

ΠΡΩΤΟΚΟΛΛΟ ZELDHASH

Κυνηγήστε τις πιο σπάνιες συναλλαγές Bitcoin και κερδίστε ZELD.

Από τον Ouziel Slama

1 Κίνητρα

- Για τη συγκίνηση του κυνηγιού. Κάθε συναλλαγή γίνεται ευκαιρία να ανακαλύψετε κάτι σπάνιο — ένας ψηφιακός θησαυρός κρυμμένος σε κοινή θέα στο blockchain.
- Αυτά τα μοτίβα αρχικών μηδενικών δεν είναι μόνο σπάνια — θα μπορούσαν επίσης να βελτιώσουν τη συμπίεση, πιθανώς βελτιστοποιώντας την αποθήκευση blockchain και την αποδοτικότητα επεξεργασίας.
- Οποιοσδήποτε μπορεί να κερδίσει ZELD κυνηγώντας σπάνιες συναλλαγές — χωρίς έναν μόνο νικητή ανά block όπως στην εξόρυξη block Bitcoin. Το κυνήγι είναι ανοιχτό σε όλους.
- Εάν επιτύχει, τα token ZELD θα μπορούσαν τελικά να επιστρέψουν τα τέλη συναλλαγών — ανταμείβοντας τους κυνηγούς που ανακαλύπτουν τα πιο σπάνια ευρήματα!

2 Εξόρυξη ZELD

Για να εξορύξετε ZELD πρέπει να μεταδώσετε μια συναλλαγή Bitcoin της οποίας το txid ξεκινά με τουλάχιστον 6 μηδενικά. Η ανταμοιβή υπολογίζεται με βάση το πώς συγκρίνεται η συναλλαγή σας με την καλύτερη συναλλαγή στο block:

- Σε ένα δεδομένο block, οι συναλλαγές που ξεκινούν με τα περισσότερα μηδενικά κερδίζουν 4096 ZELD
- Οι συναλλαγές με ένα μηδενικό λιγότερο από τις καλύτερες συναλλαγές κερδίζουν $4096/16$ ή 256 ZELD
- Οι συναλλαγές με δύο λιγότερα μηδενικά κερδίζουν $4096 / 16 / 16$ ή 16 ZELD
- κ.λπ.

Επομένως ο τύπος που χρησιμοποιείται είναι ο εξής:

$$\text{reward} = 4096 / 16 ^ {(\text{max_zero_count} - \text{zero_count})}$$

Όπου `max_zero_count` ισούται με τον αριθμό των μηδενικών που ξεκινούν την καλύτερη συναλλαγή και `zero_count` είναι ο αριθμός των μηδενικών που ξεκινούν τη συναλλαγή για την οποία υπολογίζουμε την ανταμοιβή.

Σημείωση: Οι συναλλαγές Coinbase δεν είναι επιλέξιμες για ανταμοιβές ZELD.

3 Διανομή ZELD

Τα ZELD που κερδίζονται με μια συναλλαγή που ξεκινά με 6 ή περισσότερα μηδενικά διανέμονται σε UTXO. Η διανομή γίνεται ως εξής:

- Εάν υπάρχει ένα μόνο μη-OP_RETURN UTXO, λαμβάνει ολόκληρη την ανταμοιβή.

- Εάν υπάρχουν δύο ή περισσότερα μη-OP_RETURN UTXO, η ανταμοιβή διανέμεται σε όλα τα UTXO, εκτός από το τελευταίο, αναλογικά με την αξία κάθε UTXO
- Δεδομένου ότι οι υπολογισμοί γίνονται μόνο με ακέραιους, το πιθανό υπόλοιπο της διαίρεσης διανέμεται στο πρώτο μη-OP_RETURN UTXO.

Για παράδειγμα, εάν μια συναλλαγή που κερδίζει 256 ZELD περιέχει 4 εξόδους με 500, 500, 500 και 2000 Satoshi αντίστοιχα, η πρώτη έξοδος λαμβάνει 86 ZELD από την ανταμοιβή, η δεύτερη και η τρίτη 85 ZELD.

4 Μετακίνηση ZELD

Όταν ξοδεύονται UTXO με συνημμένα ZELD, τα ZELD διανέμονται στα νέα UTXO στη συναλλαγή. Υπάρχουν δύο μέθοδοι για τη διανομή ZELD κατά τη μετακίνησή τους:

4.1 Μέθοδος 1: Αυτόματη Αναλογική Διανομή

Από προεπιλογή, η διανομή γίνεται ακριβώς με τον ίδιο τρόπο όπως οι ανταμοιβές — αναλογικά με βάση τις αξίες Bitcoin των UTXO εξόδου, εξαιρουμένης της τελευταίας εξόδου εάν υπάρχουν πολλαπλές εξόδοι.

4.2 Μέθοδος 2: Προσαρμοσμένη Διανομή μέσω OP_RETURN

Μπορείτε να καθορίσετε ακριβώς πώς πρέπει να διανεμηθούν τα ZELD συμπεριλαμβάνοντας μια έξοδο OP_RETURN στη συναλλαγή σας με προσαρμοσμένα δεδομένα διανομής. Αυτό επιτρέπει τον ακριβή έλεγχο των μεταφορών ZELD.

4.2.1 Μορφή OP_RETURN:

- Το script OP_RETURN πρέπει να περιέχει δεδομένα που ξεκινούν με το πρόθεμα 4 byte “ZELD”
- Μετά το πρόθεμα, τα δεδομένα πρέπει να κωδικοποιηθούν σε μορφή CBOR
- Τα δεδομένα CBOR πρέπει να αντιπροσωπεύουν ένα διάνυσμα ανυπόγραφων ακεραίων 64-bit (Vec)
- Κάθε ακέραιος καθορίζει πόσα ZELD να σταλούν στο αντίστοιχο UTXO εξόδου

4.2.2 Κανόνες Διανομής:

- Ο αριθμός των τιμών στον πίνακα διανομής προσαρμόζεται αυτόματα ώστε να ταιριάζει με τον αριθμό των μη-OP_RETURN εξόδων
- Εάν ο πίνακας είναι πολύ μεγάλος, οι επιπλέον τιμές αφαιρούνται
- Εάν ο πίνακας είναι πολύ μικρός, προστίθενται μηδενικά
- Το συνολικό άθροισμα των τιμών διανομής δεν μπορεί να υπερβαίνει το σύνολο των ZELD που ξοδεύονται
- Εάν το άθροισμα είναι μικρότερο από το σύνολο, η διαφορά προστίθεται στην πρώτη έξοδο
- Εάν το άθροισμα υπερβαίνει το σύνολο, η συναλλαγή επιστρέφει στην αναλογική διανομή
- Οι νέες ανταμοιβές ZELD από εξόρυξη διανέμονται πάντα αναλογικά και στη συνέχεια συνδυάζονται με την προσαρμοσμένη διανομή

4.2.3 Παράδειγμα:

Εάν έχετε 1000 ZELD για διανομή σε 3 εξόδους και θέλετε να στείλετε 600 στην πρώτη, 300 στη δεύτερη και 100 στην τρίτη, το OP_RETURN σας θα περιέχει “ZELD” ακολουθούμενο από την κωδικοποίηση CBOR του [600, 300, 100].

Σημειώσεις:

- Εάν δεν βρεθεί έγκυρη διανομή OP_RETURN, η συναλλαγή χρησιμοποιεί αυτόματα τη μέθοδο αναλογικής διανομής.
- Εάν μια συναλλαγή περιέχει μόνο μία έξοδο OP_RETURN, οποιαδήποτε ZELD συνδεδεμένα με τις εισόδους της συναλλαγής **και οποιεσδήποτε νέες ανταμοιβές** καίγονται μόνιμα επειδή δεν υπάρχουν δαπανήσιμες έξοδοι για να τα λάβουν.
- Όταν υπάρχουν πολλαπλές έξοδοι OP_RETURN, μόνο αυτή που εμφανίζεται τελευταία στη συναλλαγή και φέρει έγκυρο ωφέλιμο φορτίο ZELD+CBOR λαμβάνεται υπόψη για τη διανομή.