

Bitcoin #1

Blockchain Course
Dimitris Grigoriou, Christos Nasikas, Dionysis Zindros

Στόχος του μαθήματος

- Τι είναι το bitcoin
- Διευθύνσεις, κλειδιά
- Συναλλαγές, ρέστα
- Γράφος του bitcoin, ακμές, κόμβοι, αξίες, ιδιοκτήτες, utxo, coinbase
- Εξόρυξη, consensus, blockchain, genesis
- Proof-of-work, δυσκολία, confirmations, ανταμοιβές, fees
- Αξία του bitcoin
- Πορτοφόλια

Bitcoin

- Ψηφιακό νόμισμα
- Επιτρέπει να στέλνουμε χρήματα μέσω Internet

Πλεονεκτήματα του bitcoin

- Άμεση μεταφορά χρημάτων (< 10 sec)
 - Αντί 1 - 2 ημερών για τραπεζικές συναλλαγές
- Γρήγορη διασφάλιση συναλλαγών (10 min)
- Διαθεσιμότητα 24 ώρες το 24ωρο
- Ασφάλεια μέσω κρυπτογραφικών και μαθηματικών ιδιοτήτων
 - Αντί για ασφάλεια παραχάραξης μέσω χημικών / φυσικών ιδιοτήτων
- **Πολύ** μικρότερες χρεώσεις (~ €0.10 / συναλλαγή ανεξαρτήτως ποσού)
 - Αντί για **€1-5** χρέωση ανά μεταφορά

Πλεονεκτήματα του bitcoin

- Πραγματικά **ιδιόκτητο** χρήμα
 - Δεν ελέγχεται από κεντρικές τράπεζες όπως Federal Reserve (\$) ή Κεντρική Ευρωπαϊκή Τράπεζα (€)
 - Δεν επιδέχεται μακροοικονομικό πληθωριστικό έλεγχο
- Δεν μπορεί να λογοκριθεί
 - βλέπε υπόθεση PayPal/Wikileaks (2010)



What is bitcoin?

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



If you can't find your node, please make sure that your node or one of its peers has a connection or a channel opened to one of the nodes in the network.

Check the [FAQ](#) for more informations.

[Close](#)

World Map

Force Graph

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:

5JXesisRRU2Z7HMmwMpNtoiYk1QDMVjV3HLoYMd1PTKEkJhJT1z

Δημόσιο κλειδί:

**045a5f526dfe5d5995bf95f1229e70e21818190883c40ab3590458476ad34aaae5
9bc772b98a587035b452638b59238e2a39e954b43ab7a4f32408664d36ec1575**

Διεύθυνση: **133GT5661q8RuSKrrv8q2Pb4RwSpUTQU1Z**

Κλειδιά

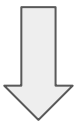
Ιδιωτικό κλειδί:

5JXesisRRU2Z7HMmwMpNtoiYk1QDMVjV3HLoYMd1PTKEkJhJT1z

Δημόσιο κλειδί:



**045a5f526dfe5d5995bf95f1229e70e21818190883c40ab3590458476ad34aaae5
9bc772b98a587035b452638b59238e2a39e954b43ab7a4f32408664d36ec1575**



Διεύθυνση: **133GT5661q8RuSKrrv8q2Pb4RwSpUTQU1Z**

Κλειδιά

Ιδιωτικό κλειδί:

5JXesisRRU2Z7HMmwMpNtoiYk1QDMVjV3HLoYMd1PTKEkJhJT1z

Δημόσιο κλειδί:

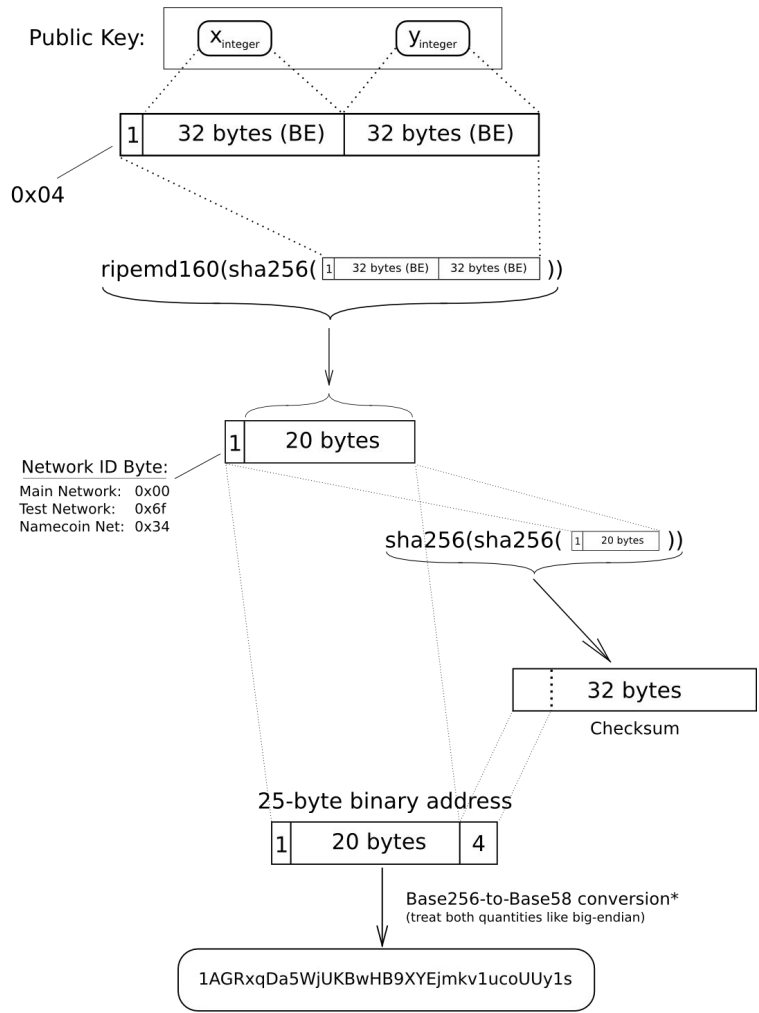


**045a5f526dfe5d5995bf95f1229e70e21818190883c40ab3590458476ad34aaae5
9bc772b98a587035b452638b59238e2a39e954b43ab7a4f32408664d36ec1575**



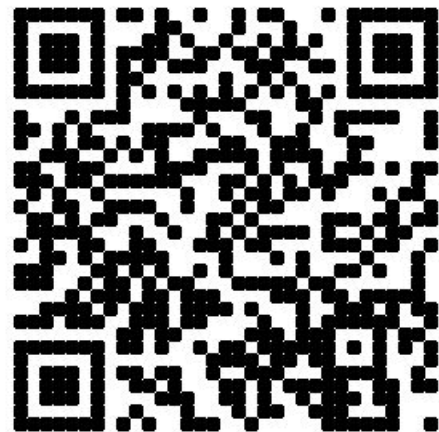
Διεύθυνση: **133GT5661q8RuSKrrv8q2Pb4RwSpUTQU1Z**

Πάντα άσσος



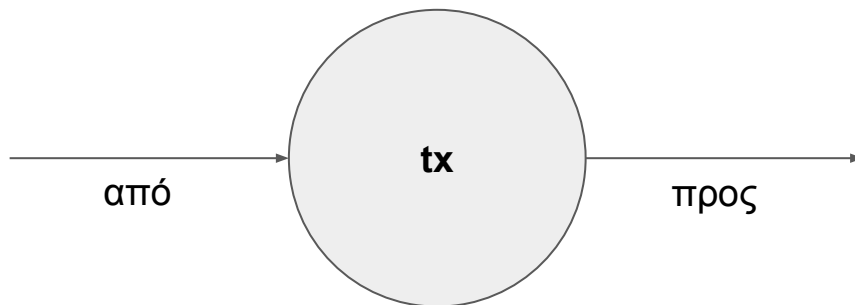
Διευθύνσεις

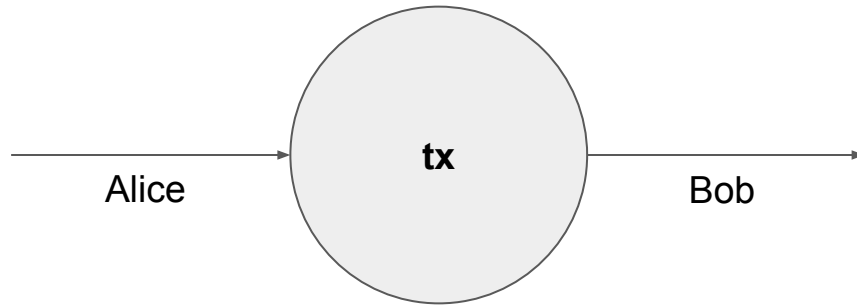
- Μοιάζουν με “αριθμούς λογαριασμών” στο τραπεζικό σύστημα
- Κάθε άνθρωπος μπορεί να έχει πολλές
- Συχνά αναπαρίστανται με **QR codes** για εύκολη ανταλλαγή χρημάτων
- Είναι δημόσια κλειδιά, μπορούμε να τις δημοσιεύουμε δίχως κίνδυνο!



Συναλλαγές

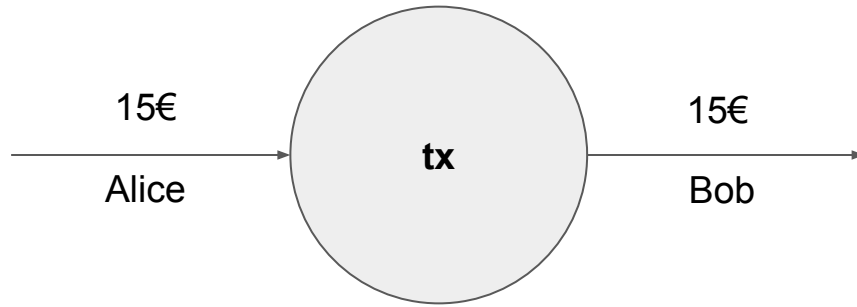
- Η βασική δομή του bitcoin είναι η **συναλλαγή** (transaction - tx)
- Μία συναλλαγή μεταφέρει χρήματα από έναν κάτοχο σε έναν άλλον

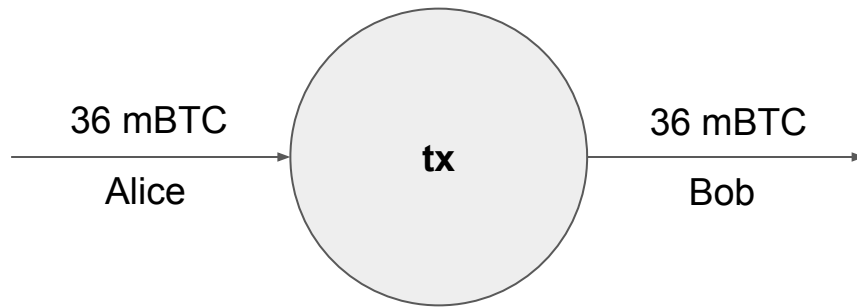




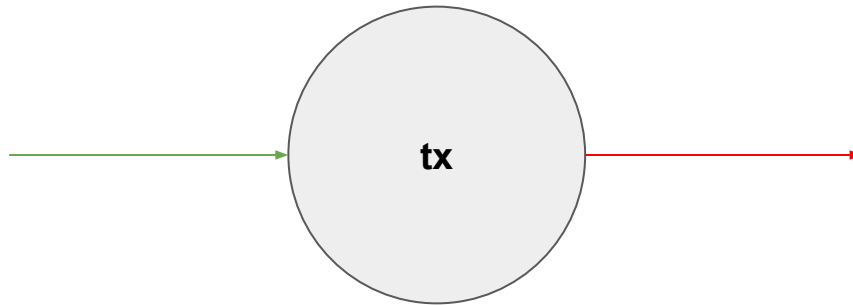
Ακμές συναλλαγών

- 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





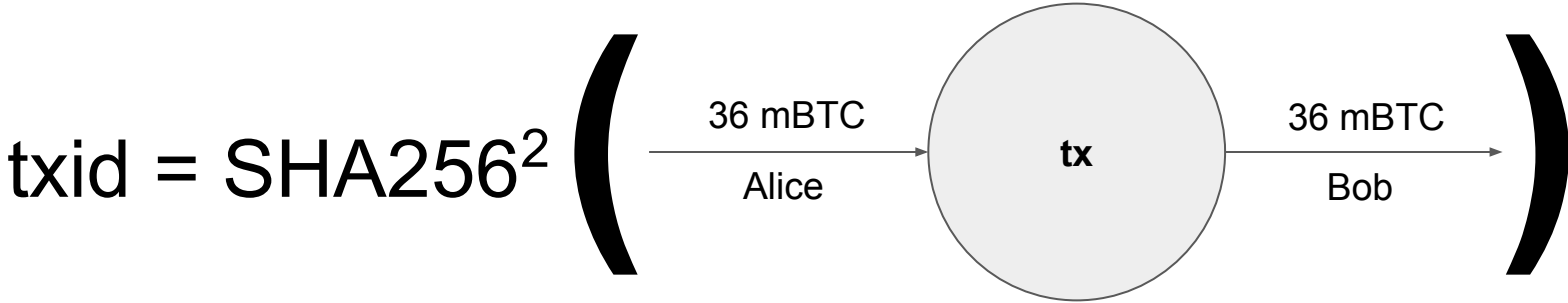
είσοδος / input

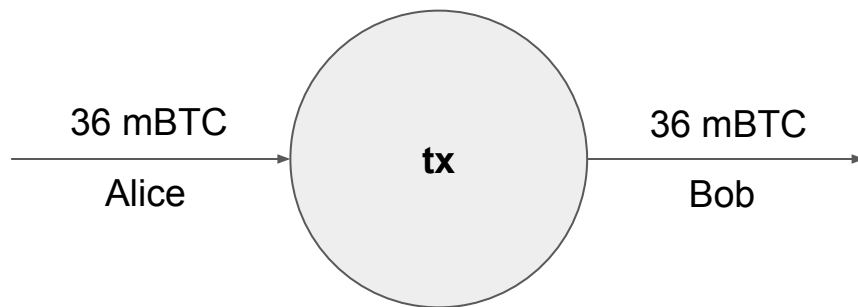


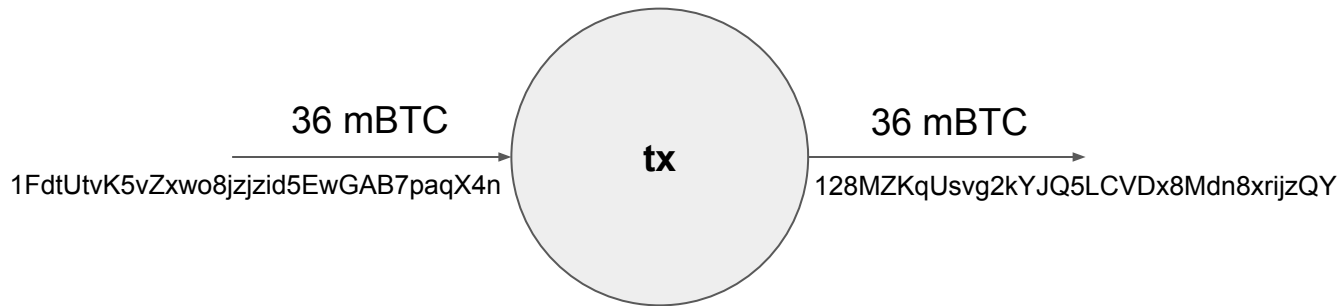
έξοδος / output

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)**



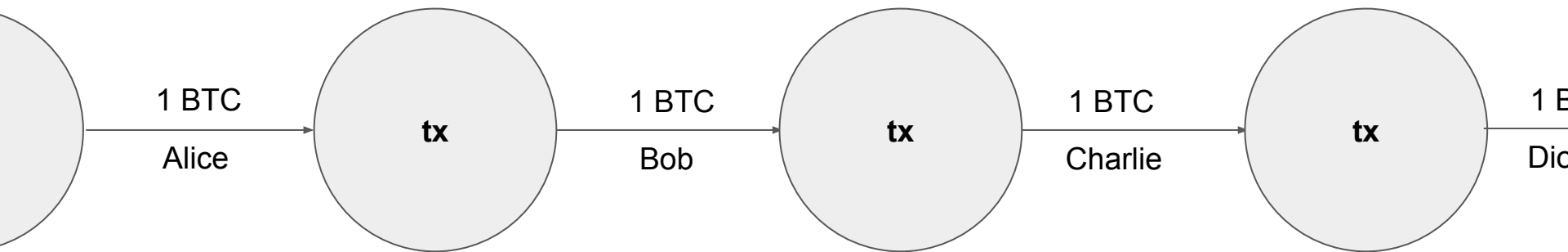




Δημόσιες συναλλαγές στο
blockchain.com

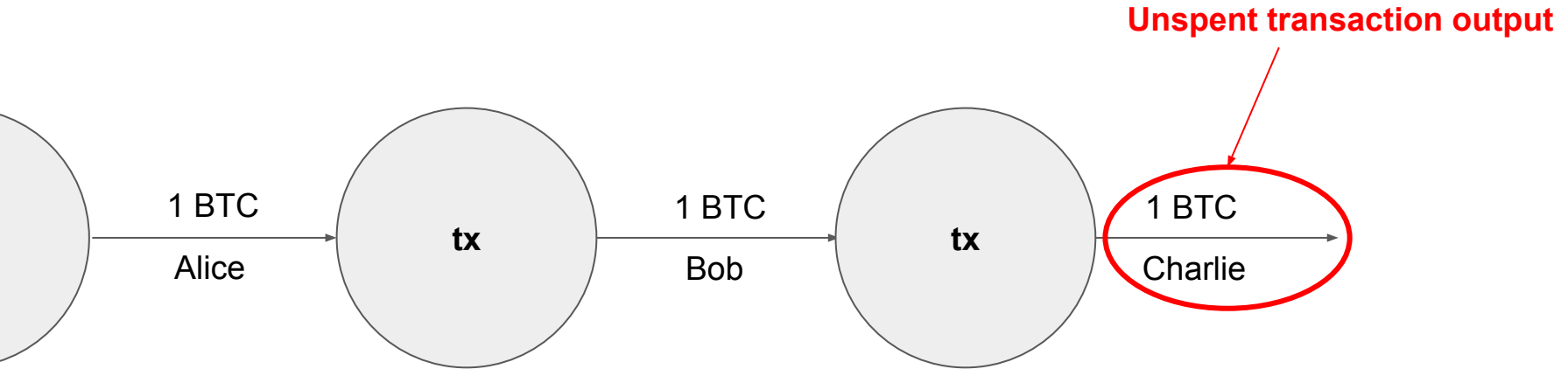
Ο γράφος συναλλαγών

- 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;

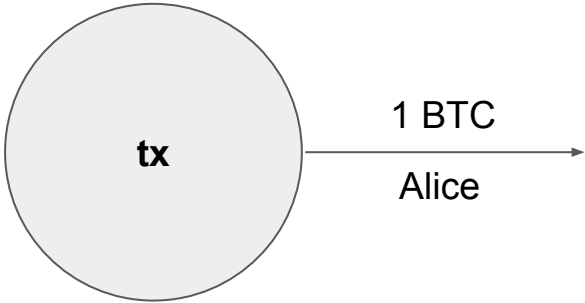
- Παράγω ένα νέο ιδιωτικό κλειδί, αντίστοιχο δημόσιο, και αντίστοιχη διεύθυνση
- Είναι σημαντικό να αλλάζουμε διευθύνσεις για λόγους ανωνυμίας
- **Στέλνω τη διεύθυνση στον πληρωτή** π.χ. μέσω email, FB, QR code κλπ.
- Παρακολουθώ το δίκτυο για κάποια συναλλαγή που με πληρώνει

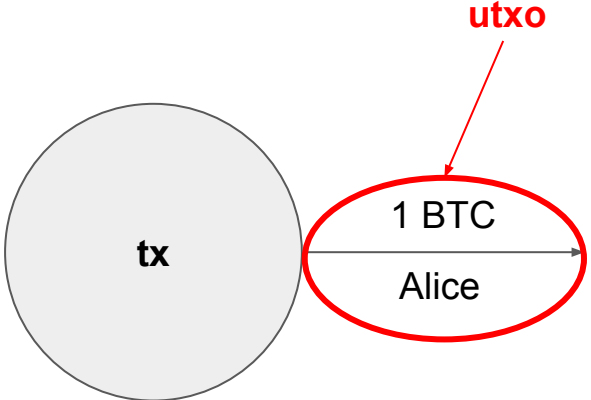
Ποια χρήματα μου ανήκουν;

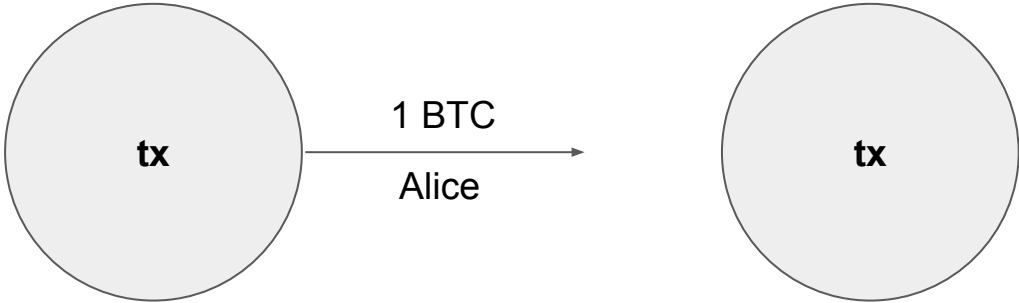
- Όσα βρίσκονται σε UTXO, δηλαδή είναι ακόμη αξόδευτα
 - Διαφορετικά έχω μεταβιβάσει την ιδιοκτησία τους σε κάποιον άλλον
- Στην εξερχόμενη ακμή αναγράφομαι ως ιδιοκτήτης
- Δηλαδή αναγράφεται ένα **δημόσιο** κλειδί για το οποίο κρατώ το ιδιωτικό κλειδί

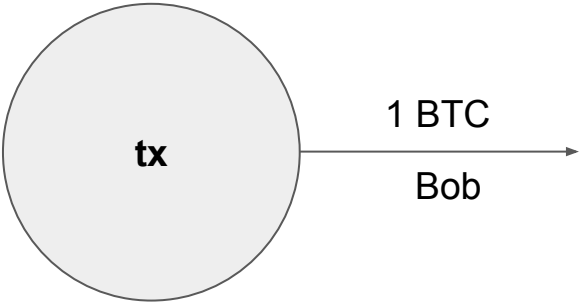
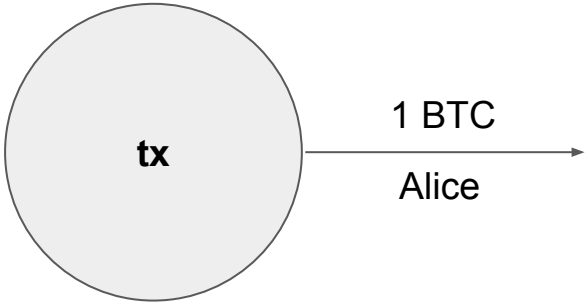
Πώς ξοδεύω χρήματα;

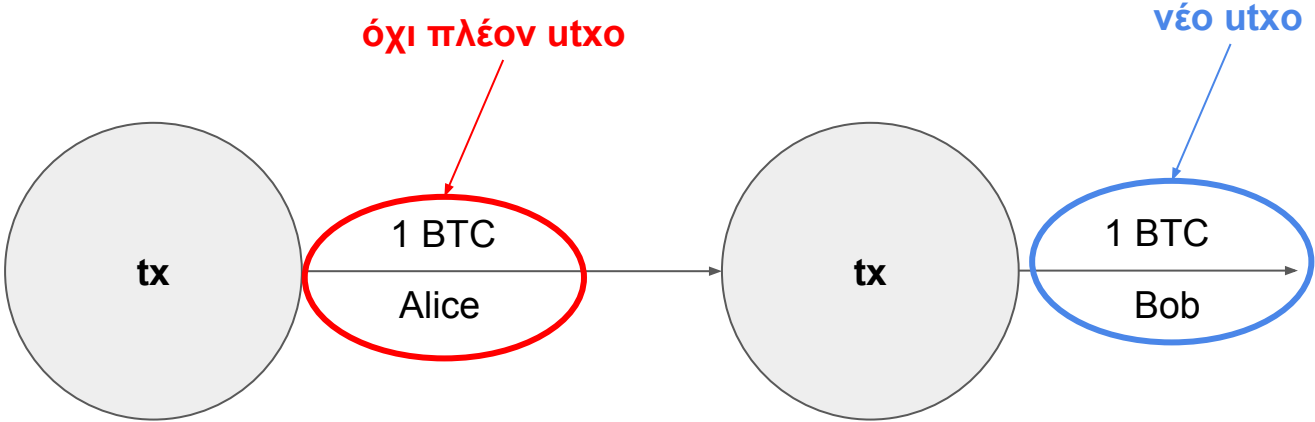
- Βρίσκω μία συναλλαγή που έχει UTXO
- Βεβαιώνομαι ότι **είμαι ο ιδιοκτήτης** της εξερχόμενης ακμής
- Δημιουργώ μία **νέα συναλλαγή**
- **Με μία εισερχόμενη και μία εξερχόμενη ακμή**
- Συνδέω την **εισερχόμενη ακμή της νέας** συναλλαγής με το **παλιό UTXO**
- Πλέον το παλιό utxo δεν είναι πλέον utxo – 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)







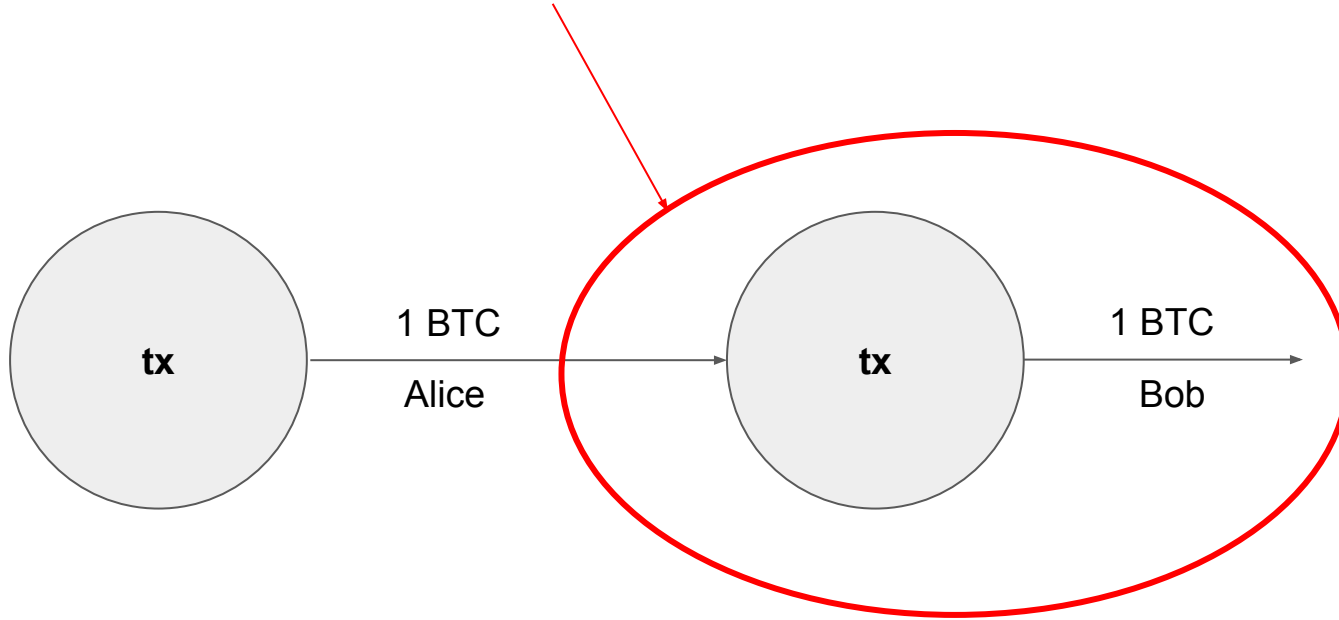


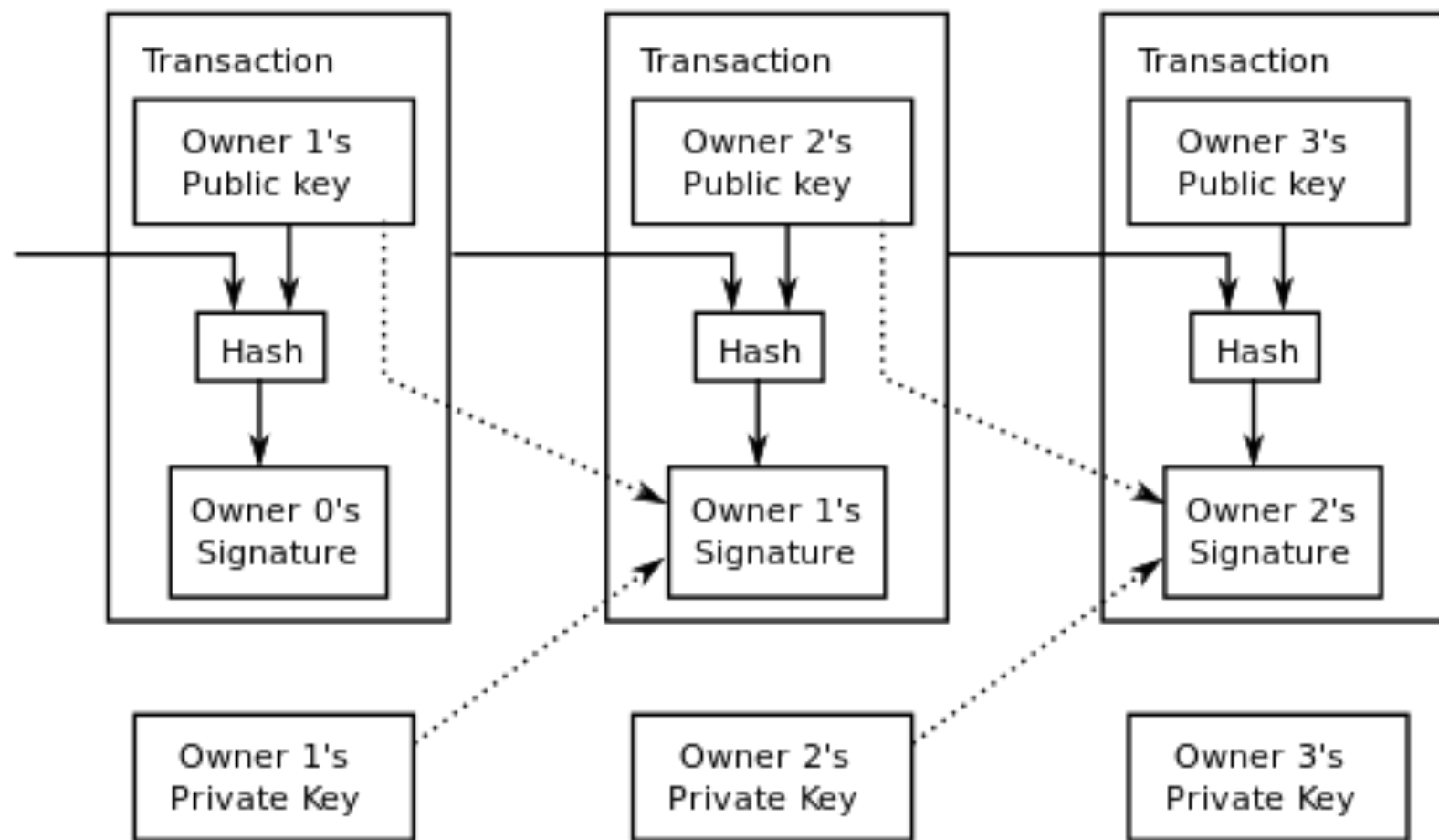


Απόδειξη ιδιοκτησίας

- 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



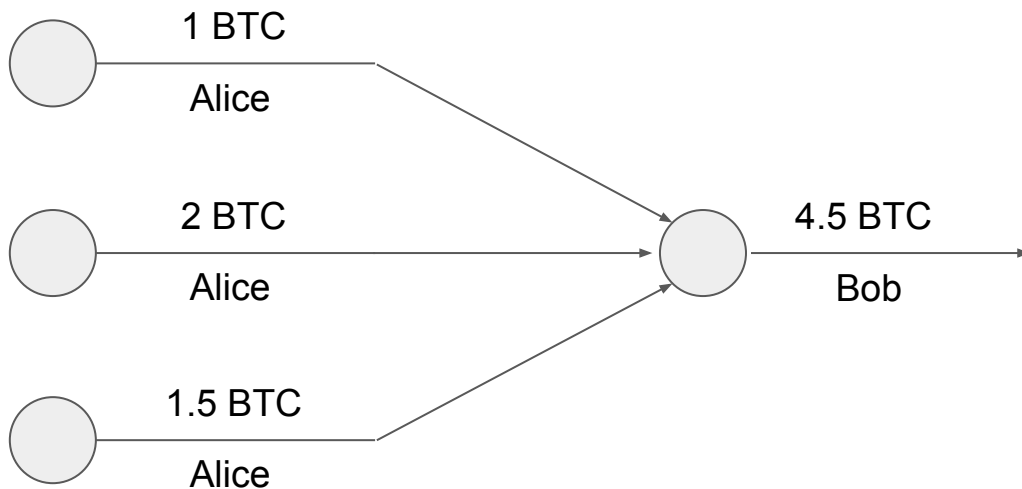


Transaction broadcasting

- **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

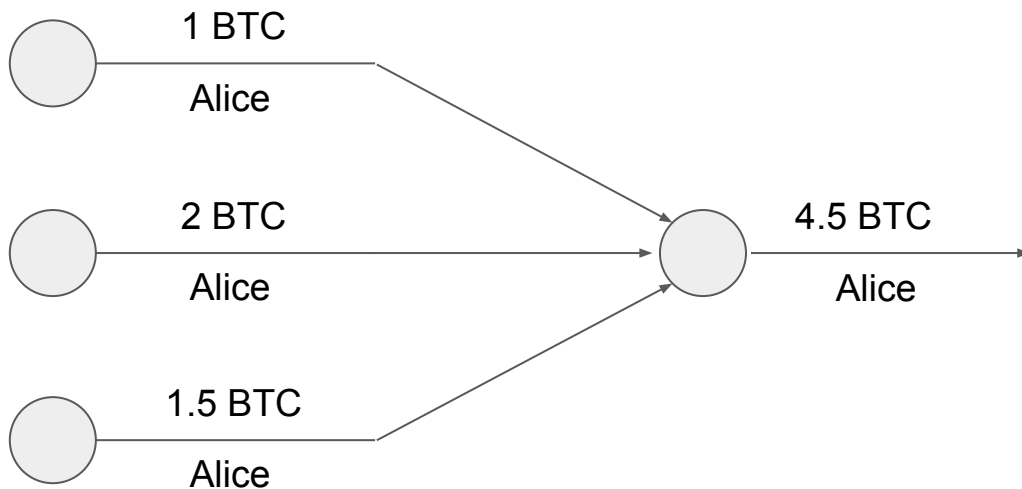
Μία συναλλαγή - πολλές είσοδοι

- 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



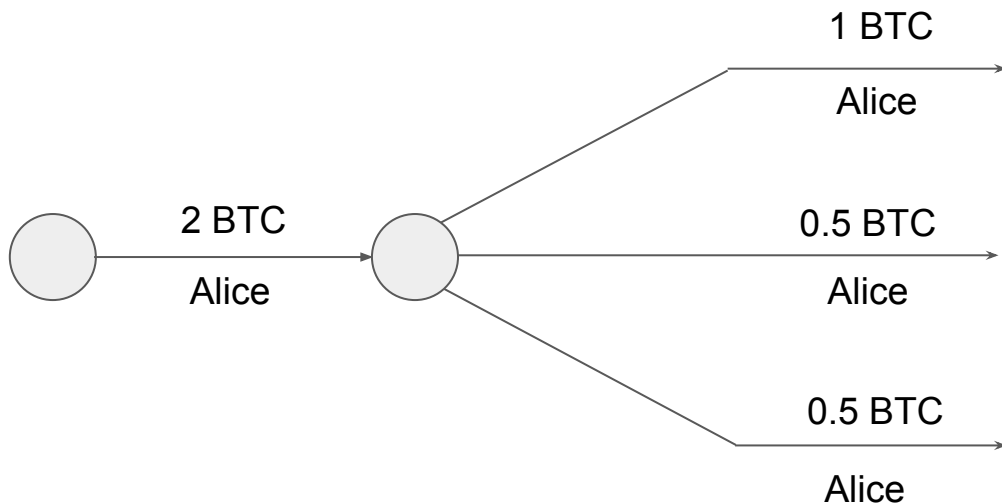
Μία συναλλαγή - πολλές είσοδοι

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



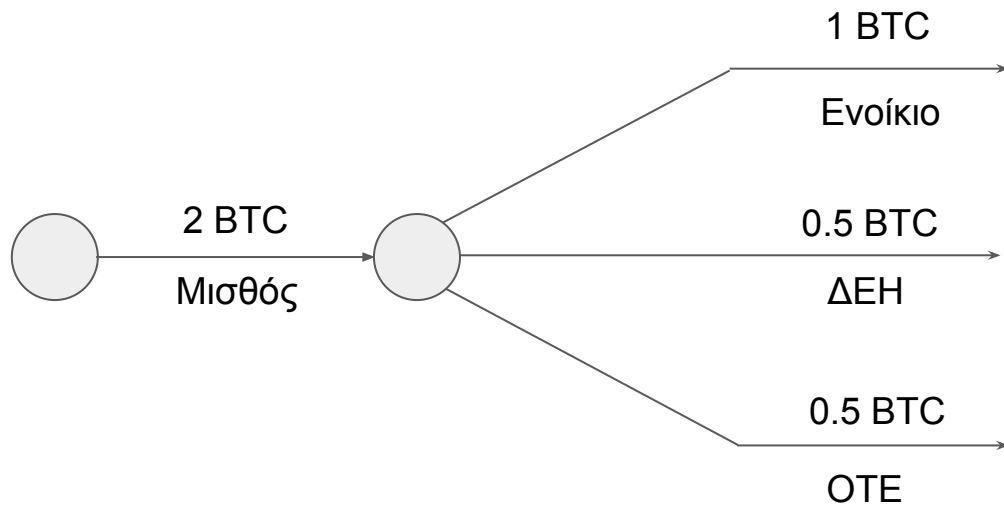
Μία συναλλαγή - πολλές έξοδοι

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



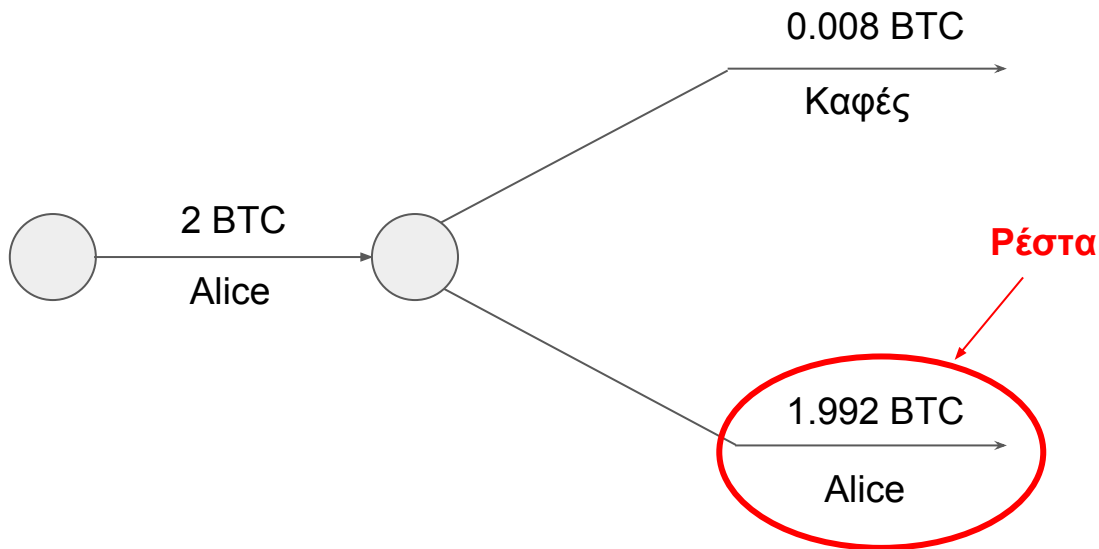
Μία συναλλαγή - πολλές έξοδοι

- 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 υτχο, δεν περιμένω από τον πωλητή



Αρχή διατήρησης του Kirchhoff

$\forall tx \in txs:$

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

Αρχή διατήρησης του Kirchhoff

Όλες οι συναλλαγές του κόσμου

$$\forall tx \in txs:$$
$$\sum_{i \in in(tx)} w(i) \geq \sum_{o \in out(tx)} w(o)$$

Αξία εισόδου

Αξία εξόδου

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 συναλλαγής 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

Πορτοφόλι

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

Desktop wallet - Exodus

The screenshot shows the Exodus desktop wallet interface. The top bar displays "EXODUS 1.59.2". The left sidebar contains navigation options: Portfolio, Wallet, Exchange, Backup, Settings, and Help. The main area shows a list of assets: Binance (0 BNB), Bitcoin (0 BTC), Bitcoin Cash (0 BCH), Decred (0 DCR), DigiByte (0 DGB), Ethereum (0 ETH), Monaco (0 MCO), TenX (0 PAY), Zcash (0 ZEC), and a "+ Add More" button. The Bitcoin section is highlighted, showing a balance of 0 BTC and €0.00 EUR, with "Send" and "Receive" buttons. Below this is a transaction history table.

Date	Type	Amount
JAN 31	Sent	0.01604578
JAN 30	Received	+ 0.01652982
JAN 28	Sent	0.15987421
JAN 28	Received	+ 0.16053
DEC 17	Sent	0.0577843
DEC 17	Received	+ 0.05853004
NOV 0	Sent	0.16434618


Mobile wallet - Android

Bitcoin 3G 10:51

SEND COINS ADDRESS BOOK PEER MONITOR

BTC 1.1163
≈ EUR 55.7050

Your Bitcoin Address:
1KGe NiDw zH5N
rdwN ETj3 hQEx
wr5H MN9e FW



			Received	Both	Sent
	balance	67.9065			
CNY	rate	416.78	● Apr 6 ←	1719Pmohr5CkidX6mQ9zYj4nTPnGDf5...	+ 0.0050
	balance	465.2653	● Apr 5 ←	Beer with Lisa	+ 0.0050
DKK	rate	328.56	● Apr 5 →	1Q4H8CY4FpnJ93SPbdz4Cqgv714KXae...	- 3.5005
	balance	366.7824	● Apr 4 →	Burger @ room77	- 0.0754
EUR (default)	rate	49.90	● Apr 4 ←	1G9Hjz1JCUqnhNQmpxLhsVL6FD8Coo4...	+ 2.2452
	balance	55.7050	● Apr 4 ←	Donation	+ 0.05
GBP	rate	40.74	● Apr 3 ←	1FUgQeguKnVFavXYqKwYB7g4YKXJ4REKjh	+ 0.05
	balance	45.4794			
HKD	rate	506.94			

Use at your own risk. Read the [safety notes](#).

Ιστορία του bitcoin

1983: David Chaum, “e-cash”: Κεντρικά ελεγχόμενο ηλεκτρονικό χρήμα

1998: Wei Dai, “bmoney”: Πρώτες αποκεντρωμένες ιδέες

2005: Nick Szabo, “bit gold”: Πρώτες ιδέες για χρήση PoW σε χρήμα

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

A young woman with blonde hair is shown in a close-up, crying. Her eyes are closed, and her mouth is open in a pained expression. Her right hand is pressed against her forehead, partially covering her eyes. The background is a soft, out-of-focus yellowish-green. The image is overlaid with large, bold, white text with black outlines.

LEAVE SATOSHI

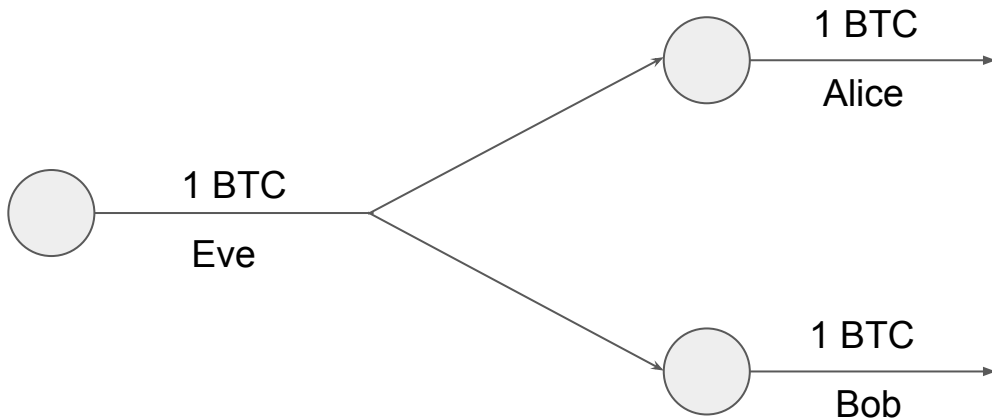
ALONE!

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

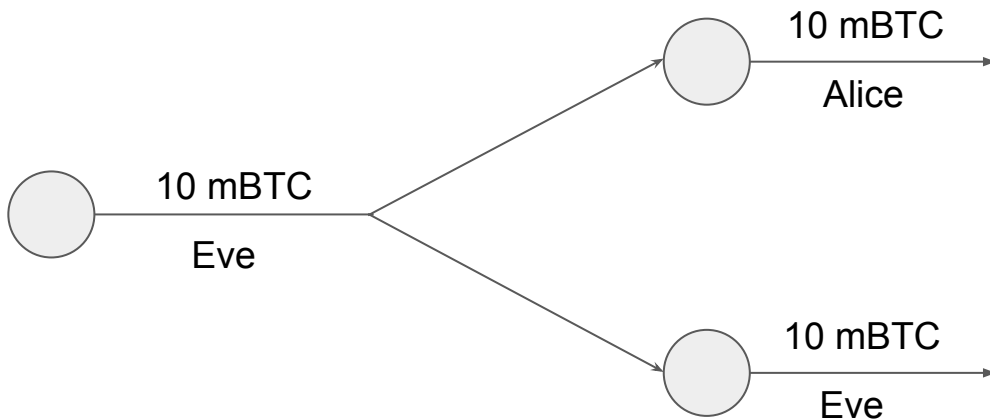
Double spending

- 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

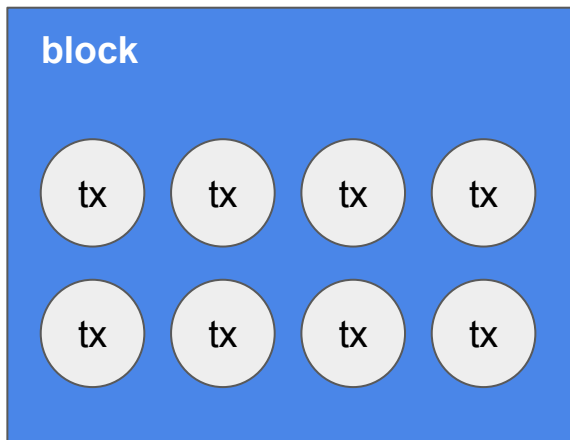


Το βέλος του χρόνου

- Θέλουμε να βάλουμε τις συναλλαγές σε μία σειρά
- Πρέπει να μπορούμε να απαντήσουμε στην ερώτηση: Η συναλλαγή A έγινε πριν την συναλλαγή B;
- Η απάντηση πρέπει να είναι **κοινή για όλους στο δίκτυο**
- Η συμφωνία σε μία κοινή αλήθεια όσο αφορά την ακολουθία συναλλαγών ονομάζεται **consensus**

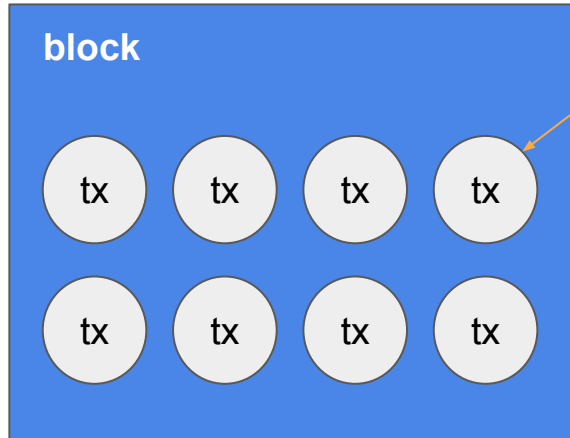
Block

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

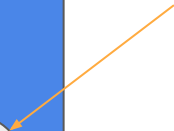


Block

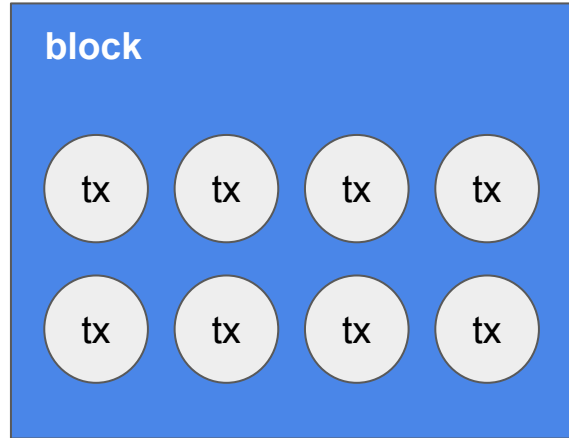
- Το δίκτυο φροντίζει να δημιουργείται καθολικά **ένα block κάθε 10 λεπτά**
- Το block που δημιουργείται κάθε 10 λεπτά περιλαμβάνει τις **πιο πρόσφατες συναλλαγές** που **δεν υπήρχαν** σε προηγούμενα blocks
- Τα blocks γίνονται **broadcast** και **relay** στο δίκτυο όπως οι συναλλαγές
- Το SHA256 των δεδομένων του block είναι το **block id**
- Μία συναλλαγή που περιλαμβάνεται σε έγκυρο block λέγεται **confirmed**



**confirmed
transaction**

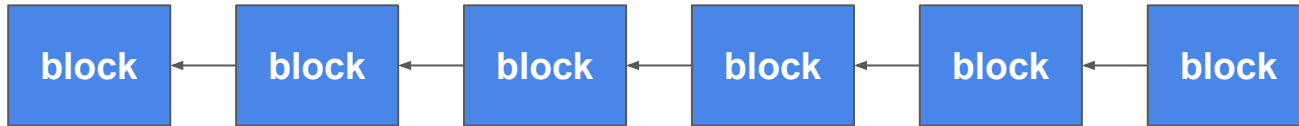


blockid = SHA256



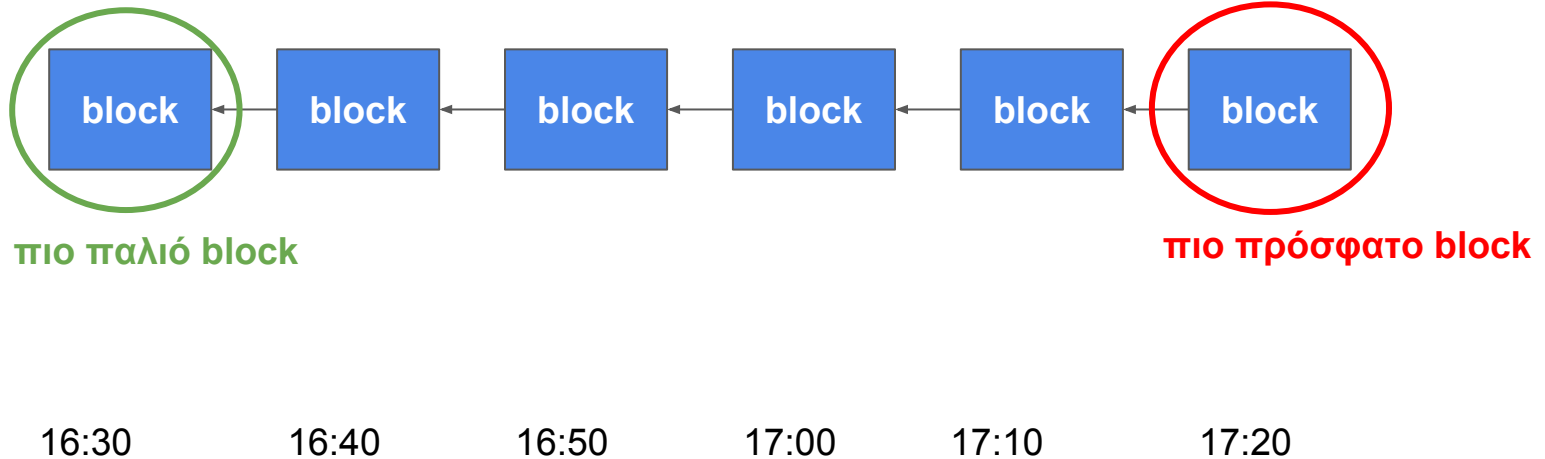
Blockchain

- 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**



Blockchain

- Επιτυγχάνει **consensus**
- Η συναλλαγή A προηγείται της συναλλαγής B αν η A περιλαμβάνεται σε προηγούμενο **block** από την B
- Αν θέλουμε να σιγουρευτούμε ότι δεν θα γίνει double spend, πρέπει να περιμένουμε το transaction να γίνει confirm

Blocks στο blockchain.com

Η παραβολή του βιβλίου που δεν τελειώνει ποτέ



Ένα “βιβλίο” συναλλαγών

- Κάθε νέα σελίδα απαιτεί προσπάθεια για να παραχθεί
- Οποιοσδήποτε μπορεί να παράγει μια σελίδα
- Οι σελίδες μπορούν να παράγονται διαρκώς εφόσον υπάρχουν ενδιαφερόμενοι που τις παράγουν



Η σημασία του consensus

- Εάν υπάρχουν διαφορετικά βιβλία τα οποία έρχονται σε αντίθεση, ποιο είναι το “σωστό” ;

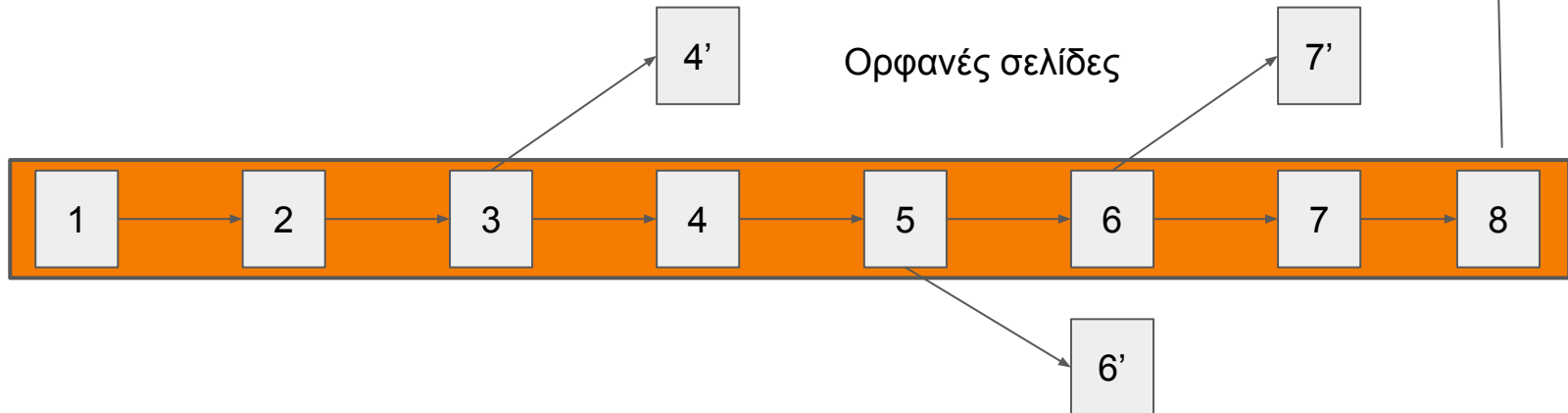
Επιλέγοντας το σωστό βιβλίο



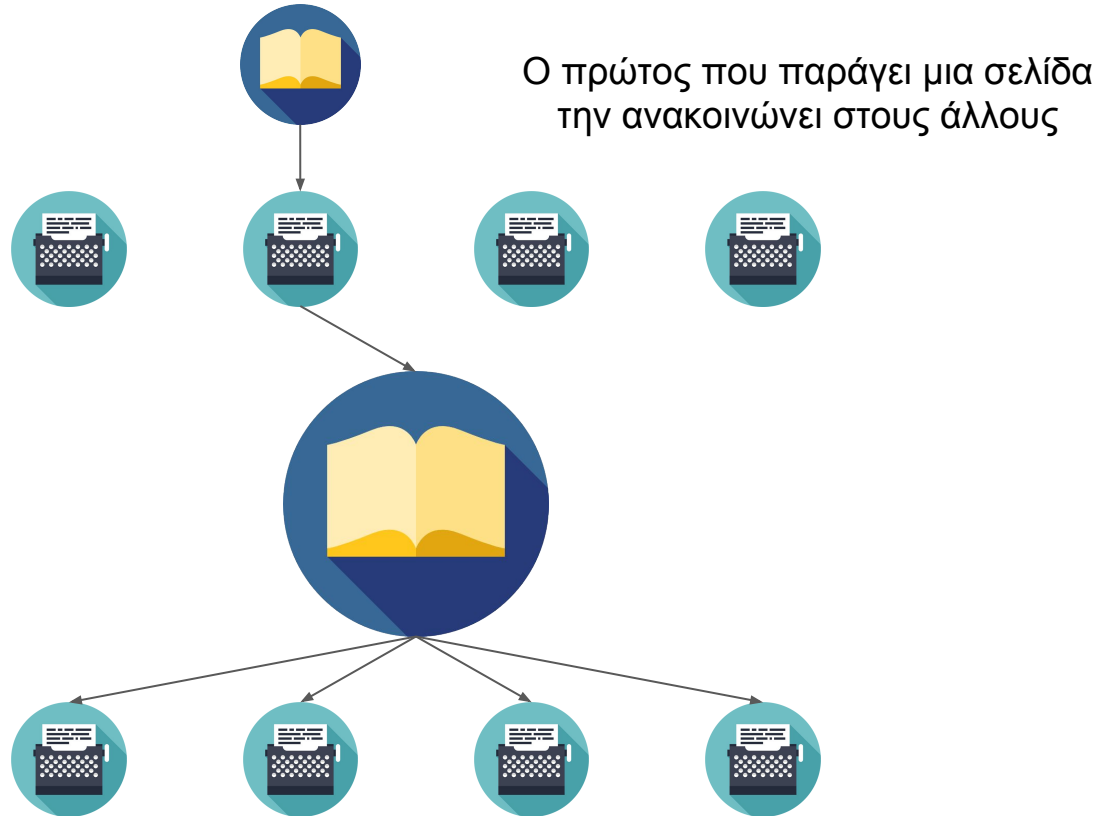
Το **σωστό βιβλίο** είναι αυτό που περιέχει τις περισσότερες σελίδες. Αν υπάρχουν πολλά, επέλεξε ένα στην τύχη.

Κατασκευάζοντας το τρέχον βιβλίο

- Κάθε σελίδα αναφέρεται στην προηγούμενη σελίδα
- Το τρέχον βιβλίο κατασκευάζεται συνδυάζοντας τη μακρύτερη σειρά σελίδων

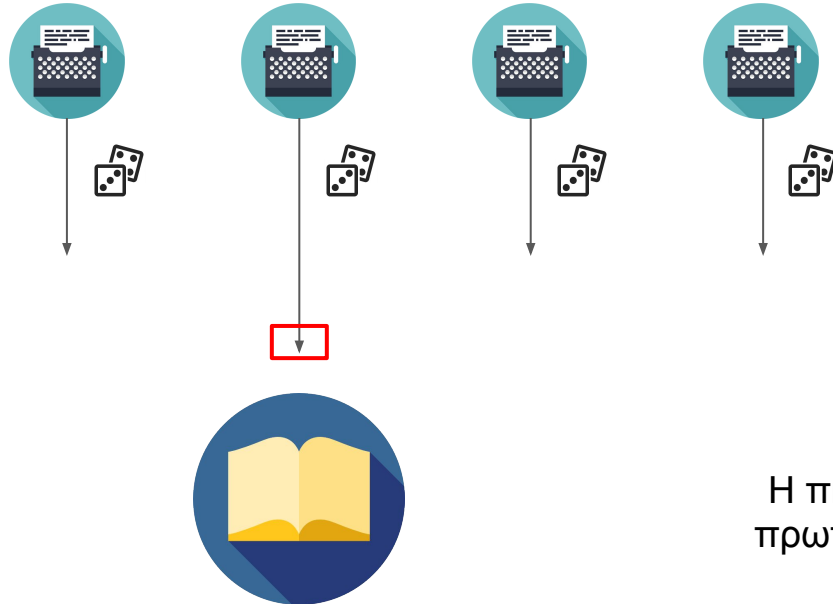


Κανόνες επέκτασης του βιβλίου



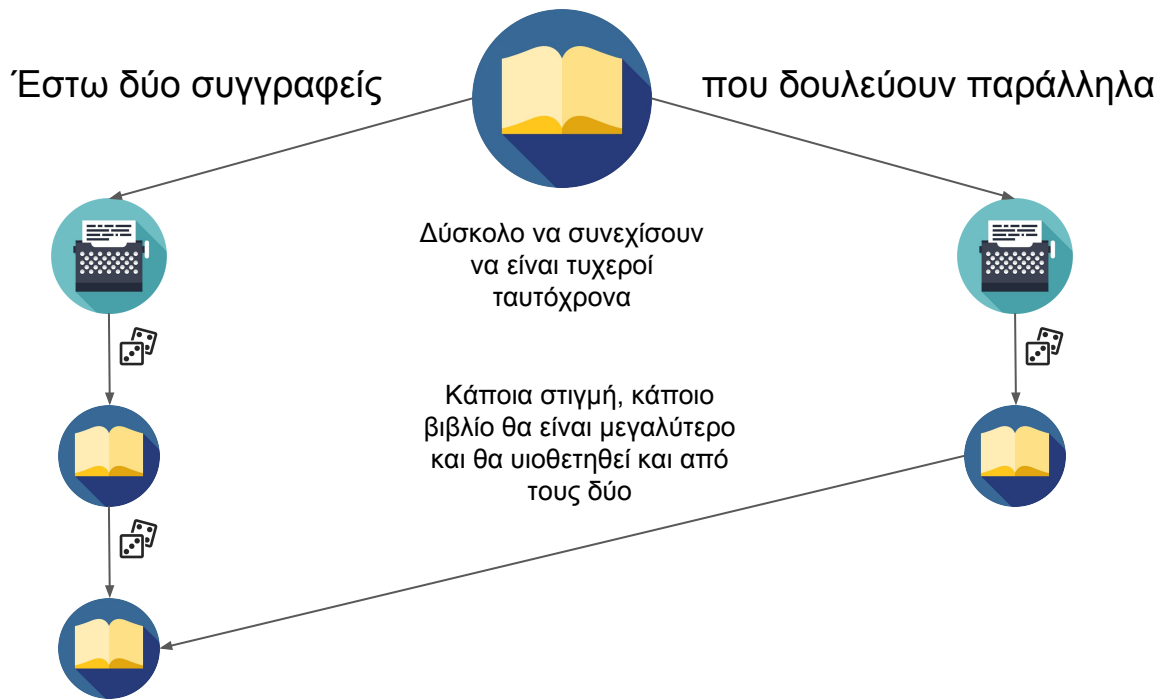
Χρειάζεται προσπάθεια για να παραχθεί μια σελίδα

Ισοδύναμα: κάθε σελίδα θέλει ένα συγκεκριμένο συνδυασμό από ένα σύνολο ζευγαριών από ζάρια



Η πιθανοτική διαδικασία είναι πρωταρχικής σημασίας για την ασφάλεια

Τα πλεονεκτήματα της τυχαιότητας

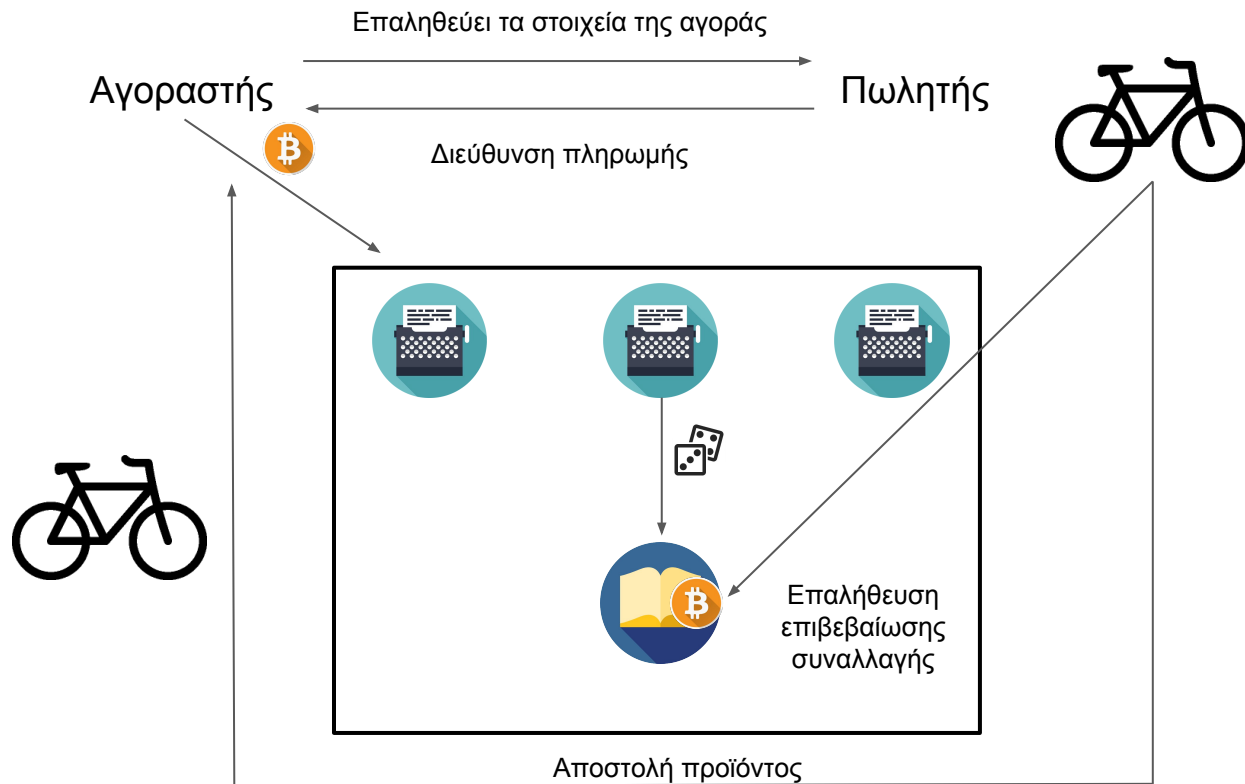


Η συμμετρία σπάει



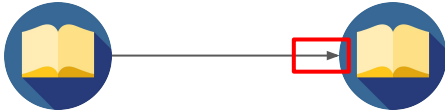

Το να είσαι συγγραφέας

- Ο καθένας μπορεί να γράψει στο βιβλίο
- Αρκεί να έχει ένα σύνολο από ζάρια
- Όσο περισσότερα ζάρια έχει τόσο μεγαλύτερη η πιθανότητα να παράγει έναν νικηφόρο συνδυασμό και να παράγει μια σελίδα

Χρησιμοποιώντας το βιβλίο



Παραβολή και πραγματικότητα

	Blockchain
	Miners
	Solving a cryptographic puzzle that is moderate hard to solve
	Using a computer to test for a solution from a large space of candidate solutions

Ποιος παράγει τα blocks?

- **Καθένας** μπορεί να παράξει ένα block
- Το σύστημα είναι ελεύθερο στον οποιονδήποτε
- Κάθε block πρέπει να περιέχει μία **απόδειξη εργασίας SHA256²**
- Η απόδειξη εργασίας έχει **δυσκολία** που είναι τέτοια ώστε το **συνολικό δίκτυο** του bitcoin να παράγει **1 block ανά 10 λεπτά σε αναμενόμενη τιμή**

$$E(\text{block generation time}) = 10 \text{ min}$$

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

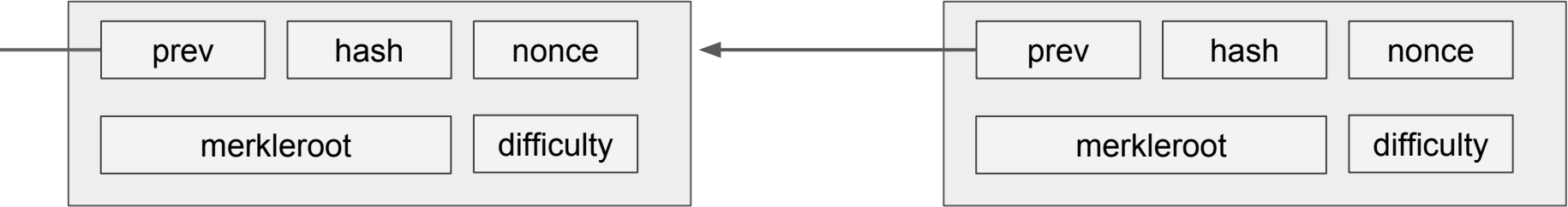
- Παρακολουθούμε το δίκτυο για **συναλλαγές** και **blocks**
- Περιλαμβάνουμε στο **υποψήφιο block** μας:
 - Όλες τις **συναλλαγές** που δεν έχουν εμφανιστεί σε προηγούμενο block που γνωρίζουμε
 - Μία αναφορά στο πιο πρόσφατο block που γνωρίζουμε ως **πατέρα**
- Αναζητούμε **απόδειξη εργασίας**
 - Η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

$$H(\text{txs} \parallel \text{nonce} \parallel \text{parent-blockid}) < T$$

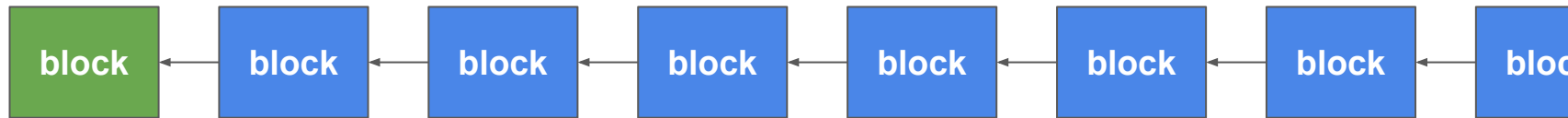
Εγκυρότητα ενός block

- 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



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

Good restaurants across the UK

Israel prepares to send tanks and troops into Gaza



Chancellor on brink of second bailout for banks

Billions more for banks as banking system's lightness

By Andrew Ross
The Chancellor has been forced to announce a second bailout for banks, this time to cover the cost of a new £200bn rescue package for the banking system. The move is seen as a sign of the government's determination to prevent a collapse of the financial system, which would have had catastrophic consequences for the economy. The package includes a £50bn guarantee for banks' deposits, a £50bn loan to the banks, and a £100bn loan to the banks to cover the cost of their losses. The Chancellor also announced that the government will provide a £20bn loan to the banks to cover the cost of their losses. The move is seen as a sign of the government's determination to prevent a collapse of the financial system, which would have had catastrophic consequences for the economy.

99p



Michael Stern Ernst, Nelson and me



Working mums
So that's how
she does it



Demos, in style
The best spots
on the planet



Salman Rushdie I won't marry again

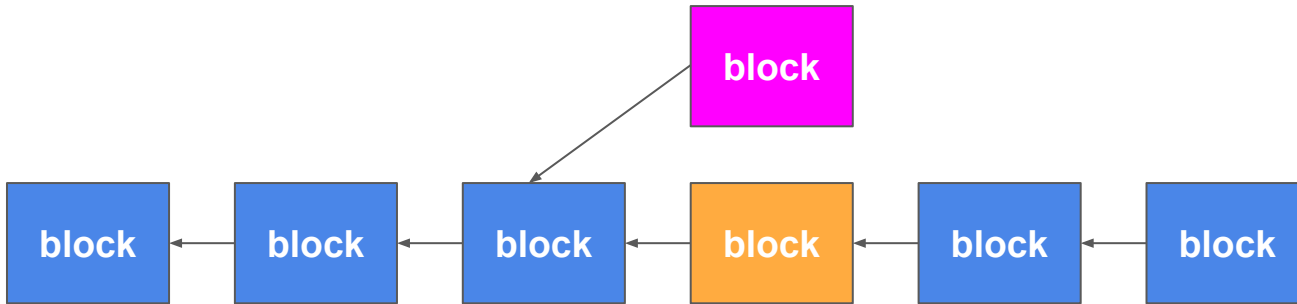


Giant killing?
Guide to the FA
Cup third round



Blockchain forks

- Κάποιες φορές μπορεί να γίνουν mine 2 έγκυρα blocks ταυτόχρονα
- Αυτό δημιουργεί ένα **blockchain fork**

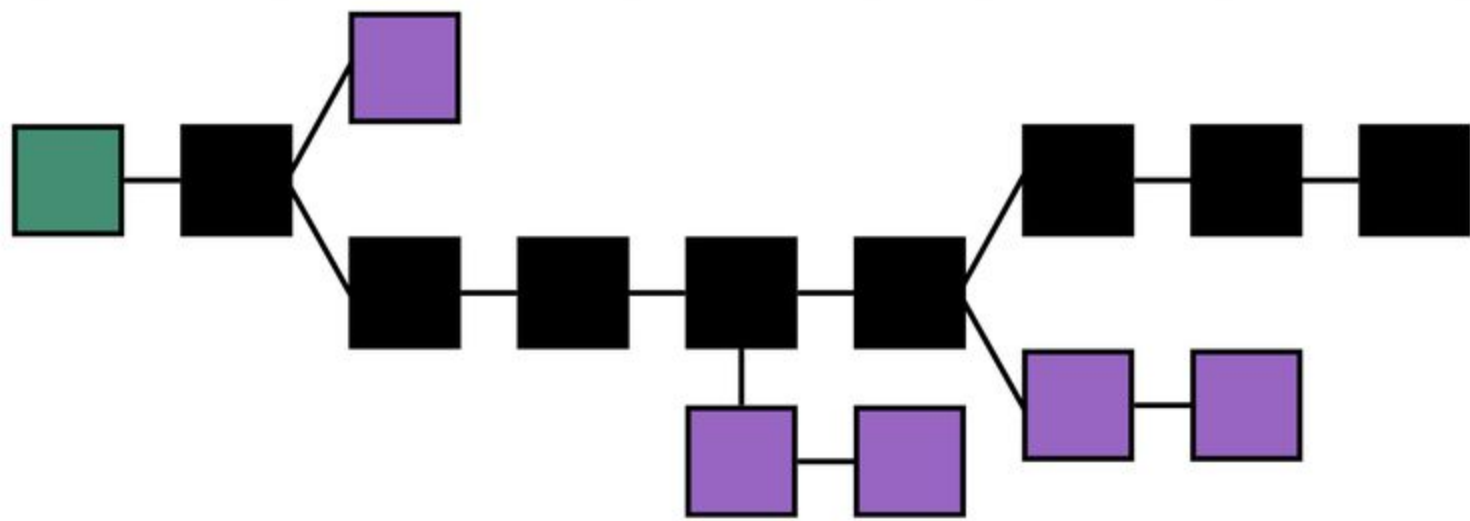


Blockchain fork

- 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

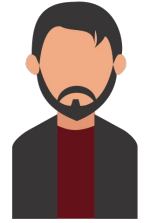
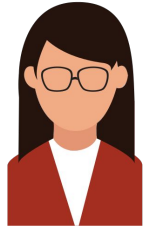
- Παρατηρούμε δύο αντίπαλα blockchains στο δίκτυο
- Το έγκυρο blockchain είναι το blockchain με **το μέγιστο ύψος**
- Αν δύο αντίπαλα blockchains έχουν το ίδιο ύψος, τότε επιλέγουμε κάποιο **αυθαίρετα**
- Το block που επιλέγουμε ως miners είναι αυτό πάνω στο οποίο κάνουμε εξόρυξη
- Το block που επιλέγουμε ως χρήστες είναι αυτό που εμπιστευόμαστε για transaction confirmation



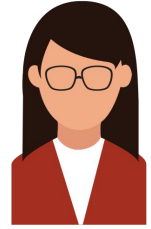
Double spending



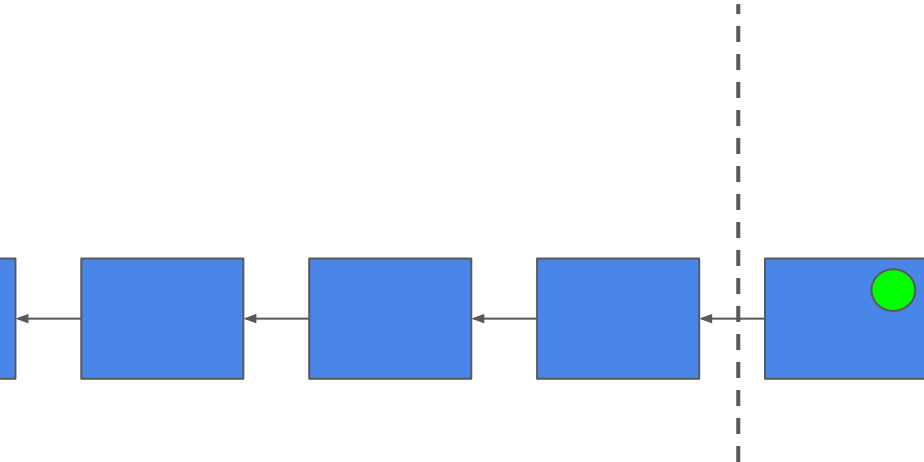
Double spending



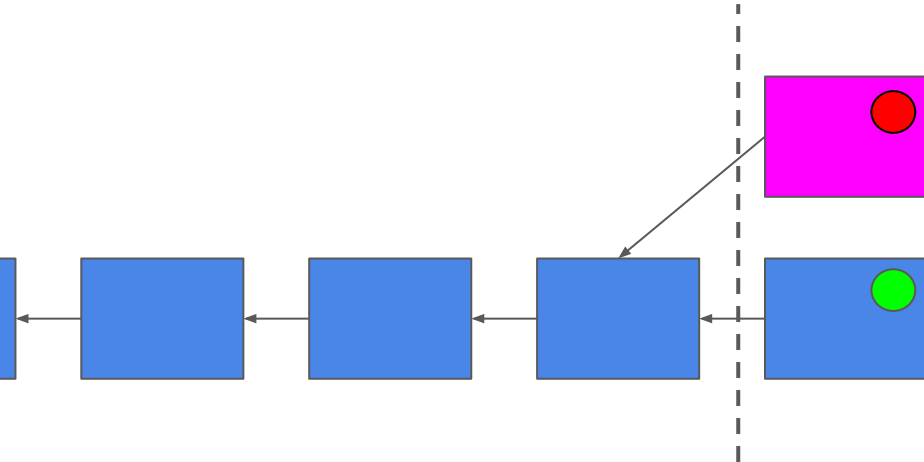
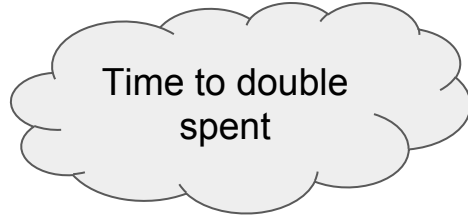
Double spending



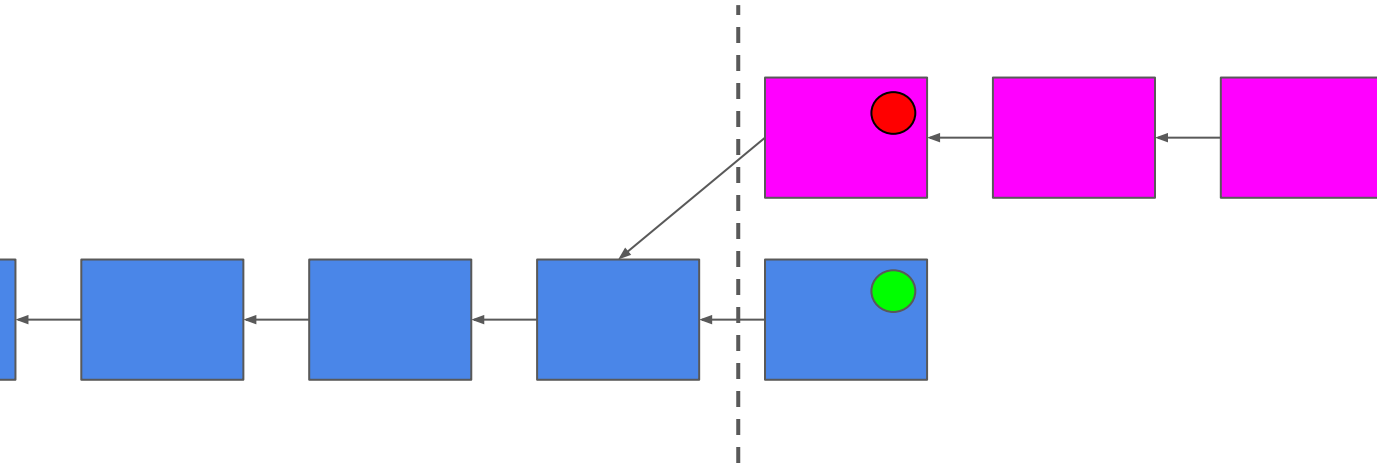
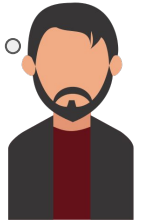
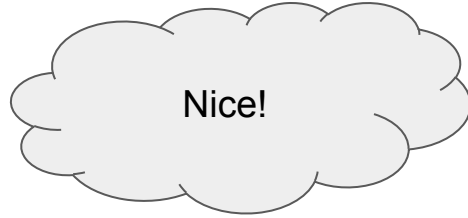
101
010



Double spending



Double spending

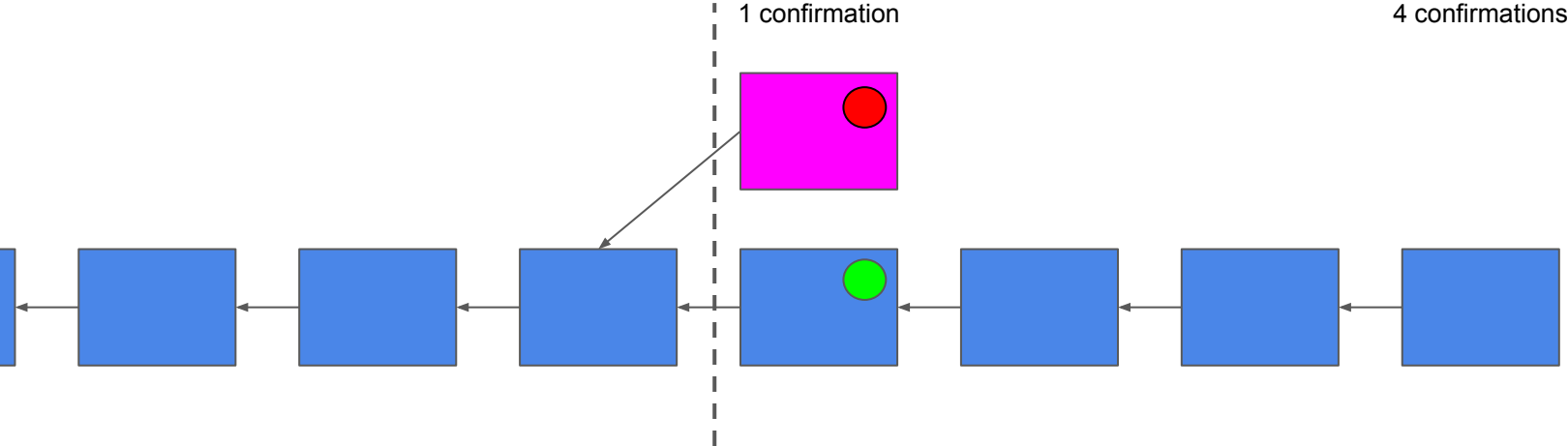


Double spending

Ok, Alice paid and I see 4 confirmations

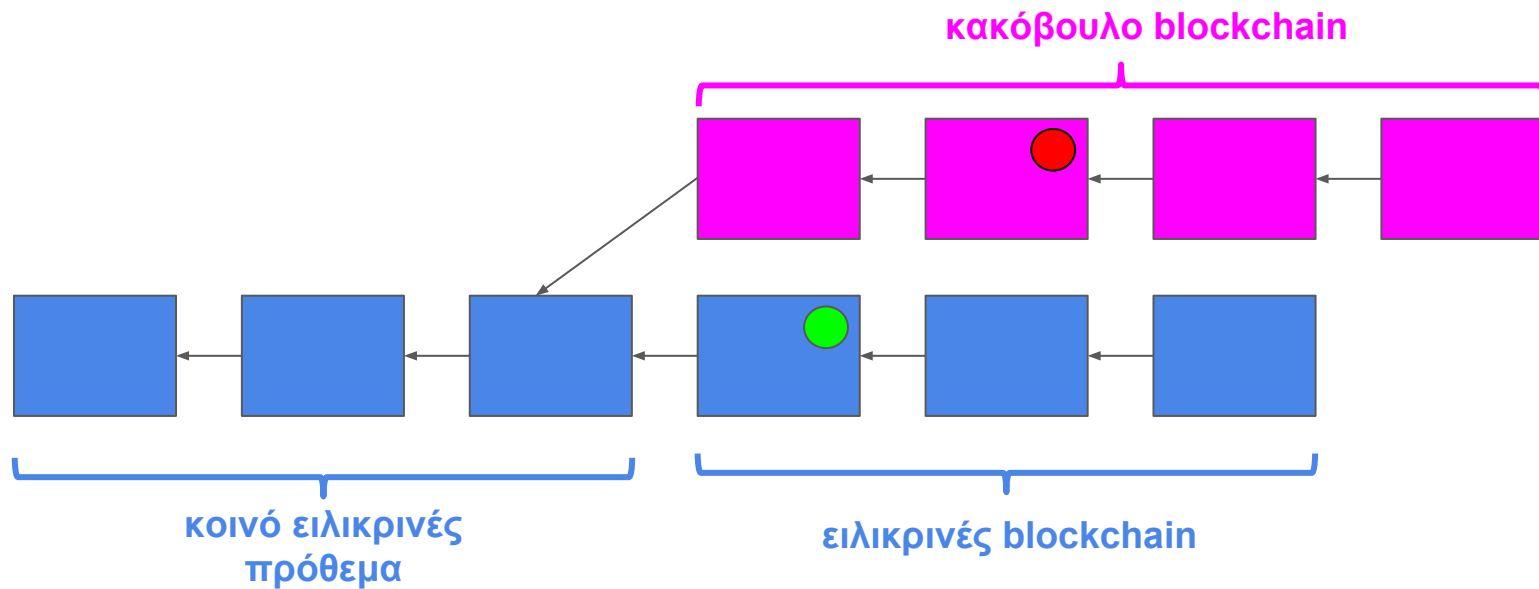


101
010



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 δικτύου
- 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:

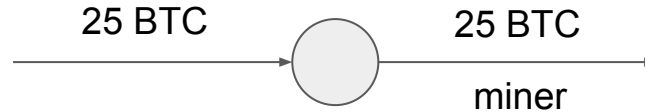
1. Με όλα τα περισσευούμενα χρήματα στις συναλλαγές που κάνει confirm:

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

Κίνητρα mining

- Ένας miner ανταμείβεται με 2 τρόπους:

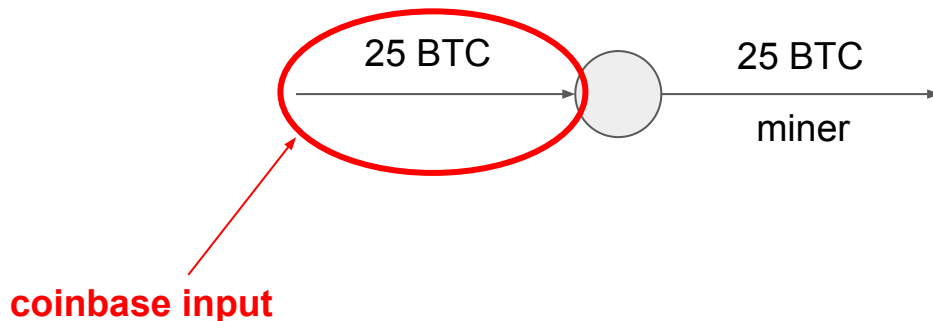
2. Με ένα coinbase transaction που επιτρέπεται να βάλει στο block αξίας 25 BTC



Κίνητρα mining

- Ένας miner ανταμοίβεται με 2 τρόπους:

2. Με ένα coinbase transaction που επιτρέπεται να βάλει στο block αξίας 25 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

Αξία του bitcoin

- Εξαιρετικά μεταβλητή
- Σήμερα, 2018: **1 BTC = 6,491 EUR**
- Τέλος 2017: 1 BTC = 17,000 EUR
- Αρχές 2015: 1 BTC = 208 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 Μαΐου 2010: Πρώτη αγορά μέσω bitcoin



22 Μαΐου 2010: Μία pizza για 10,000 BTC

Bitcoin Charts

Linear Scale Log Scale  

Zoom 1d 7d 1m 3m **1y** YTD ALL

From Sep 20, 2017 To Sep 20, 2018



Μάθαμε

- Τι είναι το bitcoin
- Διευθύνσεις, κλειδιά
- Συναλλαγές, ρέστα
- Γράφος του bitcoin, ακμές, κόμβοι, αξίες, ιδιοκτήτες, utxo, coinbase
- Εξόρυξη, consensus, blockchain, genesis
- Proof-of-work, δυσκολία, confirmations, ανταμοιβές, fees
- Αξία του bitcoin
- Πορτοφόλια