УДК 004.7

Звозникова Г.О.
студент
Пензенский государственный университет
Россия, Пенза

ОБЗОР АЛГОРИТМОВ ТЕХНОЛОГИЙ BLOCKCHAIN

Аннотация: *Одной из самой востребованной на сегодняшний день темой является Blockchain. Данная статья рассматривает наиболее популярные алгоритмы консенсуса. Рассмотрены их преимущества и недостатки. Статья ставит цель изучить наиболее современные решения на рынке блокчейн в области консенсусов.*

Ключевые слова: *консенсус, майнинг, алгоритм, механизм, блокчейн (Blockchain).*

Zvoznikova G. O.
student
Penza state University
Russia, Penza

Annotation: *One of the most popular topics today is Blockchain. This article examines the most popular consensus algorithms. Their advantages and disadvantages are considered. The article aims to study the most modern solutions in the blockchain market in the field of consensuses.*

Key words: *consensus, mining, algorithm, mechanism, blockchain.*

Технология Blockchain представляется собой распределенную базу данных, хранящей список упорядоченных записей. Каждая запись содержащий метку времени и хэш предыдущего блока. Устройства хранения базы данных не подключены к общему серверу, что позволяет повысить безопасность технологии.

Вся технология строится на работе алгоритмов. В современном мире существует множество различных алгоритмов Blockchain. Каждый

алгоритм консенсуса разработан для определенной ситуации, поэтому для каждого алгоритма можно выделить преимущества и недостатки.

На сегодняшний день наиболее популярными алгоритмами консенсуса в системах Blockchain являются Proof-of-Capacity, Proof-of-Elapsed Time, Proof of Activity, Proof of Importance, Proof of Weight.

Алгоритм Proof-of-Elapsed Time

Proof-of-Elapsed Time (доказательство потраченного времени) - механизм предотвращения высокого использования ресурсов и высокого потребления энергии.

Алгоритм состоит из узлов. Каждый участвующий узел в сети ждет произвольно выбранный промежуток времени. Первый завершивший назначенное время ожидания, находит новый блок. Каждый узел в блокчейне генерирует случайное время ожидания и переходит в спящий режим на указанный промежуток времени. Тот, кто «просыпается» первым, - и есть тот участник, у которого самое короткое время ожидания. Он «просыпается» и включает новый блок в цепочку, передавая необходимую информацию всей одноранговой сети. Механизм действий повторяется. Таким образом, чем меньше времени было потрачено на «просыпание», тем больше узлов будет обработано.

Алгоритм Proof of Activity

Proof of Activity (доказательство деятельности) – смешанный механизм, объединивший алгоритмы Proof-of-Work (POW) и Proof-Of-Stak (POS), для увеличения уровня защиты от потенциально возможных атак.

Процесс майнинга начинается как стандартный процесс POW с участием различных майнеров, пытающихся опередить друг друга в нахождении решения нового блока с помощью более высокой вычислительной мощности. При обнаружении нового блока система

переключается на POS с новым найденным блоком, содержащим только заголовок и адрес вознаграждения майнера.

Алгоритм Proof of Importance

Proof of Importance (доказательством важности) - механизм, использующейся для определения участников сети (узлы) имеющие право добавлять блок в блокчейн. Этот процесс известен как сбор блоков. В обмен на сбор блоков, узлы могут взимать комиссию за транзакции в этом блоке. Учетные записи с более высоким показателем важности будут иметь более высокую вероятность быть выбранным для сбора блоков.

Proof of Importance учитывает количество средств и активность пользователя в блокчейн сети. Такой подход вовлекает пользователей не просто держать средства у себя на счету, но и активно использовать их.

Алгоритм Proof of Capacity

Proof of Capacity (подтверждение емкости) - механизм согласованности используется в блокчейне и позволяет майнинг оборудованию использовать в сети доступное пространство на жестком диске для определения прав на майнинг вместо использования вычислительной мощности устройства.

Каждый майнер вычисляет достаточно большой объем данных, который записывается на дисковую подсистему узла. Для каждого нового блока в блокчейне, майнер читает небольшой набор данных от своего общего сохраненного объема и возвращает результат (дедлайн), как прошедшее время в секундах с момента создания последнего блока, после которого майнер сможет создать новый блок. Майнер, получивший минимальное время дедлайна, подписывает блок и получает вознаграждение за транзакции.

Таким образом вычислительные ресурсы необходимые майнеру для этой работы ограничены временем, которое необходимо для чтения

файлов из дисковой подсистемы. Этот фактор позволяет производить майнинг с достаточно высокой энергоэффективностью. Майнеры соревнуются между собой за размеры сохранных данных.

Алгоритм Proof of Weight

Proof of Weight (доказательство веса) - механизм консенсусного алгоритма определяет вес пользователя в зависимости от количества его монет". Чем больше монет - тем лучше. Сильной стороной алгоритма является высокая масштабируемость и энергоэффективность.

Алгоритм гарантирует, что большинство пользователей согласится с принятым решением. Однако большим минусом данного алгоритма является система получения вознаграждения за блок - она довольно сложная.

Сравнение алгоритмов Blockchain

В таблице 1 представлено сравнение выше описанных алгоритмов.

Таблица 1 – Сравнение алгоритмов Blockchain

	Proof-of-Capacity	Proof-of-Elapsed Time	Proof of Activity	Proof of Importance	Proof of Weight
Использование пространства на жестком диске	Да	Нет	Нет	Нет	Нет
Требуется специальное оборудование	Нет	Да	Да	Да	Да
Вычислительные ресурсы ограничены временем	Да	Да	Нет	Нет	Нет
Затрачивание большого количества времени	Да	Да	Да	Да	Да
Высокая устойчивость к атакам	Да	Да	Да	Да	Да
Высокая вычислительная мощность	Нет	Нет	Да	Да	Да
Преимущество перед большим количество валюты на кошельке	Нет	Нет	Нет	Да	Да
Возможность фиктивных транзакций	Нет	Нет	Нет	Да	Нет

По таблице 1 можно сделать вывод, что каждый алгоритм имеет свои преимущества и недостатки. Одним механизмам нужны высокая вычислительная мощность и специальное оборудование, другим большое количество времени для вычисления, но работа каждого консенсуса затрачивает большое количество времени.

Использованные источники:

1. Франкелфилд Д. Proff of Elapsed Time. [Электронный ресурс] URL: https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp / (дата обращения 26.05.2020)

2. Григорчук К. Обзор 9 алгоритмов блокчейн консенсуса. [Электронный ресурс] URL: https://hiveos.ru/forum/viewtopic.php?t=105/ (дата обращения 26.05.2020)

3. Slepak, Greg & Petrova, Anya. The DCS Theorem. /Текст : непосредственный/ — URL: https://www.researchgate.net/publication/322517870_The_DCS_Theorem/ (дата обращения: 26.05.2020).