

# TOR, OTR & BITCOIN

---

Π. Αγγελάτος, Δ. Ζήνδρος

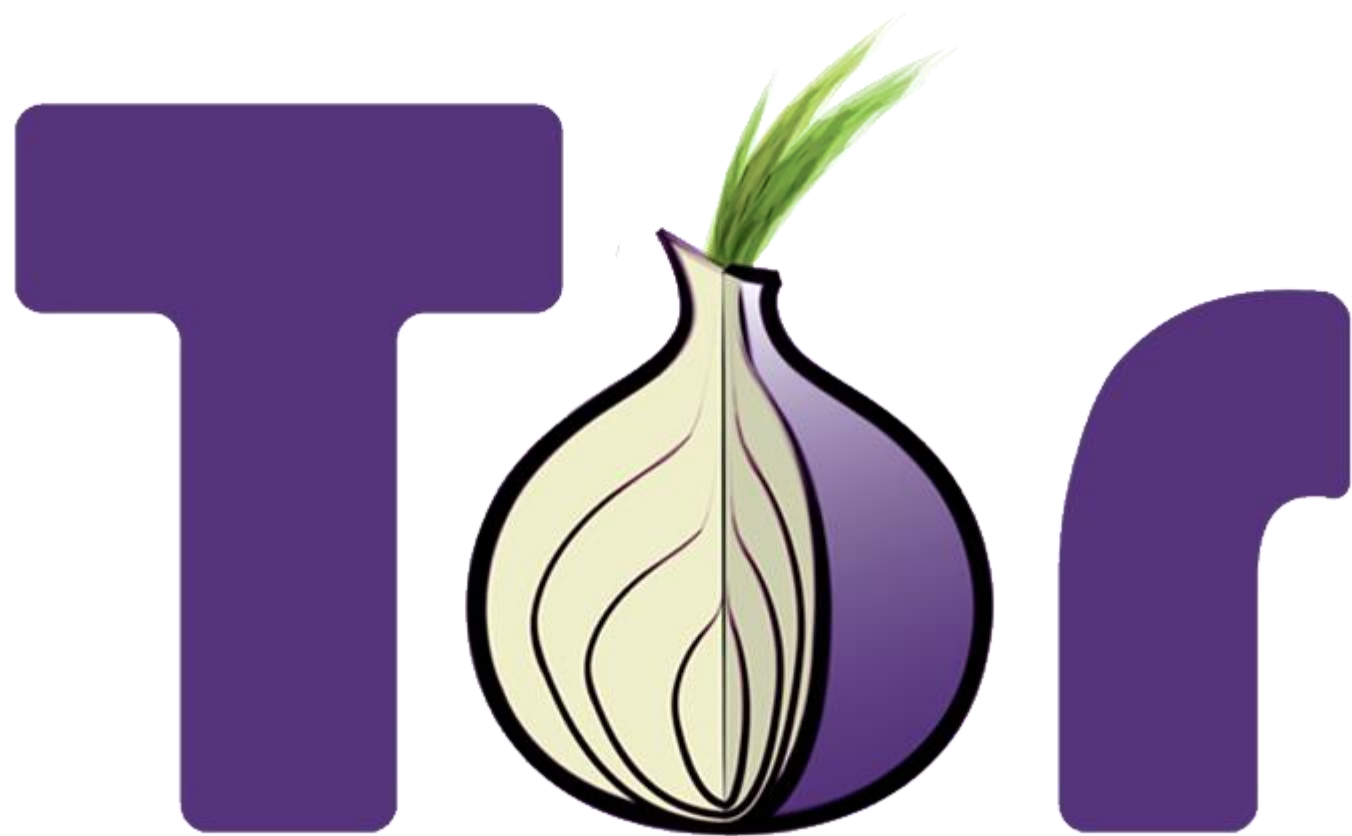


# Στόχος της ώρας

- Ανώνυμο browsing με Tor
- Onion routing
- Ασφαλές chat με OTR
- Forward secrecy
- Deniability
- Το κρυπτονόμισμα bitcoin

# Όσο ξεκινάμε...

- Κατεβάστε το OTR για το σύστημά σας:
  - Αν έχετε Linux ή Windows, Pidgin & OTR:
    - <https://www.pidgin.im/>
    - <https://otr.cypherpunks.ca>
  - Αν έχετε Mac, Adium:
    - <https://adium.im/>
- Εγκαταστήστε τα



# Ας κατεβάσουμε το Tor

- <https://www.torproject.org/>

# Αποκάλυψη ταυτότητας

- Από το IP μπορεί να βρεθούν...
  - Η θέση μας στον πλανήτη
  - Ο παροχέας Internet που χρησιμοποιούμε
  - Το πραγματικό μας όνομα (με ένταλμα)
- Κάθε ιστοσελίδα που επισκεπτόμαστε βλέπει το IP
  - ...και ενδεχομένως το καταγράφει

# Demo αποκάλυψης IP

- <http://wtfismyip.com/>

# Tor

- Ένα σύστημα που μας επιτρέπει να είμαστε ανώνυμοι
- Το IP που φαίνεται είναι διαφορετικό από το πραγματικό



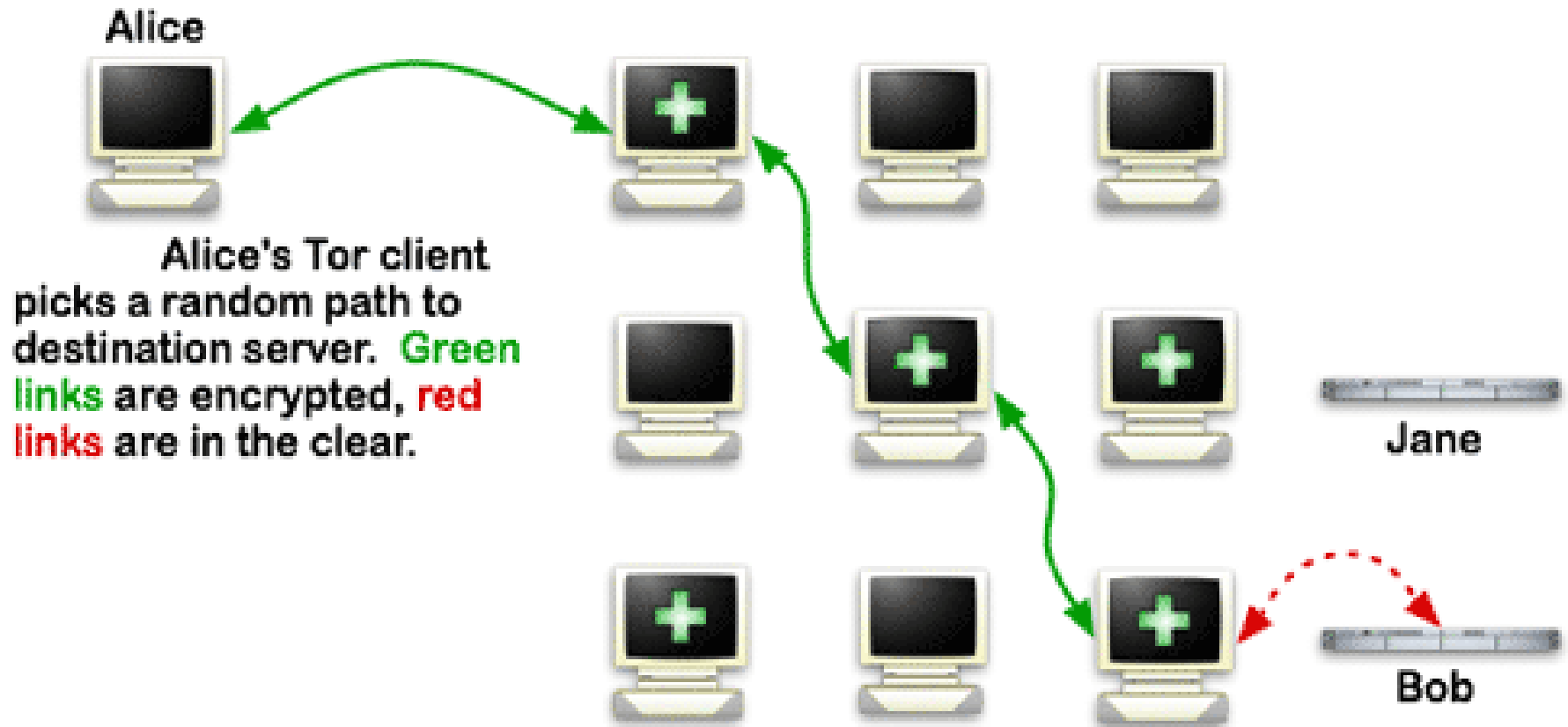
# Tor Browser Bundle

- Ακόμα και μέσω Tor ο browser μας μπορεί να ταυτοποιηθεί
  - <https://panopticklick.eff.org/>
  - Από τα διάφορα features που έχετε ενεργοποιημένα
    - Javascript, Flash, Java, Silverlight
    - Όνομα του browser
    - Λειτουργικό σύστημα
    - Εκδόσεις
- Γι' αυτό χρησιμοποιούμε το Tor Browser Bundle
  - Ίδιος browser για όλους
  - Εγκατεστημένο HTTPS everywhere
  - Απενεργοποιήστε την Javascript!

# Onion routing

- Εξασφαλίζει την ανωνυμία
- Ανάμεσα στον υπολογιστή μας και τον server υπάρχουν 3 tor nodes
- Κάθε node ξέρει μόνο για τους άμεσους γείτονές του
- Για κάθε σύνδεση, ο υπολογιστής μας διαλέγει τυχαία 3 άλλους υπολογιστές που τρέχουν το tor
- Τα δεδομένα περνούν από αυτούς

# How Tor Works



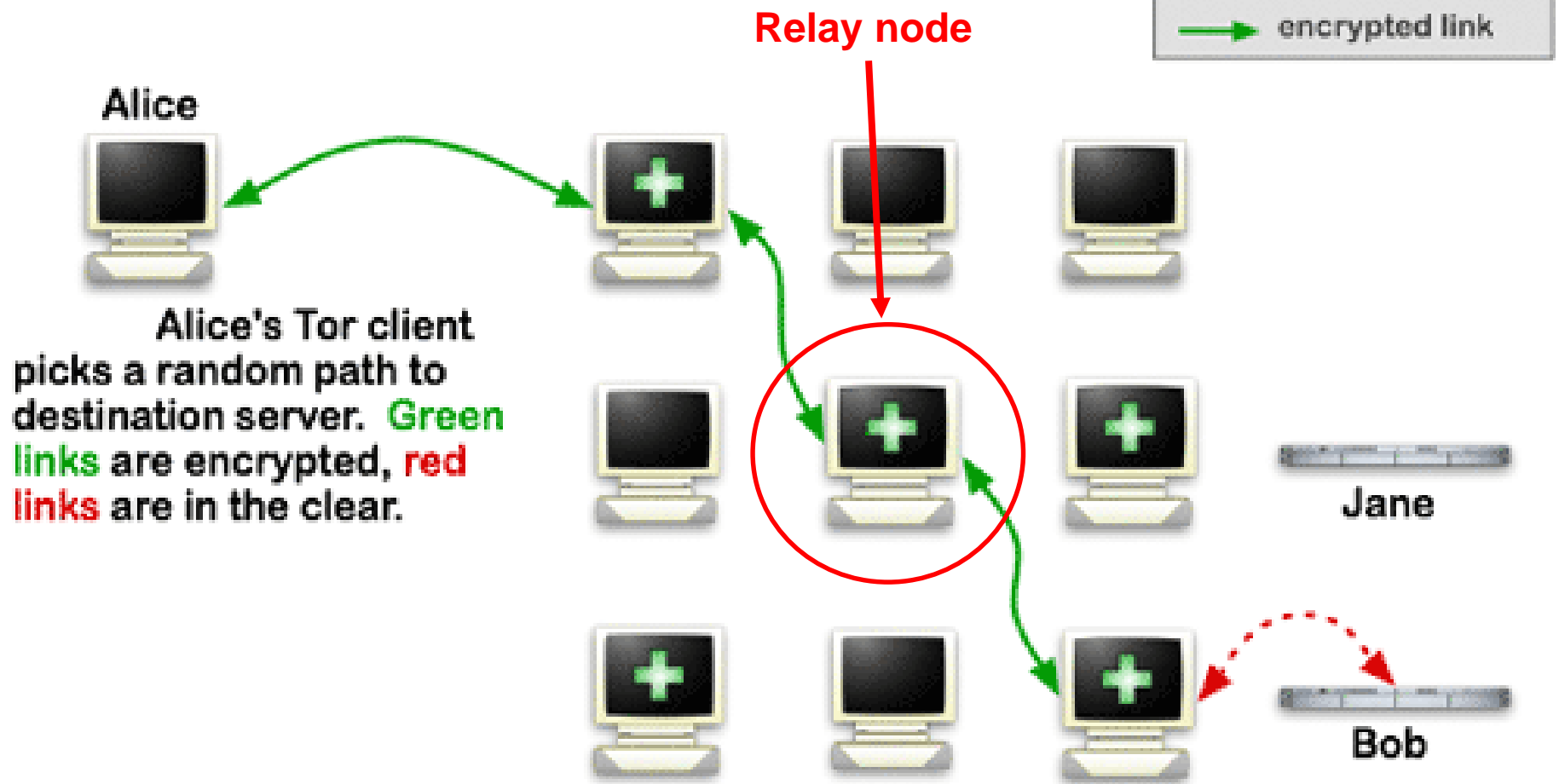
# Tor nodes

- Κάθε node έχει ένα public key
- Κάνουμε encrypt τα δεδομένα μας με το public key του καθενός από τα 3 nodes αλληπάλληλα

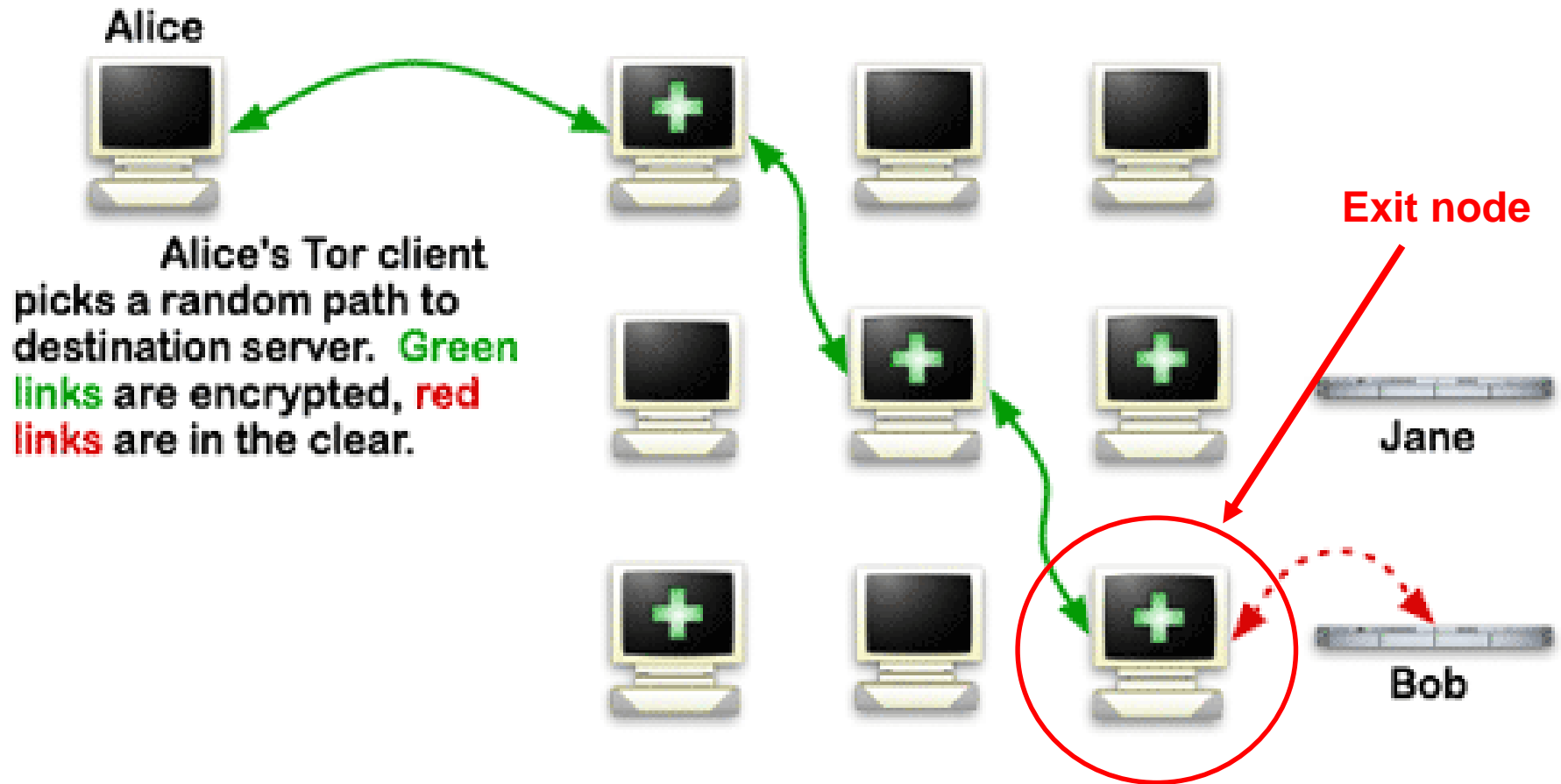
# Exit & Relay nodes

- Είναι τα nodes από τα οποία βγαίνουν τελικά τα δεδομένα
  - Μπορεί να δει/αλλάξει τα δεδομένα μας αν δεν χρησιμοποιούμε HTTPS
- Ένα node μπορεί να γίνει exit node εθελοντικά αν το επιθυμεί ο χρήστης
  - Απενεργοποιημένο by default
  - Ενδεχομένως να είστε νομικά υπεύθυνοι για το traffic που βγαίνει από τη σύνδεσή σας
- Ένα node μπορεί να γίνει relay node εθελοντικά
  - Παρακαλούμε να γίνετε
  - Δεν υπάρχει νομικό πρόβλημα

# How Tor Works



# How Tor Works



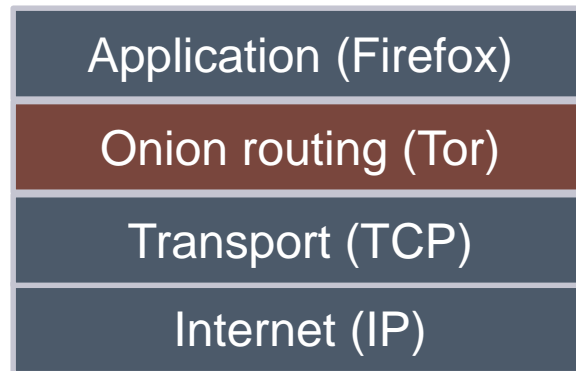
# Demo ανωνυμίας

- <http://wtfismyip.com> με Tor



# Tor: Όχι μόνο για browsing...

- Οποιαδήποτε υπηρεσία μπορεί να περάσει μέσω Tor
- Λειτουργεί ως SOCKS proxy



# Προσοχή!

- Πολλές εφαρμογές δεν δουλεύουν σωστά μέσω Tor
  - π.χ. Torrents
- Μερικές φορές το IP μας φαίνεται με τρόπους που δεν περιμένουμε
  - DNS leaks: Η εφαρμογή προσπαθεί να κάνει resolve ένα IP και στέλνει το DNS ερώτημα εκτός Tor
- Tails: Διανομή Linux που φροντίζει όλα να περνούν από Tor

[LONGFORM](#)[VIDEO](#)[REVIEWS](#)[TECH](#)[SCIENCE](#)[CULTURE](#)[DESIGN](#)[BUSINESS](#)[US & WORLD](#)[FORUMS](#)[COMMENTS](#)

# FBI agents tracked Harvard bomb threats despite Tor

By [Russell Brandom](#) on December 18, 2013 12:55 pm [Email](#) [@russellbrandom](#)

DON'T MISS STORIES *FOLLOW THE VERGE*



323k



386K followers



## HEADLINES



iTunes Festival comes to US for the first time at SXSW



HTC's 2014 One leaks out in first press image



A North Dakota town is the most expensive place to rent an apartment in the United States



UK court says nine-hour detention of Greenwald's partner was lawful



Lose yourself to dance with this 'Happy' and 'Get Lucky' mashup

**USES TOR**



**GETS ARRESTED**

# Hidden services

- Εκτός από τον client, κρύβεται και ο server
- Δεν είναι προσβάσιμα στο κανονικό Internet
  - Clearnet: Προσβάσιμα μέσω ενός κανονικού browser
  - Darknet ή Deep web: Πρόσβαση μόνο μέσω Tor
- 6 Tor relay hops
- Τα δεδομένα δεν βγαίνουν ποτέ από το Tor δίκτυο
- Αντίστοιχη διαδικασία με πριν, αλλά χωρίς exit node

OTR: Off-the-record

# Συμβατικό chat

- Παραδοσιακά συστήματα chat
  - Facebook
  - Skype
  - Google Talk
  - MSN

# Συμβατικό chat

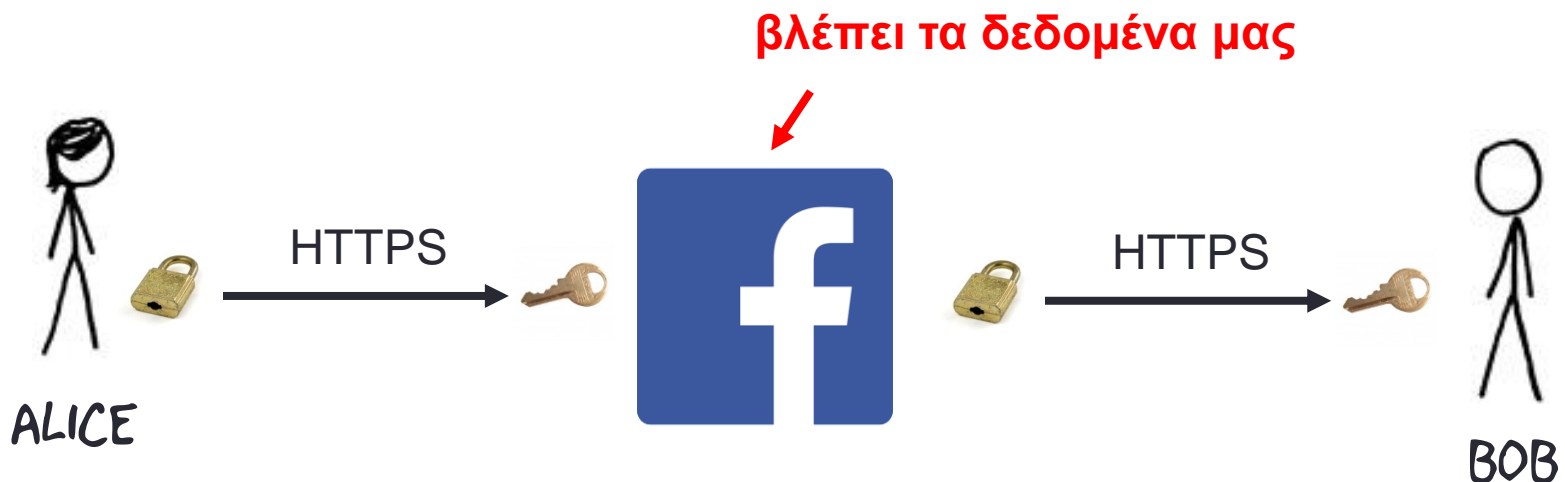
- Η Alice κρυπτογραφεί με το δημόσιο κλειδί του Facebook
- Το Facebook αποκρυπτογραφεί με το ιδιωτικό κλειδί του
- Το Facebook κρυπτογραφεί με το δημόσιο κλειδί του Bob
- Ο Bob αποκρυπτογραφεί με το ιδιωτικό κλειδί του
- Όμως η ίδια η υπηρεσία βλέπει καθαρό κείμενο





# Συμβατικό chat

- Το Facebook διαβάζει το chat μας!
- Είναι στην πράξη «νόμιμος» man-in-the-middle
- Υπηρεσία βλέπει τα δεδομένα μας
- Τα αποθηκεύει
- Μπορεί να τα αποκαλύψει αν υπάρχει ένταλμα
- Μπορεί να μας στείλει ό,τι θέλει



# Κρυπτογράφηση end-to-end

- Η Alice κρυπτογραφεί δεδομένα για τον Bob
- Το Facebook βλέπει μόνο κρυπτογραφημένα δεδομένα



# Κρυπτογράφηση

- Κάθε OTR client έχει ένα ζεύγος κλειδιών
- Ασύμμετρη κρυπτογραφία
- Κλειδιά DSA
- Έχουμε ένα αποτύπωμα ανά λογαριασμό ανά client

# Κρυπτογράφηση και πιστοποίηση

- Τα μηνύματα κρυπτογραφούνται
- ... αλλά υπογράφονται και ψηφιακά
- Μπορούμε να είμαστε σίγουροι ότι ο συνομιλητής μας έγραψε αυτά που έγραψε

# Perfect Forward Secrecy

- Για κάθε μήνυμα χρησιμοποιείται ένα τυχαίο συμμετρικό κλειδί
- Το κλειδί αυτό δεν στέλνεται ποτέ στο δίκτυο
  - Diffie-Hellman
  - ..αλλά και οι 2 συνομιλητές καταλήγουν στο ίδιο μυστικό κλειδί
- Αν ποτέ κατασχεθεί κάποιο ή και τα 2 DSA κλειδιά, δεν μπορούν να διαβαστούν παλαιότερα μηνύματα ακόμα κι αν έχουν υποκλαπεί!

# Deniability

- Ο Bob ξέρει ότι τα μηνύματα που λαμβάνει τα έχει γράψει η Alice
- Ο Bob δεν μπορεί να αποδείξει σε τρίτους μετέπειτα ότι τα έγραψε η Alice

# Επιβεβαίωση αποτυπώματος OTR

- Πρέπει να επιβεβαιώσουμε ότι το κλειδί που μας παρουσιάζεται ανήκει στον άνθρωπο που πιστεύουμε
  - Παρόμοια με την GPG υπογραφή κλειδιού
- Διάφοροι τρόποι επιβεβαίωσης
- Τυπικά ζητάμε από τον ιδιοκτήτη του OTR κλειδιού να το υπογράψει με το GPG κλειδί του
  - <http://petrosagg.com/otr.txt>
  - <https://dionyziz.com/otr>

# Επιβεβαίωση αποτυπώματος OTR

- Επιβεβαιώνουμε ότι το OTR αποτύπωμα που φαίνεται στο πρόγραμμα chat ταιριάζει με το GPG υπογεγραμμένο OTR αποτύπωμα
- Επιβεβαιώνουμε την ψηφιακή υπογραφή GPG
- Επιβεβαιώνουμε ότι το GPG κλειδί είναι αυτό το οποίο ήδη εμπιστευόμαστε



OTR demo



BITCOIN  
WWW.BITCOIN.ORG

# Όσο συνεχίζουμε...

- Κατεβάστε & εγκαταστήστε το multibit
- <https://multibit.org/>



# Τι είναι το bitcoin?

- Ψηφιακό νόμισμα
- Για αληθινές αγορές
  - Online
  - Από κοντά
- Αντικαταστάτης (?) του € και του \$





# Ιστορία

- **Wei Dai**, 1998: "[Bmoney](#)" (cypherpunks)
- **Nick Szabo**, 2005: "Bit gold"
- **Satoshi Nakamoto**, 2008: "[Bitcoin: A Peer-to-Peer Electronic Cash System](#)"
- 2009: bitcoind **open source** σε C++

# Ποιος είναι ο Satoshi Nakamoto?

- Ψευδώνυμος δημιουργός του bitcoin
- Ομάδα ή άτομο;
- Έγραψε το bitcoin paper
- Έφτιαξε την πρώτη υλοποίηση του bitcoin
- Συμμετείχε στο IRC σε συζητήσεις σχετικές με bitcoin
- Έγραφε στο bitcointalk forum
- Κατεύθυνε το bitcoin ώστε να γίνει αυτό που είναι σήμερα
- Υποστήριζε ότι ήταν από την Ιαπωνία
  - ...αλλά δεν έγραψε ποτέ λέξη Ιαπωνικών
- Εξαφανίστηκε μυστηριωδώς ξαφνικά
  - ...και δεν ξανακούσαμε από αυτόν

# Ποιος είναι ο Satoshi ρε γαμώτο?

- Ψευδώνυμος δημιουργός του bitcoin
- Ομάδα ή άτομο;
- Έγραψε το bitcoin paper
- Έφτιαξε την πρώτη υλοποίηση του bitcoin
- Συμμετείχε στο IRC σε συζητήσεις σχετικές με bitcoin
- Έγραφε στο bitcointalk forum
- Κατεύθυνε το bitcoin ώστε να γίνει αυτό που είναι σήμερα
- Υποστήριζε ότι ήταν από την Ιαπωνία
  - ...αλλά δεν έγραψε ποτέ λέξη Ιαπωνικών
- Εξαφανίστηκε μυστηριωδώς ξαφνικά
  - ...και δεν ξανακούσαμε από αυτόν

# Ποιος είναι ο Satoshi ρε γαμώτο?

- Θεωρίες συνωμοσίας...
- Είναι ένας άνθρωπος ή ομάδα;
- Ο Nick Szabo?
- Ο Wei Dai?
- Οι Dr Vili Lehdonvirta & Michael Clear?
- Οι Neal King, Vladimir Oksman & Charles Bry?
- Ο Shinichi Mochizuki?
- Ο Jed McCaleb?
- Ο Dread Pirate Roberts?
- Απ' ό,τι φαίνεται, έχει κρύψει την ταυτότητά του καλά.



**LEAVE SATOSHI**

**ALONE!**

# Πρόβλημα: Online πληρωμές

- Απαιτείται έμπιστη αρχή
- Πληρωμές με **πιστωτικές κάρτες**
- **π.χ. Visa, MasterCard**
- Ή 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
- Αλλά...
- Είναι δύσχρηστος
- **Αργές πληρωμές**
- Δύσκολη μεταφορά
- Κλοπές



# Πρόβλημα

- € και \$ ελέγχονται **κεντρικά**
- Κεντρική τράπεζα τυπώνει χρήματα
- Βλέπε Federal Reserve Bank (ιδιωτική εταιρεία)
- **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

- Ψηφιακό νόμισμα **bitcoin**
- **Peer-to-peer** δίκτυο

# Πλεονεκτήματα

- **Γρήγορες** πληρωμές
  - 1 second για μεταφορά χρημάτων
  - 10 λεπτά για κρυπτογραφική πιστοποίηση
- **Απουσία** κεντρικής αρχής
- Αξία νομίσματος προκύπτει από την **ελεύθερη αγορά**
- **Ασφάλεια** συναλλαγών
- **Ανωνυμία**
- **Αδυναμία** παραχάραξης

# 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**

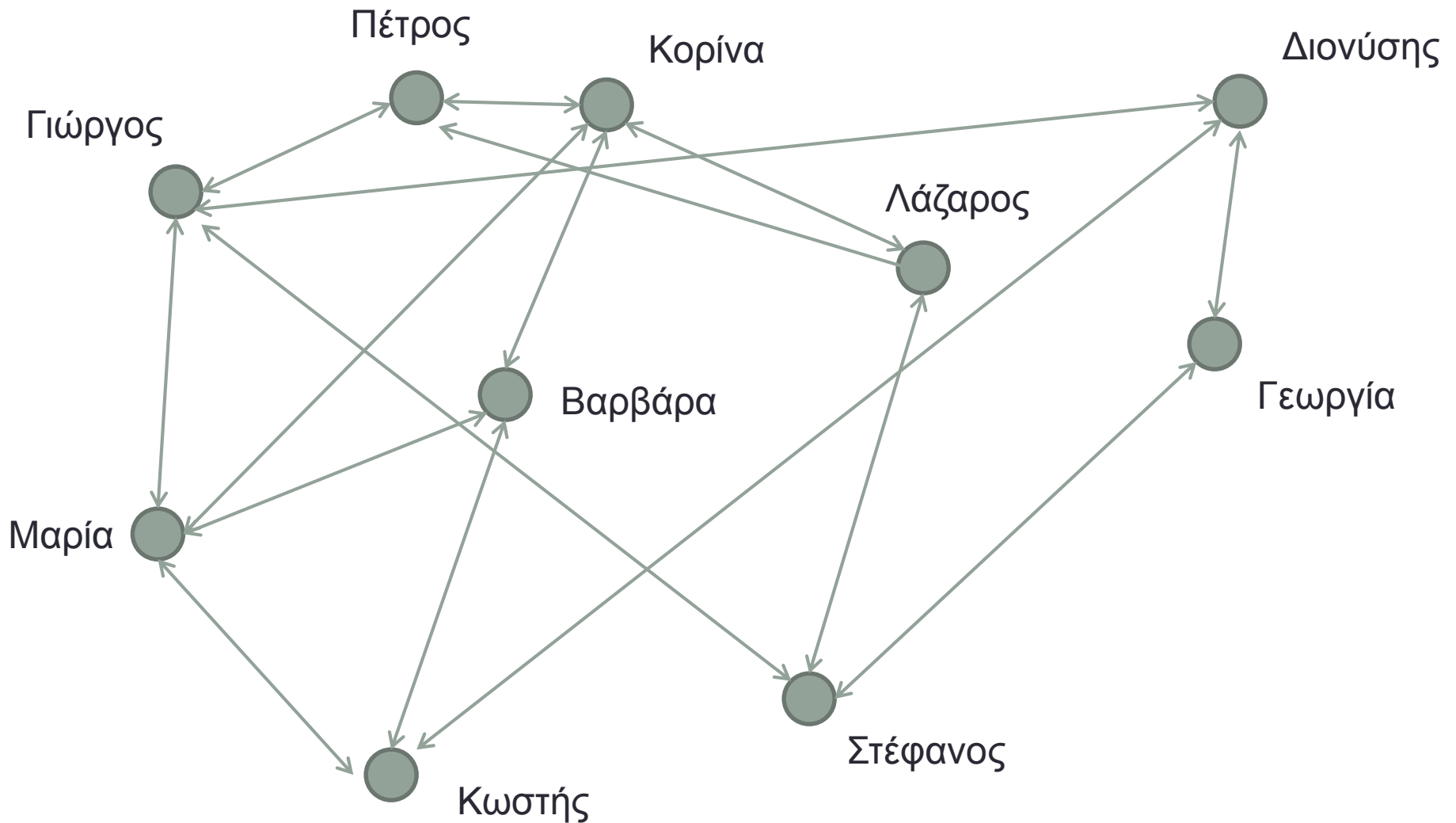
Γιατί να στηριζόμαστε σε κεντρικές αρχές;



...και όχι στην κρυπτογραφία;



# Peer-to-peer δίκτυο bitcoin



# Πιστοποίηση

- Κάθε κόμβος έχει ένα δημόσιο/ιδιωτικό κλειδί
- Δημόσιο κλειδί γίνεται **broadcast** στο δίκτυο
- Ιδιωτικό κλειδί μένει στον κόμβο

# Hash functions

- One-way συναρτήσεις
- $H(x) = y$
- Εύκολο να υπολογιστεί το  $y$  γνωρίζοντας το  $x$
- Δύσκολο να υπολογιστεί το  $x$  γνωρίζοντας το  $y$
- $x \rightarrow y$
- $y \overset{?}{\dashrightarrow} x$

# Collision resistance

- Δεδομένου  $y$ , δεν μπορεί να βρεθεί  $x$  τέτοιο ώστε:
  - $H(x) = y$
- Δεν μπορούν να βρεθούν  $\alpha, \beta$  τέτοια ώστε:
  - $H(\alpha) = H(\beta)$
- Δεδομένων  $d$  και  $c$ , δεν μπορεί να βρεθεί  $n$  τέτοιο ώστε:
  - $H(c \parallel n) < d$
  - Για αρκετά μικρά  $d$
- Ένα hash αντιστοιχεί κατά πάσα πιθανότητα **σε ένα** αρχικό μήνυμα

Έχει 12mBTC

Έχει 0BTC

$m \leftarrow \text{“Στέλνω 12mBTC στην Alice”}$

$h \leftarrow H(m)$

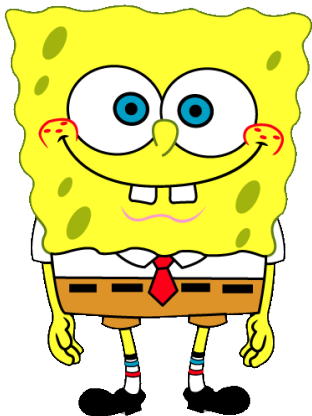
$s \leftarrow \text{sign}_{B_s}(h)$

$s$

Έχει 0BTC

$\text{verify}_{B_p}(m, s)$   
Έχει 12mBTC

Bob



Alice



# Εγκυρότητα

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

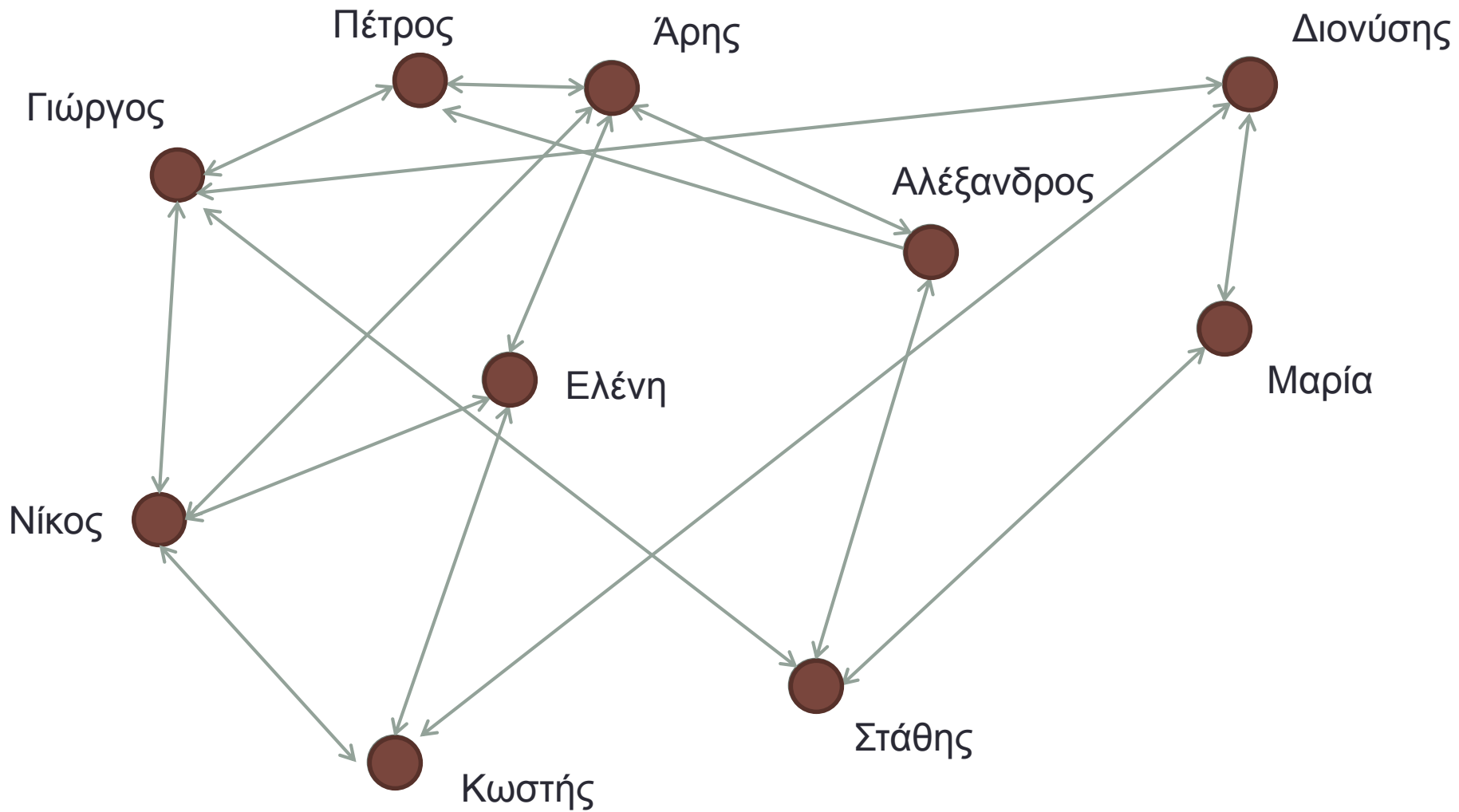
# Ποιος έχει τι

- 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



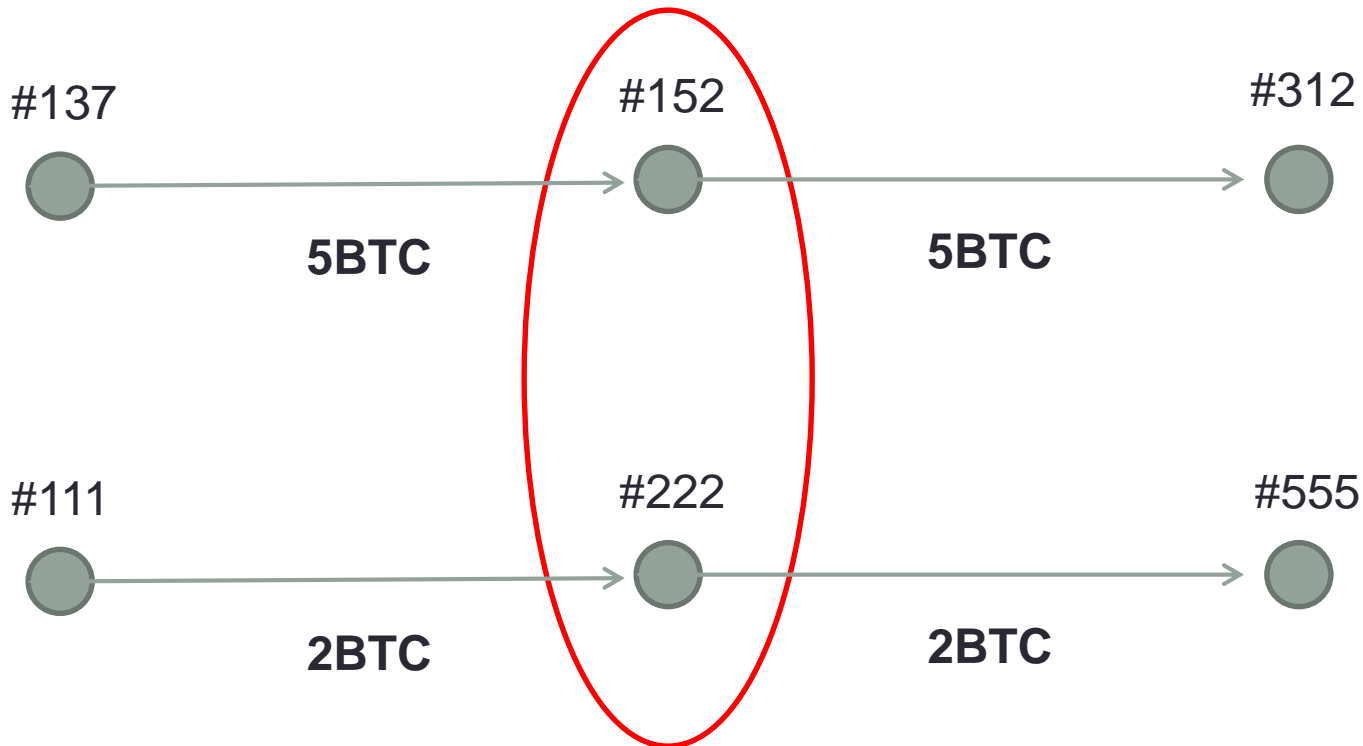


# Ανωνυμία

- Για **κάθε συναλλαγή** οι συμμετέχοντες μπορούν να χρησιμοποιήσουν 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  
 $B_p$ ,  $B_s$

$m1 \leftarrow \text{"12mBTC προς } A_p\text{"}$   
 $h1 \leftarrow H(m1)$



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



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



Δημιουργεί ένα **νέο** κλειδί  
Γι' αυτή τη συναλλαγή  
 $C_p$ ,  $C_s$

$\text{ver}_{A_p}(m2, s2)$

Δημιουργεί ένα **νέο** κλειδί  
Γι' αυτή τη συναλλαγή  
 $A_p$ ,  $A_s$

$\text{ver}_{B_p}(m1, s1)$

$m2 \leftarrow \text{"12mBTC προς } P_C\text{"}$   
 $h2 \leftarrow H(m2)$

# Νόμισμα



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



- (ουδ.) μία αλυσίδα ψηφιακών υπογραφών.

# Νόμισμα = Αλυσίδα υπογραφών

...

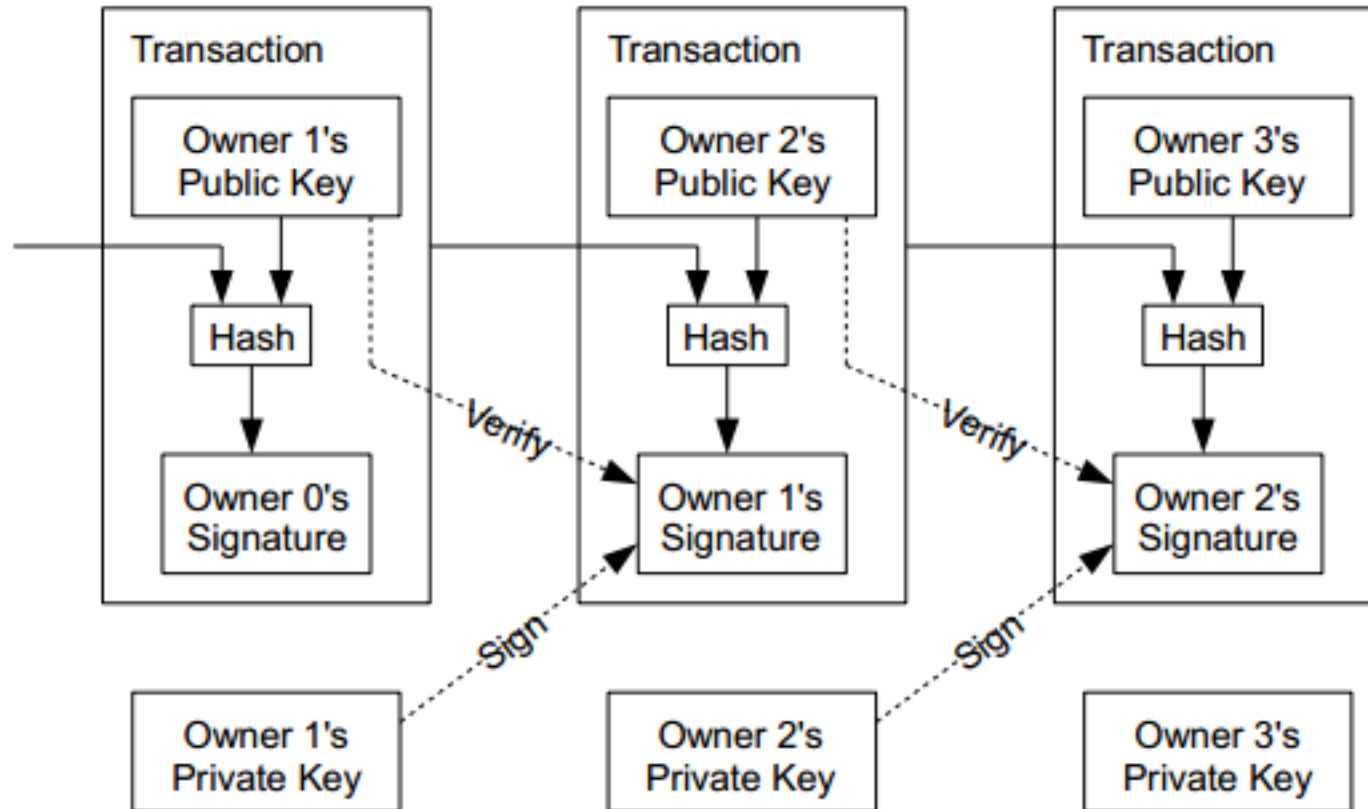
$\text{coin1} \leftarrow \text{sign}_{s_0} ( H ( \text{coin0} \parallel P1 ) )$

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

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

...

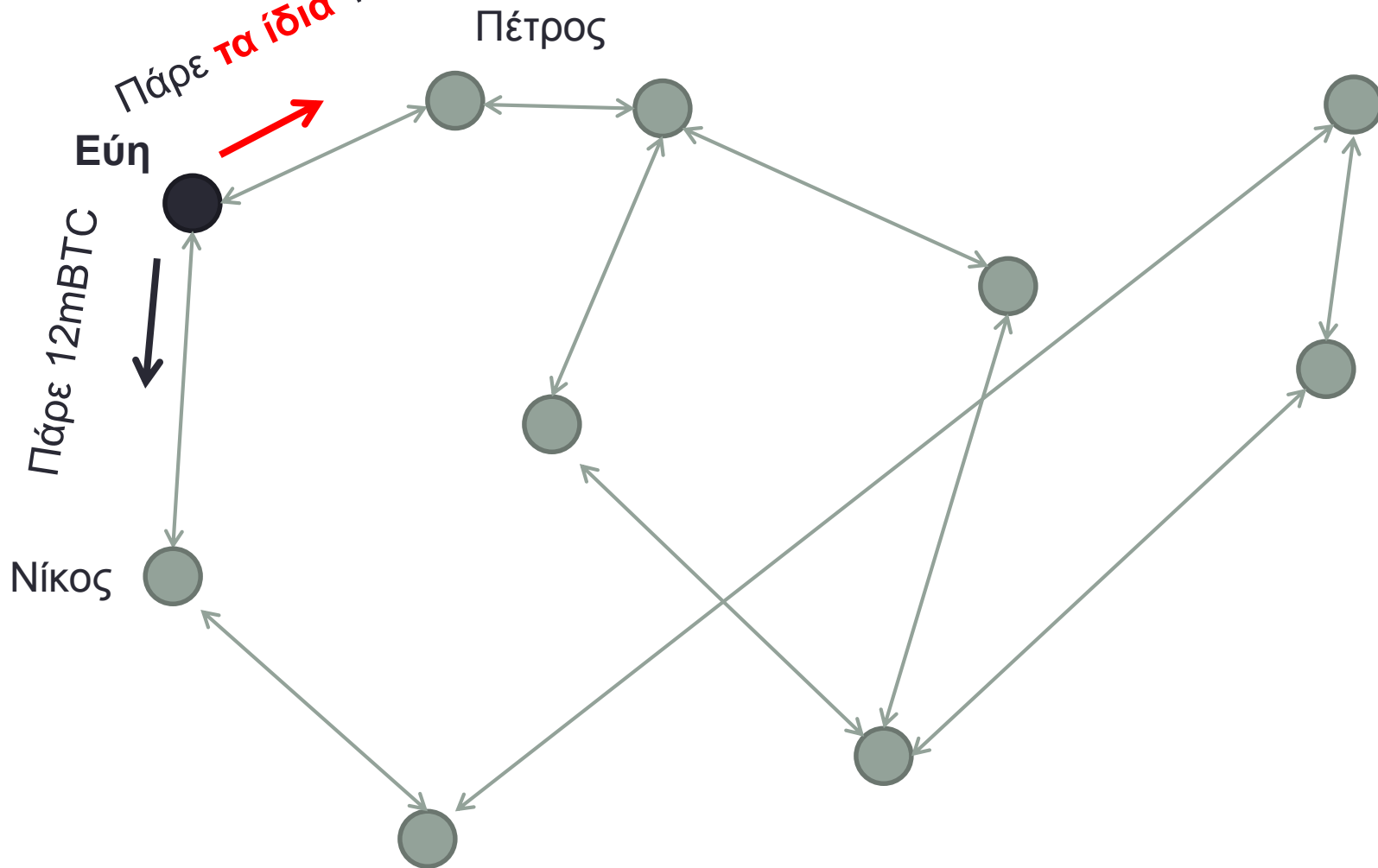




```
{
  "hash": "96f5e5394726ca5...",
  "ver": 1,
  "in": [{
    "prev_out": {
      "hash": "87750ccbebf71042d...",
      "n": 0
    },
    "scriptSig": "30440397d0c2... 49d0c04a7e52..."
  }],
  "out": [{
    "value": "0.71430000",
    "scriptPubKey": "OP_DUP OP_HASH160
99fa78c49d99f58c8dd... OP_EQUALVERIFY
OP_CHECKSIG"
  }]
}
```



# Διπλοξοδεύω



# Διπλό ξόδεμα

- Ανεπιθύμητο
- Πώς μπορεί να αποτραπεί;

Έγκυρες συναλλαγές  
=  
Συναλλαγές που **δεν** έχουν γίνει **>= δύο** φορές;

Αυτό μου επιτρέπει να ακυρώσω μία συναλλαγή που δεν θέλω!

# Το βέλος του χρόνου

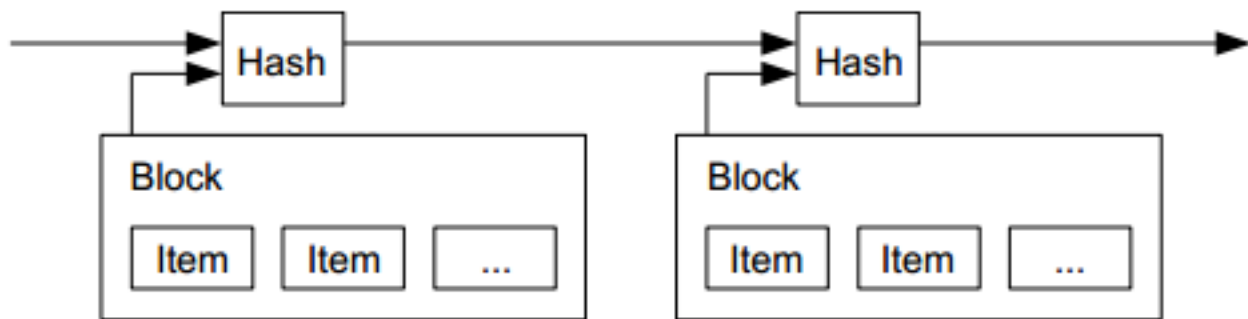
- **Έγκυρη** είναι η **πρώτη** συναλλαγή που έγινε από αυτό τον κρίκο της αλυσίδας
- **Μετέπειτα** συναλλαγές είναι **άκυρες**

# 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**
- Υπολογίζεται **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



# Ποιος θα δημιουργήσει τα blocks?

- Θα μπορούσε να υπάρχει μία έμπιστη αρχή
  - Δε μας αρέσουν οι έμπιστες αρχές 😊
  - Δεν είναι αποκεντρωμένο

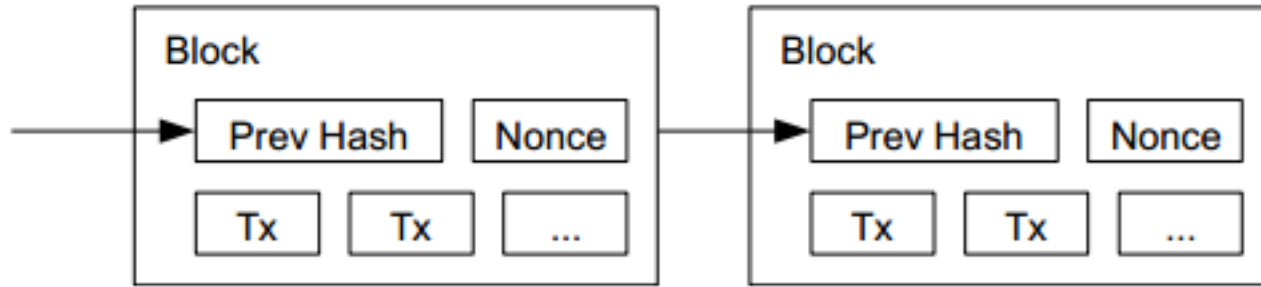
# Αν αφήσουμε τον καθένα να το κάνει μόνος του...

- Θα μπορούσε κάποιος να φτιάξει τεχνητά blocks
- Και να συνδέσει το καθένα με το προηγούμενό του
- Έτσι θα μπορούσε και πάλι να διπλοξοδέψει



# Proof-of-work

- 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 ) < 100000:
```

```
    nonce ← nonce + 1
```

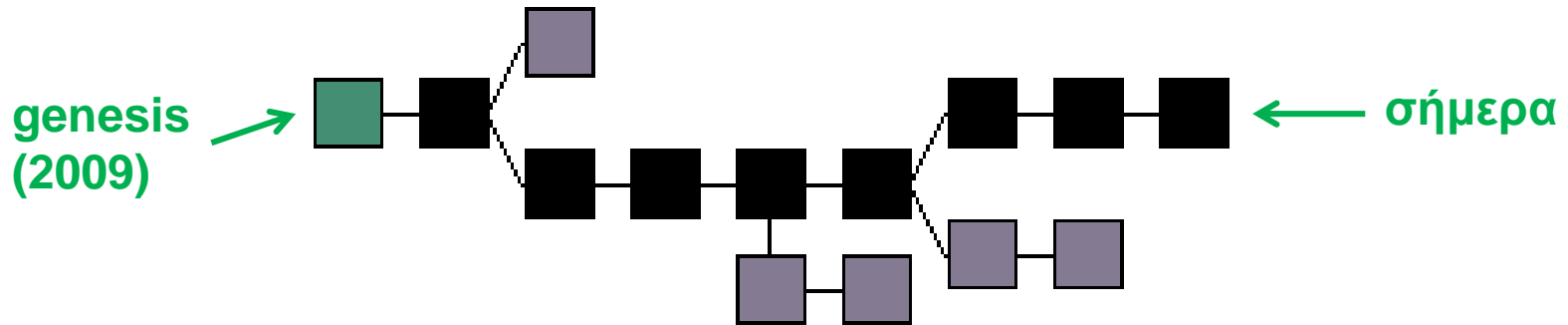
```
broadcast( block )
```

**Difficulty**



# Απόδειξη εργασίας

- Κάθε block **πιστοποιεί** τις συναλλαγές που περιέχει
- Δημιουργείται μία αλυσίδα από blocks
- Όλα τα έγκυρα blocks κληρωνομούν από το genesis





# 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



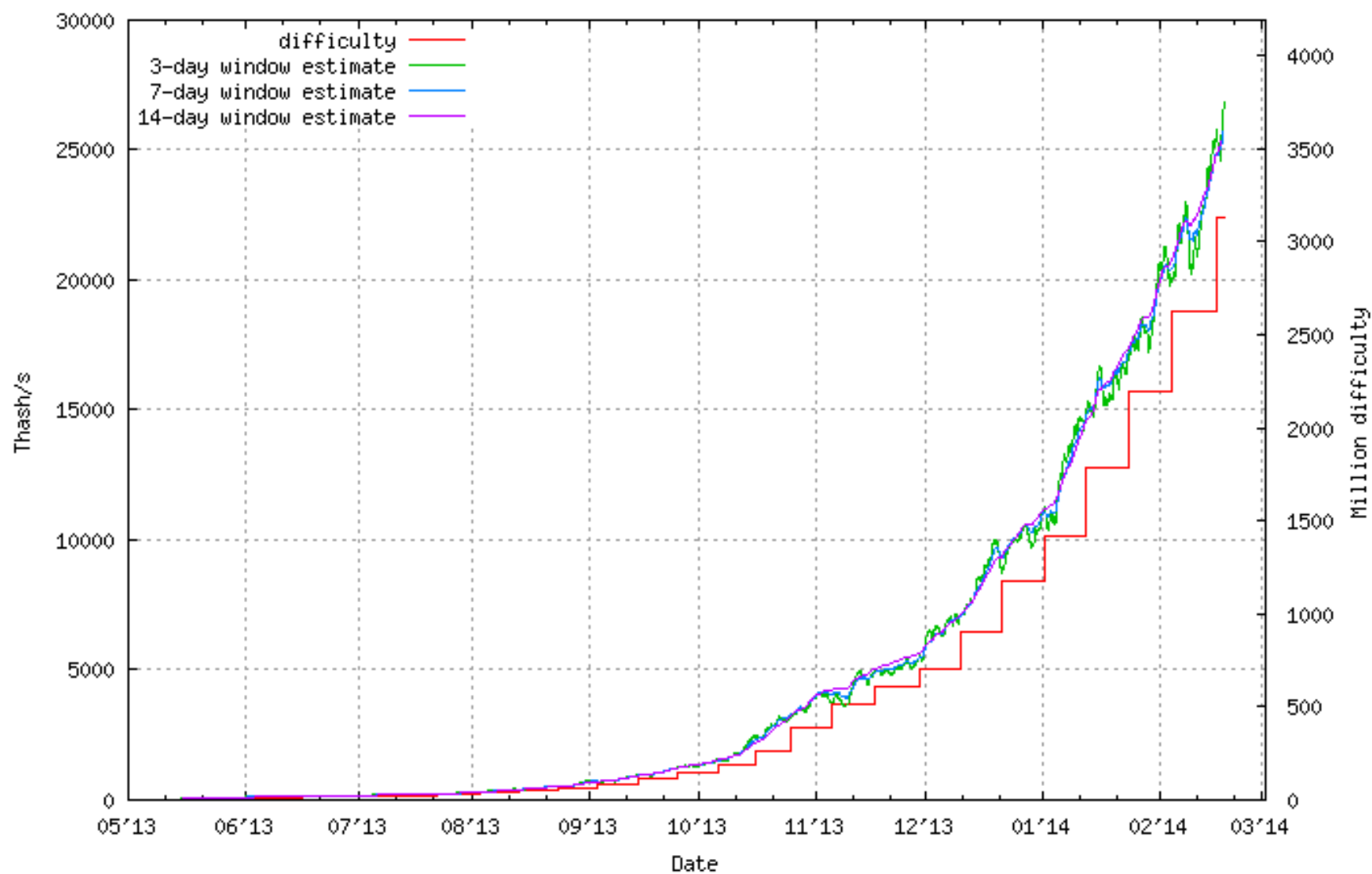
# Εξόρυξη bitcoin

- Δημιουργία block = Κέρδη σε bitcoin για το δημιουργό
- Ελεγχόμενος πληθωρισμός από το δίκτυο
- Σήμερα: 25BTC / block

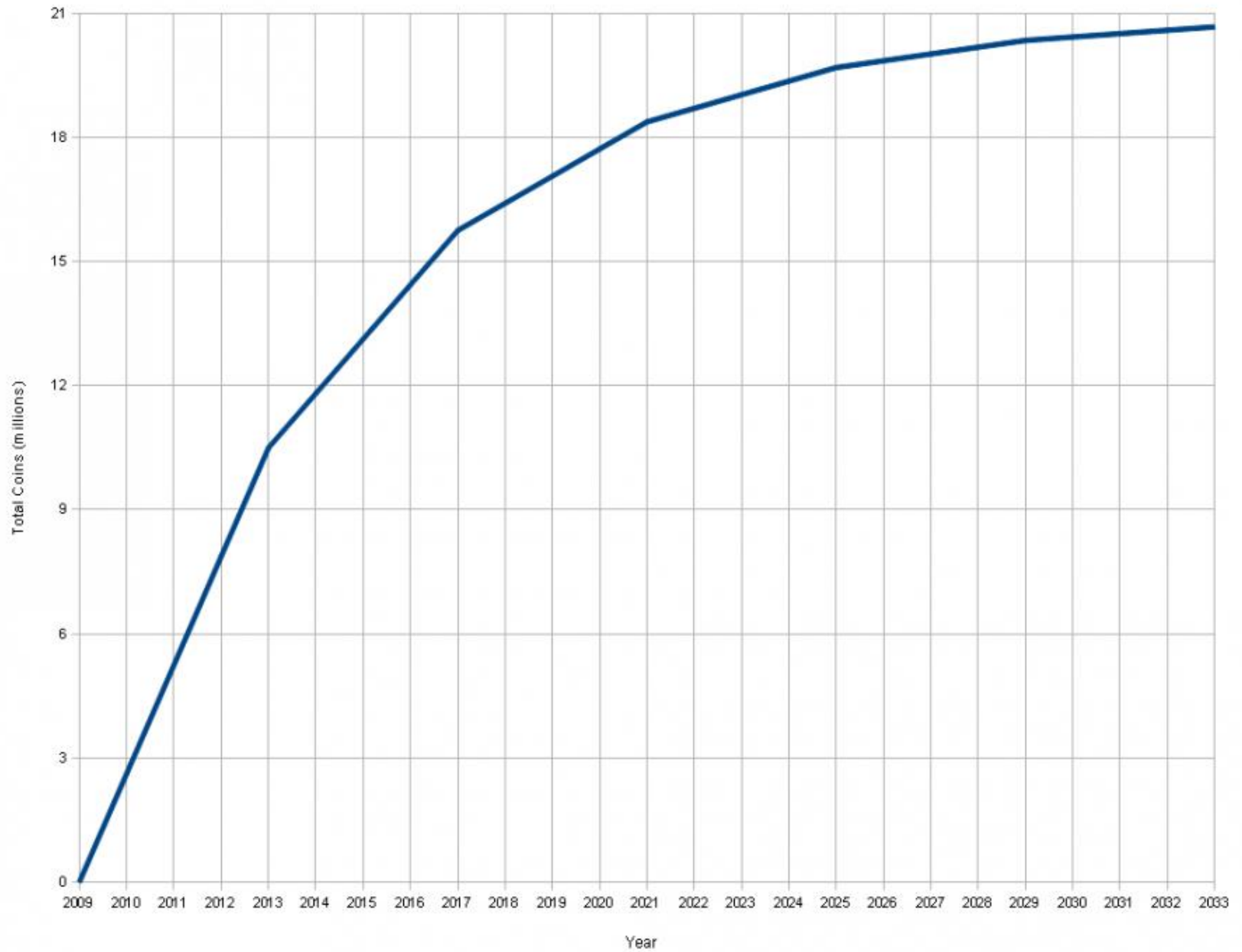
# Difficulty

- Υπολογίζεται συλλογικά από το δίκτυο
- Αλλάζει κάθε βδομάδα
- Προκύπτει από τη συνολική CPU δύναμη του δικτύου
- Ορίζεται έτσι ώστε κάθε block να παίρνει 10 λεπτά
- Αυτή τη στιγμή: 3,129,573,175

Bitcoin network: total computation speed



Total Bitcoins over time



# Τεχνικές λεπτομέρειες

- Ψηφιακές υπογραφές
  - Παραλλαγή σχήματος Elgamal (DSA) διακριτού λογαρίθμου
  - Με χρήση ελλειπτικών καμπυλών
- Hash function
  - SHA256( SHA256( \_ ) )
- Συνάρτηση εργασίας
  - SHA256( \_ )

# Το bitcoin σήμερα

17 Φεβρουαρίου 2012:

- 167,000 blocks
- 1BTC = 3.27€
- 8.3M BTC σε κυκλοφορία
- **27,000,000€ σε κυκλοφορία**
- Συχνότητα hashing δικτύου = 9THz

9 Απριλίου 2013:

- 1BTC = 73€

19 Φεβρουαρίου 2014:

- 286,000 blocks
- 1BTC = 450€
- 12.4M BTC σε κυκλοφορία
- **5,600,000,000€ σε κυκλοφορία**
- Συχνότητα hashing δικτύου = 30,000Thz

# Εναλλακτικά κρυπτονομίσματα

- Litecoin
  - Scrypt αντί για SHA
- Dogecoin
- Namecoin
  - Decentralized DNS
- Twister
  - Decentralized Twitter
- Bitmessage
  - Decentralized SMS
- Zerocoin
  - Για ανωνυμία






# Μάθαμε

- Ανώνυμο browsing με Tor
- Onion routing
- Ασφαλές chat με OTR
- Forward secrecy
- Deniability
- Το κρυπτονόμισμα bitcoin

# Συγχαρητήρια!

- Μπορείτε να μπαίνετε στο Internet **ανώνυμα**
- Μπορείτε να κάνετε chat **με ασφάλεια**
- Μπορείτε να κάνετε **αγορές με bitcoin**





# Ευχαριστούμε! Ερωτήσεις;



Αυτές οι διαφάνειες είναι:  
Creative Commons 3.0 Attribution

bitcoin.org  
Twitter: @dionyziz, @petrosagg