

БЛОКЧЕЙН-ТЕХНОЛОГИЯ ДЛЯ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ: УГРОЗЫ И ПЕРСПЕКТИВЫ

Бегларян М.Е., Добровольская Н.Ю.*

Ключевые слова: блокчейн, технология, цифровизация экономики, внедрение, криптовалюта, модель, правовое поле, законодательство, правоохранительные органы.

Аннотация.

Цель работы: рассмотреть вопросы внедрения блокчейна как технологии будущего, которая даст возможность экономить финансы, сделает прозрачными финансовые схемы, перекроет саму возможность совершать противоправные действия в экономической сфере. Но в то же время уделяется внимание и «обратной стороне медали», когда эта же технология оказывается в руках преступного сообщества.

Методы: концептуальное моделирование цифровизации экономики и внедрения цифровых процессов, формализация разработки эффективных правовых методов, имеющих методологическое значение для экономики России.

Результаты: представлена авторская позиция и предложения по будущему блокчейна для цифровизации российской экономики. Цифровизация и внедрение новых, порой чуждых и опасных технологий будет иметь сильное влияние на мировую финансовую систему и экономику, поэтому важно своевременно настраивать законодательную базу под новеллы информационного прогресса, исключая запреты.

DOI: 10.21681/1994-1404-2020-4-46-54

Введение

Блокчейн — одна из современных технологий переработки и хранения данных, представляющая собой распределенную базу данных, основными методами преобразования информации в которой являются методы распределенной обработки данных. База данных не имеет централизованного управления, единого сервера не существует, база постоянно пополняется новыми блоками. Каждый блок информации поименован и хранит не только собственную временную метку, но и метку на предыдущий блок. Таким образом, пользователь информации имеет доступ к созданию исключительно собственных блоков и помещенные в систему блокчейн блоки уже неизменны. Отсутствие централизации и блочный принцип организации данных блокчейн-технологии позволяет обеспечить повы-

шенную безопасность и конфиденциальность хранения информации [9—11].

В одних странах уже работают уличные банкоматы для перевода криптовалют в наличные денежные средства, а в других всё, что связано с криптосферой, запрещено на законодательном уровне. В рамках международного сотрудничества различные страны принимают соглашения о сотрудничестве в области обеспечения экономической безопасности, осуществляются совместные скоординированные мероприятия в информационном (цифровом) пространстве [7, 10], направленные на обеспечение информационной безопасности в государствах-участниках. Эти соглашения и мероприятия регулируют вопросы оборота криптовалюты как внеправового явления¹.

¹ Chainalysis поможет банкам и биржам определять «рискованных» пользователей криптовалют // Официальный интернет-портал Coinspot. URL: <https://coinspot.io/technology/bezopasnost/chainalysis-pomozhet-bankam-i-birzham-opredelyat-riskovannyh-polzovatelej-kriptovalyut> (дата обращения: 04.09.2020).

* **Бегларян Маргарита Евгеньевна**, кандидат физико-математических наук, доцент, заведующий кафедрой социально-гуманитарных и естественно-научных дисциплин Северо-Кавказского филиала Российского государственного университета правосудия, г. Краснодар, Российская Федерация.

E-mail: rita_beg@mail.ru

Добровольская Наталья Юрьевна, кандидат педагогических наук, доцент, доцент кафедры информационных технологий Кубанского государственного университета, Российская Федерация, г. Краснодар, Российская Федерация.

E-mail: dnu10@mail.ru

Криптовалюта и криптотехнология

В настоящее время не существует нормативного закрепления определения криптовалюты. Существует Группа разработки финансовых мер по борьбе с отмыванием денег — *Financial Action Task Force* (далее ФАТФ или *FATF*). Новая валюта имеет иной генезис — не-экономическое начало, рождается из математических принципов и расчетов, а работает как финансовый инструмент, конвертируется в традиционные валюты, но защищена с помощью криптографических методов, может привести к появлению иной, новой, внегосударственной экономики.

Исходя из происхождения, криптомонеты защищены и функционируют за счет криптографических методов (преобразований). Математические методы, компьютерные вычисления, выполняемые алгоритмы определяют валюту, автор алгоритма дает ей имя, вычисляет стоимость, определяет стартовый курс для обмена на другие деньги. Для реализации асимметричного шифрования как криптографического преобразования используются два ключа [6]: открытый и неизвестный участникам операции, которые организуют процесс передачи информации в ходе совершения сделки. *Открытый* ключ определяется алгоритмом, способом шифрования данных и является непосредственным адресом для размещения криптосредств, а *закрытый* ключ используется для генерации информации и подтверждения совершения сделки — транзакции. *Закрытый* ключ известен только участнику — владельцу криптовалюты.

Вообще, асимметричное шифрование основано на идее, что при генерации очень больших чисел (типа 2^p , где p больше, чем 256), являющихся значениями открытого и закрытого ключа, зная открытый ключ, нельзя простым перебором за разумное время подобрать значение закрытого ключа. С другой стороны, разработаны надежные алгоритмы, позволяющие таким образом зашифровать сообщение открытым ключом, чтобы расшифровать его можно было только закрытым ключом. Для того чтобы обмениваться зашифрованными сообщениями, нет необходимости оглашения закрытого ключа. Владелец двух ключей (открытого и закрытого) достаточно передать отправителю только открытый ключ, с помощью которого отправитель зашифрует сообщение. Расшифровать его самостоятельно он не сможет, это сделает только владелец ключей. Таким образом, передача закрытого ключа кому-либо не требуется.

Децентрализованность криптоденег — особенность этого платежного средства, которая делает его независимым от государства и существующего порядка в денежном обороте современного общества. Децентрализованность в данном случае основана на технологии блокчейн (*blockchain*), которая состоит из последовательности или цепи блоков в распределённом реестре; иначе говоря, последовательность транзакций/действий каждый раз шифруется с применением известных способов шифрования, при этом исполь-

зуется хэш-функция. Невозможно извлечь данные без знания закрытого ключа из транзакций, так как необходимо расшифровать все блоки; можно — обычным перебором или с использованием специальных средств, но это невыполнимая задача за реальное время.

Пользователи создают и обеспечивают работоспособность такой криптовалютной системы. Для криптовалюты не нужен управляющий центр. Деньги текут от покупателя к продавцу без налогообложений, единственное, за что платят участники операций — это за созданные майнером новые звенья цепи, структуры (обычно речь идёт о новых блоках в блокчейне) для обеспечения функционирования криптовалютных платформ. Майнер — «копатель, шахтер» в мире компьютеров, его «добыча» — это криптовалюта. Он «майнит», т. е. генерирует криптопоследовательность, и строит на этом свой высокотехнологичный, но не совсем законный бизнес.

Данная технология находит применение во многих областях деятельности социума [5, 6, 14, 15], особенно там, где важна хронология событий или четкость в закреплении каких-либо процессов или данных. Например, технология блокчейн применима для хранения данных о ядерных отходах, она должна также быть применима и в правовом поле, что принесет обществу ощутимые преференции в будущем².

В апреле 2020 г. на совещании Президента РФ с главами ведомств и министрами был представлен новый сервис Федеральной налоговой службы, который использует технологию блокчейн для идентификации единого учёта получателей льготных кредитов для малого и среднего бизнеса, пострадавшего от COVID-19. Об этом заявил глава ведомства Д. В. Егоров³. Глава Федеральной налоговой службы подчеркнул, что при разработке этого решения важно было создать «удобный и прозрачный для бизнеса, банков и государства» механизм: «Это блокчейн-платформа ФНС. У каждого участника формируется свой узел в рамках распределённых реестров, который генерирует последовательные записи. Это позволяет, с одной стороны, обеспечить безопасность данных, с другой стороны — доступ к данным всем участникам проекта. ФНС автоматически обрабатывает данные, к какой отрасли относится компания, численность компании и то, что она относится к МСП. Заявки обрабатываются практически мгновенно»⁴.

Благодаря этому ИТ-решению банки смогут одобрять заявки на выдачу беспроцентных кредитов предпринимателям для выплаты заработной платы в течение дня. Принцип распределённого реестра (блокчейн) и доступ всех участников проекта к информации

² Единый реестр правовых актов и других документов Содружества Независимых Государств [Электронный ресурс]. URL: <http://www.cis.minsk.by/reestr/ru/index.html#reestr/view/text?doc=6055> (дата обращения 20.09.2020).

³ Совещание по вопросам банковского кредитования экономики, 23 апреля 2020 г. URL: <http://kremlin.ru/events/president/news/63244>.

⁴ URL: <http://www.consultant.ru/law/hotdocs/61872.html>.

о выданных кредитах исключит повторные заявки от бизнеса.

Система протестирована совместно с ВТБ и Сбербанком и уже введена в промышленную эксплуатацию. Возможно, данный проект будет интересен другим банкам.

Пенсионный фонд России (ПФР) также планирует отслеживать информацию о трудовых отношениях при помощи технологии блокчейна. Использование распределенных баз данных позволит отказаться от громоздких бумажных документов ПФР, в которых содержатся данные о налоговых отчислениях и страховых взносах работодателей, хранящиеся на их серверах. Таким путем Фонд намерен снизить расходы, которые он тратит на хранение этой информации⁵.

Данная инициатива согласуется также с внедрением механизма электронных трудовых книжек в России⁶. Электронная книжка будет содержать информацию о трудовой деятельности человека, которую работодатель передаст в Пенсионный фонд.

Впервые о целесообразности использования блокчейна для системы индивидуального пенсионного накопления заявили негосударственные пенсионные фонды, направив соответствующее письмо в Пенсионный фонд России.

Рассмотрев основные особенности криптовалюты, более наглядно представим процесс взаимодействия между участниками договоров «купли-продажи» на примере такой валюты, как биткойн. На основании отчета FATF наиболее востребованной в настоящее время является именно эта криптовалюта [1].

Биткойн — это платежная сеть, лишенная явного центрального органа управления, работающая под протоколом P2P («точка-точка»), обслуживаемая ее пользователями, функционирующая без посредников на фоне отсутствия централизованного контроля [9].

Для того чтобы производить определенные манипуляции с биткойном, в первую очередь, необходимо создать биткойн-кошелек. Это возможно путем установки специального программного обеспечения либо использования веб-приложений и сайтов. В свою очередь, идентификация личности пользователя отсутствует либо позволяет частично привязать криптокошелек к пользователю, в основном это привязка к номеру телефона. Следует также заметить, что все транзакции технологии блокчейн являются открытыми, но идентифицировать обладателей криптокошельков практически невозможно. Это объясняется указанными выше проблемами привязки криптокошельков, а также использованием закрытого ключа при шифровании данных.

Создав криптокошелек, пользователь готов к совершению транзакций, при этом сам криптокошелек представляет собой простую, несвязанную последовательность латинских букв и цифр. Используя различные сервисы, пользователи могут обмениваться биткойнами, покупать определенные вещи и предметы за биткойны, но пополнять свой криптокошелек и выводить биткойны владельцы могут только путем использования электронных кошельков, к примеру, Qiwi-кошелька. Это, в свою очередь, позволяет правоохранительным органам получать информацию о выводе и вводе данных на определенные электронные кошельки, которые позволяют идентифицировать владельца криптокошелька.

При этом следует отметить возможности использования криптовалюты в международной экономике, в рамках выполнения транзакций между организациями и государствами. Криптовалюты обладают рядом преимуществ над устоявшимися способами совершения сделок купли-продажи и обмена цифровых финансовых активов, а именно: независимость от инфляции; отсутствие посредников при проведении сделок, невозможность заблокировать либо отозвать транзакцию; безопасность; открытость проводимых операций и др. Эти преимущества, безусловно, заманчивы и позволяют вывести мировую экономику на новый уровень взаимодействия посредством доступности и открытости проводимых операций с технологией блокчейн, обезопасить проводимые транзакции, а также дать возможно больше стабильности и устойчивости мировой экономике.

Но при этом существует еще одна сторона процесса: криптовалюта — это анонимная цифровая валюта, которая повышает вероятность проведения «теневых» сделок, а также осуществления различного рода незаконных транзакций в сфере спонсирования терроризма, купли-продажи запрещенных средств.

Данный аспект отмечается и в протокольном решении СНГ от 15 марта 2019 г. «Об обеспечении прав потребителей в сфере электронной торговли в государствах — участниках СНГ» [1]. Изменения на рынке платежных средств электронной коммерции связаны в том числе с расширением сферы применения криптовалюты и заменителей ценных бумаг (цифровых токенов), выпускаемых в виде цифровых финансовых активов. Особенностью обращения данных инструментов является отсутствие государственного регулирования и уход от использования традиционной платежной инфраструктуры кредитных организаций.

Криптовалюта и законодательство

В сети существуют такие сервисы, как *Silk Road*, *AlphaBay* и *Agora* — их можно назвать площадками для отмывания денег, которые заработаны криминальным путем. Большая часть сделок, проходящих через вышеперечисленные ресурсы, проводится с целью покупки наркотиков.

⁵ «Известия», Экономика, Контрактная цепь: Пенсионный фонд России переходит на блокчейн. URL: <https://iz.ru/781475/pavel-panov/kontraktnaia-tsep-pensionnyi-fond-rossii-perekhodit-na-blokchein>.

⁶ Федеральный закон от 16 декабря 2019 г. № 439-ФЗ «О внесении изменений в Трудовой кодекс Российской Федерации в части формирования сведений о трудовой деятельности в электронном виде». URL: http://www.consultant.ru/document/cons_doc_LAW_340241.

Используя механизмы обезличивания в процессе покупки криптообъектов, в данном случае криптоде-нег, такие деятели остаются анонимными, это не дает возможности оформить факт получения денег от нелегальной деятельности. Данный аспект ставит под вопрос обеспечение международной безопасности; перед правоохранительными органами стоит соответствующая задача получения юридических фактов, подтверждающих операции движения денежных средств, что практически невозможно сделать прямыми, традиционными методами. Можно использовать опосредованные или косвенные методы и с применением современных технологий добиться некоторого прогресса в этом процессе⁷.

Так, для определения принадлежности криптокошелька некоторому субъекту производится снятие информации с технических каналов связи, которыми пользуется данное лицо для выхода в Интернет. Анализируется входящий и исходящий трафик этого подключения. Существует также возможность реализации идентификации злоумышленника, представленная сотрудниками Люксембургского университета, которые исследовали возможности анонимности различных сервисов, в том числе криптокошельков, и указали конкретные алгоритмы деанонимизации пользователей биткойна через генерирование DDoS-атак со стороны правоохранительных органов⁸ [9]. Так, в момент реализации купли-продажи на кошелек злоумышленника обрушивается шквал запросов на производство перевода биткойнов, в свою очередь, сервис не позволяет обработать все запросы, что, безусловно, отражается во входящем и исходящем трафике лица, и посредством снифера (анализатора) трафика эти факты фиксируются и являются доказательством принадлежности криптокошелька проверяемому лицу.

В последующем перед оперативным сотрудником стоит задача отождествления криптокошелька, возможно оно лишь с выемкой устройства, к которому привязан криптокошелек. При этом данные о незаконных транзакциях могут находиться в зависимости от использованных сервисов, которые были рассмотрены выше. Так, к примеру, при использовании специального программного обеспечения все данные о транзакциях могут храниться в кэш-памяти самого устройства. Если же использовались веб-ресурсы, то следует обращать внимание на посещаемые веб-сайты, например *Coin.Space*, *BTC.com*, *bitgo.com*, *хоро.com*, *coinapult.com* и др.

Необходимо отметить работу зарубежных правоохранительных органов по идентификации и ото-

ждествлению лиц, осуществляющих незаконную деятельность с использованием криптокошельков. В частности, Федеральное бюро расследований (ФБР) США, Администрация по борьбе с наркотиками (DEA) и Европол сотрудничают с коммерческими организациями, которые предоставляют программные продукты, позволяющие отслеживать людей, участвующих в незаконной деятельности, связанной с криптовалютами. Примером может служить компания *Chainalysis*, занимающаяся криптовалютными расследованиями, выпускающая продукт под названием *Know Your Transaction (KYT)*. С использованием данной программы зарубежные правоохранительные органы успешно работают и получают необходимые данные для доказывания по делам незаконного сбыта наркотических средств⁹.

Использование криптовалютных технологий не гарантирует абсолютной анонимности еще и потому, что рано или поздно человеку необходимо воспользоваться легальными платежными системами для получения наличных денежных средств либо для придания доходам, полученным преступным путем, легального статуса. Это возможно путем вывода криптовалюты на Qiwi-кошелек, идентифицировать который легко, если осуществить запрос от правоохранительных органов в соответствующую организацию, которая предоставит данные о лице.

Безусловно, описанные механизмы обеспечения безопасности функционируют в первую очередь в рамках международного взаимодействия. Это взаимодействие должно быть направлено на обмен положительным опытом по идентификации криптокошельков, а также в плане разработки унифицированной нормативно-правовой политики в области обеспечения безопасности государств — участников СНГ.

Перспективы использования технологии блокчейн в экономике

В любой хозяйственной деятельности ключевым фактором являются данные, причем современные сферы экономики подразумевают огромные объемы информации. Эта информация для эффективной деятельности должна храниться в цифровом виде, а значит, храниться безопасно и качественно обрабатываться компьютерными методами. Кроме того, множество информации в экономической сфере требует наличия цифровых подписей [8, 13] или различных посредников. Так, например, поиск качественного продукта требует от поставщика некоторых усилий. Однако если в систему блокчейн поместить продукт или его составляющие, дополнительная проверка при приобретении продукта не потребует, информация о его происхождении будет доступна. Все поставщики смогут идентифицировать друг друга, размещая собственную информацию независимо друг от друга. Блокчейн позволяет заме-

⁷ Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в области обеспечения информационной безопасности, 20 ноября 2013 года, Санкт-Петербург. URL: <http://docs.cntd.ru/document/420278452> (дата обращения: 20.07.2020).

⁸ Об оперативно-розыскной деятельности [Электронный ресурс]: Федеральный закон № 144-ФЗ : [принят 12.08.1995] : [ред. 06.07.2016] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_7519/ (дата обращения: 07.09.2020).

⁹ URL: <https://www.chainalysis.com/company> (дата обращения: 20.09.2020).

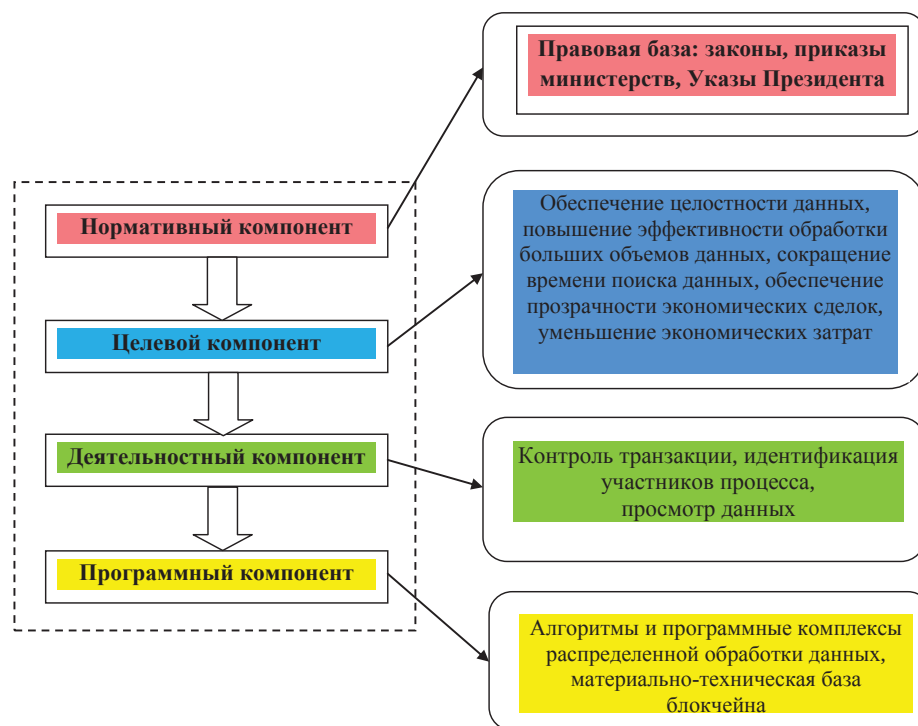


Рис. 1. Концептуальная модель использования технологии блокчейн в экономике

нить цифровую подпись, следовательно, существенно сократить армию посредников, подтверждающих подлинность тех или иных документов или процессов.

Рассмотрим модель применения технологии блокчейн в цифровой экономике (рис. 1). Модель состоит из четырех компонентов. Нормативный компонент определяет правовую базу применения блокчейн-технологии в сфере экономики.

В России обеспечение ускоренного внедрения цифровых технологий в экономике и социальной сфере является одной из национальных целей развития. Для этого в Указе Президента Российской Федерации от 7 мая 2018 г. № 204¹⁰ определены следующие задачи:

увеличение внутренних затрат на развитие цифровой экономики за счет всех источников (по доле в валовом внутреннем продукте) не менее чем в 3 раза по сравнению с 2017 г.;

создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств;

использование преимущественно отечественного программного обеспечения государственными органами, органами местного самоуправления.

Целевой компонент определяется обеспечением целостности данных, повышением эффективности обработки больших объемов данных путём сокращения

времени поиска данных, обеспечением прозрачности экономических сделок, уменьшением затрат на аренду, персонал, логистику и др. за счет использования блокчейн-технологии.

Деятельностный компонент представляет собой организацию последовательности независимых блоков, которые могут предназначаться для хранения узкоспециализированной экономической информации. Это могут быть наборы товаров, производимые фирмой, перечни сделок, совершаемых на бирже, списки заключенных контрактов и др. Концептуальность предлагаемой модели предполагает модификацию ее компонентов в соответствии с направленностью экономической деятельности. Так, например, если модель интегрировать в биржевую деятельность, то деятельностный компонент может включать журнал независимых транзакций по заключенным сделкам, блоки распределенной базы данных содержат информацию по биржевым контрактам и др.

Программный компонент модели осуществляет информационно-коммуникационную поддержку данных. Сюда относятся различные алгоритмы и программные комплексы распределенной обработки данных, материально-техническая база блокчейна, уровень которой существенно влияет на эффективность информационно-экономической деятельности.

Рассмотрим риски использования блокчейн-технологии в экономической деятельности (рис. 2).

Блокчейн-технология является прежде всего технологией распределенной обработки данных, т. е. блоки данных хранятся на различных физических серверах и не имеют централизованного управления.

¹⁰ Указ Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // Собрание законодательства Российской Федерации. 2018. № 20. Ст. 2817.

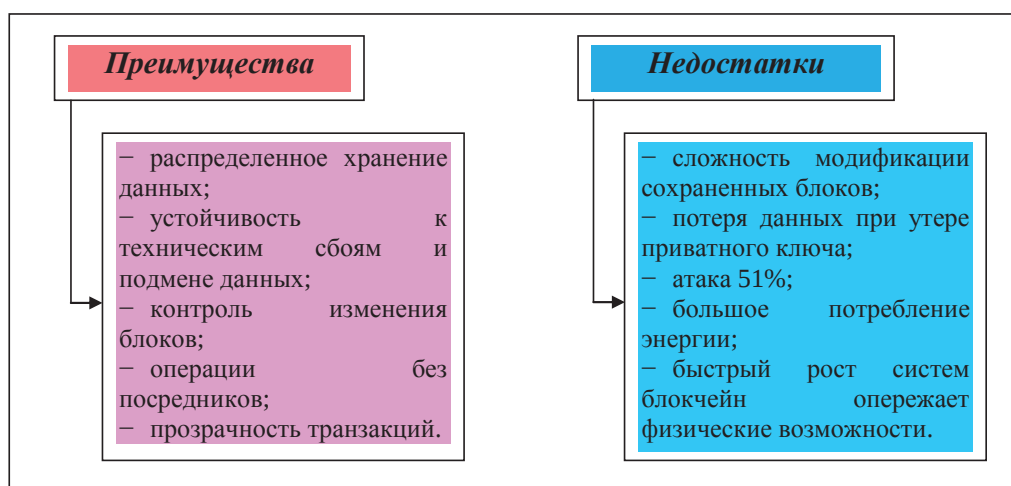


Рис. 2. Преимущества и риски применения технологии блокчейн

Такая структура физического хранения информации обеспечивается сетевыми операционными системами и на первый взгляд все пользователи базы данных имеют равные права доступа и модификации данных. Однако в распределенных базах данных разработан механизм защиты информации, основанный на различных критериях, например: фиксированный промежуток времени работы с информацией, выделенная точка доступа, указание полномочий пользователя, учет предыстории обращения к данным, контроль за непротиворечивостью модифицируемых данных. Технология распределенного хранения информации обеспечивает *устойчивость* данных к техническим сбоям системы, к подмене данных и различным хакерским атакам.

При разработке распределенной базы данных инженеры-программисты должны предложить механизмы обеспечения согласованности и изоляции данных. Эти функции являются достаточно затратными с точки зрения используемых ресурсов. Согласованность и изоляция данных требуют горизонтального масштабирования данных по нескольким признакам, например, нахождение пользователей в различных часовых поясах. Чем выше уровень согласованности данных, тем ниже уровень доступности этих данных для пользователя. Аналогично определяется уровень изоляции данных. Чем он ниже, тем выше скорость обработки данных. Системы управления базами данных предлагают разработчику несколько уровней согласованности и изоляции. Инженер-программист выбирает наиболее приемлемый уровень, ориентируясь на проблемы своей предметной области.

После сохранения данных в блоке эти данные практически невозможно изменить или удалить, следовательно, экономическая и финансовая информация надежно сохраняется и все этапы модификации фиксируются в журнале контроля транзакций. Кроме того, блокчейн позволяет проводить операции без посредника,

напрямую с участниками сделки, без подтверждения операций цифровой подписью. Вся цепочка операций в системе блокчейн прозрачна, так как любой блок доступен для просмотра.

Однако у использования технологии блокчейн существуют и недостатки. Сохраненные блоки достаточно сложно модифицировать, иногда проще создать новую цепочку блоков. Для доступа к блоку пользователь имеет публичный ключ, который можно предоставить другим пользователям, и приватный ключ, который хранится только у пользователя. Если приватный ключ утерян, то доступ к данным теряется [11].

Существует также теоретическая опасность так называемой атаки 51% («картельный сговор»). Если 51% вычислительных ресурсов системы блокчейн будут относиться к одному устройству, то целостность информации будет нарушена. Если майнер-злоумышленник завладеет 51% мощностей блокчейн платформы, то он может, в частности, выполнить следующее: разделить вычислительную цепочку на две, лишая тем самым возможности формирования нормальной последовательности действий; выполнить двойную трату средств, лишая собственников их денежных объемов; воспрепятствовать другим майнерам находить блоки цепочки; блокировать подтверждение транзакций и др. Если же владение мощностями превышает 51%, то ситуация становится критической: денежные средства переходят к злоумышленникам, структура цепочек нарушается, история транзакций удаляется.

Блокчейн требует существенных затрат энергии для своей эффективной работы. Системы блокчейн быстро расширяются, и их размер может превысить реально существующий объем памяти, тогда некоторые блоки могут быть утеряны.

Несмотря на наличие рисков применения технологии блокчейн, эта технология достаточно универсальна, она применима в различных областях деятельности человека. Экономический эффект она может дать там, где исключается ресурсоемкий посредник или этот по-

средник может использовать свое положение для противоправных действий.

Заключение

Итак, запреты никогда не давали экономике существенных преимуществ. Всякие ограничения приводят к «теневым» процессам и нарушениям существующих законов. Госдума РФ приняла 22 июля 2020 г. в третьем чтении закон «О цифровых финансовых активах»¹¹, который вступит в силу с января 2021 г. и который уже заслужил много комментариев в свой адрес. Минфин хочет ужесточить регулирование криптовалют¹².

Предлагаем некоторые действия, которые помогут преодолеть разрыв между внедрением высокотехнологичных экономических или финансовых новелл и правовым полем современного общества:

- необходимо ввести четкое разграничение между преступными действиями в области криптооборота и с использованием криптовалюты и действиями в финансовой и экономической сфере, которые находятся в правовом поле, не нарушают закон и направлены на укрепление демократии и мира в информационном обществе;
- исключить существующие разночтения в Налоговом кодексе, Законе о цифровых финансовых

активах и в пакетах инициатив Минфина по регулированию криптовалют;

- разработать понятийный аппарат на международном уровне для определения самого явления или объекта цифрового мира «криптовалюта» и операций с применением данного объекта на теоретической основе международного информационного права [12, 13];
- теоретики права и гуманитарная наука в целом должны оценить риски и угрозы от использования технологий, которые порождают новую платежную и финансовую систему, оценить положительный и отрицательный вектор развития этих технологий в информационном и цифровом будущем;
- правоохранительные органы стран СНГ, при высоком техническом оснащении и при условии подготовленности сотрудников к такого рода оперативно-розыскной работе, когда сотрудник должен разбираться в информационных технологиях, интернет-технологиях и соответствующем оборудовании, смогут противостоять новым угрозам и вызовам преступного мира, оснащенного новыми способами совершения преступных деяний [3, 4];
- необходимо уделить особое внимание образовательным стандартам, которые должны содержать такие компетенции для будущих работников правоохранительной и правотворческой деятельности, обеспечивающие знания именно в области компьютерно-технического и прикладного программного обеспечения [2]. Только при условии грамотности в этой области можно быть уверенными в безопасности будущих поколений, которые еще больше «окунутся» в информационный мир, где будут царить интернет-вещи и цифровые активы.

¹¹ Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (вступит в силу с 1 января 2021 г., за исключением подпункта «б» п. 3 ст. 17 настоящего Федерального закона, который вступит в силу с 10 января 2021 г.). URL: http://www.consultant.ru/document/cons_doc_LAW_293757/ (дата обращения: 3.09.2020).

¹² Минфин предложил ужесточить регулирование криптовалют в России. URL: <https://www.rbc.ru/crypto/news/5f6c49079a79474d36bc852b> (дата обращения и опубликования: 24.09.2020).

Литература

1. Бегларян М. Е., Добровольская Н. Ю. Блокчейн-технология в правовом пространстве // Вестник Краснодарского университета МВД России. 2018. № 2 (40). С. 108—112.
2. Бегларян М. Е., Добровольская Н. Ю. Формирование ИТ-компетенции юриста в цифровом пространстве // Правовая информатика. 2019. № 3. С. 60—70. DOI: 10.21681/1994-1404-2019-3-60-70.
3. Ващекин А. Н., Ващекина И. В. Информационное взаимодействие в системе борьбы с «отмыванием» преступных доходов: риск-ориентированный подход // Правовая информатика. 2018. № 4. С. 4—13. DOI: 10.21681/1994-1404-2018-4-04-13.
4. Ващекина И. В., Ващекин А. Н. Применение риск-ориентированного подхода при организации противодействия отмыванию нелегальных доходов в российской практике // Наука и практика. 2018. № 3. С. 61—69.
5. Вайпан В. А. Основы правового регулирования цифровой экономики // Право и экономика. 2017. № 10. С. 5—18.
6. Государство и право в новой цифровой реальности : монография / Под общ. ред. И.А. Конюховой-Умновой, Д.А. Ловцова. М.: ИНИОН РАН, 2020. 259 с. ISBN 978-5-248-00959-6.
7. Карцхия А. А. Цифровая трансформация права // Мониторинг правоприменения. 2019. № 1(30). С. 25—29. DOI: 10.21681/2226-0692-2019-1-25-29.
8. Ловцов Д. А. Системология правового регулирования информационных отношений в инфосфере : монография. М. : РГУП, 2016. 316 с.

9. Ловцов Д. А. Имплементация «цифровых» прав в экономике: информационно-правовые аспекты // Российское правосудие. 2020. № 10. С. 42—53. DOI: 10.37399/issn2072-909X.2020.10.42-53.
10. Ловцов Д. А. Информационно-правовые основы правоприменения в цифровой сфере // Мониторинг правоприменения. 2020. № 2(35). С. 44—52. DOI: 10.21681/2226-0692-2020-2-44-52.
11. Ловцов Д. А. Информационная безопасность автоматизированных блокчейн-систем: угрозы и способы повышения // Тр. II Междунар. науч.-практ. конф. «Трансформация национальной социально-экономической системы России» (22 ноября 2019 г.) / РГУП. М. : РГУП, 2020. С. 464—473. ISBN 978-5-93916-823-6.
12. Ловцов Д. А. Теория информационного права: базисные аспекты // Государство и право. 2011. № 11. С. 43—51. ISSN 0132-0769.
13. Ловцов Д. А. Системология правового регулирования информационных отношений в инфосфере: архитектура и состояние // Государство и право. 2012. № 8. С. 16—25. ISSN 0132-0769.
14. Савельев А. И. Некоторые аспекты использования смарт-контрактов и блокчейн-технологий по российскому праву // Закон. 2017. № 5. С. 94—117.
15. Черных А. М. Защищенность данных об объектах недвижимости и земельных ресурсах на базе геоинформационных и блокчейн технологий // Правовая информатика. 2019. № 4. С. 75—85. DOI: 10.21681/1994-1404-2019-4-75-85.

Рецензент: **Цимбал Владимир Анатольевич**, доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, профессор кафедры автоматизированных систем управления Филиала Военной академии имени Петра Великого, г. Серпухов, Российская Федерация.

E-mail: tsimbalva@mail.ru

BLOCKCHAIN TECHNOLOGY FOR DIGITALISATION OF ECONOMY: THREATS AND PROSPECTS

Margarita Beglarian, Ph.D. (Physics & Mathematics), Associate Professor, Head of the Department of Social & Humanitarian and Natural Scientific Disciplines of the North Caucasus Branch of the Russian State University of Justice, Krasnodar, Russian Federation.

E-mail: rita_beg@mail.ru

Natal'ia Dobrovol'skaia, Ph.D. (Paedagogics), Associate Professor at the Information Technology Department of the Kuban State University, Krasnodar, Russian Federation.

E-mail: dnu10@mail.ru

Keywords: blockchain, technology, digitalisation of economy, implementation, cryptocurrency, model, legal framework, legislation, law enforcement agencies.

Abstract.

Purpose of the paper: considering questions of implementing blockchain as a technology of the future which will make it possible to spare financial resources, make financial schemes transparent, and block the very possibility of committing illegal actions in the economic sphere. But at the same time attention is paid to 'the other side of the coin', when the same technology ends up in the hands of the criminal community.

Methods used: conceptual modelling of digitalisation of economy and implementation of digital processes, formalisation of the development of efficient legal methods having methodological significance for the Russian economy.

Results obtained: the author's position and proposals as regards the future of blockchain for the digitalisation of Russian economy are presented. Digitalisation and the introduction of new, sometimes alien and dangerous, technologies will have a strong impact on the global financial system and economy, so it is important to timely adjust the legislative framework for the information progress novelties, excluding prohibitions.

References

1. Beglarian M. E. Dobrovol'skaia N. Iu. Blokchein-tekhnologii v pravovom prostranstve. Vestnik Krasnodarskogo universiteta MVD Rossii, 2018, No. 2 (40), pp. 108-112.
2. Beglarian M. E., Dobrovol'skaia N. Iu. Formirovanie IT-kompetentsii iurista v tsifrovom prostranstve. Pravovaya informatika, 2019, No. 3, pp. 60-70. DOI: 10.21681/1994-1404-2019-3-60-70.

3. Vashchekin A. N., Vashchekina I. V. Informatsionnoe vzaimodeistvie v sisteme bor'by s "otmyvaniem" prestupnykh dokhodov: risk-orientirovannyi podkhod. Pravovaia informatika, 2018, No. 4, pp. 4-13. DOI: 10.21681/1994-1404-2018-4-04-13.
4. Vashchekina I. V., Vashchekin A. N. Primenenie risk-orientirovannogo podkhoda pri organizatsii protivodeistviia otmyvaniu nelegal'nykh dokhodov v rossiiskoi praktike. Nauka i praktika, 2018, No. 3, pp. 61-69.
5. Vaipan V. A. Osnovy pravovogo regulirovaniia tsifrovoi ekonomiki. Pravo i ekonomika, 2017, No. 10, pp. 5-18.
6. Gosudarstvo i pravo v novoi tsifrovoi real'nosti : monografiia / Pod obshch. red. I.A. Koniukhovoii-Umnovoi, D.A. Lovtsova. M.: INION RAN, 2020, 259 pp. ISBN 978-5-248-00959-6.
7. Kartskhiia A. A. Tsifrovaia transformatsiia prava. Monitoring pravoprimeneniia, 2019, No. 1(30), pp. 25-29. DOI: 10.21681/2226-0692-2019-1-25-29.
8. Lovtsov D. A. Sistemologiiia pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere : monografiia. M. : RGUP, 2016, 316 pp.
9. Lovtsov D. A. Implementatsiia "tsifrovyykh" prav v ekonomike: informatsionno-pravovye aspekty. Rossiiskoe pravosudie, 2020, No. 10, pp. 42-53. DOI: 10.37399/issn2072-909X.2020.10.42-53.
10. Lovtsov D. A. Informatsionno-pravovye osnovy pravoprimeneniia v tsifrovoi sfere. Monitoring pravoprimeneniia, 2020, No. 2(35), pp. 44-52. DOI: 10.21681/2226-0692-2020-2-44-52.
11. Lovtsov D. A. Informatsionnaia bezopasnost' avtomatizirovannykh blokchein-sistem: ugrozy i sposoby povysheniia. Tr. II Mezhdunar. nauch.-prakt. konf. "Transformatsiia natsional'noi sotsial'no-ekonomicheskoi sistemy Rossii" (22 noiabria 2019 g.) / RGUP. M. : RGUP, 2020, pp. 464-473. ISBN 978-5-93916-823-6.
12. Lovtsov D. A. Teoriiia informatsionnogo prava: bazisnye aspekty. Gosudarstvo i pravo, 2011, No. 11, pp. 43-51. ISSN 0132-0769.
13. Lovtsov D. A. Sistemologiiia pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere: arkhitektura i sostoianie. Gosudarstvo i pravo, 2012, No. 8, pp. 16-25. ISSN 0132-0769.
14. Savel'ev A. I. Nekotorye aspekty ispol'zovaniia smart-kontraktov i blokchein-tekhnologii po rossiiskomu pravu. Zakon, 2017, No. 5, pp. 94-117.
15. Chernykh A. M. Zashchishchennost' dannykh ob ob'ektakh nedvizhimosti i zemel'nykh resursakh na baze geoinformatsionnykh i blokchein tekhnologii. Pravovaia informatika, 2019, No. 4, pp. 75-85. DOI: 10.21681/1994-1404-2019-4-75-85.