

BITCOIN

Διδάσκοντες: Δ. Ζήνδρος

Επιμέλεια διαφανειών: Π. Αγγελάτος, Δ. Ζήνδρος

ΤΕΙ Λάρισας 2014



Στόχος της ώρας

- Το κρυπτονόμισμα bitcoin
- Ιστορία του bitcoin
- Πρακτική χρήση πορτοφολιών
- Δημόσια/ιδιωτικά κλειδιά
- Διπλό ξόδεμα
- Blockchain
- Άλλα κρυπτονομίσματα: Namecoin, Ethereum



BITCOIN
WWW.BITCOIN.ORG

Όσο ξεκινάμε...

- 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
- Νόμισμα σχεδιασμένο για το Internet

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

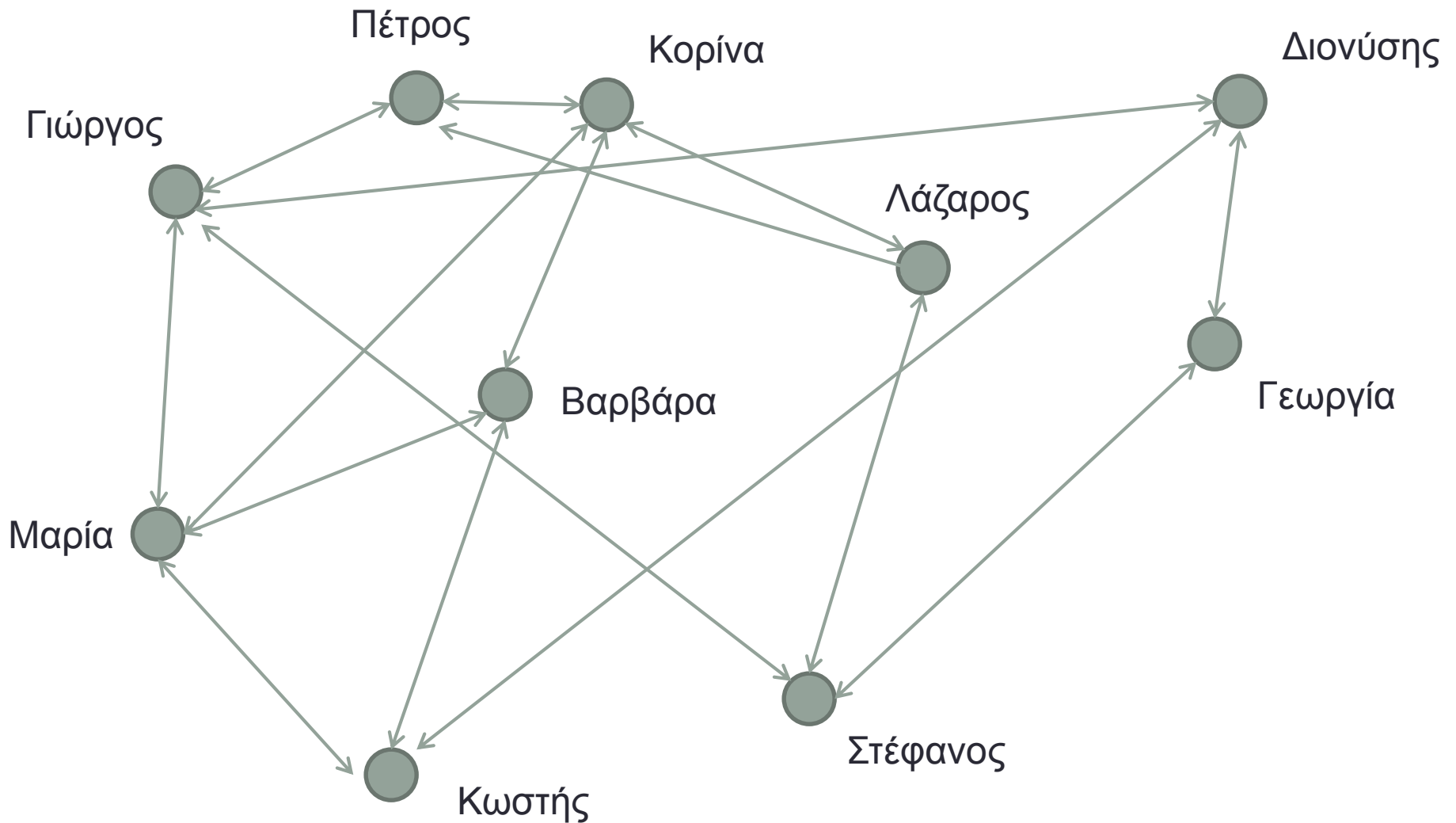
Ιδέα!

- 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 α, β 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

$m \leftarrow \text{“}\Sigma\tau\acute{\epsilon}\lambda\nu\omega\ 12\text{mBTC}\ \sigma\tau\eta\nu\ \text{Alice”}$

$h \leftarrow H(m)$

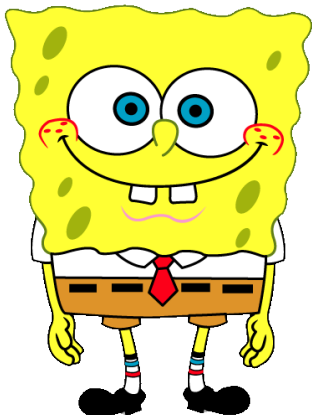
$s \leftarrow \text{sign}_{B_s}(h)$

s

Έχει 0BTC

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

Bob



Alice



Εγκυρότητα

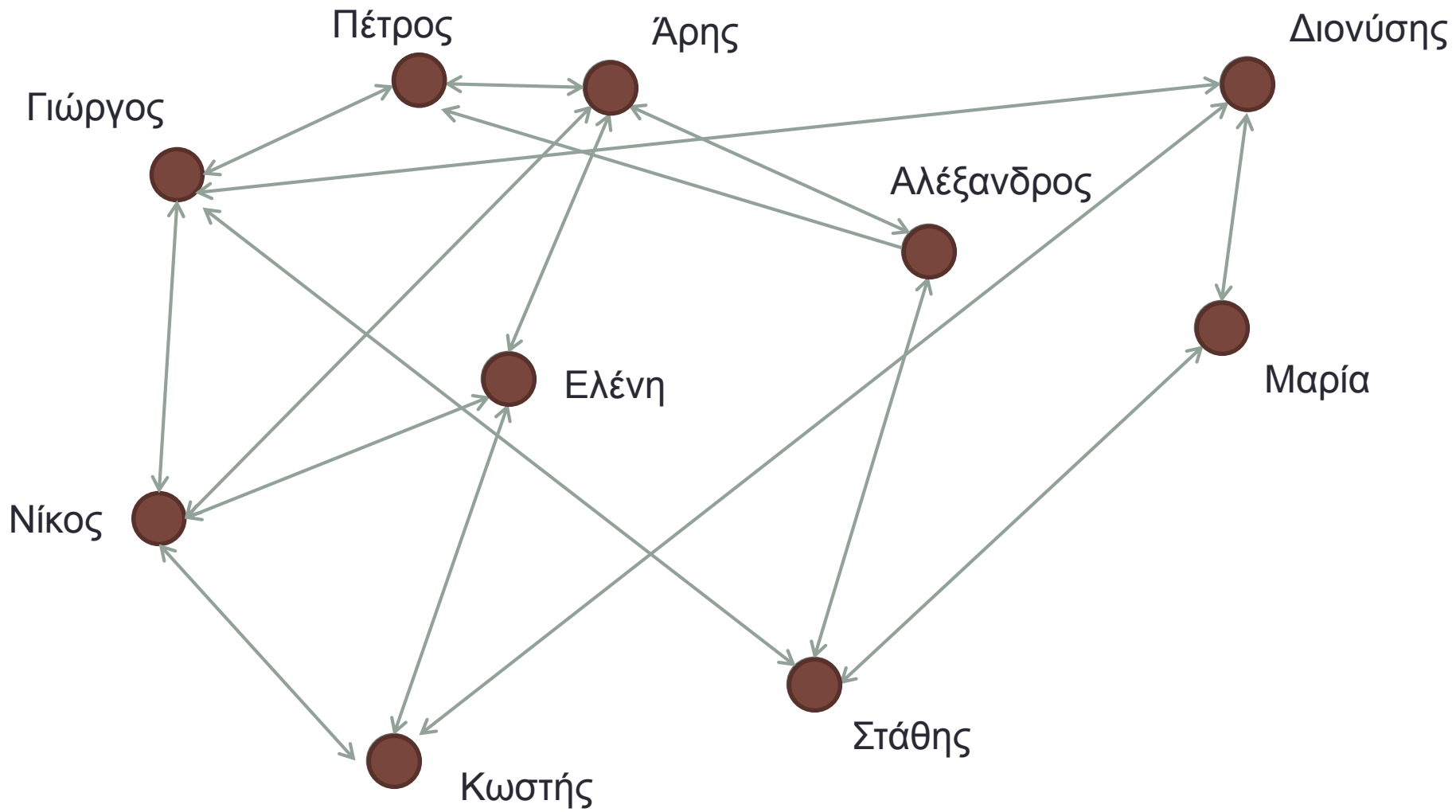
- Πώς ξέρουμε ότι το νόμισμα προήλθε από **έγκυρη πηγή** και δεν είναι **αυτοδημιούργητο**;

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**
- Δεν υπάρχει κεντρική αρχή ελέγχου
- Ο έλεγχος γίνεται από τους ίδιους τους χρήστες

Broadcasting

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

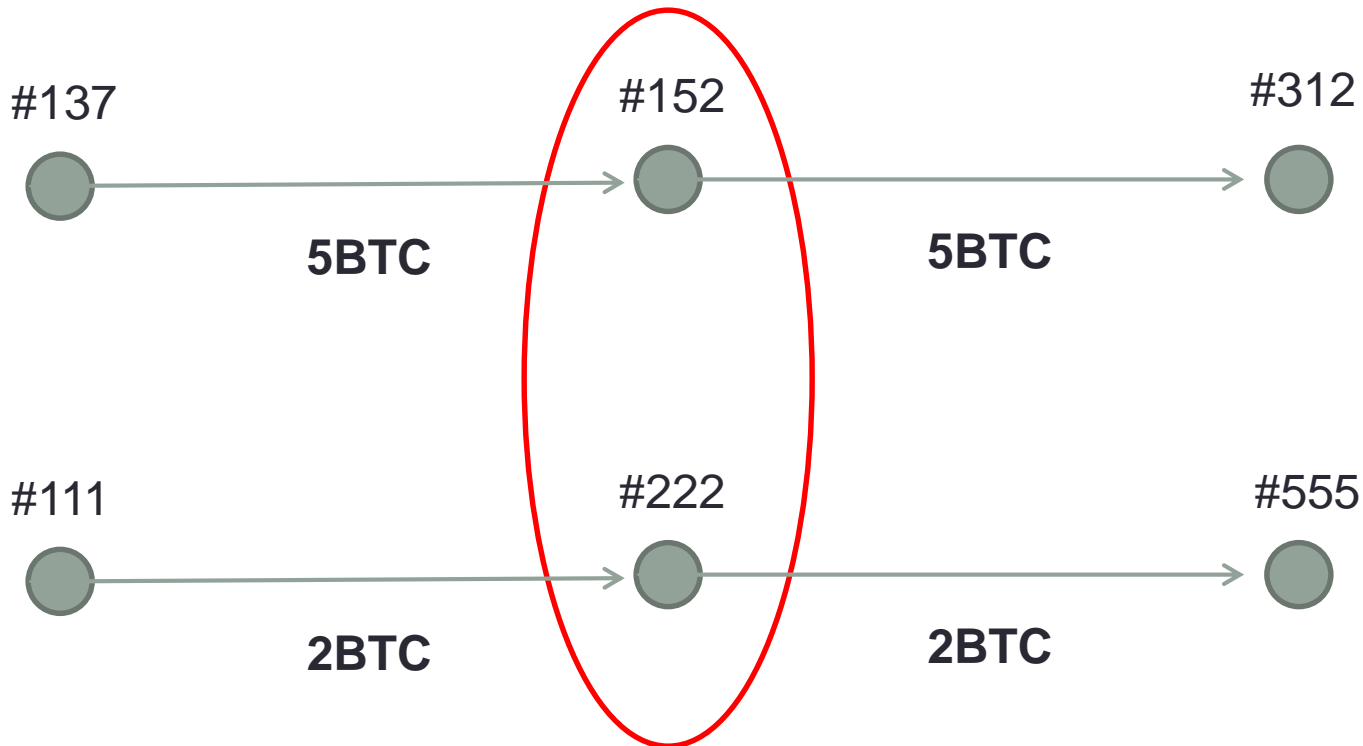


Ανωνυμία

- 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

...

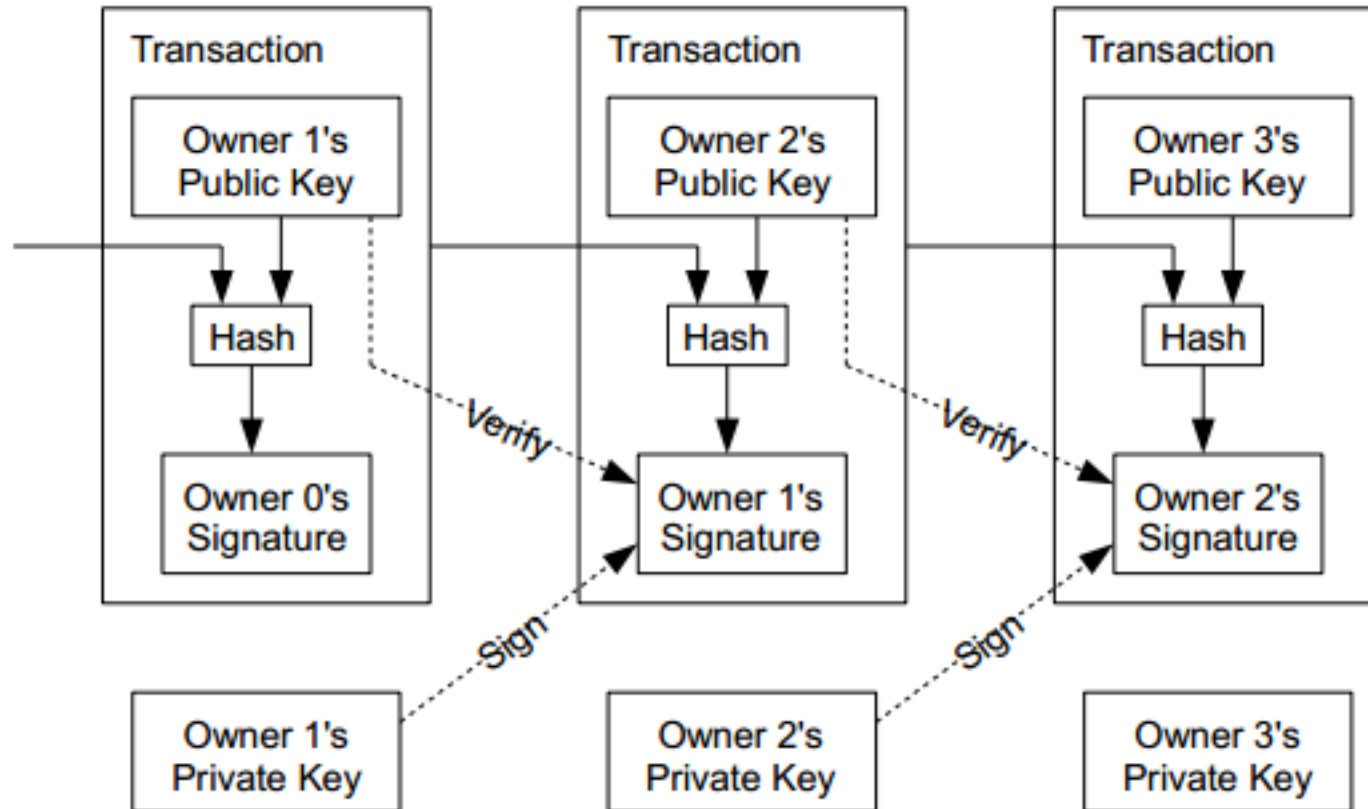
$\text{coin1} \leftarrow \text{sign}_{s_0} (H (\text{coin0} \parallel P1))$

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

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

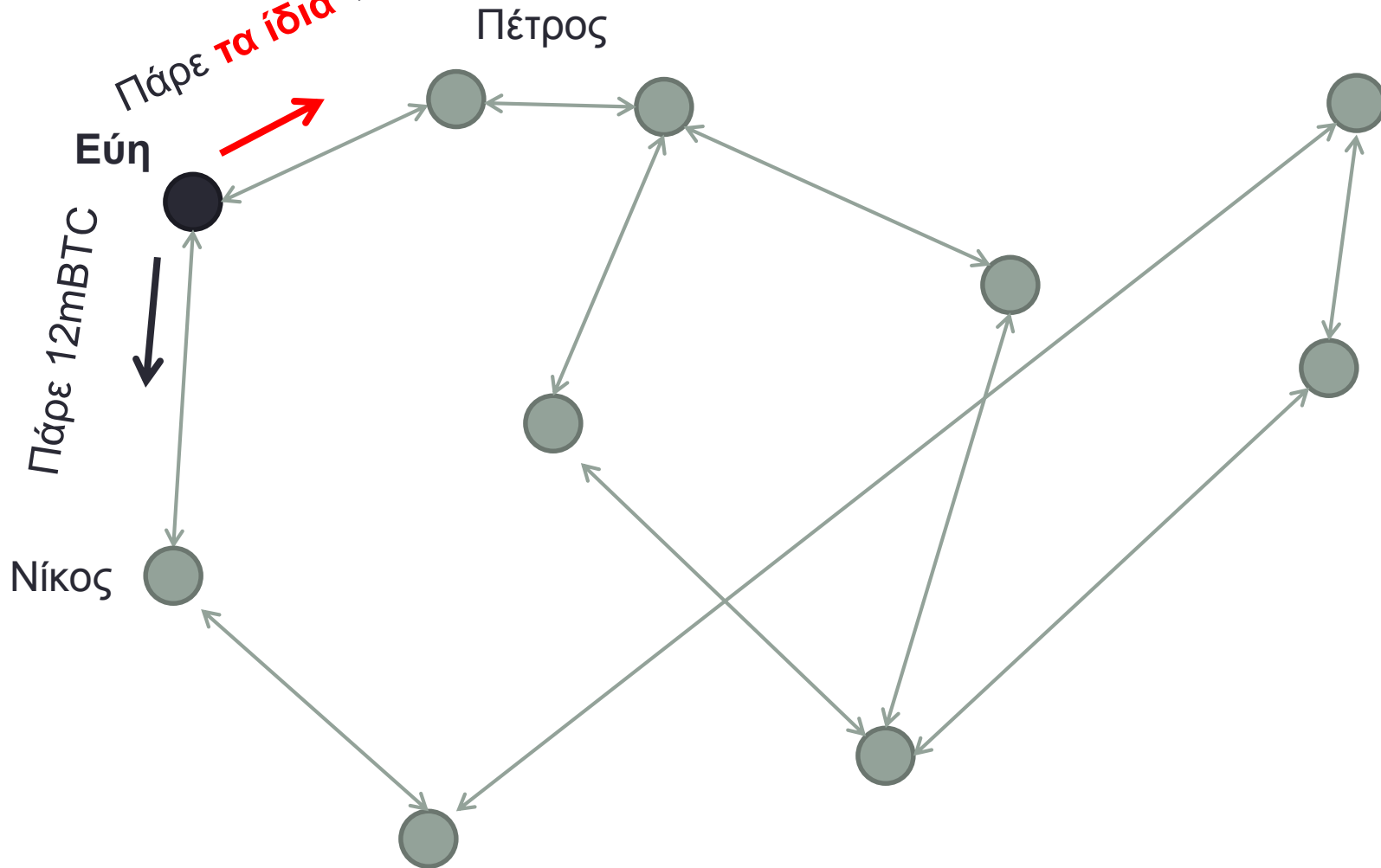
...






```
{
  "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

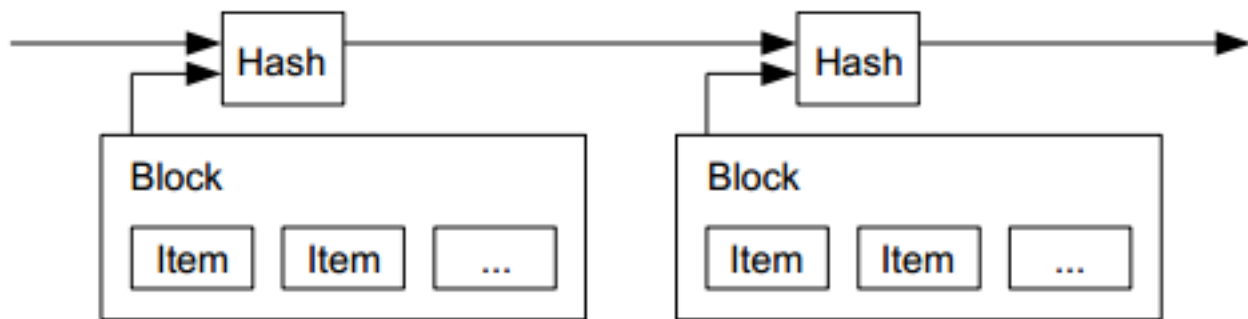
- **Έγκυρη** είναι η **πρώτη** συναλλαγή που έγινε από αυτό τον κρίκο της αλυσίδας
- **Μετέπειτα** συναλλαγές είναι **άκυρες**

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?

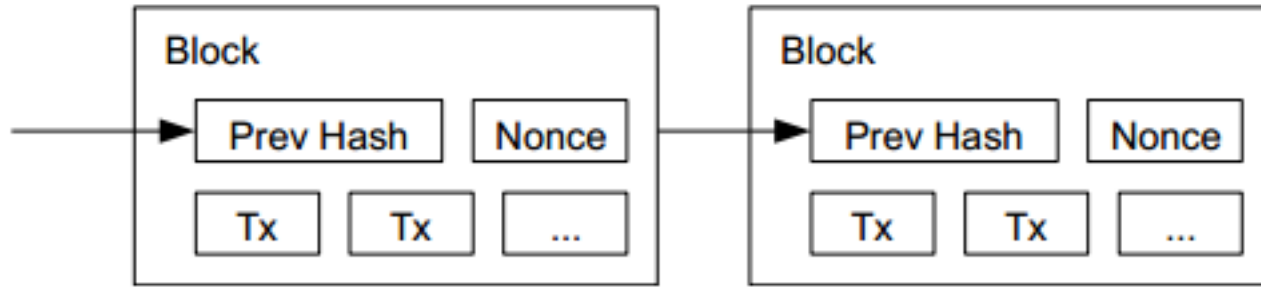
- Θα μπορούσε να υπάρχει μία έμπιστη αρχή
 - Δε μας αρέσουν οι έμπιστες αρχές 😊
 - Δεν είναι αποκεντρωμένο

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
```

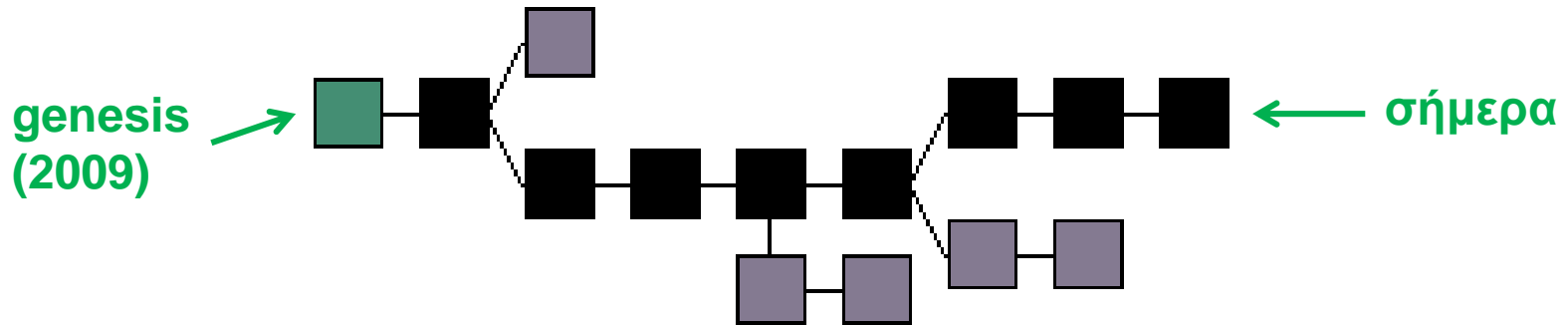
```
broadcast( block )
```

Difficulty

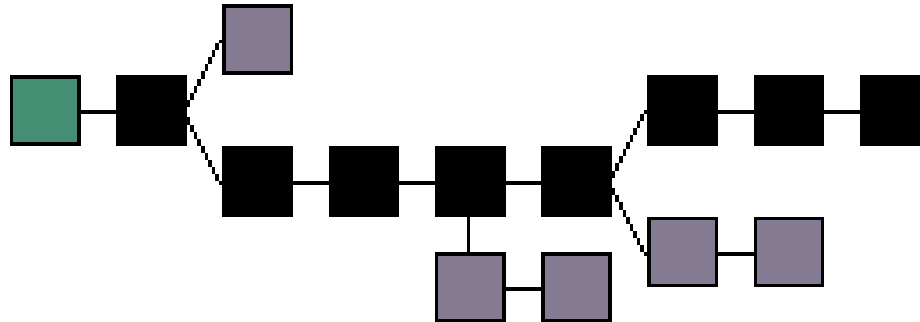


Απόδειξη εργασίας

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



Blockchain





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

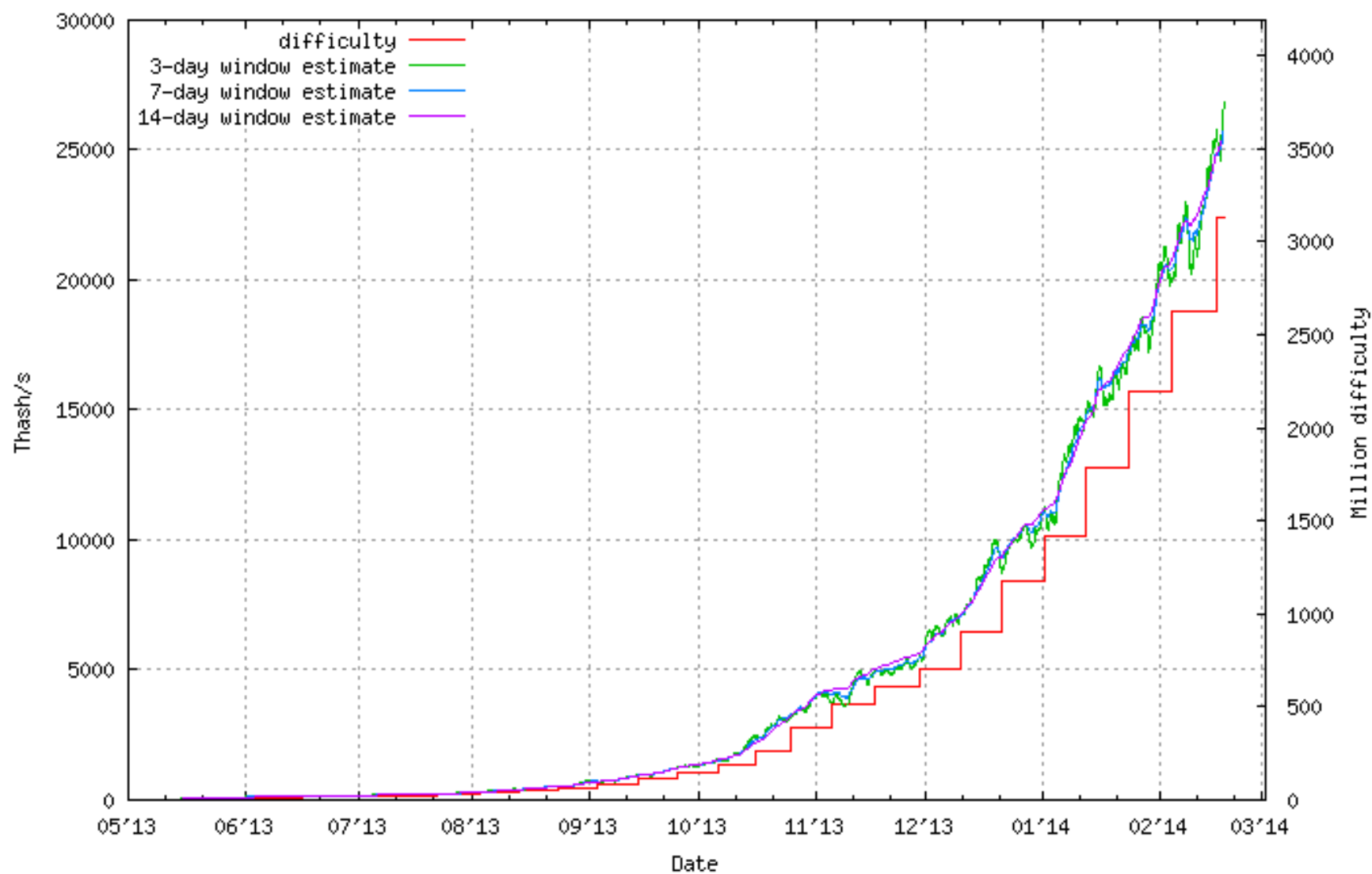
Εξόρυξη bitcoin

- Δημιουργία block = Κέρδη σε bitcoin για το δημιουργό
- Ελεγχόμενος πληθωρισμός από το δίκτυο
- Σήμερα: 25BTC / block
- Ο μόνος τρόπος παραγωγής bitcoin
- Reward = 25BTC / block υποδιπλασιάζεται κάθε 4 χρόνια

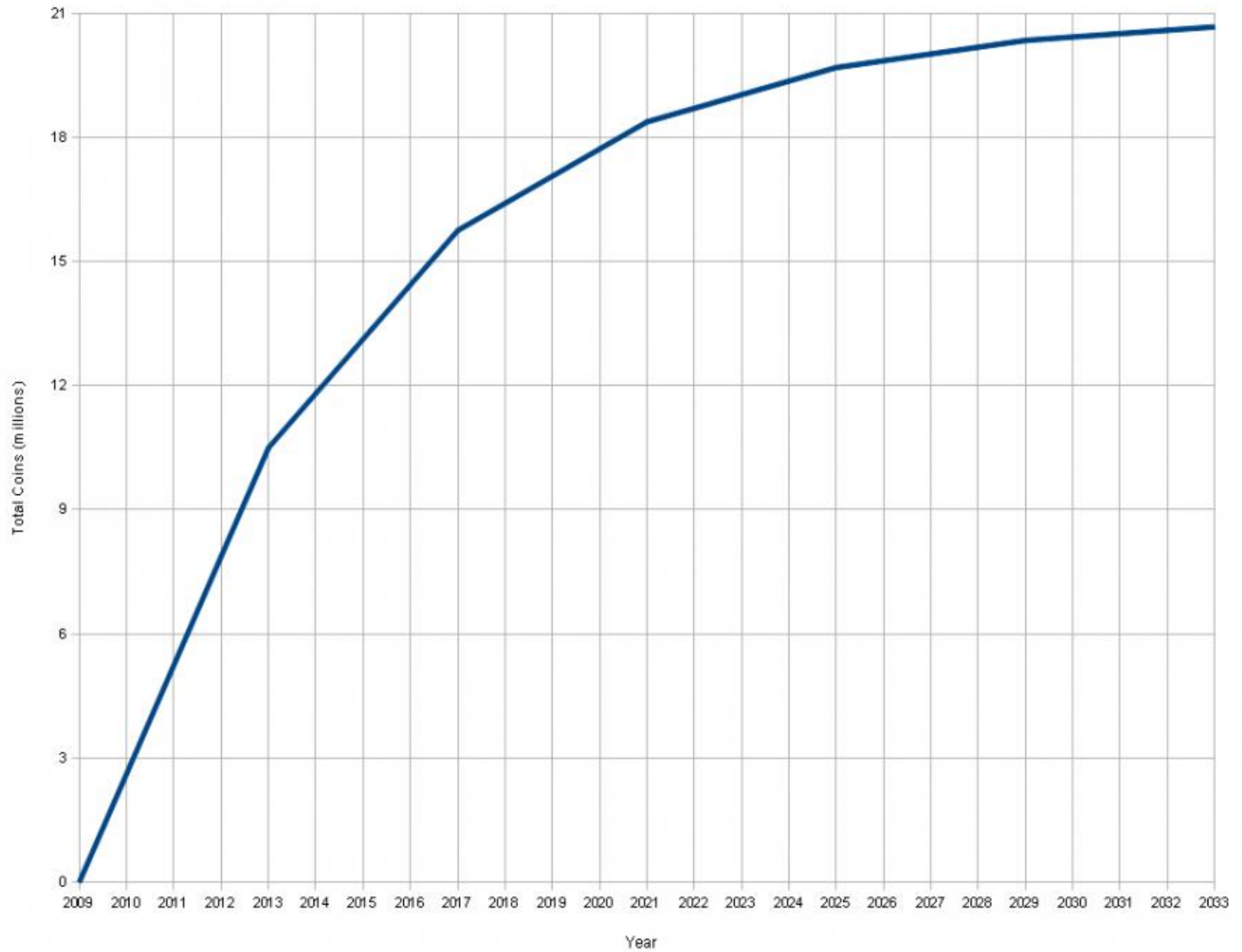
Difficulty

- 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



Υποδιαιρέσεις bitcoin

- 1 BTC μπορεί να διαιρεθεί σε:
- Μέχρι 10^8 κομμάτια
- Αξίας 10^{-8} BTC το καθένα

Πόσο αξίζει ένα bitcoin?

- Όπως και το €, όσο θεωρούμε ότι αξίζει
- Σήμερα: 1 BTC = 429€

Πώς αποκτώ bitcoin?

- Κάνω mining
 - Μη πρακτικό στις μέρες μας
 - Εκτός αν θέλεις να αφιερώσεις όλη τη ζωή σου και ένα σημαντικό κεφάλαιο χρημάτων σε αυτό
- Αγοράζω από άλλους που έχουν BTC με € ή \$
 - Καλές τιμές, αλλά χρειάζεται προσοχή
- Αγοράζω από ιδιωτικές τράπεζες που πουλάνε BTC
 - Συνήθως ασφαλέστερο
 - Κρατάνε προμήθεια
- Πουλάω κάποιο αντικείμενο για BTC
- Δουλεύω για BTC

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€

27 Μαΐου 2014:

- 302,000 blocks
- 1BTC = 429€
- 12.8M BTC σε κυκλοφορία
- **5,500,000,000€ σε κυκλοφορία**
- Συχνότητα hashing δικτύου = 76,000Thz

Bitcoin στην πράξη

Πού αποθηκεύω bitcoins?

- Στον υπολογιστή σου
- Στο laptop σου
- Στο κινητό σου
- Αποθηκεύονται σε πρόγραμμα που λέγεται «πορτοφόλι»

Διευθύνσεις Bitcoin

- Κάθε client φτιάχνει ένα πορτοφόλι
- Το πορτοφόλι περιέχει πολλαπλές διευθύνσεις
 - Οι διευθύνσεις είναι δημόσια κλειδιά
 - Μπορούν να δημοσιευθούν με ασφάλεια
 - Ξεκινούν πάντα με '1'
 - Είναι σαν αριθμοί λογαριασμών
 - 174aNr4bHZPbTgsm3xudqVKqjZYNPwKK28

Ιδιωτικά κλειδιά

- Κάθε διεύθυνση έχει και ένα ιδιωτικό κλειδί
- Αυτό αποθηκεύεται σε αρχείο
- Δεν εμφανίζεται στην οθόνη
- Οποιοσδήποτε αποκτήσει πρόσβαση στο ιδιωτικό κλειδί που αντιστοιχεί στην bitcoin διεύθυνσή μας **έχει έλεγχο των χρημάτων μας!**

Όσο συνεχίζουμε...

- Κατεβάστε το Bitcoin Wallet στο Android σας
- Play Store
- Andreas Schildbach

Τύποι πορτοφολιών

- **Πλήρως τοπικό**
- Αποθηκεύεται μόνο στον υπολογιστή μας
- Αρκετά ασφαλές
- Αρκεί να διατηρούμε τον υπολογιστή μας ασφαλή
- Σημαντικό να κρατάμε backups
- π.χ. bitcoin-qt

Τύποι πορτοφολιών

- **Πλήρως online**
- Αποθηκεύεται όλο σε ένα web service
- Έχουμε πρόσβαση μέσω του website
- Δεν χρειάζεται να τρέχουμε bitcoin πρόγραμμα
- Το web service έχει πλήρη πρόσβαση στα ιδιωτικά μας κλειδιά
- Πρόκειται ουσιαστικά για μία τράπεζα bitcoin
- Παραδίδουμε την ιδιοκτησία των χρημάτων μας!
- Ασφαλές αν πάθει κάτι ο υπολογιστής μας
- π.χ. blockchain.info

Τύποι πορτοφολιών

- **Μερικώς online**
- Το blockchain και το **κρυπτογραφημένο** ιδιωτικό κλειδί αποθηκεύονται online
- Τρέχουμε πρόγραμμα που κατεβάζει το ιδιωτικό κλειδί και το αποκρυπτογραφεί τοπικά
- Αν χάσουμε το πρόγραμμα, μπορούμε να το ξανακατεβάσουμε
- Η ασφάλειά μας περιορίζεται σε έναν κωδικό
- Η online υπηρεσία δεν έχει πρόσβαση στο ιδιωτικό κλειδί μας
- π.χ. electrum, multibit

Τύποι πορτοφολιών

- **Χάρτινο πορτοφόλι**
- Τυπώνω το ιδιωτικό κλειδί σε ένα χαρτί
- Το κρατάω σε ένα χρηματοκιβώτιο
- Το ιδιωτικό κλειδί δεν υπάρχει online ούτε σε κάποιο σκληρό δίσκο
- Δύσκολο να γίνει hack
- Πιο εύκολο να κλαπεί, να χαθεί, να πάρει φωτιά...

Τι μπορώ να κάνω με bitcoins?

- Να αγοράσω/πουλήσω αντικείμενα
 - Σήμερα πολλά ψηφιακά και φυσικά αγαθά
 - π.χ. servers, domain names, hosting
 - π.χ. βιβλία, albums, ρούχα, διακοσμητικά
 - π.χ. pizza, φαγητό, καφέ, γλυκό
- Να πληρώσω/πληρωθώ
 - π.χ. θα χαρώ να κάνω security review στο site σου για bitcoins*
 - *αλλά όχι για € 😊
- Να στοιχηματίσω στην τιμή του (foreign exchange)
 - Κακή ιδέα, υπάρχουν πολύ πιο ικανοί άνθρωποι που «παίζουν» μ' αυτό
- Να τα αποταμιεύσω ελπίζοντας ότι θα έχουν μεγαλύτερη αξία στο μέλλον

Τι ρίσκο έχει το bitcoin?

- Είσαι υπεύθυνος για τα χρήματά σου!
- Αν στα κλέψουν, στα έκλεψαν - τελείωσε
- Ενδέχεται ορισμένες κυβερνήσεις να τα καταστήσουν παράνομα
- Η διακύμανση της τιμής σε σχέση με το € είναι τεράστια
- Αν δεν έχεις ασφαλές μηχάνημα, μπορεί να πέσεις θύμα hacking

All	All	Enter address or label to search	Min amount
Date	Type	Address	Amount
✓ 2/20/14 22:01	Sent to	Stavros Messinis	-0.1185834
✓ 2/20/14 18:04	Sent to	Lydia Tsagkou	-0.02335581
✓ 2/15/14 14:24	Sent to	Themis Papameleti	-0.02210606
✓ 2/13/14 12:46	Sent to	Alex Emexezidis	-0.01265188
✓ 2/2/14 18:20	Received with	dionyziz	0.1862
✓ 1/31/14 15:02	Received with	dionyziz	0.1823
✓ 1/22/14 22:30	Sent to	gtklocker	-0.01657862
✓ 1/13/14 08:16	Received with	dionyziz	1.30922042
✓ 1/4/14 01:52	Received with	dionyziz	0.67
✓ 11/19/13 10:28	Sent to	Petros @coinbase	-4.10218609
✓ 11/19/13 09:28	Sent to	Petros @coinbase	-0.01
✓ 11/19/13 05:01	Received with	dionyziz	0.8261
✓ 10/28/13 19:29	Sent to	James (Twitter)	-2.56
✓ 10/28/13 06:01	Received with	dionyziz	0.2807
✓ 10/13/13 01:56	Received with	dionyziz	5.56538609
✓ 10/13/13 01:52	Sent to	dionyziz (Android)	-0.10
✓ 10/13/13 01:45	Received with	dionyziz	0.10
✓ 10/3/13 01:25	Sent to	(16eyGvQYSYsHPmNcuvX32objEsPQRFxv9)	-0.10
✓ 10/3/13 01:25	Sent to	(16eyGvQYSYsHPmNcuvX32objEsPQRFxv9)	-5.56538609
✓ 9/30/13 22:42	Received with	dionyziz	2.63158
✓ 9/30/13 03:41	Received with	dionyziz	2.00
✓ 9/2/13 15:48	Received with	dionyziz	0.25759289

Confirmed (5129 confirmations)
Sent to gtklocker (12CtJLCCpVjFh34NIZSyP2Pum2sptDkws)

Export



Balance 0 BTC (€0.00)

Exchange	Currency	Last
BTC-E	EUR	414.14581

Wallets

Your wallet description



0 BTC (€0.00)

New Wallet

Send

Request

Transactions

Preferences

Your address 1FLdnXgM9woJtKmFfTWhpTowf3PDgzQj7N



Label

Amount

BTC = €



New

Your receiving addresses

Label ▲	Address
	1FLdnXgM9woJtKmFfTWhpTowf3PDgzQj7N

Online

Synchronising with network...

Android Wallet demo



Your Bitcoin Address:

1GjS kw4q HTBS
hMxb xU33 fFCE
SDTo yvfY Kw



mBTC**61.88**

Received

Both

Sent

- **Feb 9** → Ody Varvounis - 9.95
- **Feb 1** → vkoukis - 1.73
- **12/19/2013** → 15oarnxoKSpb... - 2.06
- **12/4/2013** → 1CwU4DEkFW7o... - 23.10
- **11/28/2013** → 16xKFc7LaA9... - 11.10



REQUEST COINS

SEND COINS



You need to [back up your wallet!](#)



Ασφάλεια πορτοφολιού

- Μπορώ να κάνω backup το πορτοφόλι μου (αντίγραφο)
- Όλα τα backups περιέχουν τα ιδιωτικά κλειδιά
- Οποιοδήποτε backup μπορεί να χρησιμοποιηθεί για να ξοδέψω τα χρήματά μου
- Προστατεύω το πορτοφόλι μου με έναν κωδικό (συμμετρική κρυπτογράφηση ιδιωτικού κλειδιού)
- Για ασφάλεια, μπορώ να ανεβάσω το (κρυπτογραφημένο) πορτοφόλι στο Dropbox / Google Drive ή να το δώσω σε ένα φίλο μου

Πώς στέλνω bitcoins?

- Αντιγράφω την public bitcoin διεύθυνση
- Ή απλώς σκανάρω ένα QR code με το κινητό μου
- Γράφω στη συσκευή μου το ποσό που θέλω να στείλω
- Αυτό ήταν! Το ποσό φτάνει μέσα σε δευτερόλεπτα!

Αγορά με Bitcoin Demo (stickers)

Αγορά με Bitcoin Demo (domain name)

Εναλλακτικά κρυπτονομίσματα

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



Namecoin

- Δεν χρησιμοποιείται ως νόμισμα με σημαντική αξία
- Κάθε νόμισμα αντιστοιχεί σε ένα domain name
- π.χ. dionyziz.bit
- Τα νομίσματα μπορούν να ανταλλαχθούν
- Ο ιδιοκτήτης ενός νομίσματος μπορεί να το αντιστοιχίσει σε κάποια IP ή να αλλάξει την αντιστοιχία
- Η ιδιοκτησία επιβεβαιώνεται με ψηφιακή υπογραφή
- Διορθώνει όλα τα προβλήματα ιεραρχίας του DNS/PKI
- π.χ. diginotar, thepiratebay
- Απαιτεί ειδικούς DNS servers

Namecoin demo

Twister

- Decentralized Twitter
- Αποφεύγει τον κεντρικό έλεγχο από μία εταιρεία
- Κανείς δεν μπορεί να «διαγράψει» tweets
- Ακόμη και με δικαστική παρέμβαση
- Η κατοχή ονομάτων π.χ. @dionyziz παρέχεται μέσω ενός μηχανισμού σαν το namecoin
- Τα tweets διαδίδονται peer-to-peer

Ethereum

- Το ethereum είναι ένα ακόμη εναλλακτικό κρυπτονόμισμα
- Χρησιμοποιεί την ίδια ιδέα με το bitcoin, αλλά επιτρέπει να κωδικοποιήσουμε περίπλοκα συμβόλαια αστικού δικαίου
- Στο μέλλον ενδεχομένως να αντικαταστήσει το μεγαλύτερο μέρος του αστικού δικαίου
- Δεν θα υπάρχουν δικαστήρια, δικηγόροι, δικαστές για οικονομικές υποθέσεις
- Τα συμβόλαια θα είναι δεσμευτικά από πλευράς τεχνολογίας

Ethereum

- Κάθε χρήστης μπορεί να ορίσει συμβόλαιο
- Το συμβόλαιο γράφεται σε κώδικα
- Ο κώδικας «τρέχει» σε ένα peer-to-peer δίκτυο παρόμοιο με το bitcoin
- Ethereum blockchain
- Ο κώδικας κάνει enforce αυτά που λέει το συμβόλαιο
- Αποκεντρωμένα υπάρχει εγγύηση ότι θα γίνουν αυτά που γράφει
- Δεν υπάρχουν ασάφειες ή διαφορετικές ερμηνείες του κώδικα ή μικρά γράμματα - ο κώδικας είναι κώδικας

Ethereum

Παράδειγμα συμβολαίου:

- Οικονομική πλευρά ενός γάμου
- Η Alice και ο Bob συμφωνούν ότι θα παντρευτούν
- Ο Oscar είναι κουμπάρος
- Συμφωνούν ότι ο καθένας έχει προίκα 100€
- $100\text{€} + 100\text{€} = 200\text{€}$ μπαίνουν σε κοινό λογαριασμό
- Μέσω ethereum δηλώνουν πώς τα χρήματα μπορούν να ξοδευτούν

Ethereum

- **Παράδειγμα κανόνων συμβολαίου γάμου**
- Κάθε ένας από τους Alice και Bob μπορούν να ξοδέψουν ανεξάρτητα μέχρι 1€ το μήνα
- Για να ξοδευτούν περισσότερα χρειάζεται συγκατάθεση και των δύο
- Μπορεί να γίνει διαζύγιο αν συμφωνήσουν 2 από τους Alice, Bob, Oscar
- Σε περίπτωση διαζυγίου, τα χρήματα μοιράζονται 50/50 ανάμεσα στους λογαριασμούς Alice, Bob
- Ο Oscar πληρώνεται εφάπαξ 1€ αρχικά και 1€ σε περίπτωση διαζυγίου από τον κοινό λογαριασμό για τις υπηρεσίες του

Ethereum

- Σε περίπτωση διαζυγίου, δεν χρειάζεται δικαστήριο
- Είναι προσυμφωνημένο, με κώδικα, τι θα γίνει σε κάθε περίπτωση
- Το να γίνει δεν επαφύεται στην καλή θέληση των συμμετεχόντων - επιβάλλεται από τον κώδικα

Επίλογος

- Το bitcoin μπορεί να επικρατήσει ή και να μην επικρατήσει
- Η τεχνολογία του είναι σημαντική
- Θα αλλάξει τον κόσμο που δουλεύει το Internet
 - DNS (namecoin)
 - Social networks (twister)
 - Micropayments (bitcoin)
 - Chatting με privacy (bitmessage)
- Ενδεχομένως να αλλάξει:
 - Την παγκόσμια οικονομία (bitcoin)
 - Τον τρόπο που αντιμετωπίζουμε τους νόμους (ethereum)
 - Την ελευθερία του λόγου και του τύπου (twister)

Επίλογος

- Αν δεν επενδύσετε οικονομικά στο bitcoin, τουλάχιστον επενδύστε τεχνολογικά
- Μάθετε πώς δουλεύει
- Βοηθήστε μας να το βελτιώσουμε
- Βοηθήστε μας να το διαδώσουμε


Μάθαμε

- Το κρυπτονόμισμα bitcoin
- Ιστορία του bitcoin
- Πρακτική χρήση πορτοφολιών
- Δημόσια/ιδιωτικά κλειδιά
- Διπλό ξόδεμα
- Blockchain
- Άλλα κρυπτονομίσματα: Namecoin, Ethereum

Συγχαρητήρια!

- Μπορείτε να κάνετε **αγορές με bitcoin**





Ευχαριστώ! Ερωτήσεις;



Αυτές οι διαφάνειες είναι:
Creative Commons 3.0 Attribution

bitcoin.org
Twitter: @dionyziz