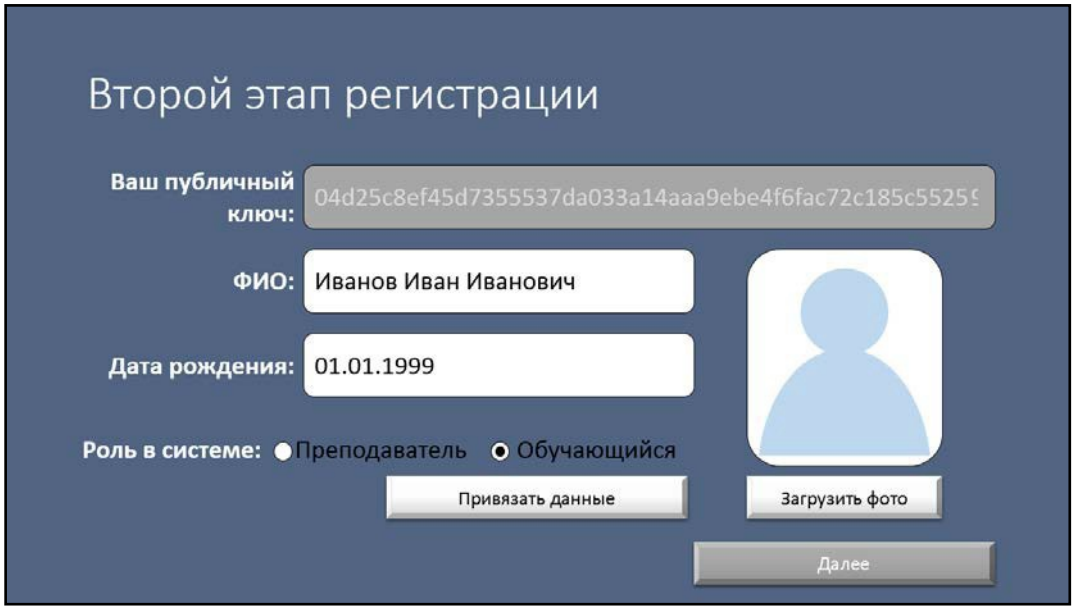


Рисунок 16 — Второй этап регистрации

Публичные ключи открыты и используется преподавателями для просмотра и внесения оценок тому или иному обучающемуся в блок в поле с массивами входных данных (рисунок 17).

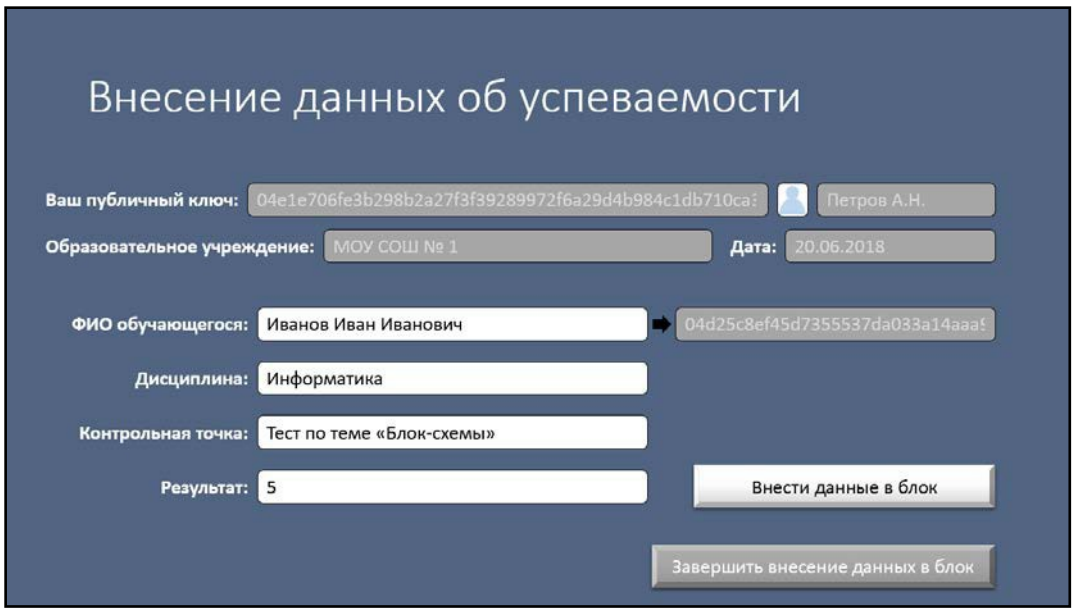


Рисунок 17 — Внесение данных об успеваемости

2.1.2 Схема работы внесения данных об успеваемости в блокчейн

На рисунке 18 представлена схема блока, в котором содержатся следующие элементы: «Номер блока», «Ключ», «Журнал успеваемости», «Предыдущий блок», «Хэш».

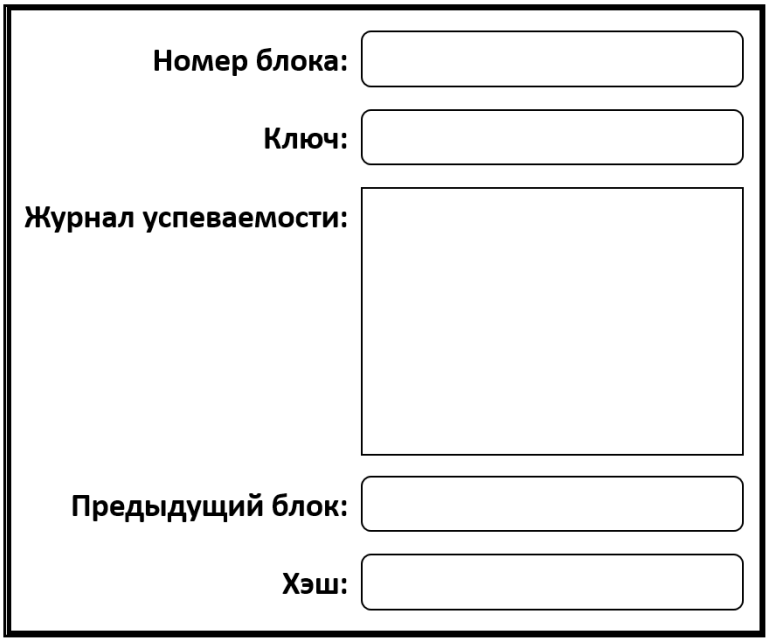


Рисунок 18 — Схема блока

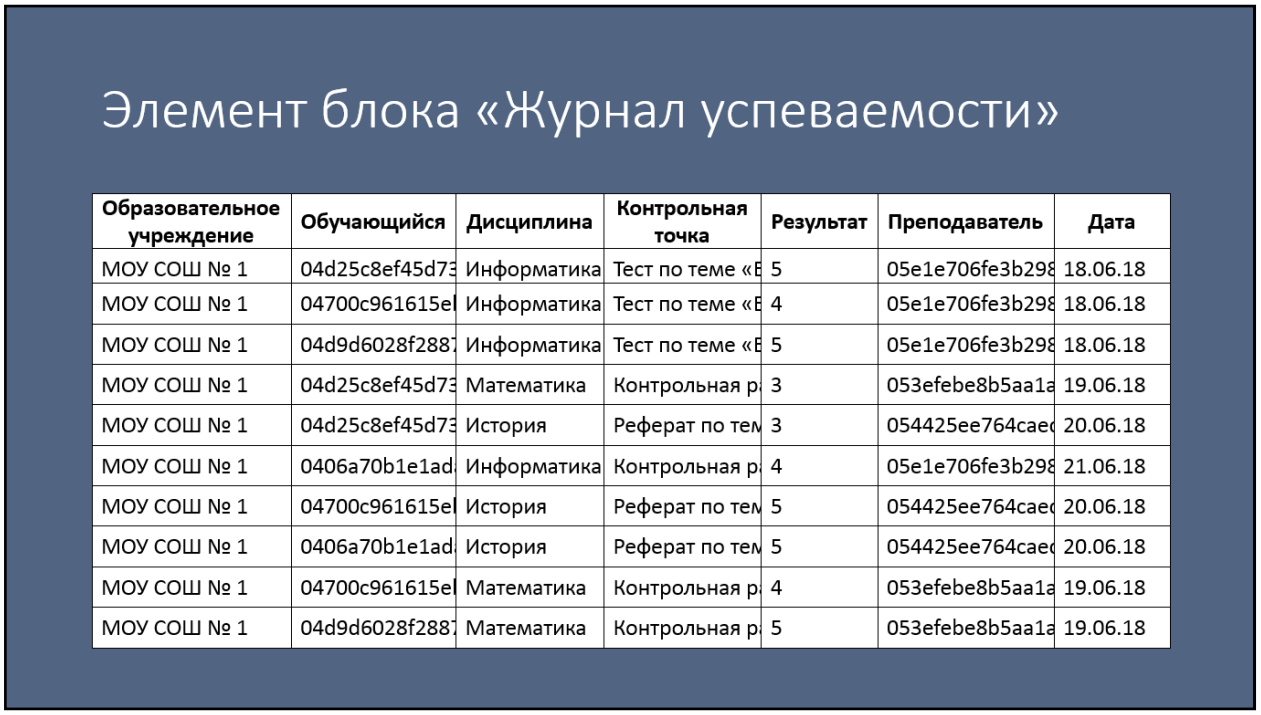
«Номер блока» содержит номер блока в цепочке в его строгой последовательности.

В качестве массива входных данных будет выступать элемент блока «Журнал успеваемости» с данными об успеваемости обучающихся на определенных этапах при прохождении контрольных точек с полями следующего вида: «Образовательное учреждение», «Обучающийся», «Дисциплина», «Контрольная точка», «Результат», «Преподаватель», «Дата» (рисунок 19).

Поля «Обучающийся» и «Преподаватель» будут содержать их публичные идентификаторы, а не имена или личные данные. Это обеспечит приватность персональных данных от просмотра извне.

Поля «Образовательное учреждение», «Дисциплина», «Контрольная точка», «Результат», «Дата» содержат соответствующую их названиям информацию без какого-либо шифрования. Таким образом, каждый участник,

зная свой публичный ключ, может узнать результат своей деятельности на всех пройденных этапах.



Образовательное учреждение	Обучающийся	Дисциплина	Контрольная точка	Результат	Преподаватель	Дата
МОУ СОШ № 1	04d25c8ef45d73	Информатика	Тест по теме «Е	5	05e1e706fe3b298	18.06.18
МОУ СОШ № 1	04700c961615el	Информатика	Тест по теме «Е	4	05e1e706fe3b298	18.06.18
МОУ СОШ № 1	04d9d6028f2887	Информатика	Тест по теме «Е	5	05e1e706fe3b298	18.06.18
МОУ СОШ № 1	04d25c8ef45d73	Математика	Контрольная р	3	053efebe8b5aa1a	19.06.18
МОУ СОШ № 1	04d25c8ef45d73	История	Реферат по тем	3	054425ee764caec	20.06.18
МОУ СОШ № 1	0406a70b1e1ad	Информатика	Контрольная р	4	05e1e706fe3b298	21.06.18
МОУ СОШ № 1	04700c961615el	История	Реферат по тем	5	054425ee764caec	20.06.18
МОУ СОШ № 1	0406a70b1e1ad	История	Реферат по тем	5	054425ee764caec	20.06.18
МОУ СОШ № 1	04700c961615el	Математика	Контрольная р	4	053efebe8b5aa1a	19.06.18
МОУ СОШ № 1	04d9d6028f2887	Математика	Контрольная р	5	053efebe8b5aa1a	19.06.18

Рисунок 19 — Элемент блока «Журнал успеваемости»

Внесенный в блок массив входных данных с помощью значения элемента блока «Ключ» преобразуется в хэш, соответствующий заданному в системе условию.

Элемент блока «Предыдущий блок» содержит хэш того блока, элемент «Номер блока» которого соответствует предыдущему значению от текущего.

Первый блок в цепочке имеет нулевое значение элемента «Предыдущий блок».

На следующем этапе процесса обучения создается новый блок с новыми данными об успеваемости, связываясь с предыдущим в цепочку (рисунок 20).

Таким образом, данные цепочки на протяжении определенного количества времени будут формировать полную картину успеваемости обучаемого, благодаря которой можно будет легко отследить все его сильные и слабые стороны и оперативно скорректировать модель обучения, сделав ее более индивидуально направленной.

Публичными элементами блока являются «Номер блока», «Журнал успеваемости», «Предыдущий блок» и «Хэш», которые могут быть скопированы и проверены на корректность.

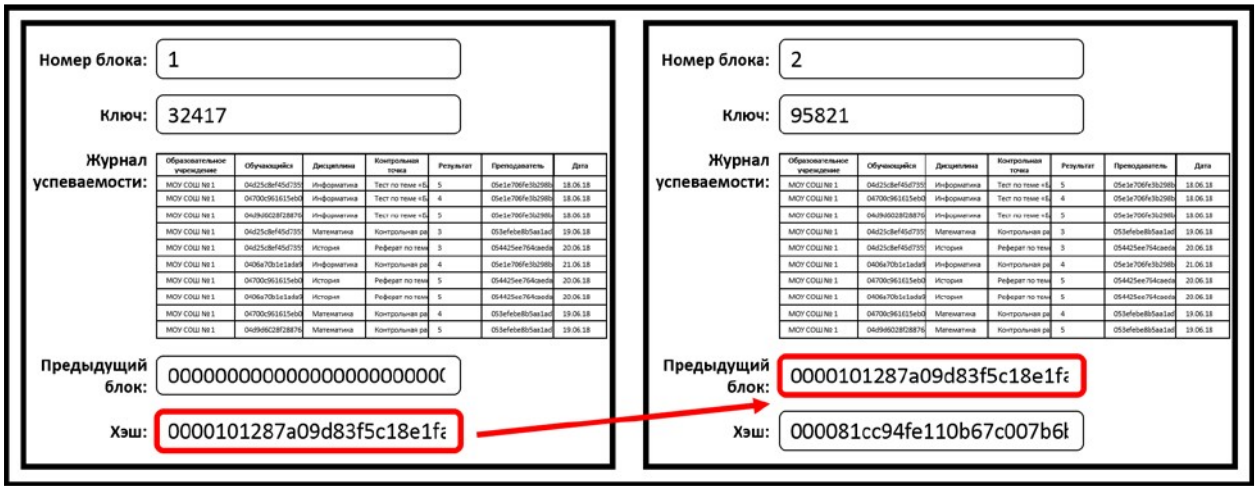


Рисунок 20 — Схема цепочки блоков

Копии цепочек блоков могут храниться на множестве узлов сети, обеспечивая сохранность и неизменность данных обучающихся, а контролирующим деятельность образовательных учреждений органам для проверки как показателей успеваемости, так и корректности внесения данных достаточно будет лишь иметь копию этой цепочки.

2.1.3 Смарт-контракты для выдачи сертификатов и дипломов о завершении обучения

В системе существует возможность технически получить доступ к таким компонентам, как:

- участники договора — это обучающийся, преподаватель, образовательное учреждение;
- предмет договора — между обучающимся и образовательным учреждением — это сертификат или диплом об окончании обучения, между преподавателем и образовательным учреждением — это выплата заработной платы.

А также анализировать, измерять и взаимодействовать с таким компонентом, как условие договора. Между обучающимся и образовательным учреждением — это показатели успеваемости, между преподавателем и образовательным учреждением — это эффективность преподавательской деятельности.

Децентрализованный характер блокчейна позволяет обходиться без третьей стороны и исполнять соглашение, касающееся предмета договора, сразу же как выполнены все необходимые условия.

Благодаря электронно-цифровым подписям, использующимся в блокчейне, каждое действие, выполненное участниками договора, будет подтверждено и сможет затем проверяться.

Таким образом, для работы осуществления смарт-контрактов выполнены условия, описанные в первой главе.

Расширим систему.

Введем регистрацию непосредственно поставщика образовательных услуг и участника договора — образовательного учреждения, к которому можно привязать все реквизиты учреждения (индекс, индивидуальный номер налогоплательщика (ИНН), код причины постановки на учёт (КПП) и т.д.), контактную информацию, адрес и реализуемые в нём образовательные программы (рисунок 21).

В предыдущей главе говорилось об том, что в элементе блока «Журнал успеваемости» будут хранится все контрольные точки, которые проходит обучающийся.

Так вот, образовательная программа и будет представлять собой этапы, которые необходимо пройти обучающемуся и будет включать в себя все необходимые компоненты: содержание, цели, задачи, этапы, учебный план и оценивающие средства.

Для преподавателя же нужно внести возможность брать нагрузку, в то время как образовательное учреждение должно её формировать.

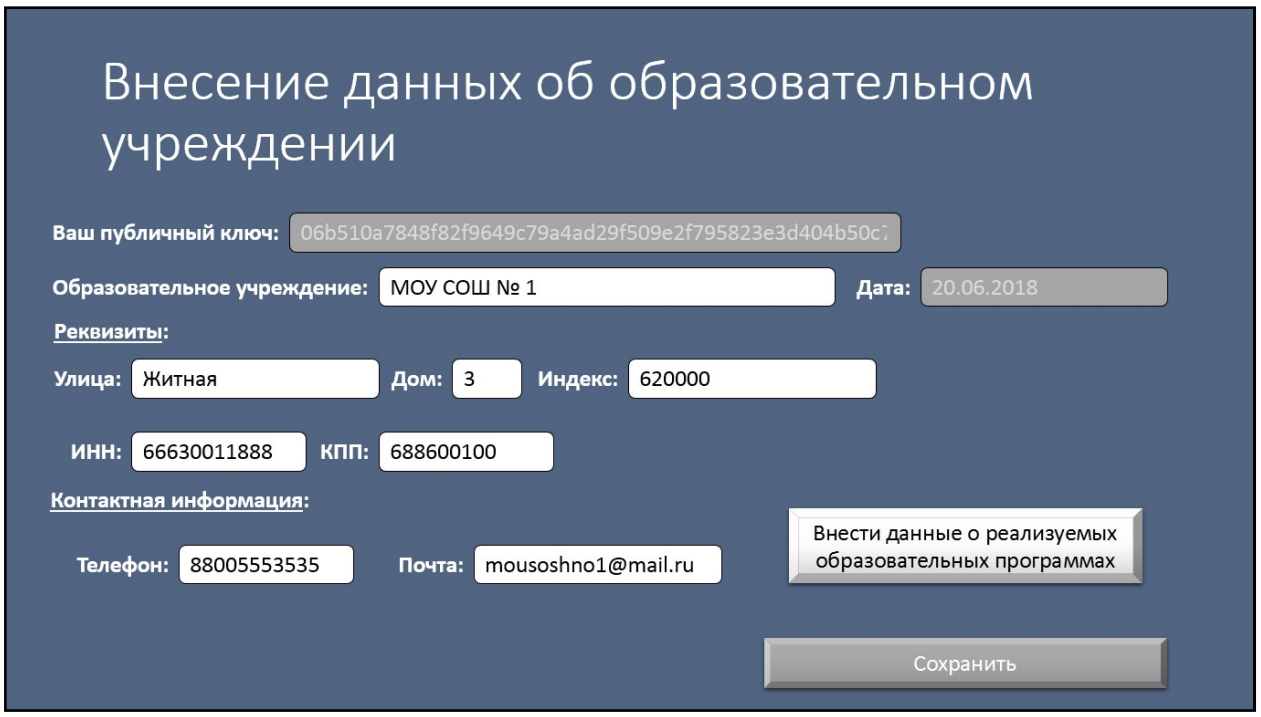


Рисунок 21 — Внесение данных об образовательном учреждении

В итоге, смарт-контракт будет исполняться для обучающегося при успешном прохождении контрольных точек, заложенных в образовательных программах и описанных разработчиками в коде, в результате которых будет выдаваться диплом или сертификат с электронно-цифровой подписью об успешном завершении обучения по определенной образовательной программе.

А для преподавателя смарт-контракт будет работать при выполнении нагрузки, за выполнение которой он будет получать заработную плату.

Благодаря тому, что система будет являться открытой и в то же время выступать гарантом выполнения условий договора, сторонние лица смогут узнать, какие образовательные программы реализуются в образовательном учреждении, и насколько они эффективно реализуются. Работодатели могут через форму для связи связаться с теми выпускниками, успеваемость которых будет удовлетворять их запросам. Образовательные учреждения могут делиться образовательными программами между собой и своими филиалами.

В общем виде схема связей в системе представлена на рисунке 22.

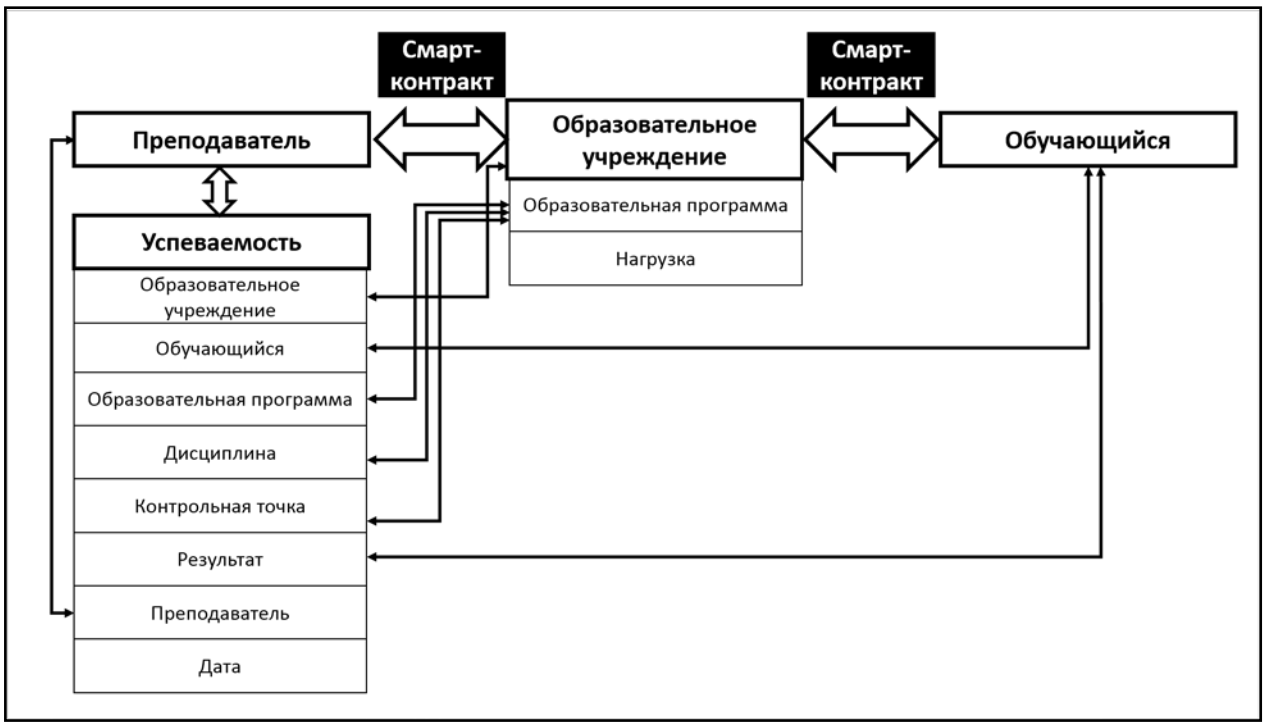


Рисунок 22 — Схема связей модели для смарт-контрактов

2.1.4 Initial coin offering и токены для финансирования системы

Для того чтобы система работала стабильно, важно, чтобы она была финансово устойчивой.

Новый способ привлечения инвестиций позволяет привлечь не только средства, но и большее количество заинтересованных лиц, которые могут способствовать развитию организации.

В системе может быть создана собственная криптовалюта организации, они же токены.

С помощью них, благодаря наличию связей в системе (рисунок 23), возможно производить следующие операции:

- оплата обучения со стороны обучающихся;
- выплата заработной платы преподавателям со стороны образовательного учреждения;
- выплата стипендий обучающимся со стороны образовательного учреждения;
- другие виды выплат внутри организации;

- покупка токенов образовательного учреждения с целью его инвестирования.

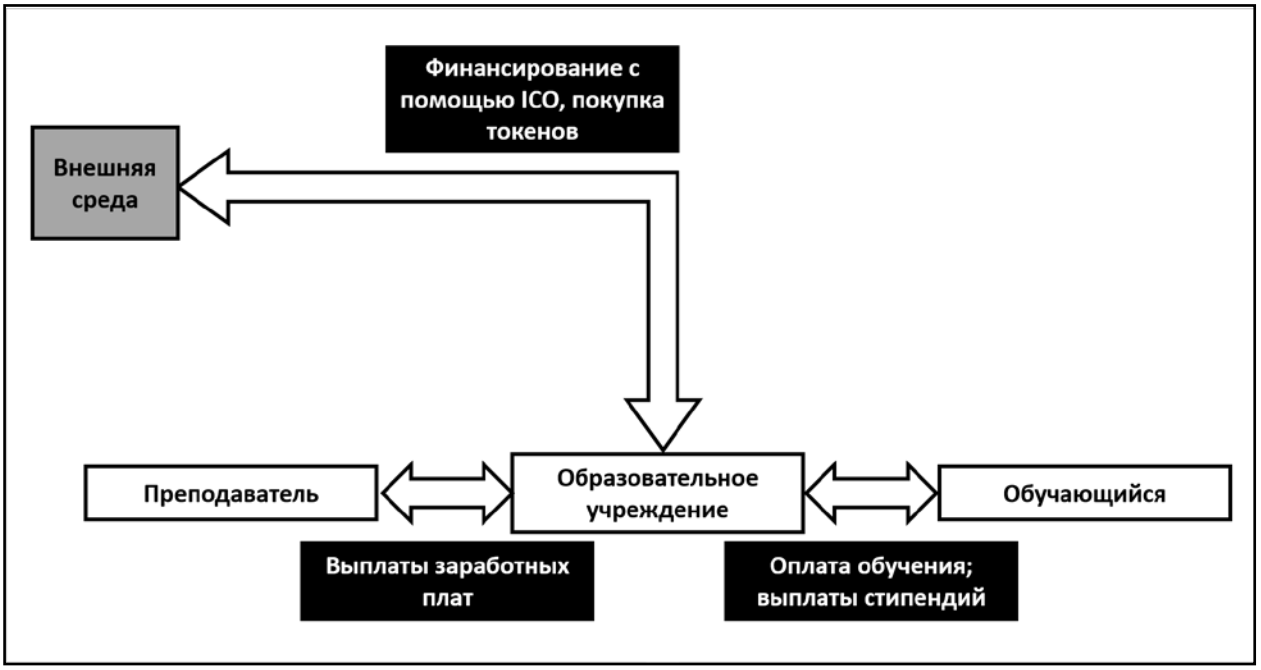


Рисунок 23 — Схема путей хождения финансов в системе

Таким образом, в системе будет собственные активы, зависящие от показателей их собственной деятельности, делая систему самодостаточной

Образовательные учреждения заинтересовано в том, чтобы вести образовательную деятельность эффективно, поскольку от этого будет зависеть спрос, напрямую выраженный в цене на их токены.

2.2 Модель реализации сценария использования технологии блокчейн как формы организации размещения научных исследований

Система является распределенной, а ее участники — равноправными. Однако выделить ключевые роли всё-таки можно. Ими являются [32]:

- *майнеры* — участники, чья роль заключается в проверке хэшей транзакций и последующем внесении их в блокчейн, за что они получают «зарплату» в виде комиссии с транзакций, а также «добыче» новой криптовалюты, которая достается тем, у кого после проверки хэшей транзакций и по-

следующем внесении блока в блокчейн создается новая цепочка блоков (размер выдаваемой криптовалюты лимитирован);

- разработчики — сообщества тех, кто занимаются доработкой, изменением, исправлением и «залатанием дыр» в системе, если таковые появляются, для обеспечения правильного и продуктивного функционирования, а также безопасности;
- биржи, обменники, владельцы популярных кошельков — это те организации, лица и ресурсы, которые позволяют приобрести криптовалюту в обмен на *фиатные деньги* либо другую криптовалюту;
- рядовые пользователи — клиенты системы, желающие приобрести криптовалюту, обменять ее или перевести свои средства другому пользователю. Как уже было сказано выше, участники системы равноправны, поэтому любой пользователь может исполнять любую из ролей.

На этих основных ролях, а также особенностях блокчейна [12], [21] можно попытаться построить систему образования и науки или некоторые процессы, происходящие в ней.

Примерная схема работы системы на основе блокчейн и ее участники представлены на рисунке 24.

В качестве блоков будут выступать исследования участников, которые выстраиваются также в цепочки на основе принадлежности к определенной теме с возможностью указать ссылки на другие блоки из других цепочек (тем).

Для подключения к системе нужно создать свой идентификатор исследователя, который будет присваиваться исследованиям при их размещении.

Каждому блоку также будет присваиваться уникальная цифровая сигнатура (подпись) для того, чтобы уже внесенные данные нельзя было изменить, что обеспечивает безопасность. Сигнатура будет проверяться математически всеми участниками (по аналогии с майнерами).

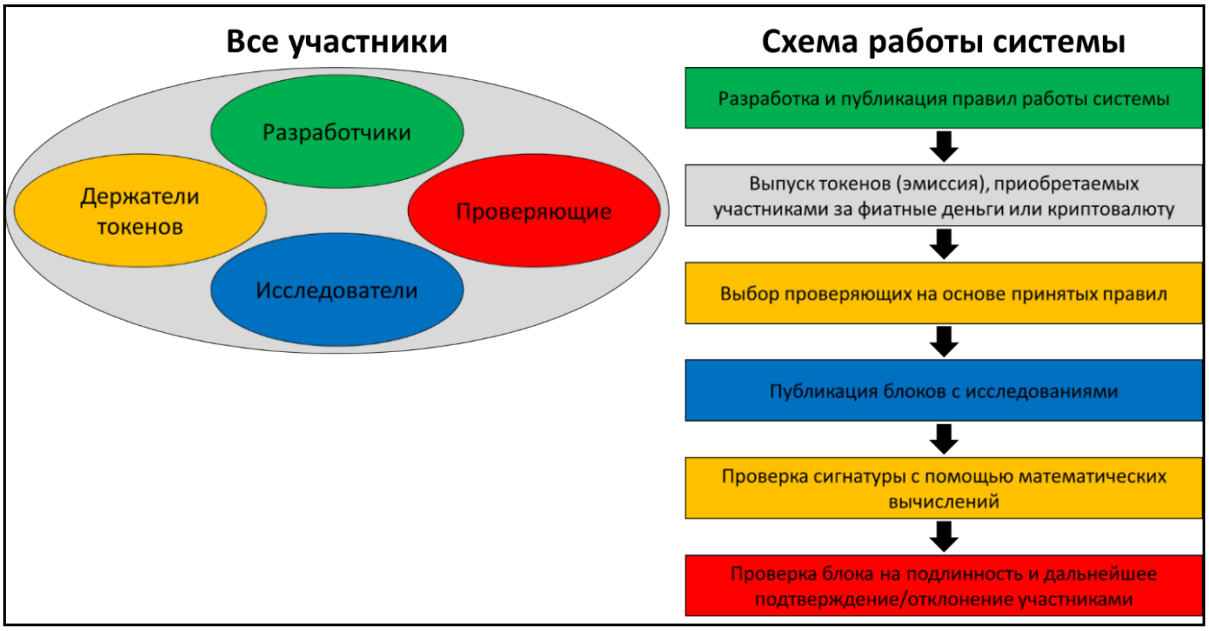


Рисунок 24 — Схема работы модели использования технологии блокчейн как цепочки блоков с исследованиями

Поскольку уникальная цифровая подпись не привязана к личным данным, это будет обеспечивать анонимность. Однако, как и в случае с криптовалютами, никто не мешает раскрыть свою личность, указав идентификатор исследователя как принадлежащий какому-либо лицу. Таким образом, над теми или иными исследованиями также смогут работать, объединяясь в группы (группы исследователей, образовательные организации и др.). Более того, в таком случае будет возможность работать на своё имя или на имя организации.

Участники системы будут проверять исследования на подлинность путём указания тех блоков или даже целых цепочек блоков, уже проверенных ранее, где информация опровергается или подтверждается. Затем остальные проверяющие участники на основе этой проверки подтверждают или отклоняют внесение блока в блокчейн.

За проверку блока участники будут получать вознаграждения в виде *токенов*, которые позволят получить доступ к блоку на его проверку, на возможность публикации исследования и которые будут иметь реальную цену, что обеспечит финансовую устойчивость системы.

Обменять или приобрести токены возможно будет на уже существующих биржах и обменниках (при условии, что система обретет популярность и биржи с обменниками начнут работать с ними).

Проверка блоков на подлинность будет доступна только определенным участникам, чтобы не допустить массового подтверждения недостоверных исследований некомпетентными пользователями. В качестве критериев выбора проверяющих могут быть: количество выпущенных исследований, объем проверенных блоков и др.

Для ограничения публикаций блоков может быть применена система рейтинга, при которой участник с определенным идентификатором, чьи исследования регулярно не подтверждаются должен будет заплатить с каждым разом всё больше токенов, чтобы иметь возможность внести свои исследования на проверку. Это снизит нагрузку на систему.

Итак, стоит подвести некоторый итог, чтобы определить преимущества и недостатки системы.

Исследователи будут заинтересованы в том, чтобы публиковать достоверные исследования, чтобы не платить большую комиссию за возможность внесения своего исследования в блокчейн и получать большую выгоду за успешно внесенные исследования.

Держатели токенов будут иметь ценный продукт, а также возможность его «добывать» (майнить) путём проверки сигнатур и подтверждения или отклонения проверки.

Первые правильно проверившие блок будут получать наибольшую выгоду, что обеспечит скорость работы и актуальность данных.

Разработчики, являющиеся участниками, будут заинтересованы в том, чтобы система функционировала правильно и была безопасной, чтобы их токены были в сохранности.

Исходя из вышеперечисленного можно сказать, что система отвечает требованиям саморегулируемости.

Каждый участник при желании и упорстве может исполнять любую из ролей, а значит можно говорить о равноправии участников.

Так как блокчейн будет содержать огромную базу только самых актуальных исследований, он будет привлекать всё новых участников на покупку токенов для возможности получить доступ к такой «кладези знаний».

Теперь для поиска нужной информации не нужно будет перебирать тонны информации, а всего лишь подключиться к системе. Всё это обеспечит доступность, прозрачность и свободу в научном совершенствовании.

Также в результате функционирования может отпасть надобность в патентах, ведь каждый блок будет защищен сигнатурой и иметь уникальный идентификатор, а также значительно снизится бюрократическая составляющая.

Возможно, система выглядит несколько утопично, поскольку участники могут оказаться незаинтересованными в проверке блоков, либо исследователи не захотят платить за возможность внесения своих исследований, или же проверка сигнатур не окажется финансово привлекательной, тем не менее, преимущества и потенциал технологии, а также возможность получить выгоду могут выступить стимулом для развития.

Также нужно понимать, что не каждое исследования имеет право становиться достоянием общественности, поскольку оно может нанести вред человеку или окружающей среде, поэтому должен существовать некоторый фильтр на соответствие законодательству и, возможно, каким-то моральным нормам, что уже относится к вопросам этики.

2.3 Апробация

Проведено два мастер-класса на тему «Подходы к применению технологии блокчейн в образовании и науке». В мастер-классах приняли участие 14 человек из области образования. Мастер-классы проходили по следующему плану:

1. Оглашение темы мастер-класса.
2. Формулировка проблем.
3. Постановка цели мастер-класса.

4. Постановка задач мастер-класса.
5. Презентация модели.
6. Обсуждение модели.
7. Подведение итогов мастер-класса.

В качестве проблем были озвучены:

1. На первом мастер-классе:
   - сложность доступа к старым академическим данным;
   - утеря или искажение старых академических данных.
2. На втором мастер-классе:
   - сложность поиска достоверной информации в Интернете;
   - сложность поиска всей цепочки развития того или иного феномена;
   - несовершенство процедуры патентования.

Целью мастер-классов было оценить, насколько возможно применение технологии блокчейн в образовании и науке.

Исходя из этого были сформулированы следующие задачи мастер-классов:

1. Разобрать устройство работы блокчейна.
2. Продемонстрировать реализованные модели, раскрыть особенности их работы.
3. Оценить уровень проработанности реализованных моделей путём выяснения их преимуществ и недостатков, а также недостающих компонентов.
4. Оценить уровень заинтересованности в технологии блокчейн среди участников мастер-класса.

Тема для участников мастер-классов оказалась новой, однако вызвала интерес, особенно сценарий использования технологии блокчейн для отслеживания успеваемости обучающегося. Состоялось обсуждение, на котором было задано много вопросов.

Для сокращения комментарии участников мастер-класса обозначаются буквой «У.», а ответы буквой «О.».

Результаты обсуждения первой модели

У.: «Зачем мне знать свою успеваемость на столь ранних этапах?».

О.: «Как преподаватель Вы можете узнать сильные и слабые стороны своего ученика. А как обучающийся Вы можете осуществлять самоконтроль».

У.: «Но ведь это потребует слишком много времени, это не рационально».

О.: «Это лишь концепция. Мы можем дать материал на самообучение. Главное, что мы узнали корень проблемы».

У.: «Вы сказали, что первый, кто подбирает удовлетворяющий условию хэш блока, получает вознаграждение. Откуда оно берётся?».

О.: «На основе заложенного алгоритма токены регулярно выпускаются в фиксированном количестве при достижении определенного количества блоков в цепи, чтобы в системе возможно было осуществлять оборот средств».

У.: «Я могу их вывести в реальные деньги?».

О.: «Технически да. Через биржу, которая будет работать с Вашими токенами или с помощью договоренности».

У.: «Почему я не могу просто использовать обычные базы данных?».

О.: «В блокчейне сложность изменения блока увеличивается в зависимости от его возраста. Это обеспечивает более высокий уровень сохранности и неизменности данных с учётом их открытости».

У.: «Хорошо. Но есть же шифрование и другие способы защиты информации».

О.: «Базы данных имеют всё-таки какой-то центр. Или хотя бы сеть центров. А значит на них может быть произведена хакерская атака».

У.: «Как быть с данными об успеваемости, которые нельзя записать оценкой или зачётом? Например, нужно сохранить реферат».

О.: «Модель схематична и может быть дополнена другими блоками. Поскольку на выходе всё равно получается однотипный хэш-код, мы может добавить загрузку других данных».

У.: «Устройство образовательного учреждения гораздо сложнее».

О.: «Безусловно. Это лишь модель, которая может быть расширена и обрастать новым и новыми компонентами по мере их необходимости. В данном случае, рассматривался один из возможных подходов через учёт успеваемости».

Результаты обсуждения второй модели

У.: «Что будет, если участники выберут недобросовестных лиц для проверки блоков?».

О.: «Поскольку выбор производят держатели токенов, необходимо сначала, так скажем, заплатить за возможность производить выбор. Это первое. А второе, это возможность ввести систему рейтинга по, например, количеству выпущенных исследований или объему проверенных блоков».

У.: «Каким образом происходит проверка блока и зачем это нужно?».

О.: «В блоке находится исследование. Чтобы не происходила публикация недостоверных или повторных исследований происходит их проверка участниками. За проверку они получают вознаграждение».

У.: «А что будет если это окажется им ненужным?».

О.: «Это возможно. Любой проект имеет риски быть проваленным. Для мотивации к проверке и создано вознаграждение».

У.: «Как быть в тех ситуациях, когда один феномен трактуется разными учеными по-разному? Это ведь последовательная цепочка блоков».

О.: «Да, всё верно. Для данной ситуации существует два решения: древовидная структура цепочек блоков или же их строгое последовательное размещение также, как и классическом блокчейне, но с полем, имеющим один хэш-код или набор хэш-кодов с исследованиями, сделанными до него».

У.: «В такой модели есть вероятность, что при ее значительном разрастании могут возникнуть зацикливания, когда одно исследование ссылается на

другое, которое, в свою очередь, через несколько итераций снова ссылается на первое».

О.: «Верно замеченная уязвимость. Тогда, пожалуй, следует сделать жёсткую последовательность таки блоков».

Подведя итог проведенным мастер-классам, можно сказать, что блокчейн вызвал интерес со стороны деятелей образования, однако в то же время вызывал всё-таки некоторое непонимание.

Что касается оценки возможности его применения, то в ходе мастер-классов не было выявлено критических моментов, которые бы поставили крест на его дальнейшей судьбе в образовании или науке.

Результаты исследования отражены в восьми публикациях в сборниках научных трудов и рассмотрены на восьми конференциях.

Выводы по второй главе

Во второй главе были описаны теоретические модели реализации двух сценариев применения технологии блокчейн: в образовании и науке.

Сценарий применения технологии блокчейн в образовании представляет собой подход к данной сфере через ведение журнала об успеваемости, благодаря которому предполагается отслеживать все академические резуль- таты обучающегося на всех этапах его обучения, создавая таким образом полную картину его деятельности.

Это позволит обнаружить сильные или слабые стороны обучающегося, откатиться на тот момент, когда началось непонимание, даже если это было очень давно, и благодаря этому скорректировать модель обучения и восполнить пробел в знаниях обучающегося.

Преимущества блокчейна позволяют держать такие записи в сохранности от изменения и несанкционированного доступа.

Расширенные и дополненные модели помимо успеваемости позволяют:

- осуществлять автоматическую выдачу электронных сертификатов и дипломов при выполнении необходимого условия по показателям успеваемости с помощью смарт-контрактов;
- благодаря наличию связей в системе, получать финансирование извне с помощью Initial coin offering и обмениваться средствами внутри, например собственными токенами.

В науке с помощью блокчейна предлагается структурировать научные исследования путём их размещения в блокчейне, в котором будет производиться их проверка на действительность путём указания тех блоков или даже целых цепочек блоков, уже проверенных ранее, где информация опровергается или подтверждается. Затем остальные проверяющие участники на основе этой проверки подтверждают или отклоняют внесение блока в блокчейн.

За проверку блока участники будут получать вознаграждения в виде токенов.

В результате функционирования модели может отпасть надобность в патентах, ведь каждый блок будет защищен сигнатурой и иметь уникальный идентификатор.

Также упрощен будет поиск информации, которая будет аккумулироваться и структурироваться в одном месте.

Для оценивания возможности применения технологии блокчейн в образовании и науки было проведено два мастер-класса.

На мастер-классах были продемонстрированы модели, описанные в рамках данного исследования.

Участники мастер-классов проявили умеренный интерес к технологии, наблюдалась сложность в понимании.

Что касается оценки возможности его применения, то в ходе мастер-классов не было выявлено критических моментов, которые бы поставили крест на его дальнейшей судьбе в образовании или науке.

ЗАКЛЮЧЕНИЕ

В ходе исследования были описаны две модели сценариев применения технологии блокчейн в образовании науке. Каждая из них представляет собой попытку теоретически описать подходы к применению технологии блокчейн в образовании и науке. Данные подходы были выведены на основе проведенного теоретического анализа, в ходе которого были: разобраны и описаны история, правовой статус и устройство работы самой технологии блокчейн, а также принципов работы технологий смарт-контрактов, Initial coin offering и токенов, использующих блокчейн в основе своей работы; проанализированы примеры применения технологии блокчейн в различных сферах деятельности; рассмотрены идеи, подходы и перспективные направления различных деятелей в области применения технологии блокчейн в образовании и науке; проанализированы источники по теме проблем и уязвимостей в российском образовании и науке с целью поиска подходов и направлений, в которых блокчейн мог бы быть применим, благодаря своим особенностям и преимуществам, выведенным в работе. Для определения того, насколько возможны такие применения блокчейна в образовании и науке были проведены два мастер-класса. Они показали возможность такого рода внедрений, тем самым подтвердив **гипотезу исследования**.

Для решения поставленной цели исследования и подтверждения гипотезы были решены следующие **задачи**:

1. Проведён анализ источников по теме устройства работы технологии блокчейн, ее правового положения и принципов работы технологий, связанных с ней.

2. Проведён анализ источников в области применения технологии блокчейн в различных сферах деятельности с целью ее применения в образовании и науке.

3. Выделены основные направления применения технологии блокчейн в образовании и науке.

4. Описаны подходы к применению технологии блокчейн в образовании и науке.

Таким образом, задачи выпускной квалификационной работы были решены, цель исследования достигнута, гипотеза получила подтверждение.

Для развития идеи и расширения исследуемой области предлагаются следующие направления дальнейших разработок:

- разработка технической модели реализации сценария использования технологии блокчейна в образовании или науке на основе теоретических моделях, разработанных в данном исследовании;
- подробное рассмотрение аспектов решения конкретной проблемы образования или науки с помощью технологии блокчейн;
- рассмотрение другого подхода к применению технологии блокчейн в образовании или науке с большей степенью проработанности и готовности к внедрению;
- рассмотрение подходов к применению технологии блокчейн в других сферах.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Аюпова А. Р. Некоторые проблемы российского патентного права [Текст] / А. Р. Аюпова, Н. Г. Хабиров // Международный научно-исследовательский журнал. — 2016. — № 11 (53). — Ч. 1. — С. 81–83.

2. Бахур В. Стоимость Microsoft превысила $600 млрд впервые за 17 лет [Электронный ресурс] / CNews — крупнейшее издание в сфере высоких технологий в России и странах СНГ. — Режим доступа: http://www.cnews.ru /news/top/2017-10-20_kapitalizatsiya_microsoft_vpervye_vernulas_k_urovnyu (дата обращения: 17.12.2017).

3. Биткойн [Электронный ресурс] / Википедия — свободная энциклопедия. — Режим доступа: https://ru.wikipedia.org/wiki/Биткойн (дата обращения: 06.06.2017).

4. Блокчейн [Электронный ресурс] / Википедия — свободная энциклопедия. — Режим доступа: https://ru.wikipedia.org/wiki/Блокчейн (дата обращения: 06.06.2017).

5. Блокчейн и IoT: перспективы взаимодействия и проблемы на пути развития [Электронный ресурс] / ForkLog — сайт про Биткойн, блокчейн, криптовалюты и финтех. — Режим доступа: https://forklog.com/blokchejn-i-iot-perspektivy-vzaimodejstviya-i-problemy-na-puti-razvitiya/ (дата обращения: 04.06.2018).

6. Блокчейн меняет музыкальную индустрию [Электронный ресурс] / ForkLog — сайт про Биткойн, блокчейн, криптовалюты и финтех. — Режим доступа: https://forklog.com/blokchejn-menyaet-muzykalnuyu-industriyu/ (дата обращения: 04.06.2018).

7. Бюрократы против преподавателей [Электронный ресурс] / Образовательный портал Newtonew. — Режим доступа: https://newtonew.com /higher/the-educational-system (дата обращения: 01.06.2018).

8. Генкин А. С. Блокчейн: Как это работает и что ждет нас завтра [Текст] / А. С. Генкин, А. А. Михеев. — Москва: Альпина Паблишер, 2018. — 592 с.

9. Интернет вещей [Электронный ресурс] / Википедия — свободная энциклопедия. — Режим доступа: https://ru.wikipedia.org/wiki /Интернет_вещей (дата обращения: 04.06.2018).

10. Исаев М. Д. Проблемы образования в государственных федеральных учреждениях высшего образования [Текст] / М. Д. Исаев // Молодой ученый. — 2017. — №2. — С. 676–678.

11. Как написать whitepaper для ICO: 12 ключевых блоков (с примерами) [Электронный ресурс] / Shard-Copywriting — копирайтинг и интернет-маркетинг в советах от Даниила Шардакова. — Режим доступа: https://shard-copywriting.ru/kak-napisat-whitepaper-ico/ (дата обращения: 13.06.2018).

12. Как устроен блокчейн и зачем он нужен [Электронный ресурс] / Афиша — медийно-сервисная платформа Rambler & Co. — Режим доступа: https://daily.afisha.ru/technology/6058-kak-ustroen-blokcheyn-i-zachem-on-nuzhen/ (дата обращения: 18.12.2017).

13. Криптовалюта [Электронный ресурс] / Википедия — свободная энциклопедия. — Режим доступа: https://ru.wikipedia.org/wiki/Криптовалюта (дата обращения: 06.06.2017).

14. Криптофонд Алекса Тапскотта отказался от выхода на IPO после выявленных ложных данных в описании проекта [Электронный ресурс] / ForkLog — сайт про Биткойн, блокчейн, криптовалюты и финтех. — Режим доступа: https://forklog.com/kriptofond-aleksa-tapskotta-otkazalsya-ot-vyhoda-na-birzhu-posle-vyyavlennyh-lozhnyh-dannyh-v-opisanii-proekta/ (дата обращения: 21.05.2018).

15. Кублин И. М. Проблемы и перспективы применения технологии блокчейн в продвижении продукции на рынок [Текст] / И. М. Кублин, Р. В. Михайлов, С. А. Санинский // Экономическая безопасность и качество. — 2018. — № 1. — С. 31–36.

16. Майнинг [Электронный ресурс] / Википедия — свободная энциклопедия. — Режим доступа: https://ru.wikipedia.org/wiki/Майнинг (дата обращения: 06.06.2017).

17. Недвижимость и блокчейн: почему технология перевернет рынок [Электронный ресурс] / Forbes — американский финансово-экономический журнал. — Режим доступа: http://www.forbes.ru/biznes/347775-nedvizhimost-i-blokcheyn-pochemu-tehnologiya-perevernet-rynok (дата обращения: 27.05.2018).

18. Об утверждении программы «Цифровая экономика Российской Федерации» [Текст]: распоряжение Правительства Российской Федерации от 28 июля 2017 года № 1632-р. — Москва: Минкомсвязь, 2017. — 88 с.

19. Об электронной подписи [Текст]: Федеральный закон Российской Федерации от 06.04.2011 N 63-ФЗ. — Москва: Кремль, 2011. — 14 с.

20. Осмоловская А. С. Смарт-контракты: функции и применение [Текст] / А. С. Осмоловская // Бизнес-образование в экономике знаний. — 2018. — №2. — С. 54–56.

21. Поляков Н. Е. Внедрение технологии блокчейн в образование: зарубежный опыт [Текст] / Н. Е. Поляков, А. В. Солодов // Управление социально-экономическими системами: теория, методология, практика: сборник статей III Международной научно-практической конференции. — Пенза: МЦНС «Наука и Просвещение», 2017. — Ч. 2. — С. 100–104.

22. Правовой режим криптовалют [Электронный ресурс] / Википедия — свободная энциклопедия. — Режим доступа: https://ru.wikipedia.org /wiki/Правовой_режим_криптовалют (дата обращения: 16.12.2017).

23. Проблемы современной российской системы образования [Электронный ресурс] / Epoch times — международный новостной медиапроект. — Режим доступа: https://www.epochtimes.ru/problemy-sovremennoj-rossijskoj-sistemy-obrazovaniya-98913405/ (дата обращения: 16.12.2017).

24. Пряников М. М. Блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы [Текст] / М. М. Пряников, А. В. Чугунов // International Journal of Open Information Technologies. — 2017. — Т. 5. — № 6. — С. 49–55.

25. Рейтинг стран мира по уровню образования [Электронный ресурс] / Гуманитарные технологии — интернет-издание информационно-аналитического агентства «Центр гуманитарных технологий». — Режим доступа: http://gtmarket.ru/ratings/education-index/education-index-info (дата обращения: 16.06.2018).

26. Сатоси Накамото [Электронный ресурс] / Википедия — свободная энциклопедия. — Режим доступа: https://ru.wikipedia.org/wiki /Сатоси_ Накамото (дата обращения: 16.12.2017).

27. Сбербанк и ФАС России запустили пилотный проект по обмену документами на основе Blockchain [Электронный ресурс] / Сбербанк — крупнейший транснациональный и универсальный банк России, Центральной и Восточной Европы. — Режим доступа: https://www.sberbank.ru/ru/press_center/all/article?newsID=cb85f87f-8dc4-46df-8fdf-eab909d0277c& blockID=1303& regionID=&lang=ru (дата обращения: 16.05.2018).

28. Свон М. Блокчейн: схема новой экономики [Текст] / М. Свон. — Москва: Олимп-Бизнес, 2017. — 230 с.

29. Смарт-контракт [Электронный ресурс] / Википедия — свободная энциклопедия. — Режим доступа: https://ru.wikipedia.org/wiki/Смарт-контракт (дата обращения: 04.06.2018).

30. Солодов А. В. Визуализация в дистанционном обучении [Текст] / А. В. Солодов, А. А. Царегородцев, Е. В. Чубаркова // Инновации в профессиональном и профессионально-педагогическом образовании: материалы 22-й Международной научно-практической конференции. — Екатеринбург: ФГАОУ ВО РГППУ, 2017. — С. 265–267.

31. Солодов А. В. Визуализация в дистанционном обучении [Текст] / А. В. Солодов, Е. В. Чубаркова // Новые информационные технологии в образовании и науке: материалы X Международной научно-практической конференции. — Екатеринбург: ФГАОУ ВО РГППУ, 2017. — С. 223–226.

32. Солодов А. В. Внедрение технологии блокчейн в образование: зарубежный опыт [Текст] / А. В. Солодов // Инновационные научные исследования: теория, методология, практика: теория, методология, практика: сбор-

ник статей XII Международной научно-практической конференции. — Пенза: МЦНС «Наука и Просвещение», 2018. — Ч. 1. — С. 215–218.

33. Солодов А. В. Массовые открытые онлайн-курсы – альтернатива традиционному образованию [Текст] / А. В. Солодов // Актуальные проблемы развития вертикальной интеграции системы образования, науки и бизнеса: экономические, правовые и социальные аспекты: материалы V Международной научно-практической конференции. — Воронеж: АНОО ВО ВЭПИ, 2016. — Т. 3. — С. 218–221.

34. Солодов А. В. Массовые открытые онлайн-курсы — особенности и перспективы [Текст] / А. В. Солодов, А. О. Прокубовская, Е. В. Чубаркова // Наука. Информатизация. Технологии. Образование: материалы XI Международной научно-практической конференции. — Екатеринбург: ФГАОУ ВО РГППУ, 2018. — С. 434–440.

35. Солодов А. В. Современные проблемы образовательной системы Свердловской области [Текст] / А. В. Солодов // Фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации: сборник статей V Международной научно-практической конференции. — Пенза: МЦНС «Наука и Просвещение», 2017. — Ч. 1. — С. 196–198.

36. Солодов А. В. Codecademy как средство обучения программированию [Текст] / А. В. Солодов // Фундаментальные и прикладные исследования: от теории к практике: материалы Международной научно-практической конференции, приуроченной ко Дню российской науки. — Воронеж; Кызыл-Кия: АНОО ВО ВЭПИ, 2017. — Т. 1. — С. 225–228.

37. Сорокина Н. В. Система образования в Волгоградской области: современное состояние и тенденции развития [Текст] / Н. В. Сорокина, Л. А. Григорьева // Научный вестник Южного института менеджмента. — 2016. — № 4. — С. 56–59.

38. Старик И. Н. Доступность образования для людей с ограниченными возможностями здоровья [Текст] / И. Н. Старик // Теория и практика общественного развития. — 2011. — №2. — С. 80–84.

39. Тапскотт Д. Технология блокчейн: то, что движет финансовой революцией сегодня [Текст] / Д. Тапскотт, А. Тапскотт; пер. К. Шашковой, Е. Ряхиной. — Москва: Эксмо, 2017. — 448 с.

40. Тапскотт, Дон [Электронный ресурс] / Википедия — свободная энциклопедия. — Режим доступа: https://ru.wikipedia.org/wiki/Тапскотт_Дон (дата обращения: 21.12.2017).

41. Токен (криптовалюта) [Электронный ресурс] / Википедия — свободная энциклопедия. — Режим доступа: https://ru.wikipedia.org /wiki/Токен_(криптовалюта) (дата обращения: 04.06.2018).

42. Хеширование [Электронный ресурс] / Википедия — свободная энциклопедия. — Режим доступа: https://ru.wikipedia.org/wiki/Хеширование (дата обращения: 20.12.2017).

43. Цветкова Л. А. Перспективы развития технологии блокчейн в России: конкурентные преимущества и барьеры [Текст] / Л. А. Цветкова // Экономика науки. — 2017. — Т. 3. — № 4. — С. 275–296.

44. Что такое Proof-of-Work и Proof-of-Stake? [Электронный ресурс] / ForkLog — сайт про Биткойн, блокчейн, криптовалюты и финтех. — Режим доступа: https://forklog.com/chto-takoe-proof-of-work-i-proof-of-stake/ (дата обращения: 12.06.2018).

45. Шарипова Н. А. Проблемы образования в России [Текст] / Н. А. Шарипова, И. С. Пермякова // Сибирский торгово-экономический журнал. — 2016. — №4. — С. 80–81.

46. Шурыгина Ю. А. Развитие критического мышления как актуальная проблема современного педагогического знания [Текст] / Ю. А. Шурыгина, Ю. А. Свечникова // Педагогическое мастерство: материалы V Международная научная конференция. — Москва: Буки-Веди, 2014. — С. 50–52.

47. Юридические аспекты применения блокчейна и использования криптоактивов [Электронный ресурс] / Голос — социальная сеть, построенная на публичном блокчейне, медиаблокчейн. — Режим доступа: https://golos.io/ru--blokcheijn/@valet/yuridicheskie-aspekty-primeneniya-blokcheina-i-ispolzovaniya-kriptoaktivov (дата обращения: 16.06.2018).

48. A Quick History of Cryptocurrencies BBTC — Before Bitcoin [Электронный ресурс] / Bitcoin Magazine — печатное издание, посвящённое Биткойну, технологии блокчейн и индустрии цифровых валют. — Режим доступа: https://bitcoinmagazine.com/articles/quick-history-cryptocurrencies-bbtc-bitcoin-1397682630/ (дата обращения: 21.05.2018).

49. Alex Tapscott [Электронный ресурс] / Википедия — свободная энциклопедия. — Режим доступа: https://en.wikipedia.org/wiki/Alex_Tapscott (дата обращения: 21.12.2017).

50. Beyond The Hype Of Blockchain In Healthcare [Электронный ресурс] / COCIR — Европейский координационный комитет радиологической, электромедицинской индустрии и здравоохранения. — Режим доступа: http://www.cocir.org/uploads/media/17069_COC_Blockchain_paper_web.pdf (дата обращения: 29.05.2018).

51. Bitcoin Series 24: The Mega-Master Blockchain List [Электронный ресурс] / Ledra Capital — многопользовательская частная группа, ориентированная на растущие крупные компании в сферах высшего образования, средств массовой информации и технологий. — Режим доступа: http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list (дата обращения: 15.06.2018).

52. Bleir B. 4 Use Cases for Blockchain for Higher Ed [Электронный ресурс] / Medium — платформа для социальной журналистики. — Режим доступа: https://medium.com/@benblair_34530/4-use-cases-for-blockchain-for-higher-ed-afeee2fc9b49 (дата обращения: 02.05.2018).

53. Bleir B. Smart Contracts for Effective Curriculum [Электронный ресурс] / Medium — платформа для социальной журналистики. — Режим доступа: https://medium.com/@benblair_34530/smart-contracts-for-effective-curriculum-30c610067c51 (дата обращения: 02.05.2018).

54. Bleir B. Using blockchain to re-imagine learning [Электронный ресурс] / Medium — платформа для социальной журналистики. — Режим доступа: https://medium.com/@KnowledgeWorks/using-blockchain-to-re-imagine-learning-fb3bf2717b09 (дата обращения: 02.05.2018).

55. Blockcerts — An Open Infrastructure for Academic Credentials on the Blockchain [Электронный ресурс] / Medium — платформа для социальной журналистики. — Режим доступа: https://medium.com/mit-media-lab/blockcerts-an-open-infrastructure-for-academic-credentials-on-the-blockchain-899a6b880b2f (дата обращения: 06.06.2018).

56. Blockchain Demo [Электронный ресурс] / Проект Андерса Браунворта. — Режим доступа: https://anders.com/blockchain/ (дата обращения: 11.06.2018).

57. Blockchain Technology Needs to Be Changing Education [Электронный ресурс] / Medium — платформа для социальной журналистики. — Режим доступа: https://medium.com/age-of-awareness/blockchain-technology-needs-to-be-changing-education-2739324281e2 (дата обращения: 06.06.2018).

58. Certificates, Reputation, and the Blockchain [Электронный ресурс] / Medium — платформа для социальной журналистики. — Режим доступа: https://medium.com/mit-media-lab/certificates-reputation-and-the-blockchain-aee03622426f (дата обращения: 06.06.2018).

59. Coinmarketcap [Электронный ресурс]. — Режим доступа: https://coinmarketcap.com/ (дата обращения: 17.12.2017).

60. Communiqué of the First G20 Meeting of Finance Ministers and Central Bank Governors of 2018 [Электронный ресурс] / Официальное коммюнике первой встречи министров финансов и руководителей центральных банков стран G20 в 2018 г. — Режим доступа: https://www.g20.org /en/news/communique-first-g20-meeting-finance-ministers-and-central-bank-governors-2018 (дата обращения: 02.05.2018).

61. Creating a Trusted Experience with Blockchain [Электронный ресурс] / Sony Global Education. — Режим доступа: https://blockchain.sonyged.com/ (дата обращения: 24.12.2017).

62. Digital diplomas [Электронный ресурс] / MIT Technology Review — журнал, издаваемый Массачусетским технологическим институтом. — Режим доступа: https://www.technologyreview.com/s/610818/digital-diplomas/ (дата обращения: 06.06.2018).

63. Don Tapscott Announces International Blockchain Research Institute [Электронный ресурс] / Официальный сайт Nasdaq. — Режим доступа: https://www.nasdaq.com/article/don-tapscott-announces-international-blockchain-research-institute-cm762234 (дата обращения: 02.05.2018).

64. Ekblaw, A. A Case Study for Blockchain in Healthcare: «MedRec» prototype for electronic health records and medical research data [Text] / A. Ekblaw, A. Azaria, J. Halamka и др. // MIT Media Lab, Beth Israel Deaconess Medical Center. — 2016. — Т. 13. — P. 1–13.

65. Febin, J. How Can Blockchain Technology Innovate Your Education [Электронный ресурс] / Hackernoon. — Режим доступа: https://hackernoon.com/how-can-blockchain-technology-innovate-your-education-d1cd80c26f08 (дата обращения: 02.05.2018).

66. G20 впервые обсудит вопросы кибербезопасности и криптовалюты [Электронный ресурс] / РИА Новости. — Режим доступа: https://ria.ru/world/20180302/1515607657.html (дата обращения: 02.05.2018).

67. G20 agrees to 'monitor' cryptocurrencies but no action yet [Электронный ресурс] / Reuters — международное агентство новостей и финансовой информации. — Режим доступа: https://www.reuters.com/article/us-g20-argentina-bitcoin/g20-agrees-to-monitor-cryptocurrencies-but-no-action-yet-idUSKBN1GW 2R9 (дата обращения: 02.05.2018).

68. G20 leaders to hold fire on cryptocurrencies amid discord: sources [Электронный ресурс] / Reuters — международное агентство новостей и финансовой информации. — Режим доступа: https://www.reuters.com/article/us-g20-argentina-bitcoin/g20-leaders-to-hold-fire-on-cryptocurrencies-amid-discord-sources-idUSKBN1GV2QR (дата обращения: 02.05.2018).

69. Grech, A., Gamilleri, A. F. Blockchain in Education [Электронный ресурс]. — Режим доступа: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education(1).pdf (дата обращения: 16.12.2017).

70. Gromovs, G. Blockchain and Internet of Things require innovative approach to logistics education [Text] / G. Gromovs, K. Lammi // Silesian University of Technology. — Katowice, 2017. — T. 12. — P. 23–34.

71. ICO (криптовалюты) [Электронный ресурс] / Википедия — свободная энциклопедия. — Режим доступа: https://ru.wikipedia.org /wiki/ICO_(криптовалюты) (дата обращения: 19.12.2017).

72. Kodak blockchain project seeks to raise $50 million in token offering [Электронный ресурс] / Reuters — международное агентство новостей и финансовой информации. — Режим доступа: https://www.reuters.com/article/us-crypto-currencies-eastman-kodak/kodak-blockchain-project-seeks-to-raise-50-million-in-token-offering-idUSKBN1IB1J7 (дата обращения: 16.05.2018).

73. Kurilla, I. Education in Russia, 2016 [Text] / I. Kurilla, ред. S. Aris, M. Neumann, R. Orttung, J. Perović и др. // Russian Analytical Digest. — 2016. — № 191. — P. 1–4.

74. Lazaroiu, C. Smart district through IoT and blockchain [Text] / C. Lazaroiu, M. Roscia // 6th IEEE International Conference on Renewable Energy Research and Applications. — San Diego, 2017. — P. 454–461.

75. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс] / Bitcoin.org. — Режим доступа: https://bitcoin.org /bitcoin.pdf (дата обращения: 16.12.2017).

76. Parker L. Authenticating academic certificates on the Bitcoin blockchain [Электронный ресурс] / Brave New Coin — компания, специализирующаяся на блокчейне и рынке криптоактивов. — Режим доступа: https://bravenewcoin.com/news/authenticating-academic-certificates-on-the-bitcoin-blockchain/ (дата обращения: 02.05.2018).

77. Sony внедряет блокчейн в сферу образования [Электронный ресурс]. — Режим доступа: https://cryptorussia.ru/news/sony-vnedryaet-blokcheyn-v-sferu-obrazovaniya (дата обращения: 24.12.2017).

78. Sony Details Blockchain Use for Education Data [Электронный ресурс] / CoinDesk — компания, специализирующаяся на цифровых медиа, событиях и информационных услугах для сообщества криптоактивов и блок-

чейн технологий. — Режим доступа: https://www.coindesk.com/sony-patent-filing-details-blockchain-use-managing-education-data/ (дата обращения: 17.05.2018).

79. Sony Eyes Blockchain Use for Digital Rights Data [Электронный ресурс] / CoinDesk — компания, специализирующаяся на цифровых медиа, событиях и информационных услугах для сообщества криптоактивов и блокчейн технологий. — Режим доступа: https://www.coindesk.com/sony-eyes-blockchain-use-for-digital-rights-data/ (дата обращения: 16.05.2018).

80. Tapscott, D., Tapscott A. The Blockchain Revolution and Higher Education [Электронный ресурс] / Educause Review. — Режим доступа: https://er.educause.edu/articles/2017/3/the-blockchain-revolution-and-higher-education (дата обращения: 02.05.2018).

81. The G20 seeks to strengthen the contribution of trade to the world's economies [Электронный ресурс] / Официальный сайт саммита G20 2018 в Аргентине. — Режим доступа: https://www.g20.org/en/news/g20-seeks-strengthen-contribution-trade-worlds-economies (дата обращения: 02.05.2018).

82. Watters, A. The Blockchain for Education: An Introduction [Электронный ресурс] / Hack Education — личный блог Одри Уоттерса. — Режим доступа: http://hackeducation.com/2016/04/07/blockchain-education-guide (дата обращения: 02.05.2018).

83. What we learned from designing an academic certificates system on the blockchain [Электронный ресурс] / Medium — платформа для социальной журналистики. — Режим доступа: https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain-34ba5874f196 (дата обращения: 06.06.2018).

Лабораторный практикум по дисциплине

Технология блокчейн и криптовалюта

Методические указания

к лабораторным работам для студентов

Лабораторная работа №1

Установка Ethereum Wallet

Цель работы: Получить представления и начальные навыки работы в сети Ethereum.
Результат: наличие установленного кошелька Ethereum Mist Wallet.

Теоретическая справка:

Индустрия криптовалют развивается стремительно быстро: каждый месяц появляются новые варианты кошельков, торговых площадок, обменных сервисов, да и ассортимент самих цифровых активов постоянно расширяется. Это новое веяние в финансовой сфере, позволяющее умелым инвесторам неплохо заработать на волатильности рынка. А чтобы проводить с криптовалютой различные спекулятивные операции и получать свою прибыль, ее нужно где-то хранить. Вариантов огромное количество и сегодня мы рассмотрим один из них: многофункциональный десктопный кошелек Ethereum Wallet.

Особенности хранилища

Прежде всего, Ethereum Wallet - это официальный кошелек для хранения Эфира и токенов, созданных на его блокчейне. Это продукт поддерживается разработчиками криптовалюты, а значит, обеспечивает максимальную надежность и защищенность ваших активов.

Бумажник имеет еще одно имя - Ethereum Mist Wallet - он является функцией браузера Mist, который в данный момент еще дорабатывается и в скором времени станет связующим приложением платформы для взаимодействия с сетью.

Ethereum Wallet поддерживает работу на следующих операционных системах:

- Windows;
- Mac OSX;
- Linux.

Само приложение полностью бесплатно, все комиссионные сборы, которые вы будете оплачивать за переводы, переходят майнерам сети Ethereum, поддерживающих ее работоспособность.

Ethereum Wallet - один из самых безопасных вариантов хранения, так как все приватные ключи и данные о ваших сбережениях хранятся локально на вашем устройстве и не попадают в сеть. Эфириум-кошелек является шлюзом для децентрализованных приложений на blockchain Ethereum.

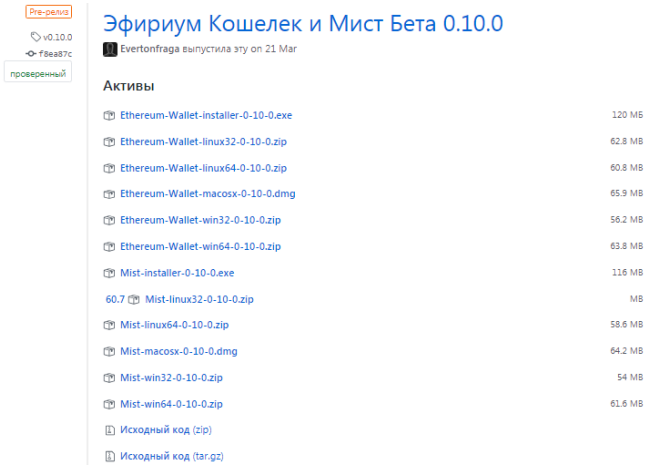
Обратите внимание на то, что приложение кошелька является довольно тяжелым, так как будет хранить полноценный блокчейн на вашем ПК, поэтому позаботьтесь о том, чтобы было достаточно свободного места (более 200 Гб).

Устанавливая Ethereum Wallet, вы имеете полную анонимность: предоставлять какие-либо личные данные или проходить процедуру верификации не придется.

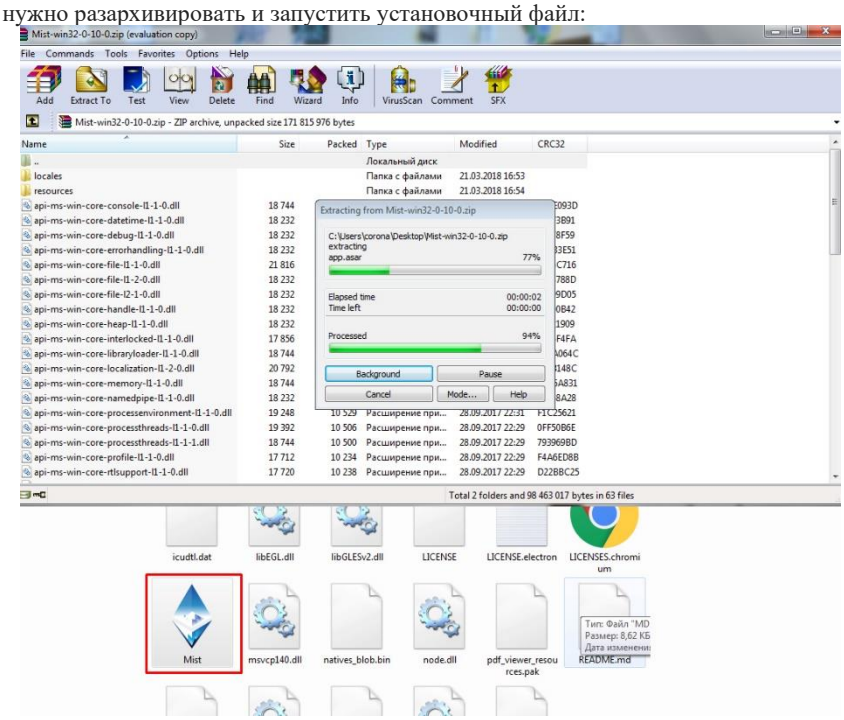
Как установить кошелек

Так как кошелек имеет официальный статус, работу начинаем непосредственно с сайта разработчика - https://ethereum.org

Все установочные файлы хранятся на Github. Выбираем свою версию и скачиваем архив на компьютер.



После этого папку нужно разархивировать и запустить установочный файл:

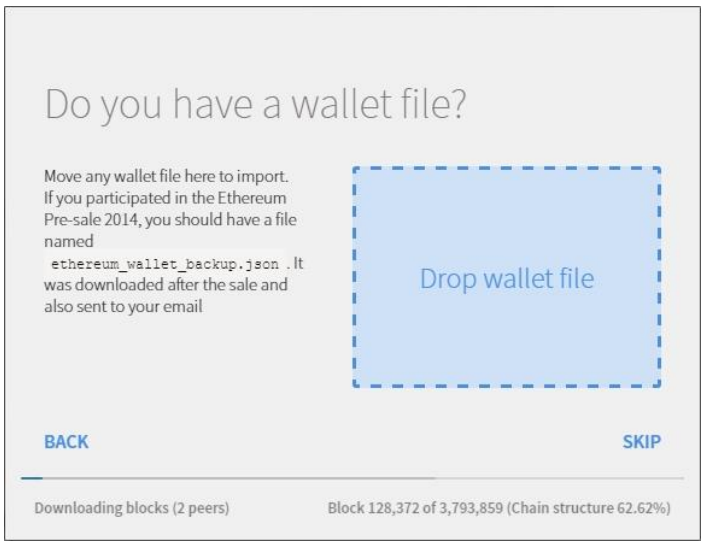


Сама программа-клиент занимает не более 150 Мб, но синхронизация блокчейна потребует около 200 Гб. После того, как установка программы пройдет успешно, перед вами откроется такое окно:

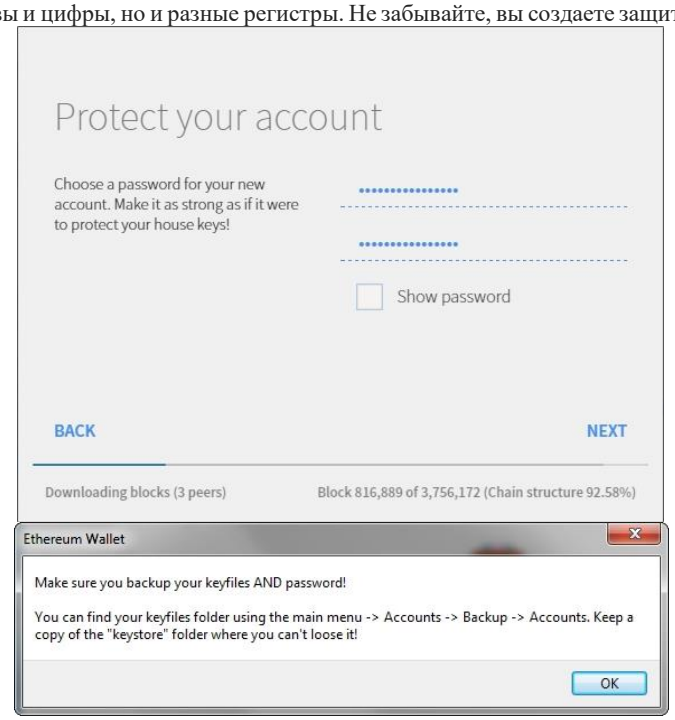
Вы должны выбрать сеть, в которой будет работать ваш кошелек:

- тестовую (для знакомства с кошельком она вполне подойдет);
- или основную (в этой версии блокчейн будет полноценно загружен).

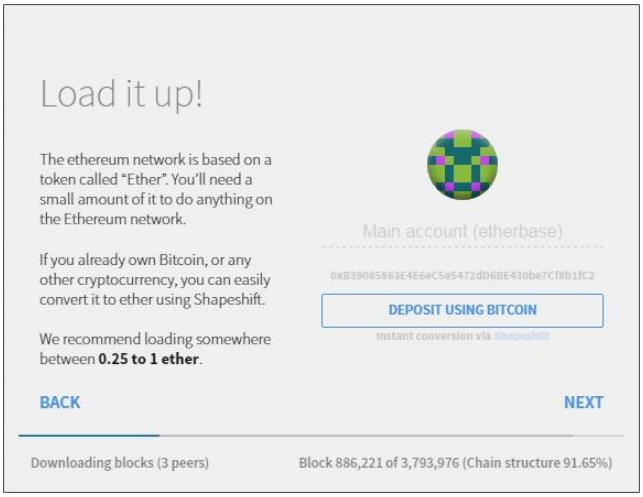
На следующем этапе можно вводить бэкап хранилища, но так как мы его не имеем, пропускаем этот шаг:



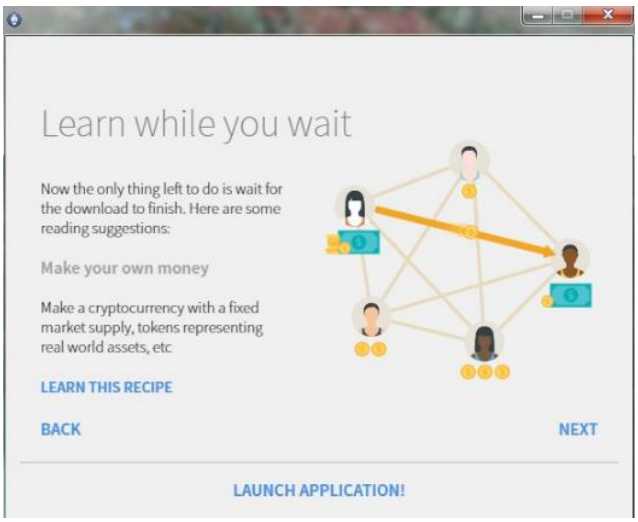
Затем открывается окно, в котором вам нужно будет создать пароль. Имейте в виду, что изменить пароль не получится, поэтому сразу отнеситесь очень серьезно к созданию сложной комбинации символов.
Используйте не только буквы и цифры, но и разные регистры. Не забывайте, вы создаете защиту своим денежным активам.



Следующее окошко напоминает нам, что использовать свой кошелек вы сможете, только имея на счету не менее 0,25 ETH. Перевести их можно прямо сейчас, используя встроенный инструмент ShapeShift. Если у вас пока нет нужных монет, вы сможете перевести их позже.

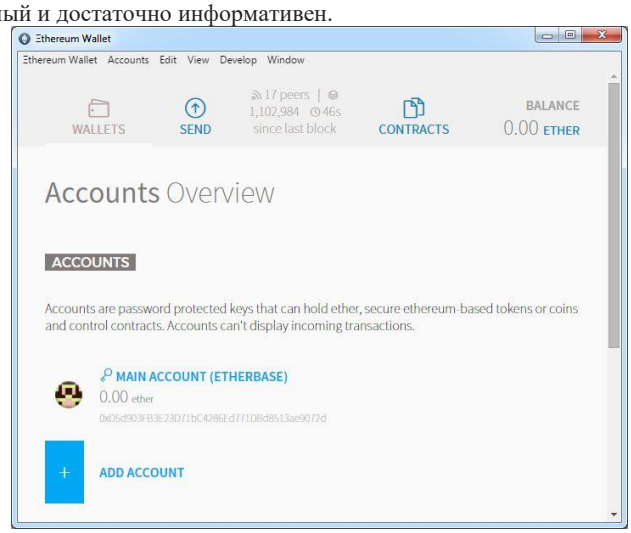


Следующее действие - синхронизация хранилища с сетью Эфириум. Этот процесс может занять несколько суток, после чего Ethereum Wallet будет полностью установлен и готов к работе.



Что внутри

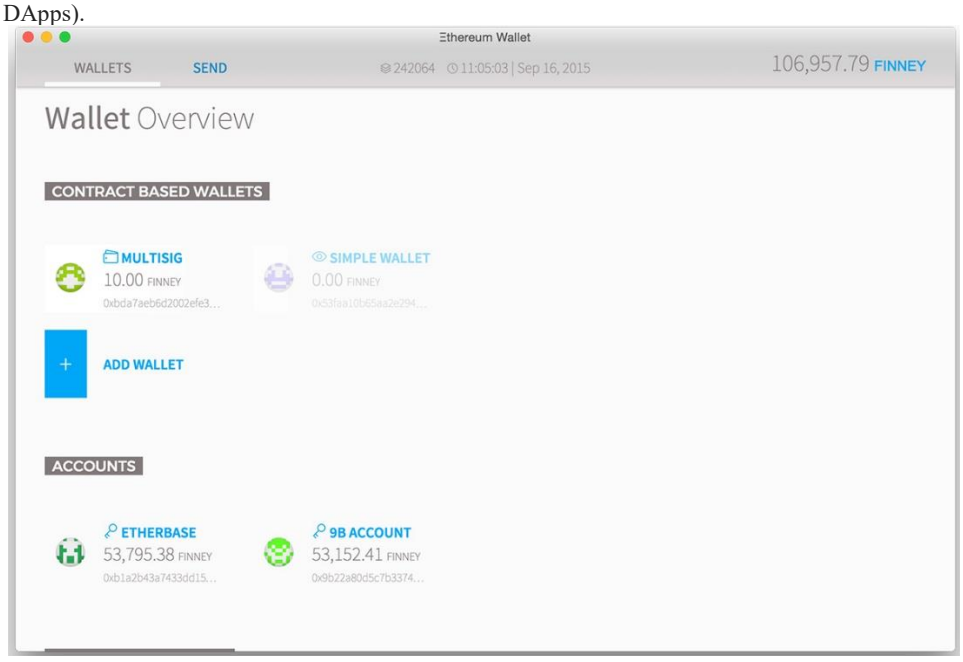
Процесс использования кошелька Ethereum Wallet будет легким не только для опытных пользователей, но и для новичков. Его интерфейс вполне понятный и достаточно информативен.



Перед тем, как пополнять баланс хранилища цифровой наличностью, лучше создать резервную копию. Для этого выбираем закладку «Аккаунты» и пункт «Резервное копирование». Сформированный файл сохраните в очень надежном месте, доступ к которому у вас будет всегда. Целесообразно иметь несколько копий.

Etereum Wallet имеет разделение на 2 основных раздела:

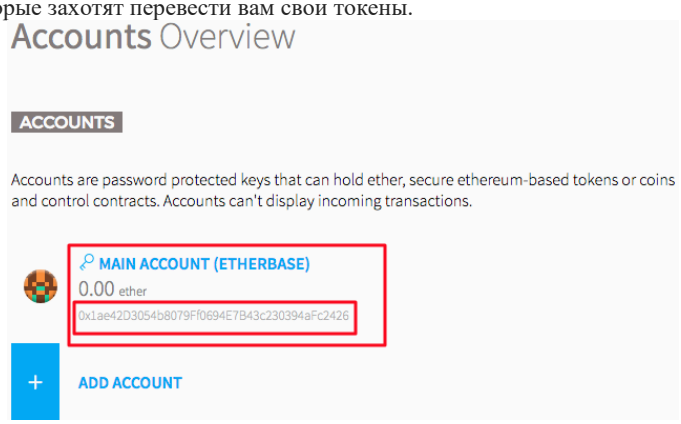
1. Accounts (в этом разделе вы сможете видеть баланс кошелька и суммы поступлений).
2. Contract Based Wallets (здесь вы сможете видеть полную информацию обо всех входящих и исходящих транзакциях и использовать DApps).



Учетный раздел (Accounts) имеет закрытый ключ с паролем и адресом, контрактный раздел (Contract Based Wallets) не имеет закрытого ключа, но имеет свой адрес, код и хранилище, с помощью которых можно не только создавать кошельки, но и всевозможные интересные децентрализованные приложения (DApps).
Можно сказать, что учетная часть кошелька отвечает за простое хранение Эфира, а контрактная часть обеспечивает управление криптовалютой.

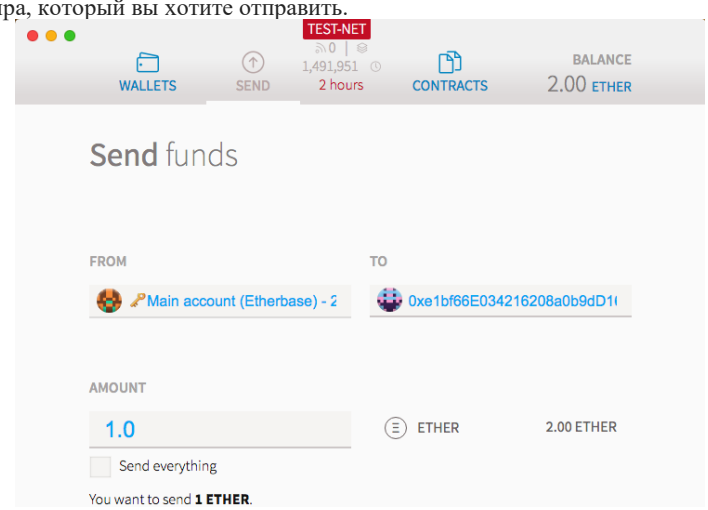
Как пользоваться кошельком

Первая задача - это пополнить баланс кошелька Эфиром. На главной странице хранилища в разделе Main account вы можете видеть адрес хранилища, на который вам нужно перечислить как минимум 0,25 ETH.
Ethereum-адреса представлены в шестнадцатеричном формате: они состоят из 40 символов. Этот адрес вы будете давать всем своим знакомым, которые захотят перевести вам свои токены.

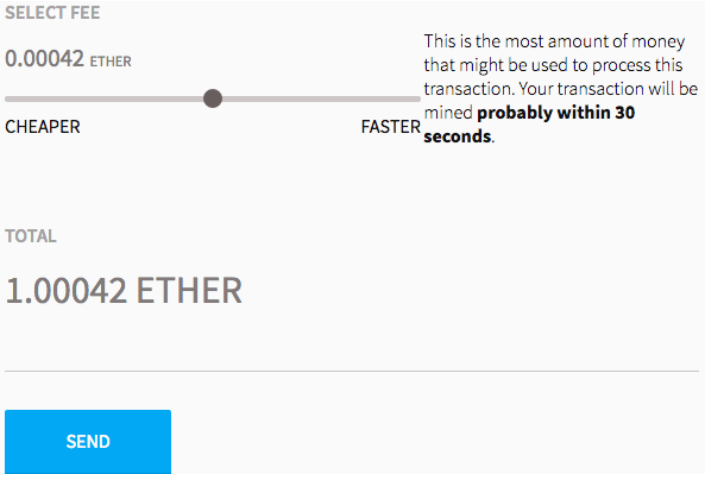


Чтобы создать исходящую транзакцию и отправить эфир из Mist Wallet, выполните следующие действия:

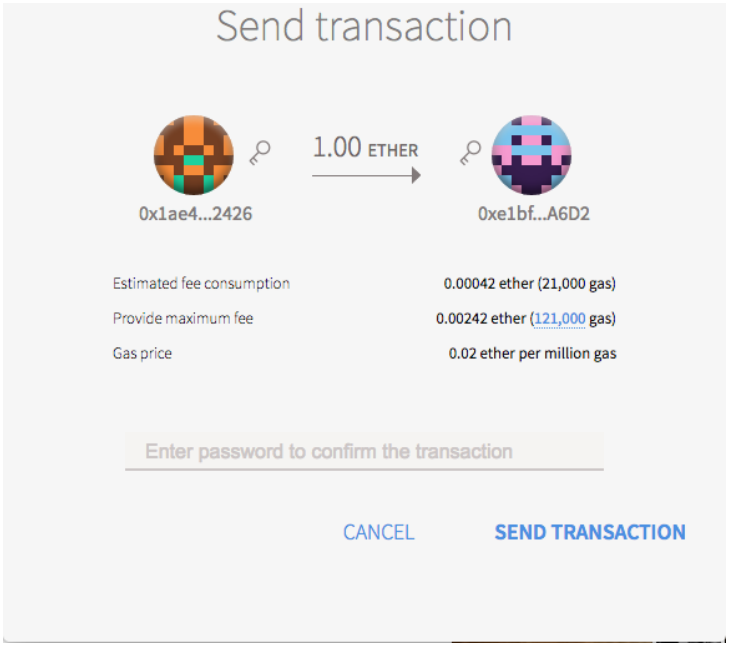
1. Перейдите к разделу SEND.
2. Укажите адрес принимающей стороны.
3. Выберите количество эфира, который вы хотите отправить.



Вы можете оставить комиссию такой, какую предложила программа по умолчанию, а можете изменять ее размер, перемещая бегунок:



Останется только ввести правильно свой пароль:



Чтобы посмотреть информацию о какой-то конкретной транзакции, перейдите в раздел «Обзор кошелька» → «Последние транзакции» и кликните на нужную операцию в списке:

Заключение

Ethereum Mist Wallet предназначен для надежного и безопасного хранения всех типов монет и токенов Эфириума, а также для смарт-контрактного взаимодействия пользователей через децентрализованные приложения браузера.

Положительные стороны Mist-кошелька - это его многофункциональность, понятный интерфейс и высокие показатели безопасности.

Из минусов можно отметить только очень долговременную синхронизацию: процесс занимает около 2 суток. Но, это плата за надежную сохранность ваших цифровых активов.

Задание

1. Установить кошелек Ethereum Mist Wallet. Подключаемся только к тестовой сети.
2. Ознакомиться с функционалом кошелька.

Контрольные вопросы

1. Почему при установке кошелька Ethereum Mist Wallet в рабочем режиме требуется большой объем свободного пространства на винчестере?
2. Какие операции доступны в кошельке Ethereum Mist Wallet?
3. Укажите недостатки кошелька Ethereum Mist Wallet?

Лабораторная работа №2

Знакомство с инструментами и средой разработки смарт-контрактов

Цель работы: изучить и закрепить на практике возможности основных инструментов разработчика смарт-контрактов.

Результат: наличие установленного кошелька MetaMask, настроенного на работу с тестовой сетью Rinkeby.

Теоретическая справка:

Смарт-контракты: что это?

Смарт-контракты, или "умные контракты", позволяют передавать некоторые ценности, например, собственность или акции, прозрачным и одновременно безопасным способом, что делает весь процесс сверхэффективным, одновременно устраняя промежуточные звенья, зачастую долгие и дорогие. Рассмотрим пример, который позволит понять, как блокчейн работает со смарт-контрактами.

Давайте представим, что есть два заинтересованных лица в сделке с недвижимостью. Один (*продавец*) желает продать жилье, а другой (*покупатель*) хочет купить это жилье. *Сделка* по продаже может быть реализована посредством блокчейна, и *покупатель* готов платить, например, биткоинами. Как только *покупатель* заплатит, то сразу получит подтверждение о транзакции, которое будет исполнено в виде виртуального смарт-контракта. *Продавец*, в свою *очередь*, передает покупателю цифровой *ключ* от *входной* двери, который будет доставлен в день, о котором заинтересованные стороны договорились. Если *продавец* вдруг передумает продавать дом, *покупатель* не получит *ключ*, блокчейн в этом случае автоматически вернет покупателю деньги в тот день, когда должен был быть получен *ключ*. А если *покупатель* получит *ключ* заранее, то блокчейн его удержит до дня, в который была договоренность осуществления передачи. Поэтому каждая из сторон получит то, что хочет, в оговоренный в контракте день: *продавец* - деньги, а *покупатель* - *ключ*. А поскольку блокчейн - это технология, основанная на пиринговой сети, договор по этой сделке будет храниться на множестве узлов, что обеспечит выполнение взятых по контракту обязательств, и ни одна из сторон не сможет изменить условия контракта после его заключения. Ну а если кто-то из сторон наберется смелости сделать это, все узлы в сети тут же об этом узнают, и проблема будет мгновенно решена.

Мы рассмотрели пример с куплей-продажей недвижимости. Но такие же соглашения могут заключаться при передаче акций, в страховании автомобилей или другого имущества и во многих других случаях. Позвольте привести несколько ключевых преимуществ смарт-контрактов.

Первое качество, за которое смарт-контракты так ценятся, это *автономность*. Смарт-контракты не могут быть изменены третьими лицами, так как только их стороны заключают соглашение. Нет необходимости обращаться к услугам юристов при заключении соглашений.

Второе преимущество, за которое люди любят - или еще полюбят - смарт-контракты, это *доверие* к ним. Смарт-контракт невозможно потерять. Они все зашифрованы и хранятся в общественном хранилище. Поэтому потеря любого из них исключена.

Это подводит к следующему плюсу - *резервированию*. Можно положиться на *надежность* смарт-контрактов, потому что они все зарезервированы. *Аннулирование* договора по причине потери его копии просто невозможно.

Следующим в списке идет *безопасность*, которая опять же связана с предыдущими двумя. Ваши смарт-контракты будут защищены современными методами шифрования данных. Это отсылает нас к вопросу доверия - вы можете полностью доверять безопасности методов шифрования. Смарт-контракт практически невозможно взломать.

Пятая причина превосходства смарт-контрактов над обычными - это *скорость* их передачи. На заключение традиционных договоров уходит уйма времени, поскольку в их эту работу вовлечено множество третьих лиц. Если речь идет о распространении кода, смарт-контракты на высоте, поскольку позволяют решать задачи в разы быстрее.

Шестая причина - это *экономия денег* на заключении договоров. Нет необходимости прибегать к услугам адвокатов. Можно просто использовать технологию смарт-контрактов.

И, наконец, огромным преимуществом является *точность*. Если все подробности контракта указаны точно, то он будет выполнен значительно точнее, чем любой другой контракт.

Инструментарий и приложения экосистемы эфириума

Прежде чем погрузиться в написание кода, стоит изучить экосистему Ethereum. Давайте разберемся, какие инструменты и подходы существуют, как они называются и взаимодействуют.

В экосистеме Ethereum широко используются такие инструменты, как Geth, *Parity*, Solidity, Remix, Truffle, Webpack, Angular и так далее. Каждый из них используется для решения конкретных задач.

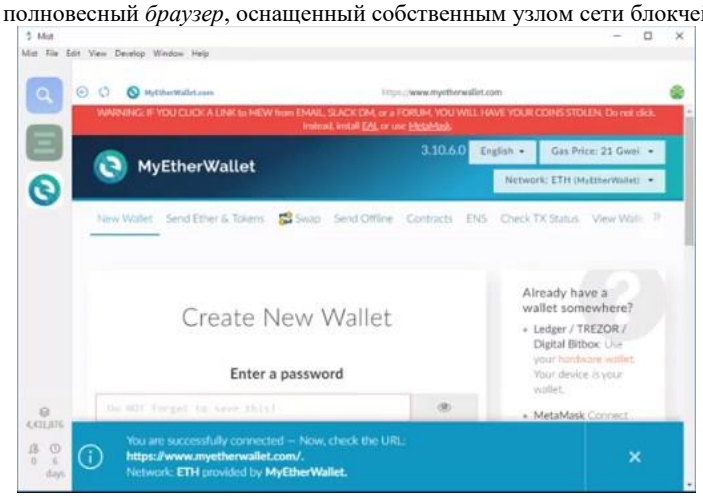
Узлы сети блокчейна: Go-Ethereum, Parity, CPP-Ethereum

Примерами узлов блокчейна выступают такие программы, как Geth, *Parity* или CPP-Ethereum. Все они работают на клиентской стороне, то есть их можно загрузить и запустить на вашем компьютере, как и для всех других пользователей сети Ethereum. Они все выполняют одну и ту же задачу: реализуют протокол Ethereum. Несмотря на то, что разные инструменты выполняют одну и ту же роль, они написаны на разных языках программирования. Развитием инструментов занимаются различные команды, которые обязательно следят за тем, чтобы даже на разных языках программирования протокол Ethereum был реализован корректно. Если проводить аналогию, то эта схема похожа на использование среды MySQL в режиме "мульти-мастер", когда все узлы выполняют одну и ту же задачу по репликации *базы данных*. Это отлично описывает то, что делают все узлы в сети блокчейна - они копируют все блоки на своих компьютерах. Поэтому при загрузке Geth, *Parity*, или CPP-Ethereum и запуске клиента после установки подключения к другим узлам будет загружено все содержимое блокчейна. *Исключение* составляет только режим "легкого клиента", когда загружаются только *заголовки* блоков.

Взаимодействие веб-сайтов и блокчейна

Рассмотрим популярные браузеры MetaMask и Mist. Оба они представляют собой связующее звено между обычным браузером для просмотра интернет-страниц и блокчейном С помощью корректно настроенного веб-сайта можно выполнять программы и отправлять команды в блокчейн. *Пользователь* сможет запустить любой *браузер*: например, *Chrome*, Firefox, *Internet* Explorer или другой *браузер*, зайти на такой *веб-сайт* и взаимодействовать с блокчейном. Для этого к блокчейну необходимо подключиться. MetaMask представляет собой надстройку для *Chrome* и Firefox, облегчающую подключение к блокчейну.

Mist, в свою *очередь* - это полновесный *браузер*, оснащенный собственным узлом сети блокчейна.



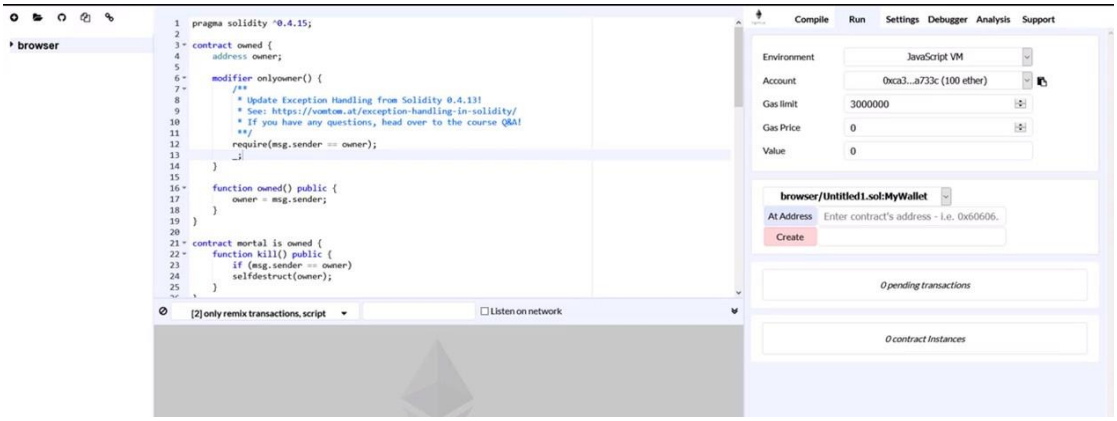
В случае с Mist, узлом блокчейна является Geth, или Go-Ethereum, непосредственно встроенный в *браузер*. MetaMask для работы использует сервис под названием Infura. В среде Infura используются узлы Geth и *Parity*, которые запущены на стороне сервера, а не на компьютере клиента, а Infura реализует подключение к ним. Чтобы познакомиться с надстройкой MetaMask, можно открыть *браузер*, например, *Chrome*, найти раздел с иконками надстроек, далее открыть MetaMask и можно начинать работать с блокчейном. Кошелек Mist выглядит так: слева *доступ* к различным разделам, есть *отображение* статуса подключения и синхронизации данных, в центре располагается собственно *браузер* Это позволяет работать с блокчейном и просматривать веб-страницы можно одновременно.

Что такое Solidity

Solidity представляет собой *язык программирования* высокого уровня. Для ее работы требуется *компилятор* solc, который формирует байткод для виртуальных машин Ethereum.Встречаются мнения, что Solidity похож на JavaScript. В первых версиях так и было, однако сейчас эти два языка значительно расходятся. Тем не менее, Solidity похож на JavaScript больше, чем любой другой *язык программирования*.

Remix, веб-среда разработки для Solidity

Remix - это облачная *среда разработки*, поддерживающая много полезных функций. *Доступ* к Remix можно получить по адресу http://remix.ethereum.org. Среда Remix позволяет создавать и запускать код на языке Solidity прямо в окне браузера. Remix оснащена встроенным отладчиком и статическим анализатором кода, а также многими другими инструментами.



На текущий момент Remix выглядит так. Слева расположен *браузер*, с помощью которого можно управлять файлами. В центре располагается окно для создания кода, а справа - *управляющие* элементы - вкладки для компиляции (*Compile*), запуска (Run), изменения настроек (Settings), отладки (*Debugger*), анализа (*Analysis*) и получения поддержки (*Support*).На вкладке Run можно выбрать среду запуска кода, например, виртуальную машину *Java*. Remix предоставляет *доступ* к нескольким счетам в эмулированной среде Ethereum для апробирования создаваемого кода. С их помощью можно размещать и обсчитывать контракты, а потом анализировать результаты благодаря наличию журнала исполнения кода.

Использование библиотек Web3.js и Eth.js

Библиотеки Web3.js и Eth.js облегчают взаимодействие между браузером и блокчейном и позволяют работать узлами сети Ethereum по протоколу *RPC* посредством *HTTP* и кода JavaScript. Если запустить локальный узел блокчейна, он откроет *интерфейс HTTP-RPC*, что позволит браузеру отправлять узлу команды, чтобы узел, в свою *очередь*, переправлял данные в блокчейн.

Библиотека Truffle и ее отличие от Web3.js

Truffle и Embark являются инструментариями для среды Solidity и разработки распределенных приложений для работы с блокчейном. Оба они поддерживают управление контрактами, их *размещение* в блокчейне, или миграцию, оснащены встроенной системой тестирования приложений, а Truffle еще и предлагает решение Truffle Boxes - предварительно настроенные среды разработки распределенных приложений, значительно облегчающие работу, такие как Truffle-React, Truffle-Webpack и так далее. При серьезном подходе к разработке приложений для блокчейна стоит уделить внимание Truffle и Embark и постепенно отходить от использования только библиотеки Web3.js.

Использование Angular, Vue.js, React и Redux в разработке приложений для блокчейна

Такие наборы инструментов, как Angular, Vue.js, React, Redux предназначены для разработки веб-страниц и непосредственно не работают с блокчейном, Truffle, Solidity и другими подобными средами. Для работы с Angular, Vue.js, React, Redux или другими инструментариями для создания веб-страниц обычно достаточно загрузить библиотеку Web3, подключиться к узлу блокчейна и настроить взаимодействие с блокчейном с помощью Web3.

Применение инструментов Browserify и Webpack

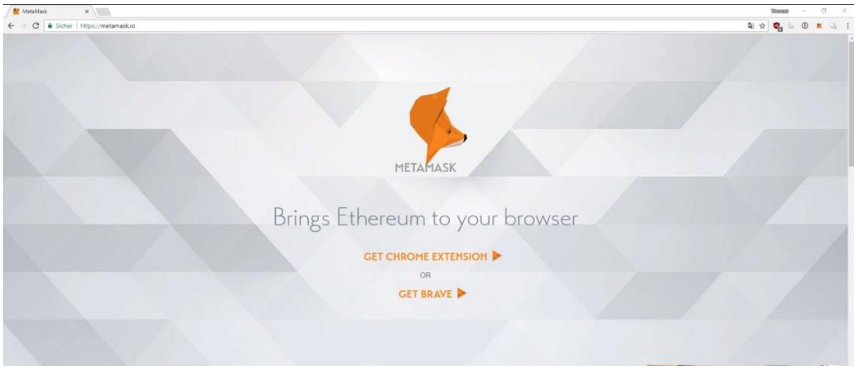
Webpack - это упаковщик файлов JavaScript, необходимо использовать тогда, когда *программа* использует большое количество файлов: Webpack собирает их воедино, разрешает все взаимозависимости между файлами, позволяя коду обращаться только к паре мастер-файлов, что значительно ускоряет загрузку веб-приложения, тк веб-серверу больше не приходится отправлять несколько сотен файлов.

Browserify делает примерно то же самое, но на базовом уровне - ведь Webpack сразу решает спектр задач по упаковке файлов для веб-разработки. Browserify представляет собой только упаковщик, разрешающий файловые взаимозависимости и объединяющий много файлов в один. *Node Package Manager*, или NPM, загружает и управляет пакетами для узлов сети Ethereum, что облегчает разработку веб-проектов.

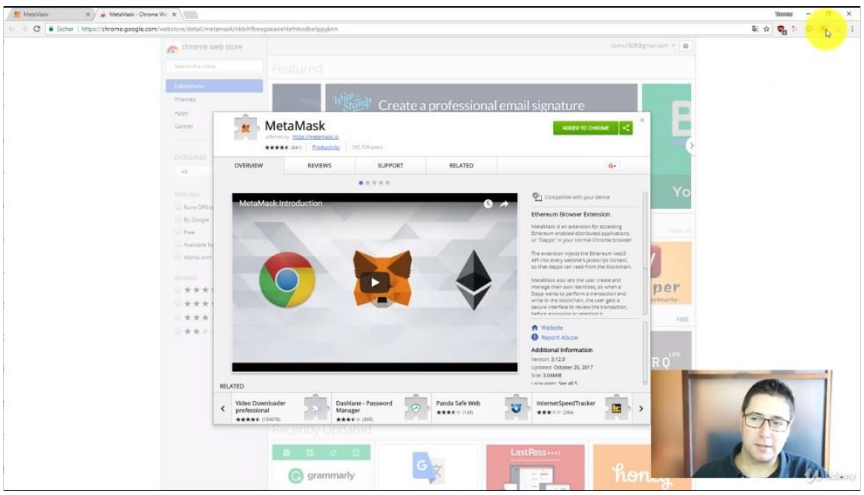
Обзор и возможности MetaMask

Поговорим о надстройке для браузера *Chrome* - MetaMask. В этом разделе установим ее, разберем функционал, а также узнаем, как получить немного эфира для тестирования MetaMask и размещения контрактор в тестовой сети Rinkeby.

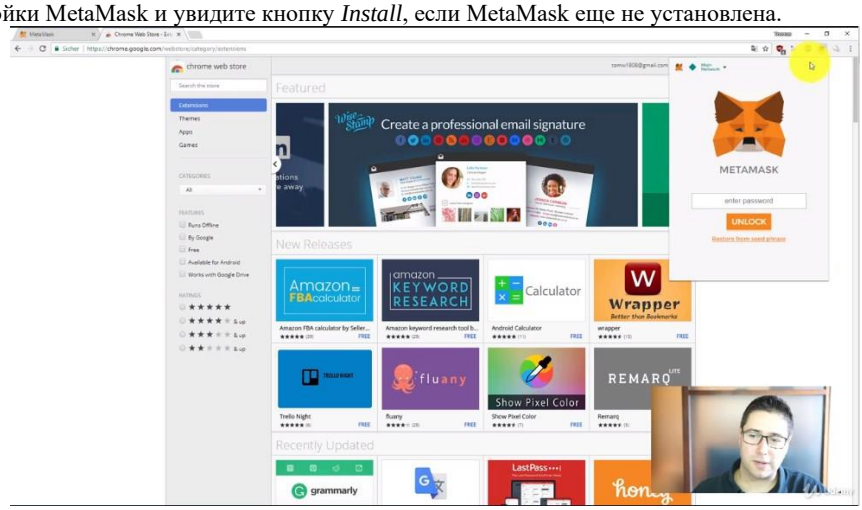
Установка MetaMask



Откроем веб-*сайт* MetaMask, маскотом которой является лисичка.



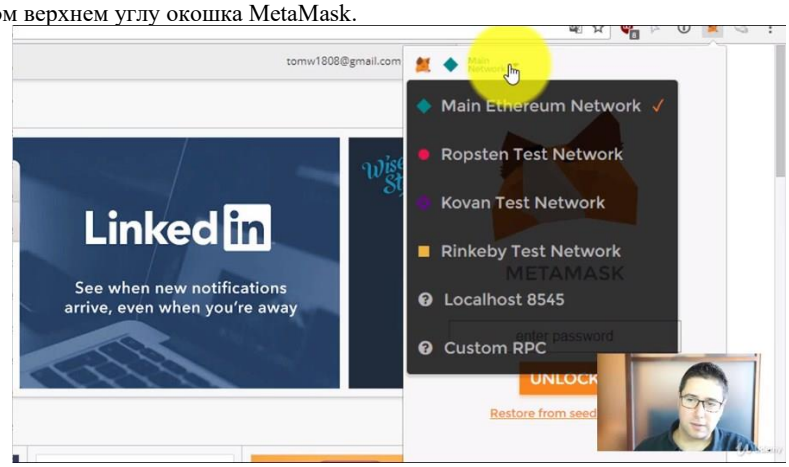
При щелчке на *Get the Chrome Extension* (*браузер Chrome* существует для всех платформ) вы перейдете на страницу установки надстройки MetaMask и увидите кнопку *Install*, если MetaMask еще не установлена.



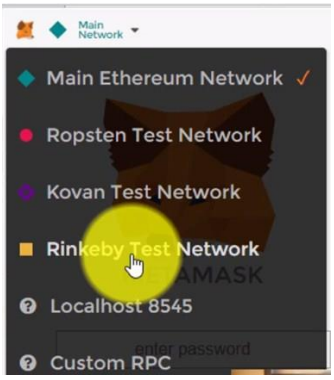
После установки MetaMask можно будет запустить с помощью ее иконки в верхнем правом углу браузера *Chrome*, а несколько простых шагов установки сопровождаются подробными инструкциями. Потребуется задать *пароль* для защиты ваших счетов, после этого можно работать с MetaMask.

Элементы MetaMask

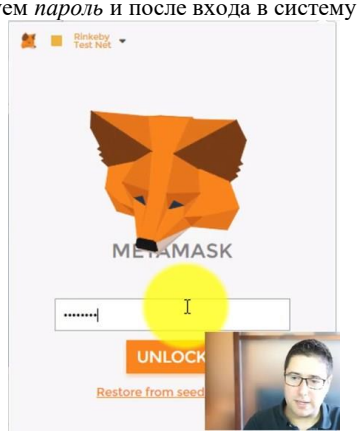
Продолжим разговор о надстройке MetaMask. Для начала выбраем *сеть*, с которой вы будете взаимодействовать - ее можно выбрать в левом верхнем углу окошка MetaMask.



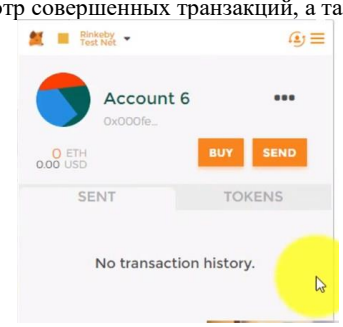
После этого необходимо опубликовать свое *приложение* в главной сети Ethereum, которое будем использовать для взаимодействия с другими смарт-контрактами, опубликованными там.



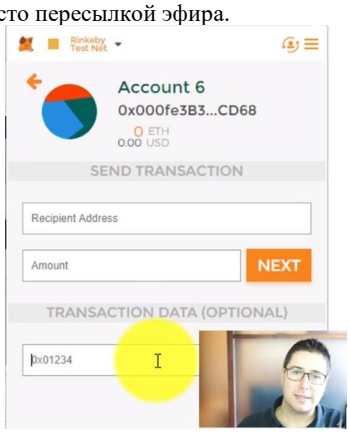
В рамках данного курса будет достаточно тестовой сети Rinkeby. Мы узнаем, как получить немного эфира для использования в этой тестовой сети, разобраться с тем, как *сеть* реагирует на запросы, посмотрим на майнинг, задержки и проблемы одновременных вычислений, характерные для блокчейна.
Теперь авторизуемся в MetaMask. Используем *пароль* и после входа в систему будет создан счет.



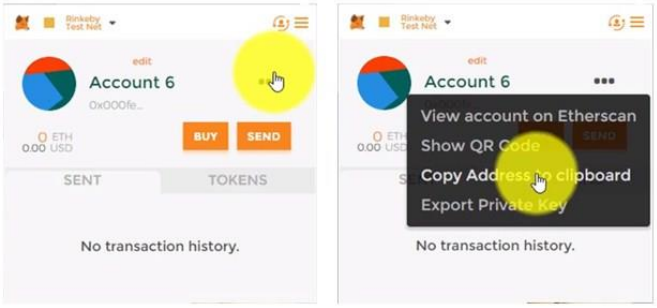
Доступен обзор имеющихся счетов, просмотр совершенных транзакций, а также жетонов среды Ethereum.



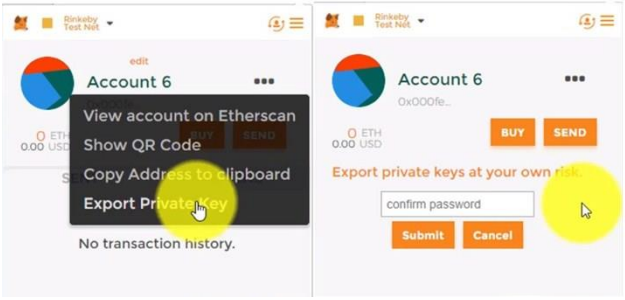
Если на счету есть эфир, его можно отправить на другой *адрес* и добавить к транзакции данные. Об этом мы поговорим позднее. На данном этапе ограничимся просто пересылкой эфира.



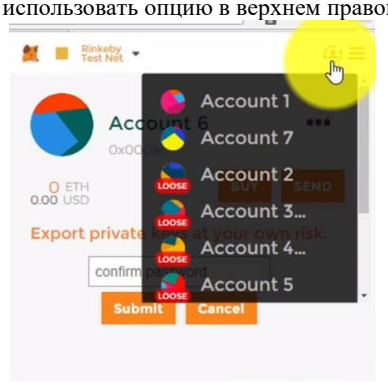
В *меню* обзора счета можно скопировать *адрес* в *буфер* обмена и экспортировать частный *ключ* вашего счета для использования его в другом приложении.



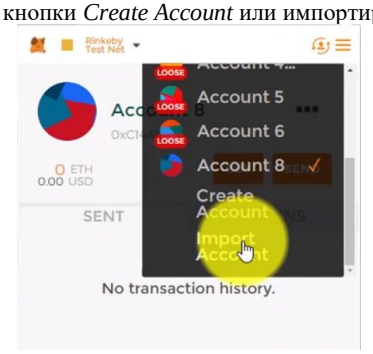
Обратите внимание, что *доступ* к счетам обеспечивается с помощью вашего частного ключа.



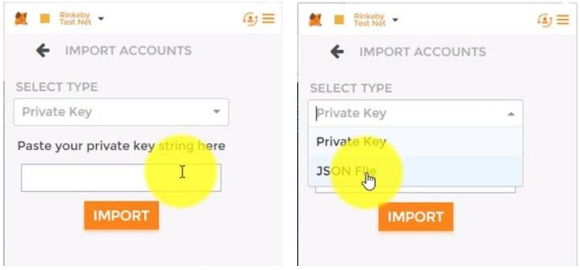
Для переключения между счетами можно использовать опцию в верхнем правом углу.



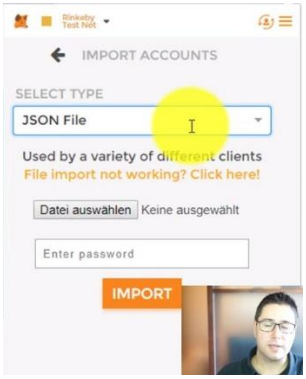
Можно создавать новые счета с помощью кнопки *Create Account* или импортировать счета с помощью *Import Account*.



Для этого потребуется частный *ключ* к счетам, предварительно созданным в Geth или другой системе, создающей ключи *JSON*.

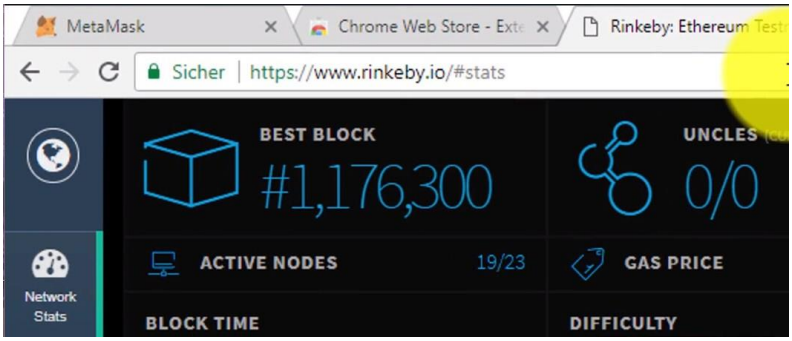


Импорт осуществляется посредством этих файлов-ключей *JSON*.

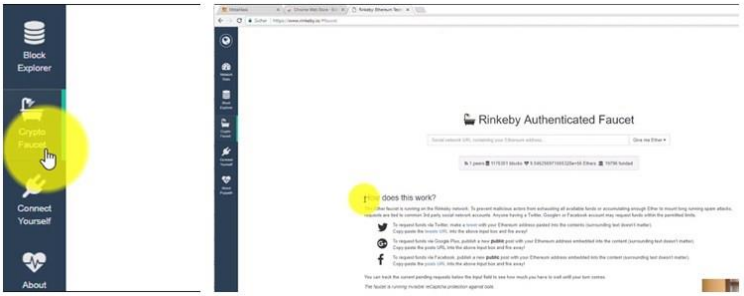


Как получить эфир для тестовой сети Rinkeby

Чтобы получить некоторое количество эфира для использования в тестовой сети Rinkeby, потребуется открыть веб-*сайт* http://rinkeby.io.

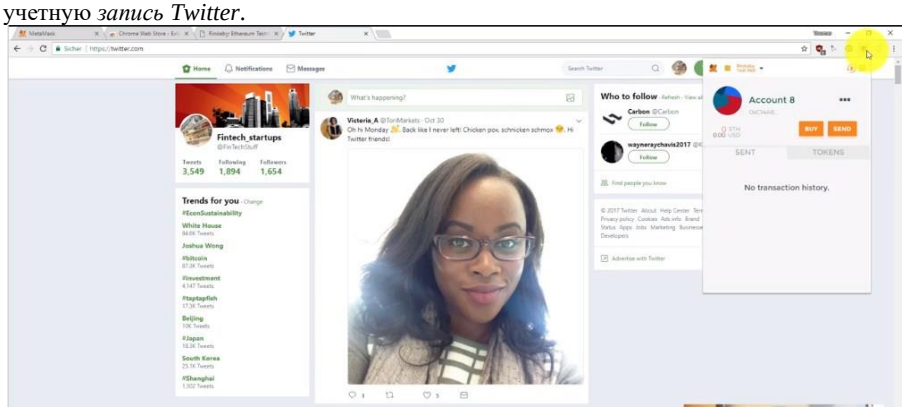


В его нижнем левом углу расположена иконка Crypto Faucet, при щелчке по которой разъясняется, как можно получить эфир на счет Rinkeby.

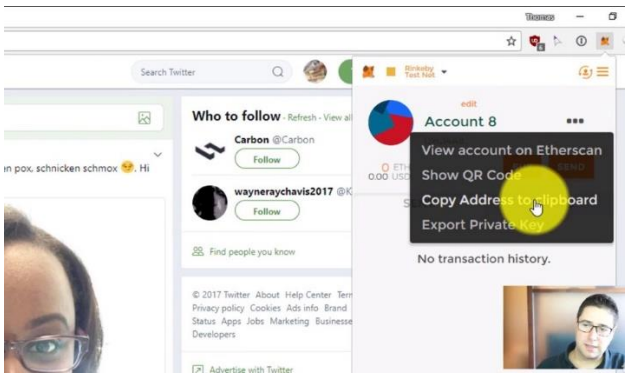


Для получения эфира достаточно опубликовать номер своего счета в *Twitter*, Google Plus или Facebook, а затем скопировать *адрес* веб-страницы с публикацией в форму на сайте rinkeby.io. Эти меры предосторожности необходимы для защиты от автоматического массового получения эфира.

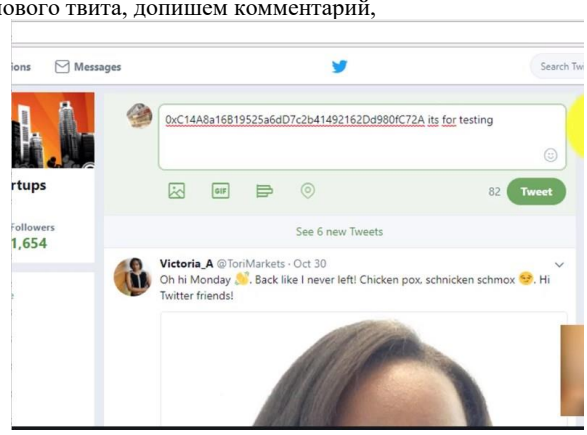
Теперь зайдем в учетную *запись Twitter*.



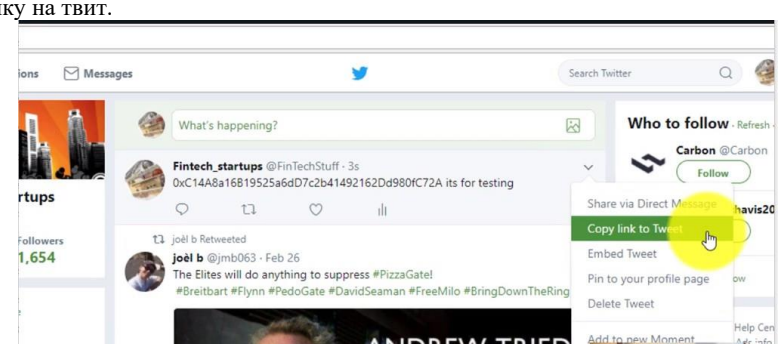
скопируем *адрес* счета из MetaMask,

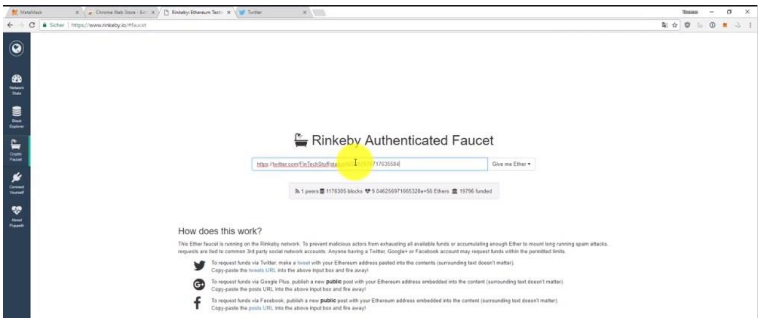


введем в *поле* для публикации нового твита, допишем комментарий,

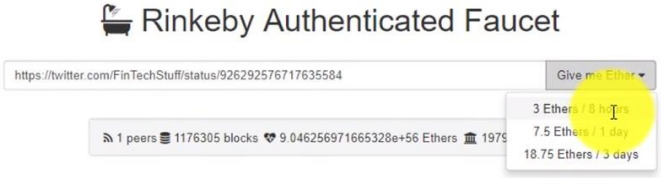


затем скопируем ссылку на твит.

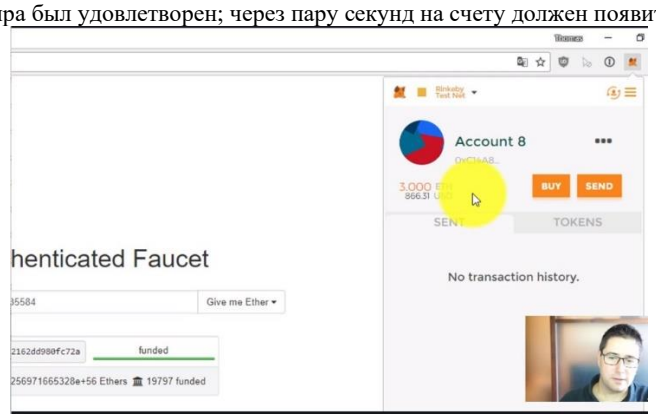




То же самое можно сделать и с помощью Facebook, единственное, в чем нужно убедиться - это должен быть публичный пост. Так, *запрос* на выделение эфира был размещен.



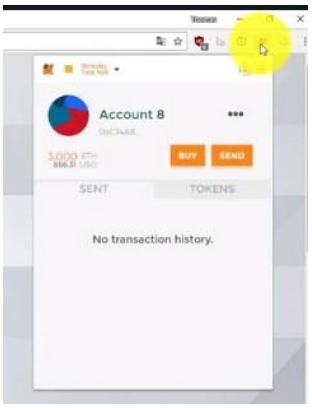
Для корректной работы системы начисления эфира потребуется отключение блокировщика рекламы. Теперь убедимся, что *запрос* на выделение эфира был удовлетворен; через пару секунд на счету должен появиться эфир.



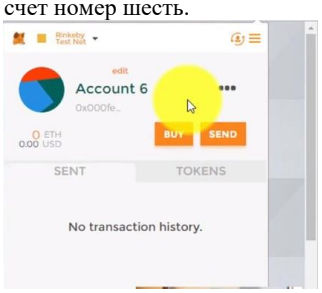
Наличие на счету эфира можно проверить с помощью сервиса Etherscan.

Пересылка эфира с помощью MetaMask

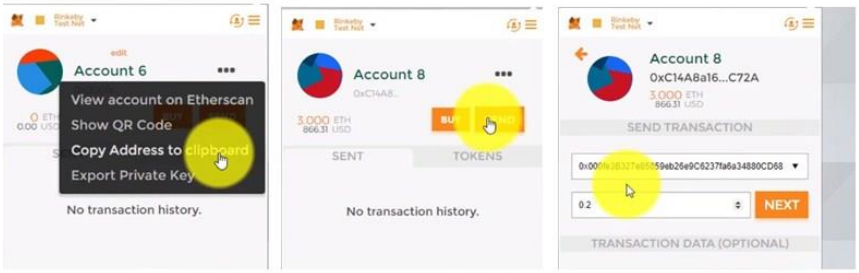
Теперь попробуем выполнить пересылку эфира между счетами с помощью MetaMask. Допустим, что на счете номер восемь есть три единицы эфира.



Необходимо переслать часть этих средств на счет номер шесть.

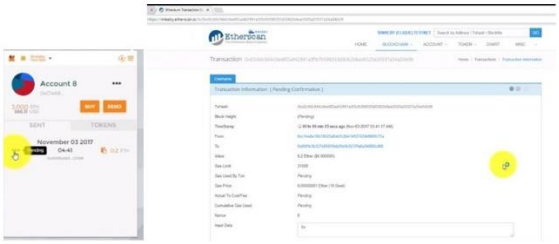


Скопируем *адрес* счета номер шесть, переключимся на счет номер восемь и отправим 0,2 единицы эфира.

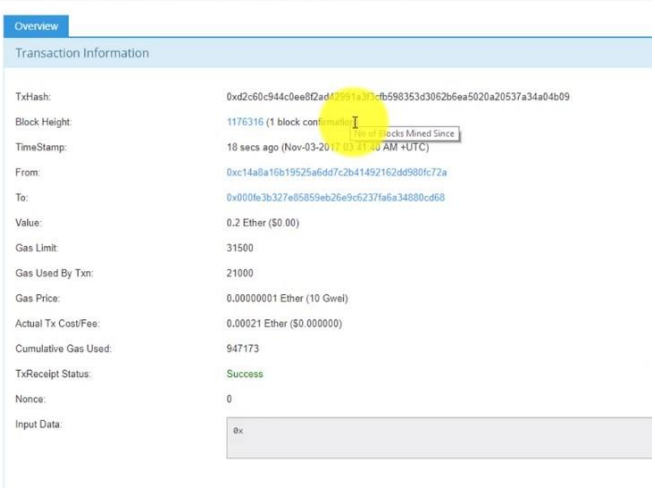


Щелкнем по *Next*, посмотрим на транзакцию и отправим ее в блокчейн.

Статус транзакции можно проверить с помощью сервиса Etherscan.

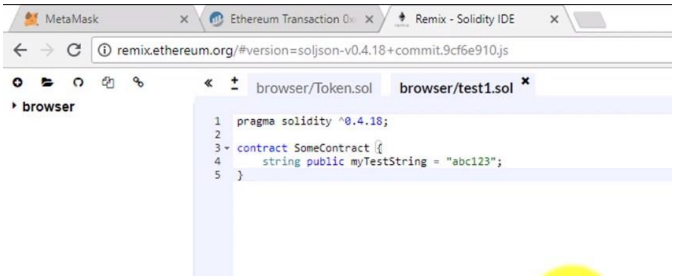


После успешно завершенного обсчета транзакции, средства будут отправлены, и будет отображаться *адрес* блока, в котором эта *транзакция* была впервые подтверждена.

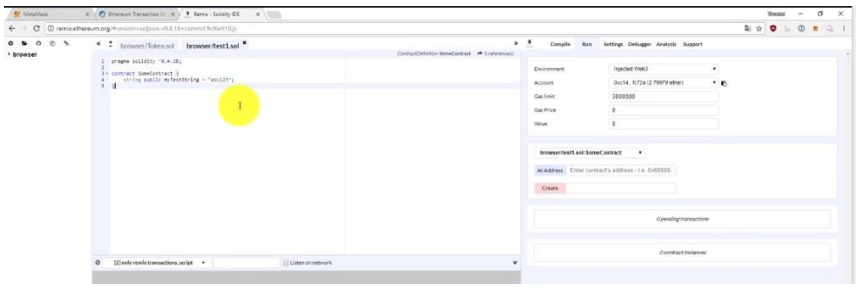


Взаимодействие MetaMask и браузера

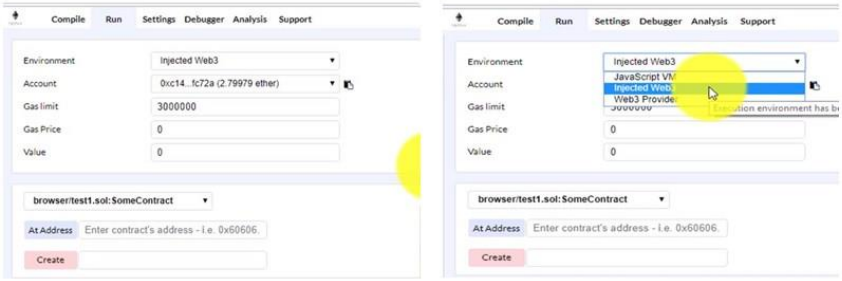
Следующей возможностью MetaMask является взаимодействие с блокчейном посредством веб-сайта. В этом случае веб-*сайт* подключается к MetaMask, MetaMask - к блокчейну с помощью сервиса Infura, а Infura, в свою *очередь*, содержит в себе запущенный клиент Geth. Позднее, когда будем разбирать тему подключения к блокчейну из браузера, данная схема будет рассмотрена подробнее - для нее возможны несколько реализаций. На текущем этапе достаточно посмотреть, что происходит в надстройке MetaMask, когда вы пытаетесь взаимодействовать с блокчейном. Откроем среду Remix, здесь есть простой смарт-контракт.

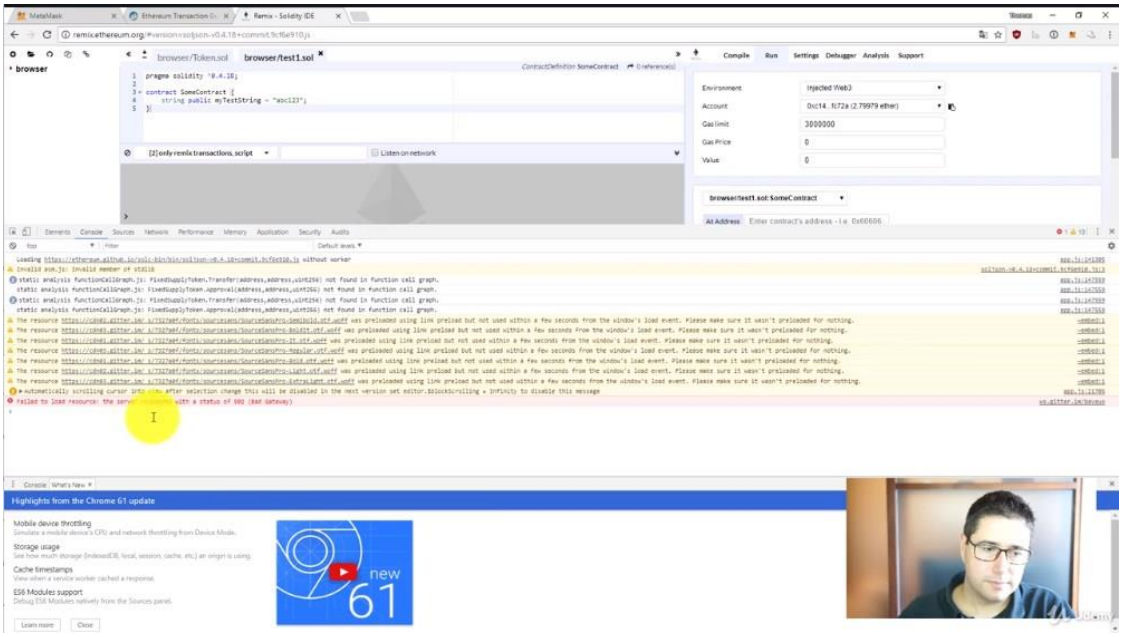


В правой стороне окна Remix видно, что в качестве опорной библиотеки выбрана Web3.

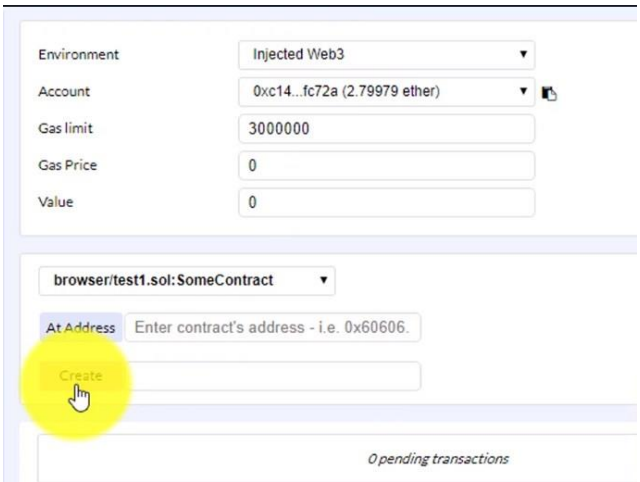


Надстройка MetaMask подключается непосредственно к окну браузера и таким образом обеспечивает *связь* с блокчейном. В раскрывающемся списке выбрана Injected Web3, а в окне разработки, доступном для любой веб-страницы, видно, что с помощью объекта *web3.currentProvider* можно работать с надстройкой MetaMask посредством обычного кода JavaScript.

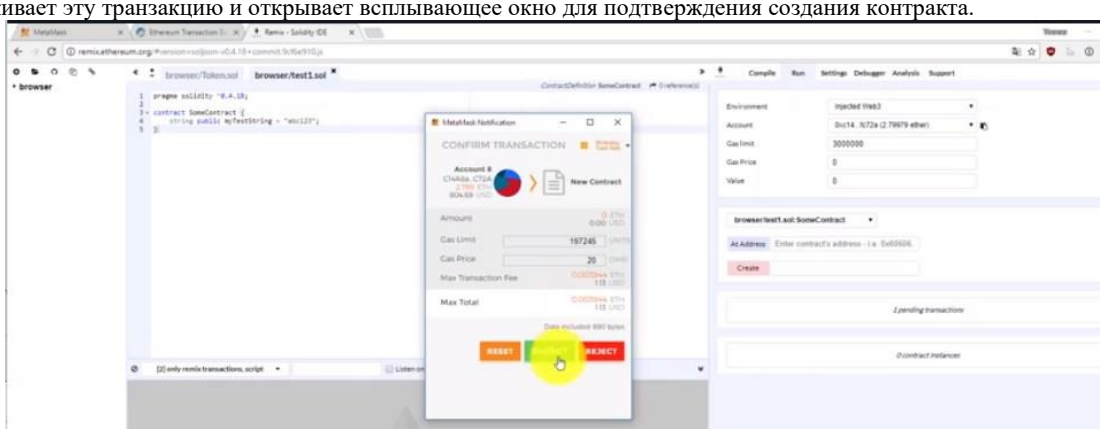




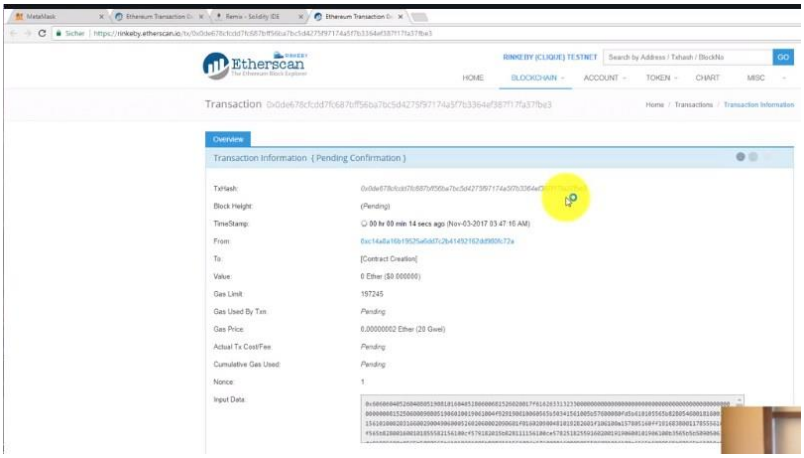
Выберем Injected Web3, затем счет - тот же самый, который открыт в надстройке MetaMask. Теперь можно перейти на вкладку Run и создать контракт.



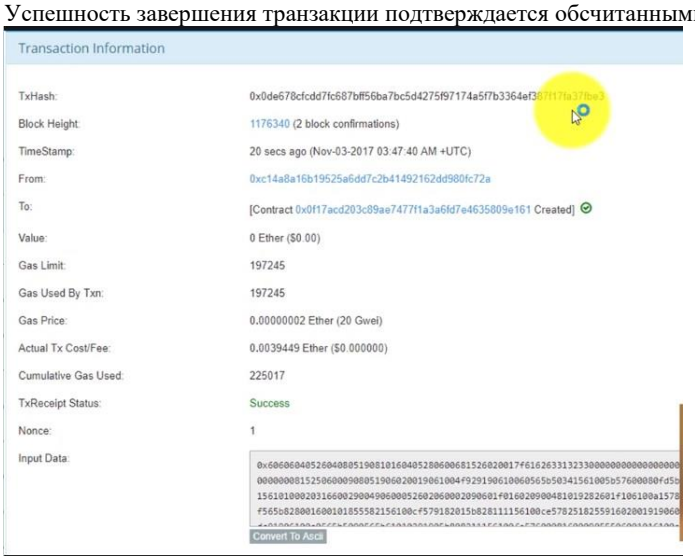
Отследим всю цепочку: контракт, написанный в среде Remix на языке JavaScript, исполняется, надстройка MetaMask отслеживает эту транзакцию и открывает всплывающее окно для подтверждения создания контракта.



Для этой процедуры потребуется израсходовать немного газа. После подтверждения MetaMask отправляет транзакцию в блокчейн.



MetaMask располагает некоторым числом узлов сети, расположенных на серверах разработчиков, которые играют роль посредника между вашим браузером и блокчейном. Если вы хотите создать и использовать свой собственный блокчейн, потребуется один из клиентов: Geth, *Parity*, Mist. Mist обеспечивает интегрированный в *браузер доступ* к блокчейну, а Geth - это работающий на вашем компьютере клиент, загружающий все блоки и предоставляющий к ним непосредственный *доступ*. Успешность завершения транзакции подтверждается обсчитанными блоками.



Основные понятия среды Ethereum

Блокчейн в среде Ethereum очень напоминает блокчейн для Bitcoin. Есть транзакции, есть эфир, подобный биткоину, есть майнеры и так далее. Однако есть и различия. Во-первых, майнеры все еще работают по механизму Proof-of-Work, то есть решают математические задачи по шифрованию данных. Это требует большого количества энергии и вычислительной мощности, а после успешного завершения к блокчейну добавляется новый блок. В скором будущем будет внедрен механизм Proof-of-Stake, который потребует приобретения определенного количества эфира, который будет использоваться для обсчета новых блоков.

Самым большим отличием от блокчейна Bitcoin является возможность размещать приложения непосредственно в блокчейне. Именно этой теме будет посвящен данный раздел.

Приложения с максимальной доступностью

Технология блокчейн подразумевает, что все приложения обладают невероятной устойчивостью и надежностью, поскольку исполняются непосредственно в блокчейне - единый *сервер* отсутствует, код выполняется на всех узлах блокчейна одновременно. Это открывает большие возможности для решения сложных вычислительных задач, а также построения высокораспределенных сред.

Основы работы среды Solidity

Среда Solidity представляет из себя высокоуровневый *язык программирования*. Существуют и другие способы разработки приложений для блокчейна, но общим правилом является необходимость компиляции текста на языке программирования в байткод, который затем размещается в блокчейн посредством транзакции. Такие транзакции очень похожи на используемые в блокчейне Bitcoin, когда вы отправляете биткойны с одного адреса на другой; в среде Ethereum для тех же целей используются единицы эфира. Если есть потребность отправить в блокчейн байткод, то он прикрепляется к транзакции как данные, а в самой транзакции при этом должно быть пустым *поле* получателя *To* - в этом случае блокчейн создаст новый *адрес* для размещения этого байткода.

Практический пример

Например, предположим, что у нас есть *функция ABC*, требующая *параметр* a. Если a меньше 50, *функция* возвращает 10, в противном случае a. *Компилятор* обрабатывает функцию, и в блокчейн отправляется новая транзация со следующими значениями полей: *from* содержит *адрес* отправителя - ваш *адрес*, *поле value* пусто, как и *поле to* (это самый важный момент), а *поле data* содержит байткод из функции, созданной в Solidity. В процессе обсчета транзакции этот код будет добавлен в очередной блок, получит собственный *адрес*, например, *0xabcdef001*, или какой-нибудь другой, и у каждого пользователя сети появится возможность взаимодействовать с этим кодом по заданному адресу.

Важность обсчета кода и учета валюты в одном блокчейне

Блокчейн представляет собой значительно распределенную базу данных. Это означает, что при сохранении в блокчейне какой-либо величины или участка кода их больше нельзя удалить, их доступность крайне высока. Ни какие-либо величины, ни участки кода не доступны из централизованного источника, поэтому никакому правительству не под силу ограничить *доступ* к ним или удалить данные из блокчейна, если только они не выключат все узлы сети по всему миру. Эта концепция напоминает сохраненные процедуры в MySQL, только применимо по отношению к коду. В частности, в среде MySQL вы можете запускать некоторые программы, изменяющие запросы *SELECT* или *RETURN* - аналогично в блокчейне, особенно в Ethereum, с помощью смарт-контрактов можно изменять значения переменных или данные, отправлять валюту и другим образом взаимодействовать с другими смарт-контрактами.

В среде Ethereum и обработка кода, и валютные *операции* проводятся в едином *поле*. Это открывает широкие возможности для различных приложений из областей условного депонирования, краудфандинга, страхового дела, операций с недвижимостью, сферы услуг, юриспруденции и прочих. В настоящее время наблюдается множество проектов, использующих возможности запуска кода в блокчейне и работы с криптовалютой с последующим проведением краудфандинговых кампаний.

Классические примеры распределенных приложений

Приведем несколько примеров распределенных приложений. Начнем с ДАО - демократических автономных организаций. Эта система представляет собой платформу для краудфандинга. Одно время широко обсуждалась в прессе, поскольку разработчики смогли привлечь шестьдесят миллионов долларов США в виде инвестиций. К большому сожалению, она впоследствии была взломана, но оставила значительный след в сознании людей, благодаря ясной логике и новому подходу к краудфандингу, при котором не представлялось возможным собрать средства и сбежать (в отличие, например, от Kickstarter, который тоже принимает средства для разработки новых продуктов, но нет гарантии, что он не обанкротится). В случае с ДАО отсутствует центральное передаточное звено, способное скрыться с деньгами, намеренно, поскольку все договоренности обеспечиваются смарт-контрактами.

Вторым распространенным типом приложений являются решения по обмену валюты. В настоящее время наблюдается всплеск числа ICO, - первичных размещений криптовалюты - реализуемых с помощью токенов стандарта *ERC*, которые можно напрямую обменивать в среде блокчейна, то есть менять токены на эфир или токены на токены, и вся эта логика хранится непосредственно в блокчейне.

Токены - это участки кода, связанные с пользовательскими учетными записями и базами данных и используемые как валюта, баллы в программах лояльности, индикаторы доли в компании, жетоны в играх виртуальной реальности и так далее. Все эти платежные средства учитываются и хранятся в среде блокчейна.

И, наконец, *базы данных*. Снабдив их некоторой логикой, можно вести в блокчейне учет владельцев земельных участков, дипломов об образовании (например, Массачусетский технологический институт выпускал свои сертификаты в

блокчейне), даже законов. В случае использования блокчейна нет необходимости прописывать положения закона в каком-то документе, вместо этого можно задать условия работы смарт-контрактов, сразу разрешая или запрещая какие-то действия в блокчейне. В перспективе можно даже прийти к автоматическому списанию средств со счета, например, в качестве штрафа за неправильную парковку.

Как работает доступ к блокчейну

Для обеспечения доступа к блокчейну используются узлы сети Ethereum, взаимодействующие друг с другом посредством протокола Ethereum. Каждый *узел сети* может обращаться к любому другому. Одним из узлов, доступных для свободной загрузки, является Go-Ethereum. Он, как и остальные реализации, подключается и взаимодействует с сетью посредством протокола Ethereum.

С другой стороны, для выполнения операций в блокчейне можно применять *удаленный вызов процедур* (*Remote Procedure Call, RPC*), запуская файлы *JSON*, созданные на JavaScript.

Удаленный вызов процедур можно реализовать через протокол *HTTP*, что позволяет взаимодействовать пользователям с узлами сети, а самим узлам - друг с другом посредством протокола Ethereum. Важно понять схему: *пользователь* работает с файлами *JSON* для удаленного вызова процедур, а узлы передают эту информацию между собой по протоколу Ethereum. Это напоминает работу в консоли MySQL, когда *пользователь* задает запросы MySQL (в случае с Ethereum отправляются команды для удаленного вызова процедур в формате *JSON*), а узлы сети MySQL обмениваются информацией по протоколу MySQL (в блокчейне узлы взаимодействуют по протоколу Ethereum).

Задание

1. Установить кошелек MetaMask. Подключаемся только к тестовой сети Rinkeby.
2. Откройте несколько счетов (минимум 3).
3. Получите эфир для дальнейшей работы.
4. Распределите полученный эфир между тремя счетами.
5. Ознакомьтесь с возможностями кошелька MetaMask.

Контрольные вопросы

1. Что такое Go-Ethereum?
2. Что такое Web3?
3. Что такое Remix?
4. Что такое Solidity?
5. Что такое MetaMask?
6. Как MetaMask взаимодействует с браузером?
7. Укажите несколько различий сети Ethereum и блокчейна Bitcoin?

Лабораторная работа №3

Знакомство с Remix - web-средой Solidity IDE.

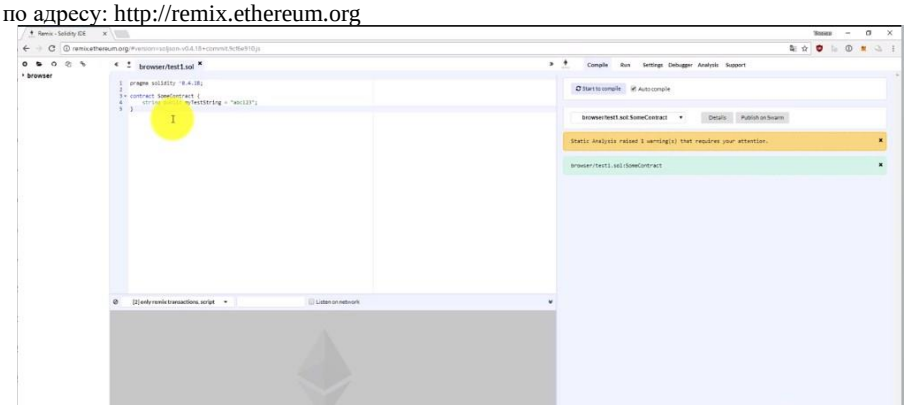
Цель работы: изучить и закрепить на практике возможности среды разработчика смарт-контрактов Remix.

Результат: практические навыки работы с инструментами среды разработчика смарт-контрактов Remix.

Теоретическая справка:

Обзор среды Remix

Откроем Remix по адресу: http://remix.ethereum.org

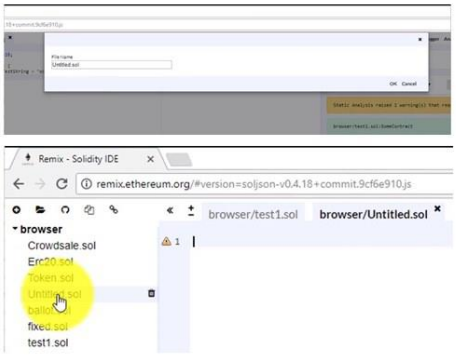


Remix - это интегрированная среда разработки, запускаемая непосредственно в браузере. Она поддерживает весь функционал, обычно ожидаемый от сред разработки, отличается тем, что работает в браузере, а также снабжена механизмом эмуляции блокчейна, в котором можно запускать распределенные приложения или контракты Solidity (смарт-контракты), а также проводить их отладку и тестирование.

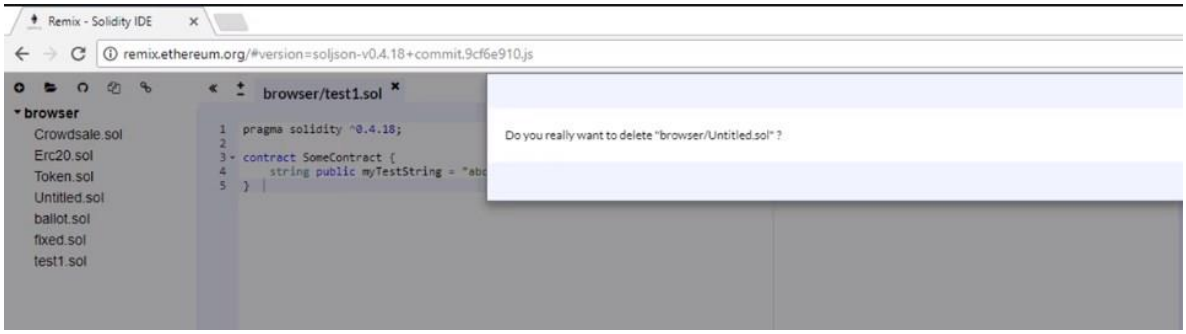
Как добавлять новые и просматривать существующие файлы в среде Remix

Обратимся к левой стороне Remix.

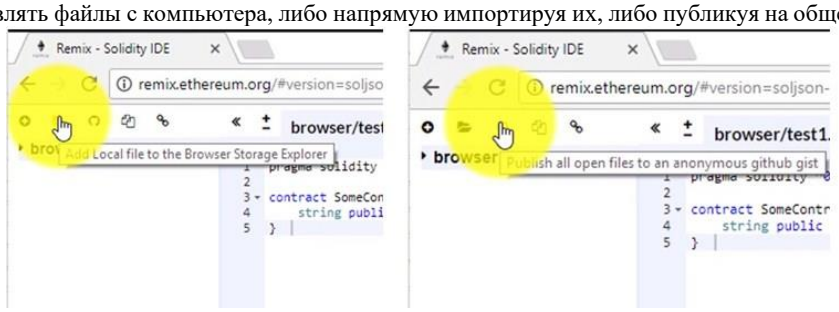
Здесь расположен файловый менеджер, с помощью которого можно создавать новые файлы, переименовывать их, после чего они становятся доступными.



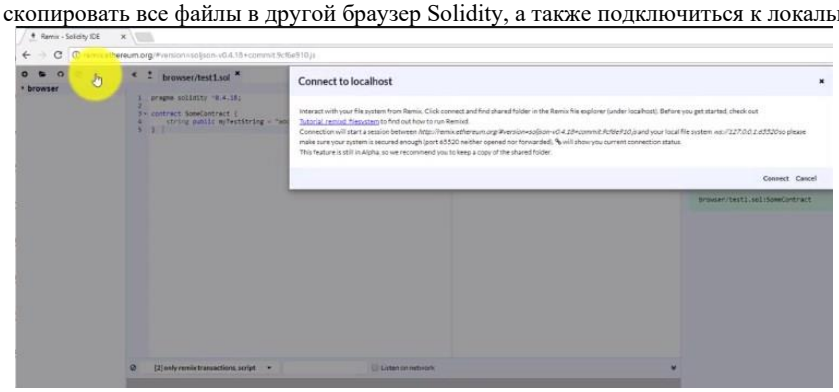
В главном окне после этого можно редактировать файлы. Закроем это окно и удалим файл.



Можно также добавлять файлы с компьютера, либо напрямую импортируя их, либо публикуя на общедоступном ресурсе.

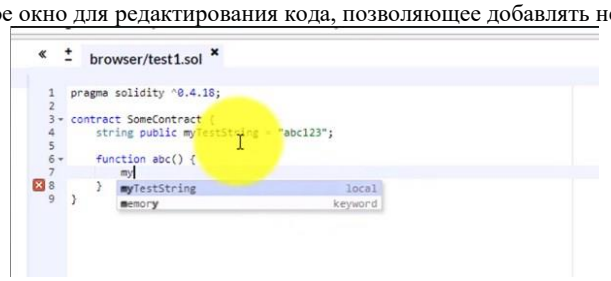


Кроме того, можно скопировать все файлы в другой браузер Solidity, а также подключиться к локальному хосту.



Главное окно редактирования

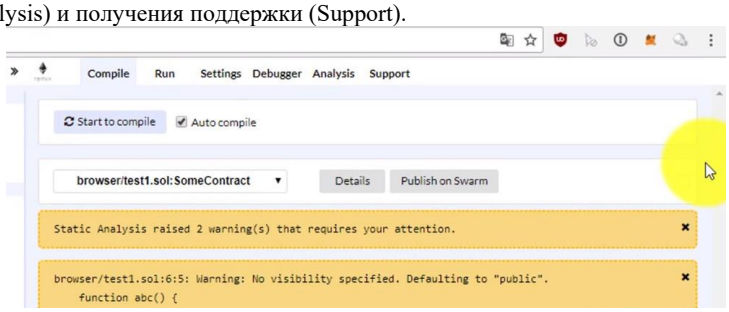
В центре расположено основное окно для редактирования кода, позволяющее добавлять необходимые функции.



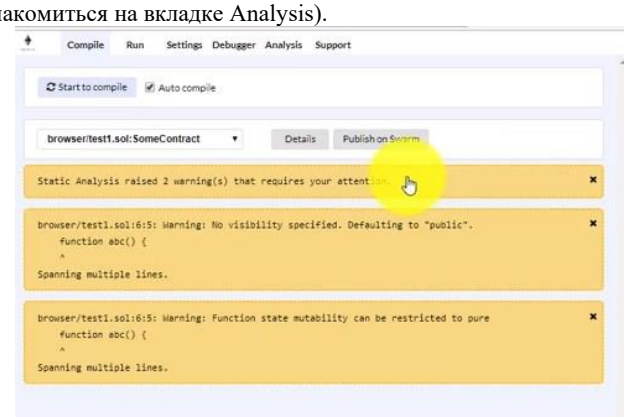
Кроме того, поддерживается функция автоматического дополнения - после набора нескольких символов система предлагает подсказки, например, что *myTestString* - это переменная.

Информация о контрактах на вкладке Compilation

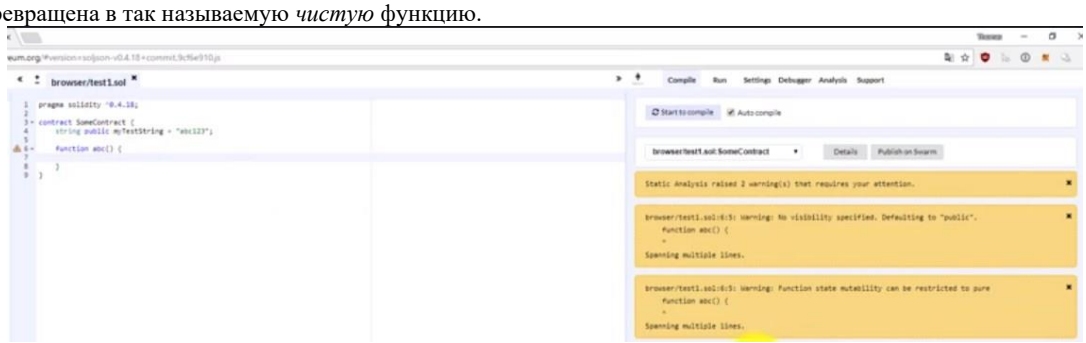
В правой части находятся несколько опций для взаимодействия со смарт-контрактом и получения информации о нем. Сверху расположены вкладки для компиляции (Compile), запуска (Run), изменения настроек (Settings), отладки (Debugger), анализа (Analysis) и получения поддержки (Support).



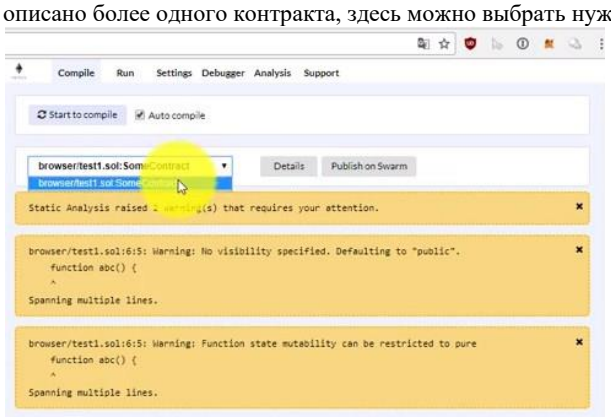
Вкладка Compile. В большинстве случаев при работе в среде Remix действует настройка автоматической компиляции Auto-Compile - код компилируется по мере ввода текста. Чуть ниже приводятся результаты статического анализа кода (подробнее с ними можно ознакомиться на вкладке Analysis).



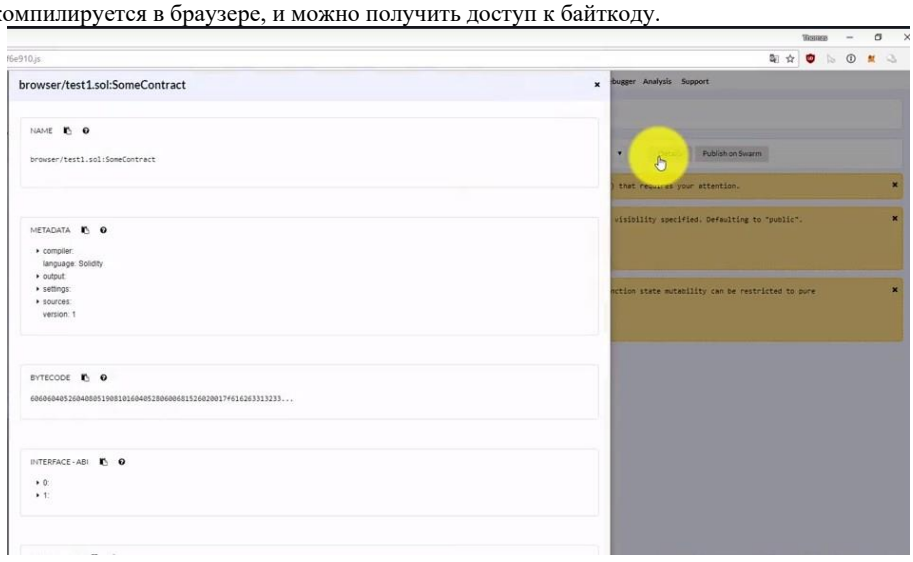
Например, для этой функции не объявлена область видимости, кроме того, она вообще не содержит инструкций и может быть превращена в так называемую *чистую* функцию.



В случае, если в файле Solidity описано более одного контракта, здесь можно выбрать нужный контракт



и получить подробную информацию о нем: название контракта, метаданные, байткод - так что видно, что контракт действительно компилируется в браузере, и можно получить доступ к байткоду.

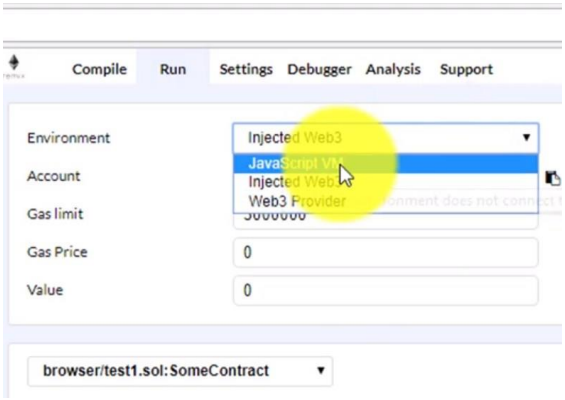


Кроме того, доступен двоичный интерфейс для приложений (API), можно скопировать участок кода в буфер обмена и использовать его для взаимодействия с контрактом посредством Mist или другого веб-кошелька для среды Ethereum.

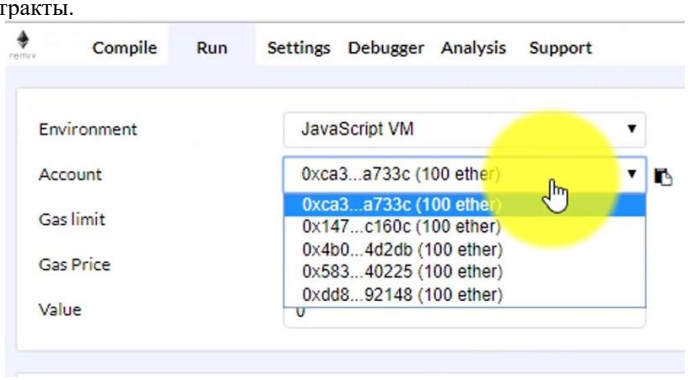
Также можно использовать этот код Web3 для непосредственной отправки контракта в Geth, и просматривать множество других сведений, например, коды операций или исполняемый байткод.

Все, что нужно знать о запуске файлов Solidity в среде Remix

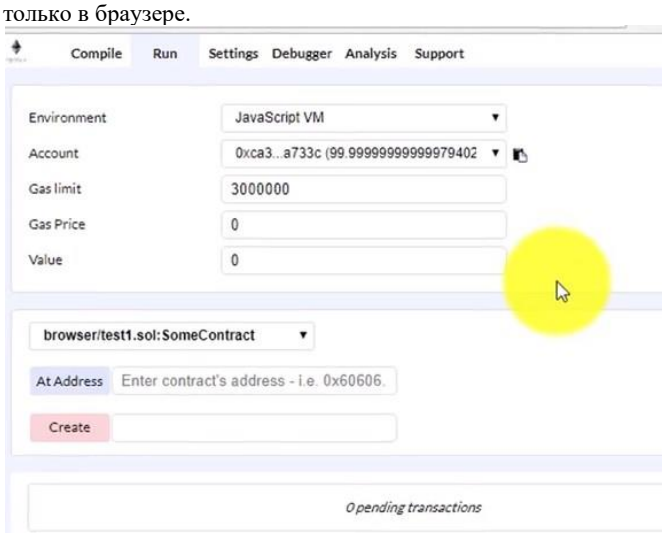
Вкладка Run. Это опция выбора среды запуска; виртуальная машина Java будет обеспечивать эмуляцию среды блокчейна прямо в браузере.



В эмулированной среде можно использовать несколько счетов, с сотней единиц эфира на каждом, и, конечно, создавать, размещать и запускать контракты.

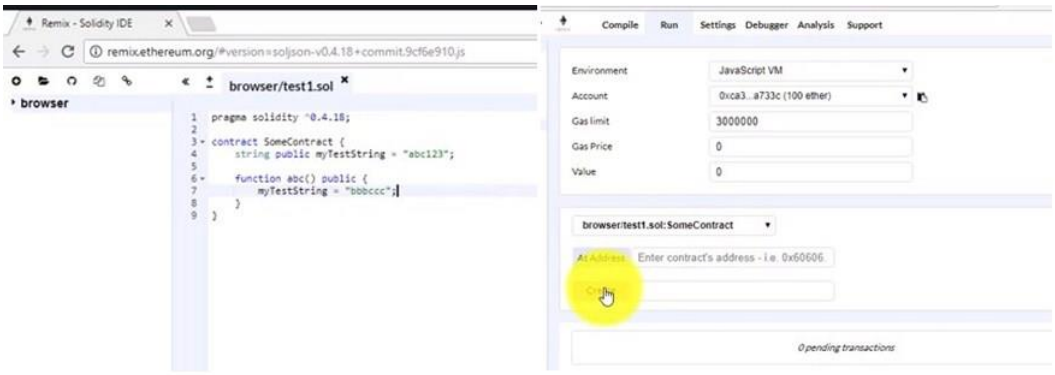


Все они будут работать в эмулированной среде блокчейна, то есть не будет подключения к MetaMask или реальному блокчейну - все происходит только в браузере.

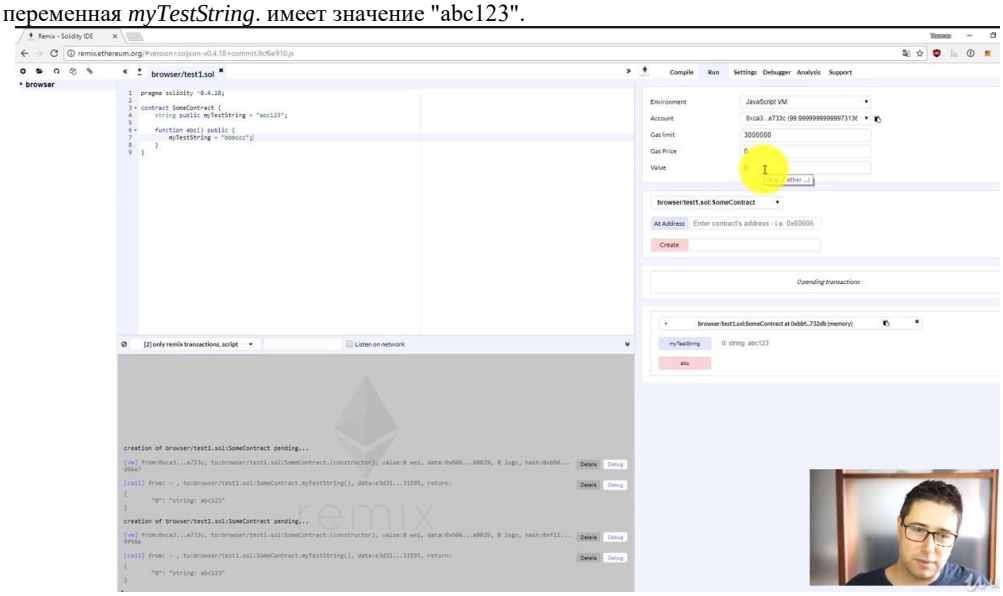


Если закрыть и открыть браузер, вся информация будет потеряна.

Для каждой транзакции, предусмотренной контрактом, можно установить свой предел расхода газа. Например, в функции *abc* (сделаем ее публичной) переменная *myTestString* меняет свое значение с "abc123" на "bbbccc". Теперь опубликуем контракт.



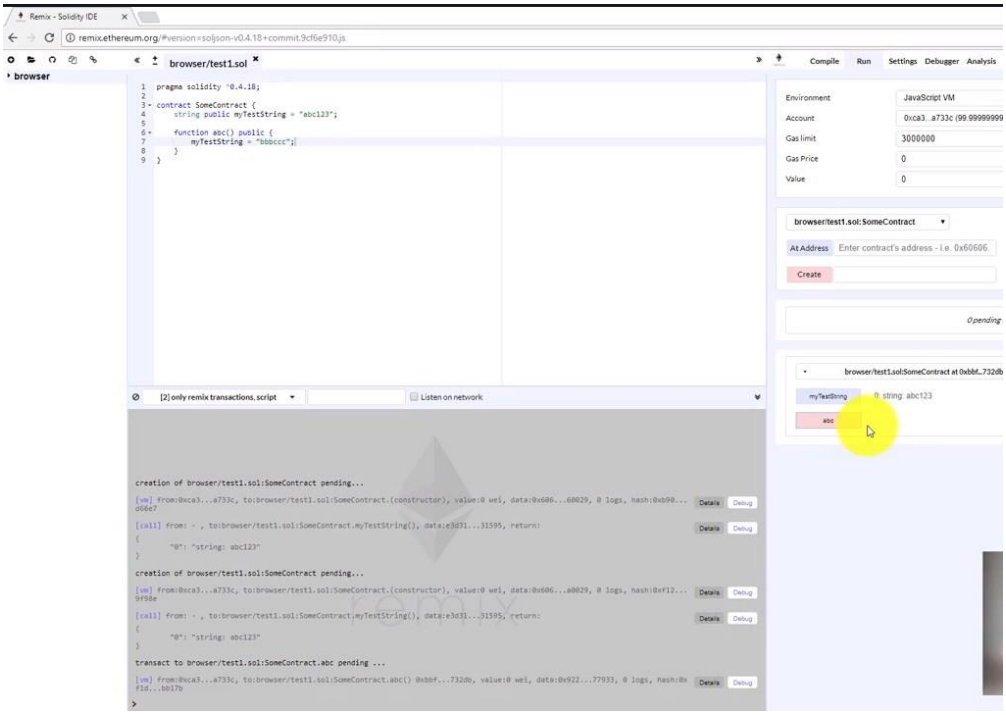
Видно, что переменная *myTestString*. имеет значение "abc123".



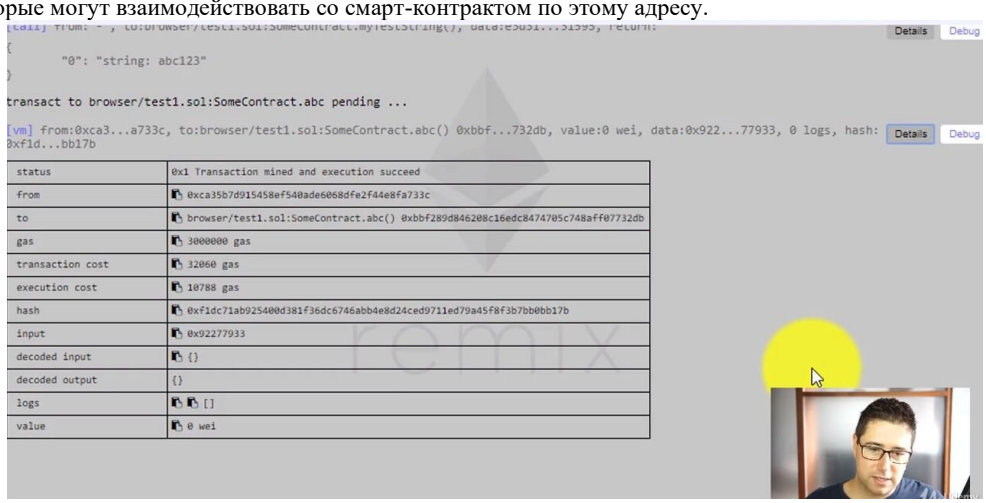
Затем можно вызвать функцию *abc*, щелкнув по ее названию. Для конкретной транзакции можно установить предел расхода газа, цену за единицу газа, а также отправить вместе с транзакцией некоторое количество валюты, например, единицу эфира.

Журнал событий в Remix

Выполним вызов функции. При вызове функции в нижней части окна отображаются все задействованные транзакции.



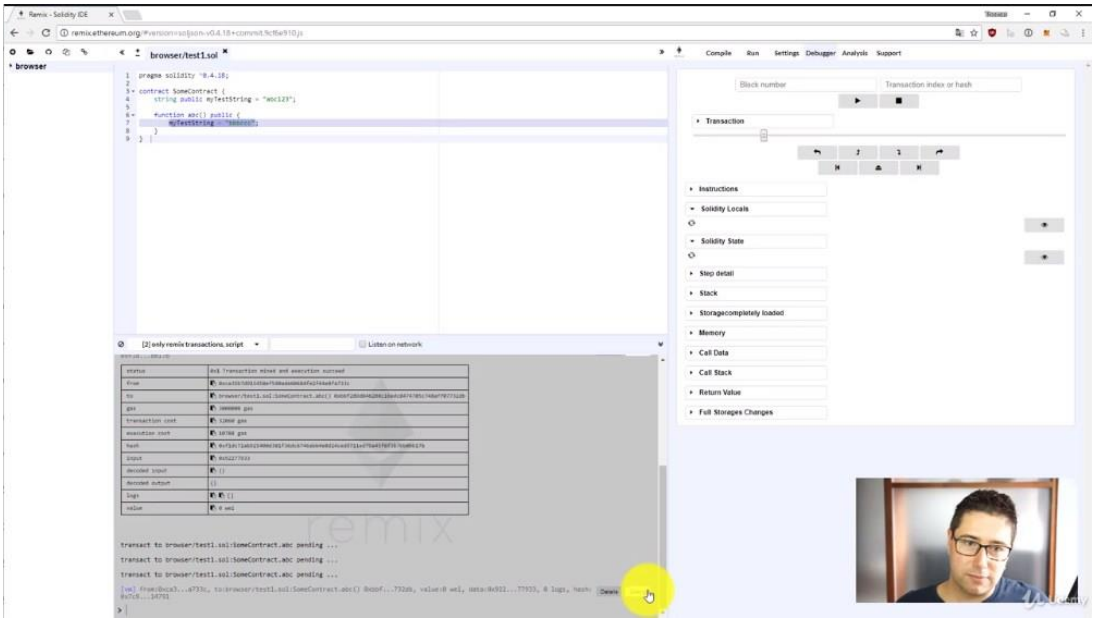
Сейчас транзакция ожидает обсчета, а затем она будет обработана сетью блокчейна. Также можно получить больше информации о транзакции. Для каждой конкретной транзакции можно увидеть, с какого адреса и на какой она была отправлена. Напомним, что сейчас все транзакции выполняются в эмулированной среде блокчейна, и существуют только внутри этого браузера. Можно увидеть установленный предел расхода газа. Также видны отправляемые в транзакции данные, которые могут взаимодействовать со смарт-контрактом по этому адресу.



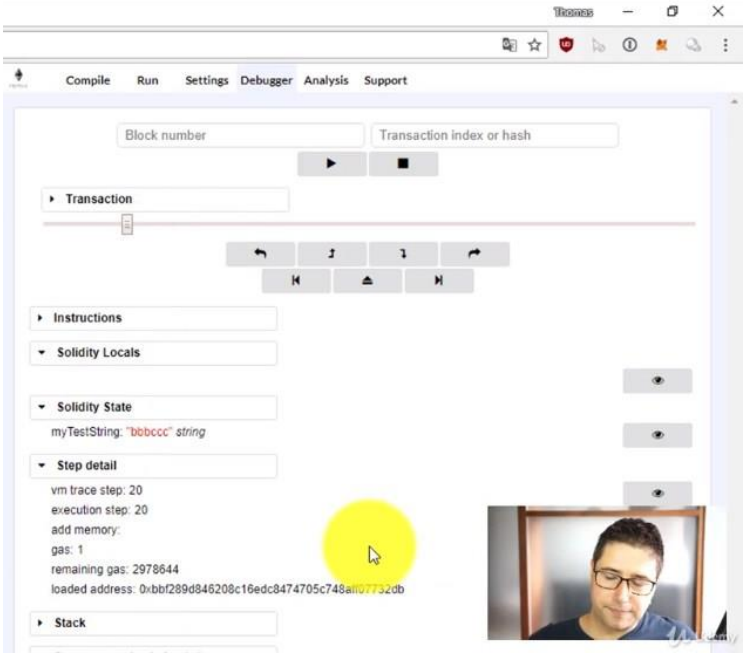
Инструментарий для отладки

В среде Remix отладчик (**вкладка Debugger**) поддерживает последовательную работу по шагам.

Очень удобно иметь отладчик, включенный непосредственно в код. Можно устанавливать точки прерывания или воспользоваться кнопкой отладки, чтобы увидеть, как проходит транзакция после отправки в сеть блокчейна.



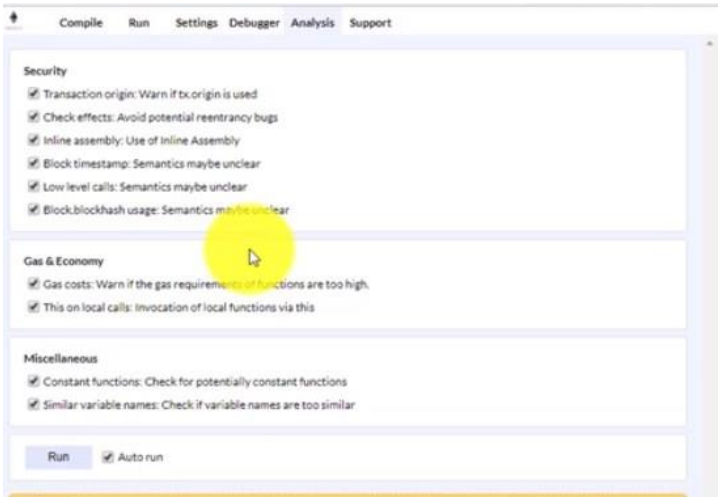
Этот функционал особенно удобен при работе со сложными функциями из большого числа шагов или циклов.



На этапе отладки можно узнать, что последняя операция кода не была выполнена или что кое-где необходимо заменить знак "меньше или равно" знаком "больше или равно" до отправки транзакции в реальный блокчейн.
Таковы типичные случаи применения отладчика. Иногда приходится иметь дело с обработкой исключений, в этих случаях отладчик позволяет быстрее установить участок возникновения исключения.

Краткий обзор инструментов для статического анализа

Вкладка Analysis содержит инструменты статического анализа.

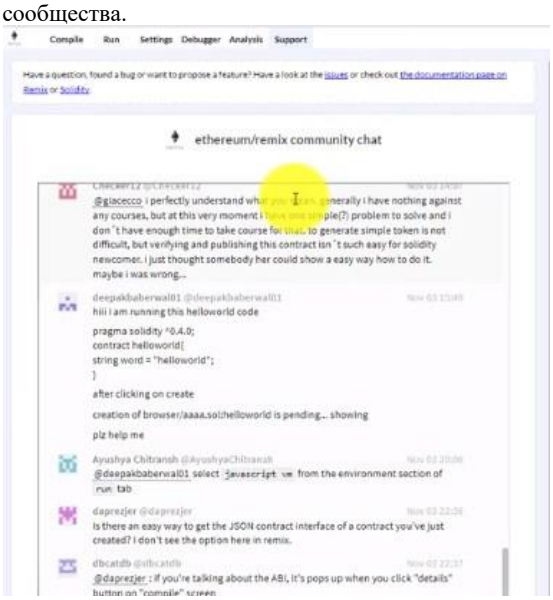


При статическом анализе код просматривается на предмет ошибок описания рабочей среды, и, в случае их нахождения, выводятся предупреждения. Например, для каких-то функций не описаны требования по расходу газа, или объявлены неиспользуемые переменные. В качестве предупреждений могут выводиться сообщения о том, что код использует временную метку блока, например, now, основанную на временной метке блока майнера, вместо временной метки блока из блокчейна.

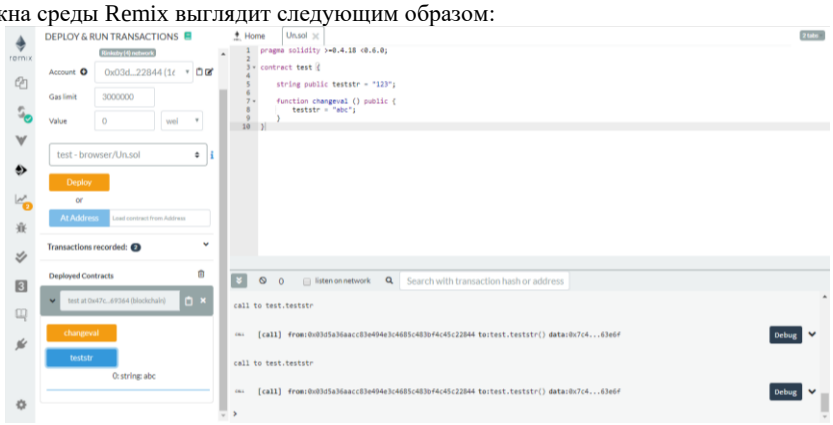
Таковы типичные предупреждения, выдаваемые инструментарием для статического анализа. Если вы уверены в своих действиях, их можно игнорировать, но зачастую они полезны при указании на опечатки или использование циклов, когда без них можно обойтись, поэтому в общем случае статическим анализом не стоит пренебрегать.

Помощь и поддержка

На **вкладке Support** можно найти прямые ссылки на чат сообщества Remix, где можно пообщаться на тему Remix или задать вопросы участникам этого сообщества.



Новый интерфейс окна среды Remix выглядит следующим образом:



Задание

1. Ознакомьтесь с возможностями, режимами работы и инструментами IDE Remix.
2. Для эксперимента используйте следующий простой смарт контракт:

```
pragma solidity >=0.4.18 <0.6.0;

contract test {

   string public teststr = "123";

   function changeval () public {
      teststr = "abc";
   }
}
```

Контрольные вопросы

1. Какие инструменты IDE Remix Вы знаете?
2. Что такое газ в Ethereum и зачем он нужен?
3. Что представляет собой смарт-контракт?