PROTOCOLO ZELDHASH

Caza las transacciones más raras de Bitcoin y gana ZELD.

Por Ouziel Slama

1 Motivaciones

- Por la emoción de la caza. Cada transacción se convierte en una oportunidad para descubrir algo raro — un tesoro digital oculto a plena vista en la blockchain.
- Estos patrones de ceros iniciales no solo son raros — también podrían mejorar la compresión, potencialmente optimizando el almacenamiento y la eficiencia de procesamiento de la blockchain.
- Cualquiera puede ganar ZELD cazando transacciones raras — no hay un único ganador por bloque como en la minería de bloques de Bitcoin. La caza está abierta a todos.
- Si tiene éxito, ¡los tokens ZELD podrían eventualmente reembolsar las tarifas de transacción — recompensando a los cazadores que descubran los hallazgos más raros!

2 Minería de ZELD

Para minar ZELD, debes transmitir una transacción de Bitcoin cuyo txid comience con al menos 6 ceros. La recompensa se calcula en función de cómo tu transacción se compara con la mejor transacción del bloque:

- En un bloque dado, las transacciones que comienzan con más ceros ganan 4096 ZELD
- Las transacciones con un cero menos que las mejores transacciones ganan 4096/16 o 256 ZELD
- Las transacciones con dos ceros menos ganan 4096 / 16 / 16 o 16 ZELD
- etc.

Por lo tanto, la fórmula utilizada es la siguiente:

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

Donde `max_zero_count` es igual al número de ceros que comienzan la mejor transacción y `zero_count` es el número de ceros que comienzan la transacción para la cual calculamos la recompensa.

Nota: Las transacciones Coinbase no son elegibles para recompensas ZELD.

3 Distribución de ZELD

Los ZELD ganados con una transacción que comienza con 6 o más ceros se distribuyen a los UTXO. La distribución se realiza de la siguiente manera:

- Si hay un único UTXO no OP_RETURN, recibe toda la recompensa.
- Si hay dos o más UTXO no OP_RETURN, la recompensa se distribuye a todos los UTXO, excepto el último, en proporción al valor de cada UTXO

- Como los cálculos se realizan solo con enteros, el posible resto de la división se distribuye al primer UTXO no OP_RETURN.

Por ejemplo, si una transacción que gana 256 ZELD contiene 4 salidas con 500, 500, 500 y 2000 Satoshis respectivamente, la primera salida recibe 86 ZELD de la recompensa, la segunda y tercera 85 ZELD.

4 Movimiento de ZELD

Cuando se gastan UTXO con ZELD adjuntos, los ZELD se distribuyen a los nuevos UTXO en la transacción. Hay dos métodos para distribuir ZELD al moverlos:

4.1 Método 1: Distribución Proporcional Automática

Por defecto, la distribución se realiza exactamente de la misma manera que las recompensas — proporcionalmente según los valores de Bitcoin de los UTXO de salida, excluyendo la última salida si hay múltiples salidas.

4.2 Método 2: Distribución Personalizada vía OP_RETURN

Puedes especificar exactamente cómo deben distribuirse los ZELD incluyendo una salida OP_RETURN en tu transacción con datos de distribución personalizados. Esto permite un control preciso sobre las transferencias de ZELD.

4.2.1 Formato OP_RETURN:

- El script OP_RETURN debe contener datos que comiencen con el prefijo de 4 bytes “ZELD”
- Después del prefijo, los datos deben estar codificados en formato CBOR
- Los datos CBOR deben representar un vector de enteros sin signo de 64 bits (Vec)
- Cada entero especifica cuántos ZELD enviar al UTXO de salida correspondiente

4.2.2 Reglas de Distribución:

- El número de valores en el array de distribución se ajusta automáticamente para coincidir con el número de salidas no OP_RETURN
- Si el array es demasiado largo, se eliminan los valores extra
- Si el array es demasiado corto, se añaden ceros
- La suma total de los valores de distribución no puede exceder el total de ZELD que se están gastando
- Si la suma es menor que el total, la diferencia se añade a la primera salida
- Si la suma excede el total, la transacción recurre a la distribución proporcional
- Las recompensas ZELD recién minadas siempre se distribuyen proporcionalmente y luego se combinan con la distribución personalizada

4.2.3 Ejemplo:

Si tienes 1000 ZELD para distribuir entre 3 salidas y quieres enviar 600 a la primera, 300 a la segunda y 100 a la tercera, tu OP_RETURN contendría “ZELD” seguido de la codificación CBOR de [600, 300, 100].

Notas:

- Si no se encuentra una distribución OP_RETURN válida, la transacción utiliza automáticamente el método de distribución proporcional.
- Si una transacción contiene solo una salida OP_RETURN, cualquier ZELD adjunto a las entradas de la transacción **y cualquier recompensa recién ganada** se queman permanentemente porque no hay salidas gastables para recibirlos.
- Cuando hay varias salidas OP_RETURN presentes, solo se considera para la distribución la que aparece en último lugar en la transacción y que lleva una carga útil `ZELD`+CBOR válida.