Bitcoin Basics

Τι είναι το bitcoin

Ψηφιακό νόμισμα (αποκεντρωμένο)

Είναι ένα crypto – currency (κρυπτό νόμισμα) έχουν εμφανιστεί από το 1980

Εικονικό όπως ο χρυσός ή το τυπωμένο χρήμα (χαρτονομίσματα και νομίσματα)

Μεταφέρεται από άτομο σε άτομο (peer to peer)

Δεν ελέγχεται από τράπεζες ή κυβερνήσεις

Δεν ανήκει σε κανέναν

Οι συναλλαγές ελέγχονται και εκτελούνται από τους κόμβους του δικτύου

Κάθε συναλλαγή καταχωρείται σε κάποιο block

Το block μοιράζεται σε όλους του κόμβους (block chain)

Όλα τα μπλοκ αποθηκεύονται σε ένα "λογιστικό βιβλίο" που είναι μοιρασμένο σε όλους του κόμβους

Δεν γίνονται επιστροφές (refunds ή chargebacks)

Συμβολίζεται με Β ή BTC.

Το bitcoin λύνει ένα πρόβλημα σε ένα δίκτυο που λέγεται «double spent»

Εμφανίστηκε το 2009 από τον Satoshi Nakamoto

Παράγεται σταδιακά μέχρι το 2140 και μέχρι 21 εκατομμύρια bitcoins

Κάθε 10 λεπτά παράγεται ένα Χ ποσό.

Διαιρείται σε μικρότερες αξίες μέχρι 0.00000001 (satoshi)

Πρακτικά αδύνατο να χακαριστεί (απαιτείται τεράστιος χρόνος και κόστος)

Μισό δις για μισή ώρα hacking (brutal force)

Ελέγχεται από τους συμμετέχοντες και κανέναν άλλο (για αυτό είναι και δημοφιλές)

FIAT νομίσματα είναι πληθωριστικά

Block chain

Είναι μια δημόσια βάση δεδομένων μοιρασμένη στους κόμβους του δικτύου.

Κάθε φορά που ένα μπλοκ ενημερώνεται, καταχωρείται στο "λογιστικό βιβλίο" (ledger) του κόμβου που ανέλαβε την εκτέλεση της συναλλαγής. Στη συνέχεια το δημοσιοποιεί στους υπόλοιπους κόμβους οι οποίοι ενημερώνουν το δικό του λογιστικό βιβλίο έτσι ώστε όλοι οι κόμβοι να μοιράζονται το ίδιο ακριβώς βιβλίο.

Κάθε συναλλαγή διακρίνεται ως input ή output.

Υποδιαιρέσεις

Το bitcoin υποδιαιρείται σε mBTC (10^{-3}), σε μBTC (10^{-6}) και σε satoshi (10^{-8}) ή 0.00000001 bitcoin.

Ιδιοκτησία

Κάθε ποσό ανήκει σε κάποιον λογαριασμό (όπως ο τραπεζικός λογαριασμός) που αντιστοιχεί στο δημόσιο κλειδί του κατόχου. Για να υλοποιηθεί για παράδειγμα μια πληρωμή θα πρέπει αυτός που πληρώνει να “κλειδώσει” την πληρωμή με το ιδιωτικό του κλειδί. Το σύστημα θα χρησιμοποιήσει το δημόσιο κλειδί του για να “ξεκλειδώσει” την πληρωμή. Αν χαθεί το ιδιωτικό κλειδί χάνονται και τα χρήματα.

Συναλλαγή

Οι συναλλαγές χωρίζονται σε inputs και outputs. Για κάθε output θα πρέπει να αφαιρεθούν κάποιο ή κάποια inputs από προηγούμενες συναλλαγές. Το ποσό είναι πάντα ένα πολλαπλάσιο του satoshi. Αν τα inputs ξεπερνούν το output κατά κάτι πρέπει να επιστραφούν τα “ρέστα”.

Σε κάθε συναλλαγή προστίθεται και η προμήθεια.

Εξόρυξη (mining)

Η αποστολή των “εξορύχων” είναι να προσφέρουν επεξεργαστική ισχύ για τη διεκπεραίωση των συναλλαγών την αρχειοθέτηση και την κρυπτογράφηση και πληρώνονται με νέα bitcoins ή από την προμήθεια της συναλλαγής.

Οι “εξορύχοι” πρέπει να αποδείξουν ότι για κάθε μπλοκ έχουν προσφέρει το έργο εκείνο (proof of work)για το οποίο πρέπει να πληρωθούν.

Κάθε 2016 blocks (περίπου 14 μέρες), η δυσκολία αλλάζει και γίνονται νέες ρυθμίσεις ανάλογα και με την απόδοση του δικτύου.

Τι είναι το χρήμα

Ένα μέσο για ανταλλαγή αγαθών.

Έχει 4 χαρακτηριστικά

1. Έχει υποδιαιρέσεις
2. Είναι ανθεκτικό
3. Έχει ίδια αξία
4. Είναι αναγνωρίσιμο

Γιατί έχει αξία

- Περιορισμένη ποσότητα
- Δεν ελέγχεται από τράπεζες ή κυβερνήσεις
- peer to peer
- Ανώνυμο
- Διάφανο (open source)
- Ελεγμένο και δοκιμασμένο για πάνω από 6 χρόνια (2009)
- Εύκολο στην αγοραπωλησία

- Χαμηλό κόστος συναλλαγής (προμήθεια)
- Πληρωμές χωρίς επιστροφές
- Δεν βασίζεται σε απτά αγαθά όπως πετρέλαιο, χρυσός κ.λπ. αλλά στην εμπιστοσύνη του κοινού
- Η αξία του εξαρτάται από την προσφορά και ζήτηση
- Προστασία από πληθωρισμό

Διαφορές από συμβατικό νόμισμα

- Δεν χρειάζεται τράπεζα ούτε τραπεζικός λογαριασμός
- Αποθηκεύεται σε ψηφιακό λογιστικό βιβλίο
- Αποστολή και λήψη είναι εύκολο όσο η αποστολή και λήψη ενός e-mail

Που αποθηκεύεται

Σε “πορτοφόλια”

https://bitcoin.org/el/choose-your-wallet

- Σκληρός δίσκος
  - απόλυτος έλεγχος
  - ανωνυμία
  - φυσική αποθήκευση στον δίσκο
  - χρειάζεται back up
  - κίνδυνος να κλαπεί ή χαθεί
  - wallet qt
- Κινητό
- Υλισμικό (κάρτα, usb type κ.λπ.)
- Τυπωμένο χαρτί (paper wallet)
- Φιλοξενία online
  - πρόσβαση από παντού
  - λειτουργούν ως ανταλλακτήρια
  - κίνδυνοι από χάκερ ή χρεωκοπία
  - https://blockchain.info/

Πως λειτουργεί ο λογαριασμός

Χρησιμοποιείται η ασύμμετρη κρυπτογραφία

1. Δημόσιο κλειδί (αλφαριθμητικό 27 – 34 χαρακτήρες)

2. Ιδιωτικό κλειδί (μένει κρυφό)

Πως αποκτώ bitcoins

1. Αγορά από φυσικό πρόσωπο ή ανταλλακτήριο
2. Πώληση από προϊόντα ή υπηρεσίες (barter)
3. Mining (με λογισμικό)

Πως μπορώ να κερδίσω

- Εξόρυξη (Mining) (όλο και πιο δύσκολο)
- Χρηματιστήριο (για έμπειρους)
- Προσφορά με εκπτώσεις και πληρωμή σε bitcoins

Θεωρίες

- Αύξηση αξίας κατά 10.000% μέσα σε λίγα χρόνια
- Πολλές πτώσεις (καταρρεύσεις) κατά 50% ή παραπάνω
- Διόρθωση μετά από πτώσεις
- Παραμένει η ερώτηση: Θα γίνει αποδεκτό (καθιερωθεί) από την αγορά σαν ένα “επίσημο” νόμισμα;

Κίνδυνοι

- Bug στο λογισμικό που θα έκανε την ασφάλεια διάτρητη
- Κυβερνητική ή πολιτική παρέμβαση που θα οδηγούσε στην κατάρρευση του νομίσματος
- Νέο κρυπτονόμισμα με λιγότερο κόστος ή περισσότερη ασφάλεια ή με κάτι πιο καινοτόμο