ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

Διπλωματική Εργασία

«Μελέτη της χρήσης Blockchain και Έξυπνων Συμβολαίων στο Διαδίκτυο των Πραγμάτων»

Ευτυχία Δημητριάδη

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΙΟΥΝΙΟΣ 2019

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

«Μελέτη της χρήσης Blockchain και Έξυπνων Συμβολαίων στο Διαδίκτυο των Πραγμάτων»

Ευτυχία Δημητριάδη

Επιβλέποντες Καθηγητές
Δρ. Βάσος Βασιλείου

Η Διπλωματική Εργασία υποβλήθηκε προς την εκπλήρωση των απαιτήσεων απόκτησης του πτυχίου Πληροφορικής του Τμήματος Πληροφορικής.

Ιούνιος 2019

Ευχαριστίες

Η διπλωματική εργασία αποτελεί μέρος ολοκλήρωσης του Πτυχίου Πληροφορικής. Θα ήθελα να ευχαριστήσω θερμά τον καθηγητή μου κύριο Βάσο Βασιλείου για τις συμβουλές, την καθοδήγηση και τον χρόνο που αφιέρωσε κατά την διάρκεια της ολοκλήρωσης της παρούσας διπλωματικής εργασίας.

Επίσης, ιδιαίτερα θερμές ευχαριστίες θα ήθελα να δώσω στην οικογένεια μου για την υποστήριξη που μου πρόσφεραν κατά την διάρκεια των σπουδών μου και σε ένα δύσκολο αγώνα.

Ευτυχία Δημητριάδη.

Περίληψη

Σκοπός της παρούσας διπλωματικής εργασίας είναι η μελέτη της τεχνολογίας Blockchain, και των έξυπνων συμβολαίων και πώς μπορούν να εφαρμοστούν για την αντιμετώπιση προκλήσεων του Διαδικτύου των Πραγμάτων.

Στο πρώτο κεφάλαιο, γίνεται μία εισαγωγική παρουσίαση όσο αφορά το θεωρητικό υπόβαθρο το οποίο σχετίζεται με το θέμα της πτυχιακής μου εργασίας. Αρχικά, γίνεται μία περιγραφή της εξέλιξη του Παγκόσμιου Ιστού. Στην συνέχεια γίνεται περιγραφή του Διαδικτύου των Πραγμάτων και της τεχνολογίας Blockchain. Τέλος, αναφέρομε στα έξυπνα συμβόλαια και ποιος είναι ο ρόλος του στην συνεργασία με την τεχνολογία Blockchain και το Διαδίκτυο των Πραγμάτων.

Στο δεύτερο κεφάλαιο, γίνεται μία περιγραφή σημαντικών προβλημάτων που υφίστανται ακόμη και σήμερα όσο αφορά το Διαδίκτυο των Πραγμάτων Το συγκεκριμένο κεφάλαιο διαχωρίζεται στις προκλήσεις που έχουν να κάνουν με τις συνδεδεμένες συσκευές και προκλήσεις δικτύων.

Στο τρίτο κεφάλαιο, παραθέτω μία τυπική λύση, όσο αφορά την εφαρμογή της τεχνολογίας Blockchain, στο Διαδίκτυο των Πραγμάτων, με σκοπό την αντιμετώπιση συγκεκριμένων προκλήσεων. Πώς ακριβώς η τεχνολογία αυτή σε συνεργασία με τα έξυπνα συμβόλαια, θα ενισχύσει και θα βελτιώσει υφιστάμενες υπηρεσίες.

Τέλος, η τεχνολογία Blockchain θα λέγαμε ότι έχει αλλάξει κατά πολύ τα δεδομένα στο περιβάλλον του Διαδικτύου των Πραγμάτων. Κλείνοντας, στο τέλος της εργασίας παραθέτω κάποια συμπεράσματα στα οποία έχω καταλήξει.

Περιεχόμενα

Σχήματα

Κεφάλαιο 1

1 ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ

1.1 Εξέλιξη του Παγκόσμιου Ιστού

Η πρώτη γενιά του Παγκόσμιου Ιστού WEB 1.0, ήταν η αρχή μιας επανάστασης για τα δεδομένα της εποχής, συνδέοντας δεδομένα και πληροφορίες στο διαδίκτυο, τα οποία μπορούσαν να παρέχουν εταιρείες και οργανισμοί. Το WEB 1.0 ξεκίνησε ως ένας ηλεκτρονικός χώρος, στον οποίο οι επιχειρήσεις μετέδιδαν πληροφορίες στους πελάτες τους, οι οποίοι είχαν παθητική συμπεριφορά. Δηλαδή οι χρήστες μπορούσαν μόνο να διαβάσουν πληροφορίες. Με το πέρασμα του χρόνου παρουσιάστηκαν προβλήματα ιδιωτικότητας των δεδομένων, πράγμα το οποίο ήταν σημαντικός παράγοντας στην εξέλιξη του διαδικτύου.

Στην συνέχεια, παρουσιάστηκε η δεύτερη γενιά WEB 2.0, η οποία φαίνεται ότι έφερε κρίσιμες αλλαγές στα μοντέλα συμπεριφοράς εφαρμογών, με κύριο σκοπό την διευκόλυνση των χρηστών του Διαδικτύου. Τα βασικά χαρακτηριστικά αυτής της γενιάς ήταν η επένδυση στην αλληλεπίδραση μεταξύ των χρηστών του Διαδικτύου με ιστοσελίδες, καθώς και την δημιουργία εργαλείων τα οποία προσφέρουν ακόμη περισσότερες δυνατότητες. Επίσης, ο αριθμός των χρηστών που μπορεί να υποστηρίξει το WEB 2.0, συγκριτικά με το WB 1.0, είχε αυξηθεί κατά πολύ.

Το WEB 2.0, όπως και η έκδοση 1.0, έχει μία κεντροποιημένη δομή. Προσφέρει την δυνατότητα ανταλλαγής πληροφοριών μεταξύ χρηστών, καθώς και την επικοινωνία μεταξύ χρηστών και οργανισμών, που μπορεί να επηρεάσουν την λήψη αποφάσεων. Η έκδοση 2.0, πρόσφερε την δυνατότητα video streaming, online gaming, οικονομικές συναλλαγές και ορισμένες P2P εφαρμογές. Τα ηλεκτρονικά καταστήματα άρχισαν να κυβερνούν την παγκόσμια οικονομία. Στις εφαρμογές αυτές, υπάρχει μία κεντρική οντότητα, είτε ένας μεσολαβητής ο οποίος έχει τον πλήρη έλεγχο. Αυτό σημαίνει ότι υπάρχει ανάγκη για εμπιστοσύνη μεταξύ των χρηστών προς αυτές τις εφαρμογές. Κάποιες από τις πιο γνωστές πλατφόρμες, οι οποίες παρουσιάστηκαν μέσω της γενιάς WEB 2.0, ήταν η Βικιπαίδεια, το Youtube, το Facebook κλπ.

Η γενιά WEB 3.0 του παγκόσμιου ιστού έρχεται με σκοπό να συνδυάσει την γνώση με διαφορετικές τεχνολογίες, ώστε να λύσει διάφορα ζητήματα προηγούμενων εκδόσεων. Γενικότερα, προσφέρει μια πιο ουσιαστική εμπειρία στους χρήστες του. Επικεντρώνεται σε ένα αποκεντρωμένο μοντέλο δικτύου, ομότιμων χρηστών. Το WEB 3.0 προσφέρει ένα επίπεδο τεχνητής νοημοσύνη, όπου οι συσκευές κατανοούν και επεξεργάζονται πληροφορίες, όπως και ένας άνθρωπος. Το περιεχόμενο των συσκευών οι οποίες συνδέονται στο Διαδίκτυο, είναι προσβάσιμο από διαφορετικά συστήματα. Επίσης χαρακτηρίζεται από ιδιότητες σημασιολογικού ιστού (Semantic Web), όπως η κοινή χρήση διαφορετικών μορφών δεδομένων σε διαφορετικά συστήματα. Η ιδέα πίσω από τον Σημασιολογικό Ιστό, είναι ότι οι δημοσιευμένες πληροφορίες, περιέχουν μετα-δεδομένα τα οποία είναι διαθέσιμα για όλους, θα μπορούν να κατανοούνται από μηχανές ώστε να βοηθήσουν την καλύτερη συλλογή και επεξεργασία τους. Η διαχείριση μετα-δεδομένων, ενισχύει την συνδεσιμότητα, την ασφάλεια και την εμπιστευτικότητα στο Διαδίκτυο.

Σχήμα 1.1: Η εξέλιξη του Παγκόσμιου Ιστού.

Η τεχνολογία Blockchain έρχεται να δώσει την λύση σε διάφορα ζητήματα του Διαδικτύου. Επίσης η χρήση ενός αποκεντρωμένου μοντέλου συμπεριφοράς, η εξάλειψη ενδιάμεσων μεσολαβητών για την επικοινωνία χρηστών του διαδικτύου, καθώς και η ενίσχυση των P2P υπηρεσιών έρχεται να λύσει προβλήματα του μοντέλου client-server το οποίο χρησιμοποιείτε στις εκδόσεις WEB 1.0 και WEB 2.0. Η τεχνολογία Blockhcain φαίνεται ότι θα αποτελέσει ένα από τα βασικά συστατικά του WEB 3.0, σε συνεργασία με άλλες τεχνολογίες.

Υπάρχουν σημαντικές προκλήσεις οι οποίες πρέπει να σημειωθούν όσο αφορά την μετάβαση στην έκδοση WEB 3.0. Για παράδειγμα, η αλλαγή από την κεντροποιημένη αρχιτεκτονική σε αποκεντρομένη αρχιτεκτονική, η διαχείριση των δεδομένων κλπ. Αυτά είναι κάποιες από τις προκλήσεις οι οποίες όπως είναι γνωστό, έχουν ήδη φέρει αρκετά προβλήματα στους χρήστες και γενικότερα στο Διαδίκτυο. Ωστόσο με την επανάσταση των Blockchain εφαρμογών σε συνεργασία με άλλες τεχνολογίες, μπορούμε να πούμε με σιγουριά ότι θα προκύψουν αρκετές αλλαγές στην αρχιτεκτονική και στον τρόπο λειτουργίας του Παγκόσμιου Ιστού [72].

Πιο κάτω παρουσιάζονται ενδεικτικά μερικές τεχνολογίες του οικοσυστήματος WEB 3.0.

Μηνύματα	Χώρος αποθήκευσης
Μηχανές Κατάστασης	Μηχανισμοί συναίνεσης
Τροφοδοσία δεδομένων	Υπολογισμοί αλυσίδας
Πολιτική Διαχείρισης	Κανάλια επικοινωνίας
Κρυπτογραφία	
Πρωτόκολλα μεταφοράς	
Πρωτόκολλα δρομολόγησης	
Peer-to-Peer Δίκτυα	

Σχήμα 1.2: Η στοίβα του Web 3.0 [72].

1.2 Το Διαδίκτυο των Πραγμάτων

1.2.1 Ορισμός του Διαδίκτυο των Πραγμάτων

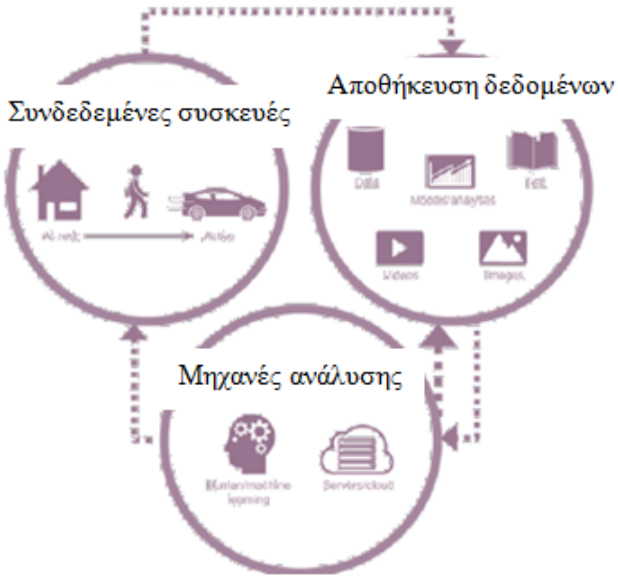
Το Internet of Things (IoT) είναι ένα δίκτυο επικοινωνίας, το οποίο επιτρέπει την σύνδεση κάθε συσκευής στο Διαδίκτυο, και επικοινωνίας τους με άλλες συσκευές οι οποίες είναι επίσης συνδεδεμένες στο Διαδίκτυο. Το Διαδίκτυο των Πραγμάτων είναι ένα περιβάλλον στο οποίο κάθε ηλεκτρονική συσκευή η οποία είναι συνδεδεμένη σε αυτό, έχει την δυνατότητα συλλογής και ανταλλαγής δεδομένων τα οποία έχουν παραχθεί κατά την διάρκεια ζωής τους, είτε δεδομένων που συλλέχθηκαν από το περιβάλλον στο οποίο βρίσκονται. Με απλά λόγια δίνετε η δυνατότητα αίσθησης, επικοινωνίας, αφής και ελέγχου των αντικειμένων τα οποία είναι συνδεδεμένα στο δίκτυο. Οι συσκευές έχουν την δυνατότητα να επικοινωνούν και να αλληλεπιδρούν με άλλα αντικείμενα [29].

Δεν έχει απλά σκοπό να «ενώσει» τους ανθρώπους, αλλά και να ενισχύσει την επικοινωνία των ανθρώπων μαζί με αντικείμενα που βρίσκονται στο περιβάλλον γύρω του. Αυτά τα αντικείμενα μπορεί να είναι οικιακές συσκευές, αυτοκίνητα με ενσωματωμένους αισθητήρες, κάμερες, κλιματιστικά, φώτα, έξυπνα ρολόγια κ.α. Από τις πιο απλές μέχρι τις πιο περίπλοκες συσκευές μπορούν να προσαρμοστούν ώστε να συνδεθούν στο διαδίκτυο και να γίνουν μέρος αυτού [29,74].

Με την άφιξη των αισθητήρων στο IoT, δίνετε η δυνατότητα συλλογής δεδομένων σε πραγματικό χρόνο. Αυτό μπορεί να βοηθήσει στην καλύτερη εξυπηρέτηση των χρηστών, ακόμη και από απόσταση. Για παράδειγμα ένας ιατρός, ο οποίος εργάζεται σε ένα εξοπλισμένο κέντρο υγείας, έχει την δυνατότητα να παρακολουθήσει εξ αποστάσεως τη συμμόρφωση των ασθενών του, όσο αφορά την θεραπεία την οποία έχει προτείνει. Ακόμη, οι υπηρεσίες κοινής ωφέλειας, τηλεπικοινωνιών και περιεχομένου επιτρέπουν στους πελάτες να παρακολουθούν υπηρεσίες και δίνουν την δυνατότητα να πραγματοποιήσουν οι ίδιοι τις πληρωμές τους. Επιπλέον, συσκευές όπως έξυπνοι θερμοστάτες και συσκευές φωτισμού μπορούν να συνδεθούν με αισθητήρες κίνησης, επιτρέποντας την αυτόματη εξοικονόμηση ενέργειας. Τέλος, οι έξυπνες βιντεοκάμερες στους δρόμους, επιτρέπουν στις έξυπνες πόλεις να ελέγχουν καλύτερα τη ροή της κυκλοφορίας, ενώ τα έξυπνα αυτοκίνητα έχουν την δυνατότητα πλοήγησης στους δρόμους, χωρίς καν να υπάρχει οδηγός [74].

Το IoT περιλαμβάνει τα εξής επίπεδα: Εφαρμογές ή άλλα εργαλεία που επιτρέπουν την ανάλυση δεδομένων, Πλατφόρμες, Δίκτυα, Συσκευές. Οι συσκευές

αντιπροσωπεύουν το περιβάλλον του IoT και γενικότερα οποιαδήποτε οντότητα είναι συνδεδεμένη με αυτό. Κάθε συσκευή παράγει δεδομένα, μεταφέροντάς τα σε ένα δίκτυο συνδεσιμότητας. Στο επίπεδο δικτύου, απαιτείται μια πλατφόρμα για την επεξεργασία των δεδομένων και την ενεργοποίηση της επικοινωνίας με απομακρυσμένους χρήστες. Επίσης η πλατφόρμα λειτουργεί ως σημείο επικοινωνίας των συσκευών με το λογισμικό εφαρμογών. Τέλος, οι εφαρμογές έχουν βασικό στόχο την επεξεργασία πληροφοριών που παράγονται από τις συσκευές [75,76].



Σχήμα 1.3: Το οικοσύστημα του IoT.

Το οικοσύστημα IoT, περιλαμβάνεται σε οντότητες όπως έξυπνα τηλέφωνα, tablets κλπ, το οποίο λειτουργεί απομακρυσμένα, με σκοπό είτε να στείλει μια εντολή, είτε να αιτηθεί για πληροφορίες μέσω του δικτύου, σε μία IoT συσκευή. Στη συνέχεια, η συσκευή θα εκτελέσει την εντολή ή θα στείλει τις πληροφορίες πίσω στο δίκτυο, όπου θα τύχουν επεξεργασίας. Όταν μια εταιρεία ενσωματώσει στα συστήματα της, τις δυνατότητες που προσφέρει η συγκεκριμένη τεχνολογία, τότε έχουν την δυνατότητα δημιουργίας μιας σταθερής πηγής πληροφόρησης, από την οποία θα γίνετε συλλογή δεδομένων, με σκοπό την λήψη αποφάσεων.

Μια οριζόντια πλατφόρμα βασισμένη σε πρότυπα επιτρέπει τον μεγαλύτερο έλεγχο προσβάσεων, για τον έλεγχο των συσκευών του Διαδικτύου των Πραγμάτων. Οι οργανισμοί έχουν την δυνατότητα διαχείρισης δεδομένων με ολοκληρωμένες

κλιμακωτές λύσεις ελέγχου ταυτότητας, σε όλους τους κόμβους του δικτύου. Το οριζόντιο μοντέλο, είναι μια ενιαία πλατφόρμα ανοιχτού κώδικα επιτρέπει σε εταιρείες να αναπτύξουν εφαρμογές IoT, που είναι συμβατές μεταξύ τους και είναι σε θέση να αλληλεπιδρούν μέσα σε ένα κοινό πλαίσιο. Η χρήση της οριζόντιας προσέγγισης των συστημάτων, αποτελεί πλεονέκτημα, προσφέροντας μεγαλύτερη ευελιξία, μειωμένο κόστος και απλοποιημένα συστήματα, δεδομένου ότι όλα λειτουργούν στην ίδια πλατφόρμα. Για παράδειγμα, ένας διαχειριστής κτιρίου έχει την δυνατότητα να παρακολουθήσει και να ελέγξει τις κάμερες ασφαλείας, φωτισμό και τους θερμοστάτες από μια ενιαία εφαρμογή.

Η έννοια του οικοσυστήματος μπορεί να εφαρμοστεί σε συγκεκριμένους οργανισμούς όπως σε μία εταιρεία η οποία κατασκευάζει έξυπνα αυτοκίνητα, στα οποία υπάρχουν ενσωματωμένοι αισθητήρες οι οποίοι στέλνουν δεδομένα της μηχανής, στον κατασκευαστή ώστε να γίνουν μελέτες με σκοπό την βελτίωση μελλοντικών μοντέλων. Επίσης η έννοια του IoT ecosystem, αξιοποιείται από βιομηχανίες και επιχειρήσεις για την δημιουργία έξυπνων πόλεων.

Λαμβάνοντας υπόψη τις τρέχουσες ανάγκες της καθημερινότητας για υψηλότερες ταχύτητες και απλότητα στις καθημερινές δραστηριότητας είναι εύκολο να σκεφτούμε ότι το αντίκτυπο στο περιβάλλον αυξάνεται κατά πολύ. Αρκετοί ερευνητές αναφέρουν σε δημοσιεύσεις τους, ότι ο συνδυασμός τεχνολογίας Blockchain- IoT είναι ισχυρός, και έχει ως στόχο να ενισχύσει αρκετές βιομηχανίες. Επίσης πολύ σημαντικό να αναφερθεί ότι, συσκευές IoT μπορούν να πραγματοποιούν αυτόνομες συναλλαγές μέσω έξυπνων συμβολαίων.

1.2.2 Οι τεχνολογίες 'κλειδί', για το Διαδίκτυο των Πραγμάτων [77,78,79]

1.2.2.1 Radio Frequency Identification (RFID)

Τα συστήματα RFID, έχουν σκοπό την αναγνώριση ραδιοσυχνοτήτων, και επιτρέπουν την αυτόματη αναγνώριση και συλλογή δεδομένων με την χρήση ραδιοκυμάτων. Τα βασικά μέρη ενός συστήματος RFID είναι δύο, οι ετικέτες (tags) και οι αναγνώστες (readers).

Οι ετικέτες, είναι μικρά chips, τα οποία αποτελούνται από μία κεραία και ένα ολοκληρωμένο κύκλωμα το οποίο έχει την δυνατότητα να αποθηκεύσει πληροφορίες.

Υπάρχουν τρείς τύποι ετικετών, οι οποίοι διαχωρίζονται βάση του τρόπου επικοινωνίας της ετικέτας με τον αναγνώστη (Οι παθητικές, οι ημι-παθητικές και οι ενεργές ετικέτες). Η ετικέτα, περιέχει δεδομένα με την μορφή ενός ηλεκτρονικού κωδικού προϊόντος (Electronic Product Code – EPC), το οποίο αποτελεί ένα παγκόσμιο σύστημα ταυτοποίησης στοιχείων. Οι πληροφορίες οι οποίες αποθηκεύονται σε μία ετικέτα, μπορεί να είναι είτε απλά αναγνώσιμες, είτε επανεγγράψιμες είτε μίας εγγραφής και πολλών αναγνώσεων.

Οι αναγνώστες, είναι αισθητήρες οι οποίοι έχουν ενσωματωμένη μία μονάδα ελέγχου, μία κεραία, και έχουν την δυνατότητα ανάκτησης δεδομένων από τις ετικέτες. Υπάρχουν τέσσερις τύποι αναγνωστών, οι οποίοι διαχωρίζονται βάση των διαστάσεων τους, την εφαρμογή τους και τις τεχνικές ιδιότητες τους (Οι σταθεροί αναγνώστες, οι ολοκληρωμένοι αναγνώστες, οι αναγνώστες χειρός, και οι ενσωματωμένοι αναγνώστες).

Η λειτουργία των συστημάτων RFID, βασίζεται στην επικοινωνία των ετικετών και των αναγνωστών. Όταν μια ετικέτα βρεθεί στην εμβέλεια της κεραίας ενός αισθητήρα, τότε η μονάδα ελέγχου του αισθητήρα, επικοινωνεί μέσω ραδιοκυμάτων με την κεραία της ετικέτας. Στην συνέχεια ενεργοποιείτε η ετικέτα, και στέλνουν στον αναγνώστη τα ανάλογα δεδομένα. Ακολούθως παρεμβαίνει το ενδιάμεσο λογισμικό (middleware), το οποίο είναι υπεύθυνο για να φιλτράρει τα αιτήματα που αποστέλλει η μονάδα ελέγχου του αναγνώστη.

1.2.2.2 Wireless Sensor Network (WSN)

Ένα ασύρματο δίκτυο αισθητήρων, αποτελείται από αυτόνομους αισθητήρες οι οποίοι συνεργάζονται μεταξύ τους, ώστε να στείλουν δεδομένα που έχουν συλλέξει αλλά και να δέχονται πληροφορίες. Συνήθως, χρησιμοποιούνται για την παρακολούθηση φυσικών ή περιβαλλοντικών συνθηκών, και μπορούν να συνεργάζονται με συστήματα RFID για την καλύτερη παρακολούθηση της κατάστασης συγκεκριμένων πραγμάτων όπως η θέση, η θερμοκρασία και οι κινήσεις τους.

Τα ασύρματα δίκτυα αισθητήρων είναι συμβατά με διαφορετικές τοπολογίες δικτύων και επιτρέπουν την επικοινωνία πολλαπλών κόμβων του δικτύου. Τα βασικά πλεονεκτήματα των ασύρματων επικοινωνιών, είναι η απόδοση, το χαμηλό κόστος και η χαμηλότερη ισχύς κατανάλωσης.

1.2.2.3 Ενδιάμεσο λογισμικό (Middleware)

Το Middleware, είναι το ενδιάμεσο λογισμικό το οποίο παρεμβάλλεται μεταξύ του λογισμικού εφαρμογών και του λειτουργικού συστήματος του δικτύου. Ένα ενδιάμεσο λογισμικό, προσφέρει υπηρεσίες με σκοπό να διευκολύνει την διαδικασία εισόδου και εξόδου πληροφοριών, και ενισχύει την επικοινωνία με την εφαρμογή. Επίσης το Middleware, χρησιμοποιεί λύσεις οι οποίες αντιμετωπίζουν ζητήματα όπως η ετερογένεια, η διαλειτουργικότητα, η ασφάλεια και η εξάρτηση μεταξύ μερών του δικτύου.

Η χρήση του Middleware, κρίνεται αναγκαία και ιδανική επιλογή στην περίπτωση ανάπτυξης εφαρμογών IoT. Το IoT, χρειάζεται σταθερές και επεκτάσιμες λύσεις από την πλευρά του ενδιάμεσου λογισμικού, ώστε να διαχειρίζεται τα δεδομένα που προέρχονται από τα στρώματα του δικτύου. Οι λύσεις ενδιάμεσου λογισμικού που χρησιμοποιούνται σε ένα περιβάλλον IoT, ακολουθούν την αρχιτεκτονική βασισμένη στις υπηρεσίες που προσφέρονται (Service Oriented Architecture - SOA). Στην ουσία, το συγκεκριμένο μοντέλο αρχιτεκτονικής προσφέρει αφαιρετικότητα, σύνθεση και διαχείριση των προσφερόμενων υπηρεσιών.

1.2.2.4 Υπολογιστικό νέφος (Cloud computing)

Το υπολογιστικό νέφος, είναι ένα μοντέλο το οποίο διαθέτει πόρους στο διαδίκτυο, και επιτρέπει την πρόσβαση των χρηστών του δικτύου σε αυτά. Πρόκειται για πόρους οι οποίοι βρίσκονται σε απομακρυσμένα σημεία στον κόσμο, και μέσω των αυτοματοποιημένων διαδικασιών που παρέχονται στους χρήστες του δικτύου, υπάρχει ευελιξία σύνδεσης.

Τα πλεονεκτήματα που προσφέρει το υπολογιστικό νέφος είναι το χαμηλό κόστος φια την διατήρηση και αναβάθμιση πληροφοριών του χρήστη, απεριόριστος χώρος αποθήκευσης, δημιουργία αντιγράφων ασφαλείας, εύκολη πρόσβαση και αρκετές αυτοματοποιημένες διαδικασίες. Όσο αφορά το πρόβλημα της διαχείρισης του μεγάλου όγκου δεδομένων στο Διαδίκτυο των πραγμάτων, το υπολογιστικό νέφος έρχεται να δώσει την λύση στην διαχείριση αρκετά μεγάλων ροών δεδομένων.

1.2.2.5 Λογισμικό εφαρμογών

Οι εφαρμογές IoT, επιτρέπουν την αλληλεπίδραση μεταξύ συσκευών και ανθρώπων με αξιόπιστο τρόπο. Επίσης, είναι σημαντικό να διασφαλιστεί ότι τα δεδομένα που έχουν ληφθεί σε συγκεκριμένα σημεία του δικτύου, έχουν ενεργήσει έγκαιρα και με τον κατάλληλο τρόπο. Γενικότερα, οι βασικές παράμετροι που πρέπει να ληφθούν υπόψη σε αυτό το σημείο, είναι η παρακολούθηση και ο έλεγχος, η διαχείριση μεγάλου όγκου δεδομένων ο διαμοιρασμός δεδομένων και η συνεργασία.

Το Διαδίκτυο των πραγμάτων είναι μία πραγματική επανάσταση αφού έχει φέρει τεράστιες αλλαγές στον χώρο, όπως για παράδειγμα ο καλύτερος σχεδιασμός των δικτύων, γρηγορότερη συνδεσιμότητα κ.α. Για τον ορθολογισμό των λειτουργιών, και την απόκτηση πλεονεκτήματος έναντι των ανταγωνιστών, προτείνεται σε επιχειρήσεις, την ενσωμάτωση όλων των πτυχών του αναδυόμενου οικοσυστήματος του Διαδικτύου (IoT ecosystem), σε μια πλατφόρμα οριζόντιας διαχείρισης.

1.2.3 Προκλήσεις στο Διαδίκτυο των Πραγμάτων [76]

Δύο από τις σημαντικότερες προκλήσεις οι οποίες πρέπει να αντιμετωπιστούν είναι η ασφάλεια και η προστασία των δεδομένων. Είναι πολύ σημαντικό τα ευαίσθητα δεδομένα να παραμένουν ασφαλή, χωρίς να υπάρχει κίνδυνος παραβίασης των προσωπικών δεδομένων οποιουδήποτε χρήστη ο οποίος είναι εγγεγραμμένος στο δίκτυο.

Ερευνητές αναφέρουν ότι, μέχρι το 2020 αναμένεται ότι θα βρίσκονται 50-200 δισεκατομμύρια συσκευές συνδεδεμένες στο IoT, 50 δισεκατομμύρια TB δεδομένων, ένας ογκώδης αριθμός, για το οποίο βέβαια εκτιμάται ότι θα υπάρχει και ένα αρκετά ψηλό κόστος διατήρησης του δικτύου. Αυτό συνεπάγει το ότι πολύ σύντομα θα επηρεαστεί ο τρόπος λειτουργίας των οργανισμών. Δηλαδή, το δίκτυο πρόκειται να μεγαλώσει κατά πολύ, και επίσης ο όγκος των δεδομένων που θα συγκεντρώνεται τις συγκεκριμένες συσκευές. Αυτό σημαίνει ότι πρέπει να βρεθούν αποδοτικοί τρόποι ανάλυσης και επεξεργασίας των δεδομένων μεταξύ μεγάλου αριθμού συσκευών.

Λόγω του μεγάλου αριθμού συσκευών, και της αυξημένης ροής δεδομένων που υπάρχει στο Διαδίκτυο των Πραγμάτων, υπάρχει ανάγκη για αυτοματοποίηση διάφορων διαδικασιών του δικτύου με σκοπό την βελτιστοποίηση της λειτουργικότητας και της αποδοτικότητας του δικτύου.

Ένα από τα βασικότερα μειονεκτήματα των εφαρμογών IoT, είναι η εξάρτηση σε ένα κεντροποιημένο cloud. Αυτό σημαίνει ότι το δίκτυο μπορεί να είναι ευάλωτο σε επιθέσεις, στις οποίες κάποιος μπορεί να κλέψει δεδομένα από συνδεδεμένες συσκευές οι οποίες είναι ενωμένες στο δίκτυο. Για παράδειγμα ο χρόνος διακοπής του διακομιστή του Cloud και η μη διαθεσιμότητα των υπηρεσιών. Τι γίνετε στις περιπτώσεις στις οποίες ένας server μπορεί να πέσει λόγω μιας διαδικτυακής επίθεσης, είτε λόγω λάθους στο λογισμικό, είτε λόγω δύναμη ή άλλων προβλημάτων.

1.3 Η Τεχνολογία Blockchain

1.3.1 Η Τεχνολογία Blockchain

Την τελευταία δεκαετία, η τεχνολογία Blockchain γίνεται μέρα με την μέρα όλο και πιο δημοφιλής. Ο όρος Blockchain, αν και ήδη γνωστός πριν το 2009, απέκτησε νέα ισχύ με την εμφάνιση του πρώτου μπλοκ (genesis block) του Bitcoin. Λίγους μήνες νωρίτερα δημοσιεύτηκε για πρώτη φορά το άρθρο "Bitcoin: A Peer-to-Peer Electronic Cash System" [6] του Satoshi Nakamoto και με αυτό έγινε η αρχή από την οποία τα κρυπτονομίσματα απέκτησαν σημαντικό ρόλο στις οικονομικές και τεχνολογικές εξελίξεις.

Το Blockchain ανήκει στην οικογένεια των Distributed Ledger Technologies (DLT). Πρόκειται για ένα τύπο κατανεμημένου δικτύου, το οποπίο επιτρέπει την αποθήκευση ταξινομημένων εγγραφών, ονομαζόμενα και ως ‘μπλοκς’, τα οποία συνδέονται με την χρήση τεχνικών κρυπτογράφησης (για παράδειγμα, στην περίπτωση του Bitcoin κάθε μπλοκ περιέχει μια λίστα συναλλαγών). Η συγκεκριμένη τεχνολογία εφαρμόζεται σε δίκτυα ομότιμων κόμβων (Peer-to-Peer Networks), στα οποία επιτρέπεται ο ισοδύναμος διαμοιρασμός πόρων μεταξύ των κόμβων του δικτύου. Ένα κατανεμημένο δίκτυο είναι ένα δίκτυο στο οποίο τυχόν ενημερώσεις, το λογισμικό και τα δεδομένα του διανέμονται σε περισσότερους από έναν υπολογιστές, οι οποίοι επικοινωνούν μεταξύ τους και εξαρτώνται ο ένας από τον άλλο.

Βασικό χαρακτηριστικό της τεχνολογίας Blockchain είναι το κατανεμημένο κατάστιχο (Distributed ledger), στο οποίο καταγράφονται όλες οι πιστοποιημένες συναλλαγές που έχουν συμβεί στο δίκτυο. Ονομάζεται κατανεμημένο επειδή δεν είναι αποθηκευμένο σε κάποια κεντρική μνήμη, αλλά κατανέμεται σε ένα δίκτυο υπολογιστών.

Ο βασικός στόχος ενός κατανεμημένου δικτύου είναι διαμοιράσει πόρους για να επιτύχει ένα κοινό στόχο. Για την επίτευξη αυτού του κοινού στόχου σε ένα δίκτυο το οποίο χρησιμοποιεί την τεχνολογία Blockchain, είναι απαραίτητο να υπάρξει μια συνεργασία με υπάρχοντες τεχνολογίες που βρίσκονται στην αγορά. Για παράδειγμα, το Bitcoin είναι ένα παράδειγμα τεχνολογίας Blockchain το οποίο συνδυάζει υπάρχοντες τεχνολογίες ώστε να επιτύχει τον σκοπό του. Για να λειτουργήσει ένα σύστημα το οποίο διαχειρίζεται ηλεκτρονικά χρήματα, χωρίς οποιαδήποτε κεντρική αρχή, είναι απαραίτητο να θεσπιστούν μέτρα για την πρόληψη διάφορων καταστάσεων όπως η πλαστογράφηση δεδομένων, και περιπτώσεις διπλών πληρωμών. Πολύ σημαντικό αποτελεί και το θέμα διατήρησης των δεδομένων ενός συστήματος από κακόβουλες επιθέσεις.

Σε ένα Blockchain, υπάρχουν οι απλοί χρήστες και οι επικυρωτές (miners). Ένας απλός χρήστης στέλνει αίτημα για μια νέα συναλλαγή. Η συναλλαγή διαδίδεται στους miners, και ελέγχεται κατά πόσο είναι έγκυρη (πάντα με βάση τους κανόνες του δικτύου). Τότε οι miners επιτρέπουν την εισαγωγή της συγκεκριμένης συναλλαγής στο δίκτυο. Ο ρόλος ενός miner, είναι επαληθεύσει την εγκυρότητα μιας συναλλαγής, να συγκεντρώσει τις διάφορες συναλλαγές σε πακέτα (μπλοκς), και παράλληλα να κάνει τις απαραίτητες εργασίες ώστε να δημιουργήσει νέα μπλοκ για νέες συναλλαγές. Αυτές οι εργασίες εξαρτώνται από τον αλγόριθμο συναίνεσης που χρησιμοποιεί το δίκτυο. Όταν λοιπόν δημιουργηθεί ένα νέο μπλοκ, τότε καταγράφεται στο κατανεμημένο κατάστιχο η νέα εισαγωγή, και στην συνέχεια η διαδίδεται στους χρήστες του δικτύου [18].

1.3.2 Τα βασικά χαρακτηριστικά της Blockchain

1.3.2.1 Δίκτυα υπολογιστών Peer to peer (P2P)

Η δομή ενός κανονικού δικτύου είναι η δομή client-server. Οποιοσδήποτε χρειαστεί να επικοινωνήσει με τον server, μπορεί να στείλει ένα query για να πάρει τις πληροφορίες που χρειάζεται. Το πρόβλημα στο μοντέλο αυτό είναι ότι όλα εξαρτώνται από τον κεντρικό server. Αν για κάποιον λόγο, ο κεντρικός server σταματήσει να λειτουργεί, τότε χάνετε η ευκαιρία πρόσβασης στις πληροφορίες. Επιπλέον ο server, ως απόλυτη αρχή, μπορεί να αποφασίζει τι είναι και τι δεν είναι αποδεκτό για το δίκτυο.

Ένα από τα σημαντικότερα χαρακτηριστικά της τεχνολογίας Blockchain, είναι ότι εφαρμόζεται σε αποκεντρωμένα δίκτυα (Peer-to-peer networks). Ένα αποκεντρωμένο δίκτυο είναι ένα δίκτυο στο οποίο δεν υπάρχει κεντρική αρχή, η οποία ορίζει και ελέγχει τα μηνύματα και τις λειτουργίες των μελών του δικτύου. Επιπλέον σε ένα δίκτυο peer-to-peer, όλες οι διεργασίες γίνονται σε συνεργασία μεταξύ των συμμετεχόντων (peers) που διατηρούν το δίκτυο. Οι συμμετέχοντες, καλούνται τερματικά ή πιο απλά κόμβοι. Κάθε κόμβος μπορεί γενικά να ενεργεί ως σημείο εισόδου για αρκετούς διαφορετικούς χρήστες στο δίκτυο Blockchain, και υποθέτουμε ότι κάθε χρήστης πραγματοποιεί συναλλαγές σε ένα δίκτυο, μέσω του δικού του κόμβου [20].

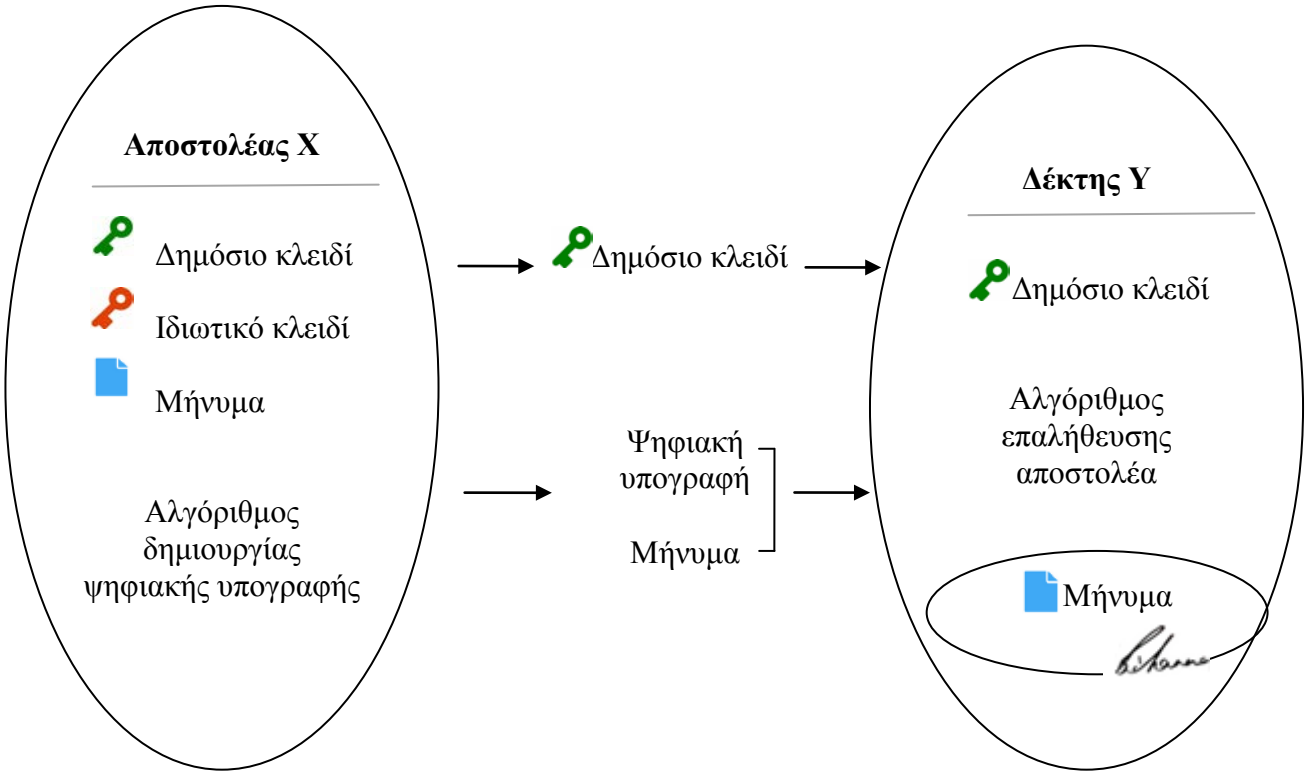
1.3.2.2 Hash code – Hash function

Ένα συνάρτηση κατακερματισμού hash, είναι ένας μηχανισμός ο οποίος χρησιμοποιείτε για τον έλεγχο παραποίησης δεδομένων. Το hash function, είναι ένας μαθηματικός αλγόριθμος ο οποίος δέχεται μία είσοδο, και την μετατρέπει σε έξοδο. Ο κωδικός hash είναι το αποτέλεσμα αυτής της μετατροπής της αρχικής πληροφορίας η οποία δόθηκε ως είσοδος. Ένα από τα μεγαλύτερα πλεονεκτήματα της συνάρτησης κατακερματισμού είναι η ανοχή σε συγκρούσεις, το οποίο σημαίνει ότι είναι αρκετά δύσκολο να αναδημιουργηθεί η αρχική πληροφορία συνεπώς και η τιμή εξόδου η οποία παράγεται από την συνάρτηση κρυπτογράφησης. Ένα από τα σημαντικότερα χαρακτηριστικά του συγκεκριμένου μηχανισμού, είναι ότι όταν λαμβάνεται η ίδια τιμή κατακερματισμού, ακόμη και μια μικρή διαφορά στα αρχικά δεδομένα θα έχουν ως αποτέλεσμα μια εντελώς διαφορετική τιμή κατακερματισμού.

1.3.2.3 Κρυπτογραφία δημόσιου κλειδιού – ψηφιακές υπογραφές

Κάθε χρήστης του Διαδικτύου, έχει την δυνατότητα αλληλεπίδρασης με το Blockchain, μέσω της χρήσης τεχνικών κρυπτογράφησης δημόσιου κλειδιού και των ψηφιακών υπογραφών. Η κρυπτογράφηση δημόσιου κλειδιού, είναι μία μέθοδος κρυπτογράφησης η οποία χρησιμοποιεί δύο διαφορετικά κλειδιά για την διαδικασία

κρυπτογράφησης και αποκρυπτογράφησης δεδομένων. Το πρόβλημα διαχείρισης των κλειδιών που ανήκουν σε ένα χρήστη, έχει επιλυθεί με την χρήση ενός ζεύγους κλειδιών, το δημόσιο και το ιδιωτικό κλειδί (public – private key). Το δημόσιο κλειδί είναι διαθέσιμο προς όλους, δηλαδή σε οποιοσδήποτε έγκυρο χρήστη του δικτύου. Επίσης μόνο ο ίδιος ο χρήστης, μπορεί να διαχειριστεί το ιδιωτικό του κλειδί. Η κρυπτογραφία δημόσιου κλειδιού επιτρέπει την ασφαλή διανομή και λήψη δεδομένων, μόνο όταν ο αποστολέας στείλει το δημόσιο κλειδί του, την ψηφιακή υπογραφή του και το μήνυμα που θέλει να στείλει. Αφού επικυρωθεί το συγκεκριμένο μήνυμα από το δίκτυο, τότε ο δέκτης του μηνύματος, χρησιμοποιεί τον αλγόριθμο επαλήθευσης, ώστε να ελέγξει εάν το μήνυμα που έχει λάβει, έχει όντως σταλεί από έγκυρο κόμβο του δικτύου. Η ασφάλεια μπορεί να διατηρηθεί, ακόμη και αν και άλλοι χρήστες του δικτύου έχουν στην διάθεση τους δημόσιο κλειδί, όσο ο δέκτης διαφυλάσσει το ιδιωτικό κλειδί του.

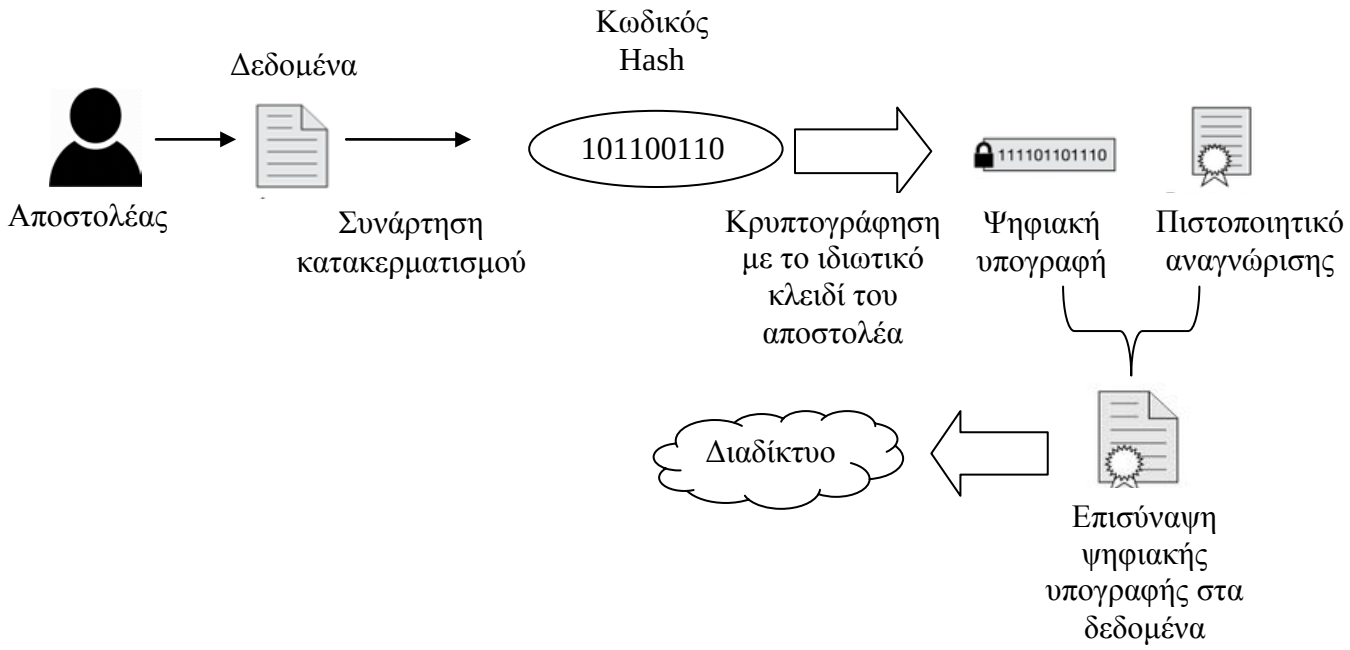


Οι ψηφιακές υπογραφές, είναι ο μηχανισμός ο οποίος χρησιμοποιείτε για την απόδειξη της γνησιότητας των δεδομένων τα οποία στέλνονται μέσα σε ένα δίκτυο, καθώς και την επαλήθευση της εγκυρότητας μιας συναλλαγής. Στην περίπτωση επικοινωνίας δύο μερών, αποστέλλεται η ψηφιακή υπογραφή του αποστολέα μαζί με τα σχετικά αρχεία. Στην συνέχεια γίνεται κρυπτογράφηση των αρχείων που πρόκειται να σταλούν, μαζί με

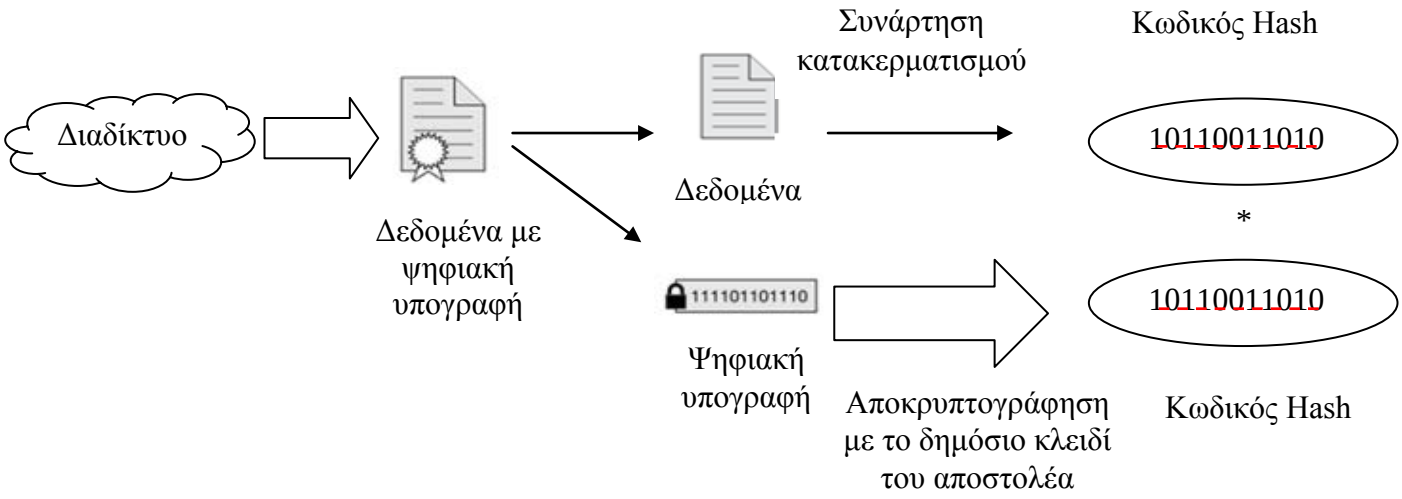
το ιδιωτικό κλειδί του αποστολέα. Ο δέκτης χρησιμοποιεί τον ίδιο κωδικό hash ως αποστολέας για να δημιουργήσει την τιμή κατακερματισμού του αρχείου, και ελέγχει την τιμή κατακερματισμού που έχει δημιουργηθεί με την τιμή κατακερματισμού που έχει παραλάβει μέσω αποκρυπτογράφησης της ψηφιακής υπογραφής του αποστολέα με το δημόσιο κλειδί του αποστολέα. Έτσι επιβεβαιώνετε ότι η ψηφιακή υπογραφή του αποστολέα, είναι αυθεντική.

Όταν κάποιος χρήστης επιθυμεί να εκτελέσει μια συναλλαγή, θα στείλει το αντίστοιχο αίτημα στο δίκτυο. Όταν μία συναλλαγή, 'υπογραφεί' με την ψηφιακή υπογραφή του χρήστη, τότε η συναλλαγή μεταδίδεται, στους γειτονικούς κόμβους, μέχρις ότου να ενημερωθούν όλοι οι κόμβοι του δικτύου για την συγκεκριμένη συναλλαγή. Η χρήση τεχνικών ασύμμετρης κρυπτογράφησης είναι μια πολύ καλή πρόταση για την εξασφάλιση της αυθεντικότητας και ακεραιότητας των δεδομένων. Η τεχνολογία Blockchain χρησιμοποιεί ένα μηχανισμό ασύμμετρης κρυπτογράφησης, ο οποίος είναι υπεύθυνος για την επικύρωση και έλεγχο των συναλλαγών.

Τα τερματικά του δικτύου ενημερώνονται για τις νέες συναλλαγές που προκύπτουν, και πρέπει να επιβεβαιώσουν ότι ανταποκρίνονται στα χαρακτηριστικά έγκυρων συναλλαγών. Εφόσον μια συναλλαγή θεωρηθεί έγκυρη και επικυρωθεί από το δίκτυο, τότε μπορεί να εισαχθεί σε ένα μπλοκ μαζί με άλλες. Το δίκτυο αποφασίζει ποιες συναλλαγές είναι έγκυρες, και τότε τις ταξινομεί και τις εισάγει σε ένα μοναδικό μπλοκ, το οποίο είναι προτεινόμενο για να μπει στην αλυσίδα. Σε ένα αποκεντρωμένο δίκτυο, οι αποφάσεις κατά την λειτουργία, οι αλλαγές ή οτιδήποτε άλλο προκύψει, λαμβάνονται από τους χρήστες που διατηρούν το δίκτυο (miners). Για το λόγο αυτό είναι σημαντικό να υπάρχει μια καλά ορισμένη διαδικασία, που οδηγεί τους miners στη λήψη μιας κοινής απόφασης. Η επιλογή των κόμβων αυτών (miners), βασίζεται στον αλγόριθμο συναίνεσης ο οποίος χρησιμοποιείτε από το δίκτυο. Επίσης, η επιλογή αυτή, κρίνεται σημαντική ώστε να αντιμετωπιστούν οι περιπτώσεις καθυστέρησης. Ωστόσο, ο στόχος παραμένει όλοι οι κόμβοι να έχουν τελικά στην μνήμη τους ένα ενημερωμένο αντίγραφο της αλυσίδας Blockchain. Για άλλη μια φορά η σημασία του αλγόριθμου συναίνεσης είναι ξεκάθαρη. Εάν όλες οι συναλλαγές που περιέχονται στο προτεινόμενο μπλοκ είναι έγκυρες, και κάθε μπλόκ αναφέρεται στο κωδικό hash του προηγούμενου μπλοκ της αλυσίδας, τότε αποφασίζεται ότι το μπλοκ είναι έγκυρο, και εισάγεται στο Blockchain. Σε αντίθετη περίπτωση, τότε η συναλλαγή απορρίπτεται.



Σχήμα 1.5: Διαδικασία δημιουργίας ψηφιακής υπογραφής [Προσαρμοσμένο από 80].



Σχήμα 1.6: Διαδικασία επαλήθευσης [Προσαρμοσμένο από 80].

1.3.2.4 Μηχανισμός συναίνεσης (Consensus mechanisms)

Το πρόβλημα της συναίνεσης, είναι ένα από τα προβλήματα που απασχολούν αρκετά χρόνια τον χώρο της κρυπτογραφίας και αρκετοί αλγόριθμοι έχουν προταθεί για την επίλυση του. Ένας αλγόριθμος συναίνεσης είναι μια διαδικασία που χρησιμοποιείται για να επιτευχθεί συμφωνία σε μια κοινή τιμή δεδομένων μεταξύ των

υπολογιστών ενός κατανεμημένου δικτύου. Οι αλγόριθμοι συναίνεσης έχουν σχεδιαστεί για να επιτυγχάνουν αξιοπιστία σε ένα δίκτυο που περιλαμβάνει πολλαπλούς κόμβους, όπου δεν υπάρχει απαραίτητα εμπιστοσύνη μεταξύ τους. Αναξιόπιστοι κόμβοι θεωρούνται αυτοί οι οποίοι δεν ακολουθούν αυστηρά τον αλγόριθμο συναίνεσης είτε γιατί έχουν κακόβουλες προθέσεις και προσπαθούν να επηρεάσουν το υπόλοιπο δίκτυο ώστε να πετύχουν κάποιο δικό τους σκοπό είτε γιατί αντιμετωπίζουν προβλήματα και δεν μπορούν να ακολουθήσουν τον αλγόριθμο (για παράδειγμα, δεν λαμβάνουν μηνύματα των άλλων κόμβων ή δεν απαντούν σε αυτά). [12,17,18,26,28]

Το κλειδί για τη λειτουργία ενός κατανεμημένου ledger, είναι να διασφαλιστεί ότι το σύνολο miners που υπάρχουν στο δίκτυο, συμφωνούν συλλογικά με το περιεχόμενο του. Αυτό είναι η δουλειά του αλγόριθμου συναίνεσης. Ειδικότερα, το δίκτυο Blockchain, είναι ένα σύνολο από κόμβους, τους οποίους χρησιμοποιούν οι χρήστες του δικτύου, και κάθε ένας από αυτούς κατέχει ένα μοναδικό αντίγραφο της εικόνας του δικτύου. Με απλά λόγια μπορούμε να υποθέσουμε ότι, το Blockchain είναι ένα κοινό ημερολόγιο μεταξύ μιας ομάδας ανθρώπων, στο οποίο καταγράφονται όλα τα γεγονότα που αφορούν την δραστηριότητα των ατόμων αυτών [12]. Το Πρωτόκολλο συναίνεσης (Consensus protocol), είναι ένας μηχανισμός ο οποίος χρησιμοποιείτε για την πιστοποίηση των χρηστών ενός δικτύου, και εξασφαλίζει ότι ακολουθούν σωστά τους κανονισμούς του δικτύου, οι οποίοι έχουν προκαθοριστεί σε προηγούμενη φάση. Επίσης, επαληθεύεται ότι οι συναλλαγές που περιέχονται σε κάθε προτεινόμενο μπλοκ (στην διαδικασία εξόρυξης), έχουν εισαχθεί με σωστή χρονολογική σειρά. Επιπλέον, χρησιμοποιείτε ώστε να επιβεβαιωθεί ότι κάθε πληροφορία που εισέρχεται σε ένα μπλοκ είναι ορθή, και ότι οι miners παίρνουν δίκαιη αποζημίωση για την επίλυση ανάλογων προβλημάτων. Η κυριότερη δυσκολία της τεχνολογίας Blockchain, είναι να επιβεβαιωθεί κατά πόσο το πρωτόκολλο συναίνεσης, χρησιμοποιείτε σωστά από τους χρήστες οι οποίοι είναι εγγεγραμμένοι σε ένα δίκτυο (P2P).

Στις δύο πιο κάτω προσεγγίσεις χρησιμοποιείτε μια διαδικασία εκλογής, μεταξύ ενός συνόλου γνωστών τερματικών του δικτύου, για την επίτευξη της συναίνεσης. Το τερματικό το οποίο θα επιλεγεί, τείνει να πληροί συγκεκριμένα χαρακτηριστικά τα οποία έχουν καθοριστεί και συνεπάγεται ότι θα είναι ένας έγκυρος χρήστης του δικτύου.

- “Nakamoto consensus” and the Byzantine Fault Tolerance (BFT).

Αυτή η προσέγγιση επιλέγει ένα «αρχηγό», μέσω μιας διαδικασία επιλογής γνωστού συγκεκριμένου τερματικού από το δίκτυο, το οποίο έχει την δυνατότητα να προτείνει κάποιο μπλοκ το οποίο θα μπορούσε να εισαχθεί στην ‘αλυσίδα των μπλοκ’ τα οποία έχουν εισαχθεί σε προηγούμενη φάση.

- Byzantine Fault Tolerance (BFT).

Στην συγκεκριμένη προσέγγιση χρησιμοποιούνται πολλαπλοί κύκλοι ώστε να επιλεγεί το καταλληλότερο επίπεδο συναίνεσης του δικτύου. Αυτή η προσέγγιση, δεν ενδείκνυται να είναι η καταλληλότερη επιλογή για το Internet of Things.

Η προσέγγιση που ενδείκνυται για το IoT είναι η επιλογή ενός μηχανισμού, ο οποίος θα παίρνει σχετικά γρήγορες αποφάσεις, ώστε να μην καθυστερεί οποιαδήποτε άλλη διαδικασία στο δίκτυο που τυχόν επηρεάζετε. Επίσης χρησιμοποιούνται μηχανισμοί οι οποίοι θα εκτελούν ελέγχους σε μεταγενέστερο στάδιο, στο οποίο θα μελετηθεί αν οι αποφάσεις οι οποίες έχουν παρθεί, έχουν προκαλέσει κάποιο σφάλμα είτε πρόβλημα.

1.3.2.4.1 Proof-of-Work (PoW)

Το Proof-of-Work είναι ένα πρωτόκολλο που έχει ως κύριο στόχο την αποτροπή επιθέσεων στον κυβερνοχώρο. Αυτές οι επιθέσεις από κακόβουλους χρήστες περιλαμβάνουν συνήθως την αποστολή πολλών μηνυμάτων ανεπιθύμητης αλληλογραφίας ή επιθέσεις άρνησης εξυπηρέτησης (επιθέσεις DDoS), οι οποίες καταστρέφουν τους υπολογιστικούς πόρους των χρηστών, προκαλώντας έτσι την επιβράδυνση των υπολογιστών τους. Η ιδέα του PoW δημοσιεύθηκε αρχικά από τους Cynthia Dwork και Moni Naor το 1993, αλλά ο όρος proof-of-work δημιουργήθηκε από τους Markus Jakobsson και Ari Juels και εμφανίστηκε δημόσια το 1999. Στο άρθρο [35] παρουσιάζεται ένας τρόπος με τον οποίο θα μπορούσε να διασφαλιστεί η εμπιστοσύνη μεταξύ των χρηστών του δικτύου. Πιο συγκεκριμένα κάθε χρήστης του δικτύου καλείτε να συμμετέχει στην διαδικασία συναίνεσης και έτσι με την απόφαση τους, θα κριθεί κατά πόσο μία συναλλαγή θα συμπεριληφθεί σε ένα μπλοκ. Αφού όλοι

οι χρήστες ψηφίσουν για το ποιες συναλλαγές πρέπει να συμπεριλήφθην στο επόμενο μπλοκ, τότε το σύνολο των συναλλαγών με τις περισσότερες ψήφους θα μπορούσαν να εισαχθούν.

Μέσα από μελέτες οι οποίες έχουν γίνει, αυτή η διαδικασία συναίνεσης, έχει κριθεί ευάλωτη σε επιθέσεις και συγκεκριμένα τις επιθέσεις Sybil, στις οποίες ένας χρήστης θα μπορούσε να δημιουργήσει πολλούς λογαριασμούς, και έτσι θα αποκτήσει μεγαλύτερη επιρροή εντός του δικτύου. Αποδείχθηκε ότι η συγκεκριμένη λύση δεν ήταν τόσο αποδοτική.

Στην συνέχεια, ο δημιουργός του Bitcoin (2009) Satoshi Nakamoto (ο οποίος ακόμα δεν γνωρίζουμε ποιος είναι), προτείνει την προσθήκη κόστους σε κάθε συναλλαγή. Συγκεκριμένα, το κόστος καθορίζεται από την επιρροή κάθε χρήστη, δηλαδή την ποσότητα ενέργειας, υπό την μορφή υπολογιστικής ισχύς στην οποία έχει πρόσβαση ένας χρήστης. Αυτό σημαίνει ότι όσο μεγαλύτερη είναι η υπολογιστική δύναμη του χρήστη, τόσο περισσότερη θα είναι η αναγκαία ενέργεια, και τόσο ψηλό θα είναι και το κόστος στο υλικό. Έτσι, με αυτό τον τρόπο αναμενόταν η επίτευξη των επιθυμητών επιπέδων συναίνεσης μεταξύ πολλών κόμβων σε ένα δίκτυο, και επίσης είναι ο τρόπος με τον οποίο διασφαλίζονται τα δεδομένα του. Ο Satoshi Nakamoto εφάρμοσε αυτήν την τεχνική στο δικό του/της ψηφιακό νόμισμα δημιουργώντας έτσι μια επανάσταση στον τρόπο που γίνονται οι συναλλαγές. Ένα κατανεμημένο σύστημα συναίνεσης χωρίς εμπιστοσύνη, σημαίνει ότι εάν ένας χρήστης θέλει είτε να στείλει, είτε να λάβει χρήματα από κάποιον, δεν χρειάζεται να εμπιστευτεί οποιοδήποτε τρίτο.

Όπως λέει και το όνομα του, το proof of work είναι ένα πρωτόκολλο που απαιτεί να αποδειχθεί ότι αυτός που εκτελεί το πρωτόκολλο έχει καταβάλει ορισμένη προσπάθεια (ή εργασία). Για να κατανοήσουμε πώς λειτουργεί με απλούς όρους, υποθέτουμε ότι βρισκόμαστε σε εξετάσεις μαθηματικών μαζί με άλλους μαθητές σε μια τάξη. Ο μαθητής που μπορεί όχι μόνο να βρει τη σωστή απάντηση αλλά και να βρει την πλήρη απόδειξη για να φτάσει στη σωστή απάντηση παίρνει πρώτος την ανταμοιβή. Όπως γνωρίζουμε αυτό απαιτεί ο συγκεκριμένος μαθητής να καταβάλει σκέψη (εγκεφαλική δύναμη), κάτι φυσικά καταναλώνει πολλή ενέργεια από το σώμα του. Στον κόσμο του Blockchain, μαθηματική εξέταση αντιστοιχεί σε ένα νέο block, ο κάθε μαθητής είναι ένας κόμβος τους δικτύου και η σκέψη που καταβάλει είναι η υπολογιστική δύναμη κάθε υπολογιστή, ενώ η ενέργεια του αντιστοιχείτε στην ηλεκτρική ενέργεια που απαιτείται για να εκτελέσει ο υπολογιστής συγκεκριμένους υπολογισμούς.

Στο πρωτόκολλο proof-of-work, κάθε επικυρωτής καλείται είτε να επιλύσει ένα μαθηματικό πρόβλημα, είτε να εκτελέσει μία συγκεκριμένη εργασία. Η λύση του προβλήματος αποτελεί και απόδειξη ότι ένας miner έχει καταβάλει την ανάλογη εργασία. Για παράδειγμα στην περίπτωση του Bitcoin, ένας miner λαμβάνει ένα bitcoin, ως επιβράβευση. Η επιβράβευση ενός miner σε μία τέτοια περίπτωση, εξαρτάται απ τα δεδομένα του δικτύου για το οποίο αναφερόμαστε. Επειδή η διαδικασία αυτή θυμίζει εξόρυξη διαμαντιών ονομάστηκε mining και αυτοί που την εκτελούν miners.

Η διαδικασία mining έχει όριο δυσκολίας, το οποίο καθορίζει τον ανταγωνιστικό χαρακτήρα της. Όσο αυξάνεται η υπολογιστική ισχύς στο δίκτυο, τόσο υψηλότερη είναι η παράμετρος δυσκολίας, αυξάνοντας έτσι και τον μέσο αριθμό των υπολογισμών που απαιτούνται για τη δημιουργία ενός νέου μπλοκ. Αυτό αυξάνει επίσης το κόστος της δημιουργίας μπλοκ, και αναγκάζονται οι miners να βελτιώσουν την αποδοτικότητα των υπολογιστών τους.

Σημαντικό πλεονέκτημα του proof-of-work, είναι ο ξεκάθαρος τρόπος με τον οποίο αντιμετωπίζει την δημιουργία forks (πιρουνιών) και τον κίνδυνο του double spending. Στην περίπτωση που δύο miners καταφέρουν και λύσουν ένα μαθηματικό πρόβλημα ταυτόχρονα (κάτι που λόγω της δυσκολίας τους προβλήματος συμβαίνει σπάνια), τότε στην αλυσίδα προστίθενται δύο νέα μπλοκ, δημιουργώντας έτσι ένα ‘πιρούνι’ (Έχουν εισαχθεί περισσότερες από μία συναλλαγές). Όσο το ‘πιρούνι’ συνεχίζει να υπάρχει, τότε υπάρχει η δυνατότητα να γίνει double spending, δηλαδή ένας χρήστης να ξοδέψει τα νομίσματά του δύο φορές. Αυτό ουσιαστικά σημαίνει ότι στην μία πλευρά του ‘πιρουνιού’ ο χρήστης ξοδεύει τα νομίσματά του σε μια συναλλαγή Α και στην άλλη πλευρά για μια συναλλαγή Β και με αυτό τον τρόπο ξοδεύετε διπλάσιο ποσό από αυτό που διαθέτει, πράγμα το οποίο θα κοστίσει. Συνήθως με την δημιουργία όμως του επόμενου μπλοκ, η απάτη αυτή θα αποκαλυφθεί.

Όταν ανακοινωθεί το νέο μπλοκ, θα έχει για γονέα ένα από τα δύο άκρα του ‘πιρουνιού’ και στην συγκεκριμένη πλευρά του ‘πιρουνιού’ το συνολικό μήκος της αλυσίδας θα είναι μεγαλύτερο. Ένας από τους κανόνες που ακολουθούν οι miners για να υπάρχει συναίνεση είναι να υιοθετούν πάντα την αλυσίδα με το μεγαλύτερο μήκος. Μόλις ανιχνευθεί το παρακλάδι του ‘πιρουνιού’ το οποίο είναι μεγαλύτερο, η απάτη αποκαλύπτεται. Ο μόνος τρόπος ένας κακόβουλος χρήστης να πετύχει την διπλή δαπάνη, θα ήταν να επεκτείνει παράλληλα και το άλλο παρακλάδι του πιρουνιού. Δηλαδή κάθε φορά που ένα νέο μπλοκ θα ανακοινώνεται στη μία πλευρά, τότε θα εισάγει και αυτός ένα νέο μπλόκ στην άλλη πλευρά. Αυτό όμως απαιτεί τεράστια

υπολογιστική δύναμη, ώστε να μπορεί να συναγωνιστεί όλους τους άλλους χρήστες του δικτύου, κάτι που φυσικά δεν είναι πάντα εφικτό. [13,15,22,23,27,32]

1.3.2.4.2 Proof-of-Stake (PoS)

Το πρωτόκολλο proof of stake (απόδειξη πονταρίσματος) έχει τον ίδιο σκοπό με το PoW, δηλαδή την επικύρωση των συναλλαγών και την επίτευξη συναίνεσης, ωστόσο η διαδικασία είναι αρκετά διαφορετική από αυτή του proof-of-work. Στην απόδειξη του πονταρίσματος, δεν υπάρχει μαθηματικό πρόβλημα που καλούνται να λύσουν οι miners. Μάλιστα, αντί για miners οι δημιουργοί των μπλόκς καλούνται και επικυρωτές. Ο δημιουργός ενός νέου μπλοκ επιλέγεται με ντετερμινιστικό τρόπο με βάση το ποντάρισμά του. Το ποντάρισμα είναι πόσα νομίσματα / μάρκες κατέχει κανείς. Για παράδειγμα, εάν ένα άτομο ποντάρει 10 νομίσματα και ένα άλλο ποντάρει 50 νομίσματα, το άτομο που πόνταρε 50 νομίσματα θα είναι 5 φορές πιο πιθανό να επιλεγεί ως ο επόμενος επικυρωτής.

Βασικό πλεονέκτημα του PoS είναι η υψηλότερη ενεργειακή απόδοση σε σχέση με το PoW. Όπως έχουμε αναφέρει το PoW, λόγω της διαδικασίας brute force και των τεράστιων υπολογισμών, απαιτεί μεγάλες ποσότητες ενέργειας. Χωρίς την διαδικασία mining, τα συστήματα PoS αποτελούν μια πολύ πιο οικολογική επιλογή. Επιπρόσθετα, τα κίνητρα που παρέχονται από τις παραλλαγές του πρωτοκόλλου PoS μπορούν να συμβάλουν καλύτερα στην προώθηση λειτουργικών δικτύων. Για παράδειγμα, σε ένα σύστημα βασισμένο στο PoW, ένας miner θα μπορούσε να έχει στην κατοχή του συγκεκριμένο ποσό νομισμάτων, τότε μπορεί να τα πωλήσει, με σκοπό να μεγιστοποιήσει τα δικά του κέρδη. Από την άλλη πλευρά, σε ένα σύστημα PoS, οι επικυρωτές πρέπει έχουν στην κατοχή τους το νόμισμα που υποστηρίζει το ίδιο το σύστημα.

Μια άλλη βασική διάκριση μεταξύ του PoS και του PoW είναι ότι στην απόδειξη πονταρίσματος δεν υπάρχει δημιουργία νέων νομισμάτων και συγκεκριμένα για την διαδικασία εξόρυξης. Αντ 'αυτού, όλα τα δεδομένα δημιουργούνται από την αρχή. Αυτό σημαίνει ότι οι επικυρωτές πρέπει να ανταμείβονται πλήρως μέσω των συναλλαγών, σε αντίθεση με τα νεοσύστατα κέρματα στην περίπτωση του PoW.

Οι δημιουργοί του Ethereum έχουν ανακοινώσει ότι σκοπεύουν να μεταβούν από το πρωτόκολλο PoW το οποίο χρησιμοποιείτε αυτή την στιγμή, σε ένα σύστημα PoS (Casper) [16]. Το Ethereum είναι μια πλατφόρμα ανοιχτού λογισμικού που βασίζεται

στην τεχνολογία Blockchain που επιτρέπει στους προγραμματιστές να δημιουργήσουν και να αναπτύξουν αποκεντρωμένες εφαρμογές. Στην πλατφόρμα του Ethereum, το νόμισμα ανταλλαγής μεταξύ των χρηστών είναι γνωστό και ως ‘ether’ και σύμφωνα με το white-paper στο οποίο πρώτη φορά παρουσιάστηκε το Ethereum, ο βασικός του στόχος ήταν η δημιουργία ενός εναλλακτικού πρωτοκόλλου με βάση το οποίο θα μπορούσαν να φτιαχτούν αποκεντρωμένες εφαρμογές [3]. Μία αποκεντρωμένη εφαρμογή έχει σίγουρα κάποιες απαιτήσεις και συμβιβασμούς τα οποία πρέπει να ληφθούν υπόψη. Για το λόγο αυτό, ένα από τα βασικά ζητήματα που καλούνται να αντιμετωπίσουν, είναι η λεγόμενη επίθεση "Nothing at stake".

Υπάρχουν αρκετά σενάρια στα οποία είναι πιθανόν να γίνουν επίθεσεις ρίσκου 51%. Όταν στο δίκτυο γίνετε χρήση του πρωτοκόλλου PoW, τότε σε επιθέσεις αυτού του είδους, το άτομο το οποίο εκτελεί αυτή την επίθεση, έχει στην διάθεση του περισσότερη υπολογιστική δύναμη (>του 51%), συγκριτικά με τους υπόλοιπους νόμιμους χρήστες του δικτύου. Αυτό σημαίνει ότι υπάρχει ψηλό κόστος υπολογιστικής ενέργειας για την δημιουργία ενός μπλοκ. Η μεγάλη κατανάλωση ενέργειας έχει χαρακτηριστεί από ερευνητές ως ένα ισχυρό κόστος, το οποίο επιβαρύνει σημαντικά το δίκτυο, και τους χρήστες. Για την μείωση του ρίσκου 51% επίθεσης, και την μείωση κατανάλωσης ενέργειας έχει προταθεί το πρωτόκολλο PoS.

Μια αντιμετώπιση της επίθεσης "Nothing at stake", έχει επιβληθεί σε κάθε επικυρωτή μια χρέωση η οποία θα δεσμεύεται για ένα χρονικό διάστημα. Η πιθανότητα επίθεσης 51% μειώνεται, λόγω των κερμάτων που επενδύει ο επικυρωτής στο δίκτυο. Δηλαδή, εάν κάποιος έχει το 51% της υπολογιστικής ισχύος σε ένα πρωτόκολλο PoS, πρέπει να κατέχει και το 51% ώστε να μπορεί να έχει τον έλεγχο. Αυτό το είδος επίθεσης, μπορεί να επηρεάσει την ακεραιότητα των δεδομένων. Το πρωτόκολλο Casper, μία παραλλαγή του πρωτόκολλου PoS, θα χρησιμοποιηθεί μια τέτοια λύση κατάθεσης στην οποία οι επικυρωτές θα πρέπει να υποβάλουν ένα ελάχιστο ποσό για να συμμετάσχουν στην δημιουργία των blocks. Το πρωτόκολλο έχει καθορίσει συγκεκριμένους κανόνες παραβίασης. Κατά την διάρκεια ζωής τους, γίνονται οι απαραίτητοι έλεγχοι μέσω του δικτύου, ώστε να επιβεβαιωθεί κατά πόσο οι χρήστες ακολουθούν σωστά τους κανονισμούς. Ένα εντοπιστεί ότι, ένας χρήστης παραβιάσει οποιοδήποτε κανονισμό, τότε η κατάθεση θα κατάσχεται. Με τον τρόπο αυτό οι δημιουργοί του Casper, θεωρούν ότι πλέον οι επικυρωτές έχουν κάτι να χάσουν, άρα θα ακολουθούν αυστηρά το πρωτόκολλο. [2,15,23,31]

1.3.2.4.3 Delegated Proof of Stake (DPoS) [2]

Το πρωτόκολλο DPoS αν και μοιάζει στο όνομα είναι αρκετά διαφορετικό από το PoS. Στο DPoS, όσοι έχουν νομίσματα ψηφίζουν για να εκλέξουν αντιπροσώπους επικυρωτές τους. Υπάρχουν 21-100 εκλεγμένοι αντιπρόσωποι σε ένα σύστημα DPoS κάτι που τους επιτρέπει να οργανώνονται αποτελεσματικά. Οι αντιπρόσωποι ανακατεύονται περιοδικά και τους δίνεται εντολή να παραδώσουν τα μπλοκ τους, και κάθε αντιπρόσωπος έχει συγκεκριμένο χρόνο για να τα δημοσιεύσει. Εάν κάποιος χάσει κάποιο μπλοκ, είτε δημοσιεύει μη έγκυρες συναλλαγές, οι χρήστες οι οποίοι έχουν στην κατοχή τους τα περισσότερα ποσοστά, θα τον αντικαταστήσουν μέσω ψηφοφορίας με κάποιον καλύτερο. Στο DPoS, οι miners μπορούν να συνεργάζονται για να κάνουν μπλοκ αντί να ανταγωνίζονται όπως σε PoW και PoS. Βασικό πλεονέκτημα του DPoS είναι η ταχύτητα του, ωστόσο το σύστημα αυτό είναι εν μέρει κεντροποιημένο, αφού συγκεκριμένοι χρήστες παίρνουν τις αποφάσεις και λειτουργούν σαν κεντρική αρχή, αντί οι αποφάσεις να λαμβάνονται από όλο το δίκτυο.

1.3.2.4.4 Proof-of capacity (PoC) [2]

Η απόδειξη χωρητικότητας είναι ένας μηχανισμός συναίνεσης που χρησιμοποιείται στην τεχνολογία Blockchain, το οποίο επιτρέπει στους miners να χρησιμοποιούν τον διαθέσιμο χώρο του σκληρού δίσκου για να αποφασίσουν τα δικαιώματα εξόρυξης. Ποιός δηλαδή θα επιλέξει το επόμενο μπλοκ. Το PoC προέκυψε ως μία από τις πολλές εναλλακτικές λύσεις στο πρόβλημα της υψηλής κατανάλωσης ενέργειας του PoW και στο πρόβλημα που προάγει εγγενώς το PoS, την αποθήκευσή εξουσίας, αντί για την δαπάνη της. Η απόδειξη της χωρητικότητας επιτρέπει στους miners να χρησιμοποιούν τον διαθέσιμο χώρο στο σκληρό δίσκο τους για να εξορύξουν για παράδειγμα τα διαθέσιμα κρυπτονομίσματα. Ένας miner αντί να δοκιμάζει επανειλημμένα τιμές μέχρι να βρει την κατάλληλη τιμή για την κεφαλίδα του μπλοκ, αποθηκεύει μια λίστα με πιθανές λύσεις σε ένα σκληρό δίσκο ώστε να τις έχει στην διάθεση του πριν αρχίσει τη διαδικασία εξόρυξης. Όσο μεγαλύτερος είναι ο σκληρός δίσκος, τόσο περισσότερες είναι οι πιθανές τιμές λύσης που μπορεί να αποθηκεύσει και με αυτόν τον τρόπο, ένας miner έχει περισσότερες πιθανότητες να κερδίσει την ανταμοιβή εξόρυξης.

1.3.2.4.5 Proof-of-Weight (PoWeight) [2]

Η απόδειξη βάρους ανήκεις την κατηγορία αλγορίθμων συναίνεσης οι οποίοι βασίζονται στο μοντέλο συναίνεσης του Algorand. Η γενική ιδέα είναι ότι όπως στο PoS το ποσοστό των μαρκών κατέχει κάποιος στο δίκτυο αντιπροσωπεύει την πιθανότητα να δημοσιεύσει αυτός το επόμενο μπλόκ, σε ένα σύστημα PoWeight χρησιμοποιείται κάποια άλλη τιμή (κάποιο άλλο βάρος). Για παράδειγμα το Proof-of-Spacetime του Filecoin χρησιμοποιεί το μέγεθος των δεδομένων που αποθηκεύει ο χρήστης σε ένα κατανεμημένο σύστημα διαχείρισης αρχείων.

1.3.2.4.6 Practical Byzantine Fault Tolerance (PBFT) [2]

Το πρωτόκολλο PBFT προσπαθεί να επιλύσει το πρόβλημα γνωστό ως Byzantine Agreement, μια παραλλαγή του προβλήματος συναίνεσης. Το πρόβλημα είναι το εξής : αρκετοί βυζαντινοί στρατηγοί και οι αντίστοιχες μερίδες του βυζαντινού στρατού περιβάλλουν μια πόλη. Πρέπει να αποφασίσουν από κοινού εάν θα επιτεθούν ή όχι. Αν ορισμένοι στρατηγοί επιτεθούν χωρίς τους άλλους, η πολιορκία τους θα τελειώσει σε τραγωδία. Οι στρατηγοί συνήθως διαχωρίζονται από απόσταση και πρέπει να ανταλλάξουν μηνύματα για να επικοινωνήσουν, μέχρι να καταλήξουν σε ένα κοινό τρόπο επίθεσης.

Αρκετά πρωτόκολλα κρυπτονομισμάτων χρησιμοποιούν έκδοση του BFT για να καταλήξουν σε συναίνεση, όπου το κάθε ένα έχει τα πλεονεκτήματα και τα μειονεκτήματά του. Από τα πιο διαδεδομένα σε αυτή την κατηγορία είναι το PBFT το οποίο αυτή τη στιγμή που χρησιμοποιείται από το Hyperledger Fabric, με λίγους προεπιλεγμένους στρατηγούς. Ένα άλλο πρωτόκολλο που προσπαθεί να επιλύσει το Byzantine Agreement είναι το Fedetated Byzantine Agreement (Ομοσπονδιακή Βυζαντινή Συμφωνία ή FBA). Το FBA είναι μια άλλη κατηγορία λύσεων για το πρόβλημα των βυζαντινών στρατηγών (Ripple, Stellar). Η γενική ιδέα είναι ότι κάθε βυζαντινός στρατηγός είναι υπεύθυνος για τη δική του αλυσίδα και ταξινομεί τις συναλλαγές και τα μηνύματα βάση χρονολογικής σειράς ώστε να καταλήξει σε μια αλήθεια. Στο Ripple, όπου χρησιμοποιείται το FBA οι στρατηγοί (επικυρωτές) προεπιλέγονται από το ίδρυμα Ripple, άρα είναι εν μέρη κεντροποιημένο σύστημα. Μια ακόμη εφαρμογή του FBA συναντάμε στο Stellar, όπου ο καθένας μπορεί να είναι ένας επικυρωτής, και κάθε χρήστης καλείται να επιλέξει ποιους θα εμπιστευτεί.

	PoW	PoS	PBFT	DPoS	Ripple	Tendermint
Διαχείριση ταυτοτήτων των κόμβων του δικτύου	Ανοικτό	Ανοικτό	Χρειάζεται άδεια	Ανοικτό	Ανοικτό	Χρειάζεται άδεια
Ανοχή ενέργειας του αντιπάλου	<25,0% υπολογιστική δύναμη	<51,0% stake	<33.3% fault replicas	<51,0% validators	<20,0% οι κόμβοι αποτελούν σημείο αποτυχίας	<33.3% ενέργεια από την διαδικασία συναίνεσης
Εξοικονόμηση ενέργειας	Όχι	Μερική	Ναι	Μερική	Ναι	Ναι
Εφαρμογές / Πλατφόρμες στις οποίες χρησιμοποιείται	Bitcoin	Etherum	Hyperledger Fabric	Bitshares	Ripple	Tendermint

Σχήμα 1.7: Αλγόριθμοι Συναίνεσης.

1.3.3 Η δομή δεδομένων Blockchain

Η δομή δεδομένων Blockchain είναι μια αναδρομικά συνδεδεμένη "αλυσίδα" από ‘μπλόκς’ (μια "αλυσίδα", η οποία μπορεί να αποθηκευτεί ως μια απλή βάση δεδομένων). Κάθε μπλοκ το οποίο ανήκει στην αλυσίδα, χαρακτηρίζεται μοναδικά από ένα μοναδικό κρυπτογραφημένο κωδικό hash. Τα ‘μπλόκς’ συνδέονται μεταξύ τους προς τα "πίσω", το καθένα αναφερόμενο στο προηγούμενο ‘μπλόκ’ της αλυσίδας [18].

Κάθε μπλοκ της αλυσίδας περιέχει το μέγεθος του μπλοκ, την κεφαλίδα (block header), τον κωδικό hash του προηγούμενου μπλοκ στην σειρά, χρονοσήμανση (αφορά τον χρόνο δημιουργίας του συγκεκριμένου μπλοκ), και δεδομένα σχετικά με τις συναλλαγές οι οποίες αντιστοιχούν στο συγκεκριμένο μπλοκ. Κάθε κόμβος ο οποίος έχει πρόσβαση σε αυτή την αλυσίδα εγγραφών, μπορεί να τις διαβάσει πληροφορίες για κάθε συναλλαγή, και ποια ήταν ακριβώς η ροή δεδομένων στο δίκτυο.

Ένα ‘μπλόκ’ χαρακτηρίζεται μοναδικά από ένα κωδικό hash, που παράγεται με τη χρήση του αλγόριθμου κρυπτογράφησης SHA-256 (Secure Hash Algorithm 256)

στην κεφαλίδα κάθε μπλοκ. Επίσης περιέχει ένα hash pointer, ο οποίος δείχνει στο προηγούμενο μπλοκ (γονικό μπλοκ) στην σειρά της αλυσίδας, ένα μετρητή (counter) που εκφράζει το πλήθος των μπλοκ στη λίστα και φυσικά την λίστα των συναλλαγών που έχουν καταχωρηθεί. Ο hash pointer περιέχει την διεύθυνση του προηγούμενου μπλοκ, όπως επίσης και τον κωδικό hash των δεδομένων του προηγούμενου μπλοκ. Αυτό είναι το χαρακτηριστικό το οποίο κάνει την τεχνολογία Blockchain εξαιρετικά αξιόπιστη. Το πρώτο μπλοκ της λίστας ονομάζεται "genesis block" και ο δείκτης του δείχνει έξω από το σύστημα [18].

Block X

Μέγεθος του Block:

Το μέγεθος του μπλοκ σε bytes.

Κεφαλίδα Block:

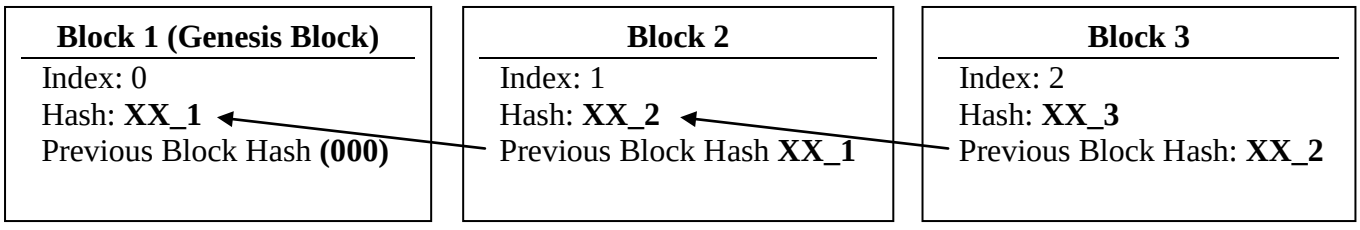
Η κεφαλίδα του μπλοκ, περιέχει τα εξής χαρακτηριστικά:

- Κωδικός hash του μπλοκ (32-byte).
- Κωδικός hash του προηγούμενου μπλοκ (32-byte).
- Ο κωδικός hash της ρίζας τν συναλλαγών που έχουν εισαχθεί σε αυτό το μπλοκ (Merkle root).
- Χρονική στιγμή δημιουργίας του μπλόκ (Timestamp).
- Επίπεδο δυσκολίας επικύρωσης του συγκεκριμένου μπλόκ (Difficulty Target).
- Τυχαίο κρυπτογραφημένο αριθμό, τον οποίο χρησιμοποιεί ο αλγόριθμος συναίνεσης (Nonce).

Συναλλαγές:

Οι συναλλαγές που έχουν καταχωρηθεί στο συγκεκριμένο μπλοκ.

Σχήμα 1.8: Η δομή ενός μπλόκ [Προσαρμοσμένο από 30].



Σχήμα 1.9: Η δομή της αλυσίδας Blockchain [Προσαρμοσμένο από 30].

Ενώ ένα ‘μπλόκ’ έχει μόνο έναν γονέα, και μπορεί προσωρινά να έχει πολλά παιδιά. Καθένα από τα παιδιά αναφέρονται στο ίδιο ‘μπλόκ’ ως γονέα και περιέχουν τον ίδιο (γονικό) hash. Πολλά παιδιά μπορεί να εμφανίζονται κατά τη διάρκεια στην περίπτωση ενός fork, μια προσωρινή κατάσταση που συμβαίνει όταν προκύπτουν ταυτόχρονα διαφορετικά νέα ‘μπλόκ’. Στην συνέχεια, μόνο ένα από τα παιδιά ‘μπλόκ’ γίνεται μέρος της αλυσίδας Blockchain, και η κατάσταση fork επιλύεται. Είναι σημαντικό να τονίσουμε ότι ακόμα κι αν ένα μπλοκ μπορεί να έχει περισσότερα από ένα παιδιά, κάθε μπλόκ μπορεί να έχει μόνο έναν γονέα. Αυτό είναι επειδή υπάρχει μόνο ένας hash pointer, ο οποίος δείχνει τον μοναδικό του γονέα [18].

Η ταυτότητα του παιδιού ‘μπλόκ’ αλλάζει αν αλλάξει η ταυτότητα του γονέα. Στην περίπτωση που τροποποιηθεί ο κωδικός hash, του γονικού μπλοκ (για παράδειγμα σε μια κακόβουλη πρόσβαση), τότε αναγκαστικά αλλάζει και ο κωδικός hash του παιδιού. Αυτό προφανώς δημιουργεί μια αλυσίδα από απαραίτητες αλλαγές στον κωδικό hash των επόμενων μπλοκ στην σειρά, και ούτω καθεξής. Αυτό σημαίνει ότι, ένα μπλοκ ακολουθείται από πολλές γενιές, και δεν μπορεί να αλλάξει χωρίς τον επαναπροσδιορισμό όλων των χαρακτηριστικών των επόμενων ‘μπλόκ’ που βρίσκονται στην αλυσίδα. Αυτή η διαδικασία, θα απαιτούσε τεράστια υπολογιστική δύναμη και το κόστος θα ήταν μεγάλο. Είναι εξαιρετικά σημαντικό, το περιεχόμενο του Blockchain να μένει αμετάβλητο, και αυτό επιτυγχάνεται με την χρήση της συνάρτησης κρυπτογράφησης (cryptographic hash function). Μια από τις πιο σημαντικές ιδιότητες της συνάρτησης κρυπτογράφησης την οποία χρειάζεται, για να είναι ασφαλής είναι η επίδραση χιονοστιβάδας (Avalanche Effect). Ακόμη και αν γίνει μια μικρή αλλαγή πάνω στην είσοδο, οι αλλαγές πάνω στο κωδικό hash θα είναι μεγάλες. Ακόμη και αν έχει αλλάξει ένα γράμμα του αλφαβήτου, ο κωδικός hash επηρεάζετε σε μεγάλο βαθμό. Έτσι θα μπορεί να γίνει αντιληπτή οποιαδήποτε κακόβουλη δράση πάνω στα δεδομένα ενός μπλοκ.

1.3.4 Τύποι Blockchain

Υπάρχουν συγκριμένοι τύποι Blockchain ανάλογα με το πώς διαχειρίζονται τα δεδομένα, τη διαθεσιμότητα τέτοιων δεδομένων και τι ενέργειες μπορούν να εκτελεστούν από έναν χρήστη. Διαχωρίζονται στις εξής κατηγορίες: Δημόσιο (public), ιδιωτικό (private) [24], και Consortium Blockchain (Blockchain κοινοπραξίας) [14]. Μία ακόμη κατηγοριοποίηση της συγκεκριμένης τεχνολογίας , είναι μεταξύ των

δικτύων των οποίων οι συμμετέχοντες χρειάζονται άδεια (permissioned Blockchain), και των δικτύων στα οποία οι συμμετέχοντες δεν χρειάζονται άδεια (permissionless Blockchain) [5,11]. Στην περίπτωση κρυπτονομισμάτων, ερευνητές χρησιμοποιούν τους όρους public/permissionless και private/ permissioned ως συνώνυμα. Ωστόσο αυτό δεν ισχύει για τις εφαρμογές του Διαδικτύου των πραγμάτων, όπου είναι σημαντικό να γίνεται διάκριση μεταξύ της ταυτότητας (ποιος μπορεί να έχει πρόσβαση στο Blockchain) και άδειας (τι μπορεί να κάνει μια συσκευή IoT χωρίς άδεια ή με άδεια).

Σε ένα δημόσιο Blockchain ο καθένας μπορεί να ενταχθεί σε αυτό χωρίς την έγκριση τρίτων και μπορεί να ενεργεί ως ένας απλός χρήστης ή ως miner ή επικυρωτής. Είναι ένα πλήρως ανοικτό public ledger, το οποίο δεν έχει καθόλου περιορισμούς σε δικαιώματα για διάβασμα είτε γράψιμο πληροφοριών στο δίκτυο. Οποιοσδήποτε μπορεί να συμμετέχει είτε να συνδεθεί στο δίκτυο, αμέσως αποκτά το δικαίωμα πρόσβασης σε πληροφορίες, όπως επίσης αποκτά και το δικαίωμα να εισάγει πληροφορίες. Οποιοσδήποτε είναι συνδεδεμένος στο δίκτυο, έχει το δικαίωμα να συμμετέχει στο πρωτόκολλο συναίνεσης, στην επικύρωση ενός νέου μπλοκ το οποίο έχει εισαχθεί, και όπως επίσης να επιβεβαιώσει ότι δεν υπάρχει κάποιο πρόβλημα με κάποιο υφιστάμενο μπλοκ το οποίο είναι ήδη μέσα στο Blockchain. Το δίκτυο έχει μια φιλοσοφία ανοικτού τύπου και η εμπιστοσύνη μεταξύ των κόμβων του δικτύου δεν είναι βασικό χαρακτηριστικό του. Στις πλείστες περιπτώσεις, ένα δημόσιο Blockchain, λειτουργεί βάση του πρωτοκόλλου PoW.

Στην περίπτωση ιδιωτικών Blockchain, υπάρχουν περιορισμοί οι οποίοι αφορούν τις δυνατότητες που έχουν οι χρήστες του δικτύου. Ο ιδιοκτήτης περιορίζει την πρόσβαση στο δίκτυο, υπάρχουν περιορισμοί σχετικά με τα δικαιώματα για διάβασμα, γράψιμο, ακόμη και δικαίωμα τροποποίησης πληροφοριών στο δίκτυο. Τα δικαιώματα που έχουν αναφερθεί, περιορίζονται σε ένα σύνολο συμμετεχόντων του δικτύου. Απαραίτητο χαρακτηριστικό το οποίο πρέπει να αναφερθεί είναι η αξιοπιστία μεταξύ των κόμβων του δικτύου. Επίσης δίνεται η δυνατότητα για γρήγορη πρόσβαση σε πληροφορίες, φθηνότερες συναλλαγές, και δίνεται η δυνατότητα ελέγχου του επιπέδου προστασίας δεδομένων στο δίκτυο. Βασικά πλεονεκτήματα του ιδιωτικού Blockchain είναι η ταχύτητα συναλλαγής που γενικά είναι ταχύτερη από το δημόσιο Blockchain, το κόστος των συναλλαγών, που είναι αρκετά μικρότερο έως και μηδενικό και η ελαστικότητα του ως προς την αλλαγή κανόνων και την τροποποίηση συναλλαγών [34]. Για παράδειγμα, συστήματα Διαχείριση Βάσεων δεδομένων, συστήματα ελέγχου διεργασιών κλπ. Συνήθως είναι συστήματα εσωτερικά σε ένα

οργανισμό, στα οποία το δικαίωμα ανάγνωσης πληροφοριών, δεν είναι ανάγκη να δοθεί σε όλους τους συμμετέχοντες του δικτύου.

Ένα Consortium Blockchain, περιλαμβάνει χαρακτηριστικά ενός δημόσιου και ενός ιδιωτικού ledger. Διαφέρουν από το δημόσιο Blockchain ακριβώς στο ότι λειτουργούν με άδεια και άρα δεν μπορεί οποιοσδήποτε με σύνδεση στο διαδίκτυο να αποκτήσει πρόσβαση σε αυτό. Πιο συγκεκριμένα, η διαδικασία συναίνεσης ελέγχεται από ένα προκαθορισμένο σύνολο χρηστών του δικτύου, και επίσης δεν επιτρέπετε σε οποιοδήποτε άτομο με πρόσβαση στο διαδίκτυο, να συμμετέχει στην διαδικασία επικύρωσης συναλλαγών. Το συγκεκριμένο δίκτυο χαρακτηρίζεται ως «μερικώς αποκεντρωμένο», αφού ο έλεγχος δεν χορηγείται σε ένα μόνο κόμβο, αλλά σε μια ομάδα προ-εγκεκριμένων κόμβων. Επιτρέπεται σε συγκεκριμένα μέλη του δικτύου να δημιουργήσουν συναλλαγές και να πάρουν αποφάσεις σχετικές με το Blockchain. Το δικαίωμα ανάγνωσης πληροφοριών που βρίσκονται στο Blockchain μπορεί να είναι δημόσιο ή να περιορίζεται στους συμμετέχοντες, το οποίο επιτρέπει σε μέλη από το δημόσιο κοινό να κάνουν έναν περιορισμένο αριθμό ερωτημάτων και να πάρουν πίσω κρυπτογραφημένες απαντήσεις, οι οποίες περιέχουν πληροφορίες οι οποίες είναι αποθηκευμένες στο Blockchain. Επίσης υπάρχον λύσεις στις οποίες τμήματα των πληροφοριών είναι δημόσια, και άλλα όχι. Παραδείγματα: R3 (χρησιμοποιούνται στον τομέα χρηματοδότησης και εμπορίου), EWF (μια πλατφόρμα ανοιχτού κώδικα με δυνατότητα επέκτασης, ειδικά σχεδιασμένη για λειτουργικές και επιχειρησιακές ανάγκες στον ενεργειακό τομέα), B3i (Ασφάλεια), πλατφόρμα Corda.

Ένα permissioned Blockchain περιορίζει τους κόμβους που μπορούν να συμβάλουν στη συναίνεση του συστήματος. Σε ένα τέτοιο Blockchain, μόνο ένα περιορισμένο σύνολο χρηστών έχει δικαίωμα να επικυρώνει συναλλαγές επίσης μπορεί να περιοριστεί η δυνατότητα δημιουργίας έξυπνων συμβολαίων μόνο σε εγκεκριμένους φορείς. Αντίθετα στο permissionless Blockchain όποιος θέλει μπορεί να ενταχθεί στο δίκτυο, να συμμετάσχει στη διαδικασία επαλήθευσης του block και να δημιουργεί έξυπνα συμβόλαια. Στο permissioneless Blockchain ένας κόμβος δεν χρειάζεται να αποδείξει την ταυτότητά του. Εφ 'όσον είναι πρόθυμος να χρησιμοποιήσει την υπολογιστική του δύναμη για να είναι μέρος του δικτύου και να επεκτείνει το Blockchain, επιτρέπεται να συμμετέχει. Στο permissioned Blockchain, ο κόμβος πρέπει να είναι εγκεκριμένος από το σύστημα για να συμμετέχει στην ανάπτυξη της αλυσίδας, και δεν έχουν όλοι οι κόμβοι πρόσβαση σε όλες τις πληροφορίες. Πολλά ιδιωτικά

Blockchain είναι και permissioned προκειμένου να ελέγχεται ποιοι χρήστες μπορούν να εκτελούν συναλλαγές, να ενεργούν ως miners στο δίκτυο κλπ.

1.3.5 Πλεονεκτήματα της τεχνολογίας Blockchain

Η τεχνολογία Blockchain, έχει βοηθήσει στην δημιουργία ισχυρών, σωστά κατανεμημένων συστημάτων, στα οποία υπάρχει ανοχή σε αποτυχίες που πιθανόν να συμβαίνουν στους κόμβους. Αυτό αποτελεί βασικό πλεονέκτημα για τα IoT δίκτυα. Επίσης, δίνετε η δυνατότητα να αναγνωρίσουν συγκρούσεις και forks, που μπορεί να υπάρξουν στο δίκτυο, και μπορούν να τα αντιμετωπίσουν αυτόματα. Έτσι δίνετε μια διεθνές αποδεκτή όψη αντιμετώπισης, συγκεκριμένων καταστάσεων στις οποίες πιθανόν να βρεθεί ένα δίκτυο.

Η Blockchain τεχνολογία επιτρέπει επίσης τη δημιουργία ασφαλών δικτύων, όπου οι συσκευές IoT θα διασυνδεθούν με αξιόπιστο τρόπο, αποφεύγοντας για παράδειγμα τις απειλές, είτε την πλαστογράφηση μίας συσκευής και κλοπή στοιχείων ταυτότητας. Δίνει δηλαδή την δυνατότητα επικοινωνίας μεταξύ δύο ή περισσότερων οντοτήτων, μεταξύ των οποίων πιθανόν να μην υπάρχει εμπιστοσύνη. Γενικότερα το Blockchain, σε συνεργασία με άλλες τεχνολογίες προσφέρουν αξιοπιστία και εμπιστοσύνη στους χρήστες του.

Προσφέρει διαφάνεια, συνέπεια και ορατότητα, στις λειτουργίες που προσφέρει. Για κάθε συναλλαγή η οποία εκτελείτε σε ένα δίκτυο αυτού του τύπου, υπάρχει απόδειξη η οποία έχει ελεγχθεί, όσο αφορά την εξουσιοδότηση της συγκεκριμένης λειτουργίας με το σύστημα.

Επίσης η τεχνολογία Blockchain προσφέρει εργαλεία πιστοποίησης ταυτότητας και εξουσιοδότησης στον ψηφιακό κόσμο. Αυτό σημαίνει ότι μειώνετε η ανάγκη για την ύπαρξη μιας κεντρικής αρχής στο δίκτυο και έτσι γίνετε εφικτή η ενεργοποίηση των ψηφιακών συσχετίσεων. Με την επισημοποίηση και την εξασφάλιση ψηφιακών σχέσεων, αυτό θα σημάνει την δημιουργία της ραχοκοκαλιάς ενός στρώματος του Διαδικτύου, για συναλλαγές και αλληλεπιδράσεις αξίας, συχνά αποκαλούμενες «Internet of Value». Πρόκειται για την χρήση της τεχνολογίας με σκοπό την βέλτιστη εμπειρία των χρηστών ενός δικτύου, ακολουθώντας συγκεκριμένες ψηφιακές στρατηγικές. Καταχωρώντας λοιπόν νόμιμα ένα κόμβο στο Blockchain, οι συσκευές θα μπορούν εύκολα να εντοπίζουν και να πραγματοποιούν αμοιβαίο έλεγχο

ταυτότητας, χωρίς την ανάγκη πιστοποίησης από κάποιο κεντρικό server. Επιπλέον το δίκτυο θα είναι επεκτάσιμο, ώστε να είναι σε θέση να υποστηρίζει δισεκατομμύρια συσκευών χωρίς την ανάγκη για πρόσθετους πόρους. Βασισμένο σε κρυπτογραφικά πρωτόκολλα, το Blockchain είναι σε θέση να προστατεύσει αποτελεσματικά την ακεραιότητα, την αυθεντικότητα, και την συνέπεια όλων των δεδομένων του δικτύου.

Επίσης έχει αποκτήσει σημαντικό ρόλο στο οικοσύστημα IoT, μειώνοντας τον χρόνο και το κόστος κάθε εργασίας και σε συνεργασία με άλλες τεχνολογίες, έχει απλοποιηθεί η διαδικασία επεξεργασίας και ανάλυσης δεδομένων. Εξασφαλίζει την ακεραιότητα των δεδομένων μέσω των αμετάβλητων εγγραφών που εισάγονται στο σύστημα, ακόμη και των ψηφιακών αναπαραστάσεων φυσικών στοιχείων.

Επιτρέπει την ανταλλαγή ψηφιακών περιουσιακών στοιχείων μεταξύ νόμιμων χρηστών του δικτύου. Οι χρήστες μπορούν να διαχειριστούν και να μεταφέρουν περιουσιακά τους στοιχεία σε πραγματικό χρόνο, χωρίς να χρειάζεται να μεσολαβήσει τράπεζα, ή χειριστές πληρωμών, ή κάποιο τρίτο πρόσωπο.

Δίνει την δυνατότητα για εκτέλεση έξυπνων συμβολαίων. Αυτοδιοικούμενα συμβόλαια τα οποία αυτοματοποιούν διαδικασίες του δικτύου. Με αυτό τον τρόπο ελέγχεται κάθε κίνηση που γίνετε στο δίκτυο, βάση των κανονισμών των οποίων έχουν ορισθεί στο συμβόλαιο του δικτύου.

1.4 Έξυπνα Συμβόλαια

Το 1994, ο Nick Szabo (νομικός και κρυπτογράφος) παρουσίασε την χρήση των έξυπνων συμβολαίων ως ένα πρωτόκολλο προγραμματισμένων λειτουργιών, το οποίο υλοποιεί όρους και προϋποθέσεις ενός συμβολαίου. Επίσης, ο Nick Szabo συνειδητοποίησε ότι το αποκεντρωμένο κατάστιχο (decentralized ledger) θα μπορούσε να χρησιμοποιηθεί για την υλοποίηση έξυπνων συμβολαίων, γι αυτό έχει προτείνει ότι, κάθε απλό συμβόλαιο θα μπορούσε να μετατραπεί σε κώδικα, ο οποίος πρόκειται να ενσωματωθεί είτε στο υλικό, είτε στο λογισμικό ενός συστήματος. Βασικός σκοπός των έξυπνων συμβολαίων, είναι η μείωση της ανάγκης έμπιστων χρηστών στο δίκτυο, όπως για την καλύτερη αντιμετώπιση κακόβουλων επιθέσεων. [26]

Στα πλαίσια της τεχνολογίας Blockchain, τα έξυπνα συμβόλαιά είναι ένα σύνολο από scripts τα οποία αποθηκεύονται στο Blockchain. Όταν ένα έξυπνο συμβόλαιο, πιστοποιηθεί από το δίκτυο, τότε το ίδιο το συμβόλαιο, αποκτά ένα μοναδικό λογαριασμό στο Blockchain. Κάθε έγκυρος χρήστης του δικτύου μπορεί να

διαβάσει την έξυπνη σύμβαση, και όταν είναι ανάγκη να ενεργοποιηθεί το συμβόλαιο, τότε στέλνεται το ανάλογο αίτημα στην διεύθυνση του στο Blockchain. Επίσης, ένα έξυπνο συμβόλαιο, περιλαμβάνει διαδικασίες οι οποίες ενεργοποιούνται βάση γεγονότων που συμβαίνουν στο δίκτυο, και στην συνέχεια οι αλλαγές, διαδίδονται εντός του δικτύου. Αυτό σημαίνει ότι κάθε κόμβος σε ένα δίκτυο BC, τρέχει ως μία εικονική μηχανή, και συνεπώς το Blockchain λειτουργεί ως μία κατανεμημένη εικονική μηχανή. Είναι η απλούστερη μορφή συστήματος αποκεντρωμένης αυτοματοποίησης διαδικασιών. Τα scripts αντιστοιχούν σε ένα σύνολο κανόνων για τους οποίους τα μέρη του δικτύου, ακόμη και εργαλεία τα οποία συνεργάζονται με το δίκτυο, συμφωνούν για την μεταξύ τους αλληλεπίδραση. Δεδομένου ότι σε κάθε συναλλαγή η οποία εκτελείτε μέσω ενός έξυπνου συμβολαίου, αντιστοιχούνται πιστοποιημένα μηνύματα τα οποία ανταλλάζονται εντός του Blockchain, κάθε χρήστης του δικτύου λαμβάνει μία έγκυρη κρυπτογραφημένη αναφορά των λειτουργιών του συμβολαίου. Κάθε έξυπνο συμβόλαιο μπορεί να κωδικοποιηθεί σε οποιοδήποτε τύπο Blockchain. [3,25]

Μια έξυπνη σύμβαση είναι ένα πρωτόκολλο, προοριζόμενο να διευκολύνει την λειτουργία κατανεμημένων δικτύων, ώστε να επαληθεύσει την εκτέλεση μιας σύμβασης. Επιτρέπουν την εκτέλεση αξιόπιστων συναλλαγών χωρίς την ανάγκη κάποιου τρίτου. Οι συναλλαγές αυτές παρακολουθούνται από το δίκτυο των υπολογιστών που τρέχουν το Blockchain και είναι μη αναστρέψιμες. Πολύ σημαντικό να αναφερθεί είναι ότι ένα έξυπνο συμβόλαιο, πρέπει να περιγράφει όλες τις πιθανές εξόδους. Επίσης ένα έξυπνο συμβόλαιο πρέπει να είναι ντετερμινιστικό, κάθε φορά που δίνετε μια συγκεκριμένη είσοδος, παράγετε μια συγκεκριμένη έξοδος.

Ανάλογα με τις λειτουργίες που υποστηρίζει το Blockchain, τότε καθορίζεται ποιος από τους χρήστες του δικτύου θα μπορούσε να αναπτύξει ένα έξυπνο συμβόλαιο. Κάθε έξυπνο συμβόλαιο, έχει την δική του κατάσταση (ένα μοναδικό λογαριασμό), και έχει την δυνατότητα να είναι ενήμερο για την κατάσταση των στοιχείων του Blockchain. Όταν το Blockchain, υποστηρίζει της συναλλαγές του Bitcoin, τότε δίνετε η δυνατότητα μεταφοράς στοιχείων μεταξύ δύο κόμβων του δικτύου. Στην περίπτωση όπου το Blockchain, υποστηρίζει έξυπνα συμβόλαια, τότε επιτρέπει διαδικασίες πολλαπλών βημάτων που συμβαίνουν μεταξύ αντισυμβαλλόμενων οντοτήτων μεταξύ των οποίων πιθανόν να μην υπάρχει εμπιστοσύνη. Αυτά που προσφέρει η συγκεκριμένη συνεργασία, είναι τα εξής. Πρόσβαση στον κώδικα , και αναγνώριση της εξόδου πριν ακόμα επικοινωνήσουν με το συμβόλαιο. Υπάρχει βεβαιότητα στην εκτέλεση της εξόδου, μιας και ο κώδικας έχει ήδη ελεγχτεί, και έχει αποθηκευτεί στο δίκτυο.

Δεδομένου ότι, σε όλες οι συναλλαγές υπάρχουν ψηφιακές υπογραφές οι οποίες ανήκουν στους χρήστες οι οποίοι λαμβάνουν μέρος στην συγκεκριμένη διαδικασία, τότε υπάρχει επαληθευσιμότητα.

Για να κατανοήσουμε καλύτερα τι είναι ένα έξυπνο συμβόλαιο, εξετάζουμε το παρακάτω παράδειγμα: Υποθέτουμε ότι θέλουμε να ενοικιάσουμε ένα διαμέρισμα το οποίο ανήκει στο άτομο Α. αυτή η απλή διαδικασία, μπορεί να γίνει μέσω του Blockchain πληρώνοντας σε κρυπτονομίσματα. Η απόδειξη μας για το ενοίκιο περιλαμβάνεται στο εικονικό συμβόλαιο και θα πρέπει να λάβουμε ένα ψηφιακό κλειδί εισόδου για το διαμέρισμα μέχρι μια καθορισμένη ημερομηνία. Αν το κλειδί δεν έρθει στην ώρα του, το Blockchain θα μας επιστρέψει τα χρήματα. Αν λάβουμε το κλειδί πριν από την ημερομηνία ενοικίασης, το συμβόλαιο κρατά και το κλειδί και την χρέωση του ενοικίου μέχρι την ορισμένη ημερομηνία.. Το σύστημα λειτουργεί με περιπτώσεις If-Then και είναι δημόσιο, συνεπώς όλοι γνωρίζουν τους όρους του συμβολαίου. Εάν ο Α δώσει το κλειδί, είναι σίγουρος ότι θα πληρώνεται και αν στείλω ένα συγκεκριμένο ποσό σε bitcoins, ξέρω ότι θα λάβω το κλειδί.

Τα έξυπνα συμβόλαια μπορούν να χρησιμοποιηθούν για κάθε είδους καταστάσεις που κυμαίνονται από χρηματοπιστωτικά παράγωγα μέχρι ασφαλιστήρια, ιδιοκτησιακό δίκαιο, χρηματοπιστωτικές υπηρεσίες, νομικές διαδικασίες και crowdfunding.

Ένα γνωστό ρητό μεταξύ των χρηστών του Ethereum είναι το "Code is law", δηλαδή "ο κώδικας είναι νόμος"[1]. Υπό αυτή την έννοια τα έξυπνα συμβόλαια δεν έχουν την δυνατότητα να αλλάξουν. Ένα έξυπνο συμβόλαιο, αφού οριστεί και εισαχθεί εντός του Blockchain, δεν υπάρχει τρόπος να αλλάξει, ή να τροποποιηθεί, εκτός σε περίπτωση καταστροφής του. Σε περίπτωση που θέλουμε να ανανεώσουμε ή να αλλάξουμε μία έξυπνη σύμβαση, η καλύτερη επιλογή είναι να καταστρέψουμε το υπάρχων συμβόλαιο και να δημιουργήσουμε ένα καινούριο, το οποίο θα περιέχει τις επιθυμητές αλλαγές. Αυτό όμως προϋποθέτει να έχουμε βρει τρόπο να συνδεθούμε ξανά με τους παλιούς χρήστες και τα έξυπνα συμβόλαια με τα οποία είχε επικοινωνία το αρχικό έξυπνο συμβόλαιο.

[1] Το ρητό χρησιμοποιήθηκε κυρίως στην περίοδο του διαχωρισμού του Ethereum σε Ethereum και Ethereum Classic.

Κεφάλαιο 2

2 ΖΗΤΗΜΑΤΑ ΚΑΙ ΠΡΟΚΛΗΣΕΙΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Το Διαδίκτυο των πραγμάτων, βρίσκεται όλο και περισσότερο στο επίκεντρο του ενδιαφέροντας, μέσω των καινοτόμων εφαρμογών που προσφέρει παγκοσμίως. Στην συνέχεια παρουσιάζονται μερικά ζητήματα που έχουν προκύψει σχετικά με το Διαδίκτυο των πραγμάτων, τα οποία αφορούν είτε τις συσκευές είτε το ίδιο το δίκτυο.

2.1 Προβλήματα Συσκευών

2.1.1 Ακεραιότητα Δεδομένων και εντολών

Είναι πλέον γνωστό ότι, οι συσκευές IoT αλληλεπιδρούν με τον φυσικό κόσμο, με σκοπό την δημιουργία νέων και καινοτόμων εφαρμογών [66]. Ένα μεγάλο μέρος των συσκευών IoT, καλείτε να διαχειριστεί κρίσιμα δεδομένα και πληροφορίες οι οποίες μπορούν να χρησιμοποιηθούν για παράδειγμα, στην ρύθμιση βιομηχανικών εγκαταστάσεων, φορητών ιατρικών συσκευών, σημάτων μεταφοράς κλπ [67].

Ένα τυπικό σύστημα IoT αποτελείται από ένα μεγάλο αριθμό συνδεδεμένων αισθητήρων και συσκευών που συνδέονται μέσω ασύρματης διασύνδεσης. Σε μια τέτοια περίπτωση, οι συσκευές IoT είναι συνήθως απλές, μικρές και χαμηλής ισχύος. Η απλή φύση των συσκευών τις καθιστά πρωταρχικό στόχο για παραβίαση [40].

Μία από τα σημαντικότερες ανάγκες που υπάρχει στο Διαδίκτυο των πραγμάτων είναι η εξασφάλισης της ακεραιότητας των δεδομένων. Συγκεκριμένα, αναφέρομε στην ασφαλή μεταφορά δεδομένων, χωρίς να έχουν αλλοιωθεί ή μεταβληθεί [60]. Επίσης σημαντικές κρίνονται και οι περιπτώσεις επαλήθευσης της ακεραιότητας των δεδομένων που συλλέγονται και παράγονται από συνδεδεμένες συσκευές στο Διαδίκτυο, των δεδομένων του λογισμικού που τρέχει σε μια συσκευή και των δεδομένων που αποθηκεύονται [69].

Μεταξύ των διαφόρων επιθέσεων που πιθανόν να συμβούν στο IoT, είναι οι επιθέσεις παραβίασης δεδομένων, οι οποίες έχουν τη δυνατότητα να προκαλούν ζημίες. Ο στόχος ενός αντιπάλου σε τέτοιες επιθέσεις είναι να τροποποιήσει τα δεδομένα του IoT έτσι ώστε να διαταράξει τη λειτουργία του συστήματος και να προκαλέσει

λανθασμένες αποφάσεις ελέγχου [40]. Οι συσκευές IoT, οι οποίες δεν είναι προστατευμένες, καθίστανται ευάλωτες σε φυσικές επιθέσεις, επιθέσεις στα κανάλια επικοινωνίας για την εξαγωγή ή την τροποποίηση κρυπτογραφημένων μηνυμάτων στη μνήμη της συσκευής [40].

Η διαδικασία σχεδιασμού ασφαλών πολιτικών των συστημάτων, περιλαμβάνει τις αρχές αποκέντρωσης, την δυνατότητα αντικατάστασης και άμυνας σε βάθος. Το κρίσιμο σημείο της διαδικασίας αυτής, είναι η αξιολόγηση, και ο εντοπισμός των ευαίσθητων πληροφοριών που υπάρχουν στο σύστημα. Ωστόσο, οι πολιτικές ασφάλειας προϋποθέτουν την ύπαρξη αρχών όπως η ακεραιότητα, η αυθεντικότητα, και η εμπιστευτικότητα.

Στις περιπτώσεις τις οποίες οι χρήστες ενός δικτύου εμπλέκονται σε μια διαδικασία επικοινωνίας με άλλους χρήστες, απαιτείται η ύπαρξη εμπιστευτικότητας και ασφάλειας των καναλιών επικοινωνίας. Κανείς δεν πρέπει να έχει πρόσβαση στις πληροφορίες οι οποίες αποστέλλονται στην μεταξύ επικοινωνία δύο ή περισσότερων χρηστών. Ένας μη εξουσιοδοτημένος χρήστης, έχει την δυνατότητα παρακολούθησης της μετάδοσης πληροφοριών, καθώς και να κρατήσει αντίγραφο των αρχείων που μεταδίδονται. Επίσης απαιτείται η εξασφάλιση της ακεραιότητας των πληροφοριών που στέλνονται. Είναι γνωστό ότι έχουν παρουσιαστεί ανά τον κόσμο αρκετές επιθέσεις παραβίασης δεδομένων. Τα σημαντικότερα ζητήματα είναι ο εντοπισμός μη εξουσιοδοτημένων χρηστών, εξασφάλιση της ακεραιότητας των σημάτων που αποστέλλονται, και εάν οι πληροφορίες αυτές προέρχονται από πραγματικό χρήστη του Διαδικτύου, και όχι κάποιον ο οποίος προσποιείτε κάποιον άλλον.

Τα πιο πάνω ζητήματα υπάγονται στην κατηγορία ασφάλειας των πληροφοριών στο Διαδίκτυο. Ερευνητές έχουν παρουσιάσει διάφορες προτάσεις με σκοπό τον μετριασμό των πιο πάνω θεμάτων. Ωστόσο παραμένει ένα από τα σημαντικότερα πεδία των τεχνολογιών Διαδικτύου.

2.1.2 Διαχείριση Ψηφιακών Ταυτοτήτων

Η ψηφιακή ταυτότητα θεωρήθηκε ως το βασικό στοιχείο για όλες τις ηλεκτρονικές υπηρεσίες και το θεμέλιο για την οικοδόμηση μηχανισμών ασφαλείας όπως η πιστοποίηση ταυτότητας και η εξουσιοδότηση [52]. Εξετάζοντας ένα μεγάλο πλήθος ανθρώπων, συσκευών IoT και πηγές δεδομένων, η μεγάλη πρόκληση είναι στο πως οι οντότητες αυτές θα εντοπίζονται στον φυσικό κόσμο και με ποιο τρόπο θα

διατεθούν οι ψηφιακές ταυτότητες σε άτομα και συσκευές μέσω δικτύων. Οι ψηφιακές ταυτότητες παραμένουν ο θεμέλιος λίθος των ηλεκτρονικών υπηρεσιών και στους οποίους ενσωματώνονται οι μηχανισμοί ασφαλείας, (όπως, η πιστοποίηση ταυτότητας, η εξουσιοδότηση και οι ασφαλείς συναλλαγές) και τα διαδικτυακά πρωτόκολλα [71].

Μια ταυτότητα αναφέρεται σε ένα σύνολο πληροφοριών που χρησιμοποιούνται για την μοναδική αναγνώριση μιας οντότητας σε ένα συγκεκριμένο πλαίσιο [49], ενώ ένα σύστημα διαχείρισης ταυτότητας αναφέρεται στη διαχείριση πληροφοριών ταυτότητας μέσω ενός συνόλου [71]. Ωστόσο, τα παραδοσιακά συστήματα κεντρικής διαχείρισης ταυτότητας στο διαδίκτυο, εγείρουν πολλές ανησυχίες για την προστασία της ιδιωτικής ζωής. Για παράδειγμα, οι περισσότερες από τις λύσεις διαχείρισης ταυτότητας βασίζονται στην προϋπόθεση ότι οι χρήστες και οι πάροχοι υπηρεσιών εμπιστεύονται το κεντρικό σύστημα διαχείρισης. Ακόμη, τα παραδοσιακά συστήματα διαχείρισης ταυτότητας υφίστανται ορισμένες μακροχρόνιες ευπάθειες ασφαλείας και επιθέσεις [39].

Τα υφιστάμενα συστήματα διαχείρισης ταυτότητας δεν μπορούν να μεταφερθούν έμμεσα σε διαδικτυακά περιβάλλοντα λόγω των φυσικών χαρακτηριστικών του IoT. Η επεκτασιμότητα, η διαλειτουργικότητα και η κινητικότητα είναι εξαιρετικά σημαντικές απαιτήσεις, με αντίκτυπο στον σχεδιασμό των συστημάτων διαχείρισης ταυτότητας για το IoT. Αναπόφευκτα, θα υπάρχουν πολλοί διαφορετικοί παροχείς ταυτότητας από διαφορετικά συστήματα διαχείρισης ταυτότητας, αν και υπάρχουν εμπορικές λύσεις για τη διαχείριση της ταυτότητας, το κόστος αναγνώρισης αυξάνεται σημαντικά [71]. Τέλος, η διαχείριση ταυτότητας για το IoT πρέπει να χαρακτηρίζεται από κινητικότητα, δηλαδή, εξασφαλίζει στους χρήστες να συνδέουν συνεχώς τις υπηρεσίες τους όταν μετακινούνται [38], και να παρέχει πιστοποίηση και εξουσιοδότηση [65].

Στον πραγματικό κόσμο, κάθε άτομο έχει την δυνατότητα να έχει την δική του ταυτότητα σε διαφορετικές μορφές, όπως η άδεια οδήγησης, κάρτα κοινωνικών ασφαλίσεων, πιστοποιητικό γέννησης κ.λπ., όπως ορίζεται από τους φορείς παροχής υπηρεσιών. Επίσης κάθε συσκευή μπορεί να προσδιοριστεί μοναδικά, μέσω ενός μοναδικού αναγνωριστικού στοιχείου. Όλα αυτά ανήκουν στην κατηγορία των μέσων ταυτοποίησης. Ας σκεφτούμε όλους τους τρόπους ταυτοποίησης κάθε ατόμου, με όλες τις διαφορετικές μορφές της ταυτότητάς τους, κατά τις online και offline αλληλεπιδράσεις τους. Για παράδειγμα, κατά τις online πληρωμές, είσοδος σε δίκτυο στο οποίο είναι αναγκαία η προσθήκη προσωπικών μας στοιχείων κ.λπ.

Κατά τις online αλληλεπιδράσεις των χρηστών του διαδικτύου, προκύπτουν κάποια σοβαρά θέματα, όσο αφορά τα προσωπικά δεδομένα. Αν όντως τα άτομα και οι οργανισμοί έχουν τον πλήρη έλεγχο των προσωπικών δεδομένων και ταυτοτήτων τους. Αν όντως υπάρχουν περιπτώσεις στις οποίες οι προσωπικές πληροφορίες χρηστών, χρησιμοποιούνται χωρίς την συγκατάθεση των ιδιοκτητών τους. Οι απαιτήσεις ασφάλειας των προσωπικών δεδομένων, αυξάνουν την πολυπλοκότητα του δικτύου, με την μετάδοση κινδύνων σε άγνωστους τελικούς χρήστες. Αν αυτές οι πληροφορίες αποθηκεύονται σε συγκεκριμένες τοποθεσίες, χωρίς να το γνωρίζουμε. Αρκετοί αναφέρουν ότι στις περιπτώσεις στις οποίες χρειάζεται εγγραφή ενός χρήστη και χρήση ενός username και password, δεν παρέχετε επαρκή ψηφιακή εμπιστοσύνη για την υιοθέτηση ψηφιακών καναλιών, και πολύ συχνά υπάρχει ανάγκη για επαναπροσδιορισμό δέσμευσης με τους χρήστες. Επιπλέον, οι λύσεις διαχείρισης ταυτότητας, χαρακτηρίζονται αρκετά δαπανηρές και πολύπλοκες.

Ας σκεφτούμε πού βρίσκεται η ταυτότητα μας διαδικτυακά, και ποίος έχει πρόσβαση σε αυτές τις πληροφορίες. Οι προσωπικές πληροφορίες μοιράζονται τακτικά χωρίς την επίγνωση των ιδιοκτητών τους, πράγμα το οποίο αποτελεί κεντρική πηγή ευαίσθητων δεδομένων για τους χάκερς. Η ανάγκη για συμμόρφωση με τους κανονισμούς ενός δικτύου οδηγούν στην αλλαγή για νέες λύσεις διαχείρισης ταυτότητας.

Η έκδοση ταυτότητας, οι ασφαλείς πληρωμές, τα παγκόσμια αρχεία ασθενών αποτελούν περιπτώσεις χρήσης της ψηφιακής ταυτότητας, η οποία ενσωματώνεται σε διάφορες συναλλαγές στις μέρες μας.

Οι πραγματικές ανάγκες ενός χρήστη του Διαδικτύου είναι να έχει τον πλήρη έλεγχο των προσωπικών του δεδομένων. Επίσης πολύ σημαντικό να μπορεί να ελέγχει ποιος έχει πρόσβαση στα προσωπικά δεδομένα του, και αν όντως οι διαδικτυακές συναλλαγές τις οποίες εκτελεί, είναι ασφαλές.

Οι ανάγκες των επιχειρήσεων, όσο αφορά τον έλεγχο των προσωπικών δεδομένων, είναι να ενισχύσουν την ροή εργασιών στον βέλτιστο βαθμό. Επιθυμούν να μειώσουν με κάθε τρόπο τα κόστη τους, ώστε να καταφέρουν να βρίσκονται επάξια απέναντι από ανταγωνιστές τους. Επιπλέον, αρκετά σημαντική είναι η χρήση καινοτόμων στρατηγικών, αντί να χρειαστεί να επενδύσουν σε μια πιο απλή στρατηγική διαχείρισης ταυτότητας.

2.1.3 Συστήματα εγγραφής συσκευών

Το πρότυπο IoT απαιτεί ευρεία διασύνδεση δισεκατομμυρίων ετερογενών συσκευών και η αρχιτεκτονική συστήματος IoT έχει σχεδιαστεί για χρήση σε διαφορετικά φυσικά περιβάλλοντα. Έτσι απαιτεί την ικανότητα χειρισμού πολλών ετερογενών συσκευών. Για το λόγο αυτό, μια σημαντική ανησυχία στο πλαίσιο της ανάπτυξης λύσεων IoT είναι ο χειρισμός της αλληλεπίδρασης με ετερογενείς συσκευές IoT [56].

Η διαχείριση συσκευών είναι ένα από τα πιο σημαντικά χαρακτηριστικά από οποιοδήποτε εργαλείο διαχείρισης του IoT. Η διατήρηση των πληροφοριών της συσκευής, της κατάστασης και των αρχείων καταγραφής, καθώς και η παροχή αναλυτικών αναφορών και στατιστικών πληροφοριών σε επίπεδο συσκευής είναι σημαντική [47]. Καθώς οι συσκευές IoT κλιμακώνονται σε δισεκατομμύρια, το σημερινό μοντέλο κεντρικής διαχείρισης δικτύου θα μπορούσε να παρουσιάσει σημεία συμφόρησης. Σε ένα σύστημα IoT, απαιτείται η υποστήριξη ενσωμάτωσης συσκευών επειδή ορισμένες εργασίες ή απαιτήσεις μπορούν να υλοποιηθούν μέσω μιας υπηρεσίας, ενώ άλλες θα εκτελεστούν μέσω της ενσωμάτωσης πολλών υπηρεσιών [62].

Ένα εργαλείο διαχείρισης συσκευών θα πρέπει να διατηρεί μια λίστα συνδεδεμένων συσκευών και να παρακολουθεί την κατάσταση λειτουργίας τους. θα πρέπει να είναι σε θέση να χειρίζεται τις ρυθμίσεις παραμέτρων, τις ενημερώσεις υλικολογισμικού ή οποιουδήποτε άλλου λογισμικού και να παρέχει χειρισμό και αναφορά σφαλμάτων σε επίπεδο συσκευής [47].

Η επιτάχυνση της ανάπτυξης του IoT έχει επιπτώσεις σε διάφορους επιστημονικούς τομείς, προκαλώντας έτσι πολλές τάσεις στην επόμενη γενιά των συστημάτων IoT. Η αλλαγή των υποδομών είναι μια από αυτές τις τάσεις, επειδή το κεντρικό πρωτότυπο υπολογιστών είναι ευδιάκριτο σε ένα σημείο αποτυχιών και τα μεγάλα κέντρα δεδομένων καταναλώνουν τεράστια ποσά ενέργειας για να τα διατηρήσουν σε λειτουργία [64]. Εναλλακτικές τεχνολογίες αναπτύσσονται για να μειώσουν τις αποτυχίες στο νέφος [63]. Οι νέες τεχνολογικές τάσεις απαιτούν τα εργαλεία διαχείρισης να ταιριάζουν με αυτές τις αλλαγές και στη συνέχεια να κλιμακώνεται με την αρχιτεκτονική και τις συσκευές [62].

Καθώς ο αριθμός των συνδεδεμένων συσκευών αυξάνεται σε μεγάλο βαθμό, το Διαδίκτυο των Πραγμάτων καλείτε να αντιμετωπίσει ζητήματα ασφαλείας ακόμη και σε πιο περίπλοκες καταστάσεις. Αδιαμφισβήτητα το IoT έχει απλοποιήσει κατά πολύ την ζωή μας, με την βοήθεια των έξυπνων συσκευών, οι οποίες μπορούν να

προγραμματιστούν, και ελέγχονται εύκολα από τους ιδιοκτήτες τους. Λόγω της ευελιξίας που προσφέρει το Διαδίκτυο των Πραγμάτων, απαιτείται να υπάρχει ιδιαίτερος χειρισμός διάφορων καταστάσεων όσο αφορά την πιστοποίηση των συνδεδεμένων συσκευών. Προκύπτουν εύλογα ερωτήματα όσο αφορά την πιστοποίηση νέων συσκευών οι οποίες πρόκειται να συνδεθούν, σε ποιες περιπτώσεις δίνετε η άδεια πρόσβασης και ποια είναι τα δικαιώματα που μπορούν να έχουν στο περιβάλλον. Επίσης υπάρχει ανάγκη για ενίσχυση της διαδικασίας αναγνώρισης και πιστοποίησης πληροφοριών οι οποίες συλλέγονται από αισθητήρες του IoT, από το περιβάλλον στο οποίο βρίσκονται.

Λόγω των διαφορετικών καταστάσεων στις οποίες πιθανόν να βρεθούν οι συσκευές, έτσι ακριβώς στη μέση διάφορων ανησυχιών υπάρχει ανάγκη για την δημιουργία ενός ισχυρού μοντέλου διαχείρισης των συσκευών αυτών. Ένα πρωτόκολλο πιστοποίησης συσκευών ακόμη και σε συνεργασία με ισχυρές τεχνολογίες, μπορεί να εξασφαλίσει την αυθεντικότητα και εγκυρότητα κάθε συσκευής. Από τα σημαντικότερα χαρακτηριστικά αυτού του συστήματος, είναι να μπορεί να προγραμματιστεί κάθε λειτουργία την οποία προσφέρει, ώστε η διαδικασία εγγραφής να μην επηρεάζει την απόδοση των συσκευών και κατά συνέπεια την υπηρεσία που θα προσφέρουν στον χρήστη.

2.1.4 Κατακερματισμός λογισμικού συσκευών

Αναμφίβολα, η κύρια πρόκληση στα συστήματα IoT που συνδέονται με το διαδίκτυο, είναι όταν επηρεάζονται από διάφορες επιθέσεις. Το λογισμικό σταματά τα λειτουργικά του βήματα και επηρεάζει δυσμενώς την κανονική λειτουργία του συστήματος [59]. Έτσι, υπάρχει πάντα η ανησυχία των τρωτών σημείων στο λογισμικό στο επίπεδο εφαρμογής, όπως συμβαίνει με όλους τους τύπους λογισμικού [58]. Ακόμη η συνδεσιμότητα των συσκευών και οι περιπτώσεις παρακολούθησης και κλοπής ιδιωτικών πληροφοριών, έχουν προκαλέσει προβληματισμό.

Αρκετές μελέτες και δημοσιεύσεις που πραγματοποιήθηκαν τα τελευταία χρόνια έχουν δείξει ότι οι επιθέσεις κακόβουλου λογισμικού, έχουν αυξηθεί δραματικά, καθώς ένα νέο δείγμα κακόβουλου λογισμικού εντοπίζεται κάθε 9 δευτερόλεπτα, σύμφωνα με τους αναλυτές ασφαλείας [46].

Το κακόβουλο λογισμικό αποτελεί τη σοβαρότερη απειλή για συσκευές IoT, οι οποίες μπορούν είτε να καταστρέψουν τη συσκευή είτε, σε ορισμένες περιπτώσεις, να

μεταφέρουν το σύστημα σε προνομιακή κατάσταση κάτω από την εξουσία του εισβολέα, όπου ο εισβολέας μπορεί να αποκτήσει σταδιακά πρόσβαση με τελικό στόχο την αλλαγή του συστήματος, να κλειδώσει τη συσκευή ή το λογισμικό του χρήστη, να μολύνει μια συσκευή [41], να συλλέξει πληροφορίες τραπεζικού λογαριασμού από μια συσκευή, να βλάψει το σύστημα, είτε διαγράφοντας δεδομένα, είτε δημιουργώντας συνθήκες που μπορούν να καταστρέψουν ολόκληρο το σύστημα ή να εισβάλλει σε ένα σύστημα, κλέβοντας την ταυτότητα και τις πληροφορίες του χρήστη [42].

Επομένως, η συνεχής αύξηση του κακόβουλου λογισμικού που σχετίζεται με συσκευές IoT έχει αυξήσει την ανάγκη για σταθερές και αποδοτικές μεθόδους ανίχνευσης και προστασίας. Σε ορισμένες περιπτώσεις, οι αριθμοί έδειξαν ότι οι τρέχουσες μέθοδοι ανίχνευσης και προστασίας δεν είναι αρκετά αποδοτικές. Έτσι, οι λύσεις ανίχνευσης πρέπει να βελτιωθούν και να καταστούν πιο ανθεκτικές στις απειλές κατά της ασφάλειας που εμφανίζονται με την πάροδο του χρόνου. Ωστόσο, έχοντας κατά νου το περιβάλλον περιορισμένων πόρων των περισσότερων συσκευών IoT, η εκτέλεση περίπλοκων λύσεων ανίχνευσης και προστασίας κακόβουλου λογισμικού σε αυτά είναι σχεδόν απαγορευμένη. Αυτό δημιουργεί νέες ερευνητικές προκλήσεις σχετικά με τον τρόπο αποτελεσματικής προστασίας των συσκευών IoT [54].

Τα περιστατικά των κακόβουλων επιθέσεων προς το λογισμικό των συνδεδεμένων συσκευών στο IoT, έχουν αυξηθεί κατά πολύ. Μπορούν να φτάσουν σε σημείο στο οποίο θα προκαλέσουν σημαντικά πρόβλημα στις ίδιες τις συσκευές. Μια κακόβουλη επίθεση αυτού του τύπου, μπορεί να αποτελέσει ακόμη και καταστροφική για την ζωή των συσκευών IoT και των ανθρώπων. Γι αυτό τον λόγο λοιπόν, είναι απαραίτητο να επιλεχθούν ισχυρές στρατηγικές, (ανάλογα πάντα με τις απαιτήσεις του δικτύου) οι οποίες μπορούν να αποτρέψουν και να αντιμετωπίσουν αυτές καταστάσεις οι οποίες αποτελούν απειλή για το δίκτυο. Επίσης υπάρχει ανάγκη για συνεχή έλεγχο των ευπαθών σημείων της διαδικασίας διαχείρισης του λογισμικού των συσκευών, ώστε να ενισχυθεί η αξιοπιστία ακόμη περισσότερο.

2.1.5 Κατανομή ενημερώσεων λογισμικού στις συσκευές IoT

Υπάρχουν επίσης σημαντικές περιπτώσεις οι οποίες πρέπει να μελετηθούν ώστε το Διαδίκτυο των Πραγμάτων να ενισχύσει ακόμη περισσότερο τον τρόπο λειτουργίας του όπως η κατανομή καινούριων ενημερώσεων λογισμικού, στις συνδεδεμένες συσκευές του δικτύου. Η κακή διαχείριση των ενημερώσεων λογισμικού μπορεί να

αποτελέσει σημαντικό μειονέκτημα όσο αφορά την λειτουργικότητα του δικτύου. Το πρόβλημα το οποίο δημιουργείτε είναι ότι δεν επιτρέπει στο δίκτυο να λαμβάνει γρήγορα αποφάσεις, πράγμα το οποίο μειώνει την αποδοτικότητα του.

Η δυνατότητα εγκατάστασης νέου λογισμικού σε συσκευές IoT είναι απαραίτητη. Οι ενημερώσεις λογισμικού χρησιμοποιούνται για την προσθήκη νέων λειτουργιών, τη διόρθωση σφαλμάτων και την επίλυση γνωστών αδυναμιών ασφάλειας. Οι προμηθευτές συσκευών IoT έχουν εργαστεί σε διαδικασίες αυτοματοποιημένης ενημέρωσης λογισμικού για τη μείωση της αλληλεπίδρασης των τελικών χρηστών και την ελαχιστοποίηση του χρόνου διακοπής των συσκευών και των συνδεδεμένων συστημάτων τους. Από την άποψη της ασφάλειας, αυτές οι αυτοματοποιημένες διαδικασίες αντιπροσωπεύουν πιθανά σημεία εισόδου για εισβολείς. Εάν δεν προστατεύονται σωστά, οι συσκευές ενδέχεται να είναι ανοικτές σε χειρισμούς, συνήθως με την εγκατάσταση κακόβουλου κώδικα σε μια συσκευή [50].

Για παράδειγμα, ο κατασκευαστής παράγει μια νέα έκδοση του λογισμικού της συσκευής και το διανέμει σε ένα μη αξιόπιστο δίκτυο του χρήστη. Η επικοινωνία μπορεί να παρακολουθείται και ένας εισβολέας μπορεί να κρατήσει όλο το αρχείο ενημέρωσης το οποίο μπορεί στη συνέχεια να το παραμετροποίηση ώστε να έχει πρόσβαση σε ευαίσθητες πληροφορίες. Έτσι, εφόσον μια ενημερωμένη έκδοση διανέμεται μέσω ενός μη αξιόπιστου δικτύου, είναι δυνατή και η υποκλοπή της. Μπορεί ακόμη να προκύψουν πρόσθετοι κίνδυνοι, όπως ο κίνδυνος φόρτωσης μη εξουσιοδοτημένων υλικολογισμικών, ο κίνδυνος φόρτωσης υλικολογισμικών σε μη εξουσιοδοτημένες συσκευές ή ο κίνδυνος σκόπιμης έκτρωσης της διαδικασίας ενημέρωσης. Ως εκ τούτου, οι επιθέσεις είναι πιο πιθανό να συμβαίνουν ακριβώς κατά τη διαδικασία των ενημερώσεων [51].

Ενώ είναι σημαντικό να παρέχονται ενημερώσεις υλικολογισμικού σε συσκευές IoT, η ενημέρωση του λογισμικού IoT δεν μπορεί να περιοριστεί σε πλήρεις ενημερώσεις υλικολογισμικού. Η μετάδοση αναβαθμίσεων ελάχιστων μεγεθών (λιγότερο από το πλήρες υλικολογισμικό) είναι επιθυμητή ώστε να ταιριάζει σε υπερβολική έλλειψη πόρων (ενέργειας, απόδοσης, μνήμης) σε δίκτυα συσκευών IoT. Ειδικότερα, μια λύση θα είναι η εμφάνιση μιας αγοράς για λογισμικό IoT ανεξάρτητου από το υλικό και θα οδηγήσει έτσι σε μια κατάσταση όπου διαφορετικοί ενδιαφερόμενοι φορείς θα μπορούσαν να δημιουργήσουν και να τροποποιήσουν διαφορετικά μέρη του λογισμικού IoT στη συσκευή [55].

Υπάρχουν αρκετές λύσεις για την αντιμετώπιση αυτού του ζητήματος. Μια καλή τεχνική κατανομής ενημερώσεων του λογισμικού των συσκευών του δικτύου, δίνει ένα πλεονέκτημα χρόνου μέσω της αυτοματοποίησης των διαδικασιών του δικτύου κάνοντας τις αποδοτικότερες.

2.2 Προβλήματα Δικτύων

2.2.1 Ανίχνευση γειτονικών κόμβων και σχηματισμός δικτύου

Οι κόμβοι ή οι συσκευές του IoT είναι κατά κύριο λόγο αισθητήρες και ενεργοποιητές σε ένα συστήματα IoT [48]. Στο δίκτυο αισθητήρων, ο αριθμός των κόμβων αισθητήρων που αναπτύσσονται μπορεί να είναι τεράστιος. Τα πρωτόκολλα επικοινωνίας πρέπει να σχεδιάζονται έτσι ώστε το δίκτυο να διατηρήσει τη σταθερότητά του. Η εισαγωγή περισσότερων κόμβων στο δίκτυο σημαίνει ότι θα ανταλλάσσονται πρόσθετα μηνύματα επικοινωνίας έτσι ώστε οι κόμβοι αυτοί να είναι ενσωματωμένοι στο υπάρχον δίκτυο.

Όμως, τα ασύρματα δίκτυα αισθητήρων αντιμετωπίζουν πολλές προκλήσεις εξαιτίας περιορισμένων πόρων (μέγεθος μνήμης, περιορισμό ισχύος, υπολογιστική ικανότητα και ασυνέπεια κατά την ανάπτυξη) [37]. Αυτοί οι περιορισμοί οδήγησαν τους ερευνητές να προτείνουν προτάσεις που αφορούν την ενεργειακή απόδοση, τη βελτιστοποίηση της λειτουργίας των δρομολογητών και την καλύτερη διαχείριση των δεδομένων [48].

Ακόμη, λόγω ελαττωμάτων κόμβων, τα δεδομένα αισθητήρα που έχουν συλλεχθεί ενδέχεται να είναι λανθασμένα. Ως εκ τούτου, είναι σημαντικό να ανιχνεύονται συμβάντα με την παρουσία λανθασμένων μετρήσεων αισθητήρων και παραπλανητικών αναφορών [68].

Σε ένα ασύρματο δίκτυο αισθητήρων που λειτουργεί σε ένα περιβάλλον χωρίς παρακολούθηση, οι κόμβοι αισθητήρων μπορούν να δημιουργήσουν λάθος αναγνώσεις και λάθος αναφορές στους γείτονές τους, προκαλώντας εσφαλμένες αποφάσεις ή έλλειψη ενέργειας. Οι πιθανές πηγές λανθασμένων αναγνώσεων και αναφορών περιλαμβάνουν το θόρυβο, τα σφάλματα και τους κακόβουλους κόμβους στο δίκτυο. Σε αντίθεση με το θόρυβο και τα ελαττώματα, οι κακόβουλοι κόμβοι μπορούν να τροποποιήσουν αυθαίρετα τα δεδομένα που έχουν ανιχνευθεί και να δημιουργήσουν σκόπιμα λάθος αναφορές [68]. Μια προσέγγιση για τον εντοπισμό των κακόβουλων

κόμβων είναι οι γειτονικοί κόμβοι να ακούν παθητικά τις μεταδόσεις και να εντοπίζουν χειρισμούς ή απώλεια πακέτων [53].

Το ζήτημα που έχει προκύψει, αφορά την διαχείριση της παραγόμενης ενέργειας. Οι κόμβοι του δικτύου χρειάζονται να αναγνωρίσουν ο ένας τον άλλο έτσι ώστε να σχηματίσουν την τοπολογία του δικτύου, πράγμα το οποίο αποτελούσε μια χρονοβόρα διαδικασία. Κατά την διαδικασία ανάπτυξης του δικτύου, παρατηρήθηκε ότι όταν οι συσκευές βρίσκονταν συνεχώς σε λειτουργία, υπήρχε σπατάλη σημαντικής ποσότητας ενέργειας. Ερευνητές επικεντρώνονται στον χρόνο που απαιτείται για την αναγνώριση της παρουσίας ενός γειτονικού κόμβου μέσα στο δίκτυο.

Οι τεχνικές ανίχνευσης γειτονικών κόμβων σχεδιάστηκαν λαμβάνοντας υπόψη την κατανάλωση ενέργειας των συσκευών, με σκοπό να είναι όσο πιο χαμηλή γίνεται χωρίς να επηρεάζεται η απόδοση του δικτύου. Ωστόσο, έχουν εντοπίσει επιπλέον ζητήματα όσο αφορά το θέμα, λόγω κινητικότητας των κόμβων σε ένα δίκτυο. Τότε η διαδικασία ανίχνευσης κόμβων, έχει ως σκοπό την κατανόηση και απόκτηση γνώσης σχετικά με τις διαθέσιμα πρότυπα επικοινωνίας, προκειμένου να χρησιμοποιούνται μόνο όταν οι κόμβοι βρίσκονται σε κοντινό σημείο στο δίκτυο. Τα θέματα που προκύπτουν είναι ότι με την διαδικασία αυτή, το σύστημα πρέπει να είναι σε θέση να αναγνωρίσει έγκαιρα τους διαθέσιμους γειτονικούς κόμβους, καθώς και σε ποια σημεία του δικτύου θεωρούνται διαθέσιμοι.

2.2.2 Διαδικασία Δρομολόγησης

Η δρομολόγηση στο IoT βρίσκεται στο προκαταρκτικό στάδιο και υπάρχουν διάφορα εμπόδια που πρέπει να αντιμετωπιστούν. Δεδομένου ότι υπάρχουν διάφορες τεχνολογίες, για τις συσκευές και τα πρότυπα δικτύωσης προστίθεται επιπλέον πολυπλοκότητα στη διαδικασία δρομολόγησης. Τα υπάρχοντα πρωτόκολλα έχουν συγκεκριμένα όρια. Έτσι, είναι σημαντικό να δημιουργηθεί ένα πρωτόκολλο δρομολόγησης για όλες τις τεχνολογίες [44].

Σε κάθε είδους επικοινωνία υπάρχει ανάγκη συνεργασίας μεταξύ δύο οντοτήτων. Καθώς το IoT περιέχει ετερογενείς συσκευές, είναι σημαντικό οι συσκευές να συνεργάζονται μεταξύ τους για να επιτύχουν τη δρομολόγηση [57].

Ένα δίκτυο μπορεί να περιέχει πολλούς κόμβους που περιορίζουν την ενέργεια. Η περιττή και υπερβολική χρήση ενέργειας μπορεί να οδηγήσει σε «νεκρούς κόμβους». Δεν είναι δυνατή η αντικατάσταση των μπαταριών των ή των ίδιων των νεκρών

κόμβων. Έτσι μπορεί να δημιουργηθούν ενεργειακά προβλήματα εξαιτίας των νεκρών κόμβων, το οποία στη συνέχεια να δημιουργήσουν εμπόδια στη διαδικασία δρομολόγησης καθώς οι συσκευές αναμετάδοσης έχουν μικρή εμβέλεια [44]. Ταυτόχρονα, υπάρχουν και άλλοι λόγοι για μεταβολές τοπολογίας, όπως η συνεχής κινητικότητα και η πλήρης εξάντληση της ενέργειας των κόμβων και των παραγόντων [57].

Σημαντικό είναι επίσης το γεγονός ότι, οι περισσότερες τεχνολογίες του IoT είναι ασύρματες και μπορεί να είναι σταθερές ή κινητές. Οι κινητές συσκευές ενδέχεται να εισέλθουν ή να εξέλθουν από το δίκτυο, γεγονός που μπορεί να αυξήσει ή να μειώσει το μέγεθος του δικτύου. Μια τέτοια μεταβολή μπορεί να επηρεάσει τη δρομολόγηση. Τα δεδομένα που δημιουργούνται στο IoT ενδέχεται να έχουν λήξει, δηλαδή έπρεπε να παραδοθούν εντός ορισμένου χρόνου. Επομένως, είναι απαραίτητη η διαχείριση με τα πρωτόκολλα δρομολόγησης για τη διατήρηση της ποιότητας της υπηρεσίας [44].

Ολοκληρώνοντας, λόγω των περιβαλλοντικών παραγόντων, των μηχανισμών ανάπτυξης ή των ενεργειακών περιορισμών, υπάρχει πάντοτε ο κίνδυνος να εκτιμηθεί η συνολική απόδοση του δικτύου. Επομένως, πρέπει να υπάρχει ένας μηχανισμός στα πρωτόκολλα δρομολόγησης για την αντιμετώπιση τέτοιων απροσδόκητων συμβάντων [43].

Υπάρχουν περιπτώσεις στις οποίες οι συσκευές ενός δικτύου, λειτουργούν με διαφορετικά πρωτόκολλα δρομολόγησης και φαίνεται υπάρχουν προκλήσεις στην συνδεσιμότητα μεταξύ ετερογενών συσκευών. Αυτές οι συσκευές, πιθανόν να διαφέρουν στον τύπο, στα πρότυπα δικτύου τα οποία χρησιμοποιούν και τον τύπο των εφαρμογών που υποστηρίζουν. Επίσης, πρέπει να σημειωθεί ότι τα πρότυπα δικτύων, θέτουν κάποιους περιορισμούς πόρων πράγμα το οποίο αποτελεί πρόκληση για την διαδικασία της δρομολόγησης. Λόγω περιορισμών που μπορεί να υπάρχουν στο περιβάλλον, από την πλευρά συσκευών, και από την πλευρά του δικτύου, υπάρχει πιθανότητα να επηρεαστεί η απόδοση του δικτύου,

Ένας ακόμη παράγοντας που μπορεί να επηρεάσει την διαδικασία δρομολόγησης δεδομένων, είναι η ανοχή σφαλμάτων. Πολύ σημαντική αποτελεί η μελέτη και η επιλογή των μηχανισμών δρομολόγησης βάση του πλαισίου του περιβάλλοντος, ώστε να αποφευχθούν πιθανές συγκρούσεις, και γενικότερα να γίνετε μια σωστή διαχείριση του δικτύου. Επίσης, η ανοχή σφαλμάτων αναφέρεται και στην

αξιοπιστία των συσκευών εκτός που την αξιοπιστία των πρωτοκόλλων που χρησιμοποιούν.

Επίσης θέματα ασφαλείας, μπορούν να επηρεάσουν την λειτουργία του δικτύου, λόγω κακόβουλων επιθέσεων στο δίκτυο. Για παράδειγμα, στην περίπτωση επίθεσης man-in-the-middle, όπου ο επιτιθέμενος παρεμβαίνει στην επικοινωνία συσκευών, και έχει την δυνατότητα να αποσπάσει ή να αλλάξει πληροφορίες που στέλνονται από τους αρχικούς συμμετέχοντες

Υπάρχει ανάγκη για ένα ισχυρό μηχανισμό ελέγχου της διαδικασίας, μέσω του οποίου θα αποτραπούν ανεπιθύμητες καταστάσεις. Έχουν παρουσιαστεί κατά καιρούς λύσεις οι οποίες μετριάζουν τους κίνδυνους αυτούς, πράγμα το οποίο βασίζετε στις ανάγκες και τις απαιτήσεις του κάθε δικτύου.

2.2.3 Over the air updates

Μια ενημέρωση over the air (OTA) είναι ένας μηχανισμός για την εξ αποστάσεως ενημέρωση του συνδεδεμένου στο διαδίκτυο υλικού με νέες ρυθμίσεις. Λόγω της ταχείας εξέλιξης του IoT και της ζήτησης περισσότερων εμπειριών από τους χρήστες, η διαδικασία ενημέρωσης του λογισμικού των πραγμάτων στο IoT διαδραματίζει σημαντικό ρόλο για την ασφάλειά του [45].

Οι ενημερώσεις OTA του υλικολογισμικού δημιουργούν διάφορα ζητήματα ασφάλειας και δεν οφείλονται απαραίτητα σε κακόβουλες επιθέσεις. Για παράδειγμα, μεταφορτώνεται λάθος λογισμικό ή το νέο λογισμικό δεν λειτουργεί ή δεν είναι δυνατή η μεταφόρτωση του λογισμικού ασφαλείας αντί της ενημέρωσης του λογισμικού. Συχνά, μια διαδικασία αποτυχημένης ενημέρωσης αναγκάζει τη συσκευή να μην είναι χρήσιμη. Όσον αφορά τις συνδεδεμένες συσκευές που χρησιμοποιούνται σήμερα, η έλλειψη ασφάλειας μπορεί να έχει δυσμενείς συνέπειες δεδομένου ότι τα αυτοκίνητα ή ακόμη και οι ιατρικές συσκευές για παράδειγμα, αποτελούν μέρος του IoT [61].

Είναι επίσης απαραίτητο σε μια συσκευή IoT για την ενημέρωση του λογισμικού της, να αξιολογηθεί συνθήκες όπως η ισχύς της μπαταρίας, το σήμα, ο επαρκής χώρος αποθήκευσης των ενημερώσεων και η μνήμη για την εκτέλεση. Ωστόσο, οι ενημερώσεις συνεπάγονται με πιθανές διακοπές [55].

Εκτός από την ασφάλεια δικτύου με την εξασφάλιση των επικοινωνιακών καναλιών για τη μετάδοση των ενημερώσεων, η ασφάλεια παρέχεται κατά κανόνα από

ελέγχους βάσει της υπογραφής. Ωστόσο, εάν είναι αξιόπιστη, η πύλη ή ο δρομολογητής (π.χ. του σπιτιού) μπορεί να υπάρξει κάποια επιβάρυνση ασφαλείας με έλεγχους στις υπογραφές για λογαριασμό συσκευών IoT [55].

Κεφάλαιο 3

3 ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN ΚΑΙ IOT

3.1 Η στοίβα της τεχνολογίας Blockchain

Επίπεδο εφαρμογής
Αποκεντρωμένος χαρακτήρας
Hosting αποκεντρωμένων εφαρμογών

Επίπεδο υπηρεσιών
Είσοδος/Εξοδος δεδομένων
Συστήματα διαχείρισης
Κανάλια επικοινωνίας
Έξυπνα συμβόλαια
Εργαλεία Oracles
Ψηφιακά στοιχεία
Ψηφιακό πορτοφόλι
Ψηφιακή ταυτότητα
Κατανεμημένα συστήματα διαχείρισης αρχείων
Υπολογισμοί εκτός αλυσίδας

Επίπεδο δικτύου και πρωτόκολλα
Πρωτόκολλα συναίνεσης
Πρωτόκολλα πρόσβασης και δικαιωμάτων των χρηστών
Πρωτόκολλα σύνδεσης
Πρωτόκολλο επικοινωνίας
Πρωτόκολλα Roll Your Own
Εικονικές μηχανές

Επίπεδο υποδομής
Δίκτυο
Κόμβοι δικτύου
Virtualization
Διαδικασία εξόρυξης
Χώρος αποθήκευσης
Tokens

Σχήμα 1.10: Η στοίβα της τεχνολογίας Blockchain.

3.1.1 Επίπεδο εφαρμογής

Το επίπεδο αυτό αντιπροσωπεύει τα συστατικά του μιας αποκεντρωμένης εφαρμογής. Πρόκειται για τον συνδυασμό στρατηγικών, οι οποίες εξυπηρετούν την φιλοσοφία επιχειρησιακής λογικής, και των αλληλεπιδράσεων μεταξύ χρηστών του δικτύου.

- **Αποκεντρωμένος χαρακτήρας εφαρμογών:**

Με την εξέλιξη της τεχνολογίας Blockchain, μία αποκεντρωμένη εφαρμογή, έχει σκοπό να αναλάβει το κεντρικό σύστημα της εφαρμογής. Οι χρήστες έχουν την δυνατότητα να συνδεθούν μέσω ενός P2P δικτύου, πάνω στο δίκτυο του Blockchain. Για την δημιουργία αποκεντρωμένων εφαρμογών, είναι απαραίτητη η ύπαρξη μηχανισμών υπολογισμού, διαχείριση εισόδων, σύστημα αποθήκευσης αρχείων και σύστημα πληρωμών.

- **Hosting αποκεντρωμένων εφαρμογών:**

Η διαδικασία Hosting, αποτελεί αναγκαία για το κομμάτι των αποκεντρωμένων εφαρμογών. Η διαδικασία hosting, θέτει τις εφαρμογές διαθέσιμες στους χρήστες του δικτύου, μέσω του νέφους. Με αυτό τον τρόπο, η εφαρμογή θα γίνει 'hosted' πάνω στο αποκεντρωμένο δίκτυο. Επίσης αυτό το επίπεδο προσφέρει υπηρεσίες υποστήριξης στους χρήστες των αποκεντρωμένων εφαρμογών. Επιτρέπει στους χρήστες του δικτύου, την εύκολη πρόσβαση σε υπηρεσίες, και μπορεί να ενσωματώσει μια εφαρμογή σε οποιαδήποτε συσκευή η οποία είναι συνδεδεμένη στο δίκτυο. Επιπλέον, υπάρχει ένα μικρό κόστος συντήρησης.

3.1.2 Επίπεδο υπηρεσιών

Το στρώμα αυτό, καλύπτει τα σημαντικότερα συστατικά, που χρειάζονται για την δημιουργία μιας αποκεντρωμένης εφαρμογής.

- **Είσοδος/Εξοδος δεδομένων:**

Η τροφοδοσία δεδομένων είναι η διαδικασία της ροής δεδομένων, η οποία αποτελεί μια από τις σημαντικότερες διαδικασίες της λειτουργίας των αποκεντρωμένων εφαρμογών. Πρόκειται για ένα μηχανισμό ο οποίος σε συνεργασία με διαφορετικά συστατικά, δίνει την δυνατότητα για λήψη ενημερωμένων πληροφοριών από αξιόπιστες πηγές. Επιπλέον, χρησιμοποιείται για την ενημέρωση των κόμβων του δικτύου.

- **Συστήματα διαχείρισης:**

Πολύ σημαντικό για μία αποκεντρωμένη εφαρμογή είναι να περιέχει συστατικά για την διαχείριση των διαδικασιών του δικτύου. Η ιδανική επιλογή για αυτό τον σκοπό είναι η χρήση ενός αποκεντρωμένου αυτόματου μηχανισμού, μειώνοντας την ανάγκη για μεσολάβηση οποιουδήποτε αρμόδιου ατόμου στην εκτέλεση μιας συναλλαγής. Οι μηχανισμοί αυτοί, διαχειρίζονται έξυπνες συμβάσεις και χρησιμοποιούν πρωτόκολλα αποκέντρωσης για την ενίσχυση της αρχιτεκτονικής της τεχνολογίας Blockchain.

- **Κανάλια επικοινωνίας:**

Πρόκειται για τα κανάλια επικοινωνίας μεταξύ των κόμβων του δικτύου, στα οποία εκτελούνται συναλλαγές. Κάθε χρήστης ενός καναλιού θα πρέπει να 'υπογράψει' τις συναλλαγές του με το ιδιωτικό του κλειδί, ώστε να εξασφαλιστεί ότι οι συγκεκριμένες

συναλλαγές είναι έγκυρες και προέρχονται από τον πραγματικό χρήστη. Επίσης, κάθε κανάλι επικοινωνίας είναι ιδιωτικό, και διαθέσιμο μόνο για τους χρήστες οι οποίοι συμμετέχουν στην συγκεκριμένη συναλλαγή. Ωστόσο, τα κανάλια έχουν περιορισμένο χρονικό διάστημα ζωής, πράγμα που σημαίνει ότι θα χαθούν μετά από ένα προκαθορισμένο χρόνο.

- **Έξυπνα συμβόλαια:**

Μια έξυπνη σύμβαση μειώνει την ανάγκη του δικτύου για επιπλέον μεσολαβητές κατά την εκπλήρωση συναλλαγών σε ένα δίκτυο. Βασίζεται στην συμφωνία των μερών του δικτύου. Κατά την διαδικασία ανάπτυξης ενός έξυπνου συμβολαίου, ορίζονται οι κανονισμοί οι οποίοι πρέπει να ακολουθούνται από τους χρήστες του δικτύου. Πρόκειται για αυτοματοποιημένες διαδικασίες οι οποίες εκτελούνται όταν πληρούνται συγκεκριμένες συνθήκες στο δίκτυο, οι οποίες έχουν επίσης ορισθεί στο αρχικό στάδιο ανάπτυξης. Ένα έξυπνο συμβόλαιο μπορεί να επεξεργαστεί μόνο από τον δημιουργό του. Επίσης πρόκειται για ένα μηχανισμό ο οποίος εξασφαλίζει ότι δεν υπάρχει οποιαδήποτε επιρροή από οποιονδήποτε και θα ενισχύσει ότι αφορά θέματα ασφαλείας σε ένα δίκτυο.

- **Εργαλεία Oracles:**

Τα Oracles, είναι εργαλεία τα οποία χρησιμοποιούνται σε ένα δίκτυο Blockchain για την υποστήριξη των έξυπνων συμβάσεων. Λειτουργεί ως πράκτορας, ο οποίος εντοπίζει πληροφορίες για την κατάσταση του πραγματικού κόσμου, και τις μεταφέρει στο έξυπνο συμβόλαιο, ώστε να επαληθεύσει τις συνθήκες εκτέλεσης των διαδικασιών του. Λόγω του ότι η τεχνολογία Blockchain, δεν έχει πρόσβαση σε πληροφορίες εκτός του δικτύου, τότε σε συνεργασία με ένα εργαλείο Oracle, θα μπορέσει να το επιτύχει. Επίσης συλλέγοντας πληροφορίες από τον πραγματικό κόσμο, ελέγχεται κάθε συνθήκη του έξυπνου συμβολαίου, και έτσι ενεργοποιούνται οι ανάλογες διαδικασίες οι οποίες καθορίζονται από την έξυπνη σύμβαση.

- **Ψηφιακά στοιχεία:**

Πρόκειται για ψηφιακές αναπαραστάσεις που αντιστοιχούν σε διαφορετικά στοιχεία που μεταφέρονται εντός ενός δικτύου.

- **Ψηφιακό πορτοφόλι:**

Το ψηφιακό πορτοφόλι είναι ένα πρόγραμμα στο οποίο αποθηκεύονται τα δημόσια και ιδιωτικά κλειδιά κάθε χρήστη, τα οποία χρησιμοποιούνται στην διαδικασία επικύρωσης τους. Επίσης έχουν την δυνατότητα αλληλεπίδρασης με άλλα δίκτυα Blockchain σε περίπτωση που χρειαστεί. Μέσω του ψηφιακού πορτοφολιού, κάθε χρήστης μπορεί να παρακολουθήσει τα ψηφιακά στοιχεία που του ανήκουν.

- **Ψηφιακή ταυτότητα:**

Η ψηφιακή ταυτότητα αποτελεί ένα σημαντικό στοιχείο στην αρχιτεκτονική των BIoT εφαρμογών. Κάθε χρήστης έχει την δυνατότητα να συνδεθεί στο Διαδίκτυο μέσω της μοναδικής ψηφιακής ταυτότητας του. Είναι απαραίτητο για κάθε χρήστη να έχει την δική του μοναδική ταυτότητα, ώστε να μπορεί να γίνει ταυτοποίηση του συγκεκριμένου χρήστη όταν είναι ανάγκη. Κάθε άτομο μπορεί να έχει πολλαπλά ψηφιακά μοναδικά αναγνωριστικά, ανάλογα με την πλατφόρμα την οποία επιθυμεί να χρησιμοποιήσει. Το βασικότερο πλεονέκτημα μιας ψηφιακής ταυτότητας είναι ότι εξασφαλίζει την ασφάλεια και την προστασία της ιδιωτικότητας των χρηστών. Στις πλείστες περιπτώσεις, μια ψηφιακή ταυτότητα ενός χρήστη, περιέχει το όνομα χρήστη, τον κωδικό πρόσβασης, ημερομηνία γέννησης, αριθμός κοινωνικών ασφαλίσεων, ιστορικό συναλλαγών κ.λπ.

- **Κατανεμημένα συστήματα διαχείρισης αρχείων (Distributed File System):**

Πρόκειται για συγκεκριμένες τοποθεσίες διακομιστών, στα οποία αποθηκεύονται δεδομένα του δικτύου. Για την πρόσβαση στον διακομιστή, απαιτείται έλεγχος εγκυρότητας της ψηφιακής ταυτότητας του χρήστη.

- **Υπολογισμοί εκτός αλυσίδας:**

Οι υπολογιστικές διαδικασίες, γίνονται εκτός του Blockchain. Είναι μια λιγότερο δαπανηρή λύση, και βοηθά στην εξοικονόμηση χρόνου συγκριτικά με τις λύσεις εφαρμογής υπολογισμών μέσα στην αλυσίδα. Οι υπολογισμοί εκτός αλυσίδας, θα εξασφαλίσουν την αξιοπιστία των δεδομένων, και δεν υπάρχει περίπτωση να τροποποιηθούν με κανένα τρόπο. Επίσης οι υπολογισμοί εκτός της αλυσίδας, παρέχουν ένα επιπλέον επίπεδο ιδιωτικότητας και ένα αντίγραφο ασφαλείας κατά την ανάπτυξη

και την λειτουργία μιας αποκεντρωμένης εφαρμογής. Για παράδειγμα, τα συστήματα εικονικής μνήμης.

3.1.3 Επίπεδο Δικτύου και πρωτόκολλα

Το επίπεδο πρωτοκόλλων περιλαμβάνει τους αλγορίθμους συναίνεσης, απαιτήσεις συμμετοχής και ο ρόλος των εικονικών μηχανών στις αποκεντρωμένες εφαρμογές.

- **Αλγόριθμοι συναίνεσης:**

Όπως έχει αναφερθεί στο κεφάλαιο 1, οι αλγόριθμοι συναίνεσης χρησιμοποιούνται για την εξασφάλιση της συμφωνίας μεταξύ των κόμβων ενός δικτύου. Το βασικότερο πλεονέκτημα το οποίο μπορεί να προσφέρει ο αλγόριθμος συναίνεσης, είναι η αξιοπιστία ακόμη και όταν δεν υπάρχει εμπιστοσύνη μεταξύ των χρηστών ενός δικτύου. Για να μπορεί να γίνει αυτό, πρέπει να ληφθεί υπόψη ότι πιθανόν να υπάρξουν περιπτώσεις στις οποίες μερικοί κόμβοι του δικτύου να μην είναι διαθέσιμοι, είτε λόγω προβλήματος, είτε δεν αποτελούν μέρος της αποκεντρωμένης εφαρμογής. Αυτό σημαίνει ότι πιθανόν να υπάρξουν απώλειες δεδομένων, και αυτό κάνει τον αλγόριθμο συναίνεσης να πρέπει να είναι ανεκτικός σε σφάλματα. Έτσι προετοιμάζοντας τον μηχανισμό για τυχόν σφάλματα, αυξάνεται η αποδοτικότητα του δικτύου.

- **Πρωτόκολλα πρόσβασης και δικαιωμάτων των χρηστών:**

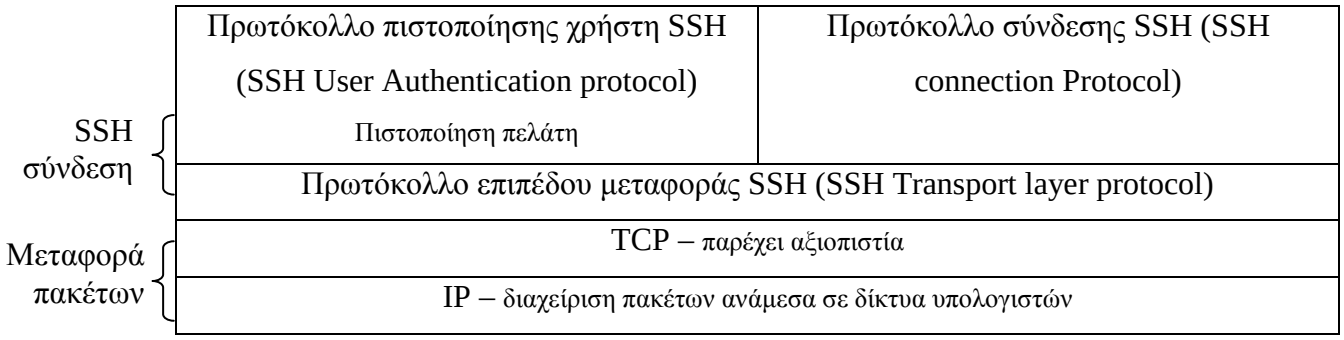
Κάθε δίκτυο βασισμένο στην τεχνολογία Blockchain, μπορεί να καθορίσει συγκεκριμένους κανόνες και περιορισμούς βάση των αναγκών του. Οι συγκεκριμένοι περιορισμοί αφορούν είτε τα δικαιώματα των χρηστών, είτε τις διαδικασίες του δικτύου. Επίσης, χρησιμοποιούνται πρωτόκολλα διαχείρισης και ελέγχου διαδικασιών, ώστε να εξασφαλιστεί ότι δεν παραβιάζεται οποιοσδήποτε περιορισμός, από οποιοδήποτε.

- **Πρωτόκολλα σύνδεσης:**

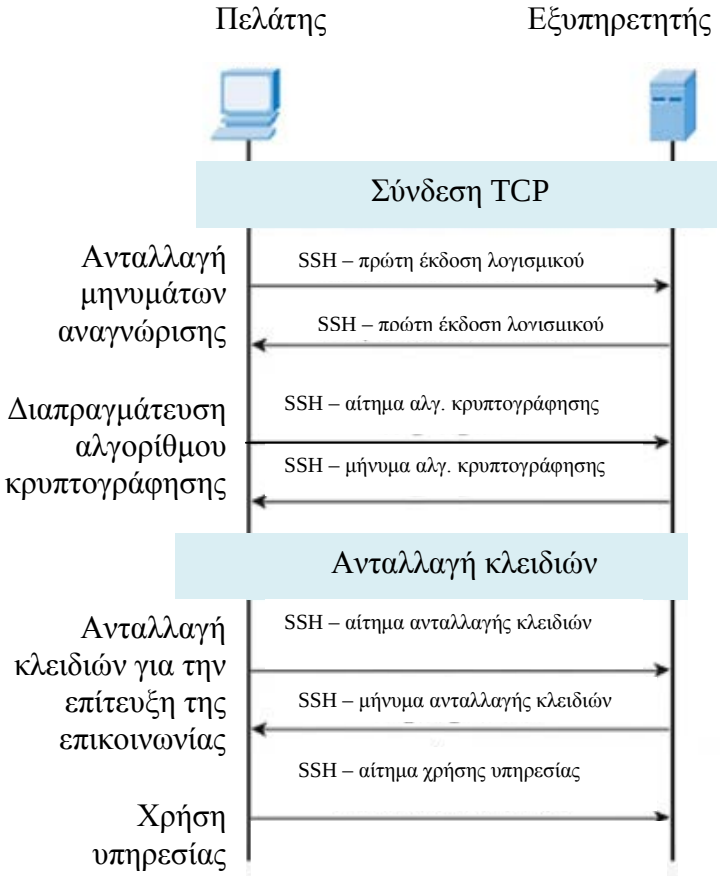
Το πρωτόκολλο Radio Link Protocol (RLP), αποτελεί ένα πρωτόκολλο σύνδεσης, το οποίο χρησιμοποιείται στα ασύρματα δίκτυα. Επίσης προσφέρει λειτουργίες όπως η αξιόπιστη μεταφορά δεδομένων, ανίχνευση απώλειας πακέτων, ανίχνευση γειτονικών κόμβων κλπ. Επιπλέον, πρόκειται για ένα συνεπές πρωτόκολλο, το οποίο εξασφαλίζει την αυθεντικότητα της συνδεσιμότητας σε ένα δίκτυο.

- **Πρωτόκολλα επικοινωνίας:**

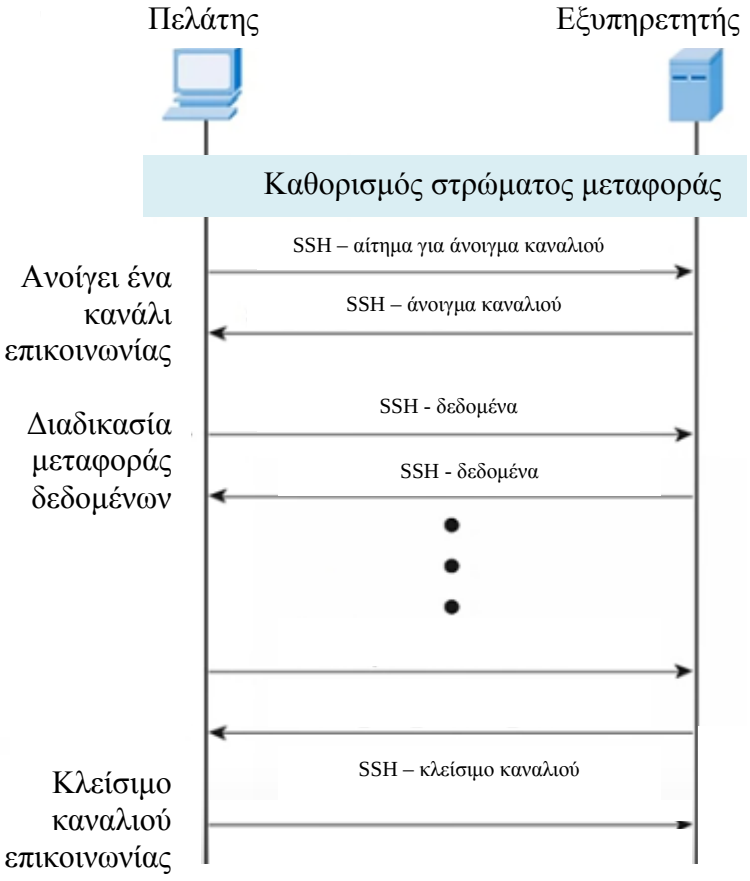
Το πρωτόκολλο Secure Shell (SSH), αποτελεί ένα από τα ευρέως γνωστά πρωτόκολλα σύνδεσης. Πρόκειται για ένα πρωτόκολλο το οποίο απευθύνεται στο μοντέλο πελάτη - εξυπηρετητή, και έχει σκοπό να ενισχύσει τις υπηρεσίες ενός δικτύου, και να εξασφαλίσει την ασφαλή μεταφορά δεδομένων μέσω αξιόπιστων καναλιών επικοινωνίας.



Σχήμα 1.11: Η στοίβα του πρωτοκόλλου SSH.



Σχήμα 1.12: Παράδειγμα ανταλλαγής πακέτων.



Σχήμα 1.13: Παράδειγμα ανταλλαγής μηνυμάτων.

- **Πρωτόκολλα Roll Your Own:**

Στις περιπτώσεις στις οποίες τα τυπικά πρωτόκολλα δεν καλύπτουν της ανάγκες της αποκεντρωμένης εφαρμογής, τότε χρησιμοποιούνται πρωτόκολλα τα οποία ορίζονται βάση συγκεκριμένων περιορισμών. Με αυτό τον τρόπο, επιτρέπεται να δημιουργηθούν πρωτόκολλα προσαρμοσμένα στις ανάγκες του δικτύου.

- **Εικονικές μηχανές:**

Πολύ σημαντικός είναι ο ρόλος μιας εικονικής μηχανής, στην αρχιτεκτονική των αποκεντρωμένων εφαρμογών. Μία εικονική μηχανή, εστιάζει στην διατήρηση της ασφάλειας, και στην εκτέλεση κώδικα ο οποίος προέρχεται από μια αναξιόπιστη πηγή, δηλαδή από οποιαδήποτε συνδεδεμένη συσκευή. Επίσης μπορεί να αποτρέψει κακόβουλες επιθέσεις, και εξασφαλίζει ότι όλα συνεχίζουν να λειτουργούν ομαλά. Η επιλογή της εικονικής μηχανής, εξαρτάται πάντα από τον τύπο και τις ανάγκες του δικτύου. Παραδείγματα εικονικών μηχανών είναι οι μηχανές Etherun, Solana, Kadena, Corda κλπ.

3.1.4 Επίπεδο Υποδομής

- **Δίκτυο:**

Όπως έχει ήδη αναφερθεί, πρόκειται για ένα αποκεντρωμένο δίκτυο στο οποίο δεν υπάρχει κεντρική αρχή κατά την διάρκεια ζωής του δικτύου.

- **Κόμβοι:**

Όταν αναφερόμαστε στους κόμβους, πρόκειται για τα σημεία αλληλεπίδρασης εντός ενός δικτύου. Επομένως, σε ένα εικονικό περιβάλλον δικτύου, κάθε συνδεδεμένη συσκευή, ονομάζεται κόμβος. Ο βασικός στόχος ενός κόμβου είναι η ενίσχυση του αποκεντρωμένου διαδικτύου και της συνεργασίας μεταξύ των χρηστών του. Επίσης υπάρχουν δίκτυα στα οποία υπάρχουν κόμβοι οι οποίοι έχουν περισσότερες δυνατότητες όπως η κατανομή εργασιών μεταξύ κόμβων κλπ, συγκριτικά με άλλους κόμβους, με απλούστερες δυνατότητες.

- **Virtualization:**

Η εικονική απεικόνιση του δικτύου, του λειτουργικού συστήματος, της επιφάνειας εργασίας κλπ, αποτελούν τους εικονικούς πόρους. Ο σκοπός αυτής της τεχνικής, είναι η καλύτερη διαχείριση και έλεγχος των χρηστών, και του φόρτου εργασίας στο δίκτυο ώστε να μειώσει τα κόστη που δημιουργούνται. Τέλος, εφαρμόζεται στα πλείστα επίπεδα δομών πληροφορικής.

- **Διαδικασία εξόρυξης (Mining):**

Μία από τις σημαντικότερες διαδικασίες για την τεχνολογία Blockchain. Πρόκειται για την διαδικασία μέσω της οποίας ελέγχεται κατά πόσο είναι έγκυρη, και στην συνέχεια να εισαχθεί στο Blockchain. Επίσης αυτή την διαδικασία διαχειρίζονται οι ‘miners’. Όταν υπάρχει μια σταθερή ροή εσόδων στο δίκτυο, τότε οι ‘miners’ θα πάρουν δίκαια το μερίδιο από το κέρδη.

- **Χώρος αποθήκευσης:**

Πρόκειται για αποκεντρωμένη μονάδα αποθήκευσης, η οποία εξασφαλίζει ένα καλύτερο και ασφαλέστερο περιβάλλον για τα δεδομένα που μεταφέρονται εντός δικτύου. Ακόμη, η αποκεντρωμένη αποθήκευση στο cloud, αποτελεί μια από τις ιδανικότερες λύσεις.

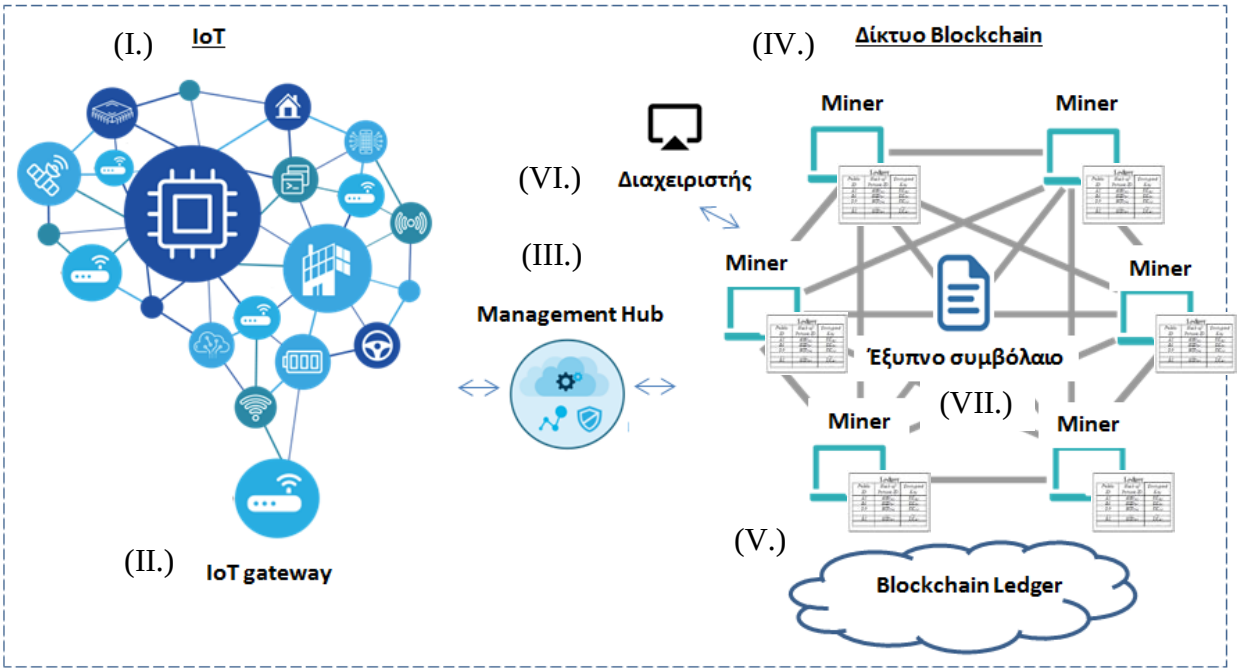
- **Tokens:**

Τα tokens, αντιπροσωπεύουν συνήθως ψηφιακές αναπαραστάσεις περιουσιακών στοιχείων. Στις πλείστες περιπτώσεις, έχουν την μορφή ψηφιακών νομισμάτων. Επίσης, συνήθως συμπεριλαμβάνεται ένα σύστημα συμβόλων, ως ένα σύστημα διαχείρισης κεφαλαίων.

3.2 Ενσωμάτωση της τεχνολογίας Blockchain στο IoT

3.2.1 Αρχιτεκτονική συνεργασίας Blockchain-IoT

Σε αυτό το υποκεφάλαιο, σας παρουσιάζω την τυπική αρχιτεκτονική συνεργασίας της τεχνολογίας Blockchain και του IoT.



Σχήμα 1.14: Αρχιτεκτονική συστημάτων Blockchain-IoT.

Τα συστατικά της αρχιτεκτονικής:

I. IoT

Πρόκειται για ένα σύνολο συσκευών και αισθητήρων τα οποία είναι συνδεδεμένα στο Διαδίκτυο, και διαθέτουν μοναδικά αναγνωριστικά στοιχεία. Η σύνδεση μεταξύ των συσκευών IoT είναι ασύρματη, και έχουν την δυνατότητα ανταλλαγής δεδομένων μεταξύ τους. Επίσης αρκετά σημαντικό να λάβουμε υπόψη, είναι οι περιορισμοί που υπάρχουν στις συσκευές IoT, όπως η υπολογιστική δύναμη, η μνήμη, η μπαταρία κλπ. Επιπλέον, η χρήση πρωτοκόλλων σύνδεσης επιτρέπει την επικοινωνία μεταξύ διαφορετικών συσκευών από διαφορετικά συστήματα και διαφορετικά δίκτυα.

Όσο αφορά την συνεργασία των συσκευών IoT και της τεχνολογίας Blockchain, δεν αποτελεί απαραίτητη προϋπόθεση ότι όλες οι συσκευές IoT επικοινωνούν με το δίκτυο Blockchain. Η συνεργασία της τεχνολογίας Blockchain, των έξυπνων συμβολαίων και του Διαδικτύου των πραγμάτων, αναμένεται να δώσει ευέλικτες και αποδοτικές λύσεις, όσο αφορά την διαδικασία διαχείρισης των συσκευών IoT και των λογισμικών τους.

II. Συσκευή IoT gateway

Ο ρόλος ενός IoT gateway σε μία αρχιτεκτονική αυτής της φύσης, είναι το σημείο επικοινωνίας των αισθητήρων και των έξυπνων συσκευών μαζί με το cloud. Συγκεκριμένα, τα IoT gateways είναι υπεύθυνα για την μεταφορά των δεδομένων από τις συσκευές IoT, στο νέφος και αντίστροφα.

III. Management Hub

Ένας κόμβος Hub, είναι μία συσκευή η οποία χρησιμοποιείται ως ένα κοινό σημείο επικοινωνίας μεταξύ κόμβων σε ένα δίκτυο, ακόμη και για την σύνδεση μεγαλύτερων τμημάτων ενός δικτύου. Σε αυτή την περίπτωση, είναι ο συνδετικός κρίκος μεταξύ ενός συνόλου συνδεδεμένων συσκευών IoT, και του δικτύου Blockchain. Ο κόμβος συνδέεται άμεσα με το δίκτυο Blockchain, και πιο συγκεκριμένα είναι υπεύθυνο να μεταφράσει δεδομένα που δέχεται από τις συσκευές IoT, ώστε να είναι αναγνώσιμα από το δίκτυο Blockchain.

IV. Δίκτυο Blockchain

Στο δίκτυο Blockchain, περιλαμβάνεται το Blockchain ledger, οι κόμβοι του δικτύου, οι κόμβοι miners, και τα έξυπνα συμβόλαια τα οποία βρίσκονται εντός της υποδομής. Το Blockchain ανήκει στην οικογένεια των κατανεμημένων ledgers, και αποτελείτε από ένα σύνολο από μπλοκς. Επίσης, το δίκτυο Blockchain σε συνεργασία με πρωτόκολλα επικοινωνίας, έχει την δυνατότητα να προσφέρει υπηρεσίες σε παγκόσμιο επίπεδο. Επίσης οι κόμβοι – miners συμμετέχουν στην διαδικασία επικύρωσης συναλλαγών που συμβαίνουν στο δίκτυο Τέλος, το Blockchain

προγραμματίζεται και προσαρμόζεται ανάλογα με τις απαιτήσεις του δικτύου, μέσω των έξυπνων συμβολαίων.

Μία εύλογη ερώτηση είναι το ποιος τύπος Blockchain είναι ο κατάλληλος για την ιδανική λύση στην αντιμετώπιση του ζητήματος. Η λύση βασίζεται στους εξής παράγοντες:

Η βασική διαφορά μεταξύ των τριών τύπων Blockchain, είναι ότι το δημόσιο Blockchain είναι αποκεντρωμένο, το ιδιωτικό είναι πλήρως κεντροποιημένο λόγω του ότι βρίσκεται υπό τον έλεγχο συγκεκριμένων χρηστών, και το Blockchain κοινοπραξίας είναι μερικώς αποκεντρωμένο.

Από πλευράς αποδοτικότητας, το ιδιωτικό και το consortium Blockchain, έχουν χαρακτηριστεί πιο αποδοτικά για τον λόγο ότι ο αριθμός των κόμβων οι οποίοι έχουν τον ρόλο του επικυρωτή (miners), είναι μικρότερος συγκριτικά με ένα δημόσιο Blockchain. Λαμβάνοντας υπόψη ότι, χρειάζεται αρκετός χρόνος για την διάδοση των συναλλαγών, και ότι οι περιορισμοί όσο αφορά την ασφάλεια στο δημόσιο Blockchain είναι πιο αυστηροί, τότε η απόδοση των συναλλαγών είναι περιορισμένη, τότε και τα επίπεδα καθυστέρησης είναι υψηλά.

Από πλευράς διαχείρισης, το ιδιωτικό και το consortium Blockchain έχουν καλύτερο έλεγχο όσο αφορά τις άδειες ανάγνωσης δεδομένων, συγκριτικά με ένα δημόσιο Blockchain. Ο λόγος είναι ότι σε ένα δημόσιο Blockchain, όλες οι συναλλαγές είναι ορατές στον οποιοδήποτε, πράγμα το οποίο δεν αποτελεί την πιο ασφαλή λύση για την προστασία των δεδομένων του δικτύου.

Όσο αφορά την διαδικασία συναίνεσης, ένα ιδιωτικό Blockchain καθορίζει είτε μία ομάδα κόμβων, είτε ένα οργανισμό ο οποίος είναι υπεύθυνος για την διαδικασία συναίνεσης στο δίκτυο. Αυτό σημαίνει ότι υπάρχει πλήρης έλεγχος της διαδικασίας, σε αντίθεση με τις περιπτώσεις των δημόσιων Blockchain, στα οποία οποιοσδήποτε κόμβος μπορεί να συμμετέχει στην διαδικασία συναίνεσης. Σύμφωνα με μελέτες, το ιδιωτικό Blockchain, έχει χαρακτηριστεί ως η ιδανική επιλογή από πλευράς ελέγχου των διαδικασιών του δικτύου.

V. Κατανεμημένο κατάστιχο (Blockchain Ledger)

Το κατανεμημένο κατάστιχο, ανήκει επίσης στην οικογένεια των Distributed Ledger Technologies. Ειδικότερα, είναι ένας τύπος Βάσης Δεδομένων, το οποίο είναι ευρέως διαθέσιμο, και συγχρονίζεται με τα μέλη ενός αποκεντρωμένου δικτύου. Τα δεδομένα,

διατηρούνται από το σύνολο των τερματικών τα οποία ανήκουν στο δίκτυο. Επίσης, με κάθε νέα συναλλαγή που εκτελείται, διανέμεται ένα αντίγραφο του ledger του δικτύου, σε όλους τους χρήστες του, ώστε να υπάρχει πλήρης διαφάνεια και συνέπεια.

VI. Διαχειριστές

Οι διαχειριστές, είναι συσκευές οι οποίες είναι υπεύθυνες για την διαχείριση των συσκευών IoT, και την επικοινωνία τους με το δίκτυο Blockchain. Στην θέση του διαχειριστή μπορεί να είναι είτε μία συσκευή, είτε ένα σύνολο συσκευών, οι οποίες θα προγραμματιστούν ανάλογα ώστε να επιτύχουν τον σκοπό τους. Τον ρόλο του διαχειριστή μπορούν να έχουν συσκευές οι οποίες λειτουργούν με τρόπο ώστε να μην αποτελούν εμπόδιο στο υλικό του συστήματος. Επίσης συστήνεται στους διαχειριστές να μην είναι συνεχώς συνδεδεμένοι στο δίκτυο Blockchain, πράγμα το οποίο θα βοηθήσει στην μείωση κατανάλωσης ενέργειας των πόρων του δικτύου.

Για σκοπούς διαχείρισης, κάθε συσκευή IoT η οποία πρόκειται να συνδεθεί στο δίκτυο, πρέπει να εγγραφεί κάτω από ένα διαχειριστή. Στην ουσία, ένας διαχειριστής, είναι υπεύθυνος για την πρόσβαση μίας συσκευής IoT, στο δίκτυο Blockchain. Αφού γίνει εγγραφή της συσκευής IoT στο δίκτυο Blockchain, τότε οι διαχειριστές έχουν συγκεκριμένα δικαιώματα σε αυτές, ανάλογα πάντα με τις απαιτήσεις του συστήματος.

VII. Smart Contract

Όπως έχει ήδη αναφερθεί, ένα έξυπνο συμβόλαιο είναι ένα σύνολο από scripts τα οποία αποθηκεύονται στο δίκτυο Blockchain, και είναι υπεύθυνα για συγκεκριμένο σκοπό. Αφού εγκριθεί, τότε αποθηκεύεται στο Blockchain, και όλοι οι εγκεκριμένοι χρήστες του δικτύου έχουν πρόσβαση σε αυτό. Κάθε διαδικασία η οποία βρίσκεται σε ένα έξυπνο συμβόλαιο, ενεργοποιείται από συναλλαγές που πραγματοποιούνται στο Blockchain.

Για σκοπούς ασφάλειας και ελέγχου, κρίνεται αναγκαία η ύπαρξη του ιδιοκτήτη του έξυπνου συμβολαίου, ο οποίος θα έχει συγκεκριμένα καθήκοντα κατά την διάρκεια ζωής του έξυπνου συμβολαίου. Εφόσον ένα έξυπνο συμβόλαιο εγκριθεί και αποθηκευτεί στο δίκτυο, τότε αποστέλλεται στον ιδιοκτήτη, η μοναδική διεύθυνση στο Blockchain, στην οποία θα αποθηκευτεί το συμβόλαιο. Για την καλύτερη διαχείριση του συστήματος, συστήνεται η χρήση ενός έξυπνου συμβολαίου και διαδικασιών για αυτό τον σκοπό.

3.2.2 Βασικές αρχές συνεργασίας Blockchain - IoT

Το δίκτυο Blockchain, σε συνεργασία με άλλες τεχνολογίες και πρότυπα, μειώνει τις εξαρτήσεις μεταξύ των κόμβων, και αντιμετωπίζει τα σημεία αποτυχίας στο δίκτυο, και δίνει την δυνατότητα χρήσης Βάσεων Δεδομένων ανοικτού κώδικα.

Η φιλοσοφία της συνεργασίας της τεχνολογίας Blockchain και του Διαδικτύου των πραγμάτων με σκοπό την διαχείριση ψηφιακών ταυτοτήτων, βασίζεται σε κατευθυντήριες αρχές οι οποίες αποσκοπούν στην βελτίωση της ιδιωτικότητας, της ασφάλειας και της χρηστικότητας των ψηφιακών υπηρεσιών για τους χρήστες, τις συσκευές αλλά και για τους παροχής υπηρεσιών. Οι βασικές αρχές οι οποίες πρέπει να ακολουθούνται είναι οι εξής:

Οι χρήστες και οι συσκευές του δικτύου, αλληλεπιδρούν άμεσα με τα συστατικά του δικτύου, χωρίς να υπάρχει ανάγκη για την ύπαρξη ενός τρίτου ατόμου, ή ενός τρίτου εργαλείου.

Η ταυτότητα των συσκευών πρέπει να προστατεύεται με την χρήση τεχνικών και πρωτοκόλλων κρυπτογραφίας, ενώ τα όλα τα μέρη τα οποία συμμετέχουν σε μια συναλλαγή είναι σημαντικό να παραμείνουν ανώνυμα.

Στην αρχιτεκτονική του συστήματος συμπεριλαμβάνεται η ελεγχόμενη διατήρηση ιστορικού συναλλαγών, στο οποίο οι εγγραφές είναι αμετάβλητες. Για είναι αυτό εφικτό, υπάρχει ένα κόστος προς τους χρήστες του δικτύου.

Ένα βασικό ζήτημα είναι η σωστή χρήση των κανόνων καταγραφής και διαμόρφωσης δεδομένων, οι οποίοι πρέπει να είναι διαθέσιμοι αποκλειστικά προς τους συμμετέχοντες του δικτύου. Επίσης η αρχιτεκτονική αυτή, δίνει την δυνατότητα ασφαλούς αποθήκευσης δεδομένων σε ένα κατανεμημένο κατάστιχο το οποίο δημοσιοποιείται προς όλους τους συμμετέχοντες του δικτύου και κάθε ψηφιακό στοιχείο κρυπτογραφείται με την χρήση κλειδιών. Η έγκριση κάθε συναλλαγής η οποία συμβαίνει στο δίκτυο είναι απαραίτητη.

Η δραστηριότητα οποιουδήποτε χρήστη είναι απαραίτητο να βρίσκεται υπό έλεγχο, ώστε να αποφευχθούν μη επιθυμητές καταστάσεις στο δίκτυο. Κατά την

επικοινωνία δύο ή περισσότερων συσκευών, ανταλλάζονται κρυπτογραφημένα μηνύματα, ώστε να επιβεβαιωθεί ότι κάθε συσκευή βρίσκεται υπό τον έλεγχο του πραγματικού ιδιοκτήτη της συσκευής. Επίσης κάθε μήνυμα που αποστέλλεται, πρέπει να υπογράφεται με το κλειδί (ψηφιακή υπογραφή) του χρήστη, τα οποία χειρίζονται μόνο από τους ιδιοκτήτες τους.

Για σκοπούς ασφαλείας, τα δεδομένα που μεταδίδονται στο δίκτυο πρέπει να είναι ορατά σε όσο το δυνατόν πιο λίγους χρήστες. Κάθε συναλλαγή που συμβαίνει στο δίκτυο, εγκρίνεται είτε από υφιστάμενους χρήστες, είτε από εξωτερικά εργαλεία, ώστε να επιβεβαιωθεί ότι δεν πρόκειται για οποιαδήποτε μη εξουσιοδοτημένη συναλλαγή. Με την χρήση των έξυπνων συμβάσεων, δίνεται η δυνατότητα συντονισμού και αυτοματοποίησης εργασιών με σκοπό την αποφυγή οποιαδήποτε δυσμενής κατάστασης.

3.3 Περιπτώσεις χρήσης

Ας σκεφτούμε το εξής σενάριο. Όπως πλέον γνωρίζουμε, οι συσκευές οι οποίες είναι συνδεδεμένες στο Διαδίκτυο, έχουν αποκτήσει την ικανότητα της μεταξύ τους επικοινωνίας. Συνοπτικά, όταν μία συσκευή Χ, στέλνει δεδομένα στο δίκτυο, τότε δημιουργείται ένα session, στο οποίο τα δεδομένα αναπαρίστανται με μια συγκεκριμένη μορφή, και μέσω των πρωτοκόλλων εφαρμογής, δίνεται η δυνατότητα διαχείρισης και μετάδοσης τους.

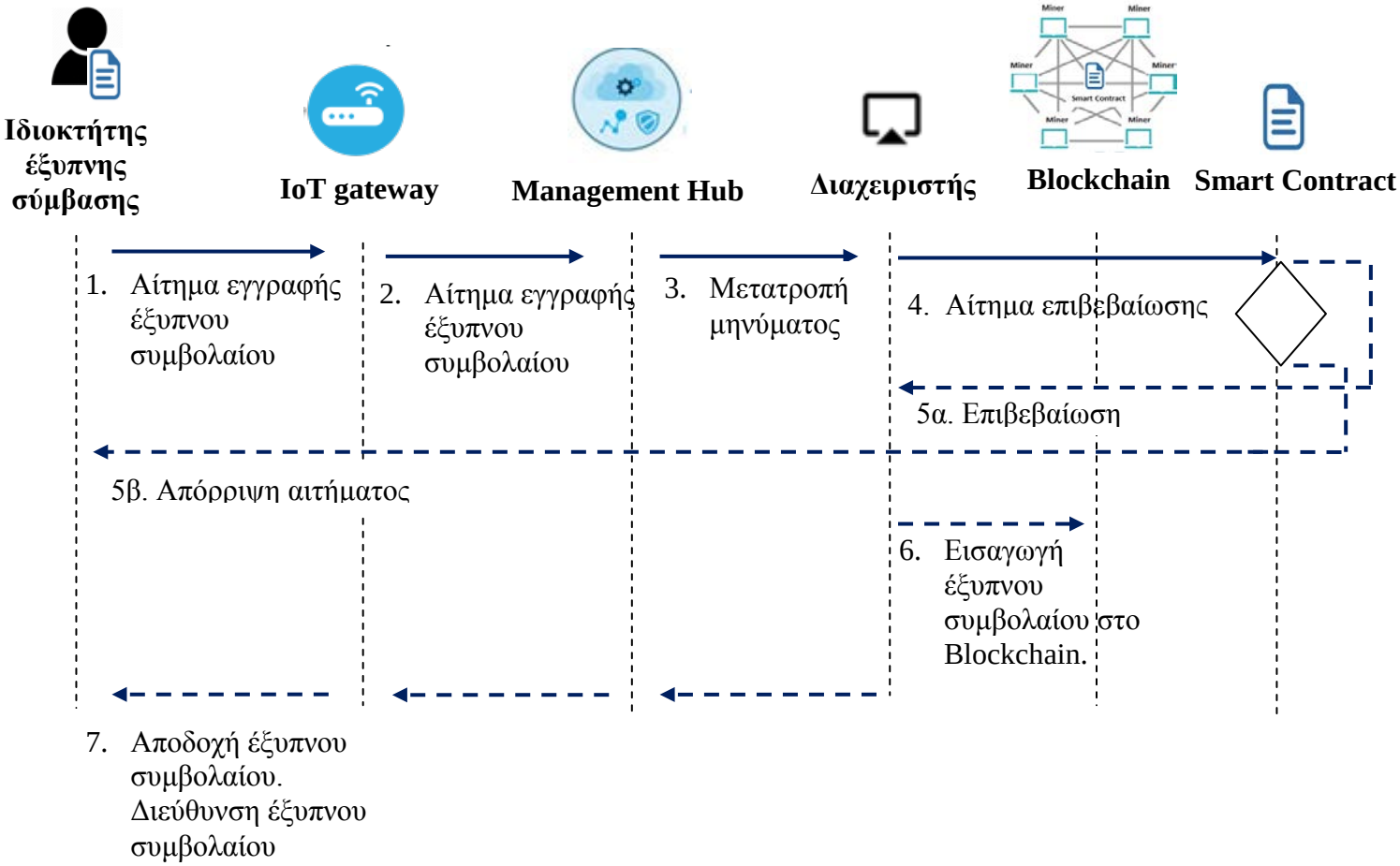
Όπως έχει αναφερθεί σε προηγούμενο κεφάλαιο, η τεχνολογία Blockchain, εφαρμόζεται σε αποκεντρωμένα δίκτυα για τα οποία διατηρείται ένα κατανεμημένο κατάστιχο συναλλαγών. Τα δεδομένα τα οποία καταγράφονται στο κατανεμημένο κατάστιχο, συγχρονίζονται με διαφορετικά συστήματα, και διαμοιράζονται στους κόμβους του δικτύου, ώστε να υπάρχει διαφάνεια. Η τεχνολογία Blockchain, καλείται να δώσει την λύση στην πρόκληση της διαχείρισης ενός υπέρογκου αριθμού συσκευών οι οποίες αναμένονται να συνδεθούν μελλοντικά στο Διαδίκτυο. Πρόκειται για συσκευές οι οποίες έχουν κατασκευαστεί σε διαφορετικά μέρη στον κόσμο, όπου ο κατασκευαστής κάθε συσκευής, εφοδιάζει την κάθε μία με ένα δημόσιο και ένα ιδιωτικό αναγνωριστικό.

Η παρακολούθηση ενός δικτύου, αποτελεί επίσης μια εξαιρετικά σημαντική διαδικασία, για την αξιόπιστη παροχή υπηρεσιών και την καλύτερη διαχείριση του. Από τις δημοφιλέστερες προσεγγίσεις, αποτελεί η παρακολούθηση της κατάστασης του δικτύου, και της παρατήρησης της συμπεριφοράς των μελών του. Οι μηχανισμοί αυτοί, προσφέρουν διαφορετικά επίπεδα διαχείρισης, και βέβαια εξαρτάται από τα χαρακτηριστικά και τις απαιτήσεις του δικτύου. Θα δούμε στην συνέχεια πώς η εφαρμογή αυτού του είδους μηχανισμών σε δίκτυα σε συνεργασία με την τεχνολογία Blockchain και των έξυπνων συμβολαίων μπορεί να εξυπηρετήσει ένα IoT περιβάλλον.

3.3.1 Διαδικασία εισαγωγής έξυπνου συμβολαίου

Έστω ότι χρήστης Χ, έχει συνδεθεί στο Διαδίκτυο και θέλει να εισάγει στο Blockchain ένα έξυπνο συμβόλαιο. Αρχικά, υπάρχει μια διαδικασία επικύρωσης της ταυτότητας του χρήστη Χ. Εφόσον γίνει ταυτοποίηση της ταυτότητας του χρήστη Χ, μέσω της διεύθυνσης του στο Blockchain, τότε δημιουργείται ένας μοναδικός κωδικός και η διεύθυνση στην οποία πρόκειται να αποθηκευτεί το συμβόλαιο (εντός του

Blockchain). Επίσης ένα συμβόλαιο, αντιστοιχείται με τον μοναδικό κωδικό του λογαριασμού του ιδιοκτήτη, στο Blockchain. Σε ένα έξυπνο συμβόλαιο καθορίζονται οι όροι και οι προϋποθέσεις, βάση των οποίων μία συναλλαγή θεωρείται έγκυρη, και τι ενέργειες αναμένονται μετά την εκτέλεση της. Γενικότερα, μία έξυπνη σύμβαση προσδιορίζει τους κανονισμούς του συστήματος και έχει στόχο να αυτοματοποιήσει όλες τις λειτουργίες ενός δικτύου.



Σχήμα 1.15: Διαδικασία εισαγωγής έξυπνου συμβολαίου.

Όταν λοιπόν ένα έξυπνο συμβόλαιο εγγραφεί επίσημα στο Blockchain, και αποκτήσει την δική του μοναδική ταυτότητα, τότε όλοι οι κόμβοι του δικτύου, ενημερώνονται για την νέα εισαγωγή, και μπορούν να στείλουν αιτήματα σε αυτό, οποιαδήποτε στιγμή. Να σημειωθεί ότι, ένα έξυπνο συμβόλαιο περιέχει αυτοματοποιημένες διαδικασίες, οι οποίες ενεργοποιούνται από γεγονότα τα οποία συμβαίνουν στο δίκτυο.

Η εισαγωγή ενός συμβολαίου διαχείρισης συσκευών, σε ένα δίκτυο Blockchain, προσφέρει ανθεκτικότητα και καλύτερο έλεγχο εντός του δικτύου. Μπορεί να δώσει απαντήσεις σε ερωτήματα όπως το ποιοι είναι οι έγκυροι κόμβοι του δικτύου,

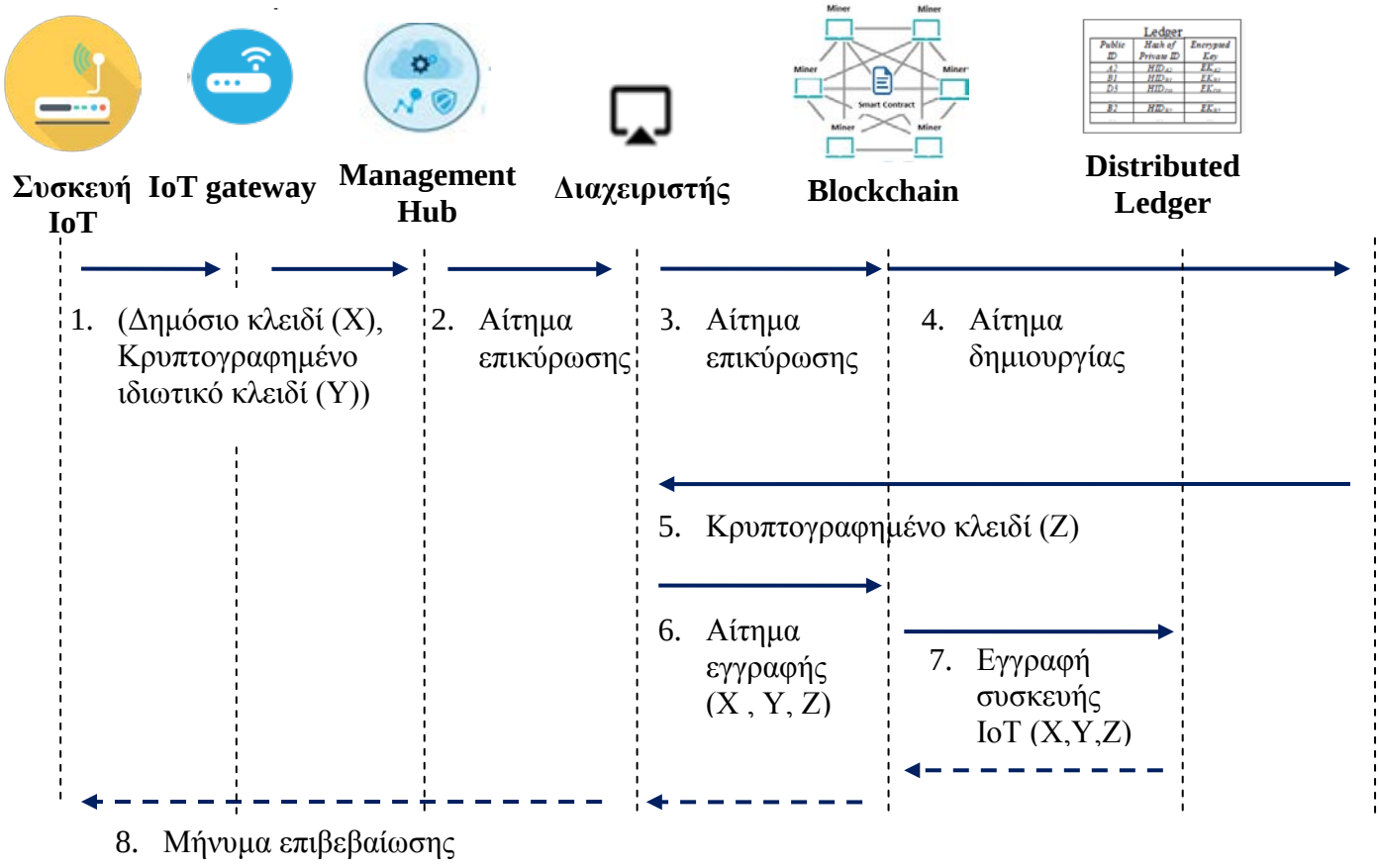
πότε ένας νέος κόμβος θεωρείται έγκυρος, αν ένας κόμβος έχει εγκαταλείψει το δίκτυο κ.λπ. Επίσης, η αξιοποίηση συστημάτων και πρωτοκόλλων διαχείρισης ψηφιακών ταυτοτήτων, πρόκειται να ενισχύσει ακόμη περισσότερο την ασφάλεια σε ένα δίκτυο αυτής της φιλοσοφίας.

3.3.2 Διαχείριση ψηφιακών ταυτοτήτων

Στην περίπτωση όπου μία συσκευή είναι συνδεδεμένη στο Διαδίκτυο, και υπάρχει ανάγκη να συνδεθεί με το δίκτυο Blockchain. Για να είναι εφικτή η επικοινωνία της συσκευής με το δίκτυο Blockchain, πρέπει να επικοινωνήσει με το IoT gateway, το οποίο θα μεταφέρει το αίτημα σύνδεσης της συσκευής προς το αντίστοιχο Management hub. Τότε το hub, θα μεταφράσει το αίτημα εγγραφής που έχει παραλάβει, και θα το στείλει στον αντίστοιχο διαχειριστή ο οποίος εξυπηρετεί την συγκεκριμένη συσκευή. Στην συνέχεια, πρέπει να γίνει πιστοποίηση της ταυτότητας της συγκεκριμένης συσκευής.

Για σκοπούς ταυτοποίησης ενός χρήστη/ συσκευής, τα συστήματα Know Your Customer (KYC), χρησιμοποιούνται με σκοπό να επαληθεύσουν την ταυτότητα κάθε χρήστη του δικτύου. Ο διαχειριστής, ζητά το μοναδικό αναγνωριστικό της συσκευής (δημόσιο κλειδί), ώστε να μπορεί να γίνει ταυτοποίηση. Εάν η συγκεκριμένη συσκευή, έχει τα κατάλληλα κλειδιά (από τον κατασκευαστή), τότε τα στέλνει στον αντίστοιχο διαχειριστή. Σε αυτό το σημείο, ο ρόλος του KYC, σε συνεργασία με το έξυπνο συμβόλαιο, είναι να ενεργοποιήσει τον μηχανισμό επικύρωσης της ταυτότητας της συσκευής, προσδιορίζοντας αν το αναγνωριστικό το οποίο έχει λάβει, είναι αυθεντικό, και ανήκει σε κάποιο χρήστη. Στην συνέχεια επιβεβαιώνεται εάν ο χρήστης πίσω από την συναλλαγή είναι όντως ο ιδιοκτήτης του αναγνωριστικού. Ακόμη, έχει την δυνατότητα να εισάγει στο δίκτυο, δεδομένα τα οποία μπορούν να αποθηκευτούν για την ταυτοποίηση της συγκεκριμένης συσκευής. Κάθε συσκευή IoT, καλείται να στείλει το δημόσιο κλειδί της, το κωδικοποιημένο ιδιωτικό κλειδί της και ίσως άλλες πληροφορίες που πιθανόν να υπάρχει ανάγκη να αποθηκευτούν (πχ. πληροφορίες για τον κατασκευαστή) ώστε να μπορεί να γίνει πιστοποίηση οποιαδήποτε στιγμή. Εφόσον η νέα συσκευή πιστοποιηθεί, τότε παράγεται ένα νέο κλειδί, το οποίο κρυπτογραφείται, και μαζί με το δημόσιο και ιδιωτικό κλειδί, η νέα συσκευή καταγράφεται στο Blockchain.

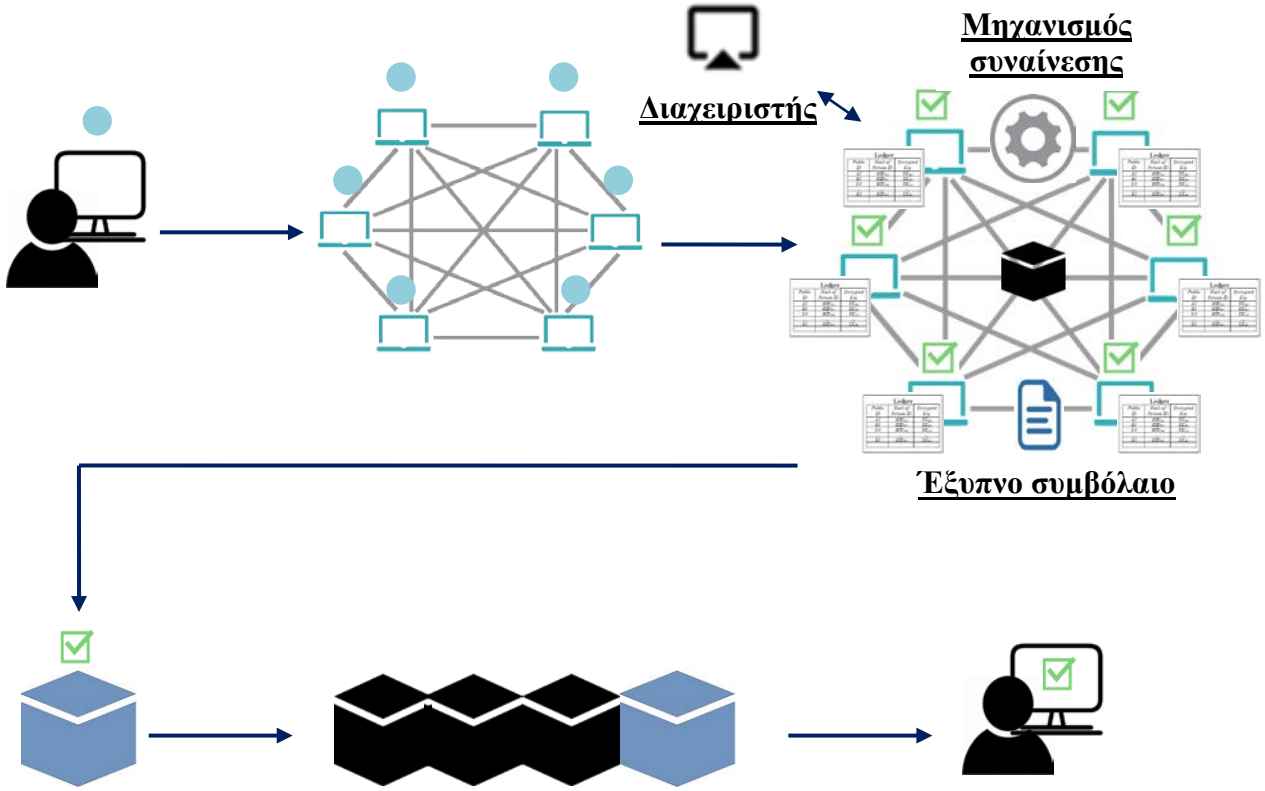
Επίσης, ένα σύστημα KYC, χρησιμοποιείται για την παρακολούθηση του δικτύου καθώς και την αξιολόγηση της καταλληλότητας των χρηστών του. Οι βασικές λειτουργίες των συστημάτων KYC, είναι η συλλογή πληροφοριών αναγνώρισης, ο έλεγχος στοιχείων ταυτοποίησης με σκοπό τον προσδιορισμό της κατάστασης του δικτύου. Επίσης γίνεται αξιολόγηση των χρηστών του δικτύου και μελετούνται πιθανοί κίνδυνοι οι οποίοι μπορεί να συμβούν, όσο αφορά τους χρήστες του δικτύου (πχ. κλοπή της ψηφιακής ταυτότητας, κλοπή δεδομένων). Συνήθως, συστήνεται η παρακολούθηση των συναλλαγών ενός χρήστη, ώστε να εξασφαλιστεί η σωστή χρήση των υπηρεσιών του δικτύου.



Σχήμα 1.16: Διαδικασία σύνδεσης συσκευών στο Blockchain.

Η τεχνολογία Blockchain, σε συνεργασία με ένα σύστημα διαχείρισης ψηφιακών ταυτοτήτων (KYC), δίνει την δυνατότητα για την εκτέλεση συναλλαγών σε παγκόσμιο επίπεδο. Πριν την εκτέλεση μίας συναλλαγής, ο ρόλος του συστήματος KYC, είναι να επαληθεύσει την εγκυρότητα των συσκευών που λαμβάνουν μέρος. Όταν το αίτημα έγκρισης της συναλλαγής, διανεμηθεί στους κόμβους του Blockchain, τότε ενεργοποιούνται αυτόματα λειτουργίες του έξυπνου συμβολαίου, μέσω των οποίων θα αποφασιστεί κατά πόσο μια συναλλαγή είναι έγκυρη. Ακολούθως, οι κόμβοι

miners καλούνται να συναινέσουν στην εκτέλεση της συναλλαγής (μέσω των αλγόριθμων συναίνεσης), και τότε ελέγχεται κατά πόσο πληρούνται οι κανονισμοί οι οποίοι περιλαμβάνονται στο έξυπνο συμβόλαιο. Εφόσον ο έλεγχος ολοκληρωθεί επιτυχώς, τότε η συναλλαγή καθίσταται έγκυρη. Επίσης όταν μία συναλλαγή πιστοποιηθεί, τότε καταγράφεται στο Blockchain ledger και ένα αντίγραφο του ενημερωμένου πλέον ledger, διανείμετε στους κόμβους του δικτύου. Στην συνέχεια δημιουργείται ένα μπλοκ, το οποίο αντιστοιχεί στην συγκεκριμένη συναλλαγή και ακολούθως ενσωματώνεται στο υφιστάμενο Blockchain. Σε αντίθετη περίπτωση, η συγκεκριμένη συναλλαγή απορρίπτεται.



Σχήμα 1.17: Πώς λειτουργεί ένα Blockchain.

Σημαντικός είναι και ο ρόλος των πρωτόκολλων σύνδεσης στην διαδικασία ταυτοποίησης των χρηστών του δικτύου, σε συνεργασία με τεχνικές κρυπτογράφησης και των μοναδικών αναγνωριστικών κλειδιών τους. Όταν δοθεί ένα αναγνωριστικό κλειδί σε μια συνδεδεμένη συσκευή, τότε αυτόματα αντιστοιχούνται σε αυτό συγκεκριμένα δικαιώματα στο δίκτυο. Όταν μία συσκευή, αποκτήσει τα 'κλειδιά πρόσβασης', τότε εξασφαλίζεται ότι για κάθε συναλλαγή στην οποία εμπλέκεται,

πρόκειται για ένα έγκυρο χρήστη του δικτύου. Για κάθε κλειδί υπάρχει ένα συγκεκριμένο χρονικό περιθώριο στο οποίο θεωρείτε έγκυρο.

Για την επικοινωνία δύο κόμβων του δικτύου, ο αποστολέας στέλνει το κρυπτογραφημένο μήνυμα του μαζί με το μοναδικό αναγνωριστικό του στον παραλήπτη. Τότε γίνεται επαλήθευση του μοναδικού αναγνωριστικού του αποστολέα μέσω της δημόσιας υποδομής που προσφέρει η τεχνολογία Blockchain. Εάν όντως αποτελεί έγκυρο χρήστη, και αν όντως επιβεβαιωθεί, το χρησιμοποιεί ώστε να ανακτήσει το δημόσιο κλειδί του αποστολέα, και στην συνέχεια να αποκωδικοποιήσει το μήνυμα του. Η τεχνολογία Blockchain χρησιμοποιεί 'επαληθεύσιμα πιστοποιητικά', τα οποία καθορίζουν και επαληθεύουν την ανταλλαγή ψηφιακών πληροφοριών. Τα πιστοποιητικά επαλήθευσης, χρησιμοποιούν τεχνικές κρυπτογράφησης και πρωτόκολλα, μέσω των οποίων επιτρέπεται η ασφαλής ανταλλαγή κλειδιών μεταξύ των κόμβων του δικτύου. Να σημειωθεί ότι για να μπορεί να γίνει ανταλλαγή κλειδιών, πρέπει να έχουν δοθεί στους εμπλεκόμενους κόμβους, τα ανάλογα δικαιώματα. Επίσης σημαντικός παράγοντας αποτελεί και ο τύπους του Blockchain, όσο αφορά τους περιορισμούς που πιθανό να υπάρχουν στο δίκτυο.

Ένα δίκτυο Blockchain επιτρέπει την δημιουργία αναγνωριστικών ταυτοτήτων. Κάθε ταυτότητα ανήκει αποκλειστικά σε ένα χρήστη, και χρησιμοποιείται για την επαλήθευση της αυθεντικότητας των χρηστών του δικτύου. Κάθε ταυτότητα βρίσκεται κάτω από τον έλεγχο του ιδιοκτήτη, οργανισμού ή συσκευής. Για κάθε συναλλαγή η οποία συμβαίνει στο δίκτυο, συσχετίζονται με αυτή οι μοναδικές ταυτότητες των εμπλεκόμενων χρηστών που έλαβαν μέρος. Τα δικαιώματα πρόσβασης τα οποία θα δοθούν σε μία συσκευή, βασίζονται στον ρόλο που έχουν στο δικτύου. Οι συσκευές αναλαμβάνουν προκαθορισμένους ρόλους, στους οποίους αντιστοιχούν συγκεκριμένα δικαιώματα και ένα σύνολο συναλλαγών που μπορούν να εκτελέσουν στα πλαίσια του δικτύου.

3.3.3 Διαχείριση κατάστασης συσκευής

Όσο αφορά τις καταστάσεις στις οποίες μπορεί να βρεθεί μια συσκευή, η διαχείρισης της, μπορεί να χωριστεί σε τρείς περιπτώσεις. Πιο κάτω, επεξηγούνται οι καταστάσεις στις οποίες μπορεί να βρεθεί μία συσκευή και πώς ακριβώς η τεχνολογία Blockchain σε συνεργασία με ένα έξυπνο συμβόλαιο, μπορεί να τις αντιμετωπίσει.

3.3.3.1 Είσοδος μίας συσκευής στο δίκτυο

Μέσω της έξυπνης σύμβασης που βρίσκεται στο Blockchain, επιβεβαιώνεται εάν αυτός ο κόμβος πληροί τις απαραίτητες προϋποθέσεις ώστε να εισέλθει στο δίκτυο. Εάν όντως πληρούνται οι απαραίτητες προϋποθέσεις, τότε δίνονται τα ανάλογα δικαιώματα στον κόμβο, και στην συνέχεια καταγράφεται στο κατανεμημένο κατάστιχο, η νέα εισαγωγή. Αυτή η πληροφορία μεταδίδεται στο δίκτυο ώστε όλοι οι κόμβοι, να ενημερωθούν για την ανανεωμένη εικόνα του δικτύου. Αυτή είναι η τυπική διαδικασία που ακολουθείται για κάθε νέο κόμβο ο οποίος πρόκειται να εισαχθεί στο δίκτυο σε μεταγενέστερη φάση. Οι έλεγχοι οι οποίοι εκτελούνται αυτόματα μέσω του έξυπνου συμβολαίου, φαίνεται ότι ενισχύουν την διαδικασία διαχείρισης των συσκευών, και γενικότερα των διαδικασιών του δικτύου.

Στην περίπτωση των δημόσιων Blockchain, δίνεται η δυνατότητα σε οποιαδήποτε συσκευή, να στείλει αίτημα πρόσβασης στο δίκτυο ώστε να αποκτήσει τα ‘κλειδιά πρόσβασης’. Στην συνέχεια, αφού επικυρωθεί ο νέος κόμβος, τότε αποστέλλονται σε αυτό, τα κλειδιά πρόσβασης και μια μοναδική ψηφιακή υπογραφή.

Στην περίπτωση των ιδιωτικών Blockchain, το δίκτυο στέλνει αίτημα στις συσκευές, για πρόσβαση σε αυτό. Για να μπορεί η νέα συσκευή να επικοινωνήσει με το δίκτυο Blockchain, πρέπει να στείλει το ανάλογο αίτημα στο IoT gateway, στην συνέχεια το gateway, θα στείλει ένα μήνυμα στο Management Hub, και τέλος το hub θα στείλει αίτημα εισδοχής της συσκευής , στην διεύθυνση του δικτύου Blockchain, και συγκεκριμένα στην διεύθυνση του έξυπνου συμβολαίου.

Στην περίπτωση που ένας υφιστάμενος κόμβος, θέλει να μάθει πληροφορίες για την κατάσταση του δικτύου, τότε θα στείλει το ανάλογο αίτημα στο έξυπνο συμβόλαιο. Τότε μέσω του έξυπνου συμβολαίου επιβεβαιώνει ότι το αίτημα έχει σταλεί από ένα έγκυρο εγγεγραμμένο κόμβο του δικτύου, το αίτημα επιβεβαιώνεται και τότε αποστέλλονται σε αυτό, οι πληροφορίες που έχει ζητήσει.

3.3.3.2 Περίοδος αδράνειας μίας συσκευής

Σε ένα έξυπνο συμβόλαιο, περιλαμβάνονται επίσης μηχανισμοί μέσω των οποίων επιβεβαιώνεται εάν ένας χρήστης είναι ενεργός ή όχι. Πρόκειται για αυτοματοποιημένα μηνύματα τα οποία στέλνονται σε όλους τους κόμβους του δικτύου, ανά τακτά χρονικά διαστήματα με σκοπό να επιβεβαιωθεί εάν υφίστανται στο δίκτυο.

Στις νέες τεχνολογίες, χρησιμοποιούνται μηχανισμοί ελέγχου των μερών ενός δικτύου, μέσω των οποίων ελέγχονται καταστάσεις είτε λειτουργίας είτε αδράνειας μιας συσκευής, είτε ολόκληρου του συστήματος. Επίσης κατά την διαδικασία ελέγχου, τα μέρη παρέχουν πληροφορίες για την κατάσταση τους, ώστε ανά πάσα στιγμή, να είναι γνωστό ποια μέρη του δικτύου είναι ενεργά και ποια όχι.

Στην περίπτωση αδράνειας μιας συσκευής, η συσκευή δεν ανταποκριθεί στο μήνυμα ελέγχου λειτουργικότητας. Τότε μέσω του έξυπνου συμβολαίου, θα σταλεί συγκεκριμένος αριθμός μηνυμάτων, σε διάστημα το οποίο έχει προκαθοριστεί από πριν ώστε επιβεβαιωθεί η λειτουργικότητα της συσκευής. Όταν η συσκευή είναι σε θέση να επανασυνδεθεί με το δίκτυο, τότε θα στείλει αίτημα για την επανασύνδεση της. Η συσκευή θα προσπαθήσει να ενωθεί σε ένα κόμβο του δικτύου, και τότε οι κόμβοι miners σε συνεργασία με την αντίστοιχη διαδικασία του έξυπνο συμβόλαιο, πρέπει να επιβεβαιώσουν την σύνδεση της, ώστε να μπορεί να έχει και πάλι πρόσβαση. Στην περίπτωση που δεν απαντήσει στα μηνύματα του δικτύου, τότε ο διαχειριστής ο οποίος προσπάθησε να επικοινωνήσει με την συσκευή, πρέπει να ενημερώσει ότι η συγκεκριμένη συσκευή έχει φύγει από το δίκτυο.

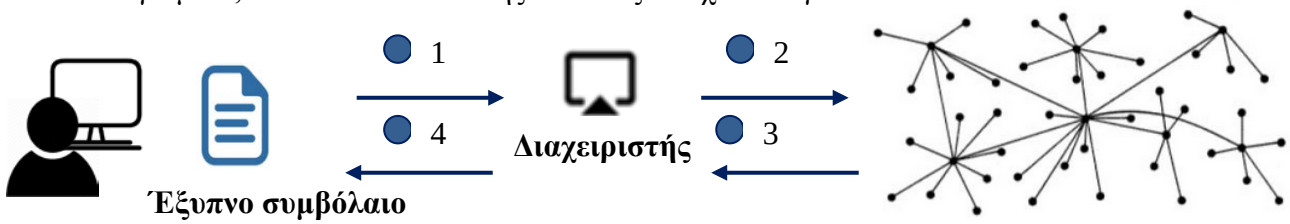
3.3.3.3 Έξοδος συσκευής από το δίκτυο

Επίσης, μέσω των έξυπνων συμβολαίων δίνεται η δυνατότητα ενεργοποίησης διαδικασιών, μέσω των οποίων επιβεβαιώνεται εάν ένας κόμβος έχει εγκαταλείψει το δίκτυο. Εάν η διαδικασία ολοκληρωθεί, και ο κόμβος δεν ανταποκριθεί μέσα σε προκαθορισμένο χρονικό διάστημα, τότε επιβεβαιώνεται ότι ο συγκεκριμένος κόμβος δεν υπάρχει πλέον στο δίκτυο. Τότε ο αντίστοιχος διαχειριστής ο οποίος προσπάθησε να επικοινωνήσει με τον συγκεκριμένο χρήστη, ενημερώνει το ledger του δικτύου Blockchain για την αλλαγή, και στην συνέχεια αντίγραφο του Blockchain διαδίδεται στο δίκτυο.

3.3.4 Κατακερματισμός λογισμικού συσκευών και κατανομή ενημερώσεων λογισμικού στις συσκευές IoT

Όπως έχει αναφερθεί, εξαιρετικά σημαντική κρίνεται και η συνεργασία της τεχνολογίας Blockchain, με τα έξυπνα συμβόλαια, όσο αφορά την διαχείριση και διάδοση των ενημερώσεων λογισμικού των συσκευών IoT. Ας υποθέσουμε ότι οι συσκευές IoT συνδέονται με επιτυχία στο δίκτυο Blockchain. Τότε αποκτούν ένα μοναδικό λογαριασμό στην υποδομή. Ο κατασκευαστής των συσκευών, εισάγει το λογισμικό των συσκευών IoT στην υποδομή. Επίσης, ο κατασκευαστής αναπτύσσει και εισάγει στο δίκτυο, ένα έξυπνο συμβόλαιο, μέσω του οποίου θα γίνεται η διαχείριση του λογισμικού των συσκευών.

Όπως και στην περίπτωση στην οποία μία έγκυρη συναλλαγή αποθηκεύεται εντός του δικτύου, έτσι και όταν το λογισμικό μίας συσκευής εισάγεται στο Blockchain, τότε αποκτά μία μοναδική διεύθυνση (δημόσιο κλειδί). Μέσω των τεχνικών κρυπτογράφησης που χρησιμοποιεί η τεχνολογία Blockchain, εξασφαλίζεται ότι δεν μπορεί να γίνει οποιαδήποτε αλλαγή στον κωδικό hash, του λογισμικού. Εάν για οποιοδήποτε λόγο, ο κωδικός hash του λογισμικού αλλάξει, αυτό σημαίνει ότι θα υπάρξει πρόβλημα στην διαδικασία κατακερματισμού των μπλόκς της αλυσίδας. Τότε, αυτόματα ενεργοποιείται η αντίστοιχη διαδικασία του έξυπνου συμβολαίου, η οποία ενημερώνει τους ιδιοκτήτες των συσκευών, στις οποίες τρέχει το συγκεκριμένο λογισμικό, και ο κατασκευαστής ο οποίος το έχει εισάγει.



Κατασκευαστής Χ

Ο κατασκευαστής των συσκευών, προσδιορίζει την ταυτότητα του, μέσω της διεύθυνσης Blockchain (το δημόσιο κλειδί του), και χρησιμοποιεί ένα έξυπνο συμβόλαιο, μέσω του οποίου καθορίζονται οι όροι διαχείρισης του λογισμικού. Τέλος, το 'υπογράφει', με το ιδιωτικό του κλειδί.

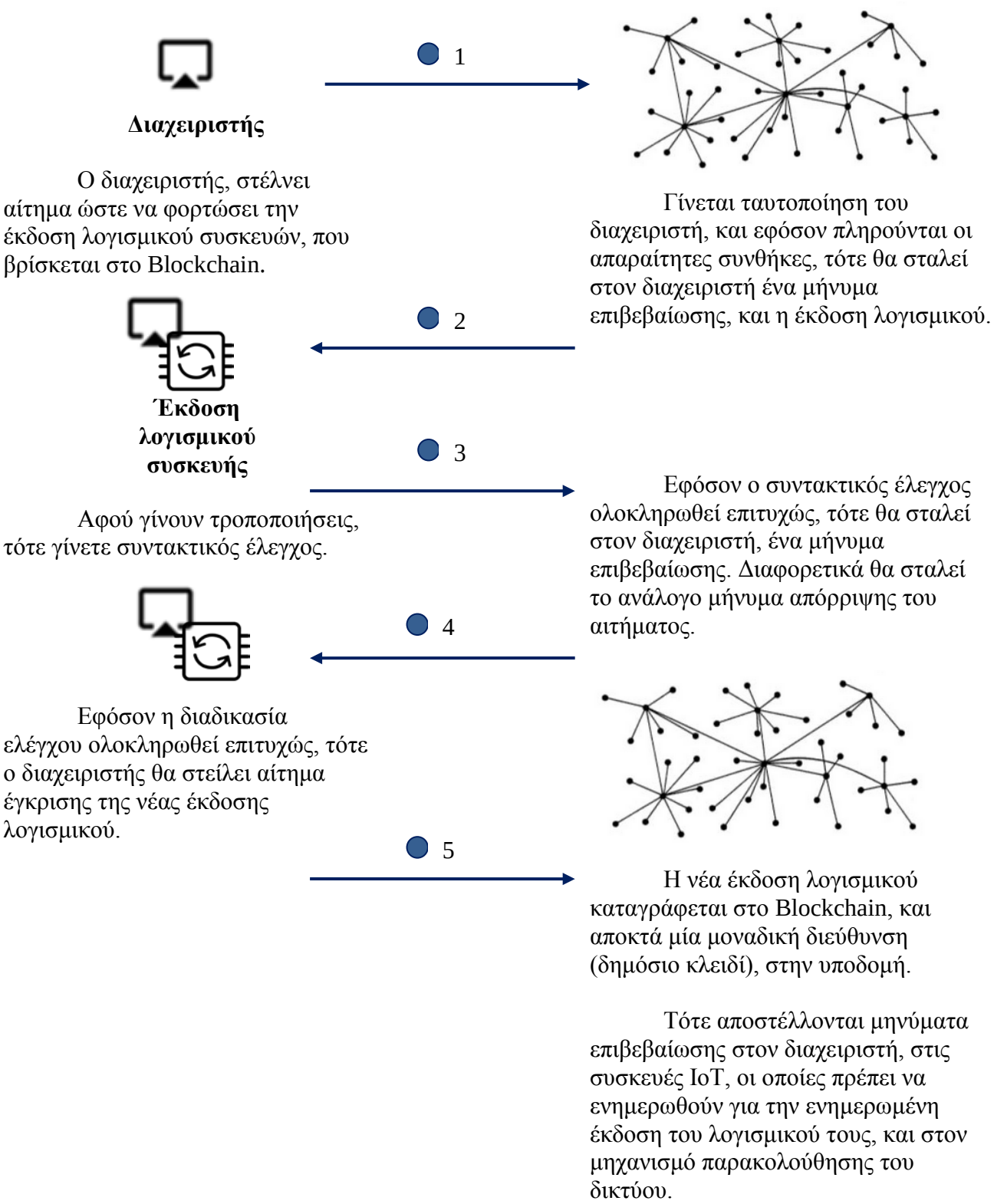
Το λογισμικό, αποκτά μία διεύθυνση Blockchain (δημόσιο κλειδί), και αποθηκεύεται στο Blockchain. Να σημειωθεί ότι, το λογισμικό συσκευών, χειρίζεται μέσω του έξυπνου συμβολαίου.

Στην συνέχεια αποστέλλεται στον κατασκευαστή, η διεύθυνση του λογισμικού στο Blockchain ώστε να ενημερωθούν και οι αντίστοιχες συσκευές.

Σχήμα 1.18: Διαχείριση λογισμικού συσκευών μέσω έξυπνου συμβολαίου [Προσαρμοσμένη εικόνα από 34, 73].

Μέσω του έξυπνου συμβολαίου, από την πλευρά του κατασκευαστή, δίνεται η δυνατότητα ελέγχου των διαδικασιών φόρτωσης, τροποποίησης λογισμικού και διάδοσης ενημερώσεων. Από την πλευρά των συσκευών IoT, η έξυπνη σύμβαση έχει σημαντικό ρόλο, όσο αφορά τον έλεγχο των διαδικασιών διαβάσματος, και εγγραφής ενημερώσεων λογισμικού των συσκευών. Επίσης και στις δύο περιπτώσεις, όταν οι έλεγχοι ολοκληρωθούν με επιτυχία, το έξυπνο συμβόλαιο στέλνει αυτοματοποιημένα μηνύματα επιβεβαίωσης.

Ο κατασκευαστής των συσκευών IoT, εξουσιοδοτεί διαχειριστές του δικτύου ώστε να έχουν την δυνατότητα τροποποίησης λογισμικού, που βρίσκεται αποθηκευμένο στο Blockchain. Βέβαια, αυτό μπορεί να γίνει μόνο για συσκευές IoT στις οποίες έχει δικαίωμα. Επομένως, αφού γίνει η ταυτοποίηση τους μέσω των ψηφιακών αναγνωριστικών τους, τότε μπορούν να προχωρήσουν στην μετατροπή. Στην συνέχεια, γίνεται συντακτικός έλεγχος της τροποποιημένης έκδοσης. Εφόσον ο έλεγχος ολοκληρωθεί επιτυχώς, τότε η διαμορφωμένη πλέον έκδοση λογισμικού, καταγράφεται στο Blockchain, και ακολούθως ενημερώνονται οι κόμβοι του δικτύου.

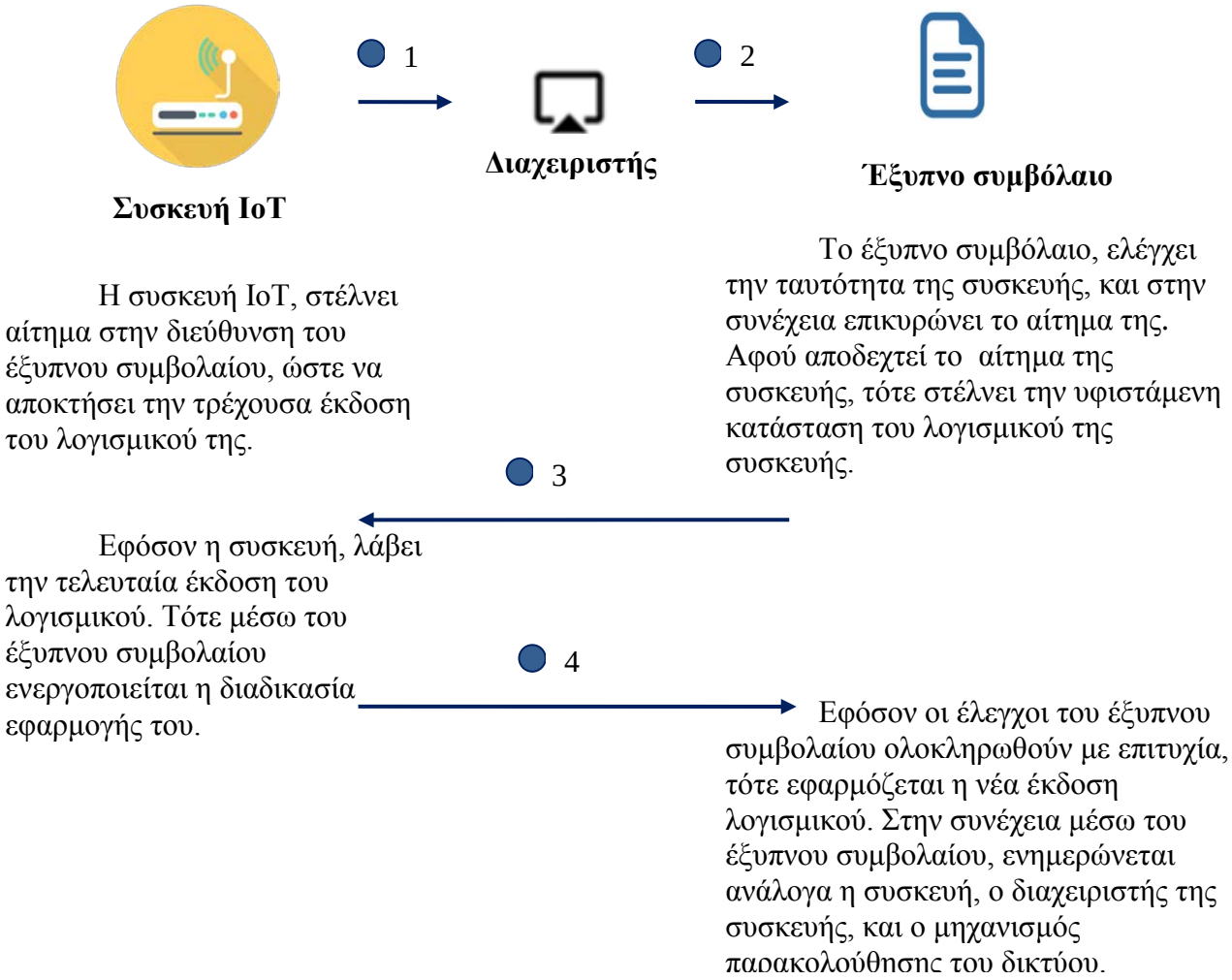


Σχήμα 1.19: Κατακερματισμός και διάδοση της έκδοσης λογισμικού συσκευών μέσω έξυπνου συμβολαίου [Προσαρμοσμένη εικόνα από 34, 73].

Μέσω των τεχνικών κρυπτογράφησης που χρησιμοποιούνται, αντιστοιχείτε ένας μοναδικός κωδικός hash, στην τελευταία έκδοση του λογισμικού που βρίσκεται στο Blockchain. Αυτό σημαίνει ότι, μια συσκευή IoT, μπορεί να στείλει αίτημα στην

διεύθυνση του έξυπνου συμβολαίου ώστε να μάθει την τελευταία έκδοση του λογισμικού της. Στην συνέχεια, γίνετε ταυτοποίηση της συγκεκριμένης συσκευής, και του ιδιοκτήτη του λογισμικού. Εάν και εφόσον, οι κόμβοι του δικτύου συναινούν, και πληρούνται όλες οι προϋποθέσεις οι οποίες συμπεριλαμβάνονται στο έξυπνο συμβόλαιο, τότε δίνετε πρόσβαση στην διεύθυνση του λογισμικού στο Blockchain. Τότε καταγράφεται ότι η συγκεκριμένη συσκευή είχε πρόσβαση στην συγκεκριμένη διεύθυνση στο Blockchain, και τότε μπορεί να έχει πρόσβαση στο ίδιο το λογισμικό, χρησιμοποιώντας το ιδιωτικό κλειδί της.

Να σημειωθεί ότι, το ιδιωτικό Blockchain, θεωρείτε η καλύτερη επιλογή, επειδή λόγω των περιορισμών που προσφέρει, εξασφαλίζεται η ασφαλής διάδοση αλλαγών διαμόρφωσης στους κόμβους του δικτύου.



Σχήμα 1.20: Διάδοση ενημερώσεων στις συσκευές IoT [Προσαρμοσμένη εικόνα από 34, 73].

Κεφάλαιο 4

4 ΕΠΙΛΟΓΟΣ

4.1 Συμπεράσματα

Συνοψίζοντας, μιλώντας για την τεχνολογία Blockchain, πρόκειται για μία αδιαμφισβήτητα υποσχόμενη τεχνολογία. Αν και ήδη έχει ήδη βελτιώσει σημαντικά πολλούς τομείς της τεχνολογίας. Οι εφαρμογές είναι αρκετές, και το σίγουρο είναι ότι τις έχει εξελίξει σε άλλο επίπεδο, συγκριτικά με τα δεδομένα του παρελθόντος.

Θεωρώ ότι η τεχνολογία Blockchain σε συνδυασμό με ένα ισχυρό μηχανισμό όπως τα έξυπνα συμβόλαια, μπορεί να αντιμετωπίσει διάφορα ζητήματα με τα οποία έρχεται αντιμέτωπο το Διαδίκτυο των Πραγμάτων. Θεωρώ ότι είναι εφικτό να γίνει εφαρμογή της σε ένα IoT περιβάλλον, και αυτό μπορεί να γίνει ιεραρχικά. Δηλαδή ξεκινώντας με μικρότερου μεγέθους εφαρμογές όπως σε ένα έξυπνο σπίτι, σε μία έξυπνη πόλη και στην συνέχεια σε πιο μεγάλα δίκτυα. Σαφώς υπάρχουν και θα περιορισμοί και από την πλευρά της τεχνολογίας απόδοση αυτού του τύπου εφαρμογών. Όμως, ορίζοντας τα δεδομένα και τις απαιτήσεις που πιθανόν να έχει μία τέτοια εφαρμογή, μπορούμε να έχουμε πολύ καλά αποτελέσματα. Από την πλευρά των έξυπνων συμβολαίων, θεωρώ ότι μπορούν να αυξήσουν την απόδοση και την ποιότητα των υπηρεσιών που προσφέρει αυτή η συνεργασία. Το σίγουρο είναι ότι μπορεί να μειώσει το ρίσκο αρκετών ζητημάτων να μειώσει τα κόστη και να δώσει μία άλλη μορφή σε επιχειρησιακά μοντέλα.

Σε ένα κόσμο ο οποίος καθοδηγείται από την πληροφορία, αναμένεται ότι θα συνεχής προκλήσεις. Γι αυτό πρέπει να λάβουμε υπόψη συμβιβασμούς και περιορισμούς των διαφορετικών τεχνολογιών, ώστε να λάβουμε το καλύτερο δυνατό αποτέλεσμα.

Βιβλιογραφία

Βιβλιογραφία

[1] A.Antonopoulos, "The Blockchain" *in Mastering Bitcoin* (2014) Sebastopol, CA, USA, O'Reilly Media, Inc, 2014

[2] A.Dorri,S. Kanhere, R. Jurdak, P.Gauravaram, "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home", presented at IEEE Percom Workshop on Security Privacy and the Internet of Things, March 2017, doi: 10.1109/PERCOMW.2017.7917634

[3] A. Dorri, S. Kanhere, R. Jurdak "Blockchain in Internet of Things: Challenges and Solutions", availiable : https://arxiv.org/ftp/arxiv/papers/1608/1608.05187.pdf

[4] A.Dorri, S. Kanhere, R.Jurdak, "Towards an Optimized Blockchain for Iot", in 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), April 2017, available: https://ieeexplore.ieee.org/document/7946872

[5] A.Reyna, C.Martín, J.Chen, E.Soler, M. Díaz, " On blockchain and its integration with IoT. Challenges and opportunities", Future Generation Computer Systems, vol.88, p.173-190, November 2018, doi: 10.1016/j.future.2018.05.046

[6] B.Asolo, "Consortium Blockchain Explained", November 2018, https://www.mycryptopedia.com/consortium-blockchain-explained/

[7] B. Mandrita, L.Junghee, R.Choo, K.Kwang "A blockchain future to Internet of Things security: A position paper" ,Digital Communications and Networks. vol.4, issue 3, p.149-160, August 2018 , doi : 10.1109/PERCOMW.2017.7917634.

[8] B.Vitalk, "A Next Generation Smart Contract & Decentralized Application Platform", (*2013),* availiable: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[9] C.Albert, "Problems With the Internet of Things You Need to Know!", June 2018 https://dzone.com/articles/problems-with-internet-of-things-you-need-to-know

[10] J.Frankenfield, "Proof of Work", April 2014, https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp

[11] J.Garay, N.Leonardos, A. Kiayias, "The Bitcoin Backbone Protocol: Analysis and Applications", Advances in Cryptology - EUROCRYPT 2015, Sofia, Bulgaria, April 2015, Proceedings, Part II, doi: 10.1007/978-3-662-46803-6_10

[12] K.Radhakrishnan, "CryptoCurrency—"Proof of Work" Vs "Proof of Stake"", April 2017 https://medium.com/@karthik.seshu/cryptocurrency-proof-of-work-vs-proof-of-stake-e1eee1420b10

[13] L.Zhechev, "What Is Ethereum Classic (ETC)? A Smart Contract Platform Betting on the "Code is Law" Philosophy", July 2018 https://cryptovest.com/reviews/what-is-ethereum-classic-etc-a-smart-contract-platform-betting-on-the-code-is-law-philosophy/

[14] M.A.Ferrag, M.Derdour, M.Mukherjee, A.Derhab, L.A.Maglaras, H.Janicke, "Blockchain Technologies for the Internet of Things: Research Issues and Challenges", *CoRR, abs/1806.09099*, 24 June 2018, doi: 10.1109/JIOT.2018.2882794

[15] M.Kramer, "Ethereum Casper Update Expected in 2019, Sharding in 2020", July 2018, https://unhashed.com/cryptocurrency-news/ethereum-sharding-update-expected-2020/

[16] M.Rouse, "Consensus Algorithm", August 2017, https://whatis.techtarget.com/definition/consensus-algorithm

[17] M.Thake, "What is Proof of Stake? (PoS)", July 2018, https://medium.com/nakamo-to/what-is-proof-of-stake-pos-479a04581f3a

[18] N.M.Kumar, P. Kumar Mallick, " Blockchain Technology for security issues and challenges in IoT", Procedia Computer Science, vol.132, p. 1815-1823, 2018, doi: 10.2016/j.procs.2018.05.140

[19] N.Marinoff, "Cardano Shares Information On Its Proof-Of-Stake Protocol", October 2018, https://www.investinblockchain.com/cardano-proof-of-stake/

[20] O.Faridi, "What is Proof of Work?", July 2018 https://www.cryptocompare.com/mining/guides/what-is-proof-of-work/

[21] S.Khatwani, "9 Most Profitable Proof Of Stake (POS) Cryptocurrencies", October 2018, https://coinsutra.com/proof-of-stake-cryptocurrencies/

[22] S.Mohammed, "Public VS Private Blockchain", August 2018, https://hackernoon.com/public-vs-private-blockchain-4b4aa9326168

[23] S.Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", (2008) https://bitcoin.org/bitcoin.pdf

[24] T.Kumar Sharma, "Advantages and disadvantages of permissionless blockchain", www.blockchain-council.org, https://www.blockchain-council.org/blockchain/advantages-and-disadvantages-of-permissionless-blockchain/

[25] T.M. Fernández-Caramés, P.Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," IEEE Xplore Digital Library, May 31, 2018, doi: 10.1109/ACCESS.2018.2842685.

[26] T. Schumann, "Consensus Mechanisms Explained: PoW vs. PoS", April 2018, https://hackernoon.com/consensus-mechanisms-explained-pow-vs-pos-89951c66ae10

[27] Y.Khaidukova,"Differences and advantages of public and private blockchains", July 2017, https://altabel.wordpress.com/2017/07/25/differences-and-advantages-of-public-and-private-blockchains/

[28] Z.Witherspoon, "A Hitchhiker's Guide to Consensus Algorithms"**,** https://hackernoon.com/a-hitchhikers-guide-to-consensus-algorithms-d81aae3eb0e3

[29] D. Annamalai, "Blockchain – What is Permissioned vs Permissionless?", Available: https://bornonjuly4.me/2017/01/10/blockchain-what-is-permissioned-vs-permissionless/, (accessed Feb. 1, 2019).

[30] "What is the Blockchain data structure?", November 2018, Available: https://cryptoticker.io/en/blockchain-data-structure/

[31] "How Blockchain Technology Works. Guide for Beginners", COINTELEGRAPH.com, Available: https://cointelegraph.com/bitcoin-for-beginners/how-blockchain-technology-works-guide-for-beginners, (accessed Jan. 1, 2019).

[32] Centre for Development of Advanced Computing, "Peer to peer network", INFOSECAWARENESS.in, Available: https://www.infosecawareness.in/peer-to-peer-network

[33] "Proof of Work vs Proof of Stake: Basic Mining Guide", BLOCKGEEKS.com, Available: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

[34] "Smart Contracts", BLOCKCHAINHUB.net, Available: https://blockchainhub.net/smart-contracts/, (accessed Jan. 8, 2019).

[35] "Smart Contracts: The Blockchain Technology That Will Replace Lawyers", BLOCKGEEKS.com, Available: https://blockgeeks.com/guides/smart-contracts/, (accessed Jan. 8, 2019).

[36] “What is Blockchain Technology? A Step-by-Step Guide For Beginners”, BLOCKGEEKS.com, Available: https://blockgeeks.com/guides/what-is-blockchain-technology/, (accessed Jan. 8, 2019).

[37] Akyildiz, I., Su, W., Sankarasubramaniam, Y. and Cayirci, E. (2002). “A Survey on Sensor Networks”. *IEEE Communications Magazine*, Vol. 40, No. 8, pp. 102 – 114.

[38] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M. (2015). “Internet of Things: A Survey on Enabling Technologies, Protocols and Applications”. *IEEE Communications Surveys & Tutorials*, Vol. 17, No. 4, pp. 2347-2376.

[39] Alpár, G., Hoepman, J. and Siljee, J. (2011). “The Identity Crisis Security, Privacy and Usability Issues in Identity Management”. *Arxiv.Org*, vol. 1101.0427, pp. 1-15.

[40] Aman, M., Sikdar, B., Chua, K. and Ali, A. (2018). “Low Power Data Integrity in IoT Systems”. *IEEE Internet of Things Journal*, Vol. 5, No. 4, pp. 3102-3113.

[41] Amro, B. (2017). “Malware Detection Techniques for Mobile Devices”. *International Journal of Mobile Network Communications & Telematics* (IJMNCT), Vol.7, No.4/5/6.

[42] Antonopoulos, A., Kapatsori, C. and Makris, Y. (2018). “Hardware Trojans in Analog, Mixed-Signal, and RF ICs”. In The Hardware Trojan War, pp.101-123, Doi: 10.1007/978-3-319-68511-3_5

[43] Dhumane, A. and Prasad, R. (2015). “Routing Challenges in Internet of Things”. *CSI Communications*, January, pp. 19-20.

[44] Dhumane, A., Prasad, R. and Prasad, J. (2016). “Routing Issues in Internet of Things: A Survey”, *Proceedings of the International Multi Conference of Engineers and Computer Scientists* (IMECS), Vol. 1, March 16 - 18, 2016, Hong Kong.

[45] Frisch, D., Reissmann, S. and Pape, C. (2017). “An Over the Air Update Mechanism for ESP8266 Microcontrollers”. *The 12th International Conference on Systems and Networks Communications* (ICSNC), October 8 – 12, Athens, Greece.

[46] G DATA (2016) “Mobile Malware Report”. Threat report: H1/2016, G DATA Software AG, Germany.

[47] Gazis, V., Gortz, M., Huber, M., Leonardi, A., Mathioudakis, K., Wiesmaier, A., Zeiger, F. and Vasilomanolakis, E. (2015). “A Survey of Technologies for the Internet of Things”. *International Wireless Communications & Mobile Computing Conference (IWCMC), Machine - to - Machine Communications*

(M2M) & Internet of Things (IoT) Workshop, Doi: 10.1109/IWCMC.2015.7289234

[48] Ghaleb, S., Subramaniam, S., Zukarnain, Z. and Muhammed, A. (2016). "Mobility management for IoT: a survey". *Journal on Wireless Communications and Networking*, Doi: 10.1186/s13638-016-0659-4

[49] ITU-T (2009). Next Generation Networks – Security. Recommendation Y.2720, ITU-T.

[50] Kvarda, L., Hnyk, P., Vojtech, L., Lokaj, Z. and Neruda, M. (2017). "Software Implementation of a Secure Firmware Update in IOT Concept", *Information and Communication Technologies and Services*, Vol. 15, No. 4, pp. 626-632.

[51] Kvarda, L., Hnyk, P., Vojtech, L., Lokaj, Z., Neruda, M. and Zitta, T. (2016). "Software Implementation of a Secure Firmware Update Solution in an IOT Context". *Information and Communication Technologies and Services*, Vol. 14, No. 4, pp. 389-396.

[52] Li, S. (2017). Chapter 4 - IoT Node Authentication. In Li, S. and Xu, L. (Eds.). *Securing the Internet of Things*, Elsevier Inc., pp. 69-95.

[53] Liu, X., Abdelhakim, M., Krishnamurthy, P. Tipper, D. (2018). "Identifying Malicious Nodes in Multihop IoT Networks using Dual Link Technologies and Unsupervised Learning". *Open Journal of Internet of Things*, Vol. 4, No. 1, pp. 109-125.

[54] Milosevic, J., Sklavos, N. and Koutsikou, K. (2016). "Malware in IoT Software and Hardware". *Workshop on Trustworthy Manufacturing and Utilization of Secure Devices* (TRUDEVICE'16), Barcelona, Spain

[55] Padilla, A., Baccelli, E., Eichinger, T. and Schleiser, K. (2016). "The Future of IoT Software Must be Updated". *IAB Workshop on Internet of Things Software Update* (IoTSU), June, Dublin, Ireland.

[56] Perumal, T., Datta, S. and Bonnet, C. (2015). "IoT Device Management Framework for Smart Home Scenarios". IEEE 4th Global Conference on Consumer Electronics (GCCE), Doi: 10.1109/GCCE.2015.7398711

[57] Poluru, R. and Naseera, S. (2017). A Literature Review on Routing Strategy in the Internet of Things. *Engineering Science and Technology Review*, Vol. 20, No. 5, pp. 50-60.

[58] Rizvi, S., Pfeffer, J., Kurtz, A. and Rizvi, M. (2018). Securing the Internet of Things (IoT): A Security Taxonomy for IoT. *12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. Doi: 10.1109/TrustCom/BigDataSE.2018.00034

[59] Sabir, M., Malik M., Ashraf, F. and Rasheed, R. (2018). Embedded IOT System: Software and Security Attacks. *International Journal of Computer Science and Network Security*, Vol.18, No.8, pp. 70-73.

[60] Sadeghi, A., Wachsmann, C. and Waidner, M. (2015). Security and Privacy Challenges in Industrial Internet of Things. *52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, 8-12 June, San Francisco, CA, USA.

[61] Schmidt, S., Tausig, M., Hudler, M. and Simhandl, G. (2016). ”Secure Firmware Update Over the Air in the Internet of Things Focusing on Flexibility and Feasibility Proposal for a Design”. *IAB Workshop on Internet of Things Software Update* (IoTSU), June, Dublin, Ireland.

[62] Umar, B., Hejazi, H., Lengyel, L. and Farkas, K. (2018). “Evaluation of IoT Device Management Tools”. The 3rd International Conference on Advances in Computation, Communications and Services, 22-26 July, Barcelona, Spain.

[63] Varghese, B., Wang, N., Barbhuiya, S., Kilpatrick, P. and Nikolopoulos, D. (2016). “Challenges and Opportunities in Edge Computing”. *IEEE International Conference on Smart Cloud*, 18-20 November, New York, NY, USA.

[64] Varghese, B. and Buyya, R. (2017). “Next generation cloud computing: New trends and research directions”. *Future Generation Computer Systems* (In press).

[65] Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A. and Kikiras, P. (2015). “On the Security and Privacy of Internet of Things Architectures and Systems”. *INTERNATIONAL Workshop on Secure Internet of Things* (SIOT 2015), Doi: 10.1109/SIOT.2015.9.

[66] Xu, L., He, W. and Li, S. (2014). “Internet of Things in Industries: A Survey”. *IEEE Transactions on Industrial informatics*, Vol. 10, No. 4, pp. 2233-2242.

[67] Yang, Y., Wu, L., Yin, G., Li, L. and Zhao, H. (2017). “A Survey on Security and Privacy Issues in Internet-of-Things”. *IEEE Internet of Things Journal*, Vol. 4, No. 5, pp. 1250-1258.

[68] Yim, S. and Choi, Y. (2012). “Neighbor-Based Malicious Node Detection in Wireless Sensor Networks”, *Wireless Sensor Network*, Vol. 12, No. 4, pp. 219-225.

[69] Yu, Y., Au, M., Ateniese, G., Huang, Z., Dai, Y., Susilo, W. and Geoyong, M. (2017). “Identity-Based Remote Data Integrity Checking With Perfect Data Privacy Preserving for Cloud Storage”. *IEEE Transactions on Information Forensics and Security*, Vol. 12, No. 4, pp. 767-778.

[70] Zanella, A., Bui, N., Castelli, A., Vangelitsa, L. and Zorzi, M. (2014). “Internet of Things for Smart Cities”. *IEEE Internet of Things Journal*, Vol. 1, No. 1, pp. 22-32.

[71] Zhu, X. and Badr, Y. (2018). “Identity Management Systems for the Internet of Things: A Survey Towards Blockchain Solutions”, *sensors*, Vol. 18, No. 12, pp. 4215.

[72] "Web3 – The Decentralized Web", BLOCKCHAINHUB.net, https://blockchainhub.net/web3-decentralized-web/

[73] Kristián Košt’ál, Pavol Helebrandt, Matej Belluš, Michal Ries and Ivan Kotuliak. (2019). “Management and Monitoring of IoT Devices Using Blockchain”, sensors.

[74] IBM Think Academy, “How It Works: Internet of Things”, Available: https://www.youtube.com/watch?v=QSIPNhOiMoE

[75] Mobiliya Labs, “INTERNET OF THINGS”, Available: https://www.mobiliya.com/practices/internet-of-things

[76] Dr.Vasos Vassiliou, [pdf], “Blockchain-based Secure Decentralization for the Internet-of-Things”

[77] Wikipedia, “RFID”, Available: https://el.wikipedia.org/wiki/RFID

[78] Technopedia, “Wireless Sensor Network (WSN)”, Acailable: https://www.techopedia.com/definition/25651/wireless-sensor-network-wsn

[79] Wikipedia, “Υπολογιστικό νέφος”, Available: https://el.wikipedia.org/wiki/Υπολογιστικό_νέφος

[80] Wikipwsi, “Electronic signatures”, Available: https://en.wikipedia.org/wiki/Electronic_signature