Blockchain and its inherent security features

Σταυρούλα Καμπουρίδου

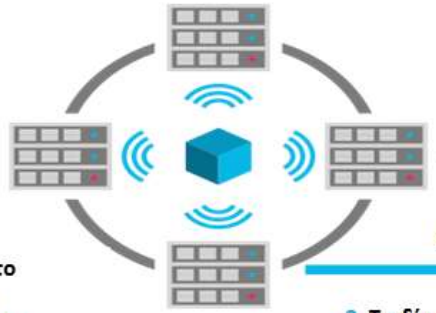
FinTech Advisor to the Governor, BoG

Head of the FinTech Innovation Hub, BoG

Οι απόψεις που παρουσιάζονται είναι δικές μου και δεν αντιπροσωπεύουν τις θέσεις της ΤτΕ και της ΕΚΤ

Πώς λειτουργεί:

1. Κάποιος ζητάει μια συναλλαγή



2. Η συναλλαγή μεταδίδεται σε όλο το ομότιμο δίκτυο των κόμβων του Blockchain

Επιβεβαίωση

Μια επιβεβαιωμένη συναλλαγή μπορεί να αφορά σε κρυπτονομίσματα, συμβόλαια, δικαιώματα δίσκων κ.α.

3. Το δίκτυο των κόμβων επιβεβαιώνει την ορθότητα της συναλλαγής και την ταυτότητα του χρήστη με τη χρήση κρυπτογραφίας και αλγορίθμων

4. Με την επιβεβαίωση της η συναλλαγή προστίθεται μαζί με άλλες για να δημιουργήσει ένα μπλοκ από επιβεβαιωμένες συναλλαγές

5. Το νέο μπλοκ προστίθεται στο τέλος του υφιστάμενου blockchain, και συνδέεται με αυτό μοναδικά

6. Η συναλλαγή έχει ολοκληρωθεί

ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ

Το κρυπτονόμισμα είναι ένα P2P αποκεντρωμένο ψηφιακό περιουσιακό στοιχείο το οποίο βασίζεται πάνω στις αρχές της κρυπτογραφίας για τη διασφάλιση του δικτύου δημιουργίας του και την επαλήθευση των συναλλαγών του

Δεν έχει εγγενή αξία, όπως πχ ο χρυσός

Δεν έχει φυσική μορφή, υπάρχει ψηφιακά στο δίκτυο

Η παραγωγή του δεν ελέγχεται από κάποιο κράτος, ή κεντρική τράπεζα και είναι αποκεντρωμένη

Bitcoin Blockchain, οι βασικές έννοιες:

Σύνοψη:

Οι **χρήστες**, έχουν λογαριασμούς, και μεταφέρουν bitcoin μεταξύ τους

Οι **συναλλαγές** αποθηκεύονται σε ένα ημερολόγιο/λογιστικό βιβλίο (το blockchain)

Το βιβλίο διατηρείται από τους **miners**, όλοι τους έχουν από ένα (το ίδιο) αντίγραφο.

Οι miners **αντικαθιστούν** τις τράπεζες και τα δίκτυα Visa / Mastercard / Amex…

Ο καθένας μπορεί να γίνει miner με την προϋπόθεση ότι θα κάνει τα παρακάτω:

1. Επένδυση σε (ισχυρό) υπολογιστή / server
2. Θα κατεβάσει & θα εκτελέσει το λογισμικό bitcoin

Από πού προέρχονται τα bitcoin;

Για τους χρήστες: αγοράζοντας τα σε κρυπτοανταλλακτήρια, cryptoATM, κάνοντας πωλήσεις (σπάνια) και ζητώντας για πληρωμή bitcoin (leasing private planes..)

Για τους miners: με εξόρυξη. . . Αυτός είναι ο τρόπος δημιουργίας bitcoin

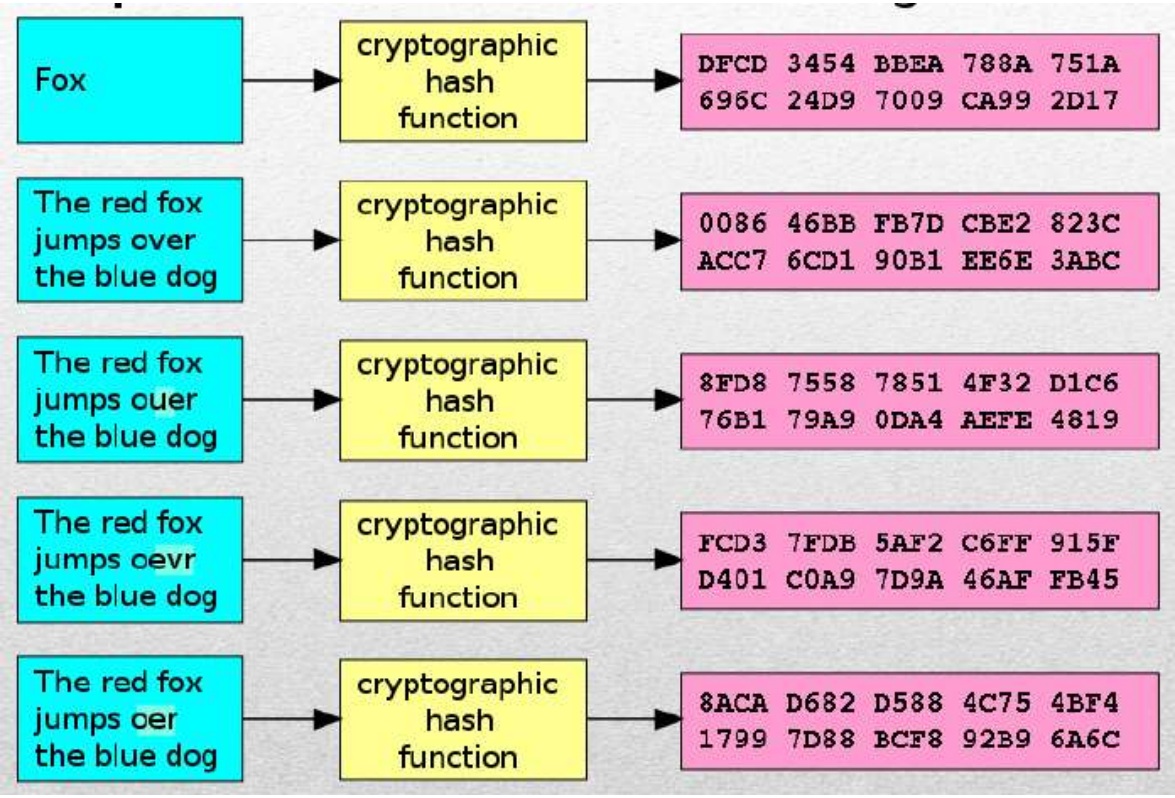
Χρήστες:

Με το bitcoin δε μιλάμε για λογαριασμούς αλλά για ηλεκτρονικά πορτοφόλια τα οποία έχουν:
Το ιδιωτικό κλειδί: 256-bit αριθμός (78 digits long). Αποτυπώνεται σε δεκαεξαδική μορφή (64 χαρακτήρες: 0-9 και A-F). **L4LSx9QmUgKqmy4mFT9sGRbzSXStjf7uQ4ZFQefni7kpDbbmeHxM**
Το ιδιωτικό κλειδί είναι σαν το “password".

Μια ηλεκτρονική διεύθυνση, συνήθως 34 χαρακτήρες (in Base58 format):
1Pw1f4WcDmp18oypcXqG4xFEhvqRVHJ252
Η διεύθυνση είναι σαν τον “τραπεζικό λογαριασμό” Αν κάνεις λάθος έστω και σε ένα ψηφίο, τα χάνεις…δεν μπορείς να τα διεκδικήσεις
Σημαντικό:
Το δημόσιο κλειδί παράγεται από το ιδιωτικό κλειδί. **Hash** (ιδιωτικό κλειδί)=δημόσιο κλειδί
Η διεύθυνση bitcoin παράγεται από το δημόσιο κλειδί. **Hash** (δημόσιο κλειδί) = διεύθυνση
Είναι υπολογιστικά αδύνατο να εξαχθεί το ιδιωτικό κλειδί από το δημόσιο κλειδί.

Hashing (συνάρτηση κατακερματισμού):

Μια hash function παίρνει είσοδο οποιουδήποτε μεγέθους και επιστρέφει μια καθορισμένη σειρά χαρακτήρων. Υπάρχουν αρκετές εκδόσεις, αυτή που χρησιμοποιείται το bitcoin είναι η SHA-256 (παράγει 256 bits). Hashing, ένα σημαντικό εργαλείο στην κρυπτογραφία: είναι μια λειτουργία **μονής κατεύθυνσης**. Είναι σχεδόν αδύνατο να εξαχθεί το input από το hash.



Συναλλαγές:

Το blockchain δεν περιέχει τα υπόλοιπα λογαριασμού (account balances). Περιέχει μόνο συναλλαγές, αλλά από την 1η ημέρα δημιουργίας του.
Μια συναλλαγή μοιάζει κάπως έτσι:
Tx: Η Alice στέλνει x bitcoin στον Bob

- Η συναλλαγή αυτή αποστέλλεται στη διεύθυνση του Bob, Hash (δημόσιο κλειδί).
- Όταν ο Bob θέλει να χρησιμοποιήσει αυτά τα bitcoin, μπορεί να το κάνει επειδή έχει το ιδιωτικό κλειδί που συνδέεται με την δημόσια διεύθυνση στο Tx του δέκτη.
- Η Αλίκη θα μπορούσε να στείλει x bitcoin στον Bob επειδή υπάρχει μια συναλλαγή στο παρελθόν όπου αυτή είναι ο παραλήπτης, οπότε έχει τα cryptocoins.

Δηλαδή: στο Bitcoin, **ξοδεύω σημαίνει “μεταφέρω" συναλλαγές**
Από τον ένα χρήστη στον άλλο. Όπως δηλαδή με τα μετρητά (χαρτονόμισμα/κέρμα)!

Miners/Ανθρακωρύχοι:

Ο Miner τρέχει/εκτελεί το bitcoin software σε έναν server:

- Ο server είναι συνδεδεμένος με άλλους υπολογιστικούς κόμβους, οι οποίοι μαζεύουν & μεταδίδουν συναλλαγές σε ένα **p2p** δίκτυο.
- Νέες συναλλαγές αποθηκεύονται σε ένα **mempool**: ένα αρχείο με ανεπιβεβαίωτες συναλλαγές.

Οι Miner διαλέγουν συναλλαγές από το mempool & τσεκάρουν ότι:

- Ο αποστολέας δεν κάνει **double-spend**: the inputs are all unspent
- Όλα τα input των συναλλαγών είναι υπογεγραμμένα από τον **ιδιοκτήτη** της συναλλαγής
- Σχηματίζουν ένα block από συναλλαγές

Μετά ξοδεύουν μεγάλη υπολογιστική ισχύ για να λύσουν ένα δύσκολο αλλά χαζό μαθηματικό πρόβλημα χρησιμοποιώντας brute computational force ->**proof – of – work**

Proof – of – work (1/2):

Οι Miner ανταγωνίζονται (δοκιμάζοντας το ένα νούμερο μετά το άλλο) με σκοπό να βρουν έναν αριθμό έτσι ώστε το hash(hash(επικεφαλίδας του block)) να ξεκινάει με Χ μηδενικά.

Τώρα το Χ είναι 19. Προσαρμόζεται κάθε 2 εβδομάδες έτσι ώστε να χρειάζονται ~10' για να επιβεβαιώσεις ένα νέο block

Το hash μπορεί να ξεκινήσει με οποιοδήποτε γράμμα μεταξύ Α και Ζ και οποιουδήποτε αριθμού μεταξύ 0 και 9. Έτσι, υπάρχουν 36 χαρακτήρες. Η πιθανότητα να βρεθεί ένα hash ξεκινώντας με 19 μηδενικά είναι (1/36) στη δύναμη των 19!

Εάν ο miner βρει τον σωστό αριθμό, το block του μεταδίδεται, οι άλλοι miner πρέπει να ξαναρχίσουν ξανά από το μηδέν!

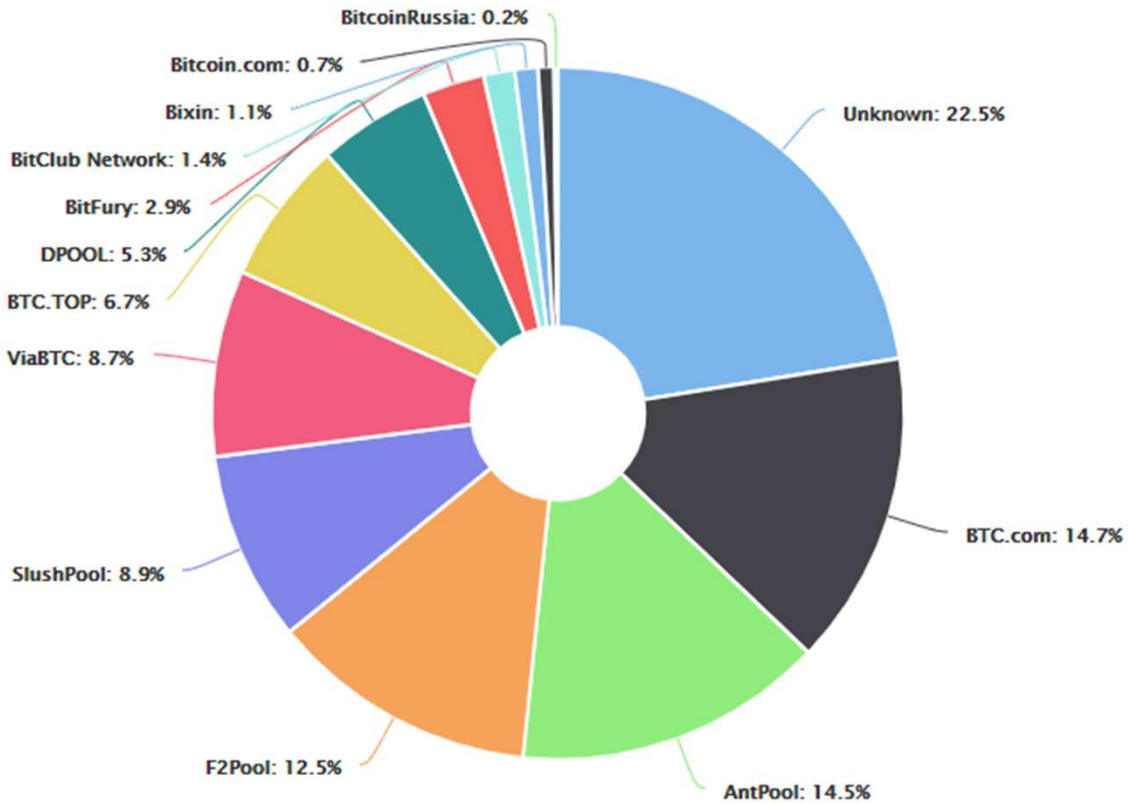
Η παρουσία σε κάθε block του hash του προηγούμενου block υποδηλώνει ότι τα block στο blockchain αλληλοσυνδέονται μεταξύ τους σαν κομμάτια σε μια αλυσίδα.

The above needs extreme amounts of energy consumption, right now the equivalent of Denmark, for a mere 94mil trx/yr. When 1 payment company (Worldpay) will have cleared ~40bil txs in 2018

Υπολογιστική ισχύς στο δίκτυο του Bitcoin (9.488 κόμβοι,15/4/2019)

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2408 (25.38%)
2	Germany	1923 (20.27%)
3	France	606 (6.39%)
4	Netherlands	497 (5.24%)
5	Canada	338 (3.56%)
6	Singapore	303 (3.19%)
7	United Kingdom	298 (3.14%)
8	n/a	286 (3.01%)
9	China	273 (2.88%)
10	Russian Federation	256 (2.70%)

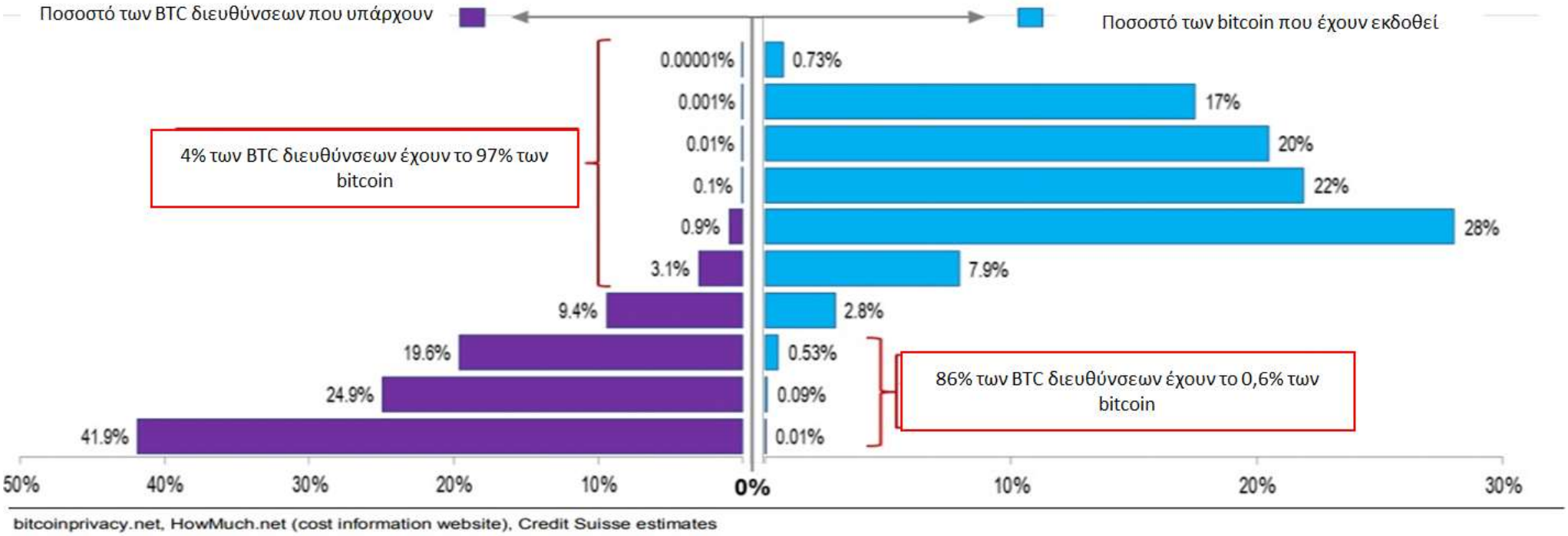


Η Ελλάδα έχει 24 κόμβους…35η
από 96 χώρες

Proof – of – work (2/2):

Το μέγεθος της ανταμοιβής καθορίζεται από τον αλγόριθμο (νομισματική πολιτική ενσωματωμένη στον αλγόριθμο!).

- Αρχικά ήταν 50 bitcoin, τώρα είναι στα **12,5=$81K**! (+τα έξοδα επεξεργασίας συναλλαγών)
- Διαιρείται με το 2 για κάθε **210.000 block**
- Θα είναι μηδέν τη χρονιά **2140** (should Bitcoin still exist).
- Συνολικό πλήθος νομισμάτων: **21 million** bitcoins



Τι συνδυάζει το Bitcoin Blockchain?

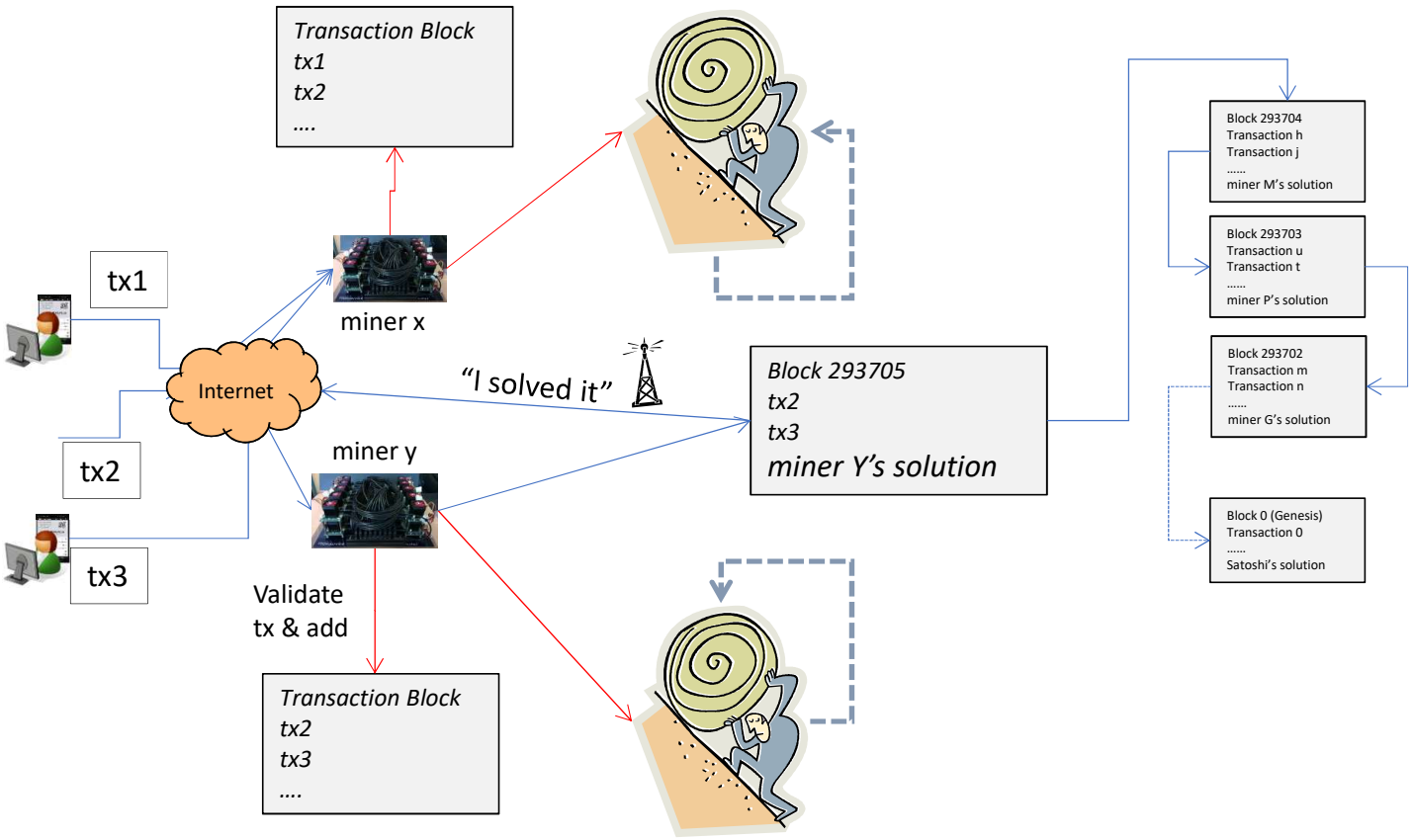
Κρυπτογραφία
Τα ιδιωτικά / δημόσια κλειδιά, οι ψηφιακές υπογραφές & οι hash functions εξασφαλίζουν την αυθεντικότητα των συναλλαγών
Blockchain
Μία βάση δεδομένων μόνο για προσάρτηση: τα προηγούμενα δεδομένα δεν μπορούν να τροποποιηθούν. Το blockchain έτσι είναι αμετάβλητο.
Proof-of-Work
Χρειάζεται χρόνος για την προσθήκη block, το πόσος χρόνος δίνεται από τη συνολική υπολογιστική ισχύ: η δυσκολία είναι μια συλλογική παράμετρος.
Κίνητρα
Οι miner ανταμείβονται (ουσιαστικά) και οι ανταμοιβές τους βρίσκονται στον αλγόριθμο του blockchain
Όλα αυτά τα στοιχεία μαζί μας δίνουν ένα αποκεντρωμένο, δημόσιο και permissionless ηλεκτρονικό σύστημα πληρωμών

Πώς δουλεύει λοιπόν το Bitcoin Blockchain?

Δημόσια/Ιδιωτικά κλειδιά

Συνάρτηση Κατακερματισμού

Κατανεμημένες Βάσεις Δεδομένων



Ευχαριστώ!