ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μελέτη τεχνολογιών για συναλλαγές με ψηφιακά νομίσματα

Λαμπριανίδης Αναστάσιος (mai19036)

Επιβλέπων Καθηγητής:
Παπαδημητρίου Παναγιώτης

Περιεχομενα

- Εισαγωγή
- Blockchain – Λογισμικό τεχνολογία
- Ψηφιακό χρήμα
- Βασικές έννοιες του Bitcoin
- Μεθοδολογία
- Λειτουργία Hyperledger
- Συμπεράσματα
- Βιβλιογραφία

ΣΤΟΧΟΙ - ΣΥΝΕΙΣΦΟΡΑ

- Κατανόηση της λειτουργίας Blockchain
- Κατανόηση λειτουργίας και τρόποι Εξόρυξης (Mining)
- Τρόπος δημιουργίας ενός δικτύου με τη χρήση του Fabric & Caliper

BLOCKCHAIN – ΛΟΓΙΣΜΙΚΟ ΤΕΧΝΟΛΟΓΙΑ (1/6)

- **ΤΙ ΕΙΝΑΙ ΤΟ BLOCKCHAIN.**

1. Δημόσια Blockchain.
2. Ιδιωτικά Blockchain.

- **ΑΠΟΤΕΛΕΙΤΑΙ ΑΠΟ ΤΡΙΑ ΣΤΟΙΧΕΙΑ:**

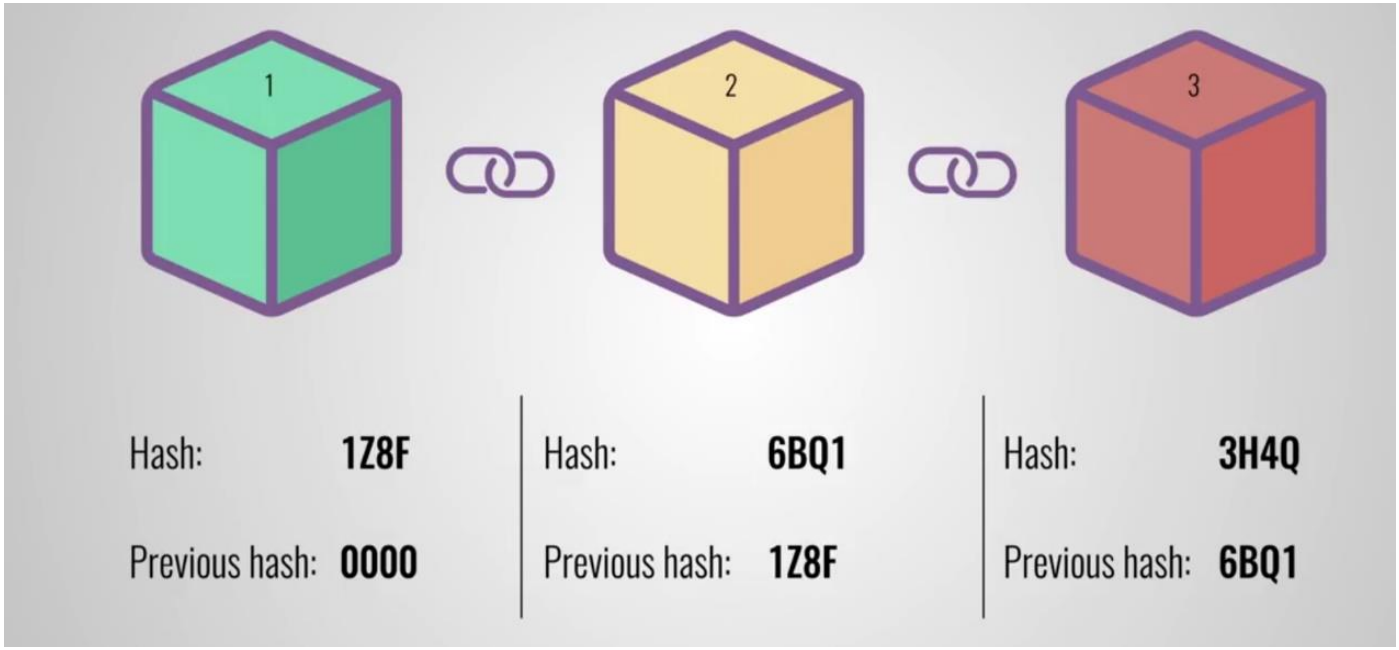
1) Τα δεδομένα,

2) Στοιχείο αναγνώρισης (Hash) και

3) Το στοιχείο αναγνώρισης του προηγούμενο Block.

BLOCKCHAIN – ΛΟΓΙΣΜΙΚΟ ΤΕΧΝΟΛΟΓΙΑ (2/6)

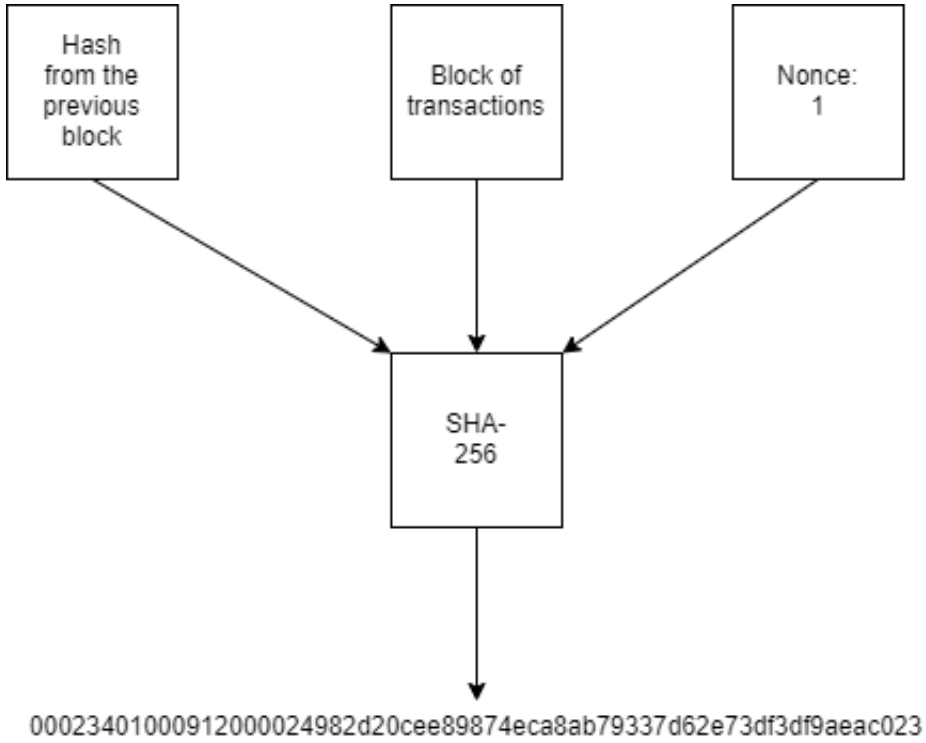
ΠΩΣ ΛΕΙΤΟΥΡΓΕΙ



BLOCKCHAIN – ΛΟΓΙΣΜΙΚΟ ΤΕΧΝΟΛΟΓΙΑ (3/6)

Proof of Work:

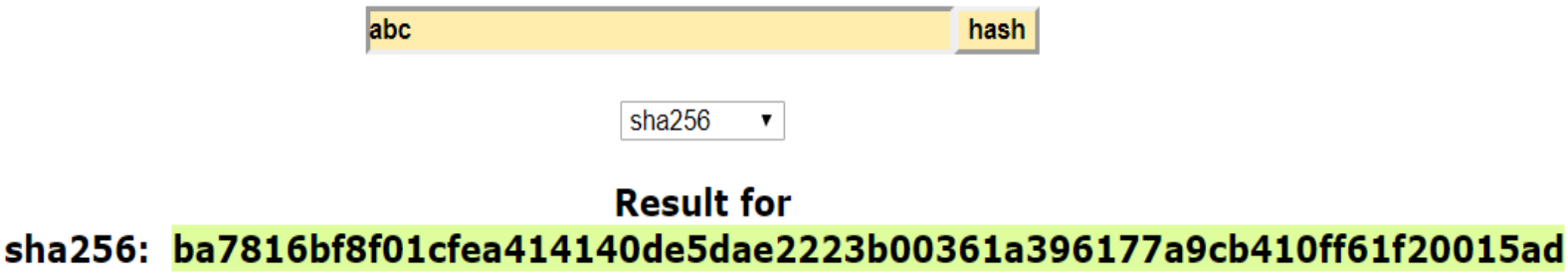
- Hash προηγούμενου μπλοκ
- Block συναλλαγών
- Nonce (τυχαίος αριθμός)



BLOCKCHAIN – ΛΟΓΙΣΜΙΚΟ ΤΕΧΝΟΛΟΓΙΑ (4/6)

SHA-256:

- Λειτουργία μονής κατεύθυνσης
- Εισαγωγή αυθαίρετου μήκους και εξαγωγή σταθερού μήκους (hash value)
- Μοναδική τιμή εξόδου



BLOCKCHAIN – ΛΟΓΙΣΜΙΚΟ ΤΕΧΝΟΛΟΓΙΑ (5/6)

- **Οφέλη**

1. Αποκεντρωποιημένο σύστημα
2. Ομοφωνία (Consensus)
3. Δυσκολία αλλοίωσης
4. Μη παραποιήσιμο (Tamper-Proof)
5. Smart Contracts
6. Μείωση κόστους.

BLOCKCHAIN – ΛΟΓΙΣΜΙΚΟ ΤΕΧΝΟΛΟΓΙΑ (6/6)

- **Μειονεκτήματα**

1. Κόστος ενέργειας
2. 51% Attack
3. Χώρος αποθήκευσης
4. Μη αποδοτικό
5. Τροποποίηση δεδομένων
6. Fork (Bitcoin Cash)

Ψηφιακα νομισματα (1/3)

- Παρόμοιες ιδιότητες με το παραδοσιακό χρήμα
- Κάνουν χρήση της κρυπτογραφίας για την ασφάλεια των συναλλαγών
- Περιλαμβάνει ένα αποκεντρωποιημένο σύστημα

Ψηφιακα νομισματα (2/3)

Τα 7 μεγαλύτερα κρυπτονομίσματα

Έτος κυκλοφορίας	Όνομα	Market Cap 12/02/19 (δις)	Hash Algorithm	Supply	Δημιουργός
2009	Bitcoin	131,356	SHA-256	21 εκατ.	Satoshi Nakamoto
2013	Ethereum	16,151	Ethash	108 εκατ.	Vitalik Buterin
2012	XRP	9,531	SHA-512	100 δις	Brad Garlinhouse & Chris Larsen
2014	Tether	4,116	SHA-256	4,2 δις	J.R Willet
2017	Bitcoin Cash	3,868	SHA-256	21 εκατ.	Split from Bitcoin
2011	Litecoin	2,919	SHA-256	84 εκατ.	Charlie Lee
2018	EOS	2,550	SHA-256	1 δις.	Daniel Larimer

Ψηφιακα νομισματα (3/3)

- **Εναλλακτικά νομίσματα**: Αποτελούν αποτέλεσμα της αντιγραφής ενός μέρους του κώδικα του Bitcoin
  - Litecoin (LTC)
  - PeerCoin(PPC)
  - Namecoin (NMC)
  - Freicoin (FRC)
  - Primecoin (XMP)
  - Auroracoin (AUR)

Βασικεσ εννοιεσ του bitcoin (1/4)

- Πορτοφόλι Bitcoin (e-Wallet)
  - Διαχείριση μονάδων Bitcoin
  - Περιέχει το ιδιωτικό κλειδί του χρήστη (Private Key)
  - Δημιουργεί και δέχεται συναλλαγές (ανανέωση των μονάδων)

Βασικες εννοιες του bitcoin (2/4)

- Ασφάλεια e-Wallet

  Πρόβλημα: Θύμα διαδικτυακής απάτης και αφαίρεσης μονάδων από το πορτοφόλι.

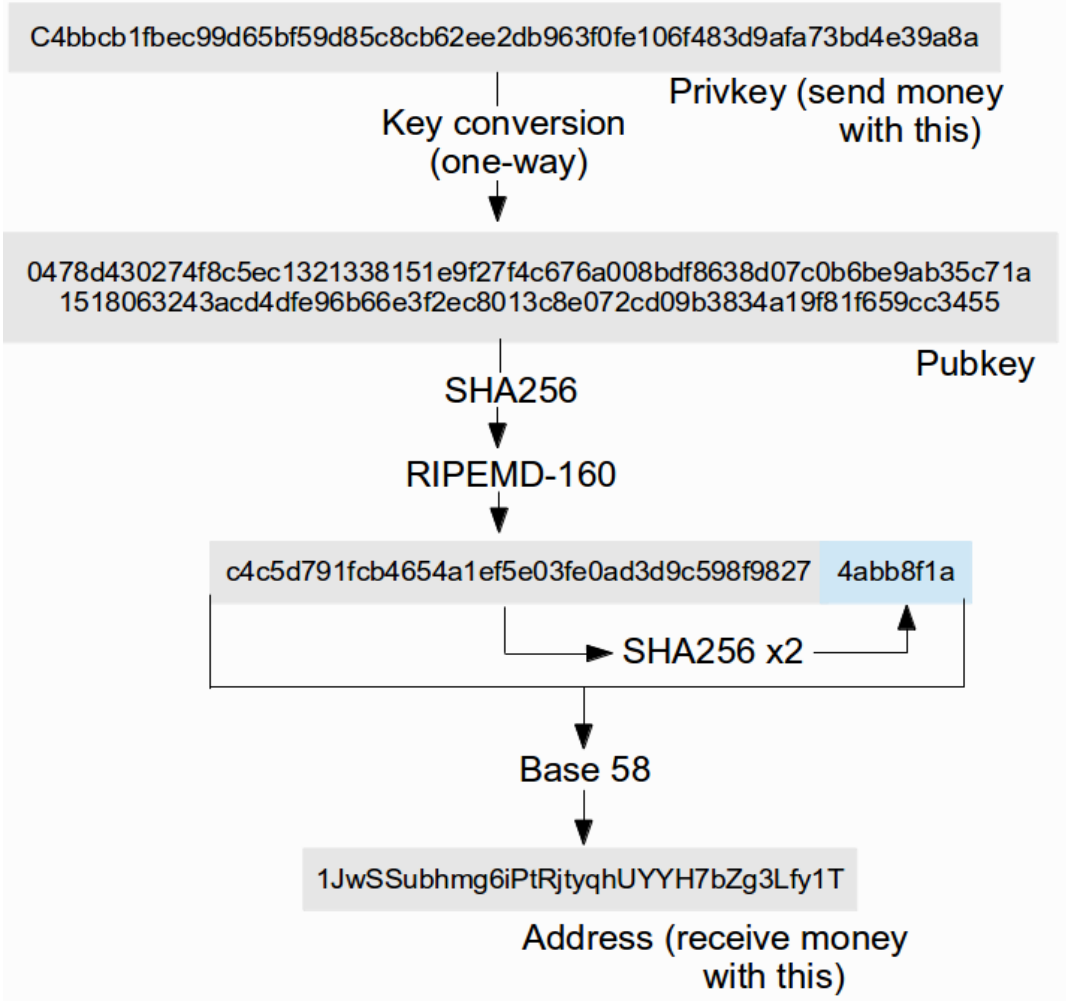
  Λύση: Το πορτοφόλι δημιουργεί 12 τυχαίες λέξεις (λέξη = αριθμός)

  Διαχείριση κλειδιού

  - Αποθήκευση κλειδιού στον τοπικό δίσκο
  - Πορτοφόλι που προστατεύεται με κωδικό
  - Αποθήκευσης κλειδιών εκτός σύνδεσης (USB)
  - Φιλοξενούμενο πορτοφόλι (χρήση διαδικτυακής ταυτοποίησης

Βασικεσ εννοιεσ του bitcoin (3/4)

- Bitcoin Address



Βασικεσ εννοιεσ του bitcoin (4/4)

- **ΣΥΣΤΗΜΑΤΑ ΕΞΟΡΥΞΗΣ**

1. CPU
2. GPU
3. FPGA
4. ASIC

- **ΕΝΑΛΛΑΚΤΙΚΟΙ ΤΡΟΠΟΙ ΕΞΟΡΥΞΗΣ**

1. Cloud mining
2. Mining pool

Μεθοδολογια (1/4)

- **Chaincode**
- **Java SDK Hyperledger Fabric**
- **Docker Engine Configuration**
- **Cryptogen-tool**
- **Configtxgen-tool (Genesis Block)**
- **Endorsement policy (And or OR)**

Μεθοδολογια (2/4)

- **Είσοδοι για την εφαρμογή αξιολόγησης (Caliper)**
  - Αρχείο διαμόρφωσης αναφοράς (Benchmark Configuration File)
  - Αρχείο διαμόρφωσης δικτύου (Network Configuration File)
  - Κύκλωμα φόρτου εργασίας (Workload Module)
  - Τεχνικά κριτήρια (Benchmark Artifacts)

Μεθοδολογια (3/4)

- **Κύρια διαδικασία (Master Process)**

1. Εκτέλεση σεναρίου εκκίνησης
2. Αρχικοποίηση του συστήματος που βρίσκεται υπό δοκιμή
3. Ανάπτυξη έξυπνων συμβολαίων
4. Εκτέλεση των γύρων (Διαδικασία του ¨Εργαζομένου¨)
5. Εκτέλεση σεναρίου εκκαθάρισης (εάν υπάρχει)

Μεθοδολογια (4/4)

- **Διαδικασία του ¨Εργαζομένου¨(Worker Process)**

1. Ενεργοποίηση της επόμενης συναλλαγής αναμένοντας τον ελεγκτή ρυθμού
2. Μεταβίβαση του ελέγχου στη μονάδα φόρτου εργασίας, μόλις ο ελεγκτής ενεργοποιήσει την επόμενη συναλλαγή

Λειτουργια hyperledger (1/3)

- **Βασικά χαρακτηριστικά σχεδίασης του Hyperledger Fabric**

1. Περιουσιακά στοιχεία (Assets)
2. Αλυσιδωτός κώδικας (Chaincode)
3. Χαρακτηριστικά βάσης (Ledger features)
4. Απόρρητο (Privacy)
5. Ασφάλεια και Υπηρεσίες μέλους (Security & Membership Services)
6. Ομοφωνία (Consensus)

Λειτουργια hyperledger (2/3)

- **Ροή συναλλαγής**

1. Ο πελάτης Α εκκινεί μια συναλλαγή
2. Έγκριση υπογραφής και εκτέλεση συναλλαγής
3. Επιθεώρηση των απαντήσεων της πρότασης
4. Συγκέντρωση των εγκρίσεων σε μια συναλλαγή
5. Επικύρωσή και δέσμευση της συναλλαγής
6. Ενημέρωση της βάσης

Λειτουργια hyperledger (3/3)

- **Βήματα για την ανάπτυξη ενός δικτύου**

1. Απόφαση σχετικά με την διαμόρφωση του δικτύου
2. Ρύθμιση ενός συμπλέγματος για τους πόρους
3. Ρύθμιση των αρχών έκδοσης πιστοποιητικών (CA)
4. Χρήση των πιστοποιητικών (CA) για την δημιουργία ταυτοτήτων και των παροχών υπηρεσιών συνδρομής (MSP)
5. Ανάπτυξη κόμβων
   - Δημιουργία μελών
   - Δημιουργία ενός μέλους/εντολέα

ΣΥΜΠΕΡΑΣΜΑΤΑ

- Επανάσταση στις ηλεκτρονικές συναλλαγές.
- Blockchain: Απλή στη λειτουργεία
- Ευάλωτη στις κακόβουλες επιθέσεις
- Με την τεχνολογία Blockchain κάθε συναλλαγή είναι πιο ασφαλής.
- Μείωση κόστους συναλλαγής.
- Αποκεντρωποιημένη τεχνολογία

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014). Innovations in payment technologies and the emergence of digital currencies. *Bank of England Quarterly Bulletin*, 262-275.
- Buterin, V. (2013). *A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM.*
- Cao, B., Zhang, Z., Feng, D., Zhang, S., Zhang, L., Peng, M., & Li, Y. (2020). Performance analysis and comparison of PoW, PoS and DAG based blockchains. *Digital Communications and Networks*, 1-12.
- Chen , L., Lee, W.-K., Chang, C.-C., Choo, K.-K., & Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. *Future Generation Computer Systems*, 420-429.
- Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*, 1-8.
- CHUEN, D. L. (2015). *HANDBOOK OF DIGITAL CURRENCY.*

ΕΥΧΑΡΙΣΤΩ ΓΙΑ ΤΗΝ ΠΡΟΣΟΧΗ ΣΑΣ!!!