Τεχνολογίες Blockchain & Αποκεντρωμένες Εφαρμογές

Ι. Μαυρίδης, Π. Φουληράς
MSN lab *http://msnlab.uom.gr*

Διάλεξη #04

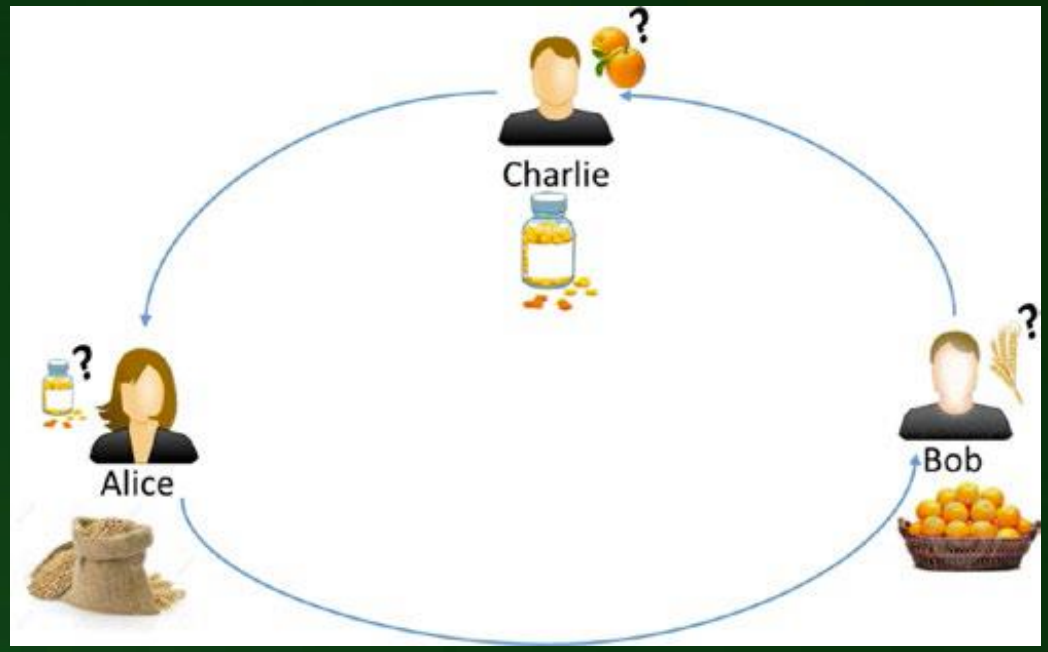
Πώς λειτουργεί το Bitcoin #2

Περιεχόμενα

- Η Ιστορία του Χρήματος
- Bitcoin
  - Τρόπος Χρήσης του BTC & Θέμα με Forks
  - Δομή Μπλοκ & Δένδρο Merkle
  - Στόχος Δυσκολίας & Genesis Block
  - Δίκτυο BTC
  - Συναλλαγές & Συναίνεση
  - Διάφορα

Ιστορικοί Τρόποι Συναλλαγών – (1)

- Ανταλλαγές Ειδών (Barter System)
  - Καλό σύστημα εάν ο ένας έχει ό,τι θέλει ο άλλος, αλλιώς χρειάζεται τρίτος που να το έχει



Ιστορικοί Τρόποι Συναλλαγών – (2)

- Επίλυση με ανταλλαγή ειδών που χρειάζονται όλοι ή οι περισσότεροι
  - Π.χ., πρόβατα, γάλα, σπόροι, γάλα, κλπ.
  - Δύσκολη όμως η αποθήκευση τέτοιων αγαθών

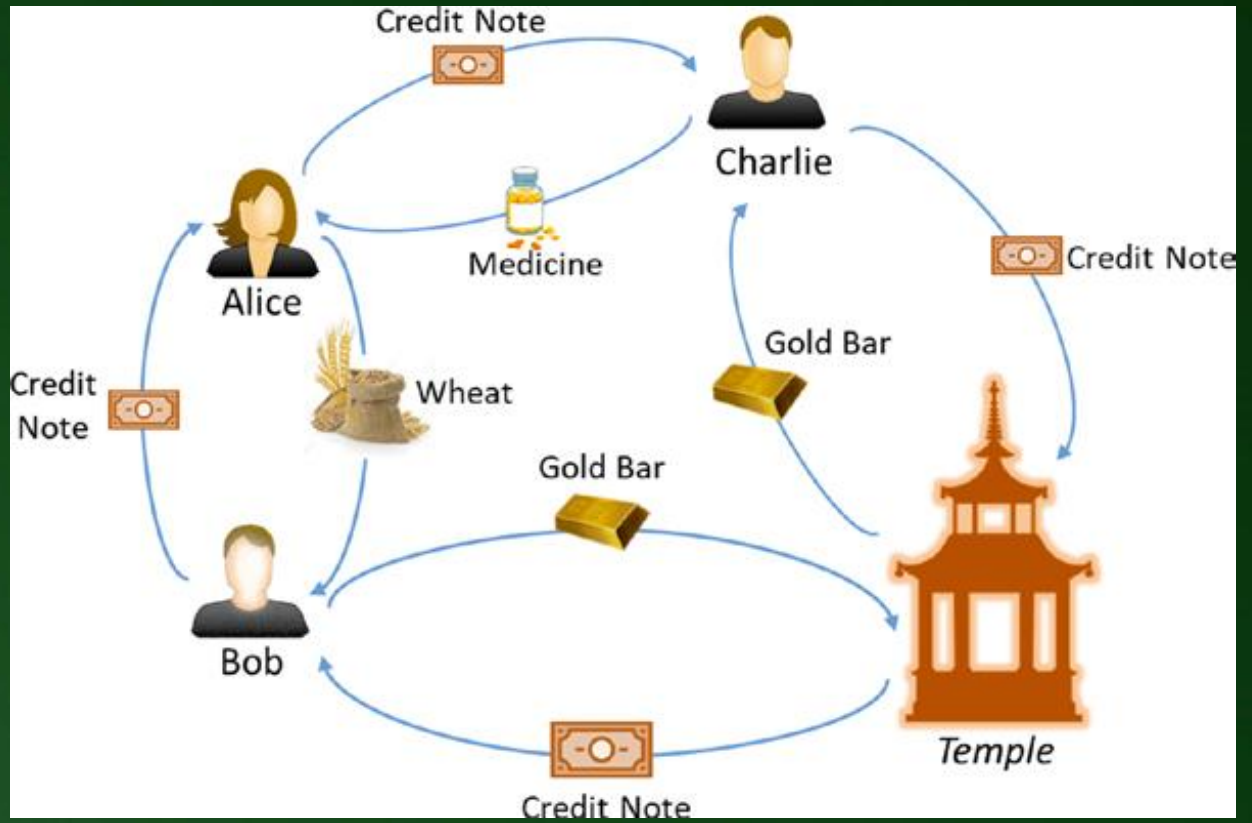
Ιστορικοί Τρόποι Συναλλαγών – (3)

- Επίλυση με ανταλλαγή μικρών μεταλλικών αντικειμένων (νομίσματα)
  - Κυρίως από χρυσό ή άργυρο επειδή δεν διαβρώνονται
  - Δημιουργία (κοπή) από κράτη για να είναι αναγνωρίσιμα ως προς την αξία τους
  - Πρόβλημα η ευπάθεια σε κλοπή

Ιστορικοί Τρόποι Συναλλαγών – (4)

- Επίλυση μέσω Ναών, επειδή υπήρχε η πεποίθηση ότι δεν θα διαπράξει κανείς ιεροσυλία
  - Κατάθεση χρυσού/αργύρου με απόδειξη παραλαβής ώστε να μπορεί αργότερα ο φέρων την απόδειξη να πάρει τα τιμαλφή
  - Ο κάτοχος της απόδειξης μπορούσε να κυκλοφορήσει την απόδειξη ως χρήμα

Αρχή της Εποχής των Τραπεζών



Εποχή των Τραπεζών – (1)

- Αρχικά κάθε χαρτονόμισμα είχε κάλυψη από αντίστοιχο χρυσό ή άργυρο
- Αργότερα το “fiat currency” (χρήμα μέσω διατάγματος) το οποίο δεν έχει καμία ενσωματωμένη αξία και εκδίδεται βασισμένο στην Πίστη (στην οικονομία, κράτος, οργανισμό, κλπ.)

Εποχή των Τραπεζών – (2)

- Η γνωστή φράση φαίνεται στα παραδείγματα κάτω

Ψηφιοποίηση του Χρήματος

- Στην δεκαετία του 1990, με την έλευση του Διαδικτύου, ακόμα και το Τραπεζικό Σύστημα άρχισε να ψηφιοποιείται
- Τα τυπωμένα χαρτονομίσματα μειώθηκαν σημαντικά με τις ευλογίες των τραπεζών και το μεγαλύτερο μέρος του χρήματος είναι πλέον λογιστικές εγγραφές σε λογαριασμούς

Τρέχον Σύστημα & Ζητήματα

- Το βασικό στοιχείο των τρεχουσών συναλλαγών είναι η Πίστη (εμπιστοσύνη) στο όλο σύστημα που στηρίζεται σε κάποιες κεντρικές οντότητες, όπως κυβερνήσεις, τράπεζες ή οργανισμούς
- Η επιρροή των οντοτήτων αυτών είναι πολύ μεγάλη, όπως και το κόστος (λόγω προμήθειας) των συναλλαγών
  - Οι συναλλαγές μέσω φυσικών νομισμάτων ήταν άμεσες (άμεση εκκαθάριση) και χωρίς προμήθεια

Περιεχόμενα

- Η Ιστορία του Χρήματος
- Bitcoin
  - Τρόπος Χρήσεως του BTC & Θέμα με Forks
  - Δομή Μπλοκ & Δένδρο Merkle
  - Στόχος Δυσκολίας & Genesis Block
  - Δίκτυο BTC
  - Συναλλαγές & Συναίνεση
  - Διάφορα

Η Αυγή του Bitcoin

- Το Bitcoin (2009) πρότεινε ένα διαφορετικό τρόπο διενέργειας και εκκαθάρισης συναλλαγών
  - Ασφαλείς ηλεκτρονικές πληρωμές (με κρυπτογράφηση και όχι εμπιστοσύνη σε τρίτον)
  - Κάλυψη όχι από χρυσό, αλλά από υπολογιστική ισχύ
  - Έχει αντέξει κυβερνοεπιθέσεις επί >10 χρόνια

Τι είναι το Bitcoin (BTC) – (1)

- Ψηφιακό κρυπτονόμισμα (χωρίς εγγύηση από τράπεζα ή άλλα TTP) για συναλλαγές p2p
- Το μέγιστο ποσό BTC θα υπάρξει το 2140 (21 εκατομμύρια)
- Δημιουργείται μέσω “mining”
  - Απαιτείται σημαντική υπολογιστική ισχύς
  - Η μικρότερη υποδιαίρεση: 1 Satoshi = 0,00000001 BTC

Τι είναι το Bitcoin (BTC) – (2)

- Οι “miners” (“εξορύκτες”) κερδίζουν BTC
  1. είτε δημιουργώντας νέα
  2. είτε ως αμοιβή για επικύρωση συναλλαγών

- Θα ισχύει μόνον το 2ο όταν ολοκληρωθεί η δημιουργία των 21 εκατομμύριων BTC
  - 50 BTC αμοιβή στην αρχή, 50% κάθε 4 χρόνια
    - 50 + 25 + 12.5 + 6.25 + 3.125 + … = 100 BTC συνολικά
  - Περίπου 210.000 block παράγονται κάθε 4 χρόνια
    - 210.000 * 100 = 21.000.000 BTC

Πώς προκύπτει η Αξία του BTC;

- Όπως προκύπτει για οποιοδήποτε αγαθό:
  - Προσφορά και Ζήτηση
    - Π.χ., γιατί έχει μεγάλη αξία ένας πίνακας του Πικάσσο;
- Αρχικά το BTC είχε μηδενική αξία
- Η σταδιακή πίστη στις συναλλαγές του και το άνω όριο των 21 εκατομμυρίων BTC (άρα περιορισμένο) του προσέδωσαν τη σημερινή του αξία

Γιατί η Αστάθεια στην Αξία του;

- Αποτελεί περιουσιακό στοιχείο υψηλού κινδύνου
- Δεν υπάρχει ένα σημείο ανταλλαγής του, αλλά πολλά με τις δικές τους τιμές ανταλλαγής
- Μεγάλη κάλυψη από τον Τύπο (θετική και αρνητική)
- Αποδοχή από εμπορικούς γίγαντες
- Απαγόρευση σε ορισμένες χώρες
- Ίσως σταθεροποιηθεί με τον χρόνο, αλλά σίγουρα θα καταρρεύσει εάν υπάρξει τεχνική του αποτυχία

Περιεχόμενα

- Η Ιστορία του Χρήματος
- Bitcoin
  - Τρόπος Χρήσης του BTC & Θέμα με Forks
  - Δομή Μπλοκ & Δένδρο Merkle
  - Στόχος Δυσκολίας & Genesis Block
  - Δίκτυο BTC
  - Συναλλαγές & Συναίνεση
  - Διάφορα

Τρόπος Χρήσης του BTC -1

- Εγκαθιστούμε ένα BTC wallet (πορτοφόλι)
  - Δημιουργεί την πρώτη μας διεύθυνση BTC (δημόσιο κλειδί)
  - Μπορούμε να δημιουργήσουμε (και πρέπει) και άλλες, επειδή η συνεχής χρήση της ίδιας διεύθυνσης μπορεί να διευκολύνει τον παραλήπτη στο να ανιχνεύσει και να καταλάβει ποιοί είμαστε
  - Το BTC δεν είναι πλήρως ανώνυμο, αλλά ψευδο-ανώνυμο
  - Δεν υπάρχει η έννοια του λογαριασμού και όλες οι εγγραφές αφορούν συναλλαγές

Τρόπος Χρήσης του BTC -2

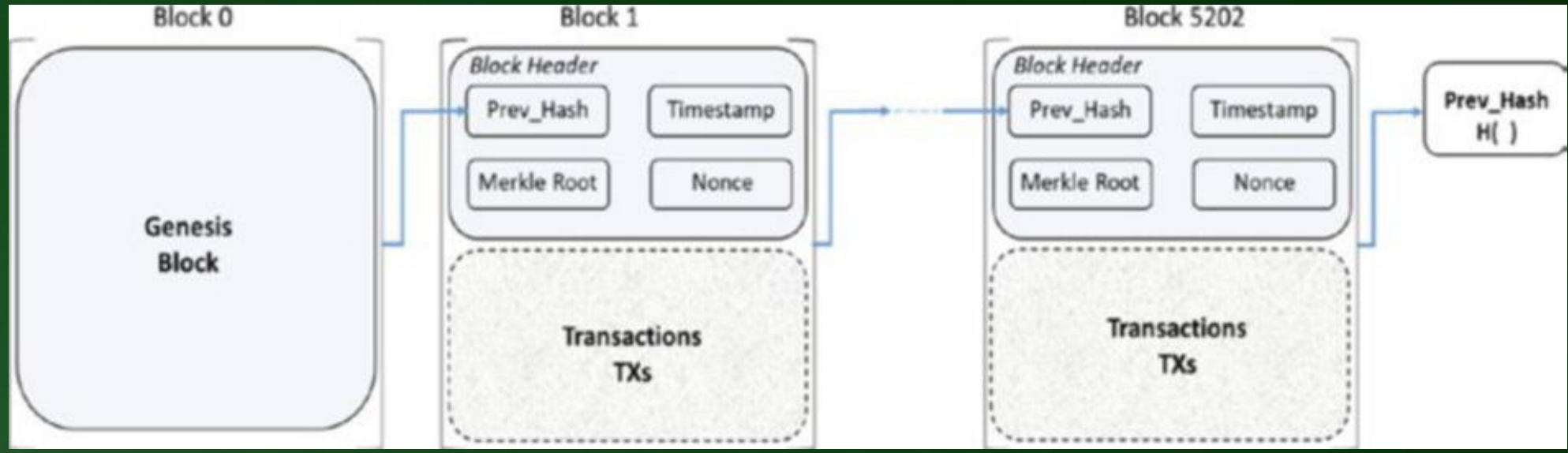
- Το BTC wallet υπολογίζει εύκολα το υπόλοιπο (για ξόδεμα) καθώς έχει τα ιδιωτικά κλειδιά που αντιστοιχούν στα δημόσια με τα οποία έγιναν συναλλαγές
- Χρειάζεται μεγάλη προσοχή στη διαχείριση των πορτοφολιών (οι πληρωμές είναι μη αντιστρέψιμες)
- Υπάρχει μεγάλη ποικιλία πορτοφολιών
  - online: υπήρξαν προβλήματα ασφάλειας
  - offline (“cold”): πιο ασφαλή για αποθήκευση του μεγαλύτερου ποσού
    - προσοχή γιατί αν χάσουμε το ιδιωτικό κλειδί, χάνουμε τα σχετιζόμενα χρήματα

Τρόπος Χρήσης του BTC -3

- Μπορεί κανείς να είναι:
  - Miner που λειτουργεί ένα πλήρη κόμβο
    - Bitcoin Core client
  - Trader ή απλός χρήστης
    - χρησιμοποιεί ανταλλακτήριο για να ανταλλάσσει BTC με εθνικό νόμισμα
      - Προσοχή και εδώ…

Το Blockchain στο BTC

- Το BTC Core client χρησιμοποιεί τη ΒΔ “LevelDB” της Google για αποθήκευση της δομής Blockchain
- Κάθε μπλοκ ταυτοποιείται από το hash του (SHA256) και περιέχει στην κεφαλίδα του το hash του προηγούμενου μπλοκ

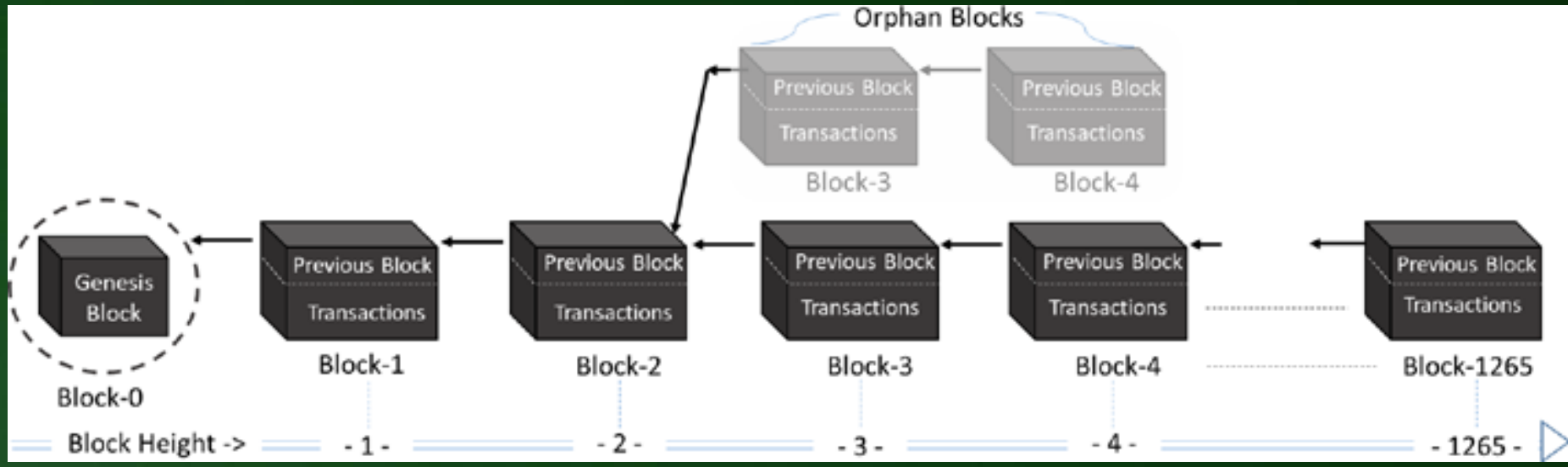


Πρακτικά Αδύνατη η Αλλοίωση Συναλλαγών

- Εάν κάποιος αλλάξει μία παλιά συναλλαγή, π.χ. στο μπλοκ 441, δεν θα ταιριάζει το Hash σε όλα τα μεταγενέστερα μπλοκ
- Ακόμα και αν το αλλάξει σε όλα τα μεταγενέστερα, θα πρέπει να το αλλάξει τουλάχιστο στο 51% των συνολικών κόμβων που έχουν αποθηκευμένα τα μπλοκ αυτά

Ορφανά μπλοκ & Forks

- Υπάρχει μόνο εάν μονοπάτι προς το Genesis μπλοκ, αλλά όχι ανάποδα
- Όταν προτείνονται ταυτόχρονα 2 έγκυρα μπλοκ, μόνο το ένα γίνεται μέρος της αλυσίδας, ενώ το άλλο γίνεται ορφανό
- Κάθε κόμβος προτιμά τη συναλλαγή που μαθαίνει πρώτα και στηρίζεται στη μακρύτερη αλυσίδα:

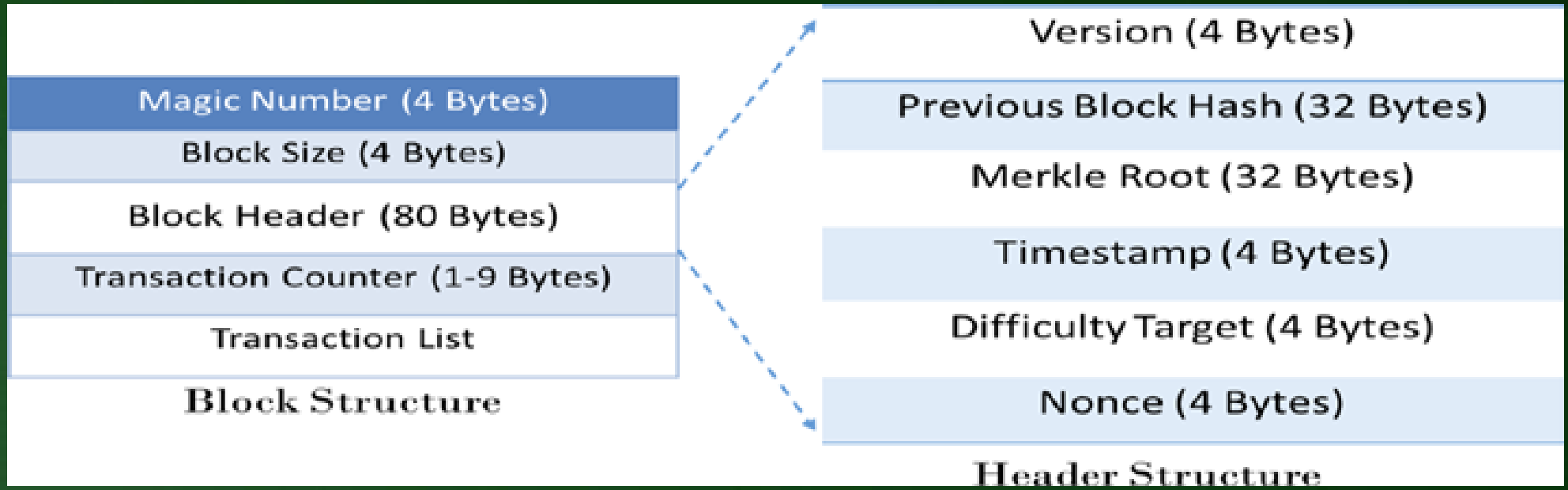


Περιεχόμενα

- Η Ιστορία του Χρήματος
- Bitcoin
  - Τρόπος Χρήσεως του BTC & Θέμα με Forks
  - Δομή Μπλοκ & Δένδρο Merkle
  - Στόχος Δυσκολίας & Genesis Block
  - Δίκτυο BTC
  - Συναλλαγές & Συναίνεση
  - Διάφορα

Δομή Μπλοκ

- Σταθερή για όλα τα μπλοκ



Δομή Μπλοκ – Λεπτομέρειες

Πεδίο	Μέγεθος (byte)	Περιγραφή
Magic Number	4	Σταθερός: 0xD9B4BEF9 (δείχνει αρχή block)
Block Size	4	Μέγεθος του block. BTC 1MB, BTC Cash 2MB
Block Header	80	Hash προηγ. block, Nonce, Merkle Root, κλπ.
Transaction Counter	1-9 (μεταβλητό μέγεθος)	Συνολικό πλήθος συναλλαγών που περιλαμβάνονται στο block
Transaction List	σταθερό μέγεθος, μεταβλητό πλήθος	Λίστα όλων των συναλλαγών του block (καταλαμβάνει το υπόλοιπο block)

Δομή Κεφαλίδας Μπλοκ – Λεπτομέρειες

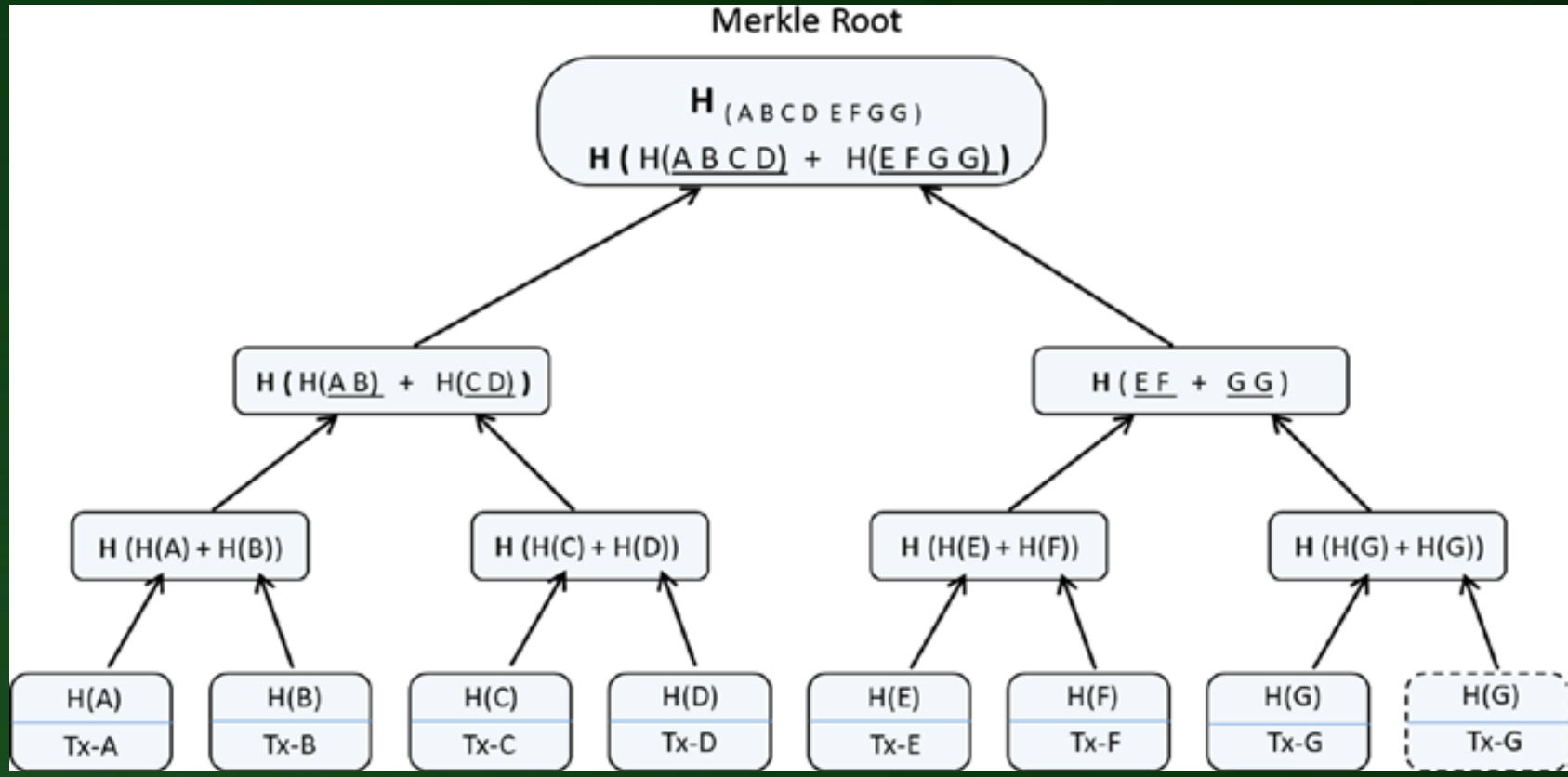
Πεδίο	Μέγεθος (byte)	Περιγραφή
Version	4	Η έκδοση πρωτοκόλλου BTC που χρησιμοποιείται
Previous Block Hash	32	Το Hash της κεφαλίδας του προηγ. μπλοκ στην αλυσίδα (SHA256)
Merkle Root	32	Η ρίζα του Merkle tree με τα hash των συναλλαγών του μπλοκ
Timestamp	4	Τοπική χρονοσφραγίδα δημιουργίας μπλοκ (σε μορφή Unix)
Difficulty Target	4	Τα bit δυσκολίας που καθορίζουν την τιμή Στόχο για το PoW
Nonce	4	Ο τυχαίος αριθμός που ικανοποίησε τον γρίφο PoW κατά την εξόρυξη

Δένδρα Merkle στο BTC

- Merkle tree: δένδρο με hash των συναλλαγών στα φύλλα
- Κάθε μπλοκ περιέχει το Hash της κεφαλίδας του προηγούμενου μπλοκ και τη δική του ρίζα Merkle
  - Είναι αρκετό αφού αν αλλάξει μια συναλλαγή στο μπλοκ, δεν θα ταιριάζει η ρίζα Merkle
  - Έτσι γίνεται γρήγορα η επιβεβαίωση

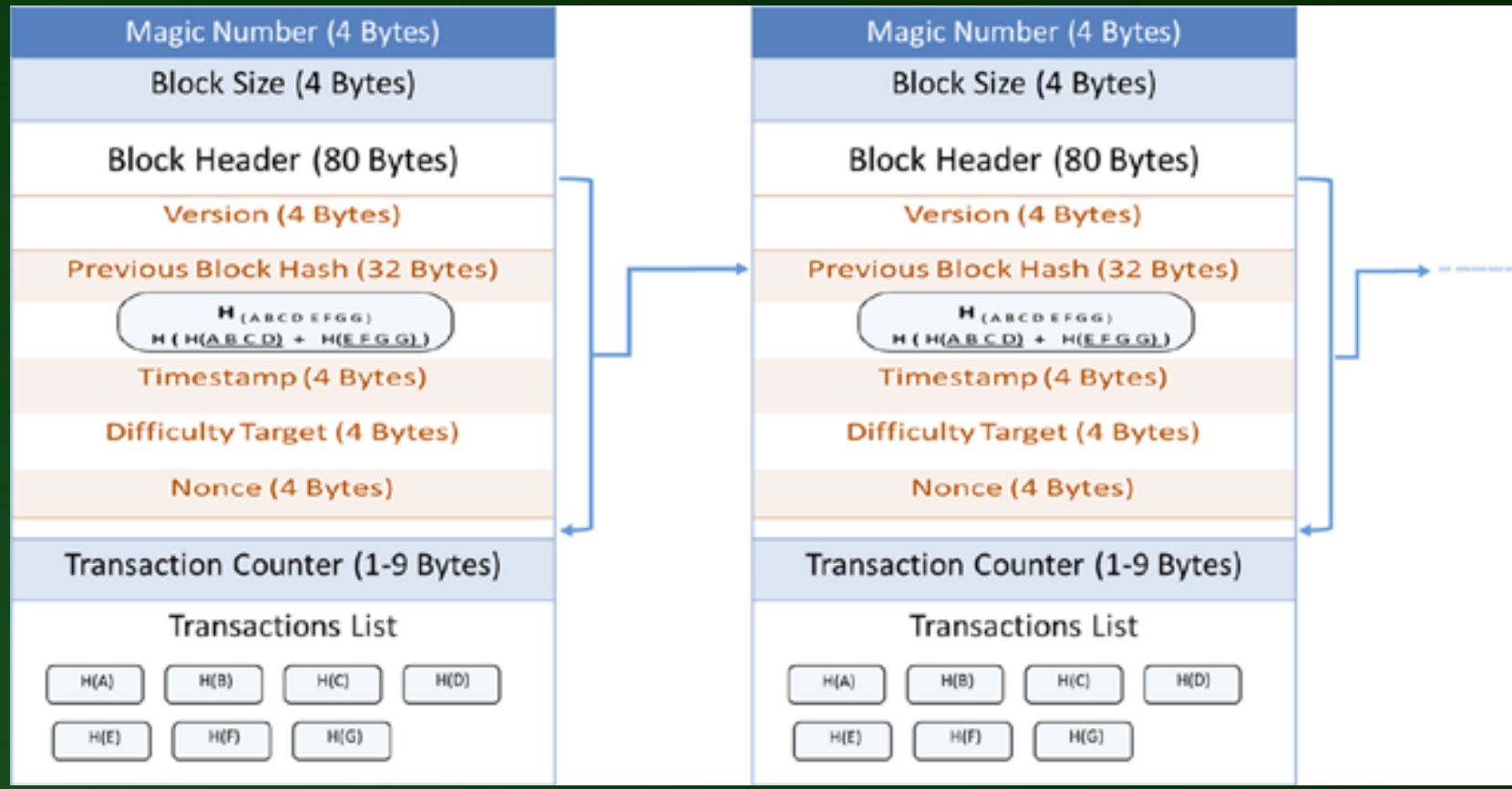
Δένδρο Merkle στο BTC – Παράδειγμα

- Hash 7 συναλλαγών στα φύλλα
  - A, B, C, D, E, F, G
  - Επανάληψη τελευταίου κόμβου



Αναπαράσταση Δένδρου Merkle στο BTC

- Το μονοπάτι Merkle προς μια συναλλαγή είναι αρκετό για να επιβεβαιωθεί η συμμετοχή της σε ένα μπλοκ



Προσοχή!

- Μία πρόσφατη συναλλαγή Tx_i δεν αποτελεί αμέσως μέρος του Blockchain
- Πρέπει να περιμένουν τα ενδιαφερόμενα μέρη τους miners να επικυρώσουν ένα ολόκληρο μπλοκ από συναλλαγές όπου θα περιλαμβάνεται και η συναλλαγή Tx_i

Περιεχόμενα

- Η Ιστορία του Χρήματος
- Bitcoin
  - Τρόπος Χρήσεως του BTC & Θέμα με Forks
  - Δομή Μπλοκ & Δένδρο Merkle
  - Στόχος Δυσκολίας & Genesis Block
  - Δίκτυο BTC
  - Συναλλαγές & Συναίνεση
  - Διάφορα

Στόχος Δυσκολίας – (1)

- Μόλις ένα μπλοκ γεμίσει με έγκυρες συναλλαγές, πρέπει να υπολογισθεί το Hash της κεφαλίδας του ώστε να είναι μικρότερο από την τιμή Στόχο που προκύπτει από τα bit δυσκολίας
- Αρχικά επιλέγεται τιμή 0 για το nonce
- Ο miner συνεχίζει αυξάνοντας το nonce και υπολογίζοντας το hash της κεφαλίδας, έως ότου η τιμή Hash γίνει μικρότερη από την τιμή Στόχο

Στόχος Δυσκολίας – (2)

- Τα 32 bit δυσκολίας καθορίζουν την τιμή Στόχο (256 bit) για την εξόρυξη του μπλοκ
  - Πρέπει να βρεθεί nonce τέτοιο ώστε το Hash της κεφαλίδας να είναι μικρότερο από την τιμή Στόχο
  - Όσο μικρότερη η τιμή Στόχος, τόσο δυσκολότερη η εύρεση
  - Με SHA256, η τιμή Hash θα είναι από 0 έως $2^{256}-1$

Στόχος Δυσκολίας – (3)

- Ο τύπος για τον υπολογισμό της τιμής Στόχου:

  target = coefficient * $2^{(8 * (\text{exponent} - 3))}$

- Παράδειγμα για bit δυσκολίας: 0x1b0404cb
  - coefficient = 0x0404cb & exponent = 0x1b
  - Άρα: target = coefficient * $2^{(8 * (\text{exponent} - 3))}$

    target = 0x0404cb * $2^{(0x08 * (0x1b - 0x03))}$

    = 0x0404cb * $2^{(0x48)}$

target = (256 bit ή 64 δεκαεξαδικά ψηφία)

0x00000000000404CB000000000000000000000000000000000000000000000000

Στόχος Δυσκολίας – (4)

- Ανά 2 εβδομάδες παράγονται 2.016 μπλοκ
  - περίπου 10’/μπλοκ (Μ.Ο.)
  - στην πράξη από 1’-15’, λόγω ασύγχρονου δικτύου
- Το επίπεδο δυσκολίας διαμορφώνεται ανάλογα
  - Για χρόνο Τ εβδομάδων εύρεσης 2016 μπλοκ
    - από το πεδίο τοπικής χρονοσήμανσης
  - Το επίπεδο δυσκολίας (difficulty target) πολλαπλασιάζεται επί Τ/2 βδομάδες
    - οπότε αυξάνεται/μειώνεται

Στόχος Δυσκολίας – Καθορισμός

- Κάθε κόμβος προτείνει τον δικό του μετά από κάθε 2.016 μπλοκ, αλλά συνήθως καταλήγουν στην ίδια τιμή επειδή ο τύπος είναι ίδιος για όλους:

  New Target = Old Target * (T/2 weeks)

  ⇨ New Target = Old Target * (time for 2.016 block σε sec / 1.209.600’’)

Στόχος Δυσκολίας – Σημαντικές Λεπτομέρειες

- Ο λόγος που ο Στόχος Δυσκολίας δεν είναι σταθερός, οφείλεται στο ότι το υλικό των Η/Υ γίνεται ισχυρότερο με την πάροδο του χρόνου
- Το “χάσμα” 10’ περίπου για τη δημιουργία κάθε μπλοκ, υπάρχει ώστε να προλαβαίνουν όλοι οι κόμβοι να προτείνουν και να καταλήγουν σε νέες προτάσεις, καθώς και να επικυρώνουν ή όχι τα προτεινόμενα μπλοκ, κλπ.

Genesis Block – (1)

- Ή “block-0” – το πρώτο μπλοκ που δημιουργήθηκε (2009) κατά την εκκίνηση του BTC
  - Είναι ορισμένο στατικά στον κώδικα του BTC (αρχείο “chainparams.cpp”) αφού είναι το πρώτο που δημιουργήθηκε και δεν δείχνει σε κάποιο προηγούμενο.
  - Π.χ., με την εντολή Bitcoin Core:

    ```
    $ bitcoin-cli getblock
    000000000019d6689c085ae165831e934ff763ae46a2a6c1
    72b3f1b60a8ce26f
    ```

    επιστρέφεται:

Genesis Block – (2α)


```
{
  "hash" : "000000000019d6689c085ae165831e934ff763ae46a2a6
  c172b3f1b60a8ce26f",
  "confirmations" : 308321,
  "size" : 285,
  "height" : 0,
  "version" : 1,
  "merkleroot" : "4a5e1e4baab89f3a32518a88c31bc87f618
  f76673e2cc77ab2127b7afdeda33b",
  "tx" : ["4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc
  77ab2127b7afdeda33b"],
```

Genesis Block – (2β)


```
  "time" : 1231006505,
  "nonce" : 2083236893,
  "bits" : "1d00ffff",
  "difficulty" : 1.00000000,
  "nextblockhash" : "000000000839a8e6886ab5951d76
  f411475428afc90947ee320161bbf18eb6048"
}
```


- Το πεδίο “time” αντιστοιχεί στο: *Saturday 3rd January 2009 11:45:05 PM*

MSNlab

Genesis Block – (2γ)

- Δοκιμάστε και το παρακάτω για το ίδιο αποτέλεσμα:

https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

- Όπως βλέπουμε υπάρχει μόνο μια συναλλαγή, που λέγεται ότι είναι τύπου “coinbase”. Αυτού του τύπου οι συναλλαγές:
  - Αφορούν την αμοιβή των miners (γένεση νέων BTC)
  - Δεν έχουν είσοδο και παράγουν μόνο νέα BTC

Περιεχόμενα

- Η Ιστορία του Χρήματος
- Bitcoin
  - Τρόπος Χρήσεως του BTC & Θέμα με Forks
  - Δομή Μπλοκ & Δένδρο Merkle
  - Στόχος Δυσκολίας & Genesis Block
  - Δίκτυο BTC
  - Συναλλαγές & Συναίνεση
  - Διάφορα

Το Δίκτυο BTC – (1)

- P2P, αποκεντρωμένο, χωρίς κεντρική εξουσία και σημείο αποτυχίας
- Κάθε κόμβος μπορεί να συμμετέχει ή να αποχωρεί δυναμικά
- Πλήρεις κόμβοι
  - Μπορούν να εκτελούν όλες τις ενέργειες.
  - Συνεχώς συνδεδεμένοι.
  - Περιέχουν όλες τις συναλλαγές (>200GB)
- Ελαφρείς κόμβοι
  - Δεν κάνουν εξόρυξη νέων μπλοκ, αλλά επικύρωση συναλλαγών μέσω SPV (Simplified Payment Verification).
  - Μπορούν να συμμετέχουν σε “Pool mining” (συνεργασία πολλών για mining νέων μπλοκ)

Το Δίκτυο BTC – (2)

- Οι ελαφρείς κόμβοι επίσης μπορούν να είναι wallets:
  - Εάν κάποιος μας αποστείλει χρήματα, μπορούμε να κατεβάσουμε από το δίκτυο BTC τις αντίστοιχες συναλλαγές, ώστε να ελέγξουμε αν πραγματικά αυτός κατείχε τα χρήματα αυτά
  - Δεν είναι όμως ασφαλείς όσο οι πλήρεις γιατί
    - περιέχουν τις επικεφαλίδες και όχι ολόκληρα τα μπλοκ
    - δεν διαθέτουν όλες τις συναλλαγές και όλα τα UTXO (unspent transaction outputs)

Ανακάλυψη Δικτύου για Νέους Κόμβους – (1)

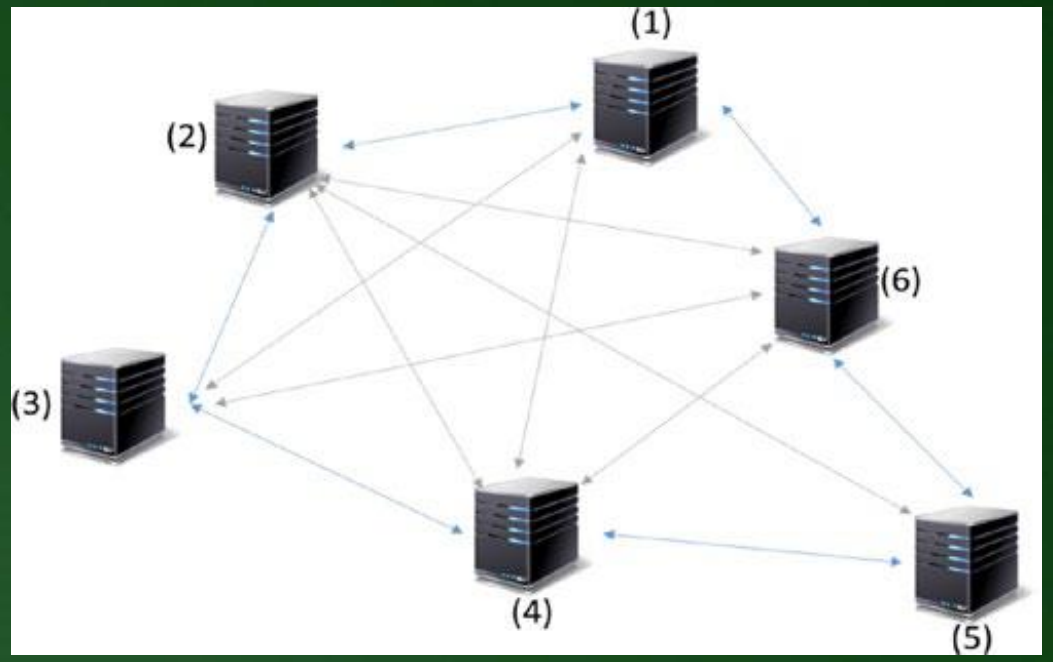
- Όταν ένας κόμβος ξεκινάει για πρώτη φορά, χρησιμοποιεί DNS seeds (DNS servers που ορίζονται στον κώδικα Bitcoin Core) που διατηρούνται από μέλη της κοινότητας BTC παρέχοντας
  - είτε στατικά DNS seeds με σχετικές διευθύνσεις IP και θύρες
  - είτε δυναμικά DNS seeds που διατηρούν λίστες με διευθύνσεις IP ενεργών κόμβων που έχουν εξ ορισμού θύρες BTC
    - 8333 για *mainnet* και 18333 για *testnet*

Ανακάλυψη Δικτύου για Νέους Κόμβους – (2)

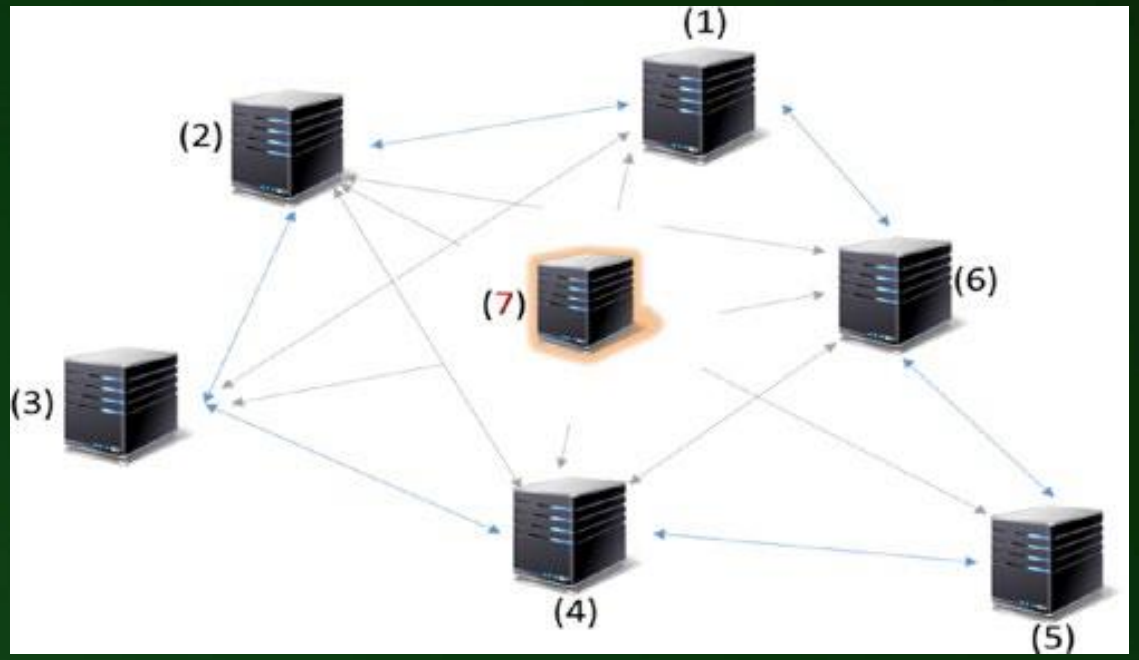
- Όλοι οι πελάτες BTC τηρούν στον κώδικά τους λίστα με διευθύνσεις IP βασικών κόμβων BTC
  - κόμβοι εκκίνησης (bootstrap)

- Στις επόμενες εικόνες εμφανίζονται τα βήματα για δίκτυο BTC 6 κόμβων, όπου ξεκινάει ο 7ος κόμβος

Ανακάλυψη Δικτύου για Νέους Κόμβους – (3)

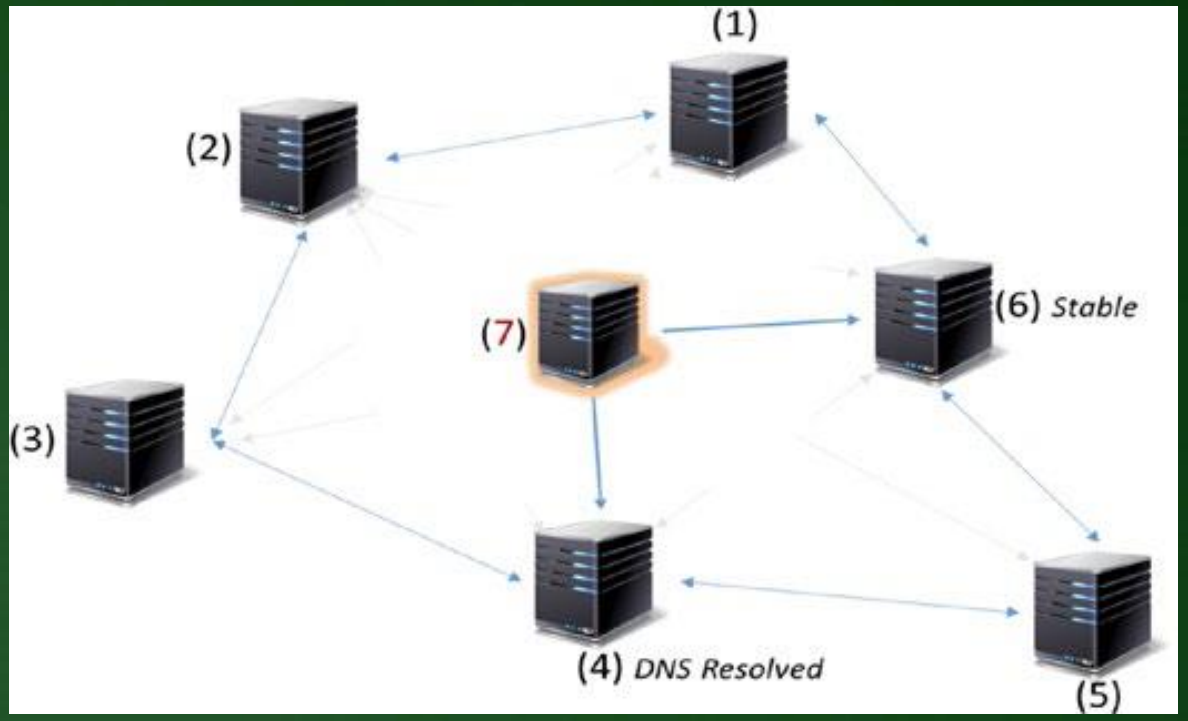


Βήμα #1

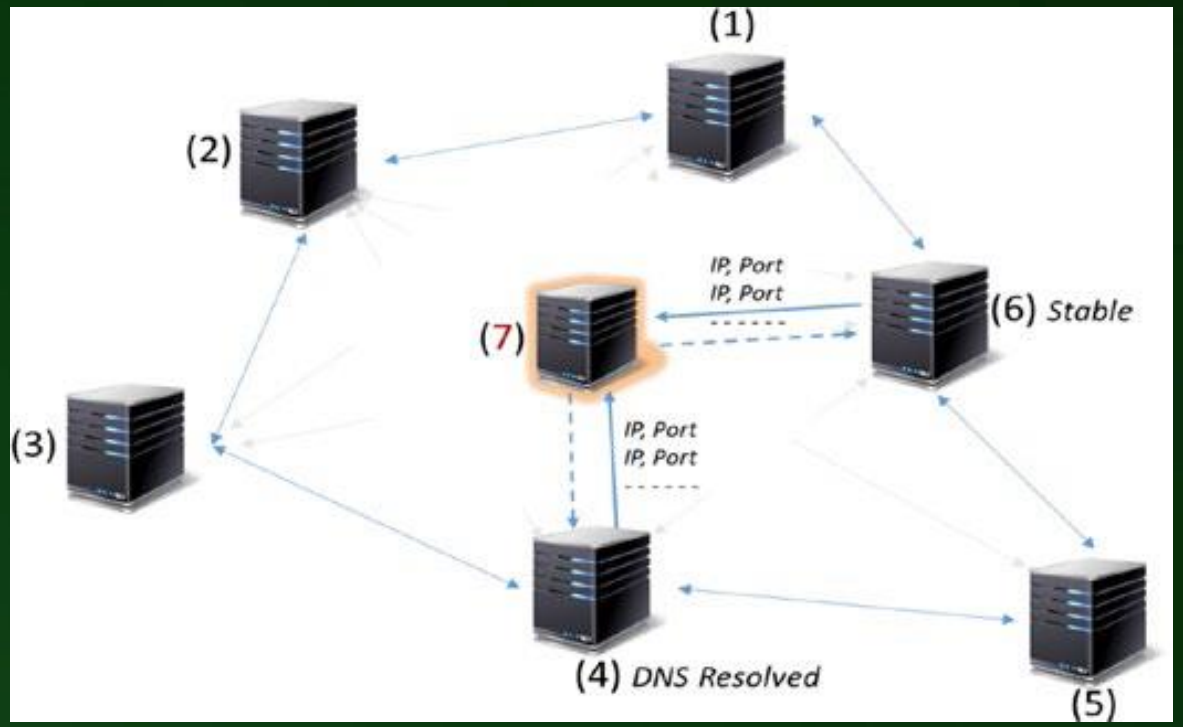


Βήμα #2

Ανακάλυψη Δικτύου για Νέους Κόμβους – (4)

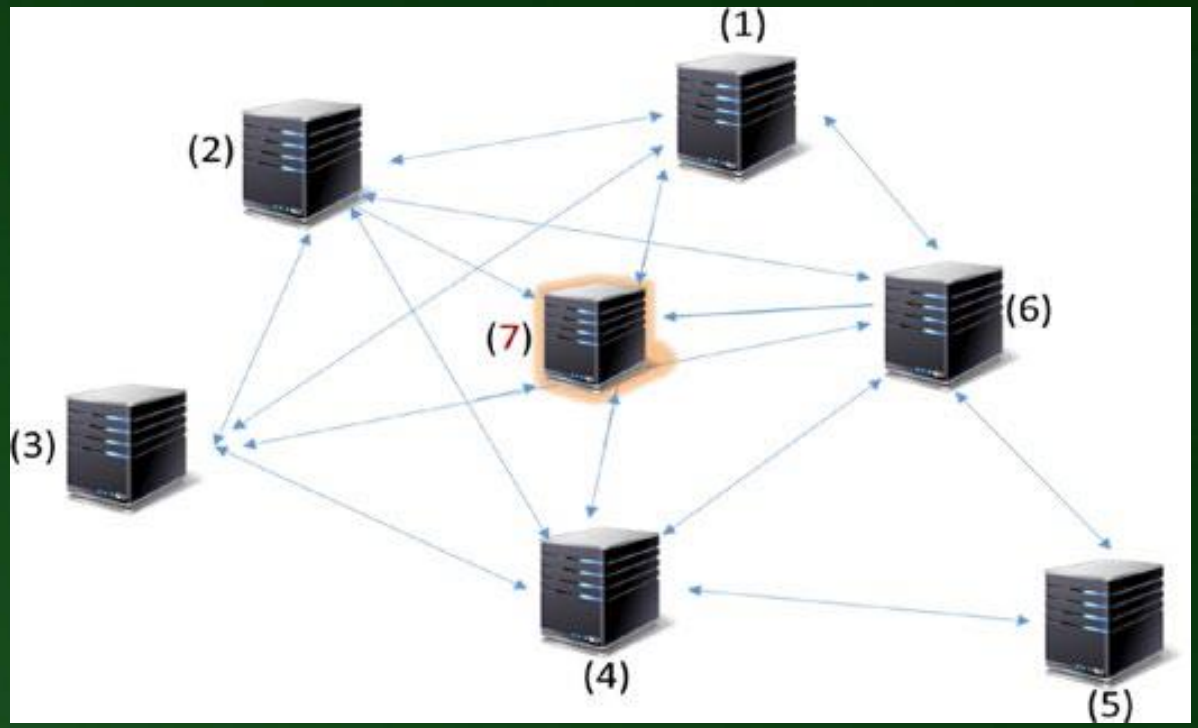


Βήμα #3



Βήμα #4

Ανακάλυψη Δικτύου για Νέους Κόμβους – (5)



Βήμα #5

Περιεχόμενα

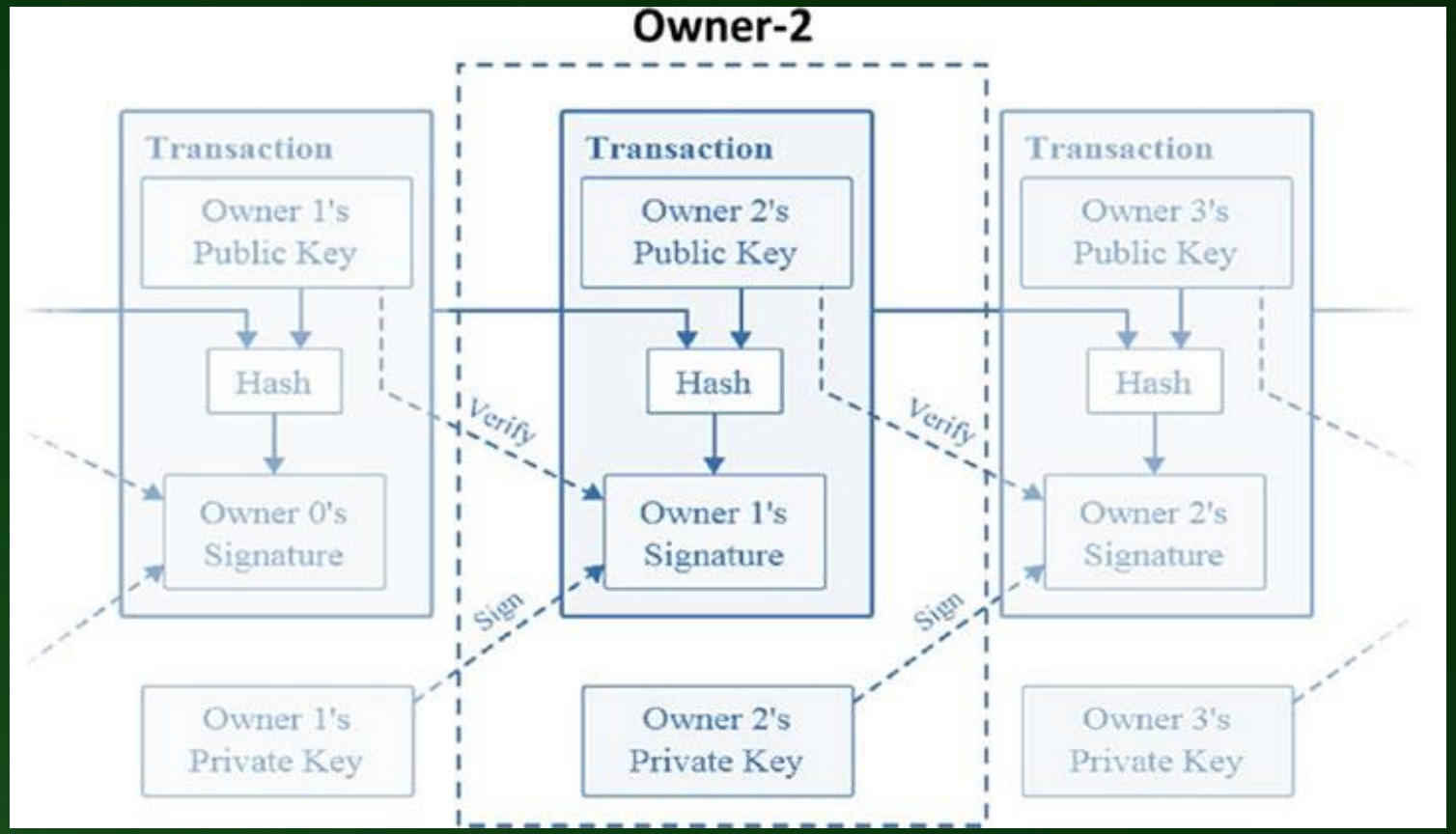
- Η Ιστορία του Χρήματος
- Bitcoin
  - Τρόπος Χρήσεως του BTC & Θέμα με Forks
  - Δομή Μπλοκ & Δένδρο Merkle
  - Στόχος Δυσκολίας & Genesis Block
  - Δίκτυο BTC
  - Συναλλαγές & Συναίνεση
  - Διάφορα

Κατηγορίες Συναλλαγών στο BTC

- Coinbase
  - Κάθε μπλοκ περιέχει μία που εισάγεται από τους ίδιους τους miners ώστε να μπορούν να δημιουργούν νέα νομίσματα
  - Οι miners δεν ελέγχουν πόσα νομίσματα μπορούν να εξορύξουν για κάθε μπλοκ
    - Ξεκίνησε με 50 BTC και συνεχίζει να μειώνεται έως ότου όλα τα BTC σε κυκλοφορία γίνουν 21 εκατομμύρια
- Regular
  - Κανονικές συναλλαγές, όπως οι ανταλλαγές νομισμάτων

Απεικόνιση Συναλλαγής στο BTC

- Ο κάτοχος (owner/payer) μπορεί να μεταφέρει BTC υπογράφοντας ψηφιακά το Hash της πρότερης (λήψη BTC) συναλλαγής μαζί με το Δημόσιο Κλειδί του παραλήπτη (payee)
- Δυνατότητα επιβεβαίωσης από όλους
  - no double-spend



Σημαντική Λεπτομέρεια

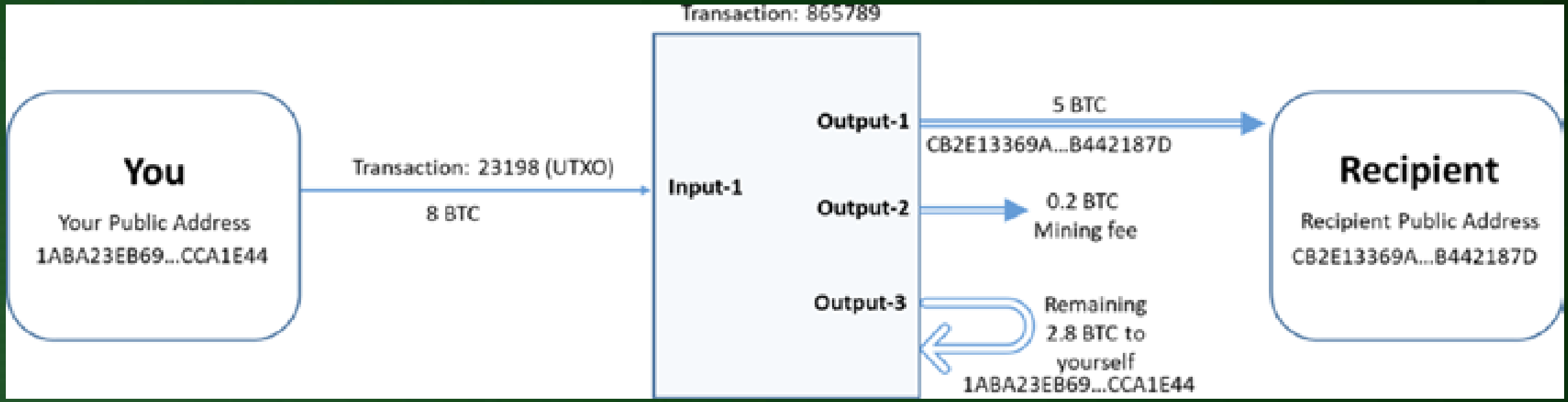
- Στο BTC δεν υπάρχει η έννοια Balance (*Υπόλοιπο Λογαριασμού*)

- Το σύνολο των διαθέσιμων BTC για κάποιον προκύπτει από το άθροισμα των εισερχομένων συναλλαγών προς τις δημόσιες διευθύνσεις του (έχει όσες θέλει)
  - unspent transaction output / UTXO
  - μπορεί να τα ξοδέψει με τα ιδιωτικά του κλειδιά

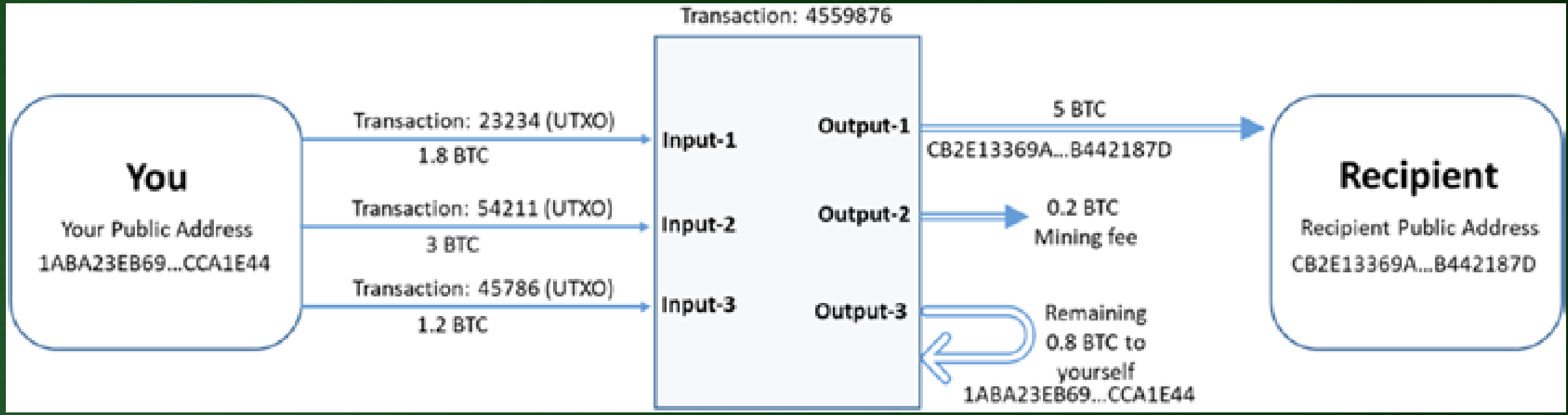
Πώς "Ξοδεύουμε" *k* BTC

- Χρησιμοποιούμε μια ή περισσότερες από τις προηγούμενες συναλλαγές, όπου λάβαμε *k* ή περισσότερα BTC
- Μεταφέρουμε
  - *k* BTC στον παραλήπτη
  - κάποιο ποσό ως transaction fee
  - το όποιο υπόλοιπο στον εαυτό μας

Ξόδεμα BTC με Μία Συναλλαγή Εισόδου



Ξόδεμα BTC με Πολλαπλές Συναλλαγές Εισόδου



Ξόδεμα BTC

- Ασχέτως αν κανείς διατηρεί κόμβο, μπορεί να κάνει συναλλαγές
- Κάθε συναλλαγή αναμεταδίδεται στο δίκτυο από τον παραλήπτη BTC για προστασία από επιθέσεις double-spend
  - gossip protocol
  - η γνώση για όλες τις συναλλαγές είναι ο μόνος τρόπος προστασίας από διπλοξόδεμα

Τι γίνεται με τις Νέες Συναλλαγές;

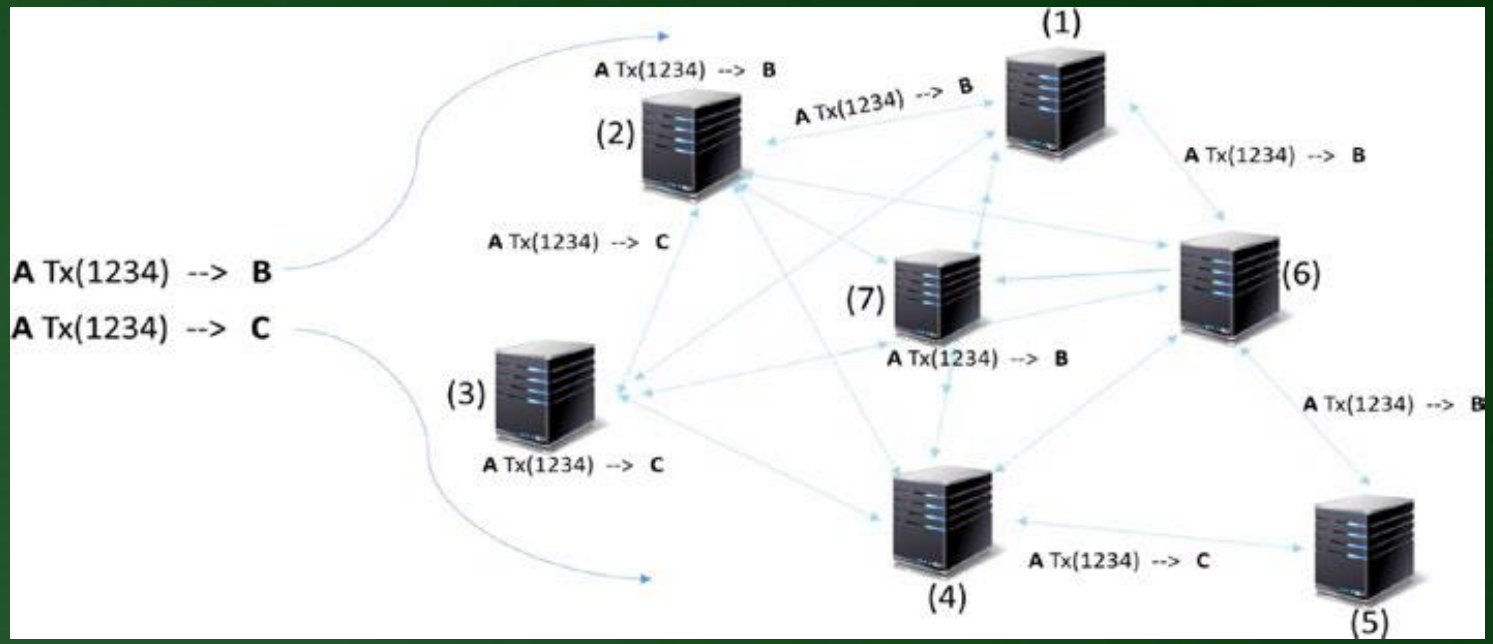
- Κάθε κόμβος
  - τηρεί μια λίστα με όλες τις συναλλαγές που αντιλήφθηκε
  - αναμεταδίδει μόνο τις νέες συναλλαγές (εκτός λίστας)
  - αφαιρεί από τη λίστα τις συναλλαγές που έχουν μπεί σε ένα έγκυρο μπλοκ που έχει γίνει μέρος του Blockchain (κανόνας μακρύτερης αλυσίδας)
    - εφόσον δεν έχει καταλήξει σε Ορφανό Μπλοκ

Τι γίνεται με τις Νέες Συναλλαγές;

- Κάθε πλήρης κόμβος
  - πρέπει να τηρεί τη συνολική λίστα των αξόδευτων συναλλαγών (UTXO), όσο μεγάλη και αν είναι, για λόγους προστασίας από διπλοξόδεμα
  - επανεκπέμπει κάθε συναλλαγή της λίστας που επιβεβαιώνει ότι δεν είναι διπλοξόδεμα
- Η αναζήτηση μεταξύ εκατομμυρίων UTXO για έλεγχο double-spend γίνεται γρήγορα καθώς είναι ταξινομημένα κατά τις τιμές hash

Παράδειγμα Αποτροπής Double Spending – (1)

- A = Alice, B = Bob, C = Charlie, (n) = Κόμβος *n*
- Α προσπαθεί να πληρώσει με την ίδια (εισερχόμενη) συναλλαγή και τους δύο (B και C)
  - Ο (2) έλαβε συναλλαγή από A: Tx(1234) -> B
  - Ο (3) έλαβε συναλλαγή από A: Tx(1234) -> C



Παράδειγμα Αποτροπής Double Spending – (2)

- Και οι δύο κόμβοι βλέπουν ως κανονικές τις συναλλαγές, αλλά όταν ο ένας την εκπέμψει στο δίκτυο, ο άλλος θα την απορρίψει
- Οι υπόλοιποι κόμβοι θα αποδεχθούν όποια καταφθάσει πιο γρήγορα σε αυτούς (αλλά μόνο μια)
- Θα “κερδίσει” τελικά η συναλλαγή που θα περιέχεται στο πρώτο μπλοκ που θα προστεθεί στο blockchain

Consensus και Block Mining – (1)

- Consensus: απαραίτητο για συνέπεια σε ένα κατανεμημένο δίκτυο, αλλά δύσκολα επιτεύξιμο
  - PoW στο BTC
- Block Mining: επιτυχής δημιουργία νέου μπλοκ στο blockchain
  - Στο BTC δεν εμποδίζεται το double-spending ως προσπάθεια (συναλλαγές UTXO), αλλά εξακριβώνεται και ακυρώνονται οι επιπρόσθετες συναλλαγές, επειδή κάθε κόμβος τηρεί πλήρες αντίγραφο όλων των συναλλαγών

Consensus και Block Mining – (2)

- Μπορεί κάποιος κόμβος να συμπεριλάβει σε προτεινόμενο μπλοκ παράνομη συναλλαγή;
  - Ναι, αλλά όλο το mining (PoW) που έκανε για την επικύρωσή του θα πάει χαμένο, αφού οι υπόλοιποι θα το ανακαλύψουν και θα απορρίψουν το μπλοκ
  - Δεν υπάρχει ένα blockchain σε ένα κόμβο μόνο, αλλά αντίγραφά του σε κάθε κόμβο

Consensus και Block Mining – (3)

- Γιατί όμως να μπαίνουν σε τόση φασαρία οι κόμβοι;
- Δύο αμοιβές:
  - "προμήθεια" για το προταθέν μπλοκ μέσω mining
    - από τα transaction fee που κατέβαλαν οι payers
    - προτιμούν να βάζουν στο μπλοκ πολλές δοσοληψίες & δη αυτές με υψηλό fee
  - block reward για τα νέα BTC που δημιουργεί
    - επιπλέον ειδική δοσοληψία: "coin creation" με παραλήπτη τον miner (coinbase)
    - αρχικά 50 BTC, αλλά μειώνεται στο μισό μετά από 210.000 μπλοκ (περίπου κάθε 4 έτη), καθώς μπορούν να υπάρξουν μόνο 21.000.000 BTC συνολικά
- Mining Reward = Block Reward + Total fees of all transactions in the Block
- Στις συναλλαγές του νέου μπλοκ περιλαμβάνεται μια coinbase συναλλαγή

Consensus και Block Mining – (4)

- Όταν ένα νέο μπλοκ φθάσει σε κάποιον κόμβο και αυτός το επιβεβαιώσει και το βάλει στο τοπικό του blockchain, οι εμπεριεχόμενες συναλλαγές είναι οριστικές;
  - Όχι! Π.χ., αν οι περισσότεροι κόμβοι χρησιμοποιούν άλλο μπλοκ αντί για το παραπάνω;

- Μπορεί να γίνει ορφανό μπλοκ αν δεν καταφέρει να αποτελέσει μέρος της μακρύτερης αλυσίδας

Consensus και Block Mining – (5)

- Κάθε επόμενο μπλοκ στην αλυσίδα αποτελεί επιβεβαίωση για τα προηγούμενα.
- Όσα τα μπλοκ προστίθενται κατόπιν, τόσες οι επιβεβαιώσεις για τις συναλλαγές μέσα στο μπλοκ.
- Πόσες επιβεβαιώσεις πρέπει να περιμένει ένας κόμβος για κάποιο μπλοκ πριν το θεωρήσει οριστικά επικυρωμένο;
  - δεν ορίζεται συγκεκριμένος αριθμός, αλλά στην πράξη τέσσερις (4) έως έξι (6) επιβεβαιώσεις θεωρούνται αρκετές

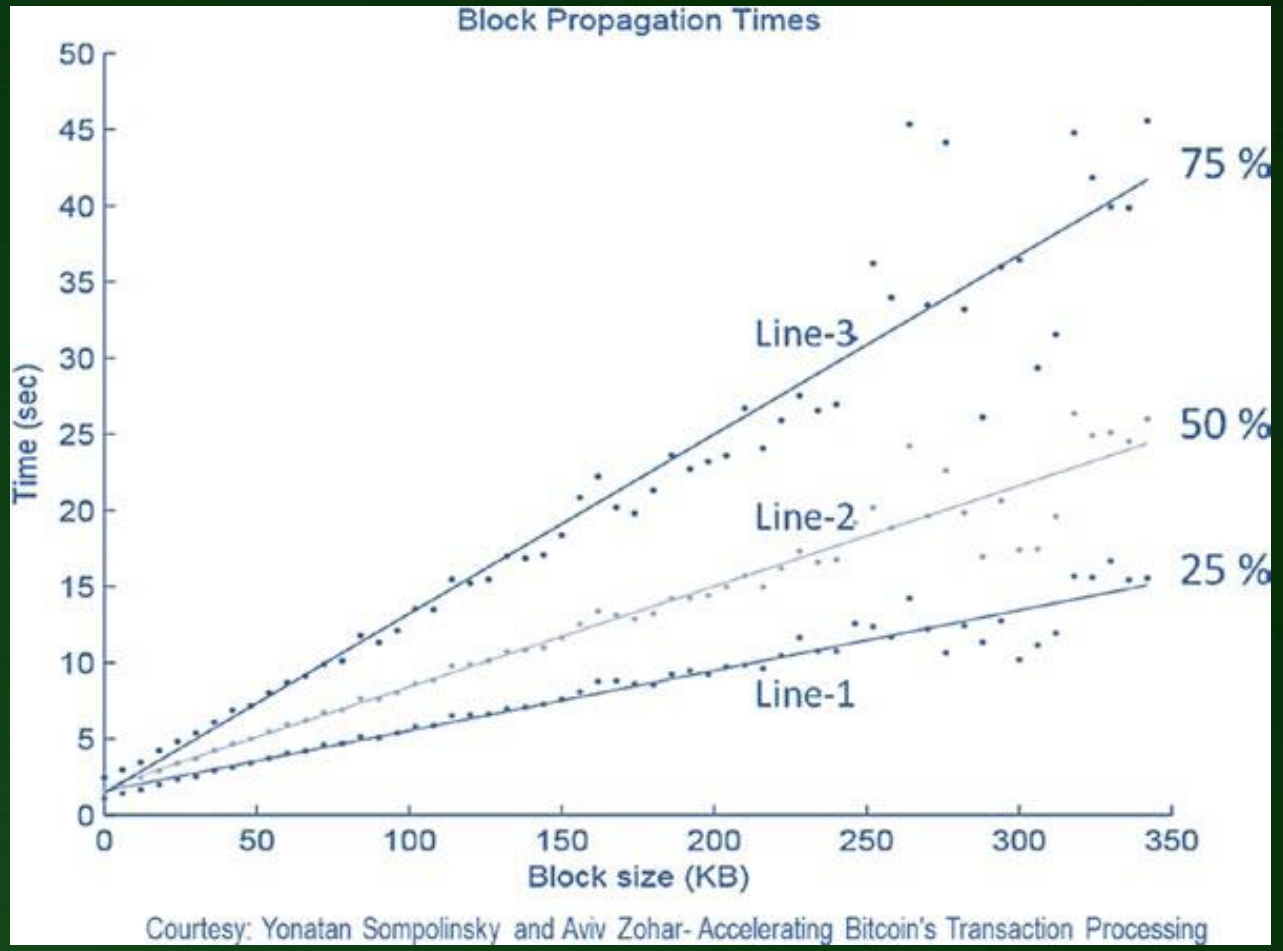
Διάδοση των Μπλοκ – (1)

- Η διάδοση των μπλοκ στο δίκτυο γίνεται όπως με τις συναλλαγές
  - Κάθε κόμβος που λαμβάνει ένα μπλοκ, ελέγχει αν είναι έγκυρο, με την εξής σειρά:
    1. έλεγχος nonce που δίνει hash μικρότερο του target
    2. έλεγχος κάθε μιας δοσοληψίας έναντι Merkle root

    αν όλες οι είναι έγκυρες, το προσθέτει στο τοπικό αντίγραφο της αλυσίδας
  - Εάν το μπλοκ είναι μέλος της μακρύτερης αλυσίδας (όπως φαίνεται σε αυτόν), το εκπέμπει παραπέρα

Διάδοση των Μπλοκ – (2)

- Όσο αυξάνει το μέγεθος του μπλοκ, αυξάνει και η καθυστέρηση
- Σχέση μεταξύ μεγέθους και χρόνου διάδοσης στο 25%, 50% και 75% των κόμβων:



Courtesy: Yonatan Sompolinsky and Aviv Zohar- Accelerating Bitcoin's Transaction Processing

Συνόψιση – (1)

- Όλες οι νέες συναλλαγές εκπέμπονται προς όλους τους κόμβους
- Κάθε κόμβος που λαμβάνει τις νέες συναλλαγές τις συλλέγει σε ένα μπλοκ
- Κάθε κόμβος-miner προσπαθεί να εκτελέσει ένα δύσκολο PoW για το νέο μπλοκ του και να το προτείνει στο δίκτυο

Συνόψιση – (2)

- Όποιος από τους κόμβους-miner σταθεί τυχερός στο να βρει ένα ορθό nonce για το PoW, εκπέμπει το μπλοκ σε όλους τους κόμβους
- Οι κόμβοι αποδέχονται το προτεινόμενο μπλοκ μόνον αν το nonce και όλες οι συναλλαγές είναι έγκυρες και δεν έχουν ξοδευτεί ήδη
- Οι κόμβοι εκφράζουν την αποδοχή του μπλοκ αυτού, με το να θεωρήσουν το Hash του ως αυτό του προηγούμενου μπλοκ για το επόμενο νέο μπλοκ που θα φτιάξουν

Περιεχόμενα

- Η Ιστορία του Χρήματος
- Bitcoin
  - Τρόπος Χρήσεως του BTC & Θέμα με Forks
  - Δομή Μπλοκ & Δένδρο Merkle
  - Στόχος Δυσκολίας & Genesis Block
  - Δίκτυο BTC
  - Συναλλαγές & Συναίνεση
  - Διάφορα θέματα

Script του BTC

- Ας εξετάσουμε τις συναλλαγές σε προγραμματιστικό επίπεδο, καθώς στην πράξη κάθε είσοδος και έξοδος συναλλαγής ενσωματώνεται σε script που
  - αποτιμώνται από αριστερά προς τα δεξιά
  - δεν είναι Turing-complete
  - δεν υποστηρίζουν την έννοια του βρόχου (loop), επομένως
    - έχουν χρόνο εκτέλεσης ανάλογο του πλήθους των συναλλαγών μόνο
    - σίγουρα τερματίζουν
  - εγχέονται μέσα στις συναλλαγές και εκτελούνται από τους miner
- Σκοπός των script είναι να μπορούν οι κόμβοι να επιβεβαιώνουν ότι τα διαθέσιμα κεφάλαια ξοδεύονται από τους πραγματικούς κατόχους τους

Επανεξέταση των Συναλλαγών BTC – (1)

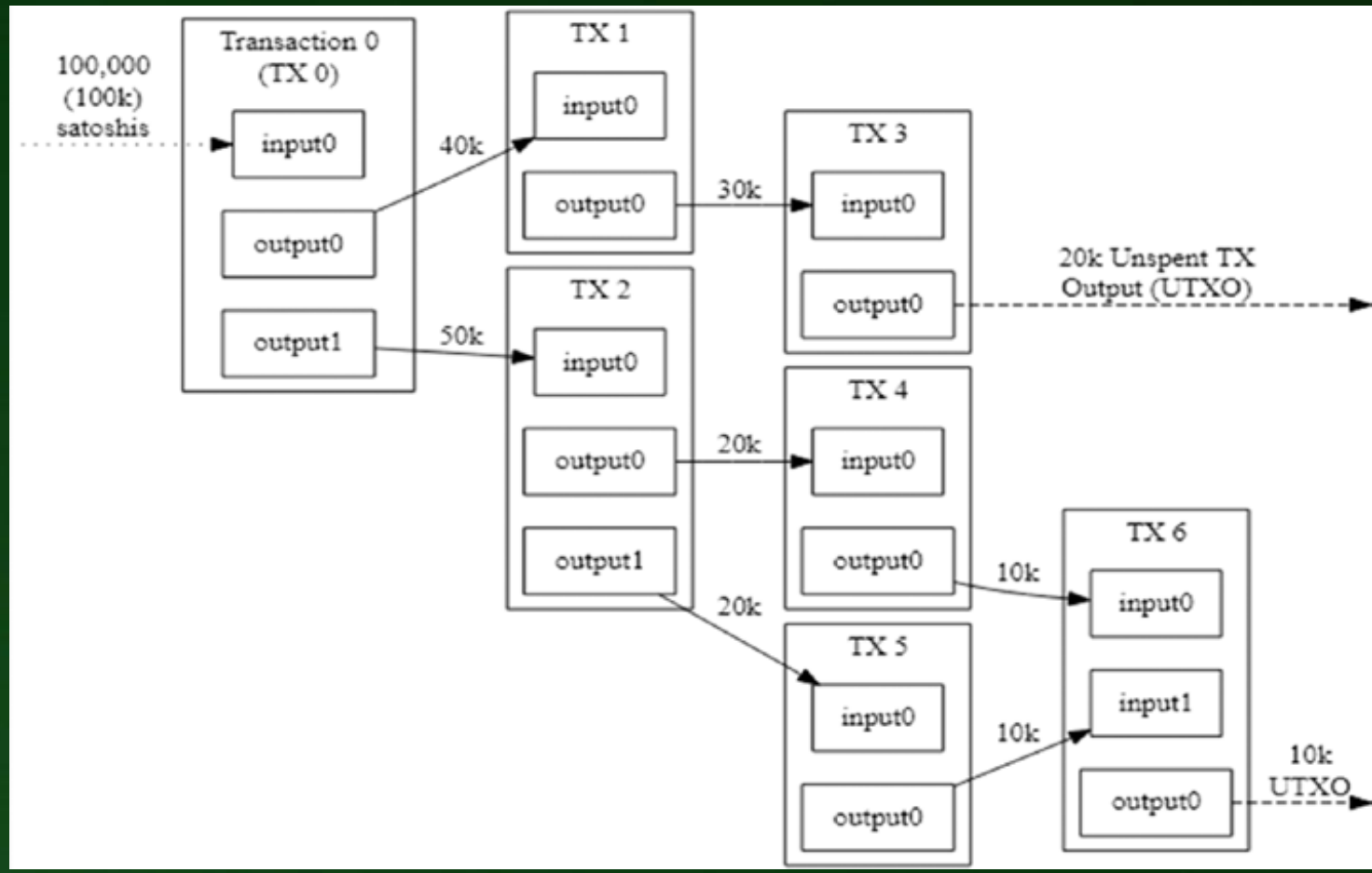
- Κάθε μεταφορά BTC φαίνεται να γίνεται από λογαριασμό/πορτοφόλι σε άλλο, αλλά στην πράξη είναι από μία συναλλαγή σε άλλη(ες)

- Μια διεύθυνση BTC προκύπτει με διπλό Hash του δημοσίου κλειδιού του συμμετέχοντος:
  - πρώτα με SHA256
  - μετά με RIPEMD160

  για τη δημιουργία διεύθυνσης BTC των 160 bit

Δομή Τυπικής Συναλλαγής BTC

- Η έξοδος προηγούμενης TX γίνεται είσοδος σε νέες συναλλαγές
- TX0: είσοδος 100K satoshi και έξοδοι (ξόδεμα) 90K
  - +10K για το fee του miner
- UTXO: το αξόδευτο υπόλοιπο
  - όταν μια συναλλαγή δεν γίνεται είσοδος σε μια νέα



Περιεχόμενο Συναλλαγών

- TX output = Μεταφερόμενο Ποσό + Output Script
- TX input = Αναφορά στο προηγ. TX output + Input Script

Output Script

- Το output script της τρέχουσας ΤΧ επιτρέπει στην επόμενη να το καταναλώσει ως είσοδο (από αριστερά προς τα δεξιά)
  - Για αυτό χρειάζεται να έχει το δημόσιο κλειδί του παραλήπτη και το μεταφερόμενο ποσό
- Όταν το output script γίνεται είσοδος στην επόμενη ΤΧ, κυρίως παρέχει έλεγχο της υπογραφής του παραλήπτη
  - Για αυτό είναι γνωστό και ως *ScriptPubKey*

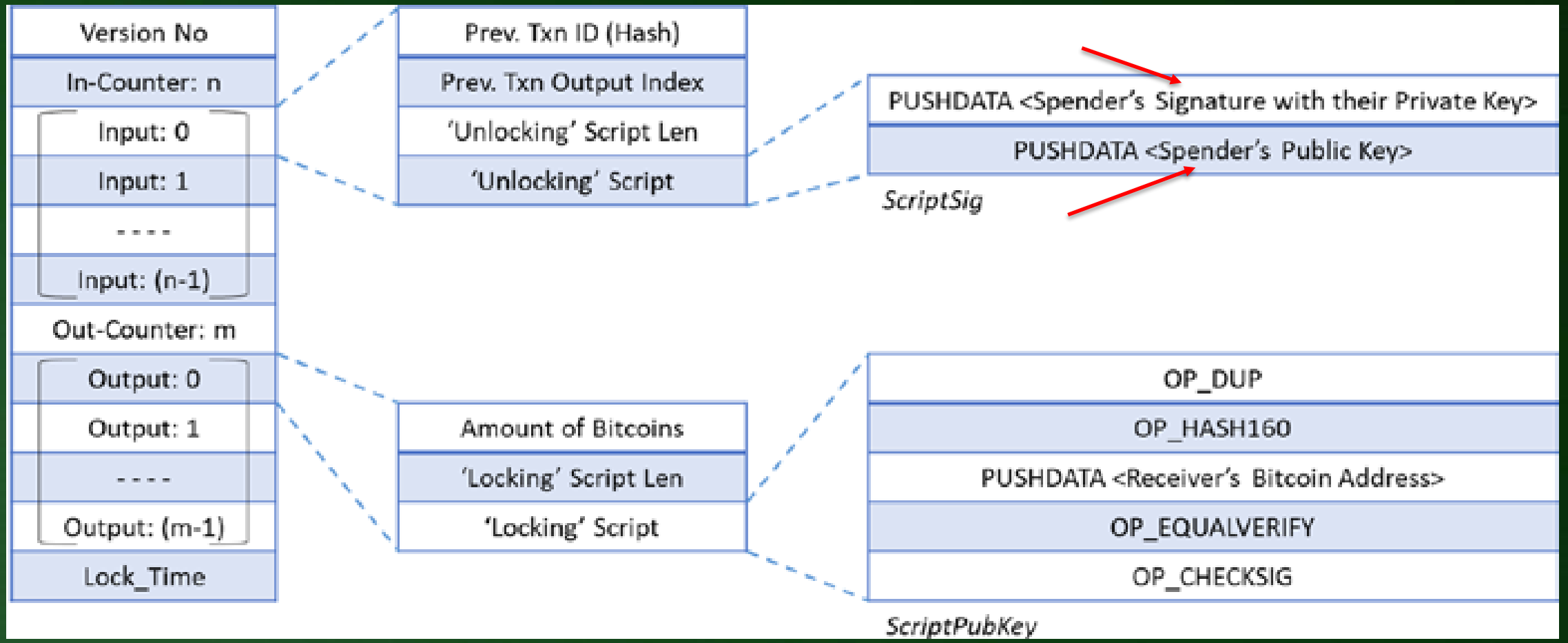
Input Script

- Το input script παρέχει το μηχανισμό κατανάλωσης της προηγ.ΤΧ
  - Για αυτό περιέχει την αναφορά στην προηγ.ΤΧ: {hash, index}
    - hash της προηγ.ΤΧ όπου έγινε η παραλαβή του ποσού για ξόδεμα
    - index για τον καθορισμό της σχετικής εξόδου της προηγ.ΤΧ
      - μπορεί να υπάρχουν πολλαπλοί παραλήπτες
- Ο παραλήπτης αξιώνει ότι είναι ο δικαιούχος του ποσού με την παρουσίαση της υπογραφής του και του δημοσίου κλειδιού του (το hash του είναι η διεύθυνση παραλήπτη της προηγ.ΤΧ)
  - Για αυτό είναι γνωστό και ως *ScriptSig* και κυρίως «σπρώχνει» υπογραφές και κλειδιά στο stack

Πεδία Τυπικής Συναλλαγής BTC

Πεδίο	Μέγεθος (σε byte)	Περιγραφή
Version No	4	Τώρα 1. Καθορίζει το σύνολο κανόνων που θα ακολουθήσουν οι κόμβοι για επικύρωση συναλλαγής
In-counter	1-9	Θετικός ακέραιος. Συνολικό πλήθος εισόδων
List of inputs	Μεταβλητό	Κατάλογος με όλες τις εισόδους της συναλλαγής
Out-counter	1-9	Θετικός ακέραιος. Συνολικό πλήθος εξόδων
List of outputs	Μεταβλητό	Κατάλογος με όλες τις εξόδους της συναλλαγής
Lock_time	4	Δεν χρησιμοποιείται προς το παρόν. Θα δηλώνει πιθανή καθυστέρηση πριν την ένταξη της ΤΧ σε μπλοκ

Με Μεγαλύτερη Λεπτομέρεια…



…βλέπουμε…

- Υπογραφές ή Δημόσια κλειδιά είναι ενσωματωμένα μέσα στα script και μέρος της συναλλαγής (βέλη)

- Η επιβεβαίωση της κάθε συναλλαγής που εκπέμπεται (από κάποιον κόμβο), ελέγχεται για εγκυρότητα από κάθε κόμβο ξεχωριστά
  - Συνδυάζει το output script της προηγούμενης συναλλαγής, με το input script της παρούσας

Πώς ακριβώς επικυρώνει την Συναλλαγή; – (1)

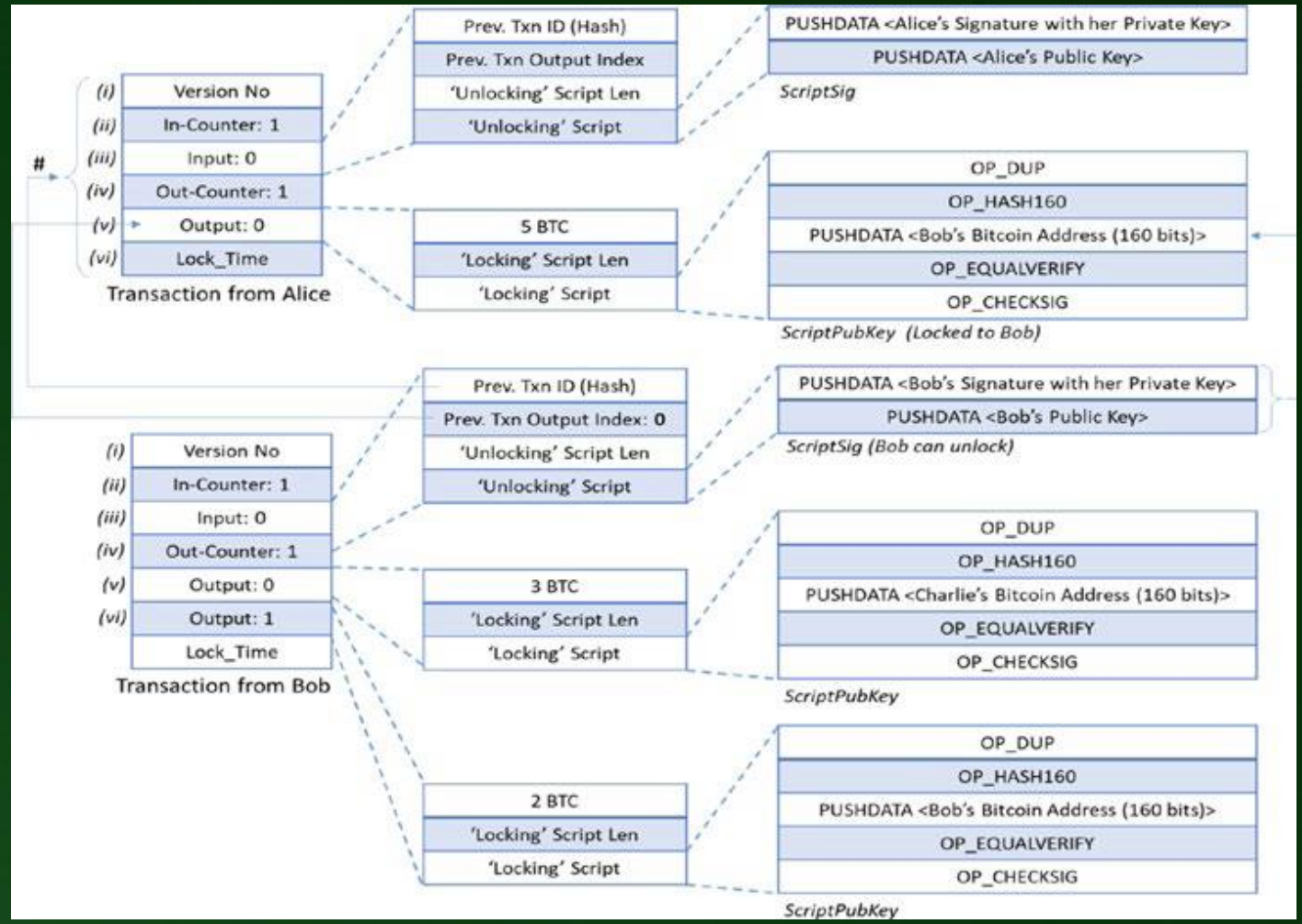
- Τα βήματα είναι (1ο μέρος):
  - Βρες την προηγούμενη συναλλαγή, η έξοδος της οποίας χρησιμοποιείται ως είσοδος για την τρέχουσα
    - Πεδίο: “Prev. Txn ID (Hash)”
  - Στην έξοδο της προηγούμενης συναλλαγής, βρες (μεταξύ διαφόρων) το ακριβές index όπου παρελήφθη το ποσό
    - Πεδίο: “Prev. Txn Output Index”
  - Κατανάλωσε το output script της προηγούμενης συναλλαγής χρησιμοποιώντας ως ‘Unlocking Script’ το “*ScriptSig*” (βλ. Με Μεγαλύτερη Λεπτομέρεια…)
    - πεδίο “‘Unlocking Script’ Length”
    - πεδίο “‘Unlocking’ Script”

Πώς ακριβώς επικυρώνει την Συναλλαγή; – (2)

- Τα βήματα είναι (2ο μέρος):
  - Ένωσε αυτό το output script με το input script, με απλό append, σχηματίζοντας το script επικύρωσης και εκτέλεσέ το
  - Το ποσό υπάρχει στο 'Locking script' ("ScriptPubKey") που κλειδώνει τις συνθήκες ξοδέματος και διασφαλίζεται ότι μόνον ο δικαιούχος της διεύθυνσης προς την οποίαν έγινε αυτή η συναλλαγή μπορεί κατόπιν να το διεκδικήσει (βλ. Με Μεγαλύτερη Λεπτομέρεια…)
  - Το script επικύρωσης (validation script) αποφασίζει εάν η είσοδος της τρέχουσας συναλλαγής έχει το δικαίωμα να ξοδέψει το προηγούμενο UTXO, επικυρώνοντας τις υπογραφές

Παράδειγμα

- Η Alice πήρε 5BTC σε μια προηγ.ΤΧ που κλειδώθηκε με ScriptPubKey.
- Η Alice αξιώνει δικαιοδοσία ξεκλειδώνοντάς την με ScriptSig και τα ξοδεύει:
  - Alice -> Bob (5 BTC)
- Ομοίως:
  - Bob -> Charlie (3 BTC)
  - Bob -> Bob (2 BTC)
    - στον εαυτό του, ως UTXO



Υπενθύμιση – (1)

- Το input script “ScriptSig” είναι το unlocking script και περιέχει 2 στοιχεία:
  - Δημόσιο Κλειδί
    - Το Hash του δίνει τη διεύθυνση προς την οποία ξοδεύθηκε η προηγούμενη συναλλαγή
  - Υπογραφή (ECDSA)
    - Η επιβεβαίωσή της αποδεικνύει ότι το Δημόσιο Κλειδί αντιστοιχεί στην παραπάνω διεύθυνση, ώστε να αξιωθεί τη δικαιοδοσία

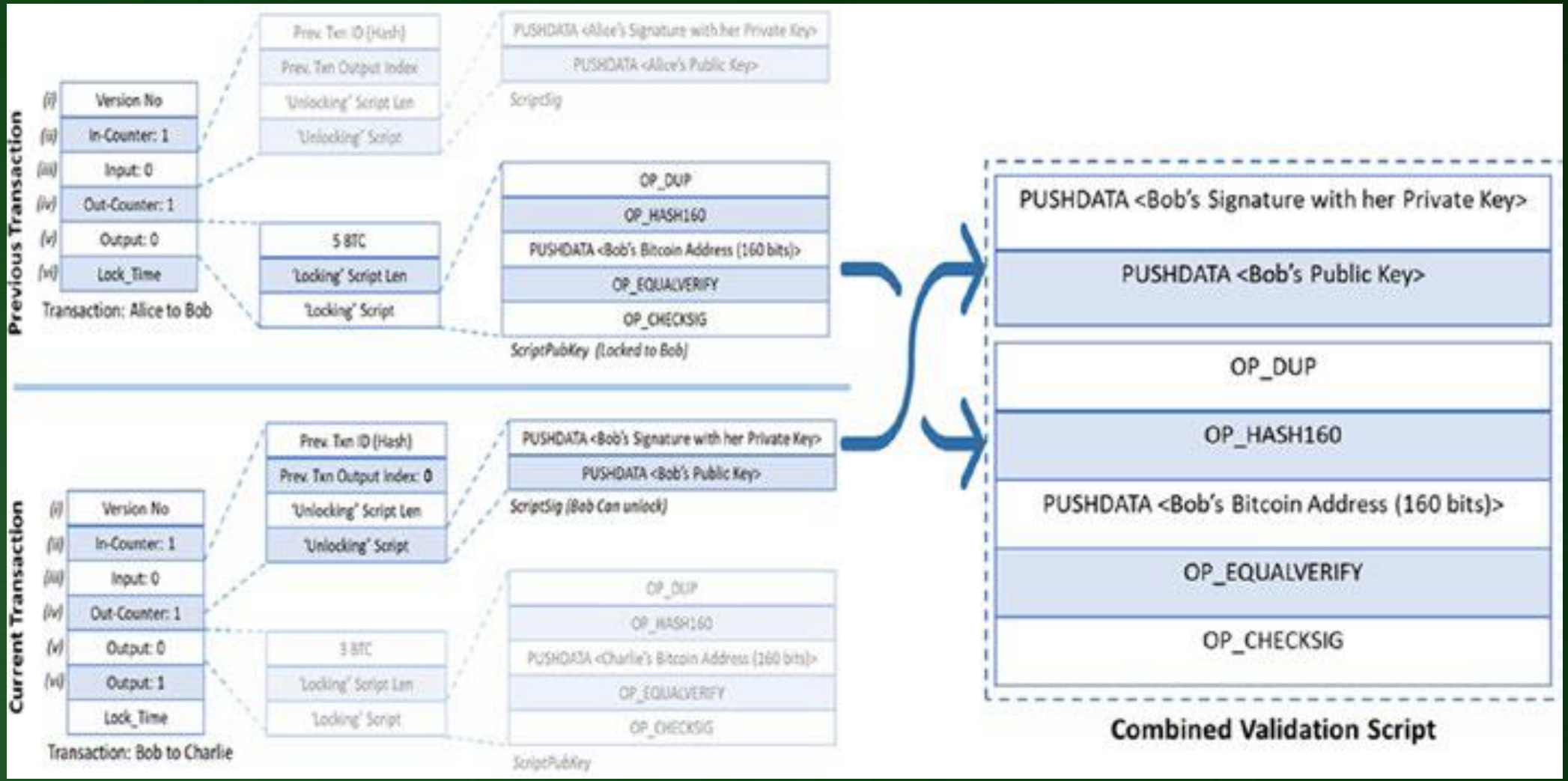
Υπενθύμιση – (2)

- Το output script “ScriptPubKey” της προηγ.συναλλαγής κλειδώνει την έξοδό της προς τον δικαιούχο της διεύθυνσης

- Αυτά τα 2 script output & input
  - το ScriptSig της τρέχουσας συναλλαγής και
  - το ScriptPubKey της προηγ. συναλλαγής

  συνδυάζονται και εκτελούνται:

Σχηματισμός του Ενιαίου Script Επικυρώσεως



Μερικά Χαρακτηριστικά Γλώσσας Script για BTC

- Ένα script BTC είτε τρέχει με επιτυχία, είτε αποτυγχάνει
- Είναι πολύ απλή γλώσσα με μόνον 256 εντολές
  - 15 είναι απενεργοποιημένες, 75 δεσμευμένες για μελλοντική χρήση
  - Βασικές: μαθηματικές, λογικές (if/then), αναφοράς σφαλμάτων, return
  - Επιπρόσθετες: κρυπτογραφικές (hashing, επαλήθευση υπογραφής, κ.ά)

Μερικά από τα διαθέσιμα Instruction Set

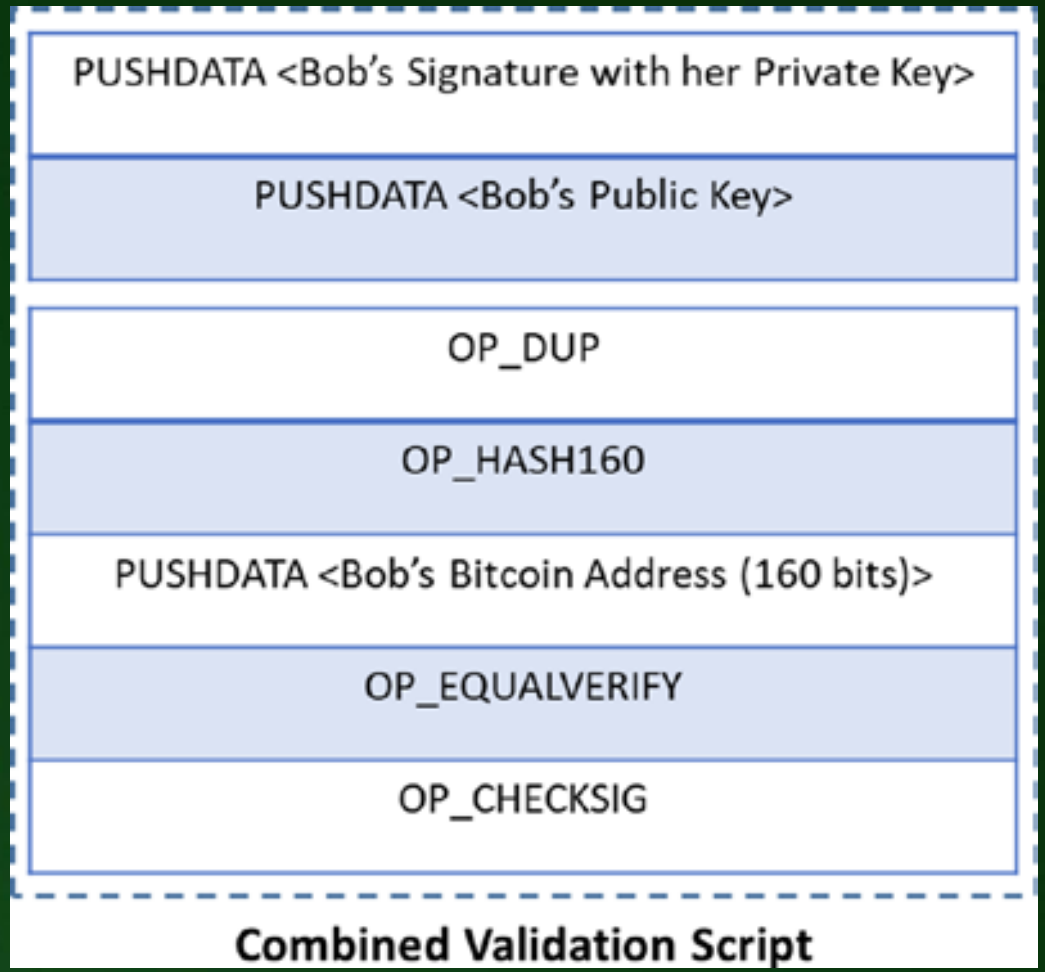
- OP_DUP
  - Δημιουργεί διπλότυπο του κορυφαίου αντικειμένου στη στοίβα
- OP_HASH160
  - Υπολογισμός hash, πρώτα με SHA256 και μετά με RIPEMD160
- OP_EQUALVERIFY
  - Αν οι είσοδοι ταιριάζουν δίνει TRUE, εάν όχι FALSE και μαρκάρει την συναλλαγή ως άκυρη
- OP_CHECKSIG
  - Ελέγχει εάν η υπογραφή εισόδου είναι έγκυρη χρησιμοποιώντας το Δημόσιο Κλειδί εισόδου για το Hash της τρέχουσας συναλλαγής

Πώς εκτελούνται οι Εντολές;

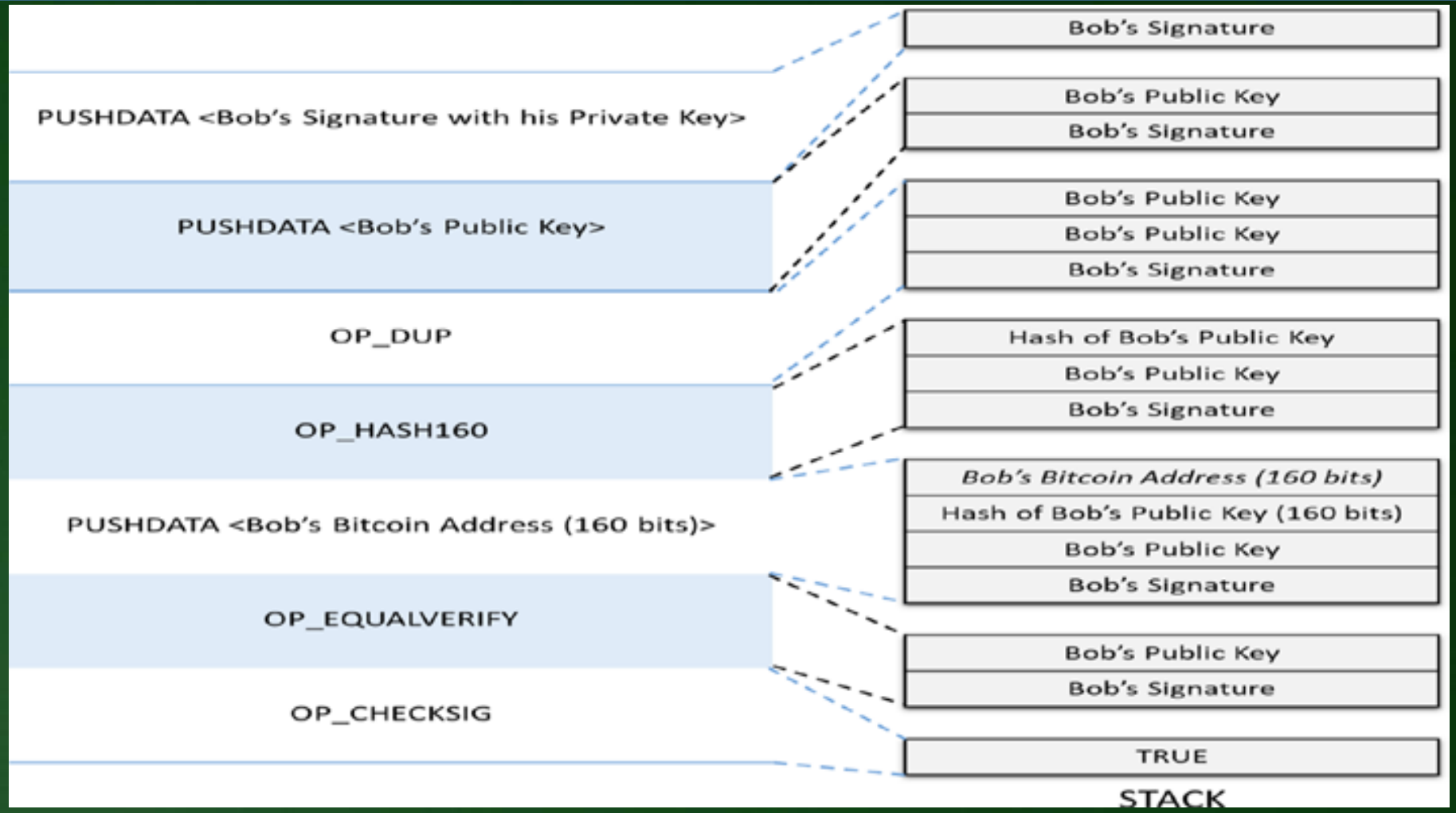
- Μόνο μνήμη για την στοίβα χρειάζεται
- Δύο είδη εντολών:
  - Data instruction (DI), για να σπρώχνουν δεδομένα στη στοίβα
  - Opcode (OP), για να εκτελούν λειτουργίες στα δεδομένα της στοίβας
- Ας δούμε ένα παράδειγμα για καλύτερη κατανόηση:

Παράδειγμα Συναλλαγής (Εντολές)

- Ο Bob προσπαθεί να ξοδέψει προς τον Charlie μια συναλλαγή που έλαβε πριν
  - συνδυασμός από *ScriptPubKey* και *ScriptSig:*



Ακολουθία Βημάτων του Script στην Στοίβα



Τα Βήματα Εκτελέσεως – (1)

1) DI: Σπρώχνει την υπογραφή του Bob στη στοίβα
2) DI: Σπρώχνει το Δημόσιο Κλειδί του Bob στη στοίβα
3) OP_DUP: Δημιουργεί διπλότυπο του Δημοσίου Κλειδιού του Bob στην κορυφή της στοίβας
4) OP_HUSH160: Υπολογίζει τα 160bit της διεύθυνσης του Bob (με SHA256 & RIPMED160 του Δημοσίου Κλειδιού του) και με αυτά αντικαθιστά το διπλότυπο του Δημοσίου Κλειδιού του στη στοίβα

Τα Βήματα Εκτελέσεως – (2)

5) DI: Σπρώχνει τη διεύθυνση του Bob στη στοίβα (160 bit)
6) OP_EQUALVERIFY: Ελέγχει τα δύο κορυφαία στοιχεία της στοίβας και αν ταιριάζουν αφαιρεί και τα δύο, διαφορετικά αναφέρει σφάλμα και τερματίζει το Script
7) OP_CHECKSIG: Ελέγχει το Δημόσιο Κλειδί με την υπογραφή του Bob για να επαληθεύσει την αυθεντικότητα του ιδιοκτήτη. Αν είναι OK, τα αφαιρεί από τη στοίβα

Λεπτομέρειες

- Εάν κάποιος προσπαθήσει να διοχετεύσει στη διαδικασία διαφορετικά script ή να καταχραστεί τα κανονικά, οι miners που περιμένουν συγκεκριμένα βήματα βάσει του προτύπου, θα το καταλάβουν και απλά θα απορρίπτουν τις συναλλαγές του

Πλήρεις Κόμβοι

- Θεμελιώδεις για την ύπαρξη του BTC
- Περιέχουν το πλήρες ιστορικό των συναλλαγών από την απαρχή του BTC και άρα είναι οι πλέον ασφαλείς
- Δεν στηρίζονται στο δίκτυο για επικύρωση των συναλλαγών, αφού έχουν διαθέσιμο το πλήρες ιστορικό,
- Χρειάζονται τα προτεινόμενα block ώστε (αφού αυτά επικυρωθούν) να ενημερώσουν το ιστορικό τους

Στην Πράξη…

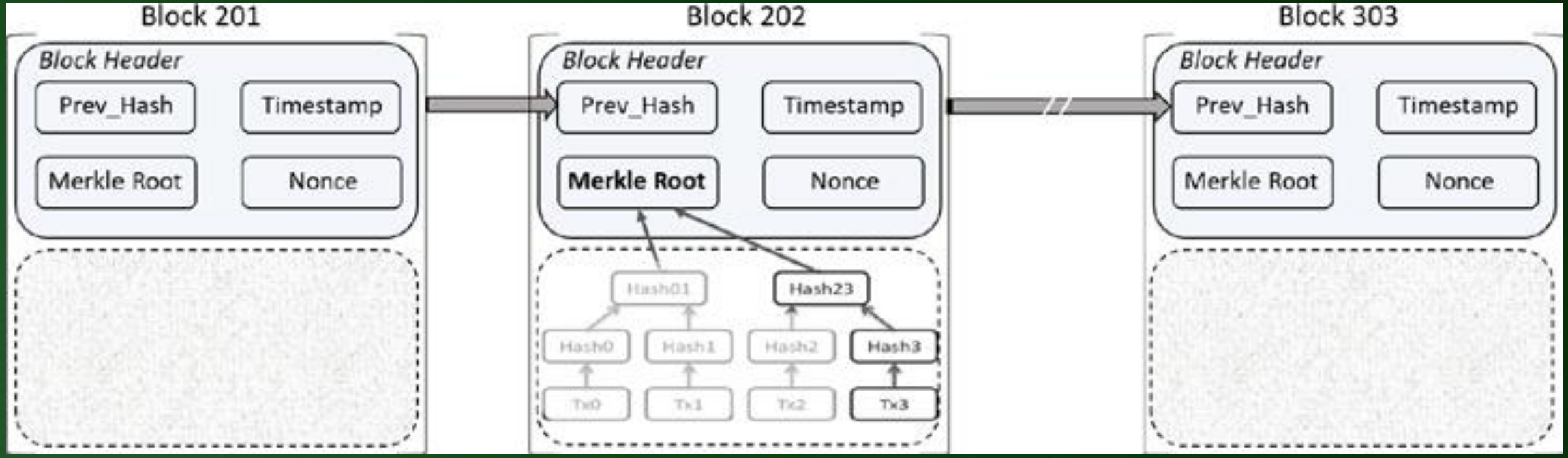
- Υπάρχουν παραλλαγές του λογισμικού BTC που χρησιμοποιούν οι πλήρεις κόμβοι

- Το μεγαλύτερο μέρος (πάνω από ¾) του δικτύου χρησιμοποιεί το λογισμικό “BTC Core”

Κόμβοι SPV (Simple Payment Verification)

- Επικυρώνουν συναλλαγές χωρίς να είναι πλήρεις κόμβοι:
  - Κατεβάζουν μόνον τις κεφαλίδες (80B) όλων των μπλοκ
    - Συνολικά μερικά MB μόνο
  - Αφού διαθέτουν τη ρίζα Merkle, ελέγχουν δύο πράγματα:
    - Αν η συναλλαγή ανήκει στο μπλοκ, από το δένδρο Merkle
    - Αν το παραπάνω μπλοκ είναι μέλος της κύριας αλυσίδας ή όχι
      - στην πράξη απαιτούνται τουλάχιστον 6 πρόσθετα μπλοκ για αυτό

Ρίζα Merkle στην Κεφαλίδα του Μπλοκ σε SPVs



Βήματα Κόμβων SPV – (1)

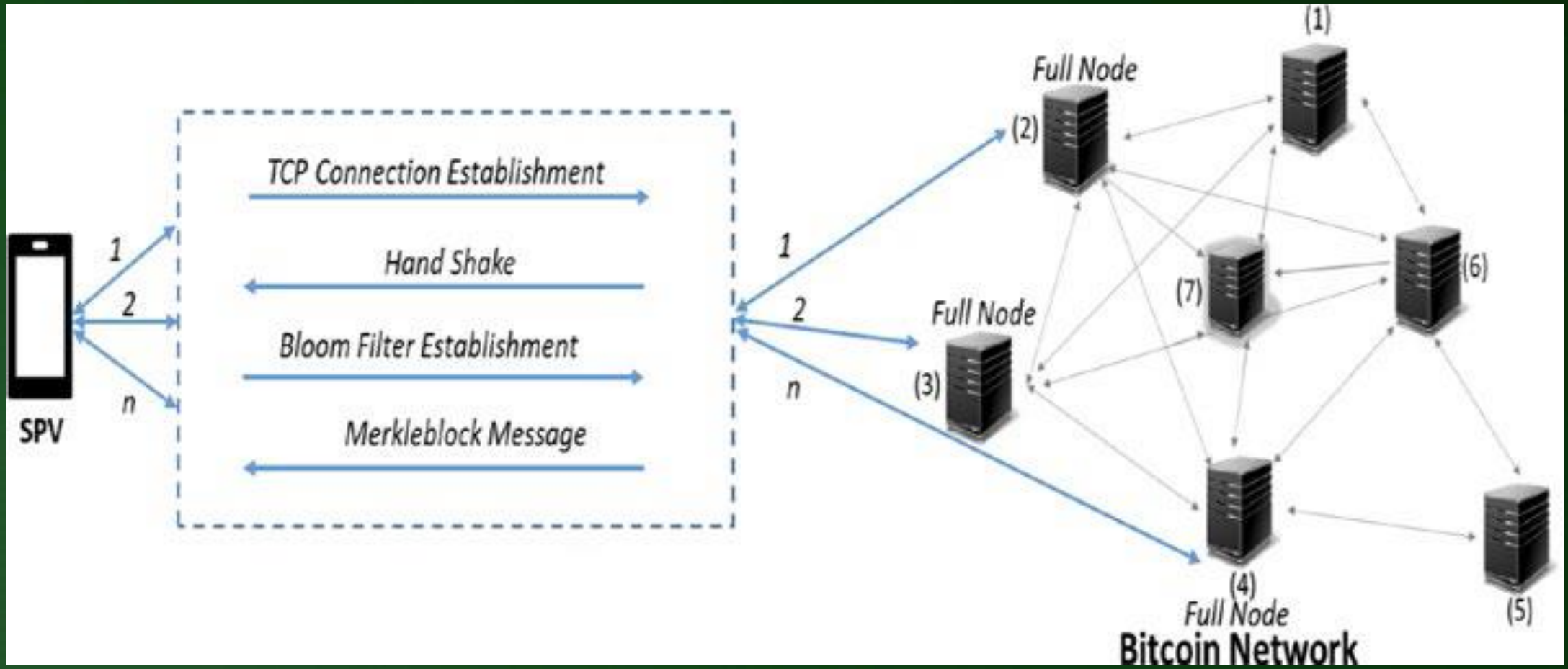
- Για κάθε ένα ομότιμο (peer) με τον οποίο συνδέεται ένας κόμβος SPV, δημιουργεί φίλτρο Bloom για τις συναλλαγές του ομότιμου (σύνδεση με πολλούς ομότιμους για αποφυγή εξαρτήσεων)
  - Φίλτρο Bloom: μικρός χώρος και γρήγορη αναζήτηση των συναλλαγών που ενδιαφέρουν αποκλειστικά τον κόμβο SPV
    - παρέχουν απόφαση για συμμετοχή σε σύνολο (set membership), με μικρή πιθανότητα για false positive (επιβεβαίωση με extra ελέγχους)
    - χωρίς να αποκαλύπτονται διευθύνσεις και κλειδιά ενδιαφέροντός του κόμβου SPV
- Οι ομότιμοι επιστρέφουν για κάθε σχετική συναλλαγή ένα μήνυμα merkleblock (λίγα KB) που περιέχει τη ρίζα και τη διαδρομή Merkle

Βήματα Κόμβων SPV – (2)

- Με τα παραπάνω, μπορεί ο κόμβος να επιβεβαιώσει αν μια συναλλαγή ανήκει σε μπλοκ της αλυσίδας

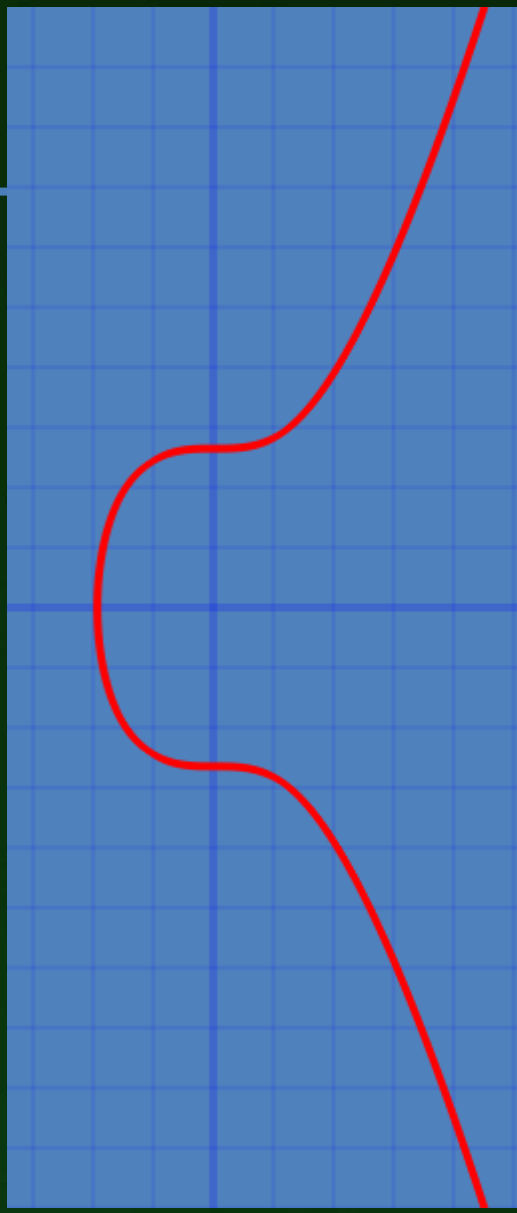
- Το επόμενο βήμα είναι να ελέγξει εάν το συγκεκριμένο μπλοκ είναι πραγματικά μέλος της πραγματικά μακρύτερης αλυσίδας

Βήματα Επικοινωνίας Κόμβου SPV με Ομότιμους



Πορτοφόλια BTC – (1)

- Αντιστοιχούν σε διευθύνσεις BTC
- Ο Bob αρχικά δημιουργεί ζεύγος κλειδιών
  - συνήθως με ECDSA και τύπο καμπύλης *secp256kl*
  - για ιδιωτικό κλειδί παράγεται μια τυχαία σειρά bit
    - συνήθως με hardware security module (HSM) για παραγωγή τυχαίων bit και προστασία ιδιωτικών κλειδιών
  - που μετασχηματίζεται ντετερμιστικά στο δημόσιο
    - άρα δεν χρειάζεται η αποθήκευση του δημοσίου

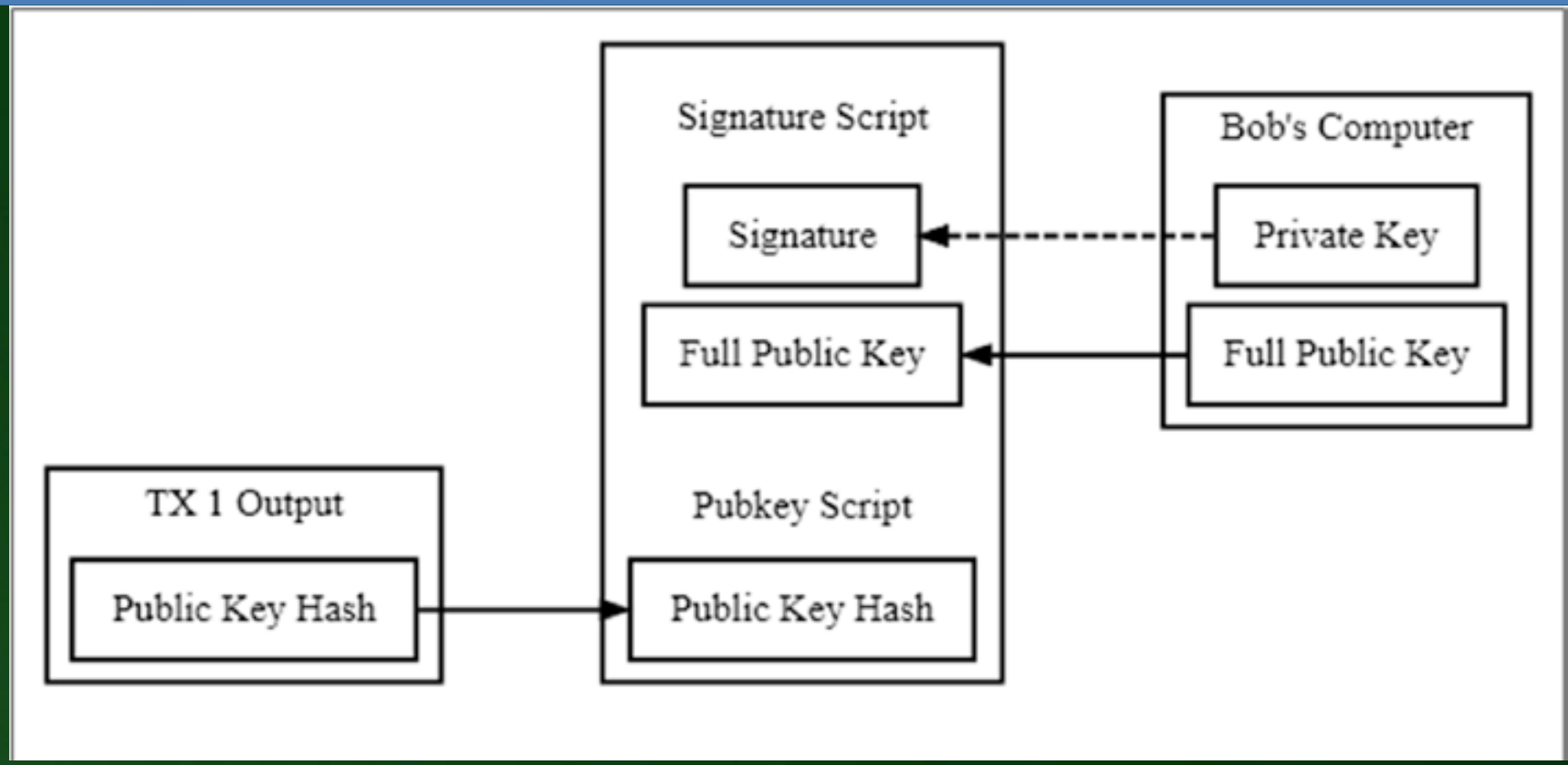


Πορτοφόλια BTC – (2)

- Ουσιαστικά, ένα πορτοφόλι BTC είναι ένας κόμβος SPV
- Χρειάζεται για να αποθηκεύει το Δημόσιο & το Ιδιωτικό Κλειδί
- Πιο ασφαλές να έχουμε ένα τουλάχιστο πορτοφόλι, συνδεδεμένο με έναν δικό μας Πλήρη Κόμβο
  - Διαφορετικά, κάθε ερώτημα από το πορτοφόλι μας προς κάποιον άλλον κόμβο (π.χ. για διεκδίκηση ποσού) θα περιέχει το Δημόσιο Κλειδί μας προκειμένου να πάρουμε τη λίστα των UTXO (πρόβλημα Ιδιωτικότητας)

Πορτοφόλια BTC – (3) Διεκδίκηση ποσού από BoB

Το δημόσιο κλειδί αποκαλύπτεται μόνο κατά τη διεκδίκηση του TX output



Πορτοφόλια BTC – (4)

- Μπορούμε να έχουμε πορτοφόλι-BTC με δικό μας λογισμικό σε υπηρεσία τρίτων (wallet-service provider)
  - Πρόβλημα: θα έχουν πρόσβαση στο Ιδιωτικό μας κλειδί (αφού αποθηκεύεται στο πορτοφόλι)
    - Είτε οι ίδιοι, είτε κάποιοι εισβολείς μπορούν να μας κλέψουν
- SPV Client: λογισμικό "BitcoinJ" για thin node
    - Βιβλιοθήκη για χρήση πρωτοκόλλου Bitcoin, διαχείριση πορτοφολιού, έναρξη/επικύρωση συναλλαγών
    - υλοποίηση σε Java, μπορεί να χρησιμοποιηθεί από JavaScript & Python

Διάδραση Πορτοφολιού BTC με Δίκτυο BTC