PROTOKOL NG ZELDHASH

Mangaso ng Pinakabihirang Transaksyon ng Bitcoin at Kumita ng ZELD.

Ni Ouziel Slama

1 Mga Motibasyon

- Para sa kasiyahan ng pangangaso. Ang bawat transaksyon ay nagiging pagkakataon upang matuklasan ang isang bagay na bihira — isang digital na kayamanan na nakatago sa harap-harapan sa blockchain.
- Ang mga pattern ng mga naunang zero ay hindi lamang bihira — maaari rin nitong mapahusay ang compression, na potensyal na mag-streamline ng blockchain storage at processing efficiency.
- Kahit sino ay maaaring kumita ng ZELD sa pamamagitan ng pangangaso ng mga bihirang transaksyon — walang iisang mananalo bawat block tulad ng sa Bitcoin block mining. Ang pangangaso ay bukas sa lahat.
- Kung matagumpay, ang mga ZELD token ay maaaring sa kalaunan ay magbayad ng mga transaction fee — gantimpalaan ang mga mangangaso na nakahanap ng pinakabihirang mga natuklasan!

2 Pagmimina ng ZELD

Upang mag-mina ng ZELD kailangan mong mag-broadcast ng Bitcoin transaction kung saan ang txid ay nagsisimula sa hindi bababa sa 6 na zero. Ang gantimpala ay kinakalkula batay sa kung paano ang iyong transaksyon ay inihahambing sa pinakamagandang transaksyon sa block:

- Sa isang partikular na block, ang mga transaksyon na nagsisimula sa pinakamaraming zero ay kumikita ng 4096 ZELD
- Ang mga transaksyon na may isang zero na mas kaunti kaysa sa pinakamahusay na transaksyon ay kumikita ng 4096/16 o 256 ZELD
- Ang mga transaksyon na may dalawang zero na mas kaunti ay kumikita ng 4096 / 16 / 16 o 16 ZELD
- atbp.

Samakatuwid ang pormulang ginagamit ay ang mga sumusunod:

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

Kung saan ang `max_zero_count` ay katumbas ng bilang ng mga zero na nagsisimula sa pinakamahusay na transaksyon at ang `zero_count` ay ang bilang ng mga zero na nagsisimula sa transaksyon kung saan kinakalkula natin ang gantimpala.

Tandaan: Ang mga Coinbase transaction ay hindi karapat-dapat para sa mga ZELD reward.

3 Pamamahagi ng ZELD

Ang mga ZELD na nakuha sa isang transaksyon na nagsisimula sa 6 o higit pang zero ay ipinamamahagi sa mga UTXO. Ang pamamahagi ay isinasagawa tulad ng sumusunod:

- Kung may iisang non-OP_RETURN UTXO, tinatanggap nito ang buong gantimpala.
- Kung may dalawa o higit pang non-OP_RETURN UTXO, ang gantimpala ay ipinamamahagi sa lahat ng UTXO, maliban sa huli, na proporsyonal sa halaga ng bawat UTXO
- Dahil ang mga kalkulasyon ay ginagawa lamang gamit ang mga integer, ang posibleng natitira sa dibisyon ay ipinamamahagi sa unang non-OP_RETURN UTXO.

Halimbawa, kung ang isang transaksyon na kumikita ng 256 ZELD ay naglalaman ng 4 na output na may 500, 500, 500 at 2000 Satoshi ayon sa pagkakasunod-sunod, ang unang output ay tumatanggap ng 86 ZELD ng gantimpala, ang ikalawa at ikatlo ay 85 ZELD.

4 Paglipat ng ZELD

Kapag ang mga UTXO na may nakalakip na ZELD ay ginastos, ang mga ZELD ay ipinamamahagi sa mga bagong UTXO sa transaksyon. May dalawang paraan para sa pamamahagi ng ZELD kapag inililipat ang mga ito:

4.1 Paraan 1: Awtomatikong Proporsyonal na Pamamahagi

Bilang default, ang pamamahagi ay ginagawa sa eksaktong parehong paraan tulad ng mga gantimpala — proporsyonal batay sa Bitcoin values ng output UTXO, hindi kasama ang huling output kung maraming output.

4.2 Paraan 2: Custom na Pamamahagi sa pamamagitan ng OP_RETURN

Maaari mong tukuyin kung paano eksaktong dapat ipamahagi ang mga ZELD sa pamamagitan ng pagsasama ng OP_RETURN output sa iyong transaksyon na may custom na distribution data. Ito ay nagbibigay-daan sa tumpak na kontrol sa mga ZELD transfer.

4.2.1 Format ng OP_RETURN:

- Ang OP_RETURN script ay dapat maglaman ng data na nagsisimula sa 4-byte prefix na “ZELD”
- Pagkatapos ng prefix, ang data ay dapat naka-encode sa CBOR format
- Ang CBOR data ay dapat kumatawan sa isang vector ng unsigned 64-bit integers (Vec)
- Ang bawat integer ay tumutukoy kung ilang ZELD ang ipapadala sa katumbas na output UTXO

4.2.2 Mga Panuntunan sa Pamamahagi:

- Ang bilang ng mga halaga sa distribution array ay awtomatikong inaayos upang tumugma sa bilang ng non-OP_RETURN outputs
- Kung ang array ay masyadong mahaba, ang mga extra na halaga ay tinatanggal
- Kung ang array ay masyadong maikli, mga zero ang idinaragdag
- Ang kabuuang halaga ng distribution values ay hindi maaaring lumampas sa kabuuang ZELD na ginagastos
- Kung ang kabuuan ay mas kaunti kaysa sa total, ang pagkakaiba ay idinaragdag sa unang output
- Kung ang kabuuan ay lumampas sa total, ang transaksyon ay babalik sa proporsyonal na pamamahagi

- Ang mga bagong na-mine na ZELD reward ay palaging ipinamamahagi nang proporsyonal at pagkatapos ay pinagsasama sa custom na pamamahagi

4.2.3 Halimbawa:

Kung mayroon kang 1000 ZELD na ipapamahagi sa 3 output at nais mong magpadala ng 600 sa una, 300 sa ikalawa, at 100 sa ikatlo, ang iyong OP_RETURN ay maglalaman ng “ZELD” na sinusundan ng CBOR encoding ng [600, 300, 100].

Mga Tala:
- Kung walang nahanap na valid na OP_RETURN distribution, ang transaksyon ay awtomatikong gumagamit ng proporsyonal na paraan ng pamamahagi.
- Kung ang isang transaksyon ay naglalaman lamang ng isang OP_RETURN output, anumang ZELD na nakalakip sa mga input ng transaksyon **at anumang bagong nakuhang gantimpala** ay permanenteng sinusunog dahil walang mga magagastos na output upang matanggap ang mga ito.
- Kapag maraming OP_RETURN output ang naroroon, tanging ang lumilitaw na huli sa transaksyon at nagdadala ng valid na `ZELD`+CBOR payload ang itinuturing para sa pamamahagi.