ΕΛΛΗΝΙΚΑ

ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ

PRIZM

Η αρχική έννοια του ψηφιακού νομίσματος

Τεχνικές προδιαγραφές Prizm Έκδοση Ιουνίου, 2020

PZM.SPACE

P R I Z M

ΕΙΣΑΓΩΓΗ

Το Bitcoin είναι το πρώτο αποκεντρωμένο ψηφιακό νόμισμα στον κόσμο, που σας επιτρέπει να αποθηκεύετε εύκολα και να μεταφέρετε κρυπτογραφημένα νομίσματα χρησιμοποιώντας τη διασύνδεση P2P για τη μετάδοση πληροφοριών, τη κωδικοποίηση (hashing) σαν σήμα συγχρονισμού για την αποφυγή διπλών χρέωσεων, καθώς και ένα αξιόπιστο σύστημα καταγραφής για τον προσδιορισμό του κατόχου των νομισμάτων. Ο μηχανισμός αυτός έχει μια αυξανόμενη τεχνολογία και επιχειρηματική υποδομή. Σύμφωνα με τον αρχικό σχεδιασμό, τα bitcoins είναι ανταλλάξιμα, κάτι το οποίο τα κάνει ένα ουδέτερο μέσο ανταλλαγής. Τα Bitcoins μπορεί να έχουν ιδιαίτερες ιδιότητες που υποστηρίζονται είτε από τον εκδότη είτε από μια δημόσια σύμβαση και να έχουν αξία ανεξάρτητη από την ονομαστική αξία στην οποία θα έπρεπε να έχει. Το Bitcoin έχει αποδείξει ότι το ηλεκτρονικό σύστημα πληρωμών P2P μπορεί πραγματικά να λειτουργήσει και να επεξεργαστεί τις πληρωμές χωρίς την εμπλοκή ενός τρίτου.

Ωστόσο, για να βασίζεται το σύνολο της ηλεκτρονικής οικονομίας σε μια πλήρως αποκεντρωμένη λύση peer-to-peer, το σύστημα πρέπει να είναι σε θέση να κάνει τα εξής:
1 - Τις διαδικασίες συναλλαγών με ασφάλεια, γρήγορα και αποτελεσματικά, που να μπορούν να ξεπερνούν τις χιλιάδες ανά ώρα.
2 - Να ενθαρρύνουν τα άτομα να συμμετέχουν στην ασφάλεια δικτύων.
3 - Να μπορούν να λειτουργούν σε παγκόσμιο επίπεδο με την ελάχιστη κατανάλωση πόρων.
4 - Και να μπορούν να χρησιμοποιηθούν από ένα ευρύ φάσμα συσκευών, συμπεριλαμβανομένων των κινητών τηλεφώνων.
Το PZM (προφέρεται ως "Prizm") πληρεί όλες αυτές τις συνθήκες. Και έχει επίσης το πρόσθετο πλεονέκτημα, μοναδικό πλεονέκτημα που ονομάζεται ΕΞΟΡΥΞΗ (PARAMINING), το οποίο δεν ανήκει σε κανένα άλλο από τα υπάρχοντα κρυπτονομίσματα.
Αλλά περισσότερο σχετικά με αυτό αργότερα.

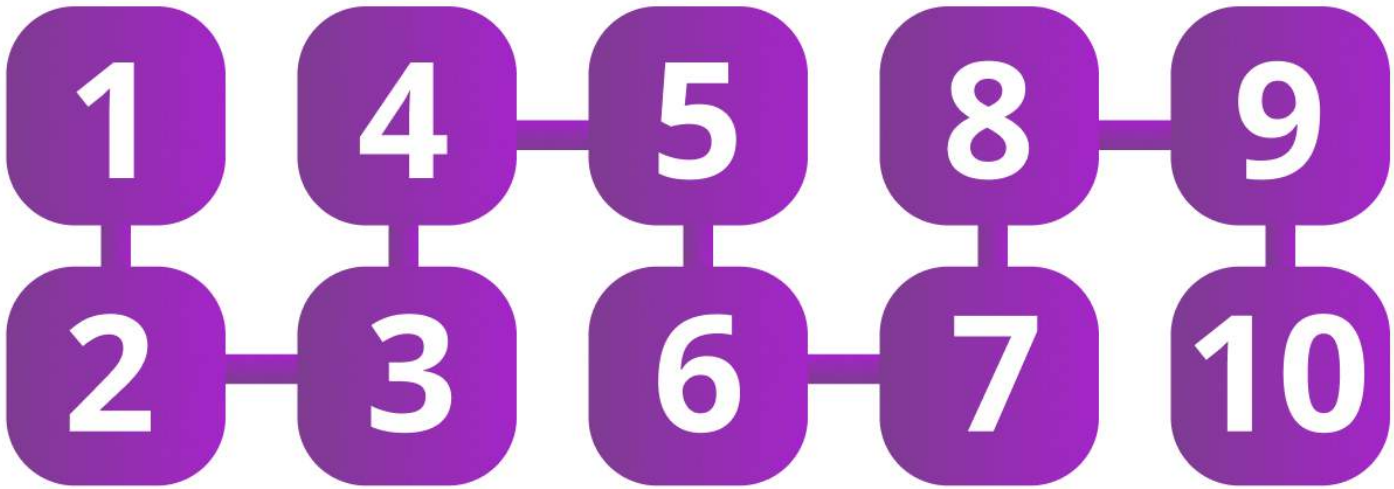
P R I Z M

ΑΝΑΣΚΟΠΗΣΗ

PRIZM - είναι ένα κρυπτονόμισμα 100% τύπου Επιβεβαίωσης Μεριδίου (Proof of Stake) που βασίζεται στον πυρήνα NEXT, που είναι γραμμένος στη γλώσσα ανοιχτού κώδικα Java. Ο μοναδικός αλγόριθμος του PRIZM Proof of Stake δεν εξαρτάται από οποιαδήποτε μεταβολή λόγω της "ηλικίας του κέρματος" όπως συμβαίνει σε άλλα κρυπτονομίσματα Επιβεβαίωσης Μεριδίου (Proof of Stake) και αντέχει στις λεγόμενες “Nothing at Stake” επιθέσεις. Ο συνολικός αριθμός των διαθέσιμων νομισμάτων ανακοινώθηκε στο μπλοκ Genesis. Η κρυπτογράφηση Curve25519 χρησιμοποιείται για να παρέχει μια ισορροπία μεταξύ ασφάλειας και την απαιτούμενη επεξεργαστικής ισχύς μαζί με τους πιο συνηθισμένους αλγόριθμους κρυπτογράφησης SHA256.

60”

Τα μπλοκ παράγονται, κατά μέσο όρο, κάθε 60 δευτερόλεπτα από λογαριασμούς σε κόμβους του δικτύου που δεν είναι αποκλεισμένοι.



Όταν κάποιος λογαριασμός που διατηρεί κόμβο δημιουργήσει με επιτυχία ένα μπλοκ, ένα συγκεκριμένο ποσό Prizm καταβάλλεται σε αυτόν. Αυτή η διαδικασία είναι γνωστή ως σφυρηλάτηση και είναι παρόμοια με την έννοια της “εξόρυξης” που χρησιμοποιούν άλλα κρυπτονομίσματα. Οι συναλλαγές θεωρούνται ασφαλείς μετά από 10 επιβεβαιώσεις στα μπλοκ. Η τρέχουσα αρχιτεκτονική και το μέγεθος του μπλοκ του PZM επιτρέπουν την επεξεργασία μέχρι και 367.200 συναλλαγών ανά ημέρα.

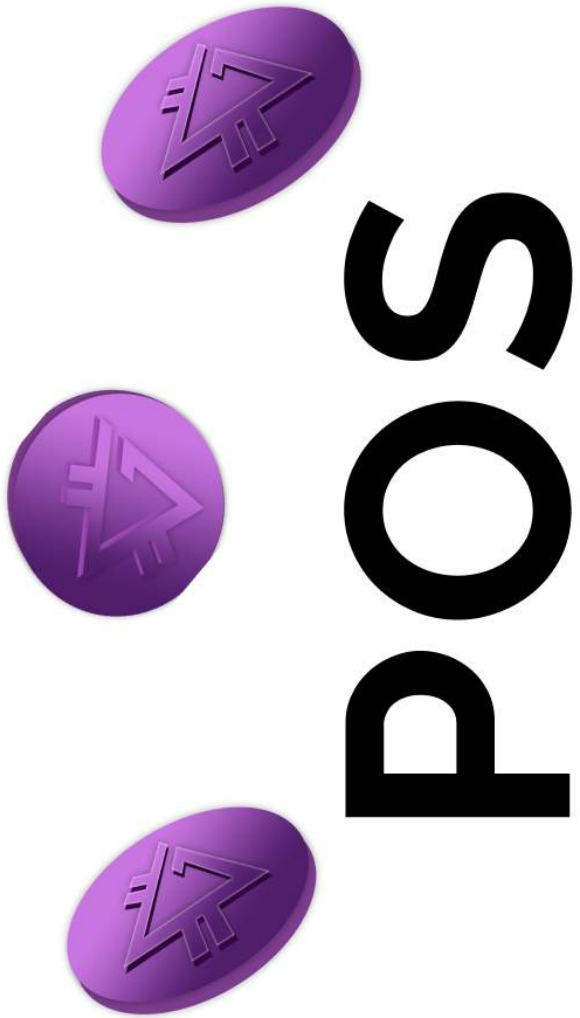
Το PZM εμπεριέχει την εφαρμογή της Διαφανής Σφυρηλάτησης που θα σας επιτρέψει να αυξήσετε την απόδοση της επεξεργασίας συναλλαγών με δύο καθοριστικούς τρόπους, χρησιμοποιώντας τον αλγόριθμο παραγωγής, το οποίο είναι καθοριστικό, σε συνδυασμό με πρόσθετους μηχανισμούς ασφαλείας του δικτύου.

PRIZM

ΤΕΧΝΟΛΟΓΙΕΣ ΠΥΡΗΝΑ

Proof of Stake

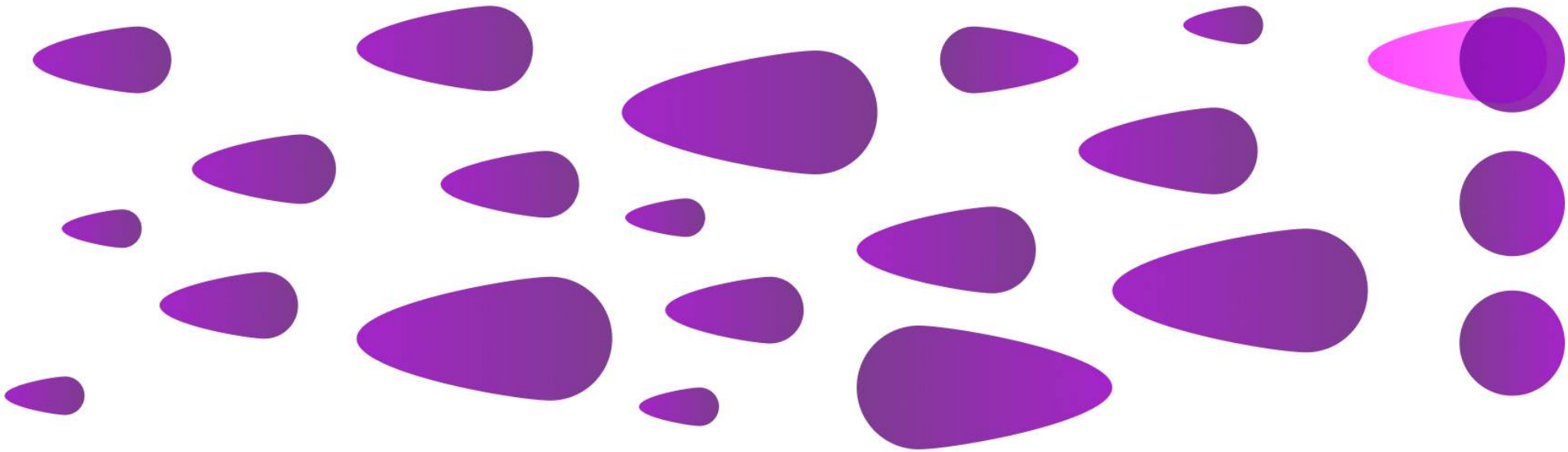
Στο παραδοσιακό μοντέλο του Proof of Work που χρησιμοποιείται από την πλειοψηφία των κρυπτονομισμάτων, η ασφάλεια του δικτύου εξασφαλίζεται από την εργασία των συμμετεχόντων. Χρησιμοποιούν τους πόρους τους (υπολογισμός / χρόνος επεξεργασίας) για να συνχωνεύσουν τις διπλές συναλλαγές και να επιβάλουν έκτακτα έξοδα σε εκείνους που προσπαθούν να βλάψουν το σύστημα συναλλαγών. Για αυτή τη δουλειά, οι συμμετέχοντες ανταμείβονται με PZM. Η συχνότητα και η πλήθος των ανταμοιβών ποικίλουν ανάλογα με τις παραμέτρους εργασίας του κρυπτονομίσματος. Αυτή η διαδικασία είναι γνωστή ως εξόρυξη. Η συχνότητα της παραγωγής μπλοκ, η οποία καθορίζει κάθε φορά και μια ανταμοιβή για την εξόρυξη κρυπτονομισμάτων, κατά κανόνα, θα πρέπει να παραμείνει σταθερή.



Ως αποτέλεσμα, ο κόπος του έργου που απαιτείται για την απόκτηση ανταμοιβών θα πρέπει να αυξάνει καθώς το δίκτυο γίνεται πιο αποδοτικό. Καθώς αναπτύσσεται το δίκτυο Proof of Work, ο κάθε χρήστης έχει λιγότερα κίνητρα να υποστηρίξει το δίκτυο, διότι η πιθανή ανταμοιβή κατανέμεται σε περισσότερους συναδέλφους. Αναζητώντας την κερδοφορία οι χρήστες συνεχίζουν να επενδύουν σε εξειδικευμένο εξοπλισμό που απαιτεί σημαντικά οικονομικά κεφάλαια και υψηλό τρέχον ενεργειακό κόστος. Με την πάροδο του χρόνου, το δίκτυο γίνεται πιο συγκεντρωμένο καθώς οι μικρότεροι εταίροι (εκείνοι που μπορούν να κάνουν λιγότερη εργασία) εγκαταλείπουν τις προσπάθειες τους ή συγκεντρώνουν τους πόρους τους σε ομάδες. Ο Δημιουργός του Bitcoin Satoshi Nakamoto, σχεδίαζε το δίκτυο του bitcoin να είναι αποκεντρωμένο εντελώς. Αλλά κανείς δεν μπορούσε να προβλέψει ότι τα κίνητρα που παρέχονται από τα συστήματα Proof of Work θα συγκέντρωνε το ενδιαφέρον των χρηστών στη διαδικασία της εξόρυξης. Αυτό οδηγεί σε ενδεχόμενες ευπάθειες.

PRIZM PROOF OF STAKE

ΤΕΧΝΟΛΟΓΙΕΣ ΠΥΡΗΝΑ



GHash. Η IO πισίνα του bitcoin έχει φτάσει στο παρελθόν το 51% της εξορυκτικής ισχύος του bitcoin, και οι πέντε κορυφαίες δεξαμενές εξορυκτικών πόρων αποτελούν το 70% της κρυπτογραφικής ισχύος του δικτύου. Επομένως η έννοια της αποκέντρωσης διατρέχει κίνδυνο να χαθεί πλήρως. Στο μοντέλο Proof of Stake που χρησιμοποιεί το Prizm, η ασφάλεια δικτύων ρυθμίζεται από εταίρους που συμμετέχουν στο δίκτυο.

Τα κίνητρα που παρέχονται από αυτόν τον αλγόριθμο δεν συμβάλλουν στη συγκέντρωση όπως στο μοντέλο του Proof of Work και τα δεδομένα δείχνουν ότι το δίκτυο Prizm παραμένει ιδιαίτερα αποκεντρωμένο από την έναρξή του: υπάρχει ένας μεγάλος (και αυξανόμενος) αριθμός μοναδικών λογαριασμών που συμβάλλουν στη δημιουργία των μπλοκ στο δίκτυο και πέντε κορυφαίους λογαριασμούς που παράγουν το 35% του συνολικού αριθμού των μπλοκ.

PRIZM

PROOF OF STAKE ΣΤΟ PRIZM

Το PRIZM χρησιμοποιεί ένα σύστημα με το οποίο κάθε "νόμισμα" στο πορτοφόλι μπορεί να θεωρηθεί ως μικροσκοπική μονάδα εξόρυξης. Όσο περισσότερα νομίσματα περιέχονται στο λογαριασμό, τόσο πιο πιθανό είναι ότι ο λογαριασμός θα λάβει το δικαίωμα να δημιουργήσει ένα μπλοκ. Η συνολική “αμοιβή” που εισπράχθηκε για τη δημιουργία του μπλοκ, θεωρείται ως το ποσό των προμηθειών για τις συναλλαγές που βρίσκονται μέσα στο μπλοκ. Το PRIZM δεν δημιουργεί νέα νομίσματα ως αποτέλεσμα της δημιουργίας μπλοκ. Το PRIZM δεν δημιουργεί νέα νομίσματα ως αποτέλεσμα της δόμησης μπλοκ. Το μοίρασμα των PZM προκύπτει ως αμοιβή αυτών που παράγουν μπλοκς, οπότε ο όρος σφυρηλάτηση (χρησιμοποιείται στη περίπτωση αυτή για τη δημιουργία σχέσεων ή συνθηκών αντί για τον όρο εξόρυξη). Τα μπλοκ που ακολουθούν δημιουργούνται βάσει επαληθεύσιμων, μοναδικών και σχεδόν απρόβλεπτων πληροφοριών από το προηγούμενο μπλοκ. Τα μπλοκ συνδέονται χάρη σε αυτούς τους συνδέσμους, δημιουργώντας μια αλυσίδα μπλοκ (και συναλλαγών) που μπορούν να εντοπιστούν πίσω στο μπλοκ Genesis. Ο χρόνος δημιουργίας μπλοκ είναι περίπου 59 δευτερόλεπτα, αλλά οι διαφορετικές πιθανότητες έχουν οδηγήσει στο γεγονός ότι ο μέσος χρόνος παραγωγής του μπλοκ μπορεί να είναι 80 δευτερόλεπτα, επίσης υπάρχουν και μεγαλύτερα διαστήματα μεταξύ των μπλοκ. Η ασφάλεια του Blockchain Βασίζεται πάντα στο σύστημα του Proof-of-Stake.

PRIZM

PROOF OF STAKE ΣΤΟ PRIZM

Οι βασικές αρχές ισχύουν για τον αλγόριθμο Proof of Stake του Prizm:

- Η σωρευμένη τιμή πολυπλοκότητας αποθηκεύεται ως παράμετρος σε κάθε μπλοκ και κάθε επόμενο μπλοκ λαμβάνει τη νέα πολυπλοκότητα του από την τιμή του προηγούμενου μπλοκ. Στην περίπτωση ασάφειας, το δίκτυο επιτυγχάνει τη συσχέτιση επιλέγοντας ένα μπλοκ ή τμήμα της αλυσίδας με την υψηλότερη αθροιστική πολυπλοκότητα.

- Προκειμένου οι κάτοχοι λογαριασμού να μην μεταφέρουν τα κεφάλαια τους από έναν λογαριασμό σε άλλο ως μέσο παραποίησης, προκειμένου να είναι σε θέση να δημιουργήσουν μπλοκς, τα νομίσματα πρέπει να παραμείνουν εντός του λογαριασμού για 1.440 μπλοκς πριν μπορέσουν να συμβάλουν στη διαδικασία παραγωγής μπλοκ. Τα νομίσματα που πληρούν αυτό το κριτήριο συμβάλλουν στην αποτελεσματική ισορροπία λογαριασμών και η ισορροπία αυτή καθορίζει την πιθανότητας σφυρηλάτησης.

- Για να αποτραπεί ένας εισβολέας να δημιουργήσει μια νέα αλυσίδα σε όλη τη διαδρομή από το μπλοκ Genesis, το δίκτυο επιτρέπει μόνο τον μετασχηματισμό της αλυσίδας 720 μπλοκ που βρίσκονται πίσω από το τρέχον μπλοκ. Οποιοδήποτε μπλοκ κάτω από αυτό το όριο απορρίπτεται. Αυτό το όριο μετακίνησης μπορεί να θεωρηθεί ως το μόνο σταθερό σημείο ελέγχου PZM.

- Λόγω της εξαιρετικά χαμηλής πιθανότητας ότι οποιοσδήποτε λογαριασμός θα αναλάβει τη διαχείριση Blockchain δημιουργώντας τη δική του αλυσίδα μπλοκ, οι συναλλαγές θεωρούνται ασφαλείς εάν κωδικοποιούνται σε ένα μπλοκ που βρίσκεται 10 μπλοκ πίσω από το τρέχον μπλοκ.

PRIZM

ΣΥΓΚΡΙΣΗ ΜΕ ΤΟ PEERCOIN POS

Το Peercoin χρησιμοποιεί το χαρακτηριστικό της ηλικίας του νομίσματος ως παράγοντα του αλγορίθμου για την πιθανότητα εξόρυξης. Σε αυτό το σύστημα, όσο περισσότερο χρονικό διάστημα είναι τα νομίσματα σας στο λογαριασμό σας (έως 90 ημέρες), τόσο μεγαλύτερη είναι η δυνατότητα (της ηλικίας νομισμάτων) να δημιουργήσουν ένα μπλοκ. Το γεγονός της δημιουργίας μπλοκ λαμβάνει υπόψη την σημασία της ηλικίας των νομισμάτων που υπάρχουν και το δίκτυο καθορίζει την επιλογή της αλυσίδας σύμφωνα με τη μεγαλύτερη συνολική ηλικία. Όταν τα Peercoin μπλοκ διαχωριστούν, η ηλικία νομισμάτων που χρησιμοποιήθηκαν επιστρέφονται στον αρχικό λογαριασμό μπλοκ.

Ως αποτέλεσμα, το κόστος για την επίθεση στο δίκτυο Peercoin είναι χαμηλό, επομένως οι εισβολείς μπορούν να συνεχίσουν να προσπαθούν να δημιουργήσουν μπλοκ (που λέγεται grinding the stake), μέχρι να πετύχουν. Το Peercoin ελαχιστοποιεί αυτούς και άλλους κινδύνους δημοσιεύοντας κεντρικά σημεία ελέγχου blockchain αρκετές φορές την ημέρα για να παγώσει το blockchain και να μπλοκάρει τις συναλλαγές. Το Prizm δεν χρησιμοποιεί την ηλικία των νομισμάτων ως μέρος του αλγορίθμου της σφυρηλάτησης. Η πιθανότητα δημιουργίας ενός μπλοκ από οποιονδήποτε λογαριασμό εξαρτάται μόνο από το τρέχον υπόλοιπο (το πλεονέκτημα του κάθε λογαριασμού), το χρόνο από τον τελευταίο μπλοκ (που μοιράζονται όλοι οι λογαριασμοί σφυρηλατούν) και από την τιμή στόχου βάσης (η οποία είναι επίσης κοινή για όλους τους λογαριασμούς).

PRIZM

ΜΑΡΚΕΣ

10 MLN
PZM

ΑΡΧΙΚΗ ΕΚΔΟΣΗ

6 BLN
PZM

ΤΕΛΙΚΗ ΕΚΔΟΣΗ

Η αρχική έκδοση είναι 10 εκατομμύρια PZM και το τελικό ποσό είναι 6 δισεκατομμύρια PZM. Τα κέρματα εκδόθηκαν με τη δημιουργία του μπλοκ Genesis (το πρώτο μπλοκ στο blockchain), το Paramining υλοποιείται σε όλες τις χώρες του κόσμου, με ονομαστικό κόστος και σε περιορισμένες ποσότητες, προκειμένου να επιτευχθεί η αρχική αποκέντρωση του Prizm. Το συνολικό ποσό του PZM θα είναι 6 δισεκατομμύρια μάρκες. Ο Λογαριασμός Genesis παράγει σήματα εξόρυξης αντι-νομισμάτων (σήμα αποστολής των νομισμάτων σε ένα συγκεκριμένο πορτοφόλι) μέχρι να φτάσει το όριο των 6 δισεκατομμυρίων PZM.

Η ύπαρξη αντι-νομισμάτων στο Genesis έχει αρκετές ενδιαφέρουσες παρενέργειες:

Όλες οι μάρκες που αποστέλλονται στο λογαριασμό Genesis καταστρέφονται αποτελεσματικά, καθώς το αρνητικό υπόλοιπο του λογαριασμού τις ακυρώνει. Η κύρια λειτουργία του Prizm είναι το ήδη υπάρχον σύστημα πληρωμών, αλλά δημιουργήθηκε για να κάνει πολλά περισσότερα.
Οι στόχοι της κοινότητας CWT μπορούν να επιτευχθούν υπό την προϋπόθεση της ισοτιμίας PZM με τα κύρια νομίσματα της Fiat.

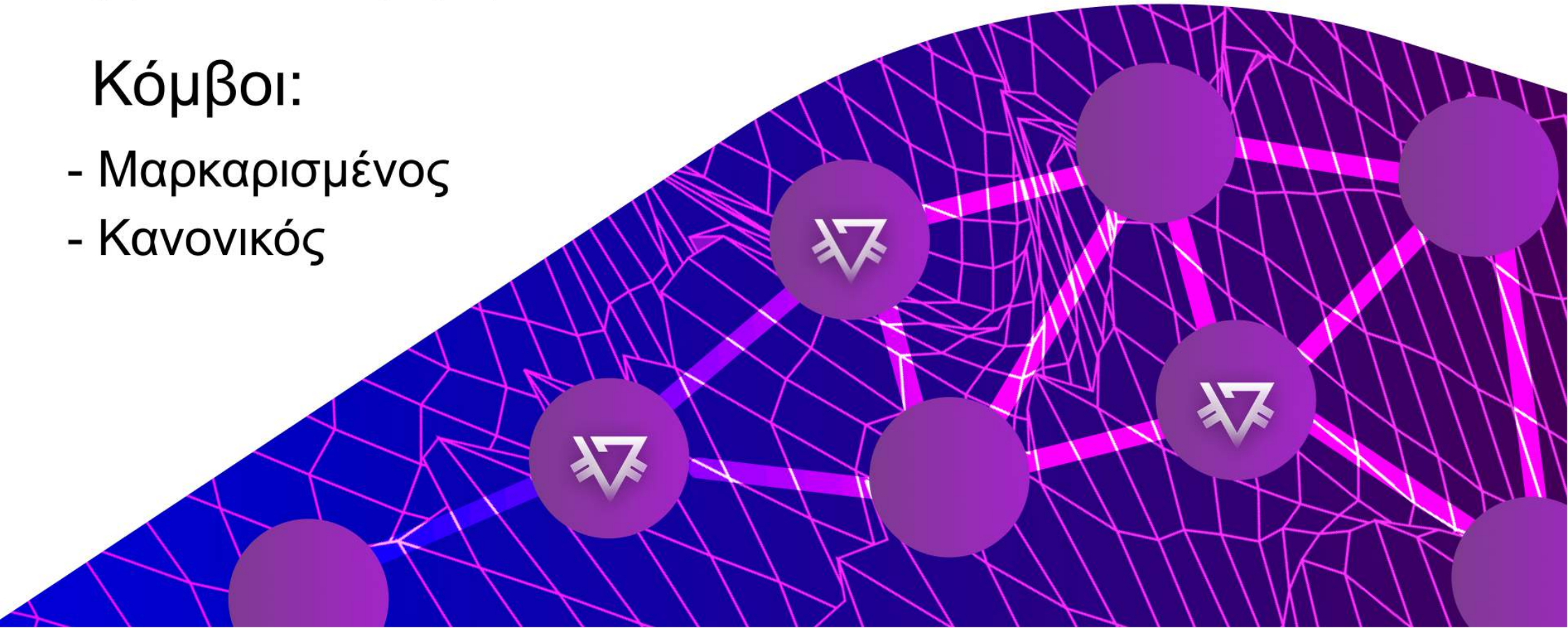
PRIZM

ΚΟΜΒΟΣ ΔΙΚΤΥΟΥ

Ο **κόμβος δικτύου Prizm** είναι οποιαδήποτε συσκευή που πραγματοποιεί συναλλαγή ή παράγει δεδομένα για μπλοκς στο δίκτυο. Κάθε συσκευή με το λογισμικό PZM χαρακτηρίζεται ως κόμβος. Οι κόμβοι μπορούν να χωριστούν σε δύο τύπους: σημειωμένοι και κανονικοί.

Κόμβοι:

- Μαρκαρισμένος
- Κανονικός



PRIZM

ΚΟΜΒΟΣ ΔΙΚΤΥΟΥ

Ένας μαρκαρισμένος κόμβος είναι απλά ένας κόμβος που επισημαίνεται με ένα κρυπτογραφημένο Token το οποίο προκύπτει από το ιδιωτικό κλειδί του λογαριασμού. Αυτό το Token μπορεί να αποκωδικοποιηθεί για να εμφανίσει τη συγκεκριμένη διεύθυνση λογαριασμού PZM και το υπόλοιπο που σχετίζονται με τον κόμβο. Η έννοια της προσθήκης ετικετών σε έναν κόμβο προσθέτει ένα επίπεδο υπευθυνότητας και εμπιστοσύνης, έτσι ώστε οι μαρκαρισμένοι κόμβοι να είναι πιο αξιόπιστοι από εκείνους που δεν είναι μαρκαρισμένοι στο δίκτυο. Όσο μεγαλύτερο το υπόλοιπο του λογαριασμού που συνδέεται με έναν μαρκαρισμένο κόμβο, τόσο μεγαλύτερη εμπιστοσύνη δίνεται σε αυτόν τον κόμβο. Στην περίπτωση κάποιου με κακόβουλες προθέσεις μπορεί να θέλει να επισημάνει έναν κόμβο για να κερδίσει εμπιστοσύνη στο δίκτυο και στη συνέχεια να χρησιμοποιήσει αυτήν την εμπιστοσύνη για κακόβουλους σκοπούς. Με αυτόν τον τρόπο (το κόστος σε PZM που απαιτείται για να χτιστεί επαρκή εμπιστοσύνη) αποτρέπεται η κακόβουλη χρήση.

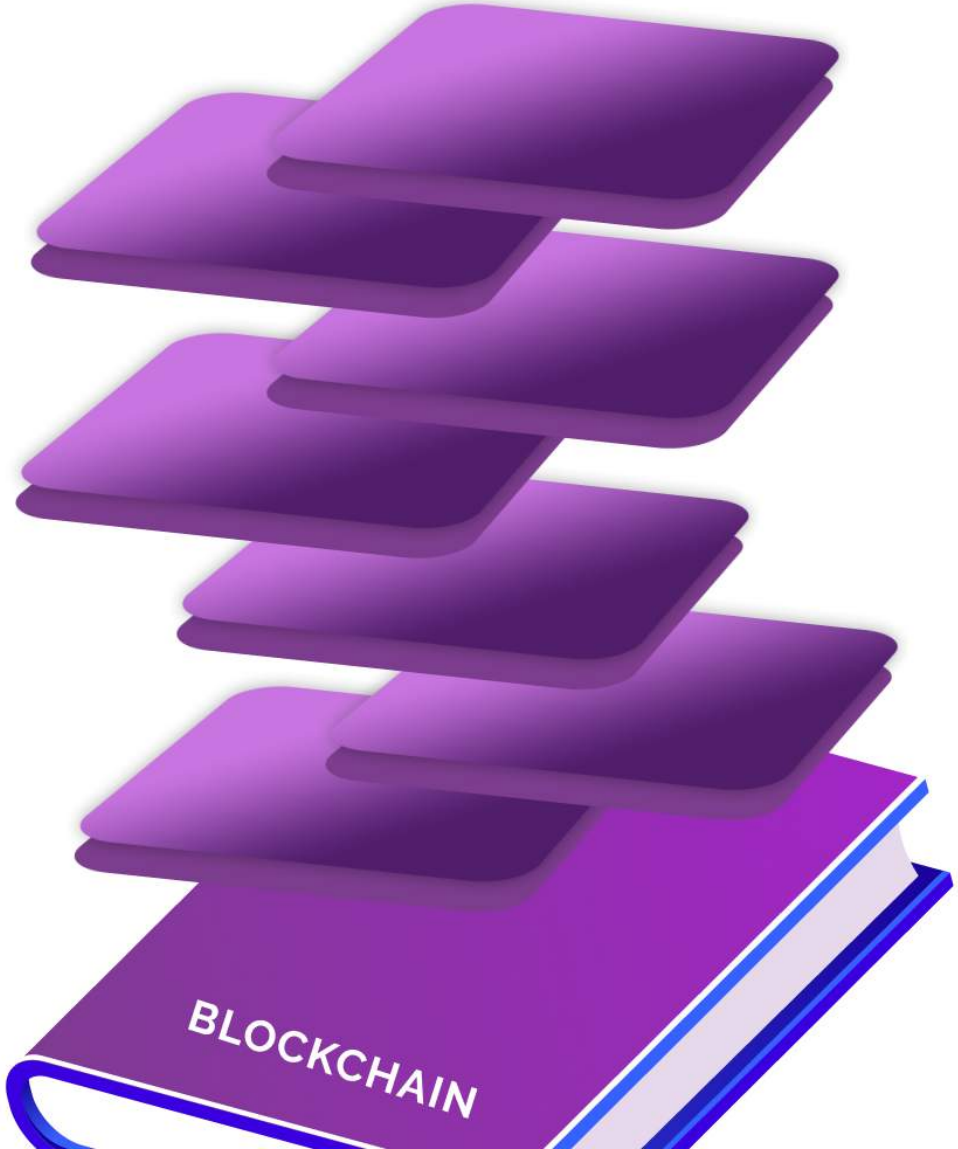
Κάθε κόμβος στο δίκτυο PZM έχει τη δυνατότητα να επεξεργάζεται και να μεταδίδει και τις δύο συναλλαγές και να αποκλείει πληροφορίες. Τα μπλοκ ελέγχονται καθώς λαμβάνονται από τους άλλους κόμβους και σε περιπτώσεις όπου δεν πραγματοποιείται έλεγχος μπλοκ, οι κόμβοι μπορούν να μπουν προσωρινά στη μαύρη λίστα για να αποτρέψουν τη διάδοση μη έγκυρων δεδομένων στα μπλοκ.

Κάθε κόμβος διαθέτει ενσωματωμένους μηχανισμούς προστασίας DDOS (Distributed Denial of services) που περιορίζουν τον αριθμό των αιτημάτων δικτύου από οποιονδήποτε χρήστη σε 30 ανά δευτερόλεπτο.

P R I Z M

ΜΠΛΟΚΣ

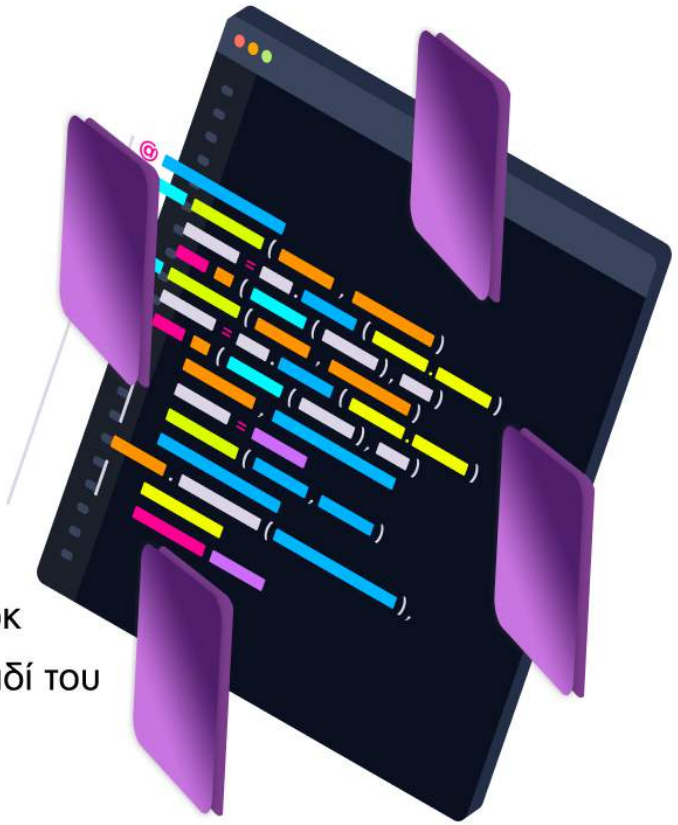
Όπως και με άλλα κρυπτονομίσματα, το PZM Ledger (Λογαριασμός συναλλαγών) είναι χτισμένο και αποθηκευμένο σε μια ακολουθία μπλοκ που είναι γνωστή ως Blockchain. Αυτό το βιβλίο εργασιών διατηρεί μια μόνιμη καταγραφή των συναλλαγών που έχουν συμβεί και καθορίζει επίσης τη σειρά με την οποία έγιναν οι συναλλαγές. Ένα αντίγραφο του Blockchain αποθηκεύεται σε κάθε κόμβο του δικτύου Prizm και κάθε λογαριασμός που διατηρεί έναν κόμβο (με την παροχή του ιδιωτικού κλειδιού αυτού του λογαριασμού) έχει τη δυνατότητα να δημιουργεί μπλοκ, υπό την προϋπόθεση ότι τουλάχιστον μία εισερχόμενη συναλλαγή στο λογαριασμό αυτόν έχει επιβεβαιωθεί 1,440 φορές. Οποιοσδήποτε λογαριασμός πληρεί αυτά τα κριτήρια ονομάζεται ενεργός λογαριασμός. Στο PZM, κάθε μπλοκ περιέχει έως και 255 συναλλαγές, για τις οποίες προηγείται μία επικεφαλίδα 192 bytes που περιέχει παραμέτρους προσδιορισμού. Κάθε συναλλαγή σε ένα μπλοκ αντιπροσωπεύεται από το πολύ 160 bytes και το μέγιστο μέγεθος ενός μπλοκ είναι 32 KB.



PRIZM

ΜΠΛΟΚΣ

Όλα τα Blocks περιέχουν τις ακόλουθες παραμέτρους



- Την έκδοση του block, το ύψος και την ταυτότητα του ID
- Την χρονοσφραγίδα του block εκφρασμένη σε δευτερόλεπτα, από το Genesis μπλοκ
- Την ταυτότητα του λογαριασμού που δημιούργησε το block, καθώς και δημόσιο κλειδί του
- Την ταυτότητα και το Hash προηγούμενου μπλοκ.
- το πλήθος των συναλλαγών που έχουν καταγραφεί στο μπλοκ
- Το συνολο των PZM που προκύπτουν από από τις κινήσεις συναλλαγών και τις προμήθειες στο μπλοκ
- Πληροφορίες, καθώς και το ID για όλες τις συναλλαγές που αναφέρονται στο μπλοκ
- Το μήκος του ωφέλιμου φορτίου του μπλοκ και τιμή της συνάρτησης Hash του ωφέλιμου φορτίου του μπλοκ
- Την τιμή του Base Target και την αθροιστική δυσκολία για το μπλοκ

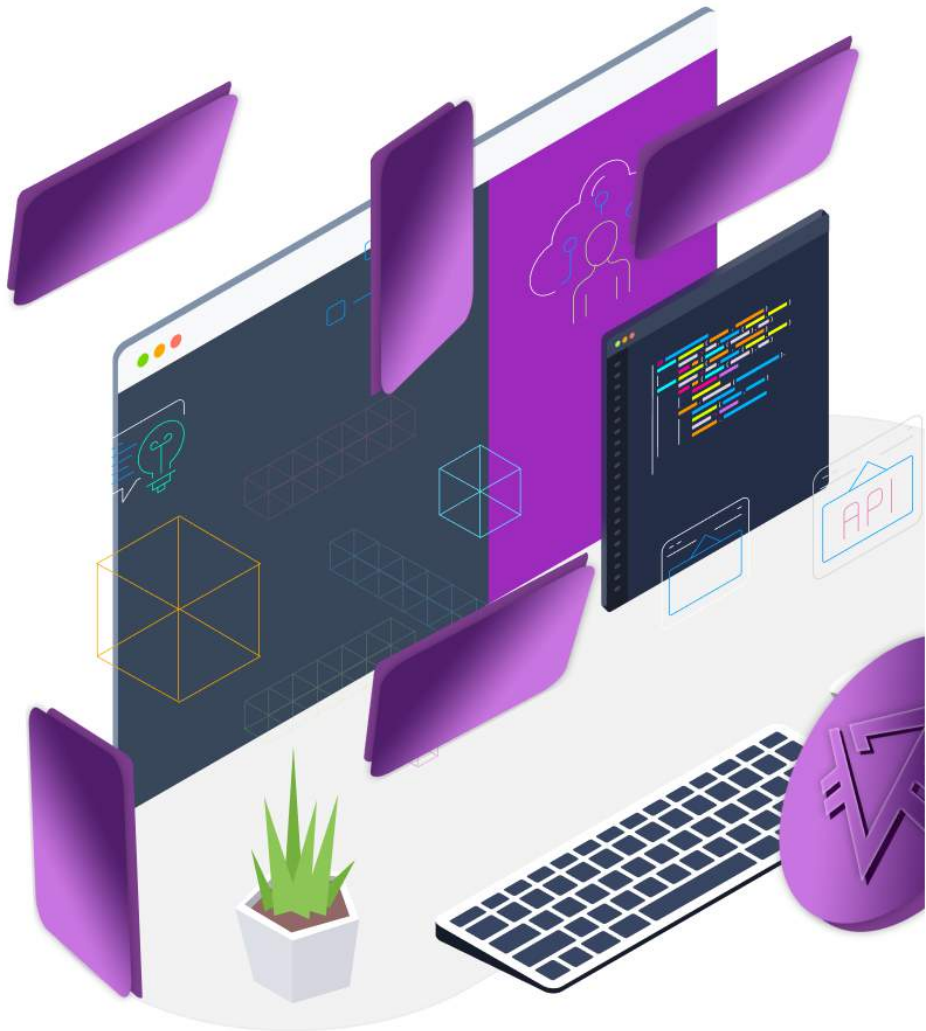
PRIZM

ΣΦΥΡΗΛΑΤΗΣΗ (ΔΗΜΙΟΥΡΓΙΑ ΤΩΝ ΜΠΛΟΚΣ)

Υπάρχουν τρεις τιμές οι οποίες είναι το κλειδί για να καθορίσουν ποιος λογαριασμός έχει το δικαίωμα να δημιουργήσει ένα μπλοκ, ο οποίος λογαριασμός έχει δικαίωμα δημιουργίας μίας μονάδας μπλοκ και να καθορίσει ποιος θα είναι ο ρόλος της σε περίπτωση προβλήματος: υποκείμενη τιμή-στόχος, τιμή στόχος και αθροιστική δυσκολία.

Τιμή αναφοράς του στόχου

Για να αποκτήσετε το δικαίωμα δημιουργίας μπλοκ, όλοι οι ενεργοί λογαριασμοί Prizm "ανταγωνίζονται" προσπαθώντας να δημιουργήσουν ένα κλειδάριθμο με χαμηλότερη από την καθορισμένη τιμή του στόχου βάσης. Αυτή η τιμή του στόχου βάσης αλλάζει από μπλοκ σε μπλοκ και προέρχεται από την τιμή στόχου βάσης του προηγούμενου μπλοκ πολλαπλασιασμένη με το χρόνο που χρειαζόταν για τη δημιουργία αυτού του μπλοκ.



Target value

Κάθε λογαριασμός υπολογίζει τη δική του τιμή στόχου, βασισμένη στην τρέχουσα ενεργή απόδοση.

Αυτή η τιμή ισούται με:

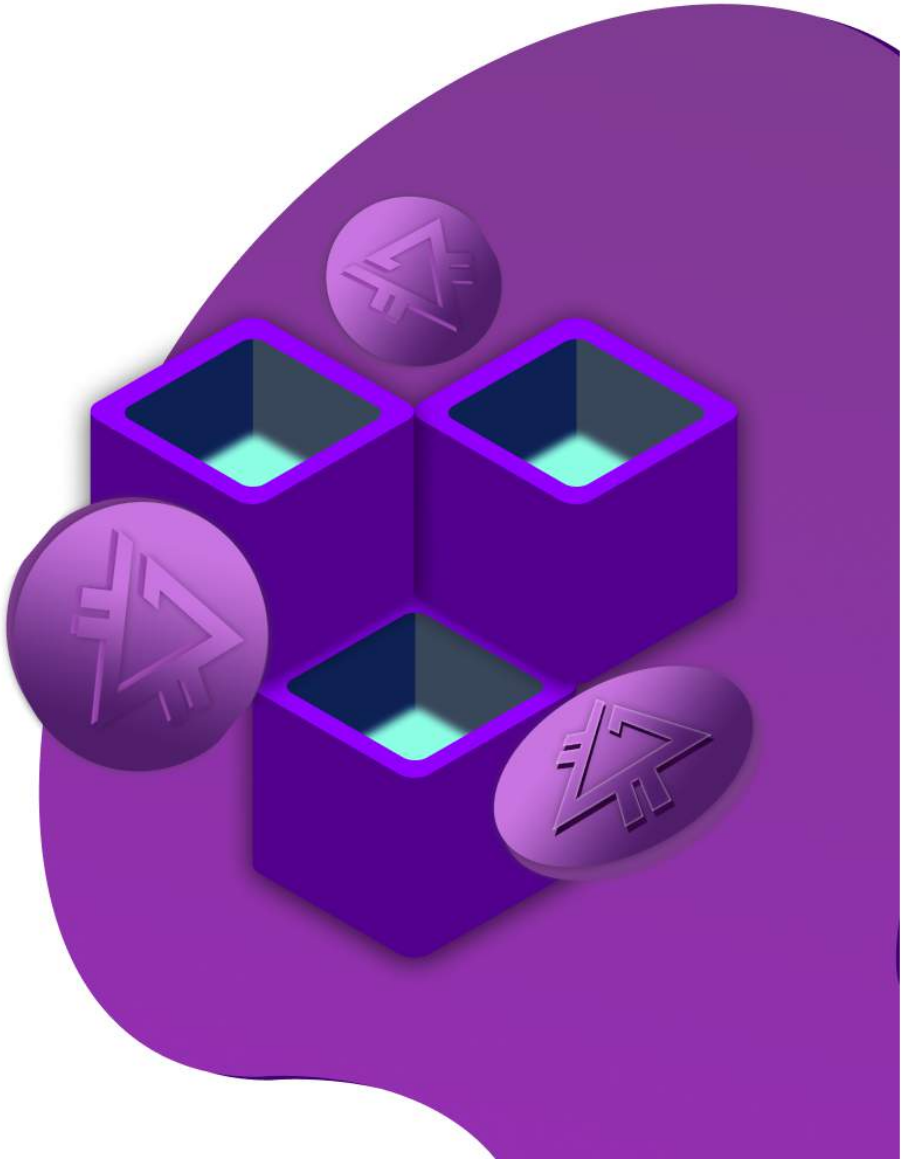
$$T = Tb \times S \times Be$$

Όπου:

T - the new target value
Tb - the reference target value
S - the elapsed time since the last block in seconds
Be - the effective account balance

Όπως μπορείτε να δείτε από τη συνάρτηση, η τιμή του στόχου αυξάνεται με το χρόνο κάθε δευτερόλεπτο που περνάει από το προηγούμενο μπλοκ.

Η μέγιστη τιμή στόχου είναι 1,53722867 x 1017, και η μικρότερη είναι η μισή από τη βασική τιμή στόχου του προηγούμενου μπλοκ. Αυτή η τιμή στόχου και η βασική τιμή στόχου είναι οι ίδιες για όλους τους λογαριασμούς που θέλουν να δημιουργήσουν πάνω σε ένα συγκεκριμένο μπλοκ. Η μόνη καθορισμένη παράμετρος λογαριασμού είναι ένα ενεργό υπόλοιπο.



Η συνολική πολυπλοκότητα

Η συνολική τιμή της πολυπλοκότητας Υπολογίζεται από την τιμή στόχου αναφοράς σύμφωνα με την συνάρτηση:

$$Dcb = Dpb + 264 / Tb$$

Όπου:

Dcb - η πολυπλοκότητα του τρέχον μπλοκ
Dpb - η πολυπλοκότητα του προηγούμενου μπλοκ
Tb - η τιμή βάσης στόχου του τρέχον μπλοκ

PRIZM

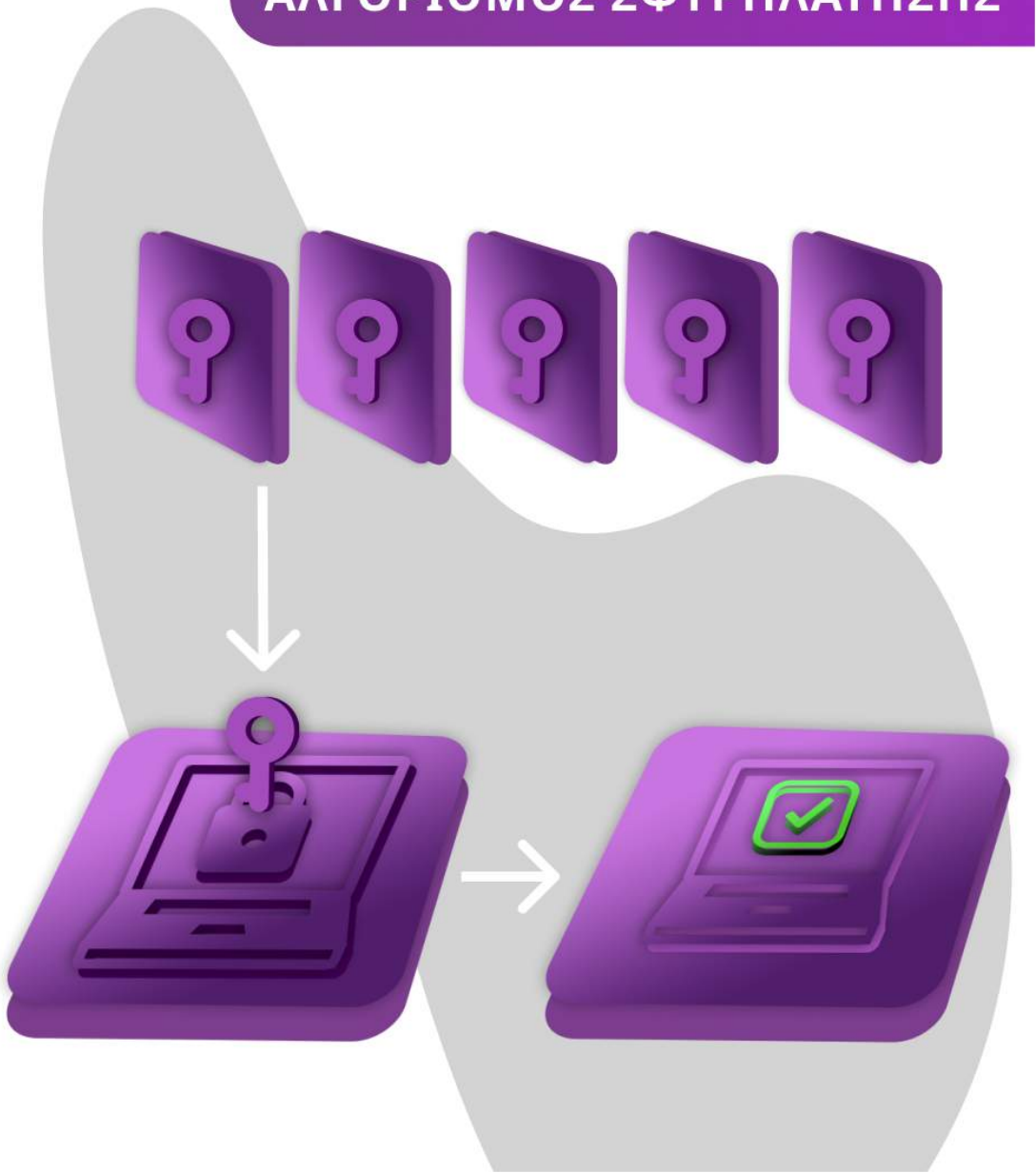
ΑΛΓΟΡΙΘΜΟΣ ΣΦΥΡΗΛΑΤΗΣΗΣ

Κάθε μπλοκ στην αλυσίδα έχει μία παράμετρο δημιουργίας υπογραφής. Για να συμμετέχει στη διαδικασία σφυρηλασίας ενός μπλοκ, ο ενεργός λογαριασμός υπογράφει κρυπτογράφοντας το προηγούμενο μπλοκ με το δικό του δημόσιο κλειδί. Αυτό δημιουργεί μια υπογραφή 64-byte που στη συνέχεια κρυπτογραφείται χρησιμοποιώντας το πρωτόκολλο SHA256. Τα πρώτα 8 bytes του κλειδάριθμου που προκύπτει δίνουν έναν αριθμό που λέγεται το “Hit” του λογαριασμού σας. Το “Hit” συγκρίνεται με την τρέχουσα τιμή-στόχο. Εάν η υπολογιζόμενη τιμή “Hit” είναι χαμηλότερη από τον στόχο, τότε μπορεί να δημιουργηθεί το επόμενο μπλοκ. Όπως σημειώνεται στη συνάρτηση της τιμής στόχου, η τιμή στόχου αυξάνεται με κάθε δευτερόλεπτο. Ακόμα κι αν υπάρχουν μόνο λίγοι ενεργοί λογαριασμοί στο δίκτυο, ένας από αυτούς θα δημιουργήσει τελικά ένα μπλοκ επειδή η τιμή στόχου θα γίνει πολύ μεγάλη. Σαν συνέπεια αυτού του γεγονότος είναι ότι μπορείτε να υπολογίσετε το χρόνο που θα χρειαστεί για οποιονδήποτε λογαριασμό να δημιουργήσει το μπλοκ συγκρίνοντας την τιμή “Hit” αυτού του λογαριασμού με την τιμή στόχου. Το τελευταίο σημείο είναι πολύ σημαντικό. Δεδομένου ότι οποιοσδήποτε κόμβος μπορεί να ζητήσει ένα αποτελεσματικό υπόλοιπο για έναν ενεργό λογαριασμό, είναι δυνατό να περάσει από όλους τους ενεργούς λογαριασμούς για να προσδιορίσει την ατομική αξία του “Hit”. Αυτό σημαίνει ότι με αρκετή ακρίβεια, μπορείτε να προβλέψετε ποιος από τους ακόλουθους λογαριασμούς θα αποκτήσει το δικαίωμα να μπλοκάρει την πλαστογράφηση. Μια τυχαία επίθεση μπορεί να πραγματοποιηθεί με τη μετακίνηση ενός ποσού σε έναν λογαριασμό που θα δημιουργήσει το επόμενο μπλοκ, ο οποίος είναι ένας άλλος λόγος για τον οποίο το ποσό PZM πρέπει να είναι στάσιμο για 1.440 μπλοκ πριν να συμβάλει στη σφυρηλάτηση (μέσω ενός ενεργού ποσού υπολοίπου). Αξιοσημείωτο είναι οτι η νέα τιμή βάσης στόχου για το επόμενο μπλοκ δεν μπορεί λογικά να προβλεφθεί, έτσι μια εικονική, καθοριστική διαδικασία προσδιορισμού του ποιος θα δημιουργήσει το επόμενο μπλοκ γίνεται ολοένα και πιο σημαντική, καθώς επιχειρούνται οι προβλέψεις για μελλοντικά μπλοκ.

P R I Z M

ΑΛΓΟΡΙΘΜΟΣ ΣΦΥΡΗΛΑΤΗΣΗΣ

Αυτό το χαρακτηριστικό του αλγόριθμου σφυρηλασίας του PRIZM βοηθά να αποτελέσει τη βάση για την ανάπτυξη και εφαρμογή του αλγορίθμου Transparent Forging. Όταν ένας ενεργός λογαριασμός έχει το δικαίωμα να δημιουργήσει ένα μπλοκ, συνδυάζει έως και 255 διαθέσιμες μη επιβεβαιωμένες συναλλαγές σε ένα νέο μπλοκ και συμπληρώνει το μπλοκ με όλες τις απαραίτητες παραμέτρους του. Αυτό το μπλοκ δημοσιεύεται έπειτα στο δίκτυο ως υποψήφιο του Blockchain. Το ωφέλιμο φορτίο που δημιουργεί τον λογαριασμό και όλες οι υπογραφές σε κάθε μπλοκ μπορεί να ελεγχθεί από όλους τους κόμβους δικτύου που το λαμβάνουν. Σε μια κατάσταση όπου παράγονται πολλαπλά μπλοκ, οι κόμβοι θα επιλέξουν το μπλοκ με την υψηλότερη συσσωρευμένη πολυπλοκότητα ως το επίσημο μπλοκ. Επειδή τα δεδομένα του μπλοκ κατανέμονται μεταξύ των μελών (peers), εντοπίζονται πιρούνια (μη εξουσιοδοτημένα παρακλάδια της αλυσίδας) και αποσυναρμολογούνται εξετάζοντας τις τιμές της συνολικής πολυπλοκότητας των αλυσίδων που είναι αποθηκευμένες σε κάθε πιρούνι.



PRIZM

ΣΦΥΡΗΛΑΤΗΣΗ

PARAMINING - είναι το βασικό πλεονέκτημα του PRIZM έναντι άλλων κρυπτονομισμάτων. Οι προγραμματιστές PRIZM πρόσθεσαν έναν μοναδικό, γραμμικό - αναχρονιστικό μηχανισμό για τον καθορισμό της ανταμοιβής για την αποθήκευση κεφαλαίων με στόχο την οικονομική ελκυστικότητα και τη σταδιακή αντικατάσταση όλων των υπαρχόντων χρηματοπιστωτικών μέσων του κόσμου από τη μάζα του PZM στον βασικό μηχανισμό διαμόρφωσης.

Δηλαδή, εκτός από τον βασικό μηχανισμό σφυρηλασίας, που δεν αυξάνει το ποσό των κεφαλαίων στο σύστημα, στο PZM υπάρχει ένας πρόσθετος μηχανισμός ParaMining, ο οποίος δημιουργεί νέα νομίσματα, σύμφωνα με τις μετρήσεις της τυπικής ανάπτυξης μαθηματικών του κανονικοποιημένου χρηματοπιστωτικού συστήματος στον τομέα της παγκόσμιας οικονομίας. Σύμφωνα με τους υπολογισμούς μας, μόνο μια τέτοια μορφή αύξησης του βάρους των νομισμάτων μπορεί να προσφέρει σταδιακή και αξιόπιστη αντικατάσταση όλων των υφιστάμενων οικονομικών μέσων.

P R I Z M

ΣΦΥΡΗΛΑΤΗΣΗ

Ο ρυθμός εξόρυξης νέων νομισμάτων που χρησιμοποιούν το ParaMining υπολογίζεται από τρεις βασικές παραμέτρους: τον αριθμό των νομισμάτων σε ένα προσωπικό πορτοφόλι, τον αριθμό των νομισμάτων στα πορτοφόλια των ακολούθων, μέχρι 88 επίπεδα και τον παράγοντα δυσκολίας εξόρυξης. Ο παράγοντας δυσκολίας υπολογίζεται ως ποσοστό και είναι ανάλογος προς τον συνολικό αριθμό των νομισμάτων που έχουν παραχθεί. Το μέγιστο επίπεδο δυσκολίας για τυπικούς λογαριασμούς είναι **98%**, το οποίο αντιστοιχεί σε 3 δισεκατομμύρια PZM που δημιουργήθηκαν. Για λογαριασμούς **HOLD - MODE**, το μέγιστο επίπεδο δυσκολίας είναι **97%**. Σύμφωνα με τα χαρακτηριστικά του, το Paramining είναι ένα σύστημα MLM 2.0 που αποκλείει όλα όσα ωθούν ένα απλό άτομο από την επιχείρηση στο διαδίκτυο, αλλά τον εμπλέκει ταυτόχρονα στην ανάπτυξη του δικτύου για να αυξήσει την ταχύτητα της εξόρυξης νομισμάτων στο προσωπικό του πορτοφόλι.

Όταν πραγματοποιείτε οποιαδήποτε συναλλαγή στο πορτοφόλι, το σύστημα ParaMining γράφει ένα blockchain που περιέχει την αξία του αριθμού των νομισμάτων του κατόχου πορτοφολιού και τον αριθμό των νομισμάτων στα πορτοφόλια των ακολούθων του, αυτή τη στιγμή δημιουργούνται νέα νομίσματα στο υπόλοιπο του πορτοφολιού.

HOLD - κρατήστε νομίσματα στο προσωπικό σας πορτοφόλι και μην κάνετε εμπόριο, εξαιτίας αυτού, μπορείτε να μειώσετε τον παράγοντα δυσκολίας στην εξόρυξη κερμάτων και να αυξήσετε την κερδοφορία του πορτοφολιού σας.

P R I Z M

ΣΦΥΡΗΛΑΤΗΣΗ

ΤΟ PARAMINING SYSTEM είναι το πιο προηγμένο εργαλείο για την προώθηση και τη διάδοση, καθώς δεν έχει αναλογίες σε κανένα σύγχρονη κρυπτονόμισμα. Το κύριο πλεονέκτημα του Paramining είναι ότι κανένας χρήστης του δικτύου δεν μπορεί να παρεμβαίνει σε αυτόν τον μηχανισμό και να πλαστογραφήσει νέα νομίσματα, όλοι οι χρήστες μπορούν να παρακολουθούν τον αριθμό των νομισμάτων που εκδίδει το σύστημα σε πραγματικό χρόνο, Το Paramining λειτουργεί σε οποιοδήποτε πορτοφόλι με υπόλοιπο άνω του 1 PZM και αυτόματα σταματά όταν επιτευχθεί υπόλοιπο 1 εκατομμυρίου PZM.

Επίσης, για πρώτη φορά εφαρμόστηκε το σύστημα δημιουργίας δεσμών παραπομπής χωρίς τη χρήση οποιωνδήποτε συνδέσμων. Αφού δημιουργήσει ένα νέο πορτοφόλι, το σύστημα καταγράφει στο blockchain από το οποίο φθάνει η πρώτη συναλλαγή και καθιερώνει μόνιμα μια αλυσίδα παραπομπής που δεν μπορεί να αλλάξει, αυτό καθιστά εύκολη την κατασκευή παγκόσμιων δικτύων MLM και την αύξηση της ταχύτητας της νέας εξόρυξης νομισμάτων.

Η τεχνική υλοποίηση δεν περιγράφεται λεπτομερώς επί του παρόντος εξαιτίας του γεγονότος ότι για όλους μας, το κύριος σκοπός είναι να δημιουργήσουμε όχι 100 "νεκρά" εργαλεία, αλλά το ένα με καλή στήριξη και καλή δουλειά. Εάν αποκαλυφθεί η τεχνογνωσία μας, τότε κάποιος θα προσπαθήσει σίγουρα να το επαναλάβει και αυτό θα οδηγήσει κατά λάθος σε μια διάσπαση της προσοχής και τη χρήση αυτής της ιδέας όχι για ευγενικούς και σημαντικούς στόχους για τον πλανήτη μας, αλλά για σκοπούς που δεν γνωρίζουμε και δεν είναι πάντα με θετική πρόθεση.

P R I Z M

ΠΕΡΙΠΤΩΣΕΙΣ ΕΞΟΡΥΞΗΣ

Για να ξεκινήσετε την εξόρυξη ενός νέου pzm, χρειάζεται ένα μόνο νόμισμα σε ένα ηλεκτρονικό πορτοφόλι και ξεκινά αυτόματα το ParaMining. Αυτή είναι μια διαδικασία που σας επιτρέπει να αυξήσετε τον αριθμό των νομισμάτων στο πορτοφόλι χωρίς κόστος ηλεκτρικής ενέργειας.

Η εξόρυξη ξεκινάει με 1 νόμισμα και σταματάει αυτόματα όταν φτάσετε το 1 εκατομμύριο νομίσματα στο πορτοφόλι σας.

Paramaning — είναι μια μοναδική μέθοδος δημιουργίας νέων νομισμάτων από όλους τους χρήστες ταυτόχρονα, που επηρεάζεται από τρεις παραμέτρους:

1 - Τον αριθμό των νομισμάτων στο προσωπικό σας πορτοφόλι
2 - Τον αριθμό των νομισμάτων της δομής των ακολούθων
3 - Τη δυσκολία εξόρυξης που ονομάζεται Paratax

1 - Αριθμός νομισμάτων στο προσωπικό πορτοφόλι σας

Αριθμός νομισμάτων στο προσωπικό πορτοφόλι (PZM)	Ημερήσιο κέρδος	Μηνιαίο κέρδος
Από 500.000 έως 1.000.000	**0,33%**	**9,9%**
Από 100.000 έως 499.999	**0,28%**	**8,4%**
Από 50.000 έως 99.999	**0,25%**	**7,5%**
Από 10.000 έως 49.999	**0,21%**	**6,3%**
Από 1.000 έως 9.999	**0,18%**	**5,4%**
Από 100 έως 999	**0,14%**	**4,2%**
Από 1 έως 99	**0,12%**	**3,6%**

2 - Τον αριθμό νομισμάτων της δομής των ακολούθων

Συνολικός όγκος	Συντελεστής
Από 1000 έως 9999	**2.18**
Από 10.000 έως 99.999	**2.36**
Από 100.000 έως 999.999	**2.77**
Από 1.000.000 έως 9.999.999	**3.05**
Από 10.000.000 έως 99.999.999	**3.36**
Από 100.000.000 έως 999.999.999	**3.88**
1.000.000.000	**4.37**

Η αρχή Paramining βασίζεται στους θεμελιώδεις νόμους της φυσικής, από την ενότητα "Ορατή ακτινοβολία". Όπως και το μοντέλο του Σύμπαντος μας, το σύστημα συνεχώς διευρύνεται, κερδίζοντας ταχύτητα, χάρη σε μια περίπλοκη επαναπροσδιορισμό του επιτοκίου με περίοδο 55 δευτερολέπτων.

PRIZM

Κάθε χρήστης με υπόλοιπο

Από 1000 έως 110 000 PZM

μπορεί να αυξήσει την περίοδο για τον υπολογισμό του σύνθετου ενδιαφέροντος, υπό την προϋπόθεση ότι το υπόλοιπο εμπλέκεται στη σφυρηλάτηση. Για να ξεκινήσετε την περίοδο **HOLD**, πρέπει να δημιουργήσετε τουλάχιστον ένα μπλοκ με στοχευμένες συναλλαγές. Η περίοδος **HOLD** δεν μπορεί να διακοπεί από μια εισερχόμενη συναλλαγή ή από τη λήψη τέλους σφυρηλάτησης. Η διάρκεια της περιόδου **HOLD** δεν περιορίζεται, υπό την προϋπόθεση ότι ο πλαστογράφος δημιουργεί τουλάχιστον ένα μπλοκ **100.000**.

Η περίοδος HOLD διακόπτεται από εξερχόμενη συναλλαγή.

PRIZM

ΠΕΡΙΠΤΩΣΕΙΣ ΕΞΟΡΥΞΗΣ

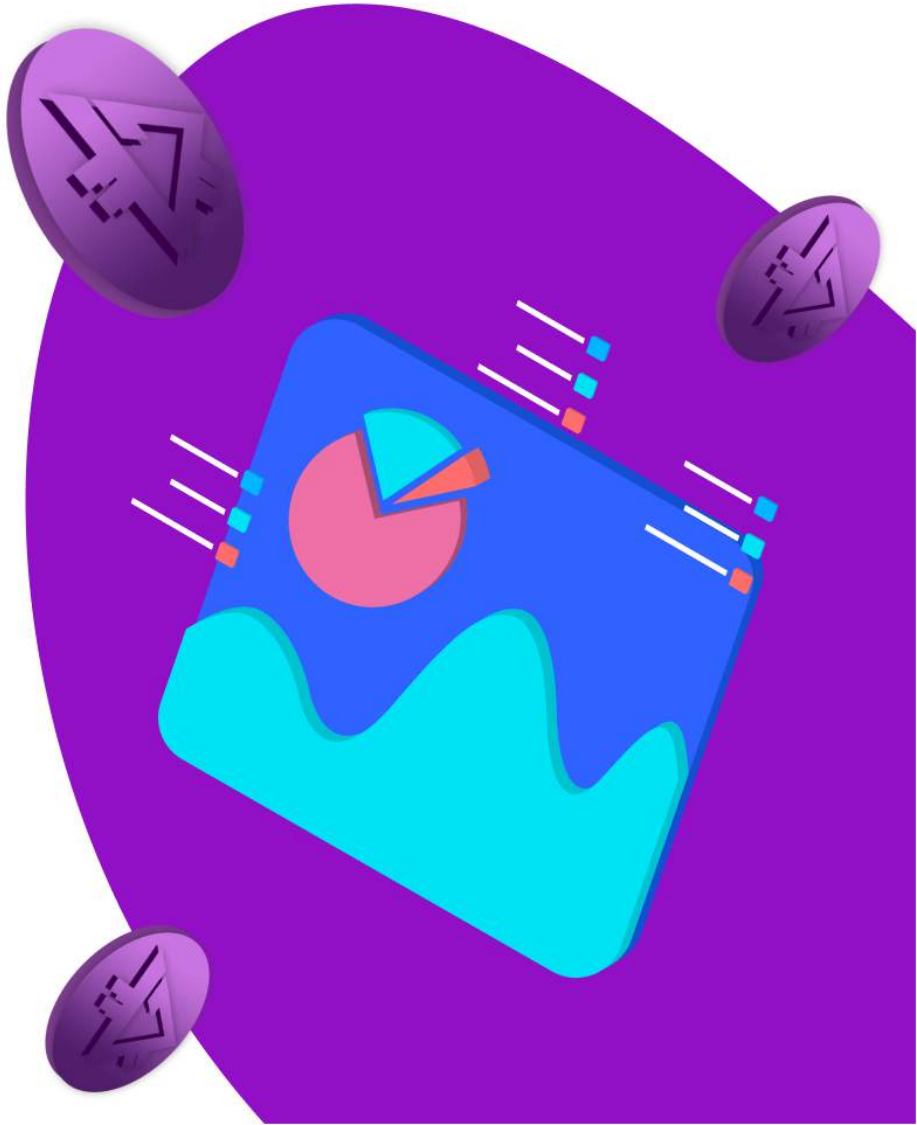
Δυσκολία Εξόρυξης

PARATAX

είναι μια γραμμική αύξηση της δυσκολίας δημιουργίας νομισμάτων, εκφραζόμενη ως ποσοστό του αριθμού των νομισμάτων που έχουν ήδη παραχθεί από όλους τους χρήστες.

Το ανώτατο όριο του Paratax θα είναι **98%** κατά την παραγωγή **3 δισεκατομμυρίων PZM.**

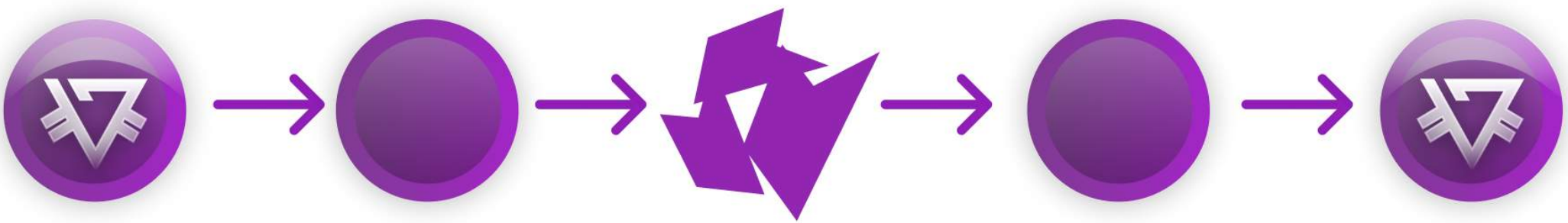
Για FORGERS των οποίων το υπόλοιπο κατά τη στιγμή της δημιουργίας του μπλοκ δεν υπερβαίνει τα **110.000 PZM**, η μέγιστη τιμή του PARATAX είναι **97%**



PRIZM

ΛΟΓΑΡΙΑΣΜΟΙ

Το Prizm έχει αναπτύξει ένα έξυπνο πορτοφόλι ως μέρος του σχεδιασμού του: όλοι οι λογαριασμοί αποθηκεύονται στο δίκτυο με προσωπικά κλειδιά για κάθε πιθανή διεύθυνση λογαριασμού, που προέρχονται απευθείας από τη ιδιωτική φράση κώδικα για κάθε λογαριασμό χρησιμοποιώντας έναν συνδυασμό λειτουργιών SHA256 και Curve25519. Κάθε λογαριασμός αντιπροσωπεύεται από έναν αριθμό 64 bit και αυτός ο αριθμός εκφράζεται ως διεύθυνση λογαριασμού χρησιμοποιώντας τη διόρθωση σφάλματος του κώδικα Solomon, ο οποίος σας επιτρέπει να ανιχνεύσετε έως και τέσσερα σφάλματα στη διεύθυνση του λογαριασμού ή να διορθώσετε έως και δύο σφάλματα . Αυτή η μορφή εφαρμόστηκε σε απάντηση στις ανησυχίες ότι μια λανθασμένη διεύθυνση λογαριασμού θα μπορούσε να οδηγήσει σε ψευδά νομίσματα ή μεταφορά κεφαλαίων προς ψευδείς λογαριασμούς που δεν μπορούν να ανακληθούν. Οι διευθύνσεις λογαριασμού προηγούνται πάντα από το "PRIZM -...", το οποίο καθιστά τις διευθύνσεις λογαριασμού Prizm εύκολα αναγνωρίσιμες και διακριτές από τις μορφές διευθύνσεων που χρησιμοποιούνται από άλλα κρυπτονομίσματα.



Ο λογαριασμός διευθύνσεων, ο κωδικοποιημένος με τον κώδικα Solomon που σχετίζεται με μια μυστική φράση πρόσβασης παράγεται με τον ακόλουθο τρόπο:

- Η μυστική φράση πρόσβασης κρυπτογραφείται χρησιμοποιώντας το πρωτόκολλο SHA256 για να δημιουργήσει το ιδιωτικό κλειδί του λογαριασμού.
- Το ιδιωτικό κλειδί κρυπτογραφείται χρησιμοποιώντας το Curve25519 για να δημιουργήσει το δημόσιο κλειδί του λογαριασμού.
- Το δημόσιο κλειδί έχει κρυπτογραφηθεί με SHA256 για να δημιουργηθεί το αναγνωριστικό λογαριασμού.
- Τα πρώτα 64 bits του λογαριασμού είναι ο ορατός αριθμός λογαριασμού.
- Κωδικοποίηση του κώδικα Solomon, ο ορατός αριθμός λογαριασμού με το πρόθεμα "PRIZM -" δημιουργεί τη διεύθυνση του λογαριασμού.

Όταν ένας λογαριασμός έχει πρόσβαση με τη μυστική φράση πρόσβασης για πρώτη φορά, δεν προστατεύεται από δημόσιο κλειδί. Όταν πραγματοποιείται η πρώτη εξερχόμενη συναλλαγή από το λογαριασμό, το δημόσιο κλειδί 256-bit που λαμβάνεται από τη φράση πρόσβασης αποθηκεύεται στο blockchain και αυτό προστατεύει το λογαριασμό. Ο χώρος διευθύνσεων για τα δημόσια κλειδιά (2256) είναι μεγαλύτερος από τον χώρο διεύθυνσης για αριθμούς λογαριασμού (264), επομένως δεν υπάρχει αντιστοιχία λέξεων-κλειδιών με τους αριθμούς λογαριασμών και πιθανές συγκρούσεις. Αυτές οι συγκρούσεις εντοπίζονται και παρεμποδίζονται ως εξής: αφού χρησιμοποιείται μια συγκεκριμένη φράση πρόσβασης για να αποκτήσετε πρόσβαση στο λογαριασμό και ο λογαριασμός προστατεύεται με δημόσιο κλειδί 256-bit, κανένα άλλο ζεύγος δημόσιου-ιδιωτικού κλειδιού δεν μπορεί να έχει πρόσβαση σε αυτόν τον αριθμό λογαριασμού.

PRIZM

Οι ιδιότητες του κεφαλαίου ενός λογαριασμού:

1 Ένα αποτελεσματικό υπόλοιπο λογαριασμού χρησιμοποιείται ως βάση για τη χρέωση του λογαριασμού σας. Ένα αποτελεσματικό υπόλοιπο λογαριασμού αποτελείται από όλα τα νομίσματα που ήταν στατικά για το λογαριασμό αυτό για 1.440 μπλοκ. Επιπλέον, η λειτουργία "Account Leasing" σας επιτρέπει να ορίσετε ένα αποτελεσματικό υπόλοιπο σε έναν άλλο λογαριασμό για μια προσωρινή περίοδο.

2 Το εγγυημένο υπόλοιπο λογαριασμού αποτελείται από όλα τα νομίσματα που ήταν στάσημα στο λογαριασμό για 1.440 μονάδες. Δυστυχώς για να είναι ένα κεφάλαιο αποτελεσματικό, δεν μπορεί να μεταφερθεί σε κανένα άλλο λογαριασμό.

3 Το βασικό υπόλοιπο του λογαριασμού βάσης αντιστοιχεί σε όλες τις συναλλαγές που έχουν τουλάχιστον μία επιβεβαίωση.
Το συνολικό υπόλοιπο του λογαριασμού αντιστοιχεί στη συνολική ποσότητα PZM που ελήφθη ως αποτέλεσμα της δημιουργίας επιτυχημένων μπλοκς.

4 Το μη επιβεβαιωμένο υπόλοιπο λογαριασμού είναι αυτό που εμφανίζεται στους πελάτες Prizm. Αντιπροσωπεύει το υπόλοιπο κεφάλαιο των τρέχουσων συναλλαγών, καθαρό από τα νομίσματα που εμπλέκονται σε μη επιβεβαιωμένες, απεσταλμένες συναλλαγές.

5 Εγγυημένη λίστα υπολοίπων περιουσιακών στοιχείων (να καταγράψετε) εγγυημένα υπόλοιπα όλων των στοιχείων ενεργητικού που σχετίζονται με συγκεκριμένο λογαριασμό.

6 Μη επιβεβαιωμένα υπόλοιπα και μη επιβεβαιωμένη λίστα υπολοίπων για όλα τα κεφάλαια που σχετίζονται με συγκεκριμένο λογαριασμό.

PRIZM

WALLET.DAT

Το Bitcoin και τα συναφή νομίσματα χρησιμοποιούν συχνά ένα κρυπτογραφημένο αρχείο, σύμφωνα με το όνομα και το πορτοφόλι, για την αποθήκευση των παραγόμενων διευθύνσεων για τη λήψη νομισμάτων. Ο επόμενος πυρήνας που χρησιμοποιείται στο Prizm ούτε προσομοιώνει αυτή τη λειτουργία, ούτε την αποκλείει. Οι προγραμματιστές των πελατών μπορούν να εφαρμόσουν ένα σύστημα στο οποίο ένα σύνολο ιδιωτικών κλειδιών για λογαριασμούς Prizm αποθηκεύεται σε ένα κρυπτογραφημένο αυτόνομο αρχείο.

Επιβεβαίωση των συναλλαγών

Όλες οι συναλλαγές PZM θεωρούνται ανεπιβεβαίωτες μέχρις ότου συμπεριληφθούν σε έγκυρο μπλοκ του δικτύου. Τα νεοσυσταθέντα μπλοκ διανέμονται στο δίκτυο από τον κόμβο (και τον συνδεδεμένο λογαριασμό) που τα δημιουργεί και η συναλλαγή που περιλαμβάνεται στο μπλοκ θεωρείται ότι λαμβάνεται με μία επιβεβαίωση. Καθώς τα επόμενα μπλοκ προστίθενται σε μια υπάρχουσα μπλοκ αλυσίδα, κάθε επιπλέον μπλοκ προσθέτει μια άλλη επιβεβαίωση στον αριθμό των επιβεβαιωμένων συναλλαγών. Εάν μια συναλλαγή δεν περιλαμβάνεται στο μπλοκ πριν τη λήξη του, θα καεί και θα διαγραφεί από την ομάδα συναλλαγών.

Ο συγχρονισμός των συναλλαγών

Κάθε συναλλαγή περιέχει μια παράμετρο προθεσμίας που έχει οριστεί ως η διάρκεια σε λεπτά από την αποστολή της συναλλαγής στο δίκτυο. Από προεπιλογή, η προθεσμία είναι 1440 λεπτά (24 ώρες). Μια συναλλαγή που στάλθηκε στο δίκτυο αλλά δεν συμπεριλήφθηκε στο μπλοκ ονομάζεται συναλλαγή που δεν επιβεβαιώνεται.

Εάν η συναλλαγή δεν συμπεριλήφθηκε στο μπλοκ πριν από την προθεσμία συναλλαγής, η συναλλαγή καταργείται από το δίκτυο. Οι συναλλαγές μπορούν να θεωρηθούν ανεπιβεβαίωτες επειδή είναι άκυρες ή παραμορφωμένες ή επειδή τα μπλοκ είναι γεμάτα με συναλλαγές που έχουν να πληρώσουν υψηλότερα ποσά. Στο μέλλον, τα χαρακτηριστικά όπως οι συναλλαγές πολλαπλών υπογραφών μπορούν να χρησιμοποιούν προθεσμίες ως μέσο για την επιβολή της λήξης της συναλλαγής.

PRIZM

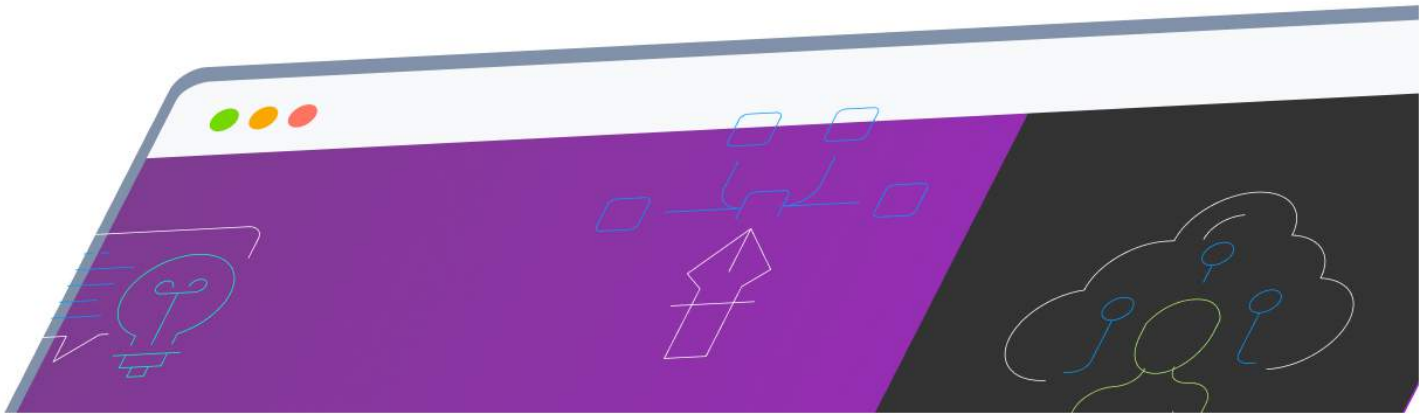
WALLET.DAT

Δημιουργία και διεκπεραίωση των συναλλαγών

Λεπτομερείς πληροφορίες σχετικά με τη δημιουργία και την διεκπεραίωση μιας συναλλαγής PZM είναι οι εξής: - Ο αποστολέας καθορίζει τις παραμέτρους της συναλλαγής.

Οι τύποι συναλλαγών αλλάζουν και καθορίζετε τον τύπο που επιθυμείτε όταν δημιουργείτε τη συναλλαγή, αλλά για όλες τις συναλλαγές πρέπει να ορίσετε πολλαπλές παραμέτρους:

- Το ιδιωτικό κλειδί για τον λογαριασμό αποστολής
- Η προθεσμία της συναλλαγής
- Προαιρετική αναφορά συναλλαγής



Η ανταλλαγή κλειδιών στο Prizm βασίζεται στον αλγόριθμο Curve25519, ο οποίος δημιουργεί κοινό μυστικό χρησιμοποιώντας την ταχύτατη και αποτελεσματική ελλειπτική καμπύλη Dilhe-Hellman με υψηλό βαθμό προστασίας. Ο αλγόριθμος παρουσιάστηκε αρχικά από τον Daniel j. Bernstein το 2OO6. Οι επόμενες υλοποιήσεις στην java εξετάστηκαν από τον Doctor Evil τον Μάρτιο του 2014. Η υπογραφή των μηνυμάτων στο Prizm πραγματοποιείται χρησιμοποιώντας τον αλγόριθμο ψηφιακής υπογραφής Elliptic-Curve (EC-KCDSA), ο οποίος ορίστηκε από την ομάδα IEEE P1363a το 1998 από την εκτελεστική ομάδα KCDSA. Και οι δύο αλγόριθμοι επιλέχθηκαν για να εξισορροπήσουν την ταχύτητα και την ασφάλεια για ένα μέγεθος κλειδιού μόνο 32 byte.

Βασικά χαρακτηριστικά

Προχωρημένη διεπαφή σε κώδικα java

Εύχρηστη εφαρμογή διαχείρισης δεύτερης γενιάς ενσωματωμένη στη βασική διανομή του λογισμικού Prizm, και η οποία μπορεί να προσπελαστεί μέσω ενός τοπικού προγράμματος περιήγησης ιστού. Η εφαρμογή διαχείρισης παρέχει πλήρη υποστήριξη για όλες τις σημαντικές λειτουργίες Prizm που χρειάζονται, ώστε τα ιδιωτικά κλειδιά των χρηστών να μην είναι ποτέ διαθέσιμα στο διαδίκτυο. Περιλαμβάνει επίσης βελτιωμένο περιβάλλον διαχείρισης και ενσωματωμένο εγχειρίδιο του javadoc για τη διεπαφή προγραμματισμού εφαρμογών του Prizm χαμηλής προτεραιότητας.

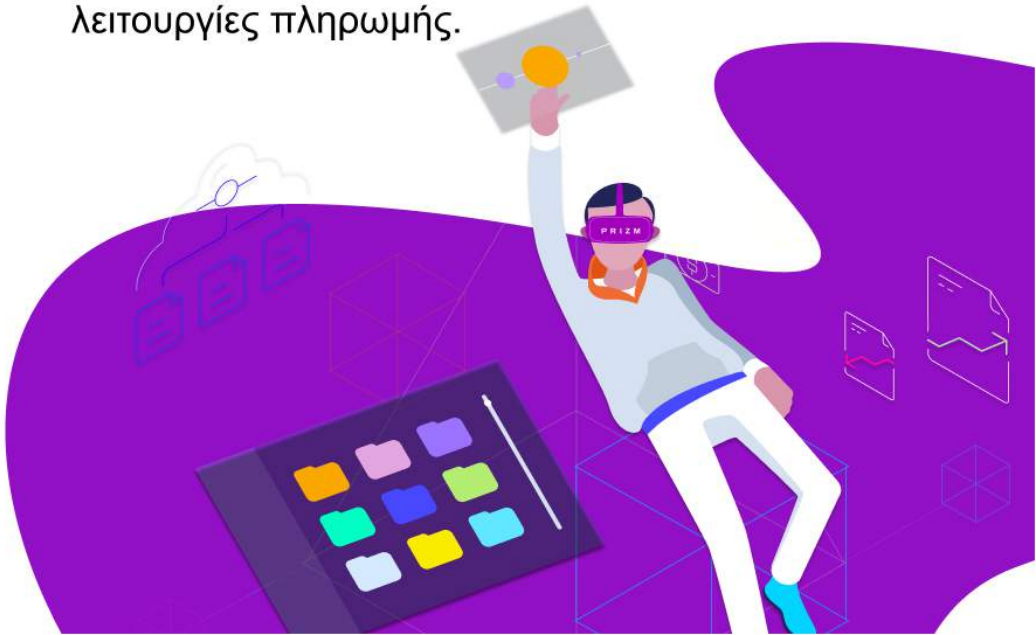
PRIZM

Φορητή συσκευή

Χάρη στην διασταυρούμενη πλατφόρμα που βασίζεται στις ρίζες του java, την κρυπτογράφηση του Proof of Stake και τη μελλοντική του ικανότητα να μειώσει το μέγεθος της αλυσίδας μπλοκ, το Prizm είναι εξαιρετικά κατάλληλο για χρήση σε μικρές συσκευές χαμηλής ισχύος, χαμηλής κατανάλωσης ενέργειας. Οι εφαρμογές και το λογισμικό Android και iPhone έχουν μεταφερθεί σε συσκευές ARM χαμηλής κατανάλωσης όπως οι πλατφόρμες RaspberryPi και CubieTruck. Η δυνατότητα εφαρμογής του Prizm σε συσκευές χαμηλής ισχύος, πάντα συνδεδεμένες όπως τα smartphones, μας επιτρέπει να παρουσιάσουμε ένα σενάριο στο οποίο υποστηρίζονται τα περισσότερα δίκτυα Prizm σε κινητές συσκευές. Το χαμηλό κόστος και η κατανάλωση πόρων αυτών των συσκευών μειώνει σημαντικά το κόστος του δικτύου σε σύγκριση με τα παραδοσιακά κρυπτονομίσματα Proof of Work.

Βασικές πληρωμές

Το πιο θεμελιώδες χαρακτηριστικό κάθε κρυπτογράφησης είναι η δυνατότητα μεταφοράς νομισμάτων από τον ένα λογαριασμό στον άλλο. Αυτός είναι ο πιο βασικός τύπος συναλλαγών του Prizm και σας επιτρέπει να χρησιμοποιείτε τις βασικές λειτουργίες πληρωμής.



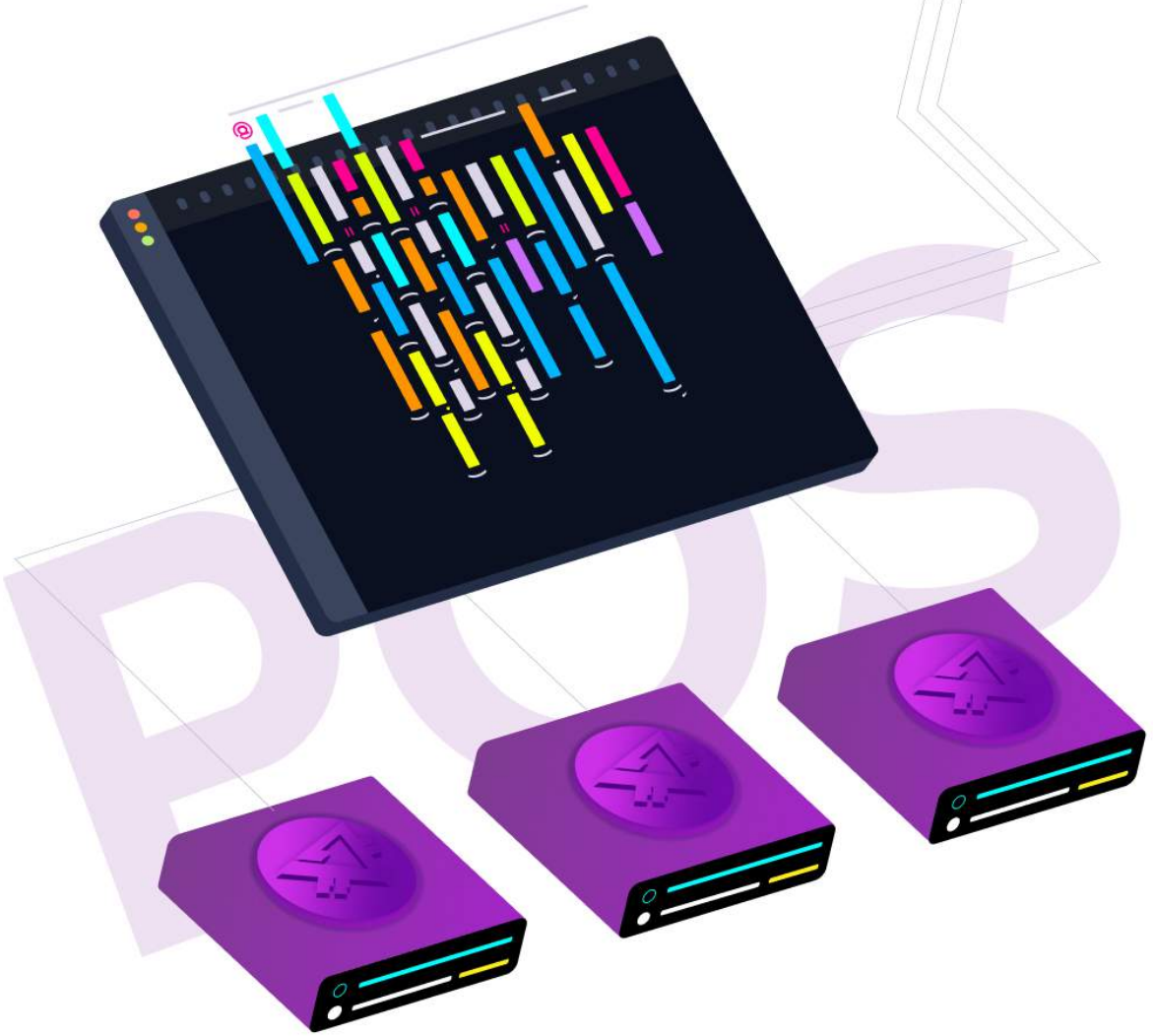
PRIZM

PRIZM ΛΕΙΤΟΥΡΓΙΕΣ ΚΛΕΙΔΙΑ

POS — Τύπος σφυρηλάτησης

Η συγχώνευση δύο τεχνολογιών ταυτόχρονα: εξόρυξη + σφυρηλάτηση. Οι πηγαίοι κώδικες είναι κλειστοί (χωρίς επένδυση), για ένα ορισμένο χρονικό διάστημα, ως προστασία έναντι των κλώνων ως εγγύηση ότι το σύστημα θα είναι “διάφανο”.

Πρόγραμμα συνεργατών 88 επιπέδων στη δομή NEXT / Proof of stake πυρήνα του κρυπτοσυστήματος
Φιλικό προς το χρήστη περιβάλλον για κινητές συσκευές
Ο κωδικός πρόσβασης χρήστη δεν αποστέλλεται στον διακομιστή



Nothing at stake

Στην επίθεση "τίποτα δεν διακυβεύεται", οι πλαστογράφοι προσπαθούν να χτίσουν μπλοκ πάνω από όλα τα πιρούνια που βλέπουν επειδή δεν τους κοστίζουν σχεδόν τίποτα και επειδή αγνοώντας οποιοδήποτε πιρούνι μπορεί να σημαίνει να χάσετε από το μπλοκ τις αμοιβές που θα κερδίζονταν εάν είχαν σχεδιαστεί αυτό το πιρούνι να γίνει η αλυσίδα με την πιο αθροιστική δυσκολία. Παρόλο που αυτή η επίθεση είναι θεωρητικά δυνατή, είναι σήμερα ανέφικτη, το δίκτυο Prizm δεν έχει να αντιμετωπίσει μεγάλα πιρούνια του blockchain και η ανταμοιβή για χαμηλά μπλοκ δεν δίνει ισχυρό κίνητρο για κέρδος. Επιπλέον, η συμβιβαστική ασφάλεια του δικτύου και η εμπιστοσύνη για ένα τόσο μικρό κέρδος θα μπορούσαν να κάνουν οποιαδήποτε νίκη απατηλή.

Επιθέσεις στο ιστορικό

Στην "επίθεση στο ιστορικό", κάποιος αποκτά μεγάλο αριθμό νομισμάτων, τα πουλάει και στη συνέχεια προσπαθεί να δημιουργήσει ένα επιτυχές πιρούνι λίγο πριν τα νομίσματα του πωληθούν ή ανταλλάχθουν. Εάν η επίθεση αποτύχει, η προσπάθεια είναι άχρηστη επειδή τα νομίσματα πωλούνται ή μεταφέρονται: Εάν η επίθεση επιτύχει, ο εισβολέας παίρνει τις μάρκες του πίσω. Οι ακραίες μορφές αυτής της επίθεσης περιλαμβάνουν την απόκτηση ιδιωτικών κλειδιών από παλιούς λογαριασμούς και τη χρήση τους για την οικοδόμηση μιας επιτυχημένης αλυσίδας απευθείας από το μπλοκ Genesis. Στο Prizm, η επίθεση στο κύριο ιστορικού συνήθως αποτυγχάνει επειδή όλα τα νομίσματα πρέπει να διατηρηθούν για 1.440 μπλοκς πριν αυτά μπορέσουν να χρησιμοποιηθούν για σφυρηλάτηση: Επιπλέον, το πραγματικό υπόλοιπο λογαριασμού που παράγει κάθε μπλοκ επαληθεύεται ως μέρος του ελέγχου του μπλοκ. Η ακραία μορφή αυτής της επίθεσης συνήθως αποτυγχάνει επειδή η μπλοκ αλυσίδα PRIZM δεν μπορεί να αναδιοργανωθεί περισσότερο από 720 μπλοκ πίσω από το τρέχον ύψος του μπλοκ. Αυτό περιορίζει το χρονικό πλαίσιο εντός του οποίου ένας κακός ηθοποιός θα μπορούσε να δημιουργήσει αυτή τη μορφή επίθεσης.

ЕФАРМОГН

Τα προβλήματα Bitcoin, που εξετάζονται στο Prizm.

Το Prizm δημιουργήθηκε ως κρυπτονόμισμα 2.0 - απάντηση στο Bitcoin. Το Prizm χρησιμοποιεί λειτουργίες που έχουν καθιερωθεί στο Bitcoin και εξετάζει τις ανησυχητικές πτυχές. Αυτή η εφαρμογή αντιμετωπίζει ζητήματα με το πρωτόκολλο Bitcoin και το δίκτυο του, τα οποία εξομαλύνονται με την τεχνολογία του Prizm.

Σχετικά με τις συναλλαγές ανά ημέρα

Μέχρι το τέλος του 2013, ο αριθμός των συναλλαγών που επεξεργάστηκαν στο δίκτυο Bitcoin έφτασε το μέγιστο 70,000 ανά ημέρα, δηλαδή περίπου 8,8 συναλλαγές ανά δευτερόλεπτο (tps). Το τρέχον τυποποιημένο μέγεθος του μπλοκ του Bitcoin που είναι ενός megabyte, που παράγεται (κατά μέσο όρο) κάθε δέκα λεπτά εξ ολοκλήρου στο site των πελατών, περιορίζει το μέγιστο εύρος ζώνης του υπάρχοντος δικτύου του Bitcoin σε περίπου 7 TPS. Συγκρίνετε αυτό με το εύρος ζώνης του δικτύου της VISA για να χειριστείτε 10.000 TPS και θα δείτε ότι το Bitcoin δεν μπορεί να ανταγωνιστεί όπως είναι σήμερα.

Μέγεθος Blockchain

Το Bitcoin Blockchain είναι μια πλήρης διαδοχική συλλογή των παραγόμενων μπλοκ δεδομένων που περιέχουν το ηλεκτρονικό βιβλίο που καταγράφει όλες τις συναλλαγές του Bitcoin που πραγματοποιήθηκαν από την έναρξή του, τον Ιανουάριο του 2009. Τέσσερα χρόνια αργότερα, τον Ιανουάριο του 2013, το μέγεθος blockchain του Bitcoin ήταν 4 gigabytes (GB) - το κατά προσέγγιση ποσό των δεδομένων που απαιτούνται για την αποθήκευση μιας ταινίας διάρκειας δύο ωρών σε ένα DVD. Δεκαοκτώ μήνες αργότερα, τον Ιανουάριο του 2014, το μέγεθος του blockchain του Bitcoin αυξήθηκε κατά σχεδόν πέντε φορές, στα 19 gigabytes (GB) 37. Το blockchain του Bitcoin εξελίσσεται εκθετικά και οι τροποποιήσεις του αρχικού πρωτοκόλλου Bitcoin απαιτούν λύση σε αυτό.

Η απάντηση του PRIZM

Στην τρέχουσα κατάσταση του, το Prizm μπορεί να χειριστεί έως και 367.200 συναλλαγές την ημέρα - περισσότερο από εννέα φορές την τρέχουσα μέγιστο αριθμό συναλλαγών του Bitcoin. Η εφαρμογή Transparent Forging επιτρέπει την άμεση επεξεργασία συναλλαγών, αυξάνοντας σημαντικά αυτό το όριο.

Χρόνος για επιβεβαίωση συναλλαγής

Ο χρόνος επιβεβαίωσης συναλλαγής για το Bitcoin κυμάνθηκε από 5 έως 10 λεπτά κατά το μεγαλύτερο μέρος τη διάρκεια του 2013. Στο τέλος του 2013 μετά την ανακοίνωση ότι οι κινεζικές τράπεζες δεν θα είχαν τη δυνατότητα επεξεργασίας Bitcoins, ο μέσος χρόνος συναλλαγής Bitcoin αυξήθηκε σημαντικά, σε 8-13 λεπτά , με περιοδικές κορυφές 19 λεπτών. Από τότε, ο χρόνος επιβεβαίωσης έχει μετατοπιστεί από 8 σε 10 λεπτά. Ωστόσο, επειδή αρκετοί έλεγχοι (συνήθως έξι προτιμώμενες επιβεβαιώσεις) απαιτούνται για την ολοκλήρωση μιας συναλλαγής Bitcoin, μία ώρα μπορεί εύκολα να περάσει πριν ολοκληρωθεί η πώληση των κεφαλαίων που καταβλήθηκαν σε Bitcoin.

Η απάντηση του PRIZM

Ο μέσος χρόνος δημιουργίας μπλοκ για το PZM ήταν ιστορικά 80 δευτερόλεπτα και ο μέσος χρόνος διεκπεραίωσης των συναλλαγών ήταν ο ίδιος. Οι συναλλαγές θεωρούνται ασφαλείς μετά από δέκα επιβεβαιώσεις, πράγμα που σημαίνει ότι οι συναλλαγές γίνονται μόνιμες σε λιγότερο από 14 λεπτά. Η εφαρμογή Transparent Forging σας επιτρέπει να κάνετε σχεδόν άμεσες συναλλαγές, οι οποίες θα μειώσουν περαιτέρω αυτόν το χρόνο.

Προβλήματα συγκέντρωσης

Η αύξηση της πολυπλοκότητας μαζί με το ποσοστό κατακερματισμού για το Bitcoin δημιούργησαν ένα υψηλό εμπόδιο για την είσοδο των νεοεισερχομένων και χαμηλότερα κέρδη για τις υπάρχουσες εγκαταστάσεις εξόρυξης. Το κίνητρο για την ενθάρρυνση των μπλοκ που χρησιμοποίησε η Bitcoin οδήγησε στη δημιουργία μεγάλων μοναδικών εγκαταστάσεων εξειδικευμένου εξοπλισμού εξόρυξης 44, καθώς και στην εξάρτηση από ένα μικρό σύνολο μεγάλων ορυχείων 45. Αυτό είχε ως αποτέλεσμα την «συγκέντρωση». Όπου Μεγάλοι όγκοι εξόρυξης συγκεντρώνονται στον έλεγχο ενός μειούμενου αριθμού ανθρώπων. Αυτό όχι μόνο δημιουργεί το είδος της δομής εξουσίας που το Bitcoin έχει σχεδιάσει να παρακάμψει, αλλά παρουσιάζει επίσης την πραγματική πιθανότητα μια ενιαία επιχείρηση εξόρυξης ή μάζα να κερδίσει το 51% της συνολικής δυναμικότητας εξόρυξης στο δίκτυο 46 και να προκαλέσει μία 51% επίθεση. Υπάρχουν επίσης επιθέσεις που απαιτούν μόνο το 25% της συνολικής δυνατότητας κατακερματισμού του δικτύου. Στις αρχές Ιανουαρίου του 2014, η GHash.io άρχισε να μειώνει οικειοθελώς τη δύναμη της δικής της εξόρυξης, καθώς πλησίαζε το επίπεδο του 51%. Λίγες μέρες αργότερα, η ισχύς στην πισίνα μειώθηκε στο 34% της συνολικής χωρητικότητας του δικτύου, αλλά η ταχύτητα άρχισε αμέσως να αυξάνεται και τον Ιούνιο του 2014 έφθασε και πάλι σε επικίνδυνα επίπεδα.

Answer of PRIZM

Τα κίνητρα που παρέχει ο αλγόριθμος Proof of Stake που χρησιμοποιείται στο Prizm παρέχουν χαμηλή απόδοση επένδυσης περίπου 0,1%. Δεδομένου ότι δεν δημιουργούνται νέα νομίσματα με κάθε μπλοκ, δεν υπάρχει επιπλέον "ανταμοιβή για εξόρυξη", η οποία διεγείρει τις κοινές προσπάθειες για τη δημιουργία μπλοκ. Τα δεδομένα δείχνουν ότι το δίκτυο Prizm παρέμεινε πολύ αποκεντρωμένο από την έναρξή του: ένας μεγάλος (και αυξανόμενος) αριθμός μοναδικών λογαριασμών προσθέτει μπλοκ στο δίκτυο.

Proof of Work - κόστος συντήρησης

Η επιβεβαίωση των συναλλαγών στα υπάρχον bitcoin και η δημιουργία νέων bitcoins για να μπουν στην κυκλοφορία απαιτούν τεράστια υπολογιστική ισχύ, η οποία πρέπει να λειτουργεί συνεχώς. Αυτή η υπολογιστική ισχύς παρέχεται από τα λεγόμενα δίκτυα εξόρυξης, τα οποία διαχειρίζονται οι ανθρακωρύχοι. Οι ανθρακωρύχοι Bitcoin ανταγωνίζονται μεταξύ τους για να προσθέσουν το επόμενο μπλοκ συναλλαγών στη συνολική αλυσίδα bitcoin. Αυτό γίνεται με το "hashing" - συνδυάζοντας όλες τις συναλλαγές Bitcoin που συμβαίνουν μέσα στα τελευταία δέκα λεπτά και προσπαθώντας να τις κρυπτογραφήσουν σε ένα μπλοκ δεδομένων, το οποίο επίσης συμπτωματικά έχει έναν ορισμένο αριθμό διαδοχικών μηδενικών. Τα περισσότερα δοκιμαστικά μπλοκ που παράγονται από τους ανθρακωρύχους δεν έχουν αυτό το στόχο για μηδενικά, έτσι κάνουν μικρές αλλαγές και προσπαθούν ξανά. Ένα δισεκατομμύριο προσπαθεί να βρει αυτό το μπλοκ που κερδίζει που ονομάζεται GH, η αξιολόγηση ενός δικτύου εξόρυξης υπολογίζεται από το πόσα GH μπορεί να εκτελεί ανά δευτερόλεπτο, που δηλώνεται με GH / sec. Ο νικητής ορυχείο, ο οποίος ήταν ο πρώτος που δημιούργησε ένα κρυπτολογικά σωστό μπλοκ Bitcoin, λαμβάνει αμέσως μια ανταμοιβή 25 νέων bitcoins - η ανταμοιβή κατά τη στιγμή της γραφής ήταν περίπου 15.750 δολάρια ΗΠΑ. Αυτός ο διαγωνισμός με το βραβείο μεταξύ των ανθρακωρύχων επαναλαμβάνεται ξανά και ξανά κάθε δέκα λεπτά περίπου. Στις αρχές του 2014, είχαν δημιουργηθεί περισσότερα από 3.500 bitcoins ημερησίως, ίσα με περίπου 2,2 εκατομμύρια δολάρια ημερησίως. Με τόσα πολλά χρήματα στο στοίχημα, οι ανθρακωρύχοι υποστήριξαν την ταχεία κούρσα εξοπλισμών στην τεχνολογία δικτύων εξόρυξης για να βελτιώσουν τις πιθανότητές τους να κερδίσουν. Αρχικά, τα bitcoins εξορυσσόταν χρησιμοποιώντας έναν κεντρικό επεξεργαστή (CPU), έναν τυπικό επιτραπέζιο υπολογιστή. Στη συνέχεια, για να αυξηθεί η ταχύτητα, χρησιμοποιήθηκε το chip της εξειδικευμένης μονάδας επεξεργασίας γραφικών (GPU) που χρησιμοποιούνταν σε κάρτες γραφικών υψηλής τεχνολογίας. Στη συνέχεια χρησιμοποιήθηκε ο μικροεπεξεργαστής με προγραμματιζόμενη διάταξη πύλης (FPGA) και στη συνέχεια η μάρκα εξειδικευμένων ολοκληρωμένων κυκλωμάτων (ASIC). Η τεχνολογία ASIC είναι η κορυφή των προτιμήσεων για τους ανθρακωρύχους, αλλά ο αγώνας των εξοπλισμών συνεχίζεται με την εμφάνιση διαφόρων γενεών τσιπ ASC.

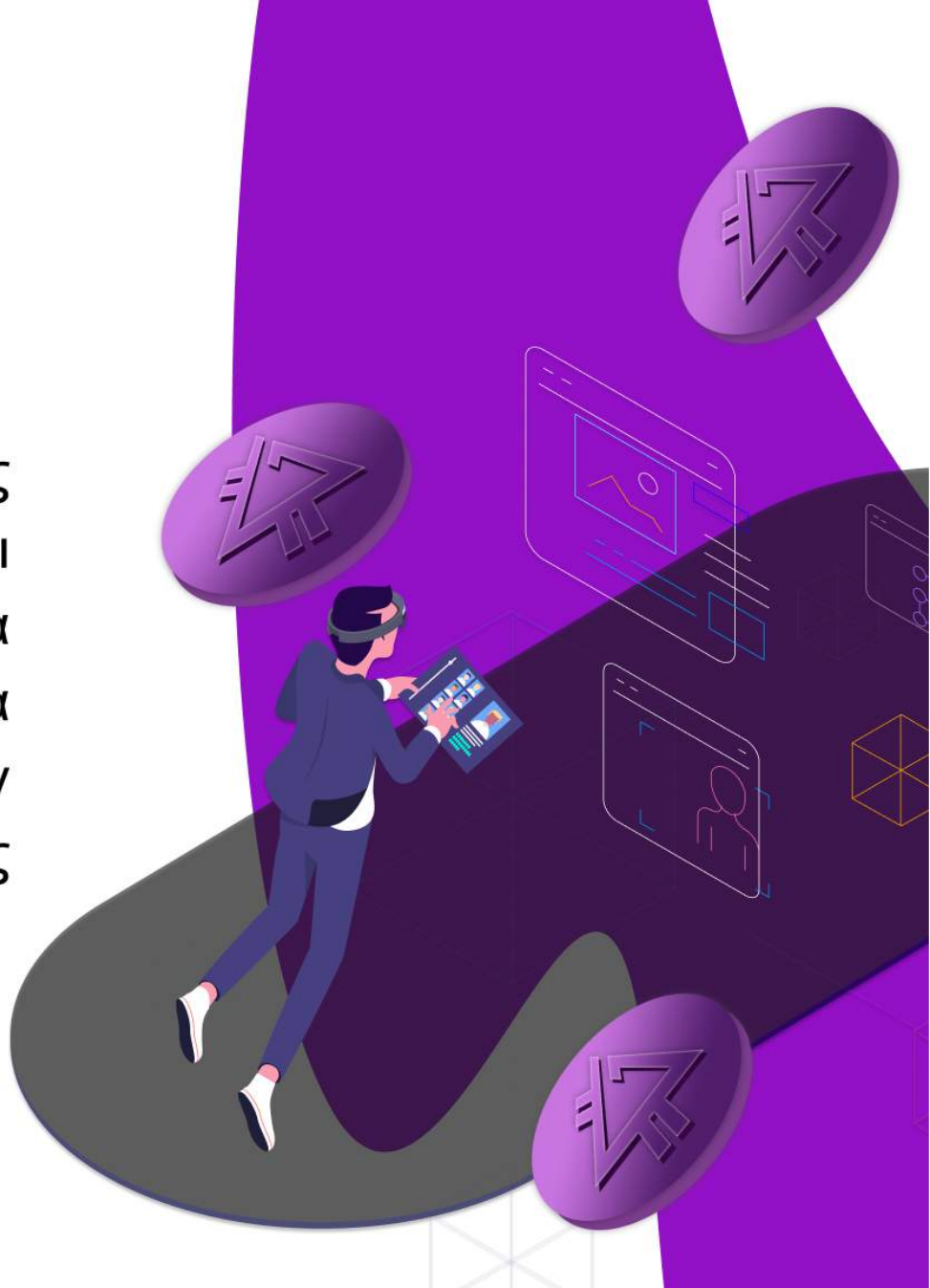
Proof of Work - κόστος συντήρησης

Η τρέχουσα γενιά των τσιπ ASIC είναι οι λεγόμενες συσκευές των 28 nm σύμφωνα με το μέγεθος των μικροσκοπικών τρανζίστορ τους σε νανόμετρα. Από το τέλος του 2014 έχουν αντικατασταθεί από δομικά στοιχεία των 20 nm ASIC. Ένα παράδειγμα δικτύου εξόρυξης τελευταίας τεχνολογίας θα ήταν μια κάρτα 28 nm ASIC "The Monarch" από τα Butterfly Labs, η οποία θα παρέχει 600 GH / sec για κατανάλωση ηλεκτρικής ενέργειας των 350 Watt και κόστος 2.200 δολαρίων. Η υποδομή εξόρυξης ορυχείων, η οποία χρησιμοποιείται επί του παρόντος για την υποστήριξη των σημερινών δραστηριοτήτων του Bitcoin, είναι εντυπωσιακή. Το Bitcoin ASIC είναι παρόμοιο με τους αυτιστικούς επιστήμονες - μπορούν μόνο να εκτελέσουν τον υπολογισμό ενός μπλοκ bitcoins και τίποτα περισσότερο, αλλά μπορούν να το κάνουν με έναν υπολογισμό στις ταχύτητες ενός υπερυπολογιστή. Τον Νοέμβριο του 2013, το περιοδικό Forbes δημοσίευσε ένα άρθρο με τίτλο "η παγκόσμια υπολογιστική ισχύς του bitcoin είναι 256 φορές πιο γρήγορη από 500 συνδυασμένους υπερυπολογιστές!". Στα μέσα Ιανουαρίου του 2014, τα στατιστικά στοιχεία που αποθηκεύτηκαν στον ιστότοπο blockchain.info, έδειξαν ότι η συνεχής υποστήριξη των λειτουργιών Bitcoin απαιτεί συνεχή ροή κρυπτογράφησης ύψους περίπου 18 εκατομμυρίων GH / s. Μέσα σε μια μέρα, αυτή η δύναμη κρυπτογράφησης παρήγαγε 1,5 τρισεκατομμύρια δοκιμαστικά μπλοκ, τα οποία δημιουργήθηκαν και απορρίφθηκαν από τη μαγιονέζα του Bitcoin, αναζητώντας το ένα μαγικό 144 μπλοκ που θα τους αποδώσει 2,2 εκατομμύρια δολάρια. Σχεδόν όλοι οι υπολογισμοί του Bitcoin δεν αποσκοπούν στην επίλυση της καταστροφής με τη μοντελοποίηση του DNA ή την αναζήτηση ραδιοφωνικών σημάτων από τον E.T. Αντ 'αυτού, σπαταλούνται τελείως. Η ισχύς και τα κόστη που συνδέονται με αυτή τη σπατάλη της υποστήριξης του Bitcoin στο φόντο είναι τεράστια. Αν όλα τα ορυχεία Bitcoin είχαν επίπεδα "Monarch", όπως περιγράφηκε παραπάνω - και δεν θα είναι μέχρι να αναβαθμιστούν - θα αντιπροσώπευαν μία πηγή από 30.000 μηχανές αξίας άνω των 63 εκατομμυρίων δολαρίων. Όπου θα κατανάλωνε περισσότερα από 10 megawatts συνεχούς ρεύματος κατά τη λειτουργία τους και ο λογαριασμός ηλεκτρικού ρεύματος να υπερβαίνει τα 3,5 εκατομμύρια δολάρια την ημέρα. Τα πραγματικά στοιχεία είναι πολύ υψηλότερα στη πραγματικότητα, με λιγότερο αποδοτική τη δεξαμενή μηχανημάτων εξόρυξης που υποστηρίζουν το Bitcoin σήμερα. Και αυτοί οι αριθμοί τώρα ανεβαίνουν την εκθετική καμπύλη ανάπτυξης ως bitcoin πορείες από την τρέχουσα μία συναλλαγή ανά δευτερόλεπτο στο μέγιστο των επτά συναλλαγών ανά δευτερόλεπτο.

Λύσεις Prizm

Η ανάλυση του κόστους και της ενεργειακής απόδοσης του δικτύου Prizm δείχνει ότι ολόκληρο το οικοσύστημα PRIZM μπορεί να διατηρηθεί για περίπου 60.000 δολάρια ετησίως, το οποίο είναι σήμερα σχεδόν 2.200 φορές φθηνότερο από το κόστος λειτουργίας του δικτύου Bitcoin.

PRIZM.SPACE



Το κόστος της συντήρησης του Proof of Work για τους κατόχους νομισμάτων

Εκτός από το τεράστιο κόστος της ηλεκτρικής ενέργειας, υπάρχει μια κρυφό κόστος για την απλή αποθήκευση των bitcoins, Για κάθε μπλοκ που παράγεται, εκείνος που δημιουργεί το μπλοκ λαμβάνει μια ανταμοιβή. Κατά τη διάρκεια αυτής της συγγραφής, μια ανταμοιβή είναι περίπου 12,5 BTC (προς το παρόν), η οποία είναι 10% πληθωρισμός στο σύνολο της προσφοράς του Bitcoin. Για κάθε $ 1.000 αξίας σε bitcoin που έχει στην κατοχή του ένα άτομο πληρώνει 100 δολάρια σε bitcoin για να «πληρώσει» τους ανθρακωρύχους για την ασφάλεια του δικτύου.

Ας είναι η δύναμη μαζί σου

Ενσωμάτωση PRIZM

Το σύστημα πληρωμών PRIZM είναι ο ευκολότερος τρόπος λήψης και αποστολής πληρωμών κρυπτονομισμάτων.

Μπορείτε εύκολα να ενσωματώσετε το PRIZM στο έργο σας, στο ηλεκτρονικό κατάστημα, σε ένα ανταλλακτήριο κλπ

Διαδικτυακό σεμινάριο:

https://pzm.space/en/pzm-integration/

Για να αρχίσετε να δουλεύετε με το PRIZM θα χρειαστεί να ξεκινήσετε τον κόμβο δικτύου (Node) και το API_Servlet.

Το λογισμικό μπορεί να λειτουργεί σε ένα διακομιστή καθώς και σε διαφορετικούς διακομιστές. Ωστόσο, είναι καλύτερο να το ξεκινήσετε σε έναν για την δική σας ευκολία σας.

Πρώτον, πρέπει να ξεκινήσετε τον κόμβο και να περιμένετε να συγχρονιστεί. Το επόμενο βήμα είναι η διαμόρφωση της μονάδας PrizmAPIServlet.

Ενσωμάτωση συστήματος πληρωμών Prizm

Κόμβος δικτύου

Το πορτοφόλι του κόμβου
https://github.com/prizmspace/PrizmCore#prizmcore-wallet-download-v1103-windows-osx-linux

Εύκολη πύλη API
https://github.com/prizmspace/PrizmCore#easy-api-gateway-prizmapiservlet

Διαμόρφωση PrizmAPIServlet

Μέσα στο συμπιεσμένο αρχείο υπάρχει ένα αρχείο που ονομάζεται

PrizmAPIServlet.properties

Αφού συμπληρώσετε τα πεδία, θα πρέπει να ξεκινήσετε το servlet από το

run-servlet.sh

στη γραμμή

passphrase: NONE

αντί για NONE θα πρέπει να γράψετε το ιδιωτικό κλειδί του πορτοφολιού που θα χρησιμοποιηθεί για το έργο σας.

στη γραμμή

sendkey: NONE

αντί για NONE θα πρέπει να γράψετε τον κωδικό πρόσβασης (θα χρησιμοποιηθεί από τη λειτουργία αποστολής νομισμάτων ως πρόσθετη προστασία από μη εξουσιοδοτημένες συναλλαγές).

Το παράδειγμα εφαρμογής στην PHP

Η περιγραφή της διαδικασίας για την παραλαβή και αποστολή νομισμάτων, με παραδείγματα έτοιμων λειτουργιών και περιγραφή των αρχών της λειτουργίας. Η βάση δεδομένων Mysql χρησιμοποιείται για την αποθήκευση της λίστας συναλλαγών, υπάρχει ένα απόθεμα του πίνακα αποθήκευσης παρακάτω, μαζί με παραδείγματα κώδικα για να συνεργαστεί με τον πίνακα (αν εφαρμόσετε το QueryBuilder, δεν θα είναι πρόβλημα).

Η βασική αρχή της εργασίας:

Υπάρχει ένα σενάριο στην εργασία Cron που υποβάλλει ένα αίτημα στο servlet κάθε 2-5 λεπτά, ώστε να μπορεί να λάβει νέες συναλλαγές στο πορτοφόλι του καταστήματος. Αφού λάβετε τη λίστα των συναλλαγών, θα πρέπει να τα αποθηκεύσετε στην τοπική βάση δεδομένων. Εάν δεν υπάρχουν εντολές στη βάση δεδομένων, θα πρέπει να εκτελέσετε την εντολή χωρίς καμία παράμετρο. Ωστόσο, εάν θέλετε να λάβετε νέες συναλλαγές, θα πρέπει να στείλετε τον αριθμό της τελευταίας συναλλαγής που έχετε ως παράμετρο.

Το παράδειγμα της λειτουργίας:

```
<?php
function historyPZM($last_id = 0)
{
 if ($last_id) {
  $url = 'http://localhost:8888/history?fromid=' . $last_id;
 } else {
  $url = 'http://localhost:8888/history';
 }
 $page = '';
 $result = get_web_page($url);
 if (($result['errno'] != 0) || ($result['http_code'] != 200)) {
  $error = $result['errmsg'];
 } else {
  $page = $result['content'];
 }
 $array_new = array();
 $xcmorewrite = explode("\n", str_replace("\r", '', $page));
 foreach ($xcmorewrite as $value) {
  if ($value) {
   $array_new[] = explode(";", $value);
  }
 }
 return $array_new;
}
?>
```

Η λειτουργία ανάκτησης περιεχομένου σελίδας:

```
<?php

function get_web_page($url)
{
 $uagent = "Opera/9.80 (Windows NT 6.1; WOW64) Presto/2.12.388 Version/12.14";
 $ch = curl_init($url);
          curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1); // recovers the web page
          curl_setopt($ch, CURLOPT_HEADER, 0); // doesn't recover headers
          curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1); // follows redirects
          curl_setopt($ch, CURLOPT_ENCODING, ""); // handles all encodings
         curl_setopt($ch, CURLOPT_USERAGENT, $uagent); // useragent
         curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, 20); // time-out of the connection
         curl_setopt($ch, CURLOPT_TIMEOUT, 20); // time-out of the answer
         curl_setopt($ch, CURLOPT_MAXREDIRS, 2); // stops after the 10th redirect

 $content = curl_exec($ch);
 $err = curl_errno($ch);
 $errmsg = curl_error($ch);
 $header = curl_getinfo($ch);
 curl_close($ch);

 $header['errno'] = $err;
 $header['errmsg'] = $errmsg;
 $header['content'] = $content;
 return $header;
}

?>
```

Η λειτουργία ανάκτησης περιεχομένου σελίδας:

You can test it through the console, for example:
curl http://localhost:8888/history

The example of the Cron-task handler script for receiving new transactions and the table structure

```
CREATE TABLE `pzm_history` (
  `id` bigint(20) NOT NULL,
  `tarif_id` int(1) NOT NULL,
  `tr_id` varchar(255) NOT NULL,
  `tr_date` varchar(255) NOT NULL,
  `tr_timestamp` int(11) NOT NULL,
  `pzm` varchar(50) NOT NULL,
  `summa` decimal(16,2) NOT NULL,
  `mess` varchar(255) NOT NULL,
  `status` int(1) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

** All necessary keys and autoincrement for ID should be added to the table

Διαχειριστής:

Σε αυτό το παράδειγμα λαμβάνετε τη λίστα των νέων συναλλαγών που θα πρέπει να αποθηκευτούν στην τοπική βάση δεδομένων.

Επομένως, διατηρείτε ιστορικό όλων των συναλλαγών στο πορτοφόλι και στο μέλλον θα τις αναζητήσετε στην τοπική βάση δεδομένων μας χρησιμοποιώντας τα βασικά δεδομένα.

```
<?php
$nomer = getLastPrmHistory();
$historys = historyPZM($nomer);

foreach ($historys as $item) {
    if ($item['0'] != "No transactions!") {

// this line adds data to the ‘pzm_history’ table using
INSERT IGNORE

PzmHistory::find()->insertIgnore([
            'tr_id' => $item['0'],
            'tr_date' => $item['1'],
            'tr_timestamp' => $item['2'],
            'pzm' => $item['3'],
            'summa' => $item['4'],
            'mess' => $item['5'],
            'status' => 0
        ]);
    }
}
```

```
function getLastPrmHistory()
{
//  this line searches for the last row in the table to get the last ID of the transactions which are in the table

if (!empty($pzmHistory = PzmHistory::find()->orderBy('id', "DESC")->first())) {
  return $pzmHistory->tr_id;
 };
 return 0;
}

?>
```

Το έργο σας πρέπει να λειτουργεί πάντα με το ίδιο Πορτοφόλι Prizm, γι 'αυτό και σε όλους τους πελάτες θα πρέπει να έχουν δοθεί οι ίδιες πληροφορίες ώστε να μπορείτε εσωτερικά στο λογαριασμό σας να αναζητήσετε τη Hash ID της συναλλαγής. Βεβαιωθείτε ότι ενημερώσατε τον πελάτη ότι πρέπει να πραγματοποιήσει μια συναλλαγή αυστηρά με τα απαραίτητα στοιχεία που υποδεικνύουν τη κρυπτογραφημένη ταυτότητα στο σχόλιο πληρωμής.

Γι’ αυτό, θα πρέπει να υπάρξει μια άλλη λειτουργία που θα αναλύει τις νέες εισερχόμενες συναλλαγές και θα καταθέτει τα νομίσματα στον εσωτερικό λογαριασμό εάν το σχόλιο πληρωμής έχει την κρυπτογραφημένη ταυτότητα της συναλλαγής του πελάτη. Επίσης, πρέπει να δημιουργήσετε ένα ξεχωριστό κουμπί "I PAID" για τον πελάτη, το οποίο θα μπορούσε να αναζητήσει και να καταγράψει νέες συναλλαγές για αυτόν τον χρήστη αφού κάνετε κλικ επάνω του.

Δευτερεύουσες λειτουργίες και λειτουργίες αποστολής νομισμάτων

Λήψη δημόσιου κλειδιού για το πορτοφόλι (λειτουργεί μόνο για ενεργά πορτοφόλια με διαθέσιμο υπόλοιπο).

```
<?php

 function destinationPZM($pzm)
   {
      $url = 'http://localhost:8888/publickey?destination=' . $pzm;
      $page = '';
      $result = get_web_page($url);
      if (($result['errno'] != 0) || ($result['http_code'] != 200)) {
         $error = $result['errmsg'];
         return '';
      } else {
         $page = $result['content'];
         $haystack = "Public key absent";
         $haystack2 = "Send error!";
         $pos = strripos($page, $haystack);
         $pos2 = strripos($page, $haystack2);
         if ($pos === false AND $pos2 === false) {
            $xcmorewrite = explode(' ', $page);
            $page = trim($xcmorewrite[0]);
            return $page;
         } else {
            return '';
         }
      }
      return $page;
   }

?>
```

Ενημέρωση για το τρέχων υπόλοιπο του πορτοφολιού:

```
<?php

 function getBalancePZM($pzm)
   {
       $ip = '*******';  // example 192.168.1.1:9976  with port
  $url = 'http://'.$ip.'/prizm?requestType=getAccount&account=' . $pzm;
       $page = '';
       $result = get_web_page($url);
  //print_r($result); die;
       if (($result['errno'] != 0) || ($result['http_code'] != 200)) {
          $error = $result['errmsg'];
          return '';
       } else {
          $page = $result['content'];
          $page = json_decode($page, true);
          if ( isset($page['balanceNQT']) ) {
            return $page['balanceNQT'] / 100;
          } else {
            return 0;
          }
       }
   }

?>
```

Η μέθοδος αποστολής νομισμάτων:

```
<?php

public function payPZM($summa, $pzm, $public_key, $text)
{
 $p2 = SENDKEY;   // this is the password that you specified during setup
 $return = false;
 $url = 'http://localhost:8888/send?sendkey=' . $p2 . '&amount=' . $summa .
'&comment=' . urlencode($text) . '&destination=' . $pzm . '&publickey=' . $public_key;
 $page = '';
 $result = get_web_page($url);

 if (($result['errno'] != 0) || ($result['http_code'] != 200)) {
  $error = $result['errmsg'];
 } else {
  $page = $result['content'];
 }

 if (preg_match('/^\+?\d+$/', $page)) {
  $return = true;
 } else {
  $return = false;
 }
 return $return;
}

?>
```

ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ

PRIZM

Η αρχική έννοια του ψηφιακού νομίσματος

Τεχνικές προδιαγραφές Prizm

Έκδοση Ιουνίου, 2020

PZM.SPACE