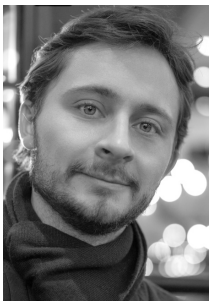
Перспективы интеграции теории игр и технологии блокчейн



С. А. Салтыков,
к. т. н., старший научный сотрудник
sergey.saltykov@gmail.com

Е. Ю. Русяева,
к. филос. н., старший научный сотрудник
1779624@mail.ru, rusyaeva@ipu.ru

Институт проблем управления им. В. А. Трапезникова РАН

Статья носит постановочный характер, в ней показано, что технология блокчейн и теоретико-игровое моделирование приоритетны друг для друга в плане дальнейшего развития. Обосновано, что игры с несовершенной информацией «покрывают» большую часть глубинных вызовов, стоящих перед блокчейн-технологией. Проанализированы всевозможные вызовы этой технологии и выделены главные из них. Для каждого из ключевых вызовов рассмотрено, в какой мере ответ на него связан с необходимостью создания новых научных результатов в некоторых разделах теории игр. Сделан вывод, что существенную часть глубинных вызовов блокчейна можно свести к теоретико-игровому проектированию ситуации многоагентного взаимодействия. В этом случае устанавливается консенсус пользователей блокчейн-системы относительно достоверности той или иной транзакции.

Ключевые слова: блокчейн, распределенные реестры, теория игр, установление консенсуса, децентрализация, масштабируемость, многоагентные системы.

Введение

В данной статье мы покажем, что технология блокчейн и теория игр приоритетны друг для друга. В подтверждение данного утверждения мы рассмотрим перспективы и возможности интеграции технологии блокчейн как одного из видов распределенных реестров, с некоторыми направлениями теории игр для их обоюдного развития. При анализе международных исследований по данной теме перед нами встал ряд вопросов.

С одной стороны, в некоторых работах говорится [1, 2], что блокчейн представляет собой синтез криптографии и теории игр. То есть авторы этих исследований считают, что если выделить две компоненты, наиболее существенно характеризующие блокчейн, то теория игр окажется среди них. Тогда получается, что роль теории игр в создании и развитии блокчейна чрезвычайно велика.

С другой стороны, имеется целый ряд научных работ, лидирующих, в том числе, среди исследований общего, обзорного характера в сервисе Гугл-академия, посвященных блокчейн-технологии в целом и вызовам, стоящим перед этой технологией. В них роль теории игр не упоминается вообще [3, 4] или упоминается лишь вскользь [2].

Таким образом, можно сделать вывод, что в настоящий момент у блокчейн-сообщества нет единого консенсусного мнения о роли теории игр в блокчейне. Но каково же истинное положение дел? Быть может, специалисты по исследованию операций намерено лоббируют роль теории игр, чтобы придать вес своим исследованиям, и реальная практика блокчейна прекрасно обходится без теоретико-игровых построений? Или же все наоборот, и блокчейн-индустрия отчаянно нуждается в прорывных идеях в теории игр? Эти прорывы могут стать залогом дальнейшего успешного стратегического развития блокчейн-индустрии, но пока рядовым блокчейн-программистам это сложно осознать, так как проблема коренится слишком глубоко? Каково детальное описание сути того, почему именно роль теории игр высока? Блокчейн-индустрия нуждается во всей теории игр в целом или в каких-то конкретных ее разделах и почему?

Попытаемся дать ответы на эти вопросы в нашем исследовании. Мы считаем, что для этого необходимо детально, не абстрагируясь от конкретных технических деталей, проанализировать глубинные вызовы, стоящие перед блокчейн-индустрией. Далее нужно показать, как именно с ответом на каждый из отдельных вызовов связана теория игр, в какой мере именно она помогает на него ответить. Еще раз подчеркнем,

что понимание технических нюансов даже, хотя бы, на принципиальном уровне, здесь необходимо для анализа: без них можно упустить самое важное. «Плоская», редукционистская картина может дать неверный ответ о роли теории игр. Поэтому в данной статье мы уделим особое внимание принципиально важным техническим деталям блокчейн-индустрии. По нашему мнению, таких детальных обоснований пока в литературе недостаточно. Например, в работе, где есть обзор вызовов [3], не выделяются главные среди них, а связь вызовов с теорией игр не указывается вообще. В других же работах есть указание на связь теории игр и блокчейна [2], но не обосновывается, в какой мере она присутствует. Кроме того, на связь блокчейна и теории игр указывается вне контекста всех стоящих вызовов перед индустрией. Такое указание выглядит как бы вырванным из контекста, и из него не ясны «пропорции» роли теории игр. В таких исследованиях может ощущаться некоторая предвзятость автора по отношению к теории, его необъективность. Чтобы избежать подобного, мы попытаемся протянуть целостную ниточку от тех внешних условий, в которых находится блокчейн-индустрия, и ее внутренних противоречий, динамизирующих ее развитие, к реальной роли новых результатов в теории игр в стратегическом развитии блокчейн-индустрии. Таким образом, определим, являются ли исследования по теории игр (и по каким именно ее разделам) приоритетными для развития такого важного элемента цифровой экономики как распределенные реестры вообще и блокчейн в частности.

Кроме того, в дополнение к главной теме статьи — как именно некоторые разделы теории игр могут помочь блокчейн-индустрии, рассмотрим органично (можно сказать, диалектически) связанную с ней тему. Покажем, как ориентация на развитие блокчейна может помочь самой теории игр выйти если не из кризиса, то из некоторого «застоя».

1. Блокчейн и теория игр: возможности интеграции

Одной из наиболее перспективных разновидностей современных электронных баз данных в эпоху больших данных (Big Date) становится распределенный реестр. Он является совокупностью равноправных копий баз данных о чем-либо. Децентрализованность, неиерархичность такого реестра — его принципиально важная характеристика, так как именно децентрализация, по мнению апологетов этой технологии, делает невозможной изменение и уничтожение данных в этом реестре злоумышленником.

Действительно, если система централизована, то для возможности манипулирования ею нужно «воздействовать» на центральное звено системы. Но если центрального звена нет, то злонамеренные изменения в любом отдельно взятом звене нивелируются, поскольку данные в такой системе копируются со всех других ее звеньев. Вот почему в децентрализованной системе нужно «захватить» большую ее часть, чтобы скомпроментировать данные. А если система велика, то взять под контроль большую ее часть может быть очень сложной и дорогой в осуществлении задачей. Таким образом, в принципе, у децентрализованных (распределенных) реестров большие перспективы.

Разумеется, все не так просто, и на практике реализация этих идей сталкивается с рядом сложностей, часть из них мы рассмотрим далее. Тем не менее, темпы развития этой технологии не снижаются. Более того, несмотря на все проблемы становления, технология распределенного реестра становится весьма приоритетной как в мире вообще, так и в России, в частности. О приоритетности развития распределенного реестра заявлено в программе «Цифровая экономика Российской Федерации», утвержденной в июле 2017 г. [5].

Цель данной статьи заключается в рассмотрении одного из видов реализации идеи распределенного реестра, технологии блокчейн, главным образом, в аспекте возможности ее интеграции с некоторыми направлениями теории игр для их обоюдного развития.

Блокчейн (от англ. blockchain — «цепочка блоков») представляет собой выстроенную по определенным правилам непрерывную последовательную цепочку блоков транзакций, содержащих некоторую информацию. Иначе говорят, что это «связный список» блоков транзакций. Копии цепочек блоков хранятся и обрабатываются независимо друг от друга на множестве разных компьютеров, т. е. представляют собой реплицированную (распределенную) базу данных [3]. Как отмечают исследователи [3], в настоящее время блокчейн-технология сталкивается с тремя основными вызовами: масштабируемость, безопасность и приватность.

Анализ обзора, приведенного в работе [4] о современных вызовах и ответах технологии блокчейн на базе 41 работы из авторитетных наукометрических баз показывает, что наиболее существенными вызовами для блокчейна являются, главным образом, необходимость установления консенсуса пользователей и масштабируемость.

В свою очередь, у теории игр тоже имеются нерешенные проблемы. Главные из них заключаются в том, что существующие формализмы, как математические, так и содержательные, описывающие многоагентное взаимодействие и внутреннюю логику поведения агента, пока весьма далеки от реальности [6]. К примеру, в классическом равновесии Нэша и его модификациях принимается не вполне реалистичное допущение о существовании только лишь общего знания, что уже не раз подвергалось критике [6, 7]. Вторая проблема после неполной адекватности математического аппарата реалиям многоагентного взаимодействия, второй глубинный вызов, стоящий перед аппаратом классических теоретико-игровых моделей — это отсутствие детализированной информации о реальном поведении агентов в многоагентных системах [6]. Для создания адекватных моделей необходимо собрать большое количество данных и о специфике протекания конкретных актов многоагентного взаимодействия, и о параметрах агентов разных групп и т. д. Именно отсутствие необходимой детальной информации и приводило к необоснованному разрастанию чрезмерно приближенных, крупноблочных теоретико-игровых моделей.

В этой же работе подчеркивается, что не все теоретико-игровые модели, особенно классические, удовлетворяют этим требованиям. Именно поэтому авторы исследования [6] обращают внимание на то, что при анализе процесса установления консенсуса в распределенных реестрах (в том числе и в блокчейне) стоит использовать повторяющиеся игры и игры с несовершенной информацией.

Раньше сбор необходимой детальной информации для создания адекватных моделей, к примеру, рефлексивных игр, тормозился отсутствием соответствующих технологических возможностей. Даже сейчас, несмотря на современную тенденцию к транспарентности, большинство социально-экономических систем остаются по-прежнему непрозрачными. Поэтому получить необходимый набор входных параметров для модели достаточно сложно, но постепенно именно технология блокчейн создает такие возможности. Также в [6] говорится, что релевантность теоретико-игровой модели реалиям блокчейна необходимое условие, но не достаточное. Авторы исследования [6] также отмечают, что требуется не только наличие всех критических параметров в модели в формализованном виде, но и правильная калибровка этих параметров. А для того, чтобы обеспечить такую калибровку, нужно проанализировать довольно большой набор данных о разных аспектах функционирования блокчейна: например, об использовании и производительности смарт-контрактов.

Таким образом, из работы [6] следует, что есть две ключевые задачи интеграции теории игр и блокчейна. Это развитие некоторых разделов теории игр с несовершенной информацией и калибровка теоретико-игровых моделей из этих разделов с использованием реальных данных функционирования распределенных реестров.

Исследователи осознают эти проблемы, и уже появляются новые интересные работы по анализу конкретных аспектов блокчейна теоретико-игровым аппаратом. Например, в статье [8] очень подробно и детально анализируются функционирование майнинговых пулов средствами кооперативной теории игр. Авторы приходят к выводу, что при любых стимулах игроки все равно заинтересованы переключаться между пулами.

Авторы работы, исследующей децентрализованный запуск смарт-контрактов [9] отмечают, что неполная рациональность пользователей блокчейна, вернее, учет их неполной рациональности, по-прежнему является открытой проблемой. Это еще раз говорит о том, что требуется создание соответствующего «неклассического» теоретико-игрового аппарата.

Из приведенного краткого анализа международных разработок видно, что многими исследователями отмечены возможные перспективы синтеза новых достижений в области теории игр с технологией блокчейн. Теоретико-игровое решение задачи установления консенсуса пользователей блокчейн-системы является ответом на многие вызовы, стоящие перед блокчейном.

Теперь необходимо определить, какая именно доля проблем блокчейна, малая или большая, упирается в теорию игр и почему именно? Действительно ли многие линии указанных проблем сходятся именно там? Какой именно раздел теории игр подойдет для разрешения проблем блокчейна и почему?

Для ответа на эти вопросы нам нужно детально, не редукционистски рассмотреть глубинные вызовы блокчейна и возможные ответы на них.

2. О технологии блокчейн

Все транзакции в блоках цепочки криптографически подписаны инициатором данной транзакции. Это означает следующее: у каждого пользователя блокчейн-системы есть два ключа — публичный (открытый) и приватный (закрытый). Приватный ключ известен только пользователю и не передается по сети, он позволяет подписывать содержимое транзакций, инициируемых пользователем. Проверить корректность подписи и, следовательно, неизменность транзакции может любой другой пользователь использованием публичного ключа инициатора транзакции, который доступен всем. Таким образом, любой может убедиться в том, что транзакция не была подделана, но изменить в ней ни бита информации не может, так как для подписывания измененной транзакции нужен никому, кроме пользователя, не известный приватный ключ.

Эти защищенные от изменения транзакции объединяются в блоки, а блоки, в свою очередь, в цепочки, причем таким образом, что каждый последующий блок содержит хеш-сумму (контрольную сумму) предыдущего блока. В этом случае, для того, чтобы изменить содержимое некоторого блока, надо изменить и все последующие за ним блоки. То есть, мы не только не можем от имени другого пользователя создать транзакцию (так как они криптографически подписаны), но даже не можем удалить имеющие транзакции из базы (это следствие объединения транзакций в блоки).

Объединяют транзакции, еще не участвующие ни в одном блоке, и объявляют их новым блоком так называемые «майнеры» — создатели блоков. Теоретически, майнер может выбрать любой из уже существующих блоков как родительский. Но практически имеет смысл выбирать лишь последний блок в самой длинной цепочке блоков (цепочка может ветвиться), так как именно самая длинная цепочка считается системой единственно валидной.

Кажется, к чему все эти сложности с разветвляющимися цепочками, почему нельзя сделать последовательность блоков единой? Роль транзакций и блоков понятна, а в чем функция ветвящейся цепочки блоков? Рассмотрим это более подробно.

Чтобы избежать централизации, которая, как отмечалось выше, рассматривается как угроза, нужно выбирать создателей блоков — майнеров — максимально случайно из большого числа не аффилированных претендентов.

Для организации случайного выбора в условиях децентрализованной сети используется пересчет хеш-суммы блока, удовлетворяющей некоторому условию (это также будет рассмотрено далее). Кто первым подо-

брал нужное значение этой суммы, тот получает право сформировать блок и получает вознаграждение.

Из-за задержек репликации в децентрализованной сети может получиться так, что несколько пользователей создали почти одновременно блоки, имеющие родительским один и тот же блок. Так что ветвление — «неизбежное зло» в условиях совершенной децентрализации. Но если блоки, содержащие частично одни и те же транзакции, организованы в разветвленную цепочку, то, как определить, какая цепочка является «правильной»?

Действительно, определять самым очевидным способом — по времени создания блока — не получится. Внутри децентрализованной базы нет ничего, чтобы могло поверить правильность простановки времени, ведь никак нельзя убедиться, что временная отметка не подделана. Поэтому транзакции в новом блоке не считаются подтвержденными. Они будут считаться таковыми, когда над блоком будет надстроено еще несколько блоков.

Майнеры самостоятельно выберут, какой из альтернативных блоков считать родительским для своих блоков, и через какое-то время вновь окажется единственная самая длинная цепочка блоков. Она и будет считаться валидной. Ветвящаяся цепочка как таковая — это лишь следствие одного из вариантов организации случайного выбора пользователя-верификатора, а не неотъемлемая часть любого распределенного реестра. То есть, три «этажа» — транзакция, блок, цепочка — не являются обязательными для любого распределенного реестра. Это лишь один из вариантов архитектуры данной системы, которая, собственно, и называется блокчейном. Другим возможным вариантом является архитектура из двух «этажей» — «транзакция — последний вариант реестра транзакций». Обе эти архитектуры призваны, в идеале, обеспечивать децентрализованную работу с транзакциями со всеми «плюсами», которые следуют из децентрализации. Данные в децентрализованной системе, в теории, нельзя не санкционированно изменить или удалить. Однако, так будет, если обеспечить «идеальную» децентрализацию. Но в реальности вышеуказанные архитектуры сталкиваются с разного рода сложностями при попытке создать полную децентрализацию.

Рассмотрим эти проблемы, их глубинные основания, а также возможные пути их решения.

3. Ключевые проблемы, вызовы технологии блокчейн

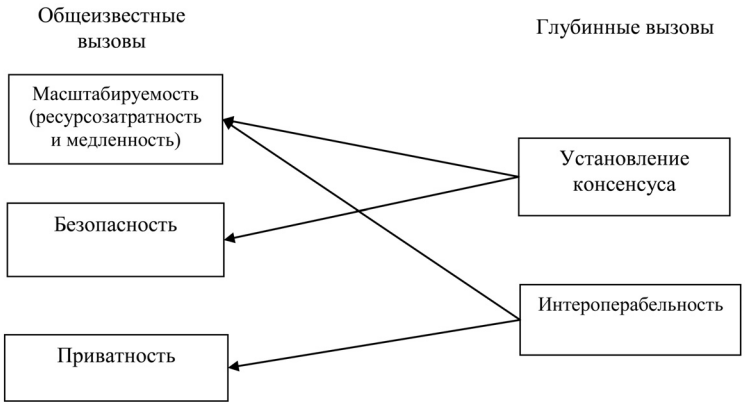
По мнению Виталика Бутерина, создателя платформы эфириум, в настоящее время блокчейн сталкивается с тремя основными вызовами: масштабируемость, безопасность и приватность [3]. Покажем, что проблемы с масштабируемостью во многом проистекают из потребности в интероперабельности блокчейнов и несовершенств наиболее часто применяемого способа верификации транзакций — proof-of-work. В свою очередь, вопросы к безопасности блокчейнов также во многом обусловлены этим способом верификации транзакций: он является причиной того, что лежит на поверхности и часто обсуждается. Это угрозы централизации блокчейна и, как следствие, переписывание его транзакций, атаки «двойная трата» и т. д.

То есть в данном разделе мы обоснуем, что если присмотреться к деталям, вызовы масштабируемости и безопасности тесно связаны между собой. Также они во многом детерминированы необходимостью решения вопросов взаимодействия блокчейнов друг с другом и проектирования новых, более совершенных способов верификации транзакций в блокчейне [3]. В этом смысле вызов приватности стоит несколько особняком, однако, как мы покажем далее, он тоже тесно связан с масштабируемостью.

Подробно рассмотрим два «общеизвестных» вызова, масштабируемость и безопасность, и лежащие за ними «глубинные» вызовы (рисунок). Также проанализируем и вызов приватности, причем, главным образом, в том аспекте, в каком он связан с двумя указанными нами «глубинными» вызовами.

3.1. Вызов масштабируемости. Ресурсозатратность

Рассмотрим вызов масштабируемости. Его суть в том, что сейчас транзакции зачастую подтверждаются слишком долго. Общее число транзакций, которые могут быть записаны в блокчейн в единицу времени, недостаточно для того, чтобы этим конкретным блокчейном пользовались миллионы пользователей. Также на данный момент неоправданно велики затраты электроэнергии на майнинг (производство) блоков цепочки транзакций.



Вызовы для блокчейна

Если попытаться существенную часть процессов жизни общества, как часто говорится в рекламных слоганах, «перевести на блокчейн», то блокчейн-платформа просто не сможет функционировать. Транзакции будут осуществляться неприемлемо медленно, очередь на верификацию транзакций будет быстро расти, а комиссии за их проведение будут неприемлемо высокими. Кроме того, затраты электроэнергии будут просто несоразмерными общественной пользе, приносимой таким блокчейном. Уже сейчас, к примеру, сеть биткоина потребляет больше электроэнергии, чем некоторые страны. И это при том, что биткоин еще не успел стать не только общепринятой блокчейн-платформой, но и даже адекватным средством осуществления платежей.

В чем одна из главных причин этих проблем? Она кроется во многом в самом часто используемом способе верификации транзакций — proof-of-work («доказательство работы»). При такой верификации блоки, размещаемые в цепочке блоков, «майнятся», т. е. «добываются». При этом многократно для чуть измененного несущественной информацией блока пересчитывается значение хеш-функции, пока оно не станет меньше некоторого значения. Грубо говоря, делается большой объем «бессмысленных» вычислений, главная цель которых — случайный выбор того, кто верифицирует транзакцию.

Но случайность выбора майнера нужна для того, чтобы избежать централизации сети. Если большая часть вычислительных мощностей будет принадлежать одному игроку, он сможет не только верифицировать именно те транзакции, какие захочет, но сможет и переписать главную цепочку блокчейна, и осуществить «двойную трату». То есть такой игрок сможет отменить свою транзакцию, где тратятся средства, а затем снова эти же средства потратить на что-то еще. Одним словом, такая полная централизация была бы крахом для блокчейн-платформы. И случайность выбора майнеров, верифицирующих транзакции, в условиях «псевдонимности» транзакций — это способ избежать подобного краха.

Изначально идея доказательства работы как способа выбора майнера была прорывной и весьма эффективно работала в сети биткоина. Но примерно через десятилетие майнинг уперся в свой технологически обусловленный потолок. С ростом вычислительных мощностей сети сложность задачи по подбору хеша все увеличивается (так как нужно подбирать меньший хеш), а энергозатраты растут. Чтобы покрыть эти затраты, майнеры увеличивают комиссии транзакций, а при меньших комиссиях перевод денег может идти несколько дней и больше.

Кроме того, из-за роста вычислительной сложности майнинга обычным пользователям персональных компьютеров больше не выгодно участвовать в майнинге, и его сейчас осуществляют несколько очень крупных пулов (объединений) майнеров. А это приводит к угрозе централизации сети со всеми вытекающими последствиями.

По иронии судьбы, майнинг, придуманный специально для того, чтобы избежать централизации, к ней же и привел, в конечном счете. В этом аспекте становится понятно, что «косметические» изменения вроде увеличения размера блока и вынесения части информации за пределы блокчейна не решат проблемы, поскольку она коренится в самой природе майнинга.

Каким может быть адекватный ответ на такой вызов? Рассмотрим его далее, а пока продолжим рассмотрение вызова масштабируемости.

3.2. Вызов масштабируемости. Интероперабельность

Другой аспект проблем масштабируемости связан с интероперабельностью блокчейнов, т. е. с возможностью их эффективного взаимодействия. Здесь вопрос ставится так: или будет один-единственный блокчейн, победивший в конкурентной борьбе и ставший блокчейн-платформой по умолчанию для цифровизации всех сторон жизни, или же будет большое множество блокчейнов различного назначения, между которыми необходимо осуществлять взаимодействие.

И здравый смысл, и опыт IT-индустрии подсказывает, что один блокчейн для всех и всего — это из области фантастики: в интернете ведь тоже нет ни то, что единственного сайта, но и даже полностью доминирующей компании. Следовательно, рано или поздно придется разным блокчейнам «общаться» друг с другом. И это необходимое условие для успешного масштабирования.

3.3.Вызов безопасности

Перейдем к вызову безопасности. Главная опасность для блокчейна заключается в возможности его захвата злоумышленниками, и считается, что захватить централизованную сеть легче, чем децентрализованную. То, что опасность централизации проистекает из самой природы майнинга, было показано выше. Более того, если мы устраним эту уязвимость и изменим способ верификации транзакций на «доказательство доли» (подробнее это будет рассмотрено далее), то одни проблемы безопасности сменятся на другие: при использовании proof-of-stake сеть подвержена атаке «ничего на кону». То есть неправильный выбор не только самого способа верификации транзакций, но и даже его параметров будет серьезной угрозой безопасности. Поэтому вывод безопасности блокчейн-платформ на новый уровень во многом обусловлен конструированием эффективного способа верификации транзакций.

Таким образом, два «глубинных» вызова, которые мы будем рассматривать дальше — это необходимость обеспечения интероперабельности блокчейнов и конструирование более эффективного способов верификации транзакций.

3.4. Вызов приватности

Рассмотрим третий «общеизвестный» вызов — приватность. По мысли создателей технологии блокчейна, «идеальный» блокчейн должен сочетать в себе открытость и приватность. Но очевидно, что это противоречивое требование нельзя выполнить полностью, до конца. Ясно, что часть информации более нуждается в приватности, другая менее. Как обеспечить

должную приватность при сохранении открытости распределенного реестра хотя бы на принципиальном уровне, пока не до конца ясно. Но идея в том, чтобы сконструировать должным образом интероперабельность блокчейнов. Это и будет глубинным вызовом, к которому сводится вызов приватности.

4. Ответы на глубинные вызовы блокчейна

4.1. Ответ на вызов масштабируемости

Потребность в масштабируемости вообще и возможность интероперабельности блокчейна в частности может обеспечить технология шардинга (от англ. «shard» — осколок), которая заключается в организации работы иерархически упорядоченной совокупности блокчейнов разного типа и назначения. При этом в такой иерархии есть корневой блокчейн.

Идея и перспектива развития шардинга заключается в том, что здесь как бы копируется структура многих социальных институтов общества. В этой аналогии корневой блокчейн играет роль суда, а дочерние блокчейны содержат информацию об операционной деятельности.

Мы видим, что в ходе естественного развития архитектуры в блокчейн-технологии появляются делегирование и многоэтажность, не получается избавиться от узлов-посредников. Это происходит из-за того, что те узлы-посредники, которые системно необходимы для функционирования в реальном мире, оказываются системно необходимы и в мире блокчейна. Таким образом, мы воссоздаем иерархически упорядоченную систему социальных институтов, однако добавляем обязательность и прозрачность выполнения контрактов. Это не получается сделать в реальном мире из-за «человеческого, слишком человеческого». То есть лозунги редукционистов оказались несостоятельными: избавиться от системной сложности мира не получается, а вот уменьшить влияние человеческого фактора вполне реально [10].

Уже появляются конкретные реализации идеи шардинга, например, Plasma [11] — это шардинг-платформа от эфириум, т. е. в корне иерархии блокчейнов в этом случае будет эфириум.

4.2. Ответ на вызов способа установления консенсуса

Ответом на второй «глубинный» вызов необходимости конструирования способа установление консенсуса, может стать proof-of-stake («доказательство доли»).

Этот вариант существенно менее энергозатратный, чем proof-of-work и гораздо более быстрый и масштабируемый. С одной стороны, он меньше подвержен угрозе «ползучей» централизации крупными пулами майнеров. Но, с другой стороны, избегая одной угрозы, этот тип установления консенсуса привносит новые проблемы. Работа валидаторов на разных концах цепочки тоже может привести к централизации. То есть одна угроза централизации заменяется на другую, и какая из них меньшее зло пока не ясно. Однако разница состоит в том, что у proof-of-stake есть шанс быть доработанным так, чтобы избежать этой угрозы, а у proof-of-work — нет. Задача состоит в том, чтобы подобрать параметры реализации proof-of-stake таким образом, чтобы сохранить преимущества и избежать угроз. На практике это не так-то легко сделать. Поэтому существующие реализации proof-of-stake вынуждены чем-то поступаться: большинство имеющихся вариантов, не являющихся proof-of-work (т. е. proof-of-stake и другие), так или иначе частично централизованы. В блокчейн-сообществе это воспринимается однозначно как негативный момент, поэтому блокчейн-разработчики по возможности вуалируют это. Однако, так как протоколы открыты, блокчейн-энтузиасты все равно докапываются до сути. Например, было показано, что консенсус сети Ripple несколько централизован [12] также, как и верификация транзакций в системе IOTA [13].

Насколько сам факт частичной централизации опасен для блокчейн-индустрии? И можно ли совсем избавиться от централизации, оставив при этом возможность для масштабирования?

4.3. Взаимоусиливающее влияние шардинга и proof-of-stake

Идеология шардинга позволяет по-новому взглянуть на необходимость частично централизованной балансировки блокчейн-системы: можно предположить, что такие функции центра-балансировщика может на себя взять корневой блокчейн. Это позволит пересмотреть отношение, в частности, к способу установления консенсуса в сети Ripple, который в профессиональном сообществе критиковали за некоторую централизованность протокола [12]. В этой связи уже не кажется странным, что многие идеи разрабатываемого консенсуса Casper в эфириум очень похожи на консенсус Ripple. Среди них такие, как: установление консенсуса в несколько раундов, формирование валидируемых наборов транзакций не самим валидатором, а другими узлами сети, а также защита от изменений последнего подтвержденного реестра. То есть к примеру, мы принимаем волевое решение, что реорганизация возможна только до какого-то n-го блока вглубь. Мы не можем закрыть от реорганизации весь блокчейн, так как есть вероятность, что несколько последних блоков верифицировали мошенники, и их нужно реорганизовать. Но при этом мы не можем позволить и реорганизацию всех блоков блокчейна, так как в случае proof-of-stake есть проблема — «ничего на кону» (nothing-on-stake). Она приводит к тому, что валидаторам выгодно работать на нескольких концах цепочки блокчейна, что приводит к ветвлению. Поэтому предлагается некое компромиссное решение — закрывать от реорганизации большую часть блокчейна.

Новый взгляд на частичную централизацию, необходимую при реализации proof-of-stake в контексте шардинга, позволяет по-новому ставить задачи о конструировании конкретной реализации proof-of-stake. При конструировании способа установления консенсуса для дочерних блокчейнов при шардинге уже нет необходимости требовать полной децентрализации. Здесь необходимые функции централизованной

балансировки дочернего блокчейна можно доверить корневому блокчейну [14].

Так, для дочерних блокчейнов нет необходимости предъявлять весь набор требований к способу установления консенсуса. Разные типы дочерних блокчейнов, по-видимому, будет нуждаться в разных способах установления консенсуса. Также можно предположить, что способы установления консенсуса для частных и публичных блокчейнов будут различны [14, 15].

Ведущие блокчейн-разработчики утверждают, что важную роль в этом конструировании может сыграть теория игр [1, 6, 8].

4.4. Ответ на вызов приватности

Ранее мы указывали, что вызов приватности во многом сводится к глубинному вызову необходимости обеспечения взаимодействия блокчейнов между собой, также отмечали, что эту интероперабельность блокчейнов позволит обеспечить идеология шардинга (иерархической организации блокчейнов). То есть иерархизация блокчейнов и есть ответ на существенную долю вызова приватности. Многим крупным субъектам экономики, таким как государства, крупные корпорации придется создавать свой блокчейн, который будет укоренен, к примеру, в эфириум [3]. Например, у банка может быть приватный, частный блокчейн, а у банковской системы в целом может быть публичный блокчейн. В перспективе это может привести к существенному снижению трансакционных издержек и увеличить число транзакций и хотя бы отчасти устранить пока неконтролируемый человеческий фактор.

Такое решение — комбинация приватных и публичных блокчейнов, в том числе в иерархии блокчейнов при шардинге — позволяет частично решить проблему приватности, оставив без корректировки главное системное качество блокчейна — открытость реестра. Так противоречие между приватностью и публичностью будет частично снято.

5. К вопросу о проблемах классической теории игр и возможных решениях этих проблем

У классической теории игр есть свои, пока не решенные проблемы. Здесь мы затронем лишь те из них, решением которых может служить блокчейн.

Как уже отмечалось, ключевая проблема, глубинный вызов, стоящий перед аппаратом классических теоретико-игровых моделей, состоит в отсутствии детализированной информации о реальном поведении агентов в многоагентных системах. Для создания адекватных моделей необходимо собрать большое количество данных и о специфике протекания конкретных актов многоагентного взаимодействия, и о параметрах агентов разных групп и т. д. Ведь, как отмечалось в [7], именно отсутствие необходимой детальной информации и приводило к необоснованному разрастанию чрезмерно приближенных, крупноблочных теоретико-игровых моделей.

Раньше сбор такой информации тормозился отсутствием соответствующих технологических возможностей. Например, в классической теории игр принималось допущение о наличии общего знания у игроков. Но это применимо лишь к очень крупным институциализированным игрокам, типа участников холодной войны и транснациональных корпораций. Только в подобных случаях можно предположить, что, скорее всего, есть общее знание обо всех параметрах ситуации и о том принципе оптимальности, который будет выбран игроками. Но для описания всех остальных общественных процессов, в которых заведомо не участвуют супер аналитики, использующие суперкомпьютеры, теория игр, в большинстве случаев, адекватно применена быть не могла. Кроме того, даже в условиях адекватных представлений об информированности агентов и выбираемых ими принципах оптимальности, идентифицировать, какая именно информированность у данных конкретных агентов, достаточно сложно в первую очередь из-за информационной непрозрачности.

Получается, что ранее теоретико-игровые модели создавались, чаще всего, как некие абстрактные, оторванные от жизни «умозрительные» теории, которые, возможно, обладали математической красотой, но содержали в себе неустранимые, слишком ограничительные допущения. Поэтому такие теории не только не соответствовали реальности, но и вряд ли могли бы ей соответствовать даже в перспективе [7].

Также, несмотря на современную тенденцию к открытым данным, большинство социально-экономических систем по-прежнему остаются довольно непрозрачными, и получить необходимый набор входных параметров для модели достаточно сложно. И в этом аспекте, в разрешении этой проблемы и может помочь технология блокчейн.

Как показывает приведенный анализ, именно в интеграции с блокчейн-технологией у теоретико-игровых моделей появляется шанс стать более применимыми к реальности. Также и блокчейн, в свою очередь, может получить шанс сконструировать эффективный мало манипулируемый способ установления консенсуса.

У теоретико-игровых моделей с несовершенной информацией появляется шанс перейти от декларативно-прикладной и условно-прикладной стадии науки к прикладной благодаря тому, что блокчейн-технология позволяет идентифицировать значения необходимых входных параметров модели, тем самым сделать модель более адекватной реальности [7]. В этом случае, потребности теории игр в развитии и потребность блокчейн-технологии в масштабируемости и безопасности, сходятся, и дают как раз ту необходимую надежду на плодотворный синтез.

Кроме того, можно рассматривать создание своих правил игры для дочернего блокчейна каждого типа как постановку отдельной теоретико-игровой задачи. При этом, в совокупности решения этих задач, получается хорошее, обширное «место делания науки» [16].

Заключение

В данной статье мы показали, что потребность блокчейн-индустрии в масштабируемости и безопасности, сводится во многом к необходимости установления консенсуса [3]. А этого можно добиться с помощью применения теоретико-игровых моделей. Тем

самым, можно говорить о том, что теория игр является тематическим приоритетом для развития технологии блокчейна как открытого распределенного реестра. Показано, что необходимость получения новых результатов в играх с несовершенной информацией «покрывает» большую часть глубинных вызовов, стоящих перед блокчейн-технологией. Для обоснования этого положения проанализированы всевозможные вызовы и выделены главные из них. Для каждого из ключевых вызовов рассмотрено, в какой мере ответ на него связан с необходимостью создания новых научных результатов в некоторых разделах теории игр.

На основе проведенного детального анализа, можно сделать вывод: технология блокчейн и теоретико-игровое моделирование нуждаются друг в друге для дальнейшего развития. Теория игр может позволить блокчейну ответить на главные вызовы, стоящие перед ним, а именно, обеспечить масштабируемость и установление консенсуса. А блокчейн, в свою очередь, предоставляет для теории игр достаточно высокоструктурированную среду для анализа, оптимально релевантную реальным процессам взаимодействия людей и общественных институтов.

Ориентация на блокчейн, образно говоря, позволяет теории игр пройти между Сциллой и Харибдой. С одной стороны, не быть полностью оторванной от реалий сложной многопараметрической жизни. С другой, за обилием конкретных деталей можно выявлять общесистемные закономерности реального многоагентного взаимодействия. Но нужно уточнить, что интеграция блокчейн-технологии в целом с теорией игр вообще представляется не вполне целесообразной. А вот интеграция отдельных разделов теории игр и отдельных аспектов технологии блокчейн вполне продуктивна. Здесь была представлена возможность именно такого рассмотрения вопросов интеграции. Поясним почему. Это касается также вопроса о доказательности положений статьи в формате формализованного знания, которое будет представлено в дальнейших исследованиях.

Дело в том, что математическую модель можно сопоставить только очень узкому аспекту функционирования технологии блокчейн. Например, важным аспектом блокчейн-технологии является майнинг, а отдельным аспектом майнинга является феномен майнинговых пулов. Майнинговым пулам как аспектам блокчейн-технологии, можно сопоставить некую теоретико-игровую модель [8]. Также важным аспектом блокчейна являются смарт-контракты, с ними связано много различных вопросов, в частности, их выполнение. Выполнение смарт-контакта — это тоже достаточно узкий аспект блокчейн-технологии, которому можно сопоставить отдельную теоретико-игровую модель [9]. И таких узких аспектов можно выделить несколько десятков, а то и больше. Теоретико-игровое описание каждого из таких аспектов — предмет отдельного исследования. В следующих публикациях будет представлена формальная постановка одной из таких задач.

Список использованных источников

1. C. Catalini (MIT), J. S. Gans (University of Toronto) Some Simple Economics of the Blockchain. http://www.cauchyinvestments.com/wp-content/uploads/2018/01/Some-Simple-Economics-of-the-Blockchain.pdf.
2. The future of cryptocurrencies: Bitcoin and beyond. https://www.nature.com/news/the-future-of-cryptocurrencies-bitcoin-and-beyond-1.18447.
3. А. Генкин, А. Михеев. Блокчейн: Как это работает и что ждет нас завтра. М.: Альпина Паблишер, 2018. 282 с.
4. Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi , Sooyong Park, Kari Smolander. Where Is Current Research on Blockchain Technology?—A Systematic Review. http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477.
5. Программа «Цифровая экономика Российской Федерации» утверждена распоряжением Правительства РФ от 28 июля 2017 г. № 1632. http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf.
6. G. Bigi, A. Bracciali, G. Meacci, E. Tuosto. Validation of Decentralised Smart Contracts through Game Theory and Formal Method. http://storre.stir.ac.uk/bitstream/1893/23914/1/bHalo_Degano2015.pdf.
7. Е. Ю. Русяева, С. А. Салтыков. Концептуальные основы теории активных систем, их развитие в теории управления организационными системами: тенденции и перспективы//Проблемы управления. 2017. № 4. С. 74-83.
8. Yoad Lewenberg, Yoram Bachrach, Yonatan Sompolinsky, Aviv Zohar, Jeffrey S. Rosensche. Bitcoin Mining Pools: A Cooperative Game Theoretic Analysis. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.695.9873&rep=rep1&type=pdf.
9. Lin Chen, Lei Xu, Nolan Shah, Zhimin Gao, Yang Lu, and Weidong Shi. Decentralized Execution of Smart Contracts: Agent Model Perspective and Its Implications. http://fc17.ifca.ai/wtsc/Decentralized%20Execution%20of%20Smart%20Contracts%20-%20Agent%20Model%20Perspective%20and%20Its%20Implications.pdf.
10. М. М. Пряников, А. В. Чугунов. Блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы. Киберленинка. https://cyberleninka.ru/article/n/blokcheyn-kak-kommunikatsionnaya-osnova-formirovaniya-tsifrovoy-ekonomiki-preimuschestva-i-problemy.
11. Salvation From Cryptokitties Draws Near: Plasma AntiCataclysm. Open source PROOF-OF-ASSET protocol to facilitate. https://blog.bankex.org/salvation-from-cryptokitties-draws-near-plasma-anticataclysm-679adb2c1738.
12. Peter Todd. Ripple Protocol Consensus Algorithm Review. May 11th 2015. https://raw.githubusercontent.com/petertodd/ripple-consensu....pdf.
13. Eric Wall. IOTA is centralized. Jun 14, 2017. https://medium.com/@ercwl/iota-is-centralized-6289246e7b4d.
14. John-David Lovelock , Martin Reynolds, Bianca Francesca Granetto, Rajesh Kandaswamy. Forecast: Blockchain Business Value, Worldwide, 2017-2030.

Published: 02 March 2017. https://www.gartner.com/doc/3627117/forecast-blockchain-business-value-worldwide.

15. Proof-of-Work vs. Proof-of-Stake: как изменится Ethereum. https://ru.insider.pro/tutorials/2017-07-14/proof-work-vs-proof-stake-kak-izmenitsya-ethereum.
16. С. А. Салтыков, Е. Ю. Русяева. Рафинирование научных построений в теориях принятия решений. М.: ИПУ РАН, 2016. 208 с.

Prospects of integration of game theory and blockchain technology

S. A. Saltykov, candidate of technical sciences, senior researcher.

E. Yu. Rusyaeva, candidate of sciences (philosophy), senior researcher.

(V. A. Trapeznikov Institute of control sciences of Russian academy of sciences)

The article is staged, it shows that the blockchain technology and game-theoretic modeling are priorities for each other in terms of further development. It is justified that games with imperfect information «cover» most of the deep-seated challenges facing blockchain technology. All possible challenges of this technology are analyzed and the main ones are identified. For each of the key challenges, it is considered to what extent the answer to it is related to the need to create new scientific results in some sections of game theory. It is concluded that an essential part of the deep-seated calls of the detachment can be reduced to a game-theoretic design of the multi-agent interaction situation. In this case, a consensus is established between users of the blockchain system on the reliability of a particular transaction.

Keywords: a blockchain, the distributed ledgers, game theory, establishment of consensus, decentralization, scalability, multi-agent systems.