



**ΤΕΙ ΗΠΕΙΡΟΥ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ**

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

**ΑΛΥΣΙΔΑ ΑΠΟ BLOCK ΚΑΙ Η ΕΦΑΡΜΟΓΗ
ΤΗΣ ΣΕ ΓΕΩΧΩΡΙΚΑ ΔΕΔΟΜΕΝΑ**

Βούλγαρης Ευριπίδης
Επιβλέπων: Μάρκος Τσίπουρας
τίτλος, βαθμίδα
ΑΡΤΑ Φεβρουάριος 2019



**ΤΕΙ ΗΠΕΙΡΟΥ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ**

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

**ΑΛΥΣΙΔΑ ΑΠΟ BLOCK ΚΑΙ Η ΕΦΑΡΜΟΓΗ
ΤΗΣ ΣΕ ΓΕΩΧΩΡΙΚΑ ΔΕΔΟΜΕΝΑ**

Βούλγαρης Ευριπίδης
Επιβλέπων: Μάρκος Τσίπουρας
τίτλος, βαθμίδα
ΑΡΤΑ Φεβρουάριος 2019

BLOCKCHAIN AND ITS APPLICATION IN GEOSPATIAL DATA

Εγκρίθηκε από τριμελή εξεταστική επιτροπή
Τόπος, Ημερομηνία

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Επιβλέπων καθηγητής
Όνομα Επίθετο, τίτλος, βαθμίδα

2. Μέλος επιτροπής
Όνομα Επίθετο, τίτλος, βαθμίδα

3. Μέλος επιτροπής
Όνομα Επίθετο, τίτλος, βαθμίδα

Ο/Η Προϊστάμενος/η του Τμήματος

Όνομα Επίθετο,

τίτλος, βαθμίδα

Υπογραφή

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Δήλωση μη λογοκλοπής

Δήλωση μη λογοκλοπής Δηλώνω υπεύθυνα και γνωρίζοντας τις κυρώσεις του Ν. 2121/1993 περί Πνευματικής Ιδιοκτησίας, ότι η παρούσα πτυχιακή εργασία είναι εξ ολοκλήρου αποτέλεσμα δικής μου ερευνητικής εργασίας, δεν αποτελεί προϊόν αντιγραφής ούτε προέρχεται από ανάθεση σε τρίτους. Όλες οι πηγές που χρησιμοποιήθηκαν (κάθε είδους, μορφής και προέλευσης) για τη συγγραφή της περιλαμβάνονται στη βιβλιογραφία.

Επίθετο, Όνομα

Υπογραφή

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω θερμά τον καθηγητή μου κύριο Μάρκο Τσίπουρα. Επίσης θα ήθελα να ευχαριστήσω την οικογένειά μου που είναι πάντα δίπλα μου.

ΠΕΡΙΛΗΨΗ

Η συγκεκριμένη πτυχιακή εργασία αναφέρεται στην τεχνολογία αλυσίδα από block, γνωστή ως blockchain , στον τρόπο που πραγματοποιείται η κρυπτογράφηση, στα πεδία εφαρμογής τέτοιων τεχνολογιών και στον τρόπο που μπορούν να ενσωματωθούν γεωχωρικά δεδομένα όπως οι συντεταγμένες. Τέλος, θα πραγματοποιηθεί μια εγκατάσταση και θα δειχθεί ένα σενάριο χρήσης κωδικοποίησης συνταγμένων.

Λέξεις κλειδιά: αλυσίδα από block, γεωχωρικά δεδομένα, κρυπτογράφηση

ABSTRACT

This thesis refers to blockchain technology, to the way encryption takes place, to the fields of application of such technologies and to the way geospatial data, such as coordinates, are incorporated. Finally, an installation will be performed and a scenario for using customized encoding will be shown.

Key words: blockchain, geospatial, cryptography

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Κεφάλαιο 1	13
1.1 Ορισμός της αλυσίδας από block	13
1.2 Εισαγωγή	15
1.3 Δομή	16
1.4.1 Blocks	17
1.4.2 Χρόνος αποκλεισμού	18
1.5 Αποκέντρωση	18
1.6 Προσβασιμότητα	20
1.7 Πλεονεκτήματα και μειονεκτήματα του blockchain	22
1.8 Επιτρεπόμενο (ιδιωτικό) blockchain	24
1.9 Μειονεκτήματα του ιδιωτικού blockchain	24
1.10 Χρήσεις	25
1.11 Κρυπτοσυχνότητες	25
1.12 Έξυπνες συμβάσεις	26
1.13 Τράπεζες	26
Κεφάλαιο 2	27
2.1 Λειτουργία	27
2.2 Hashing	30

Πτυχιακή Εργασία: BLOCKCHAIN AND ITS APPLICATION IN GEOSPATIAL DATA

2.3	Εξασφάλιση δεδομένων με τη συμβολή του Hashing	30
2.4	Δέντρα Merkle	32
Κεφάλαιο 3		34
3.1	Περιπτώσεις χρήσεων	34
3.2	Bitcoin	34
3.3	Εφαρμογές του blockchain.....	35
Κεφάλαιο 4		37
4.1	Geospatial blockchain	37
4.2	Blockchain και γεωχωρικά συστήματα.....	37
4.3	Διαφορά μεταξύ blockchain και βάσης δεδομένων	37
4.4	Τύποι blockchain.....	39
4.5	Διεύρυνση του ορίζοντα σε γεωχωρική	41
4.6	Το πεδίο δράσης του Blockchain στο IoT.....	42
4.7	Γεωπεριφερειακός δεσμός με blockchain	43
Κεφάλαιο 5		45
5.1	Hyperledger.....	45
5.2	Hyperledger Fabric.....	47
Κεφάλαιο 6		52
6.1	Υλοποίηση και Αρχιτεκτονική HYPERLEDGER FABRIC	53
6.2	Ανάλυση.....	54
6.3	Σενάριο Χρήσης	55

Location-trading-network	55
6.3 Σενάριο Χρήσης 2	63
Κεφάλαιο 7	68
7.1 Συμπεράσματα και μελλοντική έρευνα	68
Βιβλιογραφικές Παραπομπές	69

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

Εικόνα 1-πακέτα από το npm	53
Εικόνα 2- εντολές για την εγκατάσταση του Hyperledger Fabric	54
Εικόνα 3- υλοποίηση business network	54
Εικόνα 4-δημιουργία χρήστη	56
Εικόνα 5-παράδειγμα εισαγωγής χρήστη	56
Εικόνα 6-εισαγωγή χρήστη	57
Εικόνα 7-εισαγωγή δεδομένων	57
Εικόνα 8-δημιουργία location	58
Εικόνα 9-λειτουργίες blockchain	59
Εικόνα 10-λειτουργίες blockchain	59
Εικόνα 11-λειτουργίες blockchain	60
Εικόνα 12-λειτουργίες blockchain	61
Εικόνα 13-λειτουργίες blockchain	62
Εικόνα 14-λειτουργίες blockchain	62

Εικόνα 15-Δημιουργία Test	63
Εικόνα 16-Δημιουργία new participant	64
Εικόνα 17-εισαγωγή στοιχείων.....	64
Εικόνα 18-Δημιουργία χρήστη	65
Εικόνα 19- Δημιουργία χρήστη 2	65
Εικόνα 20-Δημιουργία new asset.....	66
Εικόνα 21-προβολή Transaction.....	66
Εικόνα 22-πληροφορίες Hash.....	67

Κεφάλαιο 1

1.1 Ορισμός της αλυσίδας από block

Η Αλυσίδα από block (blockchain) είναι μια δομή δεδομένων, ομαδοποιημένων σε χρονικά αριθμημένα block στην οποία διατηρείται ένα αρχείο συναλλαγών που πραγματοποιούνται σε bitcoin ή σε κάποιο άλλο κρυπτονόμισμα σε διάφορους υπολογιστές που συνδέονται σε ένα δίκτυο peer-to-peer. Η πρώτη ιστορικά εφαρμογή της εν λόγω τεχνολογίας έγινε στον χώρο των ψηφιακών νομισμάτων, και πιο συγκεκριμένα στην περίπτωση του bitcoin [1].

Ενδεικτικά, αναφέρεται ότι τα συστήματα peer-to-peer είναι μία ομάδα υπολογιστών, κάθε μία από τις οποίες λειτουργεί ως κόμβος για την κοινή χρήση αρχείων εντός της ομάδας. Αντί να έχει ένα κεντρικό διακομιστή για να λειτουργεί ως κοινόχρηστος δίσκος, κάθε υπολογιστής λειτουργεί ως διακομιστής για τα αρχεία που είναι αποθηκευμένα σε αυτόν [2].

Πτυχιακή Εργασία: BLOCKCHAIN AND ITS APPLICATION IN GEOSPATIAL DATA

Η τεχνολογία αυτή μπορεί να εφαρμοστεί σε ένα πλήθος επιπλέον περιοχών της ανθρώπινης δραστηριότητας, όπως ενδεικτικά η καταμέτρηση ψήφων, η Παιδεία, η Υγεία, η διαφύλαξη και διαφάνεια ιστορικών, πολιτιστικών, δημοσιονομικών και άλλων αρχείων, η πιστοποίηση προϊόντων και υπηρεσιών και τα κοινωνικά δίκτυα. Θα γίνει εκτενέστερη αναφορά σε κάποιες από τις εφαρμογές της τεχνολογίας blockchain παρακάτω [3].

1.2 Εισαγωγή

Το πρώτο έργο με τεχνολογία blockchain περιγράφηκε το 1991 από τους Stuart Haber και W. Scott Stornetta. Ήθελαν να εφαρμόσουν ένα σύστημα όπου τα χρονικά σήματα (αλλιώς: χρονοσήμανση - timestamps) των εγγράφων δεν μπορούσαν να αλλοιωθούν. Οι Bayer, Haber και Stornetta, το 1992, ενσωμάτωσαν στον σχεδιασμό τα δέντρα Merkle. Αυτό βελτίωσε την αποτελεσματικότητά του, επιτρέποντας τη συγκέντρωση περισσότερων πιστοποιητικών εγγράφων σε ένα block [4]. Εκτενέστερη αναφορά στο Merkle θα γίνει στη συνέχεια.

Το πρώτο blockchain επινοήθηκε από τον Satoshi Nakamoto το 2008. Ο Nakamoto χρησιμοποίησε μια μέθοδο τύπου Hashcash για να προσθέσει blocks στην αλυσίδα (chain) χωρίς να απαιτείται να υπογραφούν από ένα αξιόπιστο τρίτο άτομο, βελτιώνοντας έτσι τον σχεδιασμό [4]. Ο σχεδιασμός εφαρμόστηκε το επόμενο έτος από τον Nakamoto ως βασικό στοιχείο του Bitcoin, όπου χρησιμεύει για όλες τις συναλλαγές στο δίκτυο [5].

Τον Αύγουστο του 2014, το μέγεθος του αρχείου Bitcoin, που περιέχει αρχεία όλων των συναλλαγών που έχουν πραγματοποιηθεί στο δίκτυο, έφτασε τα 20 GB (gigabytes). Τον Ιανουάριο του 2015, το μέγεθος είχε αυξηθεί σε σχεδόν 30 GB, και από τον Ιανουάριο του 2016 έως τον Ιανουάριο του 2017, το blockchain Bitcoin αυξήθηκε από 50 GB σε 100 GB σε μέγεθος.

Οι λέξεις block και chain χρησιμοποιήθηκαν χωριστά στην αρχική υλοποίηση του Satoshi Nakamoto, αλλά ενοποιήθηκαν σε μία λέξη, το blockchain, τα τελευταία χρόνια.

Η επιχείρηση IBM (International Business Machines) άνοιξε ένα ερευνητικό κέντρο καινοτομίας στη Σιγκαπούρη τον Ιούλιο του 2016. Μια ομάδα εργασίας για το Παγκόσμιο Οικονομικό Φόρουμ συναντήθηκε τον Νοέμβριο του 2016 για να συζητήσει την ανάπτυξη μοντέλων διακυβέρνησης που σχετίζονται με το blockchain [6].

Σύμφωνα με την Accenture, μία εταιρεία παροχής συμβουλευτικών υπηρεσιών τεχνολογίας, η εφαρμογή της θεωρίας της διάδοσης των καινοτομιών υποδηλώνει ότι τα blockchains το 2016 υιοθετήθηκαν σε ποσοστό 13,5% στις χρηματοπιστωτικές υπηρεσίες. Οι εμπορικές ομάδες του κλάδου εντάχθηκαν για να δημιουργήσουν το Παγκόσμιο Φόρουμ του Blockchain (Global Blockchain Forum) το 2016, πρωτοβουλία του Επιμελητηρίου Ψηφιακού Εμπορίου (Chamber of Digital Commerce) [7].

Τον Μάιο του 2018, η εταιρεία Gartner διαπίστωσε ότι μόνο το 1% των CIO (Chief innovation officer) ανέφεραν οποιουδήποτε είδους υιοθεσίας blockchain στις οργανώσεις τους και μόνο το 8% των CIO βρισκόταν σε βραχυπρόθεσμο σχεδιασμό ή ενεργό πειραματισμό με blockchain[8].

Τον Νοέμβριο του 2018, το σχέδιο της συντηρητικού ευρωβουλευτή Emma McClarkin για χρήση της τεχνολογίας blockchain με στόχο την ενίσχυση του εμπορίου υποστηρίχθηκε από την Επιτροπή Εμπορίου του Ευρωπαϊκού Κοινοβουλίου.

1.3 Δομή

Ένα blockchain είναι ουσιαστικά ένα αποκεντρωμένο, κατανεμημένο και δημόσιο ψηφιακό δίκτυο που χρησιμοποιείται για την καταγραφή συναλλαγών σε πολλούς υπολογιστές έτσι ώστε κάθε εγγραφή που εμπλέκεται να μην μπορεί να τροποποιηθεί

αναδρομικά, χωρίς την αλλαγή όλων των επόμενων block. Αυτό επιτρέπει στους συμμετέχοντες να επαληθεύουν και να ελέγχουν τις συναλλαγές ανεξάρτητα και σχετικά ανέξοδα [5].

Ένας τέτοιος σχεδιασμός διευκολύνει τη ροή εργασίας, όπου η αβεβαιότητα των συμμετεχόντων σχετικά με την ασφάλεια των δεδομένων είναι περιορισμένη. Η χρήση ενός blockchain αφαιρεί το χαρακτηριστικό της αναπαραγωγιμότητας από ένα ψηφιακό στοιχείο (digital asset). Επιβεβαιώνει ότι κάθε μονάδα αξίας μεταφέρθηκε μόνο μία φορά, επιλύοντας το μακροχρόνιο πρόβλημα των διπλών δαπανών. Ένα blockchain έχει περιγραφεί ως πρωτόκολλο ανταλλαγής τιμών. Ένα blockchain μπορεί να διατηρήσει τα δικαιώματα του τίτλου επειδή, όταν έχει ρυθμιστεί σωστά για να διευκρινίσει τη συμφωνία ανταλλαγής, παρέχει ένα τρόπο που υποχρεώνει την προσφορά και την αποδοχή μιας συναλλαγής.

1.4.1 Blocks

Κάθε block περιλαμβάνει τον κρυπτογραφικό κατακερματισμό (cryptographic hash) του προηγούμενου block στο blockchain, συνδέοντας αυτά τα δύο block. Τα συνδεδεμένα block αποτελούν μια αλυσίδα. Αυτή η επαναληπτική διαδικασία επιβεβαιώνει την ακεραιότητα του προηγούμενου block, μέχρι το αρχικό block (genesis block).

Εκτός από ένα ασφαλές ιστορικό με βάση τον κατακερματισμό (hash, θα προτιμηθεί ο αγγλικός όρος), κάθε blockchain έχει έναν καθορισμένο αλγόριθμο για τις διαφορετικές εκδόσεις του ιστορικού. Τα block που δεν έχουν επιλεγεί για να συμπεριληφθούν στην αλυσίδα ονομάζονται ορφανά block (orphan blocks). Οι χρήστες που υποστηρίζουν τη βάση δεδομένων έχουν διαφορετικές εκδόσεις του

ιστορικού. Διατηρούν μόνο την τελευταία/πιο πρόσφατη βάση δεδομένων που τους είναι γνωστή.

Κάθε φορά που ένας ομότιμος χρήστης (peer) λαμβάνει μια νεότερη έκδοση (συνήθως η παλιά έκδοση προστιθέμενη με ένα νεότερο block), επεκτείνει ή αντικαθιστά τη δική του βάση δεδομένων και αναμεταδίδει την καινούργια στους υπόλοιπους. Δεν υπάρχει ποτέ απόλυτη εγγύηση ότι κάποια συγκεκριμένη καταχώρηση θα παραμείνει στην καλύτερη έκδοση της για πάντα. Τα blockchain κατασκευάζονται συνήθως για να προσθέτουν νεότερα block σε παλαιότερα και μπορούν να επεκταθούν με νέα block αντί να αντικαταστήσουν τα προηγούμενα [9] .

1.4.2 Χρόνος αποκλεισμού

Ο χρόνος αποκλεισμού (block time) είναι ο μέσος χρόνος που χρειάζεται για να παράξει το δίκτυο ένα επιπλέον block στο blockchain. Ορισμένα blockchains δημιουργούν ένα νέο block κάθε πέντε δευτερόλεπτα. Μέχρι τη στιγμή ολοκλήρωσης του block, τα δεδομένα που περιλαμβάνονται θα καταστούν επαληθεύσιμα. Στην τεχνολογία του κρυπτονομίσματος (cryptocurrency), αυτό συμβαίνει στην πράξη όταν πραγματοποιείται η συναλλαγή. Επομένως, στην περίπτωση αυτή, ένας μικρότερος χρόνος αποκλεισμού σημαίνει ταχύτερες συναλλαγές. Ο χρόνος αποκλεισμού για το Ethereum (μία ανοιχτού κώδικα πλατφόρμα λογισμικού που βασίζεται στην τεχνολογία blockchain) ορίζεται μεταξύ 14 και 15 δευτερολέπτων, ενώ για το Bitcoin είναι 10 λεπτά [10].

1.5 Αποκέντρωση

Με την αποθήκευση δεδομένων σε όλο το δίκτυο peer-to-peer (peer-to-peer network), το blockchain εξαλείφει έναν αριθμό κινδύνων που ελλοχεύουν όταν τα δεδομένα κρατούνται κεντρικά [5]. Το αποκεντρωμένο blockchain (decentralized blockchain)

μπορεί να χρησιμοποιεί ad-hoc μετάδοση μηνυμάτων (ad-hoc message passing) και κατανεμημένη δικτύωση (distributed networking).

Τα δίκτυα blockchain από ομότιμους χρήστες (peer-to-peer blockchain networks) δεν διαθέτουν συγκεντρωτικά σημεία ευπάθειας τα οποία μπορούν να εκμεταλλευτούν κακόβουλοι χρήστες. Οι μέθοδοι ασφαλείας της τεχνολογίας blockchain περιλαμβάνουν τη χρήση κρυπτογραφίας δημόσιου κλειδιού (public-key cryptography) [11]. Ένα δημόσιο κλειδί (public key - μια μακρά σειρά φαινομενικά τυχαίων αριθμών) είναι μια διεύθυνση στο blockchain. Οι μάρκες αξίας (value tokens) που αποστέλλονται μέσω του δικτύου καταγράφονται ως ανήκοντα σε αυτή τη διεύθυνση.

Ένα ιδιωτικό κλειδί (private key) είναι σαν ένας κωδικός πρόσβασης που δίνει στον ιδιοκτήτη του πρόσβαση στα ψηφιακά του στοιχεία ή τα μέσα για να αλληλεπιδράσει με τις διάφορες δυνατότητες που υποστηρίζουν τώρα τα blockchains. Τα δεδομένα που είναι αποθηκευμένα στο blockchain θεωρούνται γενικά απρόσβλητα [5].

Κάθε κόμβος (node) σε ένα αποκεντρωμένο σύστημα (decentralized system) έχει ένα αντίγραφο του blockchain. Η ποιότητα των δεδομένων διατηρείται με τη μαζική αναπαραγωγή βάσεων δεδομένων [12] και με την υπολογιστική αξιοπιστία (computational trust). Δεν υπάρχει κεντρικά "επίσημο" αντίγραφο και κανένας χρήστης δεν είναι "έμπιστος" περισσότερο από οποιονδήποτε άλλο [11]. Οι συναλλαγές μεταδίδονται στο δίκτυο χρησιμοποιώντας το λογισμικό. Τα μηνύματα παραδίδονται με βάση την καλύτερη δυνατή προσπάθεια (best-effort delivery). Οι κόμβοι επικυρώνουν τις συναλλαγές, τις προσθέτουν στο block που κατασκευάζουν και στη συνέχεια μεταδίδουν το ολοκληρωμένο block σε άλλους κόμβους.

Χρησιμοποιούνται διάφορα συστήματα σφράγισης χρόνου, όπως η απόδειξη εργασίας (proof-of-work), για τη σειριοποίηση αλλαγών. Οι εναλλακτικές μέθοδοι συναίνεσης περιλαμβάνουν την απόδειξη της συμμετοχής (proof-of-stake). Η ανάπτυξη ενός αποκεντρωμένου blockchain συνοδεύεται από τον κίνδυνο συγκέντρωσης (centralization) λόγω του ότι οι υπολογιστικοί πόροι που απαιτούνται για τη διεκπεραίωση μεγαλύτερων ποσοτήτων δεδομένων καθίστανται ακριβότεροι.

1.6 Προσβασιμότητα

Τα ανοιχτά blockchain είναι πιο φιλικά προς το χρήστη από κάποια παραδοσιακά αρχεία ιδιοκτησίας, που, ενώ είναι ανοιχτές στο κοινό, απαιτούν ακόμα φυσική πρόσβαση για προβολή.

Λόγω του ότι οι πρώιμες blockchains δεν απαιτούσαν την ανάγκη άδειας (permissionless network), αμφισβητήθηκε ο ορισμός του blockchain. Το κυριότερο θέμα της συζήτησης που προέκυψε είναι το αν ένα ιδιωτικό σύστημα με εξουσιοδοτημένους από μία κεντρική αρχή επαληθευτές θα πρέπει να θεωρείται blockchain. Οι υποστηρικτές των ιδιωτικών αλυσίδων (permissioned/private chains) ισχυρίζονται ότι ο όρος "blockchain" μπορεί να χρησιμοποιηθεί για κάθε δομή δεδομένων που ομαδοποιεί δεδομένα σε χρονικά επισφραγισμένα blocks.

Αυτές οι blockchain χρησιμεύουν ως κατανεμημένη έκδοση του ελέγχου πολλαπλής αντιστοίχισης (Multiversion Concurrency Control - MVCC) σε βάσεις δεδομένων. Ακριβώς όπως ο MVCC εμποδίζει δύο συναλλαγές να τροποποιούν ταυτόχρονα ένα μόνο αντικείμενο σε μια βάση δεδομένων, τα blockchains εμποδίζουν τις δύο συναλλαγές να τροποποιήσουν την ίδια ενιαία έξοδο σε ένα blockchain. Οι επικριτές υποστηρίζουν ότι τα συστήματα αυτά μοιάζουν με τις παραδοσιακές εταιρικές βάσεις δεδομένων, αδυνατώντας ουσιαστικά να υποστηρίξουν την αποκεντρωμένη

Πτυχιακή Εργασία: BLOCKCHAIN AND ITS APPLICATION IN GEOSPATIAL DATA

επαλήθευση των δεδομένων (decentralized data verification). Ο Nikolai Hampton του Computerworld ανέφερε συγκεκριμένα ότι «οι in-house λύσεις blockchain δεν θα είναι τίποτα περισσότερο από δυσκίνητες βάσεις δεδομένων» [13].

1.7 Πλεονεκτήματα και μειονεκτήματα του blockchain

Τα πλεονεκτήματα της τεχνολογίας blockchain είναι τα εξής:

- Άμεσες συναλλαγές: Οι συναλλαγές σε ένα blockchain μπορούν να γίνουν μέσα σε λίγα λεπτά [14].
- Ακεραιότητα της διαδικασίας: Οι συναλλαγές γίνονται ακριβώς όπως ορίζονται, καταργώντας την ανάγκη επίβλεψης από ένα έμπιστο τρίτο άτομο [14].
- Εξουσιοδοτημένοι χρήστες: Οι χρήστες ελέγχουν όλες τις πληροφορίες των συναλλαγών τους [14].
- Δεδομένα υψηλής ποιότητας: Τα δεδομένα είναι πλήρη, συνεπή, έγκαιρα, ακριβή και διαθέσιμα [14].
- Αντοχή και αξιοπιστία: Λόγω των αποκεντρωμένων δικτύων, το blockchain δεν έχει κεντρικό σημείο αποτυχίας και είναι σε θέση να αντέξει καλύτερα τις επιθέσεις [14].
- Διαφάνεια και αμεταβλητότητα: Οι αλλαγές στο δημόσιο blockchain είναι δημόσια ορατές από όλα τα μέρη που δημιουργούν διαφάνεια και όλες οι συναλλαγές είναι αμετάβλητες, που σημαίνει ότι δεν μπορούν να τροποποιηθούν ή να διαγραφούν [14].
- Απλοποίηση του συστήματος: Με όλες τις συναλλαγές που προστίθενται σε ένα ενιαίο δημόσιο καθολικό (ledger – θα προτιμηθεί ο ξένος όρος), μειώνει τις επιπλοκές των πολλαπλών ledgers [14].
- Ταχύτερες συναλλαγές: Οι συναλλαγές Blockchain μειώνουν τους χρόνους συναλλαγής σε λίγα λεπτά [14].

- Χαμηλότερο κόστος συναλλαγών: Με την εξάλειψη των τρίτων και των γενικών εξόδων για την ανταλλαγή περιουσιακών στοιχείων, τα blockchains έχουν τη δυνατότητα να μειώσουν σημαντικά τα τέλη συναλλαγών [14].

Τα μειονεκτήματα της τεχνολογίας blockchain είναι τα εξής:

- Έλεγχος υπογραφής: Κάθε συναλλαγή blockchain πρέπει να υπογραφεί ψηφιακά χρησιμοποιώντας ένα δημόσιο-ιδιωτικό σύστημα κρυπτογραφίας όπως το ECDSA. Αυτό είναι απαραίτητο επειδή οι συναλλαγές μεταδίδονται μεταξύ των κόμβων ομότιμα, οπότε η πηγή τους δεν μπορεί να αποδειχθεί αλλιώς. Η επαλήθευση αυτών των υπογραφών είναι υπολογιστικά πολύπλοκη και αποτελεί το κύριο εμπόδιο στις υπηρεσίες. Αντίθετα, στις συγκεντρωτικές βάσεις δεδομένων, μόλις δημιουργηθεί μια σύνδεση, δεν χρειάζεται να επαληθεύεται ξεχωριστά για κάθε αίτημα που έρχεται [14].
- Εκκολαπτόμενη τεχνολογία: Η επίλυση προκλήσεων όπως η ταχύτητα συναλλαγής και η διαδικασία επαλήθευσης θα είναι καθοριστικής σημασίας για την ευρεία εφαρμογή του blockchain [14].
- Αβεβαιότητα όσον αφορά το ρυθμιστικό καθεστώς: Επειδή τα σύγχρονα νομίσματα δημιουργήθηκαν και ρυθμίστηκαν από τις εθνικές κυβερνήσεις, το blockchain, το Bitcoin και το Ethereum αντιμετωπίζουν ένα εμπόδιο στην ευρεία υιοθέτηση από προϋπάρχοντα χρηματοπιστωτικά ιδρύματα, εάν το καθεστώς ρύθμισης της κυβέρνησής τους παραμένει μη διευθετημένο [14].
- Μεγάλη κατανάλωση ενέργειας: Οι miners (ανθρακωρύχοι) του Bitcoin blockchain επιχειρούν 450.000 τρισεκατομμύρια λύσεις ανά δευτερόλεπτο

στις προσπάθειες επικύρωσης των συναλλαγών, χρησιμοποιώντας σημαντικά ποσά ενέργειας από τη μεριά του υπολογιστή [14].

- Ανησυχία ένταξης: Οι εφαρμογές Blockchain προσφέρουν λύσεις που απαιτούν σημαντικές αλλαγές ή πλήρη αντικατάσταση των υπαρχόντων συστημάτων [14].
- Πολιτιστική αποδοχή: Το blockchain αντιπροσωπεύει μια πλήρη στροφή από έναν πλήρη κεντρικό κόσμο σε έναν πιο αποκεντρωμένο κόσμο [14].
- Κόστος: Το blockchain προσφέρει τεράστια εξοικονόμηση κόστους και χρόνου συναλλαγών, αλλά το υψηλό αρχικό κόστος κεφαλαίου μπορεί να αποθαρρύνει αρκετούς [14].
- Πλεονασμός: Δεν πρόκειται για την απόδοση ενός μεμονωμένου κόμβου, αλλά για το συνολικό ποσό του υπολογισμού που απαιτεί ένα blockchain [14].

1.8 Επιτρεπόμενο (ιδιωτικό) blockchain

Οι επιτρεπόμενες blockchains χρησιμοποιούν ένα στρώμα ελέγχου πρόσβασης για να καθορίζουν ποιος έχει πρόσβαση στο δίκτυο. Σε αντίθεση με τα δημόσια δίκτυα blockchain, οι επικυρωτές (validators) σε ιδιωτικά δίκτυα blockchain ελέγχονται από τον κάτοχο του δικτύου. Δεν βασίζονται σε ανώνυμους κόμβους για την επικύρωση των συναλλαγών. Οι αδειοδοτημένες blockchain αναφέρονται επίσης και ως «blockchain κοινοπραξίες» ή «υβριδικά blockchain».[15]

1.9 Μειονεκτήματα του ιδιωτικού blockchain

Ο Nikolai Hampton επεσήμανε στην Computerworld ότι «δεν υπάρχει ανάγκη για μία κατά 51% επίθεση σε ιδιωτικά blockchain, καθώς το ιδιωτικό blockchain ελέγχει ήδη το 100% όλων των πόρων δημιουργίας block. Μία ενδεχόμενη επίθεση ή οποιουδήποτε είδους βλάβη στα εργαλεία δημιουργίας ενός blockchain σε ένα

ιδιωτικό εταιρικό διακομιστή θα μπορούσε να οδηγήσει στον πλήρη έλεγχο του δικτύου και στη δυνατότητα μεταβολής των συναλλαγών κατά το δοκούν» [13]. Αυτό οδηγεί σε μια σειρά από ιδιαίτερα δυσμενείς αρνητικές επιπτώσεις κατά τη διάρκεια μιας χρηματοπιστωτικής κρίσης ή κρίσης χρέους, όπως η οικονομική κρίση της περιόδου 2007-2008, όπου οι πολιτικά ισχυροί παράγοντες μπορούν να πάρουν αποφάσεις που ευνοούν ορισμένες ομάδες εις βάρος άλλων.[16]

1.10 Χρήσεις

Η τεχνολογία blockchain μπορεί να ενσωματωθεί σε πολλές περιοχές. Η κύρια χρήση των blockchains σήμερα αφορά στα κρυπτονομίσματα, κυρίως το bitcoin. Πράγματα, αμφότερα τα δίκτυα του Bitcoin και της Ethereum, η οποία αναφέρθηκε προηγουμένως, βασίζονται στην τεχνολογία blockchain.[17]

Ο Steve Wilson, της Constellation Research, πιστεύει ότι η τεχνολογία αυτή έχει προωθηθεί περισσότερο από ότι θα έπρεπε. Ακόμα, για τον μετριασμό του κινδύνου, οι επιχειρήσεις είναι απρόθυμες να τοποθετήσουν το blockchain στον πυρήνα της επιχειρηματικής διάρθρωσης.

1.11 Κρυπτοσυχνότητες

Τα περισσότερα κρυπτονομίσματα χρησιμοποιούν τεχνολογία blockchain για την καταγραφή συναλλαγών. Όπως αναφέρθηκε κι προηγουμένως, το δίκτυο Bitcoin και το δίκτυο Ethereum βασίζονται και τα δύο σε blockchain. Στις 8 Μαΐου 2018, το Facebook επιβεβαίωσε ότι ανοίγει μια νέα ομάδα blockchain της οποίας θα είναι επικεφαλής ο David Marcus, ο οποίος προηγουμένως ήταν υπεύθυνος για το Messenger. Σύμφωνα με το The Verge, μία ιστοσελίδα αφιερωμένη στα νεότερα επιτεύγματα της τεχνολογίας, το Facebook σχεδιάζει να ξεκινήσει τη δική του κρυπτογράφηση για τη διευκόλυνση πληρωμών στην πλατφόρμα.[18]

1.12 Έξυπνες συμβάσεις

Οι έξυπνες συμβάσεις (smart contracts) που βασίζονται στο blockchain είναι προτεινόμενες συμβάσεις που θα μπορούσαν να εκτελεστούν μερικώς ή πλήρως ή να εφαρμοστούν χωρίς ανθρώπινη αλληλεπίδραση. Ένας από τους κύριους στόχους μιας έξυπνης σύμβασης είναι η αυτοματοποιημένη μεσεγγύηση δηλαδή μία συμφωνία ανάμεσα σε δύο πρόσωπα που ορίζει ένα τρίτο ανεξάρτητο πρόσωπο να διαχειριστεί χρήματα εκ μέρους τους με συγκεκριμένους όρους. Μια συζήτηση του προσωπικού του ΔΝΤ (Διεθνές Νομισματικό Ταμείο) ανέφερε ότι οι έξυπνες συμβάσεις που βασίζονται στην τεχνολογία blockchain θα μπορούσαν να μειώσουν τους ηθικούς κινδύνους και να βελτιστοποιήσουν τη χρήση των συμβάσεων εν γένει. Αλλά «δεν έχουν προκύψει ακόμη βιώσιμα έξυπνα συμβόλαια». Λόγω της έλλειψης ευρείας χρήσης, το νομικό τους καθεστώς παραμένει ασαφές.[19]

1.13 Τράπεζες

Οι τράπεζες ενδιαφέρονται για αυτήν την τεχνολογία επειδή έχουν τη δυνατότητα να επιταχύνουν τα συστήματα διακανονισμού τύπου back office.

Οι τράπεζες, όπως η ελβετική UBS, ανοίγουν νέα ερευνητικά εργαστήρια αφιερωμένα στην τεχνολογία blockchain, προκειμένου να διερευνήσουν τον τρόπο με τον οποίο το blockchain μπορεί να χρησιμοποιηθεί στις χρηματοπιστωτικές υπηρεσίες για να αυξήσει την αποδοτικότητα και να μειώσει το κόστος.

Η Berenberg, μια γερμανική τράπεζα, πιστεύει ότι το blockchain είναι μια "υπερεκτιμημένη τεχνολογία" που εξακολουθεί να έχει μείζονες προκλήσεις και ελάχιστες επιτυχίες.[20]

Κεφάλαιο 2

2.1 Λειτουργία

Πολλοί άνθρωποι χρησιμοποιούν την κρυπτογραφία (cryptography) σε καθημερινή βάση χωρίς να το συνειδητοποιούν, καθώς πολλές δημοφιλείς εφαρμογές ανταλλαγής μηνυμάτων (messaging apps) χρησιμοποιούν κρυπτογράφηση. Είναι επίσης μια από τις βασικές πτυχές της τεχνολογίας blockchain. Σε αυτή την ενότητα θα δώσουμε μια απλή αλλά λεπτομερή εξήγηση της κρυπτογραφίας, τόσο της συμμετρικής όσο και της ασύμμετρης κρυπτογραφίας κλειδιού [21].

Η κρυπτογραφία είναι η μέθοδος της συγκάλυψης και αποκάλυψης, αλλιώς γνωστή ως κρυπτογράφηση και αποκρυπτογράφηση (encrypting and decrypting) πληροφοριών μέσω πολύπλοκων μαθηματικών. Αυτό σημαίνει ότι οι πληροφορίες μπορούν να προβληθούν μόνο από τους επιδιωκόμενους αποδέκτες και κανέναν άλλον. Η μέθοδος περιλαμβάνει τη λήψη μη κρυπτογραφημένων δεδομένων (unencrypted data), όπως ένα απλό κείμενο και στη συνέχεια την κρυπτογράφηση χρησιμοποιώντας έναν μαθηματικό αλγόριθμο, γνωστό ως κρυπτογράφο (cipher). Αυτό παράγει ένα κρυπτογράφημα (ciphertext), ένα κομμάτι πληροφοριών που είναι εντελώς άχρηστο και ανόητο μέχρι να αποκρυπτογραφηθεί. Αυτή η μέθοδος κρυπτογράφησης είναι γνωστή ως κρυπτογράφηση συμμετρικού κλειδιού (symmetric-key cryptography) [21].

Ένα πρώιμο παράδειγμα κρυπτογραφίας ήταν ο κωδικός του Καίσαρα, τον οποίο χρησιμοποίησε ο Ιούλιος Καίσαρας για την προστασία των ρωμαϊκών στρατιωτικών μυστικών. Στον κωδικό του Καίσαρα, κάθε γράμμα σε ένα μήνυμα αντικαθίσταται από κάποιο άλλο γράμμα σε σταθερή απόσταση 3 γραμμάτων προς τα αριστερά στο

αλφάβητο. Αυτή η γνώση ήταν ουσιαστικά το κλειδί για την αποκρυπτογράφηση του μηνύματος. Η σύγχρονη κρυπτογραφία λειτουργεί στο ίδιο επίπεδο, αν και με πολύ μεγαλύτερα επίπεδα πολυπλοκότητας [21].

Η βάση κώδικα (codebase/code base) για τους περισσότερους κρυπτογράφους είναι έργο ανοιχτού κώδικα (open source). Αυτό σημαίνει ότι ο κώδικάς τους μπορεί να εξεταστεί από οποιονδήποτε. Ο πιο ευρέως χρησιμοποιούμενος κρυπτογράφος στον κόσμο, που ονομάζεται AES (Advanced Encryption Standard), είναι ελεύθερος προς χρήση από τον οποιονδήποτε και ο κώδικας του είναι ανοιχτός για προβολή από το κοινό. Ως αποτέλεσμα, έχει μελετηθεί με μεγάλη λεπτομέρεια και μέχρι σήμερα δεν έχουν εντοπιστεί τρωτά σημεία. Αυτός ο κώδικας χρησιμοποιείται επίσης από την NSA, την υπηρεσία πληροφοριών των Ηνωμένων Πολιτειών, ως το εργαλείο επιλογής για την κρυπτογράφηση πληροφοριών. Ως εκ τούτου, η ασφάλεια των πληροφοριών που καταγράφονται σε ένα blockchain μπορεί να θεωρηθεί ότι είναι εξίσου ασφαλής με κάποια από τα πιο ευαίσθητα μυστικά στον κόσμο [21].

Σε blockchain, η κρυπτογραφία χρησιμοποιείται κυρίως για δύο σκοπούς [21]:

- Εξασφάλιση της ταυτότητας του αποστολέα συναλλαγών.
- Εξασφάλιση ότι τα προηγούμενα αρχεία δεν μπορούν να αλλοιωθούν.

Η τεχνολογία blockchain χρησιμοποιεί την κρυπτογραφία ως μέσο προστασίας των ταυτοτήτων των χρηστών, διασφαλίζοντας ότι οι συναλλαγές γίνονται με ασφάλεια και εξασφαλίζοντας όλες τις πληροφορίες. Ως εκ τούτου, όποιος χρησιμοποιεί blockchain μπορεί να έχει πλήρη εμπιστοσύνη ότι μόλις καταγραφεί κάτι σε blockchain, αυτό γίνεται νόμιμα και με ασφαλή τρόπο [21].

Παρά το γεγονός ότι βασίζεται σε ένα παρόμοιο πλαίσιο, ο τύπος κρυπτογραφίας που χρησιμοποιείται σε blockchain, δηλαδή η κρυπτογραφία δημόσιου κλειδιού, είναι

πολύ καλύτερα προσαρμοσμένος στις λειτουργίες που σχετίζονται με την τεχνολογία από την κρυπτογράφηση συμμετρικού κλειδιού [21].

Τι είναι η κρυπτογραφία δημόσιου κλειδιού;

Η κρυπτογραφία δημόσιου κλειδιού (public-key cryptography), επίσης γνωστή ως ασύμμετρη κρυπτογραφία (asymmetric cryptography), αντιπροσωπεύει μια βελτίωση στην τυπική κρυπτογραφία συμμετρικού κλειδιού, καθώς επιτρέπει την μεταφορά πληροφοριών μέσω ενός δημόσιου κλειδιού που μπορεί να μοιραστεί σε άτομα [21].

Αντί να χρησιμοποιείται ένα μόνο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση, όπως συμβαίνει με την κρυπτογράφηση συμμετρικού κλειδιού, στην περίπτωση αυτή, χρησιμοποιούνται ξεχωριστά κλειδιά, ένα δημόσιο και ένας ιδιωτικό. [21].

Ένας συνδυασμός δημόσιου κλειδιού και ιδιωτικού κρυπτογραφεί τις πληροφορίες, ενώ το ιδιωτικό κλειδί του παραλήπτη και το δημόσιο κλειδί του αποστολέα το αποκρυπτογραφούν. Ένας χρήστης μπορεί να στείλει το δημόσιο κλειδί σε οποιονδήποτε χωρίς να ανησυχεί ότι κάποιος θα αποκτήσει πρόσβαση στο ιδιωτικό κλειδί του. Ο αποστολέας μπορεί να κρυπτογραφήσει αρχεία για τα οποία μπορεί να είναι σίγουρος ότι θα αποκρυπτογραφηθούν μόνο από το συμβαλλόμενο μέλος [21].

Επιπλέον, μέσω κρυπτογραφίας δημόσιου κλειδιού (public-key cryptography) παράγεται ψηφιακή υπογραφή, εξασφαλίζοντας την ακεραιότητα των δεδομένων που εμφανίζονται. Αυτό γίνεται συνδυάζοντας το ιδιωτικό κλειδί ενός χρήστη με τα δεδομένα που πρέπει να υπογραφούν, μέσω ενός μαθηματικού αλγορίθμου [21].

Δεδομένου ότι τα ίδια τα δεδομένα είναι μέρος της ψηφιακής υπογραφής, το δίκτυο δεν θα τα αναγνωρίσει ως έγκυρα αν τυχόν έχει παραβιαστεί οποιοδήποτε μέρος του. Η επεξεργασία ακόμα και της παραμικρής πτυχής των δεδομένων αναδιαμορφώνει ολόκληρη την υπογραφή, καθιστώντας την ψευδή. Μέσω αυτού, η τεχνολογία blockchain είναι σε θέση να εγγυηθεί ότι όλα τα δεδομένα που καταγράφονται σε αυτό είναι αληθή και ακριβή. Οι ψηφιακές υπογραφές είναι εκείνες που δίνουν στα δεδομένα που καταγράφονται σε ένα blockchain την ακεραιότητά τους [21].

2.2 Hashing

Η αξιοπιστία και η ακεραιότητα του blockchain βασίζεται στην μη ύπαρξη πιθανότητας αποδοχής ή καταγραφής τυχόν δόλιων δεδομένων ή συναλλαγών, όπως διπλής δαπάνης. Πράγματι, ο κατακερματισμός (hashing – θα προτιμηθεί ο ξένος όρος στην παρούσα εργασία) είναι ένας ακρογωνιαίος λίθος της τεχνολογίας στο σύνολό της και τα βασικά συστατικά για τη διατήρηση της αξιοπιστίας της [21].

Hashing είναι η διαδικασία λήψης εισόδου οποιουδήποτε μήκους και μετατροπής της σε κρυπτογραφική σταθερή έξοδο μέσω ενός μαθηματικού αλγορίθμου (για παράδειγμα το Bitcoin χρησιμοποιεί το SHA-256). Παραδείγματα τέτοιων εισροών μπορούν να περιλαμβάνουν μία σύντομη πληροφορία, όπως ένα μήνυμα ή μια τεράστια μνήμη cache από διάφορα στοιχεία, όπως ένα μπλοκ συναλλαγών ή ακόμα και όλες οι πληροφορίες που περιέχονται στο διαδίκτυο [21].

2.3 Εξασφάλιση δεδομένων με τη συμβολή του Hashing

Το Hashing αυξάνει δραματικά την ασφάλεια των δεδομένων. Όποιος προσπαθεί να αποκρυπτογραφήσει τα δεδομένα εξετάζοντας το hash δεν θα μπορεί να υπολογίσει το μήκος των κρυπτογραφημένων πληροφοριών με βάση το hash. Μια

κρυπτογραφική συνάρτηση κατακερματισμού (cryptographic hash function) πρέπει να έχει αρκετές κρίσιμες ιδιότητες για να θεωρηθεί χρήσιμη, όπως [21]:

- Αδυναμία να παράγεται η ίδια τιμή κατακερματισμού (hash value) για διαφορετικές εισροές. Αυτό είναι σημαντικό επειδή, αν δεν συνέβαινε, θα ήταν αδύνατο να παρακολουθείται η αυθεντικότητα των εισροών.
- Παραγωγή πάντοτε της ίδιας τιμής κατακερματισμού από το ίδιο μήνυμα.. Η σημασία του είναι παρόμοια με προηγούμενως.
- Ταχεία παραγωγή ενός hash για οποιοδήποτε δεδομένο μήνυμα. Αν δε συνέβαινε αυτό, το σύστημα δεν θα ήταν αποτελεσματικό.
- Αδυναμία προσδιορισμού της εισόδου με βάση την τιμή κατακερματισμού. Αυτή είναι μία από τις κυριότερες πτυχές και ιδιότητες του κατακερματισμού και της εξασφάλισης δεδομένων.
- Το γεγονός ότι ακόμα και η παραμικρή αλλαγή σε μια είσοδο αλλάζει τελείως το hash. Αυτό είναι επίσης θέμα ασφάλειας. Εάν μια μικρή αλλαγή έκανε μόνο μια μικρή διαφορά, θα ήταν πολύ πιο εύκολο να υπολογίσουμε ποια ήταν η είσοδος. Όσο καλύτερος και πιο σύνθετος είναι ο αλγόριθμος κατακερματισμού, τόσο μεγαλύτερος θα είναι ο αντίκτυπος της αλλαγής μιας εισόδου στα δεδομένα εξόδου.

Το Hashing διασφαλίζει τα δεδομένα με την παροχή βεβαιότητας ότι δεν έχει παραβιαστεί πριν εμφανιστεί από τον προοριζόμενο παραλήπτη. Έτσι, για παράδειγμα, εάν γίνει λήψη ενός αρχείου που περιέχει ευαίσθητες πληροφορίες, είναι δυνατόν το αρχείο να εκτελεστεί μέσω ενός αλγορίθμου κατακερματισμού, να υπολογιστεί το hash αυτών των δεδομένων και να συγκριθεί με αυτό που εμφανίζεται από τον αποστολέα των εν λόγω δεδομένων. Εάν τα hashes δεν ταιριάζουν, υπάρχει βεβαιότητα ότι το αρχείο τροποποιήθηκε πριν τη λήψη του.

Το πρώτο block ενός blockchain περιέχει τις συναλλαγές του, που όταν συνδυάζονται και επικυρώνονται, παράγουν ένα μοναδικό hash. Αυτό το hash και όλες οι νέες συναλλαγές που υποβάλλονται σε επεξεργασία στη συνέχεια χρησιμοποιούνται ως είσοδος για να δημιουργήσουν ένα ολοκαίνουργιο hash που χρησιμοποιείται στο επόμενο τμήμα της αλυσίδας. Αυτό σημαίνει ότι κάθε block συνδέεται πίσω στο προηγούμενο block μέσω του hash του, σχηματίζοντας μια αλυσίδα πίσω στο αρχικό block, εξού και το όνομα blockchain. Με αυτόν τον τρόπο, οι συναλλαγές μπορούν να προστεθούν με ασφάλεια, εφόσον οι κόμβοι του δικτύου συμφωνούν ως προς το πως πρέπει να είναι το hash [21].

Το Hashing αποτελεί βασική αρχή και πρωταρχική πτυχή της αμετάβλητης και καθοριστικής δυναμικής της τεχνολογίας blockchain. Διατηρεί την αυθεντικότητα των δεδομένων που καταγράφονται και προβάλλονται, και ως εκ τούτου, την ακεραιότητα ενός blockchain στο σύνολό του. Είναι μια από τις πιο τεχνικές πτυχές της τεχνολογίας, ωστόσο η κατανόησή του είναι ένα σταθερό βήμα στην κατανόηση του τρόπου λειτουργίας του blockchain και του ανυπολόγιστου δυναμικού και αξίας που έχει [21].

2.4 Δέντρα Merkle

Ένα δέντρο merkle (merkle tree), γνωστό αλλιώς και ως δέντρο κατακερματισμού (hash tree), είναι μια δομή δεδομένων που έχει χρησιμοποιηθεί για την καταγραφή δεδομένων σε ένα blockchain με ασφαλή και αποδοτικό τρόπο. Η ιδέα κατοχυρώθηκε με δίπλωμα ευρεσιτεχνίας από τον Ralph Merkle το 1979.

Το σύστημα λειτουργεί με την εκτέλεση ενός block συναλλαγών μέσω ενός αλγορίθμου για τη δημιουργία ενός hash ως μέσο επαλήθευσης της εγκυρότητας αυτών των δεδομένων με βάση τις αρχικές συναλλαγές. Το block συναλλαγών στο

σύνολό του δεν εκτελείται μέσω μιας συνάρτησης κατακερματισμού αμέσως, αλλά κάθε συναλλαγή κατακερματίζεται. Οι συναλλαγές έπειτα συνδέονται και κατακερματίζονται μαζί. Τελικά, αυτό οδηγεί στη δημιουργία ενός hash για ολόκληρο το block [21].

Όταν απεικονίζεται, αν και απλοποιημένα, η δομή του μοιάζει με εκείνη ενός δέντρου, καθώς κάθε block θα περιέχει κανονικά εκατοντάδες, αν όχι χιλιάδες, συναλλαγών.

Τα δέντρα Merkle είναι ιδιαίτερα χρήσιμα καθώς επιτρέπουν σε οποιονδήποτε να επιβεβαιώσει την εγκυρότητα μιας μεμονωμένης συναλλαγής χωρίς να χρειαστεί να μεταφορτώσει ένα ολόκληρο blockchain. Για παράδειγμα, εφόσον έχετε τη ρίζα hash (12345678), μπορείτε εύκολα να επιβεβαιώσετε τη συναλλαγή (8) καταγράφοντας τα hashes (7) (56) and (1234). Εφ' όσον είναι όλα παρόντα σε ένα blockchain, το ίδιο θα ισχύει και για τη συναλλαγή (8).

Το Hash της ρίζας merkle κανονικά περιέχεται σε μια κεφαλίδα block μαζί με:

- Το hash του προηγούμενου block
- Τη Χρονοσήμανση
- Το Nonce
- Ο αριθμός έκδοσης block
- Ο τρέχων βαθμός δυσκολίας

Κεφάλαιο 3

3.1 Περιπτώσεις χρήσεων

Τώρα που έγιναν κατανοητές οι πολλές θεωρητικές πτυχές της τεχνολογίας blockchain, είναι σημαντικό να αναφερθούν οι τρόποι με τους οποίους χρησιμοποιείται πρακτικά. Αυτό το κεφάλαιο επικεντρώνεται στις εφαρμογές της πραγματικής ζωής του blockchain και στον αντίκτυπο που έχουν στον κόσμο. Ξεκινώντας από το πιο συνηθισμένο παράδειγμα των χρήσης του blockchain, το Bitcoin, θα διαπιστωθεί πώς το blockchain αλλάζει ριζικά την κυβέρνηση και τα οικονομικά, οδηγώντας μέχρι και στη διαμόρφωση του μέλλοντος του Διαδικτύου των πραγμάτων και της αποθήκευσης δεδομένων (data storage) [3].

3.2 Bitcoin

Η πιο δημοφιλής εκπροσώπηση της χρησιμοποίησης blockchain στον κόσμο είναι η κρυπτογράφηση Bitcoin. Στην καθαρότερη μορφή του, το Bitcoin μιμείται τα κοινά σε όλους νομίσματα, επειδή είναι μέσο ανταλλαγής ή αποθήκευσης αξίας. Στην πραγματικότητα, στα περισσότερα σύγχρονα νομισματικά συστήματα το νόμισμα δεν αντιπροσωπεύεται από ένα φυσικό προϊόν. Τα νομίσματα bitcoin διατηρούν την αξία τους και αναγνωρίζονται από μια κυβέρνηση ή ένα θεσμικό όργανο ως νόμιμη πηγή νομίσματος. Το bitcoin διαφέρει από το νόμισμα που υποστηρίζεται από την Κεντρική Τράπεζα επειδή χρησιμοποιεί τη δύναμη του Διαδικτύου ως μέσο για να λειτουργεί με διαφανή, κρυπτογραφημένο και αποκεντρωμένο τρόπο [3].

Δεδομένου ότι το bitcoin δεν απαιτεί επικύρωση από κυβέρνηση ή τράπεζα, πώς λειτουργεί μια τυπική συναλλαγή σε αυτό το πρώιμο παράδειγμα blockchain; Πρώτον, και τα δύο μέρη μιας τέτοιας συναλλαγής διαθέτουν δημόσιο και ιδιωτικό κλειδί που παρέχουν ψηφιακή υπογραφή - απόδειξη ιδιοκτησίας και σημείο αναφοράς

τόσο για τον αποστολέα όσο και για τον παραλήπτη. Ο αποστολέας εκδίδει μια επιθυμητή ποσότητα bitcoin στη δημόσια διεύθυνση του δέκτη. Αφού ολοκληρωθεί η μεταφορά, η συναλλαγή, η ψηφιακή υπογραφή καθώς και η χρονική σήμανση μεταδίδονται σε όλους τους κόμβους του δικτύου για επικύρωση. Μόλις οι κόμβοι του δικτύου επιβεβαιώσουν ότι η συναλλαγή είναι έγκυρη, το block που περιέχει τις πληροφορίες προστίθεται στην αλυσίδα παρόμοιων block που προηγούνται. Σε αυτό το σημείο, η μεταφορά προστίθεται αμετάκλητα σε ένα blockchain και είναι ανοιχτή προς οποιονδήποτε να τη δει και να επιβεβαιώσει ότι πραγματοποιήθηκε [3].

3.3 Εφαρμογές του blockchain

Ενώ το Bitcoin είναι σίγουρα ένα από τα πιο συνηθισμένα παραδείγματα χρήσης και εφαρμογής της τεχνολογίας blockchain, είναι σημαντικό να αναφερθεί ότι αυτή η μέθοδος πληρωμής είναι μόνο η κορυφή του παγόβουνου στις τρέχουσες περιπτώσεις χρήσης blockchain. Αυτή η εκκολαπτόμενη τεχνολογία έχει προοπτικές για πραγματικά πρακτικές εφαρμογές σε ένα ευρύ πεδίο δραστηριοτήτων [3].

Το ledger, για παράδειγμα, επιτρέπει μια ριζικά διαφορετική μέθοδο αποθήκευσης πληροφοριών. Οι πληροφορίες αυτές δεν μονοπωλούνται από μία μερίδα ανθρώπων αλλά ανήκουν και εξουσιοδοτούνται από ένα αποκεντρωμένο δίκτυο κόμβων. Αν αναλογιστεί κανείς τις συνέπειες αυτού του νέου τρόπου κατασκευής βάσεων δεδομένων, μπορεί να περιμένει πώς η εφαρμοσμένη τεχνολογία blockchain θα έχει πραγματικά ριζοσπαστικό αντίκτυπο σε πλήθος βιομηχανιών, αγορών και φιλανθρωπικών οργανισμών. Πέρα από αυτό, ο κρυπτογραφημένος χαρακτήρας της τεχνολογίας blockchain ανοίγει νέους τρόπους αποθήκευσης και διασφάλισης των συνεχώς αυξανόμενων δικτύων ανταλλαγής δεδομένων, τα οποία αυξάνουν σε κίνηση και τον όγκο κάθε χρόνο [3].

Μερικοί από τους κλάδους ανάπτυξης και εφαρμογής του blockchain είναι [3]:

- Αποκεντρωμένη κυβέρνηση
- Blockchain στον τραπεζικό τομέα
- Blockchain στην Υγειονομική Περίθαλψη
- Blockchain στην αγορά ακινήτων
- Blockchain και Διαδίκτυο των Πραγμάτων
- Αποθήκευση δεδομένων με χρήση τεχνολογίας blockchain

Η τεχνολογία blockchain θα χρησιμοποιηθεί για τη δημιουργία νέων, αποκεντρωμένων δικτύων αποθήκευσης δεδομένων, τα οποία θα επαναφέρουν τη δύναμη επιλογής στα χέρια του τελικού χρήστη [3].

Κεφάλαιο 4

4.1 Geospatial blockchain

Πολλοί ενδιαφέρονται για την τεχνολογία blockchain και πολλοί ερευνητές εξετάζουν τρόπους με τους οποίους το blockchain μπορεί να χρησιμοποιηθεί σε γεωχωρικά συστήματα (geospatial systems). Αυτό αναμένεται επειδή τα γεωχωρικά συστήματα έχουν κάνει πολύ καλή χρήση της τεχνολογίας υπολογιστών (πχ βάσεις δεδομένων, δίκτυα, αποθηκευτικό νέφος). Η γεωχωρική τεχνολογία (geospatial technology) ενσωματώνεται ολοένα και περισσότερο σε άλλα συστήματα όπως το BIM (Building Information Modeling), το BI (Business Intelligence), το BPE (Bitcoin Price Equivalence) και ούτω καθεξής. Ως εκ τούτου, θεωρείται πως σύντομα θα αγκαλιάσει την τεχνολογία blockchain [22].

4.2 Blockchain και γεωχωρικά συστήματα

Η αλυσίδα στο blockchain είναι η αλυσίδα συναλλαγών με τη μορφή καταχώρησης δεδομένων για περιουσιακά στοιχεία τα οποία θα μπορούσαν να είναι χρήματα, εικόνες, δεδομένα, χάρτες, έγγραφα κλπ. Στην πραγματικότητα, όσα πράγματι διεκπεριώνονται είναι μάρκες/κέρματα (tokens) που περιέχουν τα μεταδεδομένα (metadata) των περιουσιακών στοιχείων. Η πραγματική φυσική μεταφορά συμβαίνει ξεχωριστά. Το block αναφέρεται στην ομαδοποίηση συναφών συναλλαγών. Ένας τρόπος να εξεταστεί ένα blockchain είναι να θεωρηθεί ως ledger όπου εισάγονται όλες οι συναλλαγές [22].

4.3 Διαφορά μεταξύ blockchain και βάσης δεδομένων

Τα blockchains είναι ανοιχτά σε όλα τα μέλη, επομένως οι συναλλαγές είναι διαθέσιμες σε όλα τα μέλη. Δεν υπάρχουν κεντρικοί διαχειριστές, καθώς πρόκειται

για ένα δίκτυο peer-to-peer. Κάθε συναλλαγή που εισάγεται στο blockchain επαληθεύεται και εγκρίνεται με συναίνεση μεταξύ των μελών. Ωστόσο, υπάρχουν επικυρωτές που ονομάζονται miners οι οποίοι μπορούν να ελέγξουν τις συναλλαγές και να τις επικυρώσουν. Τα δύο βασικά χαρακτηριστικά των blockchains είναι η εμπιστοσύνη και η αμεταβλητότητα-σταθερότητα. Ακριβώς όπως στην επιχείρηση όπου οι συναλλαγές βασίζονται στην εμπιστοσύνη, έτσι και τα μέλη λειτουργούν με εμπιστοσύνη. Η σταθερότητα εξασφαλίζεται με την αποτροπή της τροποποίησης ή διαγραφής μιας εγγραφής μιας συναλλαγής. Όταν ένα μέλος πραγματοποιεί μια συναλλαγή, επισφραγίζεται με μία συγκεκριμένη ημερομηνία και ώρα που παράγονται από τον υπολογιστή χρησιμοποιώντας το ιδιωτικό κλειδί των μελών [22].

Κάθε επόμενη συναλλαγή είναι παρόμοια επισφραγισμένη και δημιουργείται ένα νέο κλειδί που περιλαμβάνει το παλαιότερο κλειδί [22].

Τι συμβαίνει εάν η αλλαγή είναι γνήσια; Υπάρχει μια πιθανότητα διακλάδωσης (forking) και η προσωρινή δημιουργία δύο δικτύων από το ένα. Αυτό μπορεί να συμβεί με δύο τρόπους: αν δύο miners βρίσκουν ένα νέο block σχεδόν την ίδια στιγμή ή εάν υπάρχει αλλαγή στους κανόνες επικύρωσης ενός block [22].

Μία μαλακή διακλάδωση (soft fork) λαμβάνει χώρα εάν οι νέοι κανόνες είναι συμβατοί προς τα πίσω. Μία σκληρή διακλάδωση (hard fork) λαμβάνει χώρα εάν εισαχθεί ένα νέο λογισμικό, το οποίο δεν είναι συμβατό με το προηγούμενο. Μια τρίτη διακλάδωση που ονομάζεται μαλακή διακλάδωση ενεργοποιημένη από τον χρήστη [User Activated Soft Fork (UASF)] είναι αμφιλεγόμενη επειδή σημαίνει ότι οι αναβαθμίσεις λογισμικού ξεκινούν από τους χρήστες και όχι από τους αρχικούς προγραμματιστές [22].

Πρέπει να γίνει κατανοητό ότι το ledger είναι ουσιαστικά μια βάση δεδομένων συναλλαγών. Ένα blockchain έχει νόημα εάν το ledger μοιράζεται και η είσοδος των συναλλαγών μπορεί να γίνει από μια πληθώρα ατόμων που μπορεί να μην είναι γνωστά μεταξύ τους και ως εκ τούτου δεν υπάρχει εγγενής εμπιστοσύνη μεταξύ αυτών. Η αποδεκτή λύση σε μια τέτοια κατάσταση είναι η δρομολόγηση τέτοιων συναλλαγών μέσω ενός αξιόπιστου διαμεσολαβητή γνωστού σε κάθε άτομο, αλλά αυτό αυξάνει το κόστος και τον χρόνο επεξεργασίας [22].

Σε ένα blockchain ένας τέτοιος διαμεσολαβητής αντικαθίσταται από ένα δίκτυο peer to peer, στο οποίο η εξουσιοδότηση και η εγκυρότητα των συναλλαγών επιτυγχάνεται μέσω μιας διαδικασίας συναίνεσης μεταξύ των μελών. Ως εκ τούτου, ένα πολυοργανικό δίκτυο το οποίο χρειάζεται να εργαστεί χωρίς διαμεσολάβηση, του οποίου τα μέλη δεν γνωρίζονται μεταξύ τους επαρκώς ώστε να είναι σε θέση να παρέχουν εμπιστοσύνη στα πλαίσια ενός δικτύου που απαιτεί ανοιχτό πνεύμα, θα ήταν ένας ιδανικός υποψήφιος για την υλοποίηση τεχνολογίας blockchain [22].

Ωστόσο, αν υπάρχει ανάγκη για κεντρικό έλεγχο, εμπιστευτικότητα, γρήγορη απόδοση και υψηλή επεκτασιμότητα, τότε μπορεί να είναι λογικό να χρησιμοποιηθεί μια κανονική κατανεμημένη βάση δεδομένων [22].

4.4 Τύποι blockchain

Υπάρχουν τρεις τύποι blockchain, δημόσιος, ιδιωτικός και το consortium(blockchain κοινοπραξίας) . Η πιο γνωστή υλοποίηση ενός δημόσιου blockchain είναι το δίκτυο Bitcoin. Εδώ ένα δυνητικό μέλος πρέπει να ανοίξει ένα πορτοφόλι στο οποίο το σύστημα εκχωρεί ένα ιδιωτικό κλειδί. Το μέλος μπορεί πλέον να συναλλάσσεται με άλλους στο δίκτυο, καταβάλλοντας bitcoins για αγαθά, υπηρεσίες, δεδομένα, έγγραφα κ.λπ. Μπορεί να δούμε σύντομα ότι οι τράπεζες θα

προσφύγουν στη χρήση της τεχνολογίας blockchain, όχι άμεσα αλλά όχι στο πολύ μακρινό μέλλον [22].

Το δημόσιο blockchain (public blockchain) έχει δύο μειονεκτήματα. Το πρώτο είναι η διαδικασία επικύρωσης η οποία μπορεί να χρειαστεί χρόνο, καθώς υπάρχουν πολλοί χρήστες. Το δεύτερο είναι το μέγεθος του block το οποίο δεν μπορεί να είναι πολύ μεγάλο, επομένως μπορούν να μεταφερθούν μόνο οι λεπτομέρειες της συναλλαγής και όχι το αντικείμενο της συναλλαγής, για παράδειγμα τα έγγραφα [22].

Από την άλλη πλευρά, τα ιδιωτικά blockchains (private blockchains) μπορούν να δημιουργηθούν και να λειτουργούν από ιδρύματα όπως οι κυβερνητικές υπηρεσίες, οι βιομηχανίες, οι εταιρείες και οι Μη Κυβερνητικές Οργανώσεις. Το ιδιωτικό blockchain αποφεύγει αυτά τα προβλήματα περιορίζοντας τον αριθμό των χρηστών. Η ιδιότητα μέλους σε ένα ιδιωτικό blockchain αποκτάται κατόπιν πρόσκλησης. Παρά το γεγονός ότι και άλλοι μπορεί να δουν τις συναλλαγές, δεν μπορούν να συμμετάσχουν σε αυτές. Οι κανόνες που διέπουν το ιδιωτικό blockchain μπορούν να αλλάξουν εύκολα από τους διαχειριστές και η αναστροφή των συναλλαγών μπορεί να επιτραπεί από αυτούς [22].

Το Consortium blockchain (blockchain κοινοπραξίας) είναι ένα blockchain όπου η διαδικασία συναίνεσης ελέγχεται από ένα προεπιλεγμένο σύνολο κόμβων. Τα consortium είναι ταχύτερα και παρέχουν μεγαλύτερη ασφάλεια στην συναλλαγή. Αυτά τα blockchains μπορεί να θεωρηθούν «μερικώς αποκεντρωμένα». Χρησιμοποιούνται κυρίως στον τραπεζικό τομέα. Τέτοια παραδείγματα είναι το R3, το Corda, το b3I και το EWF [23].

4.5 Διεύρυνση του ορίζοντα σε γεωχωρική

Σε γεωχωρικούς όρους, δύο τομείς που προσελκύουν την υλοποίηση του blockchain είναι οι συναλλαγές γης και τα αποθετήρια δεδομένων. Στην περίπτωση των αρχείων γης, δεν υπάρχει καθιερωμένη εμπιστοσύνη μεταξύ των συμμετεχόντων και υπάρχει ανάγκη για διαφάνεια. Ο ασθενέστερος δεσμός, ο διαμεσολαβητής υπό τη μορφή του υπαλλήλου καταγραφής, μπορεί να εξαλειφθεί, αποτρέποντας τις ψευδείς συναλλαγές, παγιδεύοντας αμέσως και αντικαθιστώντας τον με το αντίγραφο συναίνεσης [22].

Σε ένα περιστασιακό έγγραφο ORF (Observer Research foundation) σχετικά με την εξασφάλιση δικαιωμάτων ιδιοκτησίας στην Ινδία μέσω της τεχνολογίας κατανεμημένου λογοτύπου (Distributed Ledger Technology), η Meghna Bal έχει καλύψει αυτές τις πτυχές εκτεταμένα. Σύμφωνα με αυτήν, η Εσθονία, η Ονδούρα, η Γεωργία, η Γκάνα και η Σουηδία εξετάζουν τα συστήματα μητρώου γης που βασίζονται σε blockchain και από αυτά, η Σουηδία έχει προχωρήσει αρκετά με ένα πιλοτικό πρόγραμμα [22].

Αναφερόμενη στο έγγραφο "Κατανόηση της ανάγκης αλλαγής", η Lantmateriet (Σουηδική Αρχή Χαρτογράφησης, Κτηματολογίου και Χωροταξίας) συνεργάστηκε με την Kairos Future (εταιρεία παροχής συμβουλών), την Telia Company (κυρίαρχη φορέα τηλεπικοινωνιών της Σουηδίας) και την Chroma Way (μια εταιρεία λύσεων blockchain) για να αναπτύξει έναν καινοτόμο τρόπο αντιμετώπισης των ζητημάτων που μαστίζουν το ισχύον πλαίσιο του κτηματολογίου [22].

Εφάρμοσαν ένα σχέδιο για τη δημιουργία μιας εφαρμογής που θα χρησιμοποιεί τεχνολογία blockchain για τη διευκόλυνση των συναλλαγών. Η επικοινωνία μεταξύ των διαφόρων ενδιαφερόμενων μερών (μεσίτης ακινήτων, τράπεζα, αγοραστής,

πωλητής και η Lantmateriet) διεξάγεται μέσω της εφαρμογής. Όλες οι πληροφορίες σχετικά με την ιδιοκτησία (ο σημερινός ιδιοκτήτης, οι κτηματολογικές έρευνες, μεταξύ άλλων) ψηφιοποιούνται και τοποθετούνται στο blockchain. Οι έξυπνες συμβάσεις διασφαλίζουν ότι αυτός ο ψηφιοποιημένος χώρος ρυθμίζεται από ορισμένους κανόνες (πχ από τις κανονιστικές πολιτικές της Σουηδίας) [22].

Η εφαρμογή χρησιμοποιείται στη συνέχεια ως διεπαφή για να διευκολύνει όλες τις συναλλαγές που αφορούν σε συγκεκριμένες ιδιοκτησίες. Η συμφωνία αγοράς εκχωρείται σε ένα μοναδικό κώδικα κατακερματισμού (hash code) και τοποθετείται στο blockchain. Οι τράπεζες, οι κτηματομεσίτες, οι αγοραστές και η Lantmateriet μπορούν να τεκμηριώσουν την ειλικρίνεια αυτής της συμφωνίας αγοράς και άλλων εγγράφων μέσω της μοναδικής ψηφιακής υπογραφής τους (κατακερματισμός στο blockchain). Οι τράπεζες μπορούν επίσης να διασφαλίσουν ότι ο αγοραστής διαθέτει αρκετά χρήματα στο λογαριασμό του ώστε να πραγματοποιήσει τη συναλλαγή. Η Lantmateriet μπορεί στη συνέχεια να εγγραφεί και να χορηγήσει τίτλο στον αγοραστή [22].

4.6 Το πεδίο δράσης του Blockchain στο IoT

Ένας άλλος σημαντικός τομέας όπου το blockchain μπορεί να χρησιμοποιηθεί αποτελεσματικά μαζί με τις γεωπεριβαλλοντικές τεχνολογίες είναι το Διαδίκτυο των Πραγμάτων [Internet of Things (IoT)]. Σήμερα, το IoT δημιουργεί μια διανοητική εικόνα ενός σύνθετου δικτύου ανθρώπων και αντικειμένων, τα οποία διαβιβάζουν δεδομένα μεταξύ τους [22].

Οι ερωτήσεις είναι ποια είναι τα δεδομένα, πώς επικυρώνονται, πώς προστατεύονται τα πράγματα και ο άνθρωπος από την παράνομη πρόσβαση [22].

Για παράδειγμα, θα μπορούσε ένα αυτόνομο φορτηγό μεταφοράς, το οποίο βασίζεται στη λειτουργία αισθητήρων, να υποκλαπεί και να οδηγηθεί προς λάθος κατεύθυνση; Θεωρούμε ότι τα δεδομένα που φέρουν τις οδηγίες ότι είναι συναλλαγές. Εάν το δίκτυο βρίσκεται σε blockchain, τότε η διαδικασία συναίνεσης θα βοηθήσει στην επικύρωση των συναλλαγών και θα εξαλείψει τις λανθασμένες οδηγίες επειδή οι παράνομες συναλλαγές θα παγιδευτούν [22].

Η διαχείριση επιχειρησιακών διαδικασιών [Business Process Management (BPM)] θα μπορούσε να εκτελέσει την εσωτερική διαδικασία κάθε οντότητας και να ενεργήσει ως συνδετικός ιστός στη μία πλευρά της συναλλαγής ή στην άλλη. Οι έξυπνες συμβάσεις θα επέκτειναν τις δυνατότητες του BPM πέρα από τους τέσσερις τοίχους ενός οργανισμού, ενεργώντας ως διαμεσολαβητής μεταξύ δύο οντοτήτων [22].

4.7 Γεωπεριφερειακός δεσμός με blockchain

Μια πολύ ενδιαφέρουσα εξέλιξη που συνδέει το γεωχωρικά δεδομένα με την τεχνολογία του blockchain είναι το FOAM, το οποίο αναπτύχθηκε από τους Kristoffer Joseffson, Ekaterina Zavyalova και Ryan John King της Ethereum. Το FOAM είναι ένα ανοιχτό πρωτόκολλο για τις αγορές γεωχωρικών δεδομένων στο blockchain του Ethereum. Αυτό συνδέει τις συντεταγμένες του blockchain με κάθε θέση εντόπισης. Το κρυπτοχωρικό επίπεδο (Crypto-spatial layer) περιέχει τη ακριβή τοποθεσία της γεωχωρικής θέσης και το Χωρικό Πορτοφόλι (Spatial Wallet) σε αυτή την τοποθεσία. Αυτά τα Χωρικά Πορτοφόλια δημιουργούνται με χρήση των Κερμάτων FOAM που δημιουργούν επίσης χωρικά κέρματα (spatial tokens). Τα χωρικά κέρματα δημιουργούν μάρκες χρησιμότητας (utility markers) με μοναδικές διευθύνσεις συντεταγμένων [22].

Ίσως η μεγαλύτερη εφαρμογή να είναι οι γεννήτριες δεδομένων (data generators) που θα μπορούσαν να καταθέσουν τα δεδομένα σε μια κρυπτοχωρική συντεταγμένη (crypto spatial coordinate), να της προσδώσουν χωρικά κέρματα και να θέσουν μηχανισμούς τιμολόγησης για τη χρήση τους. Τα δεδομένα θα μπορούσαν να περιλαμβάνουν δεδομένα από δορυφόρους, χάρτες, δεδομένα αγροτεμαχίων, δεδομένα τρισδιάστατης απεικόνιση και πολλά άλλα. Έτσι θα μπορούσε κανείς να δει μια αλλαγή στον τρόπο με τον οποίο τα χωρικά δεδομένα (πχ από τους δορυφόρους και τα μη επανδρωμένα αεροσκάφη) θα μπορούσαν εύκολα να αποτιμηθούν και να διανεμηθούν [22].

Κεφάλαιο 5

5.1 Hyperledger

Το Hyperledger είναι μια συλλογική προσπάθεια ανοιχτού κώδικα που δημιουργήθηκε με σκοπό την διεπαγγελματική προώθηση των τεχνολογιών blockchain. Πρόκειται για μια παγκόσμια συνεργασία, που φιλοξενείται από το Ίδρυμα Linux (The Linux Foundation), συμπεριλαμβανομένων των ηγετών στους τομείς της χρηματοδότησης, της Τραπεζικής, του Διαδικτύου των Πραγμάτων, των αλυσίδων εφοδιασμού, της βιομηχανοποίησης και της τεχνολογίας [24].

Το Hyperledger δεν υποστηρίζει το Bitcoin ή οποιαδήποτε άλλο κρυπτονόμισμα. Αντιθέτως, η πλατφόρμα δίνει μεγάλη έμφαση στην τεχνολογία blockchain. Αυτό συμβαίνει επειδή το blockchain έχει τη δυνατότητα να χτίσει μια νέα γενιά εφαρμογών συναλλαγών που δημιουργούν εμπιστοσύνη, λογοδοσία και διαφάνεια στον πυρήνα τους, ενώ παράλληλα εξορθολογίζει τις επιχειρηματικές διαδικασίες και τους νομικούς περιορισμούς [24].

Με το Hyperledger, το Ίδρυμα Linux στοχεύει στη δημιουργία ενός περιβάλλοντος στο οποίο οι κοινότητες προγραμματιστών λογισμικού και οι εταιρείες συναντιούνται και συντονίζονται για την οικοδόμηση πλαισίων blockchain (blockchain frameworks). Το ίδρυμα Linux ίδρυσε την πλατφόρμα τον Δεκέμβριο του 2015. Τον Φεβρουάριο του 2016 ανακοίνωσε τα πρώτα ιδρυτικά μέλη, ενώ ένα μήνα μετά προστέθηκαν άλλα δέκα μέλη [24].

Σήμερα, η Hyperledger έχει μια εντυπωσιακή λίστα με περισσότερα από 100 μέλη. Ο κατάλογος καλύπτει ένα ευρύ φάσμα γνωστών ηγετών της βιομηχανίας. Περιλαμβάνει επιχειρήσεις τεχνολογίας κινητικότητας όπως η Airbus και η Daimler,

εταιρείες πληροφορικής όπως η IBM, η Fujitsu, η SAP, η Huawei, η Nokia, η Intel και η Samsung, χρηματοπιστωτικά ιδρύματα όπως η Deutsche Börse, η American Express, η JP Morgan, η BBVA, η BNP Paribas και η Well Fargo, καθώς και νεοφυείς επιχειρήσεις blockchain (blockchain startups) όπως η Blockstream, η Netki, η Lykke, η Factom, η bloq και η Consensusys. Πολλές από τις μεγαλύτερες εταιρείες στον κόσμο της τεχνολογίας και του χρηματοπιστωτικού τομέα συναντώνται στο Hyperledger με μερικές από τις πιο σημαντικές νεοσύστατες εταιρείες [24].

Αποτελείται από περισσότερα από 10 στελέχη, τα περισσότερα με δεκαετίες εμπειρίας στον ανοιχτό κώδικα (open source) και στενές συνδέσεις με διάφορες βιομηχανίες. Χαρακτηριστικά παραδείγματα αποτελούν οι επικεφαλής του Ιδρύματος Apache και της Κοινοπραξίας W3C, καθώς και μηχανικοί της IBM και πολλοί άλλοι. Μερικά από τα μέλη του Hyperledger, όπως ο Richard Brown και ο Tamas Blumer, έχουν ήδη εργαστεί με το blockchain εδώ και χρόνια. Για τα μέλη της, το Hyperledger δεν παρέχει μόνο τεχνικές γνώσεις και πλαίσια λογισμικού αλλά και διάφορες επαφές με βιομηχανίες και προγραμματιστές [24].

Σχετικά νωρίς στην ιστορία του Hyperledger, έπρεπε να παρθεί μία σημαντική απόφαση. Ο εκτελεστικός διευθυντής Brian Behlendorf ρωτήθηκε αν θα υπάρξει ένα "Νόμισμα Hyperledger" (Hyperledger Coin), μια νομισματική μονάδα που θα τρέχει στα Hyperledger blockchains. Ο Behlendorf απάντησε ότι το ίδιο το έργο Hyperledger δεν θα οικοδομήσει ποτέ το δικό του κρυπτονόμισμα [24].

Η απόφαση αυτή διαμόρφωσε έντονα τους στρατηγικούς στόχους του Hyperledger για την οικοδόμηση βιομηχανικών εφαρμογών της τεχνολογίας blockchain και τον διακριτό διαχωρισμό του από τις επενδυτικές ενέργειες που συνήθως αναπτύσσονται

από block αλυσίδες με βάση το νόμισμα. Αυτό μπορεί να είναι πιο βαρετό, αλλά και πιο απλό στην τεχνολογία [24].

Η πλατφόρμα του Hyperledger στοχεύει στη "δημιουργία ενός επιχειρησιακού, ανοικτού πηγαίου κώδικα, διανεμημένου πλαισίου λογισμικού και βάσης κώδικα" και στη δημιουργία, προώθηση και διατήρηση μιας ανοικτής υποδομής. Επί του παρόντος, η Hyperledger είναι ο κύριος υπεύθυνος διαφόρων έργων όπως το Hyperledger Iroha, το Hyperledger Fabric, το Hyperledger Composer, Hyperledger Indy και άλλα.

Εκτός από τα παραπάνω έργα, το Hyperledger διαθέτει πολλά εργαλεία που στοχεύουν στην ευκολότερη και αποτελεσματικότερη πρόσβαση και ανάπτυξη blockchain [24].

5.2 Hyperledger Fabric

Από όλα τα έργα στα οποία δραστηριοποιείται η Hyperledger, το πιο ενδιαφέρον πιθανότατα είναι το Fabric της IBM. Αντί για ένα ενιαίο blockchain το Fabric είναι μια βάση για την ανάπτυξη λύσεων βασισμένων σε blockchain με αρθρωτή αρχιτεκτονική. Με το Fabric διαφορετικά εξαρτήματα των blockchains, όπως η συναίνεση και οι υπηρεσίες προσχώρησης μπορούν να γίνουν τύπου «τοποθέτηση και άμεσης λειτουργίας» (plug-and-play). Το Fabric έχει σχεδιαστεί για να παρέχει ένα πλαίσιο με το οποίο οι επιχειρήσεις μπορούν να συνθέσουν το δικό τους, μεμονωμένο δίκτυο blockchain που μπορεί να κλιμακωθεί γρήγορα σε περισσότερες από 1.000 συναλλαγές ανά δευτερόλεπτο [24].

Τι είναι το Fabric και πώς λειτουργεί;

Το πλαίσιο υλοποιείται στο Go. Είναι κατασκευασμένο για να προσφέρει στα blockchains της κοινοπραξίας διαφορετικούς βαθμούς αδειών. Το fabric βασίζεται σε

μεγάλο βαθμό σε ένα έξυπνο σύστημα συμβάσεων που ονομάζεται αλυσιδωτός κώδικας (Chaincode – θα προτιμηθεί ο ξένος όρος), στο οποίο κάθε ομότιμος ιστός λειτουργεί σε Docker containers, που αποτελούν τυποποιημένες μονάδες λογισμικού. [24].

Οι συμμετέχοντες πρέπει συνήθως να εγγραφούν για να λάβουν την άδεια να συμμετάσχουν και να εκδώσουν συναλλαγές σε ένα blockchain που είναι βασισμένο στο Fabric. Για να χρησιμοποιήσει τους πόρους πιο αποτελεσματικά, το Fabric έχει λιγότερους κόμβους από μια δημόσια αλυσίδα και υπολογίζει μαζικά τα δεδομένα με παράλληλο τρόπο, πράγμα που κάνει την κλίμακα Fabric πολύ καλύτερη από τις δημόσιες blockchains. Επίσης, η βασική του αρχιτεκτονική υποστηρίζει εμπιστευτικά δεδομένα, δίνοντας στα μέλη της μεγαλύτερη προστασία ιδιωτικού χαρακτήρα [24].

Μεγάλης αξίας είναι ο διαχωρισμός μεταξύ των λεγόμενων "Επικυρωτών" (Endorsers) από τους "Συναινετικούς κόμβους" (Consensus Nodes). Οι Endorsers έχουν τη δυνατότητα να δημιουργούν, να επικυρώνουν και να διαδίδουν τις συναλλαγές και τον chaincode, ενώ οι Consensus Nodes διατάσσουν τις ήδη επικυρωμένες συναλλαγές. Αυτός ο διαχωρισμός δεν ήταν ιδέα του Satoshi Nakamoto. Αντιθέτως, προέκυψε ως μια ανεπιθύμητη πραγματικότητα στα περισσότερα κρυπτονομίσματα. Βασική αρχή του Fabric είναι ο παραπάνω διαχωρισμός. Αυτό επιτρέπει στο Fabric, για παράδειγμα, να εφαρμόσει έναν καλύτερο καταμερισμό της εργασίας, έτσι ώστε να μην έχουν όλοι οι ομότιμοι τις ίδιες αρμοδιότητες [24].

Παρόλο που δεν έχει δικό του προσωπικό νόμισμα, το Fabric επιτρέπει στο χρήστη να καθορίζει τα στοιχεία από την πλευρά του πελάτη και να τα χρησιμοποιεί με το Συνθέτη του (Fabric Composer). Το πλαίσιο Έξυπνων Συμβάσεων τύπου Chaincode

(Chaincode Smart Contracts framework) της Fabric είναι παρόμοιο με το Ethereum: το Chaincode ορίζει την επιχειρησιακή λογική των περιουσιακών στοιχείων, τους κανόνες για την ανάγνωση και την τροποποίηση της λεγόμενης κατάστασης των περιουσιακών στοιχείων [24].

Εκτός από τα δημόσια blockchains των κρυπτονομισμάτων, το Fabric επιτρέπει στους συμμετέχοντες να δημιουργήσουν ένα ξεχωριστό κανάλι για τα περιουσιακά στοιχεία τους και, ως εκ τούτου, να απομονώσουν και να διαχωρίσουν τις συναλλαγές τους. Με αυτή τη μέθοδο, ο αλυσιδωτός κώδικας που απαιτείται για να διαβάσει και να αλλάξει την κατάσταση ενός περιουσιακού στοιχείου θα εγκατασταθεί μόνο σε ομότιμους που εμπλέκονται σε αυτή τη συγκεκριμένη επιχειρηματική υπόθεση [24].

Όπως και στα καλά προγράμματα συνομιλίας, τα blockchain του Fabric επιτρέπουν στο χρήστη να συμμετέχει τόσο σε ανοικτές όσο και σε ιδιωτικές αλληλεπιδράσεις.

Το Fabric χρησιμοποιεί υποδομή δημόσιου κλειδιού για την παραγωγή κρυπτογραφικών πιστοποιητικών που συνδέονται με οργανισμούς και χρήστες. Επομένως, είναι δυνατό να περιοριστούν τα δεδομένα και να παραχωρηθεί πρόσβαση σε συγκεκριμένους συμμετέχοντες [24].

Η δύναμη του Fabric φαίνεται να είναι ο υψηλός βαθμός ευελιξίας όσον αφορά την αδειοδότηση και την ιδιωτικότητα, επιτρέποντας ταυτόχρονα την υψηλή επεκτασιμότητα μέσω ενός πιο προηγμένου καταμερισμού της εργασίας των συμμετεχόντων στο δίκτυο [24].

Με λίγα λόγια, για την IBM, το Fabric χρησιμεύει ως ναυαρχίδα για την ανάπτυξη blockchain. Τον Μάρτιο του 2017, η IBM ξεκίνησε το IBM blockchain, μια υπηρεσία που επιτρέπει στους προγραμματιστές να "κατασκευάσουν γρήγορα και να φιλοξενήσουν ασφαλή δίκτυα τύπου blockchain στην IBM Cloud." Με αυτή την

κίνηση, η IBM συναγωνίζεται τη Microsoft, η οποία έχει από καιρό ενσωματώσει blockchains στην υπηρεσία Azure Cloud [24].

Ωστόσο, ενώ η Microsoft παρέχει απλά τη «φιλοξενία νέφους» (cloud host) σε διάφορα εξωτερικά blockchains, η IBM προωθεί σε μεγάλο βαθμό το δικό της blockchain πλαίσιο, το Fabric, για πολλές χρήσεις. Για παράδειγμα, στα τέλη Μαρτίου, η Natixis και η Trafigure συνεργάστηκαν με την IBM για να χρησιμοποιήσουν ένα blockchain βασισμένο στο Fabric για τη χρηματοδότηση του εμπορίου βασικών προϊόντων για συναλλαγές πετρελαίου στις ΗΠΑ. Όλα τα σημαντικά βήματα σε μια συναλλαγή πετρελαίου ψηφιοποιούνται στο blockchain, βελτιώνοντας σημαντικά τη διαφάνεια, την αποτελεσματικότητα και την ασφάλεια [24].

Τον Απρίλιο του ίδιου έτους, η IBM ανήγγειλε αρκετά νέα έργα blockchain που θα είχαν ως βάση το Fabric: Η εταιρεία συνεργάστηκε με την Sichuan Heijia για να δημιουργήσει μια πλατφόρμα βασισμένη σε blockchain για τις φαρμακευτικές προμήθειες. Τον ίδιο μήνα, η IBM άρχισε να συνεργάζεται με το Mizuho Financial Group της Ιαπωνίας και την ομώνυμη τράπεζα για να δημιουργήσει μια πλατφόρμα βασισμένη στο blockchain με σκοπό την εμπορική χρηματοδότηση. Τα έργα αυτά αποσκοπούν στον εξορθολογισμό των συναλλαγών και στη βελτίωση της αποτελεσματικότητας της αλυσίδας εφοδιασμού [14].

Σε ένα άλλο έργο που έγινε γνωστό τον Απρίλιο του 2017, η IBM συνεργάζεται με το Εθνικό Πανεπιστήμιο της Σιγκαπούρης για να αναπτύξει μια ενότητα για τη χρηματοοικονομική τεχνολογία με σκοπό τη βελτίωση της εκπαίδευσης του φοιτητή στον τομέα αυτό. Τέλος, τον Μάιο του 2017, η IBM επιλέχθηκε ως συνεργάτης των

Πτυχιακή Εργασία: BLOCKCHAIN AND ITS APPLICATION IN GEOSPATIAL DATA

TenneT, Sonnen και Vandebron για να αναπτύξει ένα blockchain για τη διαχείριση του ηλεκτρικού δικτύου στην Ολλανδία και τη Γερμανία [24].

Ενώ τα περισσότερα άλλα έργα που βασίζονται στην τεχνολογία blockchain επικεντρώνονται σε κρυπτονομίσματα και μάρκες, τα έργα γύρω από το Hyperledger επιδεικνύουν ισχυρές δυνατότητες να δημιουργήσουν τη ραχοκοκαλιά των μη νομισματικών βιομηχανικών εφαρμογών τεχνολογίας blockchain [24].

Κεφάλαιο 6

Στην παρούσα εργασία πραγματοποιήθηκε η υλοποίηση του Hyperledger όπως περιγράφεται και στην επίσημη ιστοσελίδα.

Πριν την υλοποίηση, έγινε η εγκατάσταση όλων των απαραίτητων προγραμμάτων στην πλατφόρμα στην οποία θα αναπτυχθεί το Hyperledger Fabric.

Αυτά είναι

- Τεκμηρίωση του SDK και του κόμβου SDK Hyperledger Fabric SDK .
- Hyperledger Fabric Java SDK .

Αφού κατέβηκαν, στη συνέχεια εγκαταστάθηκε το HyperLedger Fabric και είναι έτοιμο να υλοποιηθεί ένα μικρό Blockchain.

Στην εφαρμογή θα δημιουργηθεί ένα σενάριο χρήσης με χρήστες που θα μπαίνουν στο δίκτυο και ο ένας θα εκτελεί μια συναλλαγή (π.χ αποστολή συντεταγμένων).Οπότε το σενάριο υλοποίησης θα βασιστεί στην εφαρμογή Blockchain και κρυπτογράφηση συντεταγμένων για αρχή.

6.1 Υλοποίηση και Αρχιτεκτονική HYPERLEDGER FABRIC

Για τη δημιουργία του project χρησιμοποιήθηκαν οι εξής τεχνολογίες:

- Ubuntu 16.04
- Curl (sudo apt install curl)
- Git(sudo apt install git)
- Docker(sudo apt install docker.io)
- Docker Compose(sudo apt install docker-compose)
- Python 2.7(sudo apt install python)
- Nodejs(sudo apt install nodejs)
- NPM(sudo apt install npm)

Τα εξής πακέτα από το npm :

- npm install
- npm install
- npm install
- npm install

```
1  -g composer-cli
2  -g composer-rest-server
3  -g composer-playground
4  -g yo generator-hyperledger-composer
5
```

Εικόνα 1-πακέτα από το npm

6.2 Ανάλυση

Για την εγκατάσταση του Hyperledger Fabric εκτελέστηκε το παρακάτω:

```
1 mkdir ~/fabric-dev-servers
2 cd ~/fabric-dev-servers
3 curl -O https://raw.githubusercontent.com/hyperledger/composer-tools/master/packages/fabricdev-
4 servers/fabric-dev-servers.tar.gz
5 tar -xvf fabric-dev-servers.tar.gz
6 export FABRIC_VERSION=hlfv12
7 ./downloadFabric.sh
8 ./startFabric.sh
9 ./createPeerAdminCard.sh
10
```

Εικόνα 2- εντολές για την εγκατάσταση του Hyperledger Fabric

Και έτσι δημιουργήθηκε ένα τοπικό δίκτυο του Hyperledger Fabric.

Στη συνέχεια για τη δημιουργία του project υλοποιήθηκε ένα business network.

```
1 yo hyperledger-composer
```

Εικόνα 3- υλοποίηση business network

Έπειτα έγινε η μοντελοποίηση του project όπου υλοποιήθηκαν/τροποποιήθηκαν τα παρακάτω:

- Assets
- Participants
- Transactions

- Events

Προστέθηκε η λογική με javascript στο αρχείο logic.js και τροποποιήθηκαν τα permissions κατάλληλα για τις ανάγκες του project. Τέλος υλοποιήθηκαν δυο python script setup.py και run.py για την αυτόματη εκκίνηση του network και την εγγραφή του project στο δίκτυο.

6.3 Σενάριο Χρήσης

Location-trading-network

Προκειμένου να ξεκινήσει το project ακολουθήθηκαν τα παρακάτω βήματα:

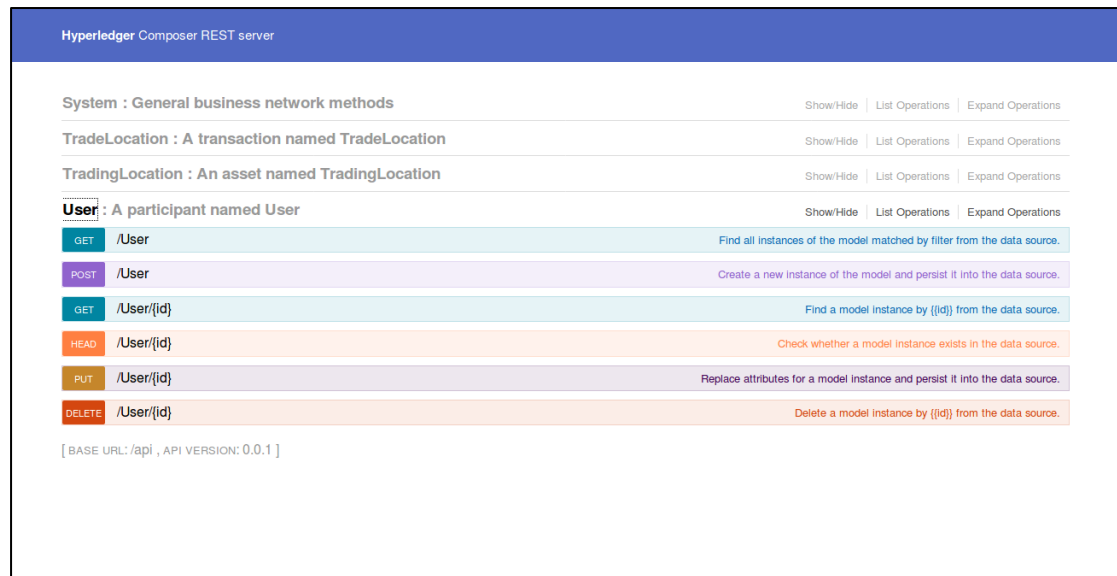
- Άνοιγμα του vm (virtual machine)
- Άνοιγμα του terminal και πάτημα cd mail-trading-network
- python setup.py && python run.py
- Ανοίγει ο browser στο playground.

Στην αρχική σελίδα ο χρήστης θα πατήσει το κουτάκι admin@ location -trading-network

connect now

Αυτό είναι το menu του blockchain. Στη συνέχεια θα πατήσει το κουμπί Test.

Πτυχιακή Εργασία: BLOCKCHAIN AND ITS APPLICATION IN GEOSPATIAL DATA



Εικόνα 4-δημιουργία χρήστη

και μεταφέρεται στο τομέα των χρηστών για να δημιουργήσουμε ένα χρήστη(User).

Στη συνέχεια θα πατήσει create new participant

Εδώ θα γίνει η εισαγωγή του χρήστη σε μορφή json

Για παράδειγμα

```
1 {  
2   "$class" : "org.example.biznet.User",  
3   "userId" : "1",  
4   "userName" : "John"  
5 }  
6
```

Εικόνα 5-παράδειγμα εισαγωγής χρήστη

Πτυχιακή Εργασία: BLOCKCHAIN AND ITS APPLICATION IN GEOSPATIAL DATA

Hyperledger Composer REST server

POST /User Create a new instance of the model and persist it into the data source.

Response Class (Status 200)
Request was successful

Model Example Value

```
{
  "class": "org.example.biznet.User",
  "userId": "string",
  "username": "string"
}
```

Response Content Type: application/json

Parameters

Parameter	Value	Description	Parameter Type	Data Type
data	<pre>{ "class": "org.example.biznet.User", "userId": "1", "username": "John" }</pre>	Model instance data	body	Model Example Value

Parameter content type: application/json

Try it out!

Εικόνα 6-εισαγωγή χρήστη

Hyperledger Composer REST server

TradingLocation : An asset named TradingLocation Show/Hide | List Operations | Expand Operations

User : A participant named User Show/Hide | List Operations | Expand Operations

GET /User Find all instances of the model matched by filter from the data source.

POST /User Create a new instance of the model and persist it into the data source.

GET /User/{id} Find a model instance by {id} from the data source.

Response Class (Status 200)
Request was successful

Model Example Value

```
{
  "class": "org.example.biznet.User",
  "userId": "string",
  "username": "string"
}
```

Response Content Type: application/json

Parameters

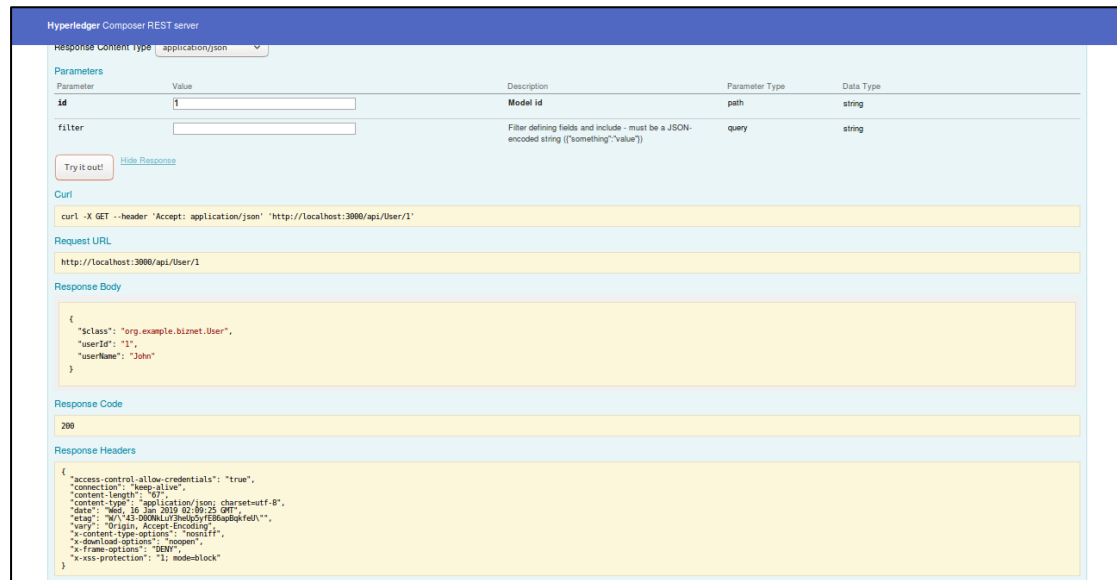
Parameter	Value	Description	Parameter Type	Data Type
id	1	Model id	path	string
filter		Filter defining fields and include - must be a JSON-encoded string ({'something':'value'})	query	string

Try it out!

Εικόνα 7-εισαγωγή δεδομένων

Πτυχιακή Εργασία: BLOCKCHAIN AND ITS APPLICATION IN GEOSPATIAL DATA

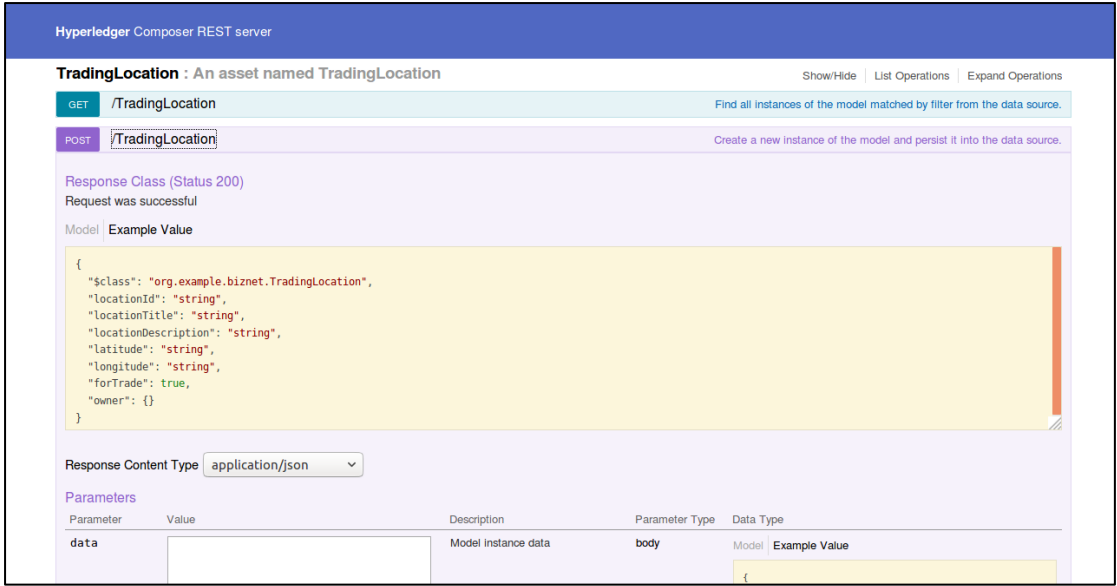
Έπειτα, θα πατήσει στο TradingMail στα δεξιά και create new asset και γίνεται η εισαγωγή των δεδομένων όπως φαίνεται στο screenshot και έτσι δημιουργήθηκε ένα location.



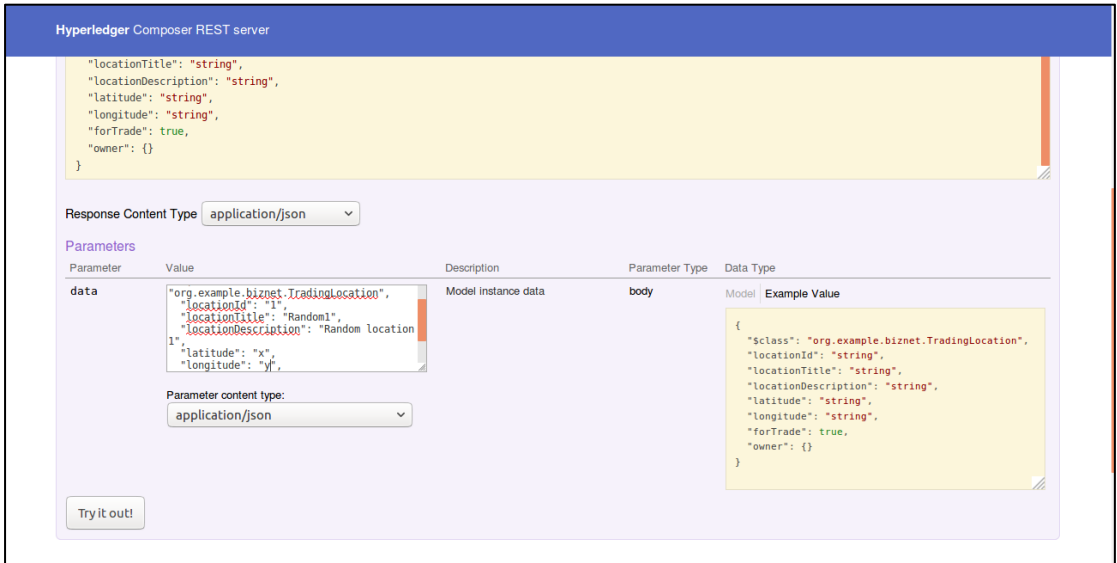
Εικόνα 8-δημιουργία location

Στα υπόλοιπα screenshot φαίνονται οι λειτουργίες του blockchain.

Πτυχιακή Εργασία: BLOCKCHAIN AND ITS APPLICATION IN GEOSPATIAL DATA



Εικόνα 9-λειτουργίες blockchain



Εικόνα 10-λειτουργίες blockchain

Hyperledger Composer REST server

Response Content Type

application/json

Parameters

Parameter	Value	Description	Parameter Type
data	<pre>{ "\$class": "org.example.biznet.TradingLocation", "locationId": "1", "locationTitle": "Random1", "locationDescription": "Random1", "latitude": "x", "longitude": "y", "forTrade": true, "owner": "resource:org.example.biznet.User#1" }</pre>	Model instance data	body

Parameter content type:

application/json

Try it out!

[Hide Response](#)

Curl

Εικόνα 11-λειτουργίες blockchain

Hyperledger Composer REST server

Response Content Type application/json

Parameters

Parameter	Value	Description	Parameter Type
data	<pre>{ "\$class": "org.example.biznet.TradingLocation", "locationId": "2", "locationTitle": "Random2", "locationDescription": "Random2", "latitude": "xx", "longitude": "yy", "forTrade": true, "owner": "resource:org.example.biznet.User#1" }</pre>	Model instance data	body

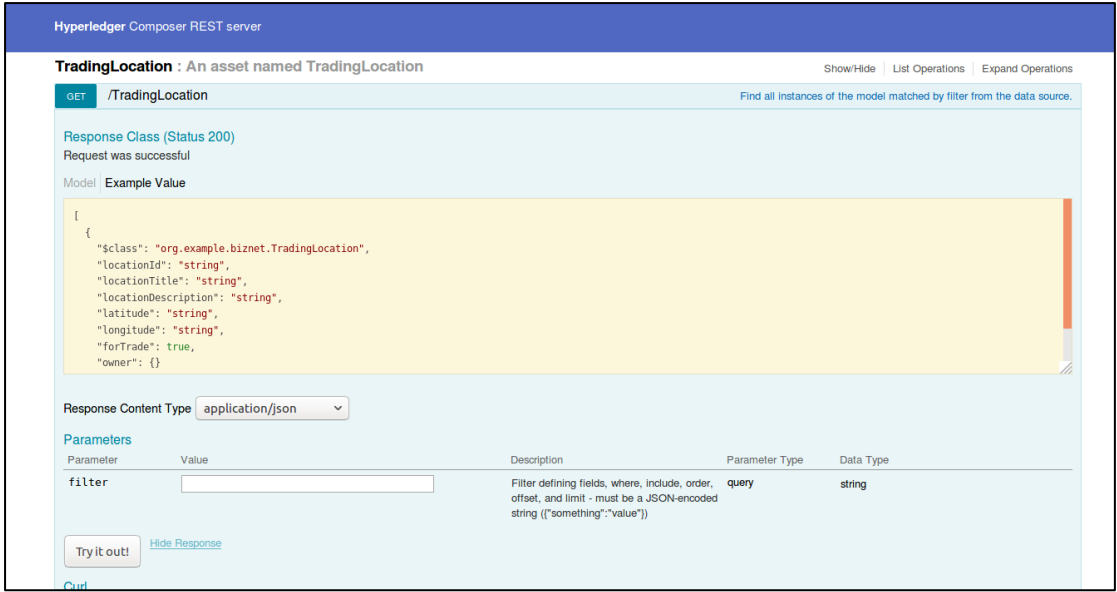
Parameter content type: application/json

Try it out! [Hide Response](#)

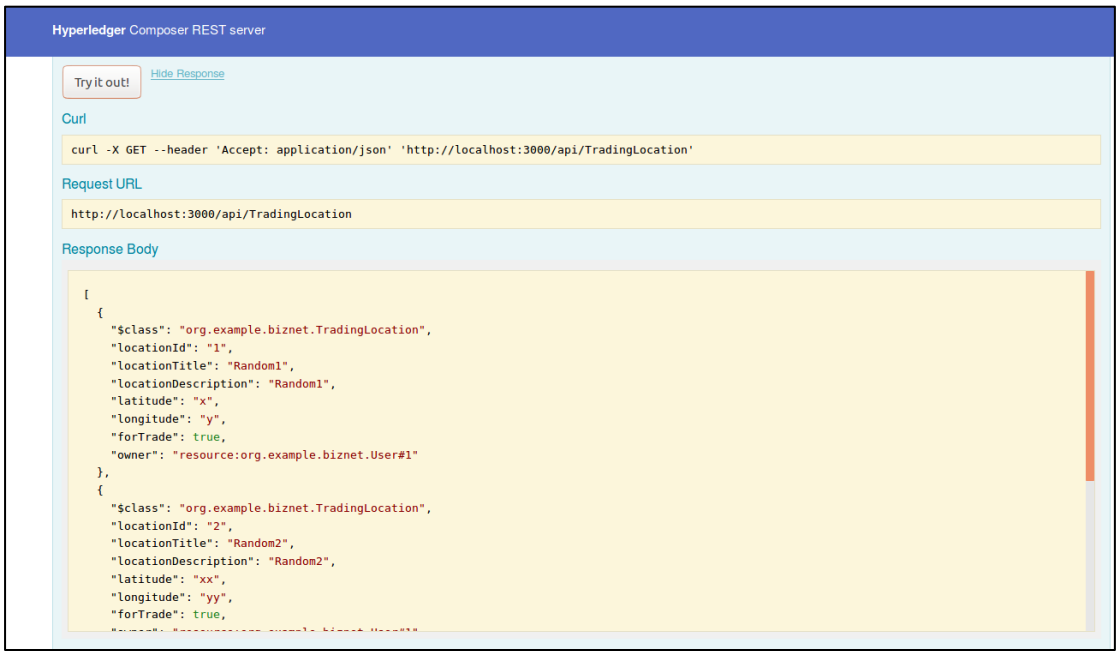
Curl

Εικόνα 12-λειτουργίες blockchain

Πτυχιακή Εργασία: BLOCKCHAIN AND ITS APPLICATION IN GEOSPATIAL DATA



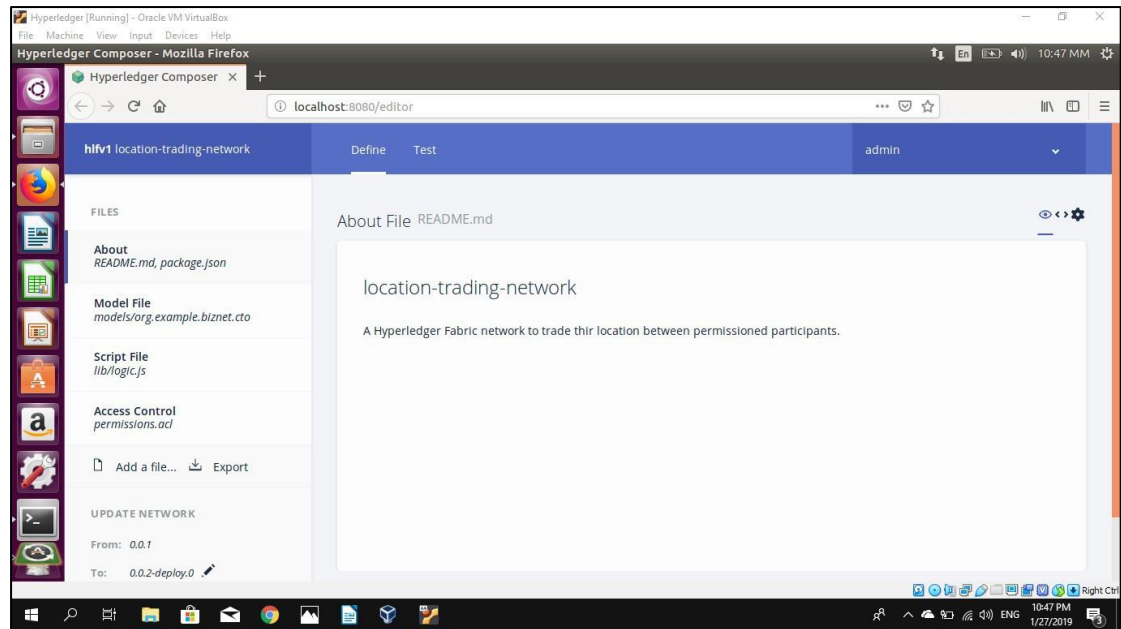
Εικόνα 13-λειτουργίες blockchain



Εικόνα 14-λειτουργίες blockchain

6.3 Σενάριο Χρήσης 2

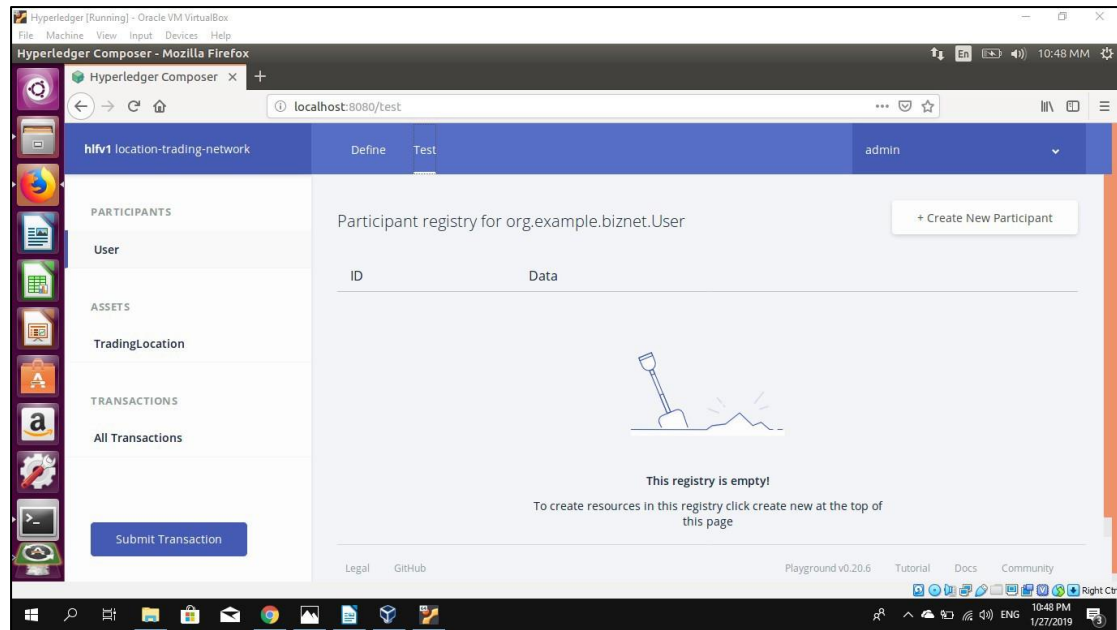
Στο μενού της εφαρμογής ο χρήστης θα πατήσει το κουμπί Test.



Εικόνα 15-Δημιουργία Test

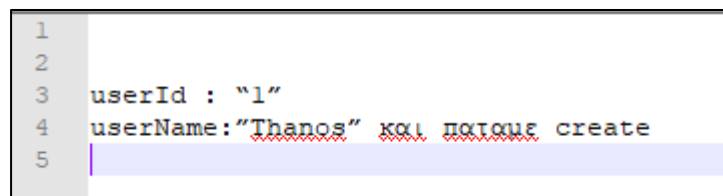
Στο μενού των χρηστών θα πατήσει create new participant για να δημιουργηθεί ένας καινούργιος.

Πτυχιακή Εργασία: BLOCKCHAIN AND ITS APPLICATION IN GEOSPATIAL DATA



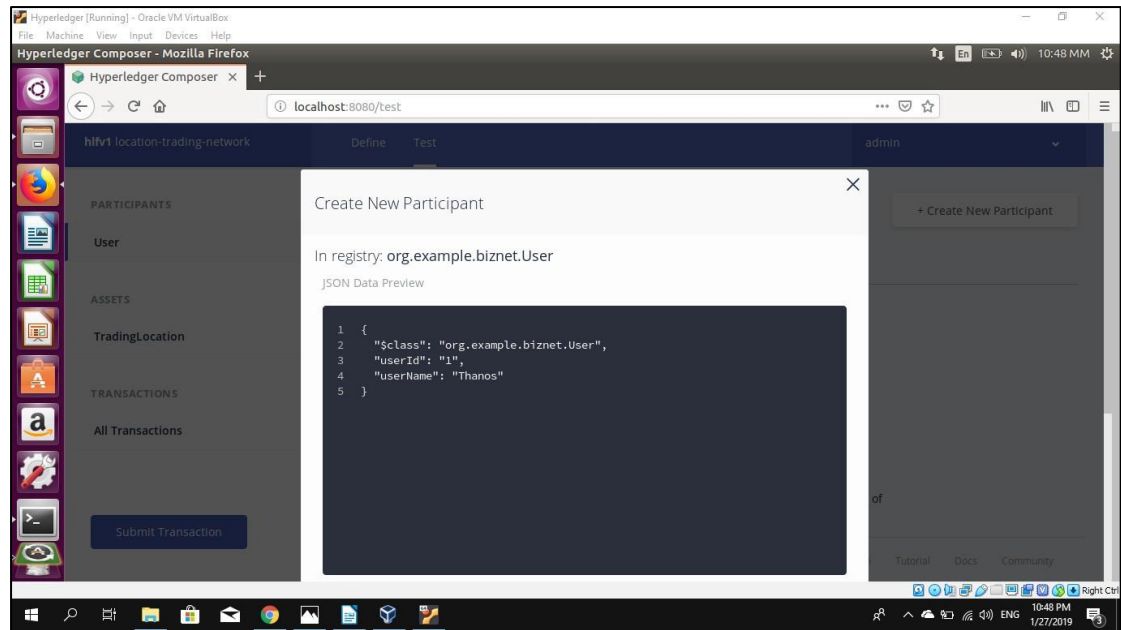
Εικόνα 16-Δημιουργία new participant

Θα γίνει εισαγωγή των στοιχείων όπως φαίνεται στην εικόνα

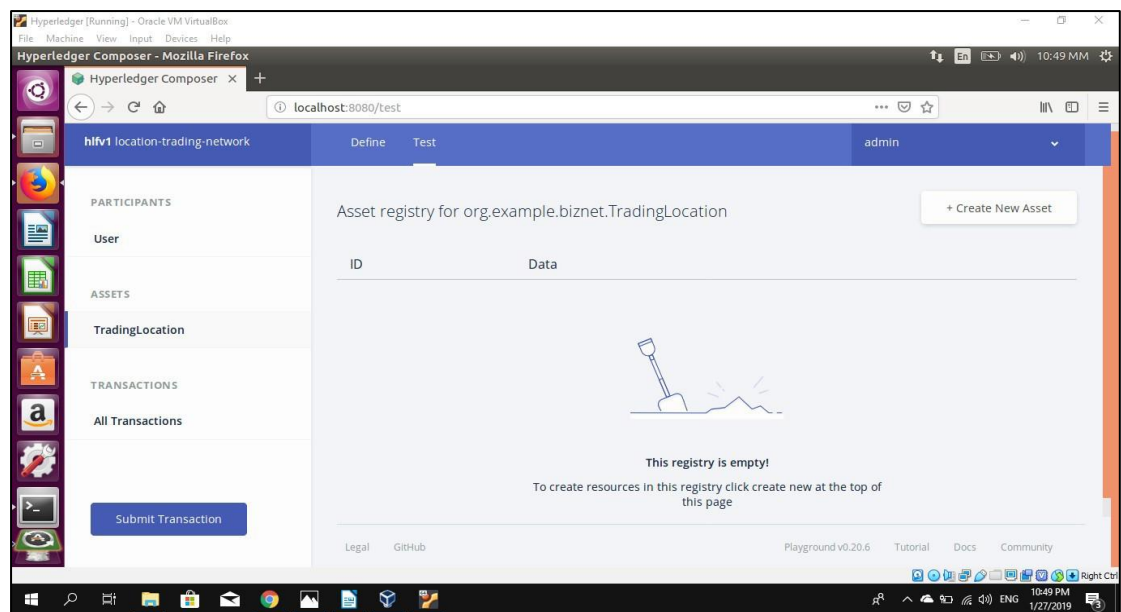


Εικόνα 17-εισαγωγή στοιχείων

Πτυχιακή Εργασία: BLOCKCHAIN AND ITS APPLICATION IN GEOSPATIAL DATA



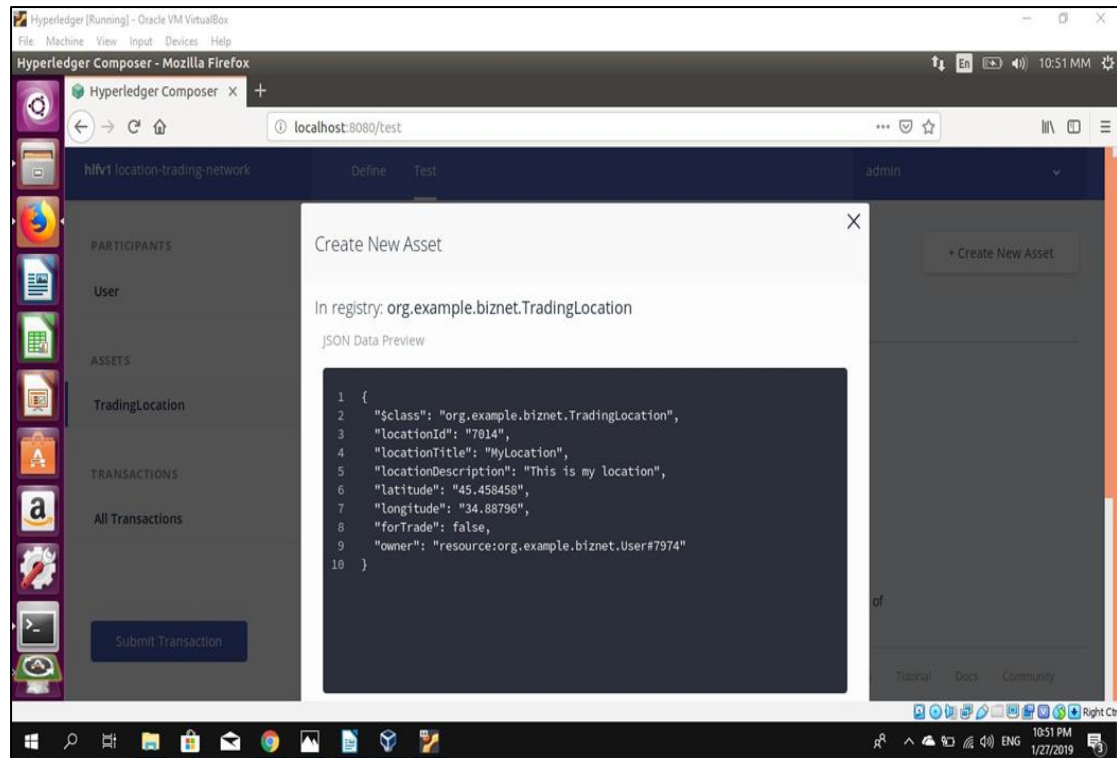
Εικόνα 18-Δημιουργία χρήστη



Εικόνα 19- Δημιουργία χρήστη 2

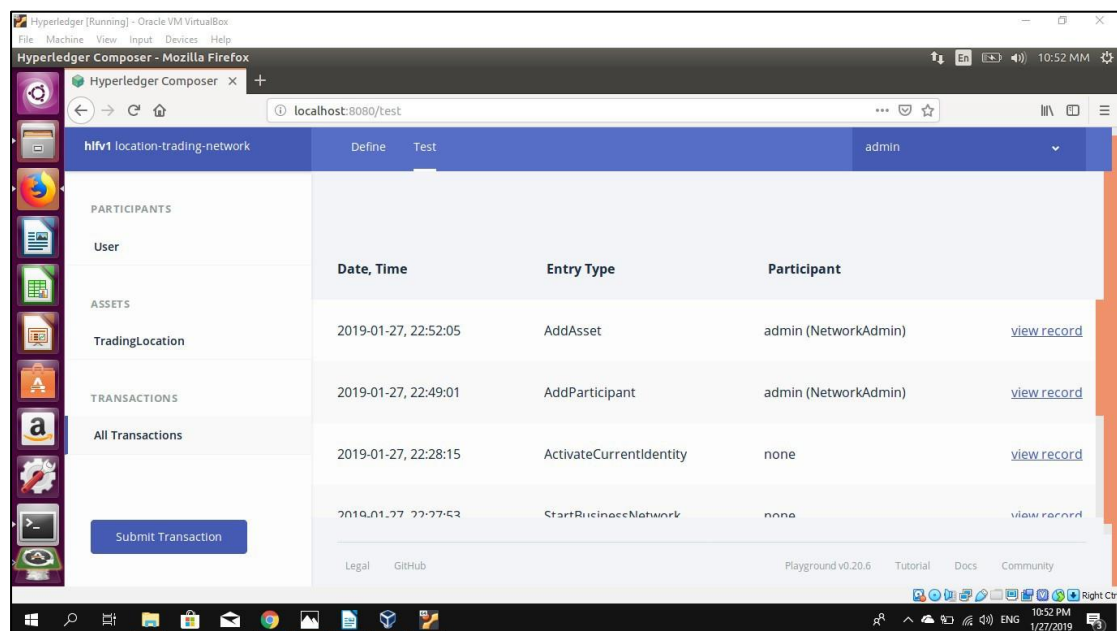
Θα πατήσει στο trading location στη δεξιά μπάρα και στη συνέχεια θα πατήσει create new asset για να δημιουργηθεί ένα location όπως φαίνεται στην εικόνα.

Πτυχιακή Εργασία: BLOCKCHAIN AND ITS APPLICATION IN GEOSPATIAL DATA



Εικόνα 20-Δημιουργία new asset

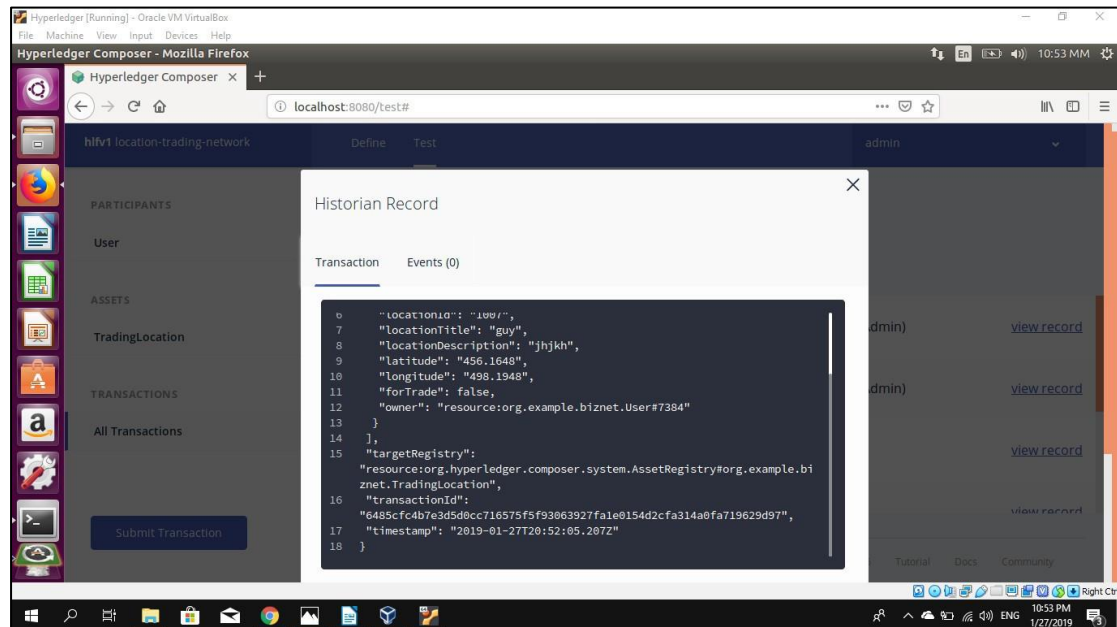
Θα πατήσει All transactions στη δεξιά μπάρα και έτσι θα μπορεί να δει όλα τα records του app.



Εικόνα 21-προβολή Transaction

Πτυχιακή Εργασία: BLOCKCHAIN AND ITS APPLICATION IN GEOSPATIAL DATA

Και τέλος θα πατήσει στο view record σε οποιοδήποτε στοιχείο υπάρχει στη λίστα και θα εμφανίζει όλες τις πληροφορίες και ειδικά το hash δηλαδή το transactionid όπως φαίνεται στην εικόνα.



Εικόνα 22-πληροφορίες Hash

Έτσι υλοποιήθηκε ένα blockchain για ανταλλαγή συντεταγμένων που μπορούν να δουν μόνο οι χρηστές με πρόσβαση στο δίκτυο.

Κεφάλαιο 7

7.1 Συμπεράσματα και μελλοντική έρευνα

Το blockchain είναι μια πολλά υποσχόμενη τεχνολογία που μπορεί να εφαρμοστεί σε ένα πλήθος επιπλέον περιοχών της ανθρώπινης δραστηριότητας όπως η Παιδεία, η Υγεία, η διαφύλαξη και διαφάνεια αρχείων, η πιστοποίηση προϊόντων και υπηρεσιών και τα κοινωνικά δίκτυα. Κάποια από τα πλεονεκτήματα αυτής της τεχνολογίας είναι οι άμεσες συναλλαγές, η ακεραιότητα της διαδικασίας, η αντοχή και αξιοπιστία, η διαφάνεια και αμεταβλητότητα, η απλοποίηση του συστήματος και οι ταχύτερες συναλλαγές. Επίσης οι διαφορετικές αρχιτεκτονικές των πλατφορμών δείχνουν ότι δεν υπάρχει ακόμα ένα κύριο μοντέλο σχεδίασης του blockchain. Εν τούτοις έχει διχάσει σε μεγάλο βαθμό την παγκόσμια κοινότητα και αυτό γιατί παρά τις καινοτόμες λύσεις που προσφέρει πρέπει να ληφθεί υπόψη η απουσία νομικής κατοχύρωσης στα δικαιώματα των χρηστών που αφορούν τα προσωπικά τους δεδομένα.

Λόγω του πρώιμου σταδίου της τεχνολογίας blockchain, οι εφαρμογές της είναι περιορισμένες. Μελλοντικά το blockchain θα μπορούσε να χρησιμοποιηθεί στις επιχειρήσεις και στις κυβερνήσεις για να αυξηθεί η διαφάνεια και να μειωθεί η διαφθορά και η γραφειοκρατία. Τέλος, το blockchain θα μπορούσε να βελτιώσει την ιατρική πρόσβαση και αποτελεσματικότητα.

Βιβλιογραφικές Παραπομπές

[1]English Oxford Living Dictionaries. Definition of blockchain in English.Ανακτήθηκε από

https://en.oxforddictionaries.com/definition/blockchain?fbclid=IwAR0bohSV-vigzAqP0GE_ObXikLpErfyB11Gdzd1HuEoMI6eYOkYd8LbyRC0

στις 15-10-2018

[2] techopedia. Definition - What does Peer-To-Peer Network (P2P Network) mean?Ανακτήθηκε από <https://www.techopedia.com/definition/25777/peer-to-peer-network-p2p-network> στις 15-10-2018

[3]Lisk.Blockchain Use Cases.Ανακτήθηκε από <https://lisk.io/academy/blockchain-basics/use-cases> στις 15-10-2018

[4] Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction.

[5] The Economist .Blockchains: The great chain of being sure about things. Ανακτήθηκε από <https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things> στις 16-10-2018

[6] Economis Project Bletchley Whitepaper Archived 11 January 2017 at the Wayback Machine .Ανακτήθηκε από

<https://web.archive.org/web/20170111135615/https://github.com/Azure/azure-blockchain-projects/blob/master/bletchley/bletchley-whitepaper.md> στις 16-10-2018

[7] Raconteur. The future of blockchain in 8 charts. Ανακτήθηκε από <https://www.raconteur.net/business-innovation/the-future-of-blockchain-in-8-charts> στις 16-10-2018

[8] Hype Killer - Only 1% of Companies Are Using Blockchain, Gartner Reports | Artificial Lawyer. Ανακτήθηκε από <https://www.artificiallawyer.com/2018/05/04/hype-killer-only-1-of-companies-are-using-blockchain-gartner-reports/> στις 17-10-2018

[9] Antonopoulos, Andreas . Bitcoin security model: trust by computation. Radar. O'Reilly. Ανακτήθηκε από <https://www.cryptocompare.com/coins/guides/why-is-ethereum-different-to-bitcoin/> στις 18-10-2018

[10] Antonio Madeira . Why is Ethereum different to Bitcoin?. CryptoCompare. Ανακτήθηκε από <https://www.cryptocompare.com/coins/guides/why-is-ethereum-different-to-bitcoin/> στις 18-10-2018

[11] Brito, Jerry; Castillo, Andrea (2013). Bitcoin: A Primer for Policymakers (PDF) (Report). Fairfax, VA: Mercatus Center, George Mason University. Archived (PDF) .Ανακτήθηκε από https://www.mercatus.org/system/files/Brito_BitcoinPrimer.pdf στις 19-10 -2018

[12] Raval, Siraj (2016). What Is a Decentralized Application". Decentralized Applications: Harnessing Bitcoin's Blockchain Technology. O'Reilly Media, Inc. pp. 1–2. ISBN 978-1-4919-2452-5. OCLC 968277125. Retrieved 6 November 2016 – via Google Books.Ανακτήθηκε από

https://books.google.gr/books?id=fvywDAAAQBAJ&pg=PA1&redir_esc=y#v=onepage&q&f=false στις 19-10-2018

[13] Hampton, Nikolai . Understanding the blockchain hype: Why much of it is nothing more than snake oil and spin. Computerworld. Ανακτήθηκε από <https://www.computerworld.com.au/article/606253/understanding-blockchain-hype-why-much-it-nothing-more-than-snake-oil-spin/> στις 20-10-2018

[14] beBee producer.Top advantages and disadvantages of blockchain technology.Ανακτήθηκε από <https://www.bebec.com/producer/@javierbebee/top-advantages-and-disadvantages-of-blockchain-technology> στις 20-10-2018

[15] Blockchains & Distributed Ledger Technologies. BlockchainHub. Ανακτήθηκε από <https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/> στις 21-10-2018

[16] Salsman, R.M. (19 September 2013). The Financial Crisis Was A Failure Of Government, Not Free Markets. Forbes.Ανακτήθηκε από <https://www.forbes.com/sites/richardsalsman/2013/09/19/the-financial-crisis-was-a-failure-of-government-not-free-markets/> στις 21-10-2018

[17] Ovenden, James. Blockchain Top Trends In 2017. The Innovation Enterprise. Ανακτήθηκε από <https://channels.theinnovationenterprise.com/articles/blockchain-top-trends-in-2017> στις 22-10-2018

[18] Wagner, Kurt . Facebook is making its biggest executive shuffle in company history. Ανακτήθηκε από <https://www.recode.net/2018/5/8/17330226/facebook-reorg-mark-zuckerberg-whatsapp-messenger-ceo-blockchain> στις 22-10-2018

[19] Virtual Currencies and Beyond: Initial Considerations (PDF). Ανακτήθηκε από

<https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf> στις 23-10-2018

[20] Kelly, Jemima. Top banks and R3 build blockchain-based payments

system. Ανακτήθηκε από <https://www.reuters.com/article/us-banks-blockchain-r3/top-banks-and-r3-build-blockchain-based-payments-system-idUSKBN1D00ZB> στις 23-

10-2018

[21] Lisk. How-Does-Blockchain-Work/What-Is-Hashing .Ανακτήθηκε από

<https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/what-is-hashing> στις

23-10-2018

[22] Geospatial world. The Game Changer of Geospatial Systems — Blockchain.

Ανακτήθηκε από <https://www.geospatialworld.net/article/blockchain-geospatial-systems/> στις 8-11-2018

[23] BlockchainHub. Blockchains & Distributed Ledger Technologies. Ανακτήθηκε

από <https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/> στις 11-11-2018

[24] Blockgeeks . What is Hyperledger? A Brief Hyperledger Tutorial. Ανακτήθηκε

από <https://blockgeeks.com/guides/hyperledger/> στις 28-11-2018