

Программные системы и вычислительные методы

Правильная ссылка на статью:

Булгаков В.Д., Гвоздевский И.Н. Модель и алгоритм консенсуса Proof of Performance // Программные системы и вычислительные методы. 2024. № 4. DOI: 10.7256/2454-0714.2024.4.71119 EDN: NAGMFW URL: https://nbpublish.com/library_read_article.php?id=71119

Модель и алгоритм консенсуса Proof of Performance

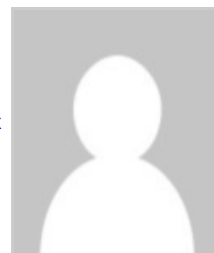
Булгаков Владислав Дмитриевич

ORCID: 0009-0006-2056-6169

аспирант; кафедра Программное обеспечение вычислительной техники и автоматизированных систем; Белгородский государственный технологический университет им. В.Г. Шухова

308012, Россия, Белгородская область, г. Белгород, ул. Костюкова, 46

✉ bulgakowlad@yandex.ru



Гвоздевский Игорь Николаевич

ORCID: 0000-0002-3235-3869

кандидат технических наук

доцент; кафедра Программное обеспечение вычислительной техники и автоматизированных систем; Белгородский государственный технологический университет им. В.Г. Шухова

308012, Россия, Белгородская область, г. Белгород, ул. Костюкова, 36, оф. 421

✉ Gvozdevskiy.in@bstu.ru



[Статья из рубрики "Models and methods of information security management"](#)

DOI:

10.7256/2454-0714.2024.4.71119

EDN:

NAGMFW

Дата направления статьи в редакцию:

25-06-2024

Дата публикации:

30-11-2024

Аннотация: В статье исследуется принцип работы модели Proof of Performance (PoP), основанной на алгоритме консенсуса, поддерживающем функции горизонтального шардинга. Модель PoP вносит изменения в традиционную структуру блоков,

используемую в алгоритмах Proof of Stake и сетях на базе ядра Tendermint. Горизонтальный шардинг позволяет распределять транзакции между несколькими узлами (шардами), что значительно увеличивает пропускную способность сети. Основная цель исследования — изучение способов повышения эффективности и масштабируемости блокчейн-сетей через динамическое распределение транзакций и адаптивное управление узлами. Важным аспектом является определение параметров и изменяемых характеристик узлов, таких как производительность и надежность для равномерного и справедливого распределения нагрузки внутри сети. Это обеспечивает адаптацию системы к изменяющимся условиям нагрузки. В работе используются аналитические и формальные методы для описания структуры блока, механизма распределения транзакций и системы наказаний и поощрений для шардов. Исследование представляет собой инновационный подход к управлению блокчейн-сетями, акцентируя внимание на производительности узлов. Модель PoP с горизонтальным шардингом обеспечивает более высокую пропускную способность и масштабируемость сети по сравнению с традиционными алгоритмами консенсуса. Предложена система динамического распределения нагрузки и адаптивного изменения весов узлов на основе их производительности, что способствует повышению эффективности и надежности сети. В результате исследования доказано, что модель Proof of Performance значительно увеличивает скорость обработки транзакций и общую производительность блокчейн-сети. Примеры применения подтверждают эффективность модели в различных типах сетей, таких как DeFi-платформы, системы управления цепочками поставок и IoT-сети. Модель PoP стимулирует узлы к поддержанию высокой производительности, обеспечивая справедливое распределение нагрузки и повышая общую устойчивость сети.

Ключевые слова:

Модель консенсуса, Алгоритм консенсуса, Шард, Блок, Доказательство производительности, Доказательство ставки, Горизонтальный шардинг, Производительность, Распределение нагрузки, Блокчейн

Введение

Актуальность проблемы повышения производительности и масштабируемости блокчейн-сетей обусловлена растущими требованиями к обработке транзакций в высоконагруженных системах, таких как финансовые технологии, системы Интернета вещей (IoT) и децентрализованные приложения (dApps). Существующие алгоритмы консенсуса, включая Proof of Stake (PoS) на базе ядра Tendermint демонстрируют ограниченную пропускную способность, обусловленную высокой нагрузкой и ограниченными ресурсами производительности узлов-валидаторов сети. Эти ограничения создают узкие места в функционировании сетей и снижают их устойчивость к изменениям нагрузки^[1].

Цель данного исследования — разработка и анализ модели Proof of Performance (PoP), которая направлена на повышение эффективности и масштабируемости блокчейн-сетей посредством внедрения технологии горизонтального шардинга. В основе PoP лежит идея равновесного распределения транзакций между узлами, что позволяет снизить нагрузку на отдельные узлы-валидаторы и повысить общую производительность сети.

Для достижения поставленной цели решаются следующие задачи:

- Разработка модифицированной структуры блока, обеспечивающей поддержку шардинга.
- Построение математической модели распределения нагрузки и расчёта производительности узлов.
- Экспериментальная проверка корректности работы модели PoP в развернутой тестовой сети.

Научная новизна работы заключается в предложении и описании новейшего алгоритма Proof of Performance, сочетающего адаптивное распределение нагрузки и учет производительности узлов, что позволяет существенно увеличить пропускную способность сети и её устойчивость к изменениям нагрузки.

Представленная работа закладывает основу для дальнейших исследований, направленных на интеграцию описанного алгоритма консенсуса в существующие блокчейн-системы и развитие технологий децентрализованного управления нагрузкой.

Описание модели Proof of Performance

В алгоритме консенсуса Proof of Stake узел, предлагающий блок (Block proposer) получает из пула транзакций (Transaction pool/mempool) определенное количество транзакций для обработки, чтобы в последующем опубликовать их в блоке, а, соответственно, в сети. Такой подход ограничивает количество транзакций, которые могут быть обработаны сетью за определенный момент времени, а также повышает нагрузку на узел, который является предлагающим в данной итерации создания блока. Более того, подход PoS к определению участника сети, который получит возможность добавить блок в сеть определяется количеством монет участника, что само по себе пагубно воздействует на философию децентрализации блокчейн-сети [\[2\]](#).

Внедрение технологии горизонтального шардинга позволит снять нагрузку с узла, предлагающего блок и распределить ее равномерно на все узлы, являющимися шардами, то есть на узлы, предоставляющие свои вычислительные мощности для процесса обработки транзакций в сети [\[3\]](#).

Далее представлена схема, которая описывает процесс обработки транзакций в алгоритмах консенсуса Proof of Stake (Рисунок 1) и Proof of Performance (Рисунок 2).

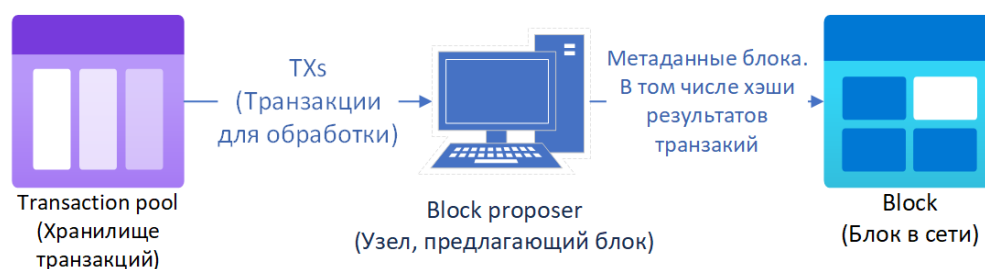


Рис.1 – Процесс обработки транзакций в алгоритме Proof of Stake

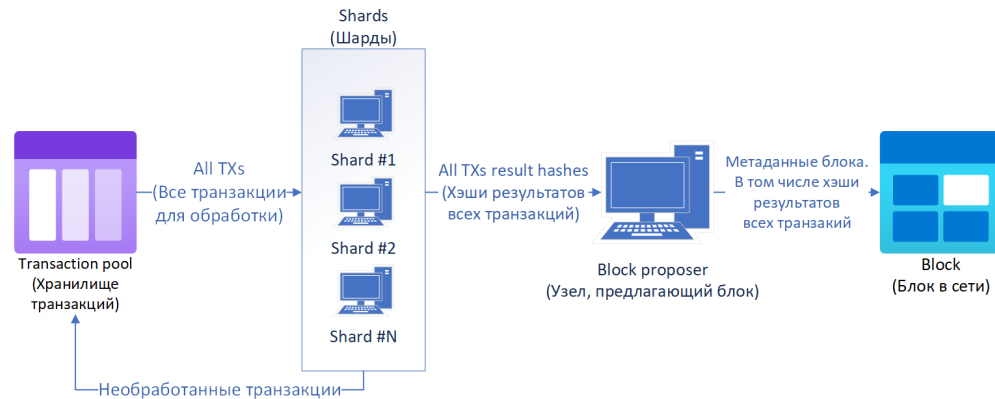


Рис.2 – Процесс обработки транзакций в алгоритме Proof of Performance

Основными преимуществами данного подхода являются:

- Единовременная обработка всех транзакций, находящихся в хранилище. В случае Proof of Stake, алгоритм не может прислать на обработку узлу количество транзакций, превышающее определенный порог, так как это пагубно скажется на производительности узла, предлагающего блок и может вызвать сбой в сети, в случае выхода этого узла из строя. В модели Proof of Performance алгоритм «достаёт» из хранилища все транзакции и распределяет их равномерно между шардами [\[4\]](#).
- Распределение нагрузки. Отсутствие диверсификации в процессе обработки транзакций является собой большую проблему в сфере блокчейна [\[5\]](#). Выход из строя узла, на котором лежит задача создания нового блока увеличивает время его создания, а в случае, если все узлы сети не справились с этой задачей, вызывает блокировку сети. Введение понятия шардов, описание их алгоритма работы и внедрение их в существующую систему позволит узлу, занятому процессом создания блоков не тратить свои вычислительные мощности на обработку транзакций. Ему предстоит лишь получить эти данные от шардов, проверить их и опубликовать в блоке.

Структура блока в модели Proof of Performance

Так как процесс учета и контроля шардинга представляет собой новую задачу, для децентрализованного хранения результатов ее решения необходимо модифицировать имеющуюся структуру блока. На данный момент, в сетях Proof of Stake преобладает следующая структура, состоящая из 15-ти полей:

- Block #N: Номер блока. Это уникальный идентификатор блока в блокчейне, указывающий на его позицию в цепочке.
- Version: Версия программного обеспечения или протокола, используемого для создания этого блока.
- ChainID: Идентификатор сети, к которой относится данный блок.
- Height: Высота блока. Это порядковый номер блока в блокчейне, начиная с генезис-блока (нулевого блока).
- Time: Временная метка, указывающая время создания блока.
- LastBlockID: Идентификатор предыдущего блока в цепочке. Это значение используется для связывания блоков в единую цепь.
- LastCommitHash: Хэш последнего подтвержденного блока. Это значение используется

для проверки корректности предыдущего блока.

- **DataHash:** Хэш данных блока. Это значение представляет собой криптографический хэш всех транзакций, включенных в блок.
- **ValidatorsHash:** Хэш валидаторов. Это значение представляет собой криптографический хэш списка валидаторов, участвующих в валидации блока.
- **NextValidatorsHash:** Хэш следующих валидаторов. Это значение представляет собой криптографический хэш списка валидаторов, которые будут участвовать в валидации следующего блока.
- **ConsensusHash:** Хэш консенсуса. Это значение представляет собой криптографический хэш параметров консенсусного алгоритма, используемого для достижения соглашения между валидаторами.
- **AppHash:** Хэш приложения. Это значение представляет собой криптографический хэш состояния приложения после выполнения всех транзакций в блоке.
- **LastResultsHash:** Хэш результатов последнего выполнения. Это значение представляет собой криптографический хэш результатов выполнения транзакций в предыдущем блоке.
- **EvidenceHash:** Хэш доказательств. Это значение представляет собой криптографический хэш всех доказательств, включенных в блок, которые могут быть использованы для выявления злонамеренных валидаторов.
- **ProposerAddress:** Адрес предлагающего блока. Это уникальный идентификатор участника сети, который предложил данный блок для добавления в цепочку.

Данная структура в виде таблицы, составляющей блок, продемонстрирована на рисунке 3.

Block #N
Version
ChainID
Heigh
Time
LastBlockID
LastCommitHash
DataHash
ValidatorsHash
NextValidatorsHash
ConsensusHash
AppHash
LastResultsHash
EvidenceHash
ProposerAddress

Рис.3 – Структура блока в алгоритме Proof of Stake

Так как данная структура нуждается в доработке и добавлении параметров для учета процесса шардинга, то структура блока в модели Proof of Performance будет включать в себя следующие дополнительные параметры:

- ShardsHash: Хэш списка шардов. Криптографический хэш, представляющий список всех узлов, которые являются шардами в сети.
- CurrentShardsHash: Хэш текущих шардов. Криптографический хэш, представляющий список шардов, участвовавших в обработке транзакций в данном блоке.
- NextShardsHash: Хэш следующих шардов. Криптографический хэш состояния шардов, которые будут участвовать в процессе обработки транзакций в следующем блоке.
- ShardsEvidenceHash: Хэш доказательств шардов. Криптографический хэш всех доказательств, включенных в блок, которые могут быть использованы для выявления злонамеренных шардов.
- DataAccordanceShardsHash: Хэш соответствия данных шардов. Криптографический хэш, обеспечивающий согласованность данных между разными шардами. Данное поле содержит хэш соответствия между шардами и обработанными ими транзакциями.

Согласно обновленной структуре, модель блока в алгоритме Proof of Performance, реализующим процесс горизонтального шардинга, будет выглядеть следующим образом:

Block #N
Version
ChainID
Heigh
Time
LastBlockID
LastCommitHash
DataHash
ShardsHash
CurrentShardsHash
NextShardsHash
ShardsEvidenceHash
DataAccordanceShardsHash
ValidatorsHash
NextValidatorsHash
ConsensusHash
AppHash
LastResultsHash
EvidenceHash
ProposerAddress

Рис.4 – Структура блока в алгоритме Proof of Performance

Эти нововведения позволяют сети учитывать вклад каждого шарда в обработку транзакций, обеспечивать безопасность данных и распределять нагрузку между узлами пропорционально их производительности.

Необходимость таких изменений обусловлена следующими факторами:

1. Проблемы текущей структуры блоков:

- Отсутствие поддержки горизонтального шардинга.
- Концентрация нагрузки на узле-валидаторе.
- Повышенная вероятность сбоя из-за перегрузки одного узла.

2. Преимущества модифицированной структуры:

- Равномерное распределение транзакций между узлами.
- Возможность адаптации к изменениям нагрузки.
- Повышение устойчивости сети за счёт децентрализации обработки данных.

Таким образом, предложенные изменения в структуре блока обеспечивают основу для эффективной реализации модели PoP и её дальнейшей интеграции в блокчейн-системы.

Распределение весов

Для того, чтобы обеспечить справедливую оценку и распределение нагрузки между шардами, алгоритм Proof of Performance берет на себя роль арбитра и обеспечивает процесс управления процедурами назначения, поощрения и наказания шардов в зависимости от их производительности.

В основе алгоритма Proof of Performance лежит система оценки производительности (Performance) каждого шарда.

Для определения производительности используются следующие параметры, влияющие на конечный результат вычислений веса шарда:

- Performance (P): Производительность шарда в обработке транзакций. Оценивается на основе успешности выполнения транзакций в текущем и предыдущих блоках.
- Weight (W): Вес шарда, определяющий уровень его конкурентной способности обрабатывать транзакции в следующем блоке.
- Penalty (Penalty): Штраф за несвоевременную или неуспешную обработку транзакций
- Reward (Reward): Поощрение за успешную обработку транзакций.

Оценка производительности P_i происходит по следующей формуле:

$$P_i = T_i / T_j$$

где T_i – общее количество транзакций, назначенных шарду, T_j – количество транзакций, успешно обработанных шардом;

Определение веса шарда является одной из главных задач алгоритма, так как неверно определенный вес может пагубно отразиться на производительности сети (например, если шард, обладающий небольшими вычислительными мощностями получит большой вес). Для определения веса (WS_{next}) используется следующая формула:

$$WS_{next} = WS_{current} * 1 + Reward_S - Penalty_S$$

где $WS_{current}$ – вес шарда в данном блоке, $Reward_S$ – коэффициент поощрения для шарда, а $Penalty_S$ – коэффициент штрафа (наказания) для шарда.

Коэффициенты поощрения и штрафа определяются следующим образом:

$$Reward_S = k_r * P_S$$

$$Penalty_S = k_p * (1 - P_S)$$

где k_r и k_p – константы, задающие влияние поощрений и штрафов на вес шарда.

После подсчета весов для следующей итерации, их необходимо нормализовать, чтобы сумма весов всех шардов не превышала 1, то есть 100%. Для этого используются следующие формулы:

$$W_{total} = \sum W^{next}$$

$$W_{snorm} = W_s / O$$

где O – сумма всех ненормализованных весов шардов, а W_{snorm} – нормализованный вес для шарда s .

Для распределения транзакций между шардами в следующем блоке используется взвешенный случайный выбор на основе обновленных нормализованных весов W_{snorm} . Общее количество транзакций делится между шардами пропорционально их весам на основе следующей формулы:

$$T_s^{next} = T * W_s^{norm}$$

где T_s^{next} – количество транзакций, назначаемых шарду s в следующем блоке.

Работоспособность алгоритма

Алгоритм работы Proof of Performance будет состоять из следующих шагов:

1. Инициализация. На этом шаге устанавливаются начальные веса всех шардов. Данный шаг выполняется только на первой итерации работы алгоритма, то есть при создании генезис (нулевого) блока;
2. Сбор транзакций. Все входящие от пользователей сети транзакции собираются в общий пул (хранилище);
3. Распределение транзакций. Транзакции распределяются между шардами на основе текущих (или первоначальных) весов;
4. Обработка транзакций. Каждый шард обрабатывает назначенные ему транзакции;
5. Оценка производительности. Производительность каждого шарда оценивается по формуле P_i [6];
6. Обновление весов. Веса шардов обновляются с учетом поощрений и штрафов.

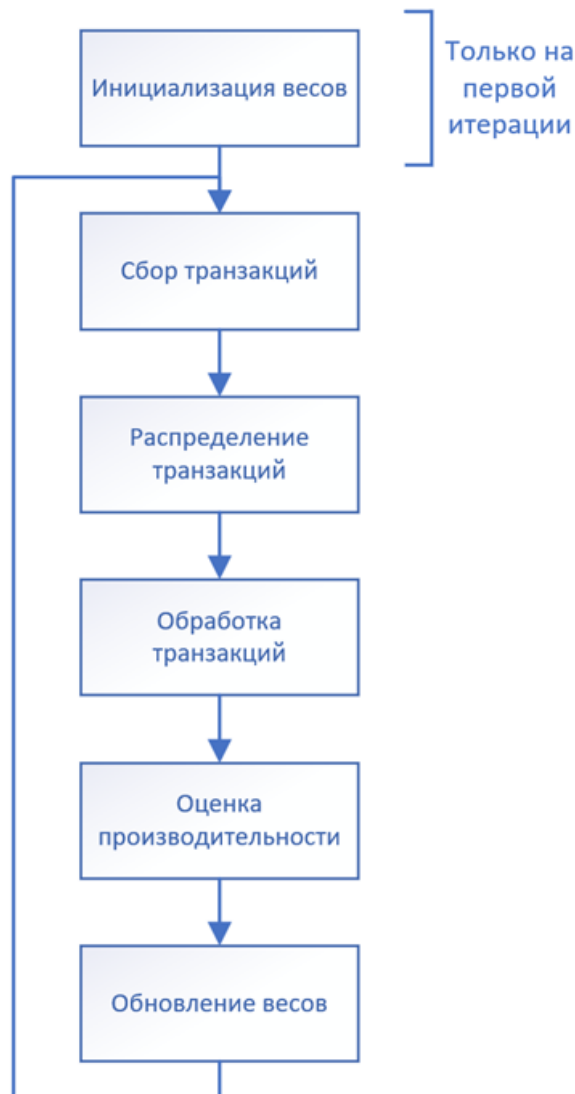


Рис.5 – Алгоритм обработки транзакций в модели Proof of Performance

Доказательство корректности работы алгоритма

Допустим, в сети имеются три шарда 3 с текущими весами $Ws1=0.3, Ws2=0.4, Ws3=0.3$. Допустим, что значения коэффициентов поощрения и наказания $kr=0.1$ и $kp=0.2$.

После создания блока заметим, что:

- 1 обработал 90% назначенных ему транзакций (P);
- 2 обработал 70% (P);
- 3 обработал 80% (P).

Тогда:

$$Rewards1=0.1*0.9=0.09;$$

$$Penaltys1=0.2*(1-0.9)=0.02;$$

$$Ws1next=0.3*1+0.09-0.02=0.3*1.07=0.321;$$

Аналогично для 3 :

$$Rewards2=0.1*0.7=0.07$$
$$Penaltys2=0.2*(1-0.7)=0.06$$
$$Ws2next=0.4*1+0.07-0.06=0.4*1.01=0.404$$

$$Rewards3=0.1*0.8=0.08$$
$$Penaltys3=0.2*(1-0.8)=0.04$$
$$Ws3next=0.3*1+0.08-0.04=0.3*1.04=0.312$$

Нормализация весов:

$$Ws1norm=0.3211.037=0.31$$
$$Ws2norm=0.4041.037=0.39$$
$$Ws3norm=0.3121.037=0.30$$

Тогда новая сумма весов всех шардов: = 1.037, а
новый вес каждого шарда:

$$= 0.309546677$$
$$= 0.38958534$$
$$= 0.30086789$$

Номер шарда	Вес «до»	Процент успеха обработки транзакций	Вес «после»
1	0.3	90	0.309546677
2	0.4	70	0.38958534
3	0.3	80	0.30086789

После обновления весов, транзакции распределяются пропорционально новым весам, обеспечивая справедливую и эффективную обработку транзакций в следующем блоке.

Допустим, публикации в сеть ожидает 1000 транзакций. Тогда, на основе новых весов, каждый шард получит:

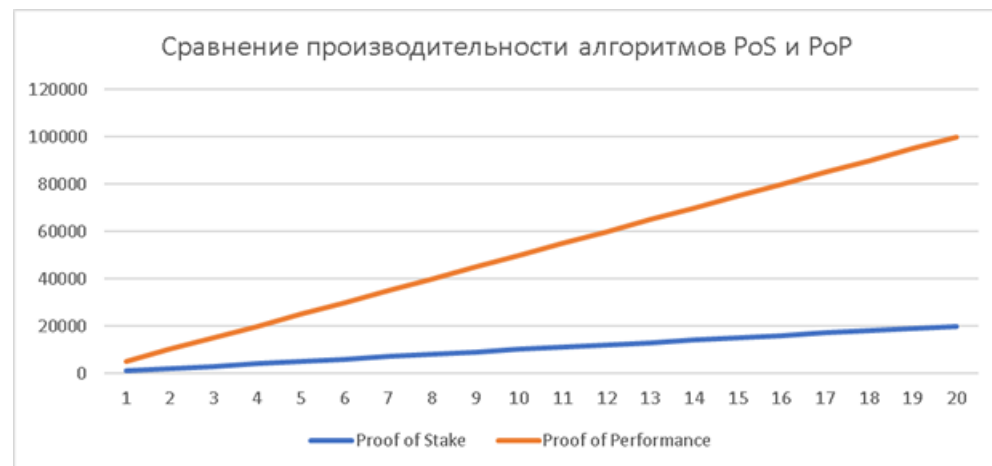
$$Ts1next=1000*0.309546677\approx310,$$
$$Ts2next=1000*0.38958534\approx390,$$
$$Ts3next=1000*0.30086789\approx300.$$

Сравнение скорости обработки транзакций в сетях Proof of Stake и Proof of Performance

Рассмотрим пример, в котором в двух сетях (А и В) существует по 5 узлов, которые поддерживают их работоспособность.

Сеть **A** работает на алгоритме консенсуса Proof of Stake. Условимся, что каждый валидатор (узел) имеет техническое оснащение, позволяющее обработать 1000 транзакций за 1 блок. Тогда, при предложении нового блока, валидатор обрабатывает 1000 транзакций и помещает их в блок, то есть скорость обработки: 1000транз/блок или 167 транз/сек (при среднем времени блока 6 секунд).

В то же время в сети **B**, которая поддерживается алгоритмом консенсуса Proof of Performance при возникновении задачи по генерации нового блока каждый шард берет на себя задачу по обработке 1000 транзакций. При условии, что шардов в сети 5, то скорость обработки транзакций будет: 5000транз/блок или же 833транз/сек. То есть производительность сети на основе алгоритма консенсуса Proof of Performance в X раз больше, чем в сетях на основе Proof of Stake, где X – количество шардов в сети.



Применение алгоритма консенсуса Proof of Performance

Алгоритм PoP может быть внедрен и оказывать положительное влияние на производительность тех блокчейн-сетей, в которых важна высокая пропускная способность при обработке транзакций, а также масштабируемость.

Алгоритм может быть полезен в сетях следующих типов:

- Сети с большим количеством децентрализованных приложений (dApps)^[7];
- Системы IoT (Интернет вещей)^[8];
- Глобальные платежные сети^[9];
- Системы управления цепочками поставок^[10].

Моделирование работы алгоритма Proof of Performance и анализ его влияния на производительность

Для оценки влияния алгоритма Proof of Performance (PoP) на производительность блокчейн-сети был проведен эксперимент, в ходе которого копия сети Polkadot, развернутая на локальном оборудовании, подвергалась нагрузке и замерам метрик производительности сети. После замеров, сеть была обновлена и в нее был внедрен алгоритм Proof of Performance на замену Proof of Stake, который использовался изначально.

Polkadot использует модель парачейнов, где несколько независимых блокчейнов подключаются к основной сети (релейной цепочке) и используют ее вычислительные

мощности для функционирования. При текущей архитектуре нагрузка от парачейнов концентрируется на одном узле в момент создания блока, что может приводить к узким местам и задержкам при обработке транзакций.

Эксперимент состоял из следующих этапов:

1. Создание копии сети Polkadot и запуск парачейнов:

- Развёртывание сети: запущена тестовая сеть, основанная на исходном коде Polkadot, с использованием алгоритма консенсуса PoS.
- Парачейны: развёрнуто 5 парачейнов, имитирующих различные децентрализованные приложения (dApps) с высокой активностью транзакций. Для имитации органической нагрузки на сеть использовались генераторы транзакций, которые публиковали в сеть определенное количество транзакций, создавая нагрузку на узлы сети.
- Конфигурация узлов: сеть состояла из 10 валидаторов для имитации реальной распределённой сети.

2. Измерение производительности сети на PoS:

- Пропускная способность транзакций: по итогам генерации сетью 50 блоков (примерно 5 минут) было обработано 15934 события (транзакции). Средняя пропускная способность составила 53 транзакции в секунду.
- Отказоустойчивость: при отключении 20% валидаторов производительность сети снизилась до 34 транзакций в секунду в течении следующих 50-ти блоков.
- Загрузка узлов: нагрузка центральных процессоров вычислительных машин, на которых располагались узлы-валидаторы находилась на уровне 90-95%, в случае, если валидатор, который располагался на данной машине, был выбран в качестве предлагающего данный блок и 10-15% в случае ожидания очереди на генерацию блока.

3. Миграция сети на алгоритм Proof of Performance:

- Сохранение текущего состояния: создан хеш текущего состояния сети для обеспечения целостности данных после перехода на новую модель консенсуса.
- Внесение предложения об обновлении: инициировано предложение об обновлении алгоритма консенсуса, которое было одобрено участниками сети.
- Обновление программного обеспечения: в исходный код ядра внесены изменения, реализующие минимальные возможности работы сети на алгоритме Proof of Performance. Обновлен алгоритм выбора шардов для обработки транзакций, а также механизм наказаний и поощрений шардов.
- Запуск обновленной сети: проведен запуск сети на основе PoP с перенесенными парачейнами.

4. Измерение производительности сети на PoP:

- Пропускная способность транзакций: по итогам генерации 50-ти блоков пропускная способность сети увеличилась до 259 транзакций в секунду, что является приростом на 487%.
- Отказоустойчивость: при отключении 20% шардов производительность снизилась примерно на 20%.
- Загрузка узлов: нагрузка центральных процессоров вычислительных машин, на которых располагались узлы-валидаторы находилась на уровне 40-60% в течении всего времени замера.

5. Сравнительный анализ результатов:

Алгоритм консенсуса	Proof of Stake	Proof of Performance
Параметр сети		
Пропускная способность (транзакций в секунду)	53	259
Время создания блока (секунд)	6	6
Процент снижения производительности при отказе 20% узлов	30	20
Загрузка узлов в нагрузке (процентов ЦП)	90-95	40-60

6. Выводы:

- Повышение производительности: внедрение PoP значительно повышает эффективность сети, делая ее более подходящей для приложений с высокой нагрузкой.
- Масштабируемость: PoP обеспечивает лучшую масштабируемость без необходимости увеличения вычислительных ресурсов отдельных узлов.
- Улучшение пользовательского опыта: снижение задержек и увеличение скорости подтверждения транзакций повышает удовлетворенность пользователей.

Сценарии внедрения алгоритма Proof of Performance

1. Децентрализованные приложения (dApps)

Сценарий внедрения:

В высоконагруженных dApps (децентрализованных приложениях), таких как децентрализованные биржи, игры или социальные сети, количество транзакций может быть очень высоким, что создает значительную нагрузку на сеть. Узлы сети могут не справляться с обработкой большого объема данных, особенно если они обладают небольшими вычислительными ресурсами.

Рекомендации по применению:

- Использование алгоритма PoP целесообразно в ситуациях, когда dApps генерируют большое количество транзакций, и требуется высокая пропускная способность сети. Обычно, в подобных ситуациях при применении алгоритма PoS индикатором того, что сеть не справляется с нагрузкой, может служить большое время ожидания подтверждения транзакций или увеличение времени генерации блока.
- Если узлы сети имеют слабые вычислительные мощности, PoP поможет распределить нагрузку и обеспечить стабильную работу приложения.

Потенциальные проблемы и вызовы:

- Синхронизация данных между шардами: возможны сложности с обеспечением согласованности данных.
- Сложность настройки: требуется настройка сети, что включает в себя изменение программного кода ядра и других сетевых параметров для поддержки шардинга и PoP.

Возможные решения:

- Внедрение эффективных алгоритмов консенсуса между шардами для обеспечения согласованности данных.
- Предоставление инструментов и документации для упрощения процесса настройки и интеграции PoP.

2. Системы Интернета вещей (IoT)

Сценарий внедрения:

В IoT-сетях множество устройств генерируют данные, которые необходимо обрабатывать в реальном времени. Ограниченные вычислительные ресурсы устройств и высокая скорость генерации данных требуют эффективного решения для обработки транзакций.

Рекомендации по применению:

- Применение PoP в крупных IoT-сетях с высокой плотностью устройств и большими объемами данных.
- Использование PoP для распределения обработки данных между узлами с более высокими вычислительными мощностями.

Потенциальные проблемы и вызовы:

- Ограниченные ресурсы устройств: IoT-устройства могут не поддерживать необходимую вычислительную нагрузку.
- Безопасность данных: обеспечение безопасности и конфиденциальности данных в распределенной сети.

Возможные решения:

- Использование промежуточных узлов или шлюзов с достаточными ресурсами для обработки данных от IoT-устройств.
- Внедрение протоколов шифрования и аутентификации для защиты данных.

3. Глобальные платежные сети

Сценарий внедрения:

Международные платежные системы требуют высокой скорости обработки транзакций и способности масштабироваться под растущие объемы операций. Задержки и низкая пропускная способность могут негативно влиять на пользовательский опыт и доверие к системе.

Рекомендации по применению:

- Внедрение PoP для ускорения обработки транзакций и увеличения пропускной способности сети.
- Использование PoP в системах с большим количеством микроплатежей, где скорость подтверждения транзакции критична.

Потенциальные проблемы и вызовы:

- Регуляторные требования: необходимо соблюдать правила KYC (знай своего клиента) и AML (противодействие отмыванию денег).
- Безопасность транзакций: обеспечение защиты от мошеннических действий и атак.

Возможные решения:

- Интеграция механизмов идентификации и верификации пользователей в систему.
- Реализация дополнительных уровней безопасности и мониторинга транзакций.

Рекомендации по интеграции алгоритма Proof of Performance в существующие блокчейн-инфраструктуры

Рекомендации по применению алгоритма PoP.

Для повышения производительности и устранения проблем, вызванных недостатком мощности отдельных узлов, следует рассмотреть для интеграции алгоритм Proof of Performance в следующих случаях:

- В сетях с высоким объемом транзакций и требованием к высокой пропускной способности.
- В случае, если узлы сети обладают небольшими вычислительными ресурсами и не справляются с нагрузкой.
- При необходимости повышения масштабируемости и отказоустойчивости сети.

Использование алгоритма может быть необязательным:

- В небольших сетях с низким объемом транзакций, где стандартные алгоритмы консенсуса, такие как PoS, удовлетворяют требованиям.
- В случаях, если требования к производительности и скорости обработки не являются критичными.

Внедрение алгоритма Proof of Performance (PoP) в существующую сеть на Proof of Stake (PoS) требует поэтапного подхода и взаимодействия с участниками сети. Ниже представлен общий алгоритм внедрения PoP:

1. Анализ и подготовка.

- Изучите текущую инфраструктуру PoS, определите цели перехода на PoP (повышение производительности, масштабируемость).
- Выявите возможные узкие места и требования к ресурсам.
- Информируйте валидаторов, разработчиков и пользователей о планах.

2. Разработка и тестирование PoP.

- Разработайте версию PoP, совместимую с архитектурой и смарт-контрактами сети.
- Создайте тестовую сеть для испытаний PoP без воздействия на основную сеть.
- Проведите нагрузочные тесты и аудиты безопасности.

3. Сохранение состояния сети.

- Создайте резервную копию текущего состояния сети.
- Сгенерируйте контрольный хеш для проверки целостности после миграции.

4. Предложение обновления консенсуса.

- Используйте механизмы голосования сети для принятия решения об обновлении сети.
- Обеспечьте достижение необходимого кворума.

5. Обновление узлов и программного обеспечения.

- Подготовьте обновленные версии ПО узлов с интегрированным PoP.
- Обеспечьте обратную совместимость для плавного перехода.

- Проведите бета-тестирование с участием ограниченного числа узлов.

6. Развёртывание обновлений

- Определите последовательность обновления узлов.
- Установите мониторинг для отслеживания процесса и быстрого реагирования.
- Предоставьте подробные руководства по обновлению.

7. Запуск обновлённой сети на PoP

- После обновления достаточного числа узлов и получения консенсуса, убедитесь в корректной работе сети.
- Сравните текущий хеш состояния сети с контрольным для подтверждения целостности данных.

8. Мониторинг:

- Обеспечьте мониторинг ключевых метрик сети: пропускную способность, время блоков, нагрузку на узлы.

Внедрение алгоритма Proof of Performance в сеть, работающую на Proof of Stake, представляет собой сложный, но управляемый процесс, который при должной подготовке и реализации может привести к значительным улучшениям производительности и масштабируемости сети.

Анализ преимуществ и недостатков алгоритма Proof of Performance

Преимущества алгоритма Proof of Performance по сравнению с другими алгоритмами консенсуса:

1. Улучшенная масштабируемость и пропускная способность

- Горизонтальный шардинг: использование PoP позволяет эффективно распределять обработку транзакций между шардами, что значительно повышает масштабируемость сети. В отличие от PoS, где нагрузка сосредоточена на узлах-валидаторах, PoP распределяет нагрузку равномерно, позволяя обрабатывать больше транзакций в единицу времени.
- Параллельная обработка: благодаря параллельной обработке транзакций в шардах, сеть может достигать высокой пропускной способности без необходимости увеличения вычислительных ресурсов отдельных узлов.

2. Повышенная отказоустойчивость и надежность сети

- Распределение нагрузки: в PoP выход из строя отдельного шарда не приводит к значительному снижению производительности сети, поскольку другие шарды могут компенсировать нагрузку.
- Снижение рисков перегрузки узлов: отсутствие концентрации обработки на отдельных узлах снижает риски перегрева и сбоев, что повышает общую стабильность сети.

3. Энергоэффективность

- Отказ от ресурсоемких вычислений: в отличие от Proof of Work (PoW), PoP не требует решения сложных криптографических задач, что снижает энергопотребление и делает сеть более экологичной и экономичной.
- Оптимизация ресурсов: узлы используют вычислительные мощности более эффективно, что снижает затраты на поддержание сети.

4. Стимулирование высокой производительности узлов

- Механизмы поощрения и штрафов: PoP мотивирует узлы поддерживать высокую производительность через систему вознаграждений и штрафов, основанных на их эффективности.

5. Гибкость и адаптивность

- Динамическое распределение нагрузки: PoP позволяет динамически изменять распределение транзакций в зависимости от текущей производительности шардов.
- Адаптация к изменяющимся условиям: сеть может быстро реагировать на изменения нагрузки и ресурсов, поддерживая оптимальную производительность.

Недостатки алгоритма Proof of Performance:

1. Сложность реализации и интеграции

- Технические сложности: Внедрение PoP требует значительных изменений в архитектуре сети и глубокого понимания механизмов шардинга.
- Необходимость разработки новых инструментов: требуется создание специальных инструментов и протоколов для обеспечения эффективной работы PoP.

2. Потенциальные риски безопасности

- Уязвимости в шардинге: распределение данных между шардами может создать дополнительные векторы атаки, если не обеспечена надлежащая безопасность.
- Сложности в согласовании данных: обеспечение консистентности и целостности данных между шардами требует надежных механизмов консенсуса.

3. Требования к ресурсам узлов

- Разнородность узлов: узлы с различными вычислительными возможностями могут испытывать сложности в поддержании необходимой производительности.
- Необходимость постоянного мониторинга: для поддержания оптимальной работы сети требуется постоянный мониторинг и управление ресурсами.

4. Сопротивление со стороны сообщества

- Изменение устоявшихся процессов: переход на PoP может встретить сопротивление от участников сети, привыкших к текущим алгоритмам.
- Обучение и адаптация: требуется время и ресурсы для обучения разработчиков и операторов узлов новым методам работы.

Сравнение с другими алгоритмами консенсуса:

1. Proof of Work (PoW):

Преимущества PoP над PoW:

- Более высокая энергоэффективность.
- Лучшая масштабируемость и пропускная способность.
- Отсутствие необходимости в дорогостоящем оборудовании для майнинга.

Недостатки PoP по сравнению с PoW:

- Более сложная система достижения консенсуса.

2. Proof of Stake (PoS):

Преимущества PoP над PoS:

- Улучшенная масштабируемость за счет горизонтального шардинга.
- Более равномерное распределение нагрузки между узлами.
- Меньшая зависимость от стейка (количества токенов) для участия в консенсусе.

Недостатки PoP по сравнению с PoS:

- Сложность внедрения в существующие сети.
- Требуется более сложных механизмов для обеспечения безопасности и согласованности данных.

3. Delegated Proof of Stake (DPoS):

Преимущества PoP над DPoS:

- Более децентрализованный подход без концентрации власти у делегатов.
- Стимулирование производительности каждого узла, а не только избранных.

Недостатки PoP по сравнению с DPoS:

- Более сложная система управления узлами и нагрузкой.
- Возможные трудности в достижении консенсуса между большим количеством шардов.

Проблемы рассмотренных алгоритмов, решение, предложенное алгоритмом PoP, доказательство решения и выводы представлены в следующей таблице:

Проблема	Решение в PoP	Доказательство	Вывод
Перегрузка узлов в PoS	Горизонтальный шардинг и адаптивное распределение весов	Математический и аппарат распределения весов	Динамическое распределение нагрузки между узлами
Снижение отказоустойчивости сети при сбоях	Распределение нагрузки между шардами	Проведенный эксперимент замера производительности сети при отключении 20% узлов	Устойчивость сети сохраняется даже при отключении 20% узлов
Ограниченная пропускная способность	Параллельная обработка транзакций	Проведенный эксперимент сравнения скорости обработки транзакций в сетях PoS и PoP	Увеличение производительности сети до 5000 транзакций/блок
Задержки при обработке транзакций в сети PoS	Распределение транзакций пропорционально производительности шардов	Проведенный эксперимент замера производительности обработки транзакций	Снижение времени ожидания обработки транзакций за счёт равномерной загрузки шардов
		Математический	Система штрафов и

Риск злоупотреблений со стороны узлов	Введение механизма оценки производительности узлов и санкций за неэффективность	аппарат распределения весов, основанный на системе штрафов и поощрений	система штрафов и поощрений мотивирует узлы к поддержанию высокой производительности
Сложность интеграции новых узлов в сеть	Механизм нормализации весов обеспечивает справедливое распределение транзакций в ходе подключения новых узлов к сети	Математический аппарат распределения весов и его справедливое назначение новых весов	Динамическое распределение нагрузки автоматически адаптируется к изменению числа узлов
Сложности в обеспечении согласованности данных	Введение дополнительных хэш-параметров для проверки согласованности	Измененная структура блока включает в себя параметры для учета согласованности данных всеми узлами сети	Хэш соответствия данных между шардами минимизирует риски расхождений в данных

Сравнение взглядов отечественных и зарубежных исследователей на проблему масштабирования блокчейн-сетей

Научные исследования в области алгоритмов консенсуса и масштабируемости блокчейн-сетей активно развиваются как в зарубежной, так и в отечественной литературе. Однако подходы к решению данных вопросов существенно различаются.

1. Зарубежные исследования.

Зарубежные работы, такие как исследование «Sharding-Based Proof-of-Stake Blockchain Protocols: Key Components & Probabilistic Security Analysis» акцентируют внимание на безопасности и вероятностной оценке устойчивости алгоритмов консенсуса. Основное внимание уделяется их применимости в условиях высокой нагрузки на сеть и возможности работы с большим количеством активных узлов. В их исследовании модели PoS процесс увеличения производительности сети рассматривается через внедрение шардинга [\[11\]](#).

Другим примером изучения процесса масштабирования блокчейн-сетей является работа Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer и Robbert van Renesse «Bitcoin-NG: A Scalable Blockchain Protocol», в которой авторы представляют протокол Bitcoin-NG. Он предлагает деление блокчейна на микро- и макроблоки для ускорения обработки транзакций. Однако в нём отсутствуют механизмы динамического распределения нагрузки между узлами, что делает его уязвимым к перегрузкам [\[12\]](#).

2. Отечественные исследования.

В работе Абдулжалилова А.З. «Методы и стратегии масштабируемости блокчейн-технологий: анализ, сравнение и перспективы» автор рассматривает несколько методов, которые обеспечивают увеличение ключевых параметров производительности сети через распределенные системы управления списками, использования шардинга, применение

sidechains и внедрение алгоритмов консенсуса, дружественным к процессу масштабирования [\[13\]](#).

Большое внимание поиску решения проблемы масштабируемости в блокчейн сетях выделяет Гребан В.Н. в своей работе «Практические проблемы использования блокчейн-технологий». В своей работе он рассматривает возможность увеличения размера блоков, использование алгоритмов консенсуса с повышенной производительностью, шардирование, развитие межблокчейных решений и оптимизацию протоколов и алгоритмов как способы решения проблемы масштабирования блокчейн-сетей [\[14\]](#).

3. Основные различия.

Аспект	Зарубежный подход	Отечественный подход
Фокус исследований	Безопасность и вероятность устойчивости алгоритмов консенсуса	Практическая реализация решений масштабируемости
Методы масштабирования	Внедрение шардинга в PoS для повышения производительности; использование микро- и макроблоков	Расширение размеров блоков, использование sidechains, межблокчейновых решений и шардирования
Решение проблемы нагрузки	Отсутствие механизмов динамического распределения нагрузки между узлами	Динамическое распределение нагрузки через адаптацию алгоритмов консенсуса и оптимизацию протоколов
Основной фокус масштабируемости	Работа с высокой нагрузкой на сеть и большим количеством активных узлов	Увеличение производительности сети с учётом ограниченных вычислительных ресурсов
Инструменты решения проблем	Оптимизация структуры блоков и их деление на микро- и макроблоки	Адаптация алгоритмов консенсуса, использование распределённых систем управления и развитие протоколов
Практическое применение	Глобальные сети с большими пулом узлов и высокими нагрузками	Локальные сети с ограниченными ресурсами и потребностью в эффективной интеграции (решения для бизнеса и госструктур)

Согласно рассмотренным взглядам на решение проблемы масштабируемости блокчейн-сетей, становится понятно, что имеет смысл поиск метода, который бы удовлетворял сразу нескольким задачам при построении процесса масштабируемости.

Модель Proof of Performance (PoP) предлагает несколько нововведений, которые вносят значительный вклад в развитие алгоритмов консенсуса и масштабировании блокчейн-сетей:

1. Интеграция горизонтального шардинга:

- В отличие от большинства существующих решений, PoP сочетает шардинг с адаптивным управлением узлами, что позволяет одновременно увеличивать пропускную способность и сохранять устойчивость сети.

2. Система динамического распределения нагрузки:

- PoP вводит механизм расчёта производительности узлов и адаптивного обновления их весов, чего нет в традиционных подходах.

3. Устойчивость к сбоям:

- Эксперименты показывают, что PoP сохраняет производительность сети даже при выходе из строя до 20% узлов, что превосходит показатели других алгоритмов, таких как PoS.

4. Практическая применимость:

- Модель PoP разработана с учётом ограниченных вычислительных ресурсов, что делает её особенно актуальной для внедрения в Российской Федерации, включая государственные и коммерческие проекты.

Таким образом, сравнение отечественных и зарубежных исследований показало, что модель PoP не только решает многие известные проблемы алгоритмов консенсуса, но и предлагает новые подходы, которые могут быть полезны в условиях реальных ограничений. Прирост научного знания заключается в разработке гибкой системы управления узлами, повышающей производительность и устойчивость блокчейн-сетей.

Заключение

В статье рассмотрен принцип работы модели Proof of Performance, учтены и описаны ее особенности, приведен разбор и пример работы алгоритма. Проведен анализ скорости обработки транзакций и определены возможные пути ее применения.

Представленная и описанная модель позволит внедрить адаптивный подход к потреблению ресурсов, а также найти компромисс между потребностями в производительности сети и затратами на поддержание ее работоспособности.

Библиография

1. Бауэр В.П., Побываев С.А., Кузнецов Н.В. Потенциал использования технологии распределенного реестра (блокчейн) в системах государственного управления // Фундаментальные исследования. 2019. № 12 (часть 2). С. 247–252.
2. Борискевич И.А. Алгоритмы консенсуса в блокчейн сетях // Белорусский государственный университет информатики и радиоэлектроники. 6-я Научная Конференция Аспирантов, Магистрантов и Студентов БГУИР. Минск, 2020. С. 116–117.
3. Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016). A Secure

- Sharding Protocol for Open Blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 17–30).
4. Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., & Ford, B. (2017). OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding. IACR Cryptology ePrint Archive, 2017(406).
5. Zamani, M., Movahedi, M., & Raykova, M. (2018). RapidChain: Scaling Blockchain via Full Sharding. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 931–948).
6. King, S., & Nadal, S. (2012). PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Retrieved from <https://bitcoin.peryaudo.org/vendor/peercoin-paper.pdf>
7. Swan, M. (2015). Blockchain 2.0: Contracts. In Blockchain: Blueprint for a New Economy (pp. 9–10). O'Reilly Media, Inc.
8. Шаламов Г. А., Петухов А. С. Слияние технологий IoT и блокчейн: от теории до реального времени // Прогрессивная экономика. 2023. № 9. С. 32. DOI: 10.54861/27131211_2021_9_32.
9. Goswami, S. (2017). Scalability analysis of blockchains through blockchain simulation. Thesis, Master of Science in Computer Science, University of Nevada, Las Vegas.
10. Zamyatin, A., Harz, D., Lind, J., Gudgeon, L., Werner, S., & Knottenbelt, W. J. (2019). XCLAIM: Trustless, Interoperable, Cryptocurrency-Backed Assets. In IEEE Symposium on Security and Privacy (pp. 193–210).
11. Makrakis, D., & Senhaji, A. (2023). Sharding-Based Proof-of-Stake Blockchain Protocols: Key Components & Probabilistic Security Analysis. Sensors, 23(5), 2819. DOI: 10.3390/s23052819.
12. Eyal, I., Gencer, A. E., Sirer, E. G., & van Renesse, R. (2016). Bitcoin-NG: A Scalable Blockchain Protocol. In Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI '16) (pp. 45–59).
13. Абдулжалилов А.З. Методы и стратегии масштабируемости блокчейн-технологий: анализ, сравнение и перспективы // Международный научный журнал «Вестник науки.» 2023. № 11 (68). Т. 4. С. 625–634.
14. Гречан В.Н. Практические проблемы использования блокчейн-технологий // Научный сетевой журнал «Столыпинский вестник.» 2024. № 9.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.

Со списком рецензентов издательства можно ознакомиться [здесь](#).

Статья посвящена исследованию и описанию модели и алгоритма консенсуса Proof of Performance (PoP) для блокчейн-сетей. В работе подробно рассматриваются основные элементы модели, преимущества предложенного алгоритма и его потенциал для повышения производительности и масштабируемости блокчейн-систем.

Методология исследования базируется на сравнительном анализе существующих алгоритмов консенсуса, таких как Proof of Stake (PoS), и предложенного алгоритма Proof of Performance. В статье представлены теоретические расчеты, алгоритмические схемы и примеры применения PoP, а также результаты моделирования, подтверждающие эффективность предложенного подхода.

Исследование актуально в свете растущих требований к производительности и масштабируемости блокчейн-сетей. Традиционные алгоритмы, такие как PoS, имеют ограничения по пропускной способности и устойчивости к нагрузкам. Внедрение новых моделей, таких как PoP, может существенно повысить эффективность обработки

транзакций и устойчивость сети к сбоям.

Научная новизна работы заключается в предложении и разработке нового алгоритма консенсуса, который использует горизонтальный шардинг для равномерного распределения нагрузки между узлами сети. Это позволяет повысить пропускную способность сети и уменьшить вероятность возникновения сбоев из-за перегрузки отдельных узлов.

Статья написана в научно-техническом стиле, характеризуется логичной структурой и последовательным изложением материала. Введение содержит обоснование актуальности темы, основная часть включает описание алгоритма, его преимущества и примеры применения. Заключение подводит итоги и намечает направления дальнейших исследований.

Авторы делают обоснованные выводы о преимуществах модели Proof of Performance, таких как увеличенная скорость обработки транзакций и улучшенная масштабируемость сети. Результаты моделирования подтверждают эффективность предложенного подхода. Статья будет интересна широкому кругу специалистов в области блокчейн-технологий, включая разработчиков, исследователей и инженеров, занимающихся вопросами повышения производительности и масштабируемости блокчейн-сетей.

Рекомендации по доработке:

Для улучшения восприятия материала и повышения его практической ценности, рекомендуется дополнить работу следующими элементами:

1. Примеры практического применения:

- Добавить конкретные примеры внедрения алгоритма Proof of Performance в реальные блокчейн-сети. Это может включать описание пилотных проектов или сценариев использования, которые помогут читателям лучше понять практическую значимость предложенного решения.

- Привести данные о потенциальных улучшениях производительности и пропускной способности сети при переходе от традиционных алгоритмов консенсуса к PoP на основе реальных кейсов.

2. Сценарии внедрения:

- Описать возможные сценарии внедрения алгоритма Proof of Performance в различных типах блокчейн-сетей, таких как децентрализованные приложения (dApps), системы Интернета вещей (IoT) и глобальные платежные сети.

- Рассмотреть потенциальные проблемы и вызовы, которые могут возникнуть при внедрении PoP, а также предложить возможные решения для их преодоления.

3. Включить практические рекомендации для разработчиков и инженеров по интеграции алгоритма PoP в существующие блокчейн-инфраструктуры. Это может включать советы по настройке сети, оптимизации вычислительных мощностей и управлению нагрузкой.

4. Провести более детальный анализ преимуществ и недостатков алгоритма Proof of Performance по сравнению с другими алгоритмами консенсуса. Это поможет читателям объективно оценить целесообразность использования PoP в различных контекстах.

Внесение указанных дополнений сделает статью более полной и информативной, а также увеличит её ценность для практического применения.

В целом, работа представляет собой значительный вклад в область исследований блокчейн-технологий и заслуживает публикации в журнале "Программные системы и вычислительные методы".

Результаты процедуры повторного рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.

Со списком рецензентов издательства можно ознакомиться [здесь](#).

Предмет исследования. С учётом выбранного заголовка статья должна быть посвящена вопросам использования модели и алгоритма консенсуса Proof of Performance. Содержание статьи соответствует заявленной теме, однако полностью её не раскрывает, т.к. не содержится обоснований авторским суждениям.

Методология исследования базируется на анализе и синтезе данных. Было бы также интересно графически представить предлагаемые рекомендации. Ценно, что при обосновании доказательств корректности работы алгоритма автор применяет математический аппарат, обеспечивающий позитивное впечатление от рецензируемой статьи. Однако важно также полученные выводы в процессе применения математического аппарата сопоставить с обозначенными проблемами использования алгоритма и путями их решения. Например, это может быть представлено в виде схемы.

Актуальность исследования обусловлена важностью изучения вопросов обработки транзакций в алгоритме Proof of Performance как для конкретных экономических агентов, так и для обеспечения цифровой трансформации в Российской Федерации. При этом потенциальную читательскую аудиторию интересуют конкретные обоснованные авторские рекомендации по решению выявленных в процессе исследования проблем.

Научная новизна в представленном на рецензирование материале частично содержится. В частности, она связана с рекомендациями по интеграции алгоритма Proof of Performance в существующие блокчейн-инфраструктуры.

Стиль, структура, содержание. Стиль изложения является научным. Текст структурирован. Содержание статьи представляет собой развёрнутый план, приведённые тезисы следует наполнить конкретными авторскими обоснованиями и дополнениями. В содержании статьи автор привёл результаты анализа преимуществ и недостатков алгоритма Proof of Performance, однако приведённые тезисы нуждаются в обосновании, а также в рекомендациях по устранению выявленных недостатков. При проведении доработки статьи было бы интересно сравнить с другими алгоритмами.

Библиография. Библиографический список состоит из 11 наименований. Ценно, что автор проработал зарубежные источники, однако абсолютно не уделил внимание отечественным научным публикациям, что говорит о недостаточной проработке методологической базы. При проведении доработки статьи данное замечание следует обязательно устранить.

Апелляция к оппонентам. Несмотря на сформированный список научных публикаций, какой-либо научной дискуссии не осуществлено. Было бы интересно показать отличия отечественной и зарубежной мысли по данному вопросу. При проведении доработки статьи необходимо обязательно полученные результаты обсудить с теми, кто были получены другими авторами. Также важно показать ответ на вопрос: "В чём состоит прирост научного знания по сравнению с уже имеющимся в литературе?"

Выводы, интерес читательской аудитории. С учётом вышеизложенного заключаем о необходимости доработки статьи с учётом обозначенных замечаний. После проведения доработки и проведения повторного рецензирования может быть решён вопрос о целесообразности опубликования данной статьи. При качественной доработке она будет востребована у лиц, занимающихся данными вопросами, в т.ч. в рамках учебного

процесса в высших учебных заведениях.

Результаты процедуры окончательного рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.

Со списком рецензентов издательства можно ознакомиться [здесь](#).

Представленная статья на тему «Модель и алгоритм консенсуса Proof of Performance» соответствует тематике журнала «Программные системы и вычислительные методы» и посвящена актуальной проблеме повышения производительности и масштабируемости блокчейн-сетей обусловлена растущими требованиями к обработке транзакций в высоконагруженных системах, таких как финансовые технологии, системы Интернета вещей (IoT) и децентрализованные приложения (dApps). Как указывают авторы в статье, существующие алгоритмы консенсуса, включая Proof of Stake (PoS) на базе ядра Tendermint демонстрируют ограниченную пропускную способность, обусловленную высокой нагрузкой и ограниченными ресурсами производительности узлов-валидаторов сети. Эти ограничения создают узкие места в функционировании сетей и снижают их устойчивость к изменениям нагрузки.

В статье представлен достаточно широкий анализ литературных российских и зарубежных источников по теме исследования.

В качестве новизны исследования авторы указывают предложение и описание новейшего алгоритма Proof of Performance, сочетающего адаптивное распределение нагрузки и учет производительности узлов, что позволяет существенно увеличить пропускную способность сети и её устойчивость к изменениям нагрузки. Представленная работа закладывает основу для дальнейших исследований, направленных на интеграцию описанного алгоритма консенсуса в существующие блокчейн-системы и развитие технологий децентрализованного управления нагрузкой.

Стиль и язык изложения материала является научным и доступным для широкого круга читателей. Статья по объему соответствует рекомендуемому объему от 12 000 знаков.

Статья достаточно структурирована - в наличии введение, заключение, внутреннее членение основной части (Описание модели Proof of Performance, Структура блока в модели Proof of Performance, Распределение весов, Доказательство корректности работы алгоритма, Сравнение скорости обработки транзакций в сетях Proof of Stake и Proof of Performance, Применение алгоритма консенсуса Proof of Performance, Моделирование работы алгоритма Proof of Performance и анализ его влияния на производительность, Сценарии внедрения алгоритма Proof of Performance, Рекомендации по интеграции алгоритма Proof of Performance в существующие блокчейн-инфраструктуры, Анализ преимуществ и недостатков алгоритма Proof of Performance, Сравнение взглядов отечественных и зарубежных исследователей на проблему масштабирования блокчейн-сетей).

Авторами рассмотрен принцип работы модели Proof of Performance, учтены и описаны ее особенности, приведен разбор и пример работы алгоритма; проведен анализ скорости обработки транзакций и определены возможные пути ее применения.

Практическая значимость статьи четко обоснована. Представленная и описанная модель позволит внедрить адаптивный подход к потреблению ресурсов, а также найти компромисс между потребностями в производительности сети и затратами на поддержание ее работоспособности.

Статья «Модель и алгоритм консенсуса Proof of Performance» может быть рекомендована к публикации в журнале «Программные системы и вычислительные методы».