ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ Μ/Υ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΝΑΥΤΙΛΙΑΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΑΣ
ΤΜΗΜΑΤΟΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ & ΤΕΧΝΟΛΟΓΙΑΣ
ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επισκόπηση δυνατοτήτων της τεχνολογίας blockchain και εφαρμογές state-of-the-art στην υγεία και άλλους τεχνολογικούς κλάδους.

Βασίλειος Χ. Χαντζιάρας

Ηλεκτρολόγος Μηχανικός και Μηχανικός Ηλεκτρονικών Υπολογιστών ΕΜΠ

Επιβλέπων Καθηγητής:

Δ. Ασκούνης

Αν. Καθηγητής

Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Ηλεκτρονικών Υπολογιστών ΕΜΠ

Αθήνα, Ιούνιος 2019

Επισκόπηση δυνατοτήτων της τεχνολογίας blockchain και εφαρμογές state-of-the-art στην υγεία και άλλους τεχνολογικούς κλάδους.

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επισκόπηση δυνατοτήτων της τεχνολογίας blockchain και εφαρμογές state-of-the-art στην υγεία και άλλους τεχνολογικούς κλάδους.

Βασίλειος Χ. Χαντζιάρας

Ηλεκτρολόγος Μηχανικός και Μηχανικός Ηλεκτρονικών Υπολογιστών ΕΜΠ

Επιβλέπων Καθηγητής: Δ. Ασκούνης, Αν. Καθηγητής
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Ηλεκτρονικών Υπολογιστών ΕΜΠ

……

Βασίλειος Χ. Χαντζιάρας

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών ΕΜΠ

Email: vassileios.chantziaras@gmail.com

Copyright © Βασίλειος Χ. Χαντζιάρας, 2019

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας διπλωματικής εργασίας, εξ' ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή με σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς το συγγραφέα.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν το συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού Μετσόβιου Πολυτεχνείου ή του Πανεπιστημίου Πειραιώς.

Ευχαριστίες

Το αντικείμενο του Ηλεκτρολόγου Μηχανικού και Μηχανικού Ηλεκτρονικών Υπολογιστών είναι ένα πολύπλευρο και εξαιρετικά ενδιαφέρον αντικείμενο. Η δια βίου εκπαίδευση στον κλάδο των μηχανικών, καθώς και η επέκταση των γνωστικών τους πεδίων είναι μια καθημερινή ανάγκη για όσους απασχολούνται σε αντικείμενα σχετικά με τον κλάδο της Πληροφορικής και της Τεχνολογίας. Η συμμετοχή μου στο Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών «Τεχνοοικονομικά Συστήματα» μου προσέφερε αρκετές γνώσεις και δεξιότητες, ενώ ταυτόχρονα διεύρυνε το αντικείμενο των βασικών σπουδών μου στο ΕΜΠ. Κατά τη διάρκεια του προγράμματος κέρδισα εμπειρίες σημαντικές για την επαγγελματική μου σταδιοδρομία.

Η παρούσα διπλωματική εργασία αποτελεί για εμένα έμπνευση για τη συνέχεια της καριέρας μου στον διαρκώς εξελισσόμενο κλάδο της Πληροφορικής και των Τηλεπικοινωνιών, καθώς και τη διεύρυνση του γνωστικού πεδίου μου σε νέες τεχνολογίες αποθήκευσης, διαμοιρασμού και κρυπτογράφησης δεδομένων.

Στο σημείο αυτό θα ήθελα να ευχαριστήσω, αρχικά, τον επιβλέποντα καθηγητή της εργασίας, κο. Δ. Ασκούνη, ο οποίος μου έδωσε την ευκαιρία να ασχοληθώ με ένα τόσο ενδιαφέρον και καινοτόμο αντικείμενο όπως είναι το blockchain και οι εφαρμογές του στους διάφορους κλάδους. Παράλληλα, θα ήθελα να ευχαριστήσω τον κο. Σ. Μουζακίτη για την άψογη συνεργασία και τη διαρκή και ιδιαίτερα σημαντική βοήθεια του στην εκπόνηση της εργασίας μου. Τέλος, θα ήθελα να ευχαριστήσω όλους εκείνους που έβαλαν έστω και ένα μικρό λιθαράκι στην περάτωση αυτής της διπλωματικής και ιδιαίτερα την οικογένεια μου για την υπομονή και τη συμπαράσταση τους καθ’ όλη τη διάρκεια των μεταπτυχιακών σπουδών μου.

Επισκόπηση δυνατοτήτων της τεχνολογίας blockchain και εφαρμογές state-of-the-art στην υγεία και άλλους τεχνολογικούς κλάδους.

Περίληψη

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια του ΔΠΜΣ «Τεχνοοικονομικά Συστήματα» και έχει ως σκοπό την γενικότερη παρουσίαση της τεχνολογίας του blockchain και της διείσδυσης της στους διάφορους κλάδους ως μεθόδου αποθήκευσης, κρυπτογράφησης και διαμοιρασμού δεδομένων. Αρχικά γίνεται μία παρουσίαση της λογικής λειτουργίας του blockchain και των τεχνικών όρων που χρησιμοποιούνται στην τεχνολογία αυτή, σε συνδυασμό με τρόπους ανάπτυξης του και πλατφόρμες που έχουν ήδη αναπτυχθεί βασισμένες σε αυτή την τεχνολογία. Έπειτα, στόχος της παρούσας εργασίας είναι να αποτυπωθούν οι παγκόσμιες τάσεις της τεχνολογίας του blockchain και η μέχρι τώρα χρήση του σε κλάδους άμεσα ή έμμεσα συνδεδεμένους με την πληροφορική, μέσα από την περιγραφή των χρήσεων της τεχνολογίας στις λειτουργίες τους και την παρουσίαση των πιο διαδεδομένων εμπορικών εφαρμογών σε κάθε κλάδο. Στη συνέχεια το αντικείμενο της παρούσας εργασίας εστιάζει σε μεγαλύτερο βαθμό στη χρήση της τεχνολογίας στον τομέα της Υγείας, μέσα από την παρουσίαση λειτουργιών και διαδικασιών του κλάδου που θα μπορούσαν να χρησιμοποιήσουν την τεχνολογία του blockchain, την παρουσίαση των διαδεδομένων εφαρμογών που έχουν βασιστεί στην τεχνολογία αυτή και στην ανασκόπηση των εμποδίων και των προοπτικών του blockchain στον κλάδο μελλοντικά. Τέλος, γίνεται μια γενικότερη ανασκόπηση των συμπερασμάτων της παρούσας εργασίας και παρουσιάζονται οι προοπτικές επέκτασης της.

Λέξεις Κλειδιά

Blockchain, κρυπτογράφηση, αποθήκευση δεδομένων, υγεία, δεδομένα ασθενών, ιατρικός φάκελος, διαμοιρασμός δεδομένων, ηλεκτρονικές συναλλαγές

Επισκόπηση δυνατοτήτων της τεχνολογίας blockchain και εφαρμογές state-of-the-art στην υγεία και άλλους τεχνολογικούς κλάδους.

Abstract

This dissertation has been prepared under the postgraduate MSc Program "Technoeconomic Systems" of "School of Electrical and Computer Engineering" and "University of Piraeus". The purpose of this thesis is, initially, the presentation of the blockchain technology and its penetration in various sectors as a method of storage, encryption and data sharing. To start with, there is a presentation of the logical functions of the blockchain along with the technical terms that are used to describe these functions and the platforms that have been developed based on this technology. Thereinafter, it aims to capture the global trends in blockchain technology and its use so far in several sectors that are more or less connected with the Information Technology sector, through the description of the uses of blockchain in functions and processes of these sectors and the presentation of the most widespread commercial applications in each sector. Furthermore, the purpose of this thesis is to focus on the use of blockchain in Healthcare through the presentation of functions and processes in Health Industry that could use the blockchain technology to create widespread applications and barriers and prospects of this technology in the future. Finally, a general overview of the conclusions and the prospects of expansion of this dissertation are presented in the last chapter.

Keywords

Blockchain, data encryption, data storage, healthcare, patients' data, health records, data sharing, e-transactions

Επισκόπηση δυνατοτήτων της τεχνολογίας blockchain και εφαρμογές state-of-the-art στην υγεία και άλλους τεχνολογικούς κλάδους.

Πίνακας Περιεχομένων

1 Εισαγωγή ... 15

1.1 Αντικείμενο και στόχοι της διπλωματικής εργασίας ... 15

1.2 Δομή της διπλωματικής εργασίας ... 15

2 Ανάλυση Τεχνολογικού Περιβάλλοντος ... 17

2.1 Τι είναι το blockchain ... 17

2.1.1 Οι συναρτήσεις hash (Hash Functions) ... 17

2.1.2 Το hashchain – Η Εσωτερική Αλυσίδα ... 18

2.1.3 Κρυπτογράφηση Δημόσιου Κλειδιού (Public Key Cryptography – PKC) ... 18

2.1.4 Η ασφάλεια των hashchains με τη χρήση Κρυπτογράφησης Δημόσιου Κλειδιού (PKC) ... 19

2.1.5 Το blockchain – Εξωτερική Αλυσίδα ... 20

2.1.6 Δημόσια και Ιδιωτικά blockchains ... 21

2.2 Πλατφόρμες ανάπτυξης εφαρμογών blockchain ... 22

2.2.1 Ethereum ... 24

2.2.2 Hyperledger ... 25

2.2.3 IBM Blockchain ... 26

2.2.4 Multichain ... 27

2.2.5 Hydrachain ... 28

2.2.6 BigchainDB ... 28

2.2.7 Openchain ... 30

2.2.8 Quorum ... 31

2.2.9 IOTA ... 32

3 Τομείς εφαρμογής και διαδεδομένες εφαρμογές ... 35

3.1 Τάσεις της τεχνολογίας στην παγκόσμια αγορά ... 35

3.2 Τομείς εφαρμογής της τεχνολογίας blockchain ... 38

3.2.1 Τραπεζικές συναλλαγές ... 38

3.2.2 Υγεία ... 39

3.2.3 Πολιτική και διακυβέρνηση ... 40

3.2.4 Αγορά ακινήτων ... 41

3.2.5 Νομικές υπηρεσίες ... 42

3.2.6 Ενοικιάσεις και διαμοιρασμός διαδρομών ... 43

3.2.7 Εκπαίδευση ... 44

3.2.8 Φιλανθρωπικοί οργανισμοί ... 45

3.2.9 Ασφάλεια ... 46
3.2.10 Αποθήκευση και υπολογιστική ισχύς στο Cloud ... 47

3.3 Διαδεδομένες εφαρμογές ... 48

3.3.1 Ripple [Τραπεζικές Συναλλαγές] ... 48
3.3.2 Smart Dubai Blockchain [Πολιτική και Διακυβέρνηση] ... 49
3.3.3 Ubitquity [Αγορά Ακινήτων] ... 50
3.3.4 OpenLaw [Νομικές Υπηρεσίες] ... 51
3.3.5 Yantha [Διαμοιρασμός Διαδρομών] ... 52
3.3.6 HireGo [Ενοικίαση Οχημάτων] ... 53
3.3.7 Blockcerts [Εκπαίδευση] ... 53
3.3.8 Insurwave [Ασφάλεια Θαλάσσιων Μεταφορών] ... 55
3.3.9 Alice [Διαχείριση Δωρεών – Φιλανθρωπικοί Οργανισμοί] ... 56
3.3.10 Storj [Αποθηκευτικός Χώρος] ... 57
3.3.11 Golem [Υπολογιστική Ισχύς] ... 58

4 Εφαρμογή του blockchain στο χώρο της Υγείας ... 61

4.1 Εφαρμογές στον τομέα της υγείας ... 61

4.1.1 Ιατρικός φάκελος ασθενών & Κοινή χρήση δεδομένων υγείας ... 61
4.1.2 Παρακολούθηση ιατρικού εξοπλισμού ... 62
4.1.3 Παραγωγή και παρακολούθηση φαρμάκων ... 63
4.1.4 Κλινικές μελέτες ... 64

4.2 Εφαρμογές και τεχνολογίες ανάπτυξης ... 64

4.2.1 MedRec – MIT Labs ... 64
4.2.2 Medicalchain ... 67
4.2.3 Gem ... 68
4.2.4 Nebula Genomics ... 70
4.2.5 Patientory ... 71

4.3 Εμπόδια και προκλήσεις ... 72

5 Συμπεράσματα – Προοπτικές ... 76

5.1 Γενικότερη αξιολόγηση εργαλείων και εφαρμογών blockchain ... 76

5.2 Αξιολόγηση εργαλείων και εφαρμογών blockchain στο χώρο της υγείας ... 77

5.3 Προοπτικές ... 78

6 Βιβλιογραφία ... 80

Επισκόπηση δυνατοτήτων της τεχνολογίας blockchain και εφαρμογές state-of-the-art στην υγεία και άλλους τεχνολογικούς κλάδους.

1 Εισαγωγή

1.1 Αντικείμενο και στόχοι της διπλωματικής εργασίας

Το blockchain και οι τεχνικές αποθήκευσης, διαμοιρασμού και κρυπτογράφησης δεδομένων έχουν γίνει ιδιαίτερα δημοφιλείς έννοιες τα τελευταία χρόνια. Αυτό συνέβη αφ' ενός γιατί αρκετές start ups σε όλο τον κόσμο, έχοντας ως βάση το Bitcoin και τις αρχές του δικτύου συναλλαγών που αυτό παρουσίασε το 2008, δημιούργησαν εφαρμογές και κρυπτονομίσματα τα οποία θα μπορούσαν να λύσουν καθημερινά προβλήματα σε πολλούς τομείς των επιχειρήσεων και των δημόσιων φορέων Τα κρυπτονομίσματα, αφ' ετέρου, έχουν αποκτήσει τα τελευταία χρόνια αρκετά μεγάλη δημοσιότητα, με αρκετούς να τα αντιμετωπίζουν ως επένδυση και άλλους να τα χρησιμοποιούν ακόμα και για καθημερινές συναλλαγές με online καταστήματα που δέχονται πληρωμές με Bitcoin, Ether ή άλλα δημοφιλή κρυπτονομίσματα.
Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια του ΔΠΜΣ «Τεχνοοικονομικά Συστήματα» και έχει ως σκοπό την γενικότερη παρουσίαση της τεχνολογίας του blockchain και της διείσδυσης της στους διάφορους κλάδους ως μεθόδου αποθήκευσης, κρυπτογράφησης και διαμοιρασμού δεδομένων. Το αντικείμενο της διπλωματικής είναι να επεξηγήσει τη λογική και τις βασικές λειτουργίες του blockchain, να παρουσιάσει τους κλάδους στους οποίους χρησιμοποιείται ή θα μπορούσε να χρησιμοποιηθεί και να εμβαθύνει στη χρήση του blockchain στον τομέα της υγείας, καθώς ο τελευταίος είναι ένας από τους τομείς με τις μεγαλύτερες ανάγκες διαμοιρασμού και ταυτόχρονα εξασφάλισης του απορρήτου των δεδομένων.

1.2 Δομή της διπλωματικής εργασίας

Κεφάλαιο 1ο:

Στο παρόν κεφάλαιο παρουσιάζεται το αντικείμενο και ο σκοπός της εργασίας, καθώς και η διάρθρωσή της σε κεφάλαια.

Κεφάλαιο 2ο:

Στο δεύτερο κεφάλαιο της παρούσας εργασίας γίνεται εισαγωγή στις έννοιες του blockchain και των hash functions, καθώς και στις μεθόδους κρυπτογράφησης με τη χρήση δημόσιων και ιδιωτικών κλειδιών. Στη συνέχεια παρουσιάζονται οι δημοφιλέστερες πλατφόρμες ανάπτυξης εφαρμογών βασισμένων σε blockchain και τα βασικά χαρακτηριστικά της κάθε μιας από αυτές.

Κεφάλαιο 3ο:

Το τρίτο κεφάλαιο πραγματεύεται τις τάσεις της τεχνολογίας του blockchain στην παγκόσμια αγορά, καθώς και τις χρήσεις που αυτό μπορεί να έχει ανά κλάδο, ξεκινώντας από την τραπεζική και καταλήγοντας σε μεθόδους αποθήκευσης και διαμοιρασμού υπολογιστικής ισχύος, καλύπτοντας ένα ιδιαίτερα ευρύ φάσμα αντικειμένων. Επιπλέον, γίνεται μία σύντομη περιγραφή γνωστών εφαρμογών που έχουν χρησιμοποιήσει την τεχνολογία του blockchain στους παραπάνω κλάδους.

Κεφάλαιο 4ο:

Στο κεφάλαιο 4 της διπλωματικής εργασίας αναλύεται η χρήση του blockchain στο χώρο της υγείας, και πιο συγκεκριμένα στο χώρο των ιατρικών φακέλων ασθενών, στην παρακολούθηση φαρμάκων και ιατρικού εξοπλισμού και στις κλινικές μελέτες. Στη συνέχεια, γίνεται αναφορά στις γνωστότερες εφαρμογές του blockchain στο χώρο της υγείας, είτε αυτές έχουν εμπορικό είτε ερευνητικό χαρακτήρα και στις τεχνολογίες που αυτές χρησιμοποιούν. Τέλος, αναφέρονται τα εμπόδια και οι προκλήσεις της εφαρμογής του blockchain στον τομέα της υγείας.

Κεφάλαιο 5ο:

Στο τελευταίο κεφάλαιο παρουσιάζονται τα συμπεράσματα της παρούσας διπλωματικής εργασίας, καθώς και οι προοπτικές επέκτασης του αντικειμένου που αυτή πραγματεύεται στα πλαίσια της χρήσης της τεχνολογίας του blockchain στην Υγεία και σε άλλους κλάδους.

Στο τέλος της διπλωματικής εργασίας παρουσιάζεται αναλυτικά η βιβλιογραφία που χρησιμοποιήθηκε.

2 Ανάλυση Τεχνολογικού Περιβάλλοντος

2.1 Τι είναι το blockchain

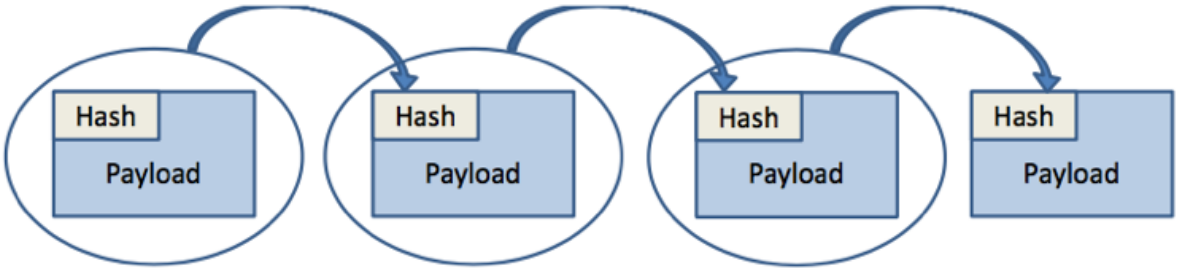
Η ιδέα του blockchain προέκυψε από την ανάγκη να υπάρξει αναπαραγωγή και μεταφορά ψηφιακής πληροφορίας με ασφαλή τρόπο χωρίς την αναγκαιότητα ύπαρξης ενός «μεσάζοντα» που διασφαλίζει την ακεραιότητα και την ασφαλή μεταφορά της. Πριν οριστεί το blockchain θα πρέπει να οριστούν κάποια επιμέρους χαρακτηριστικά στα οποία βασίζεται η λειτουργία του.

2.1.1 Οι συναρτήσεις hash (Hash Functions)

Μία **συνάρτηση hash** είναι μία μέθοδος μετατροπής δεδομένων τυχαίου μεγέθους σε μία ψηφιακή αλφαριθμητική ακολουθία με προκαθορισμένο σταθερό μήκος, η οποία λέγεται hash. Μία από τις πιο απλές συναρτήσεις hash είναι η συνάρτηση υπολοίπου διαίρεσης (modulo function), κατά την οποία μία οποιαδήποτε αλφαριθμητική ακολουθία με τυχαίο μήκος μπορεί να μετατραπεί σε έναν αριθμό (πιθανότατα πολύ μεγάλο), ο οποίος στη συνέχεια διαιρείται με μία σταθερή τιμή και το υπόλοιπο της διαίρεσης αυτής είναι το hash. Όπως είναι προφανές, το υπόλοιπο της διαίρεσης είναι μικρότερο σε μήκος από τη σταθερά με την οποία διαιρούμε. Αυτή η συνάρτηση hash είναι ιδιαίτερα απλή, αλλά δε χρησιμοποιείται γιατί η χρήση τέτοιων συναρτήσεων επιθυμεί μία επιπρόσθετη ιδιότητα, τον υπολογισμό μίας κατεύθυνσης (one way computation). Με άλλα λόγια, θα πρέπει να είναι εύκολο να υπολογίζεται ένα hash αλλά δύσκολο – πρακτικά αδύνατον – να υπολογιστούν τα στοιχεία από τα οποία προέκυψε.
Οι συναρτήσεις hash που ικανοποιούν την ιδιότητα της προηγούμενης παραγράφου συχνά αναφέρονται και ως κρυπτογραφικές συναρτήσεις hash (cryptographic hash functions), όταν είναι απαραίτητο να διακρίνονται από τις υπόλοιπες. Αυτές οι συναρτήσεις μετατρέπουν τα δεδομένα εισόδου με τόσο σύνθετο τρόπο ώστε πρακτικά ο αντίστροφος υπολογισμός να είναι αδύνατος. Οι πιο γνωστές κρυπτογραφικές συναρτήσεις είναι οι MD5, SHA 1 και SHA 2.
Όταν ένα hash, το οποίο έχει απεικονιστεί σε μία μορφή τροφοδοτείται εκ νέου ως είσοδος σε μία hash function προκύπτει ένα νέο hash. Όταν αυτή η διαδικασία επαναλαμβάνεται και τα αποτελέσματα της συνδυάζονται σε μία ακολουθία προκύπτει ένα hashchain.

2.1.2 Το hashchain – Η Εσωτερική Αλυσίδα

Το **hashchain** είναι μία ακολουθία ομογενών δομών δεδομένων – blocks – τα οποία συνδέονται μεταξύ τους με μία συνάρτηση hash. Στην ακόλουθη εικόνα φαίνεται η μορφή ενός hashchain.

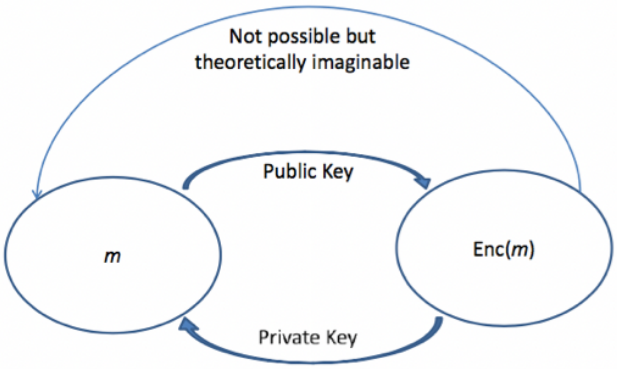


Εικόνα 1 – Σχηματική απεικόνιση ενός hashchain

Κάθε διακριτό block αποτελείται από το hash και το payload. Το hash του κάθε block υπολογίζεται από ολόκληρο το προηγούμενο block. Το payload αποτελείται από τα τυχαία δεδομένα του κάθε block. Το hashchain έχει μία πολύ σημαντική ιδιότητα: κανένα block δεν μπορεί να τροποποιηθεί χωρίς να τροποποιηθούν όλα τα υπόλοιπα μετά από αυτό. Για παράδειγμα, αν αλλάξουν τα τυχαία δεδομένα του block 1, τότε θα αλλάξει το hash του block 2 και αυτό θα οδηγήσει στην αλλαγή του hash του block 3 κ.ο.κ. .

2.1.3 Κρυπτογράφηση Δημόσιου Κλειδιού (Public Key Cryptography – PKC)

Η βασική ιδέα της **Κρυπτογράφησης Δημόσιου Κλειδιού (PKC)** είναι παρόμοια με τις συναρτήσεις hash και είναι οι υπολογισμοί μίας κατεύθυνσης. Για παράδειγμα, για κάποια δεδομένα m (message), οποιοσδήποτε μπορεί να υπολογίσει μία κρυπτογραφημένη τιμή Enc(m) (encrypted message), αλλά μόνο όποιος γνωρίζει το ειδικό κλειδί που σχετίζεται με την κρυπτογράφηση αυτή μπορεί να την αντιστρέψει και να παράγει το m από το Enc(m).
Για να επιτευχθεί η κρυπτογράφηση δημόσιου κλειδιού θα πρέπει πρώτα να δημιουργηθεί ένα ζεύγος κλειδιών, το δημόσιο και το ιδιωτικό κλειδί (public key – private key). Το δημόσιο κλειδί χρησιμοποιείται για να κρυπτογραφεί τα δεδομένα και μπορεί να είναι γνωστό στον οποιοδήποτε, ενώ το ιδιωτικό κλειδί είναι απαραίτητο για την αποκρυπτογράφηση του μηνύματος και θα πρέπει να διατηρείται κρυφό.

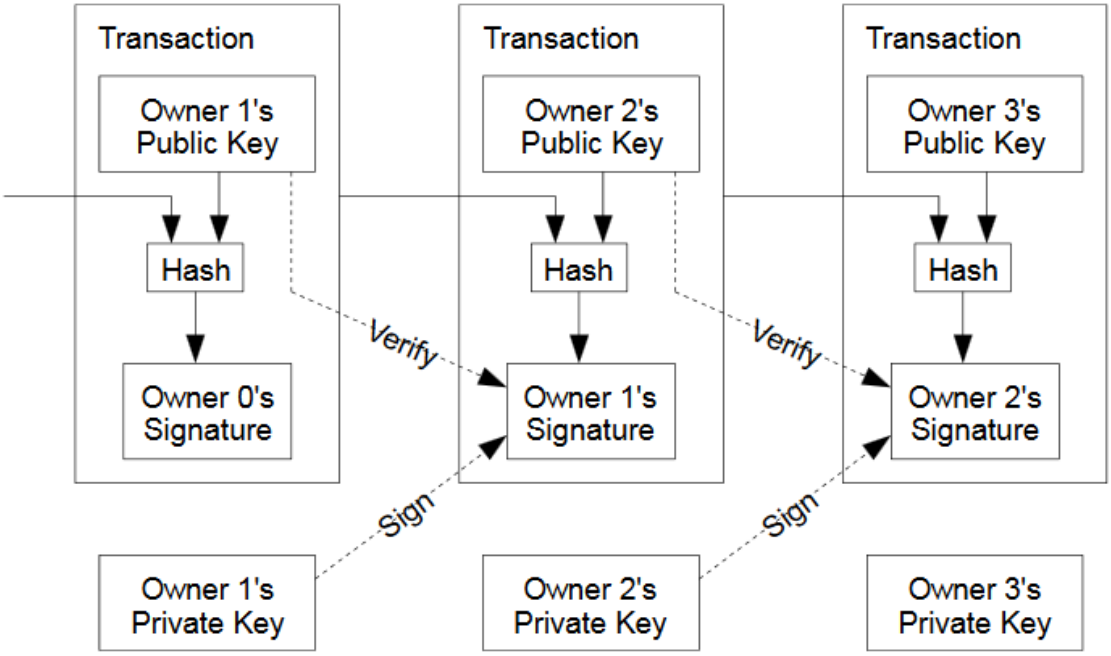


Εικόνα 2 - Η πορεία των υπολογισμών της Κρυπτογράφησης Δημόσιου Κλειδιού

Στην παραπάνω εικόνα φαίνεται η διαδικασία του PKC. Το βέλος στο πάνω μέρος της εικόνας απεικονίζει τη θεωρητική πιθανότητα της αποκρυπτογράφησης του μηνύματος χωρίς τη γνώση του private key. Για παράδειγμα, η κρυπτογράφηση RSA βασίζεται πάνω στην παραγοντοποίηση μεγάλων αριθμών.

2.1.4 Η ασφάλεια των hashchains με τη χρήση Κρυπτογράφησης Δημόσιου Κλειδιού (PKC)

Μια σημαντική παράμετρος για πλήθος εφαρμογών αποτελεί η δυνατότητα σε κάθε hashchain μόνο ένα πρόσωπο να μπορεί να δημιουργήσει ένα νέο block. Αυτό μπορεί να επιτευχθεί αρκεί κάθε επόμενο block να υπογράφεται με το private key του χρήστη του οποίου το public key είναι διαθέσιμο στο τρέχον block. Όπως φαίνεται στην ακόλουθη εικόνα, αν ένα block περιλαμβάνει το public key του owner 1 και έχει υπογραφεί από τον χρήστη owner 0, τότε ο owner 1 μπορεί να δημιουργήσει ένα επόμενο block με τη δημιουργία ενός νέου public key, το οποίο θα υπογράψει με το private key του. Το νέο public key θα έχει έναν νέο owner 2 και θα ανήκει σε όποιον έχει στην κατοχή του το αντίστοιχο private key για να υπογράψει το επόμενο block.

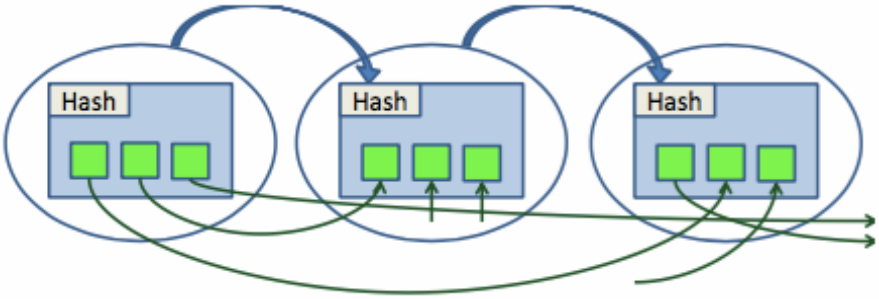


Εικόνα 3 - Ενδεικτική εσωτερική δομή ενός hashchain

Το hashchain με Κρυπτογράφηση Δημόσιου Κλειδιού μπορεί να χρησιμοποιηθεί ως ένας τρόπος για ασφαλή μεταφορά ψηφιακών «αντικειμένων», όπως τα tokens, υποθέτοντας ότι ένα hashchain αναπαριστά ένα token. Ο ιδιοκτήτης του τελευταίου block είναι και ιδιοκτήτης του token, καθώς μόνο αυτός μπορεί να το μεταβιβάσει σε κάποιον άλλο ιδιοκτήτη. Για να υλοποιηθεί, ωστόσο, ένα τέτοιο hashchain απαιτείται η ύπαρξη ενός κεντρικού χώρου στον οποίο τα blocks θα δημιουργούνται, θα αποθηκεύονται και θα μπορούν να επαληθεύονται, χωρίς να χρειάζεται ένας ενδιάμεσος και έμπιστος φορέας για τη διαχείριση της όλης διαδικασίας.

2.1.5 Το blockchain – Εξωτερική Αλυσίδα

Υποθέτοντας την ύπαρξη μιας διαρκούς διαδικασίας παραγωγής νέων blocks για ένα παγκόσμιο hashchain, καθώς και ότι σε αυτό το hashchain είναι δυνατόν να τοποθετηθούν οποιαδήποτε δεδομένα στο payload των blocks, θα ήταν δυνατόν να προσθέτουμε τα blocks κάποιων επιμέρους hashchains στο εσωτερικό των blocks αυτού του συνεχώς επεκτεινόμενου hashchain. Με πιο απλά λόγια, θα είχαμε πολλά εσωτερικά hashchains μέσα σε ένα άλλο εξωτερικό hashchain. Ο μηχανισμός αυτός λέγεται **blockchain**.



Εικόνα 4 - Ένα εξωτερικό hashchain του οποίου τα blocks περιέχουν άλλα hashchains

Στην παραπάνω εικόνα απεικονίζεται ένα (εξωτερικό) hashchain μέσα στα blocks του οποίου υπάρχουν τα blocks από εσωτερικά hashchains σε τυχαία κατανομή.

Πρακτικά, το blockchain είναι μία σειρά καταχωρήσεων που αφορούν «συναλλαγές», σε ένα δημόσιο κατάστιχο (ledger). Κάθε καινούρια ομάδα καταχωρήσεων – block – συνδέεται με τις προηγούμενες, δημιουργώντας μία αλυσίδα blockchain.

Τα blocks αυτά συνδέονται μονοσήμαντα μεταξύ τους και προκύπτουν από μία διαδικασία που ονομάζεται «proof of work», κατά την οποία επιτυγχάνεται η αλγοριθμική επίλυση ενός «δύσκολου» υπολογιστικού προβλήματος και ο δημιουργός του νέου block επιβραβεύεται για την προσφορά υπολογιστικής προσπάθειας στο δίκτυο peer to peer (p2p). Με αυτό τον τρόπο το Blockchain σχεδιάστηκε με σκοπό να λειτουργεί ως ένα αποκεντρωμένο (decentralized) κοινόχρηστο κατάστιχο (shared ledger), το οποίο είναι κοινό για όλους τους συμμετέχοντες, μιας και όλοι οι εμπλεκόμενοι αποθηκεύουν ένα αντίγραφο του και το συντηρούν – επεκτείνουν μέσω της προσφοράς πόρων για τη δημιουργία - «mining» - των νέων blocks, εξασφαλίζοντας τη διαφάνεια και την ασφάλεια των συναλλαγών.

Η ειδοποιός διαφορά είναι ότι δεν είναι πλέον απαραίτητη η ύπαρξη μίας ενδιάμεσης «έμπιστης» αρχής, καθώς την εμπιστοσύνη των συναλλασσόμενων μερών επιβεβαιώνουν οι αλγόριθμοι που καθιστούν δύσκολη την παραποίηση της αλυσίδας, καθώς η οποιαδήποτε αλλαγή απαιτεί υπολογιστικούς πόρους που στην πράξη είναι αδύνατο να έχει κάποιος στη διάθεσή του. Η δημόσια πρόσβαση στο blockchain διευκολύνει τη διαφάνεια στις συναλλαγές και τη διάχυση της πληροφορίας. Στο ίδιο πλαίσιο, διευκολύνεται η ελεγκτική διαδικασία με την εξάλειψη κάθε ενδεχομένου παραβάσεων, ακριβώς εξαιτίας της δημόσιας φύσης των δεδομένων. (Mazonka, 2016)

2.1.6 Δημόσια και Ιδιωτικά blockchains

Όταν αναφέρεται κανείς στην ανάπτυξη ενός blockchain σε μορφή δικτύου, τότε αυτό μπορεί να είναι είτε δημόσιο είτε ιδιωτικό, ανάλογα με τα δικαιώματα των χρηστών που έχουν

πρόσβαση σε αυτό, αλλά και δικαίωμα να τροποποιήσουν τις εγγραφές (blocks) του ή να δημιουργήσουν νέα blocks.

Στα **δημόσια blockchains** (permissionless ή public), το σύνολο του δικτύου είναι προσβάσιμο δημοσίως από όλους τους υπολογιστές και τις συσκευές. Ο οποιοδήποτε μπορεί να έχει πρόσβαση στον κώδικα, να ξεκινήσει την εκτέλεση ενός κόμβου του δικτύου σε κάποια τοπική συσκευή, να ξεκινήσει και να ολοκληρώσει κάποια συναλλαγή εντός του δικτύου, να ταυτοποιήσει συναλλαγές, και όλα αυτά ενώ παραμένει ανώνυμος προς το υπόλοιπο δημόσιο δίκτυο. Εν συντομία, το αποκεντρωμένο blockchain είναι προσβάσιμο με ίσες δυνατότητες από όλους, χωρίς οποιαδήποτε διαδικασία ταυτοποίησης. Παράδειγμα σε αυτή την κατηγορία αποτελούν τα blockchains καταγραφής συναλλαγών του κρυπτονομίσματος Bitcoin (BTC).

Στα **ιδιωτικά blockchains** (permissioned ή private), το οικοσύστημα στο οποίο φιλοξενείται το blockchain και τα δεδομένα αυτού είναι κλειστό, και μόνο οι εξουσιοδοτημένοι χρήστες μπορούν να εκτελούν ενέργειες, ανάλογα με τα δικαιώματα που έχουν. Τα blockchains αυτής της κατηγορίας είναι δομημένα με ένα σύνολο κανόνων που διέπουν τον τρόπο που πρέπει να γίνει η οποιαδήποτε συναλλαγή , με σκοπό να ικανοποιήσουν τις ιδιαίτερες ανάγκες ενός οργανισμού, όπως για παράδειγμα η διατήρηση ιστορικού αλλαγών (audit trail) σε βάσεις δεδομένων. Αυτός ο τύπος του blockchain διατηρεί όλα τα κύρια χαρακτηριστικά της τεχνολογίας του blockchain, όπως ο αυτόματος συγχρονισμός δεδομένων, η διατηρησιμότητα των δεδομένων, παρέχοντας ταυτόχρονα τη δυνατότητα ύπαρξης αυστηρών κανόνων ιδιωτικότητας και ασφάλειας. Παράδειγμα ιδιωτικού blockchain αποτελεί η υλοποίηση του Multichain. (A Digestible Guide to Blockchain App Development, 2018)

2.2 Πλατφόρμες ανάπτυξης εφαρμογών blockchain

Η επιλογή της πλατφόρμας ανάπτυξης μίας εφαρμογής blockchain, λόγω του ιδιαίτερα καινοτόμου χαρακτήρα της τεχνολογίας αυτής είναι ένα περίπλοκο ερώτημα, το οποίο θα πρέπει να αναλυθεί σε επιμέρους επιλογές και ερωτήσεις, ώστε να επιλεγεί η καταλληλότερη πλατφόρμα ανάπτυξης ανάλογα με τη φύση και τις ανάγκες της εκάστοτε εφαρμογής.

Όσον αφορά τη **φύση της πλατφόρμας**, το ερώτημα που θα πρέπει να απαντηθεί αφορά στο αν η πλατφόρμα θα βασίζεται σε κάποιο συγκεκριμένο κρυπτονόμισμα, αν θα βασίζεται σε smart contracts, και αν θα χρησιμοποιηθούν ένα ή περισσότερα tokens.

Το δεύτερο σημείο στο οποίο θα πρέπει να δοθεί προσοχή είναι αν η εφαρμογή που αναπτύσσεται θα κάνει οποιασδήποτε μορφής **χρήση των smart contracts**, χρησιμοποιώντας

τα ως πρωτόκολλα αυτοελέγχου που επικυρώνουν ή επιβάλλουν οποιαδήποτε ενέργεια που εκκινείται μέσω σκανδάλης (trigger) στο blockchain.

Στη συνέχεια, η επιλογή της πλατφόρμας ανάπτυξης μίας εφαρμογής είναι άμεσα συνδεδεμένη με το **πρωτόκολλο συναίνεσης (consensus protocol)** μεταξύ των χρηστών του blockchain, του τρόπου, δηλαδή, που θα χρησιμοποιείται για την οριστικοποίηση του περιεχομένου των blocks του blockchain και την αποδοχή του εν συνεχεία από τους συμμετέχοντες στο peer-to-peer δίκτυο. (Srivastav, 2018)

Τα πιο διαδεδομένα consensus protocols είναι τα ακόλουθα:

- ***Proof of Work**:* Το πρωτόκολλο Proof of Work (PoW) είναι το πρώτο πρωτόκολλο που χρησιμοποιήθηκε στο blockchain, όταν αυτό παρουσιάστηκε από τον S. Nakamoto το 2008 στα πλαίσια της δημοσίευσης του Bitcoin ως εναλλακτικού μέσου ανταλλαγής χρημάτων χωρίς την εμπλοκή τρίτων φορέων. Η λογική του βασίζεται στην παραδοχή ότι όλοι οι συμμετέχοντες στο δίκτυο συνεισφέρουν υπολογιστική ισχύ με σκοπό τη δημιουργία νέων blocks για τη συνέχιση του blockchain και την επικύρωση των συναλλαγών που καταγράφονται σε αυτό έχοντας ως κίνητρο κάποια ανταμοιβή. Συχνό παράδειγμα σε εφαρμογές κρυπτονομισμάτων αποτελεί η απόδοση στο δημιουργό του κάθε block ποσοστού από τα κόστη συναλλαγών (transaction fees) ή ακόμα και σταθερού ποσού νέων νομισμάτων που δημιουργούνται στα πλαίσια της δημιουργίας των blocks. (Proof-of-Work System, 2018)
- ***Proof of Stake**:* Το πρωτόκολλο Proof of Stake (PoS) είναι ένας τύπος αλγορίθμου με τον οποίο ένα δίκτυο κρυπτονομίσματος βασισμένο σε blockchain μπορεί να επιτύχει κατανεμημένη συναίνεση, χωρίς να δαπανώνται μεγάλα ποσά ενέργειας. Η επιλογή του δημιουργού του επόμενου block σε blockchains βασισμένα στο PoS γίνεται με βάση διάφορους συνδυασμούς πλούτου ή ηλικίας του χρήστη στο δίκτυο, με αποτέλεσμα να μην προσπαθούν ταυτόχρονα όλοι οι χρήστες να συνεισφέρουν στο δίκτυο, όπως στο PoW πρωτόκολλο και να εξοικονομούνται πόροι του δικτύου. (Proof of Stake, 2018)
- ***Proof of Elapsed Time**:* Το πρωτόκολλο Proof of Elapsed Time (PoET) είναι μία εξέλιξη του πρωτοκόλλου Proof of Work, στη βάση της λογικής ότι το PoW είναι ιδιαίτερα ενεργοβόρο, καθώς απαιτείται διαρκής προσφορά υπολογιστικής ισχύος μέχρι την επίλυση των μαθηματικών προβλημάτων από κάποιο χρήστη για τη δημιουργία κάποιου block και την ανταμοιβή του. Για την ολοκλήρωση της διαδικασίας δημιουργίας ενός block, κάθε χρήστης από τους συμμετέχοντες στο δίκτυο αντιστοιχίζεται με ένα συγκεκριμένο τυχαίο χρονικό διάστημα. Ο χρήστης με το

μικρότερο χρονικό διάστημα επιλέγεται από την εφαρμογή αυτόματα, όταν αυτό παρέλθει, για να οριστικοποιήσει το περιεχόμενο του block και να κοινοποιήσει το block στο υπόλοιπο δίκτυο. (What is Proof of Elapsed Time Consensus? (PoET), 2018)

- ***Proof of Burn**:* Το πρωτόκολλο Proof of Burn (PoB) είναι μία ακόμα εξέλιξη του πρωτοκόλλου Proof of Work, σύμφωνα με το οποίο οι χρήστες του δικτύου του blockchain θα πρέπει να αποδείξουν ότι «έκαψαν» κάποια νομίσματα. Το κάψιμο των νομισμάτων του δικτύου γίνεται μέσω της αποστολής σε μία απροσπέλαστη διεύθυνση, στην οποία επαληθεύει το σύνολο του δικτύου ότι τα νομίσματα που καταστρέφονται (burn) δεν μπορούν να ανακτηθούν από κανένα μέλος του δικτύου. Συχνά χρησιμοποιείται για την έναρξη ενός νέου κρυπτονομίσματος μέσω καταστροφής αντίστοιχης αξίας υπαρκτών νομισμάτων. (Proof Of Burn, 2018)
- ***Proof of Authority**:* Το πρωτόκολλο Proof of Authority (PoA) είναι ένα διαφορετικής λογικής πρωτόκολλο από τα προηγούμενα και χρησιμοποιείται σε ιδιωτικά δίκτυα blockchain. Η επικύρωση των συναλλαγών πραγματοποιείται από εγκεκριμένους λογαριασμούς, τους επικυρωτές, οι οποίοι τρέχουν ειδικό λογισμικό το οποίο είναι σχεδιασμένο για να δημιουργεί blocks και να επικυρώνει την ακεραιότητα του blockchain για λογαριασμό του συνόλου των χρηστών – συμμετεχόντων σε αυτό. (Rolling your own Proof-of-Authority Ethereum consortium, 2017)

Μετά την επιλογή της φύσης της πλατφόρμας και του πρωτοκόλλου επικοινωνίας των χρηστών του δικτύου, βασικό παράγοντα επιλογής της πλατφόρμας ανάπτυξης μιας εφαρμογής αποτελεί η **αναγκαιότητα χρήσης κρυπτονομισμάτων** για την διεξαγωγή συναλλαγών στα πλαίσια των λειτουργιών της εφαρμογής που πρόκειται να αναπτυχθεί.

Τέλος, μία εξίσου σημαντική επιλογή είναι ο καθορισμός του τύπου του δικτύου ως **ιδιωτικού ή δημόσιου blockchain** (βλ. ενότητα 2.1.6), ή ενός συνδυασμού των δύο σε κάποια εξειδικευμένη υβριδική λύση, ώστε να είναι καθορισμένα τα δικαιώματα των συμμετεχόντων στο blockchain, καθώς και το ποιοι θα συμμετέχουν στην ανάπτυξη και εξέλιξη του. (Srivastav, 2018)

2.2.1 Ethereum

Το Ethereum είναι μία ανοικτή πλατφόρμα η οποία επιτρέπει στον οποιοδήποτε να δημιουργήσει και να χρησιμοποιήσει στη συνέχεια αποκεντρωμένες εφαρμογές βασισμένες στο blockchain. Το αρχικό project του Ethereum δημοσιεύτηκε το 2014, όταν οι Vitalik Buterin, Gavin Wood και Jeffrey Wilcke ξεκίνησαν να δουλεύουν πάνω σε ένα blockchain

νέας γενιάς που θα βασιζόταν στα smart contracts και θα μπορούσε να χρησιμοποιηθεί για συναλλαγές πέρα από την έννοια των χρηματικών συναλλαγών, όπως ήταν η αρχική υλοποίηση του Bitcoin.

Εικόνα 5 – Το λογότυπο της πλατφόρμας Ethereum [ethereum.org]

Είναι το πιο διαδεδομένο εργαλείο ανάπτυξης εφαρμογών βασισμένων στο blockchain και ο κώδικας του ενημερώνεται διαρκώς στο GitHub από χιλιάδες προγραμματιστές που συνεισφέρουν στο λογισμικό ανοιχτού κώδικα που έχει δημοσιευτεί εκεί. Υποστηρίζει τρείς γλώσσες προγραμματισμού, την Python (pyethereum), την GoLang (gpethereum) και την C++ (cpp-ethereum).

Για την καταγραφή συναλλαγών στο κατάστιχο και για τις υπολογιστικές υπηρεσίες που προσφέρουν οι συμμετέχοντες στο δίκτυο του Ethereum μέσω επίλυσης μαθηματικών αλγορίθμων που βασίζονται στο μοντέλο Proof of Work (PoW), χρησιμοποιείται το κρυπτονόμισμα Ether (ETH), το οποίο κατά τη συγγραφή της παρούσας διπλωματικής ήταν το δεύτερο μεγαλύτερο στην παγκόσμια αγορά σε επίπεδο κεφαλαιοποίησης σύμφωνα με την ιστοσελίδα coinmarketcap.com. (What is Ethereum?, 2016)

2.2.2 Hyperledger

Το Hyperledger είναι ένα project του Linux Foundation που ξεκίνησε το 2015, όταν πολλές επιχειρήσεις που ενδιαφέρονταν για την τεχνολογία του blockchain αποφάσισαν ότι θα ήταν προτιμότερο να ενώσουν τις δυνάμεις τους με σκοπό να παράγουν ένα open-source blockchain που θα μπορούσε να χρησιμοποιείται από τον καθένα. Μέχρι τη στιγμή συγγραφής της παρούσας διπλωματικής πάνω από 230 οργανισμοί έχουν γίνει μέλη στο εγχείρημα του Hyperledger, συμπεριλαμβανομένων εταιριών πληροφορικής και υπολογιστικών συστημάτων όπως η IBM και η VMware, αλλά και εταιριών άλλων κλάδων όπως η Airbus και η JP Morgan.

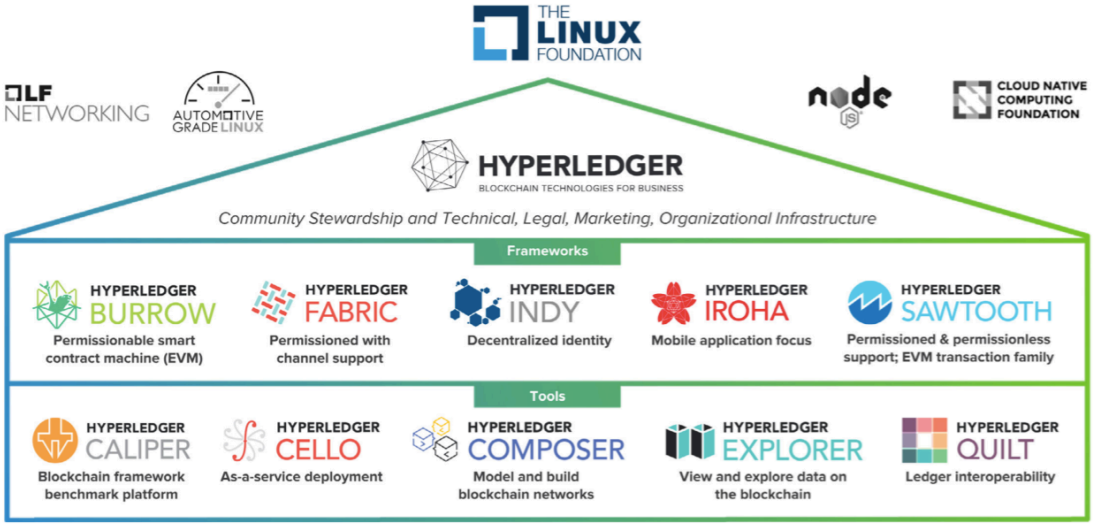
Εικόνα 6 - Το λογότυπο της πλατφόρμας Hyperledger [hyperledger.org]

Το Hyperledger καλύπτει ένα πλήρες φάσμα περιπτώσεων χρήσης, καθώς τα διαφορετικά σενάρια των διαφορετικών επιχειρήσεων που συμμετέχουν στην υλοποίηση του δημιουργούν διαφορετικές απαιτήσεις για τους χρόνους επικύρωσης, την αποκέντρωση, την εμπιστοσύνη και άλλα ζητήματα. Για να αντιμετωπιστεί αυτή η πολυμορφία, όλα τα projects του Hyperledger ακολουθούν την ίδια φιλοσοφία σχεδιασμού με τα ακόλουθα χαρακτηριστικά:

- Αρθρωτή αρχιτεκτονική
- Υψηλή ασφάλεια
- Διαλειτουργικότητα
- Ανεξαρτησία από κρυπτονομίσματα, αλλά με δυνατότητα υποστήριξης αυτών
- Δυνατότητες διασύνδεσης με APIs

Για να καλυφθεί το σύνολο των αναγκών των συμμετεχόντων στο Hyperledger, έχουν αναπτυχθεί διαφορετικά frameworks και εργαλεία που βασίζονται σε αυτό. Η επιλογή του κατάλληλου framework θα πρέπει να γίνει ανάλογα με τις απαιτήσεις της κάθε εφαρμογής ως προς την προσβασιμότητα και τα δικαιώματα, τη χρήση της εφαρμογής από κινητές συσκευές, καθώς και τη διαλειτουργικότητα με άλλες εφαρμογές. (Hyperledger.org, 2018)

Το οικοσύστημα του Hyperledger φαίνεται στην παρακάτω εικόνα του Linux Foundation.



Εικόνα 7 - Η δομή του Hyperledger project [hyperledger.org]

2.2.3 IBM Blockchain

Η πλατφόρμα IBM Blockchain είναι μια ευέλικτη υπηρεσία του IBM Cloud που προσφέρεται βασισμένη στο μοντέλο Software as a Service (SaaS). Η χρήση της πλατφόρμας αυτής επιτρέπει στα μέλη του δικτύου να ξεκινήσουν γρήγορα την ανάπτυξη εφαρμογών και να

προχωρήσουν γρήγορα μέσω ενός συνεργατικού περιβάλλοντος. Για την κάλυψη των αναγκών των χρηστών της υπηρεσίας αυτής, η IBM παρέχει διάφορα πακέτα συνδρομών.

Εικόνα 8 - Το λογότυπο του IBM Bluemix Blockchain [ibm.com]

Το προσφερόμενο blockchain είναι ένα ιδιωτικό – permissioned δίκτυο, το οποίο υποστηρίζει την ανάπτυξη εφαρμογών blockchain στο IBM Cloud μέσω σχετικής πλατφόρμας που διαθέτει η IBM στους πελάτες της. Οι υποστηριζόμενες γλώσσες προγραμματισμού για τη χρήση του IBM Blockchain είναι η Javascript και η GoLang. (IBM Blockchain, 2018)

2.2.4 Multichain

Το MultiChain είναι μία πλατφόρμα για τη δημιουργία και την ανάπτυξη ιδιωτικών blockchains είτε εντός ενός οργανισμού, είτε μεταξύ οργανισμών. Στόχος της πλατφόρμας είναι να παρέχει ιδιωτικότητα και έλεγχο στο παρεχόμενο blockchain με ένα εύκολο σε χρήση πακέτο, κυρίως σε οικονομικούς οργανισμούς και οικονομικά τμήματα οργανισμών. Αναπτύχθηκε πάνω σε κάποια χαρακτηριστικά που θεωρεί ως μειονεκτήματα του Bitcoin, όπως είναι η δημόσια δομή του δικτύου του, οι μεγάλες ανάγκες για υπολογιστική ισχύ στα πλαίσια του μοντέλου Proof of Work και της έλλειψης ελεγχόμενης πρόσβασης.

Εικόνα 9 - Το λογότυπο της πλατφόρμας MultiChain [multichain.com]

Η ανάπτυξη του MultiChain έγινε με βάση τον δημοσιευμένο κώδικα του Bitcoin, με αλλαγές και προσθήκες που διασφαλίζουν την ιδιωτικότητα και την ελεγχόμενη πρόσβαση. Έτσι, στο δίκτυο του MultiChain υπάρχει συγκεκριμένος αριθμός εγκεκριμένων miners, οι οποίοι μπορούν να δημιουργήσουν συγκεκριμένο αριθμό συνεχόμενων blocks ώστε να διασφαλίζεται η δίκαιη και ταυτόχρονη συμμετοχή όλων των πιστοποιημένων κόμβων. Η πρόσβαση των χρηστών γίνεται μέσω δημόσιων κλειδιών τα οποία ανήκουν σε λίστα δικαιωμάτων πρόσβασης. Οι υποστηριζόμενες γλώσσες προγραμματισμού για τη χρήση του MultiChain

είναι η Python, η C#, η JavaScript, η PHP και η Ruby. Η χρήση του σε εφαρμογές είναι ελεγχόμενη και ανάλογα με το χαρακτήρα της εφαρμογής ως open-source ή όχι, η παροχή της πλατφόρμας είναι δωρεάν ή επί πληρωμή. (Greenspan, 2015)

2.2.5 Hydrachain

Το Hydrachain είναι μία προσπάθεια ανάπτυξης ενός ιδιωτικού blockchain βασισμένη στο πρωτόκολλο του Ethereum που ξεκίνησε στα μέσα του 2015. Σε αντίθεση με το Ethereum δεν βασίζεται στο πρωτόκολλο Proof of Work, αλλά σε μία παραλλαγή του Proof of Authority (PoA), την οποία οι δημιουργοί της πλατφόρμας ονομάζουν Proof of Identity, και λειτουργεί όπως το PoA, καθώς μόνο οι εξουσιοδοτημένοι χρήστες μπορούν να επικυρώσουν την αλυσίδα των δεδομένων. Η δημιουργία ενός νέου block προκύπτει μετά από διαπραγμάτευση μεταξύ των εξουσιοδοτημένων χρηστών, οι οποίοι θα πρέπει να είναι όλοι διαθέσιμοι για να υπογραφεί το block και να προστεθεί στην αλυσίδα.

Εικόνα 10 - Το λογότυπο της Brainbot Technologies - Δημιουργού του Hydrachain [brainbot.com]

Το πρωτόκολλο Hydrachain είναι ένα πρωτόκολλο που υποστηρίζει τη δημιουργία smart contracts βασισμένων στη γλώσσα προγραμματισμού Python και είναι πλήρως διαλειτουργικό με το πρωτόκολλο του Ethereum. Επιπλέον, σε σύγκριση με τα υπόλοιπα πρωτόκολλα, μία πρωτοφανής δυνατότητα είναι υπό ανάπτυξη από την open source κοινότητα και αφορά στη δυνατότητα του blockchain να εκτελείται σε διαφορετικά instances και να δημιουργούνται πλήρως διαλειτουργικά blockchains που θα συνδέονται μεταξύ τους.
Η διάθεση του Hydrachain γίνεται με βάση τα πλαίσια του MIT License για τα λογισμικά ανοικτού κώδικα, ενώ η Brainbot Technologies σε συνεργασία με ένα δίκτυο εταιριών πληροφορικής παρέχει μία εμπορική μορφή του πρωτοκόλλου αυτού. Η τελευταία ενημέρωση του open source project στο GitHub έγινε στα τέλη του 2016. (HyrdaChain: Permissioned Distributed Ledger based on Ethereum, 2018)

2.2.6 BigchainDB

Το BigchainDB είναι ένα λογισμικό που συνδυάζει τις ιδιότητες του blockchain (π.χ. αποκεντρωμένη διαχείριση, διατηρησιμότητα και ιδιότητες πλήρως διαμορφώσιμες από τον

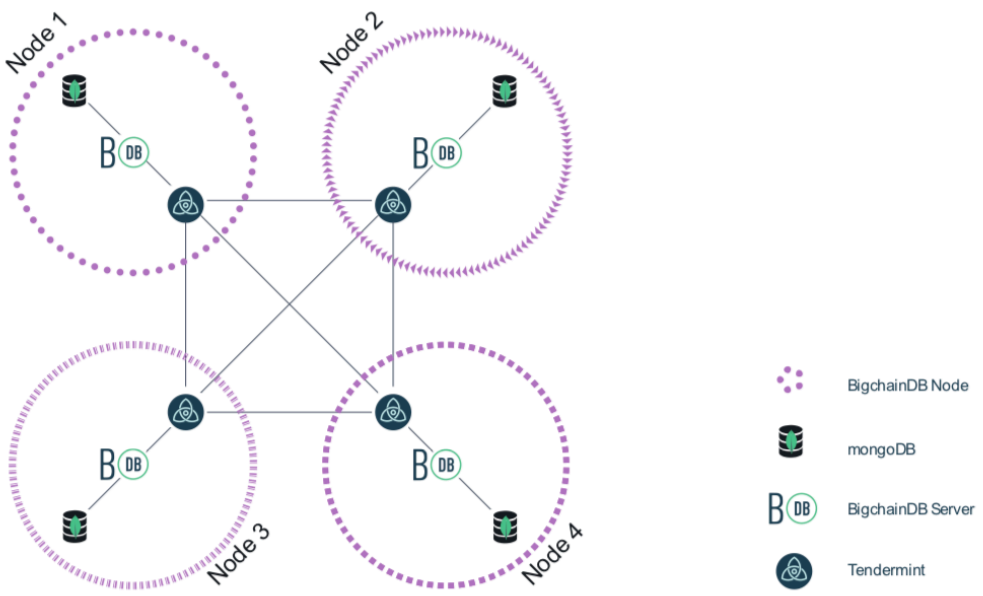
ιδιοκτήτη), με τις ιδιότητες μίας βάσης δεδομένων (π.χ. υψηλά ποσοστά συναλλαγών, χαμηλή λανθάνουσα κατάσταση (latency), δυνατότητα ύπαρξης ευρετηρίων (indexes) και ερωτήματα δομημένων δεδομένων). Η πρώτη έκδοση του διατέθηκε με τη μορφή λογισμικού ανοικτού κώδικα το 2016 και έκτοτε βελτιώνεται συνεχώς. Η πλατφόρμα δεν βασίζει τη λειτουργία της σε κάποιας μορφής κρυπτονόμισμα ή token.

Το Μάιο του 2018 δημοσιεύτηκε και η δεύτερη έκδοση του λογισμικού, BigchainDB 2.0, μαζί με το αντίστοιχο White paper. Η δεύτερη έκδοση του BigchainDB έχει σημαντικές βελτιώσεις σε σχέση με την πρώτη, καθώς είναι ανθεκτική στο Byzantine Fault Tolerance (BFT)[1], που σημαίνει ότι ακόμα και το ένα τρίτο του συνόλου των κόμβων να είναι εκτός δικτύου για τον οποιοδήποτε λόγο, το blockchain μπορεί να διατηρείται ενημερωμένο και οι κόμβοι θα συνεχίζουν να συμφωνούν μεταξύ τους. Με τη δεύτερη έκδοση, οι δημιουργοί του αναφέρουν ότι είναι έτοιμο για παραγωγικές εφαρμογές σε πολλές περιπτώσεις κλάδων, συμπεριλαμβανομένων των αλυσίδων εφοδιασμού, της διαχείρισης δικαιωμάτων πνευματικής ιδιοκτησίας, του Internet of Things, των κυβερνητικών δεδομένων και των αμετάβλητων διαδρομών ελέγχου.

Εικόνα 11 - Το λογότυπο της πλατφόρμας BigchainDB [bigchaindb.com]

Η χρήση του BigchainDB μπορεί να γίνει με οποιαδήποτε γλώσσα προγραμματισμού. Οι δημιουργοί του διαθέτουν πλήρως ενημερωμένα πακέτα λογισμικού στις γλώσσες Python και Javascript. Οι βάσεις δεδομένων που χρησιμοποιούνται σε κάθε κόμβο του δικτύου είναι βασισμένες σε MongoDB και οι συναλλαγές που πραγματοποιούνται σε κόμβο κοινοποιούνται στους υπόλοιπους κόμβους του δικτύου μέσω ενός αρχείου JSON, εξασφαλίζοντας τα πλεονεκτήματα του blockchain σε συνδυασμό με αυτά μίας σχεσιακής βάσης δεδομένων, όπως αναφέρεται και παραπάνω. (BigchainDB, 2018)

[1] Το Byzantine Fault Tolerance (BFT) είναι η αξιοπιστία ενός συστήματος ηλεκτρονικών υπολογιστών σε κατανεμημένα υπολογιστικά συστήματα, όπου τα συστατικά του κατανεμημένου συστήματος μπορεί να αποτυγχάνουν και να μην υπάρχει επαρκής πληροφόρηση σχετικά με αυτή τους την αποτυχία. Σε μία «Βυζαντινή Αποτυχία» ένας διακομιστής μπορεί να εμφανίζει ανομοιογενή συμπεριφορά απέναντι σε συστήματα ανίχνευσης βλαβών και ταυτόχρονα να παρουσιάζει διαφορετικά συμπτώματα σε διαφορετικούς παρατηρητές. Αυτό καθιστά δύσκολο για τα υπόλοιπα συστατικά να δηλώσουν ότι απέτυχαν και να απενεργοποιήσουν τα ελαττωματικά από το δίκτυο, καθώς πρώτα πρέπει να καταλήξουν συναινετικά ως προς το ποιο συστατικό είναι αυτό που αποτυγχάνει εξαρχής.



Εικόνα 12 - Παράδειγμα δομής δικτύου BigchainDB [BigchainDB 2.0 White Paper, 2018]

2.2.7 Openchain

Το Openchain είναι ένα λογισμικό κατανεμημένου κατάστιχου βασισμένο σε ανοιχτό κώδικα. Είναι κατάλληλο για οργανισμούς που επιθυμούν να εκδίδουν και να διαχειρίζονται ψηφιακά στοιχεία ενεργητικού με ένα ισχυρό, ασφαλή και επεκτάσιμο τρόπο. Το ιδιωτικό blockchain στο οποίο βασίζεται η λειτουργία του περιλαμβάνει ένα διαχειριστή, ο οποίος έχει δικαίωμα να καθορίζει τους κανόνες του κατάστιχου των συναλλαγών. Οι συναλλαγές υπογράφονται ψηφιακά από μία αρχή αρμόδια για την εκτέλεση της συγκεκριμένης εργασίας, ενώ τα διάφορα instances μπορούν να επικοινωνούν και να διαλειτουργούν μεταξύ τους. Η χρήση του μπορεί να γίνει σε εφαρμογές που βασίζονται στη γλώσσα προγραμματισμού JavaScript.

Εικόνα 13 - Το λογότυπο της πλατφόρμας Openchain [openchain.org]

Τα βασικά πλεονεκτήματα της πλατφόρμας είναι:

- Άμεση επιβεβαίωση των συναλλαγών από την κεντρική αρχή.
- Δεν υπάρχει ανάγκη εξόρυξης (mining) και τέλη για την εξόρυξη των νέων blocks.
- Έχει εξαιρετικά υψηλή επεκτασιμότητα.

- Διατηρησιμότητα μέσω καταχώρησης «αγκυρών» στο blockchain του Bitcoin που είναι μη αναστρέψιμο.
- Ύπαρξη ιεραρχικού συστήματος λογαριασμών που επιτρέπει τον καθορισμό δικαιωμάτων σε πολλαπλά επίπεδα.
- Δυνατότητα ύπαρξης πολλαπλών instances του Openchain εντός ενός οργανισμού και πλήρους διαλειτουργικότητας μεταξύ αυτών.

Το Openchain είναι ένα λογισμικό που βασίζεται στη λογική της διατήρησης της ιδιοκτησίας, το οποίο μπορεί να προσαρμοστεί σε οποιαδήποτε χρήση αυτού του χαρακτήρα. Παράδειγμα χρήσης θα μπορούσαν να αποτελούν οι αγορές των ακινήτων, των μετοχών και ομολόγων, του πετρελαίου και άλλων ορυκτών, καθώς και δικαιωμάτων ιδιοκτησίας όπως αυτά συναντώνται στην μουσική βιομηχανία και τη βιομηχανία παραγωγής λογισμικού. (Overview of Openchain, 2018)

2.2.8 Quorum

Το Quorum είναι μία πλατφόρμα βασισμένη στο Ethereum με προσανατολισμό στις επιχειρήσεις και στις ανάγκες τους, την ανάπτυξη της οποίας έχει ξεκινήσει η J.P. Morgan. Σύμφωνα με την τελευταία, το Quorum είναι η ιδανική λύση για κάθε εφαρμογή βασισμένη στο blockchain που απαιτεί υψηλές ταχύτητες και μεγάλες δυνατότητες καταγραφής και επεξεργασίας συναλλαγών μεταξύ ενός κλειστού δικτύου συναλλαγών. Στοχεύει στην εξυπηρέτηση των αναγκών της βιομηχανίας της οικονομίας και των οικονομικών αλλά μπορεί να γίνει χρήση του και σε άλλους κλάδους.

Το λογισμικό αναπτύσσεται με τη συνεισφορά της J.P. Morgan αλλά και της open source κοινότητας και η χρήση του είναι δωρεάν. Με αυτό τον τρόπο η J.P. Morgan καταφέρνει να διατηρεί το λογισμικό της ενημερωμένο και ανοικτό (GPL Licence), και ταυτόχρονα η ανάπτυξη του να συνδέεται άμεσα με την ανάπτυξη του Ethereum, καθώς οι αλλαγές που γίνονται στον κώδικα – πυρήνα του Ethereum (go-ethereum) είναι πολύ μικρές και γίνονται μόνο στα πλαίσια της μετατροπής του ανοικτού δικτύου σε ένα ιδιωτικό blockchain στοχευμένο σε καθαρά επιχειρηματικές ανάγκες. (Quorum: Advancing Blockchain Technology, 2018)

Εικόνα 14 - Το λογότυπο της πλατφόρμας Quorum [jpmorgan.com]

Βασικά πλεονεκτήματα της υλοποίησης αυτής είναι ότι η Quorum καταφέρνει να επιτυγχάνει πολύ μεγάλες ταχύτητες επικύρωσης των συναλλαγών που καταγράφονται σε αυτό, αξιοποιώντας πλήρως τα πλεονεκτήματα της διατηρησιμότητας και της κρυπτογράφησης του blockchain, και ταυτόχρονα εξασφαλίζοντας ότι οι συναλλαγές διατηρούνται ιδιωτικές χάρη στην αρχιτεκτονική της πλατφόρμας. Για τη δημιουργία του κάθε block χρησιμοποιείται ένα μοντέλο πλειοψηφίας, όπου βασισμένο στη λογική του Proof of Stake, ένας εκ των χρηστών που έχουν δικαίωμα επικύρωσης των συναλλαγών αναλαμβάνει να δημιουργήσει και να υπογράψει την εγκυρότητα του κάθε block. (Quorum: Ethereum for Enterprise Applications, 2017)

2.2.9 IOTA

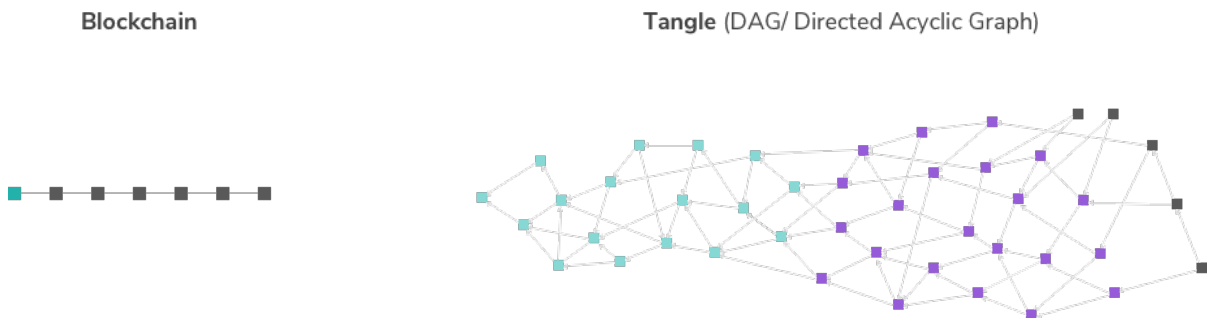
Το IOTA αποτελεί μία διαφορετική προσέγγιση χρήσης του blockchain για την καταγραφή συναλλαγών, καθώς η λογική στην οποία βασίζεται για τη λειτουργία του είναι διαφορετική από την «κλασσική» λειτουργία του blockchain που περιλαμβάνει την καταγραφή συναλλαγών σε blocks και την σύνδεση αυτών μεταξύ τους για τη δημιουργία μίας αλυσίδας που κοινοποιείται στο σύνολο των συμμετεχόντων. Οι συναλλαγές στο IOTA καταγράφονται σε μία διαφορετική προσέγγιση, το Tangle, το οποίο είναι ένα διαφορετικής αρχιτεκτονικής δημόσιο κατάστιχο συναλλαγών, στο οποίο δεν είναι απαραίτητη η δημιουργία blocks. (What is IOTA?, 2018)

Εικόνα 15 - Το λογότυπο του IOTA [iota.org]

Το Tangle είναι ένα σύνολο ανεξάρτητων μοναδικών συναλλαγών οι οποίες καταγράφονται σε ένα προσανατολισμένο ακυκλικό γράφο (DAG – Directed Acyclic Graph), όπου για να προστεθεί μία συναλλαγή απαιτείται μία μικρή ποσότητα υπολογιστικής εργασίας με την οποία ο κάθε χρήστης επικυρώνει δύο ανεπικύρωτες μέχρι εκείνη τη στιγμή συναλλαγές. Με

αυτό τον τρόπο λειτουργίας, δεν απαιτείται από το δίκτυο να έχει ιεραρχία ρόλων και ευθυνών, καθώς όλοι οι χρήστες έχουν κοινό κίνητρο να επικυρώσουν δύο συναλλαγές προσθέτοντας τη δική τους, ώστε κάποιος άλλος χρήστης να επικυρώσει στη συνέχεια τη νεότερη συναλλαγή με κάποια μεταγενέστερη. Με αυτό το σύστημα συναλλαγών «pay-it-forward» το IOTA δεν περιλαμβάνει στη λειτουργία του προσφορά οικονομικών ανταμοιβών. Η δομή αυτή επιτρέπει, επιπλέον, την υψηλή επεκτασιμότητα των συναλλαγών, καθώς όσο περισσότερη δραστηριότητα υπάρχει στο Tangle, τόσο μεγαλύτερες είναι οι ταχύτητες επικύρωσης των συναλλαγών. (Popov, 2018)

Η δομή του Tangle σε σχέση με το blockchain φαίνεται στην ακόλουθη εικόνα.



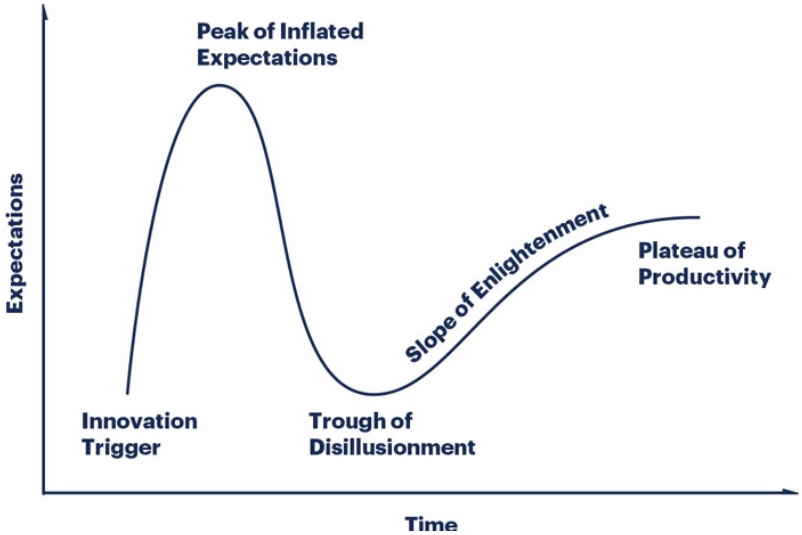
Εικόνα 16 - Η δομή του δικτύου συναλλαγών Tangle [iota.org]

Επισκόπηση δυνατοτήτων της τεχνολογίας blockchain και εφαρμογές state-of-the-art στην υγεία και άλλους τεχνολογικούς κλάδους.

3 Τομείς εφαρμογής και διαδεδομένες εφαρμογές

3.1 Τάσεις της τεχνολογίας στην παγκόσμια αγορά

Το blockchain τα τελευταία χρόνια έχει περάσει από πολλά στάδια και έχει γνωρίσει μια ιδιαίτερη δημοσιότητα, κυρίως χάρη στο Bitcoin και τα υπόλοιπα κρυπτονομίσματα που ανταλλάσσονται μεταξύ χρηστών σε τεράστιες ποσότητες καθημερινά μέσω των αντίστοιχων διαδικτυακών εφαρμογών. Εκτός όμως από τη χρήση του στην οικονομία των κρυπτονομισμάτων, ολοένα και περισσότεροι κλάδοι εντοπίζουν πλεονεκτήματα της χρήσης του blockchain σε εφαρμογές σε λειτουργίες που εκτελούνται καθημερινά και χρειάζονται τον αδιάβλητο και κοινόχρηστο χαρακτήρα του blockchain.



Εικόνα 17 - Ο κύκλος δημοσιότητας αναδυόμενων τεχνολογιών της Gartner [gartner.com]

Οι Hype Cycles της Gartner είναι η πρώτη και κυριότερη απεικόνιση των τάσεων της τεχνολογίας στην παγκόσμια αγορά. Σύμφωνα με την Gartner, κάθε τεχνολογία περνάει πέντε στάδια εξέλιξης από την αρχική εμφάνιση της ως καινοτομίας έως την πλήρως παραγωγική αξιοποίηση της. (Gartner Hype Cycle - Interpreting technology hype, 2018) Τα στάδια αυτά είναι:

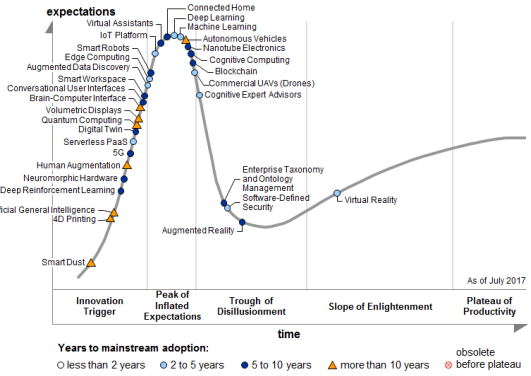
1. Innovation Trigger - Εμφάνιση καινοτομίας (πυροδότηση κύκλου)
2. Peak of Inflated Expectations - Κορύφωση προσδοκιών
3. Through of Disillusionment - Περίοδος απογοήτευσης
4. Slope of Enlightenment – Περίοδος του διαφωτισμού
5. Plateau of Productivity – Παραγωγική αξιοποίηση

Σύμφωνα με την Gartner, και τον Hype Cycle for Emerging Technologies, το blockchain τον Ιούλιο του 2016 μόλις είχε ξεπεράσει τα στάδια του Innovation Trigger, αν και ως τεχνολογία

ήταν γνωστή ήδη από το Satoshi Nakamoto[2] και το Bitcoin που πρωτοεμφανίστηκαν το 2008. Μόλις ένα χρόνο μετά, τον Ιούλιο του 2017, πλησίαζε το τέλος του σταδίου των προσδοκιών, με μία εκτίμηση ότι χρειάζεται ακόμη 5-10 έτη για να προχωρήσει στην ευρεία αποδοχή και τη χρήση σε παραγωγικές εφαρμογές.

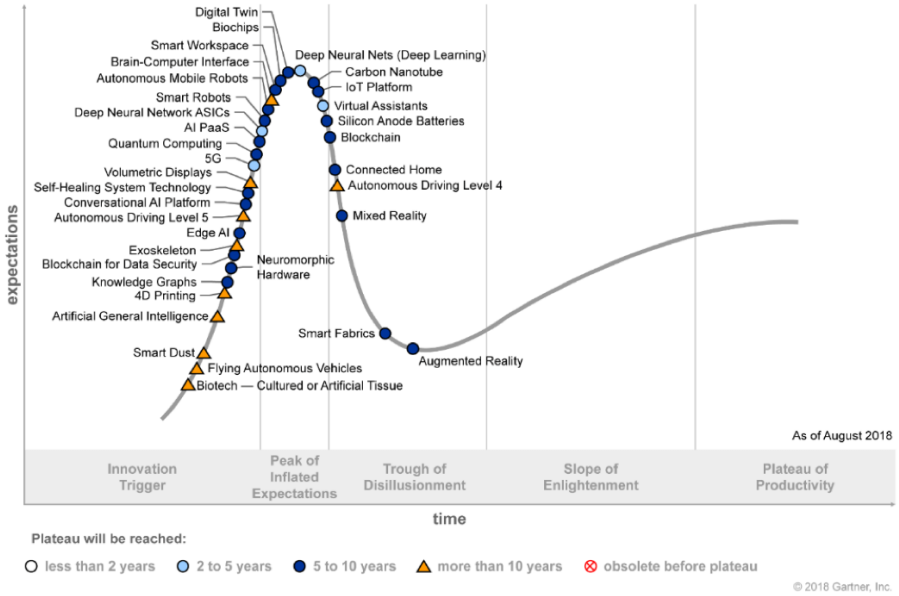
Τα αντίστοιχα γραφήματα παρατίθενται στις ακόλουθες εικόνες:

Εικόνα 18 - Gartner's Hype Cycle 2016 [Gartner.com]



Εικόνα 19 - Gartner's Hype Cycle 2017 [Gartner.com]

Σύμφωνα με το Gartner Hype Cycle for Emerging Technologies που δημοσιεύτηκε τον Αύγουστο του 2018, το blockchain κάνει τα πρώτα του βήματα στην περίοδο της απογοήτευσης, ενώ παραμένει μία τεχνολογία η οποία εκτιμάται ότι χρειάζεται ακόμη 5-10 έτη για την πλήρη παραγωγική αξιοποίηση της.



Εικόνα 20 - Gartner's Hype Cycle 2018 [smartinsights.com]

[2] Ο Satoshi Nakamoto είναι ένα πρόσωπο που σχετίστηκε με την πρώτη εμφάνιση του Bitcoin και της ιδέας του blockchain για την καταγραφή οικονομικών συναλλαγών σε ένα δημόσιο κατάστιχο με τη χρήση κρυπτογράφησης δημόσιου κλειδιού και χωρίς κάποια κεντρική ρυθμιστική αρχή. Είναι άγνωστο αν πρόκειται για πραγματικό όνομα ή ψευδώνυμο, καθώς και αν αποτελεί τον μοναδικό εμπνευστή και δημιουργό της τεχνολογίας αυτής. Παρέμεινε ενεργός στην ανάπτυξη της τεχνολογίας του Bitcoin μέχρι το 2010. [Wikipedia]

Στην ίδια κατεύθυνση ακριβώς κινούνται και αναλύσεις μεγάλων συμβουλευτικών εταιριών, όπως της Deloitte, σύμφωνα με την έρευνα της οποίας το 39% της παγκόσμιας αγοράς θεωρεί ότι το blockchain είναι υπερεκτιμημένο, με τον αριθμό αυτό να ανέρχεται σε 44% για την αγορά των Ηνωμένων Πολιτειών της Αμερικής. (Deloitte, 2018)

Στην ίδια έρευνα οι αναλυτές της Deloitte εξηγούν ότι, όπως τα πρώτα αυτοκίνητα που κινούνταν με καύσιμα φαίνονταν περίεργα και υπερεκτιμημένα στο μέσο πολίτη που χρησιμοποιούσε για την μετακίνηση του όχημα κινούμενο με άλογα ή άλλα ζώα, έτσι και το blockchain έχει υιοθετηθεί σε μεγάλο βαθμό μόνο από όσους έσπευσαν να ασχοληθούν με την αγορά των κρυπτονομισμάτων και στη συνέχεια έγινε γνωστό και στο ευρύτερο κοινό της τεχνολογίας και της καινοτομίας. Και ενώ οι περιπτώσεις χρήσης του blockchain εισέρχονται δειλά στην παραγωγή σε αυτό το χρονικό σημείο, υπάρχει πληθώρα ιδεών στην αγορά, με μεγάλες επιχειρήσεις σε όλο τον κόσμο να δημιουργούν νέες περιπτώσεις χρήσης και να επενδύουν στην τεχνολογία του blockchain, είτε μόνες τους, είτε διαμορφώνοντας κοινοπραξίες.

Σύμφωνα με το Forbes, τα αμέσως επόμενα βήματα για την τεχνολογία του blockchain είναι η δημιουργία των security tokens, τα οποία θα προσελκύσουν ολοένα και περισσότερους επενδυτές συνηθισμένους στην αγορά μετοχών σε εταιρίες. Τα κρυπτονομίσματα που διατίθενται μέχρι και σήμερα στις διαδικασίες των Initial Coin Offerings (ICOs), με τις οποίες διάφορες ιδέες και εφαρμογές βασισμένες στο blockchain εκδίδουν κρυπτονομίσματα που χρησιμοποιούνται στην ίδια την πλατφόρμα για τη λειτουργία της, δεν έχουν καταφέρει να γίνουν αρκετά σημαντικά για τους επενδυτές και θα πρέπει να υιοθετηθεί ένα μοντέλο παρόμοιο με την εμπορία δικαιωμάτων και ασφαλίστρων μετοχών για να εισέλθουν πιο «μεγάλοι παίκτες» στην αγορά του blockchain.

Επιπλέον των αλλαγών στο οικονομικό και επενδυτικό μοντέλο που παρουσιάζουν οι διάφορες πλατφόρμες που βασίζονται στο blockchain, σύμφωνα με το Forbes μέσα στα επόμενα χρόνια θα γίνουν μεγάλες αλλαγές και στα επιχειρησιακά μοντέλα λειτουργίας και ανάπτυξης εφαρμογών βασισμένων στο blockchain μέσα από τη δημιουργία μεγάλων αποκεντρωμένων οικοσυστημάτων. Τα μοντέλα σχέσεων επιχειρήσεων με πελάτες και επιχειρήσεις είναι ξεπερασμένα για να μπορούν να εφαρμοστούν ως έχουν στα peer to peer δίκτυα με τους εκατοντάδες συμμετέχοντες. (Bussmann, 2018)

3.2 Τομείς εφαρμογής της τεχνολογίας blockchain

Με βάση τις προσδοκίες που έχουν ήδη δημιουργηθεί, αλλά και τις προβλέψεις της Gartner για την επόμενη 10ετία σχετικά με το διάστημα μέχρι την παραγωγική αξιοποίηση του blockchain, είναι εύκολο να αντιληφθεί κανείς ότι το blockchain είναι μια τεχνολογία για την οποία δεν έχει κατασταλάξει ακόμη πλήρως η αγορά, και ότι τα επόμενα χρόνια θα υπάρξουν πολλές προσπάθειες εφαρμογής της στον κλάδο των οικονομικών συναλλαγών αλλά και σε άλλους κλάδους που έχουν ανάγκη από την εφαρμογή των πλεονεκτημάτων της.

Οι εφαρμογές που έχουν κάνει ήδη τα πρώτα τους βήματα στο χώρο του blockchain, είτε προτείνοντας νέα συστήματα ανταλλαγής χρημάτων, είτε ενσωματώνοντας νέες λειτουργίες σε άλλους κλάδους, αδιαμφισβήτητα αποτελούν τις πρώτες προσπάθειες και δε θα πρέπει να κρίνονται ως κάτι παραπάνω από αυτό.

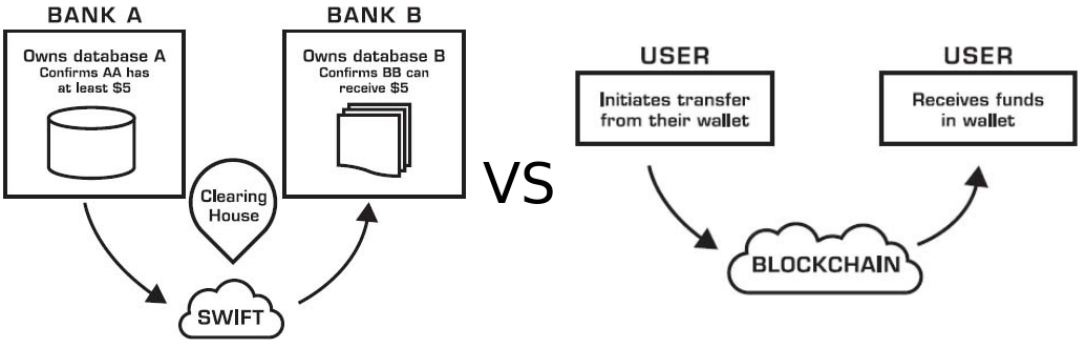
Στη συνέχεια ακολουθεί μια περιγραφή των λειτουργιών που έχουν εμφανιστεί στους πρώτους κλάδους που έχουν κάνει δοκιμές πάνω στη χρήση του blockchain για την αντικατάσταση συμβατικών τεχνολογιών ως προς ένα μέρος ή το σύνολο των λειτουργιών τους, σύμφωνα με τη λίστα του Forbes για τους εμπορικούς και βιομηχανικούς τομείς στους οποίους πρόκειται να υπάρξει διατάραξη των συνηθισμένων τεχνολογιών από τη χρήση του blockchain. (Marr, 2018)

3.2.1 Τραπεζικές συναλλαγές

Η τεχνολογία του blockchain αποτελεί βασική τεχνολογία με πολλές και υποσχόμενες προοπτικές εφαρμογής στον τραπεζικό κλάδο. Μετά την οικονομική και τραπεζική κρίση του 2008, ο τραπεζικός κλάδος αναζητά μεγάλους μετασχηματισμούς και επιδιώκει νέους τρόπους ανάπτυξης, χρησιμοποιώντας την ανάπτυξη του διαδικτύου και άλλες τεχνολογικές καινοτομίες.

Το blockchain και ο τρόπος λειτουργίας του στην καταγραφή των συναλλαγών θα μπορούσε να φέρει την επανάσταση στον τραπεζικό κλάδο και στην εκκαθάριση των πληρωμών. Η δημιουργία αποκεντρωμένων αδιάβλητων δικτύων συναλλαγών μπορεί να αυξήσει κατά πολύ την αποδοτικότητα του τραπεζικού κλάδου, διασφαλίζοντας ταυτόχρονα το αδιάβλητο των συναλλαγών και μειώνοντας την απαιτούμενη ανθρώπινη προσπάθεια για την διεκπεραίωση μιας συναλλαγής. Επιπλέον, ένα ακόμη βασικό πλεονέκτημα του blockchain είναι ότι το γεγονός ότι βασίζεται σε ένα αποκεντρωμένο δίκτυο προστατεύει τους τραπεζικούς φορείς από μία πιθανή αποτυχία ενός κεντρικού υπολογιστικού συστήματος και εγγυάται την συνέχεια της πληροφορίας με όσο το δυνατόν μεγαλύτερο ποσοστό διαθεσιμότητας.

Από την άλλη πλευρά, ο τραπεζικός κλάδος παραμένει διστακτικός στην πλήρη εφαρμογή λύσεων blockchain στις διαδικασίες του, λόγω της απουσίας κεντρικής ρυθμιστικής αρχής στο αποκεντρωμένο σύστημα καταγραφής συναλλαγών, όπως αυτό δομήθηκε και περιεγράφηκε με την πρώτη εφαρμογή του blockchain στο Bitcoin το 2008 από τον S. Nakamoto. Επιπλέον, το blockchain έχει ιδιαίτερες υπολογιστικές απαιτήσεις και για να διασφαλίζεται η ακεραιότητα του, ο τραπεζικός τομέας διατηρεί τις επιφυλάξεις του σχετικά με το αν είναι εφικτή η χρήση του blockchain σε μεγάλης κλίμακας δίκτυα συναλλαγών. (Ye Guo, 2016)
Στη συνέχεια, στην παρακάτω εικόνα φαίνεται η διαφορά ανάμεσα στην παρούσα τραπεζική λειτουργία για την διεκπεραίωση μιας συναλλαγής και στο πως αυτή θα μπορούσε να πραγματοποιηθεί με τη χρήση του blockchain. Στο αριστερό μέρος της εικόνας, η τράπεζα Α διατηρεί το λογαριασμό του προσώπου ΑΑ, ο οποίος θέλει να μεταφέρει στο πρόσωπο ΒΒ ένα ποσό στην τράπεζα Β. Η διαδικασία απαιτεί την επιβεβαίωση της διαθεσιμότητας του ποσού από την τράπεζα Α, την αποστολή σε ενδιάμεσο φορέα της διαθεσιμότητας αυτής και στη συνέχεια η τράπεζα Β λαμβάνει από τον ενδιάμεσο φορέα την επιβεβαίωση και το αντίστοιχο ποσό που πρέπει να κατατεθεί στο λογαριασμό του προσώπου Β. Με τη χρήση του blockchain, ο Α ξεκινάει μόνος του τη μεταφορά του ποσού που επιθυμεί προς τον Β. Αυτή η μεταφορά καταγράφεται στο blockchain και ανάλογα με τους κανόνες του δικτύου, όταν η συναλλαγή υπογραφεί και θεωρείται έγκυρη, ο Β λαμβάνει την αντίστοιχη αξία στο πορτοφόλι του. (Mougayar, 2016)



Εικόνα 21 – Η συμβατική μεταφορά χρημάτων και με τη χρήση blockchain [The Business Blockchain, Mougayar W., 2016]

3.2.2 Υγεία

Η υγεία αποτελεί ένα από τα μεγαλύτερα πεδία στα οποία το blockchain μπορεί να εφαρμοστεί και να βελτιώσει την καθημερινή λειτουργία τους, φέρνοντας στο επίκεντρο της τους ασθενείς και αυξάνοντας την ασφάλεια των δεδομένων των ασθενών. Η χρήση της τεχνολογίας του blockchain στην υγεία θα μπορούσε να χρησιμοποιηθεί είτε για την αποθήκευση

πληροφοριών, είτε για την παροχή συγκατάθεσης και πρόσβασης στις πληροφορίες αυτές, είτε για την ανταμοιβή των ασθενών όταν ακολουθούν ορθά μία θεραπεία ή φαρμακευτική αγωγή. (Bean, Will blockchain transform Healthcare?, 2018)

Ο τομέας της υγείας και οι πιθανές εφαρμογές του blockchain αναπτύσσονται πιο αναλυτικά στο επόμενο κεφάλαιο της παρούσας διπλωματικής εργασίας.

3.2.3 Πολιτική και διακυβέρνηση

Ένας τομέας στον οποίο η χρήση καινοτόμων λύσεων τεχνολογίας δεν είναι ιδιαίτερα διαδεδομένη είναι ο τομέας της πολιτικής και της διακυβέρνησης. Ένα από τα πιο βασικά στοιχεία των σύγχρονων δημοκρατικών κρατών είναι οι εκλογικές διαδικασίες, οπότε και οι πολίτες ή ένα υποσύνολο τους καλούνται να λάβουν μία απόφαση, είτε αυτή αφορά την εκλογή αρχών και αντιπροσώπων, είτε τη διεξαγωγή ενός δημοψηφίσματος. Πολλές από αυτές τις διαδικασίες συχνά βρίσκουν αρκετούς να αμφισβητούν τα αποτελέσματα τους και να επικαλούνται νοθεία αποτελεσμάτων ή παρατυπίες κατά την ψηφοφορία, ή ακόμη και μη προσβασιμότητα του συνόλου του εκλογικού σώματος στην εκλογική διαδικασία.

Η χρήση του blockchain σε εκλογικές διαδικασίες θα μπορούσε να διασφαλίσει στο σύνολο τους τις ψήφους και τον αδιάβλητο χαρακτήρα της ψηφοφορίας και των αποτελεσμάτων. Επιπλέον, η χρήση αποκεντρωμένων εφαρμογών θα μπορούσε να εγγυάται ότι όλοι οι συμμετέχοντες θα μπορούσαν ανά πάσα στιγμή να πιστοποιήσουν την εγκυρότητα της διαδικασίας και ταυτόχρονα να διατηρούν το δίκτυο πρακτικά αδύνατον να παραποιηθεί με οποιασδήποτε μορφής επίθεση. Ακόμη, το σύστημα ταυτοποίησης και κρυπτογράφησης διπλού κλειδιού θα μπορούσε να εξασφαλίσει την ανωνυμία των ψηφοφόρων, και ταυτόχρονα τη μοναδικότητα της ψήφου του κάθε ενός συμμετέχοντα.

Πέραν από τις εκλογικές διαδικασίες και τα συστήματα ψηφοφορίας, η τεχνολογία του blockchain θα μπορούσε να χρησιμοποιηθεί για να μειώσει ή να εξαλείψει τη γραφειοκρατία και τη διαφθορά σε πολλές κυβερνητικές υπηρεσίες. Για παράδειγμα, η πρόνοια των ατόμων με ειδικές ανάγκες και η ειδική μεταχείριση των ατόμων αυτών στα πλαίσια του κοινωνικού κράτους θα μπορούσε να γίνει αδιάβλητη αν διατηρούνταν τα στοιχεία των ατόμων αυτών σε ένα ειδικά σχεδιασμένο μητρώο.

Ένα ακόμη παράδειγμα θα μπορούσε να είναι η αυτοματοποιημένη έκδοση και υπογραφή δημοσίων εγγράφων από τον καθένα, χωρίς να απαιτούνται γραφειοκρατικές διαδικασίες και επαφή του πολίτη με κάποιο δημόσιο φορέα και το προσωπικό του, καθώς η γνησιότητα του

εγγράφου θα μπορούσε να πιστοποιείται μέσα από μία ψηφιακή υπογραφή που θα καταγράφεται σε ένα δίκτυο blockchain και θα συνδέεται με ένα αρχείο στον κρατικό φορέα. Τέλος, ένας τομέας της πολιτικής και διακυβέρνησης που θα μπορούσε να εξυπηρετήσει τις ανάγκες του μέσα από τη χρήση του blockchain είναι η προμήθεια και αποπληρωμή υπηρεσιών από άλλους φορείς ή επιχειρήσεις, καθώς και τα οικονομικά ενός κράτους ή ενός κρατικού φορέα. Πρόκειται για ένα τομέα που συνδέεται άμεσα με τα πλεονεκτήματα του blockchain στο χώρο της οικονομίας και των χρηματικών συναλλαγών. Επιπλέον το αδιάβλητο ιστορικό που διατηρείται στο blockchain διασφαλίζει την εγκυρότητα των συναλλαγών, τους συμμετέχοντες σε αυτές, καθώς και κάθε άλλη πληροφορία που πρέπει να παραμένει αδιάβλητη για τη συνέχεια του κράτους και για την διασφάλιση της διαφάνειας στις συναλλαγές του. (The Future of Government on Blockchain, 2018)

3.2.4 Αγορά ακινήτων

Σύμφωνα με τη Deloitte, ένας τομέας που θα μπορούσε να αξιοποιηθεί η τεχνολογία του blockchain είναι αυτός της αγοράς και ενοικίασης ακινήτων. Η αγορά ακινήτων παγκοσμίως έχει κάποια κοινά χαρακτηριστικά, όπως για παράδειγμα την πολυπλοκότητα των συναλλαγών μεταβίβασης ή ενοικίασης, τη διαρκή προσπάθεια ψηφιοποίησης των τίτλων ιδιοκτησίας, αλλά και την επιθυμία των συμμετεχόντων να διεξάγουν συναλλαγές γρήγορα και πολλές φορές ανώνυμα. Η χρήση του blockchain στο χώρο της παγκοσμιοποιημένης αγοράς ακινήτων θα μπορούσε να διευκολύνει σε μεγάλο βαθμό το σύνολο των διαδικασιών που απαιτούνται, από την αναζήτηση ενός ακινήτου, μέχρι την μεταβίβαση του σε κάποιον νέο ιδιοκτήτη.

Εικόνα 22

Ο κυριότερος λόγος που το blockchain θα μπορούσε να ικανοποιήσει τις ανάγκες της αγοράς ακινήτων είναι η αναγκαιότητα ύπαρξης μίας κοινής βάσης δεδομένων για το σύνολο των συναλλαγών που αφορούν τα ακίνητα. Η δυνατότητα τροποποίησης της βάσης δεδομένων αυτής από πολλούς χρήστες μπορεί να ικανοποιήσει την ανάγκη συμμετοχής πολλών ατόμων ταυτόχρονα, χωρίς ωστόσο να απαιτείται η οποιαδήποτε μεσολάβηση μεσάζοντα για την ολοκλήρωση της συναλλαγής. Τέλος, η σχεδόν στιγμιαία ολοκλήρωση των συναλλαγών και ο

αδιάβλητος χαρακτήρας της αλυσίδας αυτών μπορεί να διευκολύνει την αγορά ως προς την ταχύτητα, και ταυτόχρονα να διασφαλίσει την ελαχιστοποίηση των αμφισβητήσεων και των δικαστικών διαμαχών σχετικά με την ταυτότητα και την ιδιοκτησία των ακινήτων σε παγκόσμιο επίπεδο.

Πιο συγκεκριμένα, σύμφωνα με τη Deloitte, υπάρχουν έξι πλεονεκτήματα – ευκαιρίες χρήσης του blockchain στην αγορά ακινήτων:

1. Η βελτίωση της διαδικασίας αναζήτησης ακινήτου.
2. Διευκόλυνση των διαδικασιών προ της μίσθωσης – πώλησης με την κατάλληλη οικονομική αξιολόγηση των συμμετεχόντων
3. Διευκόλυνση των διαδικασιών της μίσθωσης και της παρακολούθησης των χρηματικών ροών
4. Καλύτερη λήψη αποφάσεων με τη χρήση δεδομένων πραγματικού χρόνου
5. Διαφανής και φθηνότερη διαχείριση τίτλων ιδιοκτησίας ακινήτων
6. Αποδοτικότερη επεξεργασία οικονομικών μεγεθών και πληρωμών

Όπως φαίνεται από τα παραπάνω πλεονεκτήματα, η βασική συνεισφορά του blockchain στην αγορά ακινήτων είναι η μείωση του χρόνου που απαιτείται για όλες τις διαδικασίες που πραγματοποιούνται στα πλαίσια του τομέα αυτού, καθώς και η διατήρηση αυτών σε ένα αδιάβλητο μηχανισμό, προσβάσιμο από όλους. (Kejriwal, 2017)

3.2.5 Νομικές υπηρεσίες

Πολλές φορές όταν γίνεται αναφορά σε μία ιδιαίτερα καινοτόμα τεχνολογία, όπως είναι το blockchain, τομείς όπως οι νομικές υπηρεσίες δεν είναι σύνηθες να αναφέρονται στους σημαντικότερους. Η χρήση του blockchain στο χώρο των νομικών υπηρεσιών μπορεί να προσφέρει στο χώρο αυτό ιδιαίτερα καινοτόμες λύσεις που θα εξασφαλίσουν τη διαφάνεια και την ταχύτερη λειτουργία του τομέα, σε όλες τις πτυχές του.

Ξεκινώντας από τη χρήση των smart contracts, είναι εύκολο να αντιληφθεί κανείς πως το blockchain μπορεί να αντικαταστήσει τα έντυπα συμβόλαια και άλλα νομικά έντυπα χάρη στις ψηφιακές υπογραφές και στον αδιάβλητο χαρακτήρα της αλυσίδας αποθήκευσης τους, μειώνοντας το χρόνο εκτέλεσης και πιστοποίησης της γνησιότητας τους και απαιτώντας λιγότερη ανθρωποπροσπάθεια.

Ακόμη, ο αδιάβλητος χαρακτήρας του blockchain ως τρόπου αποθήκευσης πληροφοριών θα μπορούσε να αξιοποιηθεί πλήρως για την καταγραφή και τήρηση αρχείου στοιχείων που σχετίζονται με νομικές υποθέσεις και ενδέχεται να χρησιμοποιηθούν σε δικαστικές διαμάχες

ή δίκες προσώπων για οποιοδήποτε ζήτημα. Το ίδιο θα μπορούσε να συμβαίνει και για τη διατήρηση του «ποινικού μητρώου» κάθε προσώπου, ώστε να μπορεί να παραμένει αδιάβλητο το ιστορικό του. Οι παραπάνω πτυχές των νομικών υπηρεσιών, βασισμένες στην τεχνολογία του blockchain, είναι εφικτό να βελτιστοποιήσουν τις διαδικασίες τους χρονικά και ταυτόχρονα να εξασφαλίσουν την απαιτούμενη διαφάνεια σε όλες τις ενέργειες του κλάδου.
Επιπλέον, ζητήματα όπως η πνευματική ιδιοκτησία και το δίκαιο της ιδιοκτησίας γενικότερα θα μπορούσαν να αξιοποιήσουν το blockchain για την κατοχύρωση δικαιωμάτων και αδειών εκμετάλλευσης πνευματικής ιδιοκτησίας, κατοχύρωσης και εκχώρησης δικαιωμάτων χρήσης πατεντών, αλλά και το σύνολο των χρηματικών ή άλλου είδους συναλλαγών που πραγματοποιούνται στα πλαίσια των παραπάνω δράσεων. Τέλος, όπως αναφέρεται πιο αναλυτικά και στην προηγούμενη παράγραφο, εκτός από τα δικαιώματα και τη μεταβίβαση άυλων στοιχείων, το blockchain μπορεί να χρησιμοποιηθεί και για τη μεταβίβαση τίτλων ιδιοκτησίας ακινήτων, διευκολύνοντας τη λειτουργία του τομέα των συμβολαιογράφων αλλά και προλαμβάνοντας διαμάχες. (DeMuro, 2018)

3.2.6 Ενοικιάσεις και διαμοιρασμός διαδρομών

Ένας κλάδος που έχει γνωρίσει πρόσφατα ιδιαίτερα μεγάλη ανάπτυξη και έγινε ιδιαίτερα δημοφιλής με την εφαρμογή μίσθωσης διαδρομών της Uber, φαίνεται ότι μπορεί να αξιοποιήσει την τεχνολογία του blockchain για την δημιουργία peer-to-peer δικτύων, τα οποία θα εξυπηρετούν την ανάγκη της μίσθωσης αυτοκινήτων για διαδρομές ή της κοινής χρήσης αυτοκινήτων (car pooling). (Decentralized Car Sharing Platform Aims to Lead the Blockchain-based Rental Market, 2018)
Ταυτόχρονα, με την ίδια λογική με το Uber λειτουργεί και η μίσθωση των ακινήτων μέσω της πλατφόρμας της Airbnb, στην οποία ιδιώτες από όλο τον κόσμο μπορούν και μισθώνουν ολόκληρα ακίνητα ή δωμάτια σε άλλους. Η δημιουργία peer-to-peer δικτύων θα μπορούσε να είναι και σε αυτό τον τομέα εφικτή, και να αποφεύγεται η οποιαδήποτε διαμεσολάβηση κάποιας πλατφόρμας που ελέγχεται από μία ή περισσότερες εταιρίες και υπόκειται σε κάποιους συγκεκριμένους κανόνες και σε αντίστοιχα κόστη.
Η χρήση του blockchain στους κλάδους της ενοικίασης και του διαμοιρασμού, είτε αυτό αφορά κάποιο ακίνητο ή μέρος αυτού, είτε αφορά τη μίσθωση ή την κοινή χρήση ενός αυτοκινήτου, μπορεί να διαμορφώσει ένα εντελώς διαφορετικό κλάδο σε σχέση με αυτά που είναι ήδη συνηθισμένα από τους πολίτες. Η ενοικίαση οποιασδήποτε μορφής θα είναι εφικτό να καταγράφεται και να κατοχυρώνεται σε ένα δίκτυο βασισμένο στο blockchain, ενώ μέσω

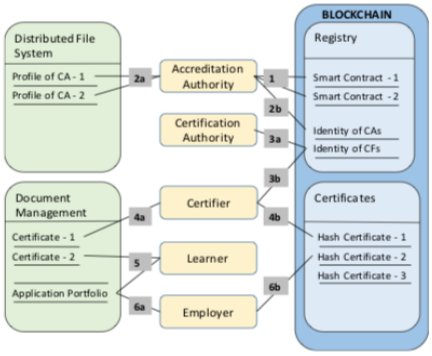
αυτού του δικτύου θα μπορούσαν να πραγματοποιούνται κάθε είδους συναλλαγές. Όπως έχει αναφερθεί και σε προηγούμενη ενότητα, στο blockchain μπορούν να καταγραφούν τόσο οι χρηματικές συναλλαγές της πληρωμής του ποσού που αντιστοιχεί στη μίσθωση ή στην κοινή χρήση, όσο και άλλου είδους συναλλαγές, όπως είναι για παράδειγμα οι ημερομηνίες της ενοικίασης, οι κριτικές για ένα χρήστη, το όχημα ή το ακίνητο του, καθώς και να χρησιμοποιηθούν ακόμη και διαφορετικές χρηματικές μονάδες μέσω της ανταλλαγής κρυπτονομισμάτων.

Αξίζει να σημειωθεί σε αυτό το σημείο ότι για τον κλάδο των ενοικιάσεων και του διαμοιρασμού ακινήτων ή οχημάτων, οι εμπλεκόμενοι στις συναλλαγές επιθυμούν σε κάθε περίπτωση την εξασφάλιση μιας αδιάβλητης και απόλυτα ακέραιας συναλλαγής, ενώ οι ρυθμιστικές αρχές της κάθε χώρας από την πλευρά τους επιθυμούν την πλήρη διαφάνεια και την διατήρηση των δεδομένων των συναλλαγών αυτών, είτε για φορολογικούς, είτε για άλλους λόγους που αφορούν στο δίκαιο της χώρας. Το blockchain μπορεί να εξασφαλίσει τις παραπάνω ανάγκες και ταυτόχρονα να μην απαιτείται η ύπαρξη ενδιάμεσων φορέων ή εταιριών που να λειτουργούν ελεγκτικά ή διαμεσολαβητικά στις συναλλαγές αυτές, απελευθερώνοντας σε ακόμη μεγαλύτερο βαθμό την αγορά αυτή αλλά και το σύνολο της αποκεντρωμένης οικονομίας. (Hil, 2018)

3.2.7 Εκπαίδευση

Όσο η δύναμη της online και της εξ' αποστάσεως εκπαίδευσης μεγαλώνει και οι εναλλακτικοί τρόποι εκπαίδευσης υιοθετούνται από ολοένα και περισσότερους ανθρώπους σε όλο τον κόσμο, η ανάγκη για την ύπαρξη ενός ανεξάρτητου τρόπου επικύρωσης της εκπαίδευσης ενός μαθητευόμενου και της διατήρησης ενός ακαδημαϊκού μητρώου γίνεται μεγαλύτερη.

Οι τίτλοι σπουδών αποτελούν μία από τις σημαντικότερες πτυχές της εκπαίδευσης και η γνησιότητα τους είναι ένα σημαντικό στοιχείο για εταιρίες και οργανισμούς κατά την πρόσληψη ή την πιστοποίηση των ικανοτήτων των εργαζομένων τους. Για το λόγο αυτό είναι ιδιαίτερα σημαντικό να διατηρείται το σύνολο των τίτλων σπουδών και των πιστοποιητικών εκπαίδευσης ενός ατόμου σε ένα «Διαβατήριο Εκπαίδευσης», το οποίο θα συνοδεύει τον κάθε άνθρωπο καθ' όλη τη διάρκεια της ζωής του.



Εικόνα 23 - Ο σχεδιασμός του Διαβατηρίου Εκπαίδευσης (Gräther et. al., 2018)

Με τη χρήση του blockchain η δημιουργία ενός τέτοιου διαβατηρίου είναι εφικτή και μπορεί να συνδυάσει αρκετά πλεονεκτήματα της τεχνολογίας αυτής με τα χαρακτηριστικά που θα πρέπει να έχει ένα τέτοιο διαβατήριο, όπως είναι η εξασφάλιση της αυθεντικότητας των πιστοποιητικών, της ταυτότητας των προσώπων που τα έχουν στην κατοχή τους και η αδιάβλητη πορεία της εξέλιξης της εκπαίδευσης του κάθε ατόμου στο χρόνο. Οι Gräther et.al. το 2018, στη δημοσίευση τους με τίτλο "Blockchain for Education: Lifelong Learning Passport" περιγράφουν αναλυτικά την υλοποίηση μιας τέτοιας εφαρμογής και καταλήγουν στο συμπέρασμα ότι τα έντυπα που εκδίδονται κατά την απόκτηση ενός τίτλου σπουδών ή μιας πιστοποίησης θα μπορούσαν να αντικατασταθούν πλήρως στο μέλλον με τη χρήση παρόμοιων υλοποιήσεων με την προτεινόμενη υλοποίηση που παρουσιάζουν στο σχετικό paper, καθώς καταπολεμούνται με αυτό τον τρόπο χρόνια ζητήματα ασφαλείας και παραχάραξης πιστοποιητικών, καθώς και η διαρκής διαθεσιμότητα τους μεταξύ του συνόλου των ενδιαφερομένων μερών. (Gräther, 2018)

Ένα εξίσου σημαντικό ζήτημα για την εκπαιδευτική και ακαδημαϊκή κοινότητα είναι η διαχείριση των δικαιωμάτων πνευματικής ιδιοκτησίας, καθώς και των αναδημοσιεύσεων βιβλίων, δημοσιεύσεων ή ερευνητικών αποτελεσμάτων. Επιπλέον, ιδιαίτερα σημαντική πολλές φορές είναι και η διασφάλιση της περιορισμένης πρόσβασης σε εκδόσεις και δημοσιεύσεις και σε άλλους ερευνητικούς ή ακαδημαϊκούς πόρους. Η χρήση του blockchain για λόγους ασφάλειας της πληροφορίας και διασφάλισης της πνευματικής ιδιοκτησίας της έρευνας θα μπορούσε να αποτελέσει ένα σημαντικό βήμα στην εξασφάλιση της σωστής διάχυσης της γνώσης. (Ark, 2018)

3.2.8 Φιλανθρωπικοί οργανισμοί

Πολλοί άνθρωποι στις μέρες μας θέλουν να προχωρήσουν σε φιλανθρωπικές δραστηριότητες και να κάνουν δωρεές σε μεγάλους ή μικρότερους φιλανθρωπικούς οργανισμούς, χωρίς ωστόσο να νιώθουν ασφαλείς και απόλυτα σίγουροι ότι τα χρήματα που θα προσφέρουν θα καταλήξουν στον πραγματικό σκοπό για τον οποίο τα προσέφεραν.

Σύμφωνα με την Changelly, μία εταιρία που δραστηριοποιείται στην ανάπτυξη μιας πλατφόρμας διαχείρισης δωρεών βασισμένης στο blockchain, η διαφθορά που εμφανίζεται σε πολλούς φιλανθρωπικούς οργανισμούς και λειτουργεί αποτρεπτικά προς τους δωρητές, μπορεί να καταπολεμηθεί μέσω της απόλυτης διαφάνειας και των αδιάβλητων συναλλαγών που μπορεί να εξασφαλίσει η χρήση του blockchain σε κάθε μορφής διακίνηση χρημάτων ή αγαθών. Το βασικό πλεονέκτημα του blockchain είναι ότι τα δεδομένα των συναλλαγών είναι

διαθέσιμα στο σύνολο των συμμετεχόντων στο δίκτυο και ταυτόχρονα τα δεδομένα αυτά δεν μπορούν να τροποποιηθούν μετά την οριστική υπογραφή τους από το peer to peer δίκτυο. Κατ' αυτό τον τρόπο οι ενδιαφερόμενοι μπορούν να λειτουργούν ελεγκτικά προς τους φιλανθρωπικούς φορείς και να επιβεβαιώνουν την ακεραιότητα των συναλλαγών τους και την επίτευξη του αρχικού στόχου τους.

Επίσης, με τη χρήση του blockchain, οι μη κερδοσκοπικοί οργανισμοί που αναλαμβάνουν το ρόλο του ενδιάμεσου μεταξύ δωρητών και παραληπτών μπορούν να μειώσουν τα έξοδα για τα λογιστικά και τα φορολογικά τους, καθώς τα οικονομικά τους στοιχεία είναι κάθε στιγμή διαθέσιμα σε οποιοδήποτε ελεγκτικό φορέα.

Ένα εμπόδιο που συναντάται, ωστόσο, στη χρήση του blockchain και των κρυπτονομισμάτων από πολλούς φιλανθρωπικούς φορείς είναι ότι – παρά το ξέσπασμα της αγοράς στα τέλη του 2017 – οι άνθρωποι δεν έχουν υιοθετήσει τα κρυπτονομίσματα και παραμένουν δύσπιστοι σχετικά με τη χρήση τους στην καθημερινότητα τους. Επιπλέον, πολλές φορές δεν είναι εύκολη η απόκτηση κρυπτονομισμάτων από τα ανταλλακτήρια που υπάρχουν ήδη και γενικότερα ο τρόπος λειτουργίας των συναλλαγών αυτών είναι σχετικά «ξένος» προς το μέσο άνθρωπο. Ακόμη, το γεγονός ότι δεν υπάρχει ρυθμιστικό πλαίσιο σε πολλές χώρες του κόσμου σχετικά με τη λειτουργία ανταλλακτηρίων κρυπτονομισμάτων, καταγραφής των συναλλαγών ή και φορολογίας των κεφαλαίων που κινούνται μέσω διαφόρων κρυπτονομισμάτων δημιουργεί ανησυχίες στους πολίτες σχετικά με τη νομιμότητα της δραστηριότητας αυτής. (Charitable Crypto: Making the World a Better Place with Blockchain, 2018)

3.2.9 Ασφάλεια

Η βασική προτεραιότητα του blockchain είναι να δημιουργήσει αποκεντρωμένους και απόλυτα ασφαλείς τρόπους καταγραφής, αποθήκευσης και κρυπτογράφησης δεδομένων. Με βάση αυτά τα χαρακτηριστικά της τεχνολογίας του blockchain, ο τομέας της ασφάλειας σε πολλούς κλάδους αναμένεται να στραφεί στη χρήση της, με σκοπό να δημιουργήσει σχεδόν απρόσβλητα από hackers δίκτυα και εφαρμογές.

Ένας τρόπος που χρησιμοποιείται το blockchain στον τομέα της ασφάλειας είναι η ταυτοποίηση χρηστών ή και συσκευών κατά τη συμμετοχή τους σε ένα δίκτυο, μία εφαρμογή, ένα υπολογιστή, ή ακόμα και σε μεγαλύτερες εγκαταστάσεις, όπως για παράδειγμα τα εργοστάσια παραγωγής ρεύματος μιας χώρας. Μέσω της χρήσης της κρυπτογραφίας που χρησιμοποιείται σε ένα δίκτυο blockchain είναι εφικτή η ταυτοποίηση μέσω ζεύγους κλειδιών (public & private keys) και η ταυτόχρονη καταγραφή των προσβάσεων αυτών χρονικά.

Σε επέκταση της παραπάνω χρήσης, μία ακόμη πιθανή εφαρμογή του blockchain, βασισμένη στον αδιάβλητο τρόπο καταγραφής των συναλλαγών σε αυτό, είναι η χρήση blockchains για την καταγραφή αλλαγών που πραγματοποιούνται σε βάσεις δεδομένων ή εφαρμογών (audit trail). Η ασφάλεια των βάσεων δεδομένων διασφαλίζεται με αυτό τον τρόπο, καθώς κάθε αλλαγή καταγράφεται στο blockchain και στη συνέχεια υπογράφεται με τα κλειδιά του χρήστη που την εκτελεί, με αποτέλεσμα να μπορούν να είναι ευκολότεροι οι έλεγχοι πλαστογραφίας ή παραχάραξης δεδομένων.

Τέλος, πέραν των καταγραφών προσβάσεων και αλλαγών, και της ταυτοποίησης χρηστών, το blockchain μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση των ίδιων των δεδομένων που αποθηκεύονται στο αποκεντρωμένο δίκτυο του, διασφαλίζοντας τη συνέχεια και την ακεραιότητα τους και διατηρώντας τα ασφαλή, καθώς κάθε κόμβος που συμμετέχει σε αυτό το δίκτυο θα διατηρεί ένα αντίγραφο αυτών και έτσι μειώνεται η πιθανότητα απώλειας ή παραχάραξης τους. (Franklin, 2018)

3.2.10 Αποθήκευση και υπολογιστική ισχύς στο Cloud

Η χρήση του blockchain στην διαχείριση υπολογιστικών πόρων σε cloud υποδομές μπορεί να πραγματοποιηθεί σε δύο μεγάλες κατηγορίες, τις αγορές αποθηκευτικού χώρου ή υπολογιστικής ισχύος και την υποδομή αποθηκευτικού χώρου ή υπολογιστικής ισχύος.

Στον τομέα των αγορών, το blockchain χρησιμοποιείται για την «ανταλλαγή» αποθηκευτικού χώρου και υπολογιστικών πόρων μεταξύ χρηστών που ενδιαφέρονται να αποκτήσουν την αντίστοιχη υπηρεσία και χρηστών που ενδιαφέρονται να διαθέσουν τις δικές τους υποδομές έναντι κάποιου αντιτίμου. Με αυτό τον τρόπο στο blockchain διατηρούνται είτε οι διαδρομές αποθήκευσης αρχείων, είτε οι συναλλαγές μεταξύ των χρηστών, είτε τα δικαιώματα πρόσβασης σε αρχεία και υπολογιστικούς πόρους. Με βάση τα στοιχεία που καταγράφονται κάθε στιγμή στο blockchain μπορούν να αποδίδονται και οι αμοιβές των χρηστών που προσφέρουν υπολογιστική ισχύ, αλλά και να ανακτώνται τα αρχεία όταν πρόκειται για υπηρεσίες αποθηκευτικού χώρου στο cloud. Βασικό χαρακτηριστικό του μηχανισμού αυτού είναι ότι τα δεδομένα δεν αποθηκεύονται στο blockchain, αλλά σε τοπικούς αποθηκευτικούς χώρους χρηστών, με αυξημένο κίνδυνο απώλειας δεδομένων των «αγοραστών» που έχουν τα δεδομένα τους στους αποθηκευτικούς χώρους τους, αν οι πρώτοι εγκαταλείψουν το δίκτυο.

Όσον αφορά τον τομέα της υποδομής αποθηκευτικού χώρου ή άλλων υπολογιστικών υποδομών, η ανάπτυξη του είναι κατά πολύ μικρότερη από αυτή της διαχείρισης συναλλαγών

μεταξύ χρηστών που προσφέρουν και χρηστών που χρειάζονται υπολογιστικούς πόρους, καθώς το blockchain από τη φύση του δεν έχει μεγάλες δυνατότητες αποθήκευσης δεδομένων με την έννοια του αποθηκευτικού χώρου αρχείων. Για να αποθηκεύονται τέτοιου είδους δεδομένα στο blockchain, οι εταιρίες που αναπτύσσουν τέτοιου είδους εφαρμογές κάνουν μεγάλες αλλαγές στην λειτουργία του blockchain, οι οποίες είναι τόσο δομικές, όσο και σε επίπεδο δικαιωμάτων πρόσβασης και μηχανισμών υπογραφής. (Lee, 2018)

3.3 Διαδεδομένες εφαρμογές

Οι εφαρμογές που έχουν αναπτυχθεί για τους τομείς που αναφέρθηκαν στην προηγούμενη ενότητα είναι πολλές και η καταγραφή του συνόλου αυτών θα ξεπερνούσε το σκοπό αυτής της διπλωματικής εργασίας. Στη συνέχεια παρουσιάζονται οι πιο γνωστές εφαρμογές που βασίζουν τη λειτουργία τους στο blockchain και προσφέρουν νέες προσεγγίσεις σε συναλλαγές και δραστηριότητες της καθημερινότητας.

3.3.1 Ripple [Τραπεζικές Συναλλαγές]

Το RippleNet, ή πιο σύντομα Ripple, όπως έχει καθιερωθεί με βάση το όνομα της εταιρίας που έχει σχεδιάσει την πλατφόρμα, είναι ένα δίκτυο εκτέλεσης γρήγορων τραπεζικών συναλλαγών χωρίς γεωγραφικούς ή άλλους οικονομικούς περιορισμούς. Σύμφωνα με τη McKinsey, το 2016 πραγματοποιήθηκαν μόνο μεταξύ επιχειρήσεων διασυνοριακές τραπεζικές συναλλαγές με συνολική αξία 135 τρισεκατομμυρίων Δολαρίων ΗΠΑ. (Global Payments 2016: Strong Fundamentals Despite Uncertain Times, 2016). Στοχεύοντας να καλύψει την ανάγκη για γρήγορες και αδιάβλητες συναλλαγές, η Ripple προσφέρει ένα αποκεντρωμένο ιδιωτικό δίκτυο συναλλαγών το οποίο απευθύνεται σε τράπεζες και άλλους παρόχους υπηρεσιών μεταφοράς χρημάτων με στόχο την διεκπεραίωση των συναλλαγών αυτών εύκολα και γρήγορα. Το δίκτυο αυτό έχει αναπτυχθεί από την ίδια την εταιρία και δε βασίζεται σε κάποια άλλη πλατφόρμα ανάπτυξης εφαρμογών blockchain, ενώ ως «καύσιμο» χρησιμοποιεί το ομώνυμο νόμισμα Ripple (XRP).

Εικόνα 24 - Το λογότυπο της εταιρίας Ripple [ripple.com]

Το Ripple ως δίκτυο, σε σχέση με άλλα δίκτυα κρυπτονομισμάτων προσφέρει πολύ μικρότερους χρόνους ταυτοποίησης συναλλαγών, οι οποίοι σύμφωνα με την επίσημη ιστοσελίδα της εταιρίας ανέρχονται σε μόλις 4 δευτερόλεπτα, σε αντίθεση, για παράδειγμα, με το Ethereum που δημιουργεί ένα block ανά δύο λεπτά και είναι ασύγκριτα πιο γρήγορο από

τις παραδοσιακές διεθνείς μεταφορές χρημάτων που χρειάζονται 3 έως 5 εργάσιμες ημέρες. Επιπλέον, η αρχιτεκτονική του του επιτρέπει να είναι επεκτάσιμο και να μπορεί να ικανοποιεί πολύ μεγάλους αριθμούς συναλλαγών, με αποτέλεσμα να μην παραμένουν συναλλαγές στην αναμονή για την υπογραφή των αντίστοιχων blocks και την ταυτοποίηση – κοινοποίηση τους στο υπόλοιπο δίκτυο. Σύμφωνα με τους δημιουργούς του, το Ripple μπορεί να επεκταθεί και να ικανοποιήσει τον ίδιο αριθμό συναλλαγών με τις συναλλαγές του διεθνούς οργανισμού διαχείρισης καρτών VISA, οι οποίες ανέρχονται σε περίπου 50 χιλιάδες το δευτερόλεπτο. Τέλος, οι συναλλαγές που εκτελούνται στο δίκτυο του Ripple είναι ιδιαίτερα φτηνές, καθώς κοστίζουν κατά μέσο όρο 0,0001 σεντς του Δολαρίου των ΗΠΑ, ανεξαρτήτως ποσού που διακινείται.

Μέχρι το τέλος του 2018, το Ripple έχει υιοθετηθεί από μεγάλους τραπεζικούς οργανισμούς, όπως είναι η Santander, η Standard Chartered, η MoneyGram και η American Express, ενώ έχει εξασφαλίσει στήριξη και χρηματοδότηση από μεγάλες εταιρίες πληροφορικής όπως η Accenture και η Seagate, αλλά και Venture Capitals όπως το Google ventures, η Core Innovation Capital και η CME Ventures. (Ripple.com, 2019)

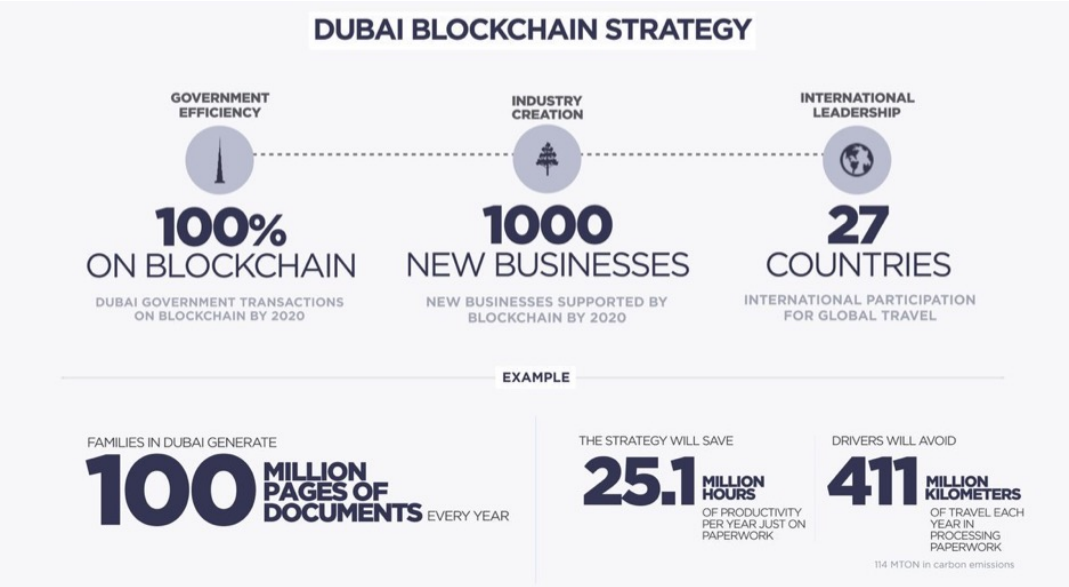
3.3.2 Smart Dubai Blockchain [Πολιτική και Διακυβέρνηση]

Σύμφωνα με τη στρατηγική ανάπτυξης του Dubai στα Ηνωμένα Αραβικά Εμιράτα, η πόλη του Dubai στοχεύει να είναι η πρώτη πόλη που θα λειτουργεί πλήρως βασισμένη στο blockchain μέχρι το 2020. Ο βασικός στόχος της πόλης στην προσπάθεια αυτή είναι να αποτελέσει τον τεχνολογικό πυρήνα της νέας δεκαετίας, διατηρώντας ταυτόχρονα τους κατοίκους της σε υψηλά επίπεδα ευχαρίστησης και ικανοποίησης στις συναλλαγές τους εντός του Dubai. Μεταξύ των υπηρεσιών αυτών είναι η διαχείριση της ενεργειακής κατανάλωσης του Dubai ως έξυπνης πόλης, η διαχείριση των οικονομικών του κράτους, η διασφάλιση της διαφάνειας σε διαγωνισμούς που απευθύνονται σε προμηθευτές, καθώς και η ψηφιακή υπογραφή των πολιτών η οποία επιτυγχάνεται μέσω της ταυτοποίησης τους από τον αριθμό του κινητού τηλεφώνου τους.

Με τη χρήση του blockchain το Dubai εξασφαλίζει την απεξάρτηση του από τα έντυπα δημόσια έγγραφα, εξοικονομώντας ταυτόχρονα 5,5 δισεκατομμύρια dirham ετησίως. Η πιλοτική εφαρμογή του προγράμματος αντικατάστασης των εντύπων δημοσίων εγγράφων με ψηφιακά έχει παρουσιάσει ιδιαίτερα θετικά αποτελέσματα, με τη μείωση κατανάλωσης χαρτιού να φτάνει στο 57% για τις έξι κρατικές υπηρεσίες που εντάχθηκαν πιλοτικά στην

πρωτοβουλία απαλοιφής των έντυπων εγγράφων. (Dubai Paperless Strategy Completes Phase One, 2019)

Επιπλέον, εκτός της εξοικονόμησης χαρτιού και της μείωσης των συναλλαγών μεταξύ πολιτών και κρατικών υπηρεσιών που απαιτούν τη χρήση εγγράφων, το Dubai, βασισμένο σε ένα σύνολο τεχνολογικών καινοτομιών όπως είναι το blockchain έχει καταφέρει να ενοποιήσει πάνω από 20 διαφορετικές κρατικές υπηρεσίες στον τομέα της ταυτοποίησης των πολιτών και της καταγραφής των συναλλαγών των πολιτών. Η λειτουργία της πλατφόρμας έχει ξεκινήσει από το φθινόπωρο του 2018, με ιδιαίτερα θετικά αποτελέσματα. Ενδεικτικά αξίζει να αναφερθεί ότι οι διαδικασίες συμβιβασμού ή πληρωμής οφειλών προς το κράτος μειώθηκε από τις 45 μέρες σε σχεδόν μηδενικό χρόνο με τις συναλλαγές να πραγματοποιούνται και να πιστοποιούνται σε πραγματικό χρόνο. (Smart Dubai launches blockchain - powered system, 2018)



Εικόνα 25 - Η στρατηγική του Dubai για το blockchain σε νούμερα [xstrategy.ae]

3.3.3 Ubitquity [Αγορά Ακινήτων]

Εικόνα 26 - Το λογότυπο της Ubitquity [ubitquity.io]

Η Ubitquity είναι μία εταιρία που ιδρύθηκε το 2015 στις Ηνωμένες Πολιτείες της Αμερικής με στόχο τη δημιουργία μιας πλατφόρμας στην οποία θα μπορούν να καταγράφονται με ασφάλεια οι τίτλοι ιδιοκτησίας ακινήτων καθώς και οι συναλλαγές που σχετίζονται με αυτούς. Η πλατφόρμα που έχει δημιουργηθεί προσφέρεται με τη μορφή Software – as – a – Service (SaaS) και βοηθά τους πελάτες της εταιρίας να διατηρούν πλήρη και ενημερωμένα μητρώα ιδιοκτησίας ακινήτων, μειώνοντας το χρόνο που απαιτείται

για την αναζήτηση των σχετικών εγγράφων και αυξάνοντας την εμπιστοσύνη και τη διαφάνεια χάρη στη χρήση της τεχνολογίας του blockchain.

Βασίζεται σε τεχνολογία blockchain που έχει αναπτυχθεί αποκλειστικά από την Ubitquity, την unanimity, η οποία επιτρέπει την ενσωμάτωση των λειτουργιών του blockchain σε ήδη υπάρχουσες εφαρμογές χωρίς να απαιτείται η χρήση κρυπτονομισμάτων και πολύπλοκες διασυνδέσεις. Πέραν της διατήρησης των συναλλαγών και των σχετικών smart contracts, στο δίκτυο της εφαρμογής διατηρούνται και έγγραφα, τα οποία κατανέμονται κρυπτογραφημένα σε ένα peer-to-peer storage. Η ανάπτυξη της λύσης unanimity δεν περιορίζεται σε ένα τύπο blockchain, καθώς μπορεί να συνεργάζεται τόσο με ιδιωτικά όσο και με δημόσια δίκτυα, ενώ είναι συμβατή ακόμη και με υβριδικά δίκτυα στα οποία υπάρχουν πολλαπλές προσβάσεις και ελέγχονται από μία κεντρική ρυθμιστική αρχή. (UBITQUITY, 2019)

3.3.4 OpenLaw [Νομικές Υπηρεσίες]

Η OpenLaw είναι μια εφαρμογή με άμεση εφαρμογή στις πτυχές του τομέα των νομικών υπηρεσιών που έχουν σχέση με συμβόλαια ή άλλα σύμφωνα. Με τη χρήση των smart contracts έχει δημιουργήσει μια δική της μορφή markup γλώσσας, η οποία είναι ικανή να αποτυπώσει στο blockchain οποιοδήποτε νομικό έγγραφο, διατηρώντας το αμετάβλητο και καταγράφοντας τη χρονική στιγμή της καταχώρησης του. Ταυτόχρονα, τα διαχειριστικά κόστη μειώνονται και μαζί με αυτά μειώνονται και οι πιθανότητες παραχάραξης των συμφώνων ή αμφισβήτησης του περιεχομένου τους από οποιοδήποτε συμβαλλόμενο μέρος.

Εικόνα 27 - Το λογότυπο της OpenLaw [openlaw.io]

Ο κύκλος ζωής ενός συμφώνου ή συμβολαίου στην πλατφόρμα του OpenLaw ξεκινά με ένα πρότυπο το οποίο βασίζεται στην markup γλώσσα της εφαρμογής. Το πρότυπο αυτό έχει το μεγαλύτερο μέρος του κειμένου προσυμπληρωμένο, ενώ ο χρήστης της εφαρμογής χρειάζεται να συμπληρώσει μόνο τα στοιχεία που καθιστούν το συμβόλαιο μοναδικό. Αν οποιαδήποτε στιγμή ο χρήστης διακόψει την καταχώρηση των στοιχείων, αυτό διατηρείται στην εφαρμογή σε πρόχειρη μορφή και παραμένει εκεί μέχρι την ολοκλήρωση της συμπλήρωσης του. Όταν όλα τα πεδία έχουν συμπληρωθεί, τότε το πρόχειρο μετατρέπεται σε smart contract, το οποίο

αποστέλλεται στους συμβαλλόμενους για υπογραφές και μετά την υπογραφή του καταγράφεται στο blockchain του Ethereum, θέτοντας το συμβόλαιο σε ισχύ και προχωρώντας στην έναρξη τυχόν διαδικασιών που έχουν καταγραφεί στην εφαρμογή ως επόμενες ενέργειες. Η εταιρία OpenLaw έχει ήδη διαμορφώσει αρκετά νομικά κείμενα στη μορφή της markup γλώσσας και στην ιστοσελίδα της αναφέρει ότι αυτά ανέρχονται μέχρι τη στιγμή συγγραφής της παρούσας εργασίας σε κάποιες δεκάδες χιλιάδες. Βασίζεται σε διεθνείς πηγές συλλογής νομικών εγγράφων, όπως είναι το LawInsider.com, ενώ σημαντικό ρόλο διαδραματίζουν και όσοι τη χρησιμοποιούν ήδη, καθώς συμμετέχουν στον έλεγχο των κειμένων και επιστρέφουν στην εταιρία σχόλια σχετικά με τα κείμενα και τις ψηφιοποιημένες εκδοχές τους με την OpenLaw Markup γλώσσα. (OpenLaw Docs, 2019)

3.3.5 Yantha [Διαμοιρασμός Διαδρομών]

Η Yantha είναι μία πλατφόρμα διαμοιρασμού διαδρομών με στόχο την κοινή χρήση αυτοκινήτων από πολλούς ανθρώπους για την ίδια ή παραπλήσια διαδρομή. Βασίζεται στη λογική του carpooling και αποτελεί μια προσπάθεια να μειωθούν τα μειονεκτήματα που εμφάνιζε η πρώτη μορφή διαμοιρασμού διαδρομών, όπως για παράδειγμα η ανάγκη για διαρκή χρήση του GPS κινητών συσκευών, οι ανησυχίες των χρηστών για την κοινή χρήση προσωπικών δεδομένων τους από τις εφαρμογές, καθώς και η έλλειψη κινήτρων για την κοινή χρήση των οχημάτων. Η εφαρμογή έχει αναπτυχθεί από τους δημιουργούς της εφαρμογής PoolMyRide που δημοσιεύθηκε το 2013 και κατάφερε να έχει πάνω από 150 χιλιάδες διαδρομές carpooling ετησίως στην Ινδία.

Εικόνα 28 - Το λογότυπο της πλατφόρμας Yantha [yantha.com]

Η δεύτερη υλοποίηση που προτείνεται μέσω της Yantha ανεξαρτητοποιεί το αυτοκίνητο των χρηστών που επιθυμούν να συμμετέχουν στο πρόγραμμα κοινής χρήσης του οχήματος, καθώς λειτουργεί με τη βοήθεια μιας συσκευής που τοποθετείται στη θύρα OBD του αυτοκινήτου και ενός ασύρματου κουμπιού που μπορεί να τοποθετηθεί οπουδήποτε μέσα στο αυτοκίνητο. Η επιβράβευση του οδηγού γίνεται μέσω του mining κρυπτονομίσματος το οποίο γίνεται κατά τη διάρκεια χρήσης του αυτοκινήτου από τη συσκευή που είναι συνδεδεμένη στην θύρα OBD κατά τη διάρκεια της κοινής χρήσης του οχήματος. Το σύνολο των διαδρομών και των συναλλαγών αποθηκεύεται στο blockchain του Ethereum,

διατηρώντας ασφαλή και άμεσα προσβάσιμα τα δεδομένα της εφαρμογής μόνο από τα εμπλεκόμενα άτομα στη συναλλαγή. (Carpooling 2.0 powered by blockchain and IoT, 2018)

3.3.6 HireGo [Ενοικίαση Οχημάτων]

Εικόνα 29 - Το λογότυπο της εφαρμογής HireGo [hirego.io]

Εκτός του διαμοιρασμού διαδρομών, η ενοικίαση οχημάτων είναι ένας ακόμα τομέας που έχει κεντρίσει το ενδιαφέρον προγραμματιστών και επενδυτών στο χώρο του blockchain. Το HireGo είναι μία εφαρμογή που αποσκοπεί στην ασφαλή ενοικίαση οχημάτων που ανήκουν σε εταιρίες ή ιδιώτες μέσω της καταγραφής των συναλλαγών ενοικίασης στο Ethereum Blockchain. Μέσω της ανάπτυξης ενός DApp στο δίκτυο του Ethereum, οι χρήστες της εφαρμογής θα μπορούν χρησιμοποιώντας μία εφαρμογή στο κινητό τους τηλέφωνο να εντοπίζουν διαθέσιμα οχήματα προς ενοικίαση στην περιοχή που βρίσκονται και να προχωρούν στην άμεση ενοικίαση και χρήση αυτών, χωρίς την αναγκαιότητα ύπαρξης ενδιάμεσου και χωρίς γραφειοκρατικές διαδικασίες.
Με τη χρήση τεχνολογιών του Internet of Things, τα διασυνδεδεμένα διαθέσιμα οχήματα θα μπορούν να ξεκλειδώνουν και να ενεργοποιούνται με τη χρήση της εφαρμογής HireGo, τη στιγμή που τα χρειάζεται ο ενδιαφερόμενος και αφού ολοκληρώσει την πληρωμή. Μέσω της εφαρμογής οι χρήστες μπορούν να καταγράφουν το σύνολο των συναλλαγών που πραγματοποιούνται στο Ethereum blockchain, να κάνουν κριτικές για τα οχήματα που ενοικιάζουν, αλλά και να δέχονται κριτικές από τον ιδιοκτήτη του οχήματος.
Η εφαρμογή τη στιγμή συγγραφής της παρούσας διπλωματικής δεν διατίθεται για χρήση προς το κοινό, αλλά βρίσκεται στο στάδιο της δημόσιας δοκιμαστικής περιόδου (Public Beta). Στόχος των ιδρυτών της είναι να έχουν ολοκληρωθεί όλα τα στάδια ανάπτυξης των λειτουργιών της μέχρι το τέλος του 2019. (HireGo, 2018)

3.3.7 Blockcerts [Εκπαίδευση]

Το Blockcerts είναι ένα ανοιχτό πρότυπο για τη δημιουργία, την έκδοση, την προβολή και την υπογραφή πιστοποιητικών βασισμένο στο blockchain. Κάθε πιστοποιητικό καταγράφεται στο blockchain και η υπογραφή του κρυπτογραφείται ψηφιακά ώστε να είναι δυνατός ο διαμοιρασμός του και το περιεχόμενο του να παραμένει αναλλοίωτο. Στόχος της εφαρμογής

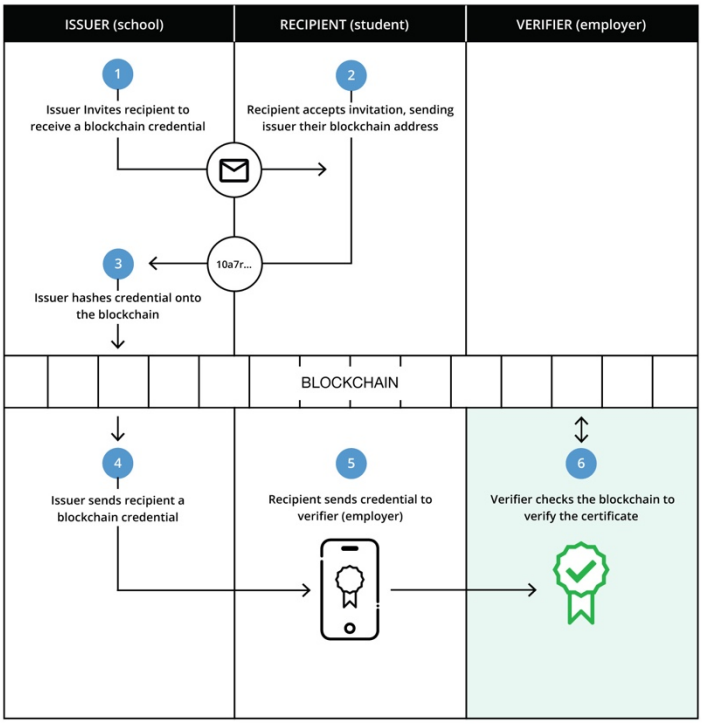
είναι να αποτελέσει μία καινοτόμα λύση μεταξύ των ανθρώπων ώστε να μπορούν να διατηρούν τα δικά τους αυθεντικά πιστοποιητικά σε μία διαχρονική βάση δεδομένων.

Ο αρχικός σχεδιασμός της εφαρμογής βασίστηκε σε πρωτότυπα που αναπτύχθηκαν στο Media Lab του MIT σε συνεργασία με τη Learning Machine, η οποία είχε ήδη αναπτύξει μία πρώτη εκδοχή της ψηφιακής υπογραφής πιστοποιητικών εκπαίδευσης. Το πρότυπο δόθηκε με τη μορφή λογισμικού ανοιχτού κώδικα και οι δύο βασικοί εμπνευστές του ενθαρρύνουν τους ενδιαφερόμενους από όλο τον κόσμο να συμμετέχουν στην εξέλιξη του. (About Blockcerts, 2019)

Η διαδικασία που ακολουθείται για την έκδοση ενός πιστοποιητικού είναι η ακόλουθη:

1. Η εκδίδουσα αρχή (Πανεπιστήμιο ή άλλος οργανισμός) προσκαλεί το χρήστη – αποδέκτη του πιστοποιητικού να δημιουργήσει ένα μοναδικό αναγνωριστικό στο blockchain.
2. Ο αποδέκτης του πιστοποιητικού αποδέχεται την πρόσκληση και δημιουργεί τον αντίστοιχο λογαριασμό, λαμβάνοντας τη μοναδική γι' αυτόν διεύθυνση.
3. Η εκδίδουσα αρχή κρυπτογραφεί το μοναδικό αναγνωριστικό και το πιστοποιητικό στο blockchain και στέλνει στον αποδέκτη το αναγνωριστικό της συναλλαγής.
4. Ο αποδέκτης μπορεί να χρησιμοποιήσει το αναγνωριστικό της συναλλαγής με οποιοδήποτε τρόπο θέλει, όπως για παράδειγμα να το στείλει σε μία εταιρία ως πιστοποίηση των γνώσεων του.
5. Η εταιρία ή ο τελικός παραλήπτης μπορεί να επιβεβαιώσει με τη συναλλαγή ότι το πιστοποιητικό είναι γνήσιο και ανήκει στον αποδέκτη του πιστοποιητικού.

Πάνω στο Blockcerts βασίζεται και η εμπορική εφαρμογή της Learning Machine, η οποία είναι διαθέσιμη στους χρήστες και μπορεί να διατηρήσει τα πιστοποιητικά τους, αποθηκεύοντας τα ακόμα και στο κινητό τους τηλέφωνο. (LearningMachine, 2019)



Εικόνα 30 - Η διαδικασία έκδοσης και επαλήθευσης πιστοποιητικού στο Blockcerts [blockcerts.org]

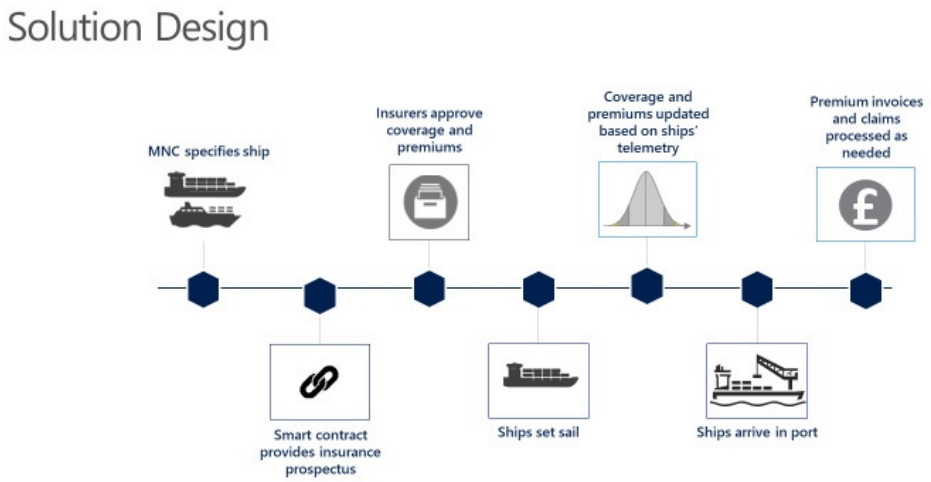
3.3.8 Insurwave [Ασφάλεια Θαλάσσιων Μεταφορών]

Σε ένα ολοένα και πιο πολύπλοκο και συνεχώς εξελισσόμενο τοπίο, όπως είναι οι θαλάσσιες μεταφορές, εταιρίες τεχνολογίας και εταιρίες του ασφαλιστικού τομέα ένωσαν τις δυνάμεις τους για τη δημιουργία του Insurwave. Στην ανάπτυξη της εφαρμογής συμμετείχαν η EY,η Guardtime, η Moller-Maersk, η Microsoft, αλλά και οι ασφαλιστικές Willis Towers Watson, XL Catlin, MS Amlin και ACORD.

Η εφαρμογή χρησιμοποιεί το blockchain και την τεχνολογία της αποκεντρωμένης αποθήκευσης του Microsoft Azure για την καταγραφή αυτοματοποιημένων συναλλαγών μεταξύ εμπορικών πλοίων. Συνδέοντας τους συμμετέχοντες σε ένα ασφαλές ιδιωτικό δίκτυο το οποίο διατηρεί πλήρες κατάστιχο των συναλλαγών και των διαδικασιών που εκτελούνται για την διεκπεραίωση τους, η πλατφόρμα αποτελεί την πρώτη εφαρμογή ψηφιακής ασφάλισης αξιών. Η Moller – Maersk συμμετείχε στην ανάπτυξη της εφαρμογής ως πιλοτικός πελάτης και συνεχίζει να τη χρησιμοποιεί παραγωγικά πλέον στο σύνολο του στόλου της.

Στόχος της εφαρμογής σύμφωνα με τον επικεφαλής του ασφαλιστικού τομέα σε παγκόσμιο επίπεδο της Ernst & Young (EY), Shaun Crawford, είναι η ολική μεταμόρφωση του τοπίου των μεταφορών και του εφοδιασμού, μειώνοντας διαρκώς τις διαδικασίες που απαιτούν την ανθρώπινη προσπάθεια και αυτοματοποιώντας το μεγαλύτερο μέρος των συναλλαγών. Πιο συγκεκριμένα, η εφαρμογή εξασφαλίζει για το σύνολο των εμπλεκόμενων μερών στις

συναλλαγές του παγκόσμιου θαλάσσιου εμπορίου χαμηλότερα διαχειριστικά κόστη και μείωση της γραφειοκρατίας που απαιτείται για την ολοκλήρωση του συνόλου των ασφαλιστικών διαδικασιών, όπως φαίνεται στην ακόλουθη εικόνα. (Ruubel, 2018)



Εικόνα 31 - Η λύση του Insurwave [customers.microsoft.com]

3.3.9 Alice [Διαχείριση Δωρεών – Φιλανθρωπικοί Οργανισμοί]

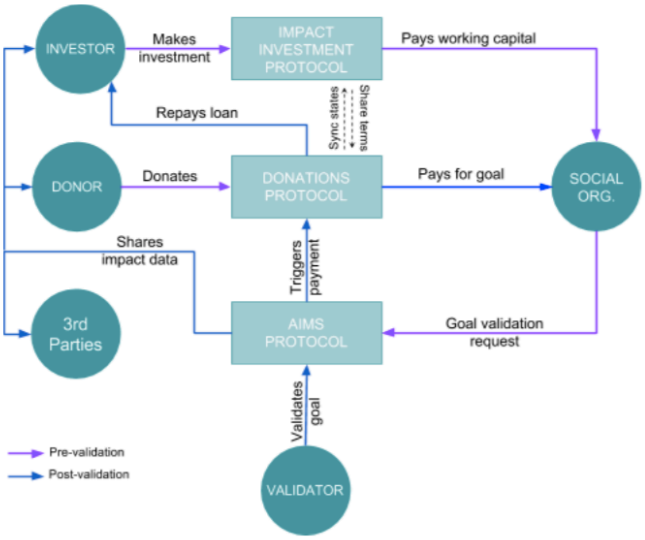
Εικόνα 32 - Το λογότυπο του Alice [alice.si]

Το Alice είναι ένα αποκεντρωμένο δίκτυο βασισμένο στο Ethereum με έντονο κοινωνικό αντίκτυπο. Βοηθάει κοινωνικούς οργανισμούς (Φιλανθρωπίες, Μη Κερδοσκοπικούς Οργανισμούς, Κοινωνικές εταιρίες κλπ.) να εκτελούν διάφορα φιλανθρωπικά έργα με απόλυτη διαφάνεια, χρησιμοποιώντας τη λογική των smart contracts του Ethereum για την καταγραφή και την εύκολη πρόσβαση του κοινού στο σύνολο των συναλλαγών που εκτελούνται στα πλαίσια της δράσης τους. Η ανάγκη για τη δημιουργία ενός τέτοιου δικτύου εντοπίστηκε από τους δημιουργούς του καθώς τα τελευταία χρόνια παρατηρείται ότι ο κόσμος έχει αποστασιοποιηθεί από τους φιλανθρωπικούς οργανισμούς και έχει χάσει την εμπιστοσύνη του προς αυτούς όσον αφορά τη διαφάνεια των δραστηριοτήτων τους.

Το Alice χρησιμοποιώντας το blockchain του Ethereum και την τεχνολογία των smart contracts, επιδιώκει να διαμορφώσει ένα διαφορετικό πρότυπο για τις φιλανθρωπικές ενέργειες, σύμφωνα με το οποίο κάθε τέτοια ενέργεια θα πρέπει να θέτει τους στόχους της από την αρχή και στη συνέχεια αυτοί να επικυρώνονται από κάποιο τρίτο. Η χρηματοδότηση των ενεργειών αυτών γίνεται μέχρι ένα αρχικό ποσό για όλους τους συμμετέχοντες στην πλατφόρμα και στη συνέχεια, μόνο αν είναι εφικτή η απόδειξη της επίτευξης των αρχικών στόχων δικαιούνται επιπλέον χρηματοδότηση. Το σύνολο των πληροφοριών για τις δράσεις,

τους στόχους και την επίτευξη αποθηκεύονται στο Ethereum και από εκεί μπορούν να ανακτηθούν και να επαληθευτούν από οποιονδήποτε το επιθυμεί. Για τη διασφάλιση της ανωνυμίας, οι συναλλαγές, οι δικαιούχοι και οι διοργανωτές των δράσεων παραμένουν εκτός του δικτύου του blockchain και κρυπτογραφούνται, έτσι ώστε μόνο διαπιστευμένοι χρήστες να μπορούν να έχουν πρόσβαση στα ευαίσθητα δεδομένα.

Εκτός από τους δωρητές, και οι επενδυτές μπορούν να επωφεληθούν από τη διαφάνεια που προσφέρει η πλατφόρμα Alice, καθώς κάθε στιγμή μπορούν να παρακολουθούν τα αποτελέσματα των διαφόρων οργανισμών στους οποίους διαθέτουν τα χρήματα τους για την κάλυψη των λειτουργικών τους εξόδων, και να αποπληρώνονται ένα μέρος του επενδυμένου κεφαλαίου τους από το πρωτόκολλο των δωρεών στο οποίο βασίζεται η εφαρμογή. (Mazet, 2017)



Εικόνα 33 - Το οικοσύστημα της πλατφόρμας Alice [alice.si]

3.3.10 Storj [Αποθηκευτικός Χώρος]

Εικόνα 34 - Το λογότυπο του Storj App [storj.io]

Το Storj είναι μία αποκεντρωμένη λύση αποθηκευτικού χώρου βασισμένη σε λογισμικό ανοικτού κώδικα και στην πλατφόρμα του Ethereum. Στόχος της πλατφόρμας είναι η δημιουργία ενός αποκεντρωμένου δικτύου διαμοιρασμού αποθηκευτικού χώρου, όπου το κόστος θα είναι μικρότερο για τους χρήστες και η ταχύτητα ανάκτησης και λήψης των αρχείων τους μεγαλύτερη από τις συμβατικές υπηρεσίες, καθώς οι τελευταίες είναι περιορισμένες ανάλογα με τις δυνατότητες των data centers τους. Επιπλέον της οικονομίας και της ταχύτητας, το Storj επιδιώκει την πλήρη ιδιωτικότητα στην πρόσβαση των αρχείων του κάθε χρήστη, καθώς χρησιμοποιεί

μεθόδους και τεχνικές κρυπτογράφησης τόσο στα αρχεία, όσο και στην αποθήκευση των συναλλαγών στο blockchain στο οποίο βασίζεται.

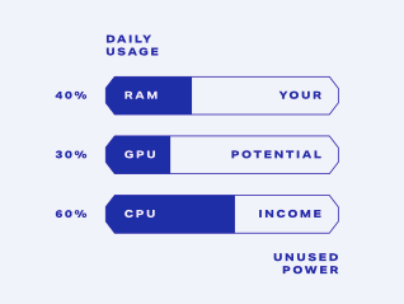
Η λειτουργία του Storj θα μπορούσε να παρομοιαστεί με το διαμοιρασμό αρχείων μέσω Torrents, χωρίς ωστόσο να είναι απόλυτα ίδια. Στο Storj τα αρχεία κατακερματίζονται σε μικρότερα κομμάτια και στη συνέχεια κρυπτογραφούνται και αποθηκεύονται με τυχαία κατανομή σε σκληρούς δίσκους σε όλο το peer-to-peer δίκτυο. Στη συνέχεια οι ιδιοκτήτες των αρχείων, κάθε φορά που χρειάζεται να ανακαλέσουν το αρχείο τους επικοινωνούν με τους υπολογιστές στους οποίους είναι αποθηκευμένα τα κομμάτια των αρχείων τους εκμεταλλευόμενοι πολλαπλάσιο bandwidth σε σχέση με τις εμπορικές λύσεις αποθηκευτικού χώρου στο Cloud. Η πληροφορία σχετικά με τις τοποθεσίες που είναι αποθηκευμένα τα κομμάτια του κάθε αρχείου μπορεί να αποκρυπτογραφηθεί μόνο από τον ιδιοκτήτη του αρχείου, εξασφαλίζοντας απόλυτη ιδιωτικότητα, καθώς οι υπόλοιποι χρήστες δεν μπορούν να το ανακτήσουν ή να αποκρυπτογραφήσουν τα τμήματα αυτού. Για τη διασφάλιση της ακεραιότητας και της διαθεσιμότητας των αρχείων, το σύστημα εκτελεί από μόνο του περιοδικούς ελέγχους στο blockchain.

Στις πρώτες εκδόσεις της πλατφόρμας, οι χρήστες θα έπρεπε να διατηρούν τα κλειδιά πρόσβασης και αποκρυπτογράφησης των αρχείων τους στον υπολογιστή τους, ώστε να μπορούν να κάνουν ανάκτηση των αρχείων τους και να τα ανοίγουν, με αποτέλεσμα να μην μπορούν να ανοίγουν τα αρχεία σε οποιοδήποτε υπολογιστή, αλλά μόνο στον υπολογιστή που είχε αποθηκευμένο το κλειδί. Η τελευταία έκδοση της πλατφόρμας που διατέθηκε στα τέλη του 2018 περιλαμβάνει μία νέα λειτουργικότητα, το Bridge, η οποία είναι η δυνατότητα αποθήκευσης των κλειδιών αποκρυπτογράφησης και ανάκτησης των αρχείων σε ένα server με ασφαλή τρόπο, ώστε ο κάθε χρήστης να έχει στοιχεία πρόσβασης στο server και μέσω αυτού να μπορεί να αποκτήσει πρόσβαση στα αρχεία του από περισσότερες από μία συσκευές. (Storj: A Decentralized Cloud Storage Network Framework, 2018)

3.3.11 Golem [Υπολογιστική Ισχύς]

Το Golem είναι ο πρώτος αποκεντρωμένος υπολογιστής, σύμφωνα με την ομώνυμη εταιρία, καθώς βασίζεται στην αχρησιμοποίητη υπολογιστική ισχύ των χρηστών που έχουν εγκατεστημένη την εφαρμογή στους υπολογιστές τους για τη δημιουργία ενός παγκόσμιου υπερ-υπολογιστή προς ενοικίαση. Ο υπερ-υπολογιστής αυτός αντλεί την ισχύ του από τους αχρησιμοποίητους υπολογιστικούς πόρους των συμμετεχόντων στο peer – to – peer δίκτυο που έχει δημιουργηθεί για να συνδέονται οι «δότες» με τους «λήπτες» υπολογιστικής ισχύος. Οι

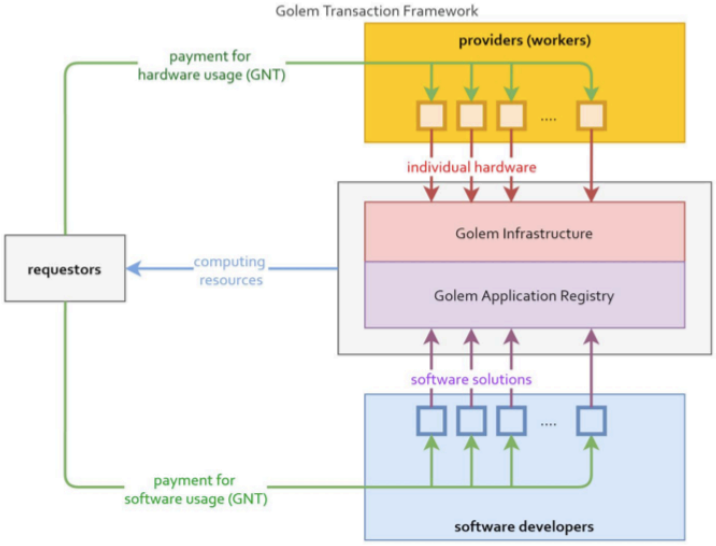
χρήστες εγκαθιστώντας την εφαρμογή Golem μπορούν να κερδίζουν Golem tokens (GNT) προσφέροντας την αδρανή (idle) επεξεργαστική ισχύ των μηχανημάτων τους, είτε να ενοικιάσουν υπολογιστική ισχύ από το δίκτυο καταβάλλοντας ανάλογα GNT.



Εικόνα 35 - Η υπολογιστική ισχύς του δικτύου Golem [golem.network]

Οι υπολογιστές που έχουν εγκατεστημένη την εφαρμογή μπορούν να εκτελούν ασύγχρονα με άλλους υπολογιστές του δικτύου διάφορες υπολογιστικές εργασίες που τους ανατίθενται. Οι λειτουργίες του Golem μπορούν να θεωρηθούν ότι ανήκουν είτε στην κατηγορία Infrastructure as a Service (IaaS) είτε στην κατηγορία Platform as a Service (PaaS), καθώς η υπολογιστική ισχύς που μοιράζεται μεταξύ των χρηστών του δικτύου προέρχεται από «κοινόχρηστα» υπολογιστικά συστήματα και μπορεί να χρησιμοποιηθεί για rendering, εφαρμογές machine learning και άλλες ιδιαίτερα απαιτητικές υπολογιστικές δραστηριότητες. Η εφαρμογή μπορεί να χρησιμοποιηθεί από οποιοδήποτε χρήστη και είναι διαθέσιμη για Windows, macOS και Linux Ubuntu υπολογιστικά συστήματα, καλύπτοντας το μεγαλύτερο ποσοστό των υπολογιστικών συστημάτων παγκοσμίως σε επίπεδο λειτουργικού συστήματος.

Οι συναλλαγές μεταξύ των συμμετεχόντων στο δίκτυο πραγματοποιούνται με τη χρήση του GNT, το οποίο είναι εμπορικά διαθέσιμο σε πολλά exchanges κρυπτονομισμάτων, αλλά και μέσω της προσφοράς υπολογιστικής ισχύος στο δίκτυο. Για την καταγραφή των συναλλαγών αυτών έχει αναπτυχθεί από την Golem μηχανισμός καταχώρησης τους στο δίκτυο του Ethereum και μέρος του κεφαλαίου που κινείται εντός του peer – to – peer δικτύου μετατρέπεται σε Ether για την εξασφάλιση των απαραίτητων πόρων για τη χρήση του Ethereum blockchain. (The Golem Project: Crowdfunding Whitepaper, 2016)



Εικόνα 36 - Το δίκτυο του Golem [golem.network]

4 Εφαρμογή του blockchain στο χώρο της Υγείας

Η κρίση που πέρασε η παγκόσμια οικονομία άφησε πίσω της αρκετές χώρες με ιδιαίτερα μειωμένα ΑΕΠ, και ένας από τους κλάδους που γνώρισε μεγάλη μείωση των κρατικών επιχορηγήσεων παγκοσμίως είναι η υγεία. Σύμφωνα με τη Wall Street Journal, οι Ηνωμένες Πολιτείες της Αμερικής σύντομα θα ξεπεράσουν το 20% του ΑΕΠ τους σε κρατικές δαπάνες για την Υγεία. Υπάρχουν πολλοί κλάδοι του τομέα της Υγείας στους οποίους μπορούν να εντοπιστούν παθογένειες και αν η μείωση του κόστους δεν φαντάζει ιδιαίτερα εύκολη, αυτό που μπορεί να βελτιωθεί άμεσα είναι η ποιότητα των παρεχόμενων υπηρεσιών προς τους πολίτες. Σύμφωνα με άρθρο του Randy Bean στο Forbes, το blockchain είναι μία τεχνολογία που μπορεί να συνεισφέρει στη βελτίωση της εμπειρίας των ασθενών από τις εφαρμογές υγείας, ενώ ταυτόχρονα μπορεί να διατηρεί τα δεδομένα τους απόρρητα και ασφαλή.

Τα τελευταία χρόνια έχουν ανακύψει στον τομέα της υγείας αρκετά ζητήματα που αφορούν την ιδιωτικότητα, τη διαφθορά, την κατάχρηση και παράνομη διακίνηση δεδομένων υγείας και άλλα λιγότερο ή περισσότερο σημαντικά για τον κάθε ασθενή προβλήματα. Η τεχνολογία και ο τρόπος λειτουργίας του blockchain θα μπορούσαν να λύσουν καθοριστικά προβλήματα και να αποκαταστήσουν την εμπιστοσύνη των ασθενών προς τους οργανισμούς παροχής υπηρεσιών υγείας, τους ερευνητικούς φορείς, τις εταιρίες που παράγουν και εμπορεύονται αγαθά άμεσα συνδεδεμένα με την υγεία, όπως για παράδειγμα φάρμακα, ιατρικά μηχανήματα κλπ., καθώς και τους κυβερνητικούς φορείς που παίζουν ένα ρυθμιστικό ή νομοθετικό ρόλο σε όλες τις παραπάνω κατηγορίες εμπλεκομένων. (Bean, Will Blockchain Transform Healthcare?, 2018)

Στη συνέχεια του κεφαλαίου αναλύονται οι εφαρμογές που μπορεί να έχει το blockchain στο χώρο της υγείας, καθώς και κάποιες γνωστές πρώτες προσπάθειες που έχουν γίνει από εταιρίες και ερευνητικούς φορείς σε όλο τον κόσμο.

4.1 Εφαρμογές στον τομέα της υγείας

4.1.1 Ιατρικός φάκελος ασθενών & Κοινή χρήση δεδομένων υγείας

Το βασικότερο σημείο που το blockchain μπορεί να ταράξει τα νερά του τομέα της υγείας είναι η αποθήκευση των δεδομένων των ασθενών στον ιατρικό τους φάκελο. Με τη χρήση της τεχνολογίας του blockchain οι ασθενείς μπορούν να έχουν την πλήρη ιδιοκτησία των δεδομένων τους, και ταυτόχρονα να είναι βέβαιοι ότι αυτά θα διατηρούνται ακέραια και ασφαλή χάρη στις τεχνικές κρυπτογράφησης στο blockchain και στο αναλλοίωτο χαρακτήρα

του τρόπου αποθήκευσης τους. Κατ' επέκταση της διατήρησης των δεδομένων των ασθενών σε ένα διαρκώς ενημερωμένο και αμετάβλητο ιατρικό φάκελο, ένα ακόμη πλεονέκτημα της τεχνολογίας του blockchain που μπορεί να αξιοποιηθεί είναι η ασφάλεια στο διαμοιρασμό των δεδομένων αυτών, καθώς και η καταγραφή του συνόλου των ατόμων ή οργανισμών που έχουν πρόσβαση σε αυτά.

Η χρήση εφαρμογών blockchain στο χώρο της υγείας θα μπορούσε να «παγκοσμιοποιήσει» τους ιατρικούς φακέλους των ασθενών στην περίπτωση που υιοθετηθεί ένας κοινός κώδικας καταγραφής του συνόλου των ιατρικών δεδομένων σε αυτό, καθώς και του διαμοιρασμού αρχείων ιατρικών απεικονίσεων και εξετάσεων μέσω ενός ενιαίου κατάστιχου, το οποίο θα μπορεί να χρησιμοποιείται από πληθώρα εφαρμογών υγείας και από ιατρούς και άλλους σχετικούς με την ιατρική κλάδους σε όλο τον κόσμο, με μόνο περιορισμό την παροχή δικαιωμάτων πρόσβασης από τον ασθενή. Οι ασθενείς θα μπορούν να απολαμβάνουν προσωποποιημένη φροντίδα και να γνωρίζουν κάθε στιγμή ποιος έχει πρόσβαση στα ιατρικά δεδομένα τους, έχοντας την ικανότητα να την περιορίσουν ή να την αφαιρέσουν εντελώς αλλάζοντας το συνδυασμό των κλειδιών κρυπτογράφησης που θα μπορούν να αποκρυπτογραφήσουν τα δεδομένα και να τα συνδέσουν με τον ασθενή ως άτομο.

Για την εξασφάλιση των απαραίτητων υπολογιστικών πόρων έχουν προταθεί διαφορετικά μοντέλα. Κάποιοι θεωρούν ότι το δίκτυο μπορεί να συντηρείται μέσω καθορισμού «προμήθειας» κατά την καταγραφή των ιατρικών δεδομένων, όπως γίνεται στις ηλεκτρονικές συναλλαγές των κρυπτονομισμάτων. Μία διαφορετική ιδέα σε ένα project του MIT που θα αναλυθεί παρακάτω προτείνει την παροχή πρόσβασης σε ερευνητικούς φορείς στον τομέα της υγείας σε ανωνυμοποιημένα δεδομένα ασθενών σε αντάλλαγμα της συντήρησης μέσω παροχής υπολογιστικών πόρων του ενιαίου δικτύου αποθήκευσης ιατρικών δεδομένων. (Liam Bell, 2018)

4.1.2 Παρακολούθηση ιατρικού εξοπλισμού

Ένα πολύ σημαντικό πρόβλημα που θα μπορούσε να αντιμετωπιστεί με τη χρήση του blockchain στο χώρο της υγείας, σύμφωνα με τη Frost & Sullivan, είναι η σήμανση του συνόλου του ιατρικού εξοπλισμού με ένα μοναδικό αναγνωριστικό, με σκοπό να μπορεί να αναγνωριστεί και να εντοπιστεί οποιαδήποτε τέτοια συσκευή με μοναδικό τρόπο, από την κατασκευή μέχρι την απόσυρση ή την ανάλωση της σε κάποιο ασθενή. (Frost&Sullivan, 2017)

Η εξοικονόμηση χρημάτων που μπορεί να προκύψει από τη χρήση μηχανισμών εντοπισμού ιατρικών υλικών και συσκευών είναι ιδιαίτερα μεγάλη. Παράδειγμα για τον ισχυρισμό αυτό

αποτελεί η μελέτη εφαρμογής του East Kent Hospital του NHS, στην οποία χρησιμοποιήθηκαν ετικέτες τεχνολογίας RFID για την καταγραφή και τον εντοπισμό αναλώσιμων συσκευών και μέσω αυτής εντοπίστηκαν σχεδόν 100 συσκευές αντλίες έγχυσης (infusion pumps) κόστους περίπου 1500 £ η κάθε μία, τις οποίες το νοσοκομείο αγνοούσε ότι έχει στο απόθεμα του καθώς οι αποθηκευτικοί χώροι του είναι διαμοιρασμένοι σε τρία κτηριακά συγκροτήματα. (Simon, 2014)

Η καταγραφή των ιατρικών συσκευών με τη χρήση του blockchain θα μπορούσε επιπλέον των ήδη γνωστών τεχνικών καταγραφής και παρακολούθησης εξοπλισμού να διασφαλίσει την αποφυγή κακόβουλων ενεργειών παραχάραξης του ιστορικού τοποθεσιών, καθώς και τη διαγραφή συσκευών. Με αυτό τον τρόπο μπορούν να αποφεύγονται οι κλοπές ή οι επανειλημμένες αγορές συσκευών, εξοικονομώντας χρήματα για τα εθνικά συστήματα υγείας των χωρών παγκοσμίως και βελτιώνοντας ταυτόχρονα τα επίπεδα εμπιστοσύνης των ασθενών στους φορείς παροχής υπηρεσιών υγείας μέσω της μείωσης των διαφόρων σκανδάλων που κατά καιρούς δημοσιεύονται από τα Μέσα Μαζικής Ενημέρωσης.

Επιπλέον της καταγραφής και του εντοπισμού, όταν μία συσκευή δυσλειτουργεί με οποιοδήποτε τρόπο, μέσω της χρήσης ενός μοναδικού αναγνωριστικού της συσκευής και της τεχνολογίας του blockchain θα μπορεί να γίνει ευκολότερη η αναγνώριση και η καταγραφή του προβλήματος και να αποφεύγονται άσκοπες αγορές προβληματικού εξοπλισμού ή εξαρτημάτων, καθώς και να γίνεται ευκολότερα η ανάκληση ή η επιδιόρθωση του προβλήματος που εμφανίζεται στις συσκευές, βελτιώνοντας την ποιότητα της παρεχόμενης υπηρεσίας υγείας προς τους ασθενείς και αυξάνοντας την αποτελεσματικότητα των θεραπειών και την ασφάλεια των ασθενών. (Frost&Sullivan, 2017)

4.1.3 Παραγωγή και παρακολούθηση φαρμάκων

Στον τομέα των φαρμάκων, η χρήση του blockchain θα μπορούσε να συνεισφέρει στην εξάλειψη των αυξανόμενων κινδύνων γύρω από τα πλαστά και τα μη εγκεκριμένα φάρμακα. Όπως συμβαίνει στην παρακολούθηση συσκευών, με τη χρήση της τεχνολογίας του blockchain, είναι εφικτό να δημιουργηθούν smart contracts τα οποία θα αποτελούν το μοναδικό αναγνωριστικό οποιασδήποτε συναλλαγής και θα κάνουν ευκολότερο τον εντοπισμό του συνόλου των συσκευασιών φαρμάκων που διακινούνται στην αγορά, καθώς και της διαδρομής που αυτά ακολουθούν από τον αρχικό κατασκευαστή μέχρι τον καταναλωτή.

Η πλήρης καταγραφή της διαδρομής των φαρμάκων μπορεί να επιτύχει ταυτόχρονα ασφάλεια για τους ασθενείς και διαφάνεια στη λειτουργία των φαρμακευτικών εταιριών και των ενδιάμεσων που συμμετέχουν στο εμπόριο των φαρμάκων.

Καταγράφοντας τη διαδρομή ενός φαρμάκου είναι ευκολότερη η ανάκληση του σε περίπτωση εντοπισμού λανθασμένων παρτίδων, η διασφάλιση των συνθηκών μεταφοράς του και η καταγραφή αυτών στην περίπτωση που το φάρμακο πρέπει να μεταφέρεται υπό συγκεκριμένες συνθήκες, καθώς και ο έλεγχος της συνταγογράφησης που συμπεριλαμβάνει αυτό το φάρμακο σε εγχώριο ή ακόμα και διεθνές επίπεδο για στατιστικούς ή επιδημιολογικούς λόγους. Ακόμη, παρακολουθώντας τα φάρμακα στο σύνολο τους, από την παραγωγή μέχρι και την αγορά και χρήση τους από τους ασθενείς – καταναλωτές, είναι ευκολότερος ο έλεγχος των φαρμακευτικών εταιριών σε επίπεδο οικονομικό και εμπορικό. Με τον έλεγχο αυτό μπορούν να μειωθούν οι κλοπές φαρμάκων και η αλλοίωση φαρμακευτικών συναλλαγών που έχουν ως στόχο τη δημιουργία μεγαλύτερου κέρδους σε βάρος των εθνικών συστημάτων υγείας και των ασφαλιστικών φορέων. (Liam Bell, 2018)

4.1.4 Κλινικές μελέτες

Η Frost & Sullivan στο έντυπο που δημοσίευσε το 2017 με τίτλο “Why Healthcare Industry Should Care About Blockchain?”, αναφέρει ότι οι κλινικές μελέτες είναι ένας ακόμα τομέας που θα μπορούσε να χρησιμοποιήσει το blockchain για να ξεπεράσει τα προβλήματα της παραχάραξης ή αλλοίωσης των αποτελεσμάτων ή ακόμα και την απόκρυψη αποτελεσμάτων ερευνών που μπορεί να είναι αντίθετες με τα συμφέροντα των εταιριών που τις χρηματοδοτούν ή των ίδιων των ερευνητών. Επιπλέον, η χρήση του blockchain διατηρεί ένα αναλλοίωτο μητρώο για τους συμμετέχοντες των ερευνών αυτών, το οποίο θα μπορεί να αποτελεί μέρος του ιατρικού τους φακέλου για όλη τη διάρκεια της ζωής τους. Εκτιμάται ότι η βιομηχανία των φαρμάκων θα μπορούσε να εξοικονομήσει έως και 200 δισεκατομμύρια δολάρια ΗΠΑ αν βελτιώσει τα αποτελέσματα των κλινικών μελετών. (Frost&Sullivan, 2017)

4.2 Εφαρμογές και τεχνολογίες ανάπτυξης

4.2.1 MedRec – MIT Labs

Η δημοσιευμένη προσέγγιση του MIT στην εφαρμογή του blockchain στους Ηλεκτρονικούς Φακέλους Υγείας (ΗΦΥ) είναι η εφαρμογή MedRec. Αφορμή για τη σύλληψη και την περιγραφή της ιδέας αυτής αποτέλεσε το γεγονός ότι οι ΗΦΥ δεν σχεδιάζονται ποτέ με στόχο

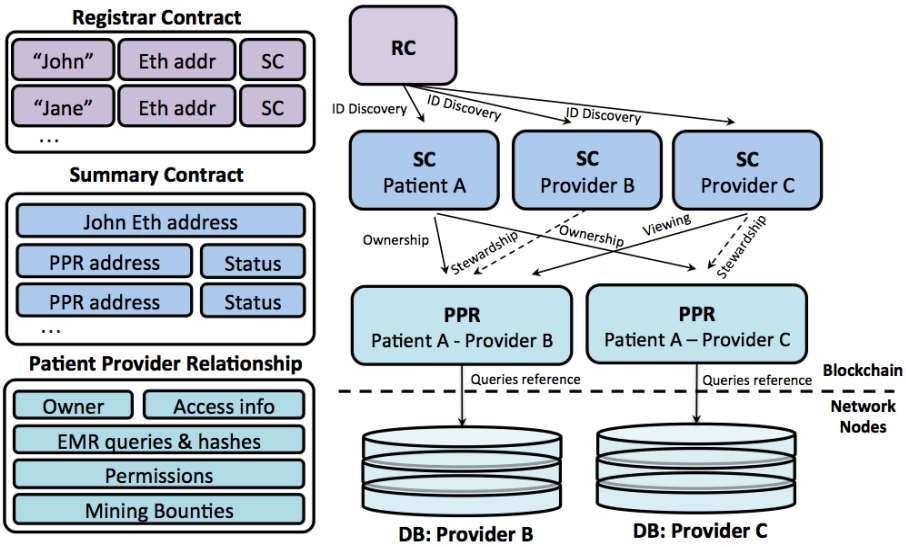
την διαχείριση των πολλαπλών ειδών φακέλων υγείας που διατηρούνται στο σύνολο των οργανισμών υγείας. Όσο οι ασθενείς επισκέπτονται πολλές και διαφορετικές εγκαταστάσεις υγείας τα δεδομένα τους κατακερματίζονται, με αποτέλεσμα να χάνεται αρκετές φορές η δυνατότητα πρόσβασης σε παλαιότερα δεδομένα και να υπάρχει σημαντική απώλεια πληροφορίας για το ατομικό ιστορικό υγείας του κάθε ασθενή. Σε αυτό συνεισφέρει και η προσέγγιση των εφαρμογών ΗΦΥ που θεωρούν ως ιδιοκτήτη των δεδομένων υγείας τον φορέα υγείας και όχι τον ίδιο τον ασθενή, με αποτέλεσμα ο διαμοιρασμός αυτών των δεδομένων μεταξύ των φορέων να μην είναι εφικτό να πραγματοποιηθεί.

Το MedRec είναι ο συνδυασμός μιας κοινωνικής ανάγκης με μία ιδιαίτερα καινοτόμα τεχνολογία – ένα σύστημα που δίνει προτεραιότητα στις ανάγκες των ασθενών δίνοντας μια διάφανη και προσιτή εικόνα του ιατρικού ιστορικού του σε κάθε φορέα υγείας, ιδιωτικό ή δημόσιο. Τα δεδομένα υγείας αποτελούν μοναδικό αποτύπωμα για τον κάθε ασθενή και η λύση που προτείνεται είναι ένα σύστημα κατανεμημένης πρόσβασης που αποσκοπεί στο να αντικαταστήσει τους ενδιάμεσους μεταξύ των διαφορετικών φορέων και των αντίστοιχων πληροφοριακών συστημάτων που αυτοί χρησιμοποιούν. Η προσέγγιση του MedRec και της υλοποίησης του μέσω του blockchain αποσκοπεί στην επίλυση τεσσάρων ιδιαίτερα σημαντικών προβλημάτων στο χώρο της υγείας:

- Την περιορισμένη, αποσπασματική και αργή πρόσβαση σε δεδομένα υγείας
- Τη διαλειτουργικότητα των πληροφοριακών συστημάτων υγείας
- Την ευκολότερη οργάνωση των δεδομένων των ασθενών
- Τη βελτιωμένη ποιότητα και ποσότητα δεδομένων υγείας που μπορούν να χρησιμοποιηθούν για ερευνητικούς σκοπούς

Η υλοποίηση του MedRec βασίζεται στο Ethereum και στα Smart Contracts που υποστηρίζει η πλατφόρμα του. Στο block που δημιουργείται στο ιδιωτικό blockchain του MedRec αποθηκεύονται μόνο δικαιώματα προβολής και ιδιοκτησίας των δεδομένων από φορείς υγείας, και όχι τα ίδια τα δεδομένα υγείας του ασθενή, ενώ με τη χρήση των smart contracts, η πλατφόρμα επιτρέπει τη διατήρηση του συνόλου των καταστάσεων ενός block, όπως για παράδειγμα η αλλαγή στα δικαιώματα προβολής ή η δημιουργία ενός νέου φακέλου στο σύστημα. Το blockchain χρησιμοποιεί πολλαπλά επίπεδα smart contracts και κατάλληλες τεχνικές κρυπτογραφίας, οι οποίες διασφαλίζουν την ανωνυμία των δεδομένων και ταυτόχρονα την συνέχεια τους στη διάρκεια του χρόνου, ώστε ο φάκελος του κάθε ασθενή να είναι ακέραιος και να μην υπάρχει απώλεια δεδομένων, ενώ ταυτόχρονα δικαίωμα πρόσβασης

σε αυτόν θα έχουν μόνο πάροχοι στους οποίους έχει δοθεί κατάλληλη εξουσιοδότηση από τον ίδιο.



Εικόνα 37 - Τα smart contracts του MedRec σε επίπεδο ασθενούς (RC), ιστορικού υγείας (SC) και δικαιωμάτων παρόχου υγείας (PPR) [MedRec White Paper, healthit.gov]

Στην πλατφόρμα του MedRec χρησιμοποιούνται τριών ειδών Smart Contracts:

- **Registrar Contract (RC)**

Χρησιμοποιείται για την αντιστοίχιση των μοναδικών αναγνωριστικών των συμμετεχόντων στο δίκτυο με τις διευθύνσεις τους στο δίκτυο του Ethereum, όπως ακριβώς λειτουργεί και ένα public key στο δίκτυο του blockchain. Χρησιμοποιούνται συμβολοσειρές αντί κρυπτογραφημένων κλειδιών για να μπορούν να χρησιμοποιούνται ήδη υπάρχουσες μορφές μοναδικών αναγνωριστικών από εφαρμογές ΗΦΥ διαφόρων φορέων. Η δημιουργία νέων αναγνωριστικών είναι περιορισμένη μόνο σε πιστοποιημένους οργανισμούς. Επιπλέον της δημιουργίας μοναδικής ταυτότητας, το RC χρησιμοποιείται και για τη σύνδεση των Summary Contracts που περιγράφονται στη συνέχεια.

- **Patient – Provider Relationship (PPR)**

Το smart contract "Patient – Provider Relationship" εκδίδεται μεταξύ δύο κόμβων που συμμετέχουν στο σύστημα, όταν ο ένας επεξεργάζεται και αποθηκεύει δεδομένα στον ιατρικό φάκελο του άλλου, καθώς και για να απεικονίσει οποιαδήποτε άλλη σχέση μεταξύ συμμετεχόντων στο δίκτυο, όπως μεταξύ φορέων για την πρόσβαση του ενός στα δεδομένα του άλλου αναφορικά με τον ιατρικό φάκελο κάποιου ασθενούς. Κάθε τέτοιου είδους συμβόλαιο ουσιαστικά περιέχει ένα ερώτημα προς τη βάση δεδομένων του κάθε φορέα, το οποίο επιστρέφει ένα συγκεκριμένο υποσύνολο δεδομένων που αφορούν έναν ασθενή, καθώς και τα δικαιώματα πρόσβασης όσον αφορά το δίκτυο που πρέπει να χρησιμοποιηθεί, τα στοιχεία πρόσβασης σε αυτό, την πόρτα δικτύου ή και την τοπολογία αυτού.

- **Summary Contract (SC)**

Το Summary Contract λειτουργεί ως ένας χάρτης αντιστοίχισης για τους συμμετέχοντες στο σύστημα, ώστε να μπορούν να εντοπίσουν το σύνολο των δεδομένων που απαρτίζουν τον ιατρικό φάκελο και να μπορούν να τον ανακτήσουν. Οι ασθενείς έχουν δικαίωμα να ανακτήσουν το σύνολο των δεδομένων που είναι συνδεδεμένα με το μοναδικό αναγνωριστικό τους, έχοντας πλήρη εικόνα των δεδομένων τους, ενώ οι πάροχοι υπηρεσιών υγείας έχουν πρόσβαση στο υποσύνολο του ιατρικού φακέλου στο οποίο ο ασθενής τους έχει επιτρέψει την πρόσβαση μέσω ενός PPR Contract. (Eckblaw, Azaria, Halamka, & Lippman, 2016)

4.2.2 Medicalchain

Εικόνα 38 - Το λογότυπο του Medicalchain [medicalchain.com]

Το Medicalchain χρησιμοποιεί την τεχνολογία του blockchain για να δημιουργήσει ένα ασθενοκεντρικό Ηλεκτρονικό Φάκελο Υγείας διατηρώντας κάθε φορά μία μοναδική και αδιάβλητη έκδοση των δεδομένων υγείας των ασθενών. Με τη χρήση του Medicalchain οι ασθενείς μπορούν να δίνουν πρόσβαση στα δεδομένα υγείας τους στους επαγγελματίες υγείας που αυτοί επιθυμούν, έχοντας ταυτόχρονα μία πλήρη καταγραφή των ενεργειών και των αλληλεπιδράσεων των τελευταίων με τα δεδομένα τους.

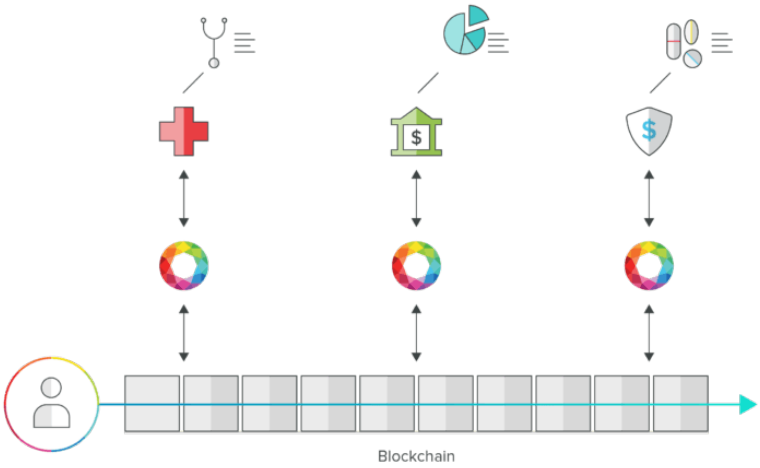
Το Medicalchain έχει δημιουργηθεί πάνω στην πλατφόρμα Hyperledger Fabric, χρησιμοποιώντας μία ιδιωτική αρχιτεκτονική για το δίκτυο blockchain στο οποίο βασίζεται επιτρέποντας διαφορετικά επίπεδα πρόσβασης, με αποτέλεσμα οι ασθενείς να μπορούν να επιλέγουν ποιοι έχουν πρόσβαση στα δεδομένα τους, πόσα από αυτά θα μπορούν να δουν και για πόση χρονική διάρκεια. Για τη λειτουργία του βασίζεται στα MedTokens, τα οποία είναι κρυπτονομίσματα που εκδόθηκαν κατά τη δημιουργία του δικτύου και διανεμήθηκαν μέσω μίας διαδικασίας πώλησης ICO έναντι 0,25$ το ένα. Ταυτόχρονα με το ιδιωτικό δίκτυο του Medicalchain, χρησιμοποιείται ένα ακόμα δίκτυο στο Ethereum στο οποίο βασίζονται όλες οι εφαρμογές που έχουν πρόσβαση στο ιδιωτικό δίκτυο του Medicalchain.

Στην παρούσα φάση ανάπτυξης του παρέχει δύο δυνατότητες στους χρήστες της εφαρμογής, την τηλεϊατρική μεταξύ ιατρού και ασθενούς και την πώληση δεδομένων υγείας για ερευνητικούς σκοπούς. Παράλληλα με αυτές τις δύο λειτουργικότητες, το Medicalchain παρέχει σε άλλους developers ή οργανισμούς να αναπτύξουν τις δικές τους συμβατές με αυτό

εφαρμογές και να τις δημοσιεύσουν σε ένα Marketplace συμβατών εφαρμογών, καθιστώντας τους ασθενείς ικανούς να μπορούν να διαμοιράζονται τα δεδομένα τους και με αυτές. (Medicalchain Whitepaper v2.1, 2018)

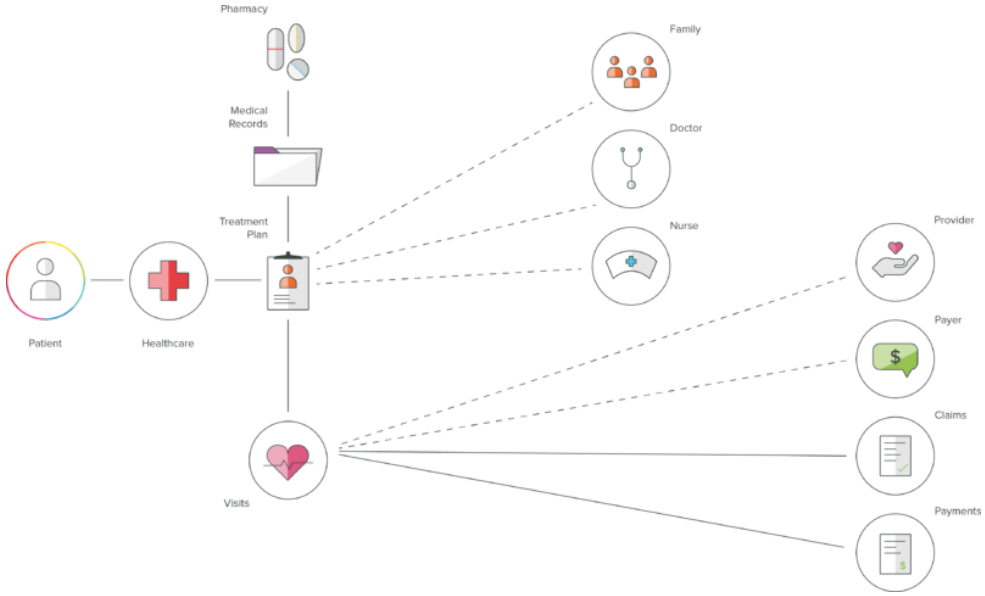
4.2.3 Gem

Το Gem είναι ένα λειτουργικό σύστημα βασισμένο στις τεχνολογίες του blockchain. Βασικός στόχος του είναι να λύσει το πρόβλημα των πολλαπλών οντοτήτων που δημιουργούνται σε διαφορετικές υπηρεσίες που άνθρωποι από όλο τον κόσμο χρησιμοποιούν καθημερινά. Στην προσπάθεια του να εξαλείψει τον κατακερματισμό των δεδομένων που αφορούν στο ίδιο πρόσωπο και χωρίζονται σε διαφορετικές οντότητες, χρησιμοποιώντας το blockchain και αρκετές μορφές διαλειτουργικότητας, το Gem δημιουργεί ένα μοναδικό παγκόσμιο αναγνωριστικό για κάθε άνθρωπο, παρέχοντας διαφάνεια σε πραγματικό χρόνο στο σύνολο των συναλλαγών του και ταυτόχρονα δημιουργώντας μία ενοποιημένη εμπειρία χρήσης.



Εικόνα 39 - Το ενοποιημένο δίκτυο ταυτότητας του Gem [enterprise.gem.co]

Όσον αφορά τον τομέα της υγείας, το Gem OS επιδιώκει να δημιουργήσει μία μοναδική ταυτότητα για κάθε ασθενή στο δίκτυο του, η οποία θα μπορεί να χρησιμοποιείται από πολλές διαφορετικές εφαρμογές σε παγκόσμιο επίπεδο και ταυτόχρονα θα αποτελεί τον ατομικό φάκελο του ασθενούς. Στην προσπάθεια αυτή η Gem έχει ήδη συνάψει αρκετές συμφωνίες, με τη μεγαλύτερη από αυτές να είναι με τη PHILIPS με στόχο να εξερευνήσουν από κοινού μια «ασθενοκεντρική προσέγγιση» στον τομέα της υγείας. (Health - Gem OS, 2019)



Εικόνα 40 - Η ενοποίηση των δεδομένων υγείας στο Gem OS [enterprise.gem.co]

Στα πλαίσια της προσπάθειας χρήσης του Gem OS στο χώρο της υγείας, η Gem παρουσίασε στο συνέδριο Consensus 2017 ένα πρώτο προϊόν που αφορά στις αποζημιώσεις των υπηρεσιών υγείας (healthcare claims). Μέσω αυτής της λύσης το Gem επιδιώκει να λύσει την έλλειψη αναφοράς σε πραγματικό χρόνο των υπηρεσιών υγείας που παρέχονται σε κάθε ασθενή στους φορείς που αποζημιώνουν τις υπηρεσίες αυτές, τα μεγάλα χρονικά διαστήματα που μεσολαβούν από την παροχή των υπηρεσιών έως την αποζημίωση του παρόχου από τους ασφαλιστικούς φορείς και τις χρονοβόρες διαδικασίες που απαιτούνται για τη δημιουργία των κατάλληλων παραστατικών που δικαιολογούν τις αξιώσεις των παρόχων από τους ασφαλιστικούς φορείς.

Χρησιμοποιώντας το Gem OS ως βάση, η λύση που προτάθηκε είναι μία πλήρης διασύνδεση των πληροφοριακών συστημάτων των διαφόρων εμπλεκομένων στη διαδικασία της παροχής υπηρεσιών υγείας και στην αποζημίωση τους, μέσω της δημιουργίας μοναδικών αναγνωριστικών των ασθενών που θα μπορούσαν να τους ταυτοποιούν σε όλα τα επιμέρους συστήματα, δημιουργώντας ταυτόχρονα στο blockchain ένα αδιάβλητο ιστορικό και βελτιώνοντας στο σύνολο της τη διαδικασία των αποζημιώσεων από τους ασφαλιστικούς φορείς. Σύμφωνα με την αναφορά του Becker Hospital που παρουσιάστηκε στο συνέδριο, ο μέσος χρόνος πριν τη χρήση της λύσης του Gem OS μεταξύ της υποβολής των δικαιολογητικών και της τελικής αποζημίωσης του νοσοκομείου ήταν 48,4 ημέρες, ενώ μετά τη δοκιμαστική χρήση του Gem OS, ο χρόνος διεκπεραίωσης μίας αποζημίωσης ήταν μόλις 5 λεπτά. (Allison, 2017)

Από τεχνολογικής πλευράς, το Gem OS βασίζεται σε μία ανεξάρτητη υλοποίηση από τα δημοφιλή δίκτυα blockchain, και μπορεί να αναπτυχθεί είτε αυτόνομα και να διαχειρίζεται

συναλλαγές που καταγράφονται στο ίδιο το Gem blockchain (on chain transactions) είτε σε συνδυασμό με άλλα πληροφοριακά συστήματα – βασισμένα στο blockchain ή σε άλλες τεχνολογίες – και να λειτουργεί ως ενδιάμεσο κατάστιχο καταγραφής τοποθεσιών των δεδομένων ενός μοναδικού προσώπου (off chain transactions). (Kannan & Smith, 2016)

4.2.4 Nebula Genomics

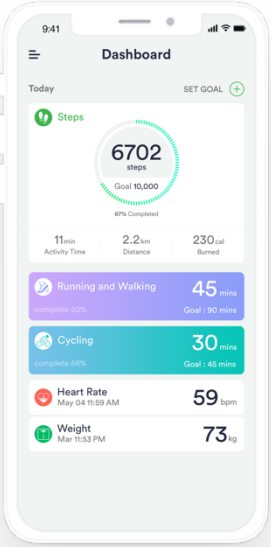
Η Nebula Genomics είναι μία πλατφόρμα αποθήκευσης, διαμοιρασμού και επεξεργασίας δεδομένων σχετικών με την βιοϊατρική. Αποτελεί μία προσπάθεια δημοσιοποίησης big data γενετικής, διασφαλίζοντας ταυτόχρονα την ιδιωτικότητα και εξασφαλίζοντας την πρόσβαση των επιστημόνων σε αυτά με τη χρήση ενός μόνο δικτύου. Μέσω της χρήσης της τεχνολογίας blockchain δεν απαιτείται η χρήση ενδιάμεσων εφαρμογών και οι αγοραστές γενετικών δεδομένων μπορούν να αλληλοεπιδράσουν απευθείας με τους ιδιοκτήτες των δεδομένων αυτών, οι οποίοι λαμβάνουν ανταμοιβές για τη συμμετοχή τους στην κοινότητα διαμοιρασμού των γενετικών δεδομένων.

Εικόνα 41 - Το λογότυπο της Nebula Genomics [nebula.org]

Στόχος της εφαρμογής είναι η άμεση σύνδεση των ασθενών με τους ερευνητές, ώστε να ελέγχεται με πιο αποτελεσματικό τρόπο η συγκατάθεση των ασθενών για την επεξεργασία των γενετικών δεδομένων τους και η ανταμοιβή των πραγματικών ιδιοκτητών των γονιδίων που είναι οι ασθενείς και όχι οι διάφορες εταιρίες και οργανισμοί που μπορεί να τα έχουν στην κατοχή τους και να τα εμπορεύονται χωρίς την συγκατάθεση των ασθενών εξασφαλίζοντας μεγάλα κέρδη από ερευνητικούς φορείς που ενδιαφέρονται για την απόκτηση τέτοιου είδους πληροφοριών. Επιπλέον, μέσω της συσσώρευσης μεγάλης ποσότητας δεδομένων, η πλατφόρμα αποσκοπεί στο να κάνει την γενετική ανάλυση των γονιδίων των ανθρώπων μία διαδικασία ταχύτερη και οικονομικότερη, καθώς όλο και περισσότεροι ερευνητικοί φορείς και ασθενείς μπορούν να συμμετέχουν στο δίκτυο του Nebula Genomics, ενισχύοντας έτσι την πρώτη ύλη για τις έρευνες και δημιουργώντας κοινές τράπεζες δεδομένων στις οποίες μπορούν να δουλεύουν ταυτόχρονα οι ερευνητές μειώνοντας το χρόνο ανάλυσης των διάφορων γονιδίων. (How it works, 2019)

4.2.5 Patientory

Το Patientory είναι μία προσπάθεια συγκέντρωσης όλων των δεδομένων υγείας ενός ασθενή σε ένα κεντρικό blockchain, ώστε οι ασθενείς να μπορούν να τα διαχειρίζονται, να παρακολουθούν την υγεία τους και να τα διαμοιράζονται με όποιον επιθυμούν. Οι ασθενείς μπορούν χρησιμοποιώντας την εφαρμογή να διατηρούν τις επισκέψεις τους στο γιατρό, τα κόστη της υγειονομικής περίθαλψης τους, την ασφάλεια τους, τη φαρμακευτική αγωγή που έχουν ακολουθήσει κατά καιρούς, τον εμβολιασμό τους και άλλες προσωπικές πληροφορίες σχετικές με την υγεία τους.



Εικόνα 42 - Η εφαρμογή Patientory [patientory.com]

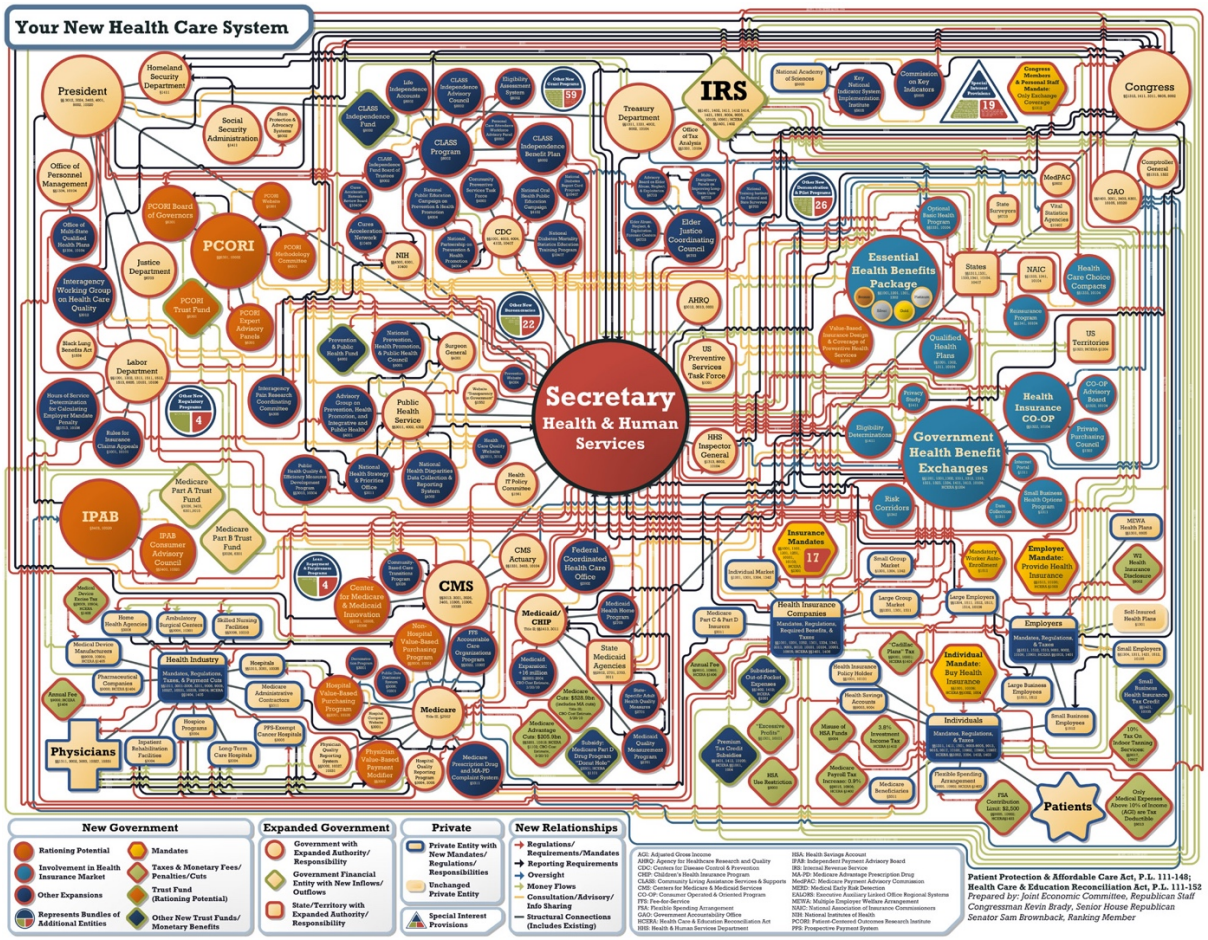
Η εφαρμογή δεν αποτελεί μία ανεξάρτητη υλοποίηση ΗΦΥ, αλλά συγκεντρώνει δεδομένα μέσω ασφαλών συνδέσμων από εξουσιοδοτημένες εφαρμογές, όπως για παράδειγμα ο Ηλεκτρονικός Φάκελος Υγείας της Epic που χρησιμοποιείται σε πληθώρα Αμερικανικών Νοσοκομείων και Ιδιωτικών Ιατρείων. Παρέχει στους ασθενείς τη δυνατότητα να έχουν τον ιατρικό φάκελο τους στο κινητό τους τηλέφωνο, άμεσα προσβάσιμο μέσω της mobile εφαρμογής της πλατφόρμας, ενώ το κόστος της εξαρτάται από τον όγκο των δεδομένων υγείας που διατηρούνται στο blockchain της και ξεκινά από μία δωρεάν βαθμίδα με αποθηκευτικό χώρο ίσο με 10 MB και στη συνέχεια αυξάνεται ανάλογα με τον αποθηκευτικό χώρο που επιθυμούν οι χρήστες. Οι πληρωμές γίνονται σε PTOY, που είναι το κρυπτονόμισμα του Patientory.

Από τεχνολογικής πλευράς, το Patientory είναι μία εφαρμογή με αλγορίθμους που υπόκεινται στην ιδιοκτησία της ίδιας της εταιρίας και δεν διατίθεται ως open source λογισμικό. Η λογική στην οποία βασίζεται η δομή του blockchain του Patientory είναι παρόμοια με αυτή του Ethereum, καθώς χρησιμοποιεί smart contracts για να κατοχυρώνει τις προσβάσεις και τα δικαιώματα των εφαρμογών στον ιατρικό φάκελο των ασθενών. (Patientory Inc. | Technology, 2018)

4.3 Εμπόδια και προκλήσεις

Η διείσδυση της τεχνολογίας σε κάθε κλάδο είναι ιδιαίτερα σημαντική για τη βελτίωση της ποιότητας των υπηρεσιών του. Στον τομέα της υγείας, η διείσδυση και η χρήση νέων τεχνολογιών είναι περισσότερο σημαντική, καθώς οι υπηρεσίες της αλλάζουν και πλέον παίρνουν μία νέα μορφή με επίκεντρο τους ασθενείς, καθιστώντας την παρούσα χρονική περίοδο μία ευκαιρία για την υιοθέτηση νέων τεχνολογιών στην προσπάθεια για την αλλαγή του πεδίου των πληροφοριακών συστημάτων της υγείας.

Η πολυπλοκότητα των συστημάτων υγείας στις περισσότερες χώρες είναι ιδιαίτερα μεγάλη. Στην ακόλουθη εικόνα απεικονίζεται το σύστημα υγείας των Ηνωμένων Πολιτειών της Αμερικής, σε μία προσπάθεια που υποκινήθηκε από τον Κ. Μπράντι στα πλαίσια συζητήσεων στο Κογκρέσο για το σύστημα υγείας των ΗΠΑ. Όπως είναι προφανές, οι εμπλεκόμενοι φορείς και οι διασυνδέσεις μεταξύ αυτών δεν είναι εύκολο να απεικονιστούν, πόσο δε μάλλον να οργανωθούν στα πλαίσια των ήδη υπαρχόντων πληροφοριακών συστημάτων.



Εικόνα 43 - Απεικόνιση του Συστήματος Υγείας των ΗΠΑ [kevinbrady.house.gov]

Η εστίαση στην ποιότητα της υγείας σημαίνει στην πράξη τη διαχείριση της υγείας των ασθενών σε όλα τα επίπεδα με το μέγιστο δυνατό αποτέλεσμα. Πολλές φορές οι διάφοροι

νόμοι και εθνικοί κανονισμοί παραβλέπουν την προτεραιότητα αυτή και εισάγουν διαδικασίες που μπορεί να απλουστεύουν τη γραφειοκρατία και ταυτόχρονα να μειώνουν την ποιότητα των παρεχόμενων υπηρεσιών. Το μεγαλύτερο πρόβλημα που συναντάται στο χώρο της υγείας διαχρονικά είναι το κενό μεταξύ των παρόχων υπηρεσιών υγείας και των φορέων που αποζημιώνουν αυτές τις παροχές, είτε αυτοί είναι δημόσιοι ασφαλιστικοί φορείς είτε ιδιωτικές ασφαλιστικές εταιρίες. Η πολυπλοκότητα των διαδικασιών αποζημιώσεων πολλές φορές λειτουργεί αποτρεπτικά ως προς τους ασθενείς για την προσφυγή τους σε κάποιο πάροχο υπηρεσιών υγείας.

Επιπλέον της πολυπλοκότητας του συστήματος υγείας και των διαδικασιών που αυτό ενσωματώνει, υπάρχουν και άλλες πτυχές του κλάδου στις οποίες εντοπίζονται παθογένειες. Για παράδειγμα, οι μισές σχεδόν κλινικές μελέτες στις ΗΠΑ δεν έχουν δηλωθεί επίσημα σε κάποιο φορέα και τα αποτελέσματα τους δε δημοσιεύονται. Ακόμη, σύμφωνα με στατιστικά στοιχεία που αφορούν στους Ηλεκτρονικούς Φακέλους Υγείας των ασθενών στις ΗΠΑ, το 40% των ΗΦΥ συμπληρώνονται με ελλιπή ή λανθασμένα δεδομένα. Τέλος, πολλοί πάροχοι υπηρεσιών υγείας βασίζονται σε παλιότερες εκδόσεις ΗΦΥ, χρησιμοποιώντας λειτουργικά συστήματα των οποίων η υποστήριξη έχει σταματήσει από τους κατασκευαστές τους και η αρχιτεκτονική επιβάλλει την τοπική αποθήκευση τους, καθιστώντας το διαμοιρασμό τους αδύνατο και κατακερματίζοντας τα δεδομένα των ασθενών στην πληθώρα παρόχων που μπορεί να επισκέπτονται κατά τη διάρκεια της ζωής τους.

Σύμφωνα με το Hype Cycle του Gartner, η τεχνολογία του blockchain έχει περάσει από το σημείο πυροδότησης της καινοτομίας και τη διόγκωση των προσδοκιών και πλέον διανύει τη φάση της απομυθοποίησης. Σε αυτή τη φάση γίνεται ξεκάθαρη η συμβολή που μπορεί να έχει η τεχνολογία του στον τομέα της υγείας, καθώς μπορεί να μεταφέρει τη δύναμη της ιδιοκτησίας των δεδομένων στους ασθενείς, δίνοντας τους το δικαίωμα να τα διατηρούν σε ένα κεντρικό αποθετήριο και στη συνέχεια να τα διαχειρίζονται και να τα διαμοιράζονται όπως αυτοί επιθυμούν.

Η δομή του blockchain επιτρέπει την απλούστευση των διαδικασιών του τομέα της υγείας όσον αφορά την αποθήκευση των δεδομένων και την πρόσβαση σε αυτά από τους εξουσιοδοτημένους χρήστες. Χρησιμοποιώντας ένα απλό παράδειγμα χρήσης του blockchain για την αποθήκευση και τη διατήρηση των δεδομένων υγείας των ασθενών στα πλαίσια μίας χώρας όπως οι ΗΠΑ, θα μπορούσαμε να έχουμε ένα κεντρικό αποθετήριο όπου το σύνολο των δεδομένων των ασθενών θα μπορούσαν να διατηρούν τους ΗΦΥ τους, οι φορείς παροχής υπηρεσιών υγείας και οι ιδιώτες γιατροί θα μπορούσαν να ενημερώνουν το φάκελο αυτό διαρκώς προσθέτοντας ποιοτική πληροφορία και έχοντας πάντα πλήρη εικόνα του ιατρικού

ιστορικού του ασθενούς, οι φορείς αποζημίωσης των υπηρεσιών θα μπορούσαν να γνωρίζουν σε σχεδόν πραγματικό χρόνο την υπηρεσία που παρασχέθηκε στον ασθενή ώστε να προχωρήσουν στην άμεση αποζημίωση της και το κράτος και οι διοικητικές υπηρεσίες του θα μπορούσαν να πραγματοποιούν οποιοδήποτε έλεγχο αντικειμενικά, βασιζόμενες στον αδιάβλητο χαρακτήρα της αποθήκευσης των δεδομένων στο blockchain.

Παράλληλα με την απλούστευση των διαδικασιών, ο ιδιαίτερα ασφαλής χαρακτήρας αποθήκευσης των δεδομένων του blockchain, μέσω της χρήσης διαφορετικών μεθόδων κρυπτογράφησης, μπορεί να διασφαλίσει το απόρρητο του ασθενούς και να δώσει στους ασθενείς τη δυνατότητα να διαχειρίζονται μόνοι τους τα δεδομένα που αφορούν στην υγεία τους και τις επιτρεπόμενες προσβάσεις σε αυτά.

Τέλος, εκτός των περιπτώσεων χρήσης του blockchain στους ΗΦΥ, η χρήση της τεχνολογίας μπορεί να πραγματοποιηθεί για την αντιμετώπιση παθογενειών και σε άλλους τομείς όπως είναι οι κλινικές μελέτες, καθώς και η διανομή και αποθήκευση των φαρμάκων, βελτιώνοντας συνολικά το επίπεδο της παρεχόμενης υγείας στους πολίτες. (Pratap, 2018)

5 Συμπεράσματα – Προοπτικές

5.1 Γενικότερη αξιολόγηση εργαλείων και εφαρμογών blockchain

Το blockchain έχει περάσει τα τελευταία χρόνια από πολλά στάδια και έχει γνωρίσει ιδιαίτερη δημοσιότητα στους ανθρώπους της τεχνολογίας, καθώς και σε αρκετούς επενδυτές. Και οι δύο αυτές μεγάλες ομάδες ανθρώπων έχουν εντοπίσει σημαντικά χαρακτηριστικά που διαφοροποιούν το blockchain από τις παραδοσιακές μεθόδους αποθήκευσης και διεκπεραίωσης ηλεκτρονικών συναλλαγών και των αντίστοιχων δεδομένων τους. Το κυριότερο χαρακτηριστικό που το διαφοροποιεί είναι ο αποκεντρωμένος χαρακτήρας του, ο οποίος εξασφαλίζει ταυτόχρονα τη βιωσιμότητα του δικτύου και τη διαρκή διαθεσιμότητα των αποθηκευμένων πληροφοριών, καθώς και την ασφάλεια των δεδομένων από προσπάθειες παραχάραξης, καθώς κάθε κόμβος διατηρεί ένα αντίγραφο της πληροφορίας και το σύνολο του δικτύου ταυτοποιεί τη γνησιότητα της.

Η χρήση του blockchain σε εφαρμογές πληροφορικής και καινοτομίας είναι ένα από τα πεδία που θα απασχολήσουν την παγκόσμια κοινότητα πληροφορικής τα επόμενα χρόνια. Για τη χρήση του σε παραγωγικές εφαρμογές μεγάλων οργανισμών, ή για την αντικατάσταση των παραδοσιακών ηλεκτρονικών συναλλαγών από υλοποιήσεις που θα βασίζονται στο blockchain, η παγκόσμια αγορά τεχνολογίας και οι εταιρίες που δραστηριοποιούνται σε αυτή αναμένεται να καταβάλουν μεγάλη προσπάθεια τα επόμενα χρόνια, χωρίς αυτό να σημαίνει ότι η τεχνολογία αυτή πρόκειται να αντικαταστήσει άμεσα τις ήδη εδραιωμένες τεχνολογίες.

Όσον αφορά τις πλατφόρμες που αναλύθηκαν στο δεύτερο κεφάλαιο της παρούσας εργασίας, προκύπτουν τα ακόλουθα συμπεράσματα:

- Η πληθώρα των διαθέσιμων μέσων και γλωσσών ανάπτυξης δεν αναμένεται να καθιερώσει κάποια από τις πλατφόρμες ως κυρίαρχο στην αγορά.
- Πολλές εφαρμογές αναμένεται να χρησιμοποιήσουν συνδυασμό ιδιωτικών και δημόσιων blockchains για τη διασφάλιση των εμπιστευτικών – απόρρητων δεδομένων τους.
- Η τεχνολογία του blockchain δεν έχει οριστικοποιηθεί ακόμη ως μορφή αποθήκευσης συναλλαγών. Η πλατφόρμα του IOTA με τον εναλλακτικό τρόπο υπογραφής των συναλλαγών και τη δημιουργία του κατευθυνόμενου γράφου επιβεβαιώνει ότι ο δρόμος μέχρι την οριστικοποίηση της τεχνολογίας του blockchain είναι μακρύς.

5.2 Αξιολόγηση εργαλείων και εφαρμογών blockchain στο χώρο της υγείας

Στο τέταρτο κεφάλαιο της παρούσας διπλωματικής έγινε εκτενής αναφορά στους πιθανούς τομείς της υγείας που θα μπορούσαν να χρησιμοποιήσουν την τεχνολογία του blockchain για τη βελτίωση της ποιότητας των παρεχόμενων υπηρεσιών προς τους ασθενείς και την βελτίωση του επιπέδου ασφάλειας των ασθενών. Οι εφαρμογές αυτές, από την αποθήκευση των ιατρικών πληροφοριών ενός ατόμου σε ένα συνεχές και αδιάβλητο ιστορικό, έως τη βελτίωση της ποιότητας συντήρησης των ιατρικών μηχανημάτων και την ευκολότερη παρακολούθηση των φαρμάκων, μπορούν να συνεισφέρουν στην απλοποίηση των διαδικασιών του τομέα της υγείας και να μειώσουν την πληθώρα υπολογιστικών συστημάτων που χρησιμοποιούνται, με το τελικό όφελος να ευνοεί τους ασθενείς, τους φορείς παροχής υπηρεσιών υγείας, αλλά και τους διοικητικούς και ασφαλιστικούς φορείς.

Αδιαμφισβήτητα το blockchain δεν είναι και ούτε πρέπει να αντιμετωπίζεται ως πανάκεια στα προβλήματα και τις παθογένειες του τομέα της υγείας. Αντίθετα, θα πρέπει να αντιμετωπιστεί ως μία ευκαιρία ενοποίησης και συγκέντρωσης των δεδομένων υγείας σε κεντρικά αποθετήρια, καθώς και ως μία από τις καλύτερες προσεγγίσεις που μπορούν να χρησιμοποιηθούν για την μεταφορά του ασθενή από το περιθώριο στο επίκεντρο των ιατρικών του δεδομένων. Η χρήση του από εφαρμογές υγείας έχει ήδη δείξει αρκετά θετικά βήματα προς την κατεύθυνση της απλούστευσης της αποθήκευσης και του διαμοιρασμού των δεδομένων υγείας των ασθενών, παρουσιάζοντας, ωστόσο, αρκετά σημεία στα οποία θα πρέπει η νομοθεσία να γίνει ξεκάθαρη και να καθορίσει τις κατευθύνσεις που θα πρέπει να ακολουθήσουν οι εφαρμογές που βασίζονται σε αυτό.

Η εφαρμογή του blockchain και η χρήση εφαρμογών που στηρίζονται σε αυτό δεν μπορεί να είναι άμεση, παρά τα πρώτα ιδιαίτερα θετικά βήματα που καταγράφονται από την πορεία των πρώτων εφαρμογών. Οι προκλήσεις που θα πρέπει να αντιμετωπιστούν αφορούν τόσο στις διαδικασίες των εθνικών συστημάτων υγείας και των εμπλεκόμενων φορέων σε αυτά, όσο και στο νομοθετικό πλαίσιο που τείνει να κάνει τις διαδικασίες αυτές ολοένα και πιο πολύπλοκες.

Το κυριότερο εμπόδιο, ωστόσο, που θα αντιμετωπίσει το blockchain κατά την είσοδο του στην αγορά της υγείας είναι η δυσπιστία των ανθρώπων σε κάθε τι καινούριο, καθώς και η δυσκολία τους να προσαρμόσουν το σκεπτικό τους σε μία απλουστευμένη δομή διαχείρισης των δεδομένων τους στην οποία οι ίδιοι θα είναι στο επίκεντρο και θα μπορούν να διαχειρίζονται το σύνολο των δεδομένων τους και τα άτομα που κάθε φορά θα έχουν πρόσβαση σε αυτά.

5.3 Προοπτικές

Η παρούσα κατάσταση της τεχνολογίας του blockchain και το παγκόσμιο ενδιαφέρον που αυτή έχει προσελκύσει είναι ευοίωνα για την συνέχεια και την εξέλιξη της τεχνολογίας από τις πειραματικές εφαρμογές στην αξιοποίηση της στην καθημερινότητα. Πολλοί τεχνολογικοί και ακαδημαϊκοί φορείς έχουν αντιληφθεί τη σημασία της εξέλιξης του blockchain και της διερεύνησης της χρήσης του στους διάφορους τομείς.

Για την πλήρη αξιοποίηση των δυνατοτήτων της τεχνολογίας του blockchain στον τομέα της υγείας και σε άλλους τομείς διακρίνονται οι εξής προοπτικές:

- **Χρειάζεται να διερευνηθούν μεθοδολογίες διατήρησης και εξόρυξης (mining) των blocks της αλυσίδας με μικρότερο ενεργειακό και περιβαλλοντικό αποτύπωμα.** Η εξόρυξη κρυπτονομισμάτων καταναλώνει ταυτόχρονα πολλούς υπολογιστικούς πόρους στα πλαίσια ενός διαρκώς αυξανόμενου ανταγωνισμού, χωρίς να αξιοποιούνται σε ικανοποιητικό βαθμό προς όφελος του δικτύου ή της ίδιας της εφαρμογής που αυτό υποστηρίζει, με αποτέλεσμα να καταναλώνεται μεγάλη ποσότητα ενέργειας.
- **Αξίζει να διερευνηθεί η δυνατότητα αποθήκευσης δεδομένων στο περιεχόμενο του κάθε block**, είτε αυτό μπορεί να γίνει με συγκεκριμένη κωδικοποίηση (π.χ. XML), είτε απευθείας ως πρωτογενής πληροφορία. Με αυτό τον τρόπο το blockchain από χώρος αποθήκευσης και διατήρησης συναλλαγών θα μπορεί να εξελιχθεί σε χώρος αποθήκευσης και κρυπτογράφησης δεδομένων, αποκτώντας μεγαλύτερο νόημα για εφαρμογές που δεν βασίζονται σε χρηματικές ή άλλες ηλεκτρονικές συναλλαγές ή σε smart contracts.
- **Ιδιαίτερο ενδιαφέρον σε ερευνητικό αλλά και πρακτικό επίπεδο διαφαίνεται να έχει η υλοποίηση του IOTA**, όπου η αλυσίδα δεν είναι μία σειριακή δομή από blocks που δεν μπορεί να μεταβληθεί, αλλά ένα σύνολο από συνδεδεμένα blocks που διαρκώς επεκτείνεται προς περισσότερες κατευθύνσεις, χάρη στην επικύρωση δύο blocks με τη χρήση ενός νέου.

Πιο συγκεκριμένα, όσον αφορά τον τομέα της υγείας:

- **Χρειάζεται να καταγραφούν οι διαθέσιμες κωδικοποιήσεις δεδομένων υγείας**, όπως για παράδειγμα οι κωδικοποιήσεις ασθενειών κατά ICD, ICPC κλπ., και η χρήση αυτών για την αποθήκευση δεδομένων υγείας ασθενών στο εσωτερικό του blockchain.
- **Θα πρέπει να διερευνηθεί η δυνατότητα διαμοιρασμού των δεδομένων των ασθενών μέσω της χρήσης ζευγαριών δημόσιων – ιδιωτικών κλειδιών**

κρυπτογράφησης, ώστε οι ασθενείς να μπορούν να έχουν τον πλήρη έλεγχο των προσβάσεων τρίτων στα προσωπικά δεδομένα υγείας τους.

- Πέραν των εφαρμογών που αφορούν τους ασθενείς και τον Ηλεκτρονικό Φάκελο Υγείας τους, **ιδιαίτερο ενδιαφέρον θα είχε η αξιοποίηση του blockchain για την παρακολούθηση μοσχευμάτων, ακριβών φαρμάκων και μηχανημάτων** που χρησιμοποιούνται σε διάφορους οργανισμούς παροχής υπηρεσιών υγείας, ώστε να αυξάνεται το επίπεδο ασφάλειας των ασθενών που λαμβάνουν τις υπηρεσίες αυτές.
- **Οι κλινικές μελέτες και τα αποτελέσματα τους είναι ιδιαίτερα σημαντικός τομέας για τη διερεύνηση της εφαρμογής ενός αδιάβλητου συστήματος αποθήκευσης πληροφοριών**, καθώς εξασφαλίζεται η μη παραχάραξη των αποτελεσμάτων τα δεδομένα των ασθενών παραμένουν ασφαλή και κρυπτογραφημένα, με ιδιοκτήτες αυτούς και μόνον αυτούς.

6 Βιβλιογραφία

Mazet, R. (2017, November). *Alice white paper.* Ανάκτηση από alice.si: https://github.com/alice-si/whitepaper

A Digestible Guide to Blockchain App Development. (2018). Ανάκτηση από AppInventiv.com: https://appinventiv.com/blog/blockchain-app-development-guide

About Blockcerts. (2019). Ανάκτηση από Blockcerts.org: https://www.blockcerts.org/about.html

Allison, I. (2017, May 20). *Gem shows off first blockchain application for health claims*. Ανάκτηση από International Business Times: https://www.ibtimes.co.uk/gem-shows-off-first-blockchain-application-health-claims-1622574

Ark, T. V. (2018, August). *20 Ways Blockchain Will Transform Education*. Ανάκτηση από Forbes.com: https://www.forbes.com/sites/tomvanderark/2018/08/20/26-ways-blockchain-will-transform-ok-may-improve-education/#471f8da64ac9

Bean, R. (2018, August 5). *Will blockchain transform Healthcare?* Ανάκτηση από Forbes.com: https://www.forbes.com/sites/ciocentral/2018/08/05/will-blockchain-transform-healthcare/#54f5058c553d

Bean, R. (2018, August). *Will Blockchain Transform Healthcare?* Ανάκτηση από Forbes.com: https://www.forbes.com/sites/ciocentral/2018/08/05/will-blockchain-transform-healthcare/#577a29a2553d

Bell, L. (2018, May). Applications of Blockchain within Healthcare. *Blockchain in Healthcare Today*, σσ. 1-7.

BigchainDB. (2018, May). *BigchainDB 2.0: The Blockchain Database.* Ανάκτηση από BigchainDB: https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf

Bussmann, O. (2018, 12 12). *4 Major Blockchain Trends to Watch for in 2019*. Ανάκτηση από Forbes: https://www.forbes.com/sites/oliverbussmann/2018/12/12/4-major-market-trends-to-watch-for-in-2019/

Carpooling 2.0 powered by blockchain and IoT. (2018). Ανάκτηση από Yantha.com: https://www.yantha.com/onepager/onepager.pdf

Charitable Crypto: Making the World a Better Place with Blockchain. (2018, 12). Ανάκτηση από Changelly Blog - Medium.com: https://medium.com/@Changelly/blockchain-in-charity-523e57ea2f8b

Decentralized Car Sharing Platform Aims to Lead the Blockchain-based Rental Market. (2018, January). Ανάκτηση από CoinTelegraph.com:

https://cointelegraph.com/news/decentralized-car-sharing-platform-aims-to-lead-the-blockchain-based-rental-market

Deloitte. (2018). *Breaking blockchain open - Deloitte's 2018 global blockchain survey.* Deloitte.com.

DeMuro, J. (2018, January). *7 ways blockchain will change the legal industry forever*. Ανάκτηση από techradar.com: https://www.techradar.com/news/7-ways-blockchain-will-change-the-legal-industry-forever

Dubai Paperless Strategy Completes Phase One. (2019, 01). Ανάκτηση από Smart Dubai: https://www.smartdubai.ae/newsroom/news-details/2019/01/16/dubai-paperless-strategy-completes-phase-one#listingPage=1&tab=event

Eckblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare: "MedRec prototype for electronic health records and medical research data.

Franklin, C. (2018). *7 ways blockchain is being used for security*. Ανάκτηση από DARKreading: https://www.darkreading.com/application-security/7-ways-blockchain-is-being-used-for-security/d/d-id/1332735

Frost&Sullivan. (2017). *Frost & Sullivan*. Ανάκτηση από Why Healthcare Industry Should Care About Blockchain?: https://ww2.frost.com/files/8615/0227/3370/Why_Healthcare_Industry_Should_Care_About_Blockchain_Edited_Version.pdf

Gartner Hype Cycle - Interpreting technology hype. (2018). Ανάκτηση από Gartner: https://www.gartner.com/en/research/methodologies/gartner-hype-cycle

Global Payments 2016: Strong Fundamentals Despite Uncertain Times. (2016). Ανάκτηση από McKinsey.com: https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/a%20mixed%202015%20for%20the%20global%20payments%20industry/global-payments-2016.ashx

Gräther, W. (2018). *20 Ways Blockchain Will Transform Education.* Ανάκτηση από https://dl.eusset.eu/bitstream/20.500.12015/3163/1/blockchain2018_07.pdf

Greenspan, G. (2015). *MultiChain Private Blockchain — White Paper.* Ανάκτηση από MultiChain: https://www.multichain.com/download/MultiChain-White-Paper.pdf

Health - Gem OS. (2019, March). Ανάκτηση από Gem: https://enterprise.gem.co/health/

Hil, L. (2018, February). *A More Secure Way to Home Share? Blockchain Technology*. Ανάκτηση από Forbes.com: https://www.forbes.com/sites/lorihil/2018/02/15/a-more-secure-way-to-home-share-blockchain-technology/#78775a445e8b

HireGo. (2018, 12). Ανάκτηση από HireGo: https://hirego.io

How it works. (2019). Ανάκτηση από Nebula Genomics: https://nebula.org/how_it_works

Hyperledger.org. (2018). *An Introduction to Hyperledger.* Linux Foundation.

HyrdaChain: Permissioned Distributed Ledger based on Ethereum. (2018). Ανάκτηση από GitHub: https://github.com/HydraChain/hydrachain

IBM Blockchain. (2018). Ανάκτηση από IBM.com: https://www.ibm.com/blockchain

Kannan , S., & Smith, M. (2016, 10). *GemOS Platform Whitepaper.* Ανάκτηση από Gem OS: https://211hzr1wjznm2pclk01j90ly-wpengine.netdna-ssl.com/wp-content/uploads/2016/10/GemOSPlatformWhitepaper.pdf

Kejriwal, S. (2017). *Blockchain in commercial real estate: The future is here!* Ανάκτηση από https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-dcfs-blockchain-in-cre-the-future-is-here.pdf

LearningMachine. (2019). *Product*. Ανάκτηση από Learning Machine: https://www.learningmachine.com/product

Lee, S. (2018, 6 8). *Blockchain Is Critical To The Future Of Data Storage - Here's Why*. Ανάκτηση από Forbes.com: https://www.forbes.com/sites/shermanlee/2018/06/08/blockchain-is-critical-to-the-future-of-data-storage-heres-why/#16b37d6333e9

Liam Bell, W. J. (2018, May). Applications of Blockchain Within Healthcare. *Blockchain In Healthcare Today*.

Marr, B. (2018, 7 16). *Here Are 10 Industries Blockchain Is Likely To Disrupt*. Ανάκτηση από Forbes.com: https://www.forbes.com/sites/bernardmarr/2018/07/16/here-are-10-industries-blockchain-is-likely-to-disrupt/#6a2d4345b5a2

Mazonka, O. (2016). Blockchain: Simple Explanation.

Medicalchain Whitepaper v2.1. (2018). Ανάκτηση από medicalchain.com: https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf

Mougayar, W. (2016). *The Business Blockchain: Promise, Practice and Application of the Next Internet Technology.* Wiley.

OpenLaw Docs. (2019, 01). Ανάκτηση από OpenLaw: https://docs.openlaw.io

Overview of Openchain. (2018). Ανάκτηση από What is Openchain: https://docs.openchain.org/en/latest/general/overview.html#what-is-openchain

Patientory Inc. | Technology. (2018). Ανάκτηση από Patientory Inc.: https://patientory.com/technology/

Popov, S. (2018). The Tangle.

Pratap, M. (2018, Aug). *Blockchain in Healthcare: Opportunities, Challenges and Applications*. Ανάκτηση από Hackernoon: https://hackernoon.com/blockchain-in-healthcare-opportunities-challenges-and-applications-d6b286da6e1f

Proof Of Burn. (2018). Ανάκτηση από Bitcoin Wiki: https://en.bitcoin.it/wiki/Proof_of_burn

Proof of Stake. (2018). Ανάκτηση από Wikipedia: https://en.wikipedia.org/wiki/Proof-of-stake

Proof-of-Work System. (2018). Ανάκτηση από Wikipedia: https://en.wikipedia.org/wiki/Proof-of-work_system

Quorum: Advancing Blockchain Technology. (2018). Ανάκτηση από J.P. Morgan: https://www.jpmorgan.com/country/GR/en/Quorum

Quorum: Ethereum for Enterprise Applications. (2017). Ανάκτηση από github.com: https://github.com/jpmorganchase/quorum-docs/blob/master/Quorum_Architecture_20171016.pdf

Ripple.com. (2019). *Ripplenet*. Ανάκτηση από Ripple: https://ripple.com/ripplenet/

Rolling your own Proof-of-Authority Ethereum consortium. (2017). Ανάκτηση από Enuma Technologies: https://blog.enuma.io/update/2017/08/29/proof-of-authority-ethereum-networks.html

Ruubel, M. (2018, May). *World's First Blockchain Platform for Marine Insurance Now in Commercial Use*. Ανάκτηση από Guardtime: https://guardtime.com/blog/world-s-first-blockchain-platform-for-marine-insurance-now-in-commercial-use

Simon, H. (2014). *Case study tracking medical devices with RFID.*

Smart Dubai launches blockchain - powered system. (2018, 09). Ανάκτηση από Smart Dubai: https://www.smartdubai.ae/newsroom/news-details/2018/09/24/smart-dubai-launches-blockchain-powered-payment-reconciliation-and-settlement-system#listingPage=1&tab=event

Srivastav, S. (2018). *A Digestible Guide to Blockchain App Development*. Ανάκτηση από AppInventiv: https://appinventiv.com/blog/blockchain-app-development-guide

Storj Labs, Inc. (2018, 10). *Storj: A Decentralized Cloud Storage Network Framework*. Ανάκτηση από Storj.io: https://github.com/storj/whitepaper

Storj: A Decentralized Cloud Storage Network Framework. (2018, 10). Ανάκτηση από Storj.io: https://storj.io/storjv3.pdf

The Future of Government on Blockchain. (2018, August). Ανάκτηση από Consensys.net: https://media.consensys.net/the-future-of-government-on-blockchain-32c8a03cf95c

The Golem Project: Crowdfunding Whitepaper. (2016, 11). Ανάκτηση από Golem Network: https://golem.network/crowdfunding/Golemwhitepaper.pdf

UBITQUITY. (2019, 01). *About UBITQUITY*. Ανάκτηση από UBITQUITY: https://www.ubitquity.io/about.html

What is Ethereum? (2016). Ανάκτηση από Ethereum.org: http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html

What is IOTA? (2018). Ανάκτηση από IOTA: https://www.iota.org/get-started/what-is-iota

What is Proof of Elapsed Time Consensus? (PoET). (2018). Ανάκτηση από Blockonomi: https://blockonomi.com/proof-of-elapsed-time-consensus/

Ye Guo, C. L. (2016). Blockchain Application and Outlook in the Banking Industry. *Financial Innovation*, 2-24.