Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Зубарев А.В., Шилов К.Д., Сулейманова М.З., Голованова Е.А., Гребёнкина А.М.

Анализ возможностей использования технологии распределённого реестра для повышения эффективности функционирования секторов российской экономики

Москва 2019

Аннотация. Были роанализированы основные механизмы достижения консенсуса в распределённых реестрах, классифицированы различные виды распределённых реестров по признакам того, кто может формировать цепочки данных и кто имеет к ним доступ. Подробно были рассмотрены такие важные приложения респределённого реестра (блокчейна), как смарт-контракты, описана схема их работы систематизированы особенности функционирования на различных платформах.

Большая часть работы посвящена подробному рассмотрению использования технологии блокчейн в финансовом секторе. На примере анализа отдельных международных и отечественных практик проанализированы выгоды от использования блокчейна в банковском секторе и в системах платежей.

В заключение приводятся рекомендации для проведения экономической политике в области внедрения технологии блокчейн.

Abstract. This study analyzed the main mechanisms for achieving consensus in distributed ledgers. Different types of distributed ledgers were classified according to the characteristics of who can form data chains and who has access to them. Such important applications of the distributed ledger (blockchain) as smart contracts were examined in detail, the principle of their work was described, the features of functioning on various platforms were systematized.

Most of the work is devoted to a detailed review of the use of blockchain technology in the financial sector. Using the analysis of individual international and domestic practices as an example, the benefits of using the blockchain in the banking sector and in payment systems are analyzed.

In conclusion, recommendations are given for economic policy in the field of blockchain technology implementation.

Зубарев А.В. старший научный сотрудник лаборатории математического моделирования экономических процессов ИПЭИ Российской академии народного хозяйства и государственной службы при Президенте РФ

Шилов К.Д. научный сотрудник Центра экономического моделирования энергетики и экологии ИПЭИ Российской академии народного хозяйства и государственной службы при Президенте РФ

Сулейманова М.З. научный сотрудник лаборатории математического моделирования экономических процессов ИПЭИ Российской академии народного хозяйства и государственной службы при Президенте РФ

Голованова Е.А. младший научный сотрудник лаборатории математического моделирования экономических процессов, ИПЭИ Российской академии народного хозяйства и государственной службы при Президенте РФ

Гребёнкина А.М. младший научный сотрудник Центра изучения проблем центральных банков ИПЭИ Российской академии народного хозяйства и государственной службы при Президенте РФ

Данная работа подготовлена на основе материалов научно-исследовательской работы, выполненной в соответствии с Государственным заданием РАНХиГС при Президенте Российской Федерации на 2018год

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

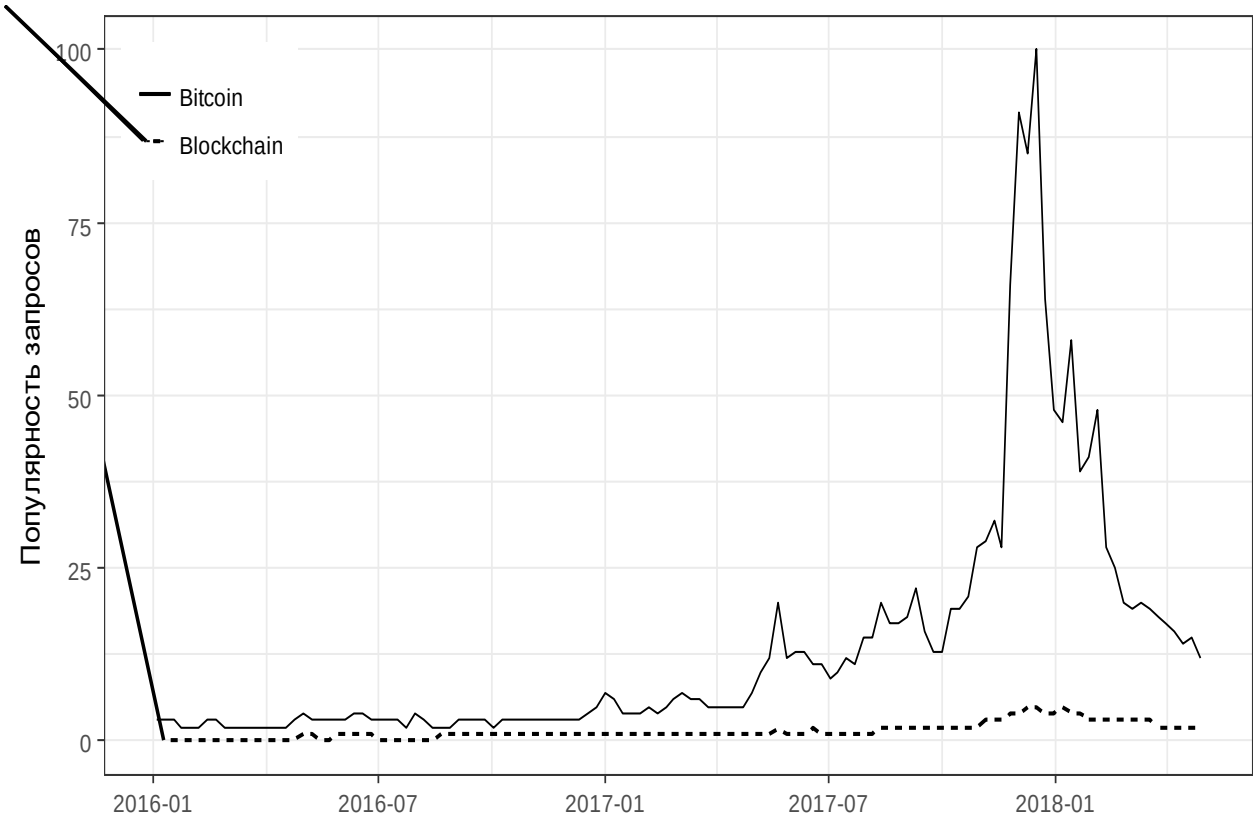
В мире в последние несколько лет значение технологии распределенного реестра или Блокчейн (BlockChain) не только активно обсуждается, но и стало обязательным для пилотного внедрения в большинстве развитых стран во многих областях экономики. Многие организации ставят своей целью разобраться в возможном применении технологии как для поиска путей развития бизнеса, так и для оптимизации текущих процессов для сокращения издержек. На текущий момент многие считают, что технология распределенного реестра имеет значение, сравнимое с такими инновациями своего времени, как интернет и телеграф. Потенциал технологии будет раскрыт постепенно в ближайшие 5-10 лет, но уже за несколько последних лет реализованы проекты применения Блокчейн в финансовой индустрии, которые открывают новые бизнес-возможности и кардинально оптимизируют текущую деятельность компаний и банков. Данные примеры свидетельствуют в пользу гипотезу о глобальном изменении роли институтов и их месте в экономике на перспективе 5-10 лет посредством упомянутой технологии. В настоящий момент актуальным представляется описание как самой технологии, так и применимости решений на открытом реестре в России для банков, финансовых институтов и других секторов экономики.

1 Обзор основных положений и принципов работы технологии распределенного реестра (блокчейн)

Понятие технологии распределённого реестра (distributed ledger technology, DLT) в современном мире неразрывно связано с понятием криптовалют, так как именно они и дали толчок к распространению одного из самого популярного вида распределённого реестра – блокчейна. Потенциал данной технологии, однако, не ограничен лишь использованием её в рамках криптовалют, хотя данная область до сих пор является самой популярной для её применения. В данной главе будет описан механизм работы распределённого реестра (в том числе блокчейна), его основные принципы и классификация.

В последние несколько лет дискуссия о криптовалютах стала одной из самых популярных. Игроки на финансовых рынках пытаются совершить выгодные вложения в различные криптовалютные инструменты, экономисты-теоретики обсуждают, насколько данный феномен укладывается в концепцию частных денег Фридриха Хайека, юристы обсуждают правовые аспекты первичного размещения криптоактивов (так называемые ICO, Initial Coin Offering). Основной же интерес широких масс до сих пор вызывает самая первая криптовалюта Bitcoin, созданная и описанная неким Сатоси Накамото в статье 2008 года [1], капитализация которой на начало мая 2018 года составляла порядка 156 млрд. долларов. В этой же статье Накамото впервые была формализована идея технологии, которая в последующем будет обозначена термином блокчейн (blockchain – цепочка блоков) и будет использована в качестве технологической основы Bitcoin’а, а также многих других криптовалют. Тем не менее, если судить по популярности поисковых запросов в сервисе Google, то можно отметить, что даже в самый пиковый период популярности тем, связанных с криптовалютами в конце 2017 года на каждые 100 поисковых запросов по слову «Bitcoin» приходилось лишь 5 запросов по слову «Blockchain» (см. рисунок 1). Данная динамика в какой-то мере свидетельствует о том, что изучение самой технологии распределённого реестра и самой популярной её реализации, блокчейна, не вызывает такого интереса, как сами криптовалюты. И если вопрос о перспективах криптовалют пока остаётся довольно дискуссионным,

то потенциал блокчейна в настоящее время осознаётся как частым бизнесом, так и государственными структурами разных стран.



Примечание – Источник: Google Trends.

Рисунок 1 – Популярность поисковых запросов Bitcoin и Blockchain

Так что же собой представляет технология распределённого реестра? По сути, это лишь некоторый особый вид базы данных. Для более подробного раскрытия этого тезиса в первой части статьи мы рассматриваем традиционные виды базы данных и то, как распределённый реестр соотносится с ними. Во второй части статьи объясняется механизм работы блокчейна на примере криптовалюты Биткоин. В третьей части приведена классификация видов распределённого реестра и обзор альтернативных механизмов консенсуса.

1.1 Традиционные базы данных

База данных, по определению, – это организованный, систематизированный набор некоторой информации. Самым распространённым на сегодняшний день видом баз данных является реляционная база данных (relational database). Обычную

базу данных можно представить в виде некоторой таблицы (сущности), состоящую из столбцов и строк (кортежей). Реляционная база данных, в свою очередь, представляет собой набор взаимоувязанных между собой некоторыми отношениями нескольких таких таблиц (сущностей). Такой вид баз данных основан на реляционной модели данных – логической модели данных, сформулированной еще в 1970 году британским учёным Э.Ф. Коддом [2]. Для работы с такими базами обычно используется декларативный язык программирования SQL. Самыми популярными реляционными системами управления баз данных являются решения, предоставляемые компаниями Oracle (Oracle Database), IBM (IBM DB2) и Microsoft (Microsoft SQL Server). Реляционные базы данных отличаются высокой степенью централизации: любые операции с данными (запрос, изменение, добавление, удаление и проч.) обрабатываются единым центром (процессором, CPU), сервера которого, чаще всего, физически расположены в одном месте и администрирование которых осуществляется неким специальным лицом/организацией. Пользователи в такой системе работают с данными в формате «запрос - ответ».

Другой крупный вид баз данных – распределённая база данных (distributed database, DDB), которая, по сути, представляет собой сеть из нескольких взаимосвязанных баз данных (нодов), распределённых в компьютерной сети. Любые операции с данными в такой базе обрабатываются децентрализовано – сетью из нескольких центров (процессоров, CPU), при этом данные распределены по различным хранилищам (серверам) и даже могут частично дублироваться. С развитием интернета, потребности компаний в хранении и обработке большого количества структурированных и неструктурированных данных росла, а распределённые базы данных оказались наиболее подходящими в плане повышенного уровня отказоустойчивости (отсутствие единой точки отказа, выход из строя которой повлечёт за собой неработоспособность всей базы) и масштабируемости (удалённая аренда облачного сервера обходиться дешевле и выгоднее для некоторых видов бизнеса, чем покупка нового физического сервера) вариантами. Известными распределёнными базами данных являются: распределённые SQL базы (от Microsoft, Oracle, IBM и др.); нереляционные NoSQL базы (MarkLogic, MongoDB др.); NewSQL (Google Spanner, Clustrix), объединяющие в себе первые два подхода; проект Hadoop, используемый для обработки и хранения

т.н. “больших данных”. Все выше перечисленные базы, так или иначе, построены на архитектуре “клиент-сервер” – клиенты посылают некоторые запросы на чтение или редактирование данных, а сервера, объединённые в распределённую сеть, их исполняют, храня эти данные у себя (см. рисунок 2).

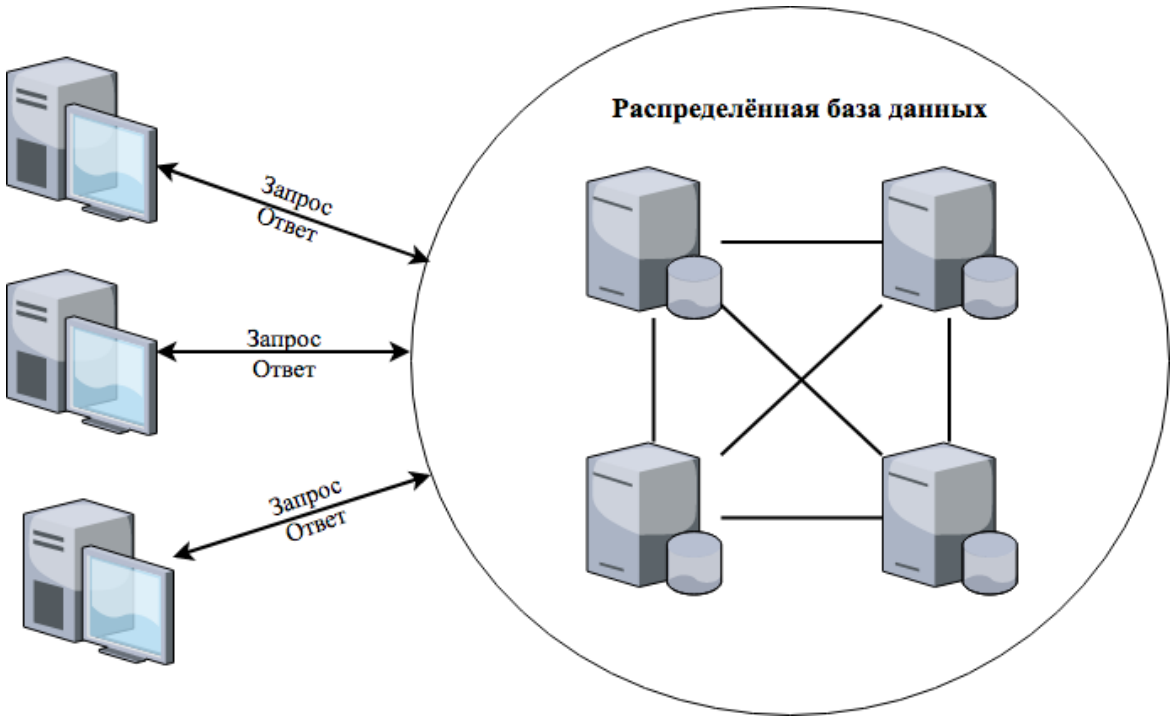


Рисунок 2 – Архитектура сети типа клиент-сервер для распределённой базы данных

Стоит также отметить, что существует и другой вид распределённой сети, называемый одноранговой пиринговой сетью (peer2peer network), в которой могут отсутствовать выделенные сервера, а каждый клиент одновременно является еще и сервером (см. рисунок 3).

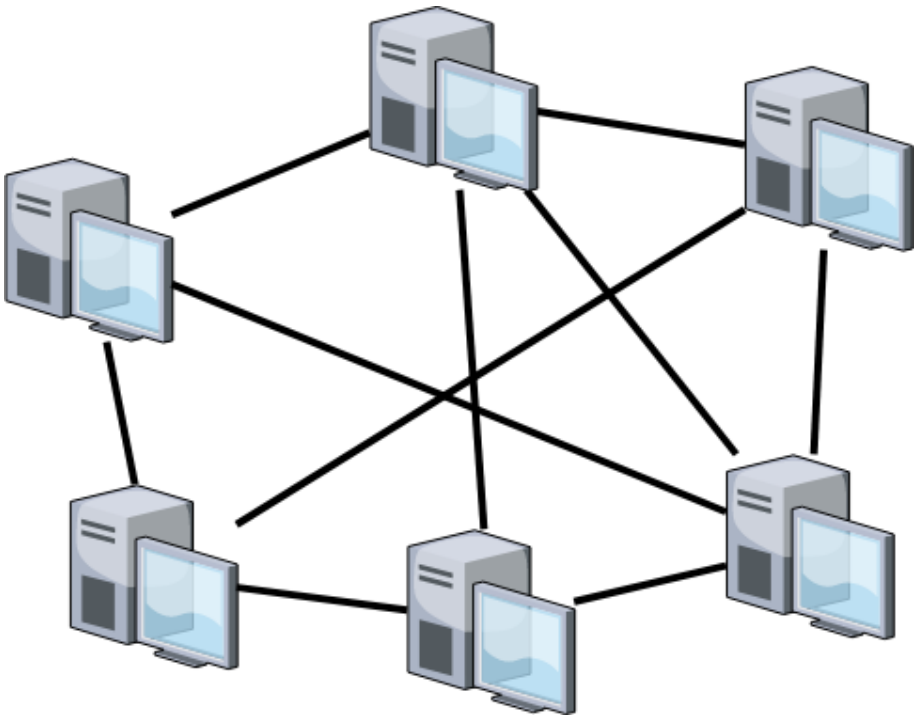


Рисунок 3 – Одноранговая сеть

В явном виде пиринговые сети, как сети без выделенных серверов, не использовались для построения корпоративных баз данных. Тем не менее, одной из самых известных реализацией такой сети стал протокол BitTorrent, позволяющий пользователям предоставлять (“раздавать”) различные файлы для скачивания другим пользователям, которые сохранив файл у себя также выступают в роли “раздающего”. Таким образом, файлы реплицируются по сети и пока хоть один из владельцев участвует в процессе обмена, файл остаётся доступен для других. Стоит отметить, что такая сеть является частично децентрализованной, так как без BitTorrent-трекера, условно говоря, сайта, который сводит пользователей друг с другом, пользователи просто не смогут взаимодействовать.

Таким образом, можно выделить несколько важных особенностей традиционных и распределённых баз данных. Первой особенностью таких баз является централизация, так как за их функционирование отвечает, обычно, один или несколько центров ответственности. Предполагается, что эти центры действуют в условиях полного доверия друг к другу, а также пользуются доверием со стороны пользователей. Под доверием в данном контексте понимается неискаженное, непротиворечивое и достоверное отражение хранимой информации, а также обеспечение бесперебойного доступа к ней. Более того, на плечах центра лежит

ответственность за проведение и валидацию (одобрение или отказ) транзакций – последовательности операций над базой (например, внесение или корректировки данных), переводящих базу из одного целостного состояния в другое.

Вторая особенность, это отражаемость данных в текущий момент времени. Каждый раз, когда клиент в некоторый момент времени обращается к базе, он видит её текущее состояние, причём чаще всего без возможности увидеть данные в том виде, в котором они были вчера, неделю назад или год назад. Конечно же, современные базы чаще всего предлагают возможности просмотра истории изменения того или иного элемента (так называемые персистентные структуры данных). Администраторами баз на регулярной основе создаются резервные копии (бэкапы), представляющие собой набор “слепков” базы в некоторый момент времени. Тем не менее, в таких базах совершенно отсутствует механизм верификации того, что информация не была изменена задним числом, что вновь приводит к проблеме доверия к администратору.

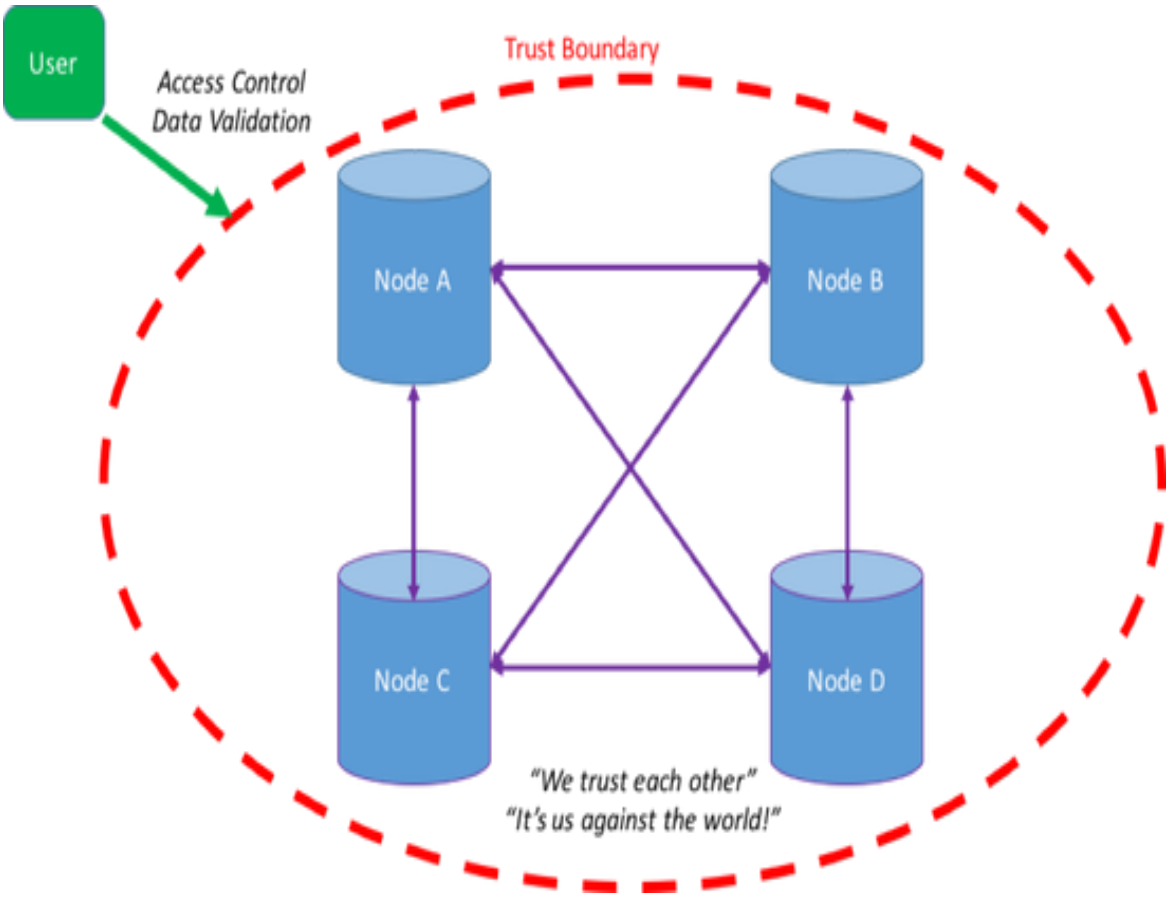
Третья особенность, это возможность клиентом выполнять базовые операции с данными, обозначаемых акронимом CRUD (create, read, update, delete) – создавать записи в базе, читать их (возможность просматривать), обновлять и удалять их.

1.2 Технология распределённого реестра

Место распределённого реестра в иерархии видов баз данных представляется не совсем очевидным. В первую очередь это связанно с путаницей терминов база данных (database) и реестр (ledger), которые чаще всего употребляются как синонимы (см. например [3] и [4]). Некоторые эксперты определяют распределённый реестр как один из видов распределённой базы данных [5]. Стоит отметить, что использование термина реестр (ledger), скорее всего, обусловлено его использованием также в качестве термина, обозначающего книгу записей некоторой финансовой информации в денежном выражении. В том числе, главная бухгалтерская книга в английском языке носит название general ledger. Следовательно, вполне логично, что первый созданный блокчейн, а именно блокчейн Биткоина, который выполняет функцию учёта транзакций в некоторой цифровой валюте, стал впоследствии называться распределённым реестром.

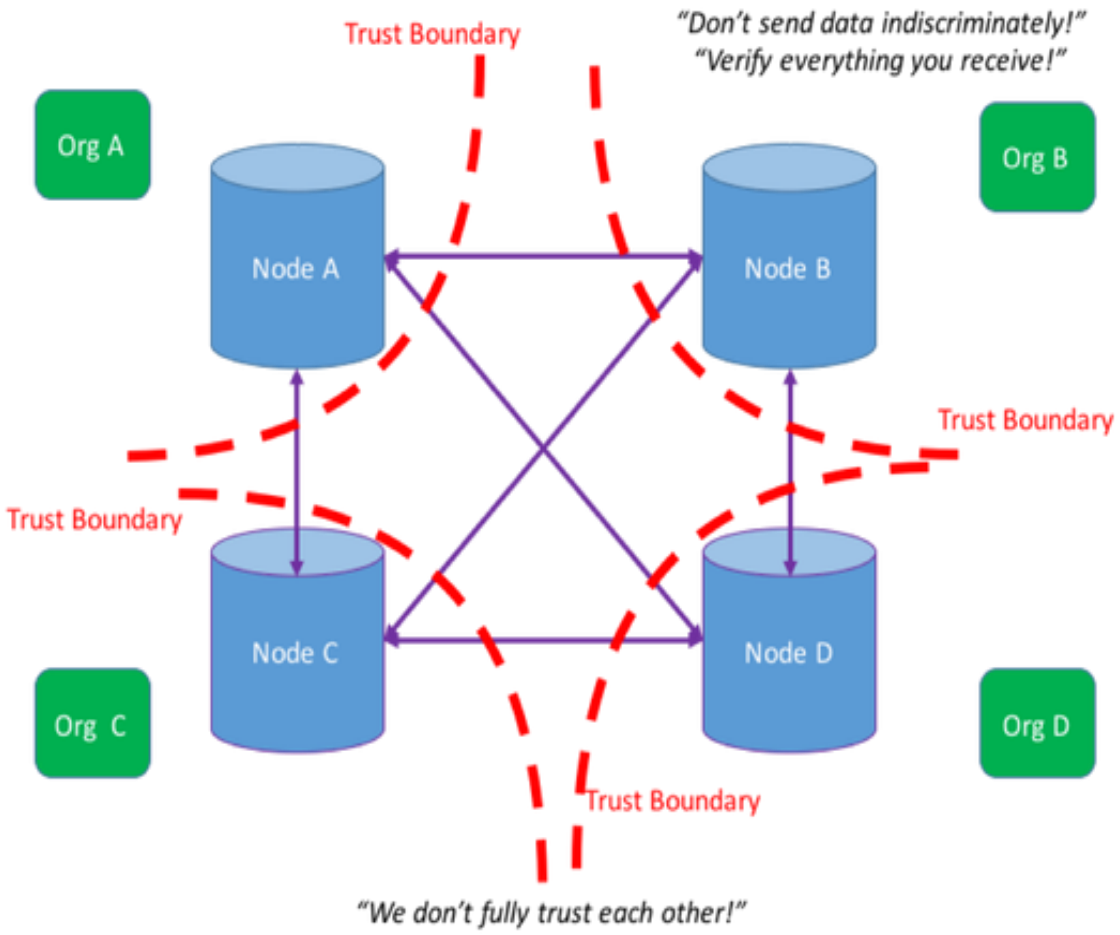
Распределённый реестр, на сегодняшний день, определяют чаще всего как некую базу данных, распределённую в компьютерной сети между различными центрами (нодами). Несмотря на общую схожесть данного определения с определением распределённой базы данных, распределённый реестр имеет ряд особенностей. В отличие от классической распределённой базы данных, где разные части базы хранятся на разных узлах, в распределённом реестре предполагается хранение всей полной и актуальной базы на каждом из нодов. Данная, на первый взгляд, избыточность обусловлена другой характеристикой распределённого реестра – отсутствием доверия пользователей друг к другу или к центру (см. [6]). Такие условия могут возникнуть, например, в случае, когда у пользователей базы данных имеются основания полагать, что центр, её администрирующий, имеет возможность манипулировать данными, нарушая их целостность и искажая информацию в них заложенную.

На рисунках 4 и 5 изображены диаграммы, схематично демонстрирующие распределённую базу данных и распределённый реестр.



Примечание – Node – узел, User – пользователь, Trust Boundary – границы доверия. Источник: [6].

Рисунок 4 – Диаграмма распределённой базы данных



Примечание – Node – узел, User – пользователь, Trust Boundary – границы доверия, Org – организация. Источник: [6].

Рисунок 5 – Диаграмма распределённого реестра

Красным пунктиром на диаграммах выше обозначены условные "границы доверия". В случае распределённой базы данных все ноды действуют в условиях полного доверия, когда как в случае распределённого реестра – доверие отсутствует, а каждый нод, за которым стоит отдельное независимое лицо/организация, требует верификации получаемых данных.

Исходя из вышеприведённой диаграммы, следует также добавить, что в условиях отсутствия доверия база данных, построенная по технологии распределённого реестра, представляет собой одноранговую пиринговую сеть. Таким образом, ноды при такой архитектуре базы становятся полноценно равнозначными участниками.

В отличие от традиционной базы данных, где вся ответственность за правильность отражаемой информации лежит на некотором центре, в

распределённом реестре все ноды участвуют в данном процессе. За счёт того, что каждый участник постоянно вносит новые записи в базу, возникает потребность в механизме, который сможет вовлечь каждый нод в процедуру согласования внесения изменений в базу, подменив, таким образом, функции центра в традиционной базе данных. Такой механизм носит название механизм (алгоритм) консенсуса.

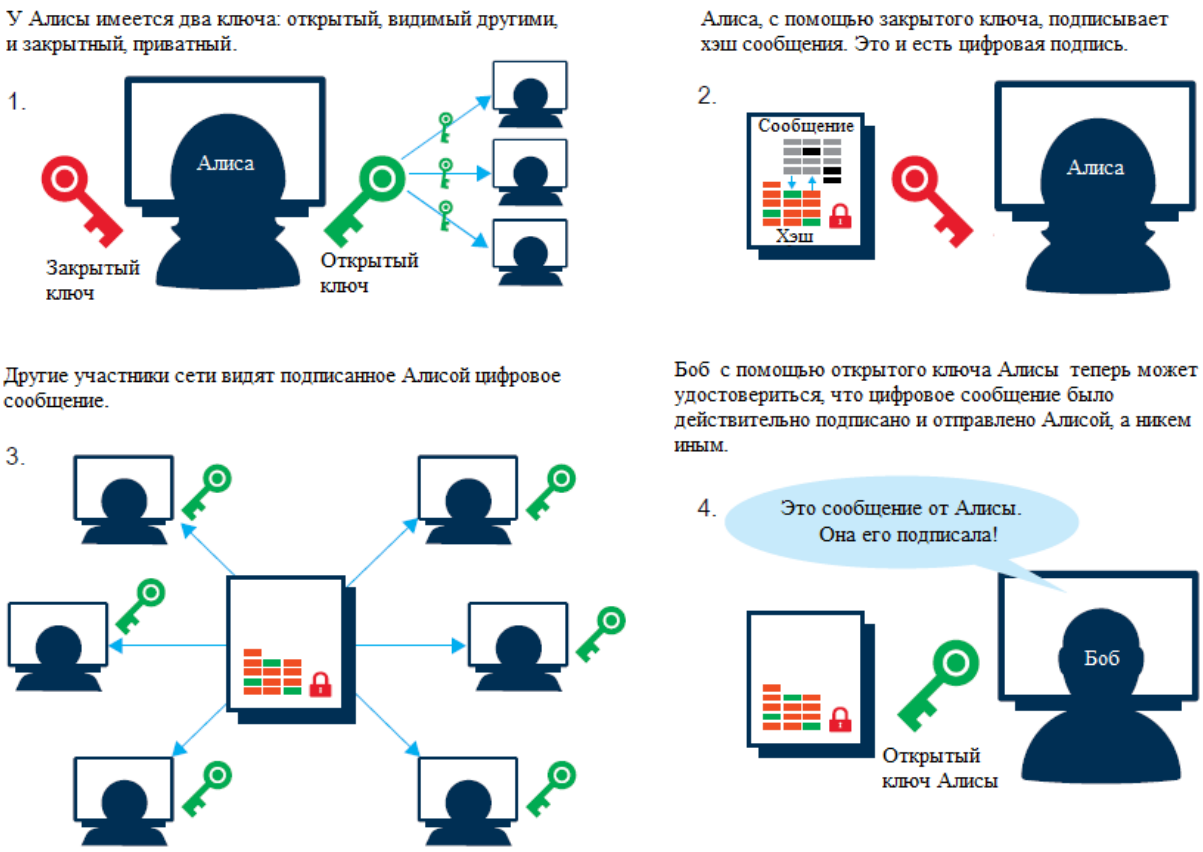
Механизм консенсуса представляет собой некий компьютерный алгоритм, который лежит в основе распределённого реестра. На сегодняшний день существует множество механизмом консенсуса. Выбор конкретного механизма обосновывается целями создания реестра, а также природой активов в нём отражённых. Задачей механизма консенсуса является определение легитимности (корректности) каждой производимой в базе транзакции и вынесение вердикта о возможности её проведения, с использованием заранее определённого метода криптографической валидации, принятого в данном распределённом реестре. Также, данный механизм автоматизирует процедуру выработки единого мнения среди участников сети относительно корректности отражения данных на текущий момент времени в распределённом реестре.

Другой важной задачей механизма консенсуса является разрешение конфликтов между некоторыми противоречащими транзакциями, проводимыми одновременно (т.н. проблема двойного расходования). Например, операция над каким-либо активом в базе, инициированная в один и тот же момент разными нодами. Механизм коненсуса, таким образом, обеспечивает последовательное выполнение всех транзакций, а также выполняет защитную функцию от захвата контроля над распределённым реестром группой лиц (нодов), для проведения некорректных (нелегальных, обеспечивающих, например, двойное расходование) транзакций (особенно, в случае общедоступного распределённого реестра).

Другой отличительной чертой распределённого реестра является активное, по сравнению с традиционными базами данных, использование криптографических методов. В первую очередь, речь идёт о криптографически стойкой хэш-функции (hash-function), которая представляет собой одностороннюю функцию $h(k)$, которая преобразовывает массив входных данных произвольной длины k в битовую строку установленной длины. Например, продемонстрируем работу хэш-функции на 128-

битного алгоритма хэширования MD5. Если $k = \text{"привет"}$, то в результате получим значение $h(k) = 608333adc72f545078ede3aad71bfe74$. Для сравнения, если в исходном k будет изменён хотя бы один байт, то $h(k)$ примет кардинально иное значение. Пусть $k = \text{"превет"}$, тогда значение $h(k) = f75c47b64316ce38ac04ec72b0ae0a98$. При этом стоит отметить, что, зная выходное значение функции, входное значение k идентифицировать вычислительно сложно за любое мыслимое время.

Вторым технологическим аспектом, связанным с криптографией в распределённом реестре, является использование пары цифровых закрытого и открытого ключей. Открытый ключ является производным от закрытого, причем создаётся также с помощью некоторой односторонней криптографически стойкой функции. Данная пара ключей служит аналогом обычной подписи на физических документах и выполняет, по сути, ту же самую функцию. Продолжая аналогию с физической подписью, можно условно сравнить открытый ключ с тем, как подпись выглядит на бумаге, а закрытый ключ – непосредственно с рукой подписанта. Наблюдая открытый ключ, получатель имеет все основания полагать, что входящее сообщение/транзакция было подписано именно с помощью закрытого ключа определённого подписанта. Иллюстрация использования цифровой подписи в условиях распределенного представлена на рисунке 6.



Примечание – Источник: [7].

Рисунок 6 – Использование концепции цифровой подписи в условиях распределённого реестра

Как продемонстрировано выше на рисунке, при отправке некоторого цифрового сообщения Алиса использует свою пару открытого и закрытого ключей. Закрытый ключ используется для осуществления непосредственной подписи сообщения на этапе отправки, в то время как открытый ключ – для проверки этой подписи получателем. В случае если данная проверка пройдена, Боб с помощью своего закрытого ключа может одобрить это сообщение/транзакцию, и тогда информация о ней будет выставлена в условную очередь на одобрение другими узлами с помощью механизма консенсуса. После одобрения сети, данное сообщение/транзакция будет внесено в реестр и реплицировано на его копии всем остальным участникам сети.

Еще одной важной особенностью распределённого реестра является хранение всей истории транзакций. В отличие от традиционных баз данных, в которых основной единицей учёта является актуальное состояние или значение какого-либо

атрибута, основной единицей учёта распределённого реестра является транзакция. Имея в распоряжении всю историю транзакций, можно узнать текущее значение того или иного атрибута. В связи с этим фактом распределённые реестры считаются необратимыми базами, так как изменение уже завершившихся транзакций, имеющих подписанное цифровой подписью определённое значение хэш-функции, невозможно. Хэш от подписанной транзакции, которая, например, представляет собой договор о передачи какого-либо актива от одного лица другому, наблюдается всеми участниками сети и одобряется механизмом консенсуса, действующим в данном распределённом реестре. Раз одобренная транзакция не может быть изменена, так как изменения хотя бы одного символа в свойствах транзакции приведёт к кардинальному пересчёту значения хэш-функции. Так как каждый нод хранит у себя копию базы, то такое изменение станет в ту же секунду известно остальным участникам. Аналогичным образом невозможно провести и процедуру удаления или отмены транзакции, если она уже однажды была одобрена другими нодами в процессе работы механизма консенсуса. Следовательно, любое изменение базы данных распределённого реестра может быть осуществлено лишь с помощью новой транзакции, удаление же или внесение правок, особенно в открытых публичных реестрах – невозможно.

Стоит также отметить, что информация в распределённом реестре, в большинстве случае, носит псевдоанонимный характер, особенно в случае открытого децентрализованного реестра. Так как все участники могут просматривать всю базу транзакций, зная, какое лицо стоит за тем или иным неким идентификационным номером (в сети Биткоин, например, это номер кошелька), любой может проследить историю транзакций интересуемого лица. Таким образом, раз поучаствовав в какой-либо транзакции, учтённой в реестре, анонимность нарушается, ведь теперь обе стороны транзакции знают, кому принадлежат данные кошельки/учётные записи.

1.3 Блокчейн

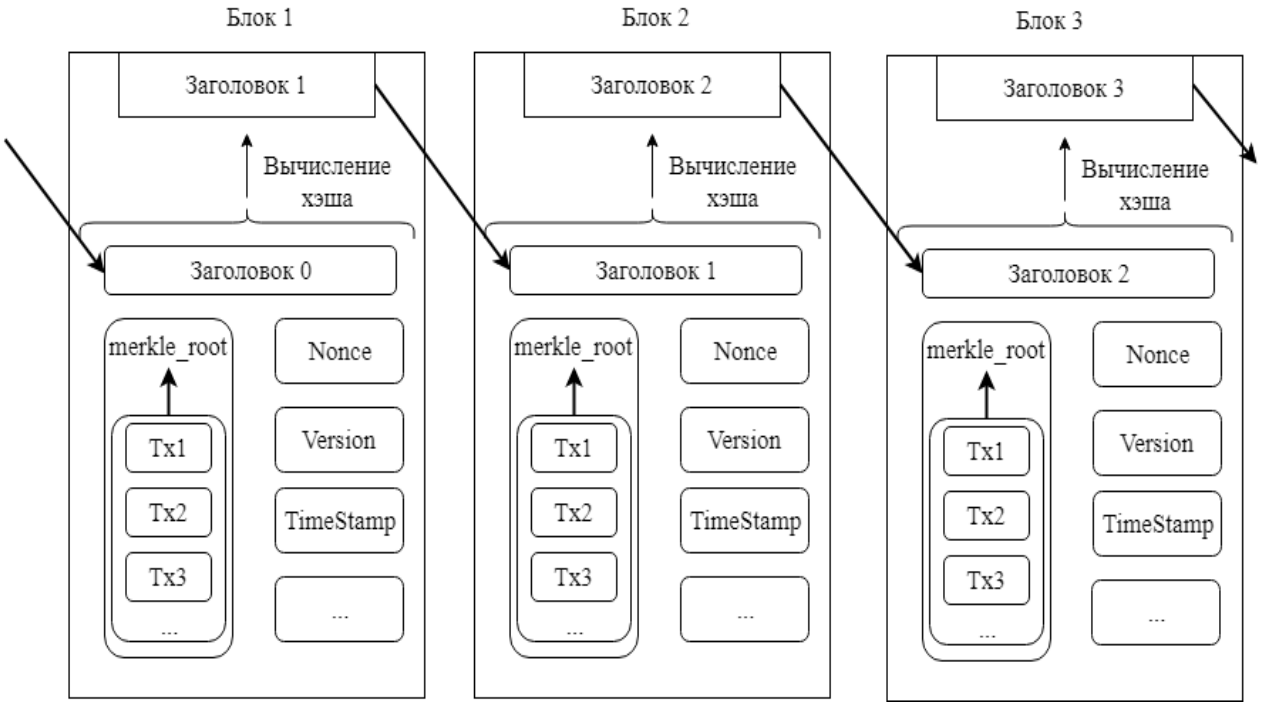
Разобравшись с основными отличиями распределённого реестра от традиционных баз данных и определив его отличительные черты, рассмотрим теперь самый первый и до сих пор самый популярный вид распределённого реестра

– блокчейн. Как уже выше было сказано, первый блокчейн был создан для обслуживания криптовалюты Биткоин, на примере которого и будет рассмотрен данный вид распределённого реестра.

Блокчейн, как следует из самого названия, представляет собой цепочку блоков. Каждый блок содержит в себе набор из совершенных в течение определённого периода времени (в биткоине это 10 минут) транзакций. Транзакции в сети Биткоин представляют собой записи, которые фиксируют передачу какого-либо количества биткоинов от одного пользователя другому. Соответственно, транзакция считается одобренной и выполненной, если она включена в какой-то блок. Всего размер блока составляет 1 Мб, средний размер записи о транзакции – 495 байт, следовательно 1 блок содержит запись о порядка двух тысячах транзакций.

Стоит отметить, что в блок заносится не сама транзакция, а некоторое 32-ух битное значение, обозначаемое в биткоине как корень Меркла (merkle_root). Данное значение высчитывается с помощью метода построения дерева Меркла (Merkle tree), представляющего собой процесс построения древовидный иерархии, в котором каждый новый уровень является значением хэш-функции от каких-то двух хэшей предыдущего уровня. На самом нижнем уровне дерева находятся значения хэш-функции от информации, содержащихся в самой транзакции (хэш от записи вида «А передал Б 10 биткоинов»). На один уровень выше высчитывается значение хэш-функции от хэшей двух транзакций. Таким образом, на самом верхнем уровне оказывается некоторый хэш, который и является тем значением корня Меркла, заносимым в блок.

Помимо хэша от набора транзакций, блок содержит так называемый заголовок (block header), уникальный для каждого блока. Его уникальность достигается за счёт того факта, что каждый заголовок является значением хэш-функции, носящей название SHA256, от информации, хранящейся в нём: списка транзакций, некоторых технических атрибутов (временной метки создания блока, версии биткоина, текущей сложности вычисления блока, nonce и др.), а также, что важно, от заголовка предыдущего блока. Таким образом, через последовательный учёт заголовков предыдущих блоков в вычислении заголовка нового осуществляется их связь, создается цепочка блоков. Схематичное изображение блокчейна представлено на рисунке 7.



Примечание – Блоками Tx1, Tx2, Tx3 условно обозначены транзакции, учёт которых с помощью построения дерева Меркла даёт значение хэш-функции merkle_root (корень Меркла). Nonce – некоторое числовое значение для перебора. Version – текущая версия Биткоина. TimeStamp – временная метка.

Рисунок 7 – Схема блокчейна

Блокчейн, на котором построен Биткоин, представляет собой полностью децентрализованный одноранговый распределённый реестр. Следовательно, сам блокчейн, цепочка блоков, представляет собой некоторый файл, копии которого находятся на всех нодах одновременно, то есть у всех участников сети, и синхронизируются друг с другом в режиме реального времени. На сегодняшний день блокчейн Биткоина занимает 181,05 Гб на жестком диске и, очевидно, что далеко не каждый из более чем 11 млн. пользователей данной криптовалюты готов выделить столько места на своём жестком диске. Для этого существуют специальные сайты и легковесные клиенты, позволяющие пользоваться биткоином без скачивания непосредственно базы. В данный момент, в сети регистрируется немногим более 10 тыс. полноценных нодов, хранящих весь блокчейн Биткоина. Так как же происходит процесс добавления новых блоков в цепочку и синхронизация между всеми этим нодами?

1.4 Задача о византийских генералах

Задача нахождения консенсуса (единого мнения относительно валидости текущего состояния данных, а также легитимности проведения транзакций) в распределённой децентрализованной сети восходит к работе [8], посвященной анализу надёжности децентрализованной системы. Авторы формализовали проблему в следующем виде.

Допустим, византийская армия осаждает некоторый вражеский город. Армия разделена на некоторые боевые единицы (полки, дивизии), каждой из которых командует свой генерал. К утру генералы должны прийти к общему решению относительно дальнейших действий (штурм или отступление). Однако среди генералов могут оказаться предатели, которые будут мешать выработке единого решения относительно плана на утро. Следовательно, существует 3 возможных исхода: если все верные генералы атакуют, то город будет взят; если все верные генералы отступят, то армия останется целой; если некоторые верные атакуют, а другие верные отступят – армия будет разгромлена. Итоговое решение достигается посредством обмена информации между генералами относительно состояния своего войска, а также оценки вражеских сил посредством некоторого условного “мессенджера” (например, голубиной почты или гонцов). Таким образом, возникает задача определения, сколько максимально в армии может быть генералов предателей, чтобы армия всё равно пришла к единому мнению?

В той же работе [8] было показано частное решение такой задачи с помощью определённого рекурсивного механизма, положенного в дальнейшем в основу семейства протоколов Paxos для достижения консенсуса в сети ненадёжных вычислений. В итоге, авторы получили результат, что единый консенсус будет найден в случае, если предателей среди генералов строго не больше одной трети. Стоит отметить, что в том виде полученный результат был, скорее, теоретическим и на практике был труднореализуем.

Следующий виток развития в дискуссии о решении такого рода задачи был дан работой [9], в которой был теоретически описан первый практически реализуемый алгоритм, устойчивый к проблеме византийских генералов (Practical Byzantine Fault Tolerance Algorithm, PFBT). Данный алгоритм способен обеспечить передачу огромного массива прямых сообщений между участниками в

одноранговой сети с минимальной задержкой. Это открыло возможности практической реализации алгоритма в различных компьютерных приложениях, в том числе и в качестве механизма консенсуса в некоторых современных распределённых реестрах.

Тем не менее, первым реализованным на практике механизмом консенсуса, который в условиях открытой одноранговой сети в форме распределённого децентрализованного реестра смог обеспечить устойчивость к проблеме византийских генералах, стал алгоритм, используемый в блокчейне Биткоина.

1.5 Доказательство работы

Механизм консенсуса, используемый в блокчейне Биткона, носит название «доказательство работы» (Proof-of-Work). Суть его заключается в том, что полноценные ноды участвуют в своего рода соревновании за первенство генерации каждого нового блока. Оно также носит названия майнинга (mining, добыча). Наградой в таком соревновании является некоторое число биткоинов (на сегодняшний день - 12.5 + комиссии от транзакций). Само по себе состязание заключается в попытке подобрать некоторый хэш определённой сложности, который будет служить заголовком нового блока. Сложность определяется самим алгоритмом в зависимости от совокупной вычислительной мощности всех нодов и корректируется каждые 2016 блоков (раз в две недели). Это делается для того, чтобы поддерживать на стабильном уровне частоту добавления нового блока в цепь (раз в 10 минут). Соответственно, будь в сети Биткоин хоть 5 участников с обычными домашними персональными компьютерами или миллион суперкомпьютеров, – блоки будут генерироваться в среднем раз в 10 минут.

Сама по себе сложность представляет собой определённое правило того, как должен выглядеть хэш, служащий заголовком блока. Сам хэш представляет собой набор из 64-ех буквенных и числовых символов, а сложность регулирует количество нулей в его начале. Например, в 2010 году начало заголовка должно содержать 8 нулей, а в 2018 уже 19, что говорит о значительном приросте мощностей в сети Биткоин. Типичный заголовок блока выглядит так«000000000000000000fc05c87cb16c87e2988984a60332d209b928a7 4d8bff5».

Сам процесс подбора хэша заключается в следующем. У участника сети, желающего помайнить, по большому счету, есть две переменные в свойствах блока, которые он может варьировать с целью подбора заголовка нужного вида: это корень Меркла и Nonce[1]. В зависимости от того, какие транзакции будут включены в блок, корень Меркла будет принимать разные значения, что, как видно на вышеприведённом рисунке 7, влияет на хэш заголовка. Тем не менее, стандартной практикой является набор в блок транзакции из списка ожидания с самой большой комиссией, которая также является прибавкой к награждению майнеру за генерацию блока. Основной процесс майнинга, следовательно, заключается в простом переборе числового значения Nonce до тех пор, пока заголовок блока не будет выглядеть надлежащим образом.

После выполнения всех необходимых условий, майнер публикует блок с указанием всех необходимых атрибутов, включая найденное значение Nonce. Зная все атрибуты, полные ноды в автоматическом режиме перепроверяют, действительно ли при таких входных данных и таком значении Nonce, хэш заголовка будет выглядеть именно так, а не иначе. После подтверждения майнеры переключаются на генерацию нового блока, а автор только что созданного получает на свой электронный биткоин-кошелек награду в виде 12.5 биткоинов (в последствии это число будет уменьшаться) и комиссии от включённых транзакций, причём награда будет получена автором лишь после того, как от его блока будут сгенерированы и подтверждены еще более 100 блоков. Данная премия в 12.5 биткоинов и представляет собой эмиссию новых биткоинов, размер которой детерминирован во времение и которая происходит в среднем каждые 10 минут.

Вполне возможно представить ситуацию, когда два майнера одновременно сгенерировали подходящие блоки, что вызывает раздвоение цепи. Тогда главной цепочкой будет считаться та, ответвление которой будет быстрее продолжено (см. рисунок 8).

[1] Nonce представляет собой некоторое число (следует рассматривать просто как набор символов), которое при приоединению к интересующему нас набору символов (текст транзакции) доставляет значение хэш-функции с заданными ограничениями.

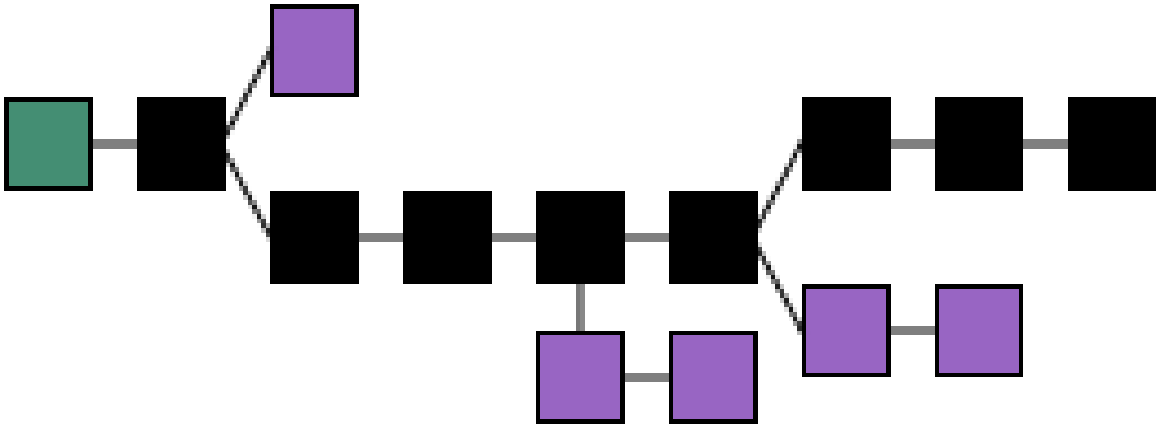


Рисунок 8 – Случай раздвоения цепочки блоков

На рисунке 8 зелёным отмечен исходный блок, чёрным – главная цепочка, фиолетовым – ответвления. Считается, что транзакция считается окончательно проведённой, если от блока, в котором она учтена, цепь блоков продлена хотя бы еще на 6 блоков. В противном случае, если транзакция по передачи некоторого количества биткоинов оказалась в отвергнутой цепочке, она становится недействительной и автоматически становится в очередь на подтверждение при генерации текущего блока. Соответственно, майнер, сгенерировавший отвергнутый блок в блокчейне Биткоина, никакого вознаграждения не получает, в отличие, например, от работы блокчейна Ethereuma, где сгенерировавший отвергнутый блок майнер всё равно получает некоторое количество валюты.

Доказательство работы считается относительно эффективным в плане предотвращения двойного расходования механизмом консенсуса. В централизованных системах создание двух транзакций, например, передающих один и тот же актив двум разным агентам невозможно в силу наличия центра, не позволяющего проведения такого рода транзакций. В блокчейне Биткоина, при подборе транзакций в блок, в случае, когда один и тот же биткоин был отправлен двум разным адресатам, возникнет конфликт, и в блок попадает лишь одна из этих транзакций. Тем не менее, существует теоретическая возможность того, что двойное расходование может быть проведено, если какое-то лицо или группа лиц будет контролировать более 50% вычислительных мощностей сети (т.н. «атака 51%»), так как в таком случае вероятность поддержания ложной цепочки блоков некоторой длины становится существенной (фактически мы получаем цепь испытаний

Бернулли, где нежелательная для нас вероятность больше 50%, что делает возможным принять ответвление из нескольких ложных некорреткных блоков большинством пользователей и вписать его в блокчейн как завершённые транзакции).

Допустим, в некоторый блок 1 попала транзакция, содержащая информацию, что А передал 1 биткоин Б, например, в счёт оплаты некоторой услуги. При этом существует другая транзакция, по которой А передал этот же 1 биткоин С. Первая транзакция попадает в блок 1, который подтверждается сетью, в то время как группа лиц, контролирующая 51% мощностей тайно создает параллельный блок 1а, в который включается вторая транзакция. Произойдёт разделение цепи, причем злоумышленники могут не публиковать блок в открытую так, что вся сеть не будет знать о раздвоении и будет считать блок 1 единственно верным блоком. Злоумышленники, при этом, продолжат генерировать блоки параллельной скрытой цепи. Так как мощностей у этой группы больше, то вполне вероятно, что они действительно успеют намайнить параллельную цепь быстрее, чем честные агенты - основную. В какой-то момент скрытая цепь будет опубликована и окажется длиннее, а значит – станет основной. Транзакция по передаче от А 1 биткоина Б станет недействительной, хотя услуга по ней уже будет оказана, а действительной окажется передача 1 биткона от А к С. На практике же, лишь единожды в 2014 году пул майнеров (объединение майнеров, которые решают задачу нахождения хэша посредством совокупной распределённой вычислительной мощности каждого участника пула) Ghash.io получил контроль над 55% мощностей сети Биткоин, что вызвало падение курса криптовалюты на 25%, а пул обязался снизить свои мощности до 40%. Тем не менее, как таковой атаки не произошло.

С другой стороны, потенциальной уязвимостью, с которой также хорошо справляется доказательство работы, является возможность изменения задним числом уже одобренной транзакции. Однако, при изменении хотя бы одной транзакции в блоке, значение хэш-функции в заголовке блока изменится. Так как этот хэш используется в вычислении заголовка следующего блока, то у всей последующей цепочки блоков, вплоть до последнего, изменятся заголовки. Так как изменение в прошлую транзакцию вносится каким-то отдельным лицом, то его цепь будет игнорироваться оставшейся цепью, так как заголовки будут не

соответствовать правилу о нескольких нулях в начале. Единственное, как возможно распространить скорректированную версию блокчейна – это пересчитать по новой все хэши, чтобы они удовлетворяли заданным условиям. Это, однако, невозможно, так как займёт очень много времени, и злоумышленник просто не сможет догнать сеть, которая как минимум с такой же скоростью, с которой прошлый блок переписывается, будет добавлять в цепь новый.

На сегодняшний день консенсус «доказательство работы» зарекомендовал себя как самый надёжный и защищённый механизмом консенсуса для открытого, публичного и децентрализованного распределённого реестра в форме блокчейна (см. например [10]). Тем не менее, несмотря на все плюсы, данный алгоритм имеет и ряд недостатков.

В первую очередь, недостатком доказательства работы называют его высокую энергозатратность. Например, по данным исследования [11] прогнозируется, что к концу 2018 года затраты на майнинг только лишь биткоинов достигнут 0,5% (7,67 ГВт) от общего энергопотребления планеты. В настоящий момент, на майнинг данной криптовалюты приходится порядка 2,55 ГВт электричества, что сопоставимо с потреблением электричества Ирландией (3,1 ГВт), а уже в Исландии на майнинг тратится больше электричества, чем потребляют обычные граждане страны.

Вторая главная проблема доказательства работы, это скорость фиксируемых в системе транзакций. Обычно, данный аргумент используется в рамках дискуссии о перспективах криптовалют в качестве полноценных платёжных средств. Например, самые популярные криптовалюты Биткоин и Эфир (Ethereum) могут проводить 7 и 20 транзакций в секунду, плюс время ожидания на подтверждение нескольких следующих блоков в цепи для полной уверенности в проведении платежа. Для сравнения, централизованная система Visa проводит 24 тыс. транзакций в секунду. С точки зрения платёжных средств, такая медлительность децентрализованных реестров в виде блокчейна играет значительную роль. Если же абстрагироваться от криптовалют и говорить о построении некоторой базы данных на блокчейне, то такая скорость фиксирования транзакций, например, по передаче прав на какой-либо актив может быть вполне приемлемой.

Блокчейн Биткоина, использующий доказательство работы в качестве механизма консенсуса, является самым знаменитым распределённым реестром. Его

основными особенностями являются полная децентрализация и открытость. Открытость заключается в том, что никто не контролирует доступ для участия в процессе обмена биткоинами, а также никто не ограничивает доступ к чтению всей базы транзакций. Любой пользователь может свободно скачать весь блокчейн, создать учётную запись (кошелек) и начать майнить биткоины. Для такого открытого и децентрализованного реестра механизм доказательства работы является лучшим вариантом, так как гарантирует надёжность данных.

Тем не менее, большое количество имплементаций технологии распределённого реестра в различных областях экономики, как в частном, так и в государственном секторе, не отвечают принципам открытости и децентрализации, которые воспринимаются многими крипто-энтузиастами в качестве необходимых условий функционирования таких систем. Однако внедрение, например, блокчейна даже с нарушением данных принципов может значительно повлиять на эффективность ведения бизнеса, удобства предоставления государственных услуг и проч. В связи с этим представляется важным представить некоторую классификацию видов распределённых реестров.

1.6 Виды распределённых реестров

Многие эксперты и исследователи предпринимали попытку классификации видов распределённого реестра (см. например [7], [12], [13] и [14]). Несмотря на употребление несколько разных терминов, в целом все исследователи сходятся к некоторому общему мнению относительно классификации распределённых реестров.

От целей, для которых создаётся распределённый реестр, зависит степень его открытости и централизации. Данные параметры, в свою очередь, влияют на выбор оптимального механизма консенсуса.

По степени открытости распределённые реестры могут быть открытые (permissionless) и закрытые (permissioned). Открытый реестр, например, блокчейн Биткоина или Эфира, как уже было сказано выше, не имеет механизма отбора участников, т.е. любой пользователь может присоединиться к сети и не может быть никоим образом ограничен в доступе к ней. В закрытом реестре, напротив, доступ предоставляется лишь тем лицам, кто удовлетворяет некоторым заранее заданным

требованиям и/или чья кандидатура одобряется владельцем или администратором распределённого реестра. Закрытый реестр, таким образом, является довольно привлекательным вариантом для правительства и регуляторов, так как даёт возможность однозначно идентифицировать участников и контролировать доступ к сети, например, посредством процедуры регистрации или выдачи лицензий. Такие реестры также легче поддаются регулированию. Обратной стороной, конечно же, является жертва главным преимуществом распределённого реестра – способности функционировать без какого-либо координационного центра. Тем не менее, закрытый распределённый реестр не обязательно предполагает наличие центрального органа, контролирующего проведение всех транзакций – ограничение может быть только на вход, тогда как внутри реестра все участники всё равно остаются в равном положении.

По степени централизации распределённые реестры бывают децентрализованными (публичными, public), частично централизованными (федеративными, federated) и полностью централизованными (частными, private). Из описания работы блокчейна Биткоина становится очевидно, что полностью децентрализованный распределённый реестр предполагает, что валидацией транзакций могут занимаются все участники сети. Также такие реестры обычно являются открытыми. Если, однако, такой реестр имеет ограничения на вход, то есть является закрытым, и/или валидацией транзакций занимается лишь ограниченное число нодов (т.е. список таких нодов представляется относительно закрытым), то распределённый реестр считается частично централизованным. Закрытый частично централизованный распределённый реестр также носит название «консорциум» (consortium). Если же валидацией транзакций в реестре занимается отдельный выделенный центр, то такой реестр является полностью централизованным.

Таким образом, выше приведённые идеи можно формализовать с помощью следующей схемы (см. рисунок 9).

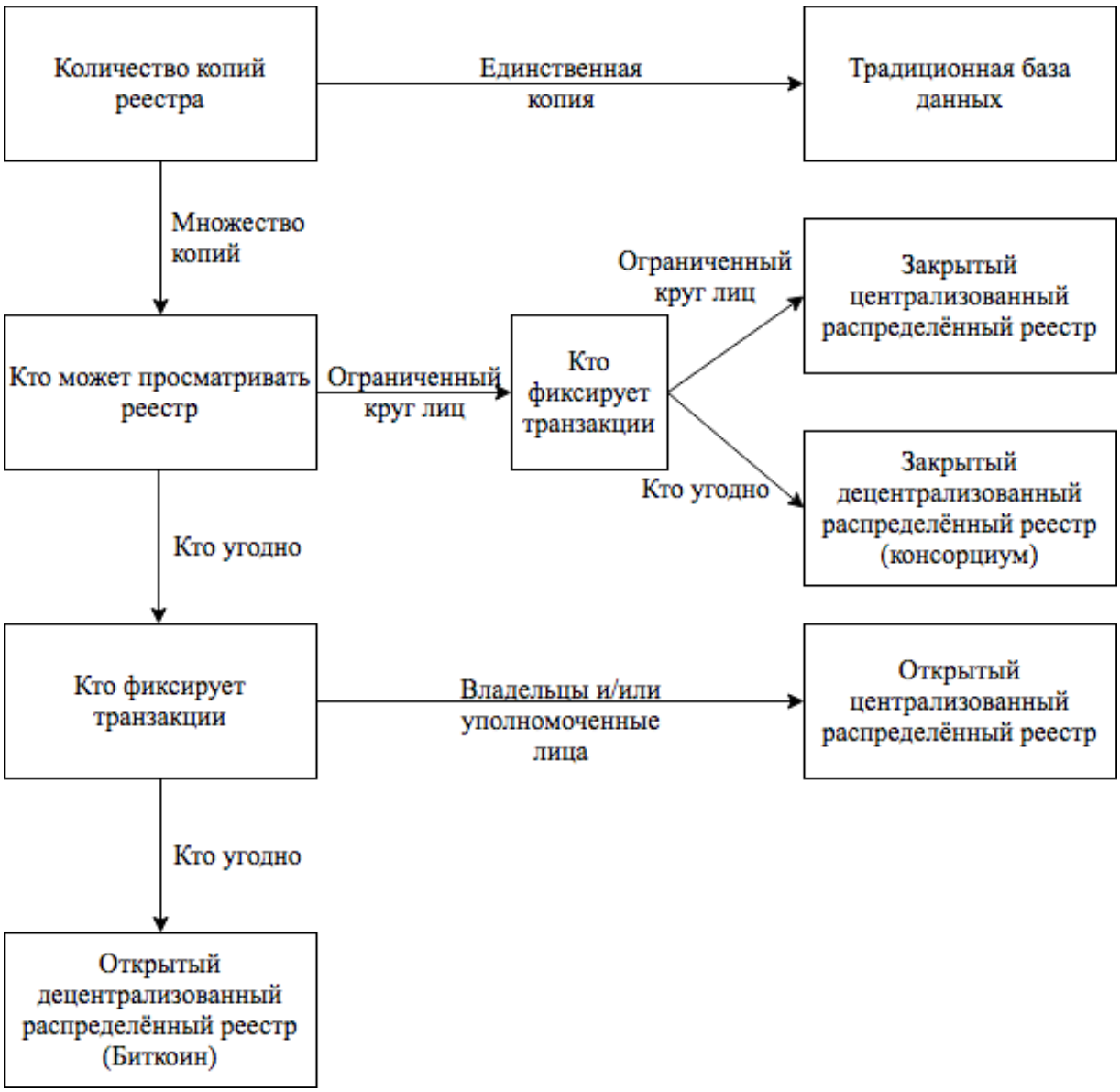


Рисунок 9 – Виды распределённого реестра по степени открытости и централизации

Очевидно, что описанный выше алгоритм консенсуса в форме доказательства работы, используемый в Биткоине, Эфире и ряде других криптовалют, является избыточным для некоторых видов распределённого реестра. Например, в закрытом централизованном реестре нет смысла некоторому уполномоченному лицо тратить большие вычислительные мощности только для того, чтобы подобрать хэш, отвечающий некоторым требованиям. Это лицо ни с кем не конкурирует за награду и имеет возможность, при желании, даже переписать информацию во всей цепочки блоков, так как оно единственное занимается майнингом. Конечно, эти изменения могут быть зафиксированы другими участниками в сети. Тем не менее, сам механизм майнинга в данном случае является избыточным.

В связи с этим, а также с попыткой решить описанные выше проблемы механизма доказательства работы, свет увидели другие алгоритмы консенсуса. Какие-то из них лучше всего применимы лишь к каким-то отдельным видам распределённого реестра с учётом открытости и централизации, другие являются более универсальными. Как уже было сказано выше, на сегодняшний день самым надёжным механизмом консенсуса для публичных децентрализованных реестров многими всё равно считается именно доказательство работы, хотя альтернатив, на которых строятся в том числе и некоторые другие криптовалюты и блокчейн-платформы, существует масса.

1.7 Доказательство владения и альтернативы

Вторым по популярности алгоритмом консенсуса на сегодняшний день является механизм доказательство владения (proof-of-stake, другое название – подтверждение доли). Основным мотивом его появления послужила обеспокоенность широкой общественности огромными вычислительными мощностями, которые тратятся “впустую” при майнинге криптовалют, основанных на доказательстве работы. В итоге, вместо использования вычислительных мощностей компьютера, в данном алгоритме консенсуса доминантой оказывается количество криптовалюты/токенов на балансе отдельного участника. Иными словами, если при использовании доказательства работы вероятность подобрать заголовок следующего блока зависит от располагаемой вычислительной мощности, то при использовании доказательства владения вероятность прямо пропорционально зависит от баланса пользователя. За счёт отсутствия сложных вычислительных задач, формирование блоков с помощью механизма доказательства владения осуществляется быстрее, чем при доказательстве работы, что увеличивает общую пропускную способность (в смысле количества транзакций в секунду) распределённого реестра.

Стоит отметить, что в первой криптовалюте Peercoin, внедрившей данный механизм консенсуса в 2012 году, учитывается не только непосредственное количество монет на счету, но и срок их хранения. Если у пользователя имеется 10 криптомонет, которые лежат на его счету 20 дней, то для целей генерации нового блока считается, что его “ставка” равняется 200 единицам. В случае траты этих 10

монет, счётчик обнуляется, и пользователь уже не может претендовать на участие в формировании нового блока. В случае же использования этих монет в генерации блоков, они “замораживаются” на счету после успешной генерации блока до тех пор, пока цепь блоков не будет продолжена далее. Если сформированный блок содержит какие-либо нелегитимные, с точки зрения других участников, транзакции, то данная цепочка отбрасывается, а замороженные средства пользователя, его создавшего – пропадают.

С одной стороны, очевидно, что возможна ситуация, в которой б*о*льшую часть монет в системе будет контролировать одно лицо, что приведёт к её централизации. Такое лицо будет иметь возможности манипулировать информацией в блоках и получит контроль над сетью. С другой стороны, теоретически можно предполагать, что злоумышленнику это будет невыгодно, так как приведёт к неустойчивости сети, падению доверия к валюте, понижению её курса, что, в первую очередь, ударит по тому, кто владеет самым большим её количеством. Впрочем, сама ситуация, когда больше 51% валюты находится в руках одного лица является труднодостижимой: для этого злоумышленнику придётся закупать монеты у других пользователей, что приведёт к росту курса и повышению затрат на её приобретение.

Другой важный аспект алгоритма доказательства владения – это отсутствие майнинга как такового. Процесс генерации нового блока в цепи, порой, при использовании данного механизма консенсуса, называют форджингом (forging – ковка). При этом в процессе создания блока не происходит добыча нового количества криптовалюты – в качестве вознаграждения выступает лишь комиссия от включённых в блок транзакций. Однако данный аспект поднимает очевидный вопрос, а как вообще, в таком случае, возникают монеты/токены/активы в таком реестре?

Один из вариантов – по аналогии с первичным размещением акций провести первичное размещение токенов/монет в определённом объёме, который впоследствии может быть увеличен новыми раундами размещения. В криптовалюте Peercoin был использован именно второй вариант. Аналогичным образом, создатели Эфира сейчас работают над механизмом консенсуса Casper (см. [15]), представляющий собой слегка модернизированный алгоритм доказательства владения, чтобы в будущем заменить им текущий механизм доказательства работы.

Другой вариант – это комбинирование обоих механизмов консенсуса (доказательства работы и доказательства владения) на постоянной основе. Такая комбинация, например, реализована в криптовалюте Emercoin, а также в корпоративных блокчейн-решениях, предлагаемых одноимённой компанией. Большая часть блоков (около 80%) в такой сети формируется с помощью доказательства владения и лишь некоторые (оставшиеся 20%) за счёт доказательства работы. Таким образом, для атаки на такую сеть злоумышленнику потребуется одновременно более 51% вычислительных мощностей всей сети и более 51% всех монет, что представляется крайне дорогостоящим предприятием.

Доказательство активности (Proof-of-Activity) представляет собой другой комбинированный механизм консенсуса, сочетающий в себе доказательства работы и владения. Описанный первый раз в работе [16] и реализованный, например, в проекте Decred, данный алгоритм представляет собой процедуру, в которой сначала майнер находит подходящий заголовок нового блока посредством подбора значения Nonce (часть доказательства работы), проект которого утверждается некоторым случайным количеством других участников (часть доказательства владения). Так как каждая монета (а точнее самая малая её часть, например, 0.00000001 монеты) имеет свой номер в блокчейне и её движение можно отследить с момента появления до текущего владельца, алгоритмом случайно выбирается одна такая монета и все, через чьи кошельки она хоть раз проходила, участвуют в одобрении нового блока. В работе [17] данная процедура носит название chain of activity, в других источниках (см., например, [16]) также встречается название follow-the-satoshi (“следуй за сатоши”, сатоши – самая малая часть биткоина, условно говоря, копейка от рубля). Таким образом, чем в большем количестве транзакций поучаствовал пользователь сети и/или чем больше монет у него находится в кошельке, тем выше вероятность его участия в процедуре принятия нового блока. Так как блок всё-таки является результатом процедуры майнинга, то награда за блок распределяется в пропорции 60% - майнеру, 30% - сторонам согласования и 10% - владельцам всего проекта Decred.

Также, в некоторых криптовалютых, например EOS, BitShares и Steem, используется несколько видоизменённый вид доказательства владения – делегированное доказательство владения (Delegated Proof-Of-Stake, DPoS). Суть

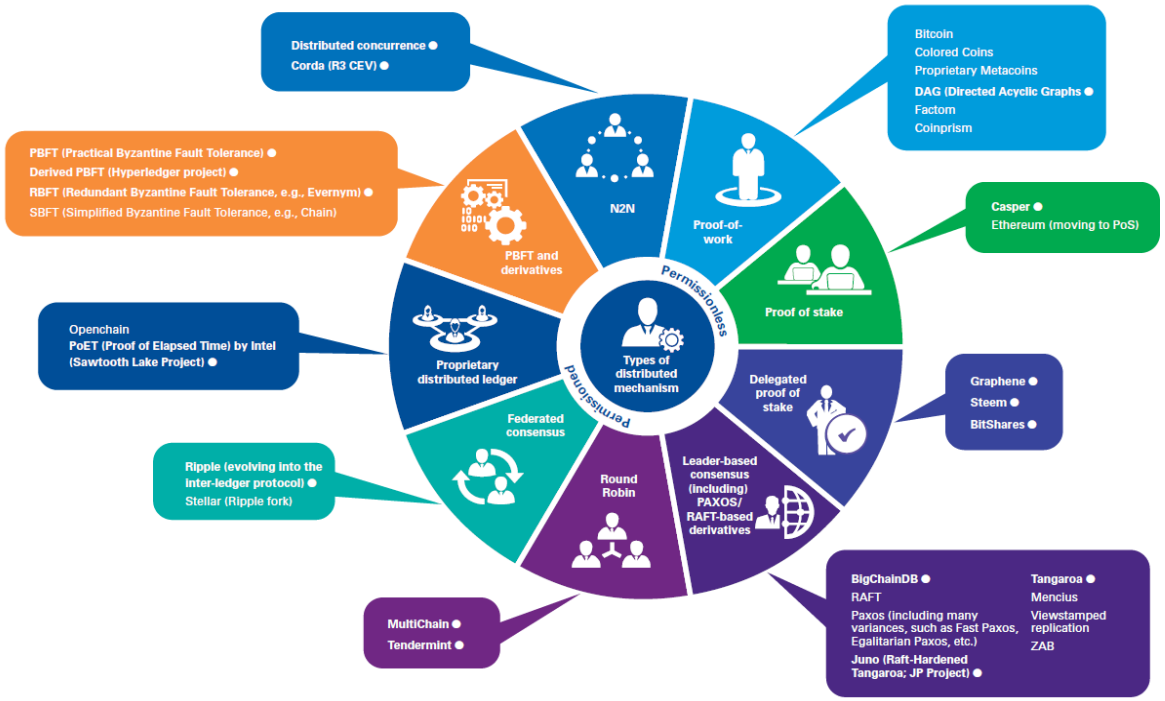
заключается в том, что теперь держатели “замораживают” свои средства не для того, чтобы повысить вероятность своего участия в генерации нового блока, а как инструмент голосования для выбора тех, кто будет заниматься генерацией блоков. Например, в блокчейне криптовалюты EOS существует 20 избираемых должностей валидаторов транзакций, еще 1 отбирается случайным образом. Пул валидаторов обновляется каждую минуту, а блок принимается, если его одобрили 50%+1% валидаторов. Выбор того, кто конкретно генерирует блок определяется некоторым псевдорандомным алгоритмом. Причём на вероятность быть отобранным одним из 21 валидаторов для генерации следующего блока не зависит от количества монет на счету и времени, проведённым в качестве валидатора и проч. Стоит отметить, что, несмотря на кажущуюся сложность, алгоритм работает автоматически, почти моментально, а новые блоки генерируются каждые 1-3 секунды, обеспечивая высокую скорость проведения транзакций. При этом обычный участник может в любой момент отдать свой голос другому кандидату в валидаторы. Таким образом, за счёт наличия системы голосования предотвращается возможность захвата блокчейна узким кругом лиц. С другой стороны, будучи в своей природе демократическим механизмом, не исключена возможность сговора между владельцами большого количества токенов и делегатами, своего рода лоббизм интересов крупного капитала через избранных представителей.

Интересным также представляется механизм консенсуса доказательства авторитета (Proof-of-Authority), при котором валидаторами становятся заранее установленный круг лиц, своего рода администраторы сети. Например, на блокчейн-платформе POA Network, первой реализовавшей такой алгоритм, стать валидатором можно лишь предварительную процедуру лицензирования с предоставлением большого количества персональных данных, которая нотариально заверяется в США. Таким образом, валидатор в таком варианте становится публичным лицом. По большому счёту, такой механизм хорошо подходит для закрытых распределённых реестров в условиях почти полного доверия между участниками.

1.8 Выводы

Технология распределённого реестра является динамично развивающейся областью, в которой новые решения предлагаются каждый день. Выше были

продемонстрированы лишь некоторые, самые основные механизмы достижения консенсуса. В действительности, практически каждый блокчейн-стартап или криптовалюта привносит что-то новое в свои продукты, пытаясь превзойти существующие ограничения в масштабируемости, скорости проведения и фиксирования транзакций и анонимности применительно ко всевозможным областям экономики. Таким образом, на сегодняшний день существует большое количество различных реализаций технологии распределённых реестров разной степени открытости, использующих разные механизмы консенсуса (см. рисунок 10).



Примечание – Источник: [18].

Рисунок 10 – Использование различных механизмов достижения консенсуса в распределённых реестрах в зависимости от степени открытости

Блокчейн и технология распределённого реестра в целом на сегодняшний день представляется крайне перспективной с точки зрения хранения данных, а также выстраивания децентрализованного механизма взаимодействия внутри фирмы, некоторого бизнес-сообщества или даже между государствами. Уже сегодня многие крупные компании из разных сфер экономики, консорциумы банков, а также центральные банки и государственные структуры запускают свои пилотные проекты, основанные на технологии распределённого реестра.

Имея представление о механизмах работы распределённого реестра, его особенностях и видах, представляется возможным провести конструктивный анализ проектов внедрения технологии в реальных секторах экономики и государственного управления и трезво оценить их перспективы.

2 Основные возможности реализации технологии в различных секторах экономики

2.1 Финансовые сервисы и продукты

2.1.1 Система платежей

Как известно, первой реализацией технологии распределённого реестра стал блокчейн, обслуживающий криптовалюту Биткоин. Многие эксперты и криптоэнтузиасты возлагают на криптовалюты и, в частности, на Биткоин как самую известную из них, большие надежды и веря, что в какой-то момент все расчёты будут проходить с помощью неподконтрольных государством виртуальных монет.

С появлением криптовалюты Эфир (Ethereum) и возможности заключать некоторые обеспеченные компьютерным алгоритмом умные контракты (smart contracts), способные отражать передачу любой ценности при наступлении определённых условий и фиксировать этот факт в публичном распределённом реестре, внимание к технологии значительно возросло. И хотя в первую очередь возникло большое количество различных технологических стартапов, направленных исключительно на расширение функционала и области применения криптовалют, ведущие финансовые организации мира увидели в самой идее распределённого реестра некоторые перспективы. Тем не менее, для некоторых финансовых институтов технология распределённого реестра может представлять определённую угрозу и риски.

Технология распределённого реестра, изначально, было создана для обеспечения прямого электронного обмена актива или ценности без привлечения третьей стороны, посредника. В реальной экономике существуют специализированные финансовые посредники (платёжные системы, системы расчёта по ценным бумагам, центральные депозитарии и контрагенты, клиринговые компании), которые гарантируют передачу активов от одного агента другому и являются техническим ядром современных финансовых отношений. Количество посредников, по сути, определяется некой “институциональной дистанцией” между контрагентами. Если они являются клиентами одного банка, то именно он будет являться посредником, и передача средств будет происходить почти мгновенно. Однако если осуществляется перевод средств из одной юрисдикции в другую, то это может занять значительное время.

Если же вообразить, что передача средств осуществляется с помощью некоего распределённого реестра, то картина будет иной. Транзакция, инициируемая отправителем, проходит процедуру валидацию с помощью механизма консенсуса, после чего считается проведённой и добавляется в реестр (например, в блокчейн). Данная процедура полностью подменяет собой клиринг (процесс определения взаимных требований или обязательств и их взаимозачёт), расчёт (сеттельмент) и, вполне возможно, некоторую систему внутреннего контроля для удостоверения того факта, что сделка, инициированная сторонами в распределённом реестре, повлекла за собой передачу некоторого товара или услуги.

Таким образом, в перспективе, при условии выбора правильной архитектуры построении распределённого реестра, за счёт уменьшения числа посредников, платежи между контрагентами из различных юрисдикций могут заметно ускориться. Ускорение обработки финансовых операций, таким образом, сможет значительно увеличить мобильность мирового капитала.

2.1.2 Сфера банковского обслуживания

Технология распределённого реестра, помимо перестройки рынка ценных бумаг, имеет потенциал как минимум значительно упростить процедуры предоставления некоторых банковских услуг. В частности, использование смарт-контрактов в перспективе может значительно повысить эффективность определённых банковских операций, в которых банки выступают посредниками между контрагентами. Преимущества распределённых реестров и, в частности, блокчейна, в части безопасности, неизменяемости внесённых данных и прозрачности в распределённой сети являются крайне привлекательными для банковского сектора в некоторых аспектах.

В первую очередь, об этом уже было сказано ранее, можно представить систему межбанковского обмена на основе технологии распределённого реестра. С помощью неё банки из разных стран смогут взаимодействовать друг с другом более эффективно в части трансграничных платежей, значительно сократив количество посредников (в виде центральных банков, например) и упростив движение капитала на рынке межбанковского обмена.

Другим перспективным направлением для банков во внедрении технологии распределённого реестра, является предоставление системы для надёжного и безопасного хранения кредитных историй частных и корпоративных лиц. Сегодня во всех странах существуют специальные учреждения, носящие в России название бюро кредитных историй, которые агрегируют информацию о всех выданных банковских кредитах в стране, составляя единый профиль кредитной истории конкретной организации или физического лица. По запросу самого лица или организации, а также заинтересованных учреждений (например, других банков), бюро предоставляет выписку с кредитной историей лица. В своей повседневной деятельности такие учреждения сталкиваются с рядом проблем, значительно снижающих их эффективность [19]. Во-первых, это долгие интервалы обновления информации в бюро, так как обычно предоставление в бюро информации по кредитам банками осуществляется на ежемесячной основе, а полное внесение поступивших данных и сверка их с текущими позициями может занимать до 7 рабочих дней. Во-вторых, проблема идентификации, заключающаяся в возможном неполном предоставлении заёмщика информации о себе или простая ошибка в работе банковских операционистов – всё это может сделать невозможным однозначное сопоставление вновь поступивших данных с каким-то отдельным лицом или компанией. В-третьих, следствием ошибки может является рассогласованность информации по одному и тому же лицо в разных кредитных бюро, что может повлиять на решение банка о выдаче лицу кредита, когда в качестве источника информации будет предоставлена неполная или ошибочная история, предоставляемая одним из кредитных бюро. В-четвёртых, это ограниченность деятельности таких бюро отдельными юрисдикциями и странами, что приводит к тому, что если лицо переезжает в новую страну, то его/её кредитная история начинается с нуля в другой стране, что, вообще говоря, при возможном обмене информации между бюро разных стран смогло бы значительно понизить соответствующие риски. Наконец, значительной проблемой является возможность утечки данных или неавторизированный доступ к ним. В 2017 году хакеры смогли украсть информацию о кредитных историях 143 миллионов человек и американского бюро кредитных историй Equifax [20]. Все вышеперечисленные проблемы можно решить посредством переноса хранения всех кредитных историй

на блокчейн с активным применением смарт-контрактов, как это предложили специалисты из австрийского Института Наук и Технологий [19]. Авторы предложили полностью работоспособный прототип распределённого реестра, который полностью заменяет собой работу всех бюро кредитных историй, снижая тем самым издержки банковского сектора, позволяет кредитным историям использоваться за пределами одной юрисдикции, снижая риски банков, и всегда предоставляет информацию практически в реальном времени.

Третье возможное поле для внедрения распределённого реестра в банковскую сферу представляет собой область стандартных банковских продуктов и услуг, таких как ипотечное кредитование, обслуживание эскроу-счетов и аккредитивов. С помощью функционала смарт-контрактов эти операции возможно сделать менее рисковыми для банка (говоря об ипотеке), а также значительно снизить операционные издержки от документарного сопровождения сделок, их сверки и осуществления сугубо посреднических функций (говоря об эксроу-счетах и аккредитивах). Большое количество банков, в том числе и в России, сегодня активно экспериментируют с внедрением блокчейна в части данных операций услуг. Подробнее примеры такого использования технологии распределённого реестра раскрыты в главах 4.3 и 4.4 настоящего отчёта.

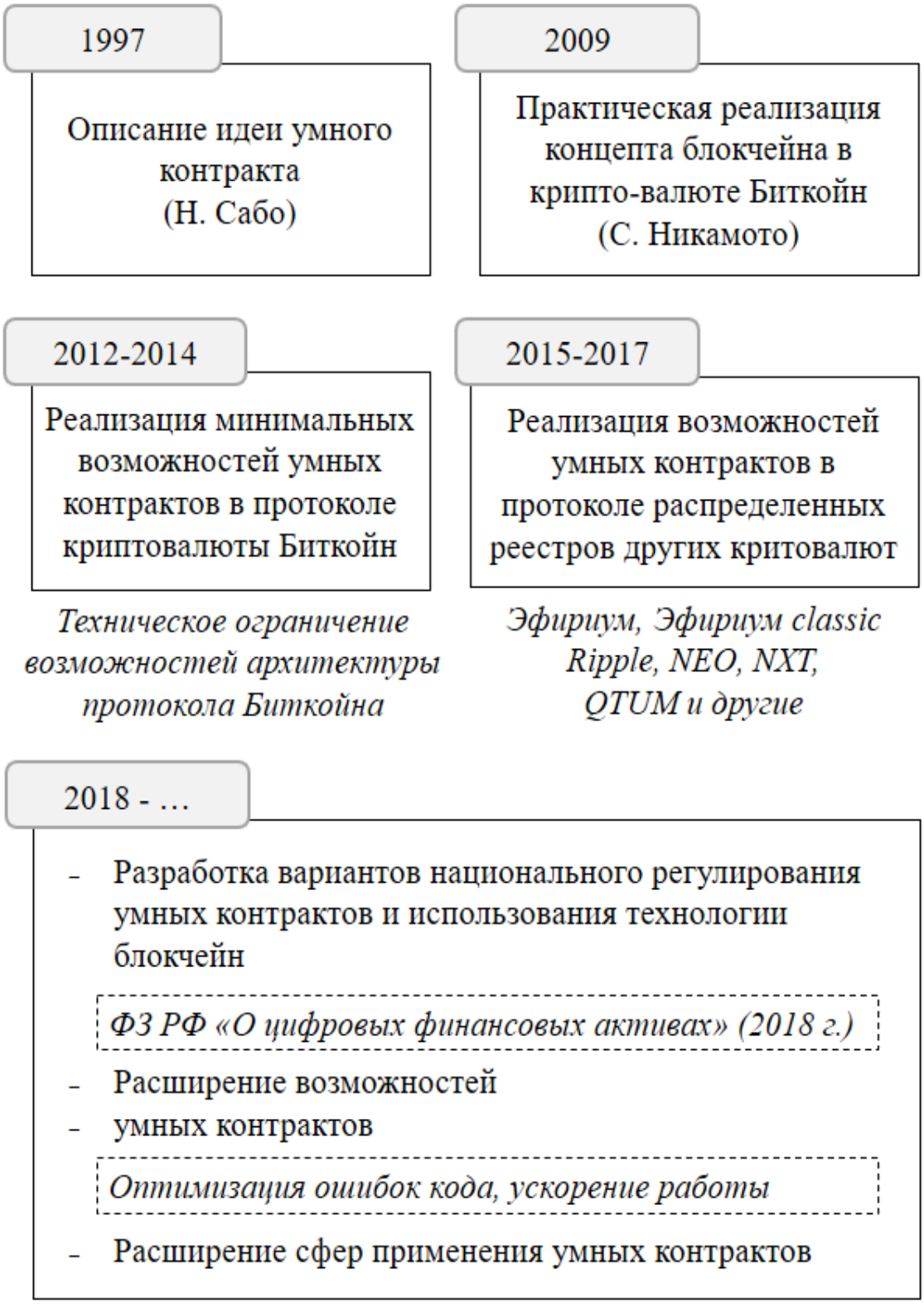
2.3 Умные контракты

В международной практике принято понимание смарт-контракта как некоторого автоматически срабатывающего правила, корректное исполнение которого обеспечивается технологией распределенного реестра. Смарт-контракт строится по линейному принципу «если то, то это» (*if this then that, ITTT*), что означает, что реализация условий контракта производится только в случае, если произошло запрашиваемое контрактом событие. Основным преимуществом умного контракта является отсутствие централизованного арбитра сделки.

Идея умного контракта была описана еще в конце XX века, но действительное практическое развитие получила только в 2010-е годы. Взрыв интереса к умным контрактам как элементу технологии распределенного реестра начался с практики применения расчетов в криптовалюте, прежде всего Биткойне, хотя именно в блокчейне Биткойна возможности реализации умных контрактов сильно

ограничены. В настоящее время умные контракты осуществляются в распределенных реестрах многих криптовалют (прежде всего Ethereum, Ripple, NXT, NEO и других), и наиболее важными вопросами их будущего развития является, во-первых, потенциал экспансии применения в разных сферах и, во-вторых, целесообразность национального и наднационального регулирования (рисунок 11).

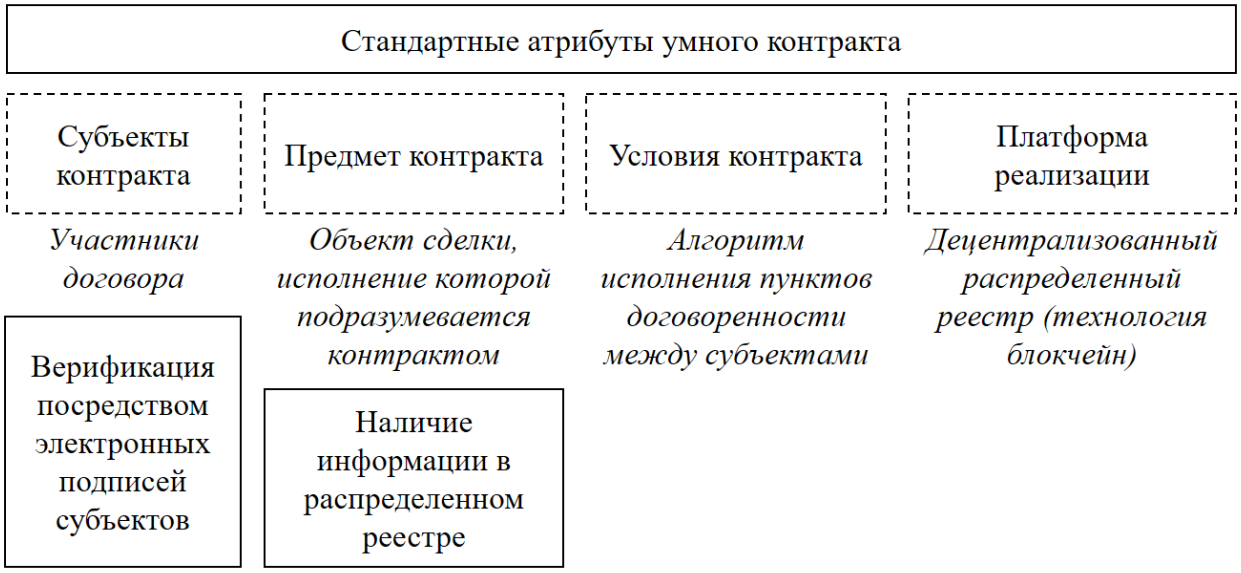
В соответствии со ст. 2 проекта Федерального закона «О цифровых финансовых активах» от 25.01.2018 г. умный контракт (или смарт-контракт) определен российским законодательством как «договор в электронной форме, исполнение прав и обязательств по которому осуществляется путем совершения в автоматическом порядке цифровых транзакций в распределенном реестре цифровых транзакций в строго определенной им последовательности и при наступлении определенных им обстоятельств».



Примечание – Составлено авторами по материалам [21].

Рисунок 11 – Этапы развития технологии умных контрактов на платформе распределенного реестра

Стандартные атрибуты умного контракта – субъект, предмет, условия, а также платформа реализации контракта – представлены на рисунке 12.



Примечание – Составлено авторами по материалам [22].

Рисунок 12 – Атрибуты умного контракта

Субъектами умного контракта выступают стороны – участники договора. Подтверждение участия сторон в заключении контракта и согласия с его условиями производится посредством обмена электронными подписями. Предметом умного контракта выступает объект сделки между его участниками, это может быть право собственности, криптовалюта и другое. Важной особенностью является то, что предметом контракта может быть только объект сделки, информация о котором уже содержится в распределенном реестре. Условиями умного контракта называют технически заданный алгоритм, исполнение которого означает исполнение пунктов контракта. Наконец, платформой реализации умного контракта выступает децентрализованный распределенный реестр.

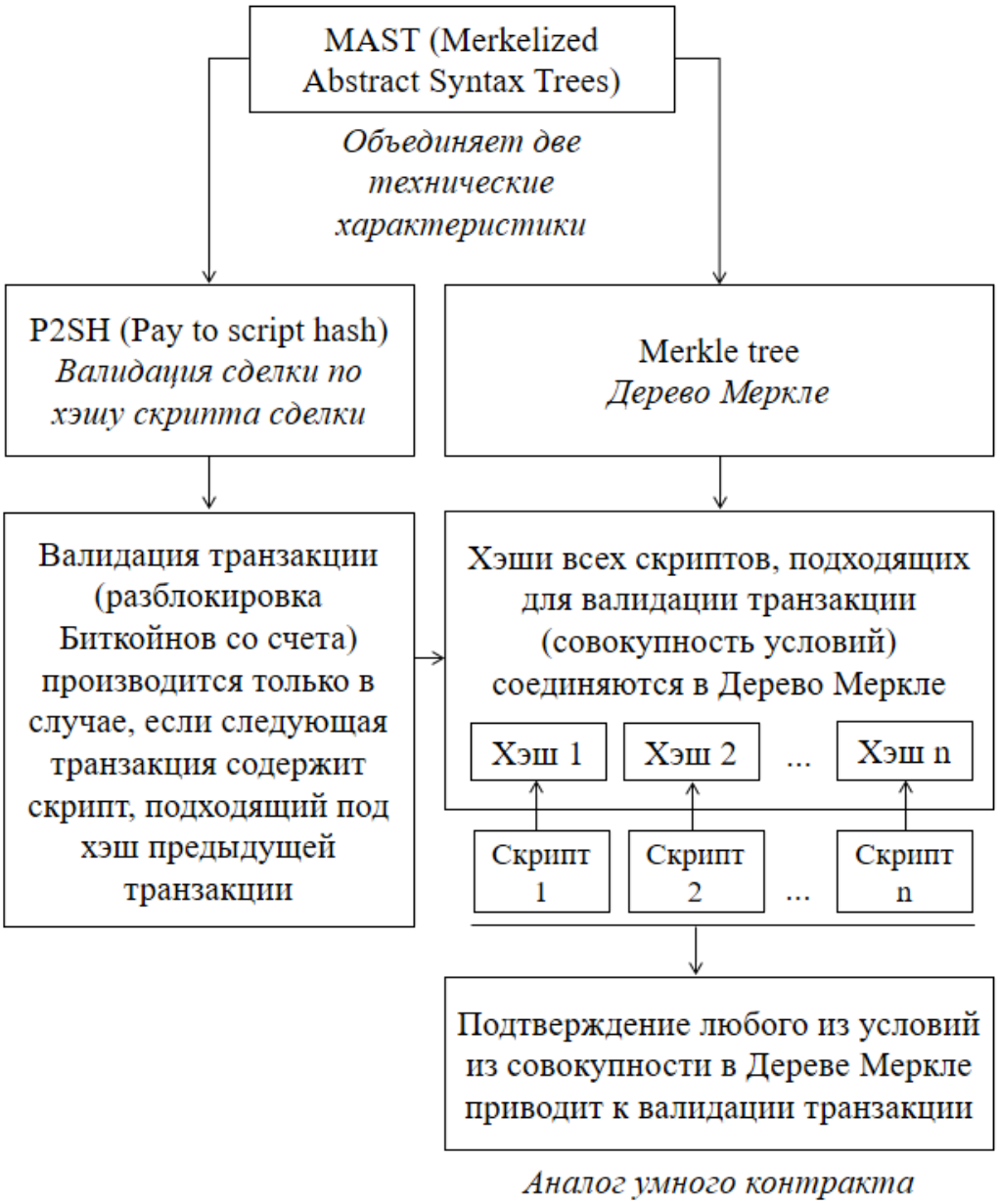
Важно отметить, что возможности заключения умного контракта сильно различаются для различных платформ их реализации. Известно, что архитектура блокчейна Биткойна не предполагает техническую возможность создания умных контрактов изначально. Однако, поскольку Биткойн является криптовалютой с наибольшей долей расчетов и распространения в мире, для его распределенного реестра разрабатываются альтернативные возможности создания умных контрактов, а также создаются надстройки блокчейна. К числу способов создания умного контракта или его аналога в распределенном реестре Биткойна можно отнести

следующие: окрашивание Биткойна, расширение протокола блокчейна Биткойна и использование надстройки блокчейна Биткойна - сайдчейна (sidechain).

Наиболее простой способ наделения Биткойна некоторыми атрибутами умного контракта был разработан в 2013 г. и заключается в так называемом окрашивании Биткойна в соответствии с его назначением для осуществления транзакции с определенным видом актива (акциями, облигациями, объектами недвижимости, золотом и иными активами). Вследствие делимости Биткойна до одной миллионной части (сатоши[2]) возникает возможность окрашивания выпуска Биткойнов так, чтобы одному сатоши ставилось в соответствие одно значение цвета. Окрашивание Биткойнов производится с использованием специального протокола EPOBC, который генерирует транзакции двух типов - транзакции генезиса и транзакции передачи [23]. Данные транзакции отличаются от других тем, что в поле информации о них (32-битное число) дополнительно вводится 6-битный тег, идентифицирующий их как транзакции генезиса либо передачи. В рамках транзакции генезиса производится выпуск окрашенных Биткойнов. Транзакция содержит информацию о количестве Биткойнов определенного цвета в выпуске, а хэш данной транзации в распределенном реестре расценивается как индикатор цвета Биткойнов данного выпуска. Далее сделки с окрашенными Биткойнами соответствующего выпуска осуществляются в рамках транзакций передачи. Окрашивание Биткойнов не является абсолютным субститутом смарт-контракта, поскольку позволяет только идентифицировать определенный выпуск Биткойнов, но не позволяет включить в код сделки другие существенные условия.

Вторым способом расширения функционала распределенного реестра Биткойна является расширение его протокола при помощи мерклизованных абстрактных синтаксических деревьев (Merkelized Abstract Syntax Trees, MAST). В настоящее время возможность реализации функционала MAST в реестре Биткойна только обсуждается, поскольку предположительно требует софтфорка – мягкого изменения правил записи транзакций в распределенный реестр. Функционал MAST объединяет технические характеристики P2SH (Pay to script hash) и деревьев Меркла и может быть схематично представлен как показано на рисунке 13.

[2]По состоянию на 03.05.2018 г. 1 сатоши составил 0,9 цента доллара США.



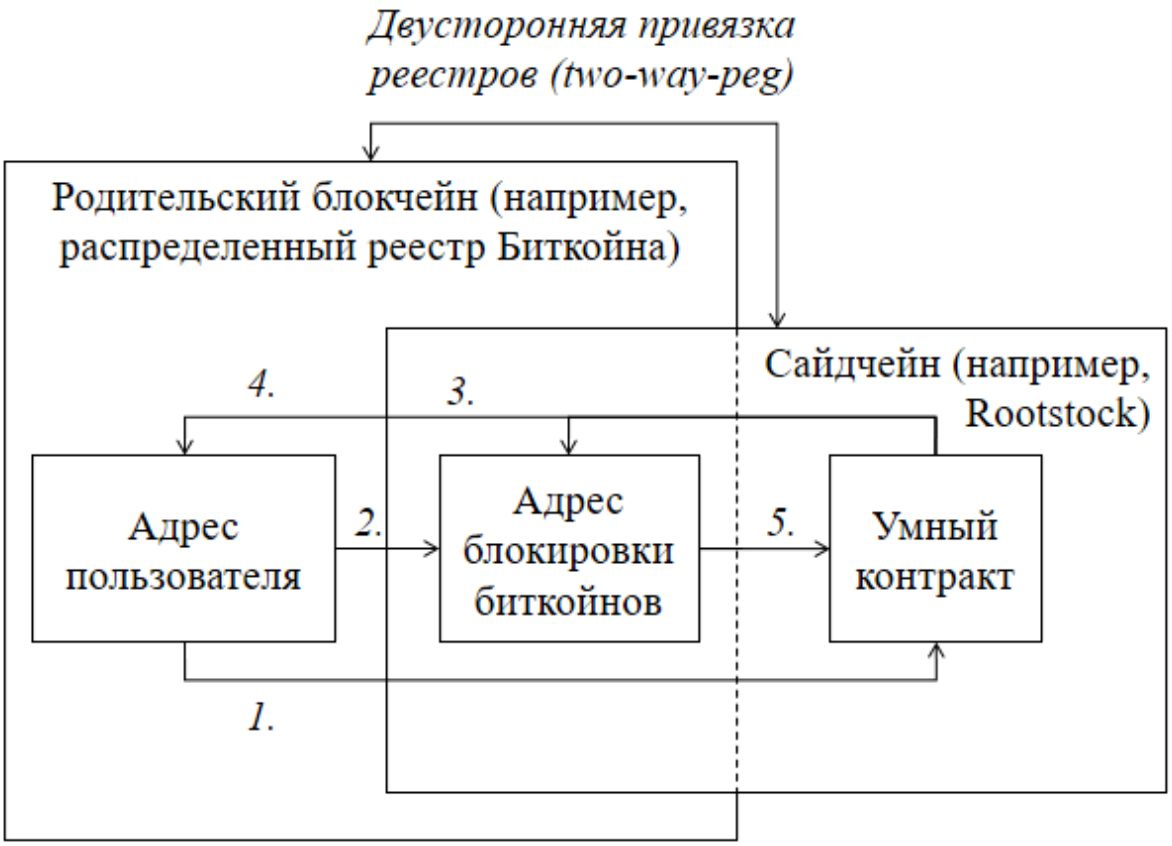
Примечание – Составлено авторами по материалам [24].

Рисунок 13 – Схема функционала MAST, расширяющая возможности создания умных контрактов в распределенном реестре Биткойна

Идея использования данного функционала заключается в том, что валидация транзакции (разблокировка Биткойнов с одного адреса и перевод их на другой адрес) реализуется в случае выполнения принципа P2SH - скрипт новой транзакции должен подходить под хэш предыдущей. К этой идее добавляется идея многовариантности взаимоисключающих условий валидации транзакции. Все возможные условия валидации транзакции соединяются в дерево Меркле, особенностью которого

является возможность проверки, содержится ли в нем конкретный набор данных (даже если не весь набор данных дерева известен). В результате разблокировка транзакции наступает в одном из случаев, когда скрипт следующей сделки подходит под один из имеющихся в дереве Меркле хэшей. В результате функционал MAST предоставляет возможность предопределения условий разблокировки транзакции в биткойнах, что может расцениваться как вариант умного контракта.

Наконец, третий вариант создания умного контракта в блокчейне Биткойна заключается в использовании надстройки для распределенного реестра – так называемого сайдчейна (sidechain) или его упрощенного варианта – двайвчейна. Сайдчейном называется дополнительный распределенный реестр, который интегрируется с родительским распределенным реестром (в данном случае блокчейном Биткойна) и транслирует информацию об осуществленных в нем сделках. Более того, сайдчейн используется не только для дискретного импорта информации о сделках из вспомогательного реестра в родительский, но и для осуществления транзакций между двумя реестрами. Если архитектура вспомогательного распределенного реестра позволяет создавать умные контракты, сайдчейн способствует появлению этой информации в блокчейне Биткойна. В настоящее время в процессе обсуждения и разработки находится драйчейн для под названием Rootstock (RSK) [25]. Rootstock является централизованной системой двусторонней привязки (two-way-peg) к блокчейну Биткойна, платформа которого сможет обеспечить доступ блокчейна Биткойна к работе с умными контрактами и децентрализованными приложениями Эфириума, написанными на языке Solidity. Схема взаимодействия родительского блокчейна и сайдчейна представлена на рисунке 14.



1. Запрос контракта
2. Удержание средств с адреса пользователя на оплату контракта
3. Проверка подлинности транзакции (мультиподписи)
4. Реализация контракта
5. Перечисление оплаты контракта

Примечание – Составлено авторами по материалам [26].

Рисунок 14 – Схема взаимодействия родительского блокчейна и умного контракта сайдчейна

Тем не менее, в настоящее время возможности сайдчейна ограничены, поскольку требуют изменения протокола Биткойна и, следовательно, софтфорка. Также недостаточно исследованной является проблема безопасности сайдчейна, поскольку сайдчейн получает финансовые ресурсы (например, плату за создание умного контракта) из родительского распределенного реестра, и защита посредством протокола PoW работает для него не так эффективно.

Как было показано выше, создание умных контрактов в распределенной реестре Биткойна имеет ограничения, в то время как другие распределенные реестры предлагают для этого более широкие возможности. В различных распределенных реестрах умные контракты создаются на разных языках (специальном, как в реестре

Эфириуема, или уже существующем, как в реестре NEO), с ограничением шаблонов видов контрактов или без ограничений, с разной степенью сложности, специализации профиля контрактов, с возможностью автоматической калибровки ошибок. Базовой платформой реализации умного контракта считается платформа Эфириума, на которой умный контракт создается на языке Solidity без ограничений по форме (шаблону) контракта. Альтернативная блокчейн платформа NEO позволяет производить автоматическую оптимизацию кода умного контракта перед запуском, что снижает скорость создания контракта, но повышает эффективность его использования в дальнейшем. Другие примеры платформ реализации умных контрактов и их характеристики представлены в таблице 1.

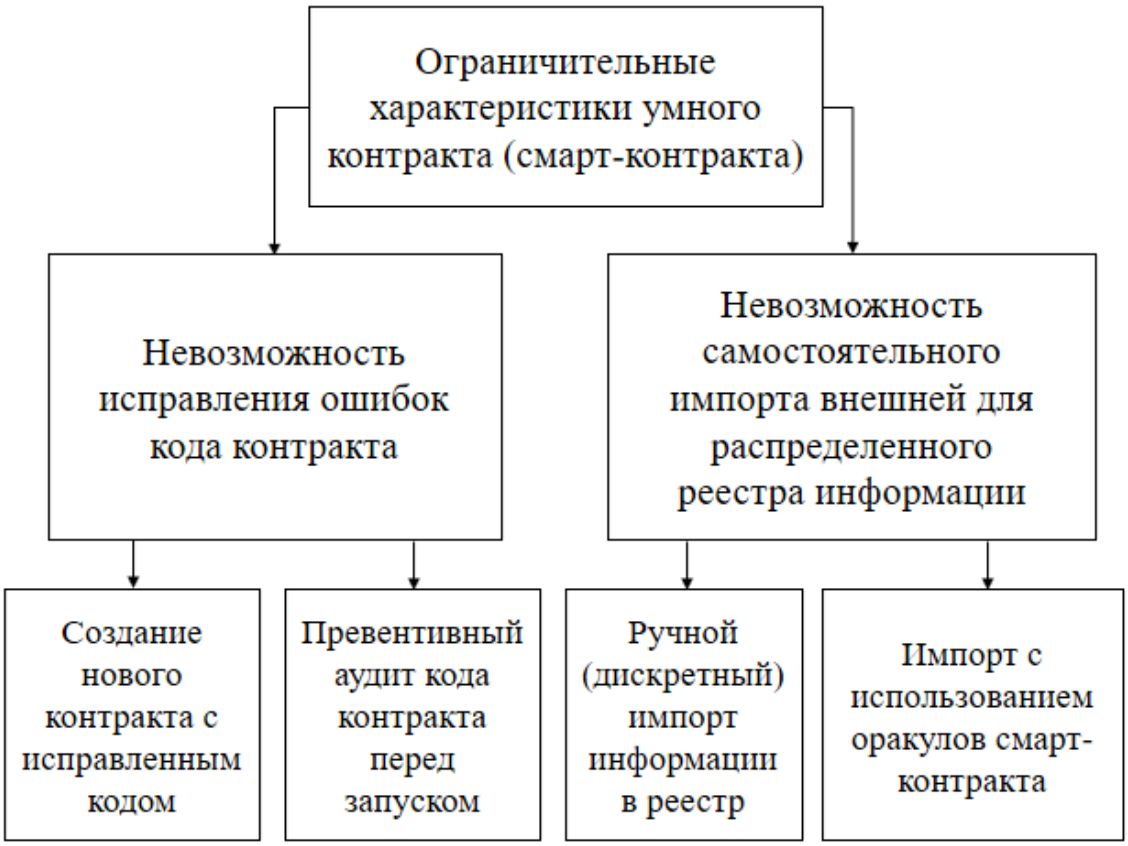
Таблица 1 – Примеры и характеристики блокчейн платформ для умных контрактов

Блокчейн платформа	Характеристики платформы
Эфириум (2015) Эфириум classic (2016)	Базовая платформа для создания умных контрактов Не накладывает ограничений на форму (шаблон) контракта Оплата вычислительных ресурсов, затраченных на создание контракта, производится в валюте блокчейна - Эфире. Количество необходимого для оплаты Эфира тем больше, чем более ресурсозатратный контракт Язык написания контракта – Solidity (стандарт ERC20)
NEO (2014)	Предоставляет возможность автоматической оптимизации кода контракта перед запуском с целью сокращения вероятности ошибки в коде Менее быстрый, но более эффективный подход к созданию контрактов, чем на платформе Эфириума
NXT (2013)	Платформа имеет ограничения формы (шаблонов) создаваемых контрактов Разработана для создания специальных контрактов, используемых впоследствии в децентрализованных приложениях платежных систем, мессенджеров и иных
QTUM (2017)	Предоставляет возможность создавать контракты нового поколения, получившие название мастер-контрактов: Мастер-контракт может разрабатываться с возможностью подключения третьего лица, от которого в контракт импортируется существенная информация Разработаны в соответствии с отраслевыми стандартами логистики, телекоммуникации, торговли и иных отраслей

Продолжение таблицы 1

Примечание – Составлено авторами.

Существующие на данный момент умные контракты обладают такими ограничениями, как невозможность исправления и невозможность импорта информации извне распределенного реестра (рисунок 15).



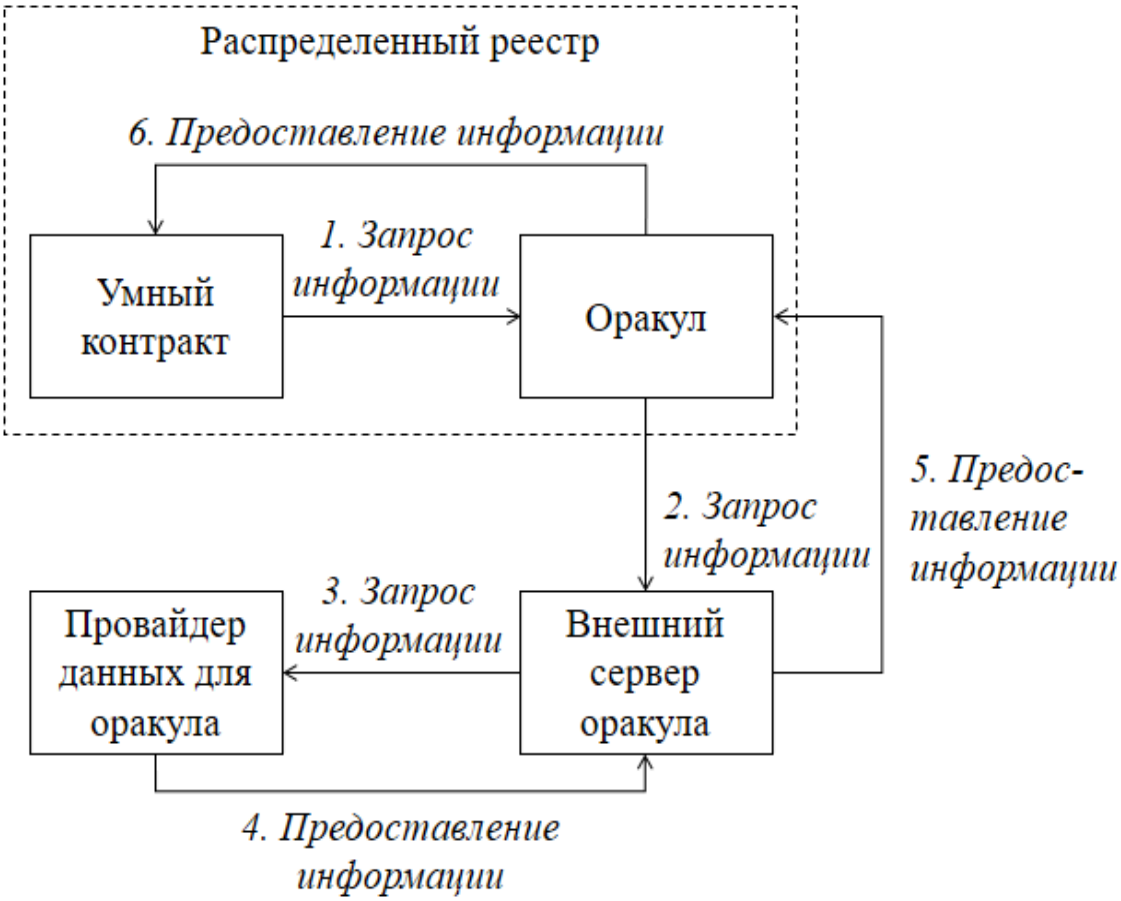
Примечание – Составлено авторами.

Рисунок 15 – Ограничительные характеристики смарт-контрактов

Невозможность изменения правила смарт-контракта означает, что выявление ошибок в коде в процессе использования контракта приводит к отказу от использования данного контракта и созданию нового. Эта особенность, с одной стороны, стимулирует появление комплексных контрактов, просчитывающих большое количество вероятных исходов; с другой стороны, именно сложность контракта увеличивает риск ошибки в написании кода. В связи с этим создание многофункциональных смарт-контрактов часто сопровождается предварительным аудитом контракта техническими профессионалами.

Вторая особенность смарт-контракта – невозможность обращения к внешней информации – означает, что контракту доступна только информация, уже помещенная ранее в распределенных реестр, внутри которого существует контракт. Тем не менее, импорт необходимой для выполнения контракта информации в распределенный реестр может производиться в ручном режиме либо с использованием оракулов.

Оракул блокчейна может быть определен как специальный инфраструктурный алгоритм, импортирующий информацию в распределенный реестр с внешнего для реестра сервера, который в свою очередь направляет запрос к провайдеру необходимых данных, как показано на рисунке 16. В результате в распределенном реестре появляется ранее отсутствовавшая информация, необходимая умному контракту для выполнения условий кода.



Примечание – Составлено авторами по материалам [27].

Рисунок 16 – Схема взаимодействия оракула и умного контракта

Данный алгоритм позволяется преодолеть ограничение, вызванное детерминированностью распределенного реестра: непрерывный импорт информации оракулом в распределенный реестр позволяет умному контракту обращаться к этой информации в режиме реального времени и проводить сопоставление фактических условий с теми, что указаны в контракте и приводят к изменению состояния сделки. Фактически схема взаимодействия оракула и умного контракта включает два основных этапа: импорт оракулом информации из внешнего мира и импорта информации умным контрактом из оракула. В зависимости от назначения умный контракт взаимодействует с контрактами разного типа: встроенными в виде программного обеспечения, аппаратным, входящим, как показано на рисунке 17.

Примечание – Составлено авторами по материалам [28].

Рисунок 17 – Схема взаимодействия умного контракта
с различными типами оракулов

В случае работы контракта с информацией оценочного или прогнозного характера информация импортируется из нескольких оракулов. Для экспорта информации из контракта во внешний мир при наступлении события (например, оплаты платежа или перехода права собственности, зафиксированного контрактом) используется исходящий оракул.

Как было обозначено в таблице 1, базовой платформой для создания умных контрактов на данный момент является блокчейн Эфириума. В этом случае умный контракт реализуется в несколько этапов. На первом этапе условия контракта записывается в соответствии с принципом "если то, то это" в виде строк кода Solidity. Далее готовый код умного контракта записывается в код блокчейна Эфириума. Наконец, в момент исполнения кода умного контракта в соответствии с заданными условиями производится обновление регистра записей на всех узлах блокчейна.

Классическим и наиболее распространенным примером реализации умного контракта на платформе Эфириума является контракт, организующий сбор средств для реализации первичного (первоначального) выпуска токенов, или ICO (initial coin offering). Такой умный контракт позволяет некоторому блокчейн-стартапу аккумулировать средства заинтересованных инвесторов в валюте Эфириума (Эфире), произвести обмен Эфира на токены и вывести полученный от ICO средства. В этом случае умный контракт состоит из иерархии нескольких контрактов и подконтрактов, взаимосвязь которых схематично может быть представлена в таблице 2.

Таблица 2 – Пример реализации умного контракта – осуществления ICO на платформе Эфириума

<table>
<tr><th>Название контракта</th><th>Характеристика контракта</th></tr>
<tr><td>Контракт Owned</td><td>Выявляет собственника контракта среди пользователей
Предоставляет собственнику контракта специальные функции, в частности, право вывода аккумулированных в рамках ICO средств</td></tr>
<tr><td>Контракт Crowdsale</td><td>Аккумулирует информацию о сборе средств и распределении токенов, а именно:
О количестве выпущенных эмитентом (собственником контракта) токенов
О количестве токенов на балансе каждого держателя
Обозначает правило реагирования контракта на изменение права собственности на токены между держателями
<table><tr><td>Подконтракт EasyToken</td><td>Аккумулирует информацию о токенах:
Полное, сокращенное название
Делимость либо неделимость
Правило вывода токена на биржу</td></tr></table></td></tr>
<tr><td>Контракт Fallback</td><td>Аккумулирует информацию о порядке действий в случае поступления валюты Эфириума (Эфира) на счет умного контракта:
Наличие свободных для продажи токенов
Текущая стоимость токенов
Количество токенов, подлежащее отправке покупателю</td></tr>
<tr><td>Контракт EasyCrowdsale</td><td>Содержит информацию о правиле вывода полученной вследствие размещения токенов валюты (Эфира)</td></tr>
</table>

Примечание – Составлено авторами по материалам [29].

Существует также множество других примеров использования умных контрактов на базе блокчейна Эфириума. Во-первых, умный контракт может сопровождать переход права собственности (в том числе на недвижимость), требующий верификации электронных подписей сторон сделки (такая возможность, например, доступна в Грузии, где внедряется технология блокчейн-сервисов регистрации прав собственности на земельные участки). Для того, чтобы такой умный контракт был реализован, информация об объекте и участниках сделки должна находиться в распределенном реестре Эфириума. В результате технология умного контракта проверяет правомочность заключения сделки (например, факт того, находится ли объект недвижимости в залоге) и фиксирует переход права собственности посредством обновления информации о сделке на каждом узле

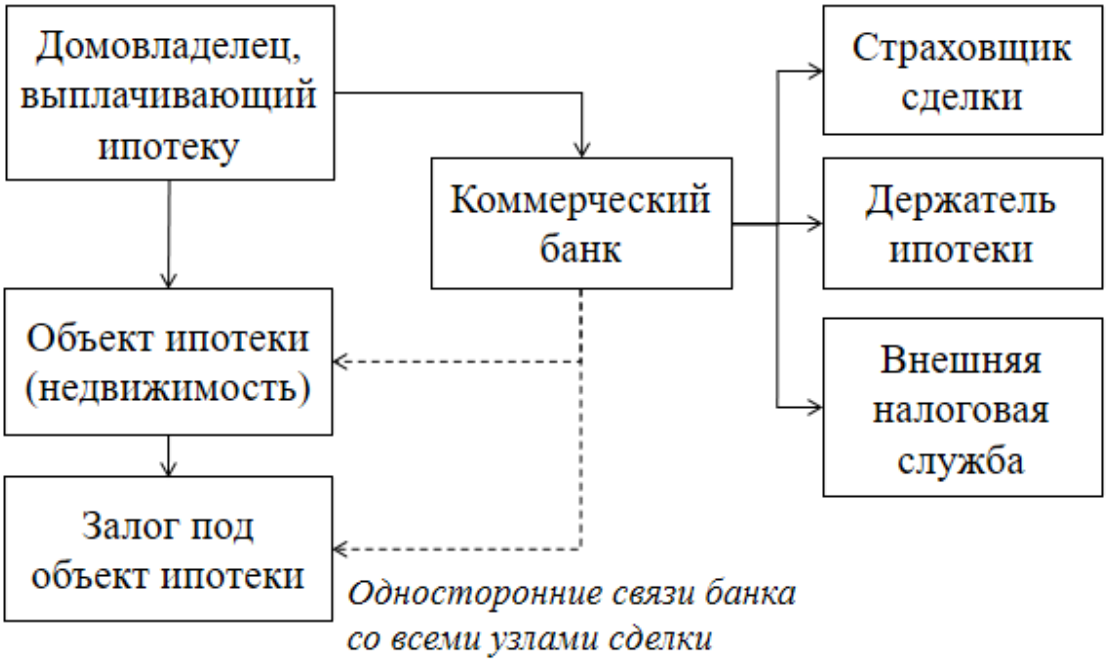
распределенного реестра, фактически исключая из этого процесса централизованного контрагента (обычно выступающего правовым гарантом подобных сделок).

Во-вторых, умный контракт может быть успешно реализован для сопровождения процесса, характеризующегося регулярностью действий контрагентов. Такой контракт может проводить автоматическое списание средств со счета арендатора за пользование объектом недвижимости, автоматическое списание выплат по ипотечному кредиту. В частности, как показано на рисунке 18, такой умный контракт в перспективе может исключить банковского контрагента из схемы осуществления ипотечной сделки. Дополнительным внешним эффектом реализации такого контракта является цифровое фиксирование кредитной и репутационной истории контрагентов, имеющее большое значение для будущих сделок.

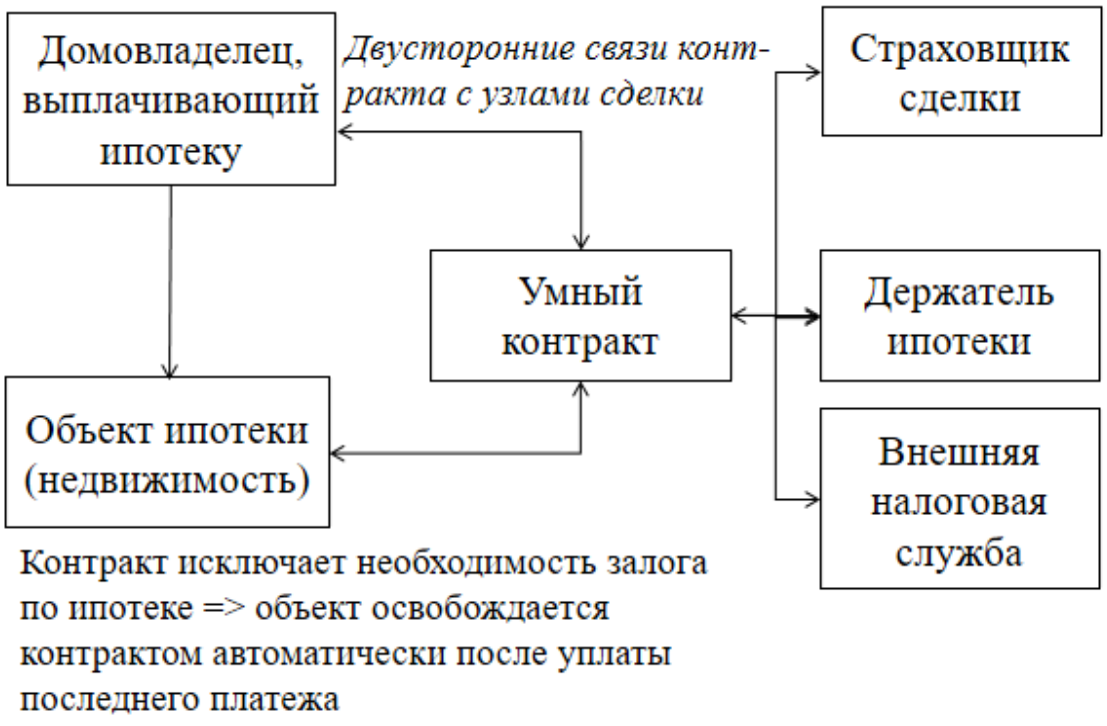
Наконец, умный контракт на платформе Эфириума может эффективно применяться в сделках с ценными бумагами и производными финансовыми инструментами. Например, совершение сделки с ценными бумагами производится между клиентами с помощью индивидуальных ключей, а передача права собственности подтверждается с помощью открытого ключа. Умный контракт при этом импортирует из оракула информацию об эмиссии ценных бумаг, фиксирует передачу права собственности, производит управление такими операциями, как выплата дивидендов.

Аналогично, в сделках с производными финансовыми инструментами умный контракт импортирует из оракула текущую информацию по инструментам, фиксирует обязательства контрагентов (например, условия выполнения операции своп), рассчитывает чистые обязательства, закрывает сделку и генерирует запись о ее результат в реестр. Использование умных контрактов в сфере производных финансовых инструментов имеет высокий потенциал, поскольку правильно запрограммированный контракт может производить хеджирование рисков клиента практически в полностью автоматизированном режиме.

1. Классическая схема ипотечных платежей



2. Схема ипотечных платежей с умным контрактом

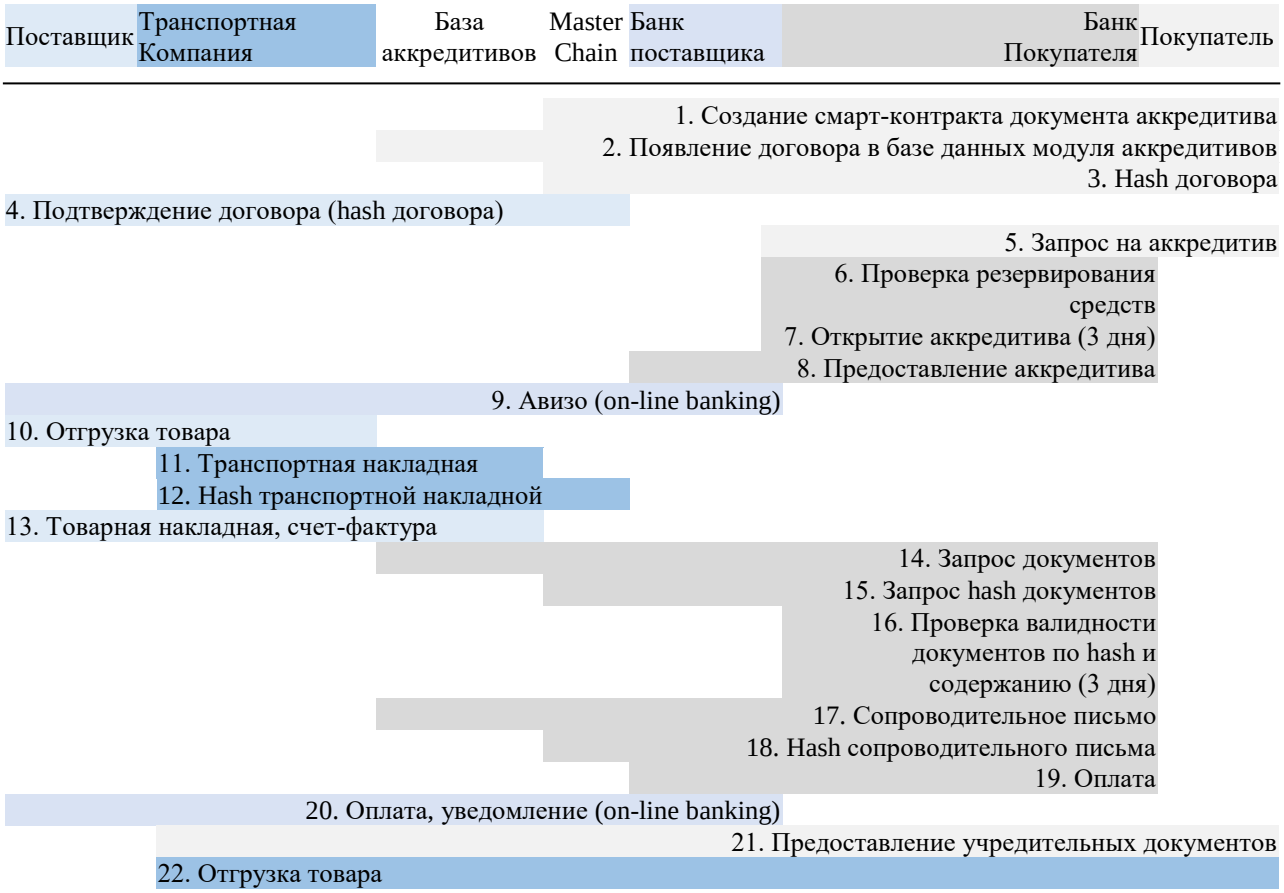


Примечание – Составлено авторами по материалам [21].

Рисунок 18 – Схема ипотечных платежей с использованием умного контракта

Как было обозначено выше, платформа Эфириума является наиболее базовой для создания умных контрактов, в связи с чем используется при разработке

национальных распределенных реестров, умных контрактов и приложений для них. В частности, в 2016 г. в России было объявлено о создании Ассоциации Финтех и разработке национального распределенного реестра финансовой информации Мастерчейн. Согласно Whitepaper Ассоциации Финтех, платформа Мастерчейн является модификацией протокола Эфириума. К началу 2018 г. в разработке находится четыре проекта использования технологии распределенного реестра и умных контрактов в финансовом секторе России. В качестве примера на рисунке 19 представлена схема проекта цифрового аккредитива, разрабатываемого Ассоциацией Финтех совместно с Альфа-банком.



Примечание – Составлено авторами по материалам [30].

Рисунок 19 – Схема проекта цифрового аккредитива на платформе Мастерчейн с использованием умного контракта между покупателем, поставщиком, транспортной компанией, банками покупателя и поставщика

Согласно представленной концепции цифрового аккредитива, умный контракт инициируется покупателем на платформе распределенного реестра Мастерчейн. Помимо непосредственных участников сделки - покупателя и

поставщика – сделку сопровождают банк покупателя, банк поставщика и администратор реестра – Ассоциация Финтех. В результате в данном случае умный контракт не несет функции верификации сделки только ее участниками, минуя посредников. Тем не менее, выполнение условий контракта инициирует хеширование записей в реестре о запуске контракта (1), создании договора аккредитива (3), транспортной накладной (12), сопроводительных документов (15) и сопроводительного письма (18). Хеширование записей умным контрактом в данном случае позволяет значительно сократить бумажный документооборот и ускорить взаимодействие контрагентов с 21 дня до 6 дней по оценкам Ассоциации Финтех.

Умные контракты создаются на разных платформах распределенных реестров, с чем в отдельных случаях связаны особенности их создания и использования. В частности, умные контракты в распределенном реестре криптовалюты Ripple были использованы для ограничения предложения одноименных токенов. В мае 2017 г. центральным контрагентом распределенного реестра - компанией Ripple - было принято решение об ограничении предложения эмитированной криптовалюты на рынке в целях поддержания стоимости криптовалюты и обеспечения предсказуемости динамики предложения, которое в свою очередь должно способствовать стабилизации спроса. Удержание (другими словами, депонирование) 55 млрд. единиц криптовалюты XRP (всего компанией было эмитировано 100 млрд. XRP) было произведено посредством 55 умных контрактов, каждый из которых дискретно удерживает 1 млрд. XRP. Условия данных умных контрактов предполагают высвобождение 1 млрд. XPR ежемесячно в течение 55 месяцев (4,5 лет) [31]. Это условие исключает единовременное значительное увеличение предложения криптовалюты, снижает риск ее внезапного обесценения и, следовательно, способствует большему доверию контрагентов. Согласно расчетам компании Ripple, представленным на рисунке 12, экспоненциальный рост предложения криптовалты с момента начала ее удержания будет наблюдаться только в первые 5-10 лет и впоследствии существенно замедлится; стабилизация объемов валюты в обращении ожидания компанией примерно через 15 лет, то есть ориентировочно к 2032 г.

Данные умные контракты были реализованы компанией Ripple при помощи гарант-сервиса Escrow, который обычно выполняет функцию агента-посредника между инвесторами и проектом ICO в целях повышения доверия контрагентов друг к другу (сервис производит временное удержание средств инвестора перед их передачей в проект до момента выполнения всех условий либо в целях поэтапной выдачи средств на проект). В случае умных контрактов Ripple сервис Escrow обеспечивает депонирование 55 умных контрактов до наступления условия - истечения срока депонирования (1 месяц для контракта № 1, 2 месяца для контракта № 2 и так далее). Как показано на рисунке 20, исполнение условия умного контракта обеспечивает инвестору доступ к дополнительному предложению криптовалюты Ripple, однако в случае, если объем окажется невостребованным инвесторами в течение месяца, он будет вновь изъят из обращения и депонирован сервисом Escrow под номером следующей учетной записи (например, № 56 для невостребованных средств учетной записи № 1 и так далее). Как было сказано выше, предполагается, что данная система умных контрактов обеспечит предсказуемость предложения криптовалюты Ripple и предотвратит избыток невостребованной валюты на рынке, потенциально оказывающий понижательное давление на ее курс.

Примечание – Составлено авторами по материалам [31].

Рисунок 20 – Технология умного контракта Ripple, обеспечивающая депонирование криптовалюты с использованием гарант-сервиса Escrow

2.4 Использование технологии распределённого реестра в образовательном секторе

Образование является одним из самых важных секторов экономики, без которого качественный экономический рост не представляется возможным. Обучение в институте даёт человеку необходимую специализацию и набор навыков, способных обеспечить ему достойную зарплату и благосостояние. Что же на этой почве может предложить технология распределённого реестра?

Для начала стоит определить и ограничить различные области образования, которые имеет смысл проанализировать с точки зрения перспектив внедрения технологии. Во-первых, разделим для начала образование на университетское и открытое, представляемое сегодня так называемыми массовыми открытыми онлайн-курсами (MOOC, Massive open online courses). Во-вторых, в рамках университетского образование имеет смысл рассматривать непосредственно образовательный процесс и сопровождающие его административно-управленческие аспекты с одной стороны, а с другой стороны – результаты образовательного процесса, документы об образовании или уведомительные сертификаты о прослушанных курсах, вкупе с учётом данных документов за пределами отдельного университета.

Естественной средой для внедрения технологии распределённого реестра в область образования являются площадки массовых онлайн-курсов. Относительно недавно российской командой разработчиков был запущен проект DISCIPLINA[3], представляющий собой блокчейн платформу, сводящую вместе студентов, учебные заведения, преподавателей, а также, в перспективе, потенциальных работодателей. Используя преимущества распределённого реестра, разработчики стремятся решить проблему создания единого реестра для учёта успеваемости студента по разным курсам, предоставляемых разными учебными заведениями, создать объективную и достоверную систему рейтингования студентов, что значительно может упростить поиск работодателями необходимых соискателей в соответствие с необходимыми знаниями для занятия той или иной позиции. Более того, в такой открытой системе оценке и рейтингованию может подвергаться совершенно всё – отзывы и рейтинги

[3] https://disciplina.io/

того или иного курса или программы, репутация университета и работодателей, использующих такой реестр. Проблема оперирования персональными данными, при этом, решается тем, в блоках будут фиксироваться лишь обезличенные хэши, когда как непосредственные достижения студентов будут храниться в их личных кабинетах. Доступ для работодателей в систему предполагается платным. Токены, оборачивающиеся в блокчейне DISCIPLINA, предполагается использовать для оплаты платных курсов и работы по созданию блоков в цепи.

Аналогичная логика действий возможна и в классическом университетском образовательном процессе, как минимум в рамках образовательных учреждений, участвующих в Болонском процессе. Основной его чертой является унифицированная система кредитов, получаемых за освоение той или иной дисциплины. Определенное количество набранных кредитов по определённым предметам позволяет студенту получить степень бакалавра, магистра или доктора наук. Унифицированность также заключается в том, чтобы упростить процедуру нострификации (процедура признания диплома страны при поступлении в образовательное учреждение другой страны) при поступлении в другой университет для получения следующей ступени образования или даже при простом переводе из одного ВУЗа в другой. Проблема совместимости кредитов по одной и той же дисциплине в разных университетах, однако, до сих пор считается довольно сложной, так как даже при полном соответствие осваиваемых тем в рамках определённого предмета, качество изложение и квалификация преподавателя может разительно отличаться. Тем не менее, часть описанного процесса, не зависящего от непосредственно преподавателя, возможно значительно упростить и автоматизировать, что и предлагают авторы доклада [32].

Авторы предполагает создать децентрализованный распределённый реестр на блокчейне, доступ к которому, однако, должен будет осуществляться некоторым механизмом регистрации и идентификации лиц к нему присоединяющихся. Предполагается, что основной единицей информации в реестре будут достижения студентов, которые, конечно же, с целью сохранения персональных данных, должны шифроваться. Скажем, если студент получает оценку за экзамен, то каждому студенту в рамках ведомости присваивается некоторый случайный идентификационный номер (различный для одного и того же студента на других

дисциплинах), который ставится в соответствие его учётной записи, доступ к которой студент имеет с помощью закрытого ключа. В метаданных такой “зачётной” транзакции о выставлении оценки должна содержаться информация о том, в каком университете был экзамен, количество кредитов, количество часов на освоение, список освоенных тем и другие необходимые данные. В случае ошибки организация должна будет создать новую транзакцию о корректировке баллов с указанием причины. Все метаданные будут является основой для создания смарт-контрактов.

Например, если две образовательные организации договариваются о принятии кредитов друг друга по определённым дисциплинам при движении контингента студентов между ними, то это фиксируется смарт-контрактом. Таким образом, при переводе студента взаимозачёт дисциплин и составление индивидуального учебного плана происходит автоматически за счёт учёта уже пройденных дисциплин в другом учебном заведении вследствие проверки на соответствие требований, установленных смарт-контрактами в такой сети.

В перспективе построение такой системы на базе технологии распределённого реестра смогло бы значительно упростить движение контингента, тем самым увеличивая мобильность населения как в рамках стран, так и за их пределами, фиксировать все достижения студентов в защищённом от подделывания реестре, а процедура выдачи дипломов стала бы более прозрачной, ввиду того, что освоение всех дисциплин всегда можно было бы отследить и проверить. Более того, автоматизация при использовании смарт-контрактов могла бы значительно упростить работу учебно-методических отделов, а также усилить учёт и контроль за количеством отчитанных часов преподавателями.

Смежной с темой образования является академическая деятельность. Специалисты из IBM предложили проект блокчейн платформы для учёта научных публикаций [33]. Решение, предложенное на базе разработки блокчейн-платформы Hyperledger Fabric, представляет собой закрытый распределённый реестр, участниками которого предполагаются ведущие международные университеты, исследовательские и научные центры и институты, а также издательства. В первую очередь, авторы видят перспективы блокчейна в данном сегменте как эффективный инструмент для выстраивания процесса рецензирования публикаций, проверки ссылок на источники, находящиеся в рамках реестра, создания системы для

простого, децентрализированного подсчёта показателей цитируемости авторов. Последнее также связано с возможностью построения системы прозрачного механизма оценки качества академических публикаций, их значимости для всего научного сообщества. В настоящее время Google Академия (Google Scholar) используется как основный источник показателя цитируемости в качестве прокси для значимости той или иной публикации или вклада исследователя. Однако механизмы, лежащие в основе данного сервиса непрозрачны и нет уверенности в том, что алгоритм, во-первых, находит все цитаты, а во-вторых, индексирует все работы автора. Создания аналогичного сервиса на базе распределённого реестра позволило бы преодолеть ограничения существующих сервисов, предоставив возможность объективной оценки деятельности академических работников.

3 Выводы и рекомендации в области экономической политики

Данная работа посвящена рассмотрению технологии распределённого реестра и анализу возможных выгод от её использования в различных секторах экономики. Первый раздел работы посвящён подробному описанию основных принципов работы технологии распределённого реестра. В нём подробно описана эволюция различных типов баз данных, одним из типов которых и является распределённый реестр. В работе проанализированы и систематизированы различные типы распределённых реестров, представлена классификация распределённых реестров по признакам доступа к формированию и чтению данных. Также подробно рассматриваются различные виды консенсусов, используемых для внесения новой информации в распределённые реестры.

Существенная часть работы посвящена таким важным приложениям технологии распределённого реестра (блокчейна), как криптовалюты и смарт-контракты (умные контракты). Подробно описана схема работы умных контрактов. Систематизированы особенности функционирования умных контрактов на различных платформах.

Также в исследовании подробно анализируются возможности использования технологии блокчейна в различных секторах экономики: финансовый сектор (в том числе банковский сектор), образовательный сектор.

Обширные возможности применения технологии блокчейн, способные привести к повышению эффективности в функционировании всей экономики и к существенному снижению издержек, требуют грамотного проведения экономической политики, которая должна быть направлена как на своевременное внедрение технологий, так и на конструирование необходимой законодательной базы. Также важен анализ возможных выгод от внедрения новых технологий в каждой конкретной области.

Для проведения качественной экономической политики можно дать следующие рекомендации. Во-первых, профильные министерства и Банк России должны способствовать проведению экспериментов с внедрением рассматриваемой технологии. При этом важно привлекать заинтересованное сообщество посредством

прозрачности экспериментов и открытого кода. Во-вторых, вместе с представителями различных стартапов работать над юридическими аспектами применимости технологии в разных отраслях. В-третьих, в реализации проектов важно начинать с малого и постепенно увеличивать масштаб: небольшие госкомпании, агентства, департаменты министерств могут начать внедрять технологии в своих внутренних процессах, потом выстраивать взаимодействие между собой, и лишь затем масштабируют это использование технологий на всю экономику. Что касается начала внедрения технологии на новых площадках (там, где ещё не внедрили), то наиболее простым видится активное использования блокчейна в здравоохранении для ведения амбулаторных карт.

ЗАКЛЮЧЕНИЕ

Технология распределённого реестра является динамично развивающейся областью, в которой новые решения предлагаются каждый день. Данная работа посвящена рассмотрению технологии распределённого реестра и анализу возможных выгод от её использования в различных секторах экономики. Первый раздел работы посвящён подробному описанию основных принципов работы технологии распределённого реестра. В нём подробно описана эволюция различных типов баз данных, одним из типов которых и является распределённый реестр. Проанализированы и систематизированы различные типы распределённых реестров, представлена классификация распределённых реестров по признакам доступа к формированию и чтению данных. Также подробно рассматриваются различные виды консенсусов, используемых для внесения новой информации в распределённые реестры.

Проанализировав большое количество кейсов, можно заключить, что практически каждый блокчейн-стартап или криптовалюта привносит что-то новое в свои продукты, пытаясь превзойти существующие ограничения в масштабируемости, скорости проведения и фиксирования транзакций и анонимности применительно ко всевозможным областям экономики. Таким образом, на сегодняшний день существует большое количество различных реализаций технологии распределённых реестров разной степени открытости, использующих разные механизмы консенсуса.

Одним из следствий развития технологии блокчейн и использующих её криптовалют является появление технологии смарт-контрактов (умных контрактов), которые являются в некотором роде надстройкой над блокчейном. В связи с этим в данной работе мы подробно описываем схему работы смарт-контрактов и систематизируем особенности функционирования смарт-контрактов на различных платформах.

В настоящее время экспансия технологии смарт-контрактов является одним из наиболее перспективных направлений цифровизации финансового сектора, и широкое внедрение технологии в практику работы финансовых компаний прогнозируется уже на горизонте трех-пяти лет. Использование смарт-контрактов в

финансовом секторе может, с одной стороны, сократить количество посредников финансовой операции (например, в случае проведения клиринговых расчетов или предоставления ипотечного займа), и, с другой стороны, выступить важным фактором сокращения различного рода издержек финансовых операций: в первую очередь временных (как в случае проекта цифрового аккредитива), пространственных (в случае удаленной идентификации клиента на основании биометрических данных), издержек асимметрии и неодинакового доступа агентов к информации (при реализации проекта “know your customer”), а также издержек пост-контрактного оппортунизма сторон любой финансовой сделки.

В российской практике технология умных контрактов внимательно отслеживается на законодательном уровне и тестируется в проектах финансовой и макропруденциальной политики. Внедрение технологии в период 2017-2018 гг. находится преимущественно на пилотных этапах с прогнозом раскрытия потенциала в течение нескольких лет. Вместе с тем предварительный анализ позволяет судить о вероятном положительном эффекте внедрения технологии на показатели конкуренции в отечественном банковском секторе, количественной эффективности проектов и качественного разнообразия предоставляемых финансовым сектором услуг.

Ещё одним важным приложением технологии распределённого реестра является сфера вопросов государственно-частного управления, а также управления внутри организации. В частности, особой популярности достигла система электронного голосования на основе платформы блокчейн. Кроме того, блокчейн используется при регистрации компаний, анализе деятельности организации, взаимодействии с другими участниками. Повсеместное использование технологии блокчейн стало осуществимым ввиду возможности свободно интегрировать цифровые идентификаторы в любую систему.

Менее изученной с точки зрения возможности применения, но не менее важной является сфера образования, где технология распределённого места пока не нашла своего места. На сегодняшний день технология имеет свои перспективы в области упрощения бюрократических процедур при движении контингента студентов между образовательными программами и учебными заведениями в рамках Болонского процесса, к которому Россия присоединилась в 2003 году, что

может значительно повысить мобильность студентов. Факультеты разных университетов будут вынуждены сильнее конкурировать за учащихся, так как при ненадлежащем уровне получаемых знаний студенту будет проще перевестись. Данный факт потенциально может повысить качество предоставляемых образовательных услуг и, следовательно, уровень человеческого капитала.

В заключение хочется отметим, что блокчейн и технология распределённого реестра в целом на сегодняшний день представляется крайне перспективной с точки зрения хранения данных, а также выстраивания децентрализованного механизма взаимодействия внутри фирмы, некоторого бизнес-сообщества или даже между государствами. Уже сегодня многие крупные компании из разных сфер экономики, консорциумы банков, а также центральные банки и государственные структуры запускают свои пилотные проекты, основанные на технологии распределённого реестра. Тем не менее, стоит понимать, что с точки зрения корпоративного и государственного сектора это всего лишь новый тип устройства базы данных, который, однако, в перспективе способен изменить облик бизнес-процессов, лежащих в основе операционной деятельности фирм, и повысить прозрачность органов власти.

СИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System // Bitcoin.org. 2008. URL: https://bitcoin.org/bitcoin.pdf

2. Codd E.F. A relational model of data for large shared data banks // Communications of the ACM. 1970. Vol. 13. No. 6. pp. 377-387.

3. Greenspan G. R3 Corda: Deep dive and technical review. A detailed look at the non-blockchain blockchain // Multichain.com. 2018. URL: https:// www.multichain.com/blog/2018/05/r3-corda-deep-dive-and-technical-review/

4. How is the blockchain different from distributed databases in terms of record keeping? // Quora.com. 2016. URL: https://www.quora.com/How-is-the-blockchain-different-from-distributed-databases-in-terms-of-record-keeping

5. Meunier S. Blockchain technology—a very special kind of Distributed Database // Medium.com. 2016. URL: https://medium.com/@sbmeunier/blockchain-technology-a-very-special-kind-of-distributed-database-e63d00781118

6. Brown R. On Distributed Databases and Distributed Ledgers // RICHARD GENDAL BROWN Thoughts on the future of finance. 2016. URL: https://gendal.me/ 2016/11/08/on-distributed-databases-and-distributed-ledgers/

7. World Bank. Distributed Ledger Technology (DLT) and Blockchain // WBG's FinTech Note | No. 1. 2017. URL: http://documents.worldbank.org/curated/en/ 177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf

8. Lamport L., Shostak R., and Pease M. The Byzantine generals problem // ACM Transactions on Programming Languages and Systems (TOPLAS). 1982. Vol. 4. No. 3. pp. 382-401.

9. Castro M., Liskov B. Practical Byzantine Fault Tolerance // OSDI. 1999. Vol. 99. pp. 178-186.

10. BitFury Group. Proof of Stake versus Proof of Work // Bitfury.com. 2015. URL: https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf

11. Vries A. Bitcoin's Growing Energy Problem // Joule. 2018. Vol. 2. No. 5. pp. 801-805.

12. Voshmgir S., Kalinov V. Types of Blockchains // In: Blockchain. A Begginers Guide / Ed. by Voshmgir S., Kalinov V. https://blockchainhub.net/, 2017. pp. 13-17.

13. Kravchenko P. Ok, I need a blockchain, but which one? // Medium.com. 2016. URL: https://medium.com/@pavelkravchenko/ok-i-need-a-blockchain-but-which-one-ca75c1e2100

14. Jew B., Samman G. Blockchain and Shared Ledgers. The New Age of the Consortium // Gilbert + Tobin. 2016. URL: https://www.gtlaw.com.au/insights/blockchain-and-shared-ledgers-new-age-consortium

15. Zamfir V. Introducing Casper “the Friendly Ghost” // Ethereum Blog. 2015. URL: https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/

16. Bentov I., Lee C., Mizrahi A. Proof of Activity: Extending Bitcoin’s Proof of Work via Proof of Stake // Cryptology ePrint Archive. 2014. URL: https://eprint.iacr.org/2014/452.pdf

17. Bentov I., Gabizon A., and Mizrahi A. Cryptocurrencies Without Proof of Work // Financial Cryptography and Data Security. FC 2016. Lecture Notes in Computer Science. 2016. Vol. 9604. pp. 142-160.

18. Seibold S., Samman G. Consensus. Immutable agreement for the Internet of value // KPMG. 2016. URL: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf

19. Goharshady A.K., Behrouz A., and Chatterjee K. Secure Credit Reporting on the Blockchain // arXiv preprint. May 2018. No. arXiv:1805.09104.

20. Greesin S. The Equifax Data Breach: What to Do // Federal Trade Comission Consumer Information. 2017. URL: https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

21. Medium Corporation. Smart contracts [Электронный ресурс] [2017]. URL: https://medium.com/vision-dti/smart-contracts-871160e7feac (дата обращения: 2.Май.2018).

22. DeCenter. Смарт-контракты и платформы для их реализации [Электронный ресурс] [2018]. URL: https://decenter.org/p/321-smart-contracts-rus (дата обращения: 2.Май.2018).

23. Github.com. EPOBC [Электронный ресурс] [2015]. URL: https://github.com/chromaway/ngcccbase/wiki/EPOBC_simple (дата обращения: 2.Май.2018).

24. Bitcoin Magazine. The next step to improve Bitcoin's flexibility, scalability and privacy is called MAST [Электронный ресурс] [2016]. URL: https://bitcoinmagazine.com/articles/the-next-step-to-improve-bitcoin-s-flexibility-scalability-and-privacy-is-called-mast-1476388597/ (дата обращения: 2.Май.2018).

25. RSK. White paper overview 2015. URL: https://uploads.strikinglycdn.com/files/ec5278f8-218c-407a-af3c-ab71a910246d/RSK%20White%20Paper%20-%20Overview.pdf (дата обращения: 2.Май.2018).

26. Bitcoinmining.com. Sidechains explained 2016. URL: https://www.bitcoinmining.com/sidechains-explained/ (дата обращения: 2.Май.2018).

27. Eskandari S., Clark J., Sundaresan V., Adham M. On the feasibility of decentralized derivatives 2018. URL: https://arxiv.org/pdf/1802.04915.pdf (дата обращения: 1.Май.2018).

28. DeCenter. Блокчейн-оракулы как связь между цифровым и реальным миром [Электронный ресурс] [2018]. URL: https://decenter.org/blockchain/360-blockchain-oracles-rus (дата обращения: 2.Май.2018).

29. DeCenter. Smart Contracts [Электронный ресурс] [2018]. URL: https://decenter.org/blockchain/344-smart-contracts-rus (дата обращения: 2.Май.2018).

30. Ассоциация Финтех. Децентрализованная сеть обмена и хранения информации "Мастерчейн". White paper, версия 1.1 2017. URL: http://fintechru.org/documents/Masterchain_whitepaper_11_08.pdf (дата обращения: 7.Март.2018).

31. Ripple.com. Ripple to Place 55 Billion XRP in Escrow to Ensure Certainty of Total XRP Supply [Электронный ресурс] [2017]. URL: https://ripple.com/insights/ripple-to-place-55-billion-xrp-in-escrow-to-ensure-certainty-into-total-xrp-supply/ (дата обращения: 7.Март.2018).

32. Sommer, Deppe G., Stehling V., Haberstroh M., and Hees. Request for Comments: Proposal of a Blockchain for the Automatic Management and Acceptance of Student Achievements // E-Prüfungs-Symposium. Aachen. 2018.

33. Novotny P., Zhang Q., Hull , Baset S., Laredo , Vaculin , Ford D., and Dillenberger D.N. Permissioned Blockchain Technologies for Academic Publishing // Information Services & Use. 2018.