PROTOCOLO ZELDHASH

Caçe as transações mais raras do Bitcoin e ganhe ZELD.

Por Ouziel Slama

1 Motivações

- Pela emoção da caça. Cada transação se torna uma oportunidade de descobrir algo raro — um tesouro digital escondido à vista de todos na blockchain.
- Esses padrões de zeros iniciais não são apenas raros — também podem melhorar a compressão, potencialmente otimizando o armazenamento e a eficiência de processamento da blockchain.
- Qualquer pessoa pode ganhar ZELD caçando transações raras — não há um único vencedor por bloco como na mineração de blocos do Bitcoin. A caça está aberta a todos.
- Se bem-sucedido, os tokens ZELD poderiam eventualmente reembolsar taxas de transação — recompensando os caçadores que descobrirem os achados mais raros!

2 Mineração de ZELD

Para minerar ZELD, você deve transmitir uma transação de Bitcoin cujo txid comece com pelo menos 6 zeros. A recompensa é calculada com base em como sua transação se compara à melhor transação do bloco:

- Em um determinado bloco, as transações que começam com mais zeros ganham 4096 ZELD
- Transações com um zero a menos que as melhores transações ganham 4096/16 ou 256 ZELD
- Transações com dois zeros a menos ganham 4096 / 16 / 16 ou 16 ZELD
- etc.

Portanto, a fórmula utilizada é a seguinte:

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

Onde `max_zero_count` é igual ao número de zeros que iniciam a melhor transação e `zero_count` é o número de zeros que iniciam a transação para a qual calculamos a recompensa.

Nota: Transações Coinbase não são elegíveis para recompensas ZELD.

3 Distribuição de ZELD

Os ZELDs ganhos com uma transação que começa com 6 ou mais zeros são distribuídos para UTXOs. A distribuição é realizada da seguinte forma:

- Se houver um único UTXO não OP_RETURN, ele recebe toda a recompensa.
- Se houver dois ou mais UTXOs não OP_RETURN, a recompensa é distribuída para todos os UTXOs, exceto o último, proporcionalmente ao valor de cada UTXO

- Como os cálculos são feitos apenas com inteiros, o possível resto da divisão é distribuído para o primeiro UTXO não OP_RETURN.

Por exemplo, se uma transação que ganha 256 ZELD contém 4 saídas com 500, 500, 500 e 2000 Satoshis respectivamente, a primeira saída recebe 86 ZELD da recompensa, a segunda e terceira 85 ZELD.

4 Movimentação de ZELD

Quando UTXOs com ZELDs anexados são gastos, os ZELDs são distribuídos para os novos UTXOs na transação. Existem dois métodos para distribuir ZELDs ao movê-los:

4.1 Método 1: Distribuição Proporcional Automática

Por padrão, a distribuição é feita exatamente da mesma forma que as recompensas — proporcionalmente com base nos valores de Bitcoin dos UTXOs de saída, excluindo a última saída se houver múltiplas saídas.

4.2 Método 2: Distribuição Personalizada via OP_RETURN

Você pode especificar exatamente como os ZELDs devem ser distribuídos incluindo uma saída OP_RETURN em sua transação com dados de distribuição personalizados. Isso permite controle preciso sobre transferências de ZELD.

4.2.1 Formato OP_RETURN:

- O script OP_RETURN deve conter dados que começam com o prefixo de 4 bytes "ZELD"
- Após o prefixo, os dados devem ser codificados no formato CBOR
- Os dados CBOR devem representar um vetor de inteiros sem sinal de 64 bits (Vec)
- Cada inteiro especifica quantos ZELDs enviar para o UTXO de saída correspondente

4.2.2 Regras de Distribuição:

- O número de valores no array de distribuição é automaticamente ajustado para corresponder ao número de saídas não OP_RETURN
- Se o array for muito longo, os valores extras são removidos
- Se o array for muito curto, zeros são adicionados
- A soma total dos valores de distribuição não pode exceder o total de ZELDs sendo gastos
- Se a soma for menor que o total, a diferença é adicionada à primeira saída
- Se a soma exceder o total, a transação recorre à distribuição proporcional
- As recompensas ZELD recém-mineradas são sempre distribuídas proporcionalmente e depois combinadas com a distribuição personalizada

4.2.3 Exemplo:

Se você tem 1000 ZELDs para distribuir entre 3 saídas e quer enviar 600 para a primeira, 300 para a segunda e 100 para a terceira, seu OP_RETURN conteria "ZELD" seguido pela codificação CBOR de [600, 300, 100].

Notas:

- Se nenhuma distribuição OP_RETURN válida for encontrada, a transação automaticamente usa o método de distribuição proporcional.
- Se uma transação contém apenas uma saída OP_RETURN, quaisquer ZELDs anexados às entradas da transação **e quaisquer recompensas recém-ganhas** são permanentemente queimados porque não há saídas gastáveis para recebê-los.
- Quando várias saídas OP_RETURN estão presentes, apenas aquela que aparece por último na transação e que carrega uma carga útil `ZELD`+CBOR válida é considerada para distribuição.