ПРОТОКОЛ ZELDHASH

Охотьтесь за редчайшими транзакциями Bitcoin и зарабатывайте ZELD.

Автор: Ouziel Slama

1 Мотивация

- Ради азарта охоты. Каждая транзакция становится возможностью обнаружить что-то редкое — цифровое сокровище, скрытое на виду в блокчейне.
- Эти паттерны ведущих нулей не просто редки — они также могут улучшить сжатие, потенциально оптимизируя хранение и эффективность обработки блокчейна.
- Любой может зарабатывать ZELD, охотясь за редкими транзакциями — без единственного победителя на блок, как в майнинге блоков Bitcoin. Охота открыта для всех.
- В случае успеха токены ZELD могут в конечном итоге возмещать комиссии за транзакции — вознаграждая охотников, которые находят редчайшие находки!

2 Майнинг ZELD

Чтобы майнить ZELD, вы должны транслировать транзакцию Bitcoin, txid которой начинается как минимум с 6 нулей. Награда рассчитывается на основе того, как ваша транзакция сравнивается с лучшей транзакцией в блоке:

- В данном блоке транзакции, начинающиеся с наибольшего количества нулей, зарабатывают 4096 ZELD
- Транзакции с одним нулём меньше, чем лучшие транзакции, зарабатывают 4096/16 или 256 ZELD
- Транзакции с двумя нулями меньше зарабатывают 4096 / 16 / 16 или 16 ZELD
- и т.д.

Поэтому используется следующая формула:

```
reward = 4096 / 16 ^ (max_zero_count - zero_count)
```

Где `max_zero_count` равно количеству нулей, которыми начинается лучшая транзакция, а `zero_count` — количество нулей, которыми начинается транзакция, для которой мы рассчитываем награду.

Примечание: Coinbase-транзакции не имеют права на награды ZELD.

3 Распределение ZELD

ZELD, заработанные транзакцией, начинающейся с 6 или более нулей, распределяются по UTXO. Распределение осуществляется следующим образом:

- Если есть один не-OP_RETURN UTXO, он получает всю награду.

- Если есть два или более не-OP_RETURN UTXO, награда распределяется между всеми UTXO, кроме последнего, пропорционально стоимости каждого UTXO
- Поскольку вычисления производятся только с целыми числами, возможный остаток от деления распределяется на первый не-OP_RETURN UTXO.

Например, если транзакция, зарабатывающая 256 ZELD, содержит 4 выхода с 500, 500, 500 и 2000 сатоши соответственно, первый выход получает 86 ZELD награды, второй и третий — по 85 ZELD.

4 Перемещение ZELD

Когда UTXO с прикреплёнными ZELD тратятся, ZELD распределяются на новые UTXO в транзакции. Существует два метода распределения ZELD при их перемещении:

4.1 Метод 1: Автоматическое пропорциональное распределение

По умолчанию распределение выполняется точно так же, как и награды — пропорционально на основе Bitcoin-стоимости выходных UTXO, исключая последний выход, если их несколько.

4.2 Метод 2: Пользовательское распределение через OP_RETURN

Вы можете точно указать, как должны распределяться ZELD, включив в вашу транзакцию выход OP_RETURN с данными пользовательского распределения. Это позволяет точно контролировать переводы ZELD.

4.2.1 Формат OP_RETURN:

- Скрипт OP_RETURN должен содержать данные, начинающиеся с 4-байтового префикса “ZELD”
- После префикса данные должны быть закодированы в формате CBOR
- Данные CBOR должны представлять вектор беззнаковых 64-битных целых чисел (Vec)
- Каждое целое число указывает, сколько ZELD отправить на соответствующий выходной UTXO

4.2.2 Правила распределения:

- Количество значений в массиве распределения автоматически корректируется для соответствия количеству не-OP_RETURN выходов
- Если массив слишком длинный, лишние значения удаляются
- Если массив слишком короткий, добавляются нули
- Общая сумма значений распределения не может превышать общее количество тратящихся ZELD
- Если сумма меньше общего количества, разница добавляется к первому выходу
- Если сумма превышает общее количество, транзакция возвращается к пропорциональному распределению
- Награды ZELD от нового майнинга всегда распределяются пропорционально, а затем объединяются с пользовательским распределением

4.2.3 Пример:

Если у вас есть 1000 ZELD для распределения по 3 выходам, и вы хотите отправить 600 на первый, 300 на второй и 100 на третий, ваш OP_RETURN будет содержать “ZELD”, за которым следует CBOR-кодировка [600, 300, 100].

Примечания:

- Если допустимое распределение OP_RETURN не найдено, транзакция автоматически использует метод пропорционального распределения.
- Если транзакция содержит только один выход OP_RETURN, любые ZELD, прикреплённые к входам транзакции, **и любые вновь заработанные награды** навсегда сжигаются, потому что нет расходуемых выходов для их получения.
- При наличии нескольких выходов OP_RETURN для распределения учитывается только тот, который появляется последним в транзакции и несёт действительную полезную нагрузку `ZELD`+CBOR.