Τι έκανε το Bitcoin ξεχωριστό;

1. Ήταν το πρώτο κρυπτονόμισμα που πέτυχε την **πλήρη αποκέντρωση**.

2. Έλυσε το **πρόβλημα της διπλής δαπάνης**, το οποίο ήταν ένα από τα βασικά προβλήματα που αφορούσαν τα περισσότερα από τα προηγούμενα κρυπτονομίσματα.

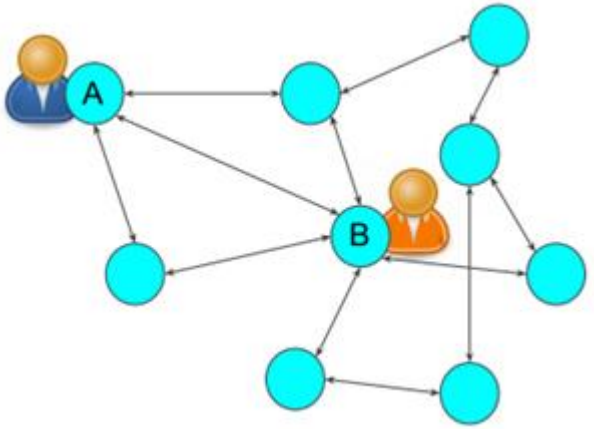
3. Είχε **ελεγχόμενο πληθωρισμό**.

4. Ήρθε σε μία περίοδο **παγκόσμιας οικονομικής κρίσης**, με πολύ έντονο το φαινόμενο της αμφισβήτησης των επίσημων νομισμάτων, καθώς και αυτών που τα έλεγχαν.

1. Πλήρης αποκέντρωση

Centralized

Decentralized



- Το νόμισμα δημιουργείται και ελέγχεται από την τράπεζα
- Η μεταφορά αξίας γίνεται μέσω κάποιου χρηματοπιστωτικού ιδρύματος
- Υψηλά τέλη (συναλλαγών, δημιουργίας λογαριασμού, προστασίας κτλ.)

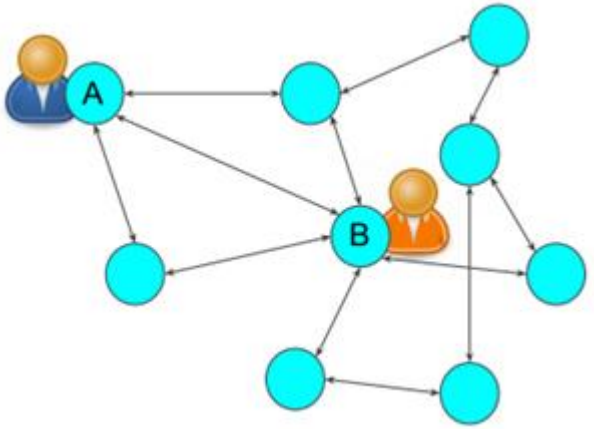
- Το νόμισμα δημιουργείται αλγοριθμικά από τους κόμβους του δικτύου
- Η μεταφορά αξίας γίνεται άμεσα μεταξύ των κόμβων, χωρίς ενδιάμεσο
- Πολύ χαμηλά τέλη (συναλλαγών) και είναι προαιρετικά

1. Πλήρης αποκέντρωση

Centralized

- Ψηφιακή μορφή ✔
- Περιορισμός ορισμένων ενεργειών λόγω ωραρίου λειτουργίας:
  - 09:00-17:00, Δευτέρα-Παρασκευή
- Τέλη συναλλαγών μεταξύ διαφορετικών χρηματοπιστωτικών ιδρυμάτων

Decentralized



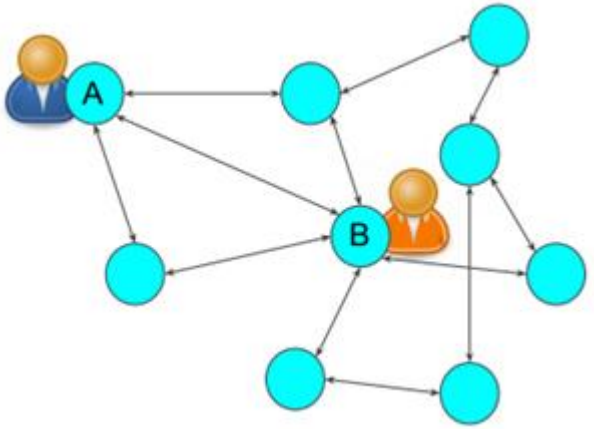
- Ψηφιακή μορφή ✔
- 24/7, μοναδικό προαπαιτούμενο η σύνδεση στο Internet
- Παγκόσμιο, δεν υπάρχουν τέλη για διασυνοριακές συναλλαγές

1. Πλήρης αποκέντρωση

Centralized

•Υψηλή ασφάλεια ✔
•Βασίζεται στις υποδομές ασφαλείας της τράπεζας
•Επιβάλλεται από την τράπεζα, το κράτος και την αστυνομία

Decentralized



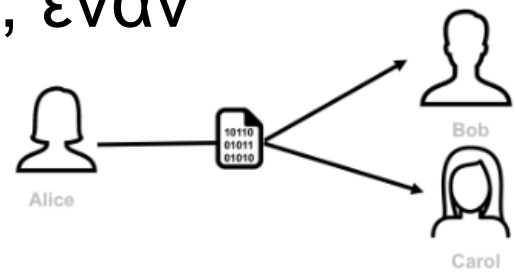
•Υψηλή ασφάλεια ✔
•Βασίζεται στο ίδιο το δίκτυο και τον σχεδιασμό του
•Λειτουργεί με εξειδικευμένους αλγορίθμους και κρυπτογραφία και επιβάλλεται από την κοινότητα του δικτύου

2. Πρόβλημα διπλής δαπάνης (double spending)

Μέχρι την εμφάνιση του Bitcoin, το πρόβλημα της διπλής δαπάνης ήταν η “αχίλλειος πτέρνα” των προγενέστερων ψηφιακών νομισμάτων.

Ήταν αδύνατο σε ένα ψηφιακό σύστημα -χωρίς τη χρήση μεσάζοντα- να αποδειχθεί ότι κάποιο άτομο δεν ξόδεψε το ίδιο ψηφιακό χρήμα πάνω από μία φορά.

Παρά τις τεχνολογικές εξελίξεις, όλες οι συναλλαγές μέσω Διαδικτύου απαιτούσαν ακόμη έναν αξιόπιστο τρίτο, όπως μία τράπεζα, έναν κυβερνητικό οργανισμό ή μία εταιρία παροχής υπηρεσιών ασφαλείας ηλεκτρονικών πληρωμών.

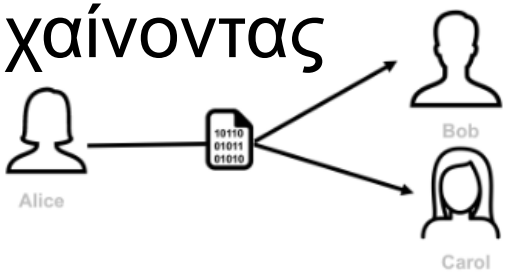


2. Πρόβλημα διπλής δαπάνης (double spending)

Το White Paper του Satoshi Nakamoto είχε τον εξής τίτλο: “**Bitcoin: A peer-to-peer electronic cash system**”. Είναι εμφανής η ιδιαίτερη βαρύτητα που δόθηκε και δίνεται ακόμη στο τμήμα “**peer-to-peer**” που ουσιαστικά εννοεί τις συναλλαγές μεταξύ ισότιμων συμβαλλόμενων.

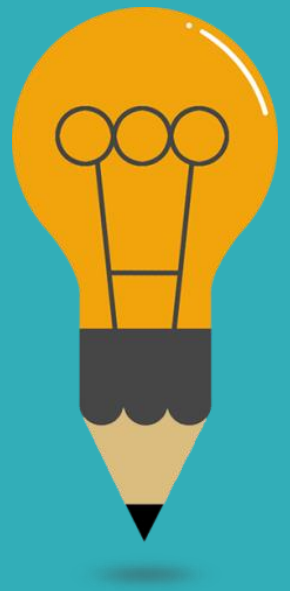
Η ιδέα του Nakamoto ξεπέρασε με ιδιοφυή τρόπο το εμπόδιο του double spending, χωρίς μάλιστα να παρεμβαίνει κάποια Κεντρική Αρχή.

Πώς; Καθιστώντας τη **συναλλαγή ορατή προς όλους**, πετυχαίνοντας έτσι τη μέγιστη δυνατή διαφάνεια!




BLOCKCHAIN

Τι είναι το Blockchain;



Το Blockchain είναι μία κατανεμημένη βάση δεδομένων που χρησιμοποιείται για τη διατήρηση ενός συνεχώς αυξανόμενου καταλόγου εγγραφών, που ονομάζονται **blocks**.

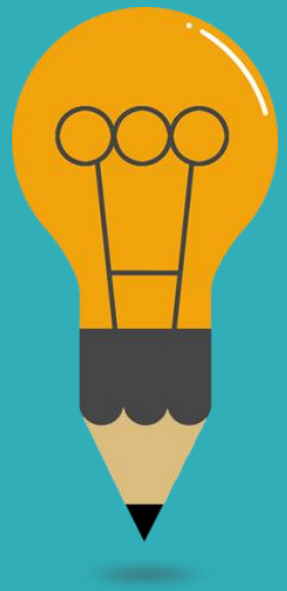
Αποτελεί μία τεχνολογία, η οποία παρουσιάζεται ως **μία δημόσια, μη δυνατόν να τροποποιηθεί το ιστορικό της, κατανεμημένη σειρά δεδομένων, ομαδοποιημένων σε χρονικά αριθμημένα «τμήματα» ή «συστοιχίες» (*blocks*)**.

*Η συνολική δαπάνη για λύσεις Blockchain ανέρχεται σε **12 δις δολάρια** (2022).*
*Επίσης, η παγκόσμια δαπάνη για AI ανέρχεται σε **58 δις δολάρια** και οι μισές επιχειρήσεις θα κάνουν τη μετάβαση στο AI με ενσωμάτωση του Blockchain.*

Τι είναι το Blockchain;

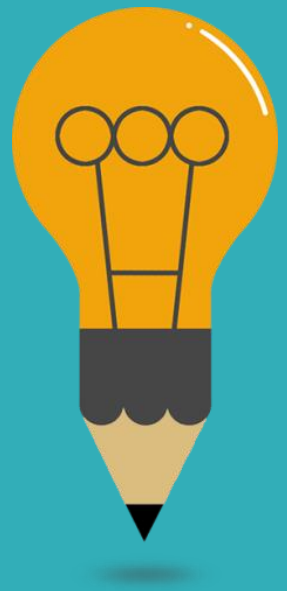
Η τεχνολογία Blockchain προκύπτει από ένα δίκτυο ανθρώπων που δημιουργούν και μοιράζονται κάτι κοινό. Το δίκτυο είναι **αποκεντρωμένο και κατανεμημένο ισόποσα,** ενώ όλα τα πρόσωπα του δικτύου δημιουργούν και μοιράζονται από κοινού ένα αρχείο το οποίο συνεχώς ενημερώνεται.

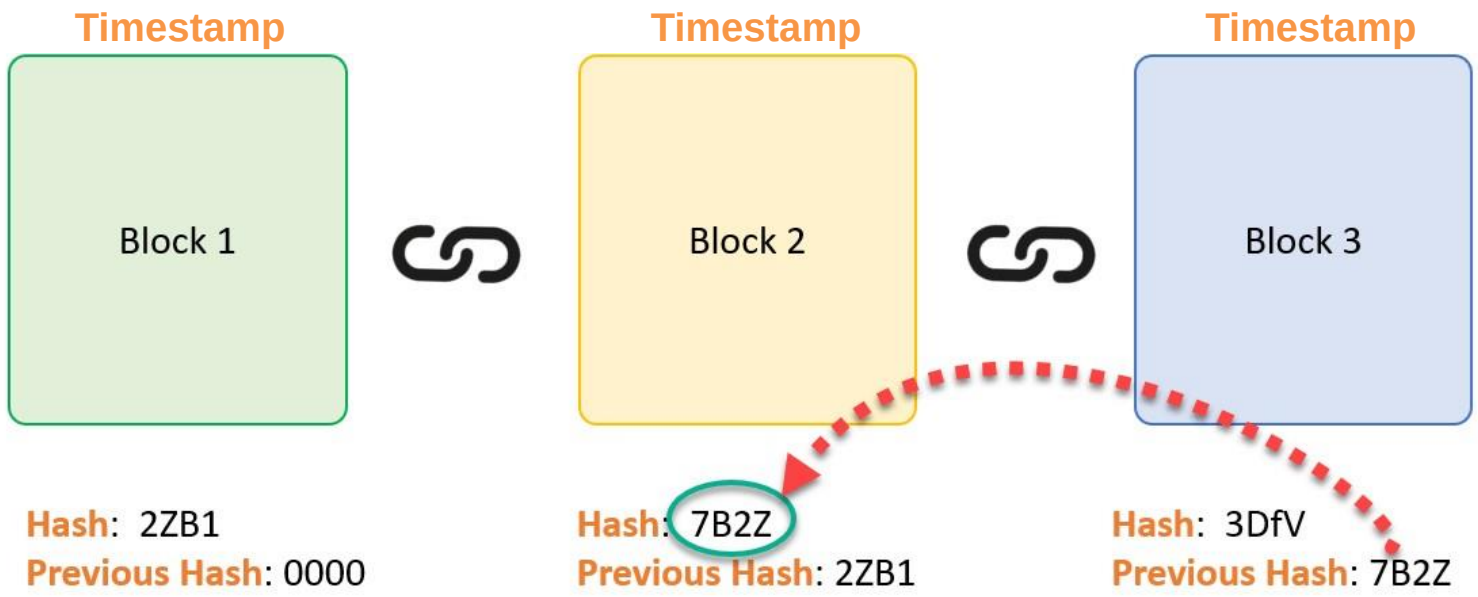
Λειτουργικά, ένα Blockchain μπορεί να χρησιμεύσει ως ένα ανοικτό, κατανεμημένο **ledger** (ημερολόγιο – λίστα ταξινόμησης) που μπορεί να καταγράφει τις συναλλαγές μεταξύ δύο μερών αποτελεσματικά, με **επαληθεύσιμο και μόνιμο τρόπο.**



Τι είναι το Blockchain;

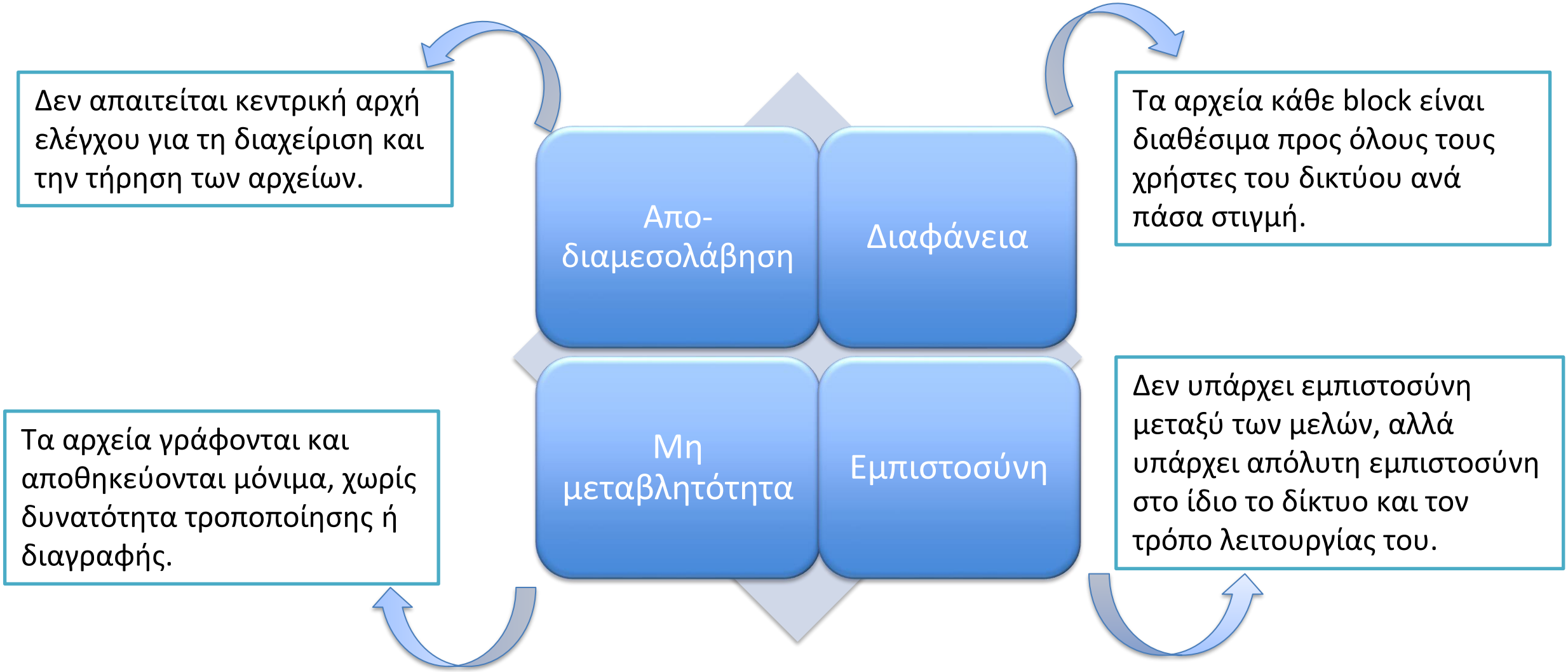
Κάθε block περιέχει ένα σύνολο δεδομένων και αναγνωρίζεται από ένα **hash**, μία **σφραγίδα χρόνου** και μία **σύνδεση με ένα προηγούμενο block**.





Hash: πρόκειται για μία μοναδική ακολουθία που δημιουργείται από μία συνάρτηση κατακερματισμού

Πλεονεκτήματα Blockchain



Μειονεκτήματα Blockchain

Εξαιτίας αυτού, ένας αυξανόμενος αριθμός υπολογιστών δεν έχει πλέον τον χώρο που απαιτείται για την αποθήκευση της πλήρους αλυσίδας με ό,τι αυτό συνεπάγεται.

Η επιβεβαίωση και η καταγραφή νέων δεδομένων στην αλυσίδα των μπλοκ μπορεί να διαρκέσει έως και κάποια λεπτά.

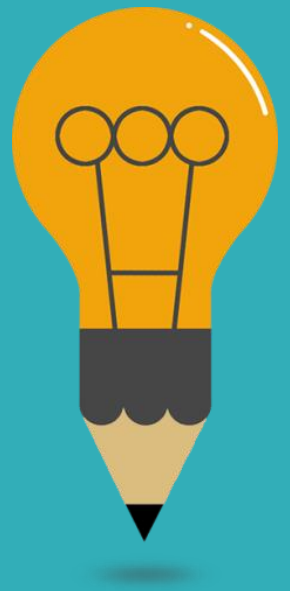
Η λειτουργία και η διατήρηση του blockchain απαιτεί μεγάλα ποσά ενέργειας. Αυτό συνεπάγεται σοβαρή επιβάρυνση του περιβάλλοντος.

Η αποκλειστικά ψηφιακή μορφή του και το νέο της ηλικίας του το καθιστούν στόχο για πιθανές επιθέσεις από χάκερς.

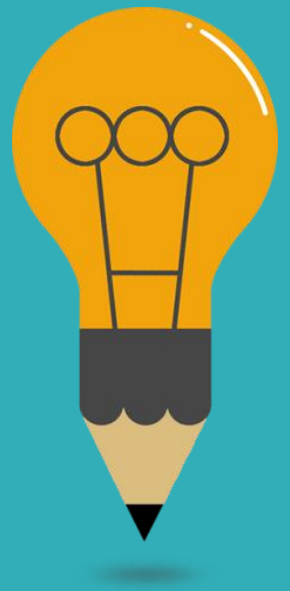
Bitcoin & Blockchain

Στην περίπτωση του Bitcoin, το Blockchain λειτουργεί ως το **δημόσιο λογιστικό βιβλίο**, μέσα στο οποίο είναι καταγεγραμμένες όλες οι **επιβεβαιωμένες συναλλαγές** μεταξύ των κόμβων του δικτύου.

Είναι ένα απαράλλακτο αρχείο που επιβεβαιώνεται από ένα ευρύ δίκτυο χρηστών και είναι το μέσο εκείνο που χρησιμοποιείται ως **απόδειξη για μία συναλλαγή**. Δεν χρειάζεται κάποια τρίτη αρχή ή κάποιος διαμεσολαβητής – και άρα ούτε το αίσθημα εμπιστοσύνης προς αυτούς – αλλά η **μαθηματική και οικουμενική απόδειξη ότι μία συναλλαγή έλαβε χώρα και ολοκληρώθηκε με επιτυχία**.



Bitcoin & Blockchain



Κάθε μπλοκ περιέχει ένα σύνολο επιβεβαιωμένων συναλλαγών σε μία συγκεκριμένη χρονική στιγμή, οι οποίες είναι διαθέσιμες προς όλους για ανάγνωση, αλλά αμετάβλητες.

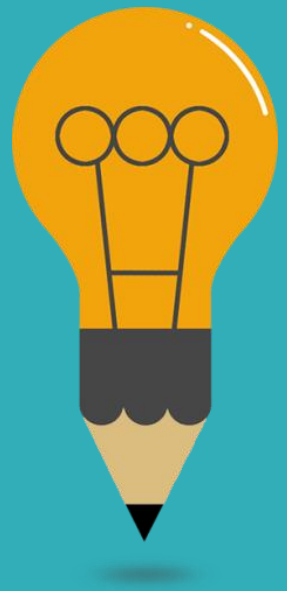
Μόλις συμπληρωθεί ένας αριθμός επιτυχημένων και επιβεβαιωμένων συναλλαγών, το block ολοκληρώνεται και αποτελεί έναν νέο κρίκο της λογιστικής αυτής αλυσίδας.

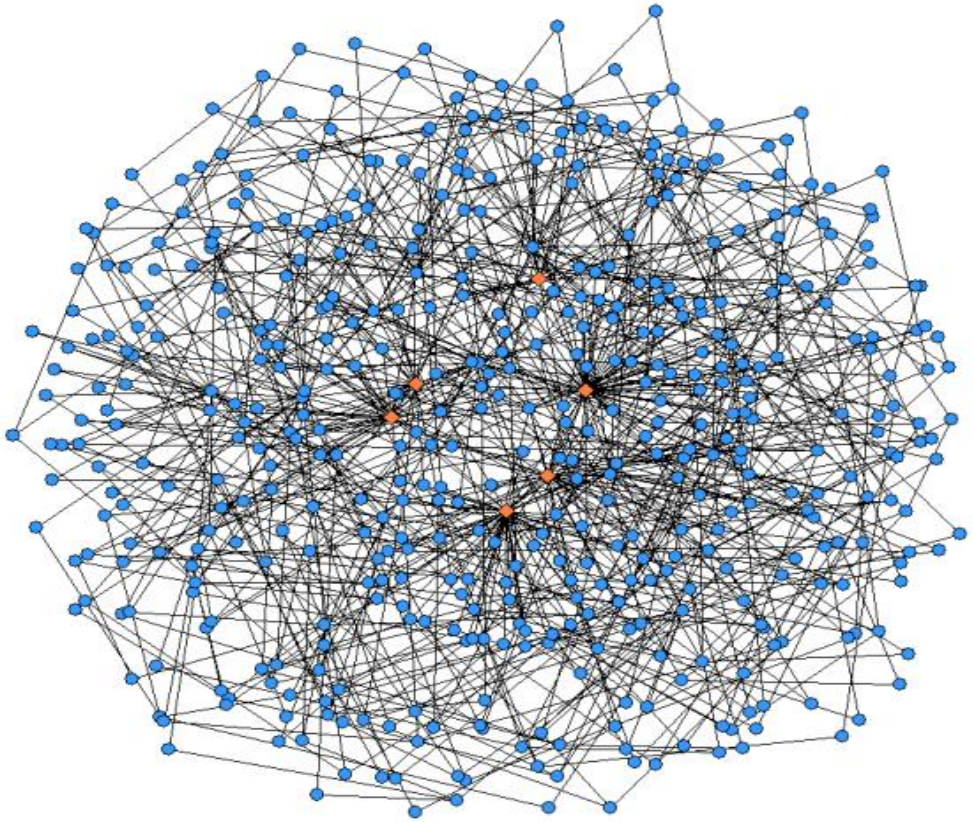
Η πρώτη συναλλαγή πραγματοποιήθηκε το 2009 από τον Nakamoto και καταγράφηκε στο πρώτο block του Blockchain, γνωστό και ως **genesis block** ή **block 0**.

Πώς λειτουργεί;

Δίκτυο:

- Όλοι οι κόμβοι του Bitcoin συνδέονται σε ένα κοινό p2p δίκτυο.
- Κάθε κόμβος τρέχει τον κώδικα του Bitcoin.
- Καθένας μπορεί ελεύθερα να συνδεθεί στο δίκτυο και να συμμετέχει.

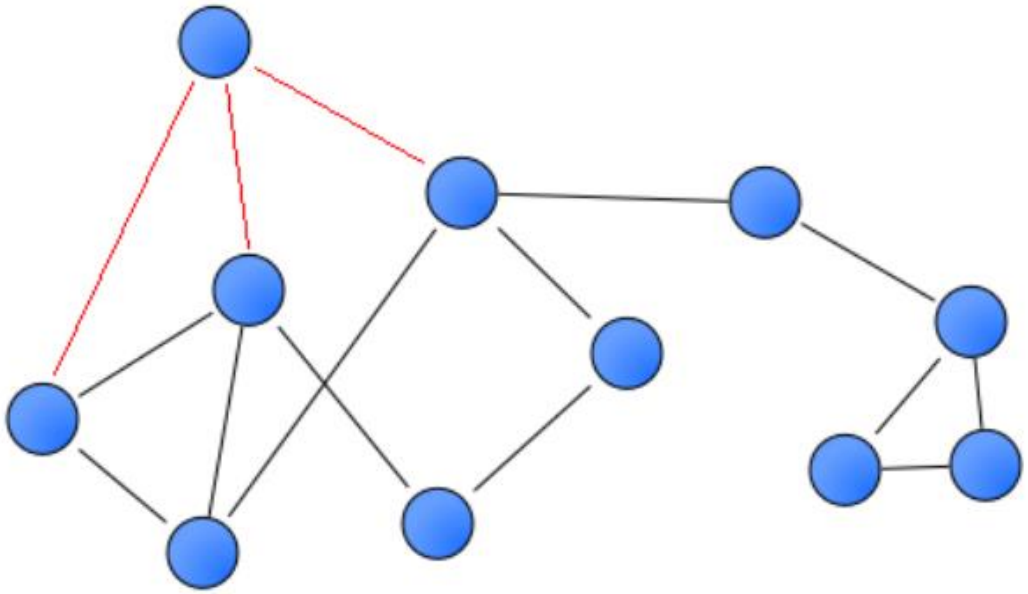


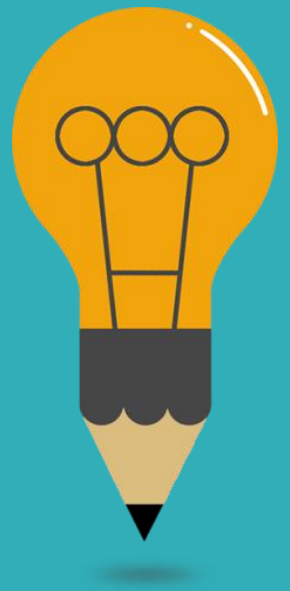


Πώς λειτουργεί;

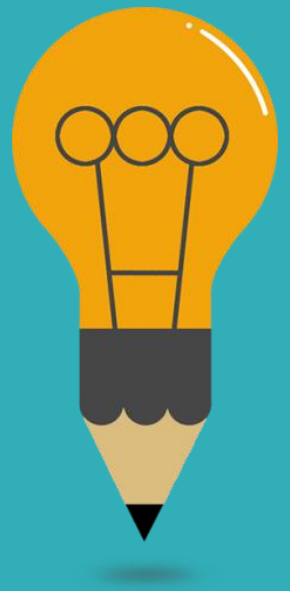
Δίκτυο:

- Κάθε ένας από τους κόμβους συνδέεται με τους γειτονικούς του.
- Ανταλλάσσουν συνέχεια οικονομικά δεδομένα.





Πώς οι κόμβοι συνδέονται μεταξύ τους;



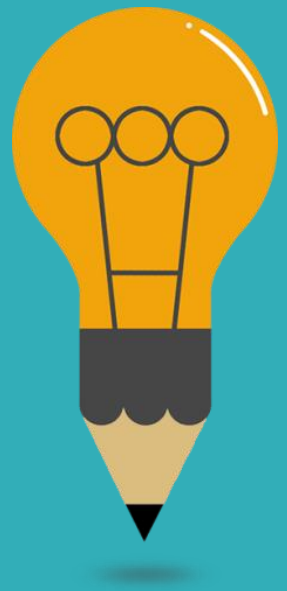
Κλειδιά:

Κάθε χρήστης Bitcoin παράγει ένα ιδιωτικό και ένα δημόσιο κλειδί.
Το δημόσιο κλειδί κωδικοποιείται σε μία διεύθυνση.
Παράδειγμα:

- Ιδιωτικό κλειδί:
  L4R3iSGxtzsYdmK1uP3GdBMiu68P7Wzx1yz29AKECuinFX
- Δημόσιο κλειδί:
  020c49ee87523337408b22b4542e808807a7763cd9eb0438
- Διεύθυνση:
  1EPVoneoy2ZbSfpLagqwZwrgfLAqSU8vZa

Κλειδιά:

Δημόσιο Κλειδί



• Με το δημόσιο κλειδί ο χρήστης λαμβάνει χρήματα. Είναι το μόνο γνώρισμα που τον ξεχωρίζει από τους υπόλοιπους χρήστες στο δίκτυο, χωρίς φυσικά να έχει την παραμικρή συσχέτιση με τα προσωπικά του στοιχεία.

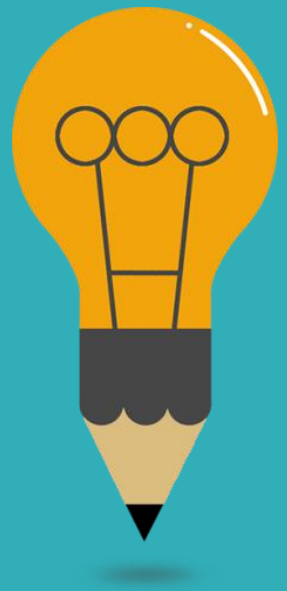
•Το μόνο που χρειάζεται κάποιος για να αποστείλει Bitcoins είναι το δημόσιο κλειδί του παραλήπτη ή αλλιώς η διεύθυνσή του.

• Κάθε χρήστης μπορεί να έχει πολλές διευθύνσεις και πολλά δημόσια κλειδιά, αλλά και να τα δημοσιεύει χωρίς κίνδυνο!

Η χρήση τους μοιάζει πολύ με αυτή των IBAN

Κλειδιά:

Ιδιωτικό Κλειδί

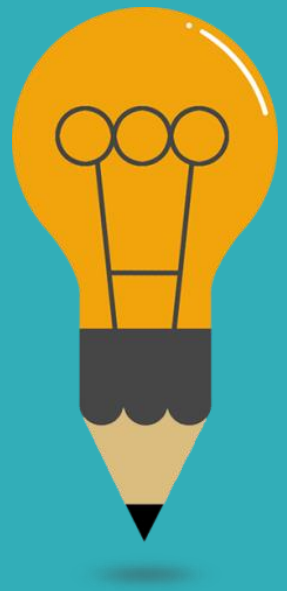


• Με το ιδιωτικό κλειδί ο χρήστης ξοδεύει χρήματα. Με το κλειδί αυτό αποδεικνύει ότι είναι ο πραγματικός κάτοχος αυτών των χρημάτων. Λειτουργεί σαν **μοναδική απόδειξη κατοχής.**

•Είναι ατομικό, μοναδικό και πρέπει να διατηρείται απόλυτα μυστικό απ' όλους!

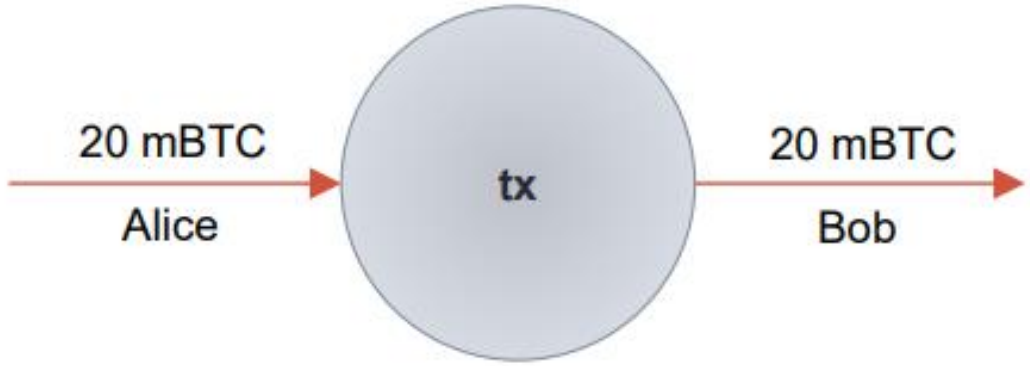
•Σε περίπτωση που κλαπεί, τότε ο χρήστης χάνει κάθε έλεγχο των χρημάτων του και δεν υπάρχει τρόπος ανάκτησής τους αλλά ούτε και του κλειδιού.

Κλειδιά:

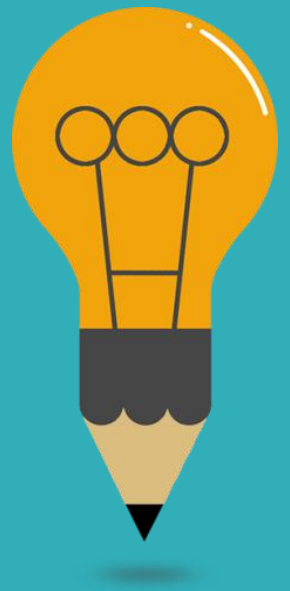


Παράδειγμα αποστολής χρημάτων

Η Alice θέλει να στείλει 20 mBTC στον Bob.

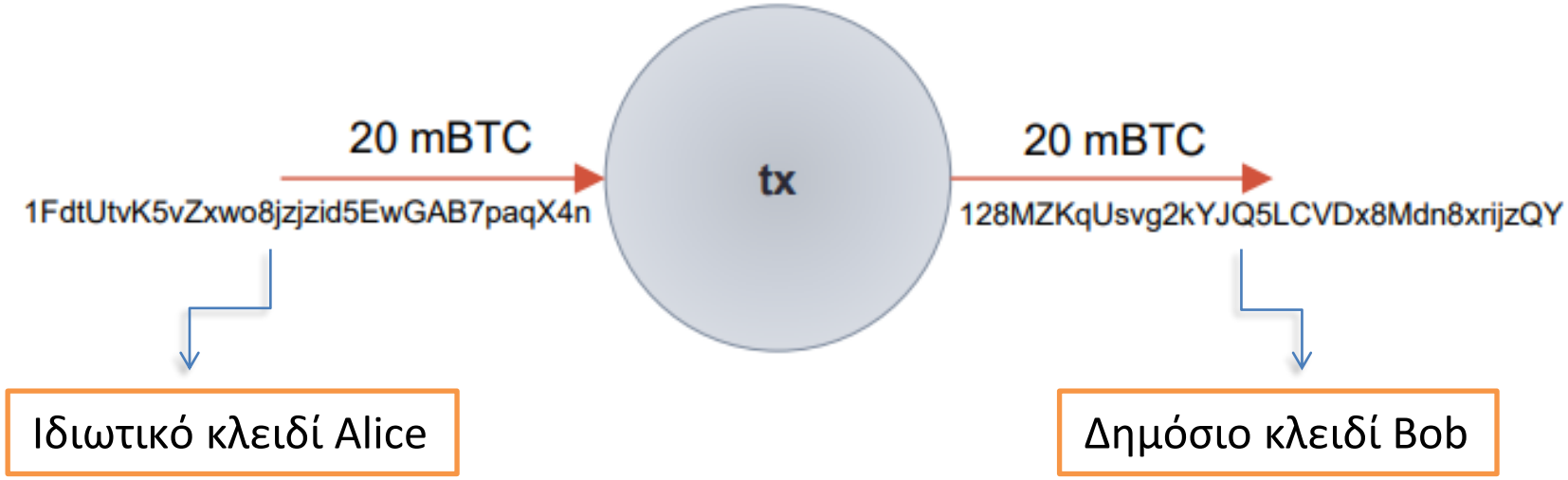


Κλειδιά:



Παράδειγμα αποστολής χρημάτων

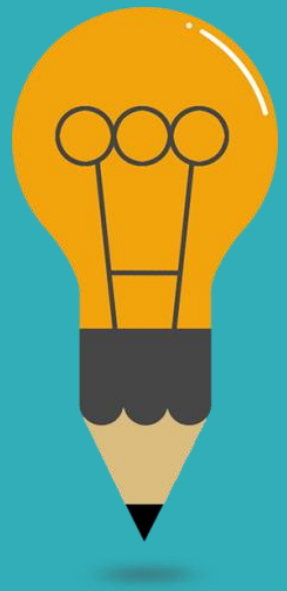
Αυτό μπορεί να συμβεί εάν η Alice γνωρίζει το **Δημόσιο κλειδί** του Bob (διεύθυνση) και εφόσον κατέχει το δικό της **Ιδιωτικό κλειδί**.

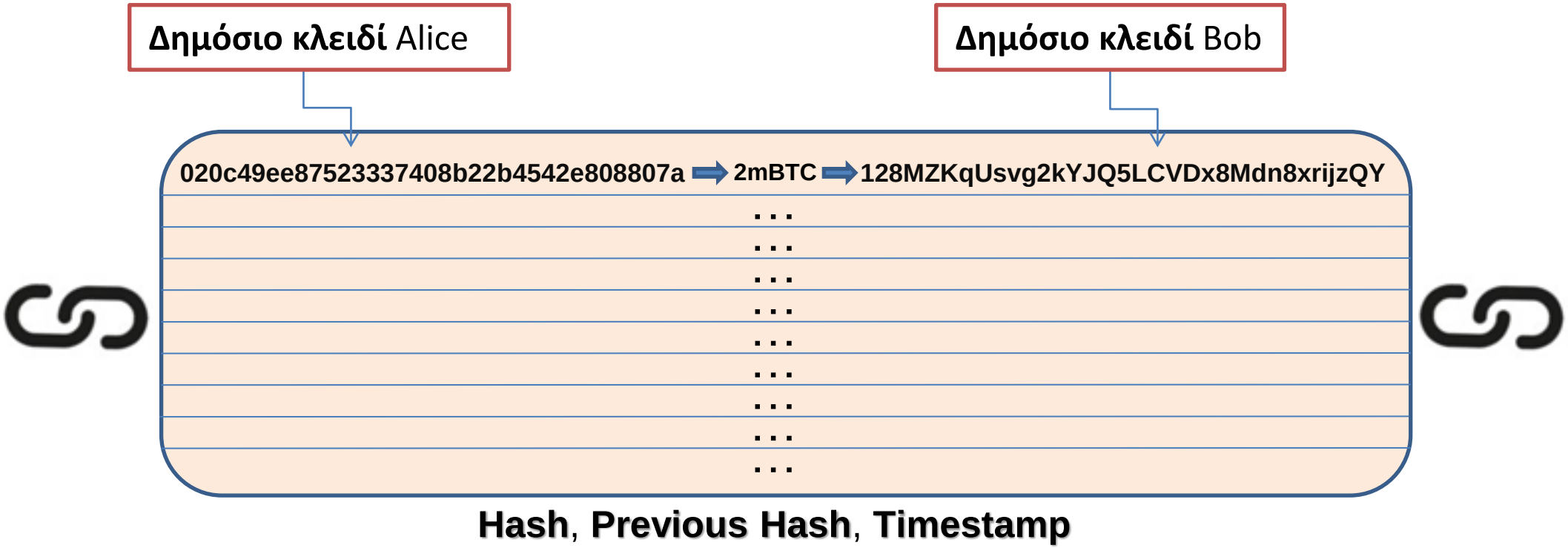


Κλειδιά:

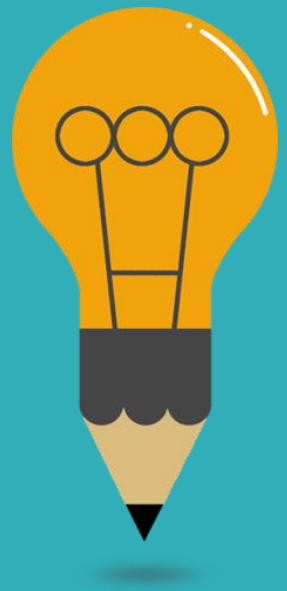
Παράδειγμα αποστολής χρημάτων

Εφόσον η συναλλαγή κριθεί επιτυχής και επιβεβαιωθεί από το δίκτυο, καταγράφεται σε ένα block του blockchain και μένει εκεί για πάντα.





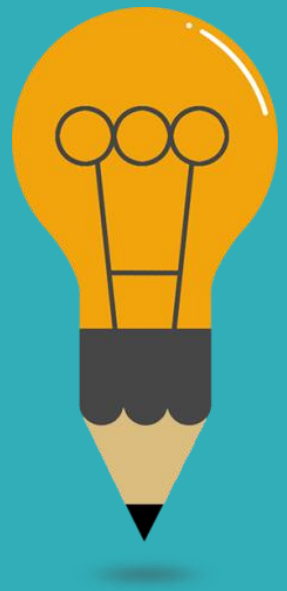
Κλειδιά:

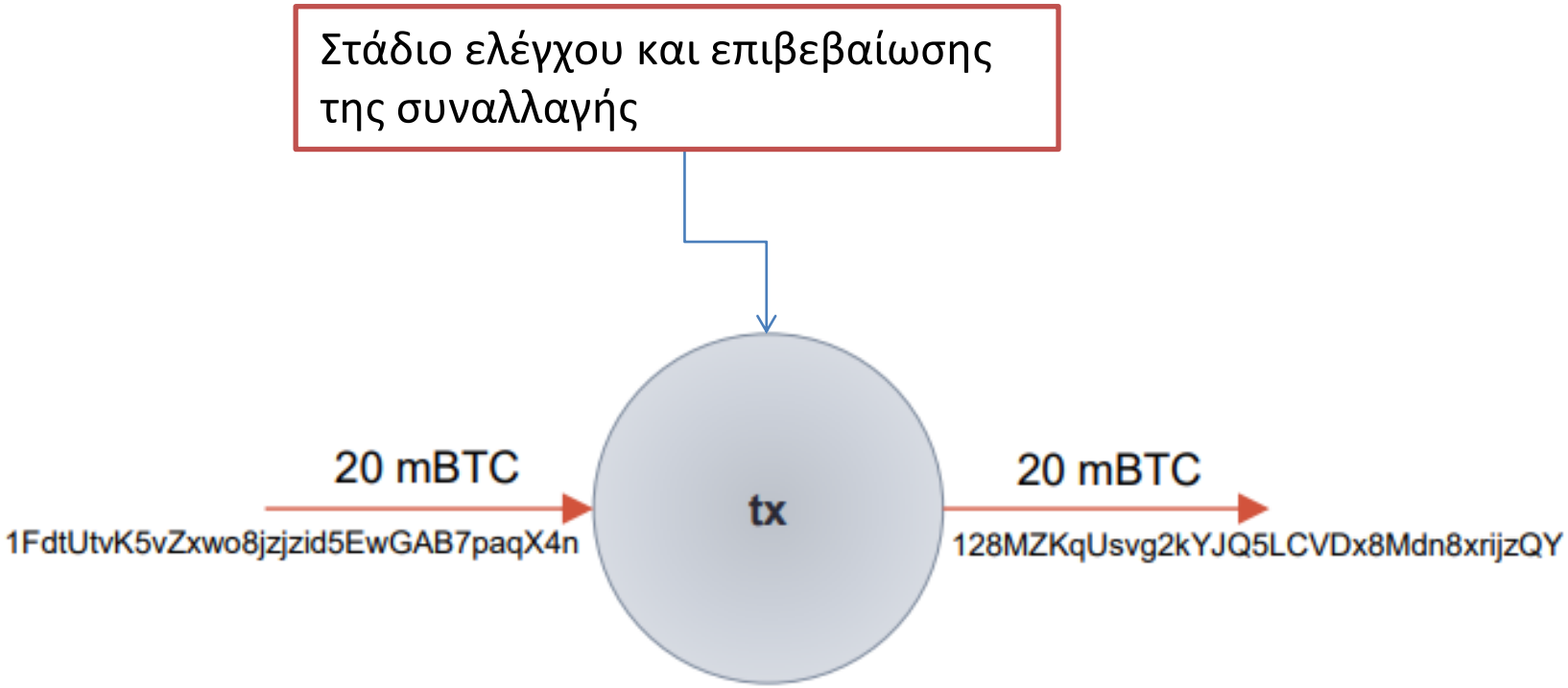


Μερικά χρήσιμα συμπεράσματα...

1. Κάθε χρήστης δημιουργεί πολλαπλά δημόσια κλειδιά.
2. Δεν γνωρίζουμε ποια δημόσια κλειδιά ανήκουν σε ποιον.
3. Ανωνυμία επιτυγχάνεται επειδή οι συναλλαγές αφορούν δημόσια κλειδιά και κάθε χρήστης μπορεί να έχει παραπάνω από ένα.
4. Οι πληρωμές γίνονται συνδέοντας κόμβους συναλλαγών μέσω των διευθύνσεών τους (δημόσια κλειδιά).
5. Το χρήμα είναι ουσιαστικά μία αλυσίδα συναλλαγών.
6. Μπορούμε να αντιληφθούμε την κάθε συναλλαγή που πραγματοποιείται ως μία πρόταση σε ένα βιβλίο και το κάθε μπλοκ ως μία σελίδα αυτού του βιβλίου.
   Το blockchain αποτελεί το βιβλίο.

Επιβεβαίωση συναλλαγών:





Mining

Εξόρυξη:

Εξόρυξη ή αλλιώς **mining** ονομάζεται η διαδικασία ελέγχου και επιβεβαίωσης των συναλλαγών ή αλλιώς η διαδικασία παραγωγής blocks.

Μέσω αυτής της διαδικασίας γίνεται και η παραγωγή των νέων Bitcoins, και από αυτό προκύπτει η επιλογή του ονόματος της εξόρυξης!

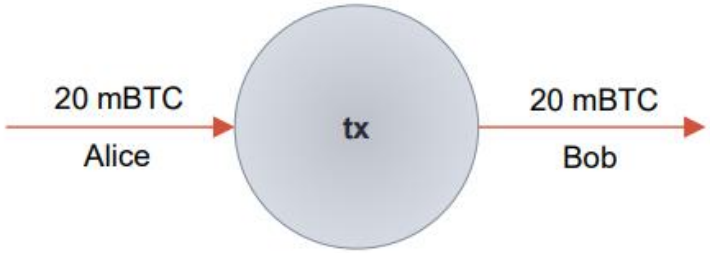
Miners:

Η εξόρυξη πραγματοποιείται από τους λεγόμενους miners.
Πρόκειται για άτομα ή ομάδες ατόμων που “ανταγωνίζονται” συνεχώς για την παραγωγή των επόμενων blocks.

Το σύστημα είναι ελεύθερο στον οποιονδήποτε, συνεπώς καθένας μπορεί να παράξει ένα block ή με άλλα λόγια να γίνει miner.

Εξόρυξη:

Έστω ότι έχουμε την παρακάτω συναλλαγή προς επιβεβαίωση:



1. Η συναλλαγή αυτή θα σταλεί σε όλο το δίκτυο του Bitcoin ή καλύτερα σε όλους τους miners προκειμένου να επαληθευτεί.
2. Οι miners με τη σειρά τους θα ανατρέξουν στο blockchain προκειμένου να εξετάσουν το ιστορικό των συναλλαγών του αποστολέα, έτσι ώστε να δουν εάν το ποσό που πρόκειται να αποσταλεί από τη συγκεκριμένη διεύθυνση είναι πράγματι διαθέσιμο.
3. Εφόσον δεν υπάρξει πρόβλημα, η συναλλαγή μπαίνει στο block του miner, **αλλά όχι στην τελική αλυσίδα (blockchain)**.

Εξόρυξη:

Κάθε block έχει συγκεκριμένη χωρητικότητα, δηλαδή χωράει συγκεκριμένο αριθμό επιβεβαιωμένων συναλλαγών (**περίπου 2.000**). Οι συναλλαγές όμως που αποστέλλονται για επιβεβαίωση σε κάθε miner είναι αμέτρητες.

- Κάθε miner διαλέγει τις ‘καλύτερες’ συναλλαγές από μία δομή με το όνομα **Mempool** (ορατή σε όλους τους miners), η οποία περιλαμβάνει όλες τις συναλλαγές προς επιβεβαίωση, προκειμένου να τις εξετάσει και στη συνέχεια να τις καταχωρήσει στο μπλοκ του.
- Το βασικό κριτήριο για την επιλογή των ‘καλύτερων’ συναλλαγών είναι το εάν προσφέρουν κάποιο **transaction fee**, δηλαδή κάποιο “φιλοδώρημα” από τον αποστολέα προκειμένου να είναι η δική του συναλλαγή, αυτή η οποία θα συμπεριληφθεί πρώτη σε κάποιο μπλοκ. Το transaction fee δεν είναι υποχρεωτικό, αλλά αποτελεί εγγύηση για την ταχύτερη επιβεβαίωση μιας συναλλαγής. **Αποτελεί τη μία εκ των δύο πηγών εισοδήματος των miners**.

Εξόρυξη:

1. Αφού το μπλοκ γεμίσει, στη συνέχεια ο miner εκτελεί κάποιους πολύπλοκους μαθηματικούς υπολογισμούς προκειμένου να λύσει ένα πρόβλημα, κατά βάση “τύχης”. Συγκεκριμένα, στο Bitcoin οι υπολογιστές των miners προσπαθούν να λύσουν τον αλγόριθμο κατακερματισμού SHA-256, μέσα από τον οποίο θα προκύψει το HASH που θα μπει στην κεφαλίδα του μπλοκ.

2. Όποιος miner λύσει **πρώτος** το παραπάνω μαθηματικό πρόβλημα, θα είναι αυτός του οποίου το μπλοκ θα καταχωρηθεί στο blockchain και ταυτόχρονα θα επιβραβευθεί με μία ποσότητα νέων Bitcoins. Αυτός είναι και ο μοναδικός τρόπος παραγωγής τους και **αποτελεί τη δεύτερη πηγή εισοδήματος των miners**.

3. Πριν καταχωρηθεί το συγκεκριμένο block μία για πάντα στο blockchain, στέλνεται για την τελική επιβεβαίωση σε όλους τους miners, έτσι ώστε να υπάρξει **συναίνεση** (consensus) σχετικά με την εγκυρότητα των συναλλαγών που περιλαμβάνει.

Εξόρυξη:

Πώς επιλέγεται ο δημιουργός κάθε επόμενου block;

Ο miner που θα λύσει πρώτος τους πολύπλοκους μαθηματικούς υπολογισμούς, θα είναι και αυτός του οποίου το μπλοκ θα καταχωρηθεί στην τελική αλυσίδα και στη συνέχεια θα επιβραβευθεί με Bitcoins. Το ποιος θα είναι ο «πρώτος» miner σε κάθε επόμενο μπλοκ είναι ένας συνδυασμός "**τύχης**" και "**ικανότητας**":

- **Τύχη:** Ο αλγόριθμος SHA-256 βασίζεται σε απίστευτα μεγάλο αριθμό δοκιμών προκειμένου να παραχθεί ένας συγκεκριμένος αριθμός κάθε φορά. Λόγω της πολύ χαμηλής πιθανότητας επιτυχούς εύρεσης, αυτό καθιστά απρόβλεπτο ποιος υπολογιστής-εργαζόμενος στο δίκτυο θα είναι σε θέση να δημιουργήσει το επόμενο μπλοκ.

- **Ικανότητα:** Η ικανότητα αφορά την υπολογιστική ισχύ κάθε υπολογιστικού κέντρου. Όσο μεγαλύτερη είναι η υπολογιστική ισχύς που κατέχει κάποιος miner, τόσο μεγαλύτερη είναι και η πιθανότητα να είναι αυτός ο οποίος θα παράξει τον ζητούμενο τυχαίο αριθμό και κατ' επέκταση το επόμενο block του blockchain.

Miners:

Proof-of-Work

Η εκτέλεση του αλγορίθμου SHA-256 από τους miners αποτελεί μία διαδικασία απόδειξης εργασίας, η οποία καθιστά το δίκτυο αξιόπιστο.

Οι πολύπλοκοι μαθηματικοί υπολογισμοί απαιτούν τεράστια υπολογιστική ισχύ (ρεύμα) και πολύ ισχυρά μηχανήματα (Η/Υ) για να εκτελεστούν. Συνεπώς, είναι μία διαδικασία με υψηλό κόστος για τους miners.

Ένας miner αποδεικνύει την αξιοπιστία του “δουλεύοντας” (**proof-of-work**), βάζοντας δηλαδή τον υπολογιστή του να εκτελέσει τον αλγόριθμο, έτσι ώστε να παράξει το hash που είναι η τελική απόδειξη της παραπάνω εργασίας και το οποίο καταχωρείται στην κεφαλίδα του μπλοκ.

Με άλλα λόγια προσφέρει στο δίκτυο την υπολογιστική ισχύ του μηχανήματός του, η οποία απαιτεί χρήματα (ρεύμα-εξοπλισμός) και σαν αντάλλαγμα κερδίζει Bitcoins.

Η διαδικασία αυτή είναι τόσο σύνθετη που κατά μέσο όρο διαρκεί περίπου **10 λεπτά**.

Miners:

Proof-of-Stake

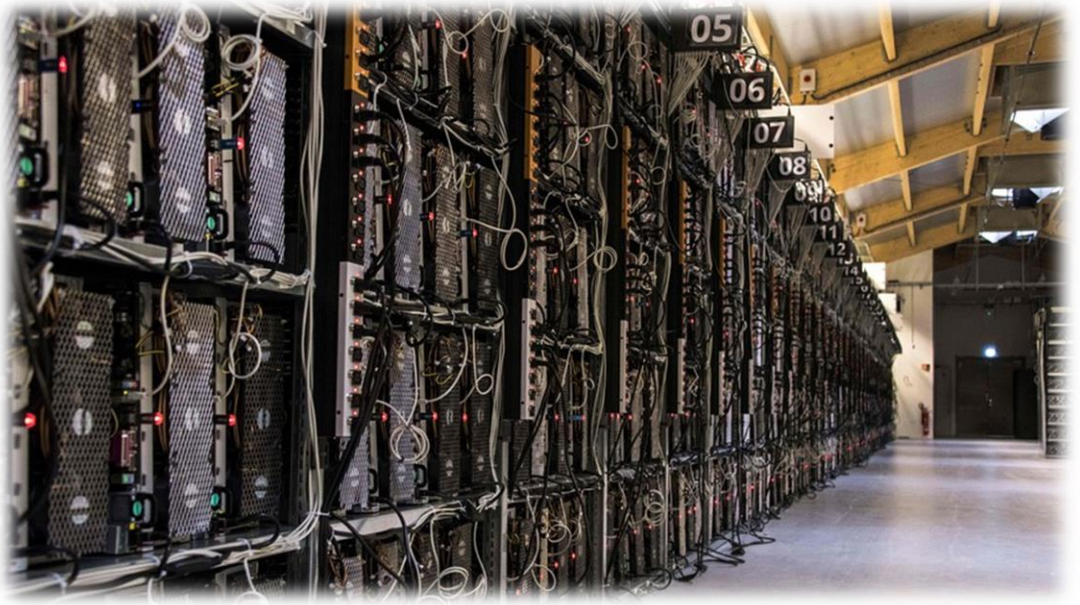
Το **Proof-of-Stake** (POS) αποτελεί μία άλλη μέθοδο για την απόδειξη αξιοπιστίας ενός "εργαζομένου" στο δίκτυο, που δημιουργήθηκε ως εναλλακτική του POW.

Σύμφωνα με αυτή τη μέθοδο, όσα περισσότερα κρυπτονομίσματα κατέχει κάποιος, τόσα περισσότερα μπλοκ δικαιούται να επαληθεύσει. Με άλλα λόγια, όσα περισσότερα κρυπτονομίσματα έχει σε σχέση με το υπόλοιπο δίκτυο (ποσοστιαία), τόσο μεγαλύτερη είναι και η υπολογιστική του ισχύς.

Οι συμμετέχοντες επιλέγονται τυχαία για να επιβεβαιώσουν τις συναλλαγές και να επαληθεύσουν τις πληροφορίες ενός μπλοκ. Για να γίνει "**επαληθευτής**" ένας κάτοχος νομισμάτων πρέπει να "**ποντάρει**" μία συγκεκριμένη ποσότητα νομισμάτων (για παράδειγμα, στο Ethereum απαιτείται ποντάρισμα 32 ETH προτού ο χρήστης μπορέσει να λειτουργήσει έναν κόμβο).

Σε αντίθεση με τη μέθοδο POW που απαιτεί τεράστια ποσά ενέργειας για την εκτέλεσή της, η POS είναι πολύ πιο οικονομική και φιλική προς το περιβάλλον.

Miners:



Mining Pools & Mining Farms

Θεωρητικά ο καθένας θα μπορούσε να γίνει miner.

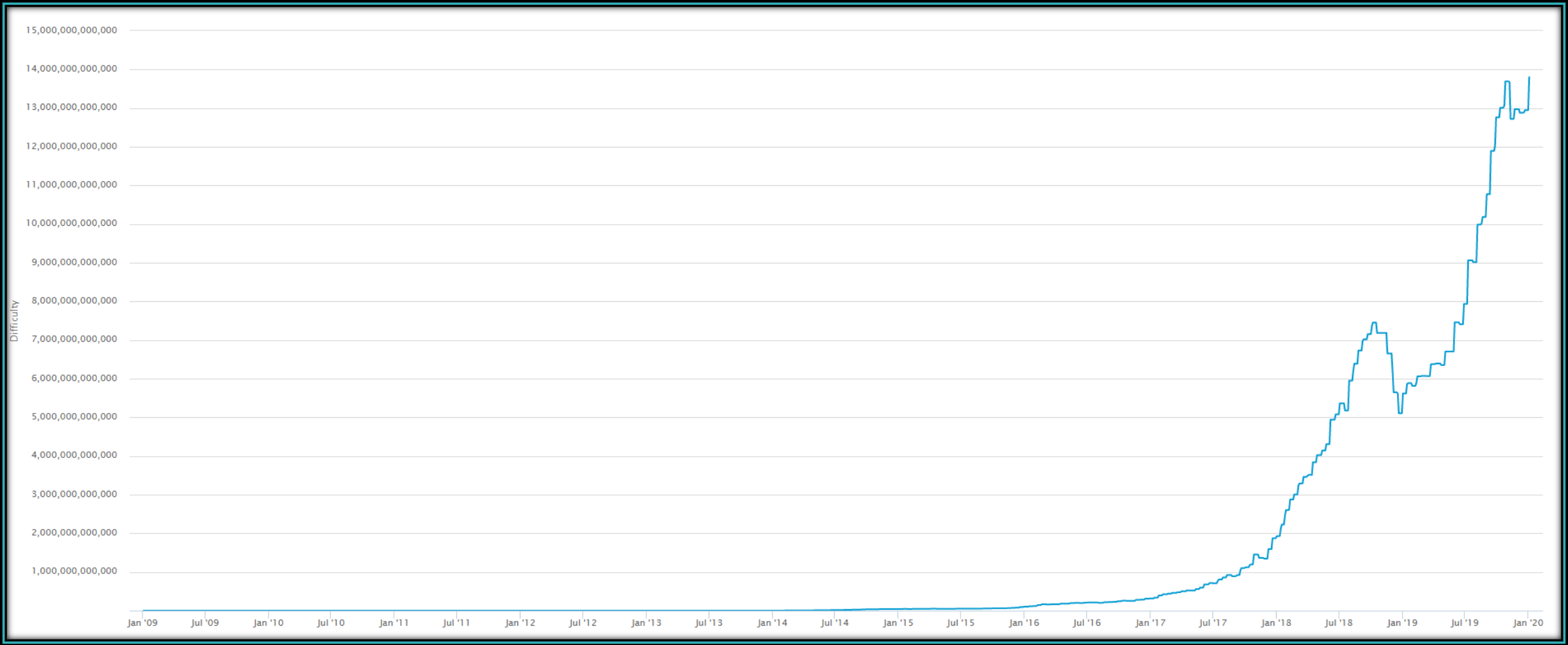
Τα τεράστια έξοδα όμως προκειμένου να στηθεί και να συντηρηθεί ένα σταθμός mining, καθώς και οι τεχνολογικές γνώσεις που απαιτούνται είναι αποτρεπτικός παράγοντας για τον απλό κόσμο.

Η εξόρυξη πλέον γίνεται κατά κύριο λόγο από τα λεγόμενα **Mining Pools** και τα **Mining Farms**.

• **Mining Pools:** πρόκειται για μία ομάδα miners οι οποίοι αποφάσισαν να συνεργαστούν -μέσω κάποιου πρωτοκόλλου- και να χρησιμοποιήσουν συνολικά την υπολογιστική ισχύ των μηχανημάτων τους για την παραγωγή ενός μπλοκ και στη συνέχεια να μοιραστούν τα έσοδα. Με άλλα λόγια λειτουργούν ομαδικά, ως ένας miner.

• **Mining Farms:** πρόκειται για πολύ μεγάλα κέντρα υπολογιστών, ειδικά σχεδιασμένα και εξοπλισμένα για mining.

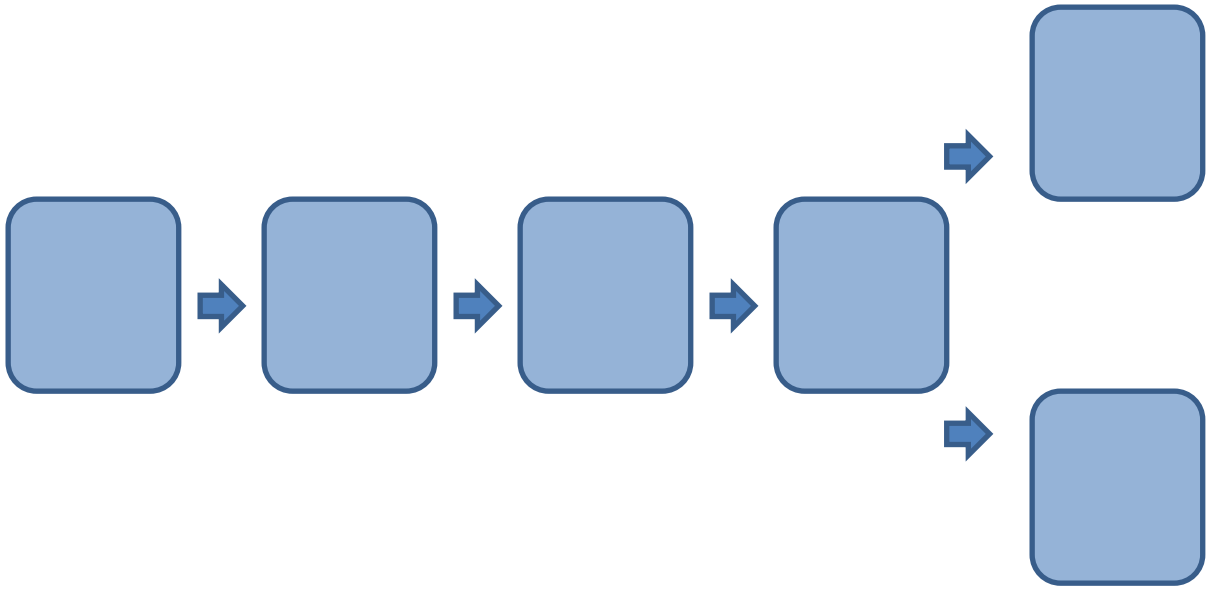
Δυσκολία εξόρυξης ενός μπλοκ:



Fork

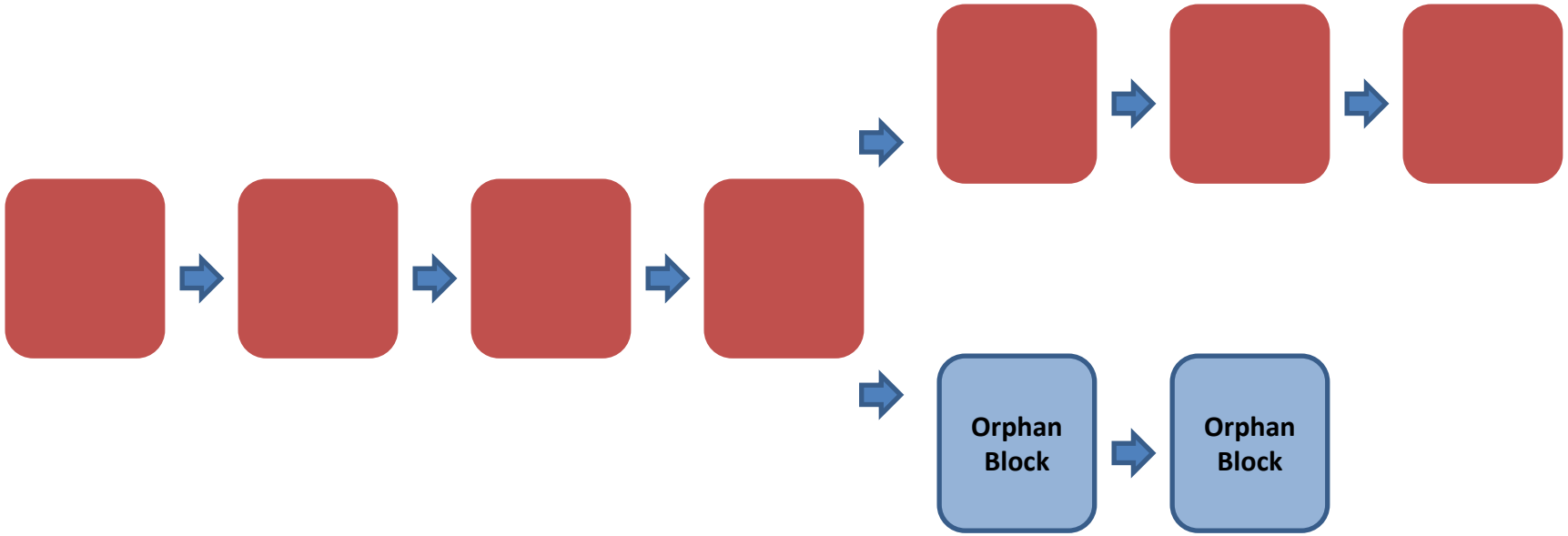
Τι θα συμβεί σε περίπτωση που δύο ή περισσότεροι miners δημιουργήσουν ένα μπλοκ σχεδόν την ίδια στιγμή;

Σε αυτή την περίπτωση το blockchain «σπάει» στα 2 και έχει την παρακάτω μορφή:



Fork

Στη συνέχεια και εφόσον αρχίσουν να προστίθενται τα επόμενα μπλοκ, μία από τις αλυσίδες θα γίνει μεγαλύτερη από την άλλη. Τα μπλοκ που δεν βρίσκονται στη μεγαλύτερη αλυσίδα ονομάζονται **ορφανά μπλοκ (orphan blocks)** και εγκαταλείπονται από το δίκτυο.



Fork

Συμπέρασμα:

Σε περιπτώσεις «διακλάδωσης» (fork) το δίκτυο θα επιλέξει κατά κύριο λόγο τη μεγαλύτερη αλυσίδα προκειμένου να συνεχίσει την ομαλή λειτουργία του. *Υπάρχουν όμως περιπτώσεις που αυτός ο κανόνας μπορεί να αγνοηθεί:*

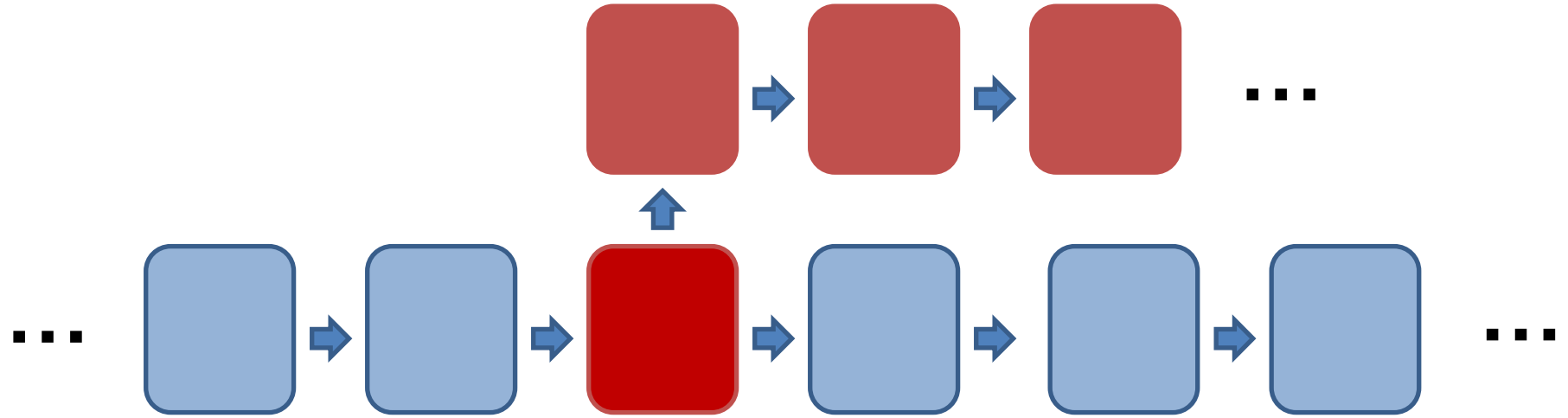
•Εντοπισμός λάθους σε κάποιο μπλοκ.

•Ασυμφωνία μεταξύ των χρηστών του δικτύου.

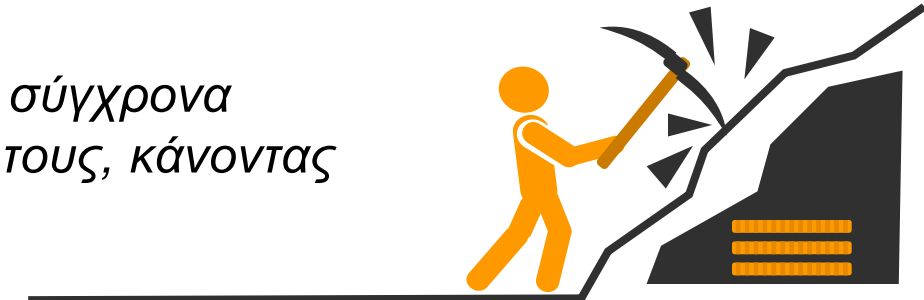
•Ενδεχόμενη επίθεση στο δίκτυο.

Fork

Σε μία τέτοια περίπτωση θα εντοπιστεί το μπλοκ που εμπεριέχει το «λάθος» ή το σημείο που παρατηρείται η «ασυμφωνία» και στη συνέχεια η ομάδα χρηστών που «διαφωνεί» θα δημιουργήσει από εκείνο το σημείο κι έπειτα τη δική της νέα εκδοχή της αλυσίδας δημιουργώντας μία «διακλάδωση» και θεωρώντας τα μπλοκ της εναλλακτικής αλυσίδας ως μη γενόμενα.



Με αυτόν τον τρόπο έχουν δημιουργηθεί και πολλά από τα πιο σύγχρονα κρυπτονομίσματα, βασισμένα σε πρωτόκολλα προγενέστερών τους, κάνοντας τροποποιήσεις και αλλαγές σε συγκεκριμένα σημεία.



Εξόρυξη:

Υπολογιστική ισχύς

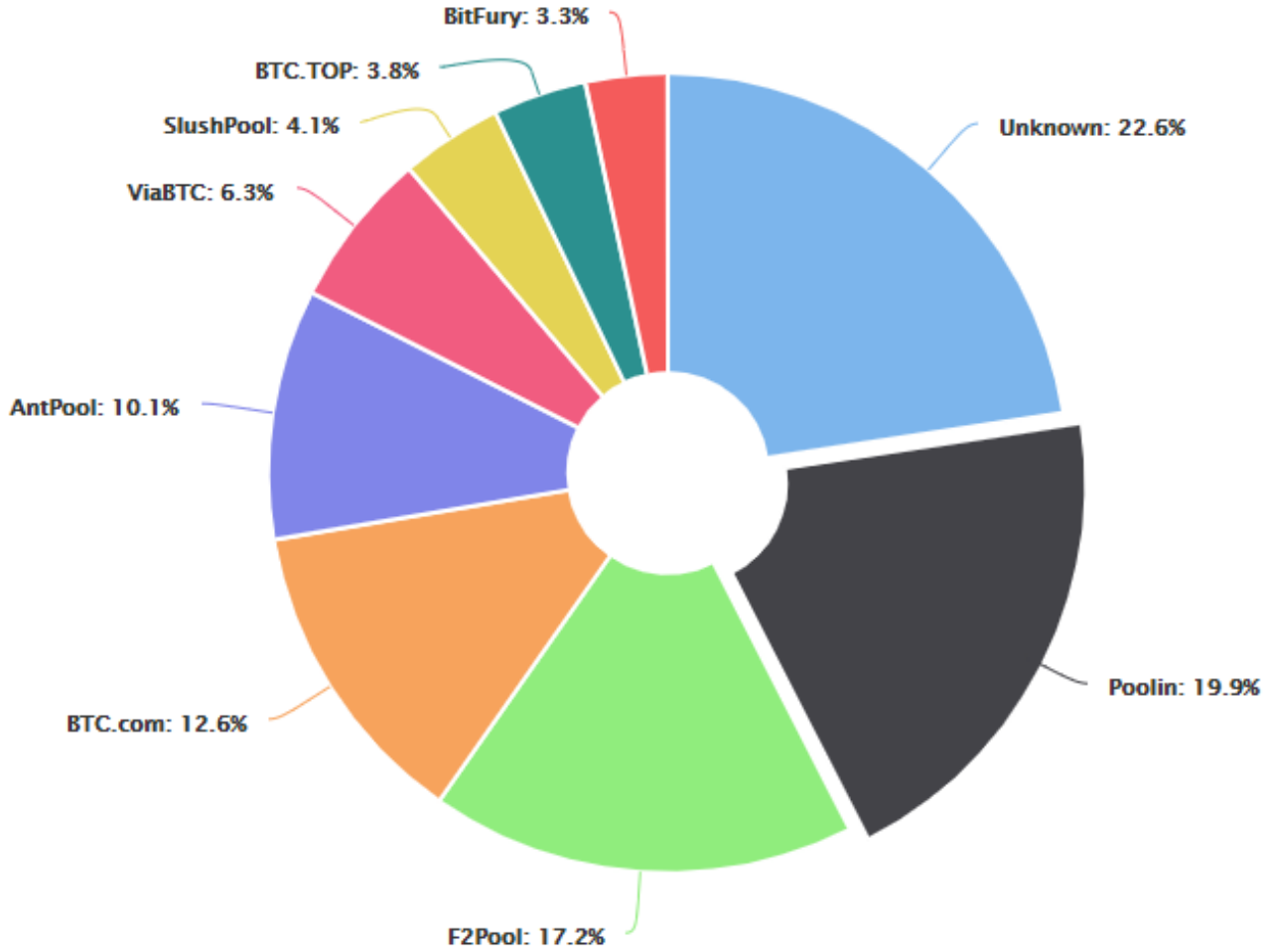
- Αυξάνοντας την υπολογιστική ισχύ, αυξάνονται και οι πιθανότητες εύρεσης της λύσης του μαθηματικού προβλήματος που θα οδηγήσει στη δημιουργία του μπλοκ. Για παράδειγμα, αν ένας miner κατέχει το 25% της συνολικής υπολογιστικής ισχύος του δικτύου, τότε έχει 25% πιθανότητες να είναι αυτός ο δημιουργός του επόμενου μπλοκ.

- Στα περισσότερα κρυπτονομίσματα πλέον η υπολογιστική ισχύς του δικτύου ανήκει κατά κύριο λόγο σε τεράστια mining farms ή mining pools που κατέχουν μέχρι και το 80% της συνολικής ισχύος! Αυτό σημαίνει στατιστικά ότι σε μία τέτοια περίπτωση, περίπου το 80% των συναλλαγών που πραγματοποιούνται στο συγκεκριμένο δίκτυο ελέγχονται και επιβεβαιώνονται από έναν πολύ μικρό αριθμό miners.

...Κίνδυνος επίθεσης 51%;

Εξόρυξη:

Κατανομή υπολογιστικής ισχύος: Bitcoin



Miners:

Υπάρχει κίνδυνος επίθεσης του 51%;

Εφόσον το δίκτυο και οι συναλλαγές που εκτελούνται σε αυτό ελέγχονται εξ ολοκλήρου από τους χρήστες του, είναι βάσιμο κάποιος να υποστηρίζει ότι μία επίθεση του 51% είναι ένας υπαρκτός κίνδυνος. Τα προηγούμενα δεδομένα σχετικά με την κατανομή της υπολογιστικής ισχύος στα περισσότερα κρυπτονομίσματα, θα μπορούσε κανείς να πει, ότι κάνουν αυτήν την ανησυχία ακόμη πιο έντονη.

Στην πραγματικότητα όμως, οι πιθανότητες να συμβεί μία επίθεση του 51% είναι μηδαμινή, καθώς είναι πολύ δύσκολο έως και αδύνατο να καταστεί κερδοφόρα για τους υποκινητές της.

Miners:

Τι θα συμβεί σε περίπτωση μιας επίθεσης του 51%;

Ακόμη κι αν ένας ή μία ομάδα κακόβουλων miners κατάφερναν να πάρουν στα χέρια τους ένα ποσοστό της τάξης του 51% της υπολογιστικής ισχύος του δικτύου -κάτι το οποίο απαιτεί υπέρογκα ποσά χρημάτων- αυτό θα είχε ως αποτέλεσμα μετά την πρώτη κιόλας παραβίαση κάποιου κανόνα (π.χ. διπλή δαπάνη νομίσματος) να ακολουθήσουν τα εξής:

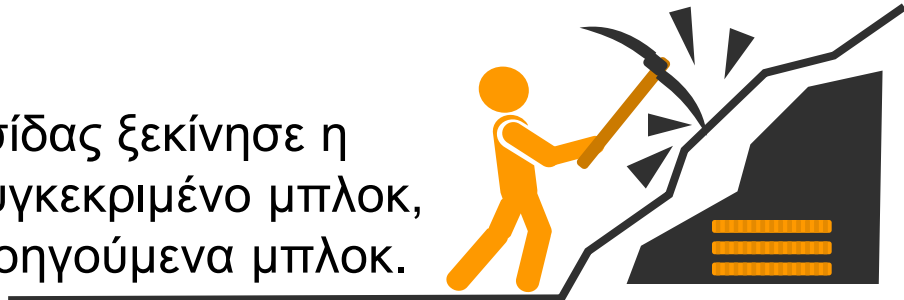
• Αρκετά σύντομα θα γίνει γνωστό στους χρήστες ότι το δίκτυο έχει «παραβιαστεί».

•Οι χρήστες θα χάσουν κάθε εμπιστοσύνη προς το νόμισμα.

•Η αξία του νομίσματος θα γνωρίσει κατακόρυφη πτώση.

•Σύντομα θα σταματήσουν να γίνονται συναλλαγές με το συγκεκριμένο νόμισμα.

•Η κοινότητα των χρηστών θα εντοπίσει σε ποιο μπλοκ της αλυσίδας ξεκίνησε η παραβίαση και στη συνέχεια θα κάνει fork παραβλέποντας το συγκεκριμένο μπλοκ, αλλά και όσα ακολούθησαν, συνεχίζοντας την αλυσίδα με τα προηγούμενα μπλοκ.



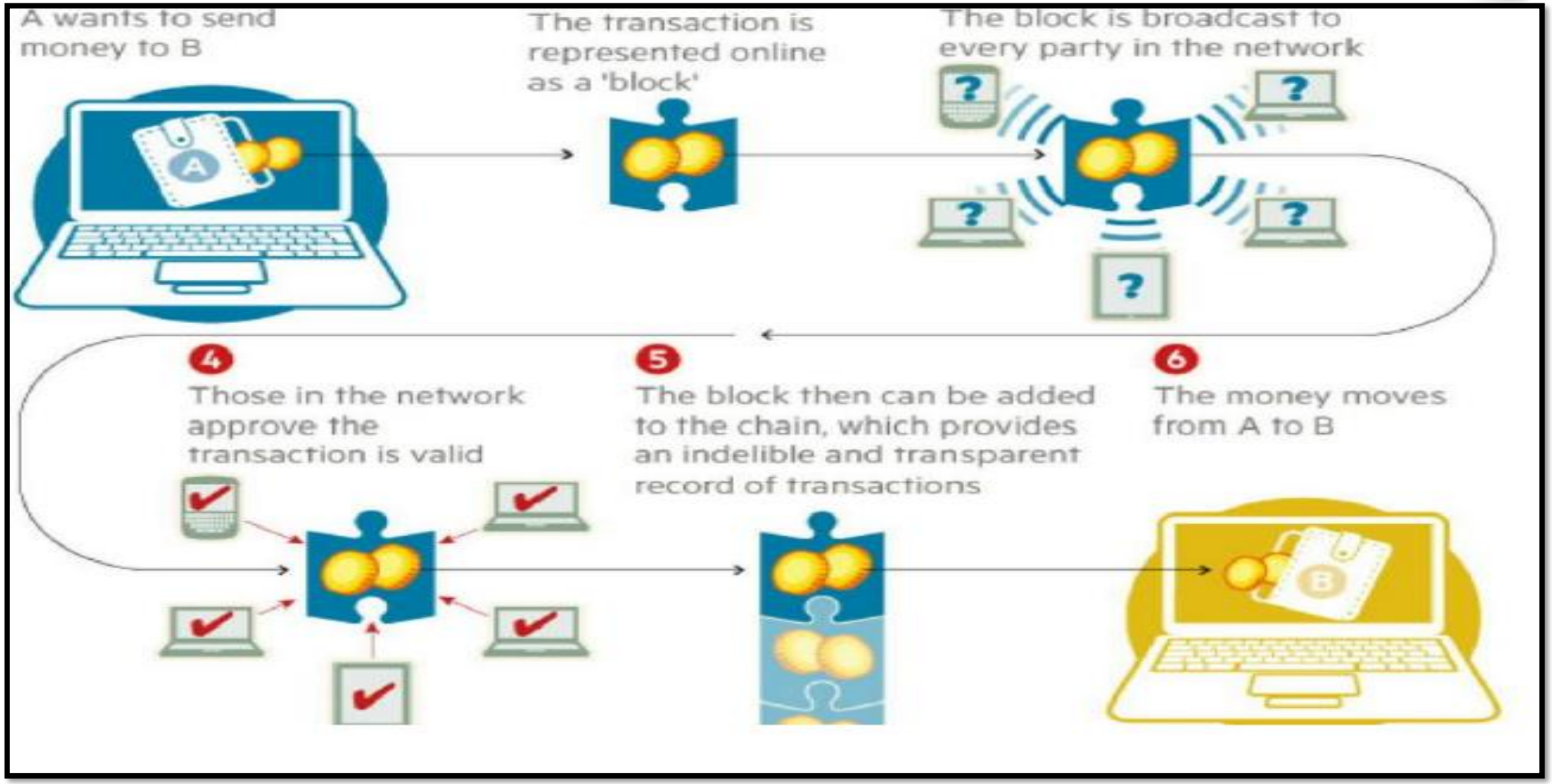
Επίθεση του 51%

Συμπέρασμα:

Μία επίθεση του 51% μπορεί πρακτικά να συμβεί αλλά είναι ασύμφορη γι' αυτόν που θα την επιδιώξει. Ο σχεδιασμός του δικτύου είναι τόσο ισχυρός που η επίθεση θα εντοπιστεί άμεσα και η αντίδραση της κοινότητας θα γίνει αστραπιαία με πολύ σοβαρές συνέπειες απομονώνοντας ουσιαστικά το κομμάτι του δικτύου που έχει παραβιαστεί.

Ακόμη και σε περίπτωση επιτυχούς επίθεσης, όπου το δίκτυο δεν θα εντοπίσει την επίθεση και οι συναλλαγές θα συνεχίσουν να εκτελούνται κανονικά, τα έξοδα που απαιτούνται για την απόκτηση του μεγαλύτερου ποσοστού της υπολογιστικής ισχύος του δικτύου καθώς και της συντήρησής του είναι τόσο μεγάλα που κανείς δεν μπορεί να εγγυηθεί ότι ο δράστης θα έχει τελικά θετικό αποτέλεσμα.

Στάδια συναλλαγής σε Bitcoin: Σχηματική απεικόνιση



Πληθωρισμός

Πληθωρισμός

Ένα από τα βασικά χαρακτηριστικά του Bitcoin που το έκαναν να ξεχωρίσει είναι ο ελεγχόμενος πληθωρισμός του.

Το νόμισμα λειτουργεί με τέτοιο τρόπο, ώστε ποτέ να μην έρθει αντιμέτωπο με φαινόμενα υπερπληθωρισμού.

Πληθωρισμός

Πώς το πετυχαίνει αυτό;

•Ο μέγιστος αριθμός κερμάτων που θα παραχθεί ποτέ, περιορίζεται αυστηρά στα **21 εκατομμύρια** Bitcoins.

•Ο αλγόριθμος «παραγωγής» των bitcoins έχει ρυθμιστεί έτσι ώστε να **υποδιαιρεί** τον αριθμό των παραγόμενων νομισμάτων κάθε **4 χρόνια** (**~210.000 blocks**).

•Σήμερα τα Bitcoins που παράγονται για κάθε μπλοκ ή αλλιώς η αμοιβή κάθε miner για την εξόρυξη ενός μπλοκ είναι 6,25 BTC, ενώ το 2024 θα είναι 3,125 BTC.

•Σε κάποια blockchain άλλων νομισμάτων, η υποδιαίρεση έχει ρυθμιστεί να γίνεται ακόμη και ανά έναν χρόνο.

Πληθωρισμός

Πώς το πετυχαίνει αυτό;

•Με τη μέθοδο αυτή, υποδιαιρείται και ο πληθωρισμός του νομίσματος κάθε 4 χρόνια, με αποτέλεσμα κάποια στιγμή να μηδενιστεί, όταν και θα παραχθεί το τελευταίο BTC!

•Όπως ο χρυσός, έτσι και τα BTC, δεν είναι απεριόριστα. Το γεγονός αυτό καθιστά το νόμισμα σπάνιο και κάνει την αξία του ανθεκτική στο πέρασμα του χρόνου.

Πληθωρισμός

Πώς το πετυχαίνει αυτό;

- Αυτή τη στιγμή έχουν παραχθεί περίπου 19.000.000 BTC.
- Το 2036 υπολογίζεται ότι θα έχει παραχθεί το 95,5% του συνόλου των BTC.
- Το τελευταίο BTC αναμένεται να παραχθεί το 2140.
- Δεδομένου ότι δεν υπάρχουν ούτε πολιτικές δυνάμεις, ούτε επιχειρήσεις που να μπορούν να αλλάξουν αυτή τη σειρά, δεν υπάρχει δυνατότητα ανάπτυξης πληθωρισμού στο σύστημα.

Ενέργεια

Απαιτήσεις εξοπλισμού

Η εξόρυξη Bitcoins γινόταν πάντοτε μέσω υπερσύγχρονων υπολογιστών με ισχυρούς επεξεργαστές και κάρτες γραφικών, οι οποίοι καταναλώνουν πολύ μεγάλη ενέργεια. Σήμερα χρησιμοποιούνται **ASICs** (**Application Specific Integrated Circuits**) που κοστίζουν χιλιάδες euros και έχουν τη δυνατότητα υπολογισμών έως **230 TH/s**.

Η συνολική κατανάλωση ηλεκτρικής ενέργειας που απαιτείται για την εξόρυξη των κρυπτονομισμάτων είναι τεράστια, με αποτέλεσμα πολλοί ειδικοί να χτυπούν το «καμπανάκι του κινδύνου» για τις περιβαλλοντικές επιπτώσεις που συνεπάγεται.

Ενέργεια

Πόσο ρεύμα «καίει» το Bitcoin;

Με τα σημερινά δεδομένα, εκτιμάται ότι η εξόρυξη Bitcoins απαιτεί περίπου **62 τεραβατώρες (TWh) ετησίως.**

Επιπλέον, εάν η τιμή του Bitcoin αυξηθεί περαιτέρω, η κατανάλωση ηλεκτρικής ενέργειας θα αυξηθεί επίσης.

Ενέργεια

Πιο συγκεκριμένα:

•Η ισχύς που καταναλώνεται από ολόκληρο το δίκτυο εξόρυξης του Bitcoin αντιστοιχεί στο 0,3% της παγκόσμιας κατανάλωσης ρεύματος.

•Υπολογίζεται ότι για κάθε συναλλαγή Bitcoin θα μπορούσαν να ηλεκτροδοτηθούν 35 νοικοκυριά για μία ολόκληρη ημέρα!

•Η Τσεχική Δημοκρατία χρησιμοποιεί περίπου 62,34 TWh ετησίως, ενώ η Ελβετία καταναλώνει 58,46 TWh, η Ελλάδα 56,89, το Ισραήλ 55 και η Ιρλανδία 25,68. Αν το Bitcoin ήταν χώρα, θα ήταν η **41η πιο ενεργειακά απαιτητική** στον πλανήτη.

•Το κόστος της εξόρυξης είναι υπέρογκο και ξεπερνά τα $3,5 δις ετησίως!

Ενέργεια


Το Bitcoin «καταβροχθίζει» ενέργεια!
ΧΡΗΣΗ
Ηλεκτρικής ενέργειας:
61,76 TWh
(0,28% του συνόλου της παγκόσμιας κατανάλωσης)
62,3 TWh
Τσεχική Δημοκρατία
56,9 TWh
Ελλάδα
25,7 TWh
Ιρλανδία
ετησίως
Αν το Bitcoin ήταν χώρα, θα ήταν 41η στην κατανάλωση ενέργειας
Η κατανάλωση ηλεκτρικής ενέργειας από το Bitcoin αντιστοιχεί:
1/70 της παγκόσμιας παραγωγής ενέργειας από το νερό
1/10 της παγκόσμιας παραγωγής ενέργειας από βιοκαύσιμα & απόβλητα
1/24 της παγκόσμιας παραγωγής ενέργειας από τον ήλιο, τον άνεμο κλπ
ΣΧΕΔΙΑΣΗ: ΠΕΓΚΥ ΒΑΡΙΤΑΚΗ
ΠΗΓΗ: Forbes, με μετρήσεις από το Πανεπιστήμιο του Κέμπριτζ

Ενέργεια

Οι συνέπειες για το περιβάλλον:

Η διαδικασία της εξόρυξης και η υπολογιστική ισχύς που απαιτείται για την πραγματοποίησή της οδηγούν στην κατανάλωση υπέρογκων ποσών ενέργειας.

Οι εκπομπές διοξειδίου του άνθρακα που προκαλούνται από τη διαδικασία της εξόρυξης αγγίζουν τους 35 μεγατόνους, όσοι περίπου εκπέμπονται από 1,5 εκατομμύριο υπερατλαντικές πτήσεις!

Οι συνέπειες της αύξησης του -ήδη αυξημένου- διοξειδίου του άνθρακα που εκπέμπεται στην ατμόσφαιρα δεν είναι άλλες από την επιδείνωση φαινομένων, όπως το φαινόμενο του θερμοκηπίου, η κλιματική αλλαγή κτλ.

Ενέργεια

Τι κάνουν οι miners;

Το μεγαλύτερο κόστος για τους miners του Bitcoin είναι η ηλεκτρική ενέργεια.
Για τον λόγο αυτό αναζητούν ολοένα και πιο απεγνωσμένα φθηνές πηγές ηλεκτρικής ενέργειας, ενώ ορισμένοι καταφεύγουν ακόμη και στην κλοπή ρεύματος.

Ενδεικτικό είναι το γεγονός πως τα μεγαλύτερα κέντρα mining είναι σε χώρες με φθηνό και άφθονο ηλεκτρικό ρεύμα.

Περίπου το 80% της εξόρυξης του Bitcoin συμβαίνει σήμερα στην Κίνα,
ενώ αναπτύσσεται και σε άλλα μέρη όπως: Ισλανδία, Ιαπωνία, Γεωργία,
Τσεχική Δημοκρατία, Ινδία, τμήματα των Ηνωμένων Πολιτειών, Βενεζουέλα.
Κοινό στοιχείο των παραπάνω χωρών, η χαμηλή τιμή ρεύματος.

Ενέργεια

Λύσεις:

1. Εκμετάλλευση ανανεώσιμων πηγών ενέργειας και δημιουργία κέντρων παραγωγής ηλεκτρικής ενέργειας για αποκλειστική χρήση mining (αρκετά χρονοβόρα ενέργεια και με πολύ υψηλό κόστος).
    - Γεωθερμική ενέργεια, ηλιακή ενέργεια, υδροηλεκτρική ενέργεια, ανεμογεννήτριες κτλ.
    - Στο πλαίσιο της μείωσης της κατανάλωσης ενέργειας, πολλοί miners ήδη έχουν εγκατασταθεί σε μέρη όπως η Ισλανδία, όπου χρησιμοποιούν φθηνή γεωθερμική ενέργεια. Αντίστοιχα, οι Κινέζοι miners χρησιμοποιούν υδροηλεκτρική ενέργεια στο Θιβέτ.
2. Αλλαγές στο πρωτόκολλο του δικτύου με σκοπό να δαπανάται λιγότερη ενέργεια.