ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/2587-5671-2020-24-5-84-99
УДК 336.012.23,336.018,336.711.2,336.741.2(045)
JEL A10, B53, E40, E42, E44

Институциональные особенности разработки конкурентоспособной криптовалюты

В.П. Бауэр[a], **В.В. Смирнов**[b] ✉
Финансовый университет, Москва, Россия
[a] https://orcid.org/0000-0002-6612-3797; [b] http://orcid.org/0000-0003-0753-2520
✉ Автор для корреспонденции

АННОТАЦИЯ

Цель статьи — уточнить основы цифровизации конкурентоспособного бизнеса и определить особенности институциональной среды, в которой разрабатывается криптовалюта как новый актив (IT-продукт) современной экономики, анализируются методы реализации на практике бизнес-моделей криптовалют. **Актуальность** статьи определена тем, что в условиях роста числа частных, государственных и межгосударственных криптовалют становится актуальной разработка конкурентоспособной российской криптовалюты (в том числе, крипторубля). **Научная новизна** статьи заключается в уточнении неформальных и формальных правил институциональной среды и связанных с ними методов, которые обеспечивают разработку конкурентоспособной криптовалюты. Показано, что в бизнес-моделях криптовалют институциональные особенности их разработки реализуются следующими **методами**: логикой и алгоритмом блокчейна, обеспечивающими условия доверия и коллаборации разработчиков криптовалют; логикой и алгоритмом консенсуса блокчейна, реализующими компромисс взаимодействия между участниками оборота криптовалют; логикой и алгоритмами, формирующими транзакции криптовалют и защиты их оборота, в том числе, за счет: генерации блоков криптовалют; формирования структуры блоков и транзакций криптовалют; криптографической защиты и хранения ключей криптовалют; майнинга (форжинга) криптовалют и др. В **результате** исследования выявлены институциональные особенности и соответствующие им методы, обеспечивающие разработку конкурентоспособной криптовалюты с детальным анализом логики алгоритмов консенсуса блокчейна, вносящих один из основных вкладов в обеспечение ее конкурентоспособности. Сделан **вывод**, что наиболее перспективными являются гибридные алгоритмы консенсуса, которые могут включать в себя как логику двух или более известных алгоритмов, так и оригинальную логику нового алгоритма. Авторы **рекомендуют** при разработке криптовалюты в первую очередь определить логику алгоритма консенсуса блокчейна, которая обеспечивает решение задачи византийских генералов, предотвращающих поведение не лучшим образом функционирующих транзакций сети и повышающих за счет этого конкурентоспособность криптовалюты.

Ключевые слова: институциональная среда; формальные и неформальные правила институциональной среды; конкуренция; криптовалюта; бизнес-модель; блокчейн; логика; алгоритм; консенсус

Для цитирования: **Бауэр В.П., Смирнов В.В. Институциональные особенности разработки конкурентоспособной криптовалюты. *Финансы: теория и практика.* 2020;24(5):84-99. DOI: 10.26794/2587-5671-2020-24-5-84-99**

ORIGINAL PAPER

Institutional Features of the Development of Competitive Cryptocurrency

V.P. Bauer[a], **V.V. Smirnov**[b] ✉
Financial University, Moscow, Russia
[a] https://orcid.org/0000-0002-6612-3797; [b] http://orcid.org/0000-0003-0753-2520
✉ Corresponding author

ABSTRACT

The **aim** of the article is to clarify the basics of the digitalization strategy of the competitive businesses and identify features of the institutional environment that ensure the development of cryptocurrency as a new asset (IT product) of the modern economy, analyze the methods of implementing the cryptocurrency business models. The **relevance** of the research paper is determined by the need to develop a competitive Russian cryptocurrency (including the crypto-ruble) with the growing private, state and cross-national cryptocurrencies. The **scientific novelty** of the study implies clarifying the informal and formal rules of the institutional environment and related methods ensuring the development of a competitive cryptocurrency. The authors consider the following **methods** to implement the institutional features of the cryptocurrencies business model development: logic and blockchain algorithm that establish trust and

collaboration between cryptocurrency developers; logic and blockchain consensus algorithm ensuring that all the parties of the blockchain network come to a common agreement (consensus); logic and blockchain algorithms that form cryptocurrency transactions and control its turnover by generating blocks of cryptocurrencies, by forming the structure of blocks and transactions of cryptocurrencies, by storing cryptocurrencies' keys and providing security, by mining (forging) cryptocurrency, etc. The **results** of the study provide a basis for identifying the institutional features and the corresponding methods providing a competitive cryptocurrency development with a detailed analysis of the blockchain consensus algorithms that ensure the competitiveness of the cryptocurrency. The **conclusions** show that the most promising are the hybrid consensus algorithms which may include both the logic of two or more known algorithms and the original logic of a new algorithm. The authors **recommend** defining the logic of the blockchain consensus algorithm as a priority when developing a cryptocurrency to ensure reliability of the transactions in the blockchain network, thus increasing the competitiveness of the cryptocurrency.
Keywords: institutional environment; formal and informal rules of the institutional environment; competition; cryptocurrency; business model; blockchain; logic; algorithm; consensus

For citation: **Bauer V.P., Smirnov V.V. Institutional features of the development of competitive cryptocurrency. *Finance: Theory and Practice*. 2020;24(5):84-99. (In Russ.). DOI: 10.26794/2587-5671-2020-24-5-84-99**

ВВЕДЕНИЕ

Первая криптовалюта «биткойн» появилась в 2009 г. на основе разработанного Сатоши Накамото алгоритма блокчейна [1], реализующего тезис о свободе творческой личности в информационном обществе от опеки государства и его регуляторов [2]. Этот тезис в 90-е гг. прошлого века выдвинули шифропанки[1] и криптоанархисты [3, 4], но, как показал П.И. Талеров [5], он тесно связан с дискуссиями XIX и XX вв. о важности рыночной конкуренции между анархистами и экономистами. Примечательно, что одним из результатов дискуссии стало выдвинутое российским анархистом П.А. Кропоткиным и принятое научным сообществом положение о том, что в природе, кроме закона всемирной борьбы за существование, действует и другой фундаментальный закон — всемирной взаимопомощи [6].

Развитие цифровых финансовых активов изменило международный мир финансов [7] и вызвало становление эры криптовалют [8], а исследования особенностей криптовалют определили их как новый финансовый актив [9].

В условиях массового появления частных [10–12], государственных (Япония[2], Китай[3,4]) и межгосударственных (в рамках БРИКС[5,6]) криптовалют и активной цифровизации российского общества[7] в стране назрел вопрос о разработке российской конкурентоспособной криптовалюты, например крипторубля [13, 14]. Результаты анализа проблемы показали, что для ее решения необходимо выявить особенности институциональной среды, формирующие криптовалюту как конкурентоспособный актив цифровой экономики, и определить методы их реализации на практике.

КОНКУРЕНЦИЯ И КОНКУРЕНТОСПОСОБНОСТЬ ИНФОРМАЦИОННЫХ (IT)-ПРОДУКТОВ

Современный энциклопедический словарь дает следующее определение конкуренции: «...конкуренция (от *позднелат. concurentia, concurrere — сталкиваться*), соперничество, соревнование людей, групп, организаций в достижении сходных целей, лучших результатов в определенной общественной сфере. Конкуренция — существенная черта различных видов деятельности, в которых происходит столкновение интересов (политика, экономика, наука, спорт и др.)»[8].

---

[1] May T.C. The Crypto Anarchist Manifesto. Nov. 92. URL: https://www.activism.net/cypherpunk/crypto-anarchy.html (дата обращения: 15.05.2020).

[2] В Японии криптовалюта получила статус платежного средства. URL: http://tass.ru/ekonomika/4144338 (дата обращения: 15.05.2020).

[3] Доренков И. Власти Китая форсируют запуск цифрового юаня. URL: https://news.crypto.pro/vlasti-kitaja-forsirujut-zapusk-cifrovogo-juanja/ (дата обращения: 15.05.2020).

[4] Балоян С. Китай запускает государственную криптовалюту: как это может изменить финансовый мир. URL: https://vc.ru/finance/122749-kitay-zapuskaet-gosudarstvennuyu-kriptovalyutu-kak-eto-mozhet-izmenit-finansovyy-mir (дата обращения 15.05.2020).

[5] Goncharov A.I., Goncharova M.V. Digital Tokens in the Tools of Modern Foreign Trade Activities by Economic Entities of the BRICS Jurisdictions. Legal Concept. 2019;18(3):31–42. DOI: 10.15688/lc.jvolsu.2019.3.5

[6] Grigoryeva Y. BRICS Token: New Wave in International Payment System. URL: http://infobrics.org/post/30179/ (дата обращения: 15.05.2020).

[7] Цифровая Россия: новая реальность. Digital McKinsey. URL: https://www.mckinsey.com/ru/~/media/McKinsey/Locations/Europe%20and%20Middle%20East/Russia/Our%20Insights/Digital%20Russia/Digital-Russia-report.ashx (дата обращения: 15.05.2020).

[8] Конкуренция. Современный энциклопедический словарь. URL: http://www.вокабула.рф/энциклопедии/современный-энциклопедический-словарь/конкуренция (дата обращения: 15.05.2020).

В монографии Е. В. Дробота отмечается, что «…конкуренция — одно из основных свойств рыночной экономики. Именно конкуренция обязывает социально и юридически свободную личность к творческой деятельности, создает условия для самореализации личности в сфере экономики в форме разработки новых конкурентоспособных товаров и услуг» [15].

Неотъемлемой частью конкуренции является конкурентоспособность продукции, определяемая как «…способность продукции быть привлекательной по сравнению с другими изделиями аналогичного вида и назначения, благодаря лучшему соответствию своих характеристик требованиям данного рынка и потребительским оценкам. Характеристики товара определяют его потребительские свойства, которые, в свою очередь, включают ряд показателей качества этого товара. Конкурентоспособность товара зависит как от отдельного показателя, так и их совокупности (синергия). Конкурентоспособность товара обеспечивается конкурентными позициями, которые занимают фирмы, производящие и распространяющие товар. Показатели, характеризующие конкурентоспособность товара < … >, представляют набор „жестких" и „мягких" показателей < … >. „Жесткие" показатели обеспечивают физическую возможность использования товара по назначению и подразделяются на следующие группы: технические < >, эргономические < … >, технологические < … > и нормативные < … >. „Мягкие" показатели характеризуют эстетические < … > и психологические < … > свойства товара»[9].

С учетом данного определения конкурентоспособности продукции под конкурентоспособностью криптовалюты будем понимать следующее.

Во-первых, конкурентоспособная криптовалюта должна иметь новое потребительское свойство, которое формирует, в отличие от существующих криптовалют, ее полезный эффект. Как будет показано ниже, это свойство обеспечивается применением специфических «жестких» и «мягких» правил институциональной среды, в которой осуществляется ее разработка.

Во-вторых, криптовалюта должна иметь характеристики, которые обеспечивают ее конкурентоспособность среди прочих криптовалют. Однако, как показано в работах [16, 17], рыночные аспект конкурентоспособности криптовалюты требует исследований правил функционирования институциональной среды крипторынка в целом, поэтому в данной статье не рассматривается.

Исследования выявили, что на практике можно использовать два принципа разработки конкурентоспособной продукции: системный и процессный [18, 19]. В первом случае присутствует конкурентная среда [20], способствующая разработке продукции. Во втором случае формируются рыночные [21] и межфирменные процессы [22] или межорганизационные структуры [23, 24], способствующие этому же процессу. Причем в работе Ю. В. Таранухи показано, что развитие экономических отношений в современных условиях приводит к эволюции и модификации указанных принципов [25].

Вопросы разработки конкурентоспособного IT-продукта проанализированы в работе Н. М. Розановой и И. В. Линевой [26]. Авторы полагают, что «…конкурентоспособный IT-продукт — инструмент современного бизнеса для трансформации традиционной бизнес-модели в цифровую модель». Авторы считают, что «…важный аспект конкурентоспособности IT-продукта остается прежним: что производить и согласно каким формализованным правилам?». Исходя из этих предпосылок, авторы резюмируют, что «…конкурентоспособный IT-продукт — инструмент современного бизнеса для трансформации традиционной бизнес-модели в цифровую модель», или, более того «…конкурентоспособный IT-продукт — цифровая модель современной компании, взаимодействующая с его ключевыми составляющими: мобильными устройствами, большими данными, облачными платформами».

Для того чтобы выявить, по каким правилам (неформальным и формальным) необходимо создавать такой конкурентоспособный IT-продукт, как криптовалюта, рассмотрим структуру и состав институциональной среды и методы, способствующие решению данной проблемы.

ПРАВИЛА ИНСТИТУЦИОНАЛЬНОЙ СРЕДЫ, ОПРЕДЕЛЯЮЩИЕ ПРАКТИКИ И МЕТОДЫ РАЗРАБОТКИ КОНКУРЕНТОСПОСОБНОЙ КРИПТОВАЛЮТЫ

В настоящее время доступна достаточно скромная библиография по вопросу формирования институциональной среды, способствующей разработке конкурентоспособной продукции. Так, в работе Р. Р. Нуреевой и ее коллег [27] данный вопрос исследуется исключительно на макроуровне. В работе И. А. Иваненко и Ф. Н. Саифидиновой [28] исследование институциональной среды увязывается с оценками нестабильности

[9] Конкурентоспособность товара. Википедия. URL: https://ru.wikipedia.org/wiki/Конкурентоспособность_товара (дата обращения 25.05.2020).

экономической ситуации, возникающими в условиях конкуренции в рыночной среде. Наиболее исчерпывающе вопрос формирования институциональной среды в условиях конкуренции исследован в монографии А.Х. Хакимова [29]. Автор изучает вопросы влияния институциональной среды на управление конкурентоспособностью предпринимательских структур в условиях интеграционных процессов рыночной среды. В работе А. Ф. Гришкова [30] обосновывается, что предприятия в целях управления конкурентоспособностью в условиях сложной институциональной среды должны разрабатывать и использовать программно-аппаратные средства динамического мониторинга и корректировки факторов конкурентоспособности.

В работах Д.Е. Сорокина [31, 32] показано, что на формирование институциональной среды современного российского общества существенное влияние оказывают не только формальные, но и неформальные правила и практики. При разработке криптовалют актуальность данной точки зрения подтверждается фактами использования такого рода правил и практик различного состава и содержания венчурными предпринимателями [33], представителями различного рода предпринимательских структур [34] и разработчиками цифровых платформ [35].

Выше было показано, что характеристики конкурентоспособности любого товара представляют собой набор «жестких» и «мягких» показателей. Определим в нашем контексте соответствующий набор «жестких» и «мягких» правил институциональной среды и методов их реализации на практике.

В исследовании будем исходить из того, что «жесткие» показатели должны обеспечивать физическую возможность использования товара по назначению. Тогда к «жестким» правилам институциональной среды в первую очередь необходимо отнести технологические решения и нормативные требования, способствующие разработке криптовалюты как одной из разновидности IT-продукта. На практике указанные правила включают в себя строгие логические методы разработки алгоритмов бизнес-моделей криптовалют и стандартизованные языки программирования, на основе которых идет разработка алгоритмов этих бизнес-моделей. Следует отметить, что вопросы программирования алгоритмов не входят в предмет исследования данной статьи.

Что касается поиска аналогов «мягких» показателей конкурентоспособности криптовалют, то к ним мы отнесем как психологические, так и этические правила взаимодействия участников институциональной среды, в которой, с одной стороны, создается криптовалюта (разработчики криптовалюты), а с другой стороны, происходит ее обращение (пользователи криптовалюты).

В первом случае особый интерес вызывают подходы к формированию команды, создающей криптовалюту. Здесь особую популярность приобрели Agile-метод гибкого управления инновационными разработками [36] и связанная с ним методология программирования Scrum [37]. Цель Agile-метода заключается в использовании формальных и неформальных правил в отношениях между членами команды разработчиков для создания в кратчайшие сроки конкурентоспособного IT-продукта, в том числе по методологии Scrum.

Конкурентоспособная криптовалюта должна иметь новое потребительское свойство, которое формирует, в отличие от существующих криптовалют, ее полезный эффект.

В рамках Agile-метода в институциональную среду разработчиков криптовалюты входят следующие ключевые элементы: определение состава участников и достижение соглашения о совместной деятельности; формирование миссии команды; установление границ доверия между участниками; определение целей, задач и сфер интересов; установление границ взаимодействия; выделение ключевых факторов успеха и контрольных точек их достижения; оценка ресурсов; выявление способностей в процессе разработки, их оценка и, при необходимости, корректировка состава команды; подведение итогов совместной работы; расформирование команды.

В рамках методологии Scrum разработка криптовалюты реализуется на практике следующими основными методами:

- логикой и алгоритмом блокчейна, обеспечивающими условия доверия и коллаборации в инновационной цифровой экономике [38] между разработчиками и пользователями криптовалют [39, 40];
- логикой и алгоритмом консенсуса блокчейна, которые решают проблему децентрализации

оборота криптовалют за счет обеспечения компромисса взаимодействия между транзакциями[10];

- логикой и алгоритмами, формирующими транзакции криптовалют и защиты их оборота, в том числе генерацию блоков криптовалют, формирование структуры блоков и транзакций и др. [41];
- логикой и алгоритмами криптографической защиты и хранения ключей криптовалют [42];
- логикой и алгоритмами майнинга [43] (форжинга[11]) криптовалют и др.

Исследования вопросов рыночной конкурентоспособности криптовалюты показали, что, во-первых, майнинг и форжинг — это процессы, без которых эмиссия криптовалют невозможна [44]. Во-вторых, определяющую роль в производительности транзакций имеет логика алгоритмов консенсуса [45]. В связи с этим рассмотрим данный вопрос более подробно.

АНАЛИЗ ЛОГИКИ АЛГОРИТМОВ КОНСЕНСУСА В БЛОКЧЕЙНЕ

Алгоритм консенсуса блокчейна является одним из наиболее важных механизмов в разработке криптовалют. Исследования российских патентоведов выявили, что в настоящее время в международном патентном ландшафте алгоритм консенсуса входит в состав практически всех наиболее цитируемых патентов, защищаемых в сфере криптовалют [46]. В общем случае консенсус — это механизм разрешения конфликтов в группе участников, задействованных в решении проблемы реализации транзакций группы участников. Группа участников должна проявить солидарность и согласие в решении проблемы выполнения транзакции. В блокчейне не реализованы принципы распределенного консенсуса, поэтому они реализуются сторонними технологиями, которые обычно применяются в системах распределенных баз данных и др. Логика работы распределенного консенсуса в блокчейне отлична от логики консенсуса в базах данных тем, что она имеет сетевой характер. В консенсусах баз данных всегда известно количество узлов, участвующих в транзакции. В консенсусе блокчейн-узлы, участвующие в транзакции, могут выбираться динамически. Поведение участников сети, в которой реализуется распределенный консенсус, описывается задачей «византийских генералов»[12]. Эта задача была сформулирована Лэмпортом, Шостаком и Пизом в 1982 г. прошлого века [47], решение было найдено в конце 90-х гг. Алгоритм консенсуса включает в себя набор логических правил в блокчейне криптовалюты, в котором определено, кто и при каких условиях может подтверждать транзакции, добавлять новые блоки и осуществлять прочие логические действия [48].

Логика алгоритмов консенсуса обеспечивает принятие автоматизированного решения в криптосистеме путем реализации следующих основных правил взаимодействия пользователей криптовалют:

- согласование: достижение максимальной степени согласия взаимодействующих сторон;
- эгалитаризм: соблюдение равноправия, равенства участников;
- кооперативность: участники заинтересованы работать сообща;
- инклюзивность: в процессе достижения консенсуса должно быть максимальное количество участников.

Стоит отметить, что консенсусом называют не только сам процесс принятия решения, но и принятое в результате такой процедуры решение, т.е. результат. Таким образом, в блокчейне алгоритмом консенсуса является набор логически увязанных правил и функций, автоматически регулирующих работу сети пользователей криптовалют. Современные алгоритмы консенсуса в блокчейне основаны на логике алгоритмов решения криптографической задачи «византийских генералов». Однако для применения в криптовалютах логика «византийской» задачи была несколько модифицирована и адаптирована под функционирование в P2P-сети. Рассматривая логику данной задачи применительно к блокчейну, можно выделить следующие ее основные аспекты:

Стойкость к цензуре. Так как блокчейн — децентрализованная система, не нуждающаяся в едином управляющем органе, то, соответственно, никто никому не может запретить заниматься майнингом, т.е. участвовать в обеспечении работы сети.

Объективность. В блокчейне находится актуальная информация, описывающая состояние сети. За счет этого записи в блокчейне не нуждаются

[10] Мурзин П.Е. Основные подходы к разработке протокола консенсуса в распределенных реестрах. URL: https://www.granit-concern.ru/pdf/Murzin_statia_razrabotka_consensa_rr.pdf (дата обращения: 15.05.2020).

[11] Что такое форжинг криптовалюты. URL: https://bulldog.black/2019/04/27/chto-takoe-fordzhing-kriptovaljuty/ (дата обращения: 15.05.2020).

[12] Задача византийских генералов. URL: https://ru.wikipedia.org/wiki/Задача_византийских_генералов (дата обращения: 15.05.2020).

в подтверждении какими-либо авторитетными источниками.

Функции механизмов консенсуса в блокчейне следующие:

Частота генерации новых блоков записей. Благодаря данным алгоритмам исключаются ситуации, каждый узел генерирует свой блок и блок, записываемый в блокчейн. Например, в сети Биткоин блоки генерируются каждые 10 минут. Однако иногда возникают ситуации, когда два или более узлов генерируют блок практически одновременно с разницей в доли секунды. В этом случае возникает конфликт, который разрешается в пользу узла, раньше всех создавшего блок. Транзакции, которые входили в конкурентный блок или блоки, помещаются в список неподтвержденных транзакций и обрабатываются в следующем блоке.

Проверка информации в блоке записей. Все участники должны подтвердить, что данные в сгенерированном блоке верны. Проверке подлежат хеши транзакций как текущего, так и предыдущего блока, а также корректность подбора числа nonce.

Размер вознаграждения в сети. Размер вознаграждения зависит от сложности сети, причем, как ни парадоксально, обратно пропорционален ее сложности.

Недопущение двойного списания средств (криптомонет). Например, в сети Биткоин при проведении транзакции в блокчейн направляются все средства. После этого необходимая сумма перечисляется получателю, а остаток возвращается отправителю.

Рассмотрим логику, присущую основным алгоритмам консенсуса, применяемых в блокчейне.

Proof of Work (PoW) *— алгоритм доказательства работы в сети.* Логика алгоритма определяет, что для достижения консенсуса в распределенной транзакции должна выполняться «работа» выделенными узлами сети, называемыми «майнерами». Основным условием алгоритма консенсуса является то, что «работа» должна быть гарантированно выполнима. Какой выделенный узел затратит меньше времени на «работу», тот получает право закрыть (совершить) транзакцию.

Идея Proof-of-Work была сформулирована в 1993 г., но название получила только в 1999 г. Массовое применение описываемого алгоритма стало возможным только с появлением работ Сатоши Накамото. Особенностью алгоритма Накамото является то, что чем больше участников сети, тем больше общая вычислительная мощность сети, а значит, чтобы уравновесить стоимость добываемых монет во времени, необходимо увеличивать сложность вычислений. Такой подход позволил неравномерно распределить количество добываемых монет по времени. Количество добываемых монет падает, стоимость каждой добытой монеты растет.

Для того чтобы заработать больше криптомонет, майнеры осуществляют увеличение вычислительной мощности оборудования, в результате которого возникает эффект «гонки». В первой реализации алгоритма Накамото для майнинга Биткоина было достаточно персонального компьютера с одним процессором. Сейчас компьютеры необходимо объединять в фермы, процессоры компьютеров — в пул или создавать большой мощности майнинг-фермы. Увеличение вычислительной мощности майнинг-ферм требует больших затрат электроэнергии, что увеличивает мировое энергопотребление при быстром устаревании вычислительной техники.

Особенностью алгоритма Накамото является то, что чем больше участников сети, тем больше общая вычислительная мощность сети, а значит, чтобы уравновесить стоимость добываемых монет во времени, необходимо увеличивать сложность вычислений.

Еще одним недостатком PoW является низкая устойчивость к атаке 51% задействованных вычислительных мощностей (компьютеров). Считается, что подобные атаки являются теоретическими, однако известно, что на несколько часов вычислительные мощности крупной российской промышленной организации были переведены на добычу одной малопопулярной криптомонеты. Добытые монеты были переведены на криптокошелек одного из сотрудников организации. Далее огромное количество криптомонет оперативно было выведено на криптобиржу, обменяно на ликвидные криптовалюты, отправлено на другую криптобиржу и там обналичено в фиатные деньги[13].

Proof of Stake (PoS) *— алгоритм доказательства доли владения криптомонетами в общем пуле*

[13] Смирнова Е. Погорели на крипте. Как наказывают за майнинг на рабочем месте. URL: https://www.forbes.ru/tehnologii/354613-pogoreli-na-kripte-kak-nakazyvayut-za-mayning-na-rabochem-meste (дата обращения: 15.05.2020).

криптомонет. Алгоритм консенсуса PoS занимает второе место по популярности его применения в реализации криптовалют. В виде идеи алгоритм Proof of Stake был предложен в 2011 г. на форуме «Bitcointalk»[14], а первая реализация протокола была представлена криптомонетой PeerCoin[15] в 2012 г. Для работы алгоритма требуются участники сети — владельцы криптовалюты. Они объединяются в группы и делегируют свои права по добыче монет одному участнику, который для всех своих доверителей формирует пул участников. Такой узел сети называется нодой.

Возможен и другой вариант, когда нода формируется одним участником сети, который на своем кошельке держит большую сумму криптовалюты. Такой участник предлагает подключиться другим участникам сети к своей ноде.

Управление деятельностью сообщества участников сети, а также правилами управления консенсусом осуществляется только владельцами нод, так как права на эту деятельность делегированы другими участниками сообщества участников сети.

Генерация блоков в сети производится нодой. Чем большее количество монет имеет нода на своем кошельке, тем больше вероятность генерации нового блока. Так, пользователь, имеющий до 10% всех криптомонет в своем криптокошельке, сможет генерировать новые блоки сети Блокчейн с вероятностью в среднем до 10%.

В алгоритмах PoS возможна предварительная генерация всего количества монет, и в дальнейшем эти монеты могут пересылаться между участниками сети. Существует много реализаций алгоритма консенсуса PoS, упомянем следующие:

- Leased Proof of Stake (LPoS) — арендованное доказательство доли владения. Это пул участников сети с небольшим количеством криптомонет, которые они сдают в аренду участникам с большим количеством криптомонет, образующим ноду (узел). Благодаря сданным в аренду криптомонетам, участники сети получают возможность получения своей доли криптомонет с майнинга нодой, в противном случае, так как доля участника сети на общем рынке данной криптовалюты минимальна, то шанс получить вознаграждение минимален.
- Delegated Proof of Stake (DPoS) — делегированное доказательство доли владения криптомонетами. Все участники сети выбирают ноды, которым делегируют права по генерации новых блоков. Выбранные участники сети — владельцы нод — принимают решения о ее развитии, а также о конфигурации сети криптовалюты.

Алгоритм PoW был первым, новые алгоритмы стараются избавиться от его недостатков. Так, в PoS не требуются громоздкие вычисления, что не приводит к расходу электроэнергии и гонкам вычислительных мощностей. Атака в 51% также принесет наибольший урон злоумышленнику, поскольку покупка такого количества криптовалюты приведет к росту ее стоимости, что потребует значительных финансовых затрат, поэтому реализация атаки сделает главным пострадавшим атакующего, так как он станет держателем большей части криптомонет.

Процесс добычи криптовалюты на основе консенсуса PoS называется форжинг. Он заключается в создании мастерноды, работающей на специально выделенном компьютере стоимостью 70–100 долл. США. Компьютер всегда подключен к сети Интернет. На выделенном компьютере постоянно работает криптокошелек с минимальным количеством криптомонет. Например: для работы ноды DASH[16] требуется 1000 криптомонет, на июнь 2020 г. по биржевому курсу это соответствует 775 600 долл. США. Работа мастерноды может принести значительную прибыль только в том случае, если операции проводить с малопопулярными криптомонетами, стоимость которых незначительна. В случае роста их стоимости можно стать обладателем большого их числа и на своем мастерноде получать регулярные выплаты.

Недостатки у PoS следующие:

- пользователь на своем кошельке вынужден держать большую сумму криптомонет и не может использовать их для своих покупок;
- PoS способствует расслоению общества. Богатые богатеют, бедные беднеют. Имеющий, например, 10% криптомонет получает 10% от всех добываемых монет.

Криптопрактика не стоит на месте, алгоритмы консенсуса PoW и PoS развиваются и развитие идет по двум направлениям усложнения их логики:

- осуществляется комбинация алгоритмов различными способами. Алгоритм PoS используется для генерирования новых блоков, для подтверждения транзакций (или наоборот);
- усложнение логики алгоритма PoS в целях устранения его недостатков.

[14] Cryptocurrencies Without Proof of Work. URL: https://link.springer.com/chapter/10.1007/978–3–662–53357–4_10 (дата обращения: 15.05.2020).

[15] Официальный сайт PeerCoin. URL: https://peercoin.net (дата обращения: 15.05.2020).

[16] Официальный сайт DASH. URL: https://www.dash.org (дата обращения: 15.05.2020).

Proof of Importance (PoI) *— алгоритм доказательства важности процесса.* По своей логике алгоритм похож на алгоритм PoS, но при генерации блока принимаются во внимание следующие критерии:

- количество криптомонет на криптокошельке ноды;
- время жизни ноды в сети;
- количество успешно завершенных транзакций нодой сети.

У данного алгоритма имеется следующая особенность: чем меньше криптомонет имеется на собственном криптокошельке ноды, тем большее влияние оказывает количество транзакций и время нахождения ноды в режиме онлайн на результат операции по добыче криптовалют.

Логика указанного алгоритма применена, например, в криптосистеме NEM[17], в которой каждой учетной записи присваивается оценка важности процесса. По мере того, когда оценка важности процесса возрастает, у процесса будет больше шансов получить награду в виде криптомонет. Для получения права на вычисление важности процесса пользователи должны иметь не менее 10 000 криптомонет NEM на балансе криптокошелька. Как сеть NEM определяет оценку важности процесса? Если кто-то владеет 10 000 криптомонет NEM или более, то происходит математический перерасчет транзакций. Рост транзакций в сети, связанной с этой учетной записью, приведет к росту оценки важности процесса. Полагают, в будущем этот порог будет изменен. Указанный метод также гарантирует то, что пользователи, которые являются держателями NEM, будут и в дальнейшем удерживать свои средства. Этот метод можно рассматривать как логику создания мастерноды. Проект также предоставляет посетителям возможность определять рейтинг важности отдельных учетных записей в сети, что является хорошим способом обеспечения дальнейшей работы децентрализованной сети. Сбор вознаграждения на блокчейне NEM почти такой же, как при традиционном майнинге. Его цель состоит в том, чтобы добавлять транзакции в блокчейн в обмен на финансовое вознаграждение.

Proof of Authority (PoA) *— алгоритм доказательства полномочий.* Участники сети дают полномочия для генерации новых блоков выбранным нодам. Алгоритм PoA может применяться в регулируемых и корпоративной криптосистемах. Алгоритм PoA не является децентрализованным, все блоки находятся под контролем разработчика. Поэтому можно ожидать, что именно алгоритм PoA может быть внедрен в государственные криптосистемы.

Proof of Capacity (PoC) и Proof of Storage *— алгоритмы подтверждения емкости рабочей памяти компьютера.* Данный алгоритм подразумевает монетизацию выделенной памяти на жестком диске компьютера участника сети. Возможны варианты реализации указанных алгоритмов для обособления вычислительной (процессорной) мощности компьютеров участников сети, которая также монетизируется.

Proof of Stake Time (PoST) *— алгоритм доказательства времени ставки с учетом возраста криптомонет.* Здесь вместо того, чтобы учитывать количество криптомонет для расчета их возраста, используется период времени, в течение которого криптомонеты удерживались по конкретному адресу. Алгоритм реализован в криптовалюте VeriCoin[18].

Delegated Proof Of Stake (DPOS) *— алгоритм делегирования доказательства доли владения криптовалютой.* DPOS используют криптовалюты EOS[19] и BitShares[20], причем EOS использует логику консенсуса для масштабирования процесса до миллионов транзакций в секунду.

DPoS отличается от Po S. В DPoS токены не голосуют за сами блоки, но голосуют за избрание делегатов, которые проведут проверку от своего имени. Их может быть в районе 21–100. Делегаты периодически переизбираются. Система работает быстро. Если избранные узлы постоянно пропускают блоки или публикуют недействительные транзакции, ставящие голосуют против них и заменяют их лучшим вариантом.

В алгоритме DPoS майнеры для того, чтобы создавать блок, осуществляют сотрудничество, что не происходит в алгоритмах PoW и Po S. Алгоритм DPoS за счет частичной централизации в создании блоков может работать на порядки быстрее, чем большинство прочих алгоритмов консенсуса.

TAPOS *— алгоритм, в котором транзакция является доказательством доли.* Алгоритм реализован в программном обеспечении криптосистемы EOS. В этой системе для каждой транзакции требуется

[17] Официальный сайт NEM. URL: https://nem.io/ru/ (дата обращения: 15.05.2020).

[18] Официальный сайт VeriCoin. URL: https://vericoin.info (дата обращения: 15.05.2020).

[19] Официальный сайт EOS. URL: https://eos.io (дата обращения: 15.05.2020).

[20] Официальный сайт BitShares. URL: https://bitshares.org (дата обращения: 15.05.2020).

использовать хэш последнего заголовка блока. Это обеспечивает следующее:

- предотвращение повтора транзакций в разных блокчейнах;
- формирование сигнала сети, свидетельствующего о том, что пользователь и его доля находятся на определенном форке;
- формирование сигнала сети, который препятствует валидаторам действовать злонамеренно в целях, непредвиденных логикой процесса.

***BFT** — алгоритм задачи «византийских генералов».* Он используется в криптовалютах Hyperledger[21], Stellar[22], Ripple[23] и др. Федеративное византийское соглашение (FBA) используется в криптовалютах Stellar и Ripple. Общая идея заключается в том, что каждый генерал-валидатор, ответственный за свою цепочку, в целях установления истины сортирует все сообщения. В Ripple генералы-валидаторы предварительно выбираются основателями Ripple. В Stellar любой может быть валидатором, поэтому пользователь сам выбирает, каким валидаторам доверять. Это обеспечивает высокую пропускную способность, низкие транзакционные издержки и масштабируемость. В настоящее время данный алгоритм также активно используется в Hyperledger Fabric. Это обеспечивает высокую пропускную способность транзакций при полной централизации всего процесса.

***dBFT** — алгоритм делегированной задачи византийских генералов* используется в NEO[24]. Разработчики NEO выбрали этот алгоритм в целях обеспечения лучшего масштабирования и ускорения производительности процесса. Для объяснения логики функционирования dBFT используем следующую упрощенную аналогию. Пусть есть страна под названием NEO. Каждому гражданину страны предоставляется право голоса при выборе лидера, который называется делегатом. Все делегаты формируют законы страны. Если граждане не согласны с тем, как делегат проголосовал за закон, они могут проголосовать за другого делегата. Затем граждане высказывают своим избранникам, что они от них желают получить. Каждый делегат должен отслеживать требования всех граждан и документировать их в книге. Эти требования будут учтены при принятии законов, направленных на то, чтобы сделать граждан счастливыми. Когда пришло время принять закон, из группы делегатов случайным образом назначается спикер. Он предлагает закон, основанный на требованиях граждан. В предлагаемом законе он объясняет, как закон повлияет на уровень счастья страны. Затем спикер лично вручает делегатам предложенный им закон. Делегаты решают, соответствует ли расчет уровня счастья, который предложил спикер, их собственным. Если 66% делегатов согласятся с тем, что подсчитанный уровень счастья верный, то закон принимается. Если менее 66% делегатов согласны, то случайным образом выбирается новый спикер и процесс выборов повторяется вновь. Таким образом, данный алгоритм предназначен для защиты граждан от предателей и некомпетентных лидеров.

Применяя эту аналогию к блокчейну NEO, постулируется, что любой, кто владеет NEO, является гражданином. Большинство держателей NEO являются обычными нодами, которые могут передавать или обменивать криптомонеты. Как и граждане страны, они не участвуют в проверке блоков. Делегаты представляют собой особые ноды учета: они проверяют каждый блок, записанный в блокчейн. Чтобы стать узлом учета, должны быть соблюдены определенные требования: наличие специального оборудования, выделенных интернет-соединений и определенного объема GAS[25] (криптомонет, которых на момент написания статьи было порядка 1000). Дальше используется следующая логика: правилом является текущий блок в блочной цепочке, а уровнем счастья — это хэш текущего блока.

Алгоритм консенсуса aBFT используется в криптовалюте Hashgraph, в которой узлы распределяют свои транзакции другим узлам произвольно. Поэтому в итоге транзакции могут «переплетаться» вокруг узлов. Hashgraph обрабатывает до 250 000 транзакций в секунду, но он не очень устойчив к атакам типа Sybil[26], поэтому подходит только для небольших частных сетей.

***Proof Of Activity (PoA)** — алгоритм доказательства деятельности* реализован в тестнете Ethereum Kovan[27]. Это алгоритм консенсуса, в котором транзакции проверяются выделенными для

[21] Официальный сайт Hyperledger. URL: https://www.hyperledger.org/projects/fabric (дата обращения: 15.05.2020).

[22] Официальный сайт Stellar. URL: https://www.stellar.org (дата обращения: 15.05.2020).

[23] Официальный сайт Ripple. URL: https://ripple.com/xrp/ (дата обращения: 15.05.2020).

[24] Официальный сайт NEO. URL: https://neo.org (дата обращения: 15.05.2020).

[25] Консенсусный протокол Neo: как удалить византийскую дефектоскопию. URL: https://steemit.com/neo/@basiccrypto/neo-s-consensus-protocol-how-delegated-byzantine-fault-tolerance-works (дата обращения: 15.05.2020).

[26] Атака Sybil. URL: https://ru.wikipedia.org/wiki/Атака Сивиллы (дата обращения: 15.05.2020).

[27] Официальный сайт Ethereum Kovan. URL: https://kovan.etherscan.io (дата обращения: 15.05.2020).

этого «учетчиками», функции которых похожи на функции «админов» системы. От «учетчиков» прочие ноды узнают о состоянии процесса. PoA имеет высокую пропускную способность и оптимизирован для частных сетей. Очевидно, что из-за централизации процесса PoA не сможет эффективно функционировать в общедоступных сетях.

Proof Of Burn *— алгоритм сжигания монет* использует Slimcoin[28]. Логика алгоритма заключается в том, что майнеру формируются трудности в добыче криптомонет без привлечения реальных ресурсов, как это делается в алгоритме PoW с его затратами на электроэнергию и оборудование. Это также и не PoS, в рамках которого необходимо накапливать криптовалюты.

Под «сжиганием» здесь понимается процесс отправки криптомонет на тот адрес, на который отправлять нельзя (это условие для разных криптовалют используется по-разному). Таким образом, сценарий процесса предполагает «намеренно глупую» логику. Но тот, кто пожертвовал криптомонетами (аналог вложения в майнинг), получает право собирать транзакционные сборы. На этапе заработка криптовалюты это очень полезно для формирования ее рыночной цены.

Proof of Weight *— алгоритм доказательство веса* используется в криптосистемах Algorand[29], Filecoin[30] и др. Это целая группа алгоритмов консенсуса. Общая идея заключается в том, что, если в PoS ваш процент токенов, принадлежащих сети, дает вероятность «обнаружения» следующего блока, то в системе PoWeight используется другое взвешенное значение. Конкретный пример: в системе Proof of Spacetime от Filecoin взвешен на количестве криптовалют IPFS, которые находятся на хранении. Другие системы могут включать в себя удельный вес таких условий, как «доказательство репутации».

Proof of Checkpoint *— алгоритм проверки совпадающих блоков*. Это гибридный алгоритм, который может использовать любую систему криптовалют PoS с алгоритмом Po W. Каждому блоку, используемому в одном алгоритме, должен быть найден аналогичный блок в другом алгоритме. Алгоритм позволяет смягчить атаки в процедуре доказательства доли владения. Однако отключенные в течение длительного периода времени узлы все равно остаются подвержены этим атакам. Отключенные узлы при включении могут быть использованы для предоставления ложной информации о блокчейне.

Directed Acyclic Graphs (DAG) *— алгоритм с направленным ациклическим графом*. Алгоритмы с логикой DAG используют системы Iota[31], Hashgraph[32], Raiblocks/Nano[33]. Логика алгоритма DAG не анализирует всю структуру блокчейна, а обрабатывает его транзакции асинхронно[34]. Это дает возможность обрабатывать значительное число транзакций в секунду.

Разработчикам криптовалют в целях обеспечения их конкурентоспособности рекомендуется ответственно выбирать алгоритм консенсуса, который формирует блокчейну криптовалюты «византийские правила».

Конкретным примером алгоритма консенсуса типа DAG является алгоритм Tangle[35], который использует система Iota. В нем для того, чтобы отправить транзакцию, необходимо подтвердить две предыдущие полученные транзакции. Логика консенсуса, реализуемая по принципу «два к одному», укрепляет «справедливость» транзакций. Поскольку консенсус определяется транзакциями, теоретически, если кто-то сможет сгенерировать треть всех транзакций, он может захватить всю сеть. Поэтому в Iota есть «двойная проверка» всех транзакций сети на централизованном узле «координатор», который вначале функционирует в целях поддержания работы системы, а затем, когда число обрабатываемых узлов становится очень большим, удаляется.

[28] Официальный сайт Slimcoin. URL: http://slimco.in (дата обращения: 15.05.2020).

[29] Официальный сайт Algorand. URL: https://www.algorand.com (дата обращения: 15.05.2020).

[30] Официальный сайт Filecoin. URL: https://filecoin.io (дата обращения: 15.05.2020).

[31] Официальный сайт Iota. URL: https://www.iota.org (дата обращения: 15.05.2020).

[32] Официальный сайт Hashgraph. URL: https://www.hedera.com (дата обращения: 15.05.2020).

[33] Официальный сайт Nano. URL: https://nano.org/en (дата обращения: 15.05.2020).

[34] Sompolinsky Y., Zohar A.A Scalable BlockDAG protocol. 2018. URL: http://diyhpl.us/~bryan/papers2/bitcoin/Phantom:%20A%20scalable%20block%20DAG%20protocol%20-%202018.pdf (дата обращения: 15.05.2020).

[35] Popov S. The tangle. 2018. URL: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf (дата обращения: 15.05.2020).

ВЫВОДЫ

Результаты исследования выявили, что на институциональные особенности разработки конкурентоспособной криптовалюты оказало влияние не только развитие информационных технологий, но и развитие философии, математики, экономики и финансов. Анализ «мягких» и «жестких» правил конкуренции, институциональной среды и методов, обеспечивающих разработку криптовалюты, свидетельствует о том, что благодаря усилиям многих ученых и программистов-практиков различных стран мира криптовалюта стала новым конкурентоспособным активом (IT-продуктом) современных финансов.

В работе детально рассмотрено одно из «жестких» правил конкуренции — логика алгоритмов консенсуса блокчейна, вносящая один из основных вкладов в обеспечение конкурентоспособности криптовалют. Выполнен анализ логики консенсуса для ограниченного числа алгоритмов, которые существуют или только находятся в экспериментальной апробации. Показано, что исторически первым алгоритмом консенсуса стал PoW, который реализован во множестве криптовалют, входящих в Топ-10 рейтинга криптовалют. Это означает, что на практике именно этот алгоритм наиболее распространен среди разработчиков криптовалют. Однако его конкурент (алгоритм PoS) уже завоевывает свою долю крипторынка, поэтому, например, осуществляется переход криптовалюты Ethereum на данный алгоритм. Исследованиями выявлено, что наиболее перспективными являются гибридные алгоритмы. Они либо совмещают в себе логику алгоритмов PoS и PoW, либо являются развитием и доработкой одного из них (чаще всего логики PoS).

По результатам исследования можно сделать следующие выводы.

Во-первых, все алгоритмы консенсуса реализуют определенные логические зависимости и у них есть как сильные, так и слабые стороны, поэтому для детального анализа этой логики необходимо быть профессиональным математиком. Чаще всего различия в названиях алгоритмов консенсуса блокчейна подчеркивают специфику логики: Work, Stake, Authority, Storage и пр.

Во-вторых, представленные в работе логики разработки алгоритмов консенсуса блокчейна применимы практически ко всем криптовалютам, поэтому они определены в качестве основных. Это:

- согласование;
- эгалитаризм (особенности его реализации определяются бизнес-моделью конкретной криптовалюты или криптосистемы);
- кооперация;
- инклюзивность (она определяет стойкость к «взлому» алгоритма, которая при разных граничных условиях может меняться, поэтому специфику инклюзивности могут выявить только прикладные математики);
- стойкость к цензуре;
- объективность;
- частота генерации новых блоков записей (зависит от технологии реализации алгоритмов консенсуса, которые, как правило, этого ограничения не имеют);
- проверка информации в блоке записей (зависит от технологии реализации алгоритма, однако для одного и того же алгоритма может быть реализовано множество способов данной проверки);
- размер вознаграждения в сети (определяется точкой зрения разработчика на его размер при реализации конкретного алгоритма консенсуса под конкретную криптовалюту);
- недопущение двойного списания криптомонет (процедура является обязательной при реализации бизнес-моделей всех типов криптовалют — логика процедуры предусматривает транзакцию, функционирующую параллельно процессу реализации основного алгоритма).

В-третьих, каждая криптовалюта имеет уникальные характеристики, анализ которых позволяет для оценки конкурентоспособности сравнивать эффективность реализации их бизнес-моделей. Практика показала, что одну и ту же бизнес-модель можно реализовать несколькими способами и на основе различных алгоритмов консенсуса. Поэтому сравнивать конкурентоспособность логики алгоритмов консенсуса можно только после того, как они будут применены в бизнес-моделях конкретных криптовалют, которые выявят их конкурентоспособность на крипторынках.

Таким образом, разработчикам криптовалют в целях обеспечения их конкурентоспособности рекомендуется ответственно выбирать алгоритм консенсуса, который формирует блокчейну криптовалюты «византийские правила». Эти правила предоставляют транзакциям информацию, за счет которой они приходят к консенсусу, обеспечивая безопасность сети, и исключают «зависание», обеспечивая живучесть сети. Однако следует еще раз подчеркнуть, что окончательный вывод о степени конкурентоспособности конкретной криптовалюты поможет сделать только рыночная криптопрактика.

СПИСОК ИСТОЧНИКОВ

1. Накамото С. Биткойн: система цифровой пиринговой наличности. Пер. с англ. URL: https://bitcoin.org/files/bitcoin-paper/bitcoin_ru.pdf (дата обращения: 15.05.2020).
2. Айзексон У. Инноваторы. Как несколько гениев, хакеров и гиков совершили цифровую революцию. Пер. с англ. М.: Манн, Иванов и Фербер; 2019. 304 с.
3. Ludlow P. High noon on the electronic frontier: Conceptual issues in cyberspace. Cambridge, MA: The MIT Press; 1996. 558 p.
4. Ludlow P. Crypto anarchy, cyberstates and pirate Utopias. Cambridge, MA: The MIT Press; 2001. 451 p.
5. Талеров П.И. Конкуренция как социальное явление и отношение к ней анархистов. Сб. мат. Всерос. конф. с междунар. участием «Междисциплинарный синтез гуманитарных наук в эпоху социокультурных и исторических трансформаций: опыт "Русского Пути"». СПб.: Изд-во РХГА; 2019:113–120.
6. Кропоткин П.А. Этика. Избранные труды. М.: Политиздат, 1991. 496 с.
7. Масленников В.В., Федотова М.А., Сорокин А.Н. Новые финансовые технологии меняют наш мир. *Вестник Финансового университета*. 2017;21(2):6–11. DOI: 10.26794/2587–5671–2017–21–2–6–11
8. Полански А. Эра криптовалюты. М.: Изд-во АСТ; 2018. 320 с.
9. Столбов М.И. К десятилетию рынка криптовалют: текущее состояние и перспективы. *Вопросы экономики.* 2019;(5):136–148. DOI: 10.32609/0042–8736–2019–5–136–148
10. Винья П., Кейси М. Эпоха криптовалют. Как биткойн и блокчейн меняют мировой экономический порядок. Пер. с англ. М.: Манн, Иванов и Фербер; 2017. 432 с.
11. Бауэр В.П., Смирнов В.В. Биткойн: генезис, практика и перспективы развития. Часть 1. *Информационное общество.* 2018;(4–5):65–75.
12. Бауэр В.П., Смирнов В.В. Биткойн: генезис, практика и перспективы развития. Часть 2. *Информационное общество*. 2019;(1–2):35–43.
13. Недосекин А.О., Рейшахрит Е.И., Абдулаева З.И. Российский крипторубль — инструмент для устойчивого развития экономики РФ. *Экономика и предпринимательство*. 2017;(9–1):65–71.
14. Глазьев С.Ю. О глубинных причинах нарастающего хаоса и мерах по преодолению экономического кризиса. 2020. URL: https://glazev.ru/articles/1-mirovoy-krizis/78041-o-glubinnykh-prichinakh-narastajushhego-khaosa-i-merakh-po-preodoleniju-jekonomicheskogo-krizisa (дата обращения: 15.05.2020).
15. Дробот Е.В. Управление конкурентоспособностью национальной экономики в условиях глобализации. СПб.: Троицкий мост; 2015. 223 с.
16. Бауэр В.П., Смирнов В.В. Сравнительный анализ криптовалют NEO и ETHEREUM в контексте становления цифровой экономики будущего. *Экономика. Налоги. Право.* 2019;12(3):116–124. DOI: 10.26794/1999–849X-2019–12–3–116–124
17. Синельникова-Мурылева Е.В., Шилов К.Д., Зубарев А.В. Сущность криптовалют: дескриптивный и сравнительный анализ. *Финансы: теория и практика*. 2019;23(6):36–49. DOI: 10.26794/2587–5671–2019–23–6–36–49
18. Тарануха Ю.В. Конкуренция. Система и процесс. М: Дело и сервис; 2012. 665 с.
19. Оскирко А.Л. Методика оценки состояния процесса управления конкурентоспособностью товаров (услуг) организации. *Colloquium-Journal*. 2019;(6–11):79–81.
20. Баин Е.Е., Воробьева Л.Г. Теоретические аспекты определения понятия «конкурентная среда в отрасли». *European Science*. 2017;(4):43–47.
21. Биксина Н.А. Конкуренция в бизнесе: полное определение понятия, виды, плюсы и минусы конкуренции. *Экономика и управление: проблемы, решения*. 2018;2(5):4–7.
22. Хакимов А.Х. Конкурентное партнерство предпринимательских организаций. *Журнал правовых и экономических исследований*. 2019;(3):200–205. DOI: 10.26163/GIEF.69.99.034
23. Катаев А.В., Катаева Т.М. Межорганизационные сетевые структуры: проблемы организации и управления. *Конкурентоспособность в глобальном мире: экономика, наука, технологии*. 2016(7–1):141–144.
24. Chi M., Zhao J., George J.F., Li Y., Zhai S. The influence of inter-firm IT governance strategies on relational performance: The moderation effect of information technology ambidexterity. *International Journal of Information Management*. 2017;37(2):43–53. DOI: 10.1016/j.ijinfomgt.2016.11.007
25. Тарануха Ю.В. Модификация конкурентного принципа в процессе эволюции конкуренции. *Общество и экономика*. 2017;(3–4):49–67.

26. Розанова Н.М., Линева И.В. Цифровая модель для современного бизнеса. *Журнал экономической теории*. 2019;16(1):46–59. DOI 10.31063/2073–6517/2019.16–1.5
27. Нуреева Р.Р., Шарафутдинов Р.И., Сафиуллин Л.Н. Цифровая конкурентоспособность: институциональные основания конкурентоспособности Российской Федерации в условиях цифровой экономки. *Экономика и предпринимательство*. 2018;(9):91–95.
28. Иваненко И.А., Саифидинова Ф.Н. Институциональная среда и конкурентные отношения на рынке. *Экономика и социум*. 2017;(12):455–457.
29. Хакимов А.Х. Проблемы управления конкурентоспособностью российских предпринимательских структур и пути их решения. СПб.: СПбГЭУ; 2019. 200 с.
30. Гришков А.Ф. Комплексная модель механизма управления конкурентоспособностью в сфере услуг. *Петербургский экономический журнал*. 2019;(2):121–133.
31. Сорокин Д.Е. О способности России к социально-экономическим трансформациям. *Экономическое возрождение России*. 2019;(1):23–28.
32. Сорокин Д.Е. Политическая экономия технологической модернизации России. *Экономическое возрождение России.* 2020;(1):18–25.
33. Романс Э. Настольная книга венчурного предпринимателя: секреты лидеров стартапов. Пер. с англ. М.: Альпина паблишер; 2015. 246 с.
34. Мараховская И.Ю. Развитие предпринимательских структур в условиях нарастания конкурентных вызовов и угроз. *Ученые записки Крымского федерального университета имени В.И. Вернадского. Экономика и управление*. 2018;4(1):79–83.
35. Еферин Я.Ю., Россотто К.М., Хохлов Ю.Е. Цифровые платформы в России: конкуренция между национальными и зарубежными многосторонними платформами стимулирует экономический рост и инновации. *Информационное общество*. 2019;(1–2):16–34.
36. Стеллман Э., Грин Дж. Постигая Agile: Ценности, принципы, методологии. Пер. с англ. М.: Манн, Иванов и Фербер; 2017. 445 с.
37. Сазерленд Дж. Scrum. Революционный метод управления проектами. Пер. с англ. М.: Манн, Иванов и Фербер; 2017. 272 с.
38. Носова С.С. Стратегия инновационной экономики в режиме коллаборации. *Экономические стратегии*. 2018;20(6):48–57.
39. Бауэр В.П., Побываев С.А., Сильвестров С.Н. Блокчейн как дополненная реальность: от гипотезы к основам теории и практики. *Экономическая наука современной России*. 2018;(1):20–32.
40. 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
41. Урахчинский И.Н., Кондратьев С.В., Хайрисламов Д.А., Кошмин М.Д. Сравнительный анализ алгоритмов шифрования в технологии «Blockchain». Сб. избр. ст. по мат. науч. конф. ГНИИ «Нацразвитие». СПб.: ГНИИ «Нацразвитие»; 2019:130–134.
42. Майорова Е.В. Методические аспекты реагирования на инциденты информационной безопасности в условиях цифровой экономики. *Петербургский экономический журнал.* 2020;(1):155–162. DOI: 10.25631/PEJ.2020.1.155.162
43. Ершова И.В., Трофимова Е.В. Майнинг и предпринимательская деятельность: в поисках соотношения. *Актуальные проблемы российского права*. 2019;(6):73–82. DOI: 10.17803/1994–1471.2019.103.6.073–082
44. Урахчинский И.Н., Хайрисламов Д.А., Кондратьев С.В., Кошмин М.Д. Сравнительный анализ алгоритмов майнинга в технологии «Blockchain». Сб. избр. ст. по мат. науч. конф. ГНИИ «Нацразвитие». СПб.: ГНИИ “Нацразвитие”; 2019:134–138.
45. Крутеева О.В., Соловьева Ю.Ю. Модель оценки эффективности майнинга криптовалюты. *Экономика и предпринимательство.* 2018;(11):1190–1193.
46. Демин В.И., Соловьев П.С., Трифонов М.И. и др. Технологии блокчейн. Современное состояние и ключевые инсайты. М.: Фед. ин-т промышленной собственности; 2018. 87 с.
47. Merkle R.C. Protocols for Public Key Cryptosystems. In: IEEE Symp. on security and privacy (Oakland, CA, 14–16 Apr. 1980). New York: IEEE; 1980:122. DOI: 10.1109/SP.1980.10006
48. Должик Д.С. Обзор и сравнение алгоритмов нахождения консенсуса в блокчейне. Мат. XIII-й Межд. отрасл. науч.-тех. конф. «Технологии информационного общества». М.: Медиа паблишер; 2019:349–351.

REFERENCES

1. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. URL: https://bitcoin.org/bitcoin.pdf (accessed on 15.05.2020).
2. Isaacson W. The innovators: How a group of hackers, geniuses, and geeks created the digital revolution. New York: Simon & Schuster; 2014. 560 p. (Russ. ed.: Isaacson W. Innovatory. Kak neskol'ko geniev, khakerov i gikov sovershili tsifrovuyu revolyutsiyu. Moscow: Mann, Ivanov and Ferber; 2019. 304 p.)
3. Ludlow P. High noon on the electronic frontier: Conceptual issues in cyberspace. Cambridge, MA: The MIT Press; 1996. 558 p.
4. Ludlow P. Crypto anarchy, cyberstates and pirate Utopias. Cambridge, MA: The MIT Press; 2001. 451 p.
5. Talerov P.I. Competition as a social phenomenon and the attitude of anarchists towards it. In: Proc. All-Russ. conf. with int. particip. "Interdisciplinary synthesis of the humanities in the era of sociocultural and historical transformations: Experience of the "Russian Way". St. Petersburg: Russian Christian Humanitarian Academy; 2019:113–120. (In Russ.).
6. Kropotkin P.A. Ethics. Selected works. Moscow: Politizdat; 1991. 496 p. (In Russ.).
7. Maslennikov V.V., Fedotova M.A., Sorokin A.N. New financial technologies are changing our world. *Vestnik Finansovogo universiteta = Bulletin of the Financial University*. 2017;21(2):6–11. (In Russ.). DOI: 10.26794/2587–5671–2017–21–2–6–6–11
8. Polanski A. The era of cryptocurrency. Moscow: AST; 2018. 320 p. (In Russ.).
9. Stolbov M.I. To the tenth anniversary of the cryptocurrency market: Current state and prospects. *Voprosy ekonomiki*. 2019;(5):136–148. (In Russ.). DOI: 10.32609/0042–8736–2019–5–136–148
10. Vigna P., Casey M.J. The age of cryptocurrency: How bitcoin and the blockchain are challenging the global economic order. London: Picador; 2016. 384 p. (Russ. ed.: Vigna P., Casey M. Epokha kriptovalyut. Kak bitkoin i blokcheyn menyayut mirovoy ekonomicheskiy poryadok. Moscow: Mann, Ivanov and Ferber; 2017. 432 p.).
11. Bauer V.P., Smirnov V.V. Bitcoin: Genesis, practice and development prospects. Part 1. *Informatsionnoe obshchestvo = Information Society*. 2018;(4–5):65–75. (In Russ.).
12. Bauer V.P., Smirnov V.V. Bitcoin: Genesis, practice, and development prospects. Part 2. *Informatsionnoe obshchestvo. = Information Society*. 2019;(1–2):35–43. (In Russ.).
13. Nedosekin A.O., Reishakhrit E.I, Abdulaeva Z.I. Russian crypto ruble — a tool for sustainable development of the Russian economy. *Ekonomika i predprinimatel'stvo = Journal of Economy and Entrepreneurship*. 2017;(9–1):65–71. (In Russ.).
14. Glaz'ev S. Yu. On the root causes of the growing chaos and measures to overcome the economic crisis. 2020. URL: https://glazev.ru/articles/1-mirovoy-krizis/78041-o-glubinnykh-prichinakh-narastajushhego-khaosa-i-merakh-po-preodoleniju-jekonomicheskogo-krizisa (accessed on 15.05.2020). (In Russ.).
15. Drobot E.V. Management of the competitiveness of the national economy in the context of globalization. St. Petersburg: Troitskii most; 2015. 223 p. (In Russ.).
16. Bauer V.P., Smirnov V.V. Comparative analysis of NEO and ETHEREUM cryptocurrencies in the context of the formation of the digital economy of the future. *Ekonomika. Nalogi. Pravo = Economics, Taxes & Law*. 2019;12(3):116–124. (In Russ.). DOI: 10.26794/1999–849X-2019–12–3–116–124
17. Sinel'nikova-Muryleva E.V., Shilov K.D., Zubarev A.V. The essence of cryptocurrencies: Descriptive and comparative analysis. *Finansy: teoriya i praktika = Finance: Theory and Practice*. 2019;23(6):36–49. (In Russ.). DOI: 10.26794/2587–5671–2019–23–6–36–49
18. Taranukha Yu.V. Competition. System and process. Moscow: Delo i servis; 2012. 665 p. (In Russ.).
19. Oskirko A.L. Methodology for assessing the status of the process of managing the competitiveness of goods (services) of an organization. *Colloquium-Journal*. 2019;(6–11):79–81. (In Russ.).
20. Bain E.E., Vorob'eva L.G. Theoretical aspects of the definition of the concept "competitive environment in the industry". *European Science*. 2017;(4):43–47. (In Russ.).
21. Biksina N.A. Competition in business: A complete definition of the concept, types, pros and cons of competition. *Ekonomika i upravlenie: problemy, resheniya.* 2018;2(5):4–7. (In Russ.).
22. Khakimov A. Kh. Competitive partnership of business organizations. *Zhurnal pravovykh i ekonomicheskikh issledovanii = Journal of Legal and Economic Studies*. 2019;(3):200–205. (In Russ.). DOI: 10.26163/GIEF.69.99.034

23. Kataev A. V., Kataeva T. M. Interorganizational network structures: Problems of organization and management. *Konkurentosposobnost' v global'nom mire: ekonomika, nauka, tekhnologii = Competitiveness in the Global World: Economics, Science, Technology*. 2016(7–1):141–144. (In Russ.).
24. Chi M., Zhao J., George J. F., Li Y., Zhai S. The influence of inter-firm IT governance strategies on relational performance: The moderation effect of information technology ambidexterity. *International Journal of Information Management*. 2017;37(2):43–53. DOI: 10.1016/j.ijinfomgt.2016.11.007
25. Taranukha Yu. V. Modification of the competitive principle in the evolution of competition. *Obshchestvo i ekonomika = Society and Economy*. 2017;(3–4):49–67. (In Russ.).
26. Rozanova N. M., Lineva I. V. Digital model for modern business. *Zhurnal ekonomicheskoi teorii = Russian Journal of the Economic Theory*. 2019;16(1):46–59. (In Russ.). DOI: 10.31063/2073–6517/2019.16–1.5
27. Nureeva R. R., Sharafutdinov R. I., Safiullin L. N. Digital competitiveness: Institutional foundations of the competitiveness of the Russian Federation in the digital economy. *Ekonomika i predprinimatel'stvo = Journal of Economy and Entrepreneurship*. 2018;(9):91–95. (In Russ.).
28. Ivanenko I. A., Saifidinova F. N. Institutional environment and competitive relations in the market. *Ekonomika i sotsium*. 2017;(12):455–457. (In Russ.).
29. Khakimov A. Kh. Problems of managing the competitiveness of Russian business structures and ways to solve them. St. Petersburg: St. Petersburg State University of Economics; 2019. 200 p. (In Russ.).
30. Grishkov A. F. A comprehensive model of the competitiveness management mechanism in the service sector. *Peterburgskii ekonomicheskii zhurnal = Saint-Petersburg Economic Journal*. 2019;(2):121–133. (In Russ.).
31. Sorokin D. E. On Russia's ability to social and economic transformations. *Ekonomicheskoe vozrozhdenie Rossii = The Economic Revival of Russia*. 2019;(1):23–28. (In Russ.).
32. Sorokin D. E. Political economy of technological modernization of Russia. *Ekonomicheskoe vozrozhdenie Rossii. = The Economic Revival of Russia*. 2020;(1):18–25. (In Russ.).
33. Romans A. The entrepreneurial Bible to venture capital: Inside secrets from the leaders in the startup game. New York: McGraw-Hill Education; 2013. 256 p. (Russ. ed.: Romans A. Nastol'naya kniga venchurnogo predprinimatelya. Sekrety liderov startapov. Moscow: Alpina Publisher; 2015. 246 p.).
34. Marakhovskaya I. Yu. The development of entrepreneurial structures in the face of increasing competitive challenges and threats. *Uchenye zapiski Krymskogo federal'nogo universiteta im. V. I. Vernadskogo. Ekonomika i upravlenie = Scientific Notes of V. I. Vernadsky Crimean Federal University. Economics and Management*. 2018;4(1):79–83. (In Russ.).
35. Eferin Ya. Yu., Rossotto K. M., Khokhlov Yu. E. Digital platforms in Russia: Competition between national and foreign multilateral platforms stimulates economic growth and innovation. *Informatsionnoe obshchestvo = Information Society*. 2019;(1–2):16–34. (In Russ.).
36. Stellman E., Greene J. Learning Agile: Understanding Scrum, XP, Lean, and Kanban. Sebastopol, CA: O'Reilly Media; 2013. 420 p. (Russ. ed.: Stellman E., Greene J. Postigaya Agile: Tsennosti, printsipy, metodologii. Moscow: Mann, Ivanov and Ferber; 2017. 445 p.).
37. Sutherland J. Scrum: The art of doing twice the work in half the time. New York: Crown Business; 2014. 256 p. (Russ. ed.: Sutherland J. Scrum. Revolyutsionnyy metod upravleniya proektami. Moscow: Mann, Ivanov and Ferber; 2017. 272 p.).
38. Nosova S. S. Strategy for an innovative economy in collaboration mode. *Ekonomicheskie strategii = Economic Strategies*. 2018;20(6):48–57. (In Russ.).
39. Bauer V. P., Pobyvaev S. A., Sil'vestrov S. N. Blockchain as an augmented reality: From a hypothesis to the basics of theory and practice. *Ekonomicheskaya nauka sovremennoi Rossii = Economics of Contemporary Russia*. 2018;(1):20–32. (In Russ.).
40. Krylov G. O., Seleznev V. M. Status and prospects of development of blockchain technology in the financial sector. *Finansy: teoriya i praktika = Finance: Theory and Practice*. 2019;23(6):26–35. (In Russ.). DOI: 10.26794/2587–5671–2019–23–6–26–35
41. Urakhchinsky I. N., Kondratiev S. V., Khayrislamov D. A., Koshmin M. D. Comparative analysis of encryption algorithms in the "Blockchain" technology. Coll. selected pap. of the Humanitarian National Research Institute "Natsrazvitie" sci. conf. St. Petersburg: HNRI "Natsrazvitie"; 2019:130–134. (In Russ.).
42. Mayorova E. V. Methodological aspects of responding to information security incidents in the digital economy. *Peterburgskii ekonomicheskii zhurnal = Saint-Petersburg Economic Journal*. 2020;(1):155–162. (In Russ.). DOI: 10.25631/PEJ.2020.1.155.162

43. Ershova I.V., Trofimova E.V. Mining and business activities: In search of balance. *Aktual'nye problemy rossiiskogo prava = Actual Problems of Russian Law*. 2019;(6):73–82. (In Russ.). DOI: 10.17803/1994–1471.2019.103.6.073–082
44. Urakhchinsky I.N., Khayrislamov D.A., Kondratiev S.V., Koshmin M.D. Comparative analysis of mining algorithms in the "Blockchain" technology. Coll. selected pap. of the Humanitarian National Research Institute "Natsrazvitie" sci. conf. St. Petersburg: HNRI "Natsrazvitie"; 2019:134–138. (In Russ.).
45. Kruteeva O.V., Solovieva Yu. Yu. A model for evaluating the effectiveness of cryptocurrency mining. *Ekonomika i predprinimatel'stvo = Journal of Economy and Entrepreneurship*. 2018;(11):1190–1193. (In Russ.).
46. Demin V.I., Solov'ev P.S., Trifonov M.I. et al. Blockchain technologies: Current status and key insights. Moscow: Federal Institute of Industrial Property; 2018. 87 p. (In Russ.).
47. Merkle R.C. Protocols for Public Key Cryptosystems. In: IEEE Symp. on security and privacy (Oakland, CA, 14–16 Apr. 1980). New York: IEEE; 1980:122. DOI: 10.1109/SP.1980.10006
48. Dolzhik D.S. Review and comparison of algorithms for finding consensus in the blockchain. In: Proc. 13th Int. sect. sci.-tech. conf. "Technology of the information society". Moscow: Media Publisher; 2019:349–351. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ / ABOUT THE AUTHORS

Владимир Петрович Бауэр — доктор экономических наук, доцент, директор Центра стратегического прогнозирования и планирования Института экономической политики и проблем экономической безопасности, Финансовый университет, Москва, Россия
Vladimir P. Bauer — Dr. Sci. (Econ.), Assoc. Prof., Head of the Centre of Strategic Forecasting and Planning, Institute for Economic Policy and Problems of Economic Security, Moscow, Russia
bvp09@mail.ru

Владимир Васильевич Смирнов — младший научный сотрудник Центра стратегического прогнозирования и планирования Института экономической политики и проблем экономической безопасности, Финансовый университет, Москва, Россия
Vladimir V. Smirnov — Junior Researcher of the Centre of Strategic Forecasting and Planning, Institute for Economic Policy and Problems of Economic Security, Moscow, Russia
Vladimir.Smirnov.fsg@gmail.com

Статья поступила в редакцию 08.06.2020; после рецензирования 20.06.2020; принята к публикации 12.08.2020.
Авторы прочитали и одобрили окончательный вариант рукописи.
The article was submitted on 08.06.2020; revised on 20.06.2020 and accepted for publication on 12.08.2020.
The authors read and approved the final version of the manuscript.