

DOI: 10.26794/2587-5671-2019-23-6-26-35

УДК 330.88:004.738.5:336.747.5(045)

JEL O33

Состояние и перспективы развития технологии блокчейн в финансовой сфере

Г.О. Крылов^а, В.М. Селезнёв^б^а Финансовый университет, Москва, Россия; ^а НИЯУ МИФИ, Москва, Россия;^б АО «Латкард», Рига, Латвия^а <https://orcid.org/0000-0001-8145-1994>; ^б <https://orcid.org/0000-0003-4521-0290>

АННОТАЦИЯ

В статье исследуются причины медленного внедрения технологии блокчейна в финансовой сфере. Авторы критически проанализировали основные декларируемые свойства блокчейн технологий: доверие, безопасность, децентрализация, неизменность хранения данных, отсутствие посредников, встроенная защита от атак, открытость. Цель исследования — показать, что декларируемые свойства блокчейна переоценены, ожидания от внедрения завышены, а задержки его адаптации за пределами криптовалют, в частности в финансовой сфере, закономерны. В основу статьи положена методология качественного и количественного анализа научных публикаций и статистических источников, посвященных адаптации блокчейна с позиции теории диффузии инноваций, условий достижения консенсуса и особенностей реализации экономико-социологических подходов к достижению консенсуса. В результате исследования сделаны следующие новые системные выводы. Блокчейн и распределенные реестры не являются принципиально новыми технологиями и в целом не обладают приписываемыми им свойствами неизменности хранения данных, достижения доверия, анонимности, низкой стоимости транзакций и дешевизны внедрения. Все существующие технологии консенсуса обладают фундаментальными недостатками. Технология криптовалют оригинальна, но была частным экспериментальным решением конкретной идеологической проблемы либертарианской политической повестки. Консенсус не обеспечивает доверия. Задержка внедрения блокчейна в традиционных финансовых институтах закономерна, поскольку технология не показывает результатов лучше, чем текущие цифровые решения, а традиционные экономические институты имеют большее общественное доверие. Практическая значимость выводов исследования заключается в том, что они могут быть использованы инвесторами.

Ключевые слова: цифровая экономика; блокчейн; базовая технология; консенсус; византийская проблема; доказательство работы; криптовалюта; доверие; смарт-контракт

Для цитирования: Крылов Г.О., Селезнёв В.М. Состояние и перспективы развития технологии блокчейн в финансовой сфере. *Финансы: теория и практика*. 2019;23(6):26-35. DOI: 10.26794/2587-5671-2019-23-6-26-35

Current State and Development Trends of Blockchain Technology in the Financial Sector

G.O. Krylov^а, V.M. Seleznev^б^а Financial University, Moscow, Russia; ^а National Research Nuclear University MEPhI, Moscow, Russia; ^б JSC LatCard,

Riga, Latvia

^а <https://orcid.org/0000-0001-8145-1994>; ^б <https://orcid.org/0000-0003-4521-0290>

ABSTRACT

The article analyzes the main reasons for the slow adoption of blockchain technology, in particular, in the financial sector. The authors critically analyzed the main declared properties of blockchain technologies: trust, security, decentralization, immutable data storage, lack of intermediaries, hardware protection against attacks, and openness. The aim of the study are to show that these blockchain properties are overestimated, the expectations of its adoption are inflated, and the delays in its adaptation outside of cryptocurrencies, in particular, in the financial sector, are natural. The article is based on a methodology for the qualitative and quantitative analysis of scientific publications and statistical sources on the

blockchain adaptation from the perspective of the theory of diffusion of innovations, the conditions and the specifics of economic and sociological approaches for consensus-building. The study resulted in the following new systemic findings. Blockchain and distributed ledgers are not fundamentally new technologies. In general, they do not have the properties of the immutable data storage, trust, anonymity, low transaction and adoption costs. All current consensus technologies have fundamental faults. Cryptocurrency technology is original, but it was a private experimental solution to a specific ideological problem of the libertarian political agenda. Consensus does not provide trust. Delayed blockchain adoption, in particular in traditional financial institutions, is natural, since the technology does not show better results than current digital solutions, and traditional economic institutions have greater public trust. The practical implications of the findings are that they may be used by investors.

For citation: Krylov G.O., Seleznev V.M. Current state and development trends of blockchain technology in the financial sector. *Finance: Theory and Practice*. 2019;23(6):26-35. DOI: 10.26794/2587-5671-2019-23-6-26-35

ВВЕДЕНИЕ

Очередной 2019 г., одиннадцатый с момента публикации манифеста биткойна, рынок блокчейна встретил с разнонаправленными трендами. Так, спекулятивный капитал потерял интерес к блокчейну. Вложения в блокчейн-стартапы упали с конца 2018 г. на 60%¹, а вложения в ICO с января по июнь 2019 г. упали в 17,8 раза относительно аналогичного периода 2018 г. (график вложений в ICO приведен на *рисунке*). При этом корпоративный сектор и стратегические инвесторы продолжили с энтузиазмом поддержку блокчейн-технологий, или, как сейчас принято говорить в корпоративном сегменте, технологий распределенного реестра.

Объявления о тестировании технологии или о стратегическом видении технологии блокчейн положительным образом влияют на капитализацию крупных компаний [1], и сегодня, похоже, нельзя иметь статус технологического лидера без инвестиций в блокчейн проекты². Вероятно, вышеприведенные факторы должны бы были свидетельствовать о начинающейся зрелости технологии, если бы не факт отсутствия сколь-нибудь массовой адаптации блокчейна за пределами биткойна и криптовалют. В этой статье мы проводим анализ причин медленной адаптации технологии (в частности, в финансовом секторе) и оправданности ожиданий от ее повсеместного внедрения.

ДЕКЛАРИРУЕМЫЕ СВОЙСТВА БЛОКЧЕЙНА

Один из наиболее значимых апологетов блокчейна крестный отец «цифровой экономики» Дон Тэпскотт

¹ По данным исследования CBInsights (CB Information Services). URL: <https://www.cbinsights.com/research/report/blockchain-trends-opportunities/> (дата обращения: 10.10.2019).

² Согласно опросу 1386 руководителей компаний с прибылью более 0,5 млрд долл. США, проведенному Deloitte зимой-весной 2019 г., 77% респондентов считают, что компания потеряет конкурентное преимущество, если не внедрит блокчейн. URL: <https://www2.deloitte.com/us/en/insights/topics/understanding-blockchain-potential/global-blockchain-survey.html> (дата обращения: 10.10.2019).

в своем opus magnum «Революция Блокчейна» (“The Blockchain Revolution”) [2] в наиболее общем виде сформулировал ожидания от внедрения блокчейна, поместив их в контекст глобальной цифровизации. Согласно Тэпскотту и прочим евангелистам технологии [3, 4], блокчейн позволит:

- создать новую экономику совместного потребления, где все экономические действия происходят без посредников;
- создать новую, полностью инклюзивную, быстродействующую финансовую систему с нулевыми накладными расходами;
- защитить экономические права по всему миру;
- полностью искоренить коррупцию и бюрократию;
- защитить авторские права (в широком смысле, права создателя) и креаторам получать вознаграждение напрямую;
- воспитать новый вид предпринимателя — блокчейн-предпринимателя и, трансформировав корпорации, создать новый честный капитализм;
- сделать высокотехнологичным все человеческое окружение, «оживив» и связав воедино все предметы;
- реализовать настоящую демократию от народа и для народа.

То есть, по мнению апологетов, блокчейн — это решение большинства насущных проблем человеческой цивилизации. В частности, для финансовых организаций предполагаются следующие выгоды от внедрения блокчейна:

- существенное сокращение затрат на IT-инфраструктуру путем упразднения бэк-офиса, который заменит блокчейн [5];
- снижение стоимости межбанковских расчетов;
- улучшение безопасности банковских данных;
- ускорение обработки транзакций;
- смарт-контракты позволят избежать ошибок и придадут новое качество финансовым услугам;
- банковский процесс станет более открытым и прозрачным [6].

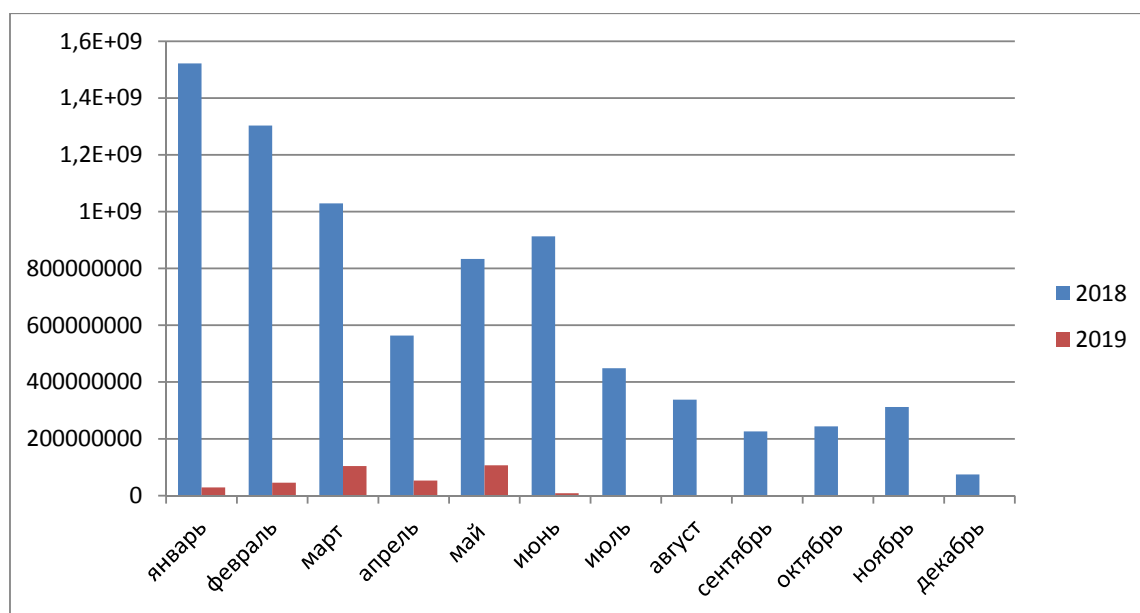


Рис. / Fig. Вложения в ICO в 2018–2019 годах (1-е полугодие) / ICO investments in 2018–2019 (the 1st half)

Источник / Source: авторская визуализация данных icodata.io* / data visualization by the author based on icodata.io data.

* Данные icodata.com. URL: <https://www.icodata.io/stats/2018>; <https://www.icodata.io/stats/2019> (дата обращения: 10.10.2019).

В основу данных прогнозов ставятся такие имманентные свойства технологии, как:

- отсутствие доверенной стороны (trustlessness);
- организация в виде одноранговой сети (peer-to-peer);
- встроенные криптографические механизмы безопасности;
- экономическая нецелесообразность атак на систему;
- анонимность;
- неизменное хранение данных;
- открытость и бесплатность.

Неудивительно, что эти обещания, сопровождаемые информационной поддержкой успеха первой криптовалюты биткоина, собрали 7,5 млрд долл. инвестиций с 2012 г., 4 млрд из которых были вложены в 2018 г.,³ что, как минимум, в 4 раза больше суммарных инвестиций в квантовые вычисления за сравнимый срок⁴. Так почему же при таком обильном финансировании внедрение блокчейна тормозит?

БЛОКЧЕЙН КАК «БАЗОВАЯ ТЕХНОЛОГИЯ»

Одно из наиболее популярных объяснений этого феномена состоит в том, что блокчейн объявляется

³ Данные Statista.com. URL: <https://www.statista.com/statistics/621207/worldwide-blockchain-startup-financing-history/> (дата обращения: 10.10.2019).

⁴ Данные CB Insights. URL: <https://www.cbinsights.com/research/report/quantum-computing/> (дата обращения: 10.10.2019).

базовой технологией (foundational technology) [7], поскольку «обладает потенциалом создать новую основу и принципы для наших экономических и социальных систем». В этом смысле блокчейн сравнивается с основным интернет-протоколом TCP/IP, а его основное приложение — криптовалюта с электронной почтой, которая была основным приложением TCP/IP в 1975 г.

По аналогии с развитием интернета строятся предсказания развития блокчейна. Сначала наступит период локальных частных решений, по аналогии с корпоративной электронной почтой, затем период замены традиционных приложений на приложения блокчейн, по аналогии с интернет-приложениями, и, наконец, произойдет переход количества в качество, и будет создана новая реальность, основанная на смарт-контрактах. Таким образом, согласно этой концепции, время прорыва пока просто не наступило, все что нужно, это просто ждать, экспериментируя с применением блокчейна в разных отраслях.

Однако объявление блокчейна потенциально базовой технологией и тезис о том, что «блокчейн — новый интернет», нам кажется существенным упрощением. Во-первых, достаточно легко убедиться (например, исследуя соответствующие статьи Wikipedia), что с самого момента создания интернет нашел огромное количество практических применений, кроме e-mail. Протоколы передачи файлов FTP и удаленного доступа к системам Telnet появились одновременно с e-mail и широко используются до сих пор. Электронные конференции Usenet появились спустя несколько лет после

почты, но именно они получили мгновенное мировое распространение, и именно в Usenet Тим Бернерс-Ли сообщил о создании www, сегодня основного сервиса интернета. И все это произошло менее чем за 10 лет от создания ТСП/IP.

Второе существенное упрощение — объявление базовой технологией собственно стека протоколов ТСП/IP. В исторической перспективе победа этого протокола, кстати, не удовлетворявшего теоретической модели взаимодействия сетей, была в значительной мере случайностью. Сетевые теоретики тогда предсказывали победы другим протоколам. При этом очевидно, что в равной степени и WWW и e-mail могли существовать и поверх протоколов других сетей, например X.25. Фундаментальной технологией, в случае проведения аналогий, следовало бы признать механизм коммутации пакетов.

Коммутация пакетов на момент создания, хотя и базировалась на предыдущих многолетних исследованиях и развитии давно заложенных концепций, тем не менее была новой технологией. Новизна же блокчейна вызывает сомнения. Собственно в биткойн-манифесте (первом блокчейн-документе) ни одной новой технологии нет. Все технологии, на которых построен блокчейн, давно известны. Базы данных, основанные на консенсусных алгоритмах (например Raft), практически используются с 1989 г. Дерево двоичных хэшей запатентовано Ральфом Мерклем в 1979 г. Алгоритм Hashcash опубликован в 1997 г., причем уже как система вознаграждения, правда для защиты от e-mail спама. А такой фундаментальный элемент современных блокчейн-технологий, как смарт-контракты, был предложен только в 2015 г. в связи с криптовалютой Ethereum. При этом вне контекста блокчейна смарт-контракты существовали еще с 1998 г. Таким образом, технологиям, лежащим в основе блокчейна в среднем более 25 лет. Будь они действительно базовыми, это достаточно большой срок, чтобы найти свое повсеместное применение.

ТЕОРИЯ ДИФфуЗИИ ИННОВАЦИЙ И ВНЕДРЕНИЕ БЛОКЧЕЙНА

Еще одним контраргументом против фундаментальности технологии является анализ с точки зрения теории диффузии инноваций. Общеизвестно, что за последний век прогресс внедрения технологий был подвержен непрерывному ускорению [8]. За 10 лет от начала коммерческой эксплуатации интернет был у 50% пользователей США, а общественное проникновение смартфонов в США от начала продажи первого смартфона до наличия смартфона у 90% населения потребовало всего 8 лет. За те же 10 лет охват населения США основным приложением блокчейна

криптовалютами достиг всего лишь 5%⁵, а в остальном мире криптовалютами пользуются менее 0,5% населения⁶. При этом, как уже отмечалось выше, общие мировые инвестиции в блокчейн весьма велики. И если воспользоваться кривой инноваций Эверетта Роджерса [9], то можно отметить интересный парадокс: инвестиции уже соответствуют уровню развития технологии «раннего большинства» [10, 11] при уровне практического проникновения технологии «новаторы». Иными словами, инвестиции не приводят к проникновению технологии. Что это, как не свидетельство отсутствия признака базовой технологии у блокчейна?

И, наконец, последнее возражение против того, что блокчейн это базовая технология, она не основана на научном прорыве [12]. Базовые технологии всегда следуют за научным прорывом: в математике или естественных науках. Разумеется, технологии блокчейн используют математическую основу, но эта технология не основана на прорывном решении математических проблем, более того, именно в нерешенность математической проблемы консенсуса ее развитие, собственно, и опирается.

ПРОБЛЕМА КОНСЕНСУСА В ТЕОРИИ УСТОЙЧИВОСТИ СИСТЕМ И СОЦИОЭКОНОМИЧЕСКИЙ ПОДХОД К ЕЕ ПРЕОДОЛЕНИЮ

Рассмотрим проблемы консенсуса подробнее, ведь на них основано такое преимущество блокчейна, как децентрализация. Лесли Лампорт сформулировал основную проблему, названную «проблемой византийских генералов», или «проблемой византийской устойчивости» (BFT), при анализе проблем устойчивости компьютерных систем [13]. Исследования проблемы показали, что ее решения существуют лишь в частных случаях. Консенсус, или «византийское соглашение», возможен лишь при конечном числе участников при условии, что злоумышленников в сети меньше, чем треть участников. А в любой асинхронной системе консенсус не гарантирован [14].

Доказано, что при возникновении возможности квантовых вычислений время достижения консенсуса с помощью квантового алгоритма будет константой [15]. Следовательно, практические алгоритмы дости-

⁵ По данным Bitcoin Market Journal. URL: <https://www.bitcoinmarketjournal.com/how-many-people-use-bitcoin/> (дата обращения: 10.10.2019).

⁶ Данные statista.com. URL: <https://www.statista.com/statistics/647374/worldwideblockchain-wallet-users/> (дата обращения: 10.10.2019).

жения консенсуса в компьютерных системах могут быть только приближительными и вероятностными. И здесь парадоксальный факт заключается в том, что решения самых популярных блокчейнов для достижения консенсуса не являются строго математическими решениями. Методы достижения консенсуса в них основаны на социоэкономических предположениях. Используемый биткоином и Ethereum метод «доказательства работы» (Proof of work, PoW) [16] полагается на гипотезу о том, что у людей, заинтересованных в «честном» функционировании системы, всегда будет больше вычислительной мощности, чем у каждого злоумышленника по отдельности. При этом заинтересованность в честности у участников сети будет обусловлена базовыми человеческими свойствами разумного эгоизма (иначе жадности), поскольку атаки двойным списанием будут обходиться экономически дороже, чем потенциально полученная выгода. И, наконец, предполагается, что сговор необходимых для атаки 51% «не жадных» участников невозможен, поскольку вычислительная мощность распределена между тысячами анонимных майнеров, которые полагают анонимность базовой ценностью. Увы, практика использования биткоина показала, что данные предположения не верны. Так, атаки двойным списанием и комбинацией двойного списания и атаки Сивиллы могут быть экономически целесообразны [17, 18]. Майнеров оказалось конечное и небольшое число, при этом их анонимность оказалась не ценностью, все основные майнинговые пулы известны. Кроме того, 70% майнинга контролируют всего 6 компаний, из них пять из Китайской Народной Республики⁷. То есть сговоры не только возможны, но и вполне вероятны.

Прекрасно понимая проблемы доказательства работы, блокчейн-сообщество активно ищет альтернативы этому протоколу. Например, Ethereum планирует перейти на алгоритм консенсуса «доказательства владения» (Proof-of-Stake). Увы, и этот протокол далеко не свободен от недостатков, поскольку разрушает децентрализацию сети и систему справедливого вознаграждения, так как привилегия принимать решения оказывается у самых богатых владельцев криптовалют, плюс к этому требуется внешний источник доверия для подтверждения «подлинной» истории транзакций [19]. Разумеется, предлагается множество и других практических консенсусных протоколов: Proof of Elapsed Time, Proof of Capacity, Delegated Proof-of-Stake, но все они в равной степени имеют недостатки, присущие эмпирическим решениям сложных математических проблем [20, 21].

⁷ По данным BTC.com. URL: https://btc.com/stats/pool?pool_mode=year (дата обращения: 10.10.2019).

БЛОКЧЕЙН: ПРОБЛЕМА ОПРЕДЕЛЕНИЯ

Комплексность и нерешенность математических проблем, связанных с блокчейном, дает в руки активных сторонников технологии еще одно объяснение задержки повсеместного внедрения. «Сложность» технологии для понимания простым человеком, по их мнению, не дает возможности объяснить людям важность ее потенциала [22]. Не будем спорить, некоторые элементы технологии требуют понимания основ прикладной математики, однако практика показывает, что объяснение принципов работы биткоина задача не слишком сложная. Сложности начинаются тогда, когда пытаются объяснить абстрактный блокчейн. Увы, хорошего определения, что же это такое блокчейн все еще не существует. Хотя большинство определений строится вокруг того факта, что блокчейн есть децентрализованный распределенный лог транзакций с консенсусом, основанным на принципе экономического вознаграждения в виде криптовалюты. Но сегодня далеко не все блокчейны являются децентрализованными, логом транзакций и основаны на криптоэкономических принципах.

Дополнительную путаницу создает современная тенденция вводить обобщающее определение «распределенный реестр» для проприетарных, непубличных эксклюзивных блокчейнов (или уже не блокчейнов по новому определению). Безусловно, трудно объяснить технологию, когда нет четкого ее определения.

БЛОКЧЕЙН КАК БАЗА ДАННЫХ С ОСОБЫМИ СВОЙСТВАМИ

Значительную путаницу вносит позиционирование блокчейна как распределенной базы данных. Строго говоря, блокчейн в подавляющем большинстве случаев (учитывая нечеткость определения) вообще не является базой данных, поскольку, во-первых, не хранит текущее состояние системы (т.е. не обладает свойством консистентности), а во-вторых, не обеспечивает доступность данных [23]. Блокчейн хранит только изменения состояний системы, т.е. является историческим журналом. В том же биткоине актуальная информация о состоянии счета хранится отдельно. Для оптимизации в подавляющем большинстве случаев блокчейны не хранят всю цепь, большинство узлов в том же биткоине хранит только заголовки блоков. Таким образом, система надеется, но не гарантирует своим дизайном, что полная информация блокчейна будет доступна. Поэтому не удивительно, например, что популярный блокчейн Ripple потерял первые 32 тысячи блоков. Просто никому не пришло в голову их сохранить!

Признание факта, что блокчейн не база данных, а журнал, позволило бы легче объяснить такое его декларируемое свойство, как возможность только добавления данных без их изменения. Свойство, вообще говоря, не столь полезное. (Какова при этом будет цена ошибки?). К счастью (или к несчастью) вопреки мнению апологетов данные блокчейна не являются неизменными *per se*. В отношении данных в публичных блокчейнах отмена операций вполне возможна по согласию сторон или в течение лимитированного периода, а в эксклюзивных распределенных реестрах по воле модерлирующей стороны.

Изменение самого блокчейна тоже вполне возможно как с помощью внешнего механизма, группой злоумышленников, для которых атака вполне может быть экономически целесообразна, так и с помощью внутреннего механизма, сговором большинства легальных майнеров. Более того, «легальные» откаты того же биткоина происходили по крайней мере трижды.

В общем, технологии блокчейна не столько сложны, сколько запутаны в упрощениях и неверных аналогиях. Плохие определения и умолчания при объяснениях наделяют технологию свойствами, которыми она не обладает, при этом ее фундаментальные недостатки покрываются дымовой завесой рекламного инфошума.

БЛОКЧЕЙН КАК ЧАСТНОЕ РЕШЕНИЕ ИДЕОЛОГИЧЕСКОЙ ПРОБЛЕМЫ ЛИБЕРТАРИАНСТВА

Следующий по значимости аргумент, объясняющий задержки внедрения блокчейна, это необходимость обучения как «блокчейн»-специалистов, так и массовое «народное» обучение блокчейну, что, конечно, требует времени [24]. Другими словами, для массового применения технологии буквально все должны постичь азы дискретной математики, прикладной криптографии и научиться составлять смарт-контракты. Должна сбыться, наконец, мечта пионера разработки персональных компьютеров, Стива Возняка, и все люди на Земле станут программистами. Увы, в реальном мире, наверное, эта мечта настолько же реалистична, как вера в то, что при настоящей демократии любой человек может быть сам себе адвокатом и успешно защищать себя в суде. В реальном мире даже профессиональные программисты, специалисты по блокчейну при первой же попытке применения смарт-контрактов, при создании инвестиционного консорциума The DAO допустили ошибку неоднозначности исполнения кода стоимостью в 60 млн долл. [25]. Так что вряд ли просвещение, даже в самом широком смысле, сможет продвинуть технологию в массы.

Зададим себе вопрос: может ли вообще стать массовой технология, которая изначально позиционировалась как экспериментальная и не претендовала на универсальность? Биткоин, декларирующий как базовые свойства анонимность и децентрализованность, был частным решением чисто идеологической проблемы криптоанархизма. Это радикальное течение либертарианской идеологии, в рамках которой давно исследовался вопрос о возможности существования независимых от государств платежных и денежных систем с частными центрами эмиссии [26]. При этом, собственно, проблемы с платежами у человечества нет с VI в. до н.э., с момента изобретения наличных денег. Поэтому не удивительно, что, будучи идеологическим продуктом, именно как деньги криптовалюты со своей высокой волатильностью оказались достаточно сомнительными [27].

ОСНОВНЫЕ ПРОБЛЕМЫ ТЕКУЩИХ РЕАЛИЗАЦИЙ БЛОКЧЕЙНА

Помимо высокой волатильности, признанными проблемами технологии являются: медленная скорость исполнения транзакций, большая энергоемкость, плохая масштабируемость [28, 29]. И действительно, в 2018 г. биткоин потреблял 47 Тв/час, что в два раза больше электрического потребления Ирландии. Скорость транзакций биткоина составляет около 7 тр/сек, а среднее время ожидания подтверждения транзакции 55 минут. Для сравнения, платежная система Visa обрабатывает 24 000 тр/сек, а среднее время ожидания 3 секунды. Причем преодоление этих проблем вряд ли возможно при сохранении децентрализации и открытости блокчейна, так как единственным практическим методом, обеспечивающим эти свойства, является энергозатратный Po W. Так что апелляция к скорости блокчейна достаточно смелое заявление. Вероятно, в США его считают быстрым относительно обработки платежных чеков, которые до сих пор составляют там 25% розничных платежей⁸, ведь национальная клиринговая система США NACHA ACH освоила платежи в тот же день только в 2016 г.

Учитывая вышеназванные проблемы, можно усомниться и в декларируемой экономии при внедрении блокчейна [30]. Консалтинговые фирмы обещают сокращение затрат на системы и инфраструктуру до 70%. Но они делают это в контексте общей цифровизации, сопровождаемой отказом от устаревших систем и модернизацией, что и без внедрения распределенных

⁸ По данным [creditcards.com](https://www.creditcards.com/credit-card-news/payment-method-statistics-1276.php). URL: <https://www.creditcards.com/credit-card-news/payment-method-statistics-1276.php> (дата обращения: 10.10.2019).

реестров очевидно сократит затраты. Да и цена хранения данных в распределенном реестре не вызывает особого энтузиазма даже при относительно высоких корпоративных ценах на классические базы данных. Среднему предприятию переход на «бесплатный» Hyperledger от IBM будет стоить около 140 тыс. долл.⁹, не считая затрат на внедрение.

ПРОБЛЕМА ДОВЕРИЯ К СИСТЕМАМ С ОТСУТСТВИЕМ ДОВЕРЕННОЙ СТОРОНЫ

И, наконец, наиболее ироничный фактор, являющийся тормозом распространения технологии. Исследование, проведенное консультантами PwC, показало, что основным сдерживающим фактором при внедрении блокчейна является отсутствие доверия [31]! Мир не доверяет технологии со встроенным «технологическим» доверием. Логично. Ведь с философской точки зрения консенсус не есть доверие. Консенсусные решения могут быть сколь угодно ошибочными и несправедливыми. Более того, генезис технологии происходит из идеологических установок радикальных революционеров, желающих переустроить мир и разрушить современный капитализм. Можем ли мы доверять анонимному большинству жадных анархистов? Не удивительно, что ни государственные институты, ни корпоративный мир не доверяют технологии, которая ставит целью разрушение современного мира.

В случае эксклюзивных блокчейнов ситуация с доверием становится еще более интересной. Сам факт создания частных эксклюзивных блокчейнов означает недоверие к публичным, с «технологическим» доверием. Потому что доверие к устоявшимся институтам выше, чем к анонимной толпе. Но, если мы доверяем условной IBM и ее аффилиатам, то возникают вопросы: зачем нам существенно более затратный и ограниченный распределенный реестр? почему бы просто не разместить свои данные в облаке доверенной компании и не подписать доверенную компанию как провайдера услуг криптографических сертификатов? Такое решение определенно будет быстрее и с лучше прогнозируемыми затратами. А если доверия нет, то как мы можем участвовать в проприетарном распределенном реестре, где доверие обеспечивается с участием стороны, которой мы не доверяем?

Чрезвычайно показательны слушания Сената США по поводу планов введения компанией Facebook крип-

⁹ По данным EY, Total cost ownership for blockchain solutions. 2019; Apr. URL: [https://www.ey.com/Publication/vwLUAssets/ey-total-cost-of-ownership-for-blockchain-solutions/\\$File/ey-total-cost-of-ownership-for-blockchain-solutions.pdf](https://www.ey.com/Publication/vwLUAssets/ey-total-cost-of-ownership-for-blockchain-solutions/$File/ey-total-cost-of-ownership-for-blockchain-solutions.pdf) (дата обращения: 10.10.2019).

товалюты Libra. Сенатор от Аризоны Марта МакСалли прямо заявила представителю компании Дейвиду Маркусу: «Я вам не доверяю, парни»¹⁰. Доверие хрупкая вещь, и даже флагман национальной экономики не может рассчитывать на специальное к себе отношение в этом плане.

Итак, подведем промежуточные итоги. Блокчейн на самом деле:

- не «новый интернет»;
- вероятно, обеспечивает консенсус, но не доверие;
- популярные консенсусные алгоритмы имеют недостатки, позволяющие злоумышленникам получить преимущества;
- не обеспечивает равноправного участия;
- не база данных и не обеспечивает неизменного вечного хранения данных.

АНОНИМНОСТЬ И БЕСПЛАТНОСТЬ БЛОКЧЕЙНА

Но, возможно, блокчейн является действительно анонимным и бесплатным? В общем случае, опять нет и нет. Большинство реализованных систем на блокчейне, начиная с биткоина, является всего лишь псевдоанонимными. Факт того, что криптокошелек не привязан к данным конкретного человека, не делает систему «анонимной». Реальные пользователи с высокой степенью достоверности вычисляются по метаданным, даже при использовании анонимайзеров и сети Tor, как спецслужбами, так и частными специалистами. При этом, в случае нелегальной деятельности, такое свойство блокчейна, как полная прозрачность транзакций, дает в руки правосудия однозначные неоспоримые доказательства [32].

Бесплатность блокчейна тоже всего лишь декларация. В США зарегистрированы более 1 тыс. патентов на распределенные реестры¹¹. Вряд ли ведущие финансовые и технологические компании патентуют технологии из альтруистических соображений. У таких компаний даже «бесплатные» технологии источник прибыли, и как мы видим, даже в области реестров с открытым исходным кодом идут корпоративные войны за контроль над технологическим контекстом, например между Intel и IBM за контроль над Hyperledger.

¹⁰ Цитируется постать: Katz M. The U.S. Senate really doesn't like Facebook's Libra cryptocurrency plans // digitaltrends.com, 2019; 16 Jul. URL: <https://www.digitaltrends.com/news/senate-facebook-libra-hearing-david-marcus/> (дата обращения 10.10.2019).

¹¹ По данным bitcoinmarketjournal.com. URL: <https://www.bitcoinmarketjournal.com/blockchain-patents/> (дата обращения: 10.10.2019).

БЛОКЧЕЙН И ТРАДИЦИОННЫЕ ИНСТИТУТЫ

Несмотря на то что единственным значимым применением блокчейна являются криптовалюты, им ни в коей мере не удалось пошатнуть классические финансовые институты. Традиционные банки с традиционным доверием к финансовой системе традиционного государства все еще лучше во всех аспектах¹². Попытки же практического внедрения технологий распределенного реестра в традиционной финансовой сфере, как и везде, по естественным, вышеприведенным причинам пока идут без особого успеха, так как, вопреки ожиданиям, технология не обеспечивает ни сокращения затрат на ИТ инфраструктуру, не снижает стоимость межбанковских расчетов и не ускоряет обработку транзакций. А такие декларируемые достоинства блокчейна, как безопасность путем использования публичной криптографии, распределенная БД и смарт-контракты вполне самостоятельные зрелые технологии, которые существуют независимо от блокчейна и могут быть внедрены в ИТ инфраструктуру финансовых организаций по отдельности [33]. Вероятно, именно поэтому наиболее успешная компания, декларирующая «межбанковские расчеты на блокчейне», Ripple, как выяснилось, для межбанковских расчетов использует традиционные инструменты, а не блокчейн¹³.

Регуляционные меры в банкинге и на финансовых рынках существуют не просто так, а для защиты инвесторов. Это не «жадность», а результат долгого развития государственных институтов.

Никакой блокчейн, кроме того, не заменит и не усилит институт демократических выборов. Голосование на блокчейне в равной степени не защищено от «вбросов», как и в случае использования традиционных урн. Как блокчейн может помочь, если потенциальный кандидат просто не допущен до демократического волеизъявления?

Системы логистики на блокчейне, как и традиционные, подвержены проблеме «мусор на входе, мусор на выходе». Например, систему отслеживания движения фруктов от производителя к покупателю

¹² По данным индекса доверия Эдельмана (Edelman Trust Barometer) в 2019 г. доверие к банкам/блокчейну/криптовалюте в среднем по всему населению Земли соответственно: 61 (доверие) / 55 (нейтральное отношение) / 35 (недоверие). URL: <https://www.edelman.com/trust-barometer> (дата обращения: 10.10.2019).

¹³ По данным Financial Times: Kelly J. Blockchain insiders tell us why we don't need blockchain. 2018; May 2. URL: <https://ftalphaville.ft.com/2018/05/02/1525253799000/Blockchain-insiders-tell-us-why-we-don-t-need-blockchain/> (дата обращения: 10.10.2019).

Walmart запустил в первый раз в 2006 г., отменил в 2009 г. и снова перезапустил в 2017 г., но уже на блокчейне [34]. Главной проблемой системы в 2006 г. был тот факт, что производители не хотят вводить в нее данные. Разумеется, внедрение блокчейна никак не решило эту проблему. При этом, как мы знаем, при известной настойчивости проблема маркировки продуктов легко решается традиционными средствами, примером чему служат российские системы ЕГАИС и Меркурий.

ВЫВОДЫ

Подводя итоги, хочется отметить, что чрезвычайно интересны социальные и культурологические аспекты возникновения «хайпа» вокруг темы блокчейна. Каким образом блокчейн-мания охватила серьезный бизнес? Каким образом на блокчейн возник социальный заказ? Как экспериментальное технологическое решение породило фактически сектантскую систему верований с чертами деструктивного культа?¹⁴ На эти вопросы еще предстоит ответить будущим исследователям, но уже сейчас есть основания полагать, что блокчейн в большей степени социальный феномен [35], чем рациональный [36].

Блокчейн и распределенные реестры не являются базовой технологией и в общем не обладают приписываемыми им свойствами неизменности хранения данных, достижения доверия, анонимности, низкой стоимости транзакций и дешевизной внедрения. Все существующие технологии консенсуса обладают фундаментальными недостатками. Технология криптовалют оригинальна, но была частным экспериментальным решением конкретной идеологической проблемы либертарианской политической повестки. Консенсус не обеспечивает доверия. Задержка внедрения блокчейна, в частности в традиционных финансовых институтах, закономерна, поскольку технология не показывает результатов лучше, чем текущие цифровые решения. Традиционные экономические институты имеют большее общественное доверие. Значительные вложения в блокчейн и распределенные реестры вряд ли скоро окупятся, но де факто гарантируют продолжение поиска применения технологии в различных областях человеческой деятельности, включая финансовую сферу.

¹⁴ В мае 2018 блокчейн предприниматель действительно создал религиозный культ «на блокчейне» под названием «0xΩ». URL: <https://www.americamagazine.org/politics-society/2019/06/14/can-technology-behind-bitcoin-be-used-build-belief-system> (дата обращения: 10.10.2019).

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Autore D.M., Clarke N., Jiang D. Bitcoin speculation or value creation? Corporate Blockchain investments and stock market reactions. *SSRN Electronic Journal*. 2019. DOI: 10.2139/ssrn.3385162
2. Tapscott D., Tapscott A. Blockchain revolution: How the technology behind Bitcoin and other cryptocurrencies is changing the world. New York: Portfolio; 2018. 432 p.
3. Swan M. Blockchain: Blueprint for a new economy. Sebastopol, CA: O'Reilly Media, Inc.; 2015. 152 p.
4. Mougayar W. The business Blockchain: Promise, practice, and application of the next Internet technology. Hoboken, NJ: John Wiley & Sons, Inc.; 2016. 209 p.
5. Fanning K., Centers D.P. Blockchain and its coming impact on financial services. *The Journal of Corporate Accounting & Finance*. 2016;27(5):53–57. DOI: 10.1002/jcaf.22179
6. Hassani H., Huang X., Silva E. Banking with Blockchain-ed big data. *Journal of Management Analytics*. 2018;5(4):256–275. DOI: 0.1080/23270012.2018.1528900
7. Iansiti M., Lakhani K.R. The truth about Blockchain. *Harvard Business Review*. 2017;95(1):118–127. URL: https://enterpriseproject.com/sites/default/files/the_truth_about_blockchain.pdf
8. McGrath R.G. The pace of technology adoption is speeding up. *Harvard Business Review*. 2013;(Nov.). URL: <https://hbr.org/2013/11/the-pace-of-technology-adoption-is-speeding-up>.
9. Rogers E.M. Diffusion of innovations. 3rd ed. New York, London: The Free Press; 1983.
10. Woodside J.M., Augustine F.K. Jr., Giberson W. Blockchain technology adoption status and strategies. *Journal of International Technology and Information Management*. 2017;26(2). URL: <http://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1300&context=jitim> (accessed on 10.10.2019).
11. Stratopoulos T.C., Wang V.X. Blockchain technology adoption. *SSRN Electronic Journal*. 2018. DOI: 10.2139/ssrn.3188470
12. Ahuja G., Lampert C.M. Entrepreneurship in the large corporation: A longitudinal study of how established firms create breakthrough invention. *Strategic Management Journal*. 2001;22(6–7):521–543. DOI: 10.1002/smj.176
13. Lamport L., Shostak R., Pease M. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems*. 1982;4(3):382–401. DOI: 10.1145/357172.357176
14. Fischer M., Lynch N., Paterson M. Impossibility of distributed consensus with one faulty process. *Journal of the ACM*. 1985;32(2):374–382. DOI: 10.1145/3149.214121
15. Ben-Or M., Hassidim A. Fast quantum Byzantine agreement. In: STOC'05. Proc. 37th Annu. ACM symp. on theory of computing (Baltimore, MD, May 22–24, 2005). New York: ACM; 2005:481–485. DOI: 10.1145/1060590.1060662
16. Krawisz D. The proof-of-work concept. Satoshi Nakamoto Institute. 2013. URL: <https://nakamotoinstitute.org/mempool/the-proof-of-work-concept/> (accessed on 10.10.2019).
17. Bissias G., Levine B.N., Ozisik A.P., Andresen G. An analysis of attacks on Blockchain consensus. URL: <https://arxiv.org/pdf/1610.07985.pdf> (accessed on 10.10.2019).
18. Zhang S., Lee J.-H. Double-spending with a Sybil attack in the Bitcoin decentralized network. *IEEE Transactions on Industrial Informatics*. 2019;15(10):5715–5722. DOI: 10.1109/TII.2019.2921566
19. Demeester T. Critique of Buterin's "A proof of stake design philosophy". Medium. 2017. URL: <https://medium.com/@tuurdemeester/critique-of-buterins-a-proof-of-stakedesign-philosophy-49fc9ebb36c6> (accessed on 10.10.2019).
20. Zhang S., Lee J.-H. Analysis of the main consensus protocols of Blockchain. *ICT Express*. 2019;5(3). DOI: 10.1016/j.icte.2019.08.001
21. Wahab A., Memood W. Survey of consensus protocols. 2018. URL: <https://arxiv.org/ftp/arxiv/papers/1810/1810.03357.pdf> (accessed on 10.10.2019).
22. Grewal-Carr V., Marshall S. Blockchain: Enigma. Paradox. Opportunity. Deloitte. 2016. URL: <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf> (accessed on 10.10.2019).
23. Stolfi J. Letter to the Editor, NIST Reports. Ref: NISTIR 8202 (DRAFT): Blockchain Technology Overview. 2018. URL: <https://www.ic.unicamp.br/~stolfi/temp/nist-report-review.pdf> (accessed on 10.10.2019).
24. Radocchia S. What's holding Blockchain back from large-scale adoption? Forbes. Sept. 21, 2017. URL: <https://www.forbes.com/sites/quora/2017/09/21/whats-holding-blockchain-back-from-large-scale-adoption> (accessed on 10.10.2019).
25. Castillo M. The DAO attacked: Code issue leads to \$ 60 million ether theft. Coindesk. June 18, 2016. URL: <https://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-theft> (accessed on 10.10.2019).
26. Karlstrøm H. Do libertarians dream of electric coins? The material embeddedness of Bitcoin. *Distinktion: Scandinavian Journal of Social Theory*. 2016;15(1):23–36. DOI: 10.1080/1600910x.2013.870083

27. Крылов Г.О., Лисицын А.Ю., Поляков Л.И. Сравнительный анализ волатильности криптовалют и фиатных денег. *Финансы: теория и практика*. 2018; 22(2):66–89. DOI: 10.26794/2587–5671–2018–22–2–66–89
Krylov G. O., Lisitsyn A. Y., Polyakov L. I. Comparative analysis of volatility of cryptocurrencies and fiat money. *Finansy: teoriya i praktika = Finance: Theory and Practice*. 2018; 22(2):66–89. (In Russ.). DOI: 10.26794/2587–5671–2018–22–2–66–89
28. Goswami S. Scalability analysis of Blockchains through Blockchain simulation. UNLV Theses, Dissertations, Professional Papers, and Capstones. 2017;(2976). URL: https://pdfs.semanticscholar.org/108f/9d7493fecd7cdb1a2a123d89a4db16b79679.pdf?_ga=2.210275989.1023187009.1572354254-1709531060.1571930732 (accessed on 10.10.2019).
29. Truby J. Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies. *Energy Research & Social Science*. 2018;44:399–410. DOI: 10.1016/j.erss.2018.06.009
30. Bloomberg J. Don't let Blockchain cost savings hype fool you. *Forbes*. Feb. 24, 2018. URL: <https://www.forbes.com/sites/jasonbloomberg/2018/02/24/dont-let-blockchain-cost-savings-hype-fool-you/#3b47f4f45811> (accessed on 10.10.2019).
31. Davis S. Likens S. Blockchain is here. What's your next move? *Pw C*. 2018. URL: <https://www.pwc.com/gx/en/issues/blockchain/blockchain-in-business.html> (accessed on 10.10.2019).
32. Bohannon J. Why criminals can't hide behind Bitcoin. *Science*. March 09, 2016. DOI: 10.1126/science.aaf4167
33. Halaburda H. Blockchain revolution without the Blockchain? *Communications of the ACM*. 2018;61(7):27–29. DOI: 10.1145/3225619
34. Stinchcombe K. Blockchain is not only crappy technology but a bad vision for the future. *Medium*. Apr. 5, 2018. URL: <https://medium.com/@kaistinchcombe/decentralized-and-trustless-crypto-paradise-is-actually-amedieval-hellhole-c1ca122efdec> (accessed on 10.10.2019).
35. Albrecht S., Lutz B., Neumann D. How sentiment impacts the success of Blockchain startups: An analysis of social media data and initial coin offerings. In: *Proc. 52nd Hawaii int. conf. on system sciences*. 2019:4545–4554. URL: <https://scholarspace.manoa.hawaii.edu/bitstream/10125/59892/0452.pdf> (accessed on 10.10.2019).
36. Lee C.C., Kriscenski J.C., Lim H.S. An empirical study of behavioral intention to use Blockchain technology. *Journal of International Business Disciplines*. 2019;14(1):1–21. URL: <https://faculty.utrgv.edu/louis.falk/jibd/JIBDmay19.pdf> (accessed on 10.10.2019).

ИНФОРМАЦИЯ ОБ АВТОРАХ / ABOUT THE AUTHORS



Григорий Олегович Крылов — доктор физико-математических наук, кандидат технических и юридических наук, профессор кафедры информационной безопасности, Финансовый университет, Москва, Россия; профессор НИЯУ МИФИ, заслуженный работник высшей школы, Москва, Россия

Grigorii O. Krylov — Dr. Sci. (Phys.-Math.), Cand. Sci. (Engin.), Cand. Sci. (Juris.), Professor, Department of Information Security, Financial University, Moscow, Russia; Professor at National Research Nuclear University MEPhI, Honorary Figure of Russian Higher Education, Moscow, Russia
nik155@yandex.ru



Владимир Михайлович Селезнёв — кандидат технических наук, магистр бизнес-менеджмента, член правления АО «Латкард» (финансовая организация электронных денег), Рига, Латвия

Vladimir M. Seleznev — Cand. Sci. (Engin.), MBM, Member of the Board, JSC LatCard (Electronic money financial institution), Riga, Latvia
v_seleznev@pisem.net

Статья поступила в редакцию: 02.09.2019; после рецензирования: 11.09.2019; принята к публикации 20.10.2019.
Авторы прочитали и одобрили окончательный вариант рукописи.

The article was submitted on 02.09.2019; revised on 11.09.2019 and accepted for publication on 20.10.2019.

The authors read and approved the final version of the manuscript.