Αρχιτεκτονικές Πληροφοριακών Συστημάτων

Κατανεμημένα Συστήματα στην Οικονομία

Κατανεμημένα συστήματα και οικονομία

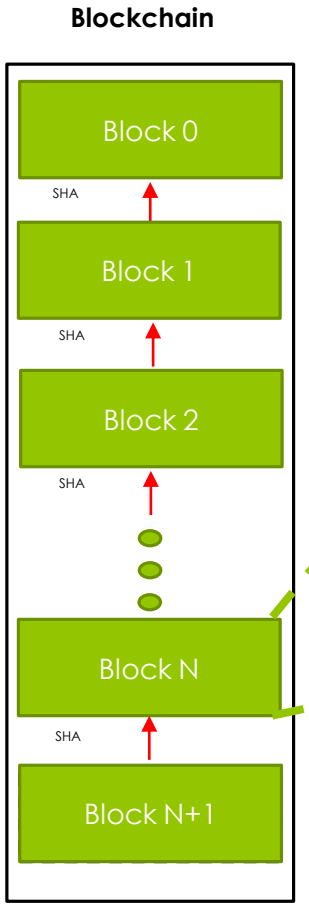
Εισαγωγή στο Blockchain

Τι είναι το Blockchain;

- Το Blockchain είναι μια σχετικά νέα, **πλήρως αποκεντρωμένη αρχιτεκτονική** κατανεμημένης επεξεργασίας και αποθήκευσης της πληροφορίας
- Βασίζεται στο «**κατανεμημένο καθολικό**» (distribuded ledger), δηλαδή σε μια κοινόκτητη και κοινόχρηστη λίστα στην οποία καταγράφονται οι συναλλαγές μεταξύ των συμμετεχόντων στο δίκτυο
- Η λίστα αυτή είναι **καθολικά αποδεκτή από όλους**, και τα δεδομένα της δεν μπορούν να αλλάξουν με κανένα τρόπο χωρίς αυτό να γίνει αντιληπτό στην κοινότητα

Το υπόλοιπο ενός τραπεζικού λογαριασμού υπολογίζεται κάθε φορά προσθέτοντας και αφαιρώντας το ποσό κάθε συναλλαγής από τη στιγμή δημιουργίας του λογαριασμού

Τι είναι το Blockchain;



Block N

Transaction data:

e.g. Transaction ID: #16 2A2B
Aris -> Nikos **10 Btc**
(wallet AF32DG14…->HT43YK213...) **10 Btc**

Block N-1 Hash:
0000070cfdeae6c1a3dc6cda8fef29495b42
228000439f880db139aa05a870

Hash:
0000006e452cbqwef36e463498d890b56d28
6a1886e767165219e22534368

Απλουστευμένο παράδειγμα block

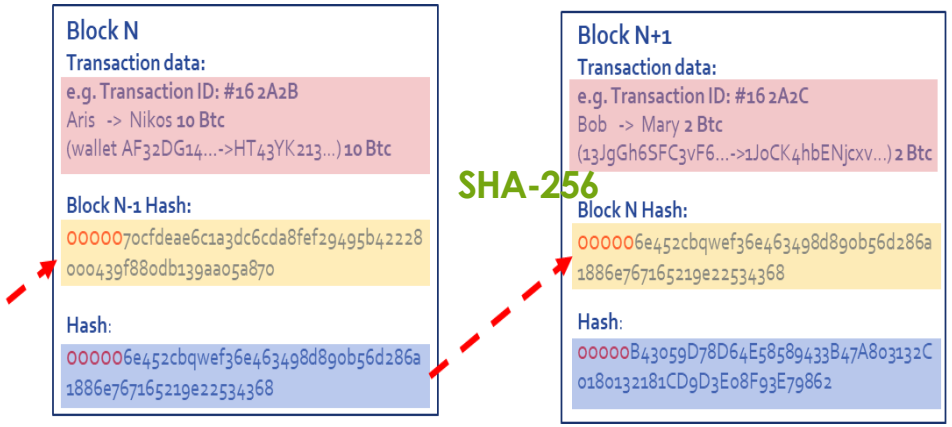
Κάθε συναλλαγή καταγράφεται σε μία **διασυνδεδεμένη λίστα** και αυτή αποθηκεύεται στους υπολογιστές «όλων»

Πως λειτουργεί το Blockchain;

Κάθε Blockchain βασίζεται σε 2 βασικούς μηχανισμούς

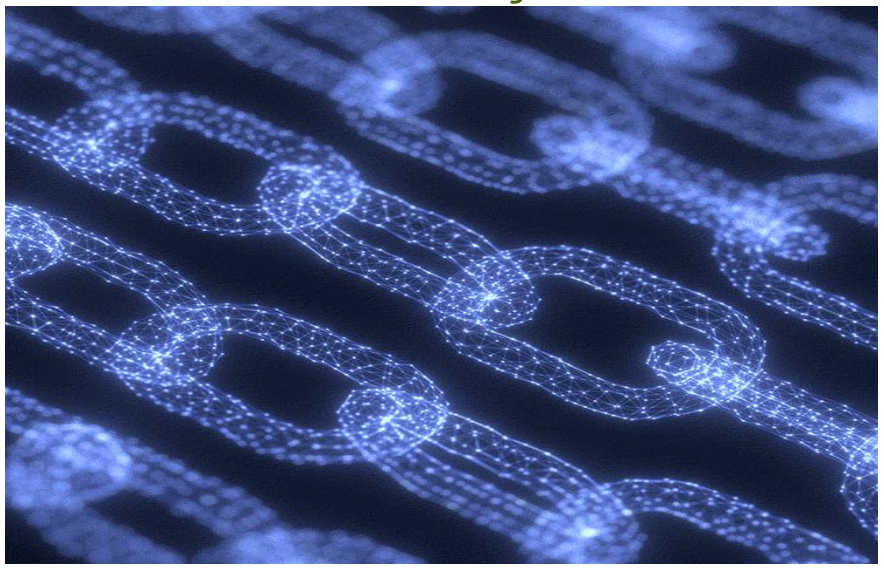
Hashing Mechanism

Ο μηχανισμός που συνδέει τους «κρίκους» της αλυσίδας



Consensus Mechanism

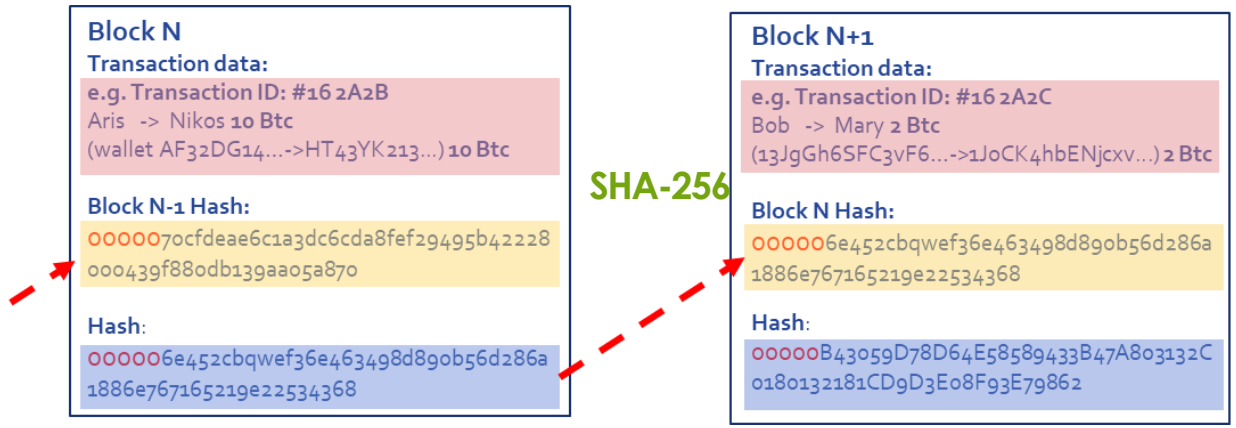
Ο μηχανισμός που διασφαλίζει ότι όλοι εργάζονται στην ίδια έκδοση της αλυσίδας



Πως λειτουργεί το Blockchain;

Μηχανισμός κατακερματισμού Hashing Mechanism

Ο μηχανισμός που συνδέει τους «κρίκους» της αλυσίδας



Σε κάθε νέο κρίκο, υπάρχει «κλειδωμένη» αναφορά στον προηγούμενο κρίκο της αλυσίδας

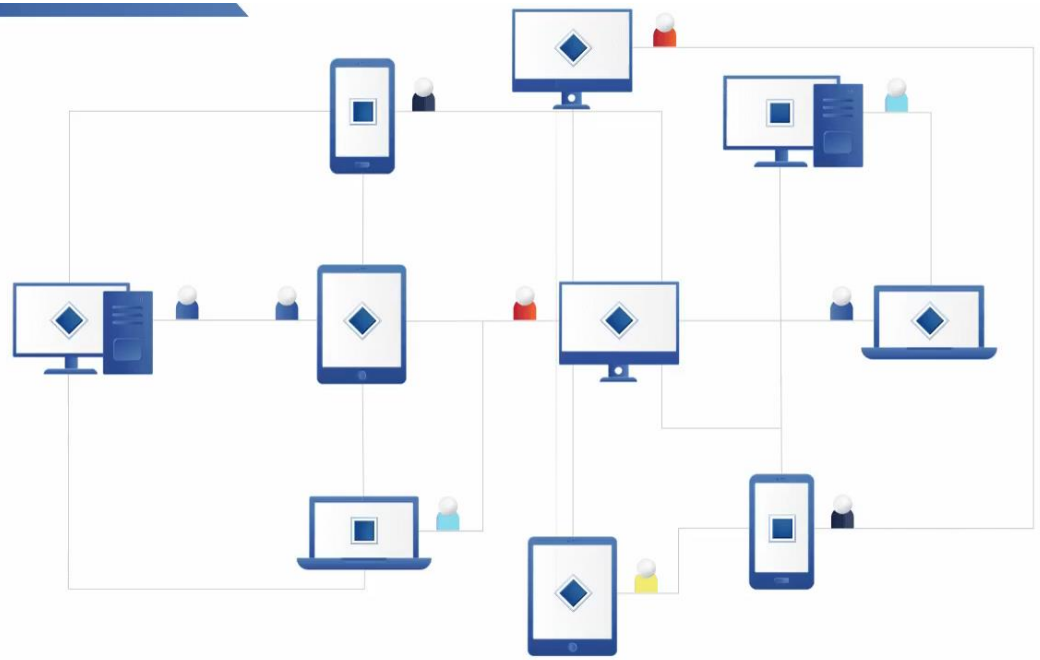
Αυτό την καθιστά απρόσβλητη σε επιθέσεις αλλοίωσης προηγούμενων εγγραφών

Hashing: μηχανισμός ο οποίος παράγει το «δακτυλικό αποτύπωμα» μιας εισόδου

Πως λειτουργεί το Blockchain;

Μηχανισμός επίτευξης συναίνεσης (Consensus Mechanism)

Ο μηχανισμός που διασφαλίζει ότι όλοι εργάζονται πάνω στην ίδια έκδοση της αλυσίδας



Η επίτευξη συναίνεσης πάνω σε ομότιμα συστήματα είναι πεδίο έντονης ερευνητικής δραστηριότητας

Πως λειτουργεί το Blockchain;

Μηχανισμός επίτευξης συναίνεσης (Consensus Mechanism)

Ο μηχανισμός που διασφαλίζει ότι όλοι εργάζονται πάνω στην ίδια έκδοση της αλυσίδας

Η επίτευξη συμφωνίας

αποτελεί κεφαλαιώδες ζήτημα των κατανεμημένων πληροφοριακών συστημάτων **στη διασφάλιση της αξιόπιστης λειτουργίας του συστήματος** παρουσία κάποιας **μη αξιόπιστης διαδικασίας**

Παράδειγμα: η επίτευξη αξιόπιστης λειτουργίας ενός κατανεμημένου συστήματος πάνω από ένα προβληματικό δίκτυο επικοινωνίας

Πως λειτουργεί το Blockchain;

Μηχανισμοί συναίνεσης (Consensus)

Το πρόβλημα των Βυζαντινών Στρατηγών (Byzantine Generals problem)

- ***n*** Στρατηγοί με τα στρατεύματά τους πολιορκούν ένα οχυρό
- προκειμένου να καταλάβουν το οχυρό **πρέπει να συμφωνήσουν μεταξύ** τους να επιτεθούν όλοι μαζί
- επικοινωνούν μεταξύ τους μόνο με προφορικά ή γραπτά **μηνύματα**

Πως λειτουργεί το Blockchain;

Μηχανισμοί συναίνεσης (Consensus)

Το πρόβλημα των Βυζαντινών Στρατηγών (Byzantine Generals problem)

- ανάμεσά τους υπάρχουν ***f*** προδότες

- Το πρόβλημα στη γενική του μορφή λύνεται* αν $\boldsymbol{f < \frac{1}{3} n}$

** 1982 Lambort, Shostak, Pease*
λύση για προφορικά μηνύματα

Πως λειτουργεί το Blockchain;

Μηχανισμοί συναίνεσης (Consensus)

Γενικές απαιτήσεις από ένα μηχανισμό συναίνεσης:

- **Απαίτηση για συμφωνία (Agreement)**
  - Όλες οι σωστές διαδικασίες ενός συστήματος πρέπει να συμφωνούν στην ίδια τιμή
- **Απαίτηση για πιστότητα (Weak validity)**
  - Η έξοδος κάποιας σωστής διαδικασίας θα πρέπει να αποτελεί είσοδο κάποιας επίσης σωστής διαδικασίας
- **Απαίτηση τερματισμού (Termination)**
  - Όλες οι διαδικασίες σταδιακά θα πρέπει να αποφασίσουν πάνω σε ένα τελικό αποτέλεσμα

Πως λειτουργεί το Blockchain;
Μηχανισμοί συναίνεσης (Consensus)

Η επίτευξη της συναίνεσης βασίζεται στην αποδοχή μιας ιδιότητας σεβαστής μεταξύ των μελών της ομάδας

Κατηγορίες μηχανισμών επίτευξης συναίνεσης σε κατανεμημένα συστήματα:

Απόδειξη έργου: PoW (Proof of Work)
Κάποιος έχει κάνει μια δουλειά και το αποδεικνύει

Απόδειξη μεριδίου: PoS (Proof of Stake)
Κάποιος κατέχει ένα μερίδιο της αλυσίδας και το αποδεικνύει

Απόδειξη χωρητικότητας: PoC (Proof of Capacity)
Κάποιος διαθέτει μεγάλη χωρητικότητα και το αποδεικνύει

…

Εισαγωγή στο Blockchain

Έξυπνα συμβόλαια – smart contracts

Τι είναι το «Έξυπνο Συμβόλαιο»;

Το έξυπνο συμβόλαιο είναι ένα **πρόγραμμα υπολογιστή**

Το οποίο **υλοποιεί τους όρους ενός συμβολαίου** του φυσικού κόσμου

Βρίσκεται **αποθηκευμένο στον(-ους) κόμβο(-ους) ενός Blockchain**
και
μπορεί να εκτελείται* μόνο μέσα σε αυτό

*Η εκτέλεση ενός Smart Contract έχει νόημα μόνο εντός της αλυσίδας που το περιέχει

Πως μοιάζει ένα έξυπνο συμβόλαιο;

Απλουστευμένο Block με Smart Contract

Block N

Transaction data:

e.g. Transaction ID: #16 2A2B
Aris -> Nikos **10 Btc**
(wallet AF32DG14…->HT43YK213...)

10 Btc

Block N-1 Hash:

0000070cfdeae6c1a3dc6cda8fef294
95b42228000439f880db139aa05a870

Hash:

0000006e452cbqwef36e463498d890
b56d286a1886e767165219e22534368

```
pragma solidity ^0.4.21;

contract Coin {
    // The keyword "public" makes those variables
    // readable from outside.
    address public minter;
    mapping (address => uint) public balances;

    // Events allow light clients to react on
    // changes efficiently.
    event Sent(address from, address to, uint amount);

    // This is the constructor whose code is
    // run only when the contract is created.
    function Coin() public {
        minter = msg.sender;
    }

    function mint(address receiver, uint amount) public {
        if (msg.sender != minter) return;
        balances[receiver] += amount;
    }

    function send(address receiver, uint amount) public {
        if (balances[msg.sender] < amount) return;
        balances[msg.sender] -= amount;
        balances[receiver] += amount;
        emit Sent(msg.sender, receiver, amount);
    }
}
```

*Οι γλώσσες προγραμματισμού των Έξυπνων συμβολαίων είναι **Turing Complete**
Μπορούν να χρησιμοποιηθούν για να αναπαραστήσουν οποιοδήποτε «πεπερασμένο αυτόματο»

Τι μπορεί να κάνει ένα έξυπνο συμβόλαιο;

Το έξυπνο συμβόλαιο μπορεί να αυτοματοποιήσει/υποκαταστήσει:

Οποιαδήποτε διαδικασία* προβλέπει υπό όρους συναλλαγή: *χρηματιστηριακές συναλλαγές, δάνεια, προγαμιαία συμφωνητικά, αγοραπωλησίες, μισθώσεις, συμβολαιογραφικές πράξεις εν γένει …*

Οποιοδήποτε τρίτο έμπιστο μέρος μπορεί να τυποποιηθεί και να περιγραφεί με όρους συμβολαίου: *μητρώα, υποθηκοφυλακεία, αρχές έκδοσης πιστοποιητικών, ενώσεις, σωματεία, συλλόγους, τράπεζες …*

Εισαγωγή στο Blockchain

Κρυπτογραφικά νομίσματα

Τι είναι τα «Κρυπτογραφικά Νομίσματα»;

Τα «Κρυπτογραφικά Νομίσματα» είναι **ψηφιακά νομίσματα*** τα οποία εκδίδονται και λειτουργούν αξιοποιώντας τις ιδιότητες των κατανεμημένων Blockchain.

Ο μηχανισμός του Blockchain έγινε δημοφιλής κυρίως εξαιτίας της εμφάνισης και της ραγδαίας αύξησης της ζήτησης των κρυπτογραφικών νομισμάτων, και ειδικότερα του Bitcoin.

*Είναι ενεργό πεδίο έρευνας και το εάν και κατά πόσο τα κρυπτογραφικά νομίσματα πληρούν τις βασικές λειτουργίες του χρήματος ήτοι μπορούν να λειτουργούν αποδοτικά:
α) ως μέσο συναλλαγής, β) ως μέσο συσσώρευσης πλούτου και γ) ως μονάδα μέτρησης αξίας

Κρυπτογραφικά Νομίσματα

#	Name	Market Cap
1	Bitcoin	$159.052.412.401
2	Ethereum	$20.071.342.744
3	XRP	$12.052.477.881
4	Bitcoin Cash	$5.111.686.961
5	Tether	$4.126.920.334
6	Litecoin	$3.895.392.439
7	EOS	$3.262.705.981
8	Binance Coin	$3.077.554.370
9	Bitcoin SV	$2.340.143.890
10	Stellar	$1.449.991.408
11	TRON	$1.262.380.260
12	Cardano	$1.100.048.986
13	Monero	$1.059.299.882
14	Chainlink	$994.040.348
15	UNUS SED LEO	$991.241.754
16	Huobi Token	$922.091.442
17	Tezos	$779.585.423
18	NEO	$749.125.999
19	Cosmos	$741.797.686
20	IOTA	$742.112.831

Η αγορά των κρυπτογραφικών νομισμάτων αποτελεί γκρίζα ζώνη σε πολλές χώρες.

Η κυκλοφορία των κρυπτογραφικών νομισμάτων στην αγορά κυμαίνεται από **νόμιμη και ελεύθερη** έως **πλήρως απαγορευμένη**.

Κοινή απαίτηση όλων η διαφάνεια και απόδοση φόρου επί των συναλλαγών.

Συνολική αποτίμηση Νοε. 2019:

$250.000.000.000

* https://coinmarketcap.com/

Η αγορά των κρυπτογραφικών νομισμάτων είναι ακόμα μη-ρυθμισμένη (unregulated).
Οι τιμές βασίζονται σε εκτιμήσεις από τα δεδομένα που παρέχουν τα υφιστάμενα επίσημα ανταλλακτήρια

Κρυπτογραφικά Νομίσματα

Θετικά:

- Κατανεμημένα συστήματα, μη υποκείμενα στους περιορισμούς των κεντρικοποιημένων αρχιτεκτονικών
- «Αποπληθωρισμένα» εξ'ορισμού
- Ομότιμα* στην περίπτωση των ανοιχτών PoW αλυσίδων

Αρνητικά:

- Αυξημένη κατανάλωση σε ενέργεια και απαίτηση σε υπολογιστικούς πόρους
- Μη κανονικοποιημένο πλαίσιο λειτουργίας
- Μεταβλητότητα αξίας