PROTOKOL ZELDHASH

Berburu Transaksi Bitcoin Paling Langka dan Dapatkan ZELD.

Oleh Ouziel Slama

1 Motivasi

- Demi sensasi berburu. Setiap transaksi menjadi peluang untuk menemukan sesuatu yang langka — harta karun digital yang tersembunyi di depan mata di blockchain.
- Pola nol di depan ini tidak hanya langka — mereka juga dapat meningkatkan kompresi, berpotensi menyederhanakan penyimpanan dan efisiensi pemrosesan blockchain.
- Siapa pun dapat mendapatkan ZELD dengan berburu transaksi langka — tidak seperti penambangan blok Bitcoin dengan pemenang tunggal per blok. Perburuan terbuka untuk semua.
- Jika berhasil, token ZELD akhirnya dapat mengganti biaya transaksi — memberi hadiah kepada pemburu yang mengungkap temuan paling langka!

2 Penambangan ZELD

Untuk menambang ZELD, Anda harus menyiarkan transaksi Bitcoin yang txid-nya dimulai dengan setidaknya 6 nol. Hadiah dihitung berdasarkan bagaimana transaksi Anda dibandingkan dengan transaksi terbaik di blok:

- Dalam blok tertentu, transaksi yang dimulai dengan nol terbanyak mendapatkan 4096 ZELD
- Transaksi dengan satu nol lebih sedikit dari transaksi terbaik mendapatkan 4096/16 atau 256 ZELD
- Transaksi dengan dua nol lebih sedikit mendapatkan 4096 / 16 / 16 atau 16 ZELD
- dst.

Oleh karena itu, rumus yang digunakan adalah sebagai berikut:

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

Dengan `max_zero_count` sama dengan jumlah nol yang memulai transaksi terbaik dan `zero_count` adalah jumlah nol yang memulai transaksi yang hadiahnya kita hitung.

Catatan: Transaksi Coinbase tidak memenuhi syarat untuk hadiah ZELD.

3 Distribusi ZELD

ZELD yang diperoleh dengan transaksi yang dimulai dengan 6 atau lebih nol didistribusikan ke UTXO. Distribusi dilakukan sebagai berikut:

- Jika ada satu UTXO non-OP_RETURN, ia menerima seluruh hadiah.
- Jika ada dua atau lebih UTXO non-OP_RETURN, hadiah didistribusikan ke semua UTXO, kecuali yang terakhir, secara proporsional dengan nilai setiap UTXO

- Karena perhitungan dilakukan hanya dengan bilangan bulat, kemungkinan sisa pembagian didistribusikan ke UTXO non-OP_RETURN pertama.

Misalnya, jika transaksi yang mendapatkan 256 ZELD berisi 4 output dengan masing-masing 500, 500, 500, dan 2000 Satoshi, output pertama menerima 86 ZELD dari hadiah, yang kedua dan ketiga 85 ZELD.

4 Memindahkan ZELD

Ketika UTXO dengan ZELD terlampir dihabiskan, ZELD didistribusikan ke UTXO baru dalam transaksi. Ada dua metode untuk mendistribusikan ZELD saat memindahkannya:

4.1 Metode 1: Distribusi Proporsional Otomatis

Secara default, distribusi dilakukan dengan cara yang sama persis seperti hadiah — secara proporsional berdasarkan nilai Bitcoin dari UTXO output, tidak termasuk output terakhir jika ada beberapa output.

4.2 Metode 2: Distribusi Kustom melalui OP_RETURN

Anda dapat menentukan dengan tepat bagaimana ZELD harus didistribusikan dengan menyertakan output OP_RETURN dalam transaksi Anda dengan data distribusi kustom. Ini memungkinkan kontrol yang tepat atas transfer ZELD.

4.2.1 Format OP_RETURN:

- Skrip OP_RETURN harus berisi data yang dimulai dengan prefiks 4-byte “ZELD”
- Setelah prefiks, data harus dikodekan dalam format CBOR
- Data CBOR harus mewakili vektor bilangan bulat tak bertanda 64-bit (Vec)
- Setiap bilangan bulat menentukan berapa banyak ZELD yang akan dikirim ke UTXO output yang sesuai

4.2.2 Aturan Distribusi:

- Jumlah nilai dalam array distribusi secara otomatis disesuaikan agar sesuai dengan jumlah output non-OP_RETURN
- Jika array terlalu panjang, nilai ekstra dihapus
- Jika array terlalu pendek, nol ditambahkan
- Jumlah total nilai distribusi tidak boleh melebihi total ZELD yang dihabiskan
- Jika jumlahnya kurang dari total, selisihnya ditambahkan ke output pertama
- Jika jumlahnya melebihi total, transaksi kembali ke distribusi proporsional
- Hadiah ZELD yang baru ditambang selalu didistribusikan secara proporsional dan kemudian digabungkan dengan distribusi kustom

4.2.3 Contoh:

Jika Anda memiliki 1000 ZELD untuk didistribusikan ke 3 output dan ingin mengirim 600 ke yang pertama, 300 ke yang kedua, dan 100 ke yang ketiga, OP_RETURN Anda akan berisi “ZELD” diikuti oleh pengkodean CBOR dari [600, 300, 100].

Catatan:

- Jika tidak ditemukan distribusi OP_RETURN yang valid, transaksi secara otomatis menggunakan metode distribusi proporsional.
- Jika transaksi hanya berisi satu output OP_RETURN, ZELD apa pun yang terlampir pada input transaksi **dan hadiah yang baru diperoleh** akan dibakar secara permanen karena tidak ada output yang dapat dihabiskan untuk menerimanya.
- Ketika beberapa output OP_RETURN hadir, hanya yang muncul terakhir dalam transaksi dan membawa payload `ZELD`+CBOR yang valid yang dipertimbangkan untuk distribusi.