Научно-исследовательская работа

Классификация известных алгоритмов блокчейн-консенсуса

Студент: Марченко Владислав ИУ7-53Б

Научный руководитель: Исаев Андрей Львович

Москва – 2022 г.

Цель и задачи

Цель: провести обзор существующих алгоритмов консенсуса для блокчейна и сравнить их по сформулированным критериям.

Задачи:

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.

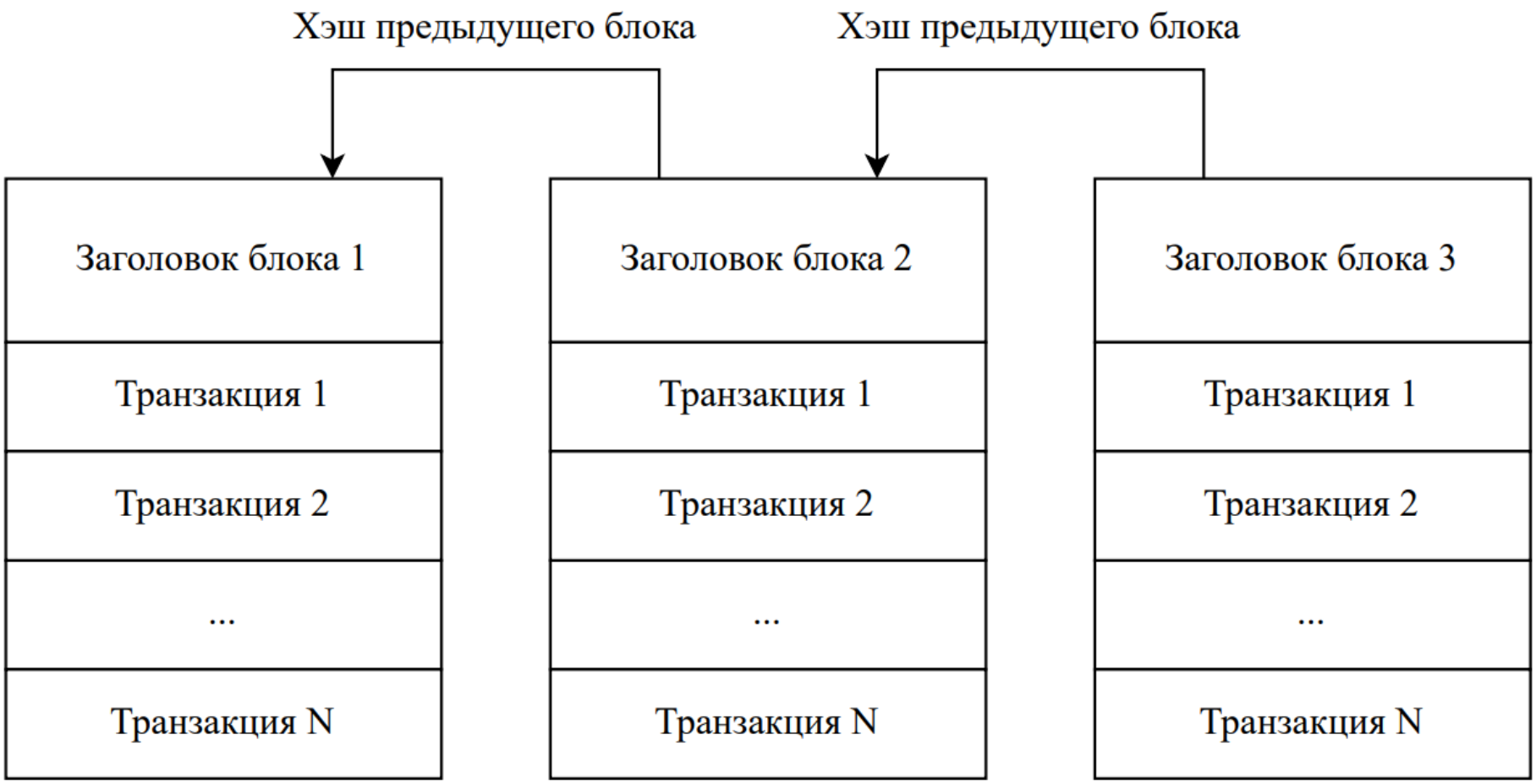
Структура блока

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

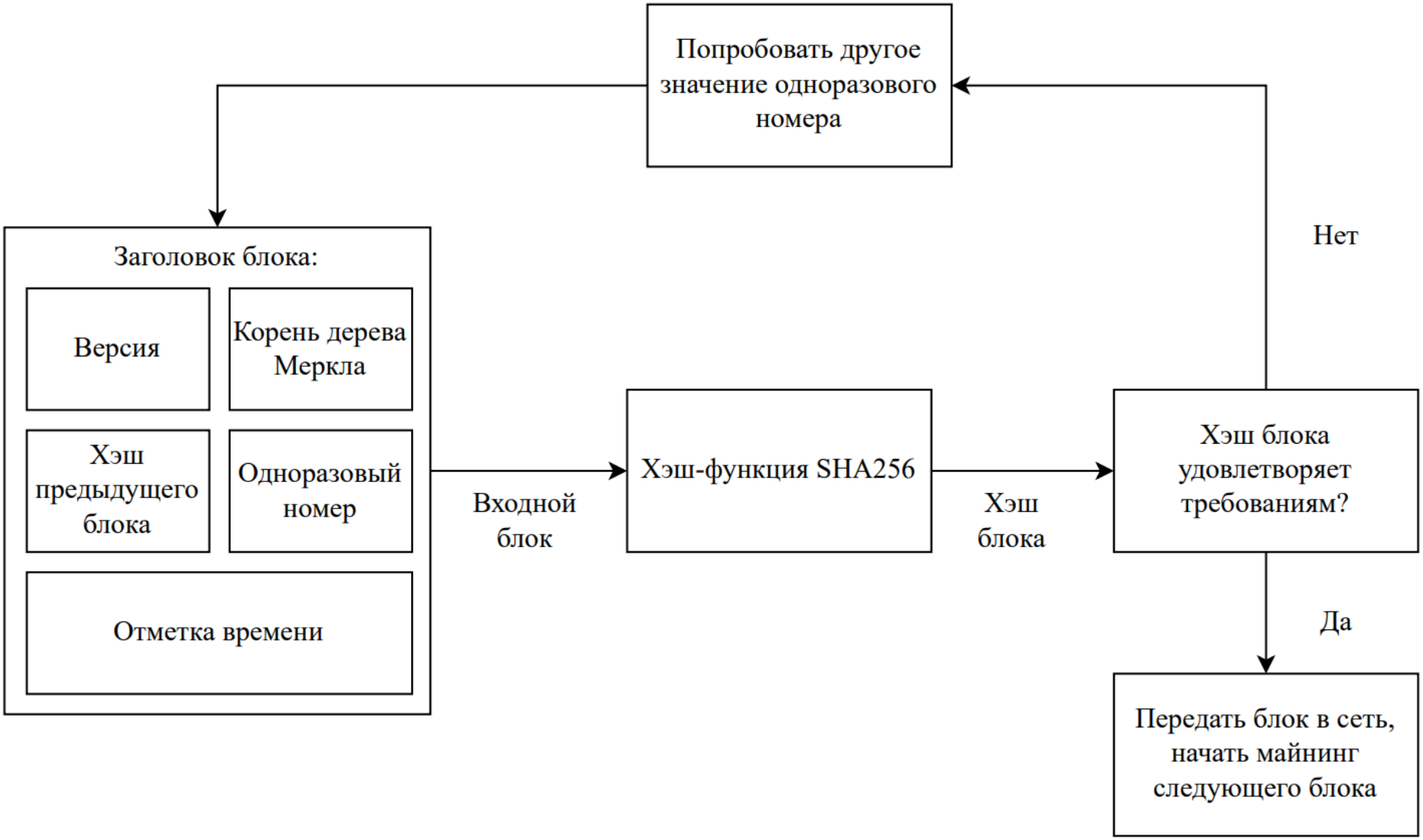
Структура заголовка блока

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

Общая структура блокчейна



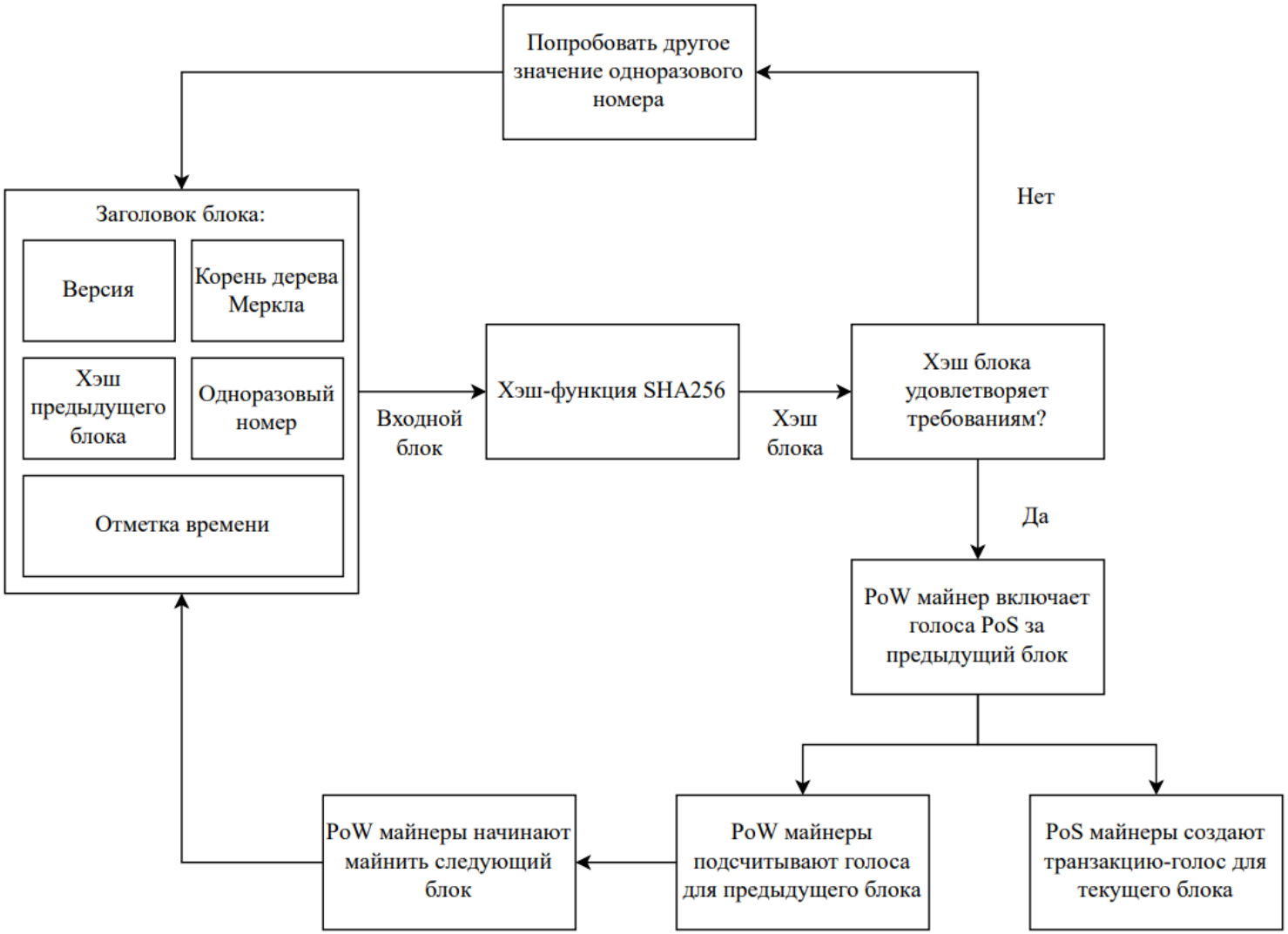
Алгоритм Proof of Work



Алгоритм Proof of Stake

1. Основан на процессе отбора, учитывающем долю валидаторов (одобренных аккаунтов).
2. Создателем следующего блока в цепи выбирается узел, который обладает большим балансом — количеством ресурсов (например, монет в криптовалюте).
3. За создание блока узел вознаграждение не получает.
4. Вознаграждение выплачивается за проведение транзакции.

Алгоритм Hybrid Consensus (PoW/PoS)



Алгоритм Proof of Capacity

1. Для майнинга выделяется определенный объем дискового пространства.
2. Вместо того, чтобы выполнять большую работу по проверке блоков, работа выполняется заранее с использованием процесса, называемого «построением графика».
3. В ходе этого процесса майнер генерирует файлы, в которых хранится большое количество хэшей, вычисленных заранее с использованием различных одноразовых номеров.
4. Эти хэши могут быть повторно использованы в процессе майнинга следующих блоков.

Алгоритм Proof of Importance

1. Узлы должны блокировать определенное количество монет.
2. Вместо простой поддержки работы узла у PoI есть некоторые дополнительные требования для поощрения за использование сети и расчета «важности» кошелька.
3. Кошельки должны иметь на балансе не менее 10000 NEM монет в течение определенного периода.
4. Взвешивание «важности» учетных записей для защиты от атак.

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

Заключение

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

В результате проведения сравнения алгоритмов блокчейн-консенсуса по трем критериям получены следующие результаты.

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