ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ Η/Υ & ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Εφαρμογή του Blockchain στο Διαδίκτυο των Πραγμάτων για κατασκευή έξυπνου σπιτιού

Βασίλης Νικόπουλος
Α.Μ: 4927

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: κ. Γ. ΠΑΥΛΙΔΗΣ

Οκτ., 2018

Ευχαριστίες

Ξεκινώντας θα ήθελα να ευχαριστήσω όλους εκείνους που συνέβαλαν και βοήθησαν στην πραγματοποίηση αυτής της διπλωματικής εργασίας.

Κυρίως θα ήθελα να ευχαριστήσω τον επιβλέποντα Καθηγητή κ. Γεώργιο Παυλίδη που μου έδωσε την ευκαιρία να αναλύσω ένα τόσο επίκαιρο και ενδιαφέρον θέμα. Επίσης τον ευχαριστώ για την βοήθειά του, την καθοδήγησή του καθώς και για την αμέριστη συμπαράστασή του καθ' όλη τη διάρκεια εκπόνησης της διπλωματικής μου εργασίας.

Ευχαριστώ επίσης και όλους τους καθηγητές μου στο τμήμα Μηχανικών Η/Υ και Πληροφορικής του Πανεπιστημίου Πατρών.

Πέρα και πάνω από όλα όμως, ευχαριστώ τους γονείς μου, για την αμέριστη και ανιδιοτελή ψυχολογική και οικονομική υποστήριξη.

Περίληψη

Δισεκατομμύρια έξυπνες συσκευές θα είναι διαθέσιμες στον ψηφιακό κόσμο λόγω της προόδου του Διαδικτύου των πραγμάτων (IoT). Ωστόσο, κάτι τέτοιο θα δημιουργούσε σημαντικές προκλήσεις ασφάλειας, ιδιωτικότητας και παροχής υπηρεσιών συνδεσιμότητας και αποθήκευσης δεδομένων. Τα σημερινά κεντρικά μοντέλα αρχιτεκτονικής στα συστήματα διασύνδεσης IoT θα αγωνιστούν για την κλιμάκωση των απαιτήσεων των μελλοντικών συστημάτων διασύνδεσης. Για την επίλυση αυτών των ζητημάτων, ο αποκεντρωμένος και συνασπισμός Blockchain και ο συνδυασμός κρυπτογραφικών διαδικασιών πίσω από αυτό, μπορεί να προσφέρει μια ενδιαφέρουσα εναλλακτική λύση.

Για μερικούς ανθρώπους, η τεχνολογία blockchain που βασίζεται στα Bitcoin και Ethereum θεωρείται ως η σημαντικότερη καινοτομία από το Διαδίκτυο. Ωστόσο, εξακολουθεί να είναι σε αρχικά στάδια. Επιπλέον, ο συνδυασμός με το IoT απαιτεί ακόμα ουσιαστικές γνώσεις σχετικά με τους συγκεκριμένους τομείς εφαρμογής, την επεκτασιμότητα, τα ζητήματα ιδιωτικού απορρήτου, τις επιδόσεις και τα πιθανά οικονομικά οφέλη.

Το Blockchain θα επιτρέψει στις συσκευές IoT να στείλουν δεδομένα σε ιδιωτικούς καταλόγους blockchain για να συμπεριληφθούν σε κοινές συναλλαγές με αρχεία ανθεκτικά στις παραβιάσεις. Η κατανεμημένη αναπαραγωγή του Blockchain επιτρέπει στις κάθετες βιομηχανίες και σε διάφορους χρήστες δεδομένων IoT να έχουν πρόσβαση και να παρέχουν δεδομένα IoT χωρίς την ανάγκη κεντρικού ελέγχου και διαχείρισης. Όλοι οι ενδιαφερόμενοι στο Διαδίκτυο μπορούν να επαληθεύσουν κάθε συναλλαγή, να αποτρέψουν τις διαφορές και να διασφαλίσουν ότι κάθε χρήστης θα λογοδοτεί για τους μεμονωμένους ρόλους του στη συνολική συναλλαγή. Έτσι, η τεχνολογία Blockchain έχει τη δυνατότητα να ξεκλειδώσει με ασφάλεια την επιχειρησιακή και επιχειρησιακή αξία των συστημάτων IoT για την υποστήριξη κοινών καθηκόντων, όπως η αίσθηση, η επεξεργασία, η αποθήκευση πληροφοριών και η επικοινωνία.

Λέξεις-κλειδιά: Blockchain, Διαδίκτυο των Πραγμάτων, συναλλαγή, ασφάλεια, έξυπνη συσκευή.

Abstract

Billions of smart devices will be available in digital world due the advancement of the Internet of Things (IoT). However, it also would create serious security, privacy, and connectivity service provisioning and data storage challenges. The current centralized architecture models in IoT systems will struggle to scale up to meet the demands of future IoT systems. To solve these issues, the decentralized and consensus-driven Blockchain and the combination of cryptographic processes behind it can offer an intriguing alternative.

For some people, the blockchain technology underlying Bitcoin and Ethereum is seen as the most important innovation since the Internet and even of this century. However, it is still in its infancy. Moreover, the combination with IoT still requires essential insights with respect to concrete application domains, scalability, privacy issues, performance, and potential financial benefits.

Blockchain will enable IoT devices to send data to private blockchain ledgers for inclusion in shared transactions with tamper-resistant records. The distributed replication of Blockchain enables vertical industries and various IoT data users to access and supply IoT data without the need for central control and management. All stakeholders in the IoT eco system can verify each transaction, preventing disputes and ensuring each user is held accountable for their individual roles in the overall transaction. Thus, Blockchain holds the potential to securely unlock the business and operational value of IoT systems to support common tasks, such as sensing, processing, storing information, and communicating.

Keywords: Blockchain, Internet of Things, transaction, Bitcoin, Ethereum, security, smart device

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Περιεχόμενα

Πρόλογος.....**Error! Bookmark not defined.**
Κεφάλαιο 1 - Περιγραφή διπλωματικής..... 10
1.1 Ο προβληματισμός που πραγματεύεται η διπλωματική 10
1.2 Στόχος της εργασίας..... 12
1.3 Βιβλιογραφική αιτιολόγηση..... 14
1.4 Βασικές έννοιες διπλωματικής 14
Κεφάλαιο 2 - Διαδίκτυο των Πραγμάτων (IoT) και τεχνολογία Blockchain..... 17
2.1 Εισαγωγή στο Διαδίκτυο των Πραγμάτων..... 17
2.2 Τρόπος και χαρακτηριστικά λειτουργίας του Διαδικτύου των Πραγμάτων..... 20
2.3 Χαρακτηριστικά λειτουργίας Έξυπνου Σπιτιού..... 22
2.4 Εισαγωγή στην τεχνολογία Blockchain 27
2.5 Οφέλη και περιορισμοί τεχνολογίας Blockchain..... 34
2.6 Άνοδος του Bitcoin και χαρακτηριστικά 37
Κεφάλαιο 3 - Προς ένα βελτιστοποιημένο Blockchain για το Διαδίκτυο των Πραγμάτων..... 41
3.1 Τομείς εφαρμογής της τεχνολογίας Blockchain 41
3.3 Μοντέλα επικοινωνίας του IoT..... 43
3.4 Αρχιτεκτονική έξυπνου σπιτιού βασισμένη στην τεχνολογία bitcoin..... 46
3.5 Αποθήκευση στο υπολογιστικό νέφος 50
3.6 Διαχείριση συναλλαγών έξυπνου σπιτιού..... 51
3.6.1 Αποθήκευση συναλλαγών έξυπνου σπιτιού 51
3.6.2 Προσπέλαση συναλλαγών έξυπνου σπιτιού 52
3.6.3 Παρακολούθηση συναλλαγών έξυπνου σπιτιού..... 53
3.7 Εκτίμηση (αξιολόγηση συναλλαγών Έξυπνου Σπιτιού)..... 53
3.7.1 Ασφάλειας και ανάλυση ιδιωτικής ζωής 55
3.8 Αξιολόγηση απόδοσης..... 58
Κεφάλαιο 4 – Έξυπνα σπίτια με τη χρήση της τεχνολογίας Blockchain 61
4.1 Λειτουργία έξυπνου σπιτιού..... 61
4.2 Ασφάλεια με τη βοήθεια του Blockchain στο έξυπνο σπίτι 66
4.2.1 Οι εκκολαπτόμενες απειλές στο εταιρικό περιβάλλον..... 69
4.2.2. Στρατηγική ασφαλείας για τις IoT συσκευές 71
Κεφάλαιο 5 - Μελλοντικές τάσεις του Διαδικτύου των Πραγμάτων 82
Βιβλιογραφία 90

Εισαγωγή

Ο όρος Διαδίκτυο των Πραγμάτων (Internet of Things) επινοήθηκε στα τέλη της δεκαετίας του 1990 από τον επιχειρηματία Kevin Ashton (Ashton, 2009), ο οποίος ήταν μέλος μιας ομάδας του Πανεπιστημίου MIT που ανακάλυψε τον τρόπο να συνδέσει τα αντικείμενα με το Διαδίκτυο μέσω μιας ετικέτας RFID[1]. Έχει δηλώσει ότι χρησιμοποίησε πρώτη φορά τη φράση Internet of Things σε μια παρουσίαση που έκανε το 1999 – και ο όρος αυτός έχει καθιερωθεί από τότε.

Ένας τεχνολογικός όρος που έχει αρχίσει σταδιακά να μπαίνει στη ζωή μας είναι το *Internet of Things (IoT)*, ή αλλιώς *Διαδίκτυο των Πραγμάτων* (Boldt, 2015). Είναι μια έννοια που αφορά τα αντικείμενα της καθημερινότητάς μας – από βιομηχανικές μηχανές μέχρι συσκευές που μπορούν να φορεθούν (wearable) που χρησιμοποιούν ενσωματωμένους αισθητήρες για τη συλλογή δεδομένων και την ανάληψη κάποιας δράσης σε αυτά μέσα σε ένα δίκτυο. Κάπως έτσι λειτουργεί ένα κτίριο που χρησιμοποιεί αισθητήρες (sensors) για την αυτόματη ρύθμιση της θέρμανσης ή του φωτισμού. Άλλο παράδειγμα είναι ο ένας εξοπλισμός της παραγωγής ενός εργοστασίου που προειδοποιεί το προσωπικό συντήρησης για μια επικείμενη βλάβη.

Στις συζητήσεις γύρω από το IoT, έχει αναγνωριστεί ότι οι τεχνολογίες ανάλυσης (*analytics*) είναι ζωτικής σημασίας για τη μετατροπή μεγάλου όγκου δεδομένων σε κατατοπιστική και χρήσιμη γνώση. Ενώ στην παραδοσιακή ανάλυση, τα δεδομένα αποθηκεύονται και μετά αναλύονται, στην περίπτωση των *δεδομένων συνεχούς ροής (streaming data),* όπως αυτά του IoT, τα μοντέλα και οι αλγόριθμοι είναι αυτοί που αποθηκεύονται και τα δεδομένα περνούν μέσα από αυτούς για ανάλυση. Αυτό το είδος της ανάλυσης καθιστά δυνατό τον εντοπισμό και την εξέταση μοτίβων καθώς τα δεδομένα δημιουργούνται, σε πραγματικό χρόνο. Έτσι, πριν αποθηκευτούν τα δεδομένα, στο υπολογιστικό νέφος (cloud) ή σε οποιοδήποτε άλλο χώρο αποθήκευσης, υπόκεινται σε επεξεργασία. Έπειτα, χρησιμοποιούμε τεχνικές ανάλυση (analytics) ώστε

[1] Οι ετικέτες RFID ή αλλιώς ταυτοποίηση μέσω ραδιοσυχνοτήτων (radio frequency identification) είναι chips που αποτελούνται από ένα ολοκληρωμένο κύκλωμα, το οποίο περιλαμβάνει μνήμη ώστε να αποθηκεύει δεδομένα-πληροφορίες και μία κεραία. Το δεύτερο μέρος είναι οι αναγνώστες ή αισθητήρες (readers), οι οποίοι ανακτούν τα δεδομένα από τις ετικέτες RFID. Οι αναγνώστες RFID έχουν ενσωματωμένα ή ξεχωριστά μια κεραία και μια μονάδα ελέγχου. Η λειτουργία των συστημάτων RFID είναι απλή και βασίζεται στη δυναμική και αμφίδρομη επικοινωνία των ετικετών και των αναγνωστών. Όταν οι ετικέτες RFID βρεθούν στην εμβέλεια της κεραίας του αναγνώστη, η μονάδα ελέγχου επικοινωνεί με ραδιοκύματα με την κεραία των ετικετών RFID.

να αποκρυπτογραφήσουμε τα δεδομένα, ενώ όλοι οι συσκευές συνεχίζουν να εκπέμπουν/λαμβάνουν δεδομένα.

Με προηγμένες τεχνικές ανάλυσης δεδομένων (advanced analytics), οι αναλύσεις ροών δεδομένων (data stream analytics) μπορούν να πάνε πέρα από την απλή παρακολούθηση των υπαρχουσών συνθηκών και την αξιολόγηση των κατώτατων ορίων στην πρόβλεψη μελλοντικών σεναρίων και στην εξέταση πολύπλοκων ερωτημάτων. Ενδεικτικές προηγμένες τεχνικές ανάλυσης δεδομένων είναι οι εξής:

Μηχανική Μάθηση (Machine Learning): ιδιαίτερα δημοφιλής τεχνολογία ανάμεσα στους ειδικούς των δεδομένων. Η εν' λόγω τεχνολογία προσφέρει αυτοματοποιημένο μοντέλο προβλεπτικής ικανότητας με χρήση αυτομάθησης και επαναληπτικών αλγορίθμων. Επιπλέον έχουμε τη *Μάθηση σε βάθος (Deep Learning):* περιλαμβάνει προηγμένα νευρωνικά δίκτυα με πολλαπλά κρυμμένα επίπεδα. Εκτελεί -κυρίως- τη διαδικασία μοντελοποίησης σε τομείς αυξημένου ενδιαφέροντος όπως τα πρότυπα, οι εικόνες και η αναγνώριση προσώπου. Επίσης υπάρχουν οι *Στατιστικές Αναλύσεις κειμένου (Text Analytics):* εξερευνούν τα αδόμητα δεδομένα και διαδραματίζουν ένα κρίσιμο ρόλο στη διαχείριση των μεγάλων δεδομένων (Big Data). Οι πιο πολύπλοκες λειτουργίες, όπως η εφαρμογή της φυσικής γλώσσας στη διαδικασία εξόρυξης χρήσιμης πληροφορίας, απαιτούν τους προηγμένους αλγόριθμους των στατιστικών αναλύσεων κειμένου. Τέλος έχουμε τη *Μοντελοποίηση όγκου και διαχείριση (Mass-modelling & Management):* δημιουργεί σε γρήγορο χρόνο χιλιάδες προβλεπτικά μοντέλα μέσω μίας αυτοματοποιημένης διαδικασίας και τα διαχειρίζεται σε πραγματικό χρόνο σε επιχειρησιακό περιβάλλον.

Για να εκτιμηθεί το μέλλον με τη χρήση αυτών των ροών δεδομένων (data streams), θα πρέπει να είναι διαθέσιμες τεχνολογίες υψηλής απόδοσης που μπορούν να προσδιορίσουν μοτίβα στα δεδομένα τη στιγμή που αυτά δημιουργούνται. Μόλις ένα μοτίβο αναγνωρίζεται, μετρήσεις ενσωματωμένες στη ροή δεδομένων, οδηγούν στην αυτόματη προσαρμογή των συνδεδεμένων συστημάτων ή δημιουργούν ειδοποιήσεις για άμεσες δράσεις και λήψη καλύτερων αποφάσεων.

Η σημασία του IoT φαίνεται στον αριθμό των αντικειμένων που είναι συνδεδεμένα με το Διαδίκτυο και στα οικονομικά οφέλη που μπορούν να προκύψουν από την ανάλυση των ροών δεδομένων (data streams). Ενδεικτικά αναφέρονται τα εξής:

- Έξυπνες λύσεις μεταφοράς επιταχύνουν την ροή της κυκλοφορίας , μειώνουν την κατανάλωση καυσίμων, θέτουν προτεραιότητες στα προγράμματα επισκευής οχημάτων και σώζουν ζωές.

- Έξυπνα ηλεκτρικά δίκτυα (smart electric grids) συνδέουν πιο αποτελεσματικά ανανεώσιμες πηγές ενέργειας, βελτιώνουν την αξιοπιστία του συστήματος και χρεώνουν τους καταναλωτές με βάση μικρότερες προσαυξήσεις.

- Μηχανές αισθητήρων παρακολούθησης κάνουν διαγνώσεις και προβλέπουν θέματα συντήρησης που εκκρεμούν και θέτουν ακόμα και προτεραιότητες στα προγράμματα του προσωπικού που είναι υπεύθυνο για τις επισκευές, για να καλύψουν αποτελεσματικότερα τις ανάγκες επισκευής εξοπλισμού αλλά και περιφερειακές ανάγκες.

- Συστήματα οδηγούμενα από δεδομένα (data-driven) χτισμένα στις υποδομές των έξυπνων πόλεων καθιστούν ευκολότερο για τους δήμους να εκτελούν τις διαδικασίες διαχείρισης αποθεμάτων, την επιβολή του νόμου και άλλα προγράμματα πιο αποτελεσματικά.

- Σε προσωπικό επίπεδο, το σύστημα ασφαλείας του σπιτιού επιτρέπει τον απομακρυσμένο έλεγχο σε κλειδαριές και θερμοστάτες και μπορεί να ρυθμίσει το κλιματιστικό και να ανοίξει τα παράθυρα του σπιτιού, με βάση τις προτιμήσεις των ιδιοκτητών.

- Στον τομέα της υγειονομικής περίθαλψης, πολλοί άνθρωποι έχουν ήδη υιοθετήσει wearable συσκευές για να παρακολουθούν τη φυσική τους άσκηση, τον ύπνο ή άλλες συνήθειες τους.

- Ο κλάδος των Τηλεπικοινωνιών θα επηρεαστεί σημαντικά από το IoT, αρκεί να σκεφτεί κανείς ότι αυτός θα είναι ο κλάδος που θα διατηρεί όλα τα δεδομένα που χρησιμοποιεί το IoT. Smartphones και άλλες προσωπικές συσκευές πρέπει να είναι σε θέση να διατηρούν μια αξιόπιστη σύνδεση στο Διαδίκτυο για να λειτουργήσει αποτελεσματικά το Διαδίκτυο των Πραγμάτων.

- Στον τομέα της ενέργειας οι έξυπνοι μετρητές (smart meters) όχι μόνο συλλέγουν δεδομένα αυτόματα, αλλά και καθιστούν και δυνατή την εφαρμογή τεχνολογιών ανάλυσης (analytics) για την παρακολούθηση και τη διαχείριση της χρήσης της ενέργειας. Παρομοίως, αισθητήρες σε συσκευές όπως οι ανεμόμυλοι

μπορούν να παρακολουθούν τα δεδομένα και να χρησιμοποιούν προγνωστική μοντελοποίηση, ώστε να προγραμματιστεί η διακοπή λειτουργίας για πιο αποδοτική χρήση της ενέργειας.

Κεφάλαιο 1 - Περιγραφή εργασίας

1.1 Ο προβληματισμός που πραγματεύεται η εργασία

Το Διαδίκτυο των Πραγμάτων είναι ένα καινούριο εγχείρημα στο χώρο της τεχνολογίας, που πραγματεύεται τη σύνδεση διαφόρων μικρών και μεγάλων συσκευών ή ακόμα και οχημάτων με ενσωματωμένους αισθητήρες και εξοπλισμό διασύνδεσης τόσο μεταξύ τους όσο και με τον κατασκευαστή, με τη δική τους διεύθυνση IP, για να μεταδίδουν και να λαμβάνουν σχετικά δεδομένα, με βασικό στόχο την παροχή πλήθους υπηρεσιών στους χρήστες. Στην ουσία είναι ένα δίκτυο που συνεχώς αναπτύσσεται, το οποίο ολοκληρώνει εργασίες, χωρίς να απασχολείται κάποιος ώστε να πραγματοποιηθούν (Dorri, 2017). Στην ουσία είναι μια τεχνολογική εξέλιξη, με την οποία έχουμε ηλεκτρονική σήμανση κάθε είδους αντικειμένων παρέχοντας ηλεκτρονική ταυτότητα σε αυτά, ώστε να υπάρχει αναγνώριση και ανίχνευση, δίνοντας την δυνατότητα επικοινωνίας μεταξύ των αντικειμένων. Έτσι με αυτό τον τρόπο οι χρήστες δε θα λειτουργούν ως ενδιάμεσοι της υπηρεσίας εντοπισμού κάποιου αντικειμένου αλλά το ίδιο το αντικείμενο θα έχει αλληλεπίδραση άμεσα και γρήγορα με το πληροφοριακό σύστημα, με το οποίο επικοινωνεί. Έτσι επιτυγχάνεται η εφαρμογή του έξυπνου σπιτιού.

Όταν μιλάμε για *έξυπνο σπίτι* στην ουσία εννοούμε ένα σπίτι που θα έχει την δυνατότητα να επικοινωνεί με τον ιδιοκτήτη του, να του παρέχει ενημέρωση για οτιδήποτε έχει ζητήσει ο χρήστης, να του παρέχει αλλαγές σε χαρακτηριστικά (όπως αλλαγή θερμοκρασίας) άμεσα, αξιόπιστα και με ασφάλεια. Το έξυπνο σπίτι παρέχει αισθητήρες οι οποίοι ενημερώνουν οποιαδήποτε στιγμή τους ζητηθεί για το αν κάποιος βρίσκεται μέσα στον χώρο, αν ο θερμοσίφωνας είναι εκτός λειτουργίας, αν όλα τα παράθυρα είναι κλειστά, και αν όχι τότε ποια από αυτά δεν είναι, για πιθανή διαρροή υγραερίου ή νερού κλπ. Όλοι αυτοί οι αισθητήρες καταγράφουν δεδομένα και έχουν αλληλεπίδραση με μια κεντρική συσκευή ελέγχου η οποία έχει σύνδεση στο Διαδίκτυο και μπορεί να ελεγχθεί και να ακολουθήσει συγκεκριμένες εντολές του ιδιοκτήτη.

Ακόμα παρέχεται η δυνατότητα να ασφαλιστούν πόρτες και παράθυρα και να ενεργοποιηθεί/απενεργοποιηθεί αντίστοιχα ο συναγερμός από απόσταση, χρησιμοποιώντας εύχρηστη εφαρμογή στο κινητό τηλέφωνο. Επίσης, είναι δυνατόν να επιτευχθεί η επιθυμητή φωτεινότητα του χώρου. Μέσω της εφαρμογής ο χρήστης μπορεί να παρακολουθήσει άμεσα, μέσω κάμερας, οποιαδήποτε δραστηριότητα παρατηρηθεί μέσα στο χώρο και άμεσα να καταγραφεί για μελλοντική χρήση.

Το Διαδίκτυο των Πραγμάτων στην ουσία αφορά τα αντικείμενα της καθημερινότητας μας, από βιομηχανικές μηχανές μέχρι συσκευές που μπορούμε να τις φορέσουμε. Οι συσκευές αυτές χρησιμοποιούν ενσωματωμένους αισθητήρες για τη συλλογή δεδομένων και την ανάληψη κάποιας δράσης σε αυτά μέσα σε ένα δίκτυο. Κάπως έτσι λειτουργεί ένα σπίτι που χρησιμοποιεί αισθητήρες για την αυτόματη ρύθμιση της θέρμανσης ή του φωτισμού. Ακόμα είναι ο εξοπλισμός παραγωγής που προειδοποιεί το προσωπικό συντήρησης για μία πιθανή βλάβη. Όλα δείχνουν ότι το Διαδίκτυο των Πραγμάτων είναι το τεχνολογικό μέλλον που θα κάνει τη ζωή μας πιο εύκολη.

Το μέλλον βρίσκεται στη μετάβαση από το δίκτυο διασυνδεμένων υπολογιστών σε ένα δίκτυο διασυνδεμένων αντικειμένων και προϊόντων. Από ηλεκτρικές συσκευές και αυτοκίνητα, έως βιβλία και είδη ρουχισμού, που χάρη σε ενσωματωμένους ηλεκτρονικούς αισθητήρες θα έχουν τη δική τους διεύθυνση IP, θα λαμβάνουν πληροφορίες από το περιβάλλον και θα αλληλοεπιδρούν.

Το Κεφάλαιο 1 της παρούσας εργασίας αναφέρει το στόχο και το βασικό προβληματισμό που διαπραγματεύεται και επίσης περιέχει μια σύντομη βιβλιογραφική αιτιολόγηση για το υλικό που χρησιμοποιήθηκε στη συγγραφή της.

Στο Κεφάλαιο 2 περιγράφεται διεξοδικά το Διαδίκτυο των Πραγμάτων (IoT) και η τεχνολογία Blockchain που εφαρμόζεται σε αυτό. Ξεκινά με μια σύντομη περιγραφή του ιστορικού του IoT και συνεχίζει με τα βασικά χαρακτηριστικά περιγραφής του τρόπου λειτουργίας του. Στη συνέχεια αναλύει την τεχνολογία Blockchain και εστιάζει στη δυναμική που διαθέτει για να εισβάλλει σε ποικίλες βιομηχανίες, συμπεριλαμβανομένων της μουσικής, του Μάρκετινγκ, της υγείας, της δημόσιας διοίκησης και αλλού και να αυξήσει την ασφάλεια των πραγματοποιούμενων συναλλαγών. Το Κεφάλαιο ολοκληρώνεται με την περιγραφή των πλεονεκτημάτων και μειονεκτημάτων της συγκεκριμένης τεχνολογίας.

Στο Κεφάλαιο 3 περιγράφεται η μετάβαση προς ένα βελτιστοποιημένο Blockchain για το Διαδίκτυο των Πραγμάτων. Ξεκινά με παραδείγματα εφαρμογής της τεχνολογίας Blockchain σε διαφορετικούς τομείς, όπως π.χ. Γεωργία, Ναυτιλία, Τραπεζική, Δίκαιο κ.λ.π. και συνεχίζει με τα μοντέλα επικοινωνίας του Διαδικτύου των Πραγμάτων, τα οποία αφού τα αναλύσει, περιγράφει στη συνέχεια

Στο Κεφάλαιο 4 περιγράφεται η χρήση της τεχνολογίας Blockchain που υπάρχει στο Διαδίκτυο των Πραγμάτων για την κατασκευή ενός έξυπνου σπιτιού.

1.2 Στόχος της εργασίας

Ο στόχος είναι η εισαγωγή των εννοιών IoT και Blockchain, τα προβλήματα των εφαρμογών τους και μια περίπτωση εφαρμογής αυτών στα έξυπνα σπίτια. Ο ιδιοκτήτης του Έξυπνου σπιτιού μπορεί να επιτηρεί τα παιδιά που είναι μόνα μέσα στο σπίτι, τους ηλικιωμένους γονείς αν είναι καλά στην υγεία τους, μέχρι και να επικοινωνήσει μαζί τους μέσω αμφίδρομης επικοινωνίας και να ενημερωθεί για ό,τι πρόβλημα προκύψει. Επίσης, μπορεί να ρωτήσει αν έχουν πάρει τα φάρμακά τους, και αν δεν το έχουν κάνει, να τους θυμίσει να τα πάρουν. Μπορεί να χειριστεί τον θερμοστάτη του καλοριφέρ από την δουλεία του και να τον ρυθμίσει στην θερμοκρασία που ο ίδιος επιθυμεί. Ακόμα, μπορεί με μια ματιά στην οθόνη του κινητού του να δει ποιος βρίσκεται στην είσοδο του σπιτιού και χτυπάει το κουδούνι και ανάλογα να ξεκλειδώσει την είσοδο για να εισέλθει, χωρίς να ενοχλήσει τους παρευρισκόμενους στην οικία.

Το Έξυπνο Σπίτι λειτουργεί αυτόνομα γιατί μπορεί να αυτό-ρυθμίζεται, για παράδειγμα προκειμένου η θερμοκρασία να παραμείνει σταθερή, θα πρέπει να ανοιγοκλείσουν οι κουρτίνες και ο εσωτερικός φωτισμός να αυξηθεί η να μειωθεί ανάλογα της φωτεινότητας στον χώρο, ο περιμετρικός συναγερμός να τεθεί σε λειτουργία με την είσοδο των παιδιών στο σπίτι, οι κάμερες να καταγράψουν μια ύποπτη κίνηση και όλα αυτά χωρίς την χρήση χειροκίνητης ρύθμισης. Έτοιμα και ρυθμισμένα σενάρια, πλήρως λειτουργικά, για τις εκάστοτε ανάγκες του ιδιοκτήτη, μπορούν να ενεργοποιηθούν, να απενεργοποιηθούν, να αντικατασταθούν και να εκτελέσουν έτσι τις ενέργειες που έχουν προγραμματιστεί για να κάνουν. Σε ένα σενάριο που απουσιάζουν όλοι από το σπίτι μπορούν αυτόματα να τίθενται σε λειτουργία όλοι οι αισθητήρες συναγερμού και οι κάμερες να προγραμματίζονται να καταγράφουν με την παραμικρή ύποπτη κίνηση. Στην περίπτωση παρουσίας κάποιου εντός της οικίας μπορεί να έχουν γίνει από πριν οι απαραίτητες ρυθμίσεις ώστε να ενεργοποιούνται οι περιμετρικοί αισθητήρες σε πόρτες και παράθυρα χωρίς να είναι ενεργοποιημένοι οι αισθητήρες κίνησης μέσα στα δωμάτια. Παράλληλα με αυτό το σενάριο μπορεί να ενεργοποιηθεί ο θερμοστάτης ώστε να διατηρεί την θερμοκρασία του χώρου στα επιθυμητά επίπεδα. Τέλος αν για κάποιο λόγο αυτός που βρίσκεται μέσα στην οικία αποχωρήσει τότε υπάρχει

η δυνατότητα ενεργοποίησης του πρώτου σεναρίου όπου δεν βρίσκεται κανένας παρών και να τεθούν σε λειτουργία οι απαραίτητές ενέργειες.

Η δημιουργία των σεναρίων, η ρύθμιση των παραμέτρων και οποιαδήποτε αλλαγή χρειαστεί να πραγματοποιηθεί, διέπονται από ευκολία και ευχρηστία, έτσι ώστε να είναι διαχειρίζονται από τον καθένα, χωρίς πολύπλοκες γνώσεις ηλεκτρονικής ή υπολογιστικών συστημάτων. Μέσα από φιλικό περιβάλλον χρήστη, από εφαρμογή σε κινητό η υπολογιστή γίνονται όλες οι ενέργειες και πραγματοποιούνται όλα τα ενδεχόμενα. Το Διαδίκτυο των πραγμάτων αποτελεί εφαρμογή των τεχνολογιών του Διαδικτύου και χρησιμοποιεί συστήματα αναγνώρισης ραδιοσυχνοτήτων RFID για ασύρματη σύνδεση. Η τεχνολογία RFID είναι μια εφαρμογή που χρησιμοποιείται για τον εντοπισμό και την ταυτοποίηση αντικειμένων με χρήση ραδιοκυμάτων σε συσκευές που είναι τοποθετημένες σε αντικείμενα πομποδέκτες.

Στην πράξη οι τεχνολογίες αυτές βρίσκουν εφαρμογή σε πιστωτικές κάρτες, σε βιβλιοθήκες, ηλεκτρονικές ταυτότητες, διπλώματα οδήγησης κλπ. Η αρχή πραγματοποιήθηκε από το ασύρματο Διαδίκτυο, τις συσκευές με Wi-Fi δυνατότητες και ενσωματωμένους αισθητήρες, όπως τα smart phones και φθάνουμε σήμερα στη λογική του Δικτύου των Πραγμάτων, όπου συνδέονται οι συσκευές με το Διαδίκτυο αλλά και μεταξύ τους. Το Δίκτυο των Πραγμάτων άρχισε να υλοποιείται με μεγάλη ψηφιοποίηση των συσκευών του και την παραγωγή μεγάλου όγκου δεδομένων, αφού υλοποιείται σε πολλές εφαρμογές σχετικές με αγορές και υπηρεσίες ή ακόμα τελειοποιεί και παλαιότερες εφαρμογές. Αν οι συσκευές περιέχουν τσιπ έχουν την δυνατότητα να συνδεθούν με το Διαδίκτυο, με αποτέλεσμα να παράγονται έξυπνες διασυνδεδεμένες συσκευές, οι οποίες θα έχουν αυτονομία, εξαιτίας των ασύρματων συνδέσεων, θα ελέγχονται αυτόματα, θα ρυθμίζονται αυτόματα και θα επισκευάζονται αυτόματα, με άμεση συνέπεια τις οικονομικές ευκαιρίες που δημιουργούνται, οι οποίες θα βασίζονται στην αλληλεπίδραση του ατόμου με το τεχνολογικό περιβάλλον.

Έχει ήδη αρχίσει να γίνεται αντιληπτό πως η εξέλιξη σημαντικών τομέων της καθημερινότητας των ανθρώπων αλλάζει διάσταση, καθώς στο κοντινό μέλλον, τα αυτοκίνητά μας, τα σπίτια μας, οι ηλεκτρονικές συσκευές μας, ακόμη και οι δρόμοι των πόλεων θα συνδέονται στο Διαδίκτυο δημιουργώντας αυτό το δίκτυο αντικειμένων που ονομάζεται Διαδίκτυο των Πραγμάτων αποτελούμενο από εκατομμύρια αισθητήρες και συσκευές που παράγουν συνεχείς ροές δεδομένων, δημιουργώντας τις ικανές συνθήκες

για καινούριες τεχνολογικές εφαρμογές. Σύμφωνα με υπολογισμούς μέχρι το 2020 θα είναι συνδεδεμένες 50 εκατομμύρια συσκευές.

Το Διαδίκτυο των Πραγμάτων χαρακτηρίζεται από βασικές παραμέτρους, όπως τα αντικείμενα, τα δίκτυα επικοινωνιών που τα συνδέουν και τα υπολογιστικά συστήματα τα οποία χρησιμοποιούν τα δεδομένα που ρέουν προς και από τα αντικείμενα. Μερικά παράδειγμα που θα μπορούσαμε να αναφέρουμε είναι οι φορητές συσκευές, τα έξυπνα μηχανήματα, τα ευφυή δίκτυα και τα έξυπνα σπίτια, που μπορούν να συνδέσουν τον πραγματικό με τον ψηφιακό κόσμο, τον φυσικό με τον ηλεκτρονικό και να αλλάξουν τις καταναλωτικές συνήθειες. Για να καταστεί ωφέλιμο το IoT, έχει ανάγκη και τα απαραίτητα Analytics των Πραγμάτων (Analytics of Things). Πρακτικά αυτό δίνει μια νέα προσέγγιση στη διαχείριση και ενοποίηση των δεδομένων, καθώς και νέους τρόπους στην ανάλυση δεδομένων συνεχούς ροής. Για την υλοποίηση του IoT είναι αναγκαία η πρόσβαση στο διαδίκτυο ακόμα και στις πιο απομακρυσμένες περιοχές, καθώς και ταυτόχρονη χρήση των τεχνολογιών (mobile και cloud) και γενικότερα εξελίξεις στα πληροφορικά συστήματα.

1.3 Βιβλιογραφική αιτιολόγηση

Στην παρούσα διπλωματική εργασία συμπεριελήφθησαν τρείς διαφορετικές βιβλιογραφικές πηγές, και αναφέρονται:

- Εργασίες (papers) και βιβλία (έντυπα και ηλεκτρονικά) σχετικά με τον κίνδυνο αγοράς.
- Άρθρα, δημοσιεύσεις στο Διαδίκτυο, τόσο στην Ελλάδα όσο και στο εξωτερικό.
- Προηγούμενες διπλωματικές, πτυχιακές εργασίες με συναφή με αυτό της παρούσας διπλωματικής εργασίας θέματα.

Μέσα στο κείμενο της εργασίας σημειώνεται με κατάλληλες παραπομπές η προαναφερθείσα βιβλιογραφική αιτιολόγηση και στο τέλος της εργασίας υπάρχει εκτενής βιβλιογραφική ανασκόπηση.

1.4 Βασικές έννοιες διπλωματικής

Οι βασικές έννοιες που διαπραγματεύεται η διπλωματική εργασία είναι το Διαδίκτυο των Πραγμάτων (IoT – Internet of Things) καθώς και η τεχνολογία Blockchain που χρησιμοποιεί για να αυξήσει την ασφάλεια των συναλλαγών που πραγματοποιούνται

(Ντόα, 2017). Πρόκειται για ένα δίκτυο συσκευών που μεταδίδουν, μοιράζουν και χρησιμοποιούν δεδομένα από το φυσικό περιβάλλον προκειμένου να παρέχουν υπηρεσίες τόσο σε επιχειρήσεις όσο και σε άτομα. Τα στοιχεία (πράγματα) του Διαδικτύου λειτουργούν είτε μεμονωμένα ή συνδεδεμένα με άλλα αντικείμενα ή άτομα και διαθέτουν μοναδικά αναγνωριστικά (identifiers). Το Διαδίκτυο των Πραγμάτων εφαρμόζεται σε πολλούς τομείς. Μερικοί από αυτούς είναι ο χώρος της υγείας, των μεταφορών, της ενέργειας και του περιβάλλοντος. Τα είδη των συσκευών του IoT είναι μεταξύ άλλων αισθητήρες, οικιακοί αυτοματισμοί, συσκευές που φοριούνται, όπως για παράδειγμα το ρολόι ή τα γυαλιά. Σε αυτό το νέο Διαδίκτυο, οι χρήστες θα είναι σε θέση να κατέχουν ψηφιακά περιουσιακά στοιχεία (digital assets) και να τα χρησιμοποιήσουν για όφελος τους.

Η τεχνολογία Blockchain αποτελεί ένα τύπο βάσης δεδομένων που δέχεται ένα πλήθος εγγραφών από τους χρήστες, τις οποίες βάζει σε ένα φύλλο δεδομένων γνωστό ως block. Κάθε χρήστης κρατάει ένα αντίγραφο αυτού του block. Καθώς οι εγγραφές αυξάνονται, κάθε block συνδέεται με μία γραμμική, χρονολογική σειρά με το επόμενο δημιουργώντας μία αλυσίδα (Blockchain), με τη χρήση μίας κρυπτογραφημένης υπογραφής. Η διαδικασία αυτή επιτρέπει στο Blockchain να χρησιμοποιείται σαν ένα δημόσιο λογιστικό βιβλίο (ledger), το οποίο μπορεί να μοιραστεί και να επιβεβαιωθεί από οποιοδήποτε εξουσιοδοτημένο χρήστη. Η ιδιότητα αυτή το καθιστά αποκεντρωμένο (decentralized), επειδή η εποπτεία της ορθότητας της συναλλαγής διαμοιράζεται σε όλους τους χρήστες του και δεν περιορίζεται όπως για παράδειγμα σε ένα χρηματοπιστωτικό ίδρυμα.

Η τεχνολογία Blockchain που χρησιμοποιείται στο IoT και το ψηφιακό νόμισμα Bitcoin είναι ένα αποκεντρωμένο, αδιάβλητο λογιστικό καθολικό που προτρέπει τους χρήστες να εμπιστεύονται τα δεδομένα (Huh, 2017). Η ανάγκη δημιουργίας ενός project που θα επιτρέπει την δημιουργία χρηματοοικονομικών εφαρμογών χωρίς την ανάγκη μεσολάβησης κάποιας τράπεζας ή μεσάζοντα δημιούργησε το Ethereum. Πρόκειται για ένα ψηφιακό νόμισμα αλλά και μια ανοικτού κώδικα πλατφόρμα blockchain με προγραμματιζόμενη λειτουργία συναλλαγών. Το Ethereum δημιούργησε ένα προγραμματιζόμενο Blockchain που υποστηρίζει έξυπνα συμβόλαια (smart contracts), προτρέποντας τους χρήστες να εμπιστεύονται τον κώδικα. Τα έξυπνα συμβόλαια επιτρέπουν την αυτόματη εκτέλεση συναλλαγών κατόπιν εκπλήρωσης συγκεκριμένων υποχρεώσεων. Για παράδειγμα, οι πωλητές θα πληρώνονται μόνο και εφόσον τα προϊόντα

τους ληφθούν με επιτυχία από τους αγοραστές. Οι εταιρείες που κάνουν χρηματοδότηση από πλήθος (crowdfunding) μπορούν να σχεδιάσουν συγκεκριμένες παραγωγικές εργασίες μόνο και εφόσον έχουν συλλέξει ένα συγκεκριμένο χρηματικό ποσό. Διαφορετικά, τα χρήματα θα επιστραφούν στους συμμετέχοντες. Χάρη στα έξυπνα συμβόλαια, δεν χρειάζεται να ανησυχούμε για την παραβίαση της σύμβασης ή για τα πιστωτικά όρια των εμπορικών μας εταίρων, επειδή το Blockchain θα εκτελέσει τις συναλλαγές μόνο και εφόσον και τα δύο μέρη έχουν εκπληρώσει τις υποχρεώσεις τους.

Κεφάλαιο 2 - Διαδίκτυο των Πραγμάτων (IoT) και τεχνολογία Blockchain

2.1 Εισαγωγή στο Διαδίκτυο των Πραγμάτων

Το Διαδίκτυο των Πραγμάτων (Internet of Things - IoT) είναι ένα δίκτυο φυσικών αντικειμένων, οχημάτων, συσκευών, κτιρίων κ.λ.π. τα οποία περιέχουν ενσωματωμένα ηλεκτρονικά συστήματα, λογισμικό, αισθητήρες και δυνατότητα σύνδεσης στο Διαδίκτυο για να μπορέσουν να συλλέγουν και να ανταλλάσσουν δεδομένα μεταξύ τους (Steve, 2014). Το Διαδίκτυο των Πραγμάτων δίνει τη δυνατότητα στα προαναφερόμενα αντικείμενα να ελέγχονται απομακρυσμένα μέσω της υπάρχουσας δικτυακής υποδομής, δημιουργώντας με τον τρόπο αυτό ευκαιρίες άμεσης ενσωμάτωσης του φυσικού κόσμου με τα υπολογιστικά συστήματα με στόχο της αύξηση της αποτελεσματικότητας και την ταυτόχρονη μείωση του κόστους. Κάθε αντικείμενο που είναι συνδεδεμένο στο IoT αναγνωρίζεται με τρόπο μοναδικό και μπορεί να λειτουργεί τόσο αυτόνομα όσο και σε συνδυασμό με την υπόλοιπη δικτυακή υποδομή.

Πολλοί οργανισμοί έχουν αναπτύξει διαφορετικούς τρόπους κατηγοριοποίησης των εφαρμογών του IoT. Για παράδειγμα το *βιομηχανικό IoT* είναι ένας όρος που χρησιμοποιείται ευρέως από τις επιχειρήσεις όταν θέλουν να περιγράψουν τις εφαρμογές του IoT που σχετίζονται με την παραγωγή αγαθών και υπηρεσιών. Άλλοι οργανισμοί επικεντρώνονται στον τύπο της κατασκευής του IoT, όπως οι φορητές συσκευές και οι εφαρμογές, ενώ άλλοι επικεντρώνονται στο γενικό πλαίσιο του IoT με βάση την τοποθεσία, όπως είναι για παράδειγμα τα έξυπνα σπίτια ή γενικότερα οι έξυπνες πόλεις. Παρόλο που η έννοια του διασυνδεδεμένου αντικειμένου προϋποθέτει αμφίδρομη επικοινωνία, το IoT δομείται κυρίως στο πρότυπο επερώτησης – απάντησης (RFID query and response). Κατά βάση, τα μοτίβα επικοινωνίας είναι δύο ειδών:

- Αντικείμενο προς άνθρωπο (thing to person) και αντίστροφα

- Αντικείμενο προς αντικείμενο (thing to thing).

Αδιαμφισβήτητα, το όραμα του IoT έχει άμεση επίδραση στην καθημερινή ζωή. Υπό αυτή την οπτική γωνία, τα «έξυπνα» αντικείμενα, ο οικιακός αυτοματισμός αλλά και οι ευκαιρίες για απομακρυσμένη υγειονομική περίθαλψη αποτελούν απλά παραδείγματα, που το IoT θα διαδραματίσει ουσιαστικό ρόλο. Παράλληλα, στον επιχειρηματικό κόσμο, ο αντίκτυπος είναι εξίσου σημαντικός. Τα ηλεκτρονικά

πλέγματα μεταφοράς ενέργειας, η αυτοματοποίηση στην εφοδιαστική αλυσίδα και τα ευφυή συστήματα κινητικότητας ανθρώπων και αγαθών, εμπεριέχονται στις προτάσεις του IoT. Τα δομικά χαρακτηριστικά που αναφέρονται στο IoT, και του προσδίδουν την αξία που έχει στη σύγχρονη ζωή, είναι τα παρακάτω:

• *Διάχυτη αίσθηση:* Πέρα από τις φυσικές αισθήσεις, με τις οποίες οι άνθρωποι αντιλαμβάνονται το φυσικό κόσμο, στα πλαίσια του IoT, εμπεριέχονται όλες οι τεχνολογίες αντίληψης και κατανόησης του περιβάλλοντος, στηριζόμενες στα ασύρματα δίκτυα. Με τον τρόπο αυτό, επιτυγχάνεται η ταυτοποίηση των αντικειμένων, είτε από τις σταθερές τους ιδιότητες (πχ. σχήμα, χρώμα, μέγεθος), είτε από τις δυναμικές (πχ. συμπεριφορά, ανάδραση). Ακόμα, περιβαλλοντικά δεδομένα όπως η θερμοκρασία και η υγρασία συνδράμουν προς την κατεύθυνση αυτή. Αντικειμενικός σκοπός του IoT είναι η ελαχιστοποίηση του κενού μεταξύ του φυσικού κόσμου και του κυβερνοχώρου, έτσι ώστε ο φυσικός κόσμος να είναι πληρέστερο έλεγχο.

• *Δίκτυο των δικτύων:* Το IoT εσωκλείει μια πληθώρα διαφορετικών δικτύων. Τα περισσότερα από αυτά δεν είναι ομοιογενή, με συνέπεια να απαιτείται ιδιαίτερη προσπάθεια για τον συγκερασμό τους. Την προσπάθεια αυτή δυσχεραίνει το γεγονός ότι τα εν λόγω δίκτυα στηρίζονται και σε διαφορετικά πρωτόκολλα επικοινωνίας. Μια ολοκληρωμένη ενοποίηση των δικτύων αυτών όμως, είναι απαραίτητη προϋπόθεση για την εποικοδομητική εγκαθίδρυση του IoT.

• *Ευφυή επεξεργαστική ικανότητα:* Οι υπολογιστικές δυνατότητες του IoT, σε αντιδιαστολή με τις αντίστοιχες ανθρώπινες, υπερτερούν στην ταχύτητα αλλά και στην πολυπλοκότητα της επεξεργασίας. Επίσης, μεγάλης σημασίας είναι το γεγονός ότι αυτή η επεξεργασία στο IoT μπορεί να γίνεται σε πραγματικό χρόνο, ταυτόχρονα δηλαδή με την εισροή των δεδομένων.

Το IoT αποτελεί ένα δίκτυο συσκευών που μεταδίδουν/αξιοποιούν δεδομένα από το φυσικό περιβάλλον, για να παρέχουν κάποια υπηρεσία και μπορούν να επικοινωνούν μέσω Διαδικτύου. Για παράδειγμα μπορεί αυτό να είναι ένα έξυπνο τηλέφωνο (smart-phone) ή ένας αισθητήρας υγρασίας εδάφους σε ένα χωράφι, που στέλνει μετρήσεις σε κάποια διαδικτυακή υπηρεσία μέσω του GSM δικτύου. Υπάρχουν ήδη παγκοσμίως, περίπου 18 δισεκατομμύρια συσκευές συνδεδεμένες στο Διαδίκτυο και προβλέπεται να φτάσουν στις 50 δισεκατομμύρια συσκευές, μέχρι το έτος 2020. Το μεγαλύτερο μέρος

από αυτές δεν είναι υπολογιστές με την παραδοσιακή μορφή (smartphone/laptop/tablet), αλλά είναι «πράγματα» (things), δηλαδή κάποιο άλλο είδος ενσωματωμένης συσκευής (embedded device) με αισθητήρες. Από μια ευρύτερη προοπτική, η συμβολή αρκετών τεχνολογιών και τάσεων της αγοράς προσφέρουν τη δυνατότητα για να διασυνδεθούν περισσότερες και μικρότερες έξυπνες συσκευές, εύκολα και φθηνά:

- Απεριόριστες δυνατότητες σύνδεσης, υψηλής ταχύτητας και χαμηλού κόστους, διάχυτη συνδεσιμότητα δικτύου, ιδίως μέσω των ασύρματων υπηρεσιών και τεχνολογιών, που έχουν τη δυνατότητα να κάνουν σχεδόν τα πάντα "συνδεθούν".

- Ευρεία υιοθέτηση IP networking. Το IP (Internet Protocol) έχει γίνει το κυρίαρχο παγκόσμιο πρότυπο για τη δικτύωση, παρέχοντας μια καλά καθορισμένη πλατφόρμα λογισμικού και εργαλεία έτσι ώστε να μπορεί να ενσωματωθεί σε ένα ευρύ φάσμα συσκευών οικονομικά και εύκολα.

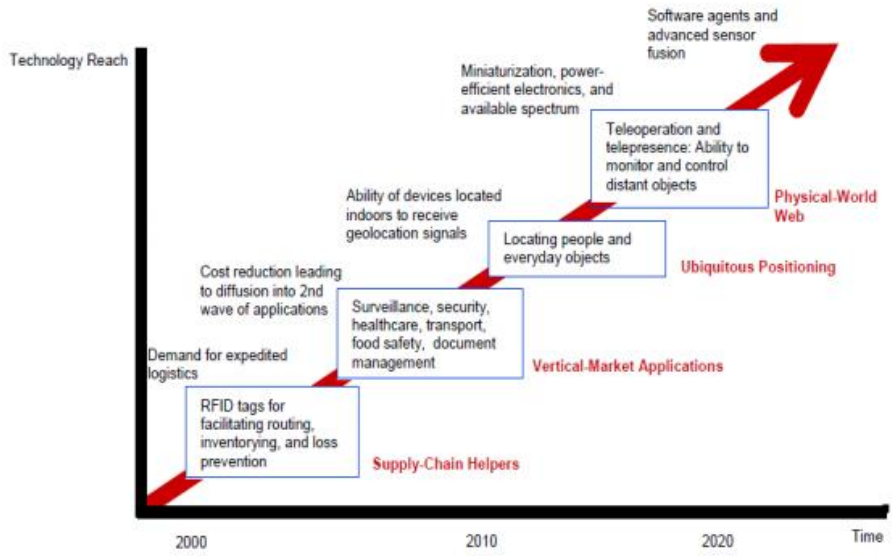
- Υπολογιστική οικονομία, όπως, για παράδειγμα, τη βιομηχανία επενδύσεων στον τομέα της έρευνας, της ανάπτυξης και της κατασκευής, Ο νόμος του Moore συνεχίζει να αποδίδει μεγαλύτερη υπολογιστική ισχύ σε χαμηλότερες τιμές και με χαμηλότερη κατανάλωση ρεύματος.

- Πλεονεκτήματα στην ανάλυση δεδομένων, δηλαδή δημιουργία νέων αλγορίθμων και ταχεία αύξηση της υπολογιστικής ισχύος, αποθήκευσης δεδομένων και υπηρεσιών cloud με σκοπό την ομαδοποίηση, τη συσχέτιση και ανάλυση των τεράστιων ποσοτήτων δεδομένων, εκ των οποίων μας δίνετε η δυνατότητα νέων ευκαιριών για την εξαγωγή πληροφοριών και γνώσεων.

- Εξάπλωση του Cloud Computing, το οποίο μπορεί να μας δώσει τη δυνατότητα για μια απομακρυσμένη διαχείριση δικτυωμένων πόρων για την επεξεργασία, κατανομή και αποθήκευση δεδομένων. Επίσης επιτρέπει σε μικρές συσκευές διανομής να χρησιμοποιούν ισχυρά back-end analytics[2] και δυνατότητες ελέγχου.

Στην Εικόνα 1 που ακολουθεί, φαίνεται η χρονολογική εξέλιξη του IoT:

[2] Τα εργαλεία λογισμικού που έχουν την δυνατότητα να μας παρέχουν πληροφορίες είτε υπό μορφή απλών δεδομένων (raw data) είτε μέσω γραφημάτων (graphs) και τάσεων (trends) σχετικά με την συμπεριφορά και τις ενέργειες των επισκεπτών σε μια ιστοσελίδα ονομάζονται Analytics, μπορούμε να τα συναντήσουμε επίσης και ως Web Analytics, Digital Analytics ή Business Analytics. Για να χρησιμοποιήσουμε τα εργαλεία αυτά συνήθως τοποθετούμε μερικές γραμμές κώδικα σε κάθε σελίδα του site από την οποία θέλουμε να αντλήσουμε πληροφορίες. Όταν η σελίδα φορτώνεται μέσω ενός internet browser εκτελείτε ο κώδικας που έχουμε εισάγει και αποστέλλονται οι σχετικές πληροφορίες στο Analytics λογισμικό για περαιτέρω επεξεργασία.



Εικόνα 1: Χρονολογική εξέλιξη του IoT (htt4)

2.2 Τρόπος και χαρακτηριστικά λειτουργίας του Διαδικτύου των Πραγμάτων

Το Διαδίκτυο των πραγμάτων (IoT) είναι ένα σημαντικό θέμα στη βιομηχανία της τεχνολογίας, την πολιτική και τους κύκλους της μηχανικής και έχει γίνει πρωτοσέλιδο τόσο στον Τύπο όσο και στα δημοφιλή μέσα μαζικής ενημέρωσης (Huh, 2017). Αυτή η τεχνολογία ενσωματώνεται σε ένα ευρύ φάσμα δικτυωμένων προϊόντων , συστημάτων και αισθητήρων , τα οποία επωφελούνται από τις προόδους στην υπολογιστική ισχύ, στην νανοτεχνολογία και τις διασυνδέσεις δικτύου, προσφέροντας νέες δυνατότητες άνευ προηγουμένου. Η εφαρμογή του IoT σε μια ευρεία κλίμακα συσκευών , υπόσχεται να μετατρέψει πολλές πτυχές του σύγχρονου τρόπου ζωής. Τα νέα προϊόντα IoT, όπως οι internet - enabled συσκευές, τα εξαρτήματα οικιακού αυτοματισμού και συστήματα διαχείρισης ενέργειας κατευθύνουν τους καταναλωτές πιο κοντά στο όραμα που ονομάζεται «έξυπνο σπίτι», προσφέροντας μεγαλύτερη αποτελεσματικότητα σε θέματα ασφάλειας και ενέργειας.

Άλλες IoT συσκευές όπως wearable συσκευές εκγύμνασης, συσκευές παρακολούθησης της υγείας και οι δικτυακές ιατρικές συσκευές μετατρέπουν τον τρόπο με τον οποίο παρέχονται οι υπηρεσίες υγειονομικής περίθαλψης. Αυτή η τεχνολογία είναι ιδιαίτερα επωφελής για τα άτομα με αναπηρίες και τους ηλικιωμένους, επιτρέποντας την βελτίωση των επιπέδων της ανεξαρτησίας και της ποιότητας ζωής τους. Συστήματα IoT όπως , δικτυακά οχήματα, ευφυή συστήματα κυκλοφορίας και

αισθητήρες ενσωματωμένοι σε δρόμους και γέφυρες τα οποία συμβάλλουν στην ελαχιστοποίηση της κυκλοφοριακής συμφόρησης και της κατανάλωσης ενέργειας, μας φέρνουν πιο κοντά στην ιδέα της «έξυπνης πόλης».

Η τεχνολογία IoT προσφέρει τη δυνατότητα χρησιμοποιώντας δικτυακούς αισθητήρες , να μεταμορφώσει τη γεωργία, τη βιομηχανία καθώς και την παραγωγή και διανομή της ενέργειας, αυξάνοντας τη διαθεσιμότητα των πληροφοριών κατά μήκος της αλυσίδας αξίας της παραγωγής. Ωστόσο , το IoT εγείρει πολλά ζητήματα και προκλήσεις που πρέπει να εξεταστούν και να αντιμετωπιστούν προκειμένου να υλοποιηθούν όλα τα παραπάνω οφέλη. Το Διαδίκτυο των πραγμάτων περιλαμβάνει όπως αναφέρθηκε στο κεφάλαιο ένα ευρύ φάσμα εφαρμογών που μεταξύ άλλων περιλαμβάνει έξυπνα δίκτυα, έξυπνες πόλεις για διαχείριση της υγείας. Παρόλα αυτά, η ολοένα και πιο πυκνή και διαδεδομένη συλλογή, επεξεργασία, διάδοση δεδομένων προκαλεί σοβαρά προβλήματα ασφάλειας και προστασίας της ιδιωτικής ζωής. Αρκετά εγγενή χαρακτηριστικά του IoT ενισχύουν τις προκλήσεις ασφάλειας και ιδιωτικότητας, όπως: έλλειψη κεντρικού ελέγχου ετερογένεια πόρων, πολλαπλές επιθέσεις. Η τεχνολογία Blockchain που υποστηρίζει το Bitcoin, το πρώτο σύστημα κρυπτοεικονισμού που ξεκίνησε το 2008, μπορεί να προσφέρει μια αποτελεσματική λύση στο ιδιωτικό απόρρητο και την ασφάλεια του Διαδικτύου.

Οποιοσδήποτε κόμβος στο δίκτυο peer-to-peer μπορεί να επιλέξει να είναι miner, δηλαδή μια οντότητα που είναι υπεύθυνη για την εξόρυξη μπλοκ ενός Blockchain με την επίλυση ενός κρυπτογραφικού παζλ πόρων που ονομάζεται *(POW – Proof Of Work)* (Brambilla, 2016). Αυτό χρησιμοποιείται για την προσθήκη νέων μπλοκ στο Blockchain. Η συγκεκριμένη τεχνολογία προσφέρει υψηλό προστασίας της ιδιωτικής ζωής, χρησιμοποιώντας ένα μεταβαλλόμενο δημόσιο κλειδί (PK - Public Key) ως ταυτότητα των χρηστών. Η συγκεκριμένη τεχνολογία έχει επίσης υιοθετήσει μια σειρά μη χρηματικών εφαρμογών, όπως είναι η απόδειξη της τοποθεσίας, τα κατανεμημένα συστήματα αποθήκευσης και τα στοιχεία (δεδομένα) περί υγειονομικής περίθαλψης. Τα σημαντικά χαρακτηριστικά των Blockchain το καθιστούν προσφιλές για την παροχή διανεμημένης ιδιωτικότητας και ασφάλειας στο IoT. Ωστόσο, δεν είναι απλή η εφαρμογή του Blockchain στο IoT και αυτό γιατί πρέπει να αντιμετωπιστούν βασικές προκλήσεις συμπεριβαλλομένων μεταξύ άλλων των εξής:

- υψηλές απαιτήσεις σε πόρους λόγω χρήσης της απόδειξη εργασίας POW,

- ζητήματα επεκτασιμότητας, που προέρχονται από την ανάγκη συναίνεσης μεταξύ των διαφορετικών χρηστών,
- μεγάλες καθυστερήσεις που αποδίδονται στο POW.

Η συμβολή του παρόντος κεφαλαίου είναι η εισαγωγή ενός *νέου τύπου BC (Blockchain) που έχει βελτιστοποιηθεί για το IoT*. Για να υποδείξουμε την ιδέα μας χρησιμοποιούμε το σενάριο ενός έξυπνου σπιτιού. Ωστόσο, η αρχιτεκτονική είναι εφαρμογή για ποικίλες περιπτώσεις χρήσης IoT. Το πλαίσιο εργασίας απαρτίζεται από τρία επίπεδα που είναι: έξυπνο σπίτι, δίκτυο επικάλυψης και αποθήκευση υπολογιστικού νέφους. Οι συσκευές του IoT στο έξυπνο σπίτι, επωφελούνται από ένα *ιδιωτικό υπολογιστικό βιβλίο ή ημερολόγιο (IL – Immutable Ledger)* που δρα με τρόπο παρόμοιο με το Blockchain , αλλά η διαχείρισή του είναι κεντρική και χρησιμοποιεί την κεντρική κρυπτογράφηση για να μειώσει τα γενικά έξοδα επεξεργασίας, ενώ οι υψηλότερες συσκευές πόρων δημιουργούν από κοινού μια κατανεμημένη επικάλυψη που παράγει ένα δημόσιο Blockchain. Οι επικοινωνίες μεταξύ οντοτήτων σε διαφορετικές βαθμίδες είναι γνωστές ως *συναλλαγές* που ομαδοποιούνται σε μπλοκ, που είναι προσαρτημένα στο Blockchain χωρίς να επιλυθεί το POW, το οποίο μειώνει σημαντικά την προσαύξηση.

Οι επαληθευμένες υπογεγραμμένες συναλλαγές είναι διαθέσιμες άμεσα για όλο το δίκτυο, γεγονός που μειώνει σημαντικά την καθυστέρηση των συναλλαγών του Διαδικτύου των πραγμάτων, όπως είναι η πρόσβαση σε δεδομένα ή ερωτήματα. Χρησιμοποιείται μια κατανεμημένη μέθοδος εμπιστοσύνης στην επικάλυψη για τη μείωση των γενικών εξόδων της επεξεργασίας κατά την επικύρωση νέων μπλοκ. Συγκεντρώνουμε ποιοτικά την ανθεκτικότητα της προτεινόμενης μεθόδου έναντι των επιθέσεων και αξιολογούμε ποσοτικά το πακέτο και τα έξοδα επεξεργασίας μέσω προσομοιώσεων.

2.3 Χαρακτηριστικά λειτουργίας Έξυπνου Σπιτιού

Με τον όρο *έξυπνο σπίτι* εννοούμε μία κατοικία, η οποία αλληλεπιδρά με ολοκληρωμένα συστήματα επικοινωνίας, για να γίνει καταγραφή και διαχείριση των διαφορετικών λειτουργών της και να βελτιωθεί έτσι ο τρόπος ζωής των ενοίκων της (Arabo, 2014). Η ανάγκη για όλο και περισσότερες ηλεκτρικές συσκευές (κουζίνα,

ψυγείο, κ.λ.π) που θα έχουν τη δυνατότητα πρόσβασης στο Διαδίκτυο, με τη χρήση του οικιακού δρομολογητή, και η ανάπτυξη των κινητών υπολογιστικών συσκευών, ανοίγει το δρόμο για τη δημιουργία έξυπνων σπιτιών. Με τον όρο *οικιακός αυτοματισμός* μπορούμε να περιγράψουμε τα έξυπνα σπίτια, και αυτό γιατί όλες οι έξυπνες συσκευές λειτουργούν συγχρονισμένα προκειμένου να πετύχουν αυτοματοποιημένες οικιακές εργασίες.

Η άνεση και η ευκολία που παρέχεται είναι ένα από τα πλεονεκτήματα που μας προσφέρει η τεχνολογία των έξυπνων σπιτιών. Επιπλέον πλεονεκτήματα είναι η γρηγορότερη ανταπόκριση στις μεταβολές του περιβάλλοντος ή σε παραβιάσεις της ασφάλειας της οικίας, αλλά και στην αποδοτικότερη ενεργειακή χρήση. Στην ουσία επιζητείται η άνεση ώστε ο ένοικος να μπορεί να είναι ήρεμος ότι θα υλοποιηθούν αυτόματα οι εργασίες του. Ήδη και οι πιο συνηθισμένες οικίες παρέχουν κάποιου είδους ανέσεις και ευκολίες. Για παράδειγμα, ο θερμοστάτης καθορίζει αυτόματα τη λειτουργία του κλιματιστικού και το πλυντήριο μπορεί να ρυθμιστεί να τελειώσει σε συγκεκριμένο χρόνο. Ακόμα, ο εγκατεστημένος συναγερμός μπορεί να ειδοποιεί αυτόματα τις αρχές σε περίπτωση παραβιάσεων.

Με την χρήση όμως του IoT αλλάζουν δραστικά κάποιες διαδικασίες. Για παράδειγμα, στην περίπτωση του θερμοστάτη, αυτός μπορεί να επικοινωνεί με το γκαράζ, ώστε να αντιλαμβάνεται την παρουσία/απουσία των ενοίκων. Επίσης, με την χρήση του πλυντηρίου είναι δυνατό να υπάρχει σύνδεση με το κινητό μας τηλέφωνο, ώστε να μας ενημερώνει για τον τερματισμό της λειτουργίας του, ή μια ενεργοποίηση του συστήματος συναγερμού μπορεί να ενεργοποιεί το κλείδωμα σε όλες τις θύρες του σπιτιού και να ειδοποιήσει τους γειτονικούς ένοικους για την παραβίαση της οικίας. Όλα τα παραπάνω στηρίζονται στη δυνατότητα οι διάφορες ηλεκτρικές συσκευές να συνδέονται στο Διαδίκτυο, αλλά και στη μεταξύ τους δικτύωση. Συνεπώς, η διαχείριση της πλειοψηφίας των ηλεκτρικών συσκευών από τα κινητά τηλέφωνα και τους υπολογιστές αποτελεί την πιο ενδεδειγμένη προοπτική. Όσο αφορά στον τομέα της οικιακής ασφάλειας, χωρίς αμφιβολία τα υπάρχοντα συστήματα ασφαλείας διαθέτουν αισθητήρες και ανιχνευτές, που εγγυώνται υψηλά επίπεδα προστασίας. Η διασύνδεση όμως αυτών των αισθητήρων με δικτυακές κάμερες και το κινητό τηλέφωνο του χρήστη που επιφέρει το IoT, προσφέρει μεγαλύτερη κάλυψη στο χώρο της ασφάλειας. Επιπλέον οι αισθητήρες, αφού είναι συνδεδεμένοι και με άλλες ηλεκτρικές συσκευές,

μπορούν να αντιληφθούν την παρουσία ή απουσία του ένοικου και ανάλογα μπορούν να βρεθούν σε λειτουργία ή να σβήσουν. Στην Εικόνα 2 που ακολουθεί, φαίνεται ένα έξυπνο σπίτι.

Εικόνα 2: Έξυπνο Σπίτι (htt6)

Εκτός του αντικλεπτικού χαρακτήρα, ένα ολοκληρωμένο σύστημα ασφάλειας ανιχνεύει καπνό, διαρροές των υδραυλικών συστημάτων ή οτιδήποτε θα μπορούσε να βλάψει την οικία, ειδοποιώντας παράλληλα τις αρμόδιες αρχές (πυροσβεστική, αστυνομία) αλλά και τον ένοικο, μέσω του ηλεκτρονικού τηλεφώνου που διαθέτει. Επιπλέον, στα πλαίσια της ορθής λειτουργίας του οικιακού εξοπλισμού, ηλεκτρικές συσκευές όπως πλυντήρια και ψυγεία είναι δυνατό να δέχονται ενημερώσεις και να ρυθμίζεται η λειτουργία τους μέσω Διαδικτύου. Αυτές οι διαδικασίες είναι ιδιαίτερα χρήσιμες στις περιπτώσεις ηλικιωμένων ανθρώπων ή ατόμων με ειδικές ανάγκες. Ακόμα υπάρχει βελτίωση στον τομέα της ενεργειακής απόδοσης και ιδιαίτερα στη χρήση των λαμπτήρων φωτισμού μιας οικίας, το IoT τους δίνει την δυνατότητα να αντιλαμβάνονται τόσο τη φωτεινότητα της ατμόσφαιρας όσο και την φυσική παρουσία ατόμων στους διάφορους χώρους της οικίας, έτσι ώστε να προσαρμόζονται ανάλογα.

Όμως, για να μπορέσουμε να έχουμε τις παραπάνω διαδικασίες, απαιτείται η δημιουργία μιας σειράς βασικών στοιχείων και παραγόντων. Δηλαδή, το IoT, στα πλαίσια του έξυπνου σπιτιού, θα πρέπει να στηρίζεται σε κάποια συγκεκριμένα στοιχεία. Οι διάφοροι αισθητήρες είναι αυτοί που θα αντιλαμβάνονται τις

περιβαλλοντικές συνθήκες είτε είναι αυτόνομοι είτε περιέχονται σε άλλες συσκευές. Στα έξυπνα σπίτια, στις συνθήκες αυτές περιέχονται:

- Η υγρασία
- Η κίνηση
- Ο θόρυβος
- Ο φωτισμός

Επιπλέον, όταν οι διάφορες συσκευές είναι δικτυωμένες μεταξύ τους, είναι δυνατόν η μία να αντιλαμβάνεται την κατάσταση λειτουργίας της άλλης. Οι τρόποι αυτοί επικοινωνίας των οικιακών συσκευών και αισθητήρων συμβάλλουν στην ανταλλαγή πληροφοριών και δεδομένων μεταξύ τους και είναι είτε ασύρματοι είτε ενσύρματοι. Οι πιο γνωστές και συχνές ασύρματες τεχνολογίες που χρησιμοποιούνται για τους συγκεκριμένους σκοπούς είναι το Bluetooth, το Wi-Fi και το Wi-MAX , αλλά και η παράλληλη σύνδεση των συσκευών με τον οικιακό δρομολογητή για την αξιοποίηση πληροφοριών του Διαδικτύου. Τέλος, διάφοροι δίαυλοι και ελεγκτές είναι απαραίτητα εργαλεία ενός έξυπνου σπιτιού και αλλιώς ονομάζονται sentrollers (sensor/controller).

Μερικά χαρακτηριστικά παραδείγματα ενός έξυπνου σπιτιού είναι ένας θερμοστάτης, ο οποίος πέρα από το γεγονός ότι αφομοιώνει τις ιδιαίτερες συνθήκες θερμοκρασίας κάθε χώρου και προσαρμόζεται σε αυτές, έχει την ιδιότητα, μέσω εντοπισμού θέσης από την εφαρμογή για κινητά τηλέφωνα που υπάρχει, να αντιλαμβάνεται το πότε ο ιδιοκτήτης βρίσκεται κοντά στο σπίτι ώστε αυτό να προθερμαίνεται. Στη συνέχεια, ένα έξυπνο σύστημα συναγερμού παρέχει την πλήρη παρακολούθηση και ελέγχει την οικία από το κινητό τηλέφωνο του εκάστοτε χρήστη.

Αισθητήρες και κάμερες αλληλεπιδρούν με το τηλέφωνο του ιδιοκτήτη και στέλνουν ειδοποιήσεις για κάθε περίεργη δραστηριότητα. Χωρίς αμφιβολία, το πιο γνωστό αντικείμενο που αποτελεί παράδειγμα IoT, και περιλαμβάνεται σταδιακά στις οικίες είναι η έξυπνη τηλεόραση (smart TV). έχει ξεπεράσει κατά πολύ τις παραδοσιακές τηλεοράσεις των προηγούμενων ετών. Με μεγάλη ακρίβεια, η smart TV παρέχει τη δυνατότητα σύνδεσης στο Διαδίκτυο, ως ένας κλασικός υπολογιστής, αλλά και ασύρματης διαχείρισης της από εφαρμογές κινητών τηλεφώνων και ταμπλετών.

Επιπλέον μπορεί να έχει επικοινωνία και με άλλα αντικείμενα, όπως κάμερες παρακολούθησης, που έχουν την δυνατότητα να μεταδίδουν εικόνα στην τηλεόραση σε πραγματικό χρόνο και ασύρματα. Εν κατακλείδι, τα έξυπνα σπίτια αποτελούν την πιο ελκυστική πρακτική IoT, η οποία μας φέρνει πιο κοντά στα σπίτια του μέλλοντος. Μέσα από τους εγκατεστημένους αισθητήρες, και της δυνατότητας που υπάρχει, για απομακρυσμένη λειτουργία τους, ανοίγονται καινούργιοι δρόμοι στην διαχείριση των κατοικιών.

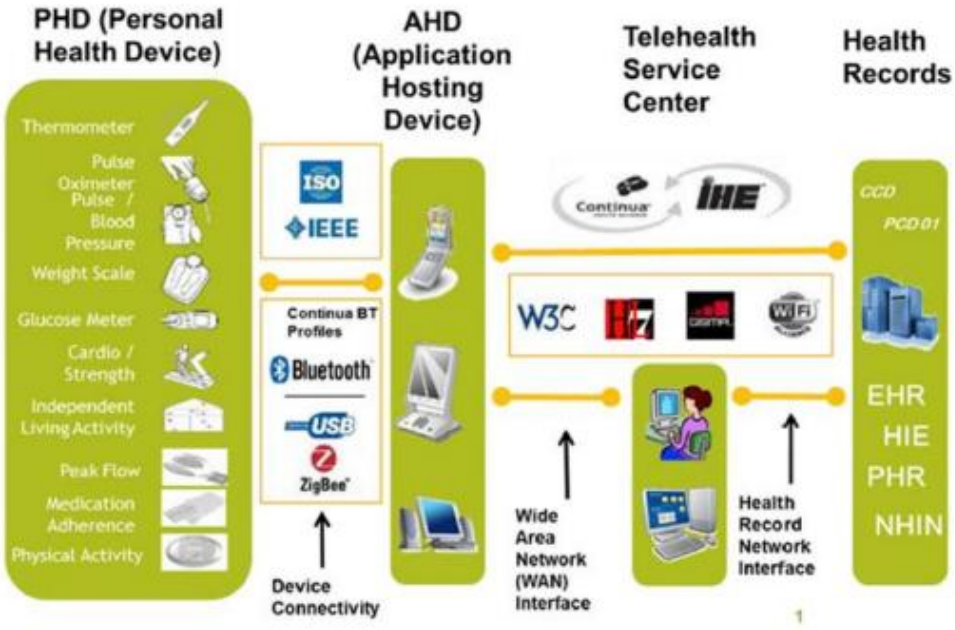
Σε ό,τι αφορά τις εφαρμογές, μέσω τηλεφώνων με ενσωματωμένους αισθητήρες RFID[3] υπάρχει η δυνατότητα να χρησιμοποιηθούν ως πλατφόρμα, για την παρατήρηση από απόσταση ιατρικών δεικτών σε ασθενείς αλλά και για τον έλεγχο της διανομής των φαρμάκων. Τα βασικά πλεονεκτήματα όμως βρίσκονται στην εξ' αποστάσεως διάγνωση και πιθανή αντιμετώπιση μιας ασθένειας αλλά και στην γρήγορη παροχή ιατρικής γνωμάτευσης σε περίπτωση πιθανών ατυχημάτων.

Ασύρματες συσκευές (EHR) είναι ικανές να εντοπιστούν μέσω IP διεύθυνσης και μπορούν να χρησιμοποιηθούν για να αποθήκευση ενός ιατρικού ιστορικού ασθενή. Ένα ηλεκτρονικό μητρώο υγείας (EHR - Electronic Health Records) ή ηλεκτρονικό ιατρικό ιστορικό (EMR) είναι η συστηματική συλλογή ηλεκτρονικά αποθηκευμένων πληροφοριών για την υγεία των ασθενών και του πληθυσμού σε ψηφιακή μορφή. Αυτά τα αρχεία μπορούν να μοιραστούν σε διαφορετικές ρυθμίσεις υγειονομικής περίθαλψης. Τα αρχεία μοιράζονται μέσω δικτύων, επιχειρηματικών πληροφοριακών συστημάτων ή άλλων δικτύων και ανταλλαγών πληροφοριών. Τα EHR μπορούν να περιλαμβάνουν μια σειρά δεδομένων, συμπεριλαμβανομένων των δημογραφικών δεδομένων, ιατρικού ιστορικού, φαρμάκων και αλλεργιών, κατάσταση ανοσοποίησης, αποτελέσματα εργαστηριακών εξετάσεων, εικόνες ακτινολογίας, ζωτικά σημεία, προσωπικές στατιστικές όπως ηλικία και βάρος και πληροφορίες χρέωσης

Οι ηλεκτρονικές αυτές καταγραφές συλλέγουν κομβικά δεδομένα για τον ασθενή, όπως για παράδειγμα αλλεργίες, προηγούμενες ασθένειες, δοσολογίες φαρμάκων, αλλά και πληροφορίες για την τρέχουσα πορεία της θεραπεία. Η χρήση αυτών των συσκευών

[3] Τα αρχικά RFID προέρχονται από τη φράση "Radio Frequency IDentification", που σημαίνει ταυτοποίηση μέσω ραδιοσυχνοτήτων. Πρόκειται για μια τεχνολογία που χρησιμοποιεί ραδιοκύματα για τον εντοπισμό και την ανάγνωση στοιχείων. Στην ουσία πρόκειται για μια μετεξέλιξη των γνωστών barcodes. Για να δουλέψει ένα σύστημα RFID χρειάζεται αφενός ένας πομποδέκτης, το RFID tag, καθώς και μια συσκευή ανάγνωσης για να το διαβάζει. Ο πομποδέκτης είναι τόσο μικρός που χωράει σε μια μικρή αυτοκόλλητη ετικέτα (RFID tag) και αποτελείται από ένα μικροτσίπ με ενσωματωμένη κεραία για να στέλνει τα δεδομένα στη συσκευή ανάγνωσης.

γίνεται δυνατή από γιατρούς και νοσηλευτές μέσω RFID ετικετών. Όλο αυτό θα μπορούσε να είναι ιδιαίτερα κομβικό σε επείγουσες καταστάσεις όπου οι ασθενείς πάσχουν από διαβήτη, Alzheimer, καρδιακές ανεπάρκειες κ.λ.π. Επίσης, βιοδιασπώμενα τσιπ μπορούν να εγκατασταθούν στο ανθρώπινο σώμα για πρόληψη και παρακολούθηση. Σε παραπληγικούς ασθενείς, εμφυτευμένα «έξυπνα» εξαρτήματα μπορούν να προκαλέσουν ηλεκτρική διέγερση στους μύες αυτών, προκειμένου να αποκαταστήσουν κινητικές λειτουργίες. Η Τηλεϊατρική είναι ο κλάδος της ιατρικής που επικεντρώνεται σε τεχνολογίες IoT προκειμένου να εξελιχθεί. Στην Εικόνα 3 που ακολουθεί, παρατηρούμε το τρόπο με τον οποίο μια συγκεκριμένη εταιρεία απεικονίζει τη διαδικασία περισυλλογής ιατρικών δεδομένων. Από τη στιγμή που ο ασθενής κάνει κάποιες προσωπικές μετρήσεις, αυτές μέσω τεχνολογιών IoT συναθροίζονται και μετά από την επεξεργασία τους κάνει τη διάγνωση ο επιβλέπων ιατρός.



Εικόνα 3: Διασυνδεδεμένες συσκευές σύμφωνα με Continua Health Alliance (htt3)

2.4 Εισαγωγή στην τεχνολογία Blockchain

Βρισκόμαστε στην αρχή μιας νέας επανάστασης που ξεκίνησε μια περιθωριακή οικονομία στο Διαδίκτυο, δηλαδή ένα εναλλακτικό νόμισμα που ονομάστηκε bitcoin και εκδόθηκε και υποστηρίχτηκε όχι από μια κεντρική αρχή, αλλά από μια αυτοματοποιημένη συναίνεση μεταξύ των δικτυωμένων χρηστών (Michael, 2015). Η πραγματικότητα της νέας επανάστασης είναι ότι δεν απαιτεί από τους χρήστες να

εμπιστεύονται ο ένας τον άλλο, αλλά μέσω μιας αυτό-αστυνόμευσης ελέγχει οποιαδήποτε κακόβουλη προσπάθεια εξαπάτησης του συστήματος θα αποδειχθεί. Με ακριβή και τεχνικό ορισμό, το bitcoin είναι ψηφιακό ρευστό που διακινείται μέσα στο Διαδίκτυο σε ένα αποκεντρωμένο σύστημα χωρίς εμπιστοσύνη, χρησιμοποιώντας ένα δημόσιο βιβλίο που ονομάζεται Blockchain. Πρόκειται για μια νέα μορφή χρημάτων που συνδυάζει την κοινή χρήση αρχείων BitTorrent με κρυπτογράφηση δημόσιου κλειδιού. Από την έναρξή της το 2009, η Bitcoin δημιούργησε μια ομάδα μιμητών εναλλακτικών νομισμάτων, χρησιμοποιώντας την ίδια γενική προσέγγιση αλλά με διαφορετικές βελτιστοποιήσεις.

Με άλλα λόγια, το Blockchain αποτελεί έναν τύπο βάσης δεδομένων που δέχεται ένα πλήθος εγγραφών από τους χρήστες, τις οποίες τοποθετεί σε ένα φύλλο δεδομένων γνωστό ως block. Κάθε χρήστης διατηρεί ένα αντίγραφο αυτού του block. Καθώς οι εγγραφές αυξάνονται, κάθε block συνδέεται με μία γραμμική, χρονολογική σειρά με το επόμενο δημιουργώντας μία αλυσίδα (Blockchain), με τη χρήση μίας κρυπτογραφημένης υπογραφής. Η διαδικασία αυτή επιτρέπει στο Blockchain να χρησιμοποιείται σαν ένα δημόσιο λογιστικό βιβλίο (ledger), το οποίο μπορεί να μοιραστεί και να επιβεβαιωθεί από οποιοδήποτε εξουσιοδοτημένο χρήστη. Η ιδιότητα αυτή το καθιστά αποκεντρωμένο (decentralized) καθότι και η εποπτεία της ορθότητας της συναλλαγής διαμοιράζεται σε όλους τους χρήστες του και δεν περιορίζεται σε ένα χρηματοπιστωτικό ίδρυμα.

Πιο συγκεκριμένα, η τεχνολογία Blockchain θα μπορούσε να γίνει το απρόσκοπτο ενσωματωμένο οικονομικό στρώμα που δεν έχει ποτέ ο Ιστός, για να λειτουργήσει ως τεχνολογική βάση για πληρωμές, αποκεντρωμένες ανταλλαγές, μεταφορές ψηφιακών περιουσιακών στοιχείων και έξυπνες συμβάσεις. Η τεχνολογία Bitcoin και Blockchain , ως τρόπος αποκέντρωσης, θα μπορούσε να είναι η επόμενη μείζονα ανατρεπτική τεχνολογία της παγκόσμια Πληροφορική (ακολουθώντας το main-frame, το PC, το Διαδίκτυο και την κοινωνική δικτύωση/κινητό τηλέφωνα), με τη δυνατότητα να αναδιαμορφώνουν όλη την ανθρώπινη δραστηριότητα.

Αν και κάπως πρώιμο, η χρήση της τεχνολογίας Blockchain και των κρυπτονομισμάτων, το άμεσο παράγωγο αυτής, είναι ικανή να εμποδίσει την εμφάνιση χρηματικών απατών. Η χρήση των έξυπνων συμβολαίων – προγράμματα και πρωτόκολλα που διευκολύνουν την πραγματοποίηση των όρων μίας συμφωνίας αφού

έχουν τηρηθεί οι διάφοροι όροι και η εκ ορισμού της τεχνολογίας καταγραφής όλων των συναλλαγών σε συνδυασμό με την κρυπτογραφική μοναδικότητα των νομισμάτων θα ελαχιστοποιήσουν τις πιθανότητες διαπροσωπικών ή και εταιρικών απατών μέσω «λογιστικών μαγειρεμάτων».

Το Blockchain είναι ένα διμερές σύστημα. Ο εξοστρακισμός των ενδιαμέσων επομένως οδηγεί σε εκμηδενισμό των τελών των συναλλαγών ή των συναλλαγματικών διαφορών που χρεώνονται από τα παραδοσιακά χρηματοπιστωτικά ιδρύματα. Οι επιπρόσθετες χρεώσεις μπορεί να αφορούν επίσης νομικές, μεσιτικές, ή άλλους είδους συμβουλευτικές υπηρεσίες. Η τεχνολογία Blockchain μπορεί να μετριάσει τις προκλήσεις ρευστότητας παρέχοντας ένα τρόπο μείωσης της τριβής μέσω της μαθηματικής επικύρωσης των συναλλαγών. Μόλις η συναλλαγή επιβεβαιωθεί, παρέχεται μία ενοποιημένη, ανθεκτική στην παραβίαση ορατότητα στο αρχείο συναλλαγών. Η χαμηλή τριβή και η καλύτερη ορατότητα βελτιώνουν την απόδοση όλων των τύπων των συναλλαγών, όχι μόνο των συναλλαγών ομολόγων και άλλων τίτλων.

Με την πρώτη ματιά, η τεχνολογία αυτή αποτελεί απειλή για το χρηματοπιστωτικό τομέα. Ωστόσο, μπορεί να επιφέρει σημαντική στην αποτελεσματικότητα τους. Αντί της συμμετοχής πολλών ανθρώπων στη διαδικασία επικύρωσης μίας συναλλαγής και μία γραφειοκρατικής διαδικασίας που διαρκεί μέρες ή εβδομάδες για διακρατικές συναλλαγές, η μαθηματική επικύρωση μπορεί να επιβεβαιώσει μεγάλο όγκο συναλλαγών αυτοματοποιημένα. Αυτή η εξέλιξη θα οδηγήσει στην κατάσταση των άμεσων συναλλαγών, εκσυγχρονίζοντας τη βιομηχανία. Τέλος, η τεχνολογία Blockchain διαθέτει τη δυναμική να εισβάλλει σε ποικίλες βιομηχανίες, συμπεριλαμβανομένων της μουσικής, του μάρκετινγκ, της υγείας, της δημόσιας διοίκησης και αλλού. Ο καταιγισμός ιδεών για συσχετιζόμενες εταιρίες και πλατφόρμες τα τελευταία χρόνια είναι σημαντικός και αποδίδει καρπούς. Πολλές εταιρίες ακόμα και χώρες πειραματίζονται ενεργά με την νέα τεχνολογία και τα αποτελέσματα είναι ιδιαιτέρως ενθαρρυντικά.

Η τεχνολογία Blockchain είναι απλά στην αρχή της και έχει σαφώς τη δυναμική να αλλάξει συνήθειες, μεθοδολογίες και συστήματα. Ωστόσο, οι αδυναμίες της τεχνολογίας είναι ορατές ακόμα και στους πιο πιστούς οπαδούς της. Για παράδειγμα, το περιβαλλοντολογικό κόστος, η έλλειψη κανονισμών, η πολυπλοκότητα της και τα

τεχνικά της προβλήματα είναι μερικά από τα τρωτά της σημεία. Όπως και να έχει, αποτελεί σίγουρα μία εναλλακτική για να αντιμετωπιστούν τα προβλήματα του τρέχοντος χρηματοοικονομικού συστήματος που είναι αρκετά, και αποτέλεσαν την αφορμή για τη δημιουργία του Blockchain μετά την αμερικανική τραπεζική κρίση του 2008.

Ένα Blockchain (μπλοκ αλυσίδας) αποτελεί ένα νέο τρόπο αποθήκευσης και μεταφοράς πληροφορίας (Alphand, 2018). Οι κεντρικές βάσεις δεδομένων έχουν χρησιμοποιηθεί εδώ και πολλά χρονιά από τις χρηματοπιστωτικές εταιρίες για την αποθήκευσης στοιχείων πελατών και την καταγραφή συναλλαγών. Πρόκειται για συστήματα προσεκτικά φυλασσόμενα και κλειστά, στα οποία επιτρέπονται μόνο προνομιούχοι χρήστες. Αυτό συνεπάγεται ορισμένες συνέπειες. Ένα συγκεντρωτικό σύστημα είναι αυτό που εξ ορισμού έχει σημείο αποτυχίας. Είναι επίσης ένα γεγονός που συνεπάγεται διαφορά ισχύος, επειδή οι προνομιακοί φορείς εκμετάλλευσης έχουν το προνόμιο να παρεμβαίνουν μονομερώς, αντιστρέφοντας μια συναλλαγή ή επιβάλλοντας νέες χρεώσεις. Το Blockchain προσφέρει μια ριζικά διαφορετική προσέγγιση. Το πρωτόκολλο Bitcoin (Arabo, 2014), το οποίο δρομολογήθηκε το 2009, καθιέρωσε για πρώτη φορά τη βιωσιμότητα της μεταβίβασης αξίας σε ομότιμη βάση μέσω του Διαδικτύου, χωρίς την ανάγκη ενός αξιόπιστου διαμεσολαβητή. Ο Satoshi Nakamoto, ο ψευδώνυμος δημιουργός του Bitcoin, επιλύει το πρόβλημα της διπλής δαπάνης: το ζήτημα ότι οι ψηφιακές πληροφορίες μπορούν εύκολα να αντιγραφούν και, ως εκ τούτου, έπρεπε προηγουμένως να συγκεντρωθεί μια κεντρική αρχή για να αντικατοπτρίζει το που βρίσκονται τα κεφάλαια.

Πιο απλά, το Blockchain είναι ένα ψηφιακό αρχείο που αποθηκεύεται σε ένα δίκτυο υπολογιστών σε όλο τον κόσμο. Αντί να εξασφαλίζει πληροφορίες περιορίζοντας την πρόσβαση, το Blockchain *μοιράζεται πληροφορίες μεταξύ όλων των χρηστών*. Η ιδιοκτησία των κεφαλαίων ελέγχεται κρυπτογραφικά και η πλήρης διαφάνεια και η αμοιβαία ιδιοκτησία του συστήματος σημαίνει ότι ένας κακός φορέας είναι άμεσα αναγνωρίσιμος και ότι αγνοούνται οι συναλλαγές που υποβάλλονται από έναν τέτοιο κόμβο. Η αποκεντρωμένη δομή του Blockchain διαθέτει πολλά βασικά χαρακτηριστικά σε αντίθεση με τις παραδοσιακές συγκεντρωτικές προσεγγίσεις, τα οποία περιγράφονται στη συνέχεια:

- *Διαφάνεια*: είναι πιθανό ο καθένας να παρακολουθεί την κίνηση κεφαλαίων από το ένα λογαριασμό στον άλλο.

- *Μεταβλητότητα*: αφού επιβεβαιωθεί, μια συναλλαγή δεν μπορεί να αντιστραφεί. Κανείς δεν μπορεί να παρεμβαίνει σε μια ολοκληρωμένη μεταφορά.

- *Χαμηλό κόστος*: τα τέλη συναλλαγών είναι ελάχιστα.

- *Διασυνοριακή επικοινωνία*: τα χρήματα μπορούν να αποστέλλονται τόσο εύκολα σε κάποιον που βρίσκεται στην άλλη άκρη του κόσμου, όσο και σε κάποιον που είναι στο επόμενο δωμάτιο.

- *Ταχύτητα*: λόγω της επίπεδης και διαφανούς φύσης του Blockchain , οι μεταφορές εμφανίζονται σχεδόν *άμεσα* και συνήθως επιβεβαιώνονται σε λεπτά, αντί για ώρες ή ημέρες.

Παρόλο που το Bitcoin έχει πολύ μεγάλη επιτυχία στη μεταφορά της αξίας και είναι μια αποτελεσματική μορφή αποκεντρωμένου χρήματος, από την αρχή αναγνωρίστηκε ότι η ίδια προσέγγιση θα μπορούσε να χρησιμοποιηθεί για την καταγραφή πληροφοριών σχεδόν οποιουδήποτε είδους στην ίδια κοινή βάση (Miller, 2015). Εκτός από τα χρήματα, οι ακολουθίες των χαρακτήρων (strings) στο Blockchain θα μπορούσαν να αντιπροσωπεύουν απλά μηνύματα, ιδιοκτησία φυσικών ή ψηφιακών περιουσιακών στοιχείων ή τίτλων, αποφάσεις ψηφοφορίας κ.ο.κ. Αυτή η ευρύτερη εφαρμογή αναπτύχθηκε από διάφορες πλατφόρμες '2.0' συμπεριλαμβανομένων των Nxt[4] και BitShares[5], μεταξύ άλλων. Αυτό εξασφαλίζει ότι η ασφάλεια των χρημάτων είναι πλήρως ενημερωμένη. Εκτός από αυτό, το Blockchain εξασφαλίζει *πλήρη ανωνυμία*. Εκτός από τον παραλήπτη και τον αποστολέα του νομίσματος, κανένας τρίτος δεν έχει πρόσβαση στα δεδομένα. Ο λόγος για αυτό είναι ότι οι πληροφορίες δεν μεταδίδονται σε κεντρικό διακομιστή. Ένα χαρακτηριστικό του νομίσματος, το οποίο εκτιμάται ιδιαίτερα από τους επενδυτές, είναι η *δυνατότητα συμμετοχής*.

[4] Το Nxt είναι κρυπτογράφηση 100% proof-of-stake (απόδειξη πονταρίσματος), κατασκευασμένο από το μηδέν σε open source Java 1. Η απόδειξη του συστήματος πονταρίσματος προσελκύει πολλή προσοχή αυτές τις μέρες, με το Ethereum να μεταβαίνει σε αυτό το σύστημα από την απόδειξη του συστήματος εργασίας. Η απόδειξη του πλειστηριασμού είναι μια εναλλακτική διαδικασία επαλήθευσης συναλλαγών σε ένα blockchain. Αυξάνεται στη δημοτικότητα και υιοθετείται από αρκετές κρυπτοσυχνότητες. Για να κατανοήσουμε την απόδειξη της συμμετοχής, είναι σημαντικό να έχουμε μια βασική ιδέα της απόδειξης της εργασίας. Από αυτή τη γραφή, η μέθοδος της απόδειξης εργασίας χρησιμοποιείται από Bitcoin, Ethereum και τις περισσότερες άλλες σημαντικές κρυπτοσυχνότητες.

[5] Το Bitshares Coin δημιουργήθηκε ως κρυπτονόμισμα που είναι αποκεντρωμένο και βασίζεται στο blockchain.

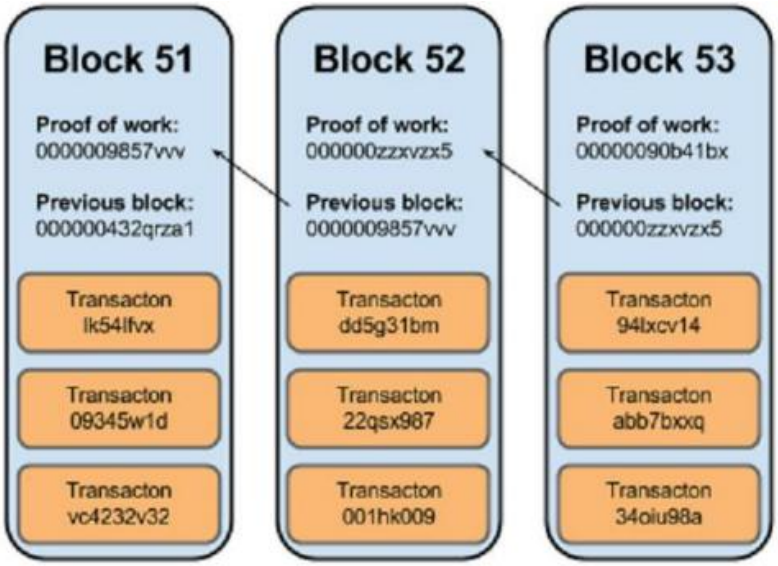
Πιο συγκεκριμένα, οι μέτοχοι και όλα τα μέλη της κοινότητας μπορούν να συμμετέχουν στις αποφάσεις σχετικά με τις μελλοντικές εξελίξεις. Αυτό ισχύει όχι μόνο για τις ανησυχίες σχετικά με την ασφάλεια αλλά και για τις αποφάσεις Μάρκετινγκ και εξυπηρέτησης. Οι επενδυτές επωφελούνται από αυτό, επειδή η δημοτικότητα του κέρματος διαδραματίζει καθοριστικό ρόλο. Και οι δύο αυτοί παράγοντες γενικά οδηγούν σε αύξηση της κεφαλαιοποίησης της αγοράς και, ως εκ τούτου, της τιμής ανά μονάδα. Για τους επενδυτές που εντάχθηκαν νωρίς, αυτό σημαίνει ισχυρές αποδόσεις κερδών. Μέχρι σήμερα, ωστόσο, όλα αυτά ήταν σχετικά περιορισμένα κατά τον ένα ή τον άλλο τρόπο και δεν είχαν την κατάλληλη μορφή στις τρέχουσες μορφές τους για υιοθέτηση από τις πραγματικές χρηματοπιστωτικές επιχειρήσεις. Το Blockchain μπορεί να αποθηκευτεί ως ένα απλό αρχείο, ή σε μια απλή βάση δεδομένων. Τα μπλοκ συνδέονται προς τα "πίσω", με το κάθε ένα να έχει αναφορά στο προηγούμενο μπλοκ στην αλυσίδα. Το Blockchain συχνά εμφανίζεται σαν μια κάθετη στοίβα, με τα μπλοκ σε επίπεδα το ένα πάνω από το άλλο και το πρώτο μπλοκ που εξυπηρετεί ως θεμέλιο της στοίβας. Η οπτικοποίηση των μπλοκ να στοιβάζονται το ένα πάνω στο άλλο έχει σαν αποτέλεσμα τη χρήση όρων όπως "ύψος" για την απόσταση από το πρώτο μπλοκ και "κορυφή" ή "άκρη" για το πιο πρόσφατο μπλοκ που προστέθηκε μέσα στην αλυσίδα.

Κάθε μπλοκ εντός της αλυσίδας του Blockchain προσδιορίζεται από μια συνάρτηση κατακερματισμού (hash function) που παράγεται με τη χρήση του SHA256[6] αλγόριθμου κρυπτογράφησης στην κεφαλίδα του μπλοκ. Κάθε μπλοκ αναφέρεται επίσης στο προηγούμενο μπλοκ (parent block) μέσα από το πεδίο *προηγούμενο μπλοκ hash* στην κεφαλή του μπλοκ. Με άλλα λόγια, κάθε μπλοκ περιέχει το hash του γονέα μέσα στη δική του επικεφαλίδα. Η ακολουθία των hash συνδέει κάθε μπλοκ προς τον γονέα του, δημιουργώντας έτσι μία αλυσίδα η οποία πηγαίνει πίσω σε όλη τη διαδρομή μέχρι το πρώτο μπλοκ που δημιουργήθηκε ποτέ, όπως φαίνεται στην Εικόνα 2 που ακολουθεί.

Παρά το γεγονός ότι ένα μπλοκ έχει ένα μόνο γονέα, μπορεί να έχει προσωρινά πολλαπλά παιδιά. Κάθε ένα από τα παιδιά αναφέρεται στο ίδιο μπλοκ ως γονέα και περιέχει το ίδιο γονικό hash στο πεδίο *προηγούμενο μπλοκ hash*. Πολλαπλά παιδιά

[6] Μέλος των κρυπτογραφικών λειτουργιών κατακερματισμού SHA-2 που έχει σχεδιάσει η NSA. Το SHA σημαίνει Algorithm Secure Hash. Οι κρυπτογραφικές λειτουργίες κατακερματισμού είναι μαθηματικές λειτουργίες που εκτελούνται σε ψηφιακά δεδομένα, με τη σύγκριση του υπολογιζόμενου "hash" (της απόδοσης από την εκτέλεση του αλγορίθμου) με μια γνωστή και αναμενόμενη τιμή hash.

μπορούν να προκύψουν κατά τη διάρκεια ενός **Blockchain fork**, που ουσιαστικά είναι μια προσωρινή κατάσταση που εμφανίζεται όταν τα διάφορα μπλοκ που ανακαλύπτονται σχεδόν ταυτόχρονα, προκύπτουν από διαφορετικούς εξορύκτες. Τελικά, μόνο ένα παιδί μπλοκ γίνεται μέρος του Blockchain και το Blockchain έχει επιλυθεί. Ακόμα κι αν ένα μπλοκ έχει περισσότερα από ένα παιδιά, μπορεί να έχει μόνο ένα γονέα. Αυτό οφείλεται στο γεγονός ότι κάθε μπλοκ έχει ένα μόνο πεδίο *προηγούμενο μπλοκ hash* το οποίο αναφέρεται στον μοναδικό γονέα του. Το πεδίο hash προηγούμενου μπλοκ είναι μέσα στην κεφαλίδα του μπλοκ και με τον τρόπο αυτό επηρεάζει το hash του τρέχοντος μπλοκ. Η ταυτότητα του παιδιού αλλάζει εάν αλλάξει η ταυτότητα του γονέα. Όταν ο γονέας έχει τροποποιηθεί με οποιονδήποτε τρόπο, αλλαγές πραγματοποιούνται στο hash του γονέα. Το αλλαγμένο hash του γονέα απαιτεί μια αλλαγή στο *hash προηγούμενου μπλοκ* δείκτη του παιδιού. Αυτό με τη σειρά του προκαλεί το hash του παιδιού να αλλάξει, το οποίο απαιτεί μια αλλαγή στο δείκτη του εγγονιού, το οποίο με τη σειρά του αλλάζει το εγγόνι, και ούτω καθεξής.



Εικόνα 4: Τρόπος λειτουργίας Blockchain (htt7)

Αυτό το αποτέλεσμα αλληλουχίας εξασφαλίζει ότι μόλις ένα μπλοκ έχει πολλές γενεές να το ακολουθούν, δεν μπορεί να αλλάξει χωρίς να αναγκάζει τον επαναϋπολογισμό όλων των μεταγενέστερων μπλοκ. Επειδή ένας τέτοιος επαναϋπολογισμός θα απαιτούσε τεράστιους υπολογισμούς, η ύπαρξη μιας μακράς αλυσίδας μπλοκ κάνει τη ιστορία του Blockchain αμετάβλητη, κάτι το οποίο αποτελεί βασικό χαρακτηριστικό της ασφάλειας του. Όταν κάποιος θέλει να προσθέσει μια συναλλαγή στην αλυσίδα, όλοι οι συμμετέχοντες στο δίκτυο θα την επικυρώσουν. Αυτό γίνεται με την εφαρμογή ενός αλγορίθμου στην συναλλαγή για την επαλήθευση της

εγκυρότητας της. Τι ακριβώς νοείται ως "έγκυρο" ορίζεται από το σύστημα Blockchain και μπορεί να διαφέρει μεταξύ των συστημάτων. Στη συνέχεια, εναπόκειται στην πλειοψηφία των συμμετεχόντων να συμφωνούν ότι η συναλλαγή είναι έγκυρη.

Ένα σύνολο των εγκεκριμένων συναλλαγών στη συνέχεια ομαδοποιείται σε ένα μπλοκ, το οποίο αποστέλλεται σε όλους τους κόμβους του δικτύου. Αυτοί με τη σειρά τους επικυρώνουν το νέο μπλοκ. Κάθε διαδοχικό μπλοκ περιέχει μια συνάρτηση κατακερματισμού (hash), η οποία αποτελεί ένα μοναδικό δακτυλικό αποτύπωμα, του προηγούμενου μπλοκ. Κατ' αυτό τον τρόπο, το Blockchain λειτουργεί ως ένα αποκεντρωμένο (decentralized) λογιστικό καθολικό, το οποίο είναι κοινό για όλους τους συμμετέχοντες, μιας και όλοι οι εμπλεκόμενοι αποθηκεύουν ένα αντίγραφό του, κάτι που εξασφαλίζει την ασφάλεια και η διαφάνεια των συναλλαγών. Η ειδοποιός διαφορά -αναφορικά με την προστασία- προκύπτει από το γεγονός ότι δεν είναι πλέον απαραίτητη η ύπαρξη μιας ενδιάμεσης «έμπιστης» αρχής (π.χ. μιας τράπεζας), ενώ η εμπιστοσύνη των συναλλασσόμενων μερών βασίζεται σε αλγοριθμική επιβεβαίωση.

2.5 Οφέλη και περιορισμοί τεχνολογίας Blockchain

Ενώ τις τελευταίες δεκαετίες το κεντρικοποιημένο μοντέλο λειτουργεί ικανοποιητικά στην πράξη, θα υπάρξει πρόβλημα όταν ο αριθμός των κόμβων ενός δικτύου μεγαλώσει αρκετά και δημιουργήσει πλήθος συναλλαγών, και αυτό θα συμβεί διότι εκτός της αύξησης των υπολογιστικών απαιτήσεων θα έχουμε αύξηση και στο κόστος (Buchman, 2016). Ακόμα, σε μια τέτοια περίπτωση μπορεί να παρατηρηθεί στους διακομιστές ενός δικτύου κυκλοφοριακή συμφόρηση (bottlenecks) και επίσης και σημεία αποτυχίας, καθιστώντας τα δίκτυα του Διαδικτύου των Πραγμάτων (IoT) ευάλωτα σε επιθέσεις τύπου DoS (Denial of Service)[7]. Επίσης, σε βιομηχανικές περιοχές είναι δύσκολη η εγκατάσταση κεντρικοποιημένων δικτύων, γιατί οι κόμβοι του IoT θα επεκταθούν σε μεγάλες περιοχές με τις ταχύτητες σύνδεσης να είναι χαμηλές.

[7] Επιθέσεις που έχουν σκοπό να αποτρέψουν τη χρήση ενός συστήματος από όλους (δηλαδή τους νόμιμους χρήστες του). Δεν γίνονται προσπάθειες παραβίασης ή κλοπής στοιχείων – Είναι όμως δυνατός ο συνδυασμός τους με άλλες επιθέσεις που γίνονται παράλληλα με σκοπό να παραπλανήσουν τα συστήματα ανίχνευσης (Intrusion Detection Systems) και τους διαχειριστές από την πραγματική απειλή

Η Blockchain τεχνολογία μπορεί να προστατεύσει αποτελεσματικά την αυθεντικότητα (authenticity) και την ακεραιότητα (integrity) των συναλλαγών και έχει την δυνατότητα να παίξει σημαντικό ρόλο στο οικοσύστημα του IoT, μειώνοντας το κόστος και το χρόνο της κάθε εργασίας. Επίσης μειώνει την ανάγκη για κανονισμούς και δίνει την δυνατότητα της ενσωμάτωσης νόμων στον κώδικα, που με την σειρά τους θα μπορούν να εκτελούνται αυτόματα. Επιπλέον, χρησιμοποιώντας αυτή την τεχνολογία θα δοθεί η δυνατότητα δημιουργίας ασφαλών δικτύων πλέγματος, όπου με τρόπο αξιόπιστο οι έξυπνες συσκευές του IoT θα μπορούν να διασυνδεθούν, αποφεύγοντας έτσι απειλές όπως η κλοπή στοιχείων ταυτότητας και η πλαστογράφηση μιας υπογραφής. Έτσι ο εντοπισμός συσκευών στην αλυσίδα Blockchain και η πραγματοποίηση ελέγχων ταυτότητας χωρίς την ανάγκη πιστοποίησης από κάποιον κεντρικό διακομιστή είναι εύκολος.

Η ύπαρξη εμποδίων που δυσχεραίνουν την ευρεία υιοθέτηση της τεχνολογίας Blockchain είναι όμως αναμφισβήτητη. Όμως, ο όγκος των συναλλαγών, το κόστος της ενέργειας, αλλά και η αποθήκευση των δεδομένων που αποτελούν τα τρία μεγαλύτερα προβλήματα, θα πρέπει να μας απασχολούν. Η χρήση των Merkle Trees[8] είναι μια πρόταση για τη μείωση της πολυπλοκότητας στην επαλήθευση μιας συναλλαγής. Είναι δεδομένο ότι η δημόσια πρόσβαση στο Blockchain κάνει ευκολότερη τη διαφάνεια στις συναλλαγές και τη διάχυση της πληροφορίας. Επιπλέον, διευκολύνεται και η ελεγκτική διαδικασία με την εξάλειψη κάθε ενδεχομένου παραβιάσεων, εξαιτίας της δημόσιας χρήσης των δεδομένων. Ακόμα, μειώνεται και η ανάγκη για μεσολαβητές που αυξάνοντας τα κόστη αποκομίζουν κέρδη, και αυτό γιατί βρίσκονται κρυπτογραφημένες μέσα στο Blockchain όλες οι πληροφορίες που αφορούν τις συναλλαγές,. Έτσι, οι τράπεζες έχουν τη δυνατότητα να εξοικονομήσουν αρκετά δισεκατομμύρια κάθε χρόνο με τη μείωση του χρόνου διακανονισμού αλλά και την κατάργηση μιας σειράς διαδικασιών και μεθόδων που κοστίζουν τόσο σε χρόνο όσο και χρήμα [4].

Στη συνέχεια, παρατίθεται μια σειρά από υπηρεσίες του χρηματοπιστωτικού κλάδου που θα μπορούσαν να βελτιωθούν και να γίνουν πιο ασφαλείς και πιο γρήγορες

[8] Στην Κρυπτογραφία ένα δέντρο κατακερματισμού ή το δέντρο Merkle είναι ένα δέντρο στο οποίο κάθε κόμβος που είναι φύλλο φέρει μια ετικέτα με την κρυπτογραφική συνάρτηση κατακερματισμού (hash) ενός μπλοκ δεδομένων και κάθε κόμβος που δεν είναι φύλλο φέρει μια ετικέτα με την κρυπτογραφική συνάρτηση κατακερματισμού (hash) των κόμβων που είναι παιδιά του. Τα δέντρα hash επιτρέπουν την αποτελεσματική και ασφαλή επαλήθευση περιεχομένου μεγάλων δομών δεδομένων.

για τη χρήση του Blockchain. Λόγω των προαναφερόμενων, μπορούμε να συμπεράνουμε ότι τα **πλεονεκτήματα** που προκύπτουν από τη χρήση της Blockchain τεχνολογίας, είναι τα ακόλουθα [5]:

- *Παροχή δεδομένων υψηλής ποιότητας:* τα δεδομένα Blockchain είναι ακριβή, συνεπή και ευρέως διαθέσιμα.
- *Απλούστευση οικοσυστήματος:* όλες οι συναλλαγές συσσωρεύονται σε ένα ενιαίο δημόσιο καθολικό (ledger), ελαχιστοποιώντας τα προβλήματα που θα μπορούσαν να δημιουργηθούν από την ύπαρξη πολλών καθολικών.
- *Χαμηλότερο κόστος συναλλαγών:* εξαλείφοντας τους μεσάζοντες και τα γενικά έξοδα που χρειάζονται για την ανταλλαγή περιουσιακών στοιχείων, πετυχαίνεται σημαντική μείωση των εξόδων συναλλαγής.
- *Ταχύτερες συναλλαγές:* σε μια τράπεζα οι συναλλαγές μπορεί να χρειαστούν και ημέρες για να μπορέσουν να διευθετηθούν. Αντίθετα, στις συναλλαγές Blockchain υπάρχει η δυνατότητα να μειωθεί ο συνολικός χρόνος συναλλαγής και αυτές να λειτουργούν χωρίς χρονικούς περιορισμούς.
- *Ακεραιότητα διαδικασιών:* Στις συναλλαγές Blockchain οι χρήστες μπορούν να εμπιστοσύνη και έτσι επί της ουσίας η ανάγκη για ένα έμπιστο τρίτο μέρος, όπως είναι οι τράπεζες, καταργείται.

Στην αντίπερα όχθη τα **μειονεκτήματα** στην τεχνολογία Blockchain , που μπορούμε να παρατηρήσουμε είναι τα ακόλουθα [6]:

- *Έλεγχος, ασφάλεια και προστασία της ιδιωτικότητας:* ενώ υπάρχει η δυνατότητα για μία ισχυρή κρυπτογράφηση, εξακολουθούν να υπάρχουν ανησυχίες για την ασφάλεια, έτσι το κοινό δυσκολεύεται να αναθέσει τα προσωπικά του δεδομένα σε ένα Blockchain.
- *Μεγάλη κατανάλωση ενέργειας:* στο Blockchain οι miners[9] εκτελούν πάρα πολλές λύσεις ανά δευτερόλεπτο για την επικύρωση των συναλλαγών, καταναλώνοντας έτσι σημαντικές ενεργειακές ποσότητες του υπολογιστή.

[9]Με τον όρο miners εννοούμε τα άτομα εκείνα που χρησιμοποιούν ειδικό λογισμικό για να λύσουν μαθηματικά προβλήματα και να λάβουν ως αντάλλαγμα συγκεκριμένες ποσότητες κρυπτονομισμάτων. Το πρώτο πράγμα που πρέπει κανείς να γνωρίζει είναι ότι η ισχύς εξόρυξης (mining power) καθορίζεται από την κάρτα γραφικών και η εξόρυξη μέσω επεξεργαστών έχει καταστεί ατελέσφορη για την περίπτωση των bitcoin. Αν και υπάρχουν

- *Υψηλό αρχικό κόστος κεφαλαίου:* ενώ το Blockchain προσφέρει τεράστια εξοικονόμηση του κόστους συναλλαγών, λόγω του υψηλού αρχικού κόστους κεφαλαίου που απαιτείται, θα μπορούσε να αποτελέσει αποτρεπτικό παράγοντα προς την χρήση της συγκεκριμένης τεχνολογίας.

2.6 Άνοδος του Bitcoin και χαρακτηριστικά

Η άνοδος του Bitcoin και των παρόμοιων πρωτοκόλλων συνοδεύτηκε από ταχεία επανεξέταση των υφιστάμενων παραδειγμάτων από τις κυβερνήσεις, τις ρυθμιστικές αρχές και τον κλάδο των χρηματοπιστωτικών υπηρεσιών (Bhardwaj, 2016). Λόγω της θέσης του Bitcoin εκτός του ελέγχου των κρατικών και χρηματοπιστωτικών αρχών και των δυνατοτήτων κατάχρησης ως μέσου απάτης, νομιμοποίησης εσόδων από παράνομες δραστηριότητες και άλλων παράνομων δραστηριοτήτων, καθώς και άλλων προβλημάτων, όπως η αστάθεια και ο μη ρυθμιζόμενος χαρακτήρας των ανταλλαγών στις οποίες οι πρώτες αντιδράσεις τείνουν να είναι σκεπτικισμός και ανησυχία. Ωστόσο, ένας αυξανόμενος αριθμός φορέων αναγνώρισε επίσης το δυναμικό της τεχνολογίας Blockchain και το ευρύ φάσμα των περιπτώσεων χρήσης, στις οποίες προσφέρεται.

Σημαντική μετατόπιση έχει σημειωθεί προς το τέλος του 2015 και το 2016, με μια σειρά εθνικών κυβερνήσεων και μεγάλων τραπεζών να διεξάγουν ενεργά έρευνα για την κατανεμημένη τεχνολογία λογιστικών βιβλίων (DLT) ως μέσο για τη δημιουργία πιο αποτελεσματικών χρημάτων και την παροχή αποτελεσματικότερων δημόσιων υπηρεσιών - τουλάχιστον η βρετανική κυβέρνηση [2], η Κίνα, η Νότια Κορέα, η Goldman Sachs και η UBS, μεταξύ άλλων. Περίπου 1 δισεκατομμύριο δολάρια επενδύθηκαν σε εταιρείες που σχετίζονται με το Bitcoin μόνο το 2015. Τα οφέλη της τεχνολογίας Blockchain για εταιρείες και οργανισμούς όλων των μεγεθών και τύπων γίνονται ολοένα και πιο σαφή. Ωστόσο, μέχρι στιγμής υπάρχουν λίγες επιλογές για όσους επιθυμούν να αναπτύξουν ή να χρησιμοποιήσουν τεχνολογία Blockchain. Πρέπει είτε να επενδύσουν το χρόνο και τα χρήματα για να δημιουργήσουν και να διατηρήσουν το δικό τους πρωτόκολλο από το μηδέν, είτε να χρησιμοποιήσουν μια υπάρχουσα ανοιχτή πλατφόρμα (όπως η ίδια η Bitcoin), με όλους τους περιορισμούς και τα προβλήματα που αυτό συνεπάγεται.

κρυπτονομίσματα που μπορεί κανείς να εξορύξει με τον επεξεργαστή, οι κάρτες γραφικών προσφέρουν πολύ μεγαλύτερη ισχύ, λύνοντας πιο γρήγορα τους αλγόριθμους.

Το Blockchain αποτελεί ήδη μια μορφή μετρητών για το Διαδίκτυο, ένα σύστημα ψηφιακών πληρωμών, και αυτό μπορεί να γίνει το "Διαδίκτυο των χρημάτων", που συνδέει τα οικονομικά με τον τρόπο που το Διαδίκτυο των πραγμάτων (IoT) συνδέουν τα μηχανήματα. Το νόμισμα και οι πληρωμές αποτελούν το πρώτο και το μεγαλύτερο προφανή εφαρμογή. Τα εναλλακτικά νομίσματα έχουν νόημα βάσει ενός οικονομικού επιχειρήματος μόνο: μείωση των τελών πληρωμής των και εμπορικών πιστωτικών καρτών παγκοσμίως από 3% όσο και μέχρι κάτω από το 1% έχει προφανή οφέλη για την Οικονομία, ειδικά στην Οικονομία 514 δισεκατομμύρια δολάρια διεθνή εμβασμάτων στην αγορά, όπου τα τέλη συναλλαγών μπορούν να τρέξουν από 7 σε 30 %.

Επιπλέον, οι χρήστες μπορούν να λάβουν άμεσα χρήματα σε ψηφιακά πορτοφόλια αντί να περιμένουν ημέρες για μεταφορές. Το Bitcoin και οι μιμητές του θα μπορούσαν να ανοίξουν το δρόμο για το νόμισμα και το εμπόριο, προκειμένου αυτό να επαναπροσδιοριστεί πλήρως. Σε γενικές γραμμές, το Bitcoin δεν είναι μόνο μια καλύτερη έκδοση της Visa, θα μπορούσε επίσης να μας επιτρέψει να κάνουμε πράγματα δεν έχουμε ακόμη σκεφτεί ακόμα. Το νόμισμα και οι πληρωμές είναι μόνο η πρώτη αίτηση. Η βασική λειτουργικότητα των νομισμάτων Blockchain είναι ότι κάθε συναλλαγή μπορεί να προέλθει και να ολοκληρωθεί απευθείας μεταξύ δύο ατόμων μέσω του Διαδικτύου. Με χρήση των altcoins[10], μπορεί να γίνει η ανταλλαγή πόρων μεταξύ ατόμων με αποκεντρωμένο, διανεμημένο και παγκόσμιο τρόπο. Με αυτήν την ικανότητα, μια κρυπτογράφηση μπορεί να είναι ένα προγραμματιζόμενο ανοιχτό δίκτυο για την αποκεντρωμένη διαπραγμάτευση όλων των πόρων, πολύ πέρα από το νόμισμα και τις πληρωμές. Έτσι, το Blockchain 1.0 για το νόμισμα και τις πληρωμές είναι ήδη επεκταθεί σε Blockchain 2.0, για να επωφεληθεί από την πιο ισχυρή λειτουργικότητα του Bitcoin ως προγραμματιζόμενα χρήματα.

[10] Εκτός από το Bitcoin, υπάρχουν εκατοντάδες άλλα ψηφιακά νομίσματα. Αυτά είναι ευρύτερα γνωστά ως '**Altcoins**', μερικά από τα πιο γνωστά είναι τα ether, litecoin, ripple, monero, dash και πολλά ακόμα. Τα altcoins διαφέρουν από το Bitcoin σε διάφορους τομείς. Μερικά έχουν διαφορετικό οικονομικό μοντέλο ή διαφορετική μέθοδο διανομής των νομισμάτων, όπως πχ altcoins που δόθηκαν στους κατοίκους μιας χώρας. Άλλα, χρησιμοποιούν διαφορετικές μεθόδους απόδειξης εργασίας με διαφορετικούς αλγόριθμους, και άλλα δεν βασίζονται καν σε μεθόδους απόδειξης εργασίας. Πολλά altcoins προσφέρουν την χρήση μιας γλώσσας προγραμματισμού, πάνω στην οποία μπορούν να αναπτυχθούν εφαρμογές, ενώ μερικά altcoin προσφέρουν βαθμό ανωνυμίας ακόμα μεγαλύτερο και από αυτόν του Bitcoin. Υπάρχουν και altcoins που εξυπηρετούν πολύ συγκεκριμένες εφαρμογές, όπως την καταχώριση domain name ή την αποθήκευση δεδομένων. Τα altcoins είναι τυπικά πιο ριψοκίνδυνα από το Bitcoin. Οι αυξομειώσεις τους στις αγορές είναι άστατες, και με την πάροδο των ετών κανένα altcoin δεν διατήρησε την αξία του σε σχέση με το Bitcoin.

Επειδή πολλές από τις ιδέες και τις έννοιες πίσω από Bitcoin και την τεχνολογία Blockchain είναι νέες και τεχνικά περίπλοκες, ένα αρνητικό σημείο είναι το γεγονός ότι οι κρυπτοσυχνότητες είναι πολύ περίπλοκες για την υιοθέτηση της νέας τεχνολογίας. Ωστόσο, το ίδιο ισχύει και για το Διαδίκτυο και γενικότερα για την αρχή κάθε νέας τεχνολογικής εποχής, οι τεχνικές λεπτομέρειες του "τι είναι" και του "πώς λειτουργεί" παρουσιάζουν ενδιαφέρον για ένα δημοφιλές κοινό. Αυτό δεν είναι πραγματικό εμπόδιο; Για παράδειγμα, δεν είναι απαραίτητο να γνωρίζουμε πώς λειτουργεί το TCP/IP, προκειμένου να σταλθεί ένα μήνυμα ηλεκτρονικού ταχυδρομείου και ότι οι νέες τεχνολογικές εφαρμογές μεταφέρονται στη δημόσια χρήση χωρίς να εξετάζονται περαιτέρω οι τεχνικές λεπτομέρειες, όσο αναπτύσσονται κατάλληλες και αξιόπιστες εφαρμογές διεπαφών.

Υπάρχουν πολλά ζητήματα ασφαλείας κρυπτογράφησης για να αντιμετωπιστεί ένα κρυπτογραφημένο κοινό με χρήσιμα πορτοφόλια πελατών, συμπεριλαμβανομένων του πως να δημιουργηθούν αντίγραφα ασφαλείας των χρημάτων, τι να κάνει κάποιος, εάν χάσει το ιδιωτικό του κλειδί και τι να κάνει αν λάβει ένα νόμισμα απαγορευμένο (δηλαδή πριν κλαπεί) σε μια συναλλαγή και τώρα δεν μπορεί να το ξεφορτωθεί. Ωστόσο, αυτά τα ζητήματα αντιμετωπίζονται από τη βιομηχανία Blockchain. Η υιοθέτηση των νομισματικών εφαρμογών θα μπορούσε να είναι απλή με αξιόπιστα χρήσιμα στοιχεία, αλλά η επιτυχής καθολική υιοθέτηση εφαρμογών μπλοκ αλυσίδων πέρα από το νόμισμα θα μπορούσε να είναι πιο λεπτή. Αποθηκεύοντας δεδομένα σε όλο του το δίκτυο, το Blockchain εξαλείφει τους κινδύνους που εγκυμονεί από το να διατηρούνται αυτά τα δεδομένα κεντρικά. Το δίκτυο του δεν έχει κεντρικά σημεία, τα οποία είναι ευπαθή και τα οποία μπορούν να εκμεταλλευτούν οι hackers. Το σημερινό Διαδίκτυο παρουσιάζει προβλήματα ασφάλειας, όπως είναι ευρέως γνωστό. Οι χρήστες χρησιμοποιούν τον συνδυασμό «όνομα χρήστη/κωδικό πρόσβασης» για να προστατέψουμε την ταυτότητα και τα περιουσιακά μας στοιχεία στο διαδίκτυο. Οι μέθοδοι ασφαλείας του Blockchain χρησιμοποιούν τεχνολογία κρυπτογράφησης.

Η βάση αυτού είναι τα επονομαζόμενα δημόσια και ιδιωτικά «κλειδιά». Ένα **δημόσιο κλειδί** (ακολουθία αριθμών που έχουν παραχθεί τυχαία) είναι η διεύθυνση του χρήστη στο Blockchain. Τα Bitcoins που στέλνονται σε όλο το δίκτυο καταγράφονται ότι ανήκουν σε αυτή την διεύθυνση. Το *ιδιωτικό κλειδί* είναι σαν ένας κωδικός που δίνει

στον ιδιοκτήτη του πρόσβαση στο Bitcoin του ή σε άλλα ψηφιακά περιουσιακά του στοιχεία.

Η δημόσια πρόσβαση στο Blockchain διευκολύνει τη διαφάνεια στις συναλλαγές καθώς και τη διάχυση της πληροφορίας. Στο ίδιο πλαίσιο, διευκολύνεται η ελεγκτική διαδικασία με την εξάλειψη κάθε ενδεχομένου παραβάσεων, ακριβώς εξαιτίας της δημόσιας φύσης των δεδομένων. Ταυτόχρονα, εξαλείφεται και η ανάγκη για ενδιάμεσα μέρη που αυξάνουν τα κόστη, αφού όλες οι πληροφορίες που αφορούν στη συναλλαγή βρίσκονται κρυπτογραφημένες μέσα στο Blockchain. Έτσι, για παράδειγμα οι τράπεζες μπορούν να εξοικονομήσουν αρκετά δισεκατομμύρια κάθε χρόνο με την ελαχιστοποίηση του χρόνου διακανονισμού, αλλά και την κατάργηση μίας σειράς διαδικασιών που κοστίζουν σε χρόνο και χρήμα. Από εκεί και πέρα, υπάρχουν μία σειρά από υπηρεσίες και λύσεις στον χρηματοπιστωτικό κλάδο που θα μπορούν να γίνουν καλύτερες, πιο ασφαλείς και να απαιτούν λιγότερο χρόνο υλοποίησης με τη χρήση του Blockchain. Όπως υπάρχουν και αρκετές ακόμη ιδέες που θα μπορούσαν να αξιοποιήσουν τη συγκεκριμένη τεχνολογία και να δημιουργήσουν πολλά νέα προϊόντα και λύσεις για τον χρηματοπιστωτικό κλάδο.

3.1 Τομείς εφαρμογής της τεχνολογίας Blockchain

Υπάρχει μια νέα τεχνολογία που έχει ταράξει τα νερά στις χρηματοπιστωτικές αγορές. Και ενώ το όνομά της – τεχνολογία κατανεμημένου καθολικού (distributed ledger technology - DLT) – μπορεί να ακούγεται τεχνικό, κάποιοι ισχυρίζονται ότι έχει τη δυνατότητα να αλλάξει ολοκληρωτικά τον τρόπο λειτουργίας των χρηματοπιστωτικών αγορών και του τραπεζικού τομέα (Zheng, 2016). Τι ακριβώς είναι λοιπόν αυτή η τεχνολογία και γιατί είναι σημαντική για κεντρικές τράπεζες όπως η ΕΚΤ[11]; Η τεχνολογία κατανεμημένου καθολικού είναι ένα εργαλείο για την καταγραφή της κυριότητας – θα μπορούσε να αναφέρεται για παράδειγμα στην κυριότητα χρήματος ή περιουσιακών στοιχείων, όπως τα ακίνητα. Σήμερα, όταν οι τράπεζες διενεργούν συναλλαγές – δηλαδή όταν μεταβιβάζεται η κυριότητα χρήματος ή χρηματοοικονομικών περιουσιακών στοιχείων – χρησιμοποιούν κεντρικά συστήματα, τα οποία συχνά διαχειρίζονται οι κεντρικές τράπεζες. Οι τράπεζες καταγράφουν τις συναλλαγές τους σε τοπικές βάσεις δεδομένων, οι οποίες επικαιροποιούνται μετά την ολοκλήρωση της συναλλαγής στο κεντρικό σύστημα. Το κατανεμημένο καθολικό, από την άλλη, είναι μια βάση δεδομένων όσον αφορά τις συναλλαγές που, αντί να αποθηκεύεται σε μια κεντρική τοποθεσία, κατανέμεται σε ένα δίκτυο πολλών υπολογιστών. Συνήθως, όλα τα μέλη του δικτύου μπορούν να διαβάζουν τις πληροφορίες και, ανάλογα με τις άδειες που τους έχουν δοθεί, να προσθέτουν στοιχεία.

Ο πιο κοινός τύπος τεχνολογίας κατανεμημένου καθολικού *ονομάζεται αλυσίδα συστοιχιών (Blockchain)*. Η ονομασία αυτή προέρχεται από το γεγονός ότι οι συναλλαγές ομαδοποιούνται προκειμένου να σχηματίσουν συστοιχίες (blocks) οι οποίες συνδέονται μεταξύ τους με χρονολογική σειρά σχηματίζοντας μια αλυσίδα (chain). Η αλυσίδα προστατεύεται στο σύνολό της από σύνθετους μαθηματικούς αλγορίθμους με σκοπό να διασφαλίζεται η ακεραιότητα και η ασφάλεια των δεδομένων. Αυτή η αλυσίδα αποτελεί την ολοκληρωμένη καταγραφή όλων των συναλλαγών που περιλαμβάνονται στη βάση δεδομένων.

Οι αλυσίδες των μπλοκ μετασχηματίζουν ήδη βασικούς κλάδους. Για τις εταιρείες, φαντάζει ιδιαίτερα ελκυστικό να έχουν μια ασφαλή εφοδιαστική αλυσίδα, να

[11] Ευρωπαϊκή Κεντρική Τράπεζα

ξεφορτωθούν τους μεσάζοντες και να μειώσουν τα κόστη. Στη συνέχεια ακολουθούν ορισμένα παραδείγματα εφαρμογής της τεχνολογίας Blockchain :

Ναυτιλία: Η Maersk, η μεγαλύτερη ναυτιλιακή εταιρεία στον κόσμο, ολοκλήρωσε μια δοκιμή χρήσης μιας αλυσίδας των μπλοκ για την παρακολούθηση των φορτίων της. Η δοκιμή περιελάβανε όχι μόνο τη Maersk αλλά και τρίτα μέρη, όπως τα ολλανδικά τελωνεία και το υπουργείο Εσωτερικής Ασφάλειας των ΗΠΑ, και όλοι μαζί παρακολουθούσαν τα εμπορευματοκιβώτια εξ' αποστάσεως. Οι κρυπτογραφικές υπογραφές καθιστούν δυσκολότερη την παραποίηση των ετικετών, ενώ το φορτίο βρίσκεται εν κινήσει, και μπορούν να μειώσουν τον χρόνο της μεταφοράς.

Τραπεζική: Ο τραπεζικός κλάδος ταλαιπωρείται από αργά συστήματα τα οποία χρειάζονται ώρες, ακόμη και μέρες, για την επικύρωση βασικών συναλλαγών, όπως η πώληση μετοχών και η μεταφορά χρημάτων. Η υιοθέτηση των Blockchain s από τη Barclays και άλλες τράπεζες δείχνει ότι τα πράγματα αλλάζουν. Στο εγγύς μέλλον, αναμένεται να αυξηθεί η ταχύτητα των τραπεζικών υπηρεσιών, ενώ οι μεσάζοντες θα αποδιοργανωθούν. Μάλιστα, οι τράπεζες σκέφτονται να χρησιμοποιήσουν αλυσίδες των μπλοκ για τη μετατροπή του συστήματος SWIFT, το οποίο χρησιμοποιείται για παγκόσμιες διατραπεζικές συναλλαγές.

Κτηνοτροφία: Η εταιρεία Walmart[12] ξεκίνησε να χρησιμοποιεί την τεχνολογία της αλυσίδας των μπλοκ το 2016 για να παρακολουθεί το ταξίδι των γουρουνιών από την Κίνα, μέσω της εφοδιαστικής αλυσίδας της εταιρείας, στο τραπέζι των Αμερικανών καταναλωτών. Και τον Αύγουστο ένας κτηνοτροφικός συνεταιρισμός στο Αρκάνσας χρησιμοποίησε κωδικούς QR σε παλέτες με κοτόπουλα για την παρακολούθηση όλων των συναλλαγών που αφορούσαν το συγκεκριμένο φορτίο. Όλα αυτά αναμένεται να βοηθήσουν τις εταιρείες να μειώσουν τα αλλοιωμένα τρόφιμα και να αποτρέψουν τη μετάδοση ασθενειών.

Δίκαιο: Όλα τα είδη συμφωνιών – από πωλήσεις ακινήτων μέχρι επιχειρηματικές αγορές και εργατικές συμβάσεις – απαιτούν δικηγόρους και δικαστήρια για να εφαρμόζονται. Πλέον, ολοένα και περισσότερες εταιρείες πειραματίζονται με «έξυπνες συβάσεις» που εκτελούνται μόνες τους: Ένα σύστημα Blockchain μπορεί, για

[12] Αμερικανική πολυεθνική εταιρία λιανικής που λειτουργεί μια αλυσίδα υπερκαταστημάτων, εκπτωτικών πολυκαταστημάτων και παντοπωλείων.

παράδειγμα, να αποδεσμεύσει τα χρήματα μιας εγγύησης μόλις ένα συμβαλλόμενο μέρος μεταφέρει έναν τίτλο ιδιοκτησίας.

Ενώ είναι ακόμα στα πρώτα στάδια ανάπτυξης του, το IoT αποτελείται ως επί το πλείστο από τεχνολογίες που επιτρέπουν τη συλλογή δεδομένων, την απομακρυσμένη παρακολούθηση και τον έλεγχο των συσκευών. Καθώς η τεχνολογία προχωράει, το IoT θα εξελιχθεί σε ένα δίκτυο αυτόνομων συσκευών που μπορούν να αλληλοεπιδρούν μεταξύ τους και με το περιβάλλον τους και να λαμβάνουν έξυπνες αποφάσεις χωρίς την ύπαρξη ανθρώπινης παρέμβασης. Σε αυτήν την εξέλιξη, η τεχνολογία Blockchain μπορεί να αναπτυχθεί και να αποτελέσει τη βάση που θα υποστηρίξει την επικοινωνία μηχανή -με - μηχανή (M2M – Machine – to - Machine). Η συγκεκριμένη τεχνολογία αποτελεί το συνδετικό κρίκο για να διευθετήσει τις όποιες ανησυχίες για την προστασία της ιδιωτικής ζωής και την αξιοπιστία του IoT. Μπορεί να χρησιμοποιηθεί για την παρακολούθηση δισεκατομμυρίων συνδεδεμένων συσκευών, καθώς επιτρέπει την επεξεργασία των συναλλαγών και του συντονισμού μεταξύ των συσκευών. Αυτό επιτρέπει μια σημαντική εξοικονόμηση για τους κατασκευαστές της βιομηχανίας IoT.

Αυτή η αποκεντρωμένη προσέγγιση θα εξαλείψει ενιαία σημεία της αποτυχίας, δημιουργώντας ένα πιο ανθεκτικό οικοσύστημα για συσκευές που θα τρέξουν πάνω σε αυτό. Οι κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούνται στην τεχνολογία Blockchain , θα καταστήσουν τα δεδομένα των καταναλωτών πιο ιδιωτικά και ασφαλή. Το καθολικό (ledger) του Blockchain είναι απαραβίαστο και δεν μπορεί να χειραγωγηθεί από κακόβουλους παράγοντες, διότι δεν υπάρχει σε μία μόνο θέση, και επιθέσεις δεν μπορούν να οργανωθούν επειδή δεν υπάρχει ένα ενιαίο νήμα της επικοινωνίας που μπορεί να υποκλαπεί. Το Blockchain καθιστά δυνατή ασφαλή, peer-to-peer ανταλλαγή μηνυμάτων και έχει ήδη αποδείξει την αξία του στον κόσμο μέσω των υπηρεσιών κρυπτονομισμάτων, όπως το Bitcoin, παρέχοντας εγγυημένες peer - to-peer υπηρεσίες πληρωμών, χωρίς την ανάγκη για τρίτους.

3.3 Μοντέλα επικοινωνίας του IoT

Από επιχειρησιακή άποψη θα πρέπει να σκεφτούμε πως οι έξυπνες συσκευές συνδέονται και επικοινωνούν μεταξύ τους (Hashemi, 2016). Το Μάρτιο του 2015, η Επιτροπή Αρχιτεκτονικής Δικτύου (IAB) κυκλοφόρησε ένα έγγραφο αρχιτεκτονικής για

τη δικτύωση των έξυπνων αντικειμένων (RFC 7452) που περιγράφει ένα πλαίσιο τεσσάρων κοινών επικοινωνιακών μοντέλων που χρησιμοποιούνται από τις έξυπνες συσκευές. Στη συνέχεια ακολουθεί το πλαίσιο που εξηγεί βασικά χαρακτηριστικά του κάθε μοντέλου.

A. Device to device Communications

Το μοντέλο επικοινωνίας device – to – device εφαρμόζεται σε δύο ή περισσότερες συσκευές που συνδέονται και επικοινωνούν μεταξύ τους με τη χρήση ενός ενδιάμεσου διακομιστή εφαρμογών (application server). Αυτές οι συσκευές επικοινωνούν σε πολλούς τύπους δικτύων, συμπεριλαμβανομένων των δικτύων IP ή του Διαδικτύου. Συχνά όμως οι συσκευές αυτές χρησιμοποιούν πρωτόκολλα, όπως το Bluetooth, το Z-Wave κ.λ.π. Το συγκεκριμένο δίκτυο επιτρέπει στις συσκευές που χρησιμοποιούν ένα συγκεκριμένο πρωτόκολλο επικοινωνίας να επικοινωνήσουν και να ανταλλάξουν μηνύματα για την επίτευξη της λειτουργίας τους.

Το συγκεκριμένο μοντέλο επικοινωνίας χρησιμοποιείται συχνά σε διάφορες εφαρμογές όπως είναι το έξυπνο σπίτι (Smart Home), το οποίο συνήθως χρησιμοποιεί μικρά πακέτα δεδομένων πληροφοριών για επικοινωνία μεταξύ έξυπνων συσκευών με σχετικά χαμηλό ποσοστό πακέτων δεδομένων. Οι έξυπνες οικιακές συσκευές, όπως οι λάμπες, οι διακόπτες φωτών κ.λ.π. στέλνουν μικρά ποσά πληροφοριών το ένα προς το άλλο, για παράδειγμα μια κλειδαριά πόρτας στέλνει μήνυμα ενεργοποίησης στα φώτα όταν ξεκλειδώνεται.

Το μοντέλο επικοινωνίας *device-to-device* (D2D) παρουσιάζει πολλά προβλήματα συμβατότητας, γεγονός που σημαίνει ότι οι κατασκευαστές έξυπνων συσκευών πρέπει να επενδύσουν σε συσκευές που υποστηρίζουν ειδικές και όχι τυποποιημένες μορφές δεδομένων. Από τη μεριά του χρήστη αυτό σημαίνει ότι το βασικό πρωτόκολλο επικοινωνίας device-to-device δεν είναι συμβατό, υποχρεώνοντας το χρήστη να επιλέξει μια οικογένεια συσκευών που χρησιμοποιούν ένα κοινό πρωτόκολλο. Αυτές οι ασυμβατότητες συχνά περιορίζουν την επιλογή του χρήστη σε συσκευές μέσα σε ένα συγκεκριμένο πρωτόκολλο, επομένως ο χρήστης επωφελείται όταν γνωρίζει ότι τα προϊόντα με συγκεκριμένη οικογένεια έχουν τη δυνατότητα να επικοινωνούν σωστά μεταξύ τους.

B. Device – to - Cloud Communications

Στο συγκεκριμένο μοντέλο επικοινωνίας η έξυπνη συσκευή συνδέεται άμεσα με μια συγκεκριμένη υπηρεσία Cloud (όπως για παράδειγμα μια εφαρμογή Παρόχου Ασύρματων Υπηρεσιών) για ανταλλαγή δεδομένων και ελέγχου της κυκλοφορίας των μηνυμάτων. Η προσέγγιση αυτή αξιοποιεί συχνά τους υπάρχοντες μηχανισμούς, όπως π.χ. το ενσύρματο Internet ή διάφορες συνδέσεις Wi-Fi, για να δημιουργηθεί έτσι μια σύνδεση μεταξύ της συσκευής και του δικτύου IP, το οποίο τελικά συνδέεται με το cloud.

Αυτό το μοντέλο επικοινωνίας χρησιμοποιείται από ορισμένες δημοφιλείς καταναλωτικές έξυπνες συσκευές όπως οι smart TV της Samsung. Μια cloud σύνδεση επιτρέπει στο χρήστη να επιτύχει απομακρυσμένη πρόσβαση στο θερμοστάτη του σπιτιού του μέσω ενός έξυπνου τηλεφώνου και επίσης να υποστηρίζει τις ενημερώσεις λογισμικού του. Αντίστοιχα και με τις smart TV της Samsung, η τηλεόραση χρησιμοποιεί μια σύνδεση στο Διαδίκτυο για να μεταδώσει πληροφορίες στο χρήστη και να του επιτρέπει παράλληλα την αμφίδρομη φωνητική αναγνώριση. Στις περιπτώσεις αυτές το μοντέλο επικοινωνίας cloud - to - device παρέχει νέες προοπτικές στο χρήστη, επεκτείνοντας τις δυνατότητες της συσκευής πέρα από τα βασικά χαρακτηριστικά της.

Είναι αρκετές οι προκλήσεις διαλειτουργικότητας που μπορούν να προκύψουν όταν προσπαθεί κανείς να ενσωματώσει συσκευές από διάφορους κατασκευαστές. Συχνά, οι υπηρεσίες της συσκευής και του cloud προέρχονται από τον ίδιο προμηθευτή. Αν τα πρωτόκολλα δεδομένων ιδιοκτησία που χρησιμοποιούνται μεταξύ της συσκευής και του cloud, η συσκευή ή ο χρήστης μπορεί να συνδέεται με μια συγκεκριμένη υπηρεσία cloud, περιορίζοντας ή εμποδίζοντας τη χρησιμοποίηση εναλλακτικών Παρόχων.

Γ. Device to Gateway Communications

Στο μοντέλο επικοινωνίας device – to – gateway η έξυπνη συσκευή συνδέεται μέσω μιας υπηρεσίας ALG (Automatic Laser Gateway) για να επιτευχθεί ένα πραγματοποιηθεί νέφος. Αυτό σημαίνει ότι είναι διαθέσιμη μια εφαρμογή λογισμικού που λειτουργεί σε μια τοπική πύλη (gateway), η οποία χρησιμοποιείται ως ενδιάμεσος μεταξύ της συσκευής και του υπολογιστικού νέφους και παρέχει ασφάλεια και άλλες λειτουργίες όπως δεδομένα ή πρωτόκολλο μετάφρασης.

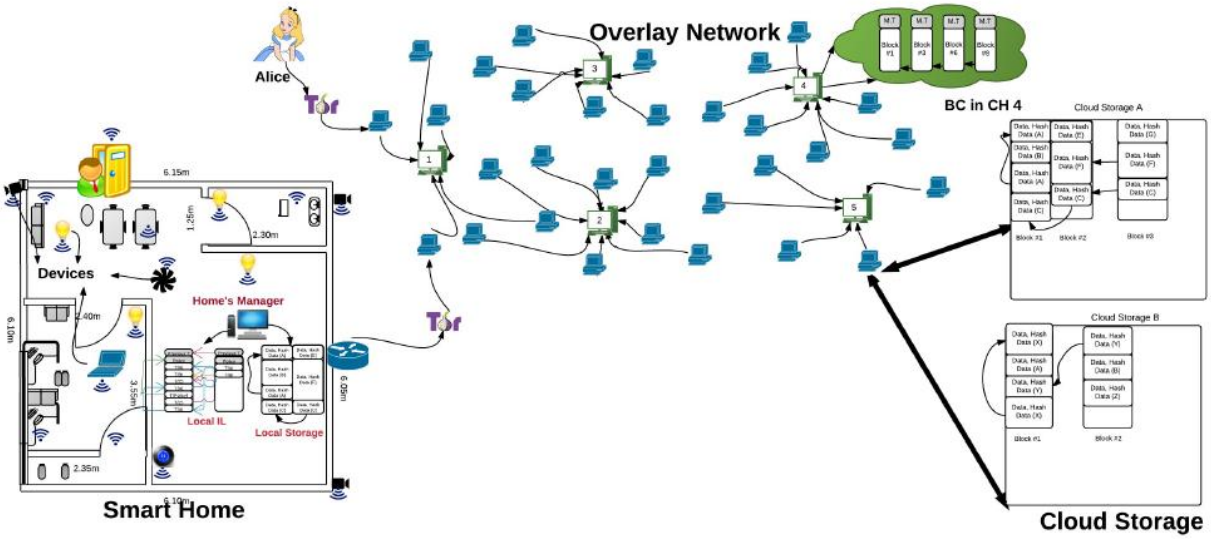
Πολλές μορφές του μοντέλου αυτού βρίσκονται στις καταναλωτικές συσκευές. Σε πολλές περιπτώσεις το local gateway είναι ένα smartphone, το οποίο χρησιμοποιεί μια εφαρμογή για να επικοινωνεί με τη συσκευή και να αναμεταδίδει στοιχεία από ένα cloud. Συχνά το μοντέλο αυτό χρησιμοποιείται από γνωστά προσωπικά αντικείμενα, όπως είναι οι personal fitness trackers. Οι συσκευές αυτές δεν έχουν τη βασική δυνατότητα να συνδέονται απευθείας σε ένα cloud, με αποτέλεσμα συχνά να βασίζονται σε μια εφαρμογή smartphone που θα πρέπει να χρησιμοποιηθεί ως ενδιάμεση πύλη, προκειμένου να συνδεθεί η συσκευή στο cloud.

Δ. Back – End – Data Sharing

Το συγκεκριμένο μοντέλο αναφέρεται στην αρχιτεκτονική που επιτρέπει στους χρήστες να εξάγουν και να αναλύσουν τα δεδομένα των έξυπνων αντικειμένων από ένα υπολογιστικό νέφος σε συνδυασμό με τα δεδομένα από άλλες πηγές. Η αρχιτεκτονική αυτή υποστηρίζει την επιθυμία του χρήστη για αποστολή δεδομένων προς τρίτους. Η προσέγγιση αυτή αποτελεί προέκταση του μοντέλου επικοινωνίας device – to – cloud, το οποίο μπορεί να οδηγήσει σε δεδομένα όπου οι έξυπνες συσκευές στέλνουν δεδομένα μόνο για μια ενιαία εφαρμογή υπηρεσιών. Το συγκεκριμένο μοντέλο επιτρέπει στα δεδομένα που συλλέγονται από την έξυπνη συσκευή να συγκεντρώνονται και να αναλύονται.

3.4 Αρχιτεκτονική έξυπνου σπιτιού βασισμένη στην τεχνολογία bitcoin

Η προτεινόμενη αρχιτεκτονική, που παρουσιάζεται στην Εικόνα 2, περιλαμβάνει τρία επίπεδα (βαθμίδες), δηλαδή το *έξυπνο σπίτι (smart home)*, την *επικάλυψη* (overlay) και την *αποθήκευση στο υπολογιστικό νέφος (cloud storage)* (Michael, 2015). Σε κάθε επίπεδο, οι οντότητες χρησιμοποιούν συναλλαγές (transactions) για να επικοινωνούν μεταξύ τους. Στη συνέχεια παρουσιάζουμε συνοπτικά τις τρεις προαναφερόμενες βαθμίδες.



Εικόνα 5: Αρχιτεκτονική έξυπνου σπιτιού (Dorri, 2017)

Το έξυπνο σπίτι αποτελείται από συσκευές IoT, τοπικό IL και ένα τοπικό αποθηκευτικό χώρο, όπως φαίνεται στο κάτω αριστερό μέρος της συγκεκριμένης εικόνας. Κάθε σπίτι έχει ένα ιδιωτικό υπολογιστικό βιβλίο ή ημερολόγιο (IL – Immutable Ledger) που είναι παρόμοιο με ένα BC (Blockchain), αλλά υφίσταται κεντρική διαχείριση από έναν *Έξυπνο Διαχειριστή Σπιτιού (SHM - Smart Home Manager)*, που επεξεργάζεται όλες τις εισερχόμενες και εξερχόμενες συναλλαγές και χρησιμοποιεί ένα κοινόχρηστο κλειδί για τοπικές επικοινωνίες με συσκευές IoT και τοπική αποθήκευση. Το τοπικό ιδιωτικό υπολογιστικό βιβλίο ή ημερολόγιο (IL) διατηρεί μια πολιτική που καθορίζεται από τον ιδιοκτήτη του σπιτιού για να εξουσιοδοτήσει τις ληφθείσες συναλλαγές. Οι τοπικές συσκευές μέσα στον κόμβο προέλευσης ή επικάλυψης ενδέχεται να δημιουργούν συναλλαγές για να μοιράζονται, να ζητούν ή να αποθηκεύουν δεδομένα.

Η επικάλυψη (overlay) είναι ένα δίκτυο peer-to-peer (P2P)[13] που φέρνει το κατανεμημένο χαρακτηριστικό στην αρχιτεκτονική μας. Οι συστατικοί κόμβοι, γνωστοί ως **κόμβοι επικάλυψης**, θα μπορούσαν να είναι *Έξυπνοι Διαχειριστές* Σπιτιού (SHMs), ή άλλες οικιακές συσκευές παροχής υψηλών πόρων ή ακόμη το smartphone/προσωπικός υπολογιστής του χρήστη. Για τη μείωση της επιβάρυνσης του δικτύου και της καθυστέρησης, οι κόμβοι μέσα στην επικάλυψη ομαδοποιούνται σε

[13] Ένα δίκτυο υπολογιστών peer-to-peer είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται ισοδύναμα τους πόρους τους. Το δίκτυο αυτό χρησιμοποιεί την επεξεργαστική ισχύ, τον αποθηκευτικό χώρο και το εύρος ζώνης (bandwidth) των κόμβων. Όλοι οι κόμβοι του δικτύου έχουν ίσα δικαιώματα.

ομάδες ή συμπλέγματα και κάθε σύμπλεγμα (cluster) επιλέγει μια κεφαλή συμπλέγματος (CH - Cluster Head). Κάθε κεφαλή συμπλέγματος (CH) έχει ένα μοναδικό δημόσιο κλειδί (PK – Public key), γνωστό από άλλα CHs στην επικάλυψη, που χρησιμοποιείται για τη δημιουργία νέων μπλοκ έτσι ώστε τα άλλα CHs να μπορούν να εξουσιοδοτούν τη γεννήτρια μπλοκ. Κάθε κόμβος είναι ελεύθερος να αλλάξει το σύμπλεγμα του, αν έχει υπερβολικές καθυστερήσεις. Επιπλέον, οι κόμβοι στο σύμπλεγμα μπορούν να επιλέξουν ένα νέο CH ανά πάσα στιγμή. Στην παρούσα εργασία, θεωρείται ότι τα προαναφερθέντα βήματα εκτελούνται κατά την εκκίνηση. **Κάθε κεφαλή συμπλέγματος (CH) διατηρεί τις ακόλουθες τρεις λίστες:**

- *Δημόσια κλειδιά αιτούντων (PK requesters):* λίστα των δημόσιων κλειδιών που επιτρέπεται να έχουν πρόσβαση στα δεδομένα για τους *Έξυπνους Διαχειριστές* Σπιτιού *(SHM)* που είναι συνδεδεμένοι σε αυτό το σύμπλεγμα. Ένα παράδειγμα μπορεί να είναι ένας Πάροχος Υπηρεσιών (SP – Service Provider) που παρέχει ορισμένες υπηρεσίες για τις έξυπνες οικιακές συσκευές.

- *Δημόσια κλειδιά αιτούμενων, δηλαδή αυτών που απαντούν (PK requestees):* λίστα των δημόσιων κλειδιών των *Έξυπνων Διαχειριστών Σπιτιού (SHMs)* που είναι συνδεδεμένοι σε αυτό το σύμπλεγμα και στους οποίους επιτρέπεται η πρόσβαση.

- *Λίστα προώθησης:* λίστα συναλλαγών που αποστέλλονται για άλλες κεφαλές συμπλέγματος (CHs) στο δίκτυο.

Οι κεφαλές συμπλέγματος (CH) της επικάλυψης (overlay) διατηρούν ένα δημόσιο Blockchain , το οποίο έχει ένα ημερολόγιο (IL) για κάθε κόμβο επικάλυψης, που εμφανίζει το ιστορικό των συναλλαγών που αποστέλλονται από τον χρήστη της επικάλυψης και χρησιμοποιείται για να κερδίσει φήμη. Οι συναλλαγές δημιουργούνται από χρήστες ή συσκευές, που θέλουν να ζητήσουν ή να μοιραστούν δεδομένα με άλλους. Η επικάλυψη (overlay) περιέχει συναλλαγές πολλαπλών υπογραφών (multisig ή multi-signature), που σημαίνει ότι πρέπει να υπογράφονται από δύο οντότητες - αιτούντες και αιτούμενους- προκειμένου να αντιμετωπίζονται ως έγκυρη συναλλαγή. Επιπλέον, κάθε συναλλαγή έχει δύο εξόδους, που υποδεικνύει τον συνολικό αριθμό των αποδεκτών ή των απορριφθέντων συναλλαγών από τους αιτούντες που δημιουργούνται από την τρέχουσα συναλλαγή.

Κατανεμημένη εμπιστοσύνη και ελαχιστοποίηση της απόδειξης εργασίας (POW): Χρησιμοποιούμε κατανεμημένη εμπιστοσύνη για να εξασφαλίσουμε ότι τα

ληφθέντα μπλοκ είναι έγκυρα και για να μειώσουμε τα γενικά έξοδα για την επαλήθευση των μπλοκ σε σχέση με το Bitcoin αυτό λειτουργεί ως εξής: ένας χρήστης που αρχικά δεν έχει ιστορικό συναλλαγών είναι ύποπτος ότι μπορεί να είναι κακόβουλος και για το λόγο αυτό, επαληθεύονται όλες οι συναλλαγές του.

Για να επαληθεύσουμε μια συναλλαγή, το πρώτο βήμα είναι να επιβεβαιώσουμε ότι ο αιτών έχει το δικαίωμα να προσαρμόζει συναλλαγές στον καθορισμένο κατάλογο, οι οποίες γίνονται με τη σύγκριση της συνάρτησης κατακερματισμού (hash)[14] του δημόσιου κλειδιού (Public Key - PK) της τρέχουσας συναλλαγής με το εξαγόμενο δημόσιο κλειδί (PK) της προηγούμενης συναλλαγής Μετά από αυτό, επαληθεύεται η υπογραφή του αιτούντα, χρησιμοποιώντας το δημόσιο κλειδί του στη συναλλαγή. Στη συνέχεια, ο επαληθευτής ελέγχει ότι μόνο μία από τις εξόδους της τρέχουσας συναλλαγής, δηλαδή ο αριθμός των επιτυχημένων ή των απορριφθέντων συναλλαγών αυξάνεται κατά ένα. Εάν τα βήματα περάσουν με επιτυχία επαληθεύεται η συναλλαγή.

Στο δίκτυο επικάλυψης, κάθε κεφαλή συμπλέγματος (CH) διατηρεί μια αξιολόγηση εμπιστοσύνης για άλλες κεφαλές συμπλέγματος, με βάση άμεσες και έμμεσες αποδείξεις. Η κεφαλή συμπλέγματος A έχει άμεση απόδειξη για τη B, εάν επαληθεύσει ένα μπλοκ που παράγεται από το B. Εάν η A λαμβάνει ένα μπλοκ που παράγεται από τη B και η A δεν έχει εμπιστοσύνη στη B, αλλά όμως μία ή περισσότερες κεφαλές συμπλέγματος υπογράφουν το μπλοκ ως έγκυρο, τότε η A έχει μια έμμεση απόδειξη για τη B. Όταν μία κεφαλή συμπλέγματος δημιουργεί ένα νέο μπλοκ, πρέπει να δημιουργήσει μια συναλλαγή πολλαπλών υπογραφών (multisig transaction), που χρησιμοποιείται για την αξιολόγηση της εμπιστοσύνης. Τότε η κεφαλή συμπλέγματος στέλνει το μπλοκ και τη συναλλαγή σε γειτονικές της, οι οποίες ελέγχουν τη συναλλαγή για άμεσες ή έμμεσες αποδείξεις. Εάν η γειτονική κεφαλή συμπλέγματος έχει άμεση απόδειξη με τη γεννήτρια μπλοκ ή άλλες κεφαλές συμπλέγματος που έχουν υπογράψει τη συναλλαγή, τότε επαληθεύει τυχαία ένα μέρος των συναλλαγών στο μπλοκ, ελέγχοντας τις υπογραφές τους. Το τμήμα των συναλλαγών που πρέπει να επαληθευτούν, αλλάζει ως συνάρτηση του αριθμού των

[14] Μαθηματική συνάρτηση που δέχεται ως είσοδο κάποιο δεδομένο τυχαίου μεγέθους και επιστρέφει ένα ακέραιο σταθερού μεγέθους αναπαράστασης. Το μέγεθος αυτό μπορεί να είναι από 32bit μέχρι 256bit ή περισσότερα, ανάλογα με το λόγο χρήσης της συνάρτησης. Οι τιμές που επιστρέφει η συνάρτηση αυτή ονομάζονται τιμές κατακερματισμού (hash values) και θα πρέπει να είναι διαφορετικές για διαφορετική είσοδο, καθώς η κύρια χρησιμότητα αυτών των συναρτήσεων είναι να ταυτοποιούν τα δεδομένα.

επιτυχώς επαληθευμένων ομάδων για την αντίστοιχη κεφαλή συμπλέγματος. Ο Πίνακας 1 που ακολουθεί, παρουσιάζει ένα παράδειγμα ενός πίνακα εμπιστοσύνης.

Πίνακας 1 Πίνακας εμπιστοσύνης άμεσης απόδειξης

Αριθμός επιτυχημένων μπλοκ	10	20	30	40	50
Ποσοστό των συναλλαγών που πρέπει να επιβεβαιωθούν	80%	60%	40%	30%	20%

Θα πρέπει να σημειώσουμε ότι ένα ορισμένο μέρος των συναλλαγών πρέπει να επαληθευτούν ακόμα και όταν μία κεφαλή συμπλέγματος θεωρείται αξιόπιστη, για την προστασία του δικτύου από εκείνες τις κεφαλές συμπλέγματος που ενδέχεται να έχουν τεθεί πρόσφατα σε κίνδυνο. Εάν μία κεφαλή συμπλέγματος δεν έχει άμεσες αποδείξεις με τη γεννήτρια των μπλοκ ή με αυτές που την υπέγραψαν, τότε ελέγχει όλες τις συναλλαγές στο ληφθέν μπλοκ.

Εάν ένα μόνο μπλοκ παράγεται από περισσότερες της μίας κεφαλές συμπλέγματος, τότε άλλες κεφαλές συμπλέγματος θα δεχθούν εκείνο το μπλοκ που προσαρτάται από την κεφαλή συμπλέγματος που έχει την μεγαλύτερη εμπιστοσύνη, προκειμένου να μειωθεί ο φόρτος επεξεργασίας επικύρωσης, λόγω της κατανεμημένης εμπιστοσύνης. Αυτό μπορεί να έχει σαν αποτέλεσμα ένα διασπασμένο Blockchain. Ωστόσο, όλα τα διασπασμένα μπλοκ θεωρούνται έγκυρα. Οι κεφαλές συμπλέγματος προσθέτουν τα πρόσφατα ληφθέντα μπλοκ στη μακρύτερη αλυσίδα μπλοκ που εξασφαλίζει την συνεκτικότητα του Blockchain.

3.5 Αποθήκευση στο υπολογιστικό νέφος

Η αποθήκευση στο υπολογιστικό νέφος ομαδοποιεί τα δεδομένα του χρήστη σε πανομοιότυπα μπλοκ που σχετίζονται με ένα μοναδικό αριθμό μπλοκ (htt2). Ο αριθμός μπλοκ χρησιμοποιείται από το SHM για έλεγχο ταυτότητας μαζί με τα αποθηκευμένα δεδομένα. Εάν η αποθήκευση μπορεί να εντοπίσει με επιτυχία τα δεδομένα με τον ληφθέντα αριθμό μπλοκ και τη συνάρτηση κατακερματισμού από το SHM, τότε επαληθεύεται ο χρήστης. Τα ληφθέντα δεδομένα από τους χρήστες αποθηκεύονται σε

μια διάταξη FIFO σε μπλοκ μαζί με την συνάρτηση κατακερματισμού των ληφθέντων δεδομένων, όπως φαίνεται στην κάτω δεξιά γωνία της Εικόνας 2. Αξίζει να σημειωθεί ότι κάθε ιδιοκτήτης σπιτιού μπορεί είτε να δημιουργήσει διαφορετικούς καταλόγους αποθηκευμένων δεδομένων για κάθε συσκευή του είτε ένα κοινό μητρώο για όλες τις συσκευές του. Το πρώτο είναι ιδιαίτερα χρήσιμο αν ο ιδιοκτήτης επιθυμεί να παρέχει πρόσβαση σε όλα τα δεδομένα μιας συγκεκριμένης συσκευής σε ένα Πάροχο Υπηρεσιών (SP).

3.6 Διαχείριση συναλλαγών έξυπνου σπιτιού

Στο παρόν κεφάλαιο εστιάζουμε στο πως γίνονται οι συναλλαγές μέσα στο προαναφερόμενο πλαίσιο.

3.6.1 Αποθήκευση συναλλαγών έξυπνου σπιτιού

Ας υποθέσουμε ότι η Alice έχει δημιουργήσει ένα λογαριασμό σε μια εγκατάσταση αποθήκευσης Cloud και έχει ρυθμίσει δικαιώματα για το θερμοστάτη του σπιτιού της, προκειμένου να γίνεται μεταφόρτωση δεδομένων σε αυτή την εγκατάσταση (Jurdak, 2017). Κατά την διάρκεια της διαδικασίας εκκίνησης, η αποθήκευση στο υπολογιστικό νέφος επιστρέφει ένα δείκτη στο πρώτο μπλοκ δεδομένων. Όταν ο έξυπνος θερμοστάτης χρειάζεται να αποθηκεύσει δεδομένα στη συσκευή υπολογιστικού νέφους, τα στέλνει στον Έξυπνο Διαχειριστή Σπιτιού (SHM - Smart Home Manager). Μετά τον έλεγχο των αδειών και την εξαγωγή του προηγούμενου αριθμού μπλοκ και της συνάρτησης κατακερματισμού (hash) από το τοπικό ιδιωτικό υπολογιστικό βιβλίο ή ημερολόγιο (IL – Immutable Ledger), ο Έξυπνος Διαχειριστής Σπιτιού δημιουργεί ένα τυχαίο αναγνωριστικό (ID) και στέλνει δεδομένα στο χώρο αποθήκευσης με αυτό το αναγνωριστικό. Υποτίθεται ότι σε κάθε δεδομένη στιγμή, δύο κόμβοι μπορούν να έχουν το ίδιο αναγνωριστικό.

Η αποθήκευση ελέγχει την εγκυρότητα της συναλλαγής εντοπίζοντας δεδομένα χρησιμοποιώντας συγκεκριμένες παραμέτρους και επιβεβαιώνει επίσης ότι υπάρχει διαθέσιμος χώρος στην αποθήκη του υπολογιστικού νέφους. Αν υπάρχει, υπολογίζει μια συνάρτηση κατακερματισμού (hash function) των ληφθέντων πακέτων δεδομένων και τη συγκρίνει με τη ληφθείσα hash της συναλλαγής. Αν οι δύο συναρτήσεις κατακερματισμού συμφωνούν, τότε τα πακέτα δεδομένων αποθηκεύονται στο χώρο

αποθήκευσης και ο νέος αριθμός μπλοκ κρυπτογραφείται με το δημόσιο κλειδί του Έξυπνου Διαχειριστή Σπιτιού (SHM PK – Smart Home Manager Public key), για να εξασφαλιστεί με τον τρόπο αυτό ότι μόνο ο πραγματικός έξυπνος διαχειριστής σπιτιού μπορεί να διαβάσει το νέο αριθμό μπλοκ. Στη συνέχεια, η συνάρτηση κατακερματισμού δεδομένων που διαθέτει ψηφιακή υπογραφή, υπογράφεται από το χώρο αποθήκευσης και αποστέλλεται στο δίκτυο επικάλυψης που θα αποθηκευτεί στο επικαλυπτόμενο BC (Blockchain). Αυτό εξασφαλίζει ότι οποιεσδήποτε περαιτέρω αλλαγές στα δεδομένα του χρήστη είναι ορατές σε όλους.

Σε κάθε έξυπνο σπίτι υπάρχει ιδιωτική ασφαλής αποθήκευση που διαχειρίζεται ο Έξυπνος Διαχειριστής Σπιτιού, ο οποίος διανέμει το κοινόχρηστο κλειδί μεταξύ των εξουσιοδοτημένων συσκευών IoT και του τοπικού χώρου αποθήκευσης. Οι συσκευές IoT χρησιμοποιούν αυτό το κλειδί για τη δημιουργία μιας συναλλαγής. Η τοπική αποθήκευση υφίσταται διαχείριση από τον ιδιοκτήτη του σπιτιού και είναι αξιόπιστη. Επομένως δεν υπάρχει πρόσθετη οικονομική επιβάρυνση.

3.6.2 Προσπέλαση συναλλαγών έξυπνου σπιτιού

Για να αποκτηθεί πρόσβαση στα αποθηκευμένα δεδομένα μιας συσκευής, ο Πάροχος Υπηρεσιών (SP) δημιουργεί και υπογράφει το τμήμα αιτήματος μιας συναλλαγής πολλαπλών εντολών (Bhga, 2016). Στη συνέχεια ο Πάροχος Υπηρεσιών (SP) στέλνει τη συναλλαγή στη δική του κεφαλή συμπλέγματος (CH). Ο τελευταίος ελέγχει και τους δύο καταλόγους PK, δηλαδή τα δημόσια κλειδιά αιτούντων (PK requesters) και τα δημόσια κλειδιά αυτών που απαντούν (PK requestees). Εάν, είτε ο αιτών της συναλλαγής multisig είναι στη λίστα κλειδιών του αιτητή CH, είτε το αιτούμενο της συναλλαγής βρίσκεται στη λίστα κλειδιών της αιτούσας, τότε μεταδίδει τη συναλλαγή στο δικό του σύμπλεγμα. Διαφορετικά, η συναλλαγή μεταδίδεται σε άλλες κεφαλές συμπλέγματος.

Όταν ο αιτών (SHM) λαμβάνει τη συναλλαγή πολλαπλών υπογραφών (multisig ή multi-signature), εξουσιοδοτεί τον Πάροχο Υπηρεσιών (SP), ελέγχοντας την τοπική πολιτική στην τοπική IL. Αν ναι, το SHM ζητά δεδομένα από την αποθήκευση, τα κρυπτογραφεί με το PK του αιτούντος και τα στέλνει στον αιτούντα (το SP). Μετά την αποστολή δεδομένων για τον αιτούντα, το SHM πρέπει να αποθηκεύσει τη συναλλαγή multisig στο τοπικό ιδιωτικό υπολογιστικό βιβλίο ή ημερολόγιο (IL – Immutable Ledg-

er) για να διατηρήσει το ιστορικό των συναλλαγών. Επιπλέον, ο Διαχειριστής Έξυπνου Σπιτιού (SHM) στέλνει τη συναλλαγή πολλαπλών υπογραφών στην κεφαλή συμπλέγματος του (CH) για αποθήκευση στην επικάλυψη Blockchain ως ένα ιστορικό αιτούντων συναλλαγών.

3.6.3 Παρακολούθηση συναλλαγών έξυπνου σπιτιού

Μία συναλλαγή παρακολούθησης ξεκινά από κόμβους επικάλυψης για την παρακολούθηση δεδομένων σε πραγματικό χρόνο μιας συσκευής. Η παρακολούθηση της επεξεργασίας συναλλαγών είναι παρόμοια με την συναλλαγή πρόσβασης. Η μόνη διαφορά είναι ότι ο Έξυπνος Διαχειριστής Σπιτιού στέλνει δεδομένα σε πραγματικό χρόνο για την ζητούμενη συσκευή. Μια συναλλαγή παρακολούθησης μπορεί επίσης να χρησιμοποιηθεί για την ρύθμιση συνεχούς ροής δεδομένων σε πραγματικό χρόνο από μία συγκεκριμένη συσκευή.

3.7 Εκτίμηση (αξιολόγηση συναλλαγών Έξυπνου Σπιτιού)

Στο παρόν κεφάλαιο συζητάμε αρχικά τις διαφορές μεταξύ των προτεινόμενων τοπικού ιδιωτικού *υπολογιστικού βιβλίου ή ημερολογίου (IL)*, επικάλυψης Blockchain και Bitcoin Blockchain. Στη συνέχεια, παρουσιάζουμε μία ποιοτική συζήτηση σχετικά με τον τρόπο τον οποίο η προτεινόμενη λύση αντιμετωπίζει κοινές επιθέσεις ασφάλειας και ιδιωτικής ζωής. Θα πρέπει να αναφέρουμε ότι το προτεινόμενο πλαίσιο αυτού του κεφαλαίου, βελτιστοποιεί το Bitcoin Blockchain για το Διαδίκτυο των Πραγμάτων (IoT), παρουσιάζοντας διαφορετικές βαθμίδες Blockchain. Κάθε βαθμίδα έχει διαφορετικά χαρακτηριστικά που την διαφοροποιούν με άλλα επίπεδα και Bitcoin Blockchain. Συνοψίζουμε τις βασικές διαφορές μεταξύ Blockchain και Bitcoin Blockchain στον Πίνακα 1 που ακολουθεί.

Πίνακας 2: Διαφορές μεταξύ Blockchain και Bitcoin Blockchain (Dorri, 2017)

#	Χαρακτηριστικό	Blockchain (BC) στο Bitcoin	Ιδιωτικό υπολογιστικό βιβλίο ή ημερολόγιο (IL)	Επικαλυπτόμενο Blockchain (BC)
1	Ορατότητα BC	Δημόσιο	Δημόσιο/Ιδιωτικό	Δημόσιο

2	Αλυσίδωση συναλλαγής	Είσοδος/Εξοδος	Προηγούμενη συναλλαγή της ίδιας συναλλαγής	Οι συναλλαγές δένονται με αλυσίδα η μία με την άλλη
3	Εξόρυξη συναλλαγής	Όλες οι συναλλαγές	Όλες οι συναλλαγές	Αυθαίρετες συναλλαγές
4	Απαίτηση εξόρυξης	απόδειξη εργασίας POW	Καμία	Καμία
5	Διάσπαση	Δεν επιτρέπεται	Επιτρέπεται	Επιτρέπεται
6	Δαπάνη	Απαγορευμένο	Μη εφαρμόσιμη	Μη εφαρμόσιμη
7	Επιβεβαίωση συναλλαγής	Υπογραφή	Καμία επιβεβαίωση	υπογραφές
8	Παράμετροι συναλλαγής	Είσοδος/Εξοδος, νομίσματα	Αριθμός μπλοκ, κρυπτογράφηση δεδομένων, χρόνου, εξόδου δημόσιου κλειδιού	Έξοδος, δημόσια κλειδιά
9	Διάδοση συναλλαγής	Μετάδοση	Μονόδρομη μετάδοση	Μονόδρομη/Πολύδρομη μετάδοση
10	Υποχώρηση στην κεφαλή του μπλοκ	Πάζλ	Πολιτικές	Μη εφαρμόσιμη
11	Επιβεβαίωση νέου μπλοκ	Μπλοκ και συναλλαγές μέσα στο BC	Καμία επιβεβαίωση	Μπλοκ και συναλλαγές μέσα στο BC
12	Έλεγχος BC	Κανένας	Ιδιοκτήτης	Καμία
13	Έλεγχος εξορυκτή	Κανένας	Κανένας	Άλλες κεφαλές συμπλέγματος και κόμβοι

14	Εμπιστοσύνη εξορυκτή	Οι εξορύκτες είναι όλοι ίδιοι	Οι διαχειριστές Έξυπνου Σπιτιού είναι όλοι ίδιοι	Ορίζονται διαφορετικά επίπεδα εμπιστοσύνης
15	Συνένωση φορτίου εξορυκτή	Κατέβασμα όλων μπλοκ στο Blockchain	Κατέβασμα όλων των μπλοκ σε λογιστικό βιβλίο	Κατέβασμα όλων μπλοκ στο Blockchain
16	Επιλογή εξορυκτή	Αυτό-επιλογή	Ο ιδιοκτήτης επιλέγει τον έξυπνο διαχειριστή σπιτιού	Οι κόμβοι μέσα στο σύμπλεγμα επιλέγουν ένα κόμβο ως κεφαλή συμπλέγματος
17	Ανταμοιβές εξορυκτή	Νομίσματα	Κανένα	Δεν ορίζεται
18	Ομάδα εξόρυξης	Επιτρέπεται	Δεν μπορεί να οριστεί	Δεν επιτρέπεται να οριστεί
19	Κακόβουλος εξορυκτής	Επιτρέπεται να συνδεθεί	Όχι δυνατό	Επιτρέπεται να συνδεθεί
20	Συνέπειες από 51% επίθεση	Διπλή δαπάνη	Όχι δυνατό	Αυξάνεται η πιθανότητα της επισήμανσης λανθασμένων μπλοκ
21	Μέθοδος κωδικοποίησης	Δημόσια/ιδιωτικά κλειδιά	Καμία ανάγκη	Δημόσια/Ιδιωτικά κλειδιά, διαμοιραζόμενο κλειδί

Θεωρείται ότι ο αντίπαλος μπορεί να είναι το CH, μια συσκευή στο σπίτι, ένας κόμβος στην επικάλυψη ή η αποθήκευση στο Cloud.

3.7.1 Ασφάλειας και ανάλυση ιδιωτικής ζωής

Θεωρείται ότι ο αντίπαλος μπορεί να είναι το CH, δηλαδή μια συσκευή στο σπίτι, ένας κόμβος στην επικάλυψη ή μία αποθήκευση στο Cloud. Οι αντίπαλοι είναι σε θέση να εμποδίσουν τις επικοινωνίες, να απορρίψουν τις συναλλαγές, να δημιουργήσουν ψευδείς συναλλαγές και να μπλοκάρουν, να αλλάξουν ή να διαγράψουν δεδομένα στο χώρο αποθήκευσης, να συνδέσουν τις συναλλαγές ενός χρήστη μεταξύ τους και να υπογράψουν

ψεύτικες συναλλαγές για να νομιμοποιήσουν τους κόμβους συμπαιγνίας. Ωστόσο δεν είναι σε θέση να σπάσουν την κρυπτογράφηση. Οι κύριες κατηγορίες απειλών είναι οι εξής:

- *Απειλές προσβασιμότητας (Accessibility threats)* που εμποδίζουν τον νόμιμο χρήστη να αποκτήσει πρόσβαση στα δεδομένα ή τις υπηρεσίες.

- *Απειλές ανωνυμίας (Anonymity threats) που εντοπίζουν την πραγματική ταυτότητα ενός χρήστη με την ανάλυση των ανώνυμων συναλλαγών και άλλων διαθέσιμων στο κοινό πληροφοριών.*

- *Απειλές ελέγχου ταυτότητας και ελέγχου πρόσβασης (Authentication and control threats),* στις οποίες ο αντίπαλος προσπαθεί να πιστοποιήσει τον εαυτό του ως νόμιμο χρήστη προκειμένου να αποκτήσει πρόσβαση στα δεδομένα.

Θεωρούμε ότι οι ακόλουθες επιθέσεις απειλούν την προσβασιμότητα:

- *Άρνηση εξυπηρέτησης (Denial Of Service - DOS):* σε αυτή την επίθεση ο εισβολέας στέλνει ένα μεγάλο αριθμό συναλλαγών σε ένα στόχο για να σπάσει την διαθεσιμότητα του. Η χρήση του συνόλου των αιτούντων και των αιτούμενων λιστών δημόσιου κλειδιού(PK) στα CHs μειώνει την επίδραση αυτής της επίθεσης καθώς ένα πακέτο δεν μεταδίδεται σε ένα Διαχειριστής Έξυπνου Σπιτιού (SHM) εκτός και αν το κλειδί του βρίσκεται σε αυτούς στους δύο βασικούς καταλόγους. Επιπλέον, εάν ένα CH λαμβάνει αρχικά ανεπιτυχή αιτήματα πρόσβασης από ένα συγκεκριμένο PK, μπορεί να αποκλείσει αυτό το PK, αφαιρώντας το αντίστοιχο κλειδί από τις λίστες κλειδιών CH. Ωστόσο, ο αντίπαλος μπορεί να πετύχει σε μια επίθεση εντός, αν χρησιμοποιεί διαφορετικά PK για την επίθεση

- *Αλλαγή επίθεσης (Modification attack):* σε αυτή την επίθεση ο αντίπαλος, ο αντίπαλος μπορεί να επιδιώξει να αλλάξει ή να διαγράψει αποθηκευμένα δεδομένα για ένα συγκεκριμένο χρήστη. Για να ξεκινήσει αυτή η επίθεση, ο αντίπαλος θα πρέπει να θέσει σε κίνδυνο την ασφάλεια αποθήκευσης του Cloud. Ωστόσο, ο χρήστης στόχος θα είναι σε θέση να ανιχνεύσει οποιαδήποτε αλλαγή στα αποθηκευμένα δεδομένα του, συγκρίνοντας τον κατακερματισμό των δεδομένων του στο νέφος με τα δεδομένα που είναι αποθηκευμένα στο τοπικό ιδιωτικό υπολογιστικό βιβλίο ή ημερολόγιο (IL – Immutable Ledger).

- *Επίθεση παύσης λειτουργίας (Dropping attack):* για να ξεκινήσει αυτή η επίθεση ο αντίπαλος πρέπει να έχει τον έλεγχο ενός CH και στη συνέχεια να παύσει τη λειτουργία όλων των ληφθέντων συναλλαγών και των μπλοκ. Μία τέτοια επίθεση θα ανιχνευόταν, δεδομένου ότι οι κόμβοι που ανήκουν στις συστατικές ομάδες δεν θα λάβουν καμία συναλλαγή ή υπηρεσία από την επικάλυψη. Σε αυτή την περίπτωση θα επιλέξουμε ένα νέο CH.

- *Επίθεση καθυστέρησης (Appending attack):* για να ξεκινήσει αυτή η επίθεση, ο αντίπαλος πρέπει να ελέγχει πολλαπλές CH που συνεργάζονται. Για να αυξηθεί η έμμεση βαθμολογία των αποδεικτικών στοιχείων, τα κακόβουλα CH υπογράφουν τη συναλλαγή πολλαπλών υπογραφών (multisig), μαζί με το μπλοκ που υποστηρίζει ότι έχει επαληθεύσει ένα άλλο μπλοκ.

Αυτό το ψεύτικο μπλοκ (fake block) μπορεί να είναι ένα μπλοκ με μία ή περισσότερες ψευδές συναλλαγές. Στην προτεινόμενη μέθοδο εμπιστοσύνης ένα τυχαίο τμήμα των συναλλαγών σε ένα ληφθέν μπλοκ είναι πάντα επικυρωμένο μεταξύ του CH και της γεννήτριας μπλοκ. Επομένως, ακόμα και αν το 51% των CHs στην επικάλυψη υπογράψει το ισχίων μπλοκ ως έγκυρο εξακολουθεί να υπάρχει η δυνατότητα ότι η ειλικρινής CH ανιχνεύει το ψεύτικο μπλοκ (αυτή η επίθεση ονομάζεται *51% επίθεση στο BitCoin*). Το πλαίσιο μας επιδεικνύει χαλαρή υποβάθμιση με την έννοια ότι υποβαθμίζεται η ανθεκτικότητα καθώς αυξάνεται ο αριθμός των κόμβων που έχουν συμβιβαστεί.

Η πιθανότητα ανίχνευσης του ψεύτικου μπλοκ είναι συνάρτηση του συνολικού αριθμού των CHs, η οποία παρουσιάζει ένα ενδιαφέροντα συνδυασμό για τον σχεδιαστή του συστήματος. Για να σπάσει η ανωνυμία του χρήστη, ένας εισβολέας μπορεί να προσπαθήσει να καταργήσει την ανωνυμία ενός χρήστη, συνδέοντας δεδομένα που σχετίζονται με την ίδια ανώνυμη ταυτότητα. Για να προστατεύονται από τέτοιες επιθέσεις σύνδεσης, οι κόμβοι επικάλυψής μπορούν να χρησιμοποιούν διαφορετικά PK για την επικοινωνία τους με κόμβους επικάλυψης ή αποθήκευση στο Cloud, έτσι ώστε κάθε μια συναλλαγή να έχει ένα μοναδικό αναγνωριστικό (ID), με αποτέλεσμα να μην καθίσταται δυνατή η σύνδεση των συναλλαγών.

Η επόμενη κατηγορία απειλών είναι κατά του *ελέγχου ταυτότητας ή αυθεντικοποίησης (authentication control)* και του *ελέγχου πρόσβασης (access control)*. Έχει αποδειχθεί σε πρόσφατη έρευνα

ότι είναι δυνατό για έναν εισβολέα να πάρει τον έλεγχο μιας έξυπνης οικιακής συσκευής ή να εισάγει μια ψεύτικη συσκευή σε ένα οικιακό δίκτυο. Ο σχεδιασμός μας χρησιμοποιεί **ιεραρχική άμυνα** κατά των επιθέσεων αυτών. Πιο συγκεκριμένα υπάρχει ένα κεντρικό SHM που ελέγχει όλα τα εισερχόμενα και εξερχόμενα πακέτα και εμποδίζει την άμεση πρόσβαση έξυπνων οικιακών συσκευών από το διαδίκτυο. Αν το SHM εντοπίσει ένα πακέτο που δεν συμμορφώνεται με τις πρακτικές που ορίζεται από τον κάτοχο, το πακέτο απομακρύνεται. Μια δεύτερη γραμμή άμυνας είναι ότι όλες οι συσκευές στο σπίτι πρέπει να έχουν μία συναλλαγή γένεσης στην IL, τους επιτρέπει να ξεκινήσουν την επικοινωνία με το SHM και άλλες συσκευές. Μία συσκευή χωρίς αντίστοιχη συναλλαγή γένεσης απομονώνεται από το δίκτυο. Αυτό εμποδίζει τον εισβολέα προκειμένου να εισάγει μη εξουσιοδοτημένες συσκευές στο δίκτυο.

3.8 Αξιολόγηση απόδοσης

Στο παρόν υποκεφάλαιο αξιολογούμε πρώτα ποσοτικά τα διάφορα γενικά έξοδα και στη συνέχεια συζητάμε τα αποτελέσματα της προσομοίωσης. Ο Πίνακας 3 που ακολουθεί, απεικονίζει μέσες μετρήσεις απόδοσης για τις βασικές συναλλαγές στην προτεινόμενη αρχιτεκτονική μας. Οι απαιτήσεις εκφράζονται ως μία συνάρτηση διαφορετικών παραμέτρων σχεδιασμού όπως πακέτων μνήμης και υπολογιστικής επιβάρυνσής και καθυστέρησης. Για να αξιολογήσουμε την απόδοση του προτεινόμενου πλαισίου, πραγματοποιούμε προσομοιώσεις με χρήση ενός προσομοιωτή NS3[15], εστιάζοντας στον δείκτη επικάλυψης.

Πίνακας 3: Υπολογισμός επιβάρυνσης (Dorri, 2017)

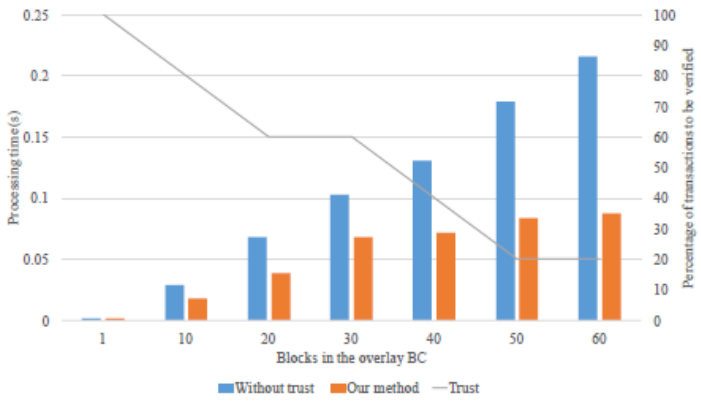
	Appending & Trust	Transactions	CH joining
Packet overhead	O(N)	O ((N*S)/2)	O (BS)
Delay	O (N/TL)	O ((N*S)/2)	O (B*T)
Computation overhead	O (N/TL)	O (N)	O (B*T)
Memory overhead	O (BS)	O(1)	O(BS)

[15] Προσομοιωτής δικτύων διακριτών γεγονότων για συστήματα Διαδικτύου που στοχεύουν κυρίως στην έρευνα και την εκπαιδευτική χρήση. Το NS3 είναι ελεύθερο λογισμικό, με άδεια χρήσης της άδειας GNU GPLv2 και διατίθεται στο κοινό για έρευνα, ανάπτυξη και χρήση.

Θα πρέπει να σημειώσουμε ότι η έξυπνη απόδοση στο σπίτι, αξιολογήθηκε από προηγούμενες εργασίες. Προσομοιώνουμε ένα δίκτυο 50 κόμβων, εκ των οποίων οι 13 είναι CH, για να μελετήσουμε την κίνηση και την επεξεργασία των γενικών εξόδων του σχεδιασμού μας. Εκτελούμε την προσομοίωση για 60 δευτερόλεπτα, κατά την διάρκεια των οποίων δημιουργούνται συνολικά 960 αλλαγές. Τα αποτελέσματα που δίνονται είναι ο μέσος όρος 10 κύκλων της προσομοίωσης.

- *Επιβάρυνση φορτίου (traffic overhead):* Αυτό αναφέρεται στο ποσό των bytes που μεταδίδονται στο overlay για τη διαχείριση του δημόσιου BlockChain. Για να συγκρίνουμε τα αποτελέσματα μας, ένα δίκτυο Bitcoin με 50 κόμβους προσομοιώνεται ως γραμμή βάσης. Τα αποτελέσματα προσομοίωσης δείχνουν ότι η μέθοδος μας δημιούργησε περίπου 37 MB, ενώ τα Bitcoin παρήγαγαν 138 MB. Ο κύριος λόγος για αυτή τη διαφορά οφείλεται στην ομαδοποίηση και στο γεγονός ότι τα πακέτα BlockChain μεταδίδονται μόνο μεταξύ των CHs, ενώ τα πακέτα Bitcoin μεταδίδονται μεταξύ όλων των κόμβων.

- *Επεξεργασία φορτίου (processing overhead):* Αυτή η μετρική αναφέρεται στον χρόνο που καταναλώνεται από τα CHs για την επιβεβαίωση νέων μπλοκ. Ως μετροπρόγραμμα (benchmark) θεωρούμε ένα δίκτυο επικάλυψης με 50 κόμβους, το οποίο δεν υλοποιεί κατανεμημένη εμπιστοσύνη. Τα αποτελέσματα της προσομοίωσης για την αξιολόγηση της επεξεργασίας φορτίου, παρουσιάζονται στην Εικόνα 6, που ακολουθεί



Εικόνα 6: Υπολογισμός επεξεργασίας φορτίου (Dorri, 2017)

4.1 Λειτουργία έξυπνου σπιτιού

Όταν ο ηλεκτρικός εξοπλισμός είναι συνδεδεμένος στην πρίζα, αλλά δεν είναι σε χρήση, αλλά όμως υπάρχει ροή ηλεκτρισμού. Αυτό σημαίνει ότι σπαταλάμε ηλεκτρική ενέργεια από πέντε έως δέκα τοις εκατό, με αποτέλεσμα να χρεωνόμαστε ρεύμα χωρίς λόγο (Jurdak, 2017). Επίσης, όταν έχουμε ηλεκτρικό εξοπλισμό συνδεδεμένο στην πρίζα μπορεί να προκληθούν και πολλά ατυχήματα όπως για παράδειγμα το ηλεκτρικό βραχυκύκλωμά. Κατά συνέπεια, πρέπει να μην ξεχνάμε να αποσυνδέουμε την ηλεκτρική συσκευή από την πρίζα. Προκειμένου να βρεθεί μια λύση για αυτά τα προβλήματα, δημιουργήθηκε το smart home. Με την πρόοδο της τεχνολογίας, πολλά ερευνητικά έργα σχετικά με το smart home έχουν αναπτυχθεί προκειμένου να διευκολύνουν την ανθρώπινη ζωή και να βελτιώσουν την ποιότητα της. Ένα έξυπνο σπίτι (smart home), απαρτίζεται από την τεχνολογία που χρησιμοποιείται για να κάνει όλες τις ηλεκτρονικές συσκευές του σπιτιού έξυπνες (intelligenat).Η τεχνολογία αυτή είναι αυτοματοποιημένη και αποτελείται από διάφορες έξυπνες συσκευές όπως προηγμένα αυτόματα συστήματα για το φωτισμό, τη θερμοκρασία ελέγχου, ασφάλειας και πολλές άλλες λειτουργίες.

Μια έξυπνη συσκευή είναι πολύ εύκολο να εγκατασταθεί και να χρησιμοποιηθεί από όλους έχοντας σκοπό να βελτιώσει πολλές πτυχές της καθημερινότητας μας. Τα 40 κυρίως μέρη που απαρτίζεται το έξυπνο σπίτι (Smart home) είναι τρία (3), το δίκτυο, οι συσκευές ελέγχου και οι συσκευές αυτοματισμού της οικίας. Το δίκτυο που χρησιμοποιείται για τη σύνδεση του αυτοματισμού με τις συσκευές ελέγχου μπορεί να είναι ενσύρματο αλλά και ασύρματο. Οι συσκευές ελέγχου χρησιμοποιούνται για την διαχείριση των συστημάτων, και η συσκευή αυτοματισμού είναι συσκευή που ελέγχει το φυσικό περιβάλλον. Ωστόσο, θα αναλύσουμε αυτά τα τρία μέρη λεπτομερώς στην ενότητα που ακολουθεί.

Τι είναι το Smart Home. Με τον όρο Smart Home θεωρούμε οποιοδήποτε προσωπικό ή εργασιακό περιβάλλον που συμπεριλαμβάνει ένα σύνολο τεχνολογικών εφαρμογών με βασικό χαρακτηριστικό την αυτοματοποίηση και τον έλεγχο των επιμέρους τμημάτων του. Το επίπεδο αυτοματοποίησης, καθώς επίσης και ο τρόπος ελέγχου διαφέρουν, αφού εξαρτώνται από αρκετές παραμέτρους. Ορισμένες από αυτές τις παραμέτρους είναι το κόστος, οι προσωπικές επιθυμίες των χρηστών, το είδος των αντικειμένων που πρόκειται να ελεγχθούν και ο τύπος του οικοδομήματος στο οποίο η τεχνολογία θα εγκατασταθεί. Το Smart Home μας δίνει τη δυνατότητα να ζούμε και να

εργαζόμαστε σε απλοποιημένα και αναβαθμισμένα περιβάλλοντα, εξασφαλίζοντας μας παράλληλα τη μείωση των πάγιων εξόδων. Μελλοντικά, το κόστος των ηλεκτρικών και ηλεκτρονικών συσκευών και συστημάτων μειώνεται, έτσι ώστε οι αυτοματισμοί του σπιτιού ή και του Smart Home να μπορούν να αξιοποιηθούν. Γενικότερα η εύκολη εγκατάσταση, το χαμηλό κόστος συντήρησης, η αθόρυβη λειτουργία, η εξοικονόμηση ενέργειας, η άνεση και ο προσωπικός έλεγχος επί του οικιακού περιβάλλοντος από απόσταση αποτελούν μερικά από τα βασικά πλεονεκτήματα της αυτοματοποίησης. Η τεχνολογία του Smart Home, συμβάλλει στην απλοποίηση της καθημερινότητας των χρηστών, πρέπει να πληροί συγκεκριμένες προϋποθέσεις, όπως:

• Τη διασφάλιση της ανθρώπινης ζωής και περιουσίας,

• Τη γνώση για τη διαχείριση της τεχνολογίας και

• Την επικοινωνία με το εξωτερικό περιβάλλον

Ένα από τα βασικά χαρακτηριστικά της τεχνολογίας των Smart Home είναι ότι οι περιφερειακές μονάδες χρησιμοποιούνται για πολλαπλές χρήσεις. Παραδείγματος χάριν, οι αισθητήρες παρουσίας μπορούν να χρησιμοποιηθούν για τον έλεγχο του φωτισμού και του συστήματος θέρμανσης, ενώ ταυτόχρονα χρησιμεύουν και για το σύστημα του συναγερμού. Ακόμα ένα παράδειγμα αφορά την οθόνη της τηλεόρασης, η οποία μπορεί να προβάλλει και την εικόνα της θυροτηλεόρασης. Τα σύγχρονα συστήματα που εφαρμόζονται στα Smart Home δίνουν την δυνατότητα στους ενοίκους για πάρα πολλές διευκολύνσεις και συμβάλλουν στην εξοικονόμηση πολύτιμου χρόνου. Οι παρεχόμενες διευκολύνσεις αυξάνονται καθώς, εκτός από τις βασικές λειτουργίες, δίνεται επίσης και η δυνατότητα στους ιδιοκτήτες των Smart Home να προγραμματίσουν το σύστημα και να δημιουργήσουν τα δικά τους σενάρια, προκειμένου να καλύψουν πλήρως τις δικές τους εξατομικευμένες ανάγκες. Τα σενάρια που μπορούν να εφαρμοστούν είναι άπειρα. Μερικά παραδείγματα, όσον αφορά στις συνήθεις λειτουργίες των Smart Home, παρουσιάζονται παρακάτω.

1. Φωτισμός: Αυτοματοποιημένος φωτισμός που μειώνεται ή αυξάνεται κατά τη διάρκεια της ημέρας, προκατασκευασμένα σενάρια φωτισμού, αυτόματη απενεργοποίηση και ενεργοποίηση των φώτων.

2. Ασφάλεια: Προστασία από πυρκαγιά, πλημμύρες, βραχυκυκλώματα,, ή οποιαδήποτε βλάβη. Σε αυτήν την περίπτωση, το Smart Home σημαίνει συναγερμό.

3. Έλεγχος θέρμανσης, κλιματισμού, αερισμού: Δυνατότητα ρύθμισης εκ των προτέρων ή απομακρυσμένα της επιθυμητής θερμοκρασίας για το σπίτι. Οι ίδιες

ρυθμίσεις μπορούν να γίνουν και για τον κλιματισμό - αερισμό, ενώ ακόμα υπάρχει η δυνατότητα αυτόματης ενεργοποίησης του εξαερισμού σε περίπτωση υψηλής συγκέντρωσης αερίων ή καπνού στο χώρο. Επίσης, η θέρμανση μπορεί να απενεργοποιείτε αν υπάρχει ανοιχτό παράθυρο ή όταν θεωρείται περιττή.

4. Έλεγχος ηλεκτρικών περσίδων και τεντών: Θα μπορούσαμε να εντάξουμε στην παραπάνω ενότητα, ωστόσο αποτελεί αυτοτελές τμήμα των συστημάτων ελέγχου ενός Smart Home. Οι περσίδες, τα παράθυρα και οι τέντες μπορούν να ανοίγουν και να κλείνουν ανάλογα με το φως, τον αέρα ακόμη και τη θερμοκρασία ρυθμίζοντας απόλυτα τις συνθήκες διαβίωσης.

5. Πολυμέσα: Δυνατότητα διασύνδεσης ηχοσυστημάτων, τηλεοράσεων, τηλεφώνων είτε μεταξύ τους, είτε με άλλες «έξυπνες» συσκευές στο σπίτι. Συμπερασματικά, στο αυτοματοποιημένο περιβάλλον ενός Smart Home όλα τα συστήματα μπορούν να λειτουργήσουν αρμονικά μεταξύ τους, ρυθμίζοντας αυτόματα τις επιθυμητές συνθήκες διαβίωσης. Το κυριότερο είναι ότι μπορούμε να ελέγξουμε εξ ολοκλήρου την κατανάλωση της ενέργειας, εξοικονομώντας το μέγιστο δυνατόν, εφόσον η λειτουργία των συσκευών, του κλιματισμού, του φωτισμού και της θέρμανσης αποκλειστικά καθορίζεται από το χρόνο που μας είναι αναγκαία Το δίκτυο του Smart Home Η τεχνολογία δικτύου του Smart home μπορεί να ταξινομηθεί σε δύο κύρια είδη, τα οποία είναι το ηλεκτρικό σύστημα και το ασύρματο σύστημα. Στο ηλεκτρικό σύστημα, ο εξοπλισμός θα πρέπει να συνδεθεί στην κύρια τροφοδοσία άμεσα, έτσι ώστε τα δεδομένα που αποστέλλονται στις συσκευές να ενεργοποιούνται ή να απενεργοποιούνται. Υπάρχουν πολλοί τύποι καλωδίων που μπορούμε να εγκαταστήσουμε σε έναν τοίχο. Πολλοί αυτοματισμοί του Smart Home συνδέονται μέσω καλωδίωσης όπως πχ οι οπτικές ίνες. Ένα παράδειγμα εξαιρετικής τεχνολογίας είναι το X10, το οποίο είναι ένα ανοικτό πρότυπο αυτοματισμού οικίας. Το X10 μεταδίδει δυαδικά δεδομένα χρησιμοποιώντας τη διαμόρφωση πλάτους (AM).Οι X10 ελεγκτές στέλνουν σήματα μέσω των υφιστάμενων AC καλωδιώσεων στο δέκτη. Πολλές όμως νέες συσκευές χρησιμοποιούν ασύρματη τεχνολογία και όχι το ηλεκτρικό σύστημα για να επικοινωνήσουν με άλλες συσκευές. Παραδείγματα ασύρματων τεχνολογιών είναι οι υπέρυθρες (IR), οι ραδιοσυχνότητες (RF), το WiFi, το Bluetooth και ούτω καθεξής. Επίσης ορισμένες τεχνολογίες δικτύου Smart home μπορούν να λειτουργήσουν και με τους δύο τρόπους και με ηλεκτρικό άλλα και ασύρματο σύστημα. Ένα παράδειγμα ασύρματης επικοινωνίας για το Smart home είναι το Z-κύμα, το οποίο είναι μια αξιόπιστη και προσιτή ασύρματη λύση οικιακού αυτοματισμού. Το Z-κύμα είναι μία ασύρματη RF based μμέθοδος για άμεσο τηλεχειρισμό των συσκευών. Το

έξυπνο σπίτι (Smart home) ελέγχει τις συσκευές που χρησιμοποιούνται για τη διαχείριση των συστημάτων του με την αποστολή δεδομένων ή την αποστολή σήματος στους ελεγκτές. Τα παραδείγματα των ελεγκτών δεν είναι μόνο το τηλεχειριστήριο, αλλά επίσης και κάποια έξυπνα αντικείμενα όπως πχ τα tablet (iPad, Galaxy tab), web browsers και Short Message Service (SMS). Επιπλέον, ορισμένα συστήματα μπορεί να έχουν ενσωματωμένο υπολογιστή που λειτουργεί ως κέντρο αντίληψης για το περιβάλλον ή τη μμονάδα αξιολόγησης Συσκευές αυτοματισμού του Smart Home

Μερικά παραδείγματα Smart συσκευών αναφέρονται στον παρακάτω πίνακα:

Οικιακές Συσκευές Πόσο έξυπνες; Ψυγείο Ρυθμίζει την θερμοκρασία ψύξης με βάση τον όγκο των προϊόντων που περιέχει Θερμοστάτης Αλλαγές θερμοκρασίας με βάση τις τρέχουσες και προσεχείς καιρικές συνθήκες

Πίνακας 4 Επίπεδα ευφυίας έξυπνου σπιτιού

Οικιακές Συσκευές	**Πόσο έξυπνες;**
Ψυγείο	Ρυθμίζει την θερμοκρασία ψύξης με βάση τον όγκο των προϊόντων που παρέχει
Θερμοστάτης	Αλλαγές θερμοκρασίας με βάση τις τρέχουσες και προσεχείς καιρικές συνθήκες
Τηλεόραση	Προτείνει τηλεοπτικά βασισμένες επιλογές του χρήστη .Ακόμα με το πρόγραμμα περιήγησης στο Διαδίκτυο θα μπορείς να ελέγχεις άλλες συνδεδεμένες συσκευές, όπως ο θερμοστάτης
Πλυντήριο πιάτων	Προσδιορίζει τη θερμοκρασία του νερού καθώς και την πλύση – ξέπλυμα βασισμένο στον όγκο φορτίου, την βρωμιά και την ώρα της ημέρας ενέργειας (Νυχτερινό ρεύμα, ώρες ξεκούρασης
Εξοπλισμός πισίνας	Καθορίζει τα επίπεδα μόλυνσης και καταργεί τη σωστή ποσότητα χημικών ουσιών προσαρμόζει τη λειτουργία της αντλίας κυκλοφορίας και χλώριο ζωοτροφών με την ώρα της ημέρας και τις καιρικές συνθήκες

i) Κουζίνα: Η κουζίνα είναι ο χώρος ο οποίος έχει λάβει τις μεγαλύτερες αναβαθμίσεις για ένα έξυπνο σπίτι (Smart Home). Για παράδειγμα, μερικές συσκευές που έχουν αναβαθμιστεί σε έξυπνες είναι τα ψυγεία, οι φούρνοι μικροκυμάτων, οι καφετιέρες και τα πλυντήρια πιάτων. Το Smart ψυγείο εφαρμόζει την τεχνολογία του έξυπνου σπιτιού (Smart home) και κάνει την καθημερινότητά μας πολύ πιο εύκολη. Συγκεκριμένα, συνδέεται στο Διαδίκτυο και επιτρέπει στους χρήστες να επικοινωνούν μαζί του, έτσι ώστε να είναι δυνατή η λήψη συνταγών και στη συνέχεια να τις εμφανίζει στην οθόνη LCD που διαθέτει. Επιπλέον, το Smart ψυγείο κάνει επίσης μια αυτόματη απογραφή των ειδών στο εσωτερικό του και μπορεί να προειδοποιήσει τους χρήστες για το τι υπάρχει διαθέσιμο. Ακόμη υπάρχουν και 45 φούρνοι μικροκυμάτων που είναι επίσης Smart. Οι Smart φούρνοι μικροκυμάτων μπορούν να επικοινωνήσουν με το Smart ψυγείο και να του προτείνουν συνταγές που βασίζονται στην είδη διατροφής που διατίθενται ήδη μέσα σε αυτό. Επίσης έχουν την δυνατότητα να ενεργοποιηθούν αυτόματα αν το επιλέξει ο χρήστης ενώ βρίσκεται μακριά από το σπίτι.

ii) Σαλόνι: Φεύγοντας από την κουζίνα κατευθυνόμαστε σε ένα άλλο μέρος του έξυπνου σπιτιού (Smart Home) το οποίο έχει λάβει αναβαθμίσεις, το σαλόνι. Έξυπνες συσκευές όπως τηλεοράσεις και ηχοσυστήματα χρησιμοποιούν αυτή την τεχνολογία για να βελτιώσουν την εμπειρία της ψυχαγωγίας. Το Smart TV, έχει πολλές λειτουργίες όπως του προσωπικού επιτραπέζιου υπολογιστή (Personal Computer) με αποτέλεσμα αυτό να οδηγεί στο να έχουμε μια διαδραστικά τηλεόραση με διαδραστικό περιεχόμενο που πλέον υπάρχει ως επιλογή. Επιπλέον, το σύστημα ελέγχου φωτισμού μπορεί να χρησιμοποιηθεί για τον έλεγχο στα οικιακά ηλεκτρικά φώτα, χρησιμοποιώντας τους ανιχνευτές κίνησης. Τα φώτα μπορούν να σβήσουν αυτόματα στο δωμάτιο όταν κάποιος φύγει από αυτό και να ενεργοποιηθούν αντίστοιχα όταν κάποιος εισέλθει σε αυτό.

iii) Υπνοδωμάτιο: Το δωμάτιο διαθέτει Smart θερμοστάτη που οι χρήστες μπορούν να ρυθμίσουν την θερμοκρασία με ένα μόλις άγγιγμά. Επίσης μπορούν να επιλέξουν μια μόνιμή νυχτερινή θερμοκρασία και μόνιμο φωτισμό για κάθε υπνοδωμάτιο. Το κρεβάτι είναι επίσης εξοπλισμένο με αισθητήρες που μπορούν να παρακολουθούν την κίνηση του ατόκου στο κρεβάτι και να ανιχνεύουν την κατάσταση της υγείας το σχετικά με τον ύπνο. Ακόμη, οι Smart συσκευές μπορούν να χρησιμοποιηθούν και σε πολλές πτυχές, όπως για παράδειγμα:

• Υγεία: Μια ιατρική συσκευή σχεδιασμένη με ενσωματωμένο λογισμικό που βοηθά τους παρόχους υγείας να παρακολουθούν συνεχώς ασθενείς με εμφυτευμένο τζιπάκι ή άλλες ιατρικές συσκευές στο σπίτι τους χωρίς νοσηλεία στο νοσοκομείο ή ιατρικές επισκέψεις σε ιδιωτικά γραφεία.. Αυτά τα σπίτια με 46 ηλεκτρονικές συσκευές υγείας μπορούν να συλλέγουν αξιόλογα στοιχεία σχετικά με την τρέχουσα κατάσταση της υγείας για την πρόληψη των ασθενειών και τη συνολική ευεξία αυτών. Οι συσκευές αυτές μπορούν ακόμη και να χρηματοδοτηθούν εν μέρει ή πλήρως από τις ασφαλιστικές εταιρείες και την κυβέρνηση.

• Ψυχαγωγία: Ο πλούτος του Internet είναι τώρα διαθέσιμος μέσω της τηλεόρασης, με τον οποίο αλλάζει ριζικά ο ορισμός του "περιεχομένου". Σήμερα οι εταιρείες μπορούν να δημιουργήσουν ανοικτές πλατφόρμες για νέες τηλεοράσεις που διαθέτουν ένα portal το οποίο περιέχει ψυχαγωγικό περιεχόμενο από πολυάριθμους τηλεοπτικούς σταθμούς • Περιβάλλον: Απομακρυσμένος έλεγχος για τον φωτισμό την θέρμανση και τον κλιματισμό. Επίσης την κατανάλωση ενέργειας και του κόστους

4.2 Ασφάλεια με τη βοήθεια του Blockchain στο έξυπνο σπίτι

Αναμφισβήτητα η νέα μεγάλη τάση στο τομέα της τεχνολογίας για την οποία όλοι συζητάνε παγκοσμίως είναι το Internet of Things (IoT) (Alphand, 2018). Στις παραμέτρους που συνοδεύουν το IoT, σημαντικό ρόλο διαδραματίζει και η ασφάλεια. Η νέα δύναμη της αλλαγής στην παγκόσμια τεχνολογική αγορά είναι το IoT. Πρόκειται, για ένα μεγάλο και πολυποίκιλο πεδίο δραστηριοποίησης, στο οποίο χρησιμοποιούνται συσκευές καθημερινής χρήσης αλλά και επαγγελματικών εφαρμογών, που συλλέγουν πληροφορίες από το περιβάλλον ή άλλες διασυνδεδεμένες συσκευές, μεταδίδοντας δεδομένα σε άλλα συστήματα ή σε συσκευές του χρήστη, προσφέροντας ευκολίες και αυτοματισμούς σε πραγματικό χρόνο. Οι διασυνδεμένες συσκευές στα πλαίσια του IoT μπορούν να καλύπτουν τομείς καθημερινής δραστηριότητας στο σπίτι και το επαγγελματικό περιβάλλον, αλλά και διαδικασιών αγορών, εφαρμογών υγείας και ασφάλειας, επικοινωνίας, μεταφορών και άλλων λειτουργιών.

Από πλευράς κατασκευαστών τεχνολογικών λύσεων η νέα τάση του IoT προσφέρει σίγουρα μια νέα μεγάλη ευκαιρία για να αναπτύξουν πρωτοποριακά προϊόντα που θα υποστηρίζουν τη συγκεκριμένη τάση. Παρόλα αυτά, όπως σε όλες τις νέες τάσεις έτσι και σε αυτή τη περίπτωση, εγείρονται ορισμένοι προβληματισμοί, αφενός για τη διαχείριση των συλλεγόμενων πληροφοριών από τρίτους αλλά και τον τρόπος που αυτές θα χρησιμοποιηθούν σε πραγματικό ή σε μελλοντικό χρόνο.

Αφετέρου και με δεδομένο ότι ο πυρήνας της συγκεκριμένης τάσης είναι η διασύνδεση στο διαδίκτυο, ανακύπτουν οι προβληματισμοί για τις τρωτότητες και τις κακόβουλες ενέργειες που πάντα ελλοχεύουν και απασχολούν τους υπεύθυνους ψηφιακής ασφάλειας. Ας αναλύσουμε λοιπόν τα βασικά σημεία προβληματισμού αλλά και τον τρόπο που θα αμυνθούμε σε ενδεχόμενες απειλές που σχετίζονται με την νέα τάση, λαμβάνοντας υπόψη, ότι το περιβάλλον του IoT είναι δαιδαλώδες και η εικόνα δεν είναι πλήρως ολοκληρωμένη όπως και η διαφορετικότητα των τρωτών σημείων εντείνει σημαντικά το πρόβλημα.

4.2.1 Προκλήσεις ασφαλείας σχετικά με τις συσκευές του IoT

Σύνθετο και μεγαλύτερο τοπίο επιθέσεων. Εκ φύσεως, το IoT δεν αποτελεί μία τεχνολογική υλοποίηση ή ένα τμήμα μιας εταιρικής υποδομής που μπορεί να είναι ελεγχόμενη (Sagirlar, 2018). Για να ψηφιοποιηθούν οι πληροφορίες από τον φυσικό κόσμο και να συνδυαστούν με στόχο την σύνδεση αυτοκινήτων, κτιρίων, βιομηχανιών, κατοικιών, ψυγείων κ.α. με το χρήστη, απαιτείται ο συνδυασμός πάρα πολλών τεχνολογιών, σε κάθε πιθανό σημείο συλλογής πληροφοριών. Αυτό οδηγεί στην ραγδαία αύξηση των τελικών σημείων σύνδεσης στο δίκτυο και άρα στον πολλαπλασιασμό των πιθανών εισόδων κακόβουλων εισβολέων.

Σχεδιασμός των IoT συσκευών. Μέχρι σήμερα, αρκετές IoT συσκευές έχουν σχεδιασθεί, παραχθεί και ήδη χρησιμοποιούνται σε ποικίλες εκφάνσεις της καθημερινότητάς μας. Οι ειδικοί σε θέματα ασφάλειας προσπάθησαν να μεταβάλλουν τη συμπεριφορά τους και να συλλέξουν πληροφορίες που θεωρούνται κατά μία έννοια ευαίσθητες ή απόρρητες, δίχως να είναι εξουσιοδοτημένοι. Δυστυχώς, οι δοκιμές ήταν επιτυχείς. Για παράδειγμα έχει αναφερθεί ότι κάποιοι άλλαξαν την συμπεριφορά ενός οχήματος, υπό κίνηση και παρακολουθήσαν εικόνες από μία οικία, μέσω μίας συσκευής παρακολούθησης ενός μωρού. Οι περιπτώσεις διείσδυσης στη διασύνδεση των συσκευών αυτών είναι αρκετές και εγείρουν ερωτήματα για τον αρχικό σχεδιασμό αυτών των συσκευών. Αποδεικνύεται, ότι πολλές ομάδες δημιουργίας των «έξυπνων» συσκευών δεν συμπεριελάμβαναν στο δυναμικό τους, ειδικούς σε θέματα ασφάλειας και ότι όλος ο σχεδιασμός υλοποιήθηκε με γνώμονα τα λειτουργικά χαρακτηριστικά, το χαμηλό κόστος και την γρήγορη ένταξη στην αγορά. Έτσι, το δίκτυο κατακλύστηκε από συσκευές με καμία ή ελάχιστη προστασία από κακόβουλες επιθέσεις, κάτι που βοήθησε στην ανάπτυξη ενός νέου περιβάλλοντος δραστηριοποίησης των εισβολέων. Το συγκεκριμένο πρόβλημα δεν αναμένεται να λυθεί άμεσα μιας και αυξάνει σημαντικά το κόστος παραγωγής και άρα την τελική τιμή των προϊόντων.

Περιορισμένη πρόσβαση στις IoT συσκευές. Σε κάθε επιχείρηση, οι συσκευές που χρησιμοποιούνται και συνδέονται στο εταιρικό δίκτυο, καλύπτουν μέρα με την μέρα τα κενά ασφάλειας που παρουσιάζουν, μέσω διαφόρων αναβαθμίσεων και patching διαδικασιών, που προσφέρονται από τους κατασκευαστές του υλικού ή του λογισμικού που χρησιμοποιούν. Πολλές από τις υπάρχουσες IoT συσκευές δεν σχεδιάστηκαν με γνώμονα την εταιρική ασφάλεια και δεν αναμενόταν να βρεθούν εντός μιας εταιρικής δομής. Έτσι, δεν διαθέτουν τις απαραίτητες αναβαθμίσεις απέναντι στις διαρκώς μεταβαλλόμενες απειλές, για να θεωρηθούν ασφαλής και αξιόπιστες Επιπρόσθετα, αν το IT τμήμα αποφασίσει να καλύψει μόνο του τα κενά ασφάλειας που εισάγονται από τις έξυπνες συσκευές, δεν είναι σίγουρο ότι θα επιτύχει τον στόχο του. Οι περισσότερες εξ' αυτών δεν διαθέτουν ούτε πληκτρολόγιο, ούτε οθόνη ούτε εν γένει κάποια διακριτή είσοδο δεδομένων, καθιστώντας αδύνατη την επικοινωνία με το λειτουργικό τους πυρήνα. Από την άλλη μεριά αν η πρόσβαση είναι εφικτή, η υπολογιστική ισχύς και οι πόροι που διαθέτει μια έξυπνη συσκευή συνήθως δεν επαρκούν για να εφαρμοστούν διεργασίες ασφάλειας και κρυπτογράφησης. Καθώς δεν υπάρχει προτυποποίηση για την υλοποίηση των έξυπνων συσκευών απαιτείται κάθε συσκευή να αντιμετωπιστεί ξεχωριστά, να εξεταστούν τα χαρακτηριστικά της και να εφαρμοστούν στοχευόμενα βελτιώσεις και περιορισμοί. Αναλογιζόμενοι το πλήθος αυτών των συσκευών σε μία εταιρική δομή, αντιλαμβανόμαστε ότι με αυτόν τον τρόπο αυξάνεται δραματικά ο εργασιακός φόρτος και φυσικά η πιθανότητα σφάλματος.

Απομακρυσμένη πρόσβαση. Κάθε συσκευή που συνδέεται απομακρυσμένα στο δίκτυο με στόχο την παρακολούθηση και τη διαμόρφωσή της, είναι θεωρητικά ευάλωτη σε επιθέσεις. Ακόμα και αν οι συσκευές δεν αποθηκεύουν τοπικά ευαίσθητα δεδομένα, παραμένουν ενεργά σημεία πρόσβασης στο εταιρικό δίκτυο. Το πρόβλημα εντείνεται αν αναλογιστούμε ότι οι συσκευές δεν διαθέτουν anti-malware λογισμικό. Οτιδήποτε χρησιμοποιεί μία IP διεύθυνση είναι στόχος και σίγουρα θα εντοπιστεί. Σε περίπτωση που οι συσκευές επικοινωνούν με cloud δομές το πρόβλημα λαμβάνει σχεδόν ανεξέλεγκτες διαστάσεις. Πέραν της περιορισμένης δυνατότητας να ελεγχθούν τα μονοπάτια των δεδομένων και η ποιότητα των εφαρμογών που τα χρησιμοποιούν, προκύπτουν και προβλήματα φυσικής δομής. Οι cloud servers που υποστηρίζουν έξυπνες συσκευές βρίσκονται συνήθως εκτεθειμένοι με καμία σχεδόν φυσική προστασία απέναντι σε μη εξουσιοδοτημένη πρόσβαση.

Ιδιωτικότητα. Ένα από τα μεγαλύτερα προβλήματα που εγείρεται με τη χρήση των IoT συσκευών είναι το πώς χρησιμοποιούνται τα δεδομένα που συλλέγουν από το περιβάλλον του χρήστη. Γιατί οι πληροφορίες που επεξεργάζεται ένα ψυγείο, ίσως να

μην είναι τόσο σημαντικές, αλλά αν συνδυαστούν με τις υπόλοιπες καταγραφές εντός μιας οικίας, ουσιαστικά μπορούν να αποκαλύψουν «ιστορίες» της καθημερινότητας των ενοίκων. Στη περίπτωση των επιχειρήσεων και των οργανισμών, μπορεί να εκτεθεί η παραγωγική τους διαδικασία και να γίνουν θύματα βιομηχανικής κατασκοπείας. Φυσικά, χωρίς την συλλογή αυτών των δεδομένων η ύπαρξη των έξυπνων συσκευών δεν θα είχε καμία αξία αφού δεν θα παρείχαν καμία διευκόλυνση στον χρήστη. Ο προβληματισμός έγκειται στον τρόπο που χρησιμοποιούνται, από ποιους και με ποιον απώτερο σκοπό. Το θέμα της ιδιωτικότητας είναι εκτενές και προς το παρόν δεν υπάρχει επαρκής νομοθεσία, που υπαγορεύει τον τρόπο που χρησιμοποιούνται οι συλλεγόμενες πληροφορίες και από ποιον. Η μόνη προστασία έγκειται στις πολιτικές ασφάλειας της κάθε εταιρείας που χρησιμοποιεί συλλεγόμενα δεδομένα με στόχο την ανάλυση και την εξαγωγή γενικών συμπερασμάτων. Για να αυξηθεί η εμπιστοσύνη και η προστασία των καταναλωτών, αυτές οι πολιτικές θα πρέπει να είναι απλές, κατανοητές και άμεσα προσβάσιμες στους τελικούς καταναλωτές ή τους εταιρικούς χρήστες.

4.2.1 Οι εκκολαπτόμενες απειλές στο εταιρικό περιβάλλον

Οι IoT συσκευές αντιμετωπίζουν τις ίδιες απειλές, όπως κάθε συσκευή που είναι συνδεδεμένη στο Internet. Βέβαια ως σημείο δράσης των εισβολέων θεωρείται περιορισμένο, αλλά όσο οι συσκευές αυξάνονται τόσο διευρύνεται το πρόβλημα. Τι μπορεί να συμβεί λοιπόν αν μία συσκευή βρεθεί υπό απειλή;

DDoS–DisruptionandDenialofService. Όταν η παραγωγική διαδικασία μιας εταιρείας στηρίζεται σε συσκευές IoT, απαιτείται η αδιάλειπτη λειτουργία τους και η προφύλαξή τους από μη εξουσιοδοτημένη πρόσβαση (Gervais, 2016). Αν παρόλα αυτά επιτευχθεί εισβολή, η πιο συνήθης απειλή είναι η δημιουργία συνθηκών «αδυναμίας εξυπηρέτησης» της επιχείρησης προς τους πελάτες της. Αν στοχεύσουν χιλιάδες IoT συσκευές ώστε να ζητήσουν εξυπηρέτηση από μία εταιρική ιστοσελίδα ή αιτηθούν ώστε να λάβουν συγκεκριμένα δεδομένα, το αποτέλεσμα της αύξησης της κίνησης δεδομένων στις γραμμές εξυπηρέτησης θα γίνει αντιληπτό στους πραγματικούς πελάτες της εταιρείας και θα μειωθεί αισθητά η απόδοση.

Ροή δεδομένων. Όλες οι νέες συσκευές που χρησιμοποιούν Wi-Fi συνδέσεις θα δημιουργήσουν μία περαιτέρω ροή δεδομένων από την ήδη υπάρχουσα, που θα πρέπει να συλλεχθεί, να επεξεργαστεί και να αναλυθεί σύμφωνα με τις εταιρικές ανάγκες. Φυσικά, νέες επιχειρηματικές ευκαιρίες θα ξεπηδήσουν αλλά συμπεριλαμβάνονται και

πολλαπλά ρίσκα. Οι οργανισμοί πρέπει να είναι σε θέση να αναγνωρίζουν τη θεμιτή από την κακόβουλη κίνηση δεδομένων και να επεμβαίνουν έγκαιρα προτού το πρόβλημα εξαπλωθεί. Ουσιαστικά, το μεγαλύτερο πρόβλημα δεν είναι η προστασία των τελικών σημείων – συσκευών, αλλά ο έλεγχος αυτής της ροής δεδομένων και των εντολών που διοχετεύουν. Για παράδειγμα, τι θα γινόταν αν ο φούρνος μικροκυμάτων σας έλεγε στο ψυγείο σας να απενεργοποιηθεί; Ποια είναι η πιθανότητα να αντιλαμβανόσασταν ότι υπάρχει πρόβλημα στον φούρνο και όχι στο ψυγείο; Επιπρόσθετα, παρατηρώντας τη λειτουργία των IoT συσκευών διαπιστώνεται ότι δραστηριοποιούνται εντελώς εκτός των εταιρικών firewall και συνάπτουν μακράς διάρκειας συνδέσεις με υπηρεσίες που παρέχονται από τρίτους. Σε πολλές περιπτώσεις η εταιρεία έχει άγνοια για αυτούς του απομακρυσμένους παρόχους υπηρεσιών και τον τρόπο προστασίας των δεδομένων και εφαρμογών τους. Το κυριότερο είναι ότι αν μία συσκευή βρεθεί σε κίνδυνο το IT τμήμα είναι πολύ πιθανό να μην το γνωρίζει, αφού υπάρχει περιορισμένη «ορατότητα» στις εσωτερικές λειτουργικές διαδικασίες της συσκευής και την σχέση λογισμικού – υλικού.

Κόστος. Κάθε εταιρεία ξοδεύει σημαντικό κεφάλαιο στην απόκτηση πόρων που θα αυξήσουν την παραγωγική της απόδοση και σε συστήματα ασφαλείας που θα καταστίσουν την δομή της άτρωτη από κακόβουλες επιθέσεις. Και ενώ είναι πλήρως κατανοητό ότι ένα laptop θα κοστίζει ένα σεβαστό ποσό και θα διατεθεί για την βελτίωση των καθημερινών διεργασιών, ένας αισθητήρας θερμοκρασίας πόσο αναμένεται να κοστίζει; Πόσα χρήματα είναι διατεθειμένη να ξοδέψει μία εταιρεία για μία έξυπνη καφετιέρα ή ένα σύστημα διαχείρισης του φωτισμού; Ως είθισται υπάρχει αναλογική σχέση μεταξύ του κόστους και της παρεχόμενης ασφάλειας. Πάροχοι που έχουν σχεδιάσει τις IoT συσκευές τους με γνώμονα την ασφάλεια σαφώς κοστολογούν τα προϊόντα τους ακριβότερα από τους υπόλοιπους. Προτού λοιπόν επιλεγεί οτιδήποτε καλείται να εισέλθει στην εταιρική δομή πρέπει να υπάρξει προσεκτική αξιολόγηση των χαρακτηριστικών παραγωγής και λειτουργίας.

Δεν θα χρησιμοποιήσω IoT συσκευές. Θα μπορούσε να είναι μία προσέγγιση από εταιρείες μικρού βεληνεκούς, αλλά είναι αλήθεια επιλογής τους; Πανεπιστήμιο που νοίκιασε ένα κτίριο για να καλύψει τις ανάγκες τους διαπίστωσε ότι ο χώρος περιείχε πολυάριθμες IoT συσκευές, από το σύστημα ψύξης-θέρμανσης έως κάμερες ασφαλείας, που είχαν αφήσει οι προηγούμενοι ενοικιαστές. Και γνωρίζετε αν ο αποθηκάριος έφερε μία έξυπνη καφετιέρα στον χώρο; Και τι γίνεται με τα wearables; Ως wearables εννοούμε μικροσκοπικούς υπολογιστές που ο χρήστης μπορεί να φοράει κατά τις καθημερινές του δραστηριότητες, όπως είναι το iWatch της Apple και τα Google Glass

. Τα περισσότερα εξ' αυτών συνδέονται στο Internet ή σε μία φορητή συσκευή μέσω Bluetooth και διαθέτουν λειτουργίες τοποθεσίας, άρα αμέσως διαπιστώνεται ροή δεδομένων και η συσκευή καθίσταται τελικό σημείο πρόσβασης. Τι θα συμβεί λοιπόν αν μία τέτοια συσκευή βρεθεί μέσα στην εταιρική δομή;

4.2.2. Στρατηγική ασφαλείας για τις IoT συσκευές

Διαφαίνεται ότι απαιτούνται αναρίθμητες διαδικασίες σε ότι αφορά την αντιμετώπιση των ρίσκων που εισάγουν οι έξυπνες συσκευές, τόσο σε εταιρικό όσο και σε οικιακό επίπεδο. Μέχρι τώρα, το IoT αποτελεί μία νέα πύλη πρόσβασης για τους εισβολείς που ολοένα αυξάνει το βεληνεκές της. Αν και η εικόνα δεν είναι ολοκληρωμένη το καθοριστικό σημείο είναι το κόστος (Salah, 2017). Πολλοί πάροχοι IoT συσκευών με στόχο την εξοικονόμηση κόστους, δεν αφήνουν πολλά περιθώρια για δραστικές βελτιώσεις στα θέματα της ασφάλειας. Άρα, το θέμα δεν είναι αν μία έξυπνη συσκευή θα πέσει θύμα εισβολής, αλλά τι γίνεται από εκεί και πέρα και πώς όλο αυτό αντιμετωπίζεται.

Ανίχνευση και παρακολούθηση. Η πρώτη κίνηση για την προστασία της εταιρικής δομής είναι ο εντοπισμός όλων των IoT συσκευών που ενδεχόμενα βρίσκονται στον χώρο. Η διαδικασία εύρεσης τους δεν είναι μία στατική διεργασία, αλλά απαιτεί την δια ζώσης διερεύνηση κάθε χώρου και συστήματος και την καταγραφή όλων των πιθανών σημείων που προκαλούν ροή δεδομένων και συνδέονται στο δίκτυο με οποιονδήποτε τρόπο. Ακολούθως, αυτές οι συσκευές πρέπει να παρακολουθούνται στενά και το IT τμήμα να εξοικειωθεί με τη συμπεριφορά τους. Για το λόγο αυτό προτείνεται η υιοθέτηση MDM (mobile device management) πλατφορμών, με τις οποίες μπορούν να τεθούν τα όρια μέσα στα οποία θα λειτουργούν αυτές οι συσκευές, θα παρακολουθούνται και θα ανιχνεύεται κάθε συμπεριφορά πέραν του φυσιολογικού. Κυρίως, θα περιοριστεί η πιθανότητα επιθέσεων που σχετίζεται με την εισερχόμενη ροή δεδομένων προς τις IoT συσκευές. Επιπρόσθετα, προτείνεται η χρήση MAM (mobile application management) πλατφορμών που εφαρμόζουν τις πολιτικές ασφαλείας της εταιρείας σε επίπεδο εφαρμογών. Πολλές εφαρμογές μπορούν να συμπεριφερθούν ως εισβολείς σε γειτονικές συσκευές. Με τη χρήση των MAM οι λειτουργίες των εφαρμογών μπορούν να περιοριστούν στο σημείο που ο διαχειριστής θεωρεί ασφαλές και επιπρόσθετα μπορεί να κρυπτογραφηθεί η ροή των δεδομένων που προέρχεται από την συσκευή. Ειδικότερα, για τις wearable συσκευές προτείνεται η χρήση WIPS (Wireless Intrusion Prevention Systems) ώστε να ανιχνεύονται και να αναφέρονται στο IT τμήμα ύποπτες συνδέσεις και πιθανές επιθέσεις. Σε συνδυασμό με

διαδικασίες geofencing, οι οποίες θα εμποδίζουν συσκευές που βρίσκονται «κοντά» στην εταιρεία και όχι μέσα σε αυτήν να έχουν πρόσβαση στο δίκτυό της και αυθεντικοποίησης των εξουσιοδοτημένων χρηστών και συσκευών, μπορεί το WYOD (Wear Your Own Device) να υιοθετηθεί με παρόμοιους κανόνες ασφαλείας, όπως και στην περίπτωση του BYOD (Bring Your Own Device). Μέσα από τα προαναφερόμενα εργαλεία θα μπορεί το IT τμήμα να δημιουργήσει μια Whitelist με εφαρμογές που επιτρέπεται να χρησιμοποιούνται από τις εταιρικές συσκευές και φυσικά μία blacklist για εφαρμογές που έχει διαπιστωθεί ότι εισάγουν υψηλό ρίσκο σε θέματα ασφάλειας.

Εκπαίδευση καταναλωτών και εργαζομένων. Όσοι κανόνες ασφάλειας και να εφαρμοστούν, αν οι τελικοί χρήστες δεν γνωρίζουν την ορθή χρήση των IoT συσκευών μοιραία αποδυναμώνεται κάθε προσπάθεια προστασίας. Σε οικιακό ή προσωπικό επίπεδο οι οργανισμοί πρέπει να εκπαιδεύσουν τους πελάτες τους για τις καλύτερες πρακτικές χρήσης των συσκευών τους. Κύρια διεργασία είναι η συχνή αλλαγή των κωδικών πρόσβασης, κυρίως των σημείων σύνδεσης στο Internet, μιας και αποτελεί την πιο συχνή αιτία εισβολών. Ειδικότερα, στις περιπτώσεις που οι συσκευές έρχονται από τον κατασκευαστή με ήδη έτοιμο προφίλ χρήσης (προεπιλεγμένα όνομα χρήστη και κωδικός πρόσβασης) τότε οι πιθανότητες εισβολής αυξάνονται σημαντικά. Επίσης, απαιτείται εκπαίδευση για την εφαρμογή αναβαθμίσεων ασφαλείας στις συσκευές τους. Ποιος καταναλωτής γνωρίζει αν υπάρχουν αναβαθμίσεις ασφαλείας για την συσκευή του ή πώς να τις υλοποιήσει; Η γνωστοποίηση και η εκπαίδευση πρέπει να είναι το κύριο μέλημα των παρόχων. Σε εταιρικό επίπεδο, οι εργαζόμενοι πρέπει να επιμορφωθούν σε θέματα χειρισμού των εταιρικών δεδομένων σχετικά με τις IoT συσκευές. Αφορά κυρίως ποιες εφαρμογές επιτρέπεται να χρησιμοποιήσουν και τι επιτρέπεται να αποθηκεύουν τοπικά στις συσκευές τους. Σημειώνεται, ότι ο υπάλληλος που εργάζεται και στο χώρο του, αν δεν σέβεται τους εταιρικούς περιορισμούς και δεν ακολουθεί τις πρακτικές ασφαλείας που προαναφέρθηκαν, μετατρέπει το οικιακό του δίκτυο σε πιθανό σημείο εισβολής στην εταιρεία.

Δικτυακή «απομόνωση». Τα όρια της εισερχόμενης ροής δεδομένων πρέπει να ασφαλιστούν αυστηρά. Αν οι IoT συσκευές δεν προσπελαύνονται απευθείας από το Internet, καθίσταται δυσκολότερο να υποστούν σε μία DDoS επίθεση. Επίσης, η αποδέσμευση της επικοινωνίας των συσκευών από cloud δομές είναι μία πρακτική που υιοθετείται τελευταίως από τις εταιρίες, ώστε να απομακρυνθεί ένα σημαντικό τμήμα απειλών. Αν πάλι η διαδικτυακή προσπέλασή της είναι καίριας σημασίας για την λειτουργία της συσκευής, τότε προτείνεται να απομονωθεί από το υπόλοιπο εταιρικό δίκτυο. Το «απομονωμένο» τμήμα του δικτύου στο οποίο θα λειτουργούν τέτοιου

είδους συσκευές πρέπει να παρακολουθείται στενά για τυχόν ασυνήθιστη συμπεριφορά και ανεξέλεγκτη ροή δεδομένων και φυσικά να είναι έτοιμες οι ενέργειες αντιμετώπισης των εισβολών παντός είδους. Η δικτυακή απομόνωση προτείνεται και για συσκευές που εισάγονται για πρώτη φορά στο δίκτυο, ώστε να εξεταστεί η συμπεριφορά τους και να τεθούν τα κατάλληλα όρια. Αν δεν λειτουργούν όλες οι IoT συσκευές του εταιρικής δομής σε δικό τους κομμάτι δικτύου , π.χ. VLAN, προτείνεται η άμεση μετακίνησή τους, ειδικά στις περιπτώσεις που διαπιστώνεται ότι η συμπεριφορά τους δεν ταιριάζει με το προφίλ των εταιρικών συσκευών. Σε αυτή την περίπτωση πρέπει να ανακατευθυνθεί η δικτυακή δραστηριότητά τους, να απομονωθούν και να ελεγχθούν για τυχόν αλλαγές στο λογισμικό τους.

Προτυποποίηση. Σημαντική διαδικασία για την προστασία των IoT συσκευών είναι οι αναβαθμίσεις των συσκευών, σύμφωνα με τις επιταγές του κατασκευαστή και την εφαρμογή των διαφόρων patches για να αντιμετωπιστούν τα τρωτά σημεία του λογισμικού τους. Το πρόβλημα είναι ότι λόγω της έλλειψης προτυποποίησης κάθε συσκευή αντιμετωπίζεται ξεχωριστά και απαιτεί χρόνο και επαγρύπνηση για να παραμένει ενημερωμένη και ασφαλής. Στον αντίποδα η έλλειψη προτυποποίησης σημαίνει ότι τα τρωτά σημεία μίας συσκευής, δεν αφορούν μία ευρύτερη γκάμα προϊόντων και κάθε φορά είναι λίγες οι συσκευές που δέχονται επίθεση ταυτόχρονα.

Εν κατακλείδι, προτού ηθελημένα εισαχθούν οι IoT συσκευές στην εταιρική δομή πρέπει να γίνει μία μελέτη των κινδύνων που εισάγονται και τα οφέλη που αναμένονται και να αξιολογηθεί αν αξίζει το ρίσκο. Γνώμονας λήψης της απόφασης θα πρέπει να είναι η μέχρις στιγμής προστασία της εταιρείας από δικτυακές και όχι μόνο απειλές και η ταχύτητα και ευελιξία που έχει επιδείξει κατά καιρούς στις νέες απειλές που ολοένα και εμφανίζονται. Επιπλέον, αν το IT τμήμα δεν απαρτίζεται από διαχειριστές με μεγάλη εμπειρία στον χώρο της ασφάλειας με τους οποίους πρέπει να συνεργαστούν οι μέτοχοι σε όλα τα επίπεδα, προτού υιοθετηθεί το IoT, τότε καλό θα ήταν να διατηρηθούν επιφυλάξεις. Τέλος, τα δεδομένα και τα μονοπάτια που ακολουθούν για να εξυπηρετήσουν το εταιρικό δίκτυο σε όλες του τις μορφές, πρέπει να είναι ήδη προστατευμένα και οι ίδιες τεχνικές ασφάλειας να εφαρμοστούν στα συλλεγόμενα δεδομένα από τις έξυπνες συσκευές. Διαφορετικά, θα προκύψουν με βεβαιότητα θέματα παραβίασης της ιδιωτικότητας και έκθεσης των ευαίσθητων ή απορρήτων δεδομένων, τόσο της εταιρείας όσο και των πελατών της.

4.3 Σενάρια λειτουργίας έξυπνου σπιτιού

Ένα έξυπνο σπίτι συλλέγει δεδομένα από αισθητήρες ενσωματωμένους στο περιβάλλον. Με τις πληροφορίες που λαμβάνει, αναλαμβάνει δράση με βάση τη φύση και το επίπεδο της απειλής που τίθεται. Μέσω τριών βημάτων αίσθηση, αξιολόγηση και πράξη που χρησιμεύουν ως βάση για την κάλυψη της τρέχουσας έρευνας και τεχνολογιών σε ασφαλείς έξυπνες κατοικίες. Πρώτον, περιγράφουμε διάφορα είδη ζητημάτων ασφαλείας που αντιμετωπίζουν τα έξυπνα σπίτια και επεξηγούν τρόπους με τους οποίους μπορεί να βοηθήσει η οικιακή τεχνολογία. Δεύτερον, περιγράφουμε τα υπάρχοντα αυτόνομα συστήματα αισθητήρων που ανιχνεύουν συγκεκριμένους τύπους απειλών και συνοψίζουν τις τρέχουσες προσεγγίσεις που λαμβάνονται για την αντιμετώπιση των απειλών. Τρίτον, εστιάζουμε στην περιοχή που έχει λάβει το μεγαλύτερο μέρος της προσοχής της έρευνας, δηλαδή την αξιολόγηση και την αναγνώριση των απειλών με βάση τα δεδομένα των αισθητήρων. Τέλος, αναλύουμε τις συνεχιζόμενες προκλήσεις για ασφαλή έξυπνα σπίτια και ιδέες για μελλοντικές κατευθύνσεις έρευνας.

Παρέχονται κίνητρα για την έρευνα για ασφαλείς τεχνολογίες έξυπνων κατοικιών μέσω μιας σειράς σεναρίων που απεικονίζουν τους τύπους απειλών που μπορεί να αντιμετωπίσουν τα έξυπνα σπίτια. Κάθε σενάριο αναδεικνύει ένα διαφορετικό είδος πρόκλησης για την ασφάλεια και τον ρόλο που μπορούν να διαδραματίσουν τα έξυπνα σπίτια βοηθώντας στην ανίχνευση, την αξιολόγηση και την αντιμετώπιση της απειλής.

Σενάριο 1: Ανίχνευση εισβολέων. Η Μαρία ζει με την οικογένειά της που είναι όλοι μακριά για την ημέρα. Το πρωί, το σπίτι εντοπίζει την άφιξη ενός ατόμου. Το σπίτι αναγνωρίζει ότι η ώρα της ημέρας και ο τύπος του αυτοκινήτου ταιριάζουν με εκείνους ενός ατόμου που πραγματοποιεί παραδόσεις προϊόντων. Το σπίτι παρέχει πρόσβαση στο γκαράζ για να αποβάλει τα στοιχεία και ειδοποιεί τη Μαρία. Όταν ο σύζυγος της Μαρίας επιστρέφει στο σπίτι το απόγευμα, το σπίτι καταγράφει την παρουσία του και ενημερώνει τη Μαρία. Αργά το βράδυ, το σπίτι αισθάνεται μια ασυνήθιστη είσοδο από το παράθυρο. Η κάμερα είναι ενεργοποιημένη για περαιτέρω αναγνώριση του ατόμου και μετάδοση του βίντεο στη Μαρία και τον σύζυγο της. Επιβεβαιώνουν ότι το άτομο είναι ο γιος τους, ο οποίος δεν διέθετε το κλειδί του και μπήκε στην οικία από ένα παράθυρο.

Σενάριο 2: Ανίχνευση συμβάντων υγείας. Ο Περικλής είναι ένας 81χρονος άντρας, ο οποίος διαγνώστηκε με ασθένεια του Parkinson πριν από πέντε χρόνια. Η κινητικότητά του μειώνεται και όταν βγαίνει από το κρεβάτι ένα βράδυ, σκοντάφτει και

πέφτει. Ο Περικλής δεν μπορεί να σηκωθεί για να ζητήσει βοήθεια, αλλά το σπίτι εντοπίζει τη διακοπή του ύπνου και την επακόλουθη έλλειψη κίνησης. Το σπίτι ζητά από τον Περικλής να επιβεβαιώσει ότι είναι εντάξει και όταν δεν λάβει απάντηση, το σπίτι έρχεται σε επαφή με τις υπηρεσίες έκτακτης ανάγκης.

Σενάριο 3: Ανίχνευση αστοχίας συστήματος κτιρίου. Η ασφάλεια των έξυπνων σπιτιών εκτείνεται πέρα από τα μεμονωμένα σπίτια, στις κοινότητες κατοίκων. Ένα συγκρότημα περιλάμβανε πενήντα διαμερίσματα, καθένα από τα οποία είναι μια έξυπνη κατοικία και τα οποία μοιράζονται μερικές βασικές πληροφορίες μεταξύ τους, όπως η ποιότητα του εσωτερικού αέρα, η θερμοκρασία και η χρήση ηλεκτρικής ενέργειας. Όταν τα διαμερίσματα σημείωσαν ότι τα επίπεδα των πτητικών οργανικών ενώσεων σε πέντε από τις κατοικίες ξαφνικά αυξήθηκαν πέρα από τα ασφαλή επίπεδα, η ένωση ενημέρωσε τους κατοίκους όλων των διαμερισμάτων για να εγκαταλείψουν τα σπίτια τους και να μην επιστρέψουν μέχρι να αντιμετωπιστεί η κατάσταση. Ένα από τα διαμερίσματα σημείωσε ότι ο κάτοικος του είχε κάπνισμα σε ένα διαμέρισμα που αναδιαμορφώθηκε και πρότεινε ότι ο συνδυασμός καπνού και ανοιχτών τοξικών χημικών μπορεί να συνέβαλε στο πρόβλημα. Αυτά τα σενάρια υπογραμμίζουν την ποικιλομορφία των ζητημάτων ασφάλειας που αντιμετωπίζουν οι κάτοικοι και, συνεπώς, και από τα έξυπνα σπίτια.

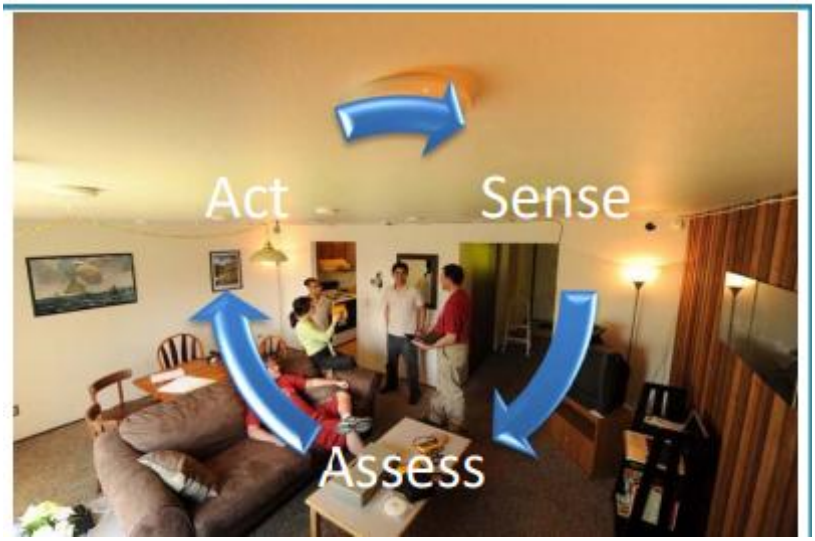
Ένα κοινό θέμα ασφάλειας στο σπίτι είναι η ανίχνευση και πρόληψη των εισβολέων, όπως φαίνεται στο Σενάριο 1. Ωστόσο, τα έξυπνα σπίτια που παρέχουν ασφάλεια πρέπει επίσης να είναι ευαίσθητα σε θέματα υγείας που μπορούν να θέσουν σε κίνδυνο την ευημερία των κατοίκων, όπως περιγράφεται στο Σενάριο 2. Αυτό περιλαμβάνει ανίχνευση πτώσεων, έλλειψη κίνησης και σημαντικές αλλαγές στα πρότυπα συμπεριφοράς. Με τον ίδιο τρόπο που η υγεία ενός έξυπνου κατοίκου κατοικίας μπορεί να παρακολουθείται από ένα ασφαλές έξυπνο οικιακό σύστημα, έτσι ώστε η υγεία του φυσικού περιβάλλοντος στο σπίτι να μπορεί και πρέπει να παρακολουθείται. Για παράδειγμα, όπως περιγράφεται στο Σενάριο 3, το κτίριο μπορεί να υποστεί διαρροές αερίων, σωλήνες κατάψυξης, πυρκαγιές και άλλα θέματα που μπορούν να απειλήσουν την υγεία των κατοίκων καθώς και του κτιρίου. Πολλές από τις αισθητήρες, την αξιολόγηση και τις στρατηγικές δράσης μπορούν να χρησιμοποιηθούν σε όλα αυτά τα σενάρια, όπως θα δούμε σε όλο το χαρτί. Ενώ τα σενάρια απεικονίζουν τις παραδοσιακές απειλές ασφάλειας σε ολόκληρη την εφημερίδα.

Ενώ τα σενάρια καταδεικνύουν τις παραδοσιακές απειλές για την ασφάλεια που μπορεί να αντιμετωπίσει ένα έξυπνο σπίτι, η ίδια η έξυπνη οικιακή τεχνολογία μπορεί να εισάγει νέες απειλές. Αυτό παροτρύνει την ανάγκη για έξυπνα συστήματα οικιακής

χρήσης να είναι ανθεκτικά και ανθεκτικά. Συγκεκριμένα, εάν υπάρχει αισθητήρας ή βλάβη συστήματος, το σπίτι πρέπει να παρέχει προστασία και βοήθεια. Ως εκ τούτου, το ίδιο το έξυπνο σπίτι πρέπει να ανιχνεύσει το σύστημα ανωμαλίες και αποτυχίες στο υλικό, το λογισμικό ή τα στοιχεία επικοινωνίας του.

4.3.1 Έξυπνο σπίτι και ανίχνευση απειλών

Οι τεχνολογίες και οι γενικότερες τεχνολογίες του Ίντερνετ των πραγμάτων εισάγουν επίσης έναν εντελώς νέο τύπο την εισβολή, δηλαδή την πειρατεία στην τεχνολογική υποδομή. Επί του παρόντος, τα έξυπνα σπίτια είναι δικαίως ευάλωτα στην πειρατεία και αυτό μπορεί να οδηγήσει όχι μόνο σε δαπανηρές αστοχίες (π.χ. τρέξτε το πλυντήριο ρούχων πολλές φορές), αλλά και απειλητικές για τη ζωή χρήστη (π.χ., αντί ανοίξει ο φούρνος στους, να ανοίξει κάποιο μάτι που δεν θέλουμε να χρησιμοποιηθεί).



Εικόνα 7: Ένα ασφαλές έξυπνο σπίτι αντιλαμβάνεται τις απειλές, τις αξιολογεί και λαμβάνει μέτρα για να κρατήσει το σπίτι και τους κατοίκους ασφαλείς

Όπως φαίνεται από την Εικόνα 7, το πρώτο βήμα ενός ασφαλούς έξυπνου σπιτιού είναι να αισθανθεί την τρέχουσα κατάσταση του περιβάλλοντος και των κατοίκων. Οι έξυπνοι οικιακοί αισθητήρες είναι πολύ διαφορετικοί και περιλαμβάνουν συχνά ένα υποσύνολο αισθητήρων για κίνηση, θερμοκρασία, φωτισμό, υγρασία, χρήση πόρτας, χρήση συσκευής και κατανάλωση ενέργειας, καθώς και κάμερες και μικρόφωνα. Με την εμφάνιση του IoT, υπάρχει πληθώρα συσκευών που παρέχουν πληροφορίες και χρησιμοποιούν το Διαδίκτυο για να επικοινωνούν μεταξύ τους καθώς και με τον κάτοικο. Σε αυτή την ενότητα, εξετάζουμε μια δειγματοληψία τεχνολογιών που παρέχουν δυνατότητες ανίχνευσης ειδικά για την παροχή ενός ασφαλούς περιβάλλοντος. Οι βιντεοκάμερες είναι ένας παραδοσιακός μηχανισμός για την

παρακολούθηση ενός περιβάλλοντος. Βρίσκονται σε πολλούς δημόσιους χώρους και παρέχουν αρχεία γεγονότων καθώς και απομακρυσμένη ή και αυτοματοποιημένη ανίχνευση απειλών. Πρόσφατα, εταιρείες όπως iControl, Nest, SmartThings, Vivint και Ring έχουν ενισχύσει το παραδοσιακό σύστημα κάμερας για το σκοπό της έξυπνης παρακολούθησης της οικιακής ασφάλειας. Οι κάμερες Vivint και Nest μπορούν να στείλουν ειδοποιήσεις στους ιδιοκτήτες σπιτιού όταν ανιχνεύουν δραστηριότητα, οπότε ο κάτοικος αναλαμβάνει το καθήκον της ερμηνείας των δεδομένων και της ανάληψης ενεργειών. Το iControl είναι ενοποιητικό, καθώς η κάμερα συνδυάζεται με ανίχνευση κίνησης, ανίχνευση ήχου και σειρήνα εισβολέα. Εναλλακτικά, το SmartThings όχι μόνο διευκολύνει την παρακολούθηση μέσω κάμερας και τις συναγερμούς κατοίκων, αλλά μπορεί να συνδέσει και άλλες συσκευές, όπως κλειδαριές θυρών, για να βοηθήσει τους κατοίκους να αναλάβουν απομακρυσμένη δράση σε περίπτωση πιθανών απειλών. Μια δεύτερη πηγή αισθητήρα περιβάλλοντος στο σπίτι για ασφάλεια είναι ηχητική. Οι Zhuang κ.ά. χρησιμοποιούν μοντέλα Gaussian για να αναλύσουν δεδομένα από μικρόφωνα για να ανιχνεύσουν ειδικά ανθρώπινες πτώσεις και να αυξήσουν το ρόλο του ηχητικού σήματος, ποσοτικοποιώντας ένα μέτρο "άγχους" στο σπίτι με βάση τους ασυνήθιστους δυνατούς θορύβους που ανιχνεύονται από τα μικρόφωνα σε όλο το σπίτι. Το μικρόφωνο συνοδεύεται από ένα φορητό επιταχυνσιόμετρο για να ανιχνεύσει εάν ο κάτοικος έχει υποστεί πτώση. Οι εμπορικά διαθέσιμες τεχνολογίες ανίχνευσης οικιακής ασφάλειας συχνά βασίζονται στον κάτοικο για να ερμηνεύσει τα δεδομένα και να προτείνει δράσεις. Αυτή η διαδικασία μπορεί να γίνει πιο αυτοματοποιημένη μέσω της χρήσης βιομετρικών στοιχείων. Η βιομετρία θα αναγνωρίζει αυτόματα τα άτομα βάσει μοναδικών ανατομικών χαρακτηριστικών, όπως η φωνή, το βάδισμα, ο αμφιβληστροειδής και το πρόσωπο καθώς και το σχήμα του σώματος (ανθρωπομετρία) και μοτίβο καρδιακού ρυθμού. Ενώ τα βιομετρικά στοιχεία χρησιμοποιούνται συχνά για μεγάλα κτίρια και λειτουργίες, δεν ενσωματώνονται τόσο συχνά σε μεμονωμένα σπίτια, λόγω της ποσότητας της κατάρτισης μοντέλων που βασίζεται στη μηχανική μάθηση και των θεμάτων προστασίας της ιδιωτικής ζωής. Στο πλαίσιο των μεμονωμένων σπιτιών, οι ερευνητές συχνά απαιτούν από τους κατοίκους να φέρουν συσκευές για τον εντοπισμό τους.

4.3.2 Ενέργειες ως απάντηση στις απειλές

Ένα έξυπνο σπίτι τυπικά εγχέεται με αισθητήρες για την παρακολούθηση του περιβάλλοντος. Όπως περιγράψαμε στην τελευταία ενότητα, αυτοί οι αισθητήρες μπορούν να δώσουν μια αρκετά ολοκληρωμένη ανάλυση και εντοπισμό πιθανών

απειλών. Υποθέτοντας ότι οι συλλεχθείσες πληροφορίες υποβάλλονται σε επεξεργασία και αναλύονται για την πιθανότητα και τον τύπο της απειλής, ένα έξυπνο σπίτι θα κάνει ιδανικά τα κατάλληλα βήματα για να δράσει για την απειλή. Η έρευνα και η τεχνολογική ανάπτυξη στον τομέα των έξυπνων κατοικιών εξελίχθηκε στο σημείο όπου τα σπίτια μπορούν να λάβουν αυτόνομες ενέργειες ώστε να απαντήσουν σε ανιχνευθέντες κινδύνους για την ασφάλεια ή την υγεία, όπως φαίνεται στην Εικόνα 8.

Εικόνα 8: Ενέργειες που λαμβάνουν χώρα σε ένα ασφαλές έξυπνο σπίτι

Η ποικιλία των βημάτων που μπορεί και πρέπει να κάνει ένα έξυπνο σπίτι δεν περιορίζεται στην ειδοποίηση και την ενημέρωση του κατοίκου. Όπως περιγράφεται στο Σενάριο 1, ορισμένα άτομα μπορούν να έχουν πρόσβαση μόνο στο γκαράζ ή στη μπροστινή βεράντα, ενώ οι τεχνικοί επισκευής θα έχουν επίσης πρόσβαση σε περιοχές του σπιτιού που χρειάζονται την προσοχή τους. Εάν ένα άτομο καταφέρει να εισέλθει σε μη εξουσιοδοτημένες περιοχές του σπιτιού, ο ιδιοκτήτης κατοικίας ενημερώνεται.

Οι ιδιοκτήτες σπιτιού μπορούν να επιλέξουν να αφήνουν τους αισθητήρες περιβάλλοντος να λειτουργούν συνεχώς και να χρησιμοποιούν τις πιο εντατικές συσκευές λήψης δεδομένων, όπως οι κάμερες, μόνο όταν είναι εκτός της οικίας. Σε τέτοιες περιπτώσεις προτείνεται μια μέθοδος για την αυτόματη ανίχνευση αυτών των καταστάσεων και την ενεργοποίηση των βιντεοκαμερών. Σε αυτό το έργο, οι αισθητήρες κίνησης και πόρτας συλλέγουν συνεχώς δεδομένα και ένα σύστημα εκμάθησης μηχανών εκπαιδεύεται για να χαρτογραφήσει αυτές τις μετρήσεις αισθητήρων σε μια ετικέτα που υποδεικνύει αν οι κάτοικοι είναι στο σπίτι ή μακριά από

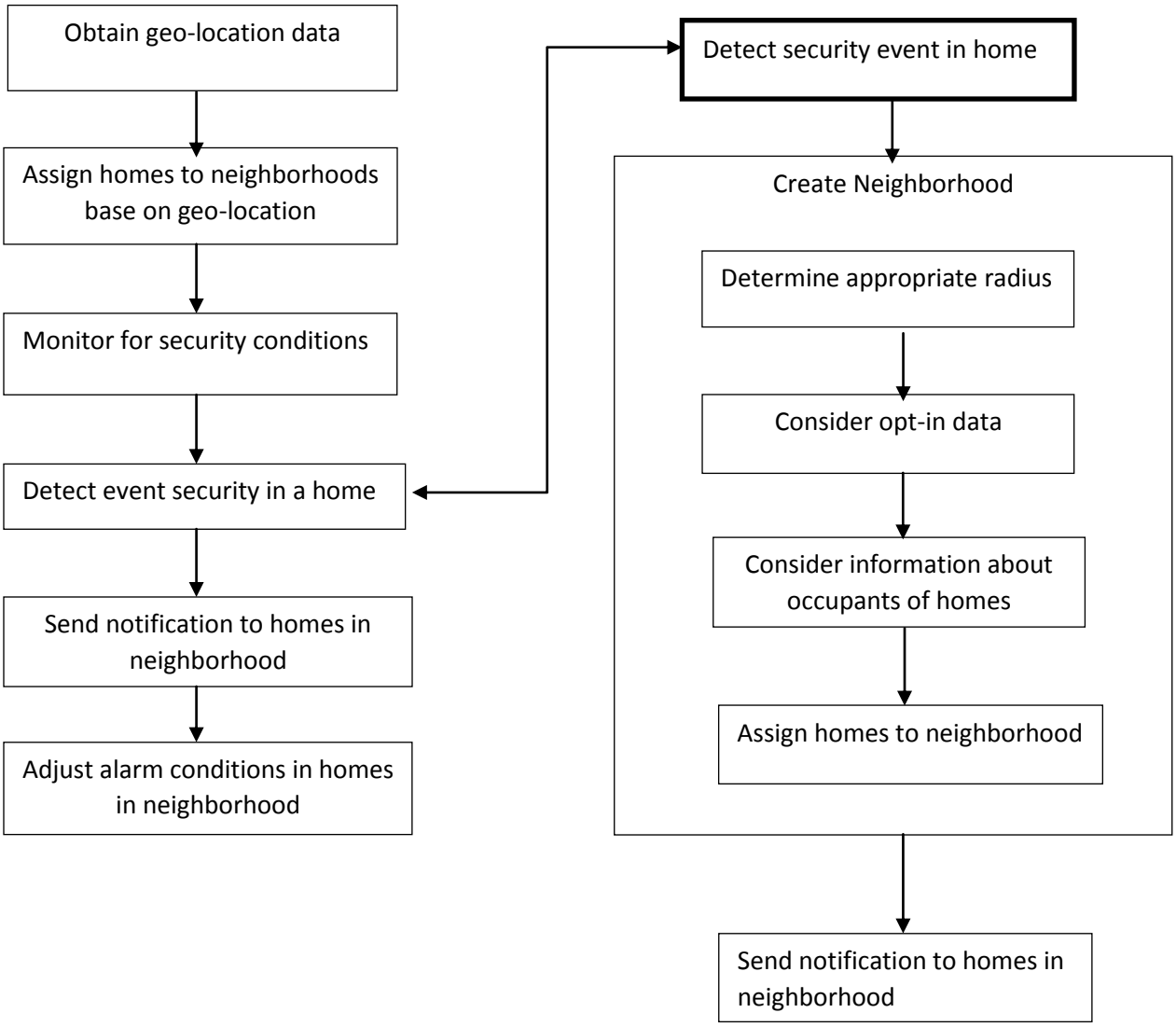
το σπίτι. Αυτή η προσέγγιση εξάγει χαρακτηριστικά, συμπεριλαμβανομένου του αριθμού των πυροδοτήσεων αισθητήρων κατά τη διάρκεια μικρού διαστήματος, ένδειξη του κατά πόσο ο κάτοικος βρίσκεται ή όχι στο κρεβάτι.. Ενώ η ανίχνευση εισβολών είναι μια κοινή εφαρμογή για συστήματα ασφαλείας, μεγάλο μέρος της τεχνολογίας μπορεί επίσης να εφαρμοστεί στην παρακολούθηση της υγείας και στην παροχή βοήθειας.

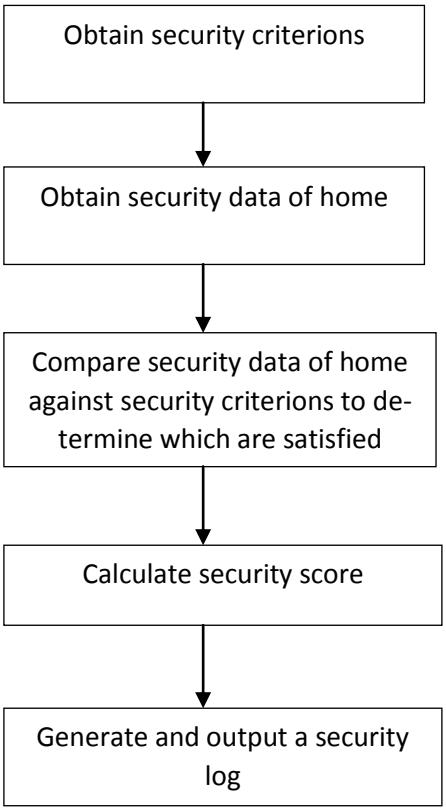
Διάφοροι ερευνητές έχουν βρει ότι η αύξηση του αριθμού των ανωμαλιών δραστηριότητας και της διακύμανσης στα πρότυπα συμπεριφοράς όπως η δραστηριότητα οι χρόνοι και η ταχύτητα περπατήματος συσχετίζονται με αλλαγές στη γνωστική υγεία. Όπως στην περίπτωση της εισβολής έρευνα ανίχνευσης, αυτά τα ευρήματα παρέχουν ιδέες που μπορούν να χρησιμοποιηθούν από έξυπνα σπίτια για να διατηρηθούν κάτοικοι ασφαλείς. Για παράδειγμα, οι κάτοικοι και οι φροντιστές τους μπορούν να χρησιμοποιήσουν αυτές τις πληροφορίες για να αλλάξουν το επίπεδο του φροντίδα που χρειάζεται το άτομο. Στη συνέχεια ακολουθεί ένας αλγόριθμος έξυπνου σπιτιού (Smart Home System Algorithm), ο οποίος ανιχνεύει κίνηση, κατάσταση φυσικού αερίου και θερμοκρασία και αναλόγως με τις τιμές που ανιχνεύει, εκτελεί διορθωτικές ενέργειες.

Algorithm 1: Smart Home System Algorithm

```
1.    if motion sensed by the PIR sensor
                        then
2.    Turned ON Light
3.  Else
4.    Keep sensing
5.  end if
6.     if MQ5 gas value greater than or
    equals to 1050 then
7.        Start Alarm
8.     else
9.        Keep sensing
10.    end if
11.        if electromagnetic door sensor
    lost the line of sight connection for
    30 sec then
12.          Start Alarm
13.         else
14.           Keep checking
15.        end if
16.            if temperature less than or
    equals to 24°C then
17.              Turned OFF Fan
18.            else
19.                if temperature greater
    than 24°C then
                      Turned ON Fan
          (Speed of Fan increased with the
              increase in temperature)
20.               end if
21.        end if
```

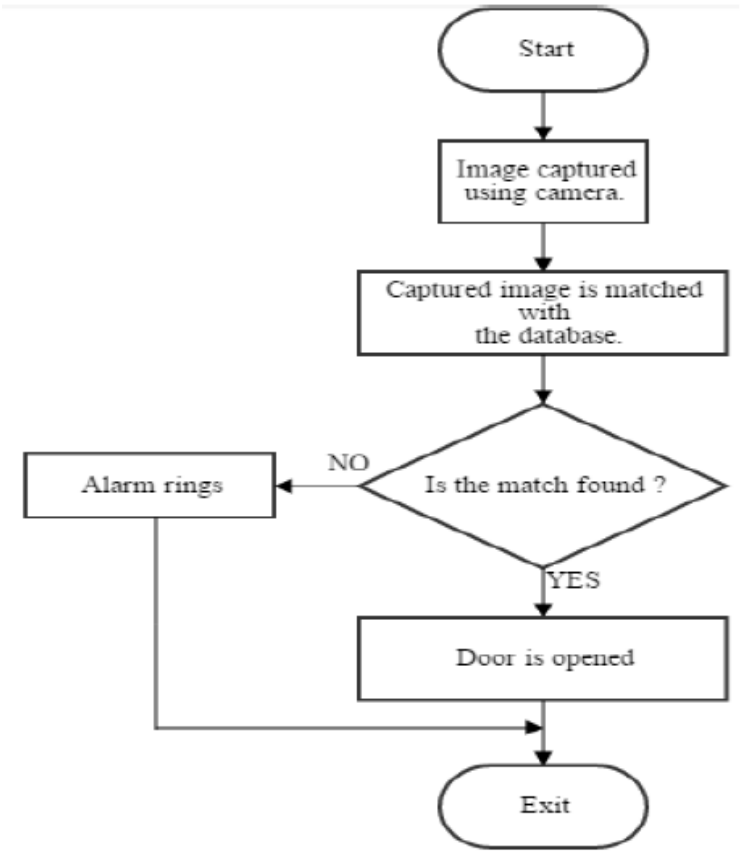
Στη συνέχεια ακολουθεί ένα διάγραμμα ροής, **το οποίο περιγράφει συνοπτικά τη λειτουργία ενός έξυπνου σπιτιού**. Η όλη διαδικασία ξεκινά από την απόκτηση δεδομένων γεωγραφικής θέσης και συνεχίζει με την εκχώρηση σπιτιών σε γειτονιές με βάση αυτά.


Obtain geo-location data
Assign homes to neighborhoods base on geo-location
Monitor for security conditions
Detect event security in a home
Send notification to homes in neighborhood
Adjust alarm conditions in homes in neighborhood
Detect security event in home
Create Neighborhood
Determine appropriate radius
Consider opt-in data
Consider information about occupants of homes
Assign homes to neighborhood
Send notification to homes in neighborhood


Obtain security criterions
Obtain security data of home
Compare security data of home against security criterions to determine which are satisfied
Calculate security score
Generate and output a security log

4.3.3 Αλγόριθμος αναγνώρισης προσώπου – Σενάριο αντιμετώπισης εισβολέα

Ένας ανεπιθύμητος εισβολέας έχει καταφέρει να ανιχνεύσει όλους τους κωδικούς ενός έξυπνου σπιτιού. Η τελευταία γραμμή άμυνας είναι ο έλεγχος προσώπου (face control) με το οποίο διασφαλίζουμε το σπίτι. Σε περίπτωση που το πρόσωπο είναι άγνωστο στέλνεται μήνυμα στο κινητό τηλέφωνο του ιδιοκτήτη, ο οποίος καθορίζει τι θα συμβεί, αν δηλαδή προκύψει λήξη συναγερμού ή εναλλακτικά αναγκαστεί να καλέσει την Αστυνομία ή την ιδιωτική ασφάλεια (σε περίπτωση διαθεσιμότητας).



Input:

1. Ανίχνευση προσώπου με χρήση κάμερας.

Process:

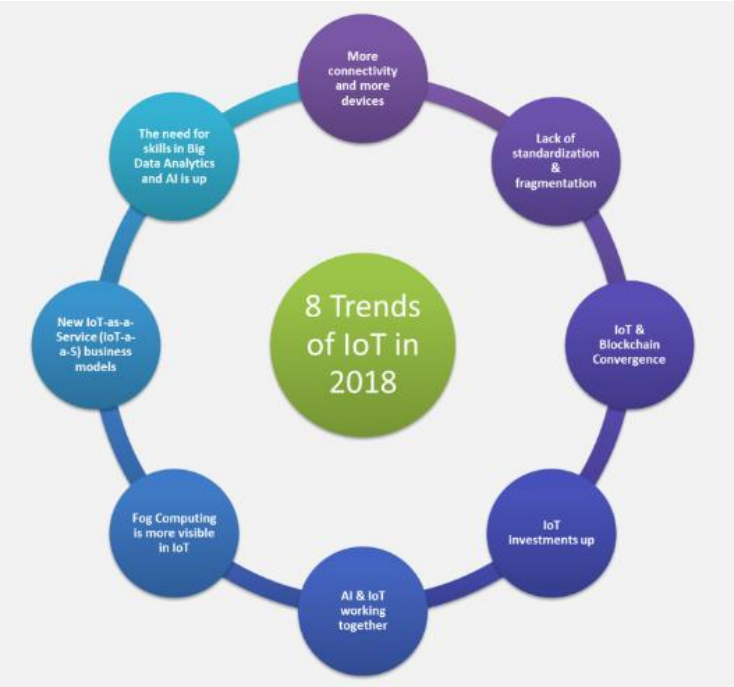
1. Σύγκριση εικόνας ατόμου με τις εικόνες των ατόμων που διαμένουν στην οικία και είναι αποθηκευμένες μέσα στη βάση δεδομένων του Η/Υ, που πραγματοποιεί την ανίχνευση.

Output:

1. Αν αποδειχθεί ταυτοπροσωπία τότε η πόρτα ανοίγει, διαφορετικά χτυπά ο συναγερμός στην εφαρμογή του χρήστη.

Κεφάλαιο 5 - Μελλοντικές τάσεις του Διαδικτύου των Πραγμάτων

Το Διαδίκτυο των Πραγμάτων (IoT) αυξάνεται με ταχείς ρυθμούς και το 2018 θα είναι ένα συναρπαστικό έτος για τη βιομηχανία του (Banafa, 2018). Οι καταναλωτές και οι επιχειρήσεις προβλέπουν την επόμενη μεγάλη καινοτομία και θέλουν να χρησιμοποιήσουν τον πρωτοποριακό αντίκτυπο του Διαδικτύου των Πραγμάτων στην καθημερινότητά τους. Το IoT αναμένεται να έχει τεράστια αύξηση προς όλες τις κατευθύνσεις και οι ακόλουθες οκτώ τάσεις που περιγράφονται στην Εικόνα 5, είναι οι κύριες εξελίξεις που αναμένεται να συμβούν.



Εικόνα 9: Μελλοντικές τάσεις του Διαδικτύου των Πραγμάτων (Banafa, 2018)

Τάση 1: *Η έλλειψη τυποποίησης θα συνεχιστεί.*

Οι ψηφιακά συνδεδεμένες συσκευές γίνονται γρήγορα ένα ουσιαστικό μέρος της καθημερινότητάς μας, αν και η υιοθέτηση του Διαδικτύου θα είναι μεγάλη και πιθανότατα αργή. Ο πρωταρχικός λόγος για αυτό είναι η έλλειψη τυποποίησης. Αν και οι ηγέτες της βιομηχανίας προσπαθούν να αναπτύξουν συγκεκριμένα πρότυπα και να απαλλαγούν από τον κατακερματισμό, θα εξακολουθούν να υπάρχουν προβλήματα. Δεν θα υπάρξουν σαφή πρότυπα στο εγγύς μέλλον αναφορικά με το IoT εκτός και αν ένας οργανισμός όπως ο IEEE βρει τον τρόπο ή μια κυβέρνηση επιβάλλει περιορισμούς στην επιχειρηματική συνεργασία με τις εταιρείες, εάν δεν χρησιμοποιούν ενιαία

πρότυπα. Τα εμπόδια που αντιμετωπίζει η τυποποίηση του IoT μπορούν να χωριστούν σε τρεις κατηγορίες:

- *Πλατφόρμα:* περιλαμβάνει τη μορφή και το σχεδιασμό των προϊόντων (UI / UX) και τα εργαλεία ανάλυσης που χρησιμοποιούνται για την ασφαλή αντιμετώπιση της μαζικής ροής δεδομένων από όλα τα προϊόντα και την κλιμάκωση. Με τον όρο *UX σχεδιαστής (Σχεδιαστής Εμπειρίας Χρήστη - User Experience Designer)* εννοούμε ένα άτομο που έχει στόχο να γίνει η αλληλεπίδραση του χρήστη με τη συσκευή όσο το δυνατόν πιο αποτελεσματική και απλή. Ο συγκεκριμένος σχεδιαστής φαντάζεται το σχεδιασμό προϊόντων από την οπτική γωνία ενός απλού χρήστη και χρησιμοποιώντας διάφορα είδη δοκιμών (όπως π.χ. χρηστικότητα, εργαστηριακές μελέτες, έρευνες ηλεκτρονικού ταχυδρομείου), παρακολουθεί το τι κάνουν οι χρήστες. Επίσης συγγράφει διάφορα σενάρια χρηστών προϊόντων και δημιουργεί πρότυπα αλληλεπίδρασης. Με τον όρο *UI σχεδιαστής (Σχεδιαστής Διεπαφής Χρήστη - User Interface Designer)* εννοούμε ένα άτομο που ενδιαφέρεται πρωτίστως για το πώς φαίνεται το προϊόν. Είναι υπεύθυνος για το πως βλέπουμε το προϊόν στην τελική του έκδοση και για το σχεδιασμό κάθε οθόνης/σελίδας με την οποία ο χρήστης αλληλεπιδρά και εξασφαλίζει ότι η διασύνδεση χρήστη επικοινωνεί οπτικά με τη λογική που έχει προσφερθεί από ένα σχεδιαστής UX. Για παράδειγμα, ένας σχεδιαστής UI που δημιουργεί ένα πίνακα δεδομένων μπορεί να φορτώσει το πιο σημαντικό περιεχόμενο στην κορυφή). Οι σχεδιαστές του UI είναι επίσης υπεύθυνοι για τη δημιουργία ενός οδηγού στυλ και μιας ενιαίας οπτικής γλώσσας που εφαρμόζεται σε όλο το προϊόν.
- *Συνδετικότητα*: περιλαμβάνει όλα τα μέρη της ρουτίνας της ημέρας και της νύχτας του καταναλωτή, από τη χρήση φορητών, έξυπνων αυτοκινήτων, έξυπνων σπιτιών και σε ένα μεγαλύτερο σχέδιο όπως οι έξυπνες πόλεις. Από την επιχειρηματική σκοπιά, έχουμε τη δυνατότητα σύνδεσης με το Βιομηχανικό Διαδίκτυο των Πραγμάτων (IIoT - Industrial Internet of Things)[16], όπου

[16] Το βιομηχανικό Διαδίκτυο των πραγμάτων, ή IIoT, είναι η χρήση του Διαδικτύου τεχνολογιών πραγμάτων για την ενίσχυση της βιομηχανικής παραγωγής και των βιομηχανικών διαδικασιών.

κυριαρχούν οι επικοινωνίες τύπου M2M (Machine – to – Machine)[17] σε αυτόν τον τομέα.

- *Εφαρμογές:* σε αυτή την κατηγορία, απαιτούνται τρεις εφαρμογές που να οδηγούν τις εξελίξεις[18] και πιο συγκεκριμένα εφαρμογές που να εκτελούν: έλεγχο πραγμάτων, συλλογή δεδομένων και ανάλυση δεδομένων. Το IoT χρειάζεται τέτοιου είδους *killer applications* για να οδηγήσει το επιχειρηματικό μοντέλο, χρησιμοποιώντας μια ενοποιημένη πλατφόρμα.

Οι τρεις κατηγορίες είναι αλληλένδετες μεταξύ τους και για το λόγο αυτό είναι προϋπόθεση να υπάρχουν όλες. Εάν λείπει κάποια, θα σπάσει αυτό το μοντέλο και θα σταματήσει η διαδικασία τυποποίησης. Χρειάζεται πολύ δουλειά για αυτή τη διαδικασία, αφού πολλές εταιρείες συμμετέχουν σε κάθε μία από τις προαναφερόμενες κατηγορίες, και κατά συνέπεια θα είναι ενθαρρυντικό να μπορέσουν να συμφωνήσουν για την ενοποίηση των προτύπων.

Τάση 2: Περισσότερη δυνατότητα σύνδεσης και περισσότερες συσκευές

Η ταχεία διάδοση του Διαδικτύου τα τρία τελευταία χρόνια έχει οδηγήσει σε δισεκατομμύρια διασυνδεδεμένες συσκευές. Καθώς ο καταναλωτής εξακολουθεί να παραμένει συνδεδεμένος με περισσότερα gadgets, ο αριθμός των συνδεδεμένων συσκευών αυξάνεται εκθετικά κάθε χρόνο. Μέχρι το 2018 τουλάχιστον θα διπλασιαστεί και θα αγγίξει ένα επιβλητικό αριθμό των 46 δισεκατομμυρίων μέχρι το 2021. Όλο και περισσότερες συσκευές IoT θα μπουν στα κανάλια, περισσότερες από ποτέ άλλοτε.

Μια σαφής ένδειξη της άμεσης εξάρτησής μας από τα gadgets και για το πως διαμορφώνεται το μέλλον μας αποτελεί το γεγονός ότι καθώς το IoT συνεχίζει να επεκτείνεται, σίγουρα θα διαπιστώσουμε αύξηση των συσκευών που συνδέονται με το δίκτυο σε διάφορους τομείς στις αγορές των επιχειρήσεων και των καταναλωτών. Οι έξυπνες συσκευές θα γίνουν de facto για να μπορούν οι χρήστες να διαχειρίζονται

[17] Αναφέρεται στην άμεση επικοινωνία μεταξύ συσκευών που χρησιμοποιούν οποιοδήποτε κανάλι επικοινωνίας, συμπεριλαμβανομένων των ενσύρματων και ασύρματων. Η επικοινωνία μηχανής με μηχανή μπορεί να περιλαμβάνει βιομηχανικά όργανα, επιτρέποντας σε έναν αισθητήρα ή ένα μετρητή να μεταδίδει τα δεδομένα που καταγράφει (όπως θερμοκρασία, επίπεδο αποθέματος κ.λπ.) στο λογισμικό εφαρμογής που μπορεί να τα χρησιμοποιήσει (για παράδειγμα, προσαρμογή μιας βιομηχανικής διαδικασίας με βάση τη θερμοκρασία ή την παραγγελία για την ανανέωση του αποθέματος). Αυτή η επικοινωνία ολοκληρώθηκε αρχικά με την αποστολή ενός απομακρυσμένου δικτύου μηχανών πληροφοριών αναμετάδοσης σε έναν κεντρικό κόμβο για ανάλυση, το οποίο στη συνέχεια μετατοπίστηκε σε ένα σύστημα όπως ένας προσωπικός υπολογιστής

[18] Οι εφαρμογές αυτές ονομάζονται *killer applications*, με την έννοια ότι οδηγούν τις εξελίξεις και πρωτοπορούν και υπερισχύουν έναντι άλλων.

συσκευές IoT. Τα οφέλη από τη χρήση έξυπνων συσκευών με αυτή την ιδιότητα περιλαμβάνουν την ενίσχυση της εμπλοκής πελατών, την αύξηση της ορατότητας και τον εξορθολογισμό της επικοινωνίας που θα περιλαμβάνει νέες διασυνδέσεις ανθρώπου - μηχανής, όπως είναι η φωνητική διασύνδεση χρήστη (VUI - Voice User Interface) ή το Chatbot. Πιο συγκεκριμένα, μια φωνητική διασύνδεση χρήστη (VUI) επιτρέπει στους χρήστες να χρησιμοποιούν φωνητική είσοδο για τον έλεγχο των υπολογιστών και των συσκευών. Οι φωνητικές εμπειρίες είναι εξαιρετικές όταν προσφέρουν έναν ταχύτερο, ευκολότερο και πιο ευχάριστο τρόπο επικοινωνίας με τις συσκευές. Οι σημερινές διεπαφές τέτοιου είδους καθίστανται όλο και πιο έξυπνες, μαθαίνοντας τα πρότυπα ομιλίας του χρήστη με την πάροδο του χρόνου και δημιουργώντας ακόμη και το δικό τους λεξιλόγιο. Από την άλλη μεριά ένα διαδραστικός πράκτορας ή τεχνητός συνομιλητής οντότητας (chatbot ή talkbot ή chatterbot) είναι ένα πρόγραμμα υπολογιστή ή μια εφαρμογή Τεχνητής Νοημοσύνης που διεξάγει συνομιλία με ακουστικές ή κειμενικές μεθόδους.

Τέτοια προγράμματα συχνά σχεδιάζονται για να προσομοιώνουν πειστικά το πώς ένας άνθρωπος θα συμπεριφερόταν ως συνομιλητικός εταίρος. Τα chatbots χρησιμοποιούνται συνήθως σε συστήματα διαλόγου για διάφορους πρακτικούς σκοπούς, συμπεριλαμβανομένης της εξυπηρέτησης πελατών ή της απόκτησης πληροφοριών. Ορισμένα chatterbots χρησιμοποιούν εξελιγμένα συστήματα επεξεργασίας φυσικής γλώσσας, αλλά πολλά απλούστερα συστήματα ανιχνεύουν λέξεις - κλειδιά στην είσοδο και στη συνέχεια δίνουν μια απάντηση με τις πιο κατάλληλες λέξεις-κλειδιά ή το πιο παρόμοιο πρότυπο διατύπωσης από μια βάση δεδομένων.

Τάση 3: Αύξηση ασφάλειας του IoT & Blockchain σύγκλιση

Όπως συμβαίνει με την περισσότερη τεχνολογία, η ασφάλεια θα αποτελέσει τη μείζονα πρόκληση που πρέπει να αντιμετωπιστεί. Καθώς το ψηφιακό περιβάλλον καθίσταται ολοένα και περισσότερο πιο υψηλής τεχνολογίας, οι συσκευές γίνονται εύκολος στόχος για τους κυβερνοεγκληματίες. Οι καταναλωτές δεν πρέπει μόνο να ανησυχούν για τα smartphones καθότι μπορεί να παραβιαστούν και άλλες συσκευές όπως αυτοκίνητα με Wi-Fi, φορητά και ιατρικές συσκευές. Η ασφάλεια είναι αναμφισβήτητα μια μεγάλη ανησυχία και πρέπει να αντιμετωπιστούν τα τρωτά της σημεία. Το Blockchain είναι μια νέα ελπίδα για την ασφάλεια του Διαδικτύου. Η

εκπληκτική κατάκτηση των κρυπτονομισμάτων, η οποία βασίζεται στην τεχνολογία Blockchain, έχει θέσει την τεχνολογία ως φορέα σημασιολογικών συναλλαγών, μειώνοντας έτσι το κόστος και εξαλείφοντας την ανάγκη εμπιστοσύνης σε μια κεντρική πηγή δεδομένων. Το Blockchain λειτουργεί με την ενίσχυση της εμπιστοσύνης για ασφαλείς, γρήγορες και διαφανείς συναλλαγές. Τα δεδομένα σε πραγματικό χρόνο από ένα κανάλι IoT μπορούν να χρησιμοποιηθούν σε τέτοιες συναλλαγές, διατηρώντας παράλληλα την ιδιωτικότητα όλων των εμπλεκόμενων μερών.

Το μεγάλο πλεονέκτημα του blockchain είναι ότι είναι δημόσιο. Όλοι οι συμμετέχοντες μπορούν να δουν τα μπλοκ και τις συναλλαγές που είναι αποθηκευμένες σε αυτά. Αυτό βέβαια δεν σημαίνει ότι όλοι μπορούν να δουν το πραγματικό περιεχόμενο της συναλλαγής, αφού προστατεύεται από το ιδιωτικό κλειδί. Ένα μπλοκ αλυσίδας είναι αποκεντρωμένο, επομένως δεν υπάρχει ενιαία αρχή που να μπορεί να εγκρίνει τις συναλλαγές ή να ορίσει συγκεκριμένους κανόνες για να γίνει αποδεκτή η συναλλαγή. Αυτό σημαίνει ότι υπάρχει μεγάλη εμπιστοσύνη, δεδομένου ότι όλοι οι συμμετέχοντες στο δίκτυο πρέπει να καταλήξουν σε συναίνεση για την αποδοχή των συναλλαγών. Το πιο σημαντικό, είναι η ασφάλεια που παρέχεται. Η βάση δεδομένων μπορεί να επεκταθεί και τα προηγούμενα αρχεία δεν μπορούν να αλλάξουν (τουλάχιστον, υπάρχει ένα πολύ υψηλό κόστος εάν κάποιος θέλει να αλλάξει προηγούμενα αρχεία). Το 2018 αυξήθηκε το ενδιαφέρον για την τεχνολογία Blockchain που θα καταστήσει τη σύνδεση των συσκευών και υπηρεσιών Blockchain και IoT.

Τάση 4: Οι επενδύσεις στο Διαδίκτυο θα συνεχιστούν

Η IDC προβλέπει ότι οι δαπάνες για το διαδίκτυο θα φθάσουν τα 1,4 τρισεκατομμύρια δολάρια το 2021 (Banafa, 2018). Αυτό συμπίπτει με τις εταιρείες που συνεχίζουν να επενδύουν στο υλικό, το λογισμικό, τις υπηρεσίες και τη συνδεσιμότητα του Διαδικτύου. Σχεδόν κάθε κλάδος θα επηρεαστεί από το IoT, πράγμα που σημαίνει ότι πολλές εταιρείες θα επωφεληθούν από την ταχεία ανάπτυξή του. Η μεγαλύτερη κατηγορία δαπανών μέχρι το 2021 θα είναι το υλικό, ειδικά μονάδες και αισθητήρες, αλλά αναμένεται να ξεπεραστεί από την κατηγορία των ταχύτερα αναπτυσσόμενων υπηρεσιών. Οι δαπάνες λογισμικού θα κυριαρχήσουν εξίσου και από το λογισμικό εφαρμογών, συμπεριλαμβανομένων των εφαρμογών για κινητά. Ο αναμφισβήτητος αντίκτυπος του IoT έχει και θα συνεχίσει να προσελκύει περισσότερους επιχειρηματίες

κεφαλαίων επιχειρηματικού κινδύνου για την ανάπτυξη καινοτόμων έργων. Είναι μία από αυτές τις λίγες αγορές που έχουν το ενδιαφέρον τόσο των αναπτυσσόμενων όσο και των παραδοσιακών επιχειρηματικών κεφαλαίων. Ενώ η ανάπτυξη το επόμενο έτος επιβεβαιώνεται αν και το πραγματικό δυναμικό δεν έχει αποκαλυφθεί ακόμη, οι επιχειρηματικές δραστηριότητες του IoT θα προτιμηθούν σε σχέση με όλους τους άλλους. Πολλές επιχειρήσεις έχουν εξασφαλίσει την προσθήκη IoT στο πρότυπο υπηρεσιών τους όπως τις βιομηχανίες μεταφορών, λιανικού εμπορίου και ασφάλισης.

Τάση 5: Το Fog Computing θα είναι πιο ορατό

Το Fog computing επιτρέπει τη λήψης αποφάσεων μέσω συσκευών IoT και προωθεί μόνο τα σχετικά δεδομένα στο Cloud, η Cisco έδωσε τον εξής ορισμό για το Fog Computing: *Η ομίχλη επεκτείνει το νέφος να είναι πιο κοντά στα πράγματα που παράγουν και δρουν σε δεδομένα IoT. Αυτές οι συσκευές, που ονομάζονται fog nodes, μπορούν να αναπτυχθούν οπουδήποτε υπάρχει σύνδεση δικτύου: σε ένα εργοστάσιο, σε όχημα ή σε εξέδρα πετρελαίου. Παραδείγματα περιλαμβάνουν βιομηχανικούς ελεγκτές, διακόπτες, δρομολογητές, ενσωματωμένους διακομιστές και κάμερες παρακολούθησης βίντεο*. Τα οφέλη από τη χρήση του Fog Computing είναι πολύ ελκυστικά για τους Παρόχους του IoT. Μερικά από τα οφέλη αυτά είναι η ελαχιστοποίηση της καθυστέρησης, η εξοικονόμηση του εύρους ζώνης δικτύου, η λειτουργία με αξιόπιστα και γρήγορες αποφάσεις.

Τάση 6: Το AI & IoT θα λειτουργήσει κλειστά

Η συγχώνευση των αναλυτικών στοιχείων δεδομένων IoT με AI για εφαρμογές που κυμαίνονται από τη συντήρηση του ανελκυστήρα έως τα έξυπνα σπίτια, θα προχωρήσει γρήγορα τα επόμενα δύο χρόνια. Οι πάροχοι υπηρεσιών παρέχουν ολοένα και περισσότερες λύσεις με ενσωματωμένα στοιχεία ανάλυσης που έχουν σχεδιαστεί για να τροφοδοτούν δεδομένα απευθείας σε αλγόριθμους AI. Ένα άλλο σημαντικό πλεονέκτημα της χρήσης του AI είναι η υποστήριξη της βελτιστοποίησης και της προσαρμογής τόσο των συσκευών IoT όσο και των σχετικών διαδικασιών και υποδομών. Η AI μπορεί να βοηθήσει στην Ανάλυση Δεδομένων του IoT στους ακόλουθους τομείς: προετοιμασία δεδομένων, ανακάλυψη δεδομένων, οπτικοποίηση δεδομένων ροής, ακρίβεια δεδομένων σε δεδομένα χρονοσειρών, προγνωστική και ανάλυση σε πραγματικό χρόνο.

Τάση 7: Νέα επιχειρηματικά μοντέλα IoT-as-a-Service (IoT-a-a-S)

Τα μετασχηματιστικά επιχειρηματικά μοντέλα θα αναπτυχθούν σε πολλές περιοχές του IoT από το 2018-2019, υποστηριζόμενες από τα εργαλεία Big Data και AI. Σε αυτά τα μοντέλα, η αξία είναι στην ευκολία της υπηρεσίας για τους τελικούς πελάτες (κατ' απαίτηση χωρίς να απαιτούνται σημαντικές εκ των προτέρων δαπάνες) και τα δεδομένα χρήσης που συλλέγονται, αναλύονται και διοχετεύονται πίσω στις επιχειρήσεις και τους προμηθευτές. Ωστόσο, το δυναμικό για τον μετασχηματισμό επιχειρηματικών μοντέλων του IoT εκτείνεται πέρα από αυτό, για να συμπεριλάβει μια αυξανόμενη ποικιλία από πιο σύνθετα επιχειρηματικά μοντέλα που λειτουργούν ως υπηρεσίες, τα οποία διαταράσσουν τις υπάρχουσες βιομηχανίες, ιδίως σε τομείς όπως η βαριά βιομηχανία, καθώς και τις έξυπνες πόλεις. Στις βιομηχανίες αυτές, οι λύσεις IoT μπορούν να επιτρέψουν περισσότερες συνεχείς, διαχειριζόμενες σχέσεις παροχής υπηρεσιών τόσο με τους προμηθευτές τεχνολογίας όσο και με τους τελικούς πελάτες. Ένα σημαντικό σημείο είναι ότι το κόστος μπορεί να συνδέεται πιο άμεσα με τη συνεχιζόμενη μετρούμενη χρήση ή με συγκεκριμένα γεγονότα ενεργοποίησης που συλλαμβάνονται από τους αισθητήρες IoT. Ένα άλλο είναι ότι το κόστος μπορεί να εξαπλωθεί με την πάροδο του χρόνου, αλλάζοντας από το Capex εκ των προτέρων σε μια πιο τακτική εκροή Opex. Παραδείγματα τέτοιων μοντέλων είναι τα συστήματα φωτισμού ως υπηρεσία (I-a-a-S), οι σιδηροδρομικές υπηρεσίες (R-a-a-S) και ακόμη και οι ανελκυστήρες ως υπηρεσία.

Τάση 8: Η ανάγκη για δεξιότητες στο Big Data Analytics της IoT και το AI θα αυξηθούν

Η δυναμική ανταλλαγή δεδομένων βρίσκεται στο επίκεντρο του IoT και το Big Data Analytics θα συμβάλει στην κατασκευή ευαίσθητων εφαρμογών. Η ενσωμάτωση των διαύλων δεδομένων IoT με την Τεχνητή Νοημοσύνη (Artificial Intelligence – AI) για την ανάκτηση αναλυτικών γνώσεων κατόπιν ζήτησης, έχει ήδη κερδίσει μεγάλη δυναμική και αναμένεται να αυξηθεί τα επόμενα χρόνια.

Βιβλιογραφία

1. **Alphand O.** Iotchain: A Blockchain security arcitecture for the internet of things [Άρθρο]. - 2018.
2. **Arabo A.** Privacy in the age of mobility and smart devices in smart homes [Συνέδριο]. - 2014. - σσ. 819-826.
3. **Ashton Kevin** That 'The Internet of things' Thing [Άρθρο]. - 2009.
4. **Banafa A.** Eight Trends of the Internet of Things in 2018 [Άρθρο]. - 2018.
5. **Bhardwaj A.** A beginner's guide to Bitcoin and Cryptocurrencies [Βιβλίο]. - 2016.
6. **Bhga A.** Blockchain platform for industrial internet of things [Άρθρο]. - 2016.
7. **Boldt B.** Without Security, is Internet of things just a Toy? [Εργασία]. - 2015.
8. **Brambilla G.** Using Block Chain for Peer-to-Peer Proof-of-Location [Επιθεώρηση]. - 2016.
9. **Buchman E.** Tendermint: Byzantine fault tolerance in the age of blockchains [Βιβλίο]. - 2016.
10. **Carminati B.** Enhancing user control on personal data udage in internet of things ecosystems [Άρθρο]. - 2016. - σσ. 291-298.
11. **David G.** Kickstarter My Heart: Extraordinary Popular Delusions and the Madness of Crowdfunding Constraints and Bitcoin Bubbles [Άρθρο]. - 2014.
12. **Dorri A.** Towards an Optimized BlockChain fot IoT [Συνέδριο]. - Pitsburgh : [s.n.], 2017.
13. **Gaur A.** Smart city architecture and its applications based on IoT [Βιβλίο]. - 2015.
14. **Gervais A.** On the security and perfomance of proof of work blockchains [Συνέδριο] // Conference on Computer and Communications Security. - 2016. - σσ. 3-16.
15. **Hashemi S. H.** World of empowered IoT users [Άρθρο]. - 2016. - σσ. 13-24.
16. **Hassanalieragh M.** Health monitoring and management using Internet-of-things sensing with cloud-based processing: Opportunities and challenges [Άρθρο]. - 2015. - σσ. 285-292.
17. **Huh S.** Managing IoT devises using blockchain platform [Άρθρο]. - 2017. - σσ. 464-467.
18. **Jing Q.** Security of the inernet of things: Perspectives and challenges [Επιθεώρηση]. - 2014. - σσ. 2481-2501.
19. **Jurdak R.** e Case Study of a Smart Home [Επιθεώρηση]. - 2017.
20. **Jurdak R.** e Case Study of a Smart Home [Επιθεώρηση]. - 2017.
21. **Kanhere S. S.** Lsb: A lightweight scalable blockchain for Iot security and privacy [Άρθρο]. - 2017.
22. **Kousaridas A.** Density-based algorithm for clusters discovery in wireless networks [Άρθρο]. - 2015. - σσ. 2126-2131.

23. **Lee B.** Blockchain-based secure firmware update for embedded devices in an internet of things environment [Άρθρο] // The Journal of Supercomputing. - 2016. - σσ. 1-16.

24. **Liu B.** Blockchain based data integrity service framework for IoT data [Άρθρο]. - 2017. - σσ. 468-475.

25. **Michael C.** Blockchain Technology: beyond Bitcoin [Άρθρο]. - 2015. - σσ. 9-10.

26. **Miller A.** Discovering Bitcoin's public topology and influential nodes [Άρθρο]. - 2015.

27. **Montjoye Y.** Protecting the privacy of metadat through safe answers [Επιθεώρηση]. - 2014.

28. **Sagirlar G.** Decentralizing Privacy Enforcement for Internet of Things Smart Objects [Άρθρο]. - April 2018.

29. **Salah K.** IoT Security: Review, Blockchain Solutions, and Open Challenges [Βιβλίο]. - 2017.

30. **Sivaraman V.** Network-level security and privacy for smarthome IoT devices [Άρθρο]. - 2015. - σσ. 163-167.

31. **Steve H.** Internet of Things, Blockchain and Shared Economy Applications [Άρθρο]. - 2014.

32. **Tschorsch F.** Bitcoin and beyond: A technical survey on decentralized digital curriencies [Άρθρο]. - 2016. - σσ. 2084-2123.

33. **Wessel R.** the Blockchain as a Narrative Technology: Investigating the Social Ontology and Normative Configurations of Cryptocurrencies [Βιβλίο]. - 2016.

34. **Wilkinson S.** Metadisk [Εργασία]. - 2014.

35. **Yue X.** Found Healthcare Inteligence on Blockchain with Novel privacy Risk Control [Άρθρο]. - 2016.

36. **Zheng Z.** An overview of blockchain technology: Architecture, consensus, and future trends [Άρθρο]. - 2016. - σσ. 557-564.

37. **Ντόα Γ.** Blockchain και η εφαρμογή του στο Internet of things [Βιβλίο]. - Αθήνα : [s.n.], 2017.

38. http://www ft.com/intl/cms/s/2/eb1f8256-7b4b-11e5- a1fe-567b37f80b64 html# axzz3qe4rV5dH

39. http://www ft.com/intl/cms/s/2/eb1f8256-7b4b-11e5- a1fe-567b37f80b64 html# axzz3qe4rV5dH

40. http://money.cnn.com/2015/11/02/technology/bitcoin-1-billion-invested/.

41. http://www.ft.com/cms/s/2/eb1f8256-7b4b-11e5-a1fe-567b37f80b64.html

42. https://research.tabbgroup.com/report/v14-009-blockchain-clearing-and-settlement-crossing-chasm.

43. https://www.ecb.europa.eu/explainers/tell-me-more /html/distributed_ledger_technology.el.html

44. http://www.fortunegreece.com/article /afti-ine-i-mania-tou-blockchain/

45. https://blockstream.com/sidechains.pdf

46. https://elementsproject.org/