ΕΝΟΤΗΤΑ 6
ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

6.2 Απειλές και μέτρα προστασίας

- Με τον όρο ***απειλή*** περιγράφουμε οποιοδήποτε γεγονός μπορεί να προκαλέσει μερική ή ολική καταστροφή των ***αγαθών***.
- ***Αγαθό*** (asset) ονομάζεται οτιδήποτε θέλουμε να προστατέψουμε.
- Το κάθε αγαθό έχει ***αξία*** (value) και αυτή η αξία των αγαθών μειώνεται αν αυτά πάθουν κάποια ***ζημιά*** (harm).
- Το αγαθό είναι ευάλωτο σε πιθανούς ***κινδύνους*** (dangers) και ***απειλές***.

6.2 Απειλές και μέτρα προστασίας

- Για να εξαλείψουμε αυτούς τους κινδύνους οι οποίοι είναι δυνατό να βλάψουν τα αγαθά μας, υιοθετούμε ***μέτρα προστασίας***.
- Η απειλή μπορεί να συμβεί με ***φυσικό*** ή με ***ηλεκτρονικό*** τρόπο.
- Κατ' αρχάς, τα data centers και όλοι οι προσωπικοί υπολογιστές γενικότερα, πρέπει να προστατεύονται από τη ***φυσική πρόσβαση*** μη εξουσιοδοτημένων χρηστών. Άρα, πρώτη και βασική παράμετρος ασφάλειας είναι ο έλεγχος της **φυσικής πρόσβασης** στα data centers.
- Επίσης, πρέπει να προστατεύονται και από ***φυσικούς* κινδύνους**, όπως φωτιά, πλημμύρες και σεισμούς. Αξίζει να σημειωθεί, πως το δίκτυο συνιστά κρίσιμη υποδομή και θα πρέπει να λειτουργεί δυνητικά σε όλες τις περιπτώσεις.

Σύγχρονος τρόπος ζωής και απειλές

Σήμερα αρκετοί χρησιμοποιούν:

- κοινωνικά δίκτυα
- ηλεκτρονικές πληρωμές
- διατραπεζικές συναλλαγές.
- Επιπρόσθετα, υπάρχουν στον κόσμο διάσπαρτοι ***κακοπροαίρετοι χρήστες-hackers***, οι οποίοι προσπαθούν με διάφορους τρόπους να αποκτήσουν πρόσβαση στον υπολογιστή μας, στα δεδομένα και στους κωδικούς μας. Ακριβώς το ίδιο επιχειρούν και σε μεγάλες εταιρείες, τράπεζες, οργανισμούς και φορείς του δημοσίου

6.3.1 Ασφάλεια σε επίπεδο υπολογιστή

Τι είναι η Ασφάλεια Υπολογιστή;

- Είναι τα μέτρα που παίρνουμε για να προστατεύσουμε τον υπολογιστή μας.
- Μας βοηθά να κρατάμε τα αρχεία μας ασφαλή.
- Μας προστατεύει από ιούς και επιθέσεις.

6.3.1 Ασφάλεια σε επίπεδο υπολογιστή

Ιοί Υπολογιστών

- Μικρά κακόβουλα προγράμματα.
- Μπαίνουν χωρίς άδεια.
- Μπορούν να καταστρέψουν αρχεία ή να κάνουν τον υπολογιστή αργό.

6.3.1 Ασφάλεια σε επίπεδο υπολογιστή

Αντιϊκό Λογισμικό (Antivirus)

- Εντοπίζει και διαγράφει ιούς.
- Ελέγχει αρχεία και προγράμματα.
- Κάνει αυτόματες ενημερώσεις.
- **Παραδείγματα:** Windows Defender, Avast, AVG.

6.3.1 Ασφάλεια σε επίπεδο υπολογιστή

Σκουλήκια (Worms)

- Είδος κακόβουλου λογισμικού που εξαπλώνεται μόνο του.
- Μπορεί να γεμίσει το δίκτυο και να το κάνει αργό.

6.3.1 Ασφάλεια σε επίπεδο υπολογιστή

Δούρειοι Ίπποι (Trojans)

- Φαίνονται ακίνδυνα προγράμματα, αλλά κρύβουν κάτι κακό.
- Ανοίγουν «πόρτες» για να μπει κάποιος στον υπολογιστή.

6.3.1 Ασφάλεια σε επίπεδο υπολογιστή

Ransomware

- Κακόβουλο Λογισμικό που κλειδώνει τα αρχεία του χρήστη.
- Ζητά «λύτρα» για να τα ξεκλειδώσει.
- Πολύ επικίνδυνο για σχολεία και οργανισμούς.

6.3.1 Ασφάλεια σε επίπεδο υπολογιστή

Firewall

- Ένα «τείχος προστασίας» που ελέγχει τι μπαίνει και τι βγαίνει από τον υπολογιστή.
- Σταματά ύποπτες συνδέσεις.
- Κάθε οικιακός υπολογιστής έχει ενσωματωμένο τείχος προστασίας στο λειτουργικό του σύστημα, ωστόσο αν ο χρήστης επιθυμεί μπορεί να εγκαταστήσει επιπλέον λογισμικό προστασίας στο σύστημά του

6.3.1 Ασφάλεια σε επίπεδο υπολογιστή

Phishing

- Ψεύτικα email ή μηνύματα που προσπαθούν να μας κλέψουν κωδικούς.
- Μοιάζουν με πραγματικές εταιρείες.
- Πολλές φορές έχουν ορθογραφικά λάθη ή περίεργους συνδέσμους.

6.3.1 Ασφάλεια σε επίπεδο υπολογιστή

Πώς Προστατευόμαστε;

- Κρατάμε τον υπολογιστή **ενημερωμένο**.
- Δεν ανοίγουμε **άγνωστα ή ύποπτα email**.
- Χρησιμοποιούμε **antivirus** (Αντιιϊκό Λογισμικό) και το αφήνουμε να ενημερώνεται αυτόματα.
- Επιλέγουμε **ισχυρούς κωδικούς**.
- Κάνουμε **backup** (Αντίγραφα Ασφαλείας) για να μην χάσουμε τα αρχεία μας.

ΠΡΟΣΟΧΗ!!

- ***Δε δίνουμε ποτέ και σε κανέναν τους κωδικούς μας!***
- Όταν θέλουμε να προβούμε σε διατραπεζική συναλλαγή, πληκτρολογούμε ολόκληρη την ηλεκτρονική διεύθυνση της τράπεζας μόνοι μας και δεν πατάμε ποτέ σύνδεσμο που μας έχουν στείλει. Βέβαια, οι πιο έμπειροι χρήστες είναι σε θέση να διακρίνουν την προέλευ ση του ηλεκτρονικού ταχυδρομείου και να καταλάβουν ότι πρόκειται για παραπλανητικό e-mail.

ΠΡΟΣΟΧΗ!!

Προστασία προσωπικών δεδομένων:

- ***Δε δίνουμε ποτέ τα προσωπικά μας στοιχεία*** (ονοματεπώνυμο, τηλέφωνο, διεύθυνση κα τοικίας, κωδικούς) στα Μέσα Κοινωνικής Δικτύωσης. Προσέχουμε την ανάρτηση φωτογραφιών. Επίσης, δεν κοινοποιούμε την πληροφορία ότι είμαστε διακοπές!

ΠΡΟΣΟΧΗ!!

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος

Στην Ελληνική Αστυνομία λειτουργεί η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος και εκεί μπορεί να απευθυνθεί οποιοσδήποτε θεωρεί ότι έχει υποστεί ζημία η ιδιωτικότητά του.

cyberalert.gr – CYBER ALERT. από τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος

Contact – cyberalert.gr

ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ

ΔΙΕΥΘΥΝΣΗ ΔΙΩΞΗΣ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ · ΠΡΟΛΗΨΗ · ΕΡΕΥΝΑ · ΚΑΤΑΣΤΟΛΗ ·

6.4 Κρυπτογραφία – Είδη κρυπτογράφησης

Τι είναι η Κρυπτογραφία;

- Είναι η επιστήμη που προστατεύει πληροφορίες.
- Μετατρέπει τα δεδομένα σε «κώδικα» που δεν μπορεί να διαβαστεί από τρίτους.
- Χρησιμοποιείται παντού: στο διαδίκτυο, στις τράπεζες, στα κινητά.

6.4 Κρυπτογραφία – Είδη κρυπτογράφησης

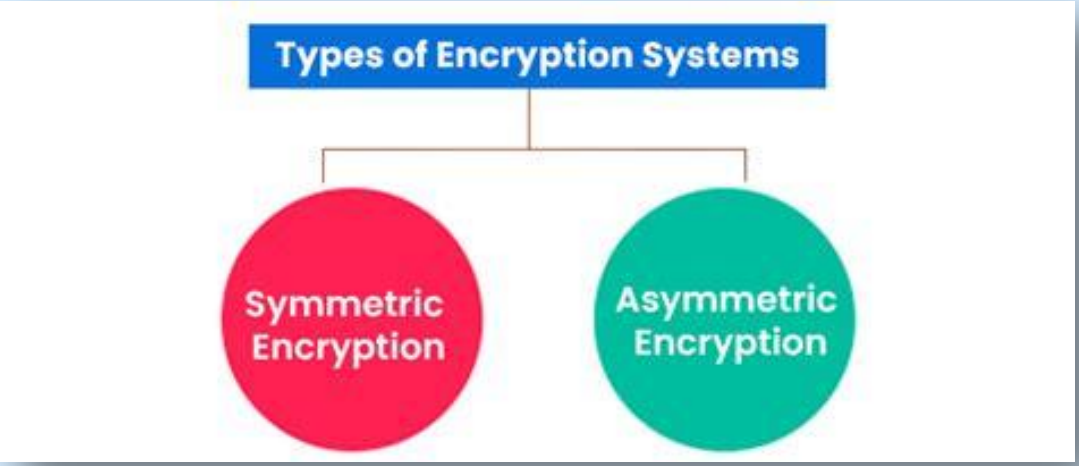
Γιατί Χρειαζόμαστε Κρυπτογραφία;

- Για να προστατεύουμε προσωπικά δεδομένα.
- Για να μην μπορούν άλλοι να διαβάσουν τα μηνύματά μας.
- Για ασφαλείς συναλλαγές στο διαδίκτυο.

6.4 Κρυπτογραφία – Είδη κρυπτογράφησης

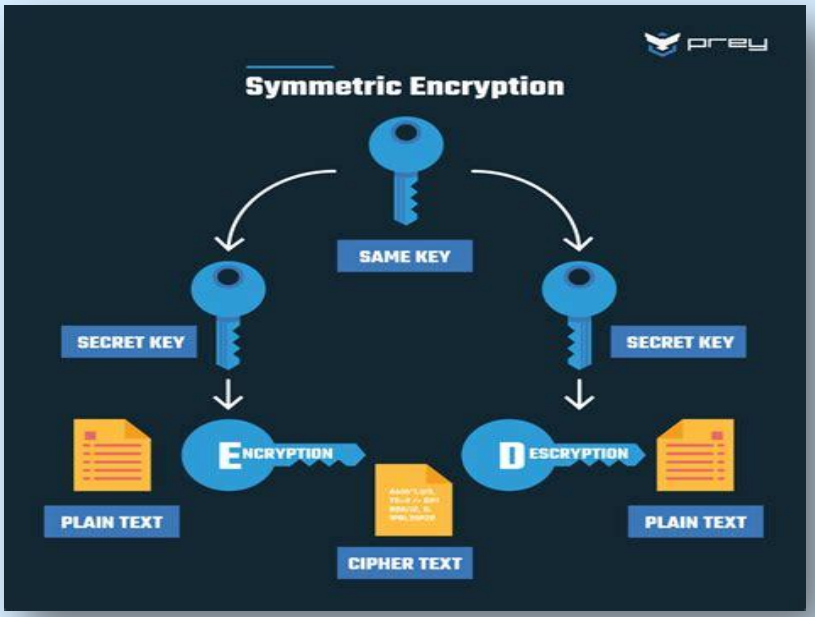
Είδη Κρυπτογράφησης

- Υπάρχουν δύο βασικές κατηγορίες:
- **Συμμετρική Κρυπτογράφηση**
- **Ασύμμετρη Κρυπτογράφηση**



6.4 Κρυπτογραφία – Είδη κρυπτογράφησης

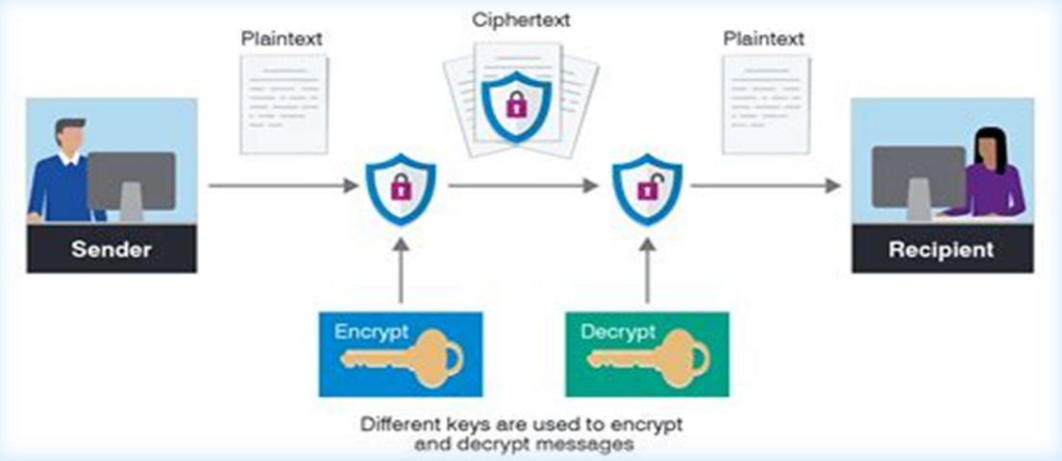
- **Συμμετρική Κρυπτογράφηση**
- Χρησιμοποιεί **ένα μόνο κλειδί** για κρυπτογράφηση και αποκρυπτογράφηση.
- Είναι **γρήγορη** και κατάλληλη για μεγάλα δεδομένα.
- Μειονέκτημα: πρέπει να βρούμε **ασφαλή τρόπο** να μοιραστούμε το κλειδί.
- **Παράδειγμα:** AES



6.4 Κρυπτογραφία – Είδη κρυπτογράφησης

Ασύμμετρη Κρυπτογράφηση

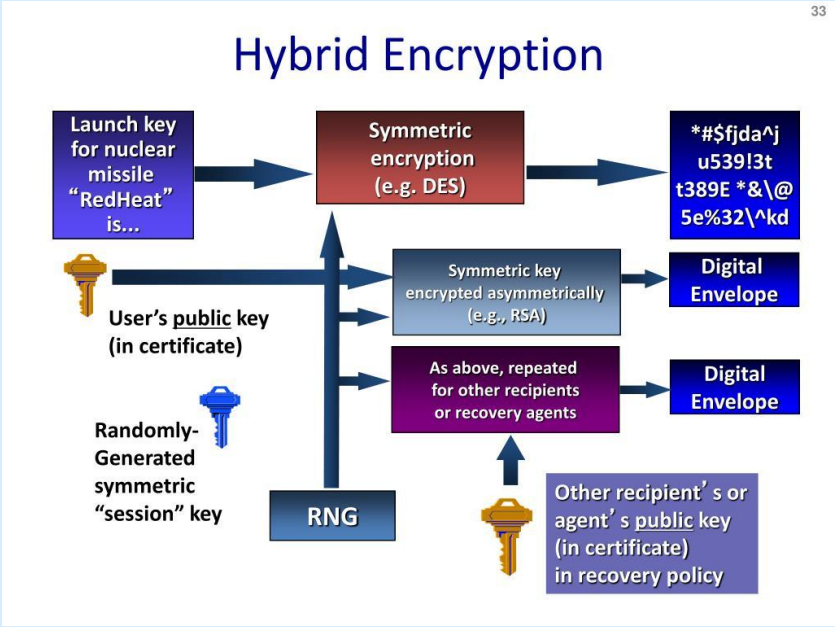
- Χρησιμοποιεί **δύο κλειδιά**:
  - **Δημόσιο κλειδί** (public key)
  - **Ιδιωτικό κλειδί** (private key)
- Το δημόσιο κλειδί το μοιραζόμαστε.
- Το ιδιωτικό κλειδί το κρατάμε μυστικό.
- **Παράδειγμα:** RSA



6.4 Κρυπτογραφία – Είδη κρυπτογράφησης

Πότε χρησιμοποιούμε κάθε είδος;

- **Συμμετρική:** όταν θέλουμε ταχύτητα.
- **Ασύμμετρη:** όταν θέλουμε ασφαλή ανταλλαγή κλειδιών ή ψηφιακές υπογραφές.
- Στην πράξη, τα συστήματα τα **συνδυάζουν (hybrid Encryption)**.



6.4 Κρυπτογραφία – Είδη κρυπτογράφησης

Ψηφιακά Πιστοποιητικά

- Είναι «ταυτότητες» για ιστοσελίδες και οργανισμούς.
- Βοηθούν να ξέρουμε ότι μια ιστοσελίδα είναι πραγματική.
- Τα βλέπουμε όταν μια σελίδα έχει **https**.

Παραδείγματα Αρχών Πιστοποίησης

- Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου: https://aped.gov.gr
- Η Υπηρεσία ψηφιακών πιστοποιητικών του Πανελλήνιου Σχολικού Δικτύου: https://ca.sch.gr/

6.4 Κρυπτογραφία – Είδη κρυπτογράφησης

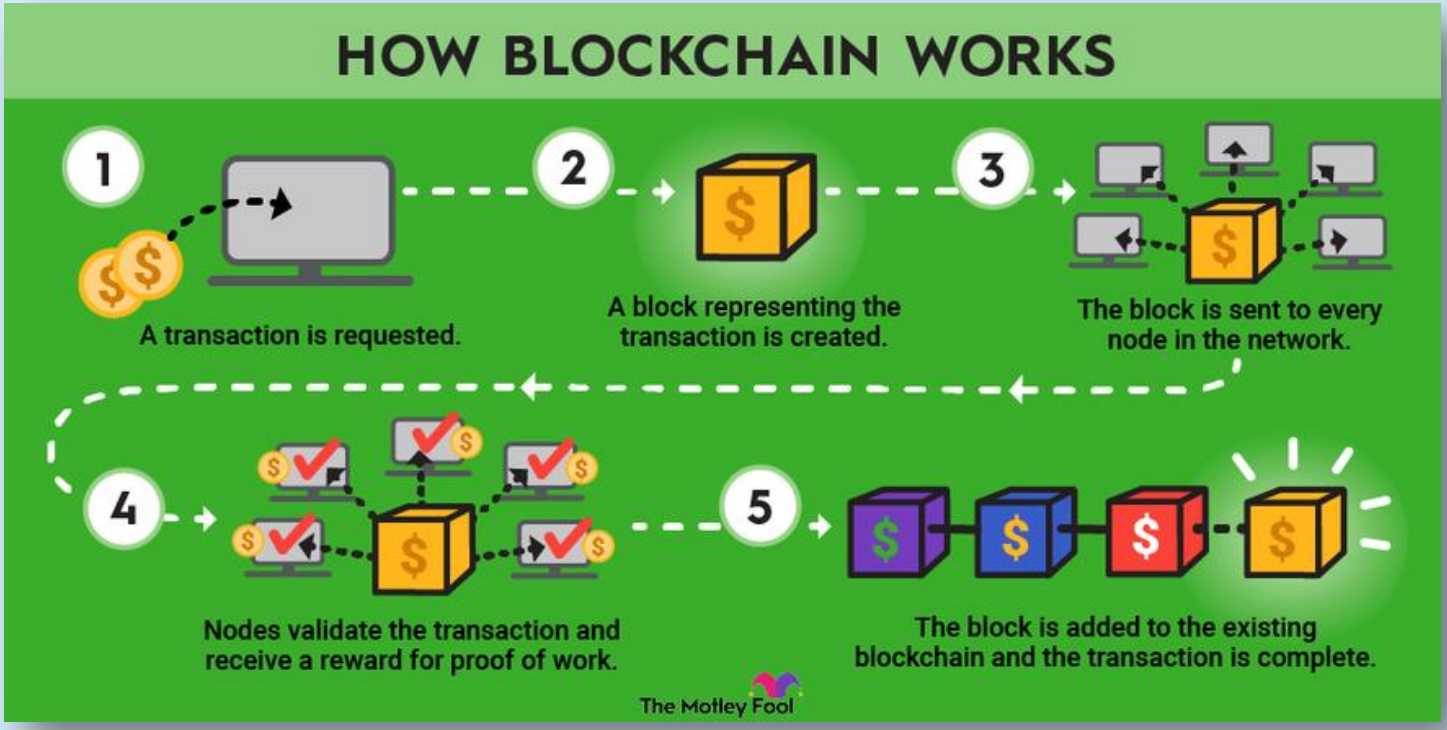
Τι είναι το Blockchain;

- Είναι μια **αλυσίδα από μπλοκ δεδομένων**.
- Κάθε μπλοκ περιέχει πληροφορίες και συνδέεται με το προηγούμενο.
- Δεν μπορεί να αλλαχθεί εύκολα → πολύ ασφαλές.
- Χρησιμοποιείται σε κρυπτονομίσματα, συμβόλαια, ψηφοφορίες.

6.4 Κρυπτογραφία – Είδη κρυπτογράφησης

Πώς λειτουργεί το Blockchain;

- Πολλοί υπολογιστές ελέγχουν και επιβεβαιώνουν τις συναλλαγές.
- Δεν υπάρχει ένας «αρχηγός» → αποκεντρωμένο σύστημα.
- Κάθε αλλαγή καταγράφεται δημόσια.



6.4 Κρυπτογραφία – Είδη κρυπτογράφησης

Τι είναι το Bitcoin;

- Είναι **ψηφιακό χρήμα**.
- Δεν υπάρχει σε χαρτί ή κέρματα.
- Δεν το ελέγχει καμία τράπεζα ή κράτος.
- Υπάρχει μόνο στο διαδίκτυο.
- Μπορείς να το στείλεις σε κάποιον όπως στέλνεις ένα email.

☐ Σκεφτείτε το σαν **ηλεκτρονικό νόμισμα** που λειτουργεί μόνο με υπολογιστές.

6.4 Κρυπτογραφία – Είδη κρυπτογράφησης

Πού "ζει" το Bitcoin;

- Το Bitcoin "ζει" μέσα σε ένα μεγάλο ψηφιακό βιβλίο που λέγεται **Blockchain**.
- Είναι σαν ένα **τετράδιο** όπου γράφονται όλες οι συναλλαγές.
- Το τετράδιο αυτό **δεν βρίσκεται σε ένα μέρος**, αλλά σε **χιλιάδες υπολογιστές** σε όλο τον κόσμο.
- Έτσι, δεν μπορεί κάποιος να το αλλάξει ή να το χακάρει ***εύκολα***.

6.4 Κρυπτογραφία – Είδη κρυπτογράφησης

Πώς αποκτά κάποιος Bitcoin;

Υπάρχουν **τρεις βασικοί τρόποι**:

1. Αγοράζοντας Bitcoin

- Από ειδικές πλατφόρμες (ανταλλακτήρια).
- Πληρώνεις με κανονικά χρήματα και παίρνεις Bitcoin.
- Είναι ο πιο συνηθισμένος τρόπος.

☐ Σαν να αγοράζεις ευρώ με δολάρια, αλλά ψηφιακά.

6.4 Κρυπτογραφία – Είδη κρυπτογράφησης

Πώς αποκτά κάποιος Bitcoin;

2. Κάνοντας "Mining" (Εξόρυξη)

- Αυτό είναι το πιο "τεχνολογικό" κομμάτι.
- Υπολογιστές λύνουν δύσκολους μαθηματικούς γρίφους.
- Όταν ένας υπολογιστής λύσει έναν γρίφο, "κερδίζει" Bitcoin ως ανταμοιβή.
- Χρειάζεται **πολύ ισχυρός υπολογιστής** και **πολλή ηλεκτρική ενέργεια**.

☐ Σκεφτείτε το σαν **ψηφιακό ορυχείο**: αντί για φτυάρια, χρησιμοποιούνται υπολογιστές.

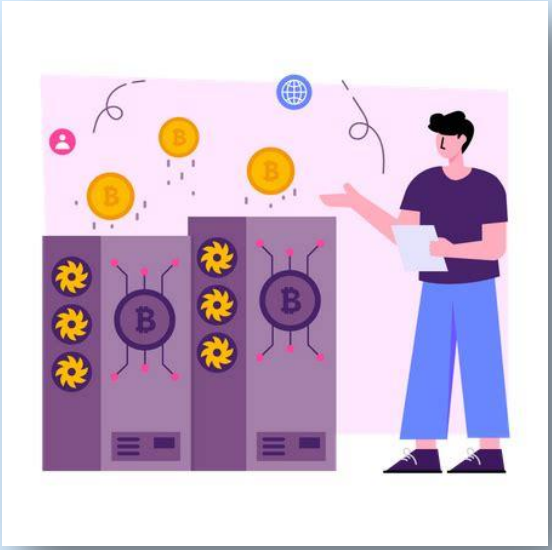
6.4 Κρυπτογραφία – Είδη κρυπτογράφησης

Πώς αποκτά κάποιος Bitcoin;

3. Κερδίζοντας Bitcoin

- Κάποιοι το δίνουν ως πληρωμή για δουλειά.
- Μπορείς να το λάβεις από κάποιον που σου το στέλνει.

☐ Σαν να σου δίνει κάποιος χρήματα, αλλά σε ψηφιακή μορφή.



6.4 Κρυπτογραφία – Είδη κρυπτογράφησης

Πού αποθηκεύεται το Bitcoin;

- Σε ένα **ψηφιακό πορτοφόλι** (wallet).

Υπάρχουν δύο είδη:

- **Hot Wallet**
  - Είναι εφαρμογή στο κινητό ή στον υπολογιστή.
  - Συνδέεται στο διαδίκτυο.
- **Cold Wallet**
  - Είναι σαν USB.
  - Δεν συνδέεται στο διαδίκτυο, άρα είναι πιο ασφαλές.
- Το πορτοφόλι έχει δύο “κλειδιά”:
  - **Δημόσιο κλειδί** → σαν διεύθυνση email (το δίνεις σε άλλους).
  - **Ιδιωτικό κλειδί** → σαν κωδικός πρόσβασης (ΔΕΝ το δίνεις ποτέ).

6.4 Κρυπτογραφία – Είδη κρυπτογράφησης

Είναι ασφαλές το Bitcoin;

- Το Blockchain είναι πολύ δύσκολο να χακαριστεί.
- Οι συναλλαγές είναι κρυπτογραφημένες.
- Δεν υπάρχει ένας “αδύναμος κρίκος” όπως μια τράπεζα.

Αλλά:

- Αν χάσεις το **ιδιωτικό κλειδί**, χάνεις τα Bitcoin σου για πάντα.
- Υπάρχουν πολλές **απάτες** (ψεύτικες ιστοσελίδες, phishing).