АЛГОРИТМЫ КОНСЕНСУСА В БЛОКЧЕЙН СЕТЯХ

Яковчик Н.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Борискевич И.А. – к.т.н.,доцент

В работе проведен сравнительный анализ алгоритмов консенсуса применяемых в блокчейн сетях.

Консенсус – это достижение согласия по некоторому вопросу. Алгоритм консенсуса может определяться как механизм, с помощью которого блокчейн сеть достигает консенсуса. Публичные (децентрализованные) блокчейн сети построены как распределенные системы, и поскольку они не полагаются на центральные органы, распределенные узлы должны согласовывать валидацию транзакции. Алгоритм консенсуса в блокчейн сети [1] представляет собой набор определенных математических правил и функций, которые позволяют достичь соглашения между всеми участниками, т.е. позволяют выбрать того, кто может добавить новый блок транзакций в цепочку и, соответственно, обеспечить работоспособность сети. В настоящее время существует несколько различных методов достижения консенсуса.

PoW (Proof of Work) – является наиболее известным способом подтверждения транзакций. Чтобы участвовать в проверке транзакции, участникам необходимо публично доказать проведенную работу. Данный алгоритм решает сложную задачу по нахождению хэша (hash) [2], который соответствует определенным правилам. Первый, кто нашел правильную комбинацию, получает возможность добавить блок в цепочку. Основным недостатком является потребление большого количества электроэнергии всеми участниками сети, в которой применяется данный алгоритм.

PoS (Proof of Stake) – в данном алгоритме вероятность того, что участник добавит следующий блок транзакций в цепочку, определяется количеством монет участника. При этом каждый сетевой узел связан с определенным адресом, и чем больше монет принадлежит этому адресу, тем больше вероятность того, что этот узел сети намайнит следующий блок [3]. Злоумышленнику, который хочет совершить мошенническую транзакцию, потребуется владеть более 50% монет для надежной обработки нужных транзакций; покупка такого количества монет спровоцирует рост цен на них и сделает такую попытку чрезмерно дорогой.

PoET (Proof of Elapsed Time) – это механизм, который предотвращает использование больших вычислительных ресурсов и высокое потребление энергии. Концепция была изобретена в начале 2016 года компанией Intel. Каждый узел в блокчейне генерирует случайное время ожидания и переходит в спящий режим на указанный промежуток времени. Тот, кто выходит из спящего режима первым, – и есть тот участник, у которого самое короткое время ожидания. При выходе из спящего режима он включает новый блок в цепочку, передавая необходимую информацию всей одноранговой сети. Затем повторяется тот же процесс для обнаружения следующего блока.

PoC (Proof of Capacity) – этот алгоритм позволяет майнинг оборудованию использовать в сети доступное пространство на жестком диске для определения прав на майнинг вместо использования вычислительной мощности устройства.

PoB (Proof of Burn) – работает по принципу разрешения майнерам сжигать или уничтожать токены виртуальной валюты, что дает им право писать блоки пропорционально сгоревшим монетам. Майнеры должны предоставить доказательства того, что они сожгли несколько монет, то есть отправили их на проверяемый ненадежный адрес. Этот подход не потребляет никаких ресурсов.

PoI (Proof of Importance) – значимость каждого пользователя в сети определяется как количество средств, имеющихся у него на балансе, и количество проведенных транзакций с и на его кошелек. В отличие от более привычного PoS, который учитывает только баланс имеющихся средств у пользователя, PoI учитывает как количество средств, так и активность пользователя в блокчейн сети.

Самым распространенным алгоритмом консенсуса в настоящее время является PoW, который применяется в сети Bitcoin. При этом для майнинга требуются большие вычислительные мощности, что приводит к значительному потреблению электроэнергии [4]. Использование описанных выше механизмов консенсуса позволит уменьшить вычислительные затраты по сравнению с PoW.

Список использованных источников:

1. ЛелуЛ. Блокчейн от А до Я. Все о технологии десятилетия / ЛелуЛ. – Москва : Эксмо, 2018 – 256с.

2. Forklog: Что такое Proof-of-Work и Proof-of-Stake? [Электронный ресурс]. – Режим доступа: https://forklog.com/chto-takoe-proof-of-work-i-proof-of-stake/. – Дата доступа: 24.03.2020.

3. Medium: Какие алгоритмы консенсуса применяются в блокчейне [Электронный ресурс]. – Режим доступа: https://link.medium.com/WZRTTxQse5/. – Дата доступа: 25.03.2020.

4. 3DNews Daily Digital Digest: На майнинг биткоинов уходит больше электроэнергии, чем потребляет вся Швейцария. [Электронный ресурс]. – Режим доступа: https://3dnews.ru/990234/. – Дата доступа: 24.03.2020.