УДК 330.47:519.688 doi: http://doi.org/10.15407/econindustry 2019.01.082

Денис Владимирович Липницкий,
канд. экон. наук
архитектор приложений, технический тренер IBM
i-Klass Center LLC.
E-mail: denis.lipnitsky@i-klass.com
https://orcid.org/0000-0002-4616-7936

ВОЗМОЖНОСТИ И ВЫЗОВЫ ДЛЯ БЛОКЧЕЙН В НОВОЙ ИНДУСТРИАЛИЗАЦИИ

Индустрия 4.0 включает создание киберфизических систем, способных децентрализованно управлять производством, продажами, самообучаться и развиваться. Функционирование таких систем нуждается в аналогичных "умных" технологиях хранения и распространения информации. Блокчейн, обеспечивший децентрализацию и кибербезопасность в сфере криптовалют и создавший "умные" контракты, стал рассматриваться как подобная технология. Однако экстраполяция блокчейн с узкой сферы цифровых денег до универсального применения в индустрии и публичном секторе столкнулась с серьезными трудностями. Некоторые из них могут быть преодолены в рамках существующего поколения блокчейн (например, улучшением алгоритмов консенсуса). Большинство же требует существенных трансформаций технологии, комбинирования ее с другими информационными и промышленными инновациями. Трудности такого переходного этапа породили критику блокчейн и, нередко, отказ от его использования. Появились гибридные решения, взявшие от блокчейн лишь часть инновационной идеи (блочную организацию реестра транзакций) и имплантировав ее в традиционные технологии. Предложено считать такие решения неполноценным "квазиблокчейном". На основе анализа эволюции блокчейна обосновано, что дальнейшее развитие его децентрализованных версий наиболее отвечает концепции Индустрия 4.0. Показано, что внедрению таких версий сейчас препятствуют внутренние противоречия: "трилемма" блокчейн плюс его высокая энергоемкость. Исследованы перспективы выхода из тупика "трилеммы" блокчейн с помощью смежных инновационных решений, таких как протокол второго уровня (Lightning Network) и ему подобные. Освещены тенденции дальнейшего развития различных форм и архитектур блокчейн. Предложена классификация, связывающая блокчейн с традиционными распределенными базами данных и учитывающая логику их развития. Проанализированы эффективные методы промышленного внедрения блокчейн, включая реализацию с его помощью цифровых счетов-фактур (e-Invoice) и коммуникаций для промышленного Интернета вещей. Выполненные исследования позволили разработать критерии выбора и оптимизации конкретных блокчейн-решений для индустриального применения.

Ключевые слова: блокчейн, Индустрия 4.0, распределенный реестр транзакций, децентрализация, "трилемма" блокчейн, "умные" контракты, алгоритмы консенсуса, e-Invoice, Интернет вещей, кибербезопасность.

Развитие современной "умной" промышленности (смарт-индустрии, Индустрии 4.0) основано на новых цифровых технологиях, видное место среди которых занимает блокчейн. Но не всё происходящее в сфере новейших компьютерных разработок оценивается однозначно. Рынки наполнены информационными продуктами, представленными как технологический прорыв. Однако есть повод сомневаться в реальной инновационности отдельных достижений. Не являются ли они лишь красивой маркетинговой обёрткой для банальных технических идей? Может быть, эф-

фект от подобных "инноваций" не столь существенен, как его преподносят (технологии "плацебо")? Это та известная проблема эффективности компьютерных технологий, о которой писал ещё Р. Солоу [1].

Данные сомнения в полной мере относятся к блокчейн (строго говоря, группе технологий, но в дальнейшем – просто технологии), алгоритмический аппарат которой по большей части существовал за десятки лет до того, как был "переизобретён" создателями биткоина (Bitcoin). Своим выходом из математических дебрей на сцену живой экономики блокчейн обязан росту вычислительных возможностей компьютеров и глобализации интернета, позволяющего при желании создать мгновенный спрос где угодно и на что угодно. Экспертные мнения относительно будущего этой технологии разнятся от восторженных до весьма сдержанных.

Э. Шмидт (генеральный директор Google) однозначно охарактеризовал блестящие перспективы блокчейн и биткоина: "Биткоин – замечательное достижение в области криптографии, и его способность создать то, что невозможно дублировать (подделать) в цифровом мире, имеет огромное значение… Множество людей построят бизнес на его основе" [2].

К. Лагард (директор-распорядитель Международного валютного фонда), поддерживая в целом идею криптовалют, выражает беспокойство из-за энергетической неэффективности первых генераций блокчейн, заявляя, что "Майнинг биткойнов – это зло для энергетики... Климат необратимо меняется, а мы лишь наблюдаем за тем, сколько угля использует Китай для майнинга биткойнов" [3].

П. Кругман (нобелевский лауреат по экономике) вообще не видит прогресса в появлении криптовалют. По его мнению, "Энтузиасты криптовалют при помощи передовой технологии пытаются отправить денежную систему на 300 лет назад". Вместо того чтобы снижать транзакционные издержки, биткоин требует непрерывно наращивать расходы на содержание лежащей в его основе блокчейн-системы в адекватном состоянии: "Высокая стоимость создания нового биткоина или передачи уже существующего необходима для того, чтобы в децентрализованной системе существовало доверие" [4].

Критики стало больше после того, как в 2018 г. лопнул спекулятивный "пузырь" криптовалют, бросив тень на блокчейн. На фоне взлетов и падений цифровых денег и бума стартапов гораздо скромнее выглядят новости о достижениях блокчейн в областях, где ему изначально пророчили блестящее будущее: реформирование государственных органов, противодействие уклонению от уплаты налогов и оптимизация бизнес-операций. Развитие блокчейн здесь протекает намного медленнее, чем в сфере криптовалют, и сталкивается с множеством препятствий, в том числе исходящих из ядра самой технологии (еще недостаточно зрелой).

Некоторые авторы идут дальше критики криптовалют и ставят под сомнение перспективы технологии блокчейн как таковой. Как яркий пример, К. Стинчкомб (основатель и руководитель компании True Link Financial) выступил с резким осуждением, заявляя, что от технологии, не реализовавшей себя за все прошедшее десятилетие нигде, кроме "песочницы" энтузиастов и неоднозначных цифровых валют, не стоит ожидать серьёзных достижений и в будущем [5].

Очевидно, что амбициозный проект перехода блокчейн от криптовалютной к генерализованной технологии привел к созданию множества ее поколений, причём зачастую в виде незавершённых разработок и конкурирующих версий, и породил не меньше затруднений и ошибок. Все это осложняет понимание предмета. Поэтому как абсолютно позитивные (звучащие обычно от заинтересованных лиц), так и уничижительные оценки грешат односторонностью.

Исследуемая в настоящей работе проблема заключается в принципиальной возможности и готовности блокчейн в нынешнем виде к использованию в реальном секторе экономики при наступлении чет-

вертой промышленной революции. Для ее решения выполнен всесторонний анализ базовых элементов технологии, ее характеристик, способствующих и препятствующих широкомасштабному применению. Изучены эволюция блокчейн, современное состояние и перспективные разработки, направленные на преодоление ограничений технологи, оценено влияние блокчейн на другие промышленные инновации.

Цель статьи − продемонстрировать, что блокчейн имеет потенциал инновационности и ресурсы, необходимые для современной индустрии. Однако содержатся они не в достижениях криптографии 70-80-х годов прошлого века, нашедших воплощение в биткоине и ему подобных (для асимметричного шифрования блокчейн − лишь одна из сфер применения). Будет показано, что блокчейн стал в значительной степени ребрендингом для распределённых вычислений, превратив их из области изучения компьютерной науки в элемент либеральной экономической идеологии. Такое распространение концепций с технической сферы на экономику породило цепную реакцию исследований и разработок, не всем из которых суждено стать полезными.

Блокчейн продвигается адептами как высокотехнологичный инструмент, приносящий, благодаря своей распределенной сути (как высшей степени децентрализации), новые свободы рынку. На его примере демонстрируется, что самоорганизация бизнеса проще и выгоднее, чем существование центрального органа – "большого брата", владеющего монополией на координацию экономической жизни.

Группа экспертов, в частности С. Дэвидсон (профессор институциональной экономики Австралийского и международного университета RMIT) и П. де Филиппи (исследователь Парижского Национального центра научных исследований CNRS) считают, что блокчейн способен вызвать трансформацию институтов, увеличивая мобильность экономических агентов, ускоряя и защищая транзакции, снижая сопутствующие издержки [6]. Э. де Сото (основатель и президент Института свободы и демократии) утверждает, что "...Правительства, которые переводят свои реестры собственности на систему, основанную на блокчейн, могут создать более прозрачную и понятную систему, которая в конечном итоге принесет пользу людям и предоставит новые экономические возможности для всех" [7].

Независимо от того, разделяют они либеральную философию блокчейн или нет, множество экономистов считают соблазнительной саму идею переложить важные институциональные функции с живой и небезупречной бюрократии на обезличенную запрограммированную машину, которой по сути является блокчейн. Однако, как и всеобщая роботизация, такое решение содержит множество сложностей и рисков, требующих осмысления. А начать следует с фундаментального понимания технологии, изучения ее версий, их сильных и слабых сторон, на чем остановимся более подробно.

В отличие от глобальной "блокчейнизации" – мечты футурологов, те версии блокчейн, которые уже используются в решении локальных задач бизнеса (цепочек поставок, в частности), выглядят менее революционно (и менее инновационно). Такой блокчейн и по идеологии, и по технологии отличатся от его приложений в сфере майнинга, эмиссии и обмена цифровых валют.

Будет показано, что предлагаемые для промышленности системы часто базируются на ограниченной децентрализации или даже централизованной (нераспределенной) архитектуре. У классического блокчейн ими заимствована лишь идея криптографически закрытого реестра транзакций, которая использована для модернизации традиционных баз данных с целью расширить их функционал (или просто следуя моде на блокчейн). Это оправдано практическими соображениями, так как полностью децентрализованные и распределенные архитектуры блокчейн действительно затратны, сложны и недоста-

точно доработаны для индустриального применения.

Напротив, ряд венчурных проектов (в большинстве своем стартапов, находящихся сейчас в активной разработке) сфокусировались на поиске оптимальных решений, способных утилизировать распределенную сущность блокчейн (то есть возможности, предоставляемые децентрализацией реестра транзакций), − решений, позволяющих за счет определенных технических компромиссов и гибридных архитектур достичь высокой производительности и других качеств, необходимых индустрии. Благодаря таким примерам будут очерчены перспективы эволюции наиболее жизнеспособных форм блокчейн из множества проектов, реализуемых в этой сфере.

Подобный взгляд на будущее блокчейн соответствует концепции неоиндустриализации и "умной" промышленности как гармоничного соединения старого и формирующегося нового технологических укладов [8].

Технологические истоки инновационности

Технология блокчейн основана на использовании распределённой базы данных (англ. *distributed ledger*). Распределённость заключается в том, что база (англ. *ledger* – реестр транзакций) сберегается в виде большого количества равноправных копий у участников (англ. *peer*) блокчейн. Нет эталонной копии или центрального хранилища (как единой точки отказа), а значит, нет и необходимости окружать его файерволом, защищать от хакерских атак или иных угроз с использованием дорогостоящих и сложных систем.

Несмотря на то что распределённая база доступна участникам (англ. *peer* – равноправный), она защищена от внесения ими недостоверных данных и ретроспективного изменения записанной информации (англ. *immutabl*e − неизменяемый). Защищённость данных, хранящихся в открытой распределённой системе, является первым важным преимуществом технологии блокчейн.

Распределённая база хранит информацию о транзакциях, совершаемых над токенами. Токен (англ. *token* – знак, жетон, талон) – цифровое абстрактное представление активов, прав или обязательств, которое является объектом количественного учёта в этой базе данных.

Транзакции являются отражением сделок между владельцами токенов. Административный центр, гарантирующий правильную регистрацию сделок, в данном случае не нужен. Его роль в блокчейн выполняет консенсус участников системы. Любой участник может инициировать регистрацию транзакции, направив изменения в базу, и только тогда, когда такие изменения будут согласованы системой (будет достигнут консенсус), они "разольются" (будут синхронизированы) по всем копиям.

Алгоритм консенсуса определяет правила, по которым автоматически вычисляется и гарантируется истинное содержимое распределенной базы данных, что особо актуально, когда ряд участников могут попытаться сфальсифицировать информацию (классическая задача "византийских генералов"). Учёные и практики стремятся к высокой надёжности и одновременно производительности таких алгоритмов [9].

Таким образом, в блокчейн отсутствие доверия между сторонами сделок (и вообще участниками), а также авторитетного центра (арбитра, единого реестра) не является проблемой. Регистрация сделок и хранение информации о них происходят распределенно (peer-to-peer, P2P), но при этом совершенно безопасно. Распределенность является вторым важным преимуществом технологии блокчейн. Следует подчеркнуть, что философия блокчейн заключается в том, что защищённость информации обеспечивается именно распределенностью системы (первое преимущество обусловлено вторым).

Распределенность (максимальная децентрализация) блокчейн также позволяет распространить эту технологию на любой тип взаимодействия участников, будь то

H2H (англ. *human-to-human* – от человека к человеку), H2M (англ. *human-to-machine* – от человека к машине) или M2M (англ. *machine-to-machine* – от машины к машине).

Благодаря присущим им свойствам токены могут служить цифровой формой представления большинства видов активов и обязательств, а блокчейн – удобной средой хранения и регистрации различных экономических и финансовых данных. На сегодняшний день основное применение токенов – это эмиссия криптовалют, осуществление платежей с криптовалютами без участия центрального банка и банков вообще. Можно сказать, что криптовалюты послужили инструментом апробации и популяризации блокчейн на первом этапе.

На втором этапе развития блокчейн предоставил возможность альтернативного сбора инвестиций (англ. *crowdfunding*) для новых проектов и стартапов в виде ICO (англ. *initial coin offering* – первичное размещение токенов). В настоящее время разворачивается третий этап развития этой технологии – ищутся лучшие способы широкого применения токенов для учёта имущественных прав, налогообложения, в том числе транснационального, реализации права выбора (голосование, экспертиза), для продажи, обмена, совместного использования любых активов (в том числе интеллектуальной собственности), тарификации в системах массового обслуживания и т.п.

Отношения клиента (владельца токенов) и блокчейн-системы начинаются с открытия клиентом счета (кошелька) в системе, на котором хранится ноль или более токенов. Вся история перемещения токенов между кошельками клиентов (транзакций) сохраняется в базе данных бесконечно (в большинстве реализаций блокчейн), начиная с первого мгновения работы системы.

Блокчейн обеспечивает почти абсолютную гарантию того, что только владелец токенов может ими суверенно распорядиться [10], а также авторизацию владельца и неприкосновенность его активов при помощи устойчивых криптографических методов [11] (асинхронное шифрование, дерево Меркла и др.). Благодаря этому свойству система блокчейн может параллельно использоваться как механизм децентрализованной и высоконадёжной проверки личности участников и предоставления им прав (для аутентификации и авторизации).

Архитектуры и их ограничения

В структурном отношении система блокчейн – это сама распределённая база плюс алгоритмы и компьютерная инфраструктура, реализующие взаимодействие с ней. Вся эта система обеспечивает хранение в распределённой базе информации о транзакциях, упакованной в блоки (англ. *block*-), нераздельно связанные между собой в цепочки (англ. *-chain*). При этом каждый блок является архивом для определённого количества последовательных транзакций, а вся цепочка блоков отражает историческую последовательность всех транзакций. Блоки связаны между собой неразрывно благодаря криптографическим алгоритмам. Вставить (или выбросить) блок из середины цепочки невозможно, такая операция будет отвергнута системой. Возможно только присоединение новых блоков к концу цепочки.

Распределённость системы подразумевает, что база данных хранится в виде полных копий на большом количестве компьютеров (узлов – англ. *node*). При этом пассивные узлы только читают информацию, а активные имеют право (по своей инициативе или поручению пассивных узлов) вставлять новые блоки транзакций в базу (присоединять к chain). В ранних криптовалютных системах все узлы обычно активны (биткоин). В отдельных архитектурах существуют служебные узлы (отвечающие за упорядочивание транзакций, маршрутизацию в сети, балансировку нагрузки и т.п.).

Все разнообразие версий блокчейн обычно разделяют на следующие формы (по режиму доступа к информации):

публичные (англ. *permissionless*), когда любой желающий может стать узлом;

полупубличные, когда активные узлы – это круг избранных, пассивные могут присоединяться более-менее свободно;

непубличные (англ. *permissioned*) – доступ всех участников администрируется.

Для более точного представления сути блокчейн следует выделить его основные архитектуры (по режиму хранения информации):

распределенные, когда реестр транзакций хранится у каждого участника;

децентрализованные, когда реестр транзакций хранится не у каждого участника, а на некотором (как правило, небольшом) количестве узлов;

централизованные, когда только один узел (сервер базы данных) используется для хранения всего реестра транзакций.

Поскольку реестр транзакций с момента создания блокчейн был назван "распределенным", одноименная архитектура рассматривается как классическая. Публичные системы являются распределенными. Потенциал таких систем для развития экономических институтов наиболее очевиден, но существует ряд серьезных ограничений данной архитектуры, которые рассмотрены ниже.

Децентрализованная архитектура лежит в основе непубличных (полупубличных) систем. Причем чем меньше количество копий (точнее, активных узлов), тем система производительнее. Как будет показано далее, это связано, в частности, с особенностями алгоритмов консенсуса. Такое свойство нередко является причиной отказа от децентрализации (склонность к ограниченной децентрализации).

Впрочем, даже централизованные системы (крайний случай) не исключают резервное копирование и потому не являются по определению небезопасными. Однако безопасность от потери данных не тождественна свойству защищенности данных от подмены и фальсификации (присущего от природы распределенным системам).

Строго говоря, непубличные, полупубличные (ограниченно децентрализованные и централизованные) архитектуры являются "квазиблокчейн" (иногда упоминаются как "эксклюзивный" блокчейн). Они жертвуют фундаментальным свойством – распределенностью как основой защиты данных – в пользу простоты реализации и высокой производительности. Криптовалюты в основном зиждутся на публичных формах. Спрос на непубличные системы предъявляют в настоящее время реальный и государственный секторы экономики.

Как информация хранится в такой системе? Каждый новый блок транзакций попадает в базу данных после верификации и "запечатывания", которое осуществляет активный узел системы. Главная её "фишка" заключается в том, чтобы обеспечить механизм консенсуса, позволяющий всем активным узлам совместно одобрить внесение информации в базу (присоединение нового блока к цепочке).

В зависимости от механизма консенсуса системы блокчейн разнятся. Первопроходец – биткоин – использует подход "доказательство работой" (англ. *proof-of-work, PoW*), когда все активные ноды за вознаграждение соревнуются между собой, кто быстрее осуществит затратную (машинные мощности, время работы процессоров, электроэнергия) операцию расчёта "магического" числа. Первый справившийся узел запечатывает и вносит блок транзакций в базу, получая за это вознаграждение в виде эмитированных биткоинов. В этом смысл так называемого майнинга. Трудоёмкость майнинга растёт с увеличением количества соревнующихся узлов, и такая конкуренция приводит к тому, что победитель в гонке (в "лотерее") всегда случаен. Если кто-то целенаправленно захочет внести в базу ряд фиктивных блоков транзакций, то ему придется раз за разом выигрывать гонку, а это статистически невозможно, разве что фальсификатор сумел бы сосредоточить у себя более 51% вычислительных мощностей (битрейтов) всей системы (проблема "уязвимости 51%" [12]). Такая ситуация является чисто гипотетической.

Недостатком "доказательства работой" PoW является то, что с увеличением

количества узлов затратность работы экспоненциально растёт (на сегодня майнеры биткоин в совокупном потреблении электроэнергии обошли Ирландию, и в свете глобального потепления биткоин выглядит аморальнее, чем просто спекулятивный актив [13]). Кроме того, из-за постоянного роста сложности каждой единицы "работы" система обречена на низкую производительность. Запечатывание каждого нового блока требует всё больше ресурсов и обычно длится дольше по времени.

Это означает, что количество транзакций в единицу времени, пропускаемых системой биткоин (и множеством подобных криптовалютных систем) ограничено сверху (уровнем развития компьютерных процессоров). В сравнении с 24К (24 тыс.) транзакций в секунду у системы VISA, биткоин спотыкается на 7 транзакциях в секунду, в результате чего клиенты часами ждут завершения криптовалютных переводов. Это делает первое поколение криптовалют неудобным и бесперспективным средством расчётно-денежных операций (что стало одной из причин раскручивания исключительно спекулятивного интереса к ним).

Преодолеть данные проблемы пытаются потомки и версии, так называемые форки (от англ. *fork* – развилка, ответвление) биткоина и новые виды криптовалют за счёт изменения структуры базы данных, формата и вместительности блоков и т. п. Но, по большому счету, обойти все присущие PoW ограничения невозможно.

В этой связи интерес представляют альтернативные механизмы достижения консенсуса. В целом данные механизмы делятся на основанные на лотерее и основанные на голосовании. В алгоритмы, основанные на лотерее, входят помимо описанного PoW также "доказательство долей владения" PoS, (от англ. *Proof-of-Stake*), "делегированное доказательство долей владения" DPoS (англ. *Delegated Proof of Stake*), "доказательство важностью" PoI (англ. *Proof-of-Importance*) и ряд их вариаций [14]. Хотя последние несколько улучшают производительность систем в сравнении с "доказательством работой", они все же имеют те же недостатки и особенности, что и PoW. В частности, они обеспечивают максимальную открытость и масштабируемость системы ценой относительно низкой пропускной способности (в транзакциях в секунду). Можно констатировать, что из-за указанных выше особенностей все эти системы заточены под майнинг криптовалют.

Основанные на голосовании алгоритмы, такие как варианты Византийского консенсуса, Paxos [15], RAFT [16], напротив, обеспечивают высокую пропускную способность за счёт низкой масштабируемости, то есть за счёт ограниченной возможности расширять количество активных (точнее выражаясь, участвующих в голосовании для достижения консенсуса) узлов. Прирост количества голосующих узлов экспоненциально увеличивает время достижения консенсуса, а значит, снижает производительность. Однако при ограниченном количестве активных узлов, например, в полуоткрытых или закрытых системах (что тождественно централизованным и слабо децентрализованным системам), этот механизм консенсуса обеспечивает высокую производительность (даже при значительном росте количества пассивных узлов), достаточную даже для его интенсивного применения в финансовом и реальном секторах экономики.

Эволюция блокчейн

За время развития технология блокчейн прошла этапы, охарактеризованные как первое и второе поколения, и в настоящее время третье поколение блокчейн находится в процессе становления. Первое поколение включает собственно биткоин и подобные ему криптовалюты. Архитектуры блокчейн, обслуживающие их, способны выполнять лишь простейшие транзакции и имеют быстро деградирующую производительность.

Второе поколение началось, по сути, с создания блокчейн для криптовалюты эфир (Ethereum) и обеспечило участникам возможность не просто осуществлять пере-

воды токенов друг другу, но и заключать между собой полноценные "умные" контракты (англ. *smart contract*). Самоисполняющиеся контракты, но с ограниченным функционалом, были возможны и в Биткоине, но там они практически не применялись. "Умные" контракты – это алгоритмы для автоматизации выполнения транзакций, написанные на специальных языках (пример − Solidity для эфира), хранящиеся в блокчейн и выполняющиеся в среде виртуальных машин (часть блокчейн второго поколения). Они обеспечивают полноту по Тьюрингу, то есть возможность написания любых вычисляемых функций [17] (вставка 1).

Вставка 1

Сфера и пример применения блокчейн

Сфера применения "умных" контрактов согласно Белой книге (White Paper) Палаты цифровой коммерции (The Chamber of Digital Commerce) [18] такова:

- цифровая идентичность, контроль над персональными данными;
- поставки ценных бумаг, расчёты по ним, выплата дивидендов;
- цифровые аккредитивы, аналоги эскроу-счетов;
- сделки, требующие сложной верификации, подтверждения множеством сторон;
- совместная бухгалтерия контрагентов для упрощения сверок и аудита;
- учёт цепочек поставки товаров для оптимизации оборотных средств;
- имущественное и медицинское страхование и т. д.

Пример использования "умного" контракта (эскроу-счет в валюте Ethereum).

Допустим, есть три инвестора (1, 2, 3), которые хотят совместно приобрести новое оборудование. Между ними отсутствует доверие. Кроме того, им трудно прийти к общему согласию относительно поставщика станков.

Стороны описывают логику сделки в виде формального документа (меморандума). На этой основе программисты создают "умный" контракт. Контракт заносят в блокчейн (в данном примере – Ethereum). Контракт включает следующие условия:

1) в течение N дней инвесторы перечисляют со своих персональных счетов в Ethereum договорённые суммы X1, X2, X3 (долевое участие) на счёт "умного" контракта;

2) если до этого срока не поступают все указанные суммы от сторон, то происходит автоматический возврат средств инвесторам и контракт "расторгается";

3) если все суммы собраны, то проверяется условие, что к этому моменту все стороны согласились с выбором продавца; если нет − то происходит "расторжение", аналогично п. 2;

4) если получено единогласное одобрение сторонами продавца (каждая сторона должна для этого вызвать определённую функцию "умного" контракта, голосуя с её помощью "за" один из M вариантов), то переходим к п. 5;

5) происходит перечисление средств X1+X2+X3 продавцу на его счёт в Ethereum. Сделка на этом этапе завершена. Контракт прекращается.

Будучи публичным и неизменяемым (сберегаясь в блокчейн), контракт теперь легко проверяется участниками (их техническими экспертами). Если он соответствует договорённостям, то стороны приступают к выполнению (детальное описание "умных" контрактов с примерами кода приведено в ряде источников: например [17; 19])

Можно утверждать, что второе поколение приоткрыло двери для масштабной дигитализации экономики, так как на основе "умных" контрактов теоретически возможно оцифровывать не только простейшие транзакции, но и технологические процессы, логистические цепочки, юридические конструкции и законодательные нормы [20]. В разработке новых поколений блокчейн в последние годы принимают

активное участие ведущие игроки мировой промышленности, торговли и финансов. Forbes опубликовал список Top-50 исследователей блокчейн, куда вошли: Toyota, Samsung, Oracle, IBM, Apple, Bank of China, Bank of America, IMG, Alibaba [21].

Однако средой массового распространения блокчейн по-прежнему остаются криптовалюты (в 2015-2018 гг. на них приходится подавляющая часть венчурного финансирования блокчейн-проектов). А проникновение блокчейн в реальный сектор весьма незначительно. По оценкам Deloitte, 40% опрошенных бизнесменов задумаются о применении блокчейн только в будущем [22]. У множества опрошенных наблюдается усталость от приевшейся технологии, так как после шумного дебюта "миттельшпиль" технологии затянулся.

Очевидно, что переход от изначально криптовалютного предназначения блокчейн к универсальному потребует более глубокой трансформации, чем ожидалась. Более сложной и длительной, чем та трансформация, что произошла при смене первого и второго поколений.

Далеко не все "узкие" места блокчейн были устранены во втором поколении. Проекты, которые сейчас формируют экосистему третьей генерации блокчейн, направлены прежде всего на преодоление глубинного противоречия, присущего технологии от момента её возникновения и названной создателем Ethereum В. Бутериным "трилеммой" блокчейн [23]. Эта "трилемма" характеризует внутреннее ограничение блокчейн, не позволяющее ему быть одновременно производительным, распределенным и оставаться безопасным. Достижение любых двух целей противоречит третьей.

Усилия исследователей и разработчиков сконцентрированы на поиске компромиссных решений "трилеммы", например, увеличении производительности технологии без существенного ущерба для децентрализации и безопасности. Более специфические задачи, стоящие перед третьим поколением, − это рост универсальности технологии для применения её в разных отраслях, упрощение взаимодействия различных систем блокчейн между собой (путём межсистемных "умных" контрактов), а также полноценная интеграция блокчейн с внешним физическим миром (как пример, создание тригеров для связи выполнения "умных" контрактов с событиями извне) [24].

Очертания третьего поколения только формируются, и альтернативным решениям ещё предстоит пройти естественный отбор. Одним из претендентов на выживание в составе нового поколения блокчейн является использование "шардинга" (от англ. *shard* – осколок, кусочек) при создании распределённой системы. В отличие от существующего сейчас хранения на каждом узле полной копии базы данных "шардинг" предлагается хранить на отдельных нодах только фрагмент базы данных. Полная база формируется как мозаика, слагающаяся из всех раздельно хранимых фрагментов. "Шардинг" существенно увеличивает производительность системы [25], что особо важно для применения в финансах и реальном секторе экономики.

В 2015 г. были разработаны Lightning Network и подобные ей подходы, названные двухуровневыми протоколами [26]. Они решают проблему низкой производительности блокчейн по-иному, чем "шардинг", а именно за счёт понижения требований безопасности для частных транзакций. Так, множество транзакций, индивидуально не критичных, например, мелких, с допустимым риском (на практике таких большинство), выполняется вне блокчейн (англ. *off-chain*), то есть без консенсуса. И только по завершении группы мелких задач их сливают вместе в одну мегатранзакцию, которую проверяют и проводят классически, а значит, помещают в блокчейн по общим правилам через консенсус. Нагрузка на систему падает, а производительность растёт. По закону больших чисел ожидают, что цена риска для множества мелких транзакций выполняемых off-chain

не превысит выигрыш от повышения скорости блокчейн в сотни и тысячи раз.

Также интересным примером выхода из тупика «трилеммы» является проект Exonum, разрабатываемый одним из лидеров производства оборудования для блокчейн и майнинга − компанией Bitfury [7]. Проект реализован как децентрализованная система с лимитированным количеством активных узлов. Благодаря такому ограниченному масштабированию и использованию оригинальных алгоритмов консенсуса достигнута высокая производительность (до 15 тыс. операций в секунду). Понимая, что криптостойкость в такой системе, возможно, будет уязвимой, создатели Exonum решили позаботиться о безопасности по-своему. Время от времени системой создаются точки синхронизации, сохраняющие контрольные суммы состояния своего блокчейн в распределенном блокчейн биткоина (максимально безопасном сегодня). Такую процедуру назвали "якорением" (анкоринг). Авторы проекта заявляют, что хотя фабрикация данных в их системе потенциально возможна, однако она однозначно не пройдет незамеченной и истина будет впоследствии легко восстановлена. Достоинства Exonum позволили ему принять участие в проекте перехода земельного кадастра Грузии на блокчейн.

Перспективы использования в реальном секторе экономики

Зарождающиеся в третьем поколении черты блокчейн могут помочь созданию полномасштабных систем, ориентированных на производственный сектор, в частности гибких механизмов расширения механизмов консенсуса. Обычный консенсус препятствует внесению в базу поддельных транзакций, решая проблему "двойного расходования" активов (англ. *double spending*). Если новые системы блокчейн позволят задействовать более сложную логику проверки транзакций на соответствие бизнес-правилам, то это определённо расширит сферу применения "умных" контрактов. Такая комплексная смарт-проверка транзакций необходима для реализации в блокчейн хозяйственных договоров, норм законодательства, учёта производственных операций, логистики и т.п.

Однако, помимо существующих пока внутренних противоречий технологии, её внедрение тормозят и традиционные барьеры сопротивления изменениям. Реинжиниринг бизнеса с целью перехода на блокчейн является весьма рискованным и дорогостоящим мероприятием для успешно работающей компании. По этой причине внедрение блокчейн, по мнению Deloitte, привлекает в основном бизнес, создаваемый "с чистого листа" [22].

Впрочем, уже есть проектные решения "под ключ", максимально облегчающие внедрение блокчейн в работающих компаниях. Одним из лидеров в сфере B2B является Hyperledger Fabric [27], основанный Linux Foundation в 2015 г. при участии IBM и переданный сообществу свободного программного обеспечения. Проект соответствует второму поколению блокчейн и непрерывно развивается, расширяя области индустриального применения (вставка 2).

Hyperledger Fabric мало похож на распределенный публичный блокчейн (например, Ethereum). Он является реализацией криптографически защищённого децентрализованного реестра транзакций на ограниченном числе узлов. Ряд таких закрытых "квазиблокчейн"-проектов (называемых здесь так в противовес открытым и распределенным "истинным" блокчейн) часто применяется для решения актуальных задач бизнеса, в частности финансовых расчётов, кредитования, таможенной очистки и налогообложения.

Наиболее известный пример – Corda, созданная консорциумом R3 (из 200 фирм, включая гигантов Barclays, Credit Suisse, Goldman Sachs, J.P. Morgan) [28]. Corda была внедрена Cargill для контроля перемещения товаров и расчётов с партнёрами и позволила увеличить прозрачность и безопасность торговых и финансовых операций, ускорить получение аккредитивов [29] и др.

Вставка 2

Блокчейн от Hyperledger Fabric

Особенность Hyperledger Fabric – это использование закрытых блокчейн, более удобных для индустриального применения, чем криптовалютные версии:

- эмиссии токенов не происходит (есть надстройки, устраняющие это ограничение);
- майнинга цифровых валют также нет, не применяются конкурентные алгоритмы консенсуса (PoW и подобные);
- используются алгоритмы консенсуса, характерные для классических распределённых баз данных, в частности византийский (возможно даже отключить консенсус вообще);
- децентрализация весьма ограничена, так масштабируются клиентские узлы, но не специализированные узлы (занятые хранением и обновлением реестра);
- точек отказа (копий реестра) более чем одна, но это не обеспечивает столь высокую защиту данных от компрометации, как распределенный блокчейн

Возникает вопрос: в полной ли мере подобные системы соответствуют философии блокчейн (безопасность за счёт распределенности)? Пожалуй, нет. Это именно "квазиблокчейн". В них не используется "якорение" или другие алгоритмы усиления надежности данных. Они являются не стимулом развития институтов (каким был провозглашен блокчейн), а скорее еще одним прикладным инструментом бизнеса. Доверие к содержимому реестра в них попрежнему зависит от доверия к хранителю (только таких теперь не один, а несколько, и каждый из них может аудировать другого). Однако для индустриального использования такие частично масштабируемые системы являются сейчас доступным выбором. Обоснованность выбора связана с ответом на вопрос: нужен ли блокчейн конкретному предприятию вообще (есть методики, упрощающие принятие этих решений [30]).

Существует то, что объединяет "квази"-продукты (нераспределённые, ограничено децентрализованные) с классическим блокчейн и наделяет первых преимуществами, благодаря которым их ставят в один ряд со вторыми. Это токенизация, то есть создание уникального, криптографически защищённого цифрового представления актива в реестре. Токенизация (как часть общей тенденции дигитализации экономики) применима не только для средств платежей, но и для товаров, услуг, прав, персоналий и т.п.

Токенизация значительно облегчает идентификацию в цифровом пространстве. Благодаря токенизации невозможно, допустим, многократно использовать один и тот же предмет в качестве обеспечения платежа или залога. Это актуально не только для материальных ценностей. Токенизация обслуживающих мощностей, сервисных часов, арендных площадей, в частности, позволит значительно повысить доверие инвесторов и облегчить предварительные продажи и финансирование девелоперов и производителей. То, что сейчас происходит как бум ICO для IT- и WEB-проектов, может стать практикой инвестирования в материальные активы.

Благодаря подобным возможностям блокчейн формирует среду не только для привлечения инвестиций, но и для оптимизации рабочего капитала. Наиболее известный пример − ускорение кредитования производственных и торговых операций посредством финансирования цепочки поставок (англ. *supply chain finance*). Использование блокчейн в качестве информационной платформы для e-Invoicing (Electronic invoicing) позволяет за счёт повышения качества информации (открытость и взаимный аудит) минимизировать риски сторон, а значит, снизить стоимость привлечения кредитов в схемах факторин-

га. В ряде публикаций рассмотрены примеры того, как компании масштаба IBM, Maersk, Dianrong заняты внедрением международных систем финансирования цепочки поставок, основанных на блокчейн [31].

Можно считать симбиоз e-Invoicing и блокчейн одной из наиболее перспективных инноваций. e-Invoicing – это единая "расшаренная" (англ. *sharing* − совместно использовать) для торгующих сторон электронная бухгалтерия (точнее, часть бухгалтерского учёта, связанная с оборотом товаров) [32]. E-Invoicing представляет собой технологию выпуска и передачи счетов-фактур, накладных и налоговых накладных торговыми партнёрами друг другу, а также фискальным органам в цифровом представлении – в отличие от бумажных или даже сканированных "безбумажных" документов.

Оцифровка счетов-фактур, введение их в блокчейн и связь с "умными" контрактами упростят сторонам торговых сделок мониторинг соблюдения договорных и законодательных норм. Технологии e-Invoicing и блокчейн развивались независимо, но, достигнув зрелости, они стали комплементарными. Ожидается, что в ближайшие годы мы увидим ещё больше примеров успешной реализации e-Invoicing на платформе блокчейн третьего поколения. Считается, что такое внедрение блокчейн может создать предпосылки для дальнейшего перехода к цифровому налогообложению (НДС-валюты, англ. *VATCoin*) [33].

Ещё одно перспективное направление использования блокчейн в промышленности – это его симбиоз с технологий Интернета вещей (англ. *Internet of Things, IoT*) [34]. Производство и совершенствование "умных" приборов происходит почти во всех отраслях промышленности. Это промышленный интернет вещей, IoT в системах планирования ресурсов предприятий, самодиагностирующееся оборудование, выполняющее самообслуживание, создание сетей миниатюрных девайсов, образующих "паутину" органов чувств для мощного искусственного интеллекта и много другое. Ввиду низкого доверия к таким IoT девайсам блокчейн может быть решением проблем безопасности, требующим, однако, одновременной высокой производительности и масштабируемости ("трилемма" блокчейн). Если в третьем поколении будут предложены разумные компромиссные решения этой головоломки, то объединение IoT и искусственного интеллекта с блокчейн может породить новый поток революционных промышленных инноваций.

Выводы. Появление блокчейн имело провокационный характер. Предложение породило спрос, а затем и ажиотаж в интересах финансовых посредников и производителей специализированных процессоров. Сгенерированные на основе блокчейн криптовалюты, несмотря на волатильность, неудобство в сфере обмена (неповоротливость, "драконовские" комиссии) и рискованность для накопления (в том числе в связи с полузаконным статусом) капитализировались до величины денежной массы отдельных стран. В этой игре с нулевой суммой проиграли только держатели валют. Даже после коррекции рынка интерес к цифровым деньгам и лежащим в их основе технологиям не остыл. Так блокчейн пережил первый кризис взросления.

Ряд лидеров разработки программного обеспечения, оседлав волну блокчейна, представили свои индустриальные решения для распределённых реестров. Но не все они в полной мере соответствовали идеологии блокчейн. Некоторые решения попросту были вынуты "из-под сукна" и базировались на скорее традиционном, чем инновационном, технологическом ядре [35]. Однако в сравнении с полноценным блокчейн (распределенным и открытым) подобные проекты имеют меньше проблем с масштабированием и меньше ограничений по сферам использования.

В целом при столь большой шумихе состоялось относительно немного внедрений блокчейн в реальном секторе экономики. Некоторые из занимавших лидирующие позиции проектов, как упомянутая R3 Corda, переживают теперь кризис и по некоторым сообщениям находились недавно на грани банкротства [36] и даже рассматривали отказ от дальнейшего использования блокчейн. Этот, второй после спекулятивного, кризис может разрешиться в третьем поколении блокчейн.

Новая генерация блокчейн ещё не приняла твёрдых очертаний, находясь в конкурентной гонке. Существует также инвестиционная ловушка. Финансовым посредникам, заработавшим на майнинге (драйверам первых поколений блокчейн), невыгодно вкладывать средства в разработку новых блокчейн-продуктов для реального сектора экономики, так как показатели окупаемости здесь значительно скромнее.

Блокчейн по-прежнему остаётся синонимом новизны. Благодаря спекулянтам и энтузиастам эта технология так вошла в моду, что её пытаются, как почтовую марку, приклеить на любой новый проект, даже там, где это неуместно. На практике важно не переоценивать блокчейн в его сегодняшнем виде. Исходя из рассмотренных особенностей можно сформулировать некоторые критерии индустриального применения этой технологии:

1. Внедрение блокчейн "per se" для замены многопользовательской базы данных оправданно, если она (база, хранящая реестр транзакций) будет находиться в режиме полного доступа у множества сторон, имеющих низкое доверие друг к другу. Такой полный доступ выгоден бизнесу, если он, в частности, ускоряет оборачиваемость рабочего капитала. Пример – совместное ведение бухгалтерии торговыми партнёрами (цепочки поставок и т.п.). Напротив, переход заурядной бухгалтерии или системы для управления взаимоотношениями с клиентами на блокчейн контрпродуктивен, несмотря на распространённую рекламу подобных решений.

2. Распределенный и открытый (permissionless) блокчейн в условиях нынешних технологий обычно мало производителен и всегда высокозатратен. Такая архитектура действительно является максимально устойчивой и безопасной из всех возможных, что в теории привлекательно, например, для государственных реестров или налоговых активов (VATCoin). Но если учесть, что все узлы (неограниченное количество узлов) необходимо постоянно вознаграждать за хранение ими реестра и проверку транзакций, то применение таких блокчейн становится убыточным (для криптовалют финансовое бремя покрывалось за счёт финансовых "пирамид"). Есть надежда, что третье поколение может разрушить этот проблемный паттерн.

3. Закрытые (permissioned), в том числе названные здесь "квазиблокчейн", системы являются усовершенствованием децентрализованной базы данных. Выбор такой архитектуры блокчейн для индустриального использования оправдан при положительном ответе на вопрос в п. 1. Затем необходимо принять количественные решения о числе распределённых копий и качественные – о механизмах консенсуса. Оптимизация этих параметров подобна поиску компромиссов в "трилемме" блокчейн. При росте количества держателей реестра безопасность повышается (в теории в два раза сложнее взломать 20 точек отказа вместо 10), однако производительность снижается, а затраты на построение и эксплуатацию системы растут. Но соображения, указанные в п. 1, требуют, чтобы каждая из сторон (не доверяющих друг другу) имела, как минимум, одну "приватную" копию реестра.

4. Сложная бизнес-логика (особенно производственных объектов) может стать препятствием для использования современных блокчейн. "Умные контракты" и механизмы проверки транзакций и консенсуса в их нынешнем виде вряд ли позволят

алгоритмизировать все бизнес-кейсы. Кроме того, будучи "запечатанной" в блокчейн в форме "умных контрактов", бизнес-логика теряет гибкость и универсальность. Ряд современных специализированных продуктов позволяет настолько упростить управление бизнес-процессами, что сравнение с ними может быть не в пользу "умных контрактов" и свести преимущества блокчейн к нулю.

Так обстоят дела с сегодняшним применением блокчейн. Что касается будущего, то развитие новой промышленности (Индустрии 4.0) с ее "умными" производствами, роботизацией, искусственным интеллектом (AI), Big Data, IoT, управляемыми спросом цепочками поставок и подобными инновациями нуждается в адекватных решениях для хранения и обмена бизнес-информацией − таких, что обеспечивают высокую доступность данных и одновременную кибербезопасность. Блокчейн, в основе которого лежит устойчивый к фальсификации распределенный реестр, способен помочь в решении ряда проблем.

Рабочий механизм блокчейн – цепочка криптографически связанных блоков транзакций, которая может оставаться (как это нередко происходит сейчас) "пятым колесом" в эффективных и без неё системах баз данных, принося только имиджевый рост продаж, или же может стать инновационной основой для децентрализованных самоорганизующихся систем M2M и H2M, формирующей новые типы взаимоотношений, новые рынки и продукты и даже способствовать прогрессу экономических институтов. Для того, чтобы такой оптимистичный прогноз реализовался, необходимо обеспечить продвижение технологии в сторону распределенных, но при этом более высокопроизводительных и эффективных по затратам систем. Это небыстрый и не предопределённый ещё путь компромиссных решений, требующих дальнейших исследований технологических и социально-экономических аспектов блокчейн в контексте "умной" промышленности.

Литература

1. Solow R. We'd better watch out. *The New York Times. Book Review.* 1987. 12 July. P. 36.

2. Rosulek M. 14 Bitcoin quotes by famous people. *Medium.* URL: https://www.newsbtc.com/2014/03/16/google-chairman-eric-schmidt-bitcoin-architecture-amazing-advancement (дата обращения: 06.02.2019).

3. Deen M. Lagarde Says Cryptocurrency Mining Is Consuming Too Much Power. *Bloomberg.* URL: https://www.bloomberg.com/news/articles/2018-01-25/lagarde-says-cryptocurrency-mining-is-consuming-too-much-power (дата обращения: 06.02.2019).

4. Krugman P. Transaction Costs and Tethers: Why I'm a Crypto Skeptic. *The New York Times*. 2018. 21 July.

5. Stinchcombe K. Ten years in, nobody has come up with a use for blockchain. *Hackernoon.* URL: https://hackernoon.com/ten-years-in-nobody-has-come-up-with-a-use-case-for-blockchain-ee98c180100 (дата обращения: 06.02.2019).

6. Davidson S., De Filippi P., Potts J. Blockchains and the Economic Institutions of Capitalism. *Journal of Institutional Economics*. 2018. 14 (4), p. 639-658. doi: http://dx.doi.org/10.1017/S1744137417000200

7. Земельный кадастр на блокчейне. *Exonum.* URL: https://exonum.com/ru/napr (дата обращения: 06.02.2019).

8. Kniaziev S. Development of smart industry as an efficient way to implement the policy of neoindustrialization in the world. *Economic of Industry*. 2017. No. 4(80), p. 5-18. doi: http://dx.doi.org/10.15407/econindustry2017.04.005

9. Babaoğlu Ö., Marzullo K. Distributed Algorithms. Berlin: Springer, 1996. 388 p.

10. Sterlin L. Is Bitcoin at Risk as Google and IBM Aim for 50-Qubit Quantum Computers? *Bitcoin News.* URL: https://news.bitcoin.com/is-bitcoin-at-risk-as-

google-and-ibm-aim-for-50-qubit-quantum-computers (дата обращения: 06.02.2019).

11. Mistry N. Introduction to Bitcoin and ECDSA. *Slideshare.* URL: https://www.slideshare.net/NikeshMistry1/introduction-to-bitcoin-and-ecdsa (дата обращения: 06.02.2019).

12. Raval S. Decentralized applications. Sebastopol, CA: O'Reilly Meida, 2018. 118 p.

13. Deign J. Bitcoin Mining Operations Now Use More Energy Than Ireland. *Greentechmedia.* URL: https://www.greentechmedia.com/articles/read/bitcoin-uses-more-energy-than-ireland (дата обращения: 06.02.2019)

14. Bashir I. Mastering Blockchain. London, UK: Packt Publishing, 2018. 540 p.

15. Surhone L., Tennoe M., Henssonow S. Paxos Algorithm. Saarbrücken: Betascript Publishin, 2011. 64 c.

16. Raft. URL: https://raft.github.io (дата обращения: 06.02.2019).

17. Dannen C. Introducing Ethereum and Solidity. New York: Apress, 2017. 185 p.

18. Earls J, Smith M, Smith R. Smart Contracts: Is the Law Ready? *Chamber of Digital Commerce.* URL: https://digitalchamber.org/smart-contracts-whitepaper (дата обращения: 06.02.2019).

19. Distributed Lab. Введение в смарт-контракты. *Habr.* URL: https://habr.com/ru/company/distributedlab/blog/413231 (дата обращения: 06.02.2019).

20. Mukhopadhyay M. Ethereum Smart Contract Development: Build blockchain-based decentralized applications using solidity. London: Packt Publishing, 2018. 288 p.

21. del Castillo M. Big Blockchain: The 50 Largest Public Companies Exploring Blockchain. *Forbes.* URL: https://www.forbes.com/sites/michaeldelcastillo/2018/07/03/big-blockchain-the-50-largest-public-companies-exploring-blockchain (дата обращения: 06.02.2019).

22. Arnold A. The 6 Major Blockchain Trends for 2018 Outlined By Deloitte. *Forbes.* URL: https://www.forbes.com/sites/andrewarnold/2018/07/27/the-6-major-blockchain-trends-for-2018-outlined-by-deloitte (дата обращения: 06.02.2019).

23. Ometoruwa T. Solving the Blockchain Trilemma: Decentralization, Security & Scalability. *Coinbureau.* URL: https://www.coinbureau.com/analysis/solving-blockchain-trilemma (дата обращения: 06.02.2019).

24. Oraclize. How it works. *Oraclize.* URL: http://www.oraclize.it (дата обращения: 06.02.2019).

25. Jordn R. How to Scale Ethereum: Sharding Explained. *Medium*. URL: https://medium.com/prysmatic-labs/how-to-scale-ethereum-sharding-explained-ba2e283b7fce (дата обращения: 06.02.2019).

26. Lightning Network. *Lightning Network.* URL: https://lightning.network (дата обращения: 06.02.2019)

27. Hyperledger. Hyperledger Business Blockchain Technologies. *Hyperledger.* URL: https://www.hyperledger.org (дата обращения: 06.02.2019).

28. Corda. Welcome to Corda. *Corda.* URL: https://docs.corda.net (дата обращения: 06.02.2019).

29. Noble L. Cargill blockchain shipping transaction cuts exchange time to 24 hours. *The Global Treasurer*. URL: https://www.theglobaltreasurer.com/2018/05/14/cargill-blockchain-shipping-transaction-cuts-exchange-time-to-24-hours (дата обращения: 06.02.2019).

30. Wüst, K., & Gervais, A. Do you Need a Blockchain? 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). Zug. 2018, pp. 45-54.

31. Hofmann E., Strewe U.M., Bosia N. Supply Chain Finance and Blockchain Technology. Berlin, Heidelberg: Springer, 2018.

32. European Commission. e-Invoicing. *European Commission.* URL: https://ec.europa.eu/growth/single-market/pub

lic-procurement/e-procurement/e-invoicing_en (дата обращения: 06.02.2019).

33. Ainsworth R., Alwohaibi M. Blockchain, Bitcoin and VAT in the GCC: the missing trader example. *Boston University School of Law. Law & Economics Working Paper*. 2018. No. 17-05.

34. Groopman J, Owyang J. The Internet of Trusted Things. *Kaleido Insight*. URL: http://www.kaleidoinsights.com/wp-content/uploads/2018/01/KI_Report_IoTBlockchain_FINAL.pdf (дата обращения: 06.02.2019).

35. Floyd D. Banks Claim They're Building Blockchains. They're Not. *Investopedia.* URL: https://www.investopedia.com/news/banks-building-blockchains-distributed-ledger-permission (дата обращения: 06.02.2019).

36. Allison I. Executives Are Leaving Blockchain Startup R3 in Management Shake-Up. *Coindesk.* URL: https://www.coindesk.com/2-executives-are-leaving-blockchain-startup-r3-in-management-shake-up (дата обращения: 06.02.2019).

References

1. Solow, R. (1987, 12 July). We'd better watch out. *The New York Times. Book Review*, p. 36.

2. Rosulek, M. (2017). 14 Bitcoin quotes by famous people. *Medium.* Retrieved from https://www.newsbtc.com/2014/03/16/google-chairman-eric-schmidt-bitcoin-architecture-amazing-advancement

3. Deen, M. (2018). Lagarde Says Cryptocurrency Mining Is Consuming Too Much Power. *Bloomberg.* Retrieved from https://www.bloomberg.com/news/articles/2018-01-25/lagarde-says-cryptocurrency-mining-is-consuming-too-much-power

4. Krugman, P. (2018, 21 July). Transaction Costs and Tethers: Why I'm a Crypto Skeptic. *The New York Times*.

5. Stinchcombe, K. (2017). Ten years in, nobody has come up with a use for blockchain. *Hackernoon.* Retrieved from https://hackernoon.com/ten-years-in-nobody-has-come-up-with-a-use-case-for-blockchain-ee98c180100

6. Davidson, S., De Filippi, P., & Potts, J. (2018). Blockchains and the Economic Institutions of Capitalism. *Journal of Institutional Economics*, 14 (4), pp. 639-658. doi: http://dx.doi.org/10.1017/S174413741700 0200.

7. Exonum (2018). Земельный кадастр на блокчейне. *Exonum*. Retrieved from https://exonum.com/ru/napr

8. Kniaziev, S. (2017). Development of smart industry as an efficient way to implement the policy of neoindustrialization in the world. *Econ. promisl.*, 4(80), pp. 5-18. doi: http://dx.doi.org/10.15407/econindustry 2017.04.005.

9. Babaoğlu, Ö., & Marzullo, K. (1996). Distributed Algorithms. Berlin, Germany: Springer.

10. Sterlin, L. (2017). Is Bitcoin at Risk as Google and IBM Aim for 50-Qubit Quantum Computers? *Bitcoin News.* Retrieved from https://news.bitcoin.com/is-bitcoin-at-risk-as-google-and-ibm-aim-for-50-qubit-quantum-computers

11. Mistry, N. (2015). Introduction to Bitcoin and ECDSA. *Slideshare.* Retrieved from https://www.slideshare.net/NikeshMistry1/introduction-to-bitcoin-and-ecdsa

12. Raval, S. (2016). Decentralized applications. Sebastopol, CA: O'Reilly Meida.

13. Deign, J. (2018). Bitcoin Mining Operations Now Use More Energy Than Ireland. Greentechmedia. Retrieved from https://www.greentechmedia.com/articles/read/bitcoin-uses-more-energy-than-ireland

14. Bashir, I. (2018). Mastering Blockchain. London, UK: Packt Publishing.

15. Surhone, L., Tennoe, M., & Henssonow, S. (2011). Paxos Algorithm. Saarbrücken, Germany. Betascript Publishing.

16. Raft (2016). Retrieved from https://raft.github.io

17. Dannen, C. (2017). Introducing Ethereum and Solidity. New York, USA: Apress.

18. Earls, J, Smith, M, & Smith, R. (2018). Smart Contracts: Is the Law Ready? *Chamber of Digital Commerce*. Retrieved from https://digitalchamber.org/smart-contracts-whitepaper.

19. Distributed Lab (2018). Введение в смарт-контракты. *Habr*. Retrieved from https://habr.com/ru/company/distributedlab/blog/413231 [in Russian].

20. Mukhopadhyay, M. (2018). Ethereum Smart Contract Development: Build blockchain-based decentralized applications using solidity. London, UK: Packt Publishing.

21. del Castillo, M. (2018). Big Blockchain: The 50 Largest Public Companies Exploring Blockchain. *Forbes.* Retrieved from https://www.forbes.com/sites/michaeldelcastillo/2018/07/03/big-blockchain-the-50-largest-public-companies-exploring-blockchain

22. Arnold, A. (2018). The 6 Major Blockchain Trends For 2018 Outlined By Deloitte. *Forbes.* Retrieved from https://www.forbes.com/sites/andrewarnold/2018/07/27/the-6-major-blockchain-trends-for-2018-outlined-by-deloitte

23. Ometoruwa, T. (2018). Solving the Blockchain Trilemma: Decentralization, Security & Scalability. *Coinbureau*. Retrieved from https://www.coinbureau.com/analysis/solving-blockchain-trilemma

24. Oraclize (2018). How it works. *Oraclize*. Retrieved from http://www.oraclize.it

25. Jordn, R. (2018). How to Scale Ethereum: Sharding Explained. *Medium.* Retrieved from https://medium.com/prysmatic-labs/how-to-scale-ethereum-sharding-explained-ba2e283b7fce

26. Lightning Network (2018). *Lightning Network.* Retrieved from https://lightning.network

27. Hyperledger (2018). Hyperledger Business Blockchain Technologies. *Hyperledger.* Retrieved from https://www.hyperledger.org

28. Corda (2018). Welcome to Corda. *Corda.* Retrieved from https://docs.corda.net

29. Noble, L. (2018). Cargill blockchain shipping transaction cuts exchange time to 24 hours. *The Global Treasurer*. Retrieved from https://www.theglobaltreasurer.com/2018/05/14/cargill-blockchain-shipping-transaction-cuts-exchange-time-to-24-hours

30. Wüst, K., & Gervais, A. (2017). Do you Need a Blockchain? 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), pp. 45-54.

31. Hofmann, E., Strewe, U. M., & Bosia, N. (2018). Supply Chain Finance And Blockchain Technology. Berlin, Heidelberg: Springer

32. European Commission. (2018). e-Invoicing. *European Commission.* Retrieved from https://ec.europa.eu/growth/single-market/public-procurement/e-procurement/e-invoicing_en

33. Ainsworth, R., & Alwohaibi, M. (2017). Blockchain, Bitcoin, and VAT in the GCC: the missing trader example. *Boston University School of Law. Law & Economics Working Paper* No. 17-05.

34. Groopman, J, & Owyang, J. (2018). The Internet of Trusted Things. *Kaleido Insight.* Retrieved from http://www.kaleidoinsights.com/wp-content/uploads/2018/01/KI_Report_IoTBlockchain_FINAL.pdf

35. Floyd, D. (2018). Banks Claim They're Building Blockchains. They're Not. *Investopedia.* Retrieved from https://www.investopedia.com/news/banks-building-blockchains-distributed-ledger-permission

36. Allison, I. (2019). Executives Are Leaving Blockchain Startup R3 in Management Shake-Up. *Coindesk.* Retrieved from https://www.coindesk.com/2-executives-are-leaving-blockchain-startup-r3-in-management-shake-up

Денис Володимирович Липницький,
канд. екон. наук
архітектор додатків, технічний тренер IBM
i-Klass Center LLC.
E-mail: denis.lipnitsky@i-klass.com
https://orcid.org/0000-0002-4616-7936

МОЖЛИВОСТІ ТА ВИКЛИКИ ДЛЯ БЛОКЧЕЙН У НОВІЙ ІНДУСТРІАЛІЗАЦІЇ

Індустрія 4.0 включає створення кіберфізичних систем, здатних децентралізовано керувати виробництвом, продажами, самонавчатися та розвиватися. Функціонування таких систем потребує аналогічних "розумних" технологій зберігання та поширення інформації. Блокчейн, забезпечивши децентралізацію та кібербезпеку у сфері криптовалют і створивши "розумні" контракти, став розглядатися як подібна технологія. Однак екстраполяція блокчейн із вузької сфери цифрових грошей до універсального застосування в індустрії та публічному секторі зіткнулася із серйозними труднощами. Частина з них можуть бути подолані в рамках удосконалення теперішньої генерації блокчейн (наприклад, удосконаленням алгоритмів консенсусу). Більшість же потребує суттєвих трансформацій технології, комбінування її з іншими інформаційними та промисловими інноваціями. Труднощі такого перехідного етапу призвели до критики блокчейн й інколи відмови від його використання. З'явилися гібридні рішення, що взяли від блокчейну лише частину інноваційної ідеї (блокову організацію реєстру транзакцій) й імплантувати її у традиційні технології. Запропоновано вважати такі рішення неповноцінним "квазіблокчейном". На основі аналізу еволюції блокчейну обґрунтовано, що розвиток його децентралізованих версій найбільшою мірою відповідає концепції Індустрія 4.0. Продемонстровано, що впровадженню таких версій зараз перешкоджають внутрішні протиріччя: "трилема" блокчейн плюс його висока енергоємність. Досліджено перспективи виходу із глухого кута "трилеми" блокчейн за допомогою суміжних інноваційних рішень, таких як протокол другого рівня (Lightning Network) тощо. Висвітлено тенденції подальшого розвитку форм та архітектур блокчейн. Запропоновано класифікацію, що зв'язує блокчейн із традиційними розподіленими базами даних й ураховує логіку їх розвитку. Проаналізовано найбільш ефективні методи промислового впровадження блокчейн, включаючи реалізацію за його допомогою цифрових рахунків-фактур (e-Invoice) і комунікацій для промислового Інтернету речей. Виконані дослідження дозволили розробити критерії вибору й оптимізації конкретних блокчейн-рішень для індустріального застосування.

Ключові слова: блокчейн, Індустрія 4.0, розподілений реєстр транзакцій, децентралізація, "трилема" блокчейн, "розумні" контракти, алгоритми консенсусу, e-Invoice, Інтернет речей, кібербезпека.

Denys V. Lypnytskyi,
PhD in Economics,
application architect, technical trainer IBM
i-Klass Center LLC.
E-mail: denis.lipnitsky@i-klass.com
https://orcid.org/0000-0002-4616-7936

OPPORTUNITIES AND CHALLENGES OF BLOCKCHAIN IN INDUSTRY 4.0

Concept of Industry 4.0 includes the creation of cyber-physical systems, capable to decentralized control over production, sales, etc., as well as self-education and self-development. Such systems' functioning requires similar "smart" technologies for information storing and distributing. Due to decentralization support, ensuring cybersecurity for cryptocurrency and creating environment for "smart" contracts, blockchain was considered as a fast solution. But blockchain's projection from the narrow scope of digital money to general purpose technology for industry and public sector faced serious difficulties. Some of them can be overcome by partial improving within the present generation of blockchain (e.g. – amending consensus' algorithms). Others require significant transformations of the core technology, coupling it with other innovations in computer science and industry. Difficulties of transition phase gave rise to criticism and even led to rejections to use blockchain in practice. Then some hybrid solutions appeared, which took only a part of blockchain's innovative idea (blocks-organized ledger) and implanted it onto old-fashioned technologies (abandoning the idea of distributed architecture). It is offered to consider such solutions as an inferior "quasi-blockchain". The evolution of blockchain has been studied and it has been proven that the development of its decentralized versions is most compatible with concept of Industry 4.0. However, industrial application of such versions, as it is shown in the paper, is hampered by the internal contradictions: blockchain "trilemma" plus inefficient energy use. Prospects for getting out of "blockchain trilemma" impasse have been explored, including some modern innovative solutions, such as the Level-2 protocol (Lightning Network). The evolution scenarios for such innovations are described. A classification, which links blockchain to classical distributed databases and takes into account the logic of their development, is proposed. The most promising fields for blockchain industrial applications, including digital invoices (e-Invoice) and Industrial Internet of Things, are studied. The research, conducted in the paper, has helped to develop a criteria to select and optimize specific blockchain solutions for industrial applications.

Keywords: blockchain, Industry 4.0, distributed leger, decentralization, blockchain "trilemma", "smart" contracts, consensus algorithms, e-Invoice, Internet of Things, cybersecurity.

JEL: O14, O31, O32.

Форматы цитирования:

Липницкий Д. В. Возможности и вызовы для блокчейн в новой индустриализации. *Экономика промышленности*. 2019. № 1(85). С. 82-100. doi: http://doi.org/10.15407/econindustry 2019.01.082

Lypnytskyi, D. V. (2019). Opportunities and challenges of blockchain in Industry 4.0. *Econ. promisl.*, 1(85), pp. 82-100. doi: http://doi.org/10.15407/econindustry2019.01.082

Представлена в редакцию 29.01.2019 г.