Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«ΠΜΣ Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Αυτοδιαχειριζόμενες Ταυτότητες με τη χρήση του οικοσυστήματος Hyperledger** **Self-Sovereign Identities using the Hyperledger ecosystem**
Ονοματεπώνυμο Φοιτητή	**Λοΐζος Εμμανουήλ**
Πατρώνυμο	**Νικόλαος**
Αριθμός Μητρώου	**ΜΠΠΛ18043**
Επιβλέπων	**Πατσάκης Κωνσταντίνος, Αναπληρωτής καθηγητής**

Ημερομηνία Παράδοσης **Δεκέμβριος 2022**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Κωνσταντίνος Πατσάκης Αναπληρωτής Καθηγητής	Ευθύμιος Αλέπης Αναπληρωτής καθηγητής	Ευάγγελος Σακκόπουλος Αναπληρωτής Καθηγητής

Ευχαριστίες

Αρχικά θα ήθελα να ευχαριστήσω τον αναπληρωτή καθηγητή κ. Κωνσταντίνο Πατσάκη για την εμπιστοσύνη που μου έδειξε με την ανάθεση της παρούσας διπλωματικής εργασίας και την άριστη συνεργασία κατά τη διάρκεια εκπόνησης της. Στη συνέχεια, θα ήθελα να ευχαριστήσω την οικογένεια και τους φίλους μου για την αδιάκοπη ενθάρρυνση και ψυχολογική στήριξη που μου παρείχαν καθ' όλη τη διάρκεια των σπουδών μου.

Περίληψη

Σε αντίθεση με τα συμβατικά δίκτυα που χρησιμοποιούνται ευρέως, η τεχνολογία Blockchain είναι ένα δίκτυο ομότιμων χρηστών που μπορεί να λειτουργεί χωρίς κεντρική αρχή. Αυτό υποδηλώνει ότι οι κόμβοι σε ένα τέτοιο δίκτυο δεν χρειάζεται να είναι επίσημα εξουσιοδοτημένοι ή επαληθευμένοι από μια κεντρική αρχή προκειμένου να συμμετέχουν σε αυτό. Δεδομένου ότι ολόκληρο το δίκτυο επικυρώνει κάθε συναλλαγή, το δίκτυο θεωρείται δεδομένο ότι είναι αξιόπιστο. Για να επιβάλει την εξουσία του στο δίκτυο, ένας χρήστης θα πρέπει να αποκτήσει τον έλεγχο της πλειοψηφίας των κόμβων, γεγονός που εξασφαλίζει και την εμπιστοσύνη με αυτό τον τρόπο. Η παρούσα μεταπτυχιακή διατριβή αποσκοπεί λοιπόν στην ανάπτυξη ενός συστήματος διαχείρισης αυτοδύναμων ταυτοτήτων (Self Sovereign Identity - SSI), αξιοποιώντας τις δυνατότητες του οικοσυστήματος Hyperledger. Οι χρήστες ενός τέτοιου συστήματος διαχείρισης θα μπορούσαν να επιλέξουν ποια από τα χαρακτηριστικά της ταυτότητάς τους θέλουν να μοιραστούν με συγκεκριμένους παρόχους υπηρεσιών προκειμένου να χρησιμοποιούν τις υπηρεσίες τους.

Abstract

In contrast to conventional, extensively utilized networks, the blockchain is a peer-to-peer network that can operate without a centralized authority. This indicates that the nodes in such a network are not needed to be formally authorized or verified by a centralized authority in order to participate in it. Since the entire network validates every transaction, the network is taken for granted to be reliable. In order to impose his authority on the network, an adversary would need to acquire control of the majority of the nodes, which assures confidence. This master thesis aims to develop a self-sovereign identity management system by utilizing the Hyperledger ecosystem capabilities. Users of such a management system could select which of their identity attributes they want to share with particular service providers in order to use their services.

Συντομογραφίες και Ακρωνύμια

- Client : Αποτελείται από διάφορους τύπους λογισμικού ή υλικού όπως για παράδειγμα ψηφιακά πορτοφόλια, πορτοφόλια λογισμικού κ.α. τα οποία χρησιμοποιούνται για την ανάπτυξη και την διαχείριση αποκεντρωμένων αναγνωριστικών εκ μέρους ενός χρήστη ταυτότητας και για την αποθήκευση των verified credentials που σχετίζονται με τον χρήστη της συγκεκριμένης ταυτότητας.
- Consensus μηχανισμός: είναι ένας μηχανισμός συνεργατικής διαδικασίας που καθορίζει τον τρόπο επίτευξης συναίνεσης μεταξύ όλων των κόμβων του Blockchain και προσδιορίζει την εγκυρότητα των εγγραφών.
- Credential : η αλλιώς διαπιστευτήριο είναι ένα σύνολο με ένα η πολλά Claims που χαρακτηρίζει μία οντότητα.
- Distributed ledger technology / DLT: Τεχνολογία κατανεμημένου καθολικού (Distributed Ledger Technology) – Ένα κατανεμημένο καθολικό (ή κοινόχρηστο καθολικό ή τεχνολογία κατανεμημένου καθολικού) είναι μια συναίνεση των αντιγραμμένων, διαμοιρασμένων και συγχρονισμένων ψηφιακών δεδομένων, τα οποία είναι κατανεμημένα σε περισσότερες τοποθεσίες, χώρες ή οργανισμούς.
- DID: η αλλιώς αποκεντρωμένη ταυτότητα είναι ένας νέος τύπος ταυτοποίησης όπου είναι αυτό-δύναμος (self sovereign), δηλαδή ολοκληρωτικά υπό τον έλεγχο του ιδιοκτήτη της ταυτότητας και μη εξαρτώμενος από ένα κεντρικό σύστημα.
- DKMS(Distributed Key Management Systems):Είναι λογισμικό υπεύθυνο για την διαχείρηση των κλειδιών, των DIDs και άλλων δεδομένων που είναι απαραίτητα για την λειτουργεία του client.
- Nodes: Ένας κόμβος σε μια αλυσίδα Blockchain μπορεί να διενεργεί διάφορες λειτουργίες. Δύναται να επιβεβαιώνει συναλλαγές και να πραγματοποιεί τη διαδικασία της εξόρυξης για να διευκολύνει τη συμφωνία και να διασφαλίσει την αλυσίδα συνήθως μέσω ενός Πρωτοκόλλου συμφωνίας
- Peer-to-peer network: Δίκτυο όπου όλα τα μέρη μπορούν να επικοινωνήσουν μεταξύ τους στέλνοντας και λαμβάνοντας μηνύματα.
- Transaction: Μια συναλλαγή που αναπαριστά μια μεταφορά αξιών από μια διεύθυνση σε μια άλλη.
- Κρυπτονόμισμα: Είναι μία peer-to-peer αποκεντρωμένη ηλεκτρονική μορφή χρήματος η οποία βασίζεται πάνω στις αρχές της κρυπτογραφίας για την διασφάλιση του δικτύου και την επαλήθευση των συναλλαγών

Πίνακας Περιεχομένων

1. Εισαγωγή

1.1. Οργάνωση Εργασίας

Το κείμενο τις εργασίας αυτής είναι χωρισμένο στα απαραίτητα κεφάλαια που χρειάζονται για την κατανόηση και την ανάγκη αξιοποίησης των τεχνολογιών Blockchain καθώς και την δημιουργία συστημάτων διαχείρισης αυτοδύναμης ταυτότητας (Self Sovereing Identity – SSI). Το παρόν κεφάλαιο, λειτουργεί ως μια εισαγωγή στο αντικείμενο της διπλωματικής εργασίας. Στο δεύτερο κεφάλαιο παρουσιάζεται ο ορισμός και μια γενική περιγραφή της τεχνολογίας Blockchain, μία ιστορική αναδρομή στο blockchain, καθώς και τους τομείς που εφαρμόζεται η τεχνολογία αυτή. Το κεφάλαιο 3 περιλαμβάνει το οικοσύστημα Hyperledger όπου παρουσιάζονται τα βασικά χαρακτηριστικά και εργαλεία του καθώς και το περιβάλλον που πρέπει να δημιουργηθεί για την εκτέλεση των blockchain. Επίσης στο κεφάλαιο αυτό παρουσιάζονται τα βασικά στοιχεία και τα πλεονεκτήματα που προσφέρουν δυο από τα δημοφιλέστερα πρότζεκτ του Hyperledger τα οποία είναι το Fabric και το Indy/Aries. Στο τέταρτο κεφάλαιο γίνεται μία ανάλυση του τρόπου λειτουργίας του προγράμματος που δημιουργήθηκε και παρουσιάζονται κάποιες τεχνικές λεπτομέρειες ενώ στο επόμενο κεφάλαιο αναλύσουμε την ανάπτυξη της εφαρμογής. Τέλος στα κεφάλαια έξι και επτά περιλαμβάνονται τα συμπεράσματα που αποκομίσαμε από την εργασία και την μελλοντική εξέλιξη που θα μπορούσε να έχει καθώς και την βιβλιογραφική αναφορά αντίστοιχα.

1.2. Παρουσίαση Προβλήματος

Με την ανάπτυξη της τεχνολογίας Blockchain, το τελευταίο χρονικό διάστημα, και την δημιουργία του οικοσυστήματος Hyperledger πολλές επιχειρήσεις επωφελήθηκαν από τα δίκτυα αυτά τα οποία προωθούν την αποκέντρωση, τη διαφάνεια και τη δικαιοσύνη με σκοπό να δημιουργήσουν λύσεις χρησιμοποιώντας το οικοσύστημα Hyperledger Fabric θέλοντας να έχουν κάποιο είδος επαλήθευσης ταυτότητας που πρέπει να γίνεται στην πλατφόρμα τους. Όμως το Fabric βασίζεται σε παραδοσιακές, κεντρικές τεχνολογίες για συγκεκριμένα μέρη της αρχιτεκτονικής του, όπως η διαχείριση δεδομένων και ταυτότητας. Έτσι δημιουργήθηκε η ανάγκη για μία εφαρμογή αυτοδιαχειριζόμενης ταυτότητας (SSI) με την οποία θα μπορεί να διατηρηθεί η ταυτότητά ασφαλής και ταυτόχρονα να αποδειχθεί η αυθεντικότητα της ταυτότητας στον επαληθευτή χωρίς να αποκαλυφθεί.

1.3. Στόχος της Εργασίας

Η παρούσα διπλωματική εργασία στοχεύει να απαντήσει στα ακόλουθα ερωτήματα:

- Τι είναι η τεχνολογία Blockchain και πώς λειτουργεί.
- Ποια είναι τα πλεονεκτήματα της τεχνολογίας Blockchain σε σχέση με την τρέχουσα χρησιμοποιούμενη τεχνολογία.
- Πώς με τη χρήση του οικοσυστήματος Hyperledger, το οποίο θα δίνει τη δυνατότητα σε έναν χρήστη να επιλέξει ποια από τα χαρακτηριστικά της ταυτότητάς του (π.χ. ηλικία, φύλλο κ.α.) θα μοιράζεται με συγκεκριμένους παρόχους υπηρεσιών, ο χρήστης θα μπορεί να έχει πρόσβαση σε ορισμένες διαδικτυακές υπηρεσίες και πόρους.

2. Τεχνολογία Blockchain

2.1. Ιστορική Αναδρομή

Η τεχνολογία Blockchain χρησιμοποιήθηκε για πρώτη φορά το 2008 από ένα άτομο ή μια ομάδα ατόμων με την ονομασία Satoshi Nakamoto για την ανάπτυξη του Bitcoin. Η πρώτη περιγραφή του Bitcoin βρίσκεται το 1998 στη λίστα αλληλογραφίας cypherpunks από τον Wei Dai. Οι Cypherpunks είναι μια ομάδα ανθρώπων που δημιουργήθηκε το 1992 από τους Eric Hughes, Timoty C May και John Gilmore και είχε ως στόχο την προώθηση της ιδιωτικότητας και της ασφάλειας. Μερικά από τα άτομα που προσχώρησαν στην ομάδα αυτή είναι ο Philip Zimmermann, δημιουργός του PGP 1.0, ο Brunce Schneier, ο Julian Assange, ιδρυτής του WikiLeaks, και άλλοι. Ο Adam Black, επίσης μέλος της ομάδας cypherpunk, εφηύρε το σύστημα Hashcash το οποίο χρησιμοποιήθηκε ως αντίμετρο για επιθέσεις άρνησης παροχής υπηρεσιών και spam ηλεκτρονικού ταχυδρομείου. Σήμερα μια παραλλαγή του Hashcash χρησιμοποιείται ως αλγόριθμος εξόρυξης για το Bitcoin.

Επίσης αξιζει να σημιωθεί ότι το 2021 η συνολική αξία των υπαρχόντων bitcoins ξεπέρασε τα 800 δισεκατομμύρια δολάρια. Υπάρχουν ακόμη και μηχανές αναζήτησης που επιτρέπουν στους χρήστες να αναζητήσουν επιχειρήσεις που δέχονται bitcoin ως νόμισμα. Πανεπιστήμια όπως το Πανεπιστήμιο Λευκωσίας δέχονται bitcoin ως πληρωμή για τα δίδακτρα. Η αύξηση της δημοτικότητας προσέλκυσε την προσοχή μεγαλύτερων συνεργασιών και τεχνολογικών οντοτήτων όχι μόνο στο bitcoin ως νόμισμα αλλά και στην υποκείμενη τεχνολογία του blockchain. Το Ίδρυμα Linux διατηρεί το οικοσύστημα Hyperledger με στόχο την ανάπτυξη πλαισίων, εργαλείων και βιβλιοθηκών για τη διευκόλυνση των επιχειρήσεων να αξιοποιήσουν τις τεχνολογίες blockchain. Ένα παράδειγμα παγκόσμιας συνεργασίας που χρησιμοποιεί και αναπτύσσει ενεργά εφαρμογές με την τεχνολογία blockchain είναι η IBM που ανέπτυξε το Food Trust. Χρησιμοποιείται από εταιρείες όπως η Nestle και η Walmart Inc. για τη βελτίωση των υπηρεσιών τους στην αλυσίδα εφοδιασμού τροφίμων.

2.2. Γενικά για την Τεχνολογία Blockchain

Μία από τις ταχύτατα αναπτυσσόμενες τάσεις στην τεχνολογία του μέλλοντος είναι και η τεχνολογία Blockchain. Το Blockchain είναι ένας κατανεμημένος λογιστικός κατάλογος (distributed ledger), δημόσιος ή ιδιωτικός, στον οποίο συναλλαγές ή δεδομένα συνδέονται μεταξύ τους σε συνδεδεμένα μπλοκ δεδομένων καθιστώντας τα πρακτικά αμετάβλητα και αδιαμφισβήτητα από όλους τους κατανεμημένους κόμβους (Nodes) στους οποίους έχει γίνει η ενημέρωση του καταλόγου. Τα μπλοκ αυτά είναι κρυπτογραφημένα με τον αλγόριθμό SHA-256 ο οποίος κρυπτογραφεί μαθηματικά και κατακερματίζει την πληροφορία του μπλοκ με τέτοιο τρόπο που να μην μπορεί να είναι αναστρέψιμος (one way encryption), πάντα με ένα σταθερό αποτέλεσμα είτε τα δεδομένα που καταχωρήσαμε είναι ένας χαρακτήρας είτε το κείμενο από ένα ολόκληρο βιβλίο όπου το κάθε block αποτελείται από δύο μέρη:

- Το σώμα (body), το οποίο περιέχει, αναλόγως την εφαρμογή, είτε ως απλό κείμενο είτε κρυπτογραφημένα, γεγονότα και συναλλαγές
- Την κεφαλίδα (header), η οποία περιέχει πληροφορίες για το ίδιο το block, όπως τη χρονική σφραγίδα (timestamp), κατακερματισμό των συναλλαγών (hashing) καθώς και κρυπτογραφημένο κατακερματισμό του προηγούμενου block, κρατώντας με αυτό τον τρόπο τη διεύθυνση του προηγούμενου block.

Με αυτόν τον τρόπο επιτυγχάνουμε την διανομή και ενημέρωση όλων των κόμβων (nodes) με το τελευταίο αντίγραφο των μπλοκ καθώς επίσης και την ασφάλεια των δεδομένων απο αλλαγές και αμφισβητήσεις. Δημιουργείται λοιπόν ένα ομότιμο Peer2Peer (p2p) κατανεμημένο δίκτυο όπου τα μέλη μπορούν να αλληλοεπιδρούν μεταξύ τους δίχως την ανάγκη για μεσολάβηση ενός έμπιστου ενδιάμεσου, με εξακριβώσιμο και αξιόπιστο τρόπο. Το ρόλο αυτό αναλαμβάνει ένας consensus μηχανισμός, ο οποίος διαφοροποιείται ανάλογα το blockchain, και μέσω του μηχανισμού αυτού, επιβεβαιώνονται οι συναλλαγές που πραγματοποιούνται στο δίκτυο και περιλαμβάνονται στα επόμενα block που θα προστεθούν στο blockchain. Η διαδικασία αυτή

είναι πιο πολύπλοκη από τον παραδοσιακό τρόπο αλλά συνάμα και πιο ασφαλής καθώς αν ένας κόμβος χαθεί το σύστημα θα συνεχίσει να λειτουργεί. Όσο πιο πολλοί κόμβοι τόσο πιο ασφαλές το δίκτυο αλλά και ταυτόχρονα και πιο αργό.

Όπως αναφέρθηκε προηγουμένως, ανάλογα με τον τύπο του blockchain, υπάρχουν διαφορετικοί μηχανισμοί συναίνεσης (consensus mechanisms). Ο πιο γνωστός είναι το Proof-of-work (PoW). Το PoW απαιτεί την επίλυση μιας περίπλοκης υπολογιστικής διαδικασίας, όπως η εύρεση κατακερματισμών με συγκεκριμένα μοτίβα, όπως για παράδειγμα ένας αριθμός με αρχικά μηδενικά, για να εξασφαλιστεί η πιστοποίηση και η επαληθευσιμότητα. Ακόμη ένας μηχανισμός είναι και το πρωτόκολλο Proof-of-Stake (PoS) το οποίο αντί να χωρίζει τα μπλοκ αναλογικά με τα σχετικά ποσοστά κατακερματισμού των εξορυκτών (δηλαδή την ισχύ εξόρυξής τους), διαχωρίζει τα μπλοκ στοιχημάτων αναλογικά με τον τρέχοντα πλούτο των εξορυκτών. Με αυτόν τον τρόπο, η επιλογή είναι πιο δίκαιη και εμποδίζει τον πλουσιότερο συμμετέχοντα να κυριαρχήσει στο δίκτυο. Πολλά blockchain, όπως το Ethereum, μετατοπίζονται σταδιακά σε PoS λόγω της σημαντικής μείωσης στην κατανάλωση ενέργειας και της βελτιωμένης επεκτασιμότητας.

Άλλη μια συναινετική προσέγγιση αποτελεί το Byzantine Fault Tolerance (BFT) και οι παραλλαγές του. Ένα επιπλέον επίπεδο, το Compute Interface, επιτρέπει στα blockchain να προσφέρουν περισσότερη λειτουργικότητα. Πρακτικά, ένα blockchain αποθηκεύει μια κατάσταση η οποία αποτελείται από όλες τις συναλλαγές που έχουν πραγματοποιηθεί από τους χρήστες, επιτρέποντας έτσι τον υπολογισμό του υπολοίπου του κάθε χρήστη. Ωστόσο, για πιο προηγμένες εφαρμογές πρέπει να αποθηκεύουμε πολύπλοκες καταστάσεις οι οποίες ενημερώνονται δυναμικά χρησιμοποιώντας κατανεμημένους υπολογιστές. Αυτή η απαίτηση οδήγησε στην δημιουργία των έξυπνων συμβολαίων (smart contracts – SC)), τα οποία είναι αυτό-εκτελούμενα σύνολα εντολών που χρησιμοποιούνται για να καταστήσουν δυνατή την ύπαρξη κατανεμημένων και αυτοματοποιημένων ροών εργασιών. Τα SC χρησιμοποιούν κόμβους του blockchain για να εκτελέσουν τους όρους μιας σύμβασης.

Τέλος, το επίπεδο Διακυβέρνησης επεκτείνει την αρχιτεκτονική blockchain για να καλύψει τις ανθρώπινες αλληλεπιδράσεις που λαμβάνουν χώρα στον φυσικό κόσμο. Πράγματι, αν και τα πρωτόκολλα blockchain είναι καλά καθορισμένα, επηρεάζονται επίσης από εισροές από διαφορετικές ομάδες ανθρώπων που ενσωματώνουν νέες μεθόδους, βελτιώνουν τα πρωτόκολλα blockchain και επιδιορθώνουν το σύστημα. Ενώ αυτά τα μέρη είναι απαραίτητα για την ανάπτυξη κάθε blockchain, αποτελούν κοινωνικές διαδικασίες εκτός αλυσίδας. Επομένως, η διακυβέρνηση του blockchain ασχολείται με τον τρόπο με τον οποίο αυτοί οι διαφορετικοί παράγοντες ενώνονται για να παράγουν, να διατηρήσουν ή να αλλάξουν τις εισροές που συνθέτουν ένα blockchain.

Τα blockchain επίσης μπορούν να διαχωριστούν σε τρείς τύπους. Τους δημόσιους καταλόγους, τους ιδιωτικούς καταλόγους και τα hybrid Blockchains. Στους δημόσιους οποιοσδήποτε μπορεί να συμμετέχει στο δίκτυο, ως χρήστες, miners, developers ή μέλη κοινότητας ώστε να γράψει και να διαβάσει χωρίς άδεια από κάποια αρχή. Όλες οι συναλλαγές διαδραματίζονται με διαφάνεια και σαφήνεια και όλοι μπορούν να τις ελέγξουν. Τα δίκτυα είναι σχεδιασμένα αποκεντρωμένα και χωρίς κανένα ατομικό ή κεντρικό έλεγχο των συναλλαγών. Ένα από τα πιο δημοφιλή παραδείγματα public blockchain, είναι το κρυπτονόμισμα Bitcoin. Στους ιδιωτικούς καταλόγους όλοι οι συμμετέχοντες στην αλυσίδα είναι γνωστοί και έμπιστοι (παράδειγμα παραγγελίες εσωτερικά σε μια εταιρεία ή ένα οργανισμό όπως μια Τράπεζα). Οι συναλλαγές είναι ιδιωτικές και διαθέσιμες μόνο σε συμμετέχοντες στο οικοσύστημα στους οποίους έχει δοθεί άδεια να ενταχθούν στο δίκτυο.

Τα ιδιωτικά blockchain είναι πιο συγκεντρωτικά από τα δημόσια blockchain δίκτυα. Τα ιδιωτικά blockchain είναι πολύτιμα για τις επιχειρήσεις που επιθυμούν να συνεργαστούν και να μοιραστούν τα δεδομένα, αλλά δεν θέλουν τα ευαίσθητα επιχειρηματικά τους δεδομένα να είναι ορατά σε ένα δημόσιο blockchain. Οι αλυσίδες αυτές είναι πιο μικρές και γρήγορες ενώ το proof of work σχετικά πιο απλό ανάλογα με την επιχειρηματική απόφαση. Τα hybrid blockchain δίκτυα συνδυάζουν τα οφέλη των private και public blockchain, δίνοντας στις επιχειρήσεις την ευελιξία να επιλέγουν ποια δεδομένα θα είναι δημόσια και διαφανή και ποια θα είναι ιδιωτικά. Τέλος, ένα ακόμη είδος blockchain είναι το consortium blockchain το οποίο διαφέρει από τα private δίκτυα στο γεγονός ότι ο έλεγχος των δεδομένων δεν γίνονται από μία οντότητα αλλά από μια ομάδα. Αυτό το συνεργατικό μοντέλο προσφέρει μερικές από τις καλύτερες περιπτώσεις χρήσης για τα οφέλη του blockchain, καθώς τα μέλη της ομάδας θα έχουν μεγαλύτερη ελευθερία στην συνεργασία τους. Η τεχνολογία Blockchain θα αλλάξει το επιχειρηματικό τοπίο εξαφανίζοντας τους διαμεσολαβητές, καθιστώντας τις συναλλαγές γρήγορες ασφαλείς και αδιαμφισβήτητες.

2.3. Τομείς Εφαρμογών Blockchain

Η τεχνολογία Blockchain ξεκίνησε να χρησιμοποιείται για πρώτη φορά αποκλειστικά και μόνο για χρηματοοικονομικές συναλλαγές και συγκεκριμένα με το ψηφιακό κρυπτονόμισμα του Satoshi Nakamoto, το Bitcoin. Η εξέλιξη όμως της τεχνολογίας του Blockchain τα τελευταία χρόνια επιτρέπει την ανάπτυξη διαφόρων εφαρμογών και σε άλλους τομείς, μερικοί από τους οποίους αναλύονται παρακάτω.

Ο κύριος τομέας εφαρμογής όπως αναφέρθηκε προηγουμένως είναι τα κρυπτονομίσματα τα οποία θεωρούνται ως μέσο συναλλαγής που βασίζονται όμως στην κρυπτογραφία για να εξασφαλίσουν τη ιδιοκτησία και τη δημιουργία νέων μονάδων νομίσματος. Ανήκουν στην κατηγορία των εναλλακτικών νομισμάτων. Η κεντρική ευρωπαϊκή τράπεζα (ECB) έχει θεωρήσει ως κρυπτονομίσματα το σύνολο εικονικών νομισμάτων, τα οποία είναι μια μορφή μη ελεγχόμενων ψηφιακών χρημάτων, εκδίδονται και ελέγχονται από τους προγραμματιστές και χρησιμοποιούνται και επικυρώνονται από τα μέλη μιας συγκεκριμένης ψηφιακής κοινότητας δηλαδή ενός Blockchain δικτύου. (Houben & Snyers, 2018).

Σήμερα υπάρχουν περισσότερα απο 300 διαφορετικά κρυπτονομίσματα όμως το πρώτο γνωστό κρυπτονόμισμα είναι το Bitcoin, που όρισε ο Satoshi Nakamoto το 2008. Με την χρήση του Bitcoin έχουμε τη δυνατότητα συναλλαγών χωρίς υποβολή προσωπικών δεδομένων, την διεκπεραιωσή τους από οποιονδήποτε και οπουδήποτε με πολύ μικρό κόστος αποστολής. Επίσης παρέχεται η δυνατότητα συμμετοχής όλων που ανήκουν στο δίκτυο. Όμως μειονεκτήματα του Bitcoin όπως η άγνωστη ταυτότητα του δημιουργού ενός κρυπτονομίσματος ή το ιστορικό χρήσης του νομίσματος για παράνομες αγορές, οδήγησαν στη δημιουργία άλλων κρυπτονομισμάτων.

Ένας ακόμη τομέας που αξιοποιεί την τεχνολογία Blockchain είναι και αυτός της υγειονομικής περίθαλψης. Τα νοσοκομεία, οι ασθενείς και άλλοι φορείς μπορούν να μοιραστούν την πρόσβαση στα δίκτυά τους χωρίς να διακυβεύουν την ασφάλεια και την ακεραιότητα των δεδομένων τους. Με άλλα λόγια το παραδοσιακό σύστημα καταχώρησης ιατρικών δεδομένων εμποδίζεται λόγω της κεντρικής αποθήκευσης των δεδομένων στα ιατρικά κέντρα. Τα αρχεία που είναι διασκορπισμένα σε διάφορα νοσοκομεία μπορεί να χαθούν και τα δεδομένα που περιέχονται δεν μπορούν να προσεγγιστούν από τον ασθενή. Επομένως, η δημιουργία μας πλατφόρμας Blockchain θα έδινε την δυνατότητα στους ασθενείς να έχουν πρόσβαση στο ιατρικό τους ιστορικό από οπουδήποτε παγκοσμίως, διευκολύνοντας την πρόσβαση στα ιατρικά δεδομένα.

Επιπρόσθετα η τεχνολογία Blockchain συμβάλλει και στην Δημοκρατία με την ανάπτυξη της ηλεκτρονικής ψηφοφορίας όπου καθίσταται πλέον πολύ πιο ασφαλής καθώς εκτός από την κρυπτογράφηση των δεδομένων με μέθοδο που καθιστά εξαιρετικά δύσκολη την παραποίησή τους, διασφαλίζεται και η διαφάνεια αφού οι συμμετέχοντες είναι σε θέση να επιβεβαιώσουν ότι οι ψήφοι τους μετρήθηκαν και ότι το περιεχόμενό τους δεν αλλοιώθηκε. Το κυριότερο πλεονέκτημα όμως είναι ότι κάθε κόμβος με πρόσβαση στο σύστημα μπορεί να βλέπει τα ίδια αποτελέσματα και κάθε ψήφος μπορεί να δικαιολογηθεί με βεβαιότητα στην πηγή της, χωρίς να διακυβεύεται η ανωνυμία των ψηφοφόρων.

Η τεχνολογία Blockchain μπορεί να χρησιμοποιηθεί επίσης και στην διαχείριση της εφοδιαστικής αλυσίδας. Με την χρήση της τεχνολογίας αυτής αναμένεται να αυξηθεί η διαφάνεια και η υπευθυνότητα στα δίκτυα της εφοδιαστικής αλυσίδας, επιτρέποντας έτσι πιο ευέλικτες αλυσίδες. Συγκεκριμένα, οι εφαρμογές που βασίζονται σε blockchain έχουν τη δυνατότητα να δημιουργήσουν καινοτομίες σε τρεις τομείς στις αλυσίδες εφοδιασμού. Αυτές είναι η ορατότητα, η βελτιστοποίηση και η ζήτηση. Το Blockchain μπορεί να χρησιμοποιηθεί στα logistics, στον εντοπισμό πλαστών προϊόντων, στη μείωση της χρήσης χαρτιού, στη διευκόλυνση της παρακολούθησης προέλευσης των προϊόντων και δίνοντας τη δυνατότητα στους αγοραστές και τους πωλητές να συναλλάσσονται απευθείας χωρίς χειραγώγηση από μεσάζοντες. Επιπλέον, έχει αποδειχθεί ότι η χρήση εφαρμογών που βασίζονται σε blockchain σε δίκτυα εφοδιαστικής αλυσίδας μπορεί να διασφαλίσει την ασφάλεια, να οδηγήσει σε πιο ισχυρούς μηχανισμούς διαχείρισης συμβολαίων μεταξύ logistics τρίτων και τετάρτων (3PL, 4PL), ενισχύοντας τους μηχανισμούς παρακολούθησης και τη διασφάλιση ιχνηλασιμότητας παρέχοντας καλύτερη διαχείριση πληροφοριών σε ολόκληρη την αλυσίδα εφοδιασμού. Ακόμη η χρήση εφαρμογών blockchain σε δίκτυα εφοδιαστικής αλυσίδας συμβάλει στην ασφάλεια των τροφίμων, προσφέρει καλύτερη εξυπηρέτηση πελατών μέσω προηγμένων αναλύσεων δεδομένων (δηλ.

κρυπτογραφημένα δεδομένα πελατών) και καινοτόμων συστημάτων συστάσεων, βελτιώνει τη διαχείριση αποθέματος και απόδοσης σε σύνθετες αλυσίδες εφοδιασμού και τέλος, μπορεί να βελτιώσει τα έξυπνα συστήματα μεταφορών και να προσφέρει νέες αποκεντρωμένες αρχιτεκτονικές παραγωγής.

3. Το Οικοσύστημα Hyperledger

3.1. Γενικά

Η επίσημη ιστοσελίδα του Hyperledger δηλώνει ότι: «Το Hyperledger είναι μια συνεργατική προσπάθεια ανοιχτής πηγής που δημιουργήθηκε για να προωθήσει τις διεπαγγελματικές τεχνολογίες blockchain. Πρόκειται για μια παγκόσμια συνεργασία, που φιλοξενείται από το ίδρυμα του Linux Foundation, συμπεριλαμβανομένων των ηγετών στον τομέα της χρηματοδότησης, της τραπεζικής, του Διαδικτύου των πραγμάτων, των αλυσίδων εφοδιασμού, της κατασκευής και της τεχνολογίας».

Το blockchain αυτό δεν υποστηρίζει κρυπτονομίσματα αλλά προσφέρει την δυνατότητα δημιουργίας μιας νέας γενιάς εφαρμογών που δημιουργούν την εμπιστοσύνη, τη λογοδοσία και τη διαφάνεια στον πυρήνα τους, ενώ παράλληλα η τεχνολογία αυτή υποσχέθηκε μια ευρύτερη και πιο θεμελιώδη επανάσταση από την τεχνολογία blockchain, δηλαδή την ροή των επιχειρηματικών διαδικασιών και των νομικών περιορισμών (Rosic, 2017).

Το Hyperledger συμβάλλει στην ανάπτυξη ενός συστήματος που δημιουργεί μια συνεργασία μεταξύ διαφόρων επιχειρήσεων και οργανισμών χωρίς τη χρήση δημόσιων blockchain εφαρμογών όπως το Bitcoin και το Ethereum. Αντί κάθε μεμονωμένος οργανισμός να δημιουργεί τη δική του blockchain λύση, χρησιμοποιείται μια κοινά αποδεκτή πλατφόρμα αποτελούμενη απο επιμέρους τμήματα, τα οποία μπορούν να επιλεχθούν και να συνδυαστούν έτσι ώστε να παρέχουν λύσεις σε κάθετα πεδία εφαρμογών. (Hyperledger , 2017)

3.1.1. Χαρακτηριστικά και Εργαλεία

Το Hyperledger διασφαλίζει και προωθεί μια σειρά επιχειρηματικών Blockchain τεχνολογιών, διεπαφών, πλαισίων, εφαρμογών και βιβλιοθηκών. Παρακάτω αναφέρονται περιληπτικά κάποια μέρη του.

Hyperledger Fabric

Το Fabric είναι μια βάση για την ανάπτυξη λύσεων βασισμένων σε blockchain με μια αρχιτεκτονική μοντέλου. Με το Fabric διαφορετικά εξαρτήματα των Blockchains, όπως η συναίνεση και οι υπηρεσίες προσχώρησης μπορούν να γίνουν «plug-and-play», δηλαδή να ενταχθούν και να τρέξουν εύκολα στο μοντελοποιημένο σύστημα. Το Fabric έχει σχεδιαστεί για να παρέχει ένα πλαίσιο με το οποίο οι επιχειρήσεις μπορούν να δημιουργήσουν το δικό τους, μεμονωμένο δίκτυο blockchain που μπορεί να κλιμακωθεί γρήγορα σε πάνω από 1.000 συναλλαγές ανά δευτερόλεπτο.

Hyperledger Indy

Ως πλατφόρμα διαχείρισης ταυτότητας το Hyperledger Indy έχει κατασκευαστεί ρητά για αποκεντρωμένη διαχείριση ταυτότητας. Προσφέρει εργαλεία και επαναχρησιμοποιήσιμα στοιχεία για τη διαχείριση ψηφιακών ταυτοτήτων σε blockchains ή άλλα κατανεμημένα λογιστικά βιβλία. Η αρχιτεκτονική Hyperledger Indy είναι κατάλληλη για κάθε εφαρμογή που απαιτεί βαριά δουλειά στη διαχείριση ταυτότητας, καθώς το Indy είναι εύκολα ερμηνεύσιμο σε πολλούς τομείς, οργανισμούς και εφαρμογές. Ως εκ τούτου, οι ταυτότητες αποθηκεύονται με ασφάλεια και μοιράζονται σε όλα τα εμπλεκόμενα μέρη.

Hyperledger Iroha

Το Hyperledger Iroha χρησιμοποιείται στην Cambodia για να δημιουργήσει ένα νέο σύστημα πληρωμών παράλληλα με την εθνική τράπεζα της Cambodia, καθώς επίσης πολλές Ιαπωνικές εταιρίες συνεργάζονται στο πλαίσιο του Iroha για προγράμματα στην υγειονομική περίθαλψη, την χρηματοδότηση και τη διαχείρηση της ταυτότητας.

Hyperledger Caliper

Το Hyperledger Caliper είναι ένα εργαλείο συγκριτικής αξιολόγησης και ένα από τα έργα του Hyperledger που φιλοξενείται από το The Linux Foundation. Το Hyperledger Caliper επιτρέπει στους χρήστες να μετρήσουν την απόδοση μιας συγκεκριμένης εφαρμογής blockchain με ένα σύνολο προκαθορισμένων περιπτώσεων χρήσης. Το Hyperledger Caliper θα παράγει αναφορές που θα περιλαμβάνουν ορισμένους δείκτες απόδοσης, όπως TPS (Transactions Per Second), λανθάνουσα κατάσταση συναλλαγών, χρήση πόρων κλπ. Στόχος είναι τα αποτελέσματα του Caliper να χρησιμοποιηθούν από άλλα έργα του Hyperledger, καθώς αναπτύσσουν τα πλαίσια τους και αναφορές στην υποστήριξη της επιλογής μιας εφαρμογής blockchain κατάλληλης για τις συγκεκριμένες ανάγκες ενός χρήστη. Στο Hyperledger Caliper είχαν αρχικά συμβάλει προγραμματιστές από την Huawei, Hyperchain, Oracle, Bitwise, Soramitsu, IBM και το Πανεπιστήμιο Τεχνολογίας και Οικονομικών της Βουδαπέστης. (Hyperledger Team, 2018)

Hyperledger Cello

Το Hyperledger Cello στοχεύει να φέρει το μοντέλο ανάπτυξης «on-the-service» στο οικοσύστημα blockchain για να μειώσει την προσπάθεια που απαιτείται για τη δημιουργία, τη διαχείριση και τον τερματισμό μπλοκ αλυσίδων. Παρέχει μια υπηρεσία αλυσίδας πολλαπλών μισθωτών αποτελεσματικά και αυτόματα πάνω από διάφορες υποδομές, π.χ. baremetal, εικονική μηχανή και περισσότερες πλατφόρμες εμπορευματοκιβωτίων. Στο Hyperledger Cello συνεισέφερε αρχικά η IBM, με χορηγούς τους Soramitsu, Huawei και Intel.

Hyperledger Explorer

Σχεδιασμένο για να δημιουργήσει μια φιλική προς το χρήστη εφαρμογή Ιστού, το Hyperledger Explorer μπορεί να προβάλλει, να επικαλείται, να αναπτύσσει και να υποβάλλει ερωτήματα σε μπλοκ, συναλλαγές και συναφή δεδομένα, πληροφορίες δικτύου (όνομα, κατάσταση, λίστα κόμβων), αλυσιδωτούς κωδικούς και οικογένειες συναλλαγών και σχετικές πληροφορίες που είναι αποθηκευμένες στο ledger. Στην αρχιτεκτονική του Hyperledger Explorer συνεισέφεραν αρχικά η IBM, η Intel και η DTCC.

Hyperledger Composer

Το Hyperledger Composer είναι ένα σύνολο εργαλείων συνεργασίας για την οικοδόμηση δικτύων επιχειρηματικών δεσμών, τα οποία καθιστούν απλό και γρήγορο για τους ιδιοκτήτες επιχειρήσεων και προγραμματιστές να δημιουργούν έξυπνες συμβάσεις και εφαρμογές αποκλεισμού για την επίλυση επιχειρηματικών προβλημάτων. Το Hyperledger Composer υποστηρίζει και διαμένει στην κορυφή της υπάρχουσας υποδομής και χρόνου εκτέλεσης του Hyperledger Fabric Blockchain.Το Hyperledger Composer παρέχει μια απλοποιημένη γλώσσα μοντελοποίησης συγκεκριμένου τομέα για τη μοντελοποίηση επιχειρηματικού δικτύου και τη JavaScript για την λογική εφαρμογή των συναλλαγών.

Hyperledger Aries

Το Hyperledger Aries παρέχει ένα κοινόχρηστο, επαναχρησιμοποιήσιμο, διαλειτουργικό κιτ εργαλείων σχεδιασμένο για πρωτοβουλίες και λύσεις που επικεντρώνονται στη δημιουργία, τη μετάδοση και την αποθήκευση επαληθεύσιμων ψηφιακών διαπιστευτηρίων. Είναι υποδομή για αλληλεπιδράσεις με βάση το blockchain, peer-to-peer. Αυτό το πρότζεκτ καταναλώνει την κρυπτογραφική υποστήριξη που παρέχεται από το Hyperledger Ursa, για την παροχή ασφαλούς μυστικής διαχείρισης και αποκεντρωμένης διαχείρισης κλειδιών.

3.1.2. Περιβάλλον Εκτέλεσης

Το λειτουργικό σύστημα που χρησιμοποιήθηκε για την εκτέλεση της εφαρμογής είναι ένα Ubuntu 20.04.4 LTS στο οποίο έχουν ανατεθεί 16 GB RAM και 4 πυρήνες από το φυσικό μηχάνημα με επεξεργαστή AMD® Ryzen 5 2500u CPU. Το blockchain network που χρησιμοποιούμε είναι το Test Network που παρέχουν τα Fabric samples ως sample δίκτυο στην έκδοση 2.2 του Hyperledger. Όλα τα scripts που παραθέτουμε ξεκινούν με αρχικό working directory το /home/test-network , εκτός από τις περιπτώσεις όπου διευκρινίζεται διαφορετικά. Το δίκτυό μας αποτελείται από ένα κανάλι mychannel με δύο οργανισμούς Org1 και Org2, με ένα peer κόμβο ο καθένας, και έναν orderer κόμβο.

3.2. Self-Sovereign Identity

Η Αυτοδιαχειριζόμενη Ταυτότητα (Self-Sovereign Identity - SSI), είναι μια προσέγγιση για την ψηφιακή ταυτότητα που επιτρέπει σε οντότητες (π.χ. άτομα, οργανισμούς και αντικείμενα) να ελέγχουν πλήρως τις πληροφορίες που χρησιμοποιούν για να αποδείξουν ποιοι είναι σε ιστότοπους , υπηρεσίες και εφαρμογές σε ολόκληρο το διαδίκτυο χωρίς να βασίζονται σε καμία εξωτερική αρχή. Το SSI παρουσιάζει μια αλλαγή, μια μετατόπιση ισχύος και ελέγχου, από τους παρόχους ταυτότητας και υπηρεσιών στους χρήστες, οι οποίοι αναλαμβάνουν την διαχείριση της ταυτότητας τους και της ροής πληροφοριών κατά τις ψηφιακές αλληλεπιδράσεις τους. Επομένως, το SSI είναι επικεντρωμένο στο χρήστη, επιτρέποντας του να δημιουργεί και να διαχειρίζεται μοναδικά αποκεντρωμένα αναγνωριστικά (DID) ανεξάρτητα από οποιοδήποτε τρίτο πάροχο και τις δυνατότητες που παρέχουν οι πάροχοι αυτοί για την διαχείριση της ταυτότητας.

Επιπλέον, τα αναγνωριστικά και τα σχετικά προσωπικά δεδομένα μπορούν να αποθηκευτούν με ασφάλεια από τους χρήστες και να παρουσιαστούν ελεύθερα όταν απαιτείται η απόδειξη της ταυτότητας. Με αυτόν τον τρόπο, τα προσωπικά δεδομένα δεν διατηρούνται πλέον σε βάσεις δεδομένων τρίτων, ενισχύοντας την ασφάλεια και το απόρρητο και μειώνοντας τον κίνδυνο που συνδέεται με τη διαρροή δεδομένων και άλλα εγκλήματα στον κυβερνοχώρο που σχετίζονται με την ταυτότητα. Μερικά από τα διάσημα περιστατικά που αφορούν κατάχρηση προσωπικών δεδομένων αποτελούν το περιστατικό Cambridge Analytica, το περιστατικό με την εταιρεία Yahoo το 2013 και το Facebook τον Απρίλιο του 2019.

Το SSI δεν εξαρτάται από μια συγκεκριμένη τεχνολογία και εφαρμογή, αλλά μπορεί να πραγματοποιηθεί με διάφορους τρόπους. Ωστόσο, μπορεί να επιτευχθεί καλύτερα με τη χρήση της τεχνολογίας αποκεντρωμένου καθολικού (Decentralized Ledger Technology - DLT), συνήθως μέσω της τεχνολογίας Blockchain, αποκεντρωμένων αναγνωριστικών (Decentralized Identifiers - DIDs) , και επαληθεύσιμων διαπιστευτηρίων (Verifiable Credentials - VC) τα οποία είναι τυποποιημένα από το World Wide Web Consortium (W3C).

Το DLT παρέχει μια εμπιστοσύνη λόγω της κρυπτογράφισης, λειτουργεί όμως ως μη αξιόπιστη, αποκεντρωμένη υποδομή δημόσιου κλειδιού (Decentralized Public-Key Infrastructure - DPKI). Στην ουσία συμπεριφέρεται ως αντικατάσταση μιας κεντρικής αρχής καταχώρισης στα παραδοσιακά συστήματα διαχείρισης ταυτότητας, όπου διατηρείται η σύζευξη του αναγνωριστικού και της μεθόδου ελέγχου ταυτότητας.

Τα DIDs είναι παγκοσμίως μοναδικά αποκεντρωμένα αναγνωριστικά, που παρέχουν ένα μέσο για έλεγχο ταυτότητας χρησιμοποιώντας κρυπτογραφικές αποδείξεις. Επιτρέποντας στις οντότητες να αποδείξουν τον έλεγχο τους, χωρίς να απαιτείται άδεια από τρίτους.

Τα VC είναι ψηφιακά διαπιστευτήρια που εκδίδονται από τον εκδότη σε έναν κάτοχο, σύμφωνα με τα οποία οι εκδότες πιστοποιούν ορισμένα χαρακτηριστικά, που περιέχουν πληροφορίες που σχετίζονται με την ταυτότητα, την αρχή έκδοσης, τον τύπο του διαπιστευτηρίου, τα διεκδικούμενα χαρακτηριστικά ή ιδιότητες, τους περιορισμούς ταυτότητας και αποδεικτικά στοιχεία που σχετίζονται με την προέλευσή τους. Τα DID και τα VC διαχειρίζονται και ελέγχονται απευθείας από τον κάτοχο ταυτότητας. Αποθηκεύονται στον ελεγχόμενο από τον χρήστη χώρο αποθήκευσης εκτός αλυσίδας και μπορούν να παρουσιαστούν σε οποιοδήποτε εξαρτημένο μέρος όταν χρειαστεί.

Πολλοί άνθρωποι έχουν γράψει σχετικά με τις αρχές της αυτοδιαχειριζόμενης ταυτότητας, συμπεριλαμβανομένων των «Νόμων της Ταυτότητας» του Kim Cameron και του World Wide Web Consortium (W3C). Αν και δεν υπάρχει σαφής πρωτόκολλο συναίνεσης σχετικά με το τι είναι το SSI, μεταξύ διαφορετικών οργανισμών, έχουν θεσπιστεί 10 βασικές αρχές που συνοψίζουν τις βασικές πτυχές του SSI οι οποίες είναι οι εξής:

- Ύπαρξη: Ένας χρήστης πρέπει να μπορεί να υπάρχει στον ψηφιακό κόσμο χωρίς την ανάγκη τρίτου παρόχου.
- Έλεγχος: Οι χρήστες πρέπει να έχουν την απόλυτη εξουσία για την ψηφιακή τους ταυτότητα και τα προσωπικά τους δεδομένα.
- Πρόσβαση: Οι χρήστες πρέπει να έχουν εύκολη και άμεση πρόσβαση στα δικά τους δεδομένα.
- Διαφάνεια: Ο τρόπος διαχείρισης και ενημέρωσης ενός συστήματος ταυτότητας και των αλγορίθμων πρέπει να είναι δημόσια διαθέσιμος και εύλογα κατανοητός. Ο σχεδιασμός της λύσης θα πρέπει να βασίζεται σε πρότυπα ανοιχτού πρωτοκόλλου και ανοιχτό λογισμικό.
- Επιμονή: Οι ταυτότητες πρέπει να είναι μακροχρόνιες. Οι υπεύθυνοι ανάπτυξης λύσεων θα πρέπει να εφαρμόσουν επαρκή θεμελιώδη υποδομή και να σχεδιάσουν βιώσιμα εμπορικά και λειτουργικά μοντέλα.
- Φορητότητα: Οι άνθρωποι πρέπει να μπορούν να φέρουν τις ταυτότητες και τα διαπιστευτήριά τους οπουδήποτε, να μεταφέρουν τα δεδομένα τους από τη μια πλατφόρμα στην άλλη και να μην περιορίζονται σε μία μόνο πλατφόρμα.
- Διαλειτουργικότητα: Οι ταυτότητες θα πρέπει να είναι όσο το δυνατόν ευρύτερα χρησιμοποιήσιμες από διάφορους ενδιαφερόμενους. Οι οργανισμοί, οι βάσεις δεδομένων και τα μητρώα πρέπει να μπορούν να επικοινωνούν γρήγορα και αποτελεσματικά μεταξύ τους παγκοσμίως μέσω ενός συστήματος ψηφιακής ταυτότητας.
- Συναίνεση: Οι χρήστες πρέπει να δώσουν ρητή άδεια σε μια οντότητα να χρησιμοποιεί ή να έχει πρόσβαση στα δεδομένα τους. Η διαδικασία έκφρασης της συναίνεσης πρέπει να είναι διαδραστική και καλά κατανοητή από τους ανθρώπους.
- Ελαχιστοποίηση: Μια λύση ψηφιακής ταυτότητας θα πρέπει να επιτρέπει στους ανθρώπους να μοιράζονται τον ελάχιστο δυνατό όγκο δεδομένων που χρειάζεται ένα άλλο μέρος για να ελαχιστοποιηθεί η κοινή χρήση υπερβολικών και περιττών προσωπικών πληροφοριών.
- Προστασία: Το δικαίωμα των ανθρώπων στην ιδιωτική ζωή πρέπει να προστατεύεται και θα πρέπει να υπάρχουν εγγυήσεις έναντι της παραποίησης και παρακολούθησης πληροφοριών. Η κίνηση δεδομένων θα πρέπει να είναι κρυπτογραφημένη από άκρο σε άκρο.

Το SSI αποτελεί μια πιθανή λύση για την επίλυση των υπαρχόντων προβλημάτων που αντιμετωπίζουν τα τρέχοντα μοντέλα ταυτότητας. Το Blockchain είναι μια καινοτόμος τεχνολογία για την εφαρμογή λύσεων SSI το οποίο συμβάλει στην ασφάλεια των αποθηκευμένων δεδομένων με την χρήση κρυπτογραφικών εργαλείων που κατέχει. Η λύση SSI που βασίζεται σε blockchain ενισχύει την εμπιστοσύνη μεταξύ των συμμετεχόντων εντός του δικτύου χωρίς να αποκαλύπτονται τα πραγματικά δεδομένα. Μερικές από τις σημαντικότερες υλοποιήσεις του SSI που βασίζονται στην τεχνολογία blockchain αποτελούν τα παρακάτω παραδείγματα.

Το uPort αποτελεί ένα παράδειγμα αυτοδιαχειριζόμενης ταυτότητας με βάση το Ethereum. Συγκεκριμένα με την εγκατάσταση μιας εφαρμογής στο τηλέφωνο ενός χρήστη μπορεί να δημιουργηθεί μια ταυτότητα. Αυτή η εφαρμογή διατηρεί όλα τα δεδομένα που συνδέονται με την ταυτότητα. Κρατάει επίσης τα ιδιωτικά κλειδιά που χρησιμοποιούνται για την υπογραφή βεβαιώσεων και την κοινή χρήση τους με άλλους. Η αποθήκευση των δεδομένων σε τοπικό επίπεδο παρέχει έλεγχο και πρόσβαση στην ταυτότητα του χρήστη και επιβάλλει στον χρήστη να παρέχει τη συγκατάθεσή του προτού μπορέσουν οι άλλοι να χρησιμοποιήσουν τις πληροφορίες. Οι ταυτότητες του UPort μπορούν να υπογράφουν βεβαιώσεις για άλλες ταυτότητες και να τις δημοσιεύουν στο blockchain δίκτυο, αυξάνοντας την αξιοπιστία του. Το uPort όμως στερείται φορητότητας. Η μόνη άλλη πληροφορία που αποθηκεύεται δημόσια στο blockchain είναι το Decentralized ID (DID). Τα DID χρησιμοποιούνται ως ταυτότητα αλλά και ως

σύνδεσμος προς το δημόσιο κλειδί του χρήστη. Όλα τα αιτήματα και οι απαντήσεις μεταφέρονται χρησιμοποιώντας συγκεκριμένα πρότυπα, που αντιπροσωπεύουν όλα τα διαφορετικά είδη ιδιωτικών πληροφοριών με δομημένο τρόπο παρέχοντας διαλειτουργικότητα. Η ταυτότητα αποτελείται επίσης από πολλά έξυπνα συμβόλαια που τοποθετούνται στο blockchain. Καθώς το ιδιωτικό κλειδί αποθηκεύεται στο τηλέφωνο, η απώλεια μιας τέτοιας συσκευής θα είχε ως αποτέλεσμα την απώλεια της ταυτότητας.

Μια ακόμη υλοποίηση SSI αποτελεί το IDchainZ το οποίο είναι ένα πρόγραμμα που δίνει τη δυνατότητα στους χρήστες να κρατούν ένα κλειδί πιστοποιημένων εγγράφων ταυτότητας και επιτρέπει σε πολλαπλά εξωτερικά μέρη να προσθέτουν, να πιστοποιούν και να ανταλλάσσουν τεκμηρίωση της γνώσης του πελάτη (know your customer - KYC) και της καταπολέμησης της νομιμοποίησης εσόδων από παράνομες δραστηριότητες (anti-money laundering - AML). Αυτό στην συνέχεια επεκτάθηκε για να χρησιμοποιηθεί για όλα τα είδη διαφορετικών εγγράφων. Ο χρήστης λοιπόν έχει την δυνατότητα να παραχωρεί άδεια σε τρίτο μέρος για πρόσβαση στα δεδομένα του. Αυτό μπορεί να περιοριστεί από τον χρήστη στη διάρκεια, τις πληροφορίες που μοιράζονται και στον αριθμό των προσβάσεων. Αυτό επιτρέπει στον χρήστη να έχει τον έλεγχο των δεδομένων του. Ο χρήστης μπορεί επίσης να ανακαλέσει την πρόσβαση στα δεδομένα του ανά πάσα στιγμή, αλλά θα χρειαστεί τα ιδιωτικά κλειδιά για να το κάνει. Διαφορετικά, τα δεδομένα θα παραμείνουν στο blockchain.

Ένα ακόμη παράδειγμα SSI αποτελεί το EverID. Σε αντίθεση με το uPort, το αποκεντρωμένο σύστημα του EverID χρησιμοποιείται για την αποθήκευση και την επιβεβαίωση δεδομένων ταυτότητας χρήστη, τεκμηρίωσης και βιομετρικών στοιχείων. Το EverID διευκολύνει την επαλήθευση των χρηστών από πολλούς τρίτους και επιτρέπει την ασφαλή μεταφορά μεταξύ των μελών του δικτύου. Αυτό σημαίνει ότι οι ισχυρισμοί των χρηστών είναι αποδεδειγμένοι. Η αποκεντρωμένη αρχιτεκτονική της πλατφόρμας παρέχει επίσης ιδιοκτησία προσωπικών δεδομένων στα οποία μπορεί να έχει πρόσβαση μόνο ο χρήστης. Τα δεδομένα του ατόμου καταγράφονται με τρόπο που επιτρέπει στο άτομο να ελέγχει πώς μοιράζονται, με ποιον και για πόσο καιρό. Αυτός ο μηχανισμός κοινής χρήσης επιβάλλεται από έξυπνα συμβόλαια για κάθε συναλλαγή με αυτοματοποιημένες λύσεις. Η υποδομή EverID λειτουργεί σε μια σειρά υπερκόμβων στο δίκτυο. Αυτοί οι υπερκόμβοι φιλοξενούν επίσης την υπηρεσία Bridge για να επιτρέπουν σε μεμονωμένα άτομα να μεταφέρουν τα δεδομένα τους σε μια εφαρμογή EverID και στον διακομιστή API για να ενεργοποιούν τις συναλλαγές από συσκευές με δυνατότητα SDK. Αυτό λοιπόν κάνει το EverID φορητό. Ακόμη αυτό που διακρίνει το EverID από άλλες λύσεις είναι ότι δεν χρειάζεται να έχει κανείς συσκευή αφού η ψηφιακή ταυτότητα (συνδυασμός βιομετρικών στοιχείων, κρατική ταυτότητα και επιβεβαιώσεις τρίτων) μπορεί να αποθηκευτεί στο cloud. Ωστόσο, το EverID δεν πληροί την ιδιότητα ελαχιστοποίησης. Όταν απαιτούνται δεδομένα για την επαλήθευση μιας αξίωσης, ο χρήστης θα αποκαλύψει πλήρως τα δεδομένα του. Αν κάποιος ενδιαφέρεται για παράδειγμα να μάθει εάν ο χρήστης είναι άνω των 18 ετών, ο χρήστης μπορεί να επιλέξει να αποκαλύψει την πλήρη ημερομηνία γέννησής του ή να μην την αποκαλύψει καθόλου. Το EverID δεν είναι επίσης ανοιχτού κώδικα, επομένως οι ισχυρισμοί που πραγματοποιούνται δεν είναι αποδείξιμοι. Αν και το EverID είναι μια λύση που βασίζεται σε blockchain, συμπεραίνουμε ότι δεν υπάρχει διαφάνεια.

Ακόμη μια σημαντική υλοποίηση SSI είναι το δίκτυο Sovrin. Είναι ένα κατανεμημένο καθολικό με δημόσια άδεια. Αυτό σημαίνει ότι οι χρήστες μπορούν να δουν τις συναλλαγές αλλά όχι απαραίτητα να ξεκινήσουν συναλλαγές. Ως αποτέλεσμα, η ανάγκη για την χρήση του proof of work (PoW) καταργείται. Αυτό δείχνει ότι χρησιμοποιούν ένα κατανεμημένο πρωτόκολλο συναίνεσης που εστιάζει περισσότερο στην ασφάλεια και την επεκτασιμότητα. Αυτή η λύση ανταποκρίνεται επίσης στην απαίτηση ελαχιστοποίησης, επιτρέποντας την επιλεκτική αποκάλυψη αξιώσεων χρησιμοποιώντας αποδείξεις μηδενικής γνώσης(zero-knowledge proofs). Επομένως, κανένα στοιχείο δεν θα κοινοποιηθεί χωρίς τη συγκατάθεση του χρήστη και αυτό δίνει στους κατόχους ταυτότητας τον έλεγχο της ψηφιακής τους ταυτότητας. Ωστόσο, υπάρχουν ορισμένα προβλήματα: δεν φαίνεται να παρέχουν ή να απαιτούν καμία (επαληθεύσιμη) εγγύηση σχετικά με την ορθή λειτουργία των πρακτόρων στο δίκτυο. Τέλος, το Sovrin δεν είναι φορητό αφού οι ταυτότητες κατέχονται αποκλειστικά από ένα τρίτο μέρος, το ίδρυμα.

Τέλος το SelfKey είναι ένα δίκτυο αυτοκυρίαρχης ψηφιακής ταυτότητας. Με το SelfKey, τα δεδομένα του χρήστη αποθηκεύονται σε συσκευή υπό τον έλεγχο του κατόχου. Αυτό δίνει στον χρήστη τον απόλυτο έλεγχο της δικής του ανεξάρτητης ταυτότητας. Όταν ένα τρίτο μέρος θέλει να συλλέξει συγκεκριμένα δεδομένα, τα οποία είναι αποθηκευμένα στο blockchain, ο χρήστης μπορεί να επιλέξει να τα αποκαλύψει. Η διαδικασία αυτού είναι παρόμοια με τον έλεγχο

ταυτότητας μέσω «σύνδεσης» ενός λογαριασμού σε ένα κοινωνικό δίκτυο όπως το Facebook. Κατά την έγκριση της συλλογής δεδομένων τρίτων, το SelfKey διασφαλίζει ότι μόνο η ελάχιστη απαραίτητη πληροφορία δεδομένων μπορεί να συλλεχθεί χρησιμοποιώντας μηδενικές αποδείξεις γνώσης (zero knowledge proofs). Το SelfKey εκπληρώνει τις ιδιότητες συναίνεσης και ελαχιστοποίησης. Για τον έλεγχο μιας ταυτότητας, το Selfkey χρησιμοποιεί αλγόριθμους ανθεκτικούς στη λογοκρισία. Αυτοί οι ανεξάρτητοι αλγόριθμοι είναι αποκεντρωμένοι. Οι αξιώσεις ταυτότητας από τον χρήστη μπορούν να επαληθευτούν μόνο από αξιόπιστες οντότητες, διασφαλίζοντας ότι η αποδεδειγμένη ιδιότητα πρέπει να πληρείται.

Υπάρχουν όμως και υλοποιήσεις της αυτοδιαχειριζόμενης ταυτότητας (SSI) οι οποίες δεν βασίζονται στην τεχνολογία του blockchain. Μία τέτοια περίπτωση αποτελούν τα Personal Data Storages (PDS). Τα PDS είναι περιβάλλοντα όπου ο χρήστης έχει τον πλήρη έλεγχο της πρόσβασης άλλων μερών. Αυτή η αρχιτεκτονική επιτρέπει τόσο τοπική όσο και (κατανεμημένη στο δίκτυο) ηλεκτρονική αποθήκευση. Καθώς τα δεδομένα αποθηκεύονται τοπικά, το ερώτημα υποβάλλεται σε επεξεργασία στο ίδιο το PDS. Μόνο η απάντηση του ερωτήματος αποστέλλεται πίσω, επιτρέποντας τον πλήρη έλεγχο των δεδομένων που χρησιμοποιούνται και την ελαχιστοποίηση των εκτιθέμενων πληροφοριών. Όταν τα δεδομένα αποθηκεύονται στο διαδίκτυο, οι κόμβοι με διαφορετικές εργασίες επικοινωνούν μεταξύ τους για προστασία από μη εξουσιοδοτημένη πρόσβαση. Τα δεδομένα χωρίζονται σε μη αποκρυπτογραφημένα κομμάτια και κατανέμονται σε πολλούς κόμβους αποθήκευσης. Ένας άλλος τύπος κόμβου, ο κόμβος δείκτη, παρακολουθεί την αντιστοίχιση του κλειδιού που χρησιμοποιείται για την αποκρυπτογράφηση των πληροφοριών και του κλειδιού κάθε μεμονωμένου τμήματος ιδιωτικών πληροφοριών. Επιπλέον οι κόμβοι ελέγχου παρακολουθούν το νόημα των πληροφοριών, τον κάτοχο των δεδομένων και σε ποιον μοιράζονται οι πληροφορίες. Το PDS δεν προτείνει τυπικές μορφές για την αποθήκευση των πληροφοριών. Αυτό σημαίνει ότι ο χρήστης έχει περισσότερο έλεγχο σχετικά με το τι αποθηκεύεται.

3.3. Hyperledger Fabric

Το Hyperledger Fabric δημιουργήθηκε υπό την αιγίδα του Linux Foundation και έχει γνωρίσει μεγάλη ανάπτυξη έκτοτε. Είναι μια κατανεμημένη, ανοιχτού κώδικα, private πλατφόρμα, σχεδιασμένη για επιχειρηματικό περιεχόμενο που προσφέρει μερικές βασικές διαφοροποιήσεις σε σχέση με άλλες δημοφιλείς blockchain πλατφόρμες. Η σημαντικότερη διαφορά είναι ότι στο κέντρο του δικτύου υπάρχει ένα κατανεμημένο ledger, το οποίο καταγράφει όλες τις συναλλαγές που συμβαίνουν στο δίκτυο.

Μερικά από τα βασικά στοιχεία του Hyperledger Fabric είναι τα ακόλουθα:

- Private/Permissioned blockchain. Δε μπορεί να συμμετέχει οποιοσδήποτε στο blockchain, ενώ οι συμμετέχοντες έχουν κάποιον κοινό σκοπό αν και δεν εμπιστεύονται απαραίτητα ο ένας τον άλλο. Ορίζονται περιορισμοί στους συμμετέχοντες σχετικοί με τα δικαιώματα πρόσβασης και γραφής.
- Η αρχιτεκτονική του είναι αρθρωτή (modular) και παραμετροποιήσιμη (configurable).
- Pluggable consensus protocols. Η διαφοροποίηση αυτή επιτρέπει στο Hyperledger Fabric να παραμετροποιείται προκειμένου να είναι αποδοτικό ανεξαρτήτως των αναγκών που προκύπτουν από την εκάστοτε περίπτωση χρήσης
- Το ledger του αποτελείται από δύο κομμάτια, την Παγκόσμια Κατάσταση (World State), όπου περιγράφει τη κατάσταση του ledger για κάποια χρονική στιγμή και το Ημερολόγιο Συναλλαγών (Transaction Log) όπου καταγράφει όλες τις συναλλαγές που οδηγούν σε κάθε κατάσταση στο World State.
- Το Fabric, ως permissioned blockchain, επιτρέπει τη προσέγγιση της εμπιστευτικότητας μέσω της αρχιτεκτονικής των καναλιών επικοινωνίας και μέσω της δυνατότητας επιλογής ορισμού δεδομένων ως ιδιωτικά, όπου μπορεί να καθοριστεί το υποσύνολο των χρηστών που θα έχουν πρόσβαση σε αυτά.

Οι χρήστες του Hyperledger Fabric χρησιμοποιούν συχνά τους όρους smart contract και chaincode εναλλακτικά. Σε γενικές γραμμές, ένα έξυπνο συμβόλαιο ορίζει τη λογική συναλλαγής που ελέγχει τον κύκλο ζωής ενός επιχειρησιακού αντικειμένου. Στη συνέχεια ταξινομείται σε αλυσιδωτή μορφή (chaincode) και ο αλυσιδωτός κώδικας αξιοποιείται από το δίκτυο. Καταλαβαίνουμε λοιπόν, ότι τα smart contracts ορίζουν τον τρόπο με το οποίο γίνονται οι συνναλαγές ενώ το chaincode τον τρόπο με τον οποίο ταξινομούνται τα smart contracts για την αξιοποίησή τους.

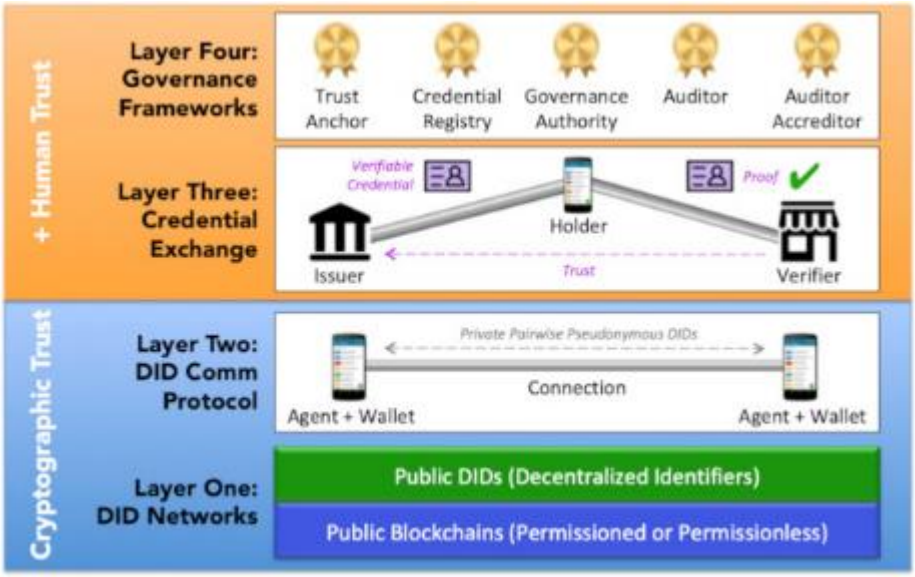
Το κύριο χαρακτηριστικό όμως που ξεχωρίζει τη προσέγγιση του Fabric σε σχέση με τις περισσότερες προσεγγίσεις στα smart contracts είναι η διαφοροποίηση του τρόπου που λειτουργούν. Στο Hyperledger Fabric για τις συναλλαγές ακολουθείται μια execute-order-validate λογική. Ο διαχωρισμός σε 3 στάδια της ροής της συναλλαγής αντιμετωπίζει προβλήματα όπως αυτά της απόδοσης του συστήματος, της κλιμάκωσης, της εμπιστευτικότητας κ.α. Η ροή της συναλλαγής μπορεί να αναλυθεί ως εξής :

- Στο πρώτο στάδιο (Execute) εκτελείται μία συναλλαγή και ελέγχεται ως προς την ορθότητα της.
- Order: Η λειτουργία διάταξης των συναλλαγών εκτελείται από την Ordering Service του συστήματος. Οι συναλλαγές που έχουν υποβληθεί από το στάδιο του execute στη συνέχεια διατάσσονται και κατανέμονται σε block. Μπορούν να ληφθούν παράλληλα πολλές συναλλαγές από διαφορετικούς χρήστες. Οι κόμβοι του ordering service λειτουργούν συλλογικά και συντονισμένα προκειμένου να δημιουργήσουν καλά καθορισμένες ακολουθίες συναλλαγών και να τις οργανώσουν σε block. Τα block αυτά αποθηκεύονται στο ledger του orderer και στη κατανέμονται στους peers που ανήκουν στο συγκεκριμένο κανάλι επικοινωνίας. Στο Fabric η υπηρεσία αυτή είναι κεντρική, αλλά μπορεί να αποτελείται από πολλούς κόμβους που δουλεύουν παράλληλα με σκοπό την ολοκλήρωση της διαδικασίας. Αυτός είναι και ο λόγος όπου το ordering service έχει σχεδιαστεί προκειμένου να μπορεί να είναι αποκεντρωμένο.
- Validate: Στο στάδιο αυτό επαληθεύονται οι συναλλαγές με βάση κάποια συγκεκριμένη πολιτική πριν τις υποβάλλουμε στο blockchain. Η πολιτική που εφαρμόζεται σε κάθε εφαρμογή καθορίζει πόσοι κόμβοι ή ποιοι από αυτούς πρέπει να εγγυηθούν για την ορθή λειτουργία του chaincode. Συνεπώς κάθε συναλλαγή χρειάζεται να εκτελεστεί από ένα υποσύνολο των κόμβων.

3.4. Hyperledger Indy

Το Hyperledger Indy είναι ένα κατανεμημένο λογιστικό βιβλίο κατασκευασμένο για αποκεντρωμένες ταυτότητες. Ο Evernym είναι ένας από τους αρχικούς ιδρυτές του Sovrin Network, ενός δημόσιου blockchain. Αυτό σημαίνει ότι όλοι μπορούν να χρησιμοποιήσουν το blockchain, αλλά μόνο οι επιτρεπόμενες οντότητες,που ονομάζονται Stewards, μπορούν να τρέξουν τους κόμβους επικύρωσης. Υπάρχουν επίσης ιδιωτικά blockchain, που σημαίνει ότι μόνο επιλεγμένες οντότητες μπορούν να συμμετάσχουν, όπως η εφαρμογή IBM Food Trust, και τα ledgers χωρίς άδεια, όπως το bitcoin, όπου ο καθένας μπορεί να ενεργήσει ως miner-validator. Επίσης από το Hypeldger Indy probject προέκυψαν τα Hypeledger Ursa και Hyperledger Aries. Το Hyperledger Ursa είναι η κοινή κρυπτογραφική βιβλιοθήκη για όλα τα έργα Hyperledger που υλοποιούν κρυπτογραφικά πρωτόκολλα όπως οι υπογραφές CLRSA. Το Hyperledger Aries είναι το πρωτόκολλο για peer to peer (p2p) συνδέσεις, πορτοφόλια, ανταλλαγή μηνυμάτων και διαχείριση κλειδιών.

Αρχικά το Indy κάλυψε τα τρία πρώτα επίπεδα τα οποία αποτελούνται από τα πορτοφόλια(L1), την επικοινωνία των DIDS(L2) και τα διαπιστευτήρια Zero knowledge Proof(ZKP) (L3). Το πρόβλημα ήταν ότι προκαλούσε σύγχυση, καθώς έδινε την εντύπωση στους νέους προγραμματιστές ότι τα L2 και L3 ήταν συνδεδεμένα με τον υποκείμενο κώδικα blockchain του Indy. Ο σαφέστερος διαχωρισμός των 4 επιπέδων αποσαφηνίζει το γεγονός ότι κάθε ένα από αυτά τα επίπεδα είναι διαλειτουργικό μεταξύ των SSI ledgers, των επαληθεύσιμων διαπιστευτηρίων κ.α. Έτσι, τώρα το Hyperledger Indy είναι υπεύθυνο για το L1 και το Hyperledger Aries είναι υπεύθυνο για τα L2 και L3. Το Aries ήταν η πρώτη υλοποίηση πορτοφολιών ανοικτού κώδικα που χρησιμοποιούσε την αρχιτεκτονική Decentralized Key Management System(DKMS).



Εικόνα 1. Self-Sovereign Identity

4. Ανάλυση και Σχεδίαση

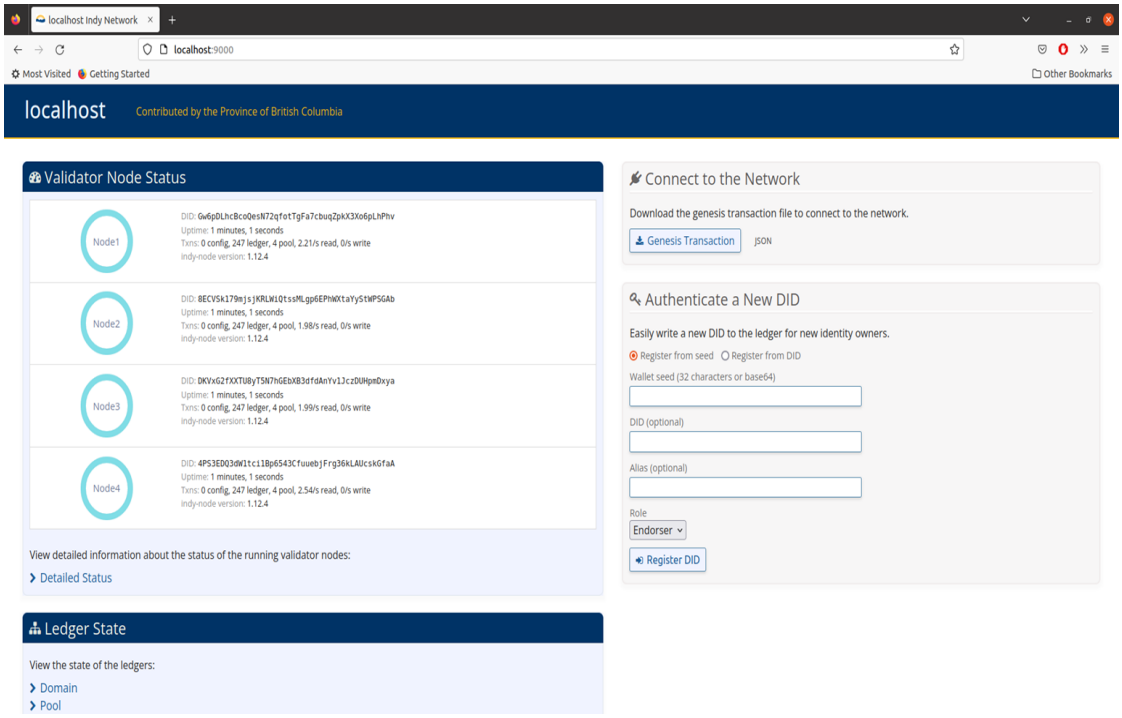
4.1. Τεχνική Υλοποίηση

Για την υλοποίηση της εφαρμογής αρχικά χρειάστηκε η εγκατάσταση του λειτουργικού συστήματος Linux και πιο συγκεκριμένα το Ubuntu 20.04.4 LTS. Στη συνέχεια εγκαταστάθηκε το περιβάλλον Docker και Docker compose τα οποία συμβάλλουν στην ευκολότερη διαχείριση των απαιτούμενων προγραμμάτων που χρειάστηκαν. Ακόμη, εγκαταστάθηκε η βάση της εφαρμογής, Hyperledger(Indy, Ursa, Aries), που προσφέρει τις γενικές λειτουργίες του δικτύου SSI, καθώς επίσης και το γραφικό περιβάλλον Von network το οποίο απαιτείται για την διαχείριση του ledger που περιλαμβάνει ένα Indy δίκτυο. Για την υλοποίηση των οντοτήτων της εφαρμογής (Agents) χρησιμοποιήθηκε η γλωσσά προγραμματισμού Python, ενώ για την υλοποίηση του γραφικού περιβάλλοντος του ιστοτόπου χρησιμοποιήθηκε η γλωσσά προγραμματισμού Javascript. Επιπλέον έγινε χρήση της βιβλιοθήκης ανάπτυξης γραφικού περιβάλλοντος ReactJS. Τέλος ο κώδικας της εφαρμογής για το Self Sovereing Identity βρίσκεται διαθέσιμος στο Github στο σύνδεσμο :

https://github.com/manosl7/hyperledger-ssi-app

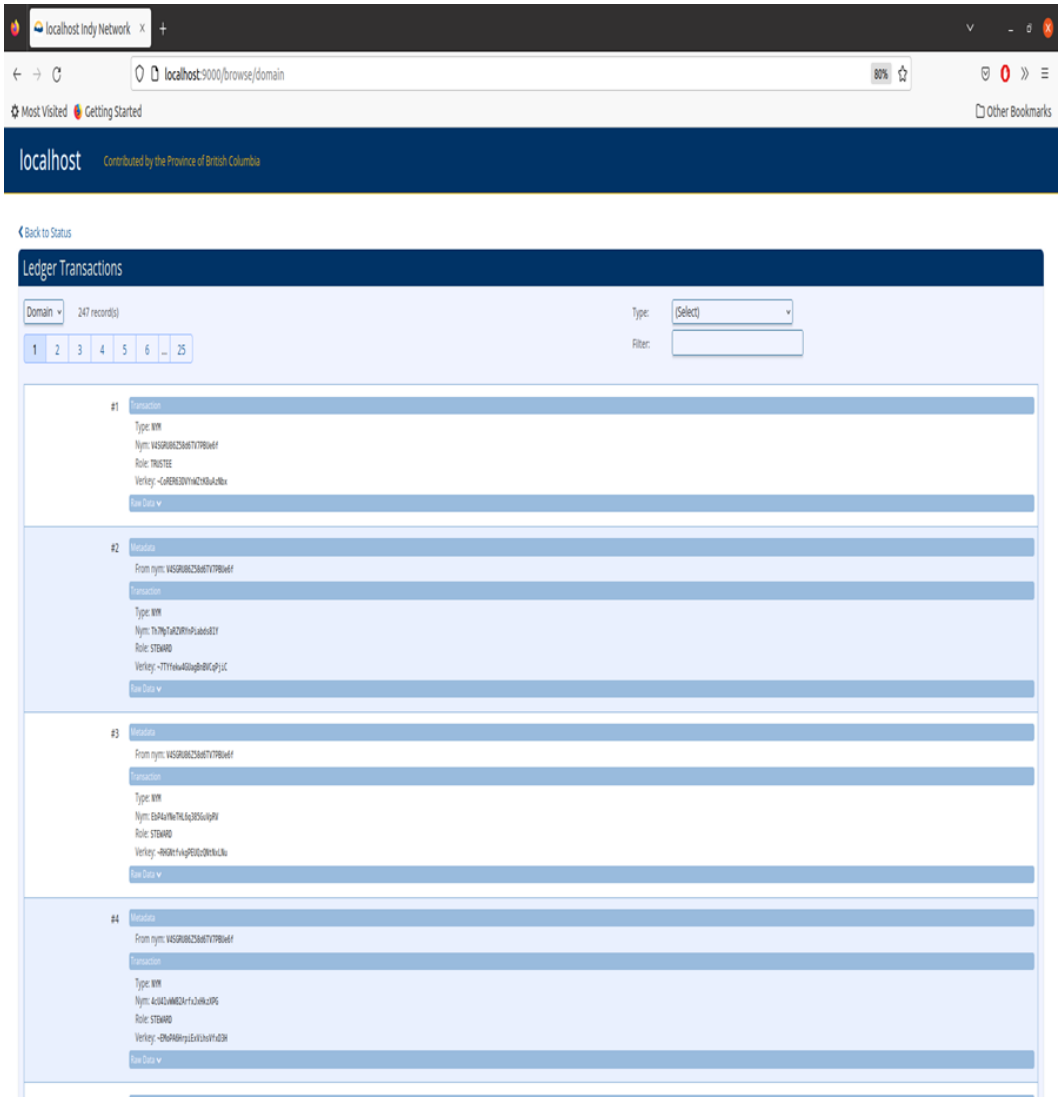
4.2. Λειτουργικότητα Δικτύου

Για το blockchain δίκτυο που τρέχει στο σύστημα έχουν δημιουργηθεί ξεχωριστά περιβάλλοντα για κάθε έναν Agent καθώς επίσης και για τους κόμβους (indy nodes) του blockchain και για τον server του δικτύου von network. Επιπρόσθετα για την εποπτεία του ledger και των nodes υπάρχει ένα γραφικό περιβάλλον το οποίο μπορούμε να το δούμε πληκτρολογώντας σε έναν Browser το link : localhost:9001 το οποίο βλέπουμε στο παρακάτω στιγμιότυπο οθόνης.



Εικόνα 2. Γραφικό περιβάλλον εποπτείας των κόμβων.

Στο γραφικό περιβάλλον που αναφέρθηκε προηγουμένως για την εποπτεία των nodes και του ledger παρατηρείτε ότι στην καρτέλα Ledger State επιλέγοντας το link Domain ανοίγει μια νέα σελίδα με τα transactions που έχουν πραγματοποιηθεί συνολικά στον ledger. Με αυτό το γραφικό περιβάλλον έχουμε την δυνατότητα να διενεργήσουμε δοκιμές και να επιβεβαιώσουμε ότι το δίκτυο λειτουργεί σωστά.



Εικόνα 3. Blockchain Transactions.

5. Ανάπτυξη Εφαρμογής

5.1. Προσέγγιση Εφαρμογής

Η παρούσα εφαρμογή παραθέτει ουσιαστικά μία από τις περιπτώσεις χρήσης του δικτύου SSI. Οι Agents που συμμετέχουν στο blockchain δίκτυο αποτελούνται από οργανισμούς, ιδιώτες και υπηρεσίες. Με την χρήση της αποκεντρωμένης ταυτότητας (DID) οι συμμετέχοντες μπορούν να αξιοποιήσουν τις δυνατότητες του δικτύου ανάλογα με τις ανάγκες τους. Ένα παράδειγμα αποτελεί και η χρήση των πιστοποιημένων προσωπικών πληροφοριών σε υπηρεσίες που απαιτούν συγκεκριμένες πληροφορίες ή χαρακτηριστικά των χρηστών. Πιο συγκεκριμένα στην παρούσα εφαρμογή η περίπτωση χρήσης αναφέρεται σε μια υλοποίηση του δικτύου SSI στο οποίο :

- Η απαραίτητη πληροφορία η οποία χρησιμοποιείται για την εμπιστοσύνη μεταξύ των οντοτήτων εμπεριέχεται μέσα στον ledger.
- Η διαδικασία της καταχώρησης των στοιχείων και η διαδικασία του διαμοιρασμού αυτών των στοιχείων πραγματοποιούνται ξεχωριστά. Δηλαδή οι κάτοχοι πρώτα

αποκτούνε τα δεδομένα τους και στη συνέχεια τα αποθηκεύουν σε ψηφιακά πορτοφόλια και εφόσον χρειαστεί τα χρησιμοποιούν.

- Η επικοινωνία πραγματοποιείται με το πανεπιστήμιο των δύο υποψηφίων και στη συνέχεια οι δύο υποψήφιοι συνδέονται με την εταιρεία που θέλει να ελέγξει την ορθότητα των πτυχίων τους. Άμεση επικοινωνία μεταξύ του πανεπιστημίου (UNIPI) και της εταιρείας που θέλει να προσλάβει ένα υποψήφιο (IBM) δεν υπάρχει διότι ανήκουν στο ίδιο δίκτυο και έτσι εμπιστεύονται ο ένας τον άλλον.
- Τα αιτήματα επαλήθευσης (proof requests) μπορούν να συγκρίνουν δεδομένα ούτως ώστε να αποδειχθούν μερικά από τα χαρακτηριστικά της ταυτότητας του χρήστη χωρίς να αποκαλυφθούν τα δεδομένα αυτά. Δηλαδή η εταιρεία που ενδιαφέρεται για την πρόσληψη ενός υποψηφίου (IBM) θα μπορέσει να ενημερωθεί μόνο για το αν ο μέσος όρος του βαθμού πτυχίου του κάθε υποψηφίου είναι μεγαλύτερος από 6 και όχι την τιμή του.

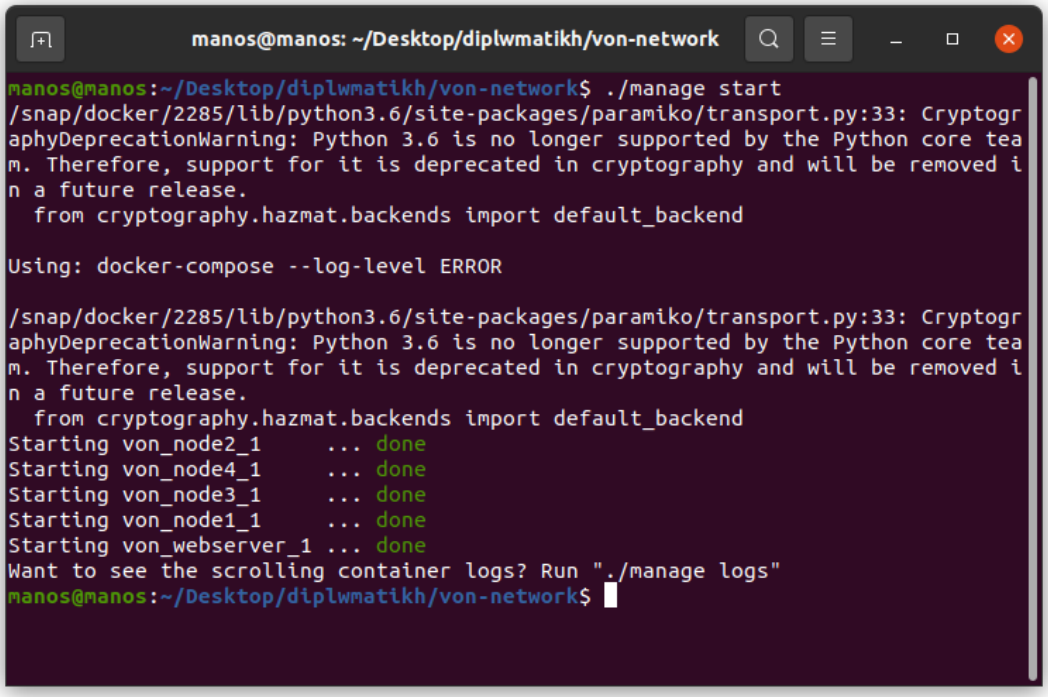
5.2. Αναλυτική Παρουσίαση

Στην παρούσα διπλωματική διατριβή υλοποιήθηκε μία εφαρμογή με την οποία θα παρουσιαστεί με ποιόν τρόπο μπορεί να πραγματοποιηθεί η κάλυψη συγκεκριμένων απαιτήσεων μεταξύ ενός εργοδότη και ενός εργαζομένου. Μία περίπτωση στην οποία μία εταιρεία απαιτεί από τους υποψήφιους εργαζομένους την υποβολή διαφόρων πιστοποιήσεων όπως ο βαθμός πτυχίου, το πανεπιστήμιο (UNIPI) κ.α.

Πιο συγκεκριμένα στο δίκτυο που έχει υλοποιηθεί έχουν εγγραφεί οι εξής οντότητες: 1) Το Πανεπιστήμιο UNIPI, 2) Οι φοιτητές Manos, Nick και 3) η Εταιρεία IBM. Στη συνέχεια το Πανεπιστήμιο UNIPI θα προσκαλέσει τους δύο φοιτητές Manos, Nick να συνδεθούν μαζί του με σκοπό την έκδοση των διαπιστευτηρίων τους δηλαδή την επικύρωση των πτυχίων των δύο φοιτητών. Στη συνέχεια αφού αποδεχθούν την πρόσκληση του πανεπιστημίου και διαπιστώσει το UNIPI ότι η σύνδεση ήταν επιτυχής για τον κάθε έναν αντίστοιχα τότε θα ληφθούν τα διαπιστευτήρια του κάθε φοιτητή και θα αποθηκευτούν στα ψηφιακά τους πορτοφόλια. Οι φοιτητές έχουν την δυνατότητα να παρουσιάσουν τις σχετικές πληροφορίες που έλαβαν σε ενδιαφερόμενες υπηρεσίες όπως είναι στην προκειμένη περίπτωση μία εταιρεία πληροφορικής (IBM) η οποία αναζητεί νέους εργαζομένους με πτυχίο στον τομέα της και μέσο όρο πτυχίου ίσο ή μεγαλύτερο από πέντε (5). Η IBM λοιπόν για να λάβει τα διαπιστευτήρια και να ελέγξει εάν οι υποψήφιοι πληρούν τα κριτήρια που έχει θέσει πρέπει πρώτα να πραγματοποιήσει μία σύνδεση με τον κάθε έναν. Αφού προσκαλέσει τους υποψήφιους να συνδεθούν μαζί της και ο Manos και Nick αποδεχθούν την πρόσκληση τότε θα εμφανιστούν στην εφαρμογή της εταιρείας οι συνδέσεις και οι μοναδικές ταυτότητες για κάθε υποψήφιο. Στη συνέχεια η IBM θα στείλει ένα μήνυμα επαλήθευσης των στοιχείων στον κάθε υποψήφιο, με βάση την μοναδική τους ταυτότητα, το οποίο θα περιλαμβάνει και τα κριτήρια που έχει θεσπίσει για την πρόσληψη ενός υποψηφίου. Τέλος με την αποδοχή του μηνύματος επαλήθευσης από τους δύο φοιτητές θα εμφανιστούν στην εφαρμογή της εταιρείας IBM τα αποδεικτικά στοιχεία με τις ενδείξεις “Status: Verified” εάν ο υποψήφιος πληρεί τα κριτήρια ή “Status: Failed” εάν δεν τα πληρεί.

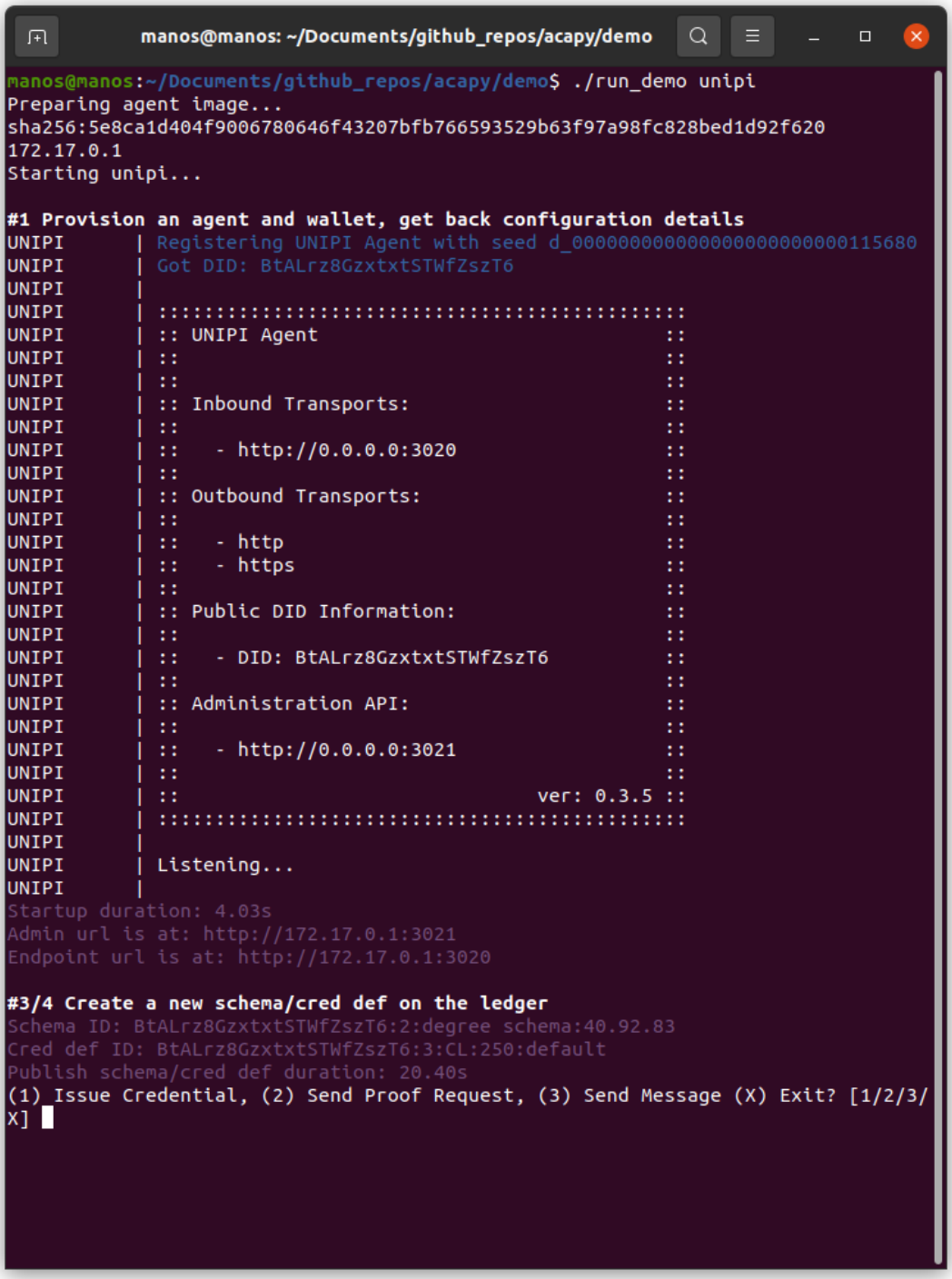
Η εφαρμογή αυτή θα μπορούσε να αξιοποιηθεί από πολλούς οργανισμούς, πανεπιστήμια και επιχειρήσεις με διαφορετικό σκοπό από τον καθένα. Στον τομέα της εκπαίδευσης, μπορούν να γίνουν διαχειρίσιμες οι διαδικασίες έκδοσης πιστοποιητικών και επαλήθευσής τους. Θα μπορεί αυτόματα να ελεγχθεί αν κάποιος έχει έγκυρο πτυχίο ή πιστοποιητικό εκπαίδευσης. Επίσης στον εργασιακό τομέα οι επιχειρήσεις που αναζητούν προσωπικό θα μπορούν να ελέγξουν την εγκυρότητα των εγγράφων του κάθε υποψηφίου και θέτοντας κάποιες απαιτήσεις να δουν αν αυτές πληρούνται χωρίς να χρειαστεί να αποκαλυφθούν ευαίσθητες πληροφορίες του κάθε υποψηφίου. Ακόμη θα μπορεί να γίνεται επαλήθευση των διαπιστευτηρίων από οργανισμούς ή εταιρίες ακόμη και αν αυτά ενδέχεται να παρουσιάζονται χρόνια μετά την έκδοσή τους ή το εκπαιδευτικό ίδρυμα που τα έχει εκδώσει να μην υπάρχει πλέον ή να έχει χάσει με κάποιο τρόπο τα αρχεία του.

Αρχικά θα πρέπει να ενεργοποιηθεί το γραφικό περιβάλλον Von network το οποίο απαιτείται για την διαχείριση του ledger. Η ενεργοποίηση πραγματοποιείται με την ακόλουθη εντολή.



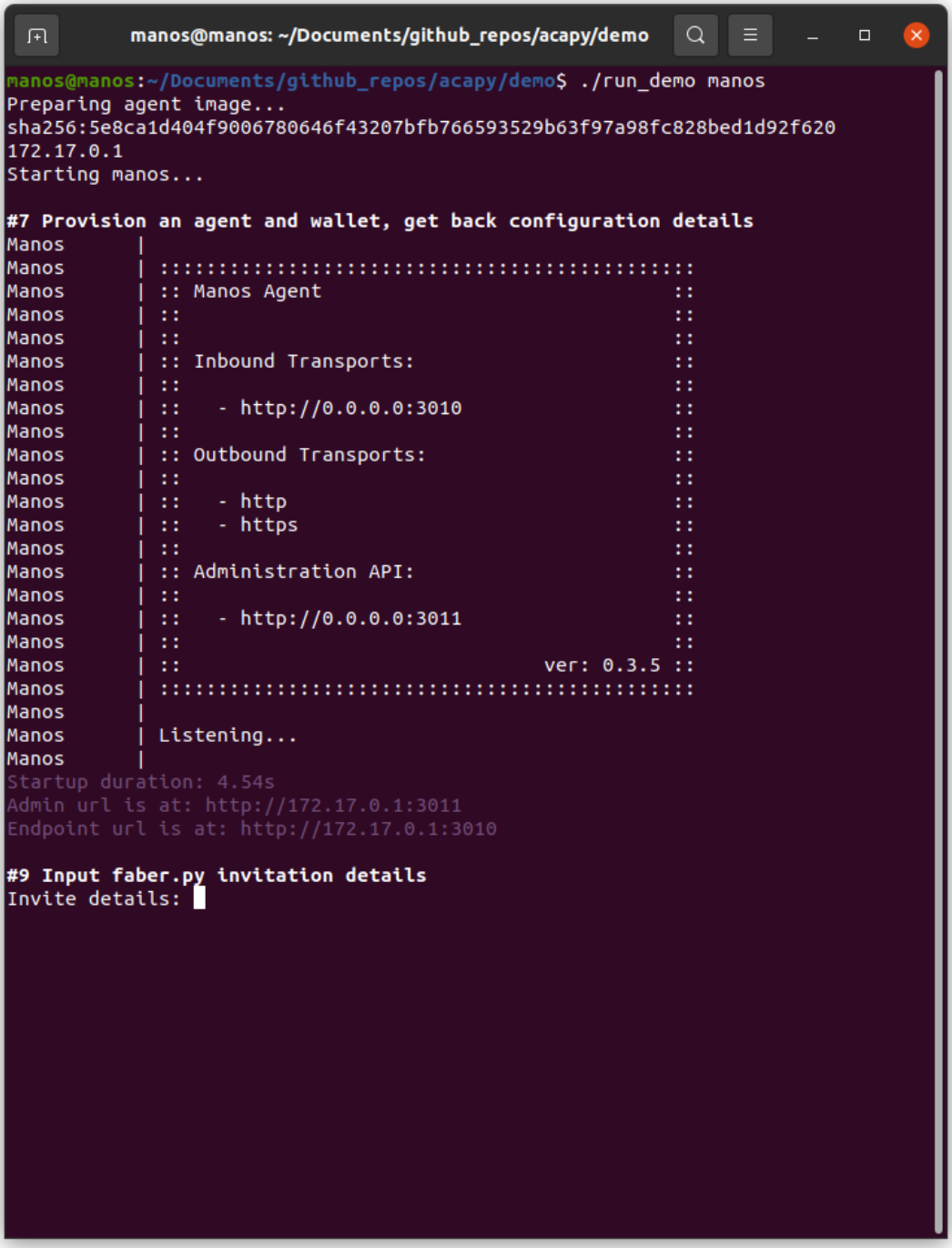
Εικόνα 4. Von Network.

Έπειτα, ανοίγουμε ένα νέο τερματικό και με την εντολή “./run_demo” μπορούμε να ξεκινήσουμε έναν Agent ο οποίος στο τερματικό όπως φαίνεται και στο παρακάτω στιγμιότυπο τυπώνει κάποιες πληροφορίες σχετικά με το port που χρησιμοποιεί, το DID που έχει κ.α.

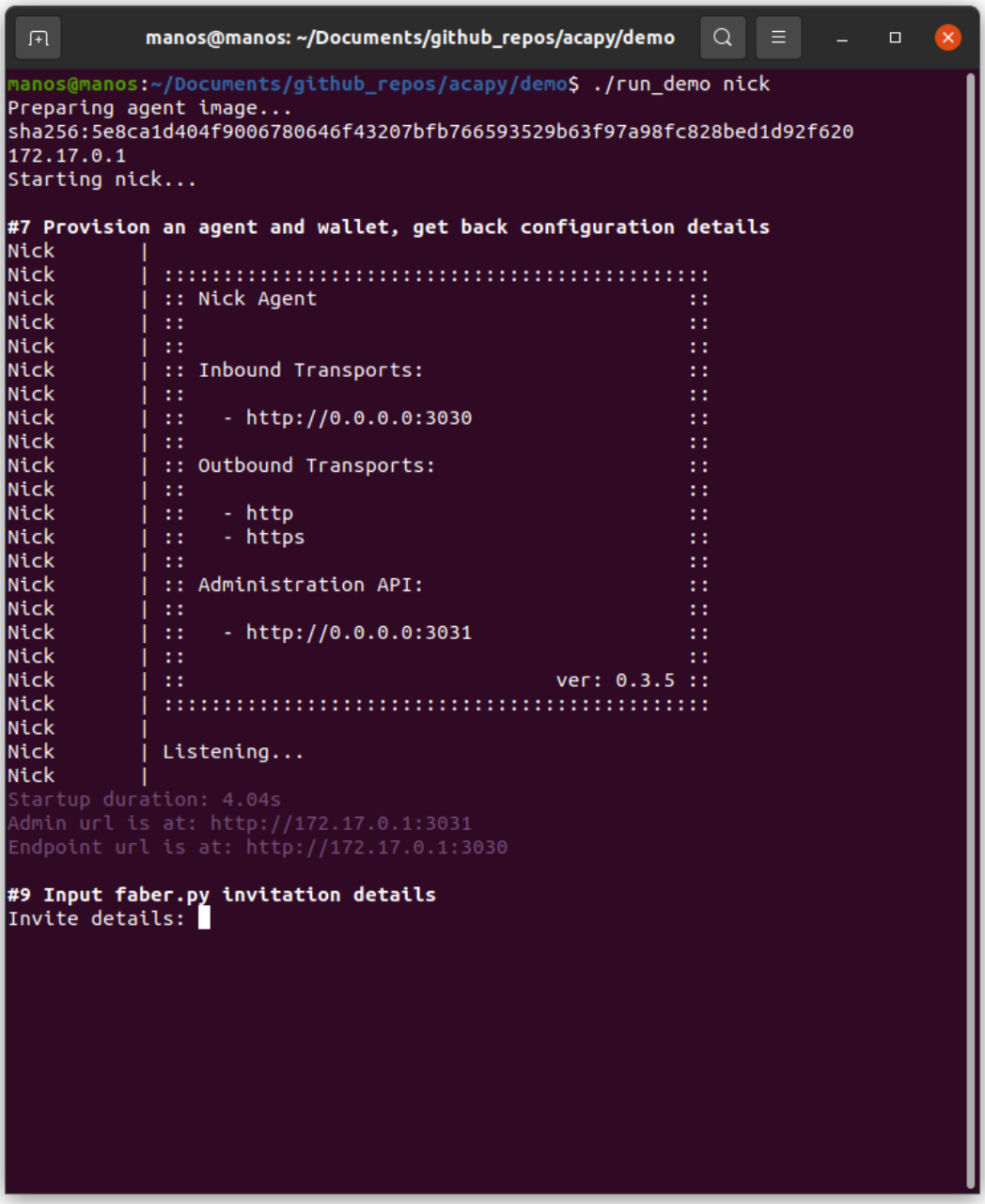


Εικόνα 5. Εκκίνηση του Agent UNIPI στο τερματικό

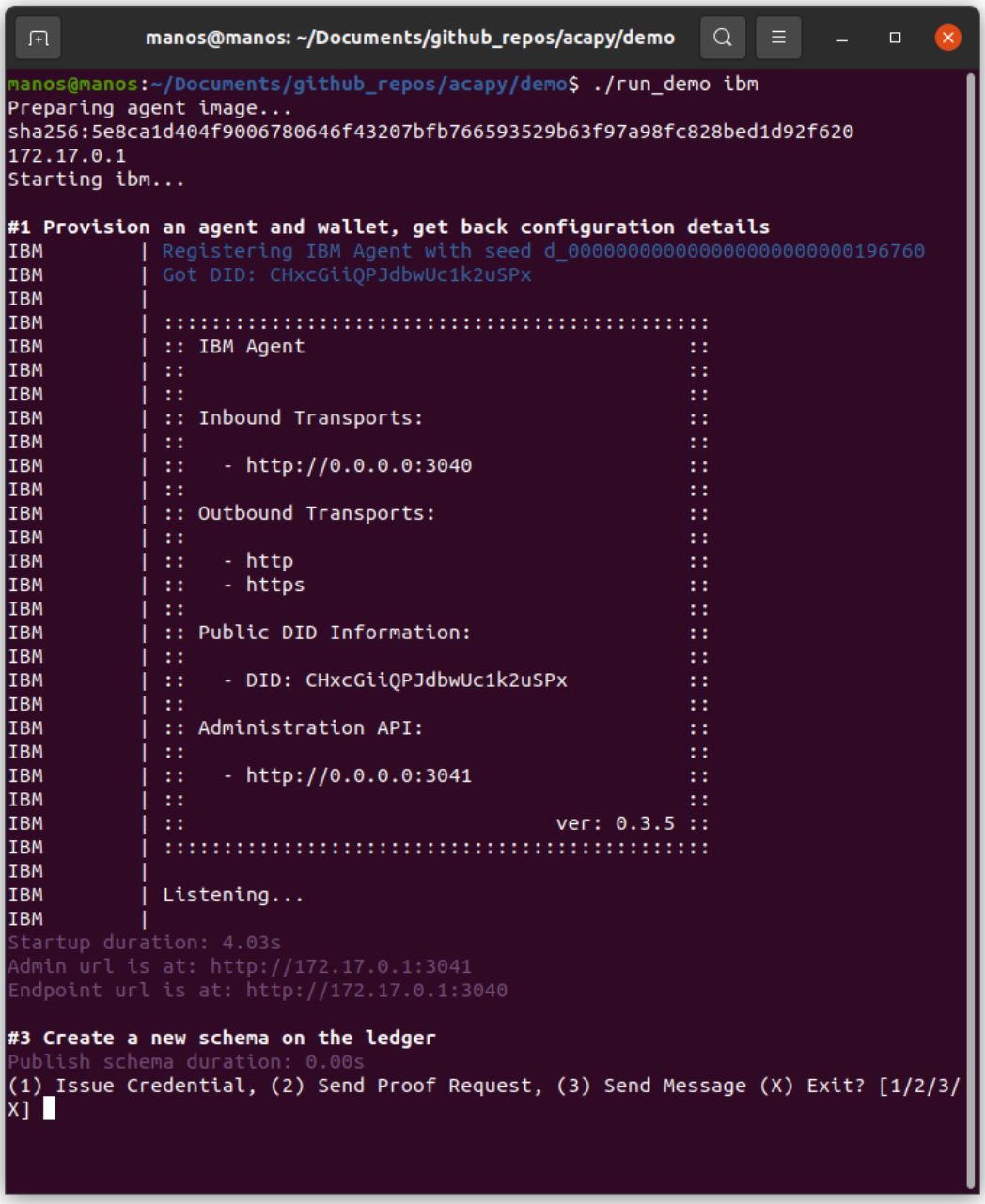
Η παραπάνω διαδικασία πραγματοποιείται ξεχωριστά για κάθε έναν Agent αντίστοιχα και διακρίνεται στα επόμενα στιγμιότυπα που παραθέτονται. Ακόμη κατά την εκκίνηση ενός Agent στον τερματικό εμφανίζεται ένα link το οποίο εμπεριέχει ένα διαδραστικό documentation των λειτουργιών και υπηρεσιών που είναι διαθέσιμες. Οι λειτουργίες αυτές διατίθενται μέσω του πρωτοκόλλου HTTP ώστε να είναι δυνατή η χρήση τους από πελάτες διαφόρων περιβαλλόντων όπως κινητές εφαρμογές, IOT μηχανές, websites κ.α.



Εικόνα 6. Εκκίνηση του Agent Manos στο τερματικό.

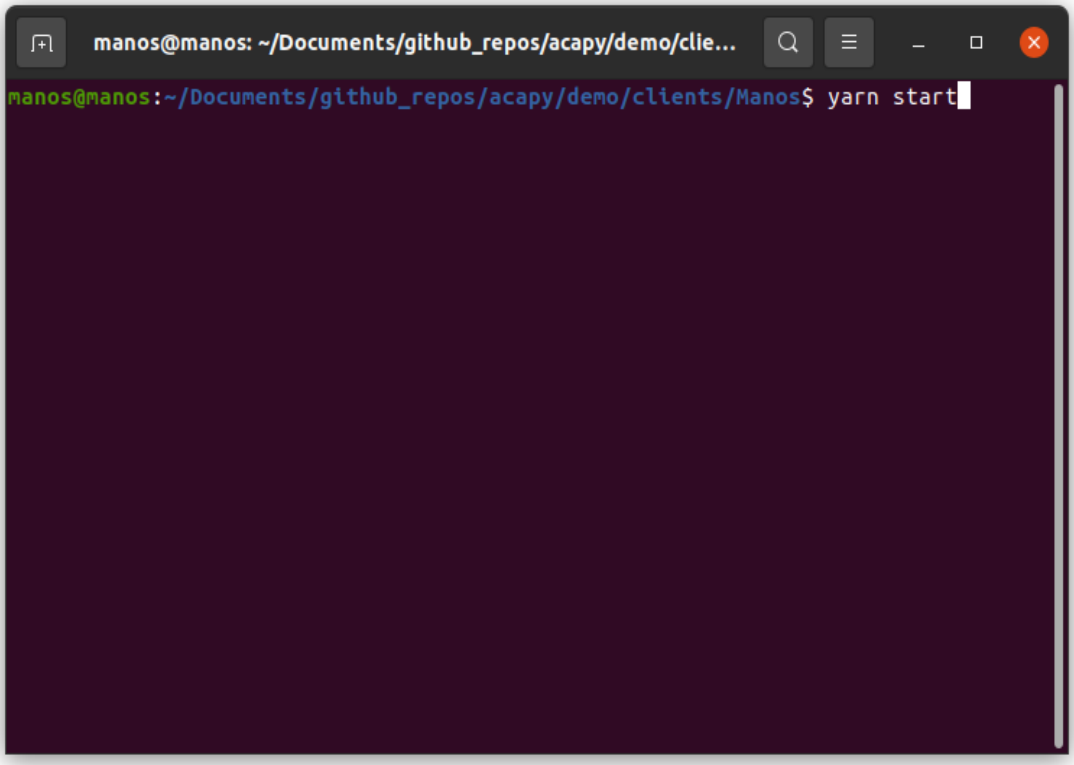


Εικόνα 7. Εκκίνηση του Agent Nick στο τερματικό.



Εικόνα 8. Εκκίνηση του Agent IBM στο τερματικό.

Στη συνέχεια, θα τεθούν σε λειτουργία οι clients όπου στο παράδειγμά αυτό αποτελούν ιστοσελίδες προσβάσιμες από όλους τους Browser οποιαδήποτε συσκευής όπως κινητό, υπολογιστή κ.α. Η εντολή με την οποία ξεκινάμε τους clients είναι η “yarn start“ η οποία εκτελείται για κάθε έναν ξεχωριστά σε διαφορετικό τερματικό παράθυρο αντίστοιχα.

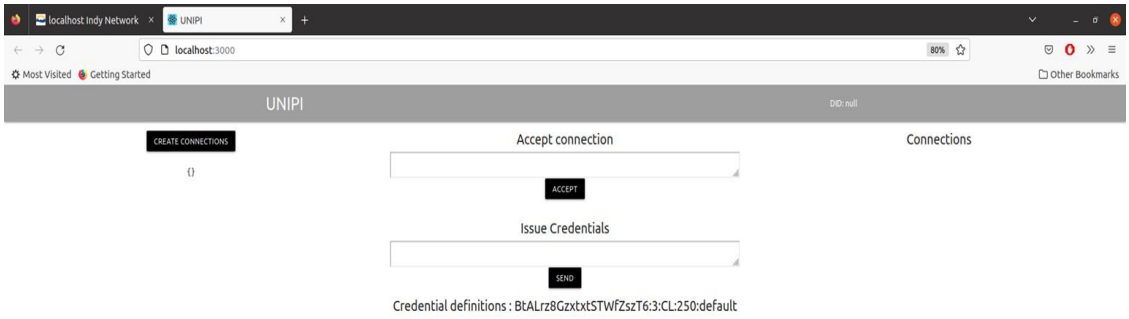


Εικόνα 9. Εκκίνηση του Client Manos στο τερματικό.

Έπειτα, με την επιτυχής έναρξη του κάθε client ξεχωριστά αναδύεται αυτόματα για κάθε έναν μία ιστοσελίδα με το γραφικό περιβάλλον που έχει υλοποιηθεί όπως διαπιστώνεται και στην επόμενη εικόνα. Στην εφαρμογή του πανεπιστημίου (UNIPI) παρατηρούμε ότι πάνω αριστερά στην ιστοσελίδα εμφανίζεται το registered DID. Ακόμη διακρίνεται η επιλογή για δημιουργία πρόσκλησης (Create Connection) καθώς επίσης η αποδοχή προσκλήσεων από άλλους χρήστες του δικτύου (Accept connection). Τέλος παρατηρείται ότι υπάρχει η επιλογή Issue Credentials για την έκδοση των διαπιστευτηρίων και δεξιά η λίστα με τους χρήστες που έχουν συνδεθεί με τον συγκεκριμένο client.

Στην ιστοσελίδα που δημιουργήθηκε για τους δύο υποψηφίους,Manos και Nick, βλέπουμε τα εξής πεδία :

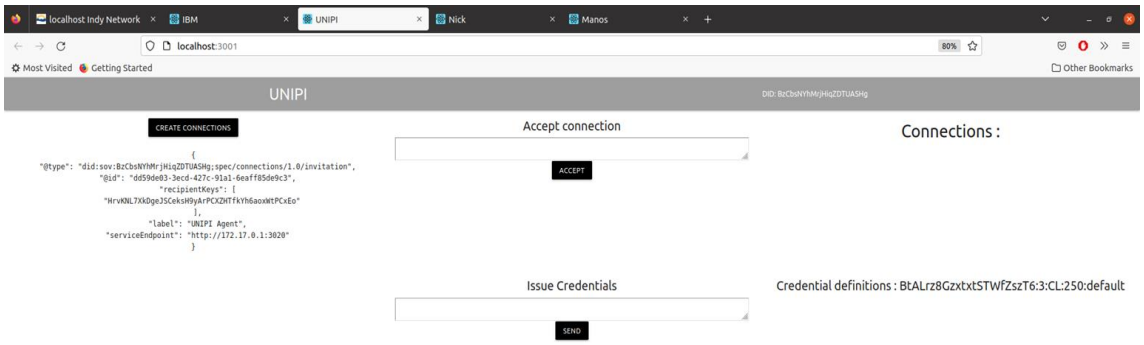
- Την αποδοχή προσκλήσεων από άλλους χρήστες του δικτύου (Accept connection)
- Δημιουργία πρόσκλησης (Create Connection)
- Την λίστα με τις ολοκληρωμένες συνδέσεις με άλλες οντότητες
- Τα διαπιστευτήρια (My Credentials)



Εικόνα 10. Γραφικό περιβάλλον της εφαρμογής UNIPI.

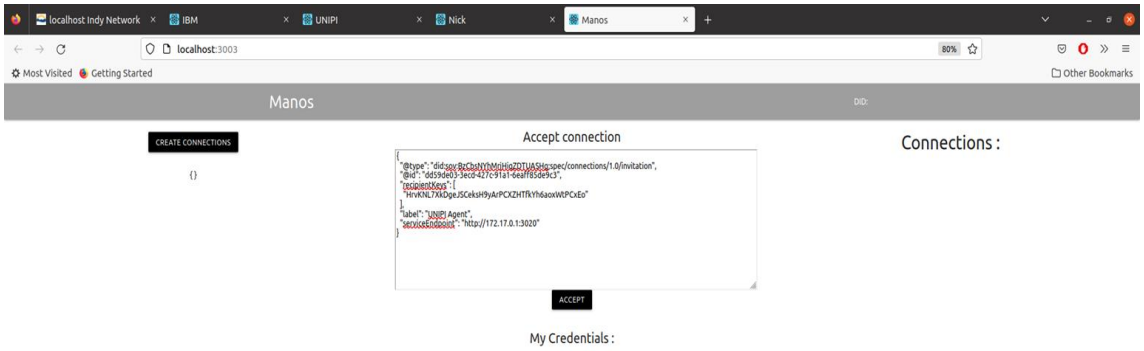
Αρχικά το πανεπιστήμιο (UNIPI) προσκαλεί τους 2 υποψηφίους φοιτητές να συνδεθούν μαζί τους ώστε να εκδώσει τα διαπιστευτήριά τους (issue credentials).

Έτσι δημιουργεί προσκλήσεις οι οποίες αποστέλλονται στους δύο φοιτητές.

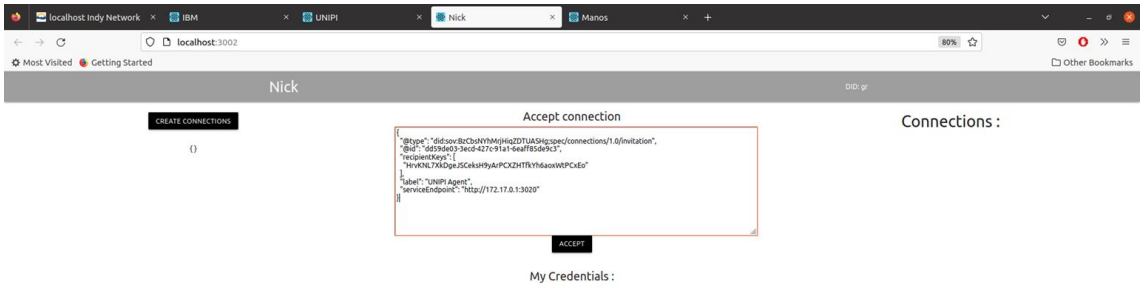


Εικόνα 11. Δημιουργία σύνδεσης με τους χρήστες.

Οι φοιτητές Manos και Nick με την σειρά τους αποδέχονται την πρόσκληση όπως φαίνεται και στα παρακάτω στιγμιότυπα.

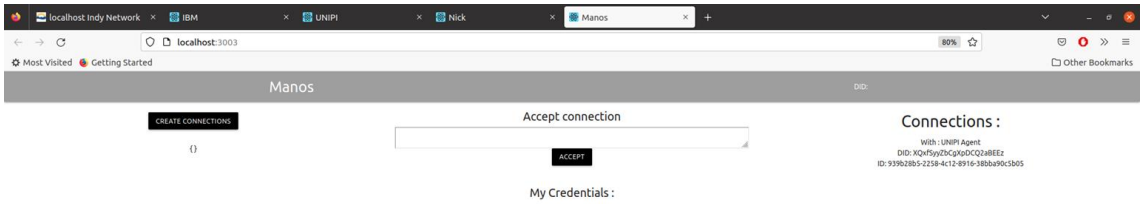


Εικόνα 12. Αποδοχή πρόσκλησης UNIPI με Manos

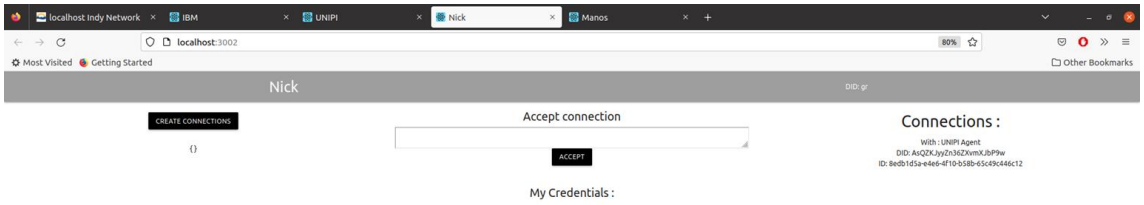


Εικόνα 13. Αποδοχή πρόσκλησης UNIPI με Nick.

Στο γραφικό περιβάλλον του Manos και του Nick παρατηρούμε ότι έχει επιτευχθεί η σύνδεση με το πανεπιστήμιο UNIPI.

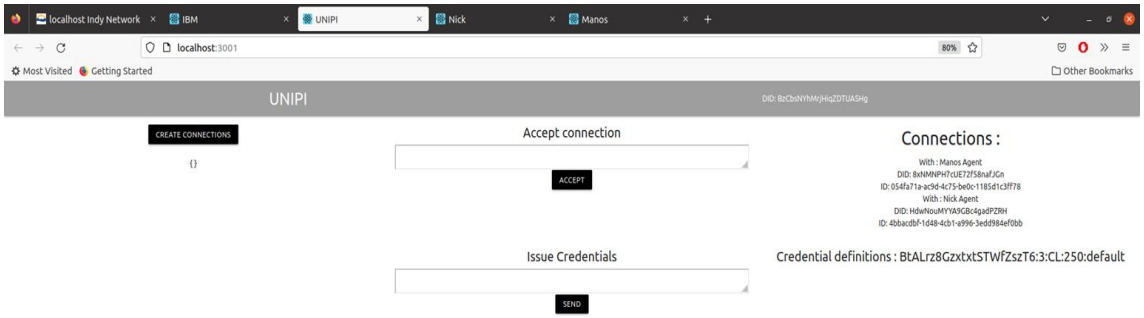


Εικόνα 14. Επίτευξη σύνδεσης UNIPI με Manos.



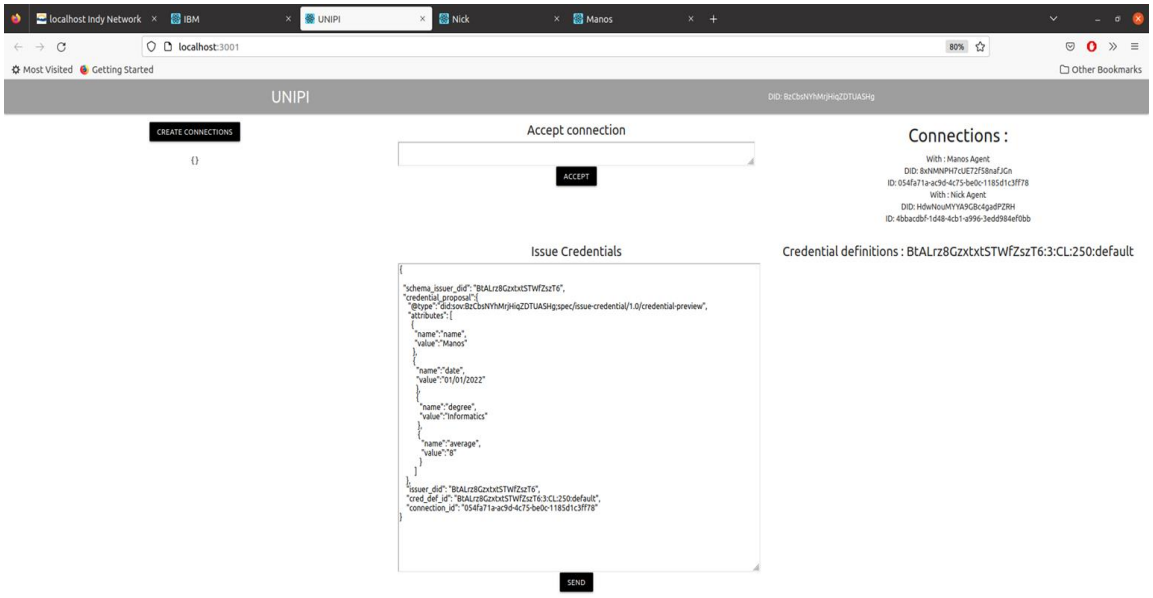
Εικόνα 15. Επίτευξη σύνδεσης UNIPI με Nick.

Στο γραφικό περιβάλλον του πανεπιστημίου παρατηρούμε και εδώ ότι έχουν επιτευχθεί οι συνδέσεις με τους δύο φοιτητές με αποτέλεσμα να αποκτήσουν μοναδικές ταυτότητες όπου θα χρησιμοποιηθούν στη συνέχεια για ανταλλαγή μηνυμάτων.

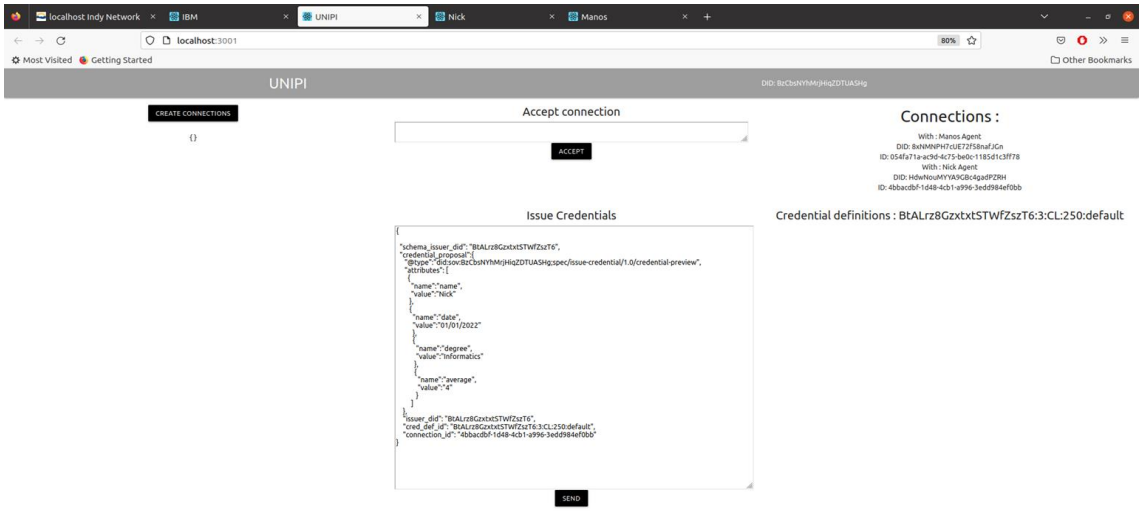


Εικόνα 16. Επίτευξη σύνδεσης UNIPI με φοιτητές.

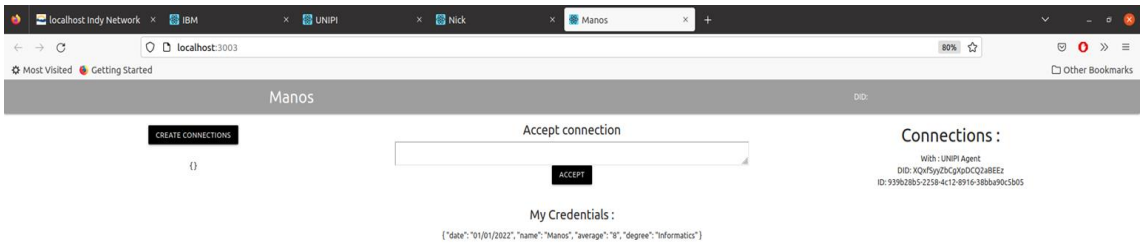
Στη συνέχεια το πανεπιστήμιο πραγματοποιεί την έκδοση των διαπιστευτηρίων (issue credentials) για τους δύο φοιτητές που προηγουμένως είχε δημιουργήσει μια σύνδεση μαζί τους. Με αυτό το βήμα επιτυγχάνεται η ασφαλής έκδοση των διαπιστευτηρίων ώστε να χρησιμοποιηθούν από τους φοιτητές. Για την εκτέλεση της εντολής αυτής χρησιμοποιείται το connection id που εκφράζει την σχέση του πανεπιστημίου με τον κάθε χρήστη, το credential definition id που εκφράζει το σχήμα των δεδομένων και τέλος η πληροφορία που κατέχει το πανεπιστήμιο για τους φοιτητές όπως είναι το όνομα του σπουδαστή, το έτος αποφοίτησης, τον τίτλο πτυχίου και τον μέσο όρο του βαθμού.



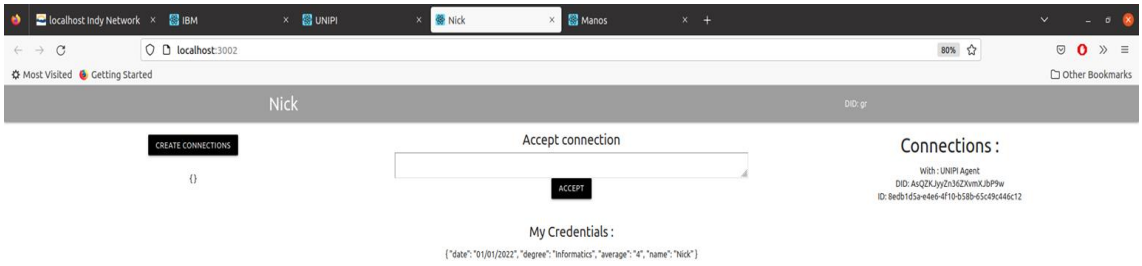
Εικόνα 17. Έκδοση διαπιστευτηρίων για τον agent Manos.



Εικόνα 18. Έκδοση διαπιστευτηρίων για τον agent Nick.



Εικόνα 19. Τα διαπιστευτήρια για τον agent Manos.



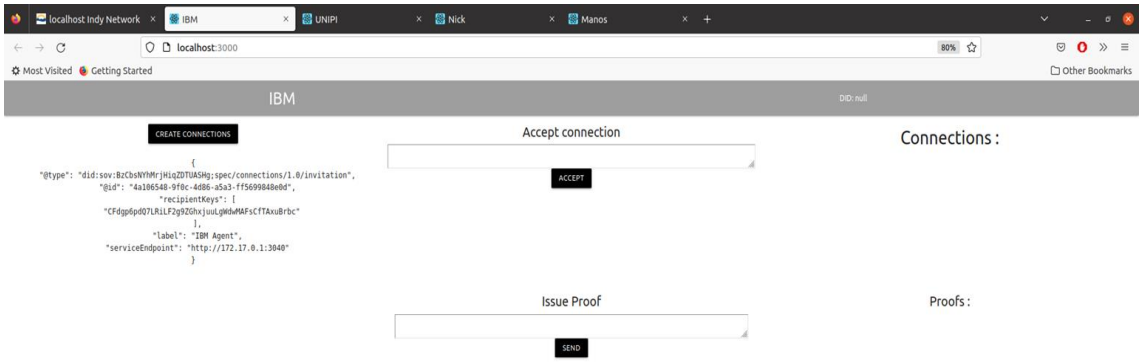
Εικόνα 20. Τα διαπιστευτήρια για τον agent Nick.

Έχοντας ολοκληρώσει τη σύνδεση των δύο φοιτητών με το πανεπιστήμιο και εφόσον έχει πραγματοποιηθεί η έκδοση των διαπιστευτηρίων τους και έχουν πλέον στην κατοχή τους την απαραίτητη πληροφορία που χρειάζονται, έρχεται με την σειρά της η IBM ώστε να ζητήσει ένα proof request από τους δύο υποψηφίους Manos και Nick με τις απαιτήσεις που έχει θέσει για να πραγματοποιήσει την πρόσληψη ενός εργαζομένου.

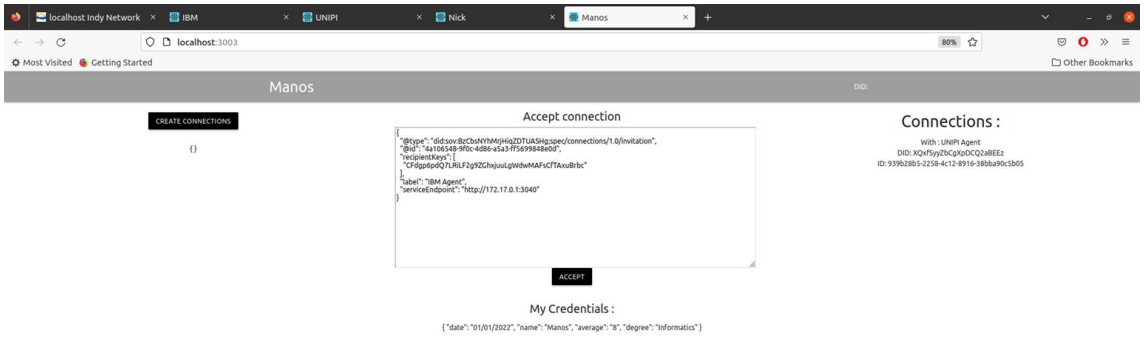
Στο γραφικό περιβάλλον της εταιρείας IBM παρατηρούνται οι εξής λειτουργίες:

- Επιλογή για δημιουργία πρόσκλησης (Create Connection)
- Αποδοχή προσκλήσεων από άλλους χρήστες του δικτύου (Accept connection).
- Δημιουργία φόρμας για αποστολή ενός proof request.
- Οι χρήστες που έχουν συνδεθεί με τον συγκεκριμένο client.
- Τα proof request από τους υποψηφίους με τα status τους.

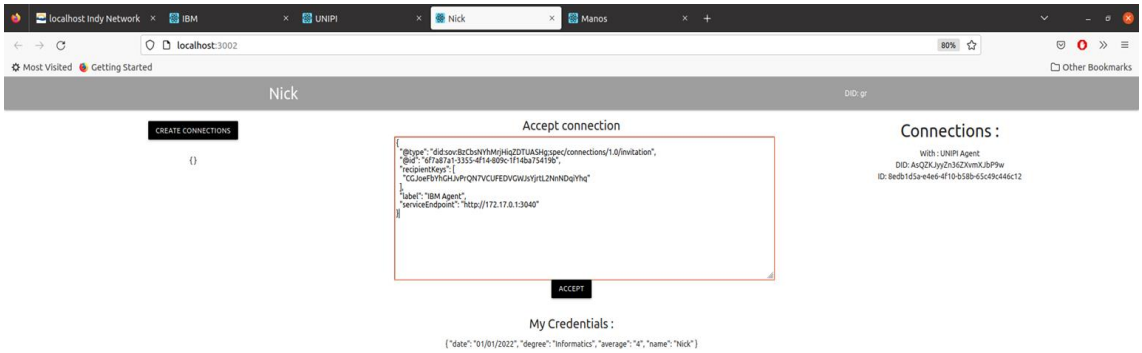
Αρχικά για να μπορέσει η εταιρεία να ζητήσει τα proof requests από τους φοιτητές θα πρέπει πρώτα να δημιουργηθεί μία σύνδεση μεταξύ τους ώστε να αρχικοποιηθεί το ασφαλές κανάλι επικοινωνίας. Αναλυτικότερα, δημιουργείται μια πρόσκληση για τον Mano και Nick όπου στη συνέχεια αποδέχονται από την πλευρά τους και καταλήγουμε να έχουν πραγματοποιηθεί οι συνδέσεις (connections) μεταξύ των IBM – Manos και IBM – Nick. Η παραπάνω διαδικασία παρατηρείται στα επόμενα στιγμιότυπα που ακολουθούν.



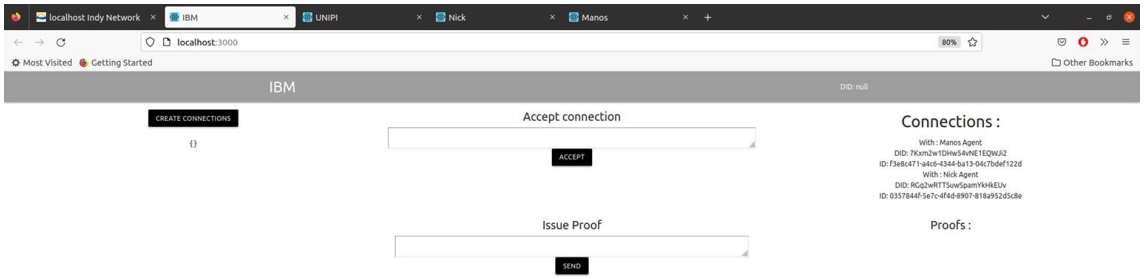
Εικόνα 21. Δημιουργία σύνδεσης της IBM με τους υποψηφίους.



Εικόνα 22. Αποδοχή σύνδεσης μεταξύ των IBM - Manos.

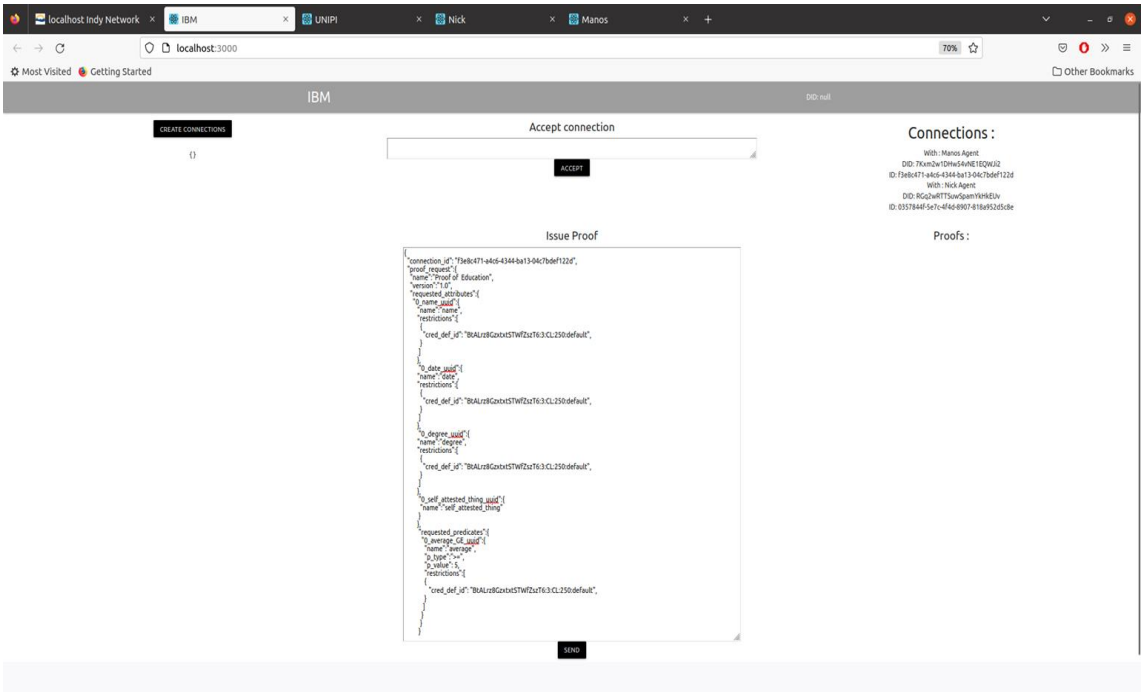


Εικόνα 23. Αποδοχή σύνδεσης μεταξύ των IBM - Nick.

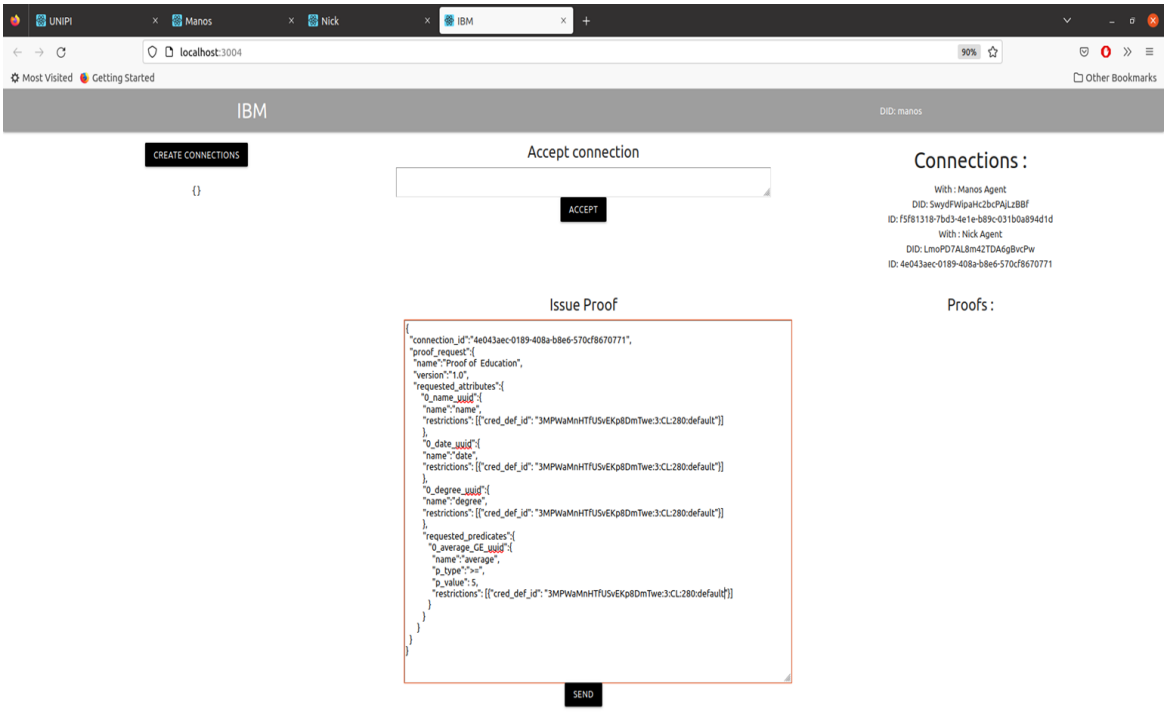


Εικόνα 24. Εμφάνιση των συνδέσεων μεταξύ των IBM – υποψηφίων και ανάθεση μοναδικής ταυτότητας για κάθε έναν αντίστοιχα.

Στη συνέχεια θα πρέπει να πραγματοποιηθεί η αίτηση για τα proof requests στους φοιτητές Manos και Nick. Για την υλοποίηση αυτή θα χρησιμοποιηθούν τα connection IDs για την επιλογή της κάθε οντότητας καθώς επίσης και το Credential Definition ID για την αξιοποίηση των χαρακτηριστικών των δεδομένων τα οποία θα χρησιμοποιηθούν στο proof. Η εταιρεία IBM που αξιολογεί τους δύο υποψήφιους θέλει να μάθει το μέσο όρο του καθενός και εάν είναι μεγαλύτερος ή όχι του 5, χωρίς όμως να χρειαστεί να δει τον ίδιο τον μέσο όρο. Θα πρέπει να στείλει λοιπόν στο κάθε ένα υποψήφιο ξεχωριστά το παρακάτω issue proof.

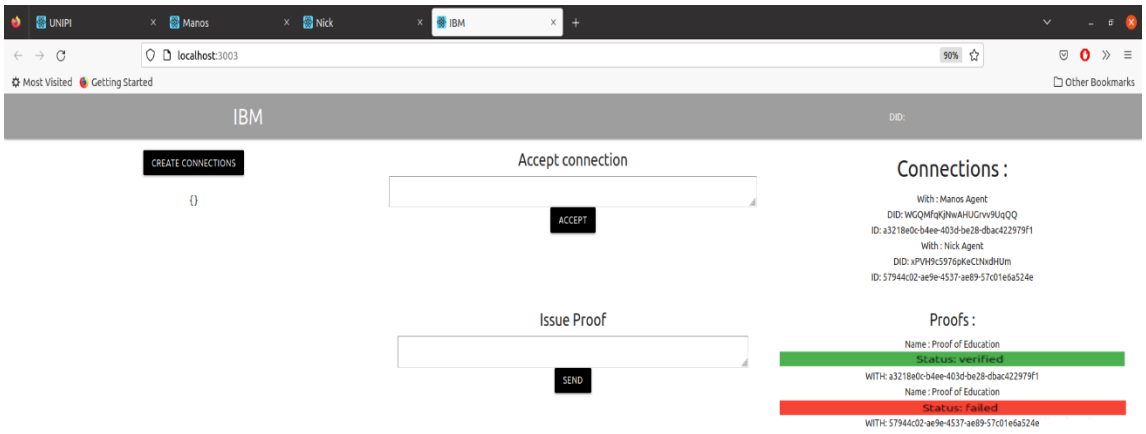


Εικόνα 25. Επαλήθευση στοιχείων από την IBM για τον φοιτητή Manos.



Εικόνα 26. Επαλήθευση στοιχείων για τον φοιτητή Nick.

Τέλος, στο σημείο αυτό οι δύο εφαρμογές των φοιτητών Manos και Nick χρησιμοποιώντας τις πληροφορίες των Digital Wallet που διαθέτουν διαμορφώνουν το κατάλληλο proof που τους ζητήθηκε από την την εταιρεία IBM και το αποστέλλουν πίσω σε αυτή. Με την σειρά της τώρα η εταιρεία επιβεβαιώνει τις πληροφορίες που έλαβε με αποτέλεσμα να εμφανιστεί το status για κάθε ένα presentation του κάθε υποψηφίου. Για τον πρώτο φοιτητή (Manos) το status του γίνεται Verified, ενώ για τον Nick το Verify αποτυγχάνει διότι ο μέσος όρος είναι πιο χαμηλός από αυτόν που ζητήθηκε από την εταιρεία IBM. Παρακάτω παρατίθεται και ένα στιγμιότυπο από τα αποτελέσματα του κάθε status για κάθε ένα χρήστη.



Εικόνα 27. Κατάσταση επαλήθευσης του IBM για τους Manos και Nick.

6. Συμπεράσματα

Αυτή η διπλωματική διατριβή είχε ως στόχο την υλοποίηση της αυτοδιαχειριζόμενης ταυτότητας πάνω στην τεχνολογία Blockchain. Αρχικά, μελετήθηκε η ιστορία της και οι δυνατότητες που προσφέρει στην ιδιωτικότητα λόγω των χαρακτηριστικών της. Στη συνέχεια, πραγματοποιήθηκε έρευνα για τις τεχνολογίες που χρησιμοποιούν Blockchain για να προσφέρουν υπηρεσίες αυτοδιαχειριζόμενης ταυτότητας (SSI). Έπειτα επιλέχθηκε να υλοποιηθεί ένα δίκτυο που πληρεί τα τελευταία ανοιχτά πρότυπα που σχετίζονται με υπηρεσίες SSI χρησιμοποιώντας σαν υποδομή το οικοσύστημα Hyperledger. Η τεχνολογία Blockchain είναι η φυσική εξέλιξη του διαδικτύου. Σχεδόν όλες οι εταιρείες ανά τον κόσμο στρέφονται προς τα ψηφιακά πλαίσια ταυτότητας που βασίζονται στην έννοια των αποκεντρωμένων αναγνωριστικών (DID) και του υπολογιστικού νέφους (cloud computing) για να αποθηκεύουν, να επεξεργάζονται και να αναλύουν τα δεδομένα τους και να εκτελούν τη ροή εργασιών τους. Το επόμενο βήμα στην εξέλιξη του διαδικτύου είναι να επιτραπεί στους καθημερινούς χρήστες να απολαύσουν τα πλεονεκτήματα της αποκεντρωμένης ταυτότητας γνωστών και ως αυτοδύναμη ταυτότητα (SSI). Οι άνθρωποι θα έχουν τον έλεγχο πάνω στην ψηφιακή ταυτότητά τους χωρίς να βασίζονται σε τρίτους. Η σταθερότητα του καθολικού συστήματος (ledger) σε συνδυασμό με τους αλγορίθμους συναίνεσης διασφαλίζει ότι η εμπιστοσύνη και η ιδιωτικότητα θα διατηρούνται σε υψηλότερο βαθμό από ό,τι προσφέρεται σήμερα.

7. Βιβλιογραφία

- Casino, Fran, Thomas K. Dasaklis, and Constantinos Patsakis. "A systematic literature review of blockchain-based applications: Current status, classification and open issues." Telematics and informatics 36 (2019): 55-81.
- Christopher Allen. The Path to Sovereign Identity, 2016. URL: https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/ThePathToSelf-SovereignIdentity.md.
- Čučko, Špela, and Muhamed Turkanović. "Decentralized and self-sovereign identity: Systematic mapping study." IEEE Access 9 (2021): 139009-139027.
- DigitalOcean Community. How To Install Node.js on Ubuntu, 2018. URL: https://www.digitalocean.com/community/tutorials
- Docker Inc. Get Docker Engine - Community for Ubuntu, 2019. URL: https://docs.docker.com/install/linux/docker-ce/ubuntu
- Houben, R. & Snyers, A., 2018. Cryptocurrencies URL: http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf
- https://bitcoin.org
- Hyperledger Composer. Hyperledger Composer Installing the development environment, 2019. URL: https://hyperledger.github.io/composer/v0.19/installing/development-tools
- Hyperledger Composer. Hyperledger Composer-Documentation, 2019. URL: https://hyperledger.github.io/composer/latest/introduction/introduction.html
- Hyperledger Fabric. Hyperledger Fabric, 2019. URL: https://hyperledger-fabric.readthedocs.io/en/release-1.2/blockchain.html
- Hyperledger Team. Hyperledger Cello, 2018. URL: https://www.hyperledger.org/projects/cello
- Hyperledger Team. Measuring Blockchain Performance with Hyperledger Caliper, 2018. URL: https://www.hyperledger.org/blog/2018/03/19/measuring-blockchain-performance-with-hyperledger-caliper
- Hyperledger. Case Study: How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric. URL: https://www.hyperledger.org/learn/publications/walmart-case-study.
- Hyperledger. Hyperledger Explorer, 2018. URL: https://www.hyperledger.org/projects/explorer
- Hyperledger. URL: https://www.hyperledger.org/.
- In What Ways Blockchain Will Disrupt Various Industries. Nikhil, R., 2018. URL: https://hackernoon.com/in-what-ways-blockchain-will-disrupt-various-industries-be7aaee58927
- Jameson Lopp. Bitcoin and the Rise of the Cypherpunks, 2016. URL: https ://www.coindesk.com/markets/2016/04/09/bitcoin-and-the-rise-of-the - cypherpunks/.
- Mühle, Alexander, et al. "A survey on essential components of a self-sovereign identity." Computer Science Review 30 (2018): 80-86.
- Nestle. Nestle expands blockchain to Zoegas coffee brand, 2020. URL: https://www.nestle.com/media/news/nestle-blockchain-zoegas-coffee-brand
- Philip Zimmerman. Creator of PGP. URL: https://philzimmermann.com/EN /background/index.html
- Richard Esplin evernym Self-Sovereign Identity and Open Source Software, 2018
- Satoshi Nakamoto. Bitcoin: A Peer to Peer Electronic Cash System, 2008. URL: https://bitcoin.org/bitcoin.pdf.

- Sovrin A Protocol and Token for SelfSovereign Identity and Decentralized Trust, 2018
- Sovrin. The Inevitable Rise of Self-Sovereign Identity, 2016
- Sovring foundation. Sovrin: A Protocol and Token for Self - Sovereign Identity and Decentralized Trust, 2018. URL: https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf.
- UK Government, Office for Science. Distributed Ledger Technology, 2016. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf
- Van Bokkem, Dirk, et al. "Self-sovereign identity solutions: The necessity of blockchain technology." arXiv preprint arXiv:1904.12816 (2019).
- What Is Hyperledger? [The Most Comprehensive Step-by-Step Guide!]. Rosic, A., 2017. URL: https://blockgeeks.com/guides/hyperledger/
- Xiao, Yang, et al. "A survey of distributed consensus protocols for blockchain networks." IEEE Communications Surveys & Tutorials 22.2 (2020): 1432-1465.