DOI: 10.30680/ECO0131-7652-2018-8-78-92

# Криптовалюты и блокчейн: потенциальные применения в государстве и бизнесе

**А.И. ПЕСТУНОВ,** кандидат физико-математических наук, Новосибирский государственный университет экономики и управления «НИНХ», Новосибирск.
E-mail: pestunov@gmail.com

Криптовалюты и распределенные реестры (блокчейны) в последнее время вызывают повышенный интерес у специалистов самых разных областей. При этом в обществе сформировался некоторый пул регулярно задаваемых вопросов, ответы на которые в полной мере пока не даны. В статье представлена аргументация по некоторым популярным вопросам, связанным с указанной тематикой. Затронуты такие проблемы, как создание национальных криптовалют и использование технологии блокчейн в бизнесе и государственной деятельности. Проанализировано мнение о том, что криптовалюты являются финансовой пирамидой. Кратко рассмотрена конфигурация распределенного реестра биткойн и потенциальное влияние на него гипотетического создания квантового компьютера.
*Ключевые слова:* криптовалюта, распределенный реестр, блокчейн, биткойн, эфириум, национальная криптовалюта, крипторубль, криптодоллар, токен, финансовая пирамида, ICO

Криптовалюты и распределенные реестры (блокчейны) в последнее время вызывают повышенный интерес у специалистов самых разных областей профессиональной деятельности. В России эти технологии выделены как одно из направлений программы «Цифровая экономика»[1], а на сайте Минфина опубликован специально подготовленный законопроект по регулированию криптовалют под названием «О цифровых финансовых активах»[2]. Особо резким взлетом интереса к данной сфере запомнился 2017 г., в течение которого сформировался некоторый пул регулярно задаваемых вопросов, ответы на которые в полной мере пока не найдены. В настоящей статье представлен обзор наиболее часто задаваемых вопросов, связанных с криптовалютами, и приведены аргументированные ответы на них.

[1] Программа «Цифровая экономика Российской Федерации». URL: government.ru/
[2] О проекте федерального закона «О цифровых финансовых активах». URL: www.minfin.ru/

## Может ли государство выпустить национальную криптовалюту?

В последнее время новости о том, что Россия планирует выпустить свою национальную криптовалюту, достаточно распространены. В связи с этим возникает желание разобраться, насколько обоснованны подобные заявления и в какой форме они могут быть реализованы. Вероятно, что независимо от реальных планов Центрального банка и Правительства РФ, это отчасти является маркетинговым ходом, способствующим формированию прогрессивного имиджа страны.

**Может ли Россия создать крипторубль?** В принципе, назвать крипторублем можно все, что угодно, в том числе и обычный рубль, и государственные облигации, и акции какой-нибудь госкорпорации (и даже частной компании). Никаких ограничений нет, поскольку официального определения «крипторубль» или «национальная криптовалюта» не существует, и каждый может вкладывать в это понятие свой смысл.

Однако, если говорить о криптовалюте как о некоем феномене, мнение о котором уже сформировалось в сообществе пионеров технологии блокчейн и подключившихся позднее энтузиастов, то можно выделить два свойства, характеризующих криптовалюты с разных сторон. Первое. Идеологически криптовалюта – это некий слабо контролируемый финансовый актив, пользоваться которым легко и дешево (и не важно, насколько эти принципы удалось реализовать на практике). При этом не требуется отчитываться о своих доходах, платить налоги и указывать источник заработка. Второе. Технологически криптовалюта – это финансовый актив, который записан не на серверах банков, объединенных в традиционную компьютерную сеть, а в блокчейне.

Таким образом, становится очевидным, что создать национальную криптовалюту в идеологическом смысле невозможно из-за того, что два слова в этом словосочетании несовместимы. «Национальная» подразумевает, что валюта централизована и подконтрольна (или, как минимум, сильно зарегулирована), а префикс «крипто-» означает, что валюта децентрализована и неподконтрольна (как минимум, слабо зарегулирована).

Что касается технологического смысла, то национальную криптовалюту выпустить вполне возможно, но по сути это будет просто другая форма безналичных денег. Тогда криптовалюту

можно рассматривать как очередное звено в цепочке (камешки и ракушки, золотые монеты, бумажные деньги, безналичные деньги). Эта эволюция обусловлена упрощением расчетов с помощью очередного типа денег. Сейчас одновременно существуют и наличные, и безналичные деньги, которые разные по сути, но законодательство их уравнивает. По аналогии часть денег (скажем, рублей) можно заменить криптовалютой, но для конечного пользователя работа с ней будет аналогична операции с безналичными деньгами. Для банковской системы это может снизить издержки и ускорить платежи. Точно так же как в ряде случаев безналичные деньги оказываются дешевле и быстрее в использовании, чем наличные.

**О криптодолларе Tether (USDT).** Хотя криптовалюта Tether, маркируемая символами USDT, в обиходе называется «криптодолларом», на самом деле это – частная криптовалюта, выпускаемая компанией Tether[3]. Цель ее создания – обеспечить участников соответствующего рынка криптовалютой со стабильным курсом. При работе с криптовалютами возникают две важные проблемы: все они крайне волатильны, но при этом на стыке фиатных[4] и криптографических валют возникают нормативно-правовые сложности, не позволяющие в полной мере осуществлять конвертацию в обоих направлениях. В частности, организации, работающие на таком стыке, могут подвергаться более частым проверкам, а их документооборот – усложняться. Так, например, одна из крупнейших криптовалютных бирж Poloniex не работает с фиатной валютой вообще[5]. В итоге, с одной стороны, участникам рынка необходимо фиксировать прибыль в стабильной низковолатильной валюте, а с другой – это не всегда возможно. Криптодоллар Tether призван решить эту проблему.

Эмиссия криптодоллара осуществляется частной компанией, но согласно документации, размещенной на ее сайте, объем эмитируемых криптодолларов равняется объему полученных ею фиатных долларов. Таким образом, Tether выступает в роли обменника, который берет на себя юридические аспекты конвертации и предоставляет участникам рынка возможность свободного

[3] Tether: digital money for a digital age. URL: tether.to/

[4] От лат. fiat – декрет. указание. Декретные деньги, не обеспеченные реальными ценностями. Фиатными являются и большинство бумажных купюр.

[5] Криптовалютная биржа Poloniex. URL: poloniex.com/

использования псевдодоллара в криптовалютном пространстве. При этом, несмотря на внешне полезную и работоспособную модель, отсутствует полная уверенность в том, что все единицы криптодоллара подкреплены реальными средствами на счетах компании.

## Как связаны криптовалюты и «блокчейн»?

**Что такое блокчейн?** В документе «Программа развития цифровой экономики» блокчейн назван распределенным реестром, и так же трактуется этот термин в настоящей статье. Блокчейн – это распределенный журнал, в который можно только добавлять записи при невозможности исправлять ранее сделанные (append-only). Этот запрет реализован на технологическом уровне и поддерживается тем, что теоретически такая возможность есть, но для ее практического осуществления необходимо выполнение условия с ничтожно малой вероятностью. В итоге, даже если в блокчейн внесена ошибочная запись, то все, что можно сделать, – это добавить еще одну запись, указав на ошибочность предыдущей.

Слово «распределенный» в данном случае означает, что все записи этого журнала дублируются на многих узлах одноранговой сети, что обеспечивает стабильность независимо от работоспособности отдельно взятого узла. Кроме того, если рассматривать блокчейн в исходном идеологическом контексте, то (по крайней мере, в теории) все узлы должны контролироваться различными, не подчиняющимися друг другу субъектами, что, в свою очередь, должно гарантировать необходимость всеобщего согласия (консенсуса) при добавлении очередной записи в журнал. Именно это требование гарантирует невозможность подделок записей. Если большая часть узлов такой сети контролируется одним управляющим центром, то по его команде можно подменить записи, а распределенность будет обеспечивать только стабильность сети, но не запрет подделок.

**Блокчейн как облачный сервис с более высоким уровнем доверия.** С некоторым упрощением блокчейн можно считать облачным сервисом с дополнительными средствами защиты, наделяющими его более высоким доверием, чем традиционные облачные технологии. И если традиционные облачные сервисы и хранилища широко используются для обработки и хранения

информации, которую нельзя отнести к критически важной, то хранить в них информацию о бухгалтерии, состоянии банковских счетов, правах собственности и другие сведения большой значимости очень рискованно, поскольку пользователь полагается лишь на надежность и честность сервиса, не имея гарантий, что данные не пропадут или не будут подделаны. В блокчейне же есть надежные инструменты защиты от этих атак, и, более того, конечный пользователь всегда может непосредственно проверить, что интересующие его данные не были подделаны.

**Криптовалюты – одно из применений распределенного реестра.** Поскольку информация о денежных счетах должна быть надежно защищена от подделок, то одно из очевидных применений блокчейна – это поддержка оборота денежных средств. И валюты, поддерживаемые блокчейном, называются криптовалютами. Таким образом, ошибочным является мнение о том, что термины «криптовалюта», «блокчейн» и «биткойн» – синонимы. Это хотя и связанные, но разные понятия.

Во-первых, биткойн – это только одна из многочисленных криптовалют, хотя и наиболее крупная по капитализации и известности, существуют и сотни других. Наибольшую капитализацию[6] имеют Etherium, Ripple, Dash, Litecoin, Cardano, NEM. Во-вторых, блокчейн – это чрезвычайно многогранная технология, а криптовалюты являются всего лишь одним из ее потенциально многочисленных приложений. И, в-третьих, блокчейнов существует довольно много, просто какие-то из них более известны, а какие-то – менее.

## Какие возможности распределенный реестр предоставляет государству и бизнесу

**Кому может быть выгоден блокчейн?** Итак, распределенный реестр – это альтернатива третьей доверенной стороны в различных бизнес-процессах, а третья доверенная сторона – это просто некий уполномоченный посредник, коим являются банки, государственные институты, службы заказа услуг и т.п. Таким образом, любой, кто пользуется услугами посредников и по каким-либо причинам считает этот вариант неоптимальным, потенциально может извлечь пользу от его замены распределенным реестром.

[6] Рыночная капитализация криптовалют. URL: coinmarketcap.com/

Причем в разных ситуациях физические лица и организации могут одновременно оказываться в роли как посредника, так и клиента такого посредника. Значит, в первом случае распределенный реестр нежелателен, ведь он просто заменяет посредника, а во втором – способен принести пользу.

Например, банки могут выступать в двух ролях: третьей доверенной стороны для своих клиентов и клиентов – при осуществлении межбанковских платежей. Таким образом, в первом случае блокчейн банкам выгоды не принесет, поскольку этот распределенный реестр сам будет играть роль третьей доверенной стороны, фактически заменяя банки. Во втором же случае банки в роли клиентов центробанков, более крупных или просто иных финансовых организаций могут выгоднее для себя использовать блокчейн с целью ускорения трансакций и снижения их стоимости.

**Использование смарт-контрактов.** Одним из предпочтительных сценариев по замене доверенных посредников может стать использование смарт-контрактов. По внешним проявлениям его можно сравнить с достаточно часто встречающимися соглашениями между взаимодействующими сторонами, когда одна из этих сторон получает возможность перевести денежные средства на свой счет при наступлении некоторого события. Например, отель может заблокировать сумму за первые сутки проживания на карте гостя, забронировавшего номер, и снять ее, если тот не заселился. Аналогичные по смыслу соглашения заключаются, когда абоненты поставщиков каких-либо услуг соглашаются с тем, чтобы с заданной периодичностью и в заданном размере производилось списание средств.

Потенциально технологии распределенных реестров при разумном использовании способны значительно упростить различные трансакции, которые сейчас осуществляются с использованием посредников: не только финансовые, но и акты регистрации собственности, гражданско-правовых отношений, сдачи-приемки и т.д. Если говорить о сфере денежно-кредитных отношений, то с использованием смарт-контрактов можно реализовывать практически любые операции: аккредитивы, займы, межбанковские платежи и т.д.

**В какой форме может быть использован блокчейн?** Защищенный распределенный реестр – это источник доверия,

который потенциально может быть более удобным и дешевым, чем те, которые используются сейчас. Однако когда идет речь об использовании блокчейна при решении конкретных бизнес-задач и анализе целесообразности его внедрения, следует понимать, что можно использовать внешний уже существующий блокчейн (например, поддерживающий биткойн или эфириум) или разработать собственный совместно со своими контрагентами. Создание чисто внутреннего блокчейна особого смысла не имеет, поскольку в таком случае все серверы будут находиться под контролем одной доверенной стороны, что приведет к избыточному усложнению информационной инфраструктуры без получения ощутимой выгоды.

Возможна также разработка некоего совместного транснационального распределенного реестра заинтересованными государствами и организациями. Тем самым каждый из таких субъектов, поддерживающих блокчейн, будет, с одной стороны, вкладывать ресурсы для его поддержания и сохранения доверия к нему, а пользоваться им смогут все. Таким образом, этот реестр уже будет сформирован согласно требованиям, заложенным такими заинтересованными структурами. Это будет не блокчейн биткойна или эфириума, которые при всей их открытости разработаны закрытой группой людей, и их архитектура и система защиты могут не устраивать банки, государства и крупные компании.

### Являются ли криптовалюты пирамидой?

**Говорить о криптовалютах как о пирамиде некорректно.** Очень важно понимать, что зарождающаяся экосистема криптовалют и распределенных реестров потенциально достаточно обширна, и внутри нее могут возникать финансовые пирамиды, что уже происходит. Действительно, некоторые компании, вышедшие на ICO, не выполняют свои обязательства и пропадают в никуда после сбора денег или после взлета курса их токенов. Поскольку криптовалюты в основном находятся вне правового поля, то привлечь таких недобросовестных лиц к ответственности довольно сложно.

Однако помимо подобных мошенников существует масса добросовестных организаций, предлагающих реальные услуги за свои валюты. Таким образом, неправильно считать все криптовалюты, в том числе самую известную из них – биткойн –

пирамидами. Заметим, что доллар или вся мировая финансовая система тоже имеют признаки пирамиды. Действительно, в последние годы накопилось много вопросов, касающихся долларовой экономики, но, несмотря на обилие проблем в этой сфере, никто не отрицает ее полезность (хотя, конечно, вряд ли ее можно считать оптимальной).

**Криптовалюты можно считать высокорискованным финансовым активом.** Несмотря на то, что между криптовалютами и финансовыми пирамидами можно провести некоторые аналогии, все же ставить между ними знак равенства нельзя. Действительно, те, кто стал заниматься майнингом или покупкой криптовалют несколько лет назад, когда о них еще мало кто знал, и их курс был ничтожно малым по сравнению с сегодняшним днем, смогли не просто заработать, но даже сделать состояние. Во многом это произошло за счет тех, кто присоединился позднее. Однако для «опоздавших» тоже существуют возможности заработать, например, «игра» на бирже или организация связанного с криптовалютами бизнеса.

Скорее, криптовалюты можно считать высокорискованным финансовым активом из-за их высокой волатильности и отсутствия регулирования в большинстве государств. Это означает, что в случае каких-либо потерь предъявить претензии будет некому. При этом попробуем провести аналогию между криптовалютами и традиционными финансовыми активами. В настоящее время общая капитализация криптовалют колеблется в диапазоне 500–800 млрд долл., но конвертировать всю эту сумму в фиатные валюты или ценности реального мира в таком объеме не удастся, поскольку объем рынка достаточно мал, и, если начать выводить крупные суммы, то курс неизбежно упадет. В связи с этим большая часть эмитированных криптовалют (в том числе биткойнов) лежит на счетах «мертвым грузом» и никогда не была использована. Данная ситуация аналогична рынку акций и банковским депозитам: если продавать акции в большом объеме или массово закрывать банковские счета, произойдет обвал.

**Ситуацию вокруг криптовалют можно считать пузырем.** По расчетам некоторых аналитиков, процессы, связанные с криптовалютами и блокчейном, развиваются по кривой Гартнера[7],

[7] Top Trends in the Gartner Hype Cycle for Emerging Technologies. URL: www.gartner.com/

характеризующей цикл развития инновационного продукта или технологии следующим образом. Вначале возникает ажиотажный спрос на все, связанное с новой технологией, и она становится переоцененной. Курс акций связанных с ней компаний резко взлетает. Однако после исчезновения ажиотажа появляется разочарование, вызванное тем, что ожидания тех благ, которые должна принести новая технология, не оправдываются. В итоге акции соответствующих компаний резко падают, однако если технология стоящая, то ряд компаний выживают и продолжают развивать эту технологию.

Существует высокая вероятность того, что пузырь на рынке криптовалют надуется и лопнет, причем, возможно, не один раз. Это подтверждается несколькими скачками курса биткойна[8]. Тем не менее принципиальная разница между пирамидами и такими «высокотехнологичными пузырями» заключается в том, что после пирамиды, как правило, не остается ничего, так как курс акций или облигаций падает до нуля, а в случае с блокчейном уже сейчас очевидна реальная польза применения связанных с ним инструментов. Опасность заключается в том, что они, вероятно, переоценены. Вследствие этого ожидается, что криптовалюты станут пузырем, который схлопнется, подобно доткомам в 2000 г.

**Чем подкреплены криптовалюты?** Ответ на этот вопрос зависит от того, что понимать под подкреплением. Токены являются аналогами жетонов-облигаций, дающих право их держателям на получение продукта или услуги, предоставляемых эмитентом токена. Правда, здесь необходимо учитывать, что значительная часть таких токенов выпущена под проекты, которые планируют выполнять обязательства лишь в будущем. Многие эмитенты гарантируют исполнение обязательств, привязывая их к смарт-контракту, гарантирующему перевод указанного дохода на счет инвестора, однако проблема заключается в том, что успешность проекта в целом никем не гарантируется.

## Современная конфигурация биткойна далека от идеала

Обсудим некоторые проблемы, которые не были прямо заявлены разработчиками биткойна, но проявились на практике.

[8] Blockchain-обозреватель. URL: www.blockchain.info/

**«Форки» и допэмиссия биткойна.** Хотя согласно настройкам оригинального приложения число биткоинов в обращении ограничено и не может превышать 21 млн (что, по задумке создателей, должно сформировать альтернативу инфляционной экономике), существует возможность создания его веток (форков), которые фактически являются новыми криптовалютами, также поддерживаемыми майнерами. Начальное количество монет на счетах пользователей не нулевое, а определяется числом монет, которые были на счетах оригинального биткойна. Таким образом, обещаемая в теории ограниченная эмиссия на практике оказывается неограниченной. В настоящее время уже создано несколько известных форков биткойна – Bitcoin Cash, Bitcoin Gold, Bitcoin Diamond, Super Bitcoin, и их потенциальное количество не ограничено. Кроме того, появляются все новые и новые криптовалюты.

**Проблемы децентрализованности биткойна.** В оригинальной статье [Nakamoto, 2008], где представлена система биткойн, она позиционировалась как децентрализованная и не подконтрольная никаким структурам. Все записи осуществляются только по согласию большинства участников. Тем не менее на практике существуют признаки того, что система не является децентрализованной в полной мере.

Во-первых, по данным на начало 2018 г.[9], десять крупнейших в мире пулов для майнинга (среди них F2Pool, AntPool, BitFury) контролировали около 80% мощности всей биткойн-сети. Этот факт говорит о принципиальной возможности сговора менеджеров таких пулов, что может позволить им не просто получать почти все эмиссионные биткойны, но и существенно замедлять (или практически блокировать) неугодные трансакции. Тем не менее такие манипуляции, конечно, должны носить умеренный характер, поскольку сильные вмешательства могут подорвать доверие к криптовалюте и уронить ее курс.

Во-вторых, обновление системы осуществляется полномочным ядром разработчиков, которые имеют значительно большее влияние в экосистеме биткойн, чем даже многие майнеры. Наличие ядра разработчиков обусловлено тем, что периодически возникает необходимость обновлять и устранять ошибки

[9] Top-10 Bitcoin mining pools. URL: fomag.ru/news/top-10-mayning-pulov-bitkoina/

в программном обеспечении, на котором биткойн базируется. Кроме того, ядро разработчиков может изменять комиссионную политику, оказывать существенное влияние на разрешение конфликтов через «жесткие вилки» (hard forks) [Natoli et al., 2017], уведомлять клиентов об обновлениях и т.д. Жесткие вилки – это такое разветвление журнала транзакций, которое невозможно разрешить в рамках установленного протокола выработки консенсуса, что приводит к необходимости вмешательства внешних разработчиков для его устранения. Все эти механизмы дают разработчикам ряд инструментов влияния на всю экосистему биткойн.

Известная «жесткая вилка» имела место 11.03.2013 г. и была связана с тем, что после очередного обновления системы произошло раздвоение блокчейна, так что часть узлов майнеров стали присоединять новые блоки к одной ветке, а часть – к другой. Такая ситуация продолжалась около 90 минут, после чего ядро разработчиков, заручившись поддержкой одного из крупнейших майнинговых пулов, внесли изменения в программное обеспечение и в одностороннем порядке признали недействительной самую длинную из этих веток, обесценив этим около 1700 трансакций. Этот инцидент стал примером того, как группа из нескольких человек оказала большее влияние, чем свыше половины мощности всей биткойн-сети [Gervais et al., 2014].

**О реальной анонимности биткойна.** Хотя биткойн заявлялся как анонимная система, на практике обеспечить анонимность в полной мере невозможно. Поскольку работа с блокчейном напрямую требует специфических навыков в области информационных технологий и информационной безопасности, то для массового пользователя она неприемлема. Для проведения платежей им необходимы посредники, такие как интернет-кошельки, интернет-магазины, сервисы для хранения ключей, криптовалютные биржи и пр. Многие из них требуют идентификационные данные по целому ряду причин, в том числе для реализации мер по противодействию отмыванию преступных доходов и финансированию терроризма. Это приводит к тому, что для обеспечения заявленной анонимности требуются дополнительные ресурсы и усилия, а для массового пользователя ее достижение вообще невозможно.

## Как создание квантового компьютера повлияет на криптовалюты?

**Почему возник этот вопрос?** Безопасность и стабильность распределенного реестра блокчейн обеспечены стойкостью ряда криптографических протоколов, рассчитанных на то, что злоумышленник может обладать современными вычислительными средствами. Длины криптографических ключей выбираются так, чтобы криптоалгоритмы имели запас стойкости на несколько десятилетий вперед[10]. Приближенные оценки осуществляются согласно эмпирическому закону Мура, смысл которого состоит в том, что приблизительно каждые два года производительность компьютеров удваивается, следовательно, потенциально и мощность абстрактного злоумышленника способна увеличиваться с такой же скоростью, которая может значительно возрасти с созданием квантового компьютера.

В настоящее время ведутся активные исследования и разработки в области квантовых вычислений, которые должны привести к появлению полноценного квантового компьютера. Важность этого направления обусловлена тем, что повышать производительность ЭВМ становится все труднее. Сейчас рост производительности достигается за счет уменьшения размера транзисторов, чтобы разместить как можно больше их на кристалле микропроцессора. Но их размеры уже стали соизмеримыми с размерами молекул, поэтому продолжать уменьшение технологически тяжело.

Квантовые компьютеры потенциально способны не просто преодолеть этот барьер и обеспечить продолжение роста производительности, но и достичь скачкообразного ускорения многих алгоритмов, в том числе и методов взлома систем защиты информации. Существует теоретическая модель квантового компьютера и созданы небольшие образцы, применимые только для самых простых вычислений. Однако создание полноценного квантового компьютера является угрозой для стойкости систем защиты информации, использующих криптографию.

**Какие элементы блокчейна испытают влияние квантового компьютера?** В работе [Aggarwal D. et al., 2017] представлены расчеты, на основании которых сделаны некоторые прогнозы

[10] Cryptographic key lengths recommendations. URL: www.keylength.com

о том, что случится с биткойном, если будет создан полноценный квантовый компьютер. Основными элементами, на которые повлияют квантовые вычисления, являются цифровая подпись ECDSA, используемая для подтверждения подлинности владельца денежных средств, и криптографическая хеш-функция SHA-256 – фундаментальный инструмент майнинга. Подтверждение транзакций по схеме доказательства выполненной работы (proof-of-work), заключающееся в частичном обращении криптографической хеш-функции методом полного перебора [Shi, 2016], может быть ускорено с помощью квантового алгоритма Гровера [Grover, 1996], но это приведет лишь к тому, что необходимо будет ждать большего числа подтвержденных блоков перед тем как считать транзакцию осуществленной. В то же время цифровую подпись ECDSA можно будет взломать с помощью квантового алгоритма Шора [Shor, 1994]. Однако на сегодня уже создан ряд криптоалгоримов, которые можно считать стойкими и для квантового компьютера.

Таким образом, создание квантового компьютера повлияет на работу блокчейна биткойна, но в принципе все проблемы могут быть решены, и система останется работоспособной и стабильной.

## Заключение

В заключение обозначим основные тезисы, раскрытые в статье. Первый рассмотренный вопрос касался возможности создания национальной криптовалюты. Это представляется вероятным в том смысле, что национальная криптовалюта будет поддерживаться не традиционными средствами, а технологией блокчейн. В то же время в идеологическом плане создание национальной криптовалюты невозможно, поскольку эти понятия несовместимы: «национальная» подразумевает подконтрольная государству, а «криптовалюта» по своему исконному смыслу должна быть неподконтрольна.

Далее рассматривалась связь между технологией блокчейн и криптовалютами. Отмечено, что криптовалюты являются одним из применений блокчейна, а в более широком контексте блокчейн способен заменить доверенных посредников в самых разных сферах деятельности.

Показано, что в зависимости от ситуации одним и тем же организациям может быть как выгодно, так и невыгодно переходить на технологию блокчейн. Если организация выступает в роли посредника, то ей это невыгодно, поскольку блокчейн просто может ее заменить. Однако там, где она является клиентом других централизованных организаций, возможна выгода.

При рассмотрении вопроса о том, можно ли отнести биткойны и другие криптовалюты к финансовым пирамидам, приведены аргументы в пользу того, что они не являются пирамидами, но их общая капитализация может резко сократиться (подобно известному пузырю доткомов).

Еще один важный тезис, затронутый в статье, заключается в том, что при современной конфигурации распределенных реестров, в частности, сети биткойн, существует целый ряд несоответствий между теоретическими концепциями и практической реализацией. Так, например, показано, что заявленные разработчиками системы свойства анонимности и децентрализованности на практике реализовать крайне сложно.

В последнем разделе статьи кратко рассматривается сценарий того, как будет работать система биткойн после создания квантового компьютера. Ускорение алгоритмов приведет к тому, что майнинг в целом не потеряет смысл, но придется ждать больше подтвержденных блоков перед осуществлением транзакции, а используемая цифровая подпись будет уязвима, и для поддержания стабильности и безопасности системы необходимо ее заменить на подпись, устойчивую к взлому на квантовом компьютере.

Статья поступила 31.01.2018.

## Литература/References

*Aggarwal D., Brennen G.* etc. (2017) Quantum attacks on Bitcoin, and how to protect against them. Cornell University e-print service «ArXiv». 1710.10377v1. 21 p. URL: https://arxiv.org/abs/1710.10377

*Gervais A., Karame G., Capkun V.* etc. (2014) Is Bitcoin a decentralized currency? *IEEE Security & Privacy*. Vol. 12. Pp. 54–60.

*Grover L.* (1996) A fast quantum mechanical algorithm for database search. Proc. 28th ACM symposium on Theory of computing. Philadelphia, Pennsylvania, USA. May 22–24. Pp. 212–219.

*Nakamoto S.* (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. Whitepaper. 9 p. URL: https://bitcoin.org/bitcoin.pdf

*Natoli C., Gramoli V.* (2017) The Balance Attack or Why Forkable Blockchains are Ill-Suited for Consortium. Proc. 47th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Denver, CO, USA, June 26–29. Pp. 579–590.

*Shi N.* (2016) A new proof-of-work mechanism for Bitcoin. *Financial Innovation*. Vol. 31. 8 p. URL: https://link.springer.com/article/10.1186/s40854–016–0045–6

*Shor P.* (1994) Algorithms for quantum computation: discrete log and factoring. Proceedings 35th Symposium on Foundations of Computer Science. Santa Fe, NM, USA. Nov. 20–22. Pp. 124–134.

## Summary

***Pestunov A. I.,*** *Novosibirsk State University of Economics and Management, Novosibirsk*

**«Blockchain» Distributed Secure Ledger and Cryptocurrencies: Potential Using in Business and Government**

Cryptocurrencies as well as distributed ledgers called «blockchains» attract a great attention during the last years, and specialists from various professional spheres arise different questions concerning this theme. At the same time, there is a pool of questions, which do not have satisfying answers in spite of their frequent mentioning. In this paper, we present some reasoning connected with some of the most popular questions of that kind. In particular, we touch such problems as launching a national cryptocurrency and exploiting the blockchain technology in business sphere and governmental activities. We also analyze a commonly heard opinion that cryptocurrencies are, in fact, no more than the Ponzi scheme. Further, we briefly sketch the Bitcoin blockchain configuration and its stability if hypothetical quantum computer would be created.

*Cryptocurrency; distributed ledger; blockchain; bitcoin; etherium; national cryptocurrency; crypto-ruble; crypto-dollar; token; ponzi scheme; ICO*