

Кашеварова Н.А.¹, Куликова М.Е.¹, Ряскина А.Д.¹

¹ Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), Москва, Россия

Обзор механизмов консенсуса и их применение в бизнес-практике

ЦИТИРОВАТЬ СТАТЬЮ:

Кашеварова Н.А., Куликова М.Е., Ряскина А.Д. Обзор механизмов консенсуса и их применение в бизнес-практике // Креативная экономика. – 2022. – Том 16. – № 12. – С. 4787–4802. doi: [10.18334/ce.16.12.116900](https://doi.org/10.18334/ce.16.12.116900)

АННОТАЦИЯ:

Статья посвящена рассмотрению наиболее популярных механизмов консенсуса, обеспечивающих решение различных бизнес-задач, а также перспективных направлений для применения блокчейн-систем. Авторами проанализированы основные алгоритмы консенсуса с точки зрения их функциональной характеристики и алгоритма работы. Также в статье представлены сферы применения блокчайна в современной бизнес-практике, где в зависимости от бизнес-процесса формируются различные требования к механизмам консенсуса, их внутренним характеристикам. По итогам проведенной работы авторами сделаны выводы о роли алгоритмов консенсуса в блокчейне и конкретных сферах бизнеса, что дает возможность оценить экологические последствия инвестирования в криптографию, что является актуальной повесткой для нашего времени в связи со стремительным и перспективным развитием блокчейн-системы. Данная статья может быть интересна для исследователей, занимающихся тенденциями инновационной экономики и развития криптовалют, а также компаниям, планирующим переводить свою деятельность или же строить в рамках блокчейн-системы с распределенными узлами.

КЛЮЧЕВЫЕ СЛОВА: блокчейн, смарт-контракт, механизм консенсуса, платформа, бизнес-процесс

ОБ АВТОРАХ

Кашеварова Наталия Александровна, доцент кафедры предпринимательства и внешнеэкономической деятельности, кандидат экономических наук (n.kashevarova@yandex.ru)

Куликова Мария Евгеньевна, студент 4-го курса (KulikovaaMariaa@yandex.ru)

Ряскина Анастасия Дмитриевна, студент 4-го курса (anastasyarayskina@gmail.com)



Kashevarova N.A.¹, Kulikova M.E.¹, Ryaskina A.D.¹

¹ Bauman Moscow State Technical University, Russia

Consensus mechanisms and their application in business practice

CITE AS:

Kashevarova N.A., Kulikova M.E., Ryaskina A.D. (2022) Obzor mekhanizmov konsensusa i ikh primenenie v biznes-praktike [Consensus mechanisms and their application in business practice]. *Kreativnaya ekonomika.* 16. (12). – 4787–4802. doi: [10.18334/ce.16.12.116900](https://doi.org/10.18334/ce.16.12.116900)

ABSTRACT:

The article is devoted to the consideration of the most popular consensus mechanisms that provide solutions for various business tasks, as well as promising directions for the application of blockchain systems. The authors have analysed the main consensus algorithms in terms of their functional characteristics and operation algorithm. The article presents areas of blockchain application in modern business practice where, depending on the business process, different requirements to consensus mechanisms and their internal characteristics are formed. The authors draw conclusions about the role of consensus algorithms in blockchain and specific areas of business, which makes it possible to assess the environmental impact of investing in cryptography. This is a relevant agenda for our time due to the rapid and promising development of the blockchain system. This article may be of interest to researchers concerned with trends in the innovation economy and the development of cryptocurrencies, as well as companies planning to transfer their operations or to build within a blockchain system with distributed nodes.

KEYWORDS: blockchain, smart contract, consensus mechanism, platform, business process

JEL Classification: M11, M21, O31, O33

Received: 01.12.2022 / **Published:** 25.12.2022

© Author(s) / Publication: CREATIVE ECONOMY Publishers

For correspondence: Kashevarova N.A. (n.kashevarova@yandex.ru)

Введение

Актуальность рассмотрения механизмов консенсуса обусловлена стремительным развитием технологии блокчейн, которая захватывает все области нашей жизнедеятельности. Компании в погоне за инновационными методами поддержания бизнеса стремятся как можно быстрее внедрить блокчейн-систему, однако не до конца понимают, в каком виде и с каким алгоритмом достижения соглашения в узлах стоит это делать. В настоящее время компании во многих отраслях экономики начинают внедрять блокчейн-решения в свои приложения и услуги, оптимизируя различные бизнес-процессы: от подтверждения подлинности товаров до контроля всего пути поставок при международных перевозках [1, 2] (*Travushkina, Shchelokova, Shboldenkov, Yusufova, 2022; Drogovoz, Kharin, 2021*). Чтобы поддерживать целостность блокчейна и гарантировать, что каждый узел поддерживает подлинную копию реестра, применяются механизмы консенсуса. Они также определяют, как новая транзакция или данные включаются в новый блок и какой узел может добавить блок и поделиться им с другими узлами в сети. Роль консенсусных алгоритмов заключается в достижении уровня надежности сети, построенной на серии узлов (устройств, соединенных с другими устройствами, как часть компьютерной сети).

В своей работе авторы опирались на результаты исследований в области развития блокчейна, отраженных в трудах: Носирова З.А. и Фомичева В.М. [3, с. 37–75] (*Nosirov, Fomichev, 2021, p. 37–75*), Криштаносова В.Б. [4, с. 13–32] (*Krishtanosov, 2020, p. 13–32*), Ташеро П. и Тессоне Дж. [5, с. 1–39] (*Tasca, Tessone, 2019, p. 1–39*), Зутши А., Грило А. и Нодехи Т. [16] (*Zutshi, Grilo, Nodehi, 2021*), Кортасино Ф., Дасаклис Т. и Пацакис К. [17, с. 55–81] (*Casino, Dasaklis, Patsakis, 2019, p. 55–81*), Хян Т.Т. [18, с. 332–336] (*Huynh, 2018, p. 332–336*), П. Де Филиппи, М. Маннан и У. Рейджерс [20] (*De Filippi, Mannan, 2020*), М. Аллес и Г.Л. Грей [21] (*Alles, Gray, 2020*), М.А. Уддин, А. Страньери, И. Гондал и В. Баласубраманьян [22] (*Uddin Md Ashraf, Stranieri Andrew, Gondal Iqbal, Balasubramanian Venki, 2020*), а также состояния механизмов консенсуса на сегодняшний день, зафиксированных в трудах: Коробейникова И.А. [6, с. 27–29] (*Korobeynikov, 2020, p. 27–29*), Крохина М.О. [7, с. 7–9] (*Krokhin, 2019, p. 7–9*), Чахкиева М.Т. [8, с. 1737–1745] (*Chakhkiev, 2022, p. 1737–1745*), Ли К., Ли Х., Уонг Х., Ан Х., Лу П., Уи П. и Чжу Ф. [9, с. 1–16] (*Li, Li, Wang, An, Lu, Yi, Zhu, 2020, p. 1–16*), Фомичева В.М. и Семибраторова И.В. [10, с. 5–19] (*Fomichyov, Semibratov, 2019, p. 5–19*), Сивлин Каур, Шитал Чатурведи, Аабха Шарма и Джаяпракаш Кап [12] (*Sivleen Kaur, Sheetal Chaturvedi, Aabha Sharma, 2022*).

Jayaprakash Kar, 2021), У. Уонг, Д.Т. Хоанг, П. Ху, З. Сюн, Д. Ниято, П. Уонг, У. Вен и Д.И. Ким [13, с. 22328–22370], Чжан И. и Сяо-Хуэй Л.И. [14] (Zhang, Xiao-Hui, 2018), Бардина А.П., Новицкого А.В. и Шумилого Ю.Ю. [15, с. 27–40] (Bardin, Novitskiy, Shumilov, 2021, p. 27–40), Ку Хе, Н. Гян, М. Л. и В. Уи [23, с. 1–10] (He, Guan, Lv, Yi, 2018, p. 1–10), Лашкари Б. и Мусилек П. [24, с. 43620–43652] (Lashkari, Musilek, 2021, p. 43620–43652).

Цель данной статьи – рассмотреть все популярные на сегодняшний день механизмы консенсуса и проанализировать их применимость для решения различных бизнес-задач, для последующего вывода о возможности эффективного и надежного использования отдельно взятых алгоритмов консенсуса в тех областях бизнеса, где это будет наиболее рационально и скординировано.

Научная новизна исследования заключается в обобщении и систематизации информации о наиболее распространенных механизмах консенсуса, применяемых в блокчейн-системах.

Обзор популярных механизмов консенсуса

Механизмы консенсуса позволяют элементам распределенных систем совместно функционировать и при этом обеспечивают высокий уровень безопасности. Исторически эти механизмы использовались для достижения консенсуса между узлами баз данных, серверами приложений и другой корпоративной инфраструктурой. В последние годы были разработаны новые механизмы консенсуса, позволяющие криптоэкономическим системам, таким как Ethereum, договариваться о состоянии сети.

Механизм консенсуса можно рассматривать как общую систему стандартов и шагов, которая позволяет распределенной системе точно и надежно координировать общие проблемы.

Понимание механизмов консенсуса позволяет оценить экологические последствия инвестирования в криптографию. Инвестиции в ESG были популярны в традиционных финансах, но аналогичные стандарты могут применяться в криптомире. Знание о механизмах консенсуса позволяет людям увидеть, как системы блокчейна работают внутри, и в конечном итоге развить более полное понимание того, как они влияют на окружающую среду. Кроме того, широкое понимание механизмов консенсуса также позволит инвесторам и регулирующим органам лучше оценить безопасность отдельных блокчейнов [4] (Krishitanosov, 2020). Например, мы знаем, что блокчейн биткойна более безопасен, чем большинство блокчейнов PoS, потому что он ис-

пользует консенсус Накамото. Лучшее понимание безопасности блокчейна в конечном итоге принесет большую прозрачность как инвесторам, так и регулирующим органам и, таким образом, будет способствовать более широкому распространению технологий распределенных реестров. Механизмы консенсуса также определяют ключевую метрику для блокчейнов, то есть скорость транзакций. Например, блокчейны, работающие на консенсусе Накамото, могут быть более безопасными, но их безопасность достигается ценой более длительного времени подтверждения. Длительное время подтверждения – это то, что обеспечивает их безопасность [5] (*Tasca, Tessone, 2019*).

Ключевые характеристики наиболее популярных механизмов консенсуса представлены в *таблице 1*.

Таблица 1

Механизмы консенсуса в блокчейне

| Механизм консенсуса | Характеристика | Алгоритм работы |
|----------------------|--|---|
| Proof-of-Work (PoW) | Устойчивость к кибератакам, так как любая успешная атака потребует не менее половины мощности хеширования всей сети; высокое энергопотребление; ограниченная масштабируемость и невысокая пропускная способность [6] (<i>Korobeynikov, 2020</i>). Используется в монетах Bitcoin, Ethereum и Litecoin | Для проверки блока майнеры должны решить произвольную математическую головоломку через устройства для майнинга. Цель головоломки – гарантировать, что определенное вычислительное усилие, называемое майнингом, выполняется майнерами, что дает им право добавлять новые транзакции в блокчейн. Тот, кто первым решит головоломку, получит награду [7] (<i>Krokhin, 2019</i>) |
| Proof-of-Stake (PoS) | Более энергоэффективен и децентрализован, чем PoW. Недостаток – мотивация в концентрации средств, что может приводить к централизации сети [8] (<i>Chakhkiev, 2022</i>). Используется в блокчейн-сетях Polkadot, EOSIO, Cardano | PoS использует псевдослучайный детерминированный алгоритм для выбора валидатора для проверки транзакций в блоке. В PoS есть валидаторы, которые выбираются среди различных консенсусных валидаторов в сети блокчейн. Чтобы стать валидатором, узел консенсуса должен выставить в качестве гарантированного депозита несколько монет в сети, чем больше этот депозит, тем выше шансы на то, что узел станет валидатором. Узел получает вознаграждение не за создание блока, а за проведение транзакции. Валидатор рискует потерять часть своего депозита, если он подтвердит мошенническую транзакцию [8] (<i>Chakhkiev, 2022</i>) |

Продолжение табл. 1

| | | |
|------------------------------|---|---|
| Leased Proof-of-Stake (LPoS) | <p>Модификация PoS.</p> <p>Любой пользователь имеет возможность передавать свой баланс в аренду майнинг-узлам, а за это майнинг-узлы делятся частью прибыли с пользователями. Таким образом, PoS позволяет получить доход от майнинговой деятельности, не ведя самого майнинга [9] (<i>Li, Li, Wang, An, Lu, Yi, Zhu, 2020</i>)</p> | <p>Майнеры запускают узлы для защиты сети Waves и получают вознаграждение. Их награды зависят от количества монет, которые они используют для майнинга. Чем больше монет, тем больше награда. Чем выше сумма узла (вместе с монетами, взятыми в аренду), тем больше шансов, что для создания следующего блока будет выбран полный узел. Если узел выбран, пользователь будет получать процент от комиссии за транзакции, которые собирает этот узел [9] (<i>Li, Li, Wang, An, Lu, Yi, Zhu, 2020</i>)</p> |
| Proof-of-Capacity (PoC) | <p>Возможность задействования любых жестких дисков, что снижает энергопотребление;</p> <p>не требуется специальное оборудование; обращения к жесткому диску занимают существенное время;</p> <p>чем больше средств проверки пространства на жестком диске, тем больше у валидатора шансов попасть на майнинг следующего блока и получить награду за блок. Используется в блокчейн-системах Filecoin, Storj, Burstcoin [10] (<i>Fomichyov, Semibratov, 2019</i>)</p> | <p>Каждый майнер вычисляет достаточно большой объем данных, который записывается на дисковую подсистему (жесткий диск, облачные системы хранения) узла. Для каждого нового блока в блокчейне майнер читает небольшой набор данных от своего общего сохраненного объема и возвращает результат (дедлайн) как прошедшее время в секундах с момента создания последнего блока, после которого майнер сможет создать новый блок. Майнер, получивший минимальное время дедлайна, подписывает блок и получает вознаграждение за транзакции [8] (<i>Chakhkiev, 2022</i>)</p> |
| Proof-of-Importance (PoI) | <p>Учитывает как количество средств, так и активность пользователя в блокчейн-сети. Такой подход заставляет пользователей не просто держать средства у себя на счету, но и активно использовать их.</p> <p>Преимущества: механизм экологичен, так как отсутствуют затраты электроэнергии на верификацию.</p> <p>Недостаток: возможность фиктивных транзакций [8] (<i>Chakhkiev, 2022</i>)</p> | <p>В обмен на сбор блоков узлы могут взимать комиссию за транзакции в этом блоке. На вероятность получить право сформировать новый блок влияет: количество криптовалюты на балансе, активность аккаунта (взаимодействие с другими пользователями), время нахождения аккаунта в сети. Обеспечивает сохранность работы блокчейна путем предоставления привилегий создания блоков участникам с наилучшей репутацией [7] (<i>Krokhin, 2019</i>)</p> |
| Proof-of-Activity (PoA) | <p>В POA процесс майнинга начинается как стандартный процесс POW с участием различных майнеров, пытающихся опередить друг друга в нахождении решения нового блока с помощью более высокой вычислительной мощности. При обнаружении нового блока система переключается на POS с новым найденным блоком, содержащим только заголовок и адрес вознаграждения майнера [11]</p> | <p>Первым делом майнер ищет верный хэш. После нахождения хэша майнер отправляет его в сеть блокчейн, где информация хэша – не полноценный готовый блок, а «заготовка». Для того чтобы сформировался блок и записался в блокчейн-сеть, PoS-майнера (холдеры) должна прописать «заготовку». Вознаграждение за блок распределяется между майнераами и холдерами [11]</p> |

Продолжение табл. 1

| | | |
|------------------------------------|---|--|
| Proof-of-Authority (Po-Autho-rity) | <p>Основанный на репутации алгоритм консенсуса, который использует ценность идентичности и репутации валидаторов блоков. Доверенные узлы выбираются лидерами сетей, что делает PoA полезным только для частных блокчейнов.</p> <p>Высокая скорость транзакций, масштабируемость, невысокая стоимость обслуживания сети (по причине отсутствия майнинга); отказ от децентрализации, возможное злонамеренное поведение участников сети, которое практически невозможно предотвратить.</p> <p>Используется в VeChain Thor, Microsoft Azure [12] (<i>Sivleen Kaur, Sheetal Chaturvedi, Aabha Sharma, Jayaprakash Kar, 2021</i>)</p> | <p>Все транзакции и блоки проверяются посредством одобренных аккаунтов (валидаторов). Проведение транзакций и создание блоков проходит в автоматическом режиме при помощи вычислительных мощностей валидатора [12] (<i>Sivleen Kaur, Sheetal Chaturvedi, Aabha Sharma, Jayaprakash Kar, 2021</i>)</p> |
| Proof-of-Burn (PoB) | <p>Протокол работает по принципу разрешения майнерам уничтожать токены виртуальной валюты, что дает им право писать блоки пропорционально горевшим монетам. Такой алгоритм имеет смысл использовать только на поздних этапах существования той или иной криптовалюты. PoB используется на платформе Slimcoin. Главным преимуществом этого механизма является тот факт, что данный подход не потребляет ресурсов [10] (<i>Fomichyov, Semibratov, 2019</i>)</p> | <p>Майнер отправляет монеты на случайный адрес сгенерированного хеша, потратить средства с этого адреса практически невозможно, так как вероятность подобрать к нему ключи стремится к нулю. За такое уничтожение монет майнер получает постоянный шанс найти PoB блок и получить за него награду. Шансы на майнинг увеличиваются при увеличении количества сожженных монет. Майнеры должны предоставить доказательства того, что они сожгли несколько монет, то есть отправили их на проверяемый ненадежный адрес</p> |
| Proof of Weight (Po-Weight) | <p>Снижает риск атаки двойной траты токенов, сохранив сеть в безопасности. Этот алгоритм обладает высокой масштабируемостью и является энергоэффективным, что является его сильной стороной. PoWeight гарантирует, что большинство пользователей согласятся с принятым решением. Однако большим минусом данного алгоритма является система получения вознаграждения за блок – она довольно сложная [10] (<i>Fomichyov, Semibratov, 2019</i>)</p> | <p>Механизм консенсуса «взвешивает» каждого пользователя и определяет его вес в зависимости от количества монет, которыми тот владеет. PoWeight гарантирует, что две трети пользователей честны – то есть имеют необходимый баланс для подтверждения веса. Эта особенность позволяет организатору сети создать на основе PoWeight сообщество из случайных владельцев монет для запуска каждого шага протокола [10] (<i>Fomichyov, Semibratov, 2019</i>)</p> |

Продолжение табл. 1

| | | |
|---------------------------------|--|---|
| Proof of History (PoH) | <p>PoH является гибридом, поскольку валидаторы в сети Solana выбираются протоколами Proof of Stake. Решает проблему согласования времени (позволяет консенсусным узлам работать быстрее, кодируя время в блокчейне).</p> <p>PoH является самым быстрым и безопасным способом достижения консенсуса в сети блокчейн. Основным преимуществом PoH является то, что узлам не нужно постоянно взаимодействовать, чтобы договориться о времени выполненной проверки [13] (Wang, Hoang, Hu, Xiong, Niyato, Wang, Wen, Kim, 2019)</p> | <p>PoH использует функцию проверяемой задержки для добавления временной задержки к генерируемым хэшам. Эта функция принимает задержку в качестве параметра, чтобы валидаторы знали порядок, в котором произошла транзакция. Выходные данные функции проверяемой задержки затем проверяются узлами валидатора с помощью последовательных вычислений. Затем блоки добавляются в блокчейн. В механизме консенсуса PoH узел содержит запись о том, что конкретная транзакция произошла в один конкретный момент времени [13] (Wang, Hoang, Hu, Xiong, Niyato, Wang, Wen, Kim, 2019)</p> |
| Delegated Proof-of-Stake (DPoS) | <p>Разновидность механизма консенсуса PoS, в которой блоки подписывают выбранные представители. Преимущества: держатели балансов имеют возможность делегировать свои голоса, при этом не передавая сам баланс; держатели балансов имеют возможность получить дополнительный доход от их владения; минимизация издержек на поддержку блокчейн-сети. В отличие от классического PoS, снижается количество ненужной работы при выборе следующего голосующего [14] (Zhang, Xiao-Hui, 2018)</p> | <p>Владельцы наибольших балансов выбирают своих представителей, каждый из которых получает право подписывать блоки в блокчейн-сети. Каждый представитель, обладающий одним процентом или более от всех голосов, попадает в совет. Из сформированного «совета директоров» выбирается следующий представитель, который подпишет следующий блок. В том случае, если по какой-либо причине представитель пропустил свою очередь в подписании, он лишается делегированных голосов и покидает «совет директоров», после чего на его место выбирается следующий наиболее подходящий кандидат. Владельцы балансов, делегируя свои голоса, не теряют над ними контроля, так как в любой момент могут их отозвать у своего представителя [14] (Zhang, Xiao-Hui, 2018)</p> |
| Proof of Elapsed Time (PoET) | <p>Более энергоэффективная модификация PoW. Одна из основных его идей – использование принципов справедливой лотереи. Все узлы имеют одинаковый шанс на вознаграждение и это справедливо для максимально возможного числа участников. Функция должна распределять выборы лидеров среди максимально широкого круга участников; стоимость контроля над процессом выбора лидера должна быть пропорциональна полученной от него выгоде; всем участникам относительно просто убедиться в том, что лидер был выбран законным образом [13] (Wang, Hoang, Hu, Xiong, Niyato, Wang, Wen, Kim, 2019)</p> | <p>Каждый узел в блокчейне генерирует случайное время ожидания и переходит в спящий режим на указанный промежуток времени. Первым «просыпается» тот участник, у которого самое короткое время ожидания. Он включает новый блок в цепочку, передавая необходимую информацию всей одноранговой сети. Затем повторяется тот же процесс для обнаружения следующего блока [13] (Wang, Hoang, Hu, Xiong, Niyato, Wang, Wen, Kim, 2019)</p> |

Окончание табл. 1

| | | |
|---|---|--|
| Byzantine Fault Tolerance (BFT) | <p>Создатели данного механизма консенсуса увидели связь между «проблемой византийских генералов» и проблемой поиска консенсуса в распределенной базе данных блокчейна. В некоторых приложениях, где целостность цепочки является обязательной, как, например, в платформах управления цифровыми активами, создание быстрой связи между сетями является краеугольным камнем использования блокчейна. Этот подход к алгоритму консенсуса основан на массовой координации. Преимущества BFT-подхода в том, что это недорогое решение, которое можно масштабировать. Тем не менее этот подход еще не завоевал доверие сообщества [15] (Bardin, Novitskiy, Shumilov, 2021)</p> | <p>BFT группирует узлы в более мелкие сети. Внутри каждой группы большинство узлов голосует за ведущий узел, который проверяет блоки на основе информации, полученной от связанных узлов. Цель системы – предотвратить участие вредоносных узлов в создании блоков, что делает блокчейн менее подверженным атакам и более быстрым, поскольку не требует, как PoW, верификации блока [8] (Chakhkiev, 2022)</p> |
| Simplified Byzantine Fault Tolerance (SBFT) | <p>Модификация BFT, отличающаяся тем, что транзакции и новые блоки могут предлагаться одним узлом [12] (Sivleen Kaur, Sheetal Chaturvedi, Aabha Sharma, Jayaprakash Kar, 2021)</p> | <p>В SBFT один назначенный генератор блоков собирает и проверяет предложенные транзакции, периодически объединяя их в новый блок. Консенсус обеспечивается генератором, который применяет правила (проверки), согласованные узлами (ядрами цепочки) к блоку и назначенным подписчиком блока. Другие (множественные) назначенные подписчики блоков ратифицируют предложенный блок своими подписями. Все члены сети знают идентификаторы подписавших блок и принимают блоки только в том случае, если они подписаны достаточным количеством подписчиков [12] (Sivleen Kaur, Sheetal Chaturvedi, Aabha Sharma, Jayaprakash Kar, 2021)</p> |
| Delegated Byzantine Fault Tolerance (DBFT) | <p>Механизм консенсуса, обеспечивающий крупномасштабное участие в консенсусе через голосование по доверенности. Владелец токена, голосуя, может выбрать бухгалтера, которого он поддерживает. Используется в системе NEO [12] (Sivleen Kaur, Sheetal Chaturvedi, Aabha Sharma, Jayaprakash Kar, 2021)</p> | <p>Все узлы выбирают группу согласованных узлов. Из этой группы «бухгалтеры» выбираются случайным образом. Остальные узлы консенсуса затем принимают роль делегатов. Выбранная группа бухгалтеров через алгоритм BFT достигает консенсуса и генерирует новые блоки [12] (Sivleen Kaur, Sheetal Chaturvedi, Aabha Sharma, Jayaprakash Kar, 2021)</p> |

Источник: составлено авторами.

Сфера применения технологии блокчейн в бизнес-практике

В процессе внедрения технологии блокчейн в различных сферах постепенно формулировались различные требования к механизмам консенсуса в части надежности, скорости транзакций и энергоэффективности. В зависимости от бизнес-процесса, в который интегрируется блокчейн, приоритетными будут те или иные характеристики. Рассмотрим бизнес-сфера, в которых может применяться технология распределенного реестра.

Отраслевые и глобальные производственные цепочки и системы Интернета вещей. Производство пищевых продуктов – отрасль, где проблема фальсификации и низкого качества поставляемой продукции имеет большое общественное значение. В 2017 году компании Walmart и IBM создали блокчейн-систему для контроля поставок на платформе Hyperledger Fabric. Ключевыми задачами системы является выявление фальсификации пищевой продукции и обеспечение отзыва товаров в случае вспышек заболеваний, связанных с некачественной продукцией. Еще одним примером блокчейн-платформы для отслеживания грузов с помощью смарт-контрактов является система CargoChain, причем данная платформа предлагает разработчикам инструменты для разработки индивидуальных корпоративных решений для клиентов [16] (*Zutshi, Grilo, Nodehi, 2021*).

Банковские и финансовые услуги. В финансовой сфере внедрение блокчейна способно снизить риски и оптимизировать координацию в процес сах, включающих несколько участников и посредников. Распространенным примером недостатка сегодняшних банковских систем является низкая скорость международных банковских переводов, занимающих несколько дней из-за требований к учету в нескольких банковских сетях. Блокчейн-система Ripple предоставляет банкам услуги мгновенных одноранговых денежных переводов, при этом из процесса исключены посредники, а процедура перевода значительно упрощается. Существует еще ряд приложений, созданных на платформе Ethereum (MakerDAO, Compound) и позволяющих отслеживать кредиты, страхование, инвестиции и различные выплаты при помощи смарт-контрактов [17] (*Casino, Dasaklis, Patsakis, 2019*).

Цифровые сертификаты, поддающиеся публичной проверке, в том числе академические, нормативные, сертификаты качества и др. Например, компания Hyland Software Inc разработала открытый блокчейн-стандарт Blockcerts, позволяющий учреждениям выдавать цифровые сертификаты различной направленности [18] (*Huynh, 2018*).

Охрана интеллектуальной собственности. Невзаимозаменяемые токены, являющиеся уникальными и неделимыми в отличие от криптовалют, обеспечивают предоставление права собственности на цифровой или физический актив и могут быть использованы для регистрации объектов интеллектуальной собственности, примером платформы такого рода является IPChain [19] (*Kashavarova, Starikova, 2022*).

Юридические соглашения. Так, например, компании Codelegit и Agrello предлагают услуги хранения юридических контрактов в блокчейн-системе [20] (*De Filippi, Mannan, 2020*).

Управление физическими активами. Платформа Bitland, пилотный проект которой был запущен в Гане, предлагает распределенный реестр для регистрации недвижимости, земли и других типов активов, обеспечивающий эффективную передачу прав собственности [21] (*Alles, Gray, 2020*).

Управление персональными данными. Блокчейн-системы для хранения и отслеживания персональных данных востребованы в сегменте здравоохранения для децентрализованного хранения и управления электронными медицинскими записями, цифровыми изображениями и цифровыми рецептами. Так, например, эстонский фонд электронного здравоохранения совместно с проектом Guardtime запустил инфраструктуру бесключевой подписи. Британский стартап FarmaTrust предлагает решения для отслеживания фармацевтических препаратов и персонализированной медицины [22] (*Uddin Md Ashraf, Stranieri Andrew, Gondal Iqbal, Balasubramanian Venki, 2020*).

Заключение

Механизмы консенсуса необходимы для обеспечения ключевой особенности блокчейн-систем – децентрализованности. В отсутствие координирующего органа участники сети должны на равноправной основе подтверждать транзакции, и это было бы невозможно в масштабах, необходимых в сегодняшней экономике, без интеллектуального алгоритма, способного автоматически проверять новые транзакции и связывать их со всем оборудованием в сети. Механизмы консенсуса развиваются, становясь более быстрыми и энергоэффективными, что расширяет возможности их практического использования. На сегодняшний день существует большое количество пилотных проектов по внедрению блокчейн-систем в финансовой сфере, логистике, ритейле, здравоохранении, охране исключительных прав и многих других областях. Свои действия каждый участник подтверждает с помощью приватного персонального ключа [23] (*He, Guan, Lv, Yi, 2018*), а решение про-

блемы доверия к экономическим системам в децентрализованных финансах решается с помощью развития византийской отказоустойчивости (BFT), разработки надежных механизмов консенсуса и создания шифрования с открытым/закрытым ключом [24] (*Lashkari, Musilek, 2021*).

В России на сегодняшний день крупные компании активно интегрируют блокчейн в свои производства. Такие компании, как «М.Видео», «Альфа-Банк», Сбербанк, уже запустили свою платформу на базе алгоритма PoW для стандартных банковских операций, что отражается на быстроте и экономности сверок документов и отчетности. «Норникель» и другие горно-металлургические компании используют блокчейн на основе механизма византийской отказоустойчивости для мониторинга цепочек поставок, где металлы обеспечиваются токенами.

ИСТОЧНИКИ:

1. Травушкина А.А., Щелокова А.Н., Шиболденков В.А., Юсуфова О.М. [Обзор перспектив развития технологии цифровых двойников продуктов, услуг и сервисов в секторе материального производства](#) // Вопросы инновационной экономики. – 2022. – № 3. – с. 1485–1502. – doi: 10.18334/vinec.12.3.115215.
2. Дроговоз П.А., Харин Н.И. [Экономический эффект от внедрения технологий цифрового производства в нефтегазовой отрасли](#) // Финансы и кредит. – 2021. – № 3. – с. 672–693. – doi: 10.24891/fc.27.3.672.
3. Носиров З.А., Фомичев В.М. [Анализ блокчейн-технологии: основы архитектуры, примеры использования, перспективы развития, проблемы и недостатки](#) // Системы управления, связи и безопасности. – 2021. – № 2. – с. 37–75. – doi: 10.24412/2410–9916–2021–2–37–75.
4. Криштаносов В.Б. Блокчейн: технологический и экономический аспекты // Труды БГТУ. – 2020. – № 2. – с. 13–32.
5. Tasca P., Tessone C.J. [A taxonomy of blockchain technologies: principles of identification and classification](#) // Ledger 4. – 2019. – № 4. – doi: 10.5195/ledger.2019.140.
6. Коробейников И.А. Особенности классификации криптовалют // Вестник магистратуры. – 2020. – № 4–3(103). – с. 27–29.
7. Крохин М.О. [Обзор современных алгоритмов консенсуса в системах блокчейн](#) // Молодой ученый. – 2019. – № 28(266). – с. 7–9.
8. Чахкиев М.Т. Алгоритмы достижения консенсуса в блокчейн-системе // Научно-образовательный журнал для студентов и преподавателей. – 2022. – № 3.
9. Li K., Li H., Wang H., An H., Lu P., Yi P., Zhu F. [PoV: An Efficient Voting-Based Consensus Algorithm for Consortium Blockchains](#) // Front. Blockchain. – 2020. – № 3(11). – doi: 10.3389/fbloc.2020.00011.

10. Фомичев В.М., Семибратов И.В. [Свойства механизмов консенсуса в технологии Блокчейн](#) // Системы высокой доступности. – 2019. – № 2. – с. 5–19.
11. Parma Bains Blockchain Consensus Mechanisms: A Primer For Supervisors // FinTech Notes No 2022/003
12. Sivleen Kaur, Sheetal Chaturvedi, Aabha Sharma, Jayaprakash Kar [A Research Survey on Applications of Consensus Protocols in Blockchain](#) // Security and Communication Networks. – 2021. – doi: 10.1155/2021/6693731.
13. Wang W., Hoang D. T., Hu P., Xiong Z., Niyato D., Wang P., Wen Y., Kim D. I. A survey on consensus mechanisms and mining strategy management in blockchain networks // IEEE Access. – 2019. – p. 22328– 22370.
14. Zhang Y., Xiao-Hui L. I. The research and implementation of an improved blockchain's consensus mechanism // Electronic Design Engineering. – 2018.
15. Бардин А.П., Новицкий А.В., Шумилов Ю.Ю. [Обработка ошибочных ситуаций в больших блокчейн-сетях алгоритмом достижения консенсуса, основанном на решении задачи византийских генералов](#) // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. – 2021. – № 4 (137). – с. 27–40.
16. Zutshi A., Grilo A., Nodehi T. The value proposition of blockchain technologies and its impact on Digital Platforms // Computers and Industrial Engineering. – 2021.
17. Casino F., Dasaklis T. K., Patsakis C. [A systematic literature review of blockchain-based applications: Current status, classification and open issues](#) // Telematics and Informatics. – 2019. – p. 55–81.
18. Huynh T. T. [Issuing and verifying digital certificates with blockchain](#) // 2018 International conference on advanced technologies for communications (ATC). – 2018. – p. 332–336. – doi: 10.1109/ATC.2018.8587428.
19. Кашеварова Н.А., Старикова И.С. [Невзаимозаменяемый токен: перспективный цифровой инструмент для бизнеса](#) // Вестник университета. – 2022. – № 3. – с. 44–51. – doi: <https://doi.org/10.26425/1816-4277-2022-3-44-51>.
20. P. De Filippi M., Mannan W. Reijers Blockchain as a confidence machine: The problem of trust & challenges of governance // Technology in Society. – 2020. – № 62.
21. Alles M., Gray G.L. “The first mile problem”: Deriving an endogenous demand for auditing in blockchain-based business processes // International Journal of Accounting Information Systems. – 2020. – p. 100465.
22. Uddin Md Ashraf, Stranieri Andrew, Gondal Iqbal, Balasubramanian Venki [Blockchain leveraged decentralized IoT eHealth framework](#) // Internet of Things. – 2020. – № 9. – p. 100159. – doi: 10.1016/j.iot.2020.100159.
23. He Q., Guan N., Lv M., Yi W. On the consensus mechanisms of blockchain/dlt for internet of things // 2018 IEEE 13th International Symposium on Industrial Embedded Systems (SIES). IEEE. 2018. – p. 1–10.
24. Lashkari B., Musilek P. A comprehensive review of blockchain consensus mechanisms // IEEE Access. 2021.

REFERENCES:

- Alles M., Gray G.L. (2020). “*The first mile problem*”: *Deriving an endogenous demand for auditing in blockchain-based business processes* *International Journal of Accounting Information Systems*. 100465.
- Bardin A.P., Novitskiy A.V., Shumilov Yu.Yu. (2021). *Obrabotka oshibochnyh situatsiy v bolshikh blokcheyn-setyakh algoritmom dostizheniya konsensusa, osnovannom na reshenii zadachi vizantiyskikh generalov* [Processing erroneous situations in large blockchain networks by a consensus algorithm based on the Byzantine generals’ problem solution]. *Vestnik MGTU im. N.E. Baumana. Ser. Priborostroenie*. (4 (137)). 27–40. (in Russian).
- Casino F., Dasaklis T. K., Patsakis C. (2019). *A systematic literature review of blockchain-based applications: Current status, classification and open issues* *Telematics and Informatics*. 36 55–81.
- Chakhkiev M.T. (2022). *Algoritmy dostizheniya konsensusa v blokcheyn-sisteme* [Algorithms for achieving consensus in the blockchain system]. *Nauchno-obrazovatelnyy zhurnal dlya studentov i prepodavateley*. (3). (in Russian).
- Drogovoz P.A., Kharin N.I. (2021). *Ekonomicheskiy effekt ot vnedreniya tekhnologiy tsifrovogo proizvodstva v neftegazovoy otrassli* [The economic benefits of digitalization in the oil and gas industry]. *Finance and credit*. (3). 672–693. (in Russian). doi: [10.24891/fc.27.3.672](https://doi.org/10.24891/fc.27.3.672).
- Fomichyov V.M., Semibratov I.V. (2019). *Svoystva mekhanizmov konsensusa v tekhnologii Blokcheyn* [Properties of consensus mechanisms in blockchain technology]. *Sistemy vysokoy dostupnosti*. (2). 5–19. (in Russian).
- He Q., Guan N., Lv M., Yi W. (2018). *On the consensus mechanisms of blockchain/dlt for internet of things 2018 IEEE 13th International Symposium on Industrial Embedded Systems (SIES)*. IEEE. 1–10.
- Huynh T. T. (2018). *Issuing and verifying digital certificates with blockchain 2018 International conference on advanced technologies for communications (ATC)*. 332–336. doi: [10.1109/ATC.2018.8587428](https://doi.org/10.1109/ATC.2018.8587428).
- Kashevarova N.A., Starikova I.S. (2022). *Nevzaimozamenyaemyy token: perspektivnyy tsifrovoy instrument dlya biznesa* [Non-interchangeable token: a promising digital tool for business]. *Vestnik Universiteta*. (3). 44–51. (in Russian). doi: <https://doi.org/10.26425/1816-4277-2022-3-44-51>.

- Korobeynikov I.A. (2020). *Osobennosti klassifikatsii kriptoanalyut* [Features of the classification of cryptocurrencies]. *Vestnik Magistratury*. (4–3(103)). 27–29. (in Russian).
- Krishtanov V.B. (2020). *Blokcheyn: tekhnologicheskiy i ekonomicheskiy aspekty* [Blockchain: technological and economic aspects]. *Trudy BGTU*. (2). 13–32. (in Russian).
- Krokhin M. O. (2019). *Obzor sovremennoy algoritmov konsensusa v sistemakh blokcheyn* [Overview of modern consensus algorithms in blockchain systems]. *The young scientist*. (28(266)). 7–9. (in Russian).
- Lashkari B., Musilek P. (2021). *A comprehensive review of blockchain consensus mechanisms IEEE Access*.
- Li K., Li H., Wang H., An H., Lu P., Yi P., Zhu F. (2020). *PoV: An Efficient Voting-Based Consensus Algorithm for Consortium Blockchains Front. Blockchain*. (3(11)). doi: [10.3389/fbloc.2020.00011](https://doi.org/10.3389/fbloc.2020.00011).
- Nosirov Z. A., Fomichev V. M. (2021). *Analiz blokcheyn-tehnologii: osnovy arhitektury, primery ispolzovaniya, perspektivy razvitiya, problemy i nedostatki* [Analysis of blockchain technology: architectural basics, application examples, future trends, problems and disadvantages]. *Sistemy upravleniya, svyazi i bezopasnosti*. (2). 37–75. (in Russian). doi: [10.24412/2410-9916-2021-2-37-75](https://doi.org/10.24412/2410-9916-2021-2-37-75).
- P. De Filippi M., Mannan W. (2020). *Reijers Blockchain as a confidence machine: The problem of trust & challenges of governance Technology in Society*. (62).
- Sivleen Kaur, Sheetal Chaturvedi, Aabha Sharma, Jayaprakash Kar (2021). *A Research Survey on Applications of Consensus Protocols in Blockchain Security and Communication Networks*. doi: [10.1155/2021/6693731](https://doi.org/10.1155/2021/6693731).
- Tasca P., Tessone C.J. (2019). *A taxonomy of blockchain technologies: principles of identification and classification Ledger* 4. (4). doi: [10.5195/ledger.2019.140](https://doi.org/10.5195/ledger.2019.140).
- Travushkina A.A., Schelokova A.N., Shiboldenkov V.A., Yusufova O.M. (2022). *Obzor perspektiv razvitiya tekhnologii tsifrovyyh dvoynikov produktov, uslug i servisov v sektore materialnogo proizvodstva* [Prospects for the development of digital twin technology of products and services in the material production]. *Russian Journal of Innovation Economics*. 12 (3). 1485–1502. (in Russian). doi: [10.18334/vinec.12.3.115215](https://doi.org/10.18334/vinec.12.3.115215).

- Uddin Md Ashraf, Stranieri Andrew, Gondal Iqbal, Balasubramanian Venki (2020). *Blockchain leveraged decentralized IoT eHealth framework Internet of Things*. (9). 100159. doi: [10.1016/j.iot.2020.100159](https://doi.org/10.1016/j.iot.2020.100159).
- Wang W., Hoang D. T., Hu P., Xiong Z., Niyato D., Wang P., Wen Y., Kim D. I. (2019). *A survey on consensus mechanisms and mining strategy management in blockchain networks IEEE Access*. 7 22328– 22370.
- Zhang Y., Xiao-Hui L. I. (2018). *The research and implementation of an improved blockchain's consensus mechanism Zhang Y, Xiao-Hui L I. The research and implementation of an improved blockchain\\'s consensus mechanism [J]. Electronic Design Engineering*, 2018.
- Zutshi A., Grilo A., Nodehi T. (2021). *The value proposition of blockchain technologies and its impact on Digital Platforms Computers and Industrial Engineering*. 155