ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

“ Η χρήση της τεχνολογίας Blockchain σε συστήματα IoT και MCS ”

“The use of Blockchain technology in IoT and MCS systems”

Ευάγγελος, Π. Ματζάνας

ΑΜ: 600

Επιβλέπουσα Καθηγήτρια: Λούτα Μαλαματή, Καθηγήτρια ΠΔΜ

Κοζάνη, Ιούλιος 2020

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

“ Η χρήση της τεχνολογίας Blockchain σε συστήματα IoT και MCS ”

“The use of Blockchain technology in IoT and MCS systems”

Ευάγγελος, Π. Ματζάνας

ΑΜ: 600

Επιβλέπουσα Καθηγήτρια: Λούτα Μαλαματή, Καθηγήτρια ΠΔΜ

Κοζάνη, Ιούλιος 2020

Περίληψη

Η δημοτικότητα και οι δυνατότητες εφαρμογής του Mobile Crowdsensing στη σημερινή εποχή αυξάνονται συνεχώς, κυρίως λόγω της ευρείας διάδοσης των κινητών συσκευών και των δυνατοτήτων ανίχνευσης και επεξεργασίας που προσφέρουν. Το Mobile Crowdsensing παρέχει τη δυνατότητα συλλογής μεγάλου όγκου δεδομένων, από κάθε κινητή συσκευή ξεχωριστά, μέσω διαφόρων τεχνικών χαμηλού, κυρίως, κόστους. Μέσω αυτού μπορεί να επιτευχθεί σημαντική βελτίωση στη συνολική εμπειρία που προσφέρουν οι κινητές συσκευές, καθώς και πολλές άλλες έξυπνες συσκευές, στα άτομα που τις χρησιμοποιούν.

Ωστόσο, πρέπει να υπάρχει παροχή των κατάλληλων κινήτρων στους χρήστες, καθώς και σιγουριά όσον αφορά τα θέματα της ασφάλειας, της ανωνυμίας και της διατήρησης της ιδιωτικότητάς τους, για να συνεχίζουν αυτοί να συμμετέχουν δίχως πρόβλημα στη συλλογή των δεδομένων. Αυτά είναι κάποια από τα χαρακτηριστικά που διαθέτει η τεχνολογία Blockchain και κάποιες πλατφόρμες, οι οποίες έχουν αναπτυχθεί με τη χρήση της τεχνολογίας αυτής. Η τεχνολογία Blockchain παρέχει ημί-ανώνυμες αλληλεπιδράσεις μεταξύ πολλαπλών μελών τους και μπορούν να χρησιμοποιηθούν και να εκμεταλλευτούν από τις εφαρμογές Crowdsensing για τη διατήρηση της ιδιωτικότητας των χρηστών των κινητών συσκευών, ενώ παράλληλα διασφαλίζεται συλλογή δεδομένων υψηλής ποιότητας.

Στην παρούσα διπλωματική εργασία μελετούνται αρχικά ξεχωριστά το Mobile Crowdsensing και η τεχνολογία Blockchain και τα χαρακτηριστικά της που μπορούμε να χρησιμοποιήσουμε σε εφαρμογές Crowdsensing. Στη συνέχεια, θα μελετήσουμε κάποιες υπάρχουσες εφαρμογές Blockchain που ήδη χρησιμοποιούνται στο Crowdsensing και θα ερευνήσουμε το τι μπορούμε να κερδίσουμε από την καθεμία, παράλληλα όμως θα δούμε και λόγους για τους οποίους το εγχείρημα της σύζευξης του Blockchain με το Crowdsensing δεν είναι ακόμα αρκετά διαδεδομένο. Τέλος, θα παρουσιάσουμε κάποιες ήδη γνωστές πλατφόρμες Blockchain και θα χρησιμοποιήσουμε τη μια από αυτές για τη δημιουργία μιας δικής μας εφαρμογής.

Λέξεις Κλειδιά

Τεχνολογία Blockchain, Mobile Crowdsensing, έξυπνα συμβόλαια, ασφάλεια, ιδιωτικότητα

Abstract

The popularity and application capabilities of Mobile Crowdsensing are constantly increasing these days, mainly due to the widespread use of mobile devices and the sensing and processing capabilities they can offer. Mobile Crowdsensing provides the ability to collect massive data information from each mobile device individually, through various low-cost manners. This can significantly improve the overall experience of mobile devices, as well as many other smart devices, to the people that use them.

However, there must be adequate incentives for users, as well as certainty about security issues, anonymity and privacy, so that they can continue to participate in data collection without any further problems. These are some of the features of Blockchain technology and some platforms that have been developed by using this technology. Blockchain technology provides semi-anonymous interactions between multiple members and can be used and exploited by Crowdsensing applications in order to maintain the privacy of mobile device users while ensuring high quality data collection.

In the following thesis, initially we study Mobile Crowdsensing and Blockchain technology separately and then the features of Blockchain that we can use in Crowdsensing applications. Next, we will look at some of the existing Blockchain applications, that are already being used in Crowdsensing and explore what we can gain from each one of them, but we will also analyze some of the reasons why the connection between Blockchain technology and Mobile crowdsensing is not yet widespread. Finally, we will present some already known Blockchain platforms and we will use one of them to create our own application.

Keywords

Blockchain technology, Mobile Crowdsensing, smart contracts, security, privacy

Πίνακας Περιεχομένων

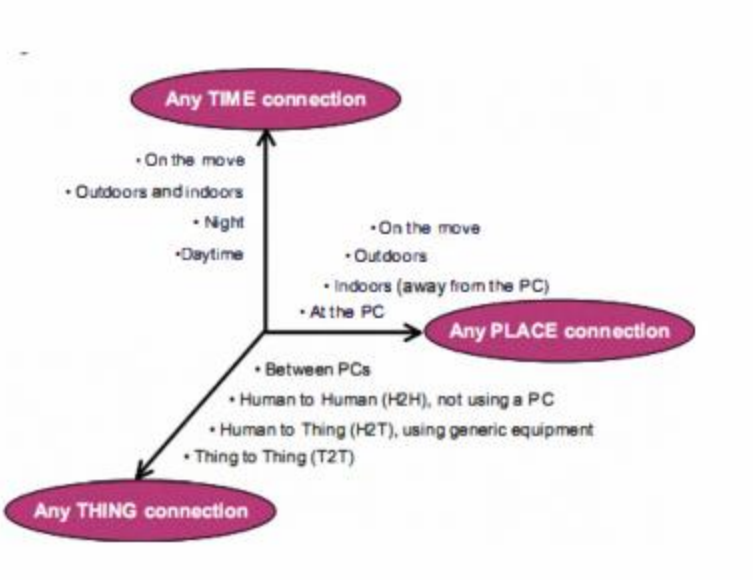
Πίνακας Συντομογραφιών

MCS	Mobile Crowdsensing
UI	User Interface
DApp	Decentralized Application
AI	Artificial Intelligence
RA	Registration Authority
DAO	Decentralized Autonomous Organization
IoT	Internet of Things
DDoS	Distributed Denial of Service
BCS	Blockchain-based Crowdsensing System
FOSS	Free and Open Source Software
API	Application Programming Interface
SDK	Software Development Kit
ΑΠ	Αρχές έκδοσης Πιστοποιητικών
CA	Certificate Authorities

Κεφάλαιο Πρώτο

1.1 Το περιβάλλον του IoT

Μέχρι σήμερα, η συντριπτική πλειονότητα των συνδέσεων στο διαδίκτυο παγκοσμίως αποτελείται από συσκευές που χρησιμοποιούνται απευθείας από ανθρώπους, όπως για παράδειγμα υπολογιστές και φορητές συσκευές. Η κύρια μορφή επικοινωνίας είναι μεταξύ ανθρώπων. Σε ένα όχι τόσο μακρινό μέλλον, όλα τα αντικείμενα θα μπορούν να συνδεθούν μεταξύ τους. Τα αντικείμενα αυτά θα μπορούν να ανταλλάξουν πληροφορίες μεταξύ τους αυτόνομα και ο αριθμός των αντικειμένων τα οποία θα είναι συνδεδεμένα στο διαδίκτυο θα είναι αρκετά μεγαλύτερος από τον αριθμό των ανθρώπων. Οι άνθρωποι μπορεί στο τέλος να γίνουν η μειοψηφία. Τα τελευταία χρόνια πραγματοποιείται ανάμιξη του φυσικού κόσμου και του κόσμου των πληροφοριών. Το μέλλον δε θα αποτελείται από ανθρώπους που θα μιλάνε με ανθρώπους, ούτε από ανθρώπους που θα έχουν πρόσβαση σε πληροφορίες. Αντιθέτως, θα αποτελείται από τη χρήση μηχανών για να υπάρχει επικοινωνία με άλλες μηχανές για λογαριασμό των ανθρώπων. Ο κόσμος μας σταδιακά εισέρχεται σε μια νέα εποχή, όπου όλοι θα μπορούν να βρίσκονται παντού ανά πάσα στιγμή, σε μια εποχή όπου θα γίνουν αντιληπτές νέες μορφές επικοινωνίας μεταξύ των ανθρώπων και των αντικειμένων, καθώς και μεταξύ των ίδιων των αντικειμένων. Η εποχή αυτή γίνεται γνωστή ως η εποχή του Internet of Things. Μια νέα διάσταση έχει προστεθεί στον κόσμο των πληροφοριών και των τεχνολογιών της επικοινωνίας, όπου θα υπάρχει οπουδήποτε και οποιαδήποτε στιγμή συνδεσιμότητα για όλους και για όλα. Η εικόνα που ακολουθεί παρουσιάζει αυτή την καινούρια διάσταση.



Εικόνα 1: Μια νέα διάσταση στο IoT

Πηγή: (https://ieeexplore.ieee.org/document/5579543) [1]

Μέχρι στιγμής δεν υπάρχει κάποια τυπική αναγνώριση για το Internet of Things. Θεωρώντας τη λειτουργικότητά του και την ταυτότητά του ως κεντρικές, φαντάζει λογικό να οριστεί ως ότι τα πράγματα έχουν ταυτότητες και εικονικές προσωπικότητες που λειτουργούν μέσα σε έξυπνους χώρους χρησιμοποιώντας έξυπνες διασυνδέσεις για να συνδεθούν και να επικοινωνήσουν μέσα σε κοινωνικά, περιβαλλοντικά και ειδικά για τους χρήστες πλαίσια. Ένας κάπως διαφορετικός ορισμός, ο οποίος δίνει έμφαση στην ανεμπόδιστη ενσωμάτωση θα μπορούσε να διατυπωθεί ως «Διασυνδεδεμένα αντικείμενα τα οποία έχουν ένα ενεργό ρόλο σε κάτι το οποίο θα μπορούσε να ονομαστεί Μελλοντικό Διαδίκτυο».

1.2 Οι κύριες τεχνολογίες του IoT

Το IoT μπορεί να χαρακτηριστεί σαν μια τεχνολογική επανάσταση, η οποία αντιπροσωπεύει το μέλλον των υπολογιστών και των επικοινωνιών, και η ανάπτυξη του χρειάζεται την υποστήριξη από μερικές καινοτόμες τεχνολογίες. Το Radio frequency identification (RFID) παρουσιάζεται ως ένας από τους βασικούς στυλοβάτες του Internet of Things. Αρχικά, τα αντικείμενα θα πρέπει να ταυτοποιούνται προκειμένου να μπορούν να συνδεθούν το ένα με το άλλο. Το RFID, το οποίο χρησιμοποιεί ραδιοκύματα για να προχωρήσει στην ταυτοποίηση διαφόρων αντικειμένων, μπορεί να παρέχει αυτή τη λειτουργία. Μερικές φορές το RFID έχει παρουσιαστεί σαν αντικαταστάτης του barcode, αλλά τα συγκεκριμένα συστήματα μπορούν να προσφέρουν πολλά

περισσότερα από αυτό. Εκτός από την ταυτοποίηση των αντικειμένων, μπορεί επίσης να εντοπίσει αντικείμενα και σε πραγματικό χρόνο, με σκοπό να λάβει σημαντικές πληροφορίες σχετικά με την τοποθεσία τους και την κατάστασή τους. Εκμεταλλευόμενο όλα τα χαρακτηριστικά που προσφέρει, το RFID έχει ήδη εφαρμοστεί σε σημαντικές εφαρμογές στους τομείς του λιανικού εμπορίου, της υγειονομικής περίθαλψης και της διαχείρισης εγκαταστάσεων. Μια ολοκληρωμένη τεχνολογία RFID μπορεί να παρέχει πολύ δυνατή και σταθερή υποστήριξη στο Internet of Things.

Μια από τις βασικότερες καινοτομίες του Internet of Things είναι η σύζευξη του φυσικού κόσμου και του κόσμου των πληροφοριών μαζί. Οι αισθητήρες παίζουν πολύ σημαντικό ρόλο στη γεφύρωση του κενού μεταξύ του φυσικού κόσμου και του κόσμου των πληροφοριών. Συλλέγουν δεδομένα από το περιβάλλον, παράγοντας έτσι άκρως πολύτιμες πληροφορίες που επηρεάζουν την ευαισθησία στον τομέα αυτόν. Με αυτό τον τρόπο, οποιεσδήποτε αλλαγές στο περιβάλλον τους μπορούν να παρακολουθούνται συνεχώς και τα αντίστοιχα αντικείμενα του περιβάλλοντος να προβούν σε συγκεκριμένες πράξεις αν χρειάζεται.

Η νανοτεχνολογία και η μικρογράφηση έχουν την ικανότητα να ενσωματώσουν νοημοσύνη σε αντικείμενα τα οποία ονομάζονται έξυπνες συσκευές (smart devices). Αυτές οι συσκευές μπορούν να επεξεργαστούν πληροφορίες, να αυτό-διαμορφωθούν, να προχωρήσουν στη λήψη αποφάσεων αυτόνομα, μέχρι σε σημείο όπου θα υπάρξει πραγματική επικοινωνία μεταξύ αντικειμένων.

1.3 Οι τάσεις στο IoT

Από μια μακρινή οπτική γωνία, η τάση ανάπτυξης στο Internet of Things περιλαμβάνει τρία βήματα: ενσωματωμένη νοημοσύνη, συνδεσιμότητα και αλληλεπίδραση.

Αρχικά, έχουμε την ενσωματωμένη νοημοσύνη, η οποία μπορεί να προχωρήσει σε ενέργειες αυτόματα. Έχουν ήδη υπάρξει πολλές εφαρμογές, για παράδειγμα: η ετικέτα RFID που έχει ενσωματωθεί σε κάποιο φαγητό μπορεί να καταγράψει τις πληροφορίες σχετικά με το συγκεκριμένο φαγητό και οι πληροφορίες αυτές μπορούν να ληφθούν με τη χρήση ενός RFID reader. Επίσης, ένα χειριστήριο για πλυντήρια μπορεί να κάνει ένα πλυντήριο να εκτελέσει το πρόγραμμά του αυτόματα. Άλλα παραδείγματα είναι τεχνητά μέλη σώματος, όπως λειτουργικά χέρια ή πόδια, συστήματα αυτόματης καθοδήγησης και εκκίνησης του κινητήρα για αυτοκίνητα, καθώς και συστήματα ελέγχου πτήσεων για αεροπλάνα. Παρόλο που όλες αυτές οι συσκευές διαθέτουν νοημοσύνη, μπορεί να παρατηρηθεί ότι δουλεύουν μόνες τους και τοπικά, χωρίς να έχουν κάποια σχέση με κάποιο δίκτυο.

Επομένως, το επόμενο βήμα είναι να μπορεί οποιαδήποτε συσκευή να συνδεθεί στο δίκτυο. Από την πλευρά των έξυπνων συνδεδεμένων συσκευών, οι έξυπνες συσκευές δεν είναι έξυπνες

επειδή είναι απλώς προικισμένες με ιδιαίτερες δυνατότητες και όλες τους οι ενέργειες είναι προ-σχεδιασμένες από άνθρωπο, είναι έξυπνες επειδή είναι συνδεδεμένες. Τα αντικείμενα μπορούν να συνδεθούν με καλώδιο αλλά και ασύρματα. Στο Internet of Things ο βασικός τρόπος σύνδεσης είναι ο ασύρματος. Με βάση την υπάρχουσα δομή, υπάρχουν πολλοί τρόποι να συνδέσει κάποιος αντικείμενα: RFID, ZigBee, WPAN, WSN, DSL, UMTS, GPRS, WiFi, WiMax, LAN, WAN, 3G κ.ά. Η σύνδεση των έξυπνων συσκευών κάνει δυνατές τις αλληλεπιδράσεις.

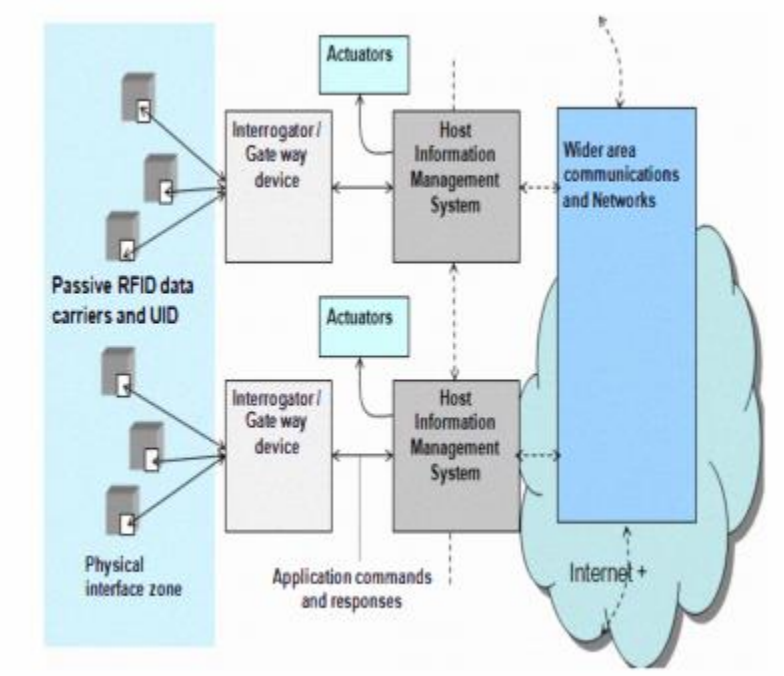
Παρόλο που μπορούμε να συνδέσουμε τα πάντα, αυτό δε σημαίνει αυτόματα και ότι τα αντικείμενα αυτά θα μπορούν να επικοινωνήσουν από μόνα τους. Επομένως, θα πρέπει να δημιουργηθούν νέα έξυπνα αντικείμενα, τα οποία θα μπορούν να επεξεργαστούν πληροφορίες, να αυτό-διαμορφωθούν, να αυτό-συντηρηθούν, να αυτό-διορθωθούν, να λαμβάνουν αποφάσεις ανεξάρτητα. Από τη στιγμή που τα αντικείμενα μπορούν να ανταλλάξουν πληροφορίες από μόνα τους, η μορφή της επικοινωνίας σταδιακά θα προσπεράσει το επίπεδο από άνθρωπο σε άνθρωπο και θα γίνει από αντικείμενο σε αντικείμενο. Όσο το Internet of Things παραμένει οδηγούμενο από εφαρμογές, θα δημιουργούνται συνεχώς νέες επιχειρηματικές εφαρμογές, οι οποίες θα μπορούν να βελτιώσουν την καινοτομία και την εξέλιξη του Internet of Things.

1.4 Η αρχιτεκτονική του IoT

Η σημερινή μορφή του διαδικτύου διαθέτει αρχιτεκτονική πέντε επιπέδων, η οποία τρέχει με πρωτόκολλα TCP/IP, τα οποία έχουν δουλέψει αποτελεσματικά για μεγάλο χρονικό διάστημα. Παρόλο αυτά, στο Internet of Things είναι συνδεδεμένα εκατομμύρια αντικείμενα, κάτι το οποίο θα προκαλέσει σταδιακά μεγαλύτερη συμφόρηση και θα χρειαστεί σίγουρα περισσότερους αποθηκευτικούς χώρους. Επιπρόσθετα με αυτά, υπάρχουν ακόμα προβλήματα όσον αφορά την ασφάλεια και τη διακυβέρνηση. Όμως, το διαδίκτυο που έχουμε σήμερα, σχεδιάστηκε τη δεκαετία του 1970 για σκοπούς που έχουν ελάχιστη σχέση με τη σημερινή του χρήση. Οι αναντιστοιχίες μεταξύ του αρχικού του σχεδιασμού και της τρέχουσας χρήσης αρχίζουν τώρα να παρεμποδίζουν την ανάπτυξη και εκμετάλλευση των πλήρων δυνατοτήτων του διαδικτύου. Επομένως, είναι αρκετά λογικό και πολύ σημαντικό να σχεδιαστεί μια νέα αρχιτεκτονική για το Internet of Things.

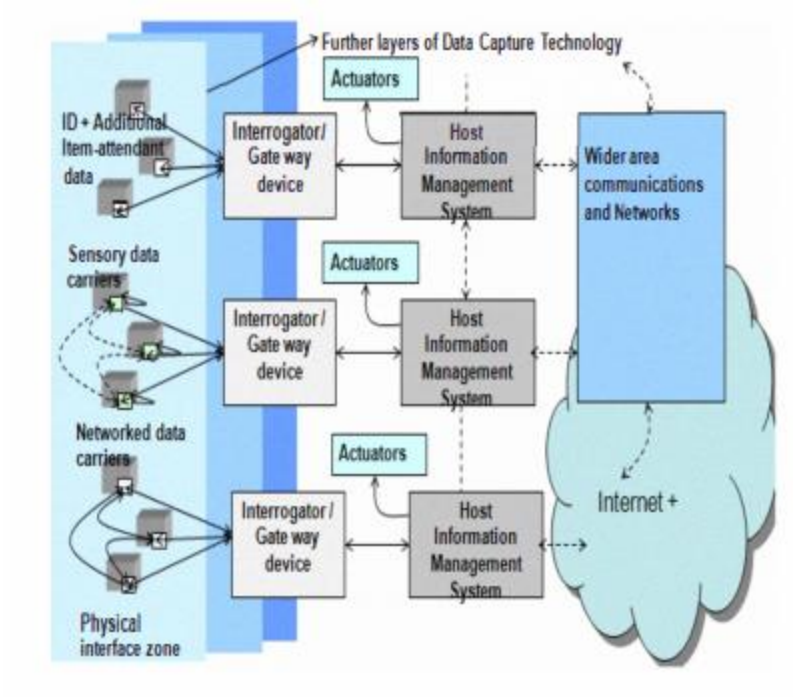
Ο επανασχεδιασμός μιας νέας αρχιτεκτονικής είναι ένα αρκετά πολύπλοκο έργο, κατά το οποίο πρέπει να ληφθούν υπόψη αρκετοί παράγοντες, όπως αξιοπιστία, σημεία σύνδεσης, δυνατότητα επέκτασης κ.ά. Σχετικά με το σχεδιασμό της αρχιτεκτονικής στο Internet of Things, αποτελεί βασικό στόχο μια αρχιτεκτονική με προσανατολισμό στις υπηρεσίες (service-oriented architecture ή SOA), αξιοποιώντας την ενοποίηση με το διαδίκτυο και τη διασύνδεση με τεχνολογίες αιχμής και τα συσχετισμένα δίκτυα. Για αυτό το στόχο, θα πρέπει να εξεταστεί το ενδεχόμενο να συμπεριληφθεί μια ολοκληρωμένη γκάμα τεχνολογιών αιχμής,

συμπεριλαμβανομένου του RFID για διασύνδεση με το φυσικό κόσμο. Επίσης, πρέπει να πραγματοποιηθεί αξιοποίηση διαφόρων εξελισσόμενων τεχνολογιών συλλογής δεδομένων οι οποίες συνδέονται με τα αντικείμενα, τοπική επικοινωνία και ασφάλεια, καθώς και ενοποίηση με το συνεχώς εξελισσόμενο διαδίκτυο και ορισμένα άλλα τεχνικά και κοινωνικό-οικονομικά θέματα. Στις εικόνες που ακολουθούν μπορεί να παρατηρηθεί το Internet of Things στο πιο βασικό του επίπεδο, μια δομή που περιλαμβάνει το RFID και άλλες τεχνολογίες αιχμής και η αρχιτεκτονική του Internet of Things.



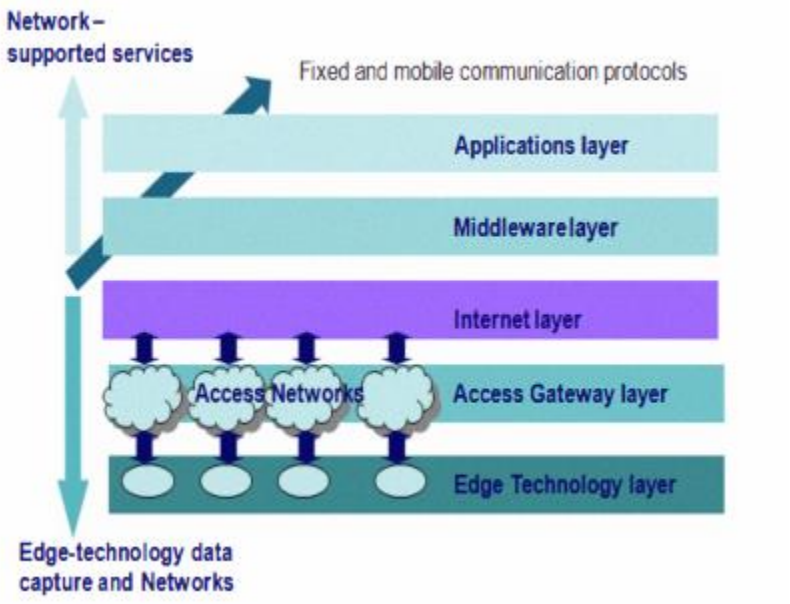
Εικόνα 2: Το IoT στο πιο βασικό του επίπεδο

Πηγή: (https://ieeexplore.ieee.org/document/5579543) [1]



Εικόνα 3: Το IoT συμπεριλαμβανομένου του RFID και άλλων τεχνολογιών αιχμής

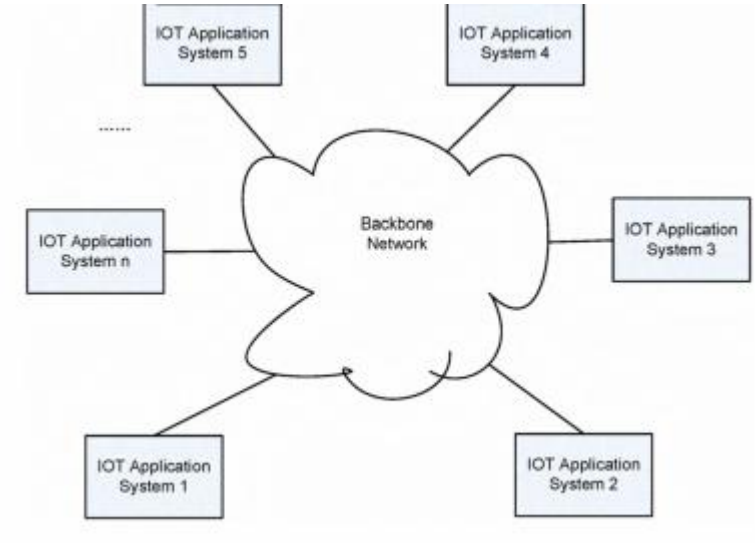
Πηγή: (https://ieeexplore.ieee.org/document/5579543) [1]



Εικόνα 4: Η αρχιτεκτονική του IoT

Πηγή: (https://ieeexplore.ieee.org/document/5579543) [1]

Έχουν γίνει αρκετές ενδιαφέρουσες προτάσεις για τη νέα αρχιτεκτονική, αλλά υπάρχουν πολλά σημαντικά θέματα για τα οποία πρέπει να βρεθεί λύση πριν προχωρήσουμε σε κάτι καινούριο. Το πρώτο θέμα είναι ότι εάν κάθε αντικείμενο είναι συνδεδεμένο και όλα τα αντικείμενα μπορούν να ανταλλάξουν πληροφορίες από μόνα τους, τότε η συμφόρηση και οι αποθηκευτικοί χώροι θα αυξηθούν ταχύτατα και εκθετικά. Η σύνδεση κάθε αντικειμένου και η ικανότητα να επικοινωνούν ανεξάρτητα είναι ένα πολύ ελκυστικό όραμα, και μπορούν σίγουρα να υπάρξουν πολλές περιπτώσεις όπου στο μέλλον δυο αντικείμενα θα πρέπει να επικοινωνήσουν το ένα με το άλλο, αλλά είναι αναγκαίο κάποιο αντικείμενο να μπορεί να μιλάει με όλα τα αντικείμενα που υπάρχουν; Συγκεκριμένα, οι βασικές συνδέσεις ενός αντικειμένου είναι με τα αντικείμενα, τα οποία βρίσκονται στο ίδιο σύστημα εφαρμογών του IoT με το συγκεκριμένο αντικείμενο. Έτσι καταλήγουμε στο ότι το Internet of Things είναι κατασκευασμένο από πολλά συστήματα εφαρμογών IoT, κάτι το οποίο μπορούμε να δούμε πιο καθαρά και στην παρακάτω εικόνα.



Εικόνα 5: Το IoT λίγο πιο καθαρά

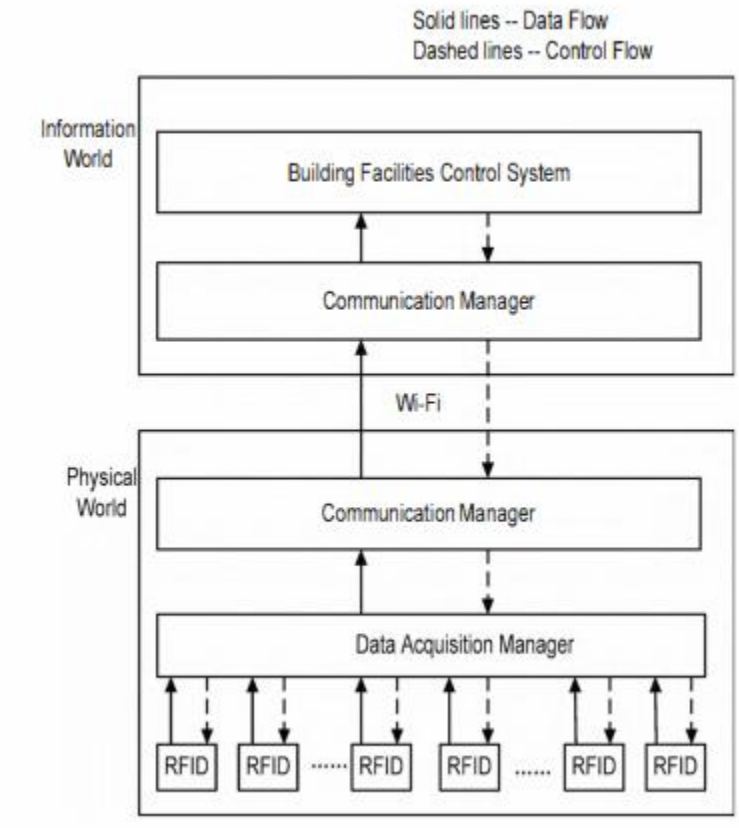
Πηγή: (https://ieeexplore.ieee.org/document/5579543) [1]

Το βασικό θέμα με τις εφαρμογές στο IoT είναι ότι ήδη υπάρχουν πολλές εφαρμογές, οι οποίες φαίνεται ότι δουλεύουν σωστά. Αλλά το πρόβλημα είναι ότι αυτά τα συστήματα εφαρμογών δουλεύουν από μόνα τους και ακόμα κι αν ένα αντικείμενο χρειάζεται να επικοινωνεί μόνο με ένα άλλο αντικείμενο του ίδιου συστήματος, αργά ή γρήγορα η τεχνολογική εξέλιξη θα ωθεί όλα τα συστήματα σε αλληλεπιδράσεις του ενός με όλα τα άλλα, ανεξάρτητα από το αν είναι αναγκαίο. Μόνο αν βρεθεί λύση στο πρόβλημα της διαλειτουργικότητας θα υπάρξει πραγματικό Internet of Things.

1.5 Παράδειγμα εφαρμογής στο IoT

Το Internet of Things δεν είναι μόνο μια θεωρία, είναι μια τεχνολογία από την οποία μπορούμε όλοι να επωφεληθούμε. Συγκεκριμένα, όπως προαναφέρθηκε, έχουν ήδη υπάρξει μερικές πετυχημένες εφαρμογές σε διάφορους τομείς όπως το λιανικό εμπόριο, το φαγητό, τα λογιστικά, οι μεταφορές. Είναι ώρα λοιπόν να περάσουμε σε ένα παράδειγμα για να δούμε πώς είναι το πραγματικό Internet of things και πώς μπορεί να βελτιώσει τις ζωές μας.

Σε μια πανεπιστημιούπολη, υπάρχουν πολλά κτήρια όπως για παράδειγμα κτήρια διδασκαλίας, κτήρια γραφείων, βιβλιοθήκη, κτήρια για σίτιση κ.ά. Σχεδόν κάθε κτήριο έχει τα δικά του συστήματα θέρμανσης, εξαερισμού, κλιματισμού και ανελκυστήρων. Όλες αυτές οι συσκευές θα πρέπει να διαχειρίζονται και να συντηρούνται αλλά αυτή η δουλειά δε γίνεται πάντα σε τέλειο επίπεδο. Εδώ μπορεί να χρησιμοποιηθεί το IoT στη διαχείριση των εγκαταστάσεων της πανεπιστημιούπολης. Στην επόμενη εικόνα βλέπουμε την αρχιτεκτονική του συστήματος αυτού.



Εικόνα 6: Η αρχιτεκτονική για διαχείριση εγκαταστάσεων

Πηγή: (https://ieeexplore.ieee.org/document/5579543) [1]

Γίνεται χρήση αρκετών ετικετών RFID στο κτήριο, οι οποίες μπορούν να παρακολουθούν τη συμπεριφορά των συστημάτων κλιματισμού και ανελκυστήρων, να συλλέξουν πληροφορίες, να αισθανθούν τις αλλαγές στο περιβάλλον τους και επίσης μπορούν να εντοπιστούν. Από τη στιγμή που ολόκληρο το πανεπιστήμιο καλύπτεται από σήμα WiFi, ο διαχειριστής συλλογής των δεδομένων κάθε κτηρίου μπορεί να μεταδώσει τα δεδομένα που έχει συλλέξει στο σύστημα ελέγχου των κτηριακών εγκαταστάσεων μέσω του WiFi. Ο υπεύθυνος επικοινωνίας έχει μια λειτουργία διασύνδεσης του φυσικού κόσμου με τον κόσμο των πληροφοριών, επομένως υπάρχει και στους δυο κόσμους. Έπειτα, το σύστημα ελέγχου του κτηρίου επεξεργάζεται τα συγκεκριμένα δεδομένα και λαμβάνει αποφάσεις βασισμένες στο αποτέλεσμα της επεξεργασίας, όπως π.χ. μπορεί να στείλει κάποιες πληροφορίες ρύθμισης πίσω στις ετικέτες RFID ή να κλείσει κάποιες μονάδες κλιματισμού. Μπορεί εύκολα να παρατηρηθεί ότι όλες οι ενέργειες μπορούν να επιτευχθούν αυτόματα χωρίς την ανθρώπινη παρέμβαση, καθώς και να πραγματοποιηθεί αποτελεσματικότερη χρήση της ενέργειας με αυτή τη μέθοδο. Επιπρόσθετα, με την ανάλυση των δεδομένων θα μπορεί να γίνει γνωστή η κατάσταση συντήρησης των εγκαταστάσεων και αν υπάρχουν μεμονωμένα προβλήματα θα μπορούσε να γίνει λήψη μέτρων για να γίνει πρόληψη της οποιασδήποτε ζημιάς που μπορεί να συμβεί [1].

Κεφάλαιο Δεύτερο

2.1 Το mobile crowdsensing

Το Mobile Crowdsensing είναι μία τεχνική κατά την οποία μια μεγάλη ομάδα ατόμων, τα οποία έχουν στην κατοχή τους κινητές συσκευές με την ικανότητα να ανιχνεύουν (sensing) και να υπολογίζουν (computing) (όπως έξυπνα κινητά τηλέφωνα, tablets, φορητές συσκευές) μοιράζονται δεδομένα συλλογικά και εξάγουν πληροφορίες για μέτρηση, χαρτογράφηση, ανάλυση, εκτίμηση ή ακόμα και πρόβλεψη διαδικασιών κοινού ενδιαφέροντος.

Η τεχνική αυτή έχει τραβήξει αρκετή προσοχή τα τελευταία χρόνια και αποτελεί ένα αξιόλογο πλέον παράδειγμα αστικής ανίχνευσης. Η κινητικότητα και η ευφυΐα των ανθρώπων είναι χαρακτηριστικά που εγγυώνται μεγαλύτερη κάλυψη και καλύτερη αντίληψη του περιβάλλοντος σε σύγκριση με τα παραδοσιακά δίκτυα αισθητήρων. Οι συσκευές στις οποίες βασίζεται το MCS έχουν γίνει αναπόσπαστο κομμάτι της καθημερινότητας των ανθρώπων και κυρίως στη δουλειά, στην επικοινωνία και στην ψυχαγωγία. Σύμφωνα με στατιστικές μελέτες, ο αριθμός των έξυπνων κινητών τηλεφώνων που πωλήθηκαν το 2018 ήταν 1.55 δισεκατομμύρια και ο αριθμός των φορητών συσκευών το ίδιο έτος έφτασε 178.91 εκατομμύρια, νούμερο το οποίο αναμένεται να ανέβει έως και τα 453.19 εκατομμύρια το 2022 [2].

Ο όρος mobile crowdsensing παρουσιάζεται πρώτη φορά από τον R. Ganti στο άρθρο «Mobile crowdsensing: current state and future challenges» [3] για να δώσει ένα πιο γενικό παράδειγμα πάνω στην ανίχνευση των κινητών συσκευών. Ο B. Guo στο άρθρο «From participatory sensing to mobile crowd sensing» επισημαίνει τη βασική διαφορά: ¨Το MCS είναι ένα νέο παράδειγμα ανίχνευσης που δίνει τη δυνατότητα στους απλούς πολίτες να συνεισφέρουν δεδομένα που ανιχνεύονται ή δημιουργούνται από τις κινητές τους συσκευές με σκοπό την εξαγωγή πληροφοριών από το πλήθος και την παροχή υπηρεσιών με επίκεντρο τους ανθρώπους¨ [4].

Το MCS είναι ένα ενδιαφέρον πλαίσιο του IoT. Με την άνευ προηγουμένου αύξηση της διαθεσιμότητας των έξυπνων κινητών τηλεφώνων και της υπολογιστικής τους ισχύος, της ποιότητας, του κόστους και της ποσότητας των αισθητήρων που έχουν εφαρμοστεί, αναδύθηκε το MCS. Τα συστήματα MCS εκμεταλλεύονται την πανταχού παρουσία των έξυπνων κινητών τηλεφώνων στο πλήθος των χρηστών για τη συλλογή δεδομένων και τη συλλογή συμπερασμάτων σχετικά με το περιβάλλον των χρηστών μέσω των αναγνώσεων που γίνονται στους αισθητήρες των έξυπνων κινητών τηλεφώνων τους.

Ένα παράδειγμα μιας εφαρμογής MCS είναι η υπηρεσία Waze που παρέχει πληροφορίες σε πραγματικό χρόνο σχετικά με την κυκλοφοριακή συμφόρηση και τις οδικές συνθήκες, συλλέγοντας ευκαιριακά τα δεδομένα που απαιτούνται όταν ο χρήστης βρίσκεται σε μια

συγκεκριμένη τοποθεσία ή με τη συμμετοχή του καθώς υποβάλλει αναφορές σχετικά με τις οδικές συνθήκες.

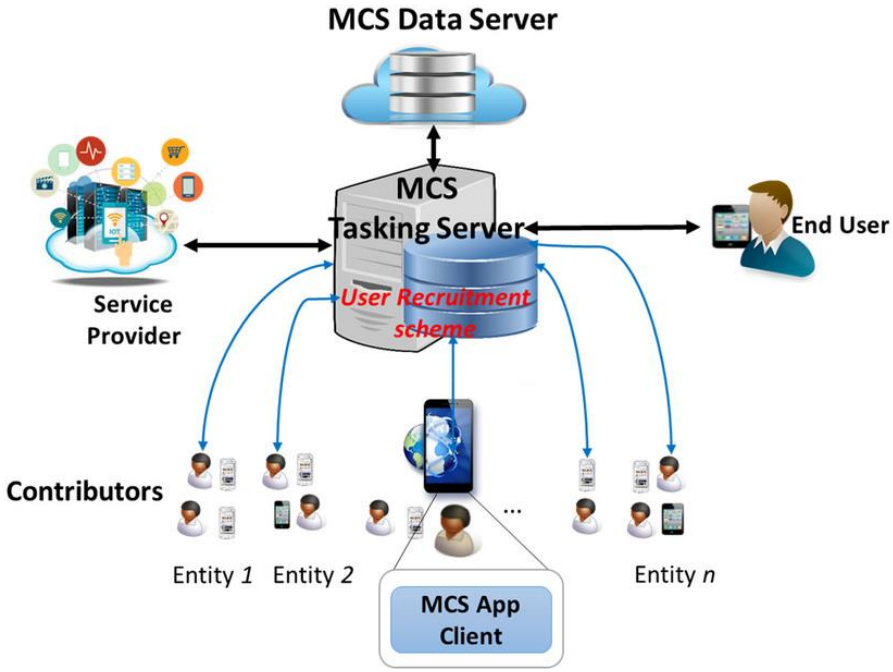
Το MCS είναι σχετικά νέο, καθώς παρουσιάστηκε πρώτη φορά στην αρχή της δεκαετίας του 2010. Ωστόσο, υπήρχαν ορισμένα συστήματα πριν από αυτό που πραγματοποιούσαν παρόμοιες εργασίες, όπως το Google Traffic το οποίο χρησιμοποιούσε από το 2007 δεδομένα GPS από κινητές συσκευές που διέθεταν σύστημα GPS. Σε ένα σύστημα MCS, οι χρήστες των έξυπνων κινητών τηλεφώνων θα έδιναν αδειοδότηση στις εφαρμογές του MCS να συλλέγουν δεδομένα από τους αισθητήρες των κινητών τους, συμφωνώντας με αυτό τον τρόπο να συμμετέχουν σε εργασίες ανίχνευσης, οι οποίες εκπληρώνονται με αντάλλαγμα κάποιο κίνητρο-πληρωμή ή κάποια υπηρεσία. Ωστόσο, ο αριθμός των διαθέσιμων χρηστών σε μια συγκεκριμένη τοποθεσία ενδέχεται να μην είναι επαρκής, γεγονός που οδηγεί σε καταστάσεις όπου τα δεδομένα είναι λιγοστά, περιορισμένα ή αραιοκατανεμημένα. Σε μια τέτοια περίπτωση, το σύστημα MCS θα πρέπει να είναι ικανό να αξιοποιήσει τα μέγιστα, χρησιμοποιώντας τεχνικές που λειτουργούν με μικρά σύνολα δεδομένων.

Επίσης, από οικονομική άποψη, η συλλογή των δεδομένων συνήθως περιλαμβάνει τη χρήση πόρων (ή πληρωμών), ειδικότερα στο συμμετοχικό MCS. Είναι επιθυμητό για το σύστημα MCS να μειώσει την απαιτούμενη ανίχνευση, βελτιστοποιώντας με αυτό τον τρόπο το κόστος του συστήματος, με τον περιορισμό της διατήρησης της ποιότητας των ανιχνεύσεων. Ο χαρακτηρισμός του λιγότερου αριθμού μετρήσεων (ή αισθητήρων) θα ήταν ένα μεγάλο όφελος για τους χειριστές και τους υπεύθυνους λήψης αποφάσεων [5].

2.2 Αρχιτεκτονική ενός συστήματος με χρήση MCS

Η γενική αρχιτεκτονική δομή ενός συστήματος MCS περιλαμβάνει τις ακόλουθες βασικές οντότητες: *α)* τους Αιτούντες, *β)* τους Εργάτες και *γ)* την Πλατφόρμα Crowdsensing. Οι αιτούντες υποβάλλουν αιτήσεις ανίχνευσης (sensing) σχετικά με τα συμφέροντά τους στην πλατφόρμα crowdsensing. Έπειτα, βλέπουν τις απαντήσεις που παρέχονται από τους εργάτες και λαμβάνουν πρόσβαση στις γνώσεις που αποκτήθηκαν αφότου η πλατφόρμα έχει αναλύσει όλα τα δεδομένα που συλλέχθηκαν. Οι αιτούντες μπορούν να αξιολογήσουν τους εργάτες με βάση τις απαντήσεις τους και ανάλογα το υιοθετημένο μοντέλο κινήτρων παρέχουν την ανάλογη ανταμοιβή στους εργάτες. Οι εργάτες είναι η βασική πηγή πληροφοριών και παίζουν μεγάλο ρόλο στη συλλογή των δεδομένων. Ανάλογα με το υποτιθέμενο μοντέλο, μπορούν να τους ανατεθούν διάφορες εργασίες, λαμβάνοντας πάντα υπόψη τις προτιμήσεις των ιδιοκτητών τους και τις απαιτήσεις τόσο των αιτούντων όσο και της πλατφόρμας crowdsensing. Πολύ σημαντικό στοιχείο αποτελεί το ότι οι ίδιοι οι εργάτες μπορούν να επιλέξουν σε ποια εργασία θέλουν να

συμμετάσχουν και να συνεισφέρουν. Η πλατφόρμα crowdsensing είναι ο βασικός σύνδεσμος επικοινωνίας μεταξύ των αιτούντων και των εργατών. Η πλατφόρμα αποθηκεύει, επεξεργάζεται και αναλύει δεδομένα, τα οποία παρέχονται από τους εργάτες και τους αιτούντες και ανάλογα το υιοθετημένο μοντέλο κινήτρων παρέχει στους εργάτες την ανταμοιβή τους. Στην παρακάτω εικόνα βλέπουμε την αρχιτεκτονική ενός δικτύου με την χρήση του MCS.



Εικόνα 7 : Αρχιτεκτονική MCS

Πηγή: (https://www.researchgate.net/figure/Mobile-Crowd-Sensing-System-Architecture_fig7_317485310)

2.3 Χαρακτηριστικά εφαρμογών με χρήση MCS

Οι εφαρμογές του MCS έχουν κάποια μοναδικά χαρακτηριστικά, τα οποία τις κάνουν να διαφέρουν από τα παραδοσιακά δίκτυα αισθητήρων. Σε σύγκριση με τα παραδοσιακά δίκτυα, το MCS έχει έναν αριθμό μοναδικών χαρακτηριστικών, τα οποία επιφέρουν καινούριες ευκαιρίες αλλά και προβλήματα. Αρχικά, οι σημερινές κινητές συσκευές έχουν αρκετά περισσότερους υπολογιστικούς, επικοινωνιακούς και αποθηκευτικούς πόρους από τους παραδοσιακούς αισθητήρες και είναι συνήθως εξοπλισμένες με δυνατότητες ανίχνευσης πολλαπλών τρόπων. Αυτές ενεργοποιούν πολλές εφαρμογές, οι οποίες απαιτούν πόρους και δυνατότητες ανίχνευσης που δεν κατέχουν οι παραδοσιακοί αισθητήρες. Επίσης, εκατομμύρια κινητές συσκευές είναι ήδη σε χρήση στο πεδίο, αφού οι άνθρωποι τις μεταφέρουν μαζί τους όπου κι αν πάνε, οτιδήποτε κι αν κάνουν. Εκμεταλλευόμενοι αυτές τις συσκευές, οι ειδικοί θα μπορούσαν να

δημιουργήσουν αποδοτικές εφαρμογές ανίχνευσης μεγάλης κλίμακας. Για παράδειγμα, αντί για την εγκατάσταση καμερών στους δρόμους, μπορεί να γίνει συλλογή δεδομένων της κίνησης στους δρόμους, καθώς και ανίχνευση κυκλοφοριακής συμφόρησης χρησιμοποιώντας τα έξυπνα κινητά τηλέφωνα που μεταφέρουν μαζί τους οι οδηγοί. Τέτοιου είδους λύσεις μειώνουν το κόστος εγκατάστασης ειδικών δομών ανίχνευσης [6].

Ο βαθμός συμμετοχής των χρηστών όσον αφορά τη συλλογή δεδομένων εμφανίζει διαφορές με βάση τις απαιτήσεις κάθε εφαρμογής. Επομένως, το MCS επιτρέπει την άμεση καθώς και την έμμεση συμμετοχή του κάθε χρήστη στη διαδικασία συλλογής δεδομένων, αξιοποιώντας είτε τη συμμετοχική ανίχνευση (participatory sensing), είτε την ευκαιριακή ανίχνευση (opportunistic sensing). Προκειμένου να γίνει ευκολότερα κατανοητό, πρέπει να εξηγηθεί ότι στη συμμετοχική ανίχνευση, ο κάθε χρήστης θα πρέπει να πραγματοποιεί μια δήλωση ότι επιλέγει συνειδητά να συμμετέχει. Επίσης, μοιάζει απαραίτητη η παροχή της υπηρεσίας του και ο ίδιος έχει τη δυνατότητα να επιλέξει τη χρονική στιγμή, το μέρος και τον τρόπο με τον οποίο θέλει να λάβει μέρος στη συλλογή των πληροφοριών. Αντίθετα, στην ευκαιριακή ανίχνευση, ο κάθε χρήστης συμμετέχει ελάχιστα ή και καθόλου και η συλλογή δεδομένων συμβαίνει στο παρασκήνιο.

Ένα ακόμα χαρακτηριστικό του MCS αποτελεί η εκμετάλλευση και η συγκέντρωση αρκετών πληροφοριών από ετερογενείς πηγές. Αρχικά, πραγματοποιεί αξιοποίηση δεδομένων τόσο από τους αισθητήρες που διαθέτουν οι κινητές συσκευές των χρηστών, όσο και από την άμεση συμμετοχή τους, όπως π.χ. όταν μοιράζονται τη γνώμη τους, καθώς επίσης και από τον τεράστιο όγκο πληροφοριών τις οποίες παρέχουν οι χρήστες στα μέσα κοινωνικής δικτύωσης. Στην εποχή μας υπάρχουν πολλές εφαρμογές, που συλλέγουν δεδομένα από τα μέσα κοινωνικής δικτύωσης για την παρακολούθηση κάποιου γεγονότος. Εξαιτίας της μεγάλης ποσότητας πληροφοριών τις οποίες παρέχουν οι ετερογενείς πηγές, το MCS μπορεί να γνωρίζει ανά πάσα στιγμή διάφορες προσωπικές πληροφορίες του κάθε χρήστη, όπως για παράδειγμα την τωρινή θέση του, την κατάστασή του, την καθημερινή του ρουτίνα και τις κοινωνικές του αλληλεπιδράσεις. Με παρόμοιο τρόπο, το MCS καταφέρνει να συλλέξει πληροφορίες σχετικές με τη συσκευή του χρήστη, όπως το επίπεδο της μπαταρίας και όλους τους πόρους που μπορεί να διαθέσει. Επιπρόσθετα, έχει την ικανότητα να συλλέξει πληροφορίες για κάποιο συγκεκριμένο μέρος, όπως για παράδειγμα τα επίπεδα της κινητικότητας σε μια συγκεκριμένη στάση λεωφορείου. Τέλος, με σκοπό κυρίως τη βελτίωση της ποιότητας των δεδομένων, μπορεί να γίνει συλλογή πληροφοριών και από διάφορες επίσημες πηγές, δηλαδή διάφορες δημόσιες αρχές.

Το αποτέλεσμα είναι ότι με το MCS υπάρχει δυνατότητα αξιοποίησης των διαθέσιμων δεδομένων τόσο εικονικά, δηλαδή από ορισμένα δεδομένα τα οποία έχουν μοιραστεί οι χρήστες στα μέσα κοινωνικής δικτύωσης, όσο και φυσικά, δηλαδή δεδομένα τα οποία έχει προσθέσει ο ίδιος ο χρήστης ή δεδομένα των οποίων η συλλογή έχει γίνει μέσω των αισθητήρων των κινητών συσκευών των χρηστών. Ωστόσο, οι συγκεκριμένες πληροφορίες έχουν διαφορετικά χαρακτηριστικά και ως αποτέλεσμα δημιουργούν νέες προκλήσεις στο σχεδιασμό συστημάτων MCS, οι οποίες έχουν ως στόχο την αποτελεσματική συγχώνευση των δεδομένων. Έτσι, η

συμμετοχή των χρηστών στη διαδικασία συλλογής δεδομένων έχει ως αποτέλεσμα την ανάμιξη της ανθρώπινης και της μηχανικής νοημοσύνης, πάνω στην οποία η προσπάθεια για μεγαλύτερη αποδοτικότητα αποτελεί βασικό θέμα στη σωστή ανάπτυξη των συστημάτων MCS. Οι άνθρωποι, από τη μια πλευρά, διαθέτουν τις απαραίτητες δυνατότητες για καλύτερη κατανόηση των ενεργειών που είναι αναγκαίο να εκτελεστούν, αλλά δε διαθέτουν τις κατάλληλες δυνατότητες όσον αφορά την ταχύτητα και την αποθήκευση, παράλληλα με τη συχνή εισαγωγή λαθών στα συστήματα. Από την άλλη πλευρά, υπάρχει το ακριβώς αντίθετο σενάριο. Οι μηχανές διαθέτουν τις καλύτερες ικανότητες σχετικά με την αποθήκευση και τον υπολογισμό, αλλά δεν έχουν την ικανότητα να προσδιορίσουν και να αποκτήσουν γνώσεις για όλα τα φαινόμενα που μπορεί να συναντήσουν. Επομένως, μπορεί να γίνει χρήση των μηχανών για την ανάθεση εργασιών στους χρήστες και οι χρήστες στη συνέχεια να συλλέγουν τα δεδομένα.

Λόγω της ανθρώπινης ανάμιξης στην ανταλλαγή δεδομένων, παρουσιάζονται πρωτοφανείς ευκαιρίες για την ανίχνευση και για τη μετάδοση των δεδομένων. Σχετικά με τη μετάδοση, μπορούν να αξιοποιηθούν από τους χρήστες διάφορες τεχνικές , όπως τα αυτοοργανωμένα δίκτυα ή τα ευκαιριακά δίκτυα και τα δίκτυα που βασίζονται στις υποδομές. Έτσι οι χρήστες μπορούν να πραγματοποιήσουν ευκαιριακή μετάδοση δεδομένων μέσω επικοινωνιών μικρής εμβέλειας, όπως το Bluetooth και το Wi-Fi, ή μετάδοση που βασίζεται στις υποδομές, κατά την οποία οι χρήστες ανεβάζουν δεδομένα μέσω του διαδικτύου από τα διάφορα δίκτυα κινητής τηλεφωνίας που υπάρχουν. Μεγάλη έκπληξη παρουσιάζει το γεγονός ότι οι εφαρμογές MCS μπορούν να είναι ανεκτικές στο θέμα των διακοπών του δικτύου.

Καταλήγοντας, ακόμα ένα χαρακτηριστικό των συστημάτων MCS είναι οι δυναμικές συνθήκες των κινητών συσκευών και η δυνατότητα επαναχρησιμοποίησης των δεδομένων που έχει συνεισφέρει μέχρι στιγμής ο κάθε χρήστης, σκοπεύοντας στην εξαγωγή πληροφοριών υψηλού επιπέδου. Αυτό σημαίνει ότι έχει γίνει χρήση διαφόρων κοινών δεδομένων σε διαφορετικές εφαρμογές και έχει πραγματοποιηθεί ανάλυσή τους με διαφορετικό τρόπο, αφού διαφορετικές εργασίες ανίχνευσης μπορούν να ολοκληρωθούν από την ίδια συσκευή, έχοντας ωστόσο διαφορετικές απαιτήσεις [7].

Στην παράγραφο που ακολουθεί θα αναλυθεί εκτενέστερα η χρήση ενός συστήματος MCS σε αντίθεση με ένα παραδοσιακό σύστημα αισθητήρων.

2.4 Σύγκριση MCS με παραδοσιακά δίκτυα αισθητήρων

Οι δυναμικές συνθήκες του συνόλου των κινητών συσκευών και η ανάγκη για την επαναχρησιμοποίηση δεδομένων σε διαφορετικές εφαρμογές μέσα στο MCS παρουσιάζουν επίσης αρκετές διαφορές με αυτές των παραδοσιακών δικτύων αισθητήρων. Στο MCS, ο πληθυσμός των κινητών συσκευών, ο τύπος των δεδομένων από τους αισθητήρες που μπορεί να

παράγει η κάθε συσκευή και η ποιότητα όσον αφορά την ακρίβεια, την αδράνεια, την αυτοπεποίθηση, μπορεί να αλλάζει συνεχώς εξαιτίας της κινητικότητας των συσκευών καθώς και των διαφορών στα επίπεδα ενέργειας και στα κανάλια επικοινωνίας, παράλληλα με τις προτιμήσεις του χρήστη της συσκευής. Το να προσδιορίσει κάποιος το σωστό σύνολο συσκευών που μπορούν να παράγουν τα επιθυμητά δεδομένα και να τις καθοδηγεί στο να ανιχνεύουν με τις κατάλληλες παραμέτρους για να διασφαλιστεί η επιθυμητή ποιότητα είναι ένα πολύ σύνθετο πρόβλημα.

Στα παραδοσιακά δίκτυα αισθητήρων, ο πληθυσμός και τα δεδομένα τα οποία μπορεί να παράγει είναι επί το πλείστον γνωστά εκ των προτέρων και με αυτό τον τρόπο ο έλεγχος της ποιότητας των δεδομένων είναι αρκετά ευκολότερος. Τα ίδια δεδομένα ανίχνευσης έχουν χρησιμοποιηθεί για διαφορετικούς σκοπούς σε ήδη υπάρχουσες εφαρμογές MCS. Για παράδειγμα, μετρήσεις του επιταχυνσιόμετρου έχουν βρει χρήση στην αναγνώριση του μέσου μεταφοράς, στην εύρεση λακκουβών στους δρόμους και στο μοτίβο των δραστηριοτήτων των ανθρώπων. Για την αποδοτική υποστήριξη πολλαπλών ταυτόχρονων εφαρμογών, είναι πολύ σημαντικό να διαπιστωθεί η ανάγκη κοινών δεδομένων και να στηριχθεί η επαναχρησιμοποίηση των δεδομένων των αισθητήρων ανάμεσα στις εφαρμογές. Εν αντιθέσει, ένα συμβατικό δίκτυο αισθητήρων προορίζεται συνήθως για μια και μοναδική εφαρμογή και η επαναχρησιμοποίηση για διαφορετικούς σκοπούς χρειάζεται σπάνια.

Επειδή οι συσκευές ανήκουν και μεταφέρονται από μεμονωμένους χρήστες, οι άνθρωποι συνήθως συμπεριλαμβάνονται στους βρόγχους. Αφενός, η ευφυΐα και η κινητικότητα των ανθρώπων μπορεί να χρησιμοποιηθεί για να βοηθήσει τις εφαρμογές να συλλέγουν υψηλότερης ποιότητας ή πιο περίπλοκα δεδομένα, τα οποία υπό άλλες συνθήκες απαιτούν εξειδικευμένα υλικά και λογισμικά. Για παράδειγμα, οι άνθρωποι μπορούν με ευκολία να αναγνωρίσουν τις ελεύθερες θέσεις πάρκινγκ και να αναφέρουν με φωτογραφίες ή γραπτά μηνύματα, ενώ ένα σύστημα σάρωσης βασισμένο σε υπέρηχους, όχι μόνο απαιτεί ειδικά υλικά αλλά και εξειδικευμένους αλγορίθμους επεξεργασίας για να διασφαλιστεί η αξιοπιστία των δεδομένων.

2.5 Η Ασφάλεια στη χρήση του MCS

Όπως με κάθε νέα τεχνολογία, οι άνθρωποι είναι φυσικό να έχουν ανησυχίες σχετικά με τα θέματα ιδιωτικότητας καθώς και προσωπικές προτιμήσεις που δεν είναι απαραίτητα ευθυγραμμισμένες με τους τελικούς στόχους των εφαρμογών του MCS. Ο χρήστης μπορεί να μη θέλει να μοιραστεί δεδομένα τα οποία περιέχουν ή φανερώνουν διάφορες ιδιωτικές ή ευαίσθητες πληροφορίες, όπως για παράδειγμα την τωρινή τους τοποθεσία [6].

Στο MCS λοιπόν, η συλλογή και η διανομή των δεδομένων απαιτεί την ανθρώπινη ανάμειξη. Αφενός, ένας χρήστης μπορεί να συμμετέχει ενεργά σε εργασίες ανίχνευσης, οι οποίες απαιτούν τις σαφείς ενέργειές του έτσι ώστε να ολοκληρωθεί η εργασία (π.χ. τη λήψη κάποιας φωτογραφίας), που αναφέρεται στη συμμετοχική ανίχνευση. Αφ' ετέρου, η καιροσκοπική ανίχνευση δεν απαιτεί σαφείς ενέργειες από το χρήστη για να εκτελεστεί μια εργασία ανίχνευσης. Η εργασία εκτελείται στο παρασκήνιο, χωρίς τη ρητή συμμετοχή των χρηστών. Παρομοίως, σύμφωνα με το μοντέλο *pull*, απαιτείται από τους χρήστες να λαμβάνουν τις ενεργές εργασίες και να επιλέγουν αυτές στις οποίες θέλουν να συνεισφέρουν, ενώ στο μοντέλο *push*, ο έλεγχος του χρήστη είναι μειωμένος και οι εργασίες προωθούνται στις κινητές συσκευές όταν τηρούνται συγκεκριμένες προϋποθέσεις και κριτήρια. Τα δεδομένα μπορούν να συλλέγονται τόσο από φυσικούς όσο και από διαδικτυακούς κόσμους, έτσι ώστε να ενσωματωθούν και να αξιοποιηθούν τα συμπληρωματικά χαρακτηριστικά και τα πλεονεκτήματά τους. Όσον αφορά τη μετάδοση των δεδομένων, οι χρήστες μπορούν να υιοθετήσουν μια συμπεριφορά αποθήκευσης και μεταφοράς, περιμένοντας έως ότου παρουσιαστεί μια καλύτερη ευκαιρία μετάδοσης (καιροσκοπική μετάδοση) ή όταν μπορέσουν να χρησιμοποιήσουν ένα σύστημα επικοινωνίας (μετάδοση βάση υποδομής) [8].

Οι συγγραφείς στο [9] παρουσιάζουν το MalloDroid, έναν αναλυτή κώδικα τον οποίο χρησιμοποίησαν για να τεστάρουν 13.500 διάσημες και δωρεάν εφαρμογές Android για τυχόν αδυναμίες ασφαλείας ενάντια σε επιθέσεις Man-in-the-Middle. Προσπάθησαν να εστιάσουν την ανάλυσή τους στα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται από τις εφαρμογές (π.χ. HTTP ή HTPS). Τα αποτελέσματα της ανάλυσής τους έδειξαν ότι 1074 από όλες τις εφαρμογές είχαν αδύναμους SSL/TLS κώδικες, κάτι που τις καθιστά ευάλωτες σε επιθέσεις Man-in-the-Middle. Επιπρόσθετα, κάποιες καταχρήσεις εντοπίστηκαν από τους συγγραφείς ενώ πραγματοποιούσαν χειροκίνητη ανάλυση σε 100 επιλεγμένες εφαρμογές συμπεριλαμβανομένων και 41 εφαρμογών που μετέδιδαν ευαίσθητες πληροφορίες των χρηστών. Είχαν καταφέρει να καταγράψουν διαπιστευτήρια σύνδεσης των περισσότερων εφαρμογών και επίσης μπορούσαν να εισάγουν και να εκτελέσουν κώδικα σε μια εφαρμογή, η οποία είχε αναπτυχθεί με τη χρήση μιας ευάλωτης δομής ανάπτυξης εφαρμογών.

Στο άρθρο [10] οι συγγραφείς παρουσιάζουν το SMV-HUNTER, ένα σύστημα το οποίο αναλύει αυτόματα εφαρμογές Android μεγάλης κλίμακας. Το σύστημα αποτελείται από ένα μέρος στατικής ανάλυσης, το οποίο αναγνωρίζει πιθανές ευάλωτες εφαρμογές και ένα μέρος δυναμικής ανάλυσης, το οποίο επικυρώνει την ευάλωτη κατάσταση των εφαρμογών. Η αποδοτικότητα αυτού του συστήματος δοκιμάστηκε με 23.418 εφαρμογές από το Google Play Store, όπου η στατική ανάλυση εντόπισε 1453 πιθανές ευάλωτες εφαρμογές και η δυναμική ανάλυση απέδειξε ότι 726 από αυτές ήταν πραγματικά ευάλωτες.

Ακόμα μια έρευνα ασφαλείας πραγματοποιείται στο [11]. Οι συγγραφείς ερευνούν το ρίσκο της ασφάλειας και της ιδιωτικότητας σε εφαρμογές mHealth βασισμένες στο Android. Η έρευνα βασίστηκε στα ακόλουθα: 1) πιθανές επιφάνειες επίθεσης, 2) κλιμάκωση απειλής, 3)

σοβαρότητα απειλής. Στο πρώτο στάδιο, αναλύθηκαν 160 εφαρμογές από το Google Play Store, οι οποίες περιλάμβαναν 80 δωρεάν εφαρμογές με θέμα την υγεία και τη φυσική κατάσταση και 80 δωρεάν ιατρικές εφαρμογές. Από τις επιφάνειες επίθεσης που αναγνωρίστηκαν, οι συγγραφείς παρουσίασαν τις περιοχές που χρειάζονται ασφάλεια, οι οποίες ήταν: υπηρεσίες τρίτων μελών, διαδίκτυο, σύνδεση, Bluetooth, αποθηκευτικός χώρος κάρτας SD, εξαγόμενα στοιχεία και πλευρικά κανάλια. Στο δεύτερο στάδιο, επέλεξαν 27 εφαρμογές για ανάλυση και παρουσίασαν 3 επιφάνειες επίθεσης που χρειάζονται ασφάλεια: διαδίκτυο, υπηρεσίες τρίτων μελών και σύνδεση. Στο τρίτο και τελικό στάδιο, επιλέχθηκαν και αναλύθηκαν 120 εφαρμογές, οι οποίες μεταδίδουν ευαίσθητες πληροφορίες, για να διευκρινιστεί η σοβαρότητα της μετάδοσης ευαίσθητων πληροφοριών μέσω διαδικτυακών επικοινωνιών. Τα αποτελέσματα έδειξαν ότι η πλειοψηφία των εφαρμογών που δοκιμάστηκαν μεταδίδουν μη κρυπτογραφημένα δεδομένα στο διαδίκτυο και επίσης χρησιμοποιούν αποθηκευτικούς χώρους τρίτων μελών και υπηρεσίες φιλοξενίας.

2.6 Προκλήσεις στο MCS

Το MCS ως νέα τεχνολογία, η οποία ακόμα αναπτύσσεται και εξελίσσεται, παρουσιάζει καθημερινά προκλήσεις οι οποίες δυσκολεύουν τη χρήση του και αλλοιώνουν την εμπειρία των χρηστών. Οι ομάδες των κινητών συσκευών, οι ικανότητες τους για ανίχνευση, υπολογισμούς, αποθήκευση και επικοινωνία μπορεί να διαφέρουν αισθητά εξαιτίας της κινητικότητας των συσκευών, των διαφορών στα ενεργειακά τους επίπεδα, της κατάστασης των καναλιών επικοινωνίας καθώς και των προτιμήσεων του κάθε χρήστη. Επομένως, ο εντοπισμός και ο προγραμματισμός εργασιών ανίχνευσης σε πολλές συσκευές με διαφορετικές δυνατότητες ανίχνευσης και διαθεσιμότητα/περιορισμούς πόρων που επιβάλλονται κάποιες φορές, αποτελεί ένα πολύ περίπλοκο και απαιτητικό ζήτημα που πρέπει να αντιμετωπιστεί.

Σε αυτό το πλαίσιο, πρέπει επίσης να ληφθεί υπόψη το γεγονός ότι οι τρέχουσες ικανότητες και το πλαίσιο λειτουργίας των συσκευών μπορεί να οδηγήσουν σε υψηλότερη ή χαμηλότερη ποιότητα δεδομένων από την άποψη της ακρίβειας και της εμπιστοσύνης. Επιπρόσθετα, διαφορετικοί τύποι δεδομένων μπορούν να παραχθούν από την ανίχνευση και να χρησιμοποιηθούν για την εξυπηρέτηση του ίδιου σκοπού, με τον καθένα να χρειάζεται διαφορετική ποιότητα δεδομένων και να απαιτεί διαφορετικά επίπεδα κατανάλωσης πόρων. Επομένως, η βελτίωση στα επίπεδα της ποιότητας των δεδομένων, παράλληλα με την ελαχιστοποίηση της κατανάλωσης πόρων που χρειάζονται είναι ακόμα ένα εμπόδιο που ψάχνει λύση. Οι υπάρχουσες λύσεις υιοθετούν κύκλους χαμηλής λειτουργίας για τους αισθητήρες που

παράγουν δεδομένα υψηλής ποιότητας (απαιτούν σχετικά υψηλά επίπεδα ενέργειας) και αποφασίζουν για τους αισθητήρες που θα χρησιμοποιηθούν κάθε φορά με βάση τα διαθέσιμα επίπεδα ενέργειας των συσκευών. Οι προτεινόμενες λύσεις, ωστόσο, θα πρέπει να λάβουν υπόψη το γεγονός ότι ένα πλήθος διαφορετικών εφαρμογών MCS που απαιτούν τους ίδιους τύπους δεδομένων, μπορούν να συνυπάρχουν ταυτόχρονα. Έτσι, είναι εξαιρετικά σημαντικό να εντοπίσουμε κοινές ανάγκες δεδομένων, να επιτρέψουμε την κοινή χρήση δεδομένων σε διαφορετικές εφαρμογές και ακόμη να δώσουμε προτεραιότητα στη συλλογή δεδομένων με βάση τον αριθμό και τις προτεραιότητες των αιτήσεων.

Η τοπική επεξεργασία των συλλεγόμενων δεδομένων σε κινητές συσκευές, πριν γίνει συγκέντρωση και επεξεργασία αυτών στο τελικό στάδιο προκειμένου να επιτευχθεί μια μορφή κατάλληλη για κατανάλωση από εφαρμογές, μπορεί επίσης να αποτελεί μια λύση στους περιορισμούς των πόρων των συσκευών, καθώς τα παραγόμενα ενδιάμεσα αποτελέσματα απαιτούν λιγότερη ενέργεια και εύρος ζώνης για τη μετάδοσή τους. Η υποκείμενη πρόκληση από αυτή την άποψη είναι ο σχεδιασμός κατάλληλων αλγορίθμων και ο προσδιορισμός κοινών τοπικών απαιτήσεων επεξεργασίας σε διαφορετικές εφαρμογές MCS [12].

Τα κίνητρα θα μπορούσαν να θεωρηθούν μια σημαντική επίπτωση στην ανθρώπινη συμμετοχή. Αναλυτικότερα, οι συσκευές που παίρνουν μέρος ενδέχεται να ξοδέψουν ενέργεια, να έχουν κάποιο χρηματικό κόστος ή μπορεί ακόμα και οι κάτοχοι των συσκευών να πραγματοποιήσουν ρητές προσπάθειες για την ανίχνευση, επεξεργασία και επικοινωνία των επιθυμητών δεδομένων. Σε αυτές τις περιπτώσεις, εάν δεν υπάρχουν αρκετά ισχυρά κίνητρα, οι ιδιοκτήτες ενδέχεται να μην είναι πρόθυμοι να συνεισφέρουν τους πόρους τους. Για να καταφέρουν οι εφαρμογές του MCS να πετύχουν, πρέπει να υπάρχουν κατάλληλοι μηχανισμοί κινήτρων για την πρόσληψη, τη δέσμευση και τη διατήρηση των ανθρώπων που συμμετέχουν [6].

Επιπλέον, η αρχιτεκτονική του MCS θα πρέπει να λάβει υπόψη και να αντιμετωπίσει αποτελεσματικά την περίπτωση δυνητικά ανακριβών/λανθασμένων δεδομένων. Οι εφαρμογές MCS ενδέχεται να υποφέρουν από παροχή ανακριβών δεδομένων λόγω της εγγενώς ανοιχτής φύσης τους. Αυτός ο τύπος δεδομένων μπορεί να παραχθεί σκόπιμα ή/και ακούσια. Η ακούσια ανακριβής παροχή δεδομένων καλύπτει περιπτώσεις παρωχημένων ή θορυβωδών δεδομένων λόγω της χρονικής περιόδου που έχει παρέλθει από τα σημεία που συλλέγονται τα δεδομένα, καθώς καλύπτει και σφάλματα, χαμηλά επίπεδα πόρων, πιθανή χαμηλή ποιότητα του ασύρματου συνδέσμου και περιβαλλοντικές αβεβαιότητες. Η σκόπιμα ανακριβής παροχή δεδομένων αναφέρεται σε λανθασμένα δεδομένα που παρέχονται με σκοπό κακόβουλα ή εγωιστικά μέρη να υποβαθμίσουν τη χρησιμότητα των δεδομένων που συλλέχθηκαν ή και να επωφεληθούν από ορισμένες καταστάσεις. Επομένως, η διατήρηση της ακεραιότητας της συλλογής δεδομένων είναι ένα σημαντικό πρόβλημα στο πλαίσιο του MCS [12].

2.7 Κατηγορίες εφαρμογών στο MCS

Μπορούμε να χωρίσουμε τις εφαρμογές στο MCS σε τρεις διαφορετικές κατηγορίες ανάλογα με τον τύπο του φαινόμενου το οποίο μετράται ή χαρτογραφείται. Αυτές είναι:

- ***Περιβαλλοντικέ***ς : Στις περιβαλλοντικές εφαρμογές MCS, τα φαινόμενα είναι εκείνα που εμφανίζονται στο φυσικό περιβάλλον. Διάφορα παραδείγματα είναι η μέτρηση των επιπέδων ρύπανσης σε μια πόλη, το επίπεδο του νερού σε διάφορα ρυάκια και η παρακολούθηση των άγριων ζώων στους βιότοπους. Τέτοιου είδους εφαρμογές επιτρέπουν τη χαρτογράφηση περιβαλλοντικών φαινομένων μεγάλης κλίμακας με το να εμπλέκουν έναν απλό πολίτη.

- ***Έργα υποδομών:*** Οι εφαρμογές έργων υποδομής περιλαμβάνουν τη μέτρηση φαινομένων μεγάλης κλίμακας που σχετίζονται με τις δημόσιες υποδομές. Κάποια παραδείγματα είναι η μέτρηση της κυκλοφοριακής συμφόρησης, η κατάσταση των δρόμων, η διαθεσιμότητα σε χώρους στάθμευσης, οι διακοπές λειτουργίας σε δημόσια έργα (όπως ένα χαλασμένο φανάρι) και η παρακολούθηση σε ζωντανό χρόνο των μέσων μαζικής μεταφοράς.

- ***Κοινωνικές:*** Τέλος, η τρίτη κατηγορία είναι οι κοινωνικές εφαρμογές, όπου οι χρήστες κατανέμουν τις πληροφορίες που συλλέγουν μεταξύ τους. Σαν παράδειγμα, οι χρήστες μπορούν να μοιραστούν τα δεδομένα της γυμναστικής τους και να συγκρίνουν τα επίπεδα άσκησής τους με τους υπόλοιπους χρήστες της κοινότητας

Για να λειτουργήσουν αποδοτικά, τα συστήματα MCS απαιτούν τη συμμετοχή και τη συνεισφορά μεγάλου αριθμού χρηστών. Παρόλο που μπορούν να επωφεληθούν ολόκληρες κοινότητες από μια τέτοια συνεισφορά, υπάρχουν άτομα, τα οποία διστάζουν να συμμετάσχουν, όντας ανήσυχα κυρίως για την ιδιωτικότητά τους. Κάπου εδώ έρχεται η τεχνολογία Blockchain για να δώσει λύσεις σε τέτοιου είδους προβλήματα.

Κεφάλαιο Τρίτο

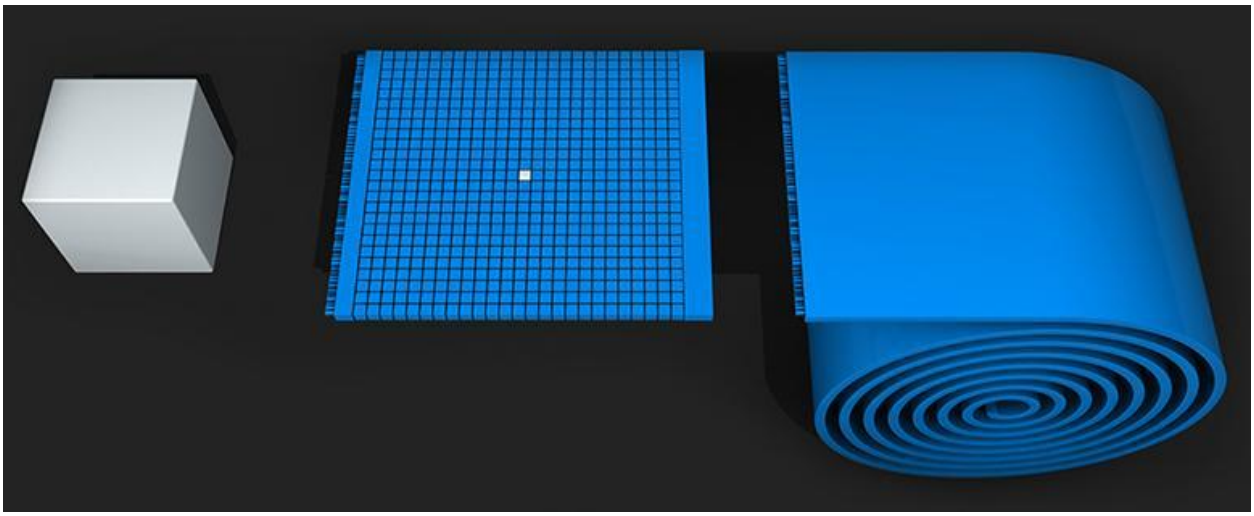
3.1 Η τεχνολογία του blockchain

Το blockchain είναι μια κατανεμημένη βάση δεδομένων, η οποία δε χρειάζεται μια κεντρική αρχή και εξαφανίζει την ανάγκη για επαλήθευση από κάποιο τρίτο μέλος. Ένα blockchain περιέχει σετ από μπλοκ και κάθε μπλοκ περιέχει ένα hash του προηγούμενου μπλοκ, δημιουργώντας έτσι μια αλυσίδα από μπλοκ από το genesis μπλοκ στο τωρινό μπλοκ. Το genesis μπλοκ είναι το πρώτο μπλοκ μέσα στο blockchain και είναι σχεδόν πάντα κωδικοποιημένο μέσα στο λογισμικό. Αποτελεί μια ειδική περίπτωση στην οποία δεν αναφέρεται σε κάποιο προηγούμενο μπλοκ. Για κάθε μπλοκ στο blockchain, υπάρχει μόνο μια διαδρομή για το genesis μπλοκ. Ωστόσο, ξεκινώντας από το genesis μπλοκ μπορεί κάποιος να συναντήσει forks. Τα forks παράγονται όταν δυο μπλοκ δημιουργούνται με διαφορά μερικών δευτερολέπτων. Όταν συμβαίνει αυτό, επιλέγεται πάντα το νεότερο μπλοκ στη μακρύτερη έγκυρη αλυσίδα. Η μακρύτερη έγκυρη αλυσίδα υπολογίζεται με βάση τη συνολική δυσκολία της αλυσίδας, και όχι τον αριθμό των μπλοκ. Τα μπλοκ σε μικρότερες αλυσίδες θεωρούνται μη έγκυρες αλυσίδες και συχνά ονομάζονται ορφανά μπλοκ.

Τα μπλοκ περιέχουν ένα σετ συναλλαγών. Μια συναλλαγή είναι μια μεταφορά αξιών μεταξύ διαφορετικών οντοτήτων, η οποία προβάλλεται στο δίκτυο και συλλέγεται μέσα στα μπλοκ. Όλες οι συναλλαγές είναι ορατές στο blockchain. Οι συναλλαγές γίνονται mine σε ένα μπλοκ από τους επονομαζόμενους pool miners ή solo miners. Η τεχνική των Pool miners είναι μια προσέγγιση κατά την οποία πολλαπλές συσκευές που λέγονται miners συνεισφέρουν στην παραγωγή ενός μπλοκ. Οι pool miners ή solo miners είναι οντότητες οι οποίες προσθέτουν καταγραφές συναλλαγών στο blockchain. Αυτή η διαδικασία ονομάζεται εξόρυξη (Mining). Η εξόρυξη είναι σκόπιμα σχεδιασμένη ώστε να χρειάζεται πόρους και να παρουσιάζει ορισμένα εμπόδια για να πραγματοποιηθεί επιτυχώς [13].

Μόλις εισέλθουν, οι πληροφορίες δεν μπορούν να διαγραφούν. Το blockchain περιέχει μια έγκυρη και επαληθευμένη καταγραφή κάθε ξεχωριστής συναλλαγής που έχει συμβεί ποτέ. Το δίκτυο, για να "σιγουρευτεί" ότι όλα τα αντίγραφα της βάσης δεδομένων είναι ίδια, πραγματοποιεί συνεχείς ελέγχους. Τα blockchains έχουν χρησιμοποιηθεί για να στηρίξουν τα κρυπτονομίσματα όπως το Bitcoin, αλλά καθημερινά αναδύονται πολλές ακόμα πιθανές τους χρήσεις. Οι καταγραφές δένονται μεταξύ τους και δημιουργούν μπλοκ και στη συνέχεια προστίθενται στην αλυσίδα το ένα μετά το άλλο. Τα βασικά μέρη είναι:

- Η καταγραφή (μπορεί να είναι οποιαδήποτε πληροφορία, για παράδειγμα μια συμφωνία)
- Το μπλοκ (ένα πακέτο καταγραφών)
- Η αλυσίδα (όλα τα μπλοκ ενωμένα μαζί).



Εικόνα 8 : Από αριστερά προς τα δεξιά: η καταγραφή, το μπλοκ, η αλυσίδα
Πηγή: (http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html **) [14]**

Στη συνέχεια θα δούμε πως εισάγεται μια νέα συμφωνία στο blockchain. Αυτό επιτυγχάνεται στα 4 ακόλουθα βήματα:

1. Καταγράφεται μια συναλλαγή. Η καταγραφή θα περιέχει τις λεπτομέρειες, καθώς και μια ψηφιακή υπογραφή από κάθε μέλος της συναλλαγής.
2. Η καταγραφή ελέγχεται από το δίκτυο. Οι υπολογιστές του δικτύου, που ονομάζονται κόμβοι, ελέγχουν τις λεπτομέρειες της συναλλαγής για να σιγουρευτούν ότι είναι έγκυρη.
3. Οι καταγραφές που έγιναν αποδεκτές από το δίκτυο προστίθενται σε ένα μπλοκ. Κάθε μπλοκ περιέχει έναν μοναδικό κωδικό που ονομάζεται hash. Επίσης, περιέχει και το hash του προηγούμενου μπλοκ στην αλυσίδα.
4. Το μπλοκ προστίθεται στην αλυσίδα. Οι κωδικοί hash ενώνουν τα μπλοκ μεταξύ τους σε συγκεκριμένη σειρά.

3.2 Οι κωδικοί hash

Οι κωδικοί hash χρησιμοποιούνται για να διατηρούν τις καταγραφές ασφαλείς. Ένας κωδικός hash δημιουργείται από μια μαθηματική συνάρτηση, η οποία λαμβάνει ψηφιακές πληροφορίες και παράγει από αυτές μια σειρά γραμμάτων και αριθμών. Στη συνέχεια αναλύονται δύο πολύ

σημαντικά χαρακτηριστικά των κωδικών hash. Ως πρώτο χαρακτηριστικό μπορεί να συγκαταλεχθεί το ότι ανεξάρτητα από το μέγεθος του αρχικού αρχείου, μια συνάρτηση hash πάντα θα παράγει έναν κωδικό ίδιου μεγέθους. Οποιαδήποτε αλλαγή συμβεί στην αρχική εισαγωγή, θα προχωρήσει στην παραγωγή καινούργιου hash. Το αλλαγμένο hash σπάει την αλυσίδα. Το επόμενο μπλοκ στην αλυσίδα έχει ακόμα το παλιό hash, έτσι για να επαναφέρει την αλυσίδα ένας hacker θα πρέπει να το επαναϋπολογίσει. Και έπειτα το επόμενο κ.ο.κ. Το να υπολογίσει ξανά κάποιος τόσα hashes θα χρειαζόταν μια τεράστια ποσότητα υπολογιστικής ισχύος.

3.3 Σύγκριση του blockchain με ένα παραδοσιακό καθολικό

Σε αντίθεση με τα παραδοσιακά καθολικά, μια βάση δεδομένων blockchain είναι αποκεντρωμένη και δεν έχει κάποιον «αφέντη». Χωρίς όμως κεντρικό έλεγχο του δικτύου, η εμπιστοσύνη αποτελεί πρόβλημα. Μια λύση είναι να επιτρέπεται η συμμετοχή μόνο σε γνωστά άτομα, όπως για παράδειγμα οι υπάλληλοι μιας εταιρείας. Άλλα blockchains όπως το δίκτυο Bitcoin, είναι ανοιχτά σε όλους. Τα μέλη είναι ανώνυμα. Δεν υπάρχει τρόπος να γνωρίζουμε αν είναι έμπιστα. Για να λυθεί αυτό το πρόβλημα και να χτιστεί εμπιστοσύνη, αυτά τα blockchains θέτουν τεστ για τους υπολογιστές που επιζητούν να εισέλθουν και να προσθέσουν καταγραφές στην αλυσίδα. Τα τεστ αυτά ονομάζονται μοντέλα συναίνεσης (consensus models). Απαιτούν από τα μέλη του δικτύου να αποδείξουν ότι είναι αυτοί που ισχυρίζονται. Ακολουθούν δυο παραδείγματα:

- ***Proof of Work***: Για να προστεθεί ένα μπλοκ στην αλυσίδα, οι κόμβοι θα πρέπει να αποδείξουν ότι έχουν κάνει «εργασία» λύνοντας ένα όλο και πιο δύσκολο υπολογιστικό puzzle. Αυτή η διαδικασία, που ονομάζεται εξόρυξη, χρησιμοποιεί αρκετή υπολογιστική ισχύ. Σε αντάλλαγμα για τη δουλειά τους, τα μέλη μπορούν να λάβουν ανταμοιβές, για παράδειγμα tokens ή bitcoins.

- ***Proof of Stake***: Οι συμμετέχοντες αγοράζουν tokens, τα οποία τους επιτρέπουν να εισέλθουν στο δίκτυο. Όσο περισσότερα tokens έχουν, τόσο περισσότερη εξόρυξη μπορούν να κάνουν [14].

3.4 Η εξόρυξη στο Bitcoin

Όπως αναφέρθηκε και στην προηγούμενη παράγραφο η εξόρυξη στο Bitcoin, είναι η διαδικασία που επιτρέπει στο blockchain να έχει αποκεντρωμένη ασφάλεια. Οι miners επικυρώνουν νέες συναλλαγές και τις καταγράφουν στο blockchain. Κατά μέσο όρο κάθε δέκα

λεπτά γίνεται εξόρυξη σε ένα νέο μπλοκ. Οι miners ανταγωνίζονται για να λύσουν ένα δύσκολο μαθηματικό πρόβλημα που βασίζεται σε κρυπτογραφικό αλγόριθμο hash. Η λύση που βρίσκουν ονομάζεται, όπως προαναφέρθηκε, Proof of Work. Αυτό αποδεικνύει ότι ένας miner ξόδεψε αρκετή ώρα και αρκετούς πόρους για να λύσει το πρόβλημα. Όταν ένα μπλοκ «λύνεται», οι συναλλαγές που περιέχει θεωρούνται επιβεβαιωμένες και τα Bitcoin που υπάρχουν στις συναλλαγές μπορούν να ξοδευτούν. Οπότε, αν λάβουμε μερικά Bitcoin στο πορτοφόλι μας, θα περάσουν περίπου 10 λεπτά για να επιβεβαιωθεί η συναλλαγή. Οι miners λαμβάνουν κάποια ανταμοιβή όταν λύνουν το πολύπλοκο μαθηματικό πρόβλημα.

Υπάρχουν δύο είδη ανταμοιβών: νέα Bitcoin ή τέλη συναλλαγών. Η ποσότητα Bitcoin που παράγεται μειώνεται κάθε 4 χρόνια (κάθε 210.000 μπλοκ για την ακρίβεια). Σήμερα, ένα νέο μπλοκ δημιουργεί 12,5 bitcoins. Αυτός ο αριθμός θα μειώνεται συνεχώς έως ότου να σταματήσουν να εκδίδονται άλλα bitcoins. Αυτό θα συμβεί κάπου στο 2140, όπου θα έχουν παραχθεί περίπου 21 εκατομμύρια bitcoins. Οι miners, όπως προαναφέρθηκε, μπορούν να λάβουν ανταμοιβή στη μορφή των τελών συναλλαγών. Ο νικητής miner μπορεί να «κρατήσει τα ρέστα» των συναλλαγών του μπλοκ. Όσο η ποσότητα Bitcoin που δημιουργείται με κάθε μπλοκ μειώνεται, τα τέλη συναλλαγών που θα λαμβάνονται από τον miner θα αυξάνονται. Μετά το 2140, ο νικητής miner θα λαμβάνει μόνο τέλη συναλλαγών σαν ανταμοιβή [15].

Η εξόρυξη μπορεί να θεωρηθεί σαν ένα "λαχείο". Δεν μπορούμε να προβλέψουμε ποιος θα λύσει το πρόβλημα. Στην περίπτωση του Bitcoin η συνάρτηση hash που χρησιμοποιείται ονομάζεται SHA256. Ένας αλγόριθμος hash πάντα παράγει ίδιο μήκος δεδομένων με τις εισαγωγές που έχουν γίνει. Είναι αδύνατο να υπολογιστεί το ίδιο hash με δυο διαφορετικές εισαγωγές. Είναι επίσης αδύνατο να γίνει πρόβλεψη του αποτελέσματος οποιωνδήποτε δεδομένων έχουν δοθεί. Το SHA256 πάντα παράγει αποτέλεσμα που έχει μήκος 256 bits. Η εξόρυξη βρίσκει το nonce, δηλαδή τη μόνη είσοδο που αλλάζει κάθε φορά που τρέχουμε τη συνάρτηση hash. Είναι πολύ εύκολο να αποδείξουμε ότι το nonce που βρέθηκε παράγει πραγματικά ένα έγκυρο hash. Όλες οι πληροφορίες είναι διαθέσιμες, ο οποιοσδήποτε μπορεί να τρέξει τη συνάρτηση hash και να επιβεβαιώσει την εγκυρότητα του hash. Επειδή είναι επίσης αδύνατο να προβλέψεις ποιο θα είναι το nonce, λειτουργεί σαν απόδειξη ότι ο miner εργάστηκε για να βρει ένα έγκυρο hash.

3.5 Περιπτώσεις χρήσης του Blockchain

Υπάρχουν πολλές περιπτώσεις όπου χρησιμοποιείται το blockchain, αλλά αρκετές υποσχόμενες χρήσεις του είναι ακόμα υπό κατασκευή. Όπως αναφέρθηκε, η πιο διάσημη χρήση του είναι στο cryptocurrency, όπως στο Bitcoin. Επίσης, πολλά οικονομικά ινστιτούτα έχουν επενδύσει στα

blockchains για να απλοποιήσουν την φύλαξη των καταγραφών για τις πληρωμές. Στην αλυσίδα εφοδιασμών, η καταγραφή συναλλαγών στο blockchain προσφέρει τρόπο να ελέγχεται η ιστορία ενός προϊόντος. Για παράδειγμα, οι εταιρείες κοσμημάτων ελπίζουν ότι στο μέλλον θα μπορούν να διαβεβαιώσουν τους πελάτες ότι τα διαμάντια δεν είναι από μέρη όπου θα μπορούσαν να χρηματοδοτήσουν κάποιον πόλεμο. Στον τομέα της υγείας, με τη χρήση του blockchain, το ιατρικό ιστορικό μπορεί να αποθηκευτεί με ασφάλεια και να ελέγχεται από τους ασθενείς. Τέλος, σημαντική θεωρείται η χρήση του blockchain στο σύστημα των εκλογών, καθώς οι καταγραφές του θα παρουσίαζαν αντίσταση στις προσπάθειες παραβίασης των ψήφων [16].

3.6 Μοντέλα Blockchain

Η τεχνολογία Blockchain έχει γίνει πλέον ευρέως γνωστή και χρησιμοποιείται από όλο και περισσότερους ανθρώπους, περισσότερες εταιρείες και περισσότερους οργανισμούς καθημερινά. Σε αυτή τη μεγάλη επιτυχία που έχει γνωρίσει τα τελευταία χρόνια, παίζει σημαντικό ρόλο η επεκτασιμότητα, η ασφάλεια και όλα τα χαρακτηριστικά που διαθέτει και κάνει τους χρήστες να το επιλέγουν. Ένα ακόμα τεράστιο προσόν που διαθέτει το Blockchain είναι οι επιλογές μοντέλων που προσφέρει. Σε κάθε διαφορετική περίπτωση χρήσης, υπάρχει και ένα διαφορετικό μοντέλο το οποίο βοηθάει τον εκάστοτε χρήστη να βγει κερδισμένος από την τεχνολογία και να βρει ακριβώς αυτό που του ταιριάζει.

Αρχικά, έχουμε τα blockchain business models. Με τη χρήση του blockchain, οι οργανισμοί μπορούν να μετατρέψουν τις επιχειρήσεις τους σε αποκεντρωμένη πλατφόρμα, κάτι το οποίο μπορεί να αλλάξει τον τρόπο εργασίας της επιχείρησης. Αλλάζει τα προσωπικά στοιχεία, τη ροή των συναλλαγών, το κέρδος και εξασφαλίζει την ανάπτυξη. Για να έχουν πλήρη επιτυχία, αυτά τα μοντέλα πρέπει να εξασφαλίσουν ότι ευνοούν τους υπαλλήλους της εταιρείας αλλά και τους τελικούς χρήστες. Η βασική ερώτηση, όμως, είναι το πως ακριβώς μπορεί κάποιος να χρησιμοποιήσει το blockchain μέσα στην επιχείρησή του. Η απάντηση έχει τρία βασικά σημεία: α) μπορείς να αποθηκεύσεις σημαντικά δεδομένα μέσα στο blockchain, τα οποία δεν μπορούν να αλλοιωθούν, β) πολλές εταιρείες έχουν χρησιμοποιήσει τη διαφάνεια του blockchain για να αυξήσουν τη λειτουργικότητα της αλυσίδας ανεφοδιασμού, και γ) πολλοί χρήστες έχουν ενσωματώσει το blockchain με τεχνητή νοημοσύνη για να δημιουργήσουν το δικό τους αποκεντρωμένο μοντέλο AI.

Η πιο γνωστή, ίσως, χρήση της τεχνολογίας blockchain είναι στα cryptocurrencies. Τα περισσότερα cryptocurrencies χρησιμοποιούν τεχνολογία blockchain για την καταγραφή των συναλλαγών. Για παράδειγμα, τα δίκτυα των Bitcoin και Ethereum βασίζονται και τα δυο όπως προείπαμε στο blockchain. Το Μάιο του 2018 το Facebook επιβεβαίωσε ότι ανοίγει μια νέα ομάδα blockchain [34] με επικεφαλής τον David Marcus, που μέχρι πριν ήταν υπεύθυνος για το

Messenger. Σύμφωνα με το The Verge, το Facebook σκοπεύει να ανοίξει το δικό του cryptocurrency για να διευκολύνει τις πληρωμές που γίνονται στην πλατφόρμα [35].

Μεγάλα τμήματα του χρηματοπιστωτικού κλάδου εφαρμόζουν κατανεμημένα καθολικά για χρήση στον τραπεζικό τομέα [36] και σύμφωνα με τις τελευταίες μελέτες, όλο αυτό συμβαίνει γρηγορότερα από ότι ήταν αναμενόμενο [37]. Οι τράπεζες δείχνουν τόσο μεγάλο ενδιαφέρον σε αυτή την τεχνολογία διότι υπάρχουν δυνατότητες για να γίνονται ταχύτερα οι διαδικασίες στο back office. Τράπεζες όπως η UBS ανοίγουν νέα εργαστήρια ερευνών, απόλυτα αφοσιωμένα στην τεχνολογία blockchain, προκειμένου να εξερευνήσουν πως μπορεί να χρησιμοποιηθεί το blockchain στις χρηματοπιστωτικές υπηρεσίες για να αυξηθεί η αποτελεσματικότητα και να μειωθεί το συνολικό κόστος [38].

Ένας τομέας-έκπληξη όπου δεν περίμενε πολύς κόσμος να δει το blockchain να χρησιμοποιείται είναι τα βιντεοπαιχνίδια. Μερικά βιντεοπαιχνίδια βασίζονται εξ ολοκλήρου στην τεχνολογία blockchain. Το πρώτο τέτοιου είδους παιχνίδι, το Huntercoin, έκανε ντεμπούτο στο χώρο το Φεβρουάριο του 2014 [39]. Ακόμα ένα παιχνίδι blockchain είναι το CryptoKitties, που εμφανίστηκε το Νοέμβριο του 2017. Το παιχνίδι έγινε περισσότερο γνωστό το Δεκέμβριο του 2017, όταν και ένας χαρακτήρας του παιχνιδιού, ένα εικονικό κατοικίδιο, πωλήθηκε για 100.000$. Παρόλο που το CryptoKitties παρουσίασε προβλήματα επεκτασιμότητας και δημιούργησε μεγάλα προβλήματα συμφόρησης στο Ethereum καθώς κατείχε το 30% των συνολικών συναλλαγών στην πλατφόρμα, παρουσίασε επίσης το πως μπορεί να χρησιμοποιηθεί το blockchain για να καταγράψουν τα περιουσιακά στοιχεία διαφόρων παιχνιδιών [40]. Το Σεπτέμβριο του 2018 δημιουργήθηκε η Blockchain Game Alliance με σκοπό να διερευνήσει διαφορετικές χρήσεις του blockchain στα βιντεοπαιχνίδια με την υποστήριξη της Ubisoft και της Fig [41].

Σημαντικό ρόλο έχει παίξει και η χρήση του blockchain στην αλυσίδα ανεφοδιασμού. Υπάρχει μεγάλος αριθμός προσπαθειών και βιομηχανικών οργανισμών που εργάζονται για να προσθέσουν το blockchain στα λογιστικά και στη διαχείριση της αλυσίδας ανεφοδιασμού. Η Walmart και η IBM τρέχουν δοκιμές για τη χρήση ενός συστήματος με βάση την τεχνολογία blockchain για καταγραφή και παρακολούθηση της αλυσίδας ανεφοδιασμού. Όλοι οι κόμβοι του blockchain χορηγούνται από τη Walmart και βρίσκονται στο IBM cloud [42].

Αρκετές εταιρείες blockchain έχουν ξεκινήσει να χρησιμοποιούν τη συγκεκριμένη τεχνολογία στο διάστημα [43]. Η Spacechain εκτόξευσε δύο νανοδορυφόρους κόμβους blockchain σε τροχιά το Φεβρουάριο και τον Οκτώβριο του 2018. Η πρώτη χρήση είναι αποκεντροποιημένη αποθήκευση δεδομένων και αρχείων στο διάστημα [44], αλλά ο τελικός στόχος είναι η μείωση της εξάρτησης σε μεγάλες εταιρείες, όπως η Google και το Facebook, οι οποίες ερευνούν κι αυτές διάφορους τρόπους να φέρνουν το διαδίκτυο σε όλους μέσω δορυφόρων στο διάστημα [45].

Άλλα μοντέλα blockchain τα οποία βρίσκονται υπό ανάπτυξη και συνεχή έρευνα είναι αυτό για την βιομηχανία ασφαλειών, τη μοιρασμένη οικονομία και το IoT.

3.7 Πλατφόρμες Blockchain

Τα τελευταία χρόνια υπάρχει σημαντική ανάπτυξη των εφαρμογών Blockchain με μεγαλύτερη ποικιλία αλλά και ποσότητα. Παρόλο που οι περισσότερο γνωστές πλατφόρμες Blockchain έχουν ήδη χρησιμοποιηθεί για να ικανοποιήσουν τις απαιτήσεις των νέων αυτών εφαρμογών, είναι ακόμα απαραίτητη μια πιο ανεξάρτητη και πρακτική αξιολόγηση της απόδοσης αυτών των πλατφορμών. Οι πληροφορίες αυτές έχουν μεγάλη σημασία για τους επαγγελματίες, έτσι ώστε να καταλάβουν τους σχετικούς περιορισμούς και να σχεδιάσουν ποια πλατφόρμα θα υιοθετήσουν για τις δικές τους εφαρμογές. Αποτελεί πολύ σημαντικό στοιχείο η μελέτη ανάλυσης της απόδοσης των ιδιωτικών πλατφορμών blockchain. Παρόλο που το blockchain αρχικά έγινε γνωστό παγκοσμίως σαν την τεχνολογία πίσω από το Bitcoin, μερικά χαρακτηριστικά του bitcoin blockchain δεν ταιριάζουν σε όλες τις εφαρμογές διαφόρων επιχειρήσεων. Λόγω αυτού, προτείνονται διάφορα ιδιωτικά blockchain για να επιτρέψουν στις επιχειρήσεις να χρησιμοποιούν χωρίς δισταγμό την τεχνολογία blockchain. Σε αντίθεση με το bitcoin blockchain, μόνο οι υπολογιστές που τους έχει επιτραπεί η πρόσβαση μπορούν να λάβουν μέρος στο ιδιωτικό δίκτυο blockchain [45]. Στη συνέχεια θα παρουσιάσουμε και θα αναλύσουμε τις περισσότερο, αλλά και κάποιες λιγότερο, γνωστές πλατφόρμες blockchain.

1. Bitcoin: Ίσως η πιο γνωστή πλατφόρμα που χρησιμοποιεί την τεχνολογία blockchain. Το Bitcoin είναι ένα συνδεδεμένο πρωτόκολλο επικοινωνίας, που διευκολύνει τη χρήση εικονικού νομίσματος, συμπεριλαμβανομένων και ηλεκτρονικών πληρωμών. Από την έναρξή του το 2009 από μια ανώνυμη ομάδα προγραμματιστών (οι οποίοι χρησιμοποιούσαν το όνομα Satoshi Nakamoto), το Bitcoin έχει υπηρετήσει περίπου 62.5 εκατομμύρια συναλλαγές μεταξύ 109 εκατομμυρίων λογαριασμών. Μέχρι το Μάρτιο του 2015, ο ημερήσιος όγκος συναλλαγών ήταν περίπου 200.000 bitcoins- σχεδόν 50$ εκατομμύρια συναλλαγματική ισοτιμία- και η συνολική αξία στην αγορά όλων των bitcoins που κυκλοφορούσαν ήταν 3,5$ δισεκατομμύρια. Οι κανόνες του bitcoin σχεδιάστηκαν από μηχανικούς χωρίς επιρροή από δικηγόρους ή ρυθμιστικές αρχές. Αντί να αποθηκεύονται οι συναλλαγές σε οποιοδήποτε διακομιστή ή σύνολο διακομιστών, το Bitcoin έχει χτιστεί σε ένα αρχείο καταγραφής συναλλαγών που διανέμεται σε ένα δίκτυο των συμμετεχόντων υπολογιστών. Περιλαμβάνει μηχανισμούς που ανταμείβουν την ειλικρινή συμμετοχή, προσελκύουν νέους χρήστες και προστατεύουν ενάντια σε διάφορες επιθέσεις.

   Ο σχεδιασμός του Bitcoin επιτρέπει μη αναστρέψιμες συναλλαγές, μια προκαθορισμένη διαδρομή δημιουργίας χρημάτων με την πάροδο του χρόνου και ένα δημόσιο ιστορικό

συναλλαγών. Οποιοσδήποτε μπορεί να δημιουργήσει ένα λογαριασμό Bitcoin, χωρίς χρέωση και χωρίς καμία κεντρική διαδικασία εξέτασης- ή έστω την απαίτηση να χρησιμοποιήσεις το αληθινό σου όνομα. Συλλογικά, οι κανόνες αυτοί αποδίδουν ένα σύστημα που θεωρείται πιο ευέλικτο, περισσότερο ιδιωτικό και λιγότερο επιδεκτικό σε ρυθμιστική εποπτεία σε σχέση με άλλες μορφές πληρωμής. Το Bitcoin ενδιαφέρει τους οικονομολόγους ως ένα εικονικό νόμισμα με προοπτική να διαταράξει τα υπάρχοντα συστήματα πληρωμών και ίσως ακόμα και διάφορα νομισματικά συστήματα. Ακόμη και στα αρχικά τους στάδια, τέτοια εικονικά νομίσματα παρέχουν μια ποικιλία ενδείξεων σχετικά με το σχεδιασμό της αγοράς και τη συμπεριφορά των αγοραστών και των πωλητών. Τα bitcoins καταγράφονται σαν συναλλαγές. Κάθε ξεχωριστό bitcoin μπορεί να εντοπιστεί και να ψάξουμε το ιστορικό του σχετικά με όλες τις συναλλαγές στις οποίες χρησιμοποιήθηκε, φτάνοντας σταδιακά στην έναρξη της κυκλοφορίας του. Όλες οι συναλλαγές Bitcoin μπορούν να διαβαστούν από όλους σε αρχεία που έχουν αποθηκευτεί σε ευρέως αναπαραγόμενες δομές δεδομένων. Το Bitcoin βασίζεται σε δυο θεμελιώδεις τεχνολογίες της κρυπτογραφίας: κρυπτογραφία δημόσιου-ιδιωτικού κλειδιού για την αποθήκευση και το ξόδεμα λεφτών και κρυπτογραφική επικύρωση των συναλλαγών.

Η παραδοσιακή κρυπτογραφία δημόσιου-ιδιωτικού κλειδιού επιτρέπει σε όλους να δημιουργήσουν ένα δημόσιο κλειδί και ένα, σχετικό με το δημόσιο, ιδιωτικό κλειδί. Τα δημόσια κλειδιά είναι σχεδιασμένα για να μοιράζονται ευρέως, εξ ου και το όνομα. Τα μηνύματα που έχουν κρυπτογραφηθεί από ένα δημόσιο κλειδί μπορούν να διαβαστούν μόνο από κάποιον που έχει στην κατοχή του αντίστοιχο ιδιωτικό κλειδί, επιτρέποντας έτσι σε όλους να κρυπτογραφήσουν ένα μήνυμα το οποίο μόνο ένας συγκεκριμένος χρήστης θα μπορεί να διαβάσει. Κάθε νέα συναλλαγή που δημοσιεύεται στο δίκτυο του Bitcoin περιοδικά μαζεύεται μαζί με τις άλλες μέσα σε ένα μπλοκ πρόσφατων συναλλαγών. Για να σιγουρευτούμε ότι δεν έχει εισέλθει κάποια συναλλαγή χωρίς αδειοδότηση, γίνεται σύγκριση ολόκληρου του μπλοκ με το πιο πρόσφατα δημοσιευμένο μπλοκ, δημιουργώντας έτσι μια σύνδεση ανάμεσα στα μπλοκ ή αλλιώς blockchain. Ένα νέο μπλοκ προστίθεται στο Blockchain περίπου κάθε δέκα λεπτά. Με αυτή τη δομή δεδομένων, ο κάθε χρήστης του Bitcoin μπορεί να επαληθεύσει ότι όντως συνέβη μια τελειωμένη συναλλαγή [46].

Η χρήση του λογισμικού είναι δωρεάν και διαθέσιμη σε όλες τις χώρες του κόσμου, εφόσον υπάρχει σύνδεση στο Internet. Η βασική λειτουργία του λογισμικού έγκειται στην εκτέλεση συναλλαγών bitcoins και την αναμετάδοση πληροφοριών ανάμεσα σε κόμβους και την επιβεβαίωση της εγκυρότητας τους για το υπόλοιπο δίκτυο. Καθώς το λογισμικό είναι ανοιχτού κώδικα, δύνανται να υπάρχουν πάρα πολύ διαφορετικές εκδόσεις και εκδοχές του. Στην ουσία, ο καθένας θα μπορούσε με τις κατάλληλες ικανότητες να δημιουργήσει ένα αντίστοιχο δίκτυο, αντιγράφοντας σε μεγάλο βαθμό το λογισμικό του Bitcoin, προσθέτοντας ή διαφοροποιώντας με ότι κανόνες επιθυμεί.

Τα βασικά πλεονεκτήματα του Bitcoin είναι:

- Ταχύτητα συναλλαγών/Διεθνής φύση
- Εξαιρετικά χαμηλό κόστος συναλλαγών
- Έλεγχος από το χρήστη/Προστασία από υφαρπαγή
- Φορητότητα/αντίγραφα ασφαλείας
- Διαφάνεια συναλλαγών/κανόνων
- Συναινετική φύση χρήσης/αλλαγών
- Αποκεντρωμένη φύση
- Υποδιαιρέσεις του νομίσματος (έως 8 δεκαδικά ψηφία)
- Μη αντιστρέψιμη φύση
- Ιδιωτικότητα συναλλαγών

Κάποια ρίσκα και ορισμένοι κίνδυνοι που υπάρχουν είναι:

- Απώλεια ιδιωτικών κλειδιών
- Ασαφές νομικό πλαίσιο
- Ασφάλεια δικτύου/Νεαρό ηλικίας
- Έλεγχος μεγάλου μέρους του δικτύου από μια κακόβουλη οντότητα
- Παραβίαση αλγορίθμων κρυπτογράφησης του δικτύου

2. Ethereum: Όπως και το Bitcoin, έτσι και το Ethereum είναι μια δημόσια πλατφόρμα blockchain με διαφορετική φιλοσοφία σχεδιασμού. Ο Vitalik Buterin μας σύστησε το Ethereum, το οποίο θα μπορούσε να διευκολύνει τις συναλλαγές όχι μόνο χρημάτων, αλλά και μετοχών, εκτάσεων γης, ψηφιακών περιεχομένων, οχημάτων και πολλών άλλων που έχουν κάποια εγγενή αξία. Η πιο καινοτόμος προσέγγιση ήταν η δημιουργία ενός επιπέδου αφαίρεσης έτσι ώστε οι συναλλαγές από διαφορετικές εφαρμογές να γενικευτούν στον κώδικα του προγράμματος που μπορεί να εκτελεστεί σε όλους τους κόμβους του Ethereum.

Στο Ethereum οι miners παράγουν Ether, ένα ανταλλάξιμο κρυπτονόμισμα, εξαιτίας του οποίου το δημόσιο δίκτυο blockchain είναι αυτοσυντηρούμενο. Οποιαδήποτε εφαρμογή δουλεύει στο Ethereum πρέπει να πληρώσει φόρους συναλλαγής τους οποίους λαμβάνουν σταδιακά οι miners για τη δουλειά που κάνουν στους κόμβους και τη συντήρηση ολόκληρου του δικτύου. Το Ethereum καθιστά δυνατή την ταχύτατη ανάπτυξη των αποκεντρωμένων εφαρμογών που μπορούσαν να αλληλεπιδράσουν μεταξύ τους, εξασφαλίζοντας πάντα επαρκή ασφάλεια. Αυτό επιτυγχάνεται με τη δημιουργία ενός αφηρημένου βασικού επιπέδου.

Σε αντίθεση με το Bitcoin, το Ethereum υποστηρίζει γλώσσες Turing-complete έτσι ώστε ο καθένας να μπορεί να γράψει έξυπνα συμβόλαια, τα οποία θα μπορούσαν εικονικά να κάνουν τα πάντα όσον αφορά τον προγραμματισμό. Επίσης, το Ethereum είναι προστατευμένο από το σχεδιασμό του και παρακολουθεί τις καταστάσεις των λογαριασμών,

κάτι το οποίο είναι πολύ διαφορετικό από το Bitcoin όπου τα πάντα παραμένουν σαν συναλλαγές και δεν υπάρχει εσωτερική μόνιμη μνήμη για τα scripts. Με τη βοήθεια ενός αφηρημένου βασικού επιπέδου, οι υποβόσκουσες πολυπλοκότητες είναι κρυμμένες από τους προγραμματιστές. Οι προγραμματιστές έχουν την ευελιξία να σχεδιάζουν τις δικές τους μεταβατικές λειτουργίες για άμεση μεταφορά αξίας και πληροφοριών, καθώς και μορφών συναλλαγών. Σε μια προσπάθεια να φτάσουν στο στόχο, η βασική καινοτομία του Ethereum ήταν η Ethereum Virtual Machine (EVM). Η υποστήριξη γλωσσών Turing-complete μέσω του EVM καθιστά εύκολη για τους προγραμματιστές τη δημιουργία εφαρμογών blockchain. Το EVM απαιτείται να τρέχει τα έξυπνα συμβόλαια. Το Ethereum δανείζεται πολλά σχέδια από τον πυρήνα του Bitcoin επειδή άντεξε στο πέρασμα του χρόνου, αλλά είναι σχεδιασμένο με διαφορετική φιλοσοφία. Η εξέλιξη του Ethereum έχει ακολουθήσει τις παρακάτω αρχές: απλό σχεδιασμό, ελευθερία προγραμματισμού, απουσία έτοιμων χαρακτηριστικών [47].

Πλεονεκτήματα του Ethereum:

- Ακολουθείται δυναμικά στο Github
- Ανοιχτό για δημόσια χρήση
- Πολλαπλές εφαρμογές γλωσσών όπως Python, C++
- Βασίζεται σε Proof-of-Work

3. Hyperledger Fabric: Το Hyperledger Fabric είναι μια εξουσιοδοτημένη πλατφόρμα λογισμικού σχεδιασμένη να είναι εξαιρετικά επεκτάσιμη και αρθρωτή, παρέχοντας έτσι εμπιστευτικότητα, ιδιωτικότητα και δυνατότητες επέκτασης blockchain επιχειρήσεων. Με τη διαθεσιμότητα παραγωγής του Fabric στα μέσα του 2017, οι επιχειρήσεις πειραματίζονται με το Fabric για την κατασκευή εφαρμογών blockchain στον πραγματικό κόσμο. Το Hyperledger Fabric, που φιλοξενείται από το Linux Foundation, ήταν η πρώτη blockchain πλατφόρμα κοινοπραξίας με παραγωγική διαθεσιμότητα της προσφοράς της. Το Fabric με την υποστήριξή του στα έξυπνα συμβόλαια είναι γενικά κατάλληλο για μια ευρεία γκάμα εφαρμογών σε πολλούς τομείς. Το Fabric απευθύνεται κυρίως σε έργα ενοποίησης, στα οποία απαιτείται Distributed Ledger Technology (DLT), η οποία δεν προσφέρει υπηρεσίες προς τους χρήστες εκτός από ένα SDK για το Node.js, Java και Go. Το Fabric υποστηρίζει chaincode σε Go και JavaScript (μέσω του Hyperledger Composer) out-of-the-box, και άλλες γλώσσες όπως Java με την εγκατάσταση των κατάλληλων ενοτήτων. Ως εκ τούτου, είναι δυνητικά πιο ευέλικτο από ότι οι ανταγωνιστές του που υποστηρίζουν μόνο μια κλειστή γλώσσα έξυπνων συμβολαίων. Το Fabric επιτρέπει στους συμμετέχοντες οργανισμούς μέσω κοινοπραξιών, την κατασκευή και την ανάπτυξη εφαρμογών blockchain. Το δίκτυο blockchain περιλαμβάνει κάποιους κόμβους που φιλοξενούν το blockchain, εκτελούν τα έξυπνα συμβόλαια (στο Fabric ονομάζονται chaincode) και διατηρεί συλλογικά την κατάσταση του λογισμικού. Τα chaincodes μπορούν να μοιραστούν από όλες τις οντότητες μέσα στις κοινοπραξίες ή μπορούν να αναπτυχθούν ιδιωτικά για να έχουν πρόσβαση μόνο

ορισμένες οντότητες. Τα ιδιωτικά chaincodes εκτελούνται μόνο σε peers με τους οποίους το chaincode είναι κοινόχρηστο και παραμένει απρόσιτο για άλλους. Αυτό επιτυγχάνεται μέσω της ιδέας των καναλιών στο Fabric όπου όλα τα chaincodes και τα δεδομένα στο κανάλι είναι προσβάσιμα μόνο σε οντότητες που αποτελούν μέρος του καναλιού [48].

Τα πλεονεκτήματα του είναι τα εξής:

- 185+ συνεργαζόμενες επιχειρήσεις
- Σπονδυλωτή (αρθρωτή) αρχιτεκτονική
- Έρευνες ιστορικού μόνο για ανάγνωση
- Η παραγωγή είναι έτοιμη για επιχειρήσεις
- Αδειοδοτημένη συνδρομή
- Προστασία ψηφιακών κλειδιών και ευαίσθητων δεδομένων

4. Multichain: Το Multichain είναι μια προκατασκευασμένη πλατφόρμα για τη δημιουργία και την ανάπτυξη ιδιωτικών blockchain, ανάμεσα σε οργανισμούς. Στοχεύει να ξεπεράσει ένα σημαντικό εμπόδιο στην ανάπτυξη της τεχνολογίας blockchain στον οικονομικό τομέα, παρέχοντας την ιδιωτικότητα και τον έλεγχο που χρειάζεται σε ένα εύχρηστο πακέτο. Όπως το λογισμικό Bitcoin Core, από το οποίο προέρχεται, το Multichain υποστηρίζει τα Windows, Linux και Mac servers και παρέχει ένα από API και επιφάνεια με γραμμή εντολών. Το Multichain επιλύει τα προβλήματα της εξόρυξης, της ιδιωτικότητας και της διαφάνειας μέσω της ολοκληρωμένης διαχείρισης των δικαιωμάτων των χρηστών. Ο βασικός στόχος είναι τριπλός: α) να σιγουρευτούν ότι η δραστηριότητα του blockchain είναι μόνο ορατή στους επιλεγμένους συμμετέχοντες, β) να εισάγουν ελέγχους οι οποίοι να επιτρέπουν τις συναλλαγές, και γ) να επιτρέψουν στην εξόρυξη να γίνεται με ασφάλεια χωρίς proof-of-work και το σχετικό κόστος. Όταν ένα blockchain είναι ιδιωτικό, τα προβλήματα που σχετίζονται με την κλιμάκωση επιλύονται εύκολα, από τη στιγμή που οι συμμετέχοντες μπορούν να ελέγξουν το μέγιστο μέγεθος των μπλοκ. Επιπρόσθετα, σαν ένα κλειστό σύστημα, το blockchain θα περιέχει μόνο τις συναλλαγές που θα ενδιαφέρουν τους συγκεκριμένους συμμετέχοντες [49].

   Κάποια από τα πλεονεκτήματά του Multichain είναι:

   - Ιδιωτικό αδειοδοτημένο δίκτυο
   - Δωρεάν και ανοιχτού κώδικα τιμολόγηση
   - Ενημερώνεται ενεργά στο Github
   - Γρήγορη ανάπτυξη
   - Υποστηριζόμενες γλώσσες: Python, C#, C++, JavaScript

5. Openchain: Όπως υποδεικνύει και το όνομα, το OpenChain είναι μια δημοφιλής πλατφόρμα blockchain ανοιχτού κώδικα, η οποία χρησιμοποιείται ευρέως σε οργανισμούς που στοχεύουν στον έλεγχο των ψηφιακών τους κεφαλαίων. Η πλατφόρμα έγινε γνωστή και επεξεργάστηκε από την Coinprism. Το σύστημα έχει προσαρμοσμένες αδειοδοτήσεις σε διάφορα επίπεδα, κάτι το οποίο το ευνοεί αρκετά σε σχέση με άλλα παρόμοια συστήματα. Το OpenChain προσδιορίζει βασικές προτεινόμενες διαδικασίες για αποτελεσματική διαχείριση ανοιχτού κώδικα. Το έργο ενισχύει την εμπιστοσύνη σε ανοιχτό κώδικα καθιστώντας απλούστερη και συνεκτικότερη την αποδοχή της αδειοδότησης του ανοιχτού κώδικα. Το OpenChain Specification ορίζει ένα βασικό σύνολο απαιτήσεων που πρέπει να ικανοποιείται από κάθε πρόγραμμα συμμόρφωσης ποιότητας. Το OpenChain Curriculum παρέχει το εκπαιδευτικό υπόβαθρο για διαδικασίες και λύσεις ανοιχτού κώδικα, ενώ ικανοποιεί μια βασική απαίτηση του OpenChain Specification. Το OpenChain Performance επιτρέπει στους οργανισμούς να επιδείξουν ότι τηρούν τις απαιτήσεις αυτές. Το αποτέλεσμα είναι ότι η υπακοή της αδειοδότησης του ανοιχτού κώδικα γίνεται περισσότερο προβλέψιμη, κατανοητή και αποδοτική για τους συμμετέχοντες της αλυσίδας εφοδιασμού λογισμικού.

   Το OpenChain κάνει το δωρεάν και ανοιχτού κώδικα λογισμικό (FOSS) περισσότερο προσιτό στους προγραμματιστές. Παρέχει μια δομή για κοινή χρήση του FOSS. Οι εταιρείες που προσαρμόζονται δημιουργούν ένα περιβάλλον που υποστηρίζει τη χρήση του FOSS εσωτερικά και την κοινή χρήση του με συνεργάτες. Επίσης, μειώνει τη συνολική προσπάθεια προσαρμογής, εξοικονομώντας χρόνο καθώς και νόμιμους και μηχανικούς πόρους. Επιτρέπει στις εταιρείες μιας αλυσίδας εφοδιασμού να εργάζονται μαζί για την προσαρμογή στο FOSS και παρέχει ένα συγκεκριμένο πρότυπο στο οποίο πρέπει όλοι να αποδίδουν. Σε αντίθεση, σε μια τυπική αλυσίδα εφοδιασμού, κάθε μέλος της αλυσίδας πρέπει να εκτελεί την προσαρμογή των λογισμικών των άλλων στην αλυσίδα, σπαταλώντας χρόνο και πόρους σε διπλή προσπάθεια.

   Το OpenChain μπορεί να προσαρμοστεί στα υπάρχοντα συστήματα που διαθέτει ο κάθε οργανισμός. Επιτρέπει την επιλογή των δικών τους διαδικασιών για να ανταπεξέρχονται στις προϋποθέσεις. Παρέχει, επίσης, πόρους που βοηθούν στο σχεδιασμό νέων διαδικασιών από το μηδέν, ή ακόμα μπορούν να επιλέξουν να χρησιμοποιήσουν τα συστήματα που έχουν ήδη στην κατοχή τους. Ακόμα, βοηθάει τις επιχειρηματικές ομάδες να δουλεύουν μαζί σε έναν κοινό σκοπό. Η γλώσσα που υποστηρίζει το OpenChain είναι το JavaScript, έχει πολλαπλούς βαθμούς πιστοποίησης και ιδιωτικό δίκτυο. Τέλος, παρέχει προσχέδια για τις νομικές, μηχανικές και επιχειρηματικές ομάδες μιας εταιρείας, ώστε να εργάζονται όλες μαζί για την προσαρμογή στο FOSS [50].

6. Mastercard Blockchain: Το Mastercard Blockchain δημιουργεί νέες εμπορικές ευκαιρίες για την ψηφιακή μεταφορά αξίας, επιτρέποντας στις επιχειρήσεις και στα οικονομικά ινστιτούτα να πραγματοποιούν συναλλαγές σε ένα κατανεμημένο καθολικό. Η τεχνολογία αυτή μπορεί

να εξυπηρετήσει πολλές περιπτώσεις χρήσης και επίσης να αφαιρέσει αρκετό χρόνο, κόστος και ρίσκο από τις χρηματοοικονομικές ροές. Παρέχοντας αδειοδοτημένη πλατφόρμα στο δίκτυο των προγραμματιστών και των συνεργατών τους, η συγκεκριμένη πλατφόρμα προσφέρει [51]:

- Ιδιωτικότητα: Η πλατφόρμα δίνει προτεραιότητα στην ιδιωτικότητα όλων των συμμετεχόντων στο blockchain. Μόνο οι άμεσοι συνεργάτες θα έχουν πρόσβαση στο εσωτερικό συγκεκριμένων συναλλαγών.
- Ευκολία στη χρήση: Επιτρέπει ενσωμάτωση των πλεονεκτημάτων του blockchain σε εφαρμογές χωρίς την επιβάρυνση της δημιουργίας ενός τοπικού κόμβου.
- Ευκαμψία: Παρέχει δείγματα για γρήγορο ξεκίνημα και τη δημιουργία μιας δομής που θα βοηθάει τους χρήστες στο σχεδιασμό του πρωτοκόλλου της εφαρμογής τους.
- Επεκτασιμότητα: Ο μηχανισμός συναίνεσης φέρνει στο blockchain μεγαλύτερη ταχύτητα επεξεργασίας και επεκτασιμότητα.
- Έναν έμπιστο συνεργάτη: Με τις υπάρχουσες δυνατότητες της Mastercard στη διάθεση των χρηστών, μπορούν να χτίσουν πραγματικές χρηματοοικονομικές εφαρμογές, οι οποίες είναι έτοιμες για χρήση στην παγκόσμια κλίμακα.

7. Ripple: Τα Ripple Labs, με την τεχνολογία Ripple, έχουν χτίσει τη φήμη τους από το 2012 στην επανάσταση πληρωμών, με προοπτική να δημιουργήσουν ένα παγκόσμιο πρωτόκολλο πληρωμών. Παρόλο που ζούμε σε ένα κόσμο που οδηγείται καθημερινά από την τεχνολογία, παραμένει αρκετά δύσκολη η μετακίνηση λεφτών παγκοσμίως. Ένα εναρμονισμένο πρωτόκολλο χρειάζεται για να ενεργεί στο χώρο μεταξύ των οικονομικών ιδρυμάτων σε όλο τον κόσμο. Σαν ανοιχτό πρωτόκολλο, το Ripple επιτρέπει σε ένα διακομιστή με αρχιτεκτονική peer-to-peer να διευκολύνει τη μετακίνηση της αξίας ανάμεσα στα οικονομικά ιδρύματα. Αυτό ουσιαστικά επιτρέπει στις εταιρείες οικονομικών υπηρεσιών να πραγματοποιούν πληρωμές απευθείας η μία στην άλλη, ανεξάρτητα από το αν βρίσκονται σε διαφορετικά δίκτυα, σε άλλες χώρες ή έχουν διαφορετικό νόμισμα. Με την εγκατάσταση ενός παγκόσμιου οικονομικού πρωτοκόλλου, το Ripple έρχεται να γκρεμίσει στην ουσία τα τείχη μεταξύ οικονομικών ιδρυμάτων. Αντί το κάθε ίδρυμα να εργάζεται μέσα στους δικούς του κανόνες και στα δικά του όρια, το RTXP (Ripple payment protocol) υπηρετεί για να δημιουργήσει ένα παγκόσμιο σετ κανόνων, το οποίο θα τηρεί κάθε ίδρυμα. Η επεξεργασία ενός και μόνο πρωτοκόλλου μεταξύ των οικονομικών ιδρυμάτων θυμίζει αρκετά τη δημιουργία του Simple Mail Transfer Protocol (SMTP) κατά τη διάρκεια των πρώτων ημερών των emails. Το Ripple Protocol επιτυγχάνει τη συναίνεση σε κάθε επίπεδο. Αποτελείται από ένα σύστημα ακαθάριστου διακανονισμού, το Ripple Transaction Protocol, διασφαλίζοντας με αυτό τον τρόπο άμεσες και σχεδόν δωρεάν πληρωμές, ανταλλαγή συναλλάγματος και εμβασμάτων, ανεξάρτητα από το μέγεθος.

   Το Ripple επιτρέπει επίσης την ταχεία και ασφαλή μεταφορά των tokens, είτε με εξουσιοδότηση, κρυπτονόμισμα, εμπόρευμα ή οποιαδήποτε άλλη μονάδα αξίας. Η τεχνολογία Ripple αντηχεί διάφορες συζητήσεις για το συνεχές της κεντροποίησης-

αποκεντροποίησης και την εμφάνιση των υβριδικών λύσεων. Είναι ένα έξυπνο μείγμα αδειοδοτημένης και μη αδειοδοτημένης αρχιτεκτονικής. Ενώ ο καθένας μπορεί να συμμετάσχει, ο κάθε συμμετέχοντας έχει τη δυνατότητα να επιλέξει αυτούς που θα επικυρώσουν μια συναλλαγή, με βάση την εμπιστοσύνη, ένα συμβόλαιο, ή μια προκαθορισμένη αξιολόγηση. Ο αλγόριθμος του Ripple δημιουργεί μια αποκεντροποιημένη αγορά μέσα στο πρωτόκολλό του. Κατά μια έννοια, είναι πιο κοντά σε ένα ledgerchain, παρά σε ένα blockchain, με το αποκεντρωμένο επίπεδο ελέγχου [52].

8. Quorum: Το Quorum είναι μια έκδοση του Ethereum με μεγάλη εστίαση στις επιχειρήσεις. Είναι ιδανικό για οποιαδήποτε εφαρμογή απαιτεί υψηλή ταχύτητα και επεξεργασία υψηλής απόδοσης των ιδιωτικών συναλλαγών μέσα σε μια αδειοδοτημένη ομάδα γνωστών συμμετεχόντων. Το Quorum αντιμετωπίζει συγκεκριμένες προκλήσεις για την υιοθέτηση τεχνολογιών blockchain μέσα στην οικονομική βιομηχανία, αλλά και πέρα από αυτή. Υποστηρίζει ιδιωτικότητα στο επίπεδο των συναλλαγών, καθώς και διαφάνεια σε ολόκληρο το δίκτυο. Επίσης, είναι ευέλικτο και μπορεί να προσαρμοστεί εύκολα, ανάλογα με τις ανάγκες κάθε εταιρείας. Όλα τα δημόσια και τα ιδιωτικά έξυπνα συμβόλαια καθώς και η γενική κατάσταση του συστήματος αντλούνται από ένα μόνο, διαμοιρασμένο, ολοκληρωμένο blockchain συναλλαγών που επαληθεύονται από τον κάθε κόμβο στο δίκτυο. Η κατάσταση των ιδιωτικών έξυπνων συμβολαίων κοινοποιείται και επαληθεύεται μόνο από τα μέλη του συμβολαίου και επιβεβαιωμένα τρίτα μέλη, όπως οι ρυθμιστές. Τα έξυπνα συμβόλαια που συντάχθηκαν για μια υπάρχουσα εφαρμογή του Ethereum, παραμένουν διαυγή και στο Quorum. Η ενίσχυση πολλών υφιστάμενων σχεδίων των έξυπνων συμβολαίων για την τήρηση των απαιτήσεων ιδιωτικότητας είναι απλή και γρήγορη. Παρακάτω υπάρχουν οι λόγοι που κάνει τους περισσότερους χρήστες να επιλέξουν το Quorum:
   - Εμπιστοσύνη: Η βασική καινοτομία του blockchain είναι η ψηφιακή εμπιστοσύνη, αποδεδειγμένη στο σύστημα χωρίς να βασίζεται σε κάποια εξωτερική αρχή. Παρομοίως, ο open source κώδικας μπορεί να απομονωθεί και να επαληθευτεί προκειμένου να σιγουρευτούν ότι κάνει ακριβώς ό,τι λέει πως κάνει.
   - Κοινότητα: Ο open source κώδικας προσκαλεί άλλους για συνεργασία και αναπτύσσεται καλύτερα μέσω της ενσωμάτωσης διαφορετικών προοπτικών. Επίσης, το Quorum εγγυάται ότι η πλατφόρμα θα παραμένει δωρεάν για πάντα και ενθαρρύνει με αυτό τον τρόπο τον πειραματισμό.
   - Ωριμότητα: Το Quorum είναι σχεδιασμένο να αναπτύσσεται και να εξελίσσεται δίπλα στο Ethereum. Επειδή, αλλάζει μόνο σε λίγα σημεία τον πυρήνα του Ethereum, το Quorum έχει τη δυνατότητα να δέχεται την πλειοψηφία των αναβαθμίσεων του Ethereum γρήγορα και χωρίς ιδιαίτερη προσπάθεια [53].

9. R3 Corda: Το 2016 η R3 δημιούργησε τη πλατφόρμα ανοιχτού κώδικα Corda. Το Corda αφαιρεί τη δαπανηρή τριβή στις επιχειρηματικές συναλλαγές επιτρέποντας στα ιδρύματα να πραγματοποιούν απευθείας συναλλαγές χρησιμοποιώντας έξυπνα συμβόλαια, ενώ παράλληλα εγγυάται για υψηλά επίπεδα ιδιωτικότητας και ασφάλειας. Από τη σύλληψή του, το Corda χτίστηκε ειδικά για τις επιχειρήσεις. Επειδή το Corda σχεδιάστηκε από την αρχή για παραγωγή, εταιρείες με σχετικά απλή δομή IT και ένα απλό δίκτυο μπορούν να το χρησιμοποιήσουν κατευθείαν. Οι δημιουργοί του προτρέπουν οποιονδήποτε έχει προγραμματιστικές δυνατότητες να πειραματιστεί και να χτίσει πάνω στον ανοιχτό κώδικα του Corda. Η Corda Enterprise είναι μια εμπορική διανομή του ανοιχτού κώδικα του Corda σχεδιασμένη ειδικά για να καλύψει τις απαιτήσεις των σύγχρονων επιχειρήσεων. Η αξιοποίηση των μοναδικών χαρακτηριστικών της κύριας προσφοράς τους, είναι η βέλτιστη επιλογή για οργανισμούς με πρόσθετες επιχειρηματικές απαιτήσεις, όπως η ανάπτυξη εντός του εταιρικού τοίχου προστασίας, υποστήριξη 24/7, προβλέψιμα εκδοτικά χρονοδιαγράμματα, αφοσιωμένη διαχείριση προϊόντων, και υποστήριξη βιομηχανικών βάσεων δεδομένων. Ένα από τα πιο σημαντικά χαρακτηριστικά του Corda είναι το Corda Network, ένα κρυφό δίκτυο το οποίο παρέχει ένα κοινό επίπεδο ταυτότητας και συναίνεσης στα δίκτυα των επιχειρήσεων. Το Corda Network επιτρέπει στα δεδομένα και στα ψηφιακά στοιχεία να μετακινούνται χωρίς τριβή σε ένα ανοιχτό δίκτυο προστατευμένα από το μοντέλο ιδιωτικότητας του Corda. Αυτό επιτρέπει στις εταιρείες να κάνουν συναλλαγές ανεμπόδιστα, όχι μόνο μέσα στις δικές τους επιχειρηματικές γραμμές, αλλά ακόμα και με τους συνεργάτες τους, επιτρέποντας έτσι στις εφαρμογές να αναπτύσσονται ταχύτατα, με ασφάλεια και οικονομικά. Το Corda Network κυβερνάται από έναν μη κερδοσκοπικό οργανισμό με βάση την Ολλανδία. Οι συμμετέχοντες στο Corda Network έχουν τη δυνατότητα να ψηφίζουν και να θέτουν τον εαυτό τους υποψήφιο για το συμβούλιο του ιδρύματος και να λαμβάνουν σημαντικές αποφάσεις που το αφορούν, συμπεριλαμβανομένων των δεδομένων και των παραμέτρων του δικτύου, καθώς και τις πολιτικές που ακολουθεί [54]. Οι βασικές δυνατότητες του πυρήνα του Corda είναι οι εξής:

   - Συναίνεση για τα δεδομένα που έχουν σημασία: Το Corda είναι σχεδιασμένο έτσι ώστε να έχει τη συναίνεση των συμμετεχόντων στα διαμοιρασμένα γεγονότα, αφαιρώντας την ανάγκη για δαπανηρό και χρονοβόρο συμβιβασμό.
   - Ιδιωτικότητα με προέλευση: Σε αντίθεση με τις παραδοσιακές πλατφόρμες blockchain, το Corda ελαχιστοποιεί τη διαρροή πληροφοριών, με το να μοιράζεται τα δεδομένα της κάθε συναλλαγής μόνο με τους συμμετέχοντες που απαιτείται.
   - Ενσωμάτωση με κληρονομημένες υποδομές: Η υιοθέτηση από τις επιχειρήσεις θα είναι μια σταδιακή προσέγγιση και το Corda έχει σχεδιαστεί για την εύκολη ενσωμάτωση και τη διαλειτουργικότητα με τα συστήματα που λειτουργούν την κάθε επιχείρηση.
   - Εφαρμογές για κάθε βιομηχανία: Το Corda είναι η πύλη σε ένα ζωντανό δίκτυο εφαρμογών blockchain για την οικονομία και το εμπόριο, γνωστό ως CorDapps, που επιλύει σύνθετα προβλήματα στον πραγματικό κόσμο.

10. Stellar: Το Stellar είναι μια πλατφόρμα που συνδέει τράπεζες, συστήματα πληρωμών και ανθρώπους. Όπως το διαδίκτυο, έτσι και το Stellar είναι ένα δίκτυο αποκεντροποιημένων διακομιστών σε πολλές διαφορετικές τοποθεσίες, οι οποίοι δίνουν ενέργεια σε ένα κατανεμημένο καθολικό. Αυτό το καθολικό καταγράφει κάθε συναλλαγή στο σύστημα για ανθρώπους και εταιρείες. Ένα ολοκληρωμένο αντίτυπο του παγκόσμιου καθολικού υπάρχει σε κάθε διακομιστή του Stellar. Μια οντότητα μπορεί να τρέξει ένα διακομιστή. Το δίκτυο γίνεται δυνατότερο όσο περισσότερους διακομιστές έχει. Αυτοί επικοινωνούν μεταξύ τους για να επικυρώσουν συναλλαγές και να συγχρονίσουν το καθολικό κάθε 2-5 δευτερόλεπτα. Αυτός ο μηχανισμός είναι γνωστός ως μηχανισμός συναίνεσης. Το καθολικό καταγράφει τα χρήματα σαν μονάδες, τα οποία εκδίδονται από κάποιους σταθεροποιητές. Οι σταθεροποιητές είναι απλές οντότητες που εμπιστεύονται οι άνθρωποι για να κρατήσουν τις καταθέσεις τους και να μοιράσουν μονάδες στο δίκτυο του Stellar για αυτές τις καταθέσεις. Συμπεριφέρονται σαν γέφυρες μεταξύ ενός δεδομένου νομίσματος και του δικτύου του Stellar. Οι τράπεζες και οι επεξεργαστές πληρωμών είναι παραδείγματα σταθεροποιητών στον πραγματικό κόσμο. Οι μονάδες μπαίνουν στον προσωπικό λογαριασμό, ο οποίος ενεργεί σαν εικονικό πορτοφόλι, με αντάλλαγμα την κατάθεση του ιδιοκτήτη του λογαριασμού. Οι σταθεροποιητές πρέπει να είναι έμπιστοι για να κρατήσουν τα λεφτά του καθενός και να τιμήσουν τις αναλήψεις. Οι μονάδες που έχουν δοθεί μπορούν να σταλθούν και να ληφθούν μεταξύ ανθρώπων στο δίκτυο.

Το Stellar έχει κατανεμημένη συναλλαγή, έτσι ώστε να μπορεί ο καθένας να στέλνει μονάδες του Ευρώ σε κάποιον φίλο του που χρησιμοποιεί μονάδες USD. Το δίκτυο θα το μετατρέψει αυτόματα από το ένα στο άλλο. Ο φίλος θα λάβει μονάδες του Ευρώ, τα οποία μπορεί να τραβήξει χρησιμοποιώντας κάποιον σταθεροποιητή που υποστηρίζει τα Ευρώ. Η διαδικασία ενσωμάτωσης του Stellar είναι αρκετά απλή. Αρχικά, πρέπει να αναγνωρίσει ο ενδιαφερόμενος ποια είναι η περισσότερο ταιριαστή χρήση για την επιχείρησή του. Στη συνέχεια, η τεχνική ομάδα θα ετοιμάσει τους πίνακες με τις βάσεις δεδομένων, θα γράψει κώδικα για να ακούει το Stellar ledger, να φέρνει εις πέρας συναλλαγές και να δοκιμάσει την ενσωμάτωση του χρήστη.

Το Stellar παρέχει λογισμικό, εργαλεία και αρχείο για να προσφέρει βοήθεια στην τεχνική πλευρά της διαδικασίας ενσωμάτωσης. Το δίκτυο του Stellar είναι δωρεάν. Δεν υπάρχουν περιορισμοί όσον αφορά την εμπορική χρήση της πλατφόρμας. Μια συναλλαγή στο δίκτυο αποτελείται από μια ή περισσότερες λειτουργίες. Πληρωμές, προσφορές, και τέλη είναι παραδείγματα λειτουργιών που μπορεί να αποτελούν μια απλή συναλλαγή. Ανάλογα το υπολογιστικό υλικό και τις ρυθμίσεις του δικτύου, μια συντηρητική εκτίμηση του ρυθμού επεξεργασίας του Stellar είναι 1000 λειτουργίες ανά δευτερόλεπτο. Υπάρχουν βασικά τέλη, τα οποία συνδέονται με κάθε λειτουργία σε μια συναλλαγή. Τα βασικά αυτά τέλη λειτουργούν για να αποτρέπουν τους χρήστες με κακόβουλες προθέσεις να πλημμυρίζουν το δίκτυο με συναλλαγές (γνωστές και ως επιθέσεις DoS). Κανείς δε βγάζει κέρδος από τα

τέλη, από τη στιγμή που το ποσό είναι πάρα πολύ μικρό. Το καθολικό συλλέγει τα τέλη και τα ανακατανέμει στη διαδικασία του πληθωρισμού. Ενώ οι συναλλαγές είναι μη αντιστρέψιμες στο δίκτυο του Stellar, είναι πιθανό να παγώσει κάποιος τα στοιχεία που έχει τοποθετήσει. Το πάγωμα ενός στοιχείου καθιστά το στοιχείο άνευ αξίας για το χρήστη, διασφαλίζοντας ότι μπορεί να αποσταλεί μόνο στο χρήστη που το έστειλε. Το δίκτυο του Stellar μετριάζει το ρίσκο μέσω μιας αποκεντροποιημένης και κατανεμημένης δομής. Αν το Stellar.org ήταν να εξαφανιστεί, το δίκτυο θα συνέχιζε να επιβεβαιώνει συναλλαγές, και οι σταθεροποιητές θα μπορούσαν ακόμα να ενσωματώνονται στο δίκτυο οποιαδήποτε στιγμή. Όλοι οι μηχανισμοί επικύρωσης του Stellar Core λειτουργούν μέσω μελών της κοινότητας, τα οποία είναι έξω από το Stellar.org. Τέλος, όλες οι συναλλαγές στο δίκτυο είναι δημόσιες. Με τη χρήση ειδικών εργαλείων όμως, είναι δυνατές και ιδιωτικές συναλλαγές [55].

11. NEO: Το NEO είναι ένα έργο ανοιχτού κώδικα που καθοδηγείται από την κοινότητα. Χρησιμοποιεί τεχνολογία blockchain και ψηφιακές ταυτότητες για την ψηφιοποίηση περιουσιακών στοιχείων και την αυτοματοποίηση της διαχείρισης ψηφιακών στοιχείων χρησιμοποιώντας έξυπνα συμβόλαια. Με τη χρήση κατανεμημένου δικτύου, στοχεύει στη δημιουργία μιας «Έξυπνης Οικονομίας». Το NEO ιδρύθηκε το 2014 και εισήλθε στο GitHub τον Ιούνιο του 2015. Το MainNet του κυκλοφόρησε τον Οκτώβριο του 2016 και λειτουργεί με σταθερή χωρητικότητα για 2 χρόνια. Το όραμα για «έξυπνη οικονομία» εγκαταστάθηκε μαζί με την ανακατασκευή του έργου το 2017. Η υποβόσκουσα υποδομή του NEO υποστηρίζει πολλαπλούς τύπους ψηφιακών στοιχείων. Οι χρήστες μπορούν να καταχωρήσουν, να μεταφέρουν και να ανταλλάξουν στοιχεία με τη σύνεσή τους στο NEO. Τα ψηφιακά πιστοποιητικά υποστηρίζονται για να χτίσουν εμπιστοσύνη στη δημόσια αλυσίδα. Αυτό παρέχει πλήρη νόμιμη προστασία για όλα τα στοιχεία που έχουν ψηφιοποιηθεί μέσω της πλατφόρμας NEO. Πωλητές και αγοραστές ψηφιακών στοιχείων και νομισμάτων θα ενώνονται με peer-to-peer χωρίς την ανάγκη συναλλαγών μέσω τρίτων. Όσον αφορά τα συμβόλαια, χρησιμοποιούνται Turing-complete έξυπνα συμβόλαια, τα οποία διαθέτουν μεγάλη σιγουριά και οριστικότητα, υποστηρίζουν ταυτόχρονες λειτουργίες και ασταμάτητη επεκτασιμότητα όταν τρέχουν στο NeoVM. Το NeoVM (Neo Virtual Machine) αποτελεί την εικονική μηχανή του NEO και παρέχει μικρότερους χρόνους εκκίνησης με ακριβή εκτέλεση. Το NeoContract υποστηρίζει πολλές γλώσσες προγραμματισμού όπως C#, Java και Python. Οι προγραμματιστές μπορούν να αναπτύξουν ταχύτατα έξυπνα συμβόλαια βασισμένα στην πλατφόρμα NEO χωρίς να μαθαίνουν μια μοναδική γλώσσα. Οι κόμβοι συναίνεσης χρησιμοποιούν BFTA (Byzantine Fault Tolerance Algorithm) για να επιδιώξουν τη συναίνεση και να σιγουρέψουν την οριστικότητα των συναλλαγών. Επίσης, βοηθάει στο να σιγουρέψουν πως το σύστημα διατηρεί την οριστικότητά του και τη διαθεσιμότητά του όσο συμβαίνει το Byzantine Fault σε λιγότερους από το 1/3 των κόμβων [56].

3.8 Blockchain και έξυπνα συμβόλαια

Μέσα στο blockchain, υπάρχουν αποθηκευμένα και τα έξυπνα συμβόλαια (smart contracts). Αφού «κατοικούν» στο blockchain, το καθένα έχει και μια μοναδική διεύθυνση. Ένα έξυπνο συμβόλαιο ενεργοποιείται όταν απευθυνόμαστε με μια συναλλαγή σε αυτό. Έπειτα, εκτελείται ανεξάρτητα και αυτόματα με προκαθορισμένο τρόπο σε κάθε κόμβο στο δίκτυο, σύμφωνα με τα δεδομένα που περιείχε η συναλλαγή που το ενεργοποίησε.

Τα έξυπνα συμβόλαια μας επιτρέπουν να έχουμε υπολογισμούς γενικού σκοπού μέσα στην αλυσίδα. Ο τομέας που εξέχουν όμως, είναι όταν τους ανατεθεί η διαχείριση αλληλεπιδράσεων με βάση τα δεδομένα, μεταξύ οντοτήτων στο δίκτυο. Στην συνέχεια ακολουθεί ένα παράδειγμα για να γίνει περισσότερο κατανοητή η έννοια. Υποθέτουμε ότι υπάρχει ένα δίκτυο όπου παίρνουν μέρος η Alice και ο Bob, και ανταλλάσσονται ψηφιακά στοιχεία τύπου X και Y. Ο Bob χρησιμοποιεί ένα έξυπνο συμβόλαιο στο δίκτυο το οποίο ορίζει:

α) Μια συνάρτηση «κατάθεση» που του επιτρέπει να καταθέσει μονάδες του X μέσα στο συμβόλαιο.

β) Μια συνάρτηση «συναλλαγή» που στέλνει πίσω μια μονάδα του X (από τις καταθέσεις του ίδιου του συμβολαίου) για κάθε 5 μονάδες Y που λαμβάνει.

γ) Μια συνάρτηση «ανάληψη» που επιτρέπει στον Bob να κάνει ανάληψη όλων των στοιχείων που δεσμεύονται στο συμβόλαιο.

Σε αυτό το σημείο να σημειωθεί ότι οι συναρτήσεις «κατάθεση» και «ανάληψη» είναι γραμμένες έτσι ώστε μόνο ο Bob (μέσω του κλειδιού του) να μπορεί να τις καλέσει, επειδή αυτή είναι η απόφαση του. Οι συναρτήσεις αυτές, θα μπορούσαν να έχουν γραφτεί έτσι ώστε να μπορεί οποιοσδήποτε χρήστης του δικτύου να τις καλέσει.

Ο Bob στέλνει μια συναλλαγή στη διεύθυνση του έξυπνου συμβολαίου, καλώντας τη συνάρτηση «κατάθεση» και μετακινώντας 3 μονάδες του X στο συμβόλαιο. Αυτή η συναλλαγή καταγράφεται στο blockchain. Η Alice, που κατέχει 12 μονάδες του Y, στέλνει μια συναλλαγή που μετακινεί 10 μονάδες του Y στη συνάρτηση «συναλλαγή» του συμβολαίου και παίρνει πίσω 2 μονάδες του X. Και αυτή η συναλλαγή καταγράφεται στο blockchain. Έπειτα, ο Bob στέλνει μια υπογεγραμμένη συναλλαγή στη συνάρτηση «ανάληψη» του συμβολαίου. Το συμβόλαιο ελέγχει την υπογραφή για να σιγουρευτεί ότι η ανάληψη ξεκίνησε από τον ιδιοκτήτη του συμβολαίου και μεταφέρει όλες του τις καταθέσεις (1 μονάδα X και 10 μονάδες Y) πίσω στον Bob.

Για καλύτερη χρήση των έξυπνων συμβολαίων θα ήταν ωφέλιμο να προσέξουμε τα παρακάτω:

- Το συμβόλαιο διαθέτει μια δική του κατάσταση και μπορεί να πάρει την επιμέλεια διαφόρων στοιχείων στο blockchain. Λέμε ότι το κάθε συμβόλαιο έχει το δικό του λογαριασμό στο blockchain και το blockchain υποστηρίζει ένα μοντέλο βασισμένο στους λογαριασμούς.
- Το συμβόλαιο μας επιτρέπει να εκφράσουμε επιχειρηματική λογική σε κώδικα (όπως π.χ. θα γίνεται συναλλαγή 1 μονάδας X για κάθε 5 μονάδες Y που λαμβάνονται)
- Ένα καλογραμμένο έξυπνο συμβόλαιο περιγράφει όλα τα πιθανά αποτελέσματά του. Για παράδειγμα, η συνάρτηση «συναλλαγή» που αναφέραμε μπορεί να είναι γραμμένη έτσι ώστε να απορρίπτει προσφορές που φέρνουν ποσότητες του Y που δεν είναι πολλαπλάσια του 5. Η συνάρτηση μπορεί επίσης να είναι γραμμένη έτσι ώστε να αναλύει την εισερχόμενη προσφορά ως το μεγαλύτερο πολλαπλάσιο του 5 (που θα ανταλλάσσεται χωρίς πρόβλημα) και το υπόλοιπο (που θα επιστρέφεται). Έτσι, μια προσφορά 12 μονάδων Y θα επέστρεφε 2 μονάδες X και 2 μονάδες Y στον αποστολέα.
- Η σχέση που επιθυμεί ο Bob να καθιερώσει με τα άλλα μέλη καθοδηγείται από τα δεδομένα. Μια συναλλαγή είναι μια υπογεγραμμένη δομή δεδομένων που υποδεικνύει τη μεταφορά κάποιας αξίας. Ο Bob χρησιμοποιεί ένα έξυπνο συμβόλαιο, το οποίο στην ουσία λέει ‘αν στείλεις σε αυτό το συμβόλαιο αυτά τα δεδομένα, η αντίδρασή του θα είναι αυτή’.
- Ένα έξυπνο συμβόλαιο ενεργοποιείται από μηνύματα/συναλλαγές που στέλνονται στη διεύθυνσή του.
- Ένα έξυπνο συμβόλαιο είναι προσδιοριστικό. Δηλαδή, η ίδια εισαγωγή θα παράγει πάντα το ίδιο αποτέλεσμα. Εάν κάποιος γράψει ένα μη προσδιοριστικό συμβόλαιο, όταν ενεργοποιηθεί θα εκτελεστεί σε κάθε κόμβο στο δίκτυο και μπορεί να επιστρέψει διάφορα τυχαία αποτελέσματα, εμποδίζοντας έτσι το δίκτυο να επιτύχει συναίνεση ως προς το αποτέλεσμα της εκτέλεσης. Σε μια καλοχτισμένη πλατφόρμα blockchain, το να γράφεις μη προσδιοριστικά έξυπνα συμβόλαια είναι είτε αδύνατο (με το να ωθείς τους προγραμματιστές του συμβολαίου να χρησιμοποιούν μια προγραμματιστική γλώσσα που δεν έχει μη προσδιοριστικές δομές), είτε δυνατόν αλλά μια προσπάθεια να ενεργοποιήσεις τέτοιο συμβόλαιο στο δίκτυο θα απορριφθεί.
- Ένα έξυπνο συμβόλαιο κατοικεί στο blockchain, και έτσι ο κωδικός του μπορεί να επιθεωρηθεί από οποιονδήποτε συμμετέχοντα στο δίκτυο.
- Από τη στιγμή που όλες οι αλληλεπιδράσεις με ένα συμβόλαιο συμβαίνουν μέσω υπογεγραμμένων μηνυμάτων στο blockchain, όλοι οι συμμετέχοντες στο δίκτυο λαμβάνουν ένα κρυπτογραφημένο μονοπάτι των ενεργειών του συμβολαίου.

Ένα blockchain που υποστηρίζει συναλλαγές τύπου Bitcoin, επιτρέπει τις μεταφορές στοιχείων μεταξύ μελών που δεν έχουν εμπιστοσύνη μεταξύ τους. Ένα blockchain που υποστηρίζει έξυπνα συμβόλαια ωστόσο, πάει ένα βήμα παραπέρα και επιτρέπει να γίνονται μεταξύ μελών χωρίς εμπιστοσύνη μεταξύ τους διαδικασίες με πολλαπλά βήματα. Οι οντότητες των συναλλαγών μπορούν να: α) επιθεωρούν τον κώδικα και να προβλέπουν το αποτέλεσμα πριν αποφασίσουν να έρθουν σε επαφή με το συμβόλαιο, β) έχουν σιγουριά για την εκτέλεση από τη στιγμή που ο

κώδικας έχει ήδη αναπτυχθεί σε ένα δίκτυο το οποίο κανείς τους δεν ελέγχει πλήρως, και γ) έχουν τη δυνατότητα επαλήθευσης της διαδικασίας αφού όλες οι αλληλεπιδράσεις υπογράφονται ψηφιακά. Η πιθανότητα για οποιαδήποτε διένεξη μηδενίζεται από τη στιγμή που οι συμμετέχοντες δεν μπορούν να διαφωνήσουν για το τελικό αποτέλεσμα της επαληθευμένης διαδικασίας στην οποία έλαβαν μέρος.

Τα έξυπνα συμβόλαια ενεργούν αυτόνομα και η συμπεριφορά τους είναι απολύτως προβλέψιμη. Έτσι μπορούν όλοι να τα εμπιστευτούν με το καθήκον της καθοδήγησης οποιασδήποτε λογικής πάνω στην αλυσίδα, η οποία μπορεί να εκφραστεί σαν συνάρτηση εισαγωγών δεδομένων πάνω στην αλυσίδα, με την προϋπόθεση τα δεδομένα που πρέπει να διαχειριστούν είναι σε συμβατό για αυτά σημείο.

Τέλος, αξίζει να σημειωθεί ότι τα έξυπνα συμβόλαια προωθούν την ιδέα των αποκεντρωμένων αυτόνομων οργανισμών (DAOs), που αποτελούν οντότητες στο blockchain των οποίων η συμπεριφορά μπορεί να τροποποιηθεί, αν ακολουθηθεί συγκεκριμένη διαδικασία που είναι κωδικοποιημένη στο συμβόλαιο. Το πιο απλό παράδειγμα είναι αυτό όπου ένα έξυπνο συμβόλαιο καλεί ένα άλλο συμβόλαιο μέσω της διεύθυνσης για να εκτελέσει τη βασική του συνάρτηση. Αυτή η διεύθυνση βρίσκεται στο μεταβλητό τμήμα της εσωτερικής βάσης δεδομένων του συμβολαίου. Το συμβόλαιο επίσης κουβαλάει μια λίστα μελών, διευθύνσεων (δημόσια κλειδιά) που μπορούν να ψηφίσουν σχετικά με τη συμπεριφορά του. Επίσης, στο συμβόλαιο μπορεί να περιέχεται ένας κανόνας, έτσι ώστε αν η πλειοψηφία αυτών που ψηφίζουν, ψηφίσουν κατά έναν συγκεκριμένο τρόπο, το συμβόλαιο θα τροποποιήσει τη συμπεριφορά του καλώντας τη διεύθυνση που μάζεψε τις περισσότερες ψήφους να εκτελέσει τη βασική του συνάρτηση [17].

3.9 Πλεονεκτήματα χρήσης του Blockchain

Οι τεχνολογίες Blockchain δεν είναι απλά μια μόνο τεχνική, αλλά περιέχουν κρυπτογραφία, μαθηματικά, αλγορίθμους και οικονομικά μοντέλα, συνδυάζοντας δίκτυα peer-to-peer και χρησιμοποιώντας κατανεμημένο αλγόριθμο συναίνεσης για την επίλυση του παραδοσιακού κατανεμημένου προβλήματος συγχρονισμού βάσεων δεδομένων, αποτελώντας έτσι μια ολοκληρωμένη δομή πολλαπλών πεδίων. Υπάρχουν πολλά οφέλη στην τεχνολογία Blockchain και με τη χρήση του έχουμε καταφέρει να λύσουμε αρκετά προβλήματα που αντιμετωπίζαμε μέχρι σήμερα. Το βασικό του πλεονέκτημα είναι η αποκεντροποίηση, κάτι που σημαίνει ότι δε χρειάζεται να βασίζεται σε κάποιο κεντρικό κόμβο. Ως εκ τούτου τα δεδομένα μπορούν να καταγραφούν, να αποθηκευτούν και να ανανεωθούν με κατανεμημένο τρόπο. Αυτό που δελεάζει αρκετούς χρήστες στο να το χρησιμοποιήσουν είναι η διαφάνεια. Οι καταγραφές των δεδομένων από το σύστημα είναι διαφανείς σε κάθε κόμβο. Επίσης, κάθε κόμβος βλέπει τις ανανεώσεις των δεδομένων, κάτι το οποίο καθιστά το Blockchain αρκετά έμπιστο. Τα περισσότερα συστήματα

Blockchain είναι ανοιχτά σε όλους. Οι καταγραφές μπορούν να ελεγχθούν δημόσια και οποιοσδήποτε μπορεί να χρησιμοποιεί τις τεχνολογίες του Blockchain για να δημιουργήσει οποιαδήποτε εφαρμογή θέλει. Η αυτονομία που προσφέρει είναι, επίσης, ένα πολύ βασικό πλεονέκτημα, καθώς κάθε κόμβος στο σύστημα μπορεί να μεταφέρει ή να ανανεώσει δεδομένα με ασφάλεια, λόγω της βάσης της συναίνεσης. Η βασική ιδέα είναι η εμπιστοσύνη από τον κάθε χρήστη ξεχωριστά, σε όλο το σύστημα και κανείς δεν μπορεί να παρέμβει σε αυτό. Έτσι λύνεται και το πρόβλημα της εμπιστοσύνης από το Blockchain. Ένα τεράστιο προσόν του Blockchain είναι ότι παραμένει αμετάβλητο. Όλες οι καταγραφές διατηρούνται για πάντα και δεν μπορούν να αλλαχτούν, εκτός αν κάποιος καταφέρει να πάρει τον έλεγχο περισσότερων από το 51% των κόμβων ταυτόχρονα. Τέλος, μεγάλο ρόλο στην ανάπτυξη του Blockchain παίζει και η ανωνυμία. Οι τεχνολογίες Blockchain έλυσαν το πρόβλημα εμπιστοσύνης μεταξύ των κόμβων, έτσι ώστε η μεταφορά δεδομένων ή ακόμα και οποιαδήποτε συναλλαγή να είναι ανώνυμη. Το μόνο που πρέπει να γνωρίζουμε είναι η διεύθυνση blockchain του άλλου ατόμου [18].

Ένα ακόμα μεγάλο πρόβλημα, το οποίο λύνει το Blockchain, είναι οι ψηφιακές πληρωμές. Οι τρέχοντες εμπορικοί μηχανισμοί για την εκκαθάριση πληρωμών βασίζονται σε κεντρικά καθολικά για να καταγράφουν όλες τις συναλλαγές και να διατηρούν τα υπόλοιπα των λογαριασμών. Στην ουσία, η συναλλαγή διαβιβάζεται μια φορά από τα συμβαλλόμενα μέρη στο διαμεσολαβητή, ελέγχεται για την εγκυρότητά της, και συνεπώς προσαρμόζονται και οι δύο λογαριασμοί. Στο Blockchain, η συναλλαγή διαβιβάζεται σε όλους τους κόμβους του δικτύου, με αποτέλεσμα να χρειάζεται περισσότερη ενέργεια και περισσότερος χρόνος. Το Blockchain όμως χρησιμοποιείται στις ψηφιακές συναλλαγές, όχι για την ταχύτητα και φτηνότερες συναλλαγές, αλλά επειδή αφαιρεί την ανάγκη για εμπιστοσύνη σε τρίτους διαμεσολαβητές. Οι συναλλαγές είναι καθαρές επειδή οι κόμβοι διαγωνίζονται για το ποιος θα επαληθεύσει κάθε συναλλαγή, ενώ δεν υπάρχει ανάγκη για εμπιστοσύνη σε κάθε κόμβο [19]. Όσον αφορά τον οικονομικό τομέα, το Blockchain μπορεί να επιτύχει την ψηφιοποίηση των περιουσιακών στοιχείων και την point-to-point μεταφορά αξίας, ανασυγκροτώντας έτσι ολόκληρη την οικονομική υποδομή. Αυτό αυξάνει σημαντικά την αποτελεσματικότητα της διαδικασίας εκκαθάρισης και διακανονισμού των χρηματοοικονομικών περιουσιακών στοιχείων μετά από τις συναλλαγές, ενώ παράλληλα μειώνει το συνολικό κόστος [20]. Ως εκ τούτου, επιλύει σε μεγάλο βαθμό πολλά από τα υπάρχοντα προβλήματα στον τραπεζικό κλάδο, τα οποία ταλαιπωρούσαν όλους τους ενδιαφερόμενους για χρόνια.

Πολλές εταιρείες χρησιμοποιούν καθημερινά τις τεχνολογίες Blockchain για την αντιμετώπιση διαφόρων προβλημάτων και εμποδίων που τις ταλαιπωρούν. Αρκετή προσοχή πρέπει να δοθεί ωστόσο στα προβλήματα που λύνει το Blockchain μέσα στο IoT. Για παράδειγμα η εταιρεία IBM χρησιμοποιεί τη μεγάλη της υποδομή υπολογιστικού νέφους για να παρέχει τις υπηρεσίες του Blockchain προκειμένου να εντοπίζονται αντικείμενα υψηλής αξίας, καθώς κινούνται μέσα στις αλυσίδες εφοδιασμού. Επιπρόσθετα, η πλατφόρμα που δημιούργησε η IBM επιτρέπει στους χρήστες να προσθέτουν επιλεγμένα δεδομένα από το IoT σε ιδιωτικά καθολικά blockchain, τα οποία μπορούν να συμπεριληφθούν σε συναλλαγές που γίνονται σε κοινή χρήση. Η πλατφόρμα

μεταφράζει τα δεδομένα από τις συνδεδεμένες συσκευές, στη μορφή που χρειάζονται τα blockchain contract APIs (application programming interface). Τα δεδομένα δεν συλλέγονται, αποθηκεύονται ή διαχειρίζονται κεντρικά. Αντιθέτως, προστατεύονται και μοιράζονται μόνο στα μέλη που λαμβάνουν μέρος στη συναλλαγή.

Ίσως η σημαντικότερη χρήση του Blockchain, σε εφαρμογές μέσα στο IoT, γίνεται για την ασφάλεια που προσφέρει. Συστήματα που βασίζονται στο blockchain και διαχειρίζονται την ταυτότητα και την πρόσβαση των χρηστών έχουν ήδη χρησιμοποιηθεί για την ασφαλή αποθήκευση πληροφοριών για την προέλευση, την ταυτότητα, τα διαπιστευτήρια και τα ψηφιακά δικαιώματα των εμπορευμάτων και των αγαθών. Από τη στιγμή που οι πληροφορίες που εισήχθησαν είναι ακριβείς, μπορεί να επιτευχθεί σταθερότητα στο blockchain. Ένα ιδιωτικό Blockchain μπορεί να χρησιμοποιηθεί για την αποθήκευση κρυπτογραφικών hashes μεμονωμένων συσκευών. Ένα τέτοιο σύστημα δημιουργεί μια μόνιμη καταγραφή της ρύθμισης και της κατάστασης της συσκευής. Αυτή η καταγραφή μπορεί αργότερα να χρησιμοποιηθεί για να επαληθευτεί η εγκυρότητα μιας συσκευής και για να σιγουρευτούμε ότι το λογισμικό της συσκευής δεν έχει αλλοιωθεί ή δεν έχει εκτεθεί σε κινδύνους. Μόνο τότε επιτρέπεται στη συγκεκριμένη συσκευή να συνδεθεί σε άλλες συσκευές ή υπηρεσίες [21].

3.10.1 Χρήση του Blockchain στο MCS

Τα συστήματα Crowdsensing έχουν γνωρίσει μεγάλη ανάπτυξη τα τελευταία χρόνια με αποτέλεσμα να τραβούν το ενδιαφέρον όλο και περισσότερων χρηστών καθημερινά. Τα περισσότερα υπάρχοντα συστήματα, όμως, βασίζονται σε κεντρικούς διακομιστές, οι οποίοι πάσχουν από χαμηλή αξιοπιστία εξαιτίας της παραδοσιακής κεντρικής αρχιτεκτονικής και του υψηλού κόστους υπηρεσίας. Δυο από τα μεγαλύτερα προβλήματα που παρουσιάζει η κεντρική αρχιτεκτονική των συστημάτων είναι η διαρροή απόρρητων πληροφοριών και το single point of failure. Είναι επίσης ευάλωτα σε επιθέσεις DDoS (Distributed Denial of Service) και επιθέσεις Sybil εξαιτίας της συμμετοχής στο όλο σύστημα κακόβουλων χρηστών. Επιπρόσθετα, το υψηλό κόστος υπηρεσίας που χρεώνει η πλατφόρμα crowdsensing, η οποία έχει το μονοπώλιο στην αγορά μπορεί να καθυστερήσει σημαντικά την ανάπτυξη του crowdsensing. Το πώς μπορούν να καταπολεμηθούν αυτά τα προβλήματα παραμένει ένα ανοιχτό θέμα για το οποίο οι ερευνητές ψάχνουν συνεχώς λύσεις.

Στο άρθρο Blockchain-based Crowd-sensing System οι συγγραφείς προτείνουν ένα σύστημα crowdsensing βασισμένο στο blockchain, το οποίο μπορεί ταυτόχρονα να εξαφανίσει τα προβλήματα ασφαλείας και ιδιωτικότητας. Προχωρούν στην υλοποίηση του BCS (blockchain-based crowdsensing system) με βάση το Ethereum, το οποίο επαληθεύει τη σκοπιμότητα και την

αποτελεσματικότητα του προτεινόμενου συστήματος. Επίσης, περαιτέρω θεωρητικές αναλύσεις και πειράματα αποδεικνύουν την ασφάλεια και την αποτελεσματικότητα του BCS. Όντας διαφορετικό από την παραδοσιακή αρχιτεκτονική, στο αποκεντρωμένο σύστημα που βασίζεται στο blockchain, δεν υπάρχει κεντρική πλατφόρμα στη διαδικασία του crowdsensing. Αντ' αυτού, με τη μόχλευση της τεχνικής blockchain, η διαδικασία crowdsensing διαχειρίζεται από ένα αποκεντρωμένο σύστημα. Γνωρίζουμε ότι σε αυτή την αρχιτεκτονική το BCS αποτελείται από πέντε ομάδες ρόλων: τους αιτούντες, τους εργάτες, τους miners, το blockchain και την πλατφόρμα επικοινωνίας. Η διαδικασία crowdsensing του BCS μπορεί να διαιρεθεί στα παρακάτω τέσσερα βήματα:

1. Οι αιτούντες αναρτούν εργασίες, στη συνέχεια αρχικοποιούν τους κανόνες εξέτασης και τα στέλνουν στην πλατφόρμα επικοινωνίας.
2. Οι εργάτες ζητούν από το blockchain δημοσιευμένα έξυπνα συμβόλαια και αποκτούν ελκυστικές εργασίες ανίχνευσης. Αφού ολοκληρώσουν τις εργασίες με την καταγραφή δεδομένα ανίχνευσης, αναρτούν τα δεδομένα στην πλατφόρμα επικοινωνίας.
3. Αναζητώντας στο blockchain και ακούγοντας την πλατφόρμα επικοινωνίας, οι miners αντλούν ανεπιβεβαίωτα δεδομένα ανίχνευσης και στη συνέχεια εξετάζουν την ποιότητα τους με βάση τους κανόνες που θέτει ο αιτών. Αφού οι miners επιβεβαιώσουν την ποιότητα των δεδομένων ανίχνευσης, θα λάβουν μαζί με τους εργάτες τις ανταμοιβές μόλις ολοκληρώσουν την προώθηση των επεξεργασμένων δεδομένων στα μπλοκ. Γενικά, οι miners κερδίζουν ανταμοιβές συμβάλλοντας την υπολογιστική ισχύ για τη διεξαγωγή των έξυπνων συμβολαίων.
4. Οι αιτούντες ακούν το blockchain περιοδικά. Μόλις αποφασίσουν ότι δε θέλουν να συνεχίσουν να συλλέγουν δεδομένα, μπορούν να στείλουν μήνυμα στο σύστημα για να κλείσουν την εργασία και να πάρουν τα χρήματα που έχουν απομείνει από το έξυπνο συμβόλαιο. Καθώς αυτό το μήνυμα θα μεταδοθεί στο σύστημα, οι miners και οι εργάτες θα σταματήσουν να εργάζονται.

Πιο συγκεκριμένα, οι αιτούντες δημιουργούν έξυπνα συμβόλαια θέτοντας απαιτήσεις για τα δεδομένα ανίχνευσης και αποθηκεύουν ένα συγκεκριμένο ποσό των καταθέσεων για τον καθορισμό των ανταμοιβών. Μετά από αυτό, όταν οι εργάτες προσελκυθούν από τις ανταμοιβές και τα δεδομένα τους επιβεβαιωθούν από τους miners, μπορούν να λάβουν αμέσως ανταμοιβές που έχουν αποθηκευτεί στο πρωτόκολλο του έξυπνου συμβολαίου. Έτσι, η φήμη του συστήματος μπορεί να χτιστεί γρήγορα και ο ενθουσιασμός των miners και των εργατών να αυξηθεί [22].

Εν συνεχεία, βλέπουμε στο άρθρο CrowdBC: A Blockchain-based Decentralized Framework for Crowdsourcing να υποστηρίζεται ακόμα μια αποκεντρωμένη δομή. Οι συγγραφείς υλοποιούν μια αποκεντρωμένη δομή για crowdsourcing βασισμένη στο blockchain, αλλά ταυτόχρονα δε βασίζεται σε κανένα κεντρικό τρίτο μέλος για να φέρει εις πέρας τη διαδικασία του crowdsourcing. Το CrowdBC εγγυάται ιδιωτικότητα, επιτρέποντας στους χρήστες να κάνουν

εγγραφή χωρίς τη χρήση της κανονικής τους ταυτότητας και να αποθηκεύουν κρυπτογραφημένες λύσεις στην κατανεμημένη αποθήκη. Κάθε ταυτότητα κάνει μια κατάθεση πριν τη συμμετοχή, κάτι το οποίο μπορεί να αποτρέψει διάφορες επιθέσεις (όπως DDoS, Sybil κ.ά.). Επιπρόσθετα, οι χρήστες δε χρειάζεται πια να πληρώσουν το ακριβό κόστος υπηρεσίας στην παραδοσιακή πλατφόρμα crowdsourcing, παρά μόνο κάποια μικρά ποσά σε τέλη συναλλαγών. Η δομή που προτείνουν ενισχύει την ευελιξία του crowdsourcing με τη χρήση Turing-complete γλώσσας προγραμματισμού για την απεικόνιση πολύπλοκων λογικών.

Στην προτεινόμενη δομή, τα έξυπνα συμβόλαια χρησιμοποιούνται για την εκτέλεση ολόκληρης της διαδικασίας της εργασίας crowdsourcing, η οποία περιλαμβάνει την ανάρτηση εργασιών, τη λήψη εργασιών, την αξιολόγηση εργασιών, την ανάθεση ανταμοιβής κ.λπ. Παρουσιάζουν τρία σταθερά έξυπνα συμβόλαια: το User Register Contract (URC), το User Summary Contract (USC) και το Requester-Worker Relationship Contract (RWRC), με τα οποία μπορούν να επιτευχθούν λειτουργίες crowdsourcing όπως η ανάρτηση και η λήψη μιας εργασίας χωρίς να βασίζεσαι σε κάποια κεντρική αρχή. Συγκεκριμένα, σε σύγκριση με τα παραδοσιακά συστήματα, το πιο χρήσιμο χαρακτηριστικό έγκειται στην αξιολόγηση των εργασιών που πρέπει να ολοκληρωθούν μέσω έξυπνων συμβολαίων και όχι μέσω ενός τρίτου μέλους. Οι συγγραφείς αναμένουν ότι αυτή η κατασκευή θα αποδειχθεί αρκετά αποτελεσματική και χρήσιμη στην πράξη.

Οι συγγραφείς εφαρμόζουν το προτεινόμενο σχήμα για να επαληθεύσουν την εφαρμοσιμότητα μέσω ενός πρωτότυπου λογισμικού βασισμένο στο Ethereum με πραγματικό σύνολο δεδομένων. Τα αποτελέσματα των πειραμάτων δείχνουν την εγκυρότητα και την αποτελεσματικότητα του προτεινόμενου συστήματος crowdsourcing. Επιπρόσθετα, είναι ανοιχτοί σε συζητήσεις για διάφορες μελλοντικές βελτιώσεις πάνω στην πρότασή τους.

Στη συνέχεια γίνεται μια πιο αναλυτική αναφορά στην προτεινόμενη δομή. Αρχικά, οι χρήστες χωρίζονται σε τρεις τύπους: τους αιτούντες, τους εργάτες και τους miners. Το CrowdBC είναι μια αποκεντρωμένη δομή crowdsourcing, η οποία μπορεί να υποστηρίξει, όπως προαναφέραμε, προγράμματα που είναι Turing-complete. Ο αιτών και ο εργάτης πρέπει να κάνουν εγγραφή για να πάρουν τα διαπιστευτήριά τους πριν την απόκτηση υπηρεσιών από το CrowdBC. Οι αιτούντες αναρτούν εργασίες μεταφέροντας την περιγραφή των εργασιών με ένα ποσό ανταμοιβής στα προγράμματα. Λαμβάνοντας τα πλεονεκτήματα των προγραμμάτων, τα οποία εκτελούνται αυτόματα σε έμπιστη πλατφόρμα blockchain, οι αιτούντες επιλέγουν τους κατάλληλους εργάτες και παίρνουν τη λύση που τους ικανοποιεί. Οι εργάτες αποτελούν την κοινότητα, έχουν συγκεκριμένες ικανότητες, ανταγωνίζονται για την εργασία και λαμβάνουν ανταμοιβές. Ο κάθε εργάτης συνδέεται με μια φήμη, η οποία αντιπροσωπεύει τη μέχρι τώρα συμπεριφορά του στην επίλυση εργασιών. Πιστοποιημένοι εργάτες, των οποίων η φήμη ικανοποιεί την ελάχιστη τιμή, μπορούν να ανταγωνιστούν για την εργασία και να υποβάλλουν λύσεις. Με τη χρήση των Turing-complete προγραμμάτων στο blockchain, ο εργάτης μπορεί να έρθει σε συμφωνία με τον αιτούντα. Μετά την αξιολόγηση των λύσεών τους, τους αποδίδεται η

αντίστοιχη ανταμοιβή. Οι miners προσθέτουν αρχεία περασμένων συναλλαγών στο blockchain και επικυρώνουν ένα νέο μπλοκ από το πρωτόκολλο συναίνεσης. Εξασφαλίζουν την ασφάλεια του blockchain και μπορούν να κερδίσουν τέλη συναλλαγών και ανταμοιβές για την εξόρυξη. Εκτός από αυτά, μπορούν να κάνουν εγγραφή στο CrowdBC και να αναρτούν ή να λαμβάνουν εργασίες [23].

Ένα ακόμα άρθρο στο οποίο προτείνεται η χρήση του blockchain στο mobile crowdsensing είναι το A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications. Οι βασικές συνεισφορές των συγγραφέων μέσω της δομής που προτείνουν είναι οι εξής:

- Προτείνουν έναν ασφαλή μηχανισμό παροχής κινήτρων που θα βασίζεται στο blockchain, η εξακρίβωση της ποιότητας των δεδομένων από τους miners μπορεί να εξαλείψει τα ζητήματα ασφάλειας και ιδιωτικότητας που προκαλούνται από μια κεντρική αρχή.
- Χρησιμοποιούν μια εκτεταμένη σύνταξη συναλλαγής για την εφαρμογή μιας ασφαλούς διανομής ανταμοιβής σύμφωνα με τις προκαθορισμένες συνθήκες μεταφοράς στο σενάριο των συναλλαγών.
- Επίσης, προτείνουν μια συνεργατική μέθοδο προστασίας της ιδιωτικότητας για να πετύχουν οι συμμετέχοντες χρήστες προστασία τύπου k-anonymity.
- Τέλος, χρησιμοποιούν μια θεωρητική ανάλυση και μελέτη προσομοίωσης για να κάνουν επίδειξη της ασφάλειας και της αποτελεσματικότητας του μηχανισμού παροχής κινήτρων που χρησιμοποιούν.

Σε αυτό το άρθρο, ο μηχανισμός παροχής κινήτρων ενθαρρύνει τους χρήστες να υποβάλλουν δεδομένα ανίχνευσης υψηλής ποιότητας βασισμένα στη δομή του blockchain, τα οποία συντηρούνται από κόμβους miners. Η κατανεμημένη δομή εξαλείφει τα ζητήματα ασφαλείας που προκαλεί μια κεντρική αρχή. Ένας χρήστης λαμβάνει διαφορετική πληρωμή ανάλογα με τη διαφορετική ποιότητα δεδομένων. Η διαδικασία όπου ο χρήστης ανεβάζει τα δεδομένα ανίχνευσης και ο διακομιστής πληρώνει για τα συγκεκριμένα δεδομένα, αντιμετωπίζεται ως συναλλαγή. Οι miners επαληθεύουν κάθε νέα συναλλαγή και τις καταγράφουν στο peer-to-peer δίκτυο. Ανά διαστήματα θα υπάρχει νέο μπλοκ, το οποίο θα μπορεί να δεχθεί εξόρυξη. Κάθε μπλοκ περιλαμβάνει όλες τις συναλλαγές που προέκυψαν από τη δημιουργία του τελευταίου μπλοκ έως τώρα. Αυτές οι συναλλαγές προστίθενται στο blockchain με τη σειρά. Η προαναφερθείσα διαδικασία και η διαχείριση των μπλοκ εμπνέονται από τη συναλλαγή στο blockchain. Η συναλλαγή, η οποία περιλαμβάνεται στο μπλοκ και προστίθεται στην αλυσίδα ονομάζεται επιβεβαιωμένη συναλλαγή. Ο χρήστης θα λάβει την ανταμοιβή του μετά την επιβεβαίωση της συναλλαγής. Υποθέτουμε ότι υπάρχουν κανόνες πληρωμής για τους miners στη δομή blockchain. Οποιοσδήποτε στο blockchain μπορεί να είναι «χρήστης» αν ανεβάζει τα δεδομένα ανίχνευσης, ή «miner» αν αξιολογεί την ποιότητα των δεδομένων ή ολόκληρη τη

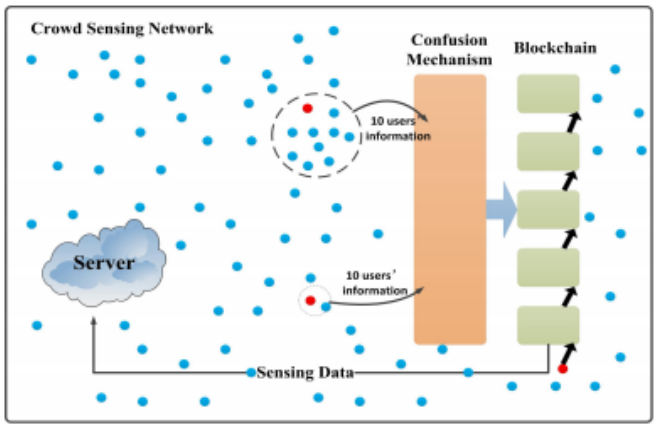
συναλλαγή. Έτσι, ένας κόμβος μπορεί να είναι «χρήστης» ή «miner» λόγω της δουλειάς του, ή σε κάποιες περιπτώσεις ακόμα και τα δυο.

Στη συνέχεια, έχουμε μια αναλυτικότερη αναφορά για το πως δουλεύει ο μηχανισμός κινήτρων. Αρχικά, ο διακομιστής εμφανίζει την εργασία ανίχνευσης με κριτήρια αξιολόγησης της ποιότητας των δεδομένων και προπληρώνει μια κατάθεση. Έπειτα, ο χρήστης εκτελεί την εργασία και ανεβάζει τα δεδομένα ανίχνευσης στο peer-to-peer δίκτυο. Οι miners επικυρώνουν την ποιότητα των δεδομένων με τη γνώση της συνάρτησης αξιολόγησης που επιτυγχάνεται από το διακομιστή, προσδιορίζουν την ποσότητα της συνεισφοράς και καθορίζουν τα κριτήρια πληρωμής. Ουσιαστικά επικυρώνουν τη συναλλαγή του διακομιστή και του χρήστη. Τελικά, σύμφωνα με τα κριτήρια πληρωμής, ο διακομιστής πληρώνει το χρήστη αφού περάσουν οι επαληθεύσεις των δεδομένων ανίχνευσης και της ταυτότητας του χρήστη. Το νέο μπλοκ περιλαμβάνει την επιβεβαιωμένη συναλλαγή και άλλες επιβεβαιωμένες συναλλαγές μέσα σε μια συγκεκριμένη περίοδο. Μετά την επαλήθευση της συναλλαγής, τα δεδομένα ανίχνευσης αποστέλλονται στο διακομιστή και η καταγραφή κατακερματισμού των δεδομένων αποθηκεύεται στο blockchain. Σημειώστε ότι η διαδικασία επαλήθευσης στο ανιχνεύσιμο δημόσιο blockchain μπορεί να ελεγχτεί από τον καθένα. Όπως οι miners μπορούν να αποκτήσουν τα περιεχόμενα της συναλλαγής όταν επικυρώνουν τα δεδομένα, μπορούν να εξαπολύσουν επίθεση πλαστοπροσωπίας ή κάποια άλλη σκευωρία για να λάβουν παράνομα την πληρωμή. Για να λυθεί αυτό το πρόβλημα, οι συγγραφείς προτείνουν μια μέθοδο επαλήθευσης συναλλαγών με τη συνεργασία των κόμβων, η οποία θα διατηρεί τις πληροφορίες απορρήτου του χρήστη μέσα σε μια ομάδα, μακριά από τις επιθέσεις διαφόρων κακόβουλων χρηστών [24].

Ένα άλλο άρθρο που περιστρέφεται γύρω από το συγκεκριμένο θέμα είναι το A blockchain-based location privacy protection incentive mechanism in crowd sensing networks. Η επέκταση της τεχνολογίας blockchain γεννήθηκε στο Bitcoin, αλλά δεν είναι μόνο για αυτό. Από τη στιγμή που η τεχνολογία blockchain έχει μοναδικές χρονικές σημάνσεις, αλυσιδωτή δομή, ασύμμετρη κρυπτογράφηση κλπ, τα δεδομένα που αποθηκεύονται στο blockchain έχουν χαρακτηριστικά όπως το ότι δεν μπορούν να πλαστοποιηθούν. Το συγκεκριμένο χαρακτηριστικό, το οποίο αποτρέπει την παραπλάνηση, έχει μεγάλη σημασία στους τομείς των έξυπνων πόλεων (smart cities), έξυπνων μεταφορών (intelligent transportation), του IoT, της οικονομίας και των συναλλαγών. Σηματοδοτεί την αρχή ενός πραγματικά αξιόπιστου διαδικτύου.

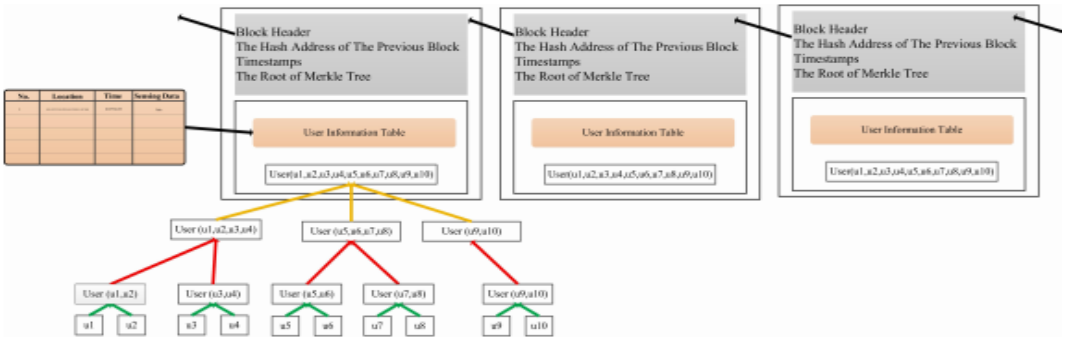
Όπως βλέπουμε στην Εικόνα 9, η δομή του δικτύου των blockchains μπορεί να χωριστεί σε τρία μέρη: ευφυή δίκτυα crowdsensing, μηχανισμός πρόκλησης αταξίας και φυσικά τα blockchains. Υπάρχουν δύο τύποι κόμβων στα δίκτυα crowdsensing. Ο ένας είναι ο συνηθισμένος κόμβος χρήστη που κουβαλάει τις πληροφορίες του χρήστη και ο άλλος είναι ένας κόμβος miner. Αυτός ο κόμβος δε φέρει πληροφορίες. Ο βασικός του ρόλος είναι να κάνει εξόρυξη το νέο χώρο του μπλοκ. Η πρωταρχική λειτουργία ενός διακομιστή σε ένα δίκτυο crowdsensing είναι η έκδοση πληροφοριών για εργασίες και η λήψη δεδομένων ανίχνευσης από το blockchain. Ο ρόλος του μηχανισμού πρόκλησης αταξίας είναι η επεξεργασία των δεδομένων

ανίχνευσης από τους κόμβους του δικτύου, η επίτευξη θωράκισης των δεδομένων του κόμβου και το να αποτρέψει τη διαρροή των προσωπικών πληροφοριών του κόμβου. Το blockchain περιλαμβάνει χαρακτηριστικά αποκεντροποίησης και φανερών πληροφοριών. Η χρήση μιας δομής blockchain μπορεί να αποτρέψει την αλλοίωση των πληροφοριών του χρήστη και να προστατέψει τις προσωπικές πληροφορίες κάθε χρήστη. Μετά την παρουσίαση των λειτουργιών κάθε μέρους, οι συγγραφείς περιγράφουν τη ροή εργασίας της δομής. Αρχικά, ο διακομιστής εκδίδει μια εργασία ανίχνευσης. Οι κόμβοι του δικτύου crowdsensing αποδέχονται την εργασία. Ο κόμβος συλλέγει τα δεδομένα ανίχνευσης και εισέρχεται στο μηχανισμό πρόκλησης αταξίας για προστασία των πληροφοριών του. Μετέπειτα, υπάρχει ένας συγκεκριμένος αριθμός miners που είναι κόκκινοι κόμβοι, στην εικόνα 9, οι οποίοι είναι υπεύθυνοι για το άνοιγμα νέων χώρων για τα μπλοκ. Ο μηχανισμός πρόκλησης αταξίας δημιουργεί ένα γκρουπ που περιλαμβάνει 10 χρήστες και έναν miner. Το γκρουπ αυτό χρησιμοποιείται για να χειριστούν τα δεδομένα των χρηστών αυτών. Μετά την αποθήκευση των δεδομένων των χρηστών στο blockchain, το blockchain θα δώσει στο χρήστη το εικονικό κέρμα σαν ανταμοιβή. Όσο μεγαλύτερη είναι η συχνότητα της συμμετοχής του χρήστη στην εργασία, τόσα περισσότερα κέρματα θα λάβει. Το εικονικό κέρμα μπορεί να ανταλλαχθεί για μετρητά. Τέλος, το blockchain αποθηκεύει τις πληροφορίες που χειρίστηκαν από το μηχανισμό πρόκλησης αταξίας, δυναμώνει την προστασία σε αυτόν και στέλνει τα δεδομένα ανίχνευσης στο διακομιστή [25].



Εικόνα 9 : Δομή κινήτρων βασισμένη στο Blockchain μέσα σε ένα δίκτυο Crowdsensing
Πηγή: (https://www.mdpi.com/1424-8220/18/11/3894/htm**) [25]**

Το blockchain γενικά έχει τα παρακάτω χαρακτηριστικά: αποκεντροποίηση, ανοικτότητα (είναι ανοιχτό για όλους), αυτονομία, ανωνυμία και οι πληροφορίες που έχει δεν μπορούν να αλλοιωθούν. Σε αυτό το άρθρο, οι συγγραφείς άλλαξαν τη δομή του blockchain. Η νέα δομή παρουσιάζεται αναλυτικά στην παρακάτω εικόνα (εικόνα 10)



Εικόνα 10 : Η εφαρμογη του Blockchain σε ένα δίκτυο Crowdsensing
Πηγή: (https://www.mdpi.com/1424-8220/18/11/3894/htm**) [25]**

Στο άρθρο MCS-Chain: Decentralized and trustworthy mobile crowdsourcing based on blockchain, οι συγγραφείς σχεδιάζουν ένα καινοτόμο σύστημα MCS βασισμένο στο blockchain, όπου η παραγωγή ενός νέου μπλοκ καθορίζεται από τη συνολική ποσότητα καταγραμμένων πληρωμών που περιμένουν να αποθηκευτούν στο επόμενο μπλοκ. Σχεδιάζουν επίσης ένα νέο αλγόριθμο συναίνεσης για την επαλήθευση των νέων μπλοκ. Εγγυάται ότι ένα μοναδικό μπλοκ μπορεί να καθοριστεί ακόμα κι αν εμφανιστούν ταυτόχρονα περισσότερα μπλοκ. Από τη στιγμή που δεν υπάρχουν έμπιστα μέλη στο σύστημα, προτείνουν ένα μηχανισμό αξιολόγησης εμπιστοσύνης για το MCS-Chain, με τον οποίο οι χρήστες θα μπορούν να επιλέγουν έμπιστους εργάτες. Αναλύουν τα θέματα της ασφάλειας και της διαθεσιμότητας του συστήματος. Για την ακρίβεια, αποδεικνύουν θεωρητικά την ασφάλεια, τη ζωτικότητα, την αποκεντροποίηση και την ανοχή στο λάθος του προτεινόμενου συστήματος. Τέλος, γίνεται εφαρμογή του MCS-Chain σε Windows και Android συσκευές και διεξάγονται διάφορα πειράματα βασισμένα στην εφαρμογή, προκειμένου να αξιολογηθεί η απόδοση του MCS-Chain. Τα πειραματικά αποτελέσματα δείχνουν την αποτελεσματικότητα και την αποδοτικότητα του προτεινόμενου συστήματος.

Στην Εικόνα 11 βλέπουμε το μοντέλο συστήματος του MCS-Chain. Το MCS-Chain περιέχει έναν αριθμό κόμβων (συμπεριλαμβανομένων και διαφόρων κινητών συσκευών) που είναι συνδεδεμένοι μεταξύ τους μέσω διαφόρων δικτύων όπως Wi-Fi, Bluetooth, κινητά δίκτυα. Οι κόμβοι του MCS μπορούν να χωριστούν σε 3 διαφορετικούς τύπους: τελικός χρήστης, εργάτης και miner, και κάθε κόμβος μπορεί να δράσει είτε σαν τελικός χρήστης, εργάτης ή miner. Μεταξύ τους, οι miners συνεργατικά διατηρούν και διαχειρίζονται το blockchain του MCS-Chain, που δημιουργήθηκε ειδικά για το mobile crowdsensing. Το Blockchain λειτουργεί σαν μια πλατφόρμα MCS, καταγράφει τις διαδικασίες του MCS και αξιολογεί την εμπιστοσύνη σε όλες τις οντότητες του συστήματος. Στο MCS-Chain, κάθε miner διατηρεί ένα αντίγραφο του blockchain και μπορεί να έχει πρόσβαση στα δεδομένα που είναι αποθηκευμένα εκτός του blockchain. Ένας τελικός χρήστης μπορεί να είναι ένα μόνο άτομο ή ένας ολόκληρος οργανισμός που δεν έχει την ικανότητα να φέρει εις πέρας μια συγκεκριμένη εργασία π.χ. συλλογή δεδομένων και επεξεργασία. Ζητάει την εκπλήρωση των εργασιών προσφέροντας την κατάλληλη πληρωμή σε αυτούς που εκτέλεσαν τις εργασίες. Εκτός αυτού, παρέχει επίσης ένα

συγκεκριμένο ποσό τέλους υπηρεσιών στους miners προκειμένου να τους δώσει κίνητρο να καταγράφουν με ειλικρίνεια και να επικυρώνουν τις σχετικές πληροφορίες εκτέλεσης εργασιών. Οι εργάτες του MCS είναι οι κόμβοι που συμμετέχουν στο crowdsourcing και εκτελούν τις εργασίες που έχουν ανατεθεί με βάση τη συμφωνία. Υπάρχουν κυρίως τρία είδη εργατών: εργάτες ανίχνευσης, εργάτες υπολογισμών και εργάτες αποθήκευσης. Η διαφορά μεταξύ τους βρίσκεται στις διαφορετικές εργασίες που διεκπεραιώνουν. Για την ακρίβεια, οι εργάτες ανίχνευσης αξιοποιούν τις κινητές συσκευές ως αισθητήρες για να συλλέξουν περιβαλλοντικά δεδομένα, όπως εικόνα, φωνή, θερμοκρασία κ.λπ. , ή να συλλέξουν απόψεις ή προσωπικά δεδομένα από τους κατόχους των συσκευών. Οι εργάτες υπολογισμών εκτελούν υπολογιστικές εργασίες και υποβάλλουν τα υπολογιστικά αποτελέσματα στον τελικό χρήστη. Οι εργάτες αποθήκευσης προσφέρουν υπηρεσίες αποθήκευσης δεδομένων με ασφαλή έλεγχο πρόσβασης στα δεδομένα [26].

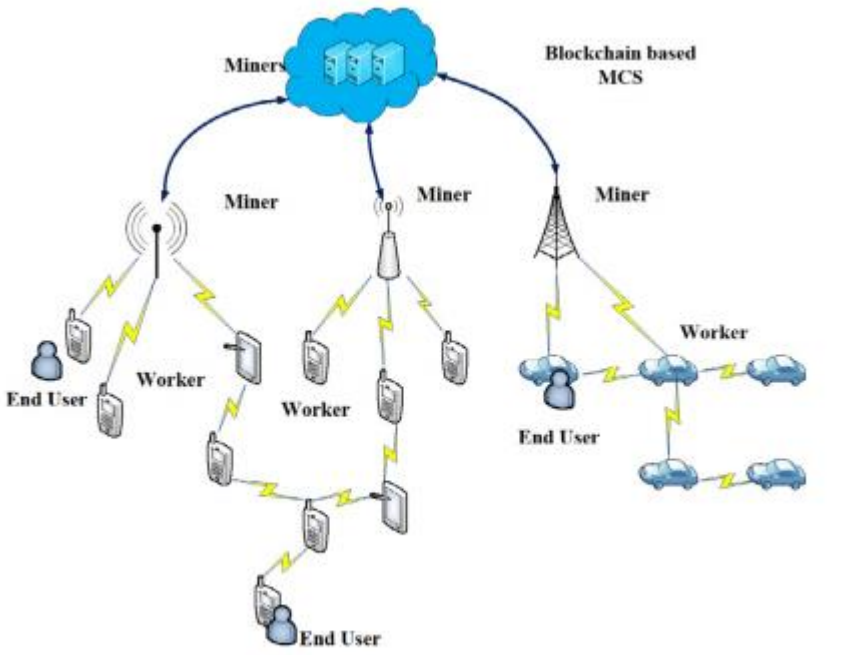
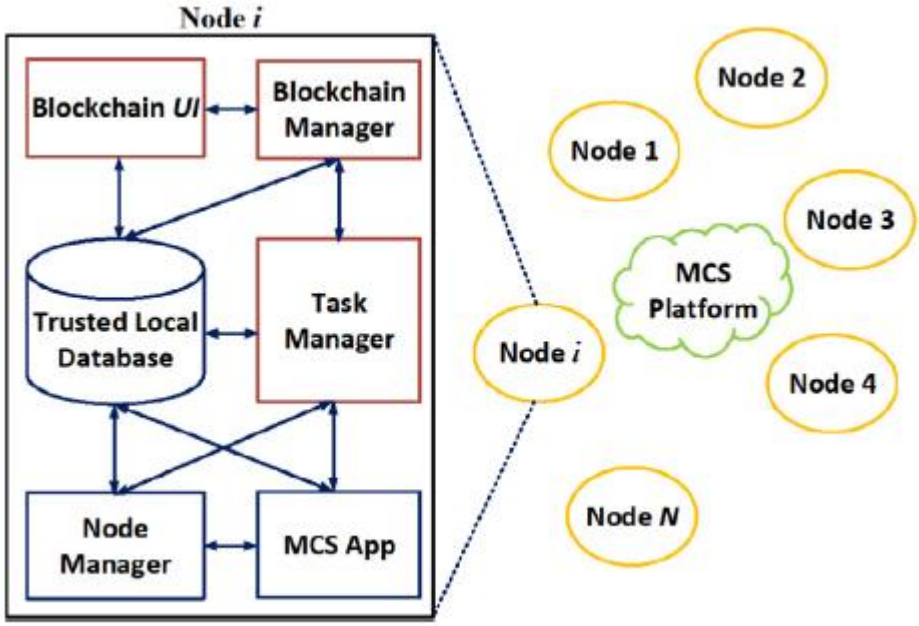


Fig. 1. MCS-Chain system model.

Εικόνα 11 : MCS-chain μοντέλο συστήματος
Πηγή: (https://www.sciencedirect.com/science/article/abs/pii/S0167739X18326967) **[26]**

Κάθε κόμβος περιέχει έναν αριθμό βασικών λειτουργικών ενοτήτων όπως βλέπουμε στην Εικόνα 12. Μια εφαρμογή MCS-Chain αναπτύσσεται για να εκτελέσει τις βασικές λειτουργίες του MCS, π.χ. αίτημα εργασίας, προσφορά εργασίας, ανάθεση εργασίας, πληρωμή και πληροφόρηση για την απόδοση. Το Blockchain UI απεικονίζει τα περιεχόμενα του MCS-Chain blockchain. Το Blockchain Manager είναι υπεύθυνο για την εκτέλεση των εργασιών που θα

έπρεπε να γίνουν από έναν miner όπως παραγωγή και επαλήθευση μπλοκ, μια παραγωγή προσωπικού ζεύγους κλειδιών για κόμβους, κατακερματισμό δεδομένων, έλεγχο ακεραιότητας δεδομένων, και επαλήθευση υπογραφών. Ο Task manager εφαρμόζεται για την εκπλήρωση εργασιών που έχουν εκχωρηθεί και συμφωνηθεί. Όλες οι πληροφορίες που σχετίζονται με τις βασικές λειτουργίες που αναφέρθηκαν αποθηκεύονται στο Trusted Local Database. Σημειώστε, όμως, ότι τα τοπικά διαπιστευτήρια μπορούν να αποθηκευτούν σε ένα πιο ασφαλές μέρος από το Trusted Local Database [26].



Εικόνα 12 : Δομή κόμβων στο MCS
Πηγή: (https://www.sciencedirect.com/science/article/abs/pii/S0167739X18326967) **[26]**

Στο άρθρο ZebraLancer: Crowdsourced Knowledge atop Open Blockchain, Privately and Anonymously, οι συγγραφείς προτείνουν ένα σύστημα που συνδυάζει την τεχνολογία blockchain με τα συστήματα crowdsourcing. Πιο συγκεκριμένα, προτείνουν ένα πρωτόκολλο βασισμένο στο blockchain για την υλοποίηση της αποκεντρωμένης υπηρεσίας crowdsourcing που ικανοποιεί: α) τη δίκαιη συναλλαγή μεταξύ δεδομένων και ανταμοιβών, για παράδειγμα ένας εργάτης θα πληρωθεί το ανάλογο ποσό σύμφωνα με την προκαθορισμένη πολιτική της αξιολόγησης των δεδομένων, β) εμπιστευτικότητα δεδομένων, π.χ. τα δεδομένα που έχουν κατατεθεί να είναι άξια εμπιστοσύνης σε οποιονδήποτε εκτός του ατόμου που έκανε την αίτηση, γ) ανωνυμία και ευθύνη.

Η διαίσθηση πίσω από τη δικαιοσύνη και την εμπιστευτικότητα είναι μια μεθοδολογία ανάθεσης και αποδείξεως στην οποία: α) ο αιτών πρέπει να καταθέσει το ποσό που αναφέρει η πολιτική σε ένα έξυπνο συμβόλαιο, β) οι υποβολές κρυπτογραφούνται υπό το δημόσιο κλειδί

του αιτούντος και θα συλλεχθούν από το blockchain, γ) η αξιολόγηση των ανταμοιβών γίνεται εξωτερικά στο αιτούντα, ο οποίος έπειτα πρέπει να στείλει οδηγίες σχετικά με το πως θα ανταμειφθούν οι εργάτες. Οι οδηγίες πρέπει να ακολουθούν την απαραίτητη πολιτική, επειδή ο αιτών είναι υποχρεωμένος να επισυνάψει μια έγκυρη zero-knowledge proof.

Η ανωνυμία των εργατών του πρωτοκόλλου των συγγραφέων μπορεί να εξασφαλίσει: α) το κοινό, συμπεριλαμβανομένων του αιτούντος και της αρχής εγγραφής, δεν μπορεί να πει με σιγουριά ότι κάποια δεδομένα προέρχονται από ένα συγκεκριμένο εργάτη, β) εάν ένας εργάτης λάβει μέρος σε διαφορετικές εργασίες που έχουν ανακοινωθεί μέσω του blockchain, κανένας δεν μπορεί να συνδέσει αυτές τις εργασίες. Κυρίως, οι συγγραφείς ασχολούνται με το θέμα της απειλής της πολλαπλής υποβολής, το οποίο επιδεινώνεται από την κατάχρηση της ανωνυμίας. Πιο συγκεκριμένα, εάν ένας εργάτης καταθέτει ανώνυμα αριθμό μεγαλύτερο από όσο επιτρέπεται σε μια εργασία, το σχήμα των συγγραφέων επιτρέπει στο blockchain να ξεχωρίσει και να απορρίψει αυτές τις υποβολές.

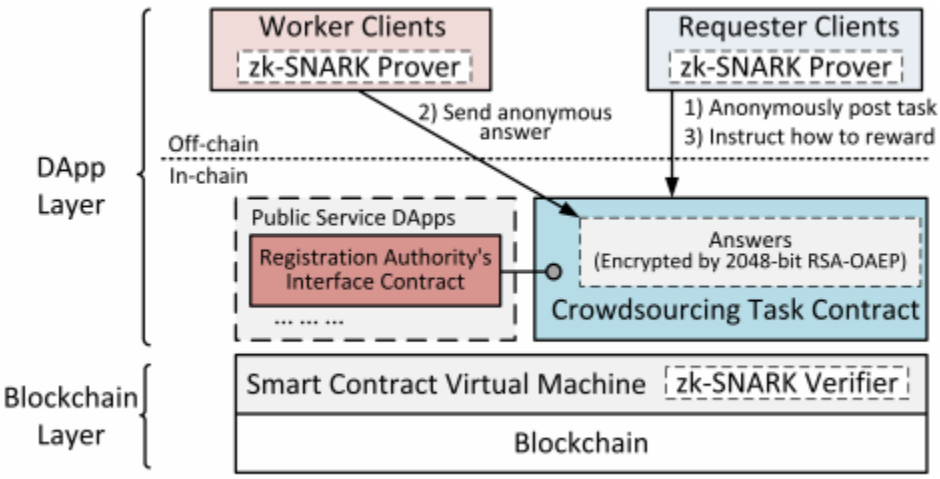
Για να επιτευχθεί ο παραπάνω στόχος της ανωνυμίας, διατηρώντας παράλληλα και την ανάληψη ευθυνών, οι συγγραφείς δημιουργούν ένα νέο κρυπτογραφικό σύστημα, που ονομάζεται common-prefix-linkable ανώνυμη επαλήθευση. Τις περισσότερες φορές ένας χρήστης μπορεί να επαληθεύσει τα μηνύματα και να πιστοποιήσει την εγκυρότητα της ταυτότητας χωρίς να συνδεθεί. Η μόνη εξαίρεση όπου κάποιος μπορεί να συνδέσει δύο επαληθευμένα μηνύματα είναι όταν μοιράζονται το ίδιο πρόθεμα και πιστοποιούνται από ένα χρήστη.

Για να χρησιμοποιήσουν το νέο σύστημα στο πρωτόκολλο τους, ένας εργάτης πρέπει να υποβάλλει μια εργασία μέσω ανώνυμης πιστοποίησης. Η αναφορά της εργασίας θα είναι μοναδική και θα πρέπει να είναι το κοινό πρόθεμα, έτσι ώστε η ειδική δυνατότητα σύνδεσης να εμποδίζει την πολλαπλή υποβολή σε μια εργασία. Ένας αιτών μπορεί επίσης να το χρησιμοποιήσει για να πιστοποιήσει κάθε εργασία που εκδίδει, και να πείσει τους εργάτες ότι δεν μπορεί να το υποβάλλει κακόβουλα για να υποβαθμίσει εσκεμμένα τις ανταμοιβές τους.

Για να παρουσιάσουν τη σκοπιμότητα της εφαρμογής του πρωτοκόλλου τους, εφαρμόζουν το σύστημα που ονομάζουν ZebraLancer για μια κοινή εργασία σχολιασμού εικόνας πάνω από το Ethereum, μια πραγματική υποδομή blockchain. Τα εντατικά πειράματα και οι αξιολογήσεις απόδοσης διεξάγονται σε δοκιμαστικό περιβάλλον του Ethereum. Δεδομένου ότι τα τρέχοντα έξυπνα συμβόλαια υποστηρίζουν μόνο πρωτόγονες λειτουργίες, η προσαρμογή τέτοιων πρωτοκόλλων που είναι συμβατά με υπάρχουσες πλατφόρμες blockchain διεξάγεται χωρίς τριβές.

Όπως βλέπουμε στην Εικόνα 13, η αποκεντρωμένη εφαρμογή (DApp) του συστήματος ZebraLancer αποτελείται από ένα μέρος πάνω στην αλυσίδα και ένα εκτός αλυσίδας. Το μέρος πάνω στην αλυσίδα αποτελείται από συμβόλαια εργασιών crowdsourcing και ένα συμβόλαιο της αρχής εγγραφής (RA). Το συμβόλαιο της RA πολύ απλά θέτει το κύριο δημόσιο κλειδί του

συστήματος ως κοινή γνώση που είναι αποθηκευμένη στο blockchain. Το μέρος εκτός αλυσίδας αποτελείται από πελάτες που κάνουν αιτήσεις και πελάτες που κάνουν τις εργασίες. Αυτοί οι πελάτες μπορεί να είναι πελάτες του blockchain και να πραγματοποιούν λειτουργίες που απαιτεί το σύστημα. Συγκεκριμένα, ένας πελάτης που κάνει αίτηση θα πρέπει να κωδικοποιήσει μια συγκεκριμένη εργασία με ένα δεδομένο μηχανισμό κινήτρων και να το ανακοινώσει σαν έξυπνο συμβόλαιο. Οι πελάτες χρειάζονται επίσης ένα ολοκληρωμένο zk-SNARK αποδεικτικό για την παραγωγή των ανώνυμων βεβαιώσεων πιστοποίησης. Επιπρόσθετα, ένας πελάτης που κάνει αίτηση θα πρέπει να χρησιμοποιήσει ένα SNARK αποδεικτικό για να παράγει αποδείξεις που θα επιβεβαιώνουν τη σωστή εκτέλεση των πολιτικών των κινήτρων.



Εικόνα 13 : Τα επίπεδα του ZebraLancer
Πηγή: (https://pdfs.semanticscholar.org/136d/3f269f44cf2fdc96efb5ea44e9675ff025af.pdf**) [27]**

Τέλος, οι συγγραφείς αναφέρουν ότι η απόδοση ασφαλείας του συστήματός τους είναι καλύτερη από αυτή άλλων συστημάτων, καθώς διαθέτει την πιο αυστηρή και δίκαιη πολιτική συναλλαγών, ανωνυμία χρηστών και εμπιστευτικότητα των δεδομένων, υπό την προϋπόθεση της ελάχιστης εμπιστοσύνης. Για παράδειγμα, το σύστημα αυτό αναγνωρίζει μια δίκαιη συναλλαγή χωρίς να διαρρέει δεδομένα σε κάποιον τρίτο κριτή πληροφοριών. Επίσης, το ZebraLancer εγγυάται την πιο ισχυρή ανωνυμία χρηστών, η οποία δεν μπορεί να σπάσει από κανένα τρίτο μέλος (ακόμα και από την αρχή εγγραφής), ενώ η ανωνυμία άλλων συστημάτων μπορεί να σπάσει από τρίτα μέλη [27].

Μια αρκετά ενδιαφέρουσα ιδέα για συνδυασμό τεχνολογίας blockchain με Mobile CrowdSensing παρουσιάζεται στο άρθρο WorkerRep: Building Trust on Crowdsourcing Platform Using Blockchain. Η συγγραφέας προτείνει μια πλατφόρμα Crowdsourcing, η οποία είναι αποκεντρωμένη και δε βασίζεται σε κάποιο τρίτο μέρος για τις βασικές της λειτουργίες, ενώ ταυτόχρονα είναι χτισμένη πάνω στο Ethereum. Επίσης, έχει το επιπρόσθετο πλεονέκτημα του μειωμένου κόστους, αφού όποιος δημοσιεύει εργασίες δεν απαιτείται να πληρώσει κανέναν

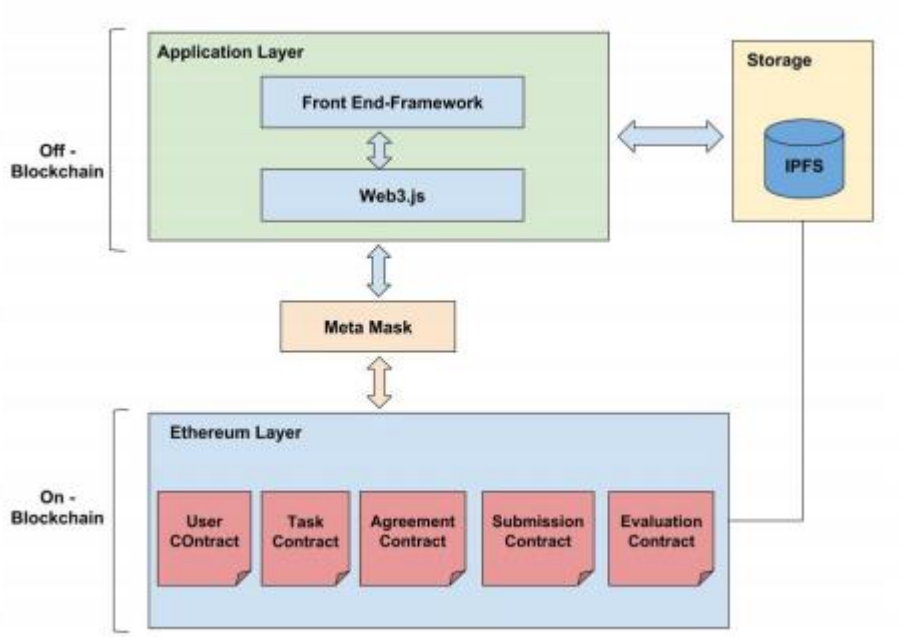
κεντρικό πράκτορα για να φέρει εις πέρας την εργασία του. Γίνεται προσπάθεια να αποτρέψουν διάφορες επιθέσεις στο σύστημα φήμης, δημιουργώντας μια ισχυρότερη μεθοδολογία αξιολόγησης υποβολής. Στη συνέχεια γίνεται αναφορά και περιγραφή των διαφόρων επιθέσεων και προβλημάτων από τα οποία κινδυνεύει το σύστημα:

- Reputation είναι η μονάδα μέτρησης του πόσο καλά έχει λειτουργήσει ένας εργάτης στις εργασίες που του έχουν ανατεθεί και πόσο καλά αξιολογεί τη δουλειά που κάνουν οι άλλοι.
- Initialization and Cold Start Problem ονομάζεται ένα πρόβλημα που αντιμετωπίζουν οι νέοι χρήστες στην πλατφόρμα, λόγω της χαμηλής βαθμολογίας φήμης που έχουν.
- Sybil attack είναι μια επίθεση όπου ένας κακόβουλος εργάτης προσπαθεί να δημιουργήσει πολλαπλές ταυτότητες μέσα στην πλατφόρμα για να αποκτήσει επιρροή μέσα στην πλατφόρμα. Γενικά, πραγματοποιείται για να γίνουν στη συνέχεια μερικές από τις παρακάτω επιθέσεις:
    - Re-entry attack πραγματοποιείται με τη δημιουργία μιας νέας ταυτότητας στην πλατφόρμα, αφήνοντας μια ταυτότητα με κακή φήμη. Γενικά, χαμηλότερη φήμη από αυτή που έχει ένας νέος εργάτης.
    - Collusion attack συμβαίνει όταν μια ομάδα εργατών προσπαθούν να συνωμοτήσουν για να αυξήσουν τη φήμη τους ή να μειώσουν τη φήμη άλλων.
    - Ballot Stuffing είναι όταν ένας εργάτης προσπαθεί να αυξήσει τη δική του φήμη.

- Unfair rating attack συμβαίνει όταν αυτός που θέτει τη βαθμολογία ευνοεί κάποιον εργάτη και δεν δίνει την πραγματική του άποψη για αυτόν.
- Reciprocity είναι όταν ένας εργάτης παλινδρομεί αρνητικά για μια αρνητική επισκόπηση που έλαβε.
- Whitewashing attack συμβαίνει όταν είτε ο εργάτης γνωρίζει πως να χειραγωγήσει το σύστημα φήμης, είτε με το να ξαναεισέλθει στο σύστημα.

Από τη στιγμή που το προτεινόμενο σύστημα είναι χτισμένο πάνω στο δίκτυο του Ethereum, τα έξυπνα συμβόλαια είναι τα πιο βασικά μπλοκ για αυτό. Το σύστημα αυτό έχει πέντε διαφορετικά είδη έξυπνων συμβολαίων: 1) UserContract: περιέχει λειτουργίες για να δημιουργηθούν νέοι χρήστες στην πλατφόρμα. 2) TaskContract: προσφέρει λειτουργίες για τη δημιουργία μιας νέας εργασίας, καθώς επιτρέπει στους χρήστες να δουν τις υπάρχουσες εργασίες στην πλατφόρμα. 3) AgreementContract: δημιουργεί μια συμφωνία μεταξύ του χρήστη που δημοσιοποιεί την εργασία και του εργάτη που ανταποκρίνεται στη συγκεκριμένη εργασία. 4) SubmissionContract: ο εργάτης επικαλείται τις λειτουργίες του συμβολαίου όταν έχει ολοκληρώσει την εργασία που του έχει ανατεθεί και είναι έτοιμος να την υποβάλει. Η βασική λειτουργία αυτού του συμβολαίου είναι να δεχθεί την υποβολή από τον εργάτη και τους

αξιολογητές για την υποβολή αυτή. 5) EvaluationContract: παρέχει διάφορες λειτουργίες στους αξιολογητές των εργασιών. Επίσης, υπολογίζει και ενημερώνει τη φήμη των εργατών με βάση πάντα τη βαθμολογία αξιολόγησης που έχουν λάβει από τους αξιολογητές. Η αρχιτεκτονική του συστήματος παρουσιάζεται στην Εικόνα 14.



Εικόνα 14 : Η αρχιτεκτονική του προτεινόμενου συστήματος
Πηγή:(https://www.researchgate.net/publication/327500576_WorkerRep_Building_Trust_on_Crowdsourcing_Platform_Using_Blockchain) [28]

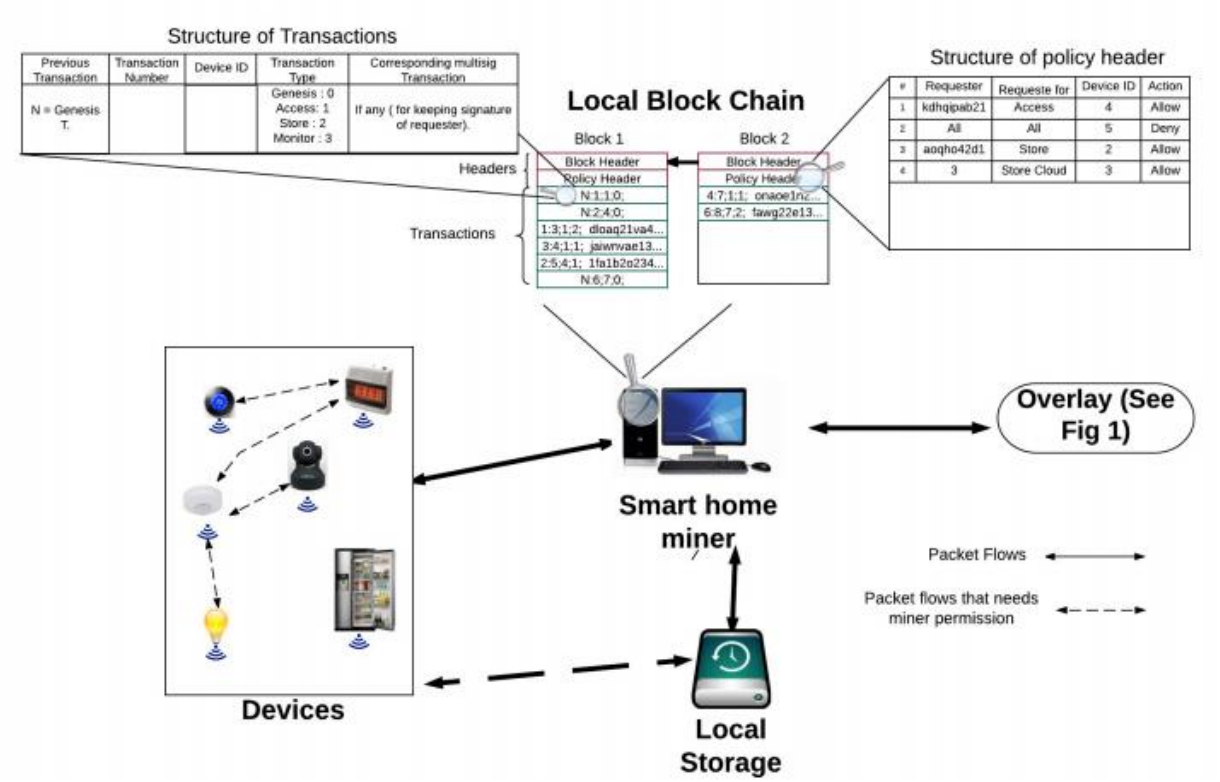
Για την υλοποίηση οποιασδήποτε λειτουργίας στην πλατφόρμα, ο χρήστης πρέπει να καλέσει τη συνάρτηση του συμβολαίου που ανταποκρίνεται στη συγκεκριμένη λειτουργία. Εάν η κλήση της συνάρτησης οδηγήσει σε αλλαγή κατάστασης του Ethereum Blockchain τότε η κλήση της συνάρτησης αντιμετωπίζεται σαν συναλλαγή. Οι συναλλαγές στο δίκτυο του Ethereum υπογράφονται κρυπτογραφικά με τη χρήση ενός αλγορίθμου ασύμμετρης κρυπτογράφησης για την αποφυγή της μη αποθάρρυνσης της προέλευσης της συναλλαγής καθώς και για τη διατήρηση της ακεραιότητας των δεδομένων. Οι miners, από την άλλη, μπορούν να αποκρυπτογραφήσουν τη συναλλαγή χρησιμοποιώντας το αρχικό δημόσιο κλειδί. Αφού την κρυπτογραφήσουν, επαληθεύουν την εγκυρότητα της συναλλαγής κάνοντας αναφορά στις συναλλαγές που έχουν σταλθεί και ληφθεί από τον αποστολέα. Εάν βρεθούν έγκυρες, αυτές οι συναλλαγές προστίθενται στο δημόσιο καθολικό. Οι συναλλαγές αυτές κοστίζουν Ethers στους χρήστες. Αλληλεπιδράσεις με το δίκτυο του Ethereum πραγματοποιούνται με τη χρήση του MetaMask. Το MetaMask είναι μια εφαρμογή που ενεργεί ως γέφυρα μεταξύ του προγράμματος περιήγησης και του Ethereum [28].

3.10.2 Χρήση του Blockchain στο IoT

Το θέμα της ασφάλειας και της ιδιωτικότητας διερευνούν οι συγγραφείς του άρθρου Blockchain for IoT Security and Privacy: The Case Study of a Smart Home. Όπως αναφέρουν, οι επικοινωνίες μεταξύ τοπικών συσκευών ή κόμβων είναι γνωστές ως συναλλαγές. Σε ένα έξυπνο σπίτι βασισμένο στο Blockchain υπάρχουν διαφορετικές συναλλαγές, από τις οποίες κάθε μια είναι σχεδιασμένη για μια συγκεκριμένη λειτουργία. Η συναλλαγή *Store* παράγεται από τις συσκευές για να αποθηκεύει δεδομένα. Μια συναλλαγή *access* παράγεται από τον ιδιοκτήτη του σπιτιού για να δώσει πρόσβαση στο αποθηκευτικό χώρο του υπολογιστικού νέφους. Η συναλλαγή *monitor* δημιουργείται κι αυτή από τον ιδιοκτήτη του σπιτιού για να παρακολουθεί περιοδικά τις πληροφορίες κάποιας συσκευής. Η προσθήκη μιας νέας συσκευής στο έξυπνο σπίτι πραγματοποιείται μέσω μιας συναλλαγής *genesis*, ενώ όταν πρέπει να αφαιρεθεί μια συσκευή αυτό γίνεται μέσω της συναλλαγής *remove*. Όλες οι προαναφερθείσες συναλλαγές χρησιμοποιούν ένα μοιρασμένο κλειδί για να ασφαλίσουν την επικοινωνία. Το σύνολο των συναλλαγών από και προς το έξυπνο σπίτι αποθηκεύονται σε ένα τοπικό ιδιωτικό blockchain.

Σε κάθε έξυπνο σπίτι, υπάρχει ένα τοπικό ιδιωτικό blockchain, το οποίο κρατάει αρχείο των συναλλαγών και έχει τη δική του πολιτική την οποία επιβάλλει στους χρήστες για εισερχόμενες και εξερχόμενες συναλλαγές. Ξεκινώντας με τη συναλλαγή genesis, οι συναλλαγές κάθε συσκευής συνδέονται μαζί σαν ένα αμετάβλητο καθολικό μέσα στο blockchain. Κάθε μπλοκ στο τοπικό blockchain περιέχει δυο επικεφαλίδες, μια επικεφαλίδα μπλοκ και μια επικεφαλίδα πολιτικής, όπως φαίνεται στην κορυφή της παρακάτω εικόνας. Η επικεφαλίδα μπλοκ έχει το hash του προηγούμενου μπλοκ για να διατηρήσει το blockchain αμετάβλητο. Η επικεφαλίδα πολιτικής χρησιμοποιείται για την αδειοδότηση συσκευών και την επιβολή της πολιτικής ελέγχου του ιδιοκτήτη όσον αφορά το σπίτι του.

Εκτός από τις επικεφαλίδες, το κάθε μπλοκ περιέχει έναν αριθμό από συναλλαγές. Για κάθε συναλλαγή αποθηκεύονται στο τοπικό blockchain πέντε παράμετροι, όπως φαίνεται στην πάνω αριστερά γωνία της εικόνας. Οι πρώτες δυο παράμετροι χρησιμοποιούνται για να συνδέσουν συναλλαγές της ίδια συσκευής μεταξύ τους και να αναγνωρίσουν κάθε συναλλαγή ξεχωριστά στο blockchain. Το ID της αντίστοιχης συσκευής της συναλλαγής εισέρχεται στο τρίτο πεδίο. Ο όρος “Transaction type” αναφέρεται στον τύπο της συναλλαγής, ο οποίος μπορεί να είναι genesis, access, store ή monitor. Η συναλλαγή αποθηκεύεται στο πέμπτο πεδίο αν προέρχεται από το δίκτυο επικάλυψης, αλλιώς αυτό το πεδίο παραμένει κενό. Το τοπικό blockchain διατηρείται και διαχειρίζεται από έναν τοπικό miner.



Εικόνα 15: Σφαιρική εικόνα του έξυπνου σπιτιού: το έξυπνο σπίτι αποτελείται από συσκευές IoT, τοπικό αποθηκευτικό χώρο, τον miner και το τοπικό blockchain

Πηγή: (https://ieeexplore.ieee.org/abstract/document/7917634) [29]

Ο miner του έξυπνου σπιτιού είναι μια συσκευή, η οποία επεξεργάζεται κεντρικά εισερχόμενες και εξερχόμενες συναλλαγές από και προς το έξυπνο σπίτι. Ο miner μπορεί να ενσωματωθεί στην πύλη του διαδικτύου του σπιτιού ή σε μια ξεχωριστή αυτόνομη συσκευή. Παρόμοια με υπάρχουσες συσκευές κεντρικής ασφάλειας, ο miner πιστοποιεί, εξουσιοδοτεί και ελέγχει τις συναλλαγές. Επιπρόσθετα, ο miner επιτυγχάνει τις ακόλουθες λειτουργίες: παράγει συναλλαγές genesis, διανέμει και ενημερώνει κλειδιά, αλλάζει τη δομή των συναλλαγών και διαμορφώνει και διαχειρίζεται το σύμπλεγμα. Ο miner συλλέγει όλες τις συναλλαγές σε ένα μπλοκ και επισυνάπτει ολόκληρο το μπλοκ στο blockchain. Για να παρέχει επιπλέον χωρητικότητα, ο miner διαχειρίζεται ένα τοπικό αποθηκευτικό χώρο.

Ο τοπικός αποθηκευτικός χώρος είναι μια αποθηκευτική συσκευή, η οποία χρησιμοποιείται από συσκευές για να αποθηκεύσουν δεδομένα τοπικά. Αυτός ο χώρος μπορεί να είναι ενσωματωμένος στον miner ή μπορεί και να είναι ξεχωριστή συσκευή. Χρησιμοποιεί μέθοδο First-in-First-out (FiFo) για να αποθηκεύσει δεδομένα και αποθηκεύει τα δεδομένα κάθε συσκευής σαν ένα καθολικό συνδεδεμένο στο σημείο εκκίνησης της συσκευής.

Στη συνέχεια γίνεται περιγραφή της διαδικασίας προσθήκης συσκευών και της επικεφαλίδας πολιτικής στο τοπικό blockchain. Για να γίνει προσθήκη μιας συσκευής στο έξυπνο σπίτι, ο miner παράγει μια συναλλαγή genesis, μοιράζοντας ένα κλειδί στη συσκευή. Το κλειδί αποθηκεύεται στη συναλλαγή genesis. Όσον αφορά την επικεφαλίδα πολιτικής, ο ιδιοκτήτης του σπιτιού δημιουργεί τις δικές του πολιτικές και προσθέτει την επικεφαλίδα πολιτικής στο πρώτο μπλοκ. Ο miner χρησιμοποιεί την επικεφαλίδα πολιτικής στο τελευταίο μπλοκ του blockchain. Επομένως, προκειμένου ο ιδιοκτήτης να ανανεώσει την πολιτική, θα πρέπει να ανανεώσει την επικεφαλίδα του τελευταίου μπλοκ.

Οι έξυπνες συσκευές μπορούν να επικοινωνήσουν απευθείας η μία με την άλλη ή με οντότητες έξω από το σπίτι. Κάθε συσκευή μέσα στο σπίτι μπορεί να ζητήσει δεδομένα από μια άλλη εσωτερική (δηλ. μέσα από το σπίτι) συσκευή για να προσφέρει ορισμένες υπηρεσίες. Για να επιτευχθεί έλεγχος για το χρήστη στις συναλλαγές μέσα στο έξυπνο σπίτι, ένα κοινό κλειδί θα πρέπει να διανέμεται από τον miner στις συσκευές που πρέπει να επικοινωνούν απευθείας η μια με την άλλη. Για τη διανομή του κλειδιού, ο miner ελέγχει την επικεφαλίδα πολιτικής ή ζητάει την άδεια του ιδιοκτήτη και έπειτα διανέμει ένα κοινό κλειδί μεταξύ των συσκευών. Αφού παραλάβουν το κλειδί, οι συσκευές επικοινωνούν απευθείας όσο το κλειδί παραμένει έγκυρο. Για να αρνηθεί την πρόσβαση, ο miner μαρκάρει το κοινό κλειδί σαν μη έγκυρο στέλνοντας ένα μήνυμα ελέγχου στις συσκευές. Τα βασικά οφέλη αυτής της μεθόδου είναι δυο: πρώτον, ο miner (και κατ' επέκταση ο ιδιοκτήτης) έχει μια λίστα με συσκευές που μοιράζονται δεδομένα, και δεύτερον, οι επικοινωνίες μεταξύ των συσκευών είναι ασφαλείς από τη στιγμή που διαθέτουν ένα κοινό κλειδί.

Η αποθήκευση δεδομένων στον τοπικό αποθηκευτικό χώρο από τις συσκευές είναι η άλλη πιθανή ροή των συναλλαγών μέσα στο σπίτι. Για να αποθηκεύσει δεδομένα τοπικά, κάθε συσκευή πρέπει να επαληθευτεί στον αποθηκευτικό χώρο με τη χρήση ενός κοινού κλειδιού. Για να αποκτήσει το κλειδί, η συσκευή πρέπει να στείλει αίτημα στον miner και αν αποκτήσει άδεια για αποθήκευση, ο miner παράγει ένα κοινό κλειδί και στέλνει το κλειδί για τη συσκευή και τον αποθηκευτικό χώρο. Λαμβάνοντας το κλειδί, ο τοπικός αποθηκευτικός χώρος δημιουργεί ένα σημείο εκκίνησης το οποίο περιέχει το κοινό κλειδί. Έχοντας το κοινό κλειδί, η συσκευή μπορεί να αποθηκεύσει δεδομένα απευθείας στον τοπικό αποθηκευτικό χώρο.

Οι συσκευές μπορεί να απαιτούν την αποθήκευση δεδομένων στον αποθηκευτικό χώρο του υπολογιστικού νέφους, κάτι το οποίο είναι γνωστό σαν συναλλαγή *store*. Η αποθήκευση δεδομένων στο υπολογιστικό νέφος είναι μια ανώνυμη διαδικασία. Για να αποθηκεύσει δεδομένα ο αιτών χρειάζεται ένα σημείο εκκίνησης που θα περιέχει έναν αριθμό των μπλοκ και ένα hash που θα χρησιμοποιηθεί για ανώνυμη επαλήθευση. Ο αποθηκευτικός χώρος του υπολογιστικού νέφους μπορεί είτε να ανήκει και να γίνεται η διαχείρισή του από τους παρόχους ασφαλείας, είτε να ανήκει και να δέχεται διαχείριση από τον ιδιοκτήτη του σπιτιού. Στην πρώτη περίπτωση, ο miner κάνει αίτηση για το σημείο εκκίνησης δημιουργώντας μια υπογεγραμμένη συναλλαγή με το κλειδί της συσκευής. Στη δεύτερη περίπτωση, η πληρωμή γίνεται μέσω

Bitcoin. Σε όλους τους τύπους αποθήκευσης, ο αποθηκευτικός χώρος αφού λάβει το αίτημα δημιουργεί ένα σημείο εκκίνησης και το στέλνει στον miner. Όταν μια συσκευή χρειάζεται να αποθηκεύσει δεδομένα στον αποθηκευτικό χώρο του υπολογιστικού νέφους, στέλνει τα δεδομένα και το αίτημα στον miner. Λαμβάνοντας το αίτημα, ο miner αδειοδοτεί τη συσκευή για να αποθηκεύσει δεδομένα στο υπολογιστικό νέφος. Αν η συσκευή έχει αδειοδοτηθεί, ο miner παίρνει τον τελευταίο αριθμό μπλοκ και το hash από το τοπικό blockchain, δημιουργεί μια συναλλαγή store και τη στέλνει μαζί με τα δεδομένα στο χώρο αποθήκευσης. Αφού τα δεδομένα αποθηκευτούν, το υπολογιστικό νέφος επιστρέφει στον miner το νέα αριθμό μπλοκ, ο οποίος χρησιμοποιείται για επιπλέον συναλλαγές αποθήκευσης.

Οι άλλες πιθανές συναλλαγές είναι οι συναλλαγές access και monitor. Αυτές οι συναλλαγές κυρίως παράγονται είτε από τον ιδιοκτήτη του σπιτιού για την παρακολούθηση του σπιτιού όταν ο ίδιος απουσιάζει, είτε από τους παρόχους ασφαλείας για την επεξεργασία των δεδομένων από τις συσκευές για προσωποποιημένες υπηρεσίες. Με τη λήψη μιας συναλλαγής access από τους κόμβους, ο miner ελέγχει αν τα δεδομένα που έχουν ζητήσει, βρίσκονται στον τοπικό χώρο αποθήκευσης ή στο υπολογιστικό νέφος. Αν τα δεδομένα είναι αποθηκευμένα στον τοπικό χώρο αποθήκευσης, τότε ο miner ζητάει τα δεδομένα από τον τοπικό χώρο αποθήκευσης και τα στέλνει σε όποιον τα ζήτησε. Αν τα δεδομένα είναι αποθηκευμένα στο υπολογιστικό νέφος, ο miner είτε ζητάει τα δεδομένα από το υπολογιστικό νέφος και τα στέλνει σε αυτόν που τα ζήτησε, είτε στέλνει τον τελευταίο αριθμό μπλοκ και το hash. Το τελευταίο σενάριο ωθεί τον αιτούντα να διαβάσει όλα τα δεδομένα που έχουν αποθηκευτεί από τη συσκευή στο υπολογιστικό νέφος και είναι ιδανικό όταν τα αποθηκευμένα δεδομένα είναι για μια μοναδική συσκευή. Ειδάλλως, η ιδιωτικότητα του χρήστη μπορεί να βρίσκεται σε κίνδυνο μέσω διαφόρων επιθέσεων που υπάρχουν.

Με τη λήψη μιας συναλλαγής monitor, ο miner στέλνει τα τωρινά δεδομένα της συσκευής στον αιτούντα. Αν ο αιτών έχει την άδεια να λαμβάνει δεδομένα για ορισμένη χρονική περίοδο τότε ο miner στέλνει τα δεδομένα περιοδικά μέχρι ο αιτών να στείλει ένα αίτημα λήξης στον miner και να καταργήσει τη συναλλαγή. Η συναλλαγή monitor επιτρέπει στους ιδιοκτήτες των σπιτιών να παρακολουθούν τις κάμερες που έχουν τοποθετήσει στο σπίτι τους ή άλλες συσκευές στις οποίες στέλνουν δεδομένα περιοδικά. Προκειμένου να αποφευχθούν πιθανές επιθέσεις, ο ιδιοκτήτης θα πρέπει να ορίσει ένα όριο στα λεπτά των περιοδικών δεδομένων. Αν η ώρα κατά την οποία ο miner στέλνει δεδομένα για τον αιτούντα φτάσει στο όριο, τότε η σύνδεση τερματίζεται από τον miner.

Όταν ένα άτομο έχει παραπάνω από ένα σπίτι, χρειάζεται διαφορετικούς miners και διαφορετικό αποθηκευτικό χώρο για κάθε ξεχωριστό σπίτι. Για να μειωθεί το κόστος και τα γενικά έξοδα σε αυτή την περίπτωση, ορίζεται ένα κοινόχρηστο δίκτυο επικάλυψης. Το κοινόχρηστο δίκτυο επικάλυψης αποτελείται από τουλάχιστον δυο έξυπνα σπίτια, τα οποία διαχειρίζονται κεντρικά σαν ένα σπίτι από τον κοινόχρηστο miner. Στο κοινόχρηστο blockchain κάθε σπίτι έχει μια συναλλαγή genesis και οι συναλλαγές genesis όλων των συσκευών

συνδέονται στη συναλλαγή genesis του σπιτιού από τον κοινόχρηστο miner του δικτύου επικάλυψης. Μια ακόμα διαφορά στο κοινόχρηστο δίκτυο επικάλυψης αφορά τις επικοινωνίες μεταξύ των σπιτιών με τον miner. Οι συσκευές οι οποίες είναι στο ίδιο σπίτι με τον miner δεν παρουσιάζουν κάποια αλλαγή, ενώ για τις συσκευές στα άλλα σπίτια καθορίζεται μια σύνδεση Virtual Private Network (VPN) μεταξύ της πύλης του διαδικτύου στο κάθε σπίτι και στον miner του κοινόχρηστου δικτύου επικάλυψης, ο οποίος οδηγεί τα πακέτα στον κοινόχρηστο miner.

Υπάρχουν τρεις απαραίτητες προϋποθέσεις ασφαλείας, με τις οποίες πρέπει να ασχολείται οποιοδήποτε σχέδιο ασφαλείας. Αυτές είναι: Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα. Η εμπιστευτικότητα διασφαλίζει ότι μόνο ο αδειοδοτημένος χρήστης έχει τη δυνατότητα να διαβάζει το μήνυμα. Η ακεραιότητα διασφαλίζει ότι το σταλμένο μήνυμα παραδίδεται στον προορισμό χωρίς καμία αλλαγή, και η διαθεσιμότητα σημαίνει ότι κάθε υπηρεσία ή κάθε δεδομένο είναι διαθέσιμα στο χρήστη οποιαδήποτε στιγμή τα χρειαστεί. Για να αυξηθεί η διαθεσιμότητα σε ένα έξυπνο σπίτι, οι συσκευές προστατεύονται από κακόβουλους αιτούντες. Αυτό επιτυγχάνεται με τη μείωση των αποδεχόμενων συναλλαγών στις οντότητες με τις οποίες η κάθε συσκευή έχει θέσει ένα κοινόχρηστο κλειδί. Οι συναλλαγές που λαμβάνονται από το δίκτυο επικάλυψης παίρνουν άδεια από τον miner πριν τις προωθήσει στις συσκευές.

Στη συνέχεια γίνεται ανάλυση της αποτελεσματικότητας της λύσης που προτείνουν οι συγγραφείς του άρθρου για την αποτροπή δυο πολύ σημαντικών επιθέσεων ασφαλείας, οι οποίες σχετίζονται σε μεγάλο βαθμό με τα έξυπνα σπίτια. Η πρώτη είναι η επίθεση Distributed Denial of Service (DDoS), κατά την οποία το άτομο που επιτίθεται χρησιμοποιεί κάποιες μολυσμένες συσκευές IoT για να καταλάβει ένα συγκεκριμένο κόμβο. Αρκετές πρόσφατες επιθέσεις έχουν αναδυθεί, οι οποίες έχουν εκμεταλλευτεί συσκευές IoT για την εκκίνηση τεράστιων επιθέσεων DDoS. Η δεύτερη είναι η επίθεση linking, κατά την οποία το άτομο που επιτίθεται καθορίζει μια σύνδεση μεταξύ πολλαπλών συναλλαγών με το ίδιο ιδιωτικό κλειδί με σκοπό να βρει την ID ενός ανώνυμου χρήστη. Αυτή η επίθεση, όπως γίνεται κατανοητό, θέτει σε ιδιαίτερο κίνδυνο την ιδιωτικότητα του χρήστη.

Ας περάσουμε πιο αναλυτικά στην επίθεση DDoS. Το σχέδιο των συγγραφέων έχει ιεραρχική άμυνα για να αντιμετωπίσει αυτή την επίθεση. Το πρώτο επίπεδο άμυνας μπορεί να καταλογιστεί στο γεγονός ότι θα ήταν απίθανο, για ένα άτομο που θέλει να επιτεθεί, να εγκαταστήσει απευθείας κακόβουλο λογισμικό στις συσκευές του έξυπνου σπιτιού από τη στιγμή που αυτές οι συσκευές δεν είναι απευθείας προσβάσιμες. Όλες οι συναλλαγές πρέπει να ελεγχθούν από τον miner. Ας υποθέσουμε όμως ότι ο επιτιθέμενος καταφέρνει με κάποιο τρόπο να μολύνει τις συσκευές. Το δεύτερο επίπεδο άμυνας προκύπτει από το γεγονός ότι όλες οι εξερχόμενες κινήσεις πρέπει να λάβουν άδεια από τον miner, εξετάζοντας την επικεφαλίδα πολιτικής τους. Από τη στιγμή που τα αιτήματα τα οποία απαρτίζουν την κίνηση της επίθεσης DDoS δε θα έχουν λάβει αδειοδότηση, δε θα τους επιτρεπόταν η έξοδος από το σπίτι. Τα επόμενα δυο επίπεδα άμυνας είναι ειδικά σχεδιασμένα και διαχειρίζονται από το στόχο της επίθεσης DDoS, ο οποίος μπορεί να είναι οποιοσδήποτε χρήστης στο δίκτυο επικάλυψης.

Όσον αφορά την προστασία από την επίθεση linking, τα δεδομένα κάθε συσκευής μοιράζονται και αποθηκεύονται από ένα μοναδικό κλειδί. Ο miner δημιουργεί μοναδικό καθολικό δεδομένων στο υπολογιστικό νέφος για κάθε συσκευή χρησιμοποιώντας διαφορετικό ιδιωτικό κλειδί. Επομένως, ο miner θα πρέπει να χρησιμοποιεί μοναδικό κλειδί για κάθε διαφορετική συναλλαγή.

Η ασφάλεια του IoT έχει κερδίσει αρκετή προσοχή τον τελευταίο καιρό, τόσο ακαδημαϊκά όσο και βιομηχανικά. Οι ήδη υπάρχουσες λύσεις δεν είναι ακριβώς ιδανικές για το IoT, κυρίως εξαιτίας της υψηλής κατανάλωσης ενέργειας. Οι συγγραφείς πρότειναν μια μέθοδο, η οποία αντιμετωπίζει αυτά τα προβλήματα εκμεταλλευόμενη το blockchain, το οποίο αποτελεί ένα αμετάβλητο καθολικό από μπλοκ. Η ιδέα περιλάμβανε τη χρήση ενός έξυπνου σπιτιού σαν αντιπροσωπευτική περίπτωση. Επέλεξαν να επισημάνουν τα διάφορα σημαντικά συστατικά του έξυπνου σπιτιού και αναφέρθηκαν στις διάφορες συναλλαγές και διαδικασίες που σχετίζονται με αυτό. Έπειτα από αναλύσεις κατέληξαν στο ότι το προτεινόμενο σχέδιο αξίζει να αναπτυχθεί περαιτέρω, εξαιτίας των πλεονεκτημάτων που προσφέρει στους χρήστες, παρόλο τις μικρές συμφορήσεις που μπορεί να δημιουργηθούν ανά διαστήματα. Τέλος, αναφέρουν ότι αυτή η έρευνα ήταν η πρώτη που στοχεύει στη διαμόρφωση του blockchain για να προσφέρει βοήθεια στον τομέα των έξυπνων σπιτιών [29].

Ιδιαίτερο ενδιαφέρον παρουσιάζει το σχέδιο που προτείνουν οι συγγραφείς του άρθρου Blockchain-Driven IoT for Food Traceability With an Integrated Consensus Mechanism. Παρουσιάζουν ένα BIFTS (Blockchain-IoT-based Food Traceability System) για το σχεδιασμό ενός ευπροσάρμοστου συστήματος blockchain-IoT για παρακολούθηση και διαχείριση δεδομένων για ικανότητα ιχνηλάτησης τροφίμων και για την επεξεργασία της διάρκειας ζωής των τροφίμων στα ράφια καθώς και της πτώσης της ποιότητας κάτω από ορισμένες συνθήκες. Αρχικά, εφαρμόζονται τεχνολογίες IoT για την ανάπτυξη μιας εφαρμογής παρακολούθησης του περιβάλλοντος με πολλαπλά TRUs (traceable resource units) για διασπορά προς τα πάνω, κάτω και κατά παρτίδες στην αλυσίδα εφοδιασμού. Στη συνέχεια, τα δεδομένα που συλλέγονται αποθηκεύονται σε μια βάση δεδομένων υπολογιστικού νέφους, ενώ η διαχείριση των κλειδιών σύνδεσης και των κύκλων ζωής των τροφίμων χρησιμοποιεί τεχνολογία blockchain. Τελικά, με αξιόπιστα και ασφαλή δεδομένα, μπορεί να επεξεργαστεί η διάρκεια ζωής των τροφίμων στα ράφια και να πραγματοποιείται συστηματική αξιολόγηση της ποιοτικής φθοράς των τροφίμων.

Σε γενικές γραμμές, η ανάπτυξη τεχνολογιών IoT αποτελείται από τρία βασικά στοιχεία: το επίπεδο των συσκευών, το επίπεδο σύνδεσης και το επίπεδο εφαρμογής, από τη συλλογή δεδομένων για τη διαχείριση εφαρμογών σε καθορισμένες πλατφόρμες ανάπτυξης IoT. Αυτό στοχεύει στην αναγνώριση του φαγητού και στην παρακολούθηση του περιβάλλοντος, παράλληλα με ταξίδια αποστολών και δραστηριότητες της αλυσίδας εφοδιασμού. Τα δεδομένα που έχουν συλλεχθεί χρησιμοποιούνται για την αξιολόγηση της διάρκειας ζωής των φαγητών και την πτώση της ποιότητας.

Στο επίπεδο των συσκευών, αισθητήρες περιβάλλοντος και κόμβοι μεταφοράς εγκαθίστανται για τη συλλογή δεδομένων των περιβαλλοντικών συνθηκών, ενώ γίνεται επίσης καταγραφή της χρονικής σήμανσης της συλλογής. Στο επίπεδο της σύνδεσης, η μετάδοση των δεδομένων μεταξύ των αισθητήρων και των κόμβων μεταφοράς πραγματοποιείται με τη χρήση τεχνολογιών ασύρματης επικοινωνίας (όπως Bluetooth και Wi-Fi), ενώ η μετάδοση των δεδομένων μεταξύ των κόμβων μεταφοράς και καθορισμένων πλατφόρμων IoT επιτυγχάνεται με τεχνολογίες επικοινωνίας machine-to-machine (M2M).

Στο επίπεδο της εφαρμογής, πλατφόρμες ανάπτυξης του IoT, όπως το IBM Cloud, εφαρμόζονται για να αναπτύξουν και να διαχειριστούν τις εφαρμογές, καθώς τα εξωτερικά συστήματα και οι βάσεις δεδομένων μπορούν να συνδεθούν με τη χρήση APIs. Επιπρόσθετα, τα δεδομένα που έχουν συλλεχθεί μπορούν να δομηθούν και να αποθηκευτούν σε μια κεντρική βάση δεδομένων υπολογιστικού νέφους για επιπλέον απάντηση διαφόρων ερωτημάτων. Ένας καθορισμένος αριθμός αισθητήρων και κόμβων μεταφοράς εφαρμόζονται στο επίπεδο κοντέινερ. Αυτό διευκολύνει την επίτευξη ισορροπίας μεταξύ του κόστους ανάπτυξης και την αποτελεσματικότητα της περιβαλλοντικής παρακολούθησης. Τα προϊόντα φαγητού στο επίπεδο κοντέινερ μεταφέρονται τυπικά μεταξύ των προμηθευτών, των κέντρων που αναλαμβάνουν τα φαγητά μετά τη συγκομιδή και των κέντρων επεξεργασίας φαγητών, με τη χρήση ενεργής συσκευασίας ψυχρής αλυσίδας μέσω διεθνών μεταφορών εμπορευμάτων.

Για το επίπεδο της παρτίδας, ένας αισθητήρας επισυνάπτεται για παλετοποίηση των προϊόντων, για παρακολούθηση κάθε παρτίδας τροφίμων. Έπειτα, η παλέτα με τα προϊόντα συνήθως μεταφέρεται με μεταφορές στο δρόμο μεταξύ των κέντρων επεξεργασίας και διανομής. Αυτό προσφέρει τα οφέλη της ευελιξίας και της οικονομικής αποδοτικότητας για χειρισμό των ειδών διατροφής σε επίπεδα παρτίδας. Τελικά, τα είδη διατροφής μπορούν είτε να πωληθούν σε κάποιο σούπερ μάρκετ, είτε να παραδοθούν σε εστιατόρια και να τα χειριστούν με τη χρήση παθητικής συσκευασίας κρύας αλυσίδας. Η εξωτερική συσκευασία των ειδών διατροφής παρέχει κωδικούς γρήγορης ανταπόκρισης (QR codes), οι οποίοι περιέχουν πληροφορίες τροφίμων, όπως όνομα, λίστα των συστατικών και πηγή προέλευσης. Επιπρόσθετα, οι πληροφορίες σχετικές με την ποιότητα του φαγητού και η περιβαλλοντική παρακολούθηση σχετίζονται με τους κωδικούς QR στις εφαρμογές που βασίζονται στο υπολογιστικό νέφος.

Κατά την επίτευξη ισορροπίας μεταξύ αξιόπιστης διαχείρισης δεδομένων και απόκτησης δεδομένων σε πραγματικό χρόνο, η τυπική ανάπτυξη blockchain δεν μπορεί να καλύψει τις απαιτήσεις των συστημάτων ιχνηλάτησης των τροφίμων. Παρόλο που η τεχνολογία blockchain έχει τα πλεονεκτήματα του αποκεντρωμένου ελέγχου, της διαφάνειας των δεδομένων, τη δυνατότητα συνεχούς ελέγχου, κατανεμημένων πληροφοριών, αποκεντρωμένης συναίνεσης και υψηλής ασφάλειας, η ανάπτυξη του blockchain χωρίς τις κατάλληλες ρυθμίσεις μπορεί να προκαλέσει διαφορετικά αρνητικά αποτελέσματα στην ιχνηλάτηση των τροφίμων. Από τη μια πλευρά, η απεριόριστη χρήση του blockchain για δραστηριότητες της αλυσίδας εφοδιασμού τροφίμων είναι αναποτελεσματικό για την ιχνηλάτηση των τροφίμων, κάτι το οποίο

καταναλώνει μεγάλο μέρος της μνήμης του συστήματος. Γι’ αυτό θα πρέπει να αναπτυχθεί στις περισσότερες βιομηχανικές εφαρμογές ένα συγκεκριμένο τελικό σημείο του blockchain. Επομένως, οι συγγραφείς προτείνουν μια υβριδική προσέγγιση στην ανάπτυξη του blockchain και του υπολογιστικού νέφους για πιο ελαφριά χαρακτηριστικά.

Μετά την εισαγωγή του BIFTS, οι τεχνολογίες blockchain-IoT είναι ευεργετικές για την ιχνηλάτηση του φαγητού και για τη διαμόρφωση των επιχειρήσεων που έχουν σχέση με τον τομέα των τροφίμων. Για την επίτευξη της ιχνηλάτησης των τροφίμων μέσω blockchain-IoT, προτιμήθηκαν τα χαρακτηριστικά του ελαφριού blockchain, ενώ τα συλλεγμένα δεδομένα εφαρμόζονται για να υποστηρίξουν τη διαδικασία πραγματοποίησης αποφάσεων στη διάρκεια ζωής των τροφίμων καθώς και στις αξιολογήσεις της φθοράς της ποιότητας. Με τη χρήση των πλεονεκτημάτων της τεχνολογίας blockchain, το προτεινόμενο σύστημα παρέχει αναβαθμίσεις στο μηχανισμό αμοιβαίας συναίνεσης, στην αξιοπιστία του συστήματος και στην αποτελεσματικότητα στον τομέα της ιχνηλάτησης, τα οποία είναι απαραίτητα για τη δημιουργία μιας θετικής ατμόσφαιρας σε αναλώσιμες επιχειρήσεις ηλεκτρονικού εμπορίου τροφίμων. Επομένως, τα πλεονεκτήματα της εγκατάστασης τους προτεινόμενου προγράμματος είναι τα εξής: α) ασφαλής και έμπιστη ιχνηλάτηση των τροφίμων στο κατανεμημένο δίκτυο της αλυσίδας εφοδιασμού, β) σχέδιο ελαφριού blockchain για τη μείωση του υπολογιστικού φόρτου και των δυνατοτήτων του εξοπλισμού, γ) ευφυή αξιολόγηση της ποιότητας των τροφίμων όσον αφορά τη διάρκεια ζωής και τη φθορά της ποιότητας με το πέρασμα του χρόνου [30].

Πίνακας σύγκρισης εφαρμογών που μελετήθηκαν

Άρθρα				
[22]	Χρησιμοποιεί το Ethereum	Χρήση έξυπνων συμβολαίων	Παρέχει ασφάλεια και αποτελεσματικότητα	Παρέχει κίνητρα-ανταμοιβές
[23]	Χρησιμοποιεί το Ethereum	Τρία είδη έξυπνων συμβολαίων	Εγγυάται Ασφάλεια-Ιδιωτικότητα	Παρέχει κίνητρα-ανταμοιβές
[24]	Χρησιμοποιεί p2p δίκτυο	Προσφέρει ασφαλείς συναλλαγές	Παροχή προστασίας τύπου k-anonymity	Προτείνει ασφαλή μηχανισμό κινήτρων
[25]	Δίκτυο χωρισμένο σε τρία μέρη	Διαθέτει σύστημα ανταλλαγής εικονικών κερμάτων για μετρητά	Διαθέτει μηχανισμό πρόκλησης αταξίας	Παρέχει εικονικά κέρματα σαν ανταμοιβές
[26]	Δίκτυο ειδικό για τη συγκεκριμένη περίπτωση	Διαθέτει τρία είδη εργατών, καθένα για διαφορετική εργασία	Προτείνει μηχανισμό αξιολόγησης εμπιστοσύνης	Παρέχει ανταμοιβές και τέλος υπηρεσιών στους Miners
[27]	Χρήση δικτύου βασισμένο στο Ethereum	Διαθέτει μεθοδολογία ανάθεσης και αποδείξεως	Εγγυάται ισχυρή ανωνυμία και προστασία χρηστών	Παρέχει δίκαιη συναλλαγή μεταξύ δεδομένων και ανταμοιβών
[28]	Πλατφόρμα χτισμένη πάνω στο Ethereum	Χρησιμοποιεί πέντε είδη έξυπνων συμβολαίων	Διαθέτει ισχυρή μεθοδολογία αξιολόγησης υποβολής	Οι συναλλαγές κοστίζουν στους χρήστες Ethers
[29]	Τοπικό δίκτυο Blockchain μαζί με Bitcoin	Διαθέτει πέντε διαφορετικές συναλλαγές	Εγγυάται εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα	Οι ανταμοιβές βασίζονται στο Bitcoin
[30]	BIFTS μαζί με μια ελαφριά έκδοση του Blockchain	Διαθέτει βάση δεδομένων υπολογιστικού νέφους	Εγγυάται αναβαθμίσεις μηχανισμού συναίνεσης, αξιοπιστία συστήματος, αποτελεσματικότητα	Διαθέτει ισορροπία μεταξύ κόστους ανάπτυξης και αποτελεσματικότητας

3.11 Λόγοι συχνής αποτυχίας του Blockchain στο MCS

Όπως έχουμε δει μέχρι στιγμής, η τεχνολογία Blockchain, παρόλο τα πολλά οφέλη της και τις διαφορετικές περιπτώσεις που μπορεί να χρησιμοποιηθεί, δεν έχει αναπτυχθεί σε μεγάλο βαθμό μέσα στα συστήματα Mobile CrowdSensing. Στην προηγούμενη ενότητα αναφερθήκαμε σε διάφορες εφαρμογές και διάφορα συστήματα που ενώνουν την τεχνολογία Blockchain με το Crowdsensing, αλλά παρατηρήσαμε πως λίγοι έχουν τολμήσει τη συγκεκριμένη προσέγγιση. Οι

λόγοι που δε γίνεται συχνότερα ή με μεγαλύτερη επιτυχία η προσπάθεια συνδυασμού των δυο αυτών τεχνολογιών είναι ότι και οι δύο έχουν κάποια μειονεκτήματα στη δομή τους, τα οποία όταν συνδυάζονται προκαλούν συνήθως περισσότερα προβλήματα από ότι οφέλη και για αυτό το λόγο αποφεύγεται από τους περισσότερους η σύζευξή τους.

Η τεχνολογία Blockchain παρόλο τις δυνατότητες και τα πλεονεκτήματα που παρέχει, έχει και αρκετά μειονεκτήματα, με το κυριότερο να είναι το πρόβλημα επεκτασιμότητας. Η συναίνεση και η επικύρωση των μπλοκ απαιτούν την παρουσία ολόκληρου του blockchain, δηλαδή όλες τις συναλλαγές που έχουν συμβεί, απαιτώντας έτσι μεγάλο χώρο αποθήκευσης. Από τη στιγμή που κάποιο σύστημα crowdsensing δεν μπορεί να διαθέσει αυτό το μέγεθος χώρου αποθήκευσης καθιστά αρκετά δύσκολη τη χρήση του blockchain μέσα σε αυτό. Ακόμα ένα θέμα του blockchain είναι αυτό που ονομάζουμε πρόβλημα επίθεσης 51%. Το συγκεκριμένο προκύπτει αν περισσότερο από το 51% των κόμβων συνεργάζονται για να δημιουργήσουν ψεύτικα μπλοκ ή αντίστροφα επιβεβαιωμένες συναλλαγές. Από τη στιγμή που μεγαλύτερη υπολογιστική δύναμη οδηγεί σε ταχύτερη δημιουργία μπλοκ, οι γνήσιοι κόμβοι δε θα είναι σε θέση να ανταγωνίζονται για μια φυσιολογική έκδοση του blockchain, καθώς οι κόμβοι θα πίστευαν μόνο τη μεγαλύτερη εκδοχή της αλυσίδας. Ένα επιπρόσθετο πρόβλημα του blockchain είναι η απαιτούμενη ενέργεια. Εκτιμάται ότι η εξόρυξη ενός μόνο Bitcoin χρειάζεται ενέργεια ίση με αυτή που καταναλώνει ένα νοικοκυριό στις Η.Π.Α. σε δυο χρόνια. Εκτιμάται επίσης ότι η κατανάλωση ενέργειας για κάθε συναλλαγή bitcoin είναι ίση με 80.000 φορές την κατανάλωση ενέργειας στην επεξεργασία μιας πιστωτικής κάρτας [31]. Τα εμπόδια όμως δε σταματούν εδώ. Ένα από τα σημαντικότερα εμπόδια που αντιμετωπίζουν τα συστήματα Blockchain είναι η ασφάλεια. Εξάλλου, το όλο σκεπτικό της χρήσης ενός blockchain είναι να επιτρέπουμε σε ανθρώπους που πριν δε γνώριζαν ή δεν εμπιστεύονταν ο ένας τον άλλον, να μοιράζονται δεδομένα με ασφαλή και προστατευμένο τρόπο. Αλλά, η ασφάλεια ακόμα και του καλύτερα δομημένου blockchain δεν αποκλείεται να αποτύχει σε μερικές περιπτώσεις (όπως στις επιθέσεις 51% που αναφέρθηκαν), ζητώντας την εφαρμογή κατάλληλων προληπτικών μηχανισμών για να μετριάσουν ή ακόμα καλύτερα να αποτρέψουν πλήρως τις παραβιάσεις ασφαλείας. Τεράστιο ρόλο παίζει και ο συμβιβασμός, της υπόσχεσης του blockchain για διαφάνεια, με τους πλέον αυστηρότερους κανόνες προστασίας της ιδιωτικότητας από την Ευρωπαϊκή Ένωση βάσει του GDPR (General Data Protection Regulation), οι οποίοι απαιτούν τη δυνατότητα διαγραφής των προσωπικών δεδομένων κατόπιν αιτήσεως [32].

Προβλήματα και προκλήσεις όμως υπάρχουν και στη λειτουργία του CrowdSensing. Είναι εξίσου σημαντικά με τα εμπόδια που αντιμετωπίζουμε στη χρήση της τεχνολογίας blockchain, μάλιστα κάποια συνδέονται και μεταξύ τους, και για αυτό το λόγο κάνει αρκετά δύσκολη, αλλά όχι ακατόρθωτη, την εκμετάλλευση του blockchain μέσα σε συστήματα CrowdSensing. Ένα πρόβλημα κομβικής σημασίας που παρουσιάζεται στο CrowdSensing είναι η αυτοματοποιημένη διαμόρφωση των αισθητήρων. Στην παραδοσιακή διάχυτη πληροφορική, μόνο ένας περιορισμένος αριθμός συσκευών ανίχνευσης (π.χ. αισθητήρες, κινητά τηλέφωνα) συνδέονται στις εφαρμογές. Ωστόσο, στο IoT, αναμένεται να συνδέονται μαζί στο διαδίκτυο μεγάλος

αριθμός συσκευών ανίχνευσης. Επομένως, η σύνδεση και η διαμόρφωση των συσκευών ανίχνευσης στις εφαρμογές αποτελεί μια πολύ σημαντική πρόκληση.

Όπως γνωρίζουμε, δεν είναι εφικτό να συνδέσουμε όλες τις συσκευές ανίχνευσης χειροκίνητα σε μια εφαρμογή ή σε ένα ενδιάμεσο λογισμικό. Θα ήταν ιδανικό να υπάρχει μια αυτοματοποιημένη ή τουλάχιστον ημί-αυτοματοποιημένη διαδικασία για να συνδέει τις συσκευές ανίχνευσης στις εφαρμογές. Για την επίτευξη της σύνδεσης των συσκευών με τις εφαρμογές, θα πρέπει οι εφαρμογές να έχουν την ικανότητα να αναγνωρίζουν τις συσκευές αυτές. Αρκετές πρόσφατες μελέτες, όπως οι Transducer Electronic Datasheet (TEDS), Open Geospatial Consortium (OGC) και Sensor Markup Languages (SensorML) παρουσιάζουν τις μελλοντικές τάσεις όσον αφορά την αντιμετώπιση του προβλήματος της σύνδεσης και της διαμόρφωσης των αισθητήρων στις εφαρμογές.

Το δεύτερο μεγαλύτερο εμπόδιο στα συστήματα CrowdSensing είναι οι περιορισμένοι πόροι που υπάρχουν. Οι συσκευές ανίχνευσης έχουν συνήθως περιορισμένους πόρους και οι περιορισμοί αυτοί οδηγούν συχνά σε αδιέξοδο. Παρόλο που παρέχονται περισσότεροι πόροι για τα κινητά τηλέφωνα, σε σχέση με τους κόμβους ανίχνευσης, τα κινητά τηλέφωνα έρχονται αντιμέτωπα με τον περιορισμό των πόρων. Διαφορετικοί τύποι δεδομένων ανίχνευσης μπορεί να είναι ανεξάρτητοι μεταξύ τους εξαιτίας των πολύτροπων δυνατοτήτων των συσκευών ανίχνευσης. Σε πρακτικά σενάρια, διαφορετικοί τύποι δεδομένων ανίχνευσης μπορούν να χρησιμοποιηθούν για τον ίδιο σκοπό. Ωστόσο, οι διαφορές στην ποιότητα και στην κατανάλωση πόρων των δεδομένων ανίχνευσης παρουσιάζουν ένα εμπόδιο στην προσπάθεια για βελτίωση της ποιότητας των δεδομένων με χαμηλή κατανάλωση πόρων. Συνεπώς, παραμένει ακόμα η πρόκληση για βελτίωση ποιότητας δεδομένων και ελαχιστοποίηση της κατανάλωσης των πόρων. Το πρόβλημα όμως που παρουσιάζει το μεγαλύτερο ενδιαφέρον, όπως και στο Blockchain, είναι η ιδιωτικότητα, η ασφάλεια και η ακεραιότητα των δεδομένων. Οι συσκευές ανίχνευσης ενδέχεται να συλλέγουν ευαίσθητα προσωπικά δεδομένα των χρηστών, με αποτέλεσμα να διακινδυνεύεται η ιδιωτικότητα και η ασφάλεια του καθενός. Για παράδειγμα, οι αισθητήρες GPS συνήθως καταγράφουν προσωπικές πληροφορίες των χρηστών, όπως τις ακριβείς διαδρομές που ακολουθούν και τις τοποθεσίες που βρίσκονται. Με την κοινή χρήση των μετρήσεων των αισθητήρων GPS, η ιδιωτικότητα των χρηστών μπορεί να αποκαλυφθεί. Ως εκ τούτου, είναι άκρως σημαντικό να διασφαλιστεί η ιδιωτικότητα του κάθε χρήστη. Επίσης, το GPS καταγράφει τις πληροφορίες που προέρχονται από καθημερινές μεταφορές που μοιράζονται μέσα σε μια ευρύτερη κοινότητα και μπορούν να χρησιμοποιηθούν για να μάθουμε πληροφορίες σχετικές με την κυκλοφοριακή συμφόρηση μέσα σε μια πόλη. Επομένως, είναι απαραίτητο να δοθεί η δυνατότητα στις εφαρμογές CrowdSensing, ώστε οι χρήστες να μπορούν να κατανοήσουν καλύτερα το περιβάλλον τους και τελικά να καταφέρουν να επωφεληθούν πλήρως από τη συνολική ανταλλαγή πληροφοριών. Προκειμένου να διατηρηθεί η τεράστια ποσότητα προσωπικών πληροφοριών των χρηστών, απαιτούνται πέρα από μεθοδολογικές προσπάθειες και συστηματικές μελέτες.

Η αρχιτεκτονική AnonySense, η οποία προτείνεται στο [33], μπορεί να υποστηρίξει την ανάπτυξη εφαρμογών που δίνουν έμφαση στην προστασία της ιδιωτικότητας και βασίζονται στο CrowdSensing. Επίσης, είναι σημαντικό να διασφαλιστεί ότι τα δεδομένα ενός ατόμου δεν αποκαλύπτονται σε αναξιόπιστα τρίτα μέλη. Για παράδειγμα, κακόβουλοι χρήστες συνήθως συνεισφέρουν λανθασμένα δεδομένα ανίχνευσης. Εν τω μεταξύ, για δικό τους όφελος, κακόβουλοι χρήστες ενδέχεται να μολύνουν σκόπιμα τα δεδομένα ανίχνευσης. Η έλλειψη μηχανισμών ελέγχου για την εξασφάλιση της εγκυρότητας της πηγής και της ακρίβειας των δεδομένων μπορεί να οδηγήσει σε ζητήματα αξιοπιστίας της πληροφόρησης. Ως εκ τούτου, μοιάζει απαραίτητο να αναπτυχθούν τεχνολογίες διατήρησης της εμπιστοσύνης και τεχνολογίες ανίχνευσης οτιδήποτε μη φυσιολογικού προκειμένου να διασφαλιστεί η ποιότητα των δεδομένων που λαμβάνονται. Το πρόβλημα της ακεραιότητας των δεδομένων πρέπει επίσης να αντιμετωπιστεί σωστά. Παρόλο που κατά καιρούς έχουν προταθεί κάποιες μέθοδοι, βασίζονται κυρίως στην συνυπάρχουσα υποδομή που μπορεί να μην είναι εγκατεστημένη σαν μάρτυρας και έχει περιορισμένη δυνατότητα κλιμάκωσης, κάτι το οποίο καθιστά αυτό το είδος μεθόδων απαγορευτικό και κατά περιόδους μη διαθέσιμο. Ο λόγος πίσω από αυτό είναι ότι η προσέγγιση βασίζεται στις εισροές που προέρχονται από την εγκατάσταση ακριβών υποδομών. Μια άλλη προσέγγιση για το χειρισμό του προβλήματος της ακεραιότητας των δεδομένων είναι η υπογραφή στα δεδομένα ανίχνευσης από αξιόπιστες πλατφόρμες. Η προσέγγιση αυτή είναι πιθανώς προβληματική λόγω του ότι η διαδικασία επαλήθευσης πρέπει να διεξάγεται ακόμα και μέσα στο λογισμικό [33].

Κεφάλαιο Τέταρτο

4.1 Hyperledger Fabric

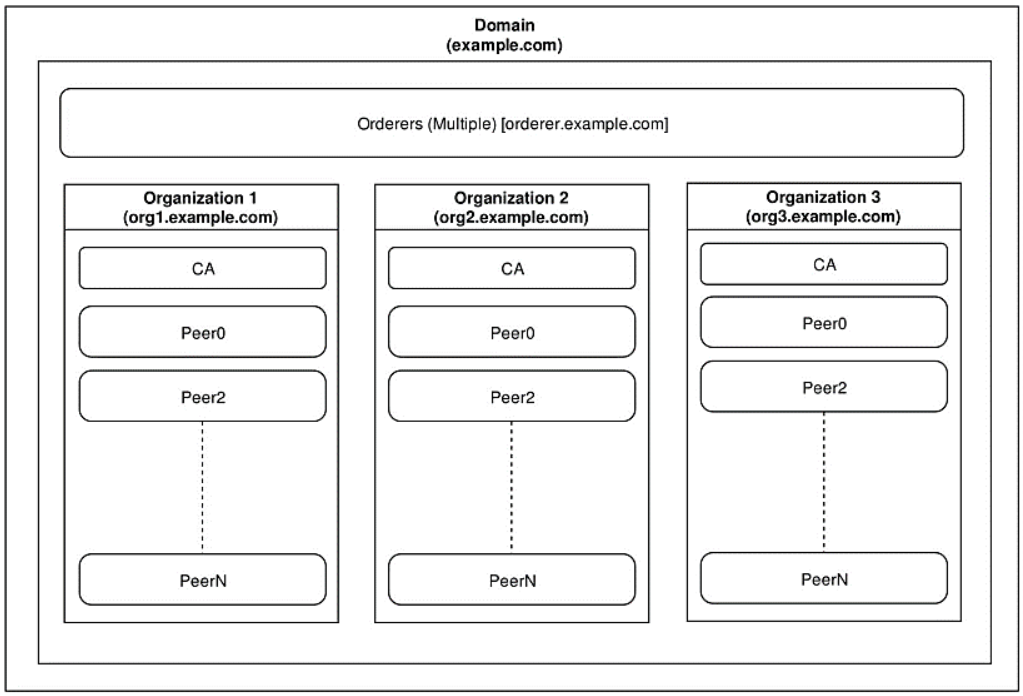
Στην παρούσα διπλωματική εργασία επιλέγουμε να δουλέψουμε πάνω στο Hyperledger Fabric. Όπως είδαμε στην προηγούμενη ενότητα, έχει αρκετά πλεονεκτήματα, κάτι το οποίο το καθιστά ελκυστικό στις επιχειρήσεις που θέλουν να εργαστούν σε μια πλατφόρμα Blockchain. Πιο συγκεκριμένα, οι επιχειρήσεις δεν μπορούν να χρησιμοποιήσουν δημόσια Blockchains λόγω των ακόλουθων λόγων:

- **Θέματα ιδιωτικότητας:** Στα δημόσια Blockchains, σαν το Bitcoin, μπορεί να εισέλθει ο οποιοσδήποτε, συμπεριλαμβανομένων ανώνυμων χρηστών καθώς και χρηστών που χρησιμοποιούν ψεύτικα ονόματα. Πολλές επιχειρήσεις, όπως διάφορα ινστιτούτα οικονομικών υπηρεσιών και πάροχοι υγειονομικής περίθαλψης, εργάζονται κάτω από αυστηρές συνθήκες ιδιωτικότητας. Δεν μπορούν να επιτρέπουν στον καθένα να έχει πρόσβαση σε ευαίσθητα δεδομένα.
- **Δυνατότητα επέκτασης:** Τα περισσότερα δημόσια Blockchains έχουν μικρή δυνατότητα επέκτασης, επειδή απαιτούνται όλοι οι κόμβοι στο δίκτυο για να επεξεργαστούν τις συναλλαγές. Αυτό έχει ως αποτέλεσμα χαμηλή απόδοση συναλλαγών.
- **Αμετάβλητα έξυπνα συμβόλαια:** Τα έξυπνα συμβόλαια δεν μπορούν να αλλάξουν από τη στιγμή που θα αναπτυχθούν και τα αποτελέσματα της εκτέλεσής τους είναι μη αναστρέψιμα. Οι επιχειρήσεις χρειάζονται τρόπους για να διασφαλίσουν ότι είναι bug-free πριν τα αναπτύξουν.
- **Αποθηκευτικά θέματα:** Από τη στιγμή που κάθε πλήρης κόμβος αποθηκεύει όλα τα δεδομένα στο δημόσιο Blockchain, οι απαιτήσεις για χώρο αποθήκευσης είναι πολύ υψηλές και αυξάνονται συνεχώς όσο κυλάει ο χρόνος. Αυτός ο αποθηκευτικός περιορισμός δεν είναι πρακτικός για τις επιχειρήσεις.
- **Μη βιώσιμο αλγόριθμο συναίνεσης:** Το Bitcoin και το Ethereum χρησιμοποιούν τον αλγόριθμο ‘proof of work’, ο οποίος απαιτεί μεγάλη υπολογιστική δύναμη. Καθώς περνάει η ώρα, η δύναμη επεξεργασίας και οι απαιτήσεις ενέργειας αυξάνονται, καθιστώντας τον αλγόριθμο μη πρακτικό για τις επιχειρήσεις.
- **Έλλειψη διακυβέρνησης:** Κανένας δεν ελέγχει τα δημόσια Blockchains, φέρνοντας έτσι την ευθύνη εκτέλεσης βελτιωτικών εργασιών σε μεμονωμένους προγραμματιστές ή κοινότητες προγραμματιστών. Οι επιχειρήσεις χρειάζονται επαρκή διακυβέρνηση για να καταφέρνουν να τρέχουν το blockchain αποτελεσματικά σε βάθος χρόνου.

Οι περισσότερες επιχειρήσεις έχουν συγκεκριμένες απαιτήσεις από ένα δίκτυο Blockchain. Χρειάζονται ένα δίκτυο, που θα μπορούν να ελέγχουν ποιος εισέρχεται σε αυτό και να μπορούν να επαληθεύουν την ταυτότητα του νέου χρήστη με ένα σύστημα ταυτοποίησης. Επίσης, έχουν ανάγκη ταχύτατες εκτελέσεις συναλλαγών για να εξοικονομούν όσο περισσότερο χρόνο είναι δυνατό. Παράλληλα, πρέπει να έχουν τη δυνατότητα να θέτουν κανόνες ελέγχου πρόσβασης για τις ευαίσθητες πληροφορίες που διαθέτουν. Άλλα χαρακτηριστικά που χρειάζονται από το δίκτυο τους είναι η αυτόματη λύση προβλημάτων, η υψηλή ανθεκτικότητα, η δυνατότητα συντήρησής του να είναι ικανοποιητική και έναν αξιόπιστο μηχανισμό συναίνεσης που θα μπορεί να ξεχωρίσει τα καθήκοντα του κάθε χρήστη. Το Hyperledger Fabric είναι μια πλατφόρμα, η οποία τηρεί αυτές τις προϋποθέσεις και την οποία οι επιχειρήσεις μπορούν να χρησιμοποιήσουν για να χτίσουν τα εταιρικά τους Blockchains καλύπτοντας όλες τους τις ανάγκες [57].

4.2 Η αρχιτεκτονική δομή του Hyperledger fabric

Για να γίνει περισσότερο κατανοητή η έννοια του Hyperledger fabric πρέπει πρώτα να μελετήσουμε την αρχιτεκτονική δομή του, την οποία μπορούμε να δούμε αναλυτικά στην εικόνα που ακολουθεί [58]:



Εικόνα 16 : Η αρχιτεκτονική του Hyperledger fabric
Πηγή: (https://dev.to/skcript/hyperledger-fabric-architecture-explained-in-detail-32bb) [58]

Όπως παρατηρούμε και στην παραπάνω εικόνα ένα σύστημα που χρησιμοποιεί το Hyperledger fabric αποτελείται από:

- Domain: Αυτός είναι ο ανώτατος χώρος ονομάτων για το αντίστοιχο έργο που θέλουμε να υλοποιήσουμε. Ας υποθέσουμε ότι δημιουργούμε ένα δίκτυο για μια αλυσίδα εφοδιασμού, συνήθως το όνομα του έργου ή το όνομα τομέα χρησιμοποιείται ως τομέας του Hyperledger Fabric.

- Orderers: Κάτω από έναν τομέα (domain), υπάρχουν παραγγελίες (μπορεί να είναι πολλαπλές) που είναι υπεύθυνες για να διασφαλίσουν ότι όλοι οι peers του δικτύου έχουν πραγματοποιήσει μια συναλλαγή. Όταν μια συναλλαγή προτείνεται και πραγματοποιείται από έναν ομότιμο, ο χρήστης που διατυπώνει την παραγγελία ενημερώνεται για τη νέα συναλλαγή και προωθεί και δεσμεύει αυτό το μπλοκ σε όλους τους γειτονικούς ομότιμους. Όσο περισσότερες είναι οι παραγγελίες τόσο μικρότερα είναι τα ποσοστά αποτυχίας.

- Οργανισμοί (organizations): Οι οργανισμοί είναι τα εμπορευματοκιβώτια για τους peers και τις αντίστοιχες αρχές έκδοσης πιστοποιητικών (CA). Κάθε οργανισμός έχει τη δική του ΑΠ (CA) και μια λίστα με συνομηλίκους. Συνήθως, οι οργανισμοί χρησιμοποιούνται για φυσικό διαχωρισμό του δικτύου blockchain όπου κάθε οργανισμός που χρησιμοποιεί το προϊόν μπορεί να δημιουργήσει τα φυσικά μηχανήματά του και να συμμετάσχει στο δίκτυό.

- Πιστοποιητικές Αρχές (CA): Η αρχή έκδοσης πιστοποιητικών είναι υπεύθυνη για τη δημιουργία πιστοποιητικών για κάθε χρήστη ξεχωριστά. Χρησιμοποιείται για την επαλήθευση της ιδιοκτησίας στο δίκτυο. Κάθε αρχή έκδοσης πιστοποιητικών συνδέεται με έναν οργανισμό.

- Peers: Οι peers είναι κόμβοι που συνδέονται με πελάτες και είναι υπεύθυνοι για την πραγματοποίηση συναλλαγών παγκοσμίως. Κάθε peer έχει το δικό του αντίγραφο συναλλαγών σε μια βάση δεδομένων couchdb. Ένας οργανισμός μπορεί να έχει περισσότερους από έναν peers. Ιδανική θα ήταν η παρουσία πολλών peers σε μια παραγγελία για αποφυγή απώλειας δεδομένων, η ύπαρξη περισσότερων από 3 ή 4 peers μπορεί να οδηγήσει σε υψηλότερα ποσοστά καθυστέρησης.

4.3 Δημιουργία ενός δικτύου με τη χρήση του Hyperledger fabric

Στις προηγούμενες παραγράφους έγινε μια γενική αναφορά για την έννοια, καθώς και τις διάφορες χρήσεις του Hyperledger fabric. Σε αυτή την παράγραφο θα αναλύσουμε τη δημιουργία ενός δικτύου με τη χρήση του Hyperledger fabric. Χρησιμοποιώντας το ήδη προεγκατεστημένο παράδειγμα στο Hyperledger fabric δημιουργούμε ένα δίκτυο που αποτελείται από δύο οργανισμούς, ο καθένας διατηρεί δύο κόμβους peer, και μια υπηρεσία παραγγελίας. Για την υλοποίηση του θα ακολουθήσουμε τα παρακάτω βήματα:

1. Πραγματοποιούμε σύνδεση ως προεπιλεγμένος χρήστης και εκτελούμε το σενάριο byfn.sh έτσι ώστε να δημιουργηθούν πιστοποιητικά και κλειδιά για το δίκτυο. Ο κώδικας που ακολουθεί πραγματοποιεί την παραπάνω διεργασία:

```
$ cd ~
sudo chmod 777 -R fabric-samples
cd fabric-samples/first-network
sudo ./byfn.sh generate
```

2. Δημιουργούμε το δίκτυο fabric εκτελώντας το σενάριο byfn.sh χρησιμοποιώντας την επιλογή up. Αναλυτικότερα ο κώδικας θα διαμορφωθεί ως εξής:

```
$ cd ~
cd fabric-samples/first-network
 sudo ./byfn.sh up
```

Αφού εισάγουμε και αυτή την εντολή θα πρέπει να εμφανίζεται το ακόλουθο αποτέλεσμα στην οθόνη μας:

3. Στην περίπτωση που θέλουμε να "κατεβάσουμε" το δίκτυο μας εκτελούμε το σενάριο byfn.sh χρησιμοποιώντας την επιλογή down για να κλείσουμε και να καθαρίσουμε το δίκτυο. Αυτή η εντολή σκοτώνει τα εμπορευματοκιβώτια, αφαιρεί το υλικό κρυπτογράφησης και τα αντικείμενα και διαγράφει τις εικόνες του κωδικού αλυσίδας. Ο παρακάτω κώδικας αναπαριστά την διαδικασία αυτή:

```
$ cd ~
cd fabric-samples/first-network
sudo ./byfn.sh down
```

4. Έπειτα, χρησιμοποιούμε το εργαλείο για την παραγωγή κρυπτογράφησης και πιστοποιητικών, που ονομάζεται cryptogen, το οποίο χρησιμοποιεί ένα αρχείο διαμόρφωσης YAML ως βάση για τη δημιουργία πιστοποιητικών. Για τη δημιουργία ενός τέτοιου αρχείου θα χρησιμοποιηθεί ο κώδικας που ακολουθεί:

```
$ cd ~
$ cd fabric-samples/first-network
$ sudo ../bin/cryptogen generate –config=./crypto-config.yaml
```

Όταν εκτελεστούν οι παραπάνω εντολές, θα μπορούμε να βρούμε έναν νέο κατάλογο που έχει δημιουργηθεί crypto-config, όπου στο εσωτερικό του υπάρχουν κατάλογοι που αντιστοιχούν στις παραγγελίες και στους ομότιμους οργανισμούς. Στο δικό μας παράδειγμα έχουμε δύο οργανισμούς, τα αντικείμενα δικτύου Org1.example.com και Org2.example.com.

5. Στη συνέχεια, δημιουργούμε τη συναλλαγή διαμόρφωσης. Το εργαλείο για τη δημιουργία της συναλλαγής διαμόρφωσης ονομάζεται configtxgen. Απαραίτητα σε αυτό το βήμα είναι το μπλοκ γένεσης παραγγελιών, η συναλλαγή διαμόρφωσης καναλιού και μια συναλλαγή ακύρωσης για κάθε ομότιμο οργανισμό. Θα υπάρχει επίσης ένα αρχείο configtx.yaml που χωρίζεται σε διάφορες ενότητες: προφίλ, οργανισμούς, παραγγελία και η εφαρμογή. Με τον κώδικα που δίνεται παρακάτω περιγράφεται η διαδικασία αυτή:

```
$ export FABRIC_CFG_PATH=$PWD
sudo ../bin/configtxgen -profile
TwoOrgsOrdererGenesisoutputBlock./channel-artifacts/genesis.block
 export CHANNEL_NAME=mychannel

sudo ../bin/configtxgen -profile TwoOrgsChannel-outputCreateChannelTx
./channel-artifacts/channel.tx -channelID $CHANNEL_NAME

sudo ../bin/configtxgen -profile TwoOrgsChannel-
outputAnchorPeersUpdate ./channel-artifacts/Org1MSPanchors.tx -
channelID $CHANNEL_NAME -asOrg Org1MSP
```

```
sudo ../bin/configtxgen -profile TwoOrgsChannel
-outputAnchorPeersUpdate ./channel-artifacts/Org2MSPanchors.tx -
channelID $CHANNEL_NAME -asOrg Org2MSP
```

6. Το εργαλείο Docker χρησιμοποιείται για την εμφάνιση κοντέινερ Docker. Χρησιμοποιούμε το docker-compose-cli.yaml για να παρακολουθούμε όλα τα κοντέινερ Docker. Αυτό πραγματοποιείται σύμφωνα με τον παρακάτω κώδικα:

```
$ cd ~
$ cd fabric-samples/first-network
$ sudo docker-compose -f docker-compose-cli.yaml up -d
```

Αφού εισάγουμε και τις παραπάνω εντολές κώδικα στην οθόνη μας θα πρέπει να εμφανίζεται κάτι αντίστοιχο με την παρακάτω εικόνα:

Στο κεφάλαιο που ακολουθεί θα μελετήσουμε ένα σενάριο περίπτωσης (case study) με τη χρήση του Hyperledger fabric, όπου και θα περιγραφούν αναλυτικά τα βήματα δημιουργίας και λειτουργίας ενός τέτοιου δικτύου.

Κεφάλαιο Πέμπτο

5.1 Ανάπτυξη ενός test network στο Hyperledger fabric

Σε αυτό το κεφάλαιο θα πειραματιστούμε με το Hyperledger Fabric, δημιουργώντας ένα test network. Όπως και στο first network, το οποίο είδαμε στην προηγούμενη ενότητα, έτσι και το test network έρχεται με ένα καλοσχεδιασμένο script που ονομάζεται network.sh. Συγκεκριμένα, κληρονομεί αρκετό κώδικα από το script byfn.sh του first network. Επίσης, στο test network μπορούμε να δημιουργήσουμε περισσότερα από ένα κανάλια, ενώ στο first network μπορούμε να δημιουργήσουμε μόνο ένα.

Το test network περιέχει τρεις οργανώσεις: μια οργάνωση Orderer και δύο οργανώσεις Peer. Οι δυο Peer οργανώσεις είναι οι Org1 και Org2. Το test network επιτρέπει δύο τρόπους παραγωγής κρυπτό-υλικών. Όταν λέμε κρυπτό-υλικά εννοούμε το ψηφιακό πιστοποιητικό και το κλειδί υπογραφής για όλα τα στοιχεία και τους χρήστες. Ο πρώτος τρόπος είναι η χρήση του binary tools cryptogen, το οποίο χρησιμοποιείται και στο first network. Ο άλλος τρόπος είναι μια πλήρης ανάπτυξη από μια αρχή πιστοποίησης (CA). Σε αυτή την περίπτωση, αναπτύσσεται μια CA σε κάθε οργανισμό και παράγονται κρυπτο-υλικά μέσα στη CA.

Το test network παρέχει ένα ευέλικτο τρόπο για τη δημιουργία ενός καναλιού, έτσι ώστε να είναι δυνατή η δημιουργία πολλών. Αυτό πραγματοποιείται με την αναδιάρθρωση των δραστηριοτήτων που σχετίζονται με το κανάλι σε ένα μόνο βήμα και σε ένα script. Μόλις καθοριστεί το ID του καναλιού κατά την εκτέλεση του script, θα πραγματοποιηθούν οι συναλλαγές διαμόρφωσης, η δημιουργία του μπλοκ δημιουργίας καναλιών και τα peers των μελών των οργανισμών που εισέρχονται στο κανάλι.

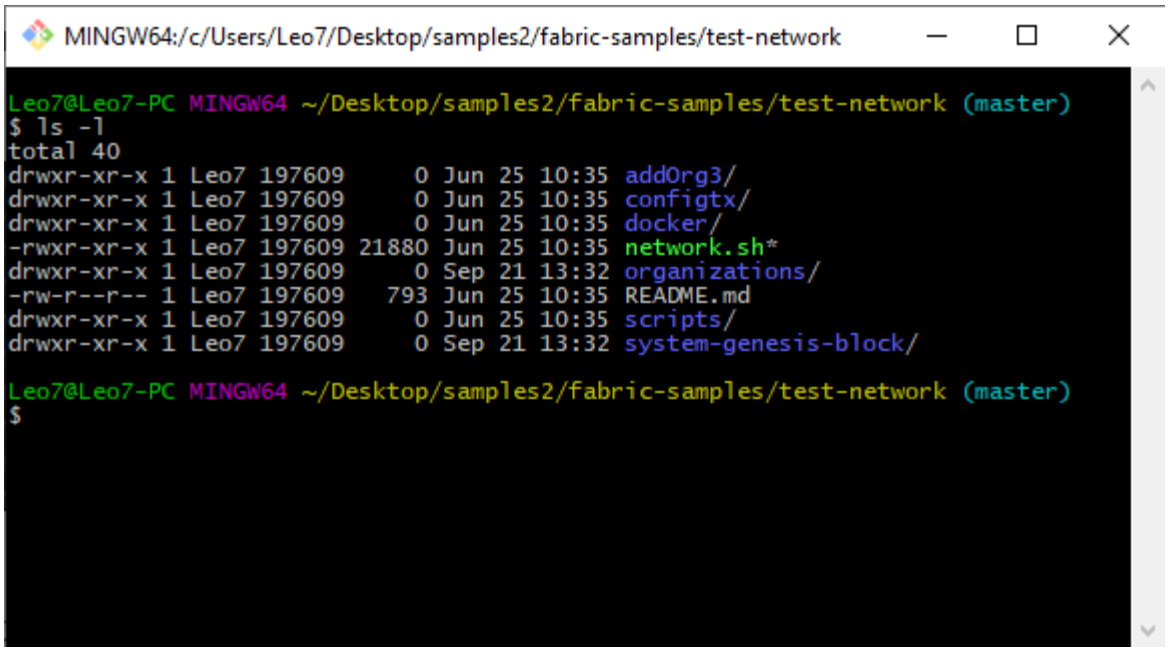
Παρόλο που το chaincode δεν αποτελεί μέρος ενός δικτύου fabric, τα scripts που παρέχονται τόσο από το test network όσο και από το first network έρχονται με δείγμα ανάπτυξης chaincode. Βοηθάει στην επιβεβαίωση ότι το δίκτυο fabric λειτουργεί σωστά με αυτό το δείγμα chaincode.

Το κύριο script για το test network είναι το network.sh. Όπως προαναφέρθηκε, κληρονομεί πολλά τμήματα από το byfn.sh του first network. Το πιο σημαντικό μέρος είναι ότι το network.sh πραγματοποιεί αναδιαρθρώσεις στη λειτουργία, με σκοπό την παροχή περισσότερων δυνατοτήτων και λειτουργιών.

Στο test network, το network.sh έρχεται με ρυθμίσεις και λειτουργίες που παρέχουν ευελιξία. Πιο συγκεκριμένα:

- Το **network.sh up** εμφανίζει τα στοιχεία χωρίς να διαμορφώσει το κανάλι. Αυτό περιλαμβάνει έναν orderer και δυο peers. Σε περίπτωση που δίνεται η επιλογή **–ca**, υπάρχουν ακόμα τρία CA κοντέινερ. Εάν δοθεί η επιλογή **–s,** εμφανίζει ακόμα δύο CouchDB κοντέινερ, ένα για κάθε peer.
- Το **network.sh up createChannel** εμφανίζει τα στοιχεία orderer, peers και όταν χρειαστούν τα CA και CouchDB. Επιπρόσθετα, δημιουργεί ένα κανάλι και τα δύο peers εισέρχονται στο κανάλι. Το προκαθορισμένο είναι το mychannel, αλλά μπορεί κάποιος να προσδιορίσει καινούριο ID καναλιού.
- Το **network.sh createChannel** χρησιμοποιείται για τη δημιουργία ενός καινούριου καναλιού, αφού το δίκτυο τρέχει ήδη. Μπορεί να χρησιμοποιηθεί μετά το network.sh up για να έρθει το πρώτο κανάλι, ή μετά το network.sh up createChannel για τη δημιουργία ενός ακόμα καναλιού. Το ID του καναλιού προσδιορίζεται με την επιλογή **-c** και τα δύο peers θα εισέλθουν στο καινούριο κανάλι. Το script δεν επιτρέπει την είσοδο σε διαμορφωμένα μέλη του καναλιού με αποτέλεσμα να εισέρχονται και τα δύο peers.
- Το **network.sh deployCC** χρησιμοποιείται αφού έχει αναπτυχθεί ένα κανάλι. Το script θα φέρει τον κωδικό του fabcar και καλεί δύο συναρτήσεις για να επαληθεύσει ότι τρέχει ο κώδικας. Μπορεί να χρησιμοποιηθεί η επιλογή **–l** για να διευκρινιστεί η γλώσσα του κώδικα. Η προκαθορισμένη είναι η Golang, ενώ στις επιλογές είναι και η JavaScript με την Java.
- Τέλος, το **network.sh down** είναι η εντολή που μπορεί να τερματίσει τα πάντα, συμπεριλαμβανομένων των περιεχομένων και όσα κοντείνερ και εικόνες έχουν σχέση με τον κώδικα. Μπορεί να χρησιμοποιηθεί όταν κάποιος θέλει ένα καθαρό περιβάλλον για να ξεκινήσει από την αρχή.

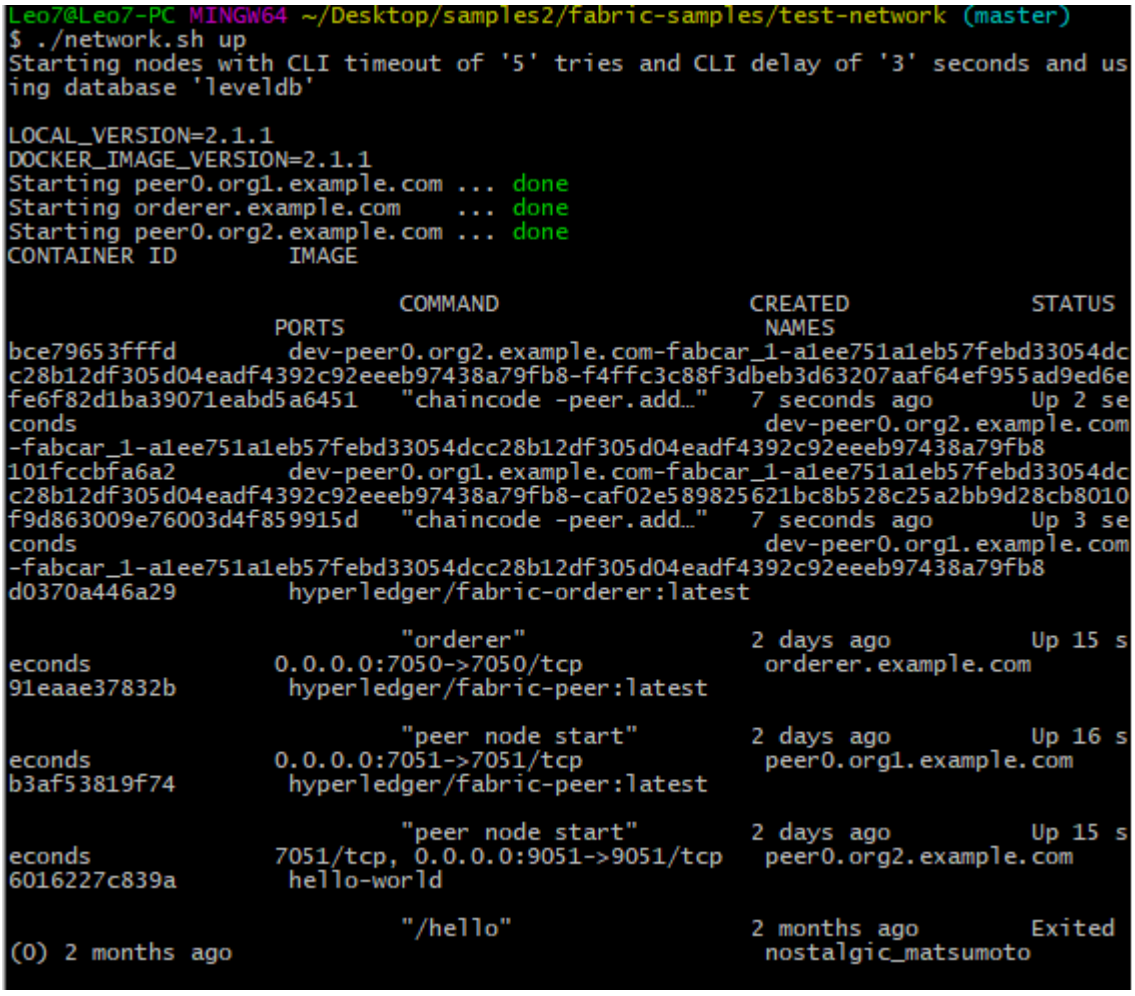
Στη συνέχεια περνάμε στην υλοποίηση του test network. Θα υπάρξει παρουσίαση διαφόρων σεναρίων. Αρχικά, ας δούμε τι περιέχει το test network**:**

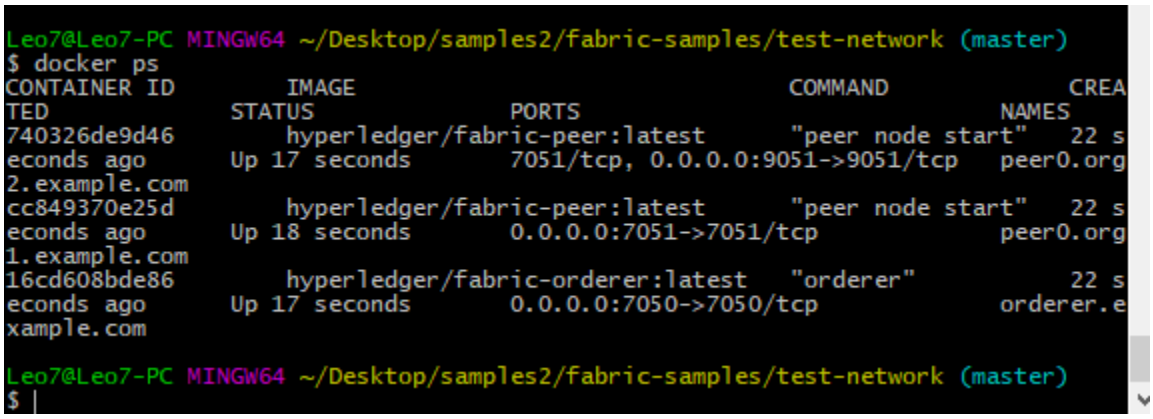


Οι κατάλογοι που θα μας απασχολήσουν είναι οι εξής:

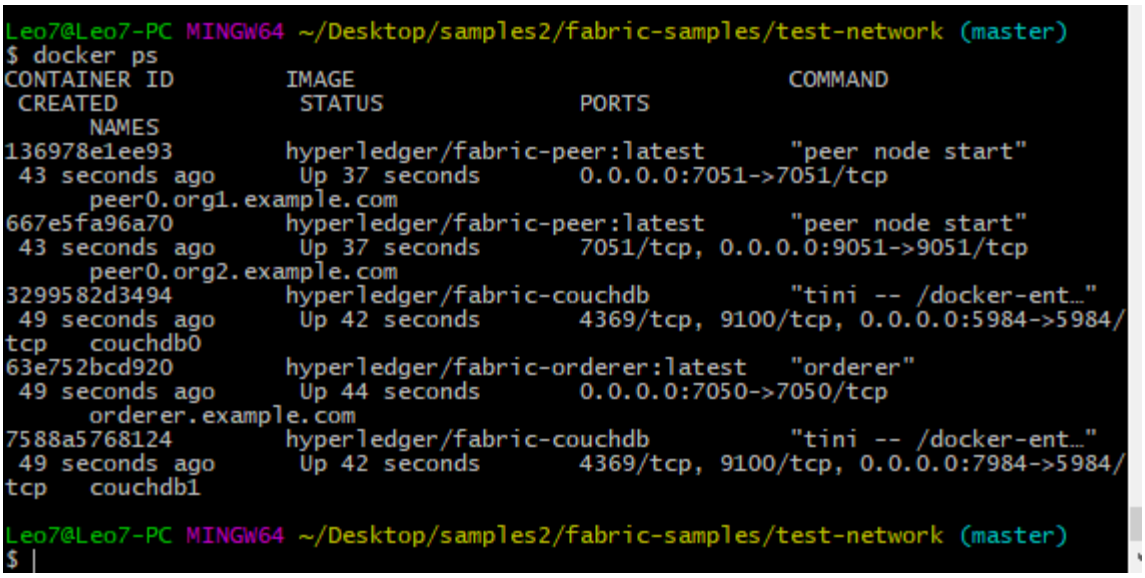
- **configtx:** εκεί βρίσκεται το configtx.yaml
- **docker:** βρίσκονται όλα τα αρχεία docker compose
- **organizations:** σε αυτό τον κατάλογο βρίσκονται όλα τα αρχεία διαμόρφωσης των crypto υλικών και τα υλικά που έχουν παραχθεί
- **scripts:** όλα τα scripts για τις διαφορετικές λειτουργίες
- **system-genesis-block:** εκεί βρίσκεται το genesis μπλοκ

Χρησιμοποιούμε την εντολή **./network.sh up** για να δημιουργήσουμε το δίκτυο και την εντολή **docker ps** για να δούμε ποια κοντείνερ τρέχουν.

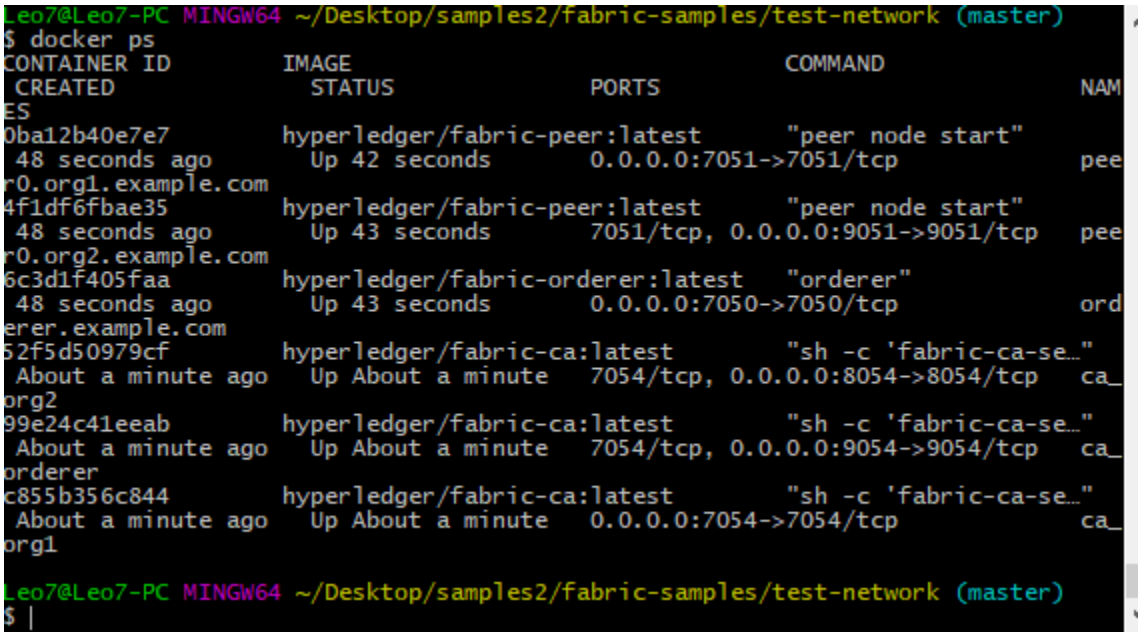




Όπως μπορούμε να διακρίνουμε τρέχουν τρία κοντέινερ, ένα orderer και δύο peers. Αν χρησιμοποιήσουμε την εντολή **network.sh up** με την επιλογή **–s couchdb,** θα δημιουργηθούν δύο CouchDB κοντέινερ, ένα για κάθε peer.



Σε περίπτωση που θέλουμε να τρέξουμε το δίκτυο με την επιλογή **–ca,** θα δούμε τρία πρόσθετα κοντέινερ, ένα για κάθε οργανισμό.

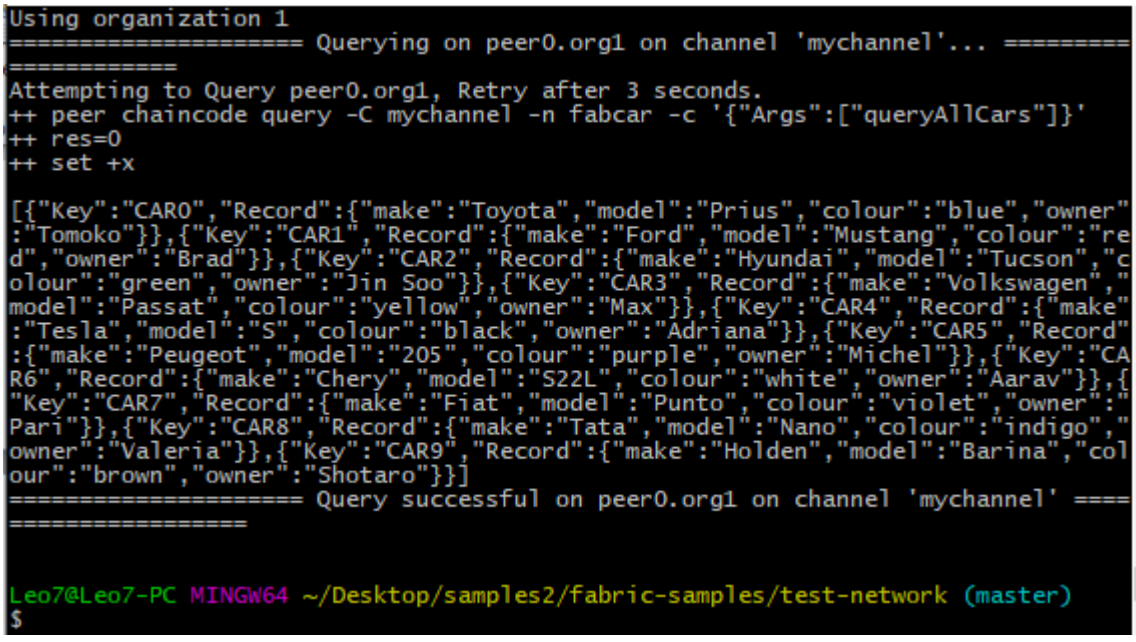


Στη συνέχεια στρέφουμε την προσοχή μας στα κανάλια. Αρχικά, θα ανεβάσουμε το δίκτυο με το προκαθορισμένο mychannel. Με την εντολή **docker exec peer0.org1.example.com peer channel list** μπορούμε να δούμε σε ποια κανάλια έχουν εισέλθει τα peers.

Παράλληλα, μπορούμε να προσθέσουμε ακόμα ένα κανάλι, το οποίο θα ονομάσουμε newchannel.

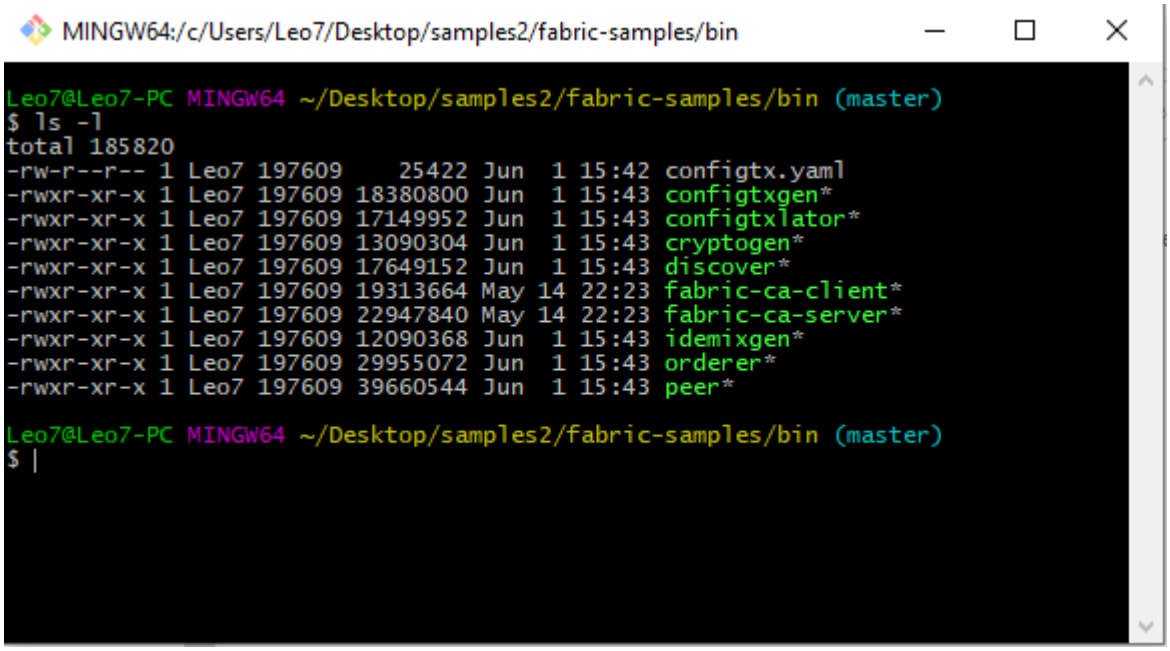
Βλέπουμε ότι έχει προστεθεί ακόμα ένα κανάλι και τα peers έχουν εισέλθει και σε αυτό.

Αν επιλέξουμε να ρίξουμε το δίκτυο και στη συνέχεια να το εκκινήσουμε με την επιλογή **deployCC**, θα μας οδηγήσει σε λάθος διότι ακόμα δεν υπάρχει τίποτα. Πρέπει αρχικά να εκκινήσουμε το test network με το προκαθορισμένο κανάλι και μετά να αναπτύξουμε τον κώδικα. Θα λάβουμε πίσω το αναμενόμενο αποτέλεσμα:



Στο first network υπάρχει ένα CLI κοντέινερ και όλες οι εντολές peer μπορούν να διευθετηθούν από το κοντέινερ είτε με τη χρήση της εντολής **docker exec cli**,είτε με τη χρήση της εντολής

docker exec –it cli bash. Στο test network δεν ορίζεται κάποιο CLI κοντέινερ. Αυτές οι εντολές peer εκτελούνται από τον τοπικό host. Το peer executable βρίσκεται εδώ:



5.2 Το Ethereum ως πλατφόρμα για την τεχνολογία Blockchain

Όπως έχει προαναφερθεί, το blockchain αποτελεί μια από τις τεχνολογίες που απαρτίζουν τη νέα γενιά του διαδικτύου. Παρουσιάζει μια άκρως αποτελεσματική λύση στα προβλήματα σχετικά με την εμπιστοσύνη, τα οποία αντιμετωπίζουν οι χρήστες. Η τεχνολογία blockchain μας επιτρέπει να αποκτήσουμε εμπιστοσύνη στις εξόδους του δικτύου, χωρίς να είναι αναγκαίο να εμπιστευτούμε όλους του συμμετέχοντες σε αυτό.

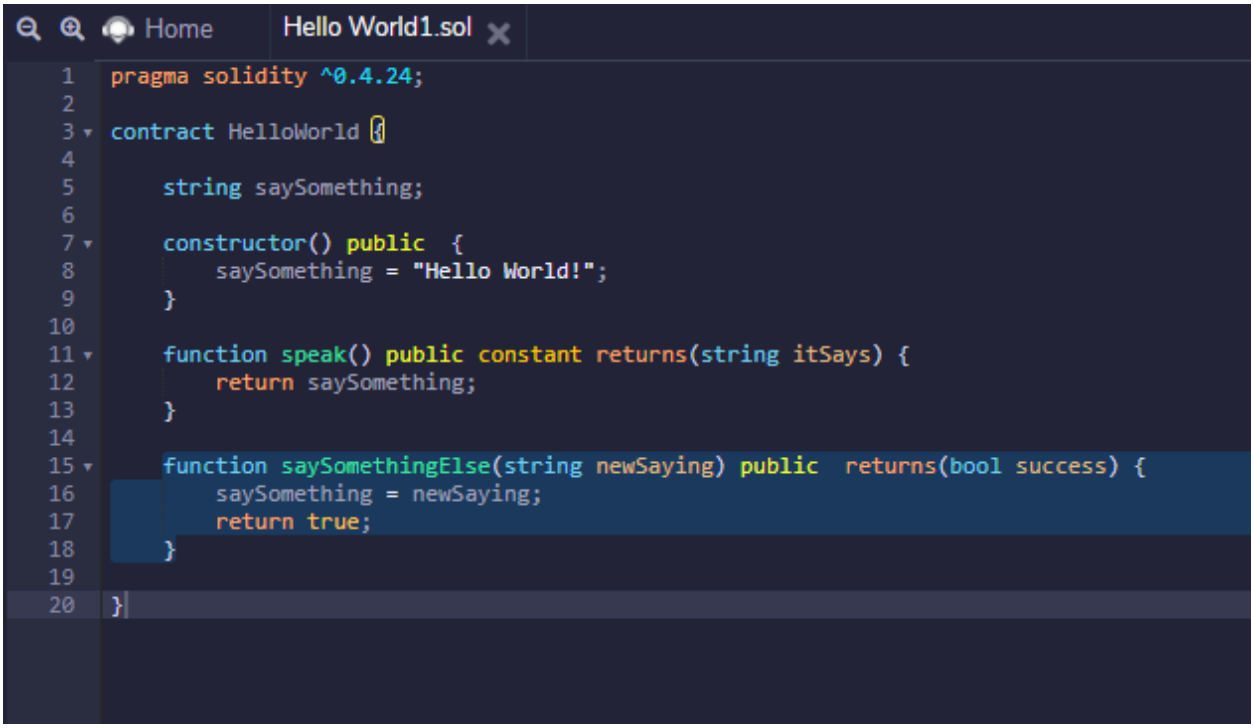
Το blockchain λειτουργεί στο διαδίκτυο, πάνω σε ένα δίκτυο ομότιμων κόμβων (P2P), οι οποίοι έχουν την ικανότητα να διατηρούν ένα πιστό αντίγραφο του συνόλου των συναλλαγών, επιτρέποντας έτσι την πραγματοποίηση συναλλαγών χωρίς να είναι αναγκαία η παρουσία κάποιου ενδιάμεσου, αλλά μόνο η βοήθεια που παρέχουν οι υπόλοιποι κόμβοι του δικτύου [59].

Η καινοτομία που διαθέτει το Ethereum σε σχέση με το Bitcoin είναι ότι το Ethereum αποτελεί μια πλατφόρμα με μεγαλύτερη ευελιξία και προσαρμοστικότητα, πάνω στην οποία μπορούν να δημιουργηθούν και να λειτουργήσουν, χωρίς να αντιμετωπίζουν προβλήματα ασφαλείας, διάφορες αποκεντρωμένες εφαρμογές. Το Bitcoin, σε αντίθεση, παρέχει κυρίως τη δυνατότητα οικονομικών κυρίως συναλλαγών του κρυπτονομίσματός του [60].

Το blockchain του Ethereum αποτελεί μια Turing complete κατανεμημένη υπολογιστική αρχιτεκτονική, μέσα στην οποία κάθε κόμβος του δικτύου πραγματοποιεί εκτέλεση και καταγραφή των ίδιων συναλλαγών, οι οποίες οργανώνονται σε μπλοκ και έτσι γίνεται η προσθήκη τους στο blockchain. Στο blockchain γίνεται κάθε φορά προσθήκη ενός μόνο μπλοκ, το οποίο θα περιέχει το Proof of Work, αν και τον τελευταίο καιρό έχουν προκύψει προβλήματα λόγω της μεγάλης κατανάλωσης ισχύος και γίνεται συζήτηση για τη μετάβαση στο Proof of Stake. Όπως έχουμε ξαναδεί νωρίτερα, οι κόμβοι οι οποίοι συντηρούν το δίκτυο και δημιουργούν τα μπλοκ ονομάζονται miners.

5.3 Αναλυτική παρουσίαση συμβολαίου Hello World

Στη συνέχεια γίνεται αναλυτική παρουσίαση των βημάτων που ακολουθήθηκαν για τη δημιουργία του συμβολαίου **Hello World** στη Solidity. Πραγματοποιήθηκε η επιλογή του συγκεκριμένου απλού έξυπνου συμβολαίου εξαιτίας των βασικών χαρακτηριστικών που διαθέτει, τα οποία χρησιμοποιούνται στα περισσότερα έξυπνα συμβόλαια στο Ethereum.



```
pragma solidity ^0.4.24;
```

Η έκδοση της Solidity που χρησιμοποιήθηκε.

```
contract HelloWorld {
```

Το συμβόλαιο που αναπτύσσουμε και το όνομα που του δίνουμε, στη συγκεκριμένη περίπτωση Hello World.

```
string saySomething;
```

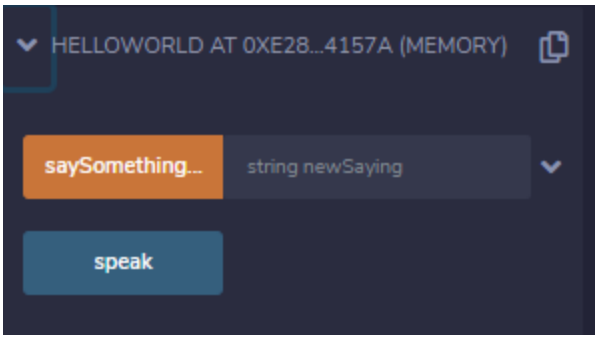
Η string που θα καλέσουμε για να εμφανίσει το μήνυμα, το οποίο θα τοποθετήσουμε στη συνέχεια.

```
constructor() public  {
        saySomething = "Hello World!";
    }
```

Ο κατασκευαστής, τον οποίο θέτουμε ως δημόσιο (public), του συμβολαίου μας Hello World. Μέσα αναθέτουμε στην string, την οποία δημιουργήσαμε νωρίτερα, το μήνυμα που θέλουμε να εμφανιστεί, στην προκειμένη περίπτωση το Hello World!

```
function speak() public constant returns(string itSays) {
        return saySomething;
    }
```

Η συνάρτηση speak εμφανίζει ένα κουμπί στη Solidity,το οποίο θα χρησιμοποιούμε κάθε φορά που θέλουμε να εμφανιστεί το μήνυμα που έχουμε τοποθετήσει στη string saySomething. Επιστρέφει τη string itSays και τη saySomething, δηλαδή θα παρουσιάζει το μήνυμα itSays Hello World!




```
function saySomethingElse(string newSaying) public  returns(bool
success) {
        saySomething = newSaying;
        return true;
    }
```

Τέλος, η συνάρτηση saySomethingElse εμφανίζει ένα κουμπί στη Solidity, που σου επιτρέπει να εισάγεις, χωρίς να αλλάξεις τον κώδικα, ένα καινούριο μήνυμα για να εμφανίζεται. Θέτουμε τη string saySomething ως newSaying και εκεί μπορούμε εκτός κώδικα να πληκτρολογήσουμε το νέο μήνυμα που θέλουμε να εμφανιστεί.

Κεφάλαιο Έκτο

6.1 Επίλογος

Είναι πλέον ευρέως αποδεκτό ότι η τεχνολογία αποτελεί μεγάλο μέρος της καθημερινής μας ζωής και μας διευκολύνει σε αρκετούς τομείς. Ελάχιστοι είναι οι τομείς της ζωής μας που δεν έχουν κάποια εξάρτιση από την τεχνολογία και όσο περνάει ο καιρός οι τομείς αυτοί θα λιγοστεύουν. Αυτό συμβαίνει επειδή η τεχνολογία χρησιμοποιείται και ανταπτύσσεται για τη διευκόλυνση της ζωής μας και πολλών καθημερινών διαδικασιών. Μια από τις τεχνολογίες που έχει ως κύριο στόχο τη διευκόλυνση της ζωής μας είναι το Mobile Crowdsensing.

Στη συγκεκριμένη διπλωματική πραγματοποιείται αρχικά μια ανάλυση του περιβάλλοντος του Internet of Things, δηλαδή όλα τα έξυπνα αντικείμενα που υπάρχουν γύρω μας και η επικοινωνία μεταξύ τους. Στη συνέχεια γίνεται μελέτη των κύριων τεχνολογιών του IoT, των διάφορων τάσεων που υπάρχουν σε αυτό, αναλύεται η αρχιτεκτονική του και τέλος παρουσιάζεται ένα παράδειγμα μιας εφαρμογής σε περιβάλλον IoT για καλύτερη κατανόησή του.

Έπειτα, πραγματοποιείται παρουσίαση του Mobile Crowdsensing. Αναλύεται η αρχιτεκτονική ενός συστήματος MCS, τα κύρια χαρακτηριστικά των εφαρμογών που χρησιμοποιούν το MCS, οι κατηγορίες των εφαρμογών που έχουν αναπτυχθεί μέχρι σήμερα και στη συνέχεια διεξάγεται μια σύγκριση του με τα παραδοσιακά δίκτυα αισθητήρων προκειμένου να δούμε αν συμφέρει να το χρησιμοποιούμε στις εφαρμογές μας και την καθημερινή μας ζωή. Αφού παρατηρηθεί η ευκολία που προσφέρει σε διάφορους τομείς της ζωής μας, γίνεται αναφορά στην ασφάλεια στη χρήση του MCS, καθώς και στις προκλήσεις που παρουσιάζουν τα συστήματα MCS και στις λύσεις που δίνονται για να ξεπεραστούν.

Στη συνέχεια, γίνεται μελέτη της τεχνολογίας Blockchain και αναλύονται οι περιπτώσεις όπου μπορεί να χρησιμοποιηθεί η συγκεκριμένη τεχνολογία. Αναφέρονται τα οφέλη που παρέχει στους χρήστες, οι δυσκολίες που παρουσιάζει, καθώς και τα έξυπνα συμβόλαια, τα οποία αποτελούν βασικό κομμάτι του Blockchain, μαζί με άλλες βασικές λειτουργίες του. Βλέπουμε γνωστές πλατφόρμες Blockchain και σημειώνουμε τι προσφέρει η κάθε μια, καθώς και τα γνωστά μοντέλα Blockchain. Επιπρόσθετα, προσπαθούμε να συνδυάσουμε την τεχνολογία Blockchain με τα συστήματα MCS και να δούμε τι πλεονεκτήματα μπορούμε να έχουμε από το συνδυασμό αυτό, καθώς πραγματοποιείται και μελέτη των ήδη υπάρχοντων συστημάτων που τα χρησιμοποιούν μαζί. Στο τέλος, παρουσιάζεται και ένας πίνακας σύγκρισης των συστημάτων που μελετήθηκαν, μαζί με τα κύρια χαρακτηριστικά του καθενός.

Μετέπειτα, πραγματοποιείται μεγαλύτερη ανάλυση του Hyperledger Fabric, μιας πλατφόρμας Blockchain που έχει αναφερθεί στα προηγούμενα κεφάλαια. Παρατηρούμε την ιδιαίτερη

αρχιτεκτονική του και προχωράμε στην ανάπτυξη ενός δοκιμαστικού δικτύου μέσα στην πλατφόρμα. Επιπρόσθετα, αναλύουμε την πλατφόρμα Ethereum ως πλατφόρμα για την τεχνολογία Blockchain και αναπτύσσουμε ένα συμβόλαιο Hello World σε αυτό.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Lu Tan, Neng Wang, Future Internet: The Internet of Things, 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE), 2010, pp. V5 376-V5 379

[2] Andrea Capponi, Claudio Fiandrino, Burak Kantarci, Luca Foschini, Dzmitry Kliazovich, Pascal Bouvry, A Survey on Mobile Crowdsensing Systems:Challenges, Solutions and Opportunities , IEEE Communications Surveys & Tutorials (Volume: 21 , Issue: 3 , thirdquarter 2019), pp. 2419 - 2465

[3] R. Ganti, F. Ye, and H. Lei, "Mobile crowdsensing: current state and future challenges," IEEE Communications Magazine, vol. 49, no. 11, pp. 32–39, Nov 2011.

[4] B. Guo, Z. Yu, X. Zhou, and D. Zhang, "From participatory sensing to mobile crowd sensing," in IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), Mar 2014, pp. 593–598

[5] Sherif B. Azmy, Ruslan Abu Sneineh, Nizar Zorba, and Hossam S. Hassanein, Small Data in IoT: An MCS Perspective, In book: Performability in Internet of Things, January 2019, pp. 209-225

[6] Konstantina Banti, Filomeni Katsimpoura, Malamati Louta, George T. Karetsos, Data Quality in Mobile Crowd Sensing Systems: Challenges and Perspectives, 9th International Conference on Information, Intelligence, Systems and Applications (IISA), 2018, pp. 1-3

[7] Μπαντή Κωνσταντίνα, Συστήματα ανίχνευσης και συλλογής πληροφοριών με χρήση έξυπνων κινητών συσκευών των χρηστών, Διπλωματική Εργασία, 2016, pp. 18-21

[8] Raghu K. Ganti, Fan Ye, and Hui Lei, Mobile Crowdsensing: Current State and Future Challenges, IEEE Communications Magazine (Volume: 49 , Issue: 11 , November 2011), pp. 32-39

[9] S. Fahl, M. Harbach, T. Muders, L. Baumgärtner, B. Freisleben, M. Smith, Why Eve and Mallory love Android: an analysis of Android SSL (in) security, in: Proceedings of the 2012 ACM Conference on Computer and Communications Security, ACM, 2012, pp. 50–61.

[10] D. Sounthiraraj, J. Sahs, G. Greenwood, Z. Lin, L. Khan, SMV-hunter: Large scale, automated detection of SSL/TLS man-in-the-middle vulnerabilities in android apps, in: In Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS'14. 2014, Citeseer, pp. 1–12

[11] D. He, M. Naveed, C.A. Gunter and K. Nahrstedt, Security concerns in Android mHealth apps, AMIA Annual Symposium Proceedings, American Medical Informatics Association (2014), pp. 645-655

[12] Malamati Louta, Konstantina Mpanti, George Karetsos, Mobile Crowd Sensing Architectural Frameworks: A Comprehensive, 7th International Conference on Information, Intelligence, Systems & Applications (IISA), 2016, pp.1-3

[13] Oscar Novo, Blockchain Meets IoT: an Architecture for Scalable Access Management in IoT, IEEE Internet of Things Journal (Volume: 5 , Issue: 2 , April 2018), pp. 1184-1195

[14]http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html, accessed at 15/06/20

[15] Dr.Liew Voon Kiong, Blockchain and Cryptocurrency, A Blockchain and Cryptocurrency Guidebook for Everyone, 2020

[16] Damien Cosset, Blockchain: What is Mining?, https://dev.to/damcosset/blockchain-what-is-mining-2eod, 2018, accessed at 15/06/20

[17] Konstantinos Christidis, Michael Devetsikiotis, Blockchains and Smart Contracts for the Internet of Things, IEEE Access (Volume: 4), 2016, pp. 2292-2303

[18] Iuon-Chang Lin, and Tzu-Chun Liao, A Survey of Blockchain Security Issues and Challenges, International Journal of Network Security 19(5):653-659, 2017

[19] Scott Ruoti, Ben Kaiser, Arkady Yerukhimovich, Jeremy Clark, Robert Cunningham,Blockchain Technology: What is it good for?, Queue vol. 17, no. 5, 2019, pp.1-23

[20] Ye Guo, Chen Liang, Blockchain application and outlook in the banking industry, Financial Innovation (2016) 2:24, 2016, pp.1-10

[21] Nir Kshetri, Can Blockchain Strengthen the Internet of Things?, IT Professional (Volume: 19 , Issue: 4 , 2017), pp. 68-72

[22] Junqin Huang, Lingkun Kong, Linghe Kong, Zhen Liu, Zhiqiang Liu and Guihai Chen, Blockchain-based Crowd-sensing System, 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), 2018, pp. 234-235

[23] Ming Li, Jian Weng, Anjia Yang, Wei Lu,Yue Zhang, Lin Hou, Jia-Nan Liu, Yang Xiang, Robert H. Deng, CrowdBC: A Blockchain-based Decentralized Framework for Crowdsourcing, IEEE Transactions on Parallel and Distributed Systems (Volume: 30 , Issue: 6 , June 1 2019), pp. 1251-1266

[24] Jingzhong Wang, Mengru Li, Yunhua He, Hong Li, Ke Xiao, Chao Wang, A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications, IEEE Access (Volume: 6), 2018, pp. 17545-17556

[25] Bing Jia, Tao Zhou, Wuyungerile Li, Zhenchang Liu, and Jiantao Zhang, A Blockchain-Based Location Privacy Protection Incentive Mechanism in Crowd Sensing Networks, Special Issue: Recent Advances in Computational Intelligence Paradigms and Machine Learning for Security, Privacy and Forensics in Cloud Computing), 2018, pp. 1-11

[26] Wei Fang, Zheng Yan, MCS-Chain: Decentralized and trustworthy mobile crowdsourcing based on blockchain, Future Generation Computer Systems, Volume 95, June 2019, pp. 649-666

[27] Yuan Lu, Qiang Tang and Guiling Wang, ZebraLancer: Crowdsource Knowledge atop Open Blockchain, Privately and Anonymously, IEEE 38th International Conference on Distributed Computing Systems (ICDCS), 2018, pp.853-864

[28] Gurpriya Kaur Bhatia, WorkerRep: Building Trust on Crowdsourcing Platform Using Blockchain, Thesis for: Masters, 2018, pp. 4-29

[29] Ali Dorri , Salil S. Kanhere , Raja Jurdak and Praveen Gauravaram, Blockchain for IoT Security and Privacy: The Case Study of a Smart Home, 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2017, pp. 1-6

[30] Yung Po Tsang, King Lun Choy, Chun Ho Wu, George To Sum Ho, Hoi Yan Lam, Blockchain-Driven IoT for Food Traceability With an Integrated Consensus Mechanism, IEEE Access (Volume: 7), 2019, pp. 129000-129017

[31] Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Das, G., Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems, IEEE Consumer Electronics Magazine, 7(4), 2018, pp. 6–14

[32] Maged N. Kamel Boulos, James T. Wilson and Kevin A. Clauson, Geospatial blockchain: promises, challenges, and scenarios in health and healthcare, International Journal of Health Geographics 17(25), 2018, pp. 1-8

[33] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos. Anonysense: Privacy-aware people-centric sensing. In Proc. of ACM MobiSys, 2008, pp. 211–224

[34] Kurt Wagner, Facebook is making its biggest executive shuffle in company history, https://www.vox.com/2018/5/8/17330226/facebook-reorg-mark-zuckerberg-whatsapp-messenger-ceo-blockchain, 2018, accessed at 20/6/20

[35] Chaim Gartenberg, Facebook reportedly plans to launch its own cryptocurrency, https://www.theverge.com/2018/5/11/17344318/facebook-cryptocurrency-token-blockchain-report-david-marcus, 2018, accessed at 20/6/20

[36] Jim Epstein, Is Blockchain Technology a Trojan Horse Behind Wall Street's Walled Garden?, https://reason.com/podcast/bitcoin-consensus-blockchain-wall-street/, 2016, accessed at 20/6/20

[37] Jemima Kelly, Banks adopting blockchain 'dramatically faster' than expected: IBM, https://www.reuters.com/article/us-tech-blockchain-ibm-idUSKCN11Y28D, 2016, accessed at 21/6/20

[38] Jemima Kelly, UBS leads team of banks working on blockchain settlement system, https://www.reuters.com/article/us-banks-blockchain-ubs-idUSKCN10Z147, 2016, accessed at 21/6/20

[39] Chiraag Patel, Huntercoin is the World's First Peer to Peer Massively Multiplayer Online Cryptocurrency Game, https://gomedici.com/huntercoin-worlds-first-peer-peer-massively-multiplayer-online-cryptocurrency-game, 2014, accessed at 21/6/20

[40]CryptoKitties craze slows down transactions on Ethereum, https://www.bbc.com/news/technology-42237162, 2017, accessed at 21/6/20

[41] Jimmy Aki, Leading Blockchain and Gaming Companies Form Blockchain Game Alliance, https://www.nasdaq.com/articles/leading-blockchain-and-gaming-companies-form-blockchain-game-alliance-2018-09-27, Bitcoin Magazine, 2018, accessed at 21/6/20

[42] Michael Corkery, Nathaniel Popper, From Farm to Blockchain: Walmart Tracks Its Lettuce, https://www.nytimes.com/2018/09/24/business/walmart-blockchain-lettuce.html, 2018, accessed at 21/6/20

[43]Alan Boyle, How satellites and blockchain go together, https://www.geekwire.com/2019/satellites-blockchain-go-together/, 2019, accessed at 22/6/20

[44] Eva Xiao, How blockchain in space aims to challenge the dominance of Google and Amazon in internet services, https://www.techinasia.com/spacechain-blockstream-blockchain-to-satellite, 2017, accessed at 21/6/20

[45] Aaron Pressman, Why Facebook, SpaceX and Dozens of Others Are Battling Over Internet Access From Space, https://fortune.com/2019/01/25/facebook-spacex-internet-access-space/?xid=soc_socialflow_twitter_FORTUNE&utm_campaign=fortunemagazine&utm_medium=social&utm_source=twitter.com, 2019, accessed at 21/6/20

[46] Rainer Böhme, Nicolas Christin, Benjamin Edelman, and Tyler Moore, Bitcoin: Economics, Technology, and Governance, Journal of Economic Perspectives 29(2):213-238, 2015

[47] Bikramaditya Singhal, Gautam Dhameja, Priyansu Sekhar Panda, Beginning Blockchain, 2018, pp. 219-266

[48] Arati Baliga, Nitesh Solanki, Shubham Verekar, Siddhartha Chatterjee, Performance Characterization of Hyperledger Fabric, 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), 2018, pp. 65-74

[49] Dr Gideon Greenspan, MultiChain Private Blockchain — White Paper, 2015, pp 1-17

[50] https://www.openchain.org, accessed at 22/6/20

[51] https://developer.mastercard.com/product/mastercard-blockchain, accessed at 22/6/20

[52] F. Xavier Olleros, Majlinda Zhegu, Research Handbook on Digital Transformations, 2016, pp. 241-243

[53] https://www.goquorum.com/, accessed at 22/6/20

[54] https://www.r3.com/corda-platform/, accessed at 22/6/20

[55] https://www.stellar.org/how-it-works/stellar-basics/, accessed at 22/6/20

[56] https://neo.org/, accessed at 22/6/20

[57]https://www.devteam.space/blog/pros-and-cons-of-hyperledger-fabric-for-blockchain-networks/, accessed at 22/6/20

[58]https://dev.to/skcript/hyperledger-fabric-architecture-explained-in-detail-32bb?fbclid=IwAR3vJSvSyMJPnUT50afb1I_petqr3m3HD6umwtCgtr0di6_HMm7UGqnGo0g+ , accessed at 23/6/20

[59] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System,» 2008. [Ηλεκτρονικό]. Available: https://bitcoin.org/bitcoin.pdf, accessed at 23/6/20

[60] «What is Ethereum?,» [Ηλεκτρονικό]. http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html , accessed at 23/6/20