PROTOCOLLO ZELDHASH

Caccia alle transazioni Bitcoin più rare e guadagna ZELD.

Di Ouziel Slama

1 Motivazioni

- Per il brivido della caccia. Ogni transazione diventa un'opportunità per scoprire qualcosa di raro — un tesoro digitale nascosto in bella vista sulla blockchain.
- Questi pattern di zeri iniziali non sono solo rari — potrebbero anche migliorare la compressione, potenzialmente ottimizzando l'archiviazione e l'efficienza di elaborazione della blockchain.
- Chiunque può guadagnare ZELD cacciando transazioni rare — nessun vincitore unico per blocco come nel mining di blocchi Bitcoin. La caccia è aperta a tutti.
- In caso di successo, i token ZELD potrebbero eventualmente rimborsare le commissioni di transazione — premiando i cacciatori che scoprono le scoperte più rare!

2 Mining di ZELD

Per minare ZELD devi trasmettere una transazione Bitcoin il cui txid inizia con almeno 6 zeri. La ricompensa viene calcolata in base a come la tua transazione si confronta con la migliore transazione nel blocco:

- In un dato blocco, le transazioni che iniziano con più zeri guadagnano 4096 ZELD
- Le transazioni con uno zero in meno rispetto alle migliori transazioni guadagnano 4096/16 o 256 ZELD
- Le transazioni con due zeri in meno guadagnano 4096 / 16 / 16 o 16 ZELD
- ecc.

La formula utilizzata è quindi la seguente:

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

Dove `max_zero_count` è uguale al numero di zeri che iniziano la migliore transazione e `zero_count` è il numero di zeri che iniziano la transazione per cui calcoliamo la ricompensa.

Nota: Le transazioni Coinbase non sono idonee per le ricompense ZELD.

3 Distribuzione dei ZELD

I ZELD guadagnati con una transazione che inizia con 6 o più zeri vengono distribuiti agli UTXO. La distribuzione viene effettuata come segue:

- Se c'è un singolo UTXO non-OP_RETURN, riceve l'intera ricompensa.
- Se ci sono due o più UTXO non-OP_RETURN, la ricompensa viene distribuita a tutti gli UTXO, tranne l'ultimo, in proporzione al valore di ciascun UTXO

- Poiché i calcoli vengono effettuati solo con numeri interi, l'eventuale resto della divisione viene distribuito al primo UTXO non-OP_RETURN.

Ad esempio, se una transazione che guadagna 256 ZELD contiene 4 output con rispettivamente 500, 500, 500 e 2000 Satoshi, il primo output riceve 86 ZELD della ricompensa, il secondo e il terzo 85 ZELD.

4 Spostamento dei ZELD

Quando gli UTXO con ZELD allegati vengono spesi, i ZELD vengono distribuiti ai nuovi UTXO nella transazione. Esistono due metodi per distribuire i ZELD durante lo spostamento:

4.1 Metodo 1: Distribuzione Proporzionale Automatica

Per impostazione predefinita, la distribuzione viene effettuata esattamente come le ricompense — proporzionalmente in base ai valori Bitcoin degli UTXO di output, escludendo l'ultimo output se ce ne sono più di uno.

4.2 Metodo 2: Distribuzione Personalizzata tramite OP_RETURN

Puoi specificare esattamente come devono essere distribuiti i ZELD includendo un output OP_RETURN nella tua transazione con dati di distribuzione personalizzati. Questo consente un controllo preciso sui trasferimenti di ZELD.

4.2.1 Formato OP_RETURN:

- Lo script OP_RETURN deve contenere dati che iniziano con il prefisso di 4 byte "ZELD"
- Dopo il prefisso, i dati devono essere codificati in formato CBOR
- I dati CBOR devono rappresentare un vettore di interi senza segno a 64 bit (Vec)
- Ogni intero specifica quanti ZELD inviare all'UTXO di output corrispondente

4.2.2 Regole di Distribuzione:

- Il numero di valori nell'array di distribuzione viene automaticamente regolato per corrispondere al numero di output non-OP_RETURN
- Se l'array è troppo lungo, i valori extra vengono rimossi
- Se l'array è troppo corto, vengono aggiunti degli zeri
- La somma totale dei valori di distribuzione non può superare il totale dei ZELD che vengono spesi
- Se la somma è inferiore al totale, la differenza viene aggiunta al primo output
- Se la somma supera il totale, la transazione torna alla distribuzione proporzionale
- Le ricompense ZELD appena minate vengono sempre distribuite proporzionalmente e poi combinate con la distribuzione personalizzata

4.2.3 Esempio:

Se hai 1000 ZELD da distribuire su 3 output e vuoi inviare 600 al primo, 300 al secondo e 100 al terzo, il tuo OP_RETURN conterrebbe "ZELD" seguito dalla codifica CBOR di [600, 300, 100].

Note:

- Se non viene trovata una distribuzione OP_RETURN valida, la transazione utilizza automaticamente il metodo di distribuzione proporzionale.
- Se una transazione contiene solo un output OP_RETURN, tutti i ZELD allegati agli input della transazione **e tutte le ricompense appena guadagnate** vengono bruciati permanentemente perché non ci sono output spendibili per riceverli.
- Quando sono presenti più output OP_RETURN, solo quello che appare per ultimo nella transazione e che porta un payload `ZELD`+CBOR valido viene considerato per la distribuzione.