[ΑΝΝ] ZERO – Διακλάδωση του Zcash με ισχυρότερες παραμάτρους εξόρυξης

Το **ZERO** είναι διακλάδωση του Zcash (το Zcash είναι διακλάδωση του Bitcoin). Συνδυάζει την ασφάλεια του Bitcoin, την ιδιωτικότητα του Zcash και επιπρόσθετα κάποιες περαιτέρω βελτιώσεις. Το ZERO εμπεριέχει την καλύτερη τεχνολογία ανωνυμίας και ιδιωτικότητας σήμερα.

**Στόχος της διακλάδωσης είναι:**

* Να τεστάρει τελείως διαφορετικές παραμέτρους βασιζόμενο στον Equihash αλγόριθμο με επιλεγμένες παραμέτρους Ν = 192, Κ=7.
* Οι οποίες θα πρέπει να στοχεύουν σε γενικά προσβάσιμο υλικό για εξόρυξη
* Να αποκτηθεί γνώση απο αυτό

Όλες αυτές οι παράμετροι είναι βελτιωμένες απο τις παρακάτω αλλαγές:

* Υψηλότερη χρονική περιπλοκότητα

Περίπου κατά 16 φορές\*

* Υψηλότερες απαιτήσεις μνήμης

Περίπου κατά 16 φορές\*

* Ταχύτερες επιβεβαιώσεις των blocks

4x

* Μικρότερες λύσεις σε όγκο

400 byte αντί για 1344 byte εισέρχονται σε κάθε block

**Γιατί επελέγησαν αυτές οι παραμέτροι:**

* Για να αποφευχθεί η ιδέα της εξόρυξης σε κινητά τηλέφωνα
* Για να γίνει αρκετά δύσκολο και να καθυστερήσει το ρίσκο των ASICs
* Οι ανάγκες σε μνήμη στοχεύουν σε συμβατικούς υπολογιστές και κάρτες γραφικών με 8GB RAM το λιγότερο.

**Αλλαγές στον διαμοιρασμό των νομισμάτων:**

* Χωρίς ανταμοιβή για τους ιδρυτές
* Χωρίς εξόρυξη προκαταβολικά
* Χωρίς αργό ξεκίνημα
* Χωρίς διαίρεση στη μέση
* Σταθερή παροχή νομισμάτων
* Ελαχιστοποίηση βίαιων στρατηγικών εξόρυξης
* Αφαιρεί το στρεσογόνα χαρακτηριστικά που επηρεάζουν δραματικά τους miners και την τιμή της αγοράς
* Χωρίς ανώτατο όριο νομισμάτων
* Χαμηλές πληθωριστικές τάσεις (που χαμηλώνουν κατά την πάροδο του χρόνου)
* Χαμηλότερο αβαντάζ για αυτούς που μπήκαν νωρίς
* Σταθερή ανταμοιβή για τους miners θα έχει ως αποτέλεσμα χαμηλότερες προμήθειες στο μέλλον
* Τουλάχιστον κάποια ανταμοιβή για χαμένα νομίσματα
* 1 block ανα 2 λεπτά κατά μέσο όρο
* 10 νομίσματα για κάθε block

**Διαμοιρασμός:**

* 7200 νομίσματα/ημέρα (H ίδια αναλογία με το BTC και το Zcash πριν την πρώτη διαίρεση στο μισό
* Μετά απο 1 χρόνο: 2 631 600
* Μετά απο 10 χρόνια: 26 316 000
* Μετά απο 20 χρόνια: 52 632 000
* Μετά απο 30 χρόνια: 78 948 000

**Επιπρόσθετες επιδράσεις των αλλαγών:**

* 4MB ανώτατο μέγεθος του Block
* Γρηγορότερα blocks σε συνδυασμό με το μεγαλύτερο μέγεθος των block και με μικρότερο μήκος λύσεων που επιτρέπει κατά πολύ μεγαλύτερη χωρητικότητα συναλλαγών σε σύγκριση με το Bitcoin και το Zcash.

**Αμετάβλητο:**

* H ίδια αρχική αξιόπιστη ρύθμιση με το Zcash

**Μικρότερες αλλαγές:**

* Το wallet.dat μετονομάστηκε σε wallet.zero (μια μικρή αλλαγή απλά για να το κάνουμε δυσκολότερο σε κακόβουλες επιθέσεις
* Κάθε νέο πορτοφόλι δημιουργείται με 10000 διευθύνσεις για να ελαχιστοποιηθεί ο κίνδυνος να χαθούν νομίσματα απο παλιά backup πορτοφολιών.
* Η ωριμότητα στο coinbase είναι στα 720 blocks (24 ώρες) για να αποφευχθoύν οι συνεχείς μεταβολές στο συνάλλαγμα

**Μελοντικοί στόχοι:**

* Να ενοποιηθούν οι διορθώσεις και οι βελτιώσεις απο το Zcash και το Bitcoin
* Να προστεθεί υποστήριξη για WIN και MAC
* Να αλλαχθούν οι παράμετροι του αλγόριθμου Equihash αν τα ASICS γίνουν διαθέσιμα ή εφικτά
* Αύξηση του μεγέθους του block αν χρειαστεί στο μέλλον

**Ονόματα και σύμβολα:**

* **Όνομα συναλλάγματος: ZERO**
* Όχι ZERO cash, ούτε ZERO coin, απλά ZERO ή ZERO συνάλλαγμα ή ZERO κρυπτοσυνάλλαγμα
* Συναλλαγματική μονάδα: ZER
* Συναλλαγματικό σύμβολο: Ƶ  
  + Unicode: U+01B5
  + HTML entity: &#437;
  + <https://en.wiktionary.org/wiki/%C6%B5>

\*Οι προβλέψεις είναι βασισμένες στην παρούσα κατάσταση και πιθανότατα θα διαφοροποιηθούν με νέες βελτιώσεις και με την εξόρυξη απο κάρτες γραφικών

Ημερομηνία υποβολής: 19 Φεβρουαρίου 2017  
  
Github: <https://github.com/zerocurrency/zero>

**ΠΡΟΣΟΧΗ: To ZERO είναι ένα εντελώς πειραματικό κομμάτι ανοιχτού κώδικα και παρέχεται όπως είναι χωρίς εγγυήσεις.**