DOI 10.37882/2223–2966.2023.04–2.07

ПОДБОР АЛГОРИТМА КОНСЕНСУСА ДЛЯ ЛОГИСТИЧЕСКОГО БЛОКЧЕЙНА

SELECTION OF THE CONSENSUS ALGORITHM FOR THE LOGISTICS BLOCKCHAIN

B. Goryachkin
I. Solokhov

Summary. The consensus mechanism is the core element of any blockchain network. The blockchain network is formed by numerous nodes that authenticate transactions occurring on the network, and the consensus mechanism allows these nodes to come to an agreement on the transactions that should be added to a new block in the blockchain network. Choosing the right algorithm guarantees the fault tolerance and security of blockchain systems. This article reviews the existing consensus algorithms and selects an algorithm that matches the characteristics of the developed logistics blockchain system.

Keywords: blockchain, consensus algorithms, proof-of-work, proof-of-stake, decentralization.

Горячкин Борис Сергеевич
Кандидат технических наук, Доцент
Московский государственный технический университет им. Н.Э. Баумана
bsgor@mail.ru
Солохов Ильдар Ринатович
Магистрант, Московский государственный технический университет им. Н.Э. Баумана
sir1504@mail.ru

Аннотация. Механизм консенсуса является основным элементом любой сети блокчейн. Сеть блокчейна формируется многочисленными узлами, которые проверяют подлинность транзакций, происходящих в сети, и механизм консенсуса позволяет этим узлам прийти к соглашению в части транзакций, которые следует добавить в новый блок в сети блокчейн. Выбор правильного алгоритма гарантирует отказоустойчивость и безопасность систем блокчейна. В данной статье проведен обзор существующих алгоритмов консенсуса и подобран алгоритм, соответствующий характеристикам разрабатываемой системы логистического блокчейна.

Ключевые слова: блокчейн, алгоритмы консенсуса, proof-of-work, proof-of-stake, децентрализация.

Введение

Блокчейн — это распределенная база данных, состоящая из «цепочки блоков», устройства хранения блоков не подключены к общему серверу, база данных позволяет контролировать достоверность транзакций без надзора каких-либо финансовых регуляторов. Реестр хранится одновременно у всех участников системы и автоматически обновляется при малейшем изменении. Каждый имеет доступ к информации о любой транзакции, когда-либо осуществленной. Пользователи выступают в качестве коллективного нотариуса, который подтверждает истинность информации в базе данных.

Блокчейн является распределенной и децентрализованной базой данных, сформированной участниками, в которой невозможно фальсифицировать данные из-за хронологической записи и публичного подтверждения всеми участниками сети транзакции. Основной и главной особенностью блокчейна является использование алгоритмов математического вычисления, и исключение «человека» и человеческого фактора при принятии решения системой.

Поскольку узлы в сети должны быть уверены в корректности полученных данных, были внедрены специальные алгоритмы — алгоритмы консенсуса. В современных системах алгоритм консенсуса представляет собой математическую задачу, решение на которую можно найти только методом перебора решений к математической функции. Перебирая случайное или псевдослучайное число, меняется значение хеш-функции блока. Сама хеш- функция включает в себя все данные блока, включая хеш предыдущего блока.

Алгоритмы консенсуса

Алгоритм консенсуса должен обладать тремя свойствами, чтобы система продолжала существовать и имела какой-то прогресс в переходе из состояния в состояние:

1. Согласованность — все корректно работающие узлы должны принять одно и то же значение.

2. Корректность — выбранное значение должно быть одним из тех, которое было предложено каким-либо корректно работающим узлом.
3. Конечность — каждый отдельный корректно работающий узел, должен рано или поздно принять финальное значение и подтвердить это.

Теорема Фишера, Линча, Патерсона (FLP) гласит, что не существует асинхронного детерминированного алгоритма принятия консенсуса, который был бы устойчив к выходу из строя одного узла и гарантировал бы все свойства консенсуса. Асинхронизм означает, что нельзя достоверно различить работает ли узел медленно, или долго идет сообщение, или же отказал узел, даже если предположить, что связь является надежной.

1. Proof-of-Work (PoW)

Proof of Work — это первый алгоритм блокчейна, представленный в сети блокчейнов. Алгоритм PoW требует от узлов в сети решения математической задачи для создания следующего блока. Это математическое решение выполняется с помощью хеш-функции. Хэш — это случайная и сложная математическая формула, которая используется для подтверждения транзакций, хранящихся в блоках. Все узлы соревнуются за то, чтобы первыми найти решение методом перебора, что требует огромного количества попыток. Тот, кто первым найдет решение, может иметь право создать новый блок, и после его проверки блок будет добавлен на платформу.

Преимуществом алгоритма Proof of Work является его высокая безопасность и значительная степень децентрализации. Однако, его основным недостатком является большее потребление энергии и ресурсов. Пользователям требуется большая вычислительная мощность, чтобы найти решение сложной математической задачи, связанной с хешированием миллиарда одноразовых номеров или более. Кроме того, для решения этой задачи потребуется некоторое время из-за сложности решения хэш-функции. Поэтому, данный алгоритм не подходит для большой и быстрорастущей сети, требующей огромного количества транзакций в секунду [1].

2. Proof-of-Stake (PoS)

Из-за очевидных недостатков алгоритма PoW, таких как пустая трата вычислительной мощности и низкая эффективность достижения консенсуса, алгоритм PoS был предложен в 2011 году. Алгоритм PoS является алгоритмом доказательства доли. В отличие от узлов алгоритма PoW для получения права учета посредством конкуренции вычислительных мощностей, алгоритм PoS выбирает узел с наибольшей долей в системе в качестве узла учета. Алгоритм PoS выдвигает концепцию токенов. Ставка узла может быть рассчитана на основе количества и времени удерживаемых им токенов. Чем больше токенов удерживает узел и чем дольше он удерживает, тем выше его капитал.

Преимущество алгоритма PoS заключается в том, что ему не нужно проходить сложный процесс «майнинга», а нужно только пройти доказательство доли для получения права учета. Это, в свою очередь, сокращает время блока и время обработки транзакций и значительно экономит время на достижение консенсуса, а эффективность консенсуса значительно повышается. Кроме того, алгоритм PoS также экономит и улучшает потребление вычислительных ресурсов по сравнению с алгоритмом PoW.

Основные недостатки данного алгоритма — это постепенная централизация сети, из-за чего участники с большим количеством средств имеют больше привилегий и подверженность атакам на раннем этапе сети [2] .

3. Delegated Proof-of-Stake (DPoS)

Основная идея алгоритма DPoS, а именно алгоритм делегированного доказательства доли, похожа на репрезентативную избирательную систему. Данный алгоритм только внешне похоже на имя Proof-of-stake, ведь детали реализации двух алгоритмов существенно отличаются друг от друга. В DPoS вместо ставки на монеты для проверки транзакций держатели токенов в ходе голосования выбирают валидаторов транзакций, которые будут формировать блоки. Вес каждого голоса определяется суммой активов голосующего. Держатели монет, в случае сомнений, могут перевыбирать кандидатов. Благодаря этому можно достичь высокой устойчивости сети. Если большая часть исполнителей вышла из строя, то сообщество тут же проголосует за их замену.

Алгоритм DPoS сочетает в себе преимущества алгоритмов PoS и PoW соответственно. Основываясь на механизме принятия нескольких решений с учетом по очереди, скорость связи между узлами в консенсусе DPoS выше, и узлы могут быстро выполнять упаковку блоков, широковещательную рассылку и проверку, а также значительно улучшают пропускную способность системных транзакций. DPoS не зависит от вычислительных ресурсов и соответственно снижает потребление энергии.

Механизм консенсуса DPoS прост и эффективен, поскольку не требует майнинга или полной проверки

узла. Вместо этого он проверяется ограниченным числом узлов-свидетелей. Это также энергосберегающее по сравнению с PoW и PoS. Несмотря на преимущества, предлагаемые данным алгоритмом, он все же не лишен недостатков. Одна из таких неисправностей — достаточная децентрализация никогда не может быть достигнута [3] .

4. Leased Proof-of-Stake (LPoS)

LPoS — еще одна модификация алгоритма Proof-of-Stake. На данный момент он поддерживается только платформой Waves. В рамках этого алгоритма, любой пользователь имеет возможность передавать свой баланс в аренду майнинг-узлам, а за это майнинг-узлы делятся частью прибыли с пользователями. Таким образом, данный алгоритм консенсуса позволяет получить доход от майнинговой деятельности, не ведя самого майнинга.

Преимущества: 1) Меньшее потребление энергии, сделку по аренде можно активировать с помощью телефона. Несколько узлов теперь могут выполнять процесс, для которого требуется несколько узлов с высокой вычислительной мощностью. 2) Более высокая скорость обработки. Системы на основе LPoS являются быстрыми и эффективными, поскольку несколько узлов участвуют в проверке транзакции в данный момент времени [4] .

5. Proof-of-Capacity (PoC)

Proof of Capacity (PoC) — это алгоритм механизма консенсуса, используемый в блокчейнах, который позволяет майнинговым устройствам в сети использовать доступное пространство на жестком диске для определения прав на майнинг и проверки транзакций. Ключевой особенностью PoC является то, что для его работы требуется очень мало энергии по сравнению с другими алгоритмами консенсуса. PoC также зависит от емкости хранилища пользователя для проверки блоков, что делает его более экологичным.

Преимущества: PoC может использовать любые обычные жесткие диски; данный алгоритм более энергоэффективен; нет необходимости в специальном оборудовании или постоянном обновлении жестких дисков; данные майнинга можно легко стереть, а диск можно повторно использовать для любых других целей хранения данных.

Недостатки: вредоносное ПО может влиять на деятельность майнинга; широкое внедрение PoC может начать «гонку вооружений» для производства жестких дисков большей емкости [5].

Сравнительный анализ алгоритмов

Чтобы определить, является ли алгоритм консенсуса подходящим для разрабатываемого блокчейн-приложения, необходимо учитывать следующие факторы:

Безопасность: все узлы должны иметь возможность давать результаты, соответствующие правилам протокола.

Участие: все узлы должны иметь возможность участвовать и вносить свой вклад в изменения, вносимые в базу данных.

Инклюзивный: алгоритм должен гарантировать, что каждый узел участвует в процессе голосования.

Равные возможности: каждый голос, полученный от узла, должен иметь равный вес в алгоритме консенсуса.

Риски, связанные с выбором неправильного протокола:

Выбор плохого алгоритма консенсуса увеличивает уязвимость цепочки. В результате которой возникает сеть, параллельная уже существовавшей. Когда происходит разветвление блокчейна, приложение начинает работать непредсказуемым образом, создавая впереди два или более расходящихся узла.

Низкая производительность: когда рассматривается непригодный алгоритм консенсуса, узел выходит из строя, либо страдает от разделения сети. Это задерживает процесс обмена сообщениями между узлами, что в конечном итоге снижает уровень производительности.

Отказ от консенсуса: в этой ситуации часть узлов не может участвовать ни в одном процессе, и, таким образом, в отсутствие их голосов консенсус не дает точных и желаемых результатов.

Проанализируем существующие алгоритмы консенсуса и сравним их характеристики. Сравнительная характеристика представлена в таблице 1:

Обоснование выбора алгоритма консенсуса для блокчейна

На основе сводной таблицы 1 выберем алгоритмы, которые подходят для реализации логистического блокчейна. Исходя из обзора моделей и их анализа, можно составить список требований к алгоритму. Алгоритм консенсуса должен быть:

Таблица 1. Сравнение алгоритмов консенсуса

Наименование	Децентрализация	Математическая задача	Скорость проведения транзакции [6, 7, 8]
PoW	есть	есть	600 секунд
PoS	есть	есть	60 секунд
DPoS	есть	есть	480 секунд
LPoS	есть	есть	300 секунд
PoC	есть	есть	420 секунд

Таблица 2. Сравнительный анализ алгоритмов после программного тестирования

Наименование	Пропускная способность	Сложность	Масштабируемость	Время добавления блока
PoW	низкая	высокая	низкая	20 секунд
PoS	высокая	высокая	высокая	5 секунд
DPoS	высокая	высокая	высокая	17 секунд

- энергоэффективным;
- с низкой стоимостью проведения транзакций;
- с большой пропускной способностью;
- простым и стойким;
- без майнинга;
- масштабируемым.

В результате можно выделить следующие алгоритмы: PoW, PoS, DPoS.

Для подбора оптимального протестируем с параметрами, максимально приближенными к действующей системе.

Выделим основные характеристики:

- пропускная способность: необходимость выполнения большого количества вычислений требует существенных временных затрат. Алгоритм PoW может выполнять 7–10 транзакций в секунду в то время, как PoS — 2000 транзакций в секунду, DPoS — 5000 транзакций в секунду [9];
- сложность: подразумевается решение некой математической задачи, чем сложнее задача, тем сложнее атака на сеть;
- масштабируемость: способность системы, сети или процесса справляться с увеличением рабочей нагрузки. Данный параметр можно оценить, как совокупность пропускной способности и сложности алгоритмов.
- время добавления блока: данный параметр определялся практическим путем. Был реализован программный код, который реализует три алгоритма.

Вычислим временную характеристику для каждого из приведенных выше алгоритмов.

1) PoW

Время генерации блока для данного алгоритма определяется следующей формулой [10]:

$$T_i = -\frac{1}{\lambda(1-h_{prev})}\log(1-p), \quad (1)$$

где T_i — время генерации блока для i-го аккаунта, сек;

λ — среднее кол-во генерируемых блоков в секунду, сек$^{-1}$;

h_{prev} — коэффициент мощности сети, безразмерная величина;

p — вероятность из равномерного распределения, безразмерная величина.

В данной формуле коэффициент мощности сети — это скорость решения криптографической задачи. Представляет собой сумму вычислительных мощностей предыдущих участников.

Полученное время — 18 секунд.

2) PoS

Время генерации блока для аккаунта i рассчитывается как [11]:

$$T_i = T_{min} + C_1\log(1 - C_2\frac{\log X_i}{b_i A_n}), \quad (2)$$

Таблица 3. Сравнение временных характеристик для различных методов.

Наименование	Формула	Программа
PoW	18 секунд	20 секунд
PoS	5 секунд	5 секунд
DPoS	21 секунда	17 секунд

где T_i — время генерации блока для i-го аккаунта, сек;

T_{min} — 5 секунд, константа, определяющая минимальный временной интервал между блоками;

C_1 — константа, равная 70 и корректирующая форму распределения интервала между блоками, безразмерная величина;

C_2 — константа, равная 5E17 и предназначенная для регулировки сложности, безразмерная величина;

X_i — генерирующая подпись, безразмерная величина;

b_i — доля баланса участника от общего баланса системы,%;

A_n — адаптивный коэффициент, регулирующий среднее время выпуска блока, безразмерная величина.

Генерирующая подпись — это первые 8 байт публичного ключа и хэша текущего блока [11].

Полученное время — 5 секунд.

3) DPoS

На основании формул (1) и (2) составим формулу для алгоритма DPoS. Так как он сочетает в себе принцип работы PoW и PoS, то время генерации блока для аккаунта i рассчитывается как:

$$T_i = C \times \left(\frac{-\log\frac{X_i}{X_{max}}}{b_i \times A_n}\right), \quad (3)$$

где T_i — время генерации блока для i-го аккаунта, сек;

C — константа, равная 70 и корректирующая форму распределения интервала между блоками;

X_i — генерирующая подпись, безразмерная величина;

b_i — доля баланса участника от общего баланса системы,%;

A_n — адаптивный коэффициент, регулирующий среднее время выпуска блока [12] .

Оценим время, полученное в результате расчета и программным методом.

Оценим разницу между значений временных характеристик, полученных формулой и программой. При подсчете значения формулой использовались значения идеальных условий, поэтому в программе оценим влияние вычислительных мощностей компьютера.

В нашем случае на исполняемый код влияет логарифмическая временная сложность.

Для алгоритма PoW получаем погрешность вычислительной мощности равной 11.1, DPoS — 19.05. Так как PoS не использует вычислительных мощностей, то есть не решает математическую задачу, поэтому получаем значение 0.

Таким образом можно составить формулу, для проверки значений, полученных программой и формулой.

$$T_f = T_p \times \left(\frac{1}{1-U}\right), \quad (4)$$

где T_f — время, полученное формулой,
T_p — время, полученное программой,
U — параметр вычислительной мощности.

Получаем значения: PoW — 18 секунд, PoS — 5 секунд, DPoS — 21 секунд.

Для реализации блокчейна необходимо использовать алгоритм с минимальным временем генерации блока. В результате наименьшее время генерации блока у алгоритма Proof-of-Stake.

Заключение

Механизм консенсуса является основным элементом любой сети блокчейн. Выбрав правильный протокол консенсуса, легче гарантировать отказоустойчивость и безопасность систем блокчейна. В данной работе были проанализированы алгоритмы и подобраны те, которые соответствуют параметрам разрабатываемой системы. Конечным результатом являлось анализирование времени получения блоков двумя способами: программой и с помощью формул. Также была проведена оценка разницы значений полученных двумя способами. Сделан вывод о влиянии на результат вычислительных мощностей компьютера и логарифмической сложности для решения математической задачи.

ЛИТЕРАТУРА

1. Mingxiao D. et al. A review on consensus algorithm of blockchain //2017 IEEE international conference on systems, man, and cybernetics (SMC) .— IEEE, 2017.— С. 2567–2572.
2. King S., Nadal S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake //self-published paper, August.— 2012.— Т. 19.— № . 1.
3. Yang F. et al. Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism //IEEE Access.— 2019.— Т. 7.— С. 118541–118555.
4. Chomsiri T., Kongsup K. P coin: high speed cryptocurrency based on random-checkers proof of stake //2018 Joint 10th International Conference on Soft Computing and Intelligent Systems (SCIS) and 19th International Symposium on Advanced Intelligent Systems (ISIS) .— IEEE, 2018.— С. 524–529.
5. Bentov I. et al. Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y //ACM SIGMETRICS Performance Evaluation Review.— 2014.— Т. 42.— № . 3.— С. 34–37.
6. Mingxiao D. et al. A review on consensus algorithm of blockchain //2017 IEEE international conference on systems, man, and cybernetics (SMC) .— IEEE, 2017.— С. 2567–2572.
7. Zhang C., Wu C., Wang X. Overview of Blockchain consensus mechanism //Proceedings of the 2020 2nd International Conference on Big Data Engineering.— 2020.— С. 7–12.
8. Baliga A. Understanding blockchain consensus models //Persistent.— 2017.— Т. 4.— № . 1.— С. 14.
9. Fan X., Chai Q. Roll-DPoS: a randomized delegated proof of stake scheme for scalable blockchain-based internet of things systems //Proceedings of the 15th EAI international conference on mobile and ubiquitous systems: computing, networking and services.— 2018.— С. 482–484.
10. Lasla N. et al. Green-PoW: An energy-efficient blockchain proof-of-work consensus algorithm //Computer Networks.— 2022.— Т. 214.— С. 109118.
11. Waves: сайт.— URL: http://docs.wavesenterprise.com/ru/1.1.2/how-the-platform-works/consensus/PoS.html#proof-of-stake (дата обращения:24.11.2022)
12. Saleh F. Blockchain without waste: Proof-of-stake //The Review of financial studies.— 2021.— Т. 34.— № . 3.— С. 1156–1190.

Журнал «Современная наука: актуальные проблемы теории и практики»

Московский государственный технический университет им. Н.Э. Баумана