ZELDHASH-PROTOKOLL

Jagen Sie die seltensten Bitcoin-Transaktionen und verdienen Sie ZELD.

Von Ouziel Slama

1 Motivation

- Für den Nervenkitzel der Jagd. Jede Transaktion wird zur Gelegenheit, etwas Seltenes zu entdecken — ein digitaler Schatz, der offen auf der Blockchain verborgen ist.
- Diese Muster führender Nullen sind nicht nur selten — sie könnten auch die Komprimierung verbessern und möglicherweise die Blockchain-Speicherung und Verarbeitungseffizienz optimieren.
- Jeder kann ZELD verdienen, indem er seltene Transaktionen jagt — kein Einzelgewinner pro Block wie beim Bitcoin-Block-Mining. Die Jagd ist für alle offen.
- Bei Erfolg könnten ZELD-Token schließlich Transaktionsgebühren erstatten — und Jäger belohnen, die die seltensten Funde aufdecken!

2 ZELD-Mining

Um ZELD zu minen, müssen Sie eine Bitcoin-Transaktion übertragen, deren txid mit mindestens 6 Nullen beginnt. Die Belohnung wird basierend darauf berechnet, wie Ihre Transaktion mit der besten Transaktion im Block verglichen wird:

- In einem gegebenen Block verdienen Transaktionen, die mit den meisten Nullen beginnen, 4096 ZELD
- Transaktionen mit einer Null weniger als die besten Transaktionen verdienen 4096/16 oder 256 ZELD
- Transaktionen mit zwei Nullen weniger verdienen 4096 / 16 / 16 oder 16 ZELD
- usw.

Daher lautet die verwendete Formel wie folgt:

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

Wobei `max_zero_count` gleich der Anzahl der Nullen ist, mit denen die beste Transaktion beginnt, und `zero_count` die Anzahl der Nullen ist, mit denen die Transaktion beginnt, für die wir die Belohnung berechnen.

Hinweis: Coinbase-Transaktionen sind nicht für ZELD-Belohnungen berechtigt.

3 ZELD-Verteilung

Mit einer Transaktion, die mit 6 oder mehr Nullen beginnt, verdiente ZELDs werden an UTXOs verteilt. Die Verteilung erfolgt wie folgt:

- Wenn es einen einzelnen Nicht-OP_RETURN-UTXO gibt, erhält er die gesamte Belohnung.
- Wenn es zwei oder mehr Nicht-OP_RETURN-UTXOs gibt, wird die Belohnung an alle UTXOs außer dem letzten im Verhältnis zum Wert jedes UTXOs verteilt

- Da die Berechnungen nur mit ganzen Zahlen durchgeführt werden, wird der mögliche Rest der Division an den ersten Nicht-OP_RETURN-UTXO verteilt.

Wenn zum Beispiel eine Transaktion, die 256 ZELD verdient, 4 Ausgaben mit jeweils 500, 500, 500 und 2000 Satoshi enthält, erhält die erste Ausgabe 86 ZELD der Belohnung, die zweite und dritte jeweils 85 ZELD.

4 ZELD verschieben

Wenn UTXOs mit angehängten ZELDs ausgegeben werden, werden die ZELDs an die neuen UTXOs in der Transaktion verteilt. Es gibt zwei Methoden zur Verteilung von ZELDs beim Verschieben:

4.1 Methode 1: Automatische proportionale Verteilung

Standardmäßig erfolgt die Verteilung genauso wie bei Belohnungen — proportional basierend auf den Bitcoin-Werten der Ausgabe-UTXOs, wobei die letzte Ausgabe ausgeschlossen wird, wenn es mehrere Ausgaben gibt.

4.2 Methode 2: Benutzerdefinierte Verteilung über OP_RETURN

Sie können genau angeben, wie ZELDs verteilt werden sollen, indem Sie eine OP_RETURN-Ausgabe in Ihre Transaktion mit benutzerdefinierten Verteilungsdaten aufnehmen. Dies ermöglicht eine präzise Kontrolle über ZELD-Überweisungen.

4.2.1 OP_RETURN-Format:

- Das OP_RETURN-Skript muss Daten enthalten, die mit dem 4-Byte-Präfix “ZELD” beginnen
- Nach dem Präfix müssen die Daten im CBOR-Format kodiert sein
- Die CBOR-Daten sollten einen Vektor von vorzeichenlosen 64-Bit-Ganzzahlen (Vec) darstellen
- Jede Ganzzahl gibt an, wie viele ZELDs an den entsprechenden Ausgabe-UTXO gesendet werden sollen

4.2.2 Verteilungsregeln:

- Die Anzahl der Werte im Verteilungs-Array wird automatisch angepasst, um der Anzahl der Nicht-OP_RETURN-Ausgaben zu entsprechen
- Wenn das Array zu lang ist, werden zusätzliche Werte entfernt
- Wenn das Array zu kurz ist, werden Nullen angehängt
- Die Gesamtsumme der Verteilungswerte darf die Gesamtzahl der ausgegebenen ZELDs nicht überschreiten
- Wenn die Summe kleiner als die Gesamtzahl ist, wird die Differenz zur ersten Ausgabe hinzugefügt
- Wenn die Summe die Gesamtzahl überschreitet, fällt die Transaktion auf proportionale Verteilung zurück
- Neu geminte ZELD-Belohnungen werden immer proportional verteilt und dann mit der benutzerdefinierten Verteilung kombiniert

4.2.3 Beispiel:

Wenn Sie 1000 ZELDs auf 3 Ausgaben verteilen möchten und 600 an die erste, 300 an die zweite und 100 an die dritte senden möchten, würde Ihr OP_RETURN "ZELD" enthalten, gefolgt von der CBOR-Kodierung von [600, 300, 100].

Hinweise:

- Wenn keine gültige OP_RETURN-Verteilung gefunden wird, verwendet die Transaktion automatisch die proportionale Verteilungsmethode.
- Wenn eine Transaktion nur eine OP_RETURN-Ausgabe enthält, werden alle an die Transaktionseingaben angehängten ZELDs **und alle neu verdienten Belohnungen** dauerhaft verbrannt, da es keine ausgebbaren Ausgaben gibt, um sie zu empfangen.
- Wenn mehrere OP_RETURN-Ausgaben vorhanden sind, wird nur diejenige für die Verteilung berücksichtigt, die zuletzt in der Transaktion erscheint und eine gültige `ZELD`+CBOR-Nutzlast trägt.