



Διονύσης Ζήνδρος
Εθνικό Μετσόβιο Πολυτεχνείο 2012

Τι είναι το bitcoin?

- Ψηφιακό νόμισμα
- Για αληθινές online αγορές
- Αντικαταστάτης (?) του € και του \$





Ιστορία

- **Wei Dai, 1998:** “[Bmoney](#)”
(cypherpunks)
- **Satoshi Nakamoto, 2009:**
”[Bitcoin: A Peer-to-Peer Electronic Cash System](#)”
- 2009: bitcoind **open source** σε C++

Πρόβλημα: Online πληρωμές

- Απαιτείται έμπιστη αρχή
- Πληρωμές με **πιστωτικές κάρτες**
- **π.χ. Visa, MasterCard**
- Έ υπηρεσιών π.χ. **PayPal κ.ό.κ.**
- **Δεν υπάρχει ανωνυμία**
- **Κόστος** για τη χρήση των υπηρεσιών
- Δεν υποστηρίζονται πολύ μικρά ποσά

Πρόβλημα

- Χρυσός έχει αντικειμενική αξία
- Είναι δύσχρηστος
- **Αργές πληρωμές**
- Δύσκολη μεταφορά
- Κλοπές



Πρόβλημα

- € και \$ ελέγχονται **κεντρικά**
- Κεντρική τράπεζα τυπώνει χρήματα
- Βλέπε Federal Reserve Bank (ιδιωτική εταιρία)
- **Κεντρικά ελεγχόμενος πληθωρισμός**

Παράδειγμα:

- Υπάρχουν 100€ σε κυκλοφορία
- Έχεις 1€ στην κατοχή σου
- Τυπώνονται άλλα 100€
- Το 1€ έχει πλέον τη μισή αξία

Πόση εμπιστοσύνη έχουμε ότι θα γίνει σωστά;

Λύση

- Πειραματικό ψηφιακό νόμισμα **bitcoin**
- **Peer-to-peer** δίκτυο

Πλεονεκτήματα

- **Γρήγορες** πληρωμές (< 10')
- **Απουσία** κεντρικής αρχής
- Η αξία του νομίσματος προκύπτει από την **ελεύθερη αγορά**
- **Ασφάλεια** συναλλαγών
- **Ανωνυμία**

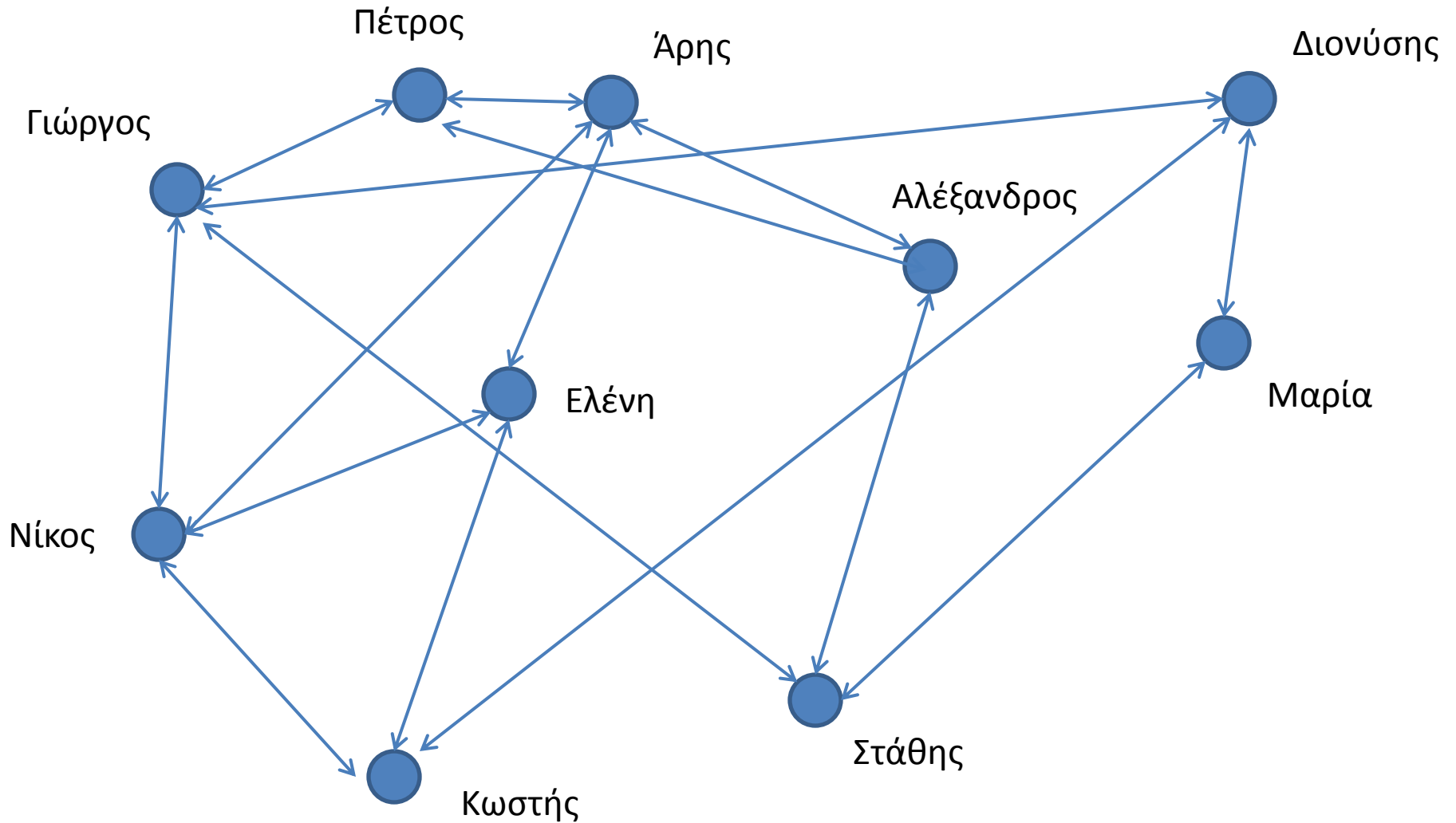
Ιδέα!

- Σύγχρονα νομίσματα \$ και €
- Είναι **εικονικά** - δεν έχουν **πραγματική** αξία
- Μπορεί να είναι **οποιοδήποτε αντικείμενο**
- Αρκεί να μην αντιγράφεται αυθαίρετα
- Συμφωνούμε: Το τάδε **χαρτί** είναι **νόμισμα**

Γιατί να στηριζόμαστε σε κεντρικές αρχές;

...και όχι στην κρυπτογραφία;

Peer-to-peer δίκτυο bitcoin



Πιστοποίηση

- Κάθε κόμβος έχει ένα δημόσιο/ιδιωτικό κλειδί
- Αυτό εγγυάται ότι **όποιος έχει** τα χρήματα, **αυτός πληρώνει**
- **Δημόσιο κλειδί** γίνεται **broadcast** στο δίκτυο
- **Ιδιωτικό κλειδί** μένει στον κόμβο

Έχει 12BTC

$m \leftarrow$ “Στέλνω 12BTC στην Alice”

$h \leftarrow H(m)$

$s \leftarrow \text{sign}_{S_B}(h)$

Έχει 0BTC

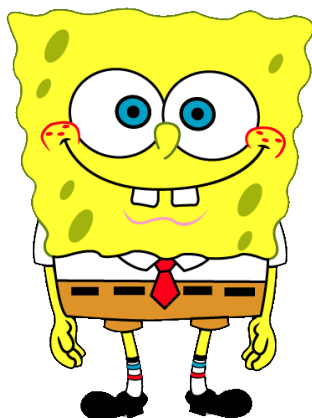
s



Έχει 0BTC

$\text{verify}_{P_B}(h)$
Έχει 12BTC

Bob



Alice



Εγκυρότητα

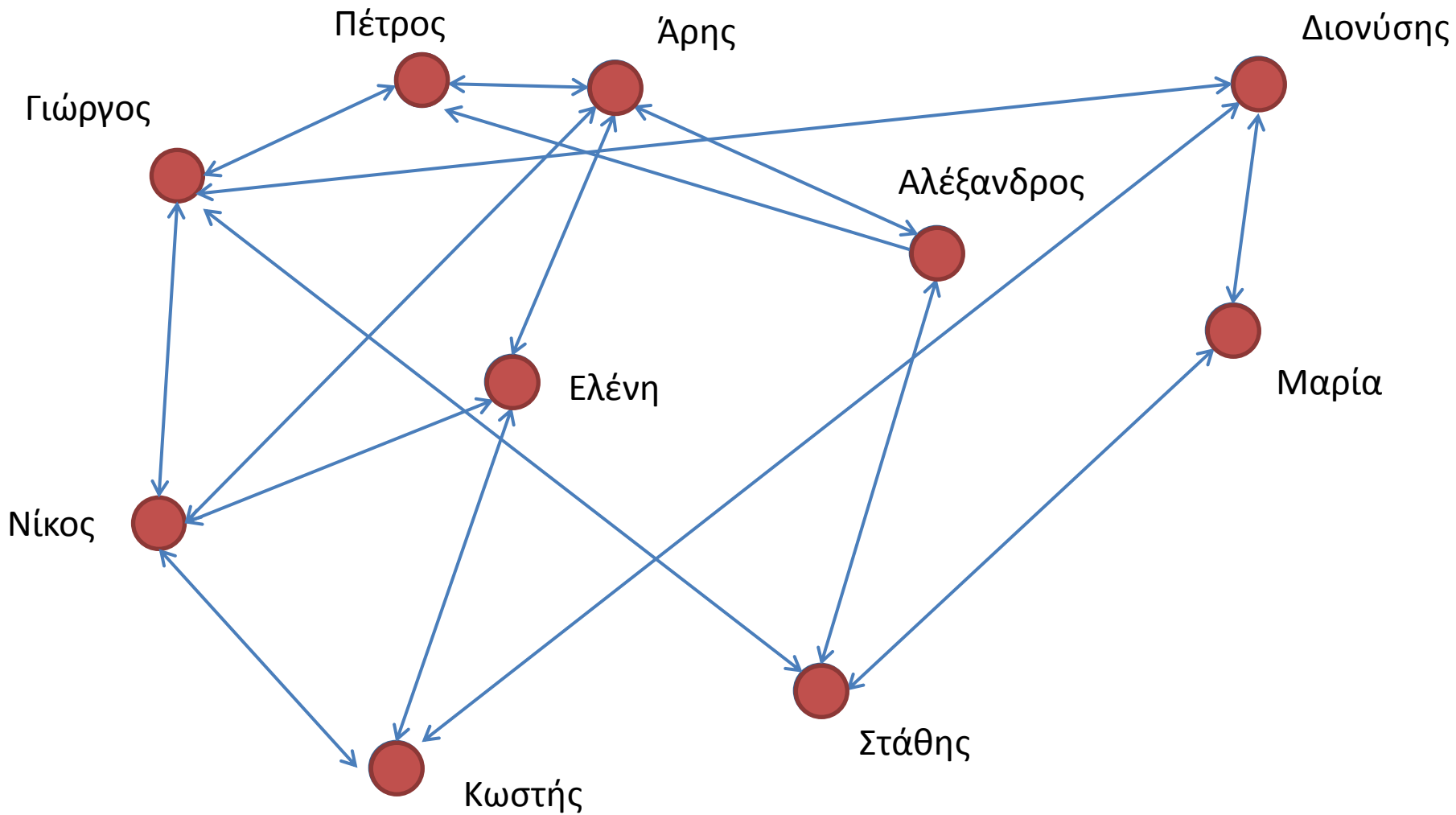
- Πώς ξέρουμε ότι το νόμισμα προήλθε από **έγκυρη πηγή** και δεν είναι **αυτοδημιούργητο**;

Ποιος έχει τι

- Το δίκτυο αποθηκεύει **συλλογικά** ποιος έχει πόσα χρήματα
- **Όλοι** ξέρουν πόσα χρήματα έχει ο Bob
- **Όλοι** ξέρουν πόσα χρήματα έχει η Alice
- Συνεπώς ο Bob δεν μπορεί να στείλει χρήματα που δεν έχει
- Για να **δώσω** χρήματα πρέπει να τα έχω **πάρει**

Broadcasting

- Κάθε συναλλαγή **δημοσιεύεται** στο δίκτυο
- Όταν στέλνω ή λαμβάνω χρήματα, το λέω στους κόμβους που είμαι συνδεδεμένος

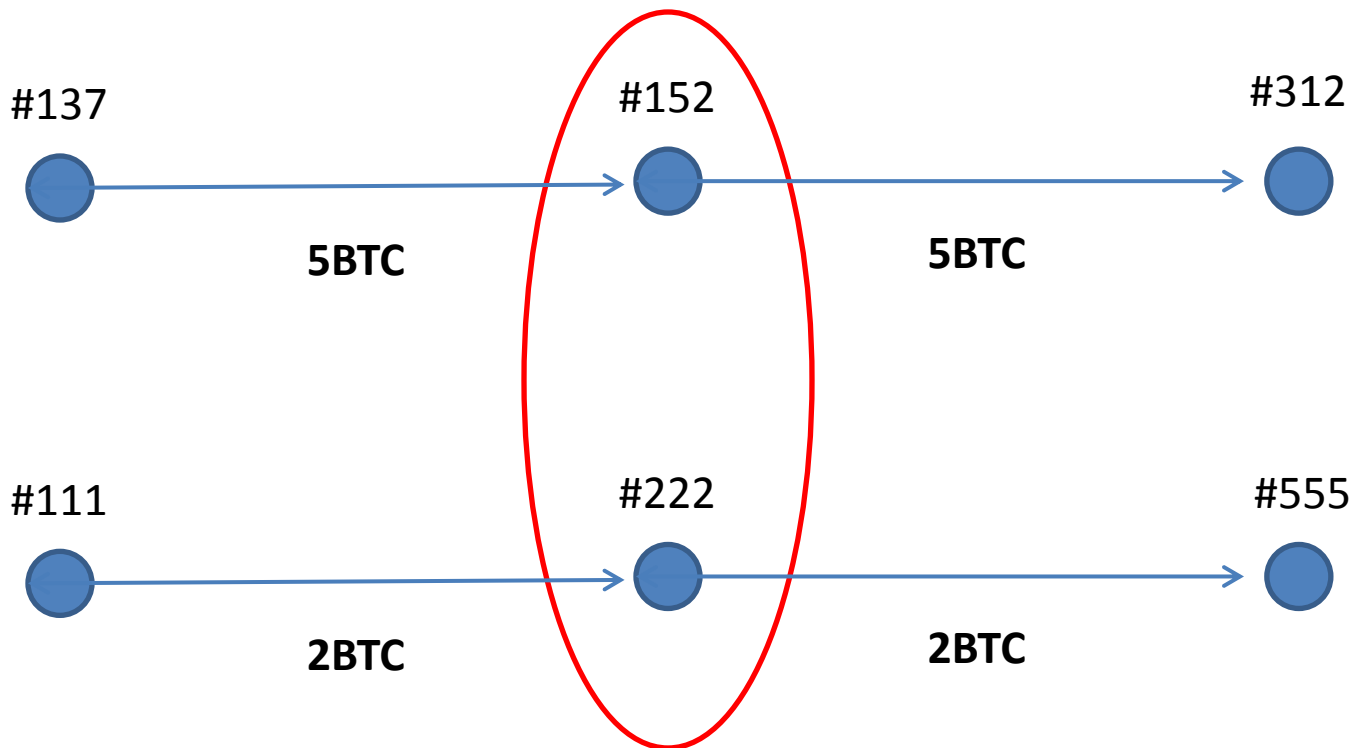


Ανωνυμία

- Για **κάθε συναλλαγή** οι συμμετέχοντες χρησιμοποιούν ένα **νέο ιδιωτικό κλειδί**
- Οι κόμβοι **δεν έχουν ονόματα** – μόνο κλειδιά



Ανωνυμία



Είναι άραγε ο ίδιος άνθρωπος;

Χρησιμοποιεί το κλειδί
με το οποίο **πήρε** τα χρήματα
PB, SB

$m1 \leftarrow \text{"12BTC προς PA"}$
 $h1 \leftarrow H(m1)$



$s1 \leftarrow \text{sign}_{SB}(h1)$



$s2 \leftarrow \text{sign}_{SA}(h2)$



Δημιουργεί ένα **νέο** κλειδί
Γι' αυτή τη συναλλαγή
PC, SC

$\text{ver}_{PA}(s2)$

Δημιουργεί ένα **νέο** κλειδί
Γι' αυτή τη συναλλαγή
PA, SA

$\text{ver}_{PB}(s1)$

$m2 \leftarrow \text{"12BTC προς PC"}$
 $h2 \leftarrow H(m2)$

Νόμισμα



- (ουδ.) το μέγεθος εκείνο βάσει του οποίου υπολογίζονται ή εκφράζονται οικονομικές αξίες.



- (ουδ.) μία **αλυσίδα ψηφιακών υπογραφών.**

Νόμισμα = Αλυσίδα υπογραφών

...

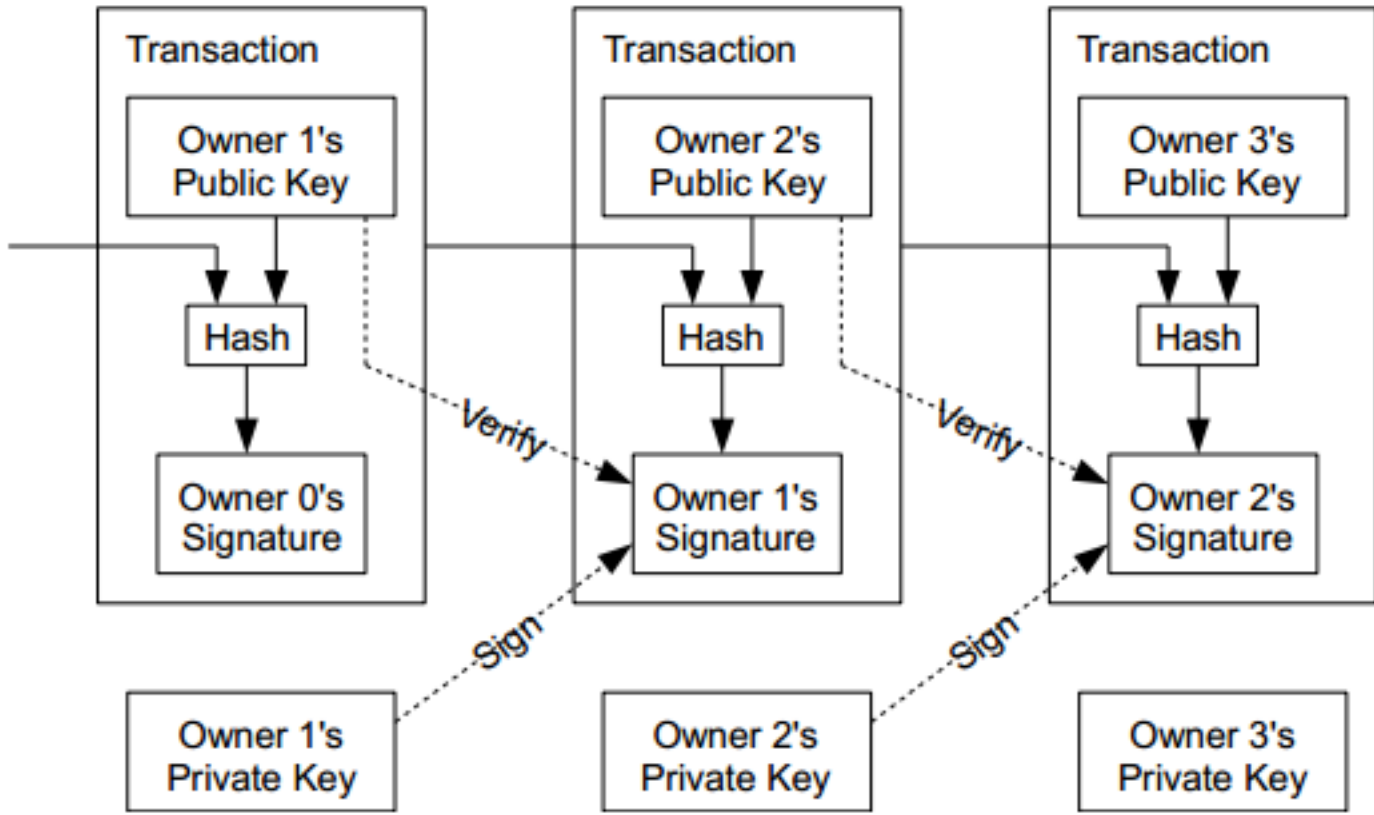
$\text{coin1} \leftarrow \text{sign}_{s_0} (H(\text{coin0} || P1))$

$\text{coin2} \leftarrow \text{sign}_{s_1} (H(\text{coin1} || P2))$

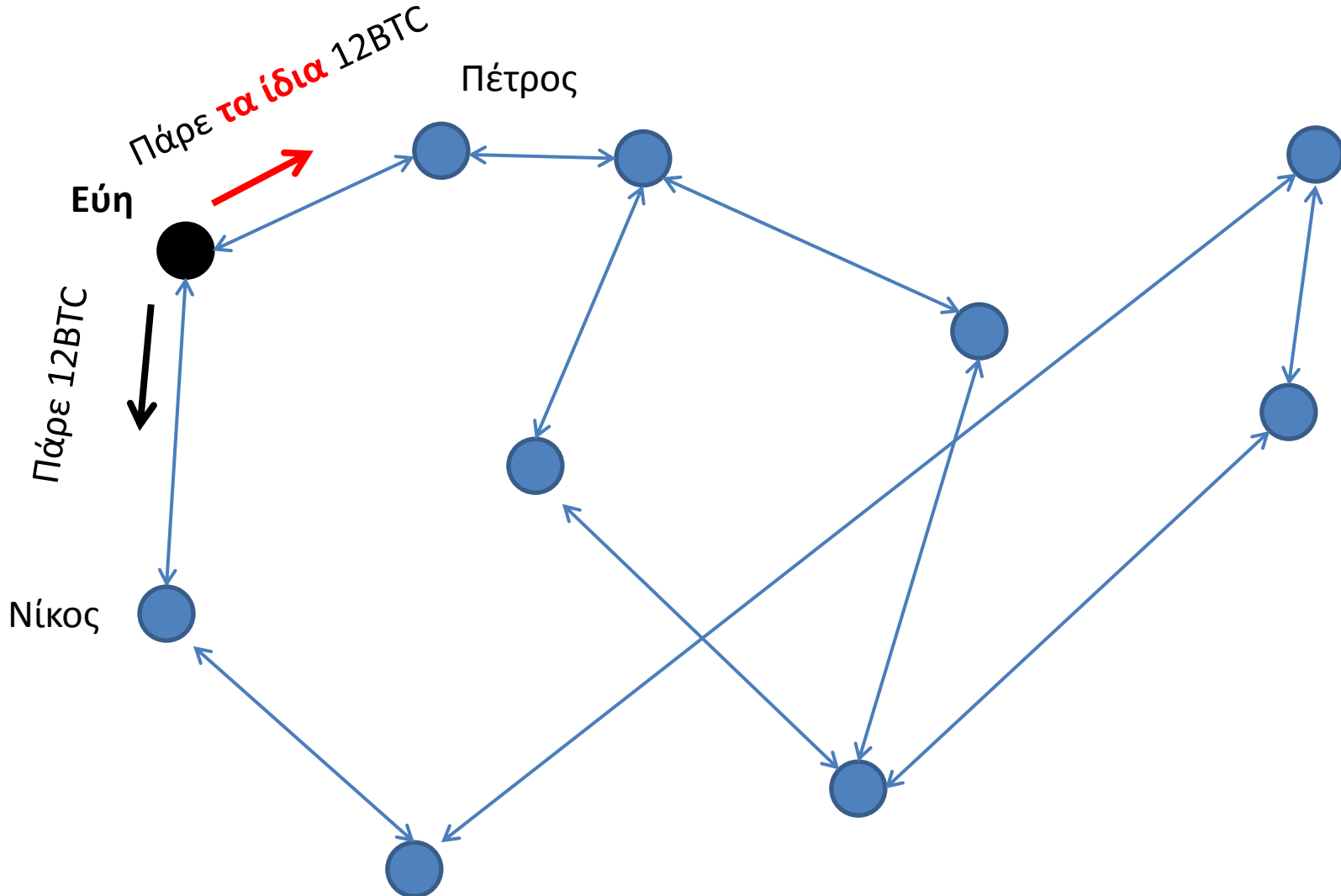
$\text{coin3} \leftarrow \text{sign}_{s_2} (H(\text{coin2} || P3))$

...





Διπλοξοδεύω



Διπλό ξόδεμα

- Ανεπιθύμητο
- Πώς μπορεί να αποτραπεί;

Έγκυρες συναλλαγές

=

Συναλλαγές που **δεν** έχουν γίνει \geq **δύο** φορές;

Αυτό μου επιτρέπει να ακυρώσω μία συναλλαγή που δεν θέλω!

Το βέλος του χρόνου

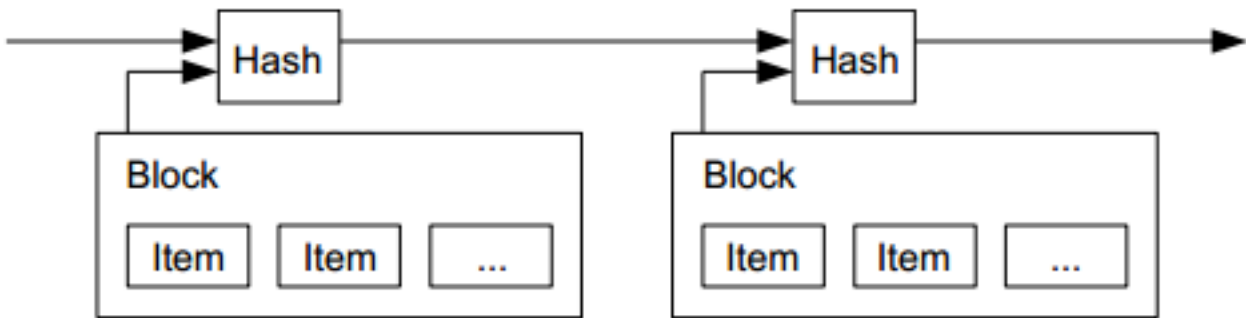
- **Έγκυρη** είναι η **πρώτη** συναλλαγή που έγινε από αυτό τον κρίκο της αλυσίδας
- **Μετέπειτα** συναλλαγές είναι **άκυρες**

Το βέλος του χρόνου

- **Πότε** έγινε μία συναλλαγή;
- Δεν μπορώ να στηριχθώ στην υπογραφή
- Η ημερομηνία μπορεί να είναι ψεύτικη

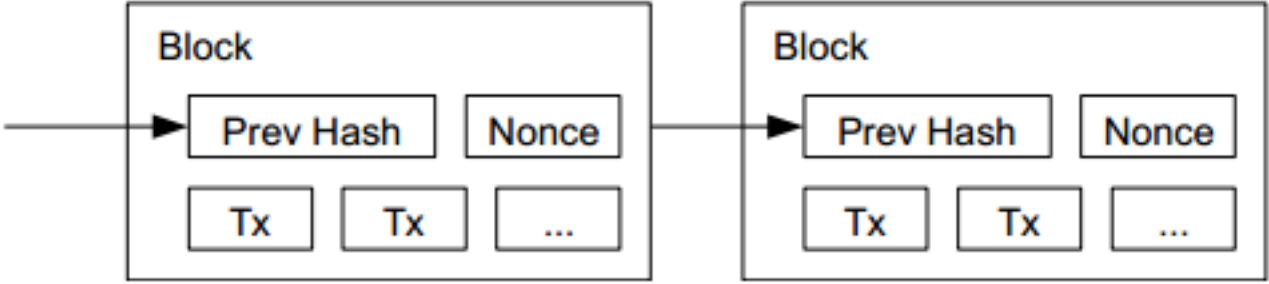
Blocks

- Οι πιο πρόσφατες συναλλαγές περιλαμβάνονται σε ένα **block**
- Υπολογίζουμε **το hash** κάθε block
- Κάθε νέο block περιέχει το **hash** του προηγούμενου
- Κάθε block δημοσιεύεται
- Κάθε επόμενο block είναι στο **μέλλον** σε σχέση με προηγούμενο
 - Αλλιώς **δεν θα μπορούσε** να ξέρει το hash του



Απόδειξη εργασίας

- Δεν μπορούμε να δημοσιεύσουμε τα blocks
 - Θα χρειαζόμασταν μια έμπιστη αρχή
- Τα blocks υπολογίζονται στα nodes και γίνονται broadcast
- Εισάγουμε μία **τεχνητή δυσκολία** δημιουργίας block
- Έτσι ένα block είναι **δύσκολο** να δημιουργηθεί

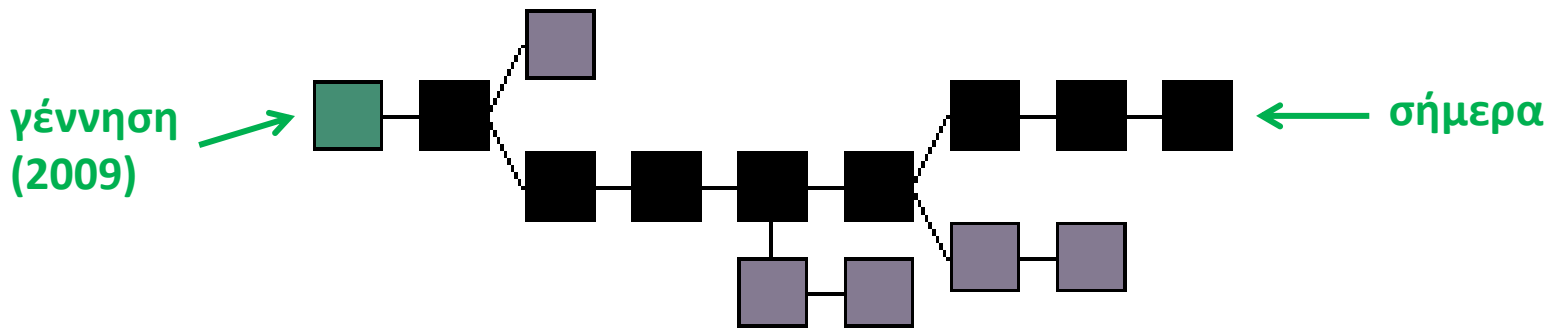


```
nonce ← 000000
while H( block || nonce ) ≠ "000000":
    nonce ← nonce + 1

broadcast( block )
```


Απόδειξη εργασίας

- Κάθε block **πιστοποιεί** τις συναλλαγές που περιέχει
- Δημιουργείται μία αλυσίδα από blocks
- Όλα τα έγκυρα blocks κληρονομούν από τη γέννηση



Απόδειξη εργασίας

- Όλοι οι κόμβοι προσπαθούν να βρουν το block
- Ο πρώτος κόμβος που θα το βρει το δημοσιεύει
- Το επόμενο block συνεχίζει από εκεί

Πιστοποίηση συναλλαγών

- Η συναλλαγή **πιστοποιείται** όταν μπει στο επόμενο block
- Γίνεται **εκθετικά δύσκολο** να δημιουργηθούν ψεύτικα blocks αργότερα
- Κάθε επόμενο block **διασφαλίζει** όλα τα προηγούμενα
- Αλλαγή σε κάποια συναλλαγή σημαίνει αλλαγή σε όλα τα επόμενα blocks

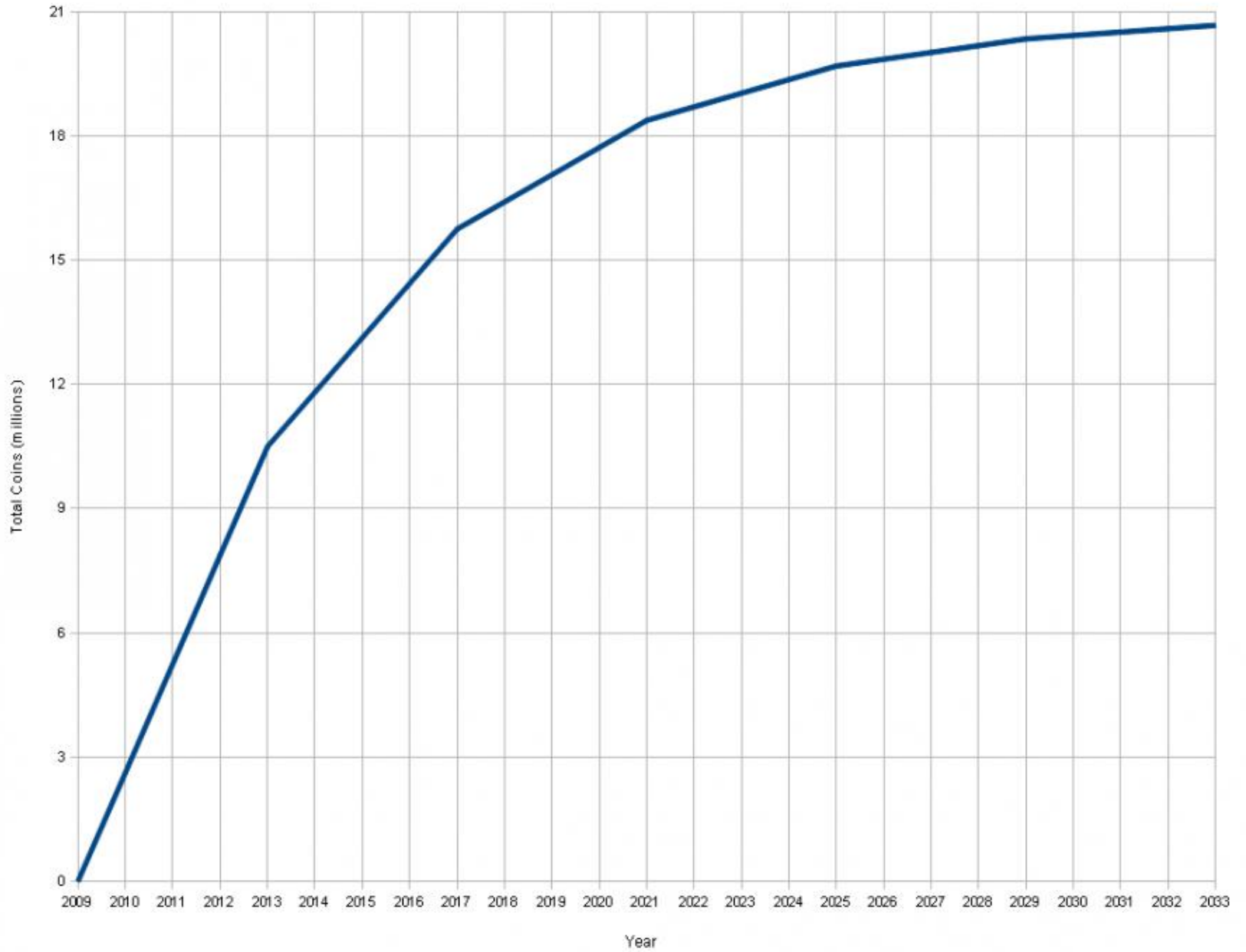
Πιστοποίηση συναλλαγών

- Κακόβουλος κόμβος χρειάζεται την πλειοψηφία της CPU του δικτύου για να παρέμβει
- Η παρέμβαση γίνεται **εκθετικά** δύσκολη όσο περνάει ο χρόνος μετά από μία συναλλαγή

Εξόρυξη bitcoin

- Δημιουργία block = Κέρδη σε bitcoin για το δημιουργό
- Ελεγχόμενος πληθωρισμός από το δίκτυο
- Σήμερα: 50BTC / block

Total Bitcoins over time




Τεχνικές λεπτομέρειες

- Ψηφιακές υπογραφές
 - Παραλλαγή σχήματος Elgamal (DSA)
 - Με χρήση ελλειπτικών καμπυλών
- Hash function
 - $\text{SHA256}(\text{SHA256}(_))$
- Συνάρτηση εργασίας
 - $\text{SHA256}(_)$

Το bitcoin σήμερα

17 Φεβρουαρίου 2012:

- 167,000 blocks
- 1BTC = 3.27€
- 8,354,750BTC σε κυκλοφορία
- **~27,000,000€ σε κυκλοφορία**
- Συχνότητα hashing δικτύου: > 9THz



Ευχαριστώ! Ερωτήσεις;

Αυτές οι διαφάνειες είναι:
Creative Commons 3.0 Attribution



bitcoin.org
Twitter: @dionyziz