PROTOKOL ZELDHASH

Buru Transaksi Bitcoin Paling Jarang dan Peroleh ZELD.

Oleh Ouziel Slama

1 Motivasi

- Untuk keseronokan memburu. Setiap transaksi menjadi peluang untuk menemui sesuatu yang jarang — khazanah digital yang tersembunyi di depan mata pada blockchain.
- Corak sifar hadapan ini bukan sahaja jarang — ia juga boleh meningkatkan pemampatan, berpotensi memperkemas penyimpanan blockchain dan kecekapan pemprosesan.
- Sesiapa sahaja boleh memperoleh ZELD dengan memburu transaksi jarang — tiada pemenang tunggal setiap blok seperti dalam perlombongan blok Bitcoin. Pemburuan terbuka kepada semua.
- Jika berjaya, token ZELD akhirnya boleh membayar balik yuran transaksi — memberi ganjaran kepada pemburu yang menemui penemuan paling jarang!

2 Perlombongan ZELD

Untuk melombong ZELD anda mesti menyiarkan transaksi Bitcoin yang txid bermula dengan sekurang-kurangnya 6 sifar. Ganjaran dikira berdasarkan bagaimana transaksi anda berbanding dengan transaksi terbaik dalam blok:

- Dalam blok tertentu, transaksi yang bermula dengan sifar paling banyak memperoleh 4096 ZELD
- Transaksi dengan satu sifar kurang daripada transaksi terbaik memperoleh 4096/16 atau 256 ZELD
- Transaksi dengan dua sifar kurang memperoleh 4096 / 16 / 16 atau 16 ZELD
- dsb.

Oleh itu formula yang digunakan adalah seperti berikut:

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

Di mana `max_zero_count` sama dengan bilangan sifar yang memulakan transaksi terbaik dan `zero_count` adalah bilangan sifar yang memulakan transaksi yang kita kira ganjarannya.

Nota: Transaksi Coinbase tidak layak untuk ganjaran ZELD.

3 Pengagihan ZELD

ZELD yang diperoleh dengan transaksi yang bermula dengan 6 atau lebih sifar diagihkan kepada UTXO. Pengagihan dilakukan seperti berikut:

- Jika terdapat satu UTXO bukan-OP_RETURN, ia menerima keseluruhan ganjaran.
- Jika terdapat dua atau lebih UTXO bukan-OP_RETURN, ganjaran diagihkan kepada semua UTXO, kecuali yang terakhir, secara berkadar dengan nilai setiap UTXO

- Memandangkan pengiraan dibuat hanya dengan integer, baki pembahagian yang mungkin diagihkan kepada UTXO bukan-OP_RETURN pertama.

Sebagai contoh, jika transaksi yang memperoleh 256 ZELD mengandungi 4 output dengan 500, 500, 500 dan 2000 Satoshi masing-masing, output pertama menerima 86 ZELD daripada ganjaran, yang kedua dan ketiga 85 ZELD.

4 Memindahkan ZELD

Apabila UTXO dengan ZELD yang dilampirkan dibelanjakan, ZELD diagihkan kepada UTXO baharu dalam transaksi. Terdapat dua kaedah untuk mengagihkan ZELD semasa memindahkannya:

4.1 Kaedah 1: Pengagihan Berkadar Automatik

Secara lalai, pengagihan dilakukan dengan cara yang sama seperti ganjaran — secara berkadar berdasarkan nilai Bitcoin UTXO output, tidak termasuk output terakhir jika terdapat berbilang output.

4.2 Kaedah 2: Pengagihan Tersuai melalui OP_RETURN

Anda boleh menentukan dengan tepat bagaimana ZELD harus diagihkan dengan memasukkan output OP_RETURN dalam transaksi anda dengan data pengagihan tersuai. Ini membolehkan kawalan tepat ke atas pemindahan ZELD.

4.2.1 Format OP_RETURN:

- Skrip OP_RETURN mesti mengandungi data yang bermula dengan awalan 4-bait “ZELD”
- Selepas awalan, data mesti dikodkan dalam format CBOR
- Data CBOR harus mewakili vektor integer 64-bit tanpa tanda (Vec)
- Setiap integer menentukan berapa banyak ZELD untuk dihantar ke UTXO output yang sepadan

4.2.2 Peraturan Pengagihan:

- Bilangan nilai dalam tatasusunan pengagihan diselaraskan secara automatik untuk sepadan dengan bilangan output bukan-OP_RETURN
- Jika tatasusunan terlalu panjang, nilai tambahan dibuang
- Jika tatasusunan terlalu pendek, sifar ditambah
- Jumlah keseluruhan nilai pengagihan tidak boleh melebihi jumlah ZELD yang dibelanjakan
- Jika jumlah kurang daripada jumlah keseluruhan, perbezaan ditambah ke output pertama
- Jika jumlah melebihi jumlah keseluruhan, transaksi kembali kepada pengagihan berkadar
- Ganjaran ZELD yang baru dilombong sentiasa diagihkan secara berkadar dan kemudian digabungkan dengan pengagihan tersuai

4.2.3 Contoh:

Jika anda mempunyai 1000 ZELD untuk diagihkan kepada 3 output dan mahu menghantar 600 kepada yang pertama, 300 kepada yang kedua, dan 100 kepada yang ketiga, OP_RETURN anda akan mengandungi “ZELD” diikuti dengan pengekodan CBOR bagi [600, 300, 100].

Nota:

- Jika tiada pengagihan OP_RETURN yang sah dijumpai, transaksi secara automatik menggunakan kaedah pengagihan berkadar.
- Jika transaksi hanya mengandungi satu output OP_RETURN, sebarang ZELD yang dilampirkan pada input transaksi **dan sebarang ganjaran yang baru diperoleh** dibakar secara kekal kerana tiada output yang boleh dibelanjakan untuk menerimanya.
- Apabila berbilang output OP_RETURN hadir, hanya yang muncul terakhir dalam transaksi dan membawa muatan `ZELD`+CBOR yang sah dipertimbangkan untuk pengagihan.