

Κρυπτονομίσματα

Κίνδυνοι και ασφάλεια



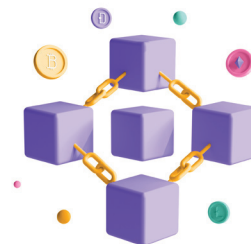
Με τη συγχρηματοδότηση
της Ευρωπαϊκής Ένωσης

Τι είναι τα κρυπτονομίσματα;

Τα κρυπτονομίσματα είναι ψηφιακά ή αλλιώς εικονικά χρήματα που χρησιμοποιούνται αποκλειστικά μέσω διαδικτύου. Δεν εκδίδονται από κράτη ή τράπεζες και δεν έχουν φυσική μορφή, καθώς υπάρχουν μόνο σε ψηφιακό περιβάλλον. Για τη λειτουργία και την προστασία τους χρησιμοποιούν ειδική τεχνολογία που βασίζεται σε μαθηματικούς κανόνες και μηχανισμούς ασφάλειας (cryptography). Γνωστά παραδείγματα κρυπτονομισμάτων είναι το Bitcoin και το Ethereum. Μπορούν να χρησιμοποιηθούν για ηλεκτρονικές συναλλαγές, για την αποστολή χρημάτων μέσω διαδικτύου, αλλά και για επενδύσεις, οι οποίες όμως συνοδεύονται από σημαντικό ρίσκο.

Τι είναι το blockchain;

Η λειτουργία των κρυπτονομισμάτων βασίζεται σε ένα τεχνολογικό δίκτυο που ονομάζεται blockchain. Πρόκειται για ένα είδος αλυσίδας από μπλοκ -μπορούμε να τα φανταστούμε σαν τουβλάκια- που περιλαμβάνουν τις συναλλαγές. Κάθε νέα επιβεβαιωμένη συναλλαγή προστίθεται στο τελευταίο μπλοκ. Αυτό το κρυπτογραφημένο σύστημα ελέγχει και εξασφαλίζει την ακεραιότητα των συναλλαγών. Η διαδικασία αυτή γίνεται χωρίς την εμπλοκή κάποιας κεντρικής αρχής, όπως για παράδειγμα μια τράπεζα ή κυβέρνηση. Και αυτό ακριβώς είναι που χαρακτηρίζει τα κρυπτονομίσματα ως «αποκεντρωμένα».



Πώς συνδέονται Blockchain & Cryptocurrency

Το blockchain αποτελεί το τεχνολογικό σύστημα, ενώ το cryptocurrency είναι το ψηφιακό νόμισμα που λειτουργεί πάνω σε αυτό. Χωρίς την ύπαρξη του blockchain, τα κρυπτονομίσματα δεν θα μπορούσαν να λειτουργήσουν. Η τεχνολογία αυτή προσφέρει αυξημένη ασφάλεια, μεγαλύτερη διαφάνεια και τη δυνατότητα πραγματοποίησης συναλλαγών χωρίς τη μεσολάβηση τραπεζών ή άλλων φορέων. Παρ' όλα αυτά, η ύπαρξη αυτών των χαρακτηριστικών δεν σημαίνει ότι απουσιάζουν οι κίνδυνοι.

Πώς λειτουργούν (γενικά):

1. **Συναλλαγή:** Ένας χρήστης στέλνει κρυπτονόμισμα σε κάποιον άλλο.
2. **Επικύρωση:** Εθελοντές στο δίκτυο (miners/validators) επαληθεύουν τη συναλλαγή λύνοντας σύνθετους αλγορίθμους.
3. **Blockchain:** Η επικυρωμένη συναλλαγή προστίθεται σε ένα νέο «μπλοκ» που συνδέεται με το προηγούμενο, δημιουργώντας την αλυσίδα.
4. **Νέα Νομίσματα:** Οι επικυρωτές ανταμείβονται με νέα κρυπτονομίσματα (εξόρυξη), σύμφωνα με τους κανόνες του δικτύου

Κίνδυνοι & ασφάλεια

Παρόλο που τα κρυπτονομίσματα βασίζονται σε τεχνολογία που θεωρείται ασφαλής, η χρήση τους κρύβει κινδύνους, ειδικά για άτομα χωρίς εμπειρία. Η αξία τους μπορεί να αλλιάξει πολύ γρήγορα, με αποτέλεσμα κάποιος να χάσει χρήματα μέσα σε πολύ μικρό χρονικό διάστημα.

Επιπλέον, στο διαδίκτυο κυκλοφορούν πολλές απάτες που υπόσχονται εύκολο ή σίγουρο κέρδος, κυρίως μέσω social media ή μηνυμάτων από αγνώστους. Είναι σημαντικό να γνωρίζουμε ότι οι συναλλαγές με κρυπτονομίσματα δεν προστατεύονται όπως οι τραπεζικές συναλλαγές. Αν γίνει κάποιο λάθος ή αν χαθούν τα στοιχεία πρόσβασης, τα χρήματα συνήθως δεν μπορούν να ανακτηθούν. Για τον λόγο αυτό, δεν πρέπει ποτέ να μοιραζόμαστε προσωπικά στοιχεία ή κωδικούς. Η καλύτερη προστασία είναι η ενημέρωση και η κριτική σκέψη. Όταν κάτι φαίνεται «πολύ καλό για να είναι αληθινό», συνήθως δεν είναι!



Πώς ενισχύουμε την ασφάλειά μας στον κόσμο των κρυπτονομισμάτων



Χρησιμοποιούμε αξιόπιστες πλατφόρμες

Αποφεύγουμε τυχαίους συνδέσμους και άγνωστες ιστοσελίδες που υπόσχονται «εύκολο κέρδος» ή πολύ υψηλές αποδόσεις.

Φροντίζουμε το ψηφιακό μας πορτοφόλι

Όπως δεν θα αφήναμε ποτέ αφύλακτο το πορτοφόλι μας σε έναν πολυσύχναστο χώρο, έτσι πρέπει να δείχνουμε την ίδια προσοχή και στο ψηφιακό μας πορτοφόλι. Κρατάμε τους κωδικούς μας μυστικούς και ενεργοποιούμε, όπου είναι δυνατό, [τον έλεγχο ταυτότητας δύο παραγόντων \(2FA\)](#).

Διατηρούμε το λογισμικό μας ενημερωμένο

Οι τακτικές αναβαθμίσεις από τις εταιρείες δεν γίνονται τυχαία. Στόχος τους είναι να διορθώνουν κενά ασφαλείας και να μας προσφέρουν μεγαλύτερη προστασία, διασφαλίζοντας τα οικονομικά και τα προσωπικά μας δεδομένα.

Αποφεύγουμε συναλλαγές με μεγάλα ποσά

Όπως ακριβώς θα ήμασταν πιο επιφυλακτικοί όταν έχουμε μαζί μας μεγάλα χρηματικά ποσά σε μετρητά, το ίδιο πρέπει να ισχύει και στις ψηφιακές συναλλαγές. Όσο μεγαλύτερο το ποσό, τόσο αυξάνεται και το ρίσκο.

Κρατάμε αντίγραφα ασφαλείας

Φροντίζουμε να δημιουργούμε ασφαλή αντίγραφα των ψηφιακών μας στοιχείων και συναλλαγών, προστατευμένα με κωδικό και αποθηκευμένα σε διαφορετικά σημεία.

Χρησιμοποιούμε ισχυρούς κωδικούς και τους αλλάζουμε συχνά

Βάζουμε κωδικούς σε όλες τις εφαρμογές και τις υπηρεσίες μας, αποφεύγοντας εύκολους ή προβλέψιμους συνδυασμούς. Δεν τους σημειώνουμε σε εμφανή σημεία και δεν τους μοιραζόμαστε ποτέ με άλλους. Η τακτική ανανέωσή τους είναι βασικό μέτρο ασφαλείας.

Μένουμε διαρκώς ενημερωμένοι

Ο ψηφιακός κόσμος αλλάζει συνεχώς και δεν μπορούμε ποτέ να είμαστε βέβαιοι για τις προθέσεις όσων βρίσκονται «απέναντί» μας. Γι' αυτό παραμένουμε σε εγρήγορση και υιοθετούμε άμεσα κάθε νέο μέτρο που ενισχύει την ηλεκτρονική μας προστασία.

Απάτες με κρυπτονομίσματα

Καθώς όλο και περισσότεροι άνθρωποι μπαίνουν στον κόσμο των κρυπτονομισμάτων, εμφανίζονται και επιτήδειοι που εκμεταλλεύονται την άγνοια, την απειρία ή την επιθυμία για γρήγορο κέρδος. Γι' αυτό είναι σημαντικό να γνωρίζουμε ποιες είναι οι πιο συνηθισμένες απάτες και πώς μπορούμε να τις αναγνωρίσουμε εγκαίρως.

- ➡ Ψεύτικες επενδυτικές ευκαιρίες που υπόσχονται γρήγορο ή σίγουρο κέρδος χωρίς ρίσκο.
- ➡ Απάτες μέσω social media, όπου άγνωστοι ή ψεύτικοι λογαριασμοί παριστάνουν ειδικούς ή επιτυχημένους επενδυτές.
- ➡ Ψεύτικες ιστοσελίδες ή εφαρμογές που μοιάζουν με κανονικές πλατφόρμες αλλά έχουν στόχο να κλέψουν χρήματα ή στοιχεία.
- ➡ Μηνύματα ή emails (phishing) που ζητούν κωδικούς, στοιχεία πρόσβασης ή προσωπικά δεδομένα.
- ➡ «Δώρα» ή giveaways σε crypto, όπου ζητείται πρώτα κάποια πληρωμή ή στοιχεία για να «ξεκλειδώσει» το κέρδος.
- ➡ Απάτες μέσα από online παιχνίδια ή chats, όπου η προσέγγιση γίνεται φιλικά και σταδιακά.

Σημαντικό να θυμόμαστε:

- ➡ Καμία σοβαρή επένδυση δεν υπόσχεται σίγουρο κέρδος.
- ➡ Αν ζητούν μυστικότητα ή γρήγορη απόφαση, είναι προειδοποιητικό σημάδι.
- ➡ Όταν χαθούν χρήματα σε crypto, συνήθως δεν υπάρχει τρόπος επιστροφής.



Τι μπορούμε να κάνουμε αν πέσουμε θύμα απάτης:

- ➡ Σταματάμε αμέσως κάθε επικοινωνία με το άτομο ή την πλατφόρμα που μας εξαπάτησε.
- ➡ Δεν στέλνουμε άλλα χρήματα ή στοιχεία, ακόμη κι αν μας υπόσχονται ότι θα τα πάρουμε πίσω.
- ➡ Κρατάμε αποδείξεις, όπως μηνύματα, emails, screenshots ή links που σχετίζονται με την απάτη.
- ➡ Αλλάζουμε τους κωδικούς μας, ειδικά αν έχουμε δώσει στοιχεία πρόσβασης.
- ➡ Αναζητάμε βοήθεια από αρμόδιους φορείς όπως [η Δ/ση Δίωξης Ηλεκτρονικού Εγκλήματος](#).
- ➡ Αναφέρουμε την απάτη στην Γραμμή καταγγελιών παράνομου περιεχομένου στο διαδίκτυο www.safeline.gr μέσω της σελίδας αναφοράς.



Πηγές

[Ευρωπαϊκή Κεντρική Τράπεζα](#)

[Investopedia](#)

[Cyberalert](#)

[Υπουργείο Ανάπτυξης](#)

[ESET](#)



SaferInternet4Kids.gr
ΓΙΑ ΕΝΑ ΑΣΦΑΛΕΣΤΕΡΟ ΔΙΑΔΙΚΤΥΟ



ITE

ΙΝΣΤΙΤΟΥΤΟ ΠΛΗΡΟΦΟΡΙΚΗΣ



Με τη συγχρηματοδότηση
της Ευρωπαϊκής Ένωσης

«Την αποκλειστική ευθύνη της παρούσας έκδοσης φέρει ο συγγραφέας της. Η Ευρωπαϊκή Ένωση δεν φέρει καμία ευθύνη για οποιαδήποτε χρήση των περιεχομένων σ' αυτήν πληροφοριών.»