

# ITIFAKI YA ZELDHASH

## Winda Miamala ya Bitcoin Adimu Zaidi na Upate ZELD.

Na Ouziel Slama

### 1 Motisha

- Kwa msisimko wa uwindaji. Kila muamala unakuwa fursa ya kugundua kitu adimu — hazina ya kidijitali iliyofichwa wazi kwenye blockchain.
- Mifumo hii ya sufuri za mbele si adimu tu — inaweza pia kuboresha ubanaji, ikiweza kurahisisha uhifadhi wa blockchain na ufanisi wa usindikaji.
- Mtu yeyote anaweza kupata ZELD kwa kuwinda miamala adimu — hakuna mshindi mmoja kwa kila block kama katika uchimbaji wa block za Bitcoin. Uwindaji uko wazi kwa wote.
- Ikiwa itafanikiwa, tokeni za ZELD zinaweza hatimaye kurudisha ada za miamala — kuwatuza wawindaji wanaogundua matokeo adimu zaidi!

### 2 Uchimbaji wa ZELD

Ili kuchimba ZELD lazima utangaze muamala wa Bitcoin ambao txid yake inaanza na angalau sufuri 6. Tuzo huhesabiwa kulingana na jinsi muamala wako unavyolinganishwa na muamala bora zaidi katika block:

- Katika block fulani, miamala inayoanza na sufuri nyingi zaidi hupata ZELD 4096
- Miamala yenye sufuri moja chini ya miamala bora zaidi hupata 4096/16 au ZELD 256
- Miamala yenye sufuri mbili chini hupata 4096 / 16 / 16 au ZELD 16
- n.k.

Kwa hivyo fomula inayotumika ni kama ifuatavyo:

$$\text{reward} = 4096 / 16 ^ {(\text{max\_zero\_count} - \text{zero\_count})}$$

Ambapo max\_zero\_count ni sawa na idadi ya sufuri zinazoanza muamala bora zaidi na zero\_count ni idadi ya sufuri zinazoanza muamala ambao tunahesabu tuzo yake.

**Kumbuka:** Miamala ya Coinbase haistahiki tuzo za ZELD.

### 3 Usambazaji wa ZELD

ZELD zilizopatikana na muamala unaoanza na sufuri 6 au zaidi zinasambazwa kwa UTXO. Usambazaji unafanywa kama ifuatavyo:

- Ikiwa kuna UTXO moja isiyo-OP\_RETURN, inapokea tuzo yote.
- Ikiwa kuna UTXO mbili au zaidi zisizo-OP\_RETURN, tuzo inasambazwa kwa UTXO zote, isipokuwa ya mwisho, kwa uwiano wa thamani ya kila UTXO

- Kwa kuwa hesabu zinafanywa tu kwa nambari kamili, baki inayowezezekana ya ugawanyaji inasambazwa kwa UTXO ya kwanza isiyo-OP\_RETURN.

Kwa mfano, ikiwa muamala unaopata ZELD 256 una matokeo 4 yenye Satoshi 500, 500, 500 na 2000 mtawalia, tokeo la kwanza linapokea ZELD 86 ya tuzo, la pili na la tatu ZELD 85.

## 4 Kuhamisha ZELD

Wakati UTXO zenye ZELD zilizoshikamishwa zinatumiwa, ZELD zinasambazwa kwa UTXO mpya katika muamala. Kuna njia mbili za kusambaza ZELD wakati wa kuzihamisha:

### 4.1 Njia ya 1: Usambazaji wa Uwiano wa Kiotomatiki

Kwa chaguo-msingi, usambazaji unafanywa kwa njia sawa kabisa na tuzo — kwa uwiano kulingana na thamani za Bitcoin za UTXO za matokeo, bila kujumuisha tokeo la mwisho ikiwa kuna matokeo mengi.

### 4.2 Njia ya 2: Usambazaji Maalum kupitia OP\_RETURN

Unaweza kubainisha haswa jinsi ZELD zinavyopaswa kusambazwa kwa kujumuisha tokeo la OP\_RETURN katika muamala wako na data ya usambazaji maalum. Hii inaruhusu udhibiti sahihi wa uhamisho wa ZELD.

#### 4.2.1 Umbizo la OP\_RETURN:

- Hati ya OP\_RETURN lazima iwe na data inayoanza na kiambishi cha byte 4 “ZELD”
- Baada ya kiambishi, data lazima ichukuliwe katika umbizo la CBOR
- Data ya CBOR inapaswa kuwakilisha vekta ya nambari kamili za 64-bit zisizo na ishara (Vec)
- Kila nambari kamili inabainisha ni ZELD ngapi zitumwe kwa UTXO ya tokeo inayolingana

#### 4.2.2 Sheria za Usambazaji:

- Idadi ya thamani katika safu ya usambazaji inarekebishwa kiotomatiki ili kulingana na idadi ya matokeo yasiyo-OP\_RETURN
- Ikiwa safu ni ndefu sana, thamani za ziada zinaondolewa
- Ikiwa safu ni fupi sana, sufuri zinaongezwa
- Jumla ya thamani za usambazaji haiwezi kuzidi jumla ya ZELD zinazotumika
- Ikiwa jumla ni chini ya jumla yote, tofauti inaongezwa kwa tokeo la kwanza
- Ikiwa jumla inazidi jumla yote, muamala unarudi kwenye usambazaji wa uwiano
- Tuzo za ZELD zilizochimbwa hivi karibuni zinasambazwa kwa uwiano kila wakati na kisha kuunganishwa na usambazaji maalum

#### 4.2.3 Mfano:

Ikiwa una ZELD 1000 za kusambaza kwa matokeo 3 na unataka kutuma 600 kwa la kwanza, 300 kwa la pili, na 100 kwa la tatu, OP\_RETURN yako itakuwa na “ZELD” ikifuatiwa na usimbuaji wa CBOR wa [600, 300, 100].

#### Vidokezo:

- Ikiwa usambazaji wa OP\_RETURN halali haupatikani, muamala unatumia kiotomatiki njia ya usambazaji wa uwiano.
- Ikiwa muamala una tokeo moja tu la OP\_RETURN, ZELD zozote zilizoshikamishwa kwa pembejeo za muamala **na tuzo zozote mpya zilizopatikana** zinachomwa kabisa kwa sababu hakuna matokeo yanayoweza kutumika kuzipokea.
- Wakati matokeo mengi ya OP\_RETURN yapo, ni lile tu linaloonekana mwisho katika muamala na kubeba mzigo halali wa ZELD+CBOR linazingatiwa kwa usambazaji.