Сергей В. Запечников[1, 2]
[1]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
[2]Центр развития криптовалют и цифровых финансовых активов ВИНИТИ РАН,
Усиевича ул., 20, г. Москва, 125190, Россия
e-mail: SVZapechnikov@mephi.ru, https://orcid.org/0000-0002-7975-6040

СИСТЕМЫ РАСПРЕДЕЛЕННОГО РЕЕСТРА КАК ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ ДОВЕРИЯ МЕЖДУ УЧАСТНИКАМИ БИЗНЕС-ПРОЦЕССОВ

DOI: http://dx.doi.org/10.26583/bit.2019.4.03

Аннотация. Статья посвящена проблеме применения систем распределенного реестра в качестве инструментария обеспечения доверия между участниками бизнес-процессов. Цель статьи состоит в том, чтобы предложить систематизированный взгляд на прикладные аспекты современных технологий распределенного реестра, опираясь на опыт исследования технического устройства и алгоритмического наполнения наиболее известных и востребованных блокчейн-платформ. Рассматриваются основные идеи, положенные в основу систем распределенного реестра, архитектура таких систем, проводится их классификация. Анализируются принципы работы и особенности двух важнейших классов систем распределенного реестра: открытого и закрытого типа. Дается обзор сфер применения и возможностей систем распределенного реестра с точки зрения потенциального потребителя этой технологии. Проводится анализ актуальных проблем развития систем распределенного реестра. Даются прогнозы о перспективных и неперспективных приложениях систем распределенного реестра. Делаются выводы о том, что технологии распределенного реестра, являясь попыткой создать универсальный инструментарий решения проблемы доверия при дистанционном осуществлении деловых отношений с использованием информационно-телекоммуникационных систем, обладают большим потенциалом роста, однако характеризуются рядом нерешенных проблем, связанных с повышением производительности и обеспечением конфиденциальности информации об участниках деловых отношений.

Ключевые слова: распределенный реестр, блокчейн-технологии, криптовалюта, консенсус, репликация сервисов, конфиденциальность.

Для цитирования: ЗАПЕЧНИКОВ, Сергей В. СИСТЕМЫ РАСПРЕДЕЛЕННОГО РЕЕСТРА КАК ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ ДОВЕРИЯ МЕЖДУ УЧАСТНИКАМИ БИЗНЕС-ПРОЦЕССОВ. Безопасность информационных технологий, [S.l.], v. 26, n. 4, p. 37–53, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1230>. Дата доступа: 01 dec. 2019. doi:http://dx.doi.org/10.26583/bit.2019.4.03 .

Sergey V. Zapechnikov[1, 2]
[1]National Research Nuclear University MEPHI,
Kashirskoe shosse, 31, Moscow, 115409, Russia
[2]Research Center for Cryptocurrencies and Digital Assets,
Usievicha str., 20, Moscow, 125190, Russia
e-mail: SVZapechnikov@mephi.ru, https://orcid.org 0000-0002-7975-6040

Distributed ledger as a tool to ensure trust among business process participants

DOI: http://dx.doi.org/10.26583/bit.2019.4.03

Abstract. The paper is devoted to the problem of using distributed ledgers as a tool to ensure trust among business process participants. The purpose of the paper is to offer a systematic review of the applied aspects of modern distributed ledger technologies, based on the experience of studying the technical and algorithmic concepts of the most famous and popular blockchain platforms. We analyze the main ideas underlying distributed ledgers, discuss in general the architecture of distributed ledger platforms, and classify existing systems. The principles of operation and features of permissionless and permissioned

blockchain platforms are considered. An overview of the scope and capabilities of distributed ledgers from the perspective of a potential consumer of this technology is given. The actual problems of distributed ledgers are analyzed. Predictions are made about promising and unpromising applications of distributed registry systems. It is concluded that distributed ledger technologies, as an attempt to create a universal tool to solve the problem of trust in the remote implementation of business relations, have great potential for growth. However, they are characterized by a number of unresolved problems related to improving throughput and ensuring the business partners' privacy.
Keywords: distributed ledger, blockchain technologies, cryptocurrency, consensus, state machine replication, confidentiality.
For citation: ZAPECHNIKOV, Sergey V. Distributed ledger as a tool to ensure trust among business process participants. IT Security (Russia), [S.l.], v. 26, n. 4, p. 37–53, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1230>. Date accessed: 01 dec. 2019. doi:http://dx.doi.org/10.26583/bit.2019.4.03.

Введение

Системы распределенного реестра – одна из самых ярких и востребованных идей последнего времени в области информационных технологий. Другие популярное название систем распределенного реестра – блокчейн-системы, или блокчейн-технологии. Им посвящено огромное количество научно-технической и научно-популярной литературы, разработано большое количество обучающих курсов, руководств пользователей и разработчиков. В этих условиях становится трудно написать о блокчейн-технологиях что-либо новое. В этой связи автор видит целью данной статьи предложить читателю систематизированный взгляд на прикладные аспекты блокчейн-технологий, опираясь на свой опыт исследования технического устройства и алгоритмического наполнения платформ, а также руководствуясь своим опытом преподавания этого предмета студентам и слушателям курсов повышения квалификации. Этот опыт подсказывает, что слушателю и читателю, скорее всего, будет не интересно глубокое погружение в описание криптографических протоколов или последовательное изложение математической теории консенсуса (хотя, по убеждению автора, в этом и заключается красота новой технологии). Гораздо важнее те эффекты, которые они способны создать для потенциального потребителя блокчейн-технологии, а также инструменты, которые они способны предоставить разработчику приложений. То и другое в совокупности способно создать некоторые новые условия для реализации многих процессов деловой деятельности. На этих аспектах блокчейн-технологий автор и предполагает сосредоточиться в данной статье.

Сразу оговоримся, что автор считает предпочтительным термин «системы распределенного реестра», а не «блокчейн-технологии». Как будет показано в дальнейшем, собственно метод выстраивания цепочки блоков (blockchain в переводе с английского – «цепочка блоков») – лишь один, хотя и совершенно необходимый компонент систем распределенного реестра. Тем не менее, ввиду широкой распространенности термина «блокчейн-технологии» в отечественной и зарубежной литературе будем в рамках настоящей статьи считать его (почти) литературным синонимом термина «системы распределенного реестра».

Вместе с тем, хотелось бы с самого начала предостеречь читателя от легкомысленного взгляда на этот предмет. Устройство систем распределенного реестра очень сложно, причем их сложность существенно выросла от первых образцов таких систем (например, Bitcoin) к нынешним гораздо более функциональным, производительным и защищенным платформам. Если бы блокчейн-платформы были так просты, как о них пишут многие популярные источники, эти платформы появились бы не в начале XXI века, а гораздо раньше. Но это не так.

Как коротко ответить на вопрос, что такое блокчейн-технологии? Автор предпочел бы ответить, что это комплекс технологий, каждая из которых по отдельности была известна ранее, но только совместное их применение позволило получить синергетический эффект. К этим технологиям относятся, прежде всего:

- одноранговые сети (peer-to-peer networks);
- системы управления базами данных, обычно базами данных типа «ключ-значение» («key – value»);
- технологии резервирования баз данных и репликации сервисов (SMR – state-machine replication);
- криптографические методы защиты информации.

Для каких целей созданы и применяются блокчейн-технологии? Автор предпочел бы ответить, что, в первую очередь, для решения проблемы доверия при совместной деловой деятельности большого круга лиц (реализации каких-либо бизнес-процессов). Системы распределенного реестра, прежде всего, предназначены для работы в обстановке, когда группа физических и (или) юридических лиц, частично или полностью не доверяющая друг другу, заинтересована в решении некоторой общей задачи. При этом важнейшей отличительной особенностью систем распределённого реестра от всех ранее известных систем информационных технологий в том, что информационная система строится не в рамках какой-то одной, выделенной организации (предприятия, учреждения), а вокруг бизнес-процесса. Ответам на эти и связанные с ними вопросы будет посвящена предлагаемая статья.

1. Основные идеи, положенные в основу систем распределенного реестра

Систематизируем основные идеи, заложенные в основу систем распределенного реестра. Прежде всего, следует отметить, что системы распределенного реестра являются разновидностью распределенных компьютерных систем. В силу этого они обладают всеми характерными чертами распределенных систем, но имеют целый ряд особенностей.

1. Система распределенного реестра – полностью *децентрализованная* система. Нет ни одного такого узла, который можно вывести из строя, чтобы разрушить или заблокировать всю систему, также нет главных и второстепенных узлов – все они равнозначны. Это свойство обеспечивается одноранговой (пиринговой) сетью.

2. Система распределенного реестра предполагает наличие в ее составе некоторой базы данных для хранения реестра. Каждый узел сети поддерживает синхронную (или почти синхронную) с остальными узлами копию общей базы данных и историю транзакций с ней. Это качество называется *репликацией* сервиса (SMR – state machine replication), а каждый отдельный узел сети, обеспечивающий реализацию этой идеи, – репликой. Репликация является развитием принципа резервирования баз данных, но предполагает не просто поддержание синхронной с остальными узлами копии базы данных, а синхронное с ними выполнение операций над копией базы данных, причем строго в одной и той же последовательности на всех узлах. Самая сложная проблема репликации – обеспечение непротиворечивости состояния реплик. Для этого используется ряд сложных технических приемов, рассмотрение которых выходит за рамки настоящей статьи.

3. Базу данных системы можно только дополнять. Никакие изменения в ранее внесенные записи не допускаются. Таким образом, формируется *нередактируемый* реестр транзакций. Эта особенность является ключевой для систем рассматриваемого типа. Реализуется она посредством криптографических механизмов, главным из которых являются криптографические хэш-функции, обладающие свойствами однонаправленности

и трудности обнаружения коллизий. Они позволяют ввести зависимости между последовательными блоками данных в базе, формируя цепочку блоков таким образом, что между каждым новым блоком и предыдущим существует однонаправленная функциональная зависимость. Внесение исправлений в любой из блоков цепочки, а именно, изменение хотя бы одного бита, приводит к необходимости внесения изменений в каждый последующий блок, что не может остаться незамеченным. Более того, в силу принципа репликации редактирование одной из копий базы данных не может остаться незамеченным, так как остальные копии базы данных остаются неизменными. Более того, механизмы обеспечения непротиворечивости при обнаружении рассинхронизации реплик стремятся как можно быстрее снова привести их в синхронное состояние. При отсутствии возможности редактировать уже имеющиеся в базе данных записи (блоки) единственным способом внесения изменений в реестр является его дополнение новыми записями (блоками).

4. Любые новые записи в реестр можно вносить только с согласия квалифицированного большинства участников. В зависимости от технологии под большинством понимается либо 1/2 + 1 голос, либо 2/3 + 1 голос участников системы. Этот принцип называется *консенсусом.* Для обеспечения консенсуса используются специальные протоколы взаимодействия узлов, которые в значительной степени различаются для систем различных типов. Проблема достижения консенсуса является одной из фундаментальных проблем распределенных вычислений [1].

5. Внесение новых записей в реестр может сопровождаться выполнением произвольного, сколь угодно сложного программного кода, в котором могут описываться правила взаимодействия участников сообщества, правила их обращения с активами, которые учитываются в базе данных, а также условия и события, возникающие за рамками системы. Такой код принято называть *смарт-контрактом*. Впервые идея смарт-контракта предложена Н. Сабо [2].

Соединение рассмотренных идей позволяет построить простейшую математическую модель системы распределенного реестра [3].

Пусть задана функциональность *F*: каждая операция *o* преобразует реестр из состояния *s* в новое состояние *s'* и может вырабатывать ответ *r*:

$$(s', r) \leftarrow F(s, o).$$

Для каждого реестра формулируется условие валидности операции, а именно, операция при текущем состоянии реестра должна удовлетворять некоторому предикату *P()*:

$$P(s, o) = "True".$$

Реестр может только пополняться, а значит, каждая операция *o* присоединяет блок валидных транзакций $\{tx\}$ к реестру. Записи реестра формируют цепочку блоков, связанных криптографической хэш-функцией:

$$h_t \leftarrow Hash([tx_1, tx_2, \ldots] \parallel h_{t-1} \parallel t).$$

Благодаря этому все содержимое реестра проверяемо, начиная с последнего блока в порядке уменьшения порядковых номеров блоков.

2. Архитектура систем распределенного реестра

Архитектуры всех существующих систем распределенного реестра могут быть обобщены в виде предлагаемой далее трехуровневой модели.

Нижний уровень – *транспортный.* Практически во всех известных системах распределенного реестра он представляет собой *одноранговую,* или пиринговую (peer-to-peer) *сеть* – сеть, состоящую из узлов, или, как принято говорить, нод (node), в которой нет выделенных клиентов и серверов, все ноды равны по своим функциям и роли в системе. В разные моменты времени они, участвуя в протоколе, могут исполнять роль либо клиента, либо сервера. Строго говоря, равны все ноды, выполняющую одну и ту же функцию, но между нодами сети может существовать разделение обязанностей (это имеет место в некоторых системах распределенного реестра нового поколения). Клиенты могут подключаться к нодам, но они не являются участниками сети. Однако одноранговая сеть не устраняет полностью клиент-серверную модель взаимодействия: клиентское программное обеспечение, предоставляющее пользователям интерфейс доступа к системе, по-прежнему взаимодействует с нодами одноранговой сети по клиент-серверной модели. И хотя традиционный сервер здесь заменяется на одноранговую сеть, но программа-клиент всегда взаимодействует с какой-то одной нодой, предполагая, что она является одной из реплик, синхронной с остальными.

Средний уровень архитектуры – *уровень хранения данных.* Это и есть распределенный реестр, ради которого создается система. Он представлен базой данных специального вида, которая поддерживается совместными усилиями всех узлов. В базе хранится собственно набор данных, представляющих ценность для сообщества бизнес-партнеров, а также история операций с этими данными (транзакций).

Если отвлечься от физического представления базы данных в виде цепочки блоков, то формируемая в реестре логическая структура данных представляет собой двудольный ациклический направленный граф (DAG – Directed acyclic graph). Два типа вершин этого графа соответствуют состояниям реестра и переходам между ними. Граф имеет единственную вершину-источник, которая соответствует генезис-блоку цепи. По мере совершения новых транзакций и формирования новых блоков происходит рост графа.

Представление этого графа в разных системах распределенного реестра может отличаться. Так, на криптовалютной платформе Bitcoin на каждой ноде хранится копия всей истории транзакций от первого блока до текущего момента времени. Состояния – в данном случае балансы электронных кошельков пользователей – хранятся только у самих пользователей в их программных или аппаратных криптокошельках – на нодах эта информация не хранится.

На платформе Hyperledger Fabric на каждой ноде хранится копия базы данных типа «ключ-значение», описывающая текущее состояние всех активов (т.е. все «несгоревшие» вершины графа) и копия всей истории транзакций от первого блока до текущего момента времени.

Каждая транзакция заверяется *электронной цифровой подписью*, чтобы можно было точно установить, кто ее автор.

Транзакции собираются в блоки, блоки в цепочку. Транзакции внутри блока связываются в специальную структуру данных, называемую деревом Меркле [4]. Часто возникает вопрос, почему транзакции собирают в блоки?

Система распределенного реестра, как правило, является высоконагруженной системой, поэтому:

- утверждение блоков транзакций сообществом перед присоединением к реестру более выгодно, чем утверждение отдельных транзакций, хотя размер блока можно сократить до одной транзакции на блок;
- в то же время пользователь не может ждать бесконечно, поэтому формирование новых блоков должно происходить с приемлемой для пользователя частотой.

Верхний уровень архитектуры – *прикладной.* В общем случае он представлен смарт-контрактами – программным кодом, исполняемым каждой нодой сети или выделенным подмножеством нод сети при одобрении (валидации) транзакций.

Простейший вариант построения прикладного уровня можно наблюдать в криптовалютных системах распределенного реестра первого поколения. Это частный случай, когда смарт-контрактов как таковых нет. Вместо этого есть просто множество наборов данных вида

(*адрес, баланс*),

где *адрес* – это некоторая числовая последовательность, символизирующая адрес электронного кошелька, принадлежащего кому-то из пользователей системы, *баланс* – сумма средств в единицах криптовалюты, содержащаяся на счету этого электронного кошелька.

Единственная разрешенная транзакция в таких системах – перевод криптовалюты между кошельками:

(адрес_1, баланс – сумма_перевода),
(адрес_2, баланс + сумма_перевода).

Условие валидности транзакции – сумма балансов двух кошельков после транзакции не должна быть больше суммы балансов кошельков до транзакции (меньше она становится в том случае, если системе уплачивается комиссия за проведение транзакции).

3. Классификация систем распределенного реестра

Под *платформой распределенного реестра (блокчейн-платформой)* будем понимать конкретное воплощение технологии распределенного реестра в виде программного комплекса, работающего на выделенной аппаратной платформе или с использованием средств виртуализации.

Платформы распределенного реестра можно подразделить на три класса: платформы открытого типа, закрытого типа и комбинированные.

Платформы *открытого типа (permissionless), или публичные* позволяют стать участниками платформы неограниченному кругу лиц, никакой регистрации или отзыва полномочий не требуется. Примерами таких платформ являются Bitcoin [5], Ethereum [6] и абсолютное большинство других криптовалютных платформ

Платформы *закрытого типа (permissioned), или частные, или корпоративные* ограничивают круг участников пределами сообщества, для участия требуется регистрация, при выходе из сообщества право доступа отзывается. Примерами таких платформ являются все платформы, созданные в рамках проекта Hyperledger (самые известные – Hyperledger Fabric, Hyperledger Iroha, Hyperledger Sawtooth) [7], а также платформы Corda [8], Tendermint [9], Quorum [10], Exonum, NEM Catapult и др.

Следует отметить, что русскоязычные названия платформ: открытого и закрытого типа – весьма условны, так как не передают смысла исходных англоязычных названий. Более точно было бы называть их соответственно платформами, не требующими разрешения на участие и требующими разрешения на участие.

Наконец, платформы *смешанного, или комбинированного, типа* – это платформы открытого типа, которые используют для достижения консенсуса технологии построения платформ закрытого типа. Пока такие платформы не находят широкого практического

применения – в этой сфере преобладают экспериментальные разработки. В качестве примеров можно привести платформы Toda-Algorand, Omniledger, BitcoinNG и др.

4. Системы распределенного реестра открытого типа

Отметим важнейшие особенности платформ распределенного реестра открытого типа.

- Участники могут легко добавляться и выходить из блокчейн-сети, от присутствия или отсутствия конкретного участника в целом ничего не зависит, возможно анонимное участие (точнее, псевдонимное, поскольку транзакции, выполненные под одним и тем же псевдонимом, отслеживаемы).
- Формирование новых блоков транзакций на этих платформах происходит посредством «доказательства выполнения работы» (proof-of-work), «доказательства обладания долей» (proof-of-stake) или другим аналогичным способом, каждый из которых реализует *принцип лотереи*.
- Для работы блокчейн-платформы открытого типа *требуется криптовалюта*, чтобы стимулировать майнеров. Это требование сохраняется вне зависимости от того, создается ли сама по себе платформа распределенного реестра как криптовалютная либо как универсальная. Таким образом, появляется требование наличия как «внешней», так и «внутренней» криптовалюты. «Внешняя» нужна для урегулирования обязательств участников в рамках исполнения смарт-контрактов, «внутренняя» – для вознаграждения нод, выполняющих полезную работу в интересах всего сообщества. «Внешняя» и «внутренняя» криптовалюта может быть одинаковой (Bitcoin) или разной (Ethereum: эфир и газ).
- Блокчейн-платформы открытого типа очень ресурсоемки (электроэнергия, машинное время): предполагается, что к 2035 году на майнинг биткоинов будет тратиться столько же электроэнергии, сколько сейчас потребляет среднее европейское государство (обычно в качестве примера приводится Дания).

Ключевой особенностью платформ открытого типа является специфический механизм достижения консенсуса при записи новых блоков в реестр. Поскольку для платформы открытого типа неизвестно точное число ее участников в каждый конкретный момент времени, невозможно отсчитать, какое количество нод должно проголосовать для достижения консенсуса. В этой связи в качестве критерия достижения консенсуса должно использоваться не просто достаточное количество участников сети, а какая-либо другая величина: достаточная доля вычислительной мощности сети, достаточная доля криптовалютных ресурсов, которой в совокупности обладают участники, стремящиеся достичь консенсуса, либо что-то еще.

Два самых широко распространенных механизма достижения консенсуса для систем распределенного реестра открытого типа носят названия доказательства выполнения работы (proof-of-work) и доказательства обладания долей (proof-of-stake).

При *доказательстве выполнения работы* каждая из нод включается в решение вычислительно сложной задачи. В системе Bitcoin, например, используется задача подбора такой случайной добавки к формируемому новому блоку реестра, чтобы хэш-код очередного нового блока, записываемого в реестр, удовлетворял условию специального вида, например, чтобы первые 20 битов хэш-кода были бы нулевыми. Поскольку хэш-функция обладает очень хорошими перемешивающими свойствами, то заранее угадать такое значение случайной добавки, при котором получится нужный хэш-код, невозможно. Единственный способ – это последовательно перебирать все возможные значения. Рано или поздно одна из нод найдет такую добавку и разошлет ее и вычисленный ею хэш-код всем остальным нодам для проверки. Как только они убедятся, что вычисление проведено

верно, новый блок будет записан каждой из нод в свою копию реестра. Такая вычислительно сложная работа делается нодами не бесплатно: тот, кто первым решит эту задачу, получит вознаграждение в криптовалюте. Сам процесс решения вычислительно сложной задачи, заканчивающийся в случае успеха получением вознаграждения, называется майнингом (mining) – буквально «добычей» криптовалюты. Чтобы нарушить безопасность блокчейна, в котором для записи транзакций используется доказательство выполнения работы, злоумышленнику нужно сосредоточить у себя более 50% вычислительной мощности сети, что значительно сложнее, чем просто создать большое число фиктивных участников, которое превысит 50% участников системы и которым не нужно делать ничего, кроме как голосовать.

При *доказательстве обладания долей* каждый из участников блокчейн-сети получает право заверить вновь созданный блок своей электронной подписью, и право это случайным образом передается от одного участника к другому с вероятностью, пропорциональной тому, какой долей криптовалюты от общего объема выпущенной в обращение криптовалюты он обладает. Этот способ побуждает участников сети не переводить средства в другие криптовалюты или в фиатные валюты, а хранить их внутри сети. Вознаграждение в виде эмиссии криптовалюты за создание нового блока здесь не предусмотрено, поэтому единственным видом вознаграждения является комиссия за совершенную транзакцию, взимаемая с отправителя средств. Для большинства блокчейн-платформ с доказательством обладания долей характерно, что весь объем криптовалюты эмитируется сразу, при запуске платформы, хотя есть варианты и с дополнительной эмиссией. Сам алгоритм «доказательства долей» устроен следующим образом: все время функционирования системы делится на временные слоты равной длины, в каждом из которых должен быть порожден один новый блок, добавляемый в реестр. Для каждого временного слота среди участников платформы псевдослучайным образом выбирается лидер. Как было отмечено выше, вероятность выбора лидером конкретного участника пропорциональна имеющейся у него доле криптовалюты. Лидер формирует блок по правилам, установленным протоколом блокчейн-сети, после чего подписывает блок своей электронной подписью и рассылает его для проверки всем остальным участникам. После того как более половины общего числа участников платформы проверят созданный лидером блок, в том числе проверят его подпись под этим блоком, и обменяются сообщениями о положительном результате проверки, блок присоединяется к реестру. Далее выбирается новый лидер для нового временного слота и т.д. Чтобы нарушить безопасность системы распределенного реестра, в которой для записи транзакций используется доказательство обладания долей, злоумышленнику нужно сосредоточить у себя более 50% финансовых ресурсов сети, что также сделать трудно, а усовершенствовав алгоритм, можно добиться того, чтобы этот порог поднялся до 90%.

Однако ни первый, ни второй способы не защищают полностью от злоупотреблений: группа злоумышленников, сговорившись, в принципе может сосредоточить у себя очень значительные вычислительные и финансовые ресурсы и записать в реестр выгодную ей информацию. Чтобы избежать такой неприятности, в последнее время все чаще используется сочетание двух способов: для записи блока проводится как доказательство выполнения работы (правда, менее трудоемкое), так и доказательство обладания долей, так что гарантии безопасности значительно повышаются.

5. Системы распределенного реестра закрытого типа

Главные особенности платформ распределенного реестра закрытого типа состоят в следующем.

- Участники не могут самостоятельно добавляться и выходить из блокчейн-сети – для этого центр регистрации, называемый на разных платформах либо удостоверяющим центром, либо провайдером членства (MSP – membership service provider) и т.п., должен выдать участнику его цифровой идентификатор и ключи.
- Формирование новых блоков транзакций происходит за 3 шага:
  1) исполнение смарт-контрактов и валидация транзакций;
  2) упорядочение отдельных транзакций в блок;
  3) выполнение протокола консенсуса.
- Протоколы, позволяющие достичь консенсуса путем голосования, гораздо менее трудоемки, чем любой из способов, используемых для платформ открытого типа (на несколько порядков величины). Как следствие, блокчейн-платформы закрытого типа обладают высоким быстродействием и хорошей масштабируемостью.
- Для работы блокчейн-платформы закрытого типа *не требуется криптовалюта*.

Как и в случае с платформами открытого типа, ключевой особенностью платформ закрытого типа является реализованный в них механизм консенсуса. Поскольку для платформ закрытого типа число участников точно известно в каждый конкретный момент времени, для достижения консенсуса может быть применен *принцип голосования*. Строго говоря, система распределенного реестра требует реализации не просто протокола консенсуса, а так называемого протокола атомарной широковещательной рассылки [11], так как репликам необходимо не просто согласовывать добавление к реестру одиночных записей, но и строго сохранять порядок транзакций, а значит, последовательность изменения состояний реестра. Тем не менее, в повседневной практике прижилось именно понятие консенсуса, поэтому при нестрогом анализе вопроса можно пользоваться и этим термином. В настоящее время известно более 700 протоколов консенсуса, работающих при различных предположениях о модели противника. Краткий обзор некоторых протоколов, реализованных на платформах закрытого типа, и их свойств, можно найти в [12]. Различают два основных типа таких протоколов: отказоустойчивые (CFT – crash fault-tolerant) и устойчивые к «византийским» атакам (BFT – byzantine fault-tolerant) *(принцип голосования)*. Под «византийскими» понимают атаки активного противника, который может вести себя произвольным образом, в том числе посылая остальным участникам сети некорректные и противоречивые сообщения. Название происходит от так называемой «задачи о византийских генералах» [13].

Использование протоколов, основанных на голосовании, предоставляет большую гибкость в построении системы распределенного реестра. Так, роли нод, исполняющих смарт-контракты, достигающих консенсуса, вносящих изменения в реестр и хранящих копии реестра в принципе могут быть разделены, что позволяет повысить быстродействие платформы и доверие к ней пользователей. Перечисленные факторы делают платформы закрытого типа очень привлекательными инструментами обеспечения доверия бизнес-процессов уровня корпораций, консорциумов, альянсов. На них также могут быть реализованы криптовалюты и приложения со смарт-контрактами, требующими расчеты в криптовалюте, но при этом криптовалюта остается только «внешней» по своей роли в системе.

6. Возможности и сферы применения систем распределенного реестра

Все множество известных применений систем распределенного реестра можно разделить на два направления: чисто реестровые применения, а также использование их в качестве платформы для функционирования децентрализованных приложений.

Чисто реестровые применения. Блокчейн-платформы могут использоваться как базы данных со специальными свойствами, обеспечивающими повышенную степень доверия между участниками, – распределенный реестр (distributed ledger).

Из рассмотренных выше технических основ функционирования блокчейн-технологий можно вывести следующие основные свойства распределенного реестра:

1) невозможно изменить историю транзакций, записанных в реестр;
2) копии реестра у всех участников блокчейн-платформы синхронизированы;
3) добавление новых блоков транзакций в реестр выполняется только в результате достижения консенсуса между участниками сообщества, поддерживающего реестр;
4) формируемая в результате ведения реестра структура данных, описывающая активы предметной области, представляет собой ациклический ориентированный граф.

Возможные сферы применения чисто реестровых приложений в основном связаны с заменой уже существующих реестров, ведущихся в традиционной форме, на децентрализованные: реестров недвижимого имущества, реестров ЗАГС, реестров акционеров и т.п., либо с созданием новых при возникновении общественной потребности в них.

Существуют платформы, поддерживающие только реестровую функцию и не поддерживающие функционирование децентрализованных приложений. Примеры таких платформ – BigchainDB, BlockCipher, FlureeDB и др. Их обычно не рассматривают в качестве полноценных блокчейн-платформ, а позиционируют как базы данных со специальными свойствами, в частности, с поддержкой блокчейна.

Децентрализованные приложения. Это та сфера применения блокчейн-технологий, в которой в наибольшей степени раскрывается их потенциал. Над распределенным реестром выстраивается прикладной уровень: смарт-контракты (альтернативные названия – chaincode, DApps и т.п.) и взаимодействующие с ними клиентские приложения – таким образом, блокчейн-платформа становится платформой децентрализованных вычислений. Фронтенд-компоненты децентрализованных приложений ничем не отличаются от традиционных клиентских приложений и вполне могут быть реализованы любым программистом, знакомым с веб-разработкой. В то же время бэкенд-компоненты существенно отличаются от традиционных серверных компонентов распределенных приложений. На смену им приходят смарт-контракты, взаимодействующие между собой и с клиентскими компонентами через соответствующие интерфейсы. Смарт-контракты исполняются параллельно всеми либо специально выделенными для этого нодами блокчейн-платформы (модель исполнения смарт-контрактов сильно зависит от выбора платформы).

Модель децентрализованных приложений хорошо коррелирует с основной бизнес-идеей блокчейн-технологий – возможностью учета в распределенном реестре жизненного цикла любых видов активов и выполнение сколь угодно сложных операций над этими активами в процессе их перехода из одной фазы (стадии) жизненного цикла в другую. В соответствии с широко распространенными среди экономистов понятиями, активом называется все, что обладает ценностью [14]. Активы делятся на реальные и финансовые. Реальные активы – это вещественные (материальные) ценности: оборудование, здания, мебель, бытовая техника и т.п. Финансовые активы – это ценности, представленные ценными бумагами. Финансовые активы, в свою очередь, делятся на денежные (деньги) и

неденежные (ценные бумаги – акции и облигации). Операции над активами могут быть обусловлены составом участников бизнес-процесса, их атрибутами и состояниями в текущий момент времени, событиями вне системы. Примерами активов, учитываемых в системах распределенного реестра, могут служить денежные средства, ценные бумаги, товары, транспортные средства и пр.

Следует отметить, что понятие актива в данном случае выходит за рамки чисто экономического, так как в реестрах может вестись учет прав и обязательств сторон, что при традиционных формах деловой деятельности не относят ни к денежным, ни к неденежным активам: например, имущественных прав, прав доступа к информации, платежных обязательств, обязательств поставки товаров или оказания услуг. Это приводит к возникновению совершенно новых обстоятельств, которые условно можно называть машиночитаемыми нормами права. Практическая реализация концепции «автоматизации» гражданско-правовых отношений пока находится лишь в самой начальной стадии.

Среди наиболее перспективных областей применения децентрализованных приложений выделяются [15]:

- системы международных банковских переводов;
- международная торговля: экспортно-импортные операции;
- системы валовых расчетов реального времени (RTGS – Real-Time Gross Settlement);
- страхование: обработка страховых случаев;
- обслуживание гарантийных обязательств производителей техники;
- логистика: управление цепочками поставок (supply chain management), в том числе транспортная логистика;
- кредитование юридических лиц: синдицированный кредит;
- медицинские информационные системы: управление доступом к медицинским данным.

Вместе с этим, мировым научно-техническим сообществом постоянно выдвигаются и прорабатываются новые идеи применения блокчейн-технологий в ранее не затронутых ими сферах.

7. Актуальные проблемы технологий распределенного реестра

Двумя главными проблемами систем распределенного реестра в настоящее время остаются производительность и информационная безопасность. Рассмотрим каждую из них подробнее.

Производительность. Скорость записи новых транзакций в базу данных распределенного реестра значительно ниже, чем в традиционных системах, а по сравнению с такими высоконагруженными системами, как международные системы платежей по банковским картам, – на несколько порядков ниже. Так, средняя пропускная способность платформы Bitcoin составляет порядка 7 транзакций в секунду, платформы Ethereum – порядка 70–100 транзакций в секунду, а баз данных систем Visa и Mastercard при пиковой нагрузке – порядка 50–70 тысяч транзакций в секунду. В связи с этим проблема масштабирования систем распределенного реестра стоит очень остро. И хотя новые платформы распределенного реестра имеют потенциально существенно более высокую производительность, достигающую нескольких тысяч или даже 10–20 тысяч транзакций в секунду, разрыв по-прежнему остается заметным.

Можно выделить несколько путей решения проблемы масштабируемости систем распределенного реестра:

- Научный поиск, разработка новых протоколов консенсуса и структур данных. Это наиболее долгий, затратный и трудоемкий путь, который требует разработки «с нуля» новых платформ на базе новых протоколов.
- Экстенсивный путь: увеличение количества транзакций в блоках, сокращение транзакционной инертности и т.п. Реализация этого способа связана с так называемыми хардфорками – обновлениями программного обеспечения нод сети, создающими проблему отсутствия обратной совместимости.
- Изменение архитектуры вычислительного процесса, а именно, вынос части вычислительной работы из смарт-контрактов вовне распределенного реестра (так называемые off-chain-вычисления). Этот путь фактически означает совмещение блокчейн-платформ с традиционными технологиями и создание распределенных систем обработки данных сложной архитектуры. Особенно часто такое решение применяется при необходимости хранения большого объема данных, которые физически невозможно сохранить в распределенном реестре – тогда данные, как правило, хранятся во внешнем облачном хранилище, а в распределенном реестре остаются лишь метаданные или их часть, например, данные, связанные с управлением правами доступа.
- Изменение архитектуры распределенного реестра. Наиболее известное решение – это создание разветвленных реестров – так называемых lightning networks. С целью разгрузки распределенного реестра от большого количества транзакций в этом случае создаются дополнительные, побочные реестры со своими локальными цепочками блоков, а в главном реестре сохраняются только корни локальных цепочек, которые служат свидетельством выполнения сразу большой серии транзакций, например, связанной с выполнением смарт-контракта.

Информационная безопасность. Большинство систем распределенного реестра в нынешнем их виде обеспечивает высокую доступность (невозможность уничтожения) и целостность (гарантии неизменности) информации, но не обеспечивает конфиденциальности информации, так как все записи в базе данных видны для всех участников системы.

Проблемы обеспечения конфиденциальности также решаются несколькими путями:

- Научный поиск, разработка и внедрение новых криптографических механизмов: вероятностных неинтерактивных доказательств, проверяемых вычислений и др. Пионерами во внедрении таких механизмов являются криптовалютные платформы zCash [16] и Monero [17], а также ориентированная на финансовые приложения платформа Quorum [10].
- Архитектурные решения на уровне блокчейн-платформы по разграничению доступа к реестру. Примером такого подхода служит механизм каналов на платформе Hyperledger Fabric [7]. Каждый канал по сути представляют собой отдельный распределенный реестр, который поддерживается нодами участников канала, составляющими подмножество нод сети. Ноды остальных участников сети, не являющихся участниками канала, просто не хранят данные из этого канала, а потому доступ к каналу для них невозможен (напомним, что Hyperledger Fabric является платформой закрытого типа, а потому доступ к ней невозможен без регистрации). Таким образом, любая блокчейн-сеть, работающая под управлением платформы Hyperledger Fabric, представляет собой множество сконфигурированных администратором каналов, что позволяет реализовать довольно сложные модели разграничения доступа, вплоть до создания системы двусторонних каналов между каждой парой участников сети

8. Перспективы развития технологий распределенного реестра

Нынешняя ситуация в сфере развития блокчейн-технологий характеризуется завершением этапа завышенных ожиданий и стабилизацией интереса к этой области как отдельной ветви информационных технологий.

По мнению автора, в ближайшем будущем блокчейн-технологии, наряду с уже широко известными и признанными отраслями информационных технологий, такими как системы управления базами данных, системами мгновенного обмена сообщениями, облачными технологиями и др., займут достойное место в современном «цифровом» мире. Блокчейн-платформы открытого и закрытого типа, по всей видимости, будут развиваться в рамках нескольких конкурирующих продуктов с вероятной тенденцией дальнейшего сокращения их числа в ходе конкурентной борьбы. Такая ситуация – появление на раннем этапе развития технологии большого количества альтернативных решений с последующим «выживанием» сильнейших – характерна для рынка информационных технологий.

Основные сферы применения систем распределенного реестра будут связаны с теми технологиями, где они способны послужить основным или ведущим инструментом обеспечения доверия между участниками бизнес-процессов, принести значительный экономический эффект. К таким сферам, несомненно, относятся логистика (управление цепями поставок, управление грузоперевозками), банковский сектор (системы межбанковских платежей), системы публичного распределения заказов и работ (разновидности краудсорсинговых систем).

Обобщая позитивные эффекты от внедрения систем распределенного реестра, можно сделать вывод, что потенциальными сферами их применения являются все те системы, которые связаны с обработкой ресурсов, имеющих высокую ценность, и при этом при традиционной реализации имеют сильно централизованную архитектуру. Примером могут служить межбанковские системы валовых расчетов реального времени. Замена централизованной архитектуры таких систем на децентрализованную способна поднять на качественно новый уровень решение проблемы обеспечения непрерывности бизнеса.

Другой потенциальной сферой применения систем распределенного реестра являются области деловой деятельности, до сих пор слабо затронутые компьютеризацией из-за ведомственной разобщенности, исторически сложившихся традиций, юридических и нормативно-правовых ограничений. Примером может служить международная торговля, где при поставке партий товаров из одной страны в другую оформляются десятки и сотни сопроводительных документов, обусловленных пограничным, таможенным, экспортным контролем, ветеринарными и фитосанитарными правилами, требованиями и интересами транспортных компаний, международных транспортных коридоров, грузовладельцев, грузополучателей, грузоперевозчиков, экспедиторов, надзорных и арбитражных органов и пр. участников процесса.

Вместе с тем, блокчейн-технологии не являются универсальных средством обеспечения доверия, а тем более автоматизации бизнес-процессов. Во многих случаях внедрение блокчейн-технологий либо не способно привнести какие-либо существенные изменения в процессы деловой деятельности, либо приводят к прямым убыткам. Примером может послужить сфера государственных и муниципальных услуг. В большинстве государств, например, традиционно существуют государственные органы, уполномоченные на ведение реестра недвижимого имущества и сделок с ним, реестра юридических лиц, реестра индивидуальных предпринимателей, реестра записи актов гражданского состояния и т.п. Замена централизованного порядка ведения таких реестров

на децентрализованный не только приводит к утрате государственного контроля за соответствующей сферой, но и не создает никаких стимулов для «рядовых» граждан или юридических лиц участвовать в поддержании такого реестра. Например, почти каждое физическое или юридическое лицо имеет некоторое недвижимое имущество, сведения о котором (или о сделках с ним) должны содержаться в реестре, но как убедить его в необходимости сохранять в своей копии реестра огромный объем сведений о «чужой» недвижимости, которые, к тому же, в большинстве случаев являются конфиденциальными? Очевидно, что в такой ситуации ведение реестров в традиционной, централизованной форме гораздо удобнее и проще. Вместе с тем, создание децентрализованного реестра нотариальных действий на базе блокчейн-платформы закрытого типа, с введением обязанности для нотариусов поддерживать ноду с экземпляром реестра выглядит вполне оправданным и позволит избежать потенциальных злоупотреблений с нотариально составленными (заверенными) документами. Таким образом, решение о реализации и внедрении систем автоматизации бизнес-процессов на основе традиционных или блокчейн-технологий зависит от очень многих факторов и в каждом случае должно приниматься обоснованно с учетом всех этих факторов и последствий.

Также, по мнению автора, чисто криптовалютные приложения блокчейна не имеют большой исторической перспективы. Аргументами в пользу такого мнения служат следующие факты. Во-первых, курсы практически всех криптовалют нестабильны, они подвержены большой волатильности, во-вторых, в отличие от фиатных валют, не существует экономического обоснования их стоимости – это чисто спекулятивный актив. Безусловно, они имеют право на существование, во-первых, как средство быстрых международных расчетов, во-вторых, как инвестиционный актив, и в-третьих, как средство расчетов между сторонами смарт-контрактов в блокчейн-платформах, но в качестве постоянного инструмента ведения бизнеса они в большинстве случаев неудобны, в первую очередь, из-за непредсказуемости рыночного курса.

Представляет интерес возможность выпуска участниками блокчейн-сообществ собственных криптовалют или, как чаще говорят, токенов. Выпуск токенов – это удобная форма краудфандинга, т.е. общественного сбора средств на осуществление какой-либо деятельности. Суть этого приема в том, что организация, которая только начинает свою деятельность и нуждается в первоначальном капитале (стартап), выпускает в обращение электронные токены, которые продает инвесторам за один или несколько видов криптовалют. Инвесторы приобретают (или не приобретают) токены, основываясь на бизнес-плане стартапа и иной маркетинговой информации, которую публикуют учредители стартапа. Чем убедительнее будет выглядеть бизнес-план и интереснее предлагаемый к реализации проект, тем больше вероятность успешной продажи токенов. В зависимости от того, какими именно благами (или услугами) учредители стартапа предполагают в дальнейшем рассчитаться с инвесторами, токены могут быть больше похожи на криптовалюту либо на электронный аналог акций – ценных бумаг, выпускаемых акционерными обществами.

Первичный выпуск в обращение токенов принято называть ICO – Initial Coin Offering**.** Краудфандинг в форме ICO имеет безусловные преимущества для учредителей стартапов по сравнению с традиционным получением средств в форме кредитования. Учредители собирают некоторую сумму средств в криптовалюте, которую они в дальнейшем могут обменивать на фиатные валюты. В то же время ICO несет значительные риски для инвесторов, поскольку сбор средств по существу происходит «под честное слово» со стороны учредителей, обещание в будущем вознаградить

инвестора либо ростом цены приобретенных им токенов, либо возможностью воспользоваться услугами или приобрести продукцию стартапа (если проект будет реализован). Такая процедура сбора средств не защищает инвестора от мошенничества. Известны многочисленные случаи, когда организаторы краудфандинга даже не собирались реализовывать заявленный проект и исчезали вместе с собранной криптовалютой. Поэтому законодательное регулирование ICO и вопросы обеспеченности токенов активами выпустившего их предприятия остаются одними из самых горячо обсуждаемых тем во многих странах мира.

Заключение

Анализ актуального положения дел в сфере создания и применения систем распределенного реестра позволяет сделать следующие выводы.

Концепция распределенного реестра является попыткой создать универсальный инструментарий решения проблемы доверия при дистанционном осуществлении деловых отношений с использованием информационно-телекоммуникационных систем. Идея распределенного реестра воплощена в целом ряде программных платформ открытого, закрытого и комбинированного типа, большинство из которых задуманы как универсальные, но некоторые имеют свою специализацию. Платформы позволяют разрабатывать прикладные программы для многих сфер деловых отношений. Наибольшую выгоду внедрение приложений на основе платформ распределенного реестра приносит в тех областях, где бизнес-процессы включают в себя значительное количество физических и юридических лиц, разделенных государственными и ведомственными барьерами. Информационная система с использованием распределенного реестра строится вокруг бизнес-процесса, а не в рамках отдельных организаций. Распределенные реестры позволяют учитывать практически все существующие виды бизнес-активов, а программная оболочка вокруг них – создавать цифровую среду для реализации договорных, нормативно-правовых и финансовых отношений между участниками бизнес-процессов с использованием инструментов машиночитаемого права и цифровых финансовых активов.

Системы распределенного реестра обладают большим потенциалом роста, однако характеризуются рядом нерешенных или не до конца решенных проблем, основные из которых связаны с повышением производительности и обеспечением конфиденциальности информации об участниках деловых отношений. Применение систем распределенного реестра совместно с развивающимися технологиями конфиденциальных вычислений (secure multi-party computations) и конфиденциального машинного обучения (privacy-preserving machine learning) способно принести большой экономический эффект, дать толчок реализации новых бизнес-процессов и развитию новых сфер деловой деятельности.

СПИСОК ЛИТЕРАТУРЫ:

1. Damgard, I. Secure distributed systems / I. Damgard, J. B. Nielsen, C. Orlandi. Electronic book, 2018. – 332 p. URL: https://blackboard.au.dk/webapps/blackboard/content/listContent.jsp?course_id=_116846_1&content_id=_1801036_1&mode=reset (дата обращения: 14.10.2019).
2. Szabo, N. Smart contracts: Building blocks for digital markets / N. Szabo. 1996. – 11 p. URL: https://pdfs.semanticscholar.org/9b6c/d3fe0bf5455dd44ea31422d015b003b5568f.pdf (дата обращения: 14.10.2019).
3. Cachin, C. Blockchain, cryptography, and consensus / C. Cachin // ITU workshop on security aspects of blockchain. Switzerland, Geneva, 2017. – 38 p. URL: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201703/Documents/Christian%20Cachin%20blockchain-itu.pdf (дата обращения: 14.10.2019).

4. Merkle, R. C. A Digital Signature Based on a Conventional Encryption Function/ R. C. Merkle // Advances in Cryptology — CRYPTO '87. Lecture Notes in Computer Science. Vol. 293. 1988. P. 369–378.
5. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system / S. Nakamoto. 2006. – 9 p. URL: https://bitcoin.org/bitcoin.pdf (дата обращения: 14.10.2019).
6. Wood, G. Ethereum: A secure decentralized generalized transaction ledger. Byzantium version / G. Wood // GitHub repository. 2019. – 39 p. URL: https://ethereum.github.io/yellowpaper/paper.pdf (дата обращения: 18.10.2019).
7. Hyperledger project site. 2019. URL: https://www.hyperledger.org/ (дата обращения: 18.10.2019).
8. Hearn, M. Corda: a distributed ledger / M. Hearn, R. G. Brown // Corda platform site. 2019. – 73 p. URL: https://www.r3.com/wp-content/uploads/2019/08/corda-technical-whitepaper-August-29-2019.pdf (дата обращения: 18.10.2019).
9. Buchman, E. The latest gossip on BFT consensus / E. Buchman, J. Kwon, Z. Milosevic // Open access paper. 2019. – 14 p. URL: https://arxiv.org/pdf/1807.04938.pdf (дата обращения: 18.10.2019).
10. Baliga, A. Performance Evaluation of the Quorum Blockchain Platform / A. Baliga, I. Subhod, P. Kamat, S. Chatterjee // Open access paper. 2019. – 8 p. URL: https://arxiv.org/pdf/1809.03421.pdf (дата обращения: 18.10.2019).
11. Cachin C. Secure and efficient asynchronous broadcast protocols / C. Cachin, K. Kursawe, F. Petzold, V. Shoup // Advances in Cryptology: CRYPTO 2001, volume 2139 of Lecture Notes in Computer Science. Springer, 2001. P. 524–541.
12. Cachin, C. Blockchain Consensus Protocols in the Wild / C. Cachin, M. Vukolic // Proc. 31st Intl. Symposium on Distributed Computing (DISC 2017), ed. Andréa W. Richa, 91:1:1–1:16. Leibniz International Proceedings in Informatics (LIPIcs). Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik. 2017. URL: http://dx.doi.org/10.4230/LIPIcs.DISC.2017.1 (дата обращения: 18.10.2019).
13. Lamport, L. The Byzantine generals problem / L. Lamport, R. Shostak, M. Pease // ACM Transactions on programming languages and systems. Vol. 4. No. 2. July 1982. P. 382–401. URL: https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf (дата обращения: 18.10.2019).
14. Шевчук, Д.А. Макроэкономика: конспект лекций / Д.А. Шевчук, В.А. Шевчук // М.: Высшее образование, 2007. – 169 с.
15. The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services // World Economic Forum. Aug. 2016. – 130 p. URL: http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf (дата обращения: 18.10.2019).
16. Hopwood, D. Zcash protocol specification / D. Hopwood, S. Bowe, T. Hornby et al. // Zcash documentation site. 2019. – 149 p. URL: https://github.com/zcash/zips/raw/master/protocol/protocol.pdf (дата обращения: 18.10.2019).
17. Alonso, K. M. Zero to Monero: A technical guide to a private digital currency; for beginners, amateurs, and experts (v. 1.0.0) / K. M. Alonso // Monero technical documentation site. 2018. – 91 p. URL: https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf (дата обращения: 18.10.2019).

REFERENCES:

[1] Damgard, I. Secure distributed systems. I. Damgard, J. B. Nielsen, C. Orlandi. Electronic book, 2018. – 332 p. URL: https://blackboard.au.dk/webapps/blackboard/content/listContent.jsp?course_id=_116846_1&content_id=_1801036_1&mode=reset (accessed: 14.10.2019).
[2] Szabo, N. Smart contracts: Building blocks for digital markets. N. Szabo. 1996. – 11 p. URL: https://pdfs.semanticscholar.org/9b6c/d3fe0bf5455dd44ea31422d015b003b5568f.pdf (accessed: 14.10.2019).
[3] Cachin, C. Blockchain, cryptography, and consensus. C. Cachin. ITU workshop on security aspects of blockchain. Switzerland, Geneva, 2017. – 38 p. URL: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201703/Documents/Christian%20Cachin%20blockchain-itu.pdf (accessed: 14.10.2019).
[4] Merkle, R. C. A Digital Signature Based on a Conventional Encryption Function/ R. C. Merkle. Advances in Cryptology — CRYPTO '87. Lecture Notes in Computer Science. Vol. 293. 1988. P. 369–378.
[5] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. S. Nakamoto. 2006. – 9 p. URL: https://bitcoin.org/bitcoin.pdf (accessed: 14.10.2019).
[6] Wood, G. Ethereum: A secure decentralized generalized transaction ledger. Byzantium version G. Wood. GitHub repository. 2019. – 39 p. URL: https://ethereum.github.io/yellowpaper/paper.pdf (accessed: 18.10.2019).
[7] Hyperledger project site. 2019. URL: https://www.hyperledger.org/ (accessed: 18.10.2019).

[8] Hearn, M. Corda: a distributed ledger M. Hearn, R. G. Brown. Corda platform site. 2019. – 73 p. URL: https://www.r3.com/wp-content/uploads/2019/08/corda-technical-whitepaper-August-29-2019.pdf (accessed: 18.10.2019).
[9] Buchman, E. The latest gossip on BFT consensus E. Buchman, J. Kwon, Z. Milosevic. Open access paper. 2019. – 14 p. URL: https://arxiv.org/pdf/1807.04938.pdf (accessed: 18.10.2019).
[10] Baliga, A. Performance Evaluation of the Quorum Blockchain Platform A. Baliga, I. Subhod, P. Kamat, S. Chatterjee. Open access paper. 2019. – 8 p. URL: https://arxiv.org/pdf/1809.03421.pdf (accessed: 18.10.2019).
[11] Cachin C. Secure and efficient asynchronous broadcast protocols C. Cachin, K. Kursawe, F. Petzold, V. Shoup. Advances in Cryptology: CRYPTO 2001, volume 2139 of Lecture Notes in Computer Science. Springer, 2001. P. 524–541.
[12] Cachin, C. Blockchain Consensus Protocols in the Wild C. Cachin, M. Vukolic. Proc. 31st Intl. Symposium on Distributed Computing (DISC 2017), ed. Andréa W. Richa, 91:1:1–1:16. Leibniz International Proceedings in Informatics (LIPIcs). Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik. 2017. URL: http://dx.doi.org/10.4230/LIPIcs.DISC.2017.1 (accessed: 18.10.2019).
[13] Lamport, L. The Byzantine generals problem / L. Lamport, R. Shostak, M. Pease. ACM Transactions on programming languages and systems. Vol. 4. No. 2. July 1982. P. 382–401. URL: https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf (accessed: 18.10.2019).
[14] Shevchuk, D.A. Makroekonomika: konspekt lektsiy D.A. Shevchuk, V.A. Shevchuk. M.: Vysshee obrazovanie, 2007. – 169 p. (in Russian).
[15] The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services. World Economic Forum. Aug. 2016. – 130 p. URL: http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf (accessed: 18.10.2019).
[16] Hopwood, D. Zcash protocol specification D. Hopwood, S. Bowe, T. Hornby et al. Zcash documentation site. 2019. – 149 p. URL: https://github.com/zcash/zips/raw/master/protocol/protocol.pdf (accessed: 18.10.2019).
[17] Alonso, K. M. Zero to Monero: A technical guide to a private digital currency; for beginners, amateurs, and experts (v. 1.0.0) K. M. Alonso. Monero technical documentation site. 2018. – 91 p. URL: https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf (accessed: 18.10.2019).

Поступила в редакцию – 18 октября 2019 г. Окончательный вариант – 18 ноября 2019 г.
Received – October 18, 2019. The final version – November 18, 2019.