Особенности закрепления принадлежности диджитализированных объектов гражданских прав

Т. Э. Зульфугарзаде
кандидат юридических наук, доцент, доцент кафедры гражданско-правовых дисциплин РЭУ им. Г. В. Плеханова.
Адрес: ФГБОУ ВО «Российский экономический университет имени Г. В. Плеханова», 117997, Москва, Стремянный пер., д. 36.
E-mail: teymurz@yandex.ru

Features of Features of Securing the Ownership of Digitalized Objects of Civil Rights

T. E. Zulfugarzade
PhD of Law, Associate Professor, Associate Professor of the Department of Civil Legal Disciplines of the PRUE.
Address: Plekhanov Russian University of Economics, 36 Stremyanny Lane, Moscow, 117997, Russian Federation.
E-mail: teymurz@yandex.ru

Аннотация

В статье в качестве предмета исследования определены основные направления в сфере закрепления с использованием технологий блокчейн принадлежности (цифровизированных, цифровых) объектов гражданских прав, прежде всего на нефиатные криптовалюты и токены (цифровые токены), а также иные активы, например, аккаунты пользователей в электронных платежных системах, популярных сетевых электронных играх, соцсетях, существующие исключительно в цифровом виде, стоимость которых может быть весьма существенной. Методика исследования основана на определении инновационных подходов в нотариальной деятельности; анализе романо-германской и англо-саксонской правовых семей (систем), на их адаптированности к децентрализации; на определении и конкретизации юридических и технико-технологических особенностей децентрализованной системы блокчейн-закрепления принадлежности объектов гражданских прав с точки зрения их отказоустойчивости, атакоустойчивости и сговоростойкости. Научную новизну исследования определяют предложения автора, направленные на совершенствование правового обеспечения рассматриваемого в работе юридического механизма блокчейн-закрепления принадлежности цифровых объектов гражданских прав, имеющих значение для защиты интересов граждан и организаций, в том числе при осуществлении коммерческой и иной экономической деятельности, а также цифровых прав, переходящих в порядке наследования (правопреемства); дальнейшую возможность использования блокчейн закрепленных цифровых прав в качестве доказательств в гражданском и арбитражном процессах.

Ключевые слова: юриспруденция, гражданское право, имущество, движимые вещи, недвижимость, интеллектуальная деятельность, средства индивидуализации, блокчейны, хэшграф, децентрализация, интернет-технологии, диджитализированные активы, смарт-контракт, цифровая экономика, криптобезопасность, эффективность, большие данные.

Abstract

The article defines the main directions in the field of blockchain-securing the ownership of digitalized (digital) objects of Civil Law, primarily for non-fiat cryptocurrencies and tokens (digital tokens), as well as other assets, for example, user accounts in electronic payment systems, popular online electronic games, social networks and others, existing exclusively in digital form, the cost of which can be very significant. The research methodology is based on the definition of innovative approaches in notarial activities; the analysis of Romano-Germanic and Anglo-Saxon legal systems, in their adaptation to decentralization; on the definition and concretization of the legal and technical-technological features of the decentralized blockchain-consolidate the identity of Civil Law objects from the point of view of their fault tolerance, attack resistance and collusion resistance. The scientific novelty of the research is determined by the author's proposals aimed at improving the legal support of the legal mechanism of the blockchain-securing the ownership of digital objects that are important for the protection of the citizens and organizations interests, including in the implementation of commercial and other economic activities, as well as digital rights passing in the order of inheritance (succession); further possibility of using blockchain-secured digital rights as evidence in Civil and Arbitration processes.

Keywords: jurisprudence, Civil Law, property rights, movable assets, real estate, intellectual activity, individualization means, blockchain, hashgraph, decentralization, Internet, technologies, digital assets, smart contracts, digital economy, crypto security, efficiency, Big Data.

Основы правового обеспечения прежде всего закрепления принадлежности объекта гражданских прав определенному лицу, а также ограничения указанного вида прав, в том числе обременения имущественных прав, закреплены в пункте 1 статьи 8.1, пункте 2 статьи 142 и пункте 2 статьи 1232 ГК РФ. Учитывая, что перечисленные нормы распространяются на госрегистрацию прав, во-первых, на имущество; во-вторых, выпуск или выдачу ценных бумаг; и в-третьих, результаты интеллектуальной деятельности (РИД) и средства индивидуализации (СИ), регистрация в обязательном порядке (обязательная регистрация) прав на движимые вещи согласно правилам, установленным пунктом 2 статьи 130 ГК РФ, не требуется, за исключением случаев, прямо предусмотренных нормативными правовыми актами.

В связи с этим неоднократно высказывалось мнение о необходимости наделить нотариальные палаты правом вести Единый реестр движимых вещей, имея в виду прежде всего дорогостоящее движимое имущество, не относящееся к предметам домашней обстановки и обихода, традиционно считающихся принадлежностью объектов недвижимости. Так, в частности, на сегодняшний день в формате деятельности Федеральной нотариальной палаты (ФНП) с 2017 г. действует Реестр уведомлений о залоге движимого имущества (Реестр залогов движимого имущества), представляющий собой общероссийский электронный реестр находящихся в залоге объектов движимого имущества, в том числе автомототехники и иных дорогостоящих товаров.

Указанный реестр является составной частью ЕИС нотариата, в которую также включен Реестр нотариальных действий (РНД). В свою очередь в РНД с 2018 г. вносятся сведения обо всех совершенных нотариальных действиях, за исключением сведений об удостоверении верности копий и подлинности подписи. В последующем планируется внесение в РНД сведений о нотариальных действиях, совершенных должностными работниками консульских учреждений за рубежом и должностными лицами органов местного самоуправления, наделенных правом совершать отдельные виды нотариальных действий.

С учетом последующего возможного наделения нотариусов правом регистрации браков и совершения иных действий в сфере записи актов гражданского состояния, объединившись с базами данных (БД) ФНС России, Росреестра, Роспатента, БД «Таможенный реестр объектов интеллектуальной собственности», БД «Реестр объектов интеллектуальной собственности» и др., ЕИС нотариата (на основании вносимых нотариусами сведений, в том числе из брачных договоров, о нажитом во время брака имуществе супругов, завещаний и иных нотариально удостоверяемых документов) постепенно трансформируется в единый сетевой ресурс (представляющий собой, равно как и все вышеперечисленные реестры и БД, централизованную технологию), в который будут вноситься сведения прежде всего о правах (их ограничении) граждан и юридических лиц на недвижимое и движимое имущество, а также РИД и СИ. Данный подход позволит унифицировать процедуры перехода прав, в том числе в порядке наследования, обеспечить надлежащую защиту прав собственников движимых вещей, а также правообладателей интеллектуальных прав.

При этом в связи с практически полным отсутствием правового регулирования в нашей стране остаются неохваченными так называемые диджитализированные (цифровые) активы (предполагаемое общее название «криптоактивы» или «цифровые финансовые активы» (ЦФА)). К такого рода криптоактивам целесообразно отнести не только нефиатные криптовалюты и токены (цифровые токены), но и иные активы, например, аккаунты пользователей в электронных платежных системах, популярных сетевых электронных играх, соцсетях и им подобные, существующие исключительно в цифровом (диджитализированном) виде, стоимость которых может быть весьма существенной. Так, в частности, стоимость хорошо «прокаченного» аккаунта пользователя сетевой игры может достигать нескольких десятков тысяч долларов; биржевая стоимость одной криптовалютной единицы – нескольких сотен либо тысяч, либо десятков тысяч долларов и т. д.

Надлежащее закрепление принадлежности объектов гражданских прав на криптоактивы физических и юридических лиц, не подпадающих под

действие нормативных правовых актов Российской Федерации, в исключительном ведении которой находится гражданское законодательство, по нашему мнению, целесообразно осуществлять, не дожидаясь принятия специальных актов федерального уровня, учитывая достаточно серьезное распространение указанных активов в интернет-сети, что позволит обеспечить права собственников и возможность легитимизации правопреемства таких прав при их переходе, в том числе в случае стойкой неспособности собственника самостоятельно управлять и распоряжаться указанными правами (во всех иных случаях криптоактивы останутся в распоряжении электронных цифровых площадок их владельцев, на которых таковые активы зарегистрированы). В указанных целях представляется важным использовать присущие современной цифровой экономике (криптоэкономике) возможности, не требующие регулирования [1. – С. 2] децентрализованных киберсистем (принцип децентрализации киберсистем в Российской Федерации применяется, в частности, с 2014 г. в ГАС «Выборы» и с 2017 г. при регистрации лекарственных средств в формате ЕАЭС и т. д.), получивших название блокчейн- и хэшграф-технологий (блокчейнов) [2. – С. 21], представляющих собой анонимные одноранговые системы записей о совершенных в цифровом формате сделках (смарт-контрактах), основанных «на безопасных криптографических протоколах» [3. – С. 2].

По мнению известного в мире специалиста по кибербезопасности и сооснователя проекта Ethereum В. Д. Бутерина, «децентрализация – термин, чаще других применяемый в криптоэкономике, она даже считается безусловным фундаментом блокчейна, но она также один из них, которые, пожалуй, определены наиболее плохо. Тысячи часов исследований и миллиарды долларов на хеширование были потрачены с единственной целью – добиться децентрализации, а также защитить и улучшить ее, а в разгаре дискуссий сторонники единого протокола (или расширения протокола) обычно используют исчерпывающий аргумент: противоположные предложения представляются слишком «централизованными» [6. – С. 1].

Обращаясь к вопросам децентрализации программно-правового обеспечения блокчейн-закрепления принадлежности объектов гражданских прав, прежде всего имеют в виду следующие три ее взаимосвязанных направления (типа): во-первых, архитектурную (де)централизацию, указывающую количество работающих в системе компьютеров и какие из них могут отказать в любой момент времени без нарушения работы всей системы; во-вторых, политическую (де)централизацию, указывающую количество лиц (граждан или организаций), единолично контролирующих компьютеры, образующие систему, и в-третьих, логическую (де)централизацию, позволяющую определить, что система представляет собой монолитный объект. Для того чтобы убедиться в этом необходим эвристический метод, состоящий в следующем: если поделить эту систему пополам вместе с ее провайдерами и пользователями, каждая часть системы автономно должна продолжить работу. Однако и он не является гарантированно точным или оптимальным для решения этой задачи.

В данной связи отметим, что традиционные корпорации централизованы стратегически (один руководитель), архитектурно (один головной офис) и логически (не смогут работать раздельно друг от друга). Системы, работающие на основе блокчейнов, децентрализованы и не подвержены негативным влияниям, присущим централизованным системам, прежде всего это касается невозможности внесения некорректных сведений в базы данных централизованно; в случаях с децентрализованной системой исправления придется вносить в каждый компьютер, находящийся в этой системе (таких может насчитываться несколько тысяч), что практически невозможно. Таким образом, блокчейны обеспечивают правовую и криптографическую защиту сведений о принадлежности объектов гражданских прав (больших данных) в более высокой степени при меньших затратах, чем традиционные централизованные информационные системы и БД.

С юридической точки зрения романо-германская правовая семья (система), равно как и континентальное право, опирается на централизованный законодательный орган, в свою очередь англо-саксонская (англо-американская) – на прецеденты и на принятые ранее решения разными судьями. При этом романо-германская система в целом и континентальное право в том числе архитектурно несколько децентрализованы, поскольку применяются многими судами, которые в той или иной степени обладают свободой действий, хотя и в меньшей степени, чем в англо-американской системе. Обе системы права централизованы логически в соответствии с принципом «Code is Law – the law is the law» («закон – есть закон») [7. – С. 2].

С точки зрения лингвофилологического подхода, языки общения между людьми децентрализованы логически. При этом не предусмотрено никакой централизованной инфраструктуры, необходимой для поддержания жизни языка общения, а правила грамматики не создаются и не контролируются одним человеком (так, например, язык эсперанто был изобретен одним человеком, но уже много десятилетий функционирует, скорее, как живой язык общения, который развивается естественным образом, избегая централизованного регулирования со стороны какого-либо лица).

В свою очередь, протокол файлообмена и сервис для синхронизации BitTorrent децентрализован логически, как и язык межчеловеческого общения. Сети доставки контента аналогичны, хотя каждая контролируется единственной компанией. Блокчейны при этом децентрализованы политически (отсутствие любых видов контроля) и архитектурно (отсутствие центральной инфраструктурной точки отказа), но централизованы логически (в них существует одно общепринятое состояние, а система ведет себя как один, фактически единый компьютер). Обычно, когда стараются подчеркнуть достоинства того или иного блокчейна, говорят о наличии «одной центральной базы данных, что, во-первых, централизация логична и, возможно, во многих случаях необходима, и во-вторых, киберсистема, имеющая название «InterPlanetary File System» (IPFS) – «межпланетарная файловая система», представляющая собой контентно-адресуемый, одноранговый гипермедийный протокол связи, тоже бы стремилась к логической децентрализации везде, где она возможна, поскольку логически децентрализованные системы лучше выживают, как правило, при разрывах сетей, хорошо работают в регионах мира с плохой системой коммуникаций и т. д.» [4. – С. 2].

Важно отметить, что архитектурная централизация часто приводит и к политической, хотя и необязательно (так, например, в странах так называемой «формальной демократии» политические деятели голосуют в какой-либо из палат парламента, хотя руководители этой палаты не получают в конечном итоге какой-либо значительной власти при принятии ею решений). В компьютеризированной системе могла бы сложиться архитектурная, а не политическая децентрализация (децентрализация политической и экономической жизни стала «трамплином для национальных государств и для капитализма» [8. – С. 13]), если в ней есть онлайн-сообщество, использующее для удобства централизованный форум, но только такой форум, в котором действует общепринятый социальный контракт с условием, что если владельцы форума начнут действовать злонамеренно, то каждый участник перейдет в другой форум (сообщества, которые объединяются против того, что они считают цензурой, на другом форуме могут столкнуться с ней на практике).

Логическая централизация усложняет архитектурную децентрализацию, но не делает ее невозможной. Например, децентрализованные консенсусные сети уже доказали свою эффективность, хотя их поддерживать сложнее, чем вышеупомянутый сервис BitTorrent. Более того, логическая централизация усложняет политическую децентрализацию: в логически централизованных системах труднее улаживать споры, просто соглашаясь еще с одним принципом «live and let live» («жить и давать жить другим») [6. – С. 4].

Особенностями децентрализованной системы блокчейн-закрепления принадлежности объектов гражданских прав являются, во-первых, отказоустойчивость (децентрализованные системы с меньшей вероятностью могут случайно выйти из строя, потому что они полагаются на многие отдельные компоненты, возможность одновременного отказа которых маловероятна); во-вторых, атакоустойчивость (децентрализованные системы являются более затратными для злоумышленников, преследующих цели их атаковать, разрушать или компрометировать, поскольку в них нет чувствительных центральных точек, которые могут быть атакованы с гораздо меньшими затратами, чем окружающие их экономические системы, и в-третьих, сговоростойкость (участникам децентрализованных систем намного труднее договориться о совместной скрытной деятельности в свою пользу за счет других участников, тогда как во все времена руководители корпоративных образований сговаривались и наносили ущерб менее скоординированным гражданам, клиентам, сотрудникам и широкой общественности (обществу), государству и мировому сообществу в целом, что можно увидеть на примере глобальных финансово-экономических кризисов, произошедших в последние три десятилетия).

С точки зрения надлежащего обеспечения кибербезопасности и защиты блокчейн-закрепленной принадлежности объектов гражданских прав, все три вышеперечисленных принципа представляют собой разумные и достаточные действия,

направленные на достижение требуемого результата. Так, например, принцип отказоустойчивости, основанный на возможности продолжения бесперебойной работы блокчейн-системы в случае прекращения работы одного или нескольких включенных в нее компьютеров, многократно апробирован во многих технических системах, в частности, резервные источники питания используются в медицинских и военных учреждениях; резервные двигатели – как основа безопасности полетов авиатехники, резервирование финансовых средств – при диверсификации финансовых портфелей и, что немаловажно, резервные компьютеры – в компьютерных сетях. Однако такая децентрализация, хотя по-прежнему эффективная и весьма важная, часто оказывается меньшей панацеей (универсальным средством от всех зол), чем та, «которую иногда предсказывает несложная математическая модель» [5. – С. 3]. Причиной этого служит общий отказ всех компьютеров и, как следствие, всей системы в целом. Несомненно, все образующие блокчейн-систему компьютеры, закупленные из одной партии у единого поставщика, теоретически могут отказать одновременно, тем не менее изначально децентрализованный подход к созданию подобных систем предопределяет случайную выборку компьютерных пользователей, приобретающих компьютеры самостоятельно и у разных поставщиков.

Вместе с тем и с юридической, и с технико-технологической точек зрения возможны и другие варианты неблагоприятного стечения обстоятельств, событий и фактов, например: 1) во всех узлах одной из блокчейн-систем работает то же самое клиентское программное обеспечение (КПО), в котором, как оказалось, появился вирус; 2) во всех узлах каждой блокчейн-системы работает одно и то же КПО, группа разработчиков которого (или группа разработчиков, предлагающих модернизацию протокола BitTorrent), как выяснилось впоследствии, преследовала криминальные цели; 3) при доказательстве работоспособности (англ. *proof-of-work, POW, PoW* – доказательство выполнения работы) один из двух наиболее известных и общепринятых алгоритмов подтверждает работоспособность блокчейна при условии пребывания не менее семидесяти процентов ее майнеров (создателей новых блоков в блокчейне) в одной и той же стране, уполномоченный государственный орган которой может закрыть все майнинг-фермы (площадки для добычи криптовалюты) в целях национальной безопасности; 4) большинство аппаратных средств для майнинга выпускаются одной и той же компанией-производителем, которую могли подкупить или принудить к внедрению так называемого бэкдора, т. е. «черного хода» – инструмента обхода системы защиты в целях отключения аппаратуры по своему усмотрению.

Во избежание вышеперечисленных неблагоприятных вариантов в блокчейнах используется альтернативный общепринятый алгоритм, известный под названием PeerCoin, использующий для доказательства доли владения (proof-of-stake – PoS), (от англ. *proof of stake* – подтверждение доли, что означает доказать право собственности на определенную сумму в валюте). Наличие не менее 70% криптоактивов в доле владения (stake) в качестве ресурса, «определяет, какой именно узел получает право на добычу следующего блока» [4. – С. 3]. При рассмотрении отказоустойчивости децентрализация, в частности, используемая алгоритмом PeerCoin, будет учитывать все вышеперечисленные аспекты и способы минимизации отказов.

В связи этим некоторые из следующих бесспорных, с нашей точки зрения, выводов представляются достаточно очевидными: 1) крайне важно располагать несколькими конкурирующими вариантами децентрализации; 2) знание технических причин, связанных с обновлением протокола BitTorrent, должно быть демократизировано, чтобы больше пользователей и майнеров блокчейн-системы могли чувствовать себя комфортно, участвуя в научных дискуссиях и при необходимости критикуя явно плохие изменения протокола BitTorrent; 3) привлечение ключевых разработчиков и исследователей должно осуществляться не одной, а несколькими организациями (или в иных случаях многие из ключевых разработчиков и исследователей могут быть волонтерами); 4) алгоритмы майнинга должны минимизировать риск централизации.

Все вышеперечисленные требования к блокчейн-системе целесообразно внести в перечень правил ее создания и последующей эксплуатации, которые должны быть обязательными для всех майнеров и пользователей такой системы. При этом в идеальном случае собственник (владелец) диджитализированных объектов гражданских прав использует закрепленное при помощи технологий блокчейн доказательство права на долю владения прежде всего для того, чтобы полностью

отказаться от риска централизации оборудования. В этом случае необходимо соблюдать меры безопасности в целях снижения вероятности возникновения новых рисков в процессе доказательства доли владения, в том числе при перемене владельца.

Обратимся к более подробному рассмотрению вопросов атакоустойчивости блокчейн-систем. В некоторых экономических моделях децентрализация вообще не имеет значения. Если создать протокол, в котором валидаторы гарантированно потеряют сколько-то миллионов долларов, если произойдет 51%-ная атака (с окончательным реверсом), то не имеет значения, контролируют ли валидаторы одну компанию или несколько десятков таких организаций: маржа экономической безопасности в размере нескольких десятков миллионов долларов также не зависит от общего количества компаний. На самом деле, по мнению В. Д. Бутерина, существуют глубокие теоретико-игровые причины, когда централизация способна даже максимизировать экономическую безопасность (модель выбора существующих блокчейнов для транзакций отражает понимание глубинных причин и взаимосвязей, поскольку включение транзакций в блоки на основании предложений майнеров/блоков на самом деле является довольно быстрочередующейся диктатурой). Тем не менее, отмечает специалист по криптозащите, как только заинтересованное лицо воспользуется более насыщенной экономической моделью, особенно такой, в которой допускается возможность принуждения (или гораздо более мягкие события, такие как целенаправленные атаки DoS против узлов), децентрализация становится более важной. Другими словами, чем меньше это соотношение, тем лучше [6. – С. 7].

Такого рода подход показывает прежде всего преимущество доказательства доли владения над доказательством работы, поскольку компьютерное оборудование легко обнаруживается, регулируется или атакуется, тогда как криптоактивы намного легче спрятать или попросту утаить. Во вторую очередь он свидетельствует о пользе наличия широкораспределенных групп разработчиков, включая географическую расположенность компьютеров, образующих блокчейн-сеть. И в-третью очередь, это означает, что при разработке консенсусных протоколов необходимо учитывать не только экономическую модель, но и модель отказоустойчивости.

Самым сложным из обозначенных трех аргументов, несомненно, является сопротивление (противодействие) сговору. Однозначно понятие «сговор» определить достаточно сложно; возможно – это некая координация, которая не нравится майнерам и другим пользователям блокчейн-сети. В реальной жизни существуют многие ситуации, в которых даже при наличии устойчивой координации между всеми майнерами может стать опасной ситуация, когда одна подгруппа способна координировать свою деятельность, в то время как другие – нет.

Одним из простых юридических примеров является антимонопольное право – преднамеренные нормативные барьеры, воздвигаемые для того, чтобы затруднить возникновение доминирующего положения на рынке через объединения промышленных групп (монопольный сговор), чтобы стать монополистом и получать дополнительную прибыль за счет других участников рынка и совокупных благ общества. Еще одним, менее значимым примером, является правило, применяемое на некоторых шахматных турнирах, запрещающее двум игрокам играть много игр друг против друга, чтобы они не пытались улучшить показатели одного из них.

В случае блокчейн-протоколов математическое и экономическое обоснование безопасности консенсуса часто в значительной степени зависит от модели несогласованного выбора или предположения, что в этой игре задействовано много мелких участников, которые принимают решения самостоятельно. Если один из участников получит более одной трети мощности майнинга (т. е. мощности, которую использует компьютер или другое оборудование на решение различных алгоритмов хеширования) в качестве доказательства работы какой-то системы, он будет способен получить дополнительную прибыль от самостоятельного майнинга.

Сторонники блокчейнов подчеркивают также, что блок-цепочки более безопасны в применении, поскольку они не могут изменять свои правила произвольно по своему желанию, хотя этот довод было бы трудно защитить в том случае, когда все разработчики программного обеспечения и протокола работали в одной компании, были частью одной семьи и находились одновременно в одном помещении. Все дело в том, что эти системы не должны действовать как своекорыстные унитарные монополии. Следовательно, блокчейны более безопасны, если они более раскоординированы.

В заключение отметим, что защита диджитализированных объектов гражданских прав, осуществляемая посредством блокчейн-закрепления принадлежности указанных объектов, представляется оптимальной в современных условиях; ее создание не требует привлечения средств бюджетов федерального и регионального уровней власти Российской Федерации и может осуществляться на основе развития общественной инициативы. При необходимости распространения такой системы и ее использования для госнужд, финансирование может осуществляться на принципах частно-государственного партнерства. Особое развитие блокчейн-закрепление принадлежности объектов гражданских прав может получить в том числе в сфере предпринимательского права, т. е. предпринимательской и иной экономической деятельности, включая деятельность по обслуживанию клиентов, а также лиц, обратившихся за квалифицированной правовой помощью в юридические компании, а в последующем, после внесения изменений и дополнений в главы 6 ГПК РФ и 7 АПК Российской Федерации, служить доказательствами в гражданском и арбитражном процессах соответственно.

Список литературы

1. *Кислый В. А.* Юридические аспекты применения блокчейна и использования криптоактивов. Издательская группа «Закон». 2017. 5 июня. – URL: https://zakon.ru/blog/2017/6/5/yuridicheskie_aspekty_primeneniya_blokchejna_i_ispolzovaniya_kriptoaktivov (дата обращения: 05.03.2019).

2. *Краснов О.* Технологический блокчейн // Журнал сетевых решений (LAN). – 2017. – № 12. – С. 20-22.

3. Особенности технологии блокчейн, 2017. 16 декабря – URL: https://utmagazine.ru/posts/21332-osobennosti-tehnologii-blokcheyn (дата обращения: 05.03.2019).

4. *Benet J.* Design Challenge: Avoid Centralization and Singletons, 2017. – URL: http://scuttlebot.io/more/articles/design-challenge-avoid-centralization-and-singletons.html (дата обращения: 05.03.2019).

5. Blockchain Technology: Implications for the Legal Industry Boston. The American Lawyer, 2018. November, 30. – P. 1-4.

6. *Buterin V. D.* The Meaning of 2017. February, 6. – URL: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274 (дата обращения: 05.03.2019).

7. *Civalleri J.* When «Code is Law» meets «Law is Law» – Inside the American Bar Association's Biggest Blockchain Event of the Year. A Medium Corporation. – 2017. – April 13. – URL: https://hackernoon.com/when-code-is-law-meets-law-is-law-inside-the-american-bar-associations-biggest-blockchain-c76e3bafbb9a (дата обращения: 05.03.2019).

8. *Ferguson N.* Civilization: The West and the Rest. – London : Penguin Group. 2012. – P. 1042.