ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

BLOCKCHAINS ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΔΕΔΟΜΕΝΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΝΙΚΟΛΑΟΣ ΔΑΣΚΑΛΟΣ

Π2014219

Επιβλέπων Καθηγητής: Φοίβος Μυλωνάς

Κέρκυρα Νοέμβριος 2018

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω θερμά την οικογένειά μου για την στήριξη και την εμπιστοσύνη που μου έδειξαν όλα αυτά τα χρόνια κατά την διάρκεια των σπουδών μου και για όλα όσα μου παρείχαν.

Επίσης θα ήθελα να ευχαριστήσω τον Αναπληρωτή Καθηγητή κ. Μυλωνά Φοίβο για την υποστήριξη στην εκπόνηση της Πτυχιακής μου Εργασίας καθώς και τον πρώην Αναπληρωτή Καθηγητή κ. Σιούτα Σπυρίδων για την βοήθεια στην εύρεση του θέματος και την υποστήριξη σε πρώτη φάση.

Τέλος ένα μεγάλο ευχαριστώ στους φίλους μου για την στήριξη όλα αυτά τα χρόνια, η εργασία αυτή είναι αφιερωμένη στον Άκη.

ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ

Κέρκυρα Νοέμβριος 2018

Τίτλος Πτυχιακής Εργασίας «Blockchains και Διαχείριση Δεδομένων»

1. Επιβλέπων Καθηγητής

Φοίβος Μυλωνάς, Αναπληρωτής Καθηγητής

2.Μέλος Επιτροπής

Τσουμάκος Δημήτριος, Αναπληρωτής Καθηγητής

3.Μέλος Επιτροπής

Θεόδωρος Ανδρόνικος, Μόνιμος Επίκουρος Καθηγητής

ΠΕΡΙΛΗΨΗ

Η συγκεκριμένη Πτυχιακή Εργασία ασχολείται με την ανάλυση της τεχνολογίας Blockchain και με την εφαρμογή της σε διάφορους τομείς της κοινωνίας. Αρχικά με βάση το Bitcoin από το οποίο προέρχεται αυτή η τεχνολογία, γίνεται μια παρουσίαση του τρόπου λειτουργίας της αλλά και μια παράθεση του ανάλογου κρυπτογραφικού υπόβαθρου αυτής της τεχνολογίας. Έπειτα, γίνεται ενασχόληση με την τεχνολογία καθ' αυτή σε μεγαλύτερο βάθος αλλά και των πλεονεκτημάτων που αυτή παρέχει. Στην συνέχεια γίνεται η σύνδεσή της με σημαντικούς τομείς της κοινωνίας όπως η Υγεία, η Εκπαίδευση, το IoT και η Εταιρική Διακυβέρνηση. Τέλος παρατίθενται τα συμπεράσματα αυτής της εργασίας καθώς και οι βιβλιογραφικές πηγές που χρησιμοποιήθηκαν για την εκπόνησή της.

ABSTRACT

This Bachelor Thesis deals with the analysis of Blockchain technology and its application in various sectors of the society. Firstly, based on Bitcoin from which this technology comes, is presented the way that this technology works and after that a cryptographic background is given. Also is discussed the technology and its advantages deeper. Then Blockchain technology connects with important sectors of society such as Health, Education, IoT and Corporate Governance. Finally, the conclusions of this work are exported and the bibliographic sources are listed.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ (σελίδα 10)

ΚΕΦΑΛΑΙΟ 2: BITCOIN Η ΑΡΧΗ

- 2.1 Εισαγωγή (σελίδα 12)
- 2.2 Η Αφορμή (σελίδα 12)
- 2.3 Συναλλαγές (σελίδα 13)
- 2.4 Λύση Διπλής Δαπάνης (σελίδα 14)
- 2.5 Τρόπος Λειτουργίας και Mining (σελίδα 15)
- 2.6 Εξοικονόμηση Χώρου στον Δίσκο και Επαλήθευση Πληρωμών (σελίδα 16)
- 2.7 Συνδυασμός και Διαίρεση Αξίας (σελίδα 17)
- 2.8 Ιδιωτικότητα (σελίδα 18)

ΚΕΦΑΛΑΙΟ 3: ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

- 3.1 Κρυπτογραφία (σελίδα 19)
- 3.2 Συναρτήσεις Κατακερματισμού (Hash Functions) (σελίδα 19)
- 3.3 Ψηφιακές Υπογραφές (σελίδα 20)
- 3.4 Peer-to-Peer Δίκτυο (σελίδα 22)
- 3.5 Έξυπνα Συμβόλαια (σελίδα 23)

ΚΕΦΑΛΑΙΟ 4: BLOCKCHAINS ΚΑΙ ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ

- 4.1 Εισαγωγή στα Blockchains (σελίδα 24)
- 4.2 Τι Προσφέρουν τα Blockchains (σελίδα 24)
- 4.3 Η Τεχνολογία Blockchain (σελίδα 26)
- 4.4 Η Αγορά (σελίδα 29)

ΚΕΦΑΛΑΙΟ 5: BLOCKCHAINS ΚΑΙ ΥΓΕΙΑ

- 5.1 Από το Bitcoin στην Υγεία (σελίδα 30)
- 5.2 Κλινικές Δοκιμές (σελίδα 32)
- 5.3 Διαμοιρασμός Δεδομένων (σελίδα 33)
- 5.4 Αρχείο Ασθενών (σελίδα 34)
- 5.5 Παρακολούθηση Φαρμάκων (σελίδα 34)
- 5.6 παρακολούθηση Συσκευών (σελίδα 35)
- 5.7 Εφοδιαστική Αλυσίδα Υγείας (σελίδα 36)
- 5.8 Internet of Healthy Things (σελίδα 37)
- 5.9 Δημόσια Υγεία (σελίδα 38)
- 5.10 Αποθήκευση Δεδομένων και Ασφάλεια (σελίδα 38)

ΚΕΦΑΛΑΙΟ 6: BLOCKCHAINS ΚΑΙ ΕΚΠΑΙΔΕΥΣΗ

- 6.1 Εισαγωγή στην Εκπαίδευση (σελίδα 40)
- 6.2 Πιστοποιητικά (σελίδα 40)
- 6.2.1 Σχετικές Εργασίες (σελίδα 42)
- 6.2.2 Παράδειγμα Συστήματος με Blockchain (σελίδα 43)
- 6.2.3 Αρχιτεκτονική Συστήματος (σελίδα 44)
- 6.3 Blockchain και Διδασκαλία (σελίδα 45)
- 6.4 Μελλοντικές Εφαρμογές (σελίδα 46)
- 6.5 Τα Αρνητικά του Blockchain (σελίδα 48)

ΚΕΦΑΛΑΙΟ 7: BLOCKCHAINS ΚΑΙ IoT

- 7.1 Εισαγωγή (σελίδα 49)
- 7.2 IoT (σελίδα 49)
- 7.3 IoT και Ασφάλεια (σελίδα 51)
- 7.3.1 Αύξηση της Ασφάλειας με Blockchain (σελίδα 53)
- 7.3.1.1 Παράδειγμα Δικτύου (σελίδα 54)
- 7.3.1.2 Παράδειγμα Εφαρμογής με Κάμερα Ασφαλείας (σελίδα 55)
- 7.4 Έξυπνο Σπίτι (σελίδα 56)
- 7.4.1 Συστατικά Στοιχεία (σελίδα 56)
- 7.4.2 Τρόπος Λειτουργίας (σελίδα 58)
- 7.4.3 Ανάλυση Ασφαλείας (σελίδα 58)
- 7.5 Blockchains και IoT στον Βιομηχανικό Τομέα (σελίδα 59)
- 7.5.1 Λύσεις Εφοδιαστικής Αλυσίδας (σελίδα 59)
- 7.5.2 Λύσεις Αυτόνομων Οχημάτων (σελίδα 61)
- 7.5.3 Παραγωγή Φυτών (σελίδα 62)

ΚΕΦΑΛΑΙΟ 8: BLOCKCHAINS ΣΤΗΝ ΕΤΑΙΡΙΚΗ ΔΙΑΚΥΒΕΝΡΗΣΗ

- 8.1 Εισαγωγή (σελίδα 63)
- 8.2 Διαφάνεια Ιδιοκτησίας (σελίδα 65)
- 8.3 Βελτιώσεις στην Ρευστότητα (σελίδα 67)
- 8.4 Επιπτώσεις σε θεσμικούς Επενδυτές και Ακτιβιστές (σελίδα 68)
- 8.5 Αντίκτυπο στους Διευθυντές (σελίδα 69)
- 8.6 Επιπτώσεις στην Μικροδομή της Αγοράς (σελίδα 70)
- 8.7 Ψηφοφορία στις Εταιρικές Εκλογές (σελίδα 71)
- 8.7.1 Ακρίβεια Εκλογών (σελίδα 72)
- 8.7.2 Κενή Ψηφοφορία (σελίδα 72)
- 8.8 Λογιστική σε Πραγματικό Χρόνο (σελίδα 73)
- 8.8.1 Λογιστική και Ενδιάμεσοι Χρηματοπιστωτικοί Οργανισμοί (σελίδα 74)
- 8.8.2 Διαχείριση Εσόδων (σελίδα 74)

- 8.8.3 Συναλλαγές με Συνδεδεμένα Μέρη (σελίδα 74)
- 8.9 Διακυβέρνηση των Blockchains (σελίδα 75)

ΚΕΦΑΛΑΙΟ 9: ΣΥΜΠΕΡΑΣΜΑΤΑ

- 9.1 Υγεία (σελίδα 77)
- 9.2 Εκπαίδευση (σελίδα 78)
- 9.3 Internet Of Things (σελίδα 78)
- 9.4 Εταιρική Διακυβέρνηση (σελίδα 79)
- 9.5 Συνολικά (σελίδα 79)

ΚΕΦΑΛΑΙΟ 10: ΒΙΒΛΙΟΓΡΑΦΙΑ (σελίδα 80)

1.ΕΙΣΑΓΩΓΗ

Στην παρούσα πτυχιακή εργασία με τίτλο «Blockchains και Διαχείριση Δεδομένων» γίνεται μια προσπάθεια παρουσίασης και ανάλυσης της τεχνολογίας Blockchain και του τρόπου με τον οποίο μπορεί αυτή να εισαχθεί σε άλλες επιστήμες, με κύριο στόχο την βελτίωση των τρέχουσων διαδικασιών. Το Blockchain αποτελεί μια νέα και πολλά υποσχόμενη τεχνολογία στον τομέα της Πληροφορικής το 2018, με πολλές έρευνες και χρηματοδοτήσεις να λαμβάνουν μέρος για την εύρεση και υλοποίηση καινοτόμων εφαρμογών που βασίζονται σε αυτήν την τεχνολογία για διάφορους τομείς της κοινωνίας. Η εργασία αυτή βασίζεται σε ένα μεγάλο πλήθος επιστημονικών άρθρων και δημοσιεύσεων των τελευταίων χρόνων (2015-2018) και αναλύει και παρουσιάζει πως αυτή η τεχνολογία μπορεί να βοηθήσει προβληματικές καταστάσεις και διαδικασίες ή να δημιουργήσει νέες.

Η αρχή γίνεται με την παρουσίαση του ψηφιακού νομίσματος Bitcoin, του Satoshi Nakamoto, που αποτελεί και την πρώτη λειτουργική εφαρμογή που βασίζεται στην τεχνολογία Blockchain. Με βάση το White Paper του Nakamoto, εξηγείται αναλυτικά ο τρόπος λειτουργίας του νομίσματος, τα πλεονεκτήματά του αλλά και η επανάσταση που φέρνει στον τομέα της πληροφορικής καθώς το βασικότερο χαρακτηριστικό του είναι ότι είναι αποκεντρωμένο και δεν ελέγχεται από κάποια τρίτη έμπιστη αρχή, όλες οι συναλλαγές γίνονται ανάμεσα στους εμπλεκόμενους χωρίς να παρεμβαίνει κάποιο τρίτο μέρος. Αυτό είναι και το βασικότερο πλεονέκτημα του Blockchain και σε αυτό βασίζονται όλες οι εφαρμογές σε πολλούς τομείς.

Στην συνέχεια γίνεται αναφορά στο κρυπτογραφικό υπόβαθρο αυτής της τεχνολογίας και έπειτα αναφέρεται αναλυτικά ο τρόπος με τον οποίο λειτουργεί με βάση το παράδειγμα του Bitcoin. Παρόλο που το Bitcoin αποτελεί ένα αμφιλεγόμενο νόμισμα η τεχνολογία που τρέχει πίσω από αυτό δεν υφίστανται καμία αρνητική κριτική διότι δουλεύει αλάνθαστα από το 2008 όπου και πρωτοπαρουσιάστηκε. Είναι υπολογιστικά αδύνατο με τα σημερινά δεδομένα να σπάσει η αλυσίδα.

Έπειτα, εξετάζεται η εισαγωγή της τεχνολογίας Blockchain σε σημαντικούς τομείς της κοινωνίας όπως είναι η Υγεία, η Εκπαίδευση, το Ίντερνετ των Πραγμάτων και η Εταιρική Διακυβέρνηση. Λόγω της αποκεντρωμένης λειτουργίας αλλά και των δημόσιων συναλλαγών η τεχνολογία αυτή έχει κεντρίσει το ενδιαφέρον των επιστημόνων της πληροφορικής για την εισαγωγή της σε διάφορα πεδία, με στόχο την απλοποίηση των διαδικασιών, την δημιουργία νέων τρόπων λειτουργίας, την ταχύτερη επίτευξη των διεργασιών με μικρότερο κόστος και πολλά ακόμα που παρουσιάζονται στα επόμενα κεφάλαια.

Σχετικά με την υγεία γίνεται λόγος για τις κλινικές δοκιμές και την διαχείρισης συγκατάθεσης του ασθενούς και το πώς το Blockchain μπορεί να αυξήσει την διαφάνεια και την ελεγκτική ικανότητα. Ο διαμοιρασμός δεδομένων αποτελεί επίσης μια από τις σημαντικότερες ευκαιρίες βελτίωσης της υγειονομικής περίθαλψης, αλλά και από τις μεγαλύτερες προκλήσεις προστασίας της ιδιωτικής ζωής. Τα ηλεκτρονικά αρχεία ασθενών σε ένα Blockchain αλλά και η παρακολούθηση φαρμάκων και συσκευών είναι τομείς στους οποίους το Blockchain έχει να προσφέρει πολλά. Επιπρόσθετα αναφέρεται πως η τεχνολογία αυτή μπορεί να βοηθήσει την εφοδιαστική αλυσίδα υγείας, το IoHT (Internet of Healthy Things), την δημόσια υγεία αλλά και την παροχή ασφάλεια σε δεδομένα υγείας.

Στον τομέα της εκπαίδευσης η κύρια ενασχόληση γίνεται στον τομέα των πιστοποιητικών και στο πως τα πιστοποιητικά θα μπορούσαν να είναι σε έναν δημόσιο κατάλογο με πολλά οφέλη τόσο για τους κατόχους όσο και για τους εκδότες αλλά και εργοδότες. Εκτός από τα πιστοποιητικά αναφέρονται τρόποι με τους οποίους μπορεί το Blockchain να βοηθήσει στην διδασκαλία, στην παιδαγωγική αλλά παρουσιάζονται και μελλοντικές καινοτόμες εφαρμογές που σχετίζονται με έξυπνα συμβόλαια μεταξύ των συμμετεχόντων στην εκπαίδευση αλλά και επιβράβευση των μαθητών μέσω της αλυσίδας.

Το ίντερνετ των πραγμάτων αποτελεί έναν τομέα νέο, ο οποίος έχει μια συνεχή εξέλιξη και μια ανοδική πορεία, η τεχνολογία Blockchain έχει να προσφέρει πολλά σε αυτόν τον τομέα στην ασφάλεια και στην αύξηση της ασφάλειας IoT στον έξυπνο σπίτι, στον βιομηχανικό τομέα δίνοντας λύσεις εφοδιαστικής αλυσίδας, και βάζοντας την συζήτηση για τα αυτόνομα αυτοκίνητα σε άλλη διάσταση για πλήρη αυτόνομα οχήματα τα οποία με την χρήση έξυπνων συμβολαίων και Blockchains θα έχουν την δυνατότητα για να κάνουν και να πληρώνουν τις επισκευές ή τον ανεφοδιασμό από μόνα τους.

Η εταιρική διακυβέρνηση αποτελεί ακόμα πολύ σημαντικό τομέα της κοινωνίας στον οποίο η τεχνολογία Blockchain έχει να προσφέρει πολλά πλεονεκτήματα σε θέματα διαφάνειας ιδιοκτησίας, βελτιώσεων στην ρευστότητα, επιπτώσεις σε θεσμικούς επενδυτές και ακτιβιστές, αντίκτυπος στους διευθυντές, επιπτώσεις στην μικροδομή της αγοράς, λογιστική σε πραγματικό χρόνο αλλά και η ψηφοφορία σε εταιρικές εκλογές και γενικότερα σε εκλογικές διαδικασίες. Το Blockchain παρέχει μηχανισμούς για την βελτιστοποίηση και σε πολλές περιπτώσεις για την ριζική αλλαγή των διαδικασιών.

Στο τελευταίο κεφάλαιο παρατίθενται τα συμπεράσματα της εργασίας και στην συνέχεια η βιβλιογραφία, η οποία βασίζεται σε ξένες κυρίως επιστημονικές εργασίες των τελευταίων ετών από διακεκριμένους εκδότες και περιοδικά.

2.BITCOIN Η ΑΡΧΗ [1]

2.1 Εισαγωγή

Η αρχή έγινε 31 Οκτωβρίου του 2008 με την δημοσίευση της επιστημονικής εργασίας με τίτλο "Bitcoin¨: A Peer-to-Peer Electronic Cash System" και συγγραφέα ένα άτομο ή μια ομάδα ατόμων με το όνομα Satoshi Nakamoto. Μέχρι και σήμερα είναι άγνωστη η ταυτότητα του συγγραφέα. Η εργασία αυτή ήταν η πρώτη ολοκληρωμένη ιδέα καθώς το ίδιο έτος στις 18 Αυγούστου δημιουργήθηκε το bitcoin.org και στις 9 Νοεμβρίου το project καταχωρήθηκε στο SourceForge.net.

Η εργασία αυτή ασχολείται με την δημιουργία ενός τύπου ηλεκτρονικού χρήματος, το οποίο θα επιτρέπει διαδικτυακές πληρωμές ανάμεσα σε δύο μέρη που συναλλάσσονται, χωρίς να εμπλέκεται στην μεταφορά κάποιο χρηματοπιστωτικό ίδρυμα, δηλαδή μια τράπεζα. Το σημαντικότερο ζήτημα σε ένα τέτοιο νόμισμα είναι η διπλή δαπάνη, οι ψηφιακές υπογραφές θα μπορούσαν να δώσουν μια λύση στην οποία όμως θα έπρεπε να εμπλέκεται και μια τρίτη αξιόπιστη αρχή για να αποτρέψει την διπλή δαπάνη. Η λύση που προτάθηκε από τον Satoshi είναι ένα peer-to-peer δίκτυο, το δίκτυο κάνει χρήση χρονοσφραγίδων για τις συναλλαγές, κάνοντας hash σε μια συνεχιζόμενη αλυσίδα που βασίζεται στον κατακερματισμό και στο "proof of work", δηλαδή μια εγγραφή δεν μπορεί να αλλάξει αν δεν επαναϋπολογιστεί το "proof of work". Η μεγαλύτερη αλυσίδα δεν παρέχει μόνο την απόδειξη των γεγονότων που έχουν γίνει αλλά αποδεικνύει ότι ήρθε με την χρήση της μεγαλύτερης επεξεργαστικής ισχύς. Για όσο χρονικό διάστημα η πλειοψηφία της επεξεργαστικής ισχύς χρησιμοποιείται από κόμβους που δεν θέλουν να βλάψουν το δίκτυο, δημιουργείται μεγαλύτερη αλυσίδα και βγαίνουν οι επιτιθέμενοι εκτός. Οι κόμβοι μπορούν να εγκαταλείψουν το δίκτυο και στην συνέχεια να ξαναεισέλθουν κατά βούληση, αποδεχόμενοι το μεγαλύτερο "proof of work" της αλυσίδας ως απόδειξη του τι συνέβη όταν ήταν εκτός.

Στόχος του Satoshi ήταν η δημιουργία ενός χρήματος το οποίο δεν ελέγχεται από κάποιο χρηματοπιστωτικό ίδρυμα, αλλά από τους ίδιους τους χρήστες. Τον Ιανουάριο του 2009 δημιουργήθηκε το πρώτο μπλοκ "Genesis Block" και στις 9 Ιανουαρίου κυκλοφόρησε και ανακοινώθηκε η πρώτη έκδοση Bitcoin v0.1. Η πρώτη συναλλαγή έγινε στις 12 Ιανουαρίου του 2009 από τον Satoshi στον Hal Finney στο μπλοκ 170. Αποτελεί ένα λογισμικό ανοικτού κώδικα, οποιοσδήποτε μπορεί να το εγκαταστήσει και να γίνει μέρος του δικτύου. Η δημοτικότητά δεν έχει σταματήσει να αυξάνεται από τότε και πλέον βρίσκει εφαρμογές σε πολλά πεδία.

2.2 Η Αφορμή

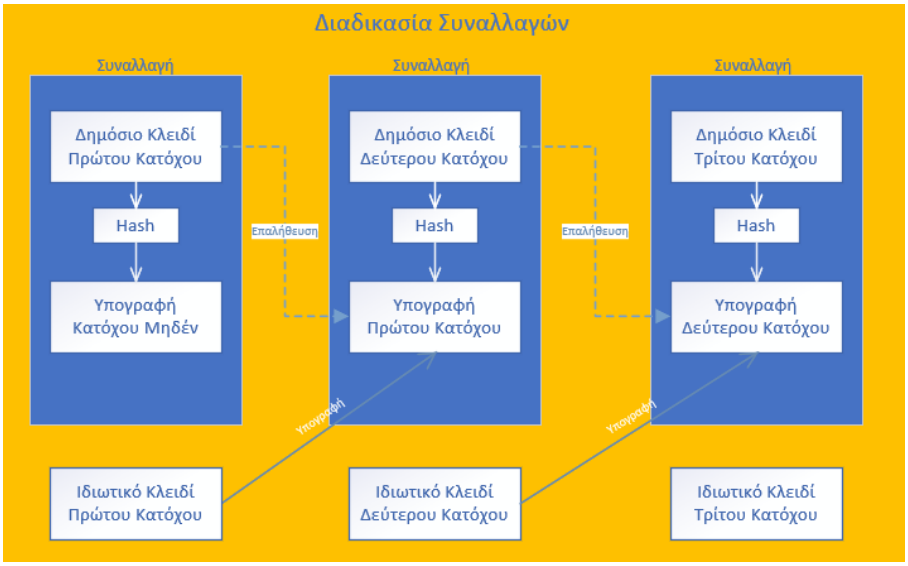
Το εμπόριο στο διαδίκτυο έχει φτάσει σε σημείο να βασίζεται αποκλειστικά στις τράπεζες, οι οποίες εξυπηρετούν ως αξιόπιστα τρίτα μέρη την επεξεργασία των συναλλαγών και την διαδικασία των ηλεκτρονικών πληρωμών. Το σύστημα αυτό λειτουργεί αρκετά καλά, αλλά έχει και κάποιες αδυναμίες οι οποίες έχουν να κάνουν με την εμπιστοσύνη. Είναι δύσκολο να γίνουν εντελώς μη αναστρέψιμες συναλλαγές, δεδομένου ότι τα χρηματοπιστωτικά ιδρύματα δεν μπορούν να αποφύγουν την διαμεσολάβηση διαφόρων. Το κόστος της διαμεσολάβησης αυξάνει και το κόστος της συναλλαγής, περιορίζοντας το κόστος του ελάχιστου μεγέθους πρακτικών συναλλαγών και μειώνοντας την

δυνατότητα για μικτές και απλές συναλλαγές. Επίσης υπάρχει ένα ευρύτερο κόστος και μια απώλεια της ικανότητας να καταβάλλονται μη αναστρέψιμες πληρωμές για αναστρέψιμες υπηρεσίες. Οι έμποροι θα πρέπει να είναι προσεκτικοί με τους πελάτες ζητώντας συνέχεια περισσότερες πληροφορίες. Ένα ορισμένο ποσοστό απάτης γίνεται αποδεκτό μέχρι και αναπόφευκτο. Το φυσικό χρήμα και οι αυτοπροσώπως συναλλαγές μπορούν να εκμηδενίσουν αυτά τα κόστη και τις αβεβαιότητες πληρωμών, αλλά δεν υπάρχει μηχανισμός για την πραγματοποίηση πληρωμών μέσω ενός καναλιού επικοινωνίας χωρίς αξιόπιστο τρίτο μέρος, δηλαδή χωρίς μια τράπεζα που ελέγχει και πραγματοποιεί την συναλλαγή.

Αυτό είναι που παρέχει το Bitcoin, ένα ηλεκτρονικό σύστημα πληρωμών το οποίο επιτρέπει σε οποιαδήποτε δύο μέρη που επιθυμούν να πραγματοποιήσουν συναλλαγές, να το κάνουν απευθείας μεταξύ τους χωρίς την ανάγκη εμπιστοσύνης σε τρίτο μέρος. Όλα τα παραπάνω βέβαια δεν μπορούν να επιτευχθούν χωρίς την κρυπτογραφία και πιο συγκεκριμένα χωρίς την κρυπτογραφική απόδειξη της εμπιστοσύνης. Συναλλαγές που δεν είναι πρακτικά εφαρμόσιμες για αντιστροφή θα προστατεύουν του πωλητές από την απάτη και οι συνήθεις μηχανισμοί θα μπορούσαν να εφαρμοστούν για την προστασία των αγοραστών. Το πρόβλημα της διπλής δαπάνης επιλύεται με την χρήση ενός peer-to-peer server με χρονοσφραγίδες και με την δημιουργία “proof of work” της χρονολογικής σειράς των συναλλαγών. Το προτεινόμενο σύστημα είναι ασφαλές για όσο χρονικό διάστημα οι καλοί κόμβοι χρησιμοποιούν περισσότερη επεξεργαστική ισχύ από τους επιτιθέμενους κόμβους στο δίκτυο.

2.3 Συναλλαγές

Το ψηφιακό νόμισμα ορίζεται ως μια αλυσίδα ψηφιακών υπογραφών. Κάθε ιδιοκτήτης μεταφέρει το κέρμα στον επόμενο υπογράφοντας ψηφιακά ένα hash της προηγούμενης συναλλαγής και το δημόσιο κλειδί του επόμενου κατόχου και την προσθήκη τους στο τέλος του νομίσματος. Ο δικαιούχος της πληρωμής μπορεί να επαληθεύσει τις υπογραφές για να επαληθεύσει και την αλυσίδα ιδιοκτησίας.

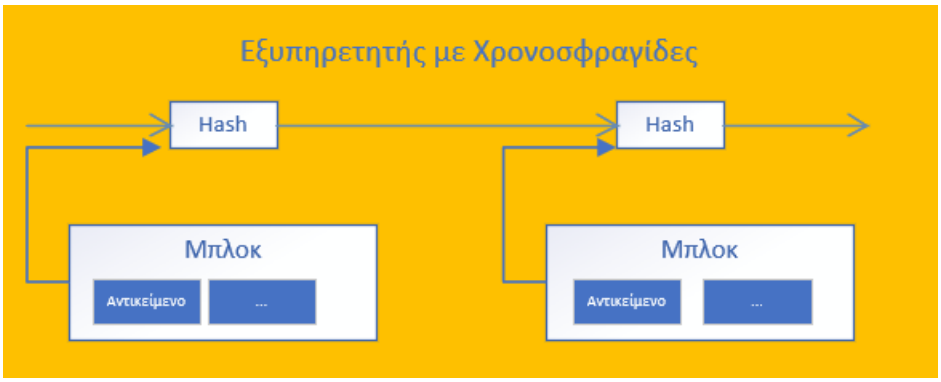


Εικόνα 1 Διαδικασία Συναλλαγών

Το πρόβλημα όπως προαναφέρθηκε είναι ότι ο δικαιούχος δεν μπορεί να επαληθεύσει ότι ένας από τους ιδιοκτήτες δεν ξόδεψε δύο φορές. Για να αποφευχθεί η λύση της κεντρικής αρχής που ελέγχει τις συναλλαγές για διπλές δαπάνες, θα πρέπει όλες οι συναλλαγές να ανακοινώνονται δημόσια, αυτό δεν μπορεί να γίνει χωρίς την ύπαρξη ενός συστήματος στο οποίο οι συμμετέχοντες συμφωνούν σε ένα ενιαίο ιστορικό παραλαβής. Ο δικαιούχος πρέπει να αποδείξει ότι κατά την στιγμή κάθε συναλλαγής η πλειονότητα των κόμβων συμφώνησε ότι ήταν η πρώτη που έφτασε.

2.4 Λύση Διπλής Δαπάνης

Η χρήση ενός εξυπηρετητή ο οποίος χρησιμοποιεί χρονοσφραγίδες μπορεί να δώσει λύση στο παραπάνω πρόβλημα. Ένας τέτοιος εξυπηρετητής δουλεύει παίρνοντας ένα hash από ένα μπλοκ με αντικείμενα που πρέπει να φέρουν χρονική σήμανση και στην συνέχεια δημοσιεύει αυτό το hash. Η χρονοσφραγίδα αποδεικνύει ότι δεδομένα υπήρχαν από πριν για να έγινε το hash. Κάθε χρονοσφραγίδα περιλαμβάνει την προηγούμενη χρονοσφραγίδα και το hash της, σχηματίζοντας έτσι μια αλυσίδα, η οποία ενισχύεται με κάθε νέα χρονοσφραγίδα.

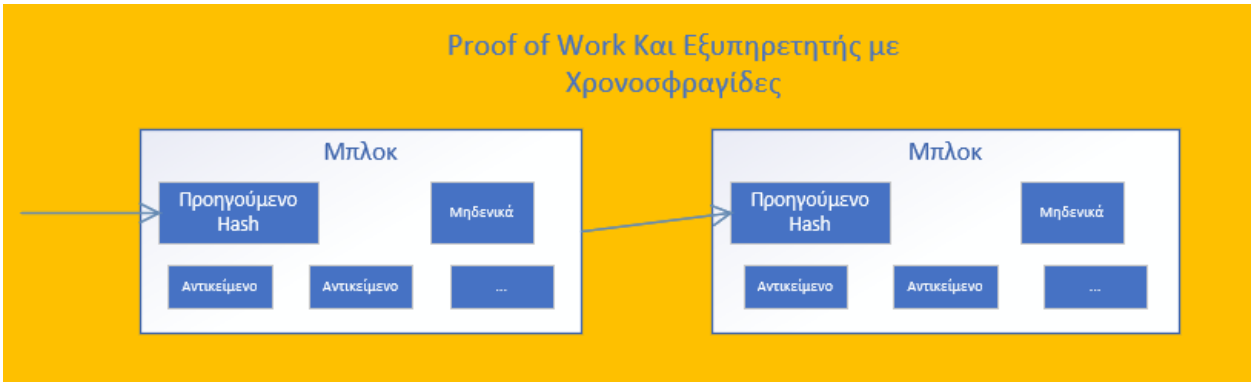


Εικόνα 2 Εξυπηρετητής με Χρονοσφραγίδες

Για την υλοποίηση του παραπάνω σε ένα peer-to-peer δίκτυο γίνεται χρήση ενός “proof-of-work”, αυτό περιλαμβάνει την σάρωση μιας τιμής, η οποία όταν περάσει από hash, το hash ξεκινάει με έναν αριθμό μηδενικών δυαδικών ψηφίων. Η μέση απαιτούμενη εργασία είναι εκθετική στον αριθμό των μηδενικών bits που απαιτούνται και μπορούν να επαληθευτούν με ένα μόνο hash. Στο συγκεκριμένο σύστημα αυξάνεται ένα μηδενικό στο μπλοκ μέχρι να βρεθεί μια τιμή που δίνει στο hash του μπλοκ τα απαιτούμενα μηδενικά bit. Όταν ο επεξεργαστής δουλέψει για την απόδειξη της εργασίας τότε το μπλοκ δεν μπορεί να αλλάξει αν δεν ξαναγίνουν όλοι οι υπολογισμοί από την αρχή. Όλα τα επόμενα μπλοκ είναι «αλυσοδεμένα» μετά από αυτό, οι εργασίες για την αλλαγή του μπλοκ θα περιλαμβάνουν την επαναφορά όλων των μπλοκ μετά από αυτό.

Η απόδειξη της εργασίας επιλύει το πρόβλημα της λήψης των αποφάσεων. Αν η πλειοψηφία βασιζόταν σε μια διεύθυνση IP μιας ψήφου, θα μπορούσε να ανατραπεί από οποιονδήποτε μπορεί να διαθέσει πολλές IP. Στην απόδειξη της εργασίας ένας επεξεργαστής ισοδυναμεί με μια ψήφο. Η απόφαση της πλειοψηφίας αντιπροσωπεύεται από την μεγαλύτερη αλυσίδα, η οποία έχει επενδύσει την μεγαλύτερη προσπάθεια αποδείξεων εργασίας μέσα σε αυτό. Αν η πλειοψηφία της ισχύς των επεξεργαστών ελέγχεται από τίμιους κόμβους, τότε η ειλικρινής αλυσίδα θα μεγαλώσει το

γρηγορότερο δυνατό και θα ξεπεράσει τις ανταγωνιστικές αλυσίδες. Για να τροποποιήσει ένας επιτιθέμενος ένα μπλοκ θα πρέπει να επαναλάβει όλους τους υπολογισμούς των μπλοκ μετά από αυτό και στην συνέχεια να καλύψει και να ξεπεράσει την εργασία των τίμιων κόμβων. Όσο πιο γρήγορα δημιουργούνται τα μπλοκ, τόσο αυξάνεται και η δυσκολία, υπάρχει ένας κινητός μέσος όρος που στοχεύει σε έναν μέσο αριθμό μπλοκ ανά ώρα.



Εικόνα 3 Proof of Work και Χρονοσφραγίδες

2.5 Τρόπος Λειτουργίας και Mining

Για να τρέξει ένα δίκτυο σύμφωνα με όλα όσα προειπώθηκαν θα πρέπει να ακολουθεί μια σειρά βημάτων. Αρχικά όλες οι νέες συναλλαγές μεταδίδονται σε όλους τους κόμβους, κάθε κόμβος συλλέγει νέες συναλλαγές σε ένα μπλοκ και προσπαθεί να βρει ένα δύσκολο proof-of-work για το μπλοκ του. Όταν το βρει, μεταδίδει το μπλοκ του σε όλους τους κόμβους, οι κόμβοι δέχονται το μπλοκ μόνο αν όλες οι συναλλαγές σε αυτό είναι έγκυρες και έχουν ήδη δαπανηθεί. Οι κόμβοι εκφράζουν την αποδοχή ενός μπλοκ, δουλεύοντας στην δημιουργία του επόμενου μπλοκ στην αλυσίδα, χρησιμοποιώντας το hash του αποδεκτού μπλοκ, όπως το προηγούμενο hash.

Οι κόμβοι θεωρούν πάντα ότι η μεγαλύτερη αλυσίδα είναι η σωστή και συνεχίζουν να εργάζονται για να την επεκτείνουν. Αν δύο κόμβοι εκπέμπουν ταυτόχρονα διαφορετικές εκδόσεις του επόμενου τμήματος, μερικοί κόμβοι μπορεί να λάβουν το ένα ή το άλλο πρώτα. Σε αυτήν την περίπτωση δουλεύουν στο πρώτο που έλαβαν, αλλά αποθηκεύουν και το άλλο κλαδί σε περίπτωση που γίνει μεγαλύτερο. Η ισοπαλία θα σπάσει όταν στην επόμενη απόδειξη εργασίας βρεθεί ότι το ένα κλαδί είναι μεγαλύτερο από το άλλο. Οι κόμβοι που δούλευαν στο πιο κοντό μεταφέρονται και λειτουργούν στο μεγαλύτερο.

Οι νέες εκπομπές συναλλαγών δεν είναι απαραίτητο να φτάσουν σε όλους τους κόμβους. Όσο φτάνουν νέοι κόμβοι, θα μπαίνουν σε ένα μπλοκ πολύ καιρό. Οι αποκλειστικές εκπομπές είναι επίσης ανεκτικές από την πτώση μηνυμάτων. Αν ένας κόμβος δεν λάβει ένα μπλοκ, θα το ζητήσει όταν λάβει το επόμενο μπλοκ και συνειδητοποιήσει ότι έλειπε ένα.

Εξ’ ορισμού, η πρώτη συναλλαγή σε ένα μπλοκ είναι μια ειδική συναλλαγή που ξεκινάει ένα νέο νόμισμα, το οποίο ανήκει στον δημιουργό του μπλοκ. Αυτό δημιουργεί ένα κίνητρο στους κόμβους να υποστηρίζουν το δίκτυο και παρέχει έναν τρόπο για την αρχική διανομή των νομισμάτων στην

κυκλοφορία, δεδομένου ότι δεν υπάρχει κεντρική αρχή για την έκδοσή τους. Η σταθερή προσθήκη μιας σταθερής ποσότητας νέων κερμάτων είναι ανάλογη με την εξόρυξη χρυσού από του ανθρακωρύχους, για την προσθήκη αυτού στην κυκλοφορία. Στην περίπτωση του Bitcoin είναι ο χρόνος της κεντρικής μονάδας επεξεργασίας και ο ηλεκτρισμός που καταναλώνεται.

Το κίνητρο αυτό μπορεί να βοηθήσει τους κόμβους να παραμείνουν ειλικρινείς. Εάν ένας άπληστος εισβολέας είναι σε θέση να συγκεντρώσει περισσότερη επεξεργαστική ισχύ από όλους τους τίμιους κόμβους, θα πρέπει να επιλέξει μεταξύ της εξαπάτησης ανθρώπων κλέβοντας πληρωμές, ή για την δημιουργία νέων νομισμάτων.

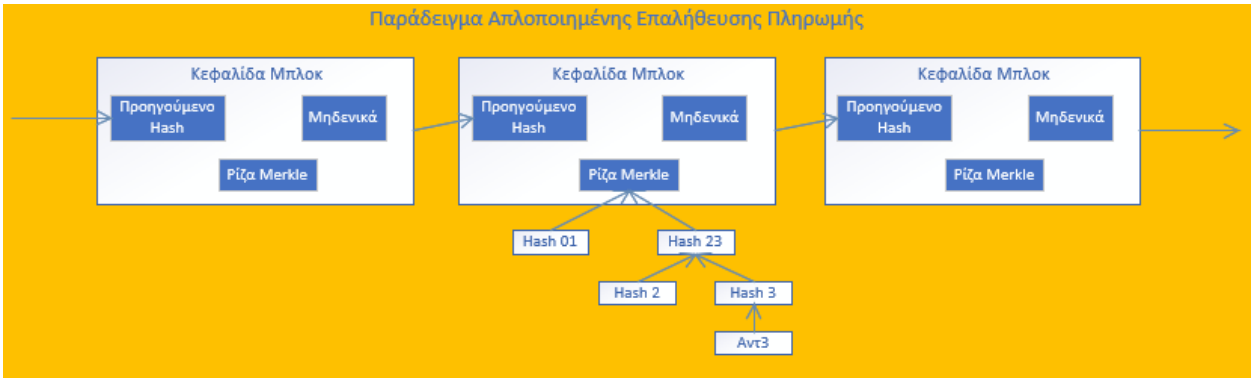
2.6 Εξοικονόμηση Χώρου στον Δίσκο και Επαλήθευση Πληρωμών

Μόλις η τελευταία συναλλαγή σε ένα κέρμα βρεθεί μετά από αρκετά μπλοκ, οι εξαντλημένες συναλλαγές πριν από αυτό μπορούν να απορριφθούν για να κερδηθεί χώρος στον δίσκο. Για την επίτευξη αυτού χρησιμοποιείται ένα Merkle Tree, ώστε να μην σπάσει το hash του μπλοκ , στο δέντρο περιλαμβάνεται μόνο η ρίζα του hash του μπλοκ.

Εικόνα 4 Merkle Tree

Μια κεφαλίδα ενός μπλοκ θα ήταν περίπου 80 bytes. Αν υποθέσουμε ότι τα μπλοκ παράγονται κάθε 10 λεπτά, 80 bytes *6*24*365=4.2MB τον χρόνο. Γίνεται λοιπόν αντιληπτό ότι ο χώρος στον δίσκο δεν αποτελεί πρόβλημα το 2018, ακόμα και αν οι κεφαλίδες θα πρέπει να διατηρηθούν στην μνήμη και όχι στον δίσκο.

Είναι δυνατή η επαλήθευση πληρωμών χωρίς την εκτέλεση ενός πλήρους κόμβου του δικτύου. Ένας χρήστης πρέπει μόνο να κρατάει ένα αντίγραφο των κεφαλίδων του μπλοκ της μακρύτερης αλυσίδας, το οποίο μπορεί να πάρει ρωτώντας κόμβους του δικτύου μέχρι να σιγουρευτεί ότι έχει την μεγαλύτερη αλυσίδα και να συνδεθεί με ένα κλαδί στο δέντρο, συνδέοντας την συναλλαγή με το μπλοκ το οποίο έχει χρονοσφραγίδα. Ο χρήστης δεν μπορεί να ελέγξει την συναλλαγή για τον εαυτό του, αλλά συνδέοντάς τον με μια θέση στην αλυσίδα, μπορεί να δει ότι ένας κόμβος του δικτύου τον έχει αποδεχθεί, και τα μπλοκ προστίθενται αφού επιβεβαιώσει περαιτέρω ότι το δίκτυο το έχει αποδεχθεί.

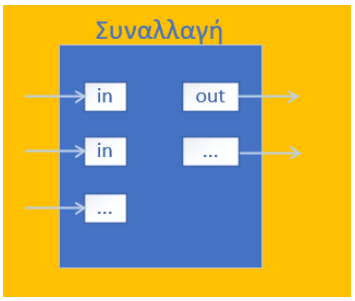


Εικόνα 5 Απλοποιημένη Επαλήθευση Πληρωμής

Ως εκ τούτου, η επαλήθευση είναι αξιόπιστη όσο οι έντιμοι κόμβοι ελέγχουν το δίκτυο, αλλά είναι ιδιαίτερα ευάλωτη όταν το δίκτυο υπερφορτωθεί από έναν εισβολέα. Ενώ οι κόμβοι του δικτύου μπορούν να επαληθεύσουν συναλλαγές για τον εαυτό τους, η απλοποιημένη μέθοδος μπορεί να ξεγελαστεί από έναν εισβολέα για όσο χρόνο αυτός υπερισχύει του δικτύου. Μια στρατηγική για την προστασία αυτού είναι να δεχτούν ειδοποιήσεις από κόμβους του δικτύου όταν εντοπίζουν ένα μη έγκυρο μπλοκ, ζητώντας από το λογισμικό του χρήστη να πραγματοποιήσει λήψη του πλήρους μπλοκ και των ειδοποιημένων συναλλαγών, για επιβεβαίωση. Οι επιχειρήσεις που λαμβάνουν συχνές πληρωμές πιθανότατα θέλουν να διαχειρίζονται τους δικούς τους κόμβους για πιο ανεξάρτητη ασφάλεια και ταχύτερη επαλήθευση.

2.7 Συνδυασμός και Διαίρεση Αξίας

Αν και είναι δυνατός ο χειρισμός των κερμάτων μεμονωμένα, θα ήταν δύσκολο να γίνει ξεχωριστή συναλλαγή για κάθε σεντ μιας μεταφοράς. Για να καταστεί δυνατή η διάσπαση και η συνδυασμένη τιμή, οι συναλλαγές περιέχουν πολλαπλές εισόδους και εξόδους. Κανονικά θα υπάρχει μια μόνο είσοδος από την μεγαλύτερη προηγούμενη συναλλαγή ή από πολλαπλές εισόδους που συνδυάζουν μικρότερες ποσότητες και το πολύ δύο έξοδοι, μια για την πληρωμή και μια για την επιστροφή της αλλαγής εάν υπάρχει, πίσω στον αποστολέα.

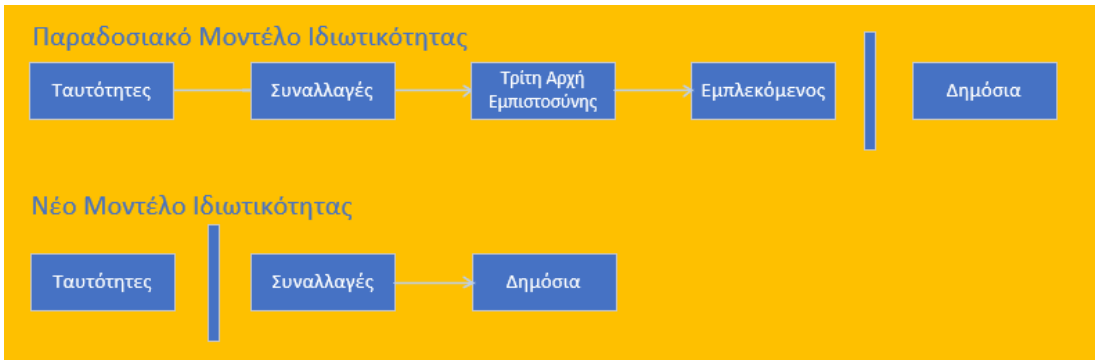


Εικόνα 6 Συναλλαγή

Θα πρέπει να σημειωθεί ότι το fan-out, όπου μια συναλλαγή εξαρτάτε από πολλές συναλλαγές, και αυτές οι συναλλαγές εξαρτώνται από πολλά άλλα, δεν αποτελεί πρόβλημα εδώ. Δεν υπάρχει ούτε ανάγκη εξαγωγής ενός πλήρους αντιγράφου του ιστορικού μιας συναλλαγής.

2.8 Ιδιωτικότητα

Το παραδοσιακό τραπεζικό μοντέλο επιτυγχάνει ένα επίπεδο προστασίας της ιδιωτικής ζωής, περιορίζοντας την πρόσβαση στην πληροφορία από τα εμπλεκόμενα μέρη και το αξιόπιστο τρίτο μέρος. Η αναγκαιότητα να ανακοινώνονται όλες οι συναλλαγές δημοσίως αποκλείει αυτήν την μέθοδο, αλλά μπορεί να διατηρηθεί η ιδιωτική ζωή παραβιάζοντας την ροή των πληροφοριών μέσα σε ένα άλλο μέρος διατηρώντας τα κλειδιά ανώνυμα. Το κοινό μπορεί να δει ότι κάποιος στέλνει ένα ποσό σε κάποιον άλλον, αλλά χωρίς τις πληροφορίες που συνδέουν τις συναλλαγές με κάποιον. Αυτό είναι παρόμοιο με το επίπεδο πληροφοριών που δημοσιεύονται από τα χρηματιστήρια, όπου ο χρόνος και το μέγεθος δημοσιοποιούνται, χωρίς όμως να λένε τα εμπλεκόμενα μέρη.



Εικόνα 7 Παραδοσιακό και Νέο Μοντέλο Ιδιωτικότητας

Ως πρόσθετο τείχος προστασίας, ένα νέο ζεύγος κλειδιών θα πρέπει να χρησιμοποιείται για κάθε συναλλαγή, ώστε να τους κρατάει συνδεδεμένους με έναν ιδιοκτήτη. Ορισμένες συνδέσεις εξακολουθούν να είναι αναπόφευκτες με πολλαπλές εισόδους οι οποίες αναγκαστικά αποκαλύπτουν ότι οι εισροές τους άνηκαν στον ίδιο ιδιοκτήτη. Το ρίσκο είναι ότι εάν αποκαλυφθεί ο ιδιοκτήτης ενός κλειδιού, η σύνδεση θα μπορούσε να αποκαλύψει και άλλες συναλλαγές που άνηκαν στον ίδιο ιδιοκτήτη.

3. ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ *[34],[35],[36],[37],[38],[39],[40],[41],[46]*

3.1 Κρυπτογραφία

Είναι η διαδικασία στην οποία βασίζεται η τεχνολογία του Blockchain, άλλωστε τα νομίσματα που έχουν δημιουργηθεί χρησιμοποιούν το πρώτο συνθετικό της λέξης αφού ορίζονται ως cryptocurrencies ή αλλιώς κρυπτονομίσματα. Η κρυπτογραφία είναι η τεχνολογία που δίνει την λύση στην τεχνολογία Blockchain.

Το προς κρυπτογράφηση μήνυμα καλείται αρχικό μήνυμα, ή απλό μήνυμα, ενώ το κρυπτογραφημένο μήνυμα καλείται κρυπτοκείμενο ή κρυπτογράφημα. Η διαδικασία μετατροπής του αρχικού μηνύματος σε κρυπτοκείμενο ονομάζεται κρυπτογράφηση. Το σύνολο των τεχνικών και δομών που χρησιμοποιούνται για την κρυπτογράφηση αποτελεί την ευρύτερη περιοχή έρευνας που είναι γνωστή ως κρυπτογραφία. Κάθε τέτοιο σύστημα ονομάζεται κρυπτογραφικό ή κρυπτογραφικός αλγόριθμος. Οι τεχνικές που χρησιμοποιούνται για την ανάκτηση ενός μηνύματος χωρίς την γνώση των χαρακτηριστικών εκείνων που χρησιμοποιήθηκαν για την κρυπτογράφηση εμπίπτουν στην περιοχή της κρυπτανάλυσης. Με απλά λόγια η κρυπτανάλυση είναι το «σπάσιμο του κώδικα». Οι περιοχές της κρυπτογράφησης περιγράφονται ενιαία με τον όρο κρυπτολογία.

Η συνάρτηση hash που χρησιμοποιείται από την τεχνολογία Blockchain αποτελεί μια κατηγορία κρυπτογραφικής συνάρτησης.

3.2 Συναρτήσεις Κατακερματισμού (Hash Functions)

Η μονόδρομη συνάρτηση κατακερματισμού ή ασφαλής συνάρτηση κατακερματισμού, είναι σημαντική όχι μόνο για την πιστοποίηση της αυθεντικότητας μηνυμάτων αλλά και για τις ψηφιακές υπογραφές.

Ο σκοπός μιας συνάρτησης κατακερματισμού είναι η παραγωγή ενός «αποτυπώματος» για ένα αρχείο, ένα μήνυμα, ή κάποιο άλλο τμήμα δεδομένων. Για να είναι χρήσιμη για πιστοποίηση αυθεντικότητας μηνύματος, μια συνάρτηση κατακερματισμού θα πρέπει να έχει τις ακόλουθες ιδιότητες.

1. Να μπορεί να εφαρμόζεται σε τμήματα δεδομένων οποιουδήποτε μεγέθους.
2. Να παράγει έξοδο συγκεκριμένου σταθερού μεγέθους.
3. Να είναι σχετικά εύκολη στον υπολογισμό για οποιοδήποτε δεδομένο Χ, καθιστώντας πρακτικά εφαρμόσιμες τις υλοποιήσεις σε υλικό και λογισμικό.
4. Για κάθε δεδομένη τιμή h, να είναι υπολογιστικά αδύνατο να βρεθεί το Χ για το οποίο H(x)=h. Αυτή η ιδιότητα αναφέρεται συχνά στην βιβλιογραφία, ως μονόδρομη ιδιότητα.
5. Για κάθε δεδομένο τμήμα Χ, να είναι υπολογιστικά αδύνατο να βρεθεί ένα Y≠X με H(x)=H(y). Αυτή αναφέρεται συχνά ως ιδιότητα ασθενούς ανθεκτικότητας σε διένεξη.
6. Να είναι υπολογιστικά αδύνατο να βρεθεί ένα ζευγάρι (x,y) τέτοιο ώστε H(x)=H(y). Αυτή αναφέρεται συχνά ως ιδιότητα ισχυρής ανθεκτικότητας σε διένεξη.

Οι τρεις πρώτες ιδιότητες αποτελούν απαιτήσεις για την πρακτική εφαρμογή μιας συνάρτησης κατακερματισμού για την πιστοποίηση αυθεντικότητας μηνυμάτων. Η τέταρτη είναι η μονόδρομη ιδιότητα. Είναι εύκολο να δημιουργήσει κάποιος έναν κωδικό με δεδομένο το μήνυμα, αλλά είναι αδύνατο να δημιουργήσει ένα μήνυμα με δεδομένο τον κωδικό. Η πέμπτη ιδιότητα εξασφαλίζει ότι είναι αδύνατο να βρεθεί ένα εναλλακτικό μήνυμα με ίδια τιμή κατακερματισμού, με το δεδομένο μήνυμα. Η έκτη ιδιότητα προστατεύει ενάντια σε μια εξελιγμένη κατηγορία επίθεσης, γνωστή ως επίθεση γενεθλίων. Μια συνάρτηση κατακερματισμού που ικανοποιεί τις πέντε πρώτες ιδιότητες αναφέρεται ως ασθενείς συνάρτηση, ενώ αν ικανοποιεί και την έκτη αναφέρεται ως ισχυρή συνάρτηση κατακερματισμού. Το Bitcoin χρησιμοποιεί μια παραλλαγή της ασφαλούς συνάρτησης κατακερματισμού SHA-256.

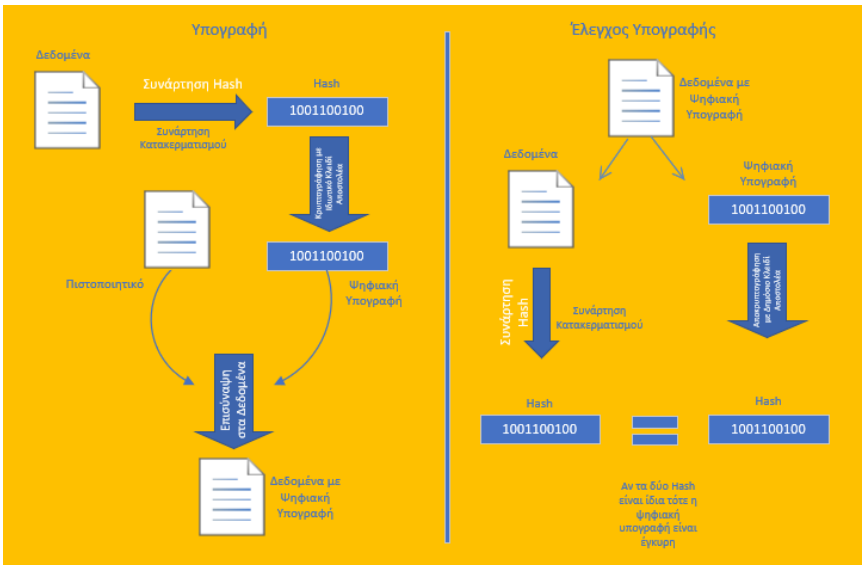
Εικόνα 8 Κρυπτογραφική Συνάρτηση SHA-1 (4 πρώτα bytes)

3.3 Ψηφιακές Υπογραφές

Έστω ότι μια οντότητα θέλει να στείλει ένα μήνυμα σε μια άλλη, και αν και δεν είναι απαραίτητο ότι το μήνυμα θα παραμείνει μυστικό, ο δέκτης θέλει να είναι σίγουρος ότι το μήνυμα προέρχεται από τον αποστολέα. Στην περίπτωση αυτή ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει το μήνυμα. Όταν ο παραλήπτης λάβει το μήνυμα, διαπιστώνει ότι μπορεί να το αποκρυπτογραφήσει με το δημόσιο κλειδί του αποστολέα, αποδεικνύοντας έτσι ότι όντως το μήνυμα στάλθηκε και κρυπτογραφήθηκε από τον αποστολέα. Κανείς άλλος δεν διαθέτει το ιδιωτικό κλειδί του αποστολέα, και έτσι κανείς άλλος δεν θα μπορούσε να δημιουργήσει ένα κρυπτογράφημα το οποίο θα μπορούσε να αποκρυπτογραφηθεί με το δημόσιο κλειδί του αποστολέα. Επομένως ολόκληρο το κρυπτογραφημένο μήνυμα λειτουργεί ως ψηφιακή υπογραφή. Επιπλέον είναι αδύνατο να τροποποιηθεί το μήνυμα χωρίς πρόσβαση στο ιδιωτικό κλειδί του αποστολέα, άρα το μήνυμα είναι πιστοποιημένο τόσο προς την προέλευση όσο και ως προς την ακεραιότητα των δεδομένων.

Εικόνα 9 Δημιουργία Κλειδιών

Συνεπώς η ψηφιακή υπογραφή είναι ένα μαθηματικό σύστημα που χρησιμοποιείται για την απόδειξη της γνησιότητας ενός ψηφιακού μηνύματος ή εγγράφου. Μια έγκυρη υπογραφή δίνει στον παραλήπτη την πιστοποίηση ότι το μήνυμα που δημιουργήθηκε ανήκει στον αποστολέα που το υπέγραψε ψηφιακά και ότι δεν αλλοιώθηκε-παραποιήθηκε κατά την μεταφορά. Οι ψηφιακές υπογραφές χρησιμοποιούν συνδυασμό μιας συνάρτησης κατακερματισμού για την δημιουργία ενός hash, σε συνδυασμό με την ασυμμετρική κρυπτογραφία για την κρυπτογράφηση και αποκρυπτογράφηση του hash. Αυτός ο συνδυασμός αποδεικνύει την ακεραιότητα του εγγράφου αλλά και την απόδειξη ταυτότητας του αποστολέα.

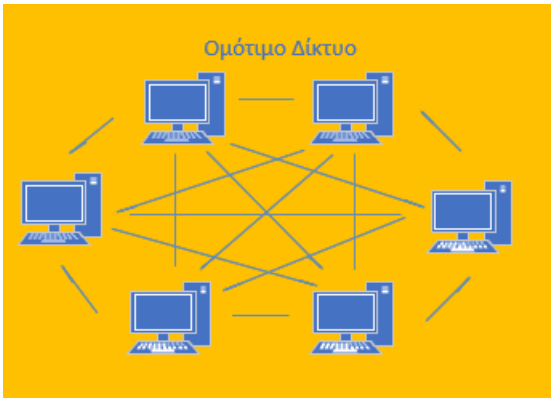


Εικόνα 10 Υπογραφή και Έλεγχος Υπογραφής

3.4 Peer-to-peer Δίκτυο

Ένα δίκτυο peer-to-peer (P2P) είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται του πόρους τους ισοδύναμα. Το δίκτυο αυτό χρησιμοποιεί την επεξεργαστική ισχύ, τον αποθηκευτικό χώρο και το εύρος ζώνης (bandwidth) των κόμβων. Όλοι οι κόμβοι του δικτύου έχουν ίσα δικαιώματα που καθορίζονται, μπορούν να διαβαστούν από όλους τους άλλους και αντίστροφα.

Ο αντίστοιχος Ελληνικός όρος είναι τα «ομότιμα δίκτυα». Στην τυπική μορφή ενός ομότιμου δικτύου, οι υπολογιστές βρίσκονται κοντά ο ένας με τον άλλον και εκτελούν παρόμοια πρωτόκολλα δικτύωσης και λογισμικό. Δεν υπάρχει υπολογιστής αφοσιωμένος στον να εξυπηρετεί τους υπόλοιπους και αυτή είναι η βασική διαφορά από την αρχιτεκτονική πελάτη-εξυπηρετητή. Κάθε κόμβος λειτουργεί ταυτόχρονα και ως πελάτης και ως εξυπηρετητής, αποτελεί μια ανοιχτή και αποκεντρωμένη αρχιτεκτονική. Ο όρος peer-to-peer αναφέρεται τόσο στις τεχνολογίες δικτύωσης όσο και στις σχετικές εφαρμογές. Στην πράξη υπάρχουν αρκετές βαθμίδες αποκέντρωσης, βάση των οποίων γίνεται κατηγοριοποίηση των ομότιμων δικτύων. Το Blockchain αποτελεί ένα ομότιμο δίκτυο.



Εικόνα 11 Ομότιμο Δίκτυο

3.5 Έξυπνα Συμβόλαια

Τα έξυπνα συμβόλαια προτάθηκαν για πρώτη φορά από τον Nick Szabo το 1994, αποτελούν πρωτόκολλα ηλεκτρονικών υπολογιστών που αποσκοπούν στην διευκόλυνση, επαλήθευση ή ακόμη και την επιβολή της διαπραγμάτευσης ή της εκτέλεσης ενός συμβολαίου στο Blockchain. Ο Szabo προτείνει ότι η έξυπνη συμβατική υποδομή μπορεί να εφαρμοστεί μέσω μητρώων επαναληπτικών περιουσιακών στοιχείων και εκτέλεσης συμβολαίων χρησιμοποιώντας κρυπτογραφικές αλυσίδες.

Ο σκοπός των έξυπνων συμβολαίων είναι να παράσχουν ασφάλεια ανώτερη από το παραδοσιακό συμβόλαιο και να μειώσουν τα κόστη συναλλαγών που συνδέονται με την σύναψη συμβολαίων. Η βασική διαφορά με τα απλά συμβόλαια είναι ότι πρόκειται για ένα αποκεντρωμένο σύστημα προσβάσιμο σε οποιονδήποτε, το οποίο δεν απαιτεί κανένα μεσολαβητικό συμβαλλόμενο μέρος και επιπλέον την ελαχιστοποίηση του κινδύνου του αντισυμβαλλόμενου, περιορίζοντας το χρόνο διακανονισμού και αυξάνοντας την διαφάνεια

Εικόνα 12 Λειτουργία Smart Contracts

4. BLOCKCHAINS ΚΑΙ ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ *[2],[42],[43],[44,[45]*

4.1 Εισαγωγή στα Blockchains

Αποτέλεσμα όλων των παραπάνω είναι η δημιουργία ενός συστήματος ηλεκτρονικών συναλλαγών το οποίο δεν βασίζεται στην εμπιστοσύνη. Το σύστημα αυτό αποτρέπει την διπλή δαπάνη καθώς είναι peer-to-peer και παράλληλα χρησιμοποιεί την απόδειξη της εργασίας, το οποίο καθιστά υπολογιστικά αδύνατο για έναν εισβολέα να επιτεθεί στο δίκτυο, διότι θα πρέπει να εκτελέσει όλες τις πράξεις από την αρχή. Οι συναλλαγές είναι όλες δημόσιες αλλά οι ταυτότητες των μερών που συναλλάσσονται παραμένουν άγνωστες. Το δίκτυο είναι απλό και ανθεκτικό, οι κόμβοι εργάζονται ταυτόχρονα με ελάχιστο συντονισμό. Δεν υπάρχει λόγος ταυτοποίησης διότι τα μηνύματα δεν πηγαίνουν σε κάποιο συγκεκριμένο μέρος, πρέπει να παραδίδονται ανάλογα με την μέγιστη δυνατή προσπάθεια. Οι κόμβοι μπορούν να βγουν και να ξαναμπούν στο δίκτυο αποδεχόμενοι την αλυσίδα απόδειξης της εργασίας ως απόδειξη του τι συνέβη όταν είχαν φύγει. Ψηφίζουν με την επεξεργαστική ισχύ τους εκφράζοντας την αποδοχή έγκυρων μπλοκ και δουλεύοντας την επέκτασή τους, τα άκυρα μπλοκ απορρίπτονται. Σε αυτό το κεφάλαιο γίνεται ανάλυση του τρόπου λειτουργίας των Blockchain με βάση όσα ειπώθηκαν στα προηγούμενα κεφάλαια. Οπότε από αυτό το σημείο γίνεται αναφορά για το Blockchain.

Ένα Blockchain είναι ουσιαστικά μια κατανεμημένη βάση δεδομένων των αρχείων ή του καταλόγου όλων των συναλλαγών ή ψηφιακά συμβάντα που έχουν εκτελεστεί και μοιράζονται οι συμμετέχοντες. Κάθε συναλλαγή στον δημόσιο κατάλογο επαληθεύεται με την συναίνεση της πλειοψηφίας των συμμετεχόντων του συστήματος. Αν οι πληροφορίες εισαχθούν μια φορά, τότε δεν μπορούν να διαγραφούν. Το Blockchain περιέχει ένα συγκεκριμένο επαληθεύσιμο αρχείο κάθε συναλλαγής που έχει γίνει. Το Bitcoin είναι το πιο δημοφιλές παράδειγμα χρήσης αυτού του μηχανισμού, αλλά και ένα από τα πιο αμφιλεγόμενα, σε αντίθεση με την τεχνολογία του blockchain η οποία βρίσκει εφαρμογές σε πολλά πεδία. Η αποδοχή είναι τεράστια και αποτελεί ένα από τα πιο πολυσυζητημένα θέματα των τελευταίων ετών με πολλές έρευνες να λαμβάνουν μέρος προσπαθώντας να εισάγουν τα πλεονεκτήματά του σε διάφορους τομείς.

Η βασική υπόθεση είναι ότι το blockchain δημιουργεί ένα σύστημα διανεμημένης συναίνεσης στον ψηφιακό online κόσμο. Αυτό επιτρέπει στις οντότητες που συμμετέχουν να γνωρίζουν με βεβαιότητα ότι ένα ψηφιακό γεγονός συνέβη, με την δημιουργία ενός αδιαμφισβήτητου αρχείου σε έναν δημόσιο κατάλογο. Ανοίγει λοιπόν την πόρτα, για την ανάπτυξη μιας δημοκρατικής, ανοιχτής και κλιμακούμενης ψηφιακής οικονομίας, από μια κεντρική. Υπάρχουν τεράστιες ευκαιρίες σε αυτήν την αποδιοργανωτική τεχνολογία και η επανάσταση σε αυτόν τον χώρο έχει μόλις αρχίσει.

4.2 Τι προσφέρει το Blockchain

Όπως προαναφέρθηκε η τεχνολογία του Blockchain σε αντίθεση με το Bitcoin δεν είναι καθόλου αμφιλεγόμενη και έχει λειτουργήσει άψογα όλα αυτά τα χρόνια, εφαρμόζετε με επιτυχία τόσο σε οικονομικές όσο και σε μη οικονομικές εφαρμογές ανά τον κόσμο. Σύμφωνα με τον Mark Andersen «Το Blockchain είναι η πιο σημαντική εφεύρεση μετά από το internet».

Η τρέχουσα ψηφιακή οικονομία βασίζεται σε μια συγκεκριμένη αξιόπιστη αρχή. Όλες οι συναλλαγές που συμβαίνουν στο διαδίκτυο βασίζονται στην εμπιστοσύνη σε κάποιον να πει την αλήθεια, είτε αυτός είναι ο πάροχος του ηλεκτρονικού ταχυδρομείου που λέει πως το mail έφτασε, είτε μια αρχή πιστοποίησης που λέει πως ένα πιστοποιητικό είναι αξιόπιστο. Θα μπορούσε επίσης να είναι μια τράπεζα που λέει πως ένα ποσό έχει παραδοθεί με επιτυχία σε πρόσωπα που βρίσκονται σε κάποια άλλη χώρα. Σύμφωνα με τα παραπάνω υπάρχει πάντα μια τρίτη οντότητα η οποία θα ασφαλίσει και θα διατηρήσει την Ιδιωτικότητα των ψηφιακών και περιουσιακών στοιχείων του καθένα. Βέβαια κανείς δεν μπορεί να εγγυηθεί ότι αυτές οι τρίτες οντότητες δεν μπορούν να παραβιασθούν.

Αυτό είναι το πρόβλημα που επιλύει η τεχνολογία Blockchain. Έχει την δυνατότητα να φέρει επανάσταση στον ψηφιακό κόσμο, επιτρέποντας έναν μηχανισμό κατανεμημένης συναίνεσης, όπου κάθε συναλλαγή γίνεται σε απευθείας σύνδεση, και συναλλαγές που έχουν γίνει στο παρελθόν μπορούν να επαληθευτούν ανά πάσα στιγμή στο μέλλον. Κάνει τα παραπάνω χωρίς να γίνονται γνωστά τα περιουσιακά στοιχεία και οι ταυτότητες των μελών. Η κατανεμημένη συναίνεση και η ανωνυμία είναι δύο από τα βασικότερα χαρακτηριστικά αυτής της τεχνολογίας.

Τα πλεονεκτήματα αυτής της τεχνολογίας αντισταθμίζουν τα ρυθμιστικά ζητήματα και τις τεχνικές προκλήσεις. Η τεχνολογία των blockchains χρησιμοποιεί επίσης τις έξυπνες συμβάσεις. Τα smart contracts είναι προγράμματα υπολογιστών που μπορούν να εκτελέσουν αυτόματα τους όρους μιας σύμβασης. Όταν πληρούνται οι όροι από τους συμμετέχοντες, τότε μπορούν να γίνουν αυτόματα πληρωμές από τους συμμετέχοντες σύμφωνα με την σύμβαση με διαφανή τρόπο.

Η έξυπνη ιδιοκτησία αποτελεί μια άλλη σχετική έννοια που αφορά τον έλεγχο της ιδιοκτησίας ενός ακινήτου ή περιουσιακού στοιχείου μέσω του Blockchain με χρήση των έξυπνων συμβολαίων. Το ακίνητο μπορεί να είναι φυσικό (σπίτι, αυτοκίνητο, κινητό τηλέφωνο) ή και μη φυσικό όπως για παράδειγμα οι μετοχές μιας εταιρείας. Αξίζει να αναφερθεί ότι και το Bitcoin δεν είναι ένα νόμισμα, αλλά έχει να κάνει με τον έλεγχο της ιδιοκτησίας των χρημάτων. Τα blockchain μπορούν να καλύψουν ένα ευρύ φάσμα εφαρμογών.

Μέσω αυτής της τεχνολογίας μπορεί να γίνει απόδειξη ύπαρξης νομικών εγγράφων, ιατρικών αρχείων, πληρωμών πιστότητας στην μουσική βιομηχανία, συμβολαίων, άδειες γάμου κλπ. Αποθηκεύοντας ένα αντίγραφο του δακτυλικού αποτυπώματος του ψηφιακού στοιχείου της αποθήκευσης του ίδιου περιουσιακού στοιχείου, μπορεί να επιτευχθεί ο στόχος ανωνυμίας και προστασίας της ιδιωτικής ζωής.

Η τεχνολογία blockchain έχει προκαλέσει μια «αναστάτωση» σε κάθε κλάδο της ψηφιακής οικονομίας, έχει την δυνατότητα να γίνει νέος κινητήρας ανάπτυξης στην ψηφιακή οικονομία, όπου όλο και περισσότερο χρησιμοποιείτε το διαδίκτυο για την διεξαγωγή ηλεκτρονικού εμπορίου αλλά και για διαμοιρασμό προσωπικών δεδομένων και γεγονότων της ζωής.

4.3 Η Τεχνολογία Blockchain

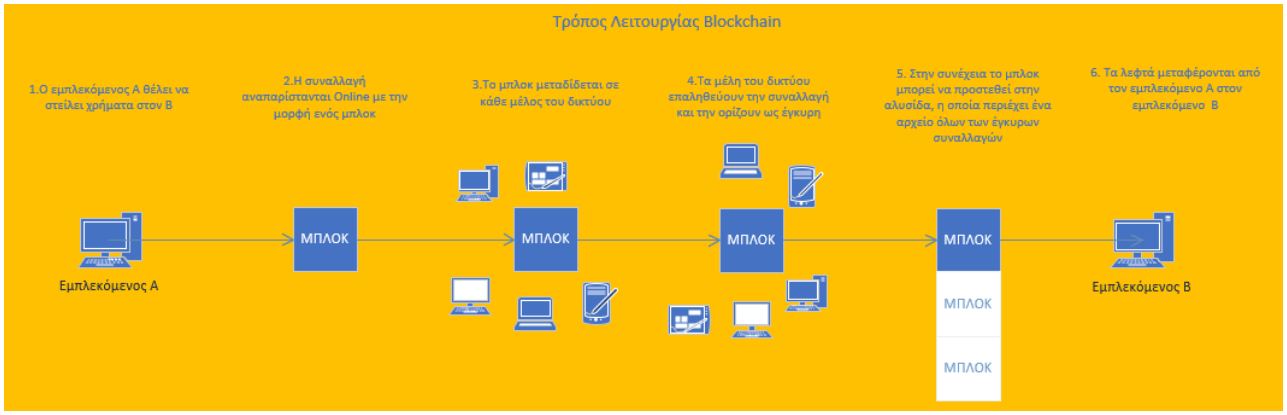
Η επεξήγηση της έννοιας του blockchain γίνεται μέσω του Bitcoin και του τρόπου λειτουργίας αυτού, άλλωστε είναι εγγενώς συνδεδεμένα μεταξύ τους, στο πρώτο κεφάλαιο αναφέρεται αναλυτικά ο τρόπος λειτουργίας του Bitcoin, σε αυτήν την ενότητα γίνεται εστίαση στην έννοια του Blockchain. Δηλαδή στην τεχνολογία η οποία μπορεί να εφαρμοσθεί σε οποιαδήποτε συναλλαγή ψηφιακών περιουσιακών στοιχείων που γίνεται ηλεκτρονικά.

Το ηλεκτρονικό εμπόριο συνδέεται αποκλειστικά με τα χρηματοπιστωτικά ιδρύματα που λειτουργούν ως αξιόπιστο τρίτο μέρος που επεξεργάζεται και διαμεσολαβεί σε οποιαδήποτε ηλεκτρονική συναλλαγή. Ο λόγος ύπαρξης τους είναι για διασφάλιση και επικύρωση των συναλλαγών, ένα ορισμένο ποσοστό απάτης είναι αναπόφευκτο στις ηλεκτρονικές συναλλαγές γι αυτό και χρησιμοποιούνται τρίτα μέρη, αποτέλεσμα αυτού είναι το υψηλό κόστος των συναλλαγών.

Εικόνα 13 Παραδοσιακό Μοντέλο Συναλλαγών

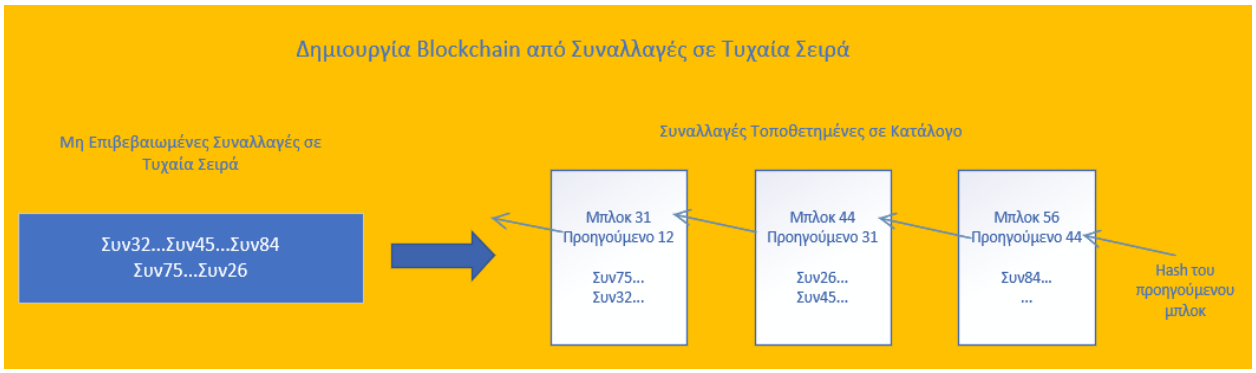
Το Bitcoin χρησιμοποιεί κρυπτογραφική απόδειξη αντί για την εμπιστοσύνη σε ένα τρίτο μέρος, για μια ηλεκτρονική συναλλαγή μέσω του διαδικτύου. Κάθε συναλλαγή προστατεύεται μέσω μιας ψηφιακής υπογραφής. Κάθε συναλλαγή αποστέλλεται στο «δημόσιο κλειδί» του δέκτη που είναι ψηφιακά υπογεγραμμένο από το «ιδιωτικό κλειδί» του αποστολέα.

Κάθε συναλλαγή μεταδίδεται σε κάθε κόμβο του δικτύου και καταγράφεται σε έναν δημόσιο κατάλογο μετά την επικύρωση. Πρέπει να επαληθεύεται η εγκυρότητα κάθε συναλλαγής πριν καταγραφεί στον δημόσιο κατάλογο. Ο κόμβος που κάνει την επαλήθευση θα πρέπει να εξασφαλίσει πριν την καταγραφή κάποιας συναλλαγής ότι αυτός που ξοδεύει είναι κάτοχος του νομίσματος (η ψηφιακή υπογραφή επικυρώνει την συναλλαγή) και ότι αυτός που ξοδεύει έχει επαρκή κρυπτογράφηση στον λογαριασμό του (ελέγχει κάθε συναλλαγή κατά τον λογαριασμό του ξενιστή στον κατάλογο για να βεβαιωθεί ότι αυτός ή αυτή έχει επαρκή υπόλοιπο στον λογαριασμό του).



Εικόνα 14 Τρόπος Λειτουργίας Blockchain

Ωστόσο υπάρχει ζήτημα διατήρησης της σειράς αυτών των συναλλαγών που μεταδίδονται σε κάθε άλλο κόμβο στο δίκτυο. Οι συναλλαγές, δεν καταφθάνουν με την σειρά με την οποία δημιουργούνται και ως εκ τούτου υπάρχει ανάγκη για ένα σύστημα που να διασφαλίζει ότι δεν θα υπάρχει διπλή δαπάνη. Λαμβάνοντας υπόψη ότι οι συναλλαγές διαπερνούν κάθε κόμβο του δικτύου, δεν υπάρχει εγγύηση ότι η σειρά με την οποία εισάγονται σε έναν κόμβο είναι η ίδια με την σειρά που δημιουργήθηκαν οι συναλλαγές. Αυτό σημαίνει ότι υπάρχει ανάγκη να δημιουργηθεί ένας μηχανισμός έτσι ώστε ολόκληρο το δίκτυο να συμφωνεί με την σειρά των συναλλαγών, πράγμα που είναι πολύ σημαντικό σε ένα κατανεμημένο σύστημα.

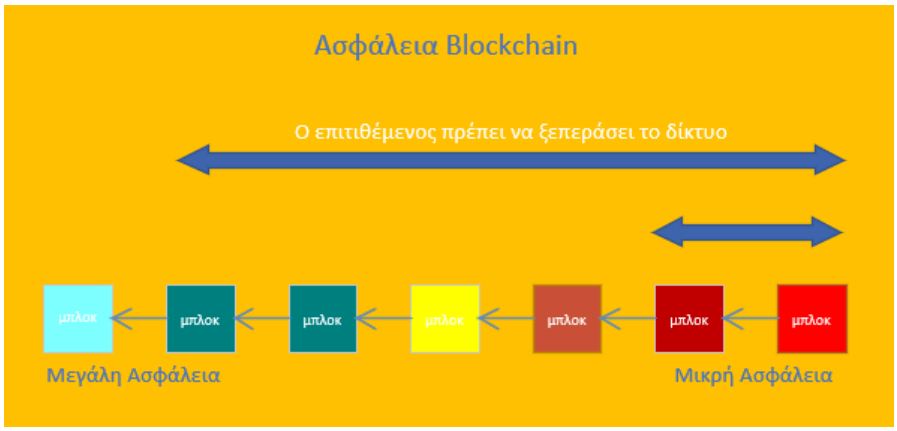


Εικόνα 15 Δημιουργία Blockchain από Συναλλαγές σε Τυχαία Σειρά

Το blockchain λύνει αυτό το πρόβλημα, οποιοσδήποτε κόμβος στο δίκτυο μπορεί να συλλέξει ανεπιβεβαίωτες τις συναλλαγές και να δημιουργήσει ένα μπλοκ. Στην συνέχεια πρέπει να μεταδώσει αυτό το μπλοκ στο υπόλοιπο δίκτυο ως πρόταση για το μπλοκ που πρέπει να είναι το επόμενο στην αλυσίδα. Μπορεί να δημιουργηθούν πολλαπλά μπλοκ από διαφορετικούς κόμβους ταυτόχρονα, δεν μπορεί να βασιστεί κανείς στην σειρά, διότι τα μπλοκ φτάνουν από διαφορετικά σημεία του δικτύου με διαφορετικές σειρές. Το πρόβλημα αυτό λύνεται με ένα μαθηματικό puzzle, κάθε μπλοκ θα είναι αποδεκτό στην αλυσίδα υπό την προϋπόθεση ότι περιέχει μια απάντηση σε ένα ιδιαίτερο μαθηματικό πρόβλημα. Δηλαδή το proof of work για το οποίο έγινε λόγος και στο προηγούμενο κεφάλαιο, ο κόμβος που δημιουργεί ένα μπλοκ πρέπει να αποδείξει ότι έχει βάλει αρκετούς υπολογιστικούς πόρους για να λύσει το μαθηματικό πρόβλημα. Η μέση απαιτούμενη προσπάθεια είναι εκθετική στον αριθμό των

μηδενικών bits που απαιτούνται, αλλά η διαδικασία επαλήθευσης είναι πολύ απλή και μπορεί να γίνει με το υπολογισμό ενός μόνο hash.

Αυτό το μαθηματικό πρόβλημα δεν είναι τετριμμένο, η επίλυσή του δεν αποτελεί μια εύκολη διαδικασία. Η πολυπλοκότητα του προβλήματος μπορεί να γίνει με τέτοιο τρόπο έτσι ώστε να θέλει μέσο χρόνο περίπου 10 λεπτά για έναν κόμβο στο δίκτυο να κάνει μια σωστή μαντεψιά και να δημιουργήσει το μπλοκ. Υπάρχει μια μικρή πιθανότητα ότι περισσότερα από ένα μπλοκ θα παράγονται στο σύστημα σε μια δεδομένη χρονική στιγμή. Ο πρώτος κόμβος για να λύσει το πρόβλημα, μεταδίδει το μπλοκ στο υπόλοιπο δίκτυο. Περιστασιακά ωστόσο, περισσότερα από ένα μπλοκ θα επιλυθούν την ίδια στιγμή, οδηγώντας σε πολλά πιθανά κλαδιά. Ωστόσο τα μαθηματικά επίλυσης είναι πολύ πολύπλοκα και ως εκ τούτου το blockchain σταθεροποιείται γρήγορα, που σημαίνει ότι κάθε κόμβος συμφωνεί για την σειρά των μπλοκ πίσω λίγο πριν το τέλος της αλυσίδας. Οι κόμβοι δίνοντας τους υπολογιστικού πόρους για να λύσουν το πρόβλημα και να δημιουργήσουν ένα μπλοκ δέχονται μια ανταμοιβή για την προσπάθεια τους, ονομάζονται ανθρακωρύχοι.



Εικόνα 16 Ασφάλεια Αλυσίδας

Το δίκτυο δέχεται μόνο την μεγαλύτερη αλυσίδα ως έγκυρη. Άρα είναι πιο δύσκολο για έναν επιτιθέμενο να εισαγάγει μια δόλια συναλλαγή, καθώς όχι μόνο πρέπει να δημιουργήσει ένα μπλοκ με την επίλυση ενός μαθηματικού προβλήματος αλλά πρέπει ταυτόχρονα να κάνει και ένα μαθηματικό αγώνα ενάντια στους υπόλοιπους καλούς κόμβους για την δημιουργία όλων των επόμενων μπλοκ, για να κάνει τους άλλους κόμβους να δεχτούν την συναλλαγή και τα μπλοκ ως έγκυρα. Αυτή η εργασία γίνεται ακόμα πιο δύσκολη καθώς τα μπλοκ της αλυσίδας είναι κρυπτογραφικά συνδεδεμένα μεταξύ τους.

4.4 Η Αγορά

Ο μηχανισμός Blockchain βρίσκει εφαρμογή τόσο σε οικονομικούς, όσο και σε μη οικονομικούς τομείς, οι οποίοι βασίζονταν παραδοσιακά σε μια τρίτη έμπιστη οντότητα για την επικύρωση και διαφύλαξη των ηλεκτρονικών συναλλαγών. Τα «Έξυπνα Συμβόλαια» που εφευρέθηκαν το 1994 από τον Nick Szabo, ήταν μια μεγάλη ιδέα για την αυτόματη εκτέλεση συμβάσεων μεταξύ των εμπλεκομένων. Ωστόσο δεν βρήκε χρήση μέχρι την δημιουργία των κρυπτογραφικών νομισμάτων ή των προγραμματιζόμενων πληρωμών. Πλέον δύο προγράμματα, τα blockchains και τα έξυπνα συμβόλαια μπορούν να λειτουργήσουν μαζί για την ενεργοποίηση πληρωμών όταν υπάρχει ενεργοποίηση μιας συμφωνίας. Τα συμβόλαια αυτά εφαρμόζονται αυτομάτως σε πρωτόκολλα υπολογιστών. Με την χρήση των Blockchains είναι πολύ πιο εύκολη η εγγραφή, επαλήθευση και εκτέλεση έξυπνων συμβολαίων. Εταιρείες ανοικτού κώδικα όπως οι Ethereum και η Codius επιτρέπουν την χρήση έξυπνων συμβολαίων με τα blockchains.

Όσον αφορά τα ηλεκτρονικά νομίσματα, πλέον έχει δημιουργηθεί ένα πλήθος από αυτά κάθε ένα από τα οποία παρέχει και διαφορετικά πλεονεκτήματα. Εκτός από το Bitcoin που είναι και το κυρίαρχο υπάρχει το Litecoin (2011) που υπόσχεται γρηγορότερη επιβεβαίωση συναλλαγών, το Ethereum (2015) που υπόσχεται την κωδικοποίηση, αποκέντρωση, ασφάλιση και συναλλαγή με οτιδήποτε, το Zcash (2017) που υπόσχεται την ασφάλεια και «σφράγιση» των συναλλαγών, το Dash (2014) που υπόσχεται ανωνυμία και μη ανιχνεύσιμες συναλλαγές, το Ripple (2012) υπόσχεται μείωση υπολογιστικής ισχύς και ελαχιστοποίηση της διαφάνειας του δικτύου, δεν επαιτεί εξόρυξη. Και ένα ακόμα μεγάλο πλήθος νομισμάτων κάθε ένα από τα οποία έχει να προσφέρει και κάτι διαφορετικό, όλα όμως βασίζονται στο πρώτο νόμισμα και τον μηχανισμό πίσω από αυτό, είναι ουσιαστικά παραλλαγές ή εξελίξεις του Bitcoin.

Έχουν δημιουργηθεί επίσης και πολλές πλατφόρμες μέσα από τις οποίες ένα χρήστης μπορεί να αγοράσει πολύ εύκολα και γρήγορα ένα νόμισμα χωρίς να απαιτεί ιδιαίτερες γνώσεις από τον χρήστη. Μια τέτοια πλατφόρμα είναι το Coinbase το οποίο παρέχει την δυνατότητα αγοράς, λειτουργεί στον ανταλλακτήριο με βάση την τρέχουσα τιμή ενός νομίσματος και ο χρήστης ανταλλάσσει πραγματικό χρήμα με ηλεκτρονικό.

Το blockchain είναι ένα από τα πιο πολυσυζητημένα θέματα τα τελευταία χρόνια και πολλές έρευνες γίνονται για το που μπορεί να εφαρμοσθεί και τι πλεονέκτημα μπορεί να προσφέρει σε κάθε κλάδο. Υπάρχουν εφαρμογές αυτού στην υγεία, στην Ιδιωτικότητα, στην εκπαίδευση, στην μηχανική, στο IOT(internet of things) και σε πολλά ακόμα πεδία που αναλύονται στα επόμενα κεφάλαια. Δεν είναι τυχαίο το ότι η Ευρωπαϊκή Ένωση ετοιμάζει έναν πανευρωπαϊκό οργανισμό για την τεχνολογία Blockchain, θέλοντας να ηγηθεί των εξελίξεων. Στόχος αυτού ο εντοπισμός και η ανάλυση των τεχνολογικών και οργανωτικών τάσεων σχετικά με τα αναδυόμενα θέματα με έναν ευέλικτο τρόπο. Στόχοι του αποτελούν ο εντοπισμός των υφιστάμενων πρωτοβουλιών, η παρακολούθηση και η ανάλυση των εξελίξεων και των τάσεων καθώς και πιθανές επιπτώσεις σχετικά με κινδύνους και ευκαιρίες στην Ευρώπη. Επίσης η ανάπτυξη και η παροχή εξειδικευμένων γνώσεων καθώς και της υποστήριξης της γνώσης, αλλά και η δημιουργία ενός forum για την συνεργασία με ενδιαφερόμενα μέρη, για ανταλλαγή εμπειριών, προβληματισμών και δημιουργία ειδικών δράσεων

5. BLOCKCHAINS ΚΑΙ ΥΓΕΙΑ [3],[4],[5],[6],[7],[8],[9]

5.1 Από το Bitcoin στην Υγεία

Η τεχνολογία Blockchain είναι μια από τις πιο πολυσυζητημένες τα τελευταία χρόνια και πολλά δισεκατομμύρια δίνονται για νέες ιδέες και νεοφυής επιχειρήσεις, με τον αριθμό αυτών να αυξάνεται συνεχώς. Πλέον η τεχνολογία αυτή δεν χρησιμοποιείται μόνο για το Bitcoin ή και αντίστοιχα νομίσματα αλλά βρίσκει εφαρμογή σε ένα τεράστιο εύρος πεδίων. Ένα από τα σημαντικότερα πεδία αποτελεί η υγεία.

Υπάρχουν πολλές διαφορές μεταξύ της τεχνολογίας Blockchain και της παραδοσιακής τεχνολογίας βάσεων δεδομένων. Στην παραδοσιακή τεχνολογία πληροφορικής κάθε οργανισμός διαχειρίζεται και εξασφαλίζει τα δικά του δεδομένα, κάτι εντελώς αντίθετο από την λογική της τεχνολογίας του Blockchain. Στο νέο αυτό μοντέλο, ένα υποσύνολο του συνόλου των δεδομένων ενός οργανισμού μετατρέπεται σε κοινόχρηστο στοιχείο μεταξύ των συμμετεχόντων στο δίκτυο, οι οποίοι συγχρονίζονται και διαχειρίζονται με συναίνεση αυτά τα δεδομένα μέσω πρωτοκόλλων και κανόνων που κωδικοποιούνται στο πλαίσιο του Blockchain. Η εμπιστευτικότητα, η ακεραιότητα και τα συμβατικά δικαιώματα επιτυγχάνονται μέσω αυτών των ισχυρών κρυπτογραφικών τεχνικών, με συναρτήσεις κατακερματισμού δημόσια και ιδιωτικά κλειδιά.

Η υγεία και η υγειονομική περίθαλψη είναι ένα σύστημα το οποίο αποτελείται από πολλά συστατικά στοιχεία όπως οι ασθενείς, οι εγκαταστάσεις για την παροχή φροντίδας, οι προμηθευτές φαρμάκων και εξοπλισμού, τον προσωπικό υγειονομικής περίθαλψης όπως το εργατικό δυναμικό για την παροχή υπηρεσιών αλλά και εκπαιδευτικά ιδρύματα για την κατάρτιση του εργατικού δυναμικού. Επίσης μέρος αυτού αποτελούν και οι πληρωτές αλλά και οι μηχανισμοί χρηματοδότησης της κυβέρνησης.

Τα περισσότερα δεδομένα στον τομέα της υγειονομικής περίθαλψης υπάρχουν σε βάσεις δεδομένων εντός των επιχειρησιακών εφαρμογών που αναπτύσσεται από μεμονωμένες οργανώσεις υγειονομικής περίθαλψης. Υπάρχει μια μεγάλη δυνατότητα, αυτή του διαμοιρασμού των δεδομένων της υγειονομικής περίθαλψης μεταξύ των δικτύων των οργανισμών, με στόχο την βελτίωση της ποιότητας φροντίδας των ασθενών αλλά και την μείωση του κόστους. Ο τομέας της υγείας έχει ήδη διάφορους τύπους δικτύων όπως τις εφοδιαστικές αλυσίδες φαρμάκων, δίκτυα πιστοποίησης προμηθευτή, ανταλλαγές πληροφοριών υγείας και άλλα.

Αυτά τα υφιστάμενα δίκτυα αντιπροσωπεύουν βραχυπρόθεσμα ευκαιρίες για το Blockchain. Σε αυτά τα δίκτυα το Blockchain έχει την δυνατότητα να αυξήσει τα επιχειρηματικά συστήματα και να ενεργοποιήσει τον ασφαλή διαμοιρασμό των δεδομένων υγείας των ασθενών, με στόχο την βελτίωση της φροντίδας αυτών και της μείωσης του κόστους.

Υπάρχουν πολλοί τομείς υγειονομικής περίθαλψης και ευεξίας που θα μπορούσαν να ενισχυθούν με την χρήση των Blockchains. Τέτοιοι τομείς είναι παρακολούθηση συσκευών, οι κλινικές δοκιμές, ο εντοπισμός/παρακολούθηση φαρμάκων, η ασφάλεια υγείας και άλλες πολλές που αναφέρονται στην συνέχεια. Στο πλαίσιο της παρακολούθησης συσκευών τα νοσοκομεία μπορούν να

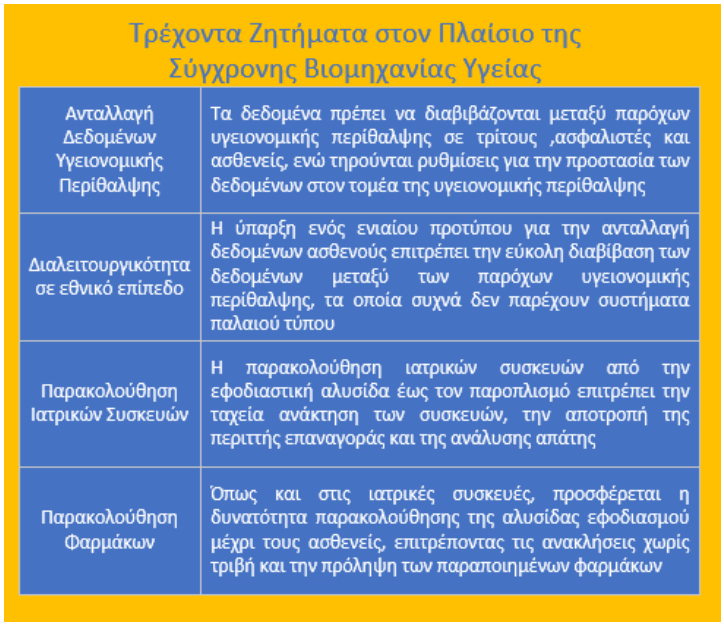
ανιχνεύσουν τα περιουσιακά τους στοιχεία μέσα σε μια υποδομή Blockchain, συμπεριλαμβανομένου και του πλήρους κύκλου ζωής μιας συσκευής. Οι πληροφορίες που συλλέγονται μπορούν στην συνέχεια να χρησιμοποιηθούν για την βελτίωση της ασφάλειας των ασθενών και την παροχή αναλύσεων μετά την αγορά, με στόχο την βελτίωση της απόδοσης.

Η υγειονομική περίθαλψη αποτελεί ένα «ευαίσθητο» τομέα, με την έννοια του ότι μπορούν να δημιουργηθούν εύκολα διαταραχές λόγο των προβλημάτων που υπάρχουν στον κλάδο. Το Blockchain μπορεί να δώσει λύση σε αυτά τα προβλήματα μέσω της αμεταβλητότητας του, της πρόληψης απάτης και της δυνατότητας ανταλλαγής δεδομένων μεταξύ των οργανισμών χωρίς να χρειάζεται εμπιστοσύνη σε κάποιο τρίτο μέρος.

Μια βασική πρόκληση όπως εντοπίστηκε από τους Frost & Sullivan, είναι η επισήμανση του ιατρικού εξοπλισμού με ένα εύκολα χρησιμοποιήσιμο αναγνωριστικό και η ενσωμάτωση εμπιστοσύνης στον εντοπισμό και την παρακολούθηση της συσκευής. Όταν μια συσκευή, όπως μια αντλία έγχυσης φαρμάκων φαίνεται να έχει μια δυσλειτουργία, η παρακολούθηση της συσκευής μπορεί να αποκαλύψει την πηγή του προβλήματος και να αποτρέψει νέα αγορά σε περίπτωση χαμένων συσκευών. Μια ισχυρή υποδομή εμπιστοσύνης που βασίζεται στον εντοπισμό ιατρικών συσκευών είναι πιθανό να μειώσει αυτές τις απειλές.

Εντός της φαρμακευτικής βιομηχανίας, το Blockchain μπορεί να βοηθήσει στην ελάττωση των αυξανόμενων κινδύνων που αφορούν πλαστά και μη εγκεκριμένα φάρμακα. Όπως και με την παρακολούθηση συσκευών, είναι δυνατόν να οριστούν έξυπνα συμβόλαια φαρμάκων και στην συνέχεια να γίνεται εντοπισμός των δοχείων των χαπιών, με ενσωματωμένο GPS σε συνδυασμό με την τεχνολογία Blockchain.

Σε κλινικές δοκιμές η τεχνολογία αυτή μπορεί να χρησιμοποιηθεί για να ξεπεραστούν τα προβλήματα των παραπλανητικών αποτελεσμάτων και της απομάκρυνσης των δεδομένων, τα οποία δεν υποστηρίζουν την πρόθεση του ερευνητή ή της πηγής χρηματοδότησης. Αυτό θα ενισχύσει την ακεραιότητα στις κλινικές δοκιμές. Επιπλέον επιτρέπει την διατήρηση ενός αμετάβλητου αρχείου καταγραφής της συγκατάθεσης του υποκειμένου. Θεωρείται ότι η φαρμακευτική βιομηχανία θα μπορούσε να επωφεληθεί από εξοικονόμηση δισεκατομμυρίων δολαρίων με την δημιουργία ενός blockchain για την εφοδιαστική αλυσίδα.



Εικόνα 17 Ζητήματα Υγείας

Με την ασφάλιση υγείας πολλοί τομείς θα μπορούσαν να επωφεληθούν από ένα αξιόπιστο αρχείο καταγραφών που αφορούν τους ασθενείς, συμπεριλαμβανομένης της βελτιωμένης αναφοράς περιστατικών και της αυτοματοποίησης των δραστηριοτήτων Οι συμβάσεις θα μπορούσαν επίσης να οριστούν σαφώς και στην συνέχεια να τεθούν σε ισχύ, όπως αυτοματοποιημένες πληρωμές για θέματα που αφορούν τους ασθενείς

Στην συνέχεια γίνεται ανάλυση των παραπάνω αλλά και άλλων εφαρμογών Blockchain που μπορούν να βοηθήσουν διάφορους τομείς την υγειονομικής περίθαλψης.

5.2 Κλινικές Δοκιμές

Οι κλινικές δοκιμές και η διαχείριση της συγκατάθεσης του ασθενούς είναι ένας τομέας όπου το blockchain έχει την δυνατότητα να αυξήσει την διαφάνεια, την ελεγκτική ικανότητα και την υπευθυνότητα των γιατρών και των ερευνητών.

Διατηρώντας έναν κατάλογο ασθενούς ο οποίος δεν μπορεί να αλλάξει ή να παραβιασθεί, οι ρυθμιστικές αρχές μπορούν να παρακολουθήσουν τα πρότυπα των κλινικών δοκιμών, εξασφαλίζοντας ότι η δοκιμή πληρή τους κανονισμούς περί συναίνεσης της εκάστοτε χώρας. Αυτό είναι ιδιαίτερα σημαντικό δεδομένου ότι οι τυποποιημένες μορφές συγκατάθεσης συγκαταλέγονται μεταξύ των πιο συνηθισμένων τύπων κλινικής απάτης. Απάτη όπως η επεξεργασία των αρχείων και η παραποίηση συγκατάθεσης των ασθενών, πράγμα που σημαίνει ότι είναι αναγκαίο να υπάρχει ένα επίπεδο αυθεντικότητας για να αποφευχθεί αυτό. Αυτό το σύστημα θα μπορούσε να ενισχυθεί ακόμα περισσότερο όπως προτείνετε από τους Benchoufi, Porter και Ravaud, εφαρμόζοντας ένα σύστημα έξυπνων συμβάσεων που εμποδίζει τους κλινικούς γιατρούς να χρησιμοποιούν δεδομένα ασθενών μέχρι να απελευθερωθεί ένα κλειδί στον τέλος μιας έξυπνης σύμβασης, που απαιτεί συγκατάθεση σε κάθε στάδιο δοκιμής.

Η διαδικασία αυτή θα πρέπει επίσης να επιτρέπει την ανάκληση της συγκατάθεσης του ασθενούς. Με την χρήση της τεχνολογίας blockchain στις κλινικές δοκιμές, τα κλινικά πειράματα έχουν την ιδιοκτησία των δικών τους δεδομένων, ενώ παράλληλα παρέχουν μια διαδρομή ελέγχου για το κλινικό προσωπικό, τους ερευνητές και τις ρυθμιστικές αρχές.

5.3 Διαμοιρασμός Δεδομένων

Ο διαμοιρασμός δεδομένων αποτελεί μια από τις μεγαλύτερες ευκαιρίες βελτίωσης της υγειονομικής περίθαλψης, αλλά και μια από τις μεγαλύτερες προκλήσεις προστασίας της ιδιωτικής ζωής. Οι Powles και Hodson, αντιμετωπίζουν την ανάγκη να υπάρχει διαφάνεια σχετικά με τον τρόπο με τον οποίο τα δεδομένα των ασθενών μοιράζονται σε τρίτα μέρη, χρησιμοποιώντας μια μελέτη περίπτωσης. Η έλλειψη συγκατάθεσης του ασθενούς στην προηγούμενη μελέτη περίπτωσης θεωρείται ως ένα από τα σημαντικότερα ζητήματα, παρά το θετικό αποτέλεσμα που είχε η σειρά προϊόντων της Google για την διάγνωση και θεραπεία των ασθενών. Στο αντίθετο άκρο η IBM και η Αμερικάνικη Ένωση άπνοιας ύπνου, χρησιμοποίησαν τον υπερυπολογιστή Watson της IBM για να μελετήσουν την άπνοια ύπνου σε χιλιάδες αμερικάνους στο σπίτι, με σαφή ενημερωμένη συγκατάθεση των ασθενών για την επίλυση σημαντικών προκλήσεων στην υγειονομική περίθαλψη.

Είναι σημαντικό να υπάρχει ένα εθνικό πρότυπο διαλειτουργικότητας στις υπηρεσίες πληροφορικής που υπάρχουν στον τομέα της υγειονομικής περίθαλψης. Η σημασία της διαλειτουργικότητας όσο αφορά στην πρόσβαση σε ηλεκτρονικά αρχεία υγείας ασθενών σε πολλά νοσοκομεία, από συστήματα που έχουν δημιουργηθεί από διαφορετικούς οργανισμούς είναι πολύ σημαντική. Αυτό το γεγονός δημιουργεί προβλήματα στους γιατρούς και τους νοσηλευτές, διότι οι περισσότερες εργασίες εξακολουθούν να γίνονται με τον παραδοσιακό τρόπο.

Η παρακολούθηση στοιχείων ιατρικών συσκευών αποτελεί ένα σημαντικό πρόβλημα στον τομέα της υγειονομικής περίθαλψης. Μια έρευνα από τον Harland Simon, σχετικά με ένα έργο που αφορά την σήμανση των ιατρικών συσκευών με RFID, επιβεβαίωσε ότι το 15% των περιουσιακών στοιχείων ενός νοσοκομείου χάνονται κάθε χρόνο, πράγμα που συνεπάγεται μεγάλο κόστος για την επαναγορά αντικειμένων που ήδη έχει το νοσοκομείο. Επιπλέον οι νοσοκόμες ξοδεύουν κατά μέσο όρο 20λεπτά ανά βάρδια για να αναζητήσουν συσκευές ή κρεβάτια που έχουν καταστραφεί, κάθε νοσοκομείο ορίζει οποιαδήποτε συσκευή κάτω από 5000ευρώ αναλώσιμη, αν δεν μπορεί να βρεθεί αγοράζετε νέα. Με την υιοθέτηση του RFID για την παρακολούθηση των ιατρικών συσκευών εξοικονομούνται αρκετά χρήματα λόγω της μη αγοράς σημαντικών ιατρικών συσκευών που είχαν χαθεί.

Η παρακολούθηση των φαρμάκων είναι ένα τελείως διαφορετικό πρόβλημα από αυτό των ιατρικών συσκευών, καθώς η κύρια ανησυχία είναι τα παραποιημένα/πλαστά φάρμακα. Μελέτες δείχνουν ότι μεγάλα ποσοστά, τουλάχιστον το 20% των φαρμάκων σε ανεπτυγμένες χώρες όπως οι ΗΠΑ είναι παραποιημένα. Η υπηρεσία τροφίμων και φαρμάκων στις ΗΠΑ ενέκρινε πρόσφατα την χρήση RFID για την παρακολούθηση των φαρμάκων από την εφοδιαστική αλυσίδα μέχρι τον ασθενή. Αυτό επιτρέπει την πλήρη παρακολούθηση της αλυσίδας και της πορείας των φαρμάκων, εξασφαλίζοντας ότι τα νοσοκομεία έχουν αγοράσει φάρμακα από νόμιμη πηγή. Η Pfizer είναι η πρώτη

φαρμακευτική εταιρεία που υιοθέτησε το e-pedirgree RFID, όπου οι ασθενείς και οι γιατροί μπορούσαν να εμπιστευτούν την πηγή και τις δυνατότητες του φαρμάκου Viagra, καθώς διαπίστωσαν ότι ήταν μεταξύ των πιο παραποιημένων φαρμάκων. Το σύστημα αυτό επέτρεπε στους χονδρέμπορους και τους φαρμακοποιούς να επαληθεύσουν την αυθεντικότητα του φαρμάκου χρησιμοποιώντας έναν απλό ανιχνευτή RFID με κόστος χαμηλό, αποτέλεσμα του χαμηλού κόστους των αντίστοιχων ετικετών.

5.4 Αρχεία Ασθενών

Η τεχνολογία Blockchain έχει σημαντική δύναμη ώστε να διαταράξει την υγειονομική περίθαλψη και να θέσει τα δεδομένα στα χέρια των ασθενών. Μια ιδιαίτερα ενδιαφέρουσα κίνηση προς αυτήν την κατεύθυνση είναι η παροχή ενός αμετάβλητου καταλόγου των αρχείων περίθαλψης στους γιατρούς και στους ασθενείς. Στον τομέα της υγείας χρειάζεται μια διαφορετική προσέγγιση για την παροχή κινήτρων στους «ανθρακωρύχους», παρέχοντας πρόσβαση σε ανώνυμα δεδομένα της υγειονομικής περίθαλψης σε αντάλλαγμα για την διατήρηση του δικτύου. Η MedRec κάνει χρήση έξυπνων συμβολαίων για την χαρτογράφηση των σχέσεων ασθενούς-παροχέα όπου το συμβόλαιο εμφανίζει μια λίστα με αναφορές που αναλύουν τις σχέσεις μεταξύ των κόμβων της αλυσίδας. Επίσης περνάνε οι σχέσεις ασθενούς-παροχέα στα χέρια του ασθενούς, δίνοντας την δυνατότητα να δέχονται, απορρίπτουν ή να τροποποιούν σχέσεις με τους παρόχους της υγειονομικής περίθαλψης, όπως νοσοκομεία, ασφαλιστικές και κλινικές.

Το Blockchain προσφέρει μια μεγάλη ευκαιρία για διαλειτουργικότητα στα συστήματα υγειονομικής περίθαλψης, ως ένας αποκεντρωμένος κατάλογος αποδεκτών γεγονότων σε ιατρικά αρχεία, όπου όλοι οι πάροχοι υγειονομικής περίθαλψης έχουν πρόσβαση σε αυτόν τον κατάλογο. Αυτό σημαίνει ότι ακόμα και αν οι διεπαφές χρήστη είναι διαφορετικές, ο κεντρικός κατάλογος θα είναι όμοιος για όλους τους παρόχους. Μια πρόκληση που υπάρχει σχετίζεται με την τρέχουσα κατάσταση των ιατρικών φακέλων μεταξύ των παρόχων, οι οποίοι περιέχουν σημαντικά ποσά ίδιων πληροφοριών κάτω από διαφορετικά αναγνωριστικά στοιχεία που μπορεί να μην συνδέονται. Αυτό δημιουργεί διπλότυπα, και καθώς μεγαλώνει η αλυσίδα, η απόδοση υποβαθμίζεται, αυτό σημαίνει ότι θα πρέπει να εξαφανιστούν τα διπλότυπα για την διατήρηση ενός αποδοτικού συστήματος, με μοναδικά ανώνυμα αναγνωριστικά στοιχεία για τον εντοπισμό των ασθενών σε όλες τις υπηρεσίες. Αυτή είναι μια επιχειρηματική πρόκληση από μόνη της, στην υιοθέτηση ενός μοντέλου που λειτουργεί με Blockchain, τα αρχεία υγείας δεν ξεκινάνε από το μηδέν, καθώς θα πρέπει να αντικατασταθούν τα υφιστάμενα συστήματα. Ο όγκος των δεδομένων που παράγονται σε περιβάλλοντα υγειονομικής περίθαλψης θα αυξηθεί σημαντικά , πράγμα που προσθέτει ένα πρόβλημα κλιμάκωσης.

5.5 Παρακολούθηση Φαρμάκων

Η παρακολούθηση φαρμάκων με την χρήση της τεχνολογίας Blockchain αποτελεί άλλη μια μεγάλη ευκαιρία, δεδομένου ότι αξιοποιεί την αμεταβλητότητα και την ανάπτυξη της αλυσίδας για την παρακολούθηση της εφοδιαστικής αλυσίδας των φαρμάκων από τον κατασκευαστή μέχρι τον ασθενή. Η Chronicled αποτελεί μια νεοφυή επιχείρηση που έχει δημιουργήσει το προϊόν Discover, το οποίο δημιουργεί ένα μοντέλο αλυσίδας που δείχνει ποιος παράγει το φάρμακο, και από πού και πότε έχει αγορασθεί από τους ασθενείς, αξιοποιώντας την αμεταβλητότητα της τεχνολογίας Blockchain για την

πρόληψη της απάτης και της κλοπής φαρμάκων. Αυτό επιτρέπει στους παρόχους υγειονομικής περίθαλψης να πληρούν τα ισχύοντα πρότυπα υγειονομικής περίθαλψης που αφορούν την ασφάλεια των φαρμακευτικών προμηθειών, πάλι όμως δίνοντας έμφαση στους παρόχους του τομέα αυτού.

Το HyperLedger αποτελεί μια ομάδα εργασίας ανοιχτού κώδικα, με επίκεντρο το πρόβλημα παραποιημένων φαρμακευτικών προϊόντων. Με την χρήση του Blockchain μπορεί να ανιχνευθεί προέλευση των παραποιημένων φαρμάκων και να απομακρυνθεί από την εφοδιαστική αλυσίδα. Το πλεονέκτημα της τεχνολογίας αυτής στην παρακολούθηση φαρμάκων πάνω από τα παραδοσιακά μέσα, είναι η αποκέντρωση της εμπιστοσύνης και της εξουσίας, δηλαδή μιας από τις βασικές αρχές αυτής της τεχνολογίας, σε ένα τέτοιο δίκτυο είναι αρκετά δύσκολο να παραπλανηθούν ή να δωροδοκηθούν οι κεντρικές αρχές. Γι αυτόν τον λόγο το ισχύον βιομηχανικό πρότυπο στον τομέα της φαρμακευτικής παρακολούθησης, e-pedigree RFID, κινείτε στην εύρεση μιας λύσης η οποία θα περιέχει την τεχνολογία Blockchain. Σε περίπτωση τροποποιημένων φαρμακευτικών προϊόντων με την τεχνολογία Blockchain μπορεί να γίνει ανίχνευση αυτών και άμεση απομάκρυνση από την εφοδιαστική αλυσίδα υγείας.

5.6 Παρακολούθηση Συσκευών

Η παρακολούθηση των ιατρικών συσκευών αποτελεί μια ακόμη ευκαιρία για την χρήση της τεχνολογίας Blockchain στον τομέα της υγειονομικής περίθαλψης. Οι νομισματικές αποταμιεύσεις που γίνονται από την παρακολούθηση συσκευών είναι σαφής. Η NHS διαπίστωσε ότι ως αποτέλεσμα μιας μελέτης περίπτωση από τον Harland Simon στην οποία εφάρμοσαν RFID στον εξοπλισμό, βρήκαν 98 αντλίες έγχυσης που δεν είχαν ιδέα ότι υπήρχαν. Με κόστος 1500 ευρώ έκαστος, εξοικονόμησαν 147.000 ευρώ χάρη σε αυτήν την μελέτη περίπτωσης. Η χρήση της τεχνολογίας Blockchain μαζί με αυτήν την τεχνολογία προσφέρει την ευκαιρία για έναν αμετάβλητο κατάλογο, ο οποίος δείχνει όχι μόνο που βρίσκεται η συσκευή μια δεδομένη στιγμή, αλλά και που βρισκόταν προηγουμένως, καθώς και ποιος είναι ο κατασκευαστής, ο μεταπωλητής και ο σειριακός αριθμός που συνδέεται με την συσκευή, βοηθώντας έτσι στην κανονιστική συμμόρφωση. Αυτή η δυνατότητα εντοπίστηκε πρώτα από τον Deloite, και ορίστηκε ως ένας από τους πιο πιθανούς αντικαταστάτες στον τομέα της υγειονομικής περίθαλψης. Πράγματι μια μελέτη της IBM έδειξε ότι το 60% των κυβερνητικών φορέων στον τομέα της υγειονομικής περίθαλψης πιστεύουν στην παρακολούθηση των ιατρικών συσκευών, διότι η διαχείρισή τους χωρίς παρακολούθηση δημιουργεί προβλήματα στον κλάδο.

Μια προσέγγιση του Blockchain προσφέρει πολλά πλεονεκτήματα σε σχέση με τα παραδοσιακό προϊόντα εντοπισμού θέσης. Το πιο προφανές είναι η αμεταβλητότητα που προσφέρει η αλυσίδα, αυτή εμποδίζει έναν κακόβουλο χρήστη να αλλάξει το ιστορικό τοποθεσίας μιας συσκευής ή να την διαγράψει από τις εγγραφές. Αυτός είναι ιδιαίτερα σημαντικός παράγοντας δεδομένου ότι η κλοπή και η παραποίηση στοιχείων ιατρικών συσκευών έχει γίνει πρόβλημα πολλών εκατομμυρίων δολαρίων τόσο στην Ευρώπη όσο και στην Αμερική.

Όπως και με την παραδοσιακή κλοπή, η τεχνολογία αυτή αποτρέπει επίσης την απώλεια και την αναδιάταξη των συσκευών, γεγονός που συνεπάγεται σημαντικό κόστος τόσο από άποψη

φροντίδας όσο και από πραγματικό κόστος εξοπλισμού. Αυτό το σύστημα δεν θα πρέπει να προσθέτει επιπλέον χρόνο εργασίας σε έναν νοσηλευτή, έναν φορέα ή έναν υπάλληλο υποστήριξης.

Όσο η τεχνολογία Blockchain μεγαλώνει μέσα στο IOT, τόσο πιο εύκολα γίνεται η υιοθεσία ενός νέου τρόπου επικοινωνίας για τις συσκευές με την χρήση μιας αλυσίδας από μπλοκ σε συνδυασμό με την χρησιμοποίηση ένα σύστημα δημοσίου κλειδιού και τον κρυπτογραφικό αλγόριθμο RSA. Με αυτόν τον τρόπο, μια συσκευή αποθηκεύει το δημόσιο κλειδί της στο Blockchain και το σχετικό ιδιωτικό κλειδί αποθηκεύεται στην συσκευή.

5.7 Εφοδιαστική Αλυσίδα Υγείας

Πιο συγκεκριμένα στην Εφοδιαστική Αλυσίδα Υγείας η σοβαρότερη και πιο συνηθισμένη απειλή είναι η διείσδυση πλαστών/υποβαθμισμένων/παραποιημένων φαρμακευτικών προϊόντων. Αυτές οι διαφορετικές μορφές «πλαστών» φαρμάκων μπορούν να εκδηλωθούν ως αποτέλεσμα εισαγωγής υποβαθμισμένων φαρμάκων χωρίς έγκριση, με κακή πρακτική κατασκευής ή ακατάλληλη αποθήκευση, και διείσδυση όλων αυτών σε μαύρες αγορές, δηλαδή σε μην νόμιμα κανάλια. Ο παγκόσμιος οργανισμός υγείας εκτιμά αυτήν την αγορά στα 75 δισεκατομμύρια δολάρια ετησίως, άλλες εκτιμήσεις φτάνουν μέχρι και τα 200 δισεκατομμύρια δολάρια τον χρόνο. Η φαρμακευτική εφοδιαστική αλυσίδα είναι ιδιαίτερα ευάλωτη σε χώρες όπως το Βιετνάμ, όπου η μεγάλη πλειοψηφία των δαπανών για φάρμακα εξαρτάτε από εισαγόμενες πηγές.

Ωστόσο τα μειονεκτήματα της εφοδιαστικής αλυσίδας δεν περιορίζονται στις αγορές με χαμηλό εισόδημα ή εκείνες που εξαρτώνται αρκετά από φάρμακα. Για παράδειγμα το 2012, η αμερικάνικη υπηρεσία τροφίμων και φαρμάκων κοινοποίησε σχεδόν 1000 εγκαταστάσεις υγειονομικής περίθαλψης και επαγγελματίες σε 48 πολιτείες, ότι μπορεί να είχαν αγοράσει και χορηγήσει ψεύτικες εκδοχές του αντικαρκινικού φαρμάκου Avastin. Κάπως έτσι ξεκίνησε το DSCSA (Drug Supply Chain Security Act), δηλαδή η δράση κατά της ασφάλισης της εφοδιαστικής αλυσίδας υγείας. Σε ένα πλαίσιο 10 χρόνων το DSCSA απαιτεί παρακολούθηση φαρμάκων και ανίχνευση, σειριοποίηση, επαλήθευση και ανίχνευση ύποπτων προϊόντων και αυστηρές οδηγίες για την αδειοδότηση των χονδρέμπορων καθώς και την υποβολή εκθέσεων. Εκτός των ΗΠΑ και άλλες παρόμοιες προσπάθειες βρίσκονται σε εξέλιξη και στην Ευρωπαϊκή Ένωση για την καταπολέμηση της παραποίησης και απομίμησης σε διάφορες χώρες μέλη.

Η τεχνολογία Blockchain θα μπορούσε να βελτιστοποιήσει την εφοδιαστική αλυσίδα υγείας σε θέματα διαχείρισης, κατασκευής και διανομή φαρμακευτικών προϊόντων. Θα μπορούσε να καταπολεμήσει την απάτη σε αντίθεση με τα τρέχοντα συστήματα και βάσεις δεδομένων. Επιπλέον θα μπορούσε να προσφέρει λειτουργικότητα ή διαδικασίες που δεν είναι διαθέσιμες με βάσεις δεδομένων και συστήματα παλιού τύπου. Θα μπορούσε επίσης να συμβαδίσει με τις τρέχουσες τεχνολογίες RFID και να προσφέρει μια ρυθμιστική λύση που μπορεί να μετριάσει τον κίνδυνο αλλά και να εξασφαλίσει καλύτερη συμμόρφωση και ασφάλεια ασθενών κάτι που ωφελεί τόσο τους κατασκευαστές όσο και τους ασθενείς. Η τεχνολογία Blockchain μπορεί να ικανοποιήσει όλες τις απαιτήσεις του DSCSA.

Συμβατότητά Blockchain με τις απαιτήσεις του DSCSA

Βασική Απαίτηση	Εφαρμογή με Blockchain	Συμβατότητα
Ταυτοποίηση Προϊόντος	Μοναδικό αναγνωριστικό προϊόντος με πληροφορίες επαληθευμένες ως μια πλευρική αλυσίδα	ΝΑΙ
Εντοπισμός Προϊόντων	Επιτρέπει τους κατασκευαστές και τους διανομείς να παρέχουν πληροφορίες σε ένα κοινόχρηστο ημερολόγιο με αυτόματη επαλήθευση σημαντικών πληροφοριών	ΝΑΙ
Επαλήθευση Προϊόντος	Δημιουργεί ένα σύστημα για την επαλήθευση του αναγνωριστικού προϊόντος και των πληροφοριών	ΝΑΙ
Ανίχνευση και Απόκριση	Επιτρέπει στους δημόσιους και ιδιωτικούς φορείς να αναφέρουν και να ανιχνεύουν τα πλαστά/παραποιημένα φάρμακα	ΝΑΙ
Ειδοποίηση	Δημιουργεί ένα σύστημα με σκοπό την ειδοποίηση των αρμοδίων σε περίπτωση που βρεθεί κάποιο πλαστό φάρμακο	ΝΑΙ
Απαίτηση Πληροφοριών	Δημιουργεί ένα κοινόχρηστο ημερολόγιο πληροφοριών προϊόντων και συναλλαγών συμπεριλαμβανομένης της επαλήθευσης και άδειας χρήσης	ΝΑΙ

Εικόνα 18 DSCSA και Blockchain

Πολλοί οργανισμοί διερευνούν ενεργά την χρήση του Blockchain για την παροχή φαρμακευτικών προϊόντων, διαχείριση αλυσίδων, με τν ανάπτυξη περιπτώσεων χρήσης, μοντέλων προσομοίωσης και προτύπων εφαρμογών Blockchain. Αυτήν την στιγμή γίνονται παγκοσμίως και ιδιαίτερα στην Αμερική πάρα πολλές προσπάθειες από πολλούς οργανισμούς κρατικούς ή μη κρατικούς, με στόχο την εκμετάλλευση των πλεονεκτημάτων αυτής της νέας τεχνολογίας. Συνολικά η συγκεκριμένη τεχνολογία μπορεί να κάνει καλύτερα την παροχή φαρμακευτικών προϊόντων στην εφοδιαστική αλυσίδα, ενώ παράλληλα αντιμετωπίζει την ανάγκη της μακροχρόνιας δημόσιας υγείας.

5.8 Internet of Healthy Things

Το Internet of Healthy Things είναι ένα υποσύνολο του Internet of Things που επικεντρώνεται στην υγεία και στην ευεξία. Αυτά τα «πράγματα» περιλαμβάνουν συσκευές όπως έξυπνα ρολόγια, αισθητήρες και γενικότερα αυτόνομες συσκευές που αφορούν καθημερινές δραστηριότητες όπως ο ύπνος, η καρδιακή λειτουργία και η ασθένεια. Οι ευπάθειες και οι ευκαιρίες σε αυτό το κομμάτι είναι παρόμοιες με αυτές των ιατρικών συσκευών, αλλά το IoHT συνδέεται με μεγαλύτερες απειλές στα δεδομένα και στην ασφάλεια, λόγο των λιγότερων αυστηρών απαιτήσεων των δοκιμών σχετικά με την ιατρική ή συσκευές που είναι περισσότερο εστιασμένες στον καταναλωτή. Το trusted IOT είναι μια συμμαχία που δημιουργήθηκε από πολλούς ενδιαφερόμενους κλάδους του IOT, με στόχο την ασφάλεια και την διευκόλυνση των διαδικασιών χρήστη με την τεχνολογία Blockchain.

Η πρώτη προσπάθεια στον τομέα του IoHT σε συνδυασμό με την τεχνολογία Blockchain είναι η εφαρμογή από το Bowhead Health, η οποία βασίζεται σε μια συνδεδεμένη συσκευή που διανέμει φαρμακευτικά προϊόντα διατροφής. Ο ασθενής προσθέτει τα προσωπικά προϊόντα υγείας και τις συνήθειές του σε μια φόρμα η οποία είναι ανώνυμη, με την βοήθεια των ανώνυμων τόκεν υγείας. Αυτό το μοντέλο προτείνετε από ένα πλήθος από εταιρείες υγειονομικής περίθαλψης (Burst IQ, Healthcoin, Scriptdrop, Solasterhealth), η Bowhead είναι μια από τις πρώτες εταιρείες Blockchain στον τομέα της υγείας, η οποία ενώνει μια δικιάς της κατασκευής συσκευή IoHT με το Blockchain. Έχοντας μια αρχική

επιτυχία τέτοιο είδους εφαρμογές και συσκευές, θα μπορούσαν στην συνέχεια να εξελιχθούν περνώντας από τις απλές συσκευές υγείας σε πιο εξειδικευμένες ιατρικές συσκευές, κάτι το οποίο αποτελεί τεχνολογική τάση τα τελευταία χρόνια.

5.9 Δημόσια Υγεία

Οι προκλήσεις της εφοδιαστικής αλυσίδας στην δημόσια υγεία περιλαμβάνουν καταστροφές και διαχείριση της έκτακτης ανάγκης, συμπεριλαμβανομένης της προστασίας των προμηθευτών για την υγειονομική περίθαλψη κατά την διάρκεια της δημόσιας υγείας, καθώς και πρόσβαση σε ουσιώδη φάρμακα, εμβόλια και εμβολιασμούς. Στο πλαίσιο της πρόσβασης σε νόμιμα και ποιοτικά φάρμακα, οι λύσεις της τεχνολογίας Blockchain, αλληλεπικαλύπτονται με τις περιπτώσεις χρήσης στην εφοδιαστική αλυσίδα φαρμάκων, αλλά επίσης επεκτείνεται στην διατήρηση επαρκής παροχής στο σημείο διανομής, περιορίζοντας τα συστήματα υγείας που σχετίζονται με την διαφθορά στην προμήθεια φαρμάκων και καταλυτική αποτελεσματική παροχή υπηρεσιών και εμπορευμάτων υγειονομικής περίθαλψης. Η τεχνολογία Blockchain στην δημόσια υγεία έχει κάνει την εμφάνισή της και με τα κρυπτονομίσματα, τα οποία αποτελούν μια εναλλακτική λύση για την υγειονομική περίθαλψη. Αυτές οι μορφές νομίσματος μπορούν να χρησιμοποιηθούν καλύτερα για θέματα φιλανθρωπίας αλλά και για την μείωση της απάτης και της διαφθοράς στην παγκόσμια υγεία.

5.10 Αποθήκευση Δεδομένων Υγείας και Ασφάλεια

Με την τεχνολογία Blockchain μπορούν όλα τα δεδομένα να αποθηκευτούν η να χαρακτηριστούν ως δεδομένα σχετικά με τις συνθήκες, αποτελέσματα εργαστηριακών μελετών, φάρμακα, αλλεργίες και χιλιάδες άλλα κλινικά χαρακτηριστικά. Τα δεδομένα υγειονομικής περίθαλψης περιλαμβάνουν επίσης λειτουργικά και διαχειριστικά δεδομένα, όπως για παράδειγμα ασφαλιστική κάλυψη, φορείς παροχής περίθαλψης, κτλ. Είναι σημαντικό αν τα δεδομένα αφορούν πρόσωπα ή μόνο οργανισμούς από την πλευρά της ιδιωτικής ζωής. Δεδομένα που μπορούν να προσδιορίσουν την τοποθεσία/επικοινωνία με ένα άτομο, αντιπροσωπεύουν αναγνωριστικές προσωπικές πληροφορίες. Όπου υπάρχουν τέτοια δεδομένα και προσωπικά, εφαρμόζονται οι κανόνες της ιδιωτικής ζωής. Αν γίνεται επεξεργασία πιο ευαίσθητων δεδομένων όπως αυτά της υγείας τότε είναι ακόμα πιο αυστηρά τα πράγματα. Τα δεδομένα υγείας σε συνδυασμό με τις αναγνωριστικές προσωπικές πληροφορίες αναφέρονται συνήθως ως προστατευμένες πληροφορίες για την υγεία και είναι πολύ αυστηρή η προστασία τους.

Μια λύση με Blockchain θα προσφέρει καινοτόμες ευκαιρίες σχεδιασμού και πιο καλή προστασία των παραπάνω δεδομένων με την χρήση των έξυπνων συμβολαίων. Η προέλευση δεδομένων, αποθήκευση δεδομένων, σε συνδυασμό με την αλυσίδα και με τα άτομα από την διακυβέρνηση και πρόσβαση σε αυτά τα κρυπτογραφημένα δεδομένα συνδέονται με όλα αυτά που προσφέρει η τεχνολογία Blockchain.

Οι πληροφορίες της υγειονομικής περίθαλψης πρέπει να είναι αξιόπιστες, με έγκυρα στοιχεία περίθαλψης, υπό την προϋπόθεση ότι οι αποφάσεις, οι θεραπείες, τα συνταγογραφούμενα φάρμακα και οι ταυτότητες των ασθενών συμμετέχουν στον κύκλο υγείας. Η τεχνολογία Blockchain παρέχει την διαβεβαίωση ότι τα δεδομένα δεν αλλοιώθηκαν και επιβεβαιώνει τις λεπτομέρειες σχετικά με την

προέλευση των δεδομένων. Μέσω κρυπτογραφικών τεχνικών, όπως ζεύγη δημοσίων και ιδιωτικών κλειδιών και την κατανεμημένη φύση των Blockchain στο ίδιο σύστημα, όλες οι πληροφορίες μοιράζονται και έχουν ένα ελεγχόμενο μονοπάτι/ιστορικό , ένα αξιόπιστο «δακτυλικό αποτύπωμα».

6. BLOCKCHAINS ΚΑΙ ΕΚΠΑΙΔΕΥΣΗ *[10],[11],[12],[13],[14],[15],[16]*

6.1 Εισαγωγή στην Εκπαίδευση

Ένας πολύ σημαντικός τομέας της κοινωνίας, εξίσου σημαντικός με αυτόν της υγείας είναι ο τομέας της εκπαίδευσης. Η τεχνολογία Blockchain μπορεί να δώσει λύσεις σε πολλά ζητήματα και προβληματικές καταστάσεις στον τομέα της εκπαίδευσης αλλά παρέχει και την δυνατότητα νέων καινοτόμων εφαρμογών οι οποίες διαφοροποιούν τις παραδοσιακές διαδικασίες ή δημιουργούν νέες. Ο τομέας των πιστοποιητικών είτε αυτά είναι πανεπιστημιακά πτυχία, είτε από σεμινάρια και είτε οποιοδήποτε είδος πιστοποιητικού αποτελεί ένα κομμάτι της εκπαίδευσης στο οποίο η τεχνολογία Blockchain μπορεί να προσφέρει ριζικές αλλαγές, στον τρόπο έκδοσης και διαχείρισης των πιστοποιητικών και όλων εργασιών επιτελούνται γύρω από αυτά. Πολλά είναι τα παραδείγματα εφαρμογών που αξιοποιούν την τεχνολογία Blockchain στον τομέα αυτό. Ο τομέας της παιδαγωγικής και της διδασκαλίας επίσης μπορεί να αλλάξει αρκετά, υπάρχουν πολλά παραδείγματα και υλοποιήσεις εφαρμογών που δίνουν στους εμπλεκόμενους κομμάτια επιτεύγματος για στοιχεία που καταχωρούν στην αλυσίδα αλλά και εφαρμογές στις οποίες ανταλλάσσεται εκπαιδευτική φήμη μεταξύ των συμμετεχόντων.

Πολλές είναι επίσης οι μελλοντικές εφαρμογές που μπορεί να δώσει τον Blockchain στον τομέα της εκπαίδευσης. Έξυπνα συμβόλαια μεταξύ μαθητών και καθηγητών, καθηγητών και σχολείων, μπορούν να προσφέρουν πολλά πλεονεκτήματα στην αξιολόγηση μαθητών και εκπαιδευτών. Βέβαια σε καμία περίπτωση η τεχνολογία αυτή, δεν μπορεί να αντικαταστήσει τον δάσκαλο, υπάρχουν πολλές εργασίες στις οποίες χρειάζεται η κριτική σκέψη και η καθοδήγηση κάτι που δεν μπορεί να προσφέρει η τεχνολογία, παρόλα αυτά μπορεί να επιφέρει πολλά οφέλη τα οποία παρατίθενται στις επόμενες ενότητες.

6.2 Πιστοποιητικά

Στον τομέα της εκπαίδευσης τα πιστοποιητικά επιβεβαιώνουν την επίτευξη ορισμένων αποτελεσμάτων εκμάθησης και ως επί το πλείστον εκδίδονται σε χαρτί ή σε άλλες φυσικές μορφές. Για παράδειγμα, ένας μαθητής έχει συμμετάσχει σε ένα εκπαιδευτικό πρόγραμμα σχετικά με την πληροφορική, μετά την επιτυχή ολοκλήρωση του κύκλου μαθημάτων, ο μαθητευόμενος λαμβάνει το πιστοποιητικό ως έντυπο έγγραφο και του δίνει την δυνατότητα να χρησιμοποιήσει τον αντίστοιχο τίτλο που αναγράφεται στο πιστοποιητικό και προσφέρεται μετά την επιτυχή ολοκλήρωση του κύκλου των μαθημάτων και πιθανών εξετάσεων. Τα πανεπιστήμια και τα εκπαιδευτικά ιδρύματα που απονέμουν βαθμούς στους φοιτητές εκδίδουν επίσης πολλά πιστοποιητικά.

Τα πιστοποιητικά αυτά περιλαμβάνουν ένα πλήθος στοιχείων, τα πιο σημαντικά είναι το είδος του ακαδημαϊκού τίτλου που επιβεβαιώνεται, το όνομα και την διεύθυνση του οργανισμού που το εκδίδει, το όνομα και την υπογραφή του αρμόδιου από τον οργανισμό έκδοσης, ώστε να επικυρωθούν τα γεγονότα και να βεβαιώσει ότι ο τίτλος είναι αληθής, φυσικά περιλαμβάνει και το όνομα του φοιτητή καθώς και την ημερομηνία εξέτασης. Ανάλογα με τον τύπο του πιστοποιητικού, μπορούν να

υπάρχουν επιπλέον δηλώσεις σχετικά με τους κανονισμούς εξέτασης, την περίοδο ισχύος ή περαιτέρω πληροφορίες απαραίτητες για την χρήση του πιστοποιητικού.

Οι μαθητευόμενοι συνήθως λαμβάνουν ένα έγγραφο που παρουσιάζει το πιστοποιητικό, η χρήση του πιστοποιητικού χαρτιού έχει το πλεονέκτημα ότι είναι δύσκολο να πλαστογραφηθεί λόγω των ενσωματωμένων χαρακτηριστικών ασφαλείας του πιστοποιητικού. Επιπρόσθετα οι παραλήπτες μπορούν εύκολα να αποθηκεύσουν πιστοποιητικά χαρτιού και να τα παρουσιάσουν σε οποιονδήποτε για κάποιον σκοπό. Ωστόσο υπάρχουν ορισμένα μειονεκτήματα όπως οι δραστηριότητες των τρίτων μερών για την επαλήθευση του πιστοποιητικού ή η ανάγκη για τις αρχές πιστοποίησης να διατηρούν ένα μητρώο ή μια βάση δεδομένων για τα πιστοποιητικά.

Μια εναλλακτική λύση απέναντι στα παραδοσιακά πιστοποιητικά είναι τα ψηφιακά πιστοποιητικά που υπογράφονται κρυπτογραφικά. Σε σύγκριση με τα παραδοσιακά πιστοποιητικά χαρτιού, η διαχείριση και η χρήση ψηφιακών πιστοποιητικών είναι πολύ πιο απλή. Ωστόσο απαιτείτε περισσότερη προσπάθεια για την διασφάλιση του μητρώου των πιστοποιητικών και ένα ανοιχτό πρότυπο για ψηφιακές υπογραφές, διαφορετικά η συνολική επαλήθευση των πιστοποιητικών καθιστάτε αδύνατη.

Συγκεκριμένα στον τομέα των πιστοποιητικών στην εκπαίδευση συναντάτε το πρόβλημα των ψεύτικων βαθμών. Η τεχνολογία Blockchain μπορεί να δώσει λύση σε όλα τα παραπάνω προβλήματα, όπως στο πιστοποιητικό χαρτιού, το ψηφιακό πιστοποιητικό ή τους ψεύτικους βαθμούς.

Στο πλαίσιο της εκπαίδευσης και της πιστοποίησης η τεχνολογία Blockchain υποστηρίζει την προστασία των πιστοποιητικών, για πλαστά πιστοποιητικά, καθώς και εύκολη επαλήθευση των πιστοποιητικών ακόμη και αν η αρχή πιστοποίησης δεν υπάρχει πλέον, επίσης προσφέρει αυτοματισμό και παρακολούθηση των διαδικασιών των πιστοποιητικών με χρονική διάρκεια ισχύος. Εντοπίζονται τρία κύρια καθήκοντα από την εξέταση των διαδικασιών πιστοποίησης με την χρήση της τεχνολογίας Blockchain. Αρχικά πρέπει να δημιουργηθούν και να διατηρηθούν οι ταυτότητες των αρχών πιστοποίησης, έπειτα αυτές να έχουν την δυνατότητα να εκδίδουν πιστοποιητικά στους εκπαιδευόμενους και τέλος είναι η επαλήθευση των πιστοποιητικών από τους εκδότες. Αυτές οι διαδικασίες θα πρέπει να υποστηρίζονται πολύ καλά από μια υποδομή βασισμένη στην τεχνολογία Blockchain, συμπεριλαμβανομένης και της κοινής χρήσης των πιστοποιητικών από τους εκπαιδευόμενους.

Η τεχνολογία Blockchain στον τομέα της εκπαίδευσης στοχεύει στην υποστήριξη κατά της πλαστογραφίας, καθώς και στην ασφαλή και πρόσβαση και διαχείριση των πιστοποιητικών ανάλογα με τις ανάγκες των εκπαιδευόμενων, των εταιρειών, των εκπαιδευτικών ιδρυμάτων και των αρχών πιστοποίησης.

6.2.1 Σχετικές Εργασίες

Σε αυτό το σημείο παρουσιάζονται σχετικά project που έχουν γίνει σε αυτόν τον τομέα της εκπαίδευσης, με συνδυασμό της τεχνολογίας Blockchain και των πιστοποιητικών.

Το πανεπιστήμιο της Λευκωσίας στην Κύπρο είναι το πρώτο ίδρυμα τριτοβάθμιας εκπαίδευσης που φυλάσσει ακαδημαϊκά πιστοποιητικά σε ένα Blockchain (βασιζόμενο στην αλυσίδα Ripple). Η τεχνολογία Blockchain για το αντικείμενο των πιστοποιητικών είναι ένας τρόπος γεφύρωσης του χάσματος ανάμεσα στο παραδοσιακό πανεπιστήμιο και στην ανάγκη ρεαλιστικών λύσεων για την αγορά. Το πανεπιστήμιο Κύπρου ανάθεσε στην δική του ομάδα ανάπτυξης λογισμικού να δημιουργήσει έναν τέτοιο μηχανισμό, για την υλοποίηση χρησιμοποιήθηκε το πρότυπο ανοικτού κώδικα Blockcerts. Το πανεπιστήμιο Κύπρου περιγράφει την όλη διαδικασία για την έκδοση και την επικύρωση των πιστοποιητικών σε μια δική του σελίδα, όλα τα πιστοποιητικά εκδίδονται σε δημόσιο Blockchain. Το 2017 έγιναν οι πρώτες δοκιμές σε ένα σύστημα δημοσίευσης όλων των διπλωμάτων με την χρήση Blockchain, αργότερα το ίδιο έτος δημιουργήθηκαν και εργαλεία λογισμικού για την επιβεβαίωση της αυθεντικότητας των διπλωμάτων. Πλέον το πανεπιστήμιο Κύπρου παραμένει μέρος του Blockcerts και χρησιμοποιεί ένα μεγάλο πλήθος από εργαλεία που παρέχονται για την βελτίωση της διεπαφής χρήστη.

Το MIT Media Lab μαζί με το Learning Machine, έναν οργανισμό ανάπτυξης λογισμικού για τις επιχειρήσεις, έχει αναπτύξει το Blockcerts, το οποίο αποτελεί ένα σύστημα ανοιχτού κώδικα για την δημιουργία, την κοινή χρήση και την επαλήθευση των εκπαιδευτικών πιστοποιητικών με την χρήση της τεχνολογίας Blockchain. Τα πιστοποιητικά στον τομέα της εκπαίδευσης περιέχουν βασικές πληροφορίες όπως το όνομα του αποδέκτη, όνομα εκδότη, ημερομηνία έκδοσης κλπ. Τα ψηφιακά πιστοποιητικά καταχωρούνται στο Blockchain κρυπτογραφικά υπογεγραμμένα και προστατεύονται από παραβίαση. Το Blockcerts καθιστά δυνατή την επαλήθευση του για ποιον εκδόθηκε το πιστοποιητικό, από ποιον εκδόθηκε το πιστοποιητικό και την επικύρωση του ίδιου του περιεχομένου του πιστοποιητικού.

Με βάση το Blockcerts στην Μάλτα δημιουργήθηκε ένα αρχικό λογισμικό για της ακαδημαϊκές και επαγγελματικές πιστοποιήσεις, στόχος της Μάλτας είναι να γίνει ένα «νησί Blockchain», με ένα πολύ μεγάλο μέρος ενεργειών να γίνονται γύρω από αυτόν τον τομέα. Επίσης η Ομοσπονδία Κρατικών Ιατρικών Συμβουλίων στις ΗΠΑ εγκαινίασε ένα πιλοτικό πρόγραμμα για την έκδοση επίσημων εγγράφων με Blockcerts στον Blockchain.

Τον Ιούλιο του 2017 η εταιρεία SAP, εισήγαγε το TrueRec, ένα ασφαλές και αξιόπιστο ψηφιακό πορτοφόλι για την αποθήκευση των επαγγελματικών και ακαδημαϊκών διαπιστευτηρίων, με βάση το Ethereum. Στην Ολλανδία ο Οργανισμός Εφαρμοσμένης Επιστημονικής Έρευνας ξεκίνησε από το 2017 το project «αυτοκυβερνητικό πλαίσιο ταυτότητας». Αυτό το πλαίσιο έχει σχεδιαστεί για να βοηθήσει στην παροχή επίσημων πληροφοριών σε ψηφιακή μορφή και να μοιράζεται ένα ελάχιστο ποσοστό προσωπικών δεδομένων που διαχειρίζεται και αποθηκεύεται σε κρυπτογραφημένη μορφή, σε ένα πορτοφόλι στο δικό του κινητό τηλέφωνο. Αυτές οι πληροφορίες παρέχουν επίσημη επιβεβαίωση της ταυτότητας του ατόμου.

6.2.2 Παράδειγμα Συστήματος με Blockchain

Το παράδειγμα συστήματος περιέχει κυρίως τις αρχές πιστοποίησης, τους εκπαιδευόμενους και τους εργοδότες. Εξασφαλίζει μεγαλύτερη αποτελεσματικότητα και βελτιωμένη ασφάλεια για τις αρχές πιστοποίησης μέσω της ψηφιοποίησης των τρέχουσων διαδικασιών, της έκδοσης και της εγγραφής των πιστοποιητικών σε ένα Blockchain καθώς και της αυτόματης παρακολούθησης των πιστοποιητικών, τα πιστοποιητικά αναγνωρίζονται από την μηχανή. Οι εκπαιδευόμενοι έχουν την δυνατότητα να διαχειρίζονται τα πιστοποιητικά τους και να παρέχουν πρόσβαση σε επιλεγμένα πιστοποιητικά σε τρίτους, δηλαδή διασφαλίζεται η προστασία του απορρήτου για τους υποψηφίους. Για τους εργοδότες προσφέρεται αξιόπιστη επαλήθευση των πιστοποιητικών.

Επί του παρόντος οι αρχές πιστοποίησης διαχειρίζονται τα δεδομένα των εκπαιδευόμενων, τα μαθήματα, και άλλους σχετικούς κανονισμούς, καθώς και τα αποτελέσματα των εξετάσεων σε δικές βάσεις δεδομένων ή σε φύλλα τύπου Excel. Αυτά τα δεδομένα χρησιμοποιούνται για την έκδοση πιστοποιητικών στους εκπαιδευόμενους. Επομένως η εισαγωγή δεδομένων και τα αποτελέσματα εξετάσεων από τα συστήματα παλαιού τύπου είναι ένα πρώτο σημαντικό χαρακτηριστικό από τις αρχές πιστοποίησης. Μετά την εισαγωγή των δεδομένων οι αρχές πιστοποίησης μπορούν να περιηγηθούν στα παραγόμενα πιστοποιητικά. Επιπρόσθετα, οι αρχές πιστοποίησης χρειάζονται μέσα για την αναζήτηση μαθητών , ή για να αποκτήσουν μια επισκόπηση των μαθητών και των αποτελεσμάτων των εξετάσεων τους σύμφωνα με τα μαθήματα. Η επισκόπηση επιτρέπει τις αρχές πιστοποίησης να εκτυπώνουν ταυτόχρονα όλα τα πιστοποιητικά ενός μαθήματος. Το δεύτερο κύριο χαρακτηριστικό των αρχών πιστοποίησης είναι η υπογραφή των πιστοποιητικών και η αποθήκευσή τους σε Blockchain. Και οι δύο ενέργειες πραγματοποιούνται εύκολα ταυτόχρονα για όλους τους μαθητές στην προαναφερθείσα επισκόπηση. Η αναγνώριση της εγκυρότητας και της αυθεντικότητας ενός συγκεκριμένου πιστοποιητικού είναι ένα επιπλέον χαρακτηριστικό για όλες τις ομάδες χρηστών. Επιπλέον οι αρχές πιστοποίησης χρειάζονται ένα μέσο για την ανάκληση πιστοποιητικών.

Οι εκπαιδευόμενοι λαμβάνουν πιστοποιητικά με ενσωματωμένες ιδιότητες ασφάλειας και στέλνουν αυτά τα πιστοποιητικά με διάφορους τρόπους σε πιθανούς εργοδότες. Οι εκπαιδευόμενοι χρειάζονται μέσα για την διαχείριση των χαρτοφυλακίων εφαρμογών καθώς και μέσα για την κατανομή τους. Μετά την κοινή χρήση χαρτοφυλακίων, οι μαθητές υποστηρίζονται με πληροφορίες σχετικά με τις δραστηριότητες του εργοδότη στα πιστοποιητικά τους, όπως η ανάγνωση η επαλήθευση. Οι αρχές πιστοποίηση μπορούν να υπενθυμίζουν στους εκπαιδευόμενους να ανακαλούν πιστοποιητικά, εάν δεν πληρούνται οι όροι ανανέωσης.

Οι εργοδότες, λαμβάνουν μόνο αντίγραφα, μερικές φορές συμβολαιογραφικά των πιστοποιητικών των εκπαιδευόμενων. Σε πρώτη ανάγνωση οι εργοδότες μπορούν να αποδείξουν την εγκυρότητα των αντιγράφων ζητώντας από τον φορέα έκδοσης την γνησιότητα και εγκυρότητα του πιστοποιητικού. Αυτό αποτελεί μια χρονοβόρα και «ακριβή» διαδικασία. Όλα τα παραπάνω χαρακτηριστικά παρατίθενται στην συνέχεια σε ένα διάγραμμα της αρχιτεκτονικής του συστήματος

Εικόνα 19 Αρχιτεκτονική Συστήματος

6.2.3 Αρχιτεκτονική του Συστήματος

Το παραπάνω σχήμα περιλαμβάνει την χρήση της τεχνολογίας Blockchain σε συνδυασμό με τα έξυπνα συμβόλαια, έναν δημόσιο αποθηκευτικό χώρο που κρατάει τις πληροφορίες των αρχών πιστοποίησης και ένα σύστημα διαχείρισης αρχείων που διαχειρίζεται πιστοποιητικά που υπάρχουν στο Blockchain. Ο τρόπος λειτουργίας του είναι ο εξής. Αρχικά δύο έξυπνα συμβόλαια υποβάλλονται στο Blockchain από την αρχή διαπίστευσης (1), το πρώτο έξυπνο συμβόλαιο υποστηρίζει την διαχείριση των ταυτοτήτων και το δεύτερο διαχειρίζεται τον κύκλο ζωής των πιστοποιητικών. Μόλις εφαρμοστούν οι συμβάσεις (2α), είναι καθήκον της αρχής πιστοποίησης να καταχωρίσει τα δημόσια κλειδιά των αρχών πιστοποίησης ως νόμιμο εκδότη πιστοποιητικών(3α) και να υποβάλει δημόσιες και μη προσωπικές πληροφορίες προφίλ στην δημόσια αποθήκη. Είναι σημαντικό να σημειωθεί ότι οι πληροφορίες προφίλ είναι μόνο για ανάγνωση και είναι ευανάγνωστες στο κοινό, δεν υπόκεινται στους μηχανισμούς ελέγχου πρόσβασης του συμβολαίου. Απλώς κατέχει μακροχρόνια προφίλ των αρχών πιστοποίησης, όπως το όνομα και η χώρα τους, αλλά δεν περιλαμβάνει καμία προσωπική πληροφορία των πιστοποιητικών ή ακόμη και των εκπαιδευόμενων. Οι καταχωρημένες αρχές πιστοποίησης προσθέτουν στην συνέχεια τα δημόσια κλειδιά των πιστοποιητικών στο μητρώο συμβολαίου και μεταβιβάζουν έτσι το δικαίωμα έκδοσης του πιστοποιητικών (3β). Δηλαδή κάτοχος του κλειδιού του ιδιωτικού πιστοποιητικού θα είναι τυπικά ένας υπάλληλος μιας αρχής πιστοποίησης που έχει το δικαίωμα να εκδίδει πιστοποιητικά και να υπογράφει στο όνομα της αρχής πιστοποίησης. Για την έκδοση πιστοποιητικών αναγράφονται όλα τα απαραίτητα στοιχεία και στην συνέχεια το πιστοποιητικό υπογράφεται από το αρμόδιο και αποθηκεύεται στο σύστημα διαχείρισης εγγράφων (4α) και το hash εγγράφεται στην αλυσίδα (4β). Για την δημιουργία και διαχείριση των χαρτοφυλακίων εφαρμογών υπάρχει μια υπηρεσία που υποστηρίζει την ευέλικτη δημιουργία και διαχείριση αυτών (5), τα χαρτοφυλάκια αυτά μπορούν να μοιραστούν σε εργοδότες οι οποίοι επαληθεύουν την εγκυρότητα των πιστοποιητικών. Η επαλήθευση γίνεται από του εργοδότες μέσω μιας υπηρεσίας επαλήθευσης (6α,6β).

Παρόλο που τα πιστοποιητικά εκδίδονται επί του παρόντος ως έγγραφα σε χαρτί, εκτιμάτε ότι στο μέλλον θα εκδίδονται κυρίως ως ψηφιακά πιστοποιητικά. Η χρήση της τεχνολογίας Blockchain έχει πολύ σημαντικά πλεονεκτήματα για τα ψηφιακά πιστοποιητικά. Παρέχει την αποκεντρωμένη και αμετάβλητη αποθήκευση ψηφιακών πιστοποιητικών και ταυτόχρονα δίνει την δυνατότητα της

επαλήθευσης από τρίτους. Επίσης στο Blockchain μπορούν πολύ εύκολα να αποθηκευτούν οι ταυτότητες των αρχών πιστοποίησης και των πιστοποιητικών.

6.3 Blockchain στην Διδασκαλία

Η τεχνολογία Blockchain στην εκπαίδευση λειτουργεί αποθηκεύοντας εκπαιδευτικά «αντικείμενα», όπως πιστοποιητικά και δημιουργικά έργα, σε έναν δημόσιο κατάλογο που έχουν πρόσβαση χιλιάδες υπολογιστές. Όσο αφορά την αξία αυτής της τεχνολογίας στην παιδαγωγική και γενικότερα στον τομέα της διδασκαλίας , οι σημαντικές πτυχές είναι ότι αυτή η τεχνολογία είναι ασφαλής, προσβάσιμη και διανεμημένη, έχοντας την δυνατότητα να κρατήσει πολλά είδη εκπαιδευτικών στοιχείων. Μια χρήση είναι η αποθήκευση αρχείων εξετάσεων και πιστοποιητικών σπουδών, μαζί με τις ημερομηνίες εγγραφών, και τους εμπλεκόμενους, όπως προαναφέρθηκε και στις προηγούμενες ενότητες. Αντί η επαλήθευση από έναν εργοδότη να γίνεται με τον παραδοσιακό τρόπο, μπορούν να επαληθευτούν μέσα από την αλυσίδα.

Αυτή η μέθοδος μπορεί να επεκταθεί σε μικρά κομμάτια επιτεύγματος. Η μάθηση μπορεί να αναγνωριστεί σε πολλά επίπεδα, από μικρά μαθησιακά γεγονότα, όπως είναι η ολοκλήρωση ενός διαδικτυακού μαθήματος, ή με την λήψη ενός πανεπιστημιακού πτυχίου το οποίο διαρκεί για πολλά χρόνια. Πολλοί οργανισμοί χρησιμοποιούν ήδη ψηφιακές κονκάρδες για να αναγνωρίσουν την μάθηση. Αυτά τα σήματα μπορούν να εγγραφούν σε ένα Blockchain, ενισχύοντας την αξιοπιστία και την παγκόσμια προσβασιμότητα των κονκάρδων. Τα άτομα μπορούν να προσθέτουν στοιχεία στο Blockchain όπως έργα τέχνης, λογοτεχνικές δημιουργίες, ακαδημαϊκές έρευνες, ή αρχεία εφευρέσεων για την παροχή ενός ασφαλούς δημοσίου καταλόγου του έργου αλλά και της ημερομηνίας δημιουργίας του.

Ένα επόμενο βήμα είναι να γίνονται συναλλαγές όπως και με το Bitcoin ,αλλά αντί για χρήματα να ανταλλάσσεται εκπαιδευτική φήμη. Ένας τρόπος να γίνει αυτό είναι να εκχωρηθεί ένα αρχικό ποσό φήμης στα πανεπιστήμια και σε ιδιώτες με βάση την κατάστασή τους. Αυτό μπορεί να σχετίζεται με την θέση τους διεθνώς ή με σημαντικά επιτεύγματα όπως για παράδειγμα ένα βραβείο νόμπελ. Στην συνέχεια θα μπορούν να απονείμουν μικρές ποσότητες αυτού του νομίσματος φήμης σε φοιτητές που αποφοιτούν ή συνεργάτες. Οργανισμοί και ιδιώτες μπορούν να κερδίσουν περισσότερη φήμη με την παροχή αναγνωρισμένων υπηρεσιών στην εκπαίδευση , όπως παρέχοντας ανοιχτά μαθήματα ή χρηματοδοτώντας έρευνα. Το αρχείο είναι δημόσιο άρα καθένας μπορεί να δει πως ένα πρόσωπο που έχει αποκτήσει εκπαιδευτική φήμη και οι κανόνες για την προσθήκη νέας φήμης συμφωνούνται ομόφωνα.

Αυτή η ιδέα εξόρυξης φήμης μπορεί να ακούγεται παράξενη, αλλά παρόμοιοι μηχανισμοί σχηματίζονται όπως τα Uber, airbnb. Δημιουργούνται πολλές τεχνολογίες για μάθηση εν κινήσει, βαθμολόγηση εκπαιδευτικών και μαθητών, παρακολούθηση δωρεών, παρακολούθηση συνεισφορών στην γνώση και την ανάθεση μικρών ποσών εκπαιδευτικών πιστώσεων ως βραβεία. Το Blockchain καθιστά αυτές τις διαδικασίες πιο ανοικτές και ορατές.

Η Sony Global Education προτείνει να δημιουργηθεί ένα ξεχωριστό Blockchain για αρχεία επιτευγμάτων. Η τεχνολογία Blockchain επιτρέπει στους ανθρώπους να δείξουν τα δημιουργικά τους

έργα και ιδέες σε όλον τον κόσμο, δημιουργώντας αξίωση και εφεύρεση και κερδίζοντας αναγνώριση. Αυτή η τεχνολογία θα μπορούσε να προσφύγει σε υπάρχοντα ιδρύματα που επιθυμούν να κινηθούν προς την ψηφιακή λειτουργία.

6.4 Μελλοντικές Εφαρμογές

Η τεχνολογία Blockchain μπορεί να εφαρμοστεί στην εκπαίδευση με πολλούς καινοτόμους τρόπους πέρα από την διαχείριση πιστοποιητικών και την αξιολόγηση επιτευγμάτων. Τόσο για τους εκπαιδευόμενους όσο και για τους καθηγητές, η τεχνολογία Blockchain έχει πολλές προοπτικές εφαρμογής για την διαμόρφωση , την σχεδίαση και την υλοποίηση μαθησιακών δραστηριοτήτων και την παρακολούθηση όλων των διαδικασιών μάθησης. Ορισμένες καινοτόμες εφαρμογές της τεχνολογίας Blockchain στον τομέα της εκπαίδευσης είναι οι ακόλουθες.

Ένα έξυπνο συμβόλαιο που εκτελείται στο δίκτυο Blockchain του Ethereum είναι ουσιαστικά ένα πρωτόκολλο υπολογιστή που προσομοιώνει μια πραγματική σύμβαση. Μπορεί να διευκολύνει την διαπραγμάτευση των συμβάσεων, να απλοποιήσει τους όρους της σύμβασης, την εκτέλεση της σύμβασης και την επαλήθευση της εκπλήρωσης της σύμβασης. Σηματοδοτεί την μοναδική και ακριβή ταυτότητα των μερών σε μια συναλλαγή μέσω ψηφιακού τρόπου και καθορίζει τα δικαιώματα και τις υποχρεώσεις και των δύο πλευρών με κωδικό. Η έξυπνη σύμβαση όχι μόνο μειώνει τα κόστη τρίτων σε παραδοσιακές συναλλαγές, αλλά εγγυάται δραματικά την ασφάλεια της συναλλαγής και την αξιοπιστία. Για παράδειγμα, στο πλαίσιο της αγοράς αυτοκινήτων, ο αγοραστής διαπραγματεύεται με τον πωλητή απευθείας αντί για δάνεια από την τράπεζα, εξοικονομώντας οποιαδήποτε πρόσθετη επεξεργασία και αμοιβές. Αν ο αγοραστής σπάσει τους κανόνες, ο κώδικας θα εκτελεστεί και η έξυπνη σύμβαση θα τερματιστεί. Το έξυπνο συμβόλαιο βελτιώνει σημαντικά την εκτελεστική εξουσία και δικαιοσύνη από την παραδοσιακή. Ως εκ τούτου, αν οι εκπαιδευτικοί και οι μαθητές εκτελούν διδασκαλία και εκμάθηση δραστηριοτήτων που βασίζονται σε έξυπνο συμβόλαιο, μερικά από τα εκπαιδευτικά ζητήματα θα επιλυθούν.

Από την πλευρά των εκπαιδευομένων, εξακολουθούν να υπάρχουν κάποιοι αρνητικοί παράγοντες που προκαλούν κακά μαθησιακά αποτελέσματα, όπως η έλλειψη κινήτρων και η οικονομική πίεση. Λόγω του χαρακτηριστικού της νομισματικής ιδιοκτησίας, το Blockchain μπορεί να χρησιμοποιηθεί για να παρακινήσει τους μαθητές με την εφαρμογή του «διαβάζω- κερδίζω». Το έξυπνο συμβόλαιο μεταξύ καθηγητών και μαθητών μπορεί να εφαρμοστεί στο εκπαιδευτικό σενάριο διδασκαλίας. Τα βραβεία σε πραγματικό χρόνο μπορούν να δοθούν μέσα από λίγα κλικ από τους εκπαιδευτές. Οι σπουδαστές θα αποκτήσουν έναν ορισμένο αριθμό ψηφιακού νομίσματος σύμφωνα με το συμβόλαιο ως ανταμοιβή. Αυτού του είδους τα χρήματα ,μπορούν να αποθηκευτούν στο πορτοφόλι εκπαίδευσης και να χρησιμοποιούνται ως δίδακτρα.

Η αξιολόγηση είναι ένα επίσης προβληματικό ζήτημα στο εκπαιδευτικό σύστημα. Η διαμορφωτική αξιολόγηση έχει υποστηριχθεί για μεγάλο χρονικό διάστημα, και όμως ακόμα δεν είναι ώριμη, επειδή δεν είναι εύκολο το να παρακολουθείτε κάθε λεπτομέρεια της διδασκαλίας και της μάθησης. Εφαρμόζοντας Blockchain και έξυπνα συμβόλαια μπορεί να αντιμετωπιστεί αυτή η πρόκληση. Ειδικότερα, η αμεταβλητότητα και η αξιοπιστία της αλυσίδας σημαίνει ότι τα δεδομένα που

καταγράφονται στην αλυσίδα είναι πιο συγκεκριμένα, αυθεντικά, και δεν κλέβονται εύκολα. Για παράδειγμα η συνεργατική μάθηση η οποία θεωρείτε μια πολύ καλή μέθοδος για την καθοδήγηση του μαθητή να συνεργαστεί με τους άλλους. Ωστόσο, συχνά συνοδεύεται από το προβλήματα εμποδίζοντας την δίκαιη αξιολόγηση. Η τεχνολογία Blockchain μπορεί να μετριάσει αυτό το φαινόμενο. Κάθε φοιτητής υποβάλλει το έργο του στην πλατφόρμα εκμάθησης μέσω του μοναδικού λογαριασμού του, το έξυπνο συμβόλαιο που τρέχει σε αυτό, θα αναθεωρήσει τις επιδόσεις του μαθητή και τα αποτελέσματα θα καταγραφούν σε μπλοκ. Όλες οι συμπεριφορές κατά την διάρκεια της συνεργασίας θα αποθηκευτούν σε μπλοκ ως αποδεικτικά στοιχεία αξιολόγησης. Επιπλέον, το δημόσιο Blockchain έχει το χαρακτηριστικό της αποκέντρωσης. Αυτό σημαίνει ότι ο κατανεμημένος κατάλογος εξασφαλίζει την συνοχή των περισσότερων κόμβων. Έτσι ως κόμβοι σε δημόσιο Blockchain, οι απόψεις των μαθητών θα λαμβάνονται υπόψη κατά την εκτίμηση τους. Σε αυτό το πλαίσιο το Blockchain διασφαλίζει την δικαιοσύνη και την αξιολόγηση.

Από την πλευρά των εκπαιδευτικών, η διδασκαλία είναι πολύπλοκη και καλλιτεχνική διαδικασία, έτσι είναι δύσκολο να αξιολογηθεί. Η παραδοσιακή μέθοδος που βασίζεται στην ανταπόκριση των μαθητών τείνει να είναι μονόπλευρη, να μην έχει υποκειμενικότητα και είναι δύσκολο να βοηθήσει στην βελτίωση των εκπαιδευτικών. Ένα νέο σύστημα αξιολόγησης μπορεί να κατασκευαστεί με βάση ένα δίκτυο Blockchain και τις έξυπνες συμβάσεις. Πρώτα, οι καθηγητές πρέπει να υποβάλουν τις προγραμματισμένες εκπαιδευτικές δραστηριότητες ως έξυπνες συμβάσεις με τα σχολεία. Κατά την διάρκεια της διδακτικής διαδικασίας , θα καταγραφούν όλες οι δραστηριότητες διδασκαλίας στο δίκτυο Blockchain. Η έξυπνη σύμβαση θα επαληθεύει την συνέπεια του διδακτικού σχεδιασμού και πρακτική, η οποία πρόκειται να αποτελέσει σημαντικό δείκτη αξιολόγησης της διδασκαλίας. Επιπλέον, ένα έξυπνο συμβόλαιο μεταξύ εκπαιδευτικών και σχολείων , καθώς και το συμβόλαιο μεταξύ εκπαιδευτικών και μαθητών μπορεί να επαληθευτεί και συμπληρωθεί μεταξύ τους. Οι εκπαιδευτικού που πληρούν τα πρότυπα θα αποκτήσουν ψηφιακό νόμισμα ως ανταμοιβή. Χρησιμεύει και στα δύο με εκτίμηση και ενθάρρυνση για τις διδακτικές δεξιότητες των εκπαιδευτικών.

Από την άποψη της ανάπτυξης τω σπουδαστών, ο επιβλέπων ή ο ακαδημαϊκός υπεύθυνος έχει την αρμοδιότητα της επίβλεψης του προγράμματος σπουδών. Έχει επίσης τις ευθύνες της παροχής βοήθειας και συμβουλών στον σπουδαστή ώστε να μπορέσει να διαμορφώσει το δικό του πρόγραμμα σπουδών αλλά και να μπορέσει να μείνει ενημερωμένος σχετικά με τις ερευνητικές δραστηριότητες και την πρόοδο των σπουδαστών. Ωστόσο στην πράξη όλα τα παραπάνω είναι αρκετά δύσκολο να ελεγχθούν ή να εποπτευθούν κάτι που συνεπάγεται με αμφιλεγόμενη ευθύνη σε περίπτωση που κάτι αρνητικό συμβεί στο μέλλον. Η τεχνολογία Blockchain σε συνδυασμό με τα έξυπνα συμβόλαια μπορεί να δώσει μια λύση σε αυτόν τον τομέα. Όλες οι λεπτομέρειες μπορούν να παρακολουθούνται από μια πλατφόρμα έξυπνων συμβολαίων και να καταγράφονται σε έναν δημόσιο κατάλογο Blockchain. Λεπτομέρειες όπως πόσες φορές έχει εξετάσει ο επιβλέπων την διατριβή σε σχέδιο αλλά και σε τελική μορφή, εάν υπάρχει κατάλληλη καθοδήγηση στους μαθητές για την επιλογή μαθημάτων και τον σχεδιασμό έρευνας, κλπ. Η τεχνολογία Blockchain παρέχει την δυνατότητα της καταγραφής των συμπεριφορών των φοιτητών αλλά και των καθηγητών, πράγμα που προστατεύει τα συμφέροντα και των δύο πλευρών.

Συνολικά η τεχνολογία Blockchain μπορεί να χρησιμοποιηθεί για την κατασκευή μιας ισορροπίας για την μέτρηση της μαθησιακής διαδικασίας και των αποτελεσμάτων αυτής. Αποτελεί μια αξιόπιστη και ισότιμη απόδειξη αξίας για όλους. Θεωρητικά η τεχνολογία αυτή μπορεί να λύσει τα προβλήματα της ασύμμετρης πληροφόρησης και της εμπιστοσύνης μεταξύ των ξένων, λόγο της αποκέντρωσης και της αμεταβλητότητας που παρέχει. Εξασφαλίζει την αυθεντικότητα επειδή οι πληροφορίες και η αξία δημοσιεύονται και διατηρούνται συλλογικά. Παρέχει έναν αξιόπιστο τρόπο για την επένδυση ταλέντων. Ο χρήστης με περισσότερη εκπαίδευση στα ψηφιακά νομίσματα έχει περισσότερες πιθανότητες να πετύχει σε μελλοντικές επενδύσεις. Ο κατάλογος του Blockchain περιλαμβάνει όλα όσα έχει μάθει ένας εκπαιδευόμενος και οι εργοδότες μπορούν να χρησιμοποιήσουν αυτές τις πληροφορίες για να προσφέρουν μια δουλειά που ταιριάζει με τις ικανότητες του καθένα. Επίσης εάν κάποιος χρήστης θέλει έναν εξαιρετικό εργοδότη μπορεί και αυτός να καταφύγει στον κατάλογο. Η τεχνολογία αυτή μεγιστοποιεί τα συμφέροντα και των δύο μερών.

6.5 Τα αρνητικά του Blockchain

Είναι αναμφισβήτητο ότι υπάρχουν δυνητικά μειονεκτήματα στην εφαρμογή της τεχνολογίας Blockchain στην εκπαίδευση. Η εκπαιδευτική διαδικασία και ειδικότερα η διαδικασία της διδασκαλία περιλαμβάνει και θέματα που πρέπει να αναθεωρούνται από τους εκπαιδευτικού, τα δοκίμια, οι παρουσιάσεις και η καθημερινή συμμετοχή αποτελούν ζητήματα που δεν λύνει η τεχνολογία Blockchain. Είναι αρκετά δύσκολο να αξιολογηθεί αυτό το είδος των μαθησιακών δραστηριοτήτων από ένα έξυπνο συμβόλαιο χωρίς την ανθρώπινη παρέμβαση του δασκάλου ή του καθηγητή.

Εάν ένα τεθεί σε χρήση από τα σχολεία ένας κατάλογος Blockchain, όλα τα δεδομένα των μαθητών θα ενσωματωθούν σε αυτόν τον κατάλογο. Η αμεταβλητότητα της τεχνολογίας θα λειτουργούσε ως «δίκοπο μαχαίρι». Δεν επιτρέπει την τροποποίηση εκπαιδευτικών αρχείων, ακόμα και για νόμιμους λόγους, που αφορούν τους μαθητές.

Επίσης δεν αντιμετωπίζονται πολλά τεχνικά ζητήματα. Ένα τέτοιο ζήτημα είναι ότι το κλασικό «proof of work», σπαταλάει ενέργεια και έχει κακή απόδοση σε ρυθμό ανά δευτερόλεπτο, κάτι που συνεπάγεται με ένα ακόμα έξοδο και εμποδίζει την εφαρμογή του στα σχολεία.

Παρόλα αυτά, η τεχνολογία αυτή παρέχει τεράστιες δυνατότητες πολλές από τις οποίες ακόμα βρίσκονται σε αρχικά στάδια, μπορεί να δώσει κίνητρο στους μαθητές εφαρμόζοντας το «μαθαίνω - κερδίζω», μπορεί να δώσει κίνητρα στους διδάσκοντες αλλά και να κάνει πιο εύκολη την ζωή τους.

7. BLOCKCHAINS ΚΑΙ IOT [17],[18],[19],[20],[21],[22],[23],[24],[25]

7.1 Εισαγωγή

Το διαδίκτυο των πραγμάτων (IoT), αποτελεί ένα δίκτυο επικοινωνίας πληθώρας συσκευών, οικιακών συσκευών, αυτοκινήτων καθώς και κάθε αντικειμένου που ενσωματώνει ηλεκτρικά μέσα, λογισμικό, αισθητήρες και συνδεσιμότητα σε δίκτυο ώστε να επιτρέπεται η σύνδεση και η ανταλλαγή δεδομένων. Απλούστερα, η φιλοσοφία του IoT είναι η σύνδεση όλων των ηλεκτρικών συσκευών μεταξύ τους ή με δυνατότητα σύνδεσης στο διαδίκτυο. Η έννοια «πράγματα», δεν είναι αυστηρά συνδεδεμένη με ορισμένα προϊόντα. Αναφέρεται σε μια ευρεία ποικιλία συσκευών εντελώς διαφορετικά μεταξύ τους, όπως για παράδειγμα αυτοκίνητα με ενσωματωμένους αισθητήρες, κάμερες, κλιματιστικά, φώτα, συστήματα ασφαλείας, smartwatches ακόμα και αυτοκίνητα των οποίων οι περίπλοκοι αισθητήρες εντοπίζουν αντικείμενα στην πορεία τους. Είναι μερικά από τα πολλά προϊόντα τεχνολογίας, βασικό χαρακτηριστικό όλων είναι η σύνδεση μεταξύ τους με απώτερο σκοπό την δυνατότητα του χρήστη να τα ελέγχει από έναν υπολογιστή ή κινητό.

Το ίντερνετ των πραγμάτων χρησιμοποιείται σε πολλούς τομείς όπως, υγειονομική περίθαλψη, βιομηχανική παραγωγή, λιανεμπόριο, τηλεπικοινωνίες, μεταφορές, ενέργεια και άλλα πολλά. Το Blockchain μπορεί να δώσει μια νέα οπτική στον τρόπο με τον οποίο επιτελούνται οι εργασίες στο IoT. Στις επόμενες ενότητες γίνεται λόγος για όλα αυτά και παρατίθενται και κάποια παραδείγματα χρήσης που περιλαμβάνουν την τεχνολογία Blockchain σε συνδυασμό με το ίντερνετ των πραγμάτων.

7.2 IoT

Πλέον εν έτη 2018, γίνεται μια στροφή προς μια αποκεντρωμένη αρχιτεκτονική έτσι ώστε ένα οικοσύστημα IoT να είναι βιώσιμο. Από την πλευρά των κατασκευαστών, το σημερινό κεντρικό μοντέλο έχει υψηλό κόστος συντήρησης λαμβάνοντας υπόψη την διανομή ενημερώσεων λογισμικού σε εκατομμύρια συσκευές για αρκετά χρόνια. Από την πλευρά των καταναλωτών, υπάρχει μια δικαιολογημένη έλλειψη εμπιστοσύνης στις συσκευές «phone home» στο παρασκήνιο, δηλαδή τις συσκευές που ελέγχουν το σπίτι, υπάρχει ανάγκη για την δημιουργία μιας προσέγγισης της ασφάλειας μέσω της διαφάνειας. Αυτά τα προβλήματα μπορούν να επιλυθούν με ένα αξιόπιστο μοντέλο ενός ομότιμου δικτύου, που μπορεί να λειτουργήσει με διαφάνεια και να διανέμει δεδομένα με ασφαλή τρόπο, η τεχνολογία Blockchain παρέχει μια κομψή λύση σε αυτό το πρόβλημα.

Όλες οι συσκευές ενός κατασκευαστή μπορούν να λειτουργούν στο ίδιο δίκτυο Blockchain. Ο κατασκευαστής έχει την δυνατότητα να εφαρμόσει ένα έξυπνο συμβόλαιο που επιτρέπει την αποθήκευση ενός hash της τελευταίας ενημέρωσης λογισμικού στο δίκτυο. Οι συσκευές παραδίδονται με την διεύθυνση του έξυπνου συμβολαίου που υπάρχει στην αλυσίδα πελάτη, ή το βρίσκουν μέσω μιας υπηρεσίας ανακάλυψης. Μπορούν να ζητήσουν στην συνέχεια την σύμβαση , και να ενημερωθούν για την νέα ενημέρωση και να την ζητήσουν μέσω του hash στο ομότιμο δίκτυο. Τα πρώτα αιτήματα για αυτό το αρχείο θα εξυπηρετηθούν από τον κόμβο του κατασκευαστή, αλλά εφόσον δοθεί σε άλλους κόμβους, ο κόμβος του κατασκευαστή μπορεί να σταματήσει να εξυπηρετεί. Με την προϋπόθεση ότι οι συσκευές έχουν ρυθμιστεί ώστε να μοιράζονται αυτό που λαμβάνουν, μια συσκευή που συνδέεται στο

δίκτυο μετά την διακοπή συμμετοχής του κατασκευαστή, μπορεί ακόμα να λάβει την ενημέρωση και να βεβαιωθεί ότι είναι σωστή. Όλα αυτά συμβαίνουν αυτόματα, χωρίς καμία αλληλεπίδραση των χρηστών. Η παραπάνω περίπτωση χρήσης είναι πολύ πιο καλή και αποδοτική από την κλασική κεντρική χρήση, όπου η συσκευή διερευνά τον εξυπηρετητή του κατασκευαστή για ενημέρωση και συχνά λαμβάνει απάντηση σφάλματος.

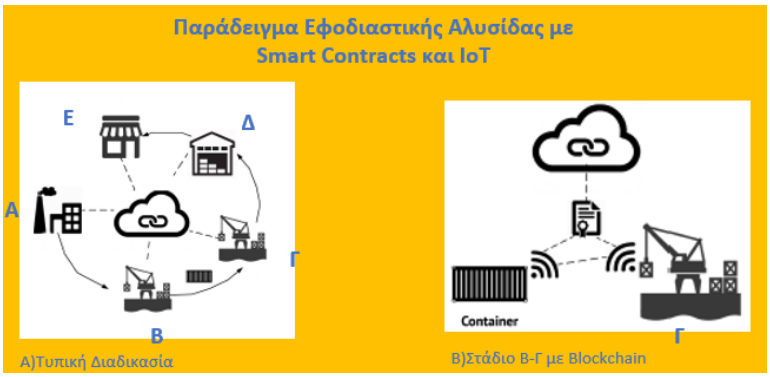
Επιπλέον, ένα δίκτυο Blockchain στο οποίο ανταλλάζονται κρυπτονομίσματα, παρέχει ένα βολικό τρόπο χρέωσης και ανοίγει ο δρόμος για μια αγορά υπηρεσιών μεταξύ συσκευών. Στο παραπάνω παράδειγμα, οι συσκευές που αποθηκεύουν ένα αντίγραφο της ενημέρωσης μπορούν να επιβραβεύονται για την εξυπηρέτηση, ώστε να διατηρηθεί το κόστος υποδομής. Άλλα παραδείγματα αποτελούν το Filecoin, που επιτρέπει σε συσκευές να νοικιάζουν τον χώρο στον δίσκο τους, το EtherAPIs, το οποίο επιτρέπει την δημιουργία εσόδων από κλήσεις API, αυτός που το καλεί θα πρέπει πρώτα να υποβάλει μια μικρή πληρωμή. Με την χρήση των κρυπτονομισμάτων κάθε συσκευή μπορεί να έχει τον δικό της τραπεζικό λογαριασμό στο διαδίκτυο, και να δανείζει τους πόρους της σε άλλες συσκευές λαμβάνοντας πάντα μια αποζημίωση για την χρήση αυτή.

Αυτό διευκολύνει επίσης την γενικότερη ανταλλαγή υπηρεσιών και περιουσίας. Το Slock.it δουλεύει με έξυπνες ηλεκτρονικές κλειδαριές, που μπορούν να ξεκλειδωθούν με μια συσκευή που φέρει το κατάλληλο τόκεν, αυτά τα τόκεν αγοράζονται στην αλυσίδα του Ethereum. Ο ιδιοκτήτης ενός Slock που επιθυμεί να νοικιάσει το σπίτι του ή το αυτοκίνητό του βάζει μια τιμή για την χρονική πρόσβαση σε αυτήν την ηλεκτρονική κλειδαριά. Μπορεί να χρησιμοποιηθεί μια εφαρμογή κινητού για να προσδιορίσει το Slock, η πληρωμή γίνεται με το αντίστοιχο νόμισμα της συγκεκριμένης υπηρεσίας και στην συνέχεια ξεκλειδώνετε. Η τιμολόγηση είναι πολύ απλή, όλα τα Slocks βρίσκονται στο ίδιο Blockchain.

Στο ίδιο θέμα, στον τομέα της ενέργειας, η ενσωμάτωση των Blockchain στο IoT, επιτρέπει μια ομότιμη αγορά όπου οι μηχανές μπορούν να αγοράζουν και να πουλούν ενέργεια αυτόματα, σύμφωνα με τα κριτήρια που ορίζει ο χρήστης. Για παράδειγμα, το TransActive Grid πειραματίζεται με την έννοια της ομότιμης αγοράς ανανεώσιμων πηγών ενέργειας σε μια γειτονιά του Μπρούκλιν. Τα ηλιακά πάνελ καταγράφουν την πλεονάζουσα παραγωγή τους σε ένα Blockchain και την πουλάνε σε γειτονικά μέρη με την χρήση έξυπνων συμβάσεων.

Η χρησιμότητα των Blockchains στο IoT δεν σταματάει εκεί. Σε ένα τυπικό παράδειγμα εφοδιαστικής αλυσίδας, ένα κοντέινερ που εγκαταλείπει την τοποθεσία του κατασκευαστή (Α), μεταφέρεται μέσω της σιδηροδρομικής γραμμής προς ένα γειτονικό λιμάνι (Β), και έπειτα αποστέλλεται προς την θύρα προορισμού (Γ), μεταφέρεται και πάλι στις εγκαταστάσεις του διανομέα (Δ) μέχρι να φτάσει στο σημείο πώλησης (Ε). Αυτή η διαδικασία περιλαμβάνει πολλά ενδιαφερόμενα μέρη και συνεχής ελέγχους στην πορεία. Κάθε ενδιαφερόμενος διατηρεί συνήθως την δική του βάση δεδομένων για την παρακολούθηση του στοιχείου, το οποίο ενημερώνεται με βάση τα στοιχεία που εισάγουν τα άλλα μέρη της αλυσίδας. Ένα δίκτυο με Blockchain που έχει ρυθμιστεί να παρακολουθεί το συγκεκριμένο περιουσιακό στοιχείο, σημαίνει αυτόματα ότι υπάρχει μια κοινή βάση δεδομένων για την παρακολούθηση, οι ενημερώσεις κατάστασης καταφθάνουν με κρυπτογραφική ασφάλεια και διαδίδονται κατά μήκος του δικτύου αυτόματα, έτσι δημιουργείται έναν ελεγχόμενο μονοπάτι

πληροφοριών. Στο παραπάνω παράδειγμα, όταν η μεταφορά φτάσει στον σημείο της θύρας προορισμού, στέλνουν ένα υπογεγραμμένο μήνυμα σε μια προκαθορισμένη και συμφωνημένη έξυπνη σύμβαση έτσι ώστε να επιτρέψει σε όλους όσους βρίσκονται στην αλυσίδα να γνωρίζουν που βρίσκεται το κοντέινερ. Δεδομένου ότι η συναλλαγή υπογράφεται, καθιστάτε κρυπτογραφικά αποδεκτή. Αυτός που λαμβάνει στα λιμενικά σημεία ενημερώνει στην ίδια έξυπνη σύμβαση την επιβεβαίωση της τοποθεσίας του κοντέινερ.

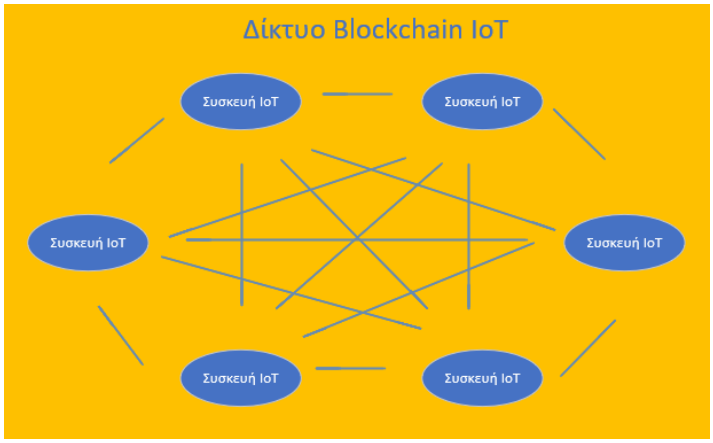


Εικόνα 20 Παράδειγμα Κοντέινερ με Smart Contracts και IoT

7.3 IoT και Ασφάλεια

Το ίντερνετ των πραγμάτων έχει πολλές εφαρμογές στην καθημερινότητα ενός ανθρώπου, όπως για παράδειγμα στην δημιουργία έξυπνων σπιτιών, έξυπνων πόλεων, στην βελτίωση της υγείας, στα αυτόνομα οχήματα κλπ. Αρκετές από αυτές τις συσκευές είναι διαθέσιμες σε όλους όπως τα έξυπνα ρολόγια, τα έξυπνα συστήματα θέρμανσης, τα κλιματιστικά και ψυγεία που χρησιμοποιούν wi-fi για την παρακολούθηση. Εκτός από όλα αυτά τα οφέλη που προφέρουν αυτές οι συσκευές, ο συγκεκριμένος τομέας αντιμετωπίζει και αρκετά προβλήματα, τα οποία είναι απαραίτητο να επιλυθούν. Έχουν δημιουργηθεί αρκετά σφάλματα στις τεχνολογίες που βρίσκονται στα θεμέλια του IoT, κάτι που τα καθιστά ευάλωτα σε επιτιθέμενους που μπορούν να επωφεληθούν από αυτά τα σφάλματα και να θέσουν σε κίνδυνο την ιδιωτική ζωή των χρηστών. Έτσι πριν την από την εφαρμογή όλων αυτών των συστημάτων IoT είναι απαραίτητο να ενισχυθεί η ασφάλεια και να εκμηδενισθούν τα σφάλματα. Η παραπάνω αποτελεί μια πολύ δύσκολη αλλά και ταυτόχρονα αναγκαία διαδικασία. Συχνά η πρακτική να είναι αυτές οι συσκευές όσο πιο φθηνές, μικρές και εύχρηστες δημιουργεί προβλήματα στις πολιτικές της ασφάλειας, γεγονός που αυξάνει τον κίνδυνο για τις παραβιάσεις.

Στην επόμενη εικόνα αναπαριστάτε ένα πρότυπο δικτύου του IoT με βάση την τεχνολογία Blockchain. Το μοντέλο επικοινωνίας περιλαμβάνει αποστολή μηνυμάτων σε ομότιμο δίκτυο, κατανεμημένη κοινή χρήση δεδομένων και αυτόνομο συντονισμό με την συσκευή. Παρόλα αυτά έχει τους δικούς του περιορισμούς οι οποίοι καθιστούν προβληματική την εφαρμογή, αυτοί οι περιορισμοί είναι η αργή επεξεργασία(λόγο Blockchain) και ο μικρός χώρος αποθήκευσης(λόγο του μεγέθους του καταλόγου που αυξάνεται συνεχώς).



Εικόνα 21 Δίκτυο Blockchain για συσκευές IoT

Ωστόσο, οι εταιρείες όπως η IOTA, που ασχολούνται με μικρούς αισθητήρες Blockchain, προτείνουν νέες προσεγγίσεις, με λιγότερες απαιτήσεις υλικού και με απλοποιημένες διαδικασίες εξόρυξης. Σε αυτό το σημείο παρουσιάζεται μια αρχιτεκτονική ενός δικτύου Blockchain. Οι κόμβοι του δικτύου συμμετέχουν ενεργά στην διαδικασία της συναλλαγής, επικυρώνουν την συναλλαγή μέσω της εξόρυξης, μπορούν να είναι προσωπικοί υπολογιστές, εξυπηρετητές κλπ. Οι πελάτες είναι οι συσκευές IoT, δεν αποθηκεύουν τον κατάλογο. Οι κόμβοι του Blockchain αλληλεπιδρούν μεταξύ τους με την χρήση APIs. Οι συσκευές IoT δημιουργούν συναλλαγές και αυτές οι συναλλαγές μεταβιβάζονται σε κόμβους του Blockchain για την επεξεργασία και αποθήκευση των δεδομένων στον κατάλογο. Για την αποφυγή επιθέσεων τύπου «man in the middle» που μπορούν να επηρεάσουν τις λεπτομέρειες της συναλλαγής ή να προκαλέσουν μια διπλή δαπάνη, πρέπει να υπάρχει απόλυτη εμπιστοσύνη μεταξύ των πελατών και των κόμβων με τους οποίους είναι συνδεδεμένοι. Τα μηνύματα που ανταλλάσσονται μεταξύ των συσκευών IoT περιέχουν δεδομένα, τα οποία είναι άμεσα συνδεδεμένα με τις συναλλαγές που μεταδίδονται από τις συσκευές που συμμετέχουν με τις συναλλαγές των κόμβων Blockchain.

Εικόνα 22 Αρχιτεκτονική Διαμοιρασμού Δεδομένων

Η σύνδεση πολλών αλυσίδων Blockchain αποτελεί μια αρκετά σημαντική διαδικασία, σύμφωνα με έρευνες στο μέλλον προβλέπεται ότι θα υπάρχει ένα μεγάλο πλήθος από αλυσίδες κάθε μια από τις οποίες θα εκτελεί και διαφορετική λειτουργία. Στο παραπάνω παράδειγμα το Blockchain αποτελεί ένα οικιακό δίκτυο, οι μορφές μηνυμάτων και τα πρωτόκολλα επικοινωνίας μεταξύ των συσκευών είναι εκτός του πεδίου εφαρμογής της τεχνολογίας Blockchain , αναφέρεται στην επικοινωνία από μηχανή σε μηχανή. Η τεχνητή νοημοσύνη μπορεί να παίξει ένα σημαντικό ρόλο σε όλο αυτό το εγχείρημα και να δημιουργήσει ένα αυτόνομο αποκεντρωμένο οργανισμό, δηλαδή σε έναν οργανισμό που εκτελείτε χωρίς καμία ανθρώπινη παρέμβαση.

7.3.1 Αύξηση της Ασφάλειας με χρήση Blockchain

Η τεχνολογία Blockchain προσφέρει μηχανισμούς για την αύξηση της ασφάλειας στον τομέα του IoT. Δίνει νέες προοπτικές στην ασφαλή επικοινωνία, στον έλεγχο ταυτότητας χρηστών, στην χρήση του σε μεγάλη κλίμακα και στην ρύθμιση της διασύνδεσης. Σε ορισμένες περιπτώσεις οι συσκευές IoT πρέπει να επικοινωνούν για την ανταλλαγή δεδομένων που απαιτούνται για την επεξεργασία μιας συναλλαγής και για την αποθήκευση στον κατάλογο.

Αυτοί οι κατάλογοι μπορούν να χρησιμοποιηθούν και για την αποθήκευση των κλειδιών κρυπτογράφησης ώστε να καθιστούν τις συναλλαγές πιο εμπιστευτικές. Μια συσκευή στέλνει ένα κρυπτογραφημένο μήνυμα χρησιμοποιώντας το δημόσιο κλειδί της συσκευής προορισμού, η οποία στην συνέχεια αποθηκεύεται στο δίκτυο του Blockchain. Ο αποστολέας ζητάει από τον κόμβο του να πάρει το δημόσιο κλειδί του δέκτη από τον κατάλογο. Στην συνέχεια ο αποστολέας κρυπτογραφεί το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του δέκτη, με αυτόν τον τρόπο μόνο ο δέκτης είναι σε θέση να αποκρυπτογραφήσει το απεσταλμένο μήνυμα χρησιμοποιώντας το ιδιωτικό κλειδί του.

Στον έλεγχο ταυτότητας των χρηστών ο αποστολέας υπογράφει ψηφιακά το μήνυμα πριν το στείλει σε άλλες συσκευές. Η συσκευή λήψης λαμβάνει το δημόσιο κλειδί από τον κατάλογο και το χρησιμοποιεί για να επαληθεύσει την ψηφιακή υπογραφή από το μήνυμα που έλαβε. Η διαδικασία της ψηφιακής υπογραφής γίνεται ως εξής, αρχικά ο αποστολέας υπολογίζει το hash ενός μηνύματος που είναι κρυπτογραφημένο με το ιδιωτικό κλειδί του, η ψηφιακή υπογραφή μεταδίδεται μαζί με το μήνυμα. Ο δέκτης στην συνέχεια αποκρυπτογραφεί την ψηφιακή υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα που είναι αποθηκευμένο στον κατάλογο, ώστε να βρει το hash όπως υπολογίστηκε από τον αποστολέα. Το μήνυμα είναι έγκυρο μόνο εάν το hash που υπολογίστηκε και το hash του μηνύματος είναι ίδια. Η εμπιστοσύνη στα ανακτημένα μηνύματα βελτιώνεται εάν η ψηφιακή υπογραφή κάθε μηνύματος αποθηκεύεται στο ημερολόγιο.

Το IoT μπορεί να χρησιμοποιηθεί νόμιμα και σε μεγάλη κλίμακα. Με την προοπτική ότι εκατομμύρια συσκευές IoT θα είναι συνδεδεμένες στο δίκτυο, κρίνεται επιτακτική η ανάγκη να δημιουργηθεί η ικανότητα της ανακάλυψης συσκευών σε κλίμακα και την διάκριση των νόμιμων και παράνομων κόμβων. Μόλις ξεκινήσει μια νέα συσκευή, πρώτα ζητάει από τους αρχικούς εξυπηρετητές να την δώσουν μια λίστα από αξιόπιστους κόμβους στο δίκτυο. Έπειτα αυτή η συσκευή εγγράφεται στον κόμβο και στην συνέχεια αρχίζει η ανταλλαγή πληροφοριών. Λαμβάνει πληροφορίες από άλλους κόμβους τις στέλνει σε άλλους κόμβους στο δίκτυο.

Σε ένα δημόσιο δίκτυο αυτή η μέθοδος μπορεί να είναι εύκολη χωρίς συγκεκριμένους περιορισμούς. Σε ένα ιδιωτικό δίκτυο πρέπει να υπάρξει βεβαίωση γιατί μόνο οι νόμιμες συσκευές μπορούν να προστεθούν στο δίκτυο του Blockchain. Για αυτό οι αρχικοί εξυπηρετητές πρέπει να πιστοποιήσουν την συσκευή πριν δώσουν την λίστα των έμπιστων κόμβων. Για να διασφαλιστεί η ακεραιότητα και εμπιστευτικότητα, κάθε επικοινωνία που γίνεται πρέπει να είναι αποτελεσματικά πιστοποιημένη και κρυπτογραφημένη. Αυτό μπορεί να γίνει με διαπιστευτήρια που είναι ήδη εγκατεστημένα στην συσκευή κατά την διάρκεια της εγκατάστασης, πρέπει να υπάρχει μια ασφαλής διαδικασία, η οποία θα μπορούσε να είναι μέρος της αλυσίδας, και να δημιουργεί διαπιστευτήρια. Τα διαπιστευτήρια επίσης θα μπορούσαν να δοθούν από τον ιδιοκτήτη της συσκευής, αρχικοποιεί την διαδικασία εγγραφής συσκευής στον διακομιστή ασφαλείας για να λάβει διαπιστευτήρια από το διαδίκτυο.

Η τεχνολογία Blockchain βοηθά πολύ στην δημιουργία μιας αξιόπιστης και ασφαλούς διαμόρφωσης της IoT συσκευής. Οι ιδιότητες της συσκευής, όπως οι λεπτομέρειες διαμόρφωσης και οι τελευταίες ενημερώσεις λογισμικού μπορούν να αποθηκευτούν στον κατάλογο. Κατά την διάρκεια εκκίνησης ο κόμβος ζητάει να πάρει το αρχείο διαμόρφωσης από τον κατάλογο. Αυτό το αρχείο πρέπει να είναι κρυπτογραφημένο ώστε να αποφευχθεί η ανακάλυψη της τοπολογίας του δικτύου ή οι λεπτομέρειες αυτού που βρίσκονται στον κατάλογο.

Η τιμή hash του τελευταίου αρχείου ρυθμίσεων για κάθε συσκευή μπορεί να φιλοξενηθεί στον κατάλογο. Χρησιμοποιώντας μια υπηρεσία cloud η συσκευή θα πρέπει να κατεβάσει το τελευταίο και πιο αξιόπιστο αρχείο ρυθμίσεων. Στην συνέχεια μπορεί να χρησιμοποιήσει την εφαρμογή του κόμβου αλυσίδας για την αντιστοίχηση των hash. Αυτό θα επιτρέψει στους διαχειριστές να αφαιρέσουν κάθε κακή εκκίνηση και να επανεκκινήσεων κάθε συσκευή, στο δίκτυο με τις πιο πρόσφατες διαμορφώσεις.

7.3.1.1 Παράδειγμα Δικτύου

Η επόμενη εικόνα δείχνει μια σειρά συσκευών που διασυνδέονται μεταξύ τους στο δίκτυο. Είναι ασφαλισμένες με Blockchain, το δίκτυο καθιστά το σύστημα αποκεντρωμένο στο οποίο δεν υπάρχει κάποια κεντρική αρχή η οποία μπορεί να εγκρίνει οποιαδήποτε συναλλαγή. Κάθε συσκευή έχει ένα αντίγραφο της συνεχώς αυξανόμενης αλυσίδας δεδομένων. Αυτό σημαίνει ότι κάθε φορά που κάποιος επιθυμεί να έχει πρόσβαση στην συσκευή και να κάνει κάποια συναλλαγή, τότε όλα τα μέλη της στο δίκτυο πρέπει να την επικυρώσουν. Μετά την ολοκλήρωση της επικύρωσης, η πραγματοποιηθείσα συναλλαγή αποθηκεύεται σε ένα μπλοκ και αποστέλλεται σε όλους τους κόμβους του δικτύου. Όλα αυτά κάνουν το σύστημα ασφαλέστερο και είναι αδύνατο για τις μη εξουσιοδοτημένες πηγές να παραβιάζουν την ασφάλεια.

Εικόνα 23 Ασφάλεια IoT Συσκευών

7.3.1.2 Παράδειγμα Εφαρμογής με Κάμερα

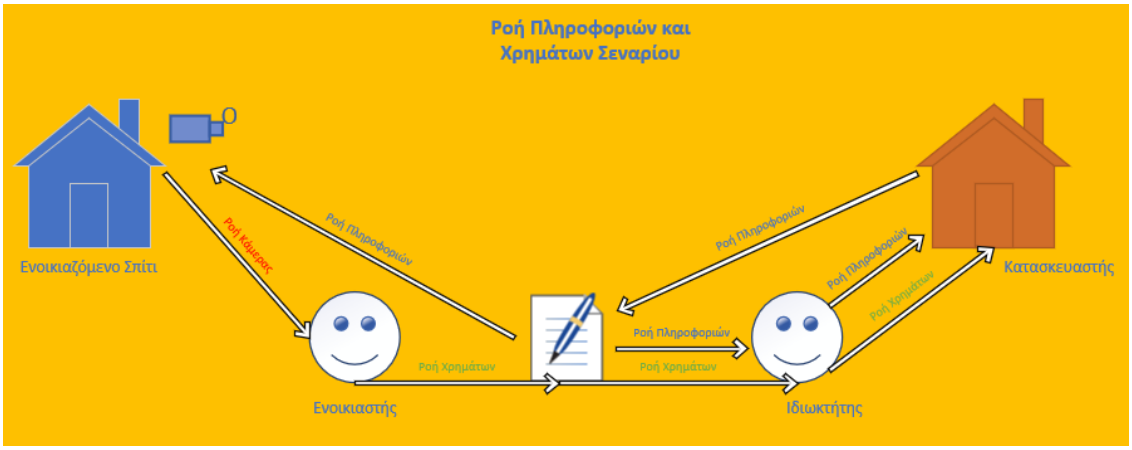
Σε αυτό το σημείο εξετάζεται ένα σενάριο με μια κάμερα ασφαλείας σε ένα ενοικιαζόμενο σπίτι. Η κάμερα ελέγχεται από ένα έξυπνο συμβόλαιο στο Blockchain, το οποίο δημιουργείται από τον κατασκευαστή της κάμερας μόλις αυτή κατασκευαστεί. Λόγο του ασύμμετρου μηχανισμού κρυπτογράφησης που χρησιμοποιείται από την κάμερα για να μεταφέρεται με ασφάλεια η ροή, το δημόσιο κλειδί της κάμερας είναι ασφαλισμένο μέσα στο έξυπνο συμβόλαιο, ενώ το ιδιωτικό κλειδί αποθηκεύεται με ασφάλεια στην συσκευή. Όταν ο αγοραστής αγοράζει την κάμερα, δίνει στον κατασκευαστή πληροφορίες σχετικά με την αλυσίδα αλλά και με την διεύθυνση ίντερνετ στην οποία επιθυμεί να αποστέλλεται η ροή της κάμερας. Όταν λάβει αυτές τις πληροφορίες ο κατασκευαστής τις κωδικοποιεί στο έξυπνο συμβόλαιο ως πληροφορίες ιδιοκτήτη και στην συνέχεια δημοσιεύεται στο Blockchain. Εκτός από το δημόσιο κλειδί της κάμερας και τις πληροφορίες ιδιοκτήτη, το έξυπνο συμβόλαιο έχει επίσης ένα σύνολο πεδίων σχετικά με τις πληροφορίες ενοικιαστή. Μετά την ενοικίαση της συσκευής ο ενοικιαστής μπορεί να γεμίσει αυτά τα πεδία αποστέλλοντας ένα μήνυμα αρχικοποίησης στην σύμβαση.

Τα πεδία πληροφοριών του ενοικιαστή περιλαμβάνουν το δημόσιο κλειδί του ενοικιαστή που πρέπει να χρησιμοποιηθεί για την κρυπτογράφηση της ροής της κάμερας και της διεύθυνσης στο διαδίκτυο στην οποία ο ενοικιαστής θέλει να αποσταλεί η ροή. Προκειμένου να αποφευχθεί η κατάχρηση ης σύμβασης από τους αντιπάλους, το μήνυμα αρχικοποίησης πρέπει να υπογραφεί από τον ιδιοκτήτη της σύμβασης. Στο συμβόλαιο θα πρέπει επίσης να γίνεται ξεκάθαρο για πόσο χρονικό διάστημα η ροή θα στέλνεται προς τον επισκέπτη, αυτή η διάρκεια καθορίζεται από το μήνυμα.

Λόγου του ότι η διάρκεια της σύμβασης αναφέρεται στο συμβόλαιο, ο ενοικιαστής μπορεί να βεβαιωθεί ότι ο κάτοχος δεν θα μπορέσει να τερματίσει την λειτουργία του συμβολαίου και να ανακατευθύνει το ρεύμα των δεδομένων πίσω στον εαυτό του ενώ το ακίνητο εξακολουθεί να είναι νόμιμα κατειλημμένο από τον ενοικιαστή. Από την άλλη μεριά, ο ιδιοκτήτης θα πρέπει επίσης να είναι σε θέση να διασφαλίσει ότι θα αποζημιωθεί για την εκμίσθωση της τροφοδοσίας της κάμερας στον ενοικιαστή. Για να εξασφαλιστεί η αποζημίωση, η σύμβαση περιέχει επίσης ένα ποσό το οποίο θα

μεταφερθεί στους ιδιοκτήτες κατά την λήξη της σύμβασης. Αυτό το ποσό είναι η αξία που σχετίζεται με το μήνυμα αρχικοποίησης που αποστέλλεται από τον ενοικιαστή και θα αποσυρθεί από τον λογαριασμό του ενοικιαστή που έλαβε την σύμβαση. Θα κλειδωθεί στην σύμβαση μέχρι το τέλος της διάρκειας, έπειτα το υπόλοιπο θα μεταφερθεί στον λογαριασμό του ιδιοκτήτη που έχει κωδικοποιηθεί με ασφάλεια στο συμβόλαιο.

Τέλος τα έξυπνα συμβόλαια πρέπει να τερματιστούν, αυτό γίνεται μέσα από μια ενέργεια, αυτό γίνεται από τον ιδιοκτήτη μόλις περάσει η περίοδος ενοικίασης. Το μήνυμα τερματισμού γίνεται δεκτό και επεξεργάζεται μόνο από το έξυπνο συμβόλαιο, εφόσον πρόκειται να προστεθεί από τον ιδιοκτήτη και εάν έχει περάσει η συμβατική περίοδος.



Εικόνα 24 Παράδειγμα με Κάμερα Ασφαλείας

7.4 Έξυπνο Σπίτι

Ένα έξυπνο σπίτι είναι οποιοδήποτε προσωπικό ή εργασιακό περιβάλλον που περικλείει ένα σύνολο τεχνολογικών εφαρμογών με κύριο χαρακτηριστικό την αυτοματοποίηση και τον έλεγχο των επιμέρους τμημάτων του.

7.4.1 Συστατικά Στοιχεία

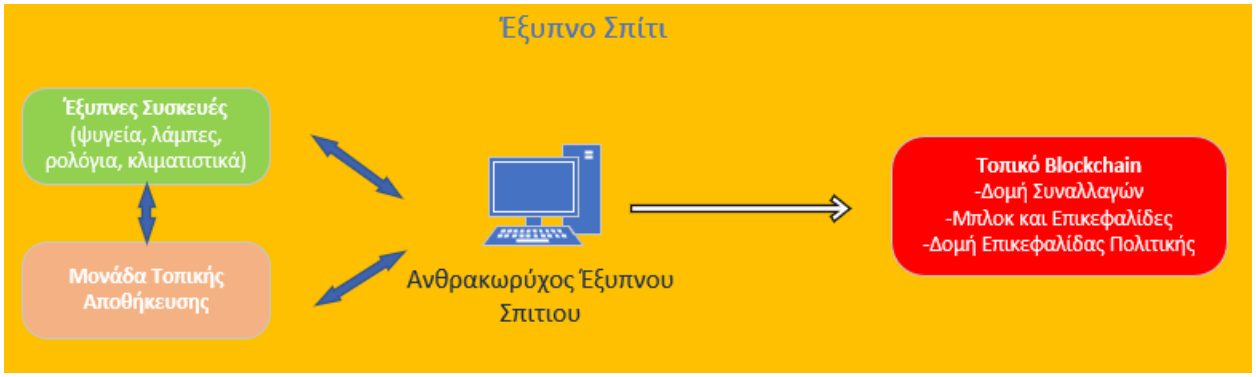
Οι επικοινωνίες μεταξύ τοπικών συσκευών ή κόμβων επικάλυψης είναι γνωστές ως συναλλαγές. Υπάρχουν διάφορες συναλλαγές σε ένα έξυπνο σπίτι που βασίζονται στην τεχνολογία Blockchain, κάθε μια σχεδιασμένη για μια συγκεκριμένη λειτουργία. Οι συναλλαγές αποθήκευσης παράγονται από τις συσκευές για την αποθήκευση δεδομένων. Μια συναλλαγή πρόσβασης δημιουργείται από τον παροχέα υπηρεσιών ή από τον ιδιοκτήτη του σπιτιού που έχει πρόσβαση στο cloud storage. Μια συναλλαγή παρακολούθησης δημιουργείται από τον ιδιοκτήτη του σπιτιού ή τους παρόχους υπηρεσιών για την περιοδική παρακολούθηση μιας συσκευής και για πληροφορίες. Η προσθήκη μιας νέας συσκευής στο έξυπνο σπίτι γίνεται μέσο μιας συναλλαγής αρχικοποίησης, ενώ μια συσκευή καταργείτε με μια συναλλαγή κατάργησης. Όλες οι παραπάνω συναλλαγές χρησιμοποιούν ένα κοινόχρηστο κλειδί για να εξασφαλιστεί η ασφάλεια της επικοινωνίας. Ένα ελαφρύ hash χρησιμοποιείται για την ανίχνευση οποιασδήποτε μεταβολής των συναλλαγών περιεχομένου κατά την

διάρκεια της μετάδοσης. Όλες οι συναλλαγές από και προς το έξυπνο σπίτι αποθηκεύονται σε ένα τοπικό ιδιωτικό Blockchain.

Σε κάθε έξυπνο σπίτι υπάρχει ένα τοπικό Blockchain, το οποίο κρατάει και παρακολουθεί τις συναλλαγές και έχει μια επικεφαλίδα πολιτικής για τις εισερχόμενες και εξερχόμενες συναλλαγές. Με αρχή την πρώτη συναλλαγή, οι συναλλαγές κάθε συσκευής είναι αλυσοδεμένες σε έναν αμετάβλητο κατάλογο Blockchain. Κάθε μπλοκ στο τοπικό δίκτυο περιέχει δύο κεφαλίδες και πολιτικές ομάδων. Η κεφαλίδα μπλοκ έχει το hash του προηγούμενου μπλοκ για να κρατήσει την αλυσίδα αμετάβλητη. Η επικεφαλίδα πολιτικής χρησιμοποιείται για την έγκριση συσκευών και την επιβολή πολιτικής ελέγχου του ιδιοκτήτη στο σπίτι του, η επικεφαλίδα έχει τέσσερις παραμέτρους. Εκτός από τις κεφαλίδες κάθε μπλοκ περιέχει και έναν αριθμό συναλλαγών, για κάθε συναλλαγή αποθηκεύονται πέντε παράμετροι στο τοπικό Blockchain.

Ο έξυπνος οικιακός ανθρακωρύχος είναι μια συσκευή που επεξεργάζεται κεντρικά τις εισερχόμενες και εξερχόμενες συναλλαγές από και προς το έξυπνο σπίτι, θα μπορούσε να ενσωματωθεί στην πύλη internet του σπιτιού ως αυτόνομη συσκευή, μπορεί να τοποθετηθεί μεταξύ συσκευών και αρχικής πύλης. Όπως και με τις υπάρχουσες κεντρικές υπηρεσίες ασφαλείας ο ανθρακωρύχος πιστοποιεί, εξουσιοδοτεί και ελέγχει τις συναλλαγές, επιπρόσθετα κάνει και άλλες λειτουργίες όπως η δημιουργία αρχικών συναλλαγών, διανομή και ενημέρωση κλειδιών και αλλαγή της διάρθρωσης των συναλλαγών. Η συσκευή αυτή συγκεντρώνει όλες τις συναλλαγές σε ένα μπλοκ και προσθέτει το πλήρες μπλοκ στην αλυσίδα, για επιπλέον δυναμικότητα διαχειρίζεται και μια αποθήκη δεδομένων.

Η τοπική συσκευή αποθήκευσης αποτελεί μια συσκευή που χρησιμοποιείται από τις συσκευές για την τοπική αποθήκευση των δεδομένων. Αυτή η αποθήκευση μπορεί να ενσωματωθεί με την συσκευή που επιτελεί την λειτουργία ανθρακωρύχου ή μπορεί να είναι και μια ξεχωριστή συσκευή.



Εικόνα 25 Συνολική Εικόνα Έξυπνου Σπιτιού

7.4.2 Τρόπος Λειτουργίας

Για να εισαχθεί μια συσκευή στο έξυπνο σπίτι, η συσκευή που επιτελεί την λειτουργία του ανθρακωρύχου δημιουργεί μια συναλλαγή αρχικοποίησης με την κοινή χρήση ενός κλειδιού με την συσκευή χρησιμοποιώντας έναν γενικευμένο κρυπτογραφικό αλγόριθμο. Το κοινόχρηστο κλειδί μεταξύ συσκευής και ανθρακωρύχου αποθηκεύεται στην αρχική συναλλαγή. Όσο για τον ορισμό της κεφαλίδας πολιτικής ο ιδιοκτήτης του σπιτιού δημιουργεί τις δικές του πολιτικές και προσθέτει την κεφαλίδα πολιτικής στο πρώτο μπλοκ. Ο ανθρακωρύχος χρησιμοποιεί την κεφαλίδα πολιτικής στο τρέχων μπλοκ, για να ενημερώσει την πολιτική που θα πρέπει να ενημερώσει ο κάτοχος που πρέπει να ενημερώσει την πολιτική του τρέχων μπλοκ.

Όλες οι συσκευές μπορούν να επικοινωνούν απευθείας μεταξύ τους αλλά και με οντότητες εκτός του έξυπνου σπιτιού, οι συσκευές εντός σπιτιού μπορούν να ζητήσουν δεδομένα από άλλες συσκευές για την παροχή κάποιας υπηρεσίας όπως για το άνοιγμα των φώτων όταν εισέλθει κάποιος στο σπίτι. Για να επιτευχθεί ο έλεγχος του χρήστη στις συναλλαγές που γίνονται εντός του σπιτιού, ένα κοινόχρηστο κλειδί θα πρέπει να δοθεί από τον ανθρακωρύχο στις συσκευές που πρέπει να επικοινωνούν άμεσα μεταξύ τους. Αυτή η μέθοδος είναι αρκετά καλή διότι από την μια ο ανθρακωρύχος/ιδιοκτήτης έχει μια λίστα συσκευών που μοιράζονται δεδομένα και από την άλλη οι επικοινωνίες μεταξύ των συσκευών είναι ασφαλείς με το κοινόχρηστο κλειδί.

Η αποθήκευση δεδομένων στην τοπική αποθήκη είναι ακόμα μια συναλλαγή εντός του σπιτιού από τις συσκευές. Για να αποθηκευτούν δεδομένα τοπικά θα πρέπει κάθε συσκευή να ταχτοποιηθεί στην περιοχή που γίνεται η αποθήκευση με την χρήση του κοινόχρηστου κλειδιού. Παίρνοντας το κοινόχρηστο κλειδί από τον ανθρακωρύχο η συσκευή μπορεί να αποθηκεύσει δεδομένα απευθείας τοπικά. Επίσης οι συσκευές μπορούν να αποθηκεύουν δεδομένα και στο cloud, και σε αυτήν την περίπτωση όλες οι διαδικασίες περνάνε από τον ανθρακωρύχο, ο οποίος επιτρέπει τις διαδικασίες για την αποθήκευση σε μια cloud υπηρεσία.

Οι δύο τελευταίες συναλλαγές, είναι η συναλλαγή πρόσβασης και η συναλλαγή ελέγχου. Στην συναλλαγή πρόσβασης ο ανθρακωρύχος βλέπει που είναι αποθηκευμένα τα δεδομένα που ζητούνται τοπικά ή στο cloud και τα επιστρέφει ενώ στην συναλλαγή ελέγχου ορίζεται ανά πόσο χρονικό διάστημα ο ιδιοκτήτης θα λαμβάνει πληροφορίες από τις συσκευές του σπιτιού.

7.4.3 Ανάλυση Ασφάλειας

Υπάρχουν τρείς βασικές απαιτήσεις ασφάλειας που πρέπει να ικανοποιούνται σε οποιοδήποτε σχέδιο ασφάλειας, αυτές είναι η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα. Η εμπιστευτικότητα βεβαιώνει ότι μόνο ο εξουσιοδοτημένος χρήστης μπορεί να διαβάσει το μήνυμα, η ακεραιότητα διασφαλίζει ότι το απεσταλμένο μήνυμα φτάνει στον προορισμό χωρίς να έχει υποστεί κάποια αλλαγή και η διαθεσιμότητα διασφαλίζει ότι κάθε υπηρεσία ή δεδομένα θα είναι διαθέσιμα στον χρήστη όταν απαιτείται. Οι δύο πρώτες απαιτήσεις ικανοποιούνται όπως προαναφέρθηκε στην προηγούμενη ενότητα. Για να αυξηθεί η διαθεσιμότητα του σπιτιού, οι συσκευές προστατεύονται από κακόβουλες αιτήσεις, αυτό γίνεται με τον περιορισμό των αποδεκτών συναλλαγών σε αυτές τις οντότητες με τις οποίες κάθε συσκευή έχει δημιουργήσει κοινόχρηστο κλειδί. Γενικά όμως τα πρόσθετα

δεν δημιουργούν σημαντικές καθυστερήσεις και δεν επηρεάζουν την διαθεσιμότητα των έξυπνων συσκευών.

Τα έξυπνα σπίτια μπορούν να δεχθούν επιθέσεις. Η κυριότερη επίθεση είναι η DDOS επίθεση, δηλαδή η επίθεση της άρνησης εξυπηρέτησης, ο εισβολέας χρησιμοποιεί πολλές μολυσμένες συσκευές με σκοπό να κατακλύσουν έναν συγκεκριμένο κόμβο στόχο. Η δεύτερη επίθεση είναι η επίθεση σύνδεσης, στην οποία ο επιτιθέμενος δημιουργεί μια σύνδεση μεταξύ πολλών συναλλαγών ή καταλόγων δεδομένων, με το ίδιο κοινόχρηστο κλειδί, για να βρει το αναγνωριστικό ενός ανώνυμου χρήστη, αυτή η επίθεση θέτει σε κίνδυνο την Ιδιωτικότητα των χρηστών. Σχετικά με τον πρώτο τρόπο επίθεσης, όλες οι συναλλαγές θα πρέπει να περνάνε από τον ανθρακωρύχο κάτι που καθιστά αδύνατο για έναν επιτιθέμενο να εγκαταστήσει κακόβουλο λογισμικό σε μια συσκευή, αφού δεν είναι απευθείας προσβάσιμες. Ως δεύτερο επίπεδο όλες οι εξερχόμενες κινήσεις πρέπει να εξουσιοδοτηθούν από τον ανθρακωρύχο εξετάζοντας την επικεφαλίδα της πολιτικής, άρα αν δεν είναι εξουσιοδοτημένες οι συναλλαγές θα μπλοκάρουν. Σχετικά με την δεύτερη επίθεση, όλα τα δεδομένα μιας συσκευής μοιράζονται και αποθηκεύονται με την χρήση ενός μοναδικού κλειδιού. Ο ανθρακωρύχος δημιουργεί ένα μοναδικό κατάλογο δεδομένων στο cloud για κάθε συσκευή χρησιμοποιώντας ένα διαφορετικό ιδιωτικό κλειδί.

Η ασφάλεια του IoT κερδίζει πολλή προσοχή τόσο στον ακαδημαϊκό χώρο όσο και στην βιομηχανία. Υπάρχουν λύσεις ασφαλείας οι οποίες δεν είναι κατάλληλες λόγο της υψηλής κατανάλωσης ενέργειας και την επεξεργασία γενικών εξόδων. Η τεχνολογία Blockchain αντιμετωπίζει αυτές τις προκλήσεις χρησιμοποιώντας έναν αμετάβλητο κατάλογο από μπλοκ.

7.5 Blockchain και IoT στον Βιομηχανικό Τομέα

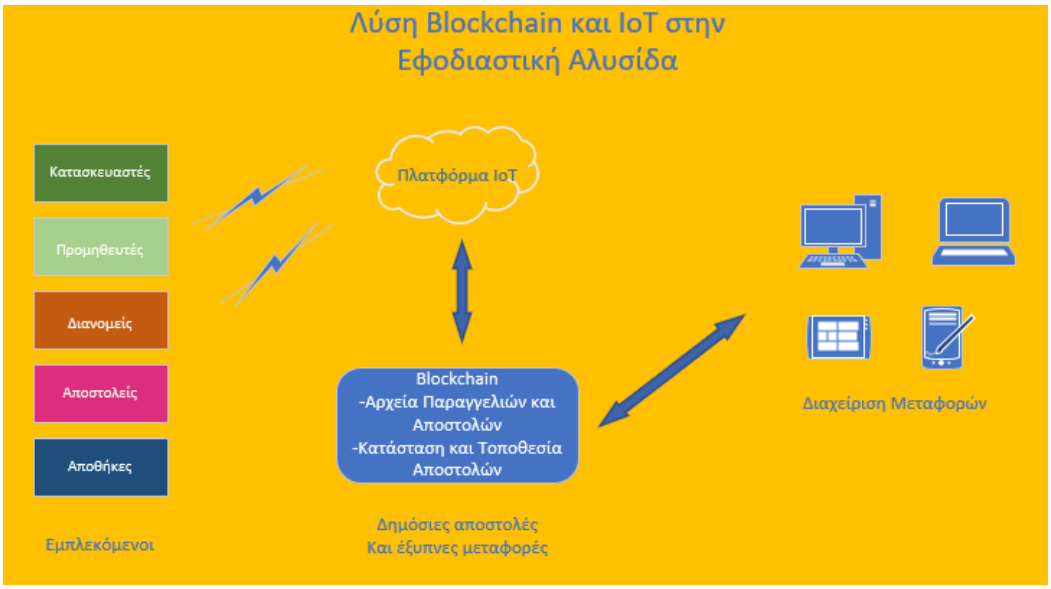
Η τεχνολογία Blockchain και το IoT είναι βασικές τεχνολογίες οι οποίες θα έχουν τεράστιο αντίκτυπο τα επόμενα 10 χρόνια για τις επιχειρήσεις στην βιομηχανική αγορά. Αυτές οι τεχνολογίες μπορούν να βελτιώσουν την αποτελεσματικότητα, παρέχουν νέες επιχειρηματικές ευκαιρίες, ρυθμίζουν τις κανονιστικές απαιτήσεις και βελτιώνουν την διαφάνεια και την ορατότητα. Το IoT επιτρέπει την καταγραφή δεδομένων σε πραγματικό χρόνο με την χρήση αισθητήρων. Καθώς οι τιμές των αισθητήρων και των ενεργοποιητών συνεχίζουν να μειώνονται, οι επιχειρήσεις του βιομηχανικού τομέα θα μπορέσουν να ξεπεράσουν τα κόστη στην υιοθέτηση τέτοιων πλατφορμών. Η τεχνολογία Blockchain επιτρέπει την κοινή χρήση βασικών δεδομένων που συλλέγονται από συσκευές IoT, χρησιμοποιώντας έναν κατανεμημένο, αποκεντρωμένο, κοινόχρηστο κατάλογο που διατίθενται στους συμμετέχοντες στο επιχειρηματικό δίκτυο.

7.5.1 Λύσεις Εφοδιαστικής Αλυσίδας

Οι περιπτώσεις χρήσης της εφοδιαστικής αλυσίδας είναι από τις πιο κοινές εφαρμογές της τεχνολογίας Blockchain για την επίλυση προβλημάτων πραγματικών επιχειρήσεων, προβλήματα που οφείλονται στην έλλειψη ορατότητας των δεδομένων αποστολής για πληροφορίες σχετικά με προϊόντα ή εξαρτήματα, η αποστολή γίνεται μέσο της εφοδιαστικής αλυσίδας. Οι καθυστερήσεις στην αποστολή οφείλονται συχνά σε μεσάζοντες στο πλαίσιο της εφοδιαστικής αλυσίδας εφοδιασμού, ο ρόλος της οποίας είναι η έγκριση των εγγράφων που σχετίζονται με αποστολές. Οι εργασίες που επιτελούνται σε

χαρτιά με τον παραδοσιακό τρόπο δεν είναι αρκετά αποδοτικές. Η γραφειοκρατία θα μπορούσε να ψηφιοποιηθεί σε μια αλυσίδα από μπλοκ. Η ανάγκη για αυτούς τους τύπους διαμεσολαβητών θα μπορούσε να αφαιρεθεί από την αλυσίδα εφοδιασμού.

Η τεχνολογία Blockchain θα κρατάει σημαντικά δεδομένα αποστολής που εκπέμπονται από τις συσκευές IoT που είναι προσαρτημένες στα προϊόντα ή εξαρτήματα καθώς η αποστολή μετακινείται από την πηγή στον προορισμό. Η πλατφόρμα IoT μπορεί να επικαλεστεί μια συναλλαγή για το δίκτυο που περιέχει την θέση του κοντέινερ αποστολής και μια χρονοσφραγίδα. Οι συναλλαγές που γίνονται στο Blockchain χρησιμεύουν ως απόδειξη της αποστολής και απόδειξη παράδοσης και αποστολές εμπορευματοκιβωτίων. Οι καθυστερήσεις της αποστολής θα ελαχιστοποιηθούν και θα οδηγήσουν τους χρόνους παράδοσης για υλικά που ρέουν σε εγκαταστάσεις παραγωγής, θα μπορούσε να προβλεφθεί με μεγαλύτερη ακρίβεια. Καταγραφή εμπορευμάτων στα επίπεδα των εγκαταστάσεων θα μπορούσαν να ευθυγραμμιστούν καλύτερα με τις πρακτικές έγκαιρης εφαρμογής.



Εικόνα 26 Blockchain και IoT στην Εφοδιαστική Αλυσίδα

Στην παραπάνω εικόνα, τα δεδομένα θέσης λαμβάνονται από αισθητήρες IoT και διαβιβάζονται σε μια πλατφόρμα IoT, η οποία καταγράφει τα δεδομένα θέσης στην αλυσίδα. Οι συμμετέχοντες στην εφοδιαστική αλυσίδα, συμπεριλαμβάνουν τους κατασκευαστές πρωτότυπου εξοπλισμού, τους προμηθευτές, τους παρόχους εφοδιαστικής τρίτων μερών, τους φορτωτές και τις αποθήκες. Κάθε συμμετέχων έχει την ορατότητα στα σχετικά δεδομένα αποστολής στο Blockchain, με βάση τον ρόλο του συμμετέχοντα. Τα συστήματα διαχείρισης εφοδιαστικής χρησιμοποιούνται από τους κατασκευαστές ώστε να κάνουν ερωτήσεις στην αλυσίδα για τα δεδομένα αποστολής και δίνουν πρόσθετες πληροφορίες αποστολής στην αλυσίδα.

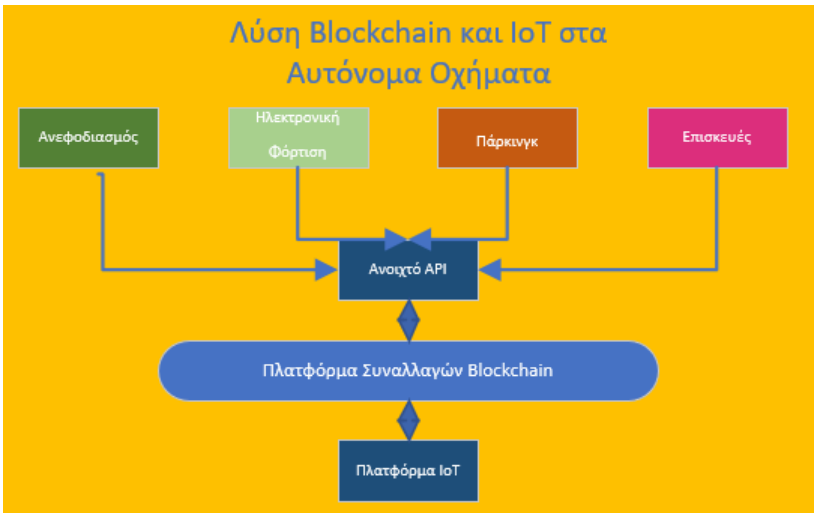
7.5.2 Λύσεις Αυτόνομων Οχημάτων

Σύμφωνα με μελέτες των κορυφαίων αυτοκινητοβιομηχανιών παγκοσμίως, θα υπάρξει ένας αρκετά μεγάλο αριθμός αυτοκινήτων με μια ικανότητα αυτονομίας οδήγησης από τις αρχές τις δεκαετίας του 2020, με τα πρώτα αυτοκίνητα να είναι κυρίως πολυτελή αυτοκίνητα ή μέρος εμπορικών στόλων.

Στην περίπτωση ενός οχήματος που θα ήταν απόλυτα αυτόνομο, θα μπορούσε να οδηγηθεί από μόνο του και συνεπώς να κάνει και ανεφοδιασμό καυσίμου ή ηλεκτρικής ενέργειας σε κάποιον σταθμό, χωρίς τον ανθρώπινο παράγοντα. Οι λύσεις συνδεδεμένων αυτοκινήτων μπορούν να επωφεληθούν από την τεχνολογία Blockchain και από τις λύσεις IoT, λόγω των έγκαιρων και ορατών δεδομένων που συλλέγονται στο Blockchain από το όχημα. Εάν οι αισθητήρες στο όχημα ανιχνεύσουν ότι απαιτείται επισκευή, το όχημα θα μπορούσε να προγραμματίσει αυτόματα ένα ραντεβού και να οδηγηθεί σε μια εγκατάσταση επισκευής. Οι κατασκευαστές αυτόνομων οχημάτων θα έχουν έγκαιρη πρόσβαση στις πληροφορίες βλάβης του κινητήρα ή του αυτοκινήτου οι οποίες συλλέγονται σε ένα Blockchain, αυτές οι πληροφορίες θα μπορούσαν να χρησιμοποιηθούν για τον καθορισμό του πόσο καλό είναι το όχημα.

Οι πελάτες επωφελούνται από το αυξημένο επίπεδο φροντίδας από τους κατασκευαστές και αυξάνεται η αυτοπεποίθηση του καταναλωτή. Οι κατασκευαστές, οι ρυθμιστικές αρχές και οι προμηθευτές θα έχουν κατάλληλη εικόνα των αποτυχιών εξαρτημάτων με την χρήση της αλυσίδας, και θα μπορούσαν να αντιδράσουν προληπτικά στις τάσεις αποτυχίας, πολύ πιο γρήγορα για να διασφαλιστεί η ασφάλεια και η ικανοποίηση των πελατών. Το όχημα θα μπορούσε να πληρώσει από μόνο του τον ανεφοδιασμό ή τις επισκευές χωρίς άμεση ανθρώπινη παρέμβαση. Μια μόνιμη καταγραφή του ανεφοδιασμού και των επισκευών μπορεί να καταγραφεί στην αλυσίδα και να μοιραστεί μεταξύ των συμμετεχόντων, δηλαδή των ιδιοκτητών των οχημάτων, των κατασκευαστών, των εγκαταστάσεων επισκευής και των εταιρειών χρηματοδότησης.

Στην επόμενη εικόνα απεικονίζονται οι αισθητήρες οχημάτων που εκπέμπουν δεδομένα στην πλατφόρμα IoT όπως η τροφοδοσία, η φόρτιση, το παρκάρισμα και οι επισκευές. Η πλατφόρμα IoT επικαλείται την κατάλληλη συναλλαγή Blockchain με βάση κανόνες που συνδέονται με τον τύπο των δεδομένων των αισθητήρων. Ένα ανοιχτό API χρησιμοποιείται από τους σταθμούς ανεφοδιασμού, φόρτισης, στάθμευσης ή επισκευής για την επίκληση μιας συναλλαγής Blockchain όταν ολοκληρωθεί η λειτουργία.



Εικόνα 27 Το παράδειγμα των Αυτόνομων Οχημάτων

7.5.3 Παραγωγή Φυτών

Μια λύση Blockchain και IoT μπορεί να επιτρέψει την πρόληψη και πρόβλεψη αποτυχιών στον τομέα της κατασκευής εξοπλισμού που αφορά τα φυτά. Οι αισθητήρες του εξοπλισμού μπορούν να ανιχνεύσουν τις συνθήκες του περιβάλλοντος, κρύο, ζέστη, υγρασία. Τα βασικά δεδομένα του κατωφλιού που συλλέχθηκαν αποθηκεύονται σε ένα Blockchain, απευθείας από τους αισθητήρες και χρησιμοποιούνται για την ανίχνευση των τάσεων των αποτυχιών με σκοπό την ενεργητική συντήρηση και τις επισκευές πριν από την αποτυχία. Τα δεδομένα αυτά, μπορούν να δώσουν χρήσιμα συμπεράσματα σχετικά με την απόδοση του εξοπλισμού, επίσης οι ρυθμιστικές αρχές και οι προμηθευτές, έχουν την δυνατότητα να αποκτήσουν λεπτομερή και ακριβή εικόνα του εξοπλισμού, με στόχο τις έγκαιρες ενέργειες επίλυσης. Οι συνεργάτες που επισκευάζουν μπορούν να παρακολουθούν την αλυσίδα για την προληπτική συντήρηση και για να καταγράψουν στην συνέχεια το έργο τους σε αυτήν.

Οι λύσεις Blockchain και IoT στον βιομηχανικό τομέα θα πρέπει να δρομολογηθούν κανονιστικά, νομικά και ασφαλιστικά, σχετικά με τις απαιτήσεις που αφορούν τα εμπορεύματα που μεταφέρονται στην εφοδιαστική αλυσίδα, τα αυτόνομα οχήματα καθώς και τον εξοπλισμό που αφορά τα φυτά. Οι καταγραφές ασφαλείας θα πρέπει να παρακολουθούνται στενά από τις ρυθμιστικές αρχές, τους ασφαλιστικούς διαχειριστές και τους νομικούς φορείς. Οι ρυθμιστικές αρχές θα πρέπει να έχουν πρόσβαση στην συμμόρφωση και στα αρχεία ασφαλείας στο Blockchain. Οι ασφαλιστικοί διαχειριστές θα ενδιαφέρονται για τα αρχεία ασφαλείας καθώς και αποτυχίες εξοπλισμού για ανάλυση κινδύνου. Τα δικηγορικά γραφεία θα χρειαστούν πρόσβαση σε αρχεία ασφαλείας και τα δεδομένα αποτυχίας του εξοπλισμού από το μπλοκ για την επίλυση προβλημάτων.

8. BLOCKCHAINS ΣΤΗΝ ΕΤΑΙΡΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ *[26],[27],[28],[29],[30],[31],[32],[33]*

8.1 Εισαγωγή

Η τεχνολογία Blockchain αντιπροσωπεύει μια νέα εφαρμογή της κρυπτογραφίας και της τεχνολογίας των πληροφοριών σε παλαιά προβλήματα διατήρησης οικονομικών αρχείων και μπορεί να οδηγήσει σε πολύ σημαντικές αλλαγές στον τομέα της εταιρικής διακυβέρνησης. Η Εταιρική Διακυβέρνηση είναι ένα σύνολο κανόνων που εφαρμόζονται στις Ανώνυμες Εταιρείες και ρυθμίζουν την λειτουργία του Διοικητικού Συμβουλίου, σε σχέση με τους μετόχους της εταιρείας. Με την Εταιρική Διακυβέρνηση επιδιώκεται η υπεύθυνη οργάνωση, λειτουργία , διοίκηση και έλεγχος μιας εταιρείας, με στόχο την αύξηση της αξίας της και την προστασία των έννομων συμφερόντων όλων των μετόχων της, κυρίως όμως των μετόχων μειοψηφίας, έναντι των μεγαλομετόχων. Πολλοί σημαντικοί παράγοντες στην οικονομική βιομηχανία έχουν αρχίσει να επενδύουν σε αυτήν την τεχνολογία, τα χρηματιστήρια έχουν προτείνει χρήση της τεχνολογίας Blockchain ως μια νέα μέθοδο για την ανταλλαγή εταιρικών μετοχών και για την παρακολούθηση της ιδιοκτησίας αυτών. Η συγκεκριμένη τεχνολογία έχει να επιφέρει πολλές αλλαγές σε διευθυντικά στελέχη, θεσμικούς επενδυτές, μικρούς μετόχους, ελεγκτές αλλά και σε άλλα μέρη που εμπλέκονται στην διακυβέρνηση. Το χαμηλότερο κόστος, η μεγαλύτερη ρευστότητα, η ακριβέστερη τήρηση αρχείων και η διαφάνεια ιδιοκτησίας που προσφέρουν τα Blockchains μπορούν να αυξήσουν σημαντικά την ισορροπία της εξουσίας μεταξύ αυτών.

Όπως έχει ειπωθεί και προηγουμένως, ένα Blockchain είναι μια βάση δεδομένων η οποία διασφαλίζεται με κρυπτογραφικές μεθόδους και προσφέρει μια εναλλακτική λύση στα κλασικά οικονομικά βιβλία. Μετά από μια έκρηξη ενδιαφέροντος το 2015, από τον τομέα των βιομηχανιών, η τεχνολογία αυτή έχει τραβήξει την προσοχή και του επιχειρηματικού κόσμου, καθώς προσφέρει έναν νέο τρόπο δημιουργίας, ανταλλαγής, και παρακολούθησης της ιδιοκτησίας των χρηματοοικονομικών περιουσιακών στοιχείων σε μια ομότιμη βάση. Τα μεγάλα χρηματιστήρια διευρύνουν την χρήση των Blockchains για την εγγραφή και την ανταλλαγή μετοχών που εκδίδονται από τις εταιρείες. Η τεχνολογία αυτή έχει επίσης την δυνατότητα να φιλοξενεί χρεόγραφα και χρηματοοικονομικά παράγωγα, τα οποία μπορούν να εκτελούνται αυτόνομα ως έξυπνα συμβόλαια. Επιπλέον μπορεί να χρησιμοποιηθεί για την διατήρηση βάσεων δεδομένων των κυβερνήσεων σχετικά με τα περιουσιακά στοιχεία γης, τα στοιχεία πολιτών, στατιστικές αλλά και για άλλους τομείς.

Η τεχνολογία αυτή προτάθηκε αρχικά ως μια μέθοδος επικύρωσης της ιδιοκτησίας ενός εικονικού νομίσματος, εφτά χρόνια μετά την επιτυχή λειτουργία σε αυτόν τον τομέα, αναγνωρίζεται ως μια εναλλακτική λύση για λογιστικά βιβλία ιδιοκτησίας. Τα Blockchains προσφέρουν πολλά πλεονεκτήματα σε σχέση με το κόστος, την ταχύτητα και την ακεραιότητα των δεδομένων σε σχέση με τις κλασικές μεθόδους απόδειξης της ιδιοκτησίας, με αποτέλεσμα πολλές επενδύσεις να γίνονται από οργανισμούς σε αυτόν τον τομέα. Οι επιχειρηματίες ερευνούν ενεργά την καταλληλότητα του Blockchain για την καταγραφή ιδιοκτησίας ενός μεγάλου φάσματος περιουσιακών στοιχείων από μετοχές και ομόλογα μέχρι ακίνητα, τσάντες και έργα τέχνης. Επιπρόσθετα μπορούν να δημιουργηθούν πολλές εφαρμογές για τις κυβερνήσεις που να διαχειρίζονται τίτλους ακινήτων, πιστοποιητικά, άδειες οδήγησης και πανεπιστημιακά πτυχία.

Η χρήση Blockchains για την καταγραφή της ιδιοκτησίας αποθεμάτων θα μπορούσε να λύσει μακροχρόνια προβλήματα που σχετίζονται με την αδυναμία των εταιρειών να τηρούν ακριβή και έγκαιρα αρχεία για το ποιος κατέχει τις μετοχές τους. Οι μελλοντικές επεκτάσεις θα μπορούσαν να επιτρέψουν στα Blockchains να έχουν εκτελέσιμα έξυπνα συμβόλαια, όπως δικαιώματα προαίρεσης αγοράς μετοχών που κατέχονται από εργαζομένους, ή δικαιώματα αγοράς μετοχών που ανήκουν σε εξωτερικούς επενδυτές. Αυτές οι έξυπνες συμβάσεις θα μπορούσαν να επεκταθούν σε τομείς όπως το προσυμφωνημένο ψήφισμα οικονομικής δυσπραγίας. Ένα από τα πιο σημαντικά είναι ότι τα Blockchains μπορούν να παρέχουν πρωτοφανή διαφάνεια ώστε να επιτρέπεται στους επενδυτές να προσδιορίσουν τις θέσεις ιδιοκτησίας του χρέους και ίδιων κεφαλαίων, μειώνοντας έτσι την ευκαιρία διεφθαρμένη συμπεριφορά των ρυθμιστικών αρχών, των εταιριών και των εμπλεκομένων. Αν μια επιχείρηση επιλέξει να κρατήσει κάποια ή όλα τα οικονομικά στοιχεία της σε έναν δημόσιο κατάλογο, όπως προτείνουν ορισμένοι ειδικοί, οι ευκαιρίες για την διαχείριση των εσόδων, για στρατηγικές χρηματοοικονομικής πληροφόρησης θα γίνουν πολύ πιο διαφανείς.

Για τους μετόχους, τα Blockchains θα μπορούσαν να προσφέρουν χαμηλότερο κόστος συναλλαγών και μεγαλύτερη διαφάνεια, ενώ επιτρέπουν την ορατή παρακολούθηση μεταβιβάσεων σε πραγματικό χρόνο από το έναν ιδιοκτήτη στον άλλον. Οι μέτοχοι μειοψηφίας ή αλλιώς οι μέτοχοι ακτιβιστές μπορούν να επωφεληθούν αρκετά από αυτήν την τεχνολογία για την ταχύτερη και φθηνότερη εξαγορά μετοχών αλλά με λιγότερη μυστικότητα από το υπάρχων σύστημα. Οι ακτιβιστές θα μπορούσαν επίσης να ρευστοποιήσουν τις θέσεις τους με μεγαλύτερη διαφάνεια κάτι το οποία καθιστά το κανάλι εξόδου από την Εταιρική Διακυβέρνηση ιδιαίτερα ελκυστικό σε βάρος της φωνής η του καναλιού παρέμβασης. Η διαχείριση της ιδιοκτησίας μπορεί να γίνει με πολύ μεγαλύτερη διαφάνεια με αγορά και πώληση εμπιστευτικών πληροφοριών που ανιχνεύονται από την αγορά σε πραγματικό χρόνο. Η εταιρική ψηφοφορία θα μπορούσε να γίνει περισσότερο ακριβής και στρατηγικές όπως η κενή ψηφοφορία που αποσκοπούν στον διαχωρισμό των δικαιωμάτων ψήφου από άλλες πτυχές της ιδιοκτησίας μετοχών θα ήταν πιο δύσκολο να εκτελεσθούν κρυφά. Οποιαδήποτε από αυτές τις αλλαγές είναι ικανή να επηρεάσει δραματικά την ισορροπία εξουσίας μεταξύ διευθυντών, μάνατζερ και μετόχων. Ωστόσο σημαντικό ρόλο παίζει ο τύπος του Blockchain που θα χρησιμοποιηθεί, δημόσιο και ανοιχτό σε οποιονδήποτε ή περιορισμένο και εξουσιοδοτημένο από ορισμένα χρηματοπιστωτικά ιδρύματα και κοινοπραξίες.

Μέχρι σήμερα η μοναδική χρήση του Blockchain στην τομέα της εταιρικής χρηματοδότησης έχει συμβεί στην Αυστραλία, όπου ανακοινώθηκε από μεγάλες εταιρείες η πρόθεση επανασχεδιασμού των συστημάτων με νέα βάση την τεχνολογία Blockchain. Σε παρόμοιο μήκος κύματος έχει κινηθεί με μελέτες στο παρελθόν ο NASDAQ αλλά και η Deutsche Borse. Ο Lee(2016), συζητά για τα πιθανά οφέλη των Blockchains στο χρηματιστήριο σε τομείς όπως κόστος και η ταχύτητα εκτέλεσης του διακανονισμού. Ο Schroeder(2015),αναλύει την νομική βάση για την αντιμετώπιση των εικονικών περιουσιακών στοιχείων σε Blockchains. Σχετικά με τον τομέα των ψηφισμάτων, το Εσθονικό χρηματιστήριο ξεκίνησε το 2016 να διεξαγάγει ψηφοφορία μετόχων σε μια πλατφόρμα Blockchain. Στα τέλη του 2016 άρχισε να παίρνει η αμερικάνική εταιρεία Overstock.com συνδρομές για έκδοση δικαιωμάτων επί μετοχών μέσω ιδιωτικού Blockchain.

Οι αναδυόμενες αγορές μπορεί να είναι μεταξύ των πρώτων που βλέπουν την τεχνολογία Blockchain να ενσωματώνεται σε χρηματιστήρια και κεφαλαιαγορές με μεγάλη κλίμακα. Η πρόβλεψη των πρώτων υιοθεσιών στις αναπτυσσόμενες χώρες βασίζεται στην σύγκλιση τριών δυνάμεων, στην ανεπάρκεια των υπαρχόντων συστημάτων τήρησης αρχείων, στην δυσπιστία των διεφθαρμένων και αναποτελεσματικών ρυθμιστικών αρχών της αγοράς και στην υψηλή διείσδυση της τεχνολογία της πληροφορίας, όπως τα smart phones. Για παράδειγμα, η ταχεία ανάπτυξη των συστημάτων κινητών πληρωμών, όπως η M-Pesa και η BitPesa στην Κένυα, καθώς και οι πρόσφατες έρευνες των κυβερνήσεων της Ονδούρας και της Δημοκρατίας της Γεωργίας για την μεταφορά των κτηματολογίων σε Blockchains, δείχνουν την προθυμία των αναδυόμενων οικονομιών να παρακάμψουν τις τεχνολογίες μεγαλύτερης ηλικίας και να γίνουν πρωτοπόροι καινοτομιών που ενσωματώνουν τα οικονομικά δεδομένα στην τεχνολογία των πληροφοριών.

Εάν η τεχνολογία Blockchain αποκτήσει κεντρικό ρόλο στην τήρηση αρχείων των εταιρειών η συντήρηση και η αναβάθμιση των ίδιων των αλυσίδων θα δημιουργούσε ενδιαφέροντα προβλήματα διακυβέρνησης. Η διακυβέρνηση ενός Blockchain ισοδυναμεί με την εξουσιοδότηση να ενημερώνει τον κώδικα του, ο οποίος μπορεί να γίνει είτε για τεχνικούς λόγους είτε για να αλλαχθούν κρίσιμοι περιορισμοί ή παραδοχές. Όπως εφαρμόζεται για το Bitcoin και για άλλα ψηφιακά νομίσματα, τα Blockchains λειτουργούν με ένα δημόσιο, αποκεντρωμένο κατάλογο, με όλους τους συμμετέχοντες σε ένα δίκτυο όπου όλοι έχουν την ευκαιρία να ενημερώνονται σε πραγματικό χρόνο. Οι προτεινόμενες αλλαγές συμβαίνουν μέσω παθητικής διαδικασίας, έγκρισης ή απόρριψης από τους κατόχους άνω του 50% την εξορυκτικής δύναμης του δικτύου, και κατ αρχήν μια αλλαγή στον κώδικα μπορεί να ξεκινήσει από οποιονδήποτε. Αυτή η αποκέντρωση της τεχνολογίας μπορεί να οδηγήσει σε σαμποτάζ. Αυτοί που σκοπεύουν να συντρίψουν το δίκτυο μπορούν να προτείνουν αλλαγές λογισμικού που φαίνονται καλοήθεις και υιοθετούνται ευρέως ή εναλλακτικά θα μπορούσαν να δελεάσουν άλλους να τις υιοθετήσουν χρησιμοποιώντας στρατηγικές που βασίζονται στην εκμετάλλευση προβλημάτων συλλογικής δράσης. Η υπέρβαση αυτών των τρωτών σημείων φαίνεται να αποτελεί σημαντική, μη ολοκληρωμένη προτεραιότητα για υποστηρικτές της δημόσιας τεχνολογίας Blockchain με την μορφή ανοιχτού κώδικα. Η εναλλακτική λύση μιας εξουσιοδοτημένης αλυσίδας, που ενημερώνεται μόνο από εξουσιοδοτημένους συμμετέχοντες, φαίνεται ελκυστική για λόγους ασφαλείας αλλά θα στερούνταν μερικά από τα σημαντικά χαρακτηριστικά μιας ανοικτής ομάδας. Η πιο ακραία εναλλακτική λύση, ένα ιδιωτικό Blockchain που ελέγχεται από μια κεντρική αρχή. Η δημιουργία τέτοιων ισχυρών τρίτων φορέων και η εξάλειψη των χρηματοπιστωτικών συναλλαγών ήταν ο κεντρικός στόχος της πρότασης του Nakamoto για σύστημα ηλεκτρονικών μετρητών από ομότιμους κόμβους.

8.2 Διαφάνεια Ιδιοκτησίας

Η έκδοση και διαπραγμάτευση εταιρικών χρεογράφων σε Blockchains θα δημιουργούσε πολλά οφέλη και επίσης ορισμένες δαπάνες που σχετίζονται με μεγαλύτερη διαφάνεια ιδιοκτησίας και ταχύτερο, φθηνότερο εμπόριο και διακανονισμούς. Η βελτίωση της διαφάνειας θα έχει σημαντικές επιπτώσεις στις ευκαιρίες κέρδους διαθέσιμες σε διευθυντικά στελέχη, θεσμικούς επενδυτές και ακτιβιστές μετοχών, διότι τα κίνητρα για την απόκτηση ιδιοκτησίας και την εκκαθάριση θα μπορούσαν να αλλάξουν σημαντικά εάν οι συναλλαγές τους ήταν ελεγχόμενες σε πραγματικό χρόνο. Βελτιώσεις στην τεχνολογία συναλλαγών θα επηρεάσουν επίσης τα κίνητρα για την απόκτηση και εκκαθάριση

κυριότητας αυτών των ομίλων. Σημαντικές παρενέργειες μπορεί να μεταφερθούν στην πραγματική οικονομία, καθώς τα μεταβαλλόμενα κίνητρα για ενημερωμένους επενδυτές στο εμπόριο μπορεί να οδηγήσουν σε πιο αξιόπιστα μηνύματα σχετικά με την αξία του ατόμου. Με την παρουσία αυτών των αλλαγών, με την πάροδο του χρόνου οι προμηθευτές κεφαλαίου θα μπορούσαν να σχεδιάσουν διαφορετικά,, επανεξετάζοντας την ανάγκη για ορισμένες περιοριστικές συμφωνίες και εκμεταλλευόμενοι τα πλεονεκτήματα της δυνατότητας των ομάδων να εκτελούν έξυπνες συμβάσεις ταυτόχρονα. Οι επιχειρήσεις μπορούν να στρατολογήσουν τα μέλη του διοικητικού συμβουλίου και τους εξωτερικούς συμβούλους με διαφορετικά σύνολα δεξιοτήτων για να αντιμετωπίσουν τις αλλαγές και τα σημαντικά θέματα, όπως κίνητρα διαχείρισης, πιθανότατα θα εξελιχθούν για να ληφθούν υπόψη της μεταβαλλόμενης φύσης των εταιρικών χρεογράφων.

Όταν χρησιμοποιούνται σε ανοικτή μορφή με ελεύθερη είσοδο και έξοδο, τα Blockchains δημιουργούν ένα αρχείο συναλλαγών που είναι γνωστό ως διανεμημένος κατάλογος, επειδή είναι ένα αντίγραφο κάθε μπλοκ συναλλαγών και διανέμεται ή καθίσταται ορατό σε όλα τα μέλη του δικτύου. Για μια εταιρεία με μετοχές που είναι δημοσιευμένες σε ένα δημόσιο Blockchain, όλοι οι μέτοχοι και άλλα ενδιαφερόμενα μέρη θα μπορούσαν ανά πάσα στιγμή να δουν την ρύθμιση της κυριότητας και να εντοπίσουν τις αλλαγές αμέσως την στιγμή που συνέβησαν.

Δεν θα έλκονται όλοι οι μέτοχοι από την ρύθμιση αυτή, ακτιβιστές και διευθυντές μπορεί να επιθυμούν να κρύψουν τις συναλλαγές τους για τους ίδιους ακριβώς λόγους που οι μικροί μέτοχοι ή οι διαχειριστές αμοιβαίων κεφαλαίων ενδεχομένως επιθυμούν να τηρούν τους κανόνες. Οι εταιρείες που θα εκδίδουν μετοχές θα πρέπει να εξισορροπήσουν αυτές τις εκτιμήσεις και να αξιολογήσουν κατά πόσο η εμπορία των μεριδίων τους θα ήταν πιο προσοδοφόρα σε ένα ιδιωτικό ή εγκεκριμένο Blockchain, όπου η ορατότητα των συναλλαγών θα μπορούσε να περιοριστεί σε μια ομάδα εταιρειών μελών ή αξιόπιστους και οι επενδυτές θα απολάμβαναν μεγαλύτερη ανωνυμία. Ακόμα και κάτω από ιδιωτικά μοντέλα Blockchain ή τα εξουσιοδοτημένα μοντέλα σε πραγματικό χρόνο το αρχείο των συναλλαγών θα δημιουργούσε πολύ πιο σύγχρονες και πλήρεις πληροφορίες για την ιδιοκτησία κάθε επιχείρησης από ότι είναι διαθέσιμο στις χρηματιστηριακές αγορές σήμερα και θα ήταν ορατό για τουλάχιστον ορισμένους παρατηρητές. Αν ο κατάλογος των συναλλαγών ήταν ορατός μόνο στους υποστηρικτές της αλυσίδας και στην κυβέρνηση, ο αντίκτυπος στις στρατηγικές εμπορικών συναλλαγών των επενδυτών και τα κίνητρα των εμπλεκομένων θα μπορούσε να είναι βαθύτατος όπως συζητείτε παρακάτω. Τελικά, μια σειρά από αλυσίδες που προσφέρουν διαφορετικούς βαθμούς ανωνυμίας επενδυτών ενδέχεται να ανταγωνίζονται στην αγορά, να προσελκύσουν εταιρικές λίστες, με εταιρείες που ταξινομούνται μεταξύ διαφορετικών πλατφορμών που απευθύνονται σε διαφορετικούς πελάτες με βάση τις προτιμήσεις τους για διαφάνεια ιδιοκτησίας.

Όλες αυτές οι εικασίες υποθέτουν ότι αυτοί που μπορούν να δουν το κατανεμημένο κατάλογο, θα είναι σε θέση να προσδιορίσουν τους κατόχους μεμονωμένων μετοχών και τους αντισυμβαλλομένους σημαντικών συναλλαγών. Για παράδειγμα, αν ένας διαχειριστής πούλησε μετοχές από το δικό του απόθεμα, υποθέτει ότι οι άλλοι όχι μόνο θα παρατηρήσουν την πώληση, αλλά θα διακρίνουν επίσης την ταυτότητα του διαχειριστή πωλήσεων. Στην πράξη αυτό δεν μπορεί να συμβεί επειδή τα περιουσιακά στοιχεία στις αλυσίδες κρατούνται μέσα σε ανώνυμα ψηφιακά πορτοφόλια τα οποία αναγνωρίζονται μόνο από σύνθετες ετικέτες παρόμοιες με τους σειριακούς

αριθμούς. Πολλοί πρώιμοι χρήστες του Bitcoin προσέλκυσαν το νόμισμα για αυτόν ακριβώς τον λόγο, επειδή πίστευαν ότι η αλυσίδα περιείχε ανωνυμία για αγορές ναρκωτικών, ξέπλυμα χρημάτων και άλλες παράνομες δραστηριότητες.

Το πόσο εύκολα μπορεί να εντοπιστεί η ταυτότητα ενός συμβαλλόμενου μέρους αποτελεί ένα θέμα συζήτησης, πολλοί υποστηρίζουν ότι η υποχρεωτική γνωστοποίηση των κωδικών ταυτοποίησης των εμπόρων θα αυξήσει την ευημερία για την αγορά στο σύνολό της. Θα περίμενε κανείς ότι η απαίτηση αναγνώρισης της ιδιοκτησίας σε ένα Blockchain θα οδηγήσει σε μια ανάπτυξη σε εξειδικευμένες ερευνητικές επιχειρήσεις οι οποίες θα παρακάμπτουν την ανωνυμία (de anonymizing), κερδίζοντας συνδρομητές με την εξακρίβωση της ιδιοκτησίας των επιμέρους ψηφιακών διευθύνσεων πορτοφολιού. Αυτή η διαδικασία ισοδυναμεί με εκσυγχρονισμό των μεθόδων αποκωδικοποίησης που χρησιμοποιούν οι συμμετέχοντες στην Wall Street εδώ και δεκαετίες, αν όχι αιώνες, προσπαθώντας να συμπεράνουν την παρουσία ορισμένων αγοραστών ή πωλητών στην αγορά, παρατηρώντας λεπτομέρειες σχετικά με το μέγεθος, το χρονοδιάγραμμα και την σειρά των συναλλαγών.

Στην αλυσίδα του Bitcoin η διατήρηση της ανωνυμίας έχει αποδειχθεί μερικές φορές αρκετά δύσκολη. Οι ειδικοί στα νομικά θέματα έχουν εντοπίσει και διώκουν επιτυχώς τους υπεύθυνους νομιμοποίησης εσόδων από παράνομες δραστηριότητες, τους εμπόρους ναρκωτικών, τους φορείς εκμετάλλευσης εικονικών καζίνο, τα σχήματα Πόνζι και άλλους κακοποιούς. Εάν μια εταιρεία εκδώσει μετοχές σε έναν δημόσιο κατάλογο, η κατάσταση θα ήταν πιθανώς παρόμοια. Ακόμα και χωρίς προχωρημένους ειδικούς θα ήταν δυνατό, μάλλον εύκολα να γίνει αντιστοίχιση ψηφιακών πορτοφολιών, μεμονωμένων χρηματιστών μετοχών, αναζητώντας τα ακατέργαστα δεδομένα για ένα συγκεκριμένο σχέδιο συναλλαγής που είναι γνωστό ότι έχει συμβεί όπως η ανάθεση μιας εταιρείας σε διαχειριστή συγκεκριμένης ποσότητας περιορισμένων μετοχών σε συγκεκριμένη ημερομηνία. Ενδεχομένως ένας κάτοχος μετοχών θα μπορούσε να παραμείνει ένα βήμα μπροστά χρησιμοποιώντας ένα διαφορετικό ψηφιακό πορτοφόλι για κάθε συναλλαγή ή σπάζοντας τις συναλλαγές σε μικρά κομμάτια χρησιμοποιώντας διάφορα πορτοφόλια ταυτόχρονα. Για την αντιμετώπιση αυτών των στρατηγικών, οι ρυθμιστικές αρχές ενδέχεται να απαιτούν εταιρική σχέση να αποκαλύψουν τα ψηφιακά τους γνωρίσματα πορτοφολιών ή τα δημόσια κλειδιά υπό ποινή του νόμου. Αυτό θα ήταν πιθανότατα μέρος μιας εξέλιξης των κανονισμών αποκάλυψης ότι οι περισσότεροι εφαρμόζονται σε διαχειριστές και σημαντικούς εξωτερικούς μετόχους, οι οποίοι τυπικά πρέπει να εντοπίζονται μετά την μεταβίβαση ορισμένων ορίων ιδιοκτησίας.

8.3 Βελτιώσεις στην Ρευστότητα

Σύμφωνα με πρόσφατες έρευνες, η ρευστότητα αποτελεί την δυνατότητα συναλλαγής σημαντικής ποσότητας ασφάλειας με χαμηλό κόστος σε σύντομο χρονικό διάστημα. Λόγω της δυνατότητας τους να μειώνουν το κόστος και να συντομεύουν τον απαιτούμενο χρόνο εκτέλεσης και διακανονισμού συναλλαγών, τα Blockchains προσφέρουν την δυνατότητα σημαντικής βελτίωσης της ρευστότητας, είτε χρησιμοποιούνται ως η κύρια πλατφόρμα για την εγγραφή και ανταλλαγή μετοχών είτε εναλλακτικά, από τις χρηματιστηριακές αγορές με πιο περιορισμένο τρόπο, προκειμένου να βελτιωθεί η διαδικασία εκκαθάρισης και διακανονισμού μετά την διαπραγμάτευση.

Οι χρηματιστηριακές συναλλαγές στις ΗΠΑ απαιτούν τρεις εργάσιμες μέρες για να ολοκληρωθούν και η ιδιοκτησία να κινηθεί επίσημα από τον πωλητή στον αγοραστή. Κατά την διάρκεια αυτού του διαστήματος, τα κεφάλαια περνούν μεταξύ των μεσιτών και των πελατών τους, καθώς και οι μετοχές μεταφέρονται στα βιβλία της μεσιτείας τους, η οποία είναι υπό την εποπτεία της Depository Trust Clearing Corp. Πολλοί άνθρωποι συμμετέχουν σε αυτήν την διαδικασία, αντίθετα μια πώληση μετοχών στο Blockchain θα μπορούσε να διευθετηθεί πολύ πιο γρήγορα, ανάλογα με τον χρόνο του κύκλου για την προσθήκη νέων μπλοκ, και δεν θα απαιτούσε πολυάριθμους μεσάζοντες, μειώνοντας το κόστος που εμφανίζεται τώρα διαφορετικά σε προμήθειες και περιθώρια προσφοράς ζήτησης. Αν και οι χρηματιστηριακές αγορές θα συνεχίσουν πιθανώς να λειτουργούν σε κάποια μορφή ώστε να διευκολύνουν την συνάντηση αγοραστών και πωλητών, η ρευστότητα θα μπορούσε να αυξάνεται σε μεγάλο βαθμό ως απάντηση στο χαμηλότερο κόστος και στην ταχύτερη ταχύτητα του διακανονισμού. Η εξοικονόμηση κόστους, σε μια αγορά Blockchain θα έπαιρνε τόσο άμεσες όσο και έμμεσες μορφές. Η άμεση εξοικονόμηση κόστους θα προέρχονταν από την μείωση του προσωπικού και τον εξορθολογισμό των διαδικασιών σε σύγκριση με αυτές που χρησιμοποιούνται σήμερα. Έμμεσες αποταμιεύσεις, ενδεχομένως μεγαλύτερες, θα προέκυπταν από τις μειωμένες, η ανάγκη των επιχειρήσεων να δεσμεύουν περιουσιακά στοιχεία ως ασφάλεια ως μορφή ομολόγων κατά την διάρκεια αυτής της διαδικασίας του διακανονισμού.

Η ρευστότητα είναι ένα κρίσιμο ζήτημα για τους διαχειριστές χαρτοφυλακίου και άλλους επενδυτές τόσο μεγάλους όσο και μικρούς. Η βελτίωση της ρευστότητας θα μπορούσε να αυξήσει την ζήτηση για αποθέματα και να έχει πολλές σημαντικές επιπτώσεις στα πρότυπα επενδύσεων και ιδιοκτησίας.

8.4 Επιπτώσεις σε Θεσμικούς Επενδυτές και Ακτιβιστές

Οι μεγάλοι εξωτερικοί μέτοχοι θα επηρεαστούν τόσο από την μεγαλύτερη διαφάνεια όσο και από την βελτίωση της ρευστότητας που μπορεί να προκύψει από την τεχνολογία Blockchain. Όπως φαίνεται και σε έρευνα του Edmans το 2014, πολλές εργασίες έχουν μελετήσει τον αντίκτυπο στους ακτιβιστές και τους θεσμικούς επενδυτές, ορισμένα μοντέλα προβλέπουν μεγαλύτερη ή μικρότερη συμμετοχή από μεγάλους μετόχους στην εταιρική διακυβέρνηση όταν υπάρχει μεγαλύτερη διαφάνεια και αυξημένη ρευστότητα.

Η μεγαλύτερη διαφάνεια θα μπορούσε ενδεχομένως να θεωρηθεί δαπανηρή από τους ακτιβιστές με αποτέλεσμα να είναι απρόθυμοι να επενδύσουν σε επιχειρήσεις που διαπραγματεύονται σε Blockchain αγορές. Η οικοδόμηση μετοχικών θέσεων μυστικά είναι μια χρονικά παλιά στρατηγική αυτών των επενδυτών, οι οποίοι επιθυμούν να ελαχιστοποιήσουν το κόστος απόκτησης τους αποφεύγοντας την δημοσιότητα καθώς αγοράζουν. Υποθέτοντας ότι η αγορά θα μπορούσε να εντοπίσει τους ακτιβιστές ως αγοραστές μετοχών, κάτι που μπορεί να είναι εμφανές λόγω του μεγάλου μεγέθους ή των γνωστών προτύπων των αγορών τους, τότε ο ακτιβισμός των μετοχών μπορεί να γίνει πιο δαπανηρός και λιγότερο επικρατής για τις επιχειρήσεις με συναλλαγές που βασίζονται στην τεχνολογία Blockchain. Πολλά μοντέλα, όπως των Kyle και Vila (1991), Collin-Dufrense και Fos (2016), Collin- Dufrense Fos (2015), δείχνουν ότι οι συναλλαγές των κατόχων είναι ιδιαίτερα κερδοφόρες κατά την περίοδο πριν από την υποχρέωση γνωστοποίησης των θέσεων ιδιοκτησίας τους.

Ωστόσο τα μοντέλα με τις αντίθετες συνέπειες εμφανίζονται στους Maug και Kahn (1998), Winton (1998), αυτά τα έγγραφα υποδηλώνουν ότι η διαφάνεια βοηθά τους βασικούς μετόχους βελτιώνοντας την ρευστότητα και μειώνοντας το κόστος. Αυτό το φαινόμενο συμβαίνει επειδή αποκαλύπτεται η παρουσία του μεγάλου μετόχου, οι άλλοι μέτοχοι περιμένουν να είναι καλά ενημερωμένοι και έτσι προσπαθούν να πουλήσουν αμέσως τις μετοχές τους από το να ρισκάρουν μια χειρότερη ανταλλαγή στο μέλλον λόγο έλλειψης πληροφοριών.

Ο αντίκτυπος της μεγαλύτερης ρευστότητας στους θεσμικούς επενδυτές και τους ακτιβιστές φαίνεται να είναι πολύπλοκος. Σε μια αγορά βασιζόμενη στην τεχνολογία Blockchain γίνεται φθηνότερη και ταχύτερη η συναλλαγή των διακανονισμών και διευκολύνει τόσο την ευκολότερη είσοδο όσο και την ευκολότερη έξοδο από τους κύριους μετόχους. Όσο μεγαλύτερη είναι η ευκολία εισόδου τόσο πιο πολύ προωθείτε η κυριότητα από θεσμούς και ακτιβιστές. Η εργασία των Edmans, Fang, Zur(2013), είναι μια από τις πολλές εργασίες που δείχνουν τα οφέλη της μεγαλύτερης ρευστότητας σε μεγάλους χώρους που οι μέτοχοι επιδιώκουν να εμπλέκονται στην διαχείριση μιας επιχείρησης. Οι Norli, Ostergaard και Schindele (2015), δείχνουν ότι οι ακτιβιστές συσσωρεύουν περισσότερες μετοχές όταν η ρευστότητα είναι μεγαλύτερη.

8.5 Αντίκτυπος στους Διευθυντές

Η ανταλλαγή μετοχών μιας εταιρείας μέσω Blockchain θα μπορούσε να μειώσει την αποτελεσματικότητα των κίνητρων διαχείρισης του μετοχικού κεφαλαίου. Οι διευθυντές εταιρειών λαμβάνουν τα περισσότερα από τα κίνητρά τους από την αποζημίωση μετοχών, από δικαιώματα προαίρεσης αγοράς μετοχών ή από περιορισμένες μετοχές. Ωστόσο, η βιβλιογραφία υποστηρίζει ότι ακόμη και όταν οι διευθυντές πραγματοποιούν συναλλαγές εντός των καθιερωμένων νομικών ορίων, αντιπροσωπεύουν το εμπιστευτικό εμπόριο ένα de facto σύστημα αποζημίωσης για αυτούς, επιτρέποντας στα στελέχη να εκμεταλλεύονται τουλάχιστον ένα ορισμένο ποσό των εμπιστευτικών πληροφοριών και να αντλήσει μέρος του κέρδους που σχετίζεται με τα πολύτιμα νέα που δημιουργούν.

Η τεχνολογία Blockchain μπορεί να επιτρέψει την παρακολούθηση της διαπραγμάτευσης μετοχών από τρίτους, να παρακολουθούν τις συναλλαγές των διευθυντών σε πραγματικό χρόνο. Οι επενδυτές ενδιαφέρονται έντονα να γνωρίζουν πότε λαμβάνουν ή εκκαθαρίζουν οι διευθυντές των ίδιων κεφαλαίων τις δικές τους επιχειρήσεις, διότι κάθε συναλλαγή αλλάζει τα κίνητρα των διευθυντικών στελεχών και επειδή οι συναλλαγές των διαχειριστών πιθανώς να σηματοδοτούν ιδιωτικές πληροφορίες για την επιχείρηση. Η διαφάνεια των συναλλαγών σε πραγματικό χρόνο θα εκθέσει τους διευθυντές σε μεγαλύτερο έλεγχο από τα διοικητικά συμβούλια και τους μετόχους, γεγονός που πιθανώς τους αναγκάζει να εμπορεύονται λιγότερο συχνά. Το καθαρό αποτέλεσμα πιθανότατα θα μειώσει τα κέρδη των διευθυντών από τις νόμιμες συναλλαγές εμπιστευτικών πληροφοριών και οι επιχειρήσεις ίσως πρέπει να πληρώσουν περισσότερα για να αντισταθμίσουν αυτήν την απώλεια. Ταυτόχρονα, οι διευθυντές μειώνουν τα κίνητρα για την δημιουργία πολύτιμων πληροφοριών που θα μπορούσαν να εκμεταλλευτούν μέσω των συναλλαγών εμπιστευτικών πληροφοριών, ενδεχομένως μειώνοντας την ευθυγράμμιση τους με τους μετόχους.

Ένα σχετικό πρόβλημα για τους διευθυντές θα ήταν η μεγαλύτερη ενημέρωση της αγοράς για το πότε οι μετοχές τους θα ενεχυριαστούν ως ασφάλεια για δάνεια ή σε σχέση με τα παράγωγα προϊόντα ή υπηρεσίες. Αυτές οι στρατηγικές χρησιμοποιούνται συχνά από τους διευθυντές για να επιτύχουν απευθείας εκκαθάριση των κεφαλαιακών τους κινήτρων χωρίς να επιβάλλουν φόρο ή σηματοδότηση δικαστικών εξόδων.

Ένα σύστημα καταχώρισης βασισμένο στο Blockchain θα αποκλείει επίσης την αναστολή της αποζημίωσης των διαχειριστικών οργάνων. Έρευνες δείχνουν ότι κατά την περασμένη δεκαετία οι διευθυντές λάμβαναν οικονομικά κέρδη και τα φορολογικά οφέλη μέσω της αναδρομικής, ποικίλης, απονομής των δικαιωμάτων προαίρεσης αγοράς μετοχών, ασκήσεις δικαιωμάτων προαίρεσης μετοχών και φιλανθρωπικά δώρα αποθέματα. Οι αλυσίδες είναι βάσεις δεδομένων όπου κάθε καταχώρηση έχει μια χρονοσήμανση και δεν μπορεί να τροποποιηθεί εφόσον εγγραφεί. Επομένως οι μεταβιβάσεις μετοχών δεν θα μπορούσαν να είναι επικαιροποιημένες ή διαφορετικά θα άλλαζε αναδρομικά μια μεταρρύθμιση που οι εξωτερικού μέτοχοι θα μπορούσαν να θεωρήσουν ως άριστη αξία ακόμη και ενώ οι διευθυντές θα το θεωρούσαν δαπανηρό.

8.6 Επιπτώσεις στην Μικροδομή της Αγοράς

Στις σημερινές αγορές, εάν οι ταυτότητες των εμπόρων είναι αδιαφανείς, τότε η διάκριση των ενημερωμένων εμπόρων από τους εμπόρους θορύβου ή τους εμπόρους ρευστότητας μπορεί να είναι δύσκολη για τους διαμορφωτές αγοράς. Αυτό ισχύει ιδιαίτερα όταν πουλάει ένας επενδυτής, δεδομένου ότι οι πολλές πωλήσεις οφείλονται σε διαταραχές ρευστότητας, ενώ οι αγορές είναι πιο πιθανό να οδηγούνται από πληροφοριακά πλεονεκτήματα, δεδομένου ότι οι θετικοί κραδασμοί ρευστότητας είναι πολύ λιγότερο συχνοί από τους αρνητικούς. Πολλές μελέτες διαπιστώνουν ότι οι συναλλαγές των διευθυντών λαμβάνουν πολύ ισχυρότερες αντιδράσεις στην αγορά όταν πρόκειται για αγορές παρά πωλήσεις. Αν οι αλυσίδες βελτιώνουν την διαφάνεια των ταυτοτήτων των επενδυτών, τότε ενημερώνεται η πώληση θα μπορούσε να γίνει ευκολότερα διαφοροποιημένη από πριν και η ταχύτητα με την οποία οι δυσμενείς ειδήσεις κατακρατούνται στις τιμές των μετοχών θα μπορούσαν ως εκ τούτου να αυξηθούν. Αυτό θα αποτελούσε μια αλλαγή για τα σημερινά πρότυπα της αγοράς, στα οποία τα καλά νέα φτάνουν στην αγορά πιο εύκολα από τα κακά νέα.

Η αυξημένη διαφάνεια ενός συστήματος καταχώρισης μετοχών με αποκλεισμούς θα μπορούσε να επιτρέψει στους διαμορφωτές της αγοράς να παρατηρούν τις θέσεις ιδιοκτητών των επενδυτών όχι μόνο στις μετοχές που διαπραγματεύονται αλλά και σε άλλες μετοχές. Ακολουθώντας την λογική των Edmans,Levit,Reilly (2016), έστω ένας επενδυτής που κατέχει δύο αποθέματα, με το κάθε ένα να διαπραγματεύεται ένας ξεχωριστός κατασκευαστής αγοράς που δεν μπορεί να παρακολουθήσει το εμπόριο της άλλης μετοχής. Εάν ο επενδυτής πουλάει, ο δημιουργός της αγοράς μπορεί να θεωρήσει το εμπόριο να βασίζεται είτε σε δυσμενείς πληροφορίες είτε σε σοκ ρευστότητας. Η δυνατότητα να παρατηρείται κατά πόσον ο επενδυτής πωλεί την άλλη μετοχή ταυτόχρονα θα βελτίωνε την ακρίβεια των συμπερασμάτων του κατασκευαστή της αγοράς σχετικά με το εάν οι επιμέρους συναλλαγές είναι ενημερωμένες ή καθοδηγούμενες από ρευστότητα. Αυτό θα μπορούσε ενδεχομένως να οδηγήσει σε αποδοτικότερες τιμές και μειωμένα ασφάλιστρα κινδύνου που χρεώνει ο δημιουργός της αγοράς. Οι πιο ενημερωτικές τιμές με την σειρά τους θα βελτίωναν την απόδοση της πραγματικής οικονομίας

επιτρέποντας στους διαχειριστές, τους επενδυτές , τους προμηθευτές και άλλους να λαμβάνουν καλύτερες αποφάσεις σχετικά με την τιμή και τον όγκο του κεφαλαίου που διατίθενται σε διαφορετικές επιχειρήσεις και έργα.

Εάν η μεγαλύτερη διαφάνεια των Blockchains αποθαρρύνει την εμπορία εμπιστευτικών πληροφοριών από διαχειριστές, όπως αναφέρθηκε παραπάνω, οι εξωτερικοί επενδυτές και οι αναλυτές θα είχαν περισσότερα κίνητρα να επενδύσουν στην απόκτηση πληροφοριών σχετικά με την επιχείρηση. Αυτό θα μπορούσε να αναδιατάξει την συνολική κατανομή των πληροφοριών στην οικονομία και ενδεχομένως να οδηγήσει σε μεγαλύτερη κατανεμητή αποδοτικότητα των εξωτερικών επενδύσεων. Η μεγαλύτερη ρευστότητα που παρέχεται από τα Blockchains θα μπορούσε να αυξήσει τα κίνητρα των αναλυτών και των επενδυτών να συλλέξουν ιδιωτικές πληροφορίες, δεδομένου ότι θα μπορούσαν πιο εύκολα να επωφεληθούν από τις πληροφορίες. Αυτό το αποτέλεσμα θα είχε αυξημένες επιπτώσεις στην διακυβέρνηση με την βελτίωση της εξωτερικής παρακολούθησης της διαχείρισης.

8.7 Ψηφοφορία στις Εταιρικές Εκλογές

Η τεχνολογία Blockchain έχει προταθεί ως η πλατφόρμα για την ψηφοφορία σε όλους τους τύπους εκλογών, και φαίνεται να είναι ένα βιώσιμο υποκατάστατο του αρχαϊκού εταιρικού πληρεξούσιου συστήματος ψηφοφορίας που έχει υπομείνει για εκατοντάδες χρόνια με εκπληκτικά λίγες παραχωρήσεις στην μοντέρνα τεχνολογία. Τον Φεβρουάριο του 2016, το χρηματιστήριο NASDAQ, ανακοίνωσε ένα πιλοτικό πρόγραμμα για την ψηφοφορία κατά ομάδες στις συνεδριάσεις των μετόχων για τις εταιρείες εισηγημένες στο χρηματιστήριο. Το NASDAQ, το οποίο είναι ο εταιρικός γονέας ενός πολύ μεγαλύτερου αποθέματος ανταλλαγών στην Νέα Υόρκη, δήλωσε στην ανακοίνωσή του ότι «η τεχνολογία Blockchain θα επιτρέψει την γρήγορη και ασφαλή καταγραφή των αποτελεσμάτων, την εξομάλυνση μιας διαδικασίας ψηφοφορίας με πληρεξούσιο, η οποία ιστορικά ήταν έντονη και κατακερματισμένη».

Πολλές μελέτες όπως αυτή των Kahan και Rock (2008), έχουν τεκμηριώσει τα τρέχοντα προβλήματα με τις εταιρικές εκλογές, που περιλαμβάνουν ανακριβείς λίστες ψηφοφόρων, ελλιπή κατανομή των ψηφοδελτίων και μερικές φορές χαοτική ψηφοφορία. Σε μια εκλογική φάση, οι ψηφοφόροι θα είχαν δικαίωμα ψήφου να λαμβάνουν μάρκες, που θα μπορούσαν να μεταδώσουν σε διευθύνσεις στο Blockchain για να καταχωρήσουν τις προτιμήσεις τους. Όπως αναφέρθηκε από τους Wright και DeFilippi (2015), η μεγαλύτερη ταχύτητα διαφάνειας και ακρίβεια ψηφοφορίας με Blockchain θα μπορούσε να παρακινήσει τους μετόχους να συμμετάσχουν πιο άμεσα στην εταιρική διακυβέρνηση και να ζητήσουν ψηφοφορία σε περισσότερα θέματα και με μεγαλύτερη συχνότητα. Λόγω της διαφάνειας των Blockchains, η εξασφάλιση της ανωνυμίας των ψηφοφόρων θα ήταν προφανές πρόβλημα, αλλά αυτό το πρόβλημα θα περιοριζόταν σε μια μειοψηφία εταιρειών, δεδομένου ότι οι περισσότερες εταιρείες δεν χρησιμοποιούν επί του παρόντος εμπιστευτικές ψηφοφορίες.

8.7.1 Ακρίβεια Εκλογών

Η ανακρίβεια των ψηφοφοριών υπό τις τρέχουσες διαδικασίες, συνεπάγεται και υψηλό βαθμό ανακρίβειας στις εταιρικές εκλογές. Σε ένα αποτέλεσμα που είναι κοντά στο 45-55 επί τοις εκατό, δεν είναι ξεκάθαρο το ποιος κέρδισε. Οι ιδιοτροπίες στον τρόπο ψηφοφορίας καθώς και οι δημοσκοπήσεις εισάγουν έναν θόρυβο στην όλη διαδικασία. Ο Listokin (2008), αναφέρει πως οι κλειστές εκλογές συνήθως καταλήγουν σε αποφάσεις που είναι υπέρ την διεύθυνσης, σε έναν αρκετά μεγάλο αριθμό περιπτώσεων, γεγονός που υποδηλώνει ότι τα αποτελέσματα υπόκεινται σε χειραγώγηση. Αναφέρει πως «σε κάποια στιγμή η διοίκηση αποκτά ακριβείς πληροφορίες για τα αποτελέσματα και με βάση αυτές τις πληροφορίες προσπαθεί να επηρεάσει την ψηφοφορία», με πιέσεις και τακτικές της τελευταίας στιγμής.

Τα οφέλη από τις εκλογές με την τεχνολογία Blockchain θα περιελάμβαναν ταχύτερη και ακριβέστερη κατάταξη των ψηφοφοριών και ίση διαφάνεια σε πραγματικό χρόνο όσον αφορά το πιθανό αποτέλεσμα της ψηφοφορίας τόσο για τους διευθυντές όσο και για τους διαφωνούντες μετόχους. Αυτό θα μπορούσε να δώσει σε κάθε πλευρά ίσες ευκαιρίες να παρέμβει στις τακτικές εκστρατείας τελευταίας στιγμής και να επιλυθούν αμφιβολίες σχετικά με τα αποτελέσματα των προσεχών εκλογών. Το καθαρό αποτέλεσμα θα μπορούσε να είναι η συχνότερη εκλογή αντιφρονούντων εκτός των υποψηφίων που εκπροσωπούν ακτιβιστές των μετόχων ή άλλων ομάδων και δυνητικά συχνότερες ήττες των προτάσεων διαχείρισης που σχετίζονται με την αποζημίωση και την διακυβέρνηση.

8.7.2 Κενή Ψηφοφορία

Η κενή ψήφος συμβαίνει όταν ένας επενδυτής χρησιμοποιεί δανειοληπτικές μετοχές ή ορισμένους συνδυασμούς παραγώγων εξασφαλίσεων για την προσωρινή απόκτηση δικαιωμάτων ψήφου, χωρίς οικονομική έκθεση στα δικαιώματα ταμειακών ροών που συνδέονται με τις υποκείμενες μετοχές. Πολλές από αυτές τις στρατηγικές βασίζονται στην μυστικότητα και μπορούν να κορυφωθούν σε επενδυτές που εμφανίζονται την ημέρα των εκλογών με πολύ περισσότερες ψήφους από ότι αναμενόταν. Ορισμένα κενά συστήματα ψηφοφορίας δεν είναι απολύτως νόμιμα, αλλά έχουν καταφέρει να πετύχουν δυσκολίες παρατήρησης και επιβολής.

Η κενή ψήφος είναι αμφιλεγόμενη. Οι αντίπαλοι τείνουν να την χαρακτηρίζουν αντιδημοκρατική καθώς περιλαμβάνει την απόκτηση δικαιωμάτων ψήφου χωριστά από τα άλλα προηγούμενα περιουσιακά στοιχεία και μπορεί ενδεχομένως να χρησιμοποιηθεί για την υποστήριξη της λανθασμένης πλευράς μιας ερώτησης ψηφοφορίας για να δημιουργήσει δυσμενείς συνέπειες και αποτελέσματα που ωφελούν κατά κάποιον τρόπο τον ψηφοφόρο. Ωστόσο, οι υποστηρικτές θεωρούν την κενή ψηφοφορία αποτελεσματική, καθώς επιτρέπει την τιμολόγηση των δικαιωμάτων ψήφου ανάλογα με το οριακό τους όφελος για τον ψηφοφόρο με την υψηλότερη αξία και παρέχει στους μετόχους της μειοψηφίας την ευκαιρία να επωφεληθούν από την πώληση. Όποια και αν είναι τα πλεονεκτήματα αυτών των επιχειρημάτων, γίνεται σαφές ότι η άσκοπη ψηφοφορία θα γίνει δυσκολότερη με την καταχώριση μετοχών , η οποία θα περιείχε τόσο διαφάνεια όσο και έγκαιρη προειδοποίηση για την αναδιάταξη των δικαιωμάτων ψήφου πριν από τις εκλογές. Για παράδειγμα, ο

απλούστερος τύπος κενής ψηφοφορίας περιλαμβάνει δανεισμό μετοχών στην αγορά δανεισμού μετοχών , με δικαιώματα ψήφου να μεταβιβάζονται στον δανειολήπτη μέχρι την επιστροφή των μετοχών. Ένα τέτοιο δάνειο θα είναι άμεσα διαφανές, παρέχοντας ειδοποίηση στους μετόχους, την διοίκηση και τους ρυθμιστικούς φορείς σχετικά με την ανακατανομή των δικαιωμάτων ψήφου. Οι αντίπαλοι θα μπορούσαν να λάβουν μέτρα για να εξουδετερώσουν την απόκτηση ψήφων από έναν κενό ψηφοφόρο και οι ρυθμιστικές αρχές θα μπορούσαν ενδεχομένως να επιβάλλουν την ψήφιση των μετοχών.

8.8 Λογιστική σε Πραγματικό Χρόνο

Μια επιχείρηση θα μπορούσε να δημοσιεύσει εθελοντικά όλες τις συνήθεις εμπορικές συναλλαγές σε έναν δημόσιο κατάλογο. Αυτό θα συνέβαινε αυτόματα αν η επιχείρηση χρησιμοποιούσε ψηφιακά νομίσματα ως μέσο ανταλλαγής, δεδομένου ότι το ίδιο το νόμισμα θα κατοικούσε σε ένα Blockchain, αλλά θα μπορούσε επίσης να γίνει με την χρήση token, όπως συζητήθηκε προηγουμένως, ή ακόμα και σε συμβατικό νόμισμα αν γίνει με την άδεια της αλυσίδας. Όπως όλες οι συναλλαγές Blockchain, τα συνηθισμένα λογιστικά δεδομένα της επιχείρησης θα μπορούσαν να καταγράφονται μόνιμα σε μια χρονοσφραγίδα εμποδίζοντας την τροποποίηση εκ των υστέρων. Το πλήρες βιβλίο της εταιρείας θα είναι τότε ορατό αμέσως σε οποιονδήποτε μέτοχο, πελάτη, δανειστή, πιστωτικό φορέα ή άλλο ενδιαφερόμενο. Οποιοσδήποτε θα μπορούσε να συγκεντρώνει τις συναλλαγές της επιχείρησης με την μορφή λογαριασμού αποτελεσμάτων και ισολογισμού ανά πάσα στιγμή και δεν θα έπρεπε πλέον να βασίζεται σε τριμηνιαίες οικονομικές καταστάσεις που καταρτίζονται από την εταιρεία και τους ελεγκτές της. Αν και αυτή η ριζική αλλαγή στην οικονομική πληροφόρηση θα έβγαινε προφανώς σε μια ιδιόκτητη πληροφορία διαθέσιμη για τους ξένους- αυτό θα έχει δύο τεράστια οφέλη. Οι μέτοχοι θα είχαν αυξήσει την εμπιστοσύνη τους στην ακεραιότητα των δεδομένων της εταιρείας και οι δαπανηροί ελεγκτές δεν χρειάζεται να προσληφθούν για να εγγυηθούν την ακρίβεια των βιβλίων και των αρχείων της εταιρείας.

8.8.1 Λογιστές και Ενδιάμεσοι Χρηματοπιστωτικοί Οργανισμοί

Σε έναν κόσμο με λογιστική σε πραγματικό χρόνο, οι καταναλωτές των πληροφοριών των οικονομικών καταστάσεων δεν θα πρέπει να βασίζονται στην κρίση των ελεγκτών και στην ακεραιότητα των διευθυντών. Αντί για αυτό θα μπορούσαν να εμπιστευτούν με βεβαιότητα τα στοιχεία σχετικά με την αλυσίδα, και να επιβάλουν την δική τους λογιστική κρίση για να κάνουν τις δικές τους μη μετρητές προσαρμογές, όπως η απόσβεση ή η ανατίμηση του αποθέματος. Οι δυνητικές αποταμιεύσεις των ΗΠΑ ισούνται με τα συνολικά έσοδα της λογιστικής βιομηχανίας, που υπερβαίνει τα 50 δισεκατομμύρια ετησίως. Το ποσό αυτό αντιπροσωπεύει το κοινωνικό κόστος για την επικύρωση από τρίτους της ακρίβειας των λογαριασμών των εταιρειών ή πιο απλά του κοινωνικού κόστους της δυσπιστίας των εταιρικών διαχειριστών. Αντί να στηριχθεί στην βιομηχανία ελέγχου, η οποία έχει υποβληθεί σε ηθικά προβλήματα και προβλήματα γραφείου, κάθε χρήστης θα μπορούσε να δημιουργήσει χωρίς κόστος τις δικές του οικονομικές καταστάσεις από τα δεδομένα της αλυσίδας, ανεξάρτητα από το χρονικό διάστημα που επιθυμεί. Οι χρήστες θα μπορούσαν να έχουν πρόσβαση στα πρωτογενή δεδομένα της εταιρείας και να δημιουργήσουν τις δικές τους αποφάσεις σχετικά με τα χρονοδιαγράμματα απόσβεσης, η επισήμανση των περιουσιακών στοιχείων στην εύλογη αγοραία αξία και η αναγνώριση

των μη ταμειακών εσόδων σε κέρδη. Για να επιβιώσουν οι λογιστές θα πρέπει να επανεξετάσουν τον εαυτό τους ως διερμηνείς των ακατέργαστων οικονομικών στοιχείων και δεδομένων μεγάλου μεγέθους και πολυπλοκότητας πολλών εταιρειών, η ζήτηση της αγοράς για τις υπηρεσίες τους θα συνεχίσει πιθανώς με κάποια μορφή.

8.8.2 Διαχείριση Εσόδων

Η λογιστική σε πραγματικό χρόνο σχετικά με το Blockchain θα μειώσει σημαντικά τις ευκαιρίες για τις επιχειρήσεις να συμμετάσχουν σε λογιστικά τεχνάσματα και να καταστρέψουν τις πραγματικές ενέργειες για να χειραγωγήσουν τα αναφερόμενα κέρδη. Με τις μη αναστρέψιμες, χρονοβόρες συναλλαγές, οι διαχειριστές δεν μπορούσαν να χρησιμοποιήσουν στρατηγικές όπως η αναπροσαρμογή των συμβάσεων πώλησης σε μια προηγούμενη περίοδο αναφοράς ή η απόσβεση λειτουργικών εξόδων τα οποία θα πρέπει να δαπανώνται άμεσα και να ωθούν σε μελλοντικές περιόδους. Εάν οι χρήστες βασίζονται στις δικές τους προσαρμοσμένες οικονομικές καταστάσεις, τα σημερινά κοινά δεδομένα και συχνότητες αναφοράς, όπως τα τριμηνιαία κέρδη ανά μετοχή, ενδέχεται να καταστούν πολύ λιγότερο σημαντικά και συνεπώς θα χειροτερεύονταν λιγότερο από τους διαχειριστές. Οι αναλυτές ασφαλείας θα πρέπει να εργαστούν σκληρότερα για να αξιολογήσουν τι εύλογες αξίες των εταιρικών αποθεμάτων, αλλά θα έχουν πολύ περισσότερες πληροφορίες για την εκπλήρωση αυτού του καθήκοντος.

Οι πιθανές συνέπειες αυτών των αλλαγών είναι σημαντικές, καθώς τα στελέχη μπορούν να διαχειριστούν τις επιχειρήσεις τους με διαφορετικό τρόπο, εάν γίνει πιο δύσκολη ή σωρευτική διαχείριση των κερδών. Σύμφωνα με έρευνες οι διαχειριστές είναι πρόθυμοι να προβούν σε άριστες επενδυτικές αποφάσεις, όπως η μείωση των θετικών επενδύσεων σε θετικού δείκτες προς όφελος των βραχυπρόθεσμων λογιστικών κερδών. Εάν η χειραγώγηση των τριμηνιαίων κερδών κατέστη πολύ λιγότερο σημαντική λόγω λογιστικής σε πραγματικό χρόνο, ίσως αυτή η στρέβλωση στις επενδυτικές πολιτικές των εταιρειών να υποχωρήσει. Ωστόσο, η απάντηση των διαχειριστών μπορεί να μην είναι απλή στην πρόβλεψη. Οι Cohen, Dey, Lys (2008), βρήκαν μια στροφή στην διαχείριση των εσόδων σε πραγματικές διαχειρίσεις κερδών μετά την θέσπιση του νόμου, η οποία περιόριζε ορισμένους τρόπους διαχείρισης των λογιστικών κερδών μέσω διακριτικής ευχέρειας.

8.8.3 Συναλλαγές με Συνδεδεμένα Μέρη

Η λογιστική σε πραγματικό χρόνο για το Blockchain θα μπορούσε να επιτρέψει στους παρατηρητές να εντοπίσουν αμέσως ύποπτες μεταβιβάσεις περιουσιακών στοιχείων και άλλες συναλλαγές που συνεπάγονται σύγκρουση συμφερόντων. Οι κανόνες αποκάλυψης των ΗΠΑ και πολλών άλλων χωρών επιβαρύνουν την διοίκηση να αναφέρει αυτομάτως αυτές τις αποκαλούμενες συναλλαγές συνδεδεμένων μερών, αλλά η συμμόρφωση πιστεύεται ότι είναι ατελής και συχνά υπόκεινται σε έντονες συζητήσεις για τις οποίες οι συναλλαγές είναι αρκετά σημαντικές να απαιτήσει γνωστοποίηση. Η διαφάνεια στον τομέα αυτό θα επηρεάσει τα διευθυντικά κίνητρα, δεδομένου ότι οι εμπλεκόμενοι θα έχουν λιγότερη δυνατότητα να αποσύρουν περιουσιακά στοιχεία από την επιχείρηση και θα επέτρεπαν στους πιστωτές να ασχολούνται με την παρακολούθηση σε πραγματικό χρόνο κατά δόλιων μεταβιβάσεων από διευθυντές οικονομικά προβληματικών επιχειρήσεων. Θα μπορούσε επίσης

να αυξήσει το κόστος για τις επιχειρήσεις αν έπρεπε να εξηγήσουν μεγάλου αριθμού μεμονωμένων συναλλαγών στο κοινό.

8.9 Διακυβέρνηση των Blockchains

Οι συμμετέχοντες σε Blockchains όπως οι εταιρείες που μπορούν να καταγράψουν τις μετοχές τους σε ένα μητρώο μετοχών, έχουν πολλούς λόγους να φροντίσουν για την διακυβέρνηση ενός αποκλειστικού τμήματος. Ένα ανοιχτός κατάλογος λειτουργεί αυτόματα από λογισμικό ενός υπολογιστή. Αυτός ο κώδικας προσδιορίζει τις βασικές εισόδους για κάθε συναλλαγή, τον χρόνο και την προτεραιότητα για την κωδικοποίηση αυτών των συναλλαγών στο Blockchain, καθώς και τα όρια των μεγεθών ή των απρόβλεπτων που σχετίζονται με κάθε συναλλαγή μεταξύ άλλων θεμάτων. Αυτές οι παράμετροι λογισμικού είναι σύμφωνες με τους κανόνες και τους κανονισμούς με τους οποίους οι εταιρείες συμφωνούν να απαριθμήσουν τις μετοχές τους και να τις εμπορευθούν από τρίτους με την επιφύλαξη συμφωνημένων περιορισμών και περιορισμών.

Όπως και με τους καθημερινούς κανόνες του χρηματιστηρίου, οι κανονισμοί που ενσωματώνονται στον κώδικα λογισμικού του Blockchain θα μπορούσαν να ευνοήσουν ορισμένες συμμετέχουσες εταιρείες σε βάρος άλλων και ως εκ τούτου η εξουσία αλλαγής αυτών των βασικών κανόνων θα μπορούσε να γίνει εξαιρετικά σημαντική. Τέλος τα Blockchains πρέπει να βασίζονται σε μια διαδικασία διακυβέρνησης στην οποία οι χρήστες συμφωνούν να αλλάξουν ένα σύνολο απαιτήσεων για τον κώδικα λογισμικού, συμπεριλαμβανομένων των διατάξεων για την επίλυση διαφορών, των κυρώσεων για παραβίαση συμφωνηθέντων κανόνων και των διαδικασιών επιβολής κυρώσεων. Σε ένα ιδιωτικό ή εξουσιοδοτημένο Blockchain, διαπραγματεύοντας αυτούς τους κανόνες, συμπεριλαμβανομένων δικαιωμάτων αποστολής, θα πρέπει να είναι παρόμοια με την διαπραγμάτευση μιας συμφωνίας εταιρικής σχέσης. Σε ένα δημόσιο μπλοκ που μπορεί να ενωθεί κανείς, η διακυβέρνηση μπορεί να γίνει πολύ πιο πολύπλοκη.

Τι θα μπορούσε να πάει στραβά για να προκαλέσει κρίση διακυβέρνησης μεταξύ των χρηστών μιας ανοικτής ομάδας, στην οποία οι συναλλαγές επικυρώνονται με απόδειξη της εργασίας. Το πιο βασικό πρόβλημα θα ήταν η επίθεση 51% στην οποία ο ένας συμμετέχων στην αλυσίδα έχει αρκετή εξουσία εξόρυξης για να αναγκάσει μια αλλαγή στο λογισμικό για να επωφεληθεί σε βάρος του καθενός. Η απόκτηση αυτής της μεγάλης χωρητικότητας μπορεί να είναι δαπανηρή ωστόσο, έτσι θα μπορούσαμε να φανταστούμε άλλες πιο λεπτές στρατηγικές. Για παράδειγμα, ένας σαμποτέρ μπορεί να παραπλανήσει τα μέλη του δικτύου να φορτώσουν μια νέα, ελαττωματική έκδοση του κώδικα παραποιώντας τις πραγματικές δυνατότητές του. Κάποιος θα μπορούσε επίσης να δελεάσει άλλους κόμβους με το δίλημμα του φυλακισμένου που τους προσφέρουν μέτριες πληρωμές τις οποίες θα δεχθούν λογικά σε αντάλλαγμα για την φόρτωση του νέου, κατώτερου λογισμικού, παρόλο που η εγκατάλειψη του παλαιού κώδικα κάνει την υπόλοιπη κοινότητα χειρότερη. Άλλες στρατηγικές διαίρεσης και κατάκτησης, χρησιμοποιώντας θεωρητική ανάλυση παιχνιδιού ως θεμέλιο θα μπορούσε επίσης να επινοηθεί. Η προστασία έναντι αυτών των τύπων επιθέσεων διακυβέρνησης μπορεί να προκύψει ως σημαντικό πρόβλημα για μπλοκ ανοικτού κώδικα και το θέμα δεν φαίνεται να έχει λάβει μεγάλη προσοχή από τον Nakamoto και άλλους δημιουργούς αλυσίδων. Παρόλο που η εργασία του Nakamoto εξέφρασε ανησυχίες σχετικά με την δυνατότητα επιθέσεων εναντίων έντιμων κόμβων από

δυνητικούς σαμποτέρ, δεν εξετάζει την δυνατότητα συμπαιγνίας μεταξύ ανθρακωρύχων σε ορυχείο κάτι που αναγνωρίζεται ως σαφής δυνητικός κίνδυνος σήμερα.

Μέχρι στιγμής η πιο ευρέως χρησιμοποιούμενη αλυσίδα είναι αυτή του Bitcoin και λειτουργεί με έναν εξαιρετικά αποκεντρωμένο τρόπο. Το λογισμικό είναι ανοικτού κώδικα και οποιοσδήποτε χρήστης μπορεί να προτείνει μια αλλαγή στον κώδικα ανά πάσα στιγμή. Για να εφαρμοστεί μια αλλαγή, απαιτείται η συναίνεση από το περισσότερο από το 50% των ανθρακωρύχων στο δίκτυο, οι οποίοι απορρίπτουν τον παλιό κώδικα και ξεκινούν την λειτουργία του νέου. Η διαδικασία είναι καθαρά παθητική και σωρευτική δεν υπάρχει κάποιο συγκεκριμένο σημείο εκλογής ή απόφασης, ούτε έχει προγραμματιστεί η αξιολόγηση του νέου κώδικα από τους χρήστες και γενικά δεν υπάρχει κάποιος χρονικός περιορισμός, ,εκτός αν αυτός που εισάγει τον νέο κώδικα τον εισαγάγει με προκαθορισμένο κώδικα εκ των προτέρων. Οι προτεινόμενες αλλαγές του κώδικα μπορούν απλά να αγνοηθούν, ενώ μπορεί να προκύψουν άλλες από εμπειρογνώμονες μέσα από online συζήτηση μεταξύ των συμμετεχόντων στο δίκτυο. Ο Metz (2015), παρέχει μια καλή εισαγωγή σε αυτήν την διαδικασία και συζητά για την τρέχουσα διαμάχη στην κοινότητα του Bitcoin σχετικά με το αν θα αυξηθούν τα μεγέθη των μπλοκ, προκειμένου να εξυπηρετηθεί υψηλότερος όγκος συναλλαγών σε πραγματικό χρόνο. Παρόλο που πολλοί συμφωνούν για την ανάγκη αλλαγών στο Bitcoin, με σκοπό την αντιμετώπιση του αυξανόμενου όγκου των συναλλαγών, πολλοί ανθρακωρύχοι αντιθέτως βλέπουν ένα όφελος για την διανομή της σημερινής περιορισμένης δυναμικότητας, και πολλές προσπάθειες υψηλού προφίλ για την επίτευξη συναίνεσης για τις μεταρρυθμίσεις έχουν αποτύχει μέχρι σήμερα.

9. ΣΥΜΠΕΡΑΣΜΑΤΑ

Όπως φαίνεται στα παραπάνω κεφάλαια, η τεχνολογία Blockchain αποτελεί μια τεχνολογία που είδη έχει αρχίσει να ενσωματώνεται σε τομείς της κοινωνίας, και προσφέρει απεριόριστες δυνατότητες για μελλοντικές εφαρμογές με στόχο την απλοποίηση των διαδικασιών, την ταχύτερη επίτευξή τους αλλά και την μεγαλύτερη αποδοτικότητα. Σε όλες τις περιπτώσεις η τεχνολογία αυτή εγγυάται την ασφάλεια καθώς είναι υπολογιστικά αδύνατο με τα σημερινά δεδομένα να σπάσει το δίκτυο. Η τεχνολογία αυτή έχει μόνο πλεονεκτήματα να προσφέρει και καθημερινά οι έρευνες πάνω στις προοπτικές της αυξάνονται, πολλές χώρες και οργανισμοί έχουν πάρει στα σοβαρά την τεχνολογία Blockchains και δουλεύουν συστηματικά πάνω σε αυτήν.

Η εργασία αυτή ασχολείται αρχικά με δύο πολύ σημαντικούς τομείς της κοινωνίας όπως είναι η Υγεία και η Εκπαίδευση, στην συνέχεια παρουσιάζεται το διαδίκτυο των πραγμάτων, ένας σχετικά νέος χώρος αλλά εκθετικά αυξανόμενος σε έρευνα και υλοποιήσεις καθώς σχετίζεται άμεσα με την καθημερινότητα αλλά και με τον τρόπο ζωής των ανθρώπων. Πολλά τα οφέλη των Blockchains και σε αυτόν τον τομέα όπως και στην Εταιρική Διακυβέρνηση που εξετάζεται τελευταία, έναν τομέα ο οποίος σε πολλές περιπτώσεις ακόμα χρησιμοποίει απαρχαιωμένες μεθόδους για τις καθημερινές διεργασίες και η τεχνολογία Blockchain μπορεί να αλλάξει ριζικά τον τρόπο με τον οποίο λειτουργεί.

9.1 Υγεία

Ο τομέας της υγείας είναι ένας τομέας στον οποίο δίνεται αρκετή προσοχή και αρκετά χρήματα ώστε να μπορεί να υπάρξει η καλύτερη δυνατή υγειονομική περίθαλψη στους ασθενείς. Είναι ένας τομέας στον οποίο τα προσωπικά και ιατρικά δεδομένα των ασθενών πρέπει να είναι πολύ καλά προστατευμένα, τα φάρμακα να είναι νόμιμα και οι συσκευές να βρίσκονται στην θέση τους όταν χρειάζεται κάποιος εργαζόμενος. Η τεχνολογία Blockchain μπορεί να δώσει λύση σε όλα αυτά και σε πολλά ακόμα προβλήματα που εμφανίζονται στον τομέα της υγείας.

Οι κλινικές δοκιμές είναι ένας τομέας στον οποίο τα Blockchains μπορούν να αυξήσουν την διαφάνεια, την ελεγκτική ικανότητα και την υπευθυνότητα των γιατρών και ερευνητών. Ο δημόσιος αμετάβλητος κατάλογος που παρέχεται από το Blockchain μπορεί να αλλάξει ριζικά τον τρόπο τον κλινικών δοκιμών για όλα τα εμπλεκόμενα μέρη προς το καλύτερο. Ο διαμοιρασμός δεδομένων επίσης με την τεχνολογία των αλυσίδων δέχεται πολλές ευκαιρίες βελτίωσης, μπορεί να θέσει τα δεδομένα στα χέρια των ασθενών με την χρήση ενός αμετάβλητου καταλόγου.

Η παρακολούθηση φαρμάκων μπορεί να προστατέψει τους ασθενείς από παραποιημένα ή νοθευμένα φάρμακα και η παρακολούθηση συσκευών να εξοικονομήσει πολλά χρήματα για τα νοσοκομεία αλλά και να ενημερώνει τους υπάλληλους όταν υπάρχει κάποιο πρόβλημα με κάποια συσκευή. Η εφοδιαστική αλυσίδα υγείας αντιμετωπίζει πολλά προβλήματα με πλαστά/υποβαθμισμένα/παραποιημένα φαρμακευτικά προϊόντα, η τεχνολογία Blockchain σε συνδυασμό με τα RFID μπορεί να προσφέρει σημαντικές λύσεις σε αυτά τα προβλήματα.

Τα δεδομένα ιατρικών συσκευών IoHT είναι πολύ σημαντικό να προστατεύονται, διότι περιλαμβάνουν δεδομένα του αναπνευστικού, της καρδιακής λειτουργίας κλπ, δηλαδή πολύ σημαντικά ιατρικά δεδομένα ασθενών. Η τεχνολογία Blockchain δίνει σημαντικές λύσεις και σε αυτά τα ζητήματα. Επίσης η τεχνολογία Blockchain μπορεί να προσφέρει μια κατηγοριοποίηση των δεδομένων των ασθενών και στην συνέχεια αποθήκευση αυτών σε δημόσιους καταλόγους έτσι ώστε να είναι εύκολα προσβάσιμα από τους αρμόδιους.

9.2 Εκπαίδευση

Ο τομέας της εκπαίδευσης είναι και αυτός ένας πολύ σημαντικός τομέας της κοινωνίας στον οποίο μπορούν να υλοποιηθούν λύσεις Blockchain οι οποίες αλλάζουν σε μεγάλο βαθμό τον τρόπο που επιτελούνται διάφορες διεργασίες. Αξίζει να αναφερθεί ότι παρόμοια με τον τομέα της υγείας, και στην εκπαίδευση έχουν γίνει ήδη πολλές εφαρμογές οι οποίες τρέχουν κανονικά από πολλούς και σημαντικούς οργανισμούς παγκοσμίως.

Οι περισσότερες εφαρμογές στον τομέα της υγείας μέχρι στιγμής, γίνονται στον τομέα των πιστοποιητικών και των πανεπιστημιακών πτυχίων. Η τεχνολογία Blockchain δημιουργεί έναν δημόσιο κατάλογο με πιστοποιητικά, στα οποία υπάρχει απόλυτη ασφάλεια και προστασία για πλαστά πιστοποιητικά. Η παραπάνω διαδικασία μπορεί να προσφέρει πολλά πλεονεκτήματα στους εκδότες, στους εργοδότες και περισσότερο από όλους στους ίδιους τους μαθητές/φοιτητές.

Η τεχνολογία αυτή μπορεί να χρησιμοποιηθεί με επιτυχία στον τομέα της διδασκαλία και της παιδαγωγικής, με κομμάτια επιτεύγματος και μικρά βραβεία για την αναγνώριση της προσπάθειας των μαθητών. Στον πανεπιστημιακό τομέα μπορεί να δίνεται φήμη μέσω του Blockchain στους σπουδαστές, η σε αυτούς οι οποίο παρουσιάζουν κάτι αξιέπαινο.

Πολλές είναι επίσης και οι μελλοντικές εφαρμογές που μπορούν να υλοποιηθούν, έξυπνα συμβόλαια μεταξύ μαθητών και καθηγητών, ή καθηγητών και σχολείων αποτελούν το μέλλον στον τομέα της εκπαίδευσης και της αξιολόγησης των μαθητών αλλά και των καθηγητών και της δουλειάς τους.

9.3 IoT

Το IoT αποτελεί κάτι νέο σε σχέση με τα δύο προηγούμενα, είναι ένας τομέας ο οποίος εξελίσσεται συνεχώς και πλέον έχει περάσει σε άλλη διάσταση αν σκεφτεί κανείς ότι γίνονται προσπάθειες ακόμη και για την δημιουργία έξυπνων πόλεων. Το IoT χρησιμοποιείται σε πολλούς τομείς της καθημερινότητας και προσφέρει πλήθος πλεονεκτημάτων.

Η τεχνολογία Blockchain μπορεί να δώσει λύσεις σε συνδυασμό με το IoT στην εφοδιαστική αλυσίδα και την παρακολούθηση της πορείας ενός προϊόντος σε αυτήν. Επίσης μπορεί να προσφέρει πολύ μεγάλη αύξηση της ασφάλειας στον συγκεκριμένο χώρο, κάτι που είναι και απαραίτητο, καθώς το IoT περιλαμβάνει πολλές συσκευές αισθητήρες ακόμα και σε μέρη του σπιτιού, οπότε κρίνεται αναγκαία η διαφύλαξη της Ιδιωτικότητας.

Μπορεί επίσης να βοηθήσει πολύ το εγχείρημα του έξυπνου σπιτιού με πολλές συσκευές οι οποίες διαχειρίζονται από έναν κεντρικό ανθρακωρύχο. Ο βιομηχανικός τομέας επίσης μπορεί να πάρει πολλά από αυτήν την τεχνολογία, όπως για παράδειγμα η δημιουργία απόλυτα αυτόνομων οχημάτων ή η έξυπνη παραγωγή φυτών.

9.4 Εταιρική Διακυβέρνηση

Η Εταιρική Διακυβέρνηση είναι ένα σύνολο κανόνων που εφαρμόζονται στις εταιρείες και ρυθμίζουν την λειτουργία του ΔΣ σε σχέση με τους μετόχους της εταιρείας. Με την Εταιρική Διακυβέρνηση επιδιώκεται η υπεύθυνη οργάνωση, λειτουργία, διοίκηση και έλεγχος μιας εταιρείας με στόχο την αύξηση της αξίας της και την προστασία των έννομων συμφερόντων όλων των μετόχων της. Η τεχνολογία Blockchain μπορεί να δώσει λύσεις σε μακροχρόνια προβλήματα αυτού του κλάδου ο οποίος σε αρκετές περιπτώσεις χρησιμοποιεί απαρχαιωμένους τρόπους και μεθόδους για τις καθημερινές διαδικασίες.

Η έκδοση και διαπραγμάτευση εταιρικών χρεογράφων σε Blockchains θα δημιουργούσε πολλά οφέλη και επίσης ορισμένες δαπάνες που σχετίζονται με μεγαλύτερη διαφάνεια ιδιοκτησίας και ταχύτερο, φθηνότερο εμπόριο και διακανονισμούς. Η πώληση μετοχών στο Blockchain θα μπορούσε να προσφέρει μεγαλύτερη ρευστότητα μειώνοντας αρκετά τα κόστη προμηθειών. Επίσης αποτέλεσμα της βελτίωσης της ρευστότητας θα ήταν η αύξηση της ζήτησης των αποθεμάτων.

Σημαντικές επιπτώσεις επίσης δημιουργούνται στους θεσμικούς επενδυτές στους ακτιβιστές αλλά και στους διευθυντές. Ο τρόπος με τον οποίο συναλλάσσονται όλοι οι παραπάνω αλλάζει ριζικά και ο έλεγχος με την χρήση αλυσίδας αυξάνεται σημαντικά. Μεγάλες οι βελτιώσεις και στον τομέα των εταιρικών ψηφοφοριών με την χρήση αλυσίδων αλλά και στην λογιστική σε πραγματικό χρόνο.

9.5 Συνολικά

Κλείνοντας, έπειτα από την ανάγνωση των παραπάνω κεφαλαίων αλλά και των συμπερασμάτων γίνεται αντιληπτό ότι η τεχνολογία Blockchain θα αποτελέσει μια από τις σημαντικότερες τεχνολογίες σε διάφορους τομείς της κοινωνίας. Οι εφαρμογές της δεν περιορίζονται σε αυτά που αναφέρονται σε αυτήν την εργασία, υπάρχει ένα πλήθος αναφορών για και άλλους πολύ σημαντικούς τομείς όπως το περιβάλλον, η μηχανική, ο τουρισμός και γενικότερα κάθε τι που έχει να κάνει με διαχείριση δεδομένων μπορεί να γίνει πλέον με την χρήση της τεχνολογίας αυτής.

Δεν αποτελεί μια τεχνολογία που θα αντικαταστήσει τον γιατρό ή το δάσκαλο, αποτελεί μια τεχνολογία η οποία μπορεί να δουλέψει εναρμονισμένα μαζί με τον γιατρό και τον δάσκαλο με στόχο το καλύτερο δυνατό αποτέλεσμα. Αποτελεί μια τεχνολογία που μπορεί να αλλάξει εξ’ ολοκλήρου τον τρόπο που επιτελούνται οι εργασίες σήμερα αλλά και τον τρόπο σκέψης σχετικά με τις δημόσιες συναλλαγές και την κρυφή ταυτότητα.

Αυτή η αποκεντρωμένη ιδιότητα που χαρακτηρίζει το Blockchain, η μη ύπαρξη τρίτου μέρους στις συναλλαγές, τα έξυπνα συμβόλαια αλλά και τεχνολογίες όπως το RFID δίνουν και θα δώσουν στο μέλλον έναν μεγάλο αριθμό καινοτόμων εφαρμογών, οι οποίες θα βοηθούν την καθημερινότητα όλων.

10. ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] «Bitcoin: A Peer-to-Peer Electronic Cash System», 2008, Satoshi Nakamoto

[2] «Blockchain Technology Beyond Blockchain», 2015, Michael Crosby, Navhiappan, Pradhan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman

[3] «Pragmatic, Interdisciplinary Perspectives on Blockchain and Distributed Ledger Technology:Pavin the Future oh Healthcare», 2018, Ron Ribitzky, James St. Clair, David I. Houdling, Chrissa T. McFarlane, Brian Ahier, Michael Gould, Heather L. Flannery, Erik Pupo, Kevin A. Clauson

[4] «Applications of Blockchain Within Healthcare», 2018, Liam Bell, William J. Buchanan, Jonathan Cameron, Owel Lo

[5] «Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare: An Exploration of Challenges and Opportunities in the Health Supply Chain», 2018, Kevin A. Clauson, Elizabeth A. Breeden, Cameron Davidson, Timothy K. Mackey

[6] «A case Study for Blockchain in Healthcare: MedRec prototype for electronic health records and medical research data», 2016, Ariel Ekblaw, Asaph Azaria, John D. Halamka, Andrew Lippuan,

[7] «Blockchain in Healthcare», 2018, Richa Sharma

[8] «Blockchain for Healthcare: The Next Generation of Medical Records», 2018, Claude Pirtle, Jesse Enhenfeld

[9] «Geospatial blockchain: promises, challenges, and scenarios in health and healthcare», 2018, Maged N. Kamel Boulos, James T. Wilson, Kevin A. Clauson

[10] «Blockchain 4 Education», 2018, Sabine Kolvenbach, Rudolf Ruland, Wolfgang Grather, Wolfgang Prinz

[11] «Blockchain for Education: Lifelong Learning Passport», 2018, Wolfgang Grather, Sabine Kolvenbach, Rudolf Ruland, Julian Schutte, Christof Ferreira Torres, Florian Wandland

[12] «Trustless Education. A Blockchain System for University Grades», 2017, John Rooksby, Kristian Dimitrov

[13] «Blockchain in Education», 2017, Grech Alexander, Camilleri Anthony F.

[14] «Exploring blockchain technology and its potential applications for education», 2018, Guang Chen, Bing Xu, Manli Lu, Nian-Shing Chen

[15] «The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward», 2016, Mike Sharples, John Domingue

[16] «Innovating Pedagology», 2016, Mike Sharples, Roberto de Roock, Rebecca Ferguson, Mark Gaved, Christothea Herodotoy, Elizabeth Koh, Agnes Kukuska-Hulme, Chee-Kit Looi, Patrick McAndrew, Bart Rienties, Martin Weller, Lung Hsiang Wong

[17] «Blockchains and Smart Contracts for the Internet of Things», 2016, Konstantinos Christideis, Michael Devetsikiotis

[18] «Blockchain: A Game Changer for Securing IoT Data», 2018, Madhusudan Singh, Adhiraj Singh, Shimo Kim

[19] «Poster Abstract: Privacy in Blockchain-Enabled IoT Devices», 2018, Arman Pouraghily, Md Nazmul Islam, Sandip Kundu, Tilman Wolf

[20] «Blockchain and the Internet of Things in the Industrial Sector», 2018, Denis Miller

[21] «Blockchain for Iot Security and Privacy: The Case Study of a Smart Home», 2017, Ali Dorri, Salil S. Kanhere, Raja Jurdak, Praveen Gauravaram

[22] «Towards an Optimized Blockchain for IoT», 2017, Ali Dorri, Salil S. Kanhere, Raja Jurdak

[23] «IoT and Blockchain Convergence: Benefits and Challenges», 2017, Ahmed Banafa

[24] «Role Applications of IoT in Online Transactions using Blockchain Technology», 2018, Akash Shandilya, Himanshu Gupta, Sunil Kumar Khatri

[25] «Blockchain και η εφαρμογή του στο Internet Of Things», 2017, Γεωργία Ντοά

[26] «Corporate Governance and Blockchains», 2017, David Yermack

[27] «A Distributed Infrastructure for Democratic Cloud Federations», 2017, Andrea Margeri, Md Sadek Ferdous, Mu Yang, Vladimiro Sassone

[28] «Comparison and Analysis of Governance Mechanisms Employeed by Blockchain-Based Distributed Autonomous Organizations», 2018, Stephen DiRose, Mo Mansouri

[29] «Violable Contracts and Governance for Blockchain Applications», 2018, Munindar P. Singh, Amit K. Chopra

[30] «Changing Governance Models by Applying Blockchain Computing», 2018, Steve Young

[31] «Blockchain: The Birth of Decentralized Governance», 2018, Benito Arrunada, Luis Garicano

[32] «Governance in Blockchain Technologies & Social Contract Theories», 2016, Wessel Reijers, Fiachra O Brolchain, Paul Haynes

[33] «Blockchain Technology and Decentralized Governance: Is the State Still Necessary?», 2015, Marcella Atzori

[34] «Βασικές Αρχές Ασφάλειας Δικτύων Εφαρμογές και Πρότυπα», 2008, William Stallings, Εκδόσεις Κλειδάριθμος

[35] «Κρυπτογραφία και Ασφάλεια Δικτύων Αρχές και Εφαρμογές», 2006, William Stallings, Εκδόσεις Ίων

[36]https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1 (Κρυπτογραφία Wiki)

[37]https://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF_%CF%84%CF%89%CE%BD_%CF%80%CF%81%CE%B1%CE%B3%CE%BC%CE%AC%CF%84%CF%89%CE%BD (IoT Wiki)

[38]https://el.wikipedia.org/wiki/%CE%A8%CE%B7%CF%86%CE%B9%CE%B1%CE%BA%CE%AE_%CF%85%CF%80%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AE (Ψηφιακή Υπογραφή Wiki)

[39] https://en.wikipedia.org/wiki/Smart_contract (Έξυπνο Συμβόλαιο Wiki)

[40] https://en.wikipedia.org/wiki/Peer-to-peer (Ομότιμο Δίκτυο Wiki)

[41]https://el.wikipedia.org/wiki/%CE%A3%CF%85%CE%BD%CE%AC%CF%81%CF%84%CE%B7%CF%83%CE%B7_%CE%BA%CE%B1%CF%84%CE%B1%CF%84%CE%B5%CE%BC%CE%B1%CF%87%CE%B9%CF%83%CE%BC%CE%BF%CF%8D (Συνάρτηση Κατακερματισμού Wiki)

[42] https://www.blockchaintechnologies.com/applications/

[43]https://www.lawspot.gr/nomika-nea/paneyropaiko-organismo-gia-tin-tehnologia-blockchain-etoimazei-i-eyropaiki-enosi

[44]https://www.lawspot.gr/nomika-nea/panepistimio-leykosias-proto-panepistimio-ston-kosmo-poy-ekdidei-diplomata-apofoiton-sto

[45] https://www.blockchain.com/

[46] https://en.wikipedia.org/wiki/Home_automation (Έξυπνο Σπίτι Wiki)