ΣΥΣΤΗΜΑ ΤΑΥΤΟΠΟΙΗΣΗ ΑΡΧΕΙΩΝ

με την χρήση της τεχνολογίας Ethereum Blockchain

Περίληψη

Το σύστημα επιτρέπει την επαλήθευση της ακεραιότητας, της αυθεντικότητας, της ύπαρξης και της κατοχής ενός οποιουδήποτε τύπου αρχείου μέσω των τεχνολογιών Ethereum Blockchain, IPFS και της κρυπτογράφησης SHA-256.

develodio

http://proof.develodio.com

Περιεχόμενα

Εισαγωγή

Τί είναι το blockchain;

Πρόκειται για ένα δημόσιο ψηφιακό λογιστικό βιβλίο που έχει σχεδιαστεί ούτως ώστε να είναι αδιαπέραστο από τους hacker. Παρόλο που χρησιμοποιείται κυρίως ως τρόπος παρακολούθησης και επαλήθευσης των νομισματικών συναλλαγών, μπορεί επίσης να εντοπίζει και να ελέγχει σχεδόν οποιοδήποτε είδος δεδομένων, καθιστώντας την μια απίστευτα ασφαλή πλατφόρμα που έχει τη δυνατότητα να αλλάξει ολόκληρο το διαδίκτυο.

Κάθε χρονολογική αλλαγή στο βιβλίο αναφέρεται ως block (μπλοκ), ενώ μια μεγαλύτερη σειρά αλλαγών ονομάζεται αλυσίδα, Blockchain.

Αυτό που κάνει το blockchain τόσο ασφαλές είναι ο distributed (διανεμημένο, χωρίς έδρα) χαρακτήρας του. Δεν υπάρχει σε κανένα διακομιστή, Master Ledger (κυρίαρχο λογιστικό βιβλίο), αντίθετα, υπάρχει στον υπολογιστή του καθενός ταυτόχρονα! Αυτό σημαίνει ότι κάθε φορά που ενημερώνεται με νέες πληροφορίες, κάθε υπολογιστής που χρησιμοποιεί την πλατφόρμα, πρέπει να συμφωνεί ότι η αλλαγή είναι έγκυρη.

Αυτό σημαίνει ότι αν κάποιος θέλησε να παραποιήσει τα αρχεία στην block chain, θα χρειαζόταν να «μπει» (hack) σε κάθε έναν από αυτούς τους υπολογιστές ταυτόχρονα, σε αντίθεση με μια ενιαία κεντρική (centralised) βάση δεδομένων.

Ο καθένας έχει πρόσβαση στο βιβλίο ανά πάσα στιγμή, αλλά χωρίς χαρακτηριστικά αναγνώρισης.

Το blockchain μπορεί να ελέγξει με ασφάλεια τις συναλλαγές μεταξύ δύο μερών ενώ μειώνει αποτελεσματικά την ανάγκη για μεσάζοντα.

Τι είναι το Ethereum Project

Το 2013, μια ομάδα προγραμματιστών ανακοίνωσε ότι εργάζονται πάνω σε ένα project που θα επιτρέπει την δημιουργία χρηματοοικονομικών εφαρμογών χωρίς την ανάγκη κάποιας τράπεζας ή μεσάζοντα.

Δύο χρόνια αργότερα εμφανίστηκε το Ethereum. Πρόκειται για ένα ψηφιακό νόμισμα αλλά και μια ανοικτού κώδικα πλατφόρμα blockchain με προγραμματιζόμενη λειτουργία συναλλαγών.

ethereum

Η τεχνολογία του blockchain είναι η κύρια διαφορά του Ethereum από το Bitcoin. Το blockchain του Ethereum δίνει την δυνατότητα να αναπτύξουμε διαφορετικές, ανεξάρτητες εφαρμογές που τρέχουν μέσω του δικτύου του.

Στο δίκτυο του Ethereum, οι εφαρμογές λέγονται smart contracts. Κατασκευάζονται κυρίως με την γλώσσα προγραμματισμού Solidity. Για κάθε εφαρμογή, ο δημιουργός θα πρέπει να καταβάλλει ένα αντίτιμο στο νόμισμα του δικτύου, το Ether.

Ουσιαστικά, το Ethereum είναι μια παγκόσμια υπολογιστική μηχανή. Αποτελείται από τους δεκάδες χιλιάδες υπολογιστές που συνδέονται στο δίκτυο για να σφραγίσουν συναλλαγές και οι

πόροι τους τρέχουν τις εφαρμογές που δημιουργούμε.

Τί είναι το IPFS;

Το IPFS είναι διανεμημένο σύστημα αρχείων peer-to-peer που επιδιώκει να συνδέσει όλες τις υπολογιστικές συσκευές με το ίδιο σύστημα αρχείων. Κατά κάποιο τρόπο, το IPFS είναι παρόμοιο με το World Wide Web, αλλά το IPFS, θα μπορούσε να θεωρηθεί ως ενιαίο σμήνος BitTorrent, ανταλλάσσοντας αντικείμενα μέσα σε αποθετήριο Git. Με άλλα λόγια το IPFS παρέχει υψηλής απόδοσης, διευθετημένο σε περιεχόμενο μοντέλο μπλοκ αποθήκευσης, με διευθετημένες σε περιεχόμενο υπερσυνδέσεις.

Τί είναι το Metamask;

Το Metamask είναι ένα plugin που συνδέει το Google Chrome ή το Firefox στο δίκτυο του Ethereum. Το Metamask είναι εύκολο στη χρήση, πάντα προσβάσιμο και αποθηκεύει τα πάντα μέσα στον υπολογιστή και όχι στο διαδίκτυο.

Κρυπτογράφηση SHA-256

Ο αλγόριθμος SHA-256 (Ασφαλής Αλγόριθμος Κατακερματισμού 256-bit) χρησιμοποιείται για κρυπτογραφική ασφάλεια.

Η συνάρτηση είναι μία από τις συναρτήσεις που ανήκουν στην κατηγορία SHA-2. Έχει σχεδιαστεί από την Υπηρεσία Εθνικής Ασφάλειας των ΗΠΑ (NSA) και δημοσιεύθηκε επίσημα το 2002 από τη NIST ως ένα FIPS.

Οι αλγόριθμοι κρυπτογραφικού κατακερματισμού παράγουν μη αναστρέψιμους και μοναδικούς κατακερματισμούς. Όσο μεγαλύτερος είναι ο αριθμός των πιθανών κατακερματισμών, τόσο μικρότερη είναι η πιθανότητα δημιουργίας του ίδιου κατακερματισμού από δύο τιμές.

Περιγραφή

Ταυτοποίηση Αρχείου

Καταχώρηση Αρχείου

Προσθήκη Κατόχου

Αφαίρεση Κατόχου