Τεχνολογίες Blockchain & Αποκεντρωμένες Εφαρμογές

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

Διάλεξη #03

Πώς λειτουργεί το Blockchain #1

Περιεχόμενα

- Στοιχεία Κρυπτογραφίας
- Θεωρία Παιγνίων
- Επιστήμη Υπολογιστών
- Πώς συνδυάζονται τα προηγούμενα στο Blockchain

Εισαγωγή – (1)

- Η Θεωρία Παιγνίων (Game Theory) δεν είναι καινούργια και έχει εφαρμογή σε πολλά πεδία
- Επίσημα εισήχθη από τον John von Neumann για αποφάσεις στα Οικονομικά
- Έγινε ακόμα πιο δημοφιλής μέσω της θεωρίας «Ισορροπία Nash» (Nash Equilibrium) από τον John Forbes Nash

Εισαγωγή – (2)

- Συνήθως αναφέρεται σε παιχνίδια (όχι παιδικά) με 2 ή περισσότερους παίκτες που έχουν κάποια στρατηγική συμπεριφορά
  - Δικηγόροι αντίπαλοι σε δικαστήριο
  - Πολιτική εκλογή
  - Σηματοδότες κυκλοφορίας (φανάρια)
  - Απόρριψη επιλογής για πρόσληψη λόγω διαφοράς μεταξύ προσφοράς και ζήτησης

Εισαγωγή – (3)

- Άρα παιχνίδι είναι οποιαδήποτε περίπτωση όπου υπάρχουν συσχετιζόμενες λογικές επιλογές
  - Οι διαθέσιμες προοπτικές για έναν παίκτη εξαρτώνται όχι μόνον από τις προσωπικές του προτιμήσεις, αλλά και από τις επιλογές που κάνουν οι υπόλοιποι σε μια δεδομένη κατάσταση

Εισαγωγή – (4)

- Η Θεωρία παιγνίων αφορά τη μελέτη στρατηγικών για πολύπλοκα παιχνίδια
  - Η τέχνη του να κάνουμε τη βέλτιστη κίνηση ή να επιλέγουμε μια τέλεια στρατηγική σε μια δεδομένη κατάσταση με βάση κάποιο στόχο του παιχνιδιού (συνθήκες νίκης)
  - Για να το πετυχαίνουμε αυτό, πρέπει να καταλαβαίνουμε τη στρατηγική του αντιπάλου, καθώς και ποιά σκέφτεται ο αντίπαλος ότι θα είναι η επόμενη κίνησή μας

Εισαγωγή – (5)

- Παράδειγμα #1: 1 παγωτό κρέμα, 1 παγωτό βανίλια και δύο αδέλφια, όπου ο μεγάλος γνωρίζει ότι όποια επιλογή να κάνει, θα την επιλέξει και ο μικρός
  - Στρατηγική μεγάλου: Αν θέλει την κρέμα, επιλέγει την βανίλια, το ίδιο κάνει ο μικρός, οπότε ο μεγάλος «υποχωρεί» κερδίζοντας την πραγματική του επιθυμία.
  - Συνολικό όμως αποτέλεσμα “win-win” αφού και οι δύο κέρδισαν αυτό που ήθελαν

Εισαγωγή – (6)

- Παράδειγμα #2: Παραγωγός λαχανικών με στόχο το μεγαλύτερο κέρδος αν τα καταφέρει να βρεθεί από τους πρώτους στη Λαχαναγορά
  - Υπάρχουν 3 διαδρομές
    - Πάντα ακολουθεί την 3η (ως καλύτερη), αλλά αυτή έχει κλείσει λόγω έργων
    - Η 1η είναι συντομότερη αλλά με στενούς δρόμους
    - Η 2η λίγο μακρύτερη αλλά με φαρδείς δρόμους (μεγαλύτερη ταχύτητα)

    Επιλέγει τη 2η καθώς
    - Η 1η απαιτεί λιγότερα καύσιμα αλλά μπορεί να υπάρχει αυξημένη κίνηση άρα μεγάλη καθυστέρηση (και μικρότερο κέρδος)
    - Η 2η θα τον οδηγήσει συντομότερα στη Λαχαναγορά, οπότε θα πετύχει το στόχο του για μεγαλύτερο κέρδος, έναντι όμως καυσίμων

Τύποι παιχνιδιών

- Πολλοί τρόποι για να ταξινομήσουμε τα παιχνίδια
  - zero-sum/non-zero-sum, simultaneous/sequential, κλπ.
- Εδώ μας ενδιαφέρουν τα cooperative/noncooperative
  - Οι παίκτες συνεργάζονται μεταξύ τους (συμμαχίες) και μπορεί να υπάρχει μια εξωτερική δύναμη για να επιβεβαιώνει κάτι τέτοιο
  - Στον αντίποδα, παίζουν μόνον ως άτομα, κοιτώντας το στενό τους συμφέρον και δεν υπάρχει εξωτερική δύναμη για να τους υποχρεώσει σε συνεργασία

MSNlab

Nash Equilibrium

- Σε οποιοδήποτε μη-συνεργατικό παίγνιο, όπου οι παίκτες γνωρίζουν τις στρατηγικές των άλλων, υπάρχει τουλάχιστον ένα σημείο ισορροπίας όπου όλοι οι παίκτες παίζουν με τις βέλτιστες στρατηγικές τους για τα μέγιστα κέρδη και κανένας παίκτης δεν θα κέρδιζε με το να άλλαζε την στρατηγική του

Παράδειγμα – Το Δίλημμα του Κρατουμένου

- Περίπτωση non-zero-sum και symmetric game (ίδια ανταμοιβή εάν εναλλαγούν οι παίκτες και παραμείνουν ίδιες οι στρατηγικές τους)
- Έστω ο Βασίλης και ο Τάκης που συλλαμβάνονται (ξεχωριστά) για το ίδιο αδίκημα και βρίσκονται σε διαφορετικά δωμάτια ανάκρισης
- Τους λένε ότι η ποινή είναι 2 έτη φυλάκισης, αλλά επιπλέον τους υποπτεύονται ότι ενέχονται και σε πρόσφατο δεύτερο αδίκημα

Τι κάνουν οι Αστυνομικοί για την Αλήθεια

- Στο Βασίλη προτείνουν ότι
  - εάν ομολογήσει, αλλά όχι ο Τάκης, η ποινή του θα πέσει από 2 σε 1 έτος, ενώ του Τάκη θα πάει σε 5 έτη
  - εάν δεν ομολογήσει, αλλά το κάνει ο Τάκης, τότε ο μεν Τάκης θα εκτίσει 1 έτος, ενώ ο Βασίλης 5
  - εάν ομολογήσουν και οι δύο θα εκτίσουν από 3 έτη
- Η ίδια πρόταση γίνεται στον Τάκη

Τι θα απαντήσουν ο Βασίλης και ο Τάκης;

- Δεν μπορούν να μιλήσουν μεταξύ τους, αλλά και δεν μπορούν να εμπιστευθούν ο ένας τον άλλον
- Καθένας έχει 2 επιλογές, αφού σκέπτεται ότι και οι 2 τους θα επιδιώξουν τη βέλτιστη για καθένα λύση:
  - *Ομολογία*: στην χειρότερη εκτίει 3 έτη (ομολογεί και ο άλλος), στην καλύτερη 1 έτος (δεν ομολογεί ο άλλος)
  - *Μη ομολογία*: στην χειρότερη εκτίει 5 έτη (ομολογεί ο άλλος), στην καλύτερη 2 έτη (δεν ομολογεί ο άλλος)
- Αυτή η κατάσταση λέγεται Ισορροπία Nash

Πίνακας Αμοιβών (Prisoner's Dilemma)

Βασίλης

Τάκης

	Ομολογία	**Μη Ομολογία**
Ομολογία	3 3	5 1
Μη Ομολογία	1 5	2 2

Τι είναι βέλτιστο;

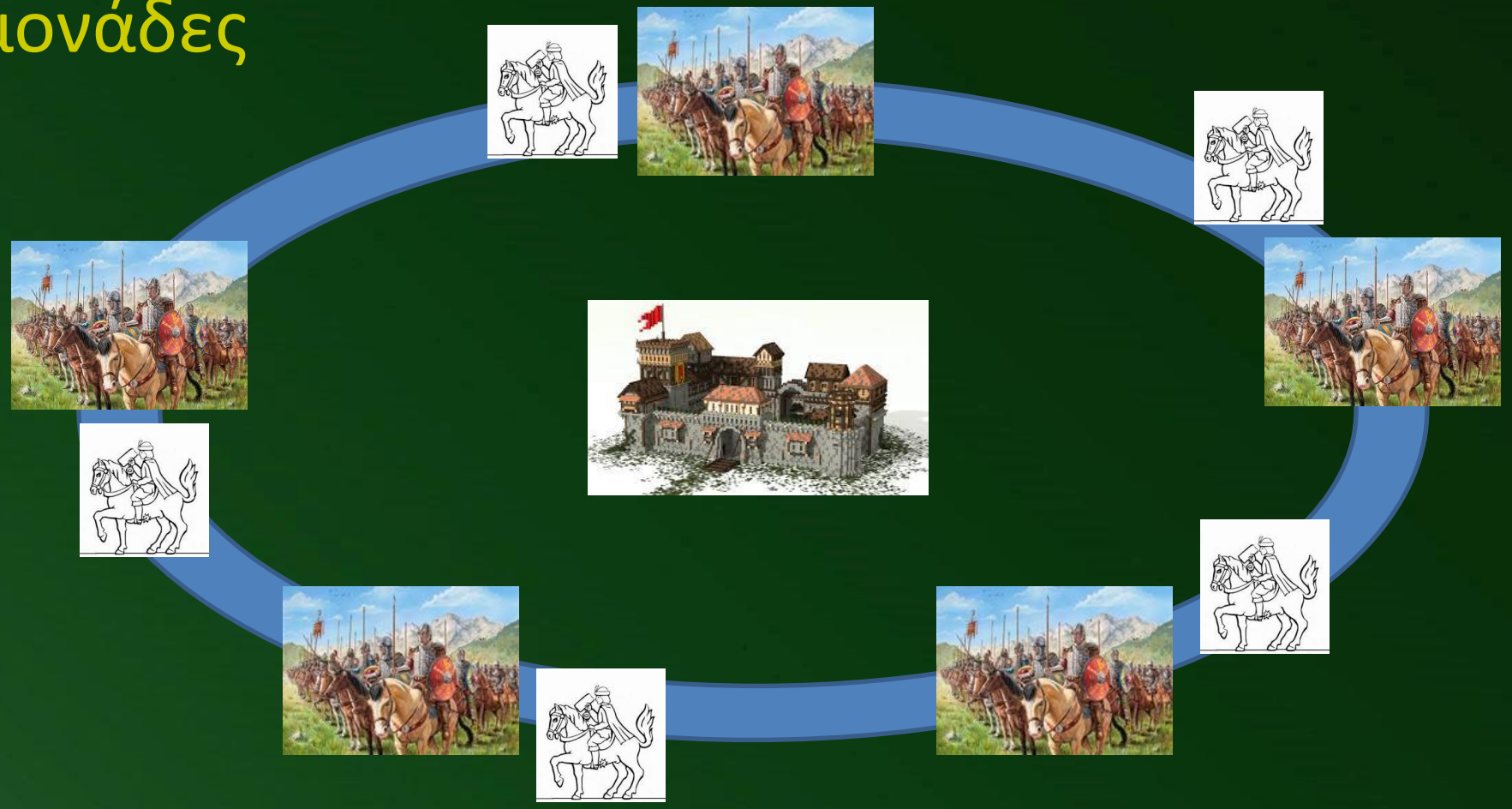
- Για τον εξωτερικό παρατηρητή η λύση είναι να μην ομολογήσουν και οι δύο με ποινή 2 έτη έκαστος
- Για τους παίκτες η Ισορροπία Nash είναι η φυσική κατάληξη που τους οδηγεί στην απόφαση της ομολογίας (και των δύο) με ποινή 3 έτη έκαστος:
  - το σημείο όπου η μεταβολή στρατηγικής δεν οδηγεί σε καλύτερο αποτέλεσμα για κάθε παίκτη (ξεχωριστά)

Πρόβλημα των Βυζαντινών Στρατηγών

- Ο Βυζαντινός στρατός επιτίθεται εναντίον μιας πόλης, αλλά είναι χωρισμένος σε 2 ή περισσότερες μονάδες (με 1 στρατηγό η κάθε μία)
- Για να νικήσει ο στρατός πρέπει όλες οι μονάδες να επιτεθούν ταυτόχρονα
- Το πρόβλημα είναι πως να φτάσουν σε ομοφωνία
  - είτε όλοι μαζί να επιτεθούν
  - είτε όλοι μαζί να υποχωρήσουν

Πρόβλημα των Βυζαντινών Στρατηγών

Παράδειγμα με 5 μονάδες



Πρακτικά Ζητήματα

- Χρειάζεται ομοφωνία (consensus) μεταξύ των στρατηγών
  - θα πρέπει να επιτεθούν αν τουλάχιστον 3 από τους 5 επιθυμούν επίθεση, αλλιώς να υποχωρήσουν
- Αφού δεν υπάρχει κεντρικός συντονισμός, εάν 1 από τους 5 είναι προδότης, θα ψήφιζε (για να ηττηθούν):
  - επίθεση με τους στρατηγούς που επιθυμούν επίθεση
  - υποχώρηση με εκείνους που επιθυμούν υποχώρηση
- Τι θα συμβεί αν μόνο 2 πιστοί στρατηγοί και ο προδότης ψηφίσουν επίθεση;

Ακόμα πιο πολύπλοκα ζητήματα

- Εάν υπάρχουν περισσότεροι προδότες;
- Πώς θα μπορούσε να επιτευχθεί συντονισμός των στρατηγών μέσω μηνυμάτων;
- Εάν ο αγγελιοφόρος συλληφθεί, σκοτωθεί ή δωροδοκηθεί από το διοικητή της πόλης;
- Εάν ο στρατηγός-προδότης πλαστογραφήσει ένα διαφορετικό μήνυμα και εξαπατήσει τους υπόλοιπους;
- Πώς να διακρίνουμε τους τίμιους από τους προδότες;

Ανάλογα σενάρια

- Πώς καταλήγει σε ομοφωνία μια ομάδα ανθρώπων σχετικά με την ημερήσια διάταξη για ψηφοφορία;
- Πως διατηρείται η συνεπής κατάσταση σε μια κατανεμημένη ή αποκεντρωμένη βάση δεδομένων;
- Πως διατηρείται η συνεπής κατάσταση των αντιγράφων blockchain μεταξύ των κόμβων ενός δικτύου;
- Οι λύσεις μπορεί να είναι πολύ διαφορετικές για διαφορετικές καταστάσεις
  - Π.χ. ο τρόπος (consensus algorithm) με τον οποίο το Bitcoin λύνει το πρόβλημα των Βυζαντινών Στρατηγών

Περιεχόμενα

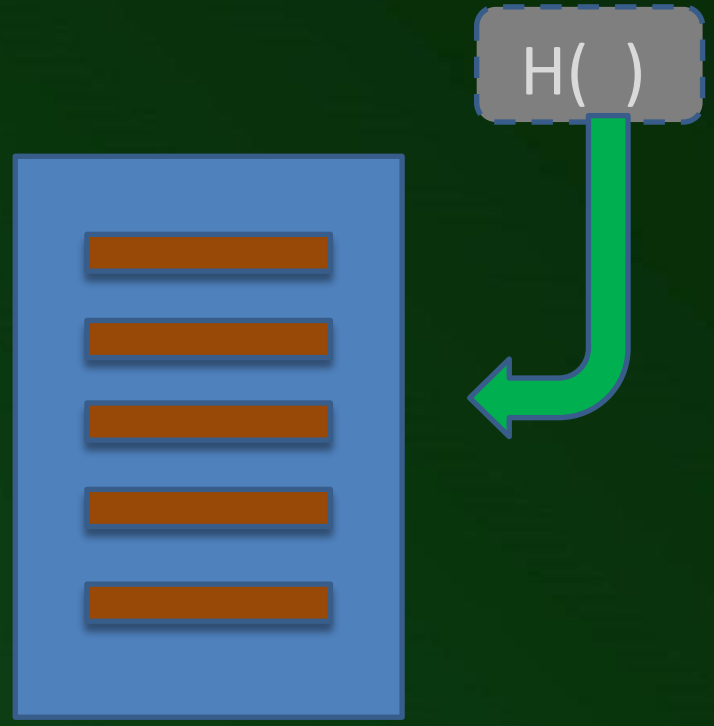
- Στοιχεία Κρυπτογραφίας
- Θεωρία Παιγνίων
- Επιστήμη Υπολογιστών
- Πώς συνδυάζονται τα προηγούμενα στο Blockchain

Το “Blockchain”

- Μια δομή δεδομένων:
  - Αλυσίδα από μπλοκ (block) συνδεδεμένα μεταξύ τους
- Τι είναι το “block”;
  - Δεδομένα για μια ή περισσότερες συναλλαγές
- Βασικό δομικό στοιχείο είναι οι δείκτες κατακερματισμού (hash pointer)

Hash Pointer

- Περίπου όπως οι δείκτες στις συνδεδεμένες λίστες
- Εδώ όμως δείχνουν στο προηγούμενο block και όχι στο επόμενο
- Επίσης παρέχουν εγγύηση ότι τα αντίστοιχα δεδομένα δεν έχουν αλλοιωθεί



Block Δεδομένων

Blockchain: μοναδική πηγή αλήθειας

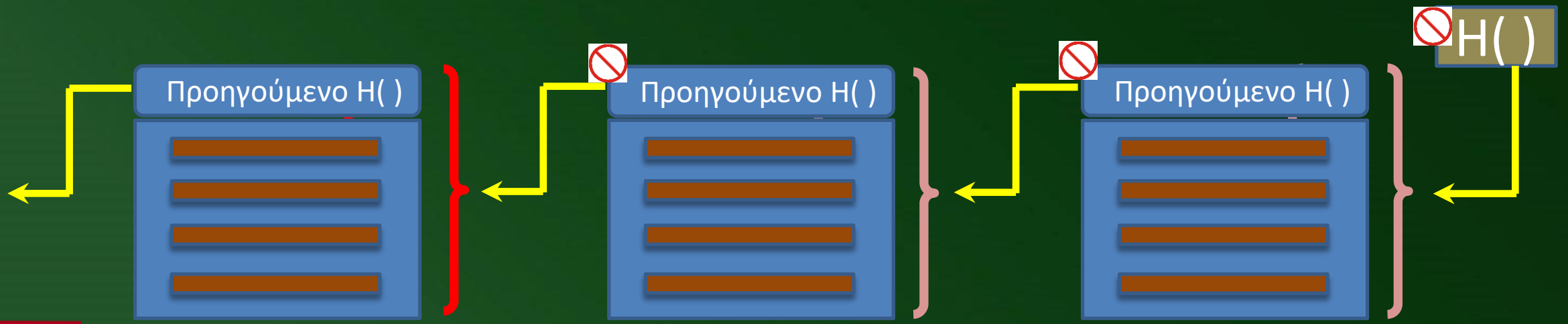
- Στη κεφαλίδα (header) κάθε block αποθηκεύεται η τιμή Hash του προηγούμενου block, ώστε να υπάρχει διασφάλιση για τη μη αλλοίωση των δεδομένων του προηγούμενου block

Παρατηρήσεις

- Η τιμή Hash() αφορά όλο το προηγούμενο block, μαζί με το προηγούμενο Hash()
- Κάθε block δείχνει στο προηγούμενο block που ονομάζεται “parent block” (γονικό)
- Το πρωταρχικό block ονομάζεται “genesis block”
- Είναι πρακτικά αδύνατο να αλλάξει κάποιος τα δεδομένα σε ένα block

Λεπτομέρειες

- Εάν κάποιος αλλάξει το περιεχόμενο ενός block;
  - Δεν ταιριάζουν οι τιμές Hash()
- Τι γίνεται εάν κάποιος αλλάξει και τις τιμές Hash();
  - Θα σπάσει την αλυσίδα, οπότε πρέπει να τροποποιήσει ολόκληρη την αλυσίδα!



Επιλογές

- Συνάρτηση κατακερματισμού
  - Συνήθως επιλέγεται η οικογένεια SHA2 ή SHA3
- Δομή του block
  - Μέγεθος block, περιοχές δεδομένων και επικεφαλίδας, πλήθος συναλλαγών ανά block κ.ά.
- Για υπάρχοντα blockchain (Bitcoin, Ethereum, Hyperledger) η δομή είναι ήδη καθορισμένη

Δένδρα Merkle

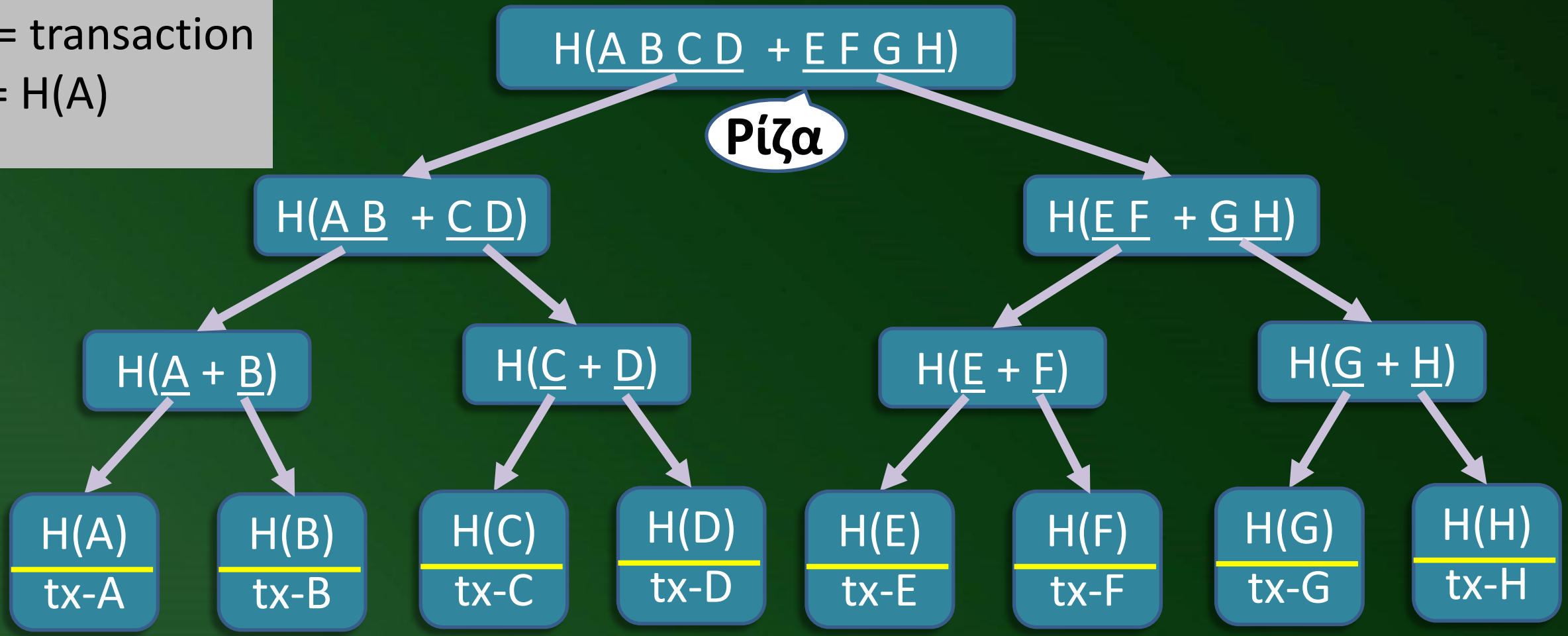
- Από τον Ralph Merkle που τα επινόησε
- Δένδρο Merkle: δυαδικό δένδρο με δείκτες hash (binary hash tree)
- Δομή δεδομένων που χρησιμοποιείται στο Bitcoin

Δένδρα Merkle

- Δομούνται με κατακερματισμό συζευγμένων δεδομένων (π.χ. συναλλαγές) στο επίπεδο φύλλου, κατόπιν ξανά κατακερματισμό των αποτελεσμάτων μέχρι το κόμβο-ρίζα, που ονομάζεται ρίζα Merkle
  - Καταστρώνονται από-κάτω-προς-τα-επάνω (bottom-up)
  - Στο Bitcoin τα φύλλα είναι πάντα συναλλαγές ενός μοναδικού block του blockchain

Παράδειγμα Δένδρου Merkle

tx = transaction
A = H(A)



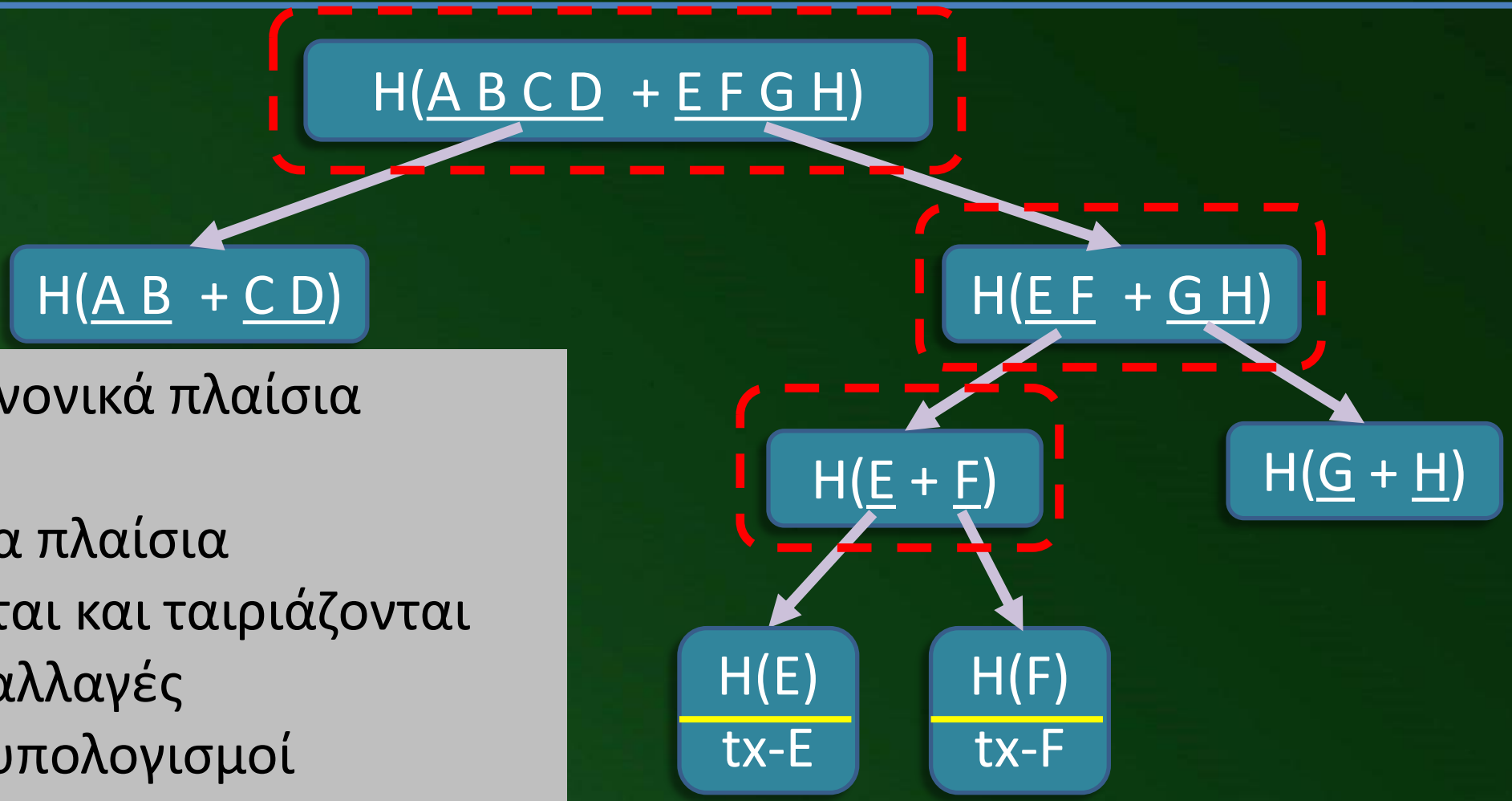
Χαρακτηριστικά των Δένδρων Merkle

- Είναι απαραβίαστα (tamper-proof)
  - Παραβίαση σε οποιοδήποτε επίπεδο θα οδηγούσε σε μη ταίριασμα των Hash που είναι αποθηκευμένα στα ανώτερα επίπεδα *και μέχρι τη ρίζα Merkle*
- Εγγυώνται την ορθή ακολουθία των συναλλαγών
  - Αφού πάλι οι τιμές Hash (έως και την ρίζα) θα άλλαζαν

Βασικά Ερωτήματα

- *Εάν δεν υπάρχει ζυγό πλήθος συναλλαγών;*
  - Λύση: επαναλαμβάνεται το Hash της τελευταίας συναλλαγής
    - Παραμένει η ίδια συναλλαγή, άρα δεν υπάρχει double-spent ή επανάληψη συναλλαγής, οπότε έχουμε ισορροπημένο δένδρο
- *Για αναζήτηση παρελθούσας συναλλαγής απ' ευθείας ή μέσω της τιμής hash της;*
  - Λύση: επιβεβαίωση αν η συναλλαγή (φύλλο) ανήκει στο δένδρο Merkle
    - χρειαζόμαστε μόνον ένα μέρος του δένδρου
    - Το πλήθος των υπολογισμών για n συναλλαγές είναι $\log n$

Παράδειγμα Επιβεβαίωσης Συναλλαγής “F”



- Μόνο τα κανονικά πλαίσια χρειάζονται
- Τα διάστικτα πλαίσια υπολογίζονται και ταιριάζονται
  - n=8 συναλλαγές
  - $\log_2 8=3$ υπολογισμοί

Υβρίδιο Δομής Blockchain και Δένδρου Merkle

- Εάν οι συναλλαγές είναι πάρα πολλές, πώς μπορούμε να έχουμε ταχύτερη επιβεβαίωσή τους;
  - Κάθε μπλοκ ήδη περιλαμβάνει το Hash του προηγούμενου
  - Συμπερίληψη και της ρίζας Merkle root σε αυτό
- Άρα, για επιβεβαίωση συναλλαγής στο μπλοκ 22456:
  - παίρνουμε τις συναλλαγές του μπλοκ και υπολογίζουμε το δένδρο Merkle
  - επιβεβαιώνουμε την υπολογισμένη ρίζα Merkle συγκρίνοντάς την με την αποθηκευμένη

“Light” Node

- Κόμβος που δεν περιέχει ολόκληρα τα block συναλλαγών, αλλά μόνο τις επικεφαλίδες τους
- Για επιβεβαίωση ότι κάποια συναλλαγή συνέβη στο παρελθόν χρειάζεται:
  - Επιβεβαίωση ότι η συναλλαγή είναι μέρος ενός μπλοκ και
    Επιβεβαίωση ότι το μπλοκ είναι μέρος της αλυσίδας (blockchain)
- Για αυτό το σκοπό, δεν απαιτείται να κατέβουν από το δίκτυο όλες οι συναλλαγές του μπλοκ, αλλά μόνο:
  - Οι επικεφαλίδες της μακρύτερης αλυσίδας PoW και
  - Η διαδρομή Merkle που συνδέει τη συγκεκριμένη συναλλαγή με το μπλοκ όπου έχει χρονοσημανθεί

Περιεχόμενα

- Στοιχεία Κρυπτογραφίας
- Θεωρία Παιγνίων
- Επιστήμη Υπολογιστών
- Πώς συνδυάζονται τα προηγούμενα στο Blockchain

Σύνοψη Προηγουμένων

- Μονοκατευθυντικές Συναρτήσεις Κατακερματισμού (δεν μπορούν να αναστραφούν), με ίδια έξοδο για ίδια είσοδο
- Ψηφιακές υπογραφές με κρυπτογραφία δημοσίου κλειδιού για αυθεντικότητα, ακεραιότητα και μη-αποποίηση
- Αξιοποίηση Θεωρίας Παιγνίων για σχεδιασμό ανθεκτικών συστημάτων όπου οι παίκτες εφαρμόζουν κανόνες για μέγιστη αμοιβή. Δεν επωφελούνται παρεκκλίνοντας από τη στρατηγική τους
- Η αξιοποίηση των Hash στη δομή δεδομένων του Blockchain παρέχει ανθεκτική (δεν παραχαράσσεται) αλυσίδα από μπλοκ
- Τα δένδρα Merkle κάνουν την επιβεβαίωση συναλλαγών ευκολότερη και ταχύτερη

Αλλά και Νέα Ερωτήματα… (1)

- Ποιος τηρεί το κατανεμημένο καθολικό των συναλλαγών;
  - Όλοι ή μερικοί;
  - Όσοι δεν έχουν αποθηκευτικό χώρο για ολόκληρο το ιστορικό των συναλλαγών ή δεν είναι αρκετά δυνατοί για να τις επεξεργάζονται;
- Με δικτυακές καθυστερήσεις, απώλειες πακέτων, εσκεμμένες επιθέσεις, κλπ, πώς παραμένει το καθολικό σε μια ενιαία, συνεπή κατάσταση;

Αλλά και Νέα Ερωτήματα… (2)

- Ποιος επικυρώνει (ή ακυρώνει) τις συναλλαγές;
  - Μερικοί εξουσιοδοτημένοι κόμβοι;
  - Όλοι οι κόμβοι φτάνουν σε ομοφωνία;
  - Αν ορισμένοι δεν είναι διαθέσιμοι σε δεδομένο χρόνο;
- Εάν κάποιοι κόμβοι επίτηδες υπονομεύουν το σύστημα, π.χ., απορρίπτοντας κάποιες συναλλαγές;
- Πώς μπορεί να γίνει αναβάθμιση του συστήματος όταν δεν υπάρχει μια κεντρική οντότητα να πάρει την ευθύνη
  - οπότε ορισμένοι κόμβοι αναβαθμίζονται και άλλοι όχι;

Επιθυμητές Ιδιότητες των Λύσεων Blockchain

- Αμεταβλητότητα (Immutability)
- Ανθεκτική σε Παραχάραξη (Forgery Resistant)
- Δημοκρατική (Democratic)
- Ανθεκτική σε Διπλοξόδεμα (Double-Spend Resistant)
- Συνεπής Κατάσταση του Καθολικού (Consistent State of the Ledger)
- Ανθεκτική & Ελέγξιμη (Resilient & Auditable)

Immutability

- Αμεταβλητότητα
- Η πιο επιθυμητή ιδιότητα προκειμένου να τηρείται η ατομικότητα (αμετάβλητο) των συναλλαγών blockchain
- Με τη μαζική δικτυακή μετάδοση των συναλλαγών, μετά από κάποιον χρόνο, προστίθενται περισσότερα block, καθιστώντας τες πλήρως αμετάβλητες
  - Πρακτικά ανέφικτη η μεταβολή πάρα πολλών block σε όλους τους κόμβους

Forgery Resistant

- Ανθεκτική σε Παραχάραξη
- Οι συναλλαγές είναι δημόσιες και το σύστημα αποκεντρωμένο, ευνοόντας επιθέσεις
  - ειδικά όταν αφορά χρήμα/αξία
- Η απαιτούμενη προστασία επιτυγχάνεται με χρήση Hash (ακεραιότητα) και ψηφιακών υπογραφών (αυθεντικότητα και μη-αποποίηση)

Democratic

- Δημοκρατική
- Ως γενική αρχή, κάθε αποκεντρωμένο σύστημα P2P πρέπει να θεωρεί ισότιμους όλους τους συμμετέχοντες, με τις αποφάσεις να λαμβάνονται κατά πλειοψηφία
  - democratic by design
  - όχι πλήρως εφαρμόσιμο σε private blockchain

Double-Spend Resistant – (1)

- Ανθεκτική σε Διπλοξόδεμα
- Επιθέσεις Διπλοξοδέματος: σύνηθες φαινόμενο, ακόμα και για συναλλαγές χωρίς χρήματα
  - Το ίδιο αντικείμενο πωλείται σε πολλαπλούς αγοραστές
  - Το υπόλοιπο λογαριασμού μας 100€, αλλά πληρώνουμε δύο ή περισσότερους αγορές μας από 90€
- Λύση Bitcoin: Η είσοδος κάθε συναλλαγής (όταν πληρώνουμε κάποιον) είναι έξοδος από κάποιαν άλλη

Double-Spend Resistant – (2)

- Εύκολα αντιμετωπίζεται σε συγκεντρωτικά συστήματα λόγω του ελέγχου των συναλλαγών από μια κεντρική αρχή

- Στα αποκεντρωμένα συστήματα blockchain η λύση έγκειται στον έλεγχο όλων των συναλλαγών του παρελθόντος, μέχρι το genesis block

Consistent State of the Ledger

- Συνεπής Κατάσταση του Καθολικού
  - Π.χ., κόμβοι που δεν είναι συγχρονισμένοι και έχασαν κάποιες συναλλαγές, ή που επίτηδες προσπαθούν την ακύρωση κάποιας συναλλαγής
- Λύση: Κατάλληλη μορφή ομοφωνίας (consensus)
  - Δύσκολο αλλά κρίσιμο σημείο
  - Διάφοροι μηχανισμοί

Resilient & Auditable

- Ανθεκτική
- Το δίκτυο θα πρέπει να είναι αρκετά ανθεκτικό σε (μεταξύ άλλων):
  - Προσωρινές αστοχίες κόμβων
  - Έλλειψη διαθεσιμότητας κάποιων κόμβων κάπου-κάπου
  - Διακυμάνσεις δικτύου και απορρίψεις διακινούμενων πακέτων
- Ελέγξιμη
- Υπάρχει από το σχεδιασμό του Blockchain ως αλυσίδα από hash
- Χρειάζεται όμως διασφάλιση ότι παραμένει η δυνατότητα με κάθε κόστος και η επιβεβαίωση συναλλαγών γίνεται ταχύτερα

Συναλλαγές Blockchain – (1/3)

- Για μεγάλο πλήθος συναλλαγών/δευτερόλεπτο επιλέγεται η ομαδοποίηση πολλών συναλλαγών σε block για
  - Σταθερότητα στο δίκτυο
  - Αντιμετώπιση του Sybil Attack (προσπάθεια επιρροής)
- Στάδια κάθε νέας συναλλαγής (βασική μορφή):
  1. Εκπέμπεται στο δίκτυο ώστε όλοι οι κόμβοι να γνωρίζουν πότε έλαβε χώρα (για αποφυγή double-spending)
  2. Ελέγχεται από τους κόμβους η αυθεντικότητά της (επικυρώνεται ή απορρίπτεται)
  3. Εκπέμπεται πάλι ως μέλος ομάδας (μπλοκ) πολλαπλών δοσοληψιών για να ενταχθεί στο blockchain

Συναλλαγές Blockchain – (2/3)

- Στάδια κάθε νέας συναλλαγής (συνέχεια):
  4. Ποιος κόμβος αποφασίζει το μπλοκ που ομαδοποιεί ορισμένες συναλλαγές; Ανάγκη για ομοφωνία
  5. Καθώς δεν υπάρχει η έννοια του καθολικού χρόνου, χρησιμοποιείται χρονοσήμανση με βάση τη σειρά άφιξης και πρόσθεσης κάθε μπλοκ στην αλυσίδα
  6. Μόλις όλοι οι κόμβοι αποδεχθούν ένα μπλοκ ομόφωνα, προστίθεται, συμπεριλαμβάνοντας το Hash του αμέσως προηγουμένου μπλοκ, στην αλυσίδα

Συναλλαγές Blockchain – (3/3)

- Σημαντικές λεπτομέρειες:
  - Τα δένδρα Merkle και η όλη δομή blockchain βοηθούν στον αποδοτικό έλεγχο εγκυρότητας μίας συναλλαγής
  - Οι υπόλοιποι κόμβοι δεν χρειάζεται να μοιράζονται πλήρη μπλοκ δεδομένων για να επικεβαιώνεται η συμμετοχή μιας συναλλαγής σε ένα μπλοκ
  - Χρειάζεται αποδοτικός τρόπος αποθήκευσης (για τις συναλλαγές και τα μεταδεδομένα τους)

Μηχανισμοί Κατανεμημένης Ομοφωνίας – (1)

- Για πρακτικούς λόγους εκπέμπεται στο δίκτυο, όχι κάθε μια συναλλαγή, αλλά ένα block προς επικύρωση και ένταξη στο blockchain
- Ποιός κόμβος όμως προτείνει ένα block;
  - Εάν γίνεται τυχαία, τότε πρέπει να μεσολαβεί ένα ικανό χρονικό διάστημα μεταξύ προτάσεων, ώστε να μην “πέφτουν” όλες μαζί
  - Ανάγκη για μηχανισμό ομοφωνίας block by block

Μηχανισμοί Κατανεμημένης Ομοφωνίας – (2)

- Μηχανισμοί ομοφωνίας από τη Θεωρία Παιγνίων
- Διασφάλιση ότι όλοι οι κόμβοι κερδίζουν τα μέγιστα, σεβόμενοι τους κανόνες:
  - Επιβράβευση των τιμίων και τιμωρία των κακών
    - Τι γίνεται στο Bitcoin, όπου μπορεί κάποιος να έχει πολλαπλές ταυτότητες (με πραγματική ανωνυμία);
    - Δύσκολη η τιμωρία, αλλά εύκολη (και επιθυμητή!) η επιβράβευση
  - Δεν μπορεί να γνωρίζει το σύστημα αν ένας επιλεγμένος κόμβος είναι κακοπροαίρετος ή τίμιος

Απόδειξη Εργασίας (PoW-Proof of Work)

- Αρκετά παλιός και δημοφιλής λόγω Bitcoin
- Κεντρική ιδέα:

  Γίνεται μια εργασία εξόρυξης (mining) πριν προταθεί ένα μπλοκ συναλλαγών στο δίκτυο

  Δύσκολη στο να γίνει (υπολογιστικά και χρονικά), αλλά εύκολη στην επικύρωση
- Π.χ., όπως για spam e-mail
  - Αν χρειάζεται πολλή δουλειά για να αποσταλεί ένα μήνυμα προς ένα αποστολέα, τότε η αποστολή προς πολλούς αποφεύγεται

Απόδειξη Εργασίας (PoW-Proof of Work)

- Στο blockchain βοηθάει με δυο τρόπους:

1. Θα χρειαστεί σίγουρα κάποιος χρόνος

2. Αν κάποιος κόμβος προσπαθήσει να εισάγει μια ψεύτικη δοσοληψία, τότε η απόρριψη του block από τους υπόλοιπους θα είναι πολύ δαπανηρή για αυτόν

PoW – Κάποιες Λεπτομέρειες

- Η δυσκολία της απαιτούμενης εργασίας θα προσαρμόζεται για να ελέγχεται η ταχύτητα δημιουργίας νέων block
- Φυσιολογικά, όσο πιο μεγάλη η υπολογιστική προσπάθεια κάποιου κόμβου, τόσο περισσότερες οι πιθανότητες να είναι ο πρώτος που θα προτείνει ένα block
  - Εάν πάλι γίνεται με τυχαίο τρόπο η επιλογή, ίσως δεν θα έχουν κίνητρο συμμετοχής στην υποδομή οι «ισχυροί»

PoW – Υπολογιστικό Πρόβλημα

- Computational puzzle που απαιτεί υπολογισμούς και χρόνο
- Π.χ., η εύρεση ενός αριθμού του οποίου το hash να ξεκινάει με «0», γίνεται με διαδοχικές δοκιμές. Η δυσκολία εντείνεται όσο μεγαλώνει το πρόθεμα του επιθυμητού hash:
  - Πιο δύσκολο το «00xxxxxxx»
  - Ακόμη πιο δύσκολο το «000xxxxxx»
- Όταν πολλοί κόμβοι προσπαθούν να βρουν τη λύση, δεν γνωρίζουμε ποιός θα προλάβει πρώτος
- Σε δημόσια blockchain, οι κόμβοι που επενδύουν τους υπολογιστικούς τους πόρους πρέπει να ανταμείβονται για τίμια συμπεριφορά

Proof of Stake (PoS)

- Δεν έχουμε επιβράβευση των miners με παραγωγή νέων νομισμάτων αλλά αλλά τέλη συναλλαγών (fee) για τους επικυρωτές (validators)
- Το συνολικό ποσό νομισμάτων υπάρχει από την αρχή και είναι σταθερό
- Οι επικυρωτές δεσμεύουν το μερίδιό τους (υποθηκεύουν το ποσό που διακυβεύεται) για να μπορούν να μετέχουν σε επικυρώσεις συναλλαγών
- Η πιθανότητα για νέο block είναι ανάλογη του μεριδίου του επικυρωτή
- Καταναλώνεται σαφώς μικρότερη ενέργεια έναντι του mining
- Παραλλαγές: Naive PoS, delegated PoS (DPoS στο Bitshares), chain-based PoS, BFT-style PoS, και Casper PoS (Ethereum)

PBFT – (1)

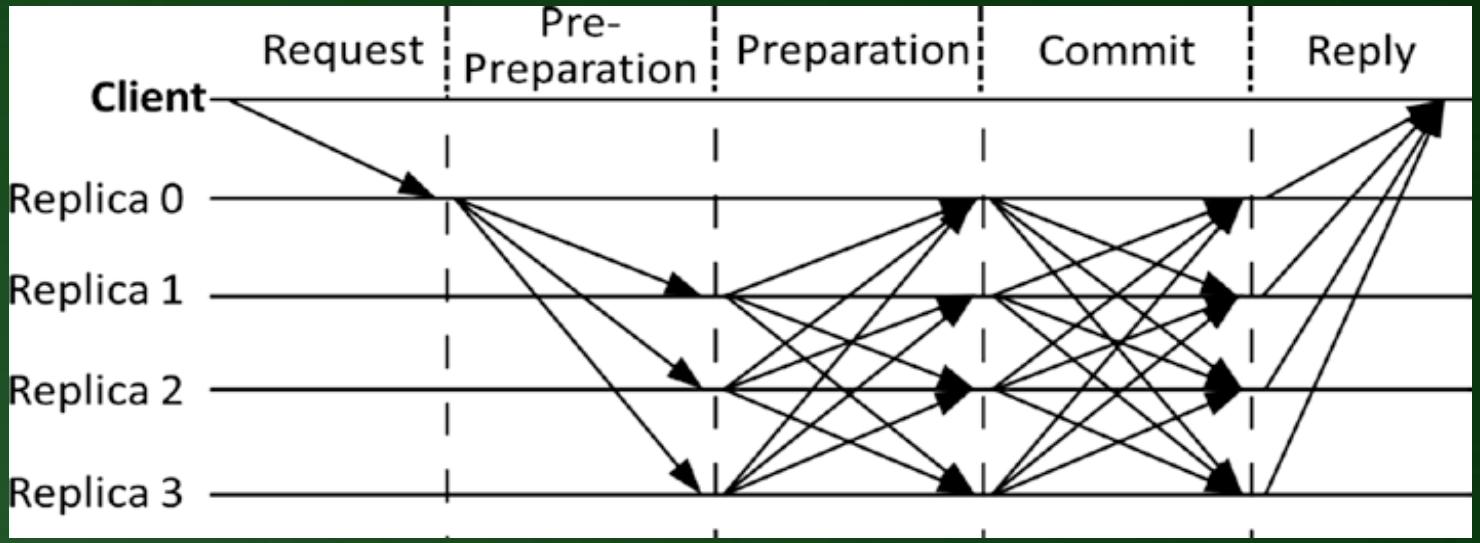
- Practical Byzantine Fault Tolerance
- Χρησιμοποιείται από Hyperledger, Stellar, Ripple
- Μοιάζει με PoS (no rewards), αλλά έχει πιο πολύπλοκη υλοποίηση
- Πολύ δημοφιλής
- Δυσχεραίνει την ανωνυμία

PBFT – (2)

Για κάθε νέο αίτημα, κάθε κόμβος εκτελεί τον υπολογισμό επικύρωσης με βάση τη ρέπλικά του και στέλνει το αποτέλεσμα στους υπόλοιπους.

Μετά, το συγκρίνει με τα αποτελέσματα των υπολοίπων και καταλήγει σε μια απόφαση που κοινοποιείται προς όλους.

Βάσει πλειοψηφίας, οι κόμβοι καταλήγουν στην τελική ομοφωνία



Εφαρμογές Blockchain - 1

- Υπάρχει τεράστια ποικιλία
  - Άλλες έχουν έναν web server ως front-end, με το blockchain ως μία βάση δεδομένων back-end
  - Άλλες είναι πλήρως αποκεντρωμένες χωρίς κεντρικό server
    - Π.χ., στο Bitcoin κάθε “αίτημα” εκπέμπεται προς όλο το δίκτυο
    - Μπορεί όμως να υπάρχει μια εφαρμογή σε έναν κεντρικό web server, που να εκκινεί ενημερώσεις Bitcoin όταν ζητηθεί

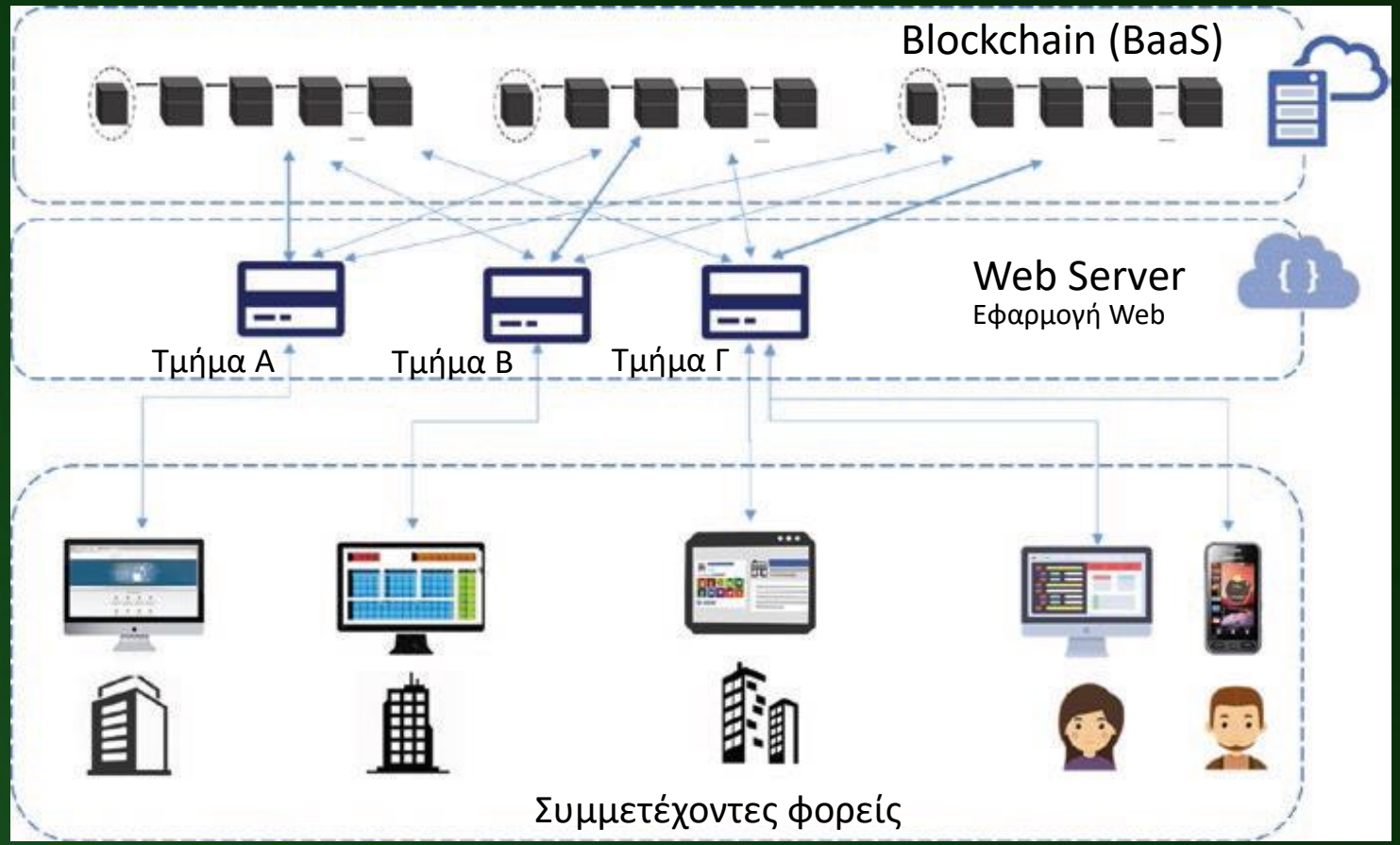
Εφαρμογές Blockchain - 2

- Εφαρμογές τύπου “public blockchain”: αποτελούν την πιο γνήσια κατηγορία αποκεντρωμένων εφαρμογών. Π.χ., Bitcoin.

- Εφαρμογές τύπου “private blockchain”: γίνεται συνήθως χρήση cloud services, όπως Azure (Microsoft), Bluemix (IBM), κ.ά.

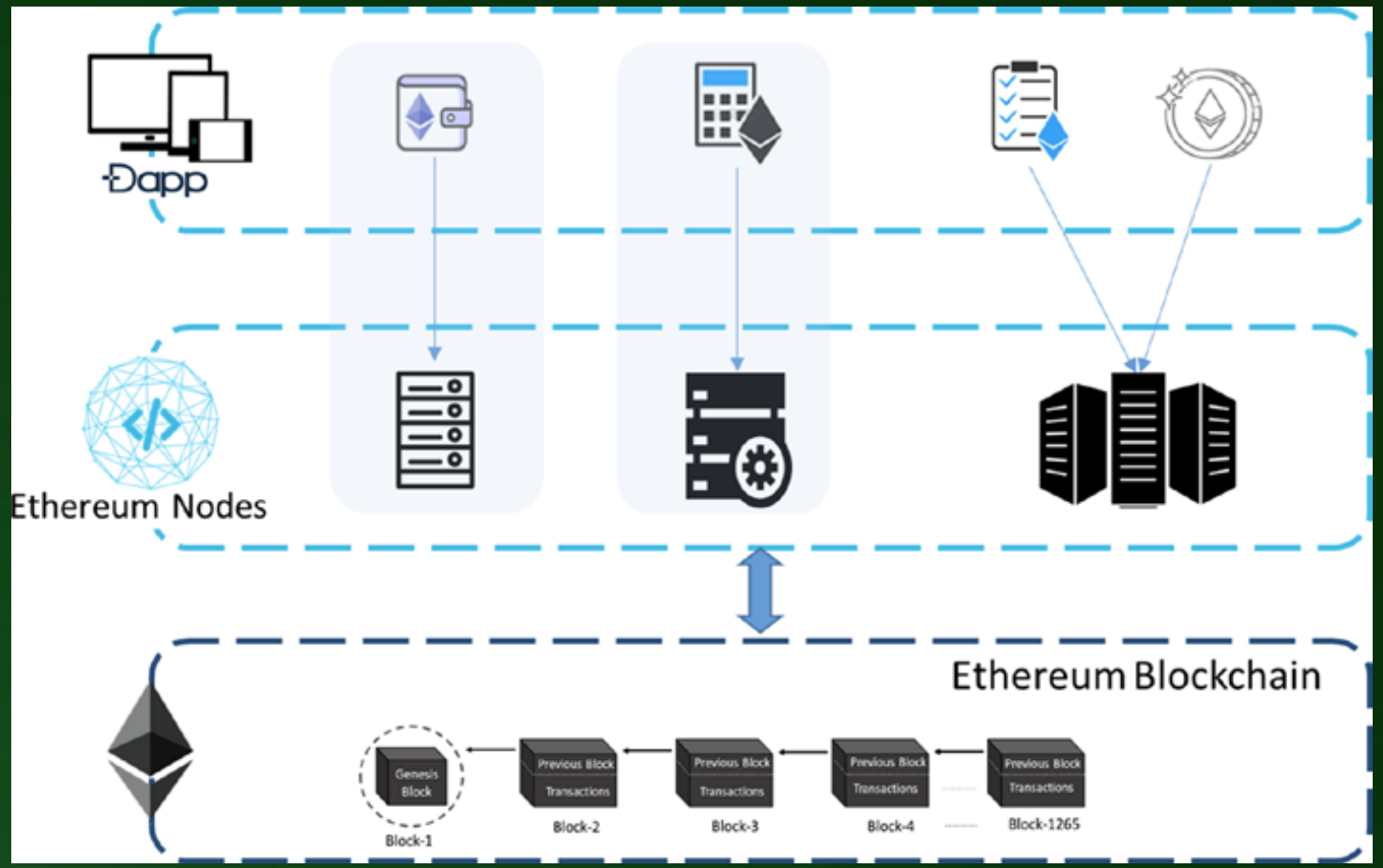
Σύστημα Blockchain με Cloud service

- Στα περισσότερα “private blockchain” αποφεύγεται το PoW για οικονομία υπολογιστικών πόρων και ηλεκτρικής ενέργειας
- PoS: ο πιο συχνά χρησιμοποιούμενος μηχανισμός ομοφωνίας



DApp (Decentralized App) σε δίκτυο Ethereum

- Permissioned on private Ethereum
- Permissionless on public Ethereum
- DApps για διαφορετικές περιπτώσεις χρήσης, αλλά επάνω από το ίδιο Ethereum Blockchain



Κλιμακώνοντας το Blockchain

- Από την φύση του δύσκολο στην κλιμάκωση
  - Π.χ., εάν παραγγείλουμε καφέ, δεν μπορούμε να πληρώσουμε με Bitcoin αφού χρειάζεται ~1 ώρα να επικυρωθεί η συναλλαγή
- Προσθήκη περισσοτέρων υπολογιστικών κόμβων βοηθάει σε Κατανεμημένα Συστήματα, αλλά όχι σε Αποκεντρωμένα, όπως είναι το Blockchain
  - Αντιθέτως αυξάνεται η καθυστέρηση!
- Μεγάλη προσπάθεια από πολλούς για επίλυση του προβλήματος

Αξιοποίηση Blockchain

- Η ανάπτυξη εφαρμογών blockchain περιορίζεται μόνο από την ευρηματικότητα
  - Καθαρές σκέτες εφαρμογές blockchain
  - Εφαρμογές που αξιοποιούν blockchain ως backend μόνο
  - Υβριδικές εφαρμογές που χρησιμοποιούν παραδοσιακές εφαρμογές σε συνδυασμό με χρήση blockchain μόνο για κάποιους ειδικούς σκοπούς
- Γενικώς παραμένει το ζήτημα της κλιμάκωσης

Ζητήματα κλιμάκωσης

- Εμφανίζονται περισσότερο σε public blockchain
  - Κάθε κόμβος (full node) διατηρεί αντίγραφο του blockchain, επικυρώνει συναλλαγές και block, εξυπηρετεί αιτήσεις άλλων (light) κόμβων, κ.ά.
  - Προσθέτουμε servers σε συγκεντρωτικά συστήματα για κλιμάκωση αλλά σε αποκεντρωμένα συστήματα μεγαλώνει η αστάθεια (latency) δικτύου
  - Όσο περισσότεροι οι κόμβοι, τόσο περισσότερες οι δοσοληψίες στο δίκτυο, άρα και οι απαιτούμενοι πόροι επεξεργασίας
- Στα private blockchain μπορούν να
  - επιβληθούν ειδικές απαιτήσεις υπολογιστικών και δικτυακών πόρων
  - μεταφέρονται υπολογισμοί εκτός του blockchain

Τεχνικές Κλιμάκωσης

- Υπολογισμός εκτός αλυσίδας (Off-Chain)
- Σπάσιμο κατάστασης (Sharding Blockchain State)

Off-Chain Computation – (1)

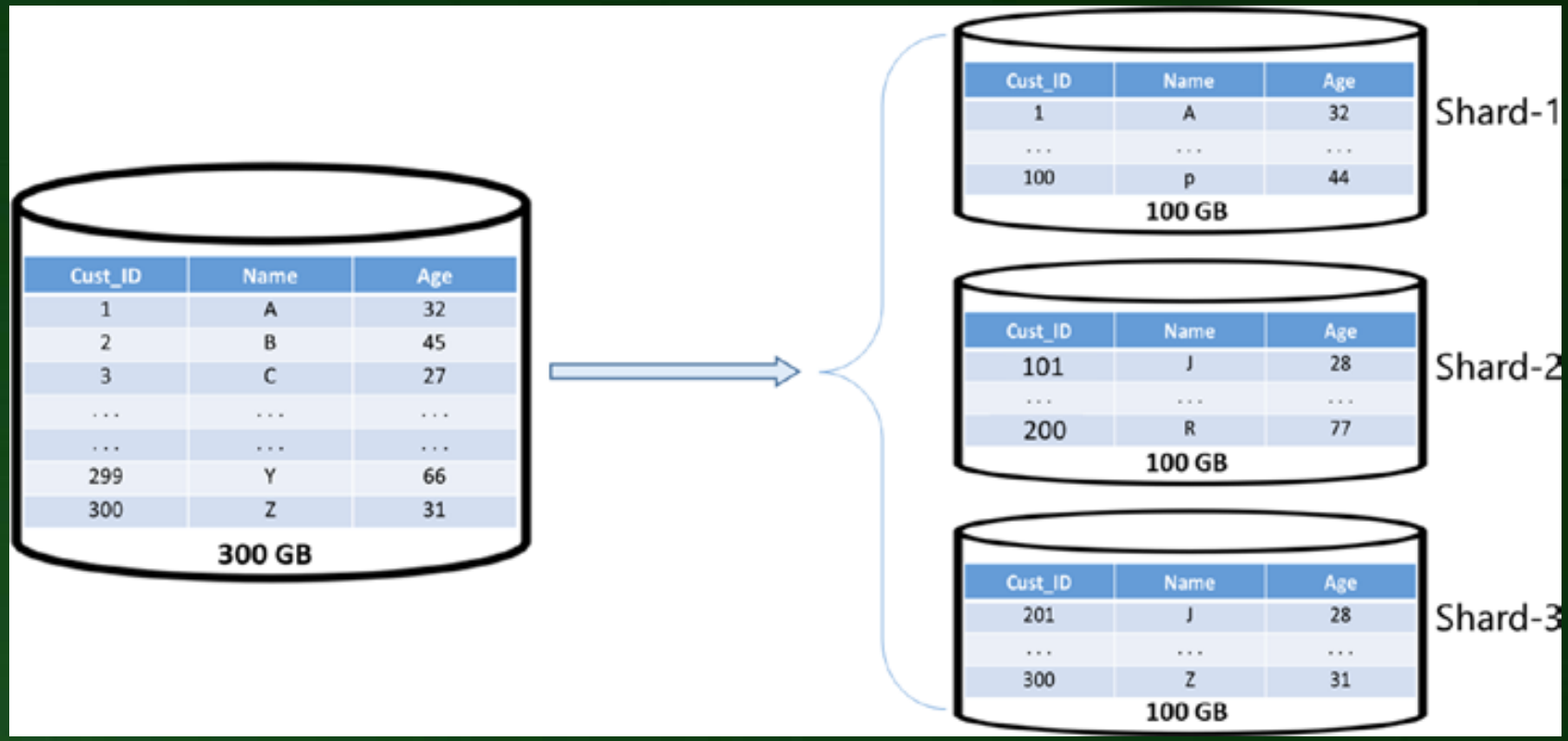
- Κεντρική ιδέα: Αφαίρεση σχεδόν όλου του υπολογιστικού φόρτου. Χρήση του blockchain μόνον για αποθήκευση
- Το πώς θα γίνει κάτι τέτοιο δεν είναι σαφώς καθορισμένο και εξαρτάται από τις συνθήκες, π.χ.:
  - με παράπλευρες αλυσίδες (side chains) – άρα όχι γνήσιο blockchain
  - “Ligthning Network” και “Zerocash” (κυρίως για ιδιωτικότητα) για Bitcoin, “Raiden Network” για Ethereum

Off-Chain Computation – (2)

- Πρόβλημα: η διαφορετική αντίληψη της κατάστασης συστήματος
  - Bitcoin: Χωρίς κατάσταση (Stateless), δεν τηρεί κατάσταση λογαριασμών, αλλά μόνο συναλλαγές
    - νέα συναλλαγή γίνεται αν καταναλωθεί η προηγούμενη
  - Ethereum: Με Κατάσταση (Stateful), το υπόλοιπο λογαριασμού είναι μέρος της πληροφορίας κατάστασης
    - καταλαμβάνει σημαντικό χώρο σε κάθε κόμβο

Sharding Blockchain State – (1)

- Προέρχεται από τις Β.Δ.
- Οριζόντια τμηματοποίηση για παράλληλο r/w



Sharding Blockchain State – (2)

- Κεντρική Ιδέα στο Blockchain:
  - Κάθε κόμβος κατεβάζει και τηρεί μόνον τα μέρη (shards) του blockchain που τον αφορούν άμεσα
  - Άρα κάθε συναλλαγή μεταδίδεται και επικυρώνεται μόνον από τους σχετιζόμενους κόμβους
- Πρόβλημα όταν χρειάζεται επικοινωνία μεταξύ διαφόρων shard