PROTOCOLUL ZELDHASH

Vânează cele mai rare tranzacții Bitcoin și câștigă ZELD.

De Ouziel Slama

1 Motivații

- Pentru emoția vânătorii. Fiecare tranzacție devine o oportunitate de a descoperi ceva rar — o comoară digitală ascunsă la vedere pe blockchain.
- Aceste tipare de zerouri inițiale nu sunt doar rare — ar putea îmbunătăți și compresia, potențial eficientizând stocarea și procesarea blockchain-ului.
- Oricine poate câștiga ZELD vânând tranzacții rare — nu există un singur câștigător pe bloc ca în mineritul de blocuri Bitcoin. Vânătoarea este deschisă tuturor.
- Dacă are succes, tokenurile ZELD ar putea în cele din urmă rambursa taxele de tranzacție — recompensând vânătorii care descoperă cele mai rare descoperiri!

2 Mineritul ZELD

Pentru a mina ZELD trebuie să difuzați o tranzacție Bitcoin al cărei txid începe cu cel puțin 6 zerouri. Recompensa se calculează în funcție de cum se compară tranzacția dvs. cu cea mai bună tranzacție din bloc:

- Într-un bloc dat, tranzacțiile care încep cu cele mai multe zerouri câștigă 4096 ZELD
- Tranzacțiile cu un zero mai puțin decât cele mai bune tranzacții câștigă 4096/16 sau 256 ZELD
- Tranzacțiile cu două zerouri mai puțin câștigă 4096 / 16 / 16 sau 16 ZELD
- etc.

Prin urmare, formula utilizată este următoarea:

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

Unde `max_zero_count` este egal cu numărul de zerouri care încep cea mai bună tranzacție și `zero_count` este numărul de zerouri care încep tranzacția pentru care calculăm recompensa.

Notă: Tranzacțiile Coinbase nu sunt eligibile pentru recompense ZELD.

3 Distribuția ZELD

ZELD-urile câștigate cu o tranzacție care începe cu 6 sau mai multe zerouri sunt distribuite către UTXO-uri. Distribuția se efectuează după cum urmează:

- Dacă există un singur UTXO non-OP_RETURN, acesta primește întreaga recompensă.
- Dacă există două sau mai multe UTXO-uri non-OP_RETURN, recompensa este distribuită tuturor UTXO-urilor, cu excepția ultimului, proporțional cu valoarea fiecărui UTXO

- Deoarece calculele se fac doar cu numere întregi, restul posibil al împărțirii este distribuit primului UTXO non-OP_RETURN.

De exemplu, dacă o tranzacție care câștigă 256 ZELD conține 4 ieșiri cu 500, 500, 500 și 2000 Satoshi respectiv, prima ieșire primește 86 ZELD din recompensă, a doua și a treia 85 ZELD.

4 Mutarea ZELD

Când UTXO-urile cu ZELD-uri atașate sunt cheltuite, ZELD-urile sunt distribuite către noile UTXO-uri din tranzacție. Există două metode pentru distribuirea ZELD-urilor la mutare:

4.1 Metoda 1: Distribuție Proporțională Automată

În mod implicit, distribuția se face exact la fel ca recompensele — proporțional pe baza valorilor Bitcoin ale UTXO-urilor de ieșire, excluzând ultima ieșire dacă există mai multe ieșiri.

4.2 Metoda 2: Distribuție Personalizată prin OP_RETURN

Puteți specifica exact cum ar trebui distribuite ZELD-urile incluzând o ieșire OP_RETURN în tranzacția dvs. cu date de distribuție personalizate. Aceasta permite controlul precis asupra transferurilor ZELD.

4.2.1 Formatul OP_RETURN:

- Scriptul OP_RETURN trebuie să conțină date care încep cu prefixul de 4 octeți "ZELD"
- După prefix, datele trebuie codificate în format CBOR
- Datele CBOR trebuie să reprezinte un vector de numere întregi nesemnate pe 64 de biți (Vec)
- Fiecare număr întreg specifică câte ZELD-uri să trimită către UTXO-ul de ieșire corespunzător

4.2.2 Reguli de Distribuție:

- Numărul de valori din matricea de distribuție este ajustat automat pentru a corespunde numărului de ieșiri non-OP_RETURN
- Dacă matricea este prea lungă, valorile suplimentare sunt eliminate
- Dacă matricea este prea scurtă, se adaugă zerouri
- Suma totală a valorilor de distribuție nu poate depăși totalul ZELD-urilor cheltuite
- Dacă suma este mai mică decât totalul, diferența se adaugă la prima ieșire
- Dacă suma depășește totalul, tranzacția revine la distribuția proporțională
- Recompensele ZELD nou minate sunt întotdeauna distribuite proporțional și apoi combinate cu distribuția personalizată

4.2.3 Exemplu:

Dacă aveți 1000 ZELD de distribuit pe 3 ieșiri și doriți să trimiteți 600 către prima, 300 către a doua și 100 către a treia, OP_RETURN-ul dvs. ar conține "ZELD" urmat de codificarea CBOR a [600, 300, 100].

Note:
- Dacă nu se găsește nicio distribuție OP_RETURN validă, tranzacția utilizează automat metoda de distribuție proporțională.

- Dacă o tranzacție conține doar o ieșire OP_RETURN, orice ZELD atașat la intrările tranzacției **și orice recompensă nou câștigată** sunt arse permanent deoarece nu există ieșiri cheltuibile pentru a le primi.
- Când sunt prezente mai multe ieșiri OP_RETURN, doar cea care apare ultima în tranzacție și poartă un payload `ZELD`+CBOR valid este luată în considerare pentru distribuție.