А.Ю. ЧУРИЛОВ

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН

Монография

ЮСТИЦ ИНФОРМ

Алексей Чурилов

Правовое регулирование применения технологии блокчейн

«Юстицинформ»
2021

УДК 347.13
ББК 67.404

Чурилов А. Ю.

Правовое регулирование применения технологии блокчейн / А. Ю. Чурилов — «Юстицинформ», 2021

ISBN 978-5-7205-1739-7

В монографии рассмотрены проблемы правового регулирования использования технологии блокчейн. Исследована криптовалюта как объект гражданских прав, в том числе проведен сравнительный анализ криптовалюты с иными объектами и определено место криптовалюты в системе объектов гражданских прав. Проанализированы особенности правового регулирования заключения смарт-контрактов и исполнения возникающих при этом обязательств. Изучены проблемы правового регулирования иных способов использования блокчейн технологии, в частности при работе с персональными данными, осуществлении предпринимательской деятельности. Монография рассчитана на широкий круг читателей и представляет интерес для преподавателей, аспирантов, студентов вузов, практикующих юристов. В формате PDF A4 сохранен издательский макет книги.

УДК 347.13
ББК 67.404

ISBN 978-5-7205-1739-7

Содержание

Алексей Чурилов
Правовое регулирование применения технологии блокчейн. Монография

Рецензенты:

Вайпан В.А. – проректор МГУ имени М.В. Ломоносова, профессор кафедры предпринимательского права Юридического факультета МГУ Почетный юрист города Москвы, доктор юридических наук

Гончарова В.А. – ассистент кафедры гражданского права Юридического института Томского государственного университета, кандидат юридических наук

A.YU. CHURILOV
LEGAL REGULATION OF THE USE OF BLOCKCHAIN TECHNOLOGY
Monograph
Moscow YUSTITSINFORM 2021

Reviewers:

Vaypan V.A. – Vice-Rector of Lomonosov Moscow State University; Professor at Business Law Department of Law Faculty, Lomonosov Moscow State University; Honorary Lawyer of Moscow; Doctor of Law

Goncharova V. A. – Assistant at the Civil Law Department; Law Institute of Tomsk State University; PhD in Law

Churilov A.Yu.

Legal regulation of the use of blockchain technology: monograph / A.Yu. Churilov. – M.: Yustitsinform, 2021. – 152 p.

The monograph examines the problems of legal regulation of the use of blockchain technology. The author investigates cryptocurrency as an object of civil rights, providing a comparative analysis of cryptocurrency with other objects and so determines the place of cryptocurrency in the system of civil rights objects. The features of the legal regulation of the conclusion of smart contracts and the performance of obligations arising in this case are analyzed. The problems of legal regulation of other ways of using blockchain technology, in particular when working with personal data, carrying out entrepreneurial activities, are studied.

The monograph is intended for a wide range of readers, it may be of interest to teachers, graduate students, university students, and practicing lawyers.

Keywords: blockchain, object of law, cryptocurrency, smart contract, contract, obligation, performance of an obligation, entrepreneurial activity, personal data.

Введение

Биткоин – это технологический tour de force.
Билл Гейтс

Технология блокчейн превратилась в настоящий Святой Грааль десятилетия. Многочисленные исследования, посвященные этой технологии; курсы повышения квалификации и вебинары, проводимые известными учеными; многочисленные попытки интегрировать блокчейн в повседневную жизнь свидетельствуют о популярности рассуждений о тех преимуществах, той «великой» пользе, которую несет в себе эта технология. По утверждениям исследователей, известные преимущества блокчейн-технологии, такие как децентрализация, прозрачность и неизменяемость транзакций, могут существенно повысить надежность и эффективность традиционных корпоративных процедур в области ведения реестра, голосования на общих собраниях, корпоративного контроля и аудита[1], помогут преодолеть недостатки в сфере государственного управления[2] и т. д. Помимо неочевидности этой самой пользы с точки зрения, как минимум, энергоэффективности[3], по-прежнему и в литературе возникают многочисленные дискуссии по вопросам правового регулирования использования блокчейна в экономическом обороте[4].

Первое упоминание технологии блокчейн (Blockchain) можно обнаружить в работе, написанной человеком или группой людей под псевдонимом Сатоши Накамото (Satoshi Nakamoto) «Биткоин: пиринговая электронная денежная система»[5]. С момента своего запуска блокчейн-технология получила применение практически во всех сферах экономики и до сих пор является предметом оживленных дискуссий в научном сообществе. Начавшаяся исключительно как платежная система, оперирующая Биткоинами, технология вышла за те рамки, которые изначально были задуманы создателем – смарт-контракты, коллегиальное принятие решений, хранение информации, государственные услуги, Интернет вещей являются далеко не единственными примерами применения блокчейн-технологии. Возникают организации, управление которыми осуществляется на платформе блокчейн[6].

При этом далеко не все существующие способы применения и использования блокчейн-технологии находятся в правовом поле, а некоторые из них нарушают требования действующего законодательства. Применение этой технологии позволяет обходить валютное регулирование, избегать валютного контроля, упрощает процесс перемещения средств, полученных преступным путем и т. д. Адекватное и корректное регулирование возникающих отношений является краеугольным камнем существования и применения блокчейн-технологии.

В связи с популяризацией и развитием технологии блокчейн можно условно выделить два «поколения» развития этой технологии – Блокчейн 1.0, включающий в себя криптовалюту и платежную систему, оперирующую этой криптовалютой, и Блокчейн 2.0, представляющий собой разнообразные «надстройки» дополнительных протоколов в сети блокчейн, которая

---

[1] *Санникова Л.В.* Блокчейн в корпоративном управлении: проблемы и перспективы // Право и экономика. 2019. № 4. С. 27–36.

[2] *Талапина Э.В.* Блокчейн в государственном управлении: правовые перспективы и риски // Законы России: опыт, анализ, практика. 2019. № 5. С. 77–82.

[3] Одна только сеть блокчейн криптовалюты Биткоин потребляет 77 тераватт-часов электроэнергии в год – столько же, сколько потребляет государство Чили (URL: https://digiconomist.net/bitcoin-energy-consumption).

[4] См., напр.: *Нам К.В.* Правовые проблемы, связанные с применением блокчейна // Судья. 2019. № 2. С. 24–27.

[5] *Satoshi Nakamoto.* Bitcoin: A Peer-to-Peer Electronic Cash System // URL: https://bitcoin.org/bitcoin.pdf.

[6] Далеко не все из них являются удачными примерами – например, печально известная The DAO, собравшая более 150 миллионов долларов инвестиций и утратившая больше трети из них в результате взлома.

включает в себя иные способы применения, такие как смарт-контракты, «умная собственность», распределенное хранение информации и обмен информацией, а также многое другое.

Технология блокчейн

Прежде чем рассматривать особенности правового регулирования этой технологии, необходимо осветить основы и особенности ее функционирования.

Блокчейн был бы невозможен без возникновения Интернета и его постоянного развития. Поскольку основой функционирования блокчейн-технологии является Интернет, следует несколько слов сказать о возникновении и развитии глобальной информационно-телекоммуникационной сети Интернет. В работе не ставится цель объяснить читателю, как работает сеть Интернет на технологическом уровне, а лишь рассматриваются основные положения, которые влияют на особенности функционирования блокчейн-технологии.

Возникновение Интернета стало следствием необходимости удовлетворения потребности человечества в соединении нескольких компьютеров, находящихся на большом расстоянии друг от друга. Прародителем интернет-сети стала телефонная сеть, которая обеспечивала доступ к одному мощному компьютеров с нескольких устройств, удаленных друг от друга на многие тысячи километров (так называемая связь терминал – компьютер). В дальнейшем появились сети компьютер – компьютер. Точкой отсчета появления Интернета в том виде, в котором мы его понимаем сейчас, можно считать 1957 год, именно тогда Министерству обороны США понадобилась некая система для быстрой и надежной передачи данных, на помощь в этом вызвалась организация под названием DARPA, собравшая четыре научных учреждения для создания уникальной, ранее не существующей компьютерной сети. В 1969 году результатом их работы выступила новейшая созданная компьютерная сеть, названная ARPANET, объединившая в себе эти четыре учреждения. Позднее сеть подверглась быстрому развитию, и к ней стали присоединяться новые учреждения. В конце 1969 года состоялся первый сеанс передачи данных, который по праву ознаменовал рождение Интернета[7]. Сеть APRANET объединяла компьютеры разных типов, работавших под управлением различных операционных систем с дополнительными модулями, реализующими коммуникационные протоколы, общие для всех компьютеров в сети. Изначально уступавший по качеству и скорости связи локальным сетям, Интернет по праву можно считать самой быстрорастущей технической системой в истории человечества. По данным ТАСС, более 53 % населения Земли, или 4,1 млрд человек в настоящее время имеют доступ к Интернету[8]. Число устройств, подключенных к Интернету во всем мире, в настоящее время превышает 22 миллиарда.

Прежде чем переходить к рассмотрению общих принципов функционирования сети Интернет, необходимо прежде осветить важнейший стандарт в этой сфере. В начале 80-х годов рядом международных организаций по стандартизации, включая International Organization for Standardization (ISO), была разработана стандартная модель взаимодействия открытых систем (Open System Interconnection или OSI). Модель OSI была разработана на основании опыта, полученного при создании компьютерных сетей, в основном глобальных, и полное описание этой модели занимает более 1000 страниц текста[9]. Модель OSI определяет уровни взаимодействия систем в сетях с коммутацией пакетов, стандартные названия уровней и функции, которые должен выполнять каждый уровень, и описывает только системные средства взаимодействия, не включая при этом средства взаимодействия приложений конечных пользователей.

---

[7] *Кравченко Е.Ю., Булгакова М.В.* Развитие глобальной сети Интернет и его использование в малом предпринимательстве // Вестник Совета молодых ученых и специалистов Челябинской области. 2015. № 3. С. 83–86.

[8] URL: https://tass.ru/obschestvo/7080150.

[9] *Хахаев И.А.* Вычислительные машины, сети и системы телекоммуникаций в таможенном деле: учебное пособие. СПб.: Университет ИТМО, 2015. 86 с.

В модели OSI средства взаимодействия разделены на семь уровней – прикладной, представления, сеансовый, транспортный, сетевой, канальный и физический.

Физический уровень (physical layer) имеет дело с передачей потока битов по физическим каналам связи. Функции физического уровня реализуются на всех без исключения устройствах, которые подключены к сети. Единицей нагрузки физического уровня является бит или, если быть более точным, поток битов, которые нужно доставить – физический уровень не обрабатывает информацию.

Канальный уровень (data link layer) обеспечивает прозрачность соединения для сетевого уровня и ответственен за доставку данных адресату и их целостность. Для этого он выполняет следующие функции: устанавливает логическое соединение между взаимодействующими узлами, согласовывает в рамках соединения скорости передатчика и приемника информации и обеспечивает надежную передачу данных, а также обнаружение и коррекцию ошибок. Единицей нагрузки канального уровня является кадр (frame), состоящий из поля данных и заголовка. На этом уровне осуществляется адресация в сети посредством реализации еще одной функции канального уровня связи – функции управления доступом к среде (Medium Access Control или MAC). Следует отметить, что протокол канального уровня работает в пределах сети, входящей в виде одного из элементов в более крупную сеть, части которой объединены протоколами сетевого уровня. Адреса, с которыми работает протокол канального уровня, используются для доставки кадров только в пределах этой сети, а для перемещения единиц нагрузки между сетями применяется протокол и адреса следующего – сетевого – уровня.

Сетевой уровень (network layer) служит для образования единой транспортной системы и называемой составной сетью, или интернетом. Следует отметить, что Интернет (с прописной буквы) является реализацией как раз составной сети, построенной на основе технологии TCP/IP. Единицей нагрузки сетевого уровня является пакет (packet), заголовок которого имеет унифицированный формат, не зависящий от формата единиц нагрузки предыдущего уровня. Функции сетевого уровня реализуются группой протоколов и специальными устройствами – маршрутизаторами, посредством которых осуществляется физическое соединение сетей. Для того чтобы протоколы сетевого уровня могли доставлять пакеты любому узлу составной сети, эти узлы должны иметь уникальные в пределах этой составной сети адреса – такие адреса называются глобальными или сетевыми. На сетевом уровне определяются два вида протоколов – маршрутизируемые протоколы (реализуют продвижение пакетов через сеть) и маршрутизирующие протоколы (с их помощью осуществляется выбор маршрута движения пакетов).

Транспортный уровень (transport layer) обеспечивает приложениям и верхним уровням – прикладному, представления и сеансовому – передачу данных с соответствующей степенью надежности. Единицей нагрузки транспортного уровня является сегмент (segment) / датаграмма (datagram). Все протоколы, начиная с транспортного уровня, реализуются уже программными средствами устройств сети – компонентами их операционных систем. К транспортным протоколам относятся TCP и UDP, о которых речь пойдет далее.

Следующие три уровня работают одновременно на нескольких уровнях модели OSI, поэтому нет четкого разделения, в частности, на сеансовый и представительский уровни.

Сеансовый уровень (session layer) управляет взаимодействием участников сети, в том числе фиксирует активность каждой из сторон и предоставляет средства синхронизации сеанса. Благодаря этому протоколу в ходе передач данных стало возможным сохранять информацию о состоянии этих передач, чтобы в случае отказа можно было вернуться к передаче данных с прерванного момента, а не начинать сначала. Единицей нагрузки сеансового уровня являются данные (data).

Уровень **представления** (presentation layer) обеспечивает представление передаваемой по сети информации без изменения ее содержания. За счет этого уровня передаваемая прикладным уровнем одной системы информация всегда понятна прикладному уровню другой

системы. На этом уровне также выполняется шифрование и дешифрование данных, например, посредством протокола SSL (Secure Socket Layer). Единицей нагрузки уровня представления являются данные (data).

Прикладной уровень (application layer) представляет собой набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к общим ресурсам – файлам, принтерам, сайтам. Единицей нагрузки прикладного уровня являются данные (data). Это самый многочисленный и разнообразный уровень, в рамках которого выполняются все высокоуровневые протоколы. Самыми распространенными протоколами этого уровня являются почтовые протоколы (SMTP, IMAO, POP3), протоколы доступа к файлам (FTP, NFS) и протокол передачи гипертекстовых сообщений (HTTP).

Основой работы Интернета и обеспечения взаимодействия различных устройств являются протоколы адресации – это «клей, который скрепляет всю сеть Интернет»[10]. В настоящее время стандартной технологией в этой сфере является стек[11] протоколов TCP/ IP. Этот протокол выполняет три основные функции – согласование использования адресов различных типов, т. е. отображение адресов различных типов друг на друга (например, доменного имени на IP-адрес или локального адреса на глобальный); обеспечение уникальности адресов в сети Интернет (обеспечивается однозначность адресации в пределах Интернета, сети, подсети и т. д.); и конфигурирование сетевых интерфейсов и сетевых приложений.

Следует отметить, что в рамках стека протоколов TCP/IP любая сеть, входящая в составную сеть, рассматривается как средство транспортировки пакетов данных между двумя соседними сетями. Каждый протокол оперирует определенной единицей передаваемых данных, названия которых, как правило, закрепляются в существующих стандартах (см. рис. 1).

[10] *Yoo Christopher S.* Protocol Layering and Internet Policy // University of Pennsylvania Law Review. 2013. Vol. 161. P. 1707–1771.

[11] В данном случае – совокупность. Под стеком протоколов понимают иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети.

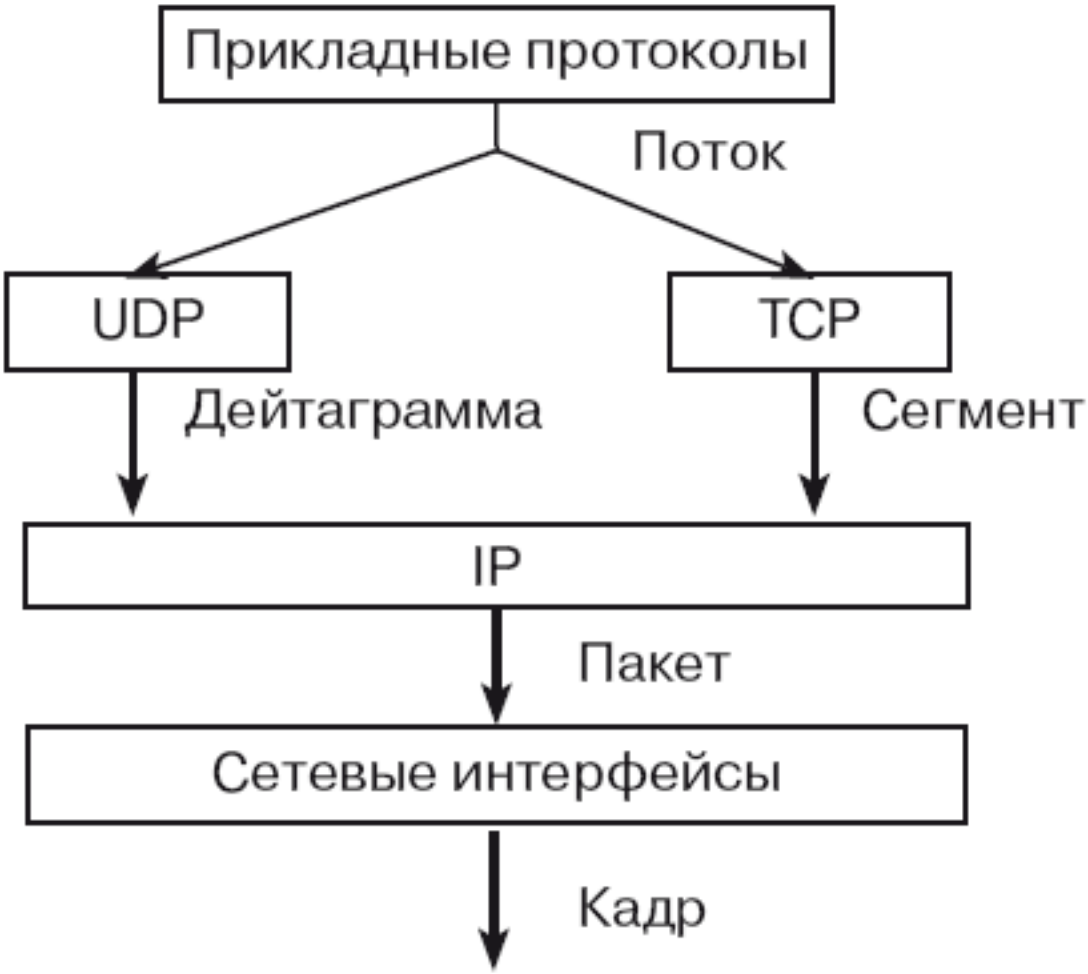


Рис. 1. Протокольные единицы данных в TCP/IP

Стек протоколов TCP/IP состоит из 4 основных уровней – прикладного, транспортного, сетевого и уровня сетевых интерфейсов. Каждый из этих уровней соответствует уровням модели OSI (см. рис. 2).

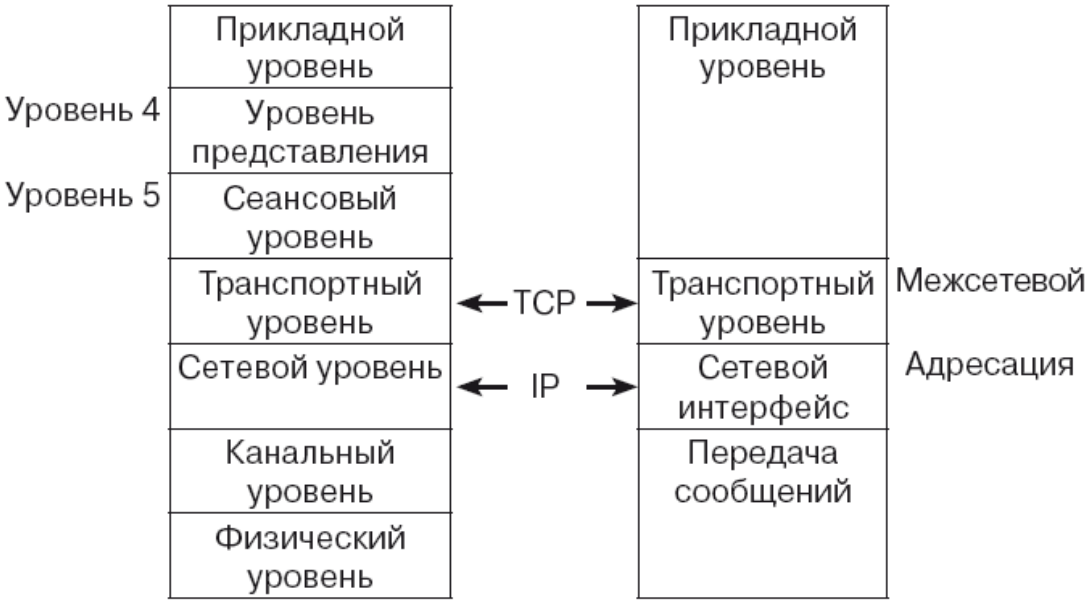


Рис. 2. Соотношение уровней модели OSI и TCP/IP

Прикладной уровень TCP/IP соответствует трем верхним уровням модели OSI (прикладному, представления и сеансовому) и состоит, в частности, из протоколов передачи данных (File Transfer Protocol, FTP), передачи почты (Simple Mail Transferring Protocol, SMTP), передачи гипертекста (Hypertext Transfer Protocol, HTTP).

Транспортный уровень, соотносящийся с транспортным уровнем модели OSI, представлен двумя важнейшими для функционирования сети, в том числе блокчейн, протоколами – протоколом управления передачей (Transmission Control Protocol, TCP) и протоколом пользовательских дейтаграмм (Usar Datagram Protocol, UDP). Для обеспечения надежной доставки данных от пользователя к пользователю протокол TCP предусматривает установление логического соединения, что позволяет ему нумеровать пакеты, подтверждать их прием, в случае потери организовывать повторные передачи, распознавать и уничтожать дубликаты, доставлять на прикладной уровень (например, при использовании FTP) пакеты в том порядке, в котором они были отправлены, что обеспечивает целостность и машиночитае-мость отправляемых данных.

Сетевой уровень, или уровень Интернета, является основным элементом архитектуры TCP/IP. Именно этот уровень обеспечивает перемещение пакетов в пределах составной сети, образованной объединением нескольких подсетей. Основным протоколом сетевого уровня является межсетевой протокол (Internet Protocol, IP). В его задачу входит передвижение пакетов данных между сетями – от одного узла к другому до тех пор, пока данные не попадут в сеть назначения.

Задача уровня **сетевых интерфейсов** достаточно проста – он отвечает только за организацию взаимодействия с подсетями, входящими в составную сеть TCP/IP – это протоколы Ethernet, FDDI, ATM, 802.11 (отвечающий за работу Wi-Fi) и другие.

В рамках TCP/IP для идентификации сетевых интерфейсов используются три типа адресов – локальные (аппаратные) адреса, сетевые адреса (IP-адреса) и символьные (доменные) имена. В большинстве сетевых технологий LAN (таких как Ethernet, FDDI) для однозначной[12] адресации интерфейсов используются MAC-адреса. Локальный в данном случае означает – действующий не во всей составной сети, а лишь в пределах подсети. Для объединения сетей

[12] Однозначность адресации имеет особое значение для реализации блокчейн-технологии и её правового регулирования.

в глобальную сеть технология TCP/IP использует глобальную систему адресации, которая не зависит от способов адресации элементов отдельных сетей. Для ее реализации формируется пара из номера сети и номера узла, которая в совокупности составляет сетевой адрес – IP-адрес, который идентифицирует не отдельный узел сети (компьютер или маршрутизатор), а одно сетевое соединение (сетевой интерфейс). При этом каждый раз, когда пакет данных отправляется адресату через составную сеть (Интернет), в его заголовке указывается IP-адрес узла назначения. Перед тем как отправить пакет в следующую сеть, маршрутизатор должен определить на основании найденного IP-адреса следующего маршрутизатора его локальный адрес. Поскольку между IP-адресом и локальным адресом узла не существует функциональной взаимосвязи, для их соотношения используется протокол разрешения адресов ARP (см. рис. 3).

Рис. 3. Процедура преобразования адресов

При этом для упрощения адресации в сети используются символьные имена соответствующих узлов. Составляющие полного символьного (или доменного) имени разделяются точкой и перечисляются в следующем порядке: простое имя хоста, имя группы хостов, имя более крупной группы (домена) и так до имени домена самого высокого уровня (например, ru, us).

Основы построения сетей в целом и сети Интернет в частности оказали существенное влияние на возникновение и развитие применения технологии блокчейн. Блокчейн-системы в своей работе используют TCP/IP протоколы и могут рассматриваться в качестве приложения прикладного уровня.

Блокчейн представляет собой базу данных, распределенную между всеми включенными в сеть блокчейн (Blockchain Network) устройствами, с использованием которой пользователи осуществляют передачу информации. Блокчейн-технология не является каким-либо единым явлением, именем собственным, – в настоящее время это собирательное название для всевозможных способов реализации идеи, лежащей в блокчейн-технологии. Для того чтобы полноправно относиться к блокчейн-технологии в том смысле, в котором она изначально была отражена в работе Сатоши Накамото, блокчейн-структура должна удовлетворять следующим критериям.

• Иметь децентрализованную технологическую основу, то есть информация должна быть распределенной между всеми узлами сети и должна поддерживаться в актуальном состоянии через процессы репликации и синхронизации.

• Поддерживать неразрывную связь между блоками данных путем формирования в каждом новом блоке ссылки на предыдущий по отношению к нему блок.

• Эффективно кодировать массивы данных в уникальные информационные блоки стандартного размера, т. е. хешировать данные.

• Применять в своей работе стойкие к взлому криптографические алгоритмы для защиты содержащейся в блоках информации.

• Использовать элементы специального подраздела математики – теории игр – для обеспечения соблюдения правил сети и достижения консенсуса при создании новых блоков [13].

Как известно, любая информация, в том числе информация о транзакциях, может быть представлена объемом данных, который в ней содержится. Так и информация о транзакциях в системе блокчейн представляет объем данных, объединенных в своего рода звенья, которые в свою очередь объединены в хронологическом порядке в цепочку блоков, в которой каждый предыдущий блок подтверждает действительность последующего путем включения информации о предыдущих транзакциях в виде особого криптографического ключа в заголовок каждого последующего блока транзакций (см. рис. 4)[14]. При этом каждый из участников сети (так называемые ноды[15]) хранит как минимум часть всей базы данных, что обеспечивает ее устойчивость к противоправным действиям со стороны как третьих лиц, так и самих участников. Под транзакцией в случае с блокчейн-технологией подразумевается любое взаимодействие между участниками блокчейн-системы – будь то передача какого-либо актива (например, криптовалюты) или передача информации – каждое из этих взаимодействий фиксируется в блоке системы.

Каждый блок, содержащий информацию о транзакциях в сети блокчейн, идентифицируется с помощью криптографического ключа – хэша (hash) – который генерируется с использованием криптографических алгоритмов, таких как SHA256 (используется в сети Биткоин)[16], SHA-3 (Ethereum) и другие. Инструмент хэширования информации является неотъемлемой частью технологии блокчейн – оно используется для адресации в блокчейн-сетях, для формирования электронной «подписи» транзакций, а также для создания новых блоков – т. е. «майнинга». Хэширование – это алгоритмический метод преобразования набора данных произвольного размера в стандартизированную строку фиксированной длины. Алгоритм преобразования, используемый в блокчейн-сетях, не допускает повторения одного и того же хэша в различных блоках, который свойственен более простым хэш-таблицам. Использование хэширования позволяет удостовериться в целостности информации, содержащейся в каждом последующем блоке в сети блокчейн, путем так называемой проверки «контрольной суммы», расчет которой основан на алгоритме хеширования. Для реализации этого подхода блокчейн-системы могут использовать, например, распределенные хэш-таблицы[17] или хэш-таблицы с прямым связыванием.

---

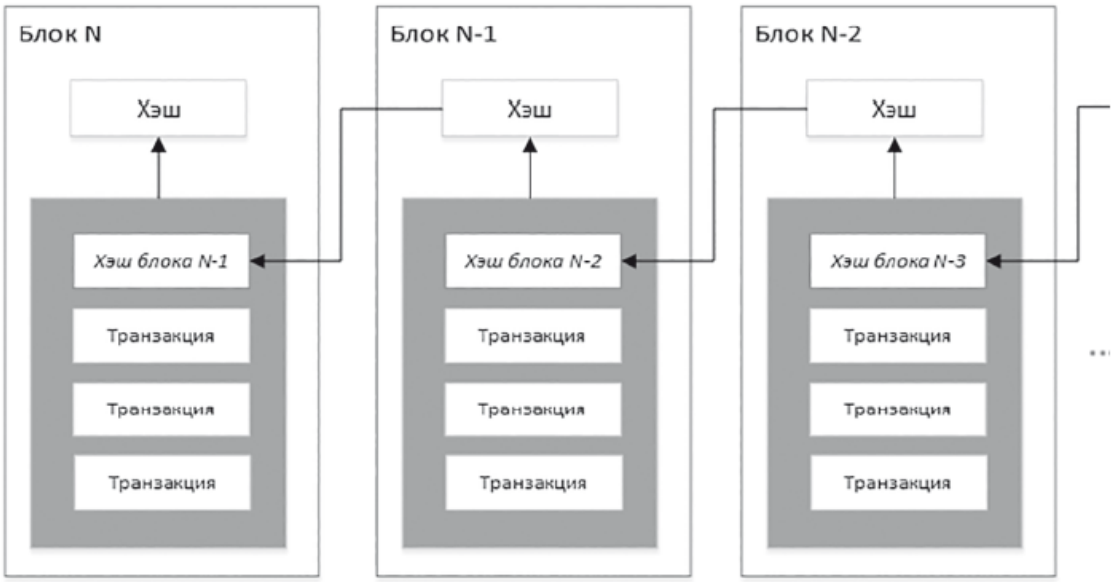
[13] Подробнее об этом см.: *Цихилов А.* Блокчейн. Принципы и основы. М.: Интеллектуальная Литература, 2019. С. 14–15.

[14] Отсюда и название технологии – Блокчейн – цепь блоков.

[15] Node.

[16] *Andreas M. Antonopoulos.* Mastering Bitcoin. O'Reily Media, 2015. P 170.

[17] *Matteo Bernardinetal.* Blockchains meet distributed hash tables: Decoupling validation from state storage // Distributed Ledger Technology Workshop. 2019. P. 43–55.



Использование такого механизма позволяет также гарантировать неизменность предыдущих блоков, поскольку хеширование каждого блока делает невозможным изменения содержания каждого предыдущего без изменения содержания каждого последующего блока – такое действие потребует такого количества времени и вычислительных мощностей систем, что делает такое действие нерациональным с экономической точки зрения (даже несмотря на привлекательную стоимость Биткоина в настоящий момент). Безусловно, когда речь идет о «неизменности» информации в сети блокчейн, это, в первую очередь, теоретическое предположение. Чем больше участников в блокчейн-системе, тем сложнее изменить содержание тех блоков, информация в которых возникла раньше, или вмешаться в процесс создания новых блоков. Вместе с тем существует возможность захвата контроля над блокчейн-сетью лицами, обладающих большими вычислительными мощностями – так называемая атака 51 %[18], при которой захват контроля над 51 % вычислительной мощности сети, необходимой для достижения консенсуса, позволит изменять как содержание предыдущих блоков, так и изменять информацию в создаваемых блоках. Такая ситуация произошла 25 апреля с блокчейн-сетью Bitcoin Gold – было похищено 18 миллионов долларов в результате атаки 51 %[19]. Более того, как уже отмечалось, каждый из участников сети хранит как минимум часть всей базы данных – следовательно, единовременно в популярных блокчейн-системах может существовать десятки тысяч копий всей информации, что еще больше усложняет попытки как-то изменить информацию о транзакциях.

Следует отметит, что майнинг, т. е. процесс добавления информации в сеть блокчейн, является основой функционирования этой технологии. На практике существуют различные способы организации майнинговой деятельности: соло-майнинг, при котором майнер добывает криптовалюту самостоятельно; майнинг через пулы – через серверы, которые могут объединять мощности персональных компьютеров многих майнеров; облачный майнинг, при котором майнер платит деньги какой-либо компании за оборудование, после чего данная компания берет на себя ответственность за установку оборудования и его настройку для работы[20].

---

[18] *Чаннов С.Е.* Использование блокчейн-технологий для ведения реестров в сфере государственного управления // Административное право и процесс. 2019. № 12. С. 29–34.

[19] *Помазанов В.В., Грищаев С.И.* Криптовалюта: криминалистическое прогнозирование // Российский следователь. 2018. № 11. С. 19–23.

[20] *Ершова И.В., Трофимова Е.В.* Майнинг и предпринимательская деятельность: в поисках соотношения // Актуальные

Важным механизмом, обеспечивающим безопасность и надежность хранения информации в сети блокчейн, является асимметричное шифрование, которое используется в этой системе. Под шифрованием понимается процесс превращения открытого текста в зашифрованный с помощью шифра – пары алгоритмов для шифрования и дешифрования соответствующей информации[21]. Ассиметричное шифрование, или шифрование с открытым ключом, позволяет устанавливать «доверительные» отношения между пользователями блокчейн-сети путем предоставления механизма для подтверждения целостности и достоверности транзакций, притом что сами транзакции фиксируются в публичной книге транзакций. В отличие от симметричного шифрования, в котором для кодирования и декодирования используется один и тот же ключ, в ассиметричном шифровании отправитель использует открытый ключ (public key) для шифрования сообщения, которое можно расшифровать только с помощью закрытого ключа (private key). Применительно к блокчейн-системам частные ключи используются для того, чтобы совершить (sign) транзакцию, которая будет отправлена на адрес, закрепленный за публичным ключом (см. рис. 5).

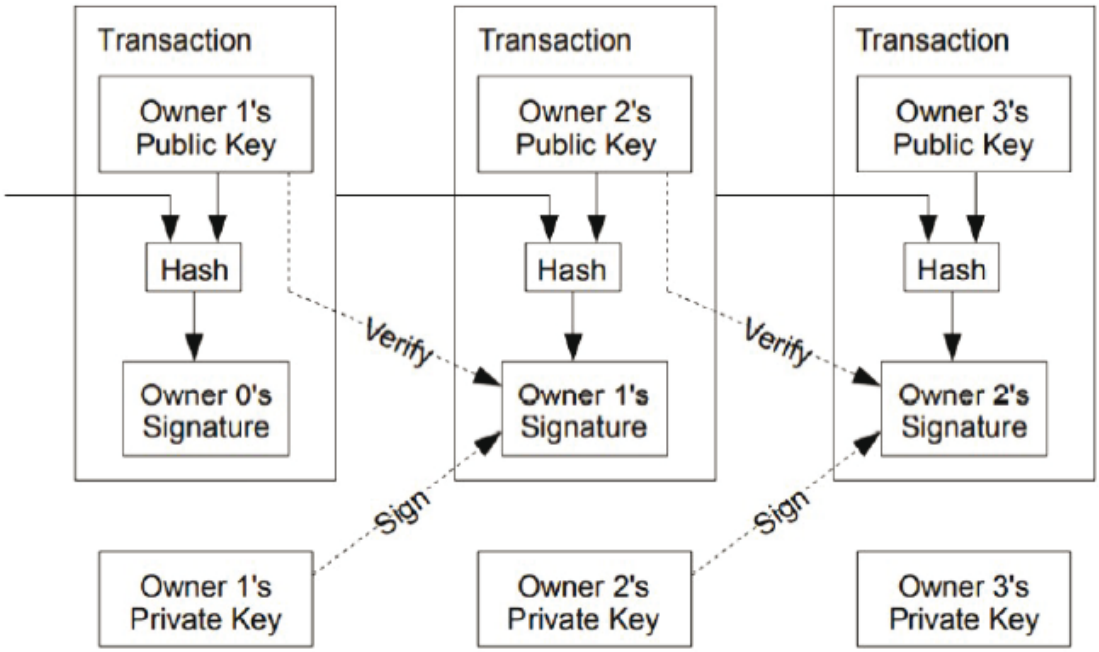


Рис. 5. Совершение транзакции в сети блокчейн

Ключевой и самой часто упоминаемой особенностью блокчейн-технологии является отсутствие какого-либо центра контроля и управления за транзакциями, осуществляющимися в сети блокчейн, поскольку транзакции подтверждаются с помощью особого криптографического механизма. Основной способ подтверждения транзакций состоит в обеспечении их публичности – каждая проведенная операция в системе передается всем устройствам сети, и только после подтверждения с их стороны запись о ней заносится в публичную книгу транзакций (shared public ledger). В этой связи разработчики этой технологии, теоретически, не могут воздействовать на целостность и достоверность транзакций. Механизм, с помощью которого подтверждаются транзакции и происходит их добавление в блоки информации и в систему блокчейн – механизм консенсуса. В настоящее время в блокчейн-системах использу-

проблемы российского права. 2019. № 6. С. 73–82.

[21] *Стивенс Р.* Алгоритмы. Теория и практические применение. М.: Издательство «Э», 2016. С. 366.

ются несколько механизмов консенсуса: доказательство работы[22], доказательство владения[23], циклический механизм[24] достижения консенсуса и другие. Каждый из этих механизмов по-своему обеспечивает надежность и достоверность информации, содержащейся в системе блокчейн. К примеру, механизм доказательства работы, который используется в системе Биткоин, в основе своей имеет выполнение участниками сети блокчейн вычислительной задачи по нахождению соответствующего требованиям системы хэша.

Особенностью технологии блокчейн ошибочно считают анонимность транзакций[25]. Действительно, для использования, к примеру, криптовалюты, по общему правилу, нет необходимости регистрироваться или идентифицировать себя иным образом, достаточно лишь указать адрес электронной почты и желаемый пароль. Для использования системы, как уже отмечалось, используется пара публичный ключ – частный ключ, с помощью которых и осуществляются транзакции в системе без раскрытия личности отправителя и получателя. Однако, по справедливому утверждению как зарубежных, так и некоторых отечественных исследователей, такую систему следует называть псевдоанонимной, нежели анонимной[26]. Это связано с особенностями адресации в любой сети, в том числе в сети Интернет – использование стека протоколов TCP/IP, как уже отмечалось, требует однозначной идентификации адресата пакета данных, чтобы он мог быть доставлен – даже использование различных программ для сокрытия IP-адреса или местонахождения не всегда могут полностью анонимизировать пользователя. Более того, с учетом публичности транзакций в большинстве блокчейн-систем, возможно ретроспективно проследить связь конкретного блока с конкретным участником или участника-ми[27]. Исследователям уже удавалось идентифицировать отдельные магазины и покупателей, которые пользуются криптовалютой[28][29]. В этой связи появились новые блокчейн-системы, которые целенаправленно маскируют личности участников – в качестве примера можно привести Zcash и Monero, – использующие особые средства шифрования транзакций и пары публичный – частный ключ.

В связи с псевдоанонимной природой блокчейн невозможно в полной мере согласиться с утверждением о том, что данная технология позволяет «достоверно фиксировать достоверные данные о принадлежности существующего в цифровой форме актива определенному **лицу** (выделено мной. – *А.Ч.)*»[19]. Дело в том, что пара публичный – частный ключ определяют не конкретное лицо, а, скорее, конкретный IP-адрес или электронную почту, при этом не обязательно владельца частного ключа, который обеспечивает доступ к виртуальным единицам сети блокчейн. Следовательно, о достоверности принадлежности актива можно говорить только

---

[22] Proof of work.

[23] Proof of stake.

[24] Round-robin.

[25] *Олиндер Н.В.* Криминалистическая характеристика электронных платежных средств и систем // Lex russica. 2015. № 10. С. 128–138; *Сальникова А.В.* Технология блокчейн как инструмент защиты авторских прав// Актуальные проблемы российского права. 2020. № 4. С. 83–90; *АрнаутовД.Р., Ерохина М.Г.* Цифровые активы в системе российского права // Российский юридический журнал. 2019. № 4. С. 148–157.

[26] *Marcin Szczepanski.* Bitcoin Market, economic and regulation. EPRS Briefing, 2014 // URL: http://www.europarl.europa.eu/RegData/bibliotheque/ briefing/2014/140793/LDM_BRI(2014)140793_REV1_EN.pdf (дата обращения: 25.01.2020); *Malte Moser.* Anonymity of Bitcoin Transactions: An Analysis of Mixing Services // Munster Bitcoin Conference, 2013; *Облачинский И.* Биткоин: зарубежный опыт // ЭЖ-Юрист. 2014. № 23. С. 8.

[27] *Фролов И.В.* Криптовалюта как цифровой финансовый актив в российской юрисдикции: к вопросу о вещной или обязательственной природе // Право и экономика. 2019. № 6. С. 5–17.

[28] *Sarah Meiklejohn, etal.* A fistful of Bitcoins: characterizing payments among men with no names // Communications of the ACM. 2016. № 4. С. 86–93.

[29] *Савельев А.И.* Договорное право 2.0: «умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 32–60.

применительно к публичному ключу, но не к какому-то конкретному лицу, поскольку оно, по общему правилу, неизвестно.

Таким образом, общий принцип работы блокчейн-технологии состоит в выполнении участниками сети совокупности последовательных операций:

1) информация о новых транзакциях передается всем участникам сети;

2) участники сети собирают все транзакции в один блок;

3) каждый участник сети выполняет операцию по достижению консенсуса в отношении каждого блока (к примеру, к системе блокчейн, оперирующей Биткоином, механизм консенсуса – «доказательство работы»);

4) когда участник сети подтверждает действительность блока, он передает информацию об этом остальным участникам сети;

5) остальные участники сети подтверждают существование этого блока только в том случае, если информация обо всех транзакциях, которая в нем содержится, действительная (к примеру, не была дважды совершена одна и та же транзакция с одним и тем же Биткоином).

6) участники сети выражают свое согласие с содержанием блока путем создания нового блока, заголовок которого будет включать в себя хэш подтвержденного блока.

За выполнение такой работы участники сети получают «вознаграждение» в виде определенного актива (например, Биткоина) – первая транзакция в каждом блоке представляет собой новый актив, который достается лицу или лицам, которые подтвердили соответствующий блок.

Децентрализованность и общедоступность блокчейн-сетей далеко не всегда является преимуществом, особенно для корпораций, которым необходимо хранить определенные сведения в тайне от широкой публики. Поэтому дальнейшим витком развития блокчейн-технологии стало появление контролируемых блокчейн-систем – в которых отсутствует свободный доступ к информации о транзакциях, создаются дополнительные требования к участникам и даже появляется распределенный, но тем не менее центр управления. В настоящее время по критерию осуществления доступа к сети блокчейн-системы можно классифицировать на две основные группы – **публичные**

Конец ознакомительного фрагмента.