# **ВВЕДЕНИЕ**

В наши дни всю большую популярность набирает разработка нового класса программного обеспечения, носящего название «децентрализованные приложения». Его основы были заложены технологиями Bitcoin и BitTorrent, успех которых вызвал интерес разработчиков к методам их реализации. Последние несколько лет весь мир был взбудоражен резко возросшей популярностью криптовалют, благодаря чему в центре внимания оказалась технология блокчейн. Как выяснилось при более тщательном анализе, сфера её применения не ограничивается только лишь созданием электронных денежных средств и платформ для обмена ими. Одним из перспективных направлений внедрения технологии блокчейн является ее использование в банковском секторе для повышения уровня безопасности операций и сокращения издержек.

Целью курсовой работы является изучение распределённой базы данных блокчейн и возможностей её применения в банковском секторе, а также анализ текущей востребованности технологии и степени её распространения среди российских банков.

Итогом данной курсовой работы будет создание программной реализации простейшей цепочки блоков на языке программирования  
Python 3.

# **1 Технология блокчейн**

## **1.1 Общая информация**

Блокчейн – это распределенная децентрализованная защищенная шифром база данных, в которой каждая совершенная транзакция записывается и становится известна всем участникам сети. Данные о совершенных транзакциях сохраняются в определенном порядке и формируют неизменную последовательность связанных блоков. После этого информация, содержащаяся в блоке, тиражируется и копируется на каждый узел, находящийся в сети. Этот алгоритм обеспечивает устойчивость данной технологии к изменению данных.

Блокчейн обычно управляется при помощи одноранговой (peer-to-peer) сети. После записи, данные в любом блоке не могут быть изменены без полного изменения всех последующих блоков, что требует согласия большинства участников сети.

М. Свон в своей книге «Блокчейн: Схема новой экономики» [1] выделает три вида блокчейн:

а) Блокчейн 1.0 – это криптовалюта. Примерами могут служить Bitcoin, [Ethereum](https://zarabotat-na-sajte.ru/bitcoin/top-perspektivnyh-kriptovalyut.html#ethereum), [Litecoin](https://zarabotat-na-sajte.ru/bitcoin/top-perspektivnyh-kriptovalyut.html#litecoin) и т.д.

б) Блокчейн 2.0 – это умные контракты (smart contracts). Это широкий класс финансовых приложений, реализующих работу с акциями, облигациями, фьючерсами, закладными и многими другими финансовыми активами. Именно этот вид Блокчейн будет рассмотрен в нашей работе.

в) Блокчейн 3.0 – все остальные приложения, основанные на данной технологии и выходящие за рамки финансовой сферы.

## **1.2 Принцип работы блокчейн**

Несмотря на то, что Блокчейн – распределенная система, и каждый участник может проводить транзакцию, не все они равноправны. Участники системы делятся на операторов (майнер/валидатор), проводящих транзакцию, регуляторов сети, отвечающих за регистрацию, и обыкновенных пользователей.

Выделяют несколько основных этапов формирования блоков.

а) Первый шаг – определение транзакции. Отправитель создает транзакцию, в которой содержится информация об адресе получателя, предмете транзакции (сумма средств, товар и т.д.) и криптографическая цифровая подпись, подтверждающая достоверность транзакции и ее правомерность. Узлы сети оповещаются о транзакции и проверяют её достоверность путем дешифрования электронной подписи. Если транзакция проходит проверку, то она встает в режим ожидания на включение в блок.

б) Создание блока. Блоки, содержащие информацию о транзакциях, связываются криптографически и хронологически в «цепочку» с помощью сложных математических алгоритмов. Новые блоки всегда добавляются строго в конец цепочки. Один из узлов сети один раз за определенный интервал времени собирает находящиеся в режиме ожидания транзакции, формирует из них блок и отправляет на подтверждение другим участникам сети на предмет проверки и присоединения к цепочке.

в) Валидация блока. Узлы, ответственные за валидацию блоков, получают просьбу проверить созданный блок. Они запускают повторяющийся процесс, который требует одобрения от других узлов-операторов для того, чтобы признать блок действительным. Процесс шифрования, известный как хеширование, выполняется большим количеством разных компьютеров, работающих в одной сети. Если в результате их расчетов все они получают одинаковый результат, то блоку присваивается уникальная цифровая сигнатура (подпись).

г) Присоединения блока к цепочке. Когда все транзакции в блоке одобряются, новый блок становится присоединенным к общей цепочке. Как только реестр будет обновлён и образован новый блок, он уже больше не может быть изменён. Таким образом подделать его невозможно. К нему можно только добавлять новые записи. Важно учесть то, что реестр обновляется на всех компьютерах в сети одновременно.

## **1.3 Блоки**

Внутренняя структура блока такова: блок включает в себя список транзакций и заголовок (header), который содержит собственный хеш, хеш предыдущего блока, хеш транзакций и дополнительную информацию. Связь между блоками за счет наличия в каждом (за исключением первого) хеша предыдущего означает, что невозможно внести изменения в блок, не изменив всю цепочку с первого блока – нельзя удалить какую-то транзакцию или вставить ее между уже совершенных.

Эти блоки образуют линейную последовательность во времени, и именно отсюда происходит слово «блокчейн». Блоки добавляются в цепочку равномерно – для Эфириума каждые 17 секунд, для Bitcoin – каждые 10 минут.

## **1.4 Умные контракты (smart contracts)**

Когда речь касается финансовых вопросов, современному человеку достаточно тяжело обойтись без посредников в их решении, будь то покупка дома, страхование имущества или приобретение ценной бумаги. Значительно упростить и удешевить эту процедуру могут помочь умные контракты.

Умный контракт – это программный алгоритм, способный выполнять функции бумажного документа. Когда происходит некоторое событие, умный контракт выполняет предопределённые пункты договора, прописанные в нём. Важной особенностью умных контрактов является то, что они находятся не на сервере, а непосредственно в цепочке блоков, а следовательно, имеют надёжную криптографическую защиту.

Умные контракты стали второй ступенью в развитии технологий блокчейн. После успеха Bitcoin появилось множество альтернативных криптовалют, которые в общих чертах копировали его код, но при этом вносили ряд дополнительных возможностей, привлекающих пользователей. Одной из таких функций как раз стали умные контракты. Ярким примером криптовалютного проекта, реализующего эту особенность, может служить Ethereum, созданный нашим соотечественником Виталием Бутериным. На сайте Ethereum подчёркивается, что платформа может быть использована для «кодификации, децентрализации, обеспечения безопасности и торговли практически всем: доменными именами, финансовыми активами, краудфандинга, управления компаниями и интеллектуальной собственностью». У Ethereum есть ряд конкурентов, таких как NEM, Hyperledger Fabric, но «золотым стандартом» в мире смарт-контрактов на сегодняшний день является он.

У умных контрактов есть ряд преимуществ и недостатков.

К плюсам данного изобретения можно отнести надёжность, неизменность, ускорение обмена активами, сокращение издержек за счёт отсутствия третьих лиц при совершении сделок, удобство.

Однако умные контракты имеют определённые риски. Первый   
из них – возможность ошибки программиста, которая приведёт к неверному выполнению условий договора. Помимо этого, умные контракты запускаются при наступлении определённых событий, и их действие нельзя отменить в случае непредвиденных ситуаций, следовательно, они не обладают достаточной гибкостью. Другим недостатком смарт-контрактов является непонимание их принципов работы широкими массами, что существенно ограничивает круг применимости.

## **1.5 Особенности задачи, решаемой технологией блокчейн**

Основная задача, для решения которой применима технология  
 блокчейн – согласование действий участников системы, объединенных одной целью, но лишенных доверия друг к другу.

Среди криптологов уже давно стала классической «задача византийских генералов», которая имеет следующую формулировку: «Византийская армия осаждает город. Генералам необходимо выработать единую стратегию действий, которая приведет к победе, даже если среди них будут предатели, намеренно искажающие информацию о численности своих отрядов и времени наступления». Блокчейн решает эту задачу при помощи механизмов достижения консенсуса.

Данная технология имеет огромный потенциал для тех систем, между участниками которых отсутствует взаимное доверие, т.к. она обеспечивает надёжное хранение персональных данных, делая недоступными изменения в них в целях мошенничества. Более того, блокчейн позволяет совершать различного рода сделки без посредников, что существенно экономит средства и время. Всё это как раз актуально для банковских систем.

## **1.6 Механизмы достижения консенсуса**

Самое ценное звено в технологии блокчейн – это алгоритмы достижения консенсуса, ведь именно они обеспечивают ей надёжность.

Существуют три основных механизма достижения согласования.

а) Доказательство работы (proof of work) – протокол защиты системы. Любой, желающий записать блок в базу данных, должен выполнить определенную сложно вычислимую задачу, построенную на принципе односторонней функции. Процесс вычисления занимает длительный срок, в то время как принимающая сторона быстро проверяет полученный результат. Перед отправкой сообщения к заголовку добавлялась некоторая отметка, подтвердить валидность которой можно только полным перебором. Проверка вычислений на принимающей стороне происходит быстро - за счет однократного вычисления SHA-1 с заранее подготовленной меткой.

На данный момент именно алгоритм доказательства работы заслужил наибольший авторитет среди прочих механизмов создания надёжных систем. Всё дело в том, что именно он способен противостоять «атакам Сивиллы», суть которых заключается в том, что злоумышленник создает множество поддельных участников и таким образом склоняет консенсус в свою сторону. Проведение подобной атаки затрудняет алгоритм доказательства выполнения работы, так как для её выполнения мошеннику придётся затратить колоссальную вычислительную мощность. Также большинство Блокчейнов взимают комиссию за участие в консенсусе, следовательно, «атака Сивиллы» станет очень дорогостоящей операцией. Нередко алгоритм proof-of-work подвергается критике из-за чрезмерной энергозатратности, но пока это единственное средство противостояния вмешательствам в систему подобного рода.

б) Proof-of-stake (доказательство доли) – протокол защиты, альтернативный proof-of-work, в котором необходимо в качестве доказательства подтвердить хранение определенной суммы на счете. С более высокой вероятностью при формировании следующего блока система выберет майнера с большим количеством средств на счете, при этом вероятность этого выбора не зависит от мощности его процессоров. Для того, чтобы подорвать надежность системы один из участников должен собрать в своих руках более 50% всех средств системы, что очень затратно.

Proof-of-stake имеет больше преимуществ по сравнению с proof-of-work. Главное – более низкие временные затраты (нет необходимости в длительных вычислениях), однако это не избавляет от возможных проблем. Также нет доказательств эффективности в защите от рисков, возникающий в криптовалютах.

Два существенных плюса этого протокола - атака на систему стоит очень дорого, и если какой-то участник ее все же проведет, то сам существенно от этого пострадает, поскольку нарушит устойчивость системы. Аргументы против – метод дает мотивацию накапливать средства на отдельных счетах, что ставит под вопрос децентрализацию; в случае образование небольшого числа участников, сосредоточивших в своих руках большинство средств, эта группа может навязать свои условия функционирования системы.

в) Delegated-proof-of-stake – усовершенствованная версия протокола защиты proof-of-stake, специфика которой заключается в том, что блоки порождаются предопределенным множеством пользователей системы   
(101 делегат), которые получают вознаграждение за свою обязанность и наказываются за злонамеренное поведение (такое как участие в двойном расходовании средств). Список пользователей, подходящих для подписания блоков, периодически изменяется в соответствии с определенными правилами; например, в Slasher делегаты избираются исходя из их доли и истории блокчейна. Делегаты могут получать голоса от всех пользователей, сила голоса зависит от доли валюты у голосующего. Delegated-proof-of-stake имеет те же достоинства и недостатки, что и proof-of-stake.

## **2 Блокчейн и банковская сфера**

## **2.1 Общий круг задач, решаемых блокчейн**

Снижение издержек, повышение уровня безопасности и более высокая прозрачность транзакций – три сильных стороны блокчейн. Потребность банков и бизнеса в этих аспектах делает блокчейн привлекательным для специалистов, работающих над разработкой программного обеспечения в данных отраслях.

Сегодня привычным для нас стало осуществление платежей через Сеть. Но в этом процессе часто принимают участие неэффективные, устаревшие системы вроде Automated Clearing House (ACH), в которых все операции выполняются централизованно, что негативно сказывается на скорости работы. Но компьютеры постоянно взаимодействуют и не должны сутками ждать, пока пройдёт платёж, поэтому следующий уровень эволюции электронных денег как раз и открывает для нас блокчейн. Огромным плюсом этой технологии является тот факт, что блокчейн не зависит от централизованной компьютерной архитектуры, что приводит к тому, что выпадение отдельных узлов на нарушит работу всей системы.

Среди современных специалистов, анализирующих возможности применения Блокчейн в банковском секторе, бытует мнение о том, что эта технология способна полностью трансформировать структуру банков, и в скором времени она станет кардинально отличаться от того, с чем мы привыкли иметь дело сегодня. Возможность избежать посредничества третьих лиц в различного рода сделках способна сделать бесполезным огромный пласт банковских услуг. Однако реализация этой задумки далеко не беспрепятственна и имеет огромное количество тонкостей, в которых мы подробно разберемся далее.

## **2.2 Границы применимости технологии blockchain**

Блокчейн, безусловно, привлекательная и очень перспективная технология, но подойдёт не для каждой системы. Существует ряд предпосылок, которые указывают на возможность внедрения блокчейн:

а) использование базы данных с общим доступом;

б) между участниками отсутствует доверие;

в) необходимость в отсутствии посредников;

г) взаимозависимость операций, потребность в создании цепочек.

Однако стоит учитывать, что даже для тех систем, где применима технология блокчейн, её внедрение имеет ряд препятствий, вызываемых самой структурой и принципами технологии. Рассмотрим некоторые из них.

а) Вопросы безопасности и privacy. Несмотря на существование решений в области безопасности с использованием сложных алгоритмов шифрования, проблемы кибербезопасности остаются одними из самых обсуждаемых. Любое программное обеспечение написано человеком, а поэтому несовершенно. Чем больше оно усложняется, тем стремительнее растёт количество уязвимостей. Вдобавок, целостность программного обеспечения и сети фундаментально важны для превращения блокчейна в инфраструктурную технологию. Если блокчейн переплетется со всеми главными финансовыми системами мира, то мощные атаки на него могут привести к катастрофическим последствиям.

б) Вопросы внедрения и интеграции. Когда организация внедряет технологию для модернизации своих бизнес-процессов, она сталкивается с проблемой переноса своих старых данных в новый формат. В данной ситуации внедрение блокчейна ничем не проще других подобных задач, а значит вопрос планирования перехода от текущих систем к блокчейну остается открытым. Сокращение издержек, которые обещает внедрение блокчейна, воодушевляет, однако внедрение потребует высоких первоначальных затрат, которые нельзя не принимать во внимание.

в) Понимание технологии. Один из наибольших операционных рисков заключается в том, что относительно небольшое число людей понимает, как он работает. Если планируется внедрять блокчейн в систему, пользователями которой являются широкие слои населения, то это может привести к неприятным последствиям. Всё дело в том, что блокчейн не защищает от самого популярного вида мошенничества – фишинга, суть которого заключается в краже конфиденциальных данных пользователей. Компрометация ключа может привести к постоянной потере средств, защищенных криптографией. К сожалению, на сегодняшний день далеко не каждый простой пользователь может похвастаться знанием элементарных правил защиты личных данных. Существует возможное решение проблемы кражи личной информации: связать открытые ключи с физической личностью или юридическим лицом, но данный механизм потребует дополнительных затрат.

г) Вопрос скорости выполнения операций. В целях защиты от атаки 51% (когда один участник сети завладевает более чем половиной вычислительной мощности системы) размер блока (на примере Биткоин) остается не более 1 мегабайта, что позволяет поддерживать децентрализацию, но значительно ограничивает скорость транзакций – 3,3 в секунду, в то время как та же Visa проводит 22 тысячи в секунду. Расширение пропускной способности хотя бы до 10 транзакций в секунду потребовало бы увеличение размера блока до 1,6 гигабайт, что, во-первых, вызвало бы проблемы у маломощных майнеров, а, во-вторых, затруднило бы распространение блоков по узлам. Уже сегодня цепочка блоков Bitcoin весит около 38 Гбайт памяти. Если впоследствии появятся Блокчейн системы, которые будут хранить не только информацию о транзакциях, но и другие, более объёмные данные, то их с высокой вероятностью ждёт неудача, так как вынуждая майнеров хранить чужие данные бесплатно, разработчик лишает их стимула поддерживать работу сети, поскольку затраты майнеров станут превышать доходы.

## **2.3 Типы блокчейн-систем**

Блокчейн системы разделяются на два типа: приватные и публичные. В приватных блокчейнах блоки создаются централизованно, и все права на проведение операций принадлежат одной организации. Участники извне могут только следить за транзакциями, в то время как управляют реестром только доверенные узлы.

Приватные Блокчейны имеют ряд достоинств:

а) более низкая стоимость транзакции – достигается за счет того, что валидность проверяется несколькими высокопроизводительными узлами, а не множеством пользовательских устройств, как в публичных блокчейнах;

б) показатель транзакций в секунду значительно выше, чем у публичных блокчейнов;

в) больший контроль над системой со стороны компании;

г) создание блоков в приватном блокчейне зачастую не требует proof-of-work. Имеется установленное число обработчиков транзакций, у каждого есть открытый и секретный ключ. Создатели блоков известны и определяются по цифровой подписи в заголовке.

При этом proof-of-work все же может быть подключен для повышения доверия к системе со стороны внешних участников (если в этом есть необходимость). Без данного проверочного механизма уровень доверия к приватному блокчейну равносилен уровню доверия к организации, которая его создала. С его внедрением конечные пользователи могут полагаться уже на объективные математические законы, которые свидетельствуют о высокой экономической стоимости атаки на систему.

Концепция приватных блокчейнов делает их далёкими от общей концепции децентрализованных приложений.

В публичных блокчейнах любой пользователь может создать блок транзакций – достаточно пройти соответствующий механизм верификации (proof-of-work или proof-of-stake).

Преимущества публичных блокчейнов:

а) обладают важным свойством сетевых эффектов. Взаимосвязь между двумя системами, функционирующими на блокчейне приводит к тому, что пользователь одного с высокой вероятностью станет пользователем второго;

б) разрешается проблема передачи «товаров». В классической системе продавец – покупатель посредник необходим, чтобы гарантировать передачу денег в одном направлении и «товаров» – в другом (за это естественно полагается комиссия). Однако наличие валюты и системы доменных имен позволяет исключить это звено за счет использования смарт-контрактов.

## **2.4 Применение блокчейн российскими банками**

Любая инновация перед внедрением требует тщательного анализа. На сегодняшний день рано говорить о повсеместном использовании технологии распределённых баз данных, отечественные банки пока находятся на стадии её изучения. В первых рядах исследователей – крупные коммерческие банки такие, как «Сбербанк», «Тинькофф», «Альфа» и др.

Первопроходцами в сфере применения блокчейн можно назвать авиакомпании S7 и Альфа-банк. Они создали приватный блокчейн, которым пользуется авиакомпания и агенты-посредники по продаже билетов. Его достоинство в том, что время расчетов посредников с S7 Airlines сократилось в разы.

Не остался в стороне и самый крупный банк России – Сбербанк. С 2014 по 2017 год Сбербанк запустил около 15 различных пилотных проектов, связанных с технологией Блокчейн. Конечно, не все они увенчались успехом, но некоторые дали действительно неплохой результат. Директор проектов Центра технологических инноваций Сбербанка Дмитрий Булычков на конференции ЦИПР Иннополисе в мае 2017 года отметил, что Сбербанк не пытается применить технологию Блокчейн везде. Она используется там, где нужна публичность, peer-to-peer (P2P) сервисы, фиксация и возможность доказательства неизменности информации и т.д.

Примером успешного проекта Сбербанка с использованием Блокчейн может стать распределенный документооборот, позволяющий обмениваться документами в зашифрованном виде посредством технологии распределенного реестра. В середине октября 2016 года Сбербанк и ФАС России запустили пилотный проект Digital Ecosystem по обмену документами на основе технологии блокчейн. В проекте участвуют компании «Аэрофлот», «Русский Уголь», «ФортеИнвест», правда о том какова их роль и подключились ли они уже к документообороту на основе блокчейна, в Сбербанке не комментируют. Данный проект является инфраструктурным, а не коммерческим: он не направлен на получение прибыли, а лишь помогает сократить количество посредников и тем самым упросить внутреннюю структуру организации.

Еще один «взлетевший» проект реализуется компаниями «Сбербанк Факторинг» и «М.Видео». В их взаимодействии была проблема сверки документов о поставках – это достаточно трудоёмкий процесс со множеством подтверждений. Все предыдущие попытки оптимизации этого процесса успехом не увенчались. Однако технология Блокчейн помогла решить эту проблему. В рамках пилотного проекта компании протестировали загрузку реестра поставок, шифрование данных, их последующую проверку и хранение по технологии блокчейн. Из процесса подтверждения поставок был исключен человеческий фактор, что позволило значительно снизить время сделок. Платформа сравнивает захэшированные данные по поставкам: если они совпадают у обоих участников, поставка подтверждается. Такой подход позволил ускорить процесс сверки и исключить риск утечки коммерчески важных данных.

Однако участие далеко не всех заинтересованных в исследовании блокчейн банках сводится к созданию инфраструктурных проектов для собственного пользования. Большинство из них решило принять участие в масштабном совместном проекте под названием «Masterchain». Masterchain – это национальная сеть Российской Федерации на блокчейне, которая создается для передачи ценности и сопутствующих данных между ее участниками. Он разрабатывается Ассоциацией развития финансовых технологий с 2016 года. В [консорциум](https://forklog.com/bank-rossii-obyavil-o-sozdanii-konsortsiuma-finteh/) по разработке данной платформы на первых порах вошли Центробанк, Сбербанк, банк «Открытие», Альфа-банк, «Тинькофф» и Qiwi. Позже к ним добавились ВТБ, Газпромбанк, Национальная система платежных карт, ПАО «АК БАРС» банк, Платежный центр РНКО и Райффайзен Банк. Проект «Мастерчейн» не разрабатывает свой блокчейн, а использует модифицированный код Ethereum. Запуск проекта плвнируется в 2019 году.

Государственный блокчейн соответствует принципам, которые устанавливает закон РФ, и имеет некоторые прерогативы:

а) Персональные данные, коммерческие тайны, документы с грифом секретно не хранятся в «Мастерчейне»,

б) Посредники при работе с системой не нужны (как и на любом блокчейне),

в) Возможность запуска смарт-контрактов (т.к. опирается на Ethereum)

г) Нет единой точки отказа, то есть система не выходит из строя с удалением одного узла в сети.

## **2.5 Правовые аспекты работы блокчейн-систем**

На данный момент в России не существует чётких правовых инструкций относительно блокчейн приложений. Мнение о том, нужны или нет дополнительные законы, регулирующие их работу, разделились на два лагеря. Некоторые эксперты считают, что нормативная фиксация технологии может замедлить её развитие, поэтому в ней нет необходимости. Однако это не исключает, что вместо законодательного регулирования будет разработан и принят отраслевой стандарт технологии. Учитывая, что применение документов по стандартизации [носит добровольный характер](http://docs.pravo.ru/document/view/72416967/?search_query=%D0%A1%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F%2B%D0%B2%2B%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B9%D1%81%D0%BA%D0%BE%D0%B9%2B%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%B8%2B%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D1%8B%D0%B2%D0%B0%D0%B5%D1%82%D1%81%D1%8F%2B%D0%BD%D0%B0%2B%D1%81%D0%BB%D0%B5%D0%B4%D1%83%D1%8E%D1%89%D0%B8%D1%85%2B%D0%BF%D1%80%D0%B8%D0%BD%D1%86%D0%B8%D0%BF%D0%B0%D1%85%3A&from_search=1), разработчики не обязаны присоединяться и внедрять положения стандарта в свои разработки.

Однако есть и исключение: [закон потребует](http://docs.pravo.ru/document/view/72416967/?search_query=%D0%BE%D0%B1%D1%8F%D0%B7%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C%2B%D0%BF%D1%80%D0%B8%D0%BC%D0%B5%D0%BD%D0%B5%D0%BD%D0%B8%D1%8F%2B%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D0%BE%D0%B2%2B%D0%BF%D0%BE%2B%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D0%B8%2B%D0%B2%2B%D0%BE%D1%82%D0%BD%D0%BE%D1%88%D0%B5%D0%BD%D0%B8%D0%B8%2B%D0%BE%D0%B1%D1%8A%D0%B5%D0%BA%D1%82%D0%BE%D0%B2%2B%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D0%B8%2C%2B%D0%BF%D1%80%D0%B5%D0%B4%D1%83%D1%81%D0%BC%D0%BE%D1%82%D1%80%D0%B5%D0%BD%D0%BD%D1%8B%D1%85%2B%D1%81%D1%82%D0%B0%D1%82%D1%8C%D0%B5%D0%B9%2B6&from_search=1) обязательное применение стандартов: в отношении оборонной продукции, работ по государственному оборонному заказу, государственной тайны иной охраняемой законом информации ограниченного доступа, а также разработок в области использования атомной энергии. В отношении блокчейн-продуктов, задействующих в своей работе охраняемую законом информацию уже существуют ограничения. Продукты, созданные на основе технологии блокчейн, подпадают под определение [информационных систем](http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=200126&dst=0&profile=0&mb=LAW&div=LAW&BASENODE=&SORTTYPE=0&rnd=261745.2029925543&ts=1645082640044988385769101424&SEARCHPLUS=%D4%E5%E4%E5%F0%E0%EB%FC%ED%FB%E9%20%E7%E0%EA%EE%ED%20%EE%F2%2027.07.2006%20N%20149-%D4%C7%20%28%F0%E5%E4.%20%EE%F2%2019.12.2016%29%20%22%CE%E1%20%E8%ED%F4%EE%F0%EC%E0%F6%E8%E8%2C%20%E8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%ED%FB%F5%20%F2%E5%F5%ED%EE%EB%EE%E3%E8%FF%F5%20%E8%20%EE%20%E7%E0%F9%E8%F2%E5%20%E8%ED%F4%EE%F0%EC%E0%F6%E8%E8%22&SRD=true#0), что означает распространение на них норм [Федерального закона](http://www.consultant.ru/document/cons_doc_LAW_61798/) "Об информации, информационных технологиях и о защите информации".

Особенного внимания в области правового регулирования заслуживают смарт-контракты. Одной из основных причин этому служит тот факт, что сторонами могут быть только лица, наделенные правовой дееспособностью, поэтому автоматизированные механизмы не могут быть самостоятельными субъектами экономической деятельности и совершать сделки. То есть внедрение смарт-контрактов должно учитывать, что сделки заключаются от имени владельца оборудования посредством передачи данных от техники.

Другим аспектом является то, что юридические издержки, которых с помощью смарт контракта можно избежать на этапе исполнения, могут перейти к этапу составления проекта. Стороны, скорее всего, захотят указать более подробный ряд нештатных ситуаций и результатов до того, как будут обязаны выполнять решения программно-управляемых контрактов, а следовательно, появится необходимость в транзакционных адвокатах.

Возможность взаимодействия взаимно недоверчивых сторон в сделках помимо очевидных достоинств имеет также ряд недостатков. К примеру, она может послужить толчком для создания новых подпольных рынков, на которых злоумышленники могли бы нанимать хакеров, убийц или террористов для совершения преступных действий. Как только контракт получит подтверждение того, что работа завершена – например, путем автоматического сканирования средств массовой информации на предмет сообщений о противозаконном акте − он предоставит средства преступникам.

Не стоит забывать и про возможность кражи криптографических ключей и другой конфиденциальной информации.

Хотя блокчейн имеет огромные перспективы, но перед тем, как окончательно прижиться в России, она, скорее всего, создаст проблемы юристам, политикам и компьютерным ученым на длительный срок.

# **3 Программная реализация**

## **3.1 Постановка задачи**

Программной реализацией является простейший блокчейн, который реализует функции вычисления хэша предыдущего блока, создания нового блока и добавления его в цепочку блоков, а также проверку целостности цепочки блоков. Конечно, основная сложность создания блока в блокчейн системе – это реализация алгоритма proof-of-work. Однако на данный момент эта задача является трудно реализуемой, но по крайней мере, будет показана общая структура построения цепочки блоков.

Идея состоит в том, чтобы создать последовательность транзакций, блок каждой из которых будет содержать имя отправителя, сумму перевода, имя получателя и хэш предыдущего блока.

Сначала создается первый блок в цепочке, так называемый генезис блок (genesis block). После этого вслед за ним записываются другие блоки, причём перед добавлением для каждого из них вычисляется хеш предыдущего блока.

Также реализована процедура проверки целостности блоков. Суть её работы заключается в следующем: для каждого из блоков, начиная со второго, определяется предыдущий блок, для предыдущего блока вычисляется хеш и сравнивается с полем «hash» текущего блока. Если они совпадают, то блок успешно проходит проверку на целостность.

Алгоритмы хеширования имеют различную надёжность. Во многом степень доверия к блокчейну определяется выбором алгоритма хеширования. В приведённой программной реализации был использован алгоритм SHA-1. Стоит отметить, что существуют другие, не менее популярные алгоритмы, к примеру, SHA-2, SHA-256 (используется в Bitcoin), MD5, которые могут использоваться для аналогичных целей. Однако высоконадёжные алгоритмы затрачивают на работу куда большее время, а в данном примере в их использовании нет смысла, поэтому и был выбран алгоритм SHA-1.

## **3.2 Выбор языка программирования**

Для написания данного проекта была выбрана версия языка   
Python 3.7.1. Его удобство заключается в том, что в нём имеется ряд библиотек для реализации основных функций блокчейна. К примеру, хеширование блоков осуществлялось при помощи библиотеки hashlib. А саму структуру блоков было выгодно задавать как json-объекты для чего была использована библиотека json. Ниже приведён код программы (рис 1, 2):