ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Κατανεμημένη διαχείριση αυτό-διαχειριζόμενης ταυτότητας

Ελευθεριάδης Αλέξανδρος
Κοντόπουλος Ιωάννης

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Γεώργιος Λιουδάκης
Διδάσκων τμήματος πληροφορικής και τηλεπικοινωνιών

Λαμία έτος 2022

÷

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Κατανεμημένη διαχείριση αυτό-διαχειριζόμενης ταυτότητας

Ελευθεριάδης Αλέξανδρος
Κοντόπουλος Ιωάννης

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Γεώργιος Λιουδάκης
Διδάσκων τμήματος Πληροφορικής και Τηλεπικοινωνιών

Λαμία έτος 2022

UNIVERSITY OF
THESSALY

SCHOOL OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE & TELECOMMUNICATIONS

Distributed self-sovereign identity management

Eleftheriadis Alexandros
Kontopoulos Ioannis

FINAL THESIS

ADVISOR

Georgios Lioudakis
Professor at University of Thessaly, Department of Informatics and Telecommunications

Lamia year 2022

«Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις [(1)], που προβλέπονται από της διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

*1. Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί **χωρίς να τα περικλείω σε εισαγωγικά** και χωρίς να αναφέρω το συγγραφέα, τη χρονολογία, τη σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάσθηκαν, χωρίς αναφορά στην πηγή. Αναφέρω πάντοτε με πληρότητα την πηγή κάτω από τον πίνακα ή σχέδιο, όπως στα παραθέματα.*

*2. Δέχομαι ότι η αυτολεξεί **παράθεση χωρίς εισαγωγικά**, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων, και παρουσίασή τους ως δική μου εργασία.*

3. Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στη συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ), προϋποθέτει ειδικές ρυθμίσεις, και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια

4. Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.

Ημερομηνία: 18/10/2022

Ο Δηλ. Ελευθεριάδης Αλέξανδρος

Ημερομηνία: 18/10/2022

Ο Δηλ. Ιωάννης Κοντόπουλος

(1) «Όποιος εν γνώσει του δηλώνει ψευδή γεγονότα ή αρνείται ή αποκρύπτει τα αληθινά με έγγραφη υπεύθυνη δήλωση
του άρθρου 8 παρ. 4 Ν. 1599/1986 τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Εάν ο υπαίτιος αυτών των πράξεων
σκόπευε να προσπορίσει στον εαυτόν του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται με κάθειρξη μέχρι 10 ετών.»

ΠΕΡΙΛΗΨΗ

Η συντριπτική πλειοψηφία των εφαρμογών διαδικτύου βασίζονται στην έννοια της ταυτότητας. Θα μπορούσε κάποιος να ισχυριστεί ότι η ταυτότητα αποτελεί αναπόσπαστο κομμάτι του διαδικτύου, αφού κάθε πάροχος μίας υπηρεσίας επιθυμεί να αναγνωρίζει μοναδικά τον εκάστοτε χρήστη του. Σήμερα το μεγαλύτερο ποσοστό τον υποσυστημάτων ταυτότητας είναι βασισμένο σε κάποιο κεντρικοποιημένο μοντέλο, στο οποίο ο χρήστης απλά *λαμβάνει* μέρος, χωρίς να έχει τον πλήρη έλεγχο των δεδομένων του. Από την άλλη, με την τεχνολογία του Blockchain, ως μία κατανεμημένη βάση δεδομένων, να λαμβάνει όλο και περισσότερη δημοσιότητα, μία νέα πρόταση έχει ανέλθει στην επιφάνια, η Κατανεμημένη Αυτοδιαχειριζόμενη Ταυτότητα. Αυτοδιαχειριζόμενη, διότι ο χρήστης βρίσκεται στο επίκεντρο του μοντέλου, έχοντας πλήρη έλεγχο των δεδομένων του και των ενεργειών που μπορεί να εκτελέσει με αυτά. Κατανεμημένη, γιατί τα δεδομένα του χρήστη δεν υφίστανται σε κάποιο φυσικό μέσο κάποιου παρόχου, αλλά στον ίδιο τον χρήστη. Όλα τα παραπάνω, σε συνδυασμό με νεοσύστατα πρωτόκολλα όπως τα Αποκεντρωμένα Αναγνωριστικά και τα Επαληθεύσιμα Διαπιστευτήρια ορίζουν τις αρχές ενός συστήματος κατανεμημένης διαχείρισης αυτοδιαχειριζόμενης ταυτότητας. Στην εργασία αυτή ορίζεται το θεωρητικό και το πρακτικό υπόβαθρο ενός συστήματος ταυτότητας, εμβαθύνοντας αρχικά στις προαναφερθείσες τεχνολογίες και υλοποιώντας ένα δίκτυο ταυτότητας, μέσω του οποίου καλύπτονται κάποιες περιπτώσεις χρήσεις που αντικατοπτρίζουν τον τρόπο με τον οποίο θα χρησιμοποιούνταν ένα σύστημα αυτοδιαχειριζόμενης ταυτότητας υπό πραγματικές συνθήκες.

ABSTRACT

The vast majority of the web applications are tightly connected to the use of some sort of identity. One could state that identity is an indivisible part of the internet since every service provider wants to uniquely identify his users. Nowadays, the biggest proportion of the identity systems are based on a centralized model, in which the user is just a part of the system and has not any control over his data. On the other side, Blockchain, in the form of a distributed database, has gained a lot of popularity recently, which led to a new solution: the Distributed Self-Sovereign Identity. Self-Sovereign since the user acts as a core part of the model with full control over his data and the actions operated on them. Distributed for the reason that data are not present in any physical mean of a provider, but it's in the user's hold. All of those mentioned above, combined with newly created protocols as Distributed Identifiers and Verifiable credentials form the roots for a Distributed Self-Sovereign Identity. This thesis provides a comprehensive overview of the theoretical and practical aspects of a self-sovereign system. Firstly, we analyze and explain the technologies mentioned above and then, we implement a distributed self-sovereign network which simulates how self-sovereign identity could be used in a real-world scenario.

Πίνακας Περιεχομένων

Η εκπόνηση της πτυχιακής χωρίστηκε στις εξής ενότητες:

Ο Ιωάννης Κοντόπουλος ανέλαβε:

- Κεφάλαιο 1: Εισαγωγή
- Κεφάλαιο 2: Blockchain
- Κεφάλαιο 2: Επαληθεύσιμα Διαπιστευτήρια
- Κεφάλαιο 3: Δημόσιες Υπηρεσίες
- Κεφάλαιο 3: Επίπεδο Εφαρμογής

Ενώ ο Αλέξανδρος Ελευθεριάδης:

- Κεφάλαιο 2: Βασικές αρχές κρυπτογραφίας
- Κεφάλαιο 2: Αποκεντρωμένα αναγνωριστικά
- Κεφάλαιο 2: Ψηφιακό Πορτοφόλι
- Κεφάλαιο 3: Μοντέλο αποκεντρωμένης ταυτότητας
- Κεφάλαιο 3: Επικοινωνία αποκεντρωμένων αναγνωριστικών
- Κεφάλαιο 3: Επίπεδο εφαρμογής

Το 4ο Κεφάλαιο και η υλοποίηση της συστήματος έγινε από κοινού. Τέλος, ο πηγαίος κώδικας του συστήματος φιλοξενείται στο GitHub.

ΚΕΦΑΛΑΙΟ 1: Εισαγωγή

Η ταυτότητα στο διαδίκτυο 1.1

Η ικανότητα ενός ατόμου (ή και οργανισμού) να αποδείξει ότι είναι αυτός που ισχυρίζεται, είναι κρίσιμη για τις ανθρώπινες αλληλεπιδράσεις μίας κοινωνίας, είτε στον διαδικτυακό κόσμο, είτε στον φυσικό. Με την ραγδαία εξέλιξη του διαδικτύου, η ανάγκη για ένα μοντέλο ψηφιακής ταυτότητας, ο τρόπος δηλαδή με τον οποίο κάποιος αποδεικνύει κάποιους ισχυρισμούς σχετικά με τον εαυτό του μέσω του διαδικτύου, έχει γίνει απαραίτητη. Το πρόβλημα, όμως, έγκειται στο γεγονός ότι το διαδίκτυο σχεδιάστηκε για την επικοινωνία και την διασύνδεση πολλαπλών *μηχανών*, ώστε να μοιράζονται πληροφορίες, χωρίς όμως να υπάρχει τρόπος να αναγνωρίσει κάποιος με ποιον συνδέεται [1]. Οι διευθύνσεις IP είναι εν γένει *φτωχές* αφού χρησιμεύουν μόνο στην διασύνδεση των μηχανών και δεν παρέχουν καμία πληροφορία για το ποιος είναι υπεύθυνος του συστήματος που του έχει ανατεθεί η εκάστοτε διεύθυνση. Άλλωστε, κακόβολοι χρήστες έχουν επιδείξει αρκετές φορές ότι είναι εφικτό να παραποιήσεις την διεύθυνση IP (ή και την διεύθυνση υλικού, MAC) πρώτού αποστείλεις ένα πακέτο πληροφορίας στην συσκευή διαδικτύου. Έτσι, δεδομένης της κλίμακας που έχει το διαδίκτυο στην σημερινή ημέρα, καθίσταται σχεδόν απίθανο να καθιερωθεί εμπιστοσύνη μεταξύ δύο μερών, χρησιμοποιώντας αποκλειστικά αναγνωριστικά σε επίπεδο δικτύου.

Εφόσον η σημερινή δομή του διαδικτύου δεν παρέχει κάποιον μηχανισμό ταυτοποίησης, η ευθύνη έχει μετατεθεί στους παρόχους υπηρεσιών διαδικτύου. Για παράδειγμα, αν κάποιος έχει ένα ηλεκτρονικό κατάστημα, πρέπει να συλλέγει πληροφορίες για τους χρήστες του και φυσικά κάποιον τρόπο για να αναγνωρίζει τον χρήστη μεμονωμένα. Κάτι τέτοιο πρέπει να γίνεται διατηρώντας την ιδιωτικότητα του χρήστη, αφού σε συνέπεια με το παραπάνω παράδειγμα, ο χρήστης δεν θα ήθελε να είναι η διεύθυνση της κατοικίας του δημόσια (αυτό γίνεται αρκετά πιο κρίσιμο στην περίπτωση που συλλέγονται δεδομένα χρεωστικών καρτών, κ.λπ.). Για την επίτευξη του παραπάνω, η πιο σύνηθες προσέγγιση είναι η χρήση ενός συνθηματικού ή κωδικού, γνωστό μόνο από τον χρήστη, σε συνδυασμό με κάποιο αναγνωριστικό (e-mail, κινητό τηλέφωνο, όνομα χρήστη, κ.λπ.) ώστε ο πάροχος να είναι σίγουρος ότι ο χρήστης είναι αυτός που ισχυρίζεται.

Από την μεριά του χρήστη η παραπάνω προσέγγιση δεν είναι καθόλου εύχρηστη, αφού για κάθε εφαρμογή ή υπηρεσία διαδικτύου θα πρέπει να δημιουργήσει έναν λογαριασμό (μία *ταυτότητα* ή και *περσόνα*), εισάγοντας, τα ίδια πολλές φορές στοιχεία, και να διατηρεί τα στοιχεία σύνδεσης του. Από την άλλη, οι επιχειρήσεις θα πρέπει να συντηρούν μία βάση δεδομένων με τα στοιχεία του εκάστοτε χρήστη, κάτι το οποίο αποτελεί κίνδυνο για την ιδιωτικότητα του, αφού οι περιπτώσεις διαρροής προσωπικών δεδομένων είναι συχνό φαινόμενο [2]. Επίσης, οι χρήστες δεν έχουν άμεσο έλεγχο των δεδομένων τους, αφού τα δεδομένα αποθηκεύονται σε κάποια βάση δεδομένων του παρόχου. Κάτι τέτοιο μπορεί να οδηγήσει σε μη επιθυμητή χρήση των προσωπικών δεδομένων. Παράδειγμα αποτελεί το σκάνδαλο που εμπεριείχε το Facebook και το Cambridge Analytica, όπου διέρρευσαν πληροφορίες για περισσότερους από 87 εκατομμύρια χρήστες του Facebook [3].

Τα μοντέλα ταυτότητας 1.2

Όπως γίνεται αντιληπτό, η ανάγκη για την ταυτοποίηση οντοτήτων στο διαδίκτυο, έχει οδηγήσει στην διερεύνηση διαφορετικών μοντέλων. Από αυτά, διακρίνονται 3 κύριες κατηγορίες [4]

Κεντρικοποιημένο μοντέλο 1.3

Το κεντρικοποιημένο μοντέλο ταυτότητας είναι το πιο ευρέως διαδεδομένο και εύκολο στην κατανόηση μοντέλο. Η δημιουργία της ταυτότητας και η εδραίωσης της εμπιστοσύνης μεταξύ ενός χρήστης και ενός οργανισμού, πραγματοποιείται μέσω ενός λογαριασμού (συνήθως μέσω ενός αναγνωριστικού και ενός κωδικού).

Σχήμα 1: το κεντρικοποιημένο μοντέλο ταυτότητας

Αυτονόητο είναι ότι για κάθε διαφορετικό οργανισμό, απαιτείται διαφορετικός λογαριασμός. Αυτό οδηγεί σε αρκετά μειονεκτήματα, με τα σημαντικότερα να είναι:

- Ο χρήστης θα πρέπει να θυμάται τα αναγνωριστικά και τους κωδικούς για κάθε υπηρεσία που χρησιμοποιεί. Αυτό γίνεται ακόμη δυσκολότερο όταν κάθε υπηρεσία εφαρμόζει διαφορετικές πολιτικές ασφαλείας. Κλασσικό παράδειγμα αποτελεί το μέγεθος ενός κωδικού, ή ότι ένας κωδικός πρέπει να περιέχει κεφαλαία γράμματα, ειδικούς χαρακτήρες, κ.λπ.
- Τα δεδομένα του χρήστη δεν είναι φορητά ή επαναχρησιμοποιήσιμα. Μάλιστα, έχουν ισχύ μόνο στον συγκεκριμένο οργανισμό.
- Εφόσον τα δεδομένα είναι αποθηκευμένα σε μια κεντρική βάση δεδομένων, υπάρχει ο κίνδυνος διαρροής.

Ταυτότητα ελεγχόμενη από κάποια κεντρική αρχή 1.4

Για να αντιμετωπιστούν κάποια από τα μειονεκτήματα της κεντρικοποιημένης ταυτότητας, αναπτύχθηκε ένα νέο μοντέλο από την βιομηχανία, το μοντέλο ελεγχόμενης ταυτότητας από κεντρική αρχή (Αγγλ. the federated identity model). Η ιδία είναι αρκετή απλή: ένας ήδη υπάρχων πάροχος υπηρεσιών αναλαμβάνει τον ρόλο του *παρόχου ταυτότητας* (Αγγλ. identity provider, IDP).

Σχήμα 2: το μοντέλο ελεγχόμενης ταυτότητας από κεντρική αρχή

Έτσι, ο χρήστης δεν χρειάζεται να συντηρεί πολλαπλούς λογαριασμούς και στοιχεία σύνδεσης, αρκεί να έχει έναν λογαριασμό στον πάροχο ταυτότητας. Αν και όπως φαίνεται, το συγκεκριμένο μοντέλο επιλύει αρκετά προβλήματα, δεν αποτελεί ιδανική λύση για το επιθυμητό επίπεδο ταυτότητας του διαδικτύου, και αυτό γιατί:

- Δεν υπάρχει ένας μοναδικός πάροχος ταυτότητας που να συνδέεται με όλες τις υπηρεσίες και εφαρμογές διαδικτύου. Έτσι, ο χρήστης χρειάζεται πολλαπλούς λογαριασμούς σε διαφορετικούς παρόχους ταυτότητας.
- Ο χρήστης μπορεί να μην επιθυμεί να μοιραστεί με τον πάροχο ταυτότητας ότι χρησιμοποιεί μια υπηρεσία.
- Οι μεγάλοι πάροχοι ταυτότητας αποτελούν κίνδυνο για την ιδιωτικότητα του χρήστη. Η ταυτότητα δεν είναι φορητή, αφού μπορεί ο χρήστης να επιθυμεί να σταματήσει να χρησιμοποιεί τον συγκεκριμένο πάροχο ταυτότητας, διακόπτοντας έτσι και κάθε άλλη υπηρεσία στην οποία συνδέθηκε χρησιμοποιώντας τον συγκεκριμένο πάροχο.

Σχήμα 3: παράδειγμα μοντέλου ταυτότητας ελεγχόμενης από κεντρική αρχή

Αποκεντρωμένο μοντέλο ταυτότητας 1.5

Τα τελευταία χρόνια, με την τεχνολογία του blockchain να λαμβάνει αρκετή δημοτικότητα, ένα νέο μοντέλο έχει κεντρίσει το ενδιαφέρον, το αποκεντρωμένο (Αγγλ. decentralized). Η βασική αρχή του μοντέλου είναι ότι δεν βασίζεται σε κάποια κεντρική αρχή, αλλά είναι πλήρως αποκεντρωμένο. Αυτό σημαίνει ότι δεν υφίσταται η έννοια του λογαριασμού όπως στα προηγούμενα μοντέλα. Αντίθετα, υπάρχει άμεση διασύνδεση μεταξύ δύο οντοτήτων, που ονομάζονται ομότιμοι (Αγγλ. peers). Σε μία ομότιμη σχέση, κανένα από τα δύο μέρη δεν έχει κάποιον «λογαριασμό», αντίθετα μοιράζονται μία σύνδεση, την οποία οποιοσδήποτε από τους δυο μπορεί να διακόψει. Μια ομότιμη σύνδεση είναι εν γένει αποκεντρωμένη, αφού οποιοσδήποτε μπορεί να συνδεθεί με οποιονδήποτε, άλλωστε αυτός είναι και ο τρόπος με τον οποίο δουλεύει το διαδίκτυο.

Η προσέγγιση του συγκεκριμένου μοντέλου είναι αρκετά μοναδική, υπό την έννοια ότι μπορεί αναπαραστήσει με πολύ μεγάλη ακρίβεια τον τρόπο με τον οποίο πραγματοποιείται η ταυτοποίηση στον φυσικό κόσμο, κάτι το οποίο είναι αρκετά έμπιστο και ευρέως δοκιμασμένο. Η εμπιστοσύνη στο φυσικό μοντέλο ταυτότητας προέρχεται από τις εξής ιδιότητες: (α) ο κάτοχος μίας ιδιότητας είναι και αυτός που την παρουσιάζει (π.χ. όταν υποδεικνύει ένα διαβατήριο), (β) υπάρχει νόμιμος και πρακτικός τρόπος να ελεγχθεί η ιδιότητα (π.χ. η φωτογραφία στο διαβατήριο να ταιριάζει με τον άνθρωπο που το υποδεικνύει), (γ) οι ιδιότητες μοιράζονται μόνο από τον κάτοχο σε αυτόν που θέλει να τις επιβεβαιώσει (π.χ. παρόλο που το κράτος έχει αναθέσει το διαβατήριο, δεν γνωρίζει που θα

το υποδείξει ο κάτοχος). Πέρα από το (β), καμία από τις άλλες ιδιότητες δεν είναι δυνατόν να καλυφθούν χρησιμοποιώντας μία κεντρική αρχή.

Σε αυτό το σημείο προκύπτουν ερωτήματα όπως το πως μετατρέπει κάποιος ένα ομότιμο δίκτυο σε ένα επίπεδο ταυτότητας για το διαδίκτυο ; Και γιατί έγινε αναφορά το blockchain, είναι απαραίτητο ;

Η απάντηση βρίσκεται στην κρυπτογραφία δημοσίου κλειδιού, έναν κρυπτογραφικό τρόπο δηλαδή με τον οποίο δύο μέρη μπορούν να ανταλλάξουν δεδομένα με ασφάλεια και ιδιωτικότητα. Όσον αφορά το blockchain, στα πλαίσια της διαχείρισης ταυτότητας χρησιμοποιείται ως ένας τρόπος για την υλοποίηση μία αποκεντρωμένης δομής δημοσίου κλειδιού (Αγγλ. decentralized public key infrastructure). Αν και θα αναλυθεί στην συνέχεια, αξίζει να αναφερθεί ότι το blockchain παρέχει την δυνατότητα για τις εξής βασικές ιδιότητες:

- Ανταλλαγή δημοσίων κλείδων, ώστε να μπορεί να εδραιωθεί μία ιδιωτική και ασφαλή σύνδεση μεταξύ δύο ομότιμων.
- Αποθήκευση κάποιων από τα δημόσια κλειδιών, ώστε να μπορεί να επιβεβαιωθεί η ψηφιακή υπογραφή των *ψηφιακών διαπιστευτηρίων* που ανταλλάζουν μεταξύ τους οι ομότιμοι.

ΚΕΦΑΛΑΙΟ 2: ΒΑΣΙΚΕΣ ΤΕΧΝΟΛΟΓΙΕΣ

Βασικές αρχές κρυπτογραφίας 2.1

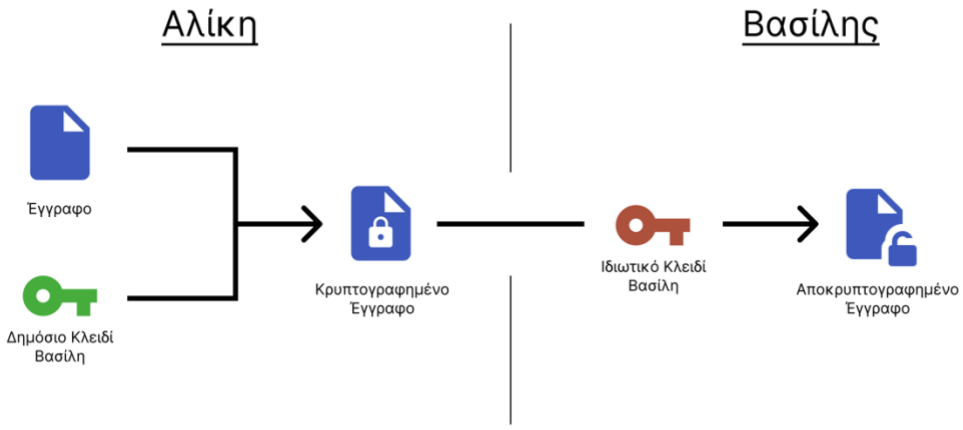
Τεχνικές κρυπτογραφίας 2.1.1

Συναρτήσεις κατακερματισμού 2.1.1.α

Σχήμα 4: συνάρτηση κατακερματισμού

Η συνάρτηση κατακερματισμού είναι μια συνάρτηση η οποία δέχεται ως είσοδο μια τιμή (ίσως κάποιο αλφαριθμητικό ή μια σειρά από κωδικολέξεις) και ως έξοδο της επιστρέφει ένα σταθερού μεγέθους, ντετερμινιστικό αποτέλεσμα, το οποίο είναι φαινομενικά τυχαίο. Το μέγεθος του αποτελέσματος είναι προκαθορισμένο από την συνάρτηση. Τα πιο σύνηθες εξ αυτών είναι 64bit, 128bit, 256bit κ.τ.λ. (δυνάμεις του δύο). Τέλος, λειτουργούν ως συναρτήσεις μίας κατεύθυνσης. Αυτό σημαίνει πως είναι πρακτικά αδύνατο να παράξει κάποιος την αρχική τιμή από το αποτέλεσμα τους.

Κρυπτογραφία δημοσίου κλειδιού 2.1.1.β



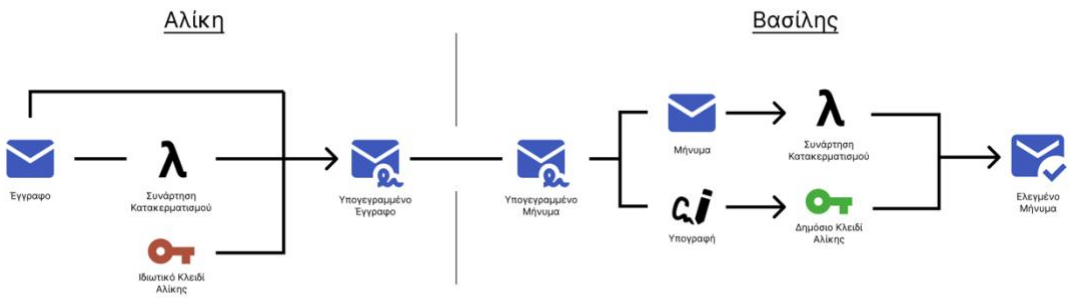
Σχήμα 5: κρυπτογραφία δημοσίου κλειδιού

Η κρυπτογραφία δημοσίου κλειδιού είναι μια κρυπτογραφική μέθοδος, η οποία χρησιμοποιεί ένα ζεύγος κλειδιών. Ως κλειδί ορίζεται μία σειρά από χαρακτήρες σταθερού μεγέθους. Κάθε ζευγάρι αποτελείται από ένα δημόσιο (γνωστό σε όλους) και ένα ιδιωτικό (γνωστό μόνο από τον ιδιοκτήτη) κλειδί. Η δημιουργία των κλειδιών αυτών γίνεται με διάφορους κρυπτογραφικούς μεθόδους, οι οποίες βασίζονται στην ιδιότητα της συνάρτησης προς μια κατεύθυνση. Το κάθε κλειδί έχει την δική του λειτουργία. Συνήθως το δημόσιο κλειδί είναι υπεύθυνο στην κρυπτογράφηση των δεδομένων και το ιδιωτικό κλειδί την αποκρυπτογράφηση. Η βασικότερη ιδιότητα της κρυπτογραφίας δημοσίου κλειδιού είναι πως τα δεδομένα που έχουν κρυπτογραφηθεί με ένα από τα δύο κλειδιά, μπορούν να αποκρυπτογραφηθούν μόνο από το ζευγάρι του.

Υπογραφές 2.1.2

Ψηφιακές υπογραφές 2.1.2.α

Μια ψηφιακή υπογραφή είναι μια κρυπτογραφική τεχνική με βασική της ιδιότητα την επαλήθευση της αυθεντικότητας ενός εγγράφου. Για την λειτουργία των υπογραφών απαραίτητη είναι η χρήση της κρυπτογραφίας δημοσίου κλειδιού.



Σχήμα 6: ψηφιακή υπογραφή

Στο σχήμα 6 υπάρχει όλος ο κύκλος μιας ψηφιακής υπογραφής (από την υπογραφή, μέχρι και την επαλήθευση).

Για την υπογραφή του εγγράφου η Αλίκη (παραπάνω φωτογραφία) ακολουθεί τα εξής βήματα:

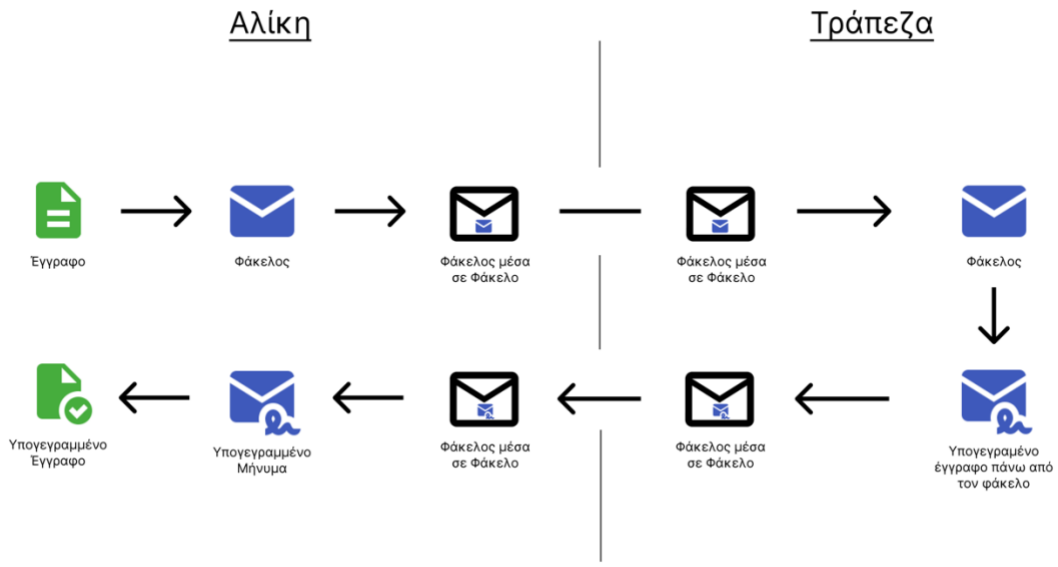
1. Αρχικά εισάγει ως είσοδο σε μία συνάρτηση κατακερματισμού το έγγραφο.
2. Στην συνέχεια, κρυπτογραφεί το αποτέλεσμα με το ιδιωτικό της κλειδί.
3. Τέλος, επισυνάπτει το αποτέλεσμα από το προηγούμενο βήμα στο έγγραφο.

Για την επαληθεύσει της υπογραφής της Αλίκης, ο Βασίλης θα ακολουθήσει τα εξής βήματα:

1. Αρχικά εισάγει το αρχικό έγγραφο ως είσοδο στην συνάρτηση κατακερματισμού.
2. Στην συνέχεια, χρησιμοποιεί το δημόσιο κλειδί της Αλίκης για να αποκρυπτογραφήσει την υπογραφή. Με αυτόν τον τρόπο, είναι σίγουρος ότι το έγγραφο έχει κρυπτογραφηθεί από την Αλίκη.
3. Τέλος, ελέγχει αν ταιριάζουν τα αποτελέσματα των βημάτων ένα και δυο.

Τυφλές υπογραφές 2.1.2.β

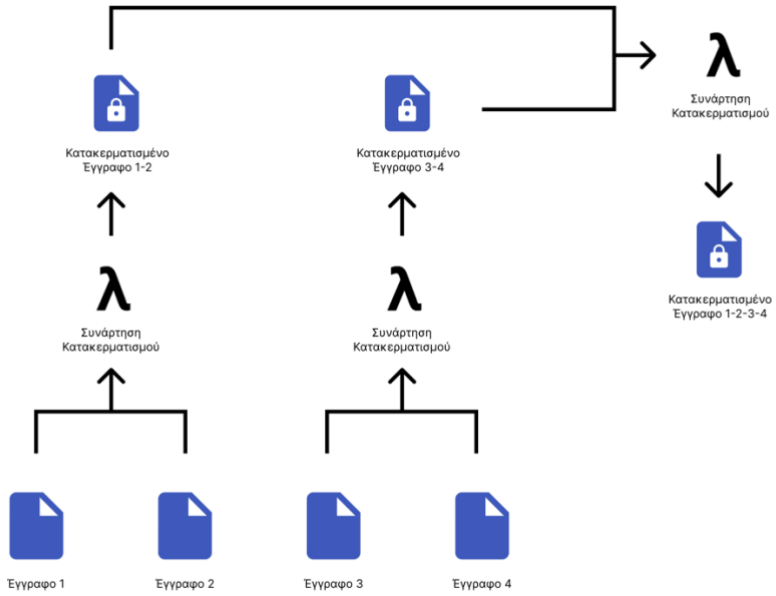
Η «τυφλές» υπογραφές είναι ένα είδους ψηφιακών υπογραφών, όπου το περιεχόμενο του μνήματος είναι «τυφλό» προτού υπογραφεί. Μια «τυφλή» υπογραφή μπορεί να επαληθευτεί ακριβώς όπως μια κανονική ψηφιακή υπογραφή. Ο λόγος που εμφανίστηκαν είναι διότι ο κάτοχος του μνήματος, μπορεί να μην επιθυμεί να μοιραστεί το περιεχόμενο του με αυτό που υπογράφει. Για παράδειγμα, ένας άνθρωπος θέλει την υπογραφή μιας τράπεζας σε ένα έγγραφο στο οποίο αναγράφεται ότι ο κάτοχος χρωστάει ένα χρηματικό ποσό σε κάποιον, χωρίς όμως να γνωρίζει η τράπεζα σε ποιον.



Σχήμα 7: τυφλή υπογραφή

Δέντρα κατακερματισμού 2.1.2.γ

Στην κρυπτογραφία, ένα δέντρο κατακερματισμού (ή ένα δέντρο Merkle), ονομάζεται το δέντρο στο οποίο κάθε φύλλο ορίζεται ως αποτέλεσμα μιας συνάρτησης κατακερματισμού. Ο εκάστοτε κόμβος αναπαρίστανται με το αποτέλεσμα της συνάρτησης κατακερματισμού των παιδιών του. Ένα δέντρο κατακερματισμού επιτρέπει έναν εύκολο και ασφαλή τρόπο επαλήθευσης κάποιου περιεχομένου, σε ένα μεγαλύτερο υποσύστημα.



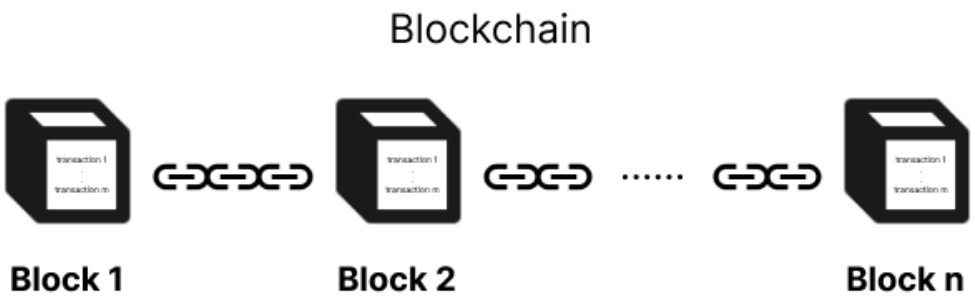
Σχήμα 8: δέντρο κατακερματισμού

Blockchain 2.2

Εισαγωγή 2.2.1

Το blockchain, ή αλλιώς μία «αλυσίδα από μπλοκ», παρουσιάστηκε το 2009 στα πλαίσια ενός κατανεμημένου, μη ελεγχόμενου από κάποια κεντρική αρχή ψηφιακού νομίσματος (Bitcoin [5]). Τροφοδοτείται από ένα μηχανισμό που ονομάζεται Τεχνολογία Κατανεμημένου Καθολικού (Αγγλ. Distributed Ledger Technology, DLT). Παρ' όλο που οι όροι blockchain και DLT χρησιμοποιούνται ως ισοδύναμοι στην βιβλιογραφία, αξίζει να επισημανθεί η διαφορά τους. Το blockchain αποτελεί ένα τύπο DLT, όπου τα δεδομένα αποθηκεύονται με μια συγκεκριμένη μορφή.

Η τεχνολογία κατανεμημένου καθολικού, αποτελεί αδιαμφισβήτητα τον πυρήνα ενός blockchain. Στην πιο βασική του ερμηνεία, ένα κατανεμημένο καθολικό είναι μία κοινή βάση δεδομένων την οποία συντηρεί συλλογικά ένα σύνολο από κόμβους (Αγγλ. nodes). Σε ένα περιβάλλον που χρησιμοποιείται blockchain, το κατανεμημένο καθολικό καταγράφει συναλλαγές (Αγγλ. transactions), τις οποίες ομαδοποιεί σε μπλοκ. Τα μπλοκ περιέχουν χρονοσήμανση επιτρέποντας έτσι στο καθολικό να διατηρεί μία χρονολογική κατάσταση. Έτσι, στο σχήμα 9 το μπλοκ 1 προέρχεται χρονικά του μπλοκ 2, όπως και το 2 του 3, και γενικά το n-1 του n. Τέλος, είναι εύκολο να παρατηρήσει κανείς ότι το όνομα που έχει λάβει το blockchain δεν είναι τυχαίο, αφού η συνολική αρχιτεκτονική μοιάζει σαν μία «αλυσίδα από μπλοκ».



Σχήμα 9: το blockchain

Τύποι Blockchain 2.2.2

Σε ένα δίκτυο blockchain, οι κάτοχοι των κόμβων μπορεί να έχουν διαφορετικούς ρόλους, γι' αυτό τον λόγο τα blockchains κατατάσσονται σε δύο κύριες κατηγορίες:

- Αδειοδοτούμενα ή ιδιωτικά (Αγγλ. permissioned ή private): Μόνο αυθεντικοποιημένοι και έμπιστοι χρήστες μπορούν να αλληλοεπιδράσουν με το καθολικό, διασφαλίζοντας έτσι την ιδιωτικότητα των δεδομένων που αποθηκεύονται στο blockchain.
- Μη αδειοδοτούμενα ή δημόσια (Αγγλ. permissionless ή public): Η πρόσβαση είναι ελεύθερη και η εμπιστοσύνη μεταξύ των μελών του δίκτυο δεν είναι υποχρεωτική.

Να σημειωθεί ότι μπορεί να υπάρξει ένας συνδυασμός των παραπάνω, ο οποίος οδηγεί σε ένα υβριδικό blockchain. Για παράδειγμα, σε ένα υβριδικό blockchain θα μπορούσανε μόνο ορισμένοι χρήστες να τροποποιήσουν την κατάσταση του καθολικού (state of the ledger), αλλά να μπορούν όλοι να διαβάσουν από αυτό.

Ταυτότητα στο blockchain 2.2.3

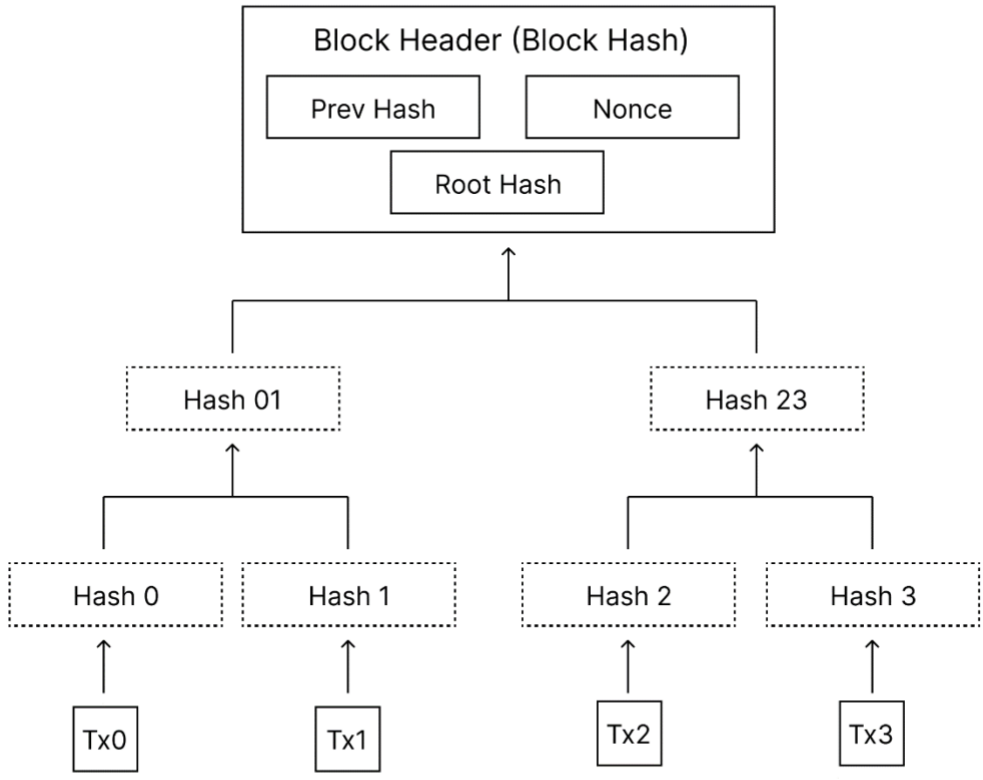
Ανάλογα με τον τύπο του blockchain, χρησιμοποιείται και διαφορετική προσέγγιση στην αναγνώριση των χρηστών.

Στα δημόσια blockchains, η ταυτότητα των χρηστών διαχειρίζεται χρησιμοποιώντας την δομή δημοσίου κλειδιού (Αγγλ. Public key Infrastructure, PKI). Ουσιαστικά, ο χρήστης δημιουργεί ένα ζευγάρι δημοσίου-ιδιωτικού κλειδιού και ύστερα χρησιμοποιεί μία συνάρτηση κατακερματισμού με είσοδο το δημόσιο κλειδί, δημιουργώντας έτσι ένα αναγνωριστικό για αυτόν. Η συνάρτηση κατακερματισμού, χρησιμοποιείται κατά κύριο λόγο για να μειώσει το μήκους της τελικής συμβολοσειράς που θα αποτελέσει το αναγνωριστικό. Τέλος, να αναφερθεί ότι διαφορετικά συστήματα χρησιμοποιούν και διαφορετικούς τρόπους για να οδηγηθούν στο παραπάνω αποτέλεσμα. Για παράδειγμα, στο σύστημα του Bitcoin το δημόσιο κλειδί κατακερματίζεται δύο φορές χρησιμοποιώντας τους αλγορίθμους SHA-256 και RipeMD-160 αντίστοιχα. Ύστερα προστίθεται στο αποτέλεσμα ένα άθροισμα ελέγχου (Αγγλ. checksum) ενός byte που αφορά το πρωτόκολλο, καταλήγοντας έτσι σε μία διεύθυνση μήκους 25 bytes. Από την άλλη, το Ethereum [6] κατακερματίζει το δημόσιο κλειδί χρησιμοποιώντας τον αλγόριθμο Keccak-256, εξάγοντας τα τελευταία 20 bytes (από τα 32) και θέτει ως πρόθεμα ένα σταθερό byte ('0x') δημιουργώντας έτσι μία διεύθυνση συνολικού μήκους 21 bytes.

Ομοίως στα ιδιωτικά blockchains, χρησιμοποιούνται διαφορετικοί τρόποι για να αναπαρασταθεί η ταυτότητα ενός χρήστη. Για παράδειγμα, στο Hyperledger Fabric [7], μία από τις μεγαλύτερες υλοποίησης ιδιωτικού blockchain, η ταυτότητα ενός χρήστη δομείται ως ένα πιστοποιητικό το οποίο αποτελείται από ένα σύνολο ιδιοτήτων (συμπεριλαβαίνοντας ένα δημόσιο κλειδί και ένα αναγνωριστικό) και συνοδεύεται από έναν κωδικό και ένα ιδιωτικό κλειδί. Οι ταυτότητες σε αυτήν τη περίπτωση δημιουργούνται αποκλειστικά από τον διαχειριστή του δικτύου.

Η δομή ενός blockchain 2.2.4

Έχοντας υπόψη το (απλοϊκό) blockchain του bitcoin, παρακάτω θα αναλυθεί η δομή του. Η κύρια λειτουργία ενός blockchain είναι να καταγράφει συναλλαγές στα λεγόμενα μπλοκ. Κάθε μπλοκ αποτελείται από 2 κύρια πεδία: την επικεφαλίδα και το περιεχόμενο. Η επικεφαλίδα περιλαμβάνει την τιμή από μία συνάρτηση κατακερματισμού που έχει λάβει ως είσοδο αρκετά πεδία δεδομένων από το μπλοκ, με τα πιο σημαντικά να είναι: η τιμή κατακερματισμού του προηγούμενου μπλοκ (Αγγλ. Prey Hash), την ρίζα από το δέντρο κατακερματισμού των συναλλαγών, μία χρονοσφραγίδα και ένα nonce. Η δομή ενός μπλοκ παρουσιάζεται στο σχήμα 10.

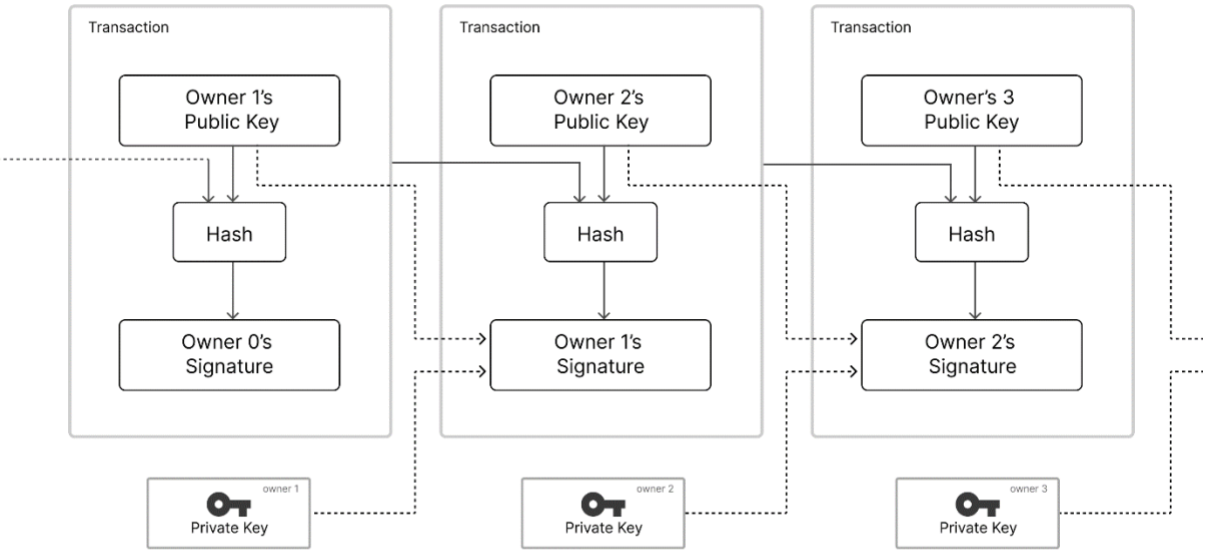


Σχήμα 10: δομή ενός μπλοκ

Μία σημαντική παρατήρηση είναι ότι κάθε μπλοκ αναφέρεται στο προηγούμενο και περιέχει μία χρονοσφραγίδα. Αυτά τα δεδομένα διασφαλίζουν ότι το blockchain έχει – και διατηρεί – μία χρονολογική σειρά, αφού ένα νέο μπλοκ δεν μπορεί να προστεθεί στην αλυσίδα αν η αναφορά στο

προηγούμενο είναι εσφαλμένη, ή αν η χρονοσφραγίδα ορίζεται σε χρόνο που προηγείται αυτόν του προηγουμένου.

Το περιεχόμενο ενός μπλοκ συνιστάται από συναλλαγές. Μία συναλλαγή υφίσταται μεταξύ δύο οντοτήτων, του παραλήπτη και του αποστολέα. Τα περιεχόμενα της περιέχουν, εκτός άλλων, το δημόσιο κλειδί του παραλήπτη, την τιμή κατακερματισμού της προηγούμενης συναλλαγής και μία υπογραφή από τον αποστολέα. Η υπογραφή του αποστολέα επιβεβαιώνεται με το δημόσιο κλειδί και έχει υπογραφθεί με το ιδιωτικό κλειδί του.



Σχήμα 11: περιεχόμενα συναλλαγών

Για να γίνει κατανοητή η αλληλεπίδραση των οντοτήτων στο blockchain, θα χρησιμοποιηθεί ένα παράδειγμα. Έστω ότι ο Βασίλης θέλει να κάνει μία συναλλαγή με την Αλίκη. Αρχικά, χρειάζεται το δημόσιο κλειδί της και το ιδιωτικό κλειδί του. Ύστερα, μέσω εξειδικευμένου λογισμικού, ο Βασίλης μπορεί να κάνει μία συναλλαγή με την Αλίκη, χρησιμοποιώντας το δημόσιο κλειδί της ως ληφθείσα διεύθυνση και υπογράφοντας την συναλλαγή με το ιδιωτικό του κλειδί. Στην συνέχεια, η συναλλαγή εκπέμπεται στο δίκτυο ώστε οι ομότιμοι να επιβεβαιώσουν ότι ο Βασίλης μπορεί να πραγματοποιήσει την συναλλαγή (π.χ. έχει αρκετό υπόλοιπο) και η συναλλαγή ομαδοποιείται μέσα σε ένα μπλοκ μαζί με άλλες. Το μπλοκ αυτό είναι έτοιμο να «εξορυχθεί» (Αγγλ.'mined'), ώστε να αποδειχθεί η ακεραιότητα του και να επιτευχθεί συναίνεση για την καινούργια κατάσταση του blockchain. Η διαδικασία της επικύρωσης των μπλοκ και της επιτυχίας συναίνεσης, ονομάζεται μηχανισμός συναίνεσης (Αγγλ. Consensus mechanism).

Μηχανισμοί συναίνεσης 2.2.5

Κάθε κόμβος που εμπλέκεται στο δίκτυο πρέπει να συμφωνεί ότι το blockchain βρίσκεται σε συγκεκριμένη μία κατάσταση. Ο αλγόριθμος ο οποίος ορίζει την διαδικασία με την οποία κάθε κόμβος επεξεργάζεται την αλλαγή κατάστασης, ονομάζεται Μηχανισμός Συναίνεσης. Σε γενικότερα πλαίσια, παρατηρούνται 2 τύποι, ο πρώτος βασίζεται σε Αποδείξεις (Αγγλ. Proofs) και ο δεύτερος στην Επικύρωση (Αγγλ. Validation). Οι μηχανισμοί που βασίζονται στις αποδείξεις είναι

καταλληλότεροι για δημόσια blockchains και αντίστοιχα, οι μηχανισμοί Επικύρωσης χρησιμοποιούνται κατά κύριο λόγο σε αδειδοτούμενα περιβάλλοντα.

Το blockchain του bitcoin, χρησιμοποιεί τον μηχανισμό Proof-of-Work (POW), και όπως παραπέμπει και το όνομα του, ο αλγόριθμός βασίζεται στο γεγονός ότι οι κόμβοι χρησιμοποιούν επεξεργαστική ισχύ για να αποδείξουν ότι έχουν εκτελέσει κάποια εργασία. Κατά την δημιουργία ενός μπλοκ, χρησιμοποιείται ένας τυχαίος αριθμός (στην βιβλιογραφία αναφέρεται ως nonce), ο οποίος επισυνάπτεται στα δεδομένα του μπλοκ και προσαυξάνεται διαδοχικά, έτσι ώστε η τελική συνάρτηση κατακερματισμού να ικανοποιεί μία δύσκολη συνθήκη που ορίζεται από το πρωτόκολλο του δικτύου. Για παράδειγμα, η τελική τιμή κατακερματισμού να ξεκινάει με 4 μηδενικά. Λόγω του γεγονότος ότι ένα μπλοκ αναφέρεται στο προηγούμενο, αν επιβεβαιωθεί είναι πρακτικά αμετάτρεπτο. Στην περίπτωση που κάποιος κακόβουλος χρήστης θέλει να τροποποιήσει τα δεδομένα ενός μπλοκ, έστω το x, πρέπει να ξανά υπολογίσει όλα τα proof-of-work από το x μέχρι το τωρινό. Κάτι τέτοιο θα απαιτούσε πρόσβαση σε ένα σημαντικό αριθμό πόρων, και έχει αποδειχθεί ότι αυτό είναι οικονομικά αδύνατο. Το κίνητρο για τους κατόχους των κόμβων που επικυρώνουν μπλοκ είναι ένα ποσό κρυπτονομίσματος, που δίνεται ως ανταμοιβή. Τέλος, όπως μπορεί να παρατηρήσει κάποιος ένα από τα σημαντικότερα μειονεκτήματα της συγκεκριμένης προσέγγισης, είναι ότι η ηλεκτρική ενέργεια που απαιτείται για την επεξεργαστική ισχύ απλώς σπαταλιέται.

Τα ιδιωτικά blockchains έχουν διαφορετικές ιδιότητες και απαιτήσεις από τα δημόσια. Γι' αυτόν τον λόγο έχουν προταθεί διαφορετικοί μηχανισμοί για την επίτευξη της συναίνεσης του δικτύου. Παράδειγμα αποτελεί η οικογένεια αλγορίθμων Proof-of-Authority, όπου επιλέγονται συγκεκριμένοι κόμβοι οι οποίοι έχουν δικαίωμα να επικυρώσουν και να δημιουργήσουν καινούργια μπλοκ. Οι παραπάνω κόμβοι ονομάζονται επαληθευτές (Αγγλ. Validators). Παραδείγματα υλοποιήσεων είναι οι αλγόριθμοι Aura[1] και Clique[2].

Επαληθεύσιμα διαπιστευτήρια 2.3

Εισαγωγή 2.3.1

Στην τωρινή καθημερινότητα, η χρήση των *διαπιστευτηρίων* είναι αρκετά σύνηθες. Κάθε φορά που χρησιμοποιείται κάποιο φυσικό έγγραφο το οποίο *επαληθεύει* κάποια ιδιότητα για μία οντότητα, αποτελεί και ένα παράδειγμα. Φυσικά, τα παραπάνω διαπιστευτήρια, όπως η αστυνομική ταυτότητα, το δίπλωμα οδήγησης ή ένα διαβατήριο, βρίσκονται σε φυσική μορφή και αυτό τα καθιστά την χρήση τους στο διαδίκτυο δύσκολη. Επίσης, τα φυσικά έγγραφα εν γένει μπορούν να πλαστογραφηθούν και απαιτούν εξειδίκευση από αυτόν που τα ελέγχει, ώστε να πιστοποιηθεί η εγκυρότητα τους. Από την άλλη, τα Επαληθεύσιμα Διαπιστευτήρια (Αγγλ. Verifiable Credentials, VCs) αποτελούν μία προσπάθεια ψηφιοποίησης των παραπάνω και έχουν προτυποποιηθεί από τον οργανισμό W3C [8], όπου με την χρήση κρυπτογραφίας, καθίσταται εξαιρετικά δύσκολο να παραποιηθούν ή να παραβιαστούν και φυσικά παρέχουν ασφάλεια και ευχρηστία στο διαδίκτυο.

Για παράδειγμα, μία περίπτωση χρήσης των VCs θα μπορούσε να είναι η δημιουργία ενός τραπεζικού λογαριασμού. Για μία τέτοια ενέργεια, ένας υπάλληλος της τράπεζας θα απαιτούσε από τον αιτών επίσημα έγραφα σε φυσικά μορφή, τα οποία επαληθεύουν κάποιες ιδιότητες του. Με την χρήση των VCs το μόνο που χρειάζεται ο αιτών είναι μία ηλεκτρονική συσκευή (συνήθως ένα έξυπνο κινητό τηλέφωνο) στην οποία θα έχει αποθηκευμένα VCs, όπως μία αστυνομική ταυτότητα η οποία πιστοποιεί την ηλικία και το όνομα του (από την κυβέρνηση) και ένα λειτουργικό λογαριασμό (από μία εταιρία παροχής ενέργειας) ο οποίος πιστοποιεί την διεύθυνση κατοικίας. Αυτονόητο είναι ότι η τράπεζα πρέπει να *εμπιστεύεται* την κυβέρνηση και την εταιρία παροχής ενέργειας, ώστε να δεχτεί

[1] https://github.com/paritytech/parity/wiki/Aura

[2] https://eips.ethereum.org/EIPS/eip-225

τα VCs. Ύστερα, με την σειρά της η τράπεζα θα αναθέσει στον αιτών ένα καινούργιο σύνολο από VCs, με τις λεπτομέρειες του τραπεζικού λογαριασμού. Τέλος, είναι στο χέρι του πως θα χρησιμοποιήσει τα καινούργια VCs από την τράπεζα, για παράδειγμα θα μπορούσε να τα προωθήσει σε κάποιον εργοδότη ώστε να λαμβάνει μηνιαίες απολαβές.

Το οικοσύστημα 2.3.2

Όπως γίνεται αντιληπτό στο οικοσύστημα των VCs εμπλέκονται αρκετές οντότητες και ρόλοι, που παρουσιάζονται στο σχήμα 12.

Σχήμα 12: το οικοσύστημα των VCs

Κατ' επέκταση τα δομικά στοιχεία της παραπάνω αρχιτεκτονικής είναι:

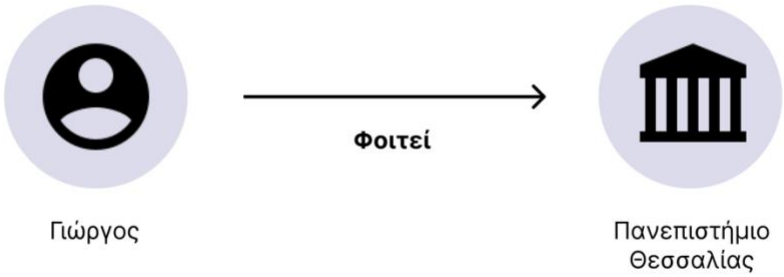
- *Εκδότης (Αγγλ. Issuer):* Η οντότητα αυτή είναι υπεύθυνη να ελέγχει τους ισχυρισμούς για ένα ή περισσότερα *υποκείμενα*, ύστερα να δημιουργεί τα αντίστοιχα VCs και τέλος, να τα μεταφέρει σε κάποιον κάτοχο. Παραδείγματα αποτελούν οι επιχειρήσεις, το ίδιο το κράτος, εκπαιδευτικά ιδρύματα, κ.λπ.
- *Υποκείμενο (Αγγλ. Subject):* Η οντότητα της οποίας οι *ιδιότητες* αποθηκεύονται σε ένα VC. Στις περισσότερες περιπτώσεις, ένας κάτοχος είναι και ο ίδιος το υποκείμενο του διαπιστευτηρίου, αλλά αυτό δεν είναι δεσμευτικό. Για παράδειγμα, ένα Κέντρο Τεχνικού Ελέγχου Οχημάτων θα μπορούσε να εκδώσει ένα διαπιστευτήριο ότι ένα όχημα έχει πιστοποιηθεί ως προς την ασφαλής λειτουργεία του. Σε αυτήν την περίπτωση το υποκείμενο είναι το όχημα, αλλά κάτοχος του διαπιστευτηρίου είναι ο ιδιοκτήτης.
- *Επαληθευτής (Αγγλ. Verifier):* Η οντότητα που λαμβάνει ένα ή περισσότερα VCs, ώστε να προβεί σε κάποια απόφαση. Σε συνέπεια με το παραπάνω παράδειγμα, οι αστυνομικές αρχές θα μπορούσαν να επαληθεύσουν το διαπιστευτήριο του αυτοκινήτου σε κάποιον έλεγχο.
- *Μητρώο Επαληθεύσιμων Δεδομένων (Αγγλ. Verifiable Data Registry):* Διαισθητικά, αποτελεί ένα μητρώο (ή και *αποθήκη*) το οποίο είναι προσβάσιμο από το διαδίκτυο και διατηρεί τα απαραίτητα δεδομένα και μεταδεδομένα τα οποία επιτρέπουν την λειτουργεία του οικοσυστήματος. Παραδείγματα μητρώων είναι έμπιστες βάσεις δεδομένων ή ένα αποκεντρωμένο καθολικό (Αγγλ. Distributed Ledger).

Βασικά Μοντέλα Δεδομένων 2.3.3

Υπό το πρίμα των VCs (αλλά και γενικά της ψηφιακής ταυτότητας) ορίζονται κάποια βασικά μοντέλα δεδομένων.

Αρχικά, ένας *Ισχυρισμός (Αγγλ. Claim)* αποτελεί μία δήλωση για ένα *Υποκείμενο,* όπου υποκείμενο θεωρούμε οποιαδήποτε οντότητα μπορεί να λάβει ιδιότητες.

Σχήμα 13: η δομή ενός ισχυρισμού



Σχήμα 14: παράδειγμα ισχυρισμού

Ύστερα, τα *Διαπιστευτήρια (Αγγλ. Credentials)* αποτελούν ένα σύνολο ενός ή και περισσότερων ισχυρισμών. Ένα διαπιστευτήριο μπορεί να περιέχει και μεταδεδομένα τα οποία περιγράφουν ιδιότητες του, όπως τον εκδότη του, την ημερομηνία λήξης, τον τρόπο ανάκλησης του, κ.λπ. Για να υφίσταται ένα διαπιστευτήριο στα πλαίσια του SSI, οι ισχυρισμοί που εμπεριέχονται θα πρέπει να είναι *επαληθεύσιμοι*, το οποίο σημαίνει ότι οποιαδήποτε στιγμή ο *επαληθευτής* θα πρέπει να είναι σε θέση να αποφασίσει:

- Ποιος έχει εκδώσει το διαπιστευτήριο.
- Το διαπιστευτήριο δεν έχει παραποιηθεί από την στιγμή έκδοσης του.
- Το διαπιστευτήριο δεν έχει λήξει ή ανακληθεί.

Σχήμα 15: αντιστοίχιση ενός VC με την προσωρινή άδεια οδήγησης

Βασικές ιδιότητες και συντακτική αναπαράσταση 2.3.4

Σύμφωνα με το μοντέλο του W3C, ο τρόπος με τον οποίο αναπαρίσταται ένα VC βασίζεται στο JSON [3] (JavaScript Object Notation), το οποίο αποτελεί ένα ανοικτό πρότυπο αναπαράστασης συνόλων δεδομένων. Ένα JSON αποτελείται από ζευγάρια με κλειδιά-τιμές, όπου κάθε ζευγάρι ορίζεται ως ένα κλειδί τύπου συμβολοχαρακτήρα, μία τιμή και μία άνω και κάτω τελειά ανάμεσα τους.

```
{
  "ιδιότητα": "φοιτητής",
  "τμήμα": "Πληροφορικής και τηλεπικοινωνιών",
  "επικοινωνία": {
    "σταθερό": "2100000000",
    "κινητό": "6900000000",
  },
}
```

Σχήμα 16: παράδειγμα JSON

Ενώ το JSON επιτρέπει την αναπαράσταση δεδομένων σε δενδροειδή μορφή, δεν υπάρχουν προκαθορισμένα σύνολα ιδιοτήτων. Όλα τα κλειδιά και οποιαδήποτε τιμή είναι αποδεκτά. Τυποποιώντας ένα σύνολο ιδιοτήτων για τα VCs, καθιστά εφικτή την αυτόματη δημιουργία και χρήση τους. Για αυτόν τον λόγο, χρησιμοποιείται το πρότυπο JSON-LD[4], το οποίο επιτρέπει την χρήση προκαθορισμένων *σχημάτων (Αγγλ. Schemas)* για την περιγραφή των δεδομένων. Για παράδειγμα ένα σχήμα αποτελεί το Person [5], το οποίο περιγράφει ιδιότητες ενός ατόμου.

Τα σχήματα τοποθετούνται στην ιδιότητα @context και ύστερα, η ιδιότητα type ορίζει ποια συγκεκριμένα σχήματα θα χρησιμοποιηθούν. Για παράδειγμα, στο Κομμάτι Κώδικα 2 χρησιμοποιούνται οι ιδιότητες από το σχήμα Verifiable-Credential το οποίο βρίσκεται στην διεύθυνση https://www.w3.org/2018/credentials/v1 και η ιδιότητα alumniOf του σχήματος Person που βρίσκεται στο https://schema.org. Όπως μπορεί να παρατηρηθεί, μία διεύθυνση μπορεί να περιέχει περισσότερα από ένα σχήματα, και να αναφέρεται συγκεκριμένα στο JSON-LD ποια χρησιμοποιούνται.

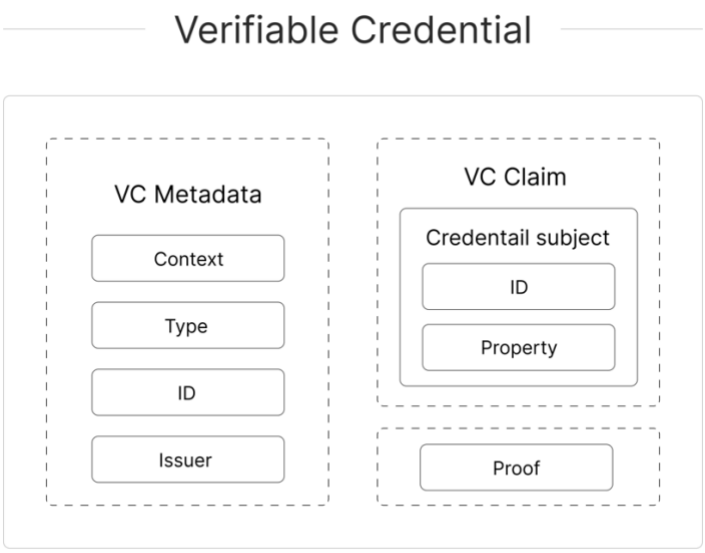
[3] https://www.json.org
[4] https://json-ld.org/
[5] https://schema.org/Person

```
{
 "@context": [
   "https://www.w3.org/2018/credentials/v1",
   "https://schema.org",
  ],
  "id": "http://example.edu/credentials/58473",
  "type": [
   "VerifiableCredential",
   "Person"
  ],
  "credentialSubject": {
   "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
   "alumniOf": "Example University"
  },
  "proof": { ... }
}
```

Σχήμα 17: παράδειγμα JSON-LD

Η συγκεκριμένη προσέγγιση είναι αρκετά ευέλικτη, αφού οποιοσδήποτε μπορεί να δημιουργήσει ένα σχήμα (το οποίο καλείται *context)*, να το μεταμορφώσει σε μία διεύθυνση στο διαδίκτυο και ύστερα να αναφέρει τις ιδιότητες του σχήματος σε ένα επαληθεύσιμο διαπιστευτήριο. Για παράδειγμα, το κράτος θα μπορούσε να δημιουργήσει ένα σχήμα για την απόκτηση πτυχίου και τα εκπαιδευτικά ιδρύματα να το χρησιμοποιούν.

Έχοντας υπόψη την συντακτική αναπαράσταση, παρακάτω παρουσιάζονται οι βασικές ιδιότητες.



Σχήμα 18: η δομή ενός VC

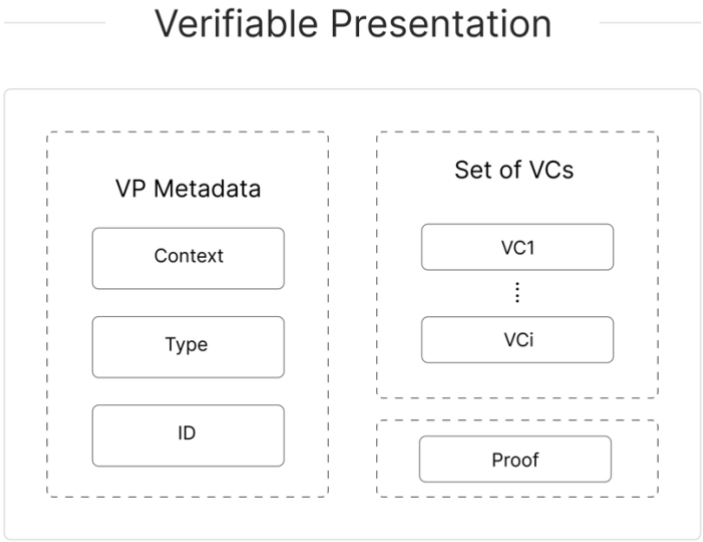
- @Context—Αποτελεί μία ακολουθία Ενιαίων Αναγνωριστικών Πόρων (Αγγλ. Unique Resource Identifier, URI), όπου κάθε URI υποδεικνύει σε ένα μηχανικά αναγνωρίσιμο (Αγγλ. machine-readable) έγγραφο. Κάθε έγγραφο, περιλαμβάνει ένα λεξιλόγιο το οποίο ένας

επαληθευτής μπορεί να τηλεφορτώσει και διαχειριστεί με αυτόματο τρόπο. Να σημειωθεί, ότι τα URIs μπορεί να υποδεικνύουν σε μια φιλική προς τον άνθρωπο προδιαγραφή, ώστε κάποιος διαχειριστής να είναι σε θέση να κατανοήσει το περιεχόμενο τους και να διαμορφώσει το λογισμικό του επαληθευτή κατάλληλα. Τέλος, κάθε URI μπορεί να περιέχει περισσότερή πληροφορία απ' ότι χρειάζεται ο επαληθευτής, οπότε χρησιμοποιείται η ιδιότητα type.

- type—Αποτελεί μία ακολουθία από URIs, τα οποία πρέπει αντιστοιχίζονται στους τύπους που έχουν οριστεί στην ιδιότητα @context. Να σημειωθεί ότι ο πρώτος τύπος πρέπει πάντα να είναι ο https://www.w3.org/2018/credentials/v1, ο οποίος μπορεί να συμπτυχθεί σε VerifiableCredentials, εφόσον έχει συμπεριληφθεί στην ιδιότητα @context.
- id—Η ιδιότητα αυτή είναι το μοναδικό αναγνωριστικό του VC, το οποίο δημιουργεί και αναθέτει ο εκδότης. Επιτρέπει σε κάποια οντότητα να μπορεί να αναφερθεί με σαφήνεια στο συγκεκριμένο VC.
- issuer—Η ιδιότητα αυτή ταυτοποιεί τον εκδότη. Είναι ένα URI, το οποίο υποδεικνύει σε ένα έγγραφο που περιέχει όλες τις πληροφορίες για τον εκδότη.
- credentialsSubject—Η ιδιότητα αυτή περιέχει τους ισχυρισμούς που κάνει ο εκδότης σχετικά με ένα υποκείμενο. Αποτελείται από ένα αναγνωριστικό και ένα σύνολο ιδιοτήτων.
- proof—Για να είναι ένα διαπιστευτήριο επαληθεύσιμο, χρειάζεται μία κρυπτογραφική υπογραφή. Η υπογραφή αυτή, αποδεικνύει τον εκδότη του VC και ότι τα περιεχόμενα του δεν έχουνε αλλοιωθεί. Να σημειωθεί, ότι υπάρχει κι' άλλος κρυπτογραφικός τρόπος απόδειξης των παραπάνω, χρησιμοποιώντας JWTs (JSON Web Tokens).

Επαληθεύσιμες Παρουσιάσεις 2.3.5

Μία Επαληθεύσιμη Παρουσίαση (Αγγλ. Verifiable Presentations, VP) επιτρέπει σε έναν κάτοχο να συνδυάσει VCs, ώστε να τα αποστείλει σε έναν επαληθευτή. Είναι παρόμοια με ένα VC, ως προς το γεγονός ότι περιέχει μεταδεδομένα σχετικά με την ίδια την παρουσίαση και την απόδειξη, η οποία είναι κρυπτογραφικά υπογεγραμμένη από τον κάτοχο. Σε σύγκριση με ένα VC, το βασικό περιεχόμενο είναι ένα σύνολο από VC. Επίσης, μία ακόμη σημαντική διαφορά είναι η απουσία του issuer, σαν ιδιότητα, κάτι το οποίο γίνεται εφικτό λόγω της χρήσης της μεθόδου ZKP (zero knowledge proof).



Σχήμα 19: δομή ενός VP

Αποκεντρωμένα Αναγνωριστικά 2.4

Εισαγωγή 2.4.1

Η ιδέα των αποκεντρωμένων αναγνωριστικών 2.4.1.α

Τα αποκεντρωμένα αναγνωριστικά είναι ένας από τους τρεις βασικότερους τεχνολογικούς πυλώνες για την υλοποίηση ενός αποκεντρωμένου συστήματος αυτοδιαχειριζόμενης ταυτότητας.

Μια αναλογία για τα νέα αυτά αναγνωριστικά που μπορεί να δοθεί είναι οι IP διευθύνσεις [9]. Τα δύο αναγνωριστικά αυτά έχουν παρόμοια χρήση, με την μεγαλύτερη τους διαφορά να παρατηρείται στο ότι τα αποκεντρωμένα αναγνωριστικά χρησιμοποιούνται στο επίπεδο εμπιστοσύνης πάνω στο διαδίκτυο, ενώ η διευθύνσεις (IP) αποσκοπούν στην επικοινωνία και διασύνδεση των οντοτήτων ενός δικτύου.

Ένα αποκεντρωμένο αναγνωριστικό ανήκει σε μια οντότητα (άνθρωπο, οργάνωση, εταιρία ή κάτι άλλο). Σε αντίθεση με τα ελεγχόμενα από κάποια κεντρική αρχή αναγνωριστικά, τα αποκεντρωμένα αναγνωριστικά έχουν σχεδιαστεί ούτω ώστε να μην βασίζονται σε κάποιο κεντρικοποιημένο σύστημα αποθήκευσης. Η λειτουργία αυτή επιτυγχάνεται με διάφορους κρυπτογραφικούς τρόπους, οι οποίοι ελέγχουν την εγκυρότητα του κατόχου.

Με μια πιο τεχνολογική προσέγγιση τα αποκεντρωμένα αναγνωριστικά είναι ένα είδος μοναδικών αναγνωριστικών (URIs), τα οποία βοηθάνε στην επανάκτηση κάποιων εγγράφων (ή μεταδεδομένων), μέσα από κάποιο αποκεντρωμένο σύστημα (όπως Blockchain). Κάθε έγγραφο εμπεριέχει κάποια μεταδεδομένα τα οποία είναι χρήσιμα για την ομαλή λειτουργία του αποκεντρωμένου και αυτοδιαχειριζόμενου συστήματος ταυτότητας.

Θεμελιώδης ιδιότητες 2.4.1.β

Ο λόγος που εμφανίστηκαν τα αναγνωριστικά αυτά, είναι επειδή έχουν τις παρακάτω τέσσερις βασικές ιδιότητες [9]:

1. **Επιμονή (Αγγλ. Persistence):** Είναι στην κατοχή μιας οντότητας για πάντα μέχρις ότου να αποσυρθούν.
2. **Αναζητούμενο (Αγγλ. Resolvable):** Είναι εύκολα αναζητήσιμα, αυτό έμμεσα παραπέμπει στην μοναδικότητα τους.
3. **Κρυπτογραφικά Επαληθεύσιμα (Αγγλ. Cryptographically-Verifiable):** Είναι κρυπτογραφικά επαληθεύσιμα, δηλαδή μπορεί να γίνει ο έλεγχος της κατοχής τους με κάποιο κρυπτογραφικό μέσο.
4. **Αποκεντρωμένο (Αγγλ. Decentralized):** Δεν βασίζονται σε κάποιο κεντρικοποιημένο σύστημα.

Υπάρχουν αρκετών ειδών αναγνωριστικά τα οποία είναι στην διάθεση μας. Κάποια από αυτά μπορεί να είναι το ονοματεπώνυμο, το τηλέφωνο όπως και διάφορα άλλα, εκ των οποίων κανένα δεν πληροί και τις **τέσσερις** ιδιότητες που προαναφέρθηκαν.

Στον πίνακα 1 υπάρχει μια σύγκριση τριών διαφορετικών αναγνωριστικών [9], μεταξύ των οποίων είναι το «URL», το «Email» και τα αποκεντρωμένα αναγνωριστικά (με όνομα did). Η σύγκριση αυτή κάνει πιο ξεκάθαρη την παρουσία αυτού του νέου είδους αναγνωριστικών.

Ιδιότητες	URL	Email	DID
Επιμονή	✗	✗	✓
Αναζητούμενο	✓	✗	✓
Κρυπτογραφικά Επαληθεύσιμα	✗	✗	✓
Αποκεντρωμένο	✗	✗	✓
Φιλικό	✓	✓	✗

Πίνακας 1: σύγκριση DID με λοιπά αναγνωριστικά

Στις ιδιότητες των αναγνωριστικών υπάρχει ένα ακόμα πεδίο με το όνομα «φιλικό», που παραπέμπει στο πόσο φιλικό είναι το εκάστοτε αναγνωριστικό προς τους ανθρώπους.

Βλέποντας τον πίνακα 1, είναι φανερό πως τα αποκεντρωμένα αναγνωριστικά πληρούν όλες τις προϋποθέσεις που χρειάζεται να έχει ένα αναγνωριστικό για ένα αποκεντρωμένο σύστημα αυτοδιαχειριζόμενης ταυτότητας, σε σχέση με τα υπόλοιπα.

Σύνταξη 2.4.2

Βασικό σχήμα 2.4.2.α

Με βάση την έκδοση 1.0 των DIDs (decentralized identifiers) από την World Wide Web Consortium [10], η οποία έχει αναλάβει την επίβλεψη και ανάπτυξη των αποκεντρωμένων αναγνωριστικών, ένα αποκεντρωμένο αναγνωριστικό αποτελείται από τρία μέρη: σχήμα, μέθοδο και αλφαριθμητικό. Παρακάτω υπάρχει η αναλυτική τους περιγραφή.

1. **Σχήμα (Αγγλ. Schema):** Ένα πρόθεμα το οποίο αναφέρεται στο είδος του αναγνωριστικού. Τα αποκεντρωμένα αναγνωριστικά έχουν την τιμή «did» ως πρόθεμα.
2. **Μέθοδος (Αγγλ. Method):** Η μέθοδος εξαγωγής του αποκεντρωμένου εγγράφου από το περιβάλλον όπου φυλάσσεται. Ουσιαστικά, το κομμάτι αυτό αναφέρεται στο σύστημα όπου είναι αποθηκευμένα κάποια μεταδεδομένα του αναγνωριστικού. Ένας πιθανός τύπος αποθήκευσης των μεταδεδομένων ενός αποκεντρωμένου αναγνωριστικού μπορεί να είναι το Blockchain. Κάποια Blockchain που υποστηρίζουν σήμερα την τεχνολογία των αποκεντρωμένων αναγνωριστικών παρουσιάζονται στον πίνακα 2.

   Το παραπάνω κομμάτι αναφέρεται στα δημόσια αποκεντρωμένα αναγνωριστικά, παρόλα αυτά υπάρχουν και ιδιωτικά. Τα ιδιωτικά αποκεντρωμένα αναγνωριστικά (ή αλλιώς «όμοια» αναγνωριστικά) μπορούν να ανταλλαχθούν μεταξύ δυο οντοτήτων, για να δημιουργήσουν μεταξύ τους κανάλια εμπιστοσύνης, ούτως ώστε να επιτύχουν μια ασφαλής επικοινωνία. Ο τρόπος με τον οποίο επιτυγχάνεται αυτό δεν πρέπει να βασίζονται σε κάποιο

σύστημα. Τέλος, ο αριθμός των ιδιωτικών αναγνωριστικών όπου μια οντότητα μπορεί να δημιουργήσει, είναι θεωρητικά άπειρος.

Για να καταλάβει μια οντότητα ότι το αναγνωριστικό είναι ιδιωτικό και όχι δημόσιο, θα πρέπει να λάβει στο πεδίο της μεθόδου την τιμή «peer».

3. **Αλφαριθμητικό (Αγγλ. Method-Specific Identifier):** Ένα μοναδικό αλφαριθμητικό το οποίο είναι υπεύθυνό για να εντοπίσει το έγγραφο με τα σωστά μεταδεδομένα, για το εκάστοτε αναγνωριστικό.

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

Πίνακας 2: μέθοδοι DID

Εφόσον είναι γνωστά τα τρία μέρη ενός αποκεντρωμένου αναγνωριστικού, ένα παράδειγμα είναι:

did:example:123456789abcdefghi

Το παραπάνω αναγνωριστικό (σχήμα, did), έχει στο example (μέθοδος) ένα έγγραφο με την τιμή 123456789abcdefghi (αλφαριθμητικό).

Σχήμα URL 2.4.2.β

Ένα URL ενός αποκεντρωμένου αναγνωριστικού (αποκεντρωμένα URL), βοηθάει στην εύρεση στοχευμένων πληροφοριών μέσα σε ένα δίκτυο. Το URL αυτό, χρησιμοποιείται κυρίως για να επιστρέψει πληροφορίες οι οποίες βρίσκονται μέσα σε ένα αποκεντρωμένο έγγραφο (μέθοδοι επαλήθευσης, υπηρεσίες κ.α.).

Τα αποκεντρωμένα URLs αποτελούνται, αρχικά από το σχήμα του αναγνωριστικού ακολουθούμενα είτε από paths, είτε από queries, είτε από fragments. Και τα τρία είδη αναφέρονται στο [RFC3986]. Πιο αναλυτικά:

1. **Path:** Το «path» (μονοπάτι) ενός αποκεντρωμένου αναγνωριστικού, έχει την ίδια λογική με το μονοπάτι ενός URI. Σε συνέπεια με τα URIs, τα μονοπάτια των αποκεντρωμένων αναγνωριστικών βοηθάνε στην μέθοδο αναζήτησης του αποκεντρωμένου εγγράφου. Ουσιαστικά, δίνουν περαιτέρω πληροφορίες για την τοποθεσία του ίδιο του εγγράφου. Για παράδειγμα:

did:example:123456/path

2. **Query:** Το «query» ενός αποκεντρωμένου αναγνωριστικού, έχει την ίδια λογική με το «query» ενός URI. Σε συνέπεια με τα URIs, τα «queries» έχουν κάποιες προκαθορισμένες

τιμές που μπορούν να λάβουν. Οι τιμές αυτές είναι «service», «relativeRef», «versionId», «versionTime», «hl». Ένα πιθανό παράδειγμα ενός «query» είναι:

did:example:123?service=files&relativeRef=/resume.pdf

3. **Fragment:** Το «fragment» ενός αποκεντρωμένου αναγνωριστικού, έχει την ίδια λογική με το «fragment» ενός URI. Τα «fragments» χρησιμοποιούνται χωρίς να βασίζονται στην μέθοδο του αποκεντρωμένου αναγνωριστικού και παραπέμπουν σε κάποια πληροφορία η οποία βρίσκεται μέσα στο αποκεντρωμένο έγγραφο. Ένα παράδειγμα ενός «fragment» είναι:

did:example:123#public-key-0

Αποκεντρωμένα Έγγραφα 2.4.3

Εισαγωγή 2.4.3.α

Ένα αποκεντρωμένο έγγραφο είναι απλά ένα JSON-LD αντικείμενο, το οποίο αποθηκεύεται σε κάποιο εύκολα προσβάσιμο μέρος. Για να μπορέσει κάνεις να αναζητήσει ένα τέτοιο έγγραφο, θα πρέπει να έχει στην κατοχή του το αντίστοιχο αναγνωριστικό. Στο κομμάτι κώδικα 1 φαίνεται ένα παράδειγμα ενός αποκεντρωμένου εγγράφου.

EXAMPLE 11: DID document with a controller property

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123456789abcdefghi",
  "controller": "did:example:bcehfew7h32f32h7af3",
}
```

Σχήμα 20: παράδειγμα εγγράφου DID. Πηγή: https://www.w3.org/TR/did-core/#example-did-document-with-a-controller-propert

Τα πεδία που εμφανίζονται στο κομμάτι κώδικα 1 είναι το «@context» (το οποίο βασίζεται στο JSON-LD πρότυπο), «id» και «controller». Όλα τα πεδία τα οποία υποστηρίζει ένα αποκεντρωμένο έγγραφο (σύμφωνα με το πρότυπο του W3C v1) εμφανίζονται στον πίνακα 3.

Πεδίο	Υποχρεωτικό
id	✔
alsoKnownAs	✘
controller	✘
verificationMethod	✘
authentication	✘
assertionMethod	✘
keyAgreement	✘
capabilityInvocation	✘
capabilityDelegation	✘
service	✘
Το **verificationMethod** πεδίο εμπεριέχει:	
id	✔
controller	✔
type	✔
publicKeyJwk	✘
publicKeyMultibase	✘
Το **service** πεδίο εμπεριέχει:	
id	✔
type	✔
serviceEndpoint	✔

Πίνακας 3: πεδία ενός εγγράφου DID

Στην πρώτη στήλη του πίνακα 3, αναγράφονται τα βασικά πεδία που μπορεί να λάβει ένα αποκεντρωμένο έγγραφο, καθώς και τα υποπεδία των «verificationMethod» και «service». Η δεύτερη στήλη αναφέρεται στην υποχρεωτικότητα τον πεδίων. Στα επόμενα κεφάλαια αναλύονται κάποια από τα βασικότερα πεδία.

Αναγνωριστικά 2.4.3.β

Ένα αποκεντρωμένο έγγραφο εμπεριέχει κάποια αναγνωριστικά. Τα αναγνωριστικά αυτά βοηθάνε στην διαλειτουργικότητα και παρέχουν μια μοναδικότητα ανάμεσα σε όλα τα έγγραφα. Η επίτευξη ενός τέτοιου προβλήματος, γίνεται με την βοήθεια τριών πεδίων. Τα πεδία αυτά είναι το «id», το «controller» και το «alsoKnownAs», εκ των οποίων το πρώτο είναι υποχρεωτικό. Πιο αναλυτικά:

- **ID**: Το πεδίο «id» έχει ως σκοπό να ορίσει τον κάτοχο του εγγράφου. Όπως είναι ήδη γνωστό, για να έχει κάποιος την κατοχή ενός εγγράφου, πρέπει να έχει το αντίστοιχο αποκεντρωμένο αναγνωριστικό. Συμπερασματικά, το πεδίο «id» του εγγράφου παίρνει την τιμή του εκάστοτε αναγνωριστικού. Ένα παράδειγμα είναι:

  { "id": "did:example:123456789abcdefghijk", …}

  Τέλος, το πεδίο «id» είναι το μόνο υποχρεωτικό ανάμεσα σε όλα τα αλλά πεδία ενός αποκεντρωμένου εγγράφου. Αυτό σημαίνει πως ένα έγγραφο μπορεί να αποτελείτε μόνο από το «id» και τίποτα άλλο.
- **Controller:** Το πεδίο αυτό ορίζει την οντότητα που μπορεί να τροποποιήσει το αναφερόμενο αποκεντρωμένο έγγραφο. Ο τρόπος με τον οποίο αποκτά άδεια η οντότητα αυτή, περιγράφεται από την μέθοδο του αποκεντρωμένου αναγνωριστικού (αποκεντρωμένο σύστημα). Όπως και στο προηγούμενο πεδίο, η τιμή του «controller» είναι ίδια με ενός αναγνωριστικού, παρόλα αυτά δεν είναι υποχρεωτική η παρουσία του.
- **Also Known As:** Η οντότητα στην οποία ανήκει το αποκεντρωμένο έγγραφο μπορεί να έχει παραπάνω από ένα αναγνωριστικά, κάτι τέτοιο μπορεί να συμβεί για διάφορους λόγους. Η αντιστοίχιση διαφορετικών αναγνωριστικών πέραν του βασικού «id» μπορεί να γίνει στο πεδίο «alsoKnownAs». Η τιμή που παίρνει το πεδίο αυτό είναι η τιμή ενός URI ή μιας λίστα από URIs.

Τρόποι επαλήθευσης 2.4.3.γ

Ένα αποκεντρωμένο έγγραφο μπορεί να εκφράσει διάφορους μεθόδους επαλήθευσης, όπως δημόσια κρυπτογραφικά κλειδιά, τα οποία μπορεί να χρησιμοποιηθούν για να αυθεντικοποίησουν ή να εξουσιοδοτήσουν κάποιες ενέργειες, οι οποίες σχετίζονται με την οντότητα του αποκεντρωμένου εγγράφου. Για παράδειγμα, μια μέθοδος αυθεντικοποίησης με την οποία ένα δημόσιο κρυπτογραφικό κλειδί μπορεί να χρησιμοποιηθεί είναι οι ψηφιακές υπογραφές. Οι ψηφιακές υπογραφές κάνουν εύκολη την αντιστοίχιση του δημοσίου και ιδιωτικού κλειδιού.

Το πεδίο όπου αποθηκεύονται τα κρυπτογραφικά κλειδιά είναι το «verificationMethod». Το πεδίο αυτό, δεν είναι υποχρεωτικό και έχει την μορφή μιας λίστας, όπου το κάθε στοιχείο αποτελείται από τα «id», «type», «controller», «publicKeyJwk» και «publicKeyMultibase». Πιο αναλυτικά:

- **ID**: Το πεδίο αυτό είναι υποχρεωτικό και παίρνει την τιμή ενός αποκεντρωμένου URL αναγνωριστικού. Για παράδειγμα, «did:example:123456789abcdefghi#key-1».

- **Type**: Το πεδίο αυτό είναι υποχρεωτικό και αναφέρεται σε μόνο μια μέθοδο επαλήθευσης, ούτως ώστε να βελτιώσει την διαλειτουργικότητα. Η τιμή του τύπου πρέπει να αναφέρεται στις προδιαγραφές των αποκεντρωμένων αναγνωριστικών.
- **Controller**: Το πεδίο «controller» είναι υποχρεωτικό και έχει την ίδια λειτουργία όπως και στα «βασικά αναγνωριστικά» του προηγούμενου κεφαλαίου.
- **Public Key JWK**: Είναι ένας τρόπος αναπαράστασης ενός κρυπτογραφικού κλειδιού σύμφωνα με το [RFC7517].
- **Public Key Multibase**: Είναι ένας τρόπος αναπαράστασης ενός κρυπτογραφικού κλειδιού.

Αυθεντικοποίηση 2.4.3.δ

Το πεδίο της αυθεντικοποίησης ενός αποκεντρωμένου εγγράφου «authentication», χρησιμοποιείτε για να ορίσει τον τρόπο με τον οποίο ένας κάτοχος θα μπορέσει να έχει πρόσβαση σε μια ιστοσελίδα ή σε κάποια άλλη πλατφόρμα. Το πεδίο είναι προαιρετικό και η τιμή που παίρνει βασίζεται στις τιμές του προηγούμενου κεφαλαίου «τρόποι επαλήθευσης». Εφόσον η αυθεντικοποίησης πάρει μέρος, εναπόκειται από το αποκεντρωμένο σύστημα είτε από κάποιον άλλο πάροχο να αποφασίσει τις περαιτέρω πράξεις.

Υπηρεσίες 2.4.3.ε

Οι υπηρεσίες είναι ένα βασικό πεδίο στα αποκεντρωμένα έγγραφα και χρησιμοποιούνται ως περαιτέρω μέσο επικοινωνίας μιας οντότητας με τον κάτοχο του εγγράφου (ή σχετικών οντοτήτων). Μια υπηρεσία μπορεί να είναι οτιδήποτε, για παράδειγμα κάποια πληροφορία ή κάποιος τρόπος αυθεντικοποίησης κ.α.

Λόγω της ελευθερίας που προσφέρουν οι υπηρεσίες στα αποκεντρωμένα έγγραφα και με βάση την ασφάλεια όλου του συστήματος της αποκεντρωμένης ταυτότητας, η αποκάλυψη προσωπικών στοιχείων, όπως διεύθυνσης αλληλογραφίας, λογαριασμούς κοινωνικών δικτύων και άλλα δεν συνιστώνται. Όλες οι πληροφορίες που βρίσκονται μέσα στις υπηρεσίες, πρέπει να αφορούν αποκλειστικά τις ίδιες τις υπηρεσίες.

Το πεδίο που χρησιμοποιεί κανείς στα αποκεντρωμένα έγγραφα για να δηλώσει μια υπηρεσία είναι το «service». Το πεδίο αυτό δεν είναι υποχρεωτικό. Ως τιμή του παίρνει μια λίστα, όπου το κάθε στοιχείο του αποτελείται από άλλα τρία πεδία, τα οποία είναι υποχρεωτικά. Τα τρία αυτά πεδία είναι το «id», «type» και το «serviceEndpoint». Πιο αναλυτικά:

- **ID**: Το πεδίο αυτό παίρνει την τιμή ενός αποκεντρωμένου αναγνωριστικού. Επίσης, δεν μπορούν να συνυπάρξουν δυο ίδια «ids» σε δυο διαφορετικές υπηρεσίες. Αν συμβεί κάτι τέτοιο το έγγραφο απορρίπτεται.
- **Type**: Το πεδίο αυτό αναφέρεται στον τύπο της υπηρεσίας και βοηθάει στην διαλειτουργικότητα της. Η τιμή που μπορεί να λάβει είναι είτε ενός αλφαριθμητικού, είτε μιας λίστας από αλφαριθμητικά. Τέλος, η τιμή ή οι τιμές που θα λάβει πρέπει να αναφέρονται στις προδιαγραφές των αποκεντρωμένων αναγνωριστικών.
- **Service Endpoint:** Η τιμή του «serviceEndpoint» πρέπει να είναι ένα έγκυρο URI ή μια λίστα από έγκυρα URIs. Τα URIs μπορούν να είναι οτιδήποτε, αρκεί να είναι συναφή με την υπηρεσία.

Επαληθεύσιμοι ισχυρισμοί 2.4.4

Μια ακόμη εμφάνιση των αποκεντρωμένων αναγνωριστικών (στο σύστημα ταυτότητας) βρίσκεται στα επαληθεύσιμα διαπιστευτήρια. Η διασύνδεση μεταξύ των δύο τεχνολογιών γίνεται

μέσω των αποκεντρωμένων εγγραφών. Πιο συγκεκριμένα, όλοι οι ισχυρισμοί που γίνονται μεταξύ διαφορετικών οντοτήτων, είναι μια πληροφορία. Η πληροφορία αυτή καταγράφεται στα αποκεντρωμένα έγγραφα, του εκάστοτε αναγνωριστικού. Συμπερασματικά τα πεδία ενός αποκεντρωμένου έγγραφου δεν είναι μόνο αυτά που αναφέρθηκαν νωρίτερα.

Ψηφιακό πορτοφόλι 2.5

Τι είναι το ψηφιακό πορτοφόλι 2.5.1

Εισαγωγή 2.5.1.α

Πέρα από τα χρήματα, ένα πορτοφόλι έχει την δυνατότητα να αποθηκεύει κάποια σημαντικά αναγνωριστικά για τον καθένα μας, κάποια από αυτά μπορεί να είναι η ταυτότητα, το δίπλωμα οδήγησης κ.α. Τα χρησιμοποιούμε σε καθημερινή βάση, αν όχι όλα μερικά από αυτά. Η μεγαλύτερη λειτουργία ενός πορτοφολιού είναι να μας κάνει πιο εύκολη την χρήση των περιεχομένων του (συμπεριλαμβανομένων των αναγνωριστικών) και να τα κρατάει ασφαλή, ούτως ώστε να μην κλαπούν.

Με την ίδια λογική, δουλεύει και ένα ψηφιακό πορτοφόλι ενός συστήματος ταυτότητας, μόνο που αντί για αναγνωριστικά, αποθηκεύει ψηφιακά διαπιστευτήρια, κάνοντας ακόμα πιο εύκολη και (κυρίως) ασφαλή την διαχείριση των αναγνωριστικών που βρίσκονται σε ένα φυσικό πορτοφόλι.

Από μια πιο τεχνική άποψη, ένα ψηφιακό πορτοφόλι είναι ένα διαχειριστικό περιβάλλον το οποίο παρέχεται στον χρήστη με κάποια γραφική διεπαφή, έτσι ώστε να μπορεί εύκολα να διαχειρίζεται κάποια κρυπτογραφικά κλειδιά.

Κάθε μέλος ενός συστήματος ταυτότητας (κάτοχος, εκδότης και επαληθευτής) θα πρέπει να έχει στην κατοχή του ένα ψηφιακό πορτοφόλι, διότι αυτό είναι που του δίνει την δυνατότητα να πάρει μέρος στο οικοσύστημα της αποκεντρωμένης αυτοδιαχειριζομενης ταυτότητας.

Βασικά χαρακτηριστικά 2.5.1.β

Όπως και το φυσικό πορτοφόλι, έτσι και σε ένα ψηφιακό αποθηκεύονται ευαίσθητες πληροφορίες. Στην περίπτωση των ψηφιακών πορτοφολιών αυτή η πληροφορία μπορεί να είναι κάποιο κλειδί ή κάποιο ψηφιακό διαπιστευτήριο. Τα βασικότερα χαρακτηριστικά που κάθε πορτοφόλι ενός συστήματος ταυτότητας θα πρέπει να πληροί, είναι τα εξής [11]:

1. **Εύκολα προσβάσιμο:** Χωρίς καθόλου κόπο μια οντότητα (η οποία θα έχει πρόσβαση στο πορτοφόλι) θα έχει τον έλεγχο όλων των δεδομένων.
2. **Ασφαλές:** Πρέπει να είναι κρυπτογραφικά ασφαλές, διότι υπάρχει μεγάλη ποσότητα ευαίσθητης πληροφορίας αποθηκευμένη. Κάνεις δεν θα πρέπει να έχει πρόσβασή σε αυτό πέρα από τον κάτοχο του και η πληροφορία θα πρέπει να είναι αποθηκευμένη τοπικά, όπως σε ένα φυσικό πορτοφόλι.
3. **Ιδιωτικό:** Η οντότητα που έχει πρόσβαση στο πορτοφόλι, έχει τον πλήρη έλεγχο να διαλέγει ποια πληροφορία θα αποκαλύπτει και σε ποιον. Για παράδειγμα, έστω ότι είμαστε σε ένα μπαρ στο οποίο ζητάνε την ηλικία για να εισέλθει κάποιος στον χώρο. Την πληροφορία αυτή την ελέγχει η οντότητα και αυτή αποφασίζει αν θα την στείλει, σε ποιόν θα την στείλει και ποιο μέρος από αυτήν θα διαλέξει να εμφανίσει.

Βασικές λειτουργίες ενός πορτοφολιού 2.5.2

Ένα ψηφιακό πορτοφόλι βασισμένο σε ένα σύστημα αυτοδιαχειριζόμενης ταυτότητας 2.5.2.α

Όλα τα πορτοφόλια είναι διαφορετικά. Ένα ψηφιακό πορτοφόλι είναι ένα σύστημα το οποίο μπορεί να υλοποιηθεί με πολλούς τρόπους. Οι δύο από τις βασικότερες τεχνολογίες που πρέπει να ακολουθεί το σύστημα ταυτότητας είναι τα αποκεντρωμένα αναγνωριστικά και τα ψηφιακά διαπιστευτήρια. Έχοντας αυτά υπόψιν, αν δεν δοθούν κάποιες οδηγίες για το πως να χρησιμοποιηθούν (οι παραπάνω δυο τεχνολογίες) η υλοποίηση του ψηφιακού πορτοφολιού μπορεί να διαφέρει, ανάλογα με το σύστημα ταυτότητας που θέλει να υποστηρίξει. Ένα παράδειγμα μπορεί να είναι κάποιο ανταλλακτήριο κρυπτονομίσματων. Τα περισσότερα ανταλλακτήρια χρησιμοποιούν αντιπροσωπευτικά πορτοφόλια (Αγγλ. hosted wallets), τα οποία δεν τα ελέγχει άμεσα ο κάτοχος, αλλά η ίδια η υπηρεσία. Έτσι, εάν κάποιος κάτοχος κάνει μια συναλλαγή μέσο της υπηρεσίας τους, τα χρήματα δεν πάνε κατευθείαν στο πορτοφόλι του, αλλά μένουν στο πορτοφόλι της υπηρεσίας.

Σε αντίθεση με το πορτοφόλι του συστήματος ταυτότητας, όλα τα στοιχεία βρίσκονται αποθηκευμένα πάνω στην συσκευή. Όλο αυτό παραπέμπει στην τρίτη ιδιότητα που αναφέρθηκε πιο πάνω.

Ιδιότητες και λειτουργίες 2.5.2.β

Αυτές είναι οι επιθυμητές λειτουργίες τις οποίες ένα αποκεντρωμένο σύστημα αυτοδιαχειριζόμενης ταυτότητας πρέπει να έχει [12]:

Σχήμα 21: κανάλια επικοινωνίας

Δημιουργία καναλιών και σχέσεων με τρίτους: Το πορτοφόλι έχει την δυνατότητα να δημιουργεί κρυπτογραφημένα κανάλια επικοινωνίας, ούτως ώστε τα μέλη στις δυο άκρες της επικοινωνίας, να ανταλλάσσουν με ασφαλή τρόπο πληροφορίες μεταξύ τους. Τα κανάλια αυτά βασίζονται στα αποκεντρωμένα αναγνωριστικά, τα οποία ανήκουν μόνο στα μέλη της επικοινωνίας. Συμπερασματικά τα αναγνωριστικά αυτά δεν είναι σε κάποιο κεντρικοποιημένο σύστημα. Τα κανάλια αυτά προσφέρουν ένα είδους φορητότητας, το οποίο σημαίνει πως αν αλλάξει μια οντότητα το πορτοφόλι του, μπορεί να συνεχίσει να έχει πρόσβαση στο κανάλι, (εφόσον κατέχει το κατάλληλο αναγνωριστικό) χωρίς να βασίζεται σε κάποιον τρίτο.

Αποθήκευση και οργάνωση των δεδομένων: Η οντότητα έχει τον έλεγχο να αποθηκεύει και να οργανώνει όπως θέλει τα δεδομένα που εμπεριέχονται μέσα στο πορτοφόλι (ψηφιακά διαπιστευτήρια κ.α.) της. Μόλις τα δεδομένα εισέλθουν στο πορτοφόλι, μπορούν να χρησιμοποιηθούν άμεσα για να επιβεβαιώσουν τυχόν αιτήματα. Το πορτοφόλι δημιουργεί μια ψηφιακή πρόσοψη για το κάθε αίτημα, την οποία η οντότητα αποφασίζει αν την στείλει ή όχι σε κάποιον τρίτο. Επίσης, τα μέλη της συναλλαγής θα πρέπει να είναι αναγνωρίσιμα μεταξύ τους, ούτως ώστε να μπορούν να στείλουν τις προσόψεις μεταξύ τους.

Τα στοιχεία που μοιράζεται ο κάτοχος, είτε θα είναι επιβεβαιωμένα από κάποιον άλλο, είτε από τον ίδιο, είτε μπορεί να είναι κάποιου ίδιους τιμή (π.χ. ναι ή όχι), για να μην αποκαλύψει περεταίρω πληροφορία. Ένα παράδειγμα θα μπορούσε να είναι αν κάποιος είναι ενήλικας. Για να είναι κάποιος ενήλικας πρέπει η ηλικία του να υπερβαίνει τα 18, αντί να αποκαλύψει κάποιος την ηλικία του μπορεί να απαντήσει στην ερώτηση αν είναι άνω τον 18 με ένα ναι ή με ένα όχι.

Μια καθαρή εικόνα με το ιστορικό των διαμοιρασμένων πιστοποιητικών: Εφόσον ένα πορτοφόλι μπορεί να κρατήσει το ιστορικό όλων των αλληλεπιδράσεων, ένας κάτοχος πρέπει να έχει την δυνατότητα να βλέπει ποιος έχει πρόσβαση σε τι. Αυτό βοηθάει στην διαφάνεια, την οργάνωση και την ασφάλεια του υποκειμένου.

Προφυλάξεις 2.5.2.γ

Ένα πορτοφόλι μπορεί να κλαπεί. Για να μην υπάρξει κάποια σοβαρή επίπτωση στα δεδομένα (εφόσον είναι αποθηκευμένα τοπικά στην συσκευή μας), πρέπει να είναι όλα κρυπτογραφημένα. Ο τρόπος με τον οποίο μπορεί να γίνει αυτό, είναι με κάποιο κωδικό πρόσβασης, είτε με οποιοδήποτε βιομετρικό μέσο *(το βήμα αυτό είναι προαιρετικό)*.

Περίπτωση κλοπής ή απώλειας του ψηφιακού πορτοφολιού 2.5.3

Αρχικά, ένα ψηφιακό πορτοφόλι συνήθως είναι το κινητό μας τηλέφωνο, οπότε όλα τα ψηφιακά διαπιστευτήρια, δημόσια και ιδιωτικά κλειδιά βρίσκονται αποθηκευμένα σε αυτό. Σε αντίθεση με ένα κεντρικοποιημένο σύστημα στο οποίο υπάρχει κάποιου είδους υπηρεσίας ανάκτησης στοιχείων, τα πράγματα στο σύστημα ταυτότητάς είναι διαφορετικά. Η δυσκολία βρίσκεται στην τοπικότητα των αρχείων, δηλαδή, τα αρχεία αυτά δεν είναι αποθηκευμένα πουθενά, αλλά μόνο στο ένα σημείο που ο κάτοχος μπορεί να ελέγξει (το κινητό του τηλέφωνο).

Είναι γνωστό πως στην περίπτωση κλοπής του πορτοφολιού, υπάρχουν κάποιες προφυλάξεις που μπορεί να πάρει κάνεις *(αναφ. 2.5.2.γ).* Πολύ συχνά όμως, αυτές οι προφυλάξεις δεν τηρούνται. Στην περίπτωση που το πορτοφόλι δεν είναι στην κατοχή του υποκειμένου και τα δεδομένα μέσα του είναι ελεύθερα και ανοιχτά, τότε πρέπει να δράσει γρήγορα, ούτως ώστε να μην επιδεινωθεί η τρέχοντα κατάσταση.

Για την αντιμετώπιση της παραπάνω κατάστασης έχουν μελετηθεί αρκετές λύσεις, παρόλα αυτά δεν υπάρχει κάποιο συγκεκριμένο πρότυπο το οποίο ακολουθεί το σύστημα ταυτότητας. Μερικές από τις προτάσεις είναι:

Ανάκληση κλειδιών και πιστοποιητικών: Η πρώτη πιθανή λύση είναι να ανακαλεστούν όλα τα κλειδιά, πιστοποιητικά και κανάλια τα οποία έχουν ήδη δημιουργηθεί με το ιδιωτικό κλειδί του υποκειμένου. Η πράξη αυτή περιθωριοποιεί αρκετά τις περεταίρω επιλογές του κλέφτη. Η ανάκληση μπορεί να γίνει εφόσον ο κάτοχος έχει πρόσβαση σε ένα άλλο πορτοφόλι το οποίο έχει εξουσιοδοτήσει. Έχοντας πρόσβαση στο πορτοφόλι και έχοντας ένα μυστικό κωδικό που έχει προκαθοριστεί, στέλνει και ενημερώνει το δημόσιο αποκεντρωμένο σύστημα ότι ανακαλεί όλα του τα δεδομένα (κλειδιά και διαπιστευτήρια). Η διαδικασία αυτή πρέπει να είναι άμεση χωρίς περιθώριο καθυστέρησης.

Πολλαπλά κλειδιά: Ένας ακόμα τρόπος για να ξεπεράσει κάποιος αυτό το πρόβλημα είναι με την χρήση πολλαπλών κλειδιών. Αυτό δουλεύει με την δημιουργία ενός δεύτερου κλειδιού, το οποίο συνιστάτε να είναι σε ένα ασφαλές σημείο (σπίτι, χρηματοφυλάκιο κ.α.). Το δεύτερο αυτό κλειδί δίνει την δυνατότητα στον κάτοχο να μεταφέρει το πορτοφόλι σε οποιαδήποτε άλλη συσκευή που εμπιστεύεται.

Εμπιστοσύνη στους πλησίον: Ο κάτοχος αναθέτει σε κάποιους γνωστούς προς αυτόν ή κοντινούς του ανθρώπους, την δυνατότητα να μεταφέρουν το πορτοφόλι του εφόσον η πλειοψηφία αυτών αναφέρει πως το κλειδί του χάθηκε. Μετά από αυτή την αναφορά, ανοίγει μια μικρή χρονική σχισμή στην οποία μπορεί να αλλάξει το ιδιωτικό του κλειδί.

Όλες οι τεχνικές που αναφέρθηκαν θα πρέπει να έχουν προκαθοριστεί προτού μπορέσει κάνεις να τις χρησιμοποιήσει. Αν δεν δημιουργηθούν τότε συμπερασματικά, δεν θα υπάρχει κάποιος τρόπος ανάκτησης ή ανάκλησης του πορτοφολιού, κάτι που μπορεί να βλάψει κάποιον αρκετά.

ΚΕΦΑΛΑΙΟ 3: Το μοντέλο ToIP

Μοντέλο αποκεντρωμένης ταυτότητας 3.1

Εισαγωγή 3.1.1

Η ιδέα ενός αποκεντρωμένου μοντέλου ταυτότητας ήταν εμπνευσμένη από το OSI (open systems interconnection) μοντέλο, το οποίο χρησιμοποιείτε μέχρι και σήμερα. Το μοντέλο αυτό θέτει κάποιες προδιαγραφές τις οποίες πρέπει κάθε τηλεπικοινωνιακό σύστημα να ακολουθεί. Με λίγα λόγια, η λογική πίσω από το μοντέλο OSI είναι να καθοδηγεί τους κατασκευαστές και προγραμματιστές διάφορων τηλεπικοινωνιακών συστημάτων, να κρατούν μια διαλειτουργικότητα μεταξύ των προϊόντων τους.

Με την λογική του OSI, στα μέσα του 2016 δημιουργήθηκε ένα νέο μη κερδοσκοπικό ερευνητικό σχέδιο με το όνομα «Trust over IP foundation», το οποίο χορηγήθηκε από το «Linux foundation». Το νέο αυτό ερευνητικό σχέδιο, είχε σκοπό να εγκαθιδρύσει ένα μοντέλο αποκεντρωμένης ταυτότητας, το οποίο και έκανε στις αρχές του Μάιου μήνα, με το όνομα «Trust over IP stack», το οποίο το χρησιμοποιούν και άλλες μη κερδοσκοπικές οργανώσεις όπως η «Sovrin».

Μοντέλο Trust over IP (ToIP) 3.1.2

Δομή 3.1.2.α

Το μοντέλο που πρότεινε το «Trust over IP foundation» έχει τέσσερα επίπεδα. Το κάθε επίπεδο έχει από ένα τεχνικό και ένα κυβερνητικό μέρος. Ο σκοπός των κυβερνητικών επιπέδων είναι ίδια με τον σκοπό του OSI μοντέλου. Ουσιαστικά, προσεγγίζουν πιο αυθαίρετα το μοντέλο «ToIP». Η πρώτη προσέγγιση του «ToIP foundation» ξεκίνησε δίνοντας μεγαλύτερη βαρύτητα στο τεχνικό μέρος της αποκεντρωμένης ταυτότητας παρά στο κυβερνητικό, παρόλα αυτά, ύστερα από αρκετές αναλύσεις και επαναλήψεις κατέληγαν να αλλάξουν την ιδία του μοντέλου ταυτότητας και να δώσουν μεγαλύτερη βάση στο κυβερνητικό.

Όσο πιο ψηλά ανεβαίνει κάνεις στα επίπεδα του μοντέλου «ToIP», τόσο περισσότερο διακρίνει πως τα διαφορετικά κυβερνητικά επίπεδα απευθύνονται σε διαφορετικές ανάγκες. Οι ανάγκες των τεσσάρων διαφορετικών κυβερνητικών επιπέδων που προτάχθηκαν από το μοντέλο είναι:

1. **Utility Governance Framework**: Στο πρώτο επίπεδο ορίζεται τι είδους εμπιστοσύνη χρειάζεται μια κοινωνία. Για παράδειγμα, ο δημόσιος ledger του «Sovrin» ή οποιοδήποτε άλλο είδος «verifiable data registry».
2. **Provider Governance Framework**: Στο δεύτερο επίπεδο ορίζονται οι απαιτήσεις (που έχει η κοινωνίας) για την διαλειτουργικότητα των ψηφιακών πορτοφολιών και ψηφιακών πρακτόρων. Μέσα σε όλα αυτά μπορεί να είναι και η επικοινωνία μεταξύ πορτοφολιών.
3. **Credential Governance Framework**: Στο τρίτο επίπεδο ορίζονται οι οντότητες που παίρνουν μέρος στο σύστημα, οι ρόλοι που έχουν και οι μεταξύ τους λειτουργίες.
4. **Ecosystem Governance Framework**: Στο τέταρτο επίπεδο ορίζεται ο τρόπος με τον οποίο διαφορετικά συστήματα αυτοδιαχειριζόμενης ταυτότητας επικοινωνούν με άλλα, έτσι ώστε να πληρούν τις προϋποθέσεις ολόκληρου του συστήματος ταυτότητας.

Σχήμα 22: τα 4 επίπεδα του μοντέλου ταυτότητας. Πηγή: https://trustoverip.org/toip-model/

Ρόλος 3.1.2.β

Ο ρόλος του «ToIP foundation», δεν είναι να ορίσει καινούργιες τεχνολογίες άλλα κάποιες προδιαγραφές, είτε μοντέλα ή σωστές πρακτικές που πρέπει παγκοσμίως όλοι να ακολουθούν, έτσι ώστε η ψηφιακή εμπιστοσύνη να πάρει μέρος.

Εφόσον οι προδιαγραφές αυτές έχουν οριστεί, από εκεί και πέρα όλο το βάρος βρίσκεται στο εκάστοτε μέλος του συστήματος ταυτότητας, έτσι ώστε να ακολουθήσει τις οδηγίες του μοντέλου. Αυτό σημαίνει [13]:

- Οι **κυβερνητικές αρχές** οι οποίες εκπροσωπούν κάποια κοινωνία οποιουδήποτε μεγέθους, θα πρέπει να χρησιμοποιούν τα πρότυπα και τις προδιαγραφές που έχουν οριστεί στα τέσσερα επίπεδα του «ToIP».
- Οι **προγραμματιστές και οι κατασκευαστές** πρέπει να εξετάζουν, να κατασκευάζουν και να αναπτύσσουν το εκάστοτε προϊόν, με βάση το μοντέλο «ToIP» (σε οποιοδήποτε επίπεδο και αν είναι).
- **Ερευνητικές ομάδες, αρχές πιστοποίησης και οργανισμοί,** πρέπει να προσφέρουν μια διαλειτουργικότητα των πιστοποιητικών με το μοντέλο «ToIP» και στον έλεγχο και στην εξέταση των εκάστοτε προϊόντων.

Μια αναλογία σχετικά με το «ToIP foundation» είναι η Εθνική Καλαθοσφαιρική Ομοσπονδία (ΕΚΟ). Η «ΕΚΟ» ορίζει όλους τους κανόνες μπάσκετ, με τους οποίους όλοι συμφωνούν και ακολουθούν, παρόλα αυτά δεν ορίζει ποιες θα είναι οι ομάδες. Τα κυβερνητικά επίπεδα είναι οι «ομάδες» που ορίζουν τα δικά τους κυβερνητικά πρότυπα (κανόνες) για τα μέλη μιας κοινωνίας (παίχτες).

Δημόσιες υπηρεσίες 3.2

Εισαγωγή 3.2.1

Τα πρώτα δυο επίπεδα του μοντέλου ταυτότητας τείνουν να είναι πιο τεχνικά από ότι τα υπόλοιπα. Η ιδέα πίσω από αυτά, είναι η διασφάλιση μιας ασφαλής και ιδιωτικής επικοινωνίας μεταξύ διαφορετικών οντοτήτων (μηχανών). Για να εφαρμοστεί κάτι τέτοιο με την χρήση της κρυπτογραφίας δημοσίου κλειδιού, θα πρέπει μια από της δυο οντότητες (που εμπλέκονται στην επικοινωνία) να επαληθεύσει την εγκυρότητα του ιδιωτικού κλειδιού της άλλης. Όλα αυτά θα πρέπει να πάρουν μέρος σε κάποια μη κεντρικοποιημένη πιστοποιημένη αρχή (Αγγλ. decentralized certificate authority). Ένα πρότυπο έχει θέσει η W3C, η οποία χρησιμοποίησε την τεχνολογία του Blockchain (ή και κάποιο άλλου είδους αποκεντρωμένου καθολικού), ούτως ώστε να αναγνωρίσει και να επαληθεύσει την προέλευση του ιδιωτικού κλειδιού μιας οντότητας.

Το πρότυπο της W3C βάζει σε λειτουργία τα αποκεντρωμένα αναγνωριστικά, την δημόσια κρυπτογραφία και τα επαληθεύσιμα διαπιστευτήρια, δίνοντας τους μια βασική θέση στην υλοποίηση του πρώτου επιπέδου. Παρόλα αυτά, το σύστημα στο οποίο θα γίνει η αλληλεπίδραση μεταξύ των οντοτήτων, μπορεί να διαφέρει, εφόσον θα πληροί τις κατάλληλες προϋποθέσεις εμπιστοσύνης. Κάποια παραδείγματα είναι, κάποιο Blockchain, κάποιου άλλου είδους αποκεντρωμένου

αναγνωριστικού, κάποιο αποκεντρωμένο σύστημα αρχείων (Αγγλ. decentralized file system) και άλλα.

Από την αντίθετη μεριά όλων αυτών, η κυβερνητική αρχή αυτού του επιπέδου, είναι ο πυλώνας όλου του μοντέλου ταυτότητας, διότι παρέχει την πολιτική με την οποία εφαρμόζεται το σύστημα, ούτως ώστε να διασφαλίσει την εμπιστοσύνη στα μετέπειτα επίπεδα.

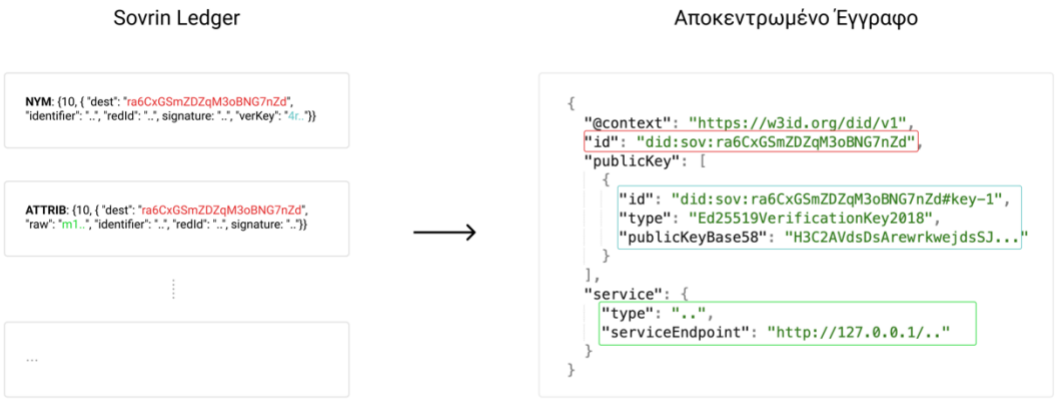
Αποθήκευση ενός εγγράφου σε κάποιο Blockchain 3.2.2

Όπως είναι γνωστό το επίπεδο αυτό είναι υπεύθυνο για την πιστοποίηση του ιδιωτικού κλειδιού μιας οντότητας, μέσω κάποιου αποκεντρωμένου συστήματος. Για να λειτουργήσει σωστά αυτή η διαδικασία, τα ιδιωτικά κλειδιά θα πρέπει να είναι αποθηκευμένα σε ένα σύστημα, ούτως ώστε η οντότητα του επαληθευτή να μπορέσει να πιστοποίηση την αυθεντικότητα του κλειδιού της δεύτερης οντότητας.

Στην αποκεντρωμένη ταυτότητα το σύστημα που χρησιμοποιείται είναι το Blockchain. Η μέθοδος με την οποία τα κλειδιά των οντοτήτων είναι αποθηκευμένα στο Blockchain, είναι μέσω των αποκεντρωμένων αναγνωριστικών και αποκεντρωμένων εγγράφων. Τα αποκεντρωμένα αναγνωριστικά, όπως έχει προαναφερθεί, ορίζουν την μέθοδο με την οποία θα εξάγουν το αποκεντρωμένο έγγραφο από το εκάστοτε σύστημα, στην περίπτωση της αποκεντρωμένης ταυτότητας το σύστημα είναι το Blockchain, ωστόσο, το Blockchain δεν αποθηκεύει άμεσα το αποκεντρωμένο έγγραφο αλλά έμμεσα. Μερικά παραδείγματα συστημάτων αποθηκεύσεις αποκεντρωμένων εγγράφων, που χρησιμοποιούνται από τα συστήματα ταυτότητας σήμερα, αναλύονται παρακάτω.

Sovrin 3.2.2.α

Το καθολικό του Sovrin είναι συμβατό με τα αποκεντρωμένα αναγνωριστικά και όχι με τα αποκεντρωμένα έγγραφα ακόμα. Η μέθοδος με την οποία το καθολικό του Sovrin χτίζει το έγγραφο παρουσιάζεται στο σχήμα 22.



Σχήμα 23: ένα αποκεντρωμένο έγγραφο στο καθολικό Sovrin. Πηγή: https://ssimeetup.org/did-resolution-given-did-how-do-retrieve-document-markus-sabadello-webinar-13/

Για να μπορέσει κάνεις να ανακαλέσει το παραπάνω έγγραφο από το καθολικό του Sovrin θα πρέπει να έχει στην κατοχή του το αποκεντρωμένο αναγνωριστικό, στην περίπτωση αυτή το

αναγνωριστικό είναι το «did:sov:ra6CxGSmZDZqM3oBNG7nZd», όπως φαίνεται και στο πεδίο «id» του αποκεντρωμένου εγγράφου. Εφόσον το αναγνωριστικό είναι γνωστό μπορεί πλέον η οντότητα να εντοπίσει και να χτίσει το αποκεντρωμένο έγγραφο μέσα από το καθολικό.

Για να χτιστεί το αποκεντρωμένο έγγραφο θα πρέπει αρχικά να βρεθούν όλες οι εγγραφές στο Blockchain. Εφόσον οι εγγραφές έχουν βρεθεί τα βήματα είναι τα εξής:

1. Στο πρώτο βήμα, θέτει το «id» με την τιμή του αποκεντρωμένου αναγνωριστικού. Για παράδειγμα «did:sov:ra6CxGSmZDZqM3oBNG7nZd».
2. Στο δεύτερο βήμα, κοιτάει την πρώτη συναλλαγή η οποία ονομάζεται **NYM**, όπου υπάρχουν στοιχεία όπως, τα δημόσια κλειδιά του αποκεντρωμένου έγγραφου. Στην φωτογραφία είναι το «publicKey».
3. Στο τρίτο βήμα, κοιτάει την δεύτερη συναλλαγή η οποία ονομάζεται **ATTRIB** η οποία προσθέτει οποιαδήποτε επιπλέον πληροφορία πάνω στο έγγραφο, μέσο του «raw» πεδίου της συναλλαγής. Η πληροφορία αυτή μπορεί να είναι κάποιο ή κάποια «service» και άλλα.

Bitcoin 3.2.2.β

Σε αντίθεση με το καθολικό του Sovrin, το Blockchain του Bitcoin δεν είναι συμβατό με τα αποκεντρωμένα έγγραφα, αλλά ούτε και με τα αποκεντρωμένα αναγνωριστικά. Η μέθοδος με την οποία το Blockchain του Bitcoin χτίζει το έγγραφο παρουσιάζεται στο σχήμα 23.

Σχήμα 24: ένα αποκεντρωμένο έγγραφο στο καθολικό Bitcoin. Πηγή: https://ssimeetup.org/did-resolution-given-did-how-do-retrieve-document-markus-sabadello-webinar-13/

Η μέθοδος είναι σχεδόν ίδια με την προηγούμενη μόνο που τώρα υπάρχει μόνο μια συναλλαγή. Για να μπορέσει κάνεις να ανακαλέσει το παραπάνω έγγραφο από το Blockchain του Bitcoin θα πρέπει να έχει στην κατοχή του το αποκεντρωμένο αναγνωριστικό. Στην περίπτωση αυτή το αναγνωριστικό είναι το «did:btcr:le3n-w3pd-1klh-78sg» και μέσω αυτού μπορεί μια οντότητα να εντοπίσει το νούμερο της συναλλαγής πάνω στο Blockchain. Το αλφαριθμητικό του αναγνωριστικού (δηλ. le3n-w3pd-1klh-78sg) είναι ένας δείκτης σε κάποια συναλλαγή σε ένα μπλοκ του Blockchain.

Για να χτιστεί το αποκεντρωμένο έγγραφο θα πρέπει αρχικά να βρεθεί η συναλλαγή στο Blockchain μέσω του αλφαριθμητικού. Εφόσον οι εγγραφές έχουν βρεθεί τα βήματα είναι τα εξής:

1. Στο πρώτο βήμα, θέτει το «id» με την τιμή του αποκεντρωμένου αναγνωριστικού. Για παράδειγμα «did:btcr:le3n-w3pd-1klh-78sg».
2. Στο δεύτερο βήμα, βρίσκει την συναλλαγή «TXIN» και μέσω αυτής βγάζει το δημόσιο κλειδί. Στο σχήμα 23 είναι το «publicKey».
3. Στο τρίτο βήμα, βρίσκει όλες τις «TXOUT». Οι συναλλαγές αυτές είναι δυο και έχουν ως τύπο το «P2PKH» και «OP_RETURN». Από τις δυο αυτές συναλλαγές, αυτή που έχει περισσότερη σημασία είναι η «OP_RETURN». Όπως φαίνεται, η συναλλαγή αυτή έχει ένα «URL» ως τιμή, η οποία προσφέρει οποιαδήποτε επιπλέον πληροφορία σχετικά με το αποκεντρωμένο έγγραφο. Μια καλύτερη αναπαράσταση υπάρχει στην φωτογραφία επάνω.

Επικοινωνία αποκεντρωμένων αναγνωριστικών 3.3

Εισαγωγή 3.3.1

Εάν το πρώτο επίπεδο είχε να κάνει με τις κρυπτογραφικές ρίζες της αποκεντρωμένης ταυτότητας, τότε το δεύτερο επίπεδο είναι τα κλαδιά της. Το δεύτερο επίπεδο αναφέρεται περισσότερο στα ψηφιακά πορτοφόλια και τους ψηφιακούς πράκτορες. Σκοπός τους είναι, ο σχηματισμός ασφαλών και ιδιωτικών καναλιών επικοινωνίας, χρησιμοποιώντας είτε δημόσια αποκεντρωμένα αναγνωριστικά (πρώτο επίπεδο) είτε ιδιωτικά. Στα ιδιωτικά αποκεντρωμένα αναγνωριστικά, η επικοινωνία μεταξύ πορτοφολιών (οντοτήτων) γίνεται απευθείας, χωρίς καμία παρέμβαση από κάποιο σύστημα (Blockchain).

Όπως οι διευθύνσεις IP κρατάνε το TCP/IP μοντέλο, έτσι και το πρωτόκολλο DIDcomm (το οποίο έχει αναλάβει η DIF «Decentralized Identity Foundation»), κρατάει το «ToIP» μοντέλο.

Παρόλου που, η επικοινωνία γίνεται απευθείας μεταξύ μηχανών (οντοτήτων), ο τρόπος με τον οποίο το ψηφιακό πορτοφόλι και ο ψηφιακός πράκτορας εφαρμόζονται έχει ύψιστη σημασία για την ασφάλεια αλλά και ιδιωτικότητα των μεμονωμένων οντοτήτων.

Εδώ είναι που έρχεται το κυβερνητικό επίπεδο. Σκοπός του είναι να θέσει κάποιες προδιαγραφές τις οποίες πρέπει να πληροί ένα ψηφιακό πορτοφόλι, καθώς και ένας ψηφιακός πράκτορα. Οι προδιαγραφές αυτές μπορεί να είναι, η ιδιωτικότητα, η ασφάλεια και η διαφύλαξη των προσωπικών δεδομένων. Τέλος, στο κυβερνητικό επίπεδο δεν ορίζεται η εφαρμογή του ίδιου του πορτοφόλι, άλλα μόνο κάποιοι κανόνες τους οποίους κάθε κατασκευαστής ή πάροχος λογισμικού πρέπει να ακολουθήσει.

Ιδιωτικά αποκεντρωμένα αναγνωριστικά 3.3.2

Οφέλη των ιδιωτικών αποκεντρωμένων αναγνωριστικών 3.3.2.α

Η ιδέα των αποκεντρωμένων αναγνωριστικών είναι βαθιά ριζωμένη στην αποκεντρωμένη ταυτότητα. Με την χρήση μόνο τον δημοσιών αναγνωριστικών, οποιαδήποτε κίνηση και αν επιχειρούσε κάνεις, για παράδειγμα να ελέγξει έναν ισχυρισμό μιας άλλης οντότητας, θα έπρεπε να αναζήτηση ολόκληρο το αποκεντρωμένο σύστημα, ούτως ώστε να διαβεβαιωθεί για τον ισχυρισμό της. Κάτι τέτοιο θα επέφερε τεράστιο φορτίο στο αποκεντρωμένο σύστημα, χωρίς λόγο. Αυτός ήταν ένας από τους λόγους που εμφανίστηκαν τα ιδιωτικά αποκεντρωμένα αναγνωριστικά.

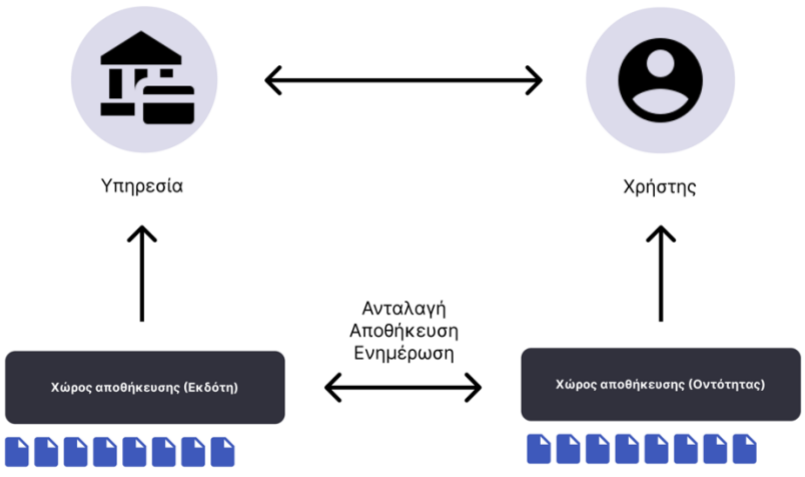
Κάποια ακόμα προτερήματα τα οποία προσφέρουν τα ιδιωτικά αναγνωριστικά, αναγράφονται παρακάτω.

- **Μέγεθος (Αγγλ. Scale)**: Το μεγαλύτερο ποσοστό ανταλλαγής των αναγνωριστικών, γίνεται μέσο των ιδιωτικών αναγνωριστικών.
- **Κόστος (Αγγλ. Cost)**: Το κόστος συναλλαγής τους (μεταξύ δύο οντοτήτων), είναι αμελητέο.
- **Ασφάλεια (Αγγλ. Security)**: Τα δεδομένα είναι αποθηκευμένα στη συσκευή της οντότητας και όχι σε κάποιο δημόσιο μέρος.
- **Ιδιωτικότητα (Αγγλ. Scale)**: Μόνο οι δύο εμπλεκόμενες οντότητες γνωρίζουν για τα αναγνωριστικά αυτά.
- **Απόδοση (Αγγλ. Scale):** Η απόδοση βελτιώνεται δραματικά.
- **Κανονισμός (Αγγλ. Regulation)**: Πλέον δεν υπάρχει κάποιο σύστημα το οποίο να χρειάζεται κανονισμούς, διότι όλα τα στοιχεία τα ελέγχει ο κάτοχος. (GDPR)

Τρόπος Λειτουργίας 3.3.2.β

Η εφαρμογή των δημοσίων αποκεντρωμένων αναγνωριστικών γίνεται με την βοήθεια του αποκεντρωμένου συστήματος (Blockchain), σε αντίθεση με τα ιδιωτικά τα οποία δεν έχουν ανάγκη από κάποιο αποκεντρωμένο μέσο.

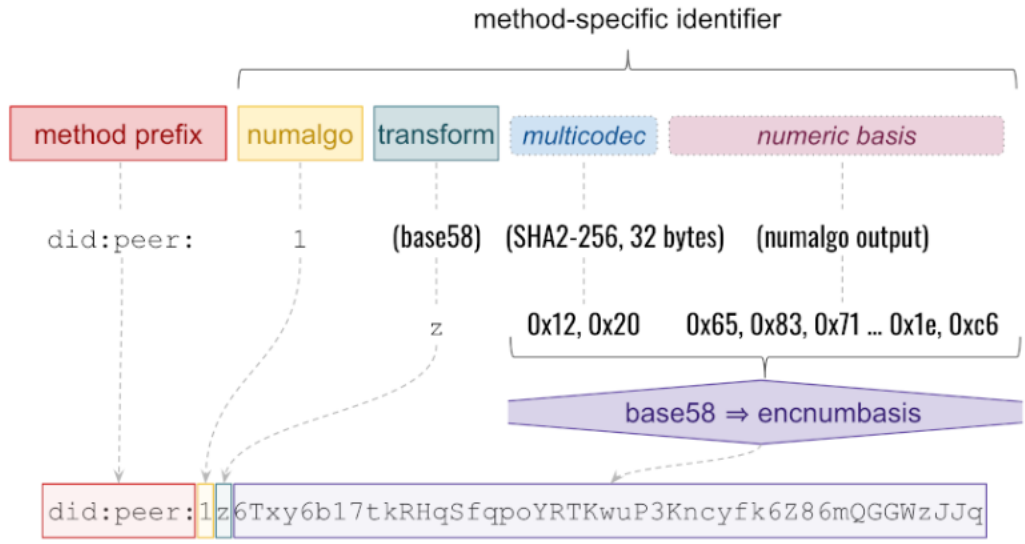
Ο τρόπος με τον οποίο δουλεύουν τα ιδιωτικά αποκεντρωμένα αναγνωριστικά είναι αρκετά απλός. Εμπλέκει δυο οντότητες, όπου η μια οντότητα, δημιουργεί ένα «ιδιωτικό» αποκεντρωμένο αναγνωριστικό (επόμενο κεφάλαιο), το βάζει μέσα σε ένα αποκεντρωμένο έγγραφο και το στέλνει στην δεύτερη. Στην συνέχεια η δεύτερη οντότητα κάνει ακριβώς τα ίδια βήματα, μόνο που το τελικό έγγραφο που έχει δημιουργήσει το στέλνει στην πρώτη οντότητα. Με αυτό τον τρόπο και οι δύο οντότητες έχουν από ένα έγγραφο του άλλου. Σε αυτό το έγγραφο αποθηκεύεται όλα τα μεταδεδομένα του καθενός. Στο σχήμα 18 υπάρχει μια αναπαράσταση τον προηγουμένων, όπου οι δυο οντότητες είναι ένας χρήστης και μια υπηρεσία.



Σχήμα 25: τρόπος λειτουργίας ιδιωτικών DID

Σχήμα 3.3.2.γ

Ένα ιδιωτικό αποκεντρωμένο αναγνωριστικό σύμφωνα με το πρότυπο της W3C [14] έχει την ίδια μορφή με ενός δημοσίου, παρόλα αυτά εμφανίζει κάποιες διαφορές στον τρόπο ερμηνείας του.



Σχήμα 26: δομή ιδιωτικού DID. Πηγή: https://identity.foundation/peer-did-method-spec

Όπως φαίνεται στο σχήμα 25, τα ιδιωτικά αποκεντρωμένα αναγνωριστικά μπορούν να χωριστούν σε τέσσερα διαφορετικά κομμάτια. Τα κομμάτια αυτά είναι, το πρόθεμα, η μέθοδο, η κωδικοποίηση και το αναγνωριστικό. Πιο αναλυτικά:

- **Πρόθεμα (Αγγλ. Method Prefix)**: Το πρόθεμα, ως γνωστόν βρίσκεται στην αρχή και κάνει δυνατή στην ερμηνεία του τύπο του αναγνωριστικού (π.χ. ιδιωτικό ή δημόσιο). Η τιμή του προθέματος κάθε ιδιωτικού αναγνωριστικού είναι «did:peer:».
- **Μέθοδος (Αγγλ. Numalgo)**: Το πρώτο bit που ακολουθεί μετά το πρόθεμα δείχνει την μέθοδο. Η μέθοδος ορίζει τον αλγόριθμο με τον οποίο υπολογίζεται το «numeric basis», όπου το «numeric basis» είναι αυτό που κάνει το αναγνωριστικό μοναδικό. Έως και σήμερα, υπάρχουν τρεις διαφορετική αλγόριθμοι με τους οποίους μπορεί να υπολογιστεί, συμπερασματικά, οι τιμές που μπορεί να λάβει η μέθοδος είναι μεταξύ 0 και 2.

  Για παράδειγμα, στην παραπάνω εικόνα η μέθοδος έχει πάρει τον αριθμό ένα. Ο μέθοδος με τον αριθμό ένα λειτουργεί με τον εξής τρόπο, παίρνει το αποκεντρωμένο έγγραφο (με όλα τα δημόσια κλειδιά και πέρα από την τιμή του αποκεντρωμένου αναγνωριστικού «id») και υπολογίζει το «SHA-256» κατακερματισμένο αλφαριθμητικό.
- **Κωδικοποίηση (Αγγλ. Transform)**: Το δεύτερο bit που ακολουθεί μετά το πρόθεμα δείχνει την τιμή της κωδικοποίησης. Η κωδικοποίηση χρησιμοποιείται στο επόμενο κομμάτι, για να υπολογίσει το αποτέλεσμα του αναγνωριστικού. Ως προεπιλεγμένη τιμή είναι η «z», που αντιστοιχίζει στην κωδικοποίηση «base58».
- **Αναγνωριστικό (Αγγλ. Multicodec + Numeric Basis)**: Το υπόλοιπο κόμματι αντιστοιχίζει στο αναγνωριστικό, το οποίο υπολογίζεται από το «multicodec» (μεταδεδομένα) και το «numeric basis». Στην συνέχεια, οι δύο αυτές τιμές παίρνανε από την κωδικοποίηση (π.χ. φωτογραφία «base58») και αποτελούν το αποτέλεσμα του αναγνωριστικού.

Μεταφορά 3.3.2.δ

Η μεταφορά των ιδιωτικών αποκεντρωμένων αναγνωριστικών έχει ως προϋπόθεση την ασφάλεια του περιεχόμενου τους. Αυτό πρέπει να τηρηθεί διότι τα αναγνωριστικά αυτά είναι μια ευαίσθητη πληροφορία, την οποία δεν θέλει κανείς να μοιραστεί πέρα από την οντότητα με την οποία επικοινωνεί.

Μια επιλογή για την ασφαλή μεταφορά είναι το πρωτόκολλο ασφαλούς επικοινωνίας [Aries RFC 0023]. Πέρα από το [Aries RFC 0023], μπορεί να χρησιμοποιηθεί και το πρωτόκολλο TLS/SSL. Κάτι το οποίο πρέπει να προσέξει κάνεις όμως, είναι πως το πρωτόκολλο αυτό βασίζεται σε τρίτους για την ομαλή λειτουργία του.

Αποθήκευση 3.3.2.ε

Τα αποκεντρωμένα αναγνωριστικά αποθηκεύονται σε κάποιο σημείο εύκολα προσβάσιμο και από τις δύο εμπλεκόμενες οντότητες. Αυτό μπορεί να είναι, ο τοπικός αποθηκευτικός χώρος των κινητών τηλεφώνων τους, κάποιος εξωτερικός χώρος αποθήκευσης κ.τ.λ. Δηλαδή, ένα χώρο στον οποίο μόνο αυτοί οι δύο θα έχουν πρόσβαση και κανένας άλλος.

Ενημέρωση ενός ιδιωτικού αποκεντρωμένου εγγράφου 3.3.2.ζ

Αν μια οντότητα επιθυμήσει να ενημέρωση κάποια δεδομένα στο αποκεντρωμένο έγγραφο μιας άλλης (π.χ. επειδή θέλει να ανακυκλώσει κάποιο κλειδί), θα πρέπει να δημιουργήσει ένα «delta». Το «delta» είναι ένα JSON αρχείο το οποίο ενημερώνει κάποιον για τις αλλαγές που πήραν μέρος.

Ένα «delta» αποτελείται από τρία πεδία. Αυτά είναι, το «change», το «by» και το «when». Πιο αναλυτικά, το «change» αναφέρεται για το τι έχει αλλάξει, το «by» είναι από ποιον έχει γίνει η αλλαγή και το «when» αναφέρεται στο πότε έγινε. Στο κομμάτι κώδικα 4 υπάρχει μια αναπαράσταση ενός «delta».

EXAMPLE 7: Delta structure

```
{
    "change": <base64url encoding of a change fragment>,
    "by": [ {"key": <id of key>, "sig": <signature value>} ... ],
    "when": <ISO8601/RFC3339 UTC timestamp with at least second precision>
}
```

Σχήμα 27: δομή delta. Πηγή: https://identity.foundation/peer-did-method-spec/

Επίπεδο μεταφοράς δεδομένων 3.4

Το επίπεδο τρία και τέσσερα, είναι τα επίπεδα όπου η ανθρώπινη εμπιστοσύνη ακμάζει. Στο τεχνικό κομμάτι, το τρίτο επίπεδο θίγει το τρίγωνο των επαληθεύσιμων διαπιστευτηρίων το οποίο έχει αναλυθεί στο δεύτερο κεφάλαιο. Στο επίπεδο αυτό, εκδότης, κάτοχος και επαληθευτής ανταλλάσσουν μεταξύ τους διαπιστευτήρια και τεκμήρια, χρησιμοποιώντας κάποια πρωτόκολλα, τα οποία βασίζονται πάνω στο δεύτερο επίπεδο.

Το κυβερνητικό κομμάτι αυτού του επιπέδου είναι αυτό που το κάνει τόσο σημαντικό. Κάθε διαπιστευτήριο το οποίο έχει την δυνατότητα να καταχωρηθεί σε μια οντότητα από οποιονδήποτε εκδότη, χρειάζεται κάποια κυβερνητική αρχή, η οποία αναλύει τους όρους και τις προϋποθέσεις έκδοσης τους. Ένας όρος μπορεί να είναι, σε ποιες οντότητες (με ποια κριτήρια) επιτρέπεται να γίνει η καταχώρηση του διαπιστευτηρίου κ.α. Ένα παράδειγμα του επιπέδου αυτό είναι τα χρήματα, όπου

μια δημόσια αρχή θέτει κάποιους κανόνες τους οποίους κάθε χαρτονόμισμα θα πρέπει να πληροί, ούτως ώστε να μπορέσει να πάρει μέρος σε οποιαδήποτε συναλλαγή.

Επίπεδο εφαρμογής 3.5

Το τέταρτο επίπεδο αναφέρεται στο επίπεδο της εφαρμογής. Το επίπεδο αυτό, έχει σχεδιαστεί με στόχο να ενεργοποιήσει την επικοινωνία μεταξύ διαφορετικών οικοσυστημάτων ταυτότητας. Ένα οικοσύστημα μπορεί να είναι ένα κράτος, μια υπηρεσία κ.α. Αυτό βέβαια δεν μπορεί να επιτευχθεί χωρίς την σωστή λειτουργία των τριών επιπέδων που αναφέρθηκαν στα προηγούμενα κεφάλαια.

Σκοπός του επιπέδου εφαρμογής είναι η άμεση μεταφορά πληροφορίας μεταξύ εφαρμογών, ιστοσελίδων, επιχειρήσεων, παρέχοντας ασφάλεια, ιδιωτικότητα και προστασία των δεδομένων που ανταλλάσσονται μεταξύ οικοσυστημάτων. Μια παρόμοια ιδέα είναι και το «sky computing», όπου στόχος της είναι να παρέχει μια μορφή διαλειτουργικότητας μεταξύ διαφορετικών «cloud hosting» υπηρεσιών.

Σχήμα 28: παράδειγμα αλληλεπίδρασης στο επίπεδο εφαρμογής

Για παράδειγμα, στο σχήμα 27 ένας άνθρωπος, ο οποίος είναι κάτοικος ενός κράτους, επιθυμεί να ταξιδέψει σε κάποιο άλλο. Για να μπορέσει να επιτύχει κάτι τέτοιο, θα πρέπει να έχει στην διάθεση του ένα διαβατήριο, το οποίο μπορεί να πιστοποιηθεί από το άλλο. Αυτό είναι ένα παράδειγμα μιας επικοινωνίας μεταξύ οικοσυστημάτων, όπου ο άνθρωπος αντιπροσωπεύει μια οντότητα και κάθε κράτος αντιπροσωπεύει ένα διαφορετικό οικοσύστημα.

ΚΕΦΑΛΑΙΟ 4: Ανάπτυξη δικτύου και λογισμικού

Εισαγωγή 4.1

Σκοπός και απαιτήσεις 4.1.1

Ο σκοπός της εφαρμογής είναι να αναδείξει τις δυνατότητες ενός συστήματος SSI, χρησιμοποιώντας την ήδη υπάρχουσα κεντρικοποιημένη δομή. Θα υποθέσουμε, λοιπόν, ότι το πανεπιστήμιο Θεσσαλίας θέλει να αρχίσει να εκδίδει πτυχία στους φοιτητές, υπό την μορφή των επαληθεύσιμων διαπιστευτηρίων. Για να πραγματοποιηθεί αυτό, χρειάζεται ένας μηχανισμός με τον οποίο το σύστημα του πανεπιστημίου Θεσσαλίας θα μπορεί να αναγνωρίζει τους φοιτητές με αυτοματοποιημένο τρόπο και ύστερα να εκδίδει το αντίστοιχο διαπιστευτήριο. Κάτι τέτοιο είναι εφικτό μέσω του συστήματος αυθεντικοποίησης που χρησιμοποιείται ήδη (όνομα και κωδικός).

Σε ένα δεύτερο κομμάτι, εφόσον ο φοιτητής λάβει την πιστοποίηση του πανεπιστημίου (π.χ. έχει αποφοιτήσει από το τμήμα), θα πρέπει να παρουσιάσει το υπάρχον διαπιστευτήριο σε κάποιον οργανισμό. Ο οργανισμός θα λάβει το διαπιστευτήριο του φοιτητή και θα επαληθεύει την εγκυρότητα του.

Όλα τα παραπάνω προϋποθέτουν τρεις οντότητες, έναν φοιτητή, ένα πανεπιστήμιο και έναν οργανισμό. Για κάθε μία από τις οντότητες εξάγονται οι εξής απαιτήσεις:

- Το πανεπιστήμιο θα πρέπει να παρέχει μία διεπαφή χρήστη, μέσω της οποίας ένας φοιτητής θα συνδέεται με τα κεντρικοποιημένα διαπιστευτήρια του, ώστε να μπορέσει να δημιουργήσει μία αποκεντρωμένη σύνδεση.
- Το πανεπιστήμιο θα πρέπει να έχει ένα διαχειριστικό περιβάλλον, στο οποίο θα:
    - Παρουσιάζονται οι συνδέσεις με τους φοιτητές.
    - Υπάρχει δυνατότητα να αναθέσει ένας διαχειριστής ένα πτυχίο, υπό την μορφή των επαληθεύσιμων διαπιστευτηρίων.
- Ένας φοιτητής θα πρέπει να συνδέεται σε ένα σύστημα όπου θα μπορεί:
    - Να δει όλες τις υπάρχουσες συνδέσεις που έχει.
    - Να δεχτεί μία πρόσκληση για να συνδεθεί με μία οντότητα (π.χ. έναν οργανισμό ή το πανεπιστήμιο).

    - Να δει τα διαπιστευτήρια που του έχουν ανατεθεί.
    - Να αποφασίσει αν θα μοιραστεί τα διαπιστευτήρια που του έχουν ανατεθεί με κάποια άλλη οντότητα.
- Ένας οργανισμός θα πρέπει να συνδέεται σε ένα σύστημα όπου θα μπορεί:
    - Να δει όλες τις υπάρχουσες συνδέσεις που έχει.
    - Να δημιουργεί μία πρόσκληση για σύνδεση.
    - Να ζητήσει από τον φοιτητή να μοιραστεί μαζί του τα διαπιστευτήρια.

Τεχνολογίες και εργαλεία 4.1.2

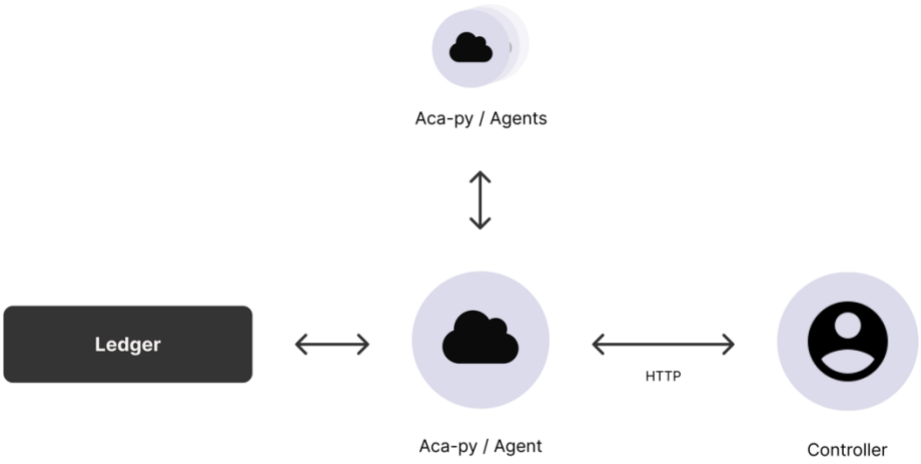
Ως κεντρικό σύστημα υποδομής της εργασίας, έχει επιλεχθεί το οικοσύστημα του οργανισμού Hyperledger. Συγκεκριμένα, έχουν χρησιμοποιηθεί τρία έργα του οργανισμού: Hyperledger Ursa, Hyperledger Aries και Hyperledger Indy.

- Το Hyperledger Ursa είναι μία βιβλιοθήκη κρυπτογραφίας, η οποία έχει ως στόχο να προσφέρει επαναχρησιμοποιήσιμες υλοποιήσεις συναρτήσεων.
- Το Hyperledger Indy είναι ένα σύνολο επαναχρησιμοποιήσιμων εργαλείων και βιβλιοθηκών με στόχο την επίτευξη της κατανεμημένης ταυτότητας με βάση το blockchain. Περιέχει, εκτός άλλων, το Indy Node το οποίο είναι ένα ειδικά φτιαγμένο blockchain για να επιλύσει το πρόβλημα της ψηφιακής ταυτότητας, τον μηχανισμό συναίνεσης Indy Plenum, κ.α.
- Το Hyperledger Aries είναι ένα σύνολο εργαλείων, πρωτοκόλλων και υλοποιήσεων με στόχο την δημιουργία, μετάδοση και αποθήκευση επαληθεύσιμων διαπιστευτηρίων.

Στο οικοσύστημα του Hyperledger, ο όρος πορτοφόλι υφίσταται σαν αποθηκευτικό μέσο. Τις υπόλοιπες λειτουργίες (π.χ. επικοινωνία με άλλες οντότητες) τις αναλαμβάνουν οι πράκτορες (Αγγλ. agents). Ένας πράκτορας είναι ένα ειδικό λογισμικό το οποίο είναι υπεύθυνο για την επικοινωνία με άλλους πράκτορες, την επικοινωνία με το καθολικό, την διαχείριση του πορτοφολιού, κ.α. Τέλος, με την σειρά τους, οι πράκτορες συνδέονται με έναν χειριστή (Αγγλ. controller), ο οποίος είναι υπεύθυνος για τις λειτουργίες που θα εκτελέσει ο πράκτορας (π.χ. πότε θα συνδεθεί με έναν άλλον, τι να συμπεριλάβει σε ένα διαπιστευτήριο, κτλ.).

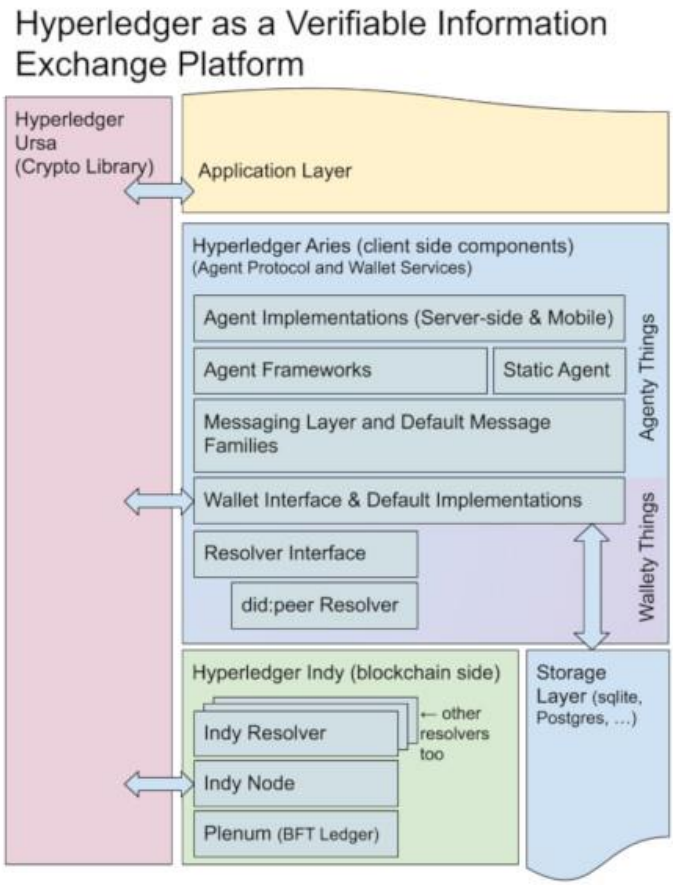
Στην συγκεκριμένη υλοποίηση, τον ρόλο του πράκτορα τον λαμβάνει το Aries Cloud Agent Python[6], ενώ ο χειριστής είναι ο εκάστοτε εξυπηρετητής της κάθε οντότητας. Το γραφικό περιβάλλον απλώς παρέχει μια φιλική διεπαφή του χειριστή προς τον χρήστη.

[6] https://github.com/hyperledger/aries-cloudagent-python



Σχήμα 29: οικοσύστημα ενός πράκτορα

Στο σχήμα 29 φαίνεται συνοπτικά το οικοσύστημα του οργανισμού Hyperledger.



Σχήμα 30: το οικοσύστημα του Hyperledger. Πηγή: https://www.hyperledger.org/blog/2019/05/14/announcing-hyperledger-aries-infrastructure-supporting-interoperable-identity-solutions

Στον πίνακα 4, παρουσιάζονται τα εργαλεία και οι τεχνολογίες που χρησιμοποιήθηκαν για την δημιουργία της εφαρμογής .

Τεχνολογία	Περιγραφή
Golang	Γλώσσα προγραμματισμού για την ανάπτυξη των διακομιστών.
JavaScript	Γλώσσα προγραμματισμού για την ανάπτυξη γραφικού περιβάλλοντος.
Typescript	Γλώσσα προγραμματισμού βασισμένη στην γλώσσα JavaScript
NextJS	Βιβλιοθήκη ανάπτυξης λογισμικού βασισμένο στην JavaScript είτε στην Typescript.
Docker	Μια πλατφόρμα εικονοποίησης σε επίπεδο λογισμικού.
Acapy	Hyperledger Aries Cloud Agent Python (ACA-Py)
Von Network	Μια μικρή υλοποίηση του Indy Node Blockchain δικτύου.

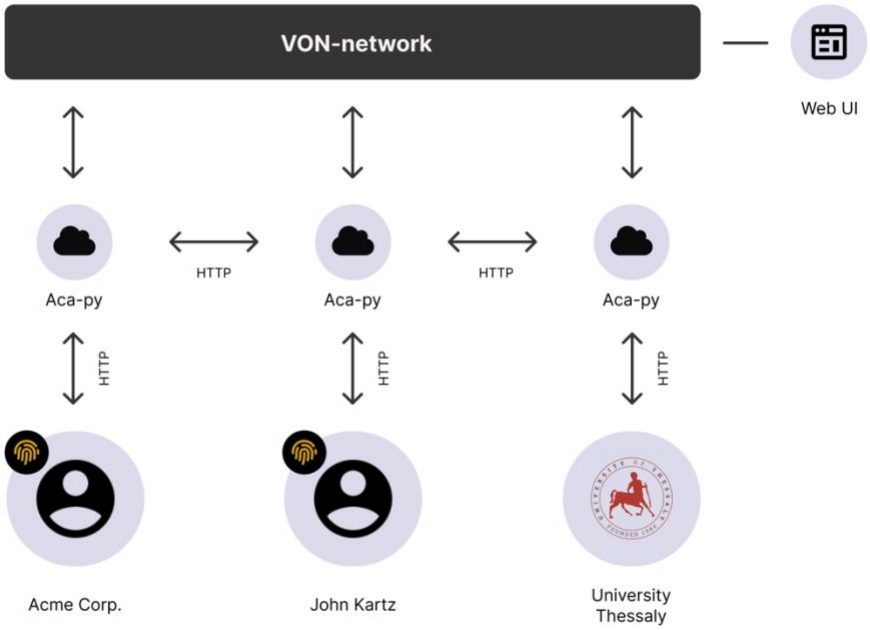
Πίνακας 4: τεχνολογίες υλοποίησης

Ανάλυση υλοποίησης και αρχιτεκτονική δικτύου 4.2

Συνολική αρχιτεκτονική δικτύου 4.2.1

Στο σχήμα 21 φαίνεται η συνολική αρχιτεκτονική του δικτύου. Όπως φαίνεται υπάρχουν οι τρείς οντότητες, όπου οι δυο εκ των οποίων (οργανισμός και φοιτητής) χρησιμοποιούν το ίδιο υποσύστημα. Τέλος η τρίτη οντότητα (πανεπιστήμιο) έχει τον δικό του ξεχωριστό υποσύστημα.

Όλα τα υποσυστήματα επικοινωνούν με τον δικό τους Aca-py (Agent), όπου το Aca-py είναι υπεύθυνο για την επικοινωνία με το VON-network.



Σχήμα 31: η συνολική αρχιτεκτονική της υλοποίησης

Το δίκτυο VON 4.2.2

Απαραίτητη είναι η ύπαρξη ενός δικτύου blockchain, και για αυτό έχει επιλεχθεί το λογισμικό ανοιχτού κώδικα VON[7] (). Το VON αποτελεί μία υλοποίηση του Hyperledger Indy Node και παρέχει την δυνατότητα σε κάποιον να τρέξει ένα blockchain δίκτυο τοπικά, καθώς και ένα γραφικό περιβάλλον (υπό την μορφή μιας εφαρμογής δικτύου) για την εξερεύνηση του blockchain.

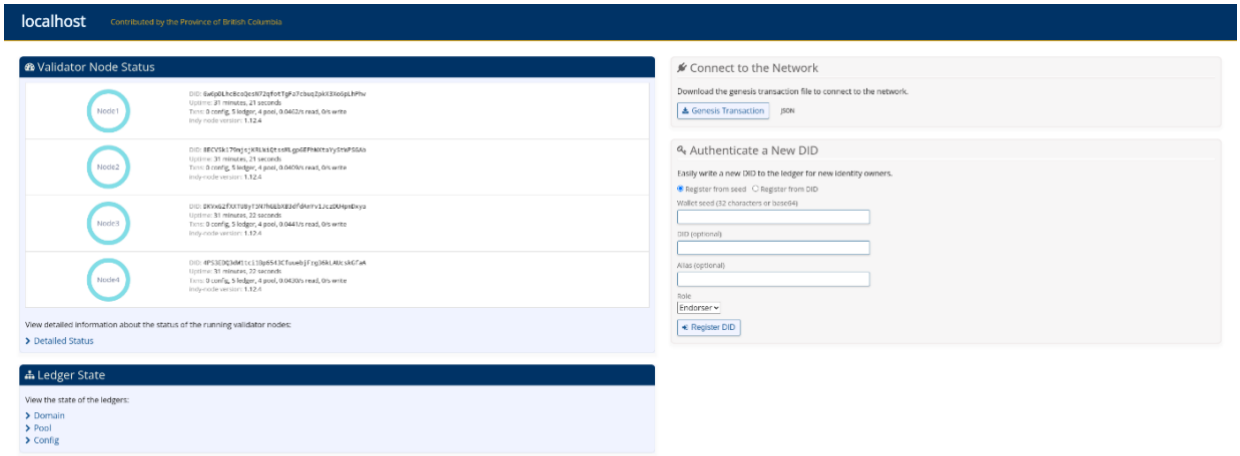
Εκτελώντας τις κατάλληλες εντολές (οι οποίες παρέχονται στο ανοιχτό αποθετήριο του VON) στο τερματικό, το δίκτυο Blockchain θα τρέξει τοπικά (χρησιμοποιώντας docker containers). Στο σχήμα 31 υπάρχουν όλες οι εικονικές μηχανές οι οποίες παίρνουν μέρος στο VON-network.

[7] https://github.com/bcgov/von-network

```
von-network on  main on 🐳 v20.10.17
➜ ./manage start

Using: docker-compose --log-level ERROR

Creating von_node4_1     ... done
Creating von_node2_1     ... done
Creating von_node1_1     ... done
Creating von_node3_1     ... done
Creating von_webserver_1 ... done
Want to see the scrolling container logs? Run "./manage logs"

von-network on  main on 🐳 v20.10.17 took 3s
➜ docker ps --format "table {{.ID}}\t{{.Names}}\t{{.CreatedAt}}\t{{.Status}}"
CONTAINER ID   NAMES           CREATED AT                      STATUS
b4f3b70fc941   von_node3_1     2022-09-26 13:09:56 +0300 EEST   Up 5 seconds
3c2b61f0034b   von_webserver_1 2022-09-26 13:09:56 +0300 EEST   Up 4 seconds
ac3218c8ec20   von_node1_1     2022-09-26 13:09:56 +0300 EEST   Up 4 seconds
c761169fe9e0   von_node4_1     2022-09-26 13:09:56 +0300 EEST   Up 5 seconds
8e8bf9100308   von_node2_1     2022-09-26 13:09:56 +0300 EEST   Up 5 seconds
```

Σχήμα 32: αποτέλεσμα εκκίνησης δικτύου VON

Πηγαίνοντας στον σύνδεσμο http://localhost:9000, εμφανίζεται το γραφικό περιβάλλον το οποίο παρέχεται μαζί με το δίκτυο. Εκεί υπάρχουν όλοι οι κόμβοι οι οποίοι τρέχουν και η κατάσταση τους.



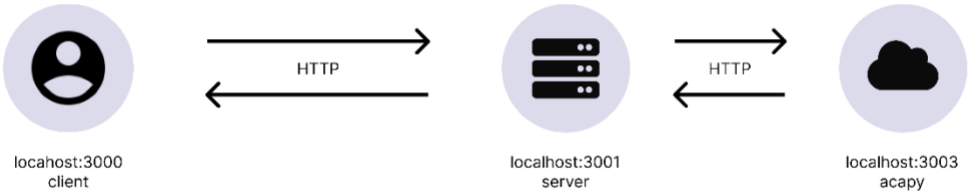
Σχήμα 33: το γραφικό περιβάλλον του δικτύου VON

Επίσης παρέχεται ένα αρχείο στο σύνδεσμο http://localhost:9000/genesis, το οποίο φυλάσσει κάποια μεταδεδομένα, τα οποία δίνουν την δυνατότητα σε κάποιον να πάρει μέρος στο VON-network. Στην συνέχεια, ακολουθώντας τον σύνδεσμο Domain, παρουσιάζονται όλες οι συναλλαγές του δικτύου. Παρατηρούμε ότι στην παρούσα κατάσταση δεν υπάρχουν συναλλαγές στο δίκτυο, παρά μόνο αυτές των αρχικών κόμβων.

Σχήμα 34: αρχικές συναλλαγές στο καθολικό

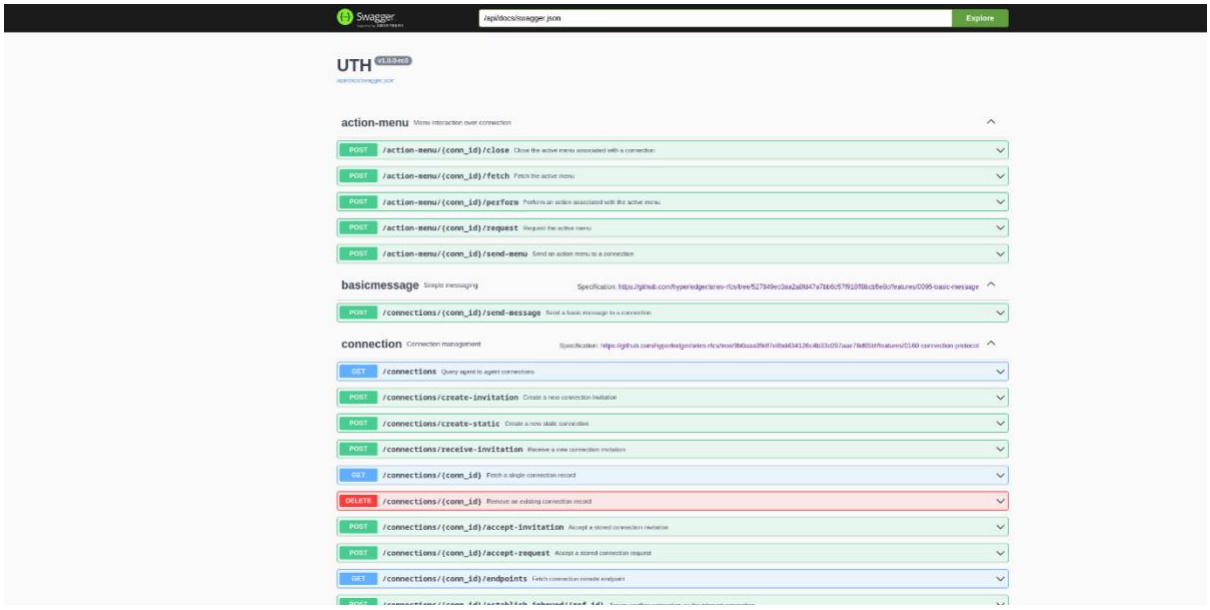
Υποσύστημα UTH 4.2.3

Το υποσύστημα του πανεπιστημίου Θεσσαλίας αποτελείται από 3 υποσυστήματα: ένα γραφικό περιβάλλον, έναν εξυπηρετητή και το ACA-py. Η επικοινωνία μεταξύ των συστημάτων γίνεται μέσω του πρωτοκόλλου HTTP.



Σχήμα 35: επικοινωνία μεταξύ υποσυστημάτων του πανεπιστημίου

Στο σχήμα 34 φαίνεται η επικοινωνία μεταξύ των τριών (client, server, ACA-py). Ο client είναι στην πόρτα 3000 και επικοινωνεί άμεσα με τον server, ο οποίος βρίσκεται στην πόρτα 3001 και ο server με την μεριά του επικοινωνεί με το ACA-py το οποίο είναι στην πόρτα 3003. Επίσης, το Aca-py παρέχει ένα διαχειριστικό περιβάλλον, στο οποίο αναγράφονται όλες οι ενέργειες που μπορεί κάποιος να εκτελέσει. Το περιβάλλον αυτό βρίσκεται στον σύνδεσμο http://localhost:3003.



Σχήμα 36: γραφικό περιβάλλον του ACA-py

Το σύστημα Aca-py έχει προγραμματιστεί έτσι ώστε κατά την εκκίνηση του να δημιουργεί ένα δημόσιο DID και να το δημοσιεύει στο καθολικό που του έχουμε αναδείξει. Στο σχήμα 36 βλέπουμε την έξοδο της εκκίνησης στο τερματικό.

```
uth-agent_1  | {
uth-agent_1  |   "did": "VeYnF5tidYy3kMR2F82UDL",
uth-agent_1  |   "seed": "khni9DDgCtxQJnC6zIBWmqj11q3fK5Yi",
uth-agent_1  |   "verkey": "GcbojJpfExd31LDJF6kEz9oUWiML5VWd2iq3bP4s3UpU"
uth-agent_1  | }
uth-agent_1  | ::::::::::::::::::::::::::::::::::::::::::::
uth-agent_1  | :: UTH                                     ::
uth-agent_1  | ::                                         ::
uth-agent_1  | ::                                         ::
uth-agent_1  | :: Inbound Transports:                     ::
uth-agent_1  | ::                                         ::
uth-agent_1  | ::   - http://0.0.0.0:3002                 ::
uth-agent_1  | ::                                         ::
uth-agent_1  | :: Outbound Transports:                    ::
uth-agent_1  | ::                                         ::
uth-agent_1  | ::   - http                                ::
uth-agent_1  | ::   - https                               ::
uth-agent_1  | ::                                         ::
uth-agent_1  | :: Public DID Information:                 ::
uth-agent_1  | ::                                         ::
uth-agent_1  | ::   - DID: VeYnF5tidYy3kMR2F82UDL         ::
uth-agent_1  | ::                                         ::
uth-agent_1  | :: Administration API:                     ::
uth-agent_1  | ::                                         ::
uth-agent_1  | ::   - http://0.0.0.0:3003                 ::
uth-agent_1  | ::                                         ::
uth-agent_1  | ::                          ver: 1.0.0-rc0 ::
uth-agent_1  | ::::::::::::::::::::::::::::::::::::::::::::
uth-agent_1  |
uth-agent_1  | Listening...
uth-agent_1  |
```

Σχήμα 37: έξοδος από την εκκίνηση του UTH ACA-py

Πηγαίνοντας στην λίστα με τις συναλλαγές του καθολικού, μπορούμε να δούμε ότι έχουν προστεθεί δύο νέες εγγραφές. Η πρώτη εγγραφή αφορά τον ρόλο του UTH στο δίκτυο, ενώ η δεύτερη περιέχει ιδιότητες, όπως την διεύθυνση στην οποία μπορεί κάποιος να επικοινωνήσει με τον πράκτορα του. Τέλος, υπάρχει μία ακόμη θύρα την οποία χρησιμοποιεί το ACA-py, η 3002. Η συγκεκριμένη θύρα χρησιμοποιείται για την επικοινωνία με τους υπόλοιπους πράκτορες.

Σχήμα 38: Η συναλλαγή τύπου NYM

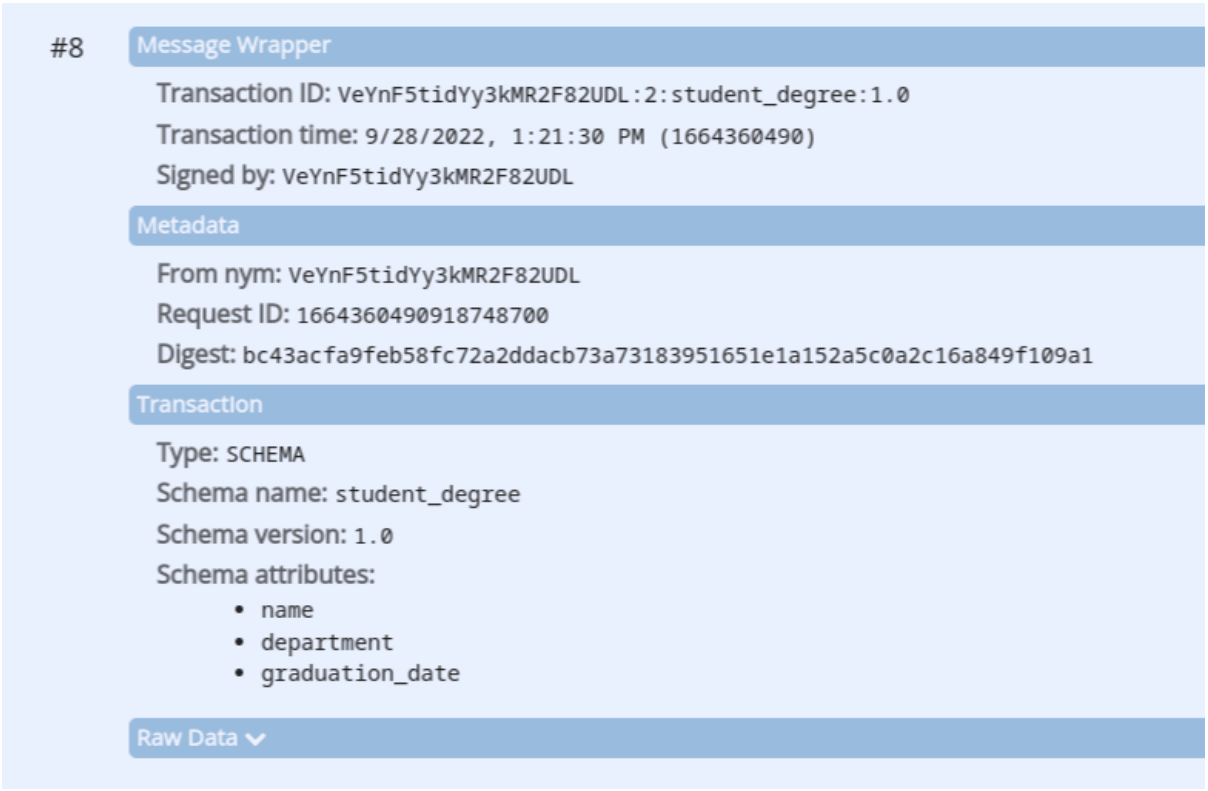
Σχήμα 39: Η συναλλαγή τύπου ATTRIB

Στην συνέχεια, ο εξυπηρετητής έχει προγραμματιστεί έτσι ώστε κατά την εκκίνηση του να επικοινωνεί με το ACA-py, να δημιουργεί το κατάλληλο σχήμα και να ορίζει τον ορισμού του διαπιστευτήριού (Αγγλ. Credential Definition) στο καθολικό. Να σημειωθεί ότι σε μία συλλογική υιοθέτηση του SSI, το σχήμα θα το δημιουργούσε κάποιος θεσμός (όπως το κράτος) και το πανεπιστήμιο απλώς θα δημιουργούσε τον ορισμό διαπιστευτηρίου. Έτσι, στην περίπτωση μας, όλα τα πτυχία θα είχανε τις ίδιες ιδιότητες.

```
→ go run cmd/server/main.go
[Fx] PROVIDE    *echo.Echo <= github.com/ealexandros/digital-story/uth/server/server.NewEcho()
[Fx] PROVIDE    *gorm.DB <= github.com/ealexandros/digital-story/uth/server/db.NewPostgres()
[Fx] PROVIDE    *lotusdb.LotusDB <= github.com/ealexandros/digital-story/uth/server/db.NewLotus()
[Fx] PROVIDE    *services.Auth <= github.com/ealexandros/digital-story/uth/server/services.NewAuth()
[Fx] PROVIDE    *services.Connections <= github.com/ealexandros/digital-story/uth/server/services.NewConnections()
[Fx] PROVIDE    *services.Credentials <= github.com/ealexandros/digital-story/uth/server/services.NewCredentials()
[Fx] PROVIDE    *acapy.Client <= github.com/ealexandros/digital-story/uth/server/acapy.New()
[Fx] PROVIDE    config.Config <= github.com/ealexandros/digital-story/uth/server/config.NewConfig()
[Fx] PROVIDE    fx.Lifecycle <= go.uber.org/fx.New.func1()
[Fx] PROVIDE    fx.Shutdowner <= go.uber.org/fx.(*App).shutdowner-fm()
[Fx] PROVIDE    fx.DotGraph <= go.uber.org/fx.(*App).dotGraph-fm()
[Fx] INVOKE             github.com/ealexandros/digital-story/uth/server/db.glob..func1()
[Fx] INVOKE             github.com/ealexandros/digital-story/uth/server/controllers.RegisterAuth()
[Fx] INVOKE             github.com/ealexandros/digital-story/uth/server/controllers.RegisterConnections()
[Fx] INVOKE             github.com/ealexandros/digital-story/uth/server/controllers.RegisterWebHooks()
[Fx] INVOKE             github.com/ealexandros/digital-story/uth/server/controllers.RegisterCredentials()
[Fx] INVOKE             github.com/ealexandros/digital-story/uth/server/acapy.RegisterStudentDegree()

Registered Schema with Name=student_degree and ID=VeYnF5tidYy3kMR2F82UDL:2:student_degree:1.0
Registered Credential Definition with ID=VeYnF5tidYy3kMR2F82UDL:3:CL:8:1

[Fx] INVOKE             main.main.func1()

   ____    __
  / __/___/ /  ___
 / _// __/ _ \/ _ \
/___/\__/_//_/\___/ v4.9.0
High performance, minimalist Go web framework
https://echo.labstack.com
____________________________________O/_______
                                    O\
⇨ http server started on [::]:3001
```

Σχήμα 40: έξοδος από την εκκίνηση του εξυπηρετητή του UTH

Στο σχήμα 40, βλέπουμε το σχήμα και τον ορισμού του διαπιστευτηρίου ως συναλλαγές στο καθολικό.

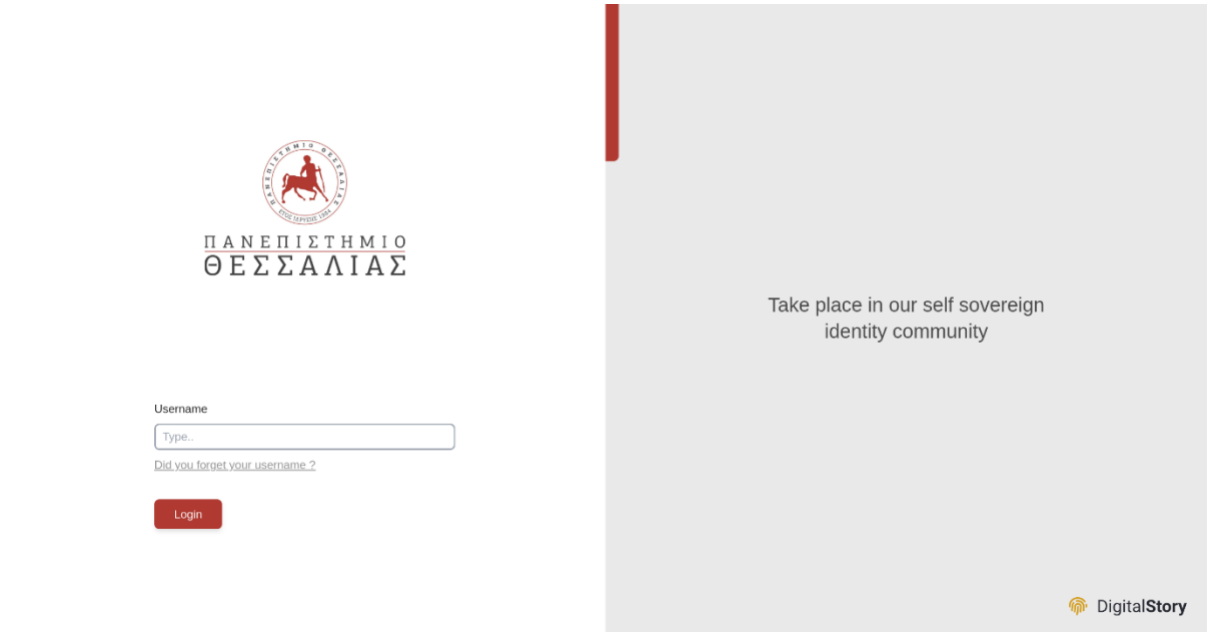


Σχήμα 41: έξοδος από την εκκίνηση του εξυπηρετητή του UTH

Σχήμα 42: η συναλλαγή με την δήλωση του διαπιστευτήριού

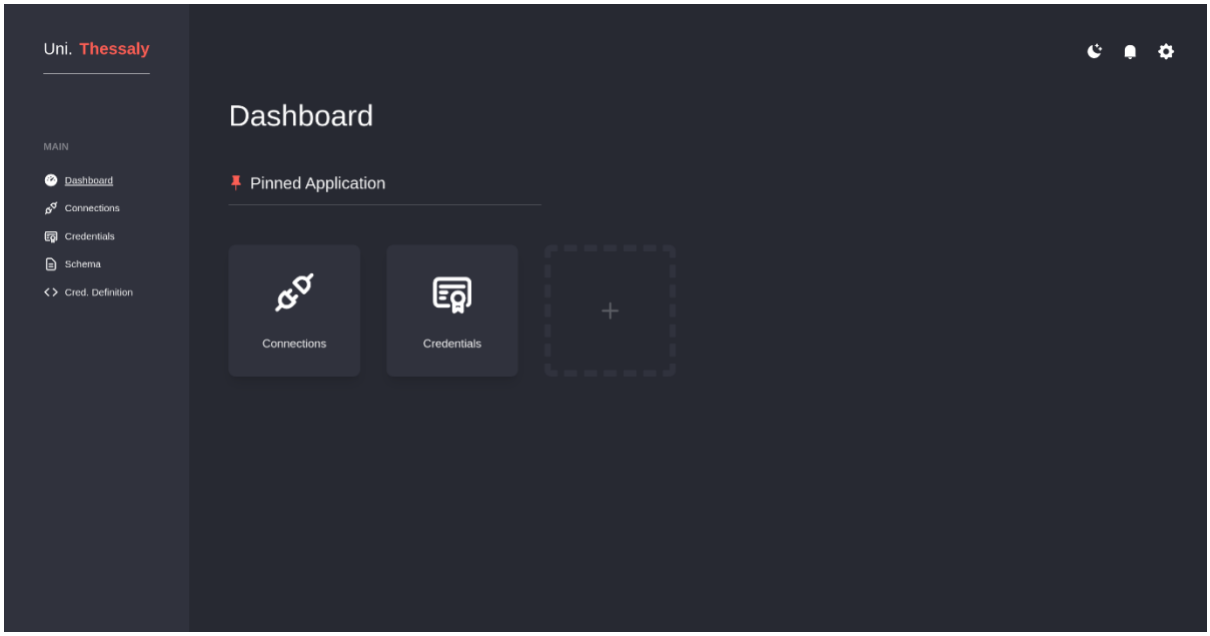
Το τελευταίο υποσύστημα του UTH, αφορά το γραφικό περιβάλλον. Αυτό χωρίζεται σε δύο κατηγορίες: την πρόσκληση του φοιτητή για να συνδεθεί με τον πράκτορα του UTH και την διαχείριση των συνδέσεων (μαζί με την ανάθεση πτυχίων).

Για να συνδεθεί ο φοιτητής με το πανεπιστήμιο θα πρέπει να το κάνει μέσω της διαδικτυακής πλατφόρμας (http://localhost:3000/signin) που έχει χτιστεί. Για τους λόγους της παρουσίασης, η σύνδεση γίνεται μονάχα με το όνομα του φοιτητή. Τέλος, αν το όνομα δεν αντιστοιχεί σε κάποιο φοιτητή τότε εμφανίζεται και το αντίστοιχο μήνυμα λάθος.



Σχήμα 43: το γραφικό περιβάλλον της σύνδεσης του φοιτητή

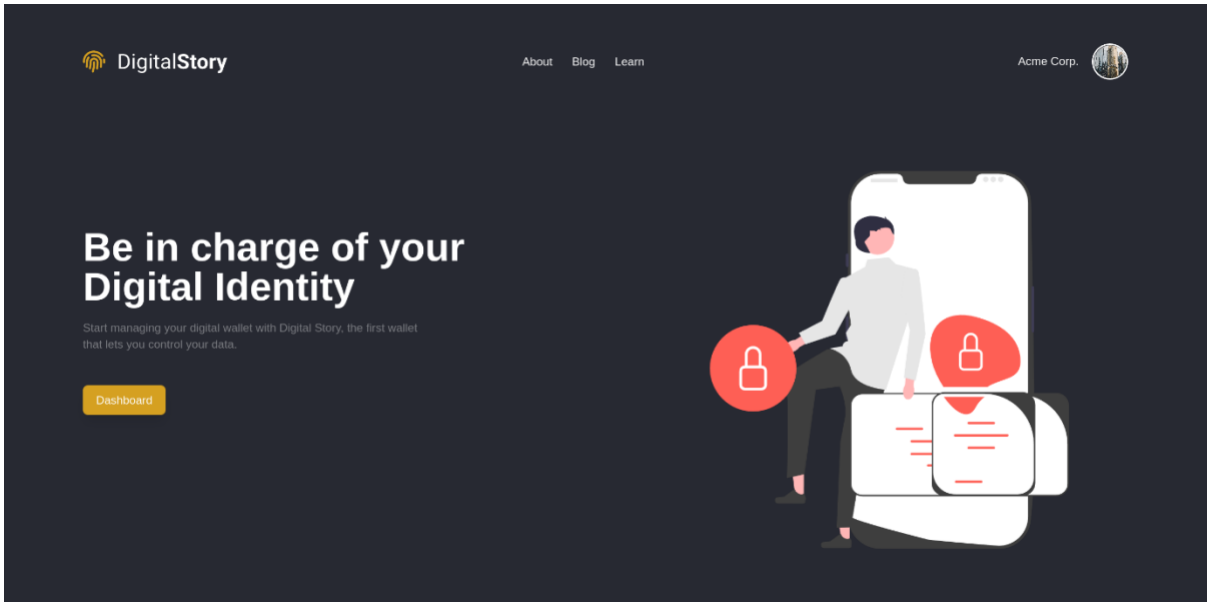
Ύστερα, στην διεύθυνση http://localhost:3000/dashboard βρίσκεται το διαχειριστικό του UTH, μέσα από το οποίο ένας διαχειριστής ελέγχει τις συνδέσεις και αναθέτει πτυχία.



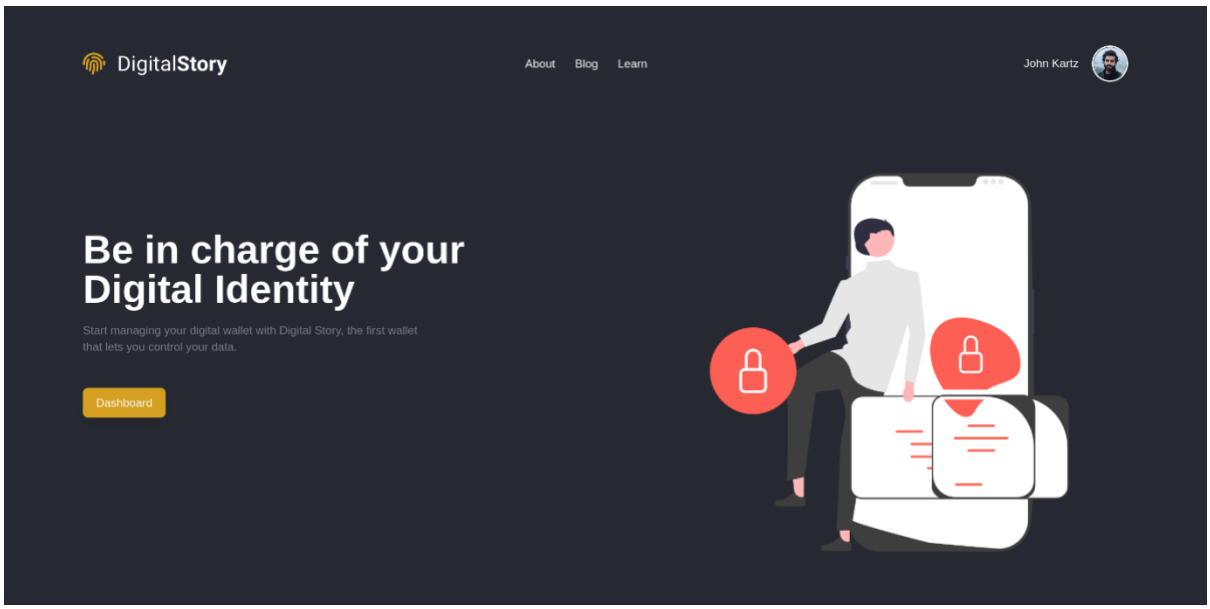
Σχήμα 44: το γραφικό περιβάλλον του διαχειριστικού του UTH

Υποσύστημα Φοιτητή και Οργανισμού 4.2.4

Για τον φοιτητή και τον οργανισμό, έχει υλοποιηθεί ένα κοινό υποσύστημα το Digital Story, το οποίο αντιπροσωπεύει μια υπηρεσία σύνδεσης σε ένα αποκεντρωμένο δίκτυο αυτοδιαχειριζόμενης ταυτότητας (στην περίπτωση της εφαρμογής, το αποκεντρωμένο σύστημα είναι το VON-network). Μέσα από το Digital Story ο φοιτητής και ο οργανισμός θα είναι σε θέση να συνδέονται και να ελέγχουν όλα τους τα στοιχεία μέσω ενός διαχειριστικού περιβάλλοντος.



Σχήμα 45: γραφικό περιβάλλον οργανισμού



Σχήμα 46: γραφικό περιβάλλον φοιτητή

Ξεκινώντας τους πράκτορες του φοιτητή και του οργανισμού στις εικόνες 20 και 21 βλέπουμε τις εξόδους από το τερματικό αντίστοιχα. Όπως παρατηρούμε, ο πράκτορας του οργανισμού χρησιμοποιεί τις θύρες 5002 και 5003, ενώ του φοιτητή 4002 και 4003. Όπως και στο υποσύστημα του UTH, υπάρχουν τα αντίστοιχα γραφικά περιβάλλοντα και εξυπηρετητές (4000 & 4001 για τον φοιτητή και 5000 & 5001 για τον οργανισμό).

```
acme-agent_1   |
acme-agent_1   | ::::::::::::::::::::::::::::::::::::::::::::
acme-agent_1   | :: Acme                                    ::
acme-agent_1   | ::                                         ::
acme-agent_1   | ::                                         ::
acme-agent_1   | :: Inbound Transports:                     ::
acme-agent_1   | ::                                         ::
acme-agent_1   | ::   - http://0.0.0.0:5002                 ::
acme-agent_1   | ::                                         ::
acme-agent_1   | :: Outbound Transports:                    ::
acme-agent_1   | ::                                         ::
acme-agent_1   | ::   - http                                ::
acme-agent_1   | ::   - https                               ::
acme-agent_1   | ::                                         ::
acme-agent_1   | :: Administration API:                     ::
acme-agent_1   | ::                                         ::
acme-agent_1   | ::   - http://0.0.0.0:5003                 ::
acme-agent_1   | ::                                         ::
acme-agent_1   | ::                           ver: 1.0.0-rc0 ::
acme-agent_1   | ::::::::::::::::::::::::::::::::::::::::::::
acme-agent_1   |
acme-agent_1   | Listening...
acme-agent_1   |
```

Σχήμα 47: έξοδος από το τερματικό κατά την εκκίνηση του οργανισμού

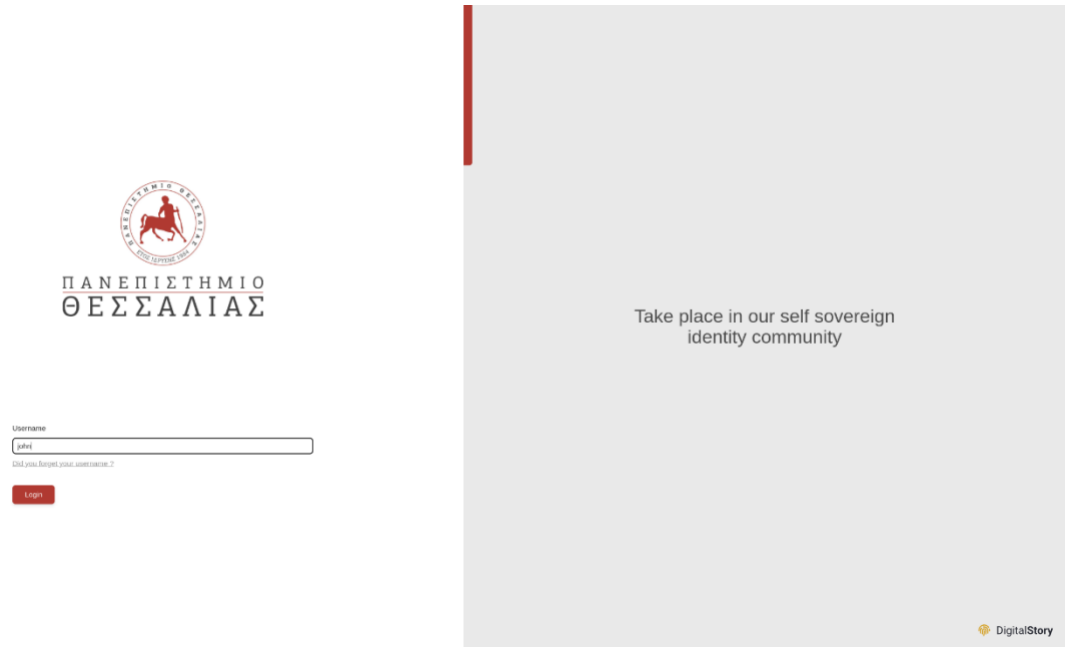
```
john-agent_1   |
john-agent_1   | ::::::::::::::::::::::::::::::::::::::::::::
john-agent_1   | :: John                                    ::
john-agent_1   | ::                                         ::
john-agent_1   | ::                                         ::
john-agent_1   | :: Inbound Transports:                     ::
john-agent_1   | ::                                         ::
john-agent_1   | ::   - http://0.0.0.0:4002                 ::
john-agent_1   | ::                                         ::
john-agent_1   | :: Outbound Transports:                    ::
john-agent_1   | ::                                         ::
john-agent_1   | ::   - http                                ::
john-agent_1   | ::   - https                               ::
john-agent_1   | ::                                         ::
john-agent_1   | :: Administration API:                     ::
john-agent_1   | ::                                         ::
john-agent_1   | ::   - http://0.0.0.0:4003                 ::
john-agent_1   | ::                                         ::
john-agent_1   | ::                           ver: 1.0.0-rc0 ::
john-agent_1   | ::::::::::::::::::::::::::::::::::::::::::::
john-agent_1   |
john-agent_1   | Listening...
john-agent_1   |
```

Σχήμα 48: έξοδος από το τερματικό κατά την εκκίνηση του φοιτητή

Περιπτώσεις χρήσης 4.3

Αλληλεπίδραση φοιτητή με UTH 4.3.1

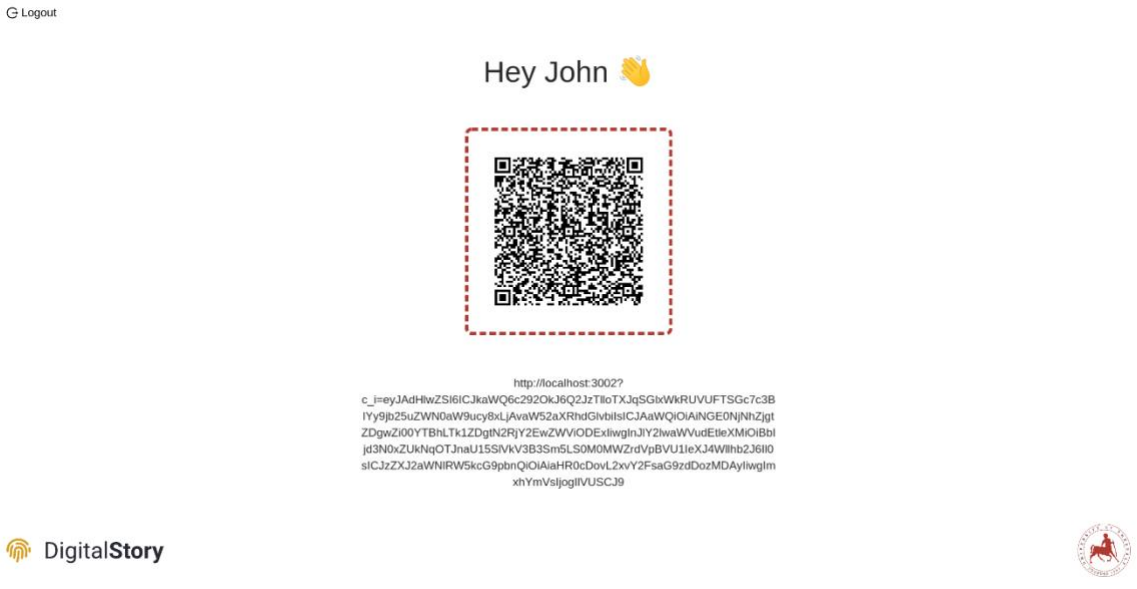
Η αλληλεπίδραση του φοιτητή με το Πανεπιστήμιο Θεσσαλίας χωρίζεται σε δύο ενέργειες. Αρχικά θα πρέπει να συνδεθεί ο πράκτορας του φοιτητή με αυτόν του Πανεπιστημίου και ύστερα, το πανεπιστήμιο να αναθέσει το πτυχίο. Για να συμβεί αυτό, ο φοιτητής εισάγει τα στοιχεία του στην πλατφόρμα του πανεπιστημίου.



Σχήμα 49: ο φοιτητής πληκτρολογεί το όνομα χρήστη του στην πλατφόρμα του πανεπιστημίου

ο φοιτητής πληκτρολογεί τα στοιχεία του στην πλατφόρμα του πανεπιστημίου.

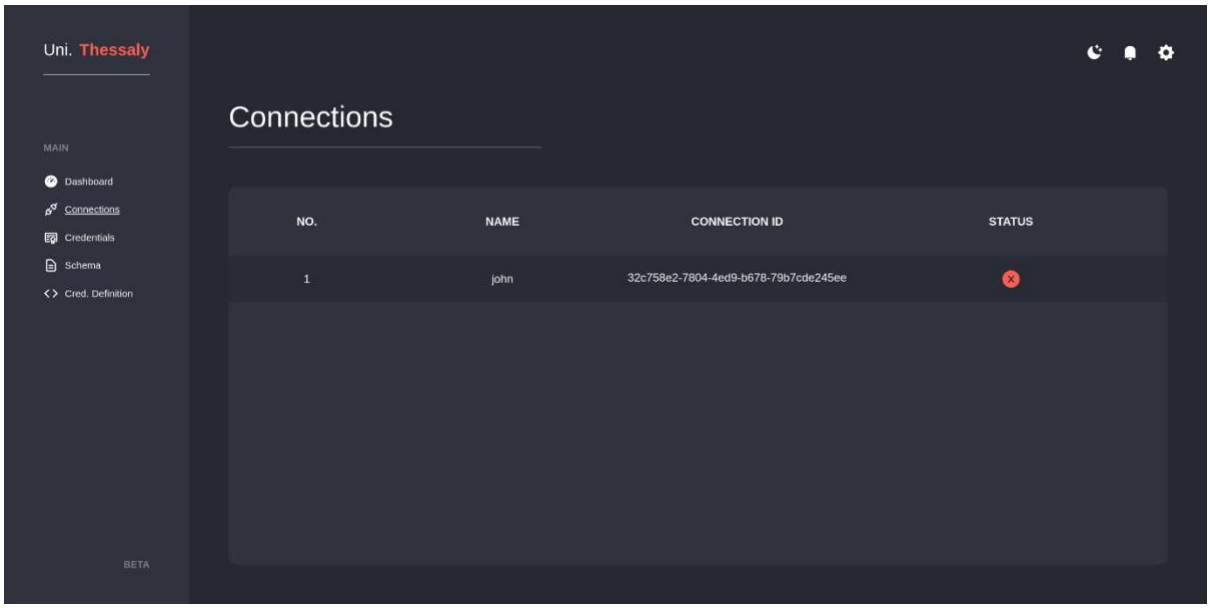
Αφού εισάγει το όνομα χρήστη του (για λόγους παρουσίασης δεν συμπεριλάβαμε κάποιον κωδικό) και πατήσει το κουμπί Login, ανακατευθύνεται στην σελίδα που φαίνεται στο σχήμα 49.



Σχήμα 50: το πανεπιστήμιο δημιουργεί τον σύνδεσμο πρόσκλησης

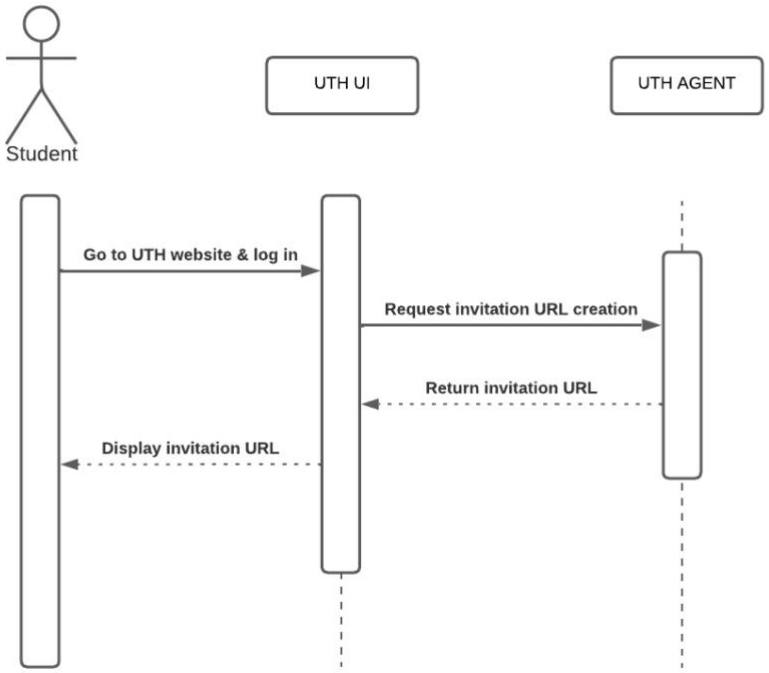
Η σελίδα στο σχήμα 49 περιέχει τον σύνδεσμο πρόσκλησης, τον οποίο ο φοιτητής θα πρέπει να εισάγει στον δικό του πράκτορα για να ξεκινήσει την σύνδεση. Στην περίπτωση που ο φοιτητής χρησιμοποιούσε κάποια εφαρμογή κινητού, θα μπορούσε να σκανάρει τον κωδικό QR, αυτοματοποιώντας την διαδικασία.

Επιλέγοντας την καρτέλα Connections στο διαχειριστικό του UTH, αναγράφονται όλες οι τρέχουσες συνδέσεις. Παρατηρούμε ότι υπάρχει μία καινούργια εγγραφή για τον φοιτητή, αλλά από την στήλη της κατάστασης (STATUS) είναι φανερό ότι η σύνδεση δεν έχει εδραιωθεί, αφού ο φοιτητής δεν έχει εκτελέσει ακόμη κάποια ενέργεια.



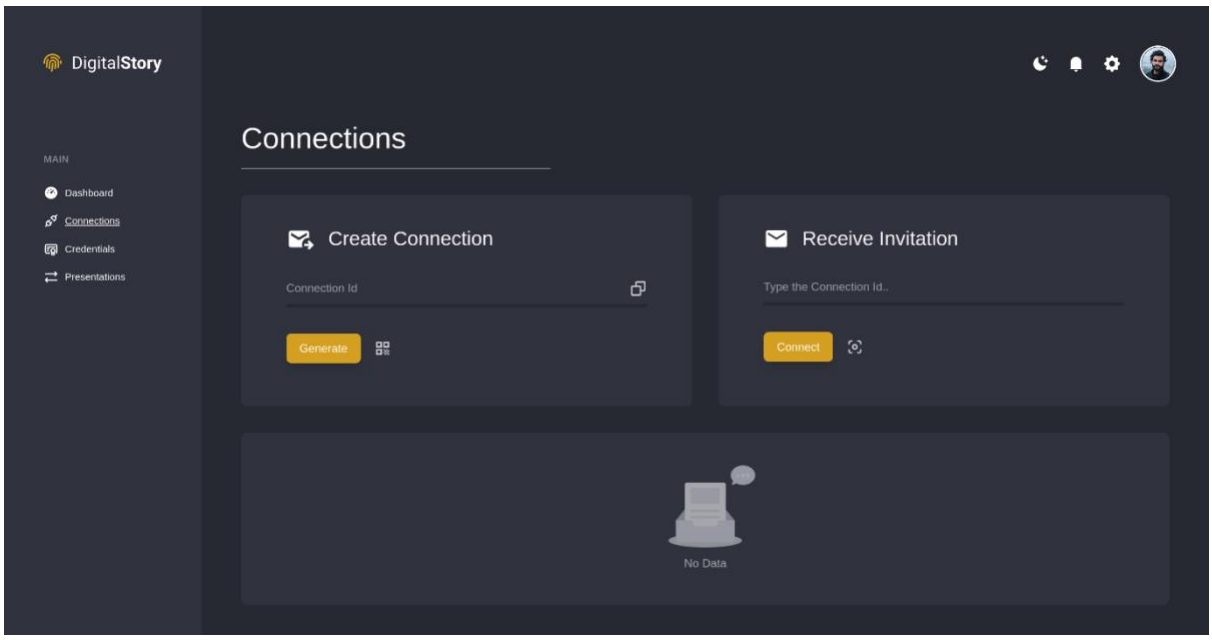
Σχήμα 51: η καρτέλα των συνδέσεων του πανεπιστημίου, πρώτού ο φοιτητής εκτελέσει κάποια ενέργεια

Ο τρόπος με τον οποίο δημιουργείται ο σύνδεσμος της πρόσκλησης είναι μέσω του πράκτορα του πανεπιστημίου. Η παραπάνω διαδικασία, περιγράφεται και από το διάγραμμα ακολουθίας στο σχήμα 22.



Σχήμα 52: διάγραμμα ακολουθίας δημιουργίας σύνδεσης

Αφού ο φοιτητής αντιγράψει τον σύνδεσμο πρόσκλησης, θα μεταβεί στο διαχειριστικό του και συγκεκριμένα στην καρτέλα Connections. Εκεί μπορεί είτε να δημιουργήσει μία καινούργια πρόσκληση ώστε να την στείλει σε έναν άλλο πράκτορα, είτε να επικολλήσει μία πρόσκληση.

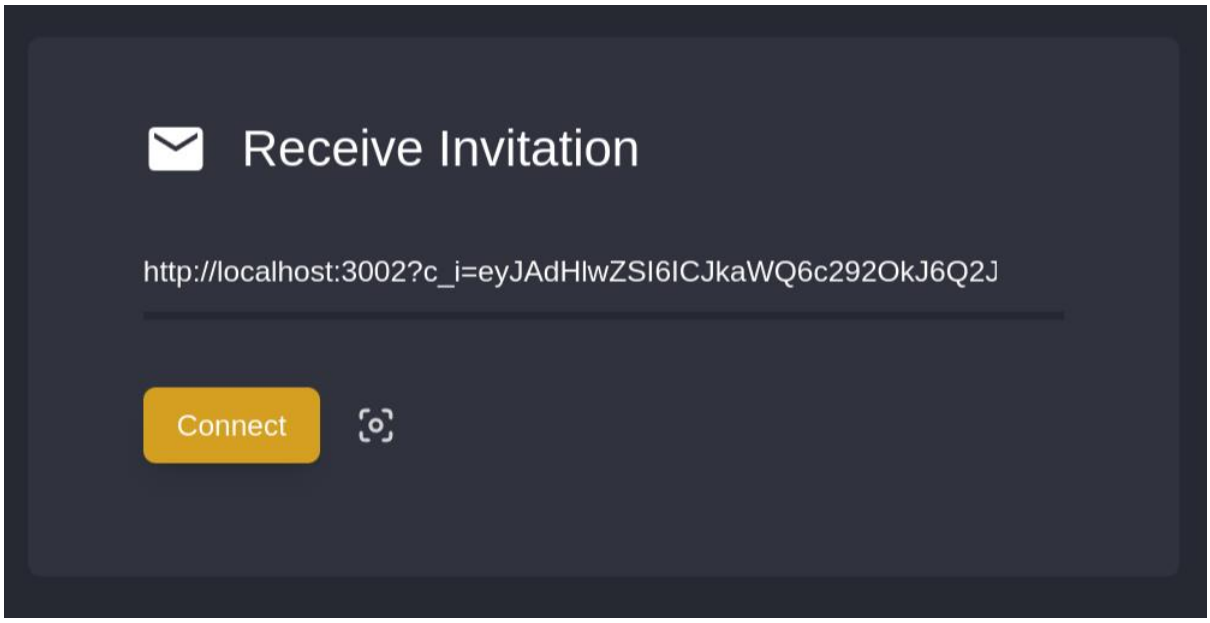


Σχήμα 53: η καρτέλα των συνδέσεων του φοιτητή, πρώτού συνδεθεί με κάποιον

Στην περίπτωση μας, ο φοιτητής εισάγει τον σύνδεσμο πρόσκλησης στο πεδίο Receive Invitation, και πατάει το κουμπί Connect. Παρ ‘όλο που η διαδικασία είναι φαινομενικά εύκολη, μία σειρά από ενέργειες λαμβάνουν μέρος στους εξυπηρετητές και στους πράκτορες των οντοτήτων. Συγκεκριμένα, σύμφωνα με το Aries RFC 0160[8]), πραγματοποιούνται τα εξής βήματα:

1) Ο φοιτητής εισάγει τον σύνδεσμο στο γραφικό του περιβάλλον. Ο εξυπηρετητής του φοιτητή κάνει ένα HTTP request με μέθοδο POST στον πράκτορα του, έχοντας ως περιεχόμενο την πρόσκληση. Έτσι, δημιουργείται και για τον φοιτητή μία σύνδεση, η οποία λαμβάνει ένα μοναδικό αναγνωριστικό.
2) Ο φοιτητής δέχεται την σύνδεση. Στην περίπτωση μας, αυτό δεν φαίνεται στο γραφικό περιβάλλον, αφού είναι μία διαδικασία που εκτελεί ο εξυπηρετητής του φοιτητή. Ειδικότερα, ο εξυπηρετητής κάνει ένα HTTP request με μέθοδο POST στο μονοπάτι /connections/{id}/accept-invitation του πράκτορα του, όπου ως {id} εισάγεται το μοναδικό αναγνωριστικό της σύνδεσης από το προηγούμενο βήμα. Ύστερα, ο πράκτορας του φοιτητή ζητάει από τον πράκτορα του πανεπιστημίου να συνδεθεί.
3) Ο πράκτορας του πανεπιστημίου λαμβάνει την αίτηση για σύνδεση και είναι η σειρά του να αποδεχτεί. Αυτό γίνεται εφικτό κάνοντας ένα HTTP request μέθοδο POST στο μονοπάτι /connections/{id}/accept-request, όπου {id} είναι το μοναδικό αναγνωριστικό της σύνδεσης για τον πράκτορα του πανεπιστημίου. Να σημειωθεί ότι ο κάθε πράκτορας έχει διαφορετικό μοναδικό αναγνωριστικό για την σύνδεση.
4) Ύστερα ο πράκτορας του πανεπιστημίου ενημερώνει τον πράκτορα του φοιτητή ότι έχει αποδεχτεί και η σύνδεση εδραιώνεται.

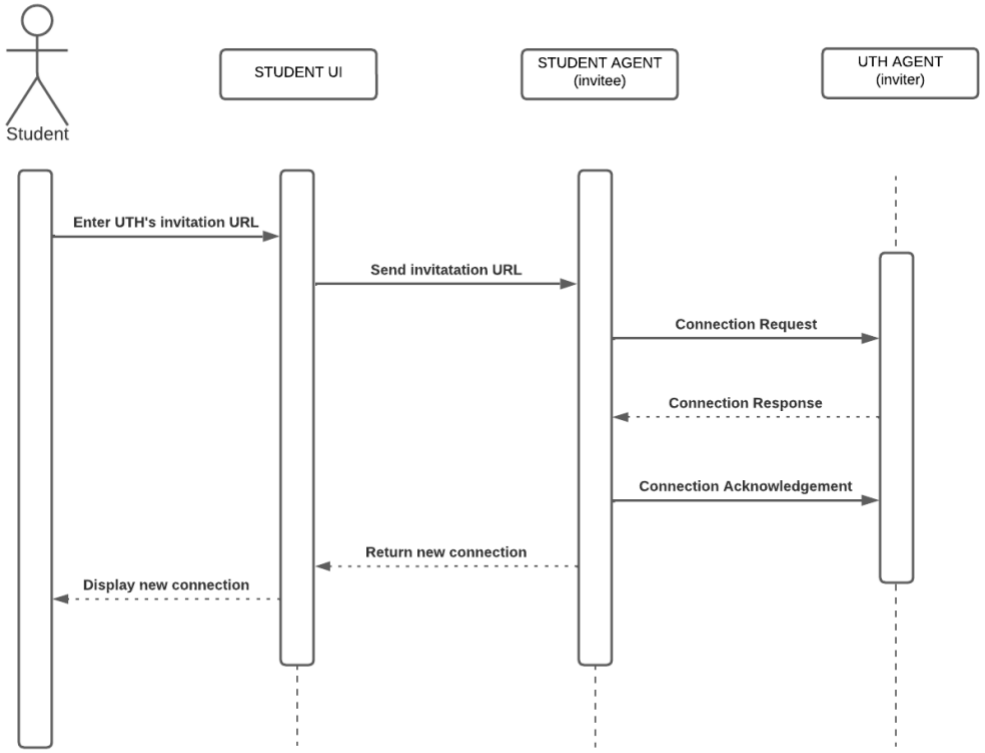
Η παραπάνω διαδικασία φαίνεται και στο διάγραμμα ακολουθίας στο σχήμα 23.



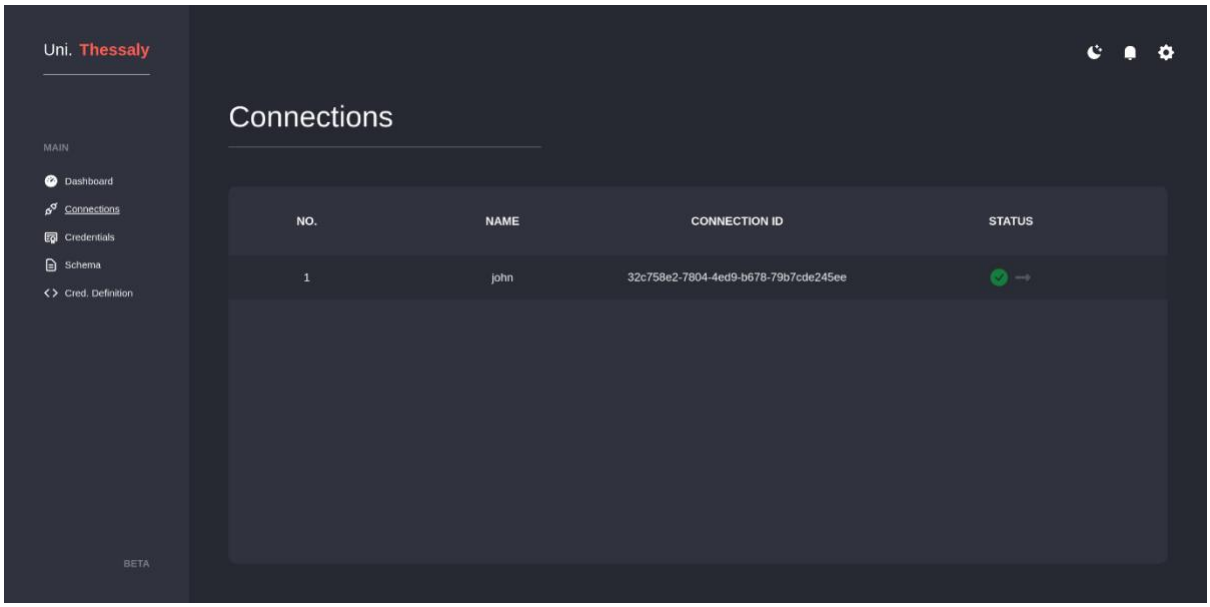
Σχήμα 54: ο φοιτητής τοποθετεί τον σύνδεση πρόσκλησης του πανεπιστημίου

Αφού πραγματοποιηθούν οι παραπάνω ενέργειες από τους εξυπηρετητές, παρατηρούμε ότι η στήλη της κατάσταση για την σύνδεση έχει αλλάξει και υποδεικνύει ότι η σύνδεση έχει εδραιωθεί.

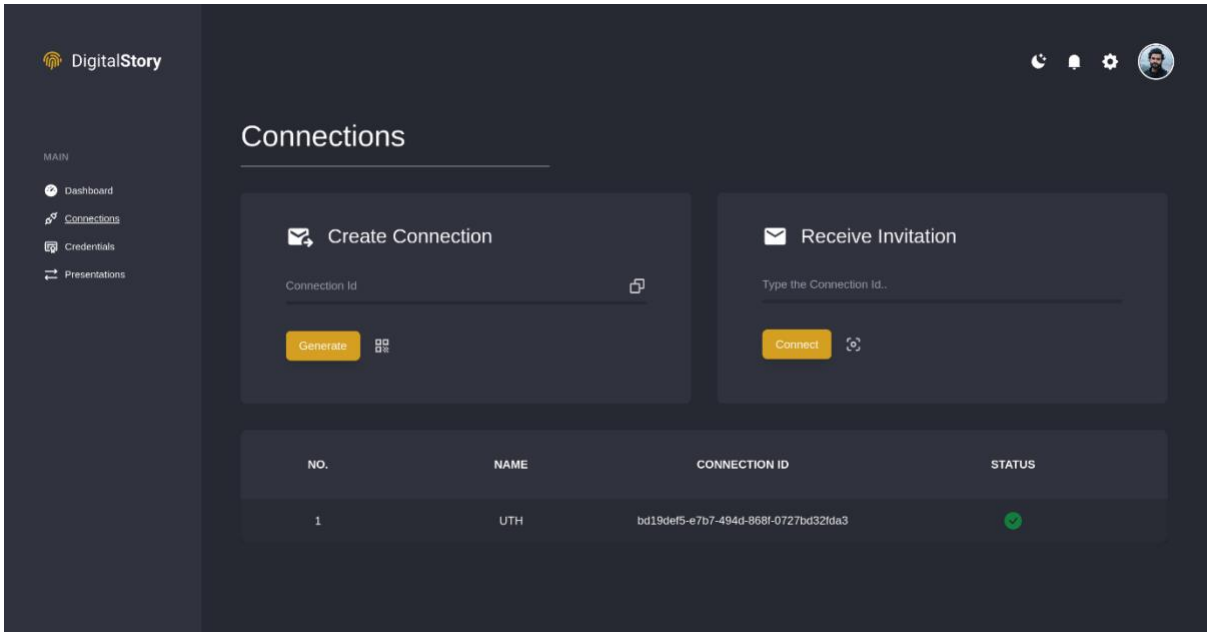
ς[8] https://github.com/hyperledger/aries-rfcs/blob/main/features/0160-connection-protocol/README.md



Σχήμα 55: διάγραμμα ακολουθίας δημιουργίας σύνδεσης μεταξύ φοιτητή και πανεπιστημίου

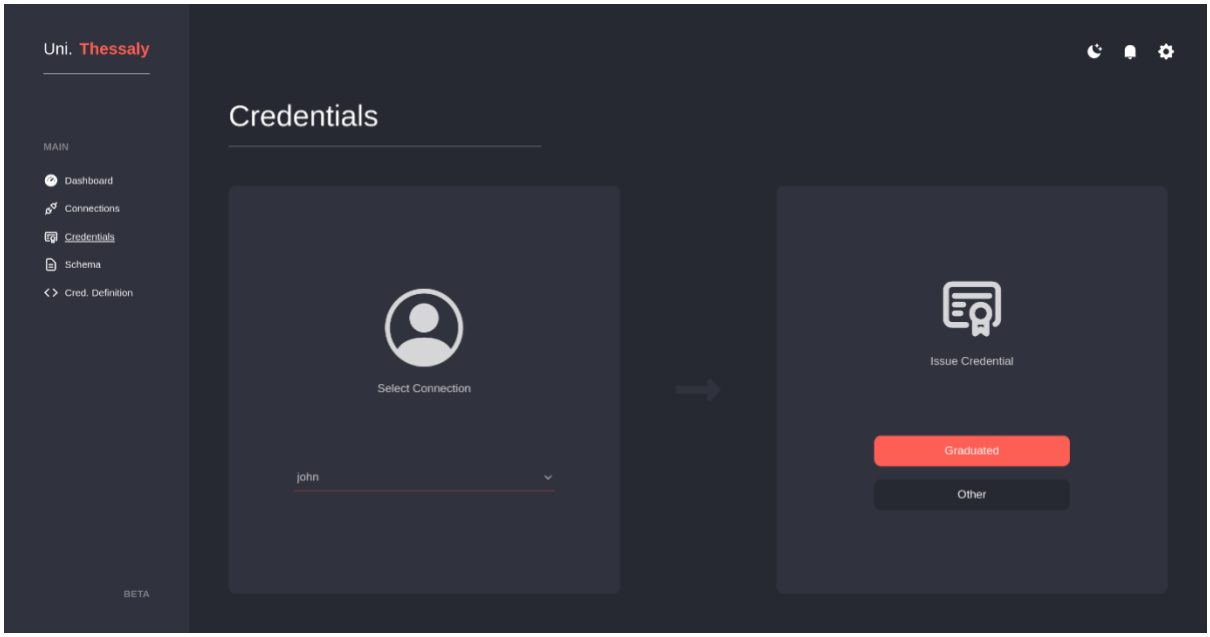


Σχήμα 56: η καρτέλα των συνδέσεων του πανεπιστημίου, αφού συνδεθεί ο φοιτητής



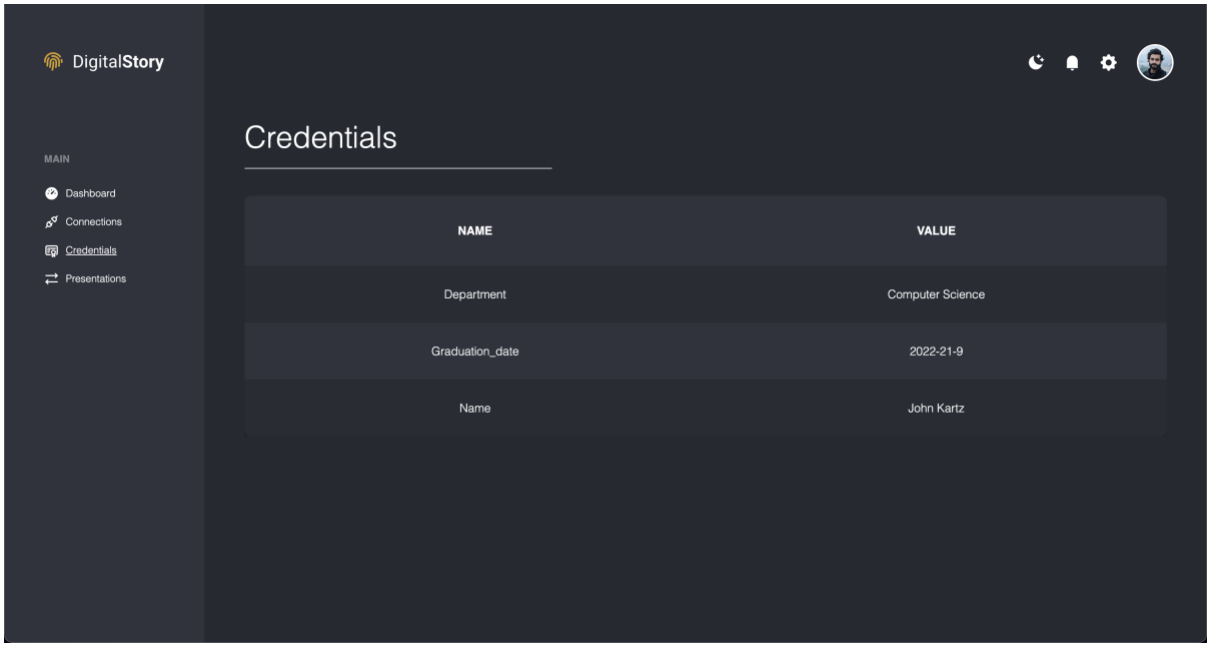
Σχήμα 57: η καρτέλα των συνδέσεων του φοιτητή, αφού εισάγει τον σύνδεσμο πρόσκλησης από το πανεπιστήμιο

Αυτό που μένει είναι το πανεπιστήμιο να εκδώσει το πτυχίο στον φοιτητή. Αυτό συμβαίνει από το διαχειριστικό του UTH, και συγκεκριμένα στην καρτέλα Credentials. Στην αριστερή στήλη επιλέγει ένας διαχειριστής μία ενεργή σύνδεση με κάποιον φοιτητή και στην δεξιά στήλη αναθέτει το πτυχίο πατώντας το κουμπί Graduated.



Σχήμα 58: το πανεπιστήμιο αναθέτει στον φοιτητή το πτυχίο

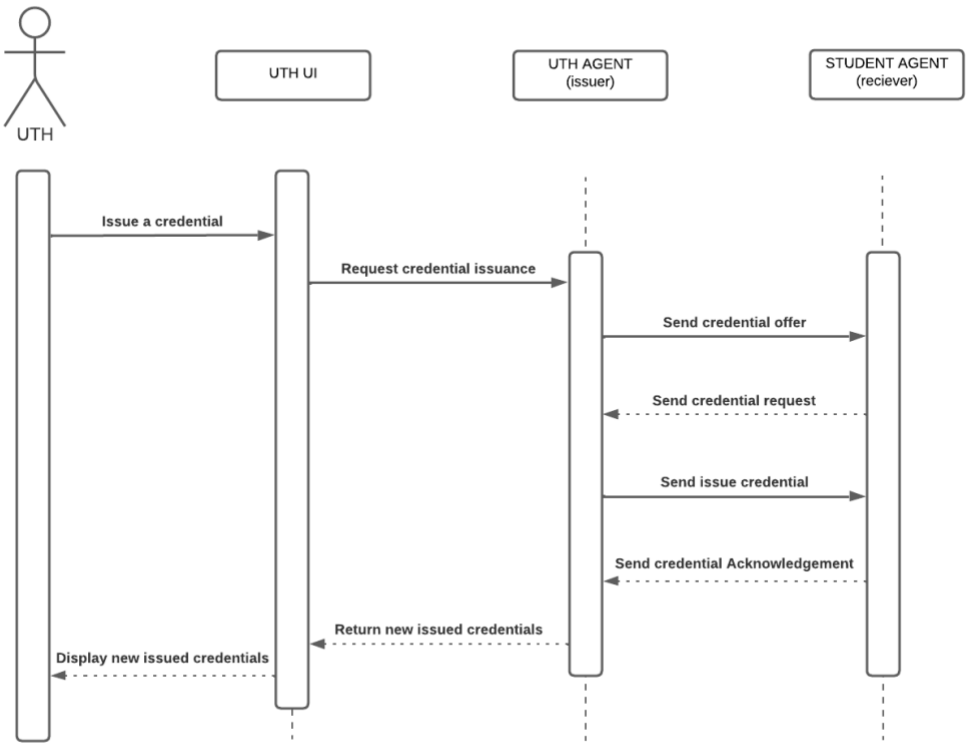
Από την πλευρά του φοιτητή, όταν του εκδοθεί το πτυχίο, στην καρτέλα Credentials μπορεί να δει τα στοιχεία που του έχουνε ανατεθεί. Στην περίπτωση μας, ο φοιτητής έχει λάβει κάποιες ιδιότητες από το πανεπιστήμιο. Να σημειωθεί πως αυτές τις τιμές το πανεπιστήμιο θα μπορούσε να τις είχε αποθηκευμένες σε μία βάση δεδομένων, όπως επίσης θα μπορούσε να είχε και περισσότερες ιδιότητες (βαθμός πτυχίου, διάρκεια φοίτησης, κ.λπ.).



Σχήμα 59: η καρτέλα των διαπιστευτηρίων του φοιτητή

Η διαδικασία με την οποία το πανεπιστήμιο αναθέτει τις ιδιότητες σε ένα φοιτητή είναι η εξής:

1. Ο εκδότης κάνει μια προσφορά στον κάτοχο που θέλει να αναθέσει τις ιδιότητες.
2. Ο κάτοχος βλέπει την προσφορά και στέλνει μια αίτηση στον εκδότη.
3. Ο εκδότης στέλνει τις ιδιότητες στον κάτοχο.
4. Ο κάτοχος στέλνει επιβεβαίωση ότι έχει λάβει τις ιδιότητες.

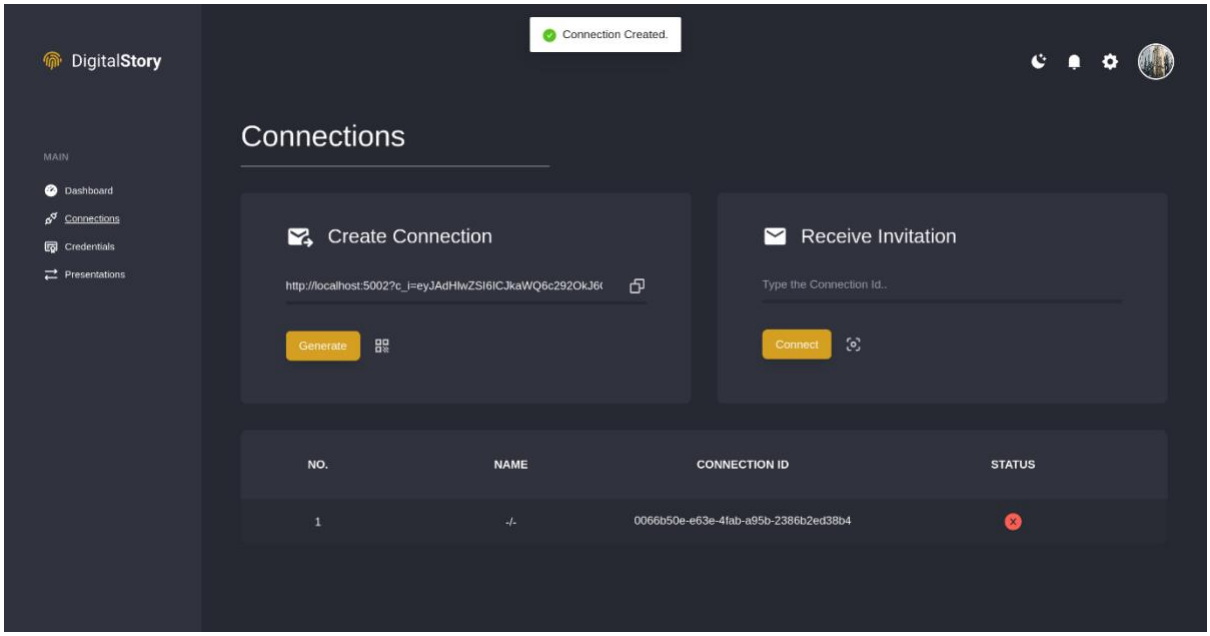


Σχήμα 60: διάγραμμα ακολουθίας ανάθεσης διαπιστευτηρίου

Αλληλεπίδραση φοιτητή με οργανισμό 4.3.2

Η αλληλεπίδραση μεταξύ του φοιτητή και του οργανισμού αποτελείται από δύο μέρη. Στο πρώτο κομμάτι οι δυο οντότητες δημιουργούν μια καινούργια σύνδεση μεταξύ τους και στο δεύτερο, ο οργανισμός επικυρώνει τις ήδη υπάρχουσες ιδιότητες του φοιτητή.

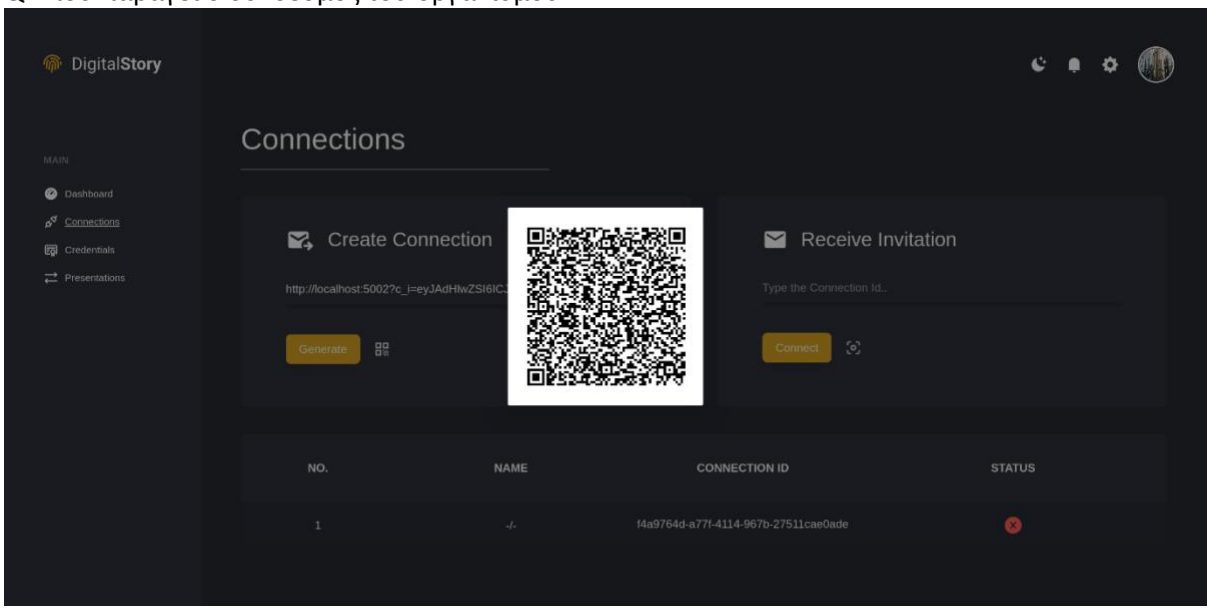
Για να πάρει μέρος η σύνδεση μεταξύ του φοιτητή και οργανισμού, μια από τις δυο οντότητες θα πρέπει να μεταβεί στην καρτέλα Connections του διαχειριστικού του. Στην συνέχεια, πατάει το κουμπί Generate, ούτως ώστε να ξεκινήσει μια καινούργια σύνδεση.



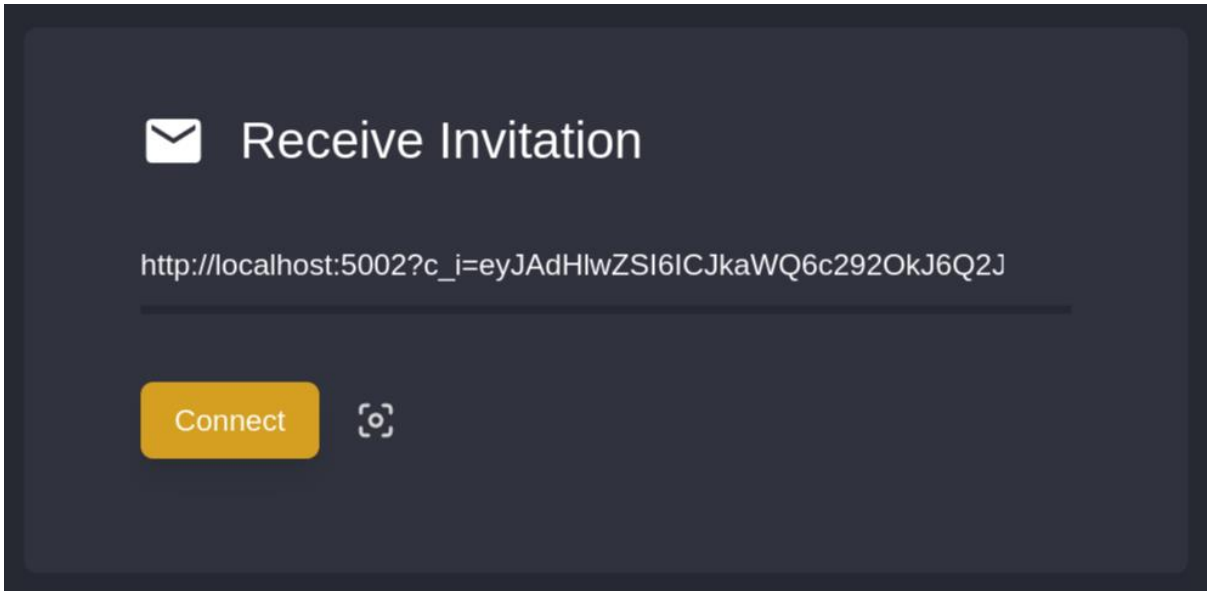
Σχήμα 61: ο οργανισμός δημιουργεί έναν σύνδεσμο πρόσκλησης για τον φοιτητή

Πιο αναλυτικά, στην παραπάνω εικόνα ο οργανισμός για να κάνει μια καινούργια σύνδεση με τον φοιτητή θα πρέπει να πατήσει το κουμπί Generate. Πατώντας το κουμπί αυτό δημιουργείτε ένας σύνδεσμος στον οποίο ο θα πρέπει να τοποθετήσει την φόρμα Receive Invitation. Η σύνδεση έχει ξεκινήσει παρόλα αυτά η στήλη της κατάστασης αναδεικνύει ότι δεν έχει εδραιωθεί.

Υπάρχουν δυο τρόποι με τους οποίος ο φοιτητής θα μπορέσει να επικυρώσει την σύνδεση του οργανισμού. Ο πρώτος έχει ήδη αναφερθεί, ο φοιτητής παίρνει τον σύνδεσμο που παρήγαγε ο οργανισμός και τον τοποθετεί στο Receive Invitation. Ο δεύτερος τρόπος είναι να σκανάρει το κωδικό QR που παράγει ο σύνδεσμος του οργανισμού. ΓΡΑΨΕ ΕΔΩ ΑΛΕΞ

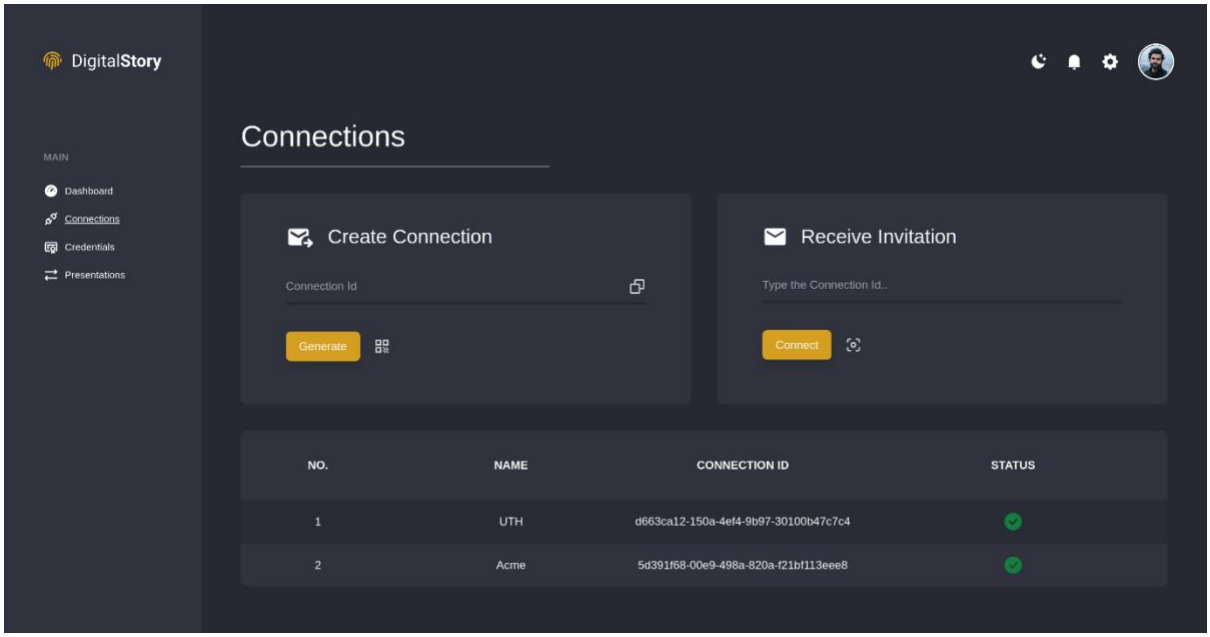


Σχήμα 62: ο σύνδεσμος πρόσκλησης του οργανισμού ως QR-code



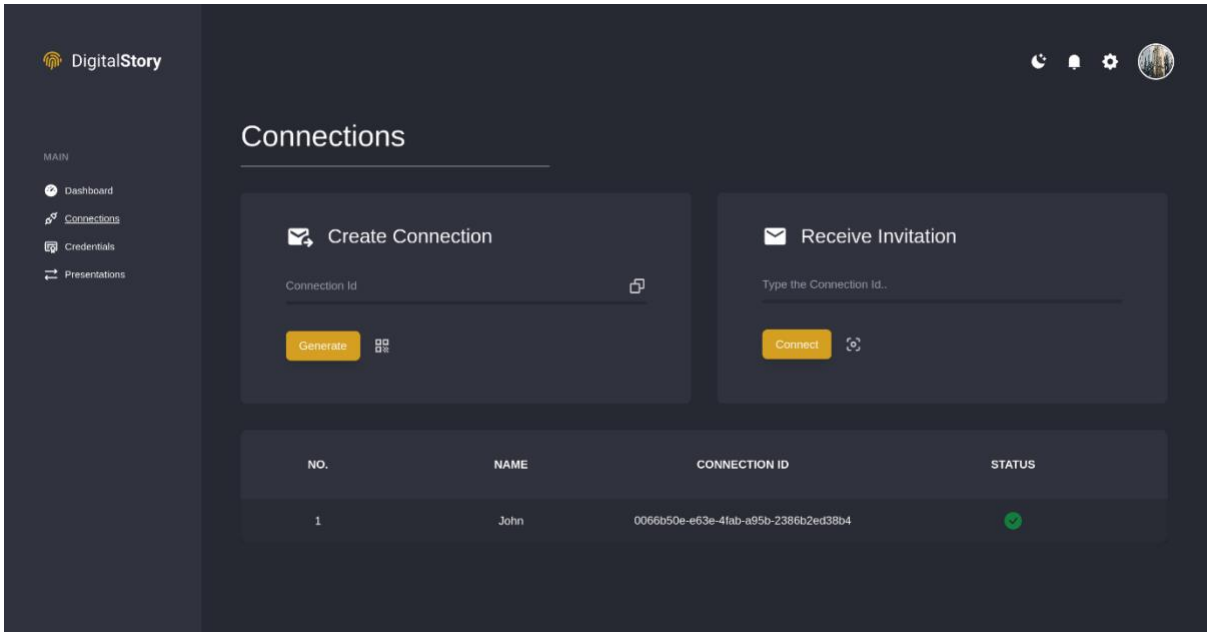
Σχήμα 63: ο φοιτητής εισάγει τον σύνδεσμο πρόσκλησης που έχει λάβει από τον οργανισμό

Εφόσον η ο φοιτητής συνδεθεί με τον οργανισμό, στην στήλη της κατάστασης θα εμφανιστεί μια ένδειξη η οποία θα παραπέμπει στην επιτυχημένη εδραίωση της σύνδεσης μεταξύ των δύο.



Σχήμα 64: η καρτέλα των συνδέσεων του φοιτητή, αφού εισάγει τον σύνδεσμο πρόσκλησης από τον οργανισμό

Αντίστοιχα, στο διαχειριστικό του οργανισμού θα αναφερθεί ότι η σύνδεση με τον φοιτητή έχει εδραιωθεί.

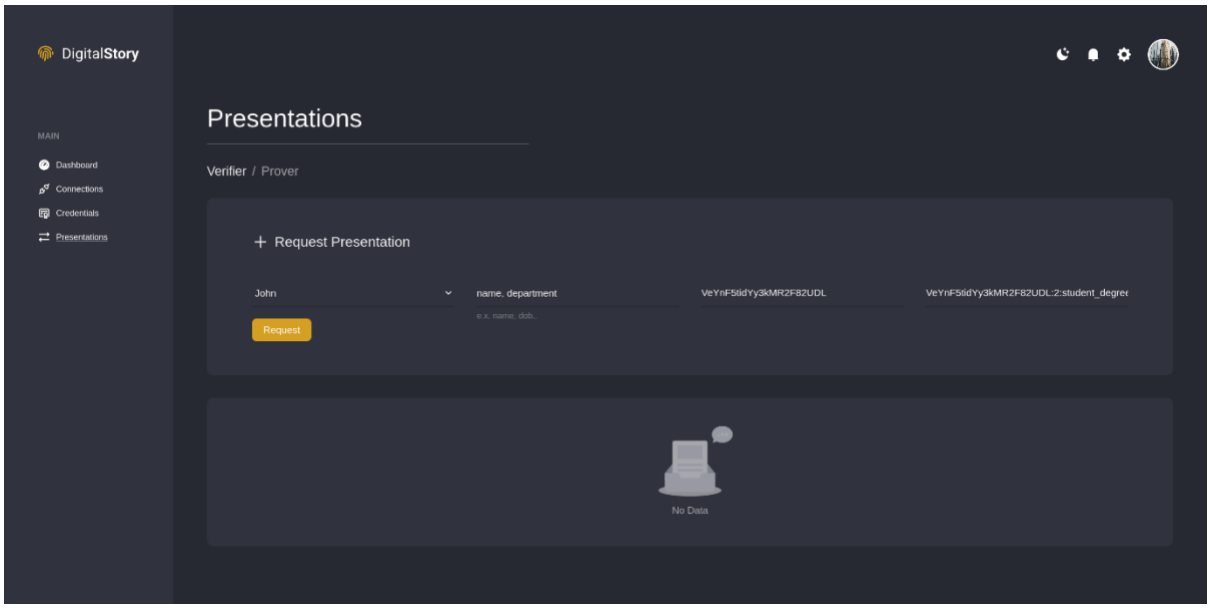


Σχήμα 65: η καρτέλα των συνδέσεων του οργανισμού, αφού ο φοιτητής εισάγει τον σύνδεσμο πρόσκλησης

Στο επόμενό κομμάτι ο οργανισμός κάνει μια αίτηση στον φοιτητή, ούτως ώστε να εξάγει κάποιες χρήσιμες ιδιότητες από αυτόν. Για να το καταφέρει αυτό, θα πρέπει να κάνει μια αίτηση στον φοιτητή ζητώντας ποιες ιδιότητες θα ήθελε να του αποκαλύψει.

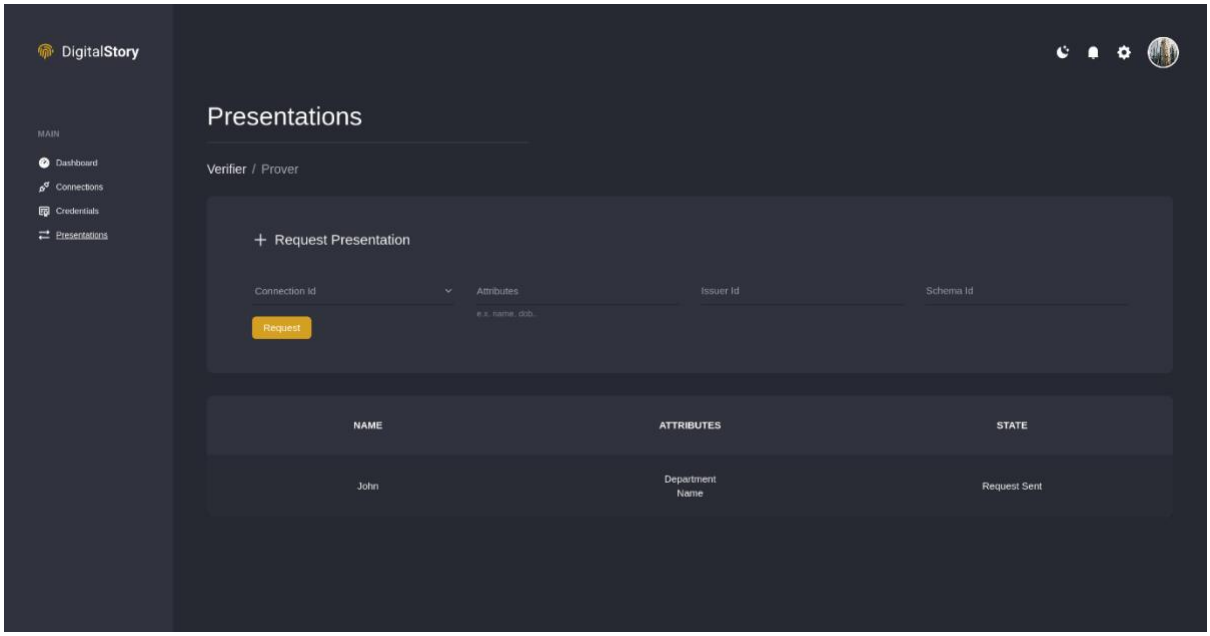
Πιο αναλυτικά, ο οργανισμός πρέπει να μεταβεί στην καρτέλα Presentations/Verifier του διαχειριστικού του και να τοποθετήσει:

1. Την σύνδεση στην οποία θέλει να κάνει την αίτηση.
2. Τις ιδιότητες που θέλει να πάρει.
3. Το αναγνωριστικό του εκδότη.
4. Το αναγνωριστικό του σχήματος



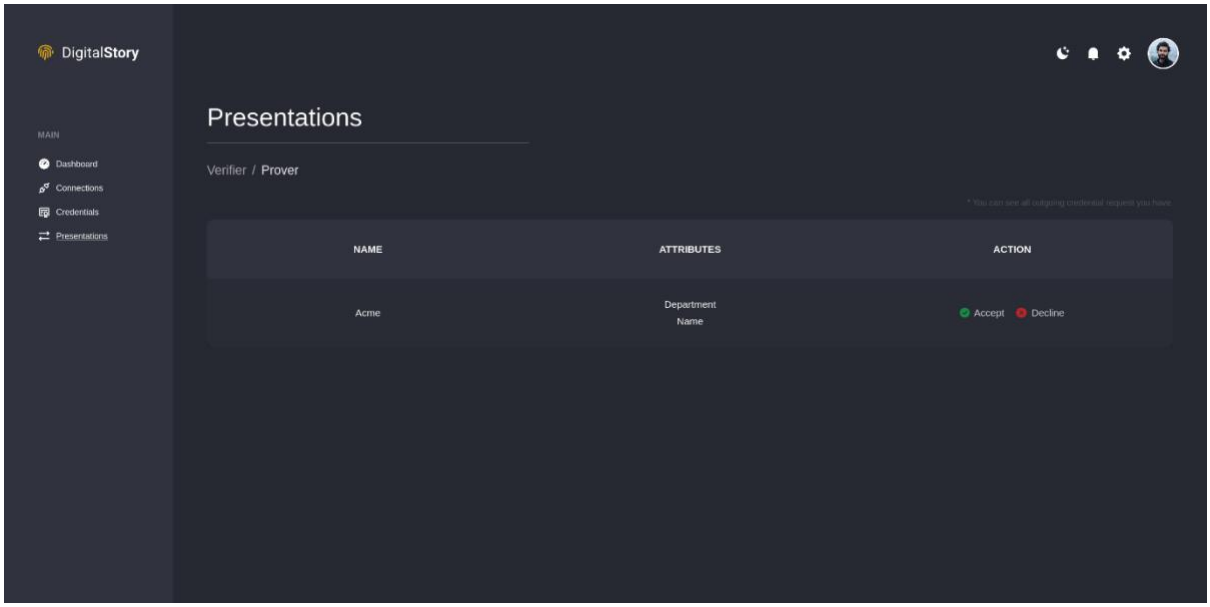
Σχήμα 66: ο οργανισμός δημιουργεί μία αίτηση επαληθεύσιμης παρουσίασης για τον φοιτητή

Μόλις τοποθετήσει τα απαιτούμενα πεδία και πατήσει το κουμπί Request, θα εμφανιστεί ένα καινούργιο έγγραφο με το όνομα της σύνδεσης, τις ιδιότητες που ζητούνται και την κατάσταση της αίτησης.



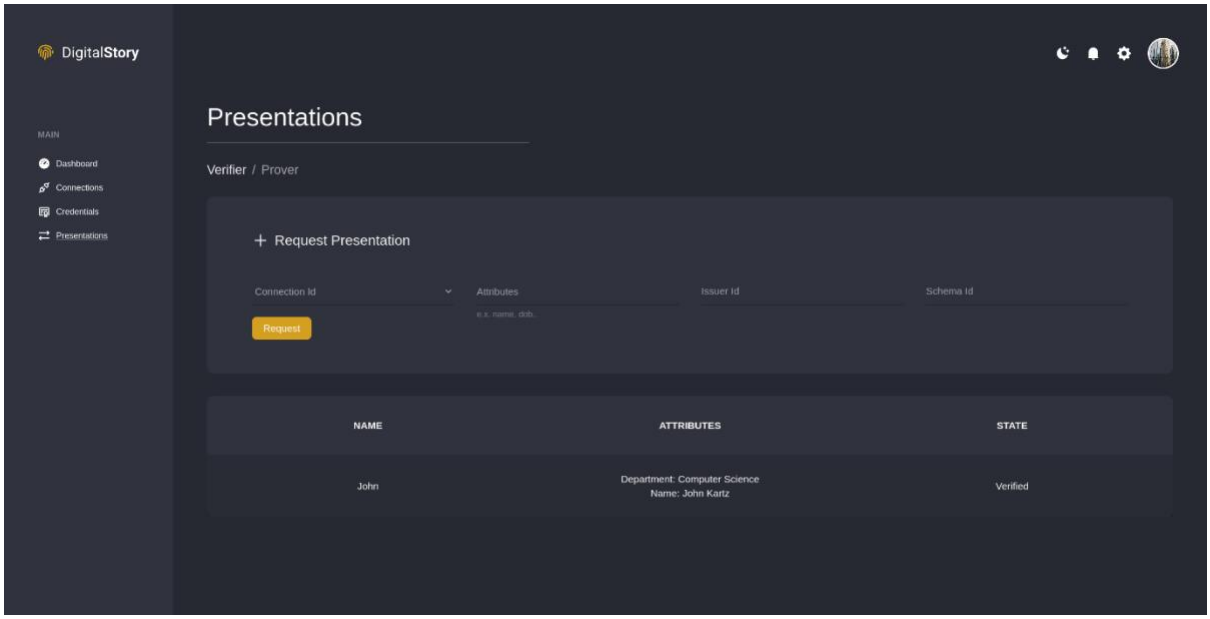
Σχήμα 67: η καρτέλα των παρουσιάσεων του οργανισμού, αφού αποστείλει την αίτηση στον φοιτητή

Εφόσον ο οργανισμός έχει στείλει την αίτηση στον φοιτητή, ο φοιτητής θα πρέπει να μεταβεί στην καρτέλα Presentation/Prover του διαχειριστικού του. Στην καρτέλα αυτή μπορεί να δει όλα του τα αιτήματα που εκκρεμούν την παρούσα στιγμή. Για να στείλει τις ιδιότητες του θα πρέπει να πατήσει το κουμπί Accept. Μόλις το πατήσει, τα στοιχεία του θα σταλούν αυτόματα στον οργανισμό.



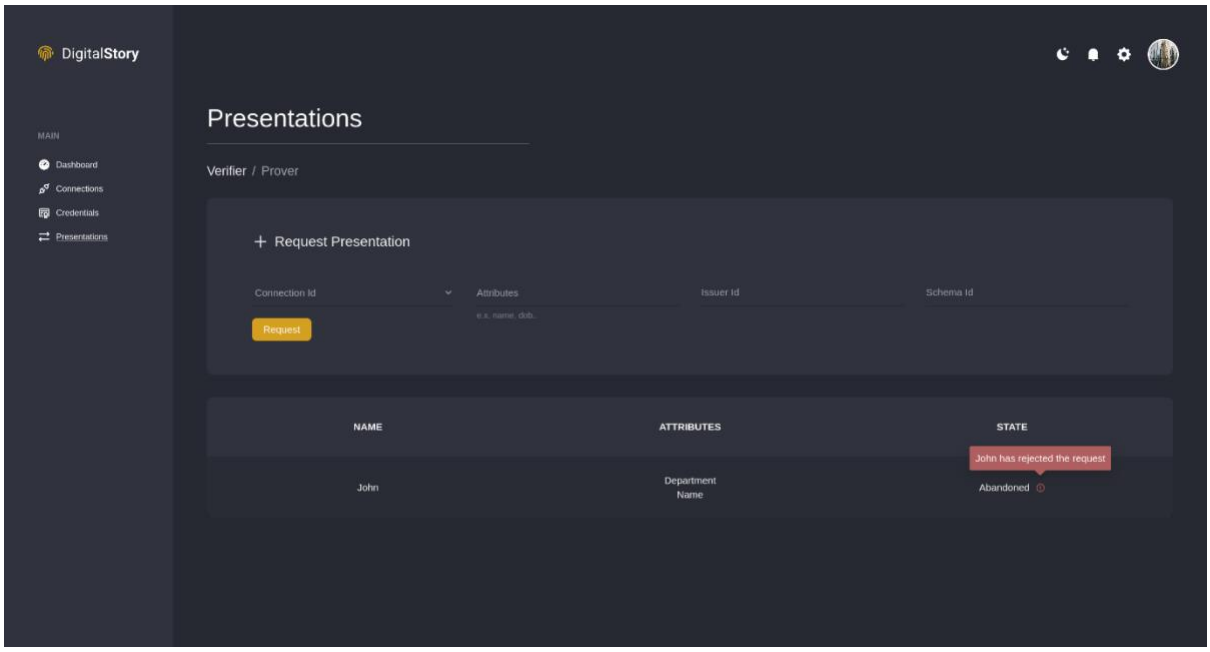
Σχήμα 68: η καρτέλα των αιτήσεων του φοιτητή, αφού αιτηθεί ο οργανισμός

Μετά την αποδοχή της αίτησης από τον φοιτητή, ο οργανισμός μπορεί να δει τις ιδιότητες που έχει ζητήσει. Αυτό μπορεί να το κάνει στην καρτέλα του Presentation/Prover. Επίσης στην στήλη της κατάστασης θα υπάρχει μια ένδειξή η οποία θα παραπέμπει ότι η αίτηση έχει πετύχει.



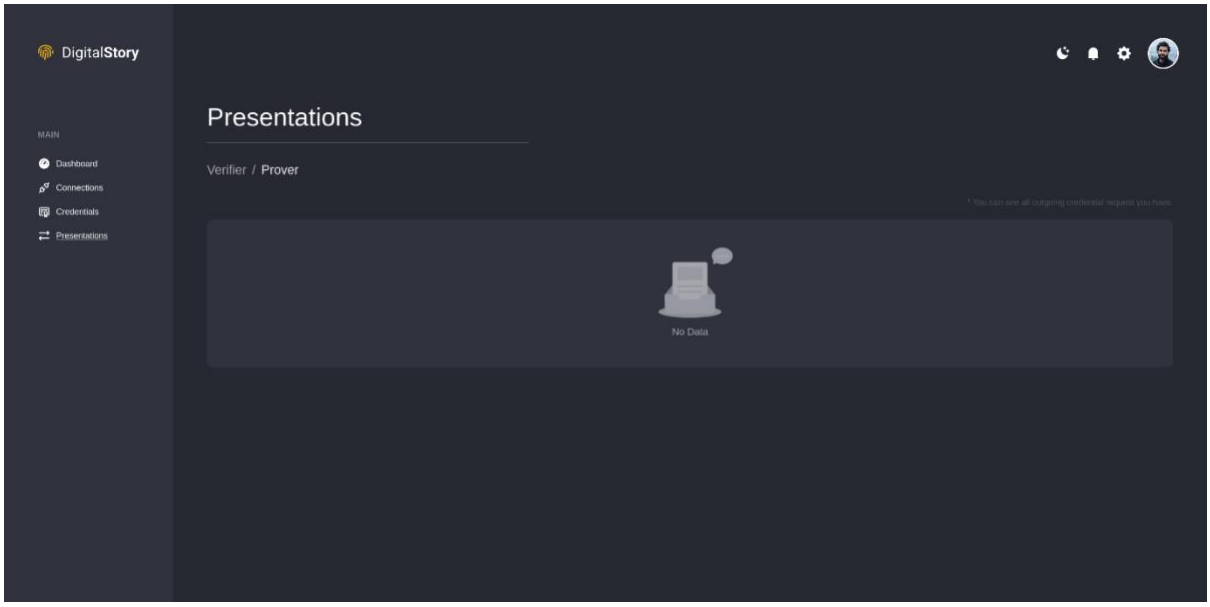
Σχήμα 69: η καρτέλα παρουσιάσεων του οργανισμού, αφού δεχτεί ο φοιτητής

Από την άλλη, αν ο φοιτητής αρνηθεί την αίτηση (π.χ. ο οργανισμός έχει ζητήσει περισσότερες ιδιότητες απ' ότι ο φοιτητής θα ήθελε να μοιραστεί), η κατάσταση της αίτηση μεταβαίνει σε Abandoned.



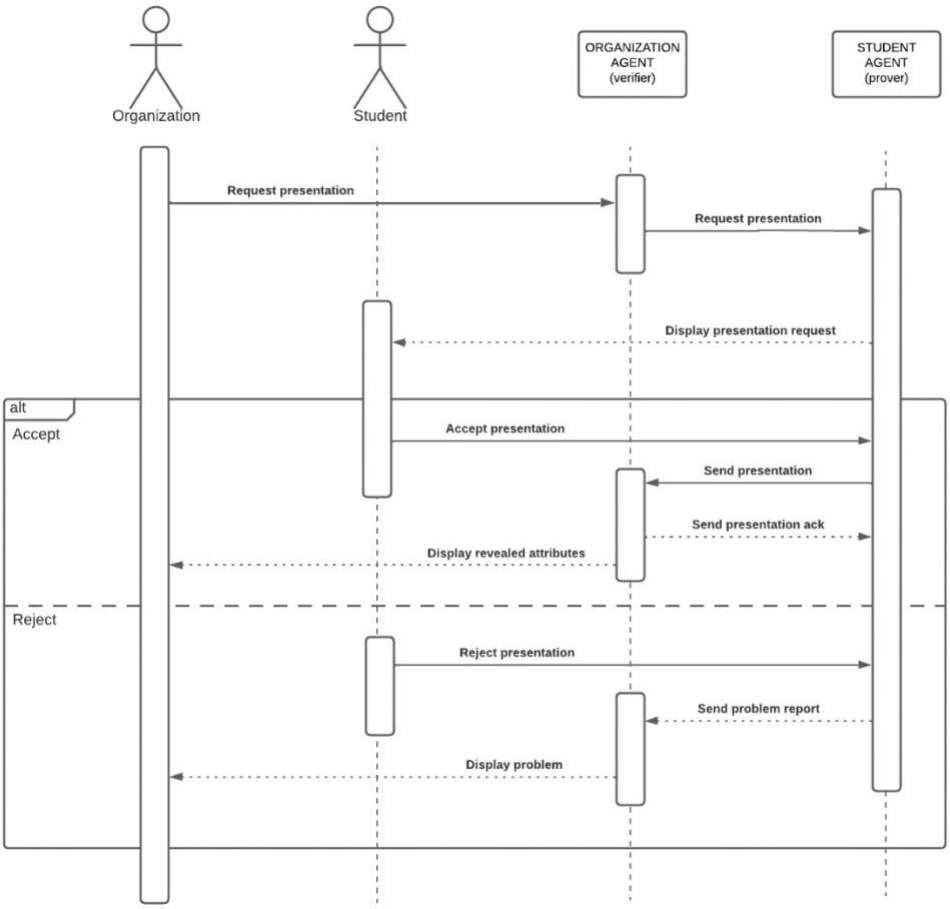
Σχήμα 70: η καρτέλα παρουσιάσεων του οργανισμού, αφού αρνηθεί ο φοιτητής

Τέλος στην καρτέλα Presentation/Prover του φοιτητή η εγγραφή με την αίτηση του οργανισμού έχει εξαφανιστεί.



Σχήμα 71: η καρτέλα παρουσιάσεων του φοιτητή, αφού δεχτεί ή αρνηθεί την αίτηση

Όπως παρατηρούμε μία παρουσίαση απαιτεί ιδιότητες και όχι διαπιστευτήρια. Στην περίπτωση του φοιτητή, το διαπιστευτήριο που έλαβε από το πανεπιστήμιο περιείχε και την ημερομηνία αποφοίτησης, όμως ο οργανισμός αιτήθηκε μόνο για το όνομα και το τμήμα.



Σχήμα 72: διάγραμμα ακολουθίας παρουσίασης

ΚΕΦΑΛΑΙΟ 5: ΣΥΜΠΕΡΑΡΜΑΤΑ

Η αυτοδιαχειριζόμενη ταυτότητα είναι η προσπάθεια ψηφιοποίησης της ταυτότητας, στην οποία υποστηρίζεται ότι κάποιος πρέπει να έχει πλήρη έλεγχο των δεδομένων του, χωρίς να χρειάζεται παρέμβαση από κυβερνητικές αρχές. Για να γίνει αυτό εφικτό, χρειάστηκαν νέα πρωτόκολλα, ιδέες και μηχανισμοί. Αρχικά, ορίστηκαν τρεις κύριες οντότητες ως συμμετέχοντες ενός τέτοιου συστήματος ο κάτοχος, ο εκδότης και ο επαληθευτής. Η σχέση μεταξύ των οντοτήτων σχηματίζει το τρίγωνο εμπιστοσύνης, όπως ακριβώς και στον πραγματικό κόσμο. Φυσικά, η επικοινωνία μεταξύ τους πρέπει να είναι ομότιμη, κάτι το οποίο οδήγησε στην ανάγκη δημιουργίας των αποκεντρωμένων αναγνωριστικών, και κατά συνέπεια των αποκεντρωμένων εγγράφων. Ύστερα, πέρα από την μοναδική αναγνώριση της εκάστοτέ οντότητας, απαραίτητη κρίνεται και η ύπαρξη μίας κατανεμημένης δομής δημοσίου κλειδιού, ώστε να μπορούν τα μέλη του συστήματος να ανταλλάσσουν κρυπτογραφικά κλειδιά, με το blockchain να είναι η πιο διάσημη λύση προς το παρών. Στην συνέχεια, για την αναπαράσταση των διαπιστευτηρίων, αναπτύχθηκε ένα νέο ανοιχτό πρότυπο, τα επαληθεύσιμα διαπιστευτήριά, τα οποία μπορούν να επαληθευτούν κρυπτογραφικά, χωρίς την ανάγκη της παρουσίας του εκδότη.

Όλες οι παραπάνω τεχνολογίες είναι ανεξάρτητες μεταξύ τους. Για την υλοποίηση της αποκεντρωμένης ταυτότητας αναπτύχθηκε ένα μοντέλο (Trust over IP model, ToIP), το οποίο σύλλεξε και ενοποίησε τα απαραίτητα δομικά στοιχεία κατατάσσοντας τα σε τέσσερα διαφορετικά επίπεδα. Κάθε ένα επίπεδο του μοντέλου ταυτότητας αποτελείται από δύο διαφορετικά μέρη, το τεχνολογικό και το κυβερνητικό μέρος.

Στην εργασία αυτή αναπτύχθηκε ένα κατανεμημένο σύστημα αυτοδιαχειριζόμενης ταυτότητας, στο οποίο καλύφθηκαν οι ελάχιστες περιπτώσεις χρήσης. Βασικός στόχος του συστήματος αυτού είναι η ανάδειξη των δυνατοτήτων ενός συστήματος SSI, χρησιμοποιώντας την ήδη υπάρχουσα κεντρικοποιημένη δομή, με την βοήθεια μιας πανεπιστημιακής αρχής, ενός φοιτητή και ενός οργανισμού. Για την υλοποίηση της χρησιμοποιήθηκαν οι τεχνολογίες Hyperledger.

Το όραμα της αποκεντρωμένης ταυτότητας είναι εξαιρετικά μεγάλο, με πολλούς ανθρώπους μέρα με την μέρα να ανακαλύπτουν καινούργιες ιδέες και νέες λύσεις στα προβλήματα που αντιμετωπίζει. Στον σύγχρονο μας κόσμο η ιδέα της ιδιωτικότητα των δεδομένων όλο ένα και μεγαλώνει, κάνοντας την αυτοδιαχειριζόμενη ταυτότητα περισσότερο ελκυστική. Για να υιοθετηθεί όμως από το ευρύτερο κοινό, θα πρέπει αρχικά να αρχίσουν να χρησιμοποιούν την αυτοδιαχειριζόμενη ταυτότητα μεγαλύτεροι φορείς (το κράτος, πάροχοι τηλεπικοινωνιών, πάροχοι ηλεκτρικού ρεύματος, κλπ.), ώστε να δρουν ως άγκυρες εμπιστοσύνης για τους υπόλοιπους παρόχους υπηρεσιών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] K. Cameron, «identityblog.com,» [Ηλεκτρονικό]. Available: https://www.identityblog.com/?p=352.

[2] C. s. organisations, «malaysiakini.com,» [Ηλεκτρονικό]. Available: https://www.malaysiakini.com/letters/411314.

[3] M. J. H. Jim Isaak, «User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection,» *Computer,* pp. 56-59, 2018.

[4] T. Ruff, «medium.com,» [Ηλεκτρονικό]. Available: https://medium.com/evernym/the-three-models-of-digital-identity-relationships-ca0727cb5186.

[5] S. Nakamoto, «bitcoin.org,» 2008. [Ηλεκτρονικό]. Available: https://bitcoin.org/bitcoin.pdf.

[6] E. org, «ethereum.org,» [Ηλεκτρονικό]. Available: https://ethereum.org/en/whitepaper/.

[7] H. org, «https://hyperledger-fabric.readthedocs.io/,» [Ηλεκτρονικό]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/whatis.html.

[8] W3C, «w3.org,» [Ηλεκτρονικό]. Available: https://www.w3.org/TR/vc-data-model/.

[9] A. Andrade-Walz, «evernym.com,» [Ηλεκτρονικό]. Available: https://www.evernym.com/blog/what-are-decentralized-identifiers-dids/.

[10] W3C, «w3.org,» [Ηλεκτρονικό]. Available: https://www.w3.org/TR/did-core/.

[11] A. Johnson, «trinsic.id,» [Ηλεκτρονικό]. Available: https://trinsic.id/what-are-ssi-digital-wallets/.

[12] A. Doerk, «ssi-ambassador.medium.com,» [Ηλεκτρονικό]. Available: https://ssi-ambassador.medium.com/digital-identity-wallet-a-place-for-your-self-sovereign-identity-5dfbd3d48a74.

[13] Sovrin, «sovrin.org,» [Ηλεκτρονικό]. Available: https://sovrin.org/taking-the-sovrin-foundation-to-a-higher-level-introducing-ssi-as-a-universal-service/.

[14] W3C, «identity.foundation,» [Ηλεκτρονικό]. Available: https://identity.foundation/peer-did-method-spec/.

[15] T. O. I. Foundation, «trustoverip.org,» [Ηλεκτρονικό]. Available: https://trustoverip.org/wp-content/uploads/2020/05/toip_introduction_050520.pdf.