DOI: 10.25559/SITITO.020.202401.92-100
УДК 004.75

Оригинальная статья

Анализ консенсус-механизмов блокчейна и их применимость к системам Интернета вещей

М. О. Мельников*, Е. В. Игонина
ФГБОУ ВО «Елецкий государственный университет им. И. А. Бунина», г. Елец, Российская Федерация
Адрес: 399770, Российская Федерация, Липецкая область, г. Елец, ул. Коммунаров, д. 28-1
* melnikov.maxx@yandex.ru

Аннотация

Консенсус-механизм является основным компонентом технологии блокчейн, позволяющим множеству узлов согласовывать консистентное представление о данных внутри сети блокчейна. Тщательно подобранный алгоритм, на основе которого происходит консенсус транзакций, может обеспечить сеть такими свойствами как отказоустойчивость и неизменяемость. В настоящее время актуальным является применение блокчейна (со всеми его преимуществами) к системам Интернет вещей (IoT), набирающих с каждым годом всё большую популярность. IoT-системы используется в важных для общества сферах таких как здравоохранение, экономика, сельское хозяйство, транспорт, также находит применение в различных формах социального обеспечения («умные города», логистические поставки, отслеживание товара, посылки и т.п.). Целостность и консистентность данных чрезвычайно важны в этих сферах, потому программно-аппаратный сбой или дискредитация данных могут нанести ущерб компании и ее клиентам, использующим IoT-устройства. Кроме того, блокчейн стал основой для децентрализованных сетей. Основной сложность внедрения блокчейн в IoT является нехватка вычислительных ресурсов этих самых «умных устройств». Из этого следует, что традиционные консенсус-алгоритмы, например, Proof of Work не применимы, так как являются чрезвычайно ресурсозатратными. В данной статье проведен сравнительный анализ популярных механизмов консенсуса по перечню выработанных критериев. На основе полученных результатов сделаны выводы, помогающие в выборе наиболее подходящих механизмов консенсуса для применимости в IoT-системах, определены условия, необходимые для их интеграции. Также рассмотрена возможность реализации как PoW, так и PoS алгоритмов в IoT-системах с помощью специально разработанных для них консенсус-алгоритмов, таких как Microchain и Proof of Supply Chain Share.

Ключевые слова: консенсус, консенсус-алгоритмы, блокчейн, IoT-системы

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Для цитирования: Мельников М. О., Игонина Е. В. Анализ консенсус-механизмов блокчейна и их применимость к системам Интернета вещей // Современные информационные технологии и ИТ-образование. 2024. Т. 20, № 1. С. 92-100. https://doi.org/10.25559/SITITO.020.202401.92-100

Original article

Analyzing Blockchain Consensus Mechanisms for Internet of Things Networks

M. O. Melnikov*, E. V. Igonina
Bunin Yelets State University, Yelets, Russian Federation
Address: 28-1 Kommunarov St., Yelets 399770, Lipetsk region, Russian Federation
* melnikov.maxx@yandex.ru

Abstract

The consensus mechanism is the main component of blockchain technology, which allows multiple nodes to agree on a consistent view of data within the blockchain network. A carefully selected algorithm, based on which the consensus of transactions occurs, can provide the network with such properties as fault tolerance and immutability. Currently, it is relevant to apply the blockchain (with all its advantages) to Internet of Things (IoT) systems, which are gaining more and more popularity every year. IoT systems are used in areas important to society such as healthcare, economics, agriculture, transport, and are also used in various forms of social security (smart cities, logistics, product tracking, parcels, etc.). Data integrity and consistency are extremely important in these areas, because hardware and software failure or discrediting the data may harm the company and its customers using IoT devices. In addition, the blockchain has become the basis for decentralized networks. The main difficulty of implementing blockchain in IoT is the lack of computing resources of these "smart devices". It follows from this that traditional consensus algorithms, for example, Proof of Work, are not applicable, as they are extremely resource-intensive. This article provides a comparative analysis of popular consensus mechanisms according to the list of developed criteria. Based on the results obtained, conclusions are drawn that help in choosing the most appropriate consensus mechanisms for applicability in IoT systems, and the conditions necessary for their integration are determined. The possibility of implementing both PoW and PoS algorithms in IoT systems using consensus algorithms specially developed for them, such as Microchain and Proof of Supply Chain Share, is also considered.

Keywords: consensus, consensus algorithms, blockchain, IoT-systems

Conflict of interests: The authors declare no conflict of interest.

For citation: Melnikov M.O., Igonina E.V. Analyzing Blockchain Consensus Mechanisms for Internet of Things Networks. *Modern Information Technologies and IT-Education.* 2024;20(1):92-100. https://doi.org/10.25559/SITITO.020.202401.92-100

Введение

Блокчейн (англ. blockchaine – цепь из блоков) представляет собой криптографически связанный распределенный реестр, главная особенность которого заключается в том, что он хранит историю транзакций в сети по типу биткойн (от англ. bitcoin, от bit – бит и coin – монета). Лежащая в основе биткойн, технология блокчейн обладает двумя важными свойствами: тройной записью и устойчивостью к взлому или фальсификации данных. В следствии того, что каждый блок в блокчейне криптографически связан с предыдущим блоком, попытка вмешательства в цепочку блокчейн завершится аннулированием криптографической связи между блоками. Следовательно, злоумышленники не способны изменить историю операций блокчейна. Учет с тройной записью является ключевой характеристикой распределенной сети. Вместо того чтобы верифицироваться по двустороннему соглашению, для предоставления доказательств своей деятельности транзакции в блокчейне передаются всей сети сразу. Это даёт возможность любому пользователю подтвердить все транзакции в блокчейне, который непосредственно связан с механизмом консенсуса. В свою очередь механизмы консенсуса позволяют блокчейнам сходиться на общесетевом соглашении о консистентном и целостном состоянии данного реестра, поэтому все узлы сети синхронизированы и принимают одну и ту же историю. Например, в системе Bitcoin консенсус достигается за счет применения алгоритмов Proof of Work (далее PoW) и Longest Chain Rule (далее LcR).

PoW – основан на поисках множества решений криптографической вычислительной головоломки, решением которой занимаются участники децентрализованной сети, именуемые майнерами. Решение вычислительных задач майнерами совершается за счет использования аппаратных ресурсов их устройств. За успешное разрешение задачи они получают финансовый стимул, из-за чего продолжается поддержка сети.

LcR – средство разрешения форков, которое занимается менеджментом конкурирующих историй блокчейна и поддерживает сеть в едином согласованном состоянию в случаях, когда происходит форк блокчейна.

В последнее время повышается интерес к применению технологии блокчейн в сфере Интернета вещей (далее IoT). Все чаще механизмы консенсуса модифицируют, чтобы достичь меньшей ресурсоемкости и большей пригодности для развертывания в IoT. На первый план в мире IoT-блокчейна вышли такие механизмы консенсуса, как Proof of Supply Chain Share (далее PoSCS) и Credit-Based PoW (далее CBPoW).

Задачи исследования

Для решения вопросов, связанных с выбором наиболее подходящих механизмов консенсуса для их использования в IoT-системах и определения условий интеграций с заданной системой, в начале необходимо обсудить критерии оценки механизмов консенсуса. В связи со сказанным, в первой части статьи рассматриваются фундаментальные свойства блокчейн. Вторая часть статьи посвящена анализу конкретных механизмов консенсуса. Анализируются консенсус-алгоритмы, наиболее часто используемые в блокчейнах, например, такие как Proof of Stake (далее PoS) и Proof of Work; далее проводится изучение информации в источниках, содержащих описание четырех новых механизмов, разработанных специально для IoT консенсуса. Осуществляется анализ рассмотренных механизмов консенсуса с помощью предложенных нами выше критериев. Уделяется внимание свойствам, которые положительно и отрицательно влияют на критические характеристики устройств IoT. В заключении приводятся рекомендации по выбору консенсуса для IoT-систем и определяются перспективы дальнейшей исследовательской работы.

Критерии консенсуса в блокчейне

Система IoT представлена широким спектром сервисных решений. Они вынуждены соответствовать большому количеству разнородных требований как к вычислительным ресурсам, так к хранению данных и энергоёмкости. Зачастую IoT-оборудование прибывают в реактивных средах, в которых разного рода датчики и механизмы непрерывно генерируют данные, совершают подключение и отключение в зависимости от потребностей в энергии, и, чаще всего, работают в децентрализованных беспроводных сетях ad hoc.

Благодаря высокой гибкости устройства IoT получают широкое распространение в таких приложениях, как «умный дом», «умный город» [1], в сфере здравоохранение [2] и цепочки поставок [3-6].

Целостность данных в блокчейн достигается за счет использования механизмов (алгоритмов) консенсуса. Механизм консенсуса представляет из себя набор правил или протоколов, которым должна следовать группа систем, чтобы принять решение о подтверждении фиксации в системе. Консенсус является критически важной частью большинства развертываний блокчейна, но выбор становится еще более важным при работе с блокчейном, ориентированным на IoT. При выборе блокчейна всегда стоит вопрос компромиссов. Некоторые системы более ресурсоемки, какие-то быстрее, а менее децентрализованные. Для сравнения блокчейнов, а именно консенсус-алгоритмов, лежащих в основе блокчейна, определим ряд требований, оказывающих влияние в системах IoT:

1. Безопасность. Некоторые реализации блокчейна могут обеспечить более высокий уровень надежности и гарантии безопасности по сравнению с традиционными IoT-сетями, завязанными на центральных точках отказа.
2. Потребление ресурсов процессора. Важным фактором при выборе механизма консенсуса будет максимальное продление времени работы аккумулятора IoT-устройства и поддержание достаточного уровня загрузки процессора.
3. Хранение данных. Если каждый узел сети хранят полную копию блокчейна, то они могут независимо проверять транзакции и помогать других узлам загружать свои блокчейны. Обычно IoT-устройства не имеют достаточного хранилища, чтобы содержать десятки гигабайт данных блокчейн. В следствии чего необходимо прийти к компромиссу, обеспечивающему безопасность и достаточный уровень децентрализацию.
4. Количество транзакции в секунду (TPS). Чем больше узлов участвует в процессе консенсуса, тем выше задержка принятия решения. Это приводит к снижению скорости работы, но повышает децентрализацию. Уменьшение количества узлов

приводит к увеличению пропускной способности транзакций в сети и уменьшает времени блокировки, что также критически важно для устройств IoT[1].

5. Децентрализация. Максимизация децентрализации сети позволяет диверсифицировать хранение данных и принятие решений в блокчейне, однако влияет на масштабируемость сети и скорость. Снижение децентрализации приводит к обратному эффекту – приоритет масштабируемости и скорости.

Механизмы консенсуса в блокчейне

Рассмотрим и проанализируем работу наиболее популярных консенсус-алгоритмов и их модификаций.

Proof of Work (*PoW*) – это консенсус-алгоритм, который используется в сети биткойн. Именно он лег в основу большинства криптовалют (посредством форков) [7]. Большая часть современных реализаций PoW основана на разрешении криптографической задачи с определенным набором параметров, и первый пользователь, который решает эту задачу, получает вознаграждение в виде специальных токенов (или их частей). Классическая схема работы выглядит следующим образом: майнеры ищут nonce (сгенерированное псевдослучайное число), которое хэшируется вместе с заголовком блока блокчейна, чтобы получить хэш блока с определенным количеством ведущих нулей [8]. Первый пользователь блокчейна, рассчитавший хэш с соблюдением всех требований, получает вознаграждение в качестве оплаты за затраченные вычислительные ресурсы. Механизм консенсуса биткойн не останавливается на одном лишь PoW, он включает в себя взаимодействие сразу двух компонентов – PoW и правила длиннейшей цепи (далее LcR). В литературе эта связка получила название «консенсус Накамото»[2]. В ней PoW отвечает сразу за две наиболее важные функции – механизм обеспечения финансового стимула для майнера (участника блокчейна) и защиту от атаки Sybil [9].

PoW на основе доверия (C*redit Base Pow, далее CBPoW*). Некоторые исследователи блокчейна предлагают систему PoW на основе «доверия», которая более подходит для работы с IoT-устройствами [10]. Авторы создали консенсус-алгоритм, который динамически регулирует сложность вычислительной задачи PoW в зависимости от того, насколько устройства соблюдает правила консенсуса. Происходит это за счёт вычисления так называемого «общего балла» (node total score) узла сети, рассчитываемого динамически путем суммирования положительного балла (positive score) и отрицательного балла (negative score) устройства. Значение положительного балла растёт за счет точного следования механизму консенсуса, в то время как отрицательный балл увеличивается. Узел не подчиняется консенсусу или проявляет признаки подозрительной активности.

Доказательство проделанной работы и удачи (*Proof of Elapsed Work and Luck, далее PoEWAL*). PoEWAL – механизм консенсуса, который по своим характеристикам похоже на PoW, но модифицирован так, чтобы его можно было использовать на устройствах с ограниченными вычислительными ресурсами [11].

В основе PoEWAL все ещё лежит решение криптографических задач, но вместо того, чтобы устройства вычисляли подходящий nonce, пользователю нужно просто «добывать» (производить вычисления) его в течение некоторого короткого временного периода. Это приводит к значительному снижению вычислительной нагрузки и энергопотребления на IoT-устройстве. По истечении времени «окна майнинга» майнеры сравнивают свои хэш-значения, полученные в момент решения вычислительной задачи. Если узел имеет наибольшую нулевую последовательность в hash-value, то система выдаёт подтверждение о получении блока из предыдущего «вычислительного раунда». Если несколько майнеров имеют одинаковые хэш-значения (по количеству нулей), то задействуется механизм Pof of Luck (далее PoL). В процессе PoL происходит сопоставление выработанных хэшей, содержащих одинаковое количество последовательных нулевых значений, а затем выбирается узел, у которого значение полученного хэша минимально [12]. В своем механизме PoEWAL использует раунды, чтобы обеспечить жесткие ограничения времени синхронизации, поскольку разработчики алгоритма предполагают, что IoT-устройства, как правило, имеют синхронизацию по времени.

Протокол византийского соглашения (*Byzantine Agreement Protocol, далее BAP*). Классическим примером блокчейна, использующего BAP, является Algorand [13]. Algorand – криптовалютный блокчейн, автором которого является Сильвио Микали (итало-американский учёный в области теории вычислительных систем, лауреат премии Тьюринга). В его сеть базируется на верифицируемой случайной функции (далее VRF) для работы механизма консенсуса, основанного на протоколе византийского соглашения [14]. Пользовательские ноды принимают участие в консенсусе за счет вычисления оценочной функции. Децентрализованный случайный маяк (далее DRB) дает возможность узлам договориться о VRF и совместно создавать один новый выходной VRF на каждом раунде вычислений.

В данном контексте VRF подразумевает обязательство по детерминированному псевдослучайному значению. Выходы функции остаются несмещенными за счет своих псевдослучайных свойств [15]. Кроме того, VRF выступает своего рода лотереей для выбора нескольких «лидеров», предлагающих блоки «комитету». Если большинство членов комитета соответствуют некоторым условиям, а узел предлагает действительный блок, то этот блок может быть сертифицирован и добавлен в блокчейн.

Доказательство доли владения (*Proof of Stake, далее PoS*). PoS зародился в начале 2012 года. Первое публичное упоминание произошло в том же году в статье исследователей Скотта Надалема и Санни Кинга[3]. Группа программистов остановилась на варианте, который подразумевал завязать работу консенсус-алгоритма с coin-age token (возраст токена). Механизм раз-

[1] Ethereum: A secure decentralised generalised transaction ledger / G. Wood [et al.] // Ethereum Project Yellow Paper, 2014.

[2] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. Portal Unicamp: Campinas, Brazil, 2008.

[3] King S., Nadal S. Pcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. [Электронный ресурс]. URL: https://bitcoin.peryaudo.org/vendor/peercoin-paper.pdf (дата обращения: 20.12.2023).

рабатывался в качестве альтернативного PoW. Авторы спроектировали систему, в которой майнер использует PoW, чтобы получить стартовый запас токенов в сети, а затем система медленно уменьшает вознаграждение за вычисления, чтобы снизить зависимость от PoW.

Как и в реализации PoW, заголовок хешируется, однако PoS не тратит ресурсы на перерасчёт none, так как выполняет вычисление только один раз. Затем совершается проверка if *coin age > (blockhash / target)*, то майнер может интегрировать вычисленный блок в цепочку. В противном случае узел ожидает следующего раунда, чтобы проверить, соответствует ли он критериям для создания блока [16]. PoS резко набрал популярность благодаря минимальным требованиям к аппаратному обеспечению и значительно меньшему энергопотреблению (если сравнивать с PoW). В данный момент второй по мировой популярности блокчейн Ethereum использует модификацию PoS в качестве базового механизма консенсуса [8].

Доказательство разделения цепи поставок (*Proof of Supply Chain Share, далее PoSCS*). PoSCS – алгоритм за авторством программиста, предпринимателя и исследователя Патрика Цанга. Первоначально механизм разрабатывался, чтобы оптимизировать организацию цепочек поставок и скоропортящихся продуктов питания [17]. Система использует IoT-сеть для мониторинга и управления узлами, а блокчейн-сеть для разного рода манипуляций данными о продуктах питания на всем жизненном цикле поставки. Также используется децентрализованное хранилище баз данных, содержащее архив с данными.

Авторы механизма отмечают, что PoW не подходит для IoT из-за высоких вычислительных затрат. Поэтому они остановились на механизме консенсуса, схожем с PoS, но решили отказаться от необходимости в валютной системе репутации. Участники блокчейна имеет несколько факторов, которые отвечают за их репутация на платформе: преданность (dev), интерес (int); удовлетворенность (sat); влияние (inf). Факторы «взвешиваются» согласной одной из трех стратегий:

– стратегии «интерес превыше всего»;
– стратегии «преданность превыше всего»;
– стратегии «умеренность».

Выборка по совокупности фактором и учет их весовых коэффициентов не позволяют алгоритму консенсуса выбирать участников, которые максимизирую только один фактор. Эти факторы и веса используются для псевдослучайного выбора производителя блока, который должен будет создавать блок.

Доказательство емкости (*Proof of Capacity, далее PoC*). Данный механизм ориентирован на емкость жесткого диска, а не на майнинг, с помощью graphics processing unit (GPU), central processing unit (CPU). Отдельно выделяют специальные устройства – ASIC (application specific integrated circuit). BurstCoin (блокчейн и одноимённая криптовалюта) взял за основу именно PoC.

Добыча блоков BurstCoin состоит из двух последовательных стадий – «черчения» (plotting) и «добычи» (майнинга). Майнинг представляет собой хэширование списка nonce и дальнейшее сохранение его на HHD или SSD диски.

Хэши как в Bitcoin, не отбрасываются, а объединяются в scoopse («черпаки», пары хэшей) и хранятся на накопители участника. Майнеры вычисляют номер scoop и используют его для построения цепочек блоков [18]. BustCoin использует Shabal-хэширование, так как оно более криптографически стойкое, чем классические SHA256 или MD5, которые используются в Bitcoin и многих других блокчейнах-сетях.

Механизм консенсуса *Microchain* представляет собой облегченный алгоритм, преимущественно предназначенный для IoT-экосистем [19]. Microchain концептуально схож с PoS и BAP: несколько пользователей-валидаторов добавляются в комитет, комитет выбирает узел для создания блока. Комитет занимается выбором случайного множество участников блокчейна, чтобы тем самым минимизировать вероятность «избрания» предвзятого или злонамеренного майнера. Консенсус использует собственный комитет – «Династия» (Dynasty). Microchain использует комбинацию компонентов: Voting based Chain Finality (VCF) и Proof of Credit (далее PoC). PoC – это консенсус PoS, который использует «вес» доверия для увеличения шансов конкретного узла на создание блока. Учитывая распределение доверительных свойств в конкретной Династии, пользователи с более высоким доверительным весом имеют больше шансов быть выбранными комитетом для производства блока.

Доказательство важности (*Proof of Importance,* далее *PoI*). Алгоритм PoI, предложенный NEM (Движение новой экономики), имеет много общего с PoS, где узлам сети необходимо зафиксировать некоторое количество токенов. Чтобы быть стать валидатором, кошелём NEM должны иметь на балансе как минимум 10 000 токенов в течение некоторого периода времени. Такой показатель важности увеличивается за счет использования сети NEM и отправки транзакций.

Гибридный консенсус *PoW/PoS.* Существуют распределённые системы, которые предпочитают использовать компромиссные вариации механизма консенсуса. Например, используя комбинацию из элементов PoW и (или) PoS. Так криптовалютный блокчейн Decred, создатели которого отказались использовать PoW из-за проблемы «двойной траты» и PoS из-за проблемы «ничего не стоит на кону», решили разработать гибридный алгоритм, который должен быть не подвержен перечисленным выше проблемам [20]. Decred также основан на майнинге блоков, которые нельзя добавлять непосредственно в блокчейн. Суть в том, что майнеры предлагают свои блоки сети PoS-узлов, которые покупают билеты (tikets) в качестве своей доли в блокчейне (похоже на концепцию лотерейных билетов)[4]. В случае если PoS-узел псевдослучайно выбран из пула билетов, только тогда он подтверждает блок и добавляет его в блокчейн.

Для более наглядного представления вышерассмотренные механизмы консенсуса представлены с помощью иллюстраций. Информация, представленная на рисунках, получена на основе проведенного исследования и анализа литературных источников. На рисунке 1 приведены общие свойства механизмов консенсуса, например, устойчивость к взлому (уязвимость 51% и 33%), время блока и количество транзакций в секунду (TPS). На рисунке 2 представлены IoT-ориентированные механизмы консенсуса (Microchain, CBPoW, PoSCS, PoEWAL). На рисунке 3 приведено сравнение рассматриваемых консенсус-алгоритмов на основе предлагаемых в настоящей работе критериев с последующим присвоением рейтинга каждому консенсусу.

[4] Jepson C. DTB001: Decred Technical Brief [Электронный ресурс]. URL: https://decred.org/dtb001.pdf (дата обращения: 20.12.2023).

Consensus	Blockchain	Block Time	TPS	Adversary Tolerance	L2 Network
PoW	Bitcoin	10 min	7	<51%	Lightening Network
	Litecoin	2.5 min	56		
	Monero	2 min	Variable		None
	Ethereum	12–14 s	15		Side Chains, Rollups
	Horizen	2.5 min	N/A		Side Chains
	CBPoW	Variable	500+		None
	PoEWAL	Variable	25		None
PoS	Ethereum (PoS)	12 s	TBD	<51%	TBD
	Algorand	4.5 s	1000	<33%	Off-chain Contracts
	Dfinity	Variable	Variable	<33%	None
	Cosmos	6 s	1000+	<33%	
	PIVX	60 s	173	<51%	
	Microchain	9 s	230+	<33%	
	PoSCS	Variable	Variable	<51%	
PoW + PoS	Decred	5 min	14	<51%	Lightening Network
PoC	BurstCoin	4 min	80+	<50%	None
PoI	NEM	1 min	4000	<51%	

Р и с. 1. Обзор механизмов консенсуса

F i g.1. Overview of consensus mechanisms

Источник: здесь и далее в статье все рисунки составлены авторами.

Source: Hereinafter in this article all figures were drawn up by the authors.

Consensus	Similar to	Decentralised	Features	Apps	Drawbacks
PoSCS	PoS	No	Reputation System	Supply Chains	Cloud Reliance
Microchain	PoS	Partially	Crypto Sortition	IoT Blockchain	Synchronous Networks
PoEWAL	PoW	Partially	Time-limited PoW	IoT Dapps	Synced Clocks
CBPoW	PoW		Credit System	Industrial IoT	DAG Coordinator

Р и с. 2. Обзор рассматриваемых механизмов консенсуса для IoT-систем

F i g. 2. An overview of the considered consensus mechanisms for IoT-systems

Consensus	Processor Usage	Security	Decentralisation	Storage	TPS	Suitable?
PoW	High	High	High	High	Low	No
PoS	Medium	High	Medium	High	Variable	Partially
PoW + PoS	High	High	High	High	Low	No
PoC	Low	High	High	High	Low	No
PoI	Low	High	High	High	High	Partially
PoSCS	Low	High	Low	Low	Variable	Partially
CBPoW	Low	High	Medium	Low	Medium	Yes
PoEWAL	Low	High	High	High	low	Partially
Microchain	Medium	High	Medium	High	Medium	Yes

Р и с. 3. Применимость механизма консенсуса для IoT-систем в соответствии с предлагаемыми критериями

F i g. 3. Applicability of the consensus mechanism for IoT-systems in accordance with the proposed criteria

Анализ полученных результатов

Проведенный нами анализ механизмов консенсуса позволяет оценить их применимость для IoT-систем в соответствии с предлагаемыми в настоящей работе критериями.

PoW можно сразу исключить из списка подходящих алгоритмов. Он чрезвычайно энергоемкий, процессороемкий и требует специального оборудования. Все это критически не приемлемо для IoT-устройств.

Можно утверждать, что PoS частично пригоден и потенциально может использоваться в IoT. Для этого консенсуса не требуется много энергии и процессорной мощности. Однако PoS все еще имеет проблемы для использования в IoT: TPS может быть недостаточным в зависимости от сценария использования, а монетарная концепция может не подходить для некоторых IoT-приложений. Пропускная способность транзакций варьируется от 90 до более 1100 TPS, как показано на рисунке 1. Производительность PoS во многом зависит от конкретной реализации алгоритма. Поэтому PoS пригоден для IoT, но лишь при определенных условиях, например, если критически важно наличие более децентрализованной сети.

Гибридные механизмы PoW/PoS являются альтернативным решением, если первостепенно разрешить проблемы «атаки 51%» и «ничего не поставлено на карту». Однако присутствие PoW в качестве стартового механизма возвращает те же проблемные моменты, с которыми сталкивается «чистый» PoW. Теоретически PoW-часть алгоритма может перенести на отдельный ASICS, а часть PoS передать IoT-устройствам. Однако на наш взгляд конфигурация предлагаемой системы будет не оправдана, в связи с чем использование такого механизма для IoT не рекомендуется.

CBPoW способен динамически регулировать сложность добычи PoW части и имеет механизм регулирования недобросовестных узлов, делая сложность добычи для них очень высокой, вплоть до того, что добыча становится практически невозможной. CBPoW также способен заменить традиционный блокчейн на DAG, что дает возможность самостоятельно уменьшить размер блокчейна, хранящегося локально на устройстве. Кроме того, этот механизм показывает хорошие результаты (рис. 1) в вопросе пропускной способность (500 TPS). Совокупность характеристик определяют CBPoW как подходящий для IoT, конкретно структура DAG, позволяет уменьшить размер, а также облегченный механизм консенсуса PoW и достаточно высокая пропускная способностью транзакций. За счет указанных характеристик CBPoW был отмечен нами на рисунке 3 как благоприятный для устройств IoT.

PoEWAL также представляется модифицированной версией PoW. Особенностью PoEWAL является то, что процесс майнинга ограничен по времени. Устройства занимаются добычей за короткие промежутки, что снижает энергопотребление и использование аппаратных ресурсов. В PoEWAL делается ставка, что используемое устройство имеет синхронизированные часы, что допустимо для IoT-устройств в беспроводной сети, собирающих различные показатели в разрезе времени. Однако указанный фактор может оказаться неприемлемым для некоторых реализаций, в которых устройства подвержены рассинхронизации. Так у PoEWAL есть два значительных ограничения: зависимость от синхронизированного времени и

низкая пропускная способность. В следствии этого на рисунке 3 мы отметили PoEWAL как частично подходящий для IoT.

PoC – достаточно новый механизм консенсуса, концептуально опирающийся на использование емкости накопителя данных как основы алгоритма. Однако объем устройства хранения на IoT-устройствах ограничен в силу аппаратных особенностей. Таким образов, очевидно, что PoC не пригоден для использования в IoT-системах.

PoI развивает идеи PoS и объединяет их с механизмом «значимости» (важности, value). Чем выше показатель важности узла в соотношении с общим количеством поставленных пользователем токенов, тем выше вероятность того, что узел будет выбран для добычи блока. PoI удовлетворяет большинству критериев, представленных на рисунке 1, что делает его подходящим кандидатом в IoT-системах. Однако достаточная его реализация представлена только в блокчейне NEM [21]. PoI упоминается в различных источниках, например [7], [22-24], где приводится только общее описание работы механизма[5]. Поэтому можно лишь частично рекомендовать PoI для IoT.

PoSCS эксплуатирует механизм bet (ставок), однако вместо финансового стимулирования в основе лежит репетиционная система. Репутация насчитывается на основе того, как пользователь взаимодействует с блокчейном. PoSCS использует облачные хранилища для архивации «истории» блокчейна. За счет этого не требуется хранить все данные непосредственно на IoT-устройствах, что решает проблему низкой емкости хранилища данных на IoT-устройствах. Учитывая результаты работы [17], пропускная способность транзакций PoSCS может быть низкой для некоторых случаев использования IoT, а дополнительная зависимость от облака становится причиной отказаться от использования данного алгоритма в некоторых реализациях умных систем. Поэтому мы считаем PoSCS частично подходящим для некоторых реализаций IoT.

Microchain адаптирует концепции PoS и делает ее более приемлемой для IoT. Узлы оперируют доверительным рейтингом, а не монетарной системой. К недостаткам можно отнести то, что Microchain использует криптографическую функцию VRF для работы алгоритма, что может повлечь высокую нагрузку на процессор устройств по мере роста сети [25]. Microchain совершил некоторые доработки относительно сетевого окружения, по этой причине он стал непригодным для публичных (public) блокчейнов. При этом механизм демонстрирует приемлемую производительность, обеспечивая более 230 TPS.

Характеристики, за счёт которых Microchain можно использовать в сфере IoT:

– реализация, не завязанная на монетарной системе;
– высокий TPS;
– низкое использование процессора в контролируемых частных сетях.

Указанные особенности позволили алгоритм Microchain признать наиболее подходящим по сравнению с другими вышерассмотренными алгоритмами, что отражено на рисунке 3.

Заключение

В настоящей работе были определены факторы существующих механизмов консенсуса, накладывающих в свою очередь дополнительные условия на ресурсограниченные IoT-устройства. Рассмотрены определения критериев для ранжирования механизмов консенсуса таких как: безопасность, скорость, децентрализация и др. Предложено краткое описание концепций механизмов и дано определение их общей схемы работы. Проанализированы такие популярные механизмы, как PoW и PoS, немного специализированных для IoT алгоритмов (CBPoW, Microchain, PoEWAL и PoSCS). Отмечено, что вышеназванные механизмы модифицируют уже существующие механизмы консенсуса PoW и PoS, но устраняют (либо минимизируют) необходимость в энергонеэффективных системах и (или) монетарных системах. В ходе проведенного анализа выявлены преимущества и недостатки каждого механизма консенсуса, а также дана оценка возможности их применения для IoT-систем.

Результаты исследования показывают, что Microchain и CBPoW в достаточной степени подходят для IoT. Microchain пригоден IoT в частных средах, а CBPoW решает вопрос локального хранения блокчейна на устройствах. PoSCS, PoEWAL, PoI (теоретически) и PoS также признаны частично подходящими. Некоторые из них решают проблемы с монетарностью, вычислительными затратами и ограничением хранения данных. Однако они имеют и ряд таких проблем: спорные механизмы синхронизации, недостаточное покрытие вопросов производительности, зависимость от облачной инфраструктуры.

Сложившаяся тенденция исследований консенсус-алгоритмов в производственной и академических средах сосредоточена на разработке механизмов, которые в достаточной степени легковесны для маломощных аппаратных устройств. В перспективе ставится задача об изучении новых подходов к процессу консенсус. В частности, проведение модификации механизмов, которые будут развернуты для достижения конкретных бизнес-задач как в частных, так и в потенциально публичных операционных средах.

References

[1] Singh S., Sharma P.K., Yoon B., Shojafar, M., Cho G.H., Ra I.H. Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustainable Cities and Society.* 2020;63:102364. https://doi.org/10.1016/j.scs.2020.102364

[2] Werner R., Lawrenz S., Rausch A. Blockchain Analysis Tool of a Cryptocurrency. In: Proceedings of the 2020 2nd International Conference on Blockchain Technology (ICBCT '20). New York, NY, USA: Association for Computing Machinery; 2020. p. 80-84. https://doi.org/10.1145/3390566.3391671

[3] Min H. Blockchain technology for enhancing supply chain resilience. *Business Horizons*. 2019;62:35-45. https://doi.org/10.1016/j.bushor.2018.08.012

[5] Top PoI Tokens by Market Capitalization [Электронный ресурс] // CoinMarketCap, 2024. URL: https://coinmarketcap.com/view/poi/ (дата обращения: 20.12.2023).

[4] Dujak D., Sajter D. Blockchain Applications in Supply Chain. In: Kawa A., Maryniak A. (eds.) SMART Supply Network. EcoProduction. Cham: Springer; 2019. p. 21-46. https://doi.org/10.1007/978-3-319-91668-2_2

[5] Sternberg H.S., Hofmann E., Roeck D. The Struggle is Real: Insights from a Supply Chain Blockchain Case. *Journal of Business Logistics.* 2021;42:71-87. https://doi.org/10.1111/jbl.12240

[6] Casado-Vara R., Prieto J., Prieta F.D., Corchado J.M. How blockchain improves the supply chain: Case study alimentary supply chain. *Procedia Computer Science*. 2018;134:393-398. https://doi.org/10.1016/j.procs.2018.07.193

[7] Salimitari M., Chatterjee M., Fallah Y.P. A Survey on Consensus Methods in Blockchain for Resource-constrained IoT networks. *Internet of Things*. 2020;11:100212. https://doi.org/10.1016/j.iot.2020.100212

[8] Conti M., Sandeep Kumar E., Lal C. Ruj S. A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys & Tutorials*. 2018;20(4):3416-3452. https://doi.org/10.1109/COMST.2018.2842460

[9] Kim J.-Y., Lee J., Moon S.-M. Trie-Hashimoto: State Trie-Based Proof-of-Work Mining for Optimizing Blockchain Storage. *IEEE Access*. 2024;12:18315-18329. https://doi.org/10.1109/ACCESS.2024.3360379

[10] Huang J., Kong L., Chen G., Wu M.Y. Towards Secure Industrial IoT: Blockchain System With Credit-Based Consensus Mechanism. *IEEE Transactions on Industrial Informatics*. 2019;15(6):3680-3689. https://doi.org/10.1109/TII.2019.2903342

[11] Andola N., Venkatesan S., Verma S. PoEWAL: A lightweight consensus mechanism for blockchain in IoT. *Pervasive and Mobile Computing*. 2020;69:101291. https://doi.org/10.1016/j.pmcj.2020.101291

[12] Wen Y., Lu F., Liu Y., Cong P., Huang X. Blockchain Consensus Mechanisms and Their Applications in IoT: A Literature Survey. In: Qiu M. (eds.) Algorithms and Architectures for Parallel Processing. ICA3PP 2020. *Lecture Notes in Computer Science*. Vol. 12454. Cham: Springer; 2020. P. 564-579. https://doi.org/10.1007/978-3-030-60248-2_38

[13] Esgin M.F., Kuchta V., Sakzad A., Steinfeld R., Zhang Z., Sun S., Chu S. Practical Post-quantum Few-Time Verifiable Random Function with Applications to Algorand. In: Borisov N., Diaz C. (eds.) Financial Cryptography and Data Security. FC 2021. *Lecture Notes in Computer Science*. Vol. 12675. Berlin, Heidelberg: Springer; 2021. p. 560-578. https://doi.org/10.1007/978-3-662-64331-0_29

[14] Gilad Y., Hemo R., Micali S., Vlachos G., Zeldovich N. Algorand: Scaling Byzantine Agreements for Cryptocurrencies. In: Proceedings of the 26th Symposium on Operating Systems Principles (SOSP '17). New York, NY, USA: Association for Computing Machinery; 2017. p. 51-68. https://doi.org/10.1145/3132747.3132757

[15] Galindo D., Liu J., Ordean M., Wong J.M. Fully Distributed Verifiable Random Functions and their Application to Decentralised Random Beacons. In: 2021 IEEE European Symposium on Security and Privacy (EuroS&P). Vienna, Austria: IEEE Computer Society; 2021. p. 88-102. https://doi.org/10.1109/EuroSP51992.2021.00017

[16] Zhang S., Lee J.H. Analysis of the main consensus protocols of blockchain. *ICT Express*. 2020;6(2):93-97. https://doi.org/10.1016/j.icte.2019.08.001

[17] Tsang Y.P., Choy K.L., Wu C.H., Ho G.T., Lam H.Y. Blockchain-Driven IoT for Food Traceability with an Integrated Consensus Mechanism. *IEEE Access*. 2019;7:129000-129017. https://doi.org/10.1109/ACCESS.2019.2940227

[18] Averin A. Cheskidov P. Review of Existing Consensus Algorithms Blockchain. In: 2019 International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS). Sochi, Russia: IEEE Computer Society; 2019. p. 124-127. https://doi.org/10.1109/ITQMIS.2019.8928323

[19] Xu R., Chen Y., Blasch E., Chen G. Microchain: A Hybrid Consensus Mechanism for Lightweight Distributed Ledger for IoT. *arXiv*:1909.10948. 2019. https://doi.org/10.48550/arXiv.1909.10948

[20] Polge J., Robert J., Traon Y.L. Permissioned blockchain frameworks in the industry: A comparison. *ICT Express.* 2021;7(2):229-233. https://doi.org/10.1016/j.icte.2020.09.002

[21] Zhang P., Schmidt D.C., White J., Dubey A. Chapter Seven – Consensus mechanisms and information security technologies. *Advances in Computers*. 2019;15:181-209. https://doi.org/10.1016/bs.adcom.2019.05.001

[22] Silvano W.F., Marcelino R. Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. *Future Generation Computer Systems.* 2020;112:307-319. https://doi.org/10.1016/j.future.2020.05.047

[23] Li J., Li N., Peng J., Cui H., Wu Z. Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies. *Energy*. 2019;168:160-168. https://doi.org/10.1016/j.energy.2018.11.046

[24] Tirado-Andrés F., Rozas A., Araujo A. A Methodology for Choosing Time Synchronization Strategies for Wireless IoT Networks. *Sensors*. 2019;19(16):3476. https://doi.org/10.3390/s19163476

[25] Auhl Z., Chilamkurti N., Alhadad R., Heyne W. A Comparative Study of Consensus Mechanisms in Blockchain for IoT Networks. *Electronics*. 2022;11(17):2694. https://doi.org/10.3390/electronics11172694

Поступила 20.12.2023; одобрена после рецензирования 03.02.2024; принята к публикации 26.02.2024.
Submitted 20.12.2023; approved after reviewing 03.02.2024; accepted for publication 26.02.2024.

Об авторах:

Мельников Максим Олегович, аспирант кафедры математического моделирования, компьютерных технологий и информационной безопасности Института математики, естествознания и техники, ФГБОУ ВО «Елецкий государственный университет им. И. А. Бунина» (399770, Российская Федерация, Липецкая область, г. Елец, ул. Коммунаров, д. 28-1), **ORCID: https://orcid.org/0000-0003-1921-3033,** melnikov.maxx@yandex.ru

Игонина Елена Викторовна, заведующий кафедрой математики и методики её преподавания Института математики, естествознания и техники, ФГБОУ ВО «Елецкий государственный университет им. И. А. Бунина» (399770, Российская Федерация, Липецкая область, г. Елец, ул. Коммунаров, д. 28-1), кандидат физико-математических наук, доцент, **ORCID: https://orcid.org/0000-0002-7369-6219,** elenaigonina7@mail.ru

Все авторы прочитали и одобрили окончательный вариант рукописи.

About the authors:

Maxim O. Melnikov, Postgraduate student of the Chair of Mathematical Modeling, Computer Technologies and Information Security, Institute of Mathematics, Natural Science and Technology, Bunin Yelets State University (28-1 Kommunarov St., Yelets 399770, Lipetsk region, Russian Federation), **ORCID: https://orcid.org/0000-0003-1921-3033,** melnikov.maxx@yandex.ru

Elena V. Igonina, Associate Professor, Head of the Chair of Mathematics and Methods of its Teaching, Institute of Mathematics, Natural Science and Technology, Bunin Yelets State University (28-1 Kommunarov St., Yelets 399770, Lipetsk region, Russian Federation), Cand. Sci. (Phys.-Math.), Associate Professor, **ORCID: https://orcid.org/0000-0002-7369-6219,** elenaigonina7@mail.ru

All authors have read and approved the final manuscript.