Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Ασφάλεια και Εμπιστευτικότητα με Βάση την Τεχνολογία Blockchain στις Έξυπνες Πόλεις

Σοφοκλής Θεοδώρου

Επιβλέπων Καθηγητής
Νικόλαος Σκλάβος

Μάϊος 2018

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Ασφάλεια και Εμπιστευτικότητα με Βάση την Τεχνολογία Blockchain στις Έξυπνες Πόλεις

Σοφοκλής Θεοδώρου

Επιβλέπων Καθηγητής
Νικόλαος Σκλάβος

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών
στον Σοφοκλή Θοδώρου
από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου.

Μάϊος 2018

ΠΕΡΙΕΧΟΜΕΝΑ

Πρόλογος

Μια γρήγορη ματιά σε ιστοσελίδες τεχνολογίας και αντίστοιχα συνέδρια, είναι αρκετή για να διαπιστώσει κάποιος μια δεσπόζουσα τεχνολογία που μονοπωλεί το ενδιαφέρον της κοινότητας της Τεχνολογίας των Πληροφοριών και Επικοινωνίας (ΤΠΕ). Η αναφορά είναι για την τεχνολογία Blockchain όπου επιχειρεί να αλλάξει τον τρόπο που αποθηκεύεται, ασφαλίζεται και διακινείται η πληροφορία. Όμως πριν κάνουμε αναφορά στο μοντέλο του Blockchain θα πρέπει να κάνουμε ένα βήμα πίσω και να προσπαθήσουμε να καταλάβουμε τι οδήγησε την κοινότητα να καταφύγει σε νέες τεχνολογίες και λύσεις. Φυσικά η λίστα με τους λόγους δεν μπορεί να εξαντληθεί, αλλά μια πρώτη ματιά θα μας δώσει ένα πρώτο στίγμα.

Είναι ευρέως καταγεγραμμένο ότι οι πόλεις ολοένα μεγαλώνουν και σε συνδυασμό με την εποχή του Internet of Things (IoT), άρχισαν να δημιουργούνται Έξυπνες Πόλεις στις οποίες πολύ σύντομα θα καλεστούμε να ζήσουμε. Το μοντέλο του IoT ξεκίνησε να κάνει τα πρώτα δειλά του βήματα στις αρχές αιώνα μας. Παρά την δυναμική που δημιουργήθηκε και την αισιοδοξία όλων των εμπλεκομένων πλευρών, άργησε να μπει και πρακτικά στην καθημερινότητα των ανθρώπων. Εντούτοις, σήμερα βλέπουμε μια εντελώς διαφορετική δυναμική να δημιουργείται και ολοένα και περισσότερες εταιρείες και οργανισμοί υλοποιούν εφαρμογές και συσκευές που εν δυνάμει θα μπορούν να συνδεθούν στο ευρύτερο δίκτυο. Για να γίνουμε πιο συγκεκριμένοι, αυτοκινητοβιομηχανίες να επενδύουν μεγάλο μέρος του προϋπολογισμού τους στην υλοποίηση εφαρμογών που θα δίνουν την δυνατότητα να ελέγχεται το αυτοκίνητο μέσα από μια εφαρμογή. Σε μεγαλύτερο σκέλος, βλέπουμε έρευνες που προτείνουν αλγόριθμους για την εξάλειψη του μποτιλιαρίσματος μέσα διαχείριση της κίνησης στου δρόμους και έξυπνο παρκάρισμα σε πραγματικό χρόνο (Roy, et al., 2016). Γίνονται προσπάθειες για να δοθούν λύσεις ακόμα και σε βιομηχανικό περιβάλλον όπου εκεί οι τεχνολογίες που χρησιμοποιούνται είναι ιδιαίτερα ευαίσθητες (SCADA). Οι λόγοι εστιάζονται κυρίως στην κρισιμότητα των βιομηχανιών που ελέγχουν αυτές οι τεχνολογίες αφού έχουν να κάνουν με κρατικές μονάδες ηλεκτροδότησης, παραγωγής ενέργειας και μεταφορών. Παρά την κρισιμότητα των βιομηχανιών αυτών γίνονται προσπάθειες εφαρμογής μίας πλατφόρμας που

θα στηρίζεται στο IoT όπου θα γίνεται ο άμεσος έλεγχος και επίβλεψη της ασφάλειας ολόκληρου του δικτύου SCADA (Shahzad, A.Y., & Elgamoudi, 2017).

Μέσα από τις νέες συνθήκες που δημιουργούνται, έχουμε και αντίστοιχα καινούργιες ανάγκες σε θέματα ασφάλειας, ταχύτητας και ανάλυσης της πληροφορίας. Εγείρονται διάφορα ερωτήματα τα οποία η κοινότητα καλείται να απαντήσει και να επανέλθει με πρακτικές λύσεις που θα μπορούν να μπουν σε εφαρμογή άμεσα. Θα μπορέσουν, για παράδειγμα, να ανταπεξέλθουν οι εταιρείες που εδώ και δεκαετίες (ίσως και αιώνες) δεν είχαν καμία υποχρέωση να συμπεριλάβουν τα θέματα ασφαλείας της πληροφορίας στο τρόπο σχεδιασμού των προϊόντων τους; Μέχρι και τις αρχές της προηγούμενης δεκαετίας, ένα πλυντήριο ήταν μια αυτόνομη συσκευή που έπρεπε να πληρεί κάποιους κανόνες ασφαλείας χωρίς να χρειάζεται να συμμορφώνεται στους κανόνες ενός ευρύτερου δικτύου. Πλέον αυτή η συσκευή θα είναι αναπόσπαστο κομμάτι του δικτύου όπου χωρίς τον κατάλληλο σχεδιασμό και έλεγχο θα μπορούσε εν δυνάμει να αποτελεί τον αδύναμο κρίκο. Πιο συγκεκριμένα, έχουμε δει παραδείγματα όπου ηλεκτρικές συσκευές όπως πλυντήρια, κάμερες ασφαλείας, συστήματα πλοήγησης κ.α. έχουν γνωστές αδυναμίες ασφάλειας όπως προκαθορισμένες διεπαφές ethernet που επιτρέπουν επιθέσεις τύπου web server directory traversal. (Bing, 2017). Ενισχύοντας την πιο πάνω άποψη, η εταιρεία FORTINET δημοσιοποίησε ένα White Paper όπου αναλύει τις συνέπειες που θα έχει η μετάβαση στην εποχή του IoT για την ασφάλεια των επιχειρήσεων (FORTINET, 2017). Ανάμεσα σε άλλα αναφέρει ότι αύτη τη στιγμή «οι περισσότερες συσκευές IoT είναι ακέφαλες, που σημαίνει ότι δεν διαθέτουν παραδοσιακό λειτουργικό σύστημα ή ακόμα και τη μνήμη και την απαιτούμενη ισχύ επεξεργασίας για την κατασκευή ασφάλειας ή την εγκατάσταση ενός ασφαλούς client».

Άλλα ερωτήματα που τίθενται είναι τα θέματα της φύλαξης και διακίνησης (και με ποια ταχύτητα θα γίνεται αυτό) της πληροφορίας. Είναι ικανές οι υπάρχουσες λύσεις να ανταπεξέλθουν στις νέες προκλήσεις που επιβάλλουν τα εκατομμύρια κόμβων στις Έξυπνες Πόλεις; Όπως προαναφέραμε στη πρώτη παράγραφο αυτού του κεφαλαίου, η τεχνολογία Blockchain κερδίζει έδαφος ως ένας τρόπος να δώσει λύσεις στα πιο πάνω ερωτήματα αλλά και σε πολλά άλλα που εγείρονται. Έχοντας σαν βάση το αποκεντρωμένο και κατανεμημένο τρόπο φύλαξης της πληροφορίας, το Blockchain, εισέρχεται ως μια εναλλακτική λύση αφού δείχνει να μπορεί να καλύψει τα κενά που δημιουργούνται από τη μετάβαση στην εποχή του

IoT και κατ' επέκταση στις Έξυπνες Πόλεις. Συγκεκριμένα, το μοντέλο Blockchain προσφέρει τη δυνατότητα να εγκαταλειφθεί η χρήση των τρεχουσών τεχνολογιών αποθήκευσης πληροφοριών σε μητρώα τρίτων, για την ασφάλεια των οποίων απαιτείται η επένδυση υπέρογκου αριθμού πόρων (Kshentri, 2017). Οι πληροφορίες αποθηκεύονται σε διαφορετικές τοποθεσίες υπό την μορφή μπλοκ και σε κάθε μία από αυτές υπάρχει ένα πιστό αντίγραφο των εν λόγω πληροφοριών. Η απουσία ενός διαμεσολαβητή μειώνει σημαντικά τους πόρους που απαιτούνται και αυξάνει την ταχύτητα της συναλλαγής. Σε ένα από τα επόμενα κεφάλαια θα δούμε εμπεριστατωμένα την χρησιμότητα και λειτουργία του μοντέλου του Blockchain και πως αυτό θα μπορούσε να αποτελέσει το όχημα προς την κατεύθυνσή των Έξυπνων Πόλεων.

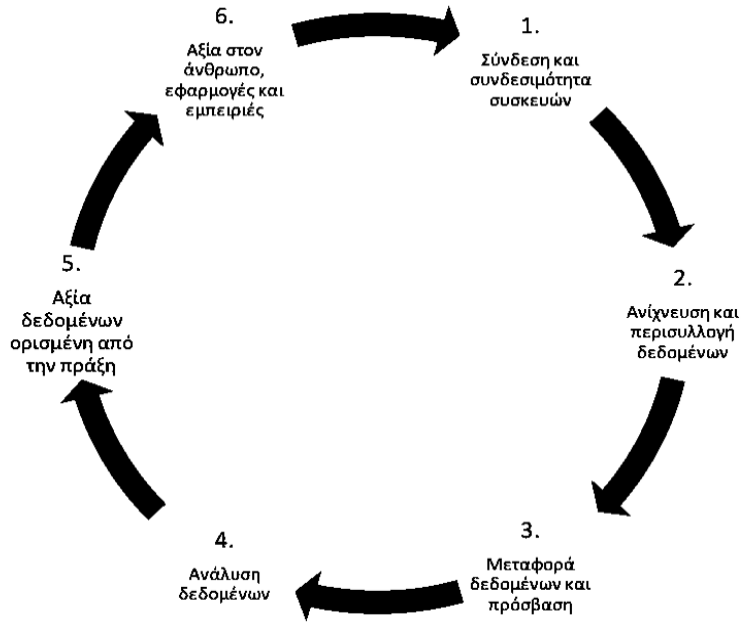
Μέσα από τις πολλές επαναστατικές αλλαγές που θα επιφέρει η εφαρμογή της τεχνολογίας του Blockchain είναι τα Έξυπνα Συμβόλαια (smart contracts). Στόχος τους θα είναι να εκτελούν αυτόνομες συναλλαγές και να αυξήσουν το ρυθμό αυτών των συναλλαγών μέσα στο χαοτικό περιβάλλον των μαζικών δεδομένων. Ακόμη, θα μειώσει την υπολογιστική ισχύ που θα απαιτείται για την διεκπεραίωση καθημερινών συναλλαγών συνεπεία των δισεκατομμυρίων συνδεδεμένων κόμβων. Τα Έξυπνα Συμβόλαια βρίσκονται στο Blockchain της υπολογιστικής πλατφόρμας του Ethereum. Έχουν την δυνατότητα μέσα από το κώδικα τους να παίρνουν αποφάσεις, να συναλλάσσονται και να αποθηκεύουν δεδομένα εφόσον το δίκτυο είναι ενεργό. Οι διάφορες συναλλαγές εκτελούνται μόνο όταν πληρούνται οι όροι που αναγράφονται στο συμβόλαιο. Το 1997, ο Nick Szabo θεωρείται ότι ήταν ο πρώτος που τεκμηρίωσε την θεωρία των Έξυπνων Συμβολαίων μέσα από το άρθρο του «Η Ιδέα των Έξυπνων Συμβολαίων» όπου μέχρι και σήμερα χρησιμοποιείται σαν η κύρια αναφορά στο συγκεκριμένο θέμα. Όπως είναι φανερό, αυτά τα συμβόλαια μπορούν να έχουν πρακτική εφαρμογή σε πολλούς τομείς της σύγχρονής ζωής και ήδη βλέπουμε κάποια δειλά βήματα προς την υλοποίηση τους.
Μέσα από αυτή την μεταπτυχιακή διατριβή θα επικεντρωθούμε κυρίως στους τομείς της ηλεκτρονικής διακυβέρνησης (e-governance) και πως αυτά τα συμβόλαια θα μπορέσουν να λύσουν κάποια βασικά προβλήματα. Ήδη κάποιες χώρες, όπως η Εσθονία έχουν υιοθετήσει πλήρως το μοντέλο της ηλεκτρονικής διακυβέρνησης. Κάποιες άλλες, κάνουν τα πρώτα βήματα , όπως για παράδειγμα την εφαρμογή της ηλεκτρονικής υπογραφής που θα επιτρέψει τις ασφαλείς και γρήγορες συναλλαγές με τις κυβερνητικές υπηρεσίες. Τα έξυπνα συμβόλαια αποσκοπούν να πάρουν ένα βήμα παραπέρα το μοντέλο της ηλεκτρονικής διακυβέρνησης αφού πλέον οι χρήστες θα μπορούν να επισυνάπτουν συμφωνίες με τους αρμόδιους φορείς ,ή ακόμα

και με άλλους συμπολίτες τους. Αυτές οι συμφωνίες θα είναι καταχωρημένες σε ένα κοινό καθολικό (ledger). Με αυτό το τρόπο επιτυγχάνεται ένας προσπελασμός του μεσάζοντα αφού το έξυπνο συμβόλαιο είναι προσβάσιμο κατευθείαν από όλους τους συμβαλλόμενους. Συνεπώς μειώνονται οι πόροι που χρειάζονται και αντιθέτως αυξάνεται η ταχύτητα διεκπεραίωσης μιας συναλλαγής. Όπως θα ήταν αναμενόμενο, η τεχνολογία Blockchain και ειδικότερα η εφαρμογή των έξυπνων συμβολαίων στην ηλεκτρονική διακυβέρνηση δεν θα μπορούσε να είναι και η τελική απάντηση στα θέματα ασφαλείας που ήδη υπάρχουν. Πολλά ερωτήματα τίθενται και η ΤΠΕ καλείται να δώσει τις ανάλογες απαντήσεις. Σε αυτή την εργασία θα προσπαθήσουμε να δούμε ποια προβλήματα ασφαλείας παρουσιάζονται. Πιο συγκεκριμένα θα δούμε κάποια ήδη υπάρχοντα έξυπνα συμβόλαια που έχουν μπει σε εφαρμογή και κατά πόσο αυτά έχουν κάποιες αδυναμίες. Επίσης θα προσπαθήσουμε να προτείνουμε εμείς κάποια έξυπνα συμβόλαια που θεωρούμε ότι θα είχαν πρακτική εφαρμογή στο γενικότερο πλαίσιο της ηλεκτρονικής διακυβέρνησης. Στο τελευταίο κομμάτι της μεταπτυχιακής διατριβής, προτείνεται ένα υβριδικό μοντέλο στο οποίο θα μπορούσε να λειτουργήσει με ασφάλεια μια Έξυπνη Πόλη . Σε αυτό το μοντέλο γίνεται αναφορά στα βασικότερα στοιχεία που αποτελούν τον πυλώνα για την προστασία των προσωπικών δεδομένων και της ασφαλούς διανομής και επεξεργασίας μεγάλου όγκου δεομένων.

Κεφάλαιο 1

Internet of Things (IoT) Μέσα στις Έξυπνες Πόλεις

Όπως έχουμε προαναφέρει στο πρόλογο, οι κοινωνίες μας οδεύουν με γοργούς ρυθμούς στην εποχή του IoT. Η βιβλιογραφία πάνω στο συγκεκριμένο θέμα είναι αρκετά πρόσφατη αφού μόνο τα τελευταία χρόνια βλέπουμε αυτό το περιβάλλον να αποκτά μια υπόσταση και να μην είναι απλά ένα μεγαλεπήβολο έργο σε εξέλιξη ή ακόμα κάποιες μεμονωμένες προσπάθειες από συγκεκριμένες κοινότητες. Με απλά λόγια, το IoT χαρακτηρίζεται ως ένα περιβάλλον όπου καθημερινά αντικείμενα που μέχρι τώρα δεν θεωρούνταν ηλεκτρονικοί υπολογιστές, αρχίζουν να χρησιμοποιούν τις δυνατότητες του διαδικτύου όπου μέσα από την διασύνδεση τους στο ευρύτερο δίκτυο έχουν την δυνατότητα να δημιουργούν, να παράγουν και να καταναλώνουν δεδομένα (Bhasin, Choudhury, Gupta, & Kumar, 2017). Όπως είναι κατανοητό από τον πιο πάνω ορισμό, το IoT θα πρέπει να βασιστεί σε ένα μεγάλο εύρος πρωτοκόλλων, εφαρμογών και τεχνολογιών για να αποφέρει το επιθυμητό αποτέλεσμα που είναι η πραγματική αξία στον άνθρωπο και την κοινωνία. Πιο κάτω παραθέτουμε ένα πίνακα που επεξηγεί τον κύκλο που πραγματοποιεί η διαδικασία από την στιγμή που μία συσκευή ενώνεται στον ευρύτερο δίκτυο μέχρι το σημείο που προσδίδει κάποια αξία προς τον άνθρωπο. Από το πιο κάτω γράφημα είναι σημαντικό να σταθούμε στα σημεία 2,3 και 4. Η καταγραφή, ανάλυση και επεξεργασία των δεδομένων σε πραγματικό χρόνο είναι κάποιες διαδικασίες που οφείλουν να υλοποιούνται σε πολύ μικρό χρονικό διάστημα έτσι ώστε να δίνουν πραγματικό όφελος στον χρήστη. Ας πάρουμε ένα πρακτικό παράδειγμα προς κατανόηση.



1.IoT συνδέσεις και συσκευές
2.Αισθητήρες σύλληψης και αποθήκευση ετικετών
Έμφαση στα δίκτυα, μεταφορά δεδομένων και cloud
Ανάλυση των Big Data και τεχνητή νοημοσύνη
Ανάλυση των εργασιών και API's
Απτά οφέλη για τον άνθρωπο

Σχήμα 1 Ο κύκλος του IoT

Πλέον βλέπουμε ότι τα αυτοκίνητα μπορούν να δεχθούν αλλά και να μεταδώσουν πραγματικά δεδομένα σχετικά με διάφορα περιστατικά που συμβαίνουν κατά τη διάρκεια της πορείας τους στο δρόμο (ατυχήματα, κυκλοφοριακό, κλειστοί δρόμοι κ.α.). Μέσα στο γενικότερο πλαίσιο των έξυπνων πόλεων αυτές οι πληροφορίες αναδιανέμονται σε όλους τους χρήστες που είναι συνδεδεμένοι εκείνη τη χρονική στιγμή στο δίκτυο. Άρα, για να έχει πραγματική αξία η συγκεκριμένη υπηρεσία, θα πρέπει η πληροφορία να φτάνει προς τους άλλους χρήστες μέσα σε πολύ μικρό χρονικό διάστημα. Συνεπώς βλέπουμε ότι η ταχύτητα τόσο της επεξεργασίας αλλά και της διανομής της επεξεργασμένης πληροφορίας είναι μέγιστης σημασίας. Πόσο μάλιστα αν αυτό έχει να κάνει με την ανάλυση Big Data όπου ο χρόνος που θα χρειάζεται θα είναι πολύ μεγαλύτερος. Μέσα από αυτό το παράδειγμα βλέπουμε μερικά από τα διάφορα προβλήματα που καλούνται να λύσουν οι επαγγελματίες του χώρου έτσι ώστε να δώσουν την κατάλληλη ώθηση στο μοντέλο του IoT στις διάφορες εταιρείες για να επενδύσουν. Για να γίνει ακόμα πιο περίπλοκο το συγκεκριμένο θέμα, θα πρέπει να αναφέρουμε ότι οι λύσεις αυτές θα πρέπει να έχουν τέτοιο κόστος που να επιτρέπει την επένδυση σε σχέση με την επιστρεφόμενη αξία. Καθόλου τυχαία γίνεται αναφορά στο The IoT Business Index 2017 του περιοδικού Economist, στους λόγους τους οποίους το IoT δεν βοηθούν την εξέλιξη του από τις ίδιες τις εταιρείες. Συνοπτικά, οι λόγοι είναι οι εξής:

- Το υψηλό κόστος επένδυσης σε νέες τεχνολογίες
- Η έλλειψη ανθρώπινου δυναμικού με τεχνικές γνώσεις σε θέματα IoT

- Ασφάλεια (Unit, 2017)

Το θέμα της ασφάλειας καθαυτό θα το δούμε σε μεταγενέστερο στάδιο αυτής της μεταπτυχιακής διατριβής. Γιατί όμως το κόστος και η έλλειψη ανθρώπινου δυναμικού είναι τόσο σημαντικοί λόγοι για να μην προχωράει με τους κατάλληλους ρυθμούς η υλοποίηση του μοντέλου του IoT; Εδώ είναι σημαντικό να αναφέρουμε ότι οι πιο πάνω λόγοι είναι αλληλένδετοι έως ένα σημείο αφού αν παραγκωνιστεί ένας από αυτούς, τότε ο επόμενος θα είναι η συνέπεια του παραγκωνισμού. Ας δούμε ένα παράδειγμά προς κατανόηση. Πολλές εταιρείες φτιάχνουν ανανεωμένες εκδόσεις των προϊόντων τους έτσι ώστε να είναι έτοιμα να εισαχθούν στον κόσμο του IoT. Σταδιακά γίνεται αντιληπτό ότι αυτό στοιχίζει αρκετά σαν επένδυση από τις εταιρείες. Ταυτόχρονα, οι παλαιότερες εκδόσεις αυτών των προϊόντων είτε θα πρέπει να αντικατασταθούν ή θα πρέπει με κάποιο τρόπο να ενσωματωθούν σε αυτό το μοντέλο. Οι περισσότερες εταιρείες προτιμούν τη δεύτερη επιλογή κυρίως λόγω κόστους. Συνεπώς, στη προσπάθεια να μειωθεί το κόστος, οι μη ειδικά σχεδιασμένες εκδόσεις αυτών των προϊόντων είναι επιρρεπής σε ευπάθειες. Άρα βλέπουμε ότι η ασφάλεια είναι ένας παράγοντας που έχει να παίξει μεγάλο ρόλο στο πως θα υλοποιηθεί το γενικότερο πλάνο που θα κινηθεί ή κάθε εταιρεία πριν τοποθετήσει τα προϊόντα της στη αγορά. Τα μη ανανεωμένα προϊόντα ή ακόμα και τα προϊόντα που δεν έχουν φτιαχτεί ειδικά για το μοντέλο του IoT, θα λειτουργούν σαν ωρολογιακές βόμβες μέσα στο δίκτυο και οι εταιρείες είτε θα πρέπει να επωμισθούν το κόστος απόσυρσης τους, είτε θα πρέπει να πάρουν την ευθύνη σε περίπτωση παραβίασης της ασφάλειας. Όπως αναφέρεται στην έρευνα του Economist σχετικά με τις επιπτώσεις του IoT, πολλές συσκευές που κυκλοφορούν στην αγορά, χρησιμοποιούν πρωτόκολλα και λογισμικά που είναι πεπαλαιωμένα χωρίς να είναι σχεδιασμένα για να είναι IP enabled. Αυτές οι συσκευές μπορούν να βγουν εκτός λειτουργίας μόνο με μια απλή σάρωση του δικτύου (Unit, 2017).

Η πρακτική εφαρμογή του IoT μπορεί να μοιραστεί σε διάφορους τομείς όπως βιομηχανική, καταναλωτική ή εμπορευματοποιημένη χρήση. Για παράδειγμα, η εφαρμογή του IoT σε εμπορευματοποιημένες μονάδες θα βοηθήσει στην δημιουργία μιας καλύτερης εικόνας σχετικά με το supply chain. Πλέον, κάποια εμπορεύματα θα μπορούν να δίνουν πληροφορίες σε πραγματικό χρόνο σχετικά με το φορτίο, το βάρος, τη θερμοκρασία, τον χρόνο άφιξης στο προορισμό και πολλά αλλά. Για το συγκεκριμένο θέμα θα κάνουμε εκτενέστερη αναφορά σε μεταγενέστερο στάδιο αυτής της μεταπτυχιακής διατριβής.

Κάποιες φορές έχουμε και διασταύρωση αυτών των τομέων όπου το βιομηχανικό IoT θα δώσει αποτελέσματα στο καταναλωτικό IoT. Για παράδειγμα η προσαρμογή αυτοκίνητων από τις εταιρείες (βιομηχανικό IoT) για να μπορούν να επεξεργάζονται και να αποστέλλουν δεδομένα της κίνησης μέσα από το δρόμο. Με αυτό το τρόπο θα γίνεται διαχείριση της κίνησης στην πόλη σε πραγματικό χρόνο (καταναλωτικό IoT) (i-scoop.eu, 2017). Όπως είναι εμφανές, ο ρόλος του IoT στην δημιουργία Έξυπνων Πόλεων είναι καθοριστικός και οι εφαρμογές που προκύπτουν είναι απεριόριστες. Απλά αναφέροντας μερικές θα μπορούσαμε να δούμε το IoT να εφαρμόζεται για την δημιουργία Έξυπνων Νοσοκομείων όπου θα δίνονται σε πραγματικό χρόνο πληροφορίες σχετικά με την υγεία των ασθενών, τη διαθεσιμότητα ιατρικών υλικών, αναφορές και ιατρικά δεδομένα ασθενών εκτός ωρών γραφείου και πολλά άλλα. Ήδη υπάρχουν στην αγορά «έξυπνα κρεβάτια» όπου το προσωπικό του νοσοκομείου μπορεί να παίρνει δεδομένα για την κατάσταση των ασθενών (π.χ. διαθέτει αισθητήρες υγρασίας) σε πραγματικό χρόνο ακόμα και σε απομακρυσμένα σημεία εκτός νοσοκομείου (μέσω εφαρμογής κινητού τηλεφώνου). Γενικότερα το κομμάτι της υγείας είναι ένας τομέας που έχει κάνει αρκετά βήματα μέχρι σήμερα για την εναρμόνιση των υφιστάμενων συστημάτων με τις ανάγκες ενός συστήματος υγείας μέσα σε μια Έξυπνη Πόλη .

Ακόμα βλέπουμε οτι το IoT να εφαρμόζεται στην δημιουργία ενός έξυπνου συστήματος διαχείρισης αποβλήτων. Με αυτό το σύστημα, θα διανέμονται τα δεδομένα σχετικά με τη διαθεσιμότητα των σταθμών αποβλήτων, την πορεία των οχημάτων περισυλλογής και για το είδος αποβλήτων που μεταφέρουν (S. Bhasin, 2017). Ήδη κάποιες χώρες, όπως η Δανία ξεκίνησαν να τοποθετούν σε περιοχές Έξυπνους Καλάθους (SmartBins) όπου χρησιμοποιώντας τεχνολογία IoT θα μπορούν να δίνουν πληροφορίες για την στάθμη των αποβλήτων, αύξηση φωτεινότητας σε περίπτωση που κάποιος πλησιάζει προς το σημείο σκυβάλων και άλλες χρήσιμές πληροφορίες που θα συλλέγονται προς ανάλυση σε ήδη εγκατεστημένα λογισμικά. Η Έξυπνη Διαχείριση Αποβλήτων έχει αποκτήσει μια μεγάλη δυναμική τα τελευταία χρόνια αφού τα βασικά πλεονεκτήματα που είναι η αισθητή μείωση του κόστους διαχείρισης και η αύξηση του ποιότητας ζωής και ασφάλειας των κατοίκων είναι βασικοί παράγοντες για να ελκύσουν το ενδιαφέρον επενδυτών (Jung, 2017). Επιπρόσθετα, η εφαρμογή ενός τέτοιου συστήματος εμπεριέχει λιγότερους κίνδυνους ασφάλειας και προστασίας προσωπικών δεδομένων σε αντίθεση με την εφαρμογή ενός έξυπνου συστήματός υγείας που είδαμε πιο πάνω. Αυτό το χαρακτηριστικό το κάνει ακόμα πιο ελκυστικό προς υλοποίηση αφού η διαδικασία και το κόστος εφαρμογής μειώνεται σημαντικά.

1.1 Έξυπνες Πόλεις

Τι ακριβώς είναι μια Έξυπνη Πόλη τελικά και κατά πόσο είναι υλοποιήσιμη στις μέρες μας; Από τα πιο πάνω παραδείγματα είδαμε σε πολύ γενικές γραμμές τις χρήσεις που θα έχει σε ένα σύγχρονο περιβάλλον πόλεως. Σκοπός αυτού του κεφαλαίου είναι να δοθεί μια γενικότερη εικόνα για τις εφαρμογές που μπορεί να έχει η τεχνολογία IoT σε μια Έξυπνη Πόλη παρά να δώσουμε με λεπτομέρεια όλες τις πιθανές χρήσεις. Μιλώντας για Έξυπνες Πόλεις, θα ήταν καλό πρώτα να προσπαθήσουμε να δούμε τι τις ορίζει. Μέσα από διάφορες ακαδημαϊκές μελέτες που έχουν δημοσιευθεί υπάρχουν διάφοροι ορισμοί που προσπαθούν να καθορίσουν την ακριβή ερμηνεία της Έξυπνης Πόλης. Είναι διακριτό ότι είναι αρκετά δύσκολο να αποδοθεί μια ακριβής ερμηνεία για κάτι που εμπεριέχει τόσες πολλές παραμέτρους. Έχουμε ξεχωρίσει την ερμηνεία της IBM (https://www.ibm.com/smarterplanet/us/en/smarter_cities/ overview) μέσα από την παραπομπή της από το Pramanika, 2017. Συγκεκριμένα αναφέρεται ότι Έξυπνη Πόλη είναι η έξυπνη χρήση της προηγμένης τεχνολογίας έτσι ώστε να μπορούν να συλλεγούν, να εξεταστούν , να επεξεργαστούν και να ενσωματωθούν μεγάλοι όγκοι χρήσιμών πληροφορίων κατευθείαν από τις πολείς που είναι ήδη σε λειτουργία. Ο Amjad (2017) αναφέρει ότι οι σημαντικότεροι στόχοι μια Έξυπνης Πόλης είναι η διατήρηση της βιωσημότητας των υπηρεσιών, η βελτίωση της ποιότητας ζωής για τους πολίτες και η δημιουργία ενός κατάλληλου περιβάλλοντος διαβιώσης μέσα στις ίδιες τις πόλεις. Ήδη πολλές πόλεις ξεκίνησαν να υλοποιούν διάφορα προγράμματα προς αυτή τη κατεύθυνση προσπαθώντας να ενεργοποιήσουν τους ανάλογους μηχανισμούς και τις αρμόδιες υπηρεσίες. Όπως γίνεται αντιληπτό, αυτό είναι ένα πολύ δύσκολο εγχείρημα αφού καλούνται να συνεργαστούν διάφοροι φορείς και εταιρείες παροχής υπηρεσιών που ειδικεύονται στην ασφάλεια, τις τηλεπικοινωνίες, την επεξεργασία δεδομένων κ.α. Στο πιο κάτω γράφημα βλέπουμε τους πιο βασικούς τομείς οι οποιοί θα αποτελέσουν το πιο βασικό κορμό των Έξυπνων Πόλεων.

Έξυπνες Πόλεις	
Έξυπνο Εμπόριο	Τραπεζικό σύστημα, Αγορά ακινήτων, Χρηματοοικονομικά
Έξυπνο Περιβάλλον	Διοίκηση αποβλήτων, νερού, ενέργειας
Έξυπνη Διακυβέρνηση	Διακυβέρνηση, Ασφάλεια, Εκπαίδευση, Υγεία
Έξυπνη Επικοινωνία	Επικοινωνίες, Ταυτοποίηση
Έξυπνη Διακίνηση	Συγκοινωνίες, Κυκλοφορία

Σχήμα 2 Βασικοί τομείς Έξυπνων Πόλεων.(Sidra Ijaz, 2016)

Όλοι αυτοί οι φορείς έχουν το δύσκολο έργο να συνεργαστούν με αρμονία μέσα σε ένα ήδη ανεπτύγμένο οικοσύστημα. Μέσα από αυτή τη συνεργασία είναι λογικό να παρουσιαστούν διάφορα προβλήματα και ειδικότερα προβλήματα ασφαλείας. Στις πιο κάτω παραγράφους θα προσπαθήσουμε να εντοπίσουμε τα προβλήματα ασφαλείας που θα προκύψουν μέσα από την εφαρμογή της τεχνολογίας IoT μέσα στις Έξυπνες Πόλεις. Όπως είναι φυσικο, τα προβλήματα δεν θα είναι μόνο σε επίπεδο ασφαλείας, εντουτοίς δεν θα καλύψουμε εις βάθος τους άλλους τομείς που μπορεί να επηρεαστούν.

1.2 Big Data

Ένα από τα βασικότερα ερωτήματα που καλούνται οι ειδικοί να απαντήσουν είναι κατά πόσο η υπάρχουσες τεχνολογίες μπορούν να επεξεργαστούν και να αναλύσουν με την ζητούμενη ταχύτητα τα Big Data. Μέχρι τώρα, κατά κύριο λόγο η συλλογή των δεδομένων γίνεται τοπικά και ο χρήστης μπορεί να τα επεξεργαστεί με τον τρόπο που αρμόζει στις δικές του ανάγκες. Μέσα στις Έξυπνες Πόλεις, αυτά τα δεδομένα θα πρέπει να διανεμηθούν με τέτοιο τρόπο (και ανάλογη ταχύτητα) έτσι ώστε να είναι χρήσιμα για το ευρύτερο κοινό. Έχουμε δει πιο πάνω το παράδειγμα της οδήγησης μέσα στις Έξυπνες Πόλεις. Ας φανταστούμε μια καθυστέρηση στην επεξεργασία δεδομένων από το σύστημα που θα ελέγχει τις διαβάσεις και τα φανάρια κυκλοφορίας. Σε μια πόλη του μεγέθους του Λονδίνου θα είναι αρκετό για να φέρει σε

απόγνωση και κίνδυνο εκατομμύρια ανθρώπους. Για να το κάνουμε ακόμα πιο περίπλοκο, θα πρέπει να βάλουμε στην εξίσωση και το γεγονός ότι οποιαδήποτε τεχνολογία χρησιμοποιηθεί για να την επεξεργασία των Big Data δεν θα πρέπει να θέτει σε αμφισβήτηση τους τρεις βασικού πυλώνες της ασφάλειας που είναι η εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα. Από το 2001 έχει αναπτυχθεί από τον (Laney, 2001) μοντέλο των τριών V για το Big Data. Τα τρία V έχουν να κάνουν με την ποσότητα (volume), την ποικιλία (variety) και την ταχύτητα (velocity) των δεδομένων που καλούνται οι έξυπνες πόλεις να διαχειριστούν. Με πιο απλά λόγια, μια Έξυπνη Πόλη θα πρέπει να μαζέψει, να επεξεργαστεί και να αναλύσει σε μεγάλες ταχύτητες μια τεράστια ποσότητα δεδομένων τα οποία θα προέρχονται από μια πληθώρα πηγών.

Όπως είναι λογικό η επεξεργασία σε πραγματικό χρόνο ενός μεγάλου όγκου δεδομένων επιφέρει αρκετούς κινδύνους ασφαλείας. Οι αιτίες αυτών των κινδύνων είναι η έλλειψη εργαλείων για να γίνει η σωστή επεξεργασία του όγκου των δεδομένων, τα προβλήματα που μπορεί να δημιουργήσουν οι μεγάλες δημόσιες βάσεις δεδομένων και ο συνεχείς διαμοιρασμός δεδομένων μεταξύ τρίτων (Sidra Ijaz, 2016). Ακόμα και σε τομείς που η τεχνολογία είναι έτοιμη να υποστηρίξει τις ανάγκες μιας Έξυπνης Πόλης, υπάρχει έλλειψη τεχνογνωσίας από πλευράς ανθρώπινου δυναμικού. Συνεπώς το πρόβλημα μεγεθύνεται αφού τα λάθη και οι παραλείψεις που μπορεί να αποφέρουν διαρροή ευαίσθητων δεδομένων λόγω κακής φύλαξης ή χειρισμού των δεδομένων αυξάνονται. Σχετικά με τον διαμοιρασμό δεδομένων μεταξύ τρίτων (third parties), οι λόγοι που μπορεί να δημιουργήσουν προβλήματα ασφαλείας μπορεί να είναι η μη συμβατότητα των λογισμικών ή των βάσεων δεδομένων. Όπως ξέρουμε, μέχρι σήμερα, ο κάθε φορέας είναι υπόλογος για τον τρόπο που κρατάει και διανείμει τα ευαίσθητα δεδομένα που χειρίζεται. Μέσα από τις Έξυπνες Πόλεις πολλές υπηρεσίες θα πρέπει να ανταλλάξουν δεδομένα με μεγάλες ταχύτητες. Κάποιες από αυτές τις υπηρεσίες ίσως χρησιμοποιούν τεχνολογίες που να μην είναι συμβατές ή ακόμα και ελεγμένες σε θέματα ασφαλείας. Αυτή η μη συμβατότητα μπορεί να επιφέρει αρκετούς κινδύνους σε θέματα ιδιωτικότητας του τελικού χρήστη. Ας πάρουμε το παράδειγμα ενός ιδιωτικού νοσοκομείου όπου δεν χρησιμοποιεί την ανάλογη τεχνολογία για να μεταφέρονται τα δεδομένα των ασθενών του με την σωστή κρυπτογράφηση. Αυτά τα δεδομένα θα πρέπει να «ταξιδέψουν» προς τα φαρμακεία που θα κληθούν να δώσουν την ανάλογη φαρμακευτική περίθαλψη στους ασθενείς αλλά ταυτόχρονα να ενημερώσει την βάση δεδομένων του Υπουργείου Υγείας. Κατά το πρώτο κομμάτι αυτής της πορείας της πληροφορίας, δημιουργούνται θέματα εμπιστευτικότητας της

πληροφορίας. Αφού η επικοινωνία μεταξύ των τρίτων δεν είναι κρυπτογραφημένη, θα μπορούσε εν δυνάμει να υποκλαπεί από μια κακόβουλη επίθεση. Ειδικότερα όσον αφορά τα θέματα του ιδιωτικού απορρήτου, ο Ballesté, et al (2013) αναλύει το μοντέλο του απορρήτου των πέντε διαστάσεων (5D) μέσα στις Έξυπνες Πόλεις. Αυτά τα πέντε σημεία που καλείται η κοινότητα της (ΤΠΕ) να διαφυλάξει είναι το απόρρητο της ιδιωτικότητας, το απόρρητο τη αναζήτησης (query), της τοποθεσίας, το απόρρητο του ίχνους (footprint) και το απόρρητο της ιδιοκτησίας. Εάν αυτό το μοντέλο ακολουθηθεί, τότε οι συγγραφείς ισχυρίζονται ότι οι Έξυπνες Πόλεις θα μπορούν να θεωρούνται ενημερωμένες στο συγκεκριμένο θέμα. Όταν μιλάμε για ένα συνονθύλευμα υπηρεσιών, ιδρυμάτων και επιχειρηματικών δραστηριοτήτων, τότε είναι λογικό να αναμένονται διάφορές τεχνικές αποκλίσεις όσον αφορά τον τρόπο εφαρμογής και αντίληψης της ασφάλειας. Είναι ήδη γεγονός ότι διάφορα προϊόντα (hardware ή λογισμικά) αναπτύσσονται με σκοπό να χρησιμοποιηθούν μέσα στις Έξυπνες Πόλεις, εντούτοις δεν έχουν επαρκή έλεγχο από τους κατασκευαστές σε θέματα ασφαλείας.

Συνοψίζοντας, οι Έξυπνες Πόλεις έχουν σαν κύριο ρόλο να δώσουν λύσεις σε καίρια παγκόσμια προβλήματα όπως η κλιματική αλλαγή, αστυφιλία, οι περιορισμένοι πόροι και η ψηλή πληθυσμιακή ανάπτυξη (AlDairi, 2017). Εντούτοις, δημιουργούνται αρκετές προκλήσεις σε θέματα ασφαλείας. Σε γενικές γραμμές θα μπορούσαμε να περιοριστούμε στα παρακάτω:

- Η έλλειψη τεχνολογιών που θα μπορούν να επεξεργαστούν και να αναλύσουν με ταχύτητα μεγάλο όγκο ποικίλων δεδομένων. Όπως είδαμε και πιο πάνω, το μοντέλο των τριών V είναι ένας βασικός πυλώνας των Έξυπνων Πόλεων ο οποίος πρέπει να εφαρμοστεί χωρίς να μπαίνει σε αμφισβήτηση το θέμα της ασφάλειας.
- Η εφαρμογή του IoT μέσα στις Έξυπνες Πόλεις θα επιφέρει μεγάλη συσσώρευση υπηρεσιών, εφαρμογών και συνδεδεμένων κόμβων. Όλα αυτά τα στοιχεία θα φέρουν στην επιφάνεια ανομοιογένεια στον τρόπο λειτουργείας τους που ίσως δημιουργήσει αρκετά κενά ασφαλείας.
- Η έλλειψη καθορισμένων προτύπων ασφαλείας είναι ένα στοιχείο που ήδη απασχολεί τους ειδικούς. Αυτή τη στιγμή δεν υπάρχει ένα γενικότερο πλαίσιο ασφαλείας που θα πρέπει να ακολουθείται έτσι ώστε να διασφαλίζεται σωστή διακίνηση , αποθήκευση και επεξεργασία δεδομένων. Ο κάθε συμβαλλόμενος κρίνει κατά το δοκούν τους τρόπους που θα πράξει τα παραπάνω. Όπως είναι φυσικό, κάποιοι δίνουν προτεραιότητα στην ασφάλεια, αλλά πολλοί άλλοι προτιμούν να κάνουν συμβιβασμούς διακινδυνεύοντας να δημιουργήσουν κενά ασφαλείας.

Στο επόμενο κεφάλαιο θα δούμε αναλυτικά την τεχνολογία του Blockchain και κατά πόσο αυτή θα μπορέσει να δώσει λύσεις στα πιο πάνω ζητήματα ασφαλείας που προκύπτουν από την λειτουργία των Έξυπνων Πόλεων. Η συγκεκριμένη τεχνολογία έχει γίνει ευρύτερα γνωστή μέσα από την άνοδο της δημοσιότητας των cryptocurrencies, πάραυτα εμείς θα προσπαθήσουμε να επικεντρωθούμε στο τρόπο λειτουργίας του συγκεκριμένου μοντέλου.

Κεφάλαιο 2

Η Τεχνολογία Blockchain στις Έξυπνες Πόλεις

Όπως προαναφέραμε στο πρόλογο αυτής της μεταπτυχιακής διατριβής, η τεχνολογία Blockchain έχει γίνει σημείο αναφοράς σαν μια πιθανή λύση στα προβλήματα ασφαλείας που δημιουργούνται από την υλοποίηση και εφαρμογή του IoT στις έξυπνες πόλεις. Σύμφωνα με τον Nelson Rosario της Marshall Gerstein & Borun LLP, Blockchain είναι ένα δίκτυο διανεμημένων καταλόγων (distributed ledger) που χρησιμοποιεί κρυπτογράφηση δημόσιου κλειδιού για να υπογράφει κρυπτογραφικά τις συναλλαγές που είναι αποθηκευμένες σε διανεμημένους καταλόγους. Οι κατάλογοι αποτελούνται από κρυπτογραφικά συνδεδεμένα τμήματα (blocks) συναλλαγών. Τα κρυπτογραφικά συνδεδεμένα τμήματα συναλλαγών σχηματίζουν αυτό που είναι γνωστό ως "Blockchain" (Rosario, 2017). Πιο απλά θα μπορούσαμε να το σκεφτούμε σαν ένα υπολογιστικό φύλλο (spreadsheet) όπου είναι προσβάσιμο από κάθε υπολογιστή που είναι μέσα στο δίκτυο. Αυτό το φύλλο κρατάει αρχείο από όλες τις συναλλαγές που κάνουν οι υπολογιστές. (Summers, 2017)

2.1 Blockchain

Για να δούμε τι θα αλλάξει η εφαρμογή της τεχνολογίας Blockchain χρησιμοποιούμε ένα απλό καθημερινό παράδειγμα πληρωμής μέσω κάρτας. Ας υποθέσουμε ότι ο Α πάει να πληρώσει με την κάρτα του τον Β. Ουσιαστικά εξουσιοδοτεί την τράπεζα του να αναζητήσει στους καταλόγους της (στη βάση δεδομένων) κατά πόσο ο Α έχει το ποσό που καλείται να πληρώσει. Εφόσον το ποσό είναι διαθέσιμο στο λογαριασμό του Α, τότε η τράπεζα καλείται να στείλει τα λεφτά στον Β για να κλείσει ο κύκλος της συναλλαγής. Ο Β θα πληρωθεί άμεσα από την τράπεζα και έμμεσα από τον Α. Με την τεχνολογία του Blockchain, η πληροφορία κατά πόσο

ο Α έχει διαθέσιμο το ποσό στον λογαριασμό του θα είναι διανεμημένη σε όλους τους ενδιαφερόμενους με την μορφή κρυπτογραφημένων τμημάτων (blocks). Έτσι, με την ανταλλαγή κλειδιών μεταξύ των ενδιαφερομένων έτσι ώστε να γίνει η αυθεντικοποίηση τους, η συναλλαγή μπορεί να πραγματοποιηθεί χωρίς την παρέμβαση του τρίτου μέλους, που σε αυτή τη περίπτωση είναι η τράπεζα. Με αυτό το τρόπο υπάρχει η πεποίθηση ότι η εξάλειψη της ανάγκης ενός τρίτου μέρους στη πραγματοποίηση μιας συναλλαγής θα έχει ως αποτέλεσμα ταχύτερες και λιγότερο δαπανηρές συναλλαγές με μεγαλύτερη διασφάλιση της ιδιωτικότητας (Schutzer, 2016).

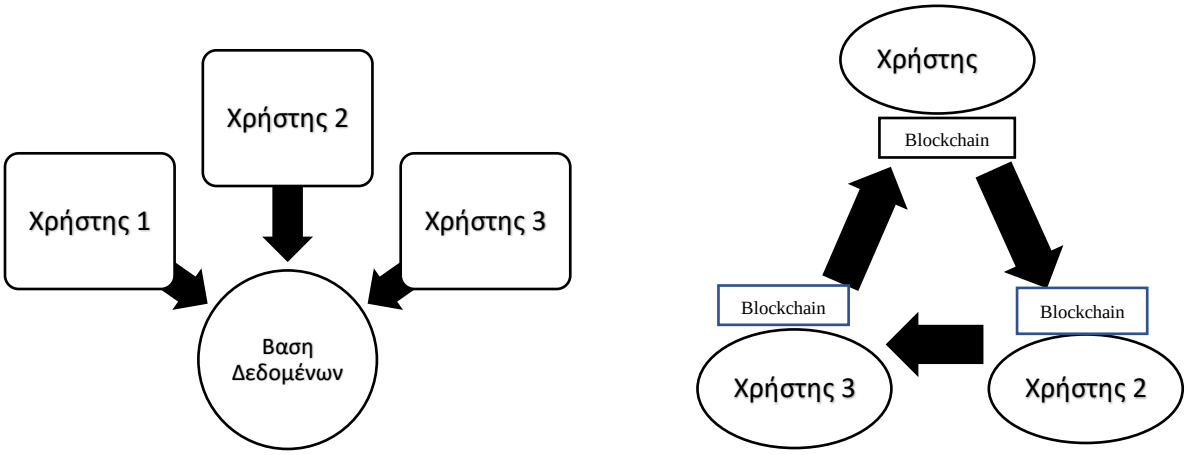
Πριν δούμε τις εφαρμογές που μπορεί να έχει αυτή η τεχνολογία, θα ήταν καλό να γίνει μια πιο εμπεριστατωμένη ανάλυση του τρόπου που λειτουργεί. Η διαδικασία έχει ως εξής:

- Κάποιος χρήστης ζητάει να διεκπεραιωθεί μια συναλλαγή.
- Η συγκεκριμένη συναλλαγή αναμεταδίδεται στο ευρύτερο δίκτυο όπου εκεί βρίσκονται συνδεδεμένοι διάφοροι κόμβοι.
- Η συναλλαγή επικυρώνεται από τους διάφορους κόμβους με την χρησιμοποίηση γνωστών αλγορίθμων. Πιο συγκεκριμένα, ένας κόμβος καλείται να λύσει ένα μαθηματικό πρόβλημα και το επιτυγχάνει με την επεξεργασία των δεδομένων που βρίσκονται μέσα στο block. Αυτά ονομάζονται μοναδικά μεταδεδομένα επικεφαλίδας (unique header metadata). Η διαδικασία επικύρωσης ονομάζεται εξόρυξη (mining) και είναι ίσως το πιο σημαντικό κομμάτι της διαδικασίας για τη υλοποίηση του Blockchain.
- Αφού ένας κόμβος καταφέρει να επιλύσει το πρόβλημα, αυτό θα πρέπει να επικυρωθεί/εγκριθεί από άλλους κόμβους.
- Οι κόμβοι που έκαναν την επικύρωση της συναλλαγής ανταμείβονται με ψευδονομισματα (cryptocurrency).
- Αφού επικυρώθηκε η συναλλαγή, τότε αναμειγνύεται με άλλες ήδη επικυρωμένες συναλλαγές και διαμορφώνουν ένα block το οποίο προστίθεται στο Blockchain. Το block αυτό είναι συνδεδεμένο με το προηγούμενο. Η σύνδεση γίνεται με την αξία hash του προηγούμενου block. Αντίστοιχα, το επόμενο block θα δεθεί με δημιουργημένο και ούτω καθεξής. Με αυτό το τρόπο δημιουργείται μια αλυσίδα από blocks, εξού και η ονομασία Blockchain.
- Η συναλλαγή έχει ολοκληρωθεί και όλοι οι κατάλογοι έχουν ενημερωθεί με την νέα πληροφορία.

2.1.1 Τι προσφέρει

Ο ιδιαίτερος τρόπος που δημιουργεί και καταγράφει τα δεδομένα η τεχνολογία του Blockchain έχει επιφέρει αλλαγές στο τομέα της ασφάλειας. Όπως εξηγήθηκε πιο πάνω, η σύνδεση των blocks με χρονολογική σειρά, και το γεγονός του ότι κάθε συναλλαγή πρέπει να επικυρωθεί από την πλειοψηφία των κόμβων κάνει το Blockchain αρκετά ελκυστικό αφού επιλύει κάποια από τα βασικά προβλήματα ασφαλείας που υπήρχαν μέχρι τώρα. Πιο κάτω περιγράφονται τα πιο βασικά πλεονεκτήματα που έχουν σημειωθεί.

Με την εφαρμογή του Blockchain, μειώνονται οι πιθανότητες να εμφανιστεί η ευπάθεια του single point of failure αφού πλέον η πληροφορία δεν είναι αποθηκευμένη σε ένα μόνο σημείο. Για να μπορέσει ένα hacker να αλλοιώσει το υπόλοιπο ενός τραπεζικού λογαριασμού, θα πρέπει να το κάνει περίπου στο 50% των λογαριασμών μέσα στο δίκτυο. Όλοι οι κόμβοι έχουν πρόσβαση στο block που περιέχει την πληροφορία που επιχειρείται να αλλοιωθεί και έτσι η οποιαδήποτε παρεκτροπή από τα αυθεντικά δεδομένα θα είναι άμεσα αναγνωρίσιμή. Στους τρόπους φύλαξης τραπεζικών δεδομένων χωρίς την τεχνολογία του Blockchain, η πρόσβαση στη βάση δεδομένων της τράπεζας που διατηρεί τον λογαριασμό του ο χρήστης, θα ήταν αρκετή για να αλλοιώσει κάποια δεδομένα π.χ. την αφαίρεση ενός χρηματικού πόσου. Στο σχήμα 4 βλέπουμε την αντίθεση που υπάρχει στους δύο διαφορετικούς τρόπους που κατακρατούνται και διανέμονται τα δεδομένα. Στην συμβατική πρόσβαση που χρησιμοποιείται κατά κόρον στις μέρες μας, υπάρχει μια εξάρτηση προς τη βάση δεδομένων και η οποιαδήποτε αδυναμία της καθιστά τη πρόσβαση στα δεδομένα προβληματική. Αντιθέτως, με την τεχνολογία Blockchain, ο κάθε χρήστης έχει το δικό του αντίτυπο της βάσης δεδομένων.



Σχήμα 3 Συμβατική πρόσβαση σε βάση δεδομένων και πρόσβαση με Blockchain

Μια άλλη λύση που μπορεί να δώσει το Blockchain είναι στη προστασία των προσωπικών δεδομένων. Είναι γεγονός στις μέρες μας να γίνεται η μεταπώληση των προσωπικών δεδομένων από τη μια εταιρεία στην άλλη για τη χρήση τους σε δευτερεύουσες διεργασίες. Πολλοί χρήστες είναι ενάντια σε αυτές τις πρακτικές αφού έχουν αμφιβολίες για τον τρόπο μεταβίβασης των δεδομένων τους μεταξύ των εμπλεκομένων όπως επίσης και για τους τρόπους φύλαξης τους. Με την χρήση της τεχνολογίας Blockchain τα προσωπικά δεδομένα θα μπορούν να ανακτηθούν από τους διανεμημένους καταλόγους μόνο με την σύμφωνη γνώμη του χρήστη. Το συγκεκριμένο τμήμα που κρατάει την πληροφορία θα είναι κρυπτογραφημένο και ο μόνος τρόπος αποκρυπτογράφησης του θα είναι η ανταλλαγή των δημοσιών κλειδιών μεταξύ των δύο μερών (Kshentri, 2017).

Σημαντική θα είναι η συνεισφορά του Blockchain στη ψηφιακή πιστοποίηση ατόμων και οργανισμών το οποίο θα κατά πολύ τις συναλλαγές μεταξύ δυο ή περισσότερων μερών. Αναφέραμε στο κομμάτι των Έξυπνων Πόλεων την σημαντικότητα της ταχύτητας και την αποφυγή της συμφόρησης μέσα στον ωκεανό δεδομένων που ονομάζεται Big Data. Με τον συμβατικό τρόπο αυθεντικοποίησης προσώπων και εγγράφων, ο χρήστης είναι υποχρεωμένος να ζητήσει τη βοήθεια από ένα εγκεκριμένο τρίτο μέρος για να επικυρώσει τη γνησιότητα του εγγράφου. Αυτό το τρίτο μέρος μπορεί να είναι είτε ένας συμβολαιογράφος, μια ελεγκτική εταιρεία, μια δημόσια υπηρεσία κ.α. Χρησιμοποιώντας την τεχνολογία Blockchain όλα τα

επίσημα έγγραφα μπορούν να υπογραφούν ψηφιακά και να επικυρωθούν από τις αρμόδιες υπηρεσίες, όπου στη συνέχεια θα τοποθετηθούν στην διανεμημένη βάση δεδομένων. Έτσι, τα συνδιαλλαζόμενα δυο μέρη, μπορούν να ανταλλάξουν έγγραφα χωρίς την ανάγκη να φέρουν και τρίτο μέρος για να επικυρώσει την αυθεντικότητα τους (Minelli, 2017). Ένα καλό παράδειγμα κατανόησης της χρήσης της ψηφιακής υπογραφής είναι το παράδειγμα της ηλεκτρονικής διακυβέρνησης που εφαρμόζεται στην Εσθονία. Η λύση της ψηφιακής υπογραφής έχει βρει εφαρμογή και σε άλλες χώρες παρόλα αυτά η Εσθονία θεωρείται από τους πρωτοπόρους στην εισαγωγή της στη δημόσια ζωή. Σε ένα από τα επόμενα κεφάλαια θα δούμε με περισσότερη λεπτομέρεια τι ακριβώς έχει εφαρμοστεί και κατά πόσο πρακτικά έχει ωφελήσει την καθημερινότητα των πολιτών.

Όπως περιγράψαμε στον τρόπο λειτουργίας του Blockchain, για να δημιουργηθεί μια συναλλαγή, θα πρέπει να επικυρωθεί από την πλειοψηφία των κόμβων μέσα στο δίκτυο. Πιο συγκεκριμένα, όταν δημιουργείται ένα block πρέπει να επιλυθεί ένα μαθηματικό πρόβλημα το όποιο ονομάζεται απόδειξη εργασίας (Proof of Work). Ακολούθως, το block αναμεταδίδεται στο υπόλοιπο δίκτυο προς επικύρωση. Αυτός ονομάζεται μηχανισμός συναίνεσης (consensus mechanism). Με τον μηχανισμό συναίνεσης επιτυγχάνεται η αξιοπιστία και η συνέπεια της συγκεκριμένης συναλλαγής (Xiaoqi, Peng, Ting, Xiapu, & Qiaoyan, 2017). Η διαδικασία έρχεται σε αντίθεση με τον τρόπο που ενημερώνεται μια συμβατική βάση δεδομένων. Οι χρήστες δεν έχουν καμία ανάμειξη στον τρόπο διαχείρισης της βάσης, πόσο μάλλον στον τρόπο που δημιουργούνται οι διάφορες συναλλαγές. Συνεπώς, βλέπουμε ότι δεν υπάρχει μια ομοιογένεια στα δεδομένα και οι χρήστες είναι υποχρεωμένοι να δείχνουν εμπιστοσύνη στο τρίτο μέρος που διαχειρίζεται τη βάση ως προς την εγκυρότητα και αξιοπιστία των δεδομένων.

Ίσως η πιο σημαντική καινοτομία που προσφέρει η τεχνολογία του Blockchain, είναι η δυνατότητα δημιουργίας και αποθήκευσης έξυπνων συμβολαίων (smart contracts). Το ψευδονόμισμα Bitcoin είναι η πιο γνωστή εφαρμογή που χρησιμοποιεί το Blockchain. Με προπύργιο την σχέση που αναπτύχθηκε μεταξύ Blockchain και Bitcoin, έχουν δημιουργηθεί παρόμοιες αποκεντρωμένες πλατφόρμες και ψευδονομίσματα όπως είναι το Etheruem (η πλατφόρμα) και το Eth (το ψευδονόμισμα). Το Etheruem είναι αμιγώς βασισμένο στην τεχνολογία του Blockchain. Η διαφορά του με το Bitcoin είναι στο ότι το Bitcoin έχει δημιουργηθεί μόνο για να καταγράφει συναλλαγές και να έχει την ιδιότητα του

ψευδονομίσματος (Summers, 2017). Επιπρόσθετα, το Etheruem έχει την ευχέρεια να διεκπεραιώσει Έξυπνα Συμβόλαια. Με απλά λόγια, τα έξυπνα συμβόλαια είναι πρωτόκολλα ψηφιακών συναλλαγών που είναι αποθηκευμένα στο Etheruem Blockchain (Minhaj & Khaled, 2017). Τα Έξυπνα Συμβόλαια μπορούν να συμφωνηθούν χωρίς να επικυρωθούν από κάποιο αρμόδιο τρίτο μέρος (π.χ. συμβολαιογράφο). Η δημιουργία τους είναι άμεση από μηχανή προς μηχανή (machine to machine) το οποίο καθιστά άνευ αντικειμένου την ανάγκη για ένα τρίτο μέρος. Σε μεταγενέστερο κεφάλαιο θα δούμε κάποια παραδείγματα από έξυπνα συμβόλαια τα οποία είναι ήδη καταχωρημένα στο Ethereum Blockchain.

2.1.2 Μειονεκτήματα

Η τεχνολογία του Blockchain έχει δώσει αρκετές ελπίδες στην ευρύτερη κοινότητα της ΤΠΕ στο ότι έρχεται να δώσει λύσεις στα διάφορα θέματα ασφάλειας, αποθήκευσής και επεξεργασίας δεδομένων. Παρόλα αυτά δεν θεωρείται πανάκεια αφού ήδη έχουν αρχίσει να διαφαίνονται κάποια μειονεκτήματα τα οποία πρέπει να αντιμετωπιστούν. Μία πρώτη ματιά δείχνει τον δισταγμό των διαφόρων βιομηχανιών στο να επενδύσουν στην κατάλληλη υποδομή που θα βοηθήσει στην υιοθέτηση του Blockchain. Οι λόγοι είναι διάφοροι και λίγο πιο κάτω θα κάνουμε μια αναφορά στα πιο βασικά μειονεκτήματα που έχουν διαφανεί.

Το γεγονός του ότι η τεχνολογία αυτή βρίσκεται σε πρώιμο στάδιο είναι ένας λόγος δισταγμού για πολλές βιομηχανίες. Μέχρι στιγμής δεν έχει δοκιμαστεί σοβαρά σε συνθήκες πραγματικής οικονομίας και επιχειρήσεων έτσι ώστε να θεωρείται μια αξιόπιστη λύση (Nikhil, 2017). Η χρήση που έχει γίνει είναι σποραδική και συνεπώς αρκετοί μεγάλοι οργανισμοί, οι οποίοι συνήθως δείχνουν το δρόμο στην ευρύτερη αγορά, βλέπουν με διστακτικότητα την υιοθέτηση της τεχνολογίας. Υπάρχει μια γενικότερη δυναμική γύρω από τις δυνατότητες του Blockchain αλλά μέχρι στιγμής είναι σε ακαδημαϊκό επίπεδο και αναμένουμε να το δούμε σε πρακτική εφαρμογή άμεσα.

Ένα άλλο μειονέκτημα που έχει καταγράφει είναι η υπολογιστική ισχύ που χρειάζεται για να μετατραπεί μια συναλλαγή σε block για να μπορέσει να προστεθεί στο Blockchain (σημ. η διαδικασία του mining η οποία έχει εξηγηθεί πιο πάνω). Υπολογίζεται ότι για μια απλή συναλλαγή Bitcoin χρειάζεται 5,000 φορές περισσότερη ενεργεία από την διεκπεραίωση μιας συναλλαγής με πιστωτική κάρτα Visa. Για αυτό το λόγο αρκετοί miners άρχισαν να

χρησιμοποιούν ολοκληρωμένα κυκλώματα, ειδικά για εφαρμογές (application-specific integrated circuits- ASICs) τα οποία δουλεύουν εξολοκλήρου για τον σκοπό αυτό. Επίσης πρέπει να προσμετρηθεί και το γενικότερο οικονομικό κόστος αφού η ηλεκτρική ενέργεια που καταναλώνεται είναι κατά πολύ αυξημένη. Υπολογίζεται ότι μέχρι το 2020 η ηλεκτρική ενέργεια που θα χρειάζεται για τις συναλλαγές των bitcoin θα είναι ίση με την ηλεκτρική ενέργεια η οποία καταναλώνεται στη Δανία (Ameer, 2017). Στην προσπάθεια να βρεθεί μια λύση πάνω στο συγκεκριμένο θέμα, η πλατφόρμα του Etheruem, έχει εντάξει τον αλγόριθμό της «απόδειξής συμμετοχής» (Proof of Stake) σε αντίθεση με τη «απόδειξή εργασίας» που χρησιμοποιείται. Με απλά λόγια, αντί οι miners να μπαίνουν σε μια διαμάχη για το ποιος θα κάνει την εξόρυξη, η ίδια η πλατφόρμα θα κάνει ανάθεση την διεργασία σε συγκεκριμένους χρήστες με βάση το αποθεματικό τους σε Ether που είναι το κρυπτονόμισμα του Ethereum (Peter, 2017). Η βασική διαφορά της απόδειξης συμμετοχής με την απόδειξη εργασίας είναι ότι στη δεύτερη ο miner δεν ανταμείβεται με κάποιο block αλλά παίρνει ως αντάλλαγμα το τέλος της συναλλαγής (transaction fee). Για αυτό το λόγο οι miners αυτού του είδους ονομάζονται «απατεώνες» (forgers) (Ameer, 2017).

Μια άλλη παράμετρος που λαμβάνεται υπόψη στα μειονεκτήματα του Blockchain λόγω του μηχανισμού συναίνεσης (consensus mechanism) είναι η ταχύτητα επικύρωσης μιας συναλλαγής. Με τον συγκεντρωτικό τρόπο δομής μιας βάσης δεδομένων, αρκεί η συναίνεση του διαχειριστή για να καταχωρηθεί μια συναλλαγή. Αυτό δημιουργεί προβλήματα όπως κίνδυνοι του single point failure, ακεραιότητας κλπ. τα οποία είδαμε σε προηγούμενο κεφάλαιο. Αντιθέτως, η τεχνολογία του Blockchain αξιώνει ότι μπορεί να εξαλείψει αυτές τις ευπάθειες, παρόλα αυτά η ανάγκη για επικύρωση μια συναλλαγής από τουλάχιστόν τους μισούς κόμβους που υπάρχουν στο δίκτυο μειώνει κατά πολύ την ταχύτητα δημιουργίας ή ενημέρωσης ενός block. Η μετάβαση από τον αλγόριθμο Proof of Work στο Proof of Stake, θεωρητικά θα μειώσει αισθητά τον χρόνο που χρειάζεται για να επικυρωθεί μια συναλλαγή και να δημιουργηθεί ένα block. Πιο συγκεκριμένα, με τη μέθοδο του Proof of Work εκτιμάται ότι χρειάζονται περίπου 10 λεπτά για την δημιουργία ενός block. Αυτή η περίοδος γίνεται προσπάθεια να μειωθεί στα 12 δευτερόλεπτα (Summers, 2017). Φυσικά ακόμα και αυτός ο χρόνος είναι αρκετά μακριά από τα επιθυμητά επίπεδα για να μπορέσουν να προσπεραστούν τα θέματα αμεσότητας στη πρόσβαση, επεξεργασία και διανομή της πληροφορίας μέσα στο περιβάλλον των έξυπνων πόλεων όπως αναφερθήκαμε σε προηγούμενο κεφάλαιο.

Ένα άλλο μειονέκτημα που φαίνεται να κερδίζει έδαφος ανάμεσα στους σκεπτικιστές του Blockchain είναι αυτό που ονομάζεται «η επίθεση του 51%» (the 51% attack). Ό ίδιος ο Satoshi Nakamoto (ή ίδια, αφού δεν ξέρουμε την πραγματική ταυτότητα του συγκεκριμένου προσώπου) αναφέρει στο κείμενο που θεωρείται το προπύργιο για την δημιουργία του Bitcoin ότι η μεθοδολογία του Proof of Work καθιστά υπολογιστικά αδύνατο για έναν επιτιθέμενο να μεταποιήσει μια συναλλαγή εφόσον η πλειοψηφία των κόμβων που κατέχουν την υπολογιστική δύναμη στο δίκτυο είναι γνήσιοι (honest) (Nakamoto, 2008). Ειδική αναφορά πρέπει να γίνει στη προϋπόθεση ότι οι κόμβοι που έχουν την πλειοψηφία «είναι γνήσιοι». Τι θα μπορούσε να συμβεί αν κάποιος κακόβουλος χρήστης κατάφερνε να ελέγχει την πλειοψηφία των κόμβων; Με αυτό το τρόπο εξηγείται η επίθεση του 51%. Μια λανθασμένη πληροφορία θεωρείται σωστή εφόσον η πλειοψηφία των ατόμων (στη περίπτωση μας κόμβων) συμφωνεί και την αποδέχεται. Πρέπει να σημειωθεί ότι πρακτικά είναι μια πολύ δύσκολη επίθεση αφού η δύναμη εξόρυξης (mining power) που χρειάζεται για ελεγχθούν τόσοι πολλοί κόμβοι είναι αρκετά μεγάλη.

2.1.3 Χρήσεις του Blockchain

Το Blockchain επιδέχεται αρκετής κριτικής λόγω της άμεσης σύνδεσης του με τα διάφορα κρυπτονομίσματα (cryptocurrencies) ωστόσο τα τελευταία χρόνια έχει καταφέρει να απεμπλακεί αφού άρχισαν να διαφαίνονται οι χρήσεις του σε άλλους τομείς πέρα από τους χρηματοοικονομικούς. Αν και έχουν περάσει δέκα χρόνια από τα πρώτα βήματα έρευνας και ανάπτυξης της τεχνολογίας του Blockchain, εντούτοις μόλις την τελευταία τριετία ξεκινήσαμε να βλέπουμε τα πρώτα δειλά σημάδια εφαρμογής της. Όπως περιγράφει ο Vinay Gupta, περίπου πριν 10 χρόνια (το 2009) εμφανίζεται το πρώτο κρυπτονόμισμα (bitcoin) που είναι βασισμένο την τεχνολογία του Blockchain. Λίγο μετά, γίνεται μια προσπάθεια να ξεχωρίσει το Blockchain από το Bitcoin και να ανευρεθούν χρήσεις της τεχνολογίας αυτής σε άλλους τομείς (Gupta, 2017). Υπολογίζεται ότι μέσα στο 2017, το 15% των τραπεζών θα χρησιμοποιούν τη τεχνολογία του Blockchain. Οι χρήσεις που προορίζονται πάνω σε αυτό είναι κυρίως σε θέματα δανεισμού, πληρωμές τραπεζικών προϊόντων λιανικής (retail payments) και δεδομένων αναφοράς (Shen, 2016).

Η διαφάνεια είναι ένα σημαντικό στοιχείο το οποίο αναζητά η αγορά αυτή τη στιγμή και το Blockchain είναι σε θέση να δώσει λύσεις σε αυτό το θέμα. Η ιδιαιτερότητα του Blockchain σε σχέση με τις υπάρχουσες τεχνολογίες είναι η δυνατότητα που παρέχει να δίνει πληροφορίες για το κάθε κομμάτι του supply chain κατευθείαν από τους εμπόρους, τους διανομείς και του προμηθευτές στον τελικό καταναλωτή. Οι παραδοσιακές τεχνολογίες που χρησιμοποιούνται εναπόκεινται στη διανομή της πληροφορίας κατευθείαν από τον ιδιοκτήτη τους προϊόντος πριν φτάσει στον καταναλωτή. Για παράδειγμα, η εταιρεία που εμπορεύεται κρέας είναι υποχρεωμένη να ενημερώσει τους καταναλωτές για την προέλευση του κρέατος και τις συνθήκες φύλαξης του μέχρι να φτάσει στον τελικό προορισμό που είναι το τραπέζι του καταναλωτή. Αυτό εμπλέκει πολλά στοιχεία προκατάληψης και επίπεδα εμπιστοσύνης κατά πόσο η εταιρεία παραγωγής θα διοχετεύσει όλη την αλήθεια προς την αγορά. Τα περιστατικά βοδινού κρέατος που περιείχαν DNA αλόγου είναι πολύ πρόσφατα. Για πολλά χρόνια αυτό αποκρυπτόταν από τους καταναλωτές και όπως μάθαμε σε μεταγενέστερο στάδιο ήταν ένα κοινό μυστικό στην συγκεκριμένη αγορά. Το Blockchain δίνει τη δυνατότητα αποκεντροποίησης της πληροφορίας αφού πλέον το κάθε κομμάτι του supply chain θα μπορεί να ενημερώνει με τις οποιεσδήποτε πληροφορίες αφορούν το συγκεκριμένο προϊόν. Συνεπώς, ο καταναλωτής, θα μπορεί να παίρνει πληροφορίες πριν ακόμα αγοράσει το προϊόν.

Ένας άλλος τομέας που διαφαίνεται ότι η τεχνολογία του Blockchain θα έχει άμεση και μαζική εφαρμογή είναι ο τομέας της υγείας (healthcare). Ήδη είδαμε κάποιες εφαρμογές στον ευρύ κόσμο των Έξυπνων Πόλεων αλλά σταδιακά δημοσιεύονται όλο και περισσότερες μελέτες για την υιοθέτηση του Blockchain. Πρόσφατα έγινε αναφορά στο Healthcoin σαν μια επαναστατική πλατφόρμα που θα έχει σαν στόχο την αποκεντροποίηση των δεδομένων και παράλληλα θα δίνει ανταμοιβή στους διαβητικούς σε προϊόντα και υπηρεσίες (Hanna, Auquier, & Toumi, 2017). Πιο συγκεκριμένα, οι διαβητικοί θα μπορούν να καταχωρούν στο Blockchain τα αποτελέσματα των εξετάσεων τους όσο αφορά τα επίπεδα αιμοσφαιρίνης και ανάλογα με το αποτέλεσμα θα ανταμείβονται με ψηφιακά διακριτικά (digital tokens). Ανάλογα με τον αριθμό διακριτικών που έχουν θα μπορούν να πάρουν είτε ανταμοιβή υπό τη μορφή μειωμένων φόρων, θεραπειών εξειδικευμένων στο διαβήτη και άλλες παρεμφερείς υπηρεσίες. Αυτό βέβαια είναι μόνο ένα παράδειγμα μέσα στη πληθώρα λύσεων που θα μπορούσε να προσφέρει το Blockchain στο συγκεκριμένο τομέα. Γενικότερα, η αποκεντροποίηση των δεδομένων έχει ως απώτερο σκοπό την δημιουργία μιας υποδομής η οποία θα παρέχει ισορροπία μεταξύ της

ασφάλειας και του απόρρητου των δεδομένων αλλά ταυτόχρονα να μπορεί να δώσει πρόσβαση σε νέες υπηρεσίες (Dios, 2016). Η κοινότητα του Blockchain θεωρεί ότι έχει όλες τις αξιώσεις για να τα καταφέρει. Ένα μεγάλο εμπόδιο που καλείται να ξεπεράσει ο τομές της υγείας είναι η σωστή διαχείριση της ταυτότητας (identity management) των ασθενών. Με την υπάρχουσα κατάσταση στον τομέα της υγείας, όλοι οι εμπλεκόμενοι (ασθενείς, γιατροί, διοικητικό προσωπικό κλπ.) είναι σε μια συνεχή διαδικασία ασφαλούς διαχείρισης της ταυτότητας, κυρίως των ασθενών. Πολλές φορές αυτό συμβαίνει για να τους δοθεί πρόσβαση σε ιατρικό ιστορικό, ενεργοποίηση ασφαλιστικών αποζημιώσεων, πρόσβαση σε άλλες ιατρικές υπηρεσίες και πολλά άλλα. Αυτό όμως έχει ως αποτέλεσμα να γίνονται καθυστερήσεις και οι ασθενείς να μην έχουν όση πρόσβαση θα ήθελαν σε συνδυασμό με περισσότερο έλεγχο στα δεδομένα τους που είναι διαθέσιμα προς τρίτους (Sarah, 2017). Έχουμε ήδη κάνει αναφορά σε προηγούμενο κεφάλαιο για την ανάγκη που έχουν οι καταναλωτές (και σε αυτό το παράδειγμα οι ασθενείς) στο να έχουν πλήρη κυριότητα των δεδομένων τους. Πολλά τρίτα μέρη κερδοφορούν αξιοποιώντας τα δεδομένα των ασθενών όχι μέσα από συμφωνίες που έχουν συνάψει με τους ίδιους αλλά με διάφορους φορείς που έχουν την κυριότητα της εκάστοτε βάσης δεδομένων. Με την μεταφορά των δεδομένων στη τεχνολογία του Blockchain, η πρόσβαση στα δεδομένα θα είναι ελεγχόμενη μόνο από τον ίδιο τον ιδιοκτήτη και όχι από τρίτους. Επίσης, θα υπάρξει μια σημαντική αύξηση στην ταχύτητα που θα μπορούν να γίνεται η μεταφορά δεδομένων από τον ένα φορέα στον άλλο. Ο ασθενής θα μπορεί να αναζητήσει τις υπηρεσίες ενός άλλου νοσοκομείου χωρίς να χρειαστεί να υποστεί τις οποιεσδήποτε καθυστερήσεις που θα δημιουργηθούν μέσα από την ανάγκη για να τακτοποιηθεί εκ νέου ο ασθενής και να σταλεί ο ιατρικός φάκελος από το ένα νοσοκομείο στο άλλο. Πλέον όλες οι πληροφορίες θα είναι καταχωρημένες σε μια βάση δεδομένων που θα είναι διανεμημένη σε όλους τους φορείς. Ο ασθενής απλά θα πρέπει να δώσει την ανάλογη πρόσβαση στο επιθυμητό αρχείο για να ξεκινήσει η διαδικασία. Όπως και στο παράδειγμα του Healthcoin, έτσι και σε αυτή τη περίπτωση, ήδη υπάρχουν έτοιμες πλατφόρμες που προσφέρουν αυτές τις υπηρεσίες σε όλους τους φορείς που εμπλέκονται στον τομέα της υγείας και θα ήθελαν να κάνουν την μετάβαση από τον παραδοσιακό τρόπο διασφάλισης μεταφοράς, και επεξεργασίας δεδομένων στον αποκεντρωμένο κόσμο του Blockchain. Μια από αυτές είναι το Gem Health Network που είναι βασισμένο πάνω στην πλατφόρμα του Ethereum. Επίσης στην πλατφόρμα του Etheruem είναι βασισμένο και το project Uport (www.uport.me) όπου επιχειρεί να δώσει λύσεις στο θέμα του ελέγχου των δεδομένων από τον ίδιο τον ιδιοκτήτη.

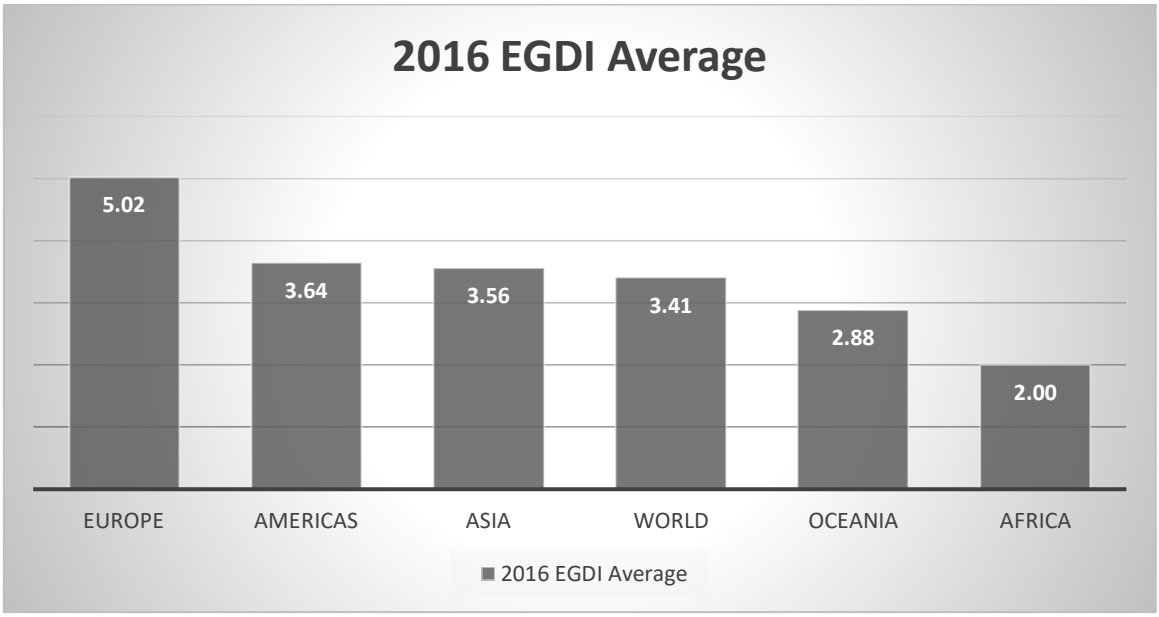
Ο τομέας που έχει ήδη επενδύσει αρκετά λεφτά στην έρευνα και μελέτη του Blockchain είναι ο χρηματοπιστωτικός. Πιο συγκεκριμένα, υπολογίζεται ότι μέσα σε 3 χρόνια έχει γίνει επένδυση 1.6 δισεκατομμυρίων δολαρίων και ότι το 80% των τραπεζών έχουν ξεκινήσει μέσα στο 2017 κάποια projects που έχουν να κάνουν με την τεχνολογία του Blockchain (McWaters, 2016). Αυτό είναι ένας ολοφάνερος δείκτης της δυναμικής που έχει αποκτήσει η συγκεκριμένη τεχνολογία. Αυτό που απομένει είναι να δούμε κατά πόσο θα μπορέσει να υπερκεράσει τις παραδοσιακές μεθόδους που λειτουργεί μια τόσο καλά παγιωμένη και πολλές φορές άκαμπτη βιομηχανία. Αναφορικά με τις χρήσεις της τεχνολογίας στον χρηματοοικονομικό τομέα, θα ήταν παράληψη να μην γίνει αναφορά στη δημιουργία των κρυπτό-νομισμάτων. Με το Bitcoin αρχικά και σε μεταγενέστερο στάδιο το Eth (το κρυπτό-νόμισμα που υποστηρίζει η πλατφόρμα του Ethereum) ήδη αρκετές συναλλαγές επιλέγουν τον αποκεντρωμένο τρόπο συναλλαγών όπου το νόμισμα δεν ελέγχεται από κάποιο κεντρικό ίδρυμα (institution) άλλα κατευθείαν από τους συνδιαλλαζομένους.

Οι πρακτικές εφαρμογές του Blockchain στην καθημερινή ζωή και ειδικότερα στο γενικότερο πλαίσιο των έξυπνων Πόλεων είναι ανεξάντλητες και θα ήταν δύσκολο να καλυφθούν μέσα από μια μόνο εργασία. Σε αυτό το κεφάλαιο κάναμε μόνο μια ενδεικτική αναφορά έτσι ώστε να γίνει αντιληπτό ότι η τεχνολογία του Blockchain περνάει σταδιακά από την θεωρία στην πράξη. Ένας μεγάλος τομέας που ήδη έχει βάλει στις τάξεις του το Blockchain είναι η ηλεκτρονική διακυβέρνηση (e-governance). Αφήσαμε πίσω εσκεμμένα αυτόν τον τομέα έτσι ώστε να μπορέσουμε να τον μελετήσουμε με περισσότερη λεπτομέρεια. Πέρα από τις πρακτικές εφαρμογές που θα εξετάσουμε, θα δούμε και τη χρήση των Έξυπνων Συμβολαίων στα οποία έχουμε κάνει μια πολύ επιφανειακή αναφορά στον πρόλογο αυτή της μεταπτυχιακής διατριβής.

Κεφάλαιο 3

Ηλεκτρονική Διακυβέρνηση

Σε μια προσπάθεια εκσυγχρονισμού και συμβατότητας με τις νέες προσκλήσεις της τεχνολογίας, βλέπουμε μεγάλα βήματα προς την υιοθέτηση της η-διακυβέρνησης από πάρα πολλές χώρες και ειδικότερα από τις ευρωπαϊκές. Βλέποντας πιο κάτω, παρατηρούμε τον δείκτη (index) που έχει δημοσιευτεί από τα Ηνωμένα Έθνη , με δεδομένα του 2016, σχετικά με τις περιοχές που προσφέρουν την δυνατότητα της η-διακυβέρνησης στους πολίτες τους. Όπως είναι εμφανές από τον πίνακα, η Ευρώπη είναι κατά πολύ πιο ψηλά από τον παγκόσμιο μέσο όρο και υπερτερεί αισθητά των χωρών της Αμερικής. Απλά να αναφέρουμε ότι αυτός ο δείκτης περιλαμβάνει δεδομένα μόνο από τις χώρες-μέλη των Ηνωμένων Εθνών παρόλα αυτά θεωρούμε ότι είναι ένα πολύ καλό δείγμα για να γίνει εξαγωγή συμπερασμάτων σχετικά με το θέμα.



Σχήμα 4 e-Governance Development Index πηγή:https://publicadministration.un.org

3.1 Η Ανάγκη για Ηλεκτρονική Διακυβέρνηση

Οι λόγοι που οδήγησαν όλο και περισσότερες κυβερνήσεις στην δημιουργία υποδομής για την ενσωμάτωση της η-Διακυβέρνησης, ανάμεσα σε πολλούς άλλους, έχουν να κάνουν κυρίως με την επιτακτική ανάγκη για διαφάνεια και ασφάλεια ανάμεσα στους πολίτες και την πολιτεία. Πιο συγκεκριμένα, η Παγκόσμια Τράπεζα έχει ορίσει την η-Διακυβέρνηση ως τη χρησιμοποίηση των ΤΠΕ έτσι ώστε οι κυβερνήσεις να βελτιώσουν την απόδοση, διαφάνεια και λογοδοσία τους όπου μετακινώντας τις υπηρεσίες τους στο διαδίκτυο ελπίζουν να καταφέρουν τα εξής:

- Μείωση κόστους
- Προώθηση οικονομικής ανάπτυξης
- Ενίσχυση της διαφάνειας και της λογοδοσίας
- Βελτίωση της παροχής υπηρεσιών (Sullivan & Burger, 2017)
- Βελτίωση της Δημόσιας Διοίκησης
- Διευκόλυνση της Ηλεκτρονικής Κοινωνίας (e-Society) (WorldBank, n.d.)

Με στόχο τα πιο πάνω, πολλές χώρες κινήθηκαν προς αυτή τη κατεύθυνση σταδιακά αφού ξεκίνησαν να επενδύουν σε νέες τεχνολογίες, εκπαίδευση κατάλληλου προσωπικού και μετατόπιση κάποιων υπηρεσιών στο διαδίκτυο σε πιλοτικό στάδιο. Η Εσθονία είναι μια από τις χώρες που έκανε τεράστια άλματα προς αυτή τη κατεύθυνση και σήμερα θεωρείται ως η χώρα πρότυπο με τον τρόπο που έχει εντάξει την η-Διακυβέρνηση στην καθημερινότητα της ευρύτερης κοινωνίας. Το 2015, όταν είχε πρωτοξεκινήσει αυτό το εγχείρημα, ο υπεύθυνός ΤΠΕ της Εσθονικής κυβέρνησης είπε ότι έχουν εφαρμόσει την η-Διακυβέρνηση βλέποντας το σαν ένα κυβερνητικό startup χωρίς να ξέρουν κατά πόσο αυτό θα δουλέψει ή όχι, ευχόμενοι τουλάχιστον να μπορεί να διαταράξει την υπάρχουσα κατάσταση (Beumer, 2015). Αυτή η δήλωση δείχνει το επίπεδο του ρίσκου που θα πρέπει να ληφθεί υπόψη για την υιοθέτηση μιας τέτοιας καινοτομίας αφού ίσως οι κοινωνίες να μην είναι ακόμα δεκτικές για να τις αφομοιώσουν. Πιο κάτω θα δούμε την θέση που θα μπορεί να κατέχει η τεχνολογία του Blockchain στην εφαρμογή και λειτουργία της η-Διακυβέρνησης και μια πρώτη πιο εις βάθος αναφορά στο ρόλο των Έξυπνων Συμβολαίων.

3.2 Το Blockchain στην η-Διακυβέρνηση

Όπως είδαμε σε προηγούμενο κεφάλαιο, οι διάφοροι εμπλεκόμενοι φορείς θα πρέπει να λύσουν κάποια θεμελιώδη ζητήματα ασφαλείας τα οποία προκύπτουν από την χρησιμοποίηση λύσεων από τρίτα μέρη. Πιο συγκεκριμένα θα πρέπει να γίνει αναφορά στα θέματα της ιδιοκτησίας των δεδομένων (data ownership), της διαφάνειας των δεδομένων και στον έλεγχο της πρόσβασης (Zyskind, Nathan, & Pentland, 2015). Η τεχνολογία του Blockchain, με την αποκεντρωμένη και ανοικτά διανεμημένη προς όλους τους εμπλεκόμενους φιλοσοφία της, έχει ήδη ξεκινήσει να μπαίνει σε εφαρμογή για να δώσει λύσεις στο μεγάλο εγχείρημα της η-Διακυβέρνησης. Σε ένα γενικότερο πλαίσιο, το Blockchain, χρησιμοποιείται σαν ένα όχημα που θα εγγυάται την ακεραιότητα της ταυτότητας του χρήστη χωρίς την ανάγκη επισημοποίησης από τα κυβερνητικά όργανα. Αφού γίνει η ταυτοποίηση, τότε θα μπορούν να γίνουν υπογραφές συμβολαίων, τραπεζικές και εταιρικές ενσωματώσεις όπως και εφαρμογές καινούργιων συστημάτων πληρωμών πέρα από τα παραδοσιακά συστήματα που χρησιμοποιούνται από τον χρηματοπιστωτικό τομέα (Sullivan & Burger, 2017). Ήδη το Τμήμα Χωροταξίας του Dubai (Dubai Land Department) έβαλε σε εφαρμογή μια πλατφόρμα βασισμένη στο Blockchain όπου οι πολίτες μπορούν να καταγράψουν όλα τα έγγραφα ακινήτων (πωλητήρια, έγγραφα ιδιοκτησίας κλπ.) και να κάνουν πληρωμές χωρίς την ανάγκη να υπάρχει φυσική παρουσία σε οποιοδήποτε κυβερνητικό κτήριο. Αφού όλη η διαδικασία γίνεται μέσω του Blockchain, η συγκεκριμένη βάση είναι διανεμημένη και σε άλλες υπηρεσίες (π.χ. Αρχή Ηλεκτρισμού και Υδάτων). Με αυτό το τρόπο εξασφαλίζεται η ταχύτερη εξυπηρέτηση μέσω αυτών των υπηρεσιών αφού τα δεδομένα σχετικά με την ιδιοκτησία είναι ήδη καταγεγραμμένα και πιστοποιημένα χωρίς την ανάγκη επανάληψης της διαδικασίας (Kwang, 2017).

Στο παράδειγμα της Εσθονίας που ήδη κάναμε μια αναφορά, έχουν εισάγει την κυβερνητική υπηρεσία του e-Πολίτη (e-Resident). Λίγο πριν την έναρξη των εργασιών της η-Διακυβέρνησης, το 2014 η κυβέρνηση της Εσθονίας ανήγγειλε ότι οποιοσδήποτε πολίτης (ανεξαρτήτου καταγωγής ή τόπου διαμονής) θα μπορούσε να κάνει αίτηση για να του χορηγηθεί η η-Ταυτότητα (e-ID). Αυτό το εγχείρημα ήταν η απαρχή της η-Διακυβέρνησης που παρουσιάστηκε λίγο αργότερα. Σύμφωνα με τον κυβερνητικό ιστότοπο που είναι υπεύθυνος για την πληροφόρηση πάνω στο θέμα, η-Ταυτότητα, πέρα από το αυτονόητο, έδινε τη δυνατότητα στους η-Πολίτες να κάνουν τα εξής ανάμεσα σε άλλα:

- Εκκίνηση εταιρείας 100% διαδικτυακά
- Πρόσβαση σε χρηματοπιστωτικούς και άλλους παρόχους πληρωμών
- Καθολική κυριότητα της εταιρείας από τον η-Πολίτη χωρίς την ανάγκη κάποιου τοπικού διευθυντή.
- Υπογραφή και πιστοποίηση εγγράφων από οπουδήποτε.
- Κρυπτογράφηση και αποστολή εγγράφων με ασφάλεια.
- Φορολογική δήλωση μέσω διαδικτύου
- Απόκτηση ανεξαρτησίας σε θέματα μετακινήσεων αφού πλέον όλα μπορούν να γίνουν ηλεκτρονικά χωρίς την ανάγκη φυσικής παρουσίας στην Εσθονία ή οπουδήποτε αλλού.

Είναι σημαντικό να αναφερθεί ότι η η-Ταυτότητα δεν αποτελεί κάποιο έγγραφο που να δίνει πραγματική υπηκοότητα ή το δικαίωμα εισόδου σε οποιαδήποτε χώρα της Ε.Ε. που θα είχε ένας υπήκοος της Εσθονίας (Estonia, n.d.).

Βλέποντας τη πληθώρα δυνατοτήτων που παρέχει η η-Ταυτότητα γίνεται αντιληπτό ότι κάποια από αυτά προσπαθούν να δώσουν λύσεις σε ζητήματα που ήδη έχουμε θέσει μέσα από αυτή τη εργασία. Για παράδειγμα το θέμα της ιδιωτικότητας και της ασφάλειας/ελέγχου των δεδομένων ενός πολίτη. Όπως γίνεται αντιληπτό, η εφαρμογή του Blockchain δεν άργησε να ενσωματωθεί στο όλο εγχείρημα έτσι ώστε να δώσει λύσεις σε προβλήματα που θα ήταν ανυπέρβλητα με την χρησιμοποίηση της παραδοσιακής βάσης δεδομένων. Η διαφύλαξη όλων των δεδομένων στην πλατφόρμα του Blockchain εξασφαλίζει την άμεση πρόσβαση όλων των ενδιαφερομένων σε αυτά χωρίς την ανάγκη για συνεχή ταυτοποίηση του προσώπου (φυσικού η νομικού). Με αυτό το τρόπο, ο δημόσιος τομέας που παραδοσιακά είναι άκαμπτος και αδιάλλακτος, κατάφερε να γίνει καινοτόμος και να είναι έτοιμος να ανταποκριθεί στις ανάγκες της κοινωνίας (Millard, 2017).

3.3 Πλατφόρμες Blockchain

Η πλατφόρμα του Bitcoin ήταν αυτή που έκανε την τεχνολογία του Blockchain ευρέως γνωστή. Λόγω των σκαμπανεβασμάτων που είχε το κρυπτονόμισμα που υποστηρίζει, έκανε τους αναλυτές από διάφορες βιομηχανίες, πέρα από την ΤΠΕ, να δώσουν περισσότερη σημασία στις δυνατότητες που έχει. Παρόλα αυτά, η πλατφόρμα του Bitcoin δεν είναι μοναδική. Σε αυτή τη

εργασία μιλήσαμε ήδη για το αντίπαλο δέος του Bitcoin που είναι το Ethereum. Το Ethereum θα μας απασχολήσει εκτενώς και στο υπόλοιπο της μεταπτυχιακής διατριβής αφού είναι το βασικό όχημα για να δημιουργηθούν τα Έξυπνα Συμβόλαια.

Αναφορικά να πούμε ότι σταδιακά άρχισαν να ξεπετάγονται διάφορες πλατφόρμες που η κάθε μια προσπαθεί να χτίσει κάτι διαφορετικό χρησιμοποιώντας το Blockchain σαν την βασική υπηρεσία στην οποία βασίζονται. Χωρίς να μπορούμε να αναφερθούμε σε όλες τα πλατφόρμες, θεωρούμε σωστό να αναφερθούμε σε κάποιες πολύ βασικές που η κάθε μια για δικούς της λόγους δείχνει να μπορεί να συνεισφέρει κάτι περισσότερο από τις άλλες.

Το Monero[1] είναι ένα ακόμα ψευδονόμισμα το οποίο βασίζεται σε ανοικτό κώδικα (open source) και οι προγραμματιστές του ισχυρίζονται ότι είναι απόλυτα ασφαλές και σχεδόν αδύνατον να ευρεθεί ο κάτοχος του. Οι μεγάλες εταιρείες όπως η Microsoft και IBM θα ήταν αδύνατον να μείνουν εκτός παιχνιδιού και για αυτό το λόγο επέλεξαν να δημιουργήσουν τις δικιές τους πλατφόρμες. Πιο συγκεκριμένα, η Microsoft δημιούργησε το Azure Blockchain[2] το οποίο είναι από μόνο του ενδιαφέρον αν αναλογιστούμε ότι η υπηρεσία Azure είναι το cloud service της Microsoft. Αντίστοιχα, η IBM έχει αναπτύξει το IBM Blockchain[3] το οποίο επίσης κάνει χρήση την ήδη εν ενεργεία υπηρεσία του cloud. Στο github[4] υπάρχει μια εκτενής λίστα με τις διάφορες πλατφόρμες από όπου ο αναγνώστης θα μπορούσε να πάρει περισσότερες πληροφορίες για τις ιδιότητες και δυνατότητες της κάθε μίας.

3.4 Ασφάλεια των Έξυπνων Συμβολαίων

Πριν δούμε ένα παράδειγμα Έξυπνου Συμβολαίου θα δούμε λίγο τον τρόπο δημιουργίας τους. Υπάρχουν κάποιες εναλλακτικές γλώσσες που χρησιμοποιούνται για την γραφή Έξυπνων Συμβολαίων όπως η Solidity, Serpent και LLL. Αυτή τη στιγμή η Solidity δείχνει να επικρατεί σαν ο πιο διαδεδομένος τρόπος γραφής (Frantz & Nowostawski, 2016). Μελετώντας τη Solidity, είναι εμφανής η επιρροή που έχει από την Javascript, την C++ και την Python. Για

[1] https://getmonero.org/
[2] https://azure.microsoft.com/en-us/solutions/Blockchain/
[3] https://www.ibm.com/Blockchain/
[4] https://github.com/imbaniac/awesome-Blockchain

την επεξεργασία κάποιων συμβολαίων χρησιμοποιήσαμε το Remix[5] σαν IDE (Intergated Development Environment) το οποίο προσφέρει εργαλεία ανεύρεσης σφαλμάτων (debugger) μέσα σε περιβάλλον δοκιμής (test environment).

Είναι εμφανές ότι ούτε η τεχνολογία του Blockchain θα μπορούσε να ξεφύγει από κάποιες σοβαρές ευπάθειες οι οποίες έπληξαν την αξιοπιστία των χρηστών για το κατά πόσο είναι σε θέση να δώσει λύσεις σε αυτό το τομέα. Μιλώντας για ευπάθειες, και ειδικότερα για τα Έξυπνα Συμβόλαια, θα προσπαθήσουμε να αναλύσουμε αυτές που έχουν εφαρμογή και στο θέμα της η-Διακυβέρνησης ακόμα και αν αυτές οι ευπάθειες έχουν εν δυνάμει εφαρμογή σε περισσότερους τομείς της ευρύτερης κοινωνίας.

3.4.1 Reentrancy vulnerability

Η ευπάθεια του Reentrancy έχει να κάνει με ένα λάθος στο προγραμματισμό των Έξυπνων Συμβολαίων όπου επέτρεπε την πολλαπλή εκτέλεση μιας εντολής πριν γίνει ενημέρωση του λογαριασμού του θύματος. Πιο συγκεκριμένα, ας υποθέσουμε ότι ο Α καλείται να δώσει κάποιο ποσό (eth) στον Β, αφού πληρούσε τα κριτήρια του συμβολαίου. Τότε ο Β τραβούσε (withdraw) το ποσό από το λογαριασμό του Α. Χρησιμοποιώντας την εντολή *msg.sender.call.value* επιτρέπει την επανάληψη της εντολής αφού το υπόλοιπο του λογαριασμού (*userBalances[msg.sender])* γίνεται 0 στο τέλος της εντολής. Άρα ο επιτιθέμενος θα μπορεί να πάρει και άλλα eth αφού ο λογαριασμός δεν θα είναι ακόμα ενημερωμένος. Πιο κάτω βλέπουμε ένα παράδειγμα από αυτή την επίθεση.

[5] https://remix.ethereum.org

```
function getBalancefrom(address user) constant returns(uint) {
  return userBalance[user];
}

function addToBalance() {
  userBalances[msg.sender] += msg.amount;
}

function withdrawBalance() {
  amountToWithdraw = userBalances[msg.sender];
  if (!(msg.sender.call.value(amountToWithdraw)//ο κώδικάς μπορει να εκτελεστει και να αφαιρεσει το ποσο πολλαπλες φορες.
  userBalances[msg.sender] = 0;
}
```

Σχήμα 5 Ευπάθεια Reentrancy

Για να επιλυθεί αυτή η ευπάθεια υπάρχουν διάφορες προσεγγίσεις αλλά η πιο σωστή είναι να γίνει μια μετατροπή στο κώδικα έτσι ώστε να μην επιτρέπεται η επανεκτέλεση της λειτουργίας (function) περισσότερες από μια φορά.

```
function getBalancefrom(address user) constant returns(uint) {
  return userBalance[user];
}

function addToBalance() {
  userBalances[msg.sender] += msg.amount;
}

function withdrawBalance() {
  amountToWithdraw = userBalances[msg.sender];
  userBalances[msg.sender] = 0;
  if (!(msg.sender.call.value(amountToWithdraw)//πλεον το υπολοιπο του λογαριασμου ειναι 0 αρα δεν μπορει να εκτελεσθει η εντολη ξανα.

}
```

Σχήμα 6 Διόρθωση ευπάθειας Reentrancy

Όπως φαίνεται πιο πάνω, θα πρέπει να γίνει αντικατάσταση των γραμμών 12 και 13 έτσι ώστε η λειτουργία να ενημερώνει τον λογαριασμό πριν δοθεί η εντολή να γίνει η απόσυρση των eth. Με αυτό το τρόπο, η δοκιμή για επανεκτέλεση της λειτουργίας απλά θα δίνει μη επαρκές υπόλοιπο που θα καταλήγει σε μη συνέχιση της διαδικασίας *(Anonymous, 2017)*.

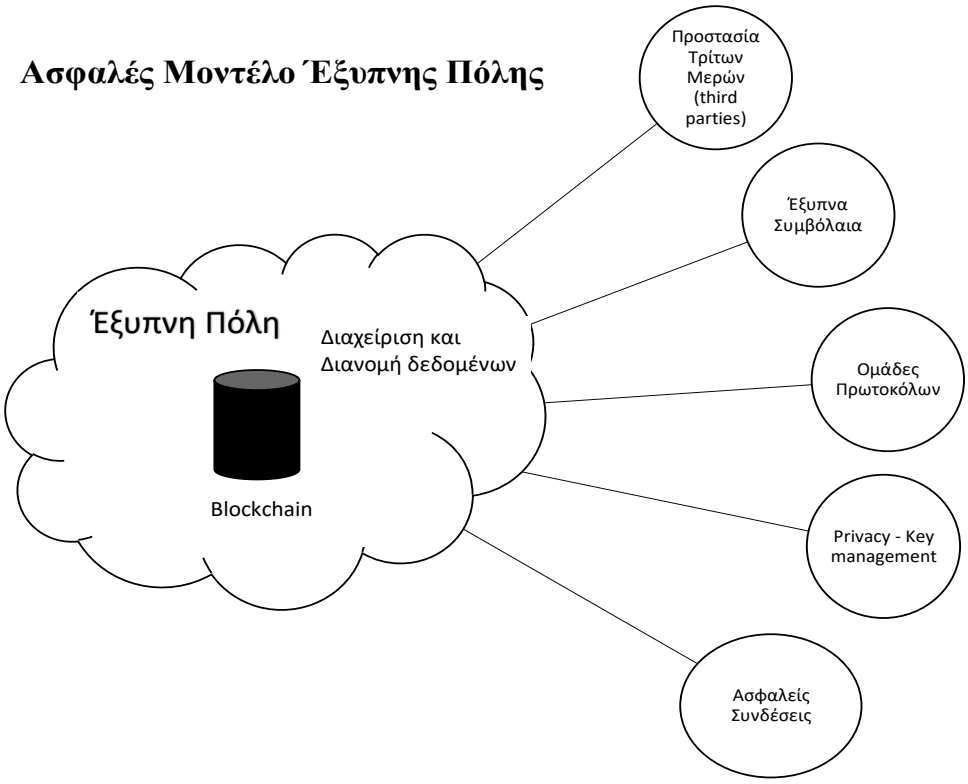
Η συγκεκριμένη ευπάθεια έγινε αρκετά γνωστή λόγω της δημοσιότητας που απέκτησε το DAO hack όπου περί το Μάιο του 2016 είχε αξία περίπου 150,000 δολαρίων. Πιο συγκεκριμένα, το DAO (Decentralised Autonomous Organisation) είναι ένα υπολογιστικό πρόγραμμα ανοικτού κώδικα όπου είχε ως σκοπό να δημιουργεί Έξυπνα Συμβόλαια τα οποία θα τρέχουν πάνω στη πλατφόρμα του Ethereum και θα έχουν να κάνουν με την ανοικτή χρηματοδότηση (crowdfunding) κάποιων startups (Magazzeni, McBurney, & Nash, 2017). Ο επιτιθέμενος αφού εντόπισε την ευπάθεια εκτελούσε την εντολή απόσυρσης κρυπτονομισμάτων επανειλημμένα. Αυτό είχε σαν συνέπεια να κλαπούν κρυπτονομίσματα αξίας 50 εκ. δολαρίων.

Η συγκεκριμένη ευπάθεια δείχνει την αδυναμία σε θέματα ακεραιότητας (integrity) το οποίο είναι βασικός πυλώνας των αρχών της ασφάλειας. Οι Magazzeni et al ανέλυσαν πολύ εμπεριστατωμένα τα βασικά ερωτήματα που πρέπει να απαντηθούν έτσι ώστε διασφαλιστεί η σωστή λειτουργία των Έξυπνων Συμβολαίων. Μέσα σε αυτά είναι και το κατά πόσο το συμβόλαιο εκτελεί την διαδικασία για την οποία προορίζεται αλλά και ταυτόχρονα χωρίς να επιτρέπει να εκτελείται οποιαδήποτε άλλη λειτουργία. Στη περίπτωση του reentrancy, το πρώτο σκέλος είναι εφικτό αφού όντως ο κώδικάς εκτελεί τον αρχικό του στόχο. Παρόλα αυτά, αφήνει περιθώρια στον επιτιθέμενο να εκτελέσει κάποιες εντολές πέρα από το επιθυμητό το όποιο θέτει σε αμφισβήτηση την ακεραιότητα του συμβολαίου.

Κεφάλαιο 4

Μοντέλο Ασφαλούς Έξυπνης Πόλης

Οι έξυπνες πόλεις είναι ήδη μέσα στη ζωή μας και αναμένεται να παίξουν μεγάλο ρόλο στην καθημερινότητα μας με διάφορους τρόπους. Η ανάπτυξή τους είναι διάχυτη παρόλα αυτά είναι διάφοροι οι τομείς που πρέπει να ληφθούν υπόψη προτού να χαρακτηρισθεί βιώσιμη λύση για την νέα εποχή. Η εξέλιξη από το IoT στις έξυπνες πόλεις μοιάζει σαν μια φυσική συνέχεια, εντούτοις, η επιτυχία τους εναπόκειται στην άψογη συνεργασία διαφόρων κλάδων και στην επεξεργασία μεγάλου όγκου δεομένων. Για αυτούς τους λόγους, υπάρχουν έντονες ανησυχίες για το συγκεκριμένο εγχείρημα. Οι έξυπνες πόλεις λειτουργούν με βάση ετερογενείς μηχανισμούς και τεχνολογίες όπου η συμβατότητα τους είναι μια μεγάλη πρόκληση σχετικά με την ασφάλεια (Chakrabarty & Engels, 2016). Σε προηγούμενα κεφάλαια μιλήσαμε για τους τομείς που θα επηρεαστούν μέσα από το περιβάλλον των έξυπνων πόλεων όπως για παράδειγμα της ενέργειας, μεταφορών κλπ. Σε αυτό το κεφάλαιο θα παρουσιάσουμε ένα υβριδικό μοντέλο έξυπνης πόλης μέσα από το πρίσμα της ασφάλειας. Όπως είναι φυσικό οι παράγοντες που επηρεάζουν μια Έξυπνη Πόλη είναι αρκετοί, εντούτοις προσπαθήσαμε να επικεντρωθούμε σε αυτούς που θεωρήθηκαν οι πιο σημαντικοί. Είναι ευρέως γνωστό ότι η πλήρης ασφάλεια είναι ένα ουτοπικό σενάριο και για αυτό το λόγο η ασφάλεια θα πρέπει να ενοποιηθεί με το δίκτυο, προκειμένου να εξαλειφθούν τυχόν εμπόδια μεταξύ αξιοπιστίας και ασφάλειας (Sklavos, Zaharakis, Kameas, & Kalapodi, 2017). Το σχεδιάγραμμα 7 δείχνει τους βασικούς τομείς τους οποίους συμπεριλάβαμε σε αυτό το μοντέλο.



Σχήμα 7 Ασφαλές Μοντέλο Έξυπνων Πόλεων

4.1 Διαχείριση και Διανομή δεδομένων

Το Blockchain αναμένεται να διαδραματίσει πρωταγωνιστικό ρόλο μέσα στο ταχείας ανάπτυξης κόσμο των Έξυπνων Πόλεων. Το IoT είναι πολύ κοντά μας και ήδη αποτελεί ένα αναπόσπαστο κομμάτι της σύγχρονης εποχής. Το Blockchain και το IoT τείνουν να ενώσουν τις δυνάμεις τους για να ανταποκριθούν στις υψηλές απαιτήσεις των έξυπνων πόλεων καθώς και να εισάγουν νέες τεχνολογίες και υπηρεσίες. Η έννοια του Blockchain στο IoT (BIoT) είναι αρκετά δημοφιλής στις πόλεις που έχουν ήδη ξεκινήσει την πρακτική εφαρμογή των έξυπνων πόλεων.

Μέσα από αυτή την μεταπτυχιακή διατριβή έχουμε αναφερθεί πολλές φορές για την αναγκαιότητα της ταχείας πρόσβασης στα δεδομένα, ιδιαίτερα σε πραγματικό χρόνο. Αυτό αναμένεται να γίνει πραγματικότητα με την εισαγωγή του BIoT στο τρόπο διαχείρισης των δεδομένων. Οι συνδεδεμένοι κόμβοι θα μπορούν να έχουν πρόσβαση στα δεδομένα με

διαφάνεια, χωρίς παρεμβολές μέσα από τους διάφορους αισθητήρες που θα είναι ενσωματωμένοι σε προϊόντα και συσκευές (SmartCity, 2018). Επιπλέον, ο συνδυασμός Blockchain και IoT θα δώσει μια επιπλέον ώθηση στις προσπάθειες που γίνονται για να καλυφθούν οι έννοιες της εμπιστοσύνης, πιστοποίησης και τυποποίησης διαφόρων στοιχείων σε μια Έξυπνη Πόλη. Ιδιαίτερη έμφαση θα δοθεί στην ικανότητα αλληλεπίδρασης μεταξύ των χρηστών χωρίς την ανάγκη συμμετοχής ενός στοιχείου τρίτου μέρους (Review, 2017).

4.2 Προστασία Τρίτων Μερών

Οι έξυπνες πόλεις θα χρειαστούν πληθώρα από εφαρμογές, μηχανισμούς και υπηρεσίες για να μπορέσουν να ανταπεξέλθουν στις ανάγκες της κοινωνίας. Η ποιότητα ζωής θα ανέβει πραγματικά μόνο αν υπάρξει μια δραματική αύξηση στο επίπεδο των υπηρεσιών που προσφέρονται. Οι εταιρείες που παρέχουν υπηρεσίες τρίτων μερών θα καλεστούν να μπουν στην εξίσωση για να ικανοποιήσουν τις απαιτήσεις των διασυνδεδεμένων τεχνολογιών. Το ιδανικό μοντέλο μιας έξυπνης πόλης περιλαμβάνει μια ισχυρή πολιτική λογοδοσίας όλων των μερών που εμπλέκονται μέσα σε αυτό το σχέδιο. Τα περιουσιακά στοιχεία και δεδομένα πρέπει να διαφυλαχθούν μέσα από ακριβής συμφωνίες συμβολαίων. Ο ξέφρενος ρυθμός λειτουργίας των έξυπνων πόλεων δεν θα αφήνει πολλά περιθώρια για μεγάλες παρεκκλίσεις. Σχετικά με αυτό το θέμα, η χρησιμοποίηση λύσεων ανοικτού κώδικα θα έχει αντίθετες συνέπειες αφού θα περιορίσει τις πολιτικές λογοδοσίας. Η ερευνήτρια Lisa Vaas ανέλυσε το παράδειγμα του Heartbleed όπου είναι μια επίθεση στον κώδικα του OpenSSL. Σε αυτή τη περίπτωση είναι πολύ δύσκολο να καταστεί υπεύθυνος κάποιος συγκεκριμένα, συνεπώς, πρέπει να μπουν σε εφαρμογή άλλες πολιτικές ασφαλείας (Vaas, 2018).

Είναι πολύ σημαντικό όπως οι ευθύνες και υποχρεώσεις να είναι καθορισμένες από την αρχή. Με αυτό το τρόπο όλοι οι εμπλεκόμενοι φορείς θα έχουν τα καθήκοντα και τα δικαιώματα τους ευθυγραμμισμένα. Οι αρμοδιότητες θα πρέπει να καθορίζονται από ισχυρές κατευθυντήριες γραμμές για τη συντήρηση των υπηρεσιών, την ανάπτυξη ασφαλών πρωτοκόλλων, την εκπαίδευση του προσωπικού και την παροχή δοκιμών για κρίσιμες λειτουργίες (Levy-Bencheton & Darra, 2015). Επιπρόσθετα, θα πρέπει να δοθεί ιδιαίτερη σημασία στην ασφάλεια των δεδομένων μέσα από σχεδιασμούς που αφορούν τη διαχείριση κινδύνων και αντιμετώπιση περιστατικών (incidence response) (Durin, 2015). Οι τοπικές αρχές πρέπει να είναι βέβαιες ότι

σε περίπτωση παραβίασης δεδομένων υπάρχει ένα προ-δραστικό σχέδιο όπου όλες οι πτυχές ασφαλείας είναι συμφωνημένες. Αυτό θα καθησυχάσει τα μέλη των έξυπνων πόλεων δημιουργώντας αίσθημα εμπιστοσύνης και ισχυρή εποπτεία προς τα τρίτα μέρη.

4.3 Αυτοματοποίηση Διαδικασιών- Έξυπνα Συμβόλαια

Σε προηγούμενη παράγραφο αυτού του κεφαλαίου μιλήσαμε για το εγχείρημα της η-Διακυβέρνησης και τις λύσεις που θα μπορεί να επιφέρει μια πλήρης υλοποίηση της. Όπως είναι λογικό, ένας ολόκληρος μηχανισμός διακυβέρνησης (ανεξάρτητα αν γίνεται με τον παραδοσιακό τρόπο ή ηλεκτρονικά) βασίζεται πάνω σε ένα μεγάλο αριθμό συμφωνιών μεταξύ δυο ή περισσοτέρων μερών. Αυτές οι συμφωνίες έχουν ως σκοπό την ομαλή λειτουργία της διακυβέρνησης αφού καθορίζουν τις διάφορες παραμέτρους και προϋποθέσεις στις οποίες όλα τα μέρη είναι υποχρεωμένα να συμμορφωθούν. Τα Έξυπνα Συμβόλαια θα διαταράξουν τον τρόπο που συνδιαλλάσσονται δυο ή περισσότερα μέρη, την ανταλλαγή υπηρεσιών και την γενικότερη αλληλεπίδραση τους μέσα στη κοινωνία. Ο απώτερος σκοπός των Έξυπνων Συμβολαίων είναι να καταστήσουν ξεπερασμένη την χρησιμοποίηση τρίτων μερών. Μέσα από αυτό θα γίνει κατορθωτό να μειωθεί ο χρόνος επεξεργασίας και οι πόροι που χρειάζονται για μια συναλλαγή.

Ας πάρουμε ένα απλό παράδειγμα ενοικίασης ενός διαμερίσματος με την χρήση ενός κτηματομεσιτικού γραφείου. Σε αυτή τη συμφωνία, έχουμε τον ενοικιαστή και τον ιδιοκτήτη που αναθέτουν τη συναλλαγή σε ένα τρίτο μέρος (τον κτηματομεσίτη) αφού δεν υπάρχει εμπιστοσύνη (trustless) μεταξύ των κυρίων μερών. Αυτή η συμφωνία περιλαμβάνει το ποσό και την ακριβή μέρα που θα γίνεται η μεταβίβαση των χρήματων. Κάποια συμβόλαια μπαίνουν ακόμα πιο βαθιά σε λεπτομέρειες όπως τον ακριβή αριθμό των επίπλων και ειδών σπιτιού που υπάρχουν στο ακίνητο κατά τη μέρα της ενοικίασης. Αφού ολοκληρωθεί η διαδικασία και όλα τα μέρη υπογράψουν τα ανάλογα έγγραφα, τότε ο κτηματομεσίτης είναι υπόχρεος να ενημερώσει τις αρμόδιες υπηρεσίες για την αλλαγή που έγινε στον ενοικιαστή. Ανάλογα, ο ενοικιαστής θα πρέπει να ενημερώσει όλους τους παρόχους (Ηλεκτρική, Τηλέφωνο κλπ.) για να έχουν τα σωστά στοιχεία στη βάση δεδομένων τους. Όλα τα πιο πάνω συμβαίνουν για μια

απλή πράξη όπου ένας ιδιοκτήτης θέλει να εξασφαλίσει το αντίτιμο που έχει συμφωνήσει με κάποιον υποψήφιο ενοικιαστή.

Με την εφαρμογή του Blockchain, τα δύο κύρια μέρη της συμφωνίας (ιδιοκτήτης- ενοικιαστής) θα μπορούν να συνάψουν ένα συμβόλαιο «αναγνώσιμο από μηχανή» (machine readable) το οποίο θα αποβάλλει από τη διαδικασία όλα τα τρίτα μέρη και η ενημέρωση όλων των αρμόδιων παρόχων και υπηρεσιών θα γίνεται άμεσα. Η δυνατότητα αποφυγής των τρίτων μερών (τράπεζες, συμβολαιογράφους, δικηγόρους) καθιστά τα Έξυπνα Συμβόλαια αρκετά ελκυστικά αφού μειώνεται αισθητά το κόστος της συναλλαγής και γίνεται αποτελεσματικότερη η διαδικασία ανάθεσης (Kõlvart, Poola, & Rull, 2016). Το Έξυπνο Συμβόλαιο θα έχει τη μορφή κώδικα όπου ουσιαστικά θα είναι ένα μηχανογραφημένο πρωτόκολλο που έχει ως κύριο στόχο την παρακολούθηση για σωστή εκτέλεση των όρων της σύμβασης (Norta, 2017). Αυτό το συμβόλαιο θα είναι καταγεγραμμένο στο Blockchain που σημαίνει ότι όλοι οι εξουσιοδοτημένοι φορείς θα έχουν άμεση πρόσβαση στα στοιχεία που τους ενδιαφέρουν. Εδώ θα πρέπει να αναφέρουμε ότι στην παρούσα φάση, ένα Έξυπνο Συμβόλαιο δεν αποτελεί ακόμα νόμιμο έγγραφο αφού δεν έχει όλες τις προϋποθέσεις που χρειάζεται για να καλύπτεται από τον περί συμβάσεων νόμο (Kõlvart, Poola, & Rull, 2016). Παίρνοντας το ακόμα παραπέρα, οι Al Khalil, Butler, O'Brien, & Ceci αναλύουν την αναγκαιότητα της ύπαρξης νομικής υποστήριξης κατά της διάρκεια της δημιουργίας των Έξυπνων Συμβολαίων ειδκότερα όταν αυτά αναφέρονται σε υπηρεσίες και τομείς που επιδεχονται αυστηρής επιτήρησης και ρυθμίσεων. Η γνώμη των δικηγόρων είναι απαραίτητη για να καθορίσει ρητά τα δικαιώματα και υποχρεώσεις των αντισυμβαλλόμενων με τρόπο που να είναι αποδεκτα από τους κανόνες της εκάστοτε βιομηχανίας που αναφέρονται (Al Khalil, Butler, O'Brien, & Ceci, 2017).

Το Ethereum είναι η βασική πλατφόρμα που δίνει τη δυνατότητα χρησιμοποίησης Έξυπνων Συμβολαίων. Ένα από τα βασικά του πλεονεκτήματα είναι η πληθώρα ευκαιριών που θα προσφέρει η αξιοποίηση τους στην καθημερινότητα των Έξυπνων Πόλεων σε αντίθεση με τις άλλες πλατφόρμες. Θα ήταν πρακτικά αδύνατο να κάναμε αναφορά σε όλους τους τομείς που έχουν εφαρμογή αλλά αναφορικά θα μπορούσαμε να σημειώσουμε την αξιοποίηση τους στην ψηφιακή υπογραφή εγγράφων, crowdfunding, ηλεκτρονική ψηφοφορία, ηλεκτρονικές δημοπρασίες και πολλά αλλά.

4.4 Πρωτόκολλα

Η τεχνολογία του Blockchain θα αναλάβει την αποθήκευση, επεξεργασία και διανομή των δεδομένων αφού αυτό θα υποστηρίζεται μέσα από τον αποκεντρωμένο τρόπο λειτουργίας της. Αυτό σίγουρα θα αποτελέσει ένα πιο ασφαλή τρόπο προσέγγισης σε αντίθεση με τις υπάρχουσες τεχνολογίες για τον τρόπο διαχείρισης των δεδομένων. Συνεπώς, θα πρέπει να εφαρμοστούν νέα χαρτοφυλάκια πρωτοκόλλων που θα μπορούν να υποστηρίξουν τη νέο-εισαχθείσα τεχνολογία. Έχουμε ήδη κάνει αναφορά στις λειτουργίες των PoW και PoS τα οποία φαίνεται να μονοπωλούν το ενδιαφέρον της κοινότητας του Blockchain λόγω της ευρείας αξιοποίησης τους από τις πλατφόρμες του Bitcoin και Ethereum αντίστοιχα. Παρόλα αυτά, σε ένα μεγάλο και πολυσύνθετο αστικό περιβάλλον όπως αυτό των έξυπνων πόλεων, αυτά τα δυο πρωτόκολλα δεν θα μπορούσαν να είναι επαρκή. Για την ώρα υπάρχουν αρκετά πρωτόκολλα που χρησιμοποιούν την πλατφόρμα του Blockchain με στόχο τη διευκόλυνση της ασφαλέστερής λειτουργίας της.

Το Proof of Activity (PoA) έχει δημιουργηθεί σαν συμπληρωματικό των ήδη αναφερθέντων πρωτοκόλλων αφού καταφέρνει να συνδυάσει τα χαρακτηριστικά και των δύο. Η αρχή της διαδικασίας είναι παρόμοια με αυτή του PoW αφού οι επίδοξοι miners ξεκινούν μια διαμάχη για το ποιος θα λύσει το κρυπτογραφικό κουίζ που θα τους επιτρέψει να διεκδικήσουν το δημιουργημένο block. Η διαφορά του από το PoW είναι ότι αντί ολόκληρου του block, θα παραληφθεί μόνο το hash της επικεφαλίδας του block. Στη συνέχεια, μπαίνει σε εφαρμογή η διαδικασία του PoS όπου διάφοροι ενδιαφερόμενοι καλούνται να επικυρώσουν μια συναλλαγή με βάση τον αριθμό των tokens που κατέχουν. Αυτό το υβριδικό πρωτόκολλο υπόσχεται έναν βελτιωμένο τρόπο τοπολογίας δικτύου που θα χρειαστεί λιγότερη ενέργεια για να λειτουργήσει. Επίσης, υπάρχουν χαμηλότερα τέλη συναλλαγών και προσφέρει αρκετά κίνητρα για τους ενδιαφερόμενους να παραμείνουν συνδεδεμένοι (Bentov, Lee, & Mizrahi, 2014).

Έχουμε ήδη κάνει αναφορά στην «επίθεση του 51%» η οποία επηρεάζει κυρίως το πρωτόκολλο PoW. Αφού οι κόμβοι μπορούν να μετατραπούν σε «εχθρούς», είναι επιτακτική ανάγκη η δημιουργία ενός πιο ασφαλούς πρωτόκολλου για την εξάλειψη της απειλής. Για το σκοπό αυτό, έχει δημιουργηθεί ένας εναλλακτικός αλγόριθμος συναίνεσης που έχει ονομαστεί Proof of Vote (PoV) και χρησιμοποιεί την πλατφόρμα του Bitcoin. Ο μηχανισμός στοχεύει να "δημιουργήσει

διαφορετική ταυτότητα ασφαλείας για τους συμμετέχοντες στο δίκτυο, έτσι ώστε η υποβολή και η επαλήθευση των blocks να αποφασίζονται από την ψηφοφορία των οργανισμών στους συνδέσμους (league) χωρίς να εξαρτάται από τρίτο διαμεσολαβητή ή ανεξέλεγκτη ευαισθητοποίηση του κοινού" (Li, Li, Hou, Li, & Chen, 2017). Σε αντίθεση με τα άλλα πρωτόκολλα (PoW και PoS), το PoV στοχεύει σε μια ελεγχόμενη ασφάλεια που θα προσφέρει λιγότερες καθυστερήσεις στον χρόνο που θα χρειάζεται για να γίνει η επαλήθευση μιας συναλλαγής.

4.5 Ιδιωτικότητα- Διαχείριση κλειδιών

Οι έξυπνες πόλεις αποτελούν μια καινούργια έννοια στη μοντέρνα εποχή και για αυτό το λόγο η διαφύλαξη της ιδιωτικότητας είναι απαραίτητη για να καταφέρουν να εδραιωθούν στην συνείδηση της κοινής γνώμης. Οι νέες τεχνολογίες θα πρέπει να είναι σε θέση να παρέχουν εμπιστοσύνη στους χρήστες, οι οποίοι στη συνέχεια θα υιοθετήσουν τις υπηρεσίες που τους προσφέρονται (Bartoli, και συν., 2011).

Κατά τη διάρκεια της επαλήθευσης της ταυτότητας του χρήστη, η σωστή και ασφαλής διαχείριση των κλειδιών θα διαδραματίσει σημαντικό ρόλο. Ειδικότερα στην εποχή του IoT, θα είναι απαραίτητα νέα είδη κρυπτογραφίας που θα είναι λιγότερο βεβαρυμμένα (lightweight cryptography schemes) για να μειώσουν τις καθυστερήσεις (latency) και τους πόρους (resources). Πρόσφατα έχουν εισαχθεί διάφορα ελαφριά κρυπτογραφικά αρχέτυπα (cryptographic primitives) για να αντικαταστήσουν τους συμβατικούς αλγορίθμους, όπως τα block ciphers, οι λειτουργίες κατακερματισμού και τα stream ciphers. Ο πολλαπλασιασμός των συνδεδεμένων συσκευών οδηγεί στην επείγουσα ανάγκη για πιο ευέλικτες λύσεις στον έλεγχο της ταυτότητας των χρηστών. Τα πλεονεκτήματα απόδοσης των lightweight ciphers είναι ότι παρέχουν μικρότερα block όπως επίσης και απλούστερα χρονοδιαγράμματα κλειδιών (key schedules) (McKay, Bassham, Sönmez, & Mouha, 2017). Τέτοια συστήματα μπορούν να εφαρμοστούν σε διάφορες πτυχές του IoT πέρα από τον έλεγχο ταυτότητας μεταξύ επεξεργαστών (machine to machine authentication). Τα ασύρματα δίκτυα θα μπορούσαν να χρησιμοποιήσουν την τεχνολογία καθώς η κατανάλωση ενέργειας, ο έλεγχος των overhead και ο μειωμένος ρυθμός απώλειας πακέτων (packet loss) αποτελούν βασικούς παράγοντες για τη βελτίωση της απόδοσης (Qin, Jia, Yang, Wang, & Ding, 2016).

4.6 Επικοινωνίες

Η ιδιωτικότητα, ανωνυμία και η ακεραιότητα είναι αναγκαίες πτυχές μέσα στο περιβάλλον των έξυπνων πόλεων. Η τεχνολογία του Blockchain είναι σε θέση να προσφέρει λύσεις στα πιο πάνω αφού αποτελούν λύσεις σε θέματα πρωταρχικής σημασίας όπως η ηλεκτρονική ψηφοφορία. Με τον παραδοσιακό τρόπο ηλεκτρονικής ψηφοφορίας, η ακεραιότητα, ιδιωτικότητα και η ανωνυμία επιτυγχάνονται μέσω ισχυρής κρυπτογραφίας. Εντούτοις, υπάρχει ένα μικρό παράθυρο αδυναμίας αυτού του είδους προστασίας ενόσω ο χρήστης αποκρυπτογραφεί το κείμενο για να το χρησιμοποιήσει. Κατά τη διάρκεια αυτού του σύντομου χρονικού κενού, οι πληροφορίες είναι σε ελεύθερη μορφή (plaintext) και ως εκ τούτου είναι ευάλωτες στην παρακολούθηση. Για να αποφευχθεί αυτός ο κίνδυνος, οι υπολογισμοί πρέπει να γίνουν χωρίς την ανάγκη αποκρυπτογράφησης των πληροφοριών.

Για αυτό το σκοπό, δημιουργήθηκε το πρωτόκολλο Enigma το οποίο χρησιμοποιεί τη πλατφόρμα του Blockchain βασισμένο σε ομοιομορφική κρυπτογραφία (homomorphic encryption). Το πρωτόκολλο δίνει τη δυνατότητα δημιουργίας υπολογισμών με βάση τα δεδομένα που είναι κρυπτογραφημένα χωρίς να είναι αναγκαία η αποκρυπτογράφηση τους (Tiwari, 2015). Με αυτό το τρόπο, διαφυλάσσεται η ιδιωτικότητα, και η ακεραιότητα της πληροφορίας. Η ομοιομορφική κρυπτογράφηση ορίζεται ως ο αλγόριθμος που επιτρέπει την εκτέλεση υπολογισμών σε κρυπτογραφημένα πεδία. Στο τέλος, οι υπολογισμοί παράγουν ένα κρυπτογραφημένο αποτέλεσμα, το οποίο αφού αποκρυπτογραφηθεί, το αποτέλεσμα παραμένει το ίδιο, σαν να έγινε ο υπολογισμός απευθείας στο απλό κείμενο (Yi, Paulet, & Bertino, 2014).

Αυτός ο τύπος πρωτοκόλλου θα μπορούσε να εφαρμοστεί σε περιπτώσεις όπου η αναγνώριση του χρήστη δεν είναι πρωταρχικής σημασίας. Για παράδειγμα, θα μπορούσε να χρησιμοποιηθεί σε (Zyskind, Nathan, & Pentland, 2015):

- Ασφαλής backend
- Τυφλή ηλεκτρονική ψηφοφορία (blind e-voting) όπου δεν απαιτείται κατανομή των ψήφων
- IoT, όπου η πηγή των πληροφοριών δεν είναι απαραίτητη π.χ. ενημερώσεις σε οδηγούς σχετικά με τροχαία ατυχήματα σε πραγματικό χρόνο
- Εσωτερική διαμερισματοποίηση (internal compartmentalization) μεγάλων οργανισμών κατά της κατασκοπείας ή δυσαρεστημένων υπαλλήλων (rogue employees).

- Ψηφιακή υπογραφή χωρίς ίχνη του ιδιωτικού κλειδιού.

Επίλογος

Μέσα από αυτή την εργασία προσπαθήσαμε να κάνουμε μια αναφορά στη τεχνολογία του Blockchain και πως αυτή θα μπορέσει να δώσει λύσεις στα ερωτήματα ασφαλείας που εγείρονται μέσα από τη μετάβαση στην εποχή του IoT και των έξυπνων πόλεων. Είδαμε τις χρήσεις του IoT και πως αυτό θα επηρεάσει την καθημερινότητα των πολιτών. Το IoT ήδη ξεκίνησε να εφαρμόζεται είτε σε βιομηχανικές μονάδες είτε για εμπορικούς σκοπούς. Οι αυτόνομες μηχανές πλέον είναι κομμάτι ενός ευρύτερου δικτύου και σαν συνέπεια αυτού του γεγονότος θα δημιουργηθούν διάφορα προβλήματα ασφαλείας τα οποία θα καλεστεί να επιλύσει η ΤΠΕ κοινότητα. Με την εφαρμογή του IoT σταδιακά μεταφερόμαστε στο κόσμο των Έξυπνων Πόλεων οι οποίες αποσκοπούν στην εκμετάλλευση της πληθώρας των δεδομένων που θα περισυλλέγονται μέσα από τη χρήση της προηγμένης τεχνολογίας με απώτερο σκοπό τη αναβάθμιση της ποιότητας ζωής. Όπως είναι φυσικό, μέσα από αυτή τη μετάβαση θα δημιουργηθεί μια νέα τάξη πραγμάτων στο τομέα της ασφάλειας. Έχουμε κάνει αναφορά στα πιο βασικά προβλήματα που θα δημιουργηθούν όπως για παράδειγμα η έλλειψη των κατάλληλων πόρων οι οποίοι θα μπορούν να αναλύσουν και να επεξεργαστούν την αφθονία των δεδομένων.

Σαν προτεινόμενη λύση που μπορεί να επιφέρει λύσεις στα προβλήματα που θα προκύψουν φαίνεται να κερδίζει έδαφος η τεχνολογία του Blockchain. Αρχικά κάναμε μια τεχνική περιγραφή της τεχνολογίας και πως λειτουργεί σε αντιδιαστολή με τον παραδοσιακό τρόπο αποθήκευσης και διακίνησής δεδομένων. Έγινε μια πιο προσεκτική ανασκόπηση στο τρόπο που δουλεύει το Blockchain και ειδικότερα στον τρόπο που δημιουργούνται τα διάφορα blocks και η διαδικασία εξόρυξης (mining). Ακολούθως, είδαμε πιο εμπεριστατωμένα τις εφαρμογές που μπορεί να έχει αυτή η τεχνολογία στην καθημερινή ζωή του ανθρώπου με παραδείγματα που αφορούν την προστασία των προσωπικών δεδομένων, την ψηφιακή ταυτοποίηση και το πιο αποδοτικό τρόπο διαχείρισης μεγαλύτερου όγκου δεδομένων. Η αποκεντρωμένη λύση στην φύλαξη των δεδομένων σε συνδυασμό με το διανεμημένο καθολικό είναι μια καλή πρώτη προσέγγιση για την εξάλειψη της ευπάθειας του single point of failure που υπάρχει στον παραδοσιακό τρόπο αποθήκευσης. Εντούτοις, υπάρχουν αρκετά μειονεκτήματα που θα πρέπει

να προσπεραστούν όπως για παράδειγμα ο χρόνος που χρειάζεται για να δημιουργηθεί ένα block λόγω του consensus mechanism που αποτελεί απαραίτητη προϋπόθεση. Για το συγκεκριμένο μειονέκτημα, η πλατφόρμα του Ethereum αξιώνει να μειώσει τον υπολογιστικό χρόνο που χρειάζεται σε 12 δευτερόλεπτα. Το πεδίο εφαρμογής του Blockchain είναι πολύ μεγάλο και θα ήταν αδύνατο να δίναμε παραδείγματα για όλους τους τομείς. Αναφερθήκαμε κυρίως στην εύρεση λύσεων στους τομείς του supply chain, της υγείας και στον άκαμπτο χρηματοπιστωτικό τομέα.

Ένα μεγάλο κομμάτι της μεταπτυχιακής διατριβής έχει καταλάβει η εφαρμογή του Blockchain στο τομέα της η-Διακυβέρνησης. Αυτή είναι μια έννοια που έχει αποκτήσει μεγάλη δυναμική τα τελευταία χρόνια με συνέπεια να βλέπουμε την εφαρμογή της σε αρκετές χώρες. Η Ευρώπη δείχνει να κρατάει τα ηνία στο συγκεκριμένο τομέα αφού υπερτερεί σε υλοποιήσιμα project των υπολοίπων ηπείρων και ειδικότερα της Αμερικής. Πιο συγκεκριμένα κάνουμε αναφορά στην Εσθονία που αυτή τη στιγμή δείχνει τον δρόμο στο θέμα της η-Διακυβέρνησης μέσα από τα διάφορα προγράμματα (e-residency) που προσφέρει σε όλους του πολίτες ανεξάρτητα από τη χώρα προέλευσης τους. Τα Έξυπνα Συμβόλαια, τα οποία εξυπηρετούνται από την πλατφόρμα του Ethereum, αποτελούν πρωτοποριακή προσθήκη στην έννοια της ηλεκτρονικής διακυβέρνησης. Προς το σκοπό αυτό, προτείναμε ένα συμβόλαιο που αποσκοπεί να αυτοματοποιηθεί η διαδικασία ενημέρωσης και διευθέτηση των λογαριασμών μεταξύ των κυβερνητικών υπηρεσιών και κάποιου η-Πολίτη που έχει αποβιώσει. Μέχρι σήμερα, είναι ευθύνη των κοντινών προσώπων να ενημερώσουν τις αρμόδιες υπηρεσίες για το γεγονός του θανάτου ενός πολίτη. Πολλές φορές η ενημέρωση είναι χρονοβόρα και δεν είναι επαρκής. Η μεταπτυχιακή διατριβή προτείνει ένα Έξυπνο Συμβόλαιο το οποίο θα «υπογραφεταί» εκ των προτέρων από τον ίδιο τον χρήστη όπου σε περίπτωση θανάτου θα γίνονται αυτόματα όλες οι διευθετήσεις για το συμβάν.

Όπως στην περίπτωση του IoT και του Blockchain, τα Έξυπνα Συμβόλαια μπορούν να εφαρμοστούν σε πολλούς τομείς των έξυπνων πόλεων αν και τα πρώτα σημάδια αδυναμιών έχουν αρχίσει να ξεπροβάλουν εκθέτοντας τα σε απειλές. Με αυτό το σκεπτικό, προτείνουμε ένα υβριδικό μοντέλο μιας έξυπνης πόλης που αποτελείται από πέντε βασικά στοιχεία που θεωρούμε απαραίτητα για τη εξασφάλιση της ασφάλειας και ιδιωτικότητας των προσωπικών δεδομένων. Το μοντέλο αυτό καλύπτει τους τομείς των πρωτοκόλλων, των επικοινωνιών, την

ασφαλή διαχείριση κλειδιών, την αυτοματοποίηση των διαδικασιών μέσα από τη χρήση των έξυπνων συμβολαίων και την ασφαλή συνδιαλλαγή με τρίτα μέρη.

Συνοψίζοντας, το Blockchain είναι ένα βασικό στοιχείο για την αποθήκευση και τη διανομή δεδομένων, το οποίο θα υποστηρίζεται από ισχυρά πρωτόκολλα ειδικά διαμορφωμένα για αυτό το σκοπό. Επιπλέον, είναι αναγκαία η δημιουργία και εφαρμογή κάποιων lightweight cryptographic primitives για τη βελτίωση του επιπέδου απόδοσης των εκατομμυρίων διασυνδεδεμένων κόμβων. Ως περαιτέρω επέκταση της μεταπτυχιακής διατριβής αυτής, θα μπορούσε να αναλυθεί το συνολικό κόστος της εφαρμογής ενός ασφαλούς έξυπνου μοντέλου πόλης. Οι Sklavos & Souras, (2006) δημιούργησαν ένα μοντέλο των διαφόρων κατηγοριών που θα πρέπει να ληφθούν υπόψη για να γίνει ενδελεχής κοστολόγηση των έξυπνων πόλεων. Τα κυριότερα στοιχεία που περιλαμβάνονται είναι ο εξοπλισμός, υλικό, το λογισμικό, οι υπηρεσίες, οι προμήθειες και το προσωπικό. Επιπλέον, είναι ζωτικής σημασίας να εξασφαλίζονται και να λειτουργούν τρίτα μέρη σε ένα αυστηρά καθορισμένο πλαίσιο, το οποίο θα τους καταστήσει υπεύθυνους σε περίπτωση παραβίασης των όρων ασφαλείας. Τα έξυπνα συμβόλαια θα βοηθήσουν στην προσπάθεια αυτή εξαλείφοντας την ανάγκη τρίτων μερών μέσω της ικανότητάς τους να δημιουργήσουν μια σύμβαση αναγνώσιμη από υπολογιστή. Τέλος, ο προτεινόμενος τρόπος έξυπνης πόλης θα πρέπει να παρέχει ισχυρά πρωτόκολλα επικοινωνίας στους πολίτες της προκειμένου να ενισχύσει την εμπιστοσύνη και να διασφαλίσει την ιδιωτικότητά τους

Παράρτημα Α

Πρόταση για Έξυπνο Συμβόλαιο για αποκατάσταση προσωπικών δεδομένων

Α.1 Σκοπός Έξυπνου Συμβολαίου

Είναι αρκετές οι περιπτώσεις που οι αρμόδιες υπηρεσίες του κράτους δεν είναι ενημερωμένες για την παρούσα κατάσταση ενός πολίτη. Πόσο μάλλον όταν αυτός ο πολίτης έχει αποβιώσει και δεν υπάρχουν κοντινοί συγγενείς για να επιληφθούν των διάφορων γραφειοκρατικών διαδικασιών που θα χρειαστούν για να «κλείσουν» οι λογαριασμοί του με το κράτος. Για παράδειγμα, πέρα από το ληξιαρχείο, θα πρέπει να ενημερωθούν οι αρμόδιες υπηρεσίες κοινωνικών ασφαλίσεων, συνταξιοδότησης (εάν δίνεται σύνταξη), κλείσιμο των κωδικών σύνδεσης στις πλατφόρμες της η-διακυβέρνησης και πολλά άλλα.

Αυτή τη στιγμή οι κρατικές υπηρεσίες εναπόκεινται στις διεργασίες των συγγενών και φίλων για να επιληφθούν όλων των πιο πάνω. Αυτή είναι μια χρονοβόρα διαδικασία για όλους και πολλές φορές μένουν αρκετές υπηρεσίες που δεν ενημερώνονται σωστά με αποτέλεσμα να σπαταλούνται πόροι και χρόνος. Υπάρχουν ακόμα και οι τραγικές περιπτώσεις που σκόπιμα δεν γίνεται η ενημέρωση των αρμοδίων υπηρεσιών έτσι ώστε να μπορούν οι πλησιέστεροι συγγενείς (next of kin) να καρπωθούν κάποιων πλεονεκτημάτων (π.χ. επίδομα σύνταξης) που θα λάμβανε ο αποθανών.

Α1.2 Η Πρόταση

Το Έξυπνο Συμβόλαιο που προτείνει αυτή η μεταπτυχιακή διατριβή έχει ως κύριο στόχο να γίνει η διαδικασία ενημέρωσης όλων των αρμοδίων υπηρεσιών σχετικά με το θάνατο ενός

προσώπου πιο αποτελεσματική, γρήγορη και ευέλικτη. Χρησιμοποιώντας τα πλεονεκτήματα που προσφέρει η τεχνολογία του Blockchain, θα μπορούν να ενημερωθούν σχεδόν ταυτόχρονα όλοι οι εμπλεκόμενοι με την ενεργοποίηση ενός ήδη δημιουργημένου Έξυπνου Συμβολαίου. Όπως έχουμε ήδη αναφέρει, μέσω του Blockchain δεν θα χρειάζεται η ενημέρωση όλων των υπηρεσιών ξεχωριστά αλλά μέσω της διανεμημένης βάσης δεδομένων θα επιτυγχάνεται η άμεση ενημέρωση τους. Τα πλεονεκτήματα που θα προκύψουν από αυτό το εγχείρημα θα είναι τα ακόλουθα:

- Τερματισμός οποιονδήποτε ωφελημάτων από το κράτος προς τον αποθανών.
- Απενεργοποίηση όλων των κωδικών που χρησιμοποιούνταν στις πλατφόρμες της η-διακυβέρνησης
- Εκκίνηση διεργασιών για την αλλαγή της κατάστασης (status) του προσώπου στα αρχεία του κράτους.
- Διευθέτηση οποιονδήποτε εκκρεμοτήτων μεταξύ προσώπου και κράτους

Α 1.3 Διαδικασία- Προϋποθέσεις

- Προφανώς, για να μπορεί να «υπογράψει» το Έξυπνο Συμβόλαιο, ο χρήστης, θα πρέπει πρώτα να είναι εγγεγραμμένος σαν η-Πολίτης όπου θα έχει τους απαραίτητους κωδικούς για να μπορεί να χρησιμοποιεί τις υπηρεσίες της η-Διακυβέρνησης.
- Μέσα από τις υπηρεσίες της η-Διακυβέρνησης θα δίνεται η δυνατότητα να δει ο χρήστης τους όρους και προϋποθέσεις του Έξυπνου Συμβολαίου και να συμπληρώσει το πιστοποιητικό/certificate (τα χαρακτηριστικά του πιστοποιητικού αναλύονται πιο κάτω) που θα είναι διαθέσιμο.
- Το πιστοποιητικό θα γίνει αποδεκτό από τη μεριά της κρατικής υπηρεσίας
- Θα ενημερωθεί το καθολικό (ledger) του Blockchain και θα μπορεί να επανακαλείται μέσα από τον μοναδικό αριθμό κατακερματισμού που θα το καθορίζει (hash number).
- Σε περίπτωση θανάτου του χρήστη, η πλατφόρμα της η-διακυβέρνησης θα είναι ανενεργή για ένα χρονικό διάστημα στο οποίο ο αποθανών προφανώς δεν θα έχει συνδεθεί. Αυτό το διάστημα θα καθοριστεί αρχικά στους 6 μήνες.

• Αφού εντοπιστεί η μηδενική ενέργεια από τον χρήστη, τότε η πλατφόρμα θα ενημερώνει τα τρία άτομα που θα έχουν προκαθοριστεί κατά τη διάρκεια της συμπλήρωσης του πιστοποιητικού για να αποτελούν τους πλησιέστερους συγγενείς (next of kin) του χρήστη.
• Τα τρία άτομα θα πρέπει επιβεβαιώσουν το γεγονός του θανάτου του χρήστη.
• Το Έξυπνο Συμβόλαιο ενεργοποιείται άμεσα.

Α.1.4 Πιστοποιητικό

Όπως αναφέρθηκε πιο πάνω, ο χρήστης θα καλεστεί να «υπογράψει» ένα πιστοποιητικό το οποίο θα καθορίσει τους όρους και προϋποθέσεις του συμβολαίου. Το πιστοποιητικό θα έχει την εξής μορφή:

Πεδίο	**Χαράκτ.**
User	sig
Officer ID	sig
E-governance ID	sig
Next of Kin 1	sig
Next of Kin 2	sig
Next of Kin 3	sig
Office issued	location
Creation	timestamp
Last modification	timestamp
Participation table	timestamp/ ring signatures

Βιβλιογραφία

Al Khalil, F., Butler, T., O'Brien, L., & Ceci, M. (2017). Trust in Smart Contracts is a Process, As Well. *FC 2017 Workshops 2017* (σσ. 510-519). Cork: International Financial Cryptography Association 2017.

AlDairi, T. (2017). Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. *The International Workshop on Smart Cities Systems Engineering* .

Ameer, R. (2017, January). *Blockgeeks*. Ανάκτηση από Proof of Work vs Proof of Stake: Basic Mining Guide: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

Amjad, M. A. (2017). Privacy Analysis of Smart City Healthcare Services. *2017 IEEE International Symposium on Multimedia.* IEEE.

Anonymous. (2017). Ethereum Contract Security Techniques and Tips. *ethereum/wiki*.

Ballesté, A. M., Pérez, P., & Solanas, A. (2013). The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City Is Possible. *IEEE Communications Magazine*, 136-141.

Bartoli, Soriano, Hernandez-Serrano, Dohler, Kountouris, & Barthel. (2011). Security and Privacy in your Smart City. *Barcelona Smart Cities Congress 2011*. Barcelona.

Bentov, I., Lee, C., & Mizrahi, A. (2014). Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake.

Beumer, J. (Σκηνοθέτης). (2015). *E-stonia - A startup country - (VPRO documentary - 2015)* [Ταινία].

Bhasin, Choudhury, Gupta, & Kumar. (2017). Smart city implementation model based on IoT. *2017 International Conference on Big Data Analytics and Computational Intelligence (ICBDAC)* (σσ. 211-216). Chirala: ICBDAC.

Bing, C. (2017, March 27). *Cyberscoop.* Ανάκτηση από Cyberscoop: https://www.cyberscoop.com/hackable-iot-washing-machine-provides-channel-breaching-hospital/

Chakrabarty, S., & Engels, D. (2016). A Secure IoT Architecture for Smart Cities. *13th IEEE Annual Consumer Communications & Networking Conference.* IEEE.

Dios, J. V. (2016, July). *Medium*. Ανάκτηση από Why We're Building the Blockchain for Healthcare : https://blog.gem.co/why-were-building-the-Blockchain-for-healthcare-bda5c09870aa

Durin, S. (2015, September 12). *Building Smart City Security*. Ανάκτηση από Techcrunch: https://techcrunch.com/2015/09/12/building-smart-city-security/

Estonia, R. o. (χ.χ.). *E-Residency*. Ανάκτηση από Republic of Estonia: https://e-resident.gov.ee/become-an-e-resident/

FORTINET. (2017, February 09). *Fortinet.* Ανάκτηση από Fortinet: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/WP-IoT.pdf

Frantz, C., & Nowostawski, M. (2016). From Institutions to Code: Towards Automated Generation of Smart Contracts. *2016 IEEE 1stt Intternattiionall Workshops on Foundattiions and Applliicattiions off Sellff-Systtems.* IEEE.

Gupta, V. (2017, February). *Harvard Business Review.* Ανάκτηση από https://hbr.org/2017/02/a-brief-history-of-Blockchain?referral=03759&cm_vc=rr_item_page.bottom

Hanna, R., Auquier, D., & Toumi. (2017, November). PHP115 - Could Healthcoin Be A Revolution In Healthcare? *Value in Health*, σ. A672.

i-scoop.eu. (2017). *The Internet of Things (IoT) – essential IoT business guide*. Ανάκτηση από i-sccop.eu: https://www.i-scoop.eu/internet-of-things-guide/#The_Internet_of_Things_in_an_infographic

Jung. (2017, January). *GreenBiz*. Ανάκτηση από IoT and Smart City trends boost smart waste collection market: https://www.greenbiz.com/article/iot-and-smart-city-trends-boost-smart-waste-collection-market

Kõlvart, M., Poola, M., & Rull, A. (2016). Smart Contracts. Στο M. Kõlvart, M. Poola, & A. Rull, *The Future of Law and eTechnologies* (σσ. 133-147). Springer, Cham.

Kshentri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, 09 22.

Kwang, T. W. (2017, 10). *eGov Innovation.* Ανάκτηση από Dubai Land Department to conduct all transactions through Blockchain: https://www.enterpriseinnovation.net/article/dubai-land-department-conduct-all-transactions-through-Blockchain-106330370

Laney, D. (2001). *3-D Data Management: Controlling Data Volume, Velocity and Variety.* MetaGroup.

Levy-Bencheton, C., & Darra, E. (2015). *Cyber security for Smart Cities.* EU: ENISA.

Li, K., Li, H., Hou, H., Li, K., & Chen, Y. (2017). Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain. *19th International Conference on High Performance Computing and Communications* (σσ. 466-473). IEEE.

Magazzeni, D., McBurney, P., & Nash, W. (2017, September). Validation and Verification of Smart Contracts: A Research Agenda. *Computer*, σσ. 50-57.

McKay, Bassham, Sönmez, & Mouha. (2017). *Report on Lightweight Cryptography.* NIST.

McWaters, J. (2016). The future of financial infrastructure. *World Economic Forum.* Deloitte Consulting LLP.

Millard, J. (2017). European Strategies for e-Governance to 2020 and Beyond. Στο M. J. Ojo A., *Government 3.0 – Next Generation Government Technology Infrastructure and Services* (σσ. 1-25). Springer, Cham.

Minelli, M. (2017, March). *Harvard Business Review.* Ανάκτηση από Blockchain Will Help Us Prove Our Identities in a Digital World: https://hbr.org/2017/03/Blockchain-will-help-us-prove-our-identities-in-a-digital-world

Minhaj, K., & Khaled, S. (2017). IoT security: Review, Blockchain solutions, and open challenges. *Future Generation Computer Systems*.

Nakamoto, S. (2008, October). *Bitcoin.org*. Ανάκτηση από https://bitcoin.org/bitcoin.pdf

Nikhil, L. (2017). Dubai Aims to Be a City Built on Blockchain. *The Wall Street Journal*.

Norta, A. (2017). *Designing a Smart-Contract Application Layer for Transacting Decentralized Autonomous Organizations* . Springer Nature Singapore Pte Ltd. 2017.

Peter, F. (2017). The Ridiculous Amount of Energy It Takes to Run Bitcoin. *Blockchain World*.

Pramanika, ∗. L. (2017, June). Smart health: Big data enabled health paradigm within smart cities. *Expert Systems With Applications*, 370-383.

Qin, Jia, Yang, Wang, & Ding. (2016). A Lightweight Authentication and Key Management Scheme for Wireless Sensor Networks. *Journal of Sensors*, 9.

Review, C. (2017). *Blockchain and IoT to Come Together as BIoT*. Ανάκτηση από CIO Review Team: https://www.cioreviewindia.com/news/Blockchain-and-iot-to-come-together-as-biot--nid-4114-cid-135.html

Rosario, N. M. (2017, March). The Emerging Blockchain Patent Landscape. *Law360*.

Roy, Siddiquee, Datta, Poddar, Ganguly, & Bhattacharjee. (2016). Smart traffic & parking management using IoT. *2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (σσ. 1-3). Vancouver: IEMCON.

Sarah, M. (2017). Building the Blockchain world: Technological commonwealth or just more of the same? *The Future of Money and Further Applications of the Blockchain*, 511–522.

Schutzer, D. (2016, January). *Financial Service Roundtable*. Ανάκτηση από CTO Corner: http://www.fsroundtable.org/cto-corner-what-is-a-Blockchain-and-why-is-it-important/

Shahzad, A., A.Y., K., & Elgamoudi, A. (2017). Secure IoT Platform for Industrial Control Systems. *2017 International Conference on Platform Technology and Service (PlatCon)* (σσ. 1-6). Busan: PlatCon.

Shen, L. (2016). *Fortune*. Ανάκτηση από http://fortune.com/2016/09/28/Blockchain-banks-2017/

Sidra Ijaz, M. A. (2016). Smart Cities: A Survey on Security Concerns . *International Journal of Advanced Computer Science and Applications,*, 612-626.

Sklavos, & Souras. (2006). Economic Models and Approaches in Information Security for Computer Networks. *International Journal of Network Security*, 14-20.

Sklavos, N., & Zaharakis, I. (2016). Cryptography and Security in Internet of Things (IoTs): Models, Schemes, and Implementations. *New Technologies, Mobility and Security (NTMS), 2016 8th IFIP International Conference.* Larnaca: IEEE.

Sklavos, Zaharakis, Kameas, & Kalapodi. (2017). Security & Trusted Devices in the Context of Internet of Things (IoT). *Euromicro Conference.* Austria: Digital System Design .

SmartCity. (2018, January 5). *Blockchain – Train of Innovative Thoughts Transforming Smart Cities*. Ανάκτηση από Smart City Press: https://www.smartcity.press/Blockchain-implementations-in-smart-cities/

Sullivan, C., & Burger, E. (2017). E-residency and Blockchain. *Computer Law & Security Review*, σσ. 470-481.

Summers, G. (2017). *Ethereum: Ethereum investing, programming, mining, Blockchains, and smart contracts; Complete User's Guide for 2018.*

Tiwari, D. (2015). *MIT'S ENIGMA: DECENTRALIZED CLOUD PLATFORM WITH GUARANTEED PRIVACY.* Ανάκτηση από Bitcoinist: http://bitcoinist.com/mit-enigma-decentralized-cloud-platform-guaranteed-privacy/

Unit, T. E. (2017). *The Internet Of Things Business Index 2017.* The Economist.

Vaas, L. (2018, February 5). *Establishing security guidelines for smart city projects*. Ανάκτηση από Hewlett Packard Enterprise: https://www.hpe.com/us/en/insights/articles/establishing-security-guidelines-for-smart-city-projects-1802.html

WorldBank. (χ.χ.). *e-Gov guideline*. Ανάκτηση από World Bank: http://siteresources.worldbank.org/INTEGOVERNMENT/Resources/e-Gov_guideline.pdf

Xiaoqi, L., Peng, J., Ting, C., Xiapu, L., & Qiaoyan, W. (2017). A survey on the security of Blockchain systems. *Future Generation Computer Systems*.

Yi, X., Paulet, R., & Bertino, E. (2014). *Homomorphic Encryption and Applications.* Springer.

Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *Security and Privacy Workshops (SPW), 2015 IEEE.* San Jose, CA, USA: IEEE.

Zyskind, G., Nathan, O., & Pentland, A. (2015). *Enigma: Decentralized Computation Platform with Guaranteed Privacy.* MIT Media Lab.