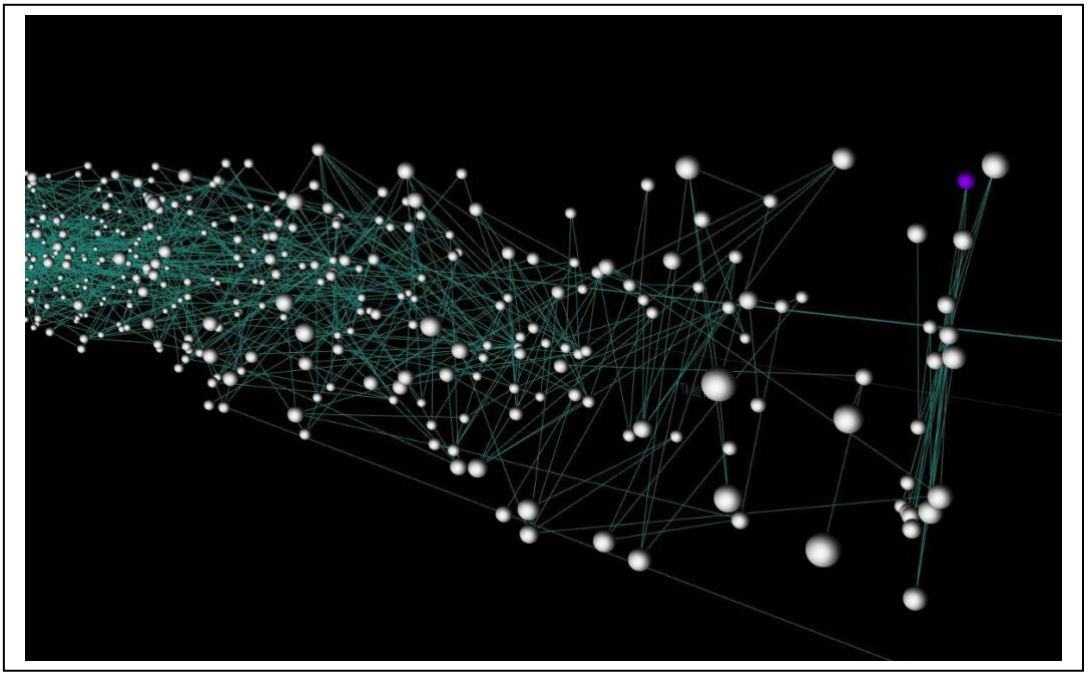
ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ & ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ

Διπλωματική Εργασία

Προστασία δεδομένων από μεταβολές στο Διαδίκτυο των Πραγμάτων με χρήση της Τεχνολογίας Κατανεμημένου Κατάστιχου (DLT)



Φοιτητής: Αλκίνοος Περατινός
ΑΜ: 50346719

Επιβλέπων Καθηγητής

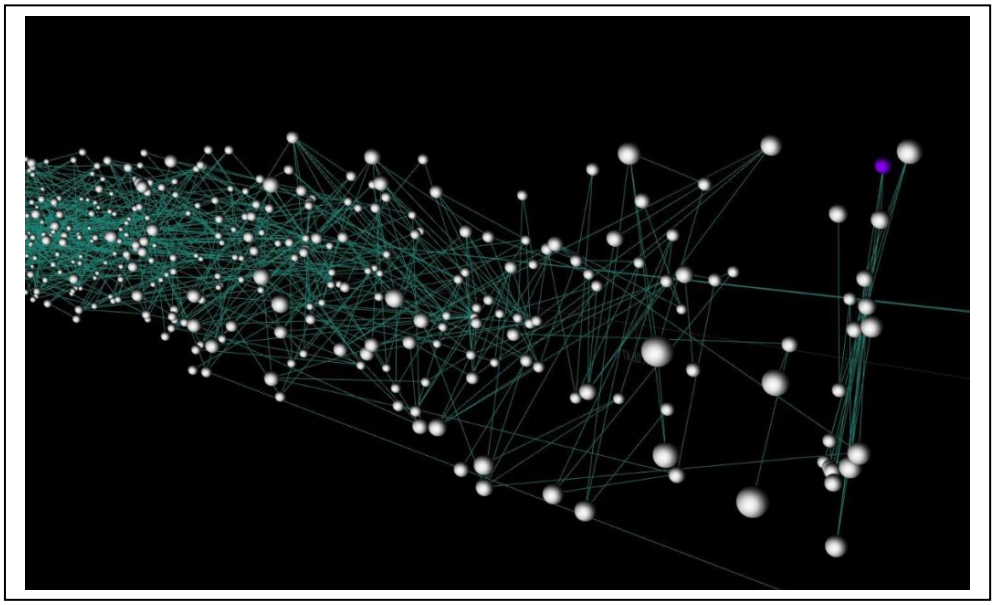
Γρηγόριος Κουλούρας
Αναπληρωτής καθηγητής

ΑΘΗΝΑ-ΑΙΓΑΛΕΩ, ΙΟΥΛΙΟΣ 2023

UNIVERSITY OF WEST ATTICA
FACULTY OF ENGINEERING
DEPARTMENT OF ELECTRICAL & ELECTRONICS ENGINEERING

Diploma Thesis

IoT data immutability by using Distributed Ledger Technology (DLT)



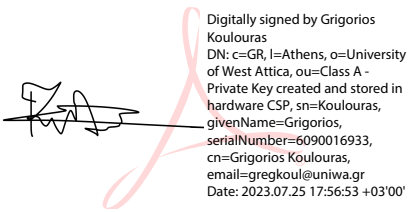
Student: Alkinoos Peratinos
Registration Number: 50346719

Supervisor

Grigorios Koulouras
Associate Professor

ATHENS-EGALEO, JULY 2023

Η Διπλωματική Εργασία έγινε αποδεκτή και βαθμολογήθηκε από την εξής τριμελή επιτροπή:

Γρηγόριος Κουλούρας, Αναπληρωτής Καθηγητής	Ξενοφών-Διονύσιος Κανδρής, Καθηγητής	Παναγιώτης Τσιάκας, Λέκτορας
 (Υπογραφή)	XENOFON DIONYSIOS KANDRIS Digitally signed by XENOFON DIONYSIOS KANDRIS Date: 2023.07.25 18:54:00 +03'00' (Υπογραφή)	Panagiotis Tsiakas Digitally signed by Panagiotis Tsiakas Date: 2023.07.25 22:36:12 +03'00' (Υπογραφή)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Αλκίνοος Περατινός του Ανδρέα, με αριθμό μητρώου 50346719 φοιτητής του Πανεπιστημίου Δυτικής Αττικής της Σχολής ΜΗΧΑΝΙΚΩΝ του Τμήματος ΗΛΕΚΤΡΟΛΟΓΩΝ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ,

Δηλώνω υπεύθυνα ότι:

«Είμαι συγγραφέας αυτής της διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.
Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του διπλώματός μου. »

Ο Δηλών
Αλκίνοος Περατινός

ALKINOOS PERATINOS
Digitally signed by ALKINOOS PERATINOS
Date: 2023.07.25 15:43:54 +03'00'

Περίληψη

Με την συνεχή, ολοένα και αυξανόμενη εισχώρηση των έξυπνων συσκευών στο Διαδίκτυο των Πραγμάτων (ΔτΠ), δημιουργείται η επιτακτική ανάγκη της μεγιστοποίησης της ασφάλειας επικοινωνίας αυτών των συσκευών και ο περιορισμός της έκθεσης των δικών μας προσωπικών πληροφοριών στο διαδίκτυο. Η εμφάνιση κακόβουλων λογισμικών, τεχνικών υποκλοπής προσωπικών δεδομένων και γενικότερα τα ζητήματα της προσωπικής ασφάλειας και της διαρροής προσωπικών δεδομένων, εμφανίστηκαν σχεδόν παράλληλα με την εμφάνιση του διαδικτύου. Η εξέλιξη του διαδικτύου από την εμφάνισή του μέχρι σήμερα, έφερε παράλληλα την ανάγκη για την εξέλιξη της ασφάλειας σε αυτό, και η ανάγκη αυτή ασφαλώς, εξακολουθεί να υφίσταται και σήμερα.

Το θέμα που θα απασχολήσει τη παρούσα Διπλωματική Εργασία (ΔΕ), είναι η αποτροπή της μεταβλητότητας των δεδομένων μεταξύ των συσκευών του ΔτΠ και του χρήστη ή το σύστημα διαχείρισης αυτών. Με τη παρούσα εργασία απαιτούμε να διασφαλίσουμε πως τα δεδομένα που φεύγουν από μια συσκευή ή έναν αισθητήρα, φτάνουν στον προορισμό τους αναλλοίωτα από οποιονδήποτε κακόβουλο ή μη παράγοντα.

Η Τεχνολογία Κατανεμημένου Κατάστιχου (Distributed Ledger Technology – DLT) είναι μία τεχνολογία που έχει χρησιμοποιηθεί αρκετά τα προηγούμενα χρόνια μεταξύ άλλων και για ηλεκτρονικές συναλλαγές κρυπτονομισμάτων με ασφάλεια και ανωνυμία. Επίσης δύναται να χρησιμοποιηθεί με παρόμοιο τρόπο για την επικυρωμένη αποστολή και λήψη οποιασδήποτε μορφής δεδομένων. Για τις ανάγκες της παρούσας εργασίας, πραγματοποιήθηκε πειραματικό μέρος, που περιλαμβάνει μία πλήρη αλυσίδα από ενέργειες που απαιτούνται για να επαληθευτεί μια πληροφορία προτού φτάσει στο τελικό προορισμό της. Στο εν λόγω πείραμα, η θερμοκρασία που μετράει ένας αισθητήρας αποθηκεύεται με τη χρήση της τεχνολογίας DLT στο IOTA ledger, και ο χρήστης όποτε επιθυμεί μπορεί να λάβει επαληθευμένες τις τιμές των μετρήσεων. Το IOTA Tangle είναι μία καινοτόμος τεχνολογία κατανεμημένου Κατάστιχου (DLT) που έχει σχεδιαστεί ειδικά για το περιβάλλον του ΔτΠ. Στη παρούσα ΔΕ παρουσιάζεται και αναλύεται η τεχνολογία πίσω από το IOTA Ledger, η οποία είναι βασισμένη σε ένα νέο τύπο DLT και όχι στο παραδοσιακό μοντέλο blockchain.

Λέξεις – κλειδιά

ΔτΠ, Τεχνολογία Κατανεμημένου Κατάστιχου, IOTA Tangle, Ασφάλεια και ΔτΠ

Abstract

With the ever-increasing appearance of smart devices into the Internet of Things (IoT), there is an imperative need to maximize the communication security of these devices, and limit the exposure of our personal information online. The emergence of malware, data eavesdropping techniques, and more generally the issues of personal security and personal data leakage, appeared almost parallel to the emergence of the internet. The evolution of the internet from its appearance until today, brought along the need for the evolution of security in it, which continues even today.

The issue that will concern this thesis is the prevention of data variability between Internet of Things (IoT) devices and the user or their management system. With this work, we require that the data leaving a device or a sensor reach its destination unaltered by any malicious agent.

By using the Distributed Ledger Technology (DLT), a technology that has been used a lot in the past years among other things like electronic currency transactions with security and anonymity, we achieve in a similar way the authenticated sending and receiving of data. For the needs of this work, an experimental part was carried out, which includes a complete chain of actions required to verify an information before it reaches the final destination. In the case of this experiment, the temperature from a sensor reaching the user, verified using DLT from the IOTA community.

The IOTA Tangle is a new and innovative distributed ledger technology (DLT) designed for the Internet of Things (IoT). IOTA technology is based on a new type of DLT, not the ordinary blockchain model.

Keywords

DLT, Distributed ledger technology, IOTA Tangle, The Tangle, security and internet of things

Περιεχόμενα

Κατάλογος Πινάκων

Κατάλογος Εικόνων

Αλφαβητικό Ευρετήριο

ΔτΠ: Διαδίκτυο των Πραγμάτων

ACL: Access Control List

AMQP: Advanced Message Queuing Protocol

CoAP: Conwtrained Application Protocol

DAG: Directed Acyclic Graph

DLT: Distributed Ledger Technology

IoT: Internet of Things

MAM: Masked authenticated messaging

MQTT: Message Queuing Telemetry Transport

PoW: Proof of WQork

PoS: Proof of Service

RBAC: Role Based Access Control

SSL: Secure Sockets Layer

TCP: Transmission Control Protocol

XMPP: Extensible Messaging and Presence Protocol

ΕΙΣΑΓΩΓΗ

Η αμεταβλητότητα των δεδομένων είναι ένα βασικό χαρακτηριστικό σε περιβάλλοντα ΔτΠ που εγγυάται την ασφάλεια και την ακεραιότητα των δεδομένων που συλλέγονται και υποβάλλονται σε επεξεργασία. Αναφέρεται στην ικανότητα των δεδομένων να παραμένουν αναλλοίωτα και αμετάβλητα, κάτι που είναι σημαντικό για την αποτροπή κακόβουλων παραγόντων. Η αμεταβλητότητα των δεδομένων είναι κρίσιμη σε περιβάλλοντα ΔτΠ, όπου τα δεδομένα συλλέγονται από διάφορες πηγές και χρησιμοποιούνται για τη λήψη κρίσιμων αποφάσεων. Αυτό είναι ιδιαίτερα σημαντικό στην περίπτωση των συσκευών ΔτΠ, καθώς είναι συνδεδεμένες στο διαδίκτυο και μπορεί να είναι ευάλωτες σε κυβερνοεπιθέσεις.

Η διασφάλιση της αμεταβλητότητας των δεδομένων στις συσκευές ΔτΠ μπορεί να επιτευχθεί μέσω διαφόρων μεθόδων, όπως οι ψηφιακές υπογραφές, οι κρυπτογραφικές συναρτήσεις κατακερματισμού και η τεχνολογία blockchain. Οι ψηφιακές υπογραφές χρησιμοποιούνται για την επαλήθευση της αυθεντικότητας των δεδομένων, ενώ οι κρυπτογραφικές συναρτήσεις κατακερματισμού χρησιμοποιούνται για τη διασφάλιση της ακεραιότητας των δεδομένων. Η τεχνολογία blockchain, από την άλλη πλευρά, χρησιμοποιείται για τη δημιουργία ενός απαραβίαστου Κατάστιχου όλων των συναλλαγών.

Η αμεταβλητότητα των δεδομένων είναι επίσης σημαντική για λόγους συμμόρφωσης και κανονιστικούς σκοπούς. Για παράδειγμα, στον τομέα της υγειονομικής περίθαλψης, τα δεδομένα που συλλέγονται από συσκευές ΔτΠ πρέπει να αποθηκεύονται με αμετάβλητο τρόπο και να συμμορφώνονται με τους νόμους περί απορρήτου των ασθενών, όπως ο (Health Insurance Portability and Accountability Act of 1996 - HIPAA). Στις χρηματοπιστωτικές υπηρεσίες, η αμεταβλητότητα των δεδομένων είναι απαραίτητη για τη συμμόρφωση με κανονισμούς όπως το πρότυπο ασφάλειας δεδομένων της βιομηχανίας καρτών πληρωμών (Payment Card Industry Data Security Standard - PCI DSS).

Εν κατακλείδι, η αμεταβλητότητα των δεδομένων είναι μια κρίσιμη πτυχή στο ΔτΠ που διασφαλίζει την ακεραιότητα των δεδομένων, αποτρέπει τη αλλοίωσή τους και βοηθά τους οργανισμούς να συμμορφώνονται με τους κανονισμούς. Με την εφαρμογή εργαλείων που επιτυγχάνουν αμετάβλητα δεδομένα στο διαδίκτυο, οι οργανισμοί μπορούν να διασφαλίσουν ότι οι συσκευές ΔτΠ είναι ασφαλείς και τα δεδομένα τους αξιόπιστα.

Αντικείμενο της διπλωματικής εργασίας

Το κύριο θέμα της ΔΕ είναι η ανάλυση και η ανάπτυξη ενός μοντέλου αποθήκευσης και προστασίας δεδομένων από μεταβολές, για την επικοινωνία συσκευών ΔτΠ με τη τεχνολογία IOTA Ledger.

Αντικείμενο της ΔΕ είναι η υλοποίηση ενός ολοκληρωμένου συστήματος που αποτελείται από δύο οντότητες.

Α. Μία συσκευή ΔτΠ, η οποία είναι ένας αισθητήρας που λαμβάνει τη θερμοκρασία και υγρασία περιβάλλοντος συνδεδεμένο στο δικτυωμένο ενσωματωμένο σύστημα (Node MCU)

Β. Ένα εικονικό μηχάνημα (VM) στο cloud, όπου έχουν υλοποιηθεί τέσσερις μικροϋπηρεσίες (micro services).

1. MQTT broker
2. SERVICE POST DATA (προς το IOTA Tangle)
3. SERVICE SEARCH DATA (απο το IOTA Tangle)
4. WEB SERVER

Η επικύρωση των δεδομένων γίνεται με τη χρήση της πλατφόρμας IOTA, η οποία έχει αναπτύξει ένα δικό της τύπο κατανεμημένου Κατάστιχου - DLT, το οποίο ονομάζει “σύμπλεγμα”, ή αλλιώς “The Tangle”. Το “Tangle” έχει παρόμοιες ιδιότητες με αυτές του blockchain και θα αναλυθεί περισσότερο τόσο αυτό όσο και οι διαφορές του με τους υπόλοιπους τύπους DLT. Αφού τα δεδομένα επικυρωθούν και ανέβουν στο “Tangle”, ο χρήστης έχει τη δυνατότητα να τα αναζητήσει με το μοναδικό τους κλειδί κατακερματισμού (hash). Τα δεδομένα αυτά, έχουν τη δυνατότητα να μεταφερθούν κρυπτογραφημένα με ευθύνη του αποστολέα χρησιμοποιώντας κάποια από τις διαθέσιμες μεθόδους κρυπτογράφησης με κλειδιά. Τέλος η πληροφορία από αυτό τον αισθητήρα καταχωρείται σε μια σελίδα διεπαφής χρήστη, δημιουργώντας ένα ψευδο-πραγματικού χρόνου (pseudo real-time) δυναμικό γράφημα θερμοκρασίας-χρόνου και υγρασίας-χρόνου.

Σκοπός και στόχοι

Σκοπός της παρούσας διπλωματικής εργασίας είναι η δημιουργία του κατάλληλου περιβάλλοντος διασύνδεσης των υπηρεσιών και η επαλήθευση ότι τα δεδομένα που φεύγουν από ένα αισθητήρα, φτάνουν στο τελικό τους προορισμό, είτε αυτός είναι μια απλή διεπαφή, είτε μια πιο σύνθετη επεξεργαστική μονάδα, αναλλοίωτα από κακόβουλους και μη παράγοντες. Κατά τη πορεία της διπλωματικής θα γίνει προσπάθεια να απαντηθούν ορισμένα ερωτήματα, όπως για παράδειγμα η έννοια του κατανεμημένου κατάστιχου, των συστημάτων ΔτΠ, του IOTA και του τρόπου με τον οποίο επαληθεύονται τα μηνύματα στο "Tangle".

Ο πρακτικός στόχος της υλοποίησης είναι να γίνει λήψη της θερμοκρασίας και της υγρασίας απο τον αισθητήρα, έπειτα να γίνει αποστολή των μετρήσεων αυτών στο "Tangle" του IOTA και τέλος να πραγματοποιηθεί ανάκτηση των δεδομένων απο το "Tangle" με σκοπό την επαλήθευση της αμεταβλητότητας τους. Στη συνέχεια θα παρουσιαστεί όλη η μεθοδολογία και τεχνολογία που χρησιμοποιήθηκε για να πραγματοποιηθεί αυτός ο σκοπός, καθώς και η ανάλυση των υπηρεσιών που χρησιμοποιήθηκαν, ώστε να γίνει κατανοητή η λειτουργία του IOTA και του Tangle.

Μεθοδολογία

Στη συγκεκριμένη διπλωματική άσκηση, δεδομένης της σημασίας που έχει η σωστή κατανόηση των μηχανισμών του blockchain στην αμεταβλητότητα των δεδομένων, είναι απαραίτητο να αντληθούν πληροφορίες από τις πιο ενημερωμένες και έγκυρες διαθέσιμες πηγές. Η βιβλιογραφία που χρησιμοποιείται για τη συγγραφή της εργασίας, η οποία παρατίθεται στο τέλος της εργασίας, αποτελείται από έγκριτη επιστημονική βιβλιογραφία (άρθρα επιστημονικών περιοδικών, διεθνών συνεδρίων και επιστημονικών βιβλίων), καθώς και από συζητήσεις σε διαδικτυακές πλατφόρμες (π.χ Discord) με τους προγραμματιστές και την ομάδα του IOTA. Για την ανάλυση και τη κατανόηση των μηχανισμών του IOTA και της υπόλοιπης τεχνολογίας, ήταν απαραίτητο τόσο το θεωρητικό υπόβαθρο όσο και η υλοποίηση αυτών των μηχανισμών σε πραγματικές συνθήκες. Αυτό συμβαίνει επειδή πρέπει πρώτα να υπάρξει η πλήρης κατανόηση της τεχνολογίας αυτής πριν ξεκινήσει η ενότητα της Υλοποίησης. Ακολουθεί η ενότητα ανάλυσης των αποτελεσμάτων της υλοποίησης σε πραγματικές συνθήκες. Τέλος, γίνεται σύγκριση των διαφορετικών τεχνολογιών DLT.

Καινοτομία

Η παρούσα διπλωματική εργασία, βασίστηκε κυρίως σε μια νέα τεχνολογία, η οποία βρίσκεται ακόμη σε στάδιο έρευνας και ανάπτυξης, αυτής του IOTA Ledger, και της ειδικής κατηγορίας της Τεχνολογίας Κατανεμημένου Κατάστιχου (DLT) που χρησιμοποιεί, με την ονομασία DAG (Directed Acyclic Graph). Με αυτή τη τεχνολογία, θα καθίσταται στο προσεχές μέλλον δυνατή, η ανταλλαγή πληροφοριών από και προς ΔτΠ συσκευές, με τα δεδομένα να περνούν αποκλειστικά μέσα από DLT συναλλαγές και η πληροφορία τους να αποθηκεύεται στο IOTA LEDGER.

Δομή διπλωματικής

Στα πρώτα κεφάλαια γίνεται μια εισαγωγή στις εφαρμογές ΔτΠ, καθώς και στη σημασία της ασφάλειας που πρέπει να έχουν τέτοιες εφαρμογές. Οι ασφαλείς συνδέσεις και η μη μεταβλητότητα δεδομένων είναι σημαντικές στις επικοινωνίες ΔτΠ, επειδή συμβάλλουν στην προστασία από μη εξουσιοδοτημένη πρόσβαση και παραβίαση των μεταδιδόμενων δεδομένων. Μια ασφαλής σύνδεση εξασφαλίζει ότι τα δεδομένα αποστέλλονται στον προβλεπόμενο παραλήπτη και προστατεύονται από υποκλοπή ή αλλοίωση από μη εξουσιοδοτημένα μέρη. Η αμεταβλητότητα των δεδομένων διασφαλίζει ότι τα δεδομένα δεν μπορούν να τροποποιηθούν μετά τη μετάδοσή τους, και συμβάλλει στη διασφάλιση της ακεραιότητας των πληροφοριών που μοιράζονται. Αυτά τα μέτρα ασφαλείας είναι σημαντικά στις επικοινωνίες ΔτΠ επειδή οι συσκευές που χρησιμοποιούνται στο ΔτΠ είναι διασυνδεδεμένες στο διαδίκτυο και δυνητικά ευάλωτες σε επιθέσεις.

Στο δεύτερο μέρος θα αναλυθεί η δομή και η λειτουργία της τεχνολογίας κατανεμημένου Κατάστιχου "DLT". Είναι πολύ σημαντικό, πριν φτάσουμε στο πρακτικό μέρος, να κατανοήσουμε πλήρως τη λειτουργία του Directed Acyclic Graph (DAG), στην οποία έχει στηρίξει η IOTA το δικό της σύστημα, που ονομάζει "The Tangle". Η τεχνολογία κατανεμημένου Κατάστιχου, ή DLT, είναι ένα αποκεντρωμένο σύστημα που επιτρέπει σε χρήστες να μοιράζονται ένα κοινό ψηφιακό ιστορικό συναλλαγών. Το DLT βασίζεται στη χρήση μιας κατανεμημένης βάσης δεδομένων, η οποία διανέμεται σε ένα δίκτυο υπολογιστών, αντί να αποθηκεύεται σε μια κεντρική τοποθεσία. Αυτό επιτρέπει σε οποιαδήποτε εξουσιοδοτημένη ΔτΠ συσκευή και οποιονδήποτε χρήστη χρησιμοποιεί το DLT για μεταφορά δεδομένων, να έχουν πρόσβαση στις ίδιες πληροφορίες, διασφαλίζοντας ότι δεν υπάρχει καμία πιθανότητα αποτυχίας, ούτε μεταποίηση της πληροφορίας που μεταφέρεται. Το DLT χρησιμοποιείται σε διάφορες εφαρμογές, όπως κρυπτονομίσματα, διαχείριση αλυσίδας εφοδιασμού και συστήματα ψηφοφορίας. Το DLT μπορεί να προσφέρει οφέλη όπως αυξημένη διαφάνεια, ασφάλεια και αμετάβλητα δεδομένα. Επιπλέον, το DLT μπορεί να επιτρέψει ταχύτερες και πιο αποτελεσματικές συναλλαγές και μπορεί να χρησιμοποιηθεί για τη μείωση του κόστους και την αύξηση της εμπιστοσύνης μεταξύ των μερών σε μια συναλλαγή.

Στο τρίτο μέρος, θα αναλυθεί η πλατφόρμα IOTA, η οποία αποτελεί μια αυτοτελή κατηγορία τεχνολογίας κατανεμημένου Κατάστιχου, βασιζόμενη στο δικό της τρόπο πιστοποίησης των συναλλαγών που ονομάζεται "The Tangle". Το IOTA είναι μια τεχνολογία κατανεμημένου Κατάστιχου ανοικτού κώδικα που έχει σχεδιαστεί για το ΔτΠ. Χρησιμοποιεί μια δομή δεδομένων κατευθυνόμενου ακυκλικού γράφου (DAG), η οποία επιτρέπει γρήγορες και δωρεάν συναλλαγές. Σε αντίθεση με άλλες τεχνολογίες που βασίζονται στο blockchain, με το IOTA, κάθε συναλλαγή επιβεβαιώνει δύο προηγούμενες συναλλαγές, γεγονός που επιτρέπει μεγαλύτερη επεκτασιμότητα και ταχύτερη επεξεργασία των συναλλαγών. Το IOTA προορίζεται να χρησιμοποιηθεί για μικροπληρωμές και μεταφορά δεδομένων στο οικοσύστημα ΔτΠ, όπου μπορεί να επιτρέψει την ασφαλή και αποτελεσματική επικοινωνία μεταξύ συσκευών. Επιπλέον, στοχεύει στο να παρέχει την υποδομή για τον αυξανόμενο αριθμό συνδεδεμένων συσκευών και τα δεδομένα που παράγουν. Έχει δυνητικές εφαρμογές σε τομείς όπως οι έξυπνες πόλεις, η βιομηχανία 4.0 και η διαχείριση της εφοδιαστικής αλυσίδας.

Τέλος, προσθέτοντας τις πληροφορίες και από τα 3 προηγούμενα μέρη, αναπτύσσεται η εφαρμογή που έχει υλοποιηθεί με τη συνδρομή της πλατφόρμας του IOTA, χρησιμοποιώντας το ως DLT για τη μεταφορά δεδομένων από τον αισθητήρα στο χρήστη.

ΚΕΦΑΛΑΙΟ 1ο : ΕΙΣΑΓΩΓΗ ΣΤΟ ΔτΠ. ΣΥΣΚΕΥΕΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑ

1.1 Εισαγωγή

Το Διαδίκτυο των Πραγμάτων (ΔτΠ) αναφέρεται σε μια έννοια συνδεδεμένων αντικειμένων και συσκευών όλων των ειδών μέσω του Διαδικτύου, ενσύρματα ή ασύρματα. Το ΔτΠ έχει αυξήσει τη δημοτικότητά του γρήγορα, καθώς χρησιμοποιείται για διάφορους σκοπούς, συμπεριλαμβανομένης της επικοινωνίας, των μεταφορών, της εκπαίδευσης και της επιχειρηματικής ανάπτυξης. Το ΔτΠ εισήγαγε την έννοια της υπερσυνδεσιμότητας, που σημαίνει ότι άνθρωποι και οργανισμοί ή εταιρείες μπορούν να επικοινωνούν μεταξύ τους από απομακρυσμένες τοποθεσίες χωρίς ιδιαίτερο κόπο. Το 1999 επινοήθηκε ο όρος «ΔτΠ» από τον Kevin Ashton με σκοπό να γίνει προώθηση της έννοιας της Αναγνώρισης Ραδιοσυχνοτήτων (RFID), η οποία περιλαμβάνει ενσωματωμένους αισθητήρες και αναγνώστες. Η αρχική ιδέα ωστόσο εισήχθη μεταξύ του 1960-1970. Κατά τη διάρκεια αυτής της περιόδου, η ιδέα ονομαζόταν διάχυτος υπολογισμός ή ενσωματωμένο Διαδίκτυο. Το 2011 και με την εισαγωγή του οικιακού αυτοματισμού, των φορητών συσκευών και των έξυπνων μετρητών ενέργειας, τα πράγματα άλλαξαν εντελώς και η δημοτικότητα της έννοιας ΔτΠ εκτοξεύτηκε. Η ταχεία έκρηξη του ΔτΠ ωφέλησε τους οργανισμούς και με διάφορους τρόπους βελτίωσε την έρευνα αγοράς και τις επιχειρηματικές στρατηγικές [1]. Ομοίως, το ΔτΠ έχει βελτιώσει τον τρόπο ζωής των ατόμων με την εισαγωγή αυτοματοποιημένων υπηρεσιών. Ωστόσο, αυτού του είδους η ανεξέλεγκτη αύξηση της χρήσης των ΔτΠ συσκευών, έχει προκαλέσει ανησυχία για τις προκλήσεις που δημιουργούνται στην ιδιωτική ζωή και ασφάλεια.

Όλο και περισσότερες πλέον συσκευές και μηχανές χρειάζονται ανάδραση για να διευκολύνουν και να βελτιώσουν τις υπηρεσίες τους, και είναι πραγματικά ελάχιστες εκείνες που πλέον δεν χρειάζονται τον απομακρυσμένο έλεγχο ή την ανταλλαγή πληροφοριών.

Οι συσκευές ΔτΠ είναι ευάλωτες σε επιθέσεις στον κυβερνοχώρο λόγω αδύναμων πρωτοκόλλων και πολιτικών ασφαλείας. Οι hacker έχουν αναπτύξει διάφορα είδη κακόβουλου λογισμικού για να μολύνουν συσκευές ΔτΠ και έχουν χρησιμοποιήσει διαφορετικές τεχνικές ψαρέματος (phishing) για να προκαλέσουν εργαζόμενους ή άτομα να μοιράζονται ευαίσθητα δεδομένα. Εάν οι κατασκευαστές συσκευών και οι ειδικοί σε θέματα ασφάλειας αξιολογήσουν με ακρίβεια τις απειλές στον κυβερνοχώρο, μπορούν να αναπτύξουν έναν αποτελεσματικό προστατευτικό μηχανισμό για την πρόληψη ή την εξουδετέρωση των απειλών στον κυβερνοχώρο.

Οι συσκευές του ΔτΠ έχουν χρησιμοποιηθεί εκτενώς σε βιομηχανικές εφαρμογές και για επαγγελματικούς σκοπούς. Ενώ οι εφαρμογές βοηθούν αυτές τις επιχειρήσεις να αποκτήσουν ανταγωνιστικό πλεονέκτημα, η υπερβολική υιοθέτηση διαφόρων έξυπνων συσκευών με κοινή χρήση και ενοποίηση δεδομένων έχει οδηγήσει σε ανησυχίες για παραβίαση του απορρήτου των δεδομένων. Είναι σημαντικό να υπάρχουν επαγγελματίες στο χώρο της ασφάλειας, για την ανάπτυξη ολοκληρωμένων μέτρων και πολιτικών ασφάλειας για την προστασία των επιχειρήσεων και τη διασφάλιση της συνέχειας των υπηρεσιών [2]. Για παράδειγμα, οι έξυπνες συσκευές οικιακής χρήσης με δυνατότητα ΔτΠ που είναι συνδεδεμένες στο τοπικό δίκτυο μπορούν να αποτελέσουν πηγή παραβίασης για τους hacker για να αποκτήσουν πρόσβαση στην επιχείρηση ή/και προσωπικά ευαίσθητα δεδομένα ή να χειραγωγήσουν και να διακόψουν τη ροή εργασιών της επιχείρησης.

Στη παρούσα διπλωματική δημιουργήθηκε ένα πλαίσιο για τη μελέτη και την περαιτέρω ανάπτυξη βέλτιστων πρακτικών ασφαλείας είτε με την εφαρμογή και ανάλυση των υφιστάμενων τεχνολογιών,

είτε με την ανάπτυξη νέων, όπως αυτή του IOTA. Με βάση τα ευρήματα, παρέχεται σύσταση για την αποφυγή τέτοιων κινδύνων και για την αποκατάσταση των πιθανών τρωτών σημείων ασφαλείας.

1.2 Ασφάλεια

Οι συσκευές στο ΔτΠ διαφέρουν από τους παραδοσιακούς υπολογιστές και τις υπολογιστικές συσκευές, κυρίως ως προς τη μικρή υπολογιστική τους δύναμη καθώς και το μικρό τους ενεργειακό αποτύπωμα, γεγονός που τις καθιστά πιο ευάλωτες στις προκλήσεις ασφαλείας. Για παράδειγμα, πολλές συσκευές στο ΔτΠ έχουν σχεδιαστεί για να αναπτύσσονται σε τεράστια κλίμακα, όπως οι έξυπνοι αισθητήρες. Αυτό ενισχύει την πιθανότητα ευπάθειας της ασφάλειάς τους. Επιπλέον, πολλά ιδρύματα και οργανισμοί, έχουν καταλήξει σε οδηγούς για τη διεξαγωγή αξιολογήσεων κινδύνου. Αυτό είναι απαραίτητο επειδή ο αριθμός των διασυνδεδεμένων συσκευών ΔτΠ είναι τεράστιος. Συνήθως, αυτές οι συσκευές επικοινωνούν με αρχιτεκτονική Publish-Subscribe, με σκοπό την ένταξη τους σε ένα έξυπνο περιβάλλον. Αυτό απαιτεί εξέταση των διαθέσιμων εργαλείων, τεχνικών και τακτικών που σχετίζονται με την ασφάλεια του ΔτΠ [3].

Παρόλο που το ζήτημα της ασφάλειας στον τομέα της πληροφορίας και της τεχνολογίας δεν είναι νέο, η εφαρμογή του ΔτΠ έχει παρουσιάσει μοναδικές προκλήσεις που πρέπει να αντιμετωπιστούν. Οι καταναλωτές θα πρέπει να μπορούν να εμπιστεύονται το ΔτΠ, τις συσκευές και τις υπηρεσίες του. Με ανεπαρκώς προστατευμένες συσκευές και υπηρεσίες ΔτΠ, αυτή είναι μια από τις πιο σημαντικές οδούς που χρησιμοποιούνται για επιθέσεις στον κυβερνοχώρο καθώς και για τη κλοπή των δεδομένων των χρηστών αφήνοντας τις ροές δεδομένων απροστάτευτες.

Υπάρχουν διάφορα τρωτά σημεία ελέγχου ταυτότητας στο ΔτΠ που το αφήνουν ανοιχτό σε επιθέσεις. Ένα από τα πιο σημαντικά ζητήματα είναι η έλλειψη προστασίας έναντι πολλαπλών απειλών. Η ασφάλεια των πληροφοριών είναι επομένως μια σημαντική ευπάθεια στον έλεγχο ταυτότητας του ΔτΠ. Για παράδειγμα, οι ανέπαφες πιστωτικές κάρτες μπορούν να χρησιμοποιηθούν για την ανάγνωση αριθμών και ονομάτων καρτών χωρίς την ανάγκη ελέγχου ταυτότητας, δίνοντας τη δυνατότητα στους hacker να αγοράζουν αγαθά χρησιμοποιώντας τον τραπεζικό λογαριασμό κάποιου άλλου. Μια άλλη διαδεδομένη επίθεση είναι η επίθεση “man in the middle”, όπου ένα τρίτο μέρος κλέβει το κανάλι επικοινωνίας για να πλαστογραφήσει τις ταυτότητες των κόμβων που εμπλέκονται στην ανταλλαγή. Αυτό επιτρέπει ουσιαστικά στον διακομιστή της τράπεζας να αναγνωρίσει τη συναλλαγή ως έγκυρη, παρόλο που δεν είναι.

1.3 Απόρρητο

Η χρησιμότητα του ΔτΠ εξαρτάται από το πόσο καλά σέβεται τις επιλογές απορρήτου των ανθρώπων. Ωστόσο, οι ανησυχίες για τις πιθανές βλάβες που συνοδεύουν το ΔτΠ ενδέχεται να εμποδίσουν την πλήρη υιοθέτησή του. Είναι σημαντικό να υπάρχει γνώση και σεβασμός ως προς τα δικαιώματα του απορρήτου των χρηστών, η οποία είναι θεμελιώδης για τη διασφάλιση της εμπιστοσύνης και της αυτοπεποίθησης των χρηστών στο ΔτΠ, στη συνδεδεμένη συσκευή και στις σχετικές υπηρεσίες που προσφέρονται. Καταβάλλεται μεγάλη προσπάθεια για να διασφαλιστεί ότι το ΔτΠ επαναπροσδιορίζει τα ζητήματα απορρήτου, όπως η μείωση της επιτήρησης και της παρακολούθησης. Ενισχύονται οι ανησυχίες για το απόρρητο λόγω της αύξησης της "νοημοσύνης" των συσκευών, όπου η διαδικασία δειγματοληψίας και η διανομή πληροφοριών στο ΔτΠ που μπορεί να γίνει σχεδόν οπουδήποτε. Η συνεχής σύνδεση των συσκευών μέσω της πρόσβασης στο Διαδίκτυο είναι επίσης ένας ουσιαστικός παράγοντας που βοηθά στην κατανόηση αυτού του προβλήματος, διότι εάν δεν υπάρχει ένας μοναδικός μηχανισμός, θα είναι αναμφισβήτητα πιο εύκολη η πρόσβαση σε προσωπικές πληροφορίες από οποιαδήποτε γωνιά του κόσμου.

1.4 Πολιτικές ασφάλειας και απορρήτου

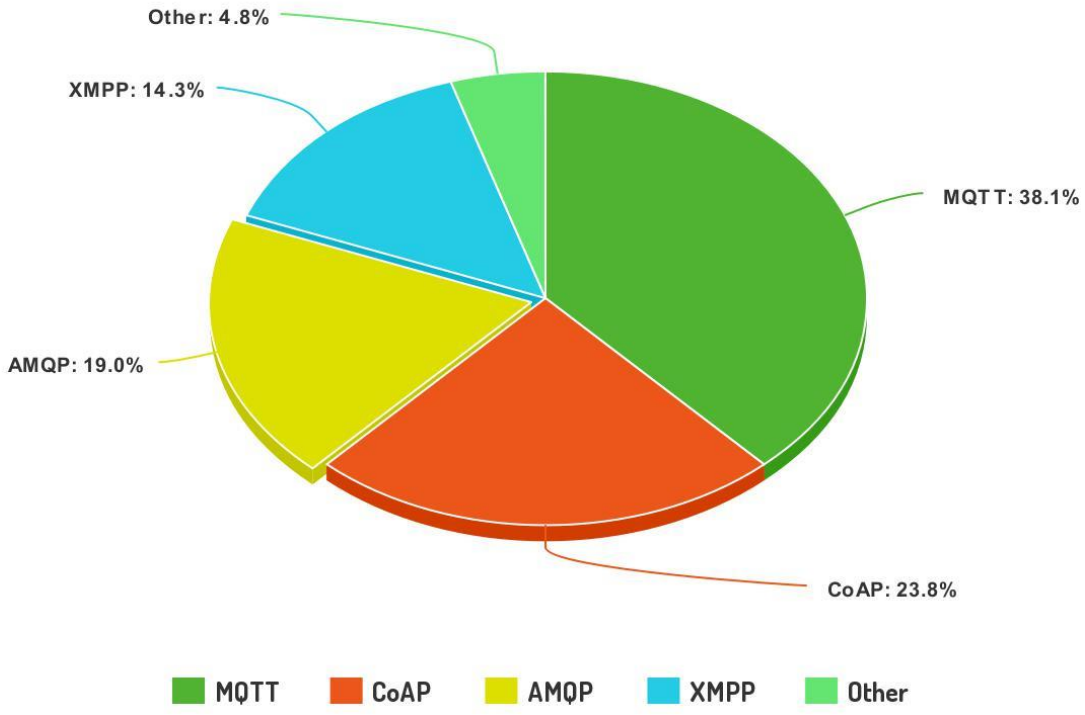
Οι υπηρεσίες που βασίζονται στο cloud είναι απαραίτητες για το ΔτΠ, παρέχοντας αποθήκευση, επεξεργασία και κοινή χρήση δεδομένων. Ωστόσο, εισάγουν επίσης νέες προκλήσεις ασφαλείας, καθώς κακόβουλοι παράγοντες στοχεύουν ευάλωτους στόχους, όπως συσκευές ΔτΠ που κάνουν συλλογή φυσικών παραμέτρων (π.χ. θερμοκρασία, υγρασία) και προώθηση δεδομένων σε υπηρεσίες νέφους. Μπορούν να ληφθούν διάφορα μέτρα για τη βελτίωση της ασφάλειας, όπως η διασφάλιση κρυπτογράφησης των δεδομένων και η χρήση πιστοποιητικών για την εμπιστοσύνη συγκεκριμένων διακομιστών. Ωστόσο, αυτά τα μέτρα βαρύνουν την κατανάλωση ενέργειας για τις συσκευές που λειτουργούν με μπαταρία (low power consumption devices).

Εν κατακλείδι, όπως με κάθε νέα τεχνολογία, έτσι και στο ΔτΠ απαιτείται προσαρμοστικότητα στο επίπεδο της ασφάλειας και στα μέτρα που λαμβάνονται για την αντιμετώπιση αυτών των προκλήσεων.

1.5 MQTT

1.5.1 Εισαγωγή

Το Διαδίκτυο των Πραγμάτων (ΔτΠ) επιτρέπει σε κόμβους ΔτΠ, να συλλέγουν και να μοιράζονται δεδομένα με άλλες συσκευές και υπηρεσίες στο διαδίκτυο χωρίς ανθρώπινη παρέμβαση. Για να καταστεί δυνατή η ασφαλής και αξιόπιστη ανταλλαγή δεδομένων μεταξύ κόμβων ΔτΠ, έχουν αναπτυχθεί διάφορα πρωτόκολλα επικοινωνίας και ανταλλαγής μηνυμάτων, όπως το Πρωτόκολλο Περιορισμένης Εφαρμογής (Constrained Application Protocol - CoAP), το Προηγμένο Πρωτόκολλο Ουράς Μηνυμάτων (Advanced Message Queuing Protocol - AMQP), Πρωτόκολλο μεταφοράς τηλεμετρίας σε ουρά μηνυμάτων (Message Queuing Telemetry Transport - MQTT) και το πρωτόκολλο επεκτάσιμης παρουσίας μηνυμάτων (Extensible Messaging and Presence Protocol - XMPP) [4] . Μεταξύ όλων, το MQTT έχει χρησιμοποιηθεί ευρέως σε διάφορα έξυπνα περιβάλλοντα όπως οι έξυπνες κατοικίες (smart home), η έξυπνη αγροτική καλλιέργεια (smart agriculture), οι βιομηχανικοί αυτοματισμοί (industrial automations), κ.λπ. Κατά κύριο λόγο η αρχιτεκτονική που χρησιμοποιείται για την υλοποίηση smart environments, είναι η αρχιτεκτονική Pub/Sub. Το πιο δημοφιλές από αυτά τα πρωτόκολλα είναι το MQTT [5].



Εικόνα 1 - Στατιστικός πίνακας σύγκρισης πρωτοκόλλων

Οι λόγοι που το καθιστούν το πιο δημοφιλές πρωτόκολλο, περιλαμβάνουν χαμηλές υπολογιστικές και ενεργειακές απαιτήσεις, καθώς και χαμηλό ρυθμό μετάδοσης δεδομένων. Το πρωτόκολλο επικοινωνίας MQTT αποτελείται από τέσσερα κύρια στοιχεία, τους **Διαμεσολαβητές** (Brokers), τους **Πελάτες** (Clients), τα **Θέματα** (Topics) και τα **Μηνύματα** (Messages). Τα θέματα στο MQTT πρωτόκολλο, δομούνται με δενδροειδή μορφή παρόμοια με αυτά που χρησιμοποιείται σε ένα file system. Συνήθως περιέχουν πληροφορίες σχετικά με τη προέλευση ή τον τύπο των μετρήσεων. Παρακάτω θα δοθούν παραδείγματα αναφορικά με τη δενδροειδή μορφή.

1.5.2 Βασικές κατηγορίες συμμετεχόντων

Στο MQTT υπάρχουν δύο διαφορετικές κατηγορίες συμμετεχόντων:

Α. **SERVER**

Ο server στο MQTT ονομάζεται Broker (μεσολαβητής), και αποτελεί το κεντρικό σημείο της τοπολογίας αστέρα (εικόνα 1). Είναι υπεύθυνος για την Αυθεντικοποίηση (Authentication), την εξουσιοδότηση (Authorisation) και τη Λίστα Ελέγχου Πρόσβασης (Access Control List).

Είναι το μοναδικό σημείο σύνδεσης για όλους τους άλλους συμμετέχοντες, επομένως είναι επίσης υπεύθυνο για την πιστοποίησή τους (Authentication).

Αποτελεί το κεντρικό στοιχείο της υλοποίησης του MQTT. Είναι υπεύθυνος για τη λήψη μηνυμάτων από τους Publishers (αποστολείς μηνυμάτων) και την προώθησή τους στους subscribers (συνδρομητές). Ο broker πρέπει να υποστηρίζει το πρωτόκολλο MQTT και να μπορεί να χειριστεί μεγάλο αριθμό ταυτόχρονων συνδέσεων. Υπάρχουν διαθέσιμες υλοποιήσεις MQTT Brokers ανοικτού κώδικα, συμπεριλαμβανομένων των Eclipse Mosquitto, HiveMQ - open source Java implementation of the MQTT broker specification- και EMQ X. Διατίθενται επίσης commercial brokers MQTT, όπως οι Amazon Web Services IoT Core και Microsoft Azure IoT Hub. Γενικότερο, γύρω από το οικοσύστημα του MQTT, συνυπάρχουν πληθώρα υπηρεσιών και λογισμικών τόσο ανοικτού κώδικα όσο και μή-ανοικτού κώδικα.

Authentication:

Η πιστοποίηση ταυτότητας, ή αλλιώς αυθεντικοποίηση (authentication), αποτελεί μέρος της ασφάλειας σε επίπεδο μεταφοράς δεδομένων στο MQTT. Με το Transport Layer Security (TLS), η επιτυχής επικύρωση ενός πιστοποιητικού πελάτη χρησιμοποιείται για την αυθεντικοποίησή του στον διακομιστή. Σε επίπεδο εφαρμογής, το πρωτόκολλο MQTT παρέχει όνομα χρήστη και κωδικό πρόσβασης για έλεγχο ταυτότητας. Ο κάθε χρήστης συνίσταται να έχει μοναδικό όνομα χρήστη και κωδικό πρόσβασης.

Authorization:

Η εξουσιοδότηση (authorization) καθορίζει τα δικαιώματα πρόσβασης σε έναν πόρο (resource). Περιλαμβάνει τον ορισμό και την επιβολή των πολιτικών που ελέγχουν τα δικαιώματα σε ένα συγκεκριμένο πόρο. Βασικά μέρη της εξουσιοδότησης αποτελούν οι ακόλουθοι όροι:

- Θέμα ή χρήστης που αναζητεί πρόσβαση σε έναν πόρο.
- Πόρος, αντικείμενο ή υπηρεσία που πρέπει να προστατευτεί από μη εξουσιοδοτημένη πρόσβαση.
- Πολιτική που καθορίζει τη πρόσβαση σε έναν πόρο.

Συνήθως χρησιμοποιούνται διάφοροι τύποι εξουσιοδότησης.

Ακρωνύμιο	Όνομα	Περιγραφή
ACL	Access Control List	Μια ACL περιλαμβάνει τα δικαιώματα που μπορεί να έχει ένας πόρος. Δικαίωμα αποτελεί το ποιος μπορεί να έχει πρόσβαση στον πόρο (π.χ. σε συγκεκριμένο topic) και ποιες είναι οι επιτρεπόμενες λειτουργίες (π.χ. publish, subscribe).
RBAC	Role Based Access Control	Το RBAC κάνει συσχέτιση των δικαιωμάτων ενός ή περισσοτέρων πόρων με έναν ρόλο. Σε κάθε ρόλο μπορούν να ενταχθούν ένας ή περισσότεροι χρήστες. Έτσι, είναι ευκολότερο να συσχετίζονται οι χρήστες με ρόλους παρά να δημιουργούνται νέες εγγραφές δικαιωμάτων για μεμονωμένους χρήστες.

Πίνακας 1 - Επεξήγηση ACL/RBAC

Encryption:

Η κρυπτογράφηση αποτελεί το πιο σημαντικό κομμάτι ασφαλείας που γνωρίζουμε σήμερα για ανταλλαγή ψηφιακών πληροφοριών. Εντούτοις το MQTT, δεν υποστηρίζει εγγενώς κάποιου είδους κρυπτογράφηση. Αντ' αυτού, χρησιμοποιούνται τα δοκιμασμένα και αξιόπιστα πρωτόκολλα SSL(Secure Sockets Layer) και TLS (Transport Layer Security), σε ξεχωριστό επίπεδο πάνω από το MQTT (MQTT over SSL.). Για να υπάρξει κρυπτογράφηση γίνεται χρήση πιστοποιητικών (certificates).

Το TLS/SSL παρέχει ένα ασφαλές κανάλι επικοινωνίας μεταξύ ενός πελάτη και ενός διακομιστή. Στον πυρήνα του, το TLS/SSL είναι κρυπτογραφικό πρωτόκολλο που χρησιμοποιεί έναν μηχανισμό "ταυτοποίησης" (handshake mechanism) για τη διαπραγμάτευση διαφόρων παραμέτρων ώστε να δημιουργηθεί μια ασφαλής σύνδεση μεταξύ του πελάτη και του διακομιστή. Αφού ολοκληρωθεί η ταυτοποίηση, δημιουργείται μια κρυπτογραφημένη επικοινωνία μεταξύ πελάτη και διακομιστή και κανένας τρίτος (man in the middle) δεν μπορεί να υποκλέψει οποιοδήποτε μέρος της επικοινωνίας. Οι διακομιστές παρέχουν ένα πιστοποιητικό X509 (που συνήθως εκδίδεται από μια αξιόπιστη αρχή και ονομάζεται Certificate Authority-CA), το οποίο οι πελάτες χρησιμοποιούν για να επαληθεύσουν την ταυτότητα του διακομιστή. Αυτός ο τρόπος κρυπτογράφησης ονομάζεται και one-way

encryption, αφού ο διακομιστής δημιουργεί ένα ζεύγος κλειδιών (private και public) και οι πελάτες λειτουργούν με βάση το public key του διακομιστή. Στην άλλη περίπτωση, με τη χρήση του 2 way certificate authentication, τόσο ο διακομιστής όσο και οι πελάτες διαθέτουν δικά τους private και public κλειδιά τα οποία χρησιμοποιούν για αμφίδρομη και ισχυρότερη κρυπτογράφηση.

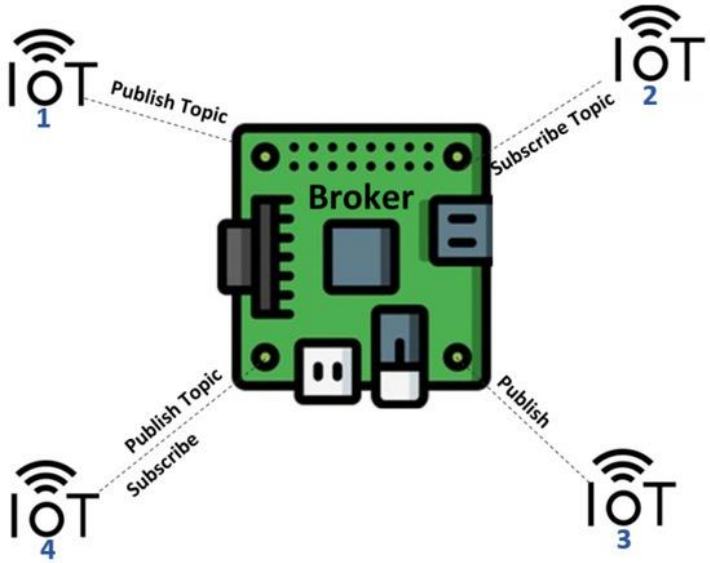
Παράδειγμα 1

Ένας διακομιστής χρησιμοποιεί one-way certificate authentication. Προκειμένου να λάβει μια κρυπτογραφημένη πληροφορία από ένα ή περισσότερους clients, μοιράζεται μαζί τους το public key που έχει δημιουργήσει. Οι clients κρυπτογραφούν το μήνυμα που θέλουν να στείλουν, το στέλνουν στο διακομιστή, και αυτός με τη σειρά του μπορεί να αποκρυπτογραφήσει το μήνυμα με βάση το private κλειδί που διαθέτει.

Στην άλλη περίπτωση, όπου είναι απαραίτητη η αμφίδρομη επικοινωνία μεταξύ διακομιστή-πελατών, ο κάθε πελάτης θα πρέπει να διαθέτει και αυτός ζεύγος κλειδιών private-public. Έτσι ο διακομιστής, θα γνωρίζει όλα τα public keys των πελατών, και όλοι οι πελάτες το public key του διακομιστή. Έτσι, δημιουργείται μια αμφίδρομη κρυπτογραφημένη επικοινωνία.

B. **CLIENTS**

Ένας Client στο MQTT θα μπορούσε να είναι μόνο Publisher, μόνο Subscriber ή και τα δύο. Οι Publishers, μεταδίδουν δεδομένα στον Broker, σε συγκεκριμένα Topics στα οποία είναι εξουσιοδοτημενοι. Η δουλειά του Broker είναι να ενημερώνει τους εξουσιοδοτημένους Subscribers (συνδρομητές) που ενδιαφέρονται για ένα topic, στέλνοντάς τους τα αντίστοιχα μηνύματα.



Εικόνα 2 - Τοπολογία αστέρα MQTT[1]

[1] Khan, M. A., Khan, M. A., Jan, S. U., Ahmad, J., Jamal, S. S., Shah, A. A., ... & Buchanan, W. J. (2021). A deep learning-based intrusion detection system for mqtt enabled iot. *Sensors*, *21*(21), 7016

Όσοι ενδιαφέρονται να ενημερώνονται για τα μηνύματα ενός topic θα πρέπει να είναι εγγεγραμμένοι σε αυτό εφόσον βρίσκονται στο access control list του Broker.

Υπηρεσία δημοσίευσης/συνδρομής (publish/subscribe):

Ο όρος "μήνυμα" αναφέρεται στα δεδομένα που περνούν μέσα από μια υπηρεσία ανταλλαγής μηνυμάτων pub/sub. Το θέμα (topic) είναι μια ονομαστική οντότητα που υποδηλώνει μια ουρά μηνυμάτων που τροφοδοτεί τους εγγεγραμμένους συνδρομητές και η "συνδρομή" δηλώνει το ενδιαφέρον για τη λήψη μηνυμάτων για ένα συγκεκριμένο θέμα. Μια συσκευή ή ένα λογισμικό αναφέρεται ως publisher εάν δημιουργεί μηνύματα και τα δημοσιεύει στην υπηρεσία ανταλλαγής μηνυμάτων για ένα συγκεκριμένο θέμα. Μια συσκευή ή ένα πρόγραμμα αναφέρεται ως subscriber εάν λαμβάνει μηνύματα για ένα συγκεκριμένο topic.

1.5.3 Ασφάλεια

Μελέτες έχουν δείξει ότι οι επιτιθέμενοι στοχεύουν συνήθως κεντρικές συσκευές επικοινωνίας, όπως brokers, σε συστήματα ΔτΠ που βασίζονται σε MQTT. Denial-of-Service (DoS), Man-in-the-Middle (MitM), σάρωση και Intrusion είναι μερικά παραδείγματα κοινών επιθέσεων σε brokers. Κατ 'αρχήν, ο πελάτης MQTT ξεκινά μια σύνδεση με έναν broker στέλνοντας ένα πακέτο σύνδεσης και, καθώς το MQTT λειτουργεί πάνω από το TCP/IP, ο broker στέλνει επιβεβαίωση σύνδεσης (connack). Εφόσον πραγματοποιηθεί η λήψη της επιβεβαίωσης, ο πελάτης τότε μπορεί να ξεκινήσει τη μετάδοση δεδομένων στον broker. Το πρωτόκολλο MQTT μπορεί να παρέχει τρία επίπεδα Ποιότητας Υπηρεσίας (QoS) που καθορίζουν το επίπεδο συμφωνίας και τη διασφάλιση της επιτυχούς επικοινωνίας μεταξύ πομπού και δέκτη στο δίκτυο [6].

Το επίπεδο QoS-0 δεν έχει μηχανισμό επιβεβαίωσης στην επικοινωνία μεταξύ αποστολέα και παραλήπτη. Επιπλέον, ένας εσωτερικός εισβολέας στέλνει πολλαπλά μηνύματα με QoS-1 και QoS-2 για να απασχολήσει τον broker με επιβεβαιώσεις, επιβάλλοντας έτσι μια επίθεση DoS.

Ο προεπιλεγμένος τρόπος ελέγχου ταυτότητας στο MQTT βασίζεται σε ένα σχήμα χρήστη-συνθηματικού και ο κωδικός πρόσβασης αποστέλλεται σε καθαρό κείμενο. Δίνεται να καθοριστεί ένας εξωτερικός εναλλακτικός μηχανισμός ελέγχου ταυτότητας όπως οι Salted Challenge Response Authentication Mechanism - SCRAM, Generic Security Service Application Program Interface - GSSAPI (Kerberos) κ.λπ..

Οι MQTT brokers μπορούν επίσης να υποστηρίζουν πρόσθετα χαρακτηριστικά, όπως πιστοποίηση ταυτότητας, κρυπτογράφηση και retained μηνύματα. Ο έλεγχος ταυτότητας επιτρέπει στις συσκευές να πιστοποιούνται στον broker χρησιμοποιώντας ονόματα χρήστη και κωδικούς πρόσβασης, πιστοποιητικά. Η κρυπτογράφηση διασφαλίζει ότι τα μηνύματα μεταδίδονται με ασφάλεια μέσω του δικτύου, αποτρέποντας την υποκλοπή και την παραποίηση. Το retained message, γνωστό και ως last known good value, επιτρέπει στους brokers να αποθηκεύουν το τελευταίο γνωστό μήνυμα σε περίπτωση που οι συνδρομητές δεν είναι διαθέσιμοι και να τα παραδίδουν αργότερα όταν συνδεθούν. Αυτή η διαδικασία, επιτυγχάνεται απο τον publisher, ο οποίος αλλάζοντας τη κατάσταση του “retained message flag”, ειδοποιεί τον broker οτι το μήνυμα που θα σταλεί, θα πρέπει να κρατηθεί για να αποσταλεί αργότερα, σε περίπτωση αποτυχίας παράδοσης.

Για μεγάλες υλοποιήσεις, όπου οι απαιτήσεις αυξάνονται, χρειάζονται δύο ή περισσότεροι brokers οι οποίοι λειτουργούν γεφυρωμένοι (bridged).

1.5.4 Επίπεδα Ποιότητας Υπηρεσίας - QoS

Το MQTT υποστηρίζει τρία επίπεδα QoS, τα οποία καθορίζουν την αξιοπιστία της παράδοσης των μηνυμάτων:

QoS 0: Παράδοση το πολύ μία φορά. Ο broker παραδίδει το μήνυμα στον subscriber μία φορά, αλλά δεν εγγυάται ότι το μήνυμα ελήφθη ή επεξεργάστηκε από τον subscriber.

QoS 1: Παράδοση τουλάχιστον μία φορά. Ο broker παραδίδει το μήνυμα στον συνδρομητή τουλάχιστον μία φορά, εξασφαλίζοντας ότι το μήνυμα δεν χάνεται, αλλά μπορεί να παραδοθεί πολλές φορές εάν ο συνδρομητής δεν επιβεβαιώσει την παραλαβή του μηνύματος.

QoS 2: παράδοση ακριβώς μία φορά. Ο broker και ο συνδρομητής ανταλλάσσουν μηνύματα για να διασφαλίσουν ότι το μήνυμα παραδίδεται ακριβώς μία φορά, εξασφαλίζοντας την αξιοπιστία της παράδοσης του μηνύματος, αλλά με μεγαλύτερη επιβάρυνση από τα QoS 0 και QoS 1.

1.5.5 Δομή εντολής-μηνύματος

Η εργαλειοθήκη του mosquitto eclipse δίνει τη δυνατότητα πειραματισμού και αποσφαλμάτωσης με χρήση των command line εργαλείων mosquitto_pub και mosquitto_sub, καθώς μπορεί να γίνει αποστολή και λήψη δοκιμαστικών μηνυμάτων. Προϋπόθεση είναι να υπάρχει ήδη κάποια δημόσια ή ιδιωτική υπηρεσία MQTT broker.

Παρακάτω παρατίθενται δυο παραδείγματα για Publish και Subscribe μέσω terminal σε τοπικό MQTT broker.

Παράδειγμα 1. Δημοσίευση μηνύματος σε Topic.

Publish: **mosquitto_pub -h localhost -p 1883 -u username -P mypassword -t devicexyz/temperature -m 18.0°C**

Παράδειγμα 2. Εγγραφή σε Topic και λήψη μηνύματος.

Subscribe: **mosquitto_sub -h localhost -p 1883 -u username -P mypassword -t devicexyz/temperature**

Δύο διαφορετικά προγράμματα/εντολές που φαίνονται στον παρακάτω πίνακα χρησιμοποιούνται για να γίνει publish ή subscribe ένα μήνυμα σε ένα topic και είναι πανομοιότυπες.

Εντολές/Παράμετροι	Επεξήγηση
mosquitto_pub	Το Command line εργαλείο χρησιμοποιείται για τη δημοσίευση ενός μηνύματος σε ένα topic
mosquitto_sub	Το Command line εργαλείο χρησιμοποιείται για την εγγραφή σε ένα topic ενδιαφέροντος. Όταν ληφθεί ένα μήνυμα από το broker, αυτός το προωθεί στους εγγεγραμμένους χρήστες
-h localhost	Η παράμετρος -h υποδηλώνει ότι πρόκειται να ακολουθήσει υποχρεωτικά η IP του "host", δηλαδή η διεύθυνση του broker από την οποία θα λάβουμε, ή θα αποστείλουμε μήνυμα. Στο συγκεκριμένο παράδειγμα το localhost αναφέρεται σε broker τον οποίο χρησιμοποιούμε στο τοπικό μας υπολογιστή. Αντί του localhost θα μπορούσε να χρησιμοποιηθεί μία IP ή κάποιο domain name.
-p 1883	Η παράμετρος -p (πεζό) δηλώνει ότι πρόκειται να ακολουθήσει η πόρτα (port) που ακούει ο server. Η πόρτα 1883 είναι η προεπιλεγμένη (default) πόρτα του MQTT Broker χωρίς SSL/TLS.
-u username	Με τη παράμετρο -u δηλώνουμε ότι θα ακολουθήσει υποχρεωτικά το όνομα χρήστη που έχουμε επιλέξει. Στη παράμετρο username τοποθετείται το όνομα χρήστη
-P password	Η παράμετρος -P (κεφαλαίο) δηλώνει ότι θα ακολουθήσει υποχρεωτικά ο κωδικός χρήστη που έχει επιλεχθεί. Στη παράμετρο password τοποθετείται ο κωδικός χρήστη
-t devicexyz/temperature	Στο MQTT, ένα θέμα είναι σαν μια ειδική λέξη που βοηθά έναν broker να καταλάβει ποια μηνύματα πρέπει να στείλει σε κάποιον. Το θέμα αποτελείται από λέξεις που χωρίζονται με μια κάθετο, από τη παράμετρο -t.
-m 18.0°C	Η παράμετρος -m χρησιμοποιείται μόνο όταν γίνεται δημοσίευση μηνύματος (mosquitto_pub) και δηλώνει ότι πρόκειται να ακολουθήσει το μήνυμα που θέλουμε να στείλουμε. Το μήνυμα που ακολουθεί σε αυτή τη περίπτωση μπορεί να βρίσκεται μέσα σε εισαγωγικά εάν υπάρχουν κενά στη πρόταση που θέλουμε να αποσταλεί..

Πίνακας 2 - Επεξήγηση εντολών Publish/Subscribe στη γραμμή εντολών

Εκτός από την ύπαρξη των command line εργαλείων, υπάρχουν και αρκετές βιβλιοθήκες σε πληθώρα γλωσσών προγραμματισμού. για να την υλοποίηση των clients.

Στη παρούσα διπλωματική έγινε χρήση του MQTT με τη χρήση της γλώσσας python και του προγραμματιζόμενου επεξεργαστή ESP8266 (NodeMCU), κατάλληλου για μικρές ΔτΠ εφαρμογές, ως αποστολέας μηνυμάτων από τον αισθητήρα θερμοκρασίας. Τα μηνύματα λαμβάνονται από τον cloud server που λειτουργεί σε καθεστώς subscriber, χρησιμοποιώντας γλώσσα Javascript σε περιβάλλον Node.js.

1.5.6 Υλοποίηση του MQTT

Η υλοποίηση του MQTT περιλαμβάνει διάφορα στοιχεία, συμπεριλαμβανομένου του **MQTT client**, του **MQTT Broker** και της υποκείμενης υποδομής δικτύου. Σε αυτή την ενότητα, γίνεται μια εισαγωγή στην υλοποίηση του MQTT, συμπεριλαμβανομένων των βιβλιοθηκών πελάτη, του λογισμικού broker και των εκτιμήσεων για το δίκτυο.

Οι βιβλιοθήκες MQTT client είναι διαθέσιμες σε πολλές γλώσσες προγραμματισμού, καθιστώντας εύκολη την ενσωμάτωση του MQTT στις εφαρμογές τους από τους προγραμματιστές. Αυτές οι βιβλιοθήκες παρέχουν ένα απλό API για την αποστολή και τη λήψη μηνυμάτων MQTT, καθώς και τη διαχείριση της σύνδεσης και το χειρισμό σφαλμάτων. Παραδείγματα δημοφιλών βιβλιοθηκών-πελατών MQTT περιλαμβάνουν το Paho MQTT για Java και Python, το MQTT.js για Node.js και το Eclipse Mosquitto για C/C++.

Κατά την εφαρμογή του MQTT, είναι σημαντικό να ληφθεί υπόψη η υποδομή δικτύου. Τα μηνύματα MQTT μεταδίδονται μέσω TCP/IP, το οποίο παρέχει αξιόπιστη μεταφορά, αλλά μπορεί να υποφέρει από καθυστέρηση και απώλεια πακέτων σε ορισμένες συνθήκες δικτύου. Για να διασφαλιστεί η αξιόπιστη παράδοση μηνυμάτων, το MQTT υποστηρίζει τρία επίπεδα ποιότητας υπηρεσίας (QoS), όπως συζητήθηκε στην προηγούμενη ενότητα. Είναι σημαντικό να γίνει επιλογή του κατάλληλου επιπέδου QoS για κάθε μήνυμα με βάση τη σημασία του και τις συνθήκες του δικτύου.

Επιπλέον, το MQTT μπορεί να υλοποιηθεί μέσω διαφορετικών πρωτοκόλλων μεταφοράς, όπως

α) MQTT over TCP/IP,

β) MQTT over TCP/IP with SSL/TLS support (MQTTS),

γ) MQTT over WebSockets και

δ) MQTTS over WebSockets.

Το MQTTS παρέχει ένα ασφαλές κανάλι επικοινωνίας, κρυπτογραφώντας τα δεδομένα που μεταδίδονται μεταξύ του πελάτη και του broker, αποτρέποντας την υποκλοπή και την παραποίηση. Η υλοποίηση του MQTTS απαιτεί την απόκτηση και εγκατάσταση ψηφιακών πιστοποιητικών και τη παραμετροποίηση του broker και του client, ώστε να είναι σε θέση να χρησιμοποιηθεί.

MQTT-SN (MQTT για Sensor Networks)

Επειδή υπάρχει ένας αρκετά μεγάλος αριθμός από αισθητήρες στα δίκτυα αισθητήρων IOT, οι περισσότεροι από αυτούς μπορούν να συνδεθούν χωρίς τη χρήση καλωδίων, ασύρματα, με το πρωτόκολλο MQTT-SN.

Τα κύρια χαρακτηριστικά αυτών των δικτύων που οδήγησαν στο σχεδιασμό αυτό είναι τα εξής:

- Υπάρχουν μικρές συσκευές που λειτουργούν με μπαταρίες και δεν έχουν μεγάλη ισχύ ή αποθηκευτικό χώρο.
- Μπορούν να μεταφέρουν μόνο μια μικρή ποσότητα πληροφοριών κάθε φορά.
- Επίσης, μπαίνουν συχνά σε κατάσταση "ύπνου", ώστε να μειώνουν τη κατανάλωση ενέργειας.

Οι κύριες διαφορές του MQTT-SN με το MQTT είναι:

- Ελάττωση του μεγέθους του μηνύματος
- Κατάργηση της ανάγκης για μόνιμη σύνδεση με τη χρήση του UDP ως πρωτοκόλλου επικοινωνίας.

Μια άλλη πτυχή της υλοποίησης του MQTT είναι η διατήρηση των μηνυμάτων (Retained messages). Οι publishers όταν θεωρούν ότι ένα μήνυμα είναι σημαντικό, ενεργοποιούν το retained flag με το οποίο δίνουν εντολή στο MQTT Broker να αποθηκεύσει το συγκεκριμένο μήνυμα με σκοπό όλοι οι παλιοί ή νέοι subscribers που θα συνδεθούν, να ενημερωθούν χωρίς καθυστέρηση με το μήνυμα αυτό. Σε κάθε topic μπορεί να υπάρξει μόνο ένα retained μήνυμα. Εάν ο publisher στείλει εκ νέου μήνυμα με retained flag ενεργοποιημένο, το προηγούμενο μήνυμα αντικαθίσταται αυτομάτως. Για το λόγο αυτό το συγκεκριμένο μήνυμα εκτός από Retained Message, ονομάζεται και Last Known Good Value. Αν πρέπει να καταργηθεί το retained message σε ένα topic, θα πρέπει να σταλεί από τον publisher ένα κενό μήνυμα με το retained flag ενεργοποιημένο.

Άλλο ένα χαρακτηριστικό της υλοποίησης MQTT είναι οι persistent συνδέσεις των συνδρομητών. Με τη παράμετρο **CLEAN SESSION=0**, τότε η σύνδεση καθίσταται persistent. Το χαρακτηριστικό διασφαλίζει ότι τα μηνύματα δεν χάνονται ακόμη και αν ο συνδρομητής είναι προσωρινά εκτός σύνδεσης. Ωστόσο, η συνεχής αποστολή μηνυμάτων απαιτεί επίσης πρόσθετο αποθηκευτικό χώρο και μπορεί να επηρεάσει την απόδοση του broker.

Κατά την υλοποίηση του MQTT, είναι σημαντικό να εξετάζεται η ασφάλεια και ο έλεγχος ταυτότητας. Οι MQTT brokers μπορούν να ρυθμιστούν ώστε να απαιτούν έλεγχο ταυτότητας, ο οποίος διασφαλίζει ότι μόνο εξουσιοδοτημένοι πελάτες μπορούν να συνδεθούν στον broker. Ο έλεγχος ταυτότητας μπορεί να υλοποιηθεί χρησιμοποιώντας ονόματα χρήστη και κωδικούς πρόσβασης, πιστοποιητικά ή tokens. Επιπλέον, οι MQTT brokers μπορούν να ρυθμιστούν ώστε να χρησιμοποιούν λίστες ελέγχου πρόσβασης (ACL), οι οποίες καθορίζουν ποιοι clients επιτρέπεται να δημοσιεύουν ή να εγγράφονται σε συγκεκριμένα θέματα.

Τέλος, η παρακολούθηση καλής λειτουργίας (monitoring) και η καταγραφή των συμβάντων (logs) αποτελούν κρίσιμες πτυχές της υλοποίησης του MQTT. Η παρακολούθηση επιτρέπει στους διαχειριστές του συστήματος να παρακολουθούν την υγεία του broker και να εντοπίζουν τυχόν προβλήματα απόδοσης ή ανωμαλίες. Η καταγραφή των συμβάντων (logs) επιτρέπει στους διαχειριστές του συστήματος να παρακολουθούν τις δραστηριότητες των πελατών και του broker, κάτι που μπορεί να είναι χρήσιμο για την αποσφαλμάτωση και την αντιμετώπιση προβλημάτων. Οι

MQTT brokers παρέχουν συνήθως εργαλεία καταγραφής και παρακολούθησης, τα οποία μπορούν να χρησιμοποιηθούν για την παρακολούθηση του συστήματος και τη διάγνωση τυχόν προβλημάτων.

1.5.7 Συμπεράσματα κεφαλαίου

Σε αυτό το κεφάλαιο είδαμε οτι έννοιες όπως η ασφάλεια, το απόρρητο και οι τεχνικές με τις οποίες δημιουργούμε ασφαλείς συνδέσεις, είναι πολύ σημαντικές όταν ανταλλάσσουμε ευαίσθητα και προσωπικά δεδομένα, ακόμα και αν αυτά αποτελούν χαρακτηριστικά του περιβάλλοντα χώρου μας. Οι αισθητήρες που είναι τοποθετημένοι στις οικιακές αλλά και βιομηχανικές συσκευές, είναι ευάλωτοι σε κυβερνοεπιθέσεις, και σε data leakage. Για το λόγο αυτό, η τεχνολογία και οι άνθρωποι που δουλεύουν πάνω σε αυτή και στην ανάπτυξή της, εργάζονται συνεχώς στη βελτιστοποίηση των ζητημάτων ασφάλειας και ακεραιότητας των πληροφοριών.

Η υλοποίηση του MQTT, ως πρωτόκολλο επικοινωνίας, περιλαμβάνει διάφορα στοιχεία, συμπεριλαμβανομένου του MQTT client, του MQTT broker και της υποκείμενης υποδομής δικτύου. Οι βιβλιοθήκες MQTT client είναι διαθέσιμες σε πολλές γλώσσες προγραμματισμού, καθιστώντας εύκολη την ενσωμάτωση του MQTT σε εφαρμογές. Οι servers που καλούνται να φιλοξενήσουν το MQTT, θα πρέπει να υποστηρίζουν το πρωτόκολλο MQTT και να διαχειρίζονται μεγάλο αριθμό ταυτόχρονων συνδέσεων. Κατά την υλοποίηση του MQTT, είναι σημαντικό να εξετάζονται οι υποδομές δικτύου, η ασφάλεια και ο έλεγχος ταυτότητας, καθώς και η παρακολούθηση και η καταγραφή. Το MQTT είναι ένα ευέλικτο και επεκτάσιμο πρωτόκολλο, γεγονός που το καθιστά ιδανική επιλογή για εφαρμογές IoT.

ΚΕΦΑΛΑΙΟ 2ο: ΤΕΧΝΟΛΟΓΙΑ ΚΑΤΑΝΕΜΗΜΕΝΟΥ ΚΑΤΑΣΤΙΧΟΥ - DLT

2.1 Εισαγωγή

Ο όρος τεχνολογία κατανεμημένου Κατάστιχου, (Distributed Ledger Technology, DLT) αναφέρεται στη τεχνολογία και στα πρωτόκολλα που καθιστούν δυνατή την ταυτόχρονη πρόσβαση, την επικύρωση εγγραφών και την αμετάβλητη ενημέρωση εγγραφών σε ένα δίκτυο που είναι διασκορπισμένο μεταξύ πολλών οργανισμών, τόπων ή χρηστών.

Λαμβάνοντας υπόψιν τις δυνατότητές του σε όλες τις επιχειρήσεις και τους τομείς, το DLT, ευρύτερα γνωστό ως τεχνολογία blockchain, εισήχθη για πρώτη φορά ως Bitcoin και αποτελεί πλέον λέξη της μόδας στον τεχνολογικό κόσμο. Με απλά λόγια, το DLT επικεντρώνεται στην έννοια ενός "αποκεντρωμένου" δικτύου σε αντίθεση με τον παραδοσιακό "συγκεντρωτικό" μηχανισμό και πιστεύεται ότι θα έχει σημαντικές επιπτώσεις σε κλάδους και οντότητες που ιστορικά στηρίζονταν σε ένα αξιόπιστο τρίτο μέρος.

Το DLT είναι ένα πρωτόκολλο που επιτρέπει την ασφαλή λειτουργία μιας αποκεντρωμένης ψηφιακής βάσης δεδομένων. Τα κατανεμημένα δίκτυα εξαλείφουν την ανάγκη μιας κεντρικής αρχής για την αποτροπή της χειραγώγησης των δεδομένων τους.

Το DLT χρησιμοποιεί κρυπτογραφικούς αλγόριθμους προκειμένου να παρέχει τη δυνατότητα της ασφαλούς αποθήκευσης οποιασδήποτε πληροφορίας αποκεντρωμένα η οποία δεν μπορεί να δεχτεί τροποποίηση [7]. Το DLT μπορεί να χαρακτηριστεί ως μια αμετάβλητη βάση Big Data. Η τεχνολογία του κατανεμημένου Κατάστιχου δεν είναι εντελώς νέα και ήδη εδώ και μερικά χρόνια πολλοί οργανισμοί αποθηκεύουν δεδομένα σε πολλαπλές τοποθεσίες, κάτι που θυμίζει αρκετά τη φιλοσοφία του DLT. Ένα από τα δημοφιλέστερα συστήματα που η χρήση του προσανατολίζεται στην αποκεντρωμένη αποθήκευση πληροφορίας είναι το Cassandra, μία βάση δεδομένων NoSQL που η λειτουργία της βασίζεται σε μια κατανεμημένη αρχιτεκτονική [8]. Το Cassandra διαθέτει τα παρακάτω χαρακτηριστικά [8]:

- **Κατανεμημένος σχεδιασμός**: Η διανομή των δεδομένων σε πολλούς κόμβους, με τον κάθε κόμβο να ευθύνεται για την ακεραιότητα των δεδομένων και το σύστημα να λειτουργεί χωρίς ενιαία θέση αποτυχίας.

- **Αντίγραφα δεδομένων**: Το πλήθος των δεδομένων αποθηκεύονται σε πολλούς κόμβους, ώστε η αποτυχία κάποιων κόμβων να μην επηρεάζει τη λειτουργία του συστήματος.

- **Μειωμένο ποσοστό αποτυχίας**: Όσο αφορά την επεξεργασία των δεδομένων που πρόκειται να κάνει το Cassandra, λόγω του σχεδιασμού του, καθίσταται ικανό να ανακτήσει κάποια αποτυχία. Αν για παράδειγμα αποτύχει ένας κόμβος, ένας άλλος συνεχίζει την επεξεργασία των δεδομένων.

- **Κλιμακούμενο μέγεθος**: Αναλόγως τις απαιτήσεις και τον όγκο των δεδομένων, το Cassandra έχει τη δυνατότητα να επεκτείνει τον αριθμό των κόμβων στο cluster.

- **Ταχύτητα ανάγνωσης και εγγραφής**: Το Cassandra είναι σχεδιασμένο ώστε να επιτρέπει ανάγνωση και εγγραφή σε οποιονδήποτε κόμβο. Ως αποτέλεσμα έχει γρήγορες εγγραφές και αναγνώσεις.

Ωστόσο, οι υφιστάμενες τεχνολογίες Big Data Storage. δε διαθέτουν την ιδιότητα της «αμεταβλητότητας». Αυτό συμβαίνει γιατί είτε κάποιος hacker είτε κάποιος που διαθέτει δικαιώματα διαχειριστή στη βάση δεδομένων, θα μπορούσε να αλλοιώσει η να αλλάξει τα δεδομένα, εφόσον αυτά βρίσκονται σε κάποιο συμβατικό data storage. Ακόμα και με τη χρήση των αποκεντρωμένων βάσεων δεδομένων όπως της Cassandra, εάν μια πληροφορία αλλάξει σε ένα κόμβο, θα μεταδώσει την αλλαγή αυτή και στους υπόλοιπους κόμβους. Άλλες υπηρεσίες που δε διαθέτουν την ιδιότητα του immutability είναι οι υπηρεσίες STaaS (STorage as a Service), και πλατφόρμες όπως dropbox, Google drive κλπ.

Σε ενα centralized σύστημα η κάθε οντότητα συνδέεται σε ένα κεντρικό σύστημα που αυτό με τη σειρά του ενημερώνει κάθε μία από τις υπόλοιπες οντότητες σε τακτική βάση. Η κεντρική οντότητα είναι το αδύνατο σημείο ενός τέτοιου κεντρικοποιημένου συστήματος, το οποίο είναι επιρρεπές σε κακόβουλες ενέργειες.

Σε αντίθεση με τα κεντρικοποιημένα συστήματα, ένα μεγάλο αποκεντρωμένο Κατανεμημένο Κατάστιχο απαρτίζεται από μεγάλο αριθμό ισότιμων κόμβων. Όσο μεγαλύτερο είναι ένα αποκεντρωμένο σύστημα τόσο πιο ανθεκτικό είναι στο κυβερνοέγκλημα. Αυτό συμβαίνει διότι ένας κακόβουλος παράγοντας θα πρέπει να πάρει τον έλεγχο ταυτόχρονα σε παραπάνω από τους μισούς κόμβους, πράγμα που είναι πρακτικά πολύ δύσκολο να συμβεί. Όλα τα nodes που κρατούν αποθηκευμένη τη πληροφορία, πρέπει να δέχονται επίθεση ταυτόχρονα για να καταφέρουν να βλάψουν την ακεραιότητα της.

Εφόσον το DLT είναι πραγματικά αποκεντρωμένο, η χρήση του προάγει υψηλό βαθμό εμπιστοσύνης μεταξύ των συμμετεχόντων και σχεδόν εξαλείφει την πιθανότητα να εμφανιστεί δόλια δραστηριότητα στην εκάστοτε εγγραφή.

2.2 Blockchain και DLT

Συχνά συναντάμε μαζί τις έννοιες DLT και Blockchain, οι οποίες λανθασμένως χρησιμοποιούνται σαν ταυτόσημες. Οι δύο αυτοί όροι δηλώνουν δύο διαφορετικά πράγματα. Για ευκολία, μπορούμε να πούμε ότι το blockchain είναι ένα είδος DLT. Αυτό δεν προκαλεί έκπληξη, αν αναλογιστεί κανείς πόσο γρήγορα αυξήθηκε το ενδιαφέρον για τις τεχνολογίες μετά την εισαγωγή του bitcoin και πόσο εναλλάξιμες μπορεί να είναι οι τεχνολογίες στην πρακτική εφαρμογή.

Το κρυπτονόμισμα Bitcoin ήταν η πρώτη εφαρμογή DLT, με την οποία η τεχνολογία έχει λανθασμένα γίνει συνώνυμη. Ωστόσο, η ιδιαιτερότητα και το ανατρεπτικό δυναμικό του υποκείμενου DLT έγκειται στα ιδιαίτερα χαρακτηριστικά του. Εξαιτίας αυτού, το DLT καθίσταται κρίσιμο για ανάλυση [9].

Χρησιμοποιώντας κρυπτογραφία, και τα δύο χρησιμοποιούνται για την αποθήκευση αποκεντρωμένων πληροφοριών. Και τα δύο δημιουργούν αμετάβλητα δεδομένα με χρονικές σφραγίδες. Και τα δύο θεωρούνται πρακτικά απαραβίαστα. Και τα δύο μπορούν να είναι δημόσια, επιτρέποντας σε οποιονδήποτε να τα χρησιμοποιήσει, όπως το bitcoin, ή με άδεια (ιδιωτικά), περιορίζοντας την πρόσβαση σε συγκεκριμένους χρήστες. Το blockchain χρησιμοποιεί μπλοκ δεδομένων που συνδέονται μεταξύ τους για τη δημιουργία του κατανεμημένου Κατάστιχου, όπως υποδηλώνει το όνομα. Ωστόσο, το DLT περιλαμβάνει συστήματα που δημιουργούν ένα κατανεμημένο Κατάστιχο χρησιμοποιώντας διάφορες έννοιες και τρόπους σχεδιασμού.

2.3 Smart contracts

Τα έξυπνα συμβόλαια είναι ουσιαστικά προγράμματα που ενεργοποιούνται και εκτελούνται αυτόματα όταν πληρούνται ορισμένες προϋποθέσεις.

Αυτά τα έξυπνα συμβόλαια (smart contracts) ενεργοποιούνται αυτόματα από υπολογιστές και καταγράφουν ενέργειες και κινήσεις στο blockchain, καθιστώντας τις πληροφορίες αμετάβλητες και αδιαμφισβήτητες.

Χωρίς τη συνδρομή ενός αξιόπιστου τρίτου μέρους, τα smart contracts επιτρέπουν, εκτελούν και επιβάλλουν συμφωνίες μεταξύ μερών που δεν εμπιστεύονται το ένα το άλλο. Τα smart contracts είναι αρχεία κώδικα που μπορούν να εκτελούνται και να λειτουργούν πάνω σε περιβάλλον blockchain. Η αυτοματοποίηση του δικτύου και η ικανότητα μετατροπής των συμβάσεων από το χαρτί σε ψηφιακές έγιναν δυνατές με τη δημιουργία των smart contracts [10]. Σε αντίθεση με τις παραδοσιακές συμβάσεις, τα smart contracts παρείχαν αυτοματοποιημένες συναλλαγές χωρίς την εποπτεία μιας κεντρικής αρχής, επιτρέποντας στους χρήστες να επισημοποιήσουν τις συμφωνίες τους και να ενισχύσουν τις σχέσεις εμπιστοσύνης. Τα έξυπνα συμβόλαια αντιγράφονται και αποθηκεύονται σε κάθε κόμβο του δικτύου blockchain για την αποτροπή της χειραγώγησης των δεδομένων ή μετατροπής του περιεχομένου των συμβολαίων.

2.4 Κατηγορίες κατανεμημένου Κατάστιχου - DLT

Τα δύο βασικά είδη κατανεμημένου κατάστιχου είναι τα δημόσια και τα ιδιωτικά. Αυτά χωρίζονται σε αυτά που χρειάζονται άδεια (permissioned) για τη συμμετοχή των χρηστών και σε αυτά που δε χρειάζονται άδεια (permissionless). Παρακάτω φαίνονται όλοι οι συνδυασμοί τους.

1. <u>Δημόσιο/επιτρεπόμενο (Public/permissioned):</u>

Επιτρέπει την ανάπτυξη ή τη διαγραφή εφαρμογών χωρίς να ειδοποιείται κανείς, χωρίς να αποκαλύπτει την ταυτότητά του ή να πληροί οποιεσδήποτε απαιτήσεις της εφαρμογής. Οι κόμβοι που απαρτίζουν το δίκτυο και λειτουργούν τις εφαρμογές πρέπει να κληθούν να συμμετάσχουν.

2. <u>Δημόσιο/χωρίς άδεια (Public/permissionless):</u>

Αυτό είναι το πιο αποκεντρωμένο είδος δικτύου. Οι εφαρμογές μπορούν να αναπτυχθούν στην παραγωγή ή να διαγραφούν χωρίς να ειδοποιήσουν κανέναν, να αποκαλύψουν το όνομά τους ή να πληρούν οποιεσδήποτε απαιτήσεις επιλεξιμότητας της εφαρμογής. Επιπλέον, οι κόμβοι του δικτύου μπορούν να συμμετέχουν και να συνεισφέρουν ελεύθερα και ανώνυμα, συνήθως με αντάλλαγμα το εγγενές νόμισμα του δικτύου.

3. <u>Ιδιωτικό/επιτρεπόμενο (Private/permissioned):</u>

Αυτό το είδος δικτύου δεν έχει αποκέντρωση. Τόσο οι εφαρμογές όσο και οι κόμβοι του δικτύου που τις εκτελούν πρέπει να τους ζητηθεί να ενταχθούν στο δίκτυο και να πληρούν συγκεκριμένα πρότυπα ή να παρέχουν στοιχεία ταυτοποίησης. Οποιοδήποτε μέρος μπορεί να εξαλειφθεί ανά πάσα στιγμή και χωρίς προειδοποίηση.

4. Ιδιωτικό / Χωρίς περιορισμούς (Private / Permissionless):

Οι εφαρμογές παραγωγής πρέπει να κληθούν για να ενταχθούν στο δίκτυο και μπορούν να διαγραφούν ανά πάσα στιγμή χωρίς προειδοποίηση. Οι κόμβοι του δικτύου, οι οποίοι εκτελούν τις εφαρμογές, μπορούν να συμμετέχουν και να συνεισφέρουν ελεύθερα και ανώνυμα, συχνά με αντάλλαγμα το εγγενές νόμισμα του δικτύου.

2.5 Τύποι DLT

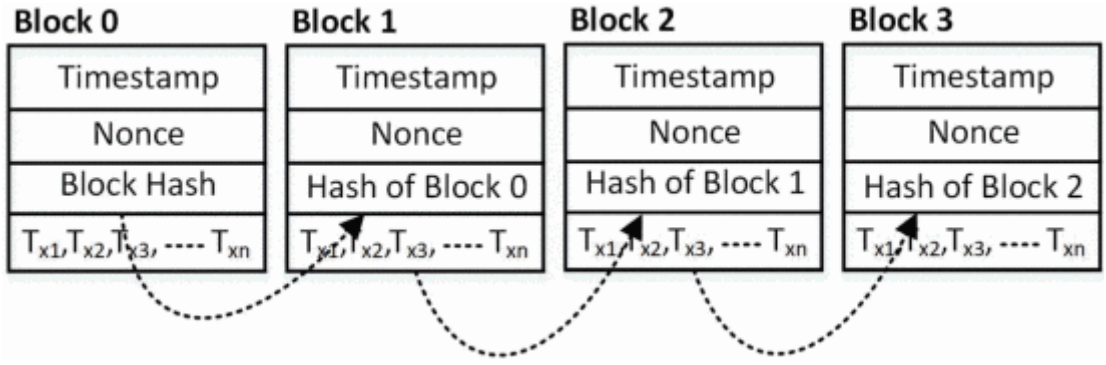
2.5.1 Blockchain

Είναι ένα από τα πιο ευρέως χρησιμοποιούμενα DLT. Το Blockchain είναι ένα είδος DLT στο οποίο οι εγγραφές συναλλαγών καταγράφονται σε ένα κατανεμημένο Κατάστιχο ως αλυσίδα από μπλοκ. Στην ουσία αποτελεί μια μακρά αλυσίδα εγγραφών ή κάθε μορφή ψηφιακών δεδομένων που καταγράφονται στη βάση δεδομένων με τη μορφή διαδοχικής σειράς.

Τα μπλοκ αποτελούνται από ψηφιακά δεδομένα. Συνήθως αποτελούνται από τρία διαφορετικά είδη τμημάτων. Ως παράδειγμα, σε μια συναλλαγή blockchain, κάποιος ολοκλήρωσε μια συναλλαγή. Η ώρα του αποστολέα, η ημερομηνία και το ποσό που στάλθηκε θα συμπεριλαμβάνονται στο μπλοκ της συναλλαγής. Το μπλοκ θα περιλαμβάνει επίσης τα στοιχεία του αποστολέα. Ωστόσο, προκειμένου να προστατευθεί η ιδιωτικότητα, το σύστημα θα χρησιμοποιήσει τη μοναδική "ψηφιακή υπογραφή".

Οι αλυσίδες μπλοκ είναι δομές δεδομένων μόνο για εγγραφή που δεν επιτρέπουν την τροποποίηση ή τη διαγραφή δεδομένων από τους διαχειριστές. Μπλοκ δεδομένων διασκορπίζονται σε ένα δίκτυο P2P. Κάθε μπλοκ χρησιμεύει ως σύνδεσμος μεταξύ των άλλων, συμπεριλαμβάνοντας την κρυπτογραφική συνάρτηση κατακερματισμού του προηγούμενου. Ο όρος "blockchain" αναφέρεται στα συνδεδεμένα μπλοκ ως ολόκληρη αλυσίδα. Η ασφάλεια, η ακεραιότητα και η αμεταβλητότητα του blockchain διατηρούνται μέσω της συνάρτησης κατακερματισμού [11].

Για τη διάκριση και τη ταυτοποίηση των συναλλαγών, κάθε μπλοκ θα έχει ένα διακριτικό αναγνωριστικό, γνωστό ως hash. Αυτός ο αλγόριθμος κατακερματισμού βοηθά στην αναγνώριση όλων των μπλοκ συναλλαγών. Η συνάρτηση αποτελείται γενικά από αλφαριθμητικούς χαρακτήρες και κάθε συνάρτηση κατακερματισμού είναι μια μοναδική και τυχαία επιλογή. Μια πολύ μικρή αλλαγή στα εισερχόμενα δεδομένα μπορεί οδηγήσει σε εντελώς διαφορετική τιμή hash.



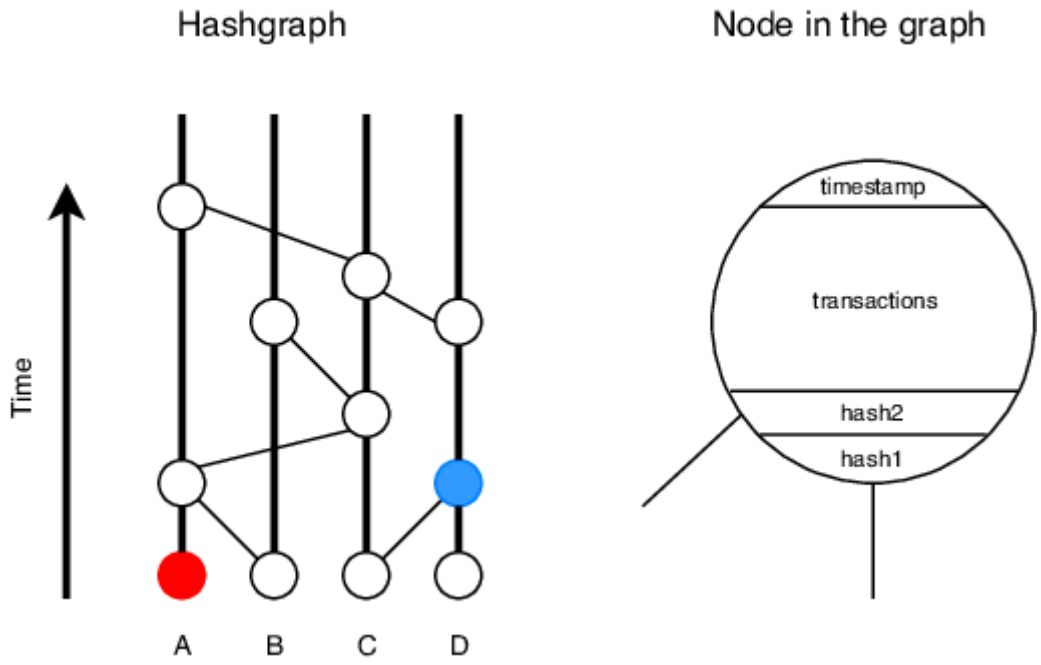
Εικόνα 3 - Η δομή του Blockchain

Ωστόσο, είναι σημαντικό οι χρήστες και οι προγραμματιστές του blockchain να γνωρίζουν τις αδυναμίες των αλγορίθμων συναίνεσης. Ένας αποκεντρωμένος αλγόριθμος συναίνεσης, όπως ο POW (proof of work), ο POS (proof of stake), ο DPOS (delegated proof of stake), ο RPCA (αλγόριθμος συναίνεσης του πρωτοκόλλου ripple) ή ο SCP (stellar consensus protocol), χρησιμοποιείται από το blockchain. Οι παραδοσιακοί κεντρικοί αλγόριθμοι συναίνεσης που χρησιμοποιούν υποδομές δημόσιου κλειδιού, όπως η πιστοποίηση του πρωτοκόλλου X.509, μπορούν να χρησιμοποιηθούν για να αποφευχθούν οι αδυναμίες των αποκεντρωμένων αλγορίθμων συναίνεσης. Αλλά επειδή ο έλεγχος ταυτότητας του πρωτοκόλλου X.509 χρησιμοποιείται τόσο ευρέως, έχουν αναφερθεί πολυάριθμες ευπάθειες. Οι τεχνικές προστασίας της ασφάλειας πρέπει επίσης να ενσωματωθούν στις εφαρμογές που κάνουν χρήση X.509 προκειμένου να χρησιμοποιηθούν με ασφάλεια οι κεντρικές εφαρμογές του Blockchain [12].

2.5.2 Hashgraph

Στο Hashgraph, πολλές συναλλαγές με την ίδια χρονοσφραγίδα μπορούν να διατηρηθούν στο DLT. Για να κρατηθούν όλες οι συναλλαγές, χρησιμοποιείται μια παράλληλη δομή. Κάθε καταχώρηση αναφέρεται ως "event" σε αυτή την περίπτωση.

Χωρίς blockchain, κανένας κόμβος στο δίκτυο δεν θα μπορεί να τροποποιήσει τις πληροφορίες ή τις συναλλαγές σε αυτό το DLT. Αυτό σημαίνει ότι κανείς στο σύστημα DLT δεν μπορεί να τροποποιήσει ή να αναβάλει όλες τις οδηγίες που θα εκτελεστούν, ούτε να επηρεάσει τη διαδικασία της συναλλαγής.



Εικόνα 4 - Hashgraph διάγραμμα

Σήμερα, το Hedera Hashgraph είναι το μόνο DLT που βασίζεται στην τεχνολογία hashgraph. Ωστόσο, η Hedera διαθέτει μια ανεπτυγμένη βιβλιοθήκη και έτοιμα αρχεία πηγαίου κώδικα, με σκοπό τη χρήση του σε API που επιτρέπουν στους προγραμματιστές να φτιάξουν τα δικά τους διακριτικά για εκτέλεση στο δίκτυο της Hedera Hashgraph.

Το Hedera Hashgraph είναι ένα DLT που διαφέρει δομικά από τα άλλα δίκτυα blockchain, αλλά εκτελεί παρόμοιες λειτουργίες. Βασίζεται σε αλγόριθμους ασφάλειας και επικύρωσης που είναι πιο αποτελεσματικοί από αυτούς που χρησιμοποιούνται σε δίκτυα blockchain.

Το Hedera Hashgraph είναι ένα ανοικτό DLT με τεχνολογία hashgraph, το οποίο είναι πιο πρακτικό από το blockchain για την εφαρμογή ενός DLT και την υποστήριξη ενός κρυπτονομίσματος.

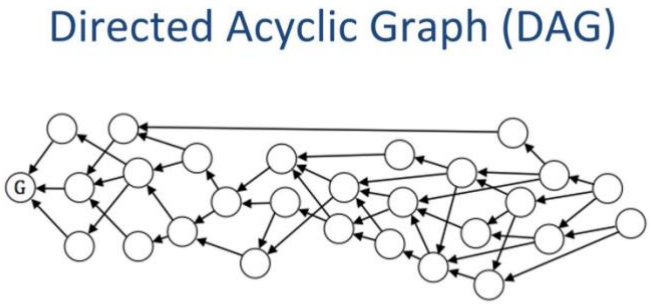
Η τεχνολογία Hashgraph έχει πολλά σημαντικά πλεονεκτήματα σε σχέση με τα blockchain. Δεν υπάρχει mining, επομένως οι περιβαλλοντικές επιπτώσεις από την εφαρμογή της τεχνολογίας μειώνονται δραματικά. Το κόστος συναλλαγής είναι επίσης δυνητικά χαμηλότερο. Ένα hashgraph μπορεί να εφαρμοστεί ως DLT με τα ίδια πλεονεκτήματα ασφάλειας και ανωνυμίας με κάποιο που βασίζεται σε blockchain, με πρόσθετα οφέλη, όπως καλύτερη απόδοση και μεγαλύτερη χωρητικότητα.

2.5.3 Directed Acyclic Graph (DAG)

Το DAG, ή Directed Acyclic Graph, είναι μια άλλη φιλόδοξη προσθήκη στην οικογένεια των DLT που δεν είναι αλυσίδα μπλοκ. Το DAG αναπτύχθηκε ως εναλλακτική λύση στο Blockchain DLT.

Κατά συνέπεια, αυτό το DLT χωρίς blockchain παρέχει όλα τα οφέλη του blockchain, ενώ παράλληλα τα βελτιώνει. Παρά το γεγονός ότι αποτελεί εναλλακτική λύση, η δομή αυτού του DLT είναι σημαντικά διαφορετική. Ένα από τα κύρια οφέλη της υλοποίησης του DAG είναι η δυνατότητα παροχής νανο-συναλλαγών χωρίς τέλη. Επειδή η επεκτασιμότητα του δικτύου βελτιώνεται με το μέγεθος.

Το DAG είναι ο τρόπος με τον οποίο λειτουργεί το IOTA, γι' αυτό θα αναλυθεί σε ξεχωριστό κεφάλαιο παρακάτω.



Εικόνα 5 - Directed Acyclic Graph

2.5.4 Holochain

Η Holochain αποτελεί την επόμενη γενιά της τεχνολογίας DLT. Η πιο αξιοσημείωτη αλλαγή στην πλατφόρμα είναι η μετάβαση από μια στρατηγική επικεντρωμένη στα δεδομένα σε μια στρατηγική επικεντρωμένη στους πράκτορες(agents). Επειδή δεν χρησιμοποιεί διαδικασία παγκόσμιας συναίνεσης, το Holochain-DLT προσφέρει ουσιαστικά απεριόριστη επεκτασιμότητα.

Ενώ το Blockchain επιδιώκει την αποκέντρωση των συναλλαγών του δικτύου, το Holochain επιδιώκει την αποκέντρωση των αλληλεπιδράσεων μεταξύ μεμονωμένων κόμβων. Κάθε κόμβος στο δίκτυο τρέχει τη δική του αλυσίδα, επιτρέποντάς του να λειτουργεί αυτόνομα, ενώ ταυτόχρονα αποτελεί μέρος ενός μεγαλύτερου δικτύου με χιλιάδες άλλους πανομοιότυπους κόμβους.

2.5.5 Tempo (Radix)

Το Tempo είναι η τελευταία νέα παραλλαγή DLT που παρουσιάζεται (Radix). Το Tempo είναι ένα νεότερο DLT που συνδυάζει τα πλεονεκτήματα της χρονοσήμανσης μαζί με άλλες δυνατότητες. Το βασικό πλεονέκτημα του Tempo είναι ότι μπορεί να χρησιμοποιηθεί χωρίς τροποποίηση τόσο για δημόσιες όσο και για ιδιωτικές μονάδες.

Επιπλέον, δεν θα απαιτούνται αξιοσημείωτες αναβαθμίσεις υλικού για την κατασκευή των αποκεντρωμένων εφαρμογών, νομισμάτων ή tokens. Η βάση δεδομένων του DLT βασίζεται σε τρεις θεμελιώδεις αρχές: μια δικτυωμένη συστάδα κόμβων, ένα κατανεμημένο παγκόσμιο DLT και συγκεκριμένοι αλγόριθμοι για τη χρονοσήμανση των γεγονότων στο DLT.

Παρόλα αυτά, παρατηρείται ότι συνεχώς εφευρίσκονται και δημιουργούνται νέοι τύποι DLT καθώς η τεχνολογία εξελίσσεται συνεχώς και οι ανάγκες της συνεχώς αυξάνονται και μεταβάλλονται.

2.6 PoW (Proof of Work) και PoS (Proof of Stake)

Proof-of-Work (PoW): Η κεντρική έννοια του PoW συνδέεται με τον αγώνα υπολογιστικών δυνατοτήτων. Τα άτομα που ασχολούνται με το mining, τους λεγόμενους miners, πραγματοποιούν επανειλημμένα hash operations, ανταγωνιζόμενοι για την ευκαιρία να σχηματίσουν το επόμενο block συνοδευόμενο από μια επιπρόσθετη ανταμοιβή. Ο πρώτος miner που πετυχαίνει τιμή hash μικρότερη από τον προκαθορισμένο στόχο, καθορίζεται ως ο νικητής. Στο PoW, απαιτείται σημαντικό επίπεδο υπολογιστικής πολυπλοκότητας για την αποφυγή του forking, αλλά αυτό επιφέρει την ενεργειακή απαίτηση που συνεπάγεται με τη δημιουργία ενός νέου block.

Proof-of-Stake (PoS): Εν αντιθέσει με το PoW που επικεντρώνεται στην υπολογιστική ισχύ, το PoS επικαλείται την "ηλικία" των νομισμάτων για να αποφύγει το υπέρογκο υπολογιστικό κόστος των hash operations. Ορίζεται ως "ηλικία" ενός νομίσματος, η περίοδος που έχει παρέλθει από τη στιγμή δημιουργίας του, πολλαπλασιαζόμενη με την αξία του. Στο PoS, ένα νόμισμα με μεγαλύτερη "ηλικία" έχει αυξημένες πιθανότητες να κερδίσει το δικαίωμα δημιουργίας ενός νέου block, και αυτή η "ηλικία" μηδενίζεται, όταν ο νικητής λαμβάνει την ανταμοιβή του.

2.7 DAG (Directed Acyclic Graph)

2.7.1 Εισαγωγή

Στη παρούσα διπλωματική πρωταρχικό ρόλο έχει ο τρίτος από τους προαναφερθέντες τύπους DLT, το DAG, καθώς είναι ο τύπος DLT που η IOTA έχει επιλέξει να βασιστεί.

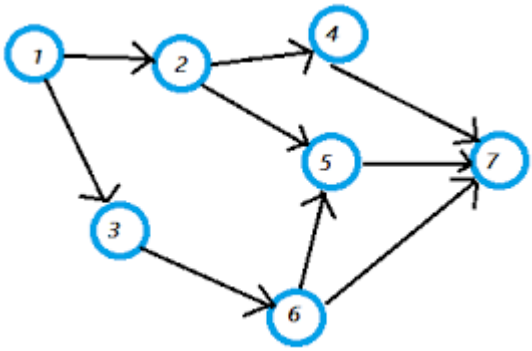
Το Directed Acyclic Graph είναι μια νεότερη προσέγγιση που συνδυάζει τα πλεονεκτήματα του blockchain με βελτιωμένες επιδόσεις. Η ιδέα του DAG δεν είναι καθόλου καινούργια. Στα μαθηματικά ένα DAG είναι ένα γράφημα που κινείται προς μία κατεύθυνση θυμίζοντας τοπολογία δενδροειδούς. Αυτό σημαίνει ότι είναι αδύνατο να διασχιστεί ολόκληρο το γράφημα ξεκινώντας από μία άκρη ή κόμβο. Οι άκρες του κατευθυνόμενου γράφου πηγαίνουν μόνο προς μία κατεύθυνση. Το γράφημα είναι μια τοπολογική ταξινόμηση, όπου κάθε κόμβος βρίσκεται σε μια συγκεκριμένη σειρά [13].

Θεωρήστε ένα σύνολο μεμονωμένων συναλλαγών (κόμβων), καθεμία από τις οποίες σχετίζεται με τουλάχιστον μία άλλη συναλλαγή με τον ακόλουθο τρόπο:

- (Directed) Κατευθυνόμενη
  Όλες οι συνδέσεις έχουν την ίδια κατεύθυνση, με τις προηγούμενες συναλλαγές να συνδέονται με τις επόμενες συναλλαγές κ.ο.κ.

- (Acyclic) Άκυκλο
  Δεν υπάρχουν κυκλικοί βρόχοι. Αφού συνδεθεί με μια άλλη συναλλαγή, μια συναλλαγή δεν μπορεί να επιστρέψει στον εαυτό της, ακόμη και αν αυτός ο κύκλος αποτελεί μέρος μεγαλύτερης διαδρομής.

- (Graph) Γράφημα
  Το πλέγμα των συναφών συναλλαγών μπορεί να αναπαρασταθεί ως κόμβοι σε ένα δίκτυο γραφημάτων, με κόμβους συνδεδεμένους μεταξύ τους [14].



Εικόνα 6 - Κόμβοι στο δίκτυο γραφημάτων

Ένα DAG, όπως προαναφέρθηκε, είναι πιο αποδοτικό στην αποθήκευση δεδομένων. Έχει δενδροειδή δομή, με συνδεδεμένους κόμβους που χρησιμεύουν ως "κλαδιά".

Επειδή κάθε κόμβος μπορεί να έχει πολλές ρίζες γονεικών nodes, το DAG επιτρέπει την ταυτόχρονη επαλήθευση περισσότερων συναλλαγών. Αυτό οφείλεται στο γεγονός ότι οι πελάτες δεν χρειάζεται

να περιμένουν να ολοκληρωθούν οι προηγούμενες συναλλαγές πριν ξεκινήσουν μια νέα, αλλά συμβαίνουν παράλληλα.

Κατά συνέπεια, σε έναν DAG, κάθε νέα συναλλαγή πρέπει να αναφέρεται σε προηγούμενες συναλλαγές πριν γίνει δεκτή στο δίκτυο. Αυτό αποτελεί ανάλογη περίπτωση με τον τρόπο που τα μπλοκ σε ένα Blockchain αλληλεπιδρούν με τα προηγούμενα μπλοκ. Αυτό συμβαίνει, καθώς μια συναλλαγή μπορεί να επαληθεύεται με ακρίβεια μόνο εφόσον παραπέμπει σε μια άλλη συναλλαγή.

Κάθε κορυφή σε ένα DAG αντιπροσωπεύει μια συναλλαγή. Επειδή δεν υπάρχουν μπλοκ, το mining δεν είναι απαραίτητο. Αντί να ομαδοποιούνται οι συναλλαγές σε μπλοκ, τοποθετούνται η μία πάνω στην άλλη. Στη συνέχεια, όπως αναφέρθηκε προηγουμένως, κάθε φορά που ένας κόμβος πραγματοποιεί μια συναλλαγή, εκτελούνται εργασίες proof-of-work για την επικύρωση των προηγούμενων συναλλαγών και την αποφυγή spam.

Σε ένα κρυπτονόμισμα που χρησιμοποιεί την τεχνολογία DAG, οι νεότερες συναλλαγές έρχονται πάνω σε αυτές που προηγήθηκαν. Το κύριο χαρακτηριστικό που διαφοροποιεί την blockchain από το DAG είναι ότι στο τελευταίο, μια πληθώρα συναλλαγών μπορεί να γίνει αναφορά ταυτοχρόνως, αντί για μόνο μία κάθε φορά.

Ορισμένα συστήματα χρησιμοποιούν έναν αλγόριθμο για να επιλέξουν ποιες "άκρες" ή συναλλαγές θα χτιστούν ανάλογα με το συσσωρευμένο βάρος (ή τον αριθμό των επιβεβαιώσεων που οδηγούν στην άκρη).

Η προστασία διπλής δαπάνης (Double-spend protection) σε DAG λειτουργεί με κόμβους που επιβεβαιώνουν παλαιότερες συναλλαγές αξιολογώντας μια διαδρομή, που ανατρέχει στην πρώτη συναλλαγή του DAG. Με τον τρόπο αυτό ελέγχεται αν ο αποστολέας έχει αρκετό υπόλοιπο. Εάν ένας χρήστης κατασκευάζει σε λανθασμένη διαδρομή, η συναλλαγή μπορεί να απορριφθεί.

2.7.2 DAG vs. Blockchain

Το DAG και το Blockchain καταγράφουν και οι δύο τις συναλλαγές σε ένα DLT, αν και με διαφορετικούς τρόπους.

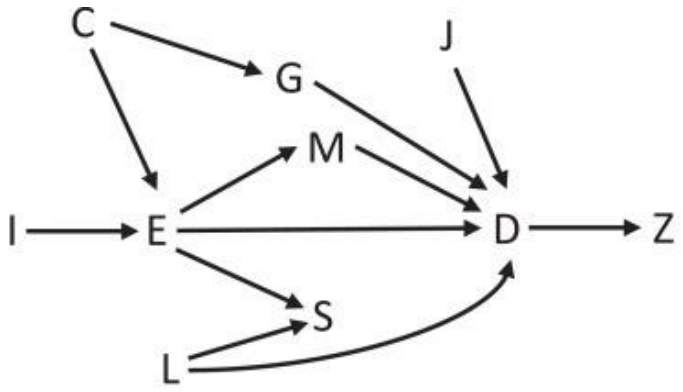
Ακολουθεί μια σύντομη σύγκριση των δύο από την άποψη των πλεονεκτημάτων και των μειονεκτημάτων [15]:

	DAG	BLOCKCHAIN
ΘΕΤΙΚΑ	• Κατάλληλο για μικροσυναλλαγές και μεγάλο όγκο συναλλαγών • Εξαλείφει την ανάγκη για mining εξοπλισμό • Τα τέλη μπορούν να μειωθούν σημαντικά • Χαμηλότερη κατανάλωση ενέργειας	• Κατοχυρωμένο και ευρέως χρησιμοποιούμενο από κρυπτονομίσματα όπως το Bitcoin και το Ethereum • Διαφανές και αμετάβλητο, εξαιρετικά ασφαλές • Οικονομικά αποδοτικό για συναλλαγές υψηλής αξίας
ΑΡΝΗΤΙΚΑ	• Ευάλωτο σε επιθέσεις λόγω χαμηλού όγκου συναλλαγών • Βρίσκεται ακόμη σε πρωταρχικό στάδιο- δεν έχει διατηρήσει ακόμη υψηλά επίπεδα αποκέντρωσης	• Απαιτήσεις αποθήκευσης και εύρους ζώνης δικτύου • Μεγάλες ποσότητες ενέργειας που καταναλώνονται • Υψηλά τέλη συναλλαγών

Πίνακας 3 - Σύγκριση DAG και Blockchain

2.7.3 Σχέσεις μεταξύ κόμβων στο DAG

Για να προσδιορίσουμε την επίδραση της E στη D, πρέπει να αποκλείσουμε όλες τις μη αιτιώδεις διαδρομές και καμία από τις διαδρομές μεταξύ των δύο μεταβλητών [16].



Εικόνα 7 - Σχέσεις μεταξύ κόμβων στο DAG [16]

Αιτιώδεις διαδρομές που συνδέουν τα E και D:

E→M→D
E→D

Μη αιτιώδεις διαδρομές που συνδέουν τα E και D και πώς να τις μπλοκάρετε:

E←C→G→D (μπλοκάρισμα με έλεγχο του C ή του G)
E→S←L→D (μπλοκαρισμένο υπό την προϋπόθεση ότι δεν ελέγχουμε το S)

Βασικοί όροι:

- Ο C συγχέει τη σχέση μεταξύ E και D.
- Το G μπορεί να προγραμματιστεί ώστε να εμποδίζει την ασαφή διαδρομή μεταξύ E και D.
- Το M βοηθά να μετριάσει την επίδραση του E στο D.
- Το S αποτρέπει τη σύγκρουση των μονοπατιών μεταξύ E και L, και παράλληλα είναι ένας μη αιτιώδης συγκρουστής μονοπατιών μεταξύ E και D. Ο έλεγχος ή ο περιορισμός του S έχει ως αποτέλεσμα μια στρεβλή σχέση μεταξύ E και D.
- Ο Z είναι απόγονος του D.
- Για την επιρροή του E στο D, το I είναι μια οργανοποιητική μεταβλητή, όπως η τυχαιοποίηση.
- Ο J επαληθεύει την ύπαρξη του D και, ως εκ τούτου, θα είναι αποτελεσματικός παράγοντας οποιουδήποτε άλλου αιτίου για το D σε τουλάχιστον ένα επίπεδο (προσθετικό ή πολλαπλασιαστικό).

Βασικές έννοιες:

• Οι διαδρομές αναπαριστούν ακολουθίες βελών, ανεξάρτητα από την κατεύθυνσή τους, που συνδέουν δύο μεταβλητές και μπορούν να είναι είτε αιτιώδεις είτε μη αιτιώδεις. [17].

• Οι διαδρομές είναι αιτιώδης αν κάθε μεταβλητή προκαλεί την επόμενη μεταβλητή (όλα τα βέλη δείχνουν προς την ίδια κατεύθυνση).

• Οι διαδρομές είναι μη αιτιοκρατικές εάν τα βέλη δεν δείχνουν όλα προς την ίδια κατεύθυνση.

• Οι παράγοντες που προκαλούν σύγχυση εμφανίζονται λόγω της κοινής ύπαρξης αιτιών (όπως το C) για τις μεταβλητές E και Δ. Για να αξιολογηθεί η επίδραση της μεταβλητής E στη μεταβλητή Δ, είναι αναγκαίο να ελεγχθούν τέτοιες κοινές αιτίες ή άλλες μεταβλητές κατά μήκος της μη αιτιώδους διαδρομής. Ο έλεγχος είτε για το C είτε για το G θα ήταν αποτελεσματικός για να εξαλειφθεί η σύγχυση που οφείλεται στο C. Η χρήση της μεταβλητής G θα μπορούσε να είναι προτιμότερη, για παράδειγμα, εάν ήταν ευκολότερο να γίνει μια αξιόπιστη μέτρηση του G υψηλής ποιότητας.

• Οι mediators (π.χ. M) προκαλούνται από την E και, με τη σειρά τους, προκαλούν τη D. Δεν θα πρέπει να ελέγχονται για να εκτιμηθεί η συνολική επίδραση της E στη D.

• Οι colliders (π.χ. S) ονομάζονται έτσι, επειδή έχουν δύο βέλη που δείχνουν προς αυτούς. Οι colliders σε ένα μονοπάτι μπλοκάρουν αυτό το μονοπάτι, εκτός αν εξαρτώνται από αυτούς (π.χ. ελέγχοντάς τους) ή από μια συνέπεια του collider.

• Οι αναλύσεις δεν πρέπει να προσαρμόζονται, να διαστρωματώνονται ή με οποιονδήποτε τρόπο να εξαρτώνται από τους απογόνους του D (π.χ. Z).

• Τροποποιητές αποτελέσματος είναι μεταβλητές που προκαλούν το D και τροποποιούν την επίδραση άλλων αιτιών του D, όπως η E. Εάν η E και η J και οι δύο προκαλούν το D, τότε η J τροποποιεί την επίδραση της E στο D τουλάχιστον σε μία κλίμακα μέτρησης αποτελέσματος (προσθετική ή πολλαπλασιαστική).

ΚΕΦΑΛΑΙΟ 3º - IOTA LEDGER

3.1 Εισαγωγή

Το Tangle του IOTA αποτελεί ένα ανοιχτό, απροσπέλαστο και κλιμακούμενο Κατανεμημένο Κατάστιχο, το οποίο είναι σχεδιασμένο για να επιτρέπει την ελεύθερη μεταφορά δεδομένων και tokens. [18].

Όπως λέει και το όνομά της, μια τεχνολογία κατανεμημένου Κατάστιχου διατηρεί ένα αρχείο με την ιδιοκτησία των tokens μεταξύ πολλαπλών κόμβων. Αυτό θα ήταν φυσιολογικό εάν όλοι οι κόμβοι υπάγονταν στην ίδια ενότητα, ωστόσο στα DLTs, η κατάσταση του συστήματος πρέπει να επικυρώνεται από μια ομάδα ανεξάρτητων κόμβων. Υπάρχει πάντα το ενδεχόμενο ένας κακόβουλος κόμβος να ενταχθεί στο δίκτυο, γι' αυτό κάθε DLT απαιτεί κάποιο μέσο προστασίας. Το πώς το IOTA εξασφαλίζει αυτό το προστατευτικό στοιχείο το καθιστά διαφορετικό από άλλα πρωτόκολλα. [19].

Το IOTA λειτουργεί πάνω στο Tangle, μια δομή στην οποία οι πιο πρόσφατες συναλλαγές επικυρώνουν τις παλαιότερες, ενώ τα περισσότερα άλλα DLTs βασίζονται σε blockchain. Για την εξασφάλιση της κατάστασης και του ιστορικού του, ένα blockchain αποτελείται από συναλλαγές που ενσωματώνονται σε μπλοκ, τα οποία συνδέονται σειριακά μεταξύ τους. Αυτό οδηγεί σε μια φυσική συμφόρηση, ένα παράδειγμα που εξηγεί την αρχή λειτουργίας του Blockchain, είναι η προσπάθεια να φορτωθεί το παγκόσμιο φορτίο για να μεταφερθεί από μια χώρα σε μια άλλη, σε ένα μόνο τρένο βαγόνι προς βαγόνι. Το IOTA το παρακάμπτει αυτό εντελώς.

Το πρωτόκολλο IOTA είναι ακόμη υπό διερεύνηση. Έχει δύο δημόσιες πλατφόρμες: το IOTA mainnet, που είναι το σταθερό δίκτυο για τη διαχείριση των IOTA tokens σας, και το Shimmer, που λειτουργεί ως το δοκιμαστικό δίκτυο για τις πιο πρόσφατες και μεγαλύτερες εκδόσεις του πρωτοκόλλου. Όταν οι αλλαγές αποδεικνύονται σταθερές στο Shimmer, έρχονται στη συνέχεια και στο mainnet. Η επόμενη μεγάλη ενημέρωση είναι το Stardust. Η μελλοντική ενημέρωση που ολοκληρώνει την προσπάθεια αποκέντρωσης ονομάζεται Coordicide.

Οι πληροφορίες του παρόντος κεφαλαίου έχουν παρθεί κατά πλειονότητα από την επίσημη ιστοσελίδα του IOTA για λόγους πιστότητας και ενημερωμένων πληροφοριών[2].

[2] https://wiki.IOTA.org

Πλεονεκτήματα IOTA

1. **Χωρίς έξοδα συναλλαγής.**
   Με το IOTA, δεν υπάρχει ανάγκη να επιβαρύνεστε με κόστη για κάθε συναλλαγή (όπως στην περίπτωση του Ethereum) ή να παρέχετε αμοιβές σε miners (όπως στο Bitcoin) για την εκτέλεση των συναλλαγών. Χωρίς miners ή επικυρωτές (validators), το IOTA λειτουργεί ως ένα πρωτόκολλο μεταφοράς δεδομένων και νομισμάτων χωρίς τέλη συναλλαγών.
2. **Ταχύτερες συναλλαγές.**
   Οι παραδοσιακές αλυσίδες μπλοκ συχνά αντιμετωπίζουν προβλήματα συμφόρησης εξαιτίας του χρόνου που απαιτείται για τη δημιουργία νέων μπλοκ. Η αλυσίδα μπλοκ του Bitcoin μπορεί να διαχειριστεί περίπου πέντε συναλλαγές ανά δευτερόλεπτο (Transactions Per Second-TPS), αν και αυτός ο αριθμός μπορεί να ποικίλει. Για το Ethereum, η τυπική απόδοση είναι περίπου 15 TPS. Στην περίπτωση του IOTA, είναι δυνατόν το δίκτυο της να επεξεργάζεται μέχρι και περίπου 1.000 συναλλαγές ανά δευτερόλεπτο.
3. **Ενεργειακά αποδοτικό.**
   Το IOTA έχει σχεδιαστεί με γνώμονα τη φιλοξενία συσκευών όπως αισθητήρες που λειτουργούν σε καθεστώς χαμηλής κατανάλωσης ενέργειας. Ακόμη και συσκευές IoT με ελάχιστη υπολογιστική ισχύ, όπως μικρές οικιακές συσκευές, μπορούν να γράψουν δεδομένα στο Tangle του IOTA.
4. **Προσαρμόσιμο σε διαφορετικές περιπτώσεις χρήσης.**
   Οι μεγάλες εταιρείες μπορούν να προσαρμόσουν το IOTA για συγκεκριμένες περιπτώσεις χρήσης. Με τη χρήση του IOTA Access, ενός πλαισίου ανοιχτού κώδικα που επιτρέπει την απομακρυσμένη πρόσβαση σε συστήματα ελέγχου, ένας ιδιοκτήτης αυτοκινήτου μπορεί, για παράδειγμα, να παραχωρήσει απομακρυσμένη πρόσβαση στο όχημά του σε κάποιον άλλο.
5. **Αποκέντρωση.**
   Η έκδοση 2.0 του IOTA είναι πλήρως αποκεντρωμένη.

Μειονεκτήματα IOTA

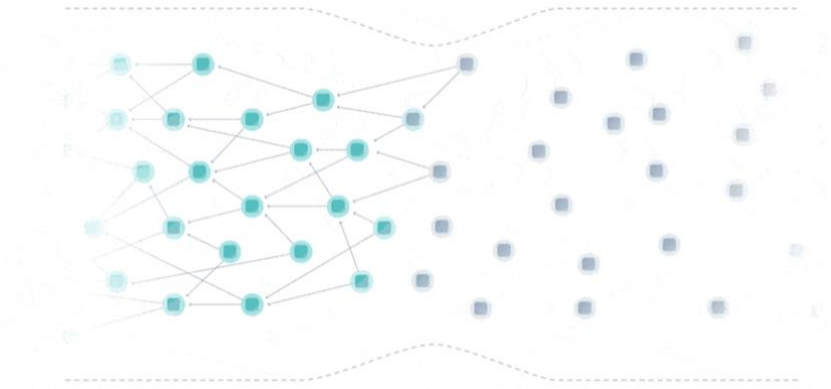
1. Ασφάλεια.
   Στις αρχές του 2020, η κοινότητα IOTA δέχτηκε ένα καταστροφικό χτύπημα όταν hackers κατάφεραν να κλέψουν tokens MIOTA αξίας πάνω από 1,5 εκατομμυρίων δολαρίων. Αυτό έγινε ορατό δεδομένου ότι οι επιτιθέμενοι φαίνεται να είχαν στοχεύσει σε λογαριασμούς υψηλής αξίας. Ως αποτέλεσμα της επίθεσης, ο ιδρυτής του IOTA, David Sonstebo, δήλωσε δημοσίως ότι θα αποζημιώσει τα θύματα της επίθεσης με προσωπικά του tokens. Το περιστατικό υπογράμμισε τη σημασία της ασφάλειας στον κόσμο των κρυπτονομισμάτων και έδωσε στο IOTA την ευκαιρία να ενισχύσει τις διαδικασίες της και τις πρακτικές της για την αποτροπή παρόμοιων περιστατικών στο μέλλον. Η νέα και βελτιωμένη έκδοση 2.0 του IOTA αποσκοπεί στη βελτίωση των ζητημάτων ασφαλείας.
2. Ικανότητα ανάπτυξης.
   Η πλατφόρμα IOTA βρίσκεται προς το παρόν σε στάδια πρώιμης εξέλιξης. Όπως αντιμετωπίζουν πολλά συστήματα κρυπτογράφησης, η προοπτική της επιτυχίας είναι συνδεδεμένη με την ολοένα και πιο εκτεταμένη υποστήριξη του δικτύου της από μια διευρυμένη λίστα συμμετεχόντων.

3.2 The Tangle

Το Tangle είναι μια δομή δεδομένων που αναπαράγεται σε ένα δίκτυο υπολογιστών (γνωστών και ως "κόμβων") και αποθηκεύει όλες τις πληροφορίες που απαιτούνται για την παρακολούθηση της ιδιοκτησίας των tokens. Δημιουργεί ένα block-DAG (κατευθυνόμενο ακυκλικό γράφημα), με κάθε νεότερο block να συνδέεται με πολλά παλαιότερα με τη μορφή δέντρου.

Οι κόμβοι του IOTA επιτυγχάνουν πλέον σταθμούς συναίνεσης, αποτελούμενους από γκρουπ ολοκληρωμένων συναλλαγών για την κατάσταση του DLT μέσω μπλοκ ορόσημων (επίσης γνωστά ως 'milestones'). Ένας κεντρικός κόμβος γνωστός ως Συντονιστής (coordinator) εκδίδει τα milestones. Ο Συντονιστής είναι μια προσωρινή λύση που θα καταργηθεί σταδιακά στο πλαίσιο των πρωτοβουλιών αποκέντρωσης του IOTA.

Το Tangle είναι ένα Fast Probabilistic Consensus (FPC) σύστημα χωρίς ηγέτη (leaderless), το οποίο επιτρέπει την ταυτόχρονη επικύρωση συναλλαγών χωρίς την ανάγκη ύπαρξής τους σε αλυσίδα (blockchain). Επιτρέπει επίσης την κατάργηση των ενδιάμεσων miner και επικυρωτών (validators). Ο παραλληλισμός, η έλλειψη ενδιάμεσων, οι ασύγχρονες δυνατότητες και η μεθοδολογία χωρίς “ηγέτη” παρέχουν μια εξαιρετικά αποδοτική λύση για πιστοποίηση των συναλλαγών ή διαμοιρασμό πληροφοριών.



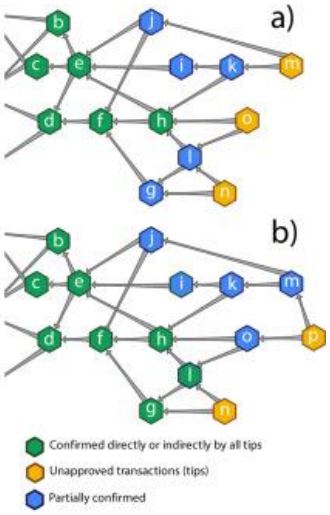
Εικόνα 8 - The Tangle, γράφημα επικύρωσης των δεδομένων

Πρακτικά αυτό σημαίνει κάτι πολύ σημαντικό και ενδιαφέρον. Όσο περισσότερο κίνηση έχει το the Tangle, και όσο περισσότερα αιτήματα έχει για επαλήθευση, τόσες περισσότερες επαληθεύσεις μπορεί να κάνει, και με ταχύτερο ρυθμό.

Για παράδειγμα, σκεφτείτε μια ομάδα ανθρώπων, που ο καθένας τους θέλει να διαμοιράσει μια πληροφορία. Ας πάρουμε για παράδειγμα τον Α, για να διαμοιράσει ο Α μία πληροφορία, θα πρέπει πρώτα να ακούσει και να επαληθεύσει ότι άκουσε τη πληροφορία που έχουν να διαμοιραστούν τουλάχιστον δύο άλλοι άνθρωποι της ομάδας αυτής, και για να διαμοιραστεί η πληροφορία του Α, θα πρέπει αντίστοιχα να του επαληθεύσουν τη πληροφορία του, δύο από τους ανθρώπους της ομάδας. Μετά από κάποιο πλήθος συναλλαγών και επαληθεύσεων κόμβων, δημιουργείται ένα milstone, το οποίο και περιέχει μονο επαληθευμένους κόμβους. Φαντάζεστε λοιπόν, ότι εάν δεν υπήρχαν αρκετοί άνθρωποι να μεταδώσεις τη πληροφορία σου (όπως και αυτοί θα περίμεναν να μεταδώσουν τη δική τους), θα έπρεπε να περιμένεις μέχρι να εμφανιστούν. Αυτό μας αποδεικνύει οτι όση περισσότερη κίνηση έχει το IOTA Tangle δίκτυο, τόσο ευκολότερα και γρηγορότερα θα επαληθευτεί μια συναλλαγή [20].

Το tip είναι μια μη επαληθευμένη συναλλαγή. Η διαδικασία επιλογής των tips του IOTA Tangle λειτουργεί με την απαίτηση ότι κάθε εισερχόμενη συναλλαγή εγκρίνει δύο tips. Η διαδικασία επιλογής του tip ωστόσο, καθίσταται σημαντική ανησυχία εάν η δενδροειδής δομή πρόκειται να επεκταθεί με υγιή τρόπο, αποφεύγοντας διάφορα προβλήματα, όπως η πρόβλεψη διπλών δαπανών [21]. Τότε, η διαδικασία επιλογής άκρων καθίσταται σημαντικό μέλημα. Ο αλγόριθμος επιλογής που χρησιμοποιείται στο IOTA είναι:

- Uniform Random Tip Selection, URTS
- AlmostURTS
- Markov Chain Monte Carlo, MCMC
- E-IOTA

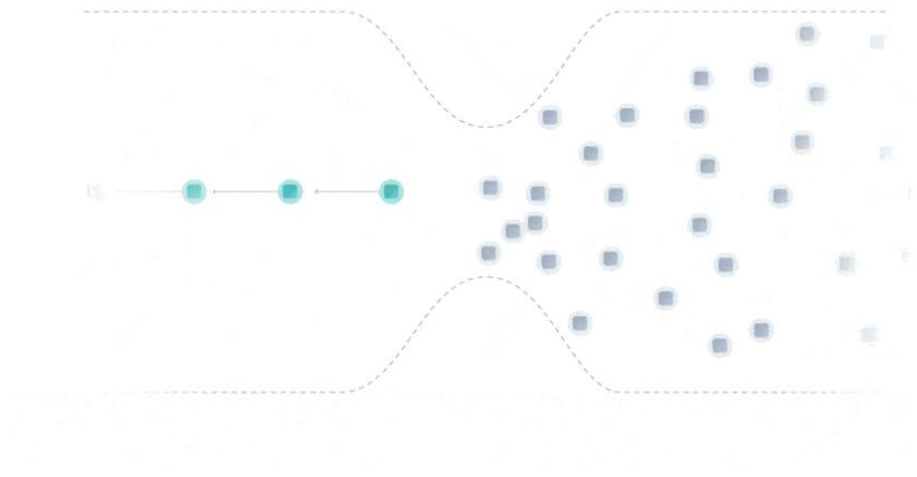


Εικόνα 9 - Γράφημα που απεικονίζει ένα μέρος του Tangle. (α) t=k, (β) t=k+1

3.3 Σχέσεις The Tangle και Blockchains

Ενώ τόσο το Tangle, όσο και οι αλυσίδες μπλοκ διατηρούν την κατάσταση του Κατάστιχού τους, το Tangle αποφεύγει τα προβλήματα που αντιμετωπίζουν τα blockchain. Το Tangle εμφανίζεται ως η λογική συνέχεια του blockchain, αποτελώντας το επόμενο βήμα στην εξέλιξη, διότι παρέχει λειτουργικότητες που ενδείκνυνται για την κατασκευή πιο αποδοτικών και επεκτάσιμων DLT συστημάτων [22].

Όπως θα δούμε και στη παρακάτω εικόνα, τα δεδομένα εισέρχονται από δεξιά προς τα αριστερά περιμένοντας σε μια "ουρά" να επαληθευτούν από κάποιο μπλοκ του blockchain. Όπως έχουμε προαναφέρει, αυτού του είδους η διαδικασία απαιτεί χρόνο, ισχύ και είναι αρκετά δαπανηρή, ιδιαίτερα για τις ανάγκες της σύγχρονης τεχνολογίας.



Εικόνα 10 - Διάγραμμα Blockchain επικύρωσης των δεδομένων

3.4 Μετάδοση δεδομένων

Το IOTA μας επιτρέπει να στέλνουμε τα δεδομένα δωρεάν. Μία από τις κύριες πτυχές του IOTA είναι η μεταφορά δεδομένων, η οποία είναι γρήγορη, αμετάβλητη, μη παραποιήσιμη και ασφαλής. Αυτή η δυνατότητα επιτρέπει στο IOTA να καλύπτει μια ευρεία γκάμα σεναρίων εφαρμογής, τα οποία η πλειονότητα των άλλων κρυπτονομισμάτων δεν είναι σε θέση να διαχειριστεί.

Οι clients, οι οποίοι μπορεί να είναι είτε ηλεκτρονικά πορτοφόλια ή προγράμματα, χρησιμοποιούν τους κόμβους IOTA για να στέλνουν και να λαμβάνουν μηνύματα (αντικείμενα δεδομένων). Οι κόμβοι λειτουργούν ως πόρτες εισόδου και εξόδου για αυτές τις επικοινωνίες, ενώ ταυτόχρονα διατηρούν επικοινωνία μεταξύ τους και με τους προσυνδεδεμένους clients.

Το IOTA είναι σε θέση να χειρίζεται ποικίλους τύπους μηνυμάτων. Ορισμένα μηνύματα μεταφέρουν αξία (το IOTA token ή ψηφιακά περιουσιακά στοιχεία), ενώ άλλα αποστέλλουν απλώς δεδομένα. Υπάρχουν επίσης μηνύματα που μπορούν να περιέχουν και τα δύο. Αυτή η ευέλικτη δυνατότητα μορφοποίησης μηνυμάτων επιτρέπει την αποκεντρωμένη διακίνηση δεδομένων και νομισμάτων σε ένα μόνο μήνυμα, ενώ ταυτόχρονα διατηρεί την απόλυτη ασφάλεια και απαλείφει κάθε κόστος. Οι κόμβοι του δικτύου είναι υπεύθυνοι για τη διασφάλιση της ασφαλούς διάδοσης όλων των μηνυμάτων στο Tangle.

3.5 Masked Authenticated Messaging (MAM)

Μια συχνή εφαρμογή του IoT είναι η μετάδοση δεδομένων αισθητήρων. Το IOTA επιτρέπει συναλλαγές χωρίς την ανταλλαγή tokens, επομένως, μια διεύθυνση μπορεί να χρησιμοποιηθεί για την αποθήκευση των δεδομένων μέτρησης. Ωστόσο, δεδομένου ότι οι συναλλαγές είναι δημόσιες, πώς μπορεί να σταματήσει ένας εισβολέας να παραποιεί δεδομένα μέτρησης ή να παρεμβαίνει με spams; Θα ήταν δυνατόν να ελεγχθεί η πρόσβαση στα δεδομένα από άλλους χρήστες; Για την επίλυση αυτού του είδους των ζητημάτων αναπτύχθηκε το Masked Authenticated Messaging (MAM).

Το IOTA επιδέχεται συναλλαγές χωρίς την ανάγκη ανταλλαγής tokens - ως εκ τούτου, μια διεύθυνση μπορεί να λειτουργήσει ως χώρος αποθήκευσης για δεδομένα μέτρησης. Παρόλα αυτά, με τις συναλλαγές να είναι δημόσιες, το MAM εισήχθη ώστε να μπορεί να εμποδίσει κάποιος έναν εισβολέα να παραποιεί δεδομένα μέτρησης ή να διαταράσσει την επικοινωνία με τη χρήση spam. Επίσης. είναι δυνατόν να περιοριστεί η πρόσβαση στα δεδομένα από άλλους χρήστες.

Το MAM λειτουργεί ως πρωτόκολλο επικοινωνίας δεδομένων, κρυπτογραφεί και πιστοποιεί τις ροές δεδομένων, είναι μια ενότητα βασισμένη στο πρωτόκολλο IOTA που παρέχει λειτουργίες για την αποστολή και ανάγνωση ροών μηνυμάτων με τη χρήση του Tangle. Η κρυπτογραφία και η πιστοποίηση ταυτότητας του συστήματος αποσκοπεί στο να διασφαλίσει ότι τα μηνύματα δεν θα αλλοιωθούν και ότι προέρχονται από συγκεκριμένο αποστολέα. Το MAM δημιουργεί μια συνδεδεμένη αλυσίδα μηνυμάτων, καθώς κάθε μήνυμα αποστέλλεται σε μια καινούργια διεύθυνση μέσω των συναλλαγών στο Tangle. Κάθε μήνυμα είναι συνδεδεμένο με το επόμενο, με κάθε συναλλαγή n να δείχνει προς τη συναλλαγή n+1. Ωστόσο, δεν μπορεί να αναγνωρίσει τη θέση της συναλλαγής n-1.

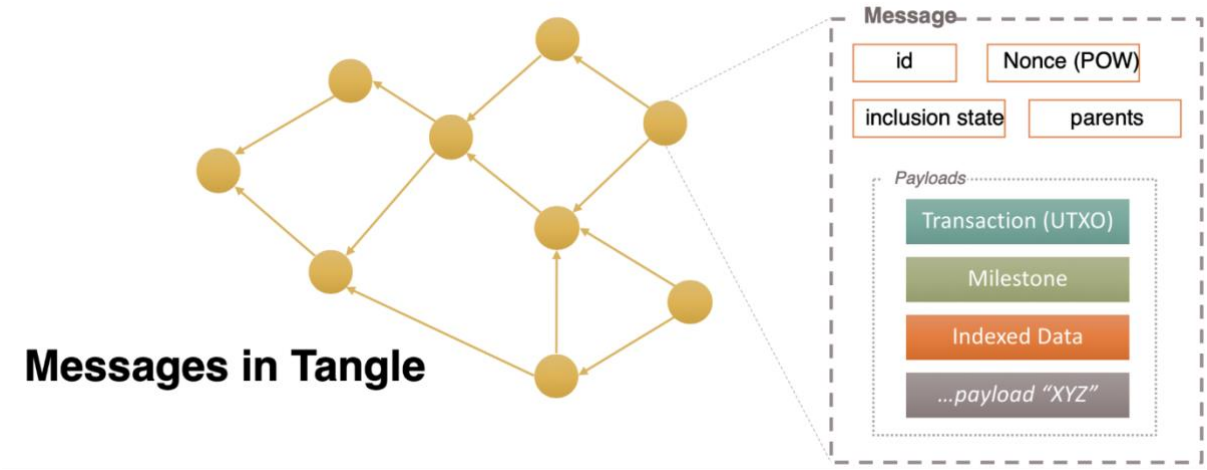
Το MAM προσφέρει τρία μοναδικά μοντέλα λειτουργίας: δημόσιο, ιδιωτικό και περιορισμένο. Στο δημόσιο μοντέλο, το root εκχωρείται ως η διεύθυνση μιας συναλλαγής στο Tangle. Από την άλλη πλευρά, το ιδιωτικό μοντέλο ορίζει τη διεύθυνση ως το "hash" της ρίζας, η οποία λειτουργεί ως μονόδρομη κρυπτογραφική συνάρτηση κατακερματισμού. Το περιορισμένο μοντέλο, επιπλέον, προσθέτει μια επιπλέον στρώση κρυπτογράφησης στο ευαίσθητο μέρος του κάθε μηνύματος, που μπορεί να αποκρυπτογραφηθεί μόνο με ένα ειδικό κλειδί. Εάν κάποιος κακόβουλος παράγοντας συναντήσει μια συναλλαγή MAM σε περιορισμένη λειτουργία, δεν θα μπορεί να αποκρυπτογραφήσει το payload του μηνύματος χρησιμοποιώντας τον κωδικό του καναλιού, καθώς αυτός είναι το hashed version του κλειδιού του καναλιού και όχι το ίδιο το κλειδί. Οποιαδήποτε προσπάθεια αναπαραγωγής του κλειδιού καναλιού μόνο από τον κωδικό του καναλιού είναι εξαιρετικά δύσκολη. Κατά την εφαρμογή της περιορισμένης λειτουργίας, η ρίζα πρέπει να χρησιμοποιηθεί από τον παραλήπτη για τον υπολογισμό της διεύθυνσης της συναλλαγής και την εύρεση των εν λόγω κρυπτογραφημένων μηνυμάτων. Η ρίζα μαζί με ένα sideKey αποτελούν αναγκαίες συνθήκες για την επιτυχή αποκρυπτογράφηση του μηνύματος.

3.6 Δομή μηνύματος στο IOTA Tangle

Ένα μήνυμα που μεταδίδεται μέσω του Tangle, αποτελεί ένα αντικείμενο το οποίο περιέχει πληροφορίες, είτε αυτές αφορούν κάποια συναλλαγή με τη χρήση token, είτε κάποιο μήνυμα πληροφορίας.

Κάθε εφαρμογή που είναι εξοικειωμένη με το πρωτόκολλο μπορεί να αποστείλει αυτά τα αντικείμενα πληροφοριών σε έναν κόμβο. Ο ρόλος ενός κόμβου IOTA είναι να επιβεβαιώνει τα εισερχόμενα μηνύματα και να τα μεταδίδει μέσω του δικτύου, υπό την προϋπόθεση ότι θεωρούνται γνήσια και συμμορφώνονται με τις τυπικές απαιτήσεις του πρωτοκόλλου.

Εάν ένας κόμβος διαπιστώσει ότι ένα μήνυμα είναι έγκυρο, θα χρησιμοποιήσει το “gossip protocol”, για να το αναμεταδώσει στους άμεσους γείτονες του. Κάθε γείτονας που λαμβάνει το μήνυμα το προωθεί στον επόμενο γείτονα και έτσι συνεχίζεται η διάδοση στο δίκτυο. Σχεδόν αμέσως, κάθε άλλος κόμβος στο δίκτυο ανιχνεύει το μήνυμα και έχει τις ίδιες πληροφορίες και γνώση για την "κατάσταση" του δικτύου στη δεδομένη στιγμή.



Εικόνα 11 - Δομή μηνύματος στο Tangle

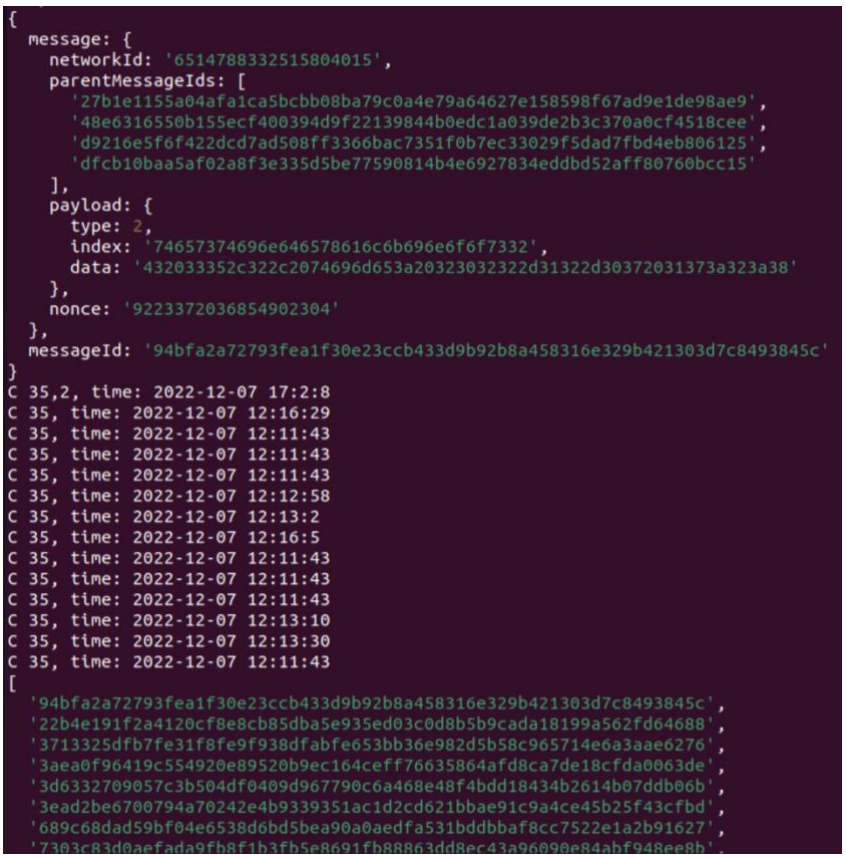
Ένα μήνυμα αποτελείται από θεμελιώδεις πληροφορίες που καθορίζουν τον τύπο και τη δομή του μηνύματος, καθώς και από διάφορα message payloads. Το payload είναι ένα συνημμένο που μπορεί να περιλαμβάνει μια συναλλαγή IOTA, καθώς και διάφορα πρόσθετα δεδομένα.

Το πρωτόκολλο IOTA ταξινομεί διάφορα πακέτα πληροφοριών και χειρίζεται ορισμένα από αυτά με διαφορετικό τρόπο από άλλα. Ως αποτέλεσμα, κάθε μήνυμα που παραδίδεται στο δίκτυο πρέπει να έχει μια μοναδική ετικέτα που εξηγεί τι είναι το μήνυμα και τι πρέπει να γίνει με αυτό. Ένας κόμβος θα παραλάβει και θα χειριστεί ένα μήνυμα μόνο εάν οι πληροφορίες αυτές παρέχονται κατάλληλα.

3.7 Αποστολή ενός μηνύματος στο IOTA Tangle

Τα μηνύματα δημιουργούνται από τους λεγόμενους πελάτες (clients). Οι clients μπορούν να είναι ένα πορτοφόλι IOTA ή οποιοδήποτε άλλο πρόγραμμα που αποστέλλει μηνύματα IOTA. Τα μηνύματα αποστέλλονται σε έναν κόμβο IOTA για επεξεργασία από τον client.

Για να διασφαλιστεί ότι ένα μήνυμα είναι γνήσιο και ότι ένας κόμβος καταλαβαίνει τι πρέπει να κάνει με αυτό, η ετικέτα του μηνύματος που παράγεται από έναν πελάτη περιλαμβάνει πολλές πληροφορίες. Αυτές οι πληροφορίες μπορεί να περιλαμβάνουν τον αποστολέα, τον παραλήπτη, την υπογραφή για την επαλήθευση της αυθεντικότητας, την ώρα και άλλες παραμέτρους που βοηθούν τον κόμβο να επεξεργαστεί και να εισαχθεί το μήνυμα στο δίκτυο.



Εικόνα 12 - μήνυμα αποστολής και αναζήτησης στο IOTA Tangle

- Message ID
  Το αναγνωριστικό μηνύματος που παράγεται ως ένα μοναδικός κρυπτογραφημένος κωδικός (cryptographic hash) των bytes που περιέχονται στο μήνυμα. Το δημιουργεί ο πελάτης (εφαρμογή) ή το πορτοφόλι που στέλνει το μήνυμα.

- Network ID
  Αποτελεί μια ένδειξη του δικτύου IOTA στο οποίο ανήκει το μήνυμα. Αυτή η πληροφορία προσδιορίζει εάν το μήνυμα ανήκει στο κύριο δίκτυο (Mainnet), σε ένα δίκτυο δοκιμών (Testnet) ή σε ένα ιδιωτικό δίκτυο. Οι κόμβοι του δικτύου θα λαμβάνουν μόνο μηνύματα που προσδιορίζουν ότι ανήκουν στο ίδιο δίκτυο με τον κόμβο, εξασφαλίζοντας έτσι την ορθότητα και την ασφάλεια του δικτύου.

- Parents length and Parents ID
  Αναφέρεται στο μήκος και την ταυτότητα των μηνυμάτων που προηγούνται του κάθε νέου μηνύματος. Για να δημιουργηθεί η δομή γραφήματος του Tangle, ένα νέο μήνυμα πρέπει να αναφέρεται σε μέχρι οκτώ προηγούμενα μηνύματα. Ο κόμβος επιλέγει αυτά τα μηνύματα και παρέχει τα αναγνωριστικά τους στον πελάτη. Ο πελάτης πρέπει να συμπεριλάβει αυτές τις πληροφορίες στην "ετικέτα" του μηνύματος. Κατ' αυτόν τον τρόπο, οι κόμβοι εξασφαλίζουν ότι η δομή του Tangle προσαρμόζεται σύμφωνα με το πρωτόκολλο.

- Μήκος Payload
  Επειδή τα μηνύματα στο IOTA έχουν περιορισμένο μέγεθος και δεν μπορούν να ξεπερνούν τα 32kb, είναι απαραίτητο να περιλαμβάνεται η πληροφορία του μεγέθους στο μήνυμα από την αρχή, προκειμένου να το γνωρίζει ο κόμβος.

- Τύπος Payload
  Η περιγραφή του τύπου του πληρωμής (payload) που περιλαμβάνεται στο μήνυμα προσδιορίζει τον τύπο των δεδομένων που αποστέλλονται. Ο κόμβος πρέπει να το γνωρίζει αυτό, δεδομένου ότι ορισμένοι τύποι payload πρέπει να αντιμετωπίζονται διαφορετικά από άλλους.

- Nonce
  Το nonce παρέχει την απαραίτητη πληροφορία για να ικανοποιηθεί το κριτήριο του Proof-of-Work. Το Proof-of-Work συνήθως εκτελείται τοπικά στη συσκευή που αποστέλλει το μήνυμα και λειτουργεί ως μέτρο προστασίας κατά των ανεπιθύμητων μηνυμάτων (spam). Ωστόσο, οι κόμβοι έχουν τη δυνατότητα να εκτελούν το Proof-of-Work αντί για τον πελάτη, αν αυτό επιτρέπεται. Αυτό είναι ιδιαίτερα χρήσιμο όταν συσκευές με περιορισμένη ισχύ (όπως αισθητήρες ή μικροελεγκτές) αποστέλλουν μηνύματα χωρίς να εκτελούν το Proof-of-Work στη δική τους συσκευή. Όταν αυτές οι συσκευές συνδέονται με έναν κόμβο που υποστηρίζει απομακρυσμένο Proof-of-Work, μπορούν να μεταδίδουν μηνύματα, ενώ ο κόμβος (που συνήθως λειτουργεί σε μια ισχυρότερη συσκευή) εκτελεί το Proof-of-Work για αυτά. Ένας από τους λόγους για τους οποίους το IOTA είναι τόσο κατάλληλο για εφαρμογές ΔτΠ και δεδομένων είναι αυτός. Οι χρήστες που θέλουν να στείλουν μεγάλο αριθμό μηνυμάτων δεδομένων από μεγάλο αριθμό συσκευών εξαιρετικά χαμηλής ισχύος, αρκεί να συνδέσουν αυτές τις συσκευές με έναν κόμβο, που μπορεί να εκτελέσει το PoW για αυτούς (ο οποίος θα είναι, στις περισσότερες περιπτώσεις, ο δικός τους κόμβος). Δεδομένου ότι η απαίτηση για το Proof of Work (PoW) στο δίκτυο του IOTA είναι γενικά πολύ χαμηλή, υπάρχει η

δυνατότητα να εκτελεστεί αυτό ακόμη και για μεγάλο αριθμό συσκευών από έναν μόνο κόμβο.

Δομή μηνύματος

<table>
<tr><th>Όνομα</th><th>Τύπος</th><th>Περιγραφή</th></tr>
<tr><td>NetworkID</td><td>uint64</td><td>Το αναγνωριστικό δικτύου είναι ένας παράγοντας που δηλώνει εάν το μήνυμα απευθύνεται στο mainnet, το testnet ή ένα ιδιωτικό δίκτυο. Αυτό το αναγνωριστικό καθορίζει επίσης τους κανόνες πρωτοκόλλου που ισχύουν για το μήνυμα. Συγκεκριμένα, αποτελείται από τα πρώτα 8 bytes του hash 'BLAKE2b-256' του συνδυασμού των συμβολοσειρών που αναφέρονται στον τύπο δικτύου και την έκδοση του πρωτοκόλλου.</td></tr>
<tr><td>Μήκος parents (parents length)</td><td>uint8</td><td>Η τιμή για τον αριθμό των μηνυμάτων που εγκρίνουμε άμεσα μπορεί να είναι οποιαδήποτε αριθμητική τιμή μεταξύ 1 και 8.</td></tr>
<tr><td>Parents</td><td>ByteArray[32 * `parents length`]</td><td>Οι μοναδικές σήμανσεις μηνυμάτων που αναφέρονται.</td></tr>
<tr><td>μήκος payload</td><td>uint32</td><td>Το μήκος του message payload. Επειδή ο τύπος του μπορεί να είναι άγνωστος στον κόμβο, απαιτείται προειδοποίηση εκ των προτέρων. Ένα μήκος 0 υποδηλώνει ότι δεν θα περιλαμβάνεται κάποιο (payload).</td></tr>
<tr><td>Payload</td><td colspan="2">
<table>
<tr><th>Όνομα</th><th>Τύπος</th><th>Περιγραφή</th></tr>
<tr><td>Τύπος Payload</td><td>uint32</td><td>Ο τύπος του (payload) θα καθοδηγήσει τον κόμβο σχετικά με τον τρόπο ανάλυσης των πεδίων που ακολουθούν. Αυτός ο τύπος θα παρέχει οδηγίες για το πώς πρέπει να ερμηνευθούν τα δεδομένα που περιέχονται στο φορτίο και πώς θα εξαχθούν τα αντίστοιχα πεδία.</td></tr>
<tr><td>Πεδία δεδομένων</td><td>οποιοσδήποτε</td><td>Πρόκειται για μια ακολουθία πεδίων, όπου η δομή των πεδίων εξαρτάται από τον τύπο του ωφέλιμου φορτίου</td></tr>
</table>
</td></tr>
<tr><td>Nonce</td><td>uint64</td><td>Το κρυπτογραφημένο hash είναι μια τιμή που επιτρέπει σε αυτό το μήνυμα να ικανοποιεί την απαίτηση Proof-of-Work.</td></tr>
</table>

Πίνακας 4 - Δομή μηνύματος στο IOTA Tangle

3.8 Επιβεβαίωση μηνύματος

Για να θεωρηθεί ένα μήνυμα ως έγκυρο, πρέπει να πληρούνται οι εξής συντακτικές προϋποθέσεις:

- Το μέγεθος του μηνύματος δεν πρέπει να ξεπερνά τα 32 KiB
- Η ανάλυση της συντακτικής δομής του μηνύματος (parsing) πρέπει να μην αφήνει κρυφές πληροφορίες - δηλαδή όλα τα στοιχεία του μηνύματος πρέπει να είναι πλήρως προσβάσιμα από τον κόμβο. Ανακριβείς πληροφορίες ενδέχεται να περιέχουν επιβλαβή κώδικα και συνεπώς απορρίπτονται.
- Ο τύπος του payload πρέπει να είναι γνωστός στον κόμβο.
- Το μήνυμα PoW Hash πρέπει να δείχνει ότι πληρούνται τα ελάχιστα κριτήρια PoW του δικτύου ή του κόμβου.
- Ο αριθμός των parent messages πρέπει να είναι από 1 έως 8.

Για να υπάρξει επεξεργασία ενός μηνύματος, πρέπει να εξασφαλιστεί ότι ικανοποιούνται οι συγκεκριμένες προϋποθέσεις και ότι μπορεί να αναγνωστεί από τον κόμβο.

3.9 Payloads

Ένα μήνυμα μπορεί να περιλαμβάνει ένα payload. Το κύριο δίκτυο mainnet, επί του παρόντος, καθορίζει τρεις κατηγορίες message payload, αλλά οι προγραμματιστές έχουν τη δυνατότητα να δημιουργήσουν προσαρμοσμένα payloads και να τα προσαρτήσουν σε μηνύματα, εφόσον πληρούν τα γενικά κριτήρια. Αυτό σημαίνει ότι ένα μήνυμα IOTA μπορεί να περιέχει διάφορα δεδομένα, συμπεριλαμβανομένου του IOTA token. Παρακάτω παρατίθεται ένας πίνακας με τα επί του παρόντος δηλωμένα βασικά payloads.

Payload	Τύπος τιμής
Payload συναλλαγής	0
Ορόσημο Payload (milestone)	1
Payload ευρετήριο (indexation)	2

Πίνακας 5 - Payloads

Ένα μήνυμα που περιέχει μόνο ένα indexation payload (δεδομένων) μπορεί να αποσταλεί χωρίς υπογραφή. Ο χρήστης μπορεί να αποθηκεύσει οποιαδήποτε πληροφορία επιθυμεί, εφόσον αυτή είναι αναλύσιμη και συμμορφώνεται με τους κανόνες δομής και μεγέθους.

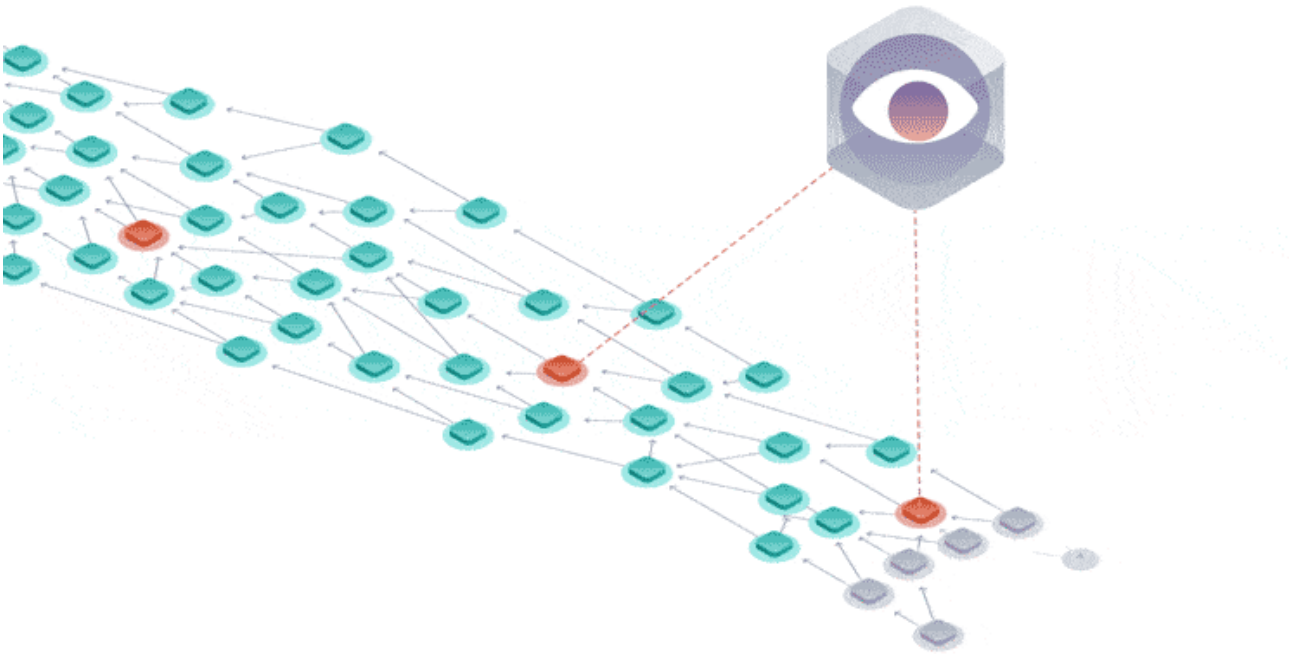
Το μήνυμα είναι αναγνωρίσιμο μέσω ενός index, το οποίο επιτρέπει σε οποιονδήποτε χρήστη να εντοπίσει το μήνυμα και τα σχετικά δεδομένα, αναζητώντας αυτόν τον index στο δίκτυο. Με αυτό το τρόπο μπορεί να δημιουργηθεί και μια "αλυσίδα" από πληροφορίες, όπως μαζικές θερμοκρασίες από ένα αισθητήρα κ.α. Το index μπορεί να χρησιμοποιηθεί ως "ευρετήριο" για τιμές ίδιου τύπου ή ενδιαφέροντος.

Σύμφωνα με τα προηγούμενα, ένα μήνυμα στο δίκτυο IOTA δεν απαιτεί έναν συγκεκριμένο παραλήπτη. Όλες οι επικοινωνίες του δικτύου μεταδίδονται σε όλους τους κόμβους και είναι διαθέσιμες σε όλους τους χρήστες του δικτύου. Επιπλέον, τα δεδομένα (data payload), εάν δεν έχουν κρυπτογραφηθεί από τον αποστολέα, είναι προσβάσιμα σε όλους τους παραλήπτες του μηνύματος.. Το πλαίσιο IOTA Streams έχει σχεδιαστεί ειδικά για την αποστολή μηνυμάτων δεδομένων μέσω του πρωτοκόλλου IOTA, τα οποία θα πρέπει να είναι διαθέσιμα μόνο σε μικρό αριθμό παραληπτών. Θα παρέχει έναν άμεσο δίαυλο επικοινωνίας προς τους παραλήπτες, ενώ παράλληλα θα κρυπτογραφεί τα δεδομένα από όλους τους υπόλοιπους στο δίκτυο, καθιστώντας το ιδανικό για ΔτΠ εφαρμογές.

Όλοι όσοι έχουν πρόσβαση στον δείκτη (index) ενός μηνύματος δεδομένων, που ορίζεται ως indexation payload, μπορούν με ευκολία να ανακτήσουν το αντίστοιχο μήνυμα. Πρέπει να γνωστοποιηθεί στον παραλήπτη ο δείκτης που χρησιμοποιήθηκε στο μήνυμα, αν θέλουμε να παραδοθεί ένα αυθαίρετο μήνυμα ή ευαίσθητα δεδομένα. Χρησιμοποιώντας έναν explorer (όπως το https://explorer.iota.org/), μπορεί να αναζητήσει στο δίκτυο όλα τα μηνύματα που περιέχουν αυτό το ευρετήριο (index).

3.10 Συντονιστής (Coordinator)

Ο Συντονιστής είναι ένας client που παρέχει υπογεγραμμένα μηνύματα, γνωστά ως ορόσημα (milestones), στα οποία βασίζονται οι κόμβοι για να επιβεβαιώσουν την επικοινωνία. Τα μηνύματα στο Tangle αξιολογούνται για επιβεβαίωση μόνο εάν αναφέρονται άμεσα ή έμμεσα από ένα πιστοποιημένο milestone.



Εικόνα 13 - Coordinator

Για την ανίχνευση γνήσιων milestones, όλοι οι κόμβοι IOTA στο ίδιο δίκτυο είναι ρυθμισμένοι με τις υπογραφές ενός αξιόπιστου κόμβου συντονιστή (coordinator node).

Η γνώση αυτών των υπογραφών επιτρέπει στους κόμβους να επικυρώνουν τις υπογραφές σε εκδοθέντα ορόσημα, για να διασφαλίσουν ότι έχουν υπογραφεί από τον αξιόπιστο συντονιστή.

Για να διασφαλιστεί ότι τα καινούργια μηνύματα επιβεβαιώνονται πάντα, ο συντονιστής μεταδίδει σε τακτική βάση (κάθε 10 δευτερόλεπτα) γνωστά milestones, υπογεγραμμένα με αυτές τις υπογραφές. Αυτή η μέθοδος εγγυάται ότι οι κόμβοι μπορούν να συγκρίνουν τους δείκτες των ορόσημων τους, για να δουν αν είναι συγχρονισμένοι με το υπόλοιπο δίκτυο.

3.11 Ανάπτυξη

Τη δεδομένη στιγμή, το IOTA βρίσκεται στην έκδοση 1.5, γνωστή ως chrysalis. Παράλληλα η ομάδα του IOTA εργάζεται πάνω σε μια εντελώς καινούρια υλοποίηση, την 2.0 (coordicide), η οποία έρχεται να βελτιώσει κατα πολύ τον τρόπο λειτουργίας της πλατφόρμας.

3.12 Nodes

Το δίκτυο των IOTA nodes ξεκίνησαν το καλοκαίρι του 2020, σε γλώσσα προγραμματισμού Go και με την ονομασία Hornet node. Με την άφιξη του Chrysalis, το IOTA χρησιμοποιώντας μια ενημερωμένη έκδοση του Hornet δημιούργησε τον νέο τους κόμβο “Bee” που βασίζεται στη γλώσσα Rust.

Το Bee, που διαθέτει πλέον και τις πιο ενημερωμένες βιβλιοθήκες του IOTA, εκτός από τη βασική του γλώσσα που είναι η rust, μπορεί να υποστηριχθεί και να χρησιμοποιηθεί μέσα από γλώσσες όπως η C, η Javascript και η Go, ανάλογα με την ανάγκη της υλοποίησης και του Hardware υλικού.

Τα nodes του IOTA μπορούν να χρησιμοποιηθούν είτε μέσα από λειτουργικό windows, Linux ή macOS. Λόγω της συνεχής ενημέρωσης της πλατφόρμας, συνίσταται η άντληση πληροφοριών εγκατάστασης και χρήσης του IOTA μέσα από την ιστοσελίδα τους ή το επίσημο GitHub repo.

Οι κόμβοι αποτελούν τον πυρήνα ενός δικτύου IOTA, χρησιμοποιώντας ειδικό λογισμικό που τους επιτρέπει να επικοινωνούν με άλλα μέρη του δικτύου και να εκτελούν σημαντικές λειτουργίες, όπως αποθήκευση και κοινή χρήση πληροφοριών.

Οι κόμβοι επιτελούν τις ακόλουθες λειτουργίες:

- Ανάρτηση νέων συναλλαγών στο Tangle
- Συγχρονισμό με το υπόλοιπο δίκτυο
- Λήψη αποφάσεων σχετικά με τις επιβεβαιώσεις των συναλλαγών
- Διατήρηση αρχείου του υπολοίπου στις διευθύνσεις.
- Παροχή των διεπαφών προγραμματισμού εφαρμογών (APIs) στους πελάτες

Προσθέτοντας νέες συναλλαγών στο Tangle

Όταν οι κόμβοι λαμβάνουν μια νέα συναλλαγή, την αποστέλλουν στο Tangle προσθέτοντάς την στην τοπική τους βάση δεδομένων. Ως αποτέλεσμα, σε οποιαδήποτε στιγμή, όλοι οι κόμβοι μπορεί να έχουν διαφορετικές συναλλαγές στις τοπικές τους βάσεις δεδομένων. Αυτές οι συναλλαγές διαμορφώνουν την αντίληψη ενός κόμβου για το Tangle. Για την κατανομή των συναλλαγών στο υπόλοιπο δίκτυο, οι κόμβοι συγχρονίζουν τις τοπικές τους βάσεις δεδομένων με τους γείτονές τους.

Συγχρονισμός δικτύου

Όπως κάθε κατανεμημένο σύστημα, όλοι οι κόμβοι που συνυπάρχουν σε ένα δίκτυο IOTA εκτελούν τον συγχρονισμό των βάσεων δεδομένων τους με τους κόμβους που βρίσκονται στο γειτονικό τους περιβάλλον, προκειμένου να δημιουργήσουν μια ενιαία πηγή πληροφοριών. Όταν ένας κόμβος, ανεξάρτητα από την τοποθεσία του στον κόσμο, λαμβάνει μια συναλλαγή, θα επιδιώξει να τη μοιραστεί με όλους τους γείτονές του. Με αυτόν τον τρόπο, **όλοι οι κόμβοι τελικά έχουν πρόσβαση σε όλες τις συναλλαγές και τις αποθηκεύουν στις τοπικές τους βάσεις δεδομένων.**

Για να επιτευχθεί συγχρονισμός, οι κόμβοι στα δίκτυα IOTA χρησιμοποιούν ένα είδος σημείων αναφοράς γνωστά ως "ορόσημα" (milestones). Αν ένας κόμβος διαθέτει στη βάση των δεδομένων του το ιστορικό των συναλλαγών, που παραπέμπουν σε ένα ορόσημο, τότε αυτό το ορόσημο θεωρείται αμετάβλητο. Κατά συνέπεια, οι κόμβοι μπορούν να αξιολογήσουν τη συγχρονισμένη κατάστασή τους, ελέγχοντας εάν ο δείκτης του τελευταίου σταθερού ορόσημου που έχει λάβει είναι ο ίδιος με τον δείκτη του πιο πρόσφατου ορόσημου που έχει λάβει. Έτσι, όταν ένας κόμβος είναι συγχρονισμένος, διαθέτει αρκετές πληροφορίες για να καθορίσει ποιες συναλλαγές θεωρεί ως επιβεβαιωμένες.

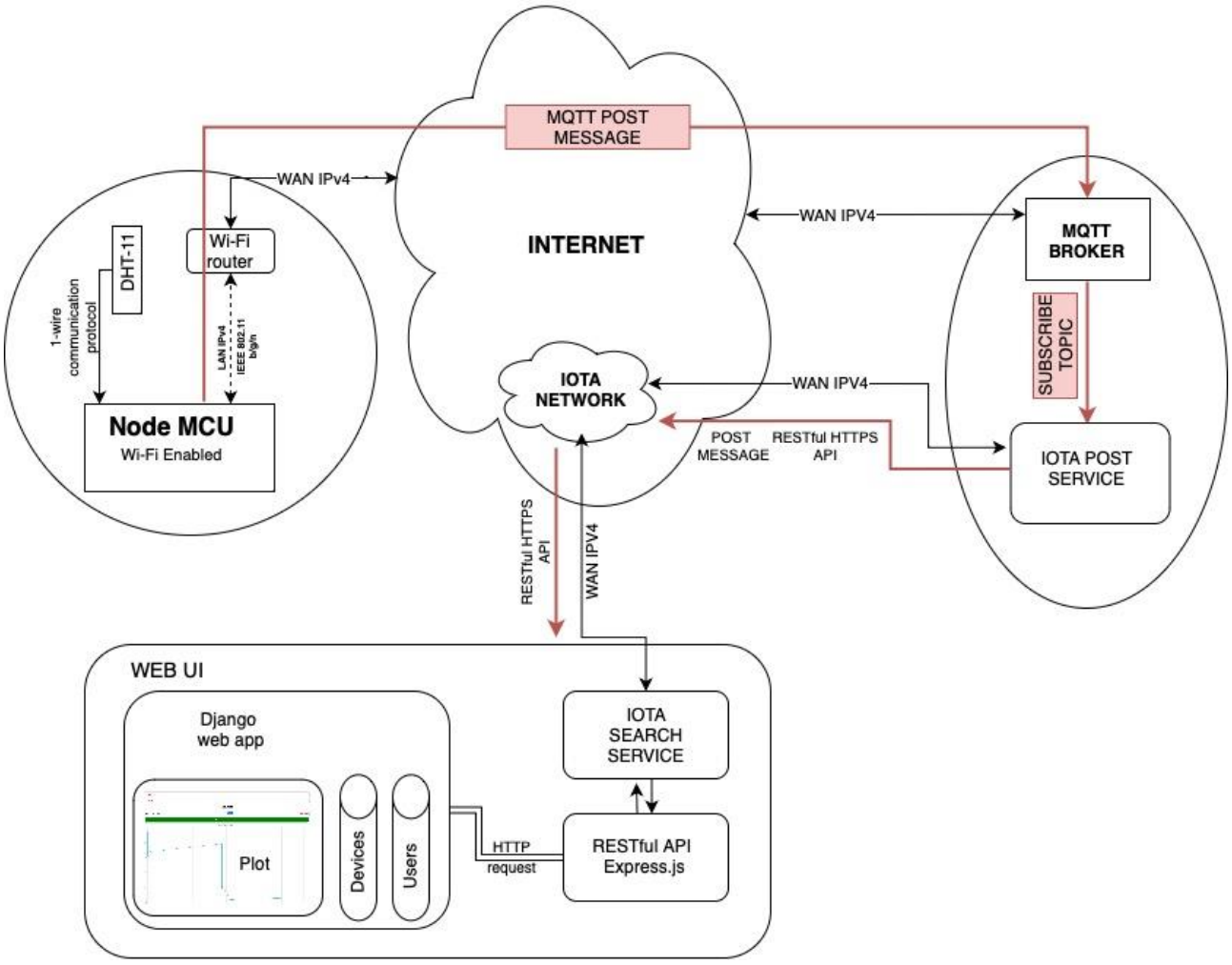
ΚΕΦΑΛΑΙΟ 4ο - ΥΛΟΠΟΙΗΣΗ

4.1 Εισαγωγή

Στη παρούσα διπλωματική, γίνεται στόχευση στη λήψη θερμοκρασιών από έναν αισθητήρα, και την αποστολή τους μέσω mqtt σε cloud υπηρεσία, όπου με τη χρήση της βιβλιοθήκης IOTA γίνεται κρυπτογράφηση και ύστερα αποστολή των δεδομένων στο IOTA Tangle. Τα δεδομένα αποθηκεύονται στο IOTA Tangle και μπορούν οποιαδήποτε στιγμή να ανακτηθούν. Για να γίνει δοκιμή σε πραγματικές συνθήκες, δημιουργήθηκε ένα πλήρες IoT οικοσύστημα, με τη πληροφορία να αποθηκεύεται στο IOTA αποκεντρωμένα. Το πειραματικό οικοσύστημα περιλαμβάνει ένα αισθητήρα θερμοκρασίας-υγρασίας, ένα Node MCU και ένα server, που διαχειρίζεται τα δεδομένα. Παρακάτω βρίσκεται η τοπολογία του πειραματικού μέρους, η οποία ακολουθείται από επί μέρους ανάλυση όλων των μερών της.

4.2 Τοπολογία

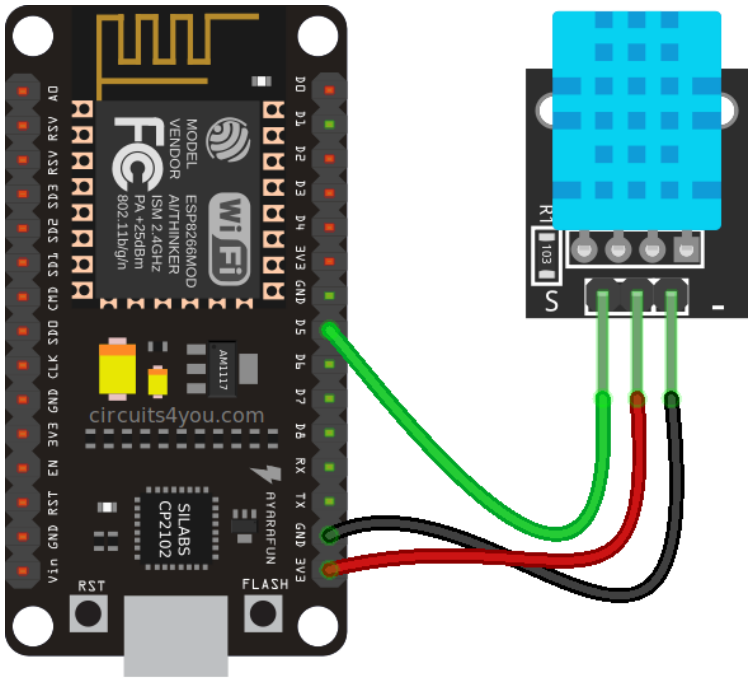
Στο παρακάτω σχήμα φαίνεται η τοπολογία του πρακτικού μέρους.



Εικόνα 14 - Τοπολογία πρακτικού μέρους

4.3 Μέρος πρώτο - Αισθητήρας

Ο ρόλος ενός αισθητήρα είναι να λάβει τη θερμοκρασία του περιβάλλοντος, στο οποίο βρίσκεται και να επικοινωνήσει με κάποια συσκευή, στέλνοντάς της ψηφιακά την πληροφορία αυτή. Ο αισθητήρας που επιλέχθηκε για να λαμβάνει τις θερμοκρασίες είναι ο DHT11, συνδεδεμένος με το ολοκληρωμένο ανοικτού κώδικα Node MCU (ESP8266). Το πρωτόκολλο επικοινωνίας μεταξύ του DHT11 και του Node MCU είναι το one-wire communication protocol. Τα δεδομένα λαμβάνονται από το Node MCU και στη συνέχεια ακολουθούν μία πορεία στο διαδίκτυο μέσω του πρωτοκόλλου επικοινωνίας "MQTT". Ο αλγόριθμος που χρησιμοποιήθηκε στο Node MCU, μετατρέπει την πληροφορία που λαμβάνει από τον αισθητήρα, ο οποίος είναι συνδεδεμένος σε κάποια από τις ψηφιακές του εισόδους, σε θερμοκρασία, χρησιμοποιώντας τη κλίμακα βαθμών Κελσίου. Όταν του ζητηθεί αυτή η θερμοκρασία, τη στέλνει στον MQTT Broker, στον οποίο είναι ρυθμισμένος να αποστέλλει τα δεδομένα.



Εικόνα 15 - Υλοποίηση καλωδίωσης DHT11 - NodeMCU

Στο NodeMCU φορτώθηκαν δύο scripts γλώσσας python.

Α. Το ένα είναι η βιβλιοθήκη "umqttsimple" του εκδότη Rui Santos[3],

Β. Το δεύτερο είναι το main.py[4] όπου έγινε παραμετροποίηση του κώδικα για τη λήψη των τιμών της θερμοκρασίας και την αποστολή των μηνυμάτων στο mqtt, βασισμένο στον κώδικα του ίδιου εκδότη.

```
# Complete project details at https://RandomNerdTutorials.com/micropython-mqtt-publish-dht11-dht22-esp32-esp8266/

import time

from umqttsimple import MQTTClient

import ubinascii

import machine

import micropython

import network

import esp

from machine import Pin

import dht

esp.osdebug(None)

import gc

gc.collect()

ssid = 'Mywifi'

password = 'mypassword'

mqtt_server = 'myMqttBrokerURL'

client_id = ubinascii.hexlify(machine.unique_id())

topic_pub_temp = 'sensor-2023-test6'

topic_pub_hum = 'sensor-2023-test6'

hum='0'

last_message = 0

message_interval = 5

station = network.WLAN(network.STA_IF)

station.active(True)

station.connect(ssid, password)

while station.isconnected() == False:

  pass
```

[3] https://github.com/RuiSantosdotme?tab=repositories

[4] https://randomnerdtutorials.com/micropython-mqtt-publish-dht11-dht22-esp32-esp8266/

```
print('Connection successful')

sensor = dht.DHT11(Pin(14))

def connect_mqtt():

  global client_id, mqtt_server

  #client = MQTTClient(client_id, mqtt_server)

  client = MQTTClient(client_id, mqtt_server, user='alkinoos', password='*******')

  client.connect()

  print('Connected to %s MQTT broker' % (mqtt_server))

  return client

def restart_and_reconnect():

  print('Failed to connect to MQTT broker. Reconnecting...')

  time.sleep(10)

  machine.reset()

def read_sensor():

  try:

    sensor.measure()

    temp = sensor.temperature()

    # uncomment for Fahrenheit

    #temp = temp * (9/5) + 32.0

    hum = sensor.humidity()

    if (isinstance(temp, float) and isinstance(hum, float)) or (isinstance(temp, int) and isinstance(hum, int)):

      temp = (b'{0:3.1f}'.format(temp))

      hum =  (b'{0:3.1f}'.format(hum))

      return temp#, hum

    else:

      return('Invalid sensor readings.')

  except OSError as e:

    return('Failed to read sensor.')

try:

  client = connect_mqtt()

except OSError as e:

  restart_and_reconnect()


while True:

  try:

    if (time.time() - last_message) > message_interval:

      temp= read_sensor()
```

```
      print(temp)

      #print(hum)

      client.publish(topic_pub_temp, temp)

      #client.publish(topic_pub_hum, hum)

      last_message = time.time()

      time.sleep(10)

  except OSError as e:

    restart_and_reconnect()
```

4.4 Μέρος Δεύτερο - Cloud services

4.4.1 MQTT BROKER - IOTA POST Services. Λήψη και αποστολή στο IOTA Tangle

Τα δεδομένα, εξερχόμενα απο το NODE MCU μέσω του πρωτοκόλλου MQTT, θα πρέπει να φτάσουν σε ένα **MQTT Broker**. Όπως αναφέρθηκε και στο θεωρητικό μέρος του MQTT, ο broker είναι ένα απαραίτητο κομμάτι του MQTT διότι λαμβάνει, στέλνει και διαχειρίζεται τα μηνύματα μεταξύ του Publisher και του Subscriber. Ο broker θα μπορούσε να αποτελεί μια αυτοτελή cloud υπηρεσία εφόσον δεν υπάρχει περιορισμός στο που μπορεί να τοποθετηθεί στην υλοποίησή μας, αρκεί να του παρέχεται πρόσβαση στο διαδίκτυο.

Στη παρούσα διπλωματική, ο broker τοποθετήθηκε εντός ενός microservice και χρησιμοποιήθηκε ως ιδιωτικός broker. Παράλληλα στην ίδια τοπολογία τοποθετήθηκε και η υπηρεσία του IOTA message post, η οποία αναλαμβάνει την αποστολή των δεδομένων που φτάνουν από το NODE MCU και μέσω του Broker στο IOTA Tangle.

Το microservice του IOTA post message, είναι γραμμένο σε γλώσσα javascript, σε περιβάλλον NodeJS.
Οι βιβλιοθήκες, που ήταν απαραίτητες για την εφαρμογή της λήψης των θερμοκρασιών μέσω mqtt, αποστολής και αναζήτησης μηνύματος από το IOTA Tangle, είναι οι εξής:

- @IOTA/client@2.2.4
- @IOTA/util.js
- @Mqtt

Το παρακάτω script που δημιουργήθηκε, λαμβάνει μέσω του MQTT, στο topic που έχει δηλωθεί, τη θερμοκρασία του αισθητήρα, και μόλις τη λάβει αυτομάτως ξεκινάει τη διαδικασία της αποστολής του στο IOTA Tangle, προσθέτοντας παράλληλα και την ώρα λήψης του μηνύματος, ώστε να γίνει σε επόμενο στάδιο η αναζήτηση και ταξινόμηση των μηνυμάτων χρονολογικά.

Καθ' όλη τη διάρκεια που το script μένει ενεργό, αναμένει τη λήψη νέου MQTT μηνύματος από τον αισθητήρα, που του έχουμε ορίσει. Όταν λάβει το μήνυμα, καλεί μια εσωτερική συνάρτηση η οποία είναι υπεύθυνη για τη προσθήκη της ημερομηνίας και ώρας λήψης της. Στη συνέχεια γίνεται κρυπτογράφηση του μηνύματος με χρήση κρυπτογραφικών αλγορίθμων και έπειτα καλείται η συνάρτηση του IOTA για την αποστολή του μηνύματος στο Tangle με το Index που έχουμε ορίσει. Το Index αποτελείται από ένα μοναδικό όνομα-ταυτότητα για κάθε αισθητήρα.

```
//---start of mqtt---

var therm ='';
var mqtt = require('mqtt');
var Topic = 'sensor-2023-test6'; //subscribe to topic
var Broker_URL = 'mqtt://my_broker_url';
var options1 = {
        clientId: 'myclientID',
        username: 'myUsername',
        password: 'myPassword',
        clean: true,
        port: 1883,
        keepalive : 60
};

var message='1';
var client  = mqtt.connect(Broker_URL, options1);
client.on('connect', mqtt_connect);
client.on('reconnect', mqtt_reconnect);
client.on('error', mqtt_error);
client.on('message', mqtt_messsageReceived);
client.on('close', mqtt_close);


function mqtt_connect()
{
    console.log("Connecting MQTT");
    client.subscribe(Topic, mqtt_subscribe);
}

function mqtt_subscribe(err, granted)
{
    console.log("Subscribed to " + Topic);
    if (err) {console.log(err);}
}
function mqtt_reconnect(err)
{
    console.log("Reconnect MQTT");
    if (err) {console.log(err);}
        client  = mqtt.connect(Broker_URL, options);
}

function mqtt_error(err)
{
  console.log("Error!");
        if (err) {console.log(err);}
}

function after_publish()
{
        //do nothing
}

function mqtt_messsageReceived(topic, message, packet)
{

        console.log('Topic=' +  topic + '  Message=' + message);
        var therm=(message);
        messagepost(therm)

}

function mqtt_close()
{
        console.log("Close MQTT");
}



async function messagepost(therm) {
    const { ClientBuilder } = require('@IOTA/client');
    var { Converter } = require('@IOTA/util.js');
dt = new Date().toISOString();

    // client will connect to testnet by default
    const client = new ClientBuilder().build();
const data = {
  temperature: therm.toString('ascii'),
  date: dt
};

const crypto = require("crypto");
const algorithm = "aes-256-cbc";
const initVector = Buffer.from([0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15]);
const Securitykey = Buffer.from([0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15]);
const message2 = JSON.stringify(data);

const cipher = crypto.createCipheriv(algorithm, Securitykey, initVector);
let encryptedData = cipher.update(message2, "utf-8", "hex");
```

```
encryptedData += cipher.final("hex");
console.log("Encrypted message: " + encryptedData);


const message = await client.message()
  .index(Topic)
  .data(encryptedData)
  .submit();

  console.log(message);

    const messagebyindex = await client.getMessage().index(Topic);


  for (message_id of messagebyindex) {
        const message_wrapper = await client.getMessage().data(message_id)
        //console.log(Buffer.from(message_wrapper.message.payload.data, 'hex').toString('utf8'));
        console.log(message_wrapper.message.payload.data);
    }
  //console.log(JSON.stringify(Converter.bytesToUtf8(messagebyindex)));
    console.log(messagebyindex);

}
```

4.4.2 Ανάλυση αποτελεσμάτων γραμμής εντολών

Κατά τη διάρκεια της κλήσης του post2.js αναμένεται από το πρόγραμμα η λήψη MQTT μηνύματος. Τη χρονική στιγμή που το πρόγραμμα λαμβάνει το MQTT μήνυμα με τη θερμοκρασία, ξεκινάει η διαδικασία αποστολής του στο Tangle του IOTA.

```
parallels@ubuntu-linux-22-04-desktop:~/UNIWA/V101/scripts$ node post2.js
Connecting MQTT
Subscribed to sensor-4kPwIE
Topic=sensor-4kPwIE  Message=9.39
{
  message: {
    networkId: '6514788332515804015',
    parentMessageIds: [
      '176ed28a9a79d09237aaf75b15a92acf2e4ae1f08d61dc4a7a8cc3c47736d586',
      '4dfd4682375bc67f27c5a5816bf4a5906bf1649d242a3baa94f0acea8c55b313',
      '840e5aa897d9487549314beb51d9784f1e8452ee37a812e2a42e0cf323fea21b',
      'f49740d2356bc712dde09e97e5fc0eb29de40651ffffacb30a1ab0c4d9afa91e'
    ],
    payload: {
      type: 2,
      index: '73656e736f722d346b50774945',
      data: '4320392e33392c20323032332d30312d32395431363a34333a33342e3439355a'
    },
    nonce: '9223372036854883392'
  },
  messageId: '76bdeefdbe40f4cc76b301107daa5a9373374c53fe882c69f152424503dadc98'
}
[]
```

Εικόνα 16 - Αποτελέσματα του post.js στη γραμμή εντολών

Μέσω της γραμμής εντολών γίνεται άντληση των εξής πληροφοριών, για τη συναλλαγή που ολοκληρώθηκε:

NetworkId: Αναφέρεται σε έναν αριθμό που προσδιορίζει σε ποιο δίκτυο IOTA ανήκει το μήνυμα (Mainnet / Testnet / ιδιωτικό δίκτυο) - Οι κόμβοι θα δέχονται μόνο μηνύματα που προσδιορίζονται ως μέρος του δικτύου στο οποίο ανήκει ο κόμβος. Εμείς βρισκόμαστε στο Chrysalis devnet.

ParentMessageIds: Όπως έχουμε αναφέρει προηγουμένως για τα parent messages, το script μας επιστρέφει τα Parent Message Ids, τα οποία χρειάζονται ώστε να επαληθευτεί η συναλλαγή μας.

Στη συνέχεια ξεκινάει το μέρος του δικού μας μηνύματος.

Το **Payload type:2**, αναφέρεται σε Payload τύπου 2,ευρετήριο (indexation). Το **Index** είναι το όνομα του αισθητήρα που έχουμε ορίσει, εμφανιζόμενο σε μορφή δεκαεξαδικού. Το **data** είναι το σώμα του μηνύματος, δηλαδή η θερμοκρασία και η ημερομηνία-ώρα λήψης της. **Nonce:** Είναι το αποτέλεσμα του PoW (Proof of work) της συναλλαγής, που μόλις δημιουργήθηκε.

MessageId: Αναφέρεται στον μοναδικό αριθμό-ταυτότητα της συναλλαγής μας. Το MessageId είναι πολύ σημαντικό, γιατί με αυτή τη μοναδική ταυτότητα μπορούμε να επαληθεύσουμε ότι το μήνυμα που έπειτα θα διαβάσουμε απο το Tangle, το έχουμε στείλει εμείς.

4.4.3 Αναζήτηση στο IOTA Tangle

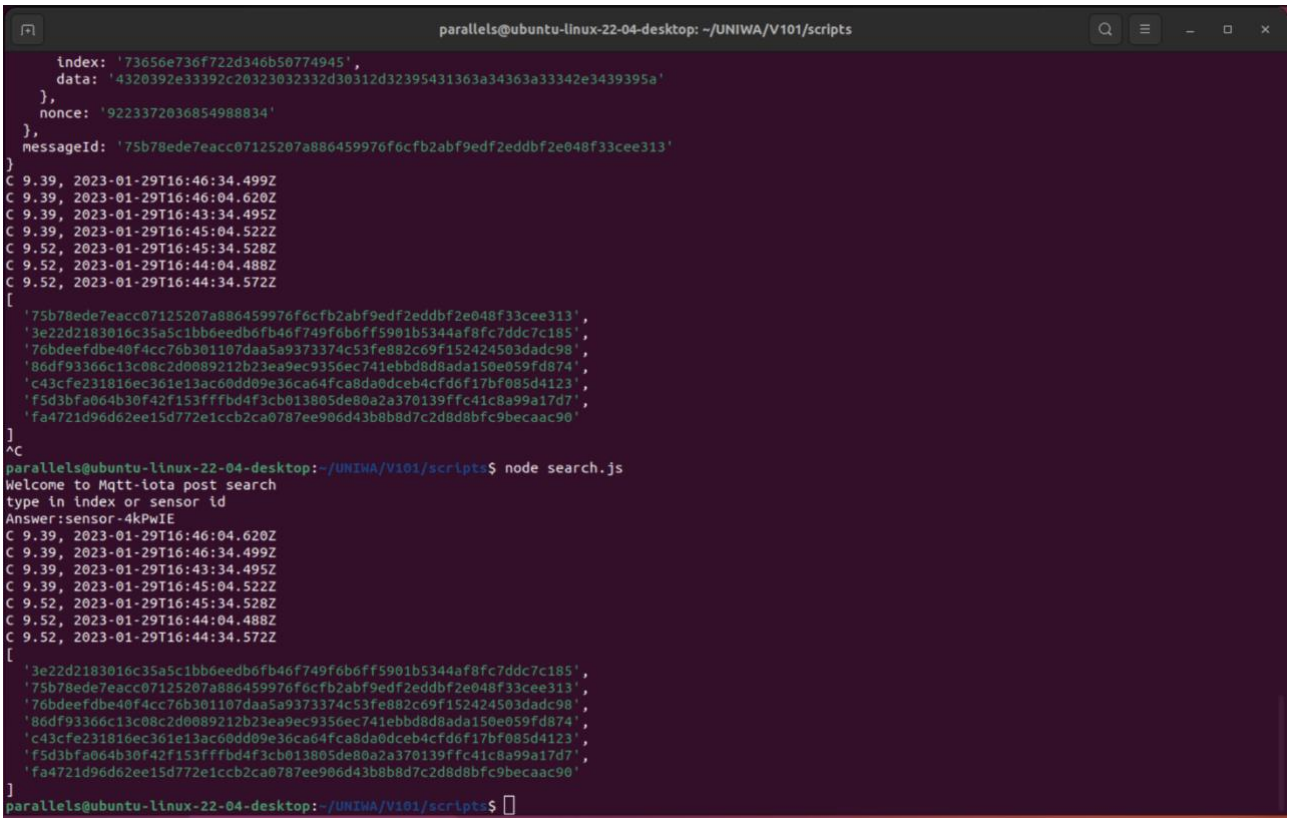
Εισαγωγή

Για να γίνει περισσότερο κατανοητός ο τρόπος λειτουργίας της αναζήτησης μηνύματος στο IOTA Tangle, είναι δυνατή η χειροκίνητη αναζήτηση πολλαπλών μηνυμάτων με το ίδιο θέμα, στο Tangle, μέσω της γραμμής εντολών. Προτού δημιουργηθεί η τελική μορφή της υπηρεσίας, μπορεί να γίνει εκτέλεση του παρακάτω κώδικα, στον οποίο δηλώνοντας το όνομα του αισθητήρα, ή πιο γενικά το Index (θέμα) με το οποίο έχουν γίνει post τα μηνύματα, αυτό επιστρέφει όλα τα μηνύματα που θα βρει στο Tangle με το index αυτό. Η αναζήτηση των index στο IOTA Tangle γίνεται με το παρακάτω script. Κάθε φορά που καλείται, αναμένει την εισαγωγή του Index από το χρήστη, ώστε να αρχίσει την αναζήτηση όλων των μπλοκ που έχουν δημοσιευτεί στο Tangle.

```
  const { ClientBuilder } = require('@IOTA/client');
const crypto = require("crypto");
async function search(sensor_id) {
  const client = new ClientBuilder().build();
  const messagebyindex = await client.getMessage().index(sensor_id);
  const temps = [];
  for (message_id of messagebyindex) {
    const message_wrapper = await client.getMessage().data(message_id);

    const algorithm = "aes-256-cbc";
    const initVector = Buffer.from([0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15]);
    const Securitykey =
Buffer.from([0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15]);
    const decipher = crypto.createDecipheriv(algorithm, Securitykey, initVector);

    const message_data2 = Buffer.from(message_wrapper.message.payload.data, 'hex').toString('utf8');
    let decryptedData = decipher.update(message_data2, "hex", "utf-8");
    decryptedData += decipher.final("utf8");
    //console.log("Decrypted message: " + decryptedData);


    //const message_data = JSON.parse(Buffer.from(message_wrapper.message.payload.data, 'hex').toString('utf8'));
    const message_data = JSON.parse(decryptedData);
    const temperature = message_data.temperature;
    //console.log(temperature);
    const date = new Date(message_data.date);
    temps.push({ temperature, date });
  }
    temps.sort((a, b) => a.date - b.date);
    console.log(JSON.stringify(temps));
  return temps;
}

// Check if the script is being run from the command line
if (require.main === module) {
  const sensor_id = process.argv[2];
  if (sensor_id) {
    search(sensor_id);
```

```
  } else {
    console.error('Please provide a sensor_id as an argument.');
  }
}

module.exports = {
  search,
};
```

Η αναζήτηση των μηνυμάτων γίνεται με παρόμοιο τρόπο όπως και η αποστολή. Καλούμε το "search.js", στη συνέχεια πληκτρολογούμε το όνομα του αισθητήρα, και ύστερα γίνεται αναζήτηση στο Tangle για όλα τα μηνύματα που έχουν αυτό το Index.



Εικόνα 17 - Αποτελέσματα αναζήτησης στο IOTA Tangle μέσω του Search.js

Η αναζήτηση μας επιστρέφει όλα τα Message data που βρίσκει στο Tangle του IOTA, με το δοσμένο Index (sensor id). Στη συνέχεια μας επιστρέφει όλα τα Message IDs των μηνυμάτων που βρέθηκαν. Ο τρόπος με τον οποίο μπορούμε να διαχειριστούμε αυτά τα μηνύματα ποικίλλει.

Για παράδειγμα, στη τελική μορφή της εφαρμογής μας, ξεχωρίζουμε και ταξινομούμε τη θερμοκρασία από τη χρονική στιγμή της λήψης της, ώστε να μπορούμε να κάνουμε σωστή απεικόνιση των αποτελεσμάτων κατά χρονολογική σειρά.

4.5 Μέρος τρίτο - Διεπαφή χρήστη

4.5.1 Django – Διαδικτυακή εφαρμογή

Εικόνα 18 - Λογότυπο Django

Το Django είναι μια διαδικτυακή εφαρμογή υψηλού επιπέδου σε γλώσσα Python, που επιτρέπει την ταχεία ανάπτυξη ασφαλών και συντηρήσιμων ιστότοπων. Είναι ανοικτού κώδικα και περιλαμβάνει όλα τα εργαλεία που χρειάζεται ένας προγραμματιστής, για να δημιουργήσει μια εφαρμογή στο διαδίκτυο και να επικοινωνήσουν με αυτή πολλαπλοί χρήστες [23]. Χρησιμοποιεί τη δομή MVT (Model View Template), το οποίο αναφέρεται στο μοντέλο (model) ως βάση δεδομένων, τη προβολή (view) ως έλεγχος λειτουργειών και πρότυπο (template) ως διεπαφή και περιβάλλον χρήστη. Λόγω της δυνατότητας ταχείας ανάπτυξής του, το Django είναι πλέον απαραίτητο στην τρέχουσα αγορά, διότι απαιτείται πολύ λιγότερος χρόνος για τη δημιουργία οποιασδήποτε εφαρμογής [24].

Εγκατασταση Django

1. Πρέπει να εγκαταστήσουμε το Django στο τοπικό μας περιβάλλον, πράγμα που σημαίνει ότι πρέπει να εγκατασταθούν η python και το pip.
   Αφού εγκατασταθεί η python & pip εκτελείται η εντολή **pip3 install Django** στο τερματικό για εγκατάσταση του Django.
2. Αφού εγκατασταθεί το Django, το επόμενο βήμα είναι η δημιουργία ενός νέου project.

   1. Εκτέλεση της εντολής:
   Django-admin startproject projectName
   Για τη δημιουργία μιας σειράς από αρχεία εκκίνησης για το project.

   2. Εκτέλεση της εντολής:
   cd projectName
   Για πλοήγηση στο νέο φάκελο του έργου.

   3.Για να ξεκινήσουμε το διακομιστή δίνουμε την εξής εντολή στο τερματικό:
   python manage.py runserver
   Ώστε να ξεκινήσει ένας τοπικός διακομιστής στο σύστημά σας.

   4.Στο πρόγραμμα περιήγησης επισκεπτόμαστε τη διεύθυνση
   http://localhost:8000/ , για να μεταβούμε στη προεπιλεγμένη σελίδα

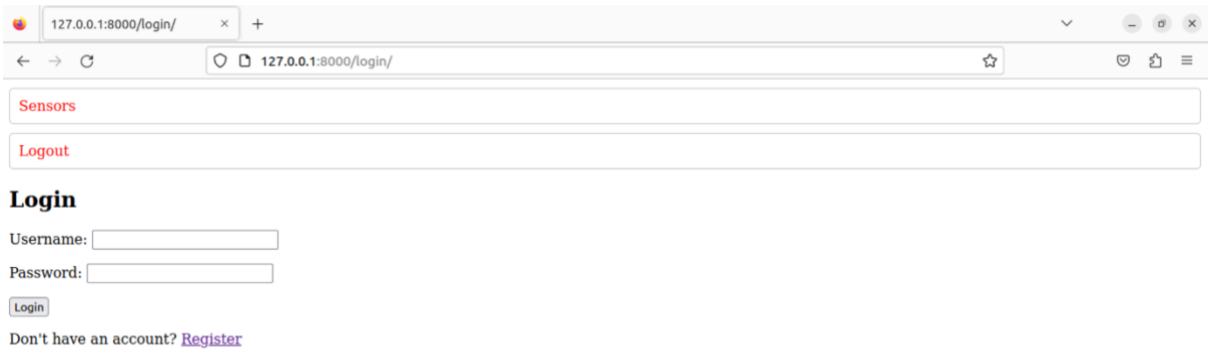
Γιατί να επιλέξουμε Django

Παρακάτω παραθέτονται μερικοί λόγοι υπέρ της χρήσης του Django [25].

1. Ανοικτού κώδικα σημαίνει δωρεάν λογισμικό.
2. Ταχύτερος προγραμματισμός - ανάπτυξη εφαρμογής
3. Πλήρως επεκτάσιμο
4. Προτεραιότητα στην ασφάλεια
5. Ενσωματωμένη πύλη διαχείρισης

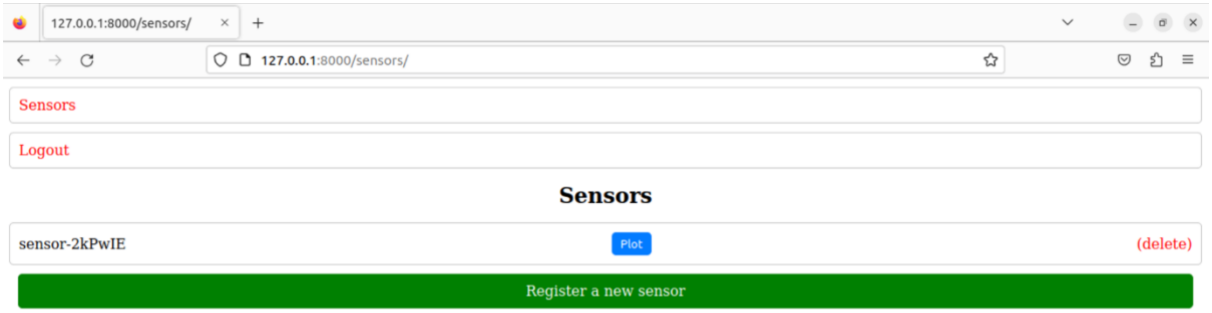
4.5.2 Διεπαφή

Στο τελικό στάδιο της εργασίας δημιουργήθηκε μια πλατφόρμα διεπαφής χρήστη, σε περιβάλλον Django, στην οποία χρήστες μπορούν να κάνουν εγγραφή και έπειτα σύνδεση, με σκοπό να προσθέσουν τους αισθητήρες που διαθέτουν, δίνοντας το μοναδικό όνομα που έχει δημιουργηθεί για κάθε αισθητήρα.

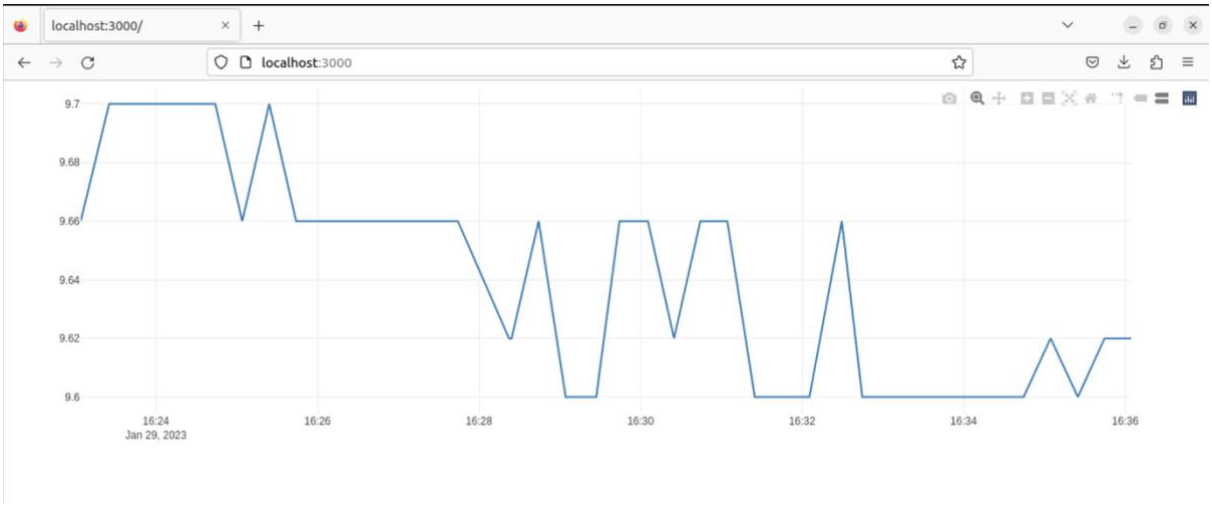


Εικόνα 19 - Σελίδα σύνδεσης χρήστη στο Django

Μόλις ο χρήστης δημιουργήσει λογαριασμό μπορεί να προσθέσει τον αισθητήρα του στη λίστα. Πατώντας το κουμπί "plot", το Django καλεί ένα microservice γραμμένο σε γλώσσα Javascript σε περιβάλλον Nodejs, το οποίο λειτουργεί ως "γέφυρα" ανάμεσα στο Django και την υπηρεσία search, που δημιουργήθηκε για την αναζήτηση του IOTA Tangle. Το microservice αυτό, είναι απαραίτητο διότι μπορεί να καλέσει το Nodejs αρχείο της αναζήτησης μηνυμάτων στο Tangle, λαμβάνοντας από το Django το όνομα του αισθητήρα. Αφού γίνει η αναζήτηση των μηνυμάτων βάση του Index, το microservice επιστρέφει ως HTTP request τα δεδομένα στο Django, όπου και καλείται μια ακόμη συνάρτηση η οποία μας δίνει την εικόνα του διαγράμματος.



Το συγκεκριμένο script κάθε φορά που λαμβάνει μια θερμοκρασία την εκχωρεί στο γράφημα, και παράλληλα ανανεώνει κάθε 2 λεπτά τη σελίδα διεπαφής του χρήστη. Ο χρόνος ανανέωσης της σελίδας είναι ενδεικτικός και μπορεί να παραμετροποιηθεί από το Django. Στη παρακάτω εικόνα διακρίνουμε τη σελίδα του γραφήματος για λήψη θερμοκρασιών σε διάστημα 10 λεπτών



Εικόνα 20 - Γράφημα στο διαχειριστικό του Django

Με τον τρόπο αυτό πλέον, ο χρήστης έχει άμεση και ασφαλή πρόσβαση στον αισθητήρα και είναι σε θέση να κάνει προβολή και διαχείριση της λίστας των αισθητήρων.

ΚΕΦΑΛΑΙΟ 5ο ΑΠΟΤΕΛΕΣΜΑΤΑ & ΣΥΜΠΕΡΑΣΜΑΤΑ

5.1 Αποτελέσματα

Στα πλαίσια της διπλωματικής εργασίας μελετήθηκαν οι τεχνολογίες IoT, MQTT, DLT, IOTA Ledger και Django. Υλοποιήθηκε μια πρωτότυπη IoT συσκευή με χρήση του Node MCU και ενός αισθητήρα θερμοκρασίας, που στέλνει και αποθηκεύει τα δεδομένα στο IOTA Ledger. Για τις ανάγκες της διπλωματικής εργασίας, υλοποιήθηκε επιπρόσθετα μία διαδικτυακή εφαρμογή που μπορεί να διαχειριστεί χρήστες και συσκευές καθώς και να απεικονίσει τα δεδομένα τους.

Για την υλοποίηση της παραπάνω εφαρμογής ήταν αναγκαία η εκμάθηση των γλωσσών javascript, python καθώς και του Framework του Django. Στη συνέχεια έγινε πληθώρα δοκιμών με χρήστες που είχαν διαφορετικά δικαιώματα και διαφορετικό αριθμό συσκευών. Οι δοκιμές που πραγματοποιήθηκαν στέφθηκαν όλες με επιτυχία.

Παράλληλα λόγω των συνεχών αναβαθμίσεων του IOTA, ήταν αναγκαία η συνεχής ενημέρωση και προσαρμογή των εφαρμογών που δημιουργήθηκαν. Τα δεδομένα, λόγω της χρήσης του δικτύου Developers net (Chrysalis Devnet) η αποθήκευση των δεδομένων έχει πεπερασμένη χρονική διάρκεια.

5.2 Στόχοι βελτίωσης

Η ενασχόληση με καινούριες γλώσσες προγραμματισμού έφερε στο προσκήνιο ανάγκες και ιδέες που θα μπορούσαν να επιτευχθούν σε μελλοντικό χρόνο, μαζί με τη βοήθεια της ομάδας του IOTA, ώστε να μεγιστοποιηθεί η ασφάλεια και η χρηστικότητα αυτής της εφαρμογής. Το IOTA βρίσκεται συνεχώς σε καθεστώς εξέλιξης και δημιουργίας νέων τεχνολογιών, και ήδη βρίσκεται μερικά βήματα πριν μοιραστεί με το κοινό τη νέα έκδοση του IOTA streams. Στη νέα έκδοση, υλοποιούνται βιβλιοθήκες που θα τοποθετούν την υπηρεσία εντός του μικροεπεξεργαστή, όπως του NODE MCU, λόγω της μειωμένης ανάγκης πλέον για υπολογιστική ισχύ.

Ένας ακόμη στόχος είναι η βελτίωση της διαδικτυακής εφαρμογής μέσω της αναβάθμισης του περιβάλλοντος διεπαφής χρήστη. Όπως για παράδειγμα θα μπορούσαν να προστεθούν πληροφορίες που αφορούν τη κατάσταση και την υγεία της IoT συσκευής και του δικτύου.

5.3 Συμπεράσματα

Η παρούσα διπλωματική εργασία έχει ως στόχο την υλοποίηση ενός συστήματος λήψης δεδομένων από ένα αισθητήρα ΔτΠ, στη συνέχεια το διαμοιρασμό αυτής της πληροφορίας με τη χρήση ενός DLT εργαλείου, που στη παρούσα εργασία υπήρξε το IOTA, και τέλος η αναζήτηση αυτού του μηνύματος μέσω του μοναδικού ονόματος ή ταυτότητας του αισθητήρα.

Για την εργασία αυτή ήταν απαραίτητη η εμβάθυνση σε αρκετές διαφορετικές τεχνολογίες, και γλώσσες προγραμματισμού, που όλες μαζί αποτέλεσαν ένα κοινό εργαλείο για ένα κοινό σκοπό. Η γνώση των ΔτΠ συστημάτων και "έξυπνων αισθητήρων", η χρήση του MQTT, η θεωρία και η πρακτική εφαρμογή των DLT αλλά και των γλωσσών προγραμματισμού Javascript, html, rust, python είναι μερικά από τα εργαλεία που χρειάζεται ένας μηχανικός για να σχεδιάσει ένα

ολοκληρωμένο πληροφοριακό σύστημα στο οποίο να επιτυγχάνονται αμετάβλητα δεδομένα στο Διαδίκτυο των Πραγμάτων.

Με τη χρήση της Τεχνολογίας Κατανεμημένου Κατάστιχου (Distributed Ledger Technology), που όπως είδαμε, εμβαθύνοντας σε αυτό, αποτελεί ένα πολύ ισχυρό εργαλείο στην τεχνολογία του σήμερα, αλλά και με τεράστιες προοπτικές επέκτασης στο μέλλον, αποδείξαμε ότι η αμεταβλητότητα των δεδομένων στο πλαίσιο του Διαδικτύου των Πραγμάτων, είναι πραγματοποιήσιμη με τη χρήση εργαλείων όπως είναι το IOTA ή αντίστοιχων τεχνολογιών DLT. Γνωρίζοντας καλύτερα τη διαδικασία διαμοιρασμού μιας πληροφορίας μέσω της Τεχνολογίας Κατανεμημένου Κατάστιχου, καθίσταται διακριτή πλέον η προοπτική περαιτέρω ανάπτυξης που έχει αυτή στον τομέα του ΔτΠ. Παράλληλα είναι σχεδόν βέβαιο πως με τις βελτιώσεις που μπορεί να δεχθεί μελλοντικά, θα αποτελέσει ένα αυτόνομο αλλά και ασφαλές εργαλείο μετάδοσης δεδομένων από μια εξουσιοδοτημένη ΔτΠ συσκευή προς το IOTA Ledger, με σκοπό την κατανεμημένη αποθήκευση των αμετάβλητων δεδομένων.

Βιβλιογραφία

[1] L. Tawalbeh, F. Muheidat, M. Tawalbeh και M. Quwaider, IoT Privacy and security: Challenges and solutions, τόμ. 10, Mdpi, 2020, p. 4102.

[2] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal και B. Sikdar, A survey on IoT security: application areas, security threats, and solution architectures, τόμ. 7, IEEE, 2019, pp. 82721-82743.

[3] R. Mahmoud, T. Yousuf, F. Aloul και I. Zualkernan, Internet of things (IoT) security: Current status, challenges and prospective measures, 2015, pp. 336-341.

[4] F. Chen, Y. Huo, J. Zhu και D. Fan, A review on the study on MQTT security challenge, 2020, pp. 128-133.

[5] B. Mishra και A. Kertesz, The use of MQTT in M2M and IoT systems: A survey, τόμ. 8, IEEE, 2020, pp. 201071-201086.

[6] M. A. Khan, M. A. Khan, S. U. Jan, J. Ahmad, S. S. Jamal, A. A. Shah, N. Pitropakis και W. J. Buchanan, A deep learning-based intrusion detection system for mqtt enabled iot, τόμ. 21, MDPI, 2021, p. 7016.

[7] J. Li και M. Kassem, Applications of distributed ledger technology (DLT) and Blockchain-enabled smart contracts in construction, τόμ. 132, Elsevier, 2021, p. 103955.

[8] D. Featherston και others, Cassandra: Principles and application, 2010, p. 27.

[9] R. Maull, P. Godsiff, C. Mulligan, A. Brown και B. Kewell, Distributed ledger technology: Applications and implications, τόμ. 26, Wiley Online Library, 2017, pp. 481-489.

[10] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa και A. Bani-Hani, Blockchain smart contracts: Applications, challenges, and future trends, τόμ. 14, Springer, 2021, pp. 2901-2925.

[11] S. Ali, G. Wang, B. White και R. L. Cottrell, A blockchain-based decentralized data storage and access framework for pinger, 2018, pp. 1303-1308.

[12] Y. Takefuji, Security Protection Mechanisms Must Be Embedded in Blockchain Applications, τόμ. 97, ACS Publications, 2020, pp. 1819-1820.

[13] Y. Li, B. Cao, M. Peng, L. Zhang, L. Zhang, D. Feng και J. Yu, Direct acyclic graph-based ledger for Internet of Things: Performance and security analysis, τόμ. 28, IEEE, 2020, pp. 1643-1656.

[14] M. Kalisch και P. Bühlman, Estimating high-dimensional directed acyclic graphs with the PC-algorithm., τόμ. 8, 2007.

[15] F. M. Benčić και I. P. Žarko, Distributed ledger technology: Blockchain compared to directed acyclic graph, 2018, pp. 1569-1570.

[16] J. C. Digitale, J. N. Martin και M. M. Glymour, Tutorial on directed acyclic graphs, τόμ. 142, Elsevier, 2022, pp. 264-267.

[17] V. Vasiliauskaite, T. S. Evans και P. Expert, Cycle analysis of Directed Acyclic Graphs, τόμ. 596, Elsevier, 2022, p. 127097.

[18] M. Zichichi, S. Ferretti και G. D'Angelo, A distributed ledger based infrastructure for smart transportation system and social good, 2020, pp. 1-6.

[19] E. Drasutis, IOTA smart contracts, Jan, 2022.

[20] W. F. Silvano και R. Marcelino, Iota Tangle: A cryptocurrency to communicate Internet-of-Things data, τόμ. 112, Elsevier, 2020, pp. 307-319.

[21] S. Rochman, J. E. Istiyanto, A. Dharmawan, V. Handika και S. R. Purnama, Optimization of tips selection on the IOTA tangle for securing blockchain-based IoT transactions, τόμ. 216, Elsevier, 2023, pp. 230-236.

[22] C. P. Igiri, D. Bhargava, C. Udanor και A. R. Sowah, Blockchain versus IOTA Tangle for Internet of Things: The Best Architecture, CRC Press, 2022, pp. 259-278.

[23] S. Jaiswal και R. Kumar, Learning Django Web Development, τόμ. 336, Packt Publishing, 2015.

[24] H. Gore, R. K. Singh, A. Singh, A. P. Singh, M. Shabaz, B. K. Singh και V. Jagota, Django: Web development simple & fast, τόμ. 25, 2021, pp. 4576-4585.

[25] G. C. Hillar, Django RESTful Web Services: The Easiest Way to Build Python RESTful APIs and Web Services with Django, Packt Publishing Ltd, 2018.