PROTOKOL ZELDHASH

Lovte nejvzácnější Bitcoinové transakce a získejte ZELD.

Autor: Ouziel Slama

1 Motivace

- Pro vzrušení z lovu. Každá transakce se stává příležitostí objevit něco vzácného — digitální poklad skrytý na očích na blockchainu.
- Tyto vzory úvodních nul nejsou jen vzácné — mohly by také zlepšit kompresi, potenciálně zefektivnit ukládání a zpracování blockchainu.
- Kdokoli může získat ZELD lovem vzácných transakcí — žádný jediný vítěz na blok jako při těžbě Bitcoin bloků. Lov je otevřen všem.
- V případě úspěchu by tokeny ZELD mohly nakonec proplácet transakční poplatky — odměňovat lovce, kteří odhalí nejvzácnější nálezy!

2 Těžba ZELD

Pro těžbu ZELD musíte vysílat Bitcoinovou transakci, jejíž txid začíná alespoň 6 nulami. Odměna se vypočítá na základě toho, jak se vaše transakce porovnává s nejlepší transakcí v bloku:

- V daném bloku transakce začínající nejvíce nulami získají 4096 ZELD
- Transakce s jednou nulou méně než nejlepší transakce získají 4096/16 nebo 256 ZELD
- Transakce se dvěma nulami méně získají 4096 / 16 / 16 nebo 16 ZELD
- atd.

Proto je použitý vzorec následující:

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

Kde `max_zero_count` se rovná počtu nul, kterými začíná nejlepší transakce, a `zero_count` je počet nul, kterými začíná transakce, pro kterou počítáme odměnu.

Poznámka: Coinbase transakce nejsou způsobilé pro odměny ZELD.

3 Distribuce ZELD

ZELD získané transakcí začínající 6 nebo více nulami se distribuují do UTXO. Distribuce se provádí následovně:

- Pokud existuje jediné non-OP_RETURN UTXO, obdrží celou odměnu.
- Pokud existují dvě nebo více non-OP_RETURN UTXO, odměna se distribuuje všem UTXO kromě posledního v poměru k hodnotě každého UTXO
- Protože výpočty se provádějí pouze s celými čísly, možný zbytek po dělení se distribuuje prvnímu non-OP_RETURN UTXO.

Například pokud transakce získávající 256 ZELD obsahuje 4 výstupy s 500, 500, 500 a 2000 Satoshi, první výstup obdrží 86 ZELD z odměny, druhý a třetí 85 ZELD.

4 Přesun ZELD

Když jsou UTXO s připojenými ZELD utraceny, ZELD se distribuují do nových UTXO v transakci. Existují dvě metody pro distribuci ZELD při jejich přesunu:

4.1 Metoda 1: Automatická proporcionální distribuce

Ve výchozím nastavení se distribuce provádí přesně stejným způsobem jako odměny — proporcionálně na základě Bitcoin hodnot výstupních UTXO, s vyloučením posledního výstupu, pokud je jich více.

4.2 Metoda 2: Vlastní distribuce přes OP_RETURN

Můžete přesně specifikovat, jak by měly být ZELD distribuovány, zahrnutím OP_RETURN výstupu ve vaší transakci s vlastními distribučními daty. To umožňuje přesnou kontrolu nad převody ZELD.

4.2.1 Formát OP_RETURN:

- OP_RETURN skript musí obsahovat data začínající 4-bajtovým prefixem "ZELD"
- Po prefixu musí být data zakódována ve formátu CBOR
- CBOR data by měla reprezentovat vektor neznaménkových 64-bitových celých čísel (Vec)
- Každé celé číslo specifikuje, kolik ZELD poslat na odpovídající výstupní UTXO

4.2.2 Pravidla distribuce:

- Počet hodnot v distribučním poli se automaticky upraví tak, aby odpovídal počtu non-OP_RETURN výstupů
- Pokud je pole příliš dlouhé, přebytečné hodnoty se odstraní
- Pokud je pole příliš krátké, přidají se nuly
- Celkový součet distribučních hodnot nemůže překročit celkové množství utrácených ZELD
- Pokud je součet menší než celkové množství, rozdíl se přidá k prvnímu výstupu
- Pokud součet překročí celkové množství, transakce se vrátí k proporcionální distribuci
- Nově vytěžené odměny ZELD jsou vždy distribuovány proporcionálně a poté kombinovány s vlastní distribucí

4.2.3 Příklad:

Pokud máte 1000 ZELD k distribuci na 3 výstupy a chcete poslat 600 na první, 300 na druhý a 100 na třetí, váš OP_RETURN bude obsahovat "ZELD" následované CBOR kódováním [600, 300, 100].

Poznámky:
- Pokud není nalezena platná OP_RETURN distribuce, transakce automaticky použije metodu proporcionální distribuce.
- Pokud transakce obsahuje pouze jeden OP_RETURN výstup, jakékoli ZELD připojené ke vstupům transakce **a jakékoli nově získané odměny** jsou trvale spáleny, protože neexistují utratitelné výstupy pro jejich přijetí.

- Když je přítomno více OP_RETURN výstupů, pro distribuci se bere v úvahu pouze ten, který se objeví v transakci jako poslední a nese platný `ZELD`+CBOR payload.