Ψηφιακά Νομίσματα, Bitcoin

Αν. Καθηγητής Π. Λουρίδας

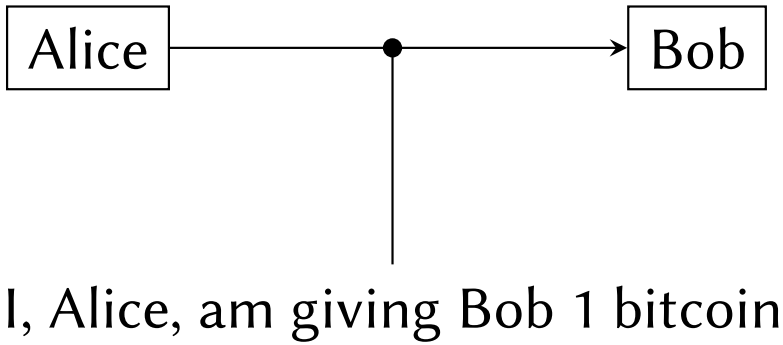
Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας,
Οικονομικό Πανεπιστήμιο Αθηνών
louridas@aueb.gr

Επισκόπηση

Πρώτο Βήμα

- Η Alice θέλει να στείλει ένα ποσό χρημάτων στον Bob.
- Δημιουργεί ένα μήνυμα “I, Alice, am giving Bob 1 bitcoin”.
- Στέλνει το μήνυμα στον Bob.

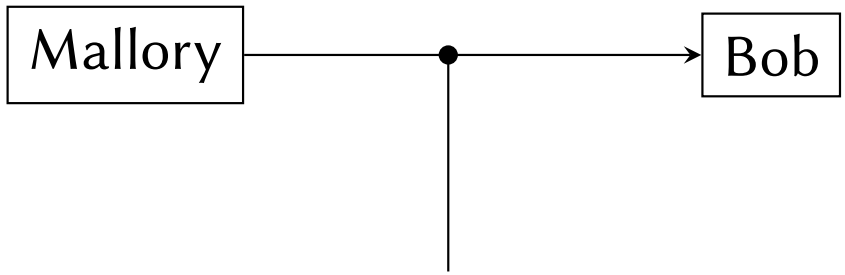
Πρώτη Προσπάθεια



Πρόβλημα

- Έστω ότι ο Mallory στέλνει το ίδιο μήνυμα στον Bob.
- Πώς μπορεί να ξέρει ο Bob ότι πράγματι η Alice του έστειλε τα χρήματα, και ότι το μήνυμα είναι αυθεντικό;

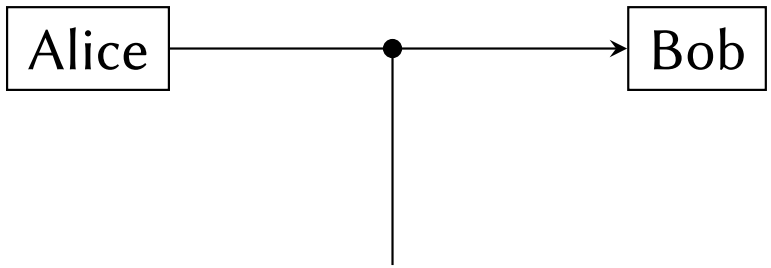
Πρόβλημα



Δεύτερη Προσπάθεια

- Η Alice θέλει να στείλει ένα ποσό χρημάτων στον Bob.
- Δημιουργεί ένα μήνυμα “I, Alice, am giving Bob 1 bitcoin”.
- Το υπογράφει με το μυστικό της κλειδί.
- Στέλνει το μήνυμα στον Bob.
- Ο Bob μπορεί να εξακριβώσει ότι είναι από την Alice ελέγχοντάς το με το δημόσιο κλειδί της.

Δεύτερη Προσπάθεια



$E_{S(A)}$(“I, Alice, am giving Bob 1 bitcoin”)

Ο Bob, που έχει το δημόσιο κλειδί της Alice θα ελέγξει την υπογραφή: $E_{P(A)}$(“I, Alice, am giving Bob 1 bitcoin”).

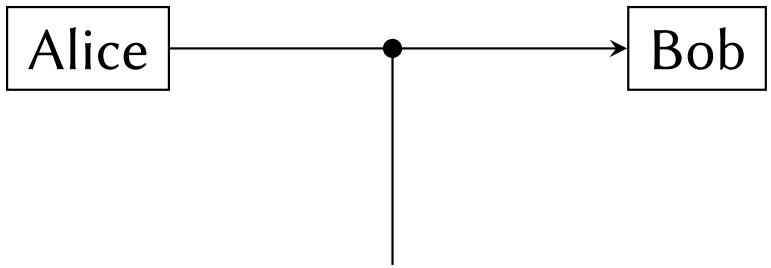
Προβλήματα

- Η Alice μπορεί να στείλει το μήνυμα όσες φορές θέλει και δεν είναι ξεκάθαρο ότι εννοεί ότι θα δώσει άλλο bitcoin κάθε φορά. Το πρόβλημα αυτό είναι γνωστό ως *doublespend*: ξοδεύεις παραπάνω από μία φορά το ίδιο ποσό.
- Ο Mallory μπορεί να υποκλέψει το μήνυμα και να το στείλει και αυτός, υποχρεώνοντας την Alice να κάνει μια δοσοληψία που δεν θέλει.

Τρίτη Προσπάθεια

- Προσθέτουμε σε κάθε νόμισμα ένα μοναδικό σειριακό αριθμό.
- Ο σειριακός αυτός αριθμός θα περιέχεται σε κάθε μήνυμα που μεταφέρει το νόμισμα.

Δεύτερη Προσπάθεια



$E_{S(A)}$(“I, Alice, am giving Bob 1 bitcoin with serial number 1234567”)

Πρόβλημα

- Πώς καθορίζονται οι σειριακοί αριθμοί;
- Ποιος μπορεί να εγγυηθεί ότι είναι μοναδικοί, αν δεν υπάρχει μια κεντρική τράπεζα που δημιουργεί το χρήμα;

Επισκόπηση

Bitcoin

- Το Bitcoin είναι ένα online σύστημα πληρωμών που εφευρέθηκε από τον Satoshi Nakamoto.
- Το 2008 ο Nakamoto δημοσίευσε ένα άρθρο στο περιέγραφε το Bitcoin σε μία λίστα ηλεκτρονικού ταχυδρομείου.
- Το 2009 δημοσίευσε την πρώτη έκδοση του λογισμικού που υλοποιεί το σύστημα και έδωσε στην κυκλοφορία τα πρώτα νομίσματα του Bitcoin, τα οποία ονομάζονται bitcoin.

Γενικά

- Η ταυτότητα του Satoshi Nakamoto δεν είναι γνωστή.
- Η δημοτικότητα του bitcoin έκτοται αυξάνεται.
- Ένα bitcoin (1 BTC ή 1 XBT) χωρίζεται σε 100.000.000 satoshi.
- Επίσης χωρίζεται σε 1000 millibitcoin (mBTC) και σε 1.000.000 microbitcoin (μBTC).

Γενικά

- Οι συμμετέχοντες στο Bitcoin αποτελούν ένα *ομότιμο δίκτυο* (peer to peer network), δηλαδή επικοινωνούν μεταξύ τους χωρίς μεσάζοντες.
- Το Bitcoin βασίζεται σε δοσοληψίες.
- Όλες οι δοσοληψίες επιβεβαιώνονται από συμμετέχουν στο δίκτυο του Bitcoin.
- Οι επιβεβαιωμένες δοσοληψίες καταγράφονται σε ένα συνολικό τεφτέρι δοσοληψιών (transaction ledger).
- Οι συμμετέχοντες αμοίβονται για την επιβεβαίωση των δοσοληψιών με νέα bitcoins που δημιουργούνται.

Επισκόπηση

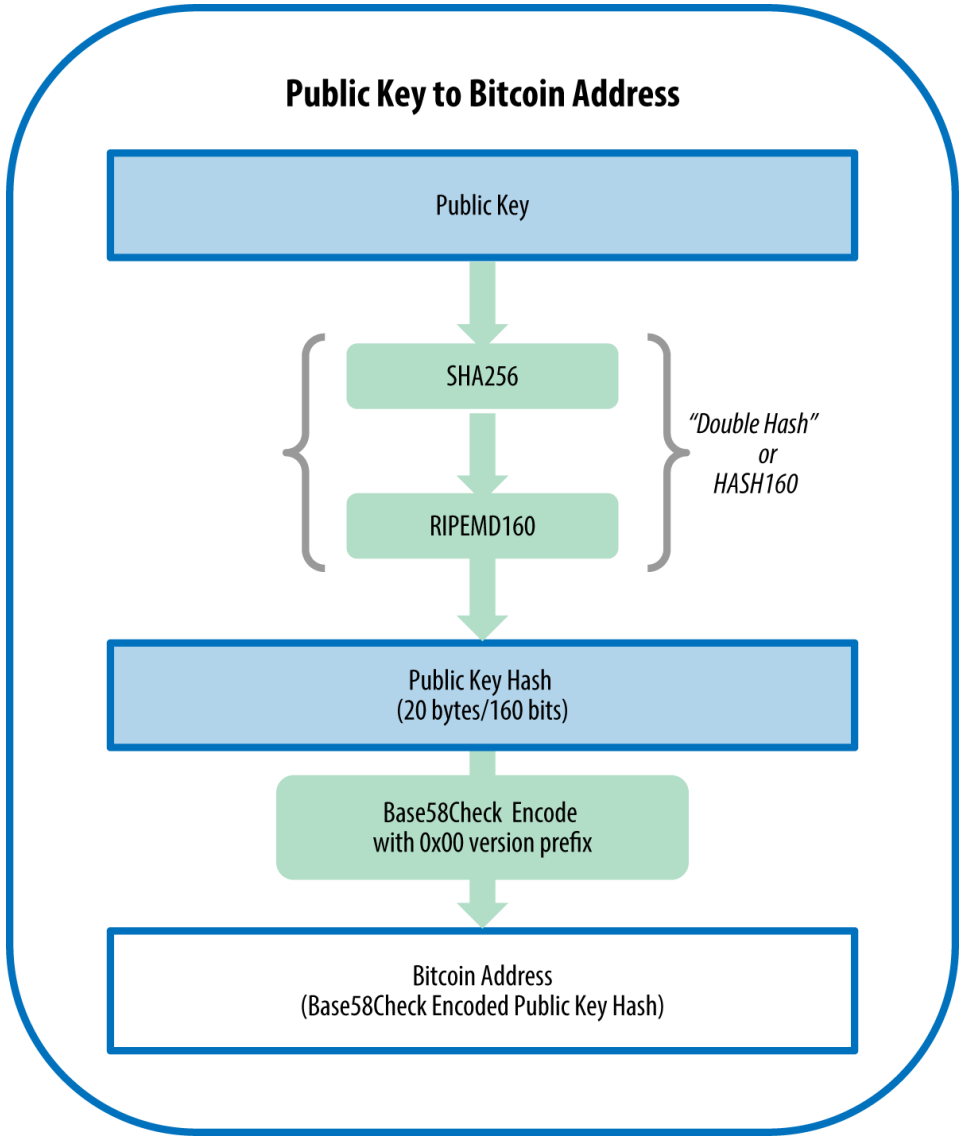
Γενικά

- Οι συμμετέχοντες στο Bitcoin επικοινωνούν μεταξύ τους μέσω *διευθύνσεων* (addresses).
- Οι διευθύνσεις στο Bitcoin είναι στην ουσία το αποτέλεσμα μιας *συνάρτησης κατακερματισμού* (hash function) στο *δημόσιο κλειδί* (public key) του χρήστη.

Ιδιωτικά και Δημόσια Κλειδιά

- Το ιδιωτικό κλειδί ενός χρήστη στο Bitcoin είναι ένας τυχαίος αριθμός που παραμένει κρυφός. Ο αριθμός αυτός μπορεί να είναι από το 1 μέχρι και $1158 \times 10^{77} - 1$, λίγο μικρότερος από το 2^{256}.
- Αν k είναι το ιδιωτικό κλειδί, το δημόσιο κλειδί είναι το αποτέλεσμα της πράξης $k \times G$.
- Προσοχή, αυτή η πράξη δεν είναι ο συνηθισμένος μας πολλαπλασιασμός.
- Η πράξη αυτή σημαίνει «προσθέτω k φορές το G», όπου το G είναι ένας *γεννήτορας* (generator) μιας *ελλειπτικής καμπύλης* (elliptic curve).

Υπολογισμός Διεύθυνσης

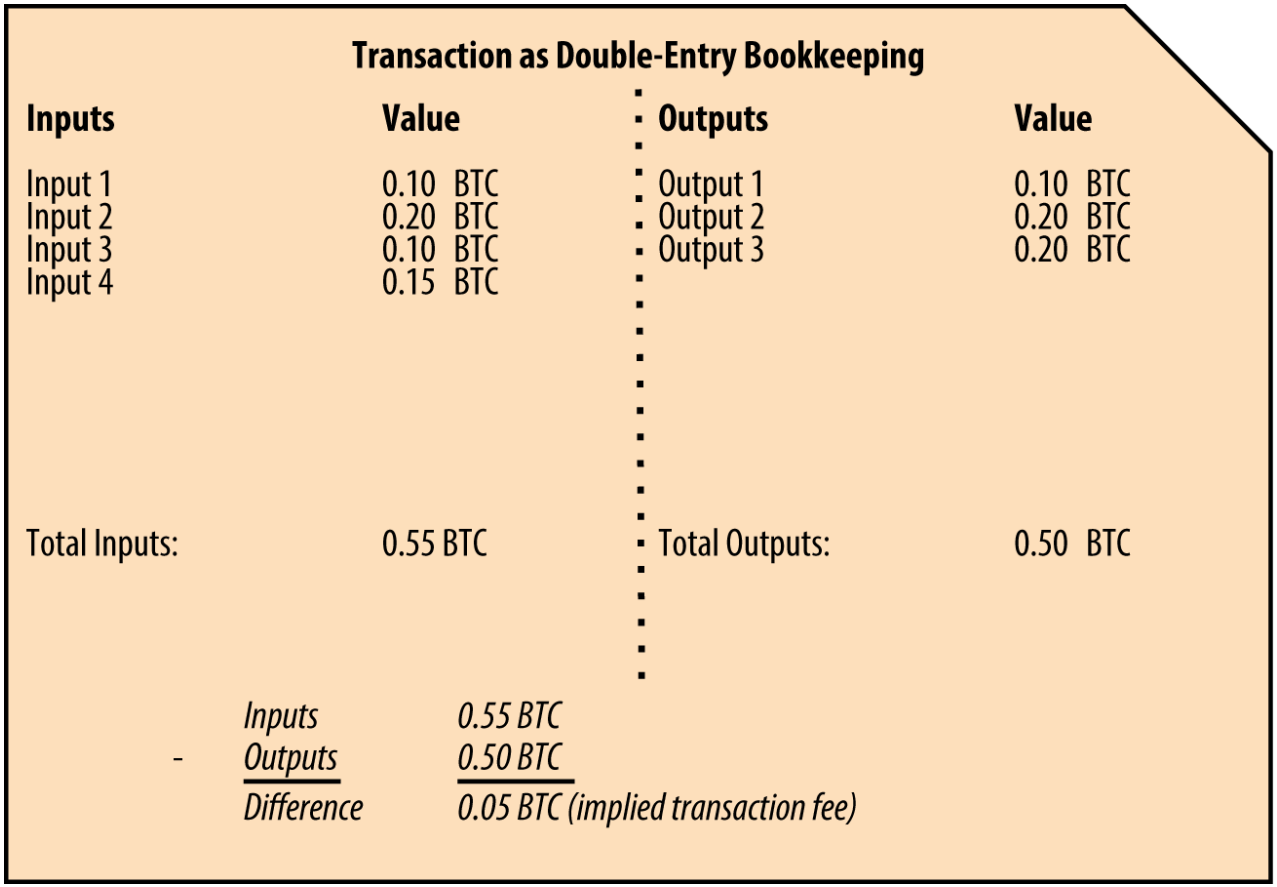


Επισκόπηση

Δοσοληψίες

- Μία *δοσοληψία* (transaction) είναι μια εντολή να μεταφερθεί ένα ποσό bitcoins από τον κάτοχό τους σε κάποιον άλλο.
- Ο νέος κάτοχος μπορεί στη συνέχεια να τα χρησιμοποιήσει σε μία νέα δοσοληψία, μεταφέροντάς τα σε έναν τρίτο, κ.ο.κ.
- Οι δοσοληψίες δημιουργούν έτσι μια αλυσίδα.
- Κάθε δοσοληψία έχει *εισόδους* (inputs) και *εξόδους* (outputs). Οι είσοδοι είναι εισροές, οι έξοδοι είναι εκροές.

Δοσοληψίες ως Διπλογραφική Λογιστική

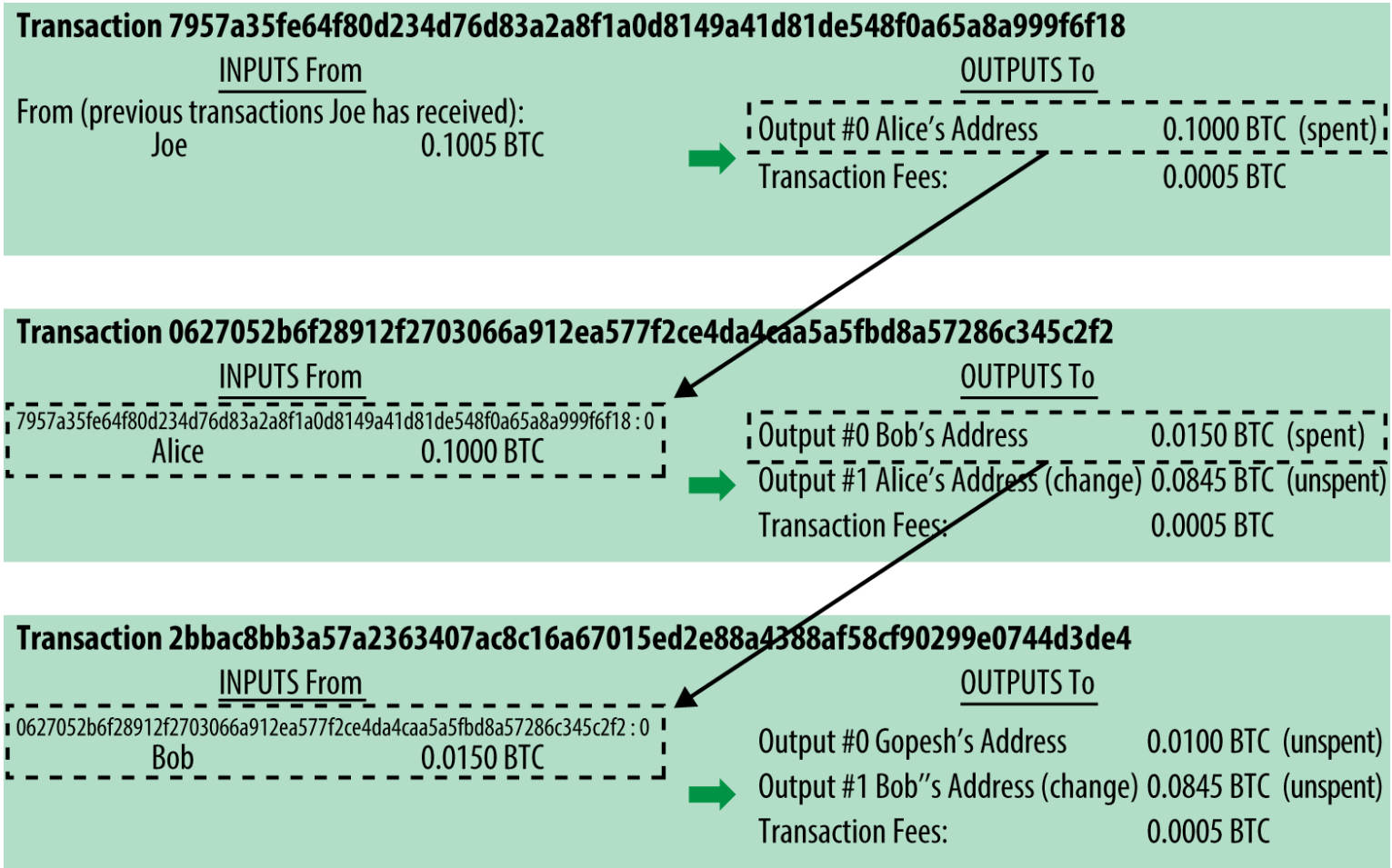


Transaction as Double-Entry Bookkeeping

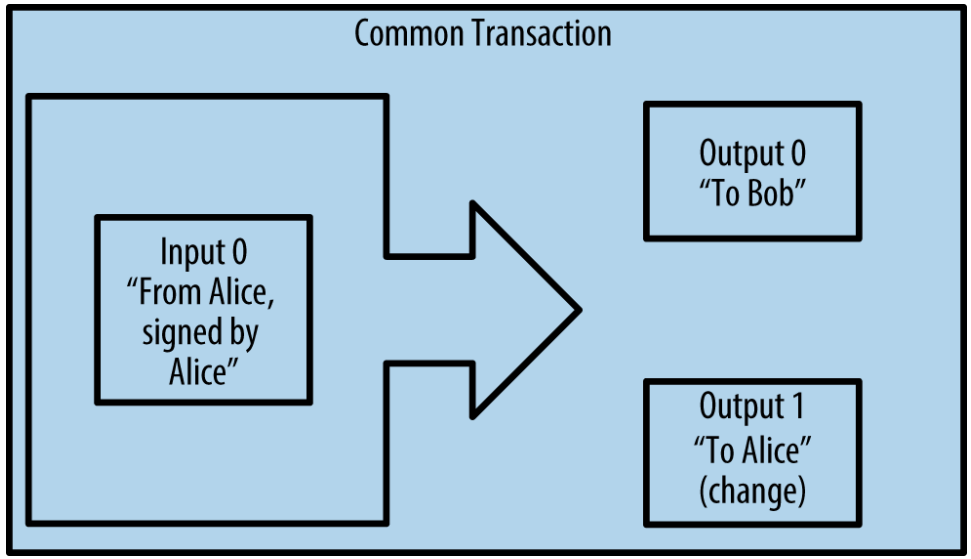
Inputs	Value	Outputs	Value
Input 1	0.10 BTC	Output 1	0.10 BTC
Input 2	0.20 BTC	Output 2	0.20 BTC
Input 3	0.10 BTC	Output 3	0.20 BTC
Input 4	0.15 BTC		
Total Inputs:	0.55 BTC	Total Outputs:	0.50 BTC

	Inputs	*0.55 BTC*
-	*Outputs*	*0.50 BTC*
	Difference	*0.05 BTC (implied transaction fee)*

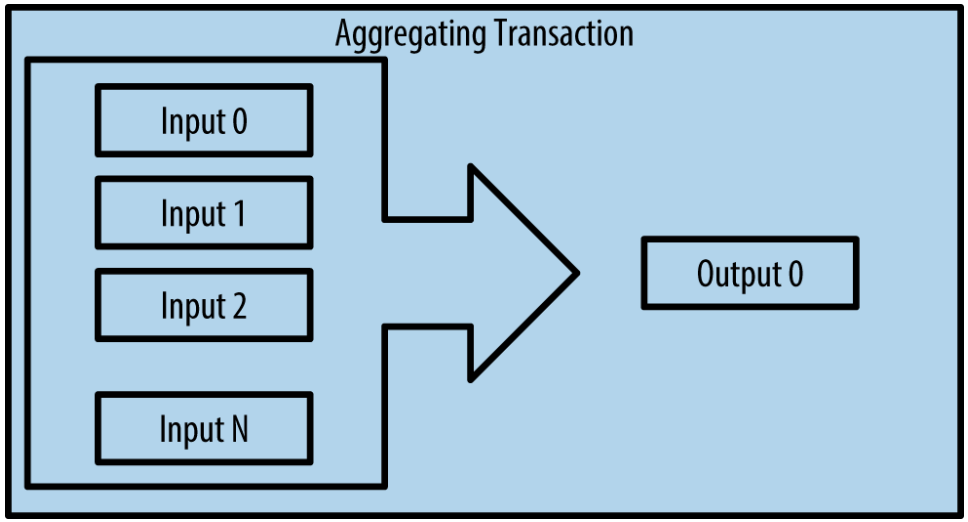
Αλυσίδα Δοσοληψιών



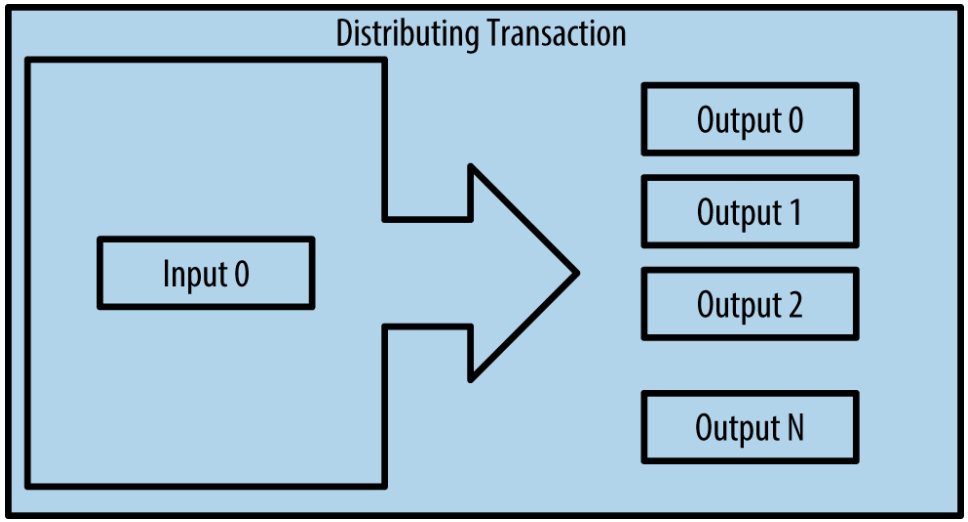
Συνήθης Δοσοληψία



Συγκεντρωτική Δοσοληψία



Διαμεριστική Δοσοληψία



Παράδειγμα Δοσοληψίας

Transaction View information about a bitcoin transaction

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK (0.1 BTC - Output)

1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA - (Unspent) 0.015 BTC

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK - (Unspent) 0.0845 BTC

97 Confirmations | 0.0995 BTC

Summary	
Size	258 (bytes)
Received Time	2013-12-27 23:03:05
Included In Blocks	277316 (2013-12-27 23:11:54 +9 minutes)

Inputs and Outputs	
Total Input	0.1 BTC
Total Output	0.0995 BTC
Fees	0.0005 BTC
Estimated BTC Transacted	0.015 BTC

Παράδειγμα Δοσοληψίας με Μία Έξοδο


```
{"hash":"7c4025...",
 "ver":1,
 "vin_sz":1,
 "vout_sz":1,
 "lock_time":0,
 "size":224,
 "in":[
   {"out":
     {"hash":"2007ae...",
      "n":0},
    "scriptSig":"304502... 042b2d..."}],
 "out":[
   {"value":"0.31900000",
    "scriptPubKey":"OP_DUP OP_HASH160 a7db6f OP_EQUALVERIFY
     ↪  OP_CHECKSIG"}]}
```

Παράδειγμα Δοσοληψίας με Πολλές Εισόδους και Εξόδους


```
{"hash":"993830...",
 "ver":1,
 "vin_sz":3,
 "vout_sz":2,
 "lock_time":0,
 "size":552,
 "in":[
   {"out": {
      "hash":"3beabc...",
      "n":0},
    "scriptSig":"304402... 04c7d2..."},
  {"out":{
      "hash":"fdae9b...",
      "n":0},
    "scriptSig":"304502... 026e15..."},
  {"out":{
      "hash":"20c86b...",
      "n":1},
    "scriptSig":"304402... 038a52..."}],
  "out":[
    {"value":"0.01068000",
      "scriptPubKey":"OP_DUP OP_HASH160 e8c306... OP_EQUALVERIFY OP_CHECKSIG"},
    {"value":"4.00000000",
      "scriptPubKey":"OP_DUP OP_HASH160 d644e3... OP_EQUALVERIFY OP_CHECKSIG"}]}
```

Επισκόπηση

Γενικά

Για κάθε δοσοληψία θα πρέπει να μπορεί να αποδειχτεί ότι:

1. Ο ιδιοκτήτης της συγκεκριμένης διεύθυνσης Bitcoin έχει λάβει το απαιτούμενο ποσό (από προηγούμενες δοσοληψίες).
2. Η δοσοληψία δημιουργείται πραγματικά από τον ιδιοκτήτη της συγκεκριμένης διεύθυνσης Bitcoin (και όχι από κάποιον που τον υποδύεται).

Η Γλώσσα Script

- Οι κανόνες που πρέπει να ισχύουν προκειμένου να πραγματοποιηθεί μια δοσοληψία περιγράφονται με μία γλώσσα, η οποία ονομάζεται Script.
- Η γλώσσα αυτή είναι μια απλή γλώσσα προγραμματισμού στοίβας (stack-based programming language).
- Η γλώσσα δεν περιέχει βρόχους ή περίπλοκους μηχανισμούς ελέγχους. Έτσι δεν μπορεί να χρησιμοποιηθεί για οποιονδήποτε υπολογισμό (δεν είναι Turing Complete).

Κλείδωμα Δοσοληψίας

- Έστω ότι έχουμε μια δοσοληψία TX1, με την οποία η Alice έχει στείλει ένα ποσό στον Bob.
- Η έξοδος της δοσοληψίας θα περιέχει κάτι της μορφής: έξοδος περιγράφεται όπως παρακάτω:

```
{
 "out":[{
    "value": "0.31900000",
    "scriptPubKey": "OP_DUP OP_HASH160 <Hash(PK_Bob)>
    ↪  OP_EQUALVERIFY OP_CHECKSIG"
 }]
}
```

- Αυτή η έξοδος σημαίνει ότι μπορεί να εξαργυρωθεί από τον χρήστη που έχει το δημόσιο κλειδί PK_Bob.

Ξεκλείδωμα Δοσοληψίας

- Ο Bob για να στείλει χρήματα στον Charlie θα δημιουργήσει μια δοσοληψία όπου στην είσοδο θα υπάρχει κάτι της μορφής:

```
{
 "in":[
   {
     "out": {
       "hash": "3beabc...",
       "n": 0
     },
     "scriptSig": "<sig> <PK_Bob>"},
   ]
}
```

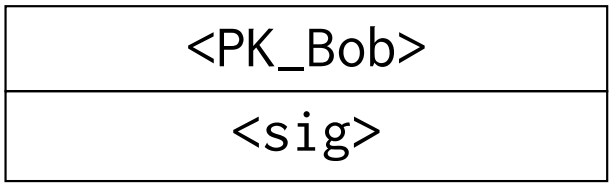
- Το <sig> είναι μια υπογραφή της δοσοληψίας και το <PK_Bob> είναι το δημόσιο κλειδί του Bob.

Επιβεβαίωση Δοσοληψίας (1)

```
<sig>
<PK_Bob>
OP_DUP
OP_HASH160
<Hash(PK_Bob)>
OP_EQUALVERIFY
OP_CHECKSIG
```

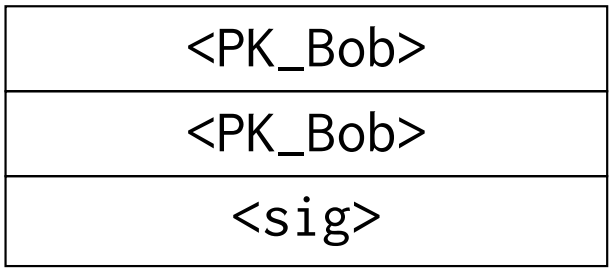
Ξεκλείδωμα Δοσοληψίας (2)

```
<PK_Bob>
OP_DUP
OP_HASH160
<Hash(PK_Bob)>
OP_EQUALVERIFY
OP_CHECKSIG
```



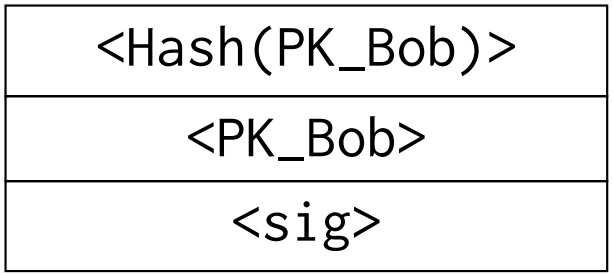
Ξεκλείδωμα Δοσοληψίας (3)

```
OP_DUP
OP_HASH160
<Hash(PK_Bob)>
OP_EQUALVERIFY
OP_CHECKSIG
```



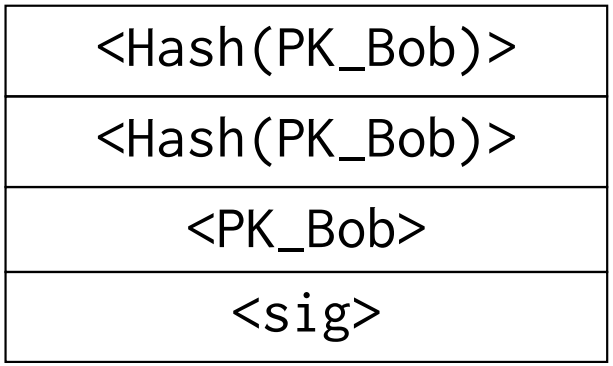
Ξεκλείδωμα Δοσοληψίας (4)

```
OP_HASH160
<Hash(PK_Bob)>
OP_EQUALVERIFY
OP_CHECKSIG
```



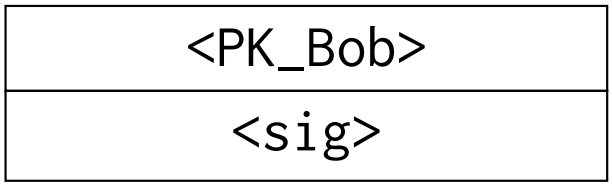
Ξεκλείδωμα Δοσοληψίας (5)

```
<Hash(PK_Bob)>
OP_EQUALVERIFY
OP_CHECKSIG
```



Ξεκλείδωμα Δοσοληψίας (6)

OP_EQUALVERIFY
OP_CHECKSIG



Ξεκλείδωμα Δοσοληψίας (7)

OP_CHECKSIG

TRUE

Επισκόπηση

Επικύρωση Δοσοληψίας

- Έστω ότι η Alice δημιουργεί μια δοσοληψία πληρωμής στον Bob.
- Πώς μπορεί ο Bob να εξασφαλίσει ότι η δοσοληψία είναι ορθή, δηλαδή ότι υπάρχουν τα απαραίτητα inputs και δεν έχουν ήδη ξοδευτεί ήδη (doublespend);
- Ο Bob θα ζητήσει από τους υπόλοιπους συμμετέχοντες στο δίκτυο του bitcoin να επικυρώσουν ότι πράγματι η δοσοληψία είναι σωστή.

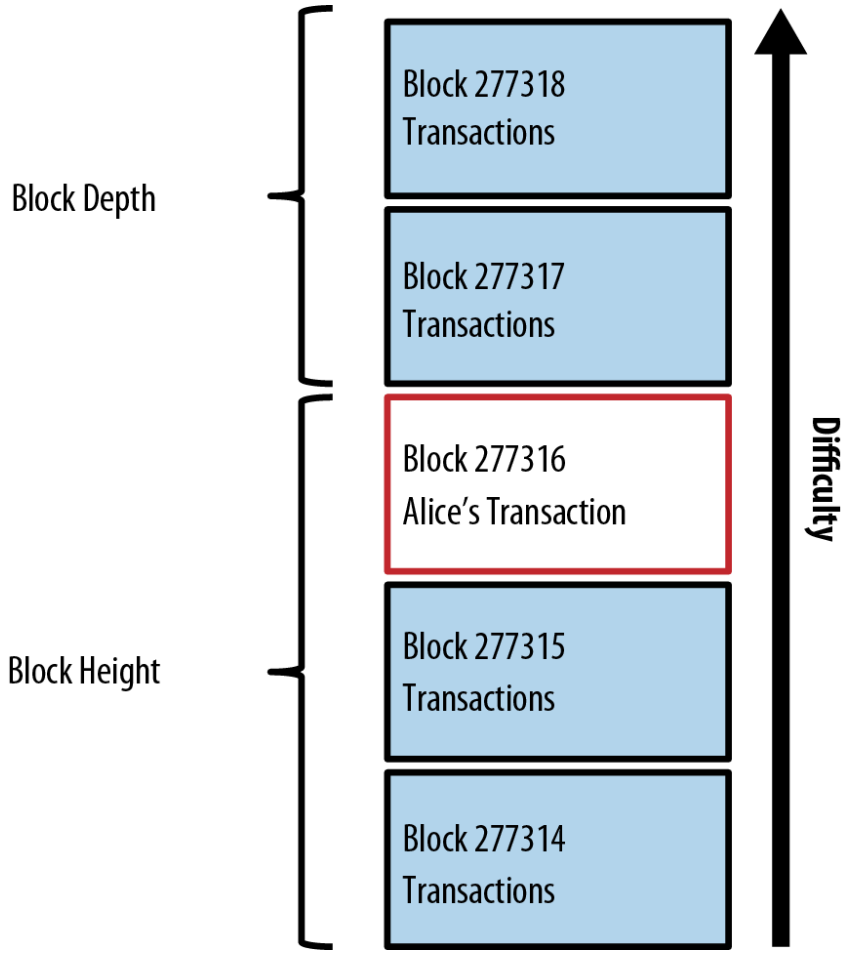
Εκπομπή Δοσοληψίας

- Μια νέα δοσοληψία εκπέμπεται (broadcast) στο υπόλοιπο δίκτυο bitcoin.
- Η δοσοληψία θα θεωρηθεί επικυρωμένη όταν την επικυρώσει η πλειοψηφία των συμμετεχόντων στο δίκτυο.
- Έτσι αν η Alice προσπαθήσει να διπλοξοδέψει στέλνοντας και στον Bob και στον Charlie μια δοσοληψία για το ίδιο bitcoin, μόνο η μία από τις δύο δοσοληψίες θα μπορέσει να επικυρωθεί.

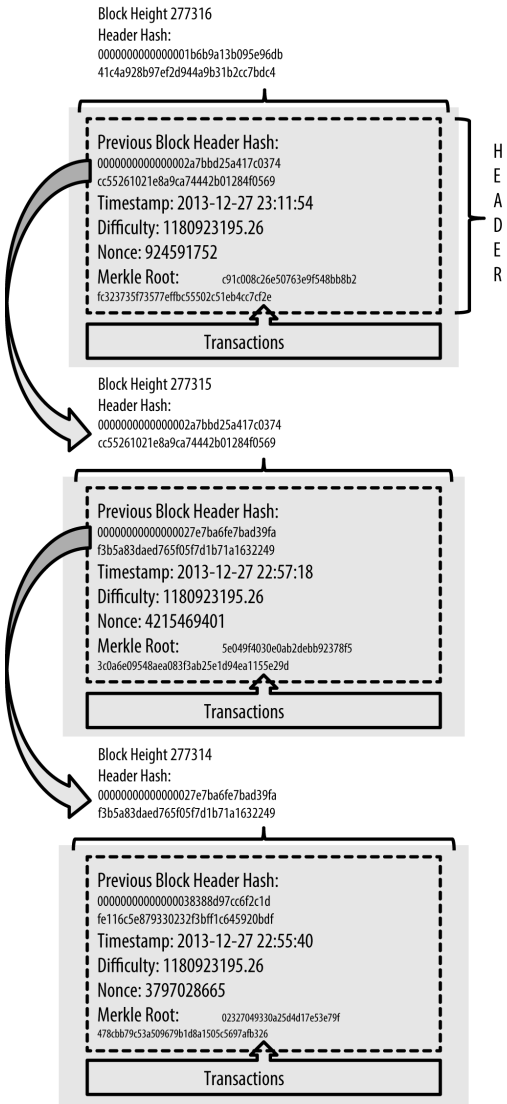
Blockchain

- Όλες οι δοσοληψίες που γίνονται στο bitcoin καταγράφονται σε μία δομή που ονομάζεται blockchain (αλυσίδα blocks).
- Κάθε block έχει μέγεθος μέχρι 1 MByte.
- Κάθε block περιέχει έναν αριθμό δοσοληψιών (π.χ. 2000).
- Κάθε block επικυρώνει το σύνολο των δοσοληψιών που περιέχει.
- Κάθε block δείχνει στο προηγούμενο επικυρωμένο block στην ιστορία του bitcoin.
- Η αλυσίδα των blocks τελειώνει στο πρώτο block που δημιουργήθηκε ποτέ, το 2009, από το δημιουργό του bitcoin Satoshi Nakamoto, το οποίο ονομάζεται genesis block και αφορά τη δημιουργία (εκ του μηδενός) των πρώτων 50 BTC (bitcoins).

Blockchain


Block Depth
Block Height
Block 277318
Transactions
Block 277317
Transactions
Block 277316
Alice's Transaction
Block 277315
Transactions
Block 277314
Transactions
Difficulty

Blockchain


Block Height 277316
Header Hash:
0000000000000001b6b9a13b095e96db
41c4a928b97ef2d944a9b31b2cc7bdc4
Previous Block Header Hash:
0000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569
Timestamp: 2013-12-27 23:11:54
Difficulty: 1180923195.26
Nonce: 924591752
Merkle Root: c91c008c26e50763e9f548bb8b2
fc323735f73577effbc55502c51eb4cc7cf2e
Transactions
HEADER
Block Height 277315
Header Hash:
0000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569
Previous Block Header Hash:
0000000000000027e7ba6fe7bad39fa
f3b5a83daed765f05f7d1b71a1632249
Timestamp: 2013-12-27 22:57:18
Difficulty: 1180923195.26
Nonce: 4215469401
Merkle Root: 5e049f4030e0ab2debb92378f5
3c0a6e09548aea083f3ab25e1d94ea1155e29d
Transactions
Block Height 277314
Header Hash:
0000000000000027e7ba6fe7bad39fa
f3b5a83daed765f05f7d1b71a1632249
Previous Block Header Hash:
00000000000000038388d97cc6f2c1d
fe116c5e879330232f3bff1c645920bdf
Timestamp: 2013-12-27 22:55:40
Difficulty: 1180923195.26
Nonce: 3797028665
Merkle Root: 02327049330a25d4d17e53e79f
478cbb79c53a509679b1d8a1505c5697afb326
Transactions

Εξόρυξη Bitcoins

- Όταν επικυρώνεται ένα block ελέγχεται η ορθότητα όλων των δοσοληψιών που περιέχει.
- Ταυτόχρονα, προκειμένου να επικυρωθεί το block θα πρέπει να λυθεί και ένα δύσκολο υπολογιστικό πρόβλημα (hard computational problem).
- Μόνο όταν λυθεί το πρόβλημα δημοσιεύεται από τον λύτη το επικυρωμένο block.
- Το επικυρωμένο block περιέχει και μία ειδική δοσοληψία που είναι η αμοιβή του λύτη και αντιστοιχεί σε ένα συγκεκριμένο αριθμό bitcoins.
- Με κάθε επικύρωση block δημιουργούνται νέα bitcoins, γι' αυτό και η διαδικασία ονομάζεται *εξόρυξη* (mining).

Έσοδα από Bitcoins

- Όταν επικυρώνεται ένα block, ο επικυρωτής λαμβάνει ως αμοιβή το συγκεκριμένο αριθμό bitcoins που αναλογεί στο block.
- Επιπλέον, λαμβάνει ως αμοιβή τα έξοδα συναλλαγών (transaction fees) που ορίζονται σε κάθε συναλλαγή στο σύστημα.

Απόδειξη Έργου

- Το δύσκολο υπολογιστικό πρόβλημα που πρέπει να λυθεί για να επικυρωθεί ένα block ονομάζεται *απόδειξη έργου* (Proof of Work, PoW).
- Γιατί υπάρχει η απόδειξη έργου;

Απόδειξη Έργου

- Έστω ότι η Alice δημιουργεί ψευδείς δοσοληψίες.
- Έστω επίσης ότι έχει πολλούς συνεργούς, οι οποίοι θα μπορούσαν να επιβεβαιώσουν την ορθότητά τους, ξεγελώντας τους υπόλοιπους χρήστες του συστήματος.
- Θα πρέπει λοιπόν να υπάρχει τρόπος ώστε η επικύρωση να κοστίζει σε υπολογιστικούς πόρους, ώστε να μην μπορεί να συνομωτήσει η πλειοψηφία των χρηστών του bitcoin για να ξεγελάσουν τους υπόλοιπους, γιατί αυτό θα έχει τεράστιο υπολογιστικό κόστος.

Απόδειξη Έργου

- Από την άλλη μεριά θέλουμε να ανταμοίψουμε τους χρήστες για τους πόρους που θα ξοδεύουν για την απόδειξη έργου.
- Αυτό το κάνουμε με την αμοιβή που δίνεται για την επικύρωση κάθε block.
- Έτσι ξέρουμε ότι θα υπάρχουν πολλοί ανεξάρτητοι χρήστες που θα προσπαθούν να επιβεβαιώσουν ένα block. Αφού μόνο ο πρώτος κερδίζει την αμοιβή, δεν μπορεί να υπάρχει συνομωσία.

Τι Είναι η Απόδειξη Έργου;

- Κάθε block έχει μια επικεφαλίδα που το συνοψίζει.
- Υπάρχει μια συνάρτηση κρυπτογραφικού κατακερματισμού (cryptographic hash), η SHA-256, οποία παίρνει μια είσοδο και παράγει στην έξοδο 256 bits. Από την είσοδο δεν μπορούμε να προβλέψουμε την έξοδο.
- Στην επικεφαλίδα υπάρχει ένα πεδίο, που ονομάζεται nonce, το οποίο παίρνει αριθμητικές τιμές.
- Η απόδειξη έργου είναι: βρες το κατάλληλο nonce ώστε να έχουμε:

$$SHA\text{-}256(H) < T$$

όπου H η επικεφαλίδα (με το nonce) και T μια τιμή που ονομάζεται *στόχος* (target).

Παράδειγμα Απόδειξης Έργου

- Έστω ότι θέλουμε η επικεφαλίδα να είναι η:
  “I am Satoshi NakamotoN”
  όπου το N στο τέλος είναι το nonce.
- Θέλουμε να βρούμε το nonce ώστε το $SHA\text{-}256(H)$ να ξεκινάει με τέσσερα μηδενικά bits, δηλαδή να είναι μικρότερο από το:

$$\underbrace{0001\overbrace{00\ldots0}^{252}}_{256}$$

- Αυτό είναι το ίδιο με το $SHA\text{-}256(H)$ να ξεκινά με ένα μηδενικό δεκαεξαδικό ψηφίο.

Παράδειγμα Απόδειξης Έργου

```
I am Satoshi Nakamoto0   =>  a80a81401765c8eddee25df36728d732acb6d135bcdee6c2f87a3784279cfaed
I am Satoshi Nakamoto1   =>  f7bc9a6304a4647bb41241a677b5345fe3cd30db882c8281cf24fbb7645b6240
I am Satoshi Nakamoto2   =>  ea758a8134b115298a1583ffb80ae62939a2d086273ef5a7b14fbfe7fb8a799e
I am Satoshi Nakamoto3   =>  bfa9779618ff072c903d773de30c99bd6e2fd70bb8f2cbb929400e0976a5c6f4
I am Satoshi Nakamoto4   =>  bce8564de9a83c18c31944a66bde992ff1a77513f888e91c185bd08ab9c831d5
I am Satoshi Nakamoto5   =>  eb362c3cf3479be0a97a20163589038e4dbead49f915e96e8f983f99efa3ef0a
I am Satoshi Nakamoto6   =>  4a2fd48e3be420d0d28e202360cfbaba410beddeebb8ec07a669cd8928a8ba0e
I am Satoshi Nakamoto7   =>  790b5a1349a5f2b909bf74d0d166b17a333c7fd80c0f0eeabf29c4564ada8351
I am Satoshi Nakamoto8   =>  702c45e5b15aa54b625d68dd947f1597b1fa571d00ac6c3dedfa499f425e7369
I am Satoshi Nakamoto9   =>  7007cf7dd40f5e933cd89fff5b791ff0614d9c6017fbe831d63d392583564f74
I am Satoshi Nakamoto10  =>  c2f38c81992f4614206a21537bd634af717896430ff1de6fc1ee44a949737705
I am Satoshi Nakamoto11  =>  7045da6ed8a914690f087690e1e8d662cf9e56f76b445d9dc99c68354c83c102
I am Satoshi Nakamoto12  =>  60f01db30c1a0d4cbce2b4b22e88b9b93f58f10555a8f0f4f5da97c3926981c0
I am Satoshi Nakamoto13  =>  0ebc56d59a34f5082aaef3d66b37a661696c2b618e62432727216ba9531041a5
```

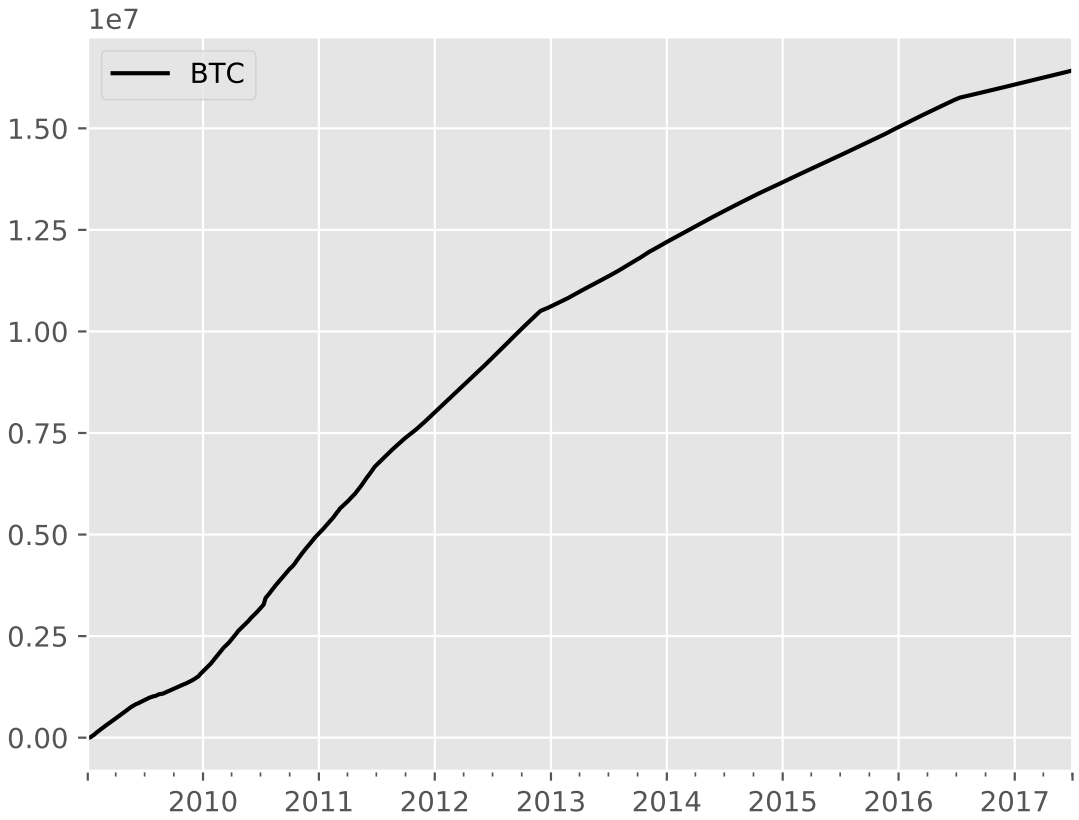
Παράδειγμα Υλοποίησης

```
import hashlib
import sys

num_bits = int(sys.argv[1])

target = 2 ** (256 - num_bits)

found = False

nonce = 0

while not found:
    to_check = "I am Satoshi Nakamoto" + str(nonce)
    result = hashlib.sha256(to_check.encode('utf-8')).hexdigest()
    nonce += 1
    if int(result, 16) < target:
        print('Nonce found:', nonce)
        print(result)
        found = True
```

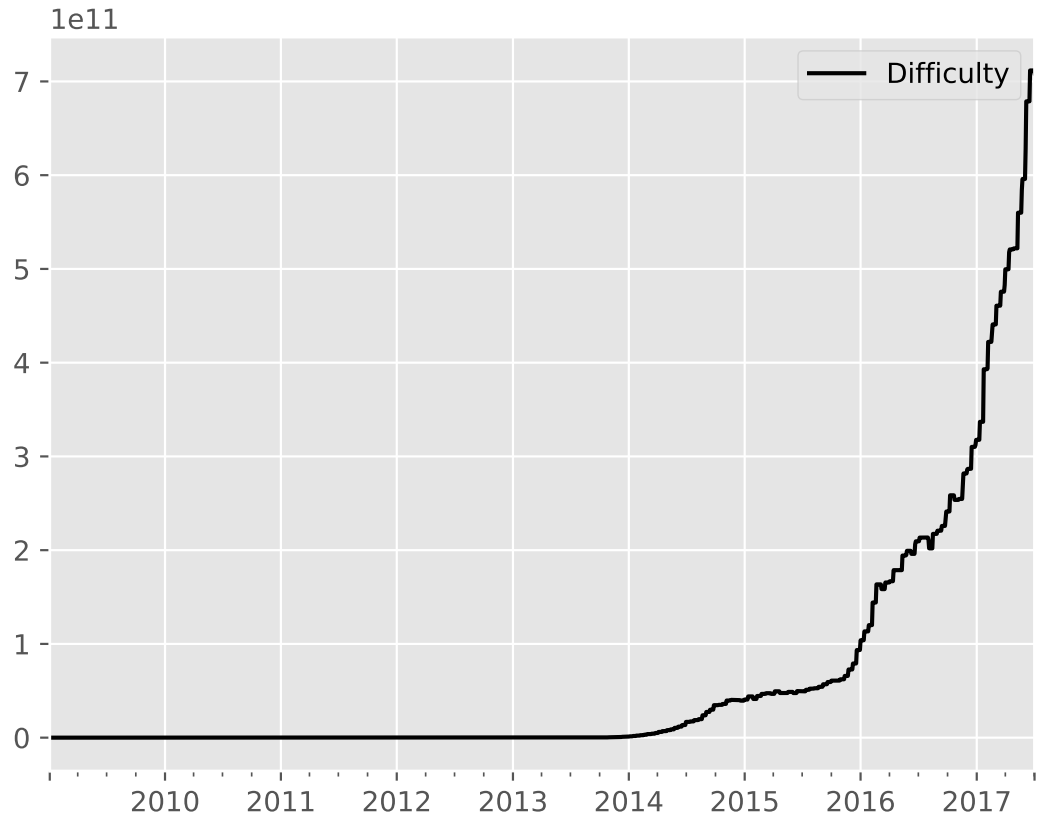
Προσαρμογή Δυσκολίας

- Ο στόχος προσαρμόζεται ώστε κάθε φορά η επίλυση του προβλήματος να διαρκεί 10 περίπου λεπτά.
- Αυτό επιτυγχάνεται απλώς με την αύξηση του αριθμού των bits που θέλουμε να είναι ίσα με μηδέν, γιατί έτσι αυξάνεται ο αριθμός των δοκιμών που πρέπει να κάνουμε για να τη βρούμε.
- Για n bits χρειαζόμαστε 2^n δοκιμές.

Αριθμός Bitcoin που Έχουν Εξορυχθεί



Δυσκολία Εξόρυξης Bitcoin



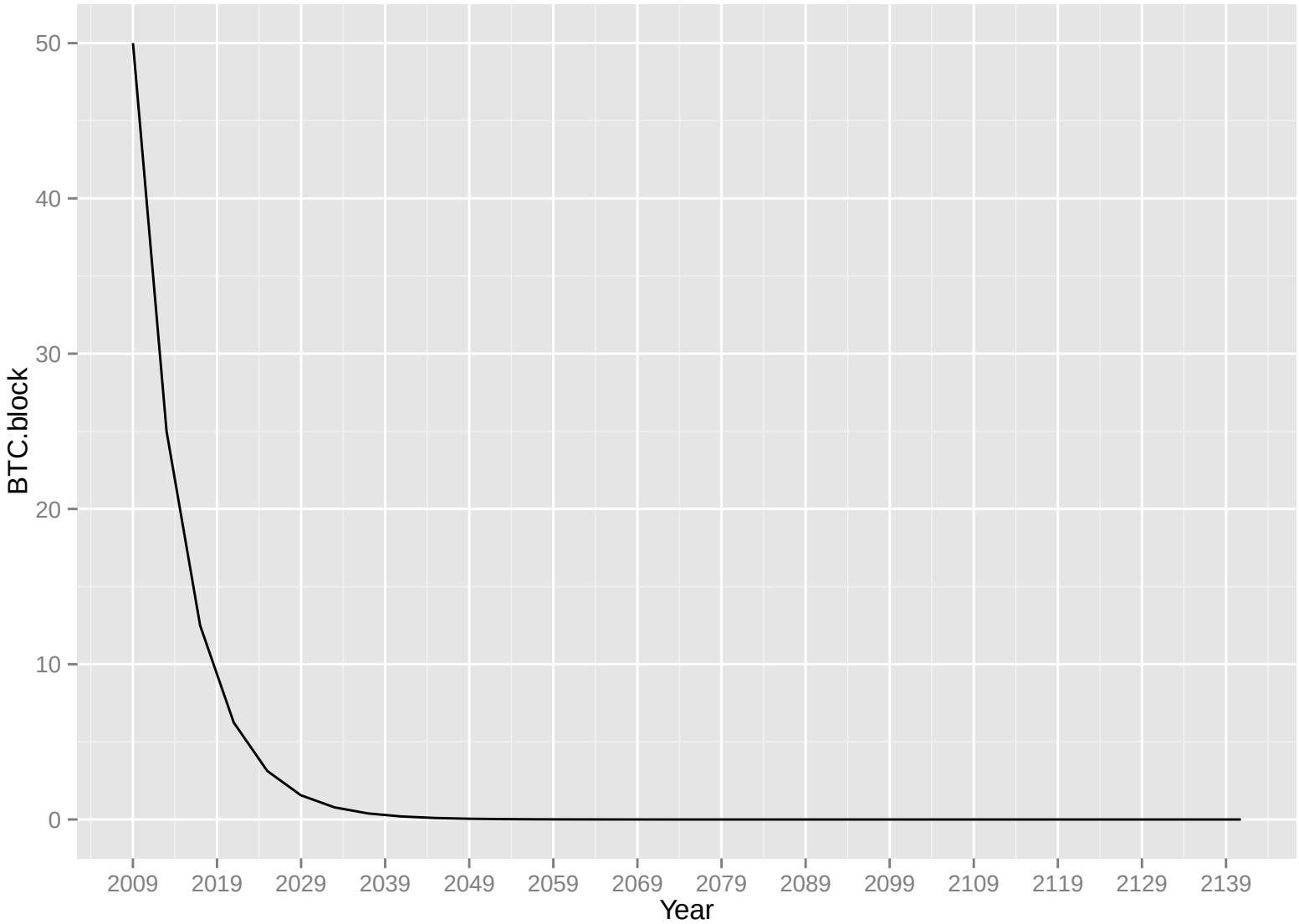
Προσαρμογή Αμοιβής

- Το ύψος της αμοιβής ανά block επίσης προσαρμόζεται.
- Ξεκίνησε με 50 BTC το 2009 και μειώνεται στο μισό κάθε 210.000 blocks.
- Αυτό αντιστοιχεί σε περίπου 4 χρόνια.
- Συνεπώς, περίπου το 2140 θα έχουν εξορυχθεί 2.099.999.997.690.000 satoshi ή περίπου 21 εκατομμύρια bitcoins.
- Αυτός είναι και ο μέγιστος αριθμός bitcoins που μπορούν να υπάρξουν.

Εξέλιξη Αμοιβής

- Η αμοιβή ξεκίνησε στα 50 BTC στις 3 Ιανουρίου 2009/
- Στις 28 Νοεμβρίου 2012 η αμοιβή μειώθηκε στα 25 BTC.
- Στις 9 Ιουλίου 2016 η αμοιβή μειώθηκε στα 12,5 BTC.

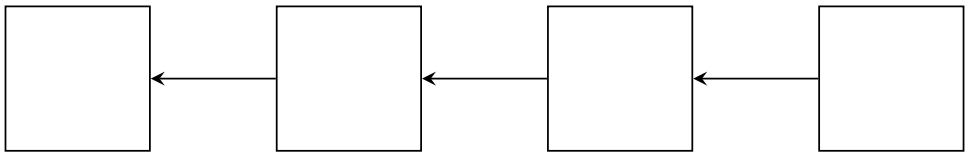
Αμοιβή ανά Block



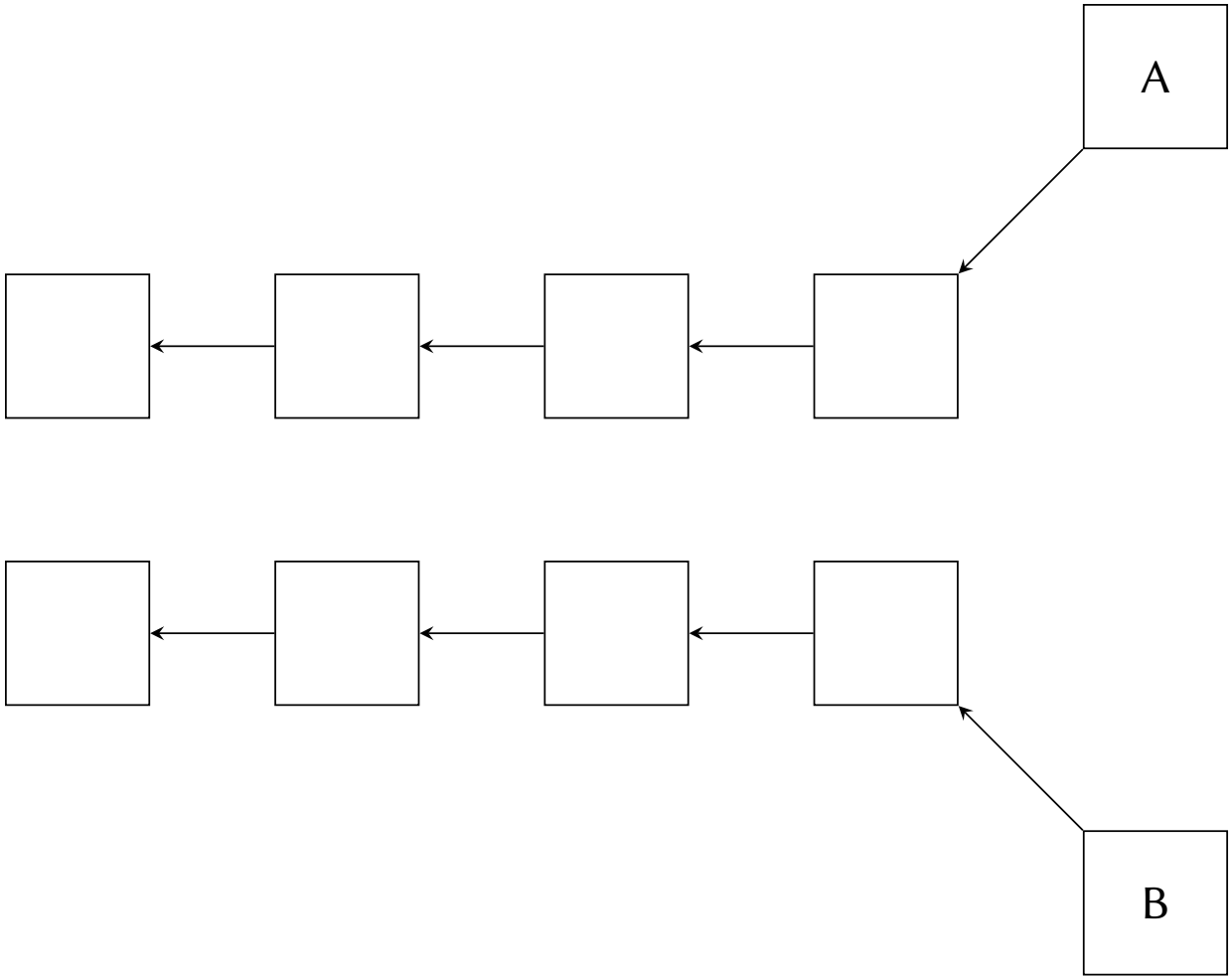
Διαχείριση Διαφορών Blockchains

- Οι δοσοληψίες προωθούνται στο δίκτυο από τον ένα κόμβο στον άλλο.
- Η συγκέντρωση των δοσοληψιών σε blocks, η επικύρωσή τους, και η ένταξη στο blockchain γίνεται ανταγωνιστικά μεταξύ των κόμβων.
- Μπορεί λοιπόν κάποια στιγμή δύο διαφορετικά blocks να επικυρωθούν από δύο ανεξάρτητους κόμβους σχεδόν ταυτόχρονα.
- Στην περίπτωση αυτή λέμε ότι εμφανίζεται μια *διακλάδωση* (fork).

Εμφάνιση Διακλάδωσης (1)



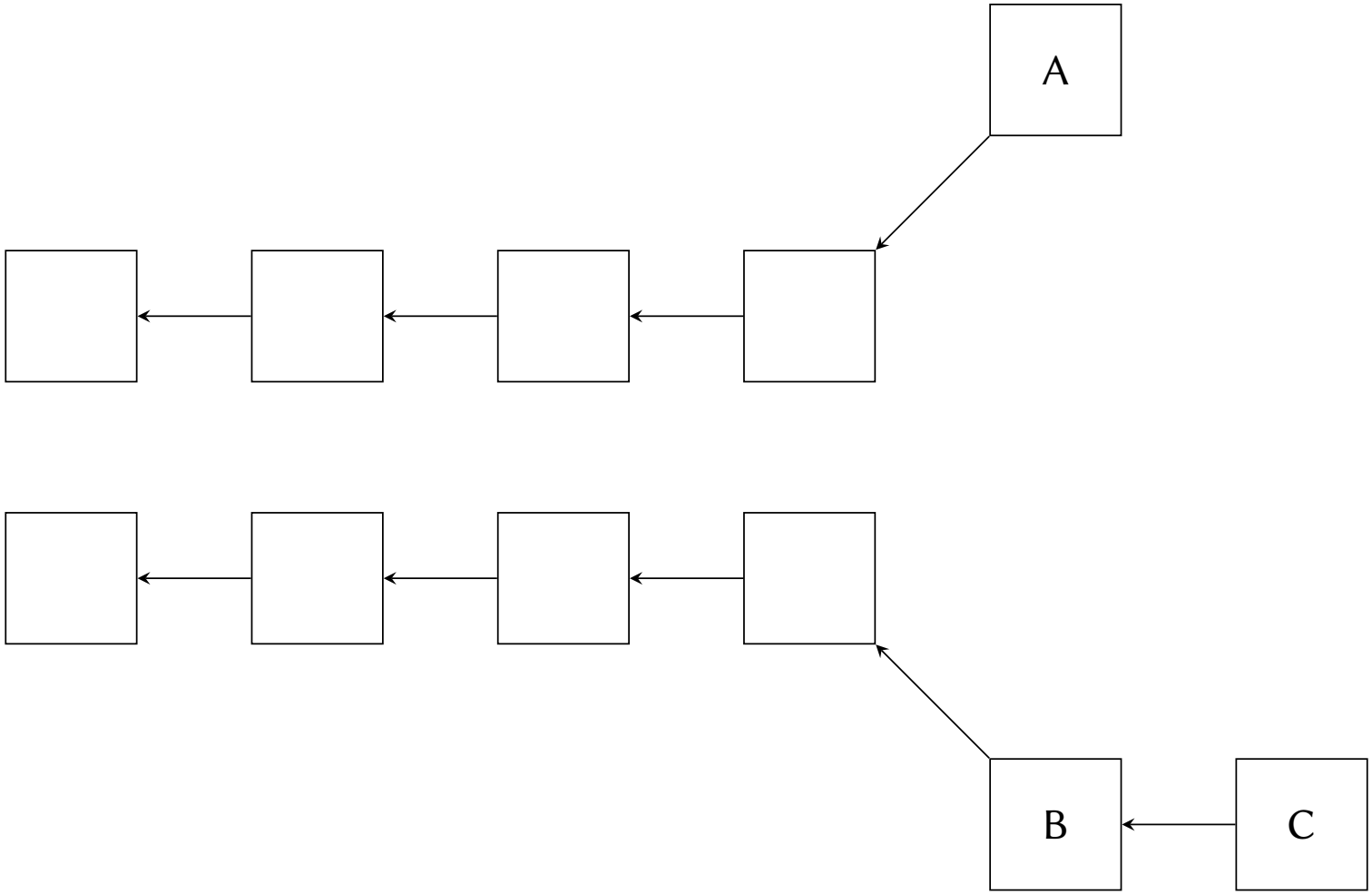
Εμφάνιση Διακλάδωσης



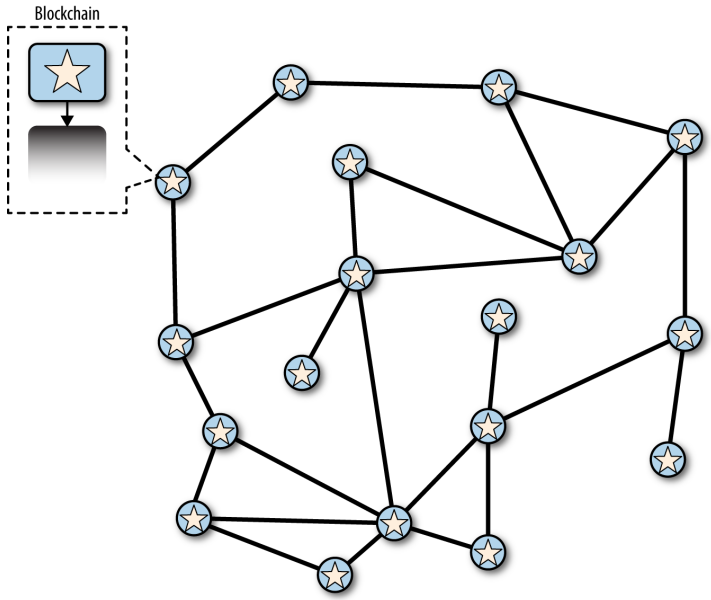
Επίλυση Διακλάδωσης (1)

- Αν προκύψει διακλάδωση, κάποιοι κόμβοι θα συνεχίσουν να εργάζονται στο ένα blockchain και κάποιοι κόμβοι θα συνεχίσουν να εργάζονται στο άλλο blockchain.
- Κάποια στιγμή όμως σε κάποιο από τα δύο blockchains θα ολοκληρωθεί πιο γρήγορα η επικύρωση του επόμενου blockchain.
- Οι κόμβοι πρέπει να ακολουθούν το μεγαλύτερο blockchain, άρα το μεγαλύτερο blockchain θα μεταδωθεί στο δίκτυο και θα επικρατήσει.
- Οι κόμβοι που εργάζονται στο άλλο blockchain θα υιοθετήσουν και αυτοί το μεγαλύτερο που θα έχει προκύψει.

Επίλυση Διακλάδωσης (2)

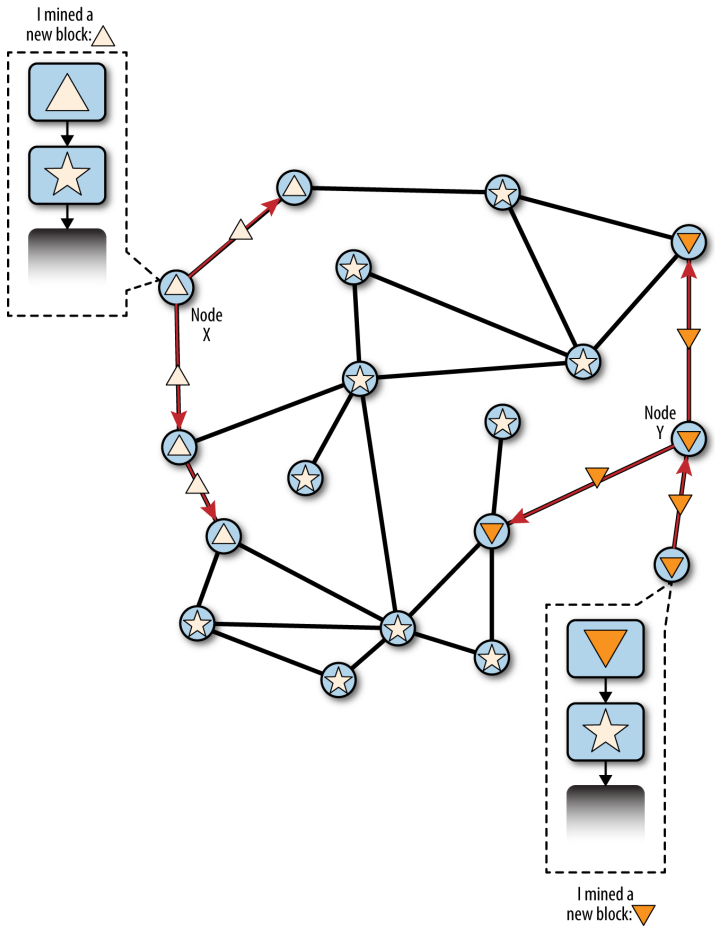


Παράδειγμα Διακλάδωσης (1)

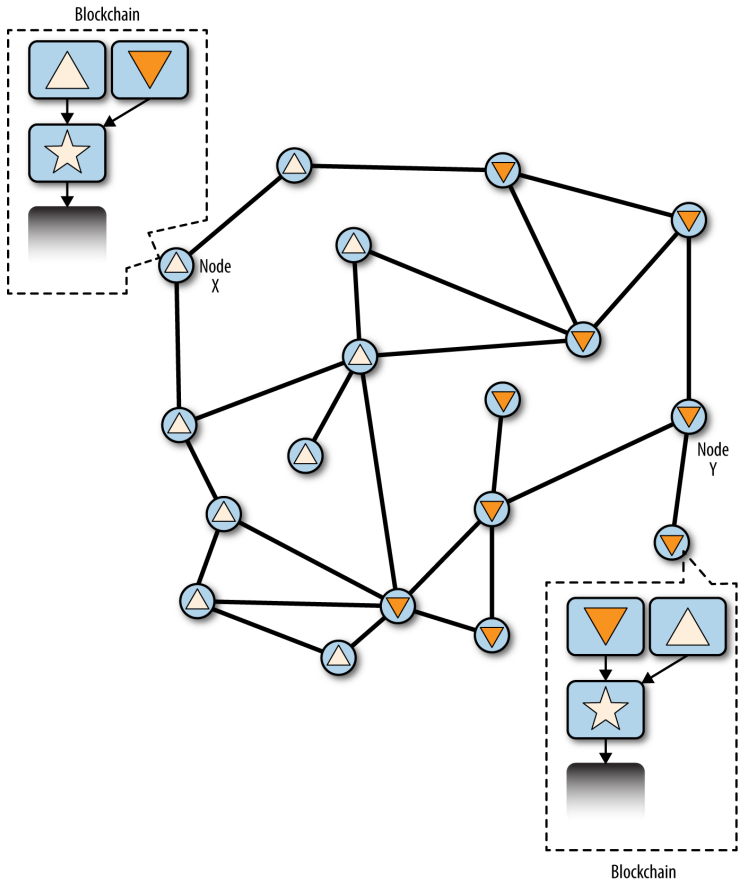


Mastering Bitcoin Open Edition, by Andreas M. Antonopoulos. Creative Commons Attribution-ShareAlike 4.0 International License.

Παράδειγμα Διακλάδωσης (2)

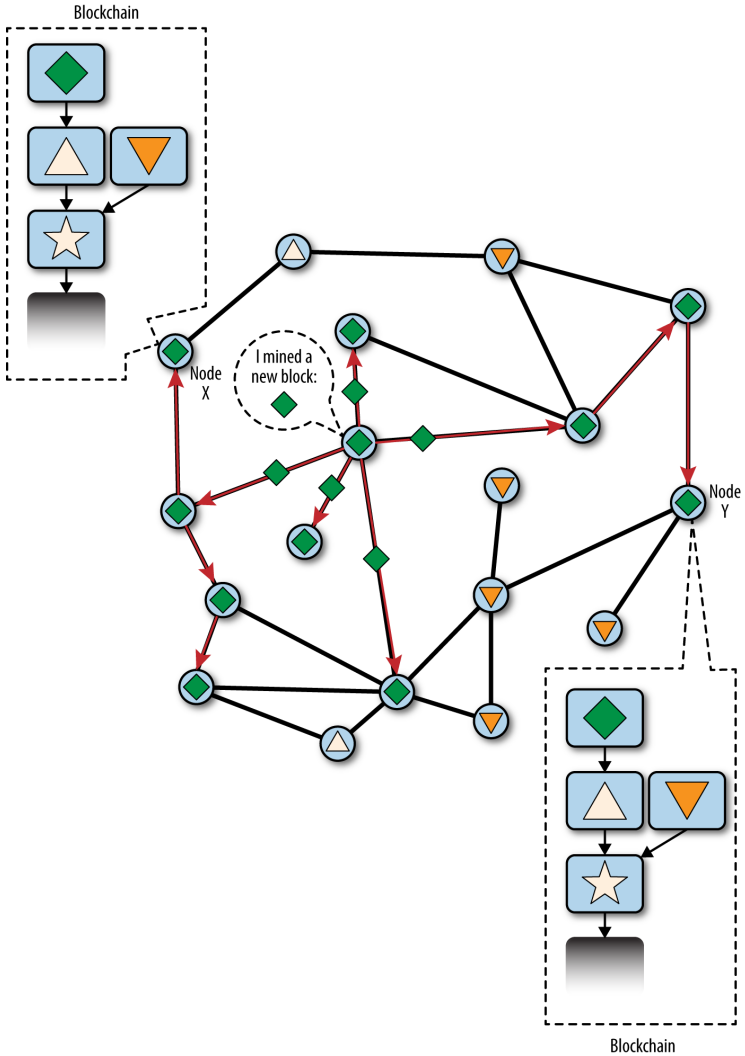


Παράδειγμα Διακλάδωσης (3)



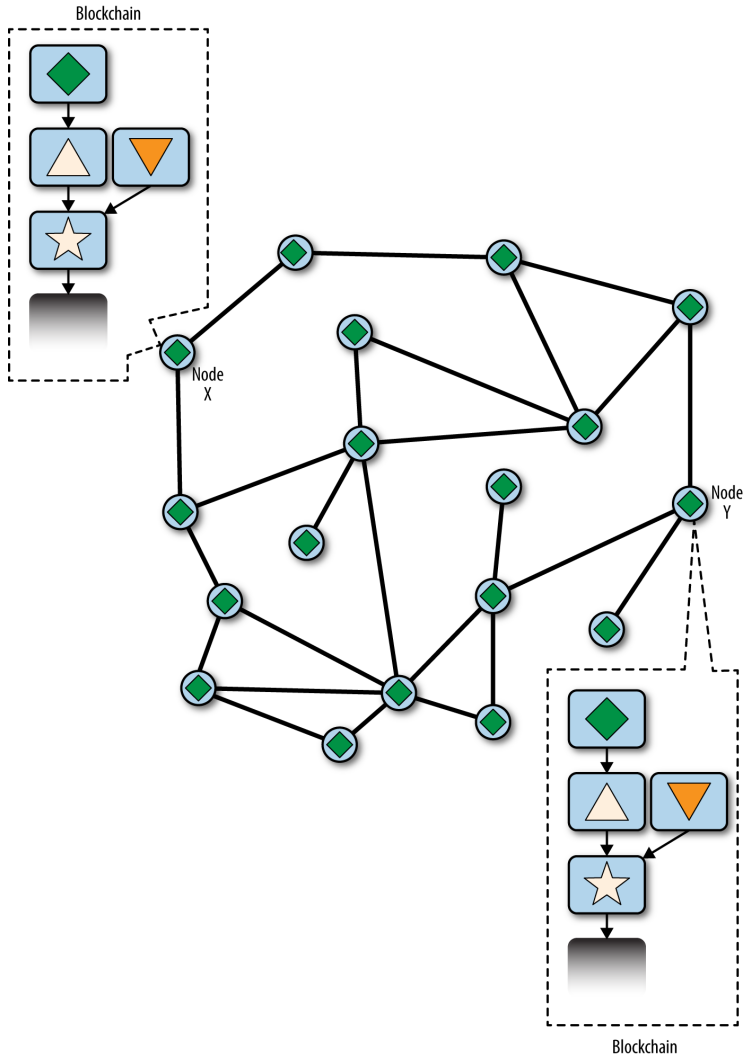
Mastering Bitcoin Open Edition, by Andreas M. Antonopoulos. Creative Commons Attribution-ShareAlike 4.0 International License.

Παράδειγμα Διακλάδωσης (4)



Mastering Bitcoin Open Edition, by Andreas M. Antonopoulos. Creative Commons Attribution-ShareAlike 4.0 International License.

Παράδειγμα Διακλάδωσης (5)



Mastering Bitcoin Open Edition, by Andreas M. Antonopoulos. Creative Commons Attribution-ShareAlike 4.0 International License.

Επισκόπηση

Γενικά

- Ο απλούστερη δοσοληψία αφορά απλώς τη μεταφορά χρημάτων μεταξύ δύο οντοτήτων.
- Δεδομένου όμως ότι η δοσοληψία υλοποιείται μέσω του κώδικα επιβεβαίωσής της, μπορούμε να φτιάξουμε πιο περίπλοκες δοσοληψίες.
- Αυτή είναι η βάση για τα *έξυπνα συμβόλαια* (smart contracts).

Διαιτησία

Έστω ότι θέλουμε να υλοποιήσουμε ένα συμβόλαιο το οποίο θα εκτελεστεί:

- Είτε αν ο αγοραστής συμφωνήσει ότι ο πωλητής έχει παραδόσει το εμπόρευμα.
- Είτε, σε περίπτωση διαφωνιών, αν ένας τρίτος φορέας, διαιτητής, αποφανθεί ότι ο πωλητής έχει πράξει ό,τι έπρεπε.

Πρωτόκολλο Διαιτησίας (1)

1. Ο αγοραστής και ο πωλητής συμφωνούν να χρησιμοποιήσουν έναν συγκεκριμένο διαιτητή.
2. Ο αγοραστής ζητά το δημόσιο κλειδί του πωλητή (K1) και το δημόσιο κλειδί του διαιτητή (K2), ενώ έχει στη διάθεσή του ένα δικό του δημόσιο κλειδί (K3).
3. Ο αγοραστής στέλνει στον πωλητή το K2. Ο πωλητής επιβεβαιώνει ότι το K2 είναι του διαιτητή. Αυτό μπορεί να γίνει στέλνοντάς του ένα τυχαίο μήνυμα και ζητώντας του να το υπογράψει με το ιδιωτικό κλειδί που αντιστοιχεί στο K2.
4. Ο αγοραστής δημιουργεί μια δοσοληψία (Tx1) με τον ακόλουθο κώδικα στην έξοδο:

   `2 <K1> <K2> <K3> 3 CHECKMULTISIGVERIFY`

Πρωτόκολλο Διαιτησίας (2)

Τώρα υπάρχουν τρεις τρόποι να κλείσει το συμβόλαιο:

1. Ο αγοραστής και ο πωλητής συμφωνούν, άρα ο αγοραστής δημιουργεί μια δοσοληψία με την υπογραφή του και τη στέλνει στον πωλητή για να προσθέσει τη δική του.
2. Ο αγοραστής και ο διαιτητής συμφωνούν, άρα τώρα ο αγοραστής στέλνει τη νέα δοσοληψία στο διαιτητή, ο οποίος την υπογράφει και ο αγοραστής παίρνει τα λεφτά του πίσω.
3. Ο διαιτητής και ο πωλητής συμφωνούν, άρα ο πωλητής δημιουργεί μια δοσοληψία με την υπογραφή του και τη στέλνει στο διαιτητή για να προσθέσει τη δική του.

Επισκόπηση

Πηγές

- How the Bitcoin protocol actually works, `http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/`
- Mastering Bitcoin: Unlocking Digital Cryptocurrencies, Andreas M. Antonopoulos, 2nd edition, O'Reilly Media, 2016.

- Mastering Bitcoin: Unlocking Digital Cryptocurrencies, Andreas M. Antonopoulos, 2nd edition, O'Reilly Media, 2016.

- Bitcoin and Cryptocurrency Technologies, Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, Princeton University Press, 2016.