LCPoA

LCPoA (Limited Confidence Proof of Activity, рус. Доказательство активности с ограниченным доверием) - гибридный алгоритм консенсуса сети блокчейн, состоящий из двух технических элементов:

1. Proof of Activity - принцип, основанный на решении задачи, схожей с задачей принципа Proof of Work, но со значительно сниженной сложностью, благодаря которому решение задачи занимает от долей секунды до нескольких минут
2. Limited Confidence(“Ограничение доверия”) - система автоматического создания “контрольных точек” в блокчейн сети

На текущий момент алгоритм используется только в сети IZZZIO, и имеет ряд преимуществ и недостатков.

Limited Confidence (LC)

Limited Confidence (рус. Ограниченное доверие) - механизм создания контрольных точек в сети, ограничивающий возможность перезаписи блоков сети блокчейн дальше заданного лимита от последнего блока. Например:

Ситуация 1

- В настройках сети примера число **LC** задано как 10
- **Клиент1** - содержит цепочку блоков от 0 до блока 30
- **Клиент2** - содержит цепочку блоков от 0 до 34, при этом у текущего клиента, блок 29 отличается от схожего блока **Клиента1**

В такой ситуации **Клиент1** скачает кусок цепи **Клиента2** от блока 29 до блока 34, т.е. блок 29 будет заменен, и цепочки обоих клиентов станут одинаковыми.

Ситуация 2

- В настройках сети примера число **LC** задано как 10
- **Клиент** - содержит цепочку блоков от 0 до блока 30
- **Атакующий** - пересоздал цепочку блоков от 1 до 31, заменив все транзакции в сети

В такой ситуации **Атакующий** предложит
синхронизировать цепочку от 1 до 31 блока, однако минимальный блок, с которого можно синхронизировать: **31 - 10 = 21**
Синхронизация с цепью атакующего в этом случае выполнена не будет.

Меньшее число LC снижает шанс перезаписи цепочки, бОльшее число снижает шанс появления несинхронизируемых (тупиковых) цепочек.

Proof of Activity

В качестве алгоритма генерации блоков используется модификация Proof of Work с пониженной сложностью. Особенность заключается в использовании в качестве nonce - Unix timestamp, а также в дополнительных проверках и ограничениях:

- В качестве общего времени используется пояс GTM+0
- В блок необходимо записывать информацию о времени старта генерации блока
- В timestamp блока записывается nonce блока

Проверяются параметры:

- Совпадение хеша блока с фильтром разрешенных хешей
- Время старта генерации блока не больше текущего времени сети, и не больше timestamp блока
- timestamp не больше текущего времени сети, и не меньше начала времени генерации блока
- timestamp и время старта генерации блока не менее timestamp предыдущего блока

При этом разрешается делать допуск по каждой проверке не более 60 секунд.

Также возможно использование классического PoW или других алгоритмов совместно с механизмом LC.

Преимущества

- Средняя скорость работы на устройствах разного класса - 1 блок в 5 секунд
- Ограничение максимальной скорости подбора блока для всех устройств - 1000 хешей в секунду, что делает использование майнеров бессмысленным
- Генерация блока может легко выполняться устройством любой мощности
- Полностью децентрализованный алгоритм, для генерации нового блока необходима только информация о последнем блоке сети
- Не требует существования токенов и вознаграждения в сети для работы

Недостатки

- При очень низкой активности сети, возможна атака на слишком большое число **LC.** Альтернативный вариант защиты - сменить работу механизма Limited

Confidence на проверку не количества блоков, а времени, прошедшего с момента добавления блока
- При работе с маленьким порогом **LC**, шанс появления большого количества тупиковых цепочек
- Ограничение генерации в 1000 блоков в секунду
- Необходимость синхронизации с мировым временем

Безопасность

Атака 51%

Базово, без использования защиты со стороны механизма Limited Confidence, описанный вариант Proof of Activity сам по себе сильно уязвим к атаке 51%. С использованием ограничения доверия - атака 51% возможна только на очень малом количестве блоков, что делает ее бессмысленной в большинстве случаев.

Свободная запись в цепочку блоков

Для защиты сети от спама блоками, **необходимо использовать дополнительные методы защиты**, например:
- Повышение сложности генерации блока алгоритмом PoA
- Комиссия за запись блока(транзакцию)
- Ограничение записи большого количества блоков от одного участника