**Αποκεντρωμένα Αναγνωριστικά. (DID)**

**# 1 Εισαγωγή.**

**# 1.1 Τι είναι τα αποκεντρωμένα αναγνωριστικά ;**

Τα αποκεντρωμένα αναγνωριστικά είναι ένας από τους βασικότερους τεχνολογικούς πυλώνες για την υλοποίηση του **αποκεντρωμένου** συστήματος αυτοδιαχειριζόμενης ταυτότητας. Μια αναλογία που θα μπορούσε κάνεις να δώσει, είναι πως τα αποκεντρωμένα αναγνωριστικά είναι όπως οι (IP) διευθύνσεις για το διαδίκτυο, μόνο που αποσκοπούν στο εμπιστευτικό επίπεδο του διαδικτύου.

Ένα αποκεντρωμένο αναγνωριστικό ανήκει σε κάποιον άνθρωπο, οργάνωση, εταιρία ή σε κάποια άλλη οντότητα. Σε αντίθεση με κάποια (federated identifiers), τα αποκεντρωμένα αναγνωριστικά έχουν σχεδιαστή με σκοπό να μην αποθηκεύονται σε κάποιο κεντρικοποιημένο σύστημα ή κάποιου άλλου είδους πάροχο. Αυτό μπορεί και επιτυγχάνεται διότι ο έλεγχος της κατοχής του γίνεται με διάφορους κρυπτογραφικούς τρόπους.

Με μια απλή προσέγγιση τα αποκεντρωμένα αναγνωριστικά είναι μοναδικά αναγνωριστικά (URIs) τα οποία βοηθάνε στην επανάκτηση των αποκεντρωμένων εγγράφων μέσα από κάποιο αποκεντρωμένο σύστημα (τύπου Blockchain). Κάθε αποκεντρωμένο έγγραφο εμπεριέχει κάποια μεταδεδομενα τα οποία δίνουν την δυνατότητα στην εμπιστοσύνη μεταξύ διαφορετικών υποκειμένων.

**# 1.2 Βασικές ιδιότητες**

Ο λόγος που εμφανίστηκαν τα αναγνωριστικά αυτά είναι επειδή δεν υπήρχε κάποια άλλη παρόμοια τεχνολογία που θα πληρούσε τις παρακάτω τέσσερις ιδιότητες:

1. **Επιμονή (Persistence):** Θα μπορεί κάποιος να το χρησιμοποιήσει για όσο θέλει μέχρις ότου να το αποσύρει.
2. **Αναζητούμενο (Resolvable):** Θα μπορεί κάποιος να το ψάξει και να εξάγει κάποια μεταδεδομένα (αποκεντρωμένα έγγραφα).
3. **Κρυπτογραφικά Επαληθεύσιμα (Cryptographically-Verifiable):** Θα μπορεί κάποιος να τα επαληθεύσει με κάποιον κρυπτογραφικό τρόπο.
4. **Αποκεντρωμένο (Decentralized):** Δεν θα βασίζεται σε κεντρικοποιημένα συστήματα.

**# 1.3 Σύγκριση αναγνωριστικών**

Υπάρχουν αρκετά αναγνωριστικά (όπως όνομα, τηλέφωνο κ.α.) τα οποία είναι στην διάθεση μας. Παρόλα αυτά κανένα δεν δίνει κάποια λύση και για τις τέσσερις ιδιότητες που προαναφέρθηκαν.

Μια σύγκριση που μπορεί να γίνει μεταξύ τριών διαφορετικών αναγνωριστικών, μπορεί να κάνει πιο ξεκάθαρη τον λόγο για τον οποίο εμφανίστηκαν τα **αποκεντρωμένα** αναγνωριστικά.

Chart, scatter chart

Description automatically generated

Όπως φαίνεται στην φωτογραφία τα αναγνωριστικά που συγκρίνονται είναι τα: *url, email, did*. Στις ιδιότητες που γίνεται η σύγκριση τους είναι και ένα ακόμα πεδίο το οποίο δεν αναφέρθηκε στο προηγούμενο κεφάλαιο (στις βασικές ιδιότητες), με το όνομα (human friendly), που παραπέμπει στο πόσο φιλικό είναι για τους ανθρώπους.

Βλέποντας την φωτογραφία είναι φανερό πως τα αποκεντρωμένα αναγνωριστικά πληρούν όλες τις λειτουργίες που χρειάζεται να έχει ένα αποκεντρωμένο σύστημα αυτοδιαχειριζόμενης ταυτότητας.

**# 2 Τεχνολογική Επισκόπηση**

**# 2.1 Πως μοιάζουν τα αποκεντρωμένα αναγνωριστικά**

Με βάση την **World Wide Web Consortium (W3C)** η οποία έχει αναλάβει για την επίβλεψη και ανάπτυξη των αποκεντρωμένα αναγνωριστικά, σύμφωνα με την έκδοση 1.0 ένα αναγνωριστικό αποτελείτε από τα εξής τρία μέρη: **σχήμα**, **μέθοδο**, **αλφαριθμητικό**.

Πιο συγκεκριμένα:

1. **Σχήμα (Schema):** Το οποίο αναφέρεται στο σχήμα του αποκεντρωμένου αναγνωριστικού. *(πιθανές τιμές: did κ.α)*
2. **Μέθοδος (Method):** Η μέθοδος που χρησιμοποιεί το αποκεντρωμένο αναγνωριστικό. Το συγκεκριμένο πεδίο αναφέρεται στον τόπο όπου βρίσκεται το (DID document), πιο συγκεκριμένα στο Blockchain το οποίο έχει αποθηκευτεί. Κάποια απο τα Blockchain που υποστηρίζουν ως και σήμερα τα (SSI) είναι τα παρακάτω:

|  |  |
| --- | --- |
| **Μέθοδος** | **Πρόθεμα** |
| Soverin | did:sov |
| Bitcoin | did:btrc |
| IPFS | did:ipid |
| Veres One | did:v1 |

Τέλος το πεδίο αυτό μπορεί να λάβει και άλλες τιμές που δεν αναφέρονται σε κάποιο Blockchain αλλά σε κάποιο πρωτόκολλο *(π.χ. peer κ.α.)*

1. **Αλφαριθμητικό (Method-Specific Identifier):** Ένα μοναδικό αλφαριθμητικό το οποίο είναι υπεύθυνό για να εντοπίσει το αποκεντρωμένο έγγραφο αναγνωριστικού μέσα από όλα τα άλλα.

Ένα παράδειγμα ενός αποκεντρωμένου αναγνωριστικού είναι:

Text

Description automatically generated

Δηλαδή πιο συγκεκριμένα στο example (Blockchain για παράδειγμα) έχουμε ένα αποκεντρωμένο έγγραφο με αναγνωριστικό 123456789abcdefghi.

**# 2.2 Αποκεντρωμένα Έγγραφα (DID Document)**

Ένα αποκεντρωμένο έγγραφο είναι απλά ένα JSON-LD αντικείμενο το οποίο είναι αποθηκευμένο σε κάποιο μέρος εύκολα προσβάσιμο από όλους.

Για να μπορέσει κάνεις να το αναζήτηση και να βρει αυτό το έγγραφο θα πρέπει να έχει στην κατοχή του το αποκεντρωμένο αναγνωριστικό που σχετίζεται με το συγκεκριμένο έγγραφο. Ο τρόπος με τον οποίο μπορεί να το κάνει αυτά είναι με βάση το τελευταίο παράδειγμα του προηγούμενου κεφαλαίου.

Πιο συγκεκριμένα, ένα αποκεντρωμένο έγγραφο μπορεί να εμπεριέχει:

1. Μια χρονική σήμανσή στην οποία δημιουργήθηκε.
2. Μια κρυπτογραφική επαλήθευση με την οποία μπορεί κάποιος να καταλάβει πως το έγγραφο αυτό είναι έγκυρο.
3. Μια λίστα από κρυπτογραφικά κλειδιά.
4. Ένα τρόπο με τον οποίο κάποιος μπορεί να πιστοποιήσει το αποκεντρωμένο έγγραφο.
5. Μια λίστα από υπηρεσίες στις οποίες το αποκεντρωμένο αναγνωριστικό μπορεί να χρησιμοποιηθεί.
6. Άλλες επεκτάσεις που μπορεί να πάρει το έγγραφο.

Ένα παράδειγμα ενός αποκεντρωμένου εγγράφου με βάση το πρότυπο της **W3C** είναι το εξής:

Graphical user interface, text, application

Description automatically generated

Όλα τα πεδία ενός αποκεντρωμένου εγγράφου είναι προαιρετικά εκτός από το «id» πεδίο, το οποίο έχει την τιμή του αποκεντρωμένου αναγνωριστικού.

Μέσα στο έγγραφο αυτό δεν υπάρχει κανένα ίχνος κάποιου προσωπικού στοιχείου, όπως κάποιου αριθμού τηλεφώνου είτε κωδικού πρόσβασης, αυτά έρχονται μέσα από τους επαληθεύσιμους ισχυρισμούς οι οποίοι αναφέρονται αμέσως μετά.

**# 2.3 Επαληθεύσιμοι Ισχυρισμοί (Verifiable Claims)**

Ένα από τα προβλήματα που λύνουν τα αποκεντρωμένα αναγνωριστικά είναι πάνω στους επαληθεύσιμους ισχυρισμούς. Όπως είναι γνωστό, για την λειτουργία ενός ισχυρισμού θα χρειαστούν τρία κομμάτια:

1. **Υποκείμενο (subject):** Συνήθως ένας απλός χρήστης, μια επιχείρηση ή οτιδήποτε το οποίο μπορεί να περιγραφή.
2. **Εκδότης (Issuer):** Συνήθως μια εταιρία, ένας οργανισμός ή κάποιος άλλος πάροχος. (όπως το πανεπιστήμιο Θεσσαλίας)
3. **Ισχυρισμός (Claim):** Οποιαδήποτε δήλωση η οποία μπορεί να γίνει πάνω στο υποκείμενο. Για παράδειγμα, έστω ότι έχουμε το πανεπιστήμιο Θεσσαλίας και έναν φοιτητή, ο ισχυρισμός θα μπορούσε να είναι πως ο φοιτητής έχει περάσει το μάθημα «Σήματα και Συστήματα».

Με λίγα λόγια, ένας επαληθεύσιμος ισχυρισμός είναι και αυτό ένα αποκεντρωμένο έγγραφο το οποίο είναι αποθηκευμένο σε κάποιο αποκεντρωμένο σύστημα. Ο τρόπος με τον οποίο μπορεί κάποιος να έχει πρόσβαση σε αυτό, είναι αν είναι κάτοχος του αποκεντρωμένου αναγνωριστικού που έχει αναθετηθεί μέσα στο έγγραφο.

Το κομμάτι του επαληθεύσιμου είναι βασισμένο σε κάποιες κρυπτογραφικές μεθόδους, οι οποίες είναι υπογεγραμμένες από τον εκδότη. (τεχνική ψηφιακών υπογραφών)

Ένα παράδειγμα ενός επαληθεύσιμου ισχυρισμού με βάση το πρότυπο της **W3C** είναι το εξής:

Graphical user interface, text, application

Description automatically generated

Στην παραπάνω εικόνα υπάρχουν όλα τα στοιχεία που χρειάζεται ένας ισχυρισμός. Έχουμε:

* “**context**”: Βασισμένο πάνω στην μέθοδο JSON-LD.
* “**id**”: Βασισμένο πάνω στην μέθοδο JSON-LD.
* “**type**”: Ο τύπος του ισχυρισμού.
* “**issuer”** Το αποκεντρωμένο αναγνωριστικό του εκδότη.
* “**issuanceDate**”: Ημερομηνία που εκδόθηκε ο ισχυρισμός.-
* “**credentialSubject**”: Ο ισχυρισμός και σε ποιον ανήκει.
* “**proof**”: Κρυπτογραφικές μέθοδος για την εγκυρότητα του ισχυρισμού.

Το βασικότερο πεδίο από όλα είναι το “**credentialSubject** ”, διότι εκεί γίνεται η ανάθεση τον ισχυρισμών από κάποιον εκδότη για κάποιο υποκείμενο. Όπως φαίνεται και στην φωτογραφία το πεδίο αυτό έχει ένα αναγνωριστικό το οποίο αναφέρεται στο υποκείμενο και όλους τους ισχυρισμούς που έρχεται μαζί του.

Συμφώνα με το W3C τα πεδία που μπορεί να πάρει ένας επαληθεύσιμος ισχυρισμός μπορεί να πάρει κι άλλες τιμές, οι οποίες δεν αναφέρονται εδώ.

**# 3 Βιβλιογραφία**

1. <https://medium.com/@adam_14796/understanding-decentralized-ids-dids-839798b91809>
2. <https://www.w3.org/TR/did-core/>
3. <https://www.evernym.com/blog/what-are-decentralized-identifiers-dids/>