

Εισαγωγή στην Τεχνολογία Blockchain

Καθηγητής Δρ. Πάνος Φιτσιλής





Στόχοι του κεφαλαίου 9

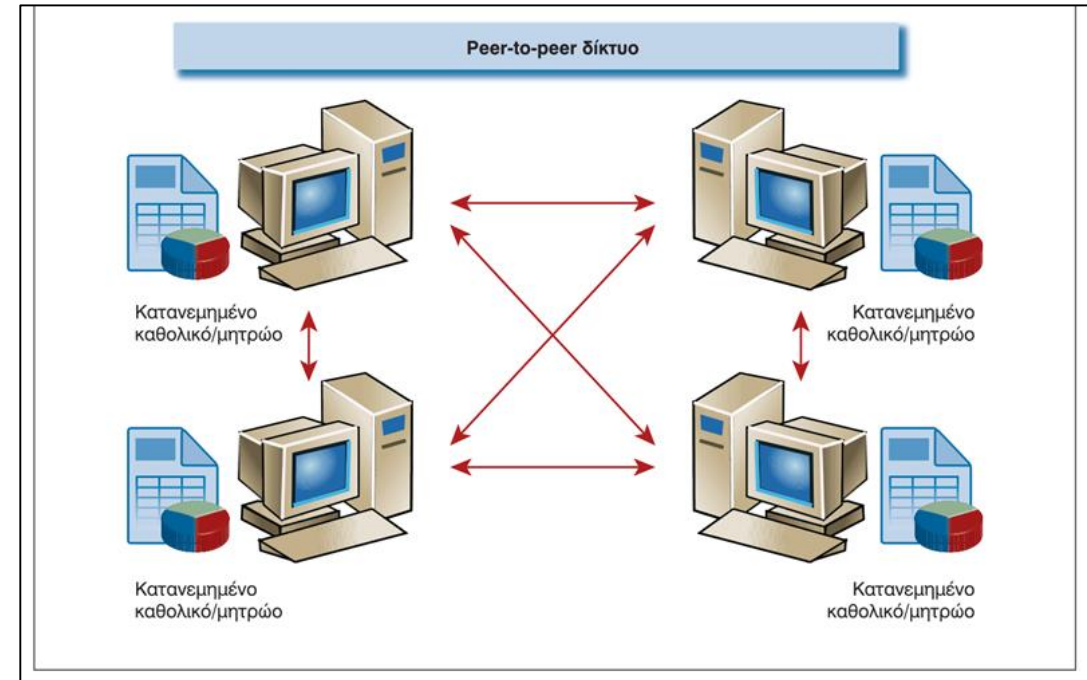
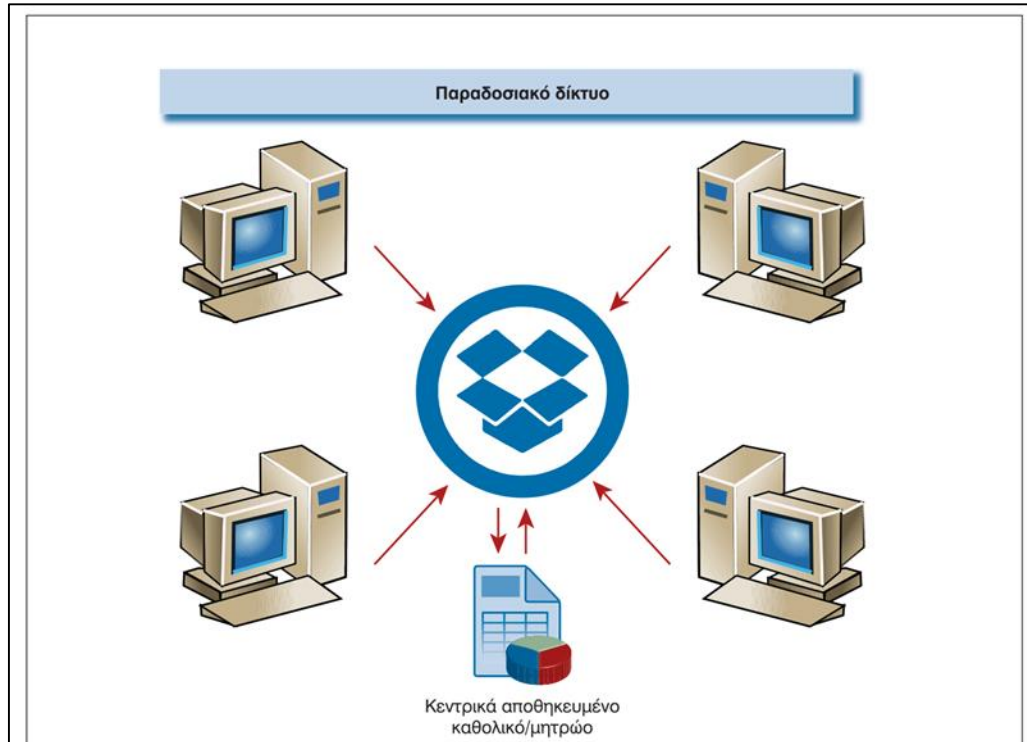
- Αφού θα έχετε ολοκληρώσει τη μελέτη αυτού του κεφαλαίου θα μπορείτε:
 - Να κατανοήσετε τον τρόπο λειτουργίας του blockchain.
 - Να κατανοήσετε τον τρόπο λειτουργίας του δικτύου bitcoin.
 - Να κατανοήσετε, σε τεχνικό επίπεδο, τις πολιτικές συναίνεσης, τη συνάρτηση κατακερματισμού, τη ρίζα και το δέντρο Merkle.
 - Να κατανοήσετε τη δομή και τον τρόπο λειτουργίας των συναλλαγών σε ένα δίκτυο block-chain.
 - Να κατανοήσετε τη λειτουργία των έξυπνων συμβάσεων και του συστήματος Ethereum.
 - Να γνωρίζετε τις εφαρμογές της τεχνολογίας blockchain



Η δημιουργία του blockchain

Το 2008, ένα άτομο ή ενδεχομένως μια ομάδα ατόμων με το όνομα *Satoshi Nakamoto* (Nakamoto, 2008) δημοσίευσε ένα άρθρο με τίτλο «*Bitcoin: A Peer-To-Peer Electronic Cash System*». Στο άρθρο αυτό περιγράφεται η λειτουργία ενός ηλεκτρονικού κρυπτονομίσματος με το όνομα *Bitcoin*, το οποίο θα επέτρεπε την απευθείας διενέργεια πληρωμών στο διαδίκτυο χωρίς να διαμεσολαβεί ένα χρηματοπιστωτικό ίδρυμα (π.χ. μια τράπεζα).

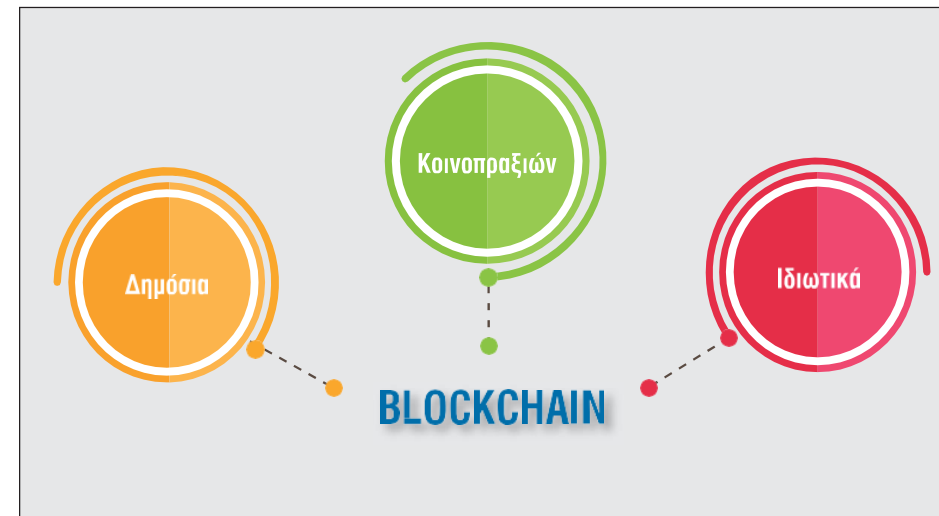






Είδη blockchain

- Ένα **δημόσιο blockchain** είναι ανοικτό σε όλους, όπου όλοι μπορούν να έχουν πρόσβαση και να συναλλάσσονται σε αυτό. Στο δημόσιο blockchain, οι συναλλαγές συμπεριλαμβάνονται στην αλυσίδα μόνο εάν είναι έγκυρες, ενώ όλοι οι χρήστες συμμετέχουν στη διαδικασία συναίνεσης
- Το **blockchain κοινοπραξιών** όπου η διαδικασία συναίνεσης ελέγχεται από ένα προεπιλεγμένο σύνολο κόμβων
- Το **ιδιωτικό blockchain (private blockchain)** όπου τα δικαιώματα εγγραφής ελέγχονται κεντρικά από έναν οργανισμό.

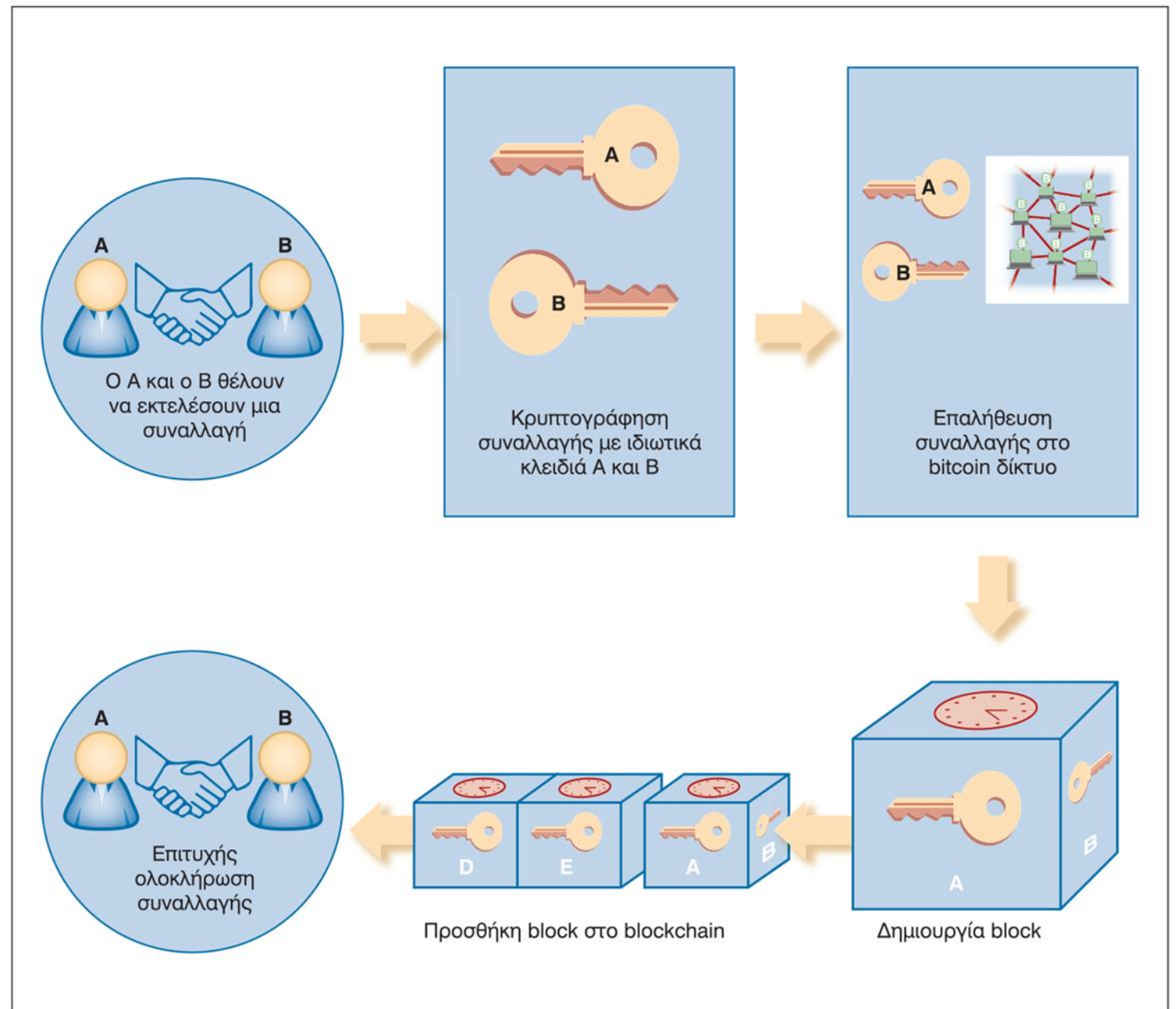




Πλεονεκτήματα της τεχνολογίας blockchain

- Τα πλεονεκτήματα της τεχνολογίας blockchain είναι τα ακόλουθα:
 - Εμπιστοσύνη χωρίς την ύπαρξη διαμεσολαβητή.
 - Ο ρόλος των χρηστών είναι αναβαθμισμένος αφού έχουν τον πλήρη έλεγχο των πληροφοριών και των συναλλαγών.
 - Τα δεδομένα είναι υψηλής ποιότητας.
 - Είναι σύστημα υψηλής αξιοπιστίας και ανοχής σε σφάλματα.
 - Υπάρχει ακεραιότητα των διαδικασιών.
 - Υπάρχει διαφάνεια και μονιμότητα των δεδομένων.
 - Απλοποίηση των οικοσυστημάτων.
 - Ταχύτερες συναλλαγές.
 - Μικρότερο κόστος συναλλαγών.

Τρόπος λειτουργίας του blockchain

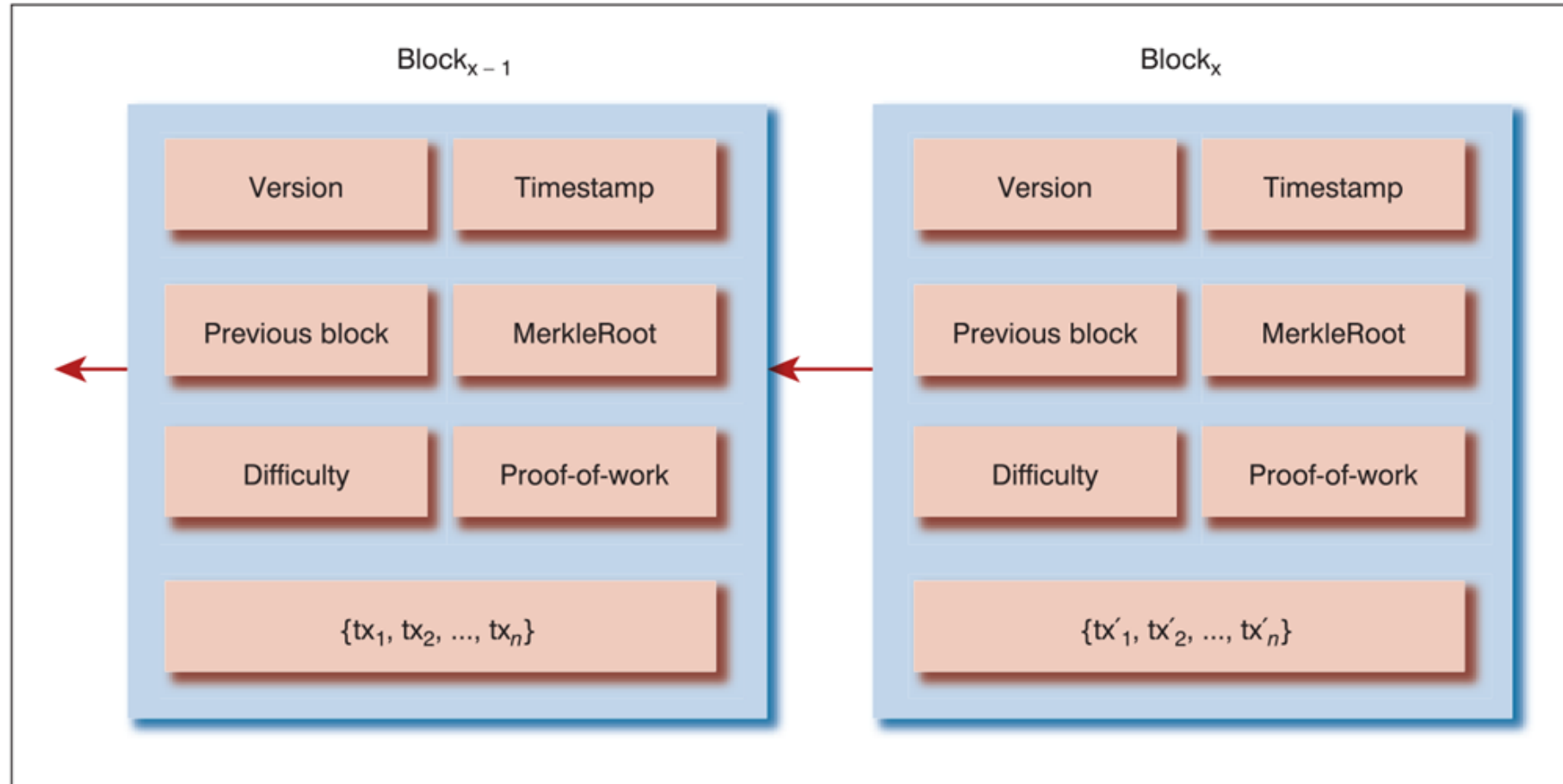


ΕΙΚΟΝΑ 10.2

Η δημιουργία του blockchain.



Η δομή του block



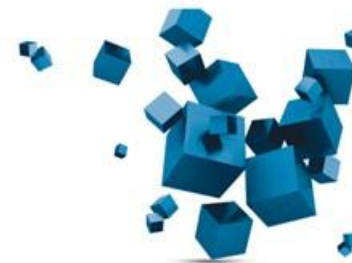
EIKONA 10.3

Η δομή του block.



Ένας εξερευνητής block

- Ένας εξερευνητής block χρησιμοποιείται για τις ακόλουθες λειτουργίες:
 - την παρακολούθηση της ροής των block και των συναλλαγών,
 - την προβολή του ιστορικού των συναλλαγών μιας δεδομένης διεύθυνσης,
 - την προβολή των δεδομένων εισόδου και εξόδου των συναλλαγών,
 - τον έλεγχο της κατάστασης του mempool, και
 - την προβολή του αρχικού block (genesis block).

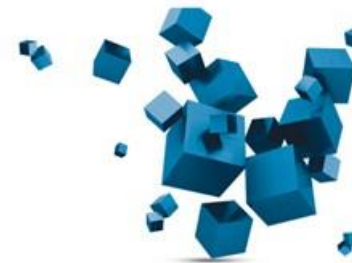


Παράδειγμα εξερευνητή

BLOCKCHAIN						
WALLET DATA API ABOUT						
LATEST BLOCKS						
SEE MORE						
Height	Age	Transactions	Total Sent	Relayed By	Size (kB)	Weight (kWU)
541496	2 minutes	1	12.50 BTC	58COIN	0.28	0.77
541495	2 minutes	1960	1,864.23 BTC	BTC.com	832.02	2,885.38
541494	3 minutes	2541	21,295.55 BTC	Unknown	1,230.61	3,992.97
541493	40 minutes	816	2,962.32 BTC	BTC.com	487.11	1,668.98

ΕΙΚΟΝΑ 10.4

Ο εξερευνητής Blockchain.info (πηγή <https://www.blockchain.com>).



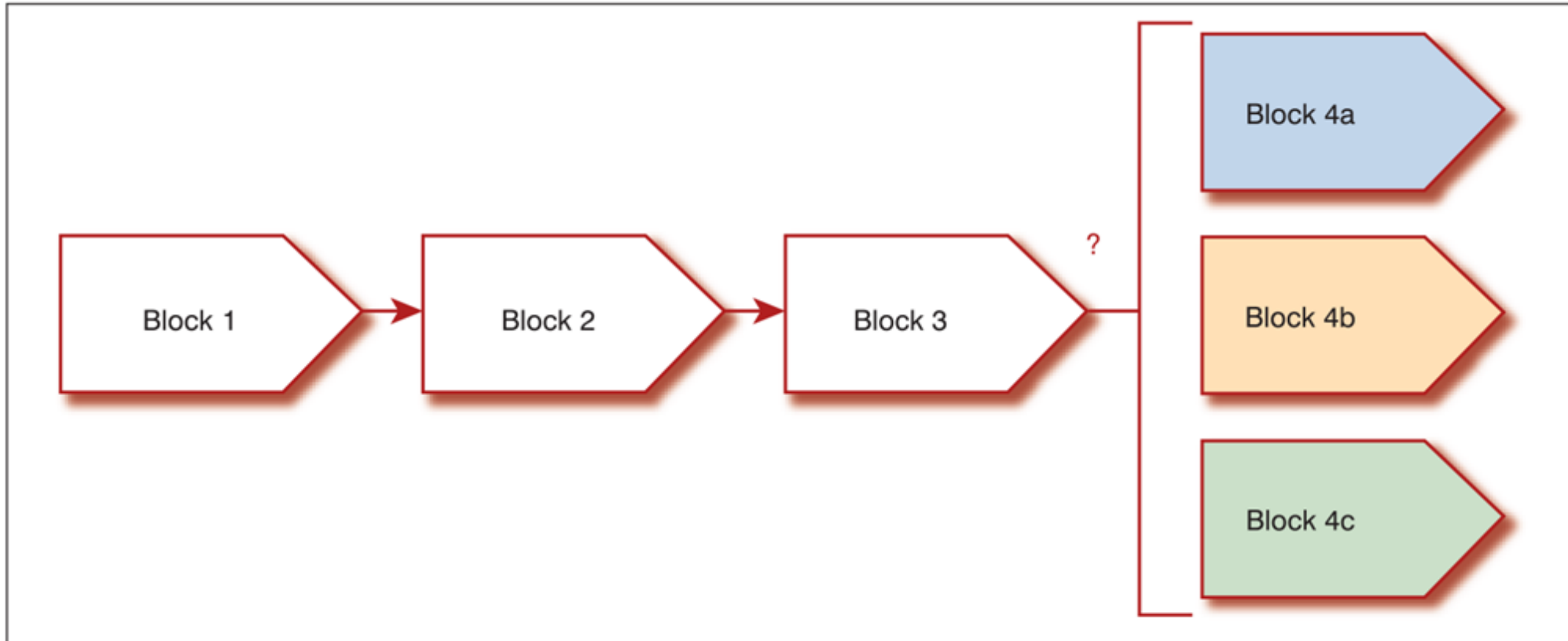
Πολιτικές συναίνεσης

- Τα blocks δεν είναι διατεταγμένα, εισάγει το πρόβλημα της διατήρησης της σειράς αυτών των συναλλαγών που μεταδίδονται σε άλλους κόμβους του peer-to-peer δικτύου.
- Οι συγκρούσεις επιλύονται με τη χρήση του κανόνα που ονομάζεται "κανόνας μακρύτερης αλυσίδας" (longest chain rule). Οι κόμβοι του δικτύου επιλέγουν το block που περιέχει την περισσότερη "εργασία" (όπου ως εργασία ορίζεται το άθροισμα των πεδίων δυσκολίας – difficulty των block του blockchain).





Επιλογή επόμενου block

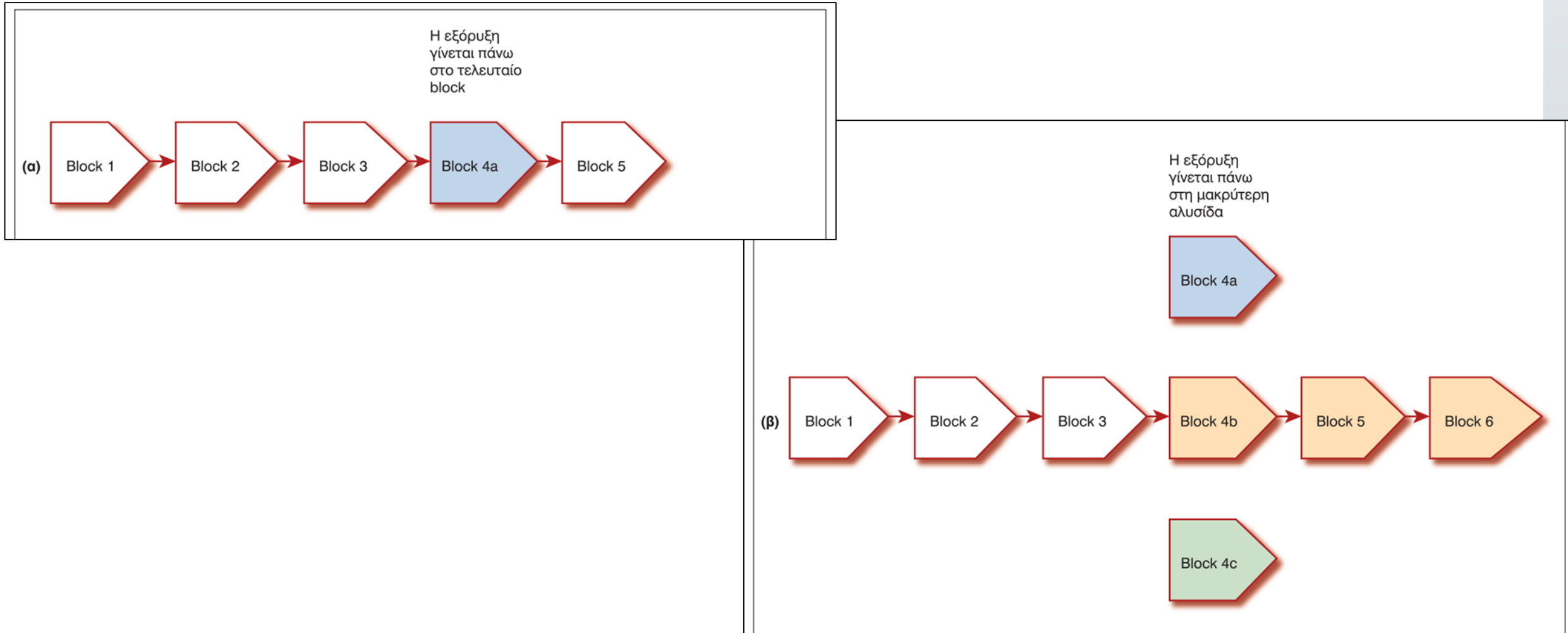


ΕΙΚΟΝΑ 10.6

Επιλογή επόμενου block.

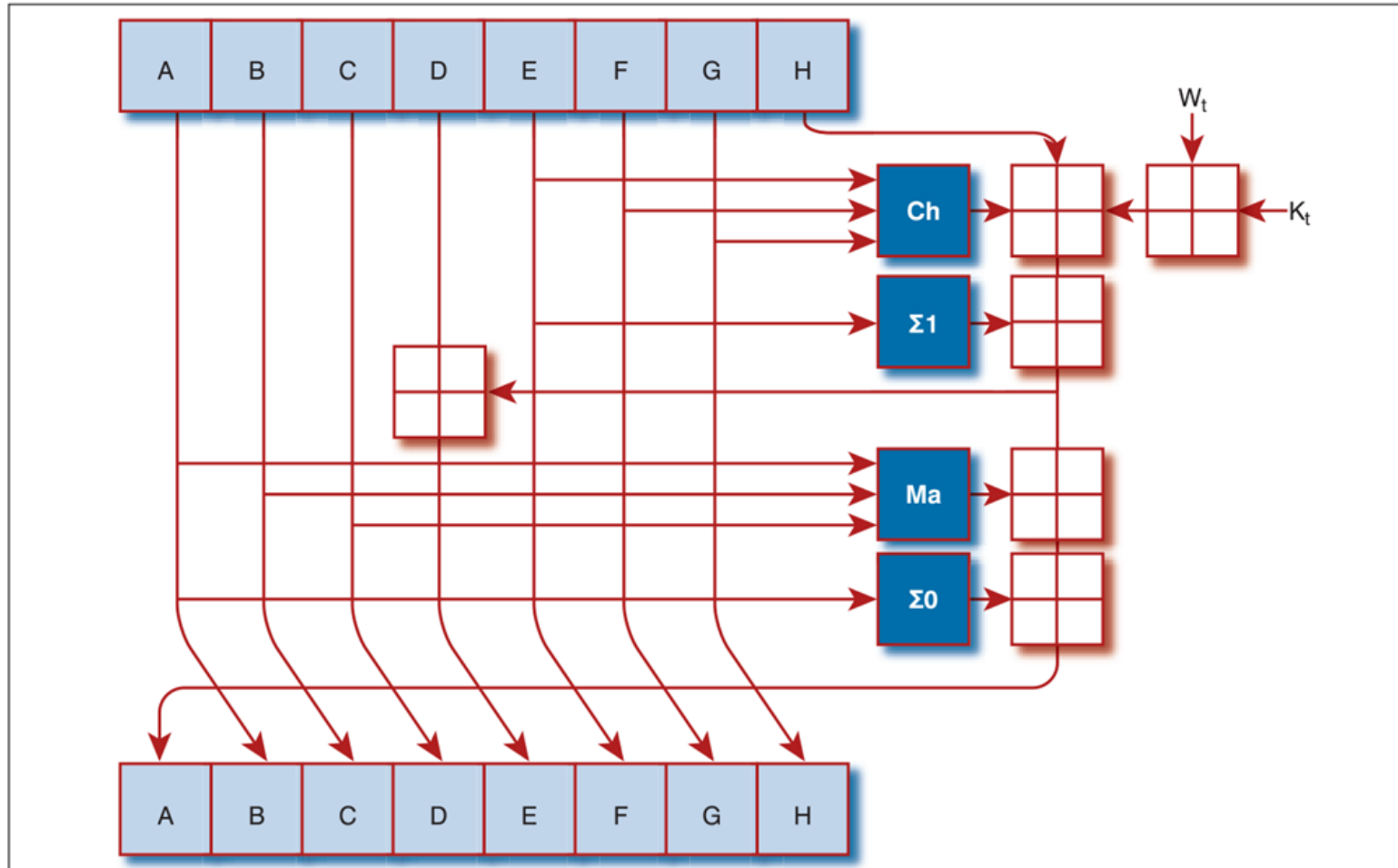


Αναδιοργάνωση των block στη λογική της μακρύτερης αλυσίδας





Η συνάρτηση κερματισμού



EIKONA 10.8

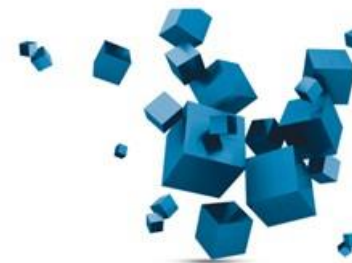
Η λειτουργία της hash συνάρτησης SHA-256 σε μια επανάληψη (πηγή <http://en.wikipedia.org>).

Ο αριθμός των εκτιμώμενων κατακερματισμών σε TH/sec



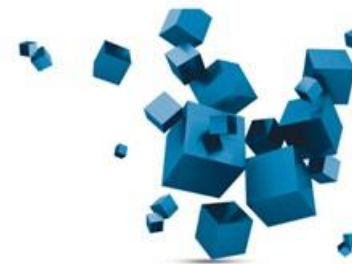
ΕΙΚΟΝΑ 10.9

Ο αριθμός των εκτιμώμενων κατακερματισμών σε TH/sec (πηγή www.blockchain.com).

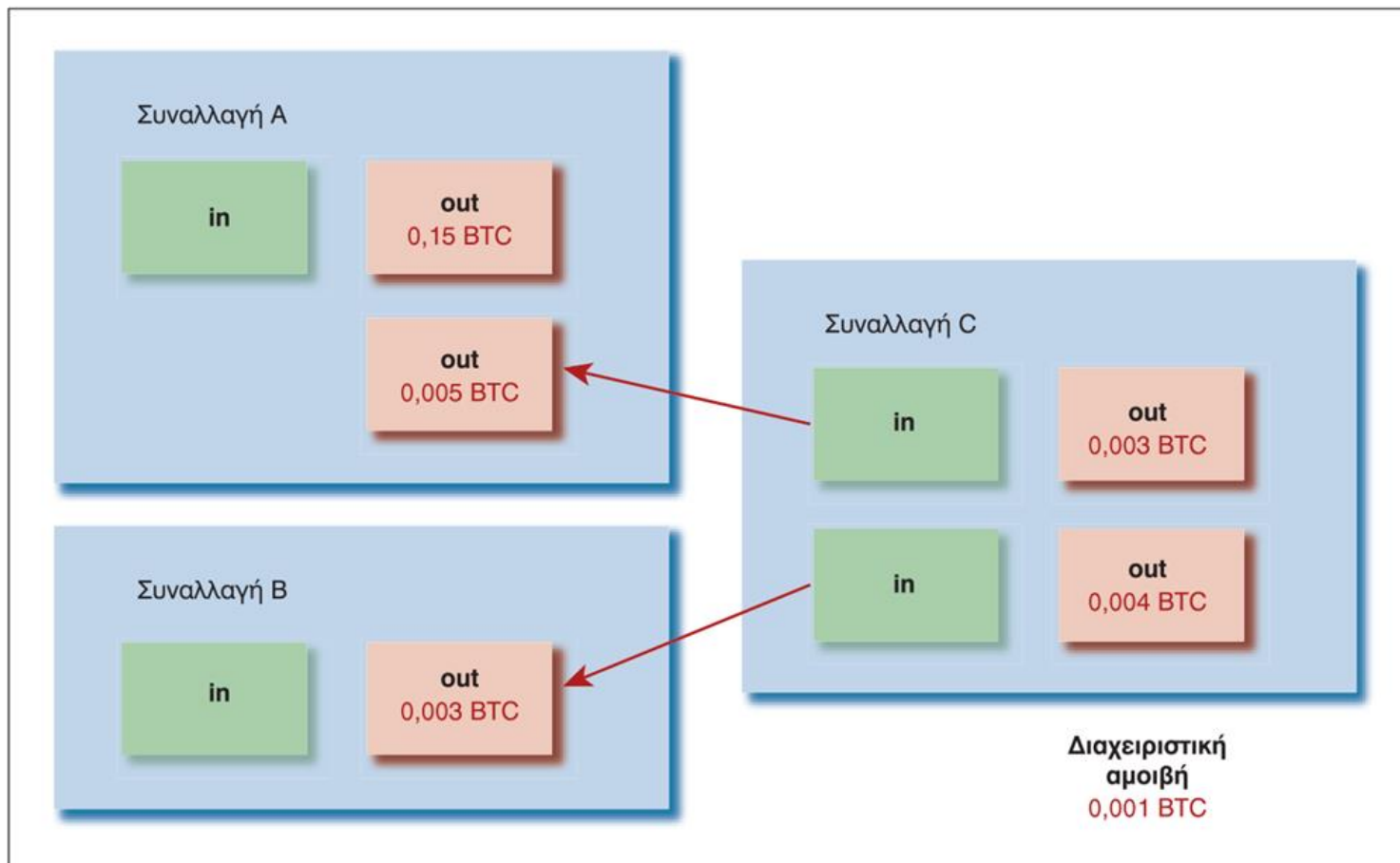


Οικονομικά στοιχεία

Η τρέχουσα εκτιμώμενη ετήσια κατανάλωση ηλεκτρικής ενέργειας του Bitcoin (TWh)	73,12
Η τρέχουσα ελάχιστη ετήσια κατανάλωση ηλεκτρικής ενέργειας του Bitcoin (TWh)	57,43
Ετήσια παγκόσμια έσοδα προερχόμενα από την εξόρυξη	\$4.839.148.964
Ετήσιο εκτιμώμενο συνολικό κόστος εξόρυξης	\$3.656.073.069
Το ποσοστό κόστους εξόρυξης ως προς τα έσοδα	75,55%
Χώρα με την μεγαλύτερη ως ποσοστό κατανάλωση ηλεκτρικής ενέργειας στο Bitcoin	Αυστρία
Εκτιμώμενη ηλεκτρική ενέργεια που χρησιμοποιήθηκε κατά την προηγούμενη ημέρα (KWh)	200.332.771
Εκτιμώμενα Watts ανά GH/s	0,147
Συνολικό Hashrate δικτύου σε PH/s (1.000.000 GH/s)	56,865
Ηλεκτρική ενέργεια που καταναλώνεται ανά συναλλαγή (KWh)	893
Αριθμός νοικοκυριών των ΗΠΑ που θα μπορούσαν να τροφοδοτηθούν αντί για το Bitcoin	6.770.506
Αριθμός νοικοκυριών των ΗΠΑ που θα μπορούσαν να τροφοδοτηθούν για μία ημέρα από την ηλεκτρική ενέργεια που καταναλώνεται για μία μόνο συναλλαγή	30,18
Η κατανάλωση ηλεκτρικής ενέργειας του Bitcoin ως ποσοστό της παγκόσμιας κατανάλωσης ηλεκτρικής ενέργειας	0,33%
Το ετήσιο αποτύπωμα άνθρακα (kt CO ₂)	35.830
Αποτύπωμα άνθρακα ανά συναλλαγή (kg CO ₂)	437,5
Πηγή: https://digiconomist.net/bitcoin-energy-consumption .	

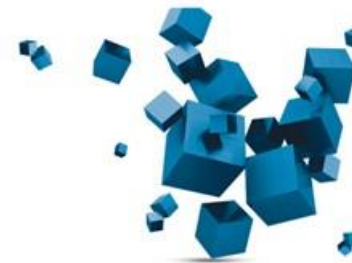


Ο τρόπος εκτέλεσης των συναλλαγών στο δίκτυο Bitcoin



ΕΙΚΟΝΑ 10.12

Ο τρόπος εκτέλεσης των συναλλαγών στο δίκτυο Bitcoin.



Ο τρόπος εκτέλεσης των συναλλαγών στο δίκτυο Bitcoin

```
{
  "hash": "90b18aa54288ec610d83ff1abe90f10d8ca87fb6411a72b2e56a169fdc9b0219",
  "ver": 1,
  "vin_sz": 1,
  "vout_sz": 2,
  "lock_time": 0,
  "size": 226,
  "in": [
    {
      "prev_out": {
        "hash": "18798F8795ded46c3086f48d5bdabe10e1755524b43912320b81ef547b2f939a",
        "n": 0
      },
      "scriptSig": "3045022100c1efcad5cdcc0dcf7c2a79d9e1566523af9c7229c78ef71ee8b6300ab...[snip]"
    }
  ],
  "out": [
    {
      "value": "5.93100000",
      "scriptPubKey": "OP_DUP OP_HASH160 4b358739fc7984b8101278988beba0cc00867adc OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value": "1678.06900000",
      "scriptPubKey": "OP_DUP OP_HASH160 55368b388ccfe22a3f837c9eee93d053460db339 OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```

EIKONA 10.13

Ο τρόπος εκτέλεσης των συναλλαγών στο δίκτυο Bitcoin.

Προβολή συναλλαγής με τον εξερευνητή



Συναλλαγή Προβολή πληροφοριών σχετικά με μια συναλλαγή Bitcoin

1460bba5092528ba401d06b5bacb6ef8b892e9c93612f092c1219b2f1bf4fff5

17A16QmavnUfCW11DAApiJxp7ARnxN5pGX

16rBbGBhUWba8cBQ8tWQxdiCm8jzDNqL5B
1CEifGC35gH9QCFFgCG8HvprZd2h51vjGp
3CMGm9sAgmwi8e7fTbfXq7z3dLMcJJo4N
17A16QmavnUfCW11DAApiJxp7ARnxN5pGX

0.0015 BTC
Αξία σε BTC 0.00476968 BTC
κάθε output 0.0802 BTC
1.09509269 BTC

9 Επιβεβαιώσεις 1.18156237 BTC

Αριθμός επιβεβαιώσεων από miners

Input

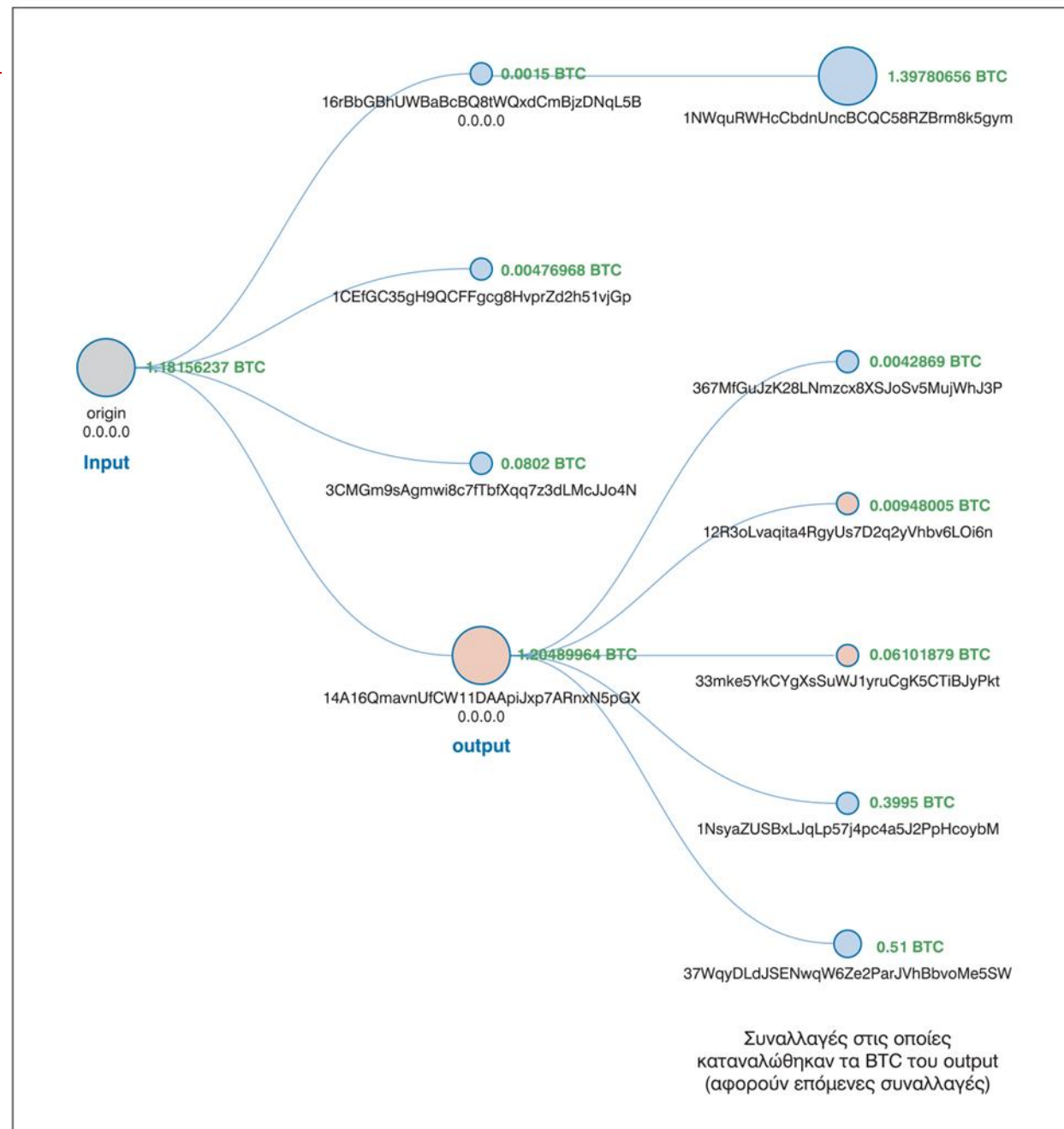
Outputs

Περίληψη	Είσοδοι και έξοδοι
Μέγεθος 323 (Bytes)	Συνολική είσοδος 1.18256237 BTC Αξία Input σε BTC
Βάρος 1292	Συνολική παραγωγή 1.18156237 BTC Αξία Output σε BTC
Λήψη χρόνου 2018-09-16 08:45:41	Αμοιβές 0.001 BTC Κόστος εκκαθάρισης συναλλαγής
Συμπεριλαμβάνεται σε μπλοκ 541638 (2018-09-16 08:48:46 + 3 λεπτά)	Χρέωση ανά byte 309.598 sat/B
Επιβεβαιώσεις 9	Χρέωση ανά μονάδα βάρους 77.399 sat/WU
Φαντάζομαι Δείτε το διάγραμμα των δένδρων	Εκτιμώμενη συναλλαγή BTC 0.0015 BTC
	Σενάρια Εμφάνιση σεναρίων & coinbase

ΕΙΚΟΝΑ 10.14

Προβολή μιας συναλλαγής με τον εξερευνητή Blockchain.info.

Προβολή του δέντρου μιας συναλλαγής με τον εξερευνητή Blockchain.info.



ΕΙΚΟΝΑ 10.15

Προβολή του δέντρου μιας συναλλαγής με τον εξερευνητή Blockchain.info.



Έξυπνες συμβάσεις (smart contracts) και το σύστημα Ethereum

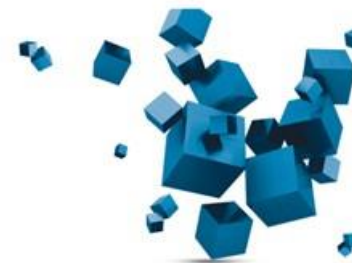
- Η ιδέα περιγράφηκε αρχικά από τον κρυπτογράφο Nick Szabo (1997) στο άρθρο του «Formalizing and Securing Relationships on Public Networks»,
- Μια έξυπνη σύμβαση είναι ένα ειδικό πρωτόκολλο που προορίζεται στο να συμβάλλει, να επαληθεύσει ή να εφαρμόσει τη διαπραγμάτευση ή την εκτέλεση μιας σύμβασης.
- Οι έξυπνες συμβάσεις επιτρέπουν την πραγματοποίηση αξιόπιστων συναλλαγών χωρίς τη διαμεσολάβηση τρίτων.
- Οι συναλλαγές αυτές είναι ιχνηλατήσιμες (traceable) και μη αναστρέψιμες (irreversible).
- Οι έξυπνες συμβάσεις περιέχουν όλες τις αναγκαίες πληροφορίες σχετικά με τους συμβατικούς όρους και εκτελούν αυτόματα όλες τις προβλεπόμενες ενέργειες.



Έξυπνες συμβάσεις

- Για να δημιουργήσουμε ένα έξυπνο συμβόλαιο χρειαζόμαστε:





Εφαρμογές τεχνολογίας blockchain

Κατηγορία	Παραδείγματα
Γενική	Συναλλαγές μεσεγγύησης, συμβάσεις, διαιτησίες, συναλλαγές με υπογραφή πολλαπλών συμβαλλομένων
Οικονομικές συναλλαγές	Χρηματιστήριο, ιδιωτικές τοποθετήσεις, crowdfunding, ομόλογα, αμοιβαία κεφάλαια, παράγωγα, συντάξεις
Δημόσια αρχεία	Τίτλοι γης και ιδιοκτησίας, εγγραφές οχημάτων, επιχειρηματικές άδειες, πιστοποιητικά γάμου, πιστοποιητικά θανάτου
Ταυτοποίηση	Άδειες οδήγησης, δελτία ταυτότητας, διαβατήρια, εγγραφές ψηφοφόρων
Ιδιωτικά αρχεία	Αξιόγραφα (I Own You – IOU), δάνεια, συμβόλαια, στοιχήματα, υπογραφές, διαθήκες, καταπιστεύματα, δεσμεύσεις
Επιβεβαίωση	Απόδειξη ασφάλισης, απόδειξη ιδιοκτησίας, συμβολαιογραφικά έγγραφα
Κλειδιά φυσικών στοιχείων	Οικίες, δωμάτια ξενοδοχείου, ενοικιαζόμενα αυτοκίνητα, κλειδιά αυτοκινήτων
Άυλα περιουσιακά στοιχεία	Διπλώματα ευρεσιτεχνίας, εμπορικά σήματα, δικαιώματα πνευματικής ιδιοκτησίας, κρατήσεις δωματίων ξενοδοχείων, κρατήσεις θέσεων παραστάσεων, αθλητικών γεγονότων, ονόματα τομέα διαδικτύου.
Πηγή: https://digiconomist.net/bitcoin-energy-consumption .	

Εισαγωγή στην Τεχνολογία Blockchain

Καθηγητής Δρ. Πάνος Φιτσιλής

