PROTOCOLE ZELDHASH

Chassez les transactions Bitcoin les plus rares et gagnez des ZELD.

Par Ouziel Slama

1 Motivations

- Pour le frisson de la chasse. Chaque transaction devient une opportunité de découvrir quelque chose de rare — un trésor numérique caché à la vue de tous sur la blockchain.
- Ces motifs de zéros en tête ne sont pas seulement rares — ils pourraient également améliorer la compression, optimisant potentiellement le stockage et l'efficacité du traitement de la blockchain.
- N'importe qui peut gagner des ZELD en chassant les transactions rares — pas de gagnant unique par bloc comme dans le minage de blocs Bitcoin. La chasse est ouverte à tous.
- En cas de succès, les tokens ZELD pourraient éventuellement rembourser les frais de transaction — récompensant les chasseurs qui découvrent les trouvailles les plus rares !

2 Minage de ZELD

Pour miner des ZELD, vous devez diffuser une transaction Bitcoin dont le txid commence par au moins 6 zéros. La récompense est calculée en fonction de la comparaison de votre transaction avec la meilleure transaction du bloc :

- Dans un bloc donné, les transactions commençant par le plus de zéros gagnent 4096 ZELD
- Les transactions avec un zéro de moins que les meilleures transactions gagnent 4096/16 ou 256 ZELD
- Les transactions avec deux zéros de moins gagnent 4096 / 16 / 16 ou 16 ZELD
- etc.

La formule utilisée est donc la suivante :

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

Avec `max_zero_count` égal au nombre de zéros par lesquels commence la meilleure transaction et `zero_count` le nombre de zéros par lesquels commence la transaction pour laquelle nous calculons la récompense.

Note : Les transactions Coinbase ne sont pas éligibles aux récompenses ZELD.

3 Distribution des ZELD

Les ZELD gagnés avec une transaction commençant par 6 zéros ou plus sont distribués aux UTXOs. La distribution s'effectue comme suit :

- S'il y a un seul UTXO non-OP_RETURN, il reçoit la totalité de la récompense.
- S'il y a deux ou plusieurs UTXOs non-OP_RETURN, la récompense est distribuée à tous les UTXOs, sauf le dernier, proportionnellement à la valeur de chaque UTXO

- Les calculs étant effectués uniquement avec des entiers, le reste éventuel de la division est distribué au premier UTXO non-OP_RETURN.

Par exemple, si une transaction gagnant 256 ZELD contient 4 sorties avec respectivement 500, 500, 500 et 2000 Satoshis, la première sortie reçoit 86 ZELD de la récompense, la deuxième et la troisième 85 ZELD.

4 Déplacement des ZELD

Lorsque des UTXOs avec des ZELD attachés sont dépensés, les ZELD sont distribués aux nouveaux UTXOs dans la transaction. Il existe deux méthodes pour distribuer les ZELD lors de leur déplacement :

4.1 Méthode 1 : Distribution proportionnelle automatique

Par défaut, la distribution s'effectue exactement de la même manière que les récompenses — proportionnellement en fonction des valeurs Bitcoin des UTXOs de sortie, en excluant la dernière sortie s'il y en a plusieurs.

4.2 Méthode 2 : Distribution personnalisée via OP_RETURN

Vous pouvez spécifier exactement comment les ZELD doivent être distribués en incluant une sortie OP_RETURN dans votre transaction avec des données de distribution personnalisées. Cela permet un contrôle précis sur les transferts de ZELD.

4.2.1 Format OP_RETURN :

- Le script OP_RETURN doit contenir des données commençant par le préfixe de 4 octets "ZELD"
- Après le préfixe, les données doivent être encodées au format CBOR
- Les données CBOR doivent représenter un vecteur d'entiers non signés de 64 bits (Vec)
- Chaque entier spécifie combien de ZELD envoyer à l'UTXO de sortie correspondant

4.2.2 Règles de distribution :

- Le nombre de valeurs dans le tableau de distribution est automatiquement ajusté pour correspondre au nombre de sorties non-OP_RETURN
- Si le tableau est trop long, les valeurs supplémentaires sont supprimées
- Si le tableau est trop court, des zéros sont ajoutés
- La somme totale des valeurs de distribution ne peut pas dépasser le total des ZELD dépensés
- Si la somme est inférieure au total, la différence est ajoutée à la première sortie
- Si la somme dépasse le total, la transaction revient à la distribution proportionnelle
- Les récompenses ZELD nouvellement minées sont toujours distribuées proportionnellement puis combinées avec la distribution personnalisée

4.2.3 Exemple :

Si vous avez 1000 ZELD à distribuer sur 3 sorties et souhaitez envoyer 600 à la première, 300 à la deuxième et 100 à la troisième, votre OP_RETURN contiendra "ZELD" suivi de l'encodage CBOR de [600, 300, 100].

Notes :

- Si aucune distribution OP_RETURN valide n'est trouvée, la transaction utilise automatiquement la méthode de distribution proportionnelle.
- Si une transaction ne contient qu'une seule sortie OP_RETURN, tous les ZELD attachés aux entrées de la transaction **ainsi que toutes les récompenses nouvellement gagnées** sont définitivement brûlés car il n'y a pas de sorties dépensables pour les recevoir.
- Lorsque plusieurs sorties OP_RETURN sont présentes, seule celle apparaissant en dernier dans la transaction et portant une charge utile `ZELD`+CBOR valide est prise en compte pour la distribution.