PROTOKÓŁ ZELDHASH

Poluj na najrzadsze transakcje Bitcoin i zdobywaj ZELD.

Autor: Ouziel Slama

1 Motywacje

- Dla dreszczyku polowania. Każda transakcja staje się okazją do odkrycia czegoś rzadkiego — cyfrowego skarbu ukrytego na widoku na blockchainie.
- Te wzorce wiodących zer są nie tylko rzadkie — mogą również poprawić kompresję, potencjalnie usprawniając przechowywanie i wydajność przetwarzania blockchaina.
- Każdy może zarabiać ZELD, polując na rzadkie transakcje — brak pojedynczego zwycięzcy na blok jak w kopaniu bloków Bitcoin. Polowanie jest otwarte dla wszystkich.
- W przypadku sukcesu tokeny ZELD mogą ostatecznie zwracać opłaty transakcyjne — nagradzając łowców, którzy odkrywają najrzadsze znaleziska!

2 Kopanie ZELD

Aby kopać ZELD, musisz nadać transakcję Bitcoin, której txid zaczyna się od co najmniej 6 zer. Nagroda jest obliczana na podstawie porównania twojej transakcji z najlepszą transakcją w bloku:

- W danym bloku transakcje zaczynające się od największej liczby zer zarabiają 4096 ZELD
- Transakcje z jednym zerem mniej niż najlepsze transakcje zarabiają 4096/16 lub 256 ZELD
- Transakcje z dwoma zerami mniej zarabiają 4096 / 16 / 16 lub 16 ZELD
- itd.

Dlatego stosowana formuła jest następująca:

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

Gdzie `max_zero_count` jest równe liczbie zer rozpoczynających najlepszą transakcję, a `zero_count` to liczba zer rozpoczynających transakcję, dla której obliczamy nagrodę.

Uwaga: Transakcje Coinbase nie kwalifikują się do nagród ZELD.

3 Dystrybucja ZELD

ZELD zarobione transakcją zaczynającą się od 6 lub więcej zer są dystrybuowane do UTXO. Dystrybucja odbywa się następująco:

- Jeśli istnieje pojedyncze UTXO nie-OP_RETURN, otrzymuje całą nagrodę.
- Jeśli istnieją dwa lub więcej UTXO nie-OP_RETURN, nagroda jest dystrybuowana do wszystkich UTXO, z wyjątkiem ostatniego, proporcjonalnie do wartości każdego UTXO
- Ponieważ obliczenia są wykonywane tylko na liczbach całkowitych, ewentualna reszta z dzielenia jest dystrybuowana do pierwszego UTXO nie-OP_RETURN.

Na przykład, jeśli transakcja zarabiająca 256 ZELD zawiera 4 wyjścia z odpowiednio 500, 500, 500 i 2000 Satoshi, pierwsze wyjście otrzymuje 86 ZELD nagrody, drugie i trzecie po 85 ZELD.

4 Przenoszenie ZELD

Gdy UTXO z dołączonymi ZELD są wydawane, ZELD są dystrybuowane do nowych UTXO w transakcji. Istnieją dwie metody dystrybucji ZELD przy ich przenoszeniu:

4.1 Metoda 1: Automatyczna dystrybucja proporcjonalna

Domyślnie dystrybucja odbywa się dokładnie tak samo jak nagrody — proporcjonalnie na podstawie wartości Bitcoin wyjściowych UTXO, z wyłączeniem ostatniego wyjścia, jeśli jest ich wiele.

4.2 Metoda 2: Niestandardowa dystrybucja przez OP_RETURN

Możesz dokładnie określić, jak ZELD mają być dystrybuowane, włączając wyjście OP_RETURN w swojej transakcji z niestandardowymi danymi dystrybucji. Pozwala to na precyzyjną kontrolę nad transferami ZELD.

4.2.1 Format OP_RETURN:

- Skrypt OP_RETURN musi zawierać dane zaczynające się od 4-bajtowego prefiksu “ZELD”
- Po prefiksie dane muszą być zakodowane w formacie CBOR
- Dane CBOR powinny reprezentować wektor 64-bitowych liczb całkowitych bez znaku (Vec)
- Każda liczba całkowita określa, ile ZELD wysłać do odpowiedniego wyjściowego UTXO

4.2.2 Zasady dystrybucji:

- Liczba wartości w tablicy dystrybucji jest automatycznie dostosowywana do liczby wyjść nie-OP_RETURN
- Jeśli tablica jest zbyt długa, dodatkowe wartości są usuwane
- Jeśli tablica jest zbyt krótka, dodawane są zera
- Całkowita suma wartości dystrybucji nie może przekroczyć całkowitej liczby wydawanych ZELD
- Jeśli suma jest mniejsza niż całość, różnica jest dodawana do pierwszego wyjścia
- Jeśli suma przekracza całość, transakcja wraca do dystrybucji proporcjonalnej
- Nowo wykopane nagrody ZELD są zawsze dystrybuowane proporcjonalnie, a następnie łączone z niestandardową dystrybucją

4.2.3 Przykład:

Jeśli masz 1000 ZELD do dystrybucji na 3 wyjścia i chcesz wysłać 600 do pierwszego, 300 do drugiego i 100 do trzeciego, twój OP_RETURN będzie zawierał “ZELD”, a następnie kodowanie CBOR [600, 300, 100].

Uwagi:
- Jeśli nie zostanie znaleziona prawidłowa dystrybucja OP_RETURN, transakcja automatycznie używa metody dystrybucji proporcjonalnej.

- Jeśli transakcja zawiera tylko jedno wyjście OP_RETURN, wszystkie ZELD dołączone do wejść transakcji **oraz wszelkie nowo zdobyte nagrody** są trwale spalane, ponieważ nie ma wydawalnych wyjść do ich otrzymania.
- Gdy obecnych jest wiele wyjść OP_RETURN, tylko to pojawiające się jako ostatnie w transakcji i niosące prawidłowy ładunek `ZELD`+CBOR jest brane pod uwagę przy dystrybucji.