Εισαγωγή στο Blockchain

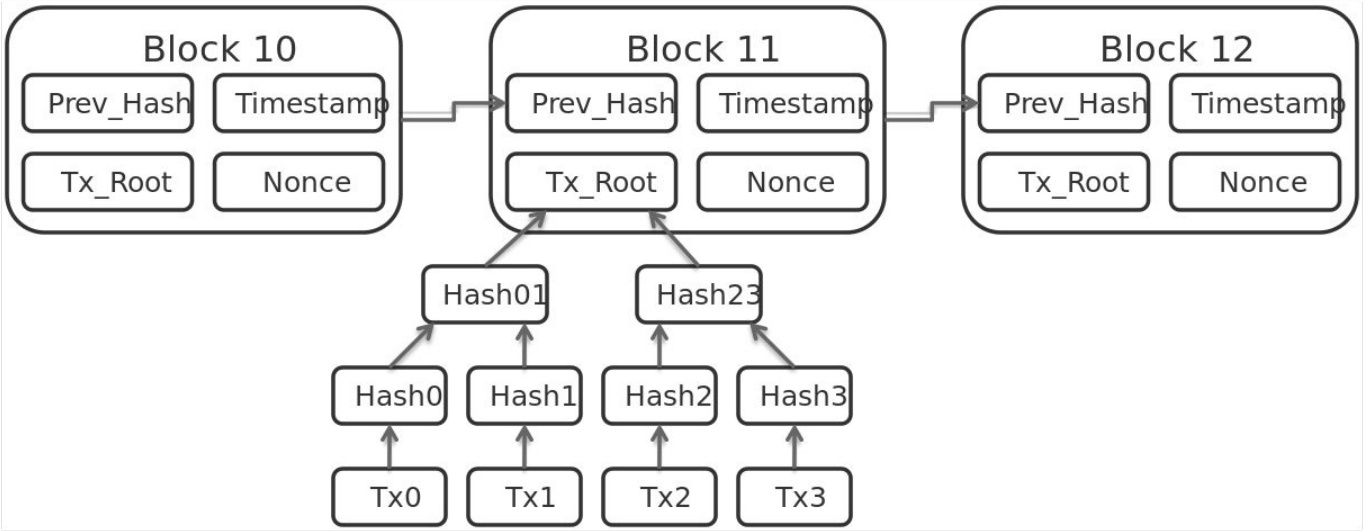
Γρηγόρης Βελέγκας

Τεχνολογία Λογισμικού, 2017-2018

Τι είναι το Blockchain;

“An open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way” - Harvard Business Review

- **Open:** Ο καθένας μπορεί να δει αυτά που είναι “γραμμένα” στο blockchain
- **Distributed:** Δεν υπάρχει κεντρική αρχή που το παράγει, η διαδικασία είναι κατανεμημένη
- **Ledger:** Ένα “log file” που καταγράφει συναλλαγές
- **Verifiable:** Δεν υπάρχει εμπιστοσύνη, ο καθένας μπορεί να ελέγξει και να επιβεβαιώσει την εγκυρότητα
- **Permanent:** Ό,τι γράφετε στο blockchain δεν αλλάζει (σχεδόν) ποτέ


Block 10
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 11
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 12
Prev_Hash
Timestamp
Tx_Root
Nonce
Hash01
Hash23
Hash0
Hash1
Hash2
Hash3
Tx0
Tx1
Tx2
Tx3

Πώς ξεκίνησαν όλα

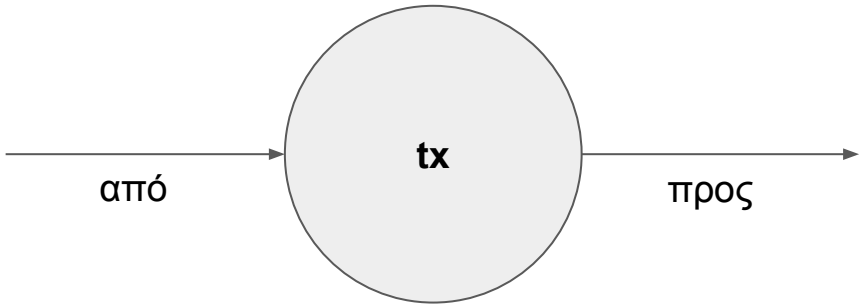
- **Double Spending:** Δεν υπήρχε κατανεμημένος και αποδοτικός τρόπος να καταλάβουμε αν κάποιος έχει ξοδέψει τα ίδια χρήματα δύο φόρες

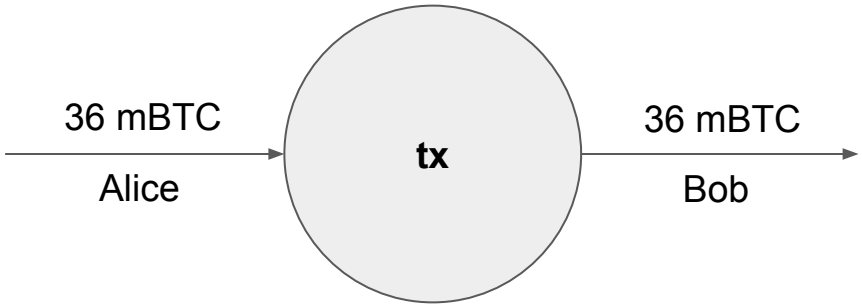
- **31/10/08:** Δημοσιεύεται το paper με τίτλο “Bitcoin: A Peer-to-Peer Electronic Cash System” από τον Satoshi Nakamoto που εισάγει το Blockchain στη cryptography mailing list του metzdowd.com

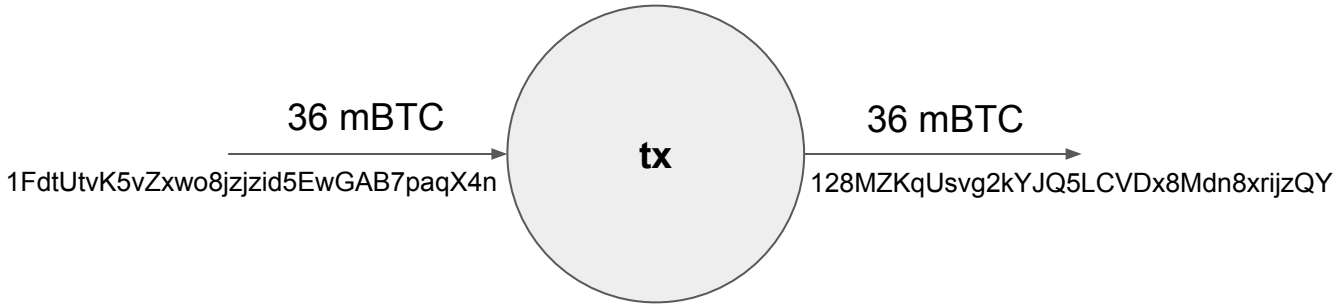
Ας δούμε πώς μοιάζουν οι συναλλαγές στο Bitcoin...

Συναλλαγές

- Η βασική δομή του bitcoin είναι η **συναλλαγή** (transaction - tx)
- Μία συναλλαγή μεταφέρει χρήματα από έναν κάτοχο σε έναν άλλον

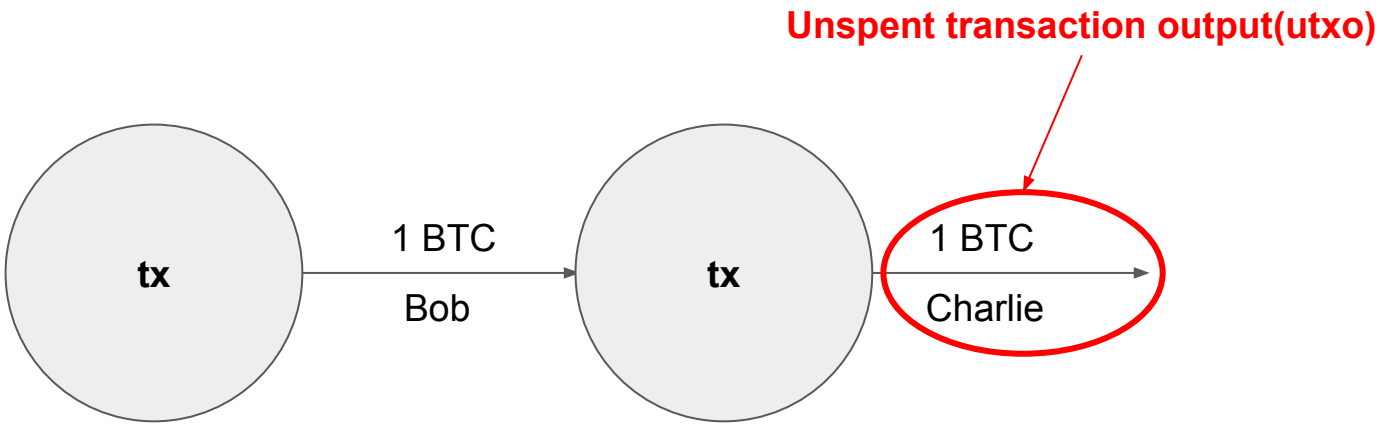


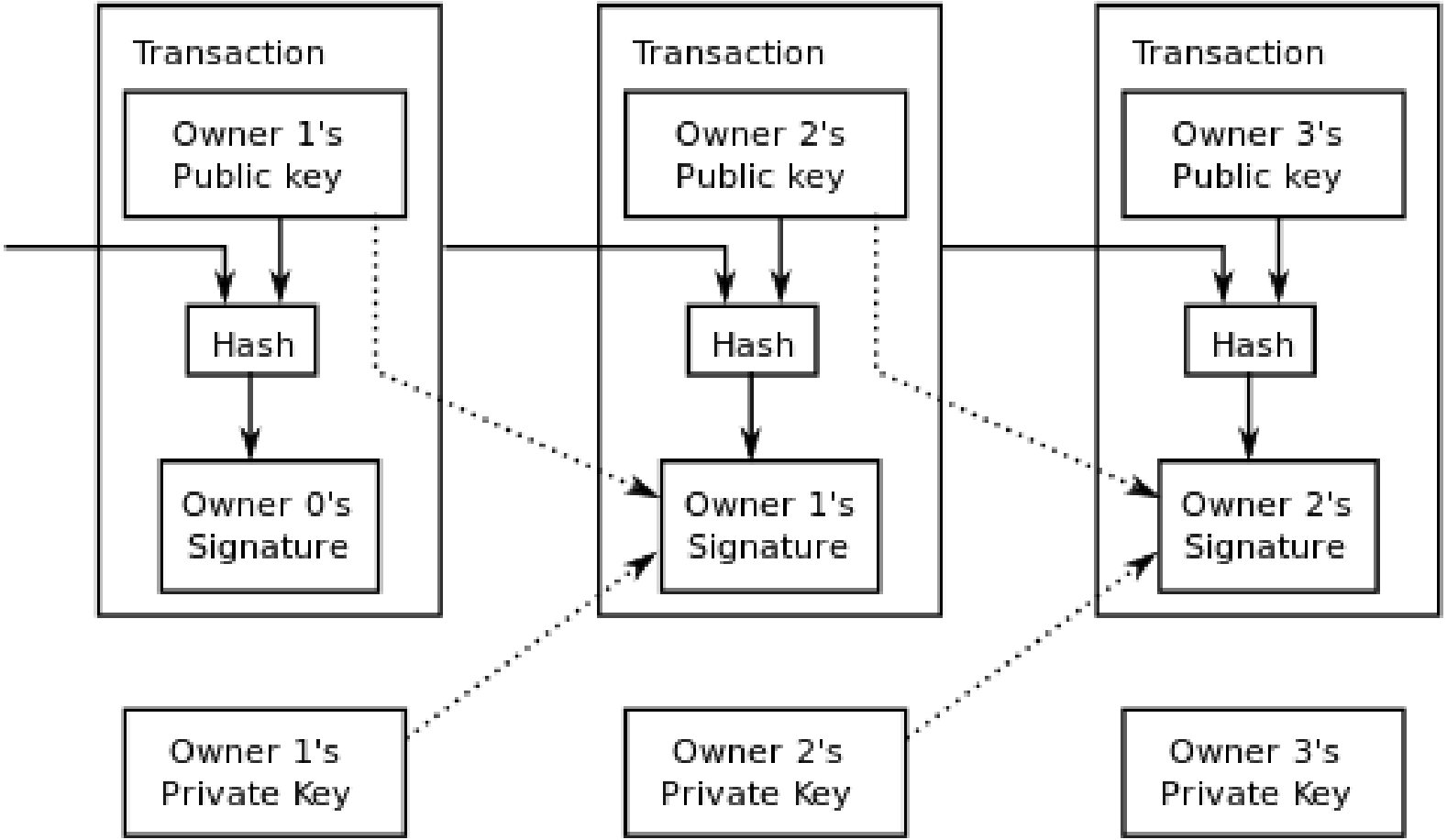

36 mBTC
Alice
tx
36 mBTC
Bob


36 mBTC
1FdtUtvK5vZxwo8jzjzid5EwGAB7paqX4n
tx
36 mBTC
128MZKqUsvg2kYJQ5LCVDx8Mdn8xrijzQY

Ο γράφος συναλλαγών

- Οι πληρωμές γίνονται **συνδέοντας** κόμβους συναλλαγών
- Το χρήμα είναι μία **αλυσίδα συναλλαγών**



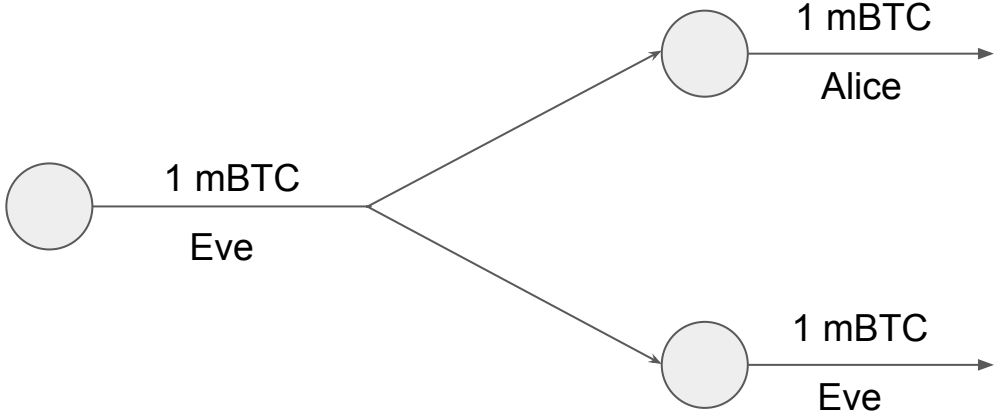

Transaction
Owner 1's Public key
Hash
Owner 0's Signature
Transaction
Owner 2's Public key
Hash
Owner 1's Signature
Transaction
Owner 3's Public key
Hash
Owner 2's Signature
Owner 1's Private Key
Owner 2's Private Key
Owner 3's Private Key

Double spending

- Τι θα γίνει αν ξοδέψω **το ίδιο UTXO** δύο φορές;
- Η συναλλαγή δεν θα είναι έγκυρη
- Η **πρώτη** συναλλαγή θα είναι έγκυρη
- Η **δεύτερη** συναλλαγή δεν θα είναι έγκυρη
- Αν είχαμε έναν κεντρικό server, αυτό θα ήταν εύκολο…
- Τότε απλώς διατηρούμε ένα σίγουρα έγκυρο UTXO
- Στο p2p δίκτυο του bitcoin μπορεί να καθυστερήσουμε να μάθουμε για κάποια συναλλαγή…
- Μπορεί η Alice να “βλέπει” διαφορετική σειρά συναλλαγών από τον Bob

Double spending attack

- Η Eve αγοράζει έναν καφέ από την Alice
- Ταυτόχρονα κάνει double spend προς τον εαυτό της
- Παίρνει τον καφέ και φεύγει
- Η Alice μαθαίνει για το double spend αργότερα

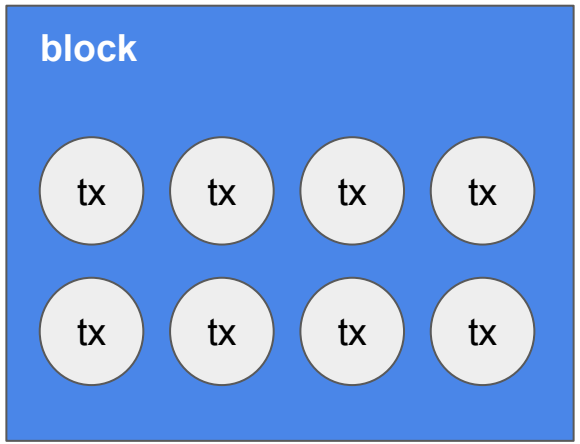


Το βέλος του χρόνου

- Θέλουμε να βάλουμε τις συναλλαγές σε μία σειρά
- Πρέπει να μπορούμε να απαντήσουμε στην ερώτηση: Η συναλλαγή Α έγινε πριν την συναλλαγή Β;
- Η απάντηση πρέπει να είναι **κοινή για όλους στο δίκτυο**
- Η συμφωνία σε μία κοινή αλήθεια όσο αφορά την ακολουθία συναλλαγών ονομάζεται **consensus**

Block

- Συλλέγει πολλά transactions
- Δεν περιέχει double spends, δηλαδή tx που ξοδεύουν το ίδιο output
- Κάθε transaction μπορεί να περιλαμβάνεται **μία φορά** σε ένα block

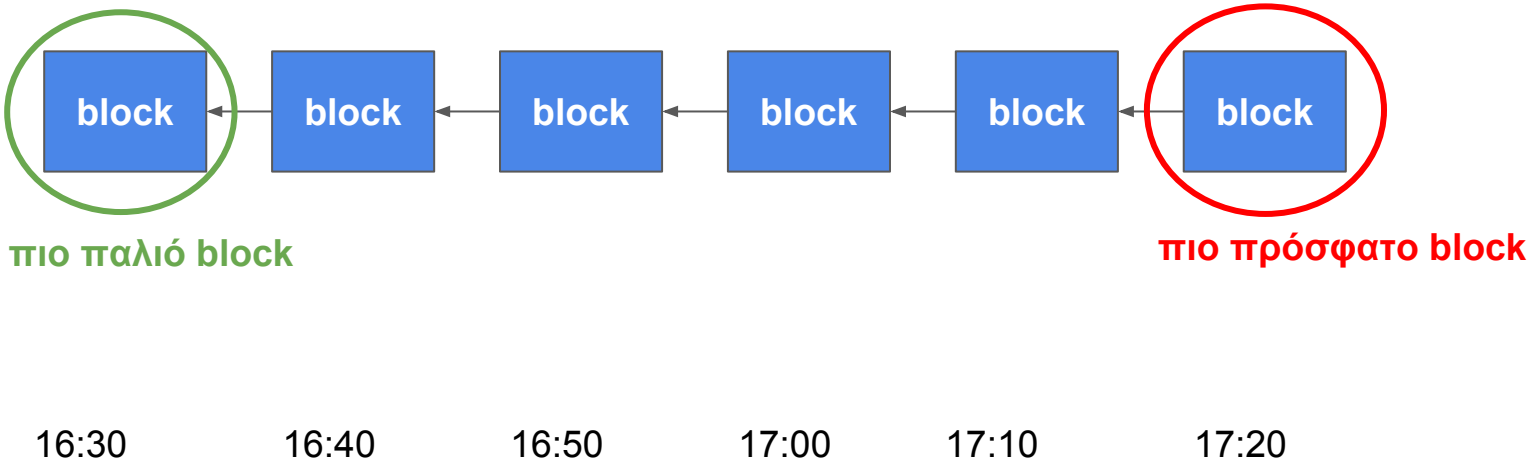


Block

- Το δίκτυο φροντίζει να δημιουργείται καθολικά **ένα block κάθε 10 λεπτά**
- Το block που δημιουργείται κάθε 10 λεπτά περιλαμβάνει τις **πιο πρόσφατες συναλλαγές** που **δεν υπήρχαν** σε προηγούμενα blocks
- Τα blocks γίνονται **broadcast** και **relay** στο δίκτυο όπως οι συναλλαγές
- Το SHA256 των δεδομένων του block είναι το **block id**
- Μία συναλλαγή που περιλαμβάνεται σε έγκυρο block λέγεται **confirmed**

Blockchain

- Κάθε block αναφέρεται στο **προηγούμενο** block
- Περιλαμβάνει ένα δείκτη στο blockid του πατέρα του
- Επόμενο block δεν μπορεί να περιέχει double spend προηγούμενου
- Αυτή η συνδεδεμένη λίστα ονομάζεται **blockchain**



Blockchain

- Επιτυγχάνει **consensus**
- Η συναλλαγή Α **προηγείται** της συναλλαγής Β αν η Α **περιλαμβάνεται σε προηγούμενο block** από την Β
- Αν θέλουμε να σιγουρευτούμε ότι δεν θα γίνει double spend, πρέπει να περιμένουμε το transaction να γίνει confirm

Ποιος παράγει τα blocks?

- **Καθένας** μπορεί να παράξει ένα block
- Το σύστημα είναι ελεύθερο στον οποιονδήποτε
- Κάθε block πρέπει να περιέχει μία **απόδειξη εργασίας SHA256**[2]
- Η απόδειξη εργασίας έχει **δυσκολία** που είναι τέτοια ώστε το **συνολικό δίκτυο** του bitcoin να παράγει **1 block ανά 10 λεπτά σε αναμενόμενη τιμή**

E(block generation time) = 10 min

Εξόρυξη

- Η διαδικασία της παραγωγής blocks ονομάζεται **εξόρυξη** (mining)
- Υπάρχουν πολλοί bitcoin **miners** που επιχειρούν να εξορύξουν blocks
- Κάθε miner έχει μία **μικρή πιθανότητα** να εξορύξει ένα δεδομένο block
- Όταν ένας miner εξορύξει επιτυχώς ένα block το κάνει **broadcast**
- Οι άλλοι miners το κάνουν **relay**

Αλγόριθμος miner

- Παρακολουθούμε το δίκτυο για **συναλλαγές** και **blocks**
- Περιλαμβάνουμε στο **υποψήφιο block** μας:
  - **Όλες τις συναλλαγές** που δεν έχουν εμφανιστεί σε προηγούμενο block που γνωρίζουμε
  - Μία αναφορά στο πιο πρόσφατο block που γνωρίζουμε ως **πατέρα**
- Αναζητούμε **απόδειξη εργασίας**
  - Η απόδειξη εργασίας γίνεται πάνω στον πατέρα και τις συναλλαγές **επιβεβαιώνοντάς** τα
- Αν βρούμε απόδειξη εργασίας κάνουμε **broadcast**
  - Διαφορετικά συνεχίζουμε έως ότου να βρούμε
- Αν μάθουμε ότι κάποιος άλλος miner βρήκε block, πετάμε την προηγούμενη δουλειά μας και συνεχίζουμε να κάνουμε mining πάνω στο πιο πρόσφατο block

Στόχος απόδειξης εργασίας

Απόδειξη εργασίας: **H(merkle root || nonce || block-parent-id) < ε**

P(ένα hash βρίσκει block) = ε / 2^{256}

- Το ε ονομάζεται **στόχος (target)**
- Το ε είναι κοινός στόχος για όλους τους miners
- Για να είναι **έγκυρο** ένα block **επιβεβαιώνεται** ότι η απόδειξη εργασίας του για το δεδομένο στόχο
- Τα κακόβουλα blocks με μικρότερη απόδειξη εργασίας δεν γίνονται δεκτά από το δίκτυο

Προσαρμογή στόχου απόδειξης εργασίας

- $\varepsilon_{genesis} = 2^{256 - 32}$
- Ο στόχος ε δεν είναι σταθερός αλλά **προσαρμόζεται**
- **Με αυτό τον τρόπο το δίκτυο πετυχαίνει αναμενόμενο block mining χρόνο 10 λεπτά**
- Το ε αλλάζει κάθε 2016 blocks (αναμενόμενες 2 εβδομάδες)
- Επανυπολογίζεται έτσι ώστε αν τα προηγούμενα 2016 είχαν φτιαχτεί με το νέο **ε**, τότε να έπαιρναν ακριβώς 2 εβδομάδες

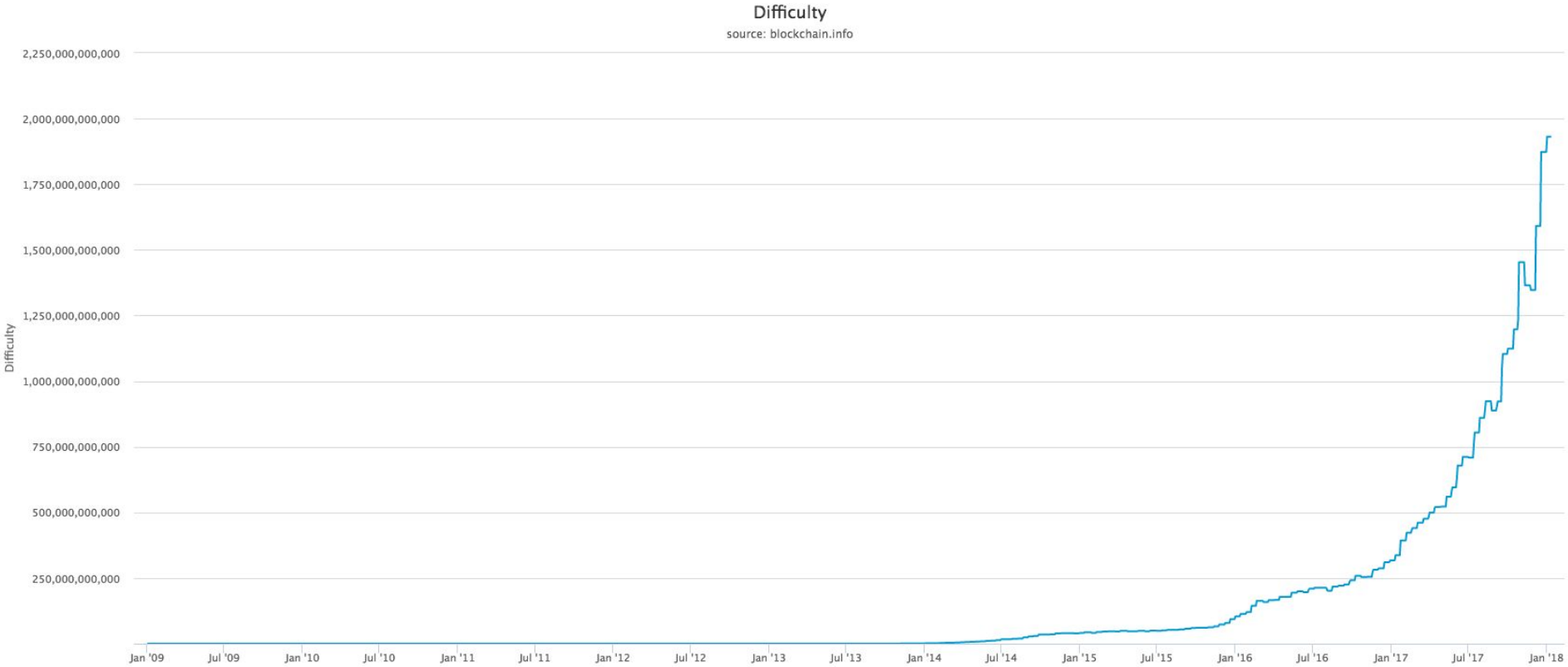
$$\epsilon' = \epsilon \frac{ts(block_n) - ts(block_{n-2016})}{2 \text{ weeks}}$$

Δυσκολία

- Ο αντίστροφος στόχος ονομάζεται **δυσκολία (difficulty)**

$$\textbf{difficulty} = \varepsilon_{\textbf{genesis}} / \varepsilon$$

$$\textbf{difficulty}_{\textbf{genesis}} = 1$$


Difficulty
source: blockchain.info
2,250,000,000,000
2,000,000,000,000
1,750,000,000,000
1,500,000,000,000
1,250,000,000,000
1,000,000,000,000
750,000,000,000
500,000,000,000
250,000,000,000
Difficulty
Jan '09
Jul '09
Jan '10
Jul '10
Jan '11
Jul '11
Jan '12
Jul '12
Jan '13
Jul '13
Jan '14
Jul '14
Jan '15
Jul '15
Jan '16
Jul '16
Jan '17
Jul '17
Jan '18

Hashcash

H(merkle root || nonce || parent-blockid) < ε

```
def generate(challenge, size):
    answer = ''.join(random.choice(string.ascii_lowercase +
                                   string.ascii_uppercase + string.digits) for x in range(size))
    attempt = challenge + answer
    return attempt, answer


sha = hashlib.sha256()


def test(st, size):
    f = False
    start = time.time()
    i = 0
    while f == False:
        i += 1
        attempt, answer = generate(st, size)
        sha.update(attempt)
        solution = sha.hexdigest()
        if solution.startswith('00000'):
            timeTook = time.time() - start
            print timeTook
            print solution
            print i / timeTook
            f = True
    print answer
```

Κίνητρα mining

- Ένας miner ανταμοίβεται με 2 τρόπους:

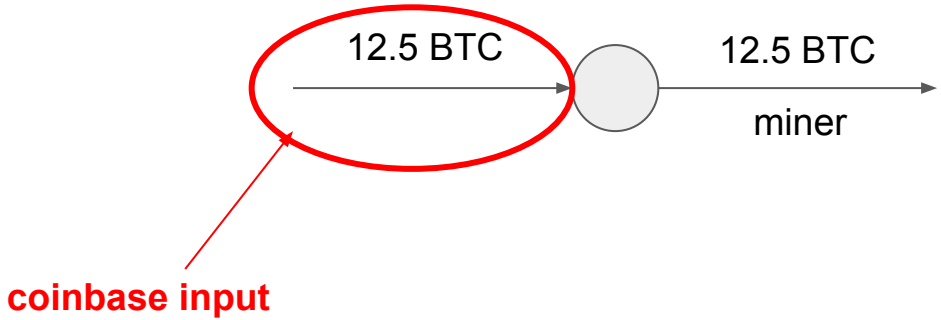
1. Με όλα τα περισσευούμενα χρήματα στις συναλλαγές που κάνει confirm:

$$fees = \sum_{tx \in block} \left(\sum_{i \in in(tx)} w(i) - \sum_{o \in out(tx)} w(o) \right)$$

Κίνητρα mining

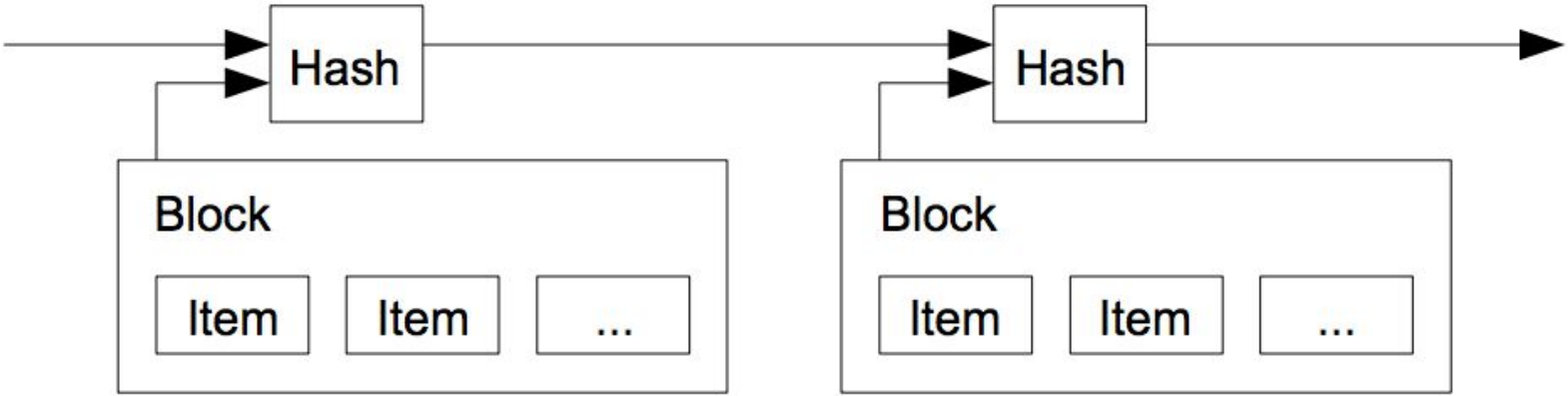
- Ένας miner ανταμοίβεται με 2 τρόπους:

2. Με **ένα** coinbase transaction που επιτρέπεται να βάλει στο block αξίας 12.5 BTC (σήμερα)



Εγκυρότητα ενός block

- Για να επιβεβαιώσουμε την εγκυρότητα ενός block:
- **Επαγωγικά** γνωρίζουμε **κάποιο ήδη έγκυρο** block
- Επιβεβαιώνουμε ότι το νέο block έχει **πατέρα** το έγκυρο block που γνωρίζουμε
- Επιβεβαιώνουμε την **απόδειξη εργασίας**
- Επιβεβαιώνουμε ότι οι συναλλαγές που περιέχει είναι έγκυρες


Hash
Hash
Block
Item
Item
...
Block
Item
Item
...

Genesis block

- Το **πρώτο** block του blockchain είναι το genesis block
- Είναι **hard-coded** στο bitcoin software
- Κάθε έγκυρο blockchain ξεκινάει από το genesis – είναι η **βάση** της επαγωγής στην επιβεβαίωση εγκυρότητας blocks

genesis block

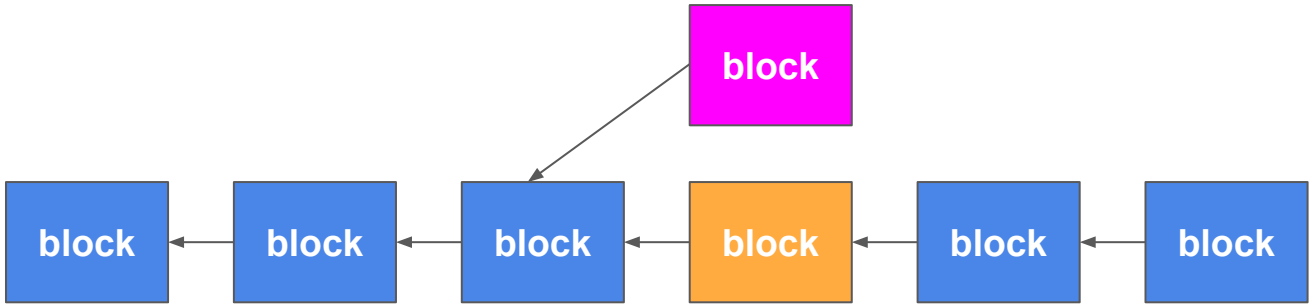
Genesis block

- Περιλαμβάνει το κείμενο “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”
- Αυτό αποδεικνύει ότι το block φτιάχτηκε **μετά** τις 3 Ιανουαρίου 2009
- Ξέρουμε επίσης ότι φτιάχτηκε **πριν** τις 3 Ιανουαρίου 2009 επειδή το παρατηρήσαμε στο δίκτυο
- Συνεπώς φτιάχτηκε **στις** 3 Ιανουαρίου 2009
- Η απόσταση ενός block από το genesis ονομάζεται **ύψος (height)**
- Το **block height του genesis** είναι **0**


THE TIMES
£1.50
Eat Out from £5
More than 900 great restaurants, including four Gordon Ramsay favourites from £15
Israel prepares to send tanks and troops into Gaza
Chancellor on brink of second bailout for banks
99p
Michael Sheen
Frost, Nixon and me
Working mums
So that's how she does it
Detox in style
The best spas on the planet
Salman Rushdie
I won't marry again
Giant killing?
Guide to the FA Cup third round

Blockchain forks

- Κάποιες φορές μπορεί να γίνουν mine 2 έγκυρα blocks “ταυτόχρονα”
- Αυτό δημιουργεί ένα **blockchain fork**



Blockchain fork

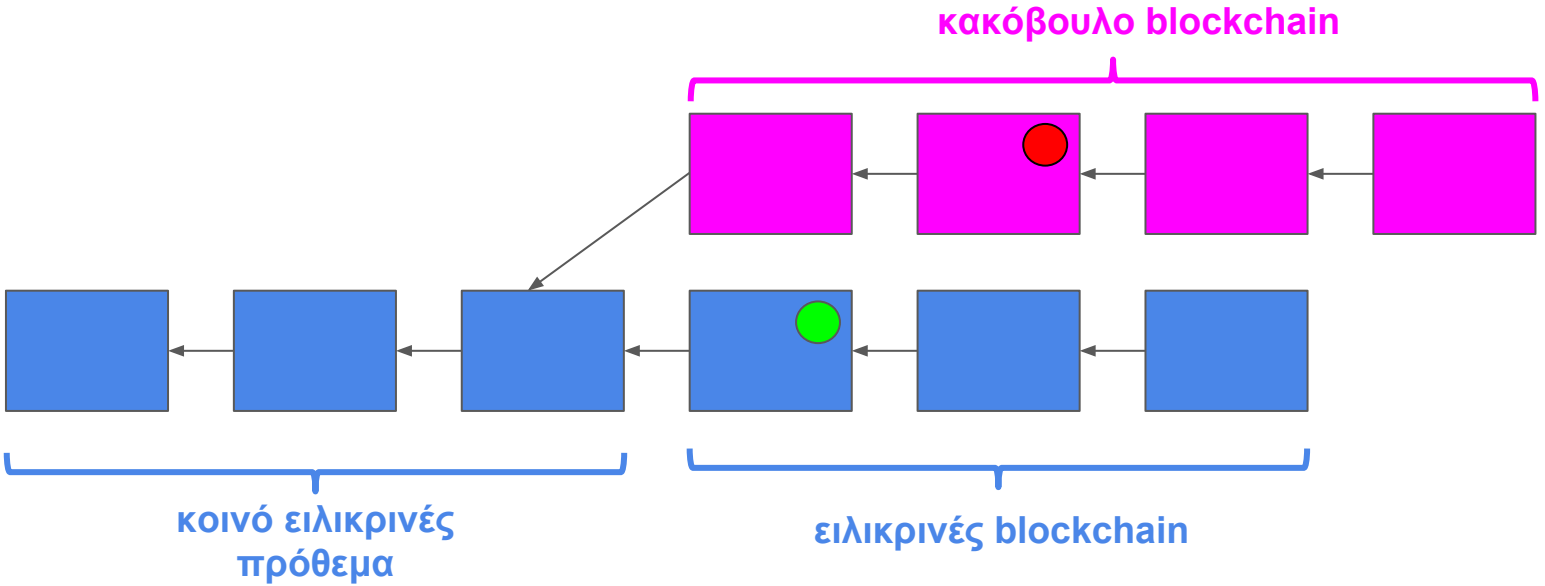
- Το blockchain fork είναι πρόβλημα διότι δεν μας επιτρέπει πια να έχουμε βέλος του χρόνου
- Επιστρέφουμε στο ίδιο πρόβλημα που είχαμε με τις συναλλαγές
- Ποιο από τα δύο blocks είναι **το πιο πρόσφατο έγκυρο block**?
- Τι γίνεται αν τα δύο αντίπαλα blocks περιλαμβάνουν **double spends**?

Αλγόριθμος επίλυσης αντίπαλων blockchains

- Παρατηρούμε δύο αντίπαλα blockchains στο δίκτυο
- Το έγκυρο blockchain είναι το blockchain με **το μέγιστο ύψος**
- Αν δύο αντίπαλα blockchains έχουν το ίδιο ύψος, τότε επιλέγουμε κάποιο **αυθαίρετα**
- Το block που επιλέγουμε ως miners είναι αυτό πάνω στο οποίο κάνουμε εξόρυξη
- Το block που επιλέγουμε ως χρήστες είναι αυτό που εμπιστευόμαστε για transaction confirmation

Double spending

- Για να κάνω double spend πρέπει να παράξω ένα κακόβουλο **παράλληλο blockchain** μεγαλύτερο ή ίσο με το ειλικρινές



Δυσκολία του double spending

- Το double spending απαιτεί μεγάλη υπολογιστική δύναμη
- Ο κακόβουλος θα πρέπει να κατέχει μεγαλύτερη υπολογιστική δύναμη από το υπόλοιπο δίκτυο
- Διαφορετικά η πιθανότητα να μπορεί να συνεχίζει να επεκτείνει το blockchain μειώνεται **εκθετικά** όσο το ειλικρινές blockchain μεγαλώνει
- Μπορεί όμως να το πετύχει αν ελέγχει το 51% της δύναμης CPU του κόσμου
- Αυτό ονομάζεται **51%-attack**

Τι μπορεί να πετύχει ένας κακός miner;

- Μπορεί να κάνει double spending;
  - ?
- Μπορεί να απαγορεύσει χρήματα από το να ξοδευτούν;
  - ?
- Μπορεί να ξοδέψει τα δικά μας χρήματα;
  - ?

Τι μπορεί να πετύχει ένας κακός miner;

- Μπορεί να κάνει double spending;
  - Ναι – φτιάχνει ένα παράλληλο blockchain που περιλαμβάνει την συναλλαγή
- Μπορεί να απαγορεύσει χρήματα από το να ξοδευτούν;
  - Ναι – φτιάχνει ένα παράλληλο blockchain που δεν περιλαμβάνει την συναλλαγή
- Μπορεί να ξοδέψει τα δικά μας χρήματα;
  - Όχι – δεν έχει τα ιδιωτικά κλειδιά μας!

DECENTRALIZE ALL THE THINGS!