ZELDHASH PROTOCOL

Jaag op de zeldzaamste Bitcoin-transacties en verdien ZELD.

Door Ouziel Slama

1 Motivaties

- Voor de spanning van de jacht. Elke transactie wordt een kans om iets zeldzaams te ontdekken — een digitale schat die in het volle zicht op de blockchain verborgen ligt.
- Deze patronen van leidende nullen zijn niet alleen zeldzaam — ze kunnen ook de compressie verbeteren, wat mogelijk de opslag en verwerkingsefficiëntie van de blockchain stroomlijnt.
- Iedereen kan ZELD verdienen door zeldzame transacties te jagen — geen enkele winnaar per blok zoals bij Bitcoin-blokmining. De jacht staat open voor iedereen.
- Bij succes zouden ZELD-tokens uiteindelijk transactiekosten kunnen vergoeden — en zo jagers belonen die de zeldzaamste vondsten ontdekken!

2 ZELD Mining

Om ZELD te minen moet je een Bitcoin-transactie uitzenden waarvan de txid begint met ten minste 6 nullen. De beloning wordt berekend op basis van hoe jouw transactie zich verhoudt tot de beste transactie in het blok:

- In een gegeven blok verdienen transacties die beginnen met de meeste nullen 4096 ZELD
- Transacties met één nul minder dan de beste transacties verdienen 4096/16 of 256 ZELD
- Transacties met twee nullen minder verdienen 4096 / 16 / 16 of 16 ZELD
- enz.

De gebruikte formule is daarom als volgt:

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

Waarbij `max_zero_count` gelijk is aan het aantal nullen waarmee de beste transactie begint en `zero_count` het aantal nullen is waarmee de transactie begint waarvoor we de beloning berekenen.

Opmerking: Coinbase-transacties komen niet in aanmerking voor ZELD-beloningen.

3 ZELD Distributie

ZELDs verdiend met een transactie die begint met 6 of meer nullen worden gedistribueerd naar UTXOs. De distributie wordt als volgt uitgevoerd:

- Als er een enkele niet-OP_RETURN UTXO is, ontvangt deze de volledige beloning.
- Als er twee of meer niet-OP_RETURN UTXOs zijn, wordt de beloning verdeeld over alle UTXOs, behalve de laatste, in verhouding tot de waarde van elke UTXO

- Aangezien de berekeningen alleen met gehele getallen worden gedaan, wordt de mogelijke rest van de deling gedistribueerd naar de eerste niet-OP_RETURN UTXO.

Als bijvoorbeeld een transactie die 256 ZELD verdient 4 outputs bevat met respectievelijk 500, 500, 500 en 2000 Satoshis, ontvangt de eerste output 86 ZELD van de beloning, de tweede en derde 85 ZELD.

4 ZELD Verplaatsen

Wanneer UTXOs met bijgevoegde ZELDs worden uitgegeven, worden de ZELDs gedistribueerd naar de nieuwe UTXOs in de transactie. Er zijn twee methoden om ZELDs te distribueren bij het verplaatsen:

4.1 Methode 1: Automatische Proportionele Distributie

Standaard wordt de distributie op precies dezelfde manier gedaan als beloningen — proportioneel op basis van de Bitcoin-waarden van de output UTXOs, met uitsluiting van de laatste output als er meerdere outputs zijn.

4.2 Methode 2: Aangepaste Distributie via OP_RETURN

Je kunt precies specificeren hoe ZELDs moeten worden gedistribueerd door een OP_RETURN output op te nemen in je transactie met aangepaste distributiegegevens. Dit maakt nauwkeurige controle over ZELD-overdrachten mogelijk.

4.2.1 OP_RETURN Formaat:

- Het OP_RETURN script moet gegevens bevatten die beginnen met het 4-byte prefix “ZELD”
- Na het prefix moeten de gegevens in CBOR-formaat zijn gecodeerd
- De CBOR-gegevens moeten een vector van unsigned 64-bit integers (Vec) voorstellen
- Elk geheel getal specificeert hoeveel ZELDs naar de overeenkomstige output UTXO moeten worden gestuurd

4.2.2 Distributieregels:

- Het aantal waarden in de distributie-array wordt automatisch aangepast om overeen te komen met het aantal niet-OP_RETURN outputs
- Als de array te lang is, worden extra waarden verwijderd
- Als de array te kort is, worden nullen toegevoegd
- Het totaal van de distributiewaarden mag het totaal van de uit te geven ZELDs niet overschrijden
- Als de som minder is dan het totaal, wordt het verschil toegevoegd aan de eerste output
- Als de som het totaal overschrijdt, valt de transactie terug op proportionele distributie
- Nieuw geminede ZELD-beloningen worden altijd proportioneel gedistribueerd en vervolgens gecombineerd met de aangepaste distributie

4.2.3 Voorbeeld:

Als je 1000 ZELDs hebt om te distribueren over 3 outputs en je wilt 600 naar de eerste, 300 naar de tweede en 100 naar de derde sturen, zou je OP_RETURN “ZELD” bevatten gevolgd door de CBOR-codering van [600, 300, 100].

Opmerkingen:

- Als er geen geldige OP_RETURN distributie wordt gevonden, gebruikt de transactie automatisch de proportionele distributiemethode.
- Als een transactie slechts één OP_RETURN output bevat, worden alle ZELDs die aan de transactie-inputs zijn bijgevoegd **en alle nieuw verdiende beloningen** permanent verbrand omdat er geen besteedbare outputs zijn om ze te ontvangen.
- Wanneer er meerdere OP_RETURN outputs aanwezig zijn, wordt alleen degene die het laatst in de transactie verschijnt en een geldige `ZELD`+CBOR payload draagt, overwogen voor distributie.