Правительство Российской Федерации

Федеральное государственное автономное образовательное

учреждение высшего образования   
"Национальный исследовательский университет   
"Высшая школа экономики"

Московский институт электроники и математики им. А. Н. Тихонова

Департамент прикладной математики

ОТЧЕТ

по курсовой работе по дисциплине

«Организационное и правовое обеспечение

информационной безопасности»

Выполнил студент гр. СКБ171

Астраханцев Роман Геннадьевич

Тема работы: **«Технология «Блокчейн» – основа безопасной экономики, история вопроса, основные идеи, цели и задачи, возможности применения, смарт-контракты»**

Москва, 2019 г.

Оглавление

[Введение 3](#_Toc10093812)

[Глава 1. Технологические основы технологии «Блокчейн» 4](#_Toc10093813)

[**1.1. История вопроса** 4](#_Toc10093814)

[**1.2. Принцип работы** 6](#_Toc10093815)

[**1.3. Алгоритмы в блокчейн сетях** 9](#_Toc10093816)

[Глава 2. Смарт-контракты и коллективное инвестирование 14](#_Toc10093817)

[***2.1. Понятие смарт-контракта, особенности, принципы работы*** 14](#_Toc10093818)

[**2.2 Смарт-контракты и ICO.** 16](#_Toc10093819)

[Глава 3. Прикладное применение технологии «Блокчейн» 17](#_Toc10093820)

[**3.1. Основные элементы и сферы применения технологии «Блокчейн»** 17](#_Toc10093821)

[**3.2. Блокчейн структуры в финансовой сфере** 19](#_Toc10093822)

[**3.3. Будущее технологии распределенных реестров** 20](#_Toc10093823)

[**Заключение** 21](#_Toc10093824)

[Список литературы 22](#_Toc10093825)

[Приложения 25](#_Toc10093826)

# **Введение**

В работе рассмотрено историческое развитие блокчейна, изучен её правовой статус и статус проектов, её использующих. Выявлены проблемы, которые призван решать блокчейн, его технологическое устройство, а также потенциальные угрозы на распределённый реестр и современные методы борьбы с ними.

Автором проанализированы сферы применения блокчейна и вопросы, которые он призван упросить в этих сферах. Выделены возможности применения блокчейна в экономической сфере, и спрогнозировано будущее этой технологии.

**Актуальность** этой работы заключена в большом интересе государственных структур, банков и крупных организаций к технологии «Блокчейн». Её экономический потенциал проявляется в возможности бес посреднических международных переводах, безопасности и гарантии верности совершённых транзакций.

**Объектом** исследования является технология «Блокчейн» и её применение в экономике.

**Предметом** исследования курсовой работы является правовой статус блокчейна, механизм достижения распределённой сетью консенсуса, а также потенциал использования в финансовой и других сферах.

**Целью** работы является изучить технологическую основу блокчейна и задачи, который он призван решать, и сделать вывод о возможностях его применения в экономике и других областях. А также сравнить отношение разных стран к криптовалютам и подытожить мировой статус криптовалют.

# **Глава 1. Технологические основы технологии «Блокчейн»**

## **1.1. История вопроса**

Не за долго до появления электронных денег обострилась проблема двойных трат – возможность использования одних и тех же электронных активов дважды, – ставшая единственным препятствием в создании цифровой валюты. Скорым её решением стала централизация платёжных систем, или создание удостоверяющего центра для проверки транзакций. Данное решение остаётся доминирующим и в 2019 году, и проблемой на данный момент является требование от пользователей той или иной платёжной системы большого уровня доверия к самой платёжной системе. К счастью, уже существуют системы свободные от посредника, основанные на блокчейне.

Идея этой технологии зародилась ещё в 1991 году, когда ученые-исследователи Стюарт Хабер и У. Скотт Шторнетта внедрили вычислительно-практическое решение для цифровых документов с штампом времени, чтобы предотвратить отложенную подпись или их подделку[1].

В 2008 году пользователь, называющий себя Сатоши Накамото, опубликовал файл с описанием протокола и принципом работы платёжной системы в виде децентрализованной сети, известной в дальнейшем как Биткоин[2]. Данная система использовала технологию «Блокчейн» для проведения транзакции между пользователями. Именно благодаря этой платёжной системе блокчейн получил распространение в массах и показал возможность создания распределённой платёжной системы без контролирующего центра, основываясь только на криптографических протоколах.

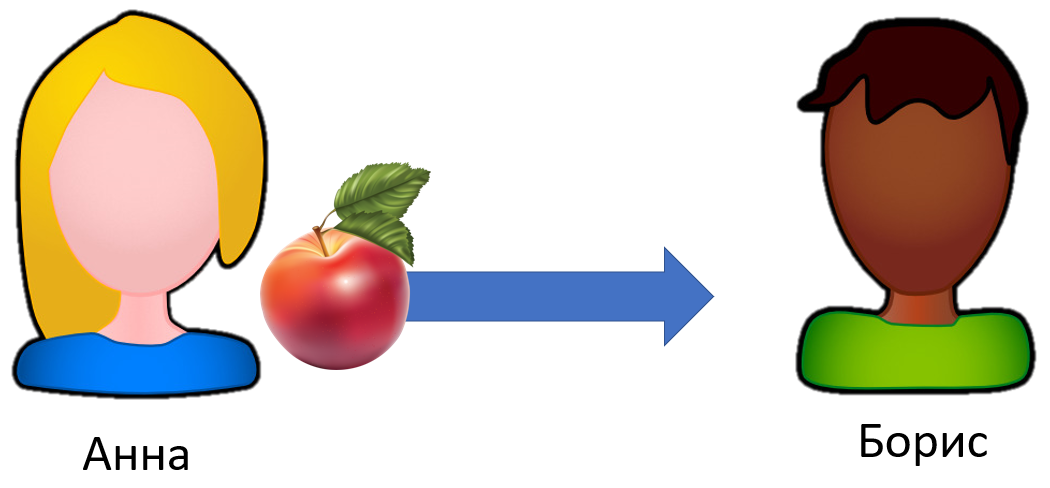
Продолжением идеи Биткоина послужила криптовалюта Эфириум, которая была запущена в 2015 году. Революционной идеей этой криптовалюты было наличие смарт-контрактов – произвольных программ, выполняющихся в самом блокчейне криптовалюты. Это послужило развитию ICO проектов и росту доверия к ним[3]. Более подробно исторические ступени развития технологии «Блокчейн» изложены в виде инфографики в приложении на стр. 1

В настоящее время эта технология нашла своё применение не только в сфере финансов, как протокол обмена криптовалютой, но и в земельных реестрах, удостоверении личности и даже электронном голосовании.

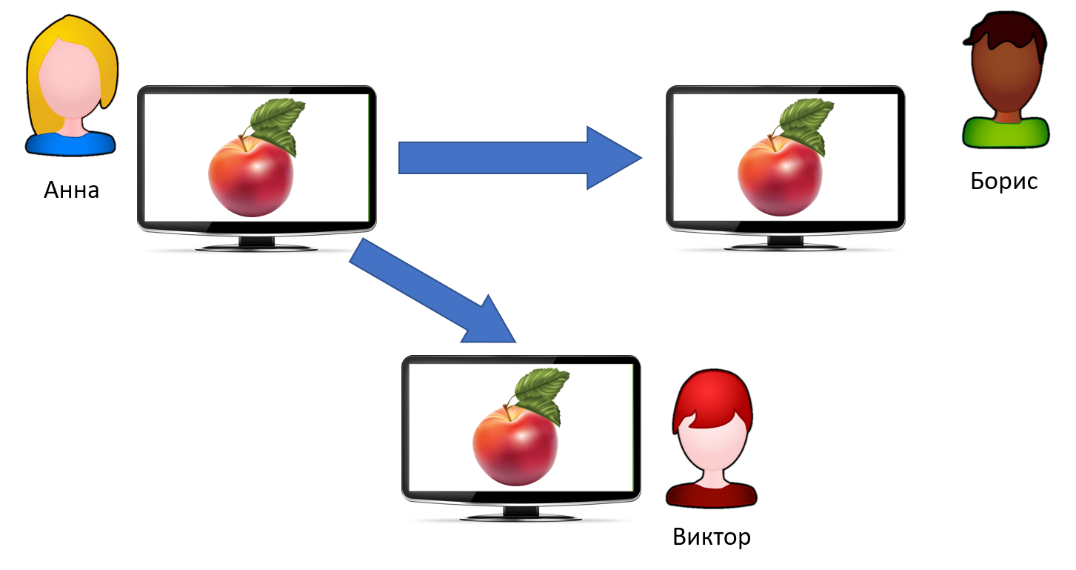
Кроме того, остаётся открытым вопрос правового статуса криптовалюты в мировом масштабе. Каждая страна по-своему определяет к какому правовому полю относятся криптовалюты. Например, по классификации Всемирного Банка США биткоин является «виртуальной валютой»[4], а Народный банк Китая вообще запретил проведение операции с биткоинами всем финансовым компаниям[5]. В России ещё до конца не понятно, чем же является криптовалюта, поскольку были случаи признания её имуществом[6], однако Банк России не признаёт криптовалюту, как законное платёжное средство[7].

## **1.2. Принцип работы**

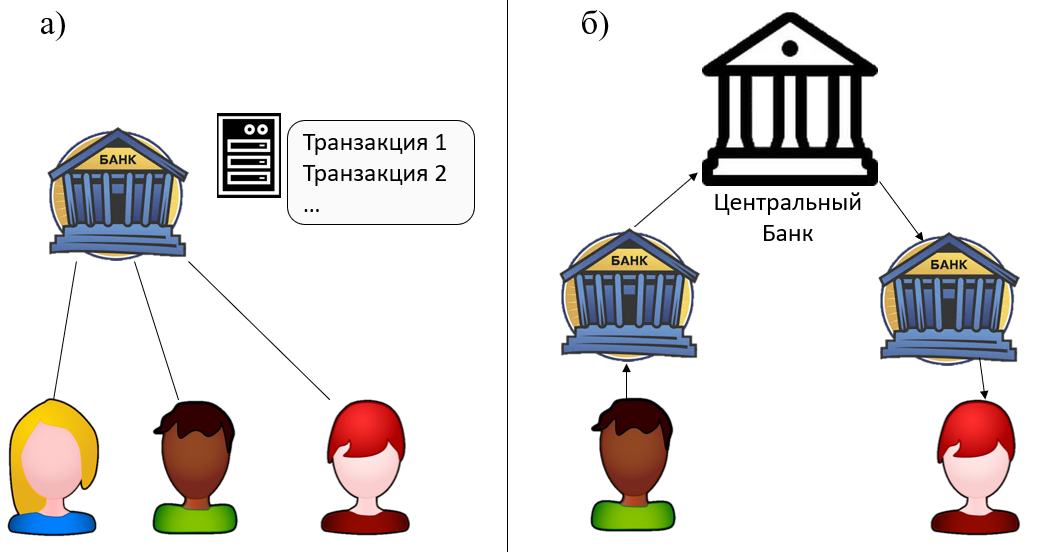
Как было указано ранее, блокчейн решает проблему двойных трат без участия посредника. Рассмотрим подробнее эту проблему и её решения. Процесс обмена ценностями или обязательствами в реальном и виртуальном мире отличается. Так, физическая передача яблока от Анны к Борису уже подтверждает невозможность передачи этого же яблока от Анны к кому-либо ещё (рис. 1). Точно такая же аналогия проводится и наличными деньгами: физически невозможно передать одну и ту же купюру двум разным людям.

 **Рис 1.** Передача *реальных* ценностей от Анны к Борису.

В цифровом мире ситуация кардинально другая: все объекты представляются в виде информации. В этом случае у Бориса нет никаких гарантий, что полученная им информация от Анны была удалена на её вычислительной машине и тем более не была передана некому Виктору (рис. 2). Это и есть проблема двойной траты, которая возникает не только в цифровом мире, но и при операциях с недвижимостью[8].

 **Рис 2.** Передача ценностей в цифровом пространстве. Пример двойных трат.

Решение этой проблемы большинством современных платёжных систем легко показать на примере банковской системы. Каждый участник имеет некий платёжный счёт, информация о котором хранится в банке. Транзакции электронных валют между клиентами одного банка регулируются его серверами (рис. 3a). Одним из способов перевода средств между клиентами разных банков может послужить согласование операции с ещё одним регулирующим центром, а именно Центральным Банком (рис. 3б). Либо же между банками может быть соглашение о согласовании транзакций между их клиентами.



**Рис 3.** Решение проблемы двойных трат на примере банковской системы:а) контролирование транзакций на серверах банка; б) пример проведения операции между пользователями разных банков через Центральный Банк.

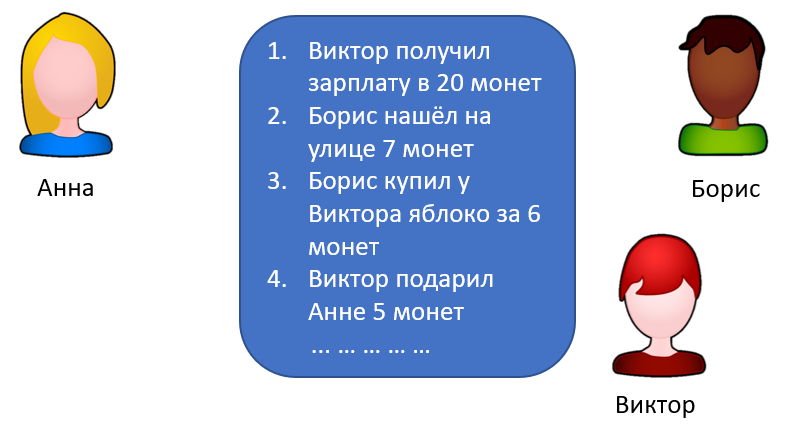
Такая система требует большого доверия пользователей к платёжной системе, потому что ненароком может произойти сбой, или случайно может добавиться или убавиться цифра на счете. Иными словами, деньги клиентов не находятся в их полном контроле.

Решением этой проблемы стала идея создания блокчейна – **распределённой базы данных, изменения в котором согласуются всеми участниками сети, выступающих в качестве коллективного нотариуса, подтверждающего истинность информации в базе данных**. Другими словами, создание единой бухгалтерской книги, хранящейся сразу у всех участников сети, имеющей ряд ухищрений для полноценной реализации идеи.

Под хитростями стоит понимать решения для масштабирования системы, определение способа подтверждения возможности приобрести то или иное благо, а также согласования проведения транзакций, то есть внесения изменений в распределённую бухгалтерскую книгу.

Записи в этом распределённом реестре решают проблему двойных трат непосредственно: они показывают откуда были получены деньги и были ли они уже потрачены или нет. Иными словами, для проведения операции уже знакомый нам Борис знает, что Анна получила свои условные 5 монет от Виктора и ещё их не потратила (рис. 4). Точно так же можно посмотреть, откуда у Виктора появились эти деньги, и раскрутить всю цепочку.

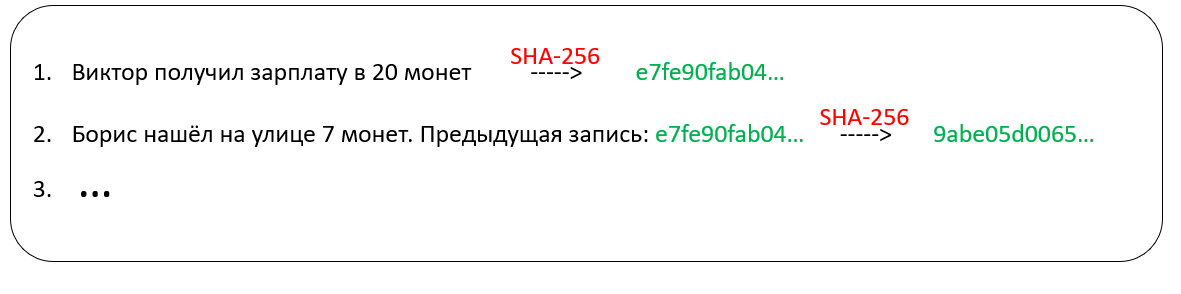
Для согласования изменений в реестре с большим числом участников пользователям предоставляется возможность решения некоторого криптографического уравнения, за решение которого участник получает награду, а все согласованные изменения вступают в силу. Такое решение поощряет участников заниматься поиском решений такого уравнения и проведению транзакций.

  **Рис 4.** Пример распределённого реестра, который демонстрирует возможность проверки валидности денег у каждого из участников при совершении транзакции (в данном случае от Виктора к Анне).

## **1.3. Алгоритмы в блокчейн сетях**

Как уже было упомянуто выше, в распределённой сети используются ряд специальных алгоритмов для нормальной работы сети. Все они имеют своё название и назначение. Самыми известными и распространёнными из них являются Proof-of-Work и Proof-of-Stake, однако меньшей популярностью пользуются Proof-of-Burn, Proof-of-Authority, а также модификации всех предыдущих алгоритмов, например Leased, Proof-of-Stake или Proof-of-Capacity[9].

Для начала стоит прояснить алгоритм формирования самой цепочки в блокчейне. Каждая транзакция должна иметь ссылку на предыдущую для подтверждения валидности транзакции, кроме того, нужно подобрать такую ссылку, чтобы нельзя было подменить какую-то транзакцию в прошлом на другую, удобную злоумышленнику. На помощь в этой проблеме приходит идея взятие хеш-функции – **функции, которая преобразует любой входной параметр в строку фиксированной длинны** – от записи предыдущей транзакции и повторение этой процедуры в каждой новой, тем самым создавая связный список (рис. 5). Нужно пояснить, что для надёжной защиты информации истории транзакций следует использовать криптографическую хеш-функцию – стойкую к коллизиям. Примером такой функции служит SHA-256. Используя атаку «дней рождения»[10] потребуется примерно 2130 операций для нахождения коллизии этой хеш-функции.

  
**Рис. 5.** Пример построения истории транзакций, в которой последующие записи зависят от всех предыдущих.

Вторым этапом в понимании работы блокчейн сети является механизм подтверждения той или иной транзакции. По распределённой сети информация распространяется последовательно, а не сразу, поэтому если некий участник утверждает, что была совершена та или иная транзакция, становится непонятно, правда ли она была проведена или это проказы злоумышленников. То есть, например, как Виктору доказать Борису, что именно он подарил Анне 5 монет, а не сама Анна решила попроказничать. Этот вопрос решается электронной цифровой подписью[11], которая подразумевает под собой генерацию закрытого и открытого ключа и использования их для подтверждения авторства транзакции. Стоит отметить, что неким аналогом адреса получателя будет являться его открытый ключ.

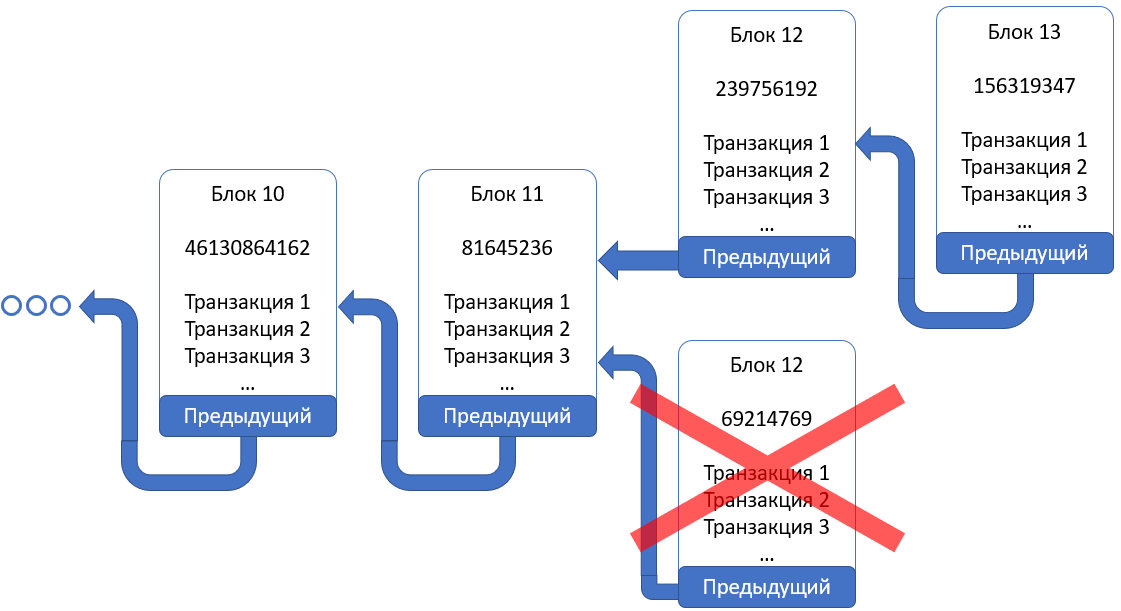
К сожалению, этих деталей ещё недостаточно для создания полностью функционирующей децентрализованной платёжной системы, потому что всё ещё возможна двойная трата. В модели, использующей только описанные выше механизмы, Анна может сказать Виктору, что тратит свои 5 монет на покупку конфеты, а Борису – на покупку яблока. В этом случае и Виктор, и Борис будут распространять эту информацию дальше по сети до тех пока, пока кто-то не получит оба этих сообщения. У этого пользователя нет возможности убедиться, какая транзакция была раньше. Для предотвращения этой проблемы была придумана концепция Proof-of-work.

Proof-of-Work– **это алгоритм создания новых транзакций, объединённых в специальный блок, основанный на подборе случайного числа такого, чтобы хеш от этого числа и всего блока был в определённом числовом диапазоне**. Блоком в данном случае называют несколько неподтверждённых, объединённых в дерево Меркла[12]. Обычно для стимуляции участников сети за нахождение новых блоков полагается награда. В случае с Биткоином хеш должен начинаться с 10 нулей, а награда за нахождение блока сокращается каждые 4 года с момента создания Биткоина и на 2019 год награда составляет 12.5 биткоинов[13] (примерно 6 млн. рублей на Май 2019). Такое требование позволяет проводить находить блоки в среднем раз в 10 минут и в целом гарантировать однозначное трактование проведение транзакций.

Однако данный алгоритм не гарантирует прекращение одновременного появления двух новых блоков, ссылающихся на один и тот же корень, он просто максимально уменьшает возможность возникновения такой ситуации. Но всё же возможность её остаётся и для понимания, какая же из веток развилки является релевантной, было принято соглашение принимать самую длинную цепочку как единственно верную. Правда транзакции, совершённые в короткой ветке, не признаются совершёнными (рис. 6). Такая система гарантирует защиту от двойных трат, однако уязвима к «атаке 51%», о которой будет рассказано позже, и становится непонятным как быть с вознаграждением за поиск блоков, а также в какой момент можно считать транзакцию совершенной. Точного ответа на эти вопросы нет, но по вероятностным соображениям были придуманы две рекомендации. Первая гласит, что вознаграждением за блок стоит пользоваться не раньше, чем через 20 новых подтверждённых блоков, что в переводе на время примерно составляет 3 часа. Вторая гласит, что результаты транзакции нужно считать валидными только через 1-5 новых подтверждённых блоков. Нет никакой обязанности их соблюдать.

Описанных выше алгоритмов и протоколов достаточно для создания криптовалюты, что и было сделано Сатоши Накамото в 2008 году.

Однако такая сеть имеет ряд угроз, обсуждаемых многими критиками. Самой известной и, по сути, единственной значимой из них является **«атака 51%»**. Очевидно, что алгоритм Proof-of-Work подразумевает под собой зависимость шанса нахождения нового блока от вычислительных мощностей. Тогда, если некий узел сети имеет чуть больше, чем 50% всех вычислительных мощностей в сети, то рано или поздно он сможет обогнать релевантную сеть и диктовать условия всему консенсусу, потому что по скорость нахождения блоков у этого узла в среднем выше, чем у всех остальных узлов вместе взятых.

  
**Рис. 6.** Пример поведения блокчейн сети в случае развилки. Нижняя ветка отклоняется по соглашению внутри сети, как самая коротка.

Значительным увеличением защиты от этой атаки является протокол Proof-of-Stake – **алгоритм, который требует создание блока с таким хешем, чтобы он был меньше, чем некое фиксированное консенсусом число, умноженное на произведение количества валюты и времени их хранения в этом узле**[14]. То есть, чем больше у узла валюты и чем дольше они остаются неиспользованными, тем выше шанс нахождения следующего блока, поскольку требуемая граница хеша для увеличивается с увеличением капитала и времени его хранения. Вероятность создания нескольких блоков подряд или с малым интервалом времени одним узлом ничтожно мала.

Такая схема подразумевает защиту от атаки 51%, однако имеет уязвимость в случае капитализации одним блоком 50% всех активов. Этот вопрос решается ограничением увеличения границы хеша блока, а также долговременной хранение активов будет невыгодно узлу в связи с увеличением цены этих активов.

Последним из алгоритмов, требующих пристального рассмотрения, является Proof-of-Burn. Его суть заключается в посылке криптовалюты на пустой адрес, в большинстве случаев – это хеш блока, с целью сжигания криптовалюты и получения награды за блок. Алгоритм подразумевает, что награда может быть представлена в виде другой криптовалюты. Ценность этого алгоритма заключается в возможности деноминации электронной валюты.

Кроме всех представленных выше алгоритмов, существует множество протоколов взаимодействия, которые являются просто модификациями своих идейных прародителей. Так, например, продолжением идеи Proof-of-Work стало разделение некоторыми участниками сети работы по нахождению новых блоков и разделению награды. Революционным продолжением этих механизмов стали смарт-контракты, которые требуют отдельной главы для их рассмотрения.

# **Глава 2. Смарт-контракты и коллективное инвестирование**

## ***2.1. Понятие смарт-контракта, особенности, принципы работы***

В 2015 году с появлением платформы Эфириум появился новый алгоритм, который был назван смарт-контрактом. По своей сути это **произвольный код, встраиваемый в блокчейн**. Для понимания технической части этого нововведения нужно немного углубиться в консенсус Эфириума, который становится понятнее в отличиях от Биткоина.

Язык общения внутри сети Биткоина является не полным по Тьюрингу, в ней нет циклов. Кроме того, новые блоки представляют из себя изменения на счётах, то есть проходя по всем изменениям можно воссоздать сколько биткоинов остаётся на счету.

У Эфириума же есть своя собственная Тьюринг-полная виртуальная машина, которая так и называется Ethereum Virtual Machine, EVM. Состояния этой машины и выступают блоками в блокчейне. Они формируются байт-кодом этой виртуальной машины. В состояниях отражено сколько Эфира стало на том или ином счету. То есть в транзакции содержится не только информация о переводе средств, но и некий байт-код для изменения состояния EVM, который исполняется людьми, находящими новый блок.

Такая конструкция наводит на мысль, о регулировании исполнения Тьюринг-полной виртуальной машины, поскольку появляются потенциально бесконечные циклы. Для этого был введен Gas, определённое количество которого должно передаваться вместе с транзакцией. Было решено брать плату за каждую исполненную команду. Эта плата настолько мала, что не требует детального экономического рассмотрения. Соответственно, если для совершения транзакции количество Gas оказалось недостаточным, то она отклоняется, а если его было больше, чем надо, то остаток возвращается заказчику.

В обычной практике смарт-контрактами выступают классы, написанные на языке Solidity, предназначенном специально для Эфириума. Они компилируются в байт-код EVM и в последствии к ним можно будет обращаться. В смарт-контрактах может быть прописана логика хранения средств, кто может их выводить и при каких условиях.

Помимо обычных кошельков для пользователей, есть ещё особые кошельки специально для смарт-контрактов, которые являются хешами самих смарт-контрактов. Чтобы обратиться к смарт-контракту, нужно совершить транзакцию на него. Выделение смарт-контрактам специальных адресов было сделано не случайно, а для того, чтобы наложить ограничение на перевод средств непосредственно человеку. То есть в такой системе смарт-контракт может перевести Эфир только другому смарт-контракту, но на адрес человека нет.

Это позволяет добиться доверия между клиентом и покупателем без лишних посредников и заключения длинных договоров. Надо просто согласовать смарт-контракт, который будет удерживать деньги до совершения операции, которую сам же смарт-контракт сможет проверить. Дальше одна из сторон обращается к смарт-контракту для получения с него средств: причём не важно будет ли то из-за отмены, или наоборот успеха сделки, ведь условия для обоих этих случаев уже были бы проверены и применены смарт-контрактом.

Иными словами, как и в настоящих договорах, ответственность за потенциальные угрозы берут на себя непосредственно составители договоров.

## **2.2 Смарт-контракты и ICO.**

С появелением смарт-контрактов стало возможным так же создание собственной криптовалюты практически любому пользователю на основе ICO (Initial coin offering). Её идея заключается в создании смарт-контракта, исполняющего роль непосредственно новой криптовалюты с полным описанием её структуры. В качестве капитализации новой валюты обычно выступает Эфир, поскольку смарт-контракты впервые появились именно в криптовалюте Эфириум. Таким образом, любой пользователь может создать свою собственную валюту и увеличивать её стоимость, повышая доверие других людей к ней. Именно этого нет в современной модели экономики всех стран.

В 2015 году разработчики платформы Эфириум разработали ERC20[17] – стандарт формирования собственных токенов, или проще говоря монет. Это послужило началом большого ажиотажа вокруг ICO в целом.

ICO представляет интерес не только с точки зрения выпуска своей валюты, но и с точки зрения экономической теории, поскольку открывает новые области исследования финансовых потоков и денежного саморегулирования. Как показывает статистика (Приложение, рис. 2), большинство ICO направлены на привлечение капитала, то есть выступают непосредственно децентрализованной валютой.

По своей сути ICO является одной из формой коллективного финансирования, что настораживает некоторые государственные органы и крупные организации. Так, например, 4 сентября 2017 года семь китайских финансовых регуляторов официально запретили все ICO в Китайской Народной Республике, требуя вернуть выручку от всех уже прошедших ICO[15]. А в июне 2018 году компания Google в своем ввела запрет на рекламу криптовалют и любого связанного с этим контента[16].

Подробная инфографика о развитии ICO представлена в приложении на странице 2 (рис. 4).

# **Глава 3. Прикладное применение технологии «Блокчейн»**

## **3.1. Основные элементы и сферы применения технологии «Блокчейн»**

Как уже было упомянуто ранее для нормальной работы блокчейна необходимы сама база данных, которая будет храниться по сети в виде связного списка, криптографическая хеш-функция, ЭЦП и какой-либо алгоритм, затрудняющий перезапись истории изменений.

Как понятно из истории и первоначальной задумки, блокчейн разрабатывался, в основном, для криптовалют и финансовой сферы. Хотя по своей сути является протоколом общения в распределённой сети для подтверждения истинности данных.

Это позволяется применять блокчейн в любой сфере, в которой подразумевается обмен информацией между пользователями. Поэтому эта технология и вызывает интерес у многих фирм, стремительно захватывая практически все сферы предпринимательской деятельности, включая здравоохранение, энергетику, промышленность, логистику, сферу услуг, телекоммуникации и финансовый сектор. Технологии распределенного реестра способствуют интенсивной децентрализации современного бизнеса.

Одной из самых важных сфер применения блокчейна стало государственное управление. Публичные записи в Росреестре, открытая избирательная система, умная налоговая система – всё это стало возможным благодаря блокчейну и смарт-контрактам. Даже возможно, что в ближайшем будущем будет создана государственная законодательная база, которая позволит любому человеку беспрепятственно следить не только за новыми законами, но и актуальными изменениями в старых.

В образовании данная технология может помочь с точки зрения прозрачной документации, уменьшив тем самым число мошенников в этой сфере. Распределённый реестр позволит государственным органам и другим заинтересованным лицам самостоятельно проверять дипломы без совершения непосредственного запроса в учебное заведение. Дополнительно можно будет в разы сократить ручную проверку бумаг и документов.

Область электронного голосования также не обошлась без внимания, поскольку блокчейн позволяет сделать сам процесс голосования полностью прозрачным, увеличивая тем самым доверие к нему. Такая практика уже применяется либертарианской партией США штата Техас[18].

Стоит так же отметить, что блокчейн систему можно создать даже для домашних нужд. Например, для контроля расходов и доходов в семье. Для этого просто нужен простой дневник, в котором будут записи о получении зарплаты или расходах на продукты, мебель или кино. В конце каждой записи должен быть хеш от предыдущей и какое-то случайное число для, чтобы итоговый хеш содержал, например, три нуля вначале. Этого достаточно, чтобы обеспечить базовую надёжность внутри малого круга лиц.

Наверное, одной из самых важных сфер применения блокчейна является противодействие компьютерным атакам. В частности, одноранговая сеть, из-за принципа своей работы, полностью защищена от воздействия DDoS-атаки. Это позволяет обезопасить множество крупных компаний от временной недееспособности и сократить убытки.

Ожидаемым вопросом после этого примера станет: «Для чего нужна такая надёжность в быту?» Такая «домашняя» модель позволяет вникнуть в концепцию блокчейна, раскрыть все его тонкости, а также понять потенциал применения этой технологии.

Наглядное представление о сферах применения технологий можно найти на странице 2 приложения (рис. 3).

## **3.2. Блокчейн структуры в финансовой сфере**

Отдельно стоит выделить финансовую сферу применения этого новшества. Криптовалюты – это мощный инструмент в создании децентрализованной платёжной системе без посредников. Помимо обычного использования, в них уже заложена эмиссия, которая может быть регулированная по соглашению участников сети. Причём, в отличие от обычных денег, подделка криптовалют невозможна и определяется протоколом взаимодействия между участниками сети. Видя это преимущества, некоторые компании, например Emniyet Taksi на популярном турецком курорте Мармари, уже перешли на такой вид платежей[19].

Особенно нужно выделить краудфандинг – коллективное финансирование – и краудлендинг – кредитование физических лиц. Благодаря смарт-контрактам стало возможным децентрализовано собирать деньги на различные нужды, например для стартапа или на ремонт моста, а также определять долю активов в новых цифровых валютах. Кроме того, кредитование стало в разы проще, с точки зрения получения займа и гарантии их возврата, поскольку история кредитов уже храниться с распределённой сети. В 2018 году Центральным банком был разработан законопроект[20], определяющий правовые основы краудфандинга. Сейчас законопроект находится на рассмотрении.

Другим важны аспектом финансовой сферы является банковский сектор, который пристально наблюдает и экспериментирует с блокчейн технологиями. Связано это с тем, что они способны значительно улучшите такие вопросы как межбанковские платежи, аутентификация пользователей и кредитование.

Российские банки обязаны идентифицировать своих клиентов в целях противодействия легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма[21]. Согласно одному исследованию[22], социальные институты тратят в среднем более $60 млн на идентификацию и проверку клиентов. Блокчейн введения могут значительно снизить эти расходы, сохраняя данные о проверенных клиентах в распределённом реестре, к которому могут иметь другие банки, страховые компании и другие аккредитованные организации.

## **3.3. Будущее технологии распределенных реестров**

Несмотря на всю описанную выше пользу технологий распределённых реестров, остаются некоторые вопросы, требующие дальнейшего развития. Так, например, вопросы масштабирования и безопасности всё ещё остаются актуальными.

Проблема увеличения числа пользователей безусловно поджидает практически любой блокчейн проект. Для его решения уже разрабатываются новые алгоритмы типа Proof-of, а также обсуждаются вопросы распараллеливания блокчена. Уже ведутся попытки создания криптовалют с большой транзакционной способностью. Так что лишь вопрос времени, когда эта проблема будет решена.

С появлением смарт-контрактов, обострился вопрос их стандартизации. В данный момент стандарты появляются только от разработчиков Эфириума, из-за чего многие сферы обделены грамотно продуманной договорной системой. Скорее всего в ближайшем будущем произойдёт образование некоторых экспертных групп, которые будут решать этот вопрос коллективным трудом.

Так же остаётся открытым вопрос правового статуса криптовалют. Несмотря на явную полезность, правительства многих стран всё ещё сомневаются в признания криптовалют на правовом уровне. Правда такой процесс абсолютно нормальный, поскольку новые технологии всегда вызывают сомнения.

Законопроект «Об экспериментальных правовых режимах в сфере цифровых инноваций», предложенный Минэкономразвития России призван укорить внедрение блокчейн-технологий путём возможности создания экспериментального правового режима на территории России. Возможно, именно Центробанк РФ станет координационно-регулирующим органов в финансовой сфере[23].

## **Заключение**

Безусловно технология «Блокчейн» является перспективной областью развития, поскольку протокол общения внутри такой сети обеспечивает значительную информационную целостность и безопасность даже при наличии некоторых угроз.

Технология готова к применению в некоторые экономические структуры. Однако всё ещё не готова быть введена в массовое пользование, возникают проблемы с масштабируемостью и скоростью обмена информации.

Главными проблемами использования блокчейна является недоверие со стороны крупных компаний к этой технологии, а также отсутствии децентрализованного протокола формирования отмены изменений в консенсусе.

Процесс формирования нормативной и регуляторной баз не является стоп-фактором для дальнейшего развития технологий «Блокчейн» и создания новых концепций применения.

В итоге можно сказать, что данная сфера будет перспективной и развивающейся ещё несколько десятков лет.

# **Список литературы**

1. The Eureka Moment That Made Bitcoin Possible / Amy Whitaker // The Wall Street Journal, 2018 – Режим доступа: <https://www.wsj.com/articles/the-eureka-moment-that-made-bitcoin-possible-1527268025>

2. Bitcoin: A Peer-to-Peer Electronic Cash System / Satoshi Nakamoto – портал Bitcoin.org , 2008 – Режим доступа: <https://bitcoin.org/bitcoin.pdf>

3. Статья «Краткая история ICO» – портал Golos, 2018, – Режим доступа: <https://golos.io/ru--kriptovalyuty/@snooze/kratkaya-istoriya-ico>

4. Intelligence assessment: Bitoin virtual currency: Unique features present distinct challenges for deterring illicit activity // Federal Bureau of Investigation, 2012, – Режим доступа: http://cryptome.org/2012/05/fbi-bitcoin.pdf

5. Статья «ЦБ Китая запретил банкам операции с Bitcoin» – портал Ведомости, 2013 – Режим доступа: <https://www.vedomosti.ru/finance/news/2013/12/05/cb-kitaya-zapretil-bankam-operacii-s-bitcoin#ixzz2myQN49z2>

6. Статья «Суд впервые признал криптовалюту имуществом» – портал РБК, 2018 – Режим доступа: <https://www.rbc.ru/finances/07/05/2018/5af0280d9a7947165a6e8c22>

7. Статья «Центробанк выступил против легализации криптовалют в России» - портал РИА Новости, 2017 – Режим доступа: <https://ria.ru/20171005/1506246580.html>

8. Н.Ю. Круглова. Хозяйственное право. — М.: Юрайт, 2011. — 885 с.

9. <https://digiforest.io/blog/blockchain-consensus-algorithms>

10. Буханцов А. Д., Дружкова И. В. О модификации алгоритма MD5 // Белгородский государственный национальный исследовательский университет, 2016, с. 176.

11. Статья «Блокчейн: возможности, структура, ЭЦП и задание для студента, часть 1» – портал Habr, 2018 – <https://habr.com/ru/post/348014/>

12. Статья «Как это работает: Деревья Меркла в биткойн сети» - портал Habr, 2018 – Режим доступа: <https://habr.com/ru/company/bitfury/blog/346398/>

13. Статья «До сокращения награды за блок осталось два года — что будет с ценой биткоина?» – портал Coinspot, 2018 – Режим доступа: <https://coinspot.io/technology/bitcoin/do-sokrashheniya-nagrady-za-blok-ostalos-dva-goda-chto-budet-s-cenoj-bitcoina/>

14. Cryptocurrencies Without Proof of Work / Iddo BentovEmail authorAriel GabizonAlex Mizrahi // International Conference on Financial Cryptography and Data Security, 2016 – Режим доступа: <https://link.springer.com/chapter/10.1007/978-3-662-53357-4_10>

15. Статья «China Outlaws ICOs: Financial Regulators Order Halt on Token Trading» – портал Coindesk, 2017, – Режим доступа: <https://www.coindesk.com/china-outlaws-icos-financial-regulators-order-halt-token-trading/>

16. Статья « Google официально запретит рекламу криптовалют и ICO в июне» – портал Forklog, 2018, – Режим доступа: <https://forklog.com/google-ofitsialno-zapretit-reklamu-kriptovalyut-i-ico-v-iyune/>

17. ERC: Token standard, 2015 – Режим доступа: <https://github.com/ethereum/eips/issues/20>

18. Статья «Libertarian Party of Texas to Store Election Results On Three Blockchains» – портал Coindesk, 2016, – Режим доступа: <https://www.coindesk.com/libertarian-party-texas-logs-votes-presidential-electors-blockchain>

19. Статья «Такси за биткоины скоро никого не удивит» – портал Bits.media, 2016, – Режим доступа: <https://bits.media/taksi-za-bitkoiny-skoro-nikogo-ne-udivit/>

20. Законопроект № 419090-7 «О привлечении инвестиций с использованием инвестиционных платформ» – Режим доступа: <https://sozd.duma.gov.ru/bill/419090-7> (дата обращения: 25.05.2019)

21. Федеральный закон "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" от 07.08.2001 N 115-ФЗ

22. Know Your Customer Surveys Reveal Escalating Costs and Complexity // Thomson Reuters, 2016 – Режим доступа: <https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html>

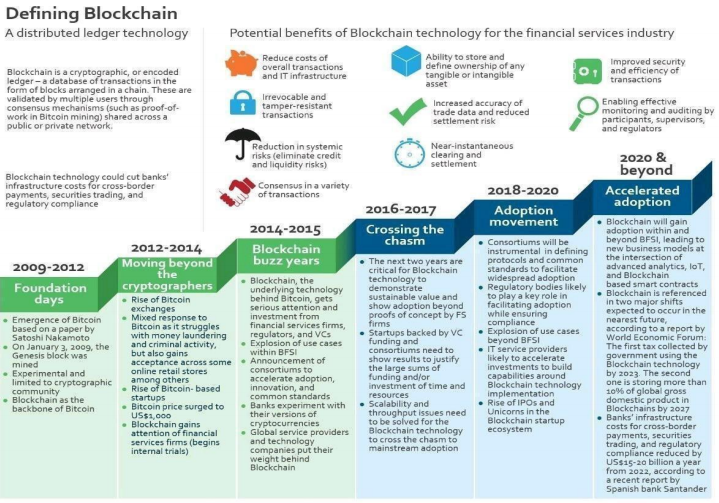
23. Статья «Центробанк РФ может стать регулятором для блокчейн-индустрии» – портал Forklog, 2019, – <https://forklog.com/tsentrobank-rf-mozhet-stat-regulyatorom-dlya-blokchejn-industrii/>

24. 10-ая ежегодная международная научно-практическая конференция «Инвестиции. Инновации. Информационные Технологии: Перспективы Технологии блокчейн. Мифы и реальность» // Школа IT-менеджмента РАНХиГС, 2018 – Режим доступа: <http://itm.ranepa.ru/doc/conf2018/BlockchainTech8.pdf>

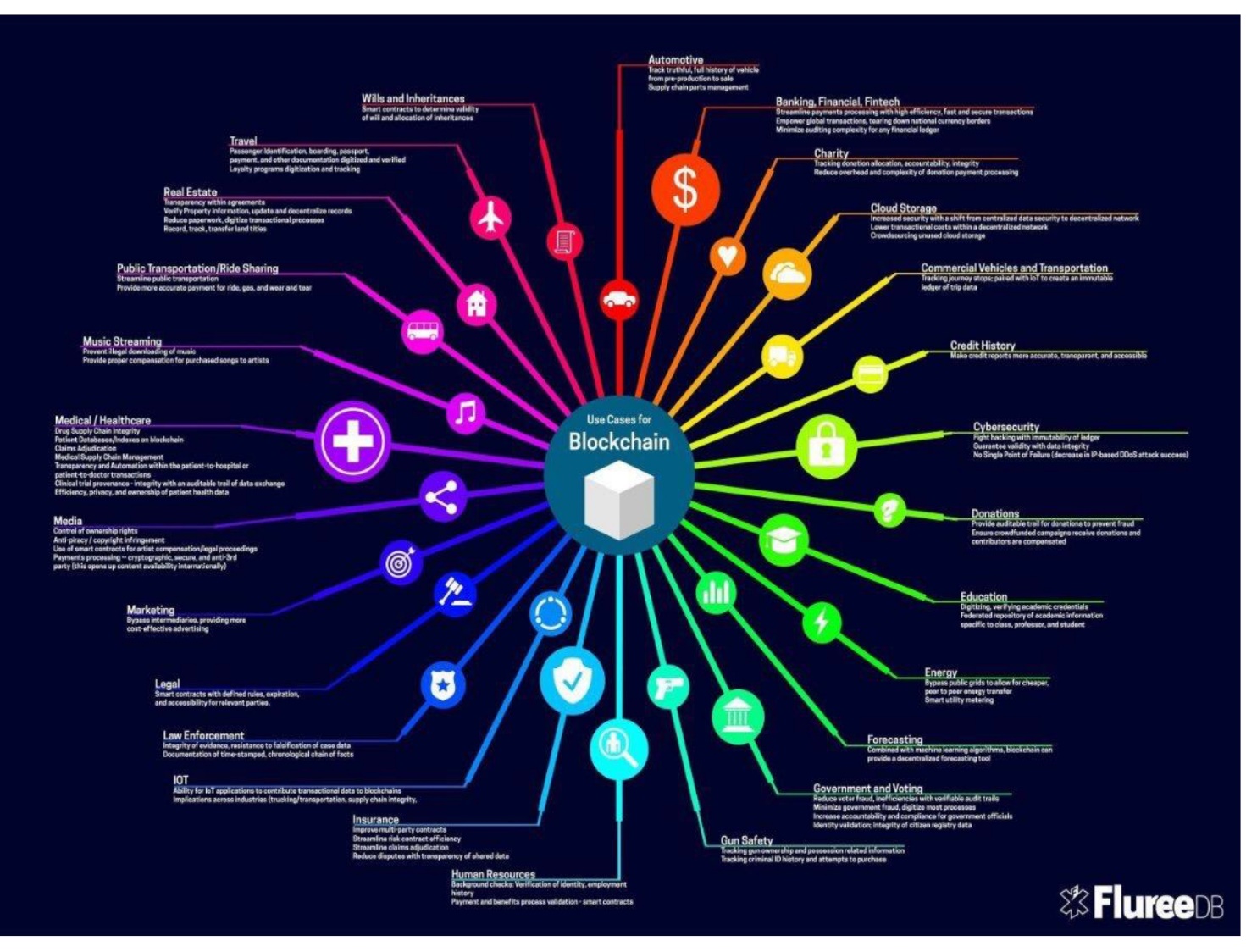
25. Статистика рынка ICO – портал Foundico, 2019 – Режим доступа: <https://foundico.com/ru/stats/> (дата обращения: 25.05.2019)

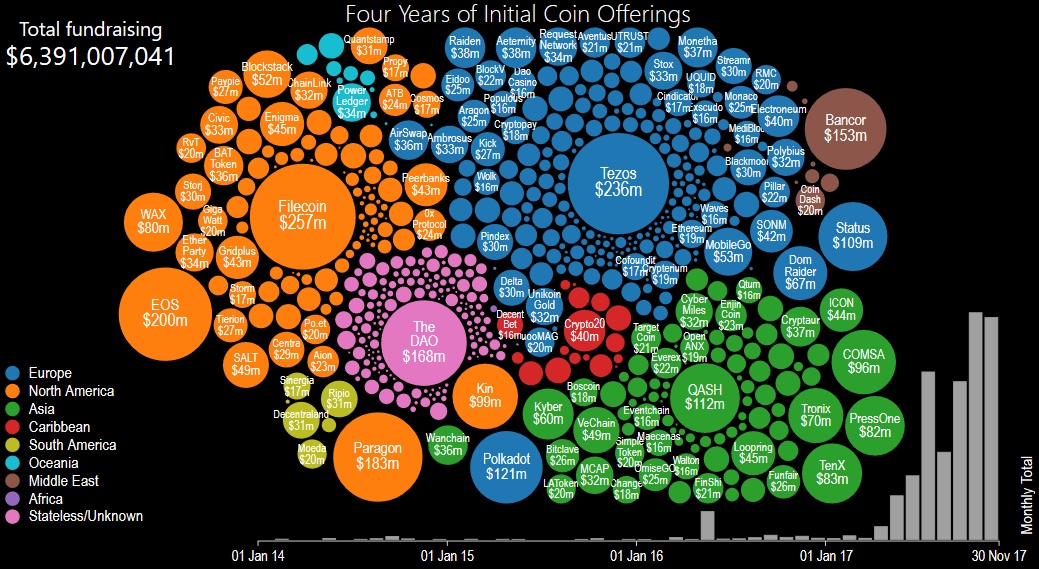
26. Статья «4 года развития ICO — инфографика» – портал Bit Expert, 2018 – Режим доступа: <https://bitexpert.io/news/4-years-ico-infographics/>

# **Приложения**

  
**Рис. 1.** История развития блокчейна с 2009 года[24].

 **Рис. 2.** Статистика по категориям ICO на 2019, единиц[25].

 **Рис. 3.** Сферы применения технологии «Блокчейн»[24].

 **Рис. 4.** История развития ICO за 4 года[26].