Bitcoin : Paying will never be the same

ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Γιώργος Σπαθούλας

Τμήμα Πληροφορικής με εφαρμογές στη Βιοϊατρική
Πανεπιστήμιο Θεσσαλίας

Λαμία

Δομή

Ηλεκτρονικό σύστημα πληρωμών

Θα σας φαινόταν ενδιαφέρον ένα ηλεκτρονικό σύστημα πληρωμών που θα ήταν :

εύχρηστο

γρήγορο

παγκόσμιο

ανεξάρτητο

προσβάσιμο

ανώνυμο

First things first...

- Εάν έχετε έρθει γιατί ακούσατε ότι μπορεί να βγάλετε εύκολα κέρδος από το **bitcoin** μάλλον θα σας απογοητεύσω ...
- Η εποχή που αυτό γινόταν (όχι τόσο εύκολα όσο νομίζετε) έχει περάσει ...
- Η σημερινή διάλεξη έχει ως στόχο :
  - να αποκτήσετε μία ιδέα για το τι είναι το **bitcoin**
  - να έρθετε σε μία πρώτη επαφή με το τεχνικό υπόβαθρο του πρωτοκόλλου
  - να σας κεντρίσει το ενδιαφέρον για να ασχοληθείτε περισσότερο

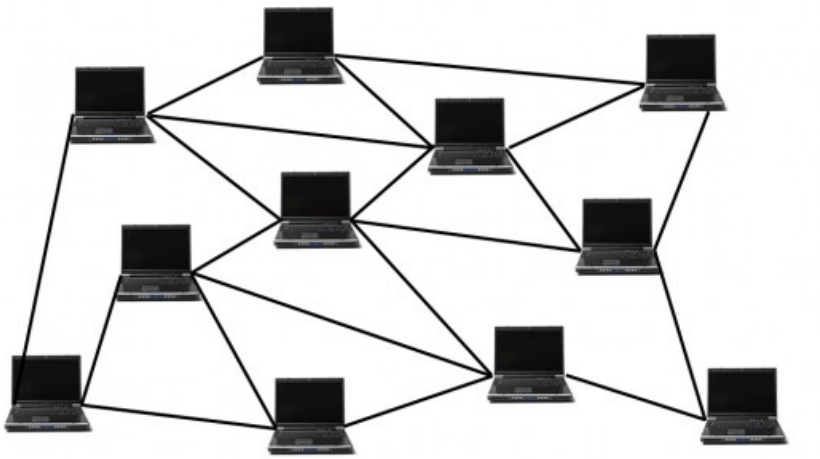
Ορισμός

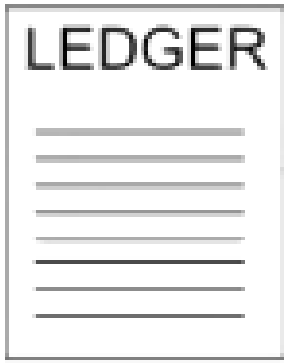
- Το **bitcoin** είναι το σύνολο των εννοιών και των τεχνολογιών που ορίζουν ένα οικοσύστημα ηλεκτρονικού χρήματος
- Η μονάδα μέτρησης του χρήματος ονομάζεται **bitcoin** και χρησιμοποιείται ώστε να μεταφερθούν ποσά από τον ένα χρήστη στον άλλο
- Οι χρήστες επικοινωνούν μέσω **internet**
- Πρόκειται για μία **p2p**, **open source** εφαρμογή
- Υπάρχει πληθώρα **clients** για όλες τις συσκευές (υπολογιστές, smartphones κτλ.)

Χρήση

- Οι χρήστες μπορούν με το **bitcoin** να κάνουν οτιδήποτε κάνουν και με τα φυσικά χρήματα
- Το **bitcoin** είναι εικονικό νόμισμα
- Οι χρήστες αποδεικνύουν την κατοχή των **bitcoins**, μέσω ενός συστήματος ψηφιακών υπογραφών δημοσίου κλειδιού
- Προσφέρει **ανωνυμία** στους χρήστες καθώς αυτοί αναγνωρίζονται από μία **διεύθυνση** άσχετη από την πραγματική τους ταυτότητα
- Η υπηρεσία είναι **p2p** και δεν υπάρχει καμία **κεντρική οντότητα** που να μπορεί να ρυθμίσει κατά οποιονδήποτε τρόπο την λειτουργία του συστήματος
- Η **δημιουργία bitcoins** είναι **προδιαγεγραμμένη** από το πρωτόκολλο και δεν ρυθμίζεται από κάποια κεντρική οντότητα

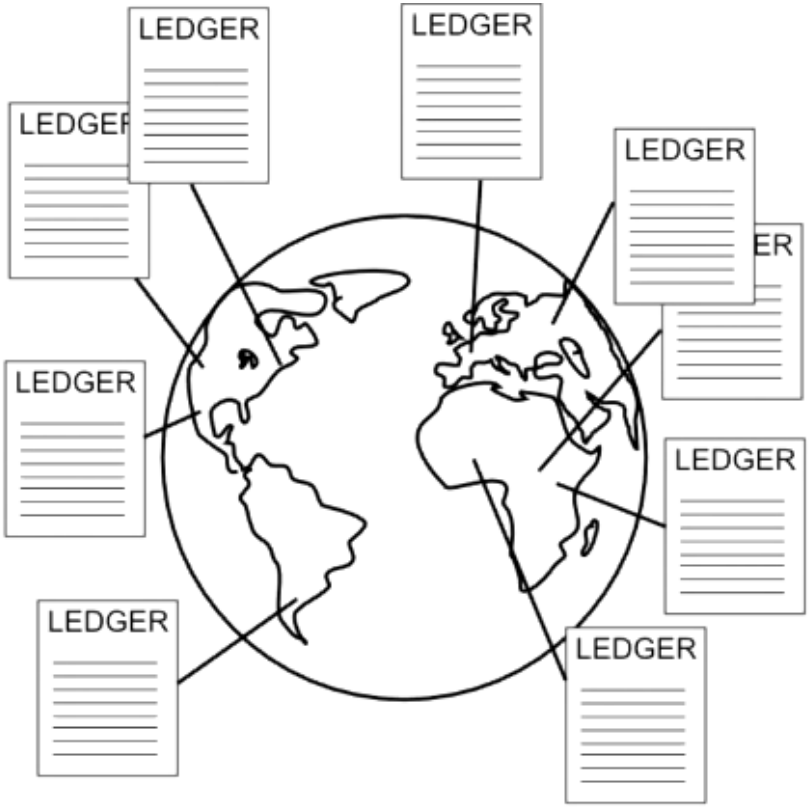
Καταγράφοντας transactions





- Συνδέουμε όλους τους **clients** σε ένα **ομότιμο p2p δίκτυο**
- Τους επιτρέπουμε να κάνουν **συναλλαγές** μεταξύ τους
- **Καταγράφουμε** σε μία **λίστα** (ledger) όλες αυτές τις **συναλλαγές**
- Αρκεί να ανατρέξουμε στην λίστα για να δούμε πόσα bitcoins έχει ο κάθε χρήστης στην διάθεσή του

Αποθήκευση του legder



- Από την φύση του δικτύου **δεν υπάρχει** κάποια **κεντρική οντότητα** στην οποία θα μπορούσε να αποθηκευθεί το legder
- Αποθηκεύουμε λοιπόν το legder **σε όλους τους κόμβους**
- Ο κάθε κόμβος ενημερώνει το δικό του αντίγραφο
- Αρκεί να ελέγξει το τοπικό του αντίγραφο για να βεβαιωθεί ότι μία συναλλαγή μπορεί να γίνει

Κεντρική ιδέα

- Οι χρήστες μπορούν να κάνουν **transactions**, μεταφέροντας **bitcoins** από τον ένα στον άλλο
- Δεν καταγράφεται πουθενά το **balance** του κάθε **λογαριασμού**
- Το μοναδικό που καταγράφεται είναι **όλα τα transactions** από την αρχή λειτουργίας του συστήματος
- Αυτή η πληροφορία αποθηκεύεται **σε όλους τους κόμβους-χρήστες** του πρωτοκόλλου
- Σήμερα το μέγεθος των μέχρι τώρα συναλλαγών είναι **52 GB** (12/2016)
- Για να μπορέσει κάποιος να κάνει μία νέα συναλλαγή πρέπει κάποια παλιότερη να πιστώνει στον λογαριασμό του το απαιτούμενο ποσό

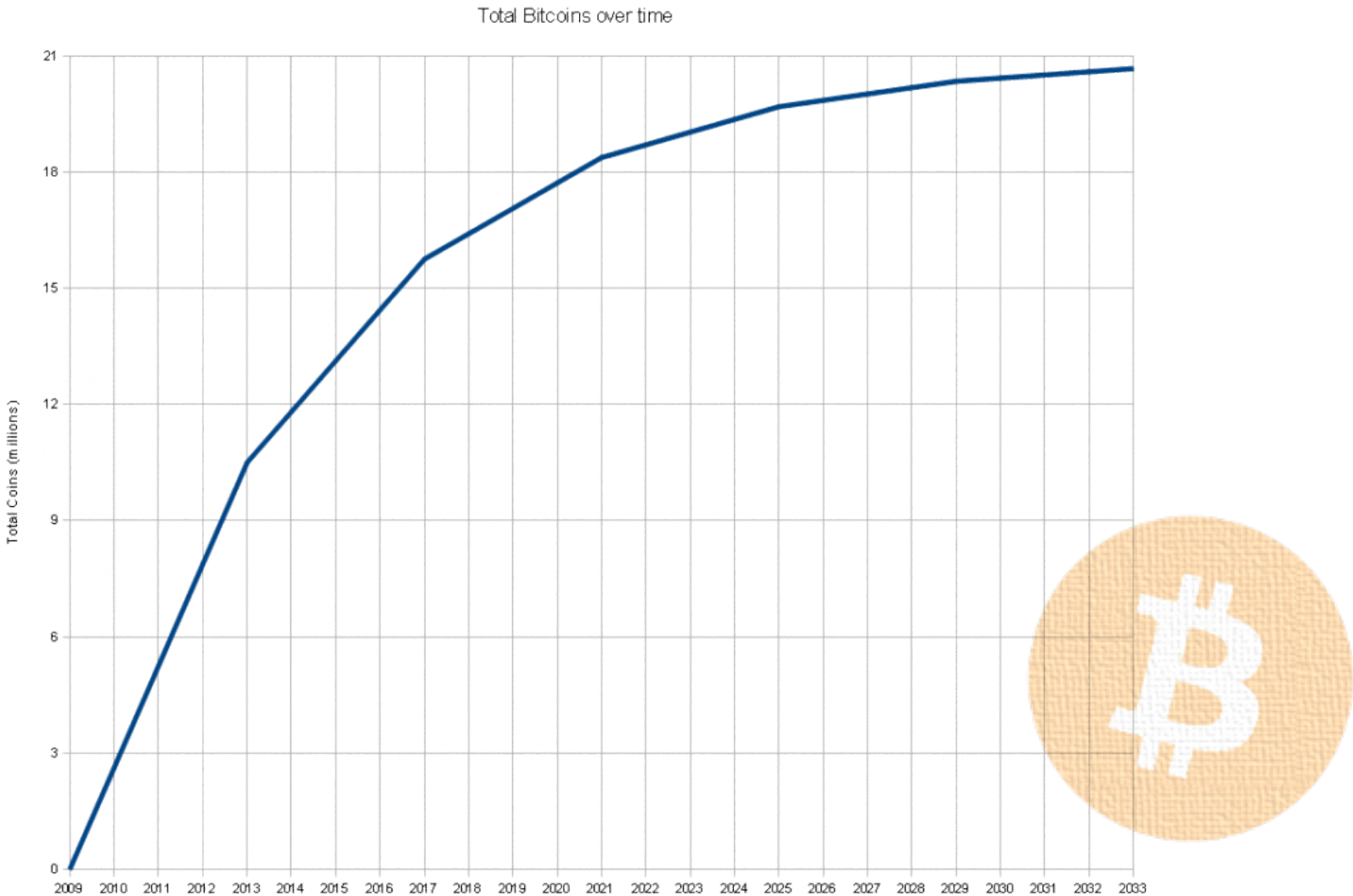
Χρήστες

- Κάθε χρήστης έχει ένα λογισμικό το οποίο ονομάζεται **wallet**
- Εκεί θεωρητικά βρίσκονται τα **bitcoins** που έχει στην κατοχή του
- Από εκεί μπορεί να στείλει μέρος τους σε κάποιον άλλο χρήστη
- Εκεί καταλήγουν τα **bitcoins** που του στέλνουν οι άλλοι
- Ο κάθε χρήστης έχει ένα **ζευγάρι κλειδιών** (δημόσιο και ιδιωτικό) και μία **διεύθυνση** η οποία παράγεται από το δημόσιο κλειδί του
- **Η χρήση του συστήματος είναι ψευδω-ανώνυμη**

Ρύθμιση πλήθους bitcoins

- Η δημιουργία των bitcoins γίνεται με συγκεκριμένο τρόπο
- Το σύστημα είναι προγραμματισμένο να παράγει bitcoins με έναν μειούμενο ρυθμό
- Συνολικά πρόκειται να παραχθούν **21.000.000 BTCs** μέχρι και το **2140**
- Σήμερα παράγονται περίπου **12.5 BTCs** κάθε **10 λεπτά**
- Ο ρυθμός αυτός **υποδιπλασιάζεται** κάθε **4 χρόνια**
- **Καμία κεντρική αρχή (πχ τράπεζα) δεν μπορεί να χειραγωγήσει το νόμισμα**

Ρύθμιση πλήθους bitcoins



Υποδιαίρεση

- Οι χρήστες μπορούν να χρησιμοποιήσουν τις υποδιαιρέσεις του bitcoin
- Η μικρότερη μονάδα είναι το 10^{-8} BTC που ονομάζεται και **shatosi**
- Έτσι τα **21.000.000 BTCs** προβλέπεται να είναι αρκετά για να καλύψουν τις ανάγκες μελλοντικά

Miners

- Βάσει μίας συγκεκριμένης διαδικασίας **χρήστες που έχουν την απαραίτητη υπολογιστική ισχύ (miners)** αναλαμβάνουν να **επικυρώνουν τις συναλλαγές** και να τις **προσθέτουν στην αλυσίδα των προηγούμενων συναλλαγών**
- Για την υπολογιστική ισχύ που καταναλώνουν **ανταμείβονται** με κάποια **BTCs**
- Αυτός είναι και ο τρόπος δημιουργίας νέων BTCs
- Στην αρχή ήταν εύκολο να κάνει κανείς mining, με τον προσωπικό του υπολογιστή
- Τώρα πια απαιτείται εξειδικευμένο hardware, και σημαντική κατανάλωση σε ηλεκτρική ενέργεια
- **Οι miners διασφαλίζουν την ορθή λειτουργία του πρωτοκόλλου**

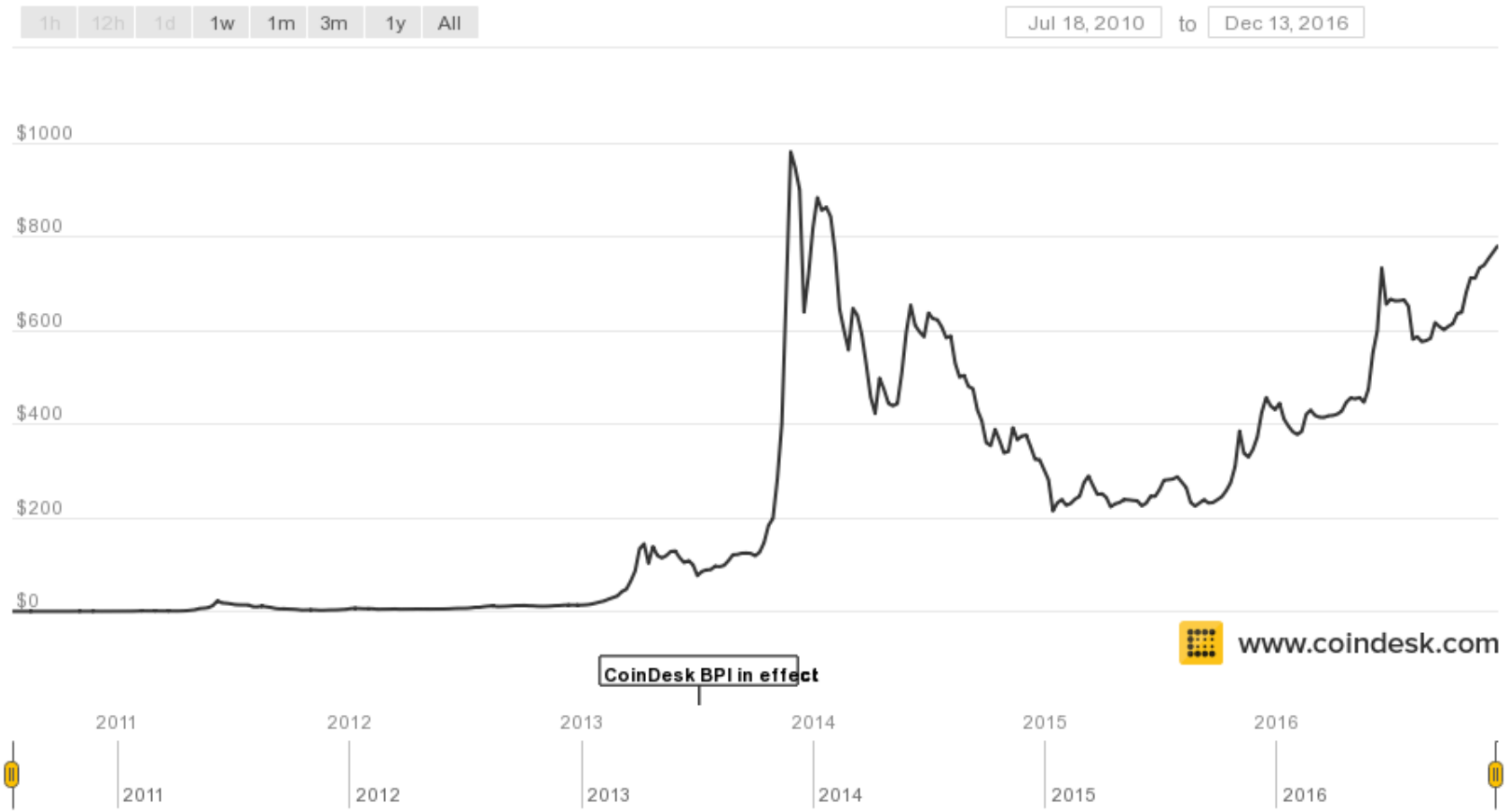
Δημιουργία

- Το **bitcoin** εφευρέθηκε το 2008 με την δημοσίευση ενός άρθρου με τον τίτλο **Bitcoin: A Peer-to-Peer Electronic Cash System** από τον **Satoshi Nakamoto**
- Ο **Satoshi Nakamoto** συνδύασε υπάρχουσες τεχνολογίες και σχεδίασε ένα πλήρως αποκεντρωμένο σύστημα ηλεκτρονικού χρήματος, τελείως ανεξάρτητο από οποιαδήποτε αρχή ελέγχου
- Λίγους μήνες μετά το 2009 υλοποίησε το σύστημα ως ένα open source project
- Η αρχική υλοποίηση αναθεωρήθηκε στην συνέχεια από μία ομάδα προγραμματιστών
- Ο **Satoshi Nakamoto** εξαφανίστηκε τον Απρίλιο του 2011
- Η αληθινή του ταυτότητα δεν έγινε ποτέ γνωστή

Αξία bitcoin

- Το **bitcoin** είναι ένα νόμισμα, ανάλογο με τα πραγματικά νομίσματα (πχ ευρώ δολάριο ή λίρα Μεγάλης Βρετανίας)
- Η αξία του καθορίζεται από την ισοτιμία του με τα άλλα νομίσματα
- Αναλόγως με την εξέλιξη του η ισοτιμία αυτή μεταβάλλεται, αλλά γενικώς διατηρεί μία ανοδική πορεία
- Η πρώτη αγορά που καταγράφηκε παγκοσμίως με **bitcoin** έγινε στις 22 Μαΐου του 2010, όταν ένας προγραμματιστής από την Φλόριντα των ΗΠΑ πλήρωσε **10.000 BTC** για **2 πίτσες**
- Τα **10000 BTC** αντιστοιχούσαν τότε με **25$**
- Σήμερα αν ο κάτοχός τους τα είχε διατηρήσει θα αντιστοιχούσαν σε περίπου **7.680.000 $** (1 BTC = 768 $)

Ιστορικό ισοτιμίας bitcoin - USD

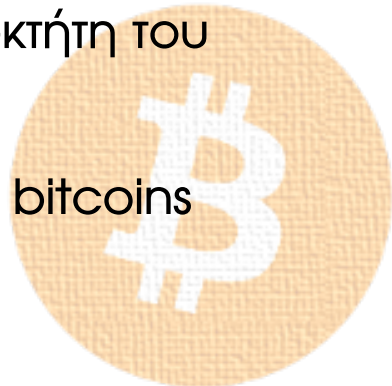


Σημαντικότερα γεγονότα

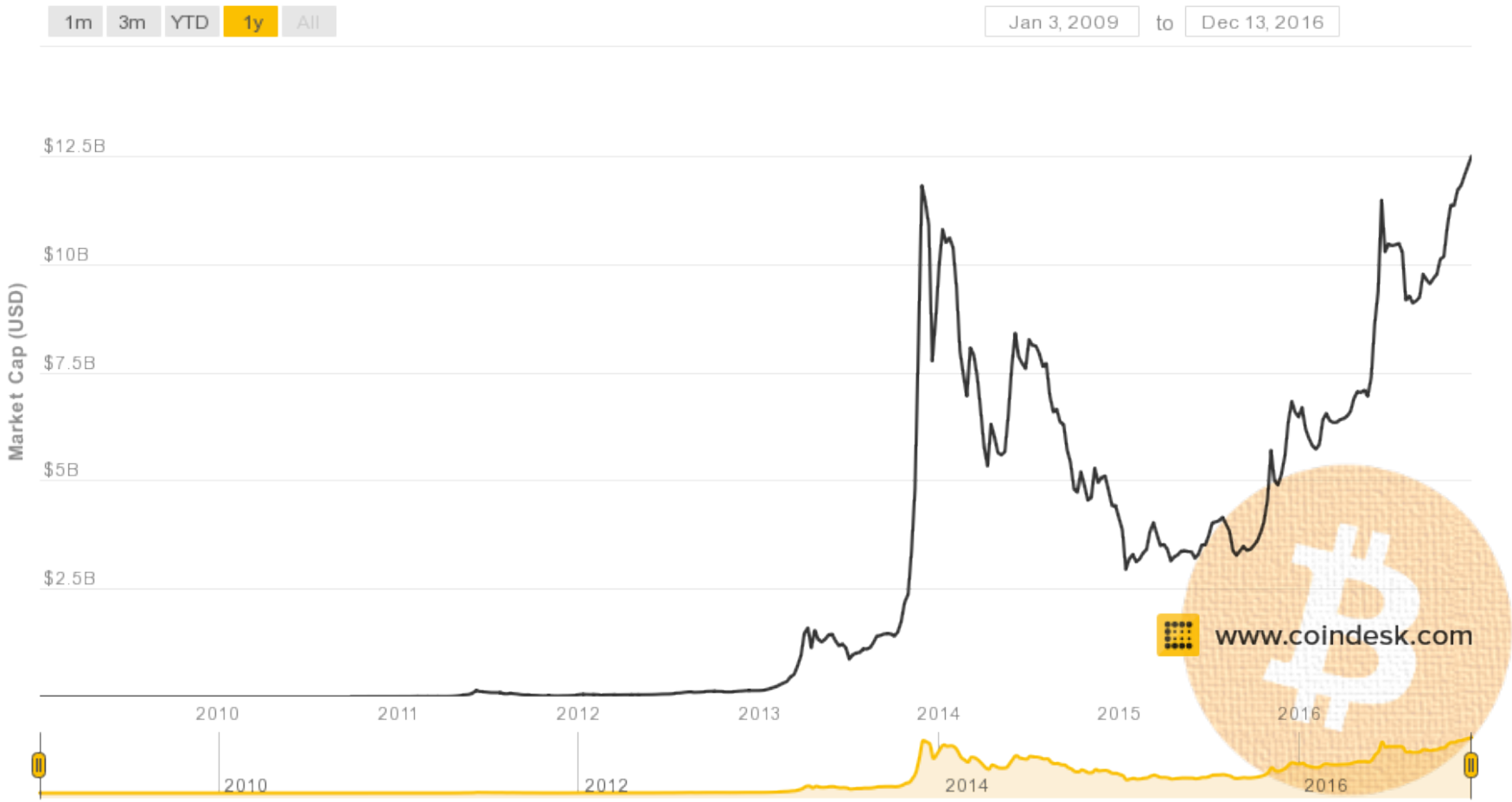
- **10/2008** Ο Satoshi Nakamoto δημοσιεύει το paper : Bitcoin: A Peer-to-Peer Electronic Cash System
- **01/2009** Το πρώτο block (genesis block) δημιουργείται
- **10/2009** Το bitcoin αποκτά για πρώτη φορά ισοτιμία με το δολάριο $1 = 1,309 BTC
- **08/2010** Ένα κενό ασφαλείας ανακαλύπτεται και δημιουργούνται 184 εκατομμύρια bitcoins
- **01/2011** Ιδρύεται Silk road, ένα ανώνυμο marketplace όπου οι συναλλαγές γινόταν σε bitcoins, και κατά βάση χρησιμοποιήθηκε για παράνομες δραστηριότητες
- **03/2013** Τα bitcoins που έχουν δημιουργηθεί έχουν φτάσει σε αξία το 1 δις δολάρια, και γενικώς το σύστημα αρχίζει να γίνεται αποδεκτό
- **11/2013** Το bitcoin συζητιέται στην Γερουσία των ΗΠΑ

Σημαντικότερα γεγονότα

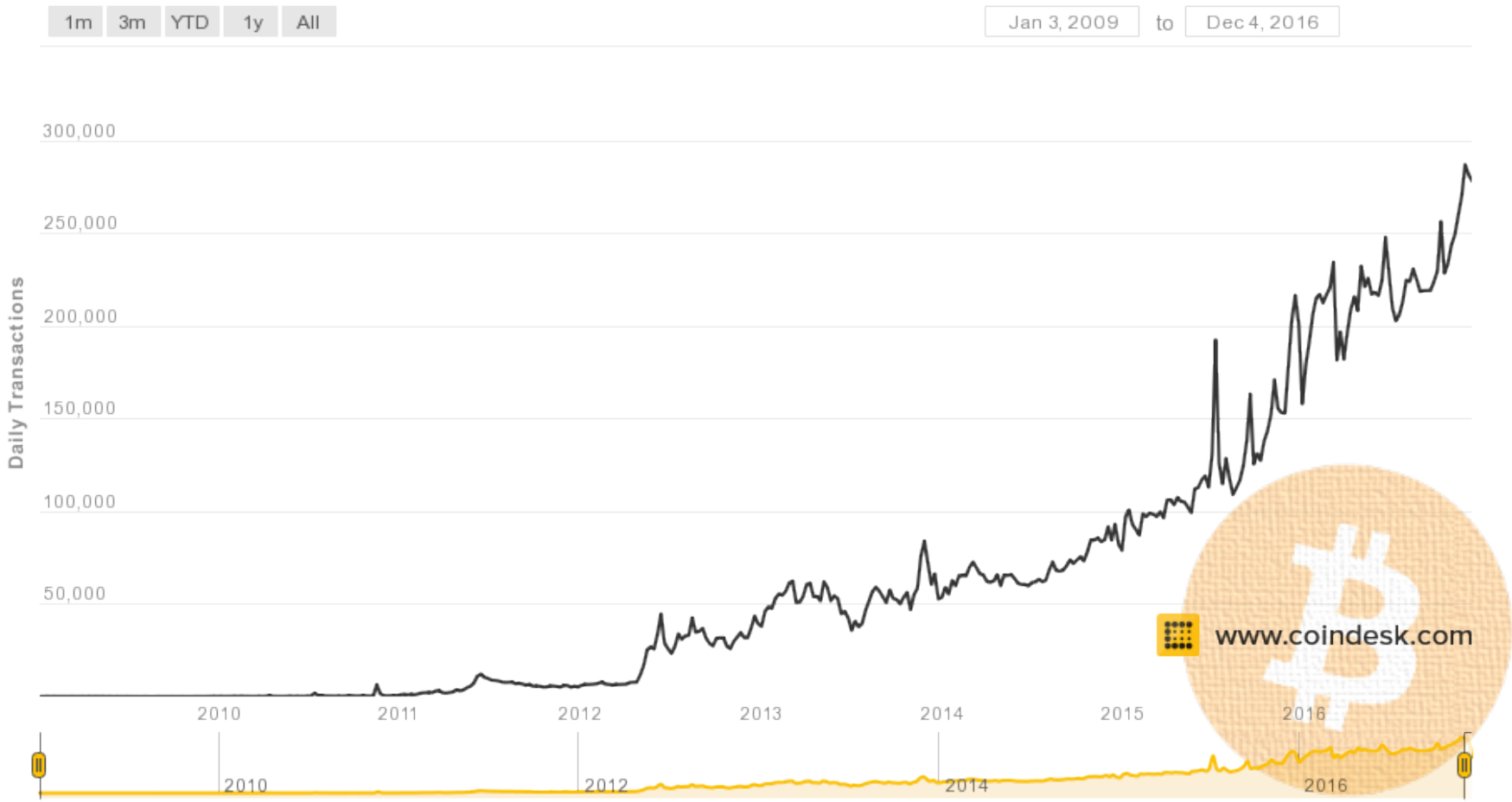
- **12/2013** Το bitcoin φτάνει στην ιστορικά υψηλότερη ισοτιμία του με το δολάριο 1124.76$ = 1 BTC
- **12/2013** Η κυβέρνηση της Κίνας κηρύσσει παράνομες τις συναλλαγές με bitcoins και η ισοτιμία σχεδόν υποτριπλασιάζεται σε λίγα 24ωρα
- **06/2014** Το FBI καταφέρνει να κλείσει το **Silk road** και δημοπρατεί τα 29,000 bitcoins που βρίσκονται στην κατοχή του ιδιοκτήτη του (εκτιμάται για ένα ποσό της τάξης των 19.000.000 $)
- **12/2014** Η Microsoft αρχίζει να δέχεται πληρωμές σε bitcoins



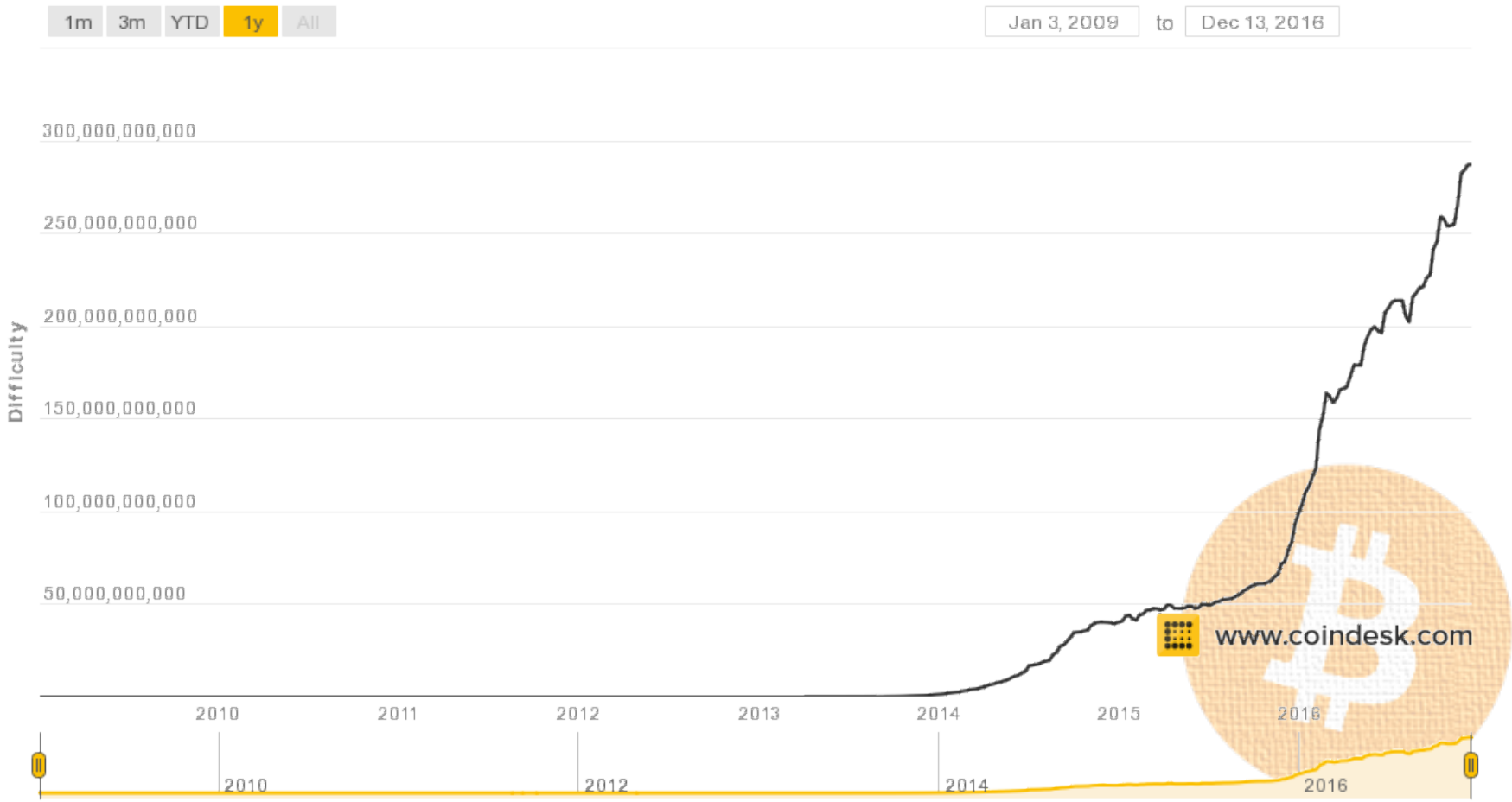
Μέγεθος αγοράς σε USD



Πλήθος transactions ανά ημέρα

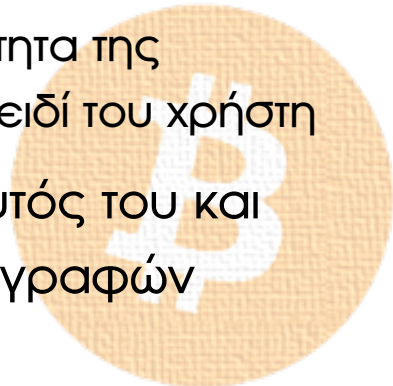


Δυσκολία mining



Σύστημα ψηφιακής υπογραφής δημοσίου κλειδιού

- Κάθε χρήστης κατέχει δύο κλειδιά:
  - **ένα δημόσιο** (γνωστό σε όλους τους άλλους)
  - και **ένα ιδιωτικό** (γνωστό μόνο στον χρήστη)
- Ότι κρυπτογραφείται με το **ιδιωτικό κλειδί** του χρήστη αποκρυπτογραφείται με το **δημόσιο κλειδί** του
- Αυτή η ιδιότητα χρησιμοποιείται με τον εξής τρόπο :
  - Ο χρήστης που θέλει να υπογράψει κάτι το κρυπτογραφεί με το ιδιωτικό του κλειδί
  - Όλοι οι υπόλοιποι μπορούν να ελέγξουν την εγκυρότητα της υπογραφής αποκρυπτογραφώντας με το δημόσιο κλειδί του χρήστη
- Έτσι ο καθένας μπορεί να υπογράψει μόνο ως ο εαυτός του και όλοι μπορούν να επικυρώσουν την ορθότητα των υπογραφών όλων των άλλων



Συναρτήσεις κατακερματισμού

- Οι συναρτήσεις κατακερματισμού είναι συναρτήσεις που δέχονται μία είσοδο οποιουδήποτε μεγέθους και παράγουν μία έξοδο σταθερού μεγέθους που ονομάζεται **σύνοψη**
- Είναι **μη αντιστρέψιμες**, δεν μπορεί κανείς από την σύνοψη να παράγει την είσοδο της συνάρτησης
- Αφού η σύνοψη έχει σταθερό μέγεθος υπάρχει η **πιθανότητα συγκρούσεων**
- Η παραμικρή αλλαγή στην είσοδο (έστω ενός χαρακτήρα) έχει ως αποτέλεσμα να αλλάζει **τελείως** η παραγόμενη σύνοψη

Blockchain

- Όλα τα **transactions** προστίθενται από τους **miners** σε κάποιο **block**
- Τα **blocks** αυτά έχουν μία σειρά από την αρχή δημιουργίας του συστήματος
- Συνολικά περιέχουν όλα τα **transactions** από καταβολής του **bitcoin**

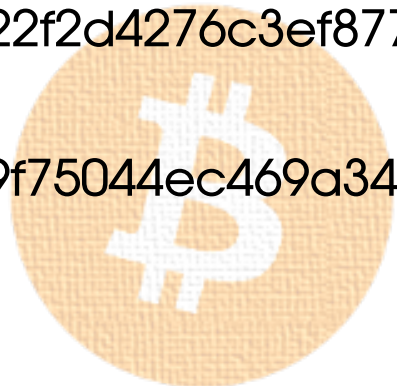
Δημιουργία block

- Μετά την δημιουργία ενός **block** όλοι οι **miners** αρχίζουν να προσπαθούν να κατασκευάσουν το επόμενο
- Ο πρώτος που θα το καταφέρει προωθεί το **νέο block** σε όλους τους υπόλοιπους
- Το **νέο block** σχετίζεται με το προηγούμενό του καθώς περιέχει το **hash** του
- Αν κάποιος προσπαθήσει να αλλάξει ένα **block** για ιδιοτελείς σκοπούς τότε θα πρέπει να αλλάξει και **τα επόμενα** καθώς το καθένα εμπεριέχει το **hash** του προηγούμενου

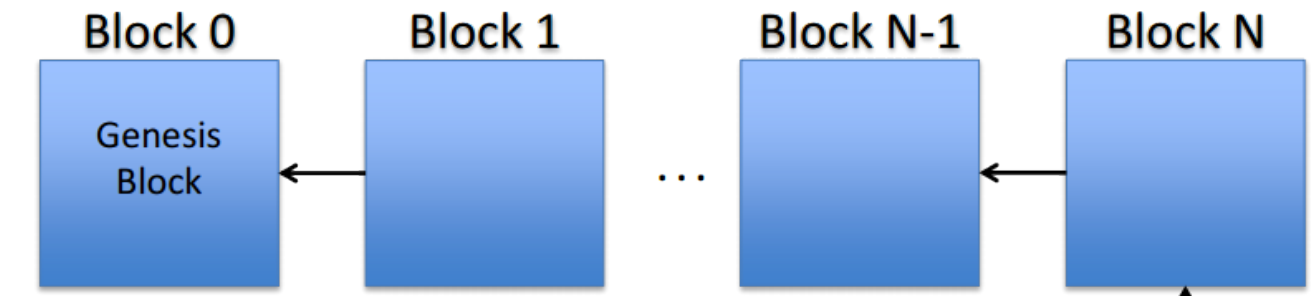
SHA-256

- Είναι μία συνάρτηση κατακερματισμού
- Έχει έξοδο 32 bit
- Η παραμικρή αλλαγή στην είσοδο προκαλεί μεγάλη αλλαγή στην έξοδο

sha256("I would like 10 bitcoins please") =
"313ff09d53623d9f3c05b4be12255963932856 6c3cca3a7622f2d4276c3ef877"
sha256("I would like 10 bitcoins please!") =
"617b0a3d0a47332f000c8a5183f0e72248fd13885a21534c9f75044ec469a34f"



Δημιουργία block



How to create a new block?

Block Header

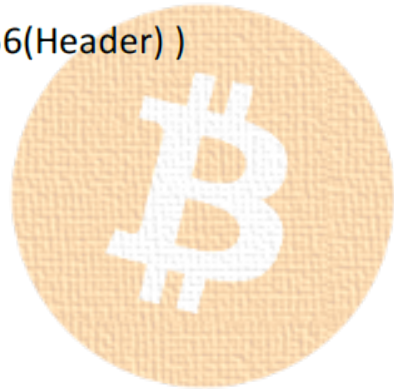
- Version
- **Previous Block Hash**
- Merkle Root
- Time Stamp
- Bits
- Nonce

80 byte header
Block Hash = Sha256(Sha256(Header))
But there is a catch…

Payload

- Transactions

Variable size



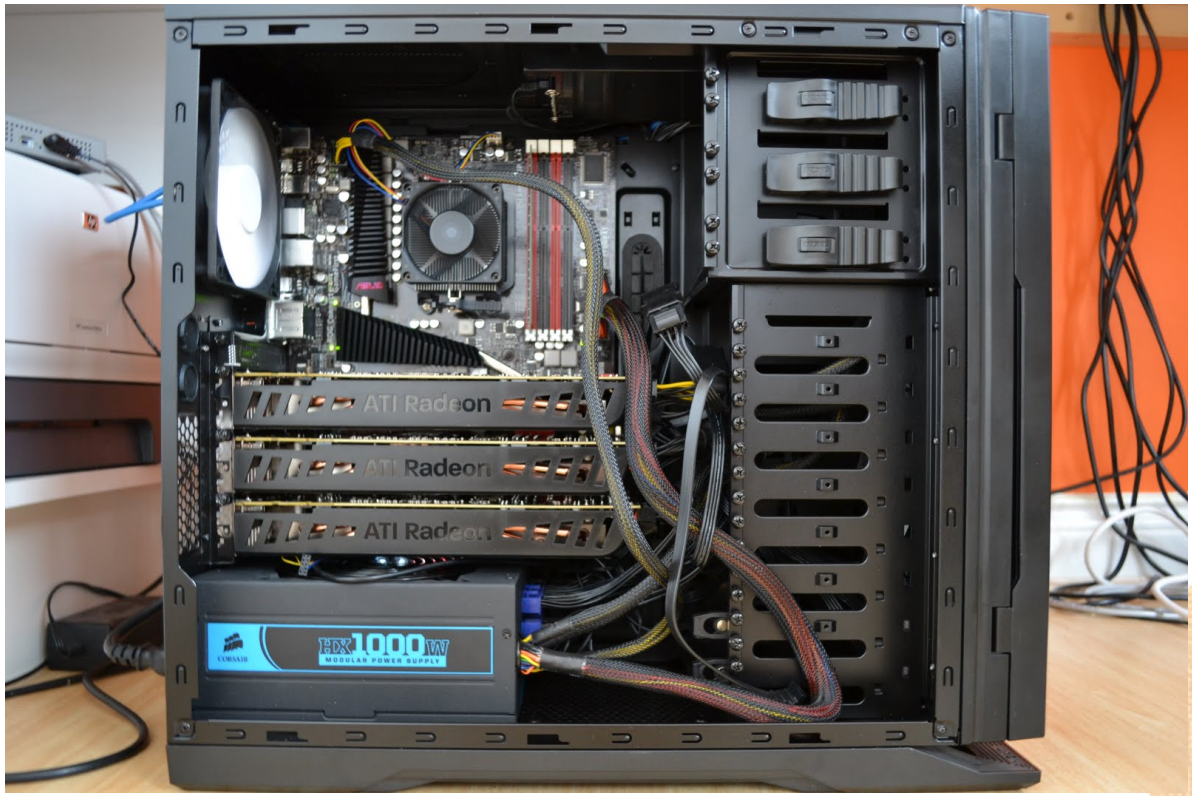
Proof of work

- Η δημιουργία του **block** είναι απλή υπόθεση όσον αφορά το υπολογιστικό κόστος
- Από τον σχεδιασμό όμως του **bitcoin** δεν αρκεί μόνο αυτό για να φτιάξει ένας **miner** ένα νέο **block**
- Απαιτείται το **hash** του **block** να είναι **μικρότερο** από μία **συγκεκριμένη τιμή** (ή αλλιώς να έχει ένα συγκεκριμένο αριθμό πρώτων bytes ίσο με το μηδέν)
- Επίσης η ποσότητα **nonce** είναι μία τυχαία ποσότητα που ορίζει ο miner
- Πρακτικά ο miner αφού φτιάξει το block δοκιμάζει πολλές τυχαίες τιμές για το **nonce** μέχρις ότου προκύψει για κάποια από αυτές αποδεκτό **hash**

Proof of work

- Η προσπάθεια που καταβάλλει ο **miner** λέγεται **proof of work**
- Προσδίδει δύο βασικές ιδιότητες στο πρωτόκολλο
  - Αναλόγως με την συνολική ισχύ του δικτύου των **miners** αλλάζει το όριο των αποδεκτών **hash** τιμών και έτσι συντηρείται **ο ρυθμός παραγωγής blocks σε 1 block / 10 λεπτά** και κατά συνέπεια συντηρείται και ο **ρυθμός παραγωγής bitcoins**
  - Επίσης καθίσταται **πολύ δύσκολο υπολογιστικά** να δοκιμάσει να **αλλάξει** κάποιος τα **ήδη δημιουργημένα blocks** με σκοπό να αναιρέσει κάποιο transaction του παρελθόντος
- Σήμερα το δίκτυο των miners έχει **πολλαπλάσια υπολογιστική ισχύ**, σε σχέση με τους ισχυρότερους υπερ-υπολογιστές του κόσμου

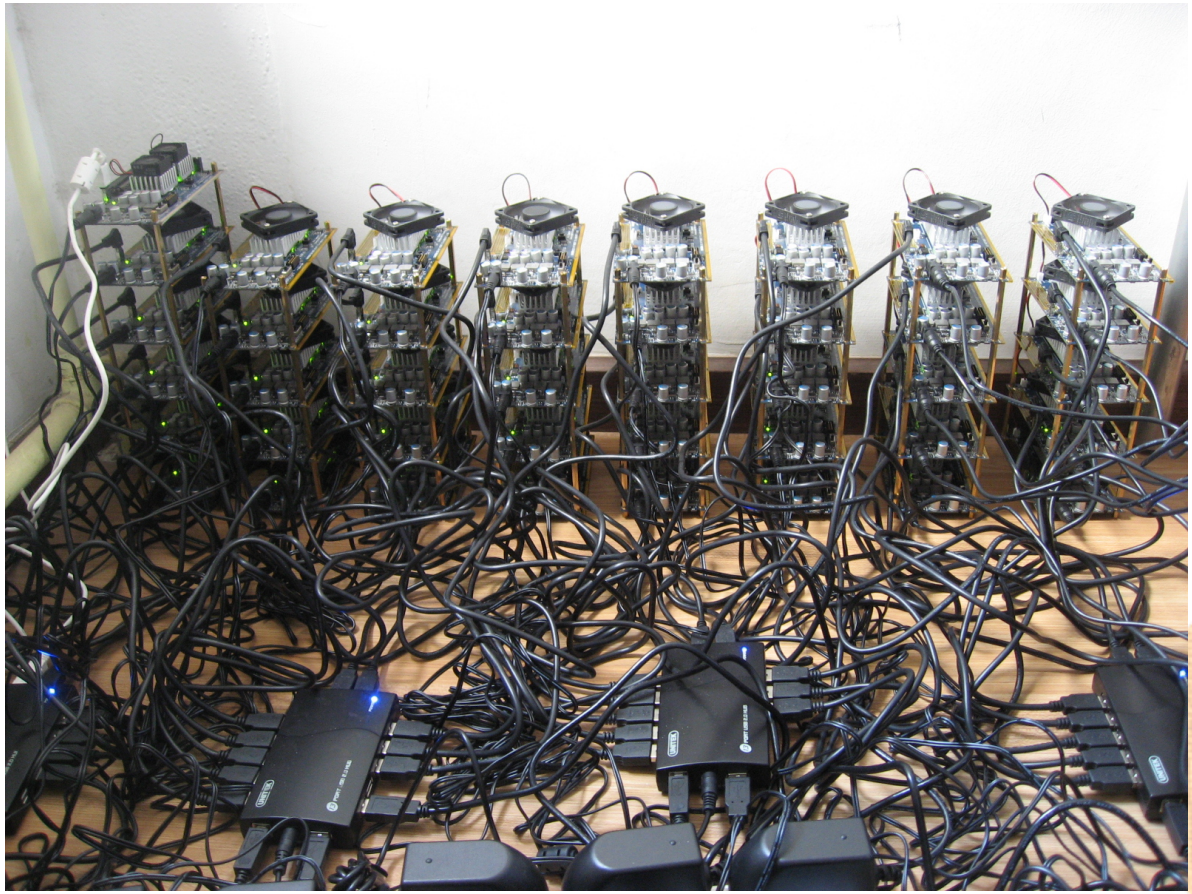
Mining history



Mining history

Mining history

Mining history



Mining history

Mining history

Mining history

... εξακολουθείτε να πιστεύετε ότι μπορείτε να γίνετε πλούσιοι από το **bitcoin mining** ...

Transactions

- Τα **transactions** αποτελούν το βασικό δομικό λίθο του πρωτοκόλλου
- Μεταφέρουν **bitcoins** μεταξύ των **χρηστών**
- Αποτελούνται από
  - **inputs**, που είναι παλιότερα **transactions** που έχουν ως αποδέκτη τον χρήστη που τώρα δημιουργεί το νέο **transaction**
  - και από **outputs** που δηλώνουν το πλήθος των **bitcoins** που θα σταλούν στον τρέχον **transactions** και τον αντίστοιχο αποδέκτη

Ένα απλό transaction

#tx 57
Αλίκη

Inputs	Outputs
	5 BTC Βύρων

- Έστω ότι η **Αλίκη** θέλει να στείλει στον **Βύρωνα 5 BTC**
- Κατασκευάζει ένα **transaction** στα **outputs** του οποίου προσθέτει ότι θέλει να στείλει **5 BTC** στον **Βύρωνα**

Η Αλίκη ελέγχει τα BTC της

#tx 12
Νεφέλη

Inputs	Outputs
.....	4 BTC Αλίκη
.....	
.....	

#tx 32
Βρασίδας

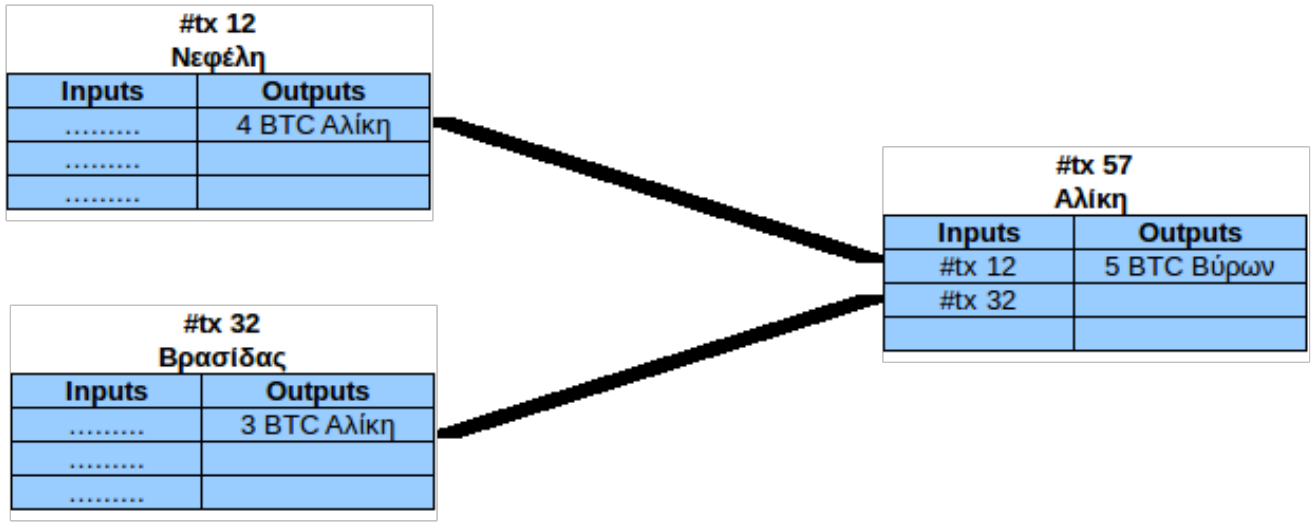
Inputs	Outputs
.....	3 BTC Αλίκη
.....	
.....	

#tx 57
Αλίκη

Inputs	Outputs
	5 BTC Βύρων

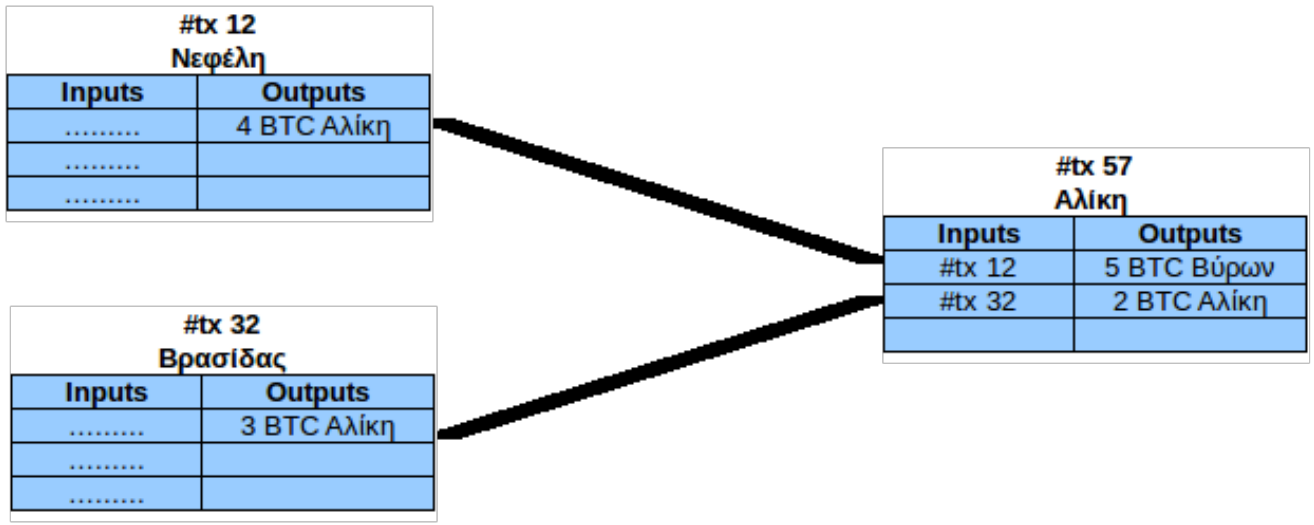
- Η **Αλίκη** πρέπει να έχει στην κατοχή της τα **5 BTC**
- Στο σύστημα είναι καταγεγραμμένα όλα τα transactions του παρελθόντος
- Οπότε η **Αλίκη** ως **inputs** χρησιμοποιεί **transactions** που **δεν έχει ξοδέψει** και αθροίζουν στο λογαριασμό της **τουλάχιστον 5 BTC**

Η Αλίκη ξοδεύει τα BTC της



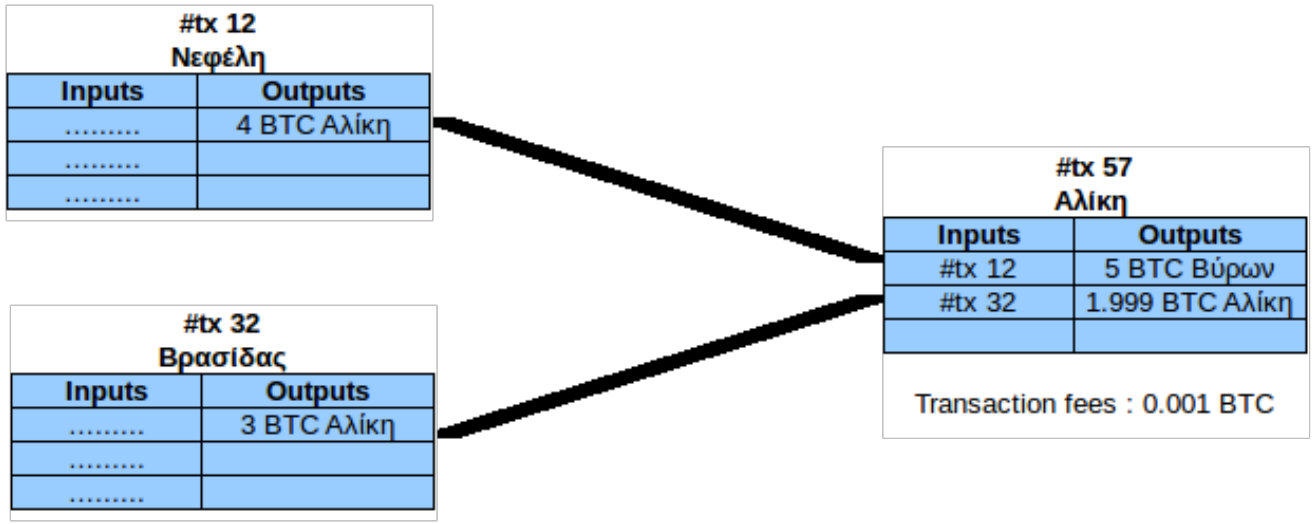
- Οπότε η **Αλίκη** ως inputs χρησιμοποιεί προηγούμενα transactions που δεν έχει ξοδέψει και αθροίζουν στο λογαριασμό της τουλάχιστον **5 BTC**
- Εν προκειμένω, τα δύο transactions **#tx12** και **#tx32** αθροίζουν στο λογαριασμό της **Αλίκης 7 BTC**

Η Αλίκη ζητάει τα ρέστα της



- Αν τα **inputs** έχουν ακριβώς άθροισμα **5 BTC** τότε το **transaction** είναι σχεδόν έτοιμο
- Συνήθως όμως αυτό δεν θα ισχύει και η Αλίκη θα πρέπει να **επιστρέφει την διαφορά στον εαυτό της** ως ένα ακόμα **output**

Who pays the miner...?



- Η **Αλίκη** μπορεί να αφήσει ένα **transaction fee** (μία μικρή διαφορά μεταξύ των **inputs** και των **outputs**), ως αμοιβή για τον **miner**
- Όσο **μεγαλύτερο** είναι το **transaction fee** τόσο **μεγαλύτερη** είναι και η **πιθανότητα** το **transaction** να ενσωματωθεί **άμεσα** σε κάποιο **block**

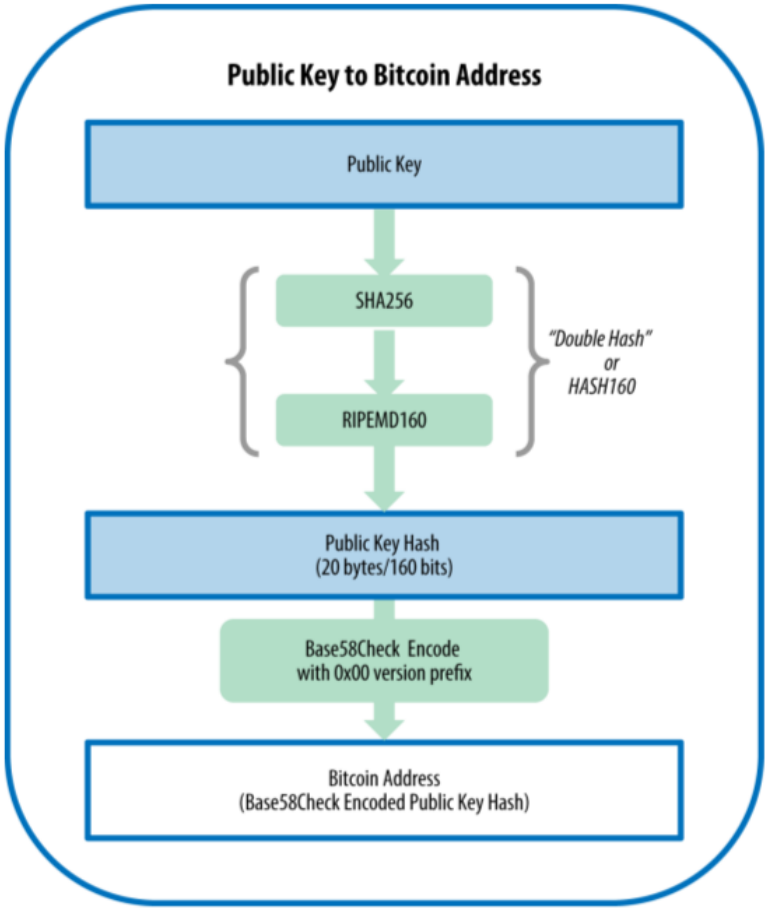
Wallet

- Είναι ο **client** που απαιτείται για την χρήση του πρωτοκόλλου
- Το **wallet** είναι το ηλεκτρονικό ανάλογο του παραδοσιακού πορτοφολιού
- Περιέχει **εικονικά** όλα τα **bitcoins** που ο χρήστης έχει στην κατοχή του
- Στην πραγματικότητα το μόνο που περιέχει ως πληροφορία για τον χρήστη είναι :
  - το ιδιωτικό του κλειδί
  - το δημόσιο κλειδί του
  - και την διεύθυνσή του

Ιδιωτικό κλειδί

- Κατά την δημιουργία του λογαριασμού επιλέγεται ένα **τυχαίο ιδιωτικό κλειδί**
- Είναι ένας ακέραιος στο διάστημα $(0, 10^{77})$
- Πρόκειται για μια μία τυχαία επιλογή, αλλά λόγω του μεγέθους του κλειδοχώρου η πιθανότητα συγκρούσεων είναι πρακτικά μηδενική
- Για να απαριθμήσει κανείς όλα τα πιθανά κλειδιά θα χρειαζόταν
  - 1**.000.000 φορές την ηλικία του σύμπαντος**, αν μπορούσε να δοκιμάζει 1 τρισεκατομμύριο κλειδιά το δευτερόλεπτο
  - την **ενέργεια** που παράγει ο **ήλιος** μέσα σε **32 χρόνια**
- Τα ιδιωτικά κλειδιά εκφράζονται στην μορφή **Wallet Import Format (WIF)**
- Παράδειγμα ιδιωτικού κλειδιού : 5KJvsngHeMpm884wtkJNzQGaCErckhHJBGFsvd3VyK5qMZXj3hS

Δημόσιο κλειδί και διεύθυνση



- Το **δημόσιο κλειδί** του λογαριασμού προκύπτει ως **σύνοψη** του **ιδιωτικού κλειδιού**
- Η **διεύθυνση** του λογαριασμού προκύπτει ως **σύνοψη** του **δημόσιου κλειδιού**
- Οπότε δεν μπορεί κανείς να εξάγει τα κλειδιά από την διεύθυνση, και επίσης δεν μπορεί να εξάγει το ιδιωτικό κλειδί από το δημόσιο

Κλειδώνοντας τα output του transaction

- Για την ορθή λειτουργία του πρωτοκόλλου χρησιμοποιείται μία script γλώσσα, που ονομάζεται **Script** και βασίζει την λειτουργία της σε μία στοίβα
- Όταν λοιπόν κάποιος δημιουργεί ένα **transaction** κλειδώνει το κάθε **output**, ώστε να μπορεί να χρησιμοποιηθεί μόνο από τον **σωστό παραλήπτη**
- Συνοδεύει το **output** με ένα **script (locking script)** που περιλαμβάνει την **διεύθυνση του παραλήπτη**
- Ο παραλήπτης κατασκευάζει ένα άλλο **script (unlocking script)** που περιέχει την **υπογραφή του hash του transaction**, καθώς και το **δημόσιο κλειδί του**

Κλειδώνοντας τα output του transaction

- Ο συνδυασμός των δύο αυτών **scripts** πρέπει να δίνει **1 (true)**, ώστε να μπορεί ο παραλήπτης να το χρησιμοποιήσει ως **input** σε ένα νέο **transaction** που θα κάνει μελλοντικά
- Τα **locking/unlocking scripts**, είναι ίσως το πιο τεχνικά περίπλοκο μέρος όλου του πρωτοκόλλου
- Από την άλλη όμως είναι **κομβικής σημασίας**, καθώς η **ευελιξία** που δίνει η συγγραφή **scripts ελέγχου**, επιτρέπουν **πιο περίπλοκες διαδικασίες**
- Για παράδειγμα με την χρήση των P2SH scripts είναι εφικτό να απαιτείται επικύρωση **m από n υπογραφών** σε ένα output

Smart contracts or Bitcoin 2.0

- Η δυναμική του **Bitcoin** είναι τα **smart contracts** ή αλλιώς **programmable money**
- Είτε πάνω στην πλατφόρμα του **Bitcoin** είτε δημιουργώντας νέα ηλεκτρονικά νομίσματα το **community** εργάζεται πάνω στην ιδέα να φτιαχτούν πιο πολύπλοκα **transactions** σε σχέση με τις συνθήκες εκτέλεσης
- Θεωρητικά θα μπορούσε αυτό το σύστημα να αντικαταστήσει τα συμβατικά συμβόλαια
- Μία άλλη κατεύθυνση είναι το **smart property**, η **ανταλλαγή ιδιοκτησίας** πάνω από το πρωτόκολλο αντί για την απλή ανταλλαγή **bitcoins**

Υπογράφοντας το transaction

- Όταν κάποιος χρήστης φτιάξει ένα **transaction** πρέπει να το υπογράψει ώστε να αποδείξει ότι είναι αυτός που κατέχει την διεύθυνση στην οποία κατευθύνονται τα **transactions** που έχει συμπεριλάβει ως **inputs**:
  - Υπογράφει το **hash** του **transaction** με το **ιδιωτικό του κλειδί** (ότι κρυπτογραφείται με το ιδιωτικό κλειδί αποκρυπτογραφείται με το αντίστοιχο δημόσιο)
  - Συμπεριλαμβάνει στο transaction την **υπογραφή**

Επικυρώνοντας το transaction

- Όταν κάποιος λάβει **transaction** το επικυρώνει εξής:
  - Αποκρυπτογραφεί την υπογραφή του αποστολέα με το δημόσιο κλειδί του
  - Αν το αποτέλεσμα συμπίπτει με το **hash** του **transaction** τότε το δημόσιο κλειδί όντως ανήκει στον αποστολέα
  - Οπότε το **transaction** έχει δημιουργηθεί όντως από αυτόν

Mining

- Κάποιοι κόμβοι (**miners**) τρέχουν την διαδικασία του **mining**
- Όταν κάποιος από τους **miners** ανακαλύψει το επόμενο έγκυρο block το προωθεί σε όλο το p2p δίκτυο
- Όλοι οι **miners** ανατρέχουν στα **ανεπιβεβαίωτα transactions** και επιλέγουν κάποια από αυτά για να φτιάξουν το νέο **block**
- Κάποιος από αυτούς σε περίπου **10 λεπτά** θα τα καταφέρει και θα πάρει ως ανταμοιβή **25 BTC** και όποιο **transaction fee** έχουν τα **transactions** που έχει συμπεριλάβει στο **block**
- Οι **miners** επιλέγουν αυτοί τα transactions, για αυτό και το **transaction fee** σχετίζεται με την ταχύτητα επιβεβαίωσης του **transaction**

Προσθήκη transactions στα blocks

- Κάποιος **κόμβος** δημιουργεί ένα νέο **transaction**
- Το προωθεί μέσω του δικτύου p2p σε όλους τους κόμβους του δικτύου
- Όποιος το λαμβάνει τσεκάρει ότι είναι έγκυρο και ότι τα παλιά **outputs** με τα οποία σχετίζεται δεν έχουν ξαναχρησιμοποιηθεί και το αποθηκεύει ως **ανεπιβεβαίωτο transaction**
- Το **transaction** αναμένει να συμπεριληφθεί σε κάποιο από τα επόμενα block που θα γίνουν mined και τότε φεύγει από τα **ανεπιβεβαίωτα** και πια είναι μέρος του **blockchain**

Πότε ένα transaction είναι OK;

- Κάθε ένα **block** που προστίθεται στο **blockchain** από εκεί και πέρα αυξάνει το βαθμό εμπιστοσύνης στο **transaction**
- Για να μπορέσει κανείς να αναιρέσει ένα **transaction** του παρελθόντος πρέπει να επιδοθεί σε ένα αγώνα δρόμου με το **υπόλοιπο δίκτυο miners** και να καταφέρει να υπολογίσει πριν από αυτούς όλα τα **blocks** από το **block** του **transaction** και μετά
- Δεδομένου του μεγέθους του δικτύου των miners και της υπολογιστικής του ισχύος αυτό είναι σχεδόν απίθανο
- Ο **Satoshi** ισχυρίστηκε ότι **6 blocks** είναι αρκετά για να θεωρήσουμε ότι ότι προηγείται πριν από αυτά είναι **σίγουρα έγκυρο transaction**
- Τα 6 blocks χρονικά ισοδυναμούν με **μία ώρα**
- Για μικρά ποσά συνήθως οι χρήστες κάνουν αμέσως δεκτή την πληρωμή ή το πολύ μετά από 1 block

Momentum

- Το **monentum** του **bitcoin** μοιάζει σήμερα, τον Μαίο του 2015 ιδιαίτερα καλό
- Δεν υπάρχει η φρενίτιδα σε όρους ισοτιμίας που υπήρξε στο τέλος του 2013
- Αντιθέτως από τις αρχές του έτους υπάρχει μία πιο ορθολογική διακύμανση στην ισοτιμία με το δολάριο
- Υπάρχουν όμως πολλά άλλα ποιοτικά στοιχεία που δείχνουν την δυναμική του **bitcoin**
- Το 2014 οι αριθμοί των :
  - των σχετικών startup εταιρειών
  - των σχετικών ακαδημαικών paper
  - των commits στα σχετικά open source projects

  εκτοξεύθηκαν σε σχέση με τα προηγούμενα χρόνια

Autonomous computing

- Το **bitcoin** είναι ένα σημαντικό βήμα προς το **Autonomous computing**
- Θεωρητικά θα μπορούσαμε να έχουμε **agents** που θα μπορούσαν να λειτουργούν εμπορικά (να συναλλάσσονται με άλλους **agents** ή **ανθρώπους**)
- Οπότε θα μπορούσε κάποιος να δημιουργήσει κάποιον **agent** που να εργάζεται για αυτόν ή ..... θα μπορούσε κάποιος **agent** να προσλάβει κάποιον άνθρωπο και να τον πληρώνει

Ανοιχτά θέματα

- Η χρήση της ιδέας του **blockchain** σε άλλους τομείς (**dns - namecoin, voting** κτλ)
- Η ενίσχυση του **bitcoin** με μηχανισμούς που θα προσφέρουν **πλήρη ανωνυμία**
- Η **ανάλυση του γράφου των transactions** με σκοπό την εξαγωγή συμπερασμάτων για την λειτουργία του πρωτοκόλλου
- **Smart contracts / Smart property**

...το **bitcoin** ως **νόμισμα** μπορεί να είναι ένα αστείο, είναι πολύ πιθανό σε δύο χρόνια να μην υπάρχει...

...η **τεχνολογία** όμως πίσω από το **bitcoin** είναι σπουδαία και είναι εδώ για να μείνει...

...ας κάνουμε το **internet** όπως έπρεπε εξ αρχής να είναι...

decentralize it

Βιβλιογραφία

- **Mastering Bitcoin: Unlocking Digital Cryptocurrencies**, Andreas Antonopoulos
- **"Bitcoin: A peer-to-peer electronic cash system."**, Nakamoto, Satoshi, Consulted 1.2012 (2008): 28.
- **How the Bitcoin Protocol Actually Works**, Jan Moller