Τεχνολογίες Blockchain & Αποκεντρωμένες Εφαρμογές

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

Διάλεξη #01

Εισαγωγή

Σκελετός Μαθήματος

1	Εισαγωγή – Βασικές έννοιες
2	Κρυπτογραφία & Συνόψεις
3	Πώς λειτουργεί το Blockchain 1
4	Πώς λειτουργεί το Blockchain 2
5	Μεταγλώττιση και Δημοσίευση Συμβολαίων
6	Εισαγωγή στο Ethereum
7	Εισαγωγή στη Solidity
8	Ανάπτυξη DApp με Javascript
9	Λογαριασμοί, Κλειδιά και Διευθύνσεις στο Ethereum
10	Συναλλαγές, Μπλοκ Συναλλαγών, Tries και MPTs
11	PoS στο Ethereum
12	Ανάπτυξη DApp με React
13	Δημοσίευση εφαρμογής DApp

Ύλη Μαθήματος

- Υλικό μαθήματος
  - διαφάνειες θεωρίας
  - εργαστηριακές δραστηριότητες
  - εργασίες
  - ενδεικτική βιβλιογραφία

Βιβλιογραφία

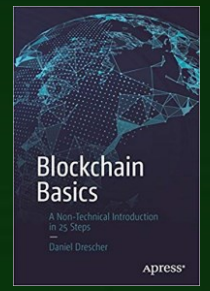
- Αλυσίδες Συστοιχιών (Blockchain)
  - Κωδικός Βιβλίου στον Εύδοξο: 118392908
  - Έκδοση: 1/2023
  - Συγγραφείς: Πατρικάκης Χαράλαμπος, Κόγιας Δημήτριος, Λελίγκιου Ελένη
  - ISBN: 978-618-5726-49-2
  - Τύπος: Ηλεκτρονικό Βιβλίο
  - Διαθέτης (Εκδότης): Ελληνικά Ακαδημαϊκά Ηλεκτρονικά Συγγράμματα και Βοηθήματα - Αποθετήριο "Κάλλιπος"

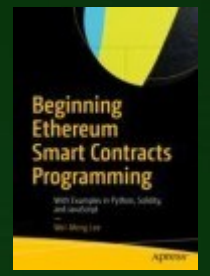
- Mastering Ethereum, Andreas M. Antonopoulos, O' Reilly, Pearson 2019

- Solidity Programming Essentials, Ritesh Modi, Packt, 2018

Συμπληρωματική Βιβλιογραφία (Εύδοξος)

- Beginning Blockchain [electronic resource]
  - Κωδικός Βιβλίου στον Εύδοξο: 91677528
  - Έκδοση: 1st ed./2018
  - Συγγραφείς: Bikramaditya Singhal / Gautam Dhameja / Priyansu Sekhar Panda
  - ISBN: 9781484234440
- Blockchain Basics [electronic resource]
  - Κωδικός Βιβλίου στον Εύδοξο: 75482546
  - Έκδοση: 1st ed./2017
  - Συγγραφείς: Daniel Drescher
  - ISBN: 9781484226049
- Beginning Ethereum Smart Contracts Programming [electronic resource]
  - Κωδικός Βιβλίου στον Εύδοξο: 91687561
  - Έκδοση: 1st ed./2019
  - Συγγραφείς: Wei-Meng Lee
  - ISBN: 9781484250860





Βαθμολογία

Ο τελικός βαθμός προκύπτει από:

- Ενδιάμεση Εργασία: 30%
- Τελική Εργασία: 70%

Εισαγωγή

- Τι θα δούμε για το Blockchain σήμερα:
  - Περί τίνος πρόκειται
  - Πώς εξελίχθηκε
  - Τι μορφή έχει (επισκόπηση)
  - Η σημερινή του σημασία με μερικά παραδείγματα από σενάρια χρήσεως

Περί τίνος πρόκειται

- Σύντομη Επισκόπηση Δικτύωσης
  - δίκτυα μεταγωγής κυκλώματος (Circuit Switching)
  - δίκτυα μεταγωγής πακέτου (Packet Switching)
    - TCP/IP, αποκεντρωμένη επικοινωνία
  - WWW (World Wide Web)
    - Web-banking, συγκεντρωτική λειτουργία

Εισαγωγή

- Τι θα δούμε για το Blockchain σήμερα:
  - Περί τίνος πρόκειται
  - Πώς εξελίχθηκε
  - Τι μορφή έχει (επισκόπηση)
  - Η σημερινή του σημασία με μερικά παραδείγματα από σενάρια χρήσεως

Κλασσικές Συναλλαγές – Εξέλιξή τους

- Αρχικά γίνονταν μέσω ανταλλαγών φυσικών αντικειμένων (barter trade)
  - Π.χ., 2 βόδια για 10 πήλινα αγγεία
- Κατόπιν μέσω νομισμάτων (χρυσά, ασημένια, χάλκινα)
- Μετά μέσω «Παραστατικών» νομισμάτων (fiat currency)

Κλασσικές Συναλλαγές – Τράπεζες

- Όλα τα προηγούμενα απαιτούν φυσική παρουσία των δύο μερών (για να υπάρχει «Πίστη»)
- Διαφορετικά χρειάζεται κάποιος ενδιάμεσος που να παρέχει την Πίστη
- Τράπεζες

Τράπεζα και Μειονεκτήματα

- Πρόκειται για ένα κεντρικοποιημένο σύστημα (τράπεζα)
- Τρίτος (Μεσάζων) που εγγυάται την Πίστη των συναλλαγών, αλλά προσθέτει:
  - Κόστος (για παρεχόμενες υπηρεσίες)
  - Χρόνο (για εκκαθάριση συναλλαγών)
  - Έχει απόλυτη σχεδόν εξουσία (που διαφθείρει)

Οι Τράπεζες δεν είναι το μόνο Παράδειγμα

- Οίκοι εκκαθάρισης (clearing houses)
  - Χρηματιστηριακές Συναλλαγές
  - Digital Rights management
- Υπηρεσίες Συμβολαίων
- Υπηρεσίες Μητρώων εν γένει

Βασικό Ερώτημα

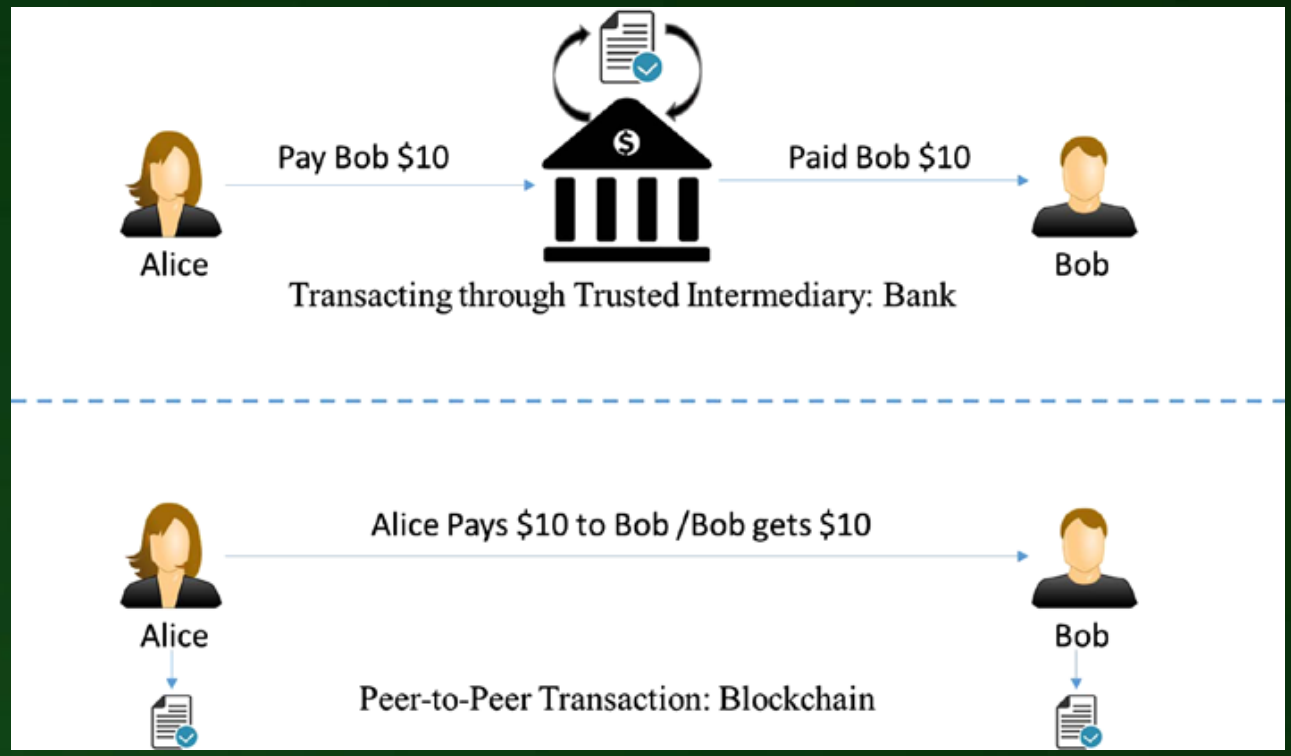
- Αφού το Διαδίκτυο προσφέρει δυνατότητα άμεσων συναλλαγών από το ένα άκρο της γης ως το άλλο, μήπως μπορούμε να τις πραγματοποιούμε χωρίς τρίτους ενδιάμεσους;
  - Άρα χωρίς πρόσθετα κόστη και καθυστερήσεις;

Εισαγωγή

- Τι θα δούμε για το Blockchain σήμερα:
  - Περί τίνος πρόκειται
  - Πώς εξελίχθηκε
  - Τι μορφή έχει (επισκόπηση)
  - Η σημερινή του σημασία με μερικά παραδείγματα από σενάρια χρήσεως

Blockchain – Η Εναλλακτική Πρόταση

- Τεχνολογία που προσφέρει «Πίστη» στις συναλλαγές
- Σύστημα συναλλαγών P2P χωρίς τη διαμεσολάβηση έμπιστων τρίτων μερών



Blockchain – Βασικά Χαρακτηριστικά (1)

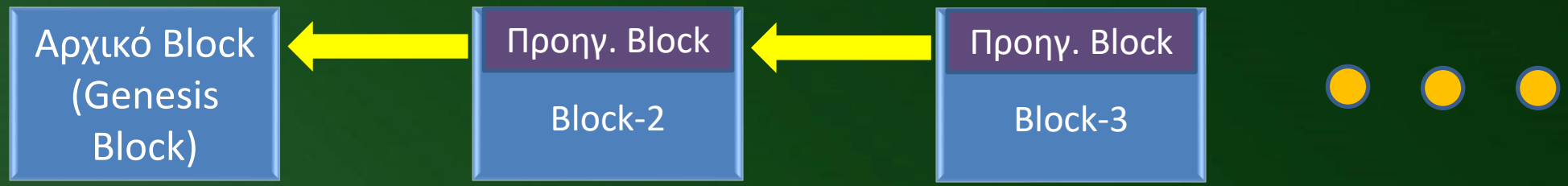
- Από τη μεριά των επιχειρήσεων: Λογιστικό Βιβλίο («Καθολικό») συναλλαγών διαμοιραζόμενο, αποκεντρωμένο και ανοικτό
  - Η Βάση Δεδομένων που το υλοποιεί επιτρέπει εγγραφές τύπου `append` μόνο.
  - Καμία εγγραφή δεν μπορεί να αλλάξει ή να διαγραφεί.
  - Όλες οι εγγραφές αντιγράφονται σε όλα τα αντίγραφα που υπάρχουν στους διάφορους κόμβους

Blockchain – Βασικά Χαρακτηριστικά (2)

- Πρόκειται για ένα επίπεδο πάνω από το Διαδίκτυο
- Συνυπάρχει στο Διαδίκτυο με άλλες τεχνολογίες
- Ένας από τους στόχους είναι η πλήρης αποκέντρωση στο πλαίσιο του ανοικτού TCP/IP
  - το Bitcoin είναι ανοικτού κώδικα

Η Βασική Δομή Δεδομένων

- Είναι το “Block”
  - Ομάδα από συναλλαγές με έναν δείκτη στο αμέσως προηγούμενο (χρονικά) Block συναλλαγών
  - Αντίγραφα ίδιων συναλλαγών σε κάθε κόμβο



Block

- Δύο βασικά μέρη:
  - Κεφαλίδα
  - Περιεχόμενο σώματος

Block

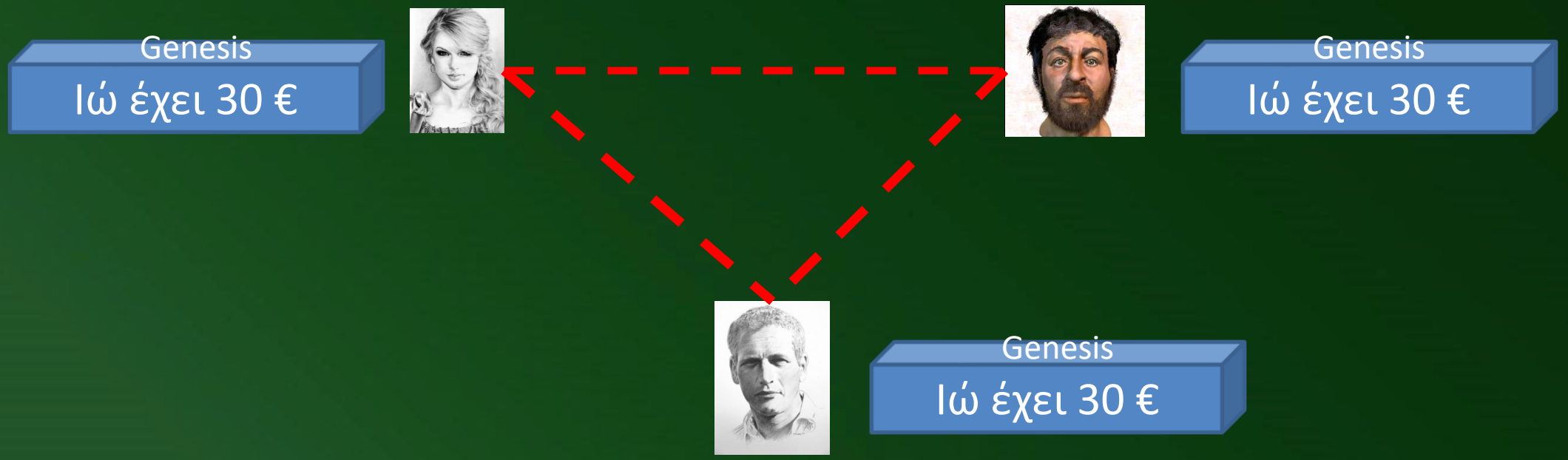
- Κάθε κεφαλίδα περιέχει τουλάχιστον
  - Δείκτη στο προηγούμενο Block
  - Hash του προηγούμενου Block
    - για να μην μπορεί να αλλοιωθεί το περιεχόμενό του

Block

- Περιεχόμενο σώματος
  - Επικυρωμένη λίστα συναλλαγών
    - Π.χ. ποσά, διευθύνσεις εμπλεκομένων, κ.ά.
- Έχοντας το τελευταίο block, μπορεί κανείς να προσπελάσει όλα τα προηγούμενα block στην αλυσίδα

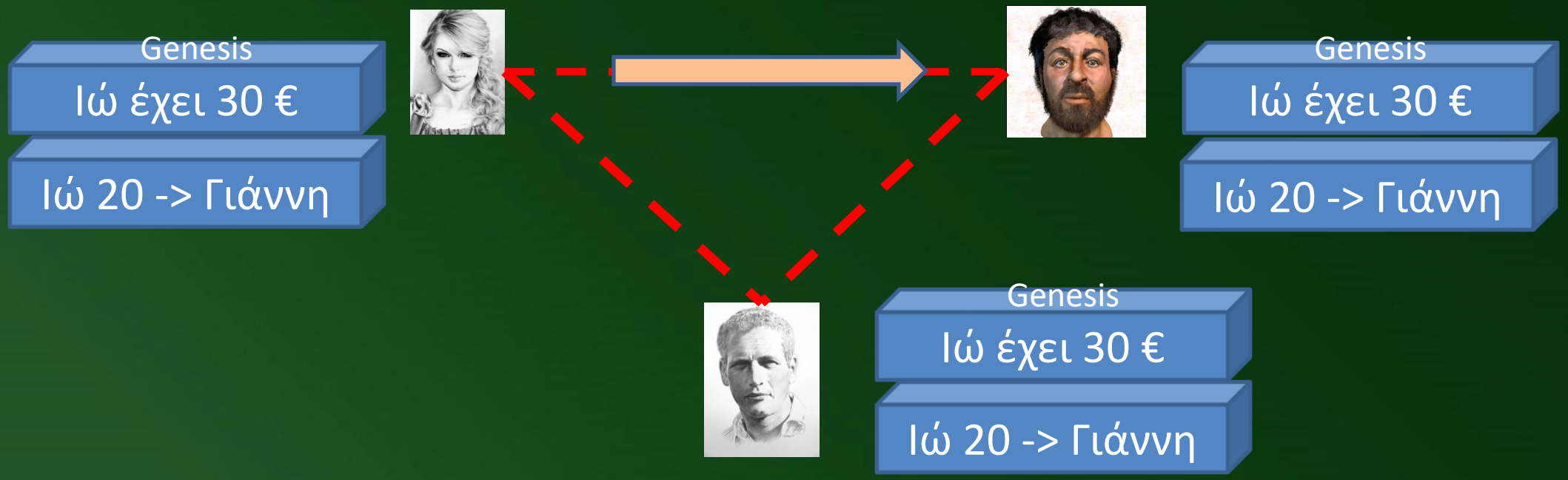
Παράδειγμα Συναλλαγών με Blockchain – (1)

- Η Ιώ έχει 30 Ευρώ, που είναι η πρώτη εγγραφή (genesis) και το γνωρίζουν οι υπόλοιποι δύο κόμβοι (Γιάννης, Κώστας)



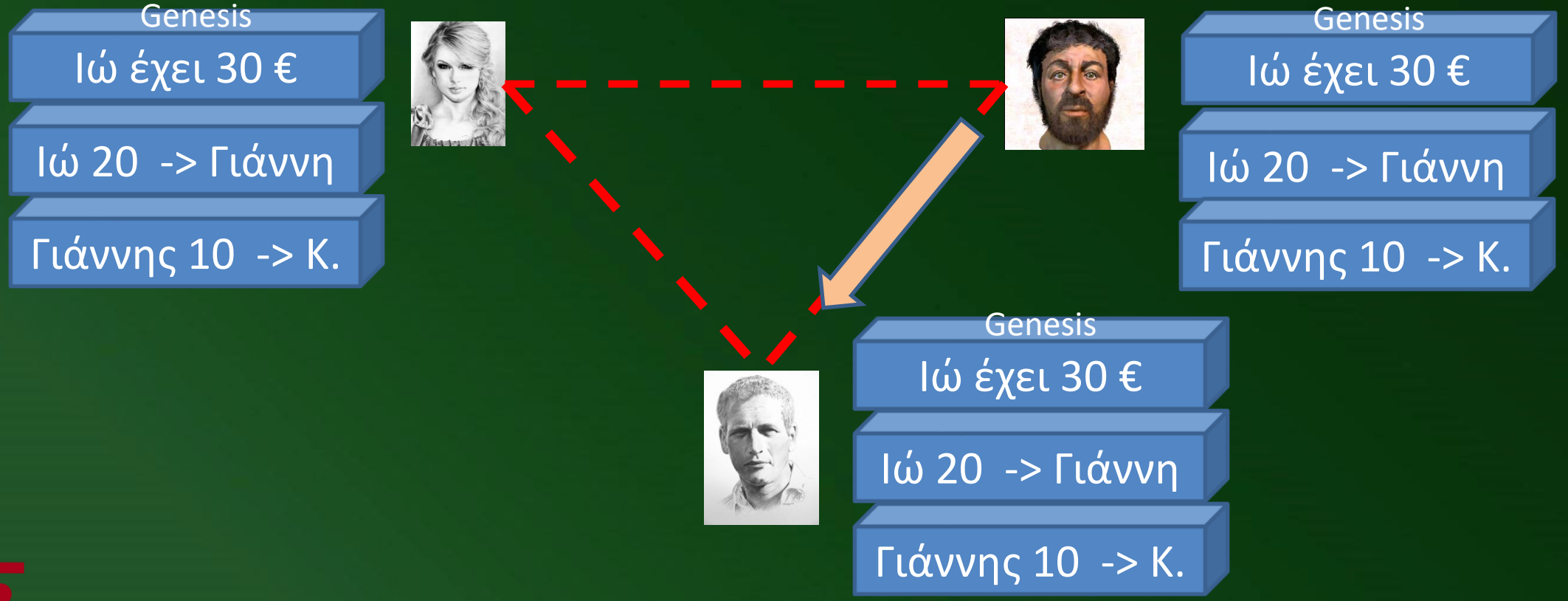
Παράδειγμα Συναλλαγών με Blockchain – (2)

- Η Ιώ πληρώνει 20 Ευρώ στον Γιάννη



Παράδειγμα Συναλλαγών με Blockchain – (3)

- Ο Γιάννης πληρώνει 10 Ευρώ στον Κώστα



Προσοχή στο Νόημα των Όρων – 1

- *Κατανεμημένο* Σύστημα
  - *Συγκεντρωτικά Κατανεμημένο* Σύστημα
    - 1 κύριος κόμβος που διαιρεί και διανέμει τις εργασίες ή τα δεδομένα στους υπολοίπους κόμβους (π.χ., Hadoop)
  - *Αποκεντρωμένα Κατανεμημένο* Σύστημα
    - Δεν υπάρχει ο κύριος κόμβος, αλλά η επεξεργασία είναι κατανεμημένη
    - Το Blockchain είναι κάτι τέτοιο

Προσοχή στο Νόημα των Όρων – 2

- Συγκέντρωση έναντι Αποκέντρωσης
  - Τεχνική αρχιτεκτονική
    - Συγκεντρωτική - Αποκεντρωμένη
  - Πολιτική αντίληψη
    - Ο έλεγχος που ένας/πολλοί έχουν σε ένα σύστημα
  - Λογική αντίληψη
    - Το πώς φαίνεται ότι είναι
      - π.χ., αν το κόψετε στην μέση τα επί μέρους υποσυστήματα συνεχίζουν να λειτουργούν ή όχι;

Προσοχή στο Νόημα των Όρων – 3

- Εταιρεία: Συγκεντρωτική ως προς τους 3 τρόπους
- BitTorrent: Αποκεντρωτικό ως προς τους 3 τρόπους
- Δίκτυο Διανομής Περιεχομένου (CDN): Αποκεντρωτικό αρχιτεκτονικά και λογικά, αλλά συγκεντρωτικό πολιτικά
- Blockchain: Αποκεντρωτικό αρχιτεκτονικά και πολιτικά, αλλά συγκεντρωτικό λογικά
  - Υπάρχει μια μόνον κατάσταση (συμφωνημένη από κοινού) και το όλο σύστημα συμπεριφέρεται ως 1 Η/Υ

Μειονεκτήματα Συγκεντρωτικών Συστημάτων

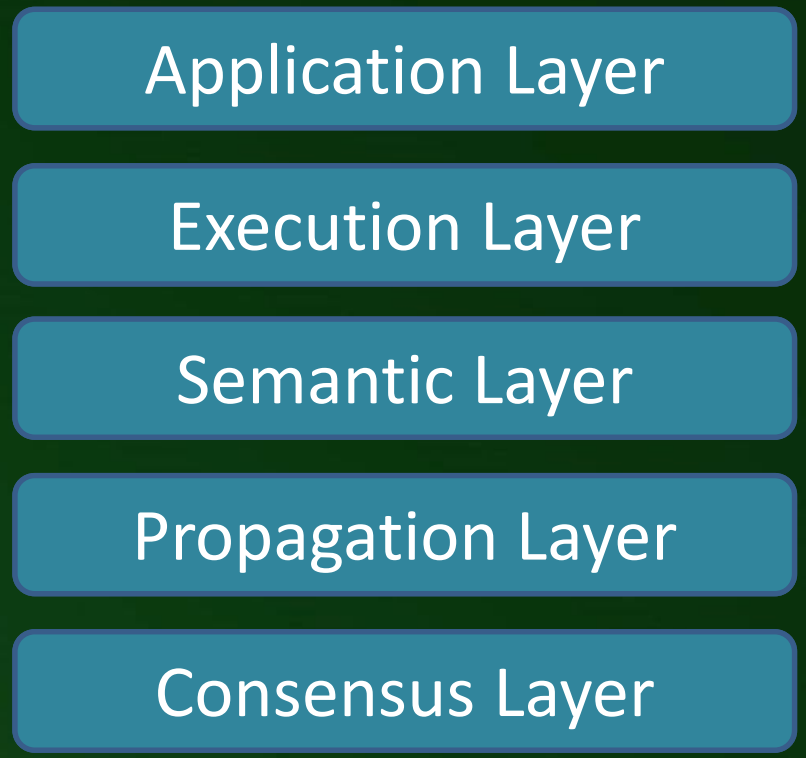
- Μοναδικό (κεντρικό) σημείο αποτυχίας
- Πιο ευάλωτα σε επιθέσεις (άρα λιγότερο ασφαλή)
- Συγκέντρωση εξουσίας μπορεί να οδηγήσει σε αντιδεοντολογικές πρακτικές
- Κλιμάκωση: είναι συχνά δύσκολη

Πλεονεκτήματα Αποκεντρωτικών Συστημάτων

- Αν και πιο δύσκολα στον σχεδιασμό, υλοποίηση και διαχείριση:
  - Δεν έχουν ένα (κεντρικό) σημείο αποτυχίας
    - άρα πιο σταθερά και ανεκτικά σε σφάλματα
  - Ανθεκτικότερα σε επιθέσεις
  - Συμμετρικά όπου όλοι οι κόμβοι έχουν την ίδια εξουσία
    - οπότε λιγότερες αντιδεοντολογικές πρακτικές και πιο δημοκρατική λειτουργία

Επίπεδα του Blockchain

- Δεν υπάρχει καθολικά αποδεκτή ταξινόμηση
- Αυτό που εμφανίζεται εδώ δεν πρέπει να συγχέεται με την στοίβα TCP/IP



Application Layer

- Εδώ ανήκει η κωδικοποίηση των επιθυμητών λειτουργιών σε ανάπτυξη εφαρμογής για τον τελικό χρήστη

- Περιλαμβάνει συνήθη στοίβα εργαλείων ανάπτυξης:
  - Server/client προγραμματιστικές δομές, scripting, API, πλαίσια ανάπτυξης κ.ά.

Execution Layer

- Εδώ εκτελούνται οι εντολές που ζητώνται από το Application Layer
  - Απλές εντολές ή πολλαπλές (π.χ. για έξυπνα συμβόλαια)
  - Bitcoin: απλά script που δεν είναι Turing-complete
  - Ethereum και Hyperledger: πολύπλοκες εντολές
    - Ethereum code σε Solidity και Ethereum Virtual Machine
    - Hyperledger chaincode σε Java ή Go και docker images

Semantic Layer

- Επικύρωση των συναλλαγών που εκτελούνται παραπάνω
- Εδώ ορίζονται οι κανόνες
  - Bitcoin: δεν έχει λογαριασμούς
  - Ethereum: έχει λογαριασμούς
    - smart contract: ειδικός τύπος λογαριασμού με εκτελέσιμο κώδικα και καταστάσεις

  οι δομές δεδομένων
  - π.χ. Merkle trees

  και πώς συνδέονται τα block μεταξύ τους

Propagation Layer

- Ασχολείται με την επικοινωνία P2P
- Αρκετά ζητήματα σχετικά με τη διάδοση των συναλλαγών/block:
  - Πώς οι κόμβοι βρίσκουν ο ένας τον άλλον
  - Πώς συνομιλούν (latency)
  - Πώς συγχρονίζονται (ως προς τις συναλλαγές)

Consensus Layer

- Ασχολείται με το πώς όλοι κόμβοι συμφωνούν σε μία συνεπή κατάσταση του «Καθολικού»
- Διάφοροι τρόποι επίτευξης τέτοιας ομοφωνίας:
  - Εξαρτώνται από το σενάριο χρήσης
    - είδος blockchain, κίνητρα συμμετοχής κ.ά.
  - Στα Ethereum και Bitcoin, μέσω του “mining”
  - Μηχανισμοί/πρωτόκολλα ομοφωνίας:
    - Proof of Stake (PoS), delegated PoS (dPoS), Practical Byzantine Fault Tolerance (PBFT), κ.ά.

Συμπερασματικά…

- Η τεχνολογία Blockchain είναι πολύ σημαντική, αφού ένα συγκεντρωτικό σύστημα έχει ζητήματα:
  - Πίστης, Ασφάλειας, Ιδιωτικότητας, Κόστους, Χρόνου
- Δεν είναι όμως πανάκεια
- Έως τώρα η πιο γνωστή εφαρμογή είναι τα Κρυπτονομίσματα, με κυριότερο το Bitcoin
- Μεγάλες εταιρείες το διερευνούν για διάφορες χρήσεις