Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н. Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н. Э. Баумана)

ФАКУЛЬТЕТ ИУ «Информатика и системы управления»

КАФЕДРА ИУ-7 «Программное обеспечение ЭВМ и информационные технологии»

РАСЧЕТНО-ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

К НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

НА ТЕМУ:

«Классификация известных алгоритмов блокчейн-консенсуса»

Студент **ИУ7-53Б** _____ **Марченко В.**

Руководитель _____ **Исаев А. Л.**

2022 г.

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет имени Н. Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н. Э. Баумана)

УТВЕРЖДАЮ

Заведующий кафедрой ИУ-7
(Индекс)
_____ И. В. Рудаков
(И. О. Фамилия)
«16» сентября 2022 г.

З А Д А Н И Е
на выполнение научно-исследовательской работы

по теме

«Классификация известных алгоритмов блокчейн консенсуса»

Студент группы **ИУ7-53Б**

Марченко Владислав

Направленность НИР

учебная

Источник тематики

НИР кафедры

График выполнения НИР: 25% к 6 нед., 50% к 9 нед., 75% к 12 нед., 100% к 15 нед.

Техническое задание
Провести обзор существующих алгоритмов консенсуса для блокчейн сетей. Сформулировать критерии сравнения алгоритмов консенсуса блокчейна. Классифицировать существующие алгоритмы консенсуса для блокчейн сетей.

Оформление научно-исследовательской работы:
Расчетно-пояснительная записка на **12-20** листах формата А4.
Перечень графического (иллюстративного) материала (чертежи, плакаты, слайды и т. п.)
Презентация на **6-10** слайдах.

Дата выдачи задания «16» сентября 2022 г.

Руководитель НИР _____ **А. Л. Исаев**
(Подпись, дата) (И. О. Фамилия)

Студент _____ **В. Марченко**
(Подпись, дата) (И. О. Фамилия)

РЕФЕРАТ

Отчет 21 с., 4 рис., 3 табл., 11 источн., 1 прил.

БЛОКЧЕЙН, КОНСЕНСУС, АЛГОРИТМЫ КОНСЕНСУСА, PROOF OF WORK, PROOF OF STAKE, PROOF OF IMPORTANCE, PROOF OF CAPACITY, HYBRID CONSENSUS

Объектом исследования является технология блокчейн.

Цель работы: классификация существующих алгоритмов блокчейн-консенсуса.

В результате исследования было проведено сравнение пяти алгоритмов блокчейн-консенсуса по трем критериям.

Область применения результатов — выбор алгоритма консенсуса при создании блокчейна.

Результат работы. Выбор механизма консенсуса зависит от целей, которые преследует разработчик при создании блокчейна. Меньше всего времени на создание нового блока в сети тратит алгоритм Proof of Stake, наиболее стойкими к двойному расходованию являются механизмы Proof of Work, Hybrid Consensus и Proof of Importance, а наибольшее количество транзакций в секунду позволяет проводить Proof of Importance.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

В настоящем отчете о НИР применяют следующие сокращения и обозначения:

HC	Алгоритм блокчейн-консенсуса Hybrid Consensus
NEM	Криптовалюта New Economy Movement
PoC	Алгоритм блокчейн-консенсуса Proof of Capacity
PoI	Алгоритм блокчейн-консенсуса Proof of Importance
PoS	Алгоритм блокчейн-консенсуса Proof of Stake
PoW	Алгоритм блокчейн-консенсуса Proof of Work

ВВЕДЕНИЕ

Блокчейн — это очередная волна перемен, которая уже начала менять структуру деловых, социальных и политических связей, а также способы перемещения средств. С другой стороны, блокчейн — это не просто перемены, а некая сущность, которая никогда не стоит на месте. Более 40 ведущих финансовых учреждений и множество фирм в различных отраслях начали осваивать блокчейн — чтобы снизить транзакционные издержки, ускорить прохождение транзакций, снизить риск мошенничества и устранить посредников. Некоторые фирмы пытаются с его помощью перестроить устаревшие системы и сервисы, чтобы вывести их на следующий уровень, а также предложить новые виды услуг [1, с. 19].

Блокчейн — это структура данных, которая представляет собой упорядоченный связный список блоков транзакций. Каждый блок в цепочке ссылается на предыдущий. Блокчейн часто визуализируют как стек с блоками, наложенными друг на друга. Первый блок в цепи является основанием стека, т. е. его нижним элементом. Визуализация блоков, наложенных друг на друга, приводит к использованию такого термина, как «высота» для обозначения расстояния от первого блока до текущего. Последний добавленный в цепь блок является вершиной стека [2, с. 163].

Блокчейн — это система записей о переносе любой ценности (а не только денег) по принципу «от равного к равному». Это означает, что нет необходимости в посредниках, таких как банки, брокеры или другие службы депонирования, которые служат доверенной третьей стороной [1, с. 21].

Но как всем в сети договориться о единой универсальной «истине» о том, кому что принадлежит, не доверяя никому? Все традиционные платежные системы зависят от модели доверия, в которой есть центральный объект, предоставляющий услуги расчетной палаты, в основном проверяющий и выполняющий все транзакции. Главное изобретение Сатоши Накамото — децентрализованный механизм эмерджентного консенсуса. Эмерджентный, потому что консенсус не достигается явным образом — нет выбора или фиксированного момента, когда достигается консенсус. Напротив, консенсус — это возникающий артефакт асинхронного взаимодействия тысяч независимых узлов, следующих простым правилам [2, с. 181].

Существует множество различных алгоритмов блокчейн-консенсуса.

Они зависят от блокчейн-сетей и их применения. Несмотря на то, что эти алгоритмы различаются по энергопотреблению, безопасности и масштабируемости, все они преследуют одну цель — обеспечить достоверность всех записей.

Цель научно-исследовательской работы: провести обзор существующих алгоритмов консенсуса для блокчейна и классифицировать их по сформулированным критериям.

Задачи научно-исследовательской работы:

1) исследовать технологию блокчейн;
2) исследовать основные механизмы, которые используются в рамках этой технологии;
3) проанализировать известные алгоритмы блокчейн-консенсуса;
4) сформулировать критерии для сравнения алгоритмов блокчейн-консенсуса;
5) сравнить алгоритмы блокчейн-консенсуса по сформулированным критериям.

1 Анализ предметной области

1.1 Технология блокчейн

Как было сказано ранее, блокчейн — это структура данных, которая представляет собой упорядоченный связный список блоков транзакций. Каждый блок в цепи идентифицируется хэшем, сгенерированным с помощью криптографического алгоритма SHA-256 в заголовке блока. Каждый блок ссылается на предыдущий, т. н. родительский блок, через поле «хэш предыдущего блока» в заголовке. Другими словами, каждый блок содержит хэш своего родителя внутри своего собственного заголовка. Последовательность хэшей, связывающих каждый блок с его родителем, создает цепочку, восходящую к первому когда-либо созданному блоку, известному как блок генезиса [2, с. 163].

Хотя у блока есть только один родитель, он может временно иметь несколько дочерних элементов. Каждый из потомков ссылается на тот же блок, что и его родитель, и содержит тот же (родительский) хэш в поле «хэш предыдущего блока». Множественные дочерние блоки возникают во время т. н. «форка» блокчейна — временной ситуации, когда разные блоки создаются почти одновременно разными майнерами. На рисунке 1.1 изображен процесс «форка».

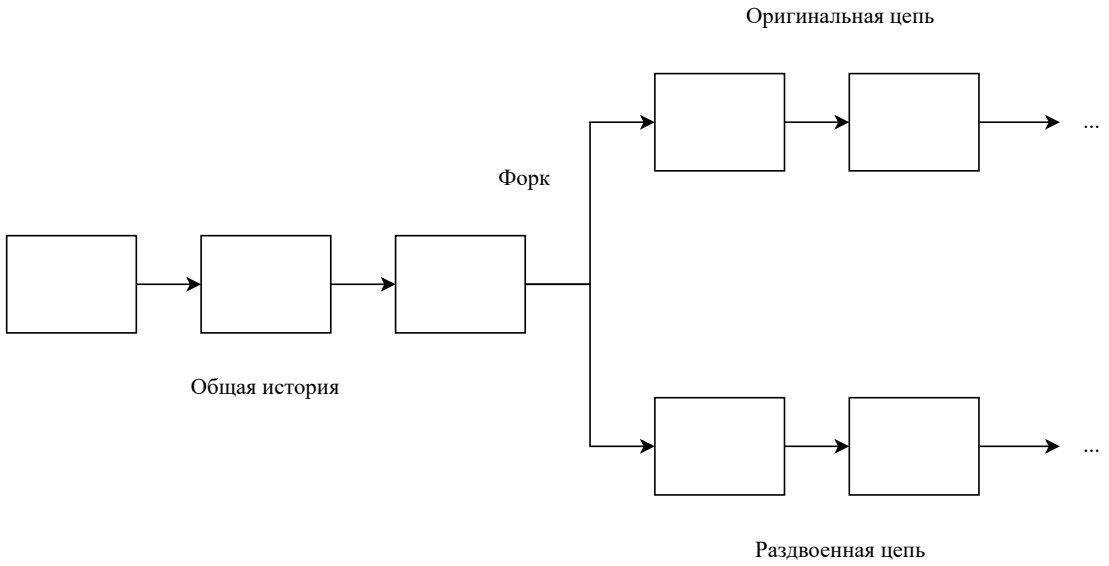

Рисунок 1.1 – Процесс «форка» [3]

В конце концов, только один дочерний блок становится частью блокчейна, и «форк» разрешается. Несмотря на то, что блок может иметь более одного дочернего элемента, каждый блок может иметь только одного родителя. Это связано с тем, что блок имеет единственное поле «хэш предыдущего блока», ссылающееся на его единственного предка [2, с. 163].

Поле «хэш предыдущего блока» находится внутри заголовка блока и тем самым влияет на хэш текущего блока. Дочерний блок изменяется, если меняется родительский. Когда родитель каким-либо образом изменяется, его хэш также изменяется. Измененный хэш родителя требует изменения поля «хэш предыдущего блока» дочернего блока. Это, в свою очередь, приводит к изменению хэша потомка, что требует изменения указателя внучатого элемента, который, в свою очередь, изменяет внука и так далее по цепи. Данный каскадный эффект гарантирует, что после того, как за блоком последовало некоторое количество поколений, его нельзя изменить без принудительного пересчета всех последующих блоков. Поскольку такой пересчет потребовал бы огромных вычислений, существование длинной цепи блоков делает длинную историю блокчейна неизменной, что является ключевой особенностью безопасности криптовалют [2, с. 164].

В блокчейне самые последние несколько блоков могут быть пересмотрены, если происходит пересчет цепи из-за «форка». Но как только происходит углубление в блокчейн за пределы шести блоков, вероятность того, что блоки изменятся, будет уменьшаться. Несколько тысяч созданных в цепи блоков — и цепь — это устоявшаяся история. Она никогда не изменится [2, с. 164]. На рисунке 1.2 изображена общая структура блокчейна.

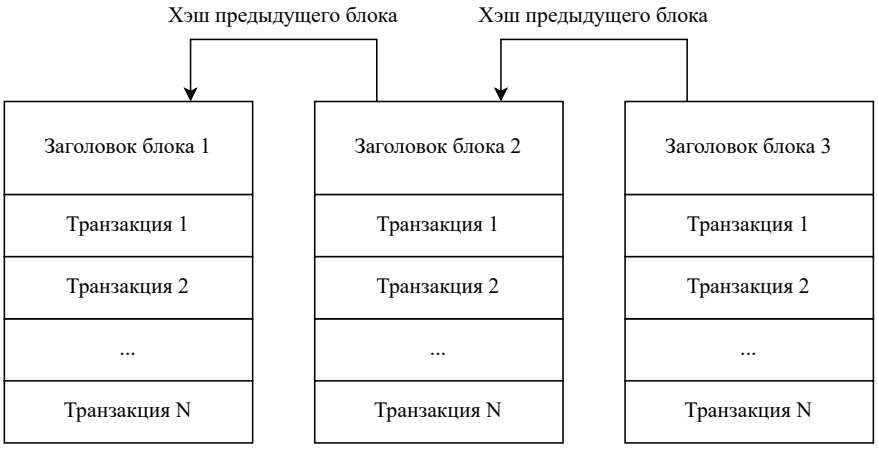

Рисунок 1.2 – Общая структура блокчейна [4]

1.2 Транзакции

Транзакция в информатике — неделимая последовательность операций, которая представляет собой логическую единицу работы с данными. Транзакции обладают следующими свойствами:

1) атомарность;

2) согласованность;

3) изоляция;

4) устойчивость.

В блокчейне транзакции — это структуры данных, которые кодируют передачу информации между участниками блокчейн-сети. Каждая транзакция является общедоступной записью в публичном реестре [2, с. 111].

1.3 Майнинг

Майнинг — это процесс многократного хэширования заголовка блока с изменением одного параметра до тех пор, пока полученный хэш не будет удовлетворять определенным требованиям. Результат хэш-функции нельзя определить заранее, и нельзя создать шаблон, который будет создавать определенное значение хэш-функции. Эта особенность хэш-функций означает, что единственный способ получить результат хэширования, соответствующий конкретной цели — это постоянно изменять случайным образом входные данные до тех пор, пока не появится желаемый результат хэширования [2, с. 192].

1.4 Структура блока

Блок — это контейнерная структура данных, которая агрегирует транзакции для включения их в публичный реестр. Блок состоит из заголовка, содержащего метаданные, за которым следует длинный список транзакций, составляющих основную часть размера блока. Заголовок блока занимает 80 байт, тогда как средний размер транзакции составляет не менее 250 байт, а в среднем блок содержит более 500 транзакций. Таким образом, полный

блок со всеми транзакциями весит в 1000 раз больше заголовка блока [2, с. 164].

В таблице 1.1 описана структура блока — указаны размеры полей в байтах, их названия и описания.

Таблица 1.1 – Структура блока

Размер	**Поле**	**Описание**
4 байта	Размер блока	Размер блока в байтах
80 байт	Заголовок блока	Несколько полей, формирующих заголовок блока
1–9 байт	Счетчик транзакций	Количество проведенных транзакций
Переменный	Транзакции	Транзакции, записанные в этом блоке

1.5 Заголовок блока

Заголовок блока состоит из трех наборов метаданных блока. Во-первых, это ссылка на хэш предыдущего блока, которая связывает текущий блок в цепи с предыдущим. Второй набор метаданных, а именно сложность, отметка времени и одноразовый номер, относятся к майнингу. Третьей частью метаданных является корень дерева Меркла — структуры данных, которая используется для эффективного суммирования всех транзакций в блоке [2, с. 165].

В таблице 1.2 описана структура заголовка блока — указаны размеры полей в байтах, их названия и описания.

Таблица 1.2 – Структура заголовка блока

Размер	**Поле**	**Описание**
4 байта	Версия	Номер версии для отслеживания обновлений программного обеспечения/протокола
32 байта	Хэш предыдущего блока	Ссылка на хэш предыдущего (родительского) блока в цепи
32 байта	Корень дерева Меркла	Хэш корня дерева Меркла транзакций этого блока
4 байта	Отметка времени	Примерное время создания этого блока в секундах (Unix-время)
4 байта	Сложность	Сложность алгоритма Proof of Work для этого блока
4 байта	Одноразовый номер	Счетчик, используемый для алгоритма Proof of Work

1.6 Блокчейн-консенсус

В распределенной системе соглашение является фундаментальной проблемой, и это обычно иллюстрируется задачей византийских генералов [5]. Блокчейн, являясь распределенной системой, основан на алгоритме консенсуса, который обеспечивает согласование состояний определенных данных между распределенными узлами. Алгоритм консенсуса — это основной компонент, который напрямую определяет поведение такой системы и производительность, которую она может достичь. Широкий спектр криптовалют, предназначенных для различных областей применения, определил множество уникальных требований, которые могут быть удовлетворены только с помощью соответствующих механизмов консенсуса. Этот факт вызвал потребность не только в изучении применимости существующих алгоритмов консенсуса в новых условиях, но и в разработке новых алгоритмов консенсуса. В результате появилось несколько алгоритмов консенсуса, каждый из которых обладает интересными свойствами и уникальными возможностями [6].

2 Классификация алгоритмов блокчейн-консенсуса

2.1 Алгоритмы блокчейн-консенсуса

2.1.1 Алгоритм Proof of Work

Proof of Work — это форма криптографического доказательства, в котором одна сторона (доказывающая) доказывает другим (верификаторам), что было затрачено определенное количество конкретных вычислительных усилий [7].

Этот механизм первоначально был предложен в 1993 году для борьбы с нежелательными электронными письмами и для контроля доступа к общим ресурсам [8].

Благодаря системе «Биткоин» алгоритм консенсуса PoW является наиболее известным способом подтверждения транзакций. Основная идея состоит в том, чтобы узлы блокчейна, подтверждающие транзакции, проделывали достаточно сложную вычислительную работу — просчет алгоритма — результат работы которого был бы легко и быстро проверяем другими узлами сети.

Первый узел, который полностью провел все необходимые вычисления, получает вознаграждение от блокчейна. Все узлы борются между собой, наращивая емкость вычислительных ресурсов, чтобы оказаться первым узлом, получившим вознаграждение.

На рисунке 2.1 изображен процесс майнинга в Proof of Work.

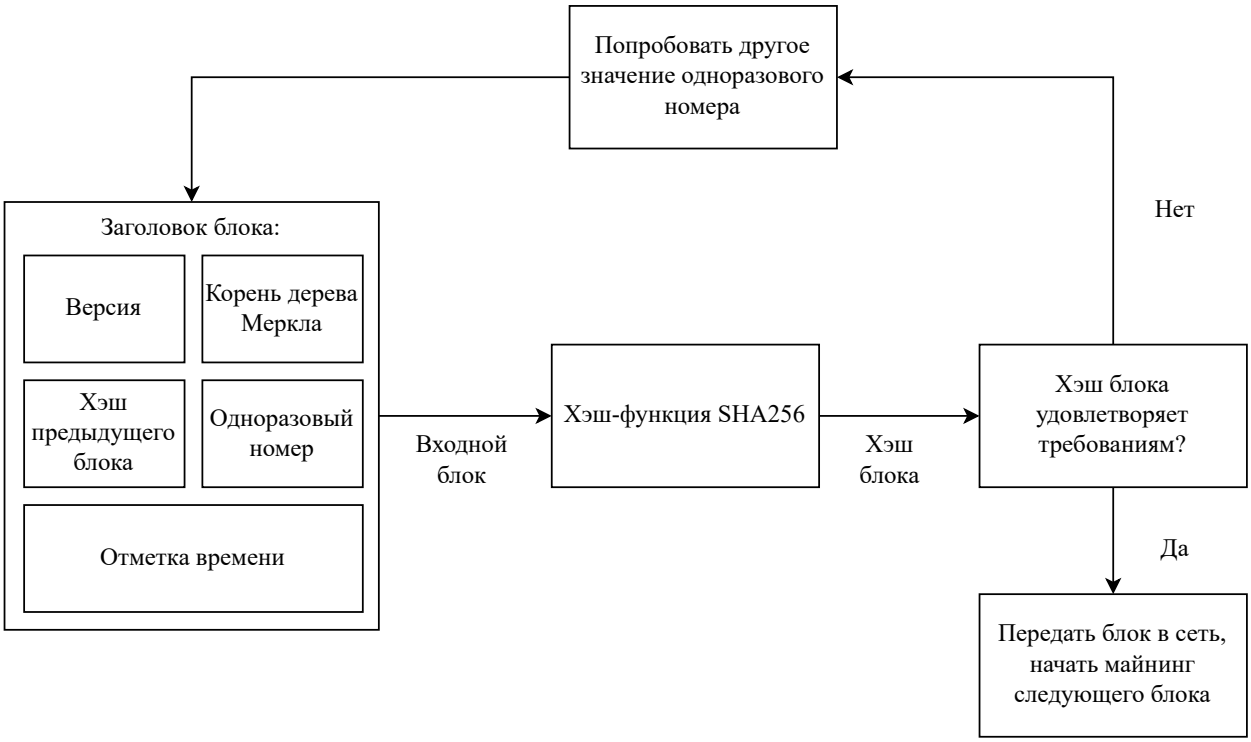

Рисунок 2.1 – Процесс майнинга в Proof of Work [9]

2.1.2 Алгоритм Proof of Stake

Proof of Stake — это предлагаемая альтернатива алгоритму Proof of Work. Вместо процесса конкуренции, как в алгоритме PoW, который зависит от энергопотребления, PoS основан на процессе отбора, учитывающем долю валидаторов (одобренных аккаунтов). Валидаторы в системе PoS являются эквивалентом майнеров в системе PoW [10, с. 361]. В этом алгоритме создателем следующего блока в цепи выбирается узел, который обладает большим балансом — количеством ресурсов, например, монет в криптовалюте. За само создание блока узел вознаграждение не получает. Вознаграждение выплачивается за проведение транзакции.

2.1.3 Алгоритм Hybrid Consensus

Ряд криптовалют используют альтернативные подходы к консенсусу, комбинируя элементы алгоритмов Proof of Work и Proof of Stake. Decred — это криптовалюта, которая увидела недостатки механизмов PoW и PoS и решила создать гибридный механизм консенсуса для решения этих проблем. Майнеры в сети Decred все еще используются для создания блоков, но не могут добавлять блоки непосредственно в блокчейн. Вместо этого

они предлагают свои блоки сети узлов PoS, которые покупают билеты в качестве своей доли. Если узел PoS выбран из этого пула билетов псевдослучайным образом, необходимо проверить блок и добавить его в цепочку блоков Decred. Эти улучшения не позволяют майнерам создавать частные цепочки и добавляют систему контрольных точек, которая предотвращает реорганизацию больших частей блокчейна в случае атаки [9].

На рисунке 2.2 изображен процесс майнинга в Hybrid Consensus.

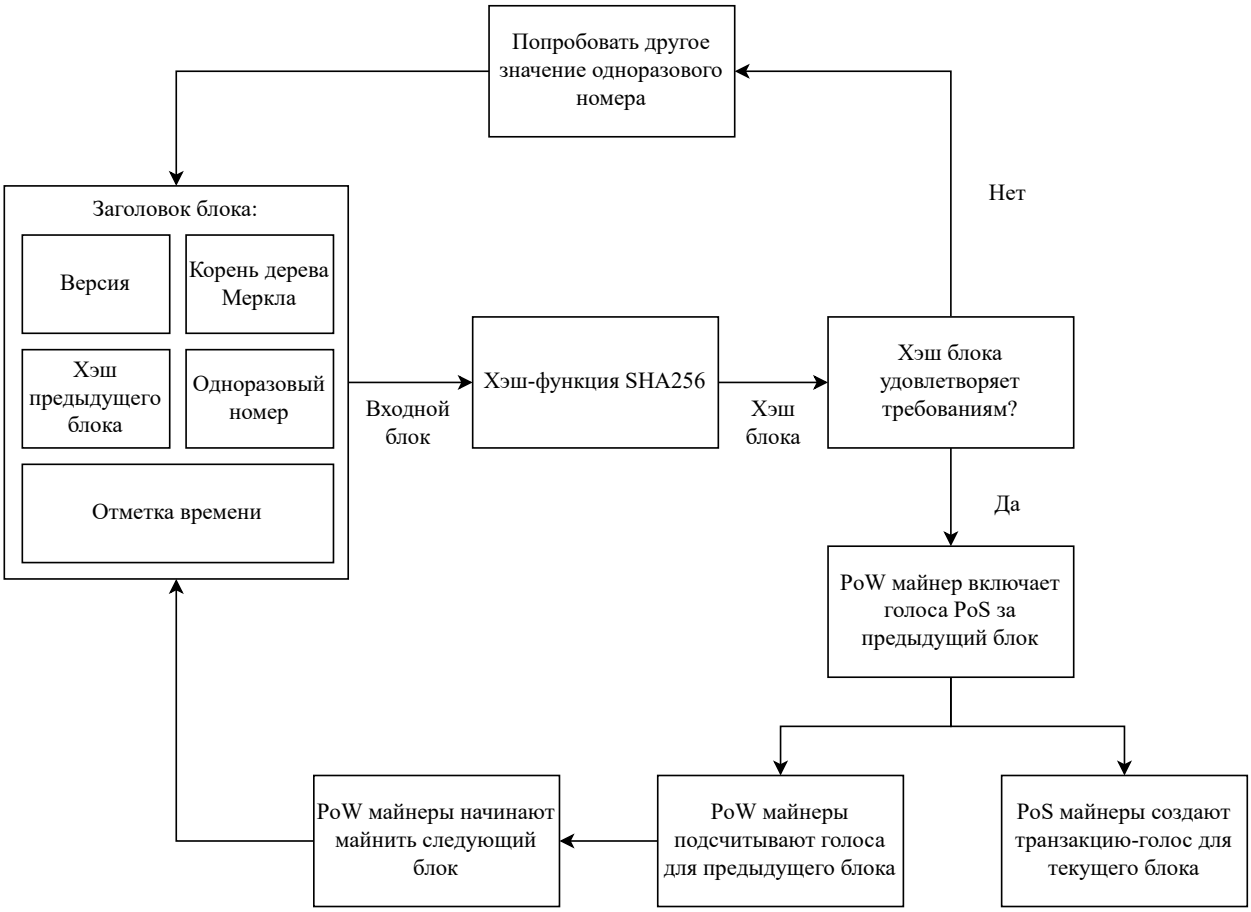

Рисунок 2.2 – Процесс майнинга в Hybrid Consensus [9]

2.1.4 Алгоритм Proof of Capacity

Этот алгоритм иногда именуется Proof of Space. PoC был предложен как альтернатива алгоритму PoW [11].

Идея этой концепции состоит в том, чтобы выделить для майнинга определенный объем дискового пространства, а не вычислительную мощность, как в алгоритме PoW. Таким образом, вместо того, чтобы выполнять большую работу по проверке блоков, как это делается в PoW, работа выполняется заранее с использованием процесса, называемого построением

графика. В ходе этого процесса майнер генерирует файлы, в которых хранится большое количество хэшей, вычисленных заранее с использованием различных одноразовых номеров. Затем эти хэши можно повторно использовать в процессе майнинга [10, с. 362].

2.1.5 Алгоритм Proof of Importance

Proof of Importance — это механизм консенсуса, первоначально предложенный криптовалютой New Economy Movement. Proof of Importance имеет сходство с Proof of Stake, где узлы должны блокировать определенное количество монет. Однако вместо того, чтобы просто поддерживать работу узла, как в случае с PoS, у PoI есть некоторые дополнительные требования для поощрения за использование сети и расчета «важности» кошелька. Чтобы быть выбранными для расчета «важности», кошельки NEM должны хранить не менее 10000 монет в течение определенного периода. Оценка «важности» также может быть увеличена за счет использования сети NEM и отправки транзакций [9].

Были приняты меры против циклических атак, которые включают отправку монет между учетными записями, контролируемыми одним субъектом, для повышения их «важности». NEM добавил механизм, который взвешивает важность учетной записи, отправляющей NEM, и минимальный вес для учетной записи, которая отправляет много монет, но получает большую часть или все свои NEM обратно. Даже если учетная запись попытается совершить циклическую атаку, она получит незначительное увеличение своей оценки важности ($<10\%$), но очень мало выиграет в денежном эквиваленте, поскольку дополнительные деньги, полученные от их более высокой важности, теряются в комиссиях за транзакции [9].

2.2 Критерии оценки алгоритмов блокчейн-консенсуса

Сравнение алгоритмов консенсуса может понадобиться в случае, когда человек хочет создать свой блокчейн. Основываясь на том, чего он хочет достичь в своей сети, разработчик решает, какой блокчейн ему нужен — публичный, частный или консорциумный. Затем необходимо выбрать подходящий механизм блокчейн-консенсуса.

Для сравнения пяти описанных выше алгоритмов блокчейн-консенуса можно выделить следующие критерии: среднее время создания нового блока в цепи (в секундах), стойкость к двойному расходованию (максимально допустимая суммарная мощность в процентах, сконцетрированная в одних руках, при которой блокчейн не подвержен мошенничеству) и количество проводимых транзакций в секунду.

2.3 Сравнение алгоритмов блокчейн-консенсуса

У алгоритмов блокчейн-консенсуса Proof of Stake и Proof of Work среднее время создания нового блока в цепи зависит от блокчейн-сети. У PoW этот показатель изменяется от 12 до 600 с, а у PoS — от 4.5 до 60 с. Среднее время создания нового блока у Hybrid Consensus составляет 300 с, у Proof of Capacity — 240 с, а у Proof of Importance — 60 с [9].

Двойное расходование — это потенциальный недостаток в протоколе криптовалют, в котором один и тот же цифровой токен может быть потрачен более одного раза.

Стойкость к двойному расходованию у алгоритмов PoW, HC и PoI одинаковая и равна 51%. У алгоритма PoC этот показатель составляет 50%. Как и в случае со средним временем создания блока, у алгоритма PoS стойкость к двойному расходованию также зависит от блокчейна. Этот показатель изменяется от 33% до 51% [9].

Количество транзакций в секунду у алгоритма PoW изменяется от 7 до 500. У механизма консенсуса PoS этот показатель в несколько раз выше — от 173 до 1000. HC позволяет проводить транзакции 14 раз в секунду, а PoC — 80 раз в секунду. Наибольшее количество транзакций в секунду, а именно 4000, позволяет проводить алгоритм PoI [9].

Приведенную выше информацию можно записать в таблицу 2.1.

Таблица 2.1 – Сравнение алгоритмов блокчейн-консенсуса

Критерий	**PoW**	**PoS**	**HC**	**PoC**	**PoI**
Среднее время создания блока, с	12–600	4.5–60	300	240	60
Стойкость к двойному расходованию, %	51	33 или 51	51	50	51
Количество транзакций в секунду	7–500	173–1000	14	80	4000

Таким образом, лучшее среднее время создания блока показывает алгоритм Proof of Stake. Наиболее стойкими к двойному расходованию являются Proof of Work, Hybrid Consensus и Proof of Importance. Наибольшее количество транзакций в секунду обеспечивает алгоритм Proof of Importance.

ЗАКЛЮЧЕНИЕ

В ходе выполнения научно-исследовательской работы была достигнута поставленная цель, а также решены все задачи:

1) исследована технология блокчейн;
2) исследованы основные механизмы, которые используются в рамках этой технологии;
3) проанализированы известные алгоритмы блокчейн-консенсуса;
4) сформулированы критерии для сравнения алгоритмов блокчейн-консенсуса;
5) проведено сравнение алгоритмов блокчейн-консенсуса по сформулированным критериям.

Исходя из данных, полученных при сравнении, нельзя определить наихудший и наилучший алгоритмы блокчейн-консенсуса. Одни алгоритмы обладают одними достоинствами, другие — иными. Выбор механизма блокчейн-консенсуса зависит от цели, которую преследует автор при создании блокчейна. К примеру, несмотря на то, что алгоритм Proof of Work позволяет проводить меньше транзакций в секунду, чем алгоритмы Proof of Stake и Proof of Importance, он имеет большую стойкость к двойному расходованию, чем PoS, и имеет меньшее среднее время создания блоков, чем PoI.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Сингхал Б.*, *Дамеджа Г.*, *Панда П. С.* Блокчейн. Руководство для начинающих разработчиков. — СПб.: БХВ-Петербург, 2019.
2. *Antonopoulos A. M.* Mastering Bitcoin. — O'Reilly Media, 2014.
3. *Sheikh H.*, *Azmathullah R. M.*, *Rizwan F.* Proof-of-Work vs Proof-of-Stake: A Comparative Analysis and an Approach to Blockchain Consensus Mechanism // International Journal for Research in Applied Science and Engineering Technology. — 2018. — Т. 6. — С. 788.
4. *Ribera E. G.* Design and Implementation of a Proof-of-Stake Consensus Algorithm for Blockchain // Universitat Politècnica de Catalunya. — 2018. — С. 8.
5. *Lamport L.*, *Shostak R.*, *Pease M.* The Byzantine Generals Problem // ACM Transactions on Programming Languages and Systems. — 1982. — Т. 4. — С. 382—401.
6. Blockchain Consensus Algorithms: A Survey / M. S. Ferdous [и др.] // Cornell University. — 2020. — С. 1.
7. A Cross-Stack Approach Towards Defending Against Cryptojacking / N. Lachtar [и др.] // IEEE Computer Architecture Letters. — 2020. — Т. 19. — С. 126—129.
8. *Dwork C.*, *Naor M.* Pricing via Processing or Combatting Junk Mail // Springer Berlin Heidelberg. — 1993. — С. 139—147.
9. A Comparative Study of Consensus Mechanisms in Blockchain for IoT Networks / Z. Auhl [и др.] // MDPI. — 2022. — С. 15.
10. An Overview of Blockchain Consensus Algorithms: Comparison, Challenges and Future Directions / K. Azbeg [и др.] // Springer. — 2020.
11. Proofs of Space / S. Dziembowski [и др.] // Annual Cryptology Conference. — 2015. — С. 585—605.

ПРИЛОЖЕНИЕ А

(Обязательное)

Презентация