УДК 004.75 **DOI: 10.18413/2518-1092-2025-10-1-0-3**

Булгаков В.Д.
Гвоздевский И.Н.

АНАЛИЗ МЕХАНИЗМОВ КОНСЕНСУСА В БЛОКЧЕЙН-СИСТЕМАХ

Белгородский государственный технологический университет им. В.Г. Шухова,
ул. Костюкова, 46, г. Белгород, 308012, Россия

e-mail: BulgakovVlad@yandex.ru

Аннотация
В статье приведен анализ основных механизмов консенсуса для блокчейн-сетей: Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated-Proof-of-Stake (DPoS), Proof-of-Authority (PoA) и Proof-of-Capacity (PoC). Описаны алгоритмы работы данных механизмов, учтены их преимущества и недостатки. Проведено сравнение и предоставлены рекомендации по применению каждого алгоритма относительно поставленных перед блокчейн-сетью задачами.
В работе подчеркивается, как отдельные параметры этих механизмов влияют на процессы проверки и генерации блоков. В ней исследуется влияние этих факторов на общую производительность блокчейн-сетей, особенно с точки зрения безопасности, децентрализации, масштабируемости и энергоэффективности.
Работа закладывает основу для будущих исследований гибридных моделей, которые могут сочетать преимущества нескольких согласованных подходов для более эффективного решения возникающих проблем безопасности и растущих требований децентрализованных приложений.
Ключевые слова: блокчейн; механизмы консенсуса; децентрализация; безопасность; масштабируемость
Для цитирования: Булгаков В.Д., Гвоздевский И.Н. Анализ механизмов консенсуса в блокчейн-системах // Научный результат. Информационные технологии. – Т.10, №1, 2025. С. 24-35. DOI: 10.18413/2518-1092-2025-10-1-0-3

Bulgakov V.D.
Gvozdevsky I.N.

ANALYSIS OF CONSENSUS MECHANISMS IN BLOCKCHAIN SYSTEMS

Belgorod State Technological University named after V.G. Shukhov,
46 Kostyukova str., Belgorod, 308012, Russia

e-mail: BulgakovVlad@yandex.ru

Abstract
This article provides an analysis of the primary consensus mechanisms employed in blockchain networks, namely Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), Proof-of-Authority (PoA), and Proof-of-Capacity (PoC). The study thoroughly describes the operational algorithms of each mechanism, examining their inherent advantages and disadvantages. It conducts a comparative analysis and offers tailored recommendations for the implementation of each consensus algorithm based on the specific challenges and objectives of blockchain systems.
Furthermore, the work emphasizes how the individual parameters of these mechanisms influence the processes of block validation and generation. It explores the impact of these factors on the overall performance of blockchain networks, particularly in terms of security, decentralization, scalability, and energy efficiency.
By integrating theoretical insights with practical considerations, this research aims to guide both practitioners and researchers in the selection and optimization of consensus protocols. It also lays the groundwork for future investigations into hybrid models that may combine the strengths of multiple consensus approaches to better address evolving security challenges and the increasing demands of decentralized applications.
Keywords: blockchain; consensus mechanisms; decentralization; security; scalability

For citation: Bulgakov V.D., Gvozdevsky I.N. Analysis of consensus mechanisms in blockchain systems // Research result. Information technologies. – T.10, №1, 2025. – P. 24-35. DOI: 10.18413/2518-1092-2025-10-1-0-3

ВВЕДЕНИЕ

На сегодняшний день мы можем сказать, что технология блокчейн вышла за рамки своего первоначального применения, задуманного и описанного в сети Bitcoin. Сегодня это не только технология, обслуживающая интересы одной определенной криптовалюты, но и большое поле для разработки и адаптации технологии под различные сферы человеческой деятельности: от финансов и образования, до логистики и государственного управления.

Согласно данным заместителя главного редактора журнала Crypto.ru Евгения Лукина, на сегодняшний день в России разработки в области блокчейна используются в следующих отраслях:

- Банковский сектор: Банк России, Сбер, ВТБ, QIWI, Тинькофф;
- Промышленный сектор: Норникель, Газпром;
- Рынок ценных бумаг: Национальный расчетный депозитарий;
- Авиаперевозки: S7 [1].

Основой безопасности, надежности и прозрачности технологии являются механизмы консенсуса – алгоритмы, позволяющие всем участникам сети достигать определенного соглашения насчет текущего ее состояния. Обеспечение децентрализации сети также возможно только благодаря включению данных алгоритмов в ее архитектуру.

Механизмы консенсуса влияют не только на то, как сеть будет обрабатывать решения и соглашения ее участников, но они также способствуют снижению риска атак, попыток мошенничества и различных манипуляций недобросовестных участников сети. Однако, не смотря на кажущуюся простоту конечной цели алгоритмов консенсуса, разнообразие существующих ныне решений и подходов в этой области говорит о сложности при выборе оптимального решения для каждого конкретного случая применения технологии.

Цель данной работы – привести наиболее конкретные и наглядные примеры механизмов консенсуса, их описание, алгоритмы и возможные поля применения. Выявить их преимущества и недостатки, а также рассмотреть, как выбор определенного алгоритма влияет на поведение и характеристики всей сети, включая параметры безопасности, масштабируемости, скорости обработки транзакций и показатели энергоэффективности.

PROOF-OF-WORK

Механизм Proof-of-Work (PoW) является одним из первых, и, пожалуй, самым известным алгоритмом консенсуса в сфере блокчейн-технологий. В его основе лежит идея о том, что участник сети, для того чтобы совершить процесс создания нового блока, должен выполнить трудоемкую задачу – «доказать работу», которая требует определенных вычислительных мощностей. Само по себе решение данной задачи не несет никакой практической пользы, кроме того, что участник, решивший ее, доказывает свою добросовестность, так как тратит ресурсы [2].

Процесс решения задачи в механизме PoW называется «майнингом». И тот участник сети, который быстрее всех находит решение задачи, получает право добавить в сеть новый блок. За это в механизме предусмотрена награда. Сама задача состоит в поиске определенного хэша, который необходимо найти участникам сети. Например, алгоритм может поставить следующую задачу: «Первый участник сети, который найдет и предоставит число, хэш которого в алгоритме хэширования SHA-256 будет начинаться с пяти нолей, получит право на создание нового блока в сети». Сложность задачи определяется самим алгоритмом и зависит от количества «майнеров» в сети – участников, которые стремятся совершить процесс создания нового блока. После того, как один из участников нашел решение задачи, он предоставляет остальным участникам сети ответ, но

само решение остается только у него. Ответа достаточно, чтобы определить, корректно ли майнер выполнил свою работу, и, в случае если большинство участников сети согласны с ответом, то майнеру предоставляется возможность создания нового блока [3].

Для представления поставленной перед майнерами задачи можно привести следующий пример:

«Лотерея проводит розыгрыш призов. Заранее известен номер победного билета, например №7236. Задача участников – купить именно победный билет. В кассе лотереи билеты продаются в случайном порядке, поэтому заранее вычислить, когда нужно прийти за билетом – невозможно. Очевидно, что участник, обладающий наибольшим количеством свободных денег, сможет купить наибольшее количество билетов, и, соответственно, увеличить свои шансы на победу. Но не исключена ситуация, что победный билет может выкупить человек, денег у которого хватит только лишь на один единственный билет.

После того, как какой-то участник сети выкупает билет №7236, он показывает его другим участникам розыгрыша. Когда участники согласны с тем, что человек действительно выкупил победный билет – он получает свой выигрыш» [4].

Данный пример описывает одну итерацию создания нового блока. После этого, «лотерея» объявляет номер нового победного билета и все начинается заново.

Алгоритм выполнения итерации по созданию блока в механизме Proof-of-Work выглядит следующим образом:

1. Сбор транзакций. Все майнеры собирают из хранилища (mempool) транзакции, которые будут включены в следующий блок. Очередность транзакций внутри mempool определяется давностью помещения их в mempool и количеством комиссии, которую готов заплатить отправитель транзакции за ее обработку.

2. Создание заголовка блока. На данном этапе формируется заголовок последующего блока. Он включает в себя релевантную информацию: временную метку (момент времени создания блока), хэш предыдущего блока и др.

3. Работа с nonce и поиск решения. Nonce (number used once) – случайное число, которое пытаются угадать (вычислить) майнеры. Цель состоит в том, чтобы при хэшировании nonce и остальной части заголовка получить результат, удовлетворяющий условиям поставленной задачи. Сам процесс подбора nonce и вычисления хэша лежит в основе алгоритма «доказательства работы». Он требует значительных вычислительных, а, соответственно и энергетических затрат.

4. Достижение консенсуса. После того, как определенный майнер решил задачу, он транслирует блок в сеть, чтобы его смогли проверить остальные участники сети. В случае, если другие майнеры подтверждают корректность вычисленного блока, то блок добавляется в сеть и вся цепочка итерации создания блока начинается заново.

Весь процесс создания нового блока с помощью механизма Proof-of-Work можно представить в виде следующий схемы (см. рисунок 1).

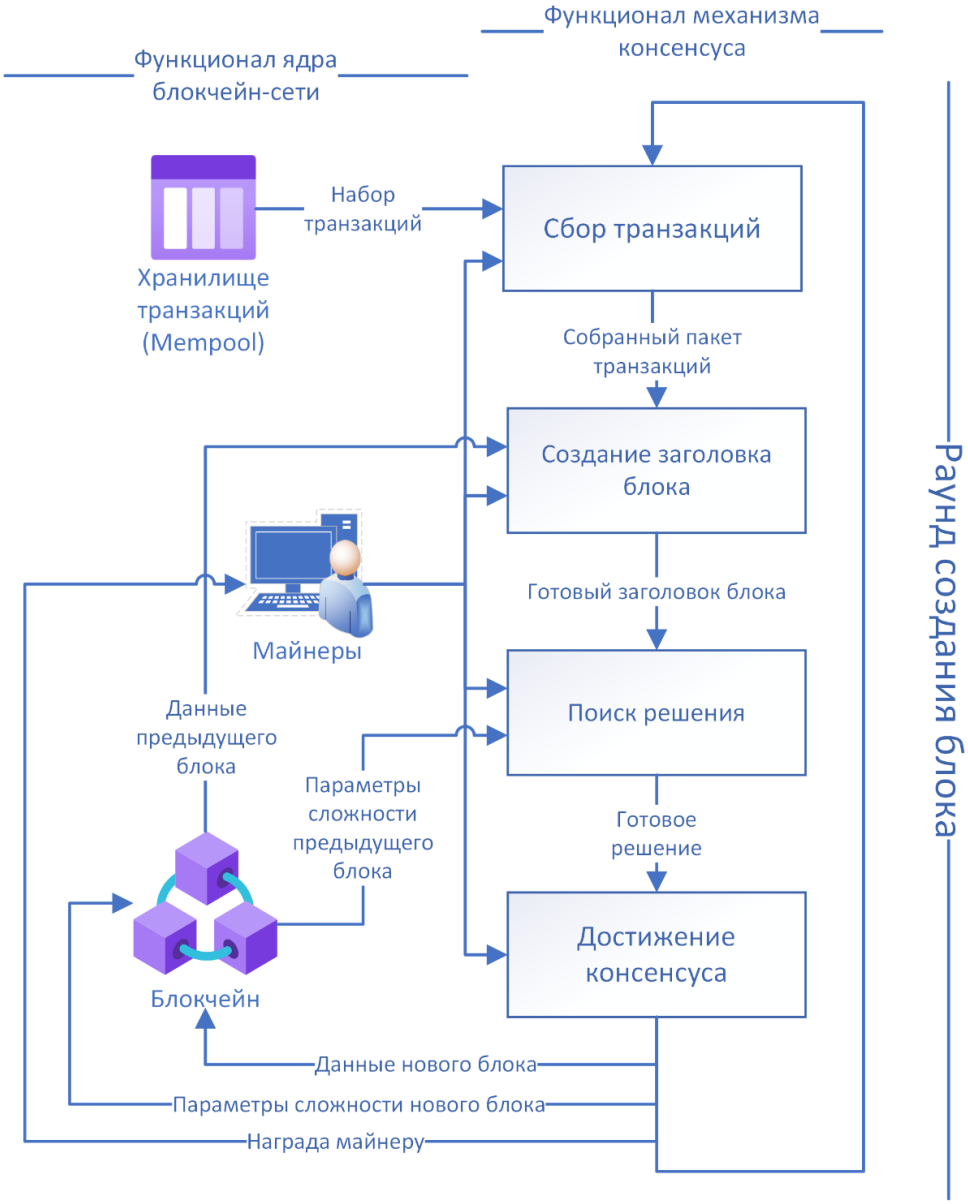

Рис. 1. Процесс создания нового блока в механизме Proof-of-Work
Fig. 1. The process of generating a new block in the Proof-of-Work mechanism

К преимуществам данного алгоритма можно отнести следующее:

- Безопасность. Алгоритм PoW способствует высокому уровню безопасности, так как для проведения атаки 51% (когда один участник или группа участников контролируют более 50% вычислительной мощности сети) злоумышленнику потребуется большое количество вычислительных мощностей, что является крайне энергозатратным.
- Простота валидации. После того, как определенный майнер решил задачу и записал в сеть новый блок, другие участники сети могут быстро проверить это, не производя повторных вычислений. Этот процесс способствует быстрой и надежной верификации состояния сети.

Недостатками алгоритма являются:

- Высокое энергопотребление. Вычислительные процессы, протекающие в ходе выполнения алгоритма, являются энергозатратными. Связанное с этим высокое энергопотребление вызывает обеспокоенность общества, так как влияет на окружающую среду [5].

- Централизация. Несмотря на теоретическую децентрализацию, на практике значительная часть вычислительных центров располагается в одних и тех же местах. В основном в странах с небольшой стоимостью электроэнергии.
- Масштабируемость. Механизм ограничивает количество транзакций, которые могут быть обработаны в каждом блоке из-за ограничений по вычислительной сложности. Это может приводить к задержкам и повышению стоимости комиссии за транзакции для конечных пользователей систем.
- Высокий порог входа. Высокие затраты на оборудование и электроэнергию являются проблемой для тех, кто хочет присоединиться к числу майнеров. Этот факт так же оказывает пагубное влияние на децентрализацию.

Несмотря на то, что механизм Proof-of-Work обеспечивает основу для безопасной и децентрализованной сети, он также несет ряд серьезных недостатков, особенно с точки зрения энергопотребления и масштабируемости. Это привело к появлению и изучению альтернативных механизмов консенсуса, таких как Proof-of-Stake (PoS), которые стремятся решить некоторые из этих проблем [6].

PROOF-OF-STAKE

Механизм Proof-of-Stake (PoS) также служит способом достижения консенсуса в блокчейн-сетях. Он создавался как альтернатива Proof-of-Work, решая некоторые из его проблем, одной из которых является потребность в больших вычислительных мощностях и связанное с этим высокое энергопотребление.

В отличие от PoW, где вероятность создания нового блока зависит от вычислительных мощностей майнера, в PoS эта вероятность определяется количеством заблокированных токенов на счету валидатора. Соответственно, чем больше токенов, относительно остальных участников сети, заблокировано на счету валидатора, тем больше вероятность того, что механизм предоставит ему возможность создать новый блок. Этот процесс исключает необходимость производить большое количество вычислительных операций, таких как добыча хэшей в Proof-of-Work [7].

По аналогии с примером «лотереи» в PoW, механизм Proof-of-Stake можно представить следующим образом: блокчейн-сеть, в которой развернут алгоритм консенсуса PoS является компанией, а участники сети – держатели акций этой компании. Некоторые участники проявляют интерес в управлении компанией и голосуют своим пакетом акций (валидаторы). Такие акционеры соревнуются в праве принимать решение, но как правило – интересы мажоритариев, то есть валидаторов с наибольшим количеством заблокированных токенов, являются более приоритетными для компании. Но в случае, если миноритарии объединят свои голоса и получат большинство – будут учтены именно их интересы.

Алгоритм создания нового блока в сети, где механизмом консенсуса является Proof-of-Stake, выглядит следующим образом:

1. **Выбор валидатора.** Алгоритм выбирает валидатора, который должен будет внести в сеть предложение о новом блоке. На случай наличия в сети валидатора, который имеет большое количество заблокированных токенов на своем счету (таких валидаторов называют китами) и может рассчитывать на повышенную вероятность выбора себя как предлагающего, в механизме предусмотрено несколько параметров, влияющих на вероятность выбора валидатора предлагающим. Одним из таких параметров является ProposerPriority. Каждый раз, когда валидатор избирается предлагающим, его приоритет предложения падает, тем самым уменьшая вероятность повторного выпадения ему шанса на создание нового блока в дальнейшем. В случае, если валидатор не был выбран предлагающим в данном раунде создания блока, его приоритет возрастает.
2. **Создание блока.** Выбранный валидатор собирает транзакции, находящиеся в хранилище, проверяет их на корректность и составляет из них новый блок. В блок также включается информация о предыдущем блоке, что создает последовательность всей цепочки блоков.

3. Подтверждение блока. Данный шаг алгоритма также называется механизмом голосования. Его смысл состоит в том, что все валидаторы сети должны проголосовать за блок, если они считают его корректным. При голосовании, валидаторы ставят на кон часть своих заблокированных токенов как залог.

4. Добавление блока в блокчейн. Когда количество голосов валидаторов за блок преодолевает значение 2/3 от общего количества токенов, заблокированных на счетах всех валидаторов, то блок добавляется в сеть и раунд по созданию нового блока начинается заново, а валидаторы получают обратно свой залог и награду за генерацию нового блока.

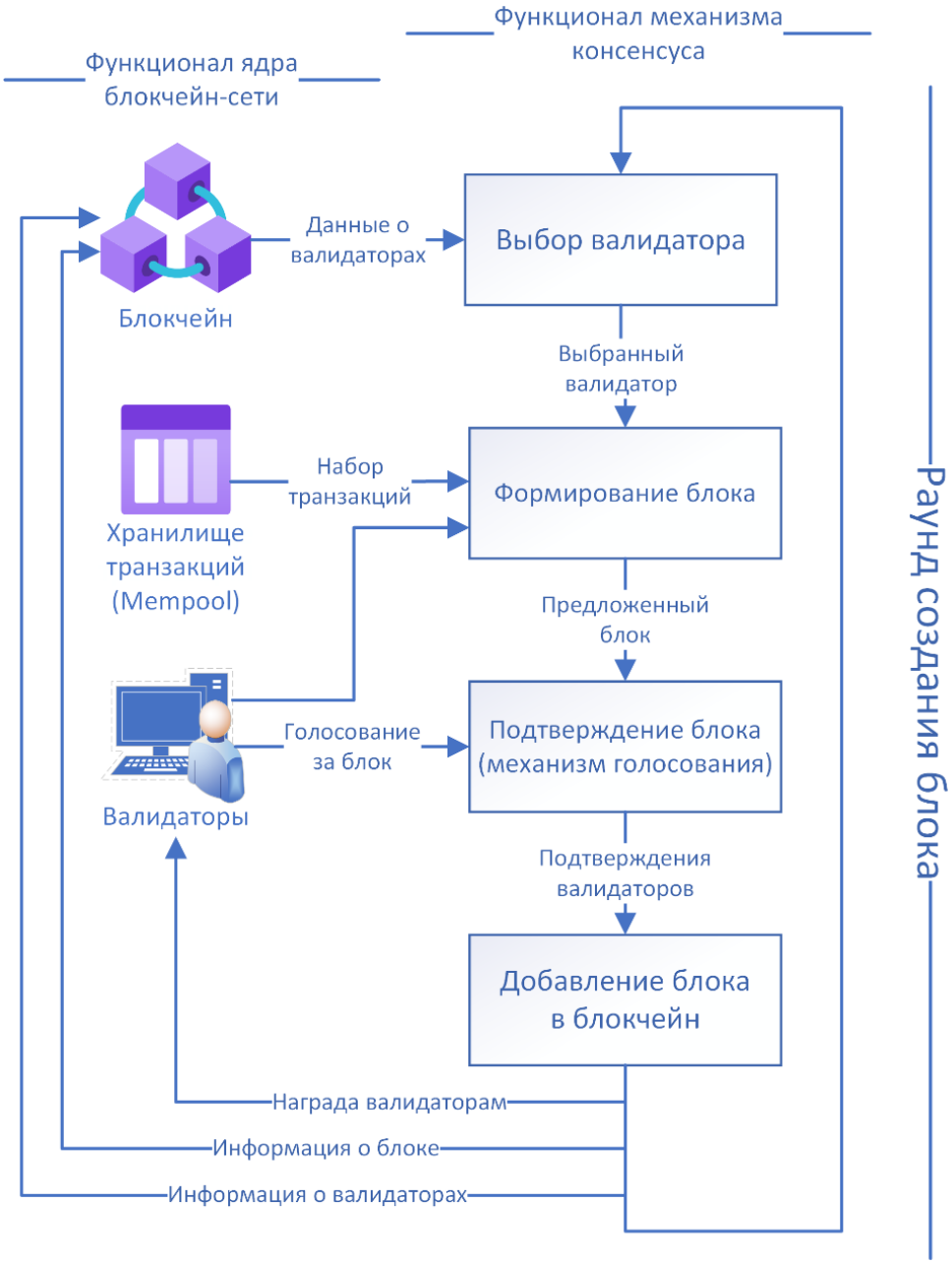

Рис. 2. Процесс создания нового блока в механизме Proof-of-Stake
Fig. 2. The process of generating a new block in the Proof-of-Stake mechanism

Преимуществами алгоритма PoS являются:

- Энергоэффективность. Как было сказано ранее, алгоритм не нуждается в больших вычислительных мощностях для выбора валидатора при генерации нового блока. Это значительно снижает энергопотребление сети, относительной сетей, использующих механизм PoW.

- Безопасность. Proof-of-Stake предлагает механизмы защиты от атак, используя систему залогов и наказаний за предложение некорректного блока.
- Децентрализация. Поскольку для участия в процессе создания и голосования за блоки не требуется больших вычислительных мощностей, то порог вхождения в число валидаторов значительно снижается относительно порога входа в число майнеров в механизме PoW. Это способствует развитию децентрализации сети.

К недостаткам механизма можно отнести:

- Первоначальное распределение. В сетях, использующих PoS большое значение будет иметь первоначальное распределение токенов, которое может способствовать централизации сети. Если большая часть токенов принадлежит небольшому количеству валидаторов, то это ставит под угрозу безопасность и децентрализацию сети.
- «Богатые становятся богаче». Как упоминалось ранее, в случае если у валидатора имеется слишком большой заблокированный баланс – «стейк», то вероятность выдвижения его как предлагающего новый блок будет завышена. Это ставит сеть под угрозу, так как такой валидатор сможет диктовать свои интересы и валидаторы с маленьким стейком не смогут перебить его голос. На практике, такая угроза нивелируется внесением в механизм дополнительных параметров, которые ограничивают приоритет таких валидаторов, но в теории угроза сохраняется.

Процессы, предлагаемые механизмом PoS, помогают обеспечить безопасность и децентрализацию сети без необходимости энергоемкого майнинга, как в PoW. Однако такие параметры сети, как выбор валидатора, механизмы голосования и расчет вознаграждений, могут варьироваться между разными реализациями PoS, каждая из которых стремиться оптимизировать механизм под собственные нужны каждой сети.

DELEGATED-PROOF-OF-STAKE

Механизм консенсуса Delegated-Proof-of-Stake (DPoS) представляет собой вариацию механизма PoS, единственным отличием от которой является возможность всех участников сети делегировать свои токены другим валидаторам, которые берут на себя ответственность за валидацию транзакций и создание блоков в сети. Это позволяет сети достигать большей производительности, снижая количество участников, непосредственно участвующих в процессе валидации.

Преимуществами DPoS являются:

- Масштабируемость. Для того, чтобы принимать участие в жизни сети, пользователю не обязательно разворачивать оборудование и настраивать собственного валидатора. В DPoS заинтересованный участник может просто делегировать имеющиеся у него токены другим валидаторам, что положительно сказывается на приток пользователей в сеть.
- Эффективность. Снижение числа участников, напрямую участвующих в процессе валидации, положительно сказывается на времени достижения консенсуса в сети, так как теперь меньшему количеству валидаторов необходимо прийти к согласию при генерации нового блока [8].

К недостаткам можно отнести:

- Централизация. Существует риск централизации при процессе голосования, так как крупные держатели токенов могут делегировать их одним и тем же валидаторам.

Delegated-Proof-of-Stake представляет собой усовершенствованный, но не лишенный недостатков механизм консенсуса, который на данный момент приобрел наибольшее распространение в сфере различных блокчейн-проектов. В будущем, успех применения данного алгоритма будет обусловлен решением задач по его адаптации и обеспечению справедливого и прозрачного распределения прав голоса.

PROOF-OF-AUTHORITY

Идея алгоритма Proof-of-Authority (PoA) заключается в том, что право создавать новые блоки и подтверждать транзакции в сети предоставляется небольшому ограниченному количеству доверенных узлов (валидаторов). Алгоритм основывается не на стейке, как PoS и не на вычислительных мощностях, как PoW, а на идентификации и репутации (авторитете) валидаторов. PoA разработан для обеспечения высокой производительности и масштабируемости в частных блокчейн-сетях, где необходимость в децентрализации не играет главной роли [9].

В плане работы, алгоритм PoA похож на алгоритм PoS, только вместо заблокированных токенов применяется авторитет валидатора, который также не может передаваться от одного пользователя к другому. Начисление или списание уровня авторитета валидатора может проводиться посредством предложений в сети, где какой-то пользователь может выдвинуть предложение, а остальные участники проголосовать. Или же уровень авторитета может модерироваться централизованно администратором сети, но такой способ противоречит фундаментальным задачам блокчейн-технологии, так как отрицательно сказывается на децентрализации.

К преимуществам механизма Proof-of-Authority можно отнести:

- Высокая производительность. Так как количество валидаторов ограничено, сети требуется меньше времени для достижения консенсуса и валидации транзакций.
- Масштабируемость. Сети, использующие механизм PoA, могут масштабироваться быстрее, чем сети, использующие PoW и PoS, благодаря упрощенному процессу валидации.
- Энергоэффективность. PoA, также как и PoS не нуждается в больших вычислительных мощностях для генерации блоков, что положительно влияет на энергопотребление сети.

К недостаткам относятся:

- Централизация. Основная проблема механизма Proof-of-Authority заключается в том, что она вносит элемент централизации в блокчейн-сеть, так как все процессы зависят от ограниченного числа валидаторов.
- Риски безопасности. Если валидаторы подвергнутся атаке и станут недобросовестными, то это поставит всю безопасность сети под риск.

Механизм Proof-of-Authority представляет собой эффективное решение для частных блокчейн-сетей, где важна высокая производительность и все участники сети известны друг другу. Важно, чтобы сети, использующие PoA, разрабатывали и применяли дополнительные механизмы для обеспечения прозрачности и безопасности.

PROOF-OF-CAPACITY

Алгоритм Proof-of-Capacity (PoC), он же Proof-of-Space, представляет собой механизм консенсуса, в котором право на создание нового блока в сети предоставляется участникам на основании количества дискового пространства. В отличие от PoW, где важны вычислительные мощности и PoS, где важно количество заблокированных на счету токенов, в PoC главную роль играет размер выделенного под нужды сети хранилища.

Участники сети, в которой реализован данный механизм консенсуса, заранее генерируют и хранят на своих дисках большие объемы данных, называемые «плотами». Эти плоты содержат возможные решения задач, которые сеть может потребовать в любой момент времени. Право на генерацию нового блока будет предоставлено тому майнеру, который быстрее всех предложит сети решение поставленной задачи.

Преимуществами данного алгоритма являются:

- Энергоэффективность. Относительно PoW, алгоритм PoC не требует высоких энергетических затрат, так как для поддержания сети от майнеров требуется высокая скорость чтения данных с накопителей, а не большие вычислительные мощности.

- Доступность. Так как для поддержания сети используется только дисковое пространство, то порог входа для майнеров значительно ниже, чем в Proof-of-Work.

Недостатками являются:

- Износ оборудования. Постоянный процесс чтения данных с дисков истощает ресурс износа оборудования.
- Безопасность. Поскольку PoC основан на возможности представления решения задачи из предварительно сгенерированного набора данных, он может быть менее безопасным, относительно других механизмов.

Алгоритм механизма Proof-of-Capacity представляет свежий подход к решению задачи по достижению консенсуса в блокчейн-сетях, поскольку делает акцент на энергоэффективности и доступности. Однако, как и в случае с остальными механизмами консенсуса, важно учитывать специфику блокчейн-системы, в которой будет использоваться механизм.

КАЧЕСТВЕННЫЙ И КОЛИЧЕСТВЕННЫЙ СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕХАНИЗМОВ КОНСЕНСУСА

Ниже представлена таблица с ключевыми качественными параметрами обозримых алгоритмов консенсуса, которые в первую очередь должны быть учтены во время решения задачи по выбору механизма для блокчейн-сети определенной специфики.

Таблица 1

Сравнение механизмов консенсуса

Table 1

Comparison of consensus mechanisms

Механизм	Энергопотребление	Уровень децентрализации	Масштабируемость	Требования к участникам	Безопасность
Proof-of-Work (PoW)	Высокое	Средний	Низкая	Высокие вычислительные мощности	Высокая
Proof-of-Stake (PoS)	Низкое	Высокий	Высокая	Владение токенами	Высокая
Delegated-Proof-of-Stake (DPoS)	Низкое	Средний	Высокая	Владение токенами	Средняя
Proof-of-Authority (PoA)	Низкое	Низкий	Высокая	Идентификация и доверие	Высокая
Proof-of-Capacity (PoC)	Низкое	Средний	Средняя	Дисковое пространство	Средняя

Для сравнения технических параметров, отражающих количественные метрики механизмов консенсуса в контексте применения их в существующих блокчейн сетях, можно выделить следующие показатели:

- Средняя скорость транзакции: скорость транзакции, в среднем, за последние 10 тысяч блоков в сети, от момента подписания отправителем до публикации блока, включающего эту транзакцию;
- Максимально возможное количество обработанных транзакций в секунду (заявленное) – TPS (заявленное): количество транзакций, которые сеть может обработать за один блок,

пересчитанное в секунды. Данный показатель заявляется разработчиками сети и может быть вычислен по формуле:

$$TPS = \frac{n}{t},$$

где n – максимально допустимое количество транзакций, которые могут быть обработаны в одном блоке, а t – среднее время создания блока (в секундах);

- Максимально возможное количество обработанных транзакций в секунду (реальное) – TPS (реальное): фактическое количество транзакций, которые были обработаны за один блок, пересчитанное в секунды. Информация взята в среднем за последние 10 тысяч блоков в сети;
- Среднее время создания блока: среднее время, за которое в сети появляется новый блок (в среднем, за последние 10 тысяч блоков в сети).

Таблица 2

Сравнение механизмов консенсуса в применении к блокчейн-сетям

Table 2

Comparison of consensus mechanisms applied to blockchain networks

Механизм консенсуса и сеть реализации	Средняя скорость транзакции (в секундах)	TPS (заявленное)	TPS (реальное)	Среднее время создания блока (в секундах)
PoW (Bitcoin)	600	7	3-5	600
PoS (Ethereum 2.0)	13	100,000	15-45	12
DPoS (Cosmos Hub)	7	10,000	1000-2500	7
PoA (VeChain)	10	10,000	50-100	11
PoC (Chia)	19	Не определено	10-20	19

По результатам проведенного сравнения, необходимо определить, какой механизм консенсуса сможет обеспечить наибольшую эффективность в конкретной сфере применения:

- Proof-of-Work. Применение в системах, где приоритет отдается безопасности и децентрализации над эффективностью использования ресурсов, масштабированию и скоростью обработки транзакций. Подходит для использования в сфере цифровых активов.
- Proof-of-Stake. Механизм подойдет для проектов, которые стремятся к масштабированию, обеспечивая при этом высокий уровень безопасности. Вариации PoS помогут компаниям, желающим перенести на блокчейн системы учета ресурсов или логистики, так как на практике, сети, использующие PoS, обладают неплохими показателями по скорости и объему транзакций.
- Delegated-Proof-of-Stake. Алгоритм подойдет для платформ, где необходима высокая скорость транзакций и масштабируемость, например, для таких, как децентрализованные социальные сети или децентрализованные приложения. Эти процессы поможет обеспечить большой, по сравнению с другими участниками сравнения, уровень скорости обработки транзакций.
- Proof-of-Authority. Наиболее эффективен в закрытых или корпоративных блокчейн-сетях, где участники заранее известны. Это делает его идеальным для приложений, требующих быстрой верификации транзакций и высокого уровня безопасности без значительного энергопотребления, таких как системы документооборота, внутреннего учета, цепочки поставок и службы идентификации. В сферах применения является аналогом PoS, но с учетом на то, что все участники сети являются идентифицированными личностями.

- Proof-of-Capacity. Подходит для систем, где важна децентрализация данных. Например, децентрализованные платформы хранения данных. Алгоритм сможет обеспечить высокий уровень безопасности данных и их децентрализованное хранение.

ЗАКЛЮЧЕНИЕ

В ходе обзора были представлены и проанализированы самые популярные механизмы консенсуса в блокчейн сетях: приведено описание алгоритмов, примеров работы, преимуществ и недостатков. Представлено качественное и количественное сравнение параметров сети и акцентированы рекомендации по употреблению алгоритмов в сетях различной специфики.

Назначение алгоритмов консенсуса является фундаментальным для поддержания блокчейн-сетей и их назначения – децентрализации и безопасности данных. Каждый механизм имеет свои собственные особенности, преимущества и недостатки.

Выбор механизма консенсуса для блокчейн-проекта требует тщательного анализа его целей, требований к энергоэффективности, безопасности, масштабированию и децентрализации. В зависимости от требований, каждый из рассмотренных алгоритмов консенсуса сможет предложить оптимальное решение для поставленных задач [10].

В будущем, по мере развития технологии блокчейн стоит ожидать появление новых механизмов консенсуса и усовершенствования текущих, что позволит еще более эффективно реализовывать потенциал блокчейн-систем в самых разных областях.

Список литературы

1. Развитие технологии блокчейн в России в 2024 году. – Crypto.ru. – URL: https://crypto.ru/blokchain-v-rossii/#kto-uzhe-primenyaet-tehnologiyu-blokcheyn (дата обращения: 10.01.2025).
2. Нестеренко В.Р., Маслова М.А. Использование технологии Blockchain для обеспечения безопасности в распределенном интернете вещей // Научный результат. Информационные технологии. – 2021. – Т. 6. – № 2. – С. 3-8.
3. Стрелец А.И., Храпов А.С., Иванников В.С., Атавина А.В. Исследование современных алгоритмов Proof-of-Work // E-Scio. 2019. – №6.
4. Алгоритм консенсуса Proof-of-Work (PoW), Proof-of-Stake (PoS). – TADVISER. – URL: https://www.tadviser.ru/index.php/Статья:Алгоритм_консенсуса_Proof-of-Work_(PoW)_и_Proof-of-Stake_(PoS) (дата обращения: 15.01.2025).
5. Семёнова Ю.Е. Энергоэффективные криптовалюты решение проблемы воздействия на окружающую среду // Инновационная экономика: перспективы развития и совершенствования. – 2023. – №7(73). – С. 141-146.
6. Абдулжалилов А.З. Методы и стратегии масштабируемости блокчейн-технологий: анализ, сравнение и перспективы // Вестник науки. – 2023. – №11(68). – Т 4. – С. 625-634
7. Попадюк А.Ю., Коровяковский Е.К., Титова Т.С. Экологические аспекты технологии распределенного реестра на примере алгоритма консенсуса Proof-of-Work // Известия Петербургского университета путей сообщения. – 2020. – Т. 17. – №1. – С. 136-143.
8. Астраханцев Роман Геннадьевич, Лось Алексей Борисович, Мухамадиева Регина Шамилевна. Анализ современных тенденций развития технологии «блокчейн» и цифровых валют // Вопросы кибербезопасности. – 2019. – №5(33). – С. 57-62.
9. Ивкин А.В., Мирошниченко Е.Л., Волкова А.А. Концепция инфраструктуры системы электронного документооборота на основе технологии «Блокчейн» // Военная мысль. – 2023. – №3. – С. 90-99.
10. 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.

References

1. Development of blockchain technology in Russia in 2024. – Crypto.ru. – URL: https://crypto.ru/blokchain-v-rossii/#kto-uzhe-primenyaet-tehnologiyu-blokcheyn (Accessed: January 10, 2025).

2. Nesterienko V.R., Maslova M.A. The Use of Blockchain Technology to Ensure Security in the Distributed Internet of Things // Reserch Result. Information Technologies. – 2021. – T. 6. – No 2. – P. 3-8.

3. Strelets A.I., Khrapov A.S., Ivannikov V.S., Atavina A.V. Study of Modern Proof-of-Work Algorithms // E-Scio. – 2019. – No. 6.

4. Consensus Algorithm: Proof-of-Work (PoW) and Proof-of-Stake (PoS). – TADVISER. – URL: https://www.tadviser.ru/index.php/Статья:Алгоритм_консенсуса_Proof-of-Work_(PoW)_и_Proof-of-Stake_(PoS) (Accessed: January 15, 2025).

5. Semyonova Yu.E. Energy-Efficient Cryptocurrencies: A Solution to the Problem of Environmental Impact // Innovative Economy: Prospects for Development and Improvement. – 2023. – No. 7(73). – P. 141-146.

6. Abdulzhalilov A.Z. Methods and Strategies for the Scalability of Blockchain Technologies: Analysis, Comparison, and Prospects // Bulletin of Science. – 2023. – No. 11(68). – T 4. – P. 625-634.

7. Popadyuk A.Yu., Korovyakovsky E.K., Titova T.S. Environmental Aspects of Distributed Ledger Technology: A Case Study of the Proof-of-Work Consensus Algorithm // Proceedings of the St. Petersburg State University of Railway Communications. – 2020. – T. 17. – No 1. – P. 136-143.

8. Astrakhantsev R.G., Los A.B., Mukhamadieva R.Sh. Analysis of Modern Trends in the Development of Blockchain Technology and Digital Currencies // Cybersecurity Issues. – 2019. – No. 5(33). – P. 57-62.

9. Ivkin A.V., Miroshnichenko E.L., Volkova A.A. The Concept of Infrastructure for an Electronic Document Management System Based on Blockchain Technology // Military Thought. – 2023. – No. 3. – P. 90-99.

10.Nosirov Z.A., Fomichev V.M. Analysis of Blockchain Technology: Architectural Foundations, Usage Examples, Development Prospects, Issues, and Drawbacks // Systems of Management, Communications, and Security. 2021. – No. 2. – P. 37-75.

Булгаков Владислав Дмитриевич, соискатель по специальности 2.3.1. Системный анализ, управление и обработка информации, статистика, Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия

Гвоздевский Игорь Николаевич, кандидат технических наук, доцент, начальник управления информатизации, Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород, Россия

Bulgakov Vladislav Dmitrievich, Applicant in the Specialty 2.3.1. System analysis, management and information processing, statistics, Belgorod State Technological University named after V.G. Shukhov, Belgorod, Russia

Gvozdevsky Igor Nikolaevich, Candidate of Technical Sciences, Associate Professor, Head of the Informatization Department of the Belgorod State Technological University named after V.G. Shukhov, Belgorod, Russia