Corelab
Computation and Reasoning Laboratory

BITCOIN

Διαφάνειες: Δημήτρης Καρακώστας – Διονύσης Ζήνδρος

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Τι είναι το Bitcoin?

Bitcoin

- Ψηφιακό νόμισμα
- Επιτρέπει να στέλνουμε χρήματα μέσω Internet

Πλεονεκτήματα του bitcoin

- Άμεση μεταφορά χρημάτων (< 1 sec)
  - Αντί 1 - 2 ημερών για τοπικές τραπεζικές συναλλαγές
  - ή 20 ημερών για διεθνείς τραπεζικές συναλλαγές
- Γρήγορη διασφάλιση συναλλαγών (10 min)
  - Αντί για 3 μήνες για διεθνείς τραπεζικές συναλλαγές ή PayPal (chargebacks)
- Ασφάλεια μέσω κρυπτογραφικών και μαθηματικών ιδιοτήτων
  - Αντί για ασφάλεια παραχάραξης μέσω χημικών / φυσικών ιδιοτήτων
- Πολύ μικρότερες χρεώσεις (~ €0.01 / συναλλαγή ανεξαρτήτως ποσού)
  - Αντί για €5 χρέωση ανά €50 μεταφοράς στην ίδια χώρα της Western Union
  - Αντί για €15 + min(€300, max(€15, 0.25% * amount)) από την Τράπεζα Πειραιώς για ξένες χώρες

Πλεονεκτήματα του bitcoin

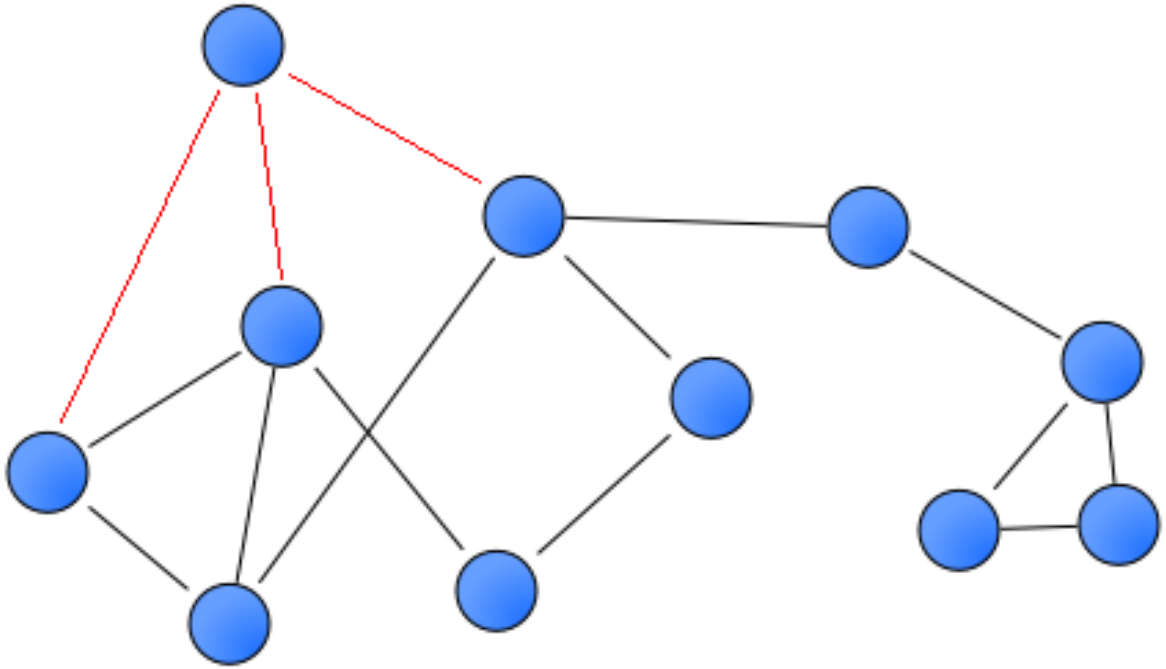
- Πραγματικά ιδιόκτητο χρήμα
  - Δεν ελέγχεται από κεντρικές τράπεζες όπως Federal Reserve ($) ή Ευρωπαϊκή Κεντρική Τράπεζα (€)
  - Δεν επιδέχεται μακροοικονομικό πληθωριστικό έλεγχο
- Δεν μπορεί να λογοκριθεί
  - βλ. υπόθεση PayPal/Wikileaks

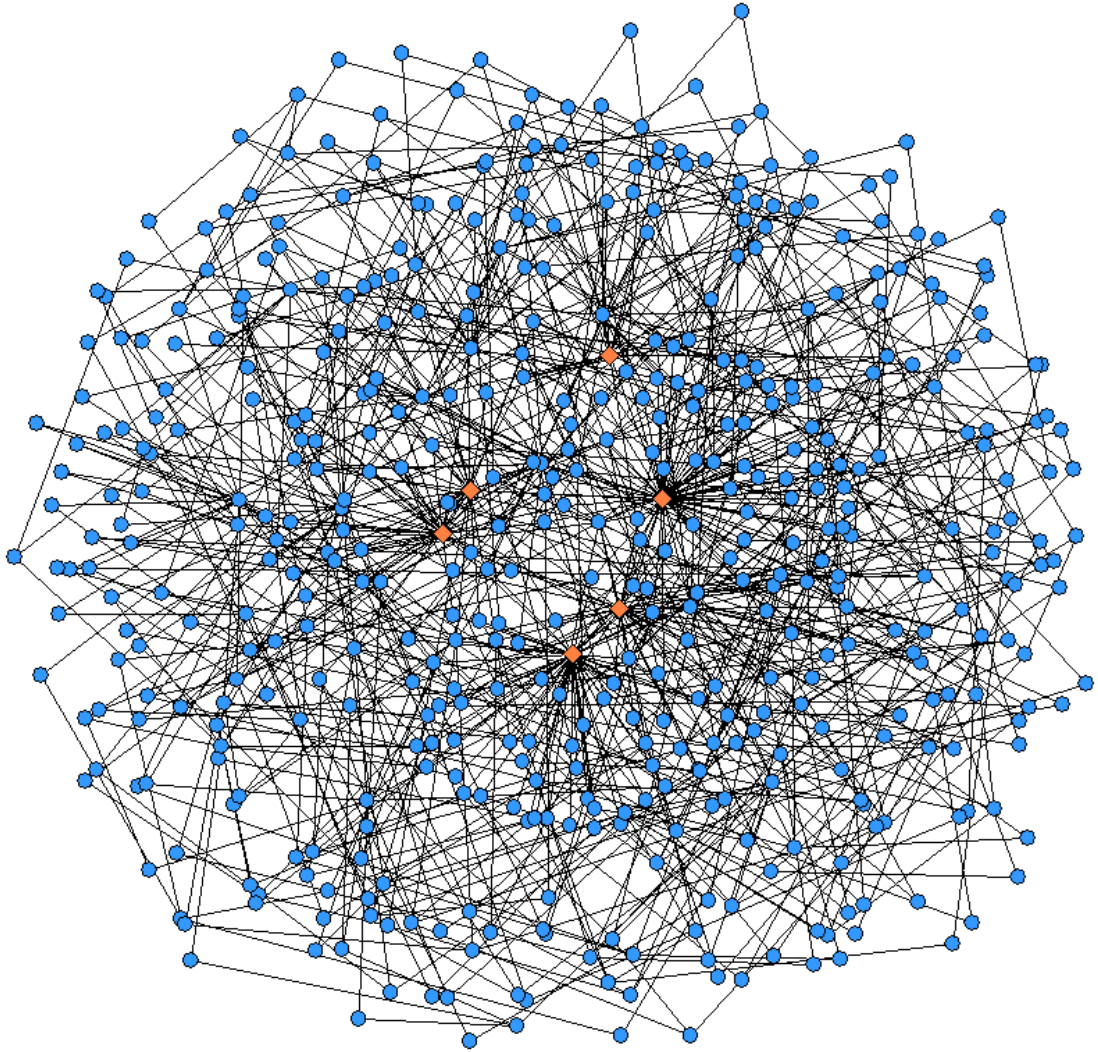
Πώς μπορώ να αποκτήσω bitcoin?

- Όπως μπορείς να αποκτήσεις ευρώ!
- Μπορείς να δουλέψεις και να πληρωθείς σε bitcoin
- Μπορείς να πουλήσεις αντικείμενα ή υπηρεσίες για bitcoin
- Μπορείς να ανταλλάξεις ευρώ για bitcoin
  - Με υπηρεσίες που προσφέρουν δυνατότητα ανταλλαγής
    - bitstamp.net, kraken.com
  - Με άλλους ανθρώπους από κοντά
    - localbitcoin.com

Το δίκτυο του bitcoin

- Όλοι οι κόμβοι του bitcoin συνδέονται σε ένα κοινό p2p δίκτυο
- Κάθε κόμβος τρέχει τον κώδικα του bitcoin
- Ο κόμβος μπορεί να τρέχει σε κινητό, υπολογιστή, κλπ.
- Είναι ανοιχτού κώδικα
- Καθένας κόμβος συνδέεται με κάποιους γειτονικούς του
- Ανταλλάσσουν συνέχεια οικονομικά δεδομένα
- Καθένας μπορεί ελεύθερα να συνδεθεί στο δίκτυο και να συμμετέχει
- Δεν υπάρχει εμπιστοσύνη στο δίκτυο!
  - Καθένας υποθέτει ότι οι γείτονές του μπορεί να λένε ψέματα





Κλειδιά

- Το bitcoin χρησιμοποιεί ελλειπτικές καμπύλες (συγκεκριμένα secp256k1)
- Κάθε χρήστης του bitcoin παράγει ένα ζεύγος κλειδιών (P, x)
  - P: δημόσιο κλειδί
  - x: ιδιωτικό κλειδί
- Το δημόσιο κλειδί P κωδικοποιείται σε μία διεύθυνση
- Με το δημόσιο κλειδί P λαμβάνουμε χρήματα
- Με το ιδιωτικό κλειδί x ξοδεύουμε χρήματα
  - Αποδεικνύουμε ότι είμαστε ο πραγματικός κάτοχος

Κλειδιά

- Ιδιωτικό κλειδί:
  - L4R3iSGxtzsYdmK1uP3GdBMiu68P7Wzx1yz29AKECuinFXTkALoZ

- Δημόσιο κλειδί:
  - 020c49ee87523337408b22b4542e808807a7763cd9eb0438d394eaacaf14275c5b

- Διεύθυνση:
  - 1EPVoneoy2ZbSfpLagqwZwrgfLAqSU8vZa

Κλειδιά

- Ιδιωτικό κλειδί:
  - L4R3iSGxtzsYdmK1uP3GdBMiu68P7Wzx1yz29AKECuinFXTkALoZ

- Δημόσιο κλειδί:
  - 020c49ee87523337408b22b4542e808807a7763cd9eb0438d394eaacaf14275c5b

- Διεύθυνση:
  - 1EPVoneoy2ZbSfpLagqwZwrgfLAqSU8vZa

Κλειδιά

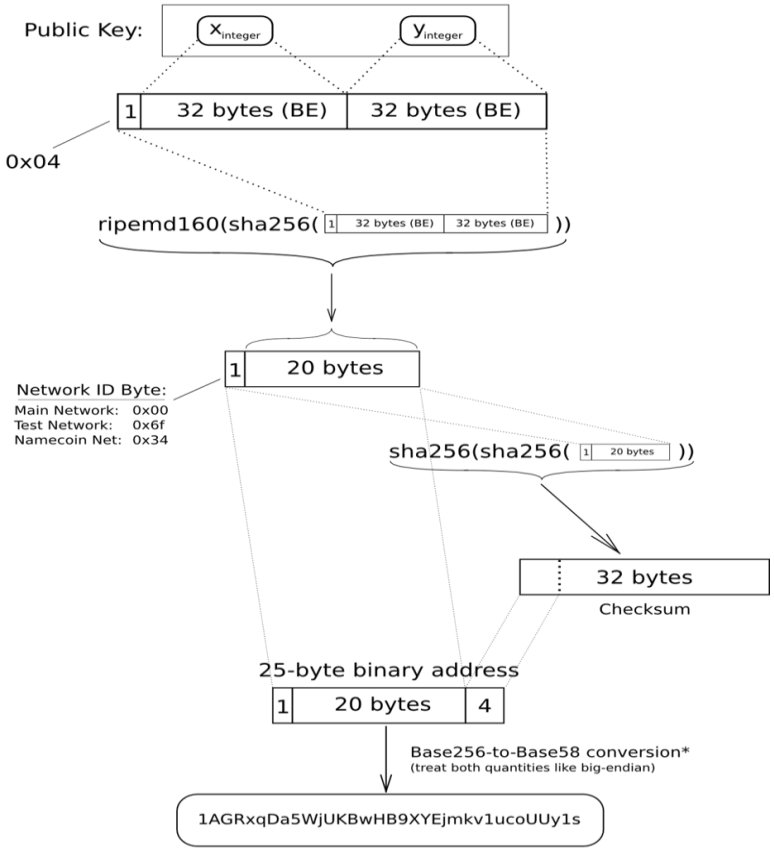
- Ιδιωτικό κλειδί:
  - L4R3iSGxtzsYdmK1uP3GdBMiu68P7Wzx1yz29AKECuinFXTkALoZ

- Δημόσιο κλειδί:
  - 020c49ee87523337408b22b4542e808807a7763cd9eb0438d394eaacaf14275c5b

- Διεύθυνση:
  - 1EPVoneoy2ZbSfpLagqwZwrgfLAqSU8vZa

Πάντα άσσος

Elliptic-Curve Public Key to BTC Address conversion



*In a standard base conversion, the 0x00 byte on the left would be irrelevant (like writing '052' instead of just '52'), but in the BTC network the left-most zero chars are carried through the conversion. So for every 0x00 byte on the left end of the binary address, we will attach one '1' character to the Base58 address. This is why main-network addresses all start with '1'

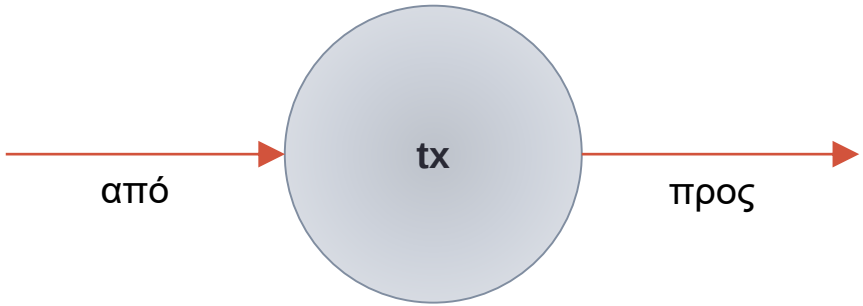
Διευθύνσεις

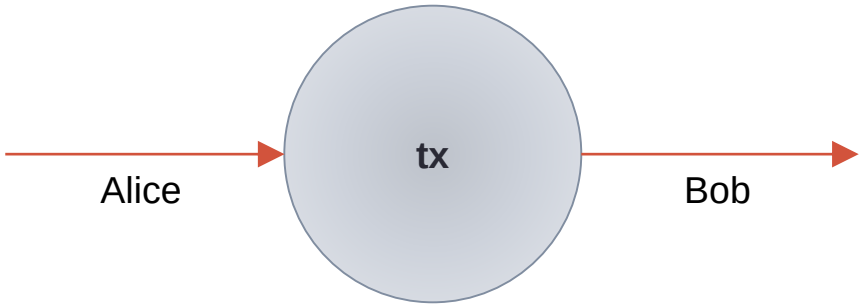
- Μοιάζουν με “αριθμούς λογαριασμών” στο τραπεζικό σύστημα
- Κάθε άνθρωπος μπορεί να έχει πολλές
- Συχνά αναπαρίστανται με QR codes για εύκολη ανταλλαγή χρημάτων
- Είναι δημόσια κλειδιά, μπορούμε να τις δημοσιεύουμε δίχως κίνδυνο!

Συναλλαγές

Συναλλαγές

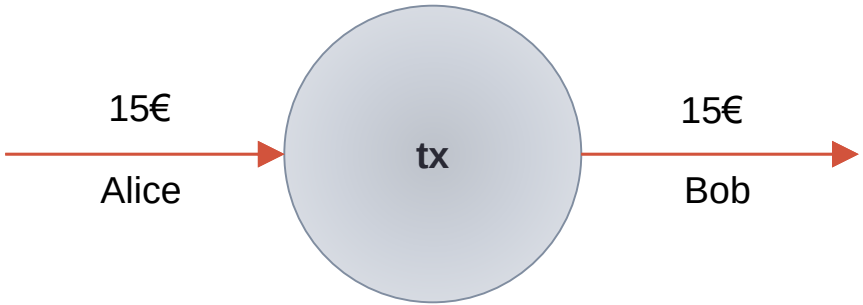
- Η βασική δομή του bitcoin είναι η συναλλαγή (transaction - tx)
- Μία συναλλαγή μεταφέρει χρήματα από έναν κάτοχο σε έναν άλλον

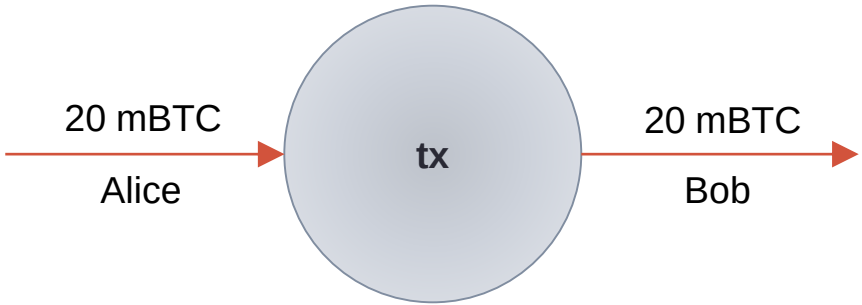



tx
Alice
Bob

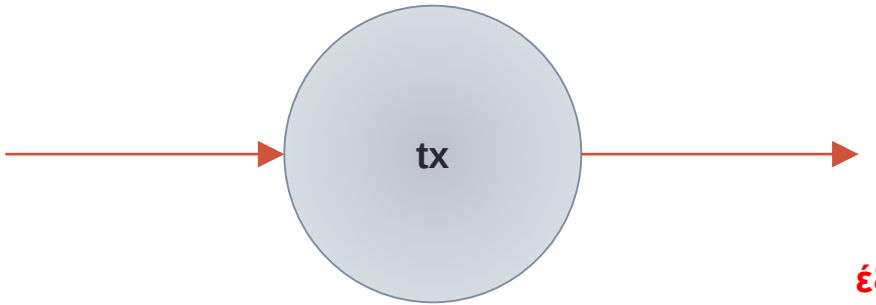
Ακμές συναλλαγών

- Μία συναλλαγή αναπαρίσταται από έναν κόμβο
- Έχει εισερχόμενες και εξερχόμενες ακμές
- Η εισερχόμενη ακμή αντιπροσωπεύει ποιος πληρώνει
- Η εξερχόμενη ακμή αντιπροσωπεύει ποιος πληρώνεται
- Οι κόμβοι δεν αντιπροσωπεύουν ιδιοκτήτες, αλλά συναλλαγές
- Οι ακμές έχουν ιδιοκτήτες
- Κάθε ακμή έχει ένα βάρος που αποτελεί την οικονομική αξία της


15€
Alice
tx
15€
Bob


20 mBTC
Alice
tx
20 mBTC
Bob

είσοδος / input

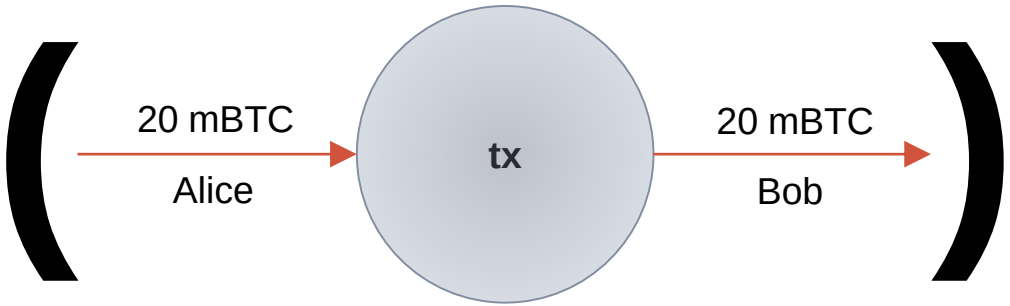


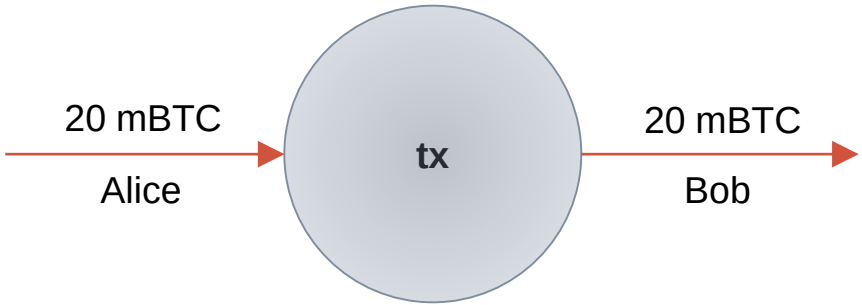
έξοδος / output

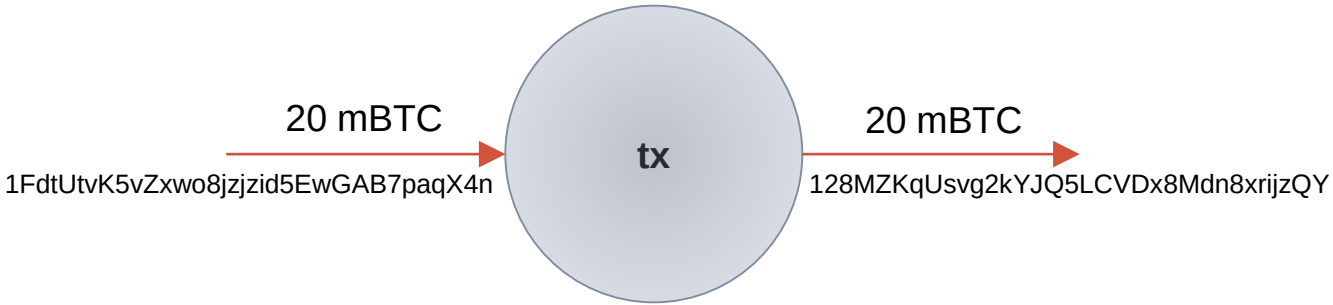
Δημόσιες συναλλαγές

- Όλες οι συναλλαγές δημοσιεύονται!
- Καθένας μπορεί να δει όλες τις συναλλαγές
- Ανωνυμία επιτυγχάνεται επειδή οι συναλλαγές αφορούν δημόσια κλειδιά
- Δεν γνωρίζουμε ποια δημόσια κλειδιά ανήκουν σε ποιον
- Κάθε χρήστης δημιουργεί πολλαπλά δημόσια κλειδιά
- Το SHA2562 των δεδομένων συναλλαγής ονομάζεται transaction id (txid)

$$\text{txid} = \text{SHA256}^2$$




20 mBTC
Alice
tx
20 mBTC
Bob

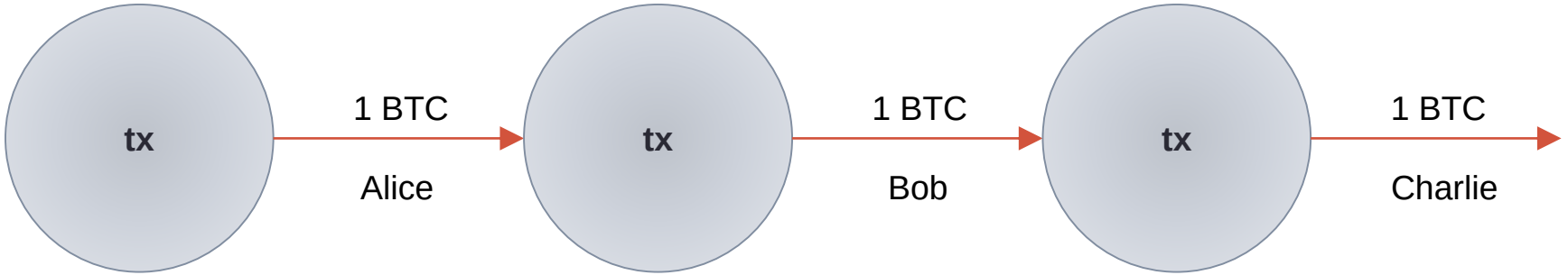

20 mBTC
1FdtUtvK5vZxwo8jzjzid5EwGAB7paqX4n
tx
20 mBTC
128MZKqUsvg2kYJQ5LCVDx8Mdn8xrijzQY

Δημόσιες συναλλαγές

- Κατεβάστε όλο το blockchain
- Αναζητήστε το txid που σας ενδιαφέρει
- Εναλλακτικά:
  - blockchain.info

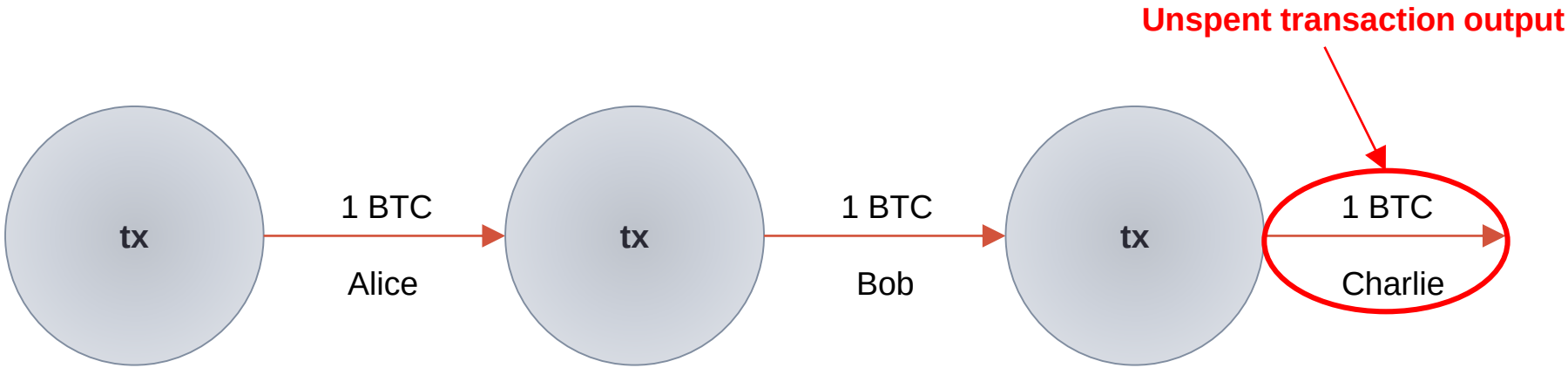
Ο γράφος συναλλαγών

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



Αξόδευτα χρήματα

- Τα χρήματα που μπορούν να ξοδευτούν είναι τα αξόδευτα χρήματα
- Είναι οι εξερχόμενες ακμές χωρίς πέρας από συναλλαγές (utxo)



Πώς ζητάω χρήματα;

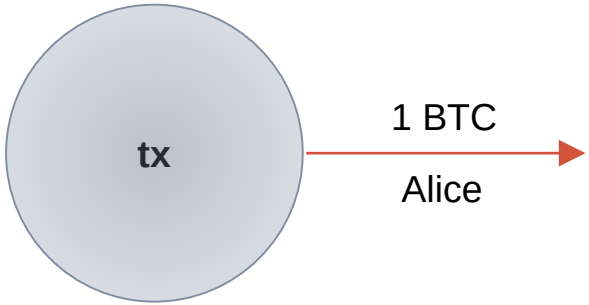
- Παράγω ένα νέο ιδιωτικό κλειδί, αντίστοιχο δημόσιο, και αντίστοιχη διεύθυνση
- Είναι σημαντικό να αλλάζουμε διευθύνσεις για λόγους ανωνυμίας
- Στέλνω τη διεύθυνση στον πληρωτή π.χ. μέσω email, FB, QR code κλπ.
- Παρακολουθώ το δίκτυο για κάποια συναλλαγή που με πληρώνει

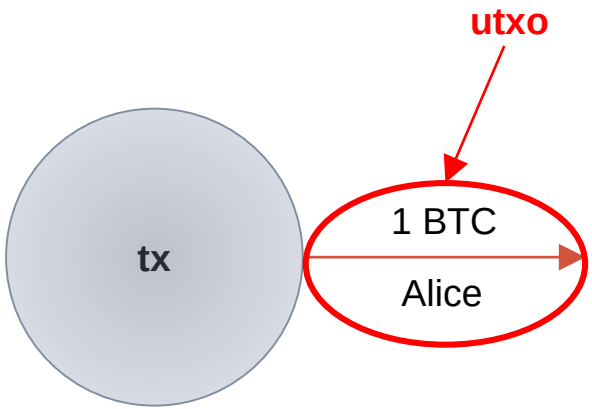
Ποια χρήματα μου ανήκουν;

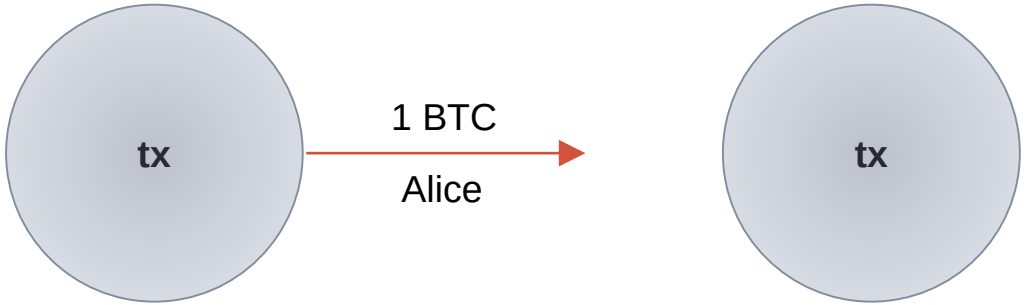
- Όσα βρίσκονται σε UTXO, δηλαδή είναι ακόμη αξόδευτα
  - Διαφορετικά έχω μεταβιβάσει την ιδιοκτησία τους σε κάποιον άλλον
- Στην εξερχόμενη ακμή αναγράφομαι ως ιδιοκτήτης
- Δηλαδή αναγράφεται ένα δημόσιο κλειδί για το οποίο κρατώ το ιδιωτικό κλειδί

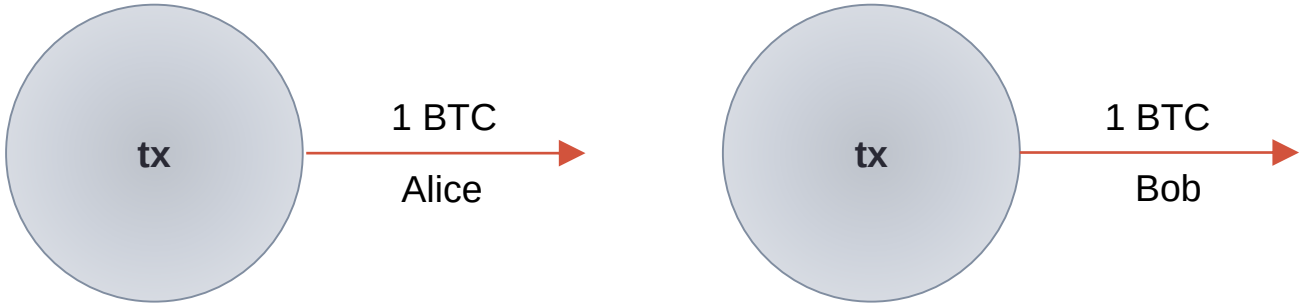
Πώς ξοδεύω χρήματα;

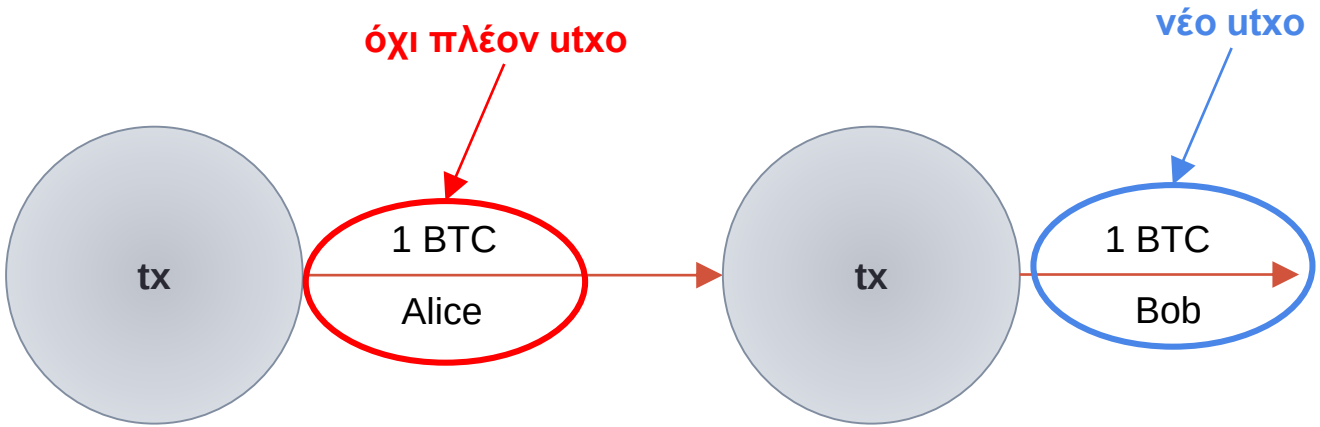
- Βρίσκω μία συναλλαγή που έχει UTXO
- Βεβαιώνομαι ότι είμαι ο ιδιοκτήτης της εξερχόμενης ακμής
- Δημιουργώ μία νέα συναλλαγή
- Με μία εισερχόμενη και μία εξερχόμενη ακμή
- Συνδέω την εισερχόμενη ακμή της νέας συναλλαγής με το παλιό UTXO
- Πλέον το παλιό utxo δεν είναι πλέον utxo – μόλις ξοδεύτηκε
- Αφήνω την εξερχόμενη ακμή της νέας συναλλαγής ασύνδετη (νέο UTXO)
- Ονομάζω την αξία της νέας εξερχόμενης ακμής
- Ονομάζω τον ιδιοκτήτη της νέας εξερχόμενης ακμής (δημόσιο κλειδί που προκύπτει από τη διεύθυνση που μου δώθηκε)


tx
1 BTC
Alice


utxo
tx
1 BTC
Alice

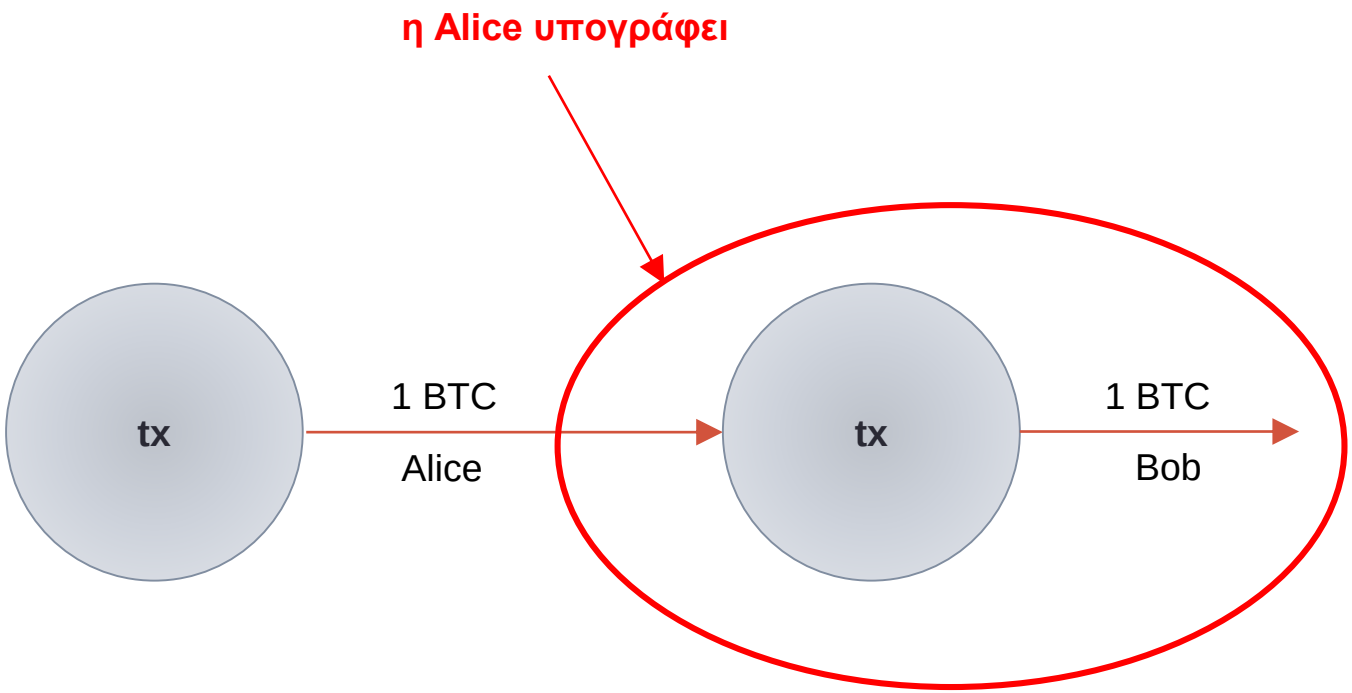

tx
1 BTC
Alice
tx

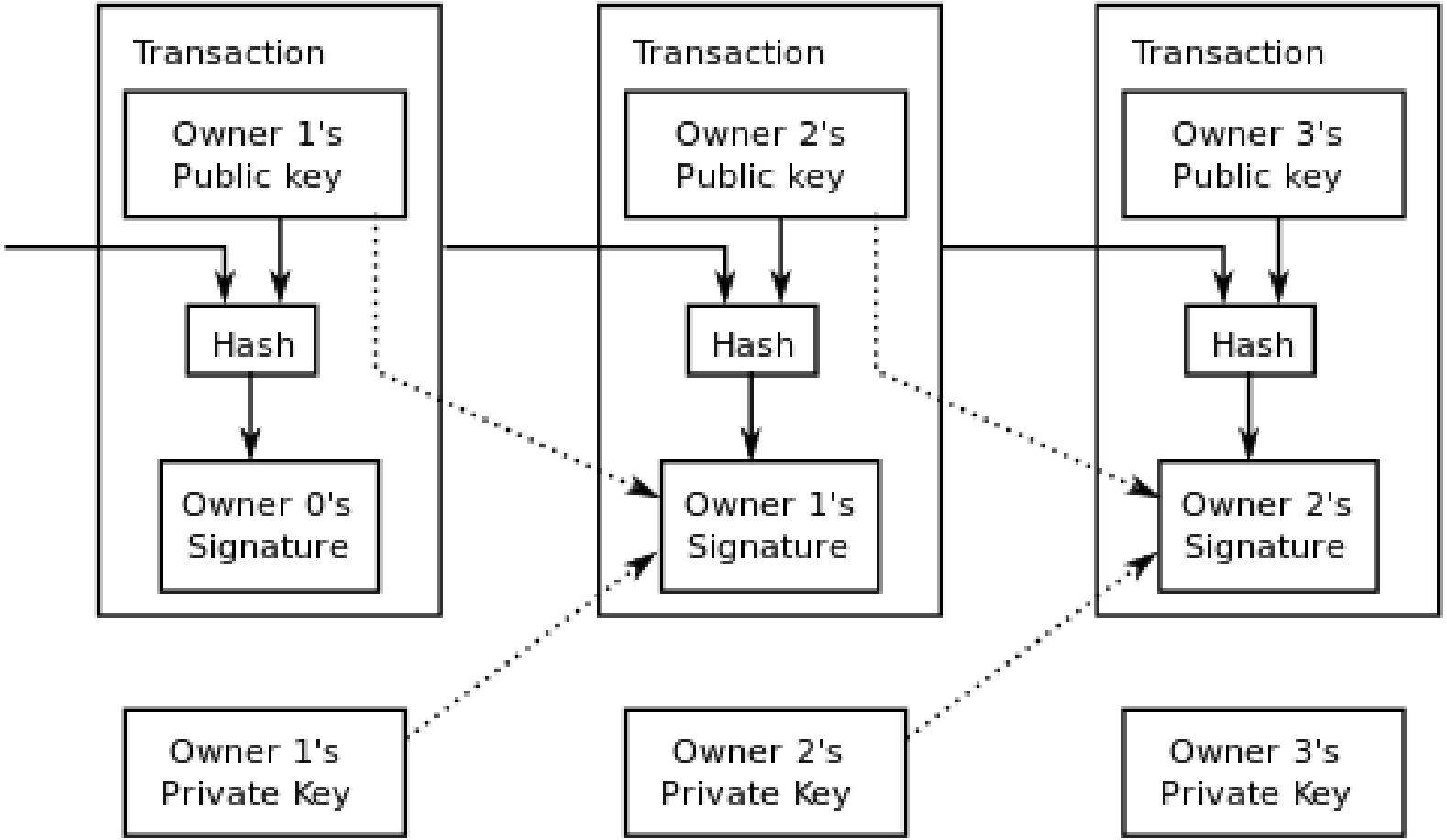

tx
1 BTC
Alice
tx
1 BTC
Bob


όχι πλέον utxo
νέο utxo
tx
1 BTC
Alice
tx
1 BTC
Bob

Απόδειξη ιδιοκτησίας

- Υπογράφω ψηφιακά το UTXO που θέλω να ξοδέψω μαζί με τις πληροφορίες της νέας συναλλαγής
- Αυτό εγγυάται ότι είμαι ο πραγματικός ιδιοκτήτης του UTXO
- Η νέα συναλλαγή πρέπει να περιλαμβάνεται στην υπογραφή
- Έτσι εγγυώμαι ότι αδειοδοτώ τον νέο ιδιοκτήτη και η υπογραφή μου δεν μπορεί να παραχαραχθεί προς λάθος ιδιοκτήτη με απλή αντιγραφή


η Alice υπογράφει
tx
1 BTC
Alice
tx
1 BTC
Bob

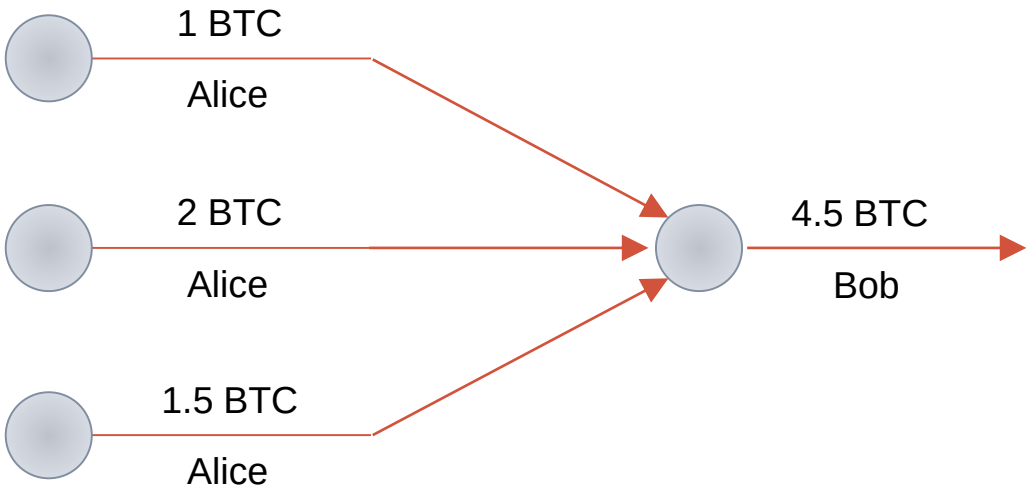

Transaction
Owner 1's Public key
Hash
Owner 0's Signature
Transaction
Owner 2's Public key
Hash
Owner 1's Signature
Transaction
Owner 3's Public key
Hash
Owner 2's Signature
Owner 1's Private Key
Owner 2's Private Key
Owner 3's Private Key

Transaction broadcasting

- Broadcast:
  - Όταν δημιουργώ μία συναλλαγή, την στέλνω σε όλους μου τους γείτονες
- Relay:
  - Οι γείτονες την στέλνουν στους δικούς τους υπό την προϋπόθεση ότι η συναλλαγή είναι έγκυρη
- Σε λίγο χρόνο, όλο το δίκτυο μαθαίνει για τη συναλλαγή μου

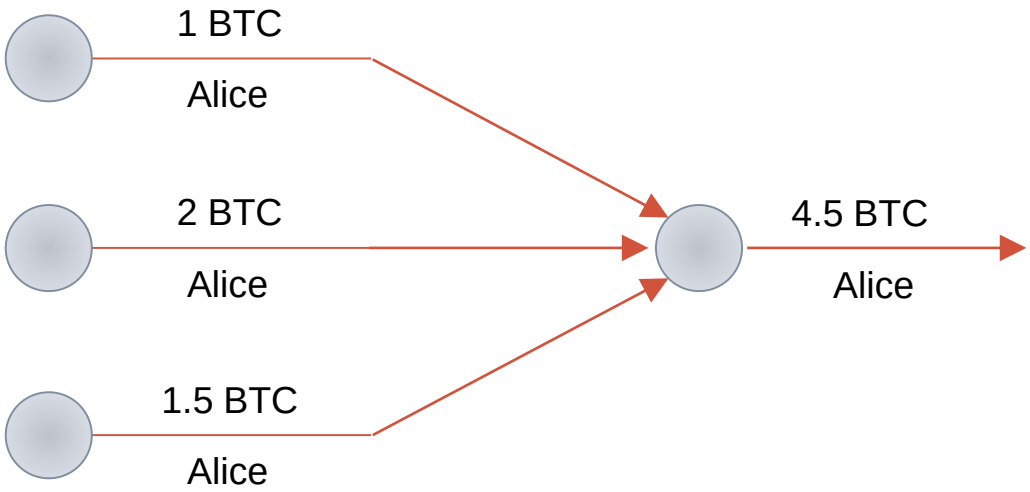
Μία συναλλαγή - πολλές είσοδοι

- Έχω λάβει χρήματα με πολλές συναλλαγές (πολλαπλά UTXOs μου ανήκουν)
- Θέλω να ξοδέψω όλα τα χρήματα μαζί
- Δημιουργώ μία συναλλαγή με πολλές εισόδους και μία έξοδο



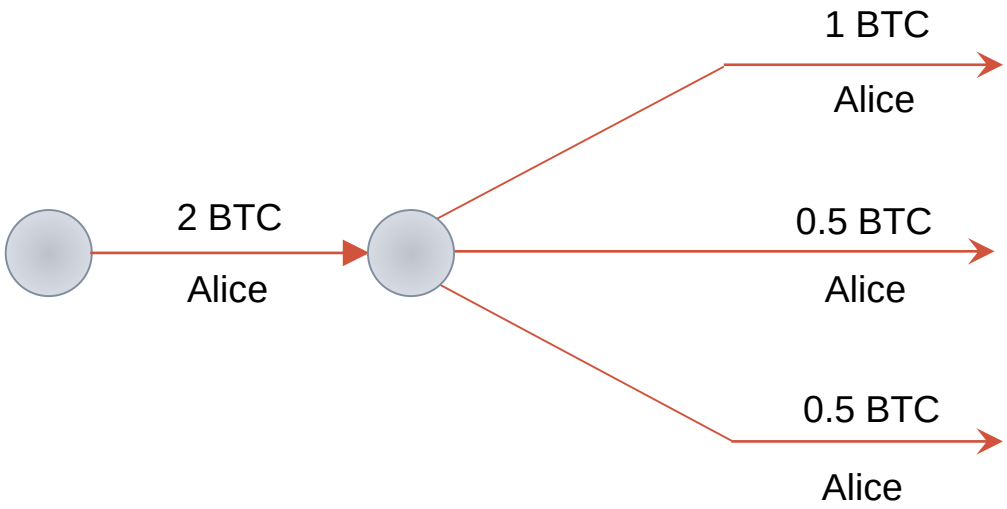
Μία συναλλαγή - πολλές είσοδοι

- Επίσης χρήσιμο αν θέλω να συνδυάσω τα χρήματά μου σε μία διεύθυνση
- Ενώνω τα UTXOs μου μέσω μίας συναλλαγής προς τον εαυτό μου



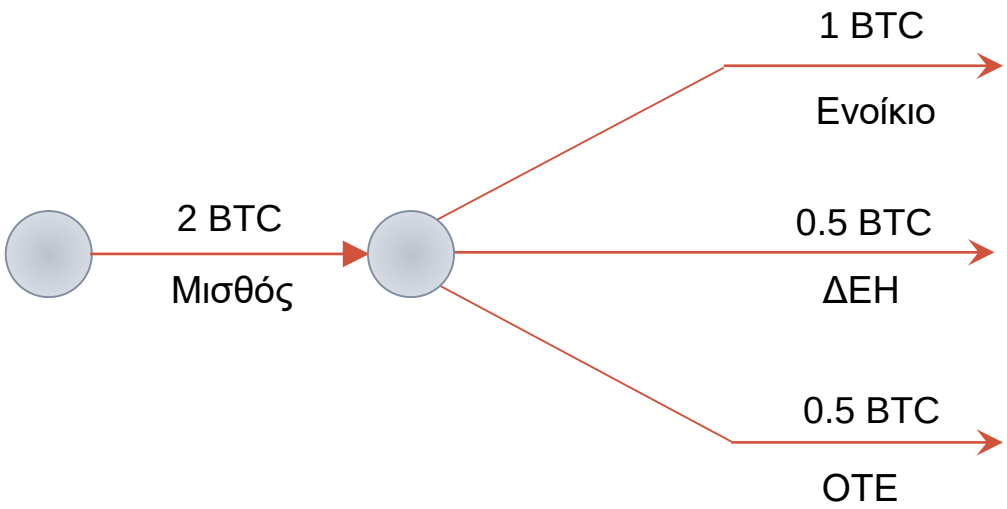
Μία συναλλαγή - πολλές έξοδοι

- Έχω μία συναλλαγή με πολλά χρήματα
- Θέλω να τα “σπάσω” σε υποδιαιρέσεις
- Φτιάχνω μία συναλλαγή με μία είσοδο και πολλές εξόδους



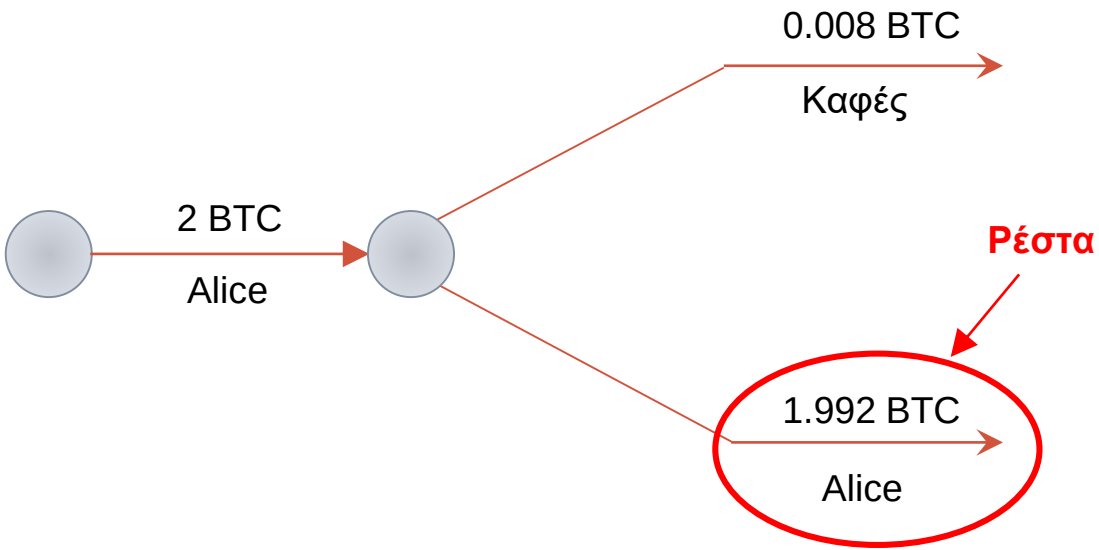
Μία συναλλαγή - πολλές έξοδοι

- Μπορώ να το χρησιμοποιήσω για να κάνω πολλαπλές πληρωμές



Μία συναλλαγή - πολλές έξοδοι

- ...ή για μία μικρή πληρωμή και να κρατήσω τα ρέστα (change)
- Τα ρέστα τα δίνω εγώ στον εαυτό μου ως utxo, δεν περιμένω από τον πωλητή

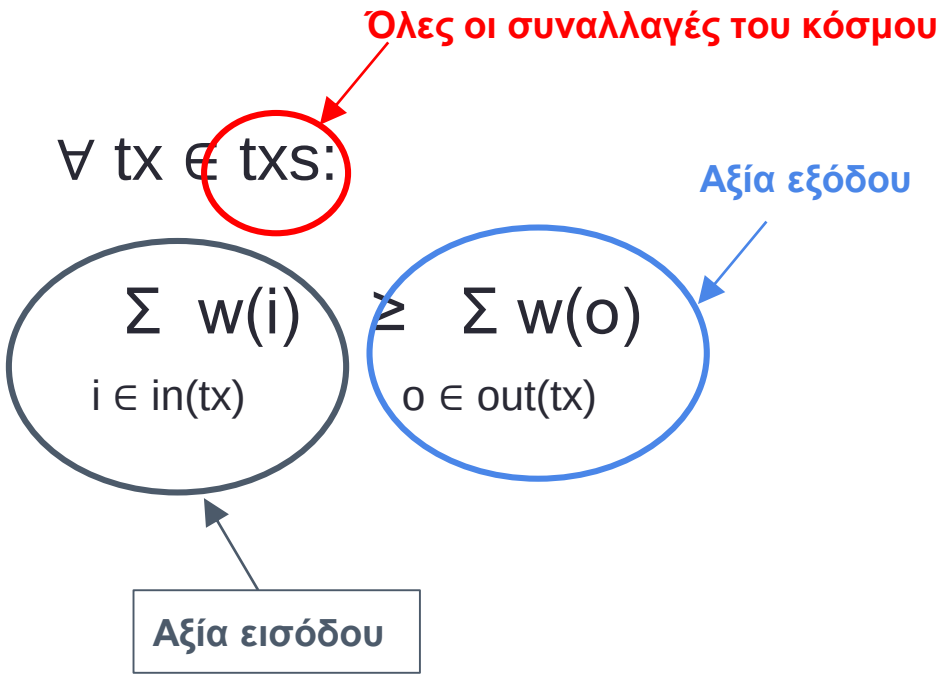


Αρχή διατήρησης του Kirchhoff

$$\forall\ tx \in txs:$$

$$\sum_{i \in in(tx)} w(i) \quad \geq \quad \sum_{o \in out(tx)} w(o)$$

Αρχή διατήρησης του Kirchhoff



Το σύνολο UTXO

- Το σύνολο όλων των UTXOs του δικτύου είναι σημαντικό
- Δείχνει σε όλους ποια χρήματα μπορούν να ξοδευτούν
- Ό,τι δεν είναι στο UTXO δεν μπορεί να ξοδευτεί
- Γι’ αυτό το λόγο, κάθε κόμβος του bitcoin διατηρεί κάθε στιγμή αυτό που πιστεύει ότι είναι το έγκυρο UTXO set

Εγκυρότητα μίας συναλλαγής

- Για να επιβεβαιώσουμε την εγκυρότητα μίας συναλλαγής:
- Επαγωγικά γνωρίζουμε κάποιες ήδη έγκυρες συναλλαγές
  - Διατηρούμε ένα έγκυρο UTXO set
- Επιβεβαιώνουμε ότι ισχύει ο νόμος του Kirchhoff
- Επιβεβαιώνουμε την ψηφιακή υπογραφή
- Επιβεβαιώνουμε ότι οι είσοδοι της νέας συναλλαγές συνδέονται στο έγκυρο UTXO set που γνωρίζουμε
  - Αυτό επιβεβαιώνει ότι τα χρήματα ξοδεύονται ακριβώς μία φορά
- Ενημερώνουμε το έγκυρο UTXO set:
  - Αφαιρούμε τα UTXOs που ξοδεύτηκαν
  - Προσθέτουμε τα UTXOs που δημιουργήθηκαν

Πόσα bitcoin έχω;

- Παρατηρώ το δίκτυο για συναλλαγές και διατηρώ ένα έγκυρο UTXO set
- Από το έγκυρο UTXO κρατώ τις ακμές που μου ανήκουν
  - Δηλαδή ακμές στις οποίες αναγράφονται δημόσια κλειδιά για τα οποία κρατώ ιδιωτικά κλειδιά
- Αθροίζω τις αξίες
- Το αποτέλεσμα είναι τα χρήματα στην ιδιοκτησία μου

Bitcoin wallet

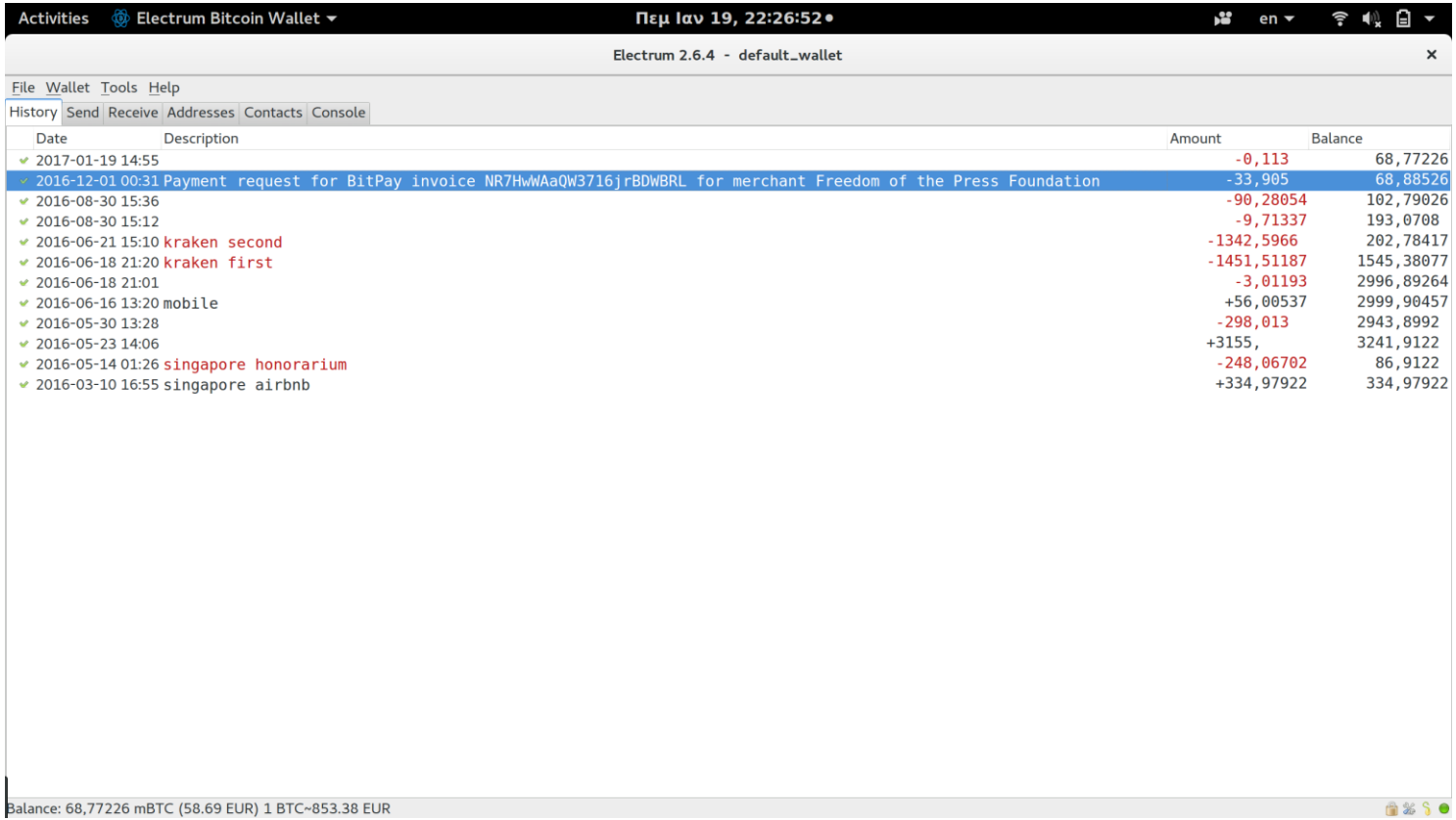
Πορτοφόλι

- Ένα σύνολο ιδιωτικών κλειδιών bitcoin
- Συνήθως ένα πρόγραμμα
- Τρέχει στον υπολογιστή ή στο κινητό

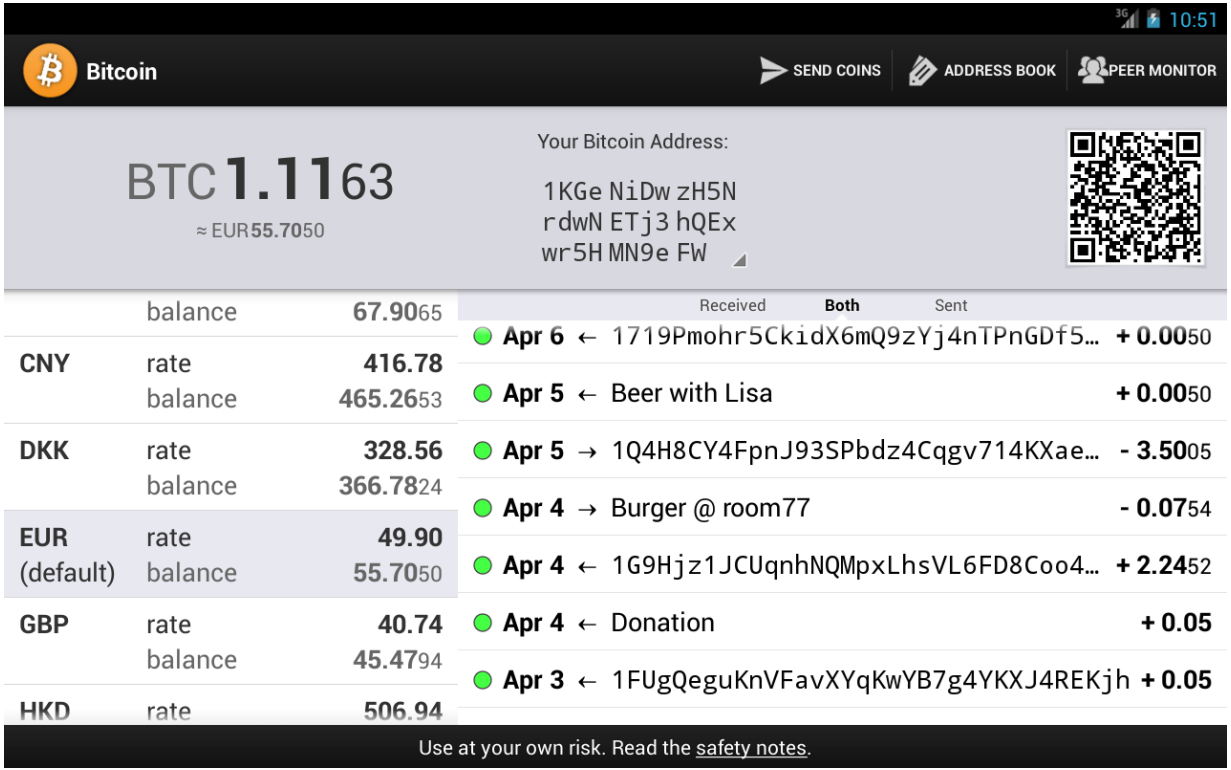
Hot και cold wallets

- Μπορώ να έχω τα κλειδιά μου σε υπολογιστή συνδεδεμένο στο Internet
  - “Hot wallet”
  - Ευκολία χρήσης
  - Βλέπω τι συναλλαγές περνάνε και πόσα χρήματα έχω
  - Μπορώ να ξοδέψω άμεσα
- Μπορώ να διατηρώ τα ιδιωτικά κλειδιά μου offline
  - “Cold wallet”
  - π.χ. τα τυπώνω σε χαρτί (paper wallet) και τα κρατώ σε χρηματοκιβώτιο
  - ή τα απομνημονεύω (brain wallet)
  - Τα κλειδιά μου είναι πιο ασφαλή από παραβιάσεις
  - Μπορώ να τα μεταφέρω σε hot wallet αν θέλω να ξοδέψω
- Hardware wallet
  - Ειδική συσκευή που διατηρεί ιδιωτικά bitcoin κλειδιά ασφαλή

Desktop wallet - Electrum



Mobile wallet - Android



Διάλειμμα

Ιστορία του bitcoin

- 1983: David Chaum, “e-cash”
  - Κεντρικά ελεγχόμενο ηλεκτρονικό χρήμα
- 1998: Wei Dai, “bmoney”
  - Πρώτες αποκεντρωμένες ιδέες
- 2005: Nick Szabo, “bit gold”
  - Πλήρης θεωρητική περιγραφή του bitcoin
- 2008: Satoshi Nakamoto, “Bitcoin: A peer-to-peer electronic cash system”
- 2009: Δημοσίευση του bitcoin software

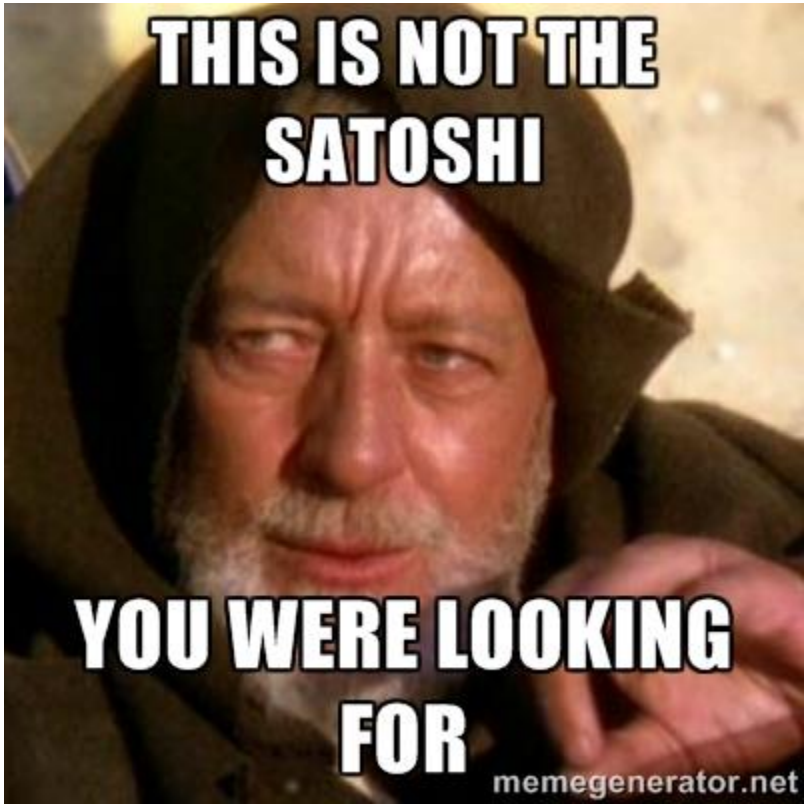
Ποιος είναι ο Satoshi Nakamoto?

- Ανώνυμος δημιουργός του bitcoin
- Ομάδα ή άτομο;
- Έγραψε το bitcoin paper
- Έφτιαξε την πρώτη υλοποίηση του bitcoin
- Συμμετείχε σε IRC συζητήσεις σχετικά 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?

- Θεωρίες συνωμοσίας…
- Είναι άνθρωπος ή ομάδα;
- Είναι ο Nick Szabo? Ο Wei Dai?
- Οι Dr Vili Lehdonvirta & Michael Clear;
- Οι Neal King, Vladimir Oksman & Charles Bry;
- Ο Shinichi Mochizuki ή ο Jed McCaleb;
- Ο Dread Pirate Roberts που έφτιαξε το μαγαζί ναρκωτικών Silk Road?
- Ο Dorian Nakamoto?
- Ο Craig Steven Wright?
- Όπως και να έχει, έκρυψε την ταυτότητά του καλά και επέλεξε να μείνει ανώνυμος

Ποιος είναι ο Satoshi ρε γαμώτο?

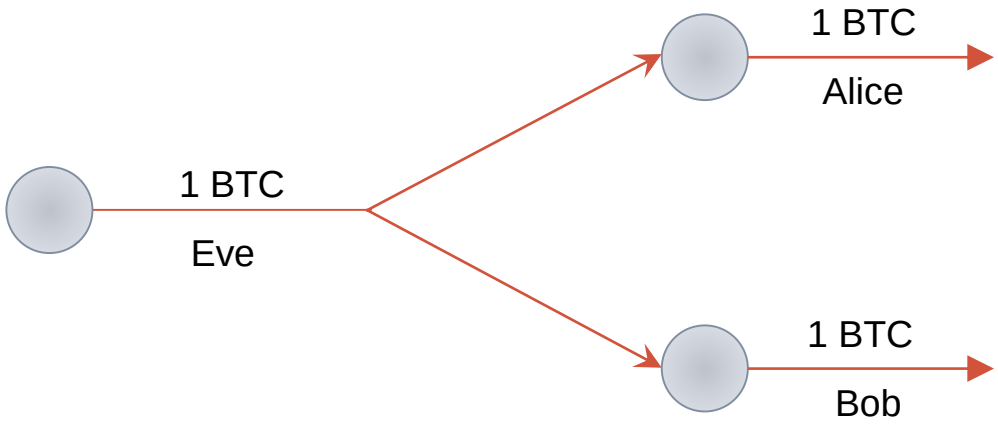


Double spending

- 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

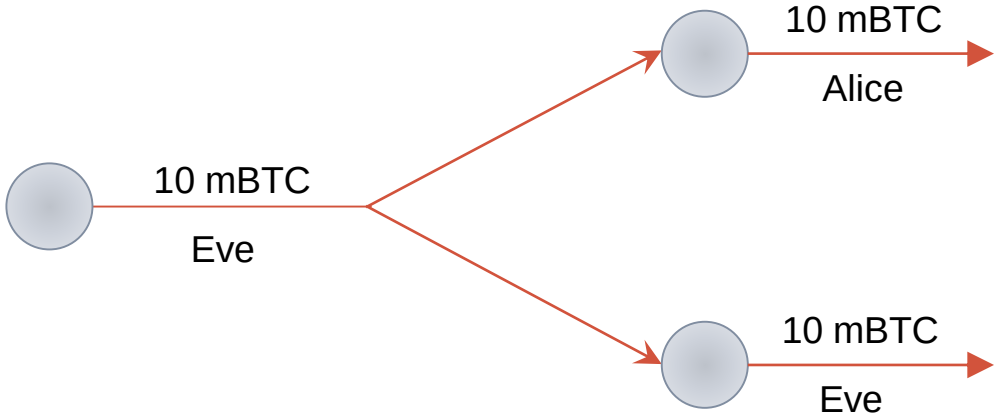
Double spending

- Δύο συναλλαγές που ξοδεύουν το ίδιο output ονομάζονται double spend
- Ο νόμος του Kirchhoff ισχύει για κάθε συναλλαγή
- Όλες οι υπογραφές είναι έγκυρες



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



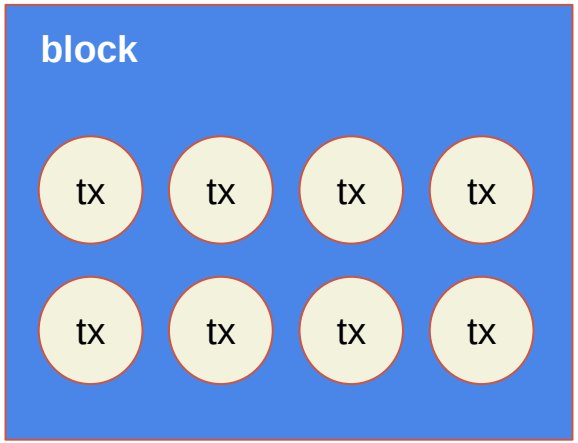
Blockchain

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

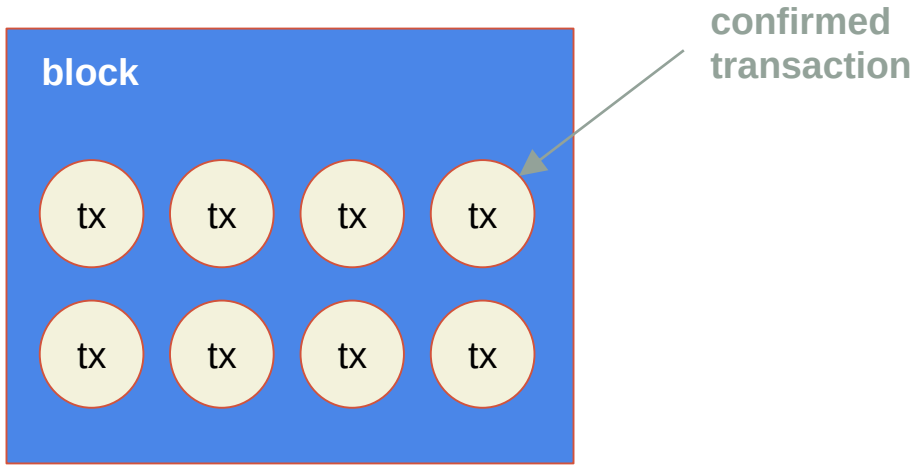
Block

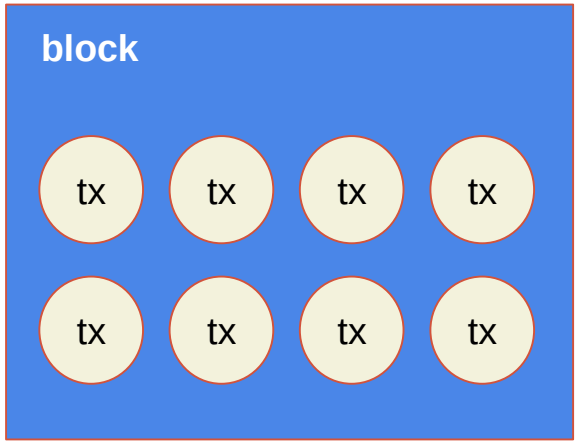
- Συλλέγει πολλά transactions
- Δεν περιέχει double spends, δηλαδή tx που ξοδεύουν το ίδιο output
- Κάθε transaction μπορεί να περιλαμβάνεται μία φορά σε ένα block



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

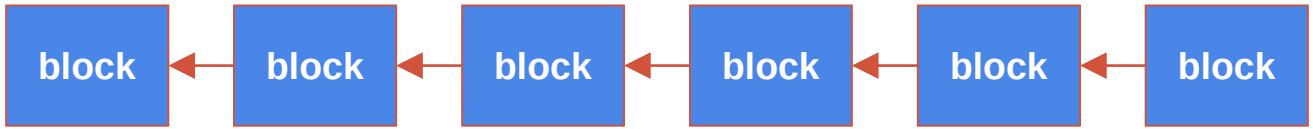

block
tx
tx
tx
tx
tx
tx
tx
tx
confirmed
transaction

blockid = SHA256 (

)

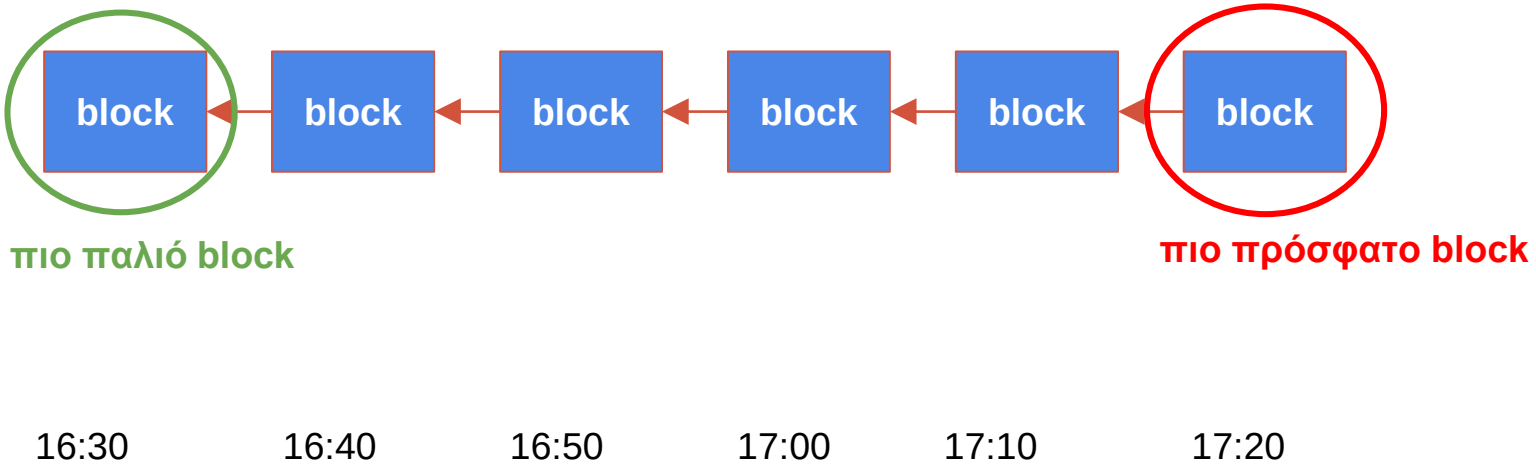
Blockchain

- 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

- 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



πιο παλιό block

πιο πρόσφατο block

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

Mining

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
- 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

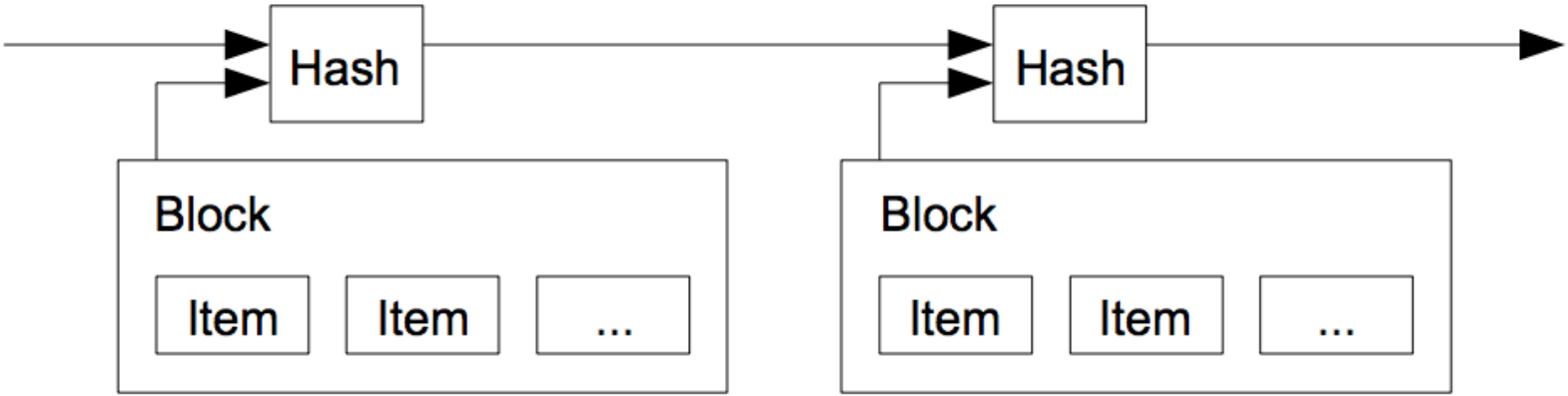
- Παρακολουθούμε το δίκτυο για συναλλαγές και blocks
- Περιλαμβάνουμε στο υποψήφιο block μας:
  - Όλες τις συναλλαγές που δεν έχουν εμφανιστεί σε προηγούμενο block που γνωρίζουμε
  - Μία αναφορά στο πιο πρόσφατο block που γνωρίζουμε ως πατέρα
- Αναζητούμε απόδειξη εργασίας
  - Η απόδειξη εργασίας γίνεται 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

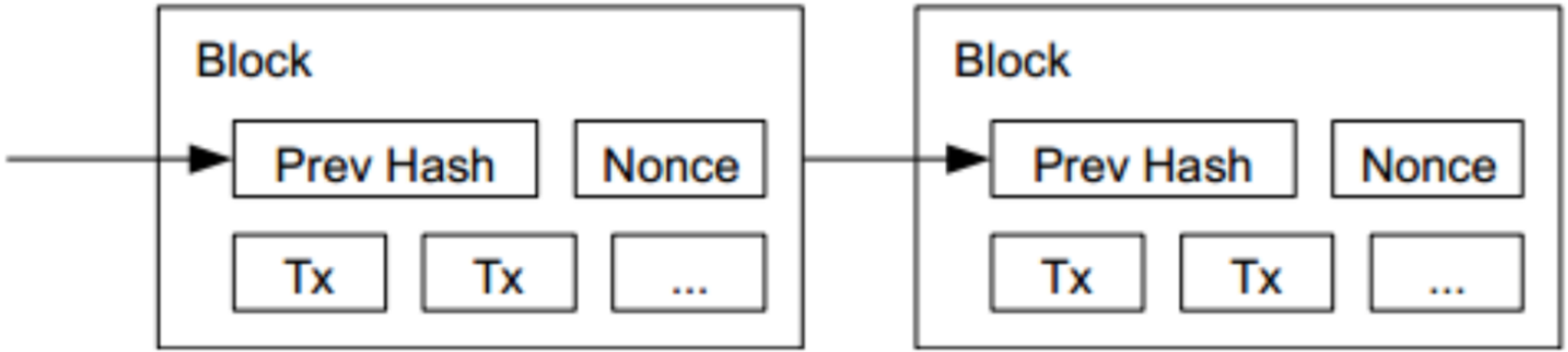
Απόδειξη εργασίας bitcoin

- H(txs || nonce || parent-blockid) < ε

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
...


Block
Prev Hash
Nonce
Tx
Tx
...
Block
Prev Hash
Nonce
Tx
Tx
...

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

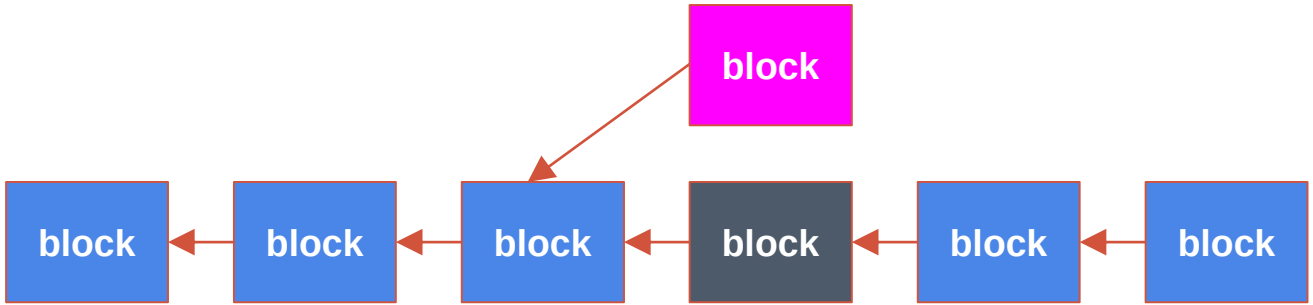
Genesis block

- 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

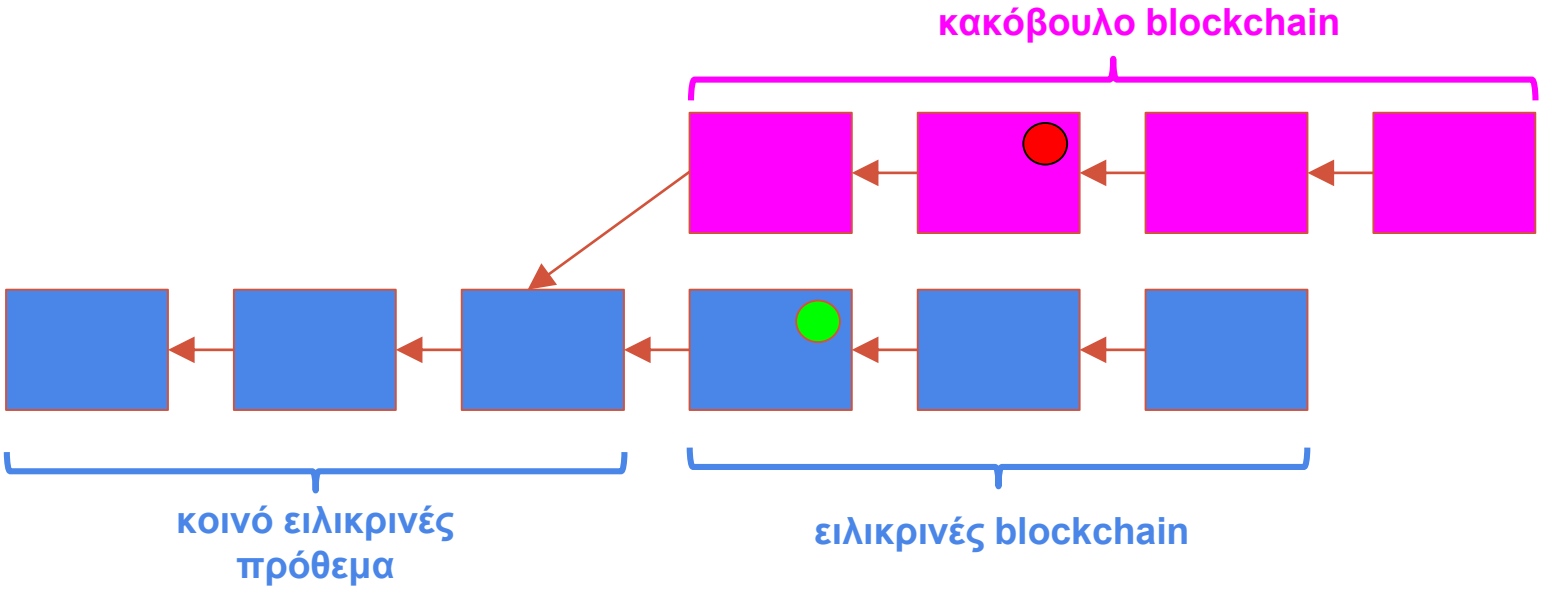
- Το blockchain fork είναι πρόβλημα διότι δεν μας επιτρέπει πια να έχουμε βέλος του χρόνου
- Επιστρέφουμε στο ίδιο πρόβλημα που είχαμε με τις συναλλαγές
- Ποιο από τα δύο blocks είναι το πιο πρόσφατο έγκυρο block?
- Τι γίνεται αν τα δύο αντίπαλα blocks περιλαμβάνουν double spends?

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
  - 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!

Κίνητρα mining

- Ένας miner ανταμοίβεται με 2 τρόπους:

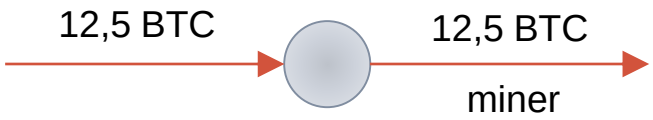
1. Με όλα τα περισσευούμενα χρήματα στις συναλλαγές που κάνει confirm:

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

Κίνητρα mining

- Ένας miner ανταμοίβεται με 2 τρόπους:

1. Με όλα τα περισσευούμενα χρήματα στις συναλλαγές που κάνει confirm
2. Με ένα coinbase transaction που επιτρέπεται να βάλει στο block, αξίας 12,5 BTC



Συναλλαγή coinbase

- Η συναλλαγή coinbase είναι η μόνη που μπορεί να έχει εισερχόμενες ακμές χωρίς αρχή
- Είναι η επαγωγική βάση στην επιβεβαίωση εγκυρότητας συναλλαγών
- Επιτρέπεται ακριβώς μία coinbase συναλλαγή ανά block
- Η αξία του coinbase απαιτείται να είναι 12,5 BTC
- Αυτός είναι ο μόνος τρόπος που παράγονται bitcoin

Τρόποι mining

- CPU: Το mining τρέχει στον επεξεργαστή
- GPU: Το mining τρέχει στην κάρτα γραφικών (παραλληλοποίηση)
- ASIC: Ειδικευμένο hardware για mining, ξεχωριστή φυσική συσκευή

Αξίζει να κάνω mining?

- Με CPU Core i7:
  - $0.04 / χρόνο
- Με GPU NVIDIA GTX590:
  - $0.13 / χρόνο
- Με GPU ATI 6990:
  - $0.58 / χρόνο
- Με ειδικευμένο hardware AntMiner S5+:
  - Έσοδα: $5136 / χρόνο
  - Κόστος ρεύματος: $2409 / χρόνο (με $0.08 / kWh)
  - Κόστος συμμετοχής σε pool: $102.74
  - Κέρδη: $2624 / έτος
  - Κόστος αγοράς: $2307
  - Κέρδος τον πρώτο χρόνο: $317

Η οικονομία του Bitcoin

Πληθωρισμός στο bitcoin

- Ο πληθωρισμός στο bitcoin είναι προκαθορισμένος
- Επιτυγχάνεται με αλγόριθμο που είναι γνωστός εξ’ αρχής σε όλους
- Συγκεκριμένα:
  - Το coinbase του block με ύψος 0 έχει είσοδο (reward) 50 BTC
  - Κάθε επόμενο block έχει coinbase εισόδου ίδιας αξίας με το προηγούμενό του
  - Κάθε 210,000 blocks (αναμενόμενη τιμή 4 χρόνια) η αξία της coinbase εξόδου πέφτει στο ½ του προηγούμενου block

total_btc_supply = $\frac{\sum_{i=0}^{32} 210000 \lfloor \frac{50.10^8}{2^i} \rfloor}{10^8}$

Πληθωρισμός στο bitcoin

- Ο πληθωρισμός στο bitcoin είναι προκαθορισμένος
- Επιτυγχάνεται με αλγόριθμο που είναι γνωστός εξ' αρχής σε όλους
- Συγκεκριμένα:
  - Το coinbase του block με ύψος 0 έχει είσοδο (reward) 50 BTC
  - Κάθε επόμενο block έχει coinbase εισόδου ίδιας αξίας με το προηγούμενό του
  - Κάθε 210,000 blocks (αναμενόμενη τιμή 4 χρόνια) η αξία της coinbase εξόδου πέφτει στο ½ του προηγούμενου block
  - Κάθε 210,000 ονομάζονται εποχή (era)

πλήθος εποχών μέχρι το reward να γίνει αμελητέο

χρόνος υποδιπλασιασμού σε blocks

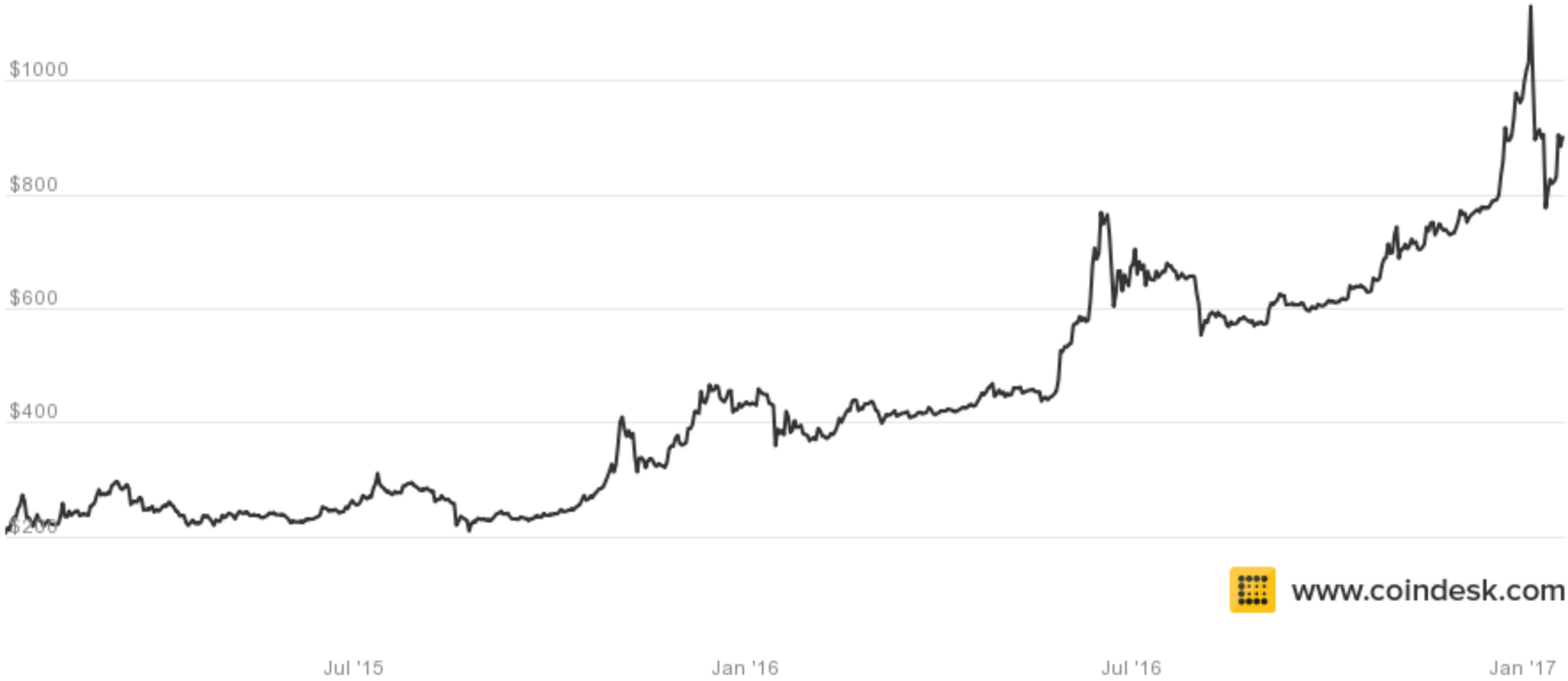
αρχικό block reward

$$\text{total\_btc\_supply} = \frac{\sum_{i=0}^{32} 210000 \left\lfloor \frac{50 \cdot 10^8}{2^i} \right\rfloor}{10^8}$$

satoshi / bitcoin

Αξία του bitcoin

- Εξαιρετικά μεταβλητή
- Ιανουάριος 2017: 1 BTC = 850 EUR
- Πριν ένα χρόνο, αρχές 2016: 1 BTC = 412 EUR
- Max 2013: 1 BTC = 900 EUR
- Min 2013: 1 BTC = 73 EUR
- 2012: 1 BTC = 4 EUR
- 2010: 1 BTC = 0.06 EUR
- 22 Μαϊου 2010: Πρώτη αγορά μέσω bitcoin


$1000
$800
$600
$400
$200
www.coindesk.com
Jul '15
Jan '16
Jul '16
Jan '17

Ευχαριστώ! Ερωτήσεις;

https://dimkarakostas.com
dimit.karakostas@gmail.com
DF46 7AFF 3398 BB31 CEA7 1E77 F896 1969 A339 D2E9