GIAO THỨC ZELDHASH

Săn lùng các giao dịch Bitcoin hiếm nhất và kiếm ZELD.

Tác giả: Ouziel Slama

1 Động lực

- Vì cảm giác hồi hộp của cuộc săn. Mỗi giao dịch trở thành cơ hội để khám phá điều gì đó hiếm có — một kho báu kỹ thuật số ẩn ngay trước mắt trên blockchain.
- Những mẫu số không đứng đầu này không chỉ hiếm — chúng còn có thể tăng cường nén, có khả năng tối ưu hóa việc lưu trữ và hiệu suất xử lý blockchain.
- Bất kỳ ai cũng có thể kiếm ZELD bằng cách săn các giao dịch hiếm — không phải một người chiến thắng duy nhất mỗi khối như trong đào khối Bitcoin. Cuộc săn mở ra cho tất cả.
- Nếu thành công, token ZELD cuối cùng có thể hoàn trả phí giao dịch — thưởng cho những thợ săn khám phá những phát hiện hiếm nhất!

2 Đào ZELD

Để đào ZELD, bạn phải phát sóng một giao dịch Bitcoin có txid bắt đầu bằng ít nhất 6 số không. Phần thưởng được tính dựa trên việc giao dịch của bạn so sánh với giao dịch tốt nhất trong khối như thế nào:

- Trong một khối nhất định, các giao dịch bắt đầu bằng nhiều số không nhất kiếm được 4096 ZELD
- Các giao dịch có ít hơn một số không so với giao dịch tốt nhất kiếm được 4096/16 hoặc 256 ZELD
- Các giao dịch có ít hơn hai số không kiếm được 4096 / 16 / 16 hoặc 16 ZELD
- v.v.

Do đó, công thức được sử dụng như sau:

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

Với `max_zero_count` bằng số lượng số không bắt đầu giao dịch tốt nhất và `zero_count` là số lượng số không bắt đầu giao dịch mà chúng ta tính phần thưởng.

Lưu ý: Các giao dịch Coinbase không đủ điều kiện nhận phần thưởng ZELD.

3 Phân phối ZELD

ZELD kiếm được với một giao dịch bắt đầu bằng 6 số không trở lên được phân phối cho các UTXO. Việc phân phối được thực hiện như sau:

- Nếu chỉ có một UTXO không phải OP_RETURN, nó nhận toàn bộ phần thưởng.
- Nếu có hai hoặc nhiều UTXO không phải OP_RETURN, phần thưởng được phân phối cho tất cả các UTXO, ngoại trừ cái cuối cùng, theo tỷ lệ giá trị của mỗi UTXO
- Vì các phép tính chỉ được thực hiện với số nguyên, phần dư có thể có của phép chia được phân phối cho UTXO không phải OP_RETURN đầu tiên.

Ví dụ, nếu một giao dịch kiếm được 256 ZELD chứa 4 đầu ra với 500, 500, 500 và 2000 Satoshi tương ứng, đầu ra đầu tiên nhận được 86 ZELD phần thưởng, đầu ra thứ hai và thứ ba nhận 85 ZELD.

4 Di chuyển ZELD

Khi các UTXO có ZELD đính kèm được chi tiêu, ZELD được phân phối cho các UTXO mới trong giao dịch. Có hai phương pháp để phân phối ZELD khi di chuyển chúng:

4.1 Phương pháp 1: Phân phối Tỷ lệ Tự động

Theo mặc định, việc phân phối được thực hiện giống hệt như phần thưởng — theo tỷ lệ dựa trên giá trị Bitcoin của các UTXO đầu ra, loại trừ đầu ra cuối cùng nếu có nhiều đầu ra.

4.2 Phương pháp 2: Phân phối Tùy chỉnh qua OP_RETURN

Bạn có thể chỉ định chính xác cách ZELD nên được phân phối bằng cách bao gồm một đầu ra OP_RETURN trong giao dịch của bạn với dữ liệu phân phối tùy chỉnh. Điều này cho phép kiểm soát chính xác việc chuyển ZELD.

4.2.1 Định dạng OP_RETURN:

- Script OP_RETURN phải chứa dữ liệu bắt đầu bằng tiền tố 4 byte “ZELD”
- Sau tiền tố, dữ liệu phải được mã hóa ở định dạng CBOR
- Dữ liệu CBOR phải đại diện cho một vector các số nguyên không dấu 64-bit (Vec)
- Mỗi số nguyên chỉ định số lượng ZELD gửi đến UTXO đầu ra tương ứng

4.2.2 Quy tắc Phân phối:

- Số lượng giá trị trong mảng phân phối được tự động điều chỉnh để khớp với số lượng đầu ra không phải OP_RETURN
- Nếu mảng quá dài, các giá trị thừa sẽ bị loại bỏ
- Nếu mảng quá ngắn, các số không được thêm vào
- Tổng các giá trị phân phối không thể vượt quá tổng ZELD đang được chi tiêu
- Nếu tổng nhỏ hơn tổng số, phần chênh lệch được thêm vào đầu ra đầu tiên
- Nếu tổng vượt quá tổng số, giao dịch quay lại phân phối theo tỷ lệ
- Phần thưởng ZELD mới đào luôn được phân phối theo tỷ lệ và sau đó kết hợp với phân phối tùy chỉnh

4.2.3 Ví dụ:

Nếu bạn có 1000 ZELD để phân phối cho 3 đầu ra và muốn gửi 600 cho cái đầu tiên, 300 cho cái thứ hai và 100 cho cái thứ ba, OP_RETURN của bạn sẽ chứa “ZELD” theo sau là mã hóa CBOR của [600, 300, 100].

Lưu ý:
- Nếu không tìm thấy phân phối OP_RETURN hợp lệ, giao dịch tự động sử dụng phương pháp phân phối theo tỷ lệ.
- Nếu một giao dịch chỉ chứa một đầu ra OP_RETURN, bất kỳ ZELD nào đính kèm với đầu vào của giao dịch **và bất kỳ phần thưởng mới kiếm được** đều bị đốt vĩnh viễn vì không có đầu ra có thể chi tiêu để nhận chúng.

- Khi có nhiều đầu ra OP_RETURN, chỉ đầu ra xuất hiện cuối cùng trong giao dịch và mang payload `ZELD`+CBOR hợp lệ mới được xem xét cho phân phối.