Πανεπιστήμιο Πειραιώς

Τμήμα Ψηφιακών Συστημάτων

Μεταπτυχιακό Ψηφιακές Επικοινωνίες και Δίκτυα

Μεταπτυχιακή Διπλωματική Εργασία

«Blockchain και η εφαρμογή του στο Internet of Things (IoT)»

Όνομα: Γεωργία Ντοά

Α.Μ.: ΜΕ11087

Επιβλέπων Καθηγητής Δημοσθένης Κυριαζής

Τριμελής εξεταστική επιτροπή:

Καθηγητής Άγγελος Ρούσκας

Επίκουρος Καθηγητής Απόστολος Μηλιώνης

Επίκουρος Καθηγητής Δημοσθένης Κυριαζής

Αθήνα Φεβρουάριος 2017

Περιεχόμενα:

Κεφάλαιο 4

Εισαγωγή

Η μοντέρνα τεχνολογία επιτρέπει στους ανθρώπους να επικοινωνούν άμεσα με την χρήση φωνητικών και βίντεο κλήσεων, emails, άμεσα μηνύματα τα οποία ταξιδεύουν από την μία συσκευή σε μία άλλη. Η επικοινωνία γίνεται διατηρώντας την εμπιστοσύνη ο ένας στον άλλο, χωρίς την παρουσία τρίτου, ανεξάρτητα από το πόσο μακριά βρίσκονται.

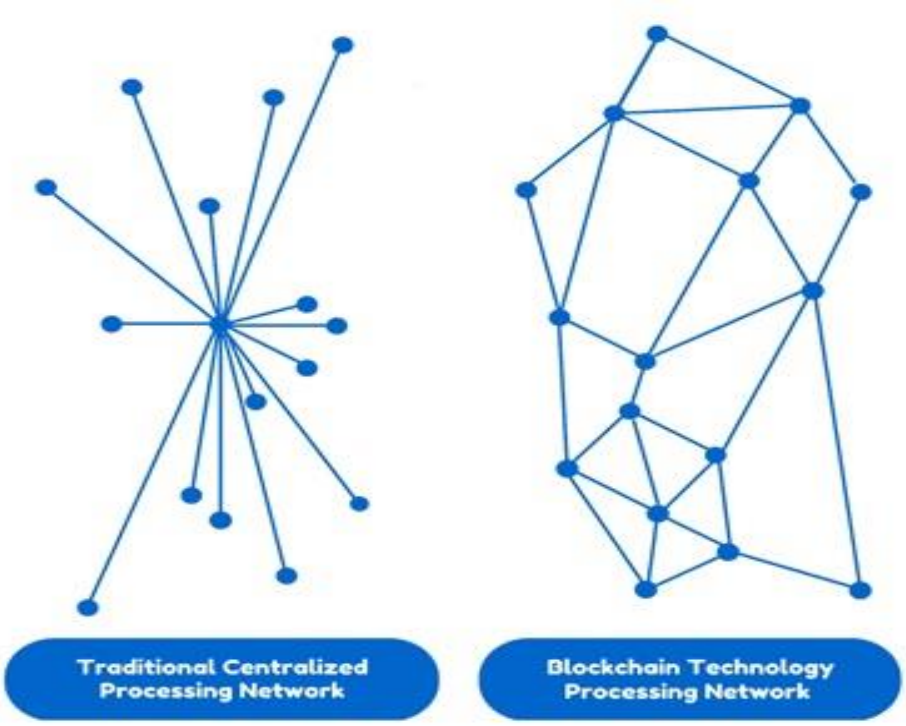
Όταν όμως σε μία επικοινωνία μεταξύ δύο σημείων χρειάζεται να γίνει μία συναλλαγή, τότε οι διαδικασίες απαιτούν την εμπιστοσύνη ενός τρίτου για εδραίωση της εμπιστοσύνης όπως ένα δικηγορικό γραφείο ή μία τράπεζα, με αποτέλεσμα το υψηλό κόστος, την απάτης και της αναποτελεσματικότητας.

Η τεχνολογία blockchain έρχεται να αλλάξει ριζικά αυτό το καθεστώς. Χρησιμοποιώντας μαθηματικά και κρυπτογραφία το blockchain παρέχει μία ανοιχτή και αποκεντρωμένη βάση δεδομένων σε κάθε συναλλαγή που περιέχει αξία όπως χρήματα, αγαθά, ακίνητη περιουσία, εργασία ή ακόμα και σημειώσεις. Δημιουργεί μία καταγραφή για κάθε συναλλαγή η οποία μπορεί να επαληθευτεί από όλη την κοινότητα. Το blockchain συνδυάζοντας την κρυπτογραφία και τα κατανεμημένα υπολογιστικά συστήματα παρέχει ασφαλείς, άμεσες peer-to-peer συναλλαγές, χωρίς την ανάγκη για τρίτους.

Αν σωστά κατασκευασμένη, η blockchain τεχνολογία προσφέρει λύση στο πρόβλημα της ασφάλειας και της ιδιωτικότητας στον Internet of Things (IoT) περιβάλλον, παρέχοντας ένα νέο υπολογιστικό στρώμα όπου τα δεδομένα μπορούν να υποβάλλονται σε επεξεργασία να αναλύονται με ασφάλεια, παραμένοντας ιδιωτικά. Το blockchain μπορεί επίσης να επιτρέψει τις μικρο-πληρωμές μεταξύ ψηφιακών συσκευών, μέσω ultra-light cryptocurrencies και έξυπνων συμβάσεων. Η

υλοποίηση των χαρακτηριστικών αυτών αναμένεται να εξασφαλίσει μια πιο αποτελεσματική κατανομή των πόρων σε παγκόσμιο επίπεδο, αν και μπορεί επίσης να οδηγήσει σε ανεπιθύμητες συνέπειες - όπως ένα hyper-tokenization της κοινωνίας και μια δυνητικά καταστροφική συγκέντρωση ισχύος στις μεγάλες παγκόσμιες πλατφόρμες. Επομένως, τα συνολικά οφέλη και τα μειονεκτήματα του blockchain πρέπει να συμπεριληφθούν, για την εύρεση μιας ισορροπίας μεταξύ της ανάγκης για την καινοτομία, την οικονομική ανάπτυξη και την κοινωνική βιωσιμότητα.

Η μέλλουσα παγκόσμια οικονομία θα κινηθεί πάνω σε αυτήν την τεχνολογία, με την οποία οποιοδήποτε άτομο με πρόσβαση στο ίντερνετ θα έχει πρόσβαση σε blockchain συναλλαγές. Third party οργανισμοί μπορεί πλέον να μην είναι αναγκαίοι για την εγκυρότητα μίας συναλλαγής.



Εικόνα 1.1

Οι χρήσεις του blockchain θα είναι άπειρες, ειδικοί προβλέπουν ότι σε λιγότερα από 10 χρόνια το blockchain θα χρησιμοποιείται για την συλλογή των φόρων από τους πολίτες. Θα είναι πιο εύκολο ακόμα η άμεση μεταφορά των χρημάτων μεταξύ δύο ανθρώπων οπουδήποτε πάνω στον πλανήτη όπου η πρόσβαση σε τράπεζες είναι δύσκολη. Οι οικονομικές απάτες θα μειωθούν σημαντικά εφόσον κάθε συναλλαγή θα καταγράφεται σε ένα δημόσιο και κατανεμημένο καθολικό (ledger) το οποίο θα είναι προσβάσιμο σε οποιονδήποτε με σύνδεση στο ίντερνετ.

Αυτό με λίγα λόγια σημαίνει ότι όλη η γραφειοκρατία και τα πεπαλαιωμένα συστήματα, φυσικά και ψηφιακά, αλλά και το προσωπικό που τα υποστηρίζει σε λίγο καιρό δεν θα έχουν λόγο ύπαρξης, με τις συναλλαγές και πιστοποιήσεις να γίνονται μέσα σε λίγα λεπτά με μεγάλη εξοικονόμηση πόρων και χρημάτων.

Οι εφαρμογές πολλές: Ψηφιακά νομίσματα, ταυτότητες, κτηματολόγιο, συμβόλαια, κλειδαριές, διακρατικό εμπόριο, χρηματοπιστωτικές συναλλαγές και στο μέλλον ακόμα και αυτόνομες επιχειρηματικές λειτουργίες μπορούν να υλοποιηθούν αλλάζοντας τα πάντα.

Το blockchain θα είναι μία παγκόσμια αποκεντρωμένη πηγή εμπιστοσύνης. Νέα δίκτυα θα εξελιχθούν για τις ανάγκες τις κοινωνίας τα οποία θα είναι πιο οικονομικά και πιο ασφαλή.

1.1 Τι είναι το blockchain - Ορισμός

Το blockchain είναι ένα υπολογιστικό μοντέλο το οποίο εμφανίστηκε για πρώτη φορά με το πρωτόκολλο Bitcoin το 2008. Το blockchain πρόκειται για μία σειρά καταχωρίσεων που αφορούν συναλλαγές, σε ένα δημόσιο σημειωματάριο (ledger) σε ένα δημόσιο ή ιδιωτικό peer-to-peer δίκτυο. Κάθε καινούρια

ομάδα καταχωρήσεων δηλαδή ένα «block» συνδέεται με τα προηγούμενα, δημιουργώντας μία αλυσίδα καταχωρίσεων από την πρώτη συναλλαγή έως την τρέχουσα δημιουργώντας το «blockchain». Ένα σύνολο των εγκεκριμένων συναλλαγών ομαδοποιείται σε ένα μπλοκ, το οποίο αποστέλλεται σε όλους τους κόμβους του δικτύου. Αυτοί με τη σειρά τους επικυρώνουν το νέο μπλοκ.

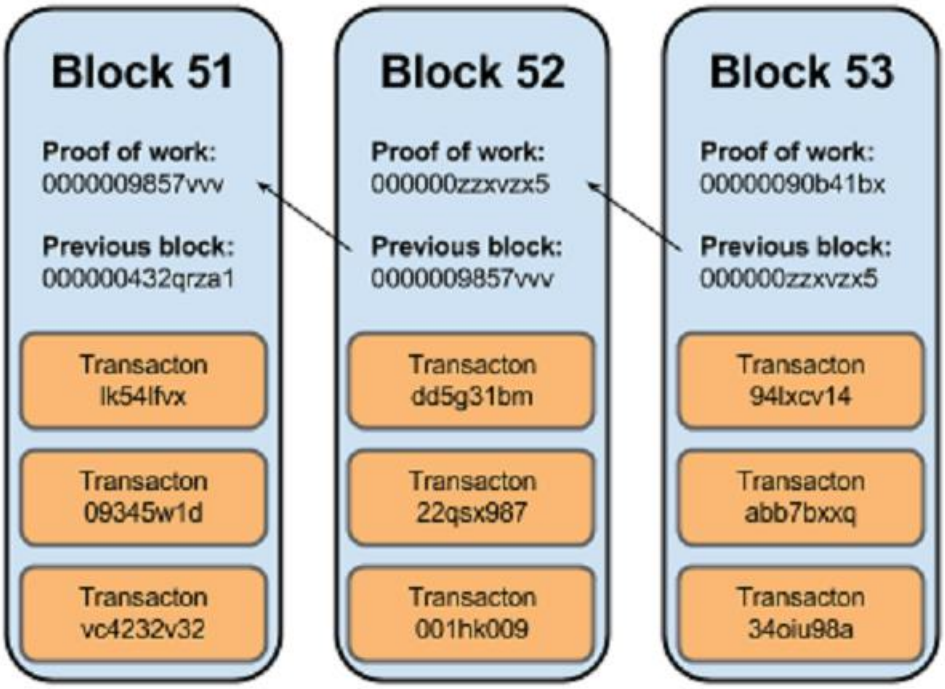
Κατά συνέπεια, το blockchain λειτουργεί ως μια ενιαία πηγή αλήθειας και τα μέλη σε ένα δίκτυο blockchain μπορούν να δουν μόνο αυτές τις συναλλαγές που σχετίζονται με αυτά.

1.2 Πως λειτουργεί το blockchain

Η δομή των δεδομένων στο blockchain είναι μία ταξινομημένη back-linked λίστα των μπλοκ των συναλλαγών. Το blockchain μπορεί να αποθηκευτεί ως ένα απλό αρχείο, ή σε μια απλή βάση δεδομένων. Π.χ. το Bitcoin αποθηκεύει τα blockchain δεδομένα χρησιμοποιώντας τη βάση δεδομένων LevelDB της Google. Τα μπλοκ συνδέονται προς τα "πίσω", με το κάθε ένα να έχει αναφορά στο προηγούμενο μπλοκ στην αλυσίδα. Το blockchain συχνά εμφανίζεται σαν μια κάθετη στοίβα, με τα μπλοκ σε επίπεδα το ένα πάνω από το άλλο και το πρώτο μπλοκ που εξυπηρετεί ως θεμέλιο της στοίβας. Η οπτικοποίηση των μπλοκ να στοιβάζονται το ένα πάνω στο άλλο έχει σαν αποτέλεσμα τη χρήση όρων όπως "ύψος" για να αναφερθούμε στην απόσταση από το πρώτο μπλοκ και "κορυφή" ή "άκρη" για να ανατρέξουμε στο πιο πρόσφατα προστιθέμενο μπλοκ.

Κάθε μπλοκ εντός του blockchain προσδιορίζεται από ένα hash το οποίο παράγεται με τη χρήση του SHA256 αλγόριθμου κρυπτογράφησης στην κεφαλίδα του μπλοκ. Κάθε μπλοκ αναφέρεται επίσης στο προηγούμενο μπλοκ, γνωστή ως γονέας

μπλοκ (parent block), μέσα από το πεδίο "προηγούμενο μπλοκ hash" στην κεφαλή του μπλοκ. Με άλλα λόγια, κάθε μπλοκ περιέχει το hash του γονέα μέσα στη δική του επικεφαλίδα . Η ακολουθία των hash συνδέει κάθε μπλοκ προς τον γονέα του, δημιουργώντας έτσι μία αλυσίδα η οποία πηγαίνει πίσω σε όλη τη διαδρομή μέχρι το πρώτο μπλοκ που δημιουργήθηκε ποτέ.



Εικόνα 1.2

Παρά το γεγονός ότι ένα μπλοκ έχει ένα μόνο γονέα, μπορεί να έχει προσωρινά πολλαπλά παιδιά. Κάθε ένα από τα παιδιά αναφέρεται στο ίδιο μπλοκ ως γωνέα και περιέχει το ίδιο γονικό hash στο πεδίο «προηγούμενο μπλοκ hash». Πολλαπλά παιδιά μπορούν να προκύψουν κατά τη διάρκεια ενός αποκαλούμενου ως «blockchain fork», μια προσωρινή κατάσταση που εμφανίζεται όταν τα διάφορα μπλοκ που ανακαλύπτονται

σχεδόν ταυτόχρονα από διαφορετικούς miners. Τελικά, μόνο ένα παιδί μπλοκ γίνεται μέρος του blockchain και το blockchain έχει επιλυθεί. Ακόμα κι αν ένα μπλοκ έχει περισσότερα από ένα παιδιά, κάθε μπλοκ μπορεί να έχει μόνο ένα γονέα. Αυτό οφείλεται στο γεγονός ότι κάθε μπλοκ έχει ένα μόνο πεδίο «προηγούμενο μπλοκ hash» το οποίο αναφέρεται στον μοναδικό γονέα του.

Το πεδίο «hash προηγούμενου μπλοκ" είναι μέσα στην κεφαλίδα του μπλοκ και με τον τρόπο αυτό επηρεάζει το hash του τρέχοντος μπλοκ. Η ταυτότητα του παιδιού αλλάζει εάν αλλάξει η ταυτότητα του γονέα. Όταν ο γονέας έχει τροποποιηθεί με οποιονδήποτε τρόπο, αλλαγές πραγματοποιούνται στο hash του γονέα. Το αλλαγμένο hash του γονέα απαιτεί μια αλλαγή στο «hash προηγούμενου μπλοκ" δείκτη του παιδιού. Αυτό με τη σειρά του προκαλεί το hash του παιδιού να αλλάξει, το οποίο απαιτεί μια αλλαγή στο δείκτη του εγγονιού, το οποίο με τη σειρά του αλλάζει το εγγόνι, και ούτω καθεξής. Αυτό το αποτέλεσμα αλληλουχίας εξασφαλίζει ότι μόλις ένα μπλοκ έχει πολλές γενεές να το ακολουθούν, δεν μπορεί να αλλάξει χωρίς να αναγκάζει τον επανυπολογισμό όλων των μεταγενέστερων μπλοκ. Επειδή ένας τέτοιος επανυπολογισμός θα απαιτούσε τεράστιους υπολογισμούς, η ύπαρξη μιας μακράς αλυσίδας μπλοκ κάνει την βαθιά ιστορία του blockchain αμετάβλητη, κάτι το οποίο αποτελεί βασικό χαρακτηριστικό της ασφάλειας του blockchain.

Όταν κάποιος θέλει να προσθέσει μια συναλλαγή στην αλυσίδα, όλοι οι συμμετέχοντες στο δίκτυο θα την επικυρώσουν. Αυτό γίνεται με την εφαρμογή ενός αλγορίθμου στην συναλλαγή για την επαλήθευση της εγκυρότητας της. Τι ακριβώς νοείται ως "έγκυρο" ορίζεται από το σύστημα blockchain και μπορεί να διαφέρει μεταξύ των συστημάτων. Στη συνέχεια, εναπόκειται

στην πλειοψηφία των συμμετεχόντων να συμφωνούν ότι η συναλλαγή είναι έγκυρη.

Ένα σύνολο των εγκεκριμένων συναλλαγών στη συνέχεια ομαδοποιείται σε ένα μπλοκ, το οποίο αποστέλλεται σε όλους τους κόμβους του δικτύου. Αυτοί με τη σειρά τους επικυρώνουν το νέο μπλοκ. Κάθε διαδοχικό μπλοκ περιέχει ένα hash, το οποίο είναι ένα μοναδικό δακτυλικό αποτύπωμα, του προηγούμενου μπλοκ.

Κατ' αυτό τον τρόπο, το blockchain λειτουργεί ως ένα αποκεντρωμένο (decentralized) λογιστικό καθολικό, το οποίο είναι κοινό για όλους τους συμμετέχοντες, μιας και όλοι οι εμπλεκόμενοι αποθηκεύουν ένα αντίγραφό του, κάτι που εξασφαλίζει την ασφάλεια και η διαφάνεια των συναλλαγών.

Η ειδοποιός διαφορά -αναφορικά με την προστασία- προκύπτει από το γεγονός ότι δεν είναι πλέον απαραίτητη η ύπαρξη μιας ενδιάμεσης «έμπιστης» αρχής (πχ. μιας τράπεζας), ενώ η εμπιστοσύνη των συναλλασσόμενων μερών βασίζεται σε αλγοριθμική επιβεβαίωση.

Ένας τρόπος για να σκεφτεί κάποιος το blockchain είναι σαν στρώσεις σε ένα γεωλογικό σχηματισμό ή ένα δείγμα από πυρήνα παγετώνα. Τα επιφανειακά στρώματα μπορεί να αλλάξουν με τις εποχές, ή ακόμα και να αφαιρεθούν πριν να έχουν ακόμα χρόνο για να εγκατασταθούν. Αλλά από τη στιγμή που θα πάμε μερικά μέτρα πιο βαθιά, τα γεωλογικά στρώματα γίνονται όλο και πιο σταθερά. Μέχρι τη στιγμή που θα δούμε μερικές εκατοντάδες μέτρα πιο κάτω, που ψάχνετε σε ένα στιγμιότυπο του παρελθόντος που έχει παραμείνει αδιατάρακτο επί χιλιετίες ή και εκατομμύρια χρόνια. Στο blockchain, τα πιο πρόσφατα μπλοκ μπορεί να αναθεωρηθούν αν υπάρχει επανυπολογισμός της αλυσίδας ο οποίος οφείλεται σε ένα blockchain fork. Τα έξι πιο πρόσφατα μπλοκ είναι σαν μερικά μέτρα κάτω από τη γη. Αλλά μόλις κάποιος κοιτάξει

βαθύτερα στο blockchain, πέραν των έξι μπλοκ, τα μπλοκ είναι όλο και λιγότερο πιθανό να αλλάξει. Λίγες χιλιάδες μπλοκ πίσω (ένα μήνα) και το blockchain είναι πλέον εγκατεστημένο και ποτέ δεν θα αλλάξει.

1.3 Τύποι του blockchain

Υπάρχουν τρεις κύριοι τύποι blockchains:

- Σε δημόσια blockchain (αποκαλούμενα επίσης permition-less), ο καθένας μπορεί να διαβάσει ή να γράψει δεδομένα στο blockchain. Ορισμένα δημόσια blockchains περιορίζουν την πρόσβαση σε ανάγνωση ή γραφή. Το Bitcoin για παράδειγμα, χρησιμοποιεί μια προσέγγιση όπου ο καθένας μπορεί να γράψει ή να διαβάσει χρησιμοποιώντας το κατάλληλο software. Οποιοσδήποτε στον κόσμο μπορεί να διαβάσει και να στείλει συναλλαγές, να συμμετάσχει στη διαδικασία συναίνεσης, δηλαδή τη διαδικασία για τον προσδιορισμό ποια μπλοκ θα προστεθούν στην αλυσίδα. Τα δημόσια blockchains είναι ανοικτού κώδικα και ο καθένας μπορεί να είναι μέρος τους. Οποιοσδήποτε μπορεί να εξερευνήσει το blockchain, να στείλει συναλλαγές ή συμβάσεις. Παραδείγματα δημόσιων blockchain είναι το Bitcoin και το Ethereum.

- Σε ιδιωτικά blockchain, όλοι οι συμμετέχοντες είναι γνωστοί εκ των προτέρων και αξιόπιστοι. Τα δικαιώματα για γραφή διατηρούνται κεντρικά σε έναν οργανισμό. Τα δικαιώματα για ανάγνωση μπορεί να είναι δημόσια ή περιορίζονται σε μία συγκεκριμένη έκταση. Είναι πιθανό εφαρμογές να περιλαμβάνουν τη διαχείριση βάσεων

δεδομένων, τον έλεγχο, και πολλά άλλα να είναι εσωτερικά σε μία εταιρεία και έτσι δημόσια αναγνωσιμότητα μπορεί να μην είναι καθόλου απαραίτητη.

- Ένα consortium blockchain είναι ένα blockchain όπου η διαδικασία συναίνεσης ελέγχεται από ένα προ-επιλεγμένο σύνολο των κόμβων. Για παράδειγμα, θα μπορούσε κανείς να φανταστεί μια κοινοπραξία 15 χρηματοπιστωτικών ιδρυμάτων, καθένα από τα οποία διαθέτει ένα κόμβο και των οποίων οι 10 πρέπει να υπογράψουν κάθε μπλοκ έτσι ώστε το μπλοκ να είναι έγκυρο. Το δικαίωμα ανάγνωσης του blockchain μπορεί να είναι δημόσιο ή να περιορίζεται στους συμμετέχοντες, το οποίο επιτρέπει σε μέλη από το δημόσιο κοινό να κάνουν έναν περιορισμένο αριθμό ερωτημάτων και να πάρουν πίσω κρυπτογραφικές αποδείξεις ορισμένων τμημάτων του blockchain. Αυτά τα blockchains μπορεί να θεωρηθούν «μερικώς αποκεντρωμένα».

Ένα blockchain αποτελείται από δύο τύπους στοιχείων:

- Οι συναλλαγές είναι οι ενέργειες που δημιουργήθηκαν από τους συμμετέχοντες στο σύστημα.

- Τα μπλοκ καταγράφουν τις συναλλαγές και βεβαιώνουν ότι είναι στη σωστή σειρά και δεν έχουν αλλοιωθεί. Τα μπλοκ καταγράφουν επίσης μια σφραγίδα χρόνου, όταν προστίθενται συναλλαγές.

Η Blockchain τεχνολογία έχει γίνει ένα από τα πιο trending θέματα στον κόσμο των ηλεκτρονικών υπολογιστών τα

τελευταία δύο χρόνια. Το κοινό έχει έρθει κατά κύριο λόγο σε επαφή με τα blockchains μέσω της χρήσης των bitcoins, αλλά υπάρχουν περισσότερα οφέλη από τα blockchains παρά από τα ψηφιακά νομίσματα.

1.4 Οφέλη του blockchain

Ενώ το κεντρικοποιημένο μοντέλο έχει λειτουργήσει τέλεια τις τελευταίες δεκαετίες, θα γίνει προβληματικό όταν ο αριθμός των κόμβων του δικτύου μεγαλώσει σε εκατομμύρια, δημιουργώντας δισεκατομμύρια συναλλαγές, διότι θα αυξηθούν εκθετικά οι υπολογιστικές απαιτήσεις και κατ' επέκταση το κόστος.

Οι διακομιστές μπορούν επίσης να γίνουν ένα σημείο κυκλοφοριακής συμφόρησης και ένα ενιαίο σημείο της αποτυχίας, η οποία θα κάνει τα δίκτυα IoT (Internet of Things) ευάλωτα σε Denial of Service (DoS / DDoS) επιθέσεις, όπου στοχεύονται οι διακομιστές πλημυρίζοντας τους με κίνηση από επικίνδυνες συσκευές.

Αυτό μπορεί να έχει καθοριστική επίδραση στα IoT οικοσυστήματα, ιδιαίτερα εκείνα που λαμβάνουν πιο ευαίσθητες εργασίες.

Επιπλέον, κεντρικοποιημένα δίκτυα θα είναι δύσκολο να εγκατασταθούν σε πολλές βιομηχανικές περιοχές, όπως τα μεγάλα αγροκτήματα, όπου οι κόμβοι IoT θα επεκταθούν σε μεγάλες περιοχές με χαμηλές ταχύτητες σύνδεσης.

Βασισμένο σε κρυπτογραφικά πρωτόκολλα, το blockchain είναι σε θέση να προστατεύσει αποτελεσματικά την ακεραιότητα, την αυθεντικότητα, την δυνατότητα ελέγχου καθώς και την συνέπεια όλων των συναλλαγών. Μπορεί επίσης να παίξει ένα

σημαντικό ρόλο στο οικοσύστημα IoT, μειώνοντας τον χρόνο και το κόστος κάθε εργασίας, επεξεργάζοντας και αναλύοντας τα δεδομένα, παραμένοντας ιδιωτικά ή ημι-ιδιωτικά.

Σύμφωνα με την αρχή της προστασίας της ιδιωτικής ζωής, το blockchain ελαχιστοποιεί την ανάγκη για κανονισμούς και καθιστά επίσης δυνατό να ενσωματωθούν νόμοι στον κώδικα, ώστε να μπορούν να εκτελούνται αυτόματα.

Το blockchain είναι επομένως πιο λειτουργικό από άλλες σύνθετες Private-Enhancing τεχνολογίες (PET) , οι οποίες μπορεί να αποδειχθούν να είναι ανέφικτες ή ανεπαρκής.

Η Blockchain τεχνολογία θα επιτρέψει επίσης τη δημιουργία ασφαλών δικτύων πλέγματος, όπου οι συσκευές IoT θα διασυνδεθούν με αξιόπιστο τρόπο, αποφεύγοντας τις απειλές, όπως η πλαστογράφηση μίας συσκευής και κλοπή στοιχείων ταυτότητας.

Με κάθε νόμιμο κόμβο να έχει καταχωρηθεί στο blockchain, οι συσκευές θα μπορούν εύκολα να εντοπίζουν και να πραγματοποιούν αμοιβαίο έλεγχο ταυτότητας, χωρίς την ανάγκη πιστοποίηση από κάποιο κεντρικό διακομιστή, καθώς και το δίκτυο θα είναι επεκτάσιμο για να υποστηρίξει τα δισεκατομμύρια των συσκευών χωρίς την ανάγκη για πρόσθετους πόρους.

1.5 Προβλήματα και προκλήσεις

Υπάρχουν πολλά εμπόδια που παρεμποδίζουν την ευρεία υιοθέτηση του Blockchain. Το κόστος της ενέργειας, η αποθήκευση των δεδομένων και ο όγκος των συναλλαγών είναι οι τρεις μεγαλύτερες ανησυχίες. Σύμφωνα με το Ινστιτούτο Διεθνούς Έκθεσης Οικονομικών, «η συνδυασμένη ηλεκτρική

κατανάλωση των [blockchain] υπολογιστών είναι αρκετή για την ηλεκτροδότηση περίπου 135.000 αμερικανικών νοικοκυριών." Το ποσοστό αυτό αντιπροσωπεύει μόνο υπάρχοντες υπολογιστές blockchain και δεν υπολογίζεται η μαζική ανάπτυξη των Blockchain πλατφόρμων στο εγγύς μέλλον.

Η των αποθήκευση δεδομένων είναι ένα βασικό εμπόδιο για την επεκτασιμότητα του Blockchain. Σε ένα πλήρως αποκεντρωμένο, δημόσιο Blockchain, το μέγεθος ενός συγκεκριμένου μπλοκ γίνεται όλο και πιο μεγάλο και δαπανηρό να αποθηκεύσει δεδομένα. Πολλοί ειδικοί ελπίζουν με την άνοδο της συμπίεσης των δεδομένων να μειωθεί σημαντικά το κόστος της αποθήκευσης δεδομένων.

Μια ενδιαφέρουσα πρόταση είναι η χρήση των Merkle Trees για τη μείωση του πλεονάσματος στην επαλήθευσης της συναλλαγής, απαιτώντας να κατέβει μόνο μια μερική μερίδα του συνόλου της αλυσίδας για να επαληθευτεί η συναλλαγή. Επίσης, το ίδιο το μέγεθος του μπλοκ είναι ένα σημαντικό εμπόδιο για την αύξηση του μεγέθους του όγκου συναλλαγών.

1.6 Σύνοψη πλεονεκτημάτων-μειονεκτημάτων

Πλεονεκτήματα

- Αποδιαμεσολάβηση
  Δύο μέρη είναι σε θέση να κάνουν μια συναλλαγή χωρίς την επίβλεψη ή την διαμεσολάβηση ενός τρίτου μέρους.

- Εξουσιοδοτημένοι χρήστες
  Οι χρήστες έχουν τον έλεγχο όλων των πληροφοριών και των συναλλαγών τους.

- Υψηλής ποιότητας δεδομένα
  Τα blockchain δεδομένα είναι πλήρης, συνεπής, έγκαιρα, ακριβή και ευρέως διαθέσιμα.

- Αντοχή, αξιοπιστία και μακροζωία
  Λόγω των αποκεντρωμένων δικτύων, το blockchain δεν έχει ένα κεντρικό σημείο αποτυχίας και είναι σε καλύτερη θέση να αντέξει σε κακόβουλες επιθέσεις.

- Ακεραιότητα της διαδικασίας
  Οι χρήστες μπορούν να εμπιστευθούν ότι οι συναλλαγές θα εκτελούνται όπως ακριβώς ορίζουν οι εντολές του πρωτοκόλλου, καταργώντας την ανάγκη για ένα έμπιστο τρίτο μέρος.

- Διαφάνεια και αμεταβλητότητα
  Οι αλλαγές στο δημόσιο blockchain είναι ορατές στο κοινό από όλα τα μέρη δημιουργώντας διαφάνεια, καθώς και όλες οι συναλλαγές είναι αμετάβλητες, που σημαίνει ότι δεν μπορούν να τροποποιηθούν ή να διαγραφούν.

- Απλούστευση του οικοσυστήματος
  Όλες οι συναλλαγές προστίθενται σε ένα ενιαίο δημόσιο καθολικό (ledger), μειώνοντας έτσι την ακαταστασία και τις επιπλοκές των πολλαπλών ledgers.

- Ταχύτερες συναλλαγές
  Οι συναλλαγές σε μία τράπεζα μπορεί ενδεχομένως να χρειαστούν μέρες για την εκκαθάριση και τελική διευθέτηση, ιδίως εκτός του ωραρίου εργασίας. Οι blockchain συναλλαγές μπορούν να μειώσουν το χρόνο συναλλαγής σε λεπτά και επεξεργάζονται 24/7.

- Χαμηλότερο κόστος συναλλαγών
  Με την εξάλειψη των μεσαζόντων τρίτων και των γενικών εξόδων για την ανταλλαγή περιουσιακών στοιχείων, τα blockchains έχουν τη δυνατότητα να μειώσουν σημαντικά τα έξοδα συναλλαγής.

Μειονεκτήματα

- Εκκολαπτόμενη τεχνολογία
  Η επίλυση των προκλήσεων όπως η ταχύτητα των συναλλαγών, η διαδικασία επαλήθευσης, και τα όρια των δεδομένων θα είναι καθοριστικής σημασίας στο να γίνει το blockchain ευρέως εφαρμόσιμο.

- Αβέβαιο ρυθμιστικό καθεστώς
  Επειδή τα σύγχρονη νομίσματα δημιουργούνται και ελέγχονται από τις εθνικές κυβερνήσεις, το blockchain και το Bitcoin αντιμετωπίζουν εμπόδια στην ευρεία υιοθέτηση από τα προϋπάρχοντα χρηματοπιστωτικά ιδρύματα, εφόσον το καθεστώς ρύθμιση της κυβέρνησης του παραμένει ακαθόριστο.

- Μεγάλη κατανάλωση ενέργειας
  Οι miners του blockchain για το δικτύο Bitcoin επιχειρούν 450.000 τρισεκατομμύρια λύσεις ανά δευτερόλεπτο για την επικύρωση των συναλλαγών, χρησιμοποιώντας σημαντικές ποσότητες ενέργειας του υπολογιστή.

- Έλεγχος, ασφάλεια και προστασία της ιδιωτικότητας
  Ενώ υπάρχουν λύσεις, συμπεριλαμβανομένων των ιδιωτικών blockchains και ισχυρή κρυπτογράφηση, εξακολουθούν να υπάρχουν ανησυχίες στον κυβερνοχώρο για την ασφάλεια που πρέπει να αντιμετωπιστούν πριν το ευρύ κοινό αναθέσει τα προσωπικά του δεδομένα σε ένα blockchain.

- Ανησυχίες ενσωμάτωσης
  Οι blockchain εφαρμογές προσφέρουν λύσεις που απαιτούν σημαντικές αλλαγές, ή την πλήρη αντικατάσταση των υπαρχόντων συστημάτων. Για να πραγματοποιηθούν αυτές οι αλλαγές, οι εταιρείες πρέπει να καταστρώσουν σχέδια στρατηγικής για την μετάβαση.

- Πολιτιστική έκδοση
  Το blockchain αντιπροσωπεύει μια πλήρη στροφή προς ένα αποκεντρωμένο δίκτυο που απαιτεί την συμφωνία των χρηστών και των φορέων της.

- Κόστος
  Το blockchain προσφέρει τεράστια εξοικονόμηση του κόστους, των συναλλαγών και του χρόνου, αλλά το υψηλό αρχικό κόστος κεφαλαίου θα μπορούσε να αποτελέσει αποτρεπτικό παράγοντα.

2. Internet of Things (IoT)

2.1 Ορισμός

Το Internet of Things είναι μία έννοια που αφορά τα αντικείμενα της καθημερινότητας μας, από βιομηχανικές μηχανές μέχρι wearable συσκευές που χρησιμοποιούν ενσωματωμένους αισθητήρες για τη συλλογή δεδομένων και την ανάληψη κάποιας δράσης σε αυτά μέσα σε ένα δίκτυο.

Η ιδέα πίσω από το Internet of Things, είναι η σύνδεση όλων των ηλεκτρονικών συσκευών μεταξύ τους ή/και με το Internet.

Η Cisco σε μία πρόσφατη μελέτη της προβλέπει ότι μέχρι το 2020 θα υπάρχουν πάνω από 50 δισεκατομμύρια συσκευές συνδεδεμένες στο Διαδίκτυο.

Ο όρος που θα μπορούσε να χρησιμοποιηθεί καλύτερα για το IoT είναι «σύνδεση των στοιχείων που μας ενδιαφέρουν στο διαδίκτυο». Με λίγα λόγια το IoT εφαρμόζεται σε ένα εξάρτημα που αποτελείται από αισθητήρες και μία σύνδεση δικτύου. Με αυτόν τρόπο μπορεί κάποιος να ελέγξει, να παρακολουθήσει, να διαχειριστεί ή και να επιβλέψει από την εργασία, το σπίτι, ή το αυτοκίνητο, αντικείμενα που τον ενδιαφέρουν.

Ο όρος “Internet of Things” (IoT ή αλλιώς Διαδίκτυο των Πραγμάτων) επινοήθηκε στα τέλη της δεκαετίας του 1990 από τον επιχειρηματία Kevin Ashton , ο οποίος είναι ένας από τους ιδρυτές του Auto-ID Center στο MIT. Ο Ashton ήταν μέρος μιας ομάδας που ανακάλυψε τον τρόπο να συνδέσει τα αντικείμενα με το διαδίκτυο μέσω μιας ετικέτας RFID. Έχει δηλώσει ότι χρησιμοποίησε πρώτη φορά τη φράση “Internet of Things” σε μια παρουσίαση που έκανε το 1999 και ο όρος αυτός καθιερώθηκε από τότε.

Το Internet όπως το γνωρίζουμε αυτή τη στιγμή αποτελεί τη ραχοκοκαλιά του Internet of Things, ωστόσο δεν είναι απαραίτητο οι συσκευές να έχουν απευθείας πρόσβαση σε

αυτό. Για παράδειγμα, ένα fitness band συλλέγει αμέτρητα δεδομένα για τη φυσική σου κατάσταση και την υγεία σου, τα μεταδίδει στο smartphone ή το tablet σου μέσω Bluetooth και στη συνέχει αυτά περνάνε online, στην cloud υπηρεσία που χρησιμοποιείς για την καταγραφή τους. Πρακτικά, δηλαδή, μιλάμε για ένα περιβάλλον συλλογής δεδομένων από οποιαδήποτε ηλεκτρονική συσκευή ή μικροσκοπικό αισθητήρα υπάρχει γύρω μας.

Κάπως έτσι λειτουργεί ένα κτίριο που χρησιμοποιεί αισθητήρες (sensors) για την αυτόματη ρύθμιση της θέρμανσης ή του φωτισμού. Άλλο παράδειγμα είναι ο ένας εξοπλισμός παραγωγής που προειδοποιεί το προσωπικό συντήρησης για μία επικείμενη βλάβη.

Με απλά λόγια το Internet of Things είναι το τεχνολογικό μέλλον που θα κάνει τη ζωή μας πιο εύκολη.

Εικόνα 2.1

2.2 Οφέλη του Internet of Things (IoT)

Είναι πολλά τα οφέλη που μπορούμε να αποκομίσουμε από την ανάλυση των data streams μεταξύ διαφόρων συσκευών. Εδώ είναι μερικά παραδείγματα των επιπτώσεων του Internet of Things σε διάφορους κλάδους:

- Έξυπνες λύσεις μεταφοράς επιταχύνουν την ροή της κυκλοφορίας , μειώνουν την κατανάλωση καυσίμων.
- Έξυπνα ηλεκτρικά δίκτυα (smart electric grids) συνδέουν πιο αποτελεσματικά ανανεώσιμες πηγές ενέργειας, βελτιώνουν την αξιοπιστία του συστήματος και χρεώνουν τους καταναλωτές με βάση μικρότερες προσαυξήσεις.
- Μηχανές αισθητήρων παρακολούθησης κάνουν διαγνώσεις και προβλέπουν θέματα συντήρησης που εκκρεμούν, βραχυπρόθεσμα stock-out αποθεμάτων, και θέτουν ακόμα και προτεραιότητες στα προγράμματα του προσωπικού που είναι υπεύθυνο για τις επισκευές για να καλύψουν αποτελεσματικότερα τις ανάγκες επισκευής εξοπλισμού.
- Data-driven συστήματα, χτισμένα στις υποδομές των «έξυπνων πόλεων» καθιστούν ευκολότερο για τους δήμους να «τρέχουν» τις διαδικασίες διαχείρισης αποθεμάτων, την επιβολή του νόμου και άλλα προγράμματα πιο αποτελεσματικά.

Υπάρχουν όμως και πολλά οφέλη από τη χρήση του IoT και σε προσωπικό επίπεδο. Συνδεδεμένες συσκευές χαράζουν τη δική τους πορεία τόσο στον κόσμο των επιχειρήσεων όσο και στη μαζική αγορά:

- Τελειώνει το γάλα στο ψυγείο. Αυτόματη λήψη υπενθύμισης στο κινητό από το ψυγείο για αγορά ενώ ο χρήστης είναι εκτός σπιτιού.
- Το σύστημα ασφαλείας του σπιτιού, επιτρέπει τον απομακρυσμένο έλεγχο από απόσταση των κλειδαριών και του θερμοστάτη, ή ρυθμίζει το κλιματιστικό ώστε να δροσίσει το σπίτι ή να ανοίξει τα παράθυρα.

2.3 Κίνδυνοι και προκλήσεις του IoT

Η μεγαλύτερη πρόκληση που θα κληθούν να αντιμετωπίσουν οι εταιρείες, είναι η ασφάλεια. Τόσο του τεράστιου δικτύου συνδεδεμένων «πραγμάτων» που, όπως όλα δείχνουν, θα δημιουργηθεί μέσα στα επόμενα χρόνια, όσο και του όγκου δεδομένων που θα συγκεντρώνεται από αυτά.

Όταν, για παράδειγμα, αισθητήρες συλλέγουν δεδομένα για την κατάσταση της υγείας ενός ανθρώπου, πρέπει να διασφαλιστεί ότι αυτά τα δεδομένα θα παραμένουν ασφαλή και δεν πρόκειται ποτέ να πέσουν στα χέρια των λάθος ανθρώπων. Επιπλέον, με δισεκατομμύρια συνδεδεμένες συσκευές, θα μπορούσε κάποιος να εισβάλει σε ένα δίκτυο μέσω ενός έξυπνου πλυντηρίου που είναι συνδεδεμένο σε αυτό.

Μια άλλη μεγάλη πρόκληση για τις εταιρείες, είναι επίσης η εύρεση αξιόπιστων και ενεργειακά αποδοτικών τρόπων αποθήκευσης και ανάλυσης των δεδομένων που θα παράγουν ταυτόχρονα δισεκατομμύρια συσκευές.

Παράλληλα όμως με την ανάπτυξη του IoT αυξάνεται και η ανάγκη για δυνατότητα διαχείρισης σε πραγματικό χρόνο αυξημένων απαιτήσεων κίνησης δεδομένων. Αυτό γίνεται εύκολα αντιληπτό καθώς θα πρέπει να παρέχεται επαρκές

εύρος ζώνης για να καλύπτει από έναν αισθητήρα τοποθετημένο σε μία πόρτα, μέχρι υψηλής ευκρίνειας βίντεο που θα προέρχεται από μία κάμερα ασφαλείας. Ανάλογες θα είναι φυσικά και οι απαιτήσεις σε επίπεδο κρυπτογράφησης και ασφάλειας των δεδομένων.

Συνολικά, τα επόμενα χρόνια αναμένεται μία έξαρση του αριθμού των συνδεδεμένων συσκευών, των τοποθεσιών που αυτές βρίσκονται και φυσικά των λειτουργιών που αυτές θα εκτελούν. Ενδεικτικά μπορούμε να αναφέρουμε τα μελλοντικά νοσοκομεία: πέρα από τις standalone συνδεδεμένες συσκευές θα υπάρχουν πληθώρα συσκευών οι οποίες θα βρίσκονται συνδεδεμένες με τους σταθμούς παρακολούθησης ασθενών του νοσηλευτικού προσωπικού.

Σε πολλούς από αυτούς τους κινδύνους έρχεται να βοηθήσει το blockchain όπως θα δούμε στο παρακάτω κεφάλαιο.

2.4 Οι προκλήσεις για τους επαγγελματίες της πληροφορικής

Σύμφωνα με το τρέχον επιχειρηματικό μοντέλο, οι εκάστοτε Διευθύνσεις Πληροφορικής συνήθως καλούνται να διαχειριστούν προκλήσεις που σχετίζονται κυρίως με την επιτυχημένη αλλά και την ασφαλή υλοποίηση της διασύνδεσης όλων των συσκευών. Ενδεικτικά, κάποιες από αυτές τις προκλήσεις είναι:

- Η αποτελεσματική αυθεντικοποίηση και η διαχείριση δικαιωμάτων πρόσβασης των χρηστών.
- Απαιτήσεις κανονιστικής συμμόρφωσης και σχετικά αιτήματα αποστολής δεδομένων σε Δημόσιες Αρχές και Εποπτικούς Οργανισμούς.

- Το άγνωστο πολλές φορές κόστος διαχείρισης και αποθήκευσης του τεράστιου όγκου δεδομένων που συλλέγεται, αλλά και της συντήρησης της αναγκαίας δικτυακής υποδομής.
- Έλλειψη εξειδικευμένων γνώσεων και δεξιοτήτων.
- Η ιδιοκτησία των δεδομένων που συλλέγονται και που πολλές φορές ανήκουν σε κάποια άλλη Διεύθυνση εκτός Πληροφορικής (π.χ. Marketing, Ανθρωπίνων Πόρων, Εμπορική κτλ.).

2.5 Τι πιστεύουν οι καταναλωτές

Υπάρχει ένα κενό μεταξύ του τι πιστεύουν οι καταναλωτές και πώς τελικά δρουν. Έτσι, ενώ μπορεί να ανησυχούν για την ασφάλεια των προσωπικών τους δεδομένων, παρόλα αυτά δεν ακολουθούν τις βέλτιστες πρακτικές προστασίας αυτών σε ατομικό επίπεδο. Οι περισσότεροι καταναλωτές ανησυχούν ότι τα δεδομένα τους θα κλαπούν. Παρόλα αυτά συνεχίζουν να ακολουθούν επικίνδυνες πρακτικές, όπως ίδιο λογαριασμό χρήστη και κωδικό πρόσβασης σε μία πληθώρα διαφορετικών εφαρμογών και websites (>50%) ή ακόμη και καταγραφής των κωδικών για να τους θυμούνται. Αυτή η ισορροπία μεταξύ της απαίτησης για περισσότερη ασφάλεια και για προστασία της ιδιωτικότητας και της συνεχούς επιθυμίας για ευκολία χρήσης των συστημάτων θα είναι όλο και πιο έντονη, καθώς θα αυξάνεται ο αριθμός των διασυνδεδεμένων συσκευών. Αν λοιπόν επιβεβαιωθεί η πρόβλεψη της Cisco και υπάρχουν 50 δισεκατομμύρια διασυνδεδεμένες συσκευές το 2020, οι οργανισμοί και οι επιχειρήσεις πρέπει να προσπαθήσουν πολύ ώστε να κερδίσουν την εμπιστοσύνη των καταναλωτών σε ό,τι

αφορά στην προστασία των προσωπικών δεδομένων. Γενικότερα, η μεγαλύτερη ανησυχία των καταναλωτών σύμφωνα με έρευνες, αναδείχθηκε ότι είναι η πιθανότητα κάποιος μη εξουσιοδοτημένος χρήστης (π.χ. hacker) να αποκτήσει πρόσβαση στις συσκευές και στους λογαριασμούς τους και να προχωρήσει σε μία κακόβουλη ενέργεια.

2.6 Τα προβλήματα του κεντρικοποιημένου IoT

Τα σημερινά οικοσυστήματα IoT βασίζονται σε συγκεντρωτικά, με μεσάζοντες μοντέλα επικοινωνίας, αλλιώς γνωστά ως το πρότυπα server - client. Όλες οι συσκευές εντοπίζονται, πιστοποιείται η αυθεντικότητά τους και συνδέονται μέσω cloud servers οι οποίοι υποστηρίζουν τεράστιες δυνατότητες επεξεργασίας και αποθήκευσης. Η σύνδεση μεταξύ των συσκευών θα πρέπει να γίνει αποκλειστικά μέσω του διαδικτύου, ακόμη και αν τυχαίνει να είναι μερικά μέτρα μακριά.

Ενώ το μοντέλο αυτό συνδέει γενικές υπολογιστικές συσκευές για δεκαετίες και θα συνεχίσει να υποστηρίζει μικρής κλίμακας δίκτυα IoT όπως τα βλέπουμε σήμερα, δεν θα είναι σε θέση να ανταποκριθεί στις αυξανόμενες ανάγκες των τεράστιων οικοσυστημάτων IoT του αύριο.

Οι υπάρχουσες λύσεις IoT είναι ακριβές λόγω του υψηλού κόστους των υποδομών και συντήρησης που σχετίζονται με centralized clouds, μεγάλα συμπλέγματα διακομιστών και δικτυακό εξοπλισμό. Το τεράστιο ποσό των επικοινωνιών που θα πρέπει να αντιμετωπιστεί όταν οι συσκευές IoT αυξηθούν σε δεκάδες δισεκατομμύρια θα αυξήσει σημαντικά τις δαπάνες αυτές.

Ακόμα κι αν οι πρωτοφανής οικονομικές και μηχανικές προκλήσεις ξεπεραστούν, οι cloud servers θα παραμείνουν ένα εμπόδιο και το σημείο της βλάβης (point of failure) που μπορεί να διαταράξει το σύνολο του δικτύου.

Επιπλέον, η διαφοροποίηση της ιδιοκτησίας μεταξύ των συσκευών και την υποστήριξη της cloud δομής τους, καθιστά την machine-to-machine (M2M) επικοινωνία δύσκολη. Δεν υπάρχει ενιαία πλατφόρμα που συνδέει όλες τις συσκευές και καμία εγγύηση ότι οι υπηρεσίες cloud που προσφέρονται από διαφορετικούς κατασκευαστές είναι διαλειτουργικές και συμβατές.

2.7 Εφαρμογές του IoT

«Internet of Things» ή αλλιώς και «διαδίκτυο των πραγμάτων», είναι ένας όρος που συζητιέται πολύ στις μέρες μας και τείνει να αποτελέσει την καθημερινότητα εκατομμυρίων ανθρώπων στο άμεσο μέλλον. Πρόκειται για μια ιδέα που αφορά συσκευές, αντικείμενα και γενικότερα «πράγματα», τα οποία είναι συνδεδεμένα αδιαλείπτως μεταξύ τους και μάλιστα σε παγκόσμια εμβέλεια, ενώ έκαναν την εμφάνισή τους με την τεχνολογία RFID. Στη συνέχεια, η έννοια αυτή συνέχισε να επεκτείνεται έως το σημερινό όραμα που προβλέπει μια πληθώρα ετερόκλητων αντικειμένων που αλληλεπιδρούν με το φυσικό περιβάλλον.

Smart Cities

Μια υλοποίηση λοιπόν της παραπάνω αυτής έννοιας είναι οι έξυπνες πόλεις ή αλλιώς και «smart cities». Αφορά τη βελτίωση των πόλεων στην επίλυση προβλημάτων και την καινοτομία με χρήση νοημοσύνης – ευφυΐας, η οποία προσδιορίζεται ανάλογα με τους Πολίτες, τα συνεργαζόμενα συστήματα, τη γενικότερη ψηφιακή υποδομή και τα εργαλεία που μια κοινότητα είναι σε θέση να προσφέρει στους Πολίτες της. Μια έξυπνη πόλη επομένως, στηρίζεται σε έξι πλαίσια κυρίως βασικών αξόνων, που έχουν να κάνουν με την περιφερειακή ανταγωνιστικότητα, τις μεταφορές, την οικονομία, τους φυσικούς πόρους, το κεφάλαιο τόσο το ανθρώπινο όσο και το κοινωνικό, καθώς και την ποιότητα ζωής, σε συνδυασμό με τη συμμετοχή των Πολιτών στη διακυβέρνηση των πόλεων.

Smart Lighting

Μια λύση συνεπώς για την υλοποίηση επιμέρους τομέων της έξυπνης πόλης αποτελεί η έξυπνη φωταγώγηση ή αλλιώς και «smart lighting». Η κεντρική ιδέα αναφέρεται στην απομακρυσμένη διαχείριση δημόσιας φωταγώγησης που θα ελέγχεται από συνδυασμό δεδομένων που θα προκύπτουν από αισθητήρες φωτός, βροχής και κίνησης μέσω των οποίων θα ρυθμίζεται το άναμμα και το σβήσιμό τους. Πιθανές επιπρόσθετες δυνατότητες είναι η διαφοροποίηση λειτουργίας του συστήματος σε κατοικημένες περιοχές και σε μη κατοικημένες περιοχές, καθώς επίσης και η προσαρμοσμένη συμπεριφορά του συστήματος σε περιπτώσεις έκτακτης ανάγκης.

Έξυπνο σύστημα

Το «Έξυπνο σύστημα» θα αποτελείται από συσκευές, οι οποίες θα μπορούν να επικοινωνούν μεταξύ τους, στο πλαίσιο δημιουργίας ενός ασύρματου δικτύου αισθητήρων, του οποίου η τοπολογία θα ρυθμίζεται ανάλογα με τις απαιτήσεις της εκάστοτε τοποθεσίας. Επίσης, σε κάθε συσκευή θα υπάρχουν αισθητήρες φωτός, κίνησης και υγρασίας για τη ρύθμιση των λαμπτήρων, ενώ κάθε επιμέρους συσκευή θα συνδέεται, μέσω Zigbee τεχνολογίας σε ένα gateway, όπου και θα γίνεται η αποστολή των δεδομένων που θα συλλέγονται από τους αισθητήρες, προκειμένου να πραγματοποιηθεί η περαιτέρω συγκέντρωσή τους σε βάση δεδομένων, η επεξεργασία – διαχείριση και η παροχή ή η παρουσίαση τους σε κάθε φορέα, αρχή ή φυσικό πρόσωπό που το επιθυμεί.

Οφέλη – Πλεονεκτήματα συστήματος

Οι ευρωπαϊκές χώρες ξοδεύουν πάνω από 10 δισ. ευρώ το χρόνο για τον φωτισμό των δρόμων, ποσό που αντιστοιχεί στο 40% των δαπανών της κάθε χώρας για την ενέργεια. Επιπλέον, η ενέργεια αυτή μεταφράζεται σε 40 εκατ. τόνους εκπομπών διοξειδίου του άνθρακα το χρόνο. Το παρόν σύστημα μειώνει το κόστος ενέργειας και τις εκπομπές διοξειδίου του άνθρακα κατά 80%, ενώ το κόστος συντήρησής του μειώνεται κατά 50%, χάρη στους ενσωματωμένους ασύρματους αισθητήρες που ειδοποιούν το κέντρο ελέγχου όταν ένας λαμπτήρας χρειάζεται επισκευή.

Αντίστοιχου τύπου μικρή έρευνα θα διεξαχθεί και για τη χώρα μας, μέσω της συγκέντρωσης ομοειδών δεδομένων διαφόρων περιοχών της, προκειμένου να δημιουργηθεί η βάση για μια περισσότερο ρεαλιστική αξιολόγηση των πλεονεκτημάτων που αναμένεται να προσφέρει το παρόν σύστημα. Ωστόσο, σε

γενικές γραμμές, αναμένεται ότι θα συμβάλει στην παροχή καλύτερης εξυπηρέτησης και ασφάλειας στους Πολίτες, σε συνδυασμό με μείωση των εκπομπών διοξειδίου του άνθρακα και φυσικά της εξοικονόμησης ενέργειας και κόστους.

Οι ασύρματες επικοινωνίες στην υπηρεσία της Έξυπνης Πόλης

Η ολοένα αυξανόμενη ανάγκη για βελτίωση της ποιότητας ζωής των κατοίκων στα μεγάλα αστικά κέντρα έχει ωθήσει τα τελευταία χρόνια την παγκόσμια κοινότητα στη δημιουργία ενός νέου πεδίου επιστημονικής έρευνας με τον όρο Έξυπνη Πόλη. Βασική περιοχή της έρευνας αυτής αποτελεί το IoT (Internet of Things), το οποίο σύμφωνα με την Gartner περιλαμβάνεται μεταξύ άλλων στις 10 κορυφαίες στρατηγικές τάσεις της τεχνολογίας που θα έχουν σημαντικό αντίκτυπο στις επιχειρήσεις τα επόμενα τρία χρόνια.

Ο όρος IoT περιγράφει την ιδέα ενός κόσμου όπου διάφορες συσκευές και φυσικά αντικείμενα είναι συνδεδεμένα στο διαδίκτυο. Στην εξέλιξη λοιπόν του Internet σε IoT πρωταρχικό ρόλο έχουν οι συσκευές. Κάθε αντικείμενο θα χρησιμοποιεί συστήματα αναγνώρισης ραδιοσυχνοτήτων (RFID) όπως το NFC, το Bluetooth Low Energy (Apple iBeacon, Paypal Beacon) και το WiFi για την ανταλλαγή πληροφοριών.

Οι εφαρμογές που θα μπορούσαν να επωφεληθούν από τη νέα εποχή στην οποία εισέρχεται το διαδίκτυο σχετίζονται με τα έξυπνα κτίρια, τις ευφυείς μεταφορές, την εξοικονόμηση ενέργειας και νερού, τον τουρισμό, τη δημόσια υγεία και ασφάλεια, την εκπαίδευση, τη συμμετοχή των πολιτών στα κοινά.

Στη συνέχεια θα δούμε αναλυτικά μία από τις διαθέσιμες τεχνολογίες στην υπηρεσία της Έξυπνης Πόλης, το NFC.

Περιγραφή της τεχνολογίας NFC

Το NFC (Near field communication) ή αλλιώς «επικοινωνία κοντινού πεδίου» αποτελεί μια ασύρματη τεχνολογία διασυνδεσιμότητας η οποία επιτρέπει την ανταλλαγή πληροφοριών ανάμεσα σε συσκευές όπως smartphones και tablets.

Το NFC είναι ένα ανοικτό πρότυπο και προωθείται κυρίως μέσω του NFC Forum το οποίο δημιουργήθηκε από τις εταιρείες Nokia, Philips και Sony και αριθμεί περισσότερα από 180 μέλη παγκοσμίως.

Η λειτουργία του NFC είναι αρκετά απλή: αρκεί να πλησιάσουν μεταξύ τους δύο συσκευές που υποστηρίζουν NFC για να αλληλοεπιδράσουν και να ανταλλάξουν πληροφορίες σε αντίθεση με τις τεχνολογίες Bluetooth και WiFi στις οποίες προϋπόθεση για την επικοινωνία των συσκευών αποτελεί η εδραίωση της σύνδεσης (ενεργοποίηση-ανακάλυψη-σύζευξη).

Η συχνότητα λειτουργίας της τεχνολογίας NFC είναι τα 13.56 MHz ενώ υποστηρίζει ταχύτητες μεταφοράς δεδομένων έως και 424 kbps. Η απόσταση που μπορούν να αλληλοεπιδράσουν δύο NFC συσκευές θεωρητικά είναι τα 20 εκατοστά αλλά πρακτικά δεν ξεπερνάει τα 4-5 εκατοστά.

Το πλαίσιο λειτουργίας της NFC τεχνολογίας ορίζει δύο τρόπους λειτουργίας:

- Τον ενεργό, κατά τον οποίο και οι δύο συσκευές παράγουν ένα RF σήμα μέσω του οποίου πραγματοποιείται η μεταφορά των δεδομένων, και
- Τον παθητικό, κατά τον οποίο μόνο η μία συσκευή παράγει RF σήμα ενώ η άλλη συσκευή λειτουργεί ως «στόχος» μεταφέροντας τα δεδομένα στην πρώτη χωρίς να τροφοδοτείται από εξωτερική πηγή ενέργειας (π.χ. μπαταρίες).

Η τεχνολογία NFC έχει ενσωματωθεί σε πληθώρα συσκευών από κατασκευαστές όπως Nokia, HTC, Samsung, RIM (Blackberry), Sony και LG οι οποίοι στηρίζουν την τεχνολογία αυτή. Μεταξύ των παραπάνω, έρχονται να προστεθούν και εταιρείες λογισμικού όπως η Google η οποία διαθέτει διεπαφές (API's) που επιτρέπουν στην προγραμματιστική κοινότητα να αναπτύξουν εφαρμογές που στηρίζονται στην τεχνολογία NFC. Σύμφωνα με μελέτη της Berg Insight, πάροχο επιχειρηματικής ευφυΐας για τη βιομηχανία των τηλεπικοινωνιών, η εγκατεστημένη βάση των NFC συσκευών αναμένεται να φτάσει τα 2,1 δισεκατομμύρια μονάδες μέχρι το τέλος του 2017 αποτελώντας έτσι βασική τεχνολογική συνιστώσα όλων των έξυπνων συσκευών.

Ας δούμε όμως ορισμένες εφαρμογές οι οποίες είναι ήδη διαθέσιμες και αξιοποιούν την τεχνολογία NFC.

- Στη λιανική, όπου μια συσκευή NFC μπορεί να λειτουργεί ως scanner διαβάζοντας πληροφορίες από RFID tags (μικρά αυτοκόλλητα τσιπ). Για παράδειγμα θα μπορούσε κάποιος να πλησιάζει τη συσκευή του σε RFID tags τοποθετημένα στην είσοδο ενός πολυκαταστήματος και να λαμβάνει τις προσφορές σε διάφορα είδη. Αντίστοιχα, το ίδιο σενάριο θα μπορούσε να αφορά και ένα σουπερμάρκετ ή ακόμη και ένα εστιατόριο όπου με τον ίδιο τρόπο θα μπορεί ο καταναλωτής να ενημερώνεται για τις τιμές των προϊόντων, τις προσφορές και επιπλέον για τα συστατικά των προϊόντων και τη διατροφική τους αξία.

- Σε οποιουδήποτε είδους πληρωμές, για παράδειγμα στις καθημερινές αγορές μικρής αξίας, αντικαθιστώντας μετρητά (κέρματα), πιστωτικές, χρεωστικές και προπληρωμένες κάρτες. Το 2007 η Visa εισήγαγε μια ανεπαφική (contactless) τεχνολογία πληρωμής την Visa

payWave, που επιτρέπει στους κατόχους Visa να πλησιάζουν την κάρτα τους ή τη φορητή τους συσκευή σε τερματικά πληρωμής για να πραγματοποιήσουν τη συναλλαγή (πληρωμή). Παρόμοια τεχνολογία έχει υλοποιήσει και η Mastercard με το Paypass την οποία διαθέτει η Eurobank στην ελληνική αγορά για την πραγματοποίηση συναλλαγών σε επιλεγμένα καταστήματα (Γερμανός, Cosmote, ZARA, Bershka, Jumbo, Starbucks, κ.α.).

- Ως επαγγελματική κάρτα, για την ανταλλαγή των στοιχείων των επαφών (όνομα, διεύθυνση, τηλέφωνο, email, κτλ.). που είναι καταχωρημένα στις συσκευές μας.

Οι παραπάνω εφαρμογές είναι ενδεικτικές των δυνατοτήτων της τεχνολογίας NFC η οποία μπορεί να απλοποιήσει και να διευκολύνει την καθημερινότητά μας.

3. Blockchain και Internet of Things (IoT)

3.1 Εισαγωγή

Ενώ είναι ακόμα στα πρώτα στάδια ανάπτυξης του, το IoT αποτελείται ως επί το πλείστων από τεχνολογίες που επιτρέπουν τη συλλογή δεδομένων, την απομακρυσμένη παρακολούθηση και τον έλεγχο των συσκευών. Καθώς η τεχνολογία προχωράει, το IoT θα εξελιχθεί σε ένα δίκτυο αυτόνομων συσκευών που μπορούν να αλληλοεπιδρούν μεταξύ τους και με το περιβάλλον τους και να κάνουν έξυπνες αποφάσεις χωρίς ανθρώπινη παρέμβαση.

Εδώ το blockchain μπορεί να λάμψει και να αποτελέσει τη βάση που θα υποστηρίξει μια κοινή οικονομία που βασίζεται στην μηχανή-to-machine (M2M) επικοινωνία.

Η Blockchain τεχνολογία είναι ο συνδετικός κρίκος για να διευθετήσει τις ανησυχίες προστασία της ιδιωτικής ζωής και την αξιοπιστία του IoT. Μπορεί να χρησιμοποιηθεί για την παρακολούθηση δισεκατομμύρια συνδεδεμένων συσκευών, που επιτρέπει την επεξεργασία των συναλλαγών και του συντονισμού μεταξύ των συσκευών. Αυτό επιτρέπει σημαντική εξοικονόμηση για τους κατασκευαστές της βιομηχανίας IoT. Αυτή η αποκεντρωμένη προσέγγιση θα εξαλείψει ενιαία σημεία της αποτυχίας, δημιουργώντας ένα πιο ανθεκτικό οικοσύστημα για συσκευές που θα τρέξουν πάνω σε αυτό. Οι κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούνται στα blockchains θα κάνει τα δεδομένα των καταναλωτών πιο ιδιωτικά και ασφαλή.

Το καθολικό (ledger) του blockchain είναι απαραβίαστο και δεν μπορεί να χειραγωγηθεί από κακόβουλους παράγοντες, διότι δεν υπάρχει σε μία μόνο θέση, και επιθέσεις δεν μπορούν να οργανωθούν επειδή δεν υπάρχει ένα ενιαίο νήμα της επικοινωνίας που μπορεί να υποκλαπεί. Το blockchain καθιστά δυνατή ασφαλή, peer-to-peer ανταλλαγή μηνυμάτων και έχει

ήδη αποδείξει την αξία του στον κόσμο μέσω των υπηρεσιών cryptocurrencies όπως το Bitcoin, παρέχοντας εγγυημένες peer-to-peer υπηρεσίες πληρωμών, χωρίς την ανάγκη για τρίτους.

Οι αποκεντρωμένες και αυτόνομες δυνατότητες του blockchain το κάνει ένα ιδανικό συστατικό για να γίνει ένα θεμελιώδες στοιχείο των IoT λύσεων. Δεν αποτελεί έκπληξη ότι οι τεχνολογίες των επιχειρήσεων IoT έχουν γίνει γρήγορα μια από τις πρώτες εφαρμογές της τεχνολογίας blockchain.

Σε ένα δίκτυο IoT, το blockchain μπορεί να κρατήσει μια αμετάβλητη καταγραφή της ιστορίας των έξυπνων συσκευών. Αυτή η λειτουργία επιτρέπει την αυτόνομη λειτουργία των έξυπνων συσκευών χωρίς την ανάγκη για κεντρική αρχή. Ως αποτέλεσμα, το blockchain ανοίγει την πόρτα σε μια σειρά από σενάρια IoT που ήταν εξαιρετικά δύσκολα, αν όχι αδύνατο να εφαρμοστούν χωρίς αυτό.

Βλέπουμε ήδη πρωτοβουλίες αναδυόμενες σε αυτόν τον τομέα, συμπεριλαμβανομένου του ADEPT (Automated Αποκεντρωμένης P2P Τηλεμετρίας), ένα αποκεντρωμένο σύστημα IoT που δημιουργήθηκε από την IBM και την Samsung, το οποίο επιτρέπει σε δισεκατομμύρια συσκευές την μετάδοση συναλλαγών και την εκτέλεση εργασιών αυτο-συντήρησης.

Η πλατφόρμα έχει δοκιμαστεί σε διάφορα σενάρια, μεταξύ των οποίων ένα που περιλαμβάνει ένα έξυπνο πλυντήριο που μπορεί αυτόματα να παραγγείλει και να πληρώσει για τα απορρυπαντικά με bitcoins ή άλλο νόμισμα και είναι σε θέση να διαπραγματευτεί για την καλύτερη τιμή η οποία βασίζεται στις προτιμήσεις του ιδιοκτήτη του.

Καθώς είναι η ραχοκοκαλιά όλων αυτών των αλληλεπιδράσεων, το blockchain δημιουργεί μία ασφαλής πλατφόρμα που είναι ανεξάρτητη και φροντίζοντας ο καθένας να παίζει δίκαια και ότι δεν υπάρχει ενιαία οντότητα η οποία έχει τον έλεγχο.

Το Blockchain θα επιτρέψει επίσης τη νομισματοποίηση δεδομένων, όπου οι ιδιοκτήτες των συσκευών και αισθητήρων IoT θα μπορούν να μοιραστούν τα IoT δεδομένα που δημιουργούνται σε αντάλλαγμα για μικροπληρωμές σε πραγματικό χρόνο. Το Tilepay, για παράδειγμα, προσφέρει μία ασφαλής, αποκεντρωμένη online αγορά, όπου οι χρήστες μπορούν να κάνουν register τις συσκευές τους στο blockchain και να πωλήσουν τα δεδομένα τους σε πραγματικό χρόνο, σε αντάλλαγμα με ψηφιακό νόμισμα.

3.2 Πλεονεκτήματα αποκεντρωμένων IoT δικτύων

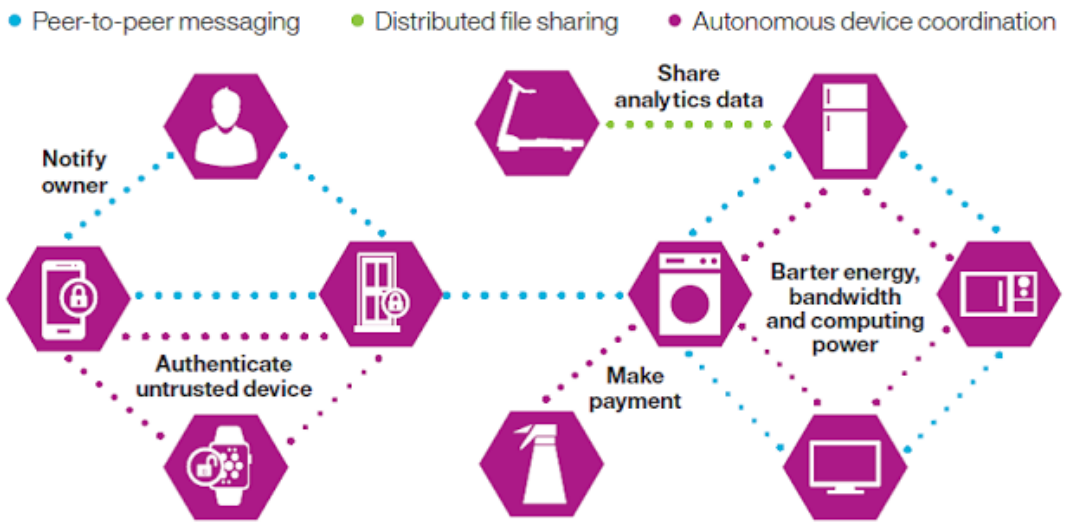
Μια αποκεντρωμένη προσέγγιση για IoT δικτύωση θα έλυνε πολλά από τα παραπάνω ερωτήματα. Υιοθετώντας ένα τυποποιημένο μοντέλο επικοινωνίας peer-to-peer για να επεξεργάζονται τα εκατοντάδες δισεκατομμύρια των συναλλαγών μεταξύ των συσκευών θα μειώσει σημαντικά το κόστος που συνδέεται με την εγκατάσταση και διατήρηση μεγάλων συγκεντρωτικών data centers και θα διανείμει τους υπολογισμούς και τις ανάγκες αποθήκευσης σε όλη τα δισεκατομμύρια των συσκευών που σχηματίζουν τα δίκτυα IoT. Αυτό θα αποτρέψει την αποτυχία σε κάθε ενιαίο κόμβο σε ένα δίκτυο φέρνοντας την κατάρευση όλου του δικτύου.

Ωστόσο, η ίδρυση peer-to-peer επικοινωνιών θα παρουσιάσει το δικό του σύνολο των προκλήσεων, επικεφαλής ανάμεσά τους το θέμα της ασφάλειας. Και όπως όλοι γνωρίζουμε, η ασφάλεια του IoT είναι πολύ περισσότερο από προστασία των ευαίσθητων δεδομένων. Η προτεινόμενη λύση θα πρέπει να διατηρήσει το απόρρητο και την ασφάλεια στα τεράστια δίκτυα IoT και να προσφέρει κάποια μορφή επικύρωσης και της

συναίνεσης για τις συναλλαγές για την πρόληψη της πλαστογράφησης και της κλοπής.

Για να εκτελεστούν οι λειτουργίες των παραδοσιακών λύσεων IoT χωρίς κεντρικό έλεγχο, κάθε αποκεντρωμένη προσέγγιση πρέπει να υποστηρίξει τρεις θεμελιώδεις λειτουργίες:

- Peer-to-peer ανταλλαγή μηνυμάτων
- Κατανεμημένη κοινή χρήση αρχείων
- Αυτόνομο συντονισμό της συσκευής



Εικόνα 3.1

3.3 Πλατφόρμες blockchain για το IoT

3.3.1 Enigma

Ο Guy Zyskind, ο Oz Nathan και ο Alex Sandy Pentland ανέπτυξαν μία πλατφόρμα που ονομάζεται Enigma, ένα δίκτυο peer-to-peer το οποίο βασίζεται σε ένα αποκεντρωμένο σύστημα διαχείρισης των προσωπικών δεδομένων, που επιτρέπει σε διαφορετικά συμβαλλόμενα μέρη την από κοινού την αποθήκευση και τον υπολογισμό των δεδομένων, διατηρώντας παράλληλα τα δεδομένα εντελώς ιδιωτικά. Η πλατφόρμα αυτή εγγυάται την ιδιωτικότητα βάσει σχεδιασμού, συνδυάζοντας αποτελεσματικά blockchain τεχνολογία και off-chain αποθήκευση δεδομένων.

Πως λειτουργεί

Το Enigma είναι μια αποκεντρωμένη πλατφόρμα υπολογισμού με εγγυημένη προστασία της ιδιωτικής ζωής. Στόχος στον σχεδιασμό του enigma ήταν η προστασία της ιδιωτικής ζωής ήδη από τον σχεδιασμό, end-to-end αποκεντρωμένες εφαρμογές, χωρίς καμία ανάγκη για ένα έμπιστο τρίτο μέρος.

Το Enigma είναι ιδιωτικό. Χρησιμοποιώντας ασφαλή multi-party υπολογισμούς (sMPC ή MPC), τα δεδομένα υπολογίζονται με ένα κατανεμημένο τρόπο, χωρίς ένα έμπιστο τρίτο μέρος. Τα δεδομένα είναι χωρισμένα μεταξύ των διαφόρων κόμβων και υπολογίζουν τις λειτουργίες μαζί, χωρίς διαρροή πληροφοριών σε άλλους κόμβους. Συγκεκριμένα, κανένας μεμονωμένος κόμβος δεν έχει πρόσβαση στα δεδομένα στο σύνολό τους. Αντ'αυτού, κάθε κόμβος έχει ένα χωρίς νόημα κομμάτι από αυτό.

Το Enigma είναι επεκτάσιμο. Σε αντίθεση με τα κλασικά blockchains, οι υπολογισμοί και η αποθήκευση δεδομένων δεν αναπαράγονται από κάθε κόμβο στο δίκτυο. Μόνο ένα μικρό υποσύνολο κόμβων εκτελεί τους υπολογισμούς σε διαφορετικά τμήματα των δεδομένων.

Το νέο πρόγραμμα Enigma φέρνει την ικανότητα να γίνονται υπολογισμοί στα δεδομένα, χωρίς υπάρχει πρόσβαση στο ίδια τα ανεπεξέργαστα δεδομένα.

Σήμερα, η ανταλλαγή δεδομένων είναι μια μη αναστρέψιμη διαδικασία, από την στιγμή που θα αποσταλούν, δεν υπάρχει κανένας τρόπος δεν υπάρχει κανένας τρόπος να τα πάρουν πίσω. Η πρόσβαση σε δεδομένα για ασφαλής υπολογισμούς είναι αναστρέψιμη και ελεγχόμενη, αφού κανείς, αλλά μόνο ο αρχικός ιδιοκτήτης(ες) των δεδομένων μπορούν να δουν τα ανεπεξέργαστα δεδομένα. Αυτό αποτελεί μία θεμελιώδη αλλαγή στην τρέχουσες προσεγγίσεις για την ανάλυση των δεδομένων.

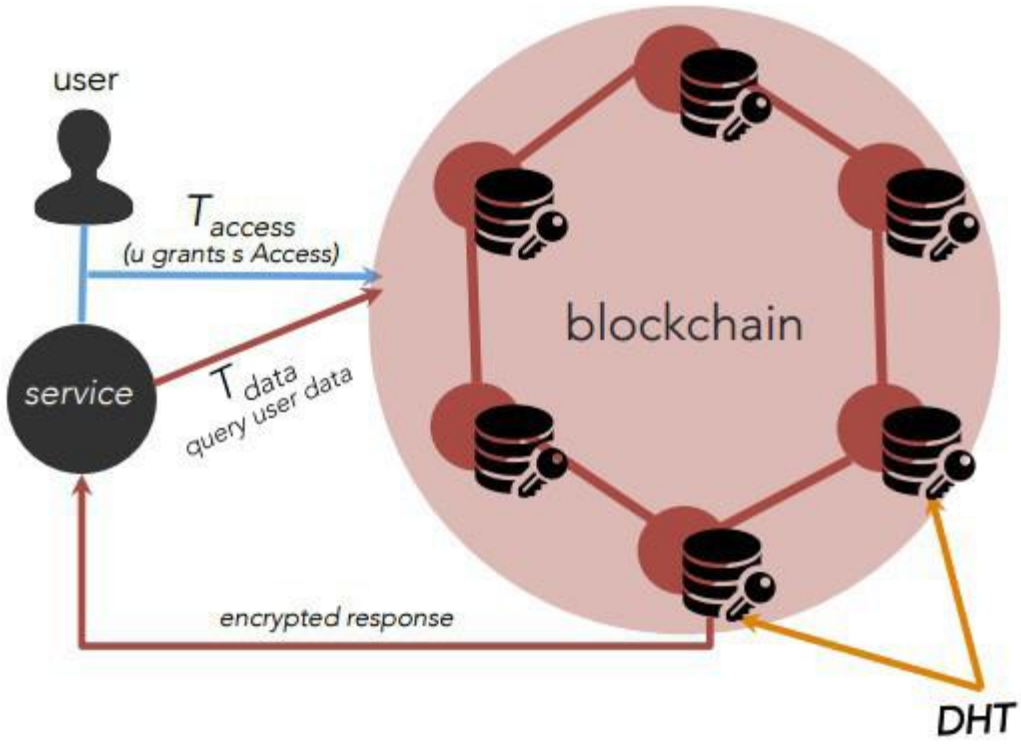
Σχεδιασμός

Το Enigma έχει σχεδιαστεί για να συνδεθεί σε ένα υπάρχον blockchain και να αναθέτει τους πολύπλοκους υπολογισμούς σε ένα δίκτυο off-chain. Όλες οι συναλλαγές διευκολύνονται από το blockchain, το οποίο επιβάλλει ελεγχόμενη πρόσβαση η οποία βασίζεται σε ψηφιακές υπογραφές και προγραμματιζόμενα δικαιώματα.

Ο κώδικας εκτελείται τόσο στο blockchain (δημόσια μέρη) όσο και στο Enigma (ιδιωτικό ή υπολογισμός πολύπλοκων κομματιών). Η εκτέλεση του Enigma εξασφαλίζει την ιδιωτικότητα και την ορθότητα, ενώ ένα blockchain μόνο του

μπορεί να εξασφαλίσει μόνο το τελευταίο. Οι αποδείξεις της ορθής εκτέλεσης αποθηκεύονται στο blockchain και μπορούν να ελεγχθούν. Παρέχεται μια scripting γλώσσα για το σχεδιασμό end-to-end αποκεντρωμένων εφαρμογών που χρησιμοποιούν ιδιωτικές συμβάσεις, οι οποίες είναι παραλλαγές των έξυπνων συμβάσεων που μπορούν να χειριστούν ιδιωτικές πληροφορίες (δηλαδή, η κατάστασή τους δεν είναι αυστηρά δημόσια).

Η εκτέλεση του κώδικα στα blockchains είναι αποκεντρωμένη, αλλά δεν διανέμεται, έτσι ώστε κάθε κόμβος εκτελεί τον ίδιο κώδικα και διατηρεί την ίδια δημόσια κατάσταση. Στο Enigma, η υπολογιστική εργασία διανέμεται αποτελεσματικά σε όλο το δίκτυο. Ένας διερμηνέας διασπά την εκτέλεση του ιδιωτικού συμφωνητικού, όπως απεικονίζεται στο Σχήμα 2.2, με αποτέλεσμα τη βελτίωση του χρόνου εκτέλεσης, διατηρώντας παράλληλα τόσο την ιδιωτικότητα όσο και την επαληθευσιμότητα.



Σχέδιο 3.2 Πηγή Zyskind, Nathan and Pentland, 2015

Κύρια χαρακτηριστικά του Enigma

- Off-blockchain αποθήκευση δεδομένων. Το Enigma προστατεύει την ιδιωτικότητακαι είναι σχεδιασμένο να είναι ανεκτικό σε σφάλματα. Αποτελείται από ένα αποκεντρωμένο off-chain κατανεμημένο hash-table (DHT), μια ιδιωτική αλυσίδα κόμβων προσβάσιμα μέσω του blockchain. Αποθηκεύει αναφορές στα δεδομένα, αλλά όχι τα ίδια τα δεδομένα, τα οποία χωρίζονται και διανέμονται τυχαία. Κανένας κόμβος δεν έχει πρόσβαση σε ολόκληρο το σύνολο των δεδομένων.

- Το blockchain. Λειτουργεί ως μη έμπιστος αυτοματοποιημένος διαχειριστής ελέγχου πρόσβασης. Αναγνωρίζει τους ιδιοκτήτες των δεδομένων, παρέχει ελεγχόμενη πρόσβαση σε άλλους κόμβους και χρησιμεύει ως απαραβίαστη καταγραφή των γεγονότων.

- Επιβολή υπολογισμού της ιδιωτικότητας . Το κατανεμημένο υπολογιστικό μοντέλο Enigma βασίζεται σε ασφαλή Multi Party Computation (MPC). Ερωτήματα δεδομένων και υπολογισμοί υποβάλλονται σε επεξεργασία με ένα εντελώς κατανεμημένο τρόπο, χωρίς την ανάγκη από ένα τρίτο μέρος. Κάθε κόμβος εκτελεί υπολογισμούς πάνω σε διαφορετικά τμήματα των δεδομένων χωρίς την αποκρυπτογράφηση τους πρώτα και χωρίς την διαρροή των δεδομένων στους κόμβους. Το αποτέλεσμα εξασφαλίζεται μέσω ενός επαληθεύσιμου μυστικά μοιραζόμενου σχήματος.

- Off-chain βαριά επεξεργασία. Πολύπλοκοι υπολογισμοί και ανάλυση των δεδομένων γίνονται μόνο εκτός της αλυσίδας. Εφόσον οι συναλλαγές δεν αναπαράγονται σε κάθε κόμβο, το blockchain δεν έχει προβλήματα επεκτασιμότητας. Ο μειωμένος πλεονασμός στην αποθήκευση και στους υπολογισμούς των δεδομένων επιτρέπει ακόμη πιο πολύπλοκους υπολογισμούς.

Οφέλη του Enigma

- Κυριότητα δεδομένων και την ανταμοιβή: Οι χρήστες κατέχουν και ελέγχουν τους προσωπικά δεδομένα; μπορούν επίσης να λάβουν ένα κουπόνι ως αποζημίωση για τη χρήση των δεδομένων τους.

- Διαφάνεια και δυνατότητα ελέγχου: οι χρήστες μπορούν να παρακολουθούν ό, τι τα δεδομένα που συλλέγονται, πώς θα είναι προσβάσιμα και από ποιον.

- Λεπτομερής έλεγχο πρόσβασης: οι χρήστες μπορούν να τροποποιήσουν το σύνολο των δικαιωμάτων και να ανακαλέσουν την πρόσβαση σε δεδομένα που συλλέχθηκαν ανά πάσα στιγμή. Παραδοσιακές mobile εφαρμογές, αντίθετα, απαιτούν χρήστες να συμφωνήσουν σε ένα σύνολο δικαιωμάτων, έτσι ώστε να μπορούν μόνο αυτοί να μπορούν να αποχωρήσουν.

- Πρόσβαση στα δεδομένα και χρήση: οι ενδιαφερόμενα κόμβοι μπορούν να έχουν πρόσβαση και να

χρησιμοποιούν τα δεδομένα, χωρίς να ανησυχούν για την ασφάλεια. Κίνδυνοι που σχετίζονται με την αλυσίδα διαχείρισης δεδομένων θα μειωθούν αναλόγως.

- Ελάχιστη ρυθμιστική παρέμβαση: νόμοι σχετικά με τη συλλογή, την αποθήκευση και την ανταλλαγή ευαίσθητων δεδομένων μπορεί να απλοποιηθεί.

- Ενσωματωμένη ρύθμιση: νομικό πλαίσιο μπορεί να ενσωματωθεί και να εκτελείται αυτόματα μέσω του blockchain κώδικα.

- Παροχή νομικών αποδεικτικών στοιχείων: το blockchain εξασφαλίζει την ακεραιότητα των δεδομένων και παρέχει ένα απαραβίαστο log των γεγονότων, ενεργώντας ως νομική απόδειξη για την πρόσβαση και την αποθήκευση δεδομένων.

3.3.2 IOTA-TANGLE

Το IOTA είναι μια cryptocurrency πλατφόρμα η οποία δημιουργήθηκε από τον David Sønstebø και αναπτύχθηκε ειδικά για μικρο-πληρωμές και στοχεύει στο να γίνει ένα πρότυπο σύστημα διακανονισμού του IoT και της μηχανής-προς-μηχανή (M2M) οικονομίας.

Εκτός από τις επιχειρήσεις-προς-επιχειρήσεις εφαρμογές, το IOTA μπορεί επίσης να χρησιμοποιηθεί για τα νοικοκυριά και για wearable συσκευές. Για παράδειγμα, επιτρέπει στους χρήστες να έχουν την κυριότητα και να πωλούν τα δεδομένα τους σε πραγματικό χρόνο, αντί να παρακολουθούνται εν άγνοιά τους για ανάλυση της αγοράς.

Πιθανές IOTA εφαρμογές είναι αναμφίβολα πολύ υποσχόμενες. Όπως ο δημιουργός του επισήμανε, η αυξανόμενη ανάπτυξη του IoT οδηγεί στην εμφάνιση του λεγόμενου Fog and Mist Computing. Το Fog and Mist μειώνει την καθυστέρηση του δικτύου που υπάρχει όταν μεγάλα κέντρα δεδομένων Cloud, βρίσκονται πολύ μακριά από τις τελικές συσκευές.

Ειδικότερα, το Fog ωθεί εφαρμογές μεγάλης υπολογιστικής έντασης στην πύλη, ενώ ο Mist ωθεί τις λιγότερο υπολογιστικά εντατικές εργασίες στις άκρες του δικτύου, δηλαδή προς τους ίδιους αισθητήρες και τους ενεργοποιητές της συσκευής.

Αναμένεται οι συναλλαγές στο Fog και Mist περιβάλλον να αυξηθούν εκθετικά, επιτρέποντας την άνοδο σε νέα επιχειρηματικά μοντέλα, προϊόντα και υπηρεσίες.

Είναι ως εκ τούτου ζωτικής σημασίας για τη βιομηχανία να βασίζεται σε ένα real-time και αποκεντρωμένο σύστημα διακανονισμού, χωρίς καμία επιβάρυνση.

Το IOTA προσφέρει επίσης μια έγκυρη και μοναδική λύση για το πρόβλημα της ασφάλειας στο περιβάλλον IoT. Μέσα από hashes των δεδομένων, επιτρέπει την πιστοποιημένες, απαραβίαστες και αποκεντρωμένες συναλλαγές μεταξύ των συσκευών και των αισθητήρων, έτσι ώστε η αλληλεπίδραση μηχανής προς μηχανή να μπορεί να αυτοματοποιηθεί με έναν ασφαλή τρόπο.

Το IOTA είναι χτισμένο στην κορυφή του «Tangle», ένα ελαφρύ blockchain "χωρίς blocks" και το πιο σημαντικό χωρίς τέλη (fees), ένας βασικός παράγοντας για τη διατήρηση κόστους-αποτελεσματικότητας.

Σύμφωνα με τα λόγια του Sønstebø, «το IOTA είναι σήμερα το μόνο έργο που λύνει το ζήτημα της κλιμάκωσης και των τελών χωρίς ad hoc λύσεις που θέτουν σε κίνδυνο την ακεραιότητα της ασφάλειας ή του αποκεντρωμένου χαρακτήρα της οικονομίας».

Κύρια χαρακτηριστικά του IOTA-Tangle

Τα κύρια χαρακτηριστικά της αρχιτεκτονικής Tangle είναι

τα ως εξής:

- Η τυπική αλυσίδα των μπλοκ των δικτύων όπως το Bitcoin, έχει αντικατασταθεί από ένα κουβάρι ή DAG (directed acyclic graph), δηλαδή μία συλλογή κόμβων που δρα ως καθολικό προς την αποθήκευση των συναλλαγών.

- Το δίκτυο είναι ασύγχρονο και οι συναλλαγές επιβεβαιώνονται από τις άμεσες και έμμεσες εγκρίσεις των κόμβων. Δεν επιβάλλετε κανένας κανόνας προς την έγκριση, μόνο οι κανόνες αναφοράς υπάρχουν.

- Σε περίπτωση αντικρουόμενων συναλλαγών, ένας κόμβος αποφασίζει ποια συναλλαγή θα μείνει ορφανή μέσα από έναν αλγόριθμο που προβλέπει ποια συναλλαγή είναι πιο πιθανή να εγκριθεί από το δίκτυο.

- Οι κόμβοι πρέπει να λύσουν ένα απαιτητικό μαθηματικό παζλ για την επαλήθευση μιας συναλλαγής και θα πρέπει να διαδίδονται μέσω του δικτύου. Σε περίπτωση που ένας κόμβος είναι υπερβολικά χαλαρός, θα αφαιρεθεί από τους άλλους κόμβους.

- Οι συναλλαγές δεν εγκρίνονται σε blocks, αλλά μεμονωμένα και χωρίς καμία επιβάρυνση.

Τροφοδοτούμενη από το Tangle και από ανθεκτικούς κβαντικούς αλγορίθμους, η IOTA αρχιτεκτονική είναι αποτελεσματική, επεκτάσιμη, πολύ ελαφριά και σύμφωνα με τους προγραμματιστές, πιο ανθεκτική σε παραβιάσεις ασφάλειας από οποιαδήποτε άλλη cryptocurrency πλατφόρμα.

Επιπλέον, το IOTA είναι διαλειτουργικό, μπορεί να επικοινωνεί με άλλα καθιερωμένα blockchains όπως το Bitcoin και το Ethereum, παρέχοντας σημεία ελέγχου για αυτά τα δίκτυα και ενισχύοντας το οικοσύστημά τους.

Πράγματι, η πρόθεση των προγραμματιστών με το IOTA δεν είναι να αντικαταστήσει τα ανοικτά blockchains εντελώς, αλλά να είναι συμπληρωματικό προς το τρέχων οικοσύστημα και να λειτουργεί σε συνδυασμό με αυτό.

Οφέλη του IOTA-Tangle

Ένα από τα κύρια αποτελέσματα που θα φέρει η άφιξη του IoT στην κοινωνία, είναι η κατανομή των πόρων. Δεδομένου ότι ο αριθμός των συσκευών αυξάνεται και οι δύο αυτές ενεργοποιούν, αλλά και απαιτούν πολλούς τεχνολογικούς πόρους. Διαχείριση των εν λόγω πόρων είναι το κλειδί. Για να λειτουργήσει σωστά το IoT χρειάζεται ανοικτότητα και διαλειτουργικότητα, ακόμη και μεταξύ των ανταγωνιστών. Δεν υπάρχει κανένας λόγος να πιστεύουμε ότι οι εταιρείες θα υιοθετήσουν αυθόρμητα ένα αλτρουιστικά επιχειρηματικό μοντέλο, οπότε η αγορά θα εξυψωθεί οργανικά. Εδώ θα δούμε μερικές από τις περιπτώσεις χρήσης όπου οι IOTA συναλλαγές θα είναι αναγκαίες και χρήσιμες.

- ✓ Κατανεμημένοι υπολογισμοί

Όπως τα σπίτια, οι δρόμοι και οι πόλεις μας βυθίζονται σε μια απέραντη θάλασσα αισθητήρων και ενεργοποιητών, θα υπάρξει μια αδιάκοπη ζήτηση για υπολογιστική ισχύ για να αναλύσει την αέναη ροή των δεδομένων από τους αισθητήρες αυτούς. Στέλνοντας τα δεδομένα πίσω στο σύννεφο για ανάλυση είναι πολύ δαπανηρό λόγω των περιορισμών του εύρους ζώνης και των καθυστερήσεων. Αντ 'αυτού το σύννεφο πρέπει να περιλαμβάνει τις συσκευές αυτές.

Αυτό σημαίνει ότι θα δούμε έναν συνδυασμό των έξυπνων αισθητήρων, όπου η υπολογιστική ικανότητα εμπεριέχεται στον ίδιο τον αισθητήρα (Mist Computing), σε συνδυασμό με σταθμούς επεξεργασίας που απλώνονται (ομίχλη Computing). Οι IOTA μικρο-συναλλαγές επιτρέπουν τα δεδομένα του αισθητήρα στον κόμβο Α να υποβληθούν σε επεξεργασία με επεξεργαστές του κόμβου Β σε πραγματικό χρόνο. Σε αντάλλαγμα ο κόμβος Β μπορεί να χρησιμοποιήσει τα iotas που παίρνει αντισταθμίζεται με το να αγοράσει τα στοιχεία από τον κόμβο Α ή οποιονδήποτε άλλο τεχνολογικού πόρο από άλλο κόμβο μέσα σε αυτό το συμβιωτικό οικοσύστημα.

- ✓ Κατανεμημένα δεδομένα

Θα υπάρξουν δεκάδες δισεκατομμύρια αισθητήρων στον κόσμο μας μέχρι το 2025. Αυτά τα δεδομένα μπορεί να είναι χρήσιμα για παραπάνω από έναν κόμβο. Ωστόσο, λόγω των φυσικών περιορισμών του εύρους ζώνης, την αποθήκευση και την ενέργεια, καθώς και το κόστος του υλικού, είναι απίθανο ότι αυτά τα δεδομένα πραγματικού χρόνου θα μοιραστούν ελεύθερα, εκτός και αν οι ιδιοκτήτες αυτών των δεδομένων αισθητήρων αποζημιωθούν.

Όπως είδαμε στην προαναφερθείσα διανέμεται σενάριο computing ο ιδιοκτήτης μιας τεχνολογικής πόρων μπορεί να το εμπόριο σε μια ελεύθερη αγορά μέσω του IOTA να αγοράσει κάποια πόρων που χρειάζονται. Αυτό σημαίνει επίσης ότι οι εταιρείες μπορούν να πληρώσουν ιδιώτες για την ανταλλαγή άμεσων δεδομένων που θα έχουν αξία για τις εταιρείες, είτε μέσω της ανάπτυξης του προϊόντος ή του marketing, την αφαιρόντας την υποκειμενικότητα και επιτρέποντας την ακριβή ανάλυση της αγοράς.

- ✓ Κατανεμημένη αποθήκευση

Ακριβώς όπως θα υπάρξει μια περίσσεια υπολογιστική ισχύ εξαπλωμένη ως αποτέλεσμα του πολλαπλασιασμού των συσκευών, έτσι θα υπάρχει ένας τεράστιος χώρος αποθήκευσης. Αυτή η αδράνεια των πόρων αποθήκευσης θα μπορούσε εύκολα να γίνει χρήσιμη και πάλι με το πραγματικό χρόνο αποζημίωσης που λαμβάνει χώρα μέσω του IOTA.

- ✓ Κατανεμημένο Bandwidth

Ένα από τα μεγαλύτερα εμπόδια που αντιμετωπίζει ένα σύστημα IoT είναι το ζήτημα των παρεμβολών. Όλοι έχουμε έστω μία φορά την ενοχλητική εμπειρία της γειτονικής σύνδεσης στο internet που παρεμβαίνει με την δική μας, γεγονός που οδηγεί σε αποσυνδέσεις και καθυστερήσεις. Για τον ελεύθερο χρόνο στο σπίτι είναι ενοχλητικό, όμως για την βιομηχανία και την κοινωνία των υποδομών μπορεί να είναι εξαιρετικά δαπανηρό. Μέσω μικρο-συναλλαγών μπορεί κανείς να αποζημιώσει και να παροτρύνει για την κοινή χρήση του δικτύου, μειώνοντας τον αριθμό των συνολικών ενεργών κόμβων σε ένα περιορισμένο χώρο και κατά συνέπεια τη μείωση των παρεμβολών.

- ✓ Κατανεμημένη Ενέργεια

Με τη συνεχιζόμενη υιοθέτηση ηλιακών συλλεκτών και project για σπίτια όπως το Project Sunroof της Google και το Powerwall του Τέσλα, είναι δυνατόν να προβλέψει κάοπιος ένα μέλλον όπου η ενέργεια μπορεί να κατανεμηθεί. Και πάλι σε πραγματικό χρόνο αποζημίωση για κοινή χρήση αυτών των τεχνολογικών πόρων, θα ενεργοποιήσει νέες καινοτομίες και μια πιο δίκαιη διαβίωσης για όλους. Στην επερχόμενη εποχή της

ασύρματης ενέργειας, είναι εύκολο να φανταστεί κανείς ηλιακούς συλλέκτες πώλησης ηλεκτρικής ενέργειας με αισθητήρες στη σκιά.

3.3.3 ADEPT

Με την από κοινού έρευνα της Samsung Electronics, η IBM αποτελεί μια από τις πρώτες εταιρίες που έκανε από τα πρώτα βήματα για κινηθεί προς την κατεύθυνση blockchain λύσεις για το IoT, με στόχο την ανάπτυξη ενός νέου επιχειρηματικού προτύπου και οράματος του κόσμου, την Οικονομία των Πραγμάτων.

Σε ένα σχέδιο που κυκλοφόρησε τον Ιανουάριο του 2015 με τίτλο «ADEPT: Μια επαγγελματική IoT προοπτική», η εταιρεία πρότεινε ένα έργο blockchain-based που ονομάζεται ADEPT, δηλαδή Αυτόνομη Αποκεντρωμένη Peer-to-Peer Τηλεμετρία (Autonomous Decentralized Peer-to-Peer Telemetry).

Η τελική έκδοση του εν λόγω εγγράφου εκδόθηκε στο διαδίκτυο, με τίτλο «Δημοκρατία των συσκευών- Διασφαλίζοντας το μέλλον του IoT » (Device democracy - Saving the future of the Internet of Things).

Η IBM αναγνωρίζει την αξία ενός blockchain με βάση την αποκεντρωμένη προσέγγιση στο IoT, προκειμένου να αποκτήσει μεγαλύτερη επεκτασιμότητα, αξιοπιστία, ασφάλεια, καθώς και προστασία.

Το αποτέλεσμα είναι «το Διαδίκτυο των Αποκεντρωμένων, Αυτόνομων Πραγμάτων» (“the Internet of Decentralized, Autonomous Things) μια δυναμική δημοκρατία αντικειμένων

συνδεδεμένων με ένα καθολικό ψηφιακό μοχλό, το οποίο παρέχει στους χρήστες μια ασφαλή ταυτοποίηση και γνησιότητα. Η έννοια αυτή, στο όραμα της IBM, πρόκειται να διαμορφώσει ένα ολοκαίνουργιο μοντέλο επιχειρηματικότητας στο πολύ άμεσο μέλλον.

Η αρχιτεκτονική ADEPT βασίζεται στο TeleHash (όπως το πρωτόκολλο ανταλλαγής μηνυμάτων), στο BitTorrent (ως ένα αποτελεσματικό στρώμα διανομής) και στο Ethereum (ως πλατφόρμα για τις έξυπνες συμβάσεις και Αποκεντρωμένες αυτόνομες οργανώσεις).

Κύρια χαρακτηριστικά του ADEPT

Τα κύρια χαρακτηριστικά μπορούν να συνοψισθούν ως εξής.

- Διαφανές σύστημα και πλήρως κατανεμημένο: Η επικύρωση των συναλλαγών γίνεται μέσω ενός συνδυασμού της απόδειξης εργασίας (proof-of-work) και την απόδειξη της συμμετοχής (proof-of-stake).

- Αρχιτεκτονική κατάλληλη για διαφορετικούς κόμβους: οι κόμβοι του δίκτυού μπορούν να διακριθούν ανάλογα με το επίπεδο της υπολογιστικής τους ισχύς και μνήμης:

    1. Απλοί Peers (π.χ. Raspberry Pi, Beaglebone, ή Arduino) έχουν χαμηλους πόρους: μπορούν να εκτελέσουν μηνυμάτων και λειτουργούν ως απλα πορτοφόλια, αλλά δεν είναι σε θέση να διαχειριστουν blockchain,

αλλα μονον να αποκτήσουν τα blockchain συναλλαγών από άλλες αξιόπιστους Peers.

2. Οι τυπικοί Peers είναι εξοπλισμένοι με υψηλότερα μέσα αποθήκευσης και πόρους επεξεργασίας, έτσι ώστε να μπορούν ανταποκριθούν στις απαιτήσεις των blockchain και να υποστηρίζουν απλούς Peers, ανάλογα με τις δυνατότητές τους. Καθώς το κόστος των chips πέφτει, η IBM αναμένει ότι ένας αυξανόμενος αριθμός των έξυπνων αντικειμένων θα είναι σε θέση να συμπεριλαμβάνονται σε αυτήν κατηγορία των κόμβων.

3. Οι Peers ανταλλαγής ή ADEPT Peers έχουν μεγάλη μνήμη και υπολογιστική ισχύ, έτσι ώστε να είναι σε θέση να διαχειριστούν και να αποθηκεύουν πλήρη αντίγραφα blockchain. Μπορούν να φιλοξενήσουν αγορές και μπορούν να ανήκουν σε οργανώσεις ή σε άλλους εμπορικούς φορείς, παρέχοντας blockchain αναλυτικής υπηρεσίας και να είναι σε θέση να πραγματοποιήσουν σύνθετα ερωτήματα. Αυτοί οι κόμβοι αποτελούν τον πυρήνα της ADEPT φιλοσοφίας και τις γρήγορες διαδρομές ενός νέου οικονομικού προτύπου. Πράγματι, μπορούν εκτελέσουν το ρόλο των οικονομικών ανταλλαγών μεταξύ των κοινοτήτων, στο βαθμό που είναι σε θέση να εξισορροπήσουν τη ζήτηση και την παροχής υπηρεσιών, τα περιουσιακά στοιχεία και τα προϊόντα. Μπορούν να λάβουν υπόψη τους διαθέσιμους πόρους σε μια κοινότητα και να βρουν τους αγοραστές σε μια άλλη, εκτελώντας τη λειτουργία του «Ρευστοποίηση των περιουσιακών στοιχείων".

- Αυτονομία των συσκευών: μέσα από έξυπνες συμβάσεις που εκτελούνται στο Ethereum, οι συσκευές μπορούν να εκτελέσουν αυτόνομα πληρωμές, συμφωνίες, να εμπορευθούν και να ανταλλάξουν πόρους μεταξύ τους. Μπορούν επίσης να ανιχνεύσουν πιθανά επιχειρησιακά προβλήματα και να τα λύσουν.

- Ένα μοντέλο με επίκεντρο τον χρήστη: συσκευές θα ενεργούν προς το καλύτερο συμφέρον του χρήστη και όχι των τρίτων (π.χ. κατασκευαστές, κυβερνήσεις ή φορείς παροχής υπηρεσιών).

- Blockchain από προεπιλογή: προϊόντα και συσκευές θα πρέπει να έχουν καταγραφεί από τον κατασκευαστή σε εάν καθολικό blockchain, κατά την έναρξη του κύκλου ζωής στους.

Προβλήματα του ADEPT

Το ADEPT αποτελεί μια ενδιαφέρουσα προσπάθεια του κλάδου για να γίνει το οικοσύστημα IoT πιο βιώσιμο, μέσω μιας αποκεντρωμένης, peer-to-peer και με επίκεντρο τον χρήστη προσέγγιση. Για την λειτουργία της πλατφόρμας όμως χρειάζεται να ξεπεραστούν αρκετά τεχνικά ζητήματα, τα οποία είναι τα εξής:

- Επεκτασιμότητα: για το IoT να διαχειριστεί ένα παγκόσμιο blockchain τελικά αποτελεί μια τεράστια πρόκληση,

δεδομένου ότι το blockchain αποθηκεύει τα αρχεία όλων των συναλλαγών από την πρώτη συναλλαγή που πραγματοποιήθηκε. Σύμφωνα με τους προγραμματιστές της IBM, sidechains, treechains, και μίνι-blockchains μπορούν να χρησιμοποιηθούν για την αντιμετώπιση των προβλημάτων αυτών.

- Peer-list: το blockchain μπορεί να αποθηκεύσει το ιστορικό ενός έξυπνου αντικείμενου, αλλά δεν έχει σχεδιαστεί για να αναγνωρίσει τα ίδια τα αντικείμενα. Ως εκ τούτου, ένα peer-list απαιτείται. Εφόσον η ταυτότητα ενός αντικείμενου έχει αναγνωριστεί, το αναγνωριστικό αυτό μπορεί να χρησιμοποιηθεί για περιήγηση στο blockchain.

- Single Points of Failure: κακόβουλοι χρήστες μπορούν να εκμεταλλευτούν απόρρητα ή άγνωστα τρωτά σημεία της ανταλλαγής του κώδικα των κόμβων και ενδεχομένως να ρίξουν ολόκληρο το δίκτυο.

- Προστασία Προσωπικών Δεδομένων: όλοι οι κόμβοι του δικτύου blockchain έχουν πρόσβαση στις συναλλαγές του άλλου, οπότε η προστασία του blockchain δεν είναι εγγυημένη.

3.4 Προβλήματα των εφαρμογών blockchain για το IoT

Η ανάπτυξη των blockchains, των cryptocurrencies και των έξυπνων συμβάσεων για το IoT εξακολουθεί να συνεπάγεται

διάφορα θέματα και ανησυχίες, σε τεχνικό και κοινωνικό επίπεδο.

Ιδιωτικότητα. Στο blockchain, η προστασία της ιδιωτικότητας και του απορρήτου εξακολουθεί να αποτελεί πρόβλημα, αφού όλοι οι κόμβοι του δικτύου έχουν πρόσβαση στα δεδομένα των άλλων και οι συναλλαγές είναι επίσης ορατές σε όσους εξερευνήσουν την blockchain. Για να ξεπεραστεί αυτό το πρόβλημα, οι συμμετέχοντες μπορούν να χρησιμοποιούν διαφορετικές διευθύνσεις κατά την αποστολή ή τη λήψη των συναλλαγών. Άλλες μέθοδοι όπως η ομομορφική κρυπτογράφηση (homomorphic encryption) και το zeroknowledge proof είναι επίσης αποτελεσματικά, εφόσον οι εισόδους στις συναλλαγές είναι ορατές στους αποστολείς και παραλήπτες μόνο, επιτρέποντας όμως σε όλους τους άλλους κόμβους του δικτύου να ελέγχουν την εγκυρότητα της συναλλαγής. Αυτές οι τεχνικές, ωστόσο, μπορεί να αποδειχθούν χρονοβόρες, μη πρακτικές ή όχι βελτιστοποιημένες για περιορισμένο από πόρους περιβάλλον IoT. Οι προγραμματιστές του Enigma έχουν προτείνει την καλύτερη λύση μέχρι τώρα, μέσω της αποθήκευσης δεδομένων εκτός της αλυσίδας και την διασφάλιση Multi Party Computation (sMPC). Αυτή η πλατφόρμα είναι πολλά υποσχόμενη και αντιπροσωπεύει ένα καλό παράδειγμα της ιδιωτικότητας εκ κατασκευής.

4. Blockchain υλοποιήσεις

4.1 Εισαγωγή

Υπάρχουν διάφορα καινοτόμα συστήματα πληρωμών στην αγορά σήμερα, πολλά από τα οποία είναι χτισμένα σε πλατφόρμες όπως το κινητό τηλέφωνο, το διαδίκτυο και τις ψηφιακές κάρτες. Αυτά τα εναλλακτικά συστήματα πληρωμών έχουν δει ενθαρρυντικά αποτελέσματα ή ακόμα και συνεχή ανάπτυξη από τους όμοιούς τους PayPal, Apple Pay, Πορτοφόλι Google, Alipay, TenPay, Venmo, M-Pesa, BitPay, Moven, BitPesa, PayLah !, Dash, FAST, Transferwise, και άλλα.

Η αυξανόμενη χρήση των ψηφιακών νομισμάτων επιτρέπει τις ταχύτερες, πιο ευέλικτες και πιο καινοτόμες πληρωμές και τρόπους για την χρηματοδότηση αγαθών και υπηρεσιών. Ένα ψηφιακό νόμισμα, όμως, ξεχωρίζει από τα υπόλοιπα. Το Bitcoin είναι ένα από τα πιο γνωστά ψηφιακά νομίσματα που υπάρχουν σήμερα.

Μία λύση στο πρόβλημα των διπλών δαπανών είναι χρησιμοποιώντας ένα δίκτυο peer-to-peer. Μια peer-to-peer έκδοση του ηλεκτρονικού χρήματος θα επιτρέψει τις απευθείας πληρωμές να αποστέλλονται απευθείας από το ένα άτομο στο άλλο χωρίς να περάσει από κάποιο τραπεζικό ίδρυμα. Οι ψηφιακές υπογραφές παρέχουν μέρος της διαδικασίας, αλλά τα κυρίως πλεονεκτήματα θα χαθούν αν ένα έμπιστο τρίτο μέρος εξακολουθεί να απαιτείται για την αποφυγή της διπλής δαπάνης.

4.2 Τι είναι το Bitcoin

Το Bitcoin είναι ένα συναινετικό δίκτυο που παρέχει τη δυνατότητα ενός νέου συστήματος πληρωμών και μιας εντελώς

ψηφιακής μορφής χρημάτων. Είναι το πρώτο αποκεντρωμένο δίκτυο πληρωμής μεταξύ ομότιμων (peer-to-peer) που λειτουργεί από τους χρήστες του χωρίς κεντρική αρχή ή μεσάζοντες. Από τη σκοπιά του χρήστη, το Bitcoin είναι λίγο πολύ σαν τα μετρητά χρήματα του Διαδικτύου.

Πιο συγκεκριμένα, το Bitcoin είναι ένα κρυπτονόμισμα (cryptocurrency), το οποίο είναι ένα υποσύνολο του τι είναι γενικά γνωστό σήμερα ως ένα ψηφιακό νόμισμα. Το Bitcoin είναι ένα μοναδικό cryptocurrency που θεωρείται ευρέως ότι είναι το πρώτο του είδους του. Όπως και πολλά άλλα cryptocurrencies που δημιουργήθηκαν μετά από αυτό, το Bitcoin χρησιμοποιεί τη δύναμη του διαδικτύου για την επεξεργασία των συναλλαγών του.

Το δίκτυο τοποθετεί χρονικές σφραγίδες στις συναλλαγές προσθέτοντας ένα hash σε μια συνεχή hash-based proof-of-work αλυσίδα, σχηματίζοντας μία εγγραφή που δεν μπορεί να αλλάξει χωρίς να επαναληφθεί το proof-of-work. Η μακρύτερη αλυσίδα χρησιμεύει ως απόδειξη της ακολουθίας των γεγονότων που συνέβησαν.

Όσο η πλειοψηφία της δύναμης της CPU ελέγχεται από κόμβους που δεν συνεργάζονται για επιτεθούν στο δίκτυο, θα δημιουργήσει τη μεγαλύτερη αλυσίδα και θα ξεπεράσει τους επιτιθέμενους. Το ίδιο το δίκτυο απαιτεί την ελάχιστη δομή. Τα μηνύματα που μεταδίδονται σε best effort βάση και οι κόμβοι μπορούν να αφήσουν και να επανέλθουν στο δίκτυο κατά βούληση, αποδέχοντας την μεγαλύτερη proof-of-work αλυσίδα ως απόδειξη του τι συνέβη, ενώ είχαν φύγει.

Κανείς δεν είναι ιδιοκτήτης του δικτύου Bitcoin όπως ακριβώς και κανένας δεν είναι ιδιοκτήτης της τεχνολογίας πίσω από το email. Το Bitcoin ελέγχεται από όλους τους χρήστες Bitcoin σε όλο τον κόσμο. Ενώ οι προγραμματιστές βελτιώνουν το λογισμικό, δεν μπορούν να εξαναγκάσουν καμία αλλαγή στο

πρωτόκολλο Bitcoin, διότι όλοι οι χρήστες είναι ελεύθεροι να επιλέξουν την έκδοση του λογισμικού που χρησιμοποιούν. Για να διατηρηθεί η συμβατότητα, όλοι οι χρήστες πρέπει να χρησιμοποιούν το λογισμικό που υπακούει στους ίδιους κανόνες. Το Bitcoin μπορεί να λειτουργήσει σωστά μόνο με την πλήρη συναίνεση μεταξύ όλων των χρηστών. Ως εκ τούτου, όλοι οι χρήστες και οι προγραμματιστές έχουν ισχυρό κίνητρο να προστατεύουν αυτήν την γενική συναίνεση.

4.3 Η Ιστορία πίσω από το Bitcoin

Τον Νοέμβριο του 2008, κάποιος με το όνομα χρήστη Satoshi Nakamoto δημοσίευσε στο διαδίκτυο ένα έγγραφο 9 σελίδων με τίτλο «Bitcoin: A Peer-to-Peer Electronic Cash System", στο οποίο περιέγραφε ένα όραμα για ένα κατανεμημένο σύστημα ψηφιακού χρήματος.

Τον Ιανουάριο του 2009, ο Satoshi Nakamoto κυκλοφόρησε την πρώτη έκδοση του λογισμικού Bitcoin ανοιχτού κώδικα στην ιστοσελίδα SourceForge και το πρωτόκολλο Bitcoin άρχισε να τρέχει. Ο Nakamoto εξορύσσει τα πρώτα 50 bitcoins. Το πρωτόκολλο ήταν μια σημαντική ανακάλυψη στην κρυπτογραφία, αν και βασίστηκε σε εξελίξεις που είχαν προηγηθεί, αλλά δεν είχε συνδυαστεί ακόμα.

Το Bitcoin έτρεξε αθόρυβα στο παρασκήνιο, ένα θέμα ενθουσιασμού και γοητείας για ένα αφιερωμένο σε αυτό πλήθος προγραμματιστών αλλά και σε μεγάλο βαθμό εκτός του υπόλοιπου κόσμου. Η συζήτηση για το bitcoin διανεμήθηκε σε διάφορα φόρουμ και δεν ήταν μέχρι το τέλος του έτους, όπου τότε ιδρύθηκε το πρώτο ειδικό φόρουμ για το Bitcoin. Αυτό βοήθησε τους προγραμματιστές να συνεργαστούν πιο έυκολα με άλλους προγραμματιστές, καθώς ο κώδικας βελτιωνόταν.

Μέχρι τα μέσα του 2009, άνθρωποι εκτός από ο Satoshi Nakamoto συνέβαλαν ενεργά στη βάση ανοικτού κώδικα στην ιστοσελίδα του Github.

Το πρωτόκολλο ήταν μια σημαντική ανακάλυψη στην κρυπτογραφία, αν και βασίστηκε σε πολλές καινοτομίες κρυπτογραφίας που προηγήθηκαν. Μια κοινότητα ειδικών στην κρυπτογραφία και υποστηρικτές της προστασίας δεδομένων γνωστοί ως Cypherpunks (cypher not cyber) έπαιξαν καθοριστικό ρόλο στην αναγνώριση της ιδιοφυΐής τεχνική του Bitcoin και στην κατανόηση των επιπτώσεών της. Πολλά μέλη της κοινότητας αυτής θα παίξουν σημαντικό ρόλο αργότερα στην ιστορία του Bitcoin. Ως το τέλος του 2009, το Bitcoin δεν είχε μια «εμπορική τιμή» και μόλις 309 άτομα είδαν τη σχετική σελίδα της Wikipedia.

Το Bitcoin «οικοσύστημα» ήταν σε μεγάλο βαθμό απλώς μια καταγραφή των συναλλαγών Bitcoin (blockchain), ένα σύνολο από online φόρουμ συναλλαγές όπου οι χρήστες επικοινωνούσαν μεταξύ τους και διοργάνωναν συναλλαγές και ο κώδικας του λογισμικού ανοιχτού κώδικα. Δεν υπήρχαν υπηρεσίες πορτοφολιού, επεξεργαστές πληρωμών ή πραγματική διεπαφή χρήστη πέρα από γραμμή εντολών και raw κώδικα. Η πρώτη εμπορική συναλλαγή πραγματοποιήθηκε τον Μάιο του 2010: ένας προγραμματιστής στη Φλόριντα ξόδεψε 10.000 bitcoins σε μια πίτσα.

Το 2011, Bitcoin άρχισε να ωριμάζει ως ένα ψηφιακό σύστημα πληρωμών, αν και η χρήση του περιορίζεται από τις φιλοδοξίες των πρώτων χρηστών.

Ο ανώνυμος χαρακτήρας του ψηφιακού νομίσματος, το κατέστησε ιδανικό για online μαύρη αγορά. Εκείνη τη χρονιά εμφανίστηκε το Silk Road, μια ηλετκτρονική αγορά για παράνομα αγαθά (κυρίως φάρμακα) που χρησιμοποιούσε το Bitcoin ως μέθοδο πληρωμής. Το Silk Road ήταν ένας από τους

πρωταρχικούς εισαγωγείς του κοινού στο Bitcoin, με αποτέλεσμα αρκετοί πολιτικοί να κατηγορούν το νόμισμα για ξέπλυμα χρήματος και ναρκωτικά.

Τα μέσα μαζικής ενημέρωσης, επίσης, άρχισε να μιλούν για αυτό. Γράφτηκαν πολλά άρθρα από εφημερίδες και ακαδημαικούς και οι πολιτικοί προειδοποιούσαν εναντίον του.

Άλλες υπηρεσίες προς τους καταναλωτές επίσης αρχίζουν να αναδύονται. Η ιστοσελίδα WikiLeaks άρχισε να δέχεται Bitcoin δωρεές. Ένα iPad app ξεκίνησε. Το Bitpay, μια υπηρεσία που σας επιτρέπουν στους έμπορους να δέχονται bitcoins μέσω τηλεφώνου, ιδρύθηκε και υποστήριζε ότι έχει 100 εμπόρους. Περισσότερες συναλλαγές δημιουργήθηκαν, επιτρέποντας στους ανθρώπους να ανταλλάσουν bitcoins για άλλα νομίσματα.

Ο κώδικας Bitcoin υπέστη επίσης μια σημαντική αλλαγή. Έως το 2011, Satoshi Nakamoto επέβλεψε τη διατήρηση του κώδικα. Ο Satoshi ποτέ δεν ζήτησε να γνωρίσει κανέναν και επικοινωνούσε μόνο στο φόρουμ και με άμεσα μηνύματα. Τον Απρίλιο του 2011, ο Satoshi Nakamoto έγραψε το τελευταίο επαληθευμένο ηλεκτρονικό του ταχυδρομείο, αφήνοντας τον Gavin Andreson υπεύθυνο του έργου, και αποχώρησε χωρίς να εμφανιστεί πουθενά ξανά από τότε. Ο Andreson επίλεξε γρήγορα τέσσερις άλλους να μοιράζονται την ευθύνη του Bitcoin και εισήγαγε ορισμένους δομημένους τρόπους ενημέρωσης του κώδικα

4.4 Τα κύρια χαρακτηριστικά του Bitcoin

- Είναι ένα ψηφιακό συναλλακτικό σύστημα μέσω Internet και συνεπώς υφίσταται μόνο μέσα σε ψηφιακά συστήματα, δηλαδή δεν έχει υλική υπόσταση (χαρτονομίσματα π.χ.). Τα ψηφιακά νομίσματα Bitcoin φυλάσσονται στο ψηφιακό πορτοφόλι του χρήστη
- Δεν έχει κεντρικό έλεγχο και η λειτουργία του βασίζεται στην επικοινωνία των υπολογιστών μεταξύ τους, μέσω του Internet
- Όσα υπολογιστικά συστήματα συνεισφέρουν την επεξεργαστική τους ισχύ στο δίκτυο του Bitcoin, δημιουργούν νομίσματα, προφυλάσσουν το δίκτυο από επιθέσεις κι ελέγχουν την ορθότητα κι εγκυρότητα των συναλλαγών που γίνονται σε αυτό (η διαδικασία αυτή είναι προαιρετική)
- Η δημιουργία των νομισμάτων είναι ελέγξιμη κι έτσι αποτρέπονται φαινόμενα όπως ο πληθωρισμός, που μειώνει την αξία ενός νομίσματος
- Η ανταλλαγή Bitcoins μεταξύ χρηστών, σε οποιοδήποτε σημείο στον κόσμο κι αν βρίσκονται, γίνεται εύκολα με τη χρήση ενός προγράμματος
- Οι αμοιβές για τη μεταφορά Bitcoins είναι απειροελάχιστες (μικρότερες των πέντε λεπτών του ευρώ)
- Υπάρχουν υπηρεσίες που ανταλλάσσουν Bitcoins για άλλα νομίσματα όπως ευρώ, δολάρια, κλπ ή και για άλλα κρυπτονομίσματα
- Οι Bitcoin συναλλαγές είναι μη αναστρέψιμες, δηλαδή αν στείλουμε νομίσματα σε ένα φίλο, δεν υπάρχει

δυνατότητα ν’ αναστρέψουμε τη συναλλαγή. Ο μόνος τρόπος για να λάβουμε τα νομίσματά μας πίσω, είναι να γίνει νέα συναλλαγή από τον φίλο προς εμάς.

4.5 Πως λειτουργεί το Bitcoin

Ένας νέος χρήστης μπορεί να ξεκινήσει με το Bitcoin χωρίς να καταλαβαίνει τις τεχνικές λεπτομέρειες. Εφόσον εγκατασταθεί το Bitcoin πορτοφόλι στον υπολογιστή ή στο κινητό τηλέφωνο, θα δημιουργήσει την πρώτη Bitcoin διεύθυνση και μπορούν να δημιουργηθούν και περισσότερες οποτεδήποτε χρειαστεί. Ανταλλάσοντας τις διευθύνσεις με τους άλλους χρήστες, μπορούν να γίνουν πληρωμές και εισπράξεις. Στην πραγματικότητα, αυτό είναι αρκετά παρόμοιο με την λειτουργία του ηλεκτρονικού ταχυδρομείου, με την εξαίρεση ότι οι διευθύνσεις Bitcoin θα πρέπει να χρησιμοποιούνται μόνο για μια φορά.

Υπόλοιπα Λογαριασμού - Blockchain:

Η αλυσίδα των μπλοκ (blockchain) είναι ένα κοινόχρηστο δημόσιο λογιστικό βιβλίο πάνω το οποίο βασίζεται ολόκληρο το δίκτυο Bitcoin. Όλες οι επιβεβαιωμένες συναλλαγές συμπεριλαμβάνονται στην αλυσίδα των μπλοκ. Με αυτό τον τρόπο, τα πορτοφόλια Bitcoin μπορούν να υπολογίζουν το διαθέσιμο υπόλοιπο και οι νέες συναλλαγές μπορούν να επαληθεύονται ότι δαπανώνται bitcoins τα οποία στην πραγματικότητα κατέχονται από αυτόν που τα δαπανά. Η ακεραιότητα και η χρονολογική σειρά της αλυσίδας των μπλοκ εφαρμόζονται με την κρυπτογραφία.

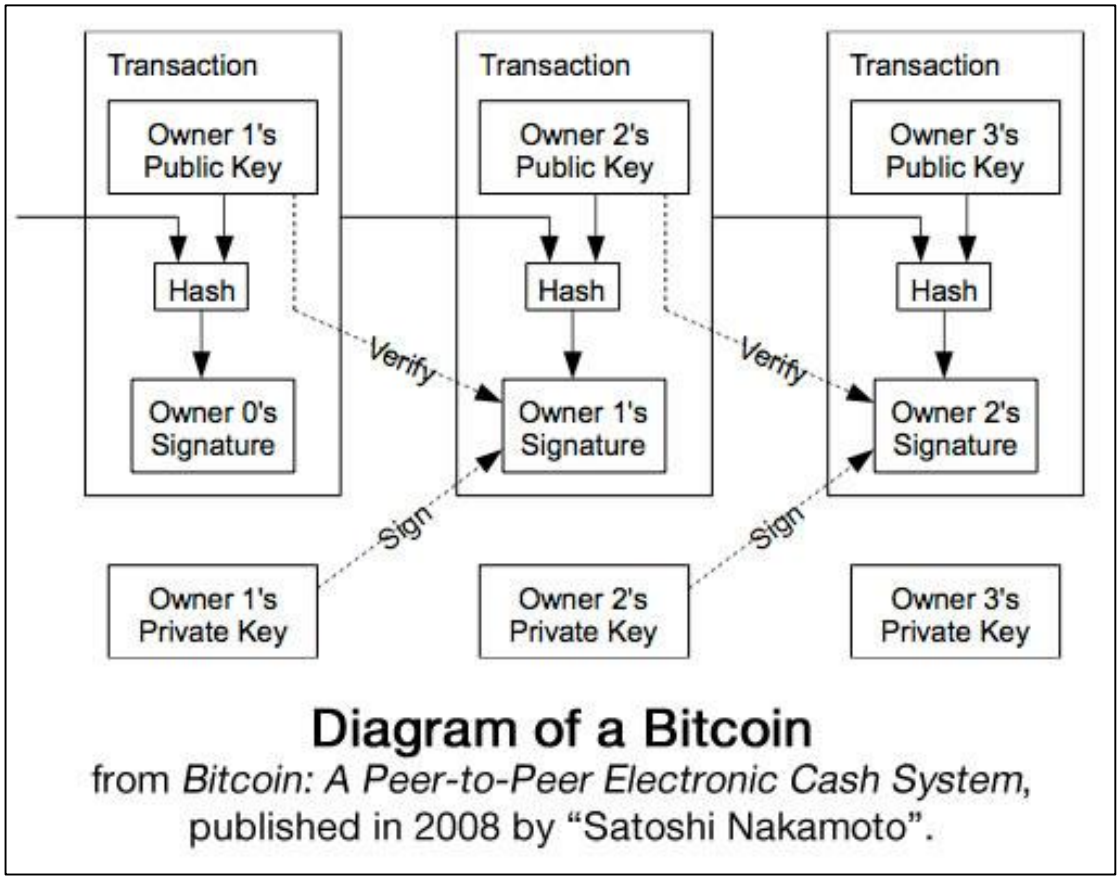
Συναλλαγές - ιδιωτικά κλειδιά:

Μια συναλλαγή είναι μια μεταφορά αξίας μεταξύ πορτοφολιών Bitcoin η οποία συμπεριλαμβάνεται στην αλυσίδα των μπλοκ (blockchain). Τα πορτοφόλια Bitcoin κρατάνε ένα μυστικό κομμάτι δεδομένων που ονομάζεται ιδιωτικό κλειδί ή φύτρο (seed), το οποίο χρησιμοποιείται για να υπογράψει συναλλαγές παρέχοντας μια μαθηματική απόδειξη η οποία έχει προέλθει από το πορτοφόλι του ιδιοκτήτη. Η υπογραφή επίσης εμποδίζει τη συναλλαγή από το να τροποποιηθεί από τον οποιονδήποτε μόλις αυτή έχει εκδοθεί. Όλες οι συναλλαγές μεταδίδονται μεταξύ των χρηστών και συνήθως ξεκινάνε να επιβεβαιώνονται από το δίκτυα στα επόμενα 10 λεπτά μέσω μια διαδικασίας που ονομάζεται εξόρυξη.

Επεξεργασία - εξόρυξη:

Η εξόρυξη είναι ένα κατανεμημένο συναινετικό σύστημα που χρησιμοποιείται για την επιβεβαίωση συναλλαγών σε αναμονή συμπεριλαμβάνοντας αυτές στην αλυσίδα των μπλοκ (block chain). Επιβάλλει μια χρονολογική σειρά στην αλυσίδα των μπλοκ, προστατεύει την ουδετερότητα του δικτύου και επιτρέπει σε διαφορετικούς υπολογιστές να συμφωνήσουν σχετικά με την κατάσταση του συστήματος. Για να επιβεβαιωθούν, οι συναλλαγές πρέπει να εντάσσονται σε ένα μπλοκ (block) που υπακούει σε πολύ αυστηρούς κανόνες κρυπτογραφίας που θα επαληθευτούν από το δίκτυο. Οι κανόνες αυτοί εμποδίζουν τα προηγούμενα μπλοκ (blocks) από το να τροποποιηθούν, διότι κάτι τέτοιο θα ακύρωνε όλα τα ακόλουθα μπλοκ. Η εξόρυξη δημιουργεί επίσης το ισοδύναμο μιας ανταγωνιστικής λοταρίας, η οποία εμποδίζει κάθε άτομο από το να προσθέσει εύκολα νέα διαδοχικά μπλοκ (blocks) στην αλυσίδα των μπλοκ (blockchain). Με αυτόν τον τρόπο, κανένα άτομο δεν μπορεί να ελέγξει τι περιλαμβάνεται στην αλυσίδα

των μπλοκ ή να αντικαταστήσει τμήματα της αλυσίδας αυτής για να ακυρώσει τις δικές του δαπάνες.



Σχέδιο 4.1

4.6 Τρόποι απόκτησης Bitcoins

Υπάρχουν δύο τρόποι για να αποκτήσει κανείς BitCoin. Ο ένας είναι να επισκεφθεί διαδικτυακά ανταλλακτήρια, όπως το Mt.Gox, και να αγοράσει Bitcoin από τα ήδη υπάρχοντα, πληρώνοντας την αντιστοιχία τους με κανονικά χρήματα. Ο δεύτερος είναι να γίνει ο ίδιος «εκδότης» BitCoin, μέσω της εγκατάστασης ειδικού λογισμικού στον υπολογιστή που αξιοποιεί την υπολογιστική του ισχύ για να διενεργεί εργασίες κρυπτογράφησης σχετικές με την ασφάλεια των συναλλαγών σε

BitCoin. Για κάθε επιτυχή κρυπτογράφηση ο χρήστης αμείβεται με 50 εκατομμυριοστά του Bitcoin.

Υπάρχουν ήδη πάνω από 12,3 εκατομμύρια Bitcoins και συνεχώς αυξάνονται, αλλά οι δημιουργοί του νομίσματος έχουν θέσει ως ανώτατο όριο τα 21 εκατομμύρια Bitcoins. Προκειμένου το όριο αυτό να μην προσεγγιστεί σύντομα (στόχος είναι αυτό να συμβεί το 2140), ο ρυθμός εκτύπωσης θα μειώνεται κατά το ήμισυ κάθε 4 χρόνια. Ο αυστηρά προβλέψιμος χαρακτήρας της ποσότητας Bitcoin που βρίσκεται ανά πάσα στιγμή σε κυκλοφορία αποτελεί σημαντικό πλεονέκτημα, σε μια εποχή που τα περισσότερα «πραγματικά» νομίσματα τυπώνονται με όλο και ταχύτερο ρυθμό.

4.7 Πλεονεκτήματα και μειονεκτήματα

Ποια είναι τα πλεονεκτήματα του Bitcoin;

- ***Ελευθερία πληρωμών*** - Είναι δυνατή η αποστολή και η λήψη οποιουδήποτε χρηματικού ποσού άμεσα, οπουδήποτε στον κόσμο, οποιαδήποτε στιγμή. Χωρίς αργίες, χωρίς σύνορα και χωρίς επιβαλλόμενα όρια. Το Bitcoin επιτρέπει στους χρήστες του να έχουν τον πλήρη έλεγχο των χρημάτων τους.
- ***Πολύ χαμηλά τέλη*** - Προς το παρόν, οι πληρωμές με Bitcoin γίνονται είτε με μηδενικά είτε με εξαιρετικά χαμηλά τέλη. Οι χρήστες μπορεί να συμπεριλάβουν τέλη στις συναλλαγές τους προκειμένου να έχουν προτεραιότητα στην διεκπεραίωση, κάτι που έχει ως αποτελέσματα την γρηγορότερη επικύρωση των συναλλαγών από το δίκτυο. Επιπροσθέτως, οι επεξεργαστές για εμπόρους υπάρχουν για να τους

βοηθήσουν στην επεξεργασία πληρωμών, μετατρέποντας τα bitcoins σε πιστωτικό χρήμα και καταθέτοντας τα κεφάλαια απευθείας στον τραπεζικό λογαριασμό των εμπόρων καθημερινά. Καθώς αυτές οι υπηρεσίες βασίζονται στο Bitcoin, μπορούν να προσφέρονται με πολύ χαμηλότερα τέλη σε σχέση με την PayPal ή δίκτυα πιστωτικών καρτών.

- ***Λιγότεροι κίνδυνοι για τους εμπόρους*** - Οι συναλλαγές με Bitcoin είναι ασφαλείς, μη αναστρέψιμες και δεν περιέχουν προσωπικές πληροφορίες ή ευαίσθητα προσωπικά δεδομένα των πελατών. Αυτό προστατεύει τους εμπόρους από ζημίες που προκαλούνται από απάτες ή δόλιους αντιλογισμούς χρέωσης (chargebacks). Οι έμποροι μπορούν εύκολα να επεκταθούν σε νέες αγορές όπου είτε οι πιστωτικές κάρτες δεν είναι διαθέσιμες, είτε τα ποσοστά απάτης είναι πολύ υψηλά. Το αποτελέσματα σε καθαρό κέρδος είναι χαμηλότερα τέλη, μεγαλύτερες αγορές και λιγότερα διοικητικά κόστη.
- ***Ασφάλεια και έλεγχος*** - Οι χρήστες του Bitcoin έχουν πλήρη έλεγχο των συναλλαγών τους. Είναι ανέφικτο για τους εμπόρους να επιβάλλουν ανεπιθύμητες ή απαρατήρητες χρεώσεις όπως μπορεί να συμβεί με άλλες μεθόδους πληρωμής. Οι πληρωμές με Bitcoin μπορούν να διεξαχθούν χωρίς να συνδέονται προσωπικές πληροφορίες με την συναλλαγή. Αυτό προσφέρει ισχυρή προστασία κατά της κλοπής ταυτότητας. Οι χρήστες του Bitcoin μπορούν επίσης να προστατέψουν τα χρήματά τους με αντίγραφα ασφαλείας και κρυπτογράφηση.
- ***Διαφανής και ουδέτερος*** – Όλες οι πληροφορίες που αφορούν τον εφοδιασμό του Bitcoin με χρήματα είναι άμεσα διαθέσιμες στο blockchain για τον οποιονδήποτε να τις επιβεβαιώσει και να τις χρησιμοποιήσει σε

πραγματικό χρόνο. Κανένα άτομο ή οργανισμός δεν μπορεί να ελέγξει ή να πλαστογραφήσει το πρωτόκολλο του Bitcoin διότι είναι κρυπτογραφικά ασφαλές. Αυτό επιτρέπει στον πυρήνα του Bitcoin να είναι αξιόπιστος αφού είναι απόλυτα ουδέτερος, διαφανής και προβλέψιμος.

Ποια είναι τα μειονεκτήματα του Bitcoin;

- ***Βαθμός αποδοχής*** - Πολλοί άνθρωποι δεν είναι ακόμα ενήμεροι για το Bitcoin. Καθημερινά, όλο και περισσότερες επιχειρήσεις δέχονται τα bitcoins γιατί θέλουν τα πλεονεκτήματα κάνοντας χρήση αυτών, αλλά η λίστα παραμένει μικρή και χρειάζεται να μεγαλώσει ακόμα έτσι ώστε να επωφεληθούμε από τα αποτελέσματα του δικτύου.
- ***Αστάθεια*** – Η συνολική αξία των bitcoins σε κυκλοφορία και ο αριθμός των επιχειρήσεων που χρησιμοποιούν το Bitcoin είναι ακόμα πολύ μικρός σε σύγκριση με αυτό που θα μπορούσε να είναι. Συνεπώς, σχετικά μικρά γεγονότα, συναλλαγές, ή επιχειρηματικές δραστηριότητες μπορούν να επηρεάσουν σημαντικά την τιμή. Θεωρητικά, η αστάθεια αυτή θα μειωθεί καθώς οι αγορές Bitcoin και η τεχνολογία ωριμάζουν. Ποτέ στο παρελθόν δεν έχει δει ο κόσμος ένα νεοσύστατο νόμισμα, οπότε είναι πραγματικά δύσκολο να φανταστούμε το πώς θα εξελιχθεί.
- ***Συνεχής εξέλιξη*** - Το λογισμικό του Bitcoin είναι ακόμα σε έκδοση beta με πολλά ημιτελή χαρακτηριστικά σε ενεργή εξέλιξη. Καινούρια εργαλεία, λειτουργίες και υπηρεσίες εξελίσσονται για να κάνουν το Bitcoin πιο ασφαλές και προσβάσιμο στις μάζες. Μερικές από αυτές δεν είναι ακόμα έτοιμες για όλους. Οι περισσότερες επιχειρήσεις

Bitcoin είναι νέες και δεν προσφέρουν ασφάλεια ακόμα. Γενικότερα, το Bitcoin είναι ακόμα σε διαδικασία ωρίμανσης.

4.8 Ethereum

Η τεχνολογία πίσω από τα κρυπτονομίσματα όπως το Bitcoin είναι όλα τα σχετικά με την αποκέντρωση. Η blockchain τεχνολογία του Bitcoin την οποία έφερε στον κόσμο ο Satoshi Nakamoto εισήγαγε ένα ισχυρό, πρακτικό τρόπο για να πραγματοποιήσει κάποιος συναλλαγές με ασφάλεια επιτρέποντας μας για πρώτη φορά να έχουμε ένα πραγματικά αποκεντρωμένο νόμισμα. Αλλά η δύναμη της blockchain τεχνολογίας έφερε πολλά στον κόσμο πιστεύοντας ότι υπάρχουν πολλά περισσότερα που θα μπορούσαμε να κάνουμε. Οι άνθρωποι άρχισαν να αναρωτιούνται γιατί, από τη στιγμή που είναι δυνατόν να έχουμε ένα δίκτυο για την επικύρωση των Bitcoin συναλλαγών, δεν θα μπορούσαμε να έχουμε ένα δίκτυο να λειτουργεί αξιόπιστα για πιο περίπλοκες "έξυπνες συμβάσεις" και ακόμη μεγαλύτερο λογισμικό;

Πριν από δύο χρόνια, ένας 20χρονος προγραμματιστής Bitcoin, ο Vitalik Buterin σχεδίασε μια νέα πλατφόρμα που ονομάζεται Ethereum. Δουλεύοντας με μια γρήγορα αναπτυσσόμενη ομάδα, το Ethereum συγκέντρωσε πάνω από 14 εκατομμύρια δολάρια σε μια Bitcoin crowdfunding εκστρατεία και ξεκίνησε με τεράστιους στόχους για να διαταράξει τον τρόπο που χτίζουμε τις εφαρμογές, τα κοινωνικά δίκτυα, τα χρηματοπιστωτικά συστήματα, ακόμα και τις επιχειρήσεις.

Το 2014, οι Ethereum ιδρυτές Vitalik Buterin, Gavin Wood και Jeffrey Wilcke άρχισαν να δουλεύουν ένα επόμενης γενιάς

blockchain, που είχε την φιλοδοξία να υλοποιήσει μία γενική, πλήρως έμπιστη έξυπνη πλατφόρμα σύμβασης.

4.9 Τι είναι το Ethereum

Το Ethereum είναι μια ανοιχτή πλατφόρμα blockchain που επιτρέπει σε οποιονδήποτε να κατασκευάσει και να χρησιμοποιήσει αποκεντρωμένες εφαρμογές που τρέχουν σε blockchain τεχνολογία. Όπως και το Bitcoin, κανείς δεν ελέγχει ή κατέχει το Ethereum, είναι ένα έργο ανοιχτού πηγαίου κώδικα που χτίστηκε από πολλούς ανθρώπους σε όλο τον κόσμο. Αλλά σε αντίθεση με το πρωτόκολλο Bitcoin, το Ethereum σχεδιάστηκε για να είναι προσαρμόσιμο και ευέλικτο. Είναι εύκολο να δημιουργηθούν νέες εφαρμογές στην πλατφόρμα Ethereum και είναι ασφαλές για οποιονδήποτε να χρησιμοποιήσει αυτές τις εφαρμογές.

Το Ethereum είναι ένα αποκεντρωμένο πρωτόκολλο blockchain που εκτελεί έξυπνα συμβόλαια: εφαρμογές που τρέχουν ακριβώς όπως έχουν προγραμματιστεί, χωρίς καμία δυνατότητα διακοπής της παραγωγής, λογοκρισίας, απάτης ή παρέμβασης τρίτων. Το Ether είναι η ενσωματωμένη νομισματική μονάδα της πλατφόρμας Ethereum.

Ως πλατφόρμα λογισμικού, το Ethereum είναι σαν το Bitcoin, δηλαδή στο ότι είναι χτισμένο σε ένα blockchain και όλα όσα συμβαίνουν τροφοδοτούνται και ελέγχονται από υπολογιστές σε όλο το δίκτυο. Διαθέτει επίσης μια ενσωματωμένη νομισματική μονάδα που ονομάζεται “Ether”, η οποία λειτουργεί σαν το Bitcoin. Αλλά η κύρια καινοτομία του Ethereum είναι ότι περιλαμβάνει επίσης μια πλήρη γλώσσα προγραμματισμού (η οποία ονομάζεται “Turing-complete”). Αυτό είναι κάτι που το Bitcoin δεν έχει, και το οποίο επιτρέπει

στους προγραμματιστές να σχεδιάζουν πολύ μεγαλύτερες εφαρμογές που θα εκτελούνται και θα επιβεβαιώνονται από το δίκτυο. Η πλατφόρμα επιτρέπει στους προγραμματιστές να δημιουργούν “Αποκεντρωμένες Εφαρμογές” (Decentralized Apps ή DApps), οι οποίες είναι, για το χρήστη, σχεδόν πανομοιότυπες με μια τυπική εφαρμογή web, αλλά των οποίων η κύρια βάση δεδομένων και ο server είναι το blockchain.

Αν και δεν μπορούν όλες οι εφαρμογές να μεταφραστούν άμεσα σε μια αποκεντρωμένη αρχιτεκτονική, το Ethereum έχει περισσότερο νόημα σε μέρη όπου η διαφάνεια και η ειλικρίνεια έχουν αξία ή χρειάζονται. Για παράδειγμα, τα τελευταία χρόνια πολλές εταιρείες εισαγωγής παρουσιάζουν αυξημένα επίπεδα διαφάνειας για τον τρόπο που λαμβάνονται οι αποφάσεις. Πολλές εταιρείες έχουν εισαγάγει διαφανείς πολιτικές αποδοχών. Οι εταιρείες θα έχουν σύντομα τη δυνατότητα να έχουν τα πιο σημαντικά στοιχεία διακυβέρνησής τους, να διαχειρίζονται το blockchain, τροφοδοτούμενα από εφαρμογές όπως το Boardroom, τα οποία κατασκευάζονται στην Ethereum πλατφόρμα. Μπορούμε να φανταστούμε όλες τις αποφάσεις μιας εταιρείας π.χ. αποφάσεις για τις αποδοχές, τις επενδύσεις και την έγκριση έργων, οι οποίες διακινήθηκαν μέσω ενός συστήματος ψηφοφορίας που δεν θα μπορούσε να είναι πλαστό και το οποίο υποβλήθηκε σε επεξεργασία και έλεγχο σύμφωνα με κανόνες που ορίζονται στον κώδικα.

Ένα άλλο startup υψηλού προφίλ βασισμένο στην πλατφόρμα Ethereum είναι το Augur, το οποίο κατασκευάζει μία έξυπνη πλατφόρμα πρόγνωσης και έχει ήδη λάβει χρηματοδότηση 4 εκατομμυρίων δολαρίων σε κρυπτονόμισμα. Η κοινότητα γύρω από το Ethereum αυξάνεται με ταχείς ρυθμούς, και πολλά άλλα startups ετοιμάζονται να δημιουργήσουν προϊόντα. Οι μεγάλες εταιρείες επενδύουν επίσης πολύ χρόνο και χρήματα στο χώρο, προσπαθώντας να καταλάβουν πώς το Ethereum και οι σχετικές

τεχνολογίες μπορούν να διαταράξουν τα υφιστάμενα θεσμικά όργανα, ιδίως στον τομέα των χρηματοπιστωτικών βιομηχανιών.

Η υπόθεση για αποκέντρωση είναι επίσης ισχυρή, αν αναλογιστεί κανείς την τεράστια μόχλευση που κατέχεται από μερικά από τα μεγαλύτερα κοινωνικά δίκτυα και online αγορές. Μόλις αυτή την εβδομάδα, το TechCrunch πήρε την ιστορία ενός superhost Airbnb ο οποίος τερματίστηκε με μηδενική προειδοποίηση για αδιευκρίνιστους λόγους. Το Uber έχει επικριθεί για την έλλειψη διαφάνειας γύρω από την απενεργοποίηση του οδηγού. Και όποιος έχει χρησιμοποιήσει το Facebook για οποιοδήποτε χρονικό διάστημα γνωρίζει τον αγώνα ενάντια στην διαρκώς μεταβαλλόμενες ρυθμίσεις απορρήτου. Φανταστείτε την επόμενη γενιά των αγορών και των εφαρμογών κοινωνικής δικτύωσης, όπου οι κανόνες θα ψηφίζονται από τους χρήστες και όπου οι πολιτικές δεν θα μπορούν να αλλάξουν από μια μικρή ομάδα.

Το Ethereum αποτελείται από 7 μέρη:

- Κρυπτονόμισμα: όπως το Bitcoin, αλλά το όνομα είναι Ether.
- Blockchain: μια κατανεμημένη βάση δεδομένων.
- Μηχανισμός συναίνεσης: προστατεύει τη βάση δεδομένων με την επίλυση εξισώσεων κρυπτογράφησης και hashing.
- Mining: ένα παγκόσμιο δίκτυο υπολογιστών που επιβεβαιώνουν μία νέα συναλλαγή, εκτελούν το

μηχανισμό συναίνεσης και προσθέτουν μπλοκ στο blockchain περίπου κάθε 12 δευτερόλεπτα.

- Προγραμματισμός: σε αντίθεση με το Bitcoin, στο Ethereum μπορούν να αποθηκευτούν προγράμματα λογισμικού, που ονομάζονται έξυπνες συμβάσεις. Αυτά μπορούν να ελέγξουν τους λογαριασμούς, τα χρήματα και να κάνουν εργασίες όπως κάθε πρόγραμμα, αλλά αυτόνομα.

- Εικονική μηχανή: τα παραπάνω προγράμματα έχουν ανάγκη να εκτελεστούν κάπου, έτσι όλοι οι υπολογιστές συμμετέχουν στις εργασίες του δικτύου ως ένα μοναδικό μηχάνημα, σαν να ήταν μια εξειδικευμένη υπηρεσία cloud.

- Mist πρόγραμμα περιήγησης: είναι σαν το Bitcoin Core client, αλλά είναι σαν ένα πρόγραμμα περιήγησης και μπορούν να χρησιμοποιηθούν αποκεντρωμένες εφαρμογές που στηρίζονται στο Ethereum.

4.10 Ethereum Virtual Machine (EVM)

Το Ethereum είναι ένα προγραμματιζόμενο blockchain. Αντί να δώσει στους χρήστες ένα σύνολο προκαθορισμένων λειτουργιών (π.χ. Bitcoin συναλλαγές), το Ethereum επιτρέπει στους χρήστες να δημιουργήσουν τις δικές τους λειτουργίες οποιασδήποτε πολυπλοκότητας επιθυμούν. Με αυτόν τον τρόπο, το Ethereum χρησιμεύει ως πλατφόρμα για πολλούς διαφορετικούς τύπους εφαρμογών αποκεντρωμένων blockchain, που περιλαμβάνουν αλλά δεν περιορίζονται σε κρυπτονομίσματα.

Το Ethereum αναφέρεται σε μια σουίτα πρωτοκόλλων που καθορίζουν μια πλατφόρμα για αποκεντρωμένες εφαρμογές. Στην καρδιά της σουίτας βρίσεκται το Ethereum Virtual Machine (EVM), το οποίο μπορεί να εκτελέσει κώδικα αυθαίρετης αλγοριθμικής πολυπλοκότητας. Σε όρους της επιστήμης των υπολογιστών, το Ethereum είναι "Turing complete". Οι προγραμματιστές μπορούν να δημιουργήσουν εφαρμογές που τρέχουν στο EVM με τη χρήση φιλικών γλωσσών προγραμματισμού οι οποίες βασίζονται σε υφιστάμενες γλώσσες όπως JavaScript και Python.

Όπως κάθε blockchain, έτσι και το Ethereum περιλαμβάνει επίσης ένα πρωτόκολλο δικτύου peer-to-peer. Η Ethereum blockchain βάση δεδομένων συντηρείται και ενημερώνεται από πολλούς κόμβους που συνδέονται με το δίκτυο. Κάθε κόμβος του δικτύου διαχειρίζεται το EVM και εκτελεί τις ίδιες οδηγίες. Για το λόγο αυτό, το Ethereum μερικές φορές περιγράφεται ως «ο υπολογιστής του κόσμου».

Αυτός ο μαζικός παραλληλισμός των υπολογιστών σε ολόκληρο το δίκτυο Ethereum δεν γίνεται για να κάνει τους υπολογισμούς πιο αποτελεσματικούς. Στην πραγματικότητα, αυτή η μέθοδος καθιστά τους υπολογισμούς στο Ethereum πολύ πιο αργούς και πιο ακριβούς από ότι σε ένα παραδοσιακό "υπολογιστή". Αντίθετα, κάθε Ethereum κόμβος τρέχει το EVM, προκειμένου να διατηρηθεί η συναίνεση σε ολόκληρο το blockchain. Αυτή η αποκεντρωμένη συναίνεση δίνει στο Ethereum ακραία επίπεδα ανοχής σφαλμάτων, εξασφαλίζει μηδενικό downtime και κάνει τα δεδομένα που είναι αποθηκευμένα στο blockchain για πάντα αναλλοίωτα.

Η Ethereum πλατφόρμα παρόμοια με τις γλώσσες προγραμματισμού, εναπόκειται στους προγραμματιστές να αποφασίσουν που θα πρέπει να χρησιμοποιείται. Ωστόσο, είναι σαφές ότι ορισμένοι τύποι εφαρμογών επωφελούνται περισσότερο από άλλους από τις δυνατότητες του Ethereum.

Συγκεκριμένα, το ethereum είναι κατάλληλο για εφαρμογές που αυτοματοποιούν την άμεση αλληλεπίδραση μεταξύ των κόμβων ή διευκολύνουν τη συντονισμένη δράση της ομάδας σε ένα δίκτυο. Για παράδειγμα, οι αιτήσεις για το συντονισμό peer-to-peer αγορών, ή την αυτοματοποίηση των σύνθετων χρηματοπιστωτικών συμβάσεων. Το Bitcoin επιτρέπει στα άτομα να ανταλλάσσουν μετρητά χωρίς τη συμμετοχή από τυχόν μεσάζοντες όπως τα χρηματοπιστωτικά ιδρύματα, τράπεζες, ή κυβερνήσεις.

Το αντίκτυπο του Ethereum μπορεί να είναι πιο εκτεταμένο. Στη θεωρία, οι οικονομικές αλληλεπιδράσεις ή ανταλλαγές οποιασδήποτε πολυπλοκότητας θα μπορούσαν να πραγματοποιηθούν αυτόματα και αξιόπιστα με τη χρήση κώδικα που εκτελείται σε Ethereum. Πέρα από οικονομικές εφαρμογές, οποιαδήποτε περιβάλλοντα όπου η εμπιστοσύνη, η ασφάλεια και η μονιμότητα είναι σημαντικά, για παράδειγμα μητρώα περιουσιακών στοιχείων, ψήφοι, διακυβέρνηση και το Internet of Thigns, θα μπορούσαν να επηρεαστούν μαζικά από την πλατφόρμα Ethereum.

4.11 Πως λειτουργεί το ethereum

Το Ethereum ενσωματώνει πολλά χαρακτηριστικά και τεχνολογίες που θα είναι γνωστά στους χρήστες του Bitcoin, ενώ εισάγει επίσης πολλές τροποποιήσεις και καινοτομίες.

Όπως αναφέρθηκε προηγουμένως, το Ethereum είναι ένα αποκεντρωμένο πρωτόκολλο blockchain που εκτελεί έξυπνα συμβόλαια. Ένα έξυπνο συμβόλαιο (smart contract) αναφέρεται σε μία κωδικοποιημένη λογική που κινεί τα ψηφιακά στοιχεία όταν ενεργοποιείται από απαραίτητα γεγονότα. Είναι παρόμοια με μια σειρά από "If, then" δηλώσεις, όπου τα «if» είναι οι προϋποθέσεις που πρέπει να πληρούνται

προκειμένου να προκαλέσει τα "then". Η ιδέα ταιριάζει καλά με την τεχνολογία blockchain επειδή τα blockchains προσφέρουν εγγύηση για μελλοντική εκτέλεση, σε αποκεντρωμένη βάση, με το που η έξυπνη σύμβαση αποτυπωθεί μέσα σε ένα μπλοκ.

Οι υπό όρους συναλλαγές που εκτελούνται μέσα σε ένα blockchain είναι υπολογιστικά ακριβά, επειδή κάθε υπολογιστής που είναι μέρος του δικτύου πρέπει να εκτελέσει την ίδια λογική και να ενημερώσει την κατάσταση του blockchain. Με άλλα λόγια, κάθε φορά που μια έξυπνη σύμβαση ενεργοποιείται, κάθε υπολογιστής πρέπει να εκτελεί το ίδιο έργο, καταναλώνοντας σημαντικούς πόρους και καθιστώντας τη διαδικασία αναποτελεσματική σε σύγκριση με παράλληλες αρχιτεκτονικές επεξεργασίας. Ως εκ τούτου, δεν είναι κάθε υπό όρους συναλλαγή κατάλληλη για την εκτέλεση μέσω blockchain, αλλά μόνο εκείνες οι συναλλαγές που χρησιμοποιούν τις περιπτώσεις που απαιτούν την κατανεμημένη και ασφαλή φύση ενός κοινού καθολικού (ledger). Μόλις εφαρμοστούν πιο εξελιγμένες λύσεις όπως η διανομή των δεδομένων σε πολλαπλά μηχανήματα, η οποία μπορεί να βοηθήσει να παραλληλιστούν καλύτερα τα υπολογιστικά καθήκοντα και χώρος αποθήκευσης, οι συναλλαγές υπό όρους μπορεί να αποδειχθούν λιγότερο υπολογιστικά ακριβές στο δίκτυο και έτσι να διευρυνθεί το πεδίο εφαρμογής των εφαρμογών.

Όπως και στο Bitcoin, οι χρήστες πρέπει να πληρώνουν μικρές πληρωμές συναλλαγής με το δίκτυο. Αυτό προστατεύει το Ethereum blockchain από επιπόλαιες ή κακόβουλες υπολογιστικές εργασίες, όπως οι DDoS επιθέσεις ή άπειρους βρόγχους. Ο αποστολέας της συναλλαγής πρέπει να πληρώσει για κάθε βήμα του «προγράμματος» που ενεργοποιείται, συμπεριλαμβανομένων του υπολογισμού και της αποθήκευσης

της μνήμης. Τα τέλη αυτά καταβάλλονται σε Ether, το νόμισμα του Ethereum.

Αυτές οι αμοιβές συναλλαγής συλλέγονται από τους κόμβους που επικυρώνουν το δίκτυο. Αυτοί οι κόμβοι λέγονται ανθρακωρύχοι (miners) και είναι οι κόμβοι του δικτύου Ethereum που λαμβάνουν, διαδίδουν, ελέγχουν και να εκτελούν συναλλαγές. Μετά οι ανθρακωρύχοι ομαδοποιούν τις συναλλαγές - το οποίο περιλαμβάνει πολλές ενημερώσεις για την κατάσταση των λογαριασμών στο blockchain Ethereum - σε αυτό που καλείται "μπλοκ" και οι ανθρακωρύχοι στη συνέχεια ανταγωνίζονται μεταξύ τους για το αν το μπλοκ τους να είναι το επόμενο που θα προστεθεί στο blockchain. Οι ανθρακωρύχοι ανταμείβονται με ether για κάθε επιτυχημένο μπλοκ που προστίθεται. Αυτό παρέχει το οικονομικό κίνητρο για τους ανθρώπους να αφιερώσουν το hardware και την ηλεκτρική ενέργεια στο δίκτυο Ethereum.

Ακριβώς όπως και στο δίκτυο Bitcoin, οι ανθρακωρύχοι έχουν σαν στόχο την επίλυση ενός πολύπλοκου μαθηματικού προβλήματος, προκειμένου να προστεθεί ένα μπλοκ με επιτυχία. Αυτό είναι γνωστό ως proof of work (απόδειξη της εργασίας). Κάθε υπολογιστικό πρόβλημα που απαιτεί περισσότερους πόρους για να λυθεί αλγοριθμικά από ό, τι χρειάζεται για να εξακριβώσει την λύση, είναι ένας καλός υποψήφιος για την απόδειξη της εργασίας. Για να αποθαρρύνουν τη κεντρικοποίηση λόγω της χρήσης εξειδικευμένου υλικού (π.χ. ASIC), όπως έχει συμβεί στο δίκτυο Bitcoin, το Ethereum επέλεξε ένα υπολογιστικό πρόβλημα απαιτεί μνήμη. Εάν το πρόβλημα απαιτεί μνήμη, καθώς και CPU, το ιδανικό υλικό είναι στην πραγματικότητα ένας γενικός υπολογιστής. Το γεγονός αυτό καθιστά την Ethereum απόδειξη της εργασίας ASIC-ανθεκτική, επιτρέποντας μια πιο

αποκεντρωμένη κατανομή της ασφάλειας από blockchains των οποίων η εξόρυξη κυριαρχείται από εξειδικευμένο υλικό, όπως το Bitcoin.

4.12 Διαφορές Ethereum και Bitcoin

Υπάρχουν πολλές μικρές διαφορές ανάμεσα στις δύο blockchain-based εφαρμογές. Ο μέσος χρόνος κάθε μπλοκ στο Bitcoin είναι περίπου 10 λεπτά, ενώ στο Ethereum είναι 12 δευτερόλεπτα. Αυτός ο μικρός χρόνος οφείλεται στο πρωτόκολλο GHOST του Ethereum. Ταχύτερο μπλοκ σημαίνει ότι οι επιβεβαιώσεις είναι πιο γρήγορες. Ωστόσο, υπάρχουν και περισσότερα ορφανά μπλοκ.

Μια άλλη βασική διαφορά μεταξύ τους είναι η νομισματική προσφορά τους. Περισσότερα από τα δύο τρίτα όλων των διαθέσιμων bitcoin έχουν ήδη εξορυχθεί, με το μεγαλύτερο μέρος πηγαίνει στους πρόωρους ανθρακωρύχους. Το Ethereum έθεσε το αρχικό του κεφαλαίο με προπώληση και μόνο το ήμισυ περίπου των κερμάτων του θα έχουν εξορυχθεί από το πέμπτο έτος της ύπαρξής του.

Η ανταμοιβή για την εξόρυξη Bitcoin είναι περίπου μισή κάθε τέσσερα χρόνια και αυτή τη στιγμή αποτιμάται στα 12,5 bitcoins. Το Ethereum επιβραβεύει τους ανθρακωρύχους με βάση τον αλγόριθμο της απόδειξης της εργασίας που ονομάζεται Ethash, με 5 ether να δίνονται για κάθε μπλοκ. Το Ethash είναι memory hard hashing αλγόριθμος, ο οποίος ενθαρρύνει την αποκεντρωμένη εξόρυξη από ιδιώτες, παρά τη χρήση των πιο συγκεντρωτικών ASICs όπως με το Bitcoin.

Το Bitcoin και το Ethereum τιμολογούν επίσης τις συναλλαγές τους με διαφορετικούς τρόπους. Στο Ethereum η κοστολόγηση

των συναλλαγών εξαρτάται από τις ανάγκες αποθήκευσης, της πολυπλοκότητάς τους και τη χρήση του εύρους ζώνης. Στο Bitcoin, οι συναλλαγές περιορίζονται από το μέγεθος του μπλοκ και ανταγωνίζονται ισότιμα η μία με το άλλη.

Το Ethereum διαθέτει το δικό του Turing complete εσωτερικό κώδικα, πράγμα που σημαίνει ότι οτιδήποτε μπορεί να υπολογιστεί με αρκετή υπολογιστική ισχύ και αρκετό χρόνο. Το Bitcoin δεν έχει αυτή τη δυνατότητα. Ενώ υπάρχουν σίγουρα πλεονεκτήματα για το Turing-complete, η πολυπλοκότητα του φέρνει και επιπλοκές ασφαλείας, οι οποίες συνέβαλαν στην επίθεση DAO στο παρελθόν.

Επίσης το Bitcoin και το Ethereum έχουν διαφορετικό σκοπό. Ενώ το Bitcoin δημιουργείται ως εναλλακτική λύση πληρωμής και είναι έτσι ένα μέσο συναλλαγής πληρωμής και αποθήκευσης αξίας, το Ethereum αναπτύσσεται ως μια πλατφόρμα που διευκολύνει τις συμβάσεις και τις peer-to-peer εφαρμογές μέσω του δικού του νομίσματος. Ενώ Bitcoin και Ether είναι και τα δύο ψηφιακά νομίσματα, ο πρωταρχικός σκοπός του Ether δεν είναι να καθιερωθεί ως εναλλακτική λύση πληρωμής (σε αντίθεση με Bitcoin), αλλά να διευκολύνει και να έχει κέρδος η λειτουργία των Ethereum ώστε να επιτρέπει στους προγραμματιστές να δημιουργήσουν και να τρέξουν κατανεμημένες εφαρμογές. (Distributed Apps).

Εν ολίγοις, το Ethereum είναι μια πρόοδος με βάση την αρχή του blockchain που υποστηρίζει bitcoin αλλά με έναν σκοπό που δεν ανταγωνίζεται το Bitcoin. Ωστόσο, η δημοτικότητα και η αυξανόμενη αγορά του Ether, το φέρνει σε ανταγωνισμό με όλα τα κρυπτονομίσματα, ειδικά από τη σκοπιά των συναλλαγών. Στο σύνολό τους, το Bitcoin και το Ethereum είναι διαφορετικές υλοποιήσεις χρησιμοποιώντας την τεχνολογία blockchain και πρόκειται να εγκατασταθούν, οδηγούμενες από διαφορετικές προθέσεις.

Συμπεράσματα

Το blockchain και η τεχνολογία κατανεμημένης υποδομής είναι συναρπαστικές πολλά υποσχόμενες εξελίξεις για τον κλάδο των χρηματοπιστωτικών υπηρεσιών. Ενώ υπάρχουν σημαντικά δυνητικά οφέλη από την εφαρμογή της τεχνολογίας, το να την εφαρμόσει κάποιος με επιτυχία είναι μια πρόκληση. Λαμβάνοντας υπόψη προσεκτικά το πώς η τεχνολογία θα μπορούσε να καλύψει τις ανάγκες των επιχειρήσεων, καθώς και το ρόλο άλλων εξωτερικών και εσωτερικών παραγόντων, οι επιχειρήσεις μπορούν να βελτιώσουν σημαντικά την πιθανότητα ότι οι πρωτοβουλίες τους για την κατανεμημένη υποδομή θα πετύχουν.

Η blockchain τεχνολογία έχει μεγάλες δυνατότητες για να οδήγησει το επόμενο κύμα της καινοτομίας στο IoT και μπορεί να προωθήσει την εμφάνιση νέων επιχειρηματικών μοντέλων, τροποποιώντας σημαντικά τα υπάρχοντα συστήματα και τις διαδικασίες. Πιθανές επιπτώσεις της εφαρμογής της, ωστόσο, θα πρέπει να λαμβάνουν υπόψη συγκεκριμένα πλαίσια χρήσης. Οι μελέτες που πραγματοποιήθηκαν, μας οδηγήσαν σε πολύ διαφορετικά συμπεράσματα για τα συνολικά οφέλη και τα μειονεκτήματα του IoT βασισμένου σε blockchain για την κοινωνία στο σύνολό της.

Από τη μια πλευρά, blockchain πλατφόρμες όπως το Enigma ανταποκρίνονται πολύ κατάλληλα στο θέμα των χρηστών της ιδιωτικότητας και μπορεί αισιοδοξώς να υλοποιηθεί ως βέλτιστη πρακτική στον κλάδο. Επίσης, το IOTA αποτελεί ένα ιδανικό πρωτόκολλο μετάδοσης δεδομένων για το IoT, επιλύοντας το μείζον προβλήμα της ασφάλειας μέσω της αποκεντρωμένης και απαραβίαστης ανταλλαγής δεδομένων μεταξύ των συσκευών χωρίς τέλη.

Από την άλλη πλευρά, όμως, η ανάπτυξη της blockchain τεχνολογίας εντός μίας παγκόσμιας, κεντρικής πλατφόρμας δεν μετριάζει τις πιθανές επιπτώσεις του IoT. Συγκεκριμένα, μια ευρεία διάδοση και χρήση των μηχανισμών ανταμοιβής, έξυπνων συμβάσεων και συστήματα μικρο-πληρωμών θα πρέπει να είναι υπολογίζονται προσεκτικά κατά ανθρωπολογική και κοινωνική διάσταση της τεχνολογικής καινοτομίας.

Συνεπώς, συνιστάται, να βρεθεί μια ισορροπία μεταξύ της ανάγκης για την καινοτομία, την οικονομική την ανάπτυξη και την κοινωνική βιωσιμότητα.

Αναφορές:

[1] https://www.weforum.org/

[2] http://www.cnn.gr/money/tech/story/6299/h-elliniki-startup-piso-apo-tin-texnologia-blockchain

[3] http://venturebeat.com/2016/11/20/how-blockchain-can-change-the-future-of-iot/

[4] http://www.itech4u.gr/tech/hands-on/item/7262-internet-of-things-se-apla-ellinika/7262-internet-of-things-se-apla-ellinika

[5] http://venturebeat.com/2016/11/20/how-blockchain-can-change-the-future-of-iot/

[6] http://www.enigma.co/enigma_full.pdf

[7] https://medium.com/@DavidSonstebo/iota-97592581f985#.b2ws3ik1m

[8] http://blog.ots.gr/tag/internet-of-things/

[9] Mastering Bitcoin, unlocking digitan crypto-currencies, Andreas M. Antonopoulos, εκδόσεις O'reilly

[10] https://www.linkedin.com/pulse/blockchain-102-different-types-terry-zhang

[11]https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/blockchain-technology-9-benefits-and-7-challenges.html

[12] http://www.itsecuritypro.gr/contents_article.php?id=293&catid=2

[13] http://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html

[14] https://bitcoinx.gr/%CE%BE%CE%B5%CE%BA%CE%AF%CE%BD%CE%B7%CE%BC%CE%B1-%CE%BC%CE%B5-%CF%84%CE%BF-bitcoin/

[15] https://bitcoin.org/bitcoin.pdf

[16] https://bitcoin.org/el/how-it-works

[17] https://bitcoin.org/el/faq

[18] http://news247.gr/eidiseis/weekend-edition/kathe-nomisma-exei-duo-opseis-etsi-kai-to-bitcoin.2870396.html

[19] http://gr.newsbtc.com/ethereum-apokentromeno-web/

[20] http://gr.newsbtc.com/ethereum-ine-defteri-ependitiki-efkeria-meta-bitcoin/

[21] https://ark-invest.com/research/smart-contracts-work

[22] http://ethdocs.org/en/latest/introduction/what-is-ethereum.html

[23] http://gavwood.com/paper.pdf

[24] http://www.investopedia.com/articles/investing/031416/bitcoin-vs-ethereum-driven-different-purposes.asp

[24] http://www.huffingtonpost.com/ameer-rosic-/ethereum-vs-bitcoin-whats_b_13735404.html