ΠΡΟΧΩΡΗΜΕΝΕΣ ΚΡΥΠΤΟΓΡΑΦΙΚΕΣ ΥΠΗΡΕΣΙΕΣ: ΨΗΦΙΑΚΑ ΑΚΑΔΗΜΑΪΚΑ ΔΙΠΛΩΜΑΤΑ

Δημήτρης Μητρόπουλος

dimitro@grnet.gr

Diplomata

Αποθήκευση και Επαλήθευση Ακαδημαϊκών Διπλωμάτων στο Blockchain

Κίνητρα

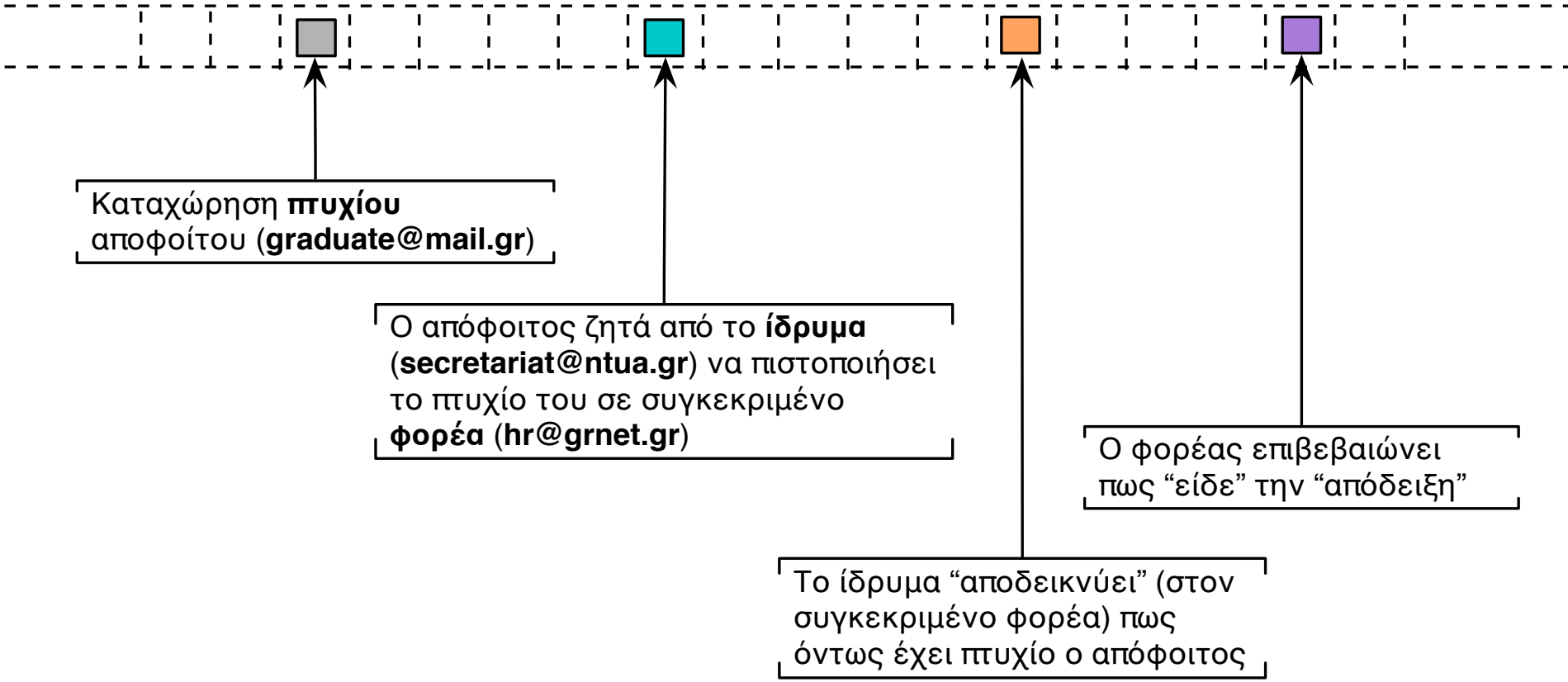
- **Γραφειοκρατία**: μια γραμματεία ενός πανεπιστημίου πρέπει να επαληθεύσει χιλιάδες πτυχία υποψηφίων ακαδημαϊκών θέσεων μέσα σε ένα έτος.
- **Πλαστά Πτυχία**: περισσότεροι από 2000 δημόσιοι υπάλληλοι έχουν (είχαν;) πλαστά πτυχία.

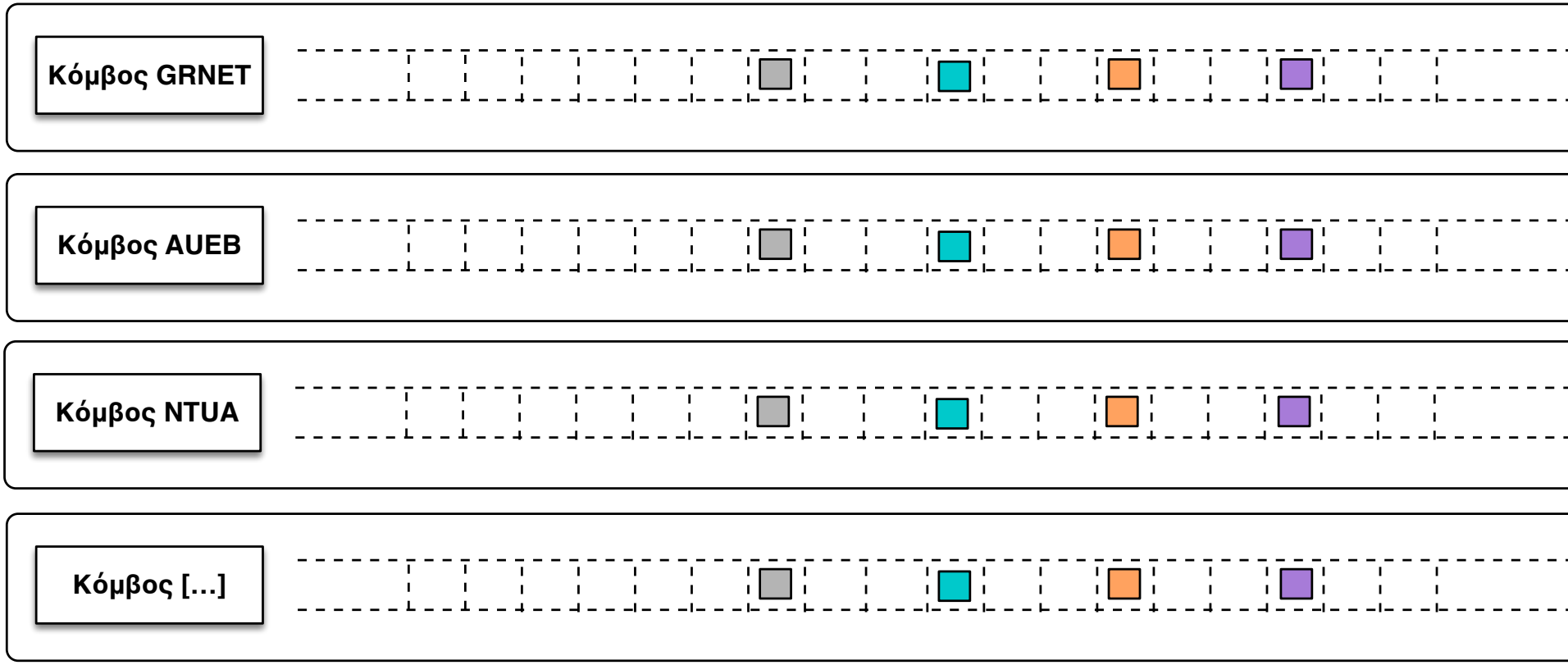
Γιατί Blockchain;

Αντεπιχείρημα: Ψηφιακό πτυχίο που θα φέρει την ψηφιακή υπογραφή του πανεπιστημίου.

- Δεν θέλουμε να καταγράφουμε μόνο το γεγονός της απονομής ενός πτυχίου, αλλά και όλου του **ιστορικού** της χρησιμοποίησής του (ή ανάκλησής του).
- Θέλουμε να μην παραβιάζεται η **ιδιωτικότητα** των κατόχων.

Ένα πτυχίο αποτελεί προσωπικό δεδομένο. Ένα «ψηφιακό» πτυχίο είναι εύκολο να διαρρεύσει.


Καταχώρηση **πτυχίου** αποφοίτου (**graduate@mail.gr**)
Ο απόφοιτος ζητά από το **ίδρυμα** (**secretariat@ntua.gr**) να πιστοποιήσει το πτυχίο του σε συγκεκριμένο **φορέα** (**hr@grnet.gr**)
Το ίδρυμα “αποδεικνύει” (στον συγκεκριμένο φορέα) πως όντως έχει πτυχίο ο απόφοιτος
Ο φορέας επιβεβαιώνει πως “είδε” την “απόδειξη”


Κόμβος GRNET
Κόμβος AUEB
Κόμβος NTUA
Κόμβος [...]

Αποθήκευση Δεδομένων

Τα δεδομένα δεν αποθηκεύονται καθεαυτά. Αντ'αυτού, αποθηκεύονται **κρυπτογραφημένα** μεταδεδομένα.

Υλοποίηση

- Έχουμε αναπτύξει συγκεκριμένο **πρωτόκολλο μηδενικής γνώσης** (zero-knowledge protocol) που υλοποιεί την καταγραφ του ιστορικού.
- Τρέχει σε **διαφορετικά** blockchains (λ.χ. HyperLedger, Cardano).
- **Δεν** χρειαζόμαστε το πρωτόκολλο **Proof-of-Work**.
- Το blockchain θα μπορούν να προσπελάσουν **εξουσιοδοτημένε** οντότητες (χωρίς αυτό να είναι απαραίτητο).
- Βρισκόμαστε σε προχωρημένο στάδιο υλοποίησης μιας **εφαρμογής** (backend + graphical user interface) που θα μπορού να χρησιμοποιούν όλοι οι εμπλεκόμενοι.

Επιπλέον

- Η πλατφόρμα μπορεί:
  - ✓ να ενσωματώσει χαρακτηριστικά από τεχνολογίες όπως το **Self-sovereign Identity** (SSI).
  - ✓ να είναι συμβατή με την ρύθμιση **electronic IDentification, Authentication and trust Services** (eIDAS) της Ευρωπαϊκής Ένωσης.

Πλαίσιο

- **PRIViLEDGE**: Privacy-Enhancing Cryptography in Distributed Ledgers. H2020 EU Project.
- **European Blockchain Partnership (EBP)**: Όπου η αποθήκευση και επαλήθευση ακαδημαϊκών τίτλων στο blockchain είναι μια από τις 4 βασικές μελέτες περίπτωσης.

Ευχαριστούμε!