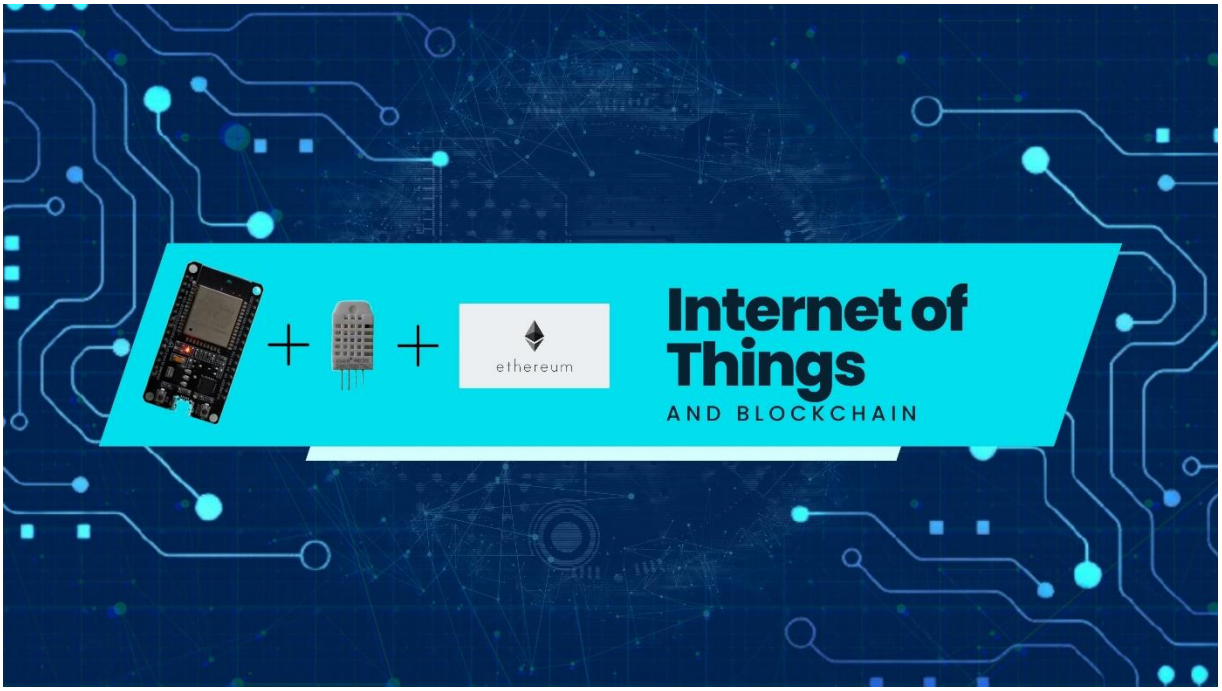
ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ & ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ

Διπλωματική Εργασία

Χρήση της τεχνολογίας κατανεμημένου καθολικού για αποθήκευση δεδομένων ενός συστήματος του διαδικτύου των πραγμάτων



Φοιτητής: Μαντζουράτου Μαρία
ΑΜ: 50106532

Επιβλέπων Καθηγητής

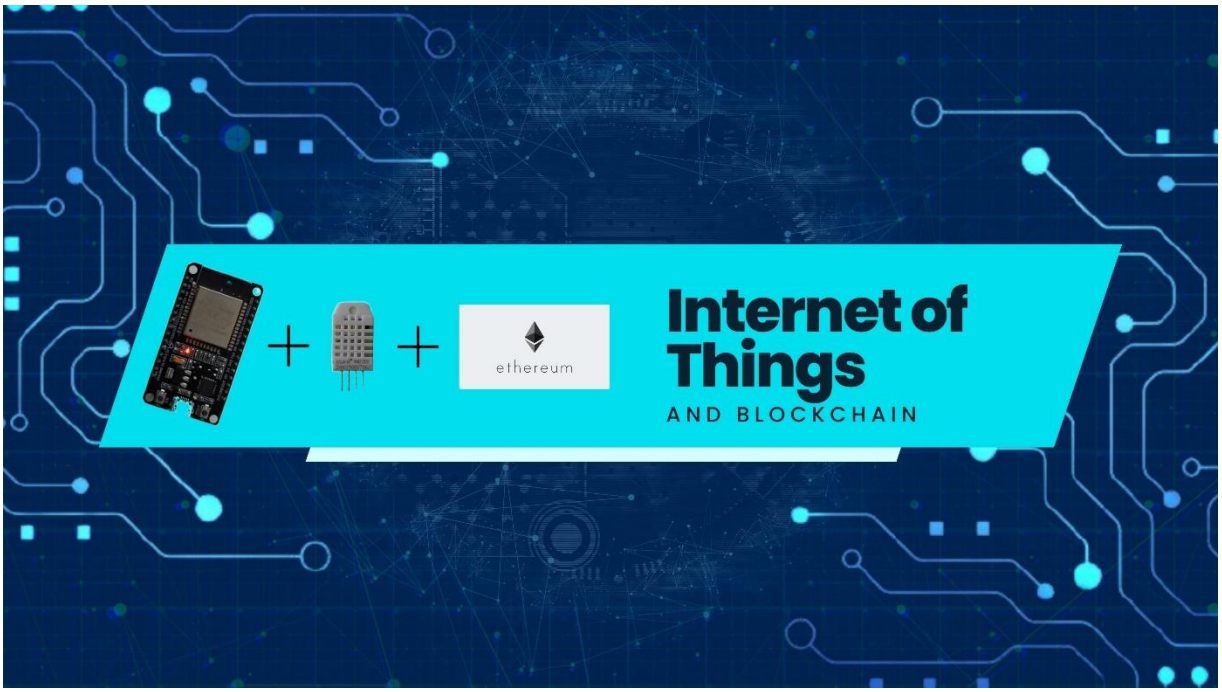
Κόγιας Δημήτριος
Ακαδημαϊκός Υπότροφος

ΑΘΗΝΑ-ΑΙΓΑΛΕΩ, Ιούλιος 2024

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

Diploma Thesis

Using Distributed Ledger Technology for data storage of an Internet of Things system



Student: Mantzouratou Maria
Registration Number: 50106532

Supervisor

Kogias Dimitrios
Academic Scholar

ATHENS-EGALEO, July 2024

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

Κόγιας Δημήτριος, Ακαδημαϊκός Υπότροφος	Πατρικάκης Χαράλαμπος, Καθηγητής	Παπαδόπουλος Περικλής, Καθηγητής
Dimitrios Kogias Digitally signed by Dimitrios Kogias Date: 2024.07.29 12:03:16 +03'00' (Υπογραφή)	Digitally signed by CHARALAMPOS PATRIKAKIS Date: 2024.07.31 09:16:01 +03'00' (Υπογραφή)	PERIKLIS PAPADOPOULOS Digitally signed by PERIKLIS PAPADOPOULOS Date: 2024.07.31 09:40:00 +03'00' (Υπογραφή)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο/η κάτωθι υπογεγραμμένος/η Μαντζουράτου Μαρία του Σπυρίδωνος, με αριθμό μητρώου 50106532 φοιτητής/τρια 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.
Επιθυμώ την απαγόρευση πρόσβασης στο πλήρες κείμενο της εργασίας μου μέχρι …… και έπειτα από αίτησή μου στη Βιβλιοθήκη και έγκριση του επιβλέποντος/ουσας καθηγητή/ήτριας.»

Ο/Η Δηλών/ούσα
Μαντζουράτου Μαρία

(Υπογραφή φοιτητή/ήτριας)

Περίληψη

Η αυξανόμενη εξάπλωση των συσκευών Διαδικτύου των Πραγμάτων (IoT) έχει οδηγήσει σε μαζική ροή δεδομένων που παράγονται από αυτές τις διασυνδεδεμένες συσκευές. Οι παραδοσιακές κεντρικές λύσεις αποθήκευσης δεδομένων αντιμετωπίζουν σημαντικές προκλήσεις στη διαχείριση των μεγάλων όγκων δεδομένων IoT και την αντιμετώπιση ζητημάτων ασφάλειας, διαφάνειας και αξιοπιστίας. Αυτή η διπλωματική εργασία εξετάζει την ολοκλήρωση της τεχνολογίας Blockchain σε ένα σύστημα IoT, χρησιμοποιώντας τον μικροελεγκτή ESP32 και τον αισθητήρα DHT22, για την επίτευξη αποτελεσματικής και ασφαλούς αποθήκευσης δεδομένων.

Η μελέτη ξεκινά με την παρουσίαση των βασικών εννοιών του IoT και της τεχνολογίας Blockchain, με έμφαση στα μοναδικά χαρακτηριστικά που καθιστούν το Blockchain μια ελκυστική επιλογή για την αντιμετώπιση των περιορισμών των συμβατικών μεθόδων αποθήκευσης δεδομένων σε συστήματα IoT. Μια εκτενής ανασκόπηση της βιβλιογραφίας για την αποθήκευση δεδομένων IoT με χρήση Blockchain παρέχει απόψεις για την τρέχουσα κατάσταση, εντοπίζει κενά στην έρευνα και προτείνει δυνατές κατευθύνσεις για μελλοντική έρευνα.

Το κείμενο παρουσιάζει τον σχεδιασμό και την υλοποίηση ενός καινοτόμου συστήματος IoT. Χρησιμοποιεί τον μικροελεγκτή ESP32 για τη συλλογή περιβαλλοντικών δεδομένων μέσω του αισθητήρα DHT22 και αποθηκεύει ασφαλώς αυτά τα δεδομένα με τη χρήση της τεχνολογίας Blockchain. Η αποκεντρωμένη φύση του Blockchain εξασφαλίζει την αμεταβλητότητα των δεδομένων και την ανοχή σφαλμάτων, βελτιώνοντας τη συνολική αξιοπιστία της υποδομής IoT.

Τα αποτελέσματα δείχνουν ότι το σύστημα IoT που ενισχύεται από την τεχνολογία Blockchain παρέχει βελτιωμένη ασφάλεια κατά την αντιμετώπιση της παραποίησης δεδομένων, μειωμένη ευπάθεια σε μοναδικά σημεία αποτυχίας και ενισχυμένη διαφάνεια στη διαχείριση δεδομένων. Ωστόσο, η μελέτη εντοπίζει επίσης ορισμένες προκλήσεις, συμπεριλαμβανομένης της κλιμάκωσης και των απαιτήσεων πόρων, που ενθαρρύνουν περαιτέρω έρευνα και προτάσεις βελτιστοποίησης.

Συνοψίζοντας, αυτή η διπλωματική εργασία υπογραμμίζει το δυναμικό της τεχνολογίας Blockchain ως μια εφικτή λύση για την αποθήκευση δεδομένων σε συστήματα IoT, ειδικά όταν χρησιμοποιείται ο μικροελεγκτής ESP32 και ο αισθητήρας DHT22. Τα ευρήματα προσφέρουν πολύτιμες πληροφορίες για τις διαρκείς προσπάθειες βελτίωσης της ενσωμάτωσης της τεχνολογίας Blockchain στην υποδομή IoT, προσφέροντας καθοδήγηση σε ερευνητές, προγραμματιστές και επαγγελματίες που αναζητούν ασφαλείς και αποκεντρωμένες λύσεις διαχείρισης δεδομένων στον κόσμο των διασυνδεδεμένων συσκευών. Εκμεταλλευόμενοι τα πλεονεκτήματα της τεχνολογίας αυτής, τα συστήματα IoT μπορούν να επωφεληθούν από την ενισχυμένη ασφάλεια και αξιοπιστία των δεδομένων, προετοιμάζοντας το έδαφος για ένα πιο ανθεκτικό και αποδοτικό οικοσύστημα IoT στο μέλλον.

Λέξεις – κλειδιά

Blockchain, Διαδίκτυο των Πραγμάτων (ΔτΠ), Αποθήκευση Δεδομένων, ESP32, DHT22, Αποκέντρωση, Ασφάλεια, Αξιοπιστία, Έξυπνες Συσκευές

Abstract

The increasing prevalence of Internet of Things (IoT) devices has led to a massive influx of data generated by these interconnected devices. Traditional centralized data storage solutions face significant challenges in managing the vast volumes of IoT data while addressing security, transparency, and reliability concerns. This thesis explores the integration of blockchain technology into an IoT system, utilizing the ESP32 microcontroller and DHT22 sensor, to achieve efficient and secure data storage.

The study begins by introducing the fundamental concepts of IoT and blockchain technology, emphasizing the unique features that make blockchain an attractive candidate for addressing the limitations of conventional data storage methods in IoT systems. An extensive literature review on blockchain-based IoT data storage provides insights into the current state of the art, identifies research gaps, and suggests potential directions for future investigation.

Building on this foundation, the thesis presents the design and implementation of a novel IoT system. It utilizes the ESP32 microcontroller to collect environmental data through the DHT22 sensor and securely stores this data using blockchain technology. The decentralized nature of blockchain ensures data immutability and fault tolerance, enhancing the overall reliability of the IoT infrastructure.

To evaluate the effectiveness of the proposed solution, a series of experiments are conducted to assess data storage efficiency, data retrieval speeds, and resource utilization. A comparative analysis against traditional centralized storage systems quantifies the benefits and limitations of blockchain integration for IoT data storage.

The results demonstrate that the blockchain-enabled IoT system provides improved security against data tampering, reduced vulnerability to single points of failure, and enhanced transparency in data management. However, the study also identifies certain challenges, including scalability and resource requirements, prompting further research and optimization recommendations.

In conclusion, this thesis highlights the potential of blockchain technology as a viable solution for data storage in IoT systems, particularly when utilizing the ESP32 microcontroller and DHT22 sensor. The findings contribute valuable insights to the ongoing efforts to enhance blockchain integration into IoT infrastructure, offering guidance to researchers, developers, and practitioners seeking secure and decentralized data management solutions in the realm of interconnected devices. By leveraging the strengths of blockchain technology, IoT systems can benefit from enhanced data security and reliability, laying the groundwork for a more robust and efficient IoT ecosystem in the future.

Keywords

Blockchain, IoT, Data Storage, ESP32, DHT22, Decentralization, Security, Reliability, Smart Devices.

Περιεχόμενα

Κατάλογος Πινάκων

Κατάλογος Εικόνων

ΕΙΣΑΓΩΓΗ

Τα τελευταία χρόνια, ο αναπτυσσόμενος τομέας του Διαδικτύου των Πραγμάτων (IoT) έχει εισάγει έναν διασυνδεδεμένο κόσμο, όπου συσκευές, αισθητήρες και συστήματα που επικοινωνούν και συνεργάζονται για να βελτιστοποιήσουν την αποτελεσματικότητα πολλών βιομηχανιών. Με την πολλαπλασιαστική αύξηση των συσκευών IoT και των μαζικών ποσοτήτων δεδομένων που δημιουργούν, η ανάγκη για αξιόπιστες, ασφαλείς και κλιμακούμενες λύσεις αποθήκευσης δεδομένων έχει γίνει μία πρωταρχική ανησυχία. Ως απάντηση σε αυτές τις προκλήσεις, η ένταξη της τεχνολογίας Blockchain στα συστήματα IoT έχει εμφανιστεί ως μια ελπιδοφόρα λύση, υπόσχοντας να επαναστατήσει τον τρόπο που διαχειριζόμαστε, αποθηκεύουμε και ασφαλίζουμε τα δεδομένα από συσκευές IoT.

Το Blockchain, αρχικά έγινε γνωστό ως η θεμελιώδης τεχνολογία στα κρυπτονομίσματα και έχει εξελιχθεί σε ένα ευέλικτο και αποκεντρωμένο πλαίσιο με ευρείες εφαρμογές πέρα από τις χρηματοοικονομικές συναλλαγές. Τα ενσωματωμένα χαρακτηριστικά του, όπως η διαφάνεια, η αναλλοίωτη φύση και η ανθεκτικότητα στις παραβιάσεις το καθιστούν ιδανικό, για την αντιμετώπιση των κρίσιμων ζητημάτων της ακεραιότητας δεδομένων, της ασφάλειας και της εμπιστοσύνης στα οικοσυστήματα IoT.

Η παρούσα διπλωματική αποσκοπεί στην εξερεύνηση της συμβιωτικής σχέσης μεταξύ των τεχνολογιών IoT και Blockchain, με έμφαση στην εκμετάλλευση του Blockchain για την αποθήκευση δεδομένων που παράγονται από συσκευές IoT. Αναλύοντας τις κύριες προκλήσεις που αντιμετωπίζουν τα συμβατικά κεντρικά συστήματα αποθήκευσης δεδομένων στα περιβάλλοντα IoT, αυτή η έρευνα θα εξετάσει τα δυνητικά οφέλη και τις πρακτικές συνέπειες της υιοθέτησης του Blockchain ως εναλλακτικής αποκεντρωμένης λύσης αποθήκευσης δεδομένων.

Αντικείμενο της διπλωματικής εργασίας

Το αντικείμενο της διπλωματικής εργασίας είναι η μελέτη και ανάπτυξη της χρήσης της τεχνολογίας blockchain για την αποθήκευση δεδομένων σε συστήματα Διαδικτύου των Πραγμάτων (IoT). Συγκεκριμένα, εξετάζει την ενσωμάτωση του blockchain σε ένα σύστημα IoT που χρησιμοποιεί τον μικροελεγκτή ESP32 και τον αισθητήρα DHT22.

Η διπλωματική εργασία αποσκοπεί στην ανάπτυξη μιας πρακτικής και αξιόπιστης λύσης που ενσωματώνει την τεχνολογία του blockchain στο σύστημα IoT, προσφέροντας βελτιωμένη ασφάλεια των δεδομένων, πρόληψη απάτης, καθώς και αποτροπή ανεπιθύμητων μεταβολών στα δεδομένα. Επιπλέον, η ενσωμάτωση του blockchain αντιμετωπίζει το πρόβλημα των κεντρικών σημείων αποτυχίας, προσφέροντας αξιοπιστία και ανθεκτικότητα στο σύστημα.

Σκοπός και στόχοι

Ο σκοπός αυτής της εργασίας είναι να διερευνήσει τη χρήση της τεχνολογίας blockchain για την αποθήκευση δεδομένων σε συστήματα Διαδικτύου των Πραγμάτων (IoT) που χρησιμοποιούν τον μικροελεγκτή ESP32 και τον αισθητήρα DHT22.

Μεθοδολογία

Η μεθοδολογία που θα ακολουθηθεί για την εκπόνηση αυτής της διπλωματικής εργασίας έχει σχεδιαστεί με γνώμονα την συστηματική προσέγγιση, την ολοκληρωμένη έρευνα και την αποτελεσματική υλοποίηση των στόχων.

- Συλλογή απαραίτητης βιβλιογραφίας για όλες τις τεχνολογίες που θα χρησιμοποιηθούν.

- Εύρεση παρόμοιων εφαρμογών που έχουν υλοποιηθεί.
- Προσπάθεια υλοποίησης και προγραμματισμού του συστήματος.
- Συμπεράσματα και μελλοντική εργασία.

Καινοτομία

Τα καινοτόμα και πρωτότυπα στοιχεία της διπλωματικής εργασίας περιλαμβάνουν:

Εφαρμογή της Τεχνολογίας Blockchain στο IoT: Η χρήση της τεχνολογίας blockchain στον τομέα του Internet of Things (IoT) είναι αναδυόμενη και αποτελεί ένα πρωτότυπο πεδίο έρευνας. Στην εργασία αυτή, θα εξεταστεί πώς το blockchain μπορεί να ενσωματωθεί με επιτυχία σε ένα σύστημα IoT, προσφέροντας ασφάλεια και αξιοπιστία στη διαχείριση δεδομένων των συνδεδεμένων συσκευών.

Ασφάλεια Δεδομένων μέσω του Blockchain: Το Blockchain παρέχει ένα ασφαλές πλαίσιο για την αποθήκευση δεδομένων, όπου κάθε μπλοκ συσχετίζεται με το προηγούμενο μπλοκ, και οι αλλαγές δεν μπορούν να πραγματοποιηθούν χωρίς τη συναίνεση όλων των μελών του δικτύου. Στην εργασία αυτή, θα μελετηθεί πώς η τεχνολογία Blockchain μπορεί να ενισχύσει την ασφάλεια των δεδομένων και να τα προστατεύσει από ανεπιθύμητη τροποποίηση.

Δομή

Στο πρώτο κεφάλαιο γίνεται μια εισαγωγή στην τεχνολογία Blockchain, περιλαμβάνοντας την προέλευση, τη διάκριση μεταξύ δημοσίων και ιδιωτικών blockchain, και την ιστορία του Ethereum. Επίσης, παρουσιάζονται τα βασικά χαρακτηριστικά και έννοιες που σχετίζονται με το Ethereum, όπως η αποθήκευση ιδιωτικών κλειδιών, τα blocks, τα μοντέλα συναίνεσης, η απόδειξη εργασίας (proof of work) και τα έξυπνα συμβόλαια.

Στο δεύτερο κεφάλαιο αναλύεται το Διαδίκτυο των Πραγμάτων (IoT), η ενσωμάτωσή του με την τεχνολογία blockchain και οι δυσκολίες που προκύπτουν κατά την ενσωμάτωση τους. Επιπλέον, εξετάζονται θέματα ασφάλειας και έξυπνων συμβολαίων στο πλαίσιο του IoT. Στο τρίτο κεφάλαιο παρουσιάζονται υλοποιήσεις blockchain που είναι συμβατές με το IoT, περιλαμβάνοντας πλατφόρμες και εφαρμογές. Επιπλέον, εξετάζονται αρχιτεκτονικές των εφαρμογών τους και η εφαρμογή των έξυπνων συμβολαίων.

Το τέταρτο και τελευταίο κεφάλαιο περιλαμβάνει την υλοποίηση ενός συστήματος IoT και τη σύνδεσή του με την πλατφόρμα Ethereum. Συγκεκριμένα, αναλύονται τα μέσα που χρησιμοποιούνται, όπως το Arduino, το ESP32 και ο αισθητήρας DHT22. Επιπλέον, παρουσιάζεται η πειραματική διάταξη και τέλος αναφέρονται τα συμπεράσματα και οι προοπτικές για μελλοντική εργασία.

1 ΚΕΦΑΛΑΙΟ 1ο : Εισαγωγή στην τεχνολογία Blockchain

Η τεχνολογία Blockchain έχει αναδειχθεί ως μια πρωτοποριακή καινοτομία με τη δυνατότητα να διαταράξει τις παραδοσιακές βιομηχανίες και να αναδιαμορφώσει το ψηφιακό μας τοπίο. Η αποκεντρωμένη και αμετάβλητη φύση του προσφέρει μοναδικά πλεονεκτήματα, όπως ενισχυμένη ασφάλεια, διαφάνεια και εμπιστοσύνη μεταξύ των συμμετεχόντων. Αυτό το κεφάλαιο χρησιμεύει ως εισαγωγή στην τεχνολογία blockchain, θέτοντας τις βάσεις για μια λεπτομερή εξερεύνηση των εσωτερικών λειτουργιών της.

1.1 Ορισμός και προέλευση

Ο ορισμός υπογραμμίζει την αποκεντρωμένη φύση του blockchain και τη λειτουργία του ως κατανεμημένου καθολικού. Το Blockchain ορίζεται ως μια τεχνολογία που επιτρέπει την ασφαλή και διαφανή καταγραφή και επαλήθευση των συναλλαγών, χρησιμοποιώντας ένα δίκτυο υπολογιστών για τη διατήρηση μιας κοινής βάσης δεδομένων.

Η τεχνολογία του Blockchain μπορεί να χαρακτηριστεί ως μια από τις μεγαλύτερες εφευρέσεις του αιώνα, δεδομένης της επίδρασης που έχει σε διάφορους τομείς, όπως στον χρηματοοικονομικό, τη βιομηχανία, ακόμα και την εκπαίδευση. Άγνωστο σε πολλούς είναι το γεγονός ότι η ιστορία του Blockchain, ξεκινάει στις αρχές του 1990. Τα τελευταία χρόνια όμως έχει αρχίσει να γίνεται πιο δημοφιλές και να χρησιμοποιείται σε διάφορες εφαρμογές. [5]

Οι Stuart Haber και W. Scott Stornetta δημιούργησαν τον πρώτο τύπο του Blockchain το 1991, που αποτελούταν από μια κρυπτογραφικά ασφαλή αλυσίδα από block με την οποία κανείς δεν μπορούσε να παραβιάσει τις χρονικές σημάνσεις των εγγράφων. Ένα χρόνο αργότερα, αναβάθμισαν το σύστημά τους ώστε να περιλαμβάνει τα Merkle trees τα οποία ενίσχυσαν την αποτελεσματικότητα επιτρέποντας έτσι τη συλλογή περισσότερων εγγράφων σε ένα block. Ωστόσο το 2008 η ιστορία του blockchain αρχίζει να γίνεται αυτό που γνωρίζουμε σήμερα χάρη στο έργο του Satoshi Nakamoto. Τότε σχεδίασε το πρώτο blockchain από όπου η τεχνολογία εξελίχθηκε και βρήκε το δρόμο της σε πολλές εφαρμογές πέρα από τα κρυπτονομίσματα. Ο Satoshi Nakamoto κυκλοφόρησε την πρώτη δημοσίευση σχετικά με την τεχνολογία το 2009. Εκεί, παρείχε λεπτομέρειες για το πώς η τεχνολογία ήταν καλά εξοπλισμένη για να ενισχύσει την ψηφιακή εμπιστοσύνη, δεδομένης της πτυχής της αποκέντρωσης που σήμαινε ότι κανείς δεν θα είχε ποτέ τον έλεγχο. [5]

Πριν το Bitcoin υπήρχαν κι άλλα συστήματα ηλεκτρονικών χρημάτων, αλλά κανένα από αυτά δεν πέτυχε ευρεία χρήση. Η χρήση του Blockchain βοήθησε το Bitcoin να εφαρμοστεί σε ένα κατανεμημένο σύστημα, όπου κανένας χρήστης δεν είχε τον έλεγχο των ηλεκτρονικών χρημάτων και έτσι δεν υπήρξε αποτυχία σε κανένα σημείο, το οποίο βοήθησε στην προώθηση της χρήσης του. Το κυριότερο πλεονέκτημά του ήταν να επιτρέπει τις άμεσες συναλλαγές μεταξύ χρηστών χωρίς την ανάγκη κάποιου αξιόπιστου τρίτου. Επίσης, επέτρεψε την δημιουργία καινούριων κρυπτονομισμάτων για ανταμοιβή σε όσους χρήστες καταφέρνουν να δημιουργήσουν νέα Block και να διατηρήσουν αντίγραφα του καθολικού (οι χρήστες αυτοί λέγονται miners στο Bitcoin). Η αυτοματοποιημένη πληρωμή των χρηστών επέτρεψε την κατανεμημένη διαχείριση του συστήματος. [7]

Στο Bitcoin, το Blockchain επιτρέπει στους χρήστες να είναι ανώνυμοι, αλλά τα αναγνωριστικά των λογαριασμών τους δεν είναι ανώνυμα. Επίσης, όλες οι συναλλαγές είναι ορατές δημόσια. Αυτό επέτρεψε στο Bitcoin να προσφέρει ψευδοανωνυμία επειδή οι λογαριασμοί δημιουργούνται χωρίς καμία διαδικασία ταυτοποίησης. [7]

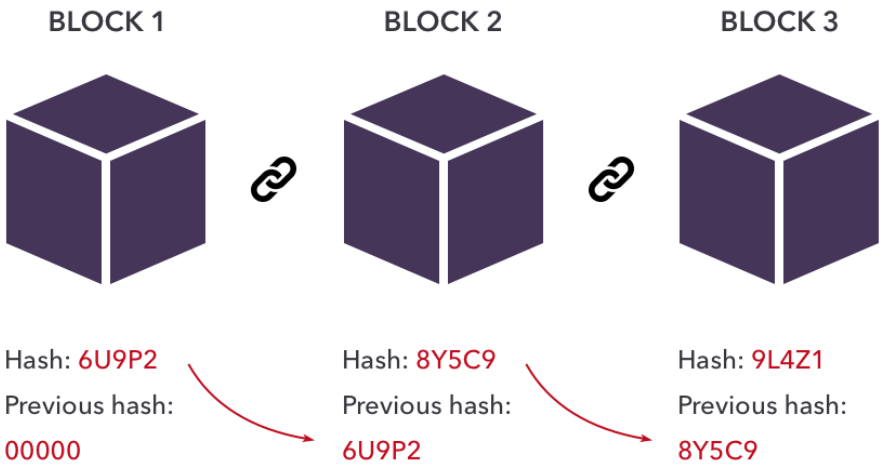
Εφόσον το Bitcoin επιτρέπει την ανωνυμία, ήταν σημαντικό να υπάρχουν μηχανισμοί που να δημιουργούν εμπιστοσύνη σε ένα περιβάλλον που οι χρήστες δεν μπορούν να ταυτοποιηθούν εύκολα. Πριν τη χρήση της τεχνολογίας του Blockchain, η εμπιστοσύνη αυτή προερχόταν από μεσολαβητές που εμπιστεύονταν και οι δυο μεριές. Χωρίς αυτούς, η αναγκαία εμπιστοσύνη μέσα σε ένα Blockchain δίκτυο ενεργοποιείται από τα παρακάτω χαρακτηριστικά:

- Καθολικό – η τεχνολογία χρησιμοποιεί ένα καθολικό για να παρέχει πλήρες ιστορικό συναλλαγών. Σε αντίθεση με τις κλασσικές βάσεις δεδομένων, οι συναλλαγές και οι αξίες σε ένα Blockchain δεν παρακάμπτονται.
- Ασφάλεια – τα Blockchain είναι κρυπτογραφικά ασφαλή, εξασφαλίζοντας ότι τα δεδομένα που περιέχονται στο καθολικό δεν έχουν παραβιαστεί και είναι επιβεβαιωμένα.
- Διαφάνεια – το καθολικό είναι κοινοποιημένο μεταξύ πολλαπλών συμμετεχόντων. Αυτό παρέχει διαφάνεια σε όλους, στο Blockchain δίκτυο.
- Κατανομή – το Blockchain μπορεί να είναι κατανεμημένο. Αυτό επιτρέπει την κλιμάκωση του αριθμού των κόμβων ενός δικτύου Blockchain για να γίνει πιο ανθεκτικό σε επιθέσεις από κακούς παράγοντες. Αυξάνοντας τον αριθμό των κόμβων, η ικανότητα ενός κακού παράγοντα να επηρεάσει το συναινετικό πρωτόκολλο, που χρησιμοποιείται στο Blockchain, μειώνεται. [7]

Για την καλύτερη κατανόηση του Blockchain, θα γίνει μια αναφορά στο κατανεμημένο εδάφιο (Distributed ledger). Το κατανεμημένο εδάφιο θα μπορούσε να συγκριθεί με μία βάση δεδομένων η οποία είναι στην κατοχή και μπορεί να ενημερωθεί από τον κάθε χρήστη (ή κόμβο) σε ένα μεγάλο δίκτυο. Οι καταγραφές αυτές δεν διαχειρίζονται από έναν κεντρικό φορέα αλλά αντίθετα κατασκευάζονται και διαχειρίζονται από τον κάθε κόμβο που συμμετέχει στο δίκτυο. Στη συνέχεια κάθε κόμβος του δικτύου επεξεργάζεται κάθε συναλλαγή βγάζοντας ο καθένας ένα αποτέλεσμα και τελικά ψηφίζεται το αποτέλεσμα στο οποίο συμφωνεί η πλειοψηφία. Έπειτα ενημερώνεται το εδάφιο και ο κάθε κόμβος κρατάει από ένα ίδιο αντίγραφο. [3]

Σε αντίθεση με τη βάση δεδομένων, σε ένα εδάφιο δεν γίνεται αλλαγή ή διαγραφή των δεδομένων παρά μόνο πρόσθεση καινούριων συναλλαγών. [1]

Ένα Blockchain είναι μία κατανεμημένη δομή δεδομένων που καταγράφει όλες τις συναλλαγές που έχουν πραγματοποιηθεί στο δίκτυό του, επιτρέποντας την ανταλλαγή συναλλαγών μεταξύ χρηστών που δεν έχουν μεταξύ τους εμπιστοσύνη και χωρίς την ανάγκη για αξιόπιστο τρίτο πρόσωπο. Το Blockchain αποτελείται από μια ταξινομημένη λίστα blocks, με κάθε block να αναγνωρίζεται από το κρυπτογραφικό του αποτύπωμα και να αναφέρει το αποτύπωμα του προηγούμενου block, δημιουργώντας έτσι μια αλυσίδα από blocks. Κάθε block περιέχει ένα σύνολο συναλλαγών Όσο προστίθενται νέα blocks, τα παλιότερα γίνονται δυσκολότερο να τροποποιηθούν. Τα νέα blocks αναπαράγονται σε όλα τα αντίγραφα του δικτύου, επιλύοντας αυτόματα τυχόν συγκρούσεις χρησιμοποιώντας τους καθιερωμένους κανόνες. [1],[7]



Εικόνα 1.1: Αλυσίδα από Blocks [30]

1.2 Δημόσιο και ιδιωτικό Blockchain

Υπάρχουν πολλοί διαφορετικοί τύποι τεχνολογίας blockchain που είναι κατάλληλοι για διαφορετικές περιπτώσεις χρήσης. Για παράδειγμα, υπάρχουν δημόσια Blockchain και ιδιωτικά Blockchain.

Ένα δημόσιο blockchain δεν έχει περιορισμούς. Οποιοσδήποτε έχει σύνδεση στο διαδίκτυο μπορεί να αποκτήσει πρόσβαση στο δίκτυο και να ξεκινήσει την επικύρωση μπλοκ και την αποστολή συναλλαγών. Τυπικά, τέτοια δίκτυα τείνουν να προσφέρουν κάποιου είδους αμοιβή για χρήστες που επικυρώνουν τα μπλοκ.

Ούτως ή άλλως, αυτό το δίκτυο τείνει να χρησιμοποιεί αλγόριθμους συναίνεσης Proof of Work ή Proof of Stake για την επικύρωση των συναλλαγών. Είναι ένα «δημόσιο» δίκτυο με την πραγματική έννοια.

Ήταν το μοντέλο που πρότεινε ο Satoshi Nakamoto το 2009. Αργότερα, οι επιχειρηματικές εταιρείες άρχισαν να δείχνουν ενδιαφέρον για την τεχνολογία blockchain και τροποποίησαν τη φύση του αποκεντρωμένου καθολικού και εισήγαγαν τις ιδιωτικές αλυσίδες μπλοκ.

Στο δημόσιο blockchain, μπορεί να γίνει λήψη του πρωτοκόλλου ανά πάσα στιγμή και δεν θα χρειαστεί άδεια από κανέναν. Τα δημόσια blockchain απεικονίζουν το ιδανικό μοντέλο που κάνει τον κλάδο της τεχνολογίας τόσο επικερδή.

Έτσι, είναι εντελώς αποκεντρωμένο, κανένας οργανισμός δεν ελέγχει το οικοσύστημα. Ενώ ένα ιδιωτικό blockchain μπορεί να αλλάξει και να τροποποιηθεί από τον ιδιοκτήτη του οργανισμού. [23]

1.3 Η ιστορία του Ethereum

Ο Vitalik Buterin ήταν ένας από τους ερευνητές που ένιωθαν ότι το Bitcoin δεν εκμεταλλευόταν όλες τις δυνατότητες του Blockchain. Έτσι ξεκίνησε να φτιάξει ένα εύπλαστο δίκτυο Blockchain το οποίο θα μπορούσε να εκτελεί διάφορες λειτουργίες πέρα του να είναι ένα κατανεμημένο. Το Ethereum γεννήθηκε σαν δημόσιο Blockchain το 2013 με πρόσθετες λειτουργίες συγκριτικά με το Bitcoin, κάτι το οποίο αποδείχθηκε κομβική στιγμή στην ιστορία του Blockchain. [5]

Ενεργοποιώντας τη δυνατότητα που επιτρέπει στους χρήστες να δημιουργούν έξυπνα συμβόλαια (smart contracts), ο Vitalik κατάφερε να διαφοροποιήσει το Ethereum από το Bitcoin και το έκανε μια πλατφόρμα ανάπτυξης αποκεντρωμένων εφαρμογών πέρα από κρυπτονόμισμα. [5]

Από τη στιγμή που κυκλοφόρησε το Ethereum επίσημα, έχει εξελιχθεί σε μια από τις μεγαλύτερες εφαρμογές της τεχνολογίας του Blockchain δεδομένης της ικανότητάς του να υποστηρίζει έξυπνα συμβόλαια (smart contracts) που χρησιμοποιούνται για την εκτέλεση διαφόρων λειτουργιών. [5]

1.4 Βασικά χαρακτηριστικά και έννοιες που σχετίζονται με το Ethereum

Έξυπνα συμβόλαια: Ένα από τα καθοριστικά χαρακτηριστικά του Ethereum είναι η δυνατότητα εκτέλεσης έξυπνων συμβολαίων. Τα έξυπνα συμβόλαια είναι αυτοεκτελούμενες συμφωνίες που έχουν τους όρους (της συμφωνίας) απευθείας γραμμένους σε γραμμές κώδικα στο blockchain Ethereum. Εκτελούν αυτόματα ενέργειες μόλις εκπληρωθούν προκαθορισμένες προϋποθέσεις, παρέχοντας εμπιστοσύνη, ασφάλεια και αυτοματισμό σε διάφορες εφαρμογές.

Ether (ETH): Το Ether είναι το εγγενές κρυπτονόμισμα της πλατφόρμας Ethereum. Εξυπηρετεί πολλαπλούς σκοπούς εντός του δικτύου.

Αποκεντρωμένες εφαρμογές (DApps): Το Ethereum επιτρέπει την ανάπτυξη αποκεντρωμένων εφαρμογών, γνωστών και ως DApps. Τα DApps είναι χτισμένα στο blockchain Ethereum, αξιοποιώντας τη λειτουργικότητα του έξυπνου συμβολαίου για τη δημιουργία εφαρμογών που είναι ανθεκτικές στη λογοκρισία, το χρόνο διακοπής λειτουργίας και τις δόλιες δραστηριότητες. Τα DApps έχουν τη δυνατότητα να διαταράξουν τις παραδοσιακές βιομηχανίες και να εισαγάγουν νέα μοντέλα διακυβέρνησης και ιδιοκτησίας.

1.5 Κρυπτογραφία ασύμμετρου κλειδιού

Η τεχνολογία του Blockchain χρησιμοποιεί κρυπτογραφία ασύμμετρου κλειδιού (αναφέρεται επίσης ως κρυπτογραφία δημόσιου κλειδιού). Η κρυπτογραφία ασύμμετρου κλειδιού χρησιμοποιεί ένα ζευγάρι κλειδιών, ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί τα οποία είναι μαθηματικά συγγενή. Το δημόσιο κλειδί, παρόλο που είναι δημόσιο, είναι φτιαγμένο με τέτοιο τρόπο, που δεν μειώνεται η ασφάλεια, αλλά το ιδιωτικό κλειδί πρέπει να παραμείνει κρυφό για να διατηρήσουν τα δεδομένα την κρυπτογραφική τους προστασία. Παρόλο που τα κλειδιά έχουν άμεση σχέση μεταξύ τους, δεν μπορεί κάποιος να προσδιορίσει το ιδιωτικό κλειδί με βάση το δημόσιο. Για την κρυπτογράφηση μπορεί να χρησιμοποιηθεί είτε το δημόσιο είτε το ιδιωτικό κλειδί, ενώ για την αποκρυπτογράφηση χρησιμοποιείται το κλειδί που δεν χρησιμοποιήθηκε στην κρυπτογράφηση. [7]

Η κρυπτογραφία ασύμμετρου κλειδιού επιτρέπει μια σχέση εμπιστοσύνης μεταξύ των χρηστών οι οποίοι δεν γνωρίζονται ή δεν υπάρχει εμπιστοσύνη μεταξύ τους, προσφέροντας ένα μηχανισμό επαλήθευσης της ακεραιότητας και της γνησιότητας των συναλλαγών ενώ ταυτόχρονα επιτρέπει στις συναλλαγές να παραμένουν δημόσιες. Για να γίνει αυτό, οι συναλλαγές είναι «ψηφιακά υπογεγραμμένες». Αυτό σημαίνει ότι ένα ιδιωτικό κλειδί έχει χρησιμοποιηθεί για την κρυπτογράφηση μιας συναλλαγής έτσι ώστε οποιοσδήποτε έχει ένα δημόσιο κλειδί να μπορεί να το αποκρυπτογραφήσει. Εφόσον το δημόσιο κλειδί διατίθεται ελεύθερα, η κρυπτογράφηση της συναλλαγής με το ιδιωτικό κλειδί αποδεικνύει ότι ο υπογράφων έχει πρόσβαση στο ιδιωτικό κλειδί. Εναλλακτικά, αν η κρυπτογράφηση δεδομένων γίνει με το δημόσιο κλειδί του χρήστη, τότε η αποκρυπτογράφηση θα μπορεί να γίνει μόνο από όσους έχουν πρόσβαση στο ιδιωτικό κλειδί. Ένα μειονέκτημα όμως της κρυπτογραφίας ασύμμετρου κλειδιού είναι ότι είναι αργή στον υπολογισμό. [7]

Αυτό έρχεται σε αντίθεση με την κρυπτογραφία συμμετρικού κλειδιού στην οποία χρησιμοποιείται ένα μόνο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Με την κρυπτογραφία συμμετρικού κλειδιού οι χρήστες πρέπει να έχουν ήδη μια σχέση εμπιστοσύνης μεταξύ τους, για την ανταλλαγή του κοινόχρηστου κλειδιού. Σε ένα συμμετρικό σύστημα, τυχόν κρυπτογραφημένα

δεδομένα που μπορούν να αποκρυπτογραφηθούν με το κοινόχρηστο κλειδί επιβεβαιώνει ότι στάλθηκαν από άλλο χρήστη με πρόσβαση στο κοινόχρηστο κλειδί. Κανένας χρήστης ο οποίος δεν έχει πρόσβαση στο κοινόχρηστο κλειδί δεν μπορεί να δεν τα κρυπτογραφημένα δεδομένα. Συγκριτικά με την κρυπτογραφία ασύμμετρου κλειδιού, η κρυπτογραφία συμμετρικού κλειδιού είναι γρηγορότερη στον υπολογισμό. Εξαιτίας αυτού, όταν κάποιος ισχυρίζεται ότι κρυπτογραφεί κάτι που χρησιμοποιεί κρυπτογραφία ασύμμετρου κλειδιού, συχνά τα δεδομένα κρυπτογραφούνται με κρυπτογραφία συμμετρικού κλειδιού και στη συνέχεια το συμμετρικό κλειδί κρυπτογραφείται χρησιμοποιώντας κρυπτογραφία ασύμμετρου κλειδιού. Αυτό το κόλπο μπορεί να επιταχύνει σημαντικά την κρυπτογράφηση ασύμμετρου κλειδιού. [7]

Περίληψη της χρήσης της κρυπτογραφίας ασύμμετρου κλειδιού σε ένα δίκτυο Blockchain:

- Τα ιδιωτικά κλειδιά χρησιμοποιούνται για την ψηφιακή υπογραφή των συναλλαγών
- Τα δημόσια κλειδιά χρησιμοποιούνται για την παραγωγή διευθύνσεων
- Τα δημόσια κλειδιά χρησιμοποιούνται για την επαλήθευση υπογραφών που χρησιμοποιούνται από ιδιωτικά κλειδιά.
- Η κρυπτογραφία ασύμμετρου κλειδιού παρέχει τη δυνατότητα επαλήθευσης ότι ο χρήστης που μεταφέρει κάποια αξία σε ένα άλλο χρήστη, έχει στην κατοχή του το ιδιωτικό κλειδί που μπορεί να υπογράψει τη συναλλαγή. [7]

1.6 Αποθήκευση ιδιωτικού κλειδιού

Με μερικά δίκτυα Blockchain, οι χρήστες πρέπει να διαχειρίζονται και να αποθηκεύουν με ασφάλεια τα δικά τους ιδιωτικά κλειδιά. Αντί να τα καταγράφουν χειροκίνητα, συχνά χρησιμοποιούν λογισμικό για την ασφαλή αποθήκευσή τους. Αυτό το λογισμικό συχνά αναφέρεται ως πορτοφόλι. Το πορτοφόλι μπορεί να αποθηκεύσει ιδιωτικά κλειδιά, δημόσια κλειδιά και σχετικές διευθύνσεις. Μπορεί επίσης να πραγματοποιεί και άλλες λειτουργίες, όπως τον υπολογισμό της συνολικής αξίας των ψηφιακών δεδομένων που μπορεί να έχει ένας χρήστης. [7]

Αν ένας χρήστης χάσει ένα ιδιωτικό κλειδί, τότε οποιοδήποτε ψηφιακό στοιχείο που σχετίζεται με αυτό το κλειδί θα χαθεί, επειδή είναι υπολογιστικά ανέφικτη η αναγέννηση του ίδιου ιδιωτικού κλειδιού. Αν ένα ιδιωτικό κλειδί κλαπεί, τότε ο εισβολέας θα έχει πρόσβαση σε όλα τα ψηφιακά στοιχεία που ελέγχονται από αυτό το ιδιωτικό κλειδί. Η ασφάλεια των ιδιωτικών κλειδιών είναι τόσο σημαντική, που πολλοί χρήστες χρησιμοποιούν ειδικά ασφαλή υλικά για την αποθήκευσή τους. Εναλλακτικά, οι χρήστες μπορούν να επωφεληθούν από μια αναδυόμενη βιομηχανία υπηρεσιών μεσεγγύησης ιδιωτικού κλειδιού. [7]

1.7 Καθολικά

Ένα καθολικό είναι μια συλλογή από συναλλαγές. Τα παλαιότερα χρόνια, χρησιμοποιούσαν χαρτί και στυλό για την καταγραφή της ανταλλαγής αγαθών και υπηρεσιών, ενώ στην σύγχρονη εποχή τα καθολικά αποθηκεύονται ψηφιακά, συχνά σε μεγάλες βάσεις δεδομένων που ανήκουν και λειτουργούν από ένα κεντρικό αξιόπιστο τρίτο πρόσωπο για λογαριασμό μιας κοινότητας χρηστών. [7]

Υπάρχει αυξημένο ενδιαφέρον για τη διερεύνηση της κατανομής της κυριότητας του καθολικού. Η τεχνολογία Blockchain επιτρέπει μια τέτοια προσέγγιση χρησιμοποιώντας την κατανεμημένη κυριότητα όσο και την κατανεμημένη φυσική αρχιτεκτονική. Το αυξανόμενο ενδιαφέρον για την κατανομή της κυριότητας των καθολικών οφείλεται στην εμπιστοσύνη, την ασφάλεια και την αξιοπιστία που σχετίζονται με καθολικά με κεντρική κυριότητα:

- Τα κεντρικά καθολικά ενδέχεται να χαθούν ή να καταστραφούν. Ένας χρήστης πρέπει να έχει εμπιστοσύνη στον ιδιοκτήτη, ότι θα κάνει σωστή δημιουργία αντιγράφων ασφαλείας του συστήματος.
- Τα κεντρικά καθολικά μπορεί να βρίσκονται σε ένα δίκτυο, όπου όλο το λογισμικό, το υλικό και η υποδομή μπορεί να είναι ίδια. Λόγω αυτού του χαρακτηριστικού, η συνολική ανθεκτικότητα του συστήματος μπορεί να μειωθεί αφού μια επίθεση σε ένα μέρος του δικτύου θα επηρεάσει τα πάντα.
- Τα κεντρικά καθολικά ενδέχεται να βρίσκονται εξ ολοκλήρου σε συγκεκριμένες γεωγραφικές τοποθεσίες (παράδειγμα σε μια χώρα). Αν συμβούν διακοπές δικτύου σε αυτή την περιοχή, το καθολικό και οι υπηρεσίες που εξαρτώνται από αυτό μπορεί να μην είναι διαθέσιμα.
- Οι συναλλαγές δεν γίνονται με διαφάνεια και μπορεί να μην είναι έγκυρες. Ένας χρήστης πρέπει να εμπιστεύεται ότι ο ιδιοκτήτης επικυρώνει κάθε ληφθείσα συναλλαγή.
- Η λίστα συναλλαγών ενδέχεται να μην είναι πλήρης. Ένας χρήστης πρέπει να εμπιστεύεται ότι ο ιδιοκτήτης περιλαμβάνει όλες τις έγκυρες συναλλαγές που έχουν ληφθεί.
- Τα δεδομένα συναλλαγών ενδέχεται να έχουν τροποποιηθεί. Ένας χρήστης πρέπει να εμπιστεύεται ότι ο ιδιοκτήτης δεν αλλάζει τις προηγούμενες συναλλαγές.
- Το κεντρικό σύστημα μπορεί να μην είναι ασφαλές. Ένας χρήστης πρέπει να εμπιστεύεται το συσχετισμένο σύστημα υπολογιστών και τα δίκτυα να λαμβάνουν κρίσιμες ενημερώσεις κώδικα ασφαλείας και να έχουν εφαρμοσμένες βέλτιστες πρακτικές για την ασφάλεια. Το σύστημα μπορεί να έχει παραβιαστεί και να έχουν υποκλαπεί προσωπικές πληροφορίες λόγω της μη αποτελεσματικής ασφάλειας. [7]

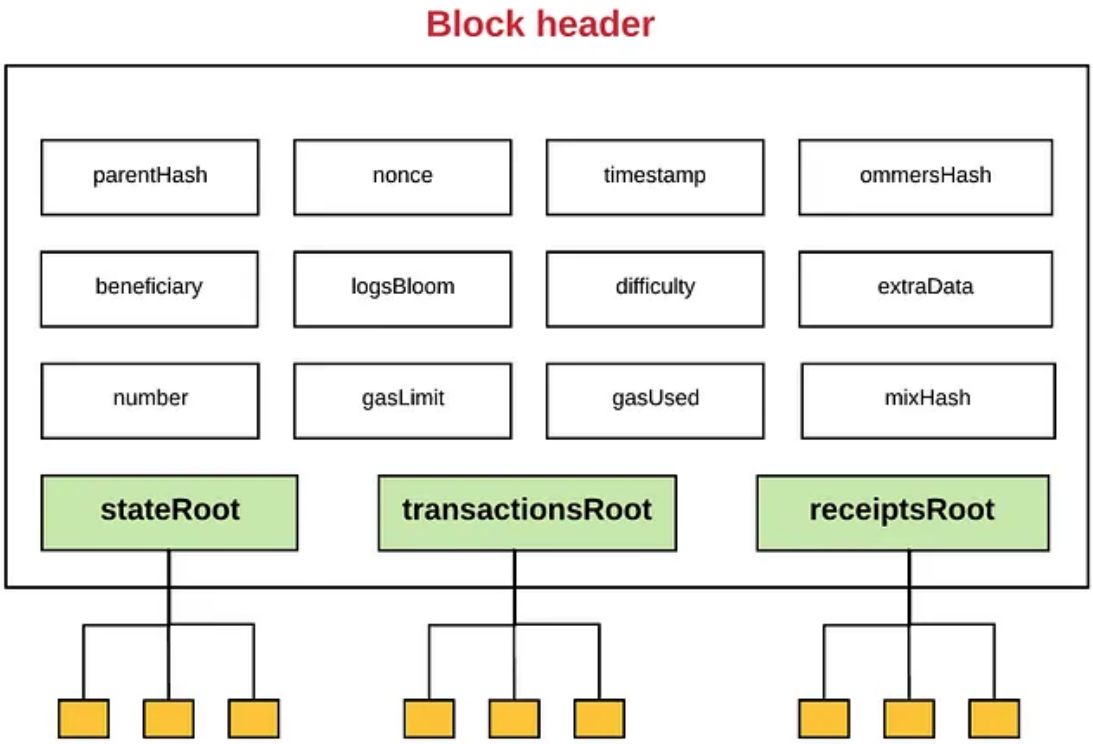
1.8 Blocks

Οι χρήστες ενός Blockchain δικτύου υποβάλλουν υποψήφιες συναλλαγές στο δίκτυο Blockchain μέσω λογισμικού (εφαρμογές υπολογιστή, εφαρμογές smartphone, ψηφιακά πορτοφόλια, υπηρεσίες web και άλλα). Το λογισμικό αποστέλλει αυτές τις συναλλαγές σε έναν ή περισσότερους κόμβους εντός του δικτύου Blockchain. Οι επιλεγμένοι κόμβοι μπορεί να είναι αποθηκευτικοί πλήρεις κόμβοι, καθώς και κόμβοι δημοσίευσης. Οι υποβαλλόμενες συναλλαγές στη συνέχεια διαδίδονται στους άλλους κόμβους του δικτύου, αλλά αυτό καθαυτό δεν τις τοποθετεί στο Blockchain. Για πολλές υλοποιήσεις με βάση το Blockchain, αφού μια συναλλαγή σε εκκρεμότητα έχει διανεμηθεί στους κόμβους, πρέπει να περιμένει σε μια ουρά μέχρι να προστεθεί στο Blockchain από ένα κόμβο δημοσίευσης. [7]

Οι συναλλαγές προστίθενται στο Blockchain όταν ένας κόμβος δημοσιεύει ένα Block, το οποίο περιέχει μια κεφαλίδα και τα δεδομένα του. Η κεφαλίδα του Block περιέχει τα μεταδεδομένα για αυτό το Block. Τα δεδομένα του Block περιέχουν μια λίστα επικυρωμένων και αυθεντικών συναλλαγών οι οποίες έχουν υποβληθεί στο δίκτυο Blockchain. Η εγκυρότητα και η αυθεντικότητα διασφαλίζονται ελέγχοντας ότι η συναλλαγή είναι σωστά μορφοποιημένη και ότι οι πάροχοι των ψηφιακών στοιχείων σε κάθε συναλλαγή (αναφέρονται στις τιμές «εισόδου» της συναλλαγής) έχουν υπογράψει κρυπτογραφικά τη συναλλαγή. Αυτό επιβεβαιώνει ότι οι πάροχοι των ψηφιακών στοιχείων, για μια συναλλαγή, είχαν πρόσβαση στο ιδιωτικό κλειδί που μπορούσε να υπογράψει πάνω από τα διαθέσιμα ψηφιακά στοιχεία. Οι άλλοι πλήρεις κόμβοι θα ελέγξουν την εγκυρότητα και την αυθεντικότητα όλων των συναλλαγών σε ένα δημοσιευμένο μπλοκ και δεν θα αποδεχτούν ένα μπλοκ εάν περιέχει μη έγκυρες συναλλαγές. [7]

Θα πρέπει να σημειωθεί ότι κάθε εφαρμογή Blockchain μπορεί να ορίσει τα δικά της πεδία δεδομένων. Ωστόσο, πολλές υλοποιήσεις Blockchain χρησιμοποιούν πεδία δεδομένων όπως τα παρακάτω:

1.8.1 Κεφαλίδα του Block (Block header)



Εικόνα 1.2: Κεφαλίδα του Block

- Ο αριθμός του Block γνωστός και ως ύψος του Block σε κάποια δίκτυα Blockchain.
- Η τιμή Hash της κεφαλίδας του προηγούμενου Block.
- Μια hash αναπαράσταση των δεδομένων μπλοκ (μπορούν να χρησιμοποιηθούν διαφορετικές μέθοδοι για να γίνει αυτό, όπως η δημιουργία ενός δέντρου Merkle και αποθήκευση του κεντρικού Hash ή χρησιμοποιώντας ένα Hash όλων των συνδυασμένων δεδομένων των Block)
- Μια χρονική σήμανση.
- Το μέγεθος του Block
- Η τιμή Nonce. Για δίκτυα Blockchain που χρησιμοποιούν mining, αυτός είναι ένας αριθμός τον οποίο χειρίζεται ο κόμβος δημοσίευσης για την επίλυση του hash γρίφου. Άλλα δίκτυα Blockchain μπορεί να το περιλαμβάνουν ή να το χρησιμοποιούν για άλλο σκοπό εκτός από την επίλυση ενός hash γρίφου.

1.8.2 Δεδομένα του Block

- Μια λίστα συναλλαγών και συμβάντων καθολικού που περιλαμβάνονται στο Block.
- Μπορεί να υπάρχουν και άλλα δεδομένα. [7]

1.9 Μοντέλα συναίνεσης

Μια βασική πτυχή της τεχνολογίας Blockchain είναι ο καθορισμός του χρήστη που δημοσιεύει το επόμενο μπλοκ. Αυτό επιλύεται μέσω της εφαρμογής ενός από τα πολλά πιθανά μοντέλα συναίνεσης. Για τα δίκτυα Blockchain που λέγονται Permissionless υπάρχουν γενικά πολλοί κόμβοι δημοσίευσης που ανταγωνίζονται ταυτόχρονα για τη δημοσίευση του επόμενου Block. Συνήθως αυτό συμβαίνει για το κέρδος κρυπτονομισμάτων ή έξοδα συναλλαγών. Αυτοί οι χρήστες γενικά δεν εμπιστεύονται ο ένας τον άλλο και ο μόνος τρόπος που μπορεί να γνωρίζονται είναι μόνο από τις δημόσιες διευθύνσεις τους. Κάθε εκδοτικός κόμβος είναι πιθανό να υποκινείται από την επιθυμία για οικονομικό κέρδος και όχι την ευημερία των άλλων κόμβων δημοσίευσης ή ακόμα και το ίδιο το δίκτυο. [7]

Σε μια τέτοια περίπτωση, γιατί ένας χρήστης να διαδώσει ένα μπλοκ που προσπαθεί ένας άλλος χρήστης να δημοσιεύσει; Επίσης ποιος επιλύει διενέξεις όταν πολλοί κόμβοι δημοσιεύουν ένα μπλοκ την ίδια στιγμή; Για να λειτουργήσει αυτό, οι τεχνολογίες Blockchain χρησιμοποιούν μοντέλα συναίνεσης για να ενεργοποιήσουν μια ομάδα χρηστών που έχουν αμοιβαία δυσπιστία να συνεργαστούν. [7]

1.10 Τεχνική συναίνεσης: απόδειξης εργασίας (Proof of work)

Στην τεχνική συναίνεσης γνωστή με το όνομα απόδειξης εργασίας (POW), ένας χρήστης δημοσιεύει το επόμενο μπλοκ όντας ο πρώτος που θα λύσει ένα υπολογιστικά εντατικό γρίφο. Η λύση του γρίφου είναι η απόδειξη ότι έχουν κάνει την εργασία. Ο γρίφος είναι σχεδιασμένος έτσι, που η επίλυσή του είναι πολύ δύσκολη, αλλά ο έλεγχος για τον αν είναι σωστή είναι εύκολος. Αυτό επιτρέπει σε όλους τους άλλους κόμβους να επικυρώνουν εύκολα τυχόν προτεινόμενα επόμενα μπλοκ και οποιαδήποτε προτεινόμενα μπλοκ που δεν ικανοποιούν το παζλ να απορρίπτονται. [7]

Μια κοινή μέθοδος γρίφου είναι να απαιτείται η σύνοψη hash μιας κεφαλίδας να είναι μικρότερη από την τιμή του στόχου. Οι κόμβοι δημοσίευσης κάνουν πολλές μικρές αλλαγές στην κεφαλίδα του μπλοκ τους προσπαθώντας να βρουν ένα hash που να πληροί την απαίτηση. Για κάθε προσπάθεια, ο κόμβος δημοσίευσης πρέπει να υπολογίσει το hash για ολόκληρη την κεφαλίδα του Block. Αυτή είναι μια υπολογιστικά εντατική διαδικασία εφόσον επαναλαμβάνεται πολλές φορές. Η τιμή του στόχου μπορεί να τροποποιηθεί με την πάροδο του χρόνου για την προσαρμογή της δυσκολίας (είτε πάνω είτε κάτω) για την επιρροή της ποσότητας των Block που θα δημοσιεύονται. [7]

Οι προσαρμογές στον στόχο δυσκολίας στοχεύουν στο να διασφαλίσουν ότι καμία οντότητα δεν μπορεί να αναλάβει την παραγωγή Block, αλλά αυτό έχει ως αποτέλεσμα οι υπολογισμοί επίλυσης γρίφων να απαιτούν σημαντική κατανάλωση πόρων. Εξαιτίας της σημαντικής κατανάλωσης πόρων από ορισμένα δίκτυα Blockchain απόδειξης εργασίας, υπάρχει μία κίνηση που προσθέτει κόμβους δημοσίευσης σε περιοχές που υπάρχει πλεόνασμα φθηνής ηλεκτρικής ενέργειας. [7]

Μια σημαντική πτυχή αυτού του μοντέλου είναι ότι η εργασία που τίθεται σε ένα γρίφο δεν επηρεάζει την πιθανότητα κάποιου να λύσει το τρέχον ή κάποιο μελλοντικό γρίφο, επειδή οι γρίφοι είναι ανεξάρτητοι. Αυτό σημαίνει ότι όταν ένας χρήστης λαμβάνει ένα ολοκληρωμένο Block από άλλο χρήστη, δίδεται κίνητρο να απορρίψει την τρέχουσα εργασία του και να αρχίσει να δημιουργεί από το καινούριο Block που μόλις έλαβε γιατί γνωρίζουν ότι οι άλλοι κόμβοι δημοσίευσης θα κατασκευαστούν από αυτό. [7]

1.11 Πλατφόρμα Ethereum

Το Ethereum είναι μια Blockchain-based πλατφόρμα λογισμικού που χρησιμοποιείται κυρίως για την υποστήριξη του δεύτερου μεγαλύτερου κρυπτονομίσματος στον κόσμο με κεφαλαιοποίηση μετά το Bitcoin. Όπως και άλλα κρυπτονομίσματα, το Ethereum μπορεί να χρησιμοποιηθεί για αποστολή και λήψη αντιτίμου παγκοσμίως και χωρίς κάποιο τρίτο μέρος να παρακολουθεί ή να παρεμβαίνει απροσδόκητα. [10]

Η κύρια χρήση του Ethereum Blockchain σήμερα είναι η ανταλλαγή αντιτίμου, συχνά μέσω του τοπικού token του Blockchain, του Ether. Ωστόσο, πολλοί από τους προγραμματιστές εργάζονται στο κρυπτονόμισμα λόγω των μακροπρόθεσμων δυνατοτήτων του και του φιλόδοξου οράματος των προγραμματιστών του να χρησιμοποιήσουν το Ethereum για να δώσουν στους χρήστες περισσότερο έλεγχο των οικονομικών τους και των διαδικτυακών τους δεδομένων. Η φιλόδοξη ιδέα, η οποία μερικές φορές οδηγεί στο να αναφέρεται το Ethereum ως παγκόσμιος υπολογιστής, έχει δεχτεί το μερίδιο των κριτικών που λένε ότι μάλλον δεν θα λειτουργήσει. Αλλά αν το πείραμα κυκλοφορήσει όπως είχε προγραμματιστεί, θα δημιουργήσει εφαρμογές πολύ διαφορετικές από το Facebook και τη Google, στις οποίες οι χρήστες εμπιστεύονται εν γνώση τους ή εν αγνοία τους τα δεδομένα τους. [10]

Οι λάτρεις του Ethereum στοχεύουν να επιτρέψουν τον έλεγχο στους χρήστες με τη βοήθεια ενός Blockchain, μιας τεχνολογίας που αποκεντρώνει τα δεδομένα έτσι ώστε χιλιάδες άνθρωποι σε όλο τον κόσμο να λαμβάνουν ένα αντίγραφο. Οι προγραμματιστές μπορούν να χρησιμοποιήσουν το Ethereum για τη δημιουργία εφαρμογών χωρίς ηγεσία, το οποίο σημαίνει ότι τα δεδομένα ενός χρήστη δεν μπορούν να παραβιαστούν από τους δημιουργούς της υπηρεσίας. [10]

Το Blockchain είναι ένα σύστημα καθολικού που βασίζεται σε ένα peer-to-peer δίκτυο, το οποίο διατηρεί αρχεία συναλλαγών που αντιπροσωπεύουν μεταφορές αντιτίμων μεταξύ λογαριασμών. Στο δίκτυο, όλοι οι κόμβοι λαμβάνουν συναλλαγές, τις συσκευάζουν σε ένα Block που είναι συνδεδεμένο με το προηγούμενο Block και το μεταδίδουν. Σύμφωνα με τον μηχανισμό συναίνεσης, αν οι περισσότεροι κόμβοι λάβουν και αποδεχτούν ένα μπλοκ, τότε το μπλοκ θα είναι μέρος του καθολικού. [11]

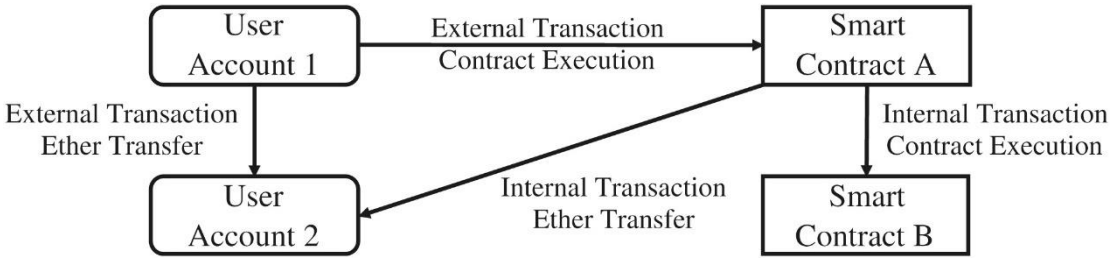
Στο Ethereum, υπάρχουν δύο είδη λογαριασμών: οι λογαριασμοί χρηστών και οι λογαριασμοί έξυπνων συμβολαίων. Οι λογαριασμοί χρηστών αντιπροσωπεύουν συμμετέχοντες, συμπεριλαμβανομένων εκείνων που καλούν λειτουργίες έξυπνων συμβολαίων, των προγραμματιστών (που αναπτύσσουν έξυπνα συμβόλαια στο Ethereum) και των miners (των οποίων οι κόμβοι λειτουργούν για να συνεισφέρουν στο καθολικό). Οι λογαριασμοί έξυπνου συμβολαίου αντιπροσωπεύουν το έξυπνο συμβόλαιο που είναι ένας τύπος προγραμμάτων που αποθηκεύονται και μπορούν να εκτελούνται σε Blockchains, που ονομάζεται επίσης chaincode (κώδικας στην αλυσίδα). Το Ethereum είναι το πρώτο blockchain που παρέχει πλήρη γλώσσα προγραμματισμού Turing για την ανάπτυξη έξυπνων συμβολαίων. [11]

Οι συναλλαγές μπορούν να ταξινομηθούν σε δυο κατηγορίες:

Από τη μία πλευρά, σύμφωνα με τα δεδομένα της συναλλαγής, οι συναλλαγές μπορούν να χωριστούν σε μεταφορές ETH και εκτελέσεις συμβολαίων. Μια μεταφορά ETH αντιπροσωπεύει ότι ένας λογαριασμός χρήστη μεταφέρει κάποιο ETH σε έναν άλλο. Μια εκτέλεση συμβολαίου αντιπροσωπεύει ότι ένας λογαριασμός καλεί μια συνάρτηση ενός έξυπνου συμβολαίου με ορισμένα δεδομένα ως είσοδο και κάποιο ETH ως χρέωση για την εκτέλεση του συμβολαίου. [11]

Από την άλλη πλευρά, σύμφωνα με αυτόν που ξεκινάει την συναλλαγή, οι συναλλαγές μπορούν να χωριστούν σε εξωτερικές συναλλαγές, οι οποίες ξεκινούν από λογαριασμούς χρηστών και εξωτερικές συναλλαγές, οι οποίες ξεκινούν από λογαριασμούς έξυπνων συμβολαίων. [11]

Το παρακάτω σχήμα (Σχήμα 1) δείχνει τη σχέση μεταξύ των δύο ταξινομήσεων. Αν ο στοχευόμενος λογαριασμός μιας συναλλαγής είναι λογαριασμός χρήστη, η συναλλαγή ανήκει στη μεταφορά ETH. Αν ο στοχευόμενος λογαριασμός μιας συναλλαγής είναι λογαριασμός έξυπνου συμβολαίου, η συναλλαγή ανήκει στην εκτέλεση συμβολαίου.



Εικόνα 1.3: Σχέση μεταξύ των δύο ταξινομήσεων συναλλαγών [11]

Οι λογαριασμοί πρέπει να πληρώνουν προμήθεια για όλες τις συναλλαγές. Αυτά τα τέλη ονομάζονται gas στο οικοσύστημα Ethereum. [11]

1.12 Έξυπνα συμβόλαια (Smart Contracts)

Ένα έξυπνο συμβόλαιο είναι ένας εκτελέσιμος κώδικας που εκτελείται στο Blockchain για να διευκολύνει, να εκτελέσει και να επιβάλει τους όρους μιας συμφωνίας. Ο κύριος στόχος ενός έξυπνου συμβολαίου είναι η αυτόματη εκτέλεση των όρων συμφωνίας εφόσον πληρούνται οι καθορισμένοι όροι. Έτσι, τα έξυπνα συμβόλαια υπόσχονται χαμηλές χρεώσεις συναλλαγών σε σύγκριση με τα παραδοσιακά συστήματα που απαιτούν την επιβολή ενός αξιόπιστου τρίτου μέρους και εκτελεί τους όρους μιας συμφωνίας. Η ιδέα των έξυπνων συμβολαίων προήλθε από τον Szabo το 1994. Ωστόσο, η ιδέα δεν είδε το φως μέχρι την εμφάνιση της τεχνολογίας Blockchain. [1]

Πολλοί διαφορετικοί ορισμοί ενός έξυπνου συμβολαίου έχουν συζητηθεί στη βιβλιογραφία. Ο συγγραφέας στο [8], ταξινόμησε όλους τους ορισμούς σε δύο κατηγορίες, τον κώδικα έξυπνου συμβολαίου και το νομικό έξυπνο συμβόλαιο. [1] Κώδικας έξυπνου συμβολαίου σημαίνει κώδικας που αποθηκεύεται, επαληθεύεται και εκτελείται σε μια αλυσίδα μπλοκ. [8] Η δυνατότητα αυτού του έξυπνου συμβολαίου εξαρτάται εξ ολοκλήρου από τη γλώσσα προγραμματισμού που χρησιμοποιείται για να εκφράσει το συμβόλαιο και τα χαρακτηριστικά του Blockchain. [1] Το νομικό έξυπνο συμβόλαιο σημαίνει κώδικας για ολοκλήρωση ή αντικατάσταση των νομικών συμβολαίων. [8] Η ικανότητα αυτού του έξυπνου συμβολαίου δεν εξαρτάται από την τεχνολογία αλλά αντίθετα σε νομικούς, πολιτικούς και επιχειρηματικούς θεσμούς. Το επίκεντρο αυτής της μελέτης θα είναι στον πρώτο ορισμό, αυτόν του κώδικα έξυπνου συμβολαίου. [1]

Ένα έξυπνο συμβόλαιο έχει υπόλοιπο λογαριασμού, ιδιωτικό χώρο αποθήκευσης και εκτελέσιμο κώδικα. Η κατάσταση του συμβολαίου περιλαμβάνει την αποθήκευση και το υπόλοιπο του συμβολαίου. Η κατάσταση αποθηκεύεται στο Blockchain και ενημερώνεται κάθε φορά που γίνεται επίκληση του συμβολαίου. Μόλις το συμβόλαιο αναρτηθεί στο Blockchain δίκτυο, ο κώδικας δεν μπορεί να αλλάξει. Για την εκτέλεση του συμβολαίου, οι χρήστες μπορούν να στείλουν μια συναλλαγή στη διεύθυνση του συμβολαίου. Αυτή η συναλλαγή στη συνέχεια θα εκτελεστεί από κάθε συναινετικό κόμβο (τους miners) στο δίκτυο για να επιτευχθεί συναίνεση σχετικά με το αποτέλεσμά

του. Η κατάσταση του συμβολαίου στη συνέχεια θα ενημερωθεί ανάλογα. Το συμβόλαιο μπορεί, με βάση τη συναλλαγή που λαμβάνει, να διαβάζει/εγγράφει στον ιδιωτικό του χώρο αποθήκευσης, να αποθηκεύει χρήματα στο υπόλοιπο του λογαριασμού του, να κάνει αποστολή/λήψη μηνυμάτων ή χρημάτων από χρήστες ή άλλα συμβόλαια ή ακόμα και να δημιουργεί νέα συμβόλαια. [1]

Υπάρχουν δύο τύποι έξυπνων συμβολαίων, τα ντετερμινιστικά και τα μη ντετερμινιστικά έξυπνα συμβόλαια. Ένα ντετερμινιστικό συμβόλαιο είναι ένα έξυπνο συμβόλαιο που όταν εκτελείται, δεν απαιτεί καμία πληροφορία από ένα εξωτερικό παράγοντα (εκτός του Blockchain). Ένα μη ντετερμινιστικό έξυπνο συμβόλαιο είναι ένα συμβόλαιο που εξαρτάται από πληροφορίες (τα oracles ή ροές δεδομένων) από ένα εξωτερικό παράγοντα. [1] Ένα Oracle στέλνει δεδομένα από τον έξω κόσμο, όπως η ημερήσια θερμοκρασία ή ο αριθμός των ψήφων που έλαβε ένας πολιτικός υποψήφιος, σε ένα Blockchain όπως το Ethereum. Ένα έξυπνο συμβόλαιο στο Blockchain μπορεί στη συνέχεια να χρησιμοποιήσει τα δεδομένα, συνήθως για να αποφασίσει αν θα διανείμει χρήματα και σε ποιον. Ένα oracle βοηθά ένα έξυπνο συμβόλαιο Ethereum να εκτελεί αυτόματα την ακολουθία εργασιών. Τα έξυπνα συμβόλαια είναι εργαλεία που γίνονται δυνατά από Blockchains όπως το Ethereum, τα οποία εκτελούν τους όρους μιας σχέσης μόνο αν πληρούνται οι σωστές προϋποθέσεις. [9]

1.13 Πλατφόρμα για έξυπνα συμβόλαια

Τα έξυπνα συμβόλαια μπορούν να αναπτυχθούν και να αναρτηθούν σε διαφορετικές πλατφόρμες του Blockchain (όπως, Ethereum, Bitcoin και NXT). Οι διάφορες πλατφόρμες προσφέρουν ξεχωριστά χαρακτηριστικά για την ανάπτυξη έξυπνων συμβολαίων. Ορισμένες πλατφόρμες υποστηρίζουν γλώσσες προγραμματισμού υψηλού επιπέδου για την ανάπτυξη έξυπνων συμβολαίων. [1]

- Το Bitcoin είναι μια δημόσια πλατφόρμα Blockchain η οποία μπορεί να χρησιμοποιηθεί για την επεξεργασία κρυπτογραφικών συναλλαγών, αλλά με πολύ περιορισμένη υπολογιστική ικανότητα. Το Bitcoin χρησιμοποιεί μια stack-based γλώσσα προγραμματισμού. Η ικανότητα να δημιουργεί έξυπνα συμβόλαια με πλούσια λογική, χρησιμοποιώντας μια scripting γλώσσα προγραμματισμού, είναι πολύ περιορισμένη. Στο Bitcoin, μια απλή λογική που απαιτεί πολλαπλές υπογραφές για την υπογραφή μιας μεμονωμένης συναλλαγής πριν την επιβεβαίωση της πληρωμής, είναι δυνατή. Ωστόσο, η σύνταξη συμβολαίων με σύνθετη λογική δεν είναι δυνατή λόγω περιορισμών της scripting γλώσσας του Bitcoin. Για παράδειγμα, δεν υποστηρίζει ούτε βρόχους, ούτε όρια ανάληψης. Για την υλοποίηση ενός βρόχου, ο μόνος δυνατός τρόπος είναι η επανάληψη του κώδικα πολλές φορές, κάτι που είναι αναποτελεσματικό. [1]

- Το NXT είναι μια δημόσια πλατφόρμα Blockchain που περιλαμβάνει ενσωματωμένα έξυπνα συμβόλαια ως πρότυπα. Το NXT επιτρέπει την ανάπτυξη έξυπνων συμβολαίων μόνο χρησιμοποιώντας αυτά τα πρότυπα. Δεν επιτρέπει ωστόσο, προσαρμοσμένα έξυπνα συμβόλαια λόγω της έλλειψης πληρότητας Turing της scripting γλώσσας. [1]

- Το Ethereum είναι μια δημόσια πλατφόρμα Blockchain που μπορεί να υποστηρίξει προηγμένα και προσαρμοσμένα έξυπνα συμβόλαια με τη βοήθεια μιας Turing complete γλώσσας προγραμματισμού. Η πλατφόρμα Ethereum μπορεί να υποστηρίξει όρια αναλήψεων, βρόχους, χρηματοοικονομικά συμβόλαια και τυχερά παιχνίδια. Ο κώδικας των έξυπνων συμβολαίων Ethereum είναι γραμμένος σε μια stack-based bytecode γλώσσα και εκτελείται σε ένα Ethereum virtual machine (EVM). Αρκετές γλώσσες υψηλού επιπέδου (όπως Solidity, Serpent και LLL) μπορούν να χρησιμοποιηθούν για τη σύνταξη έξυπνων συμβολαίων Ethereum. Ο κώδικας αυτών των γλωσσών

στη συνέχεια μπορεί να μεταγλωττιστεί σε bytecode EVM για να τρέξει. Το Ethereum είναι αυτή τη στιγμή η πιο κοινή πλατφόρμα για την ανάπτυξη έξυπνων συμβολαίων. [1]

1.14 Εφαρμογές έξυπνων συμβολαίων

Υπάρχουν πολλές πιθανές εφαρμογές που μπορούν να χρησιμοποιηθούν τα έξυπνα συμβόλαια. Κάποιες από αυτές είναι:

- Internet of things και έξυπνο σπίτι: υπάρχουν δισεκατομμύρια κόμβοι που μοιράζονται δεδομένα μεταξύ τους μέσω του διαδικτύου. Μια πιθανή περίπτωση χρήσης των συμβολαίων που είναι βασισμένα σε Blockchain είναι να επιτρέπεται στους κόμβους να μοιράζονται ή να έχουν πρόσβαση σε διαφορετικές ψηφιακές ιδιότητες χωρίς ένα αξιόπιστο τρίτο μέρος. Υπάρχουν διάφορες εταιρείες που ερευνούν αυτή την περίπτωση χρήσης. Για παράδειγμα, η Slock.it είναι μια γερμανική εταιρεία που χρησιμοποιεί έξυπνα συμβόλαια που βασίζονται στο Ethereum για ενοικίαση, πώληση χωρίς τη συμμετοχή αξιόπιστου τρίτου μέρους. [1]

- Διαχείριση δικαιωμάτων μουσικής: μια πιθανή περίπτωση χρήσης είναι η καταγραφή των δικαιωμάτων ιδιοκτησίας της μουσικής στο Blockchain. Ένα έξυπνο συμβόλαιο μπορεί να επιβάλει την πληρωμή για τους κατόχους μουσικής όταν μια μουσική χρησιμοποιείται για εμπορικούς σκοπούς. Διασφαλίζει επίσης ότι η πληρωμή διανέμεται μεταξύ των ιδιοκτητών της μουσικής. [1]

- Ηλεκτρονικό εμπόριο: μια πιθανή περίπτωση χρήσης είναι η διευκόλυνση του εμπορίου μεταξύ μη αξιόπιστων μερών (πχ πωλητής και αγοραστής) χωρίς αξιόπιστο τρίτο μέρος. Αυτό θα είχε ως αποτέλεσμα τη μείωση του κόστους των συναλλαγών. Τα έξυπνα συμβόλαια μπορούν να απελευθερώσουν την πληρωμή στον πωλητή μόνο όταν ο αγοραστής είναι ικανοποιημένος με το προϊόν ή την υπηρεσία που έλαβαν. [1]

Υπάρχουν και άλλες πιθανές εφαρμογές όπως η ηλεκτρονική ψηφοφορία, πληρωμή στεγαστικού δανείου, ασφάλιση αυτοκινήτου, κατανεμημένη αποθήκευση αρχείων, διαχείριση ταυτότητας κ.α. [1]

1.15 Αποκεντρωμένες Εφαρμογές

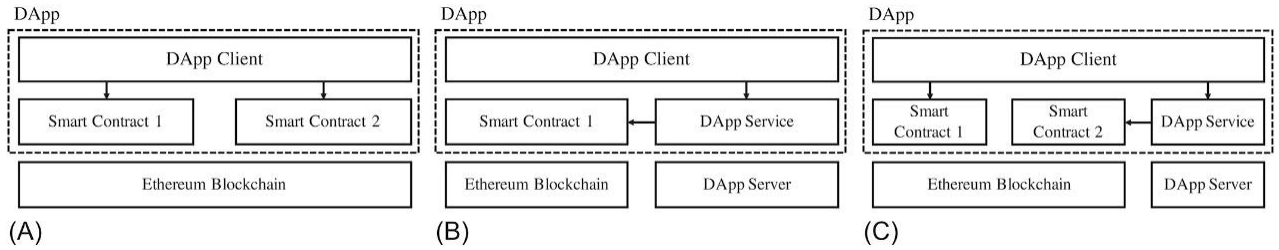
Κοιτώντας σε ένα τυπικό App store παρατηρείται ότι υπάρχουν πολλά πολύχρωμα κουτάκια που αντιπροσωπεύουν τα πάντα, από τραπεζικές εφαρμογές, εφαρμογές γυμναστικής ή ακόμα και εφαρμογές μηνυμάτων. Το μακροπρόθεσμο όραμα της κοινότητας του Ethereum είναι να κάνει εφαρμογές που να μοιάζουν ακριβώς με αυτές, αλλά να λειτουργούν διαφορετικά από πίσω. Εν ολίγοις, ο στόχος είναι οι εφαρμογές Ethereum να επιστρέψουν τον έλεγχο των δεδομένων αυτών των υπηρεσιών, στον κάτοχό τους. [10]

Οι εφαρμογές που έχουν δημιουργηθεί στο Ethereum και προσφέρουν αυτή τη λειτουργία είναι γνωστές ως αποκεντρωμένες εφαρμογές. Οι χρήστες χρειάζονται Ether, το τοπικό token του Ethereum, για να τις χρησιμοποιήσουν. [10]

1.16 Ethereum Dapp

Το Ethereum Blockchain παρέχει δυνατότητες υπολογισμού και αποθήκευσης μέσω του μηχανισμού των έξυπνων συμβολαίων. Επομένως, οι DApps του Ethereum μπορούν να αναπτύξουν έξυπνα συμβόλαια για να χρησιμοποιήσουν τις δυνατότητες που παρέχει το Ethereum για την εφαρμογή επιχειρηματικών λογικών. Θεωρητικά, όλες οι διαδικασίες και τα δεδομένα ενός DApp που βασίζεται σε Blockchain θα πρέπει να αντιμετωπίζονται και να αποθηκεύονται στο Blockchain για καθαρή

αποκέντρωση. Ωστόσο, λόγω της συμφόρησης απόδοσης των υπερσύγχρονων συστημάτων Blockchain, τα τρέχοντα DApps συνήθως εφαρμόζουν μόνο τμήματα της λειτουργικότητάς τους στο Blockchain. Ως αποτέλεσμα, τρία είδη αρχιτεκτονικών υιοθετούνται από το Ethereum DApps στην πράξη, όπως φαίνεται στο Σχήμα 2: άμεσες, έμμεσες και μικτές. Για DApps της άμεσης αρχιτεκτονικής (σχήμα 2A), ο πελάτης αλληλεπιδρά άμεσα με έξυπνα συμβόλαια που αναπτύσσονται στο Ethereum. Τα DApps της έμμεσης αρχιτεκτονικής (Σχήμα 2B) διαθέτουν υπηρεσίες back-end που εκτελούνται σε έναν κεντρικό διακομιστή και ο πελάτης αλληλεπιδρά με έξυπνα συμβόλαια μέσω του διακομιστή. Τα DApps μικτής αρχιτεκτονικής συνδυάζουν τις δύο προηγούμενες αρχιτεκτονικές όπου ο πελάτης αλληλεπιδρά με έξυπνα συμβόλαια τόσο άμεσα όσο και έμμεσα μέσω ενός διακομιστή υποστήριξης. [11]



Εικόνα 1.4: Τρία είδη αρχιτεκτονικών αποκεντρωμένων εφαρμογών (DApp) Α. Άμεσο, Β. Έμμεσο, Γ. Μικτό [11].

Η Solidity είναι η γλώσσα προγραμματισμού για την ανάπτυξη έξυπνων συμβολαίων στην κοινότητα του Ethereum. Είναι μια γλώσσα τύπου JavaScript στην οποία υπάρχουν συμβόλαια (όπως classes), συναρτήσεις (functions) και συμβάντα (events). Ο πηγαίος κώδικας ενός έξυπνου συμβολαίου μεταγλωττίζεται σε bytecode για να αναπτυχθεί στο Ethereum. μετά την ανάπτυξη, το συμβόλαιο θα λάβει μια διεύθυνση. [11]

2 ΚΕΦΑΛΑΙΟ 2ο : Διαδίκτυο των πραγμάτων

Ο κύριος στόχος του IoT είναι να δημιουργήσει ένα περιβάλλον όπου συσκευές και αισθητήρες μπορούν να συνδεθούν στο διαδίκτυο και να επικοινωνούν μεταξύ τους και με τον χρήστη, προσφέροντας έτσι αυτοματοποίηση, άνεση και αποδοτικότητα σε διάφορους τομείς της καθημερινότητας. Άλλος στόχος είναι η συλλογή και η ανάλυση δεδομένων από αισθητήρες και συσκευές για τη λήψη αποφάσεων βασισμένες σε δεδομένα (data-driven decisions) και τη βελτιστοποίηση διαδικασιών.

2.1 Αρχές

Συνδεσιμότητα: Η βασική αρχή του IoT είναι η δυνατότητα σύνδεσης και επικοινωνίας μεταξύ συσκευών και αισθητήρων μέσω του δικτύου, είτε αυτό είναι το διαδίκτυο είτε ένα εσωτερικό δίκτυο.

Αυτοματοποίηση: Η αυτοματοποίηση είναι σημαντική αρχή του IoT, καθώς επιτρέπει στις συσκευές και τους αισθητήρες να λειτουργούν αυτόνομα και να λαμβάνουν αποφάσεις χωρίς την ανθρώπινη παρέμβαση

Διαφάνεια: Η διαφάνεια είναι σημαντική για το IoT, καθώς οι χρήστες πρέπει να γνωρίζουν τι δεδομένα συλλέγονται από τις συσκευές και πώς αυτά χρησιμοποιούνται.

Ασφάλεια: Λόγω της συνδεσιμότητας, η ασφάλεια είναι ένα κρίσιμο στοιχείο του IoT. Οι συσκευές πρέπει να προστατεύονται από εξωτερικές επιθέσεις και οι χρήστες πρέπει να είναι ενήμεροι για τυχόν κινδύνους.

2.2 Ενσωμάτωση του ΔτΠ με το Blockchain

Το Διαδίκτυο των Πραγμάτων (ΔτΠ) μετασχηματίζει και βελτιστοποιεί τις μη αυτόματες διαδικασίες για να τις κάνει μέρος της ψηφιακής εποχής, λαμβάνοντας όγκους δεδομένων που παρέχουν γνώση πρωτόγνωρου επιπέδου. Αυτή η γνώση διευκολύνει την ανάπτυξη έξυπνων εφαρμογών όπως βελτίωση της διαχείρισης και της ποιότητας ζωής των πολιτών μέσω της ψηφιοποίησης των υπηρεσιών στις πόλεις. Τα τελευταία χρόνια, οι υπολογιστικές τεχνολογίες του νέφους (Cloud) έχουν συμβάλει στο να παρέχουν στο ΔτΠ την απαραίτητη λειτουργικότητα για την ανάλυση και την επεξεργασία πληροφοριών και τις μετατρέπουν σε ενέργειες και γνώση σε πραγματικό χρόνο. Αυτή η πρωτοφανής ανάπτυξη του ΔτΠ έχει ανοίξει νέες δυνατότητες στην κοινωνία όπως σε μηχανισμούς πρόσβασης και κοινοποίησης πληροφοριών. Οι κεντρικές αρχιτεκτονικές όπως αυτή που χρησιμοποιείται στο Cloud έχει συμβάλει σημαντικά στην ανάπτυξη του ΔτΠ. Ωστόσο, όσον αφορά τη διαφάνεια των δεδομένων, οι χρήστες δεν έχουν ξεκάθαρη εικόνα για το που και πως θα χρησιμοποιηθούν οι πληροφορίες που παρέχουν. [12]

Η ενσωμάτωση τεχνολογιών όπως το ΔτΠ και το Cloud έχει αποδειχθεί ότι είναι ανεκτίμητη. Ομοίως, πρέπει να αναγνωριστούν οι τεράστιες δυνατότητες του Blockchain που μπορεί να φέρει στο ΔτΠ. Το Blockchain μπορεί να εμπλουτίσει το ΔτΠ παρέχοντας μια αξιόπιστη υπηρεσία κοινής χρήσης, όπου οι πληροφορίες είναι αξιόπιστες και μπορούν να εντοπιστούν. Οι πηγές δεδομένων μπορούν να εντοπιστούν ανά πάσα στιγμή και τα δεδομένα να παραμείνουν αμετάβλητα με την πάροδο του χρόνου, αυξάνοντας την ασφάλειά τους. Ένα βασικό βήμα είναι οι πληροφορίες του ΔτΠ να μπορούν να κοινοποιούνται με ασφάλεια μεταξύ πολλών συμμετεχόντων. Για παράδειγμα, το να γνωρίζουμε που βρίσκονται πολλαπλά προϊόντα διατροφής, ανά πάσα στιγμή, είναι ένας σημαντικός παράγοντας για να διασφαλιστεί η ασφάλεια των τροφίμων. Αυτή η διαδικασία θα μπορούσε να απαιτήσει τη συμμετοχή πολλών μερών, όπως κατασκευαστών, σίτισης, διανομής κ.α.. Μια διαρροή δεδομένων σε οποιοδήποτε μέρος της αλυσίδας θα μπορούσε να θεωρηθεί απάτη και να επιβραδύνει την

διαδικασία αναζήτησης της μόλυνσης, που μπορεί να επηρεάσει σημαντικά τις ζωές των πολιτών και να επιφέρει τεράστιες οικονομικές καταστροφές σε εταιρείες, ακόμα και χώρες. Ένας καλύτερος έλεγχος σε αυτούς τους τομείς θα αύξανε την ασφάλεια των τροφίμων, θα βελτίωνε την ανταλλαγή δεδομένων μεταξύ των μερών που συμμετέχουν και θα μείωνε το χρόνο αναζήτησης σε περίπτωση κάποιας μόλυνσης των προϊόντων, που μπορεί να σώσει ζωές. Επιπλέον, σε άλλους τομείς όπως οι έξυπνες πόλεις και τα έξυπνα αυτοκίνητα, η κοινή χρήση αξιόπιστων δεδομένων θα μπορούσε να βοηθήσει τη συμπερίληψη νέων συμμετεχόντων στα οικοσυστήματα και να συμβάλλουν στη βελτίωση των υπηρεσιών τους. Επομένως, η χρήση του Blockchain βοηθά στην συμπλήρωση του ΔτΠ με αξιόπιστες πληροφορίες. Η τεχνολογία του Blockchain αναγνωρίζεται ως το κλειδί για την επίλυση της επεκτασιμότητας, της ιδιωτικότητας και των προβλημάτων που σχετίζονται με το ΔτΠ. [12] Στο επόμενο κεφάλαιο θα γίνει αναφορά σε παραδείγματα και λύσεις που συνδυάζουν το Blockchain με το ΔτΠ.

Από την δική μας οπτική το ΔτΠ μπορεί να επωφεληθεί από τη λειτουργικότητα του Blockchain και να βοηθήσει περαιτέρω σε αναπτυσσόμενες τεχνολογίες του ΔτΠ. Πιο συγκεκριμένα οι βελτιώσεις που μπορεί να φέρει αυτή η ενοποίηση μπορεί να είναι:

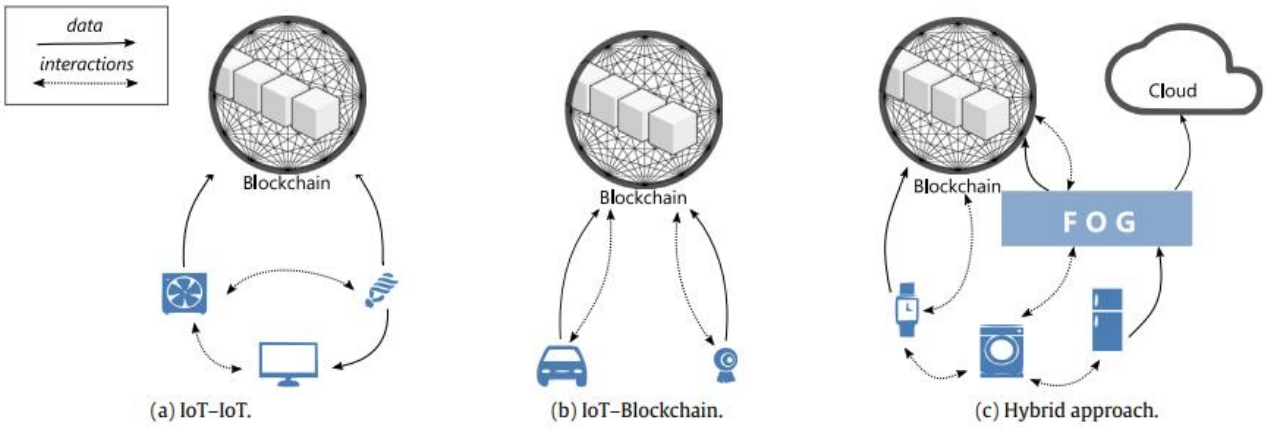
- Αποκέντρωση και επεκτασιμότητα: η μετάβαση από μια κεντρική αρχιτεκτονική P2P θα αφαιρέσει κεντρικά σημεία αστοχιών και σημείων συμφόρησης. Θα βοηθήσει επίσης την αποτροπή σεναρίων που ελέγχουν την επεξεργασία και αποθήκευση πληροφοριών πολλών ανθρώπων από μερικές ισχυρές εταιρίες. Άλλα οφέλη που προκύπτουν από την αποκέντρωση της αρχιτεκτονικής είναι η βελτίωση της ανοχής των σφαλμάτων και η επεκτασιμότητα του συστήματος.
- Ταυτότητα: χρησιμοποιώντας ένα κοινό σύστημα Blockchain οι συμμετέχοντες είναι σε θέση να αναγνωρίσουν όλες τις συσκευές. Τα δεδομένα που παρέχονται και τροφοδοτούνται στο σύστημα είναι αμετάβλητα και προσδιορίζει τα πραγματικά δεδομένα που παρέχονται από μία συσκευή. Επιπρόσθετα, το Blockchain μπορεί να παρέχει αξιόπιστη κατανεμημένη αυθεντικοποίηση και εξουσιοδότηση των συσκευών για εφαρμογές του ΔτΠ. Αυτό θα αντιπροσώπευε μια βελτίωση στον τομέα του ΔτΠ και των συμμετεχόντων του.
- Αυτονομία: η τεχνολογία του Blockchain ενδυναμώνει τις δυνατότητες των εφαρμογών της νέας γενιάς, καθιστώντας δυνατή την ανάπτυξη αυτόνομων έξυπνων πόρων και εξοπλισμού ως υπηρεσία. Με το Blockchain, οι συσκευές είναι σε θέση να αλληλοεπιδρούν μεταξύ τους χωρίς τη χρήση κάποιου διακομιστή. Οι εφαρμογές του ΔτΠ θα μπορούσαν να επωφεληθούν από αυτή τη λειτουργικότητα για να παρέχουν συμβατότητα μεταξύ των συσκευών και των εφαρμογών.
- Αξιοπιστία: οι πληροφορίες του ΔτΠ μπορούν να παραμείνουν αμετάβλητες και να διανεμηθούν με την πάροδο του χρόνου στο Blockchain. Οι συμμετέχοντες του συστήματος είναι σε θέση να επαληθεύσουν την αυθεντικότητα των δεδομένων και να είναι βέβαιο ότι δεν έχουν παραβιαστεί. Επιπλέον, αυτή η τεχνολογία επιτρέπει την ιχνηλασιμότητα και τον απολογισμό των δεδομένων των αισθητήρων. Η αξιοπιστία είναι η βασική πτυχή που φέρνει το Blockchain στο ΔτΠ.
- Ασφάλεια: οι πληροφορίες και οι επικοινωνίες μπορούν να διασφαλιστούν εάν αποθηκεύονται ως συναλλαγές του Blockchain. [27] Το Blockchain μπορεί να αντιμετωπίζει τις ανταλλαγές μηνυμάτων των συσκευών ως συναλλαγές, επικυρωμένες από έξυπνα συμβόλαια, διασφαλίζοντας έτσι την επικοινωνία μεταξύ συσκευών. Τα τρέχοντα ασφαλή πρότυπα πρωτόκολλα που χρησιμοποιούνται στο ΔτΠ μπορούν να βελτιστοποιηθούν με την εφαρμογή του Blockchain. [26]
- Αγορά υπηρεσιών: το Blockchain μπορεί να επιταχύνει τη δημιουργία ενός οικοσυστήματος υπηρεσιών και δεδομένων του ΔτΠ, όπου οι συναλλαγές μεταξύ των peers θα γίνεται χωρίς τη χρήση κάποιου φορέα. Οι μικροϋπηρεσίες μπορούν εύκολα να αναπτυχθούν και οι μικροπληρωμές μπορούν

να γίνονται με ασφάλεια σε περιβάλλον χωρίς εμπιστοσύνη. Αυτό θα βελτιώσει τη διασύνδεση του ΔτΠ και την πρόσβαση σε δεδομένα του στο Blockchain.

- Ασφαλής ανάπτυξη κώδικα: αξιοποιώντας τον ασφαλή και αμετάβλητο αποθηκευτικό χώρο του Blockchain, ο κώδικας μπορεί να είναι ασφαλής και να τοποθετείται σε συσκευές. Οι κατασκευαστές μπορούν να παρακολουθούν τις ενημερώσεις και την κατάσταση των συσκευών.

Μια άλλη πτυχή που πρέπει να ληφθεί υπόψη σχετίζεται με τις αλληλεπιδράσεις στο ΔτΠ. Κατά την ενσωμάτωση του Blockchain, πρέπει να αποφασιστεί που θα πραγματοποιηθούν αυτές οι αλληλεπιδράσεις: μέσα στο ΔτΠ, σε ένα υβριδικό σχεδιασμό που θα περιλαμβάνει ΔτΠ και Blockchain ή μόνο μέσω Blockchain. Το fog computing έχει επίσης φέρει επανάσταση στο ΔτΠ με την συμπερίληψη ενός νέου επιπέδου μεταξύ του cloud computing και των συσκευών του ΔτΠ και θα διευκόλυνε αυτή την ενσωμάτωση. Παρακάτω περιγράφονται αυτές οι εναλλακτικές λύσεις με τα πλεονεκτήματα και τα μειονεκτήματά τους:

- ΔτΠ - ΔτΠ: αυτή η προσέγγιση θα μπορούσε να είναι η ταχύτερη από άποψη καθυστέρησης και ασφάλειας, εφόσον μπορεί να λειτουργήσει εκτός σύνδεσης. Οι συσκευές του ΔτΠ πρέπει να μπορούν να επικοινωνούν μεταξύ τους, κάτι το οποίο σημαίνει ότι χρειάζονται μηχανισμοί επικοινωνίας μεταξύ τους. Μόνο ένα μέρος των δεδομένων του ΔτΠ αποθηκεύεται στο Blockchain ενώ οι αλληλεπιδράσεις του ΔτΠ γίνονται χωρίς τη χρήση του Blockchain. Αυτό θα ήταν χρήσιμο σε σενάρια με αξιόπιστα δεδομένα του ΔτΠ όπου οι αλληλεπιδράσεις γίνονται με πολύ μικρή καθυστέρηση.
- ΔτΠ - Blockchain: σε αυτή την περίπτωση, όλες οι αλληλεπιδράσεις γίνονται μέσω Blockchain, επιτρέποντας έτσι ένα αμετάβλητο αρχείο αλληλεπιδράσεων. Αυτό διασφαλίζει ότι όλες οι επιλεγμένες αλληλεπιδράσεις είναι ανιχνεύσιμες καθώς οι πληροφορίες τους μπορούν να αναζητηθούν στο Blockchain και επιπλέον αυξάνει την αυτονομία των συσκευών του ΔτΠ. Εφαρμογές του ΔτΠ που πωλούν ή ενοικιάζουν, μπορούν να αξιοποιήσουν αυτήν την προσέγγιση για να παρέχουν τις υπηρεσίες τους. Ωστόσο, η καταγραφή όλων των αλληλεπιδράσεων στο Blockchain θα είχε σαν αποτέλεσμα την αύξηση του εύρους ζώνης και των δεδομένων, κάτι που είναι μια από τις γνωστές προκλήσεις στο Blockchain. Από την άλλη πλευρά, όλα τα δεδομένα του ΔτΠ που σχετίζονται με αυτές τις συναλλαγές θα πρέπει επίσης να αποθηκεύονται στο Blockchain.
- Υβριδικός σχεδιασμός: στη συγκεκριμένη προσέγγιση οι αλληλεπιδράσεις και τα δεδομένα παίρνουν μέρος στο Blockchain και τα υπόλοιπα μοιράζονται απευθείας μεταξύ των συσκευών του ΔτΠ. Μια από τις προκλήσεις είναι η επιλογή των αλληλεπιδράσεων που θα πρέπει να περνούν μέσω του Blockchain και η παροχή του τρόπου για την απόφαση αυτή σε χρόνο εκτέλεσης. Η καλύτερη λύση σε αυτήν την προσέγγιση θα ήταν να ενσωματωθούν και οι δύο τεχνολογίες, καθώς αξιοποιεί τα οφέλη του Blockchain και τα οφέλη από τις αλληλεπιδράσεις του ΔτΠ σε πραγματικό χρόνο. Παράλληλα, σε αυτήν την περίπτωση θα μπορούσε να συμμετέχει το fog computing, ακόμα και το cloud computing, για να συμπληρώσει τους περιορισμούς του Blockchain και του ΔτΠ. Για παράδειγμα, το fog computing περιλαμβάνει λιγότερες υπολογιστικά περιορισμένες συσκευές, όπως πύλες και είναι πιθανό μέρος που μπορεί να γίνει mining με τον ίδιο τρόπο όπως σε άλλες περιπτώσεις που χρησιμοποιούν συσκευές του ΔτΠ. [12]



Εικόνα 2.1: Αλληλεπιδράσεις Blockchain-IoT [12]

Σε μία τυπική ανάπτυξη του ΔτΠ, χρησιμοποιούνται συσκευές περιορισμένων πόρων ως τερματικοί κόμβοι (nodes) που επικοινωνούν με μια πύλη που είναι υπεύθυνη για προώθηση των δεδομένων των αισθητήρων σε ανώτερα επίπεδα (cloud ή server). Κατά την ενσωμάτωση του Blockchain, αν οι τερματικοί κόμβοι πρέπει να αλληλοεπιδρούν με το Blockchain, θα μπορούσε να παρέχεται κρυπτογραφική λειτουργία για τις συσκευές του ΔτΠ. Αυτό είναι το κλειδί για την επίτευξη της αυτονομίας του ΔτΠ, η οποία χρησιμοποιεί πιο εξελιγμένο υλικό (hardware) και υψηλότερο υπολογιστικό κόστος. Η ενσωμάτωση των πυλών σε αυτές τις λύσεις είναι επίσης πιθανό, με τον ίδιο τρόπο που γίνεται κα στις υπόλοιπες αναπτύξεις, ωστόσο τα οφέλη της χρήσης του Blockchain σε αυτήν την περίπτωση είναι λιγότερα. Παρά την επέκταση του Blockchain δεν θα είχε νόημα η χρήση του σε πολλές εφαρμογές, όπου οι βάσεις δεδομένων παρέχουν αρκετή λειτουργικότητα. Η απόφαση για το πότε αξίζει η χρήση του Blockchain κυρίως εξαρτάται από τις απαιτήσεις της εφαρμογής. Για παράδειγμα, όταν απαιτείται υψηλή απόδοση, το Blockchain από μόνο του μπορεί να μην είναι σωστή λύση, αλλά θα μπορούσε να εφαρμοστεί μια υβριδική προσέγγιση για την βελτιστοποίησή του. [12]

Έχουν αρχίσει να εμφανίζονται συμμαχίες εταιριών, για να γεφυρώσουν το χάσμα μεταξύ του ΔτΠ και του Blockchain. Επίσης, υπάρχει αυξανόμενος αριθμός συσκευών με ενσωματωμένες δυνατότητες Blockchain που είναι διαθέσιμες στην αγορά. Το EthEmbedded επιτρέπει την εγκατάσταση πλήρων κόμβων Ethereum σε ενσωματωμένες συσκευές όπως το Rasberry Pi, το Beagleberry Pi το Beaglebone Black και το Odroid. Οι πλήρεις κόμβοι πρέπει να αποθηκεύουν ολόκληρο το Blockchain για πλήρη επικύρωση συναλλαγών και μπλοκ και έτσι η ανάπτυξή τους γίνεται πολύ περιορισμένη σε συσκευές ΔτΠ. [12]

Μια άλλη εναλλακτική στην ενσωμάτωση του Blockchain με το ΔτΠ είναι η ενοποίηση μεταξύ του ΔτΠ και του cloud computing. [28] Αυτή η ενσωμάτωση έχει χρησιμοποιηθεί τα τελευταία χρόνια για να ξεπεραστούν οι περιορισμοί του ΔτΠ: η επεξεργασία, η αποθήκευση και η πρόσβαση. Ωστόσο, το cloud computing παρέχει συνήθως μια κεντρική αρχιτεκτονική, η οποία σε αντίθεση με το Blockchain, περιπλέκει την αξιόπιστη κοινή χρήση με πολλούς συμμετέχοντες. Η ενοποίηση μεταξύ του Blockchain και του ΔτΠ προορίζεται για την αντιμετώπιση προηγούμενων περιορισμών εκτός από τη διατήρηση αξιόπιστων στοιχείων. Το fog computing έχει σαν στόχο να διανείμει και να φέρει το computing (λειτουργικότητα?) πιο κοντά στις τελικές συσκευές, ακολουθώντας μια κατανεμημένη προσέγγιση όπως είναι το Blockchain. Αυτό μπορεί να ενσωματώσει πιο ισχυρές συσκευές από το ΔτΠ όπως πύλες και edge nodes, οι οποίοι στη συνέχεια μπορούν να επαναχρησιμοποιηθούν ως στοιχεία του Blockchain. Επομένως, το fog computing θα μπορούσε να διευκολύνει την ενσωμάτωση του ΔτΠ με το Blockchain. [12]

2.3 Δυσκολίες στην ενσωμάτωση ΔτΠ – Blockchain

Η ενσωμάτωση της τεχνολογίας του Blockchain με το ΔτΠ δεν είναι κάτι ασήμαντο. Το Blockchain σχεδιάστηκε για ένα σενάριο διαδικτύου με ισχυρούς υπολογιστές και αυτό απέχει πολύ από την πραγματικότητα του ΔτΠ. Οι συναλλαγές στο Blockchain είναι ψηφιακά υπογεγραμμένες και επομένως οι συσκευές που μπορούν να λειτουργούν με κάποιο νόμισμα πρέπει να έχουν αυτή τη λειτουργία. [12].

2.4 Αποθήκευση και επεκτασιμότητα

Η χωρητικότητα και η επεκτασιμότητα του Blockchain εξακολουθούν να είναι θέμα υπό συζήτηση, αλλά στο πλαίσιο των εφαρμογών του ΔτΠ οι εγγενείς περιορισμοί της χωρητικότητας και της επεκτασιμότητας καθιστούν αυτές τις προκλήσεις ακόμα μεγαλύτερες. Υπό αυτήν την έννοια το Blockchain μπορεί να φαίνεται ακατάλληλο για εφαρμογές του ΔτΠ, ωστόσο, υπάρχουν τρόποι με τους οποίους αυτοί οι περιορισμοί θα μπορούσαν να ελαττωθούν ή να αποφευχθούν τελείως. Στο ΔτΠ οι συσκευές μπορούν να παράγουν gigabyte (GBs) δεδομένων σε πραγματικό χρόνο και αυτός ο περιορισμός αντιπροσωπεύει ένα μεγάλο εμπόδιο για την ενσωμάτωσή του με το Blockchain. Είναι γνωστό ότι ορισμένες τρέχουσες εφαρμογές του Blockchain μπορούν να επεξεργαστούν μόνο μερικές συναλλαγές ανά δευτερόλεπτο και αυτό θα μπορούσε να είναι μια πιθανή συμφόρηση για το ΔτΠ. Επιπλέον το Blockchain δεν είναι σχεδιασμένο για να αποθηκεύει μεγάλες ποσότητες δεδομένων όπως αυτές που παράγονται στο ΔτΠ. Μια ενοποίηση αυτών των τεχνολογιών θα πρέπει να μπορεί να αντιμετωπίσει αυτές τις προκλήσεις. [12]

2.5 Ασφάλεια

Οι εφαρμογές του ΔτΠ θα πρέπει να αντιμετωπίσουν τα προβλήματα ασφάλειας σε διάφορα επίπεδα, αλλά με μία πρόσθετη πολυπλοκότητα λόγω έλλειψης απόδοσης και την υψηλής ετερογένειας των συσκευών. Επιπλέον, το ΔτΠ περιλαμβάνει ένα σύνολο ιδιοτήτων που επηρεάζουν την ασφάλεια, όπως πχ η κινητικότητα, η ασύρματη επικοινωνία και η επεκτασιμότητα. [12]

Ο αυξανόμενος αριθμός επιθέσεων σε δίκτυα ΔτΠ και οι σοβαρές τους επιπτώσεις, καθιστούν ακόμα πιο απαραίτητη τη δημιουργία ενός ΔτΠ με πιο εξελιγμένη ασφάλεια. Πολλοί ειδικοί βλέπουν το Blockchain ως την τεχνολογία κλειδί για την παροχή των απαραίτητων βελτιώσεων ασφαλείας του ΔτΠ. Ωστόσο, μία από τις κύριες προκλήσεις στην ενσωμάτωση του ΔτΠ με το Blockchain είναι η αξιοπιστία των δεδομένων που παράγονται από το ΔτΠ. Το Blockchain μπορεί να διασφαλίσει ότι τα δεδομένα στην αλυσίδα είναι αμετάβλητα και μπορεί να αναγνωρίσει τους μηχανισμούς τους, ωστόσο όταν φτάσουν τα δεδομένα ήδη διεφθαρμένα στο Blockchain, παραμένουν και διεφθαρμένα. Τα διεφθαρμένα δεδομένα μπορεί να προκύψουν από πολλές καταστάσεις χωρίς να είναι απαραίτητα κακόβουλες. Η καλή λειτουργία της αρχιτεκτονικής του ΔτΠ επηρεάζεται από πολλούς παράγοντες όπως το περιβάλλον, οι συμμετέχοντες, οι βανδαλισμοί και οι βλάβες των συσκευών. Μερικές φορές οι ίδιες οι συσκευές και οι αισθητήρες και οι εκκινητές τους αποτυγχάνουν να λειτουργήσουν σωστά από την αρχή. Αυτή η κατάσταση δεν μπορεί να εντοπιστεί μέχρι να ελεγχθεί η εν λόγω συσκευή, ή μερικές φορές λειτουργεί σωστά για λίγο και αλλάζει συμπεριφορά για κάποιο λόγο (Βραχυκύκλωμα, αποσύνδεση, κτλ). Εκτός από αυτές τις καταστάσεις, υπάρχουν πολλές απειλές που μπορούν να επηρεάσουν το ΔτΠ, όπως η υποκλοπή, η άρνηση υπηρεσίας ή ελέγχου.[29] Για το λόγο αυτό, οι συσκευές ΔτΠ θα πρέπει να ελεγχθούν διεξοδικά πριν την ενσωμάτωσή τους με το Blockchain και θα πρέπει να βρίσκονται και να περιφράσσονται στο σωστό μέρος για την αποφυγή βλαβών αλλά και τη συμπερίληψη τεχνικών ανίχνευσης των βλαβών της συσκευής αμέσως μόλις συμβούν.

Αυτές οι συσκευές είναι πιο πιθανό να παραβιαστούν, καθώς οι περιορισμοί τους περιορίζουν τις ενημερώσεις υλικολογισμικού, εμποδίζοντας την ενεργοποίησή τους λόγω πιθανών σφαλμάτων ή παραβιάσεων ασφαλείας. Επιπλέον, μερικές φορές είναι δύσκολο να ενημερωθούν οι συσκευές μία προς μία, όπως στις παγκόσμιες ΔτΠ αναπτύξεις. Επομένως, πρέπει να τοποθετηθούν μηχανισμοί αναβάθμισης και επαναδιαμόρφωσης στο ΔτΠ για να συνεχίσει να λειτουργεί για πολύ καιρό.

Η ενοποίηση του ΔτΠ με το Blockchain μπορεί να έχει επιπτώσεις σχετικά με τις επικοινωνίες του ΔτΠ. Αυτή τη στιγμή, τα πρωτόκολλα εφαρμογών του ΔτΠ όπως τα CoAP και MQTT χρησιμοποιούν άλλα πρωτόκολλα ασφαλείας όπως TLS ή DTLS για την παροχή ασφαλών επικοινωνιών.[26] Αυτά τα ασφαλή πρωτόκολλα είναι πολύπλοκα και βαριά εκτός από το ότι απαιτούν κεντρική διαχείριση και διακυβέρνηση βασικών υποδομών. Στο δίκτυο Blockchain κάθε συσκευή ΔτΠ θα έχει το δικό της GUID (Global Unique identifier) και ένα ζεύγος ασύμμετρου κλειδιού θα εγκαθίσταται μόλις συνδεθεί στο δίκτυο. Αυτό θα απλοποιούσε τα τρέχοντα πρωτόκολλα ασφαλείας που συνήθως πρέπει να ανταλλάσσουν PKI πιστοποιητικά και θα επέτρεπε τη χρήση τους σε συσκευές με λιγότερες δυνατότητες.

2.6 Έξυπνα συμβόλαια (Smart Contracts)

Τα έξυπνα συμβόλαια έχουν αναγνωριστεί ως η καλύτερη εφαρμογή της τεχνολογίας του Blockchain, αλλά όπως αναφέρθηκε υπάρχουν αρκετές προκλήσεις που πρέπει να αντιμετωπιστούν ακόμη. Το ΔτΠ θα μπορούσε να ωφεληθεί από τη χρήση των έξυπνων συμβολαίων, ωστόσο ο τρόπος με τον οποίο μπορούν να ταιριάξουν σε εφαρμογές ΔτΠ ποικίλει.

Από πρακτική άποψη, ένα συμβόλαιο είναι μια συλλογή κώδικα (συναρτήσεις) και δεδομένα (καταστάσεις) που βρίσκονται σε μια συγκεκριμένη διεύθυνση Blockchain. Οι δημόσιες λειτουργίες σε ένα συμβόλαιο, μπορούν να καλούνται από συσκευές. Οι λειτουργίες μπορούν επίσης να ενεργοποιούν συμβάντα, οι εφαρμογές να τις ακούσουν προκειμένου να αντιδράσει σωστά το γεγονός που πυροδοτήθηκε. Για να αλλάξει η κατάσταση ένός συμβολαίου, δηλαδή για να τροποποιηθεί το Blockchain, πρέπει η συναλλαγή να δημοσιευτεί στο δίκτυο. Οι συναλλαγές υπογράφονται από τους αποστολείς και πρέπει να γίνουν αποδεκτές από το δίκτυο.

Το ΔτΠ έχει την ικανότητα να ανιχνεύει και να ενεργοποιεί μέσω του διαδικτύου σε πολλές εφαρμογές.[28] Στο παράδειγμα της ιχνηλασιμότητας, η συσκευασία των τροφίμων θα είναι εξοπλισμένη με αισθητήρες με δυνατότητα μέτρησης των περιβαλλοντικών συνθηκών και να συνδέεται στο Blockchain (με υπογεγραμμένες συναλλαγές). Στο Blockchain ένα συμβόλαιο θα παρείχε λειτουργίες για να την έναρξη της αποστολής, την ολοκλήρωση της αποστολής και να καταγράφει και να αναζητά τις μετρήσεις. Όταν οι μετρήσεις υπερβαίνουν ένα προκαθορισμένο όριο, ένα συμβάν θα εκτελούταν. Οι εφαρμογές διαχείρισης θα μπορούσαν να ακούν αυτά τα συμβάντα και να ειδοποιούν τους κατασκευαστές, τις εταιρίες μεταφορών και τους πελάτες. Εάν δεν υπάρξουν συμβάντα, τότε το Blockchain θα μπορεί να εγγυηθεί ότι η αποστολή πραγματοποιήθηκε σε βέλτιστες συνθήκες. Τα έξυπνα συμβόλαια θα παρείχαν μια ασφαλή και αξιόπιστη μηχανή επεξεργασίας για το ΔτΠ, κάνοντας καταγραφή και διαχείριση όλων των αλληλεπιδράσεών τους. Οι ενέργειες θα ήταν το αποτέλεσμα μιας αξιόπιστης και ασφαλούς επεξεργασίας. Επομένως, τα έξυπνα συμβόλαια μπορούν με ασφάλεια να μοντελοποιήσουν τη λογική των εφαρμογών του ΔτΠ.

Από τη μία πλευρά, η χρήση των έξυπνων συμβολαίων απαιτεί τη χρήση των oracles που είναι ειδικές οντότητες που παρέχουν πραγματικά δεδομένα με αξιόπιστο τρόπο. Η επικύρωση αυτών των έξυπνων συμβολαίων θα μπορούσε να τεθεί σε κίνδυνο, καθώς το ΔτΠ μπορεί να είναι ασταθές. Επιπλέον, η πρόσβαση σε πολλαπλές πηγές δεδομένων θα υπερφόρτωνε αυτά τα συμβόλαια. Αυτή

την εποχή, τα έξυπνα συμβόλαια διανέμονται και αποκεντρώνονται, αλλά δεν μοιράζονται πόρους για τη διανομή εργασιών και την αντιμετώπιση του μεγάλου υπολογιστικού όγκου. Δηλαδή, η εκτέλεση των έξυπνων συμβολαίων γίνεται σε έναν μόνο κόμβο, ενώ ταυτόχρονα η εκτέλεση του κώδικα γίνεται από πολλούς κόμβους. Αυτή η διανομή γίνεται μόνο για τη διαδικασία της επικύρωσης, αντί να χρησιμοποιείται για τη διανομή εργασιών. Το ΔτΠ έχει αξιοποιήσει τις κατανεμημένες δυνατότητες του cloud computing και των Big data για να αυξήσει την επεξεργαστική τους ισχύ. Από τότε οι Data mining τεχνικές μπορούν να αντιμετωπίσουν τα δεδομένα του ΔτΠ σαν σύνολο, επιτρέποντας την καλύτερη κατανόηση του ΔτΠ, δηλαδή της επεξεργαστικής ισχύος που αυξήθηκε λόγω του Cloud computing. Τα Big data επιτρέπουν ταυτόχρονα την επεξεργασία μεγάλου όγκου δεδομένων, επιτρέποντας την εξαγωγή πληροφοριών από μεγάλα σύνολα δεδομένων, κάτι που προηγουμένως ήταν πολύ δύσκολο να γίνει. Στην ενσωμάτωση του ΔτΠ με το Blockchain, τα έξυπνα συμβόλαια θα πρέπει να αξιοποιήσουν την κατανεμημένη φύση τους για να ενεργοποιήσουν τις επεξεργαστικές τους δυνατότητες που παρέχονται σε άλλα παραδείγματα (big data και cloud computing) και απαιτούνται στο ΔτΠ.

Τα έξυπνα συμβόλαια θα πρέπει επίσης να λαμβάνουν υπόψη την ετερογένεια και τους περιορισμούς που υπάρχουν στο ΔτΠ. Οι μηχανισμοί φιλτραρίσματος και οργάνωσης θα πρέπει να συμπληρώνονται από τα έξυπνα συμβόλαια για να ενεργοποιήσουν τις εφαρμογές για την εξυπηρέτηση του ΔτΠ ανάλογα με το θέμα και τις απαιτήσεις. Ένας μηχανισμός ανακάλυψης θα μπορούσε να επιτρέπει τη συμπερίληψη της συσκευής εν κινήσει, κάνοντας αυτές τις εφαρμογές πιο ισχυρές. Τέλος, οι μηχανισμοί ενεργοποίησης απευθείας από τα έξυπνα συμβόλαια θα επέτρεπαν ταχύτερες αντιδράσεις με το ΔτΠ. [12]

3 ΚΕΦΑΛΑΙΟ 3ο : Υλοποιήσεις Blockchain που είναι συμβατές με το Διαδίκτυο των Πραγμάτων

Πρόσφατα εμφανίστηκαν πλατφόρμες και εφαρμογές Blockchain από πολλές διαφορετικές περιοχές, λόγω των πλεονεκτημάτων που προσφέρει αυτή η τεχνολογία. Αυτό το κεφάλαιο ερευνά τις πιο αντιπροσωπευτικές εφαρμογές και πλατφόρμες που συνδυάζουν το ΔτΠ και το Blockchain.

3.1 Πλατφόρμες blockchain για το ΔτΠ

Το Blockchain έχει αναγνωριστεί ως μια καινοτόμα τεχνολογία που μπορεί να επηρεάσει έντονα πολλούς κλάδους. Ο αριθμός των πλατφορμών είναι τόσο μεγάλος και βρίσκεται σε διαρκή αλλαγή που είναι αδύνατον να γίνει σε όλα ανάλυση, όμως σε αυτό το κεφάλαιο θα γίνει αναφορά στα πιο δημοφιλή και τα πιο κατάλληλα για το τομέα του ΔτΠ.

Το Bitcoin ήταν το πρώτο κρυπτονόμισμα και η πρώτη Blockchain πλατφόρμα. Παρέχει έναν μηχανισμό για την πραγματοποίηση χρηματικών συναλλαγών με γρήγορο, φθηνό και αξιόπιστο τρόπο, ο οποίος μπορεί να ενσωματωθεί σε εφαρμογές ως ασφαλές σύστημα πληρωμών. Στον τομέα του ΔτΠ, οι αυτόνομες συσκευές μπορούν να χρησιμοποιήσουν το Bitcoin για να πραγματοποιούν μικροπληρωμές, λειτουργώντας κυρίως ως πορτοφόλια. Γενικά όταν η χρήση του Blockchain περιορίζεται σε μικροπληρωμές, οι εφαρμογές είναι συνδεδεμένες με το νόμισμα, κάτι που μπορεί να είναι μειονέκτημα, καθώς η υποτίμηση του νομίσματος μπορεί να επηρεάσει αρνητικά την εφαρμογή. Όπως αναφέρθηκε η χρήση έξυπνων συμβολαίων είναι μία κοινή λύση κατά την ενσωμάτωση του Blockchain με το ΔτΠ. Το Bitcoin περιλαμβάνει μια γλώσσα scripting που επιτρέπει τον ορισμό συγκεκριμένων συνθηκών κατά την εκτέλεση συναλλαγών. Ωστόσο, το γλώσσα αυτή είναι αρκετά περιορισμένη σε σύγκριση με άλλες πλατφόρμες έξυπνων συμβολαίων. [12]

Όπως αναφέρθηκε μία από τις πλατφόρμες που είχε σημαντικό αντίκτυπο τον τελευταίο καιρό είναι το Ethereum.[31] Το Ethereum ήταν ένα από τα πρωτοποριακά Blockchain που συμπεριλάμβαναν έξυπνα συμβόλαια. Το Ethereum μπορεί να περιγράφεται και ως Blockchain με ενσωματωμένη προγραμματιστική γλώσσα (Solidity) και ως εικονική μηχανή που βασίζεται στη συναίνεση που τρέχει παγκοσμίως (Ethereum Virtual Machine EVM). Η συμπερίληψη των έξυπνων συμβολαίων απομακρύνει το Blockchain από τα νομίσματα και διευκολύνει την ενσωμάτωση αυτής της τεχνολογίας σε νέους τομείς. Αυτό μαζί με την ενεργή και ευρεία κοινότητά του κάνει το Ethereum την πιο δημοφιλή πλατφόρμα για την ανάπτυξη εφαρμογών. Οι περισσότερες εφαρμογές του ΔτΠ χρησιμοποιούν Ethereum ή είναι συμβατές με αυτό. Η απλούστερη προσέγγιση είναι να οριστεί ένα έξυπνο συμβόλαιο όπου οι συσκευές μπορούν να δημοσιεύουν τα μέτρα και τις πολιτικές τους, που αντιδρούν στις αλλαγές. Το Hyperlrdger είχε επίσης μεγάλη απήχηση. Είναι μία πλατφόρμα ανοιχτού κώδικα στην οποία έχουν αναπτυχθεί διάφορα έργα που σχετίζονται με το Blockchain, μεταξύ των οποίων το Hyperledger Fabric, που είναι ένα Blockchain που στερείται αδειών και δεν έχει κρυπτονόμισμα και στις οποίες βασίζονται εμπορικές υλοποιήσεις όπως η πλατφόρμα Blockchain της IBM. Αυτό παρέχει διαφορετικά στοιχεία για συναίνεση και ιδιότητα μέλους. Η κατανεμημένη εφαρμογή μπορεί να αναπτυχθεί στο Blockchain χρησιμοποιώντας γλώσσες γενικού σκοπού. Οι συσκευές του ΔτΠ μπορούν να παρέχουν δεδομένα στο Blockchain μέσω της πλατφόρμας IBM Watson IoT, που διαχειρίζεται συσκευές και επιτρέπει την ανάλυση και το φιλτράρισμα δεδομένων. Η πλατφόρμα Bluemix της IBM διευκολύνει την ενσωμάτωση της τεχνολογίας Blockchain προσφέροντάς την ως υπηρεσία. Η χρήση αυτής της πλατφόρμας επιταχύνει την ανάπτυξη

πρωτότυπων εφαρμογών στην οποία ήδη έχουν αναπτυχθεί αρκετές περιπτώσεις χρήσης. Υπάρχει ένα έργο σε εξέλιξη για την ιχνηλασιμότητα των τροφίμων που χρησιμοποιεί την πλατφόρμα. [32]

Η πλατφόρμα Multichain επιτρέπει τη δημιουργία και την ανάπτυξη ιδιωτικών Blockchain. Το Multichain χρησιμοποιεί ένα API που επεκτείνει τον πυρήνα του αρχικού Bitcoin API με νέα λειτουργικότητα, που επιτρέπει την διαχείριση περιουσιακών στοιχείων, αδειών, συναλλαγών κτλ. Επιπλέον, προσφέρει ένα εργαλείο γραμμής εντολών για την αλληλεπίδραση με το δίκτυο και διαφορετικοί clients μπορούν να αλληλοεπιδρούν μέσω JSON-RPC με το δίκτυο όπως Node.js, Java, C# και Ruby. Το Multichain είναι ένας κλάδος του Bitcoin core, όπου ο κώδικάς του μεταγλωττίζεται για 64 bit αρχιτεκτονικές.

Το Litecoin είναι τεχνικά πανομοιότυπο με το Bitcoin, αλλά διαθέτει ταχύτερους χρόνους επιβεβαίωσης συναλλαγών και βελτιωμένη απόδοση αποθήκευσης χάρη στη μείωση του χρόνου δημιουργίας μπλοκ (από 10 λεπτά σε 2.5) και το proof of work, το οποίο βασίζεται σε scrypt, που είναι μια λειτουργία παραγωγής κλειδιών βάση κωδικού πρόσβασης. Αυτό σημαίνει ότι οι υπολογιστικές απαιτήσεις των κόμβων του Litecoin είναι λιγότερες, επομένως είναι πιο κατάλληλο για IoT. [33]

Το Lisk προσφέρει μια πλατφόρμα Blockchain στην οποία μπορούν να οριστούν subblockchains ή sidechains με αποκεντρωμένες εφαρμογές Blockchain και διάφορες επιλογές κρυπτονομισμάτων για χρήση (πχ. Bitcoin, Ethereum, κτλ). Γνωστό ως πλατφόρμα Blockchain για προγραμματιστές Javascript, το Lisk προσφέρει επίσης υποστήριξη για δημιουργία και ανάπτυξη αποκεντρωμένων εφαρμογών εντός της πλατφόρμας που θα χρησιμοποιηθούν απευθείας από τους τελικούς χρήστες, δημιουργώντας έτσι ένα σύστημα διαλειτουργικών υπηρεσιών Blockchain. Οι εφαρμογές που αναπτύσσονται μπορούν να χρησιμοποιούν νόμισμα LSK ή μπορούν να δημιουργούν ειδικά προσαρμοσμένα tokens. Το Lisk χρησιμοποιεί εξουσιοδοτημένη proof of stake συναίνεση. Επίσης, συνεργάζεται με το chain of things για να εξετάσει εάν η τεχνολογία Blockchain μπορεί να είναι αποτελεσματική στην εδραίωση της ασφάλειας εντός του ΔτΠ. [34]

Το Quorum είναι μια πλατφόρμα Blockchain που αναπτύχθηκε για να παρέχει στη βιομηχανία χρηματοοικονομικών υπηρεσιών μια εγκεκριμένη εφαρμογή του Ethereum με υποστήριξη για το απόρρητο των συναλλαγών και των συμβολαίων. Επιτρέπει πολλαπλούς μηχανισμούς συναίνεσης και επιταχύνει το απόρρητο των δεδομένων μέσω κρυπτογραφίας και τμηματοποίησης. Η πλατφόρμα πρόσφατα ενσωμάτωσε την τεχνολογία ZeroCash για να αποκρύψει όλες τις αναγνωρίσιμες πληροφορίες σχετικά με μία συναλλαγή. Η πλατφόρμα Quorum χρησιμοποιείται από το Chronicled για τη δημιουργία συνδέσμων μεταξύ φυσικών πόρων και του Blockchain.

Το HDAC είναι ένα συμβόλαιο του ΔτΠ και μία πλατφόρμα συναλλαγών M2M που βασίζεται στο Blockchain. Χρησιμοποιεί ένα συνδυασμό δημόσιων και ιδιωτικών Blockchains και δημιουργεί κβαντικούς τυχαίους αριθμούς για την εξασφάλιση αυτών των συναλλαγών. Το δημόσιο Blockchain HDAC κρυπτονόμισμα, μπορεί να χρησιμοποιηθεί αποτελεσματικά με πολλαπλά ιδιωτικά Blockchain.

Πλατφόρμα	Blockchain	Συναίνεση	Κρυπτονόμισμα	Έξυπνα Συμβόλαια
Ethereum	Δημόσια και με άδεια	PoS	Ether (ETH)	Yes
Hyperledger	Με άδεια	PBTF/SIEVE	None	Yes
Multichain	Με άδεια	PBTF	Multi-currency	Yes
Litecoin	Δημόσια	Scrypt	Litecoins (LTC)	No
Lisk	Δημόσια και με άδεια	DPoS	LSK	Yes
Quorum	Με άδεια	Multiple	ETH	Yes
HDAC	Με άδεια	ePoW	Multiasset	Yes

Πίνακας 3.1: Πλατφόρμες Blockchain για τη δημιουργία εφαρμογών Blockchain [12]

Ο πίνακας 1 δείχνει τη σύγκριση των πλατφορμών Blockchain για δημιουργία εφαρμογών IoT. Τα έξυπνα συμβόλαια υπάρχουν στις περισσότερες πλατφόρμες, ενεργοποιώντας έτσι τη λογική εφαρμογής πέρα από τις συναλλαγές. Σε περίπτωση ανάπτυξης ενός Blockchain, υπάρχουν δύο επιλογές, με κρυπτονόμισμα ή χωρίς κρυπτονόμισμα. Μια καθιερωμένη πλατφόρμα με κρυπτονόμισμα όπως το Ethereum μπορεί να παρέχει την απαραίτητη υποδομή για μια εφαρμογή Blockchain. Αυτό μπορεί να θεωρηθεί ως ανάπτυξη δικού μας Cloud ή ως χρήση του AWS της Amazon ή του Cloud της Google. Ωστόσο, στην περίπτωση το Blockchain η διανομή είναι η βάση της αξιοπιστίας του. Από την άλλη πλευρά, η χρήση μιας πλατφόρμας χωρίς κρυπτονόμισμα όπως το Hyperledger Fabric απαιτεί τη συμμετοχή μιας κοινοπραξίας και μιας υποδομής για την έναρξη ενός Blockchain. Το PBTF και το PoS είναι οι πιο συχνά χρησιμοποιούμενες συναινέσεις. Τα δικαιώματα και το απόρρητο υπάρχουν στις περισσότερες πλατφόρμες, επομένως οι κοινοπραξίες και οι global εφαρμογές μπορούν να δημιουργηθούν από αυτά. [12]

3.2 Εφαρμογές Blockchain

Στα οικονομικά, υπήρξε μια σημαντική εμφάνιση κρυπτονομισμάτων (1486 σύμφωνα με το coinmarketcap) που έχουν δημιουργήσει μια νέα αγορά και έχουν ενεργοποιήσει νέους τρόπους πληρωμής και επένδυσης. Παραδείγματα αυτών είναι το Ripple, το Litecoin, το Nxt, το Peercoin, το Bitshres, το Dogecoin, το Namecoin, το Dash, το Monero κτλ. Αυτή η νέα αγορά επίσης οδήγησε στην εμφάνιση νέων εφαρμογών για πληρωμές, ανταλλαγές χρημάτων και υποδομές συναλλαγών για αυτά τα νέα νομίσματα. [12]

Πέρα από τα οικονομικά, το κατανεμημένο και αξιόπιστο καθολικό του Blockchain έχει αναγνωριστεί ως ιδανική λύση για τα συστήματα ιχνηλασιμότητας. Ό,τι είναι οι οικονομικές συναλλαγές για το Bitcoin, έχουν γίνει οι αλλαγές των plotted αντικειμένων. Με αυτόν τον τρόπο η αλυσίδα αποθηκεύει τα αντικείμενα και τις αλλαγές τους, επιτρέποντας μια πλήρη, ανοιχτή και αξιόπιστη ιχνηλασιμότητα, δυνατή μόνο μέσω αυτής της τεχνολογίας. Υπάρχουν κάποια έργα σε εξέλιξη από διακεκριμένες εταιρίες όπως πχ η IBM, η Unilever, η Walmart και η Nestle που

συνεργάζονται για την ιχνηλασιμότητα των τροφίμων [35] ή η Renault για την παρακολούθηση του ιστορικού συντήρησης των οχημάτων. [36],[12]

Η επαλήθευση ταυτότητας έχει επίσης γίνει μια δημοφιλής εφαρμογή της τεχνολογίας και το Blockchain παρέχει ένα ανοιχτό και αξιόπιστο κατανεμημένο καθολικό που μπορεί να χρησιμοποιηθεί για την αποθήκευση ταυτοτήτων. Αυτό καθιστά δυνατή την global διαχείριση. Στον τομέα της ηλεκτρονικής διακυβέρνησης πολλές χώρες έχουν προτείνει τη χρήση τεχνολογιών Blockchain, για παράδειγμα: για διαβατήρια στο Ντουμπάι, ηλεκτρονική ταυτότητα στην Εσθονία, για την ψηφιοποίηση πιστοποιητικών γέννησης στο Ιλινόις και στην Ινδία για εγγραφή γης. [12]

Επιπλέον, η ενσωμάτωση των έξυπνων συμβολαίων ανοίγει πολλές προοπτικές για πολλούς κλάδους: την ενέργεια, τις ασφάλειες, τα στεγαστικά δάνεια, τις πληρωμές των δικαιωμάτων μουσικής, τα ακίνητα, τα τυχερά παιχνίδια κτλ. Η αποθήκευση στο cloud, η εκπαίδευση ή η ηλεκτρονική υγεία (e-health) είναι άλλου τομείς στους οποίους έχει προταθεί η τεχνολογία του Blockchain. Ο Πίνακας 2 παραθέτει μερικές από αυτές τις εφαρμογές σε διάφορους τομείς. [12]

Application	Classification
Ripple Litecoin Nxt Peercoin Dogecoin Namecoin Dash Monero	Cryptocurrency
BitPay Abra	New payment infrastructures
BitNation Onename Keybase ShoCard	Identity verification
Passport management e-identity Birth certificates Land registration Follow my vote	e-government
Tierion Proof of Existence Factom Everledger MIT’s digital diploma	Verification of ownership or provenance
Provenance.org SkuChain IBM Food traceability Renault vehicle maintenance history tracking	Product traceability
Robomed Medrec	e-health
Synechron	Energy, insurance and mortgages
Ubitquity	Real estates

Atlant	
Slock.it	Renting, sharing and selling
DAO.Casino Peerplays Wagerr	Gambling and betting
Storj	Cloud storage
Sony education history	Education
Ujo Resonate	Music royalty payments

Πίνακας 3.2: Εφαρμογές Blockchain [12]

3.3 Εφαρμογές ΔτΠ – Blockchain και οι αρχιτεκτονικές τους

Οι εφαρμογές ΔτΠ – Blockchain βρίσκονται ακόμα σε αρχικό στάδιο. Ωστόσο, η ενσωμάτωση του ΔτΠ με το Blockchain εξελίσσεται και αναπτύσσεται ραγδαία. Παρακάτω θα παρουσιαστούν τα χαρακτηριστικά και οι αρχιτεκτονικές των εφαρμογών ΔτΠ – Blockchain. Οι αρχιτεκτονικές αυτές χωρίζονται σε δυο κατηγορίες: [13]

3.3.1 Συγκεκριμένη εφαρμογή

Ο όρος συγκεκριμένη εφαρμογή αναφέρεται στο αυτόνομο λογισμικό ή σύστημα που χρησιμοποιεί το ΔτΠ και το Blockchain ως βασικό υλικό στις εμπορικές τους λειτουργίες. Τα βασικά επίπεδα αυτής της κατηγορίας είναι το επίπεδο εφαρμογής (application layer) και το φυσικό επίπεδο (physical layer). Οι συσκευές του ΔτΠ και οι λειτουργίες της εφαρμογής καθορίζουν τη φύση της ΔτΠ - Blockchain εφαρμογής. Το επίπεδο του Blockchain και το επίπεδο του δικτύου είναι υπεύθυνα για την αποθήκευση και την επικοινωνία. Μερικές εφαρμογές ΔτΠ – Blockchain με απλή αρχιτεκτονική δεν περιλαμβάνουν το επίπεδο του ενδιάμεσου λογισμικού. [13]

Στο [14] γίνεται παρουσίαση της δομής LSB του Blockchain που δίνει έμφαση στην ασφάλεια και το απόρρητο σε ένα έξυπνο σπίτι. Η αρχιτεκτονική του LSB φαίνεται στον πίνακα 3 το physical layer περιλαμβάνει διάφορους τύπους έξυπνων συσκευών. Οι έξυπνες συσκευές υψηλών πόρων είναι υπεύθυνες για τη διαχείριση ενός κοινού Blockchain για τη διασφάλιση του απορρήτου και της ασφάλειας των χρηστών. Οι συσκευές του ΔτΠ μικρών πόρων είναι υπεύθυνες για την end-to-end επικοινωνία και την επεξεργασία των εισερχομένων και των εξερχομένων αιτημάτων. Οι έξυπνες συσκευές είναι εγγεγραμμένες στο δίκτυο του Blockchain. Το Middleware επίπεδο παρέχει επικαλυπτόμενη διαχείριση Blockchain που μπορεί να μειώσει τα γενικά έξοδα διαχείρισης του Blockchain. Οι εφαρμογές έξυπνου σπιτιού επιτυγχάνουν τον οικιακό αυτοματισμό. [13]

IoT Blockchain	Application layer	Middleware layer	Blockchain layer	Network layer	Physical layer
Smart home	Smart home application	overlay Blockchain management	commercial Blockchain	P2P Network	Smart device
LO3 Energy	Energy shopping application	Exergy token system	Public Blockchain solution	Low latency Network	Grid Edge, Solar plane
Slock.it	Dapp	None	Ethereum	Commercial Network	Electronic Locks
Hybrid - IoT	IoT application	Hybrid - IoT platform	PoW Blockchain, BFT Blockchain	P2P Network	Full peer, Light peer, Sensor
BPIIoT	Manufacturing Dapps	Single - board computers	Blockchain Network bridge	P2P Network	IoT devices
JD.com	JD.com	Blockchain gateway service	BFT Blockchain	P2P Network	IoT devices
IoT data Service Framework	Data user application	Data integrity service Framework	Ethereum	P2P Network	IoT devices
IoT Chain	Authorized access	OSCAR, ACE Framework	Ethereum	Commercial Network	IoT devices

Πίνακας 3.3: Περίληψη αρχιτεκτονικών ΔτΠ – Blockchain [13]

Το LO3 Energy παρουσιάζει μια αγορά P2P για την ηλιακή ενέργεια. Η αρχιτεκτονική του LO3 φαίνεται στον πίνακα 3. Το φυσικό στρώμα του LO3 περιλαμβάνει ηλεκτρικό δίκτυο και ηλιακά πάνελ. Αναλύουν την επιπλέον ενεργειακή απόδοση και την ανεβάζουν στο Blockchain μέσω ενός δικτύου χαμηλής καθυστέρησης [13]. Τα μικροδίκτυα της LO3 Energy βασίζονται στην εξουσιοδοτημένη πλατφόρμα Exergy και χρησιμοποιούν το τοπικό νόμισμα XRG ενώ επιτρέπουν στα μέλη να πραγματοποιούν συναλλαγές P2P. Επιπλέον, οι προμηθευτές, που είναι παραγωγοί και καταναλωτές της δικής τους ανανεώσιμης ενέργειας, μπορούν να πουλήσουν αυτήν την ενέργεια σε άλλα μέλη του μικροδικτύου με διαφάνεια και ιχνηλασιμότητα [15].

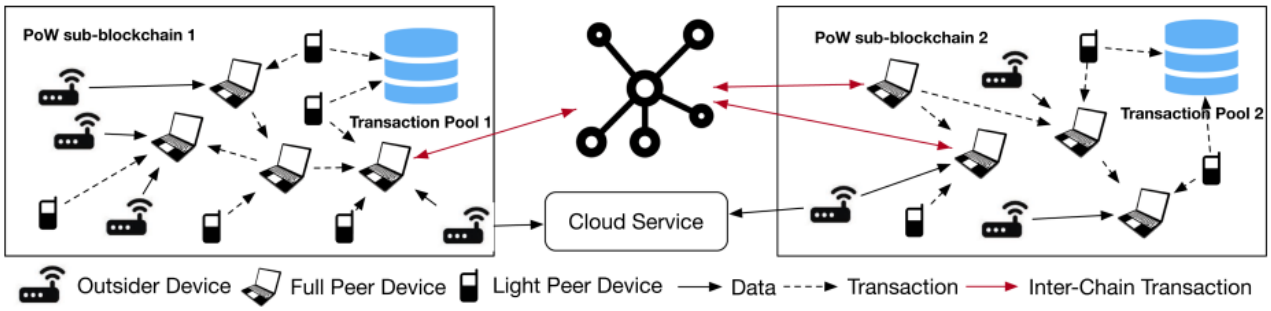
Το Slock.it είναι μια υπάρχουσα εφαρμογή ΔτΠ – Blockchain στην αγορά. Λειτουργεί με ηλεκτρονικές «κλειδαριές» οι οποίες ξεκλειδώνουν με το κατάλληλο νόμισμα. Ο πελάτης που επιθυμεί να πουλήσει την ιδιοκτησία του μπορεί να ορίσει τιμή στην κλειδαριά. Ο πελάτης μπορεί να περιηγηθεί στα αγαθά και να πληρώσει το ποσό που ζητήθηκε σε κρυπτονομίσματα για να ξεκλειδώσει την κλειδαριά. Η αρχιτεκτονική του Slock.it εμφανίζεται στον πίνακα 3. Έχει μία απλή αρχιτεκτονική που αποτελείται από κατανεμημένες εφαρμογές, Ethereum Blockchain, εμπορικό δίκτυο και ηλεκτρονικές κλειδαριές. [13]

3.3.2 Η πλατφόρμα εφαρμογής ως υπηρεσία

Η πλατφόρμα της εφαρμογής ως υπηρεσία αναφέρεται στο λογισμικό υποστήριξης που συνδέει τα πάντα σε ένα σύστημα ΔτΠ – Blockchain. Ενσωματώνει συσκευές ΔτΠ και την τεχνική του Blockchain και παρέχει μια απλή πλατφόρμα διαχείρισης για προγραμματιστές. Διευκολύνει την επικοινωνία, τη ροή δεδομένων και τη διαχείριση συσκευών. Το βασικό επίπεδο αυτής της

κατηγορίας είναι το Middleware επίπεδο. Η φύση του Middleware επιπέδου καθορίζει τις λειτουργίες της υπηρεσίας της πλατφόρμας. Σε αυτή την κατηγορία, τα στοιχεία του Application επιπέδου και του Physical επιπέδου δεν καθορίζονται. Το επίπεδο Blockchain και το Network επίπεδο χρειάζεται να υποστηρίζουν τις λειτουργίες του ενδιάμεσου λογισμικού. Για παράδειγμα, να επιτρέπεται ο έλεγχος της ακεραιότητας των δεδομένων στο έξυπνο συμβόλαιο. [13]

Στο [16] προτείνεται μια νέα πλατφόρμα IoT-Blockchain, το «Hybrid-IoT». Η πλατφόρμα εφαρμόζει την συναίνεση με βάση το PoW και τους αλγόριθμους BFT. Τα Sub-Blockchains και τα Inter-Blockchains ορίζονται ως δομές περιοχής του IoT-Blockchain. Η εικόνα 1 δείχνει την αρχιτεκτονική του υβριδικού ΔτΠ. Στην αρχιτεκτονική αυτή, δύο PoW Sub-Blockchain συνδέονται με ένα BFT πλαίσιο διασύνδεσης (inter – connector framework). [13]



Εικόνα 3.1: αρχιτεκτονική του υβριδικού ΔτΠ [13]

Στο [17] γίνεται εισαγωγή της πλατφόρμας για το βιομηχανικό ΔτΠ (BPIIoT). Αυτή η πλατφόρμα επιτρέπει στους χρήστες να αναπτύσσουν εφαρμογές (DApps) με τα χαρακτηριστικά του Blockchain. Η αρχιτεκτονική του φαίνεται στον Πίνακα 3. Στην πλατφόρμα, οι συσκευές του ΔτΠ πρέπει μα εγγραφούν σε ένα δίκτυο Blockchain. Οι χρήστες μπορούν να αναπτύξουν εφαρμογές σε Single-board computers (SBC) για τον έλεγχο και τη διαχείριση του δικτύου και των συσκευών του ΔτΠ. [13]

Η ηλεκτρονική επιχειρηματική εταιρεία «JD.com» δημοσιεύει μια πλατφόρμα Blockchain «JD Blockchain Open Platform» που εστιάζει στην παροχή ΔτΠ λύσεων με την τεχνολογία του Blockchain. Αυτή η πλατφόρμα Blockchain παρέχει υπηρεσία Blockchain gateway, υπηρεσία Blockchain node και υπηρεσία Blockchain consensus network. Η αρχιτεκτονική του φαίνεται στον πίνακα 3. Η πλατφόρμα χρησιμοποιεί ένα τύπου BFT consensus αλγόριθμο. Επίσης, χρησιμοποιείται ένα πρωτόκολλο ελέγχου ταυτότητας για τον έλεγχο του αριθμού των προσβάσεων στο δίκτυο του Blockchain. Το σύστημα έχει τρία είδη peers: τα consensus peers, τα gateway peers και τις συσκευές του ΔτΠ. Τα gateway peers λειτουργούν στο Middleware επίπεδο για να ενσωματώνουν εισόδους και πρωτόκολλα από χαμηλότερα επίπεδα. [13]

Στο [19] προτείνεται ένα πλαίσιο για την εφαρμογή της ακεραιότητας και της ασφάλειας των δεδομένων του IoT που βασίζεται σε ένα σύστημα Blockchain. Επίσης, περιγράφονται τα κρίσιμα στοιχεία του προτεινόμενου πλαισίου υπηρεσιών ακεραιότητας αποκεντρωμένων δεδομένων. Το πλαίσιο επιτυγχάνει πλήρη αποκέντρωση με πρωτόκολλο επαλήθευσης της ακεραιότητας των δεδομένων. Παρέχει αξιόπιστη επαλήθευση της ακεραιότητας των δεδομένων στους χρήστες σε ένα ΔτΠ σύστημα χωρίς να απαιτείται ελεγκτής. Η αρχιτεκτονική του φαίνεται στον πίνακα 3. Στο πλαίσιο αυτό, η συσκευή του ΔτΠ είναι υπεύθυνη για τη δημιουργία δεδομένων και την εγγραφή των δεδομένων στο Ethereum. Ο χρήστης μπορεί να ελέγξει την ακεραιότητα των δεδομένων που παρέχεται από την υπηρεσία ακεραιότητας δεδομένων μέσω μιας εφαρμογής. [13]

Στο [20] προτείνεται μια αρχιτεκτονική, η «IoT Chain» (αλυσίδα του ΔτΠ) η οποία συνδυάζει την αρχιτεκτονική OSCAR [21] και το πλαίσιο εξουσιοδότησης ACE [22]. Στο IoTChain, κάθε εγγεγραμμένος χρήστης έχει ένα εξουσιοδοτημένο νόμισμα. Αυτό προσδιορίζει το ιδιαίτερο προνόμιο ενός συνόλου πόρων. Όταν ένας χρήστης επιθυμεί να έχει πρόσβαση σε ένα αντικείμενο, τότε πρέπει να στείλει μια συναλλαγή με τα απαιτούμενα δεδομένα στη διεύθυνση του έξυπνου συμβολαίου. Στη συνέχεια, το έξυπνο συμβόλαιο θα δημιουργήσει ένα εξουσιοδοτημένο νόμισμα για τα δεδομένα του χρήστη. Αυτή η αρχιτεκτονική χρησιμοποιεί το Blockchain αντί για τον κεντρικό διακομιστή εξουσιοδότησης ACE. Η αρχιτεκτονική του IoTChain φαίνεται στον Πίνακα 3. Σε αυτήν την αρχιτεκτονική, η συσκευή IoT είναι υπεύθυνη για την παραγωγή δεδομένων. ο κάτοχος των δεδομένων είναι υπεύθυνος για τη μεταφόρτωση των δεδομένων στο Blockchain. Η αρχιτεκτονική OSCAR και το πλαίσιο εξουσιοδότησης ACE είναι υπεύθυνα για τη διασφάλιση της ασφάλειας των δεδομένων του χρήστη. [13]

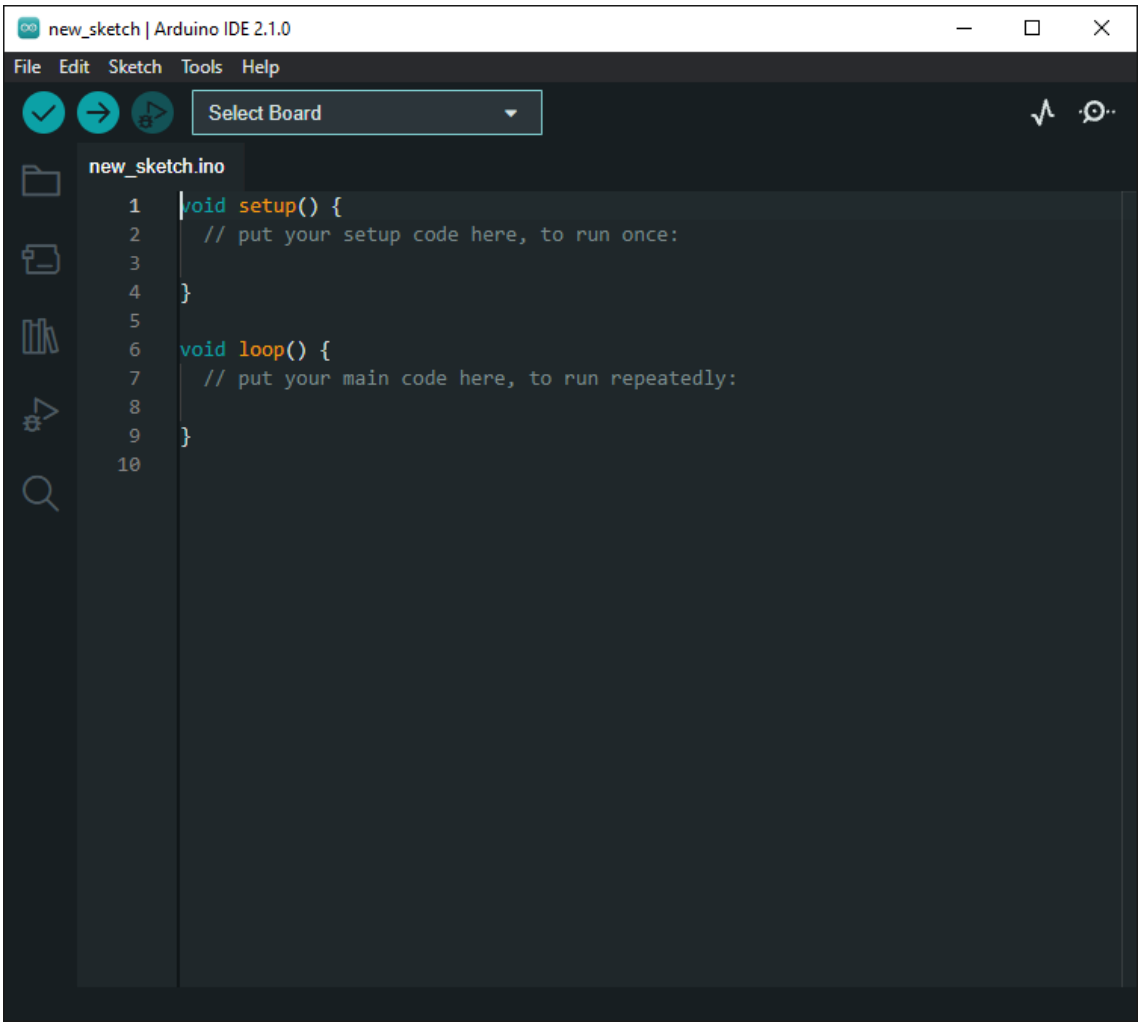
4 ΚΕΦΑΛΑΙΟ 4ο : Υλοποίηση Συστήματος του Δικτύου των πραγμάτων και σύνδεση με Ethereum Blockchain

Τα τελευταία χρόνια, το Internet of Things (IoT) έχει αναδυθεί ως ένα υποσχόμενο πεδίο με σημαντικό δυναμικό για να επανασχεδιάσει τον τρόπο που αλληλοεπιδρούμε με την τεχνολογία. Τα IoT συστήματα είναι σχεδιασμένα για να συνδέονται και να επικοινωνούν με άλλες συσκευές και υπηρεσίες, τα οποία μπορούν να αξιοποιηθούν για να δημιουργηθούν έξυπνα σπίτια, έξυπνα συστήματα μεταφορών και άλλες καινοτόμες εφαρμογές. Ένα από τα προβλήματα στην ανάπτυξη των συστημάτων IoT είναι η αποθήκευση και επεξεργασία των τεράστιων ποσοτήτων δεδομένων που παράγονται από αυτές τις συσκευές.

Μια λύση για αυτό το πρόβλημα είναι η χρήση της τεχνολογίας του blockchain, η οποία παρέχει έναν ασφαλή και αποκεντρωμένο τρόπο για την αποθήκευση και διαχείριση δεδομένων. Το Ethereum είναι μία από τις πιο δημοφιλείς πλατφόρμες blockchain και είναι ιδιαίτερα κατάλληλη για την ανάπτυξη έξυπνων συμβολαίων, τα οποία είναι αυτόματα εκτελούμενα προγράμματα που μπορούν να χρησιμοποιηθούν για την αυτοματοποίηση της εκτέλεσης συναλλαγών στο blockchain. Σε αυτή τη διπλωματική, ο στόχος είναι να εξερευνηθεί πώς μία συσκευή IoT, όπως ένα ESP32 με αισθητήρα θερμοκρασίας και υγρασίας DHT22, μπορεί να συνδεθεί σε ένα δίκτυο Ethereum blockchain για να αποθηκεύσει τα δεδομένα της σε ένα έξυπνο συμβόλαιο. Για τον προγραμματισμό του ESP32 θα χρησιμοποιηθεί το περιβάλλον του Arduino.

Για να επιτύχει αυτό, θα πρέπει να δημιουργηθεί ένα έξυπνο συμβόλαιο που μπορεί να αποθηκεύει τα δεδομένα θερμοκρασίας και υγρασίας που στέλνει η συσκευή IoT. Το έξυπνο συμβόλαιο θα γραφεί σε Solidity, η οποία είναι μια γλώσσα προγραμματισμού που χρησιμοποιείται για την ανάπτυξη έξυπνων συμβολαίων στην πλατφόρμα Ethereum. Το έξυπνο συμβόλαιο θα ορίζει έναν χαρτογράφο (mapping) που αντιστοιχεί τις διευθύνσεις Ethereum των συσκευών στις αναγνώσεις θερμοκρασίας και υγρασίας που αποθηκεύονται σε μια δομή (struct).

4.1 Τι είναι το Arduino



Εικόνα 4.1: Περιβάλλον Arduino

Το λογισμικό Arduino αναφέρεται στο Περιβάλλον Ανάπτυξης Ενσωματωμένων Συστημάτων (IDE) που χρησιμοποιείται για την προγραμματισμό και την ανάπτυξη έργων με τις καρτέλες μικροελεγκτή Arduino. Το λογισμικό Arduino επιτρέπει στους χρήστες να γράφουν, να συγκεντρώνουν και να μεταφορτώνουν κώδικα στην καρτέλα μικροελεγκτή, και περιλαμβάνει έναν επεξεργαστή κώδικα, έναν μεταγλωττιστή και έναν σειριακό παρακολουθητή, μεταξύ άλλων χαρακτηριστικών.

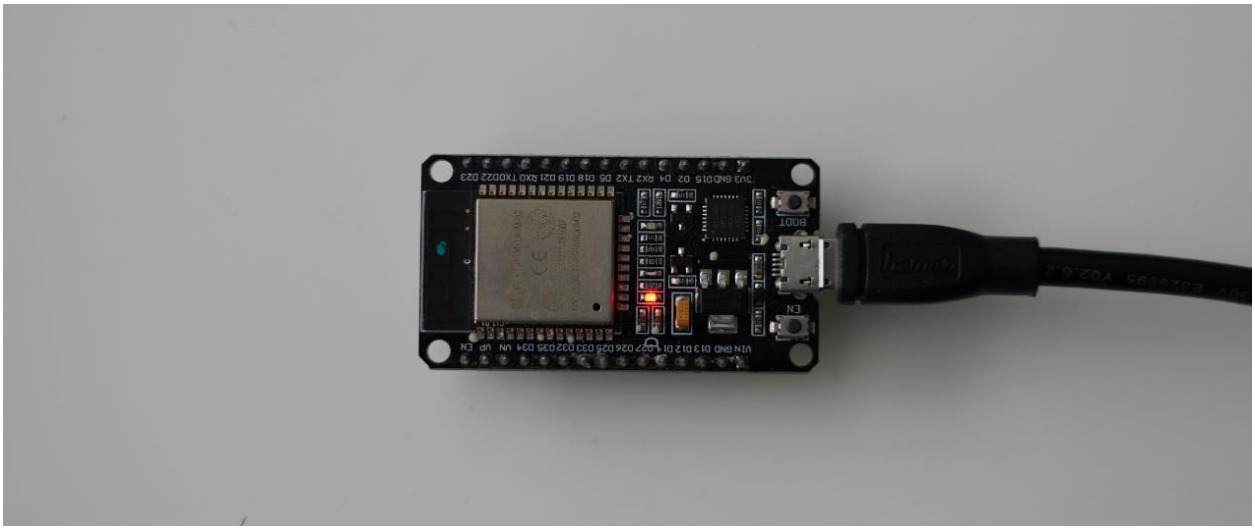
Το λογισμικό είναι ανοιχτού κώδικα και μπορεί να ληφθεί δωρεάν από την ιστοσελίδα του Arduino. Χρησιμοποιεί μια απλοποιημένη έκδοση της γλώσσας προγραμματισμού C++. Οι χρήστες μπορούν να δημιουργήσουν μια ευρεία γκάμα έργων, από απλά αναβοσβήματα LED έως πολύπλοκα ρομποτικά συστήματα. Το λογισμικό παρέχει μια εκτενή βιβλιοθήκη προγραμμάτων που έχουν προγραμματιστεί εκ των προτέρων και μπορούν να χρησιμοποιηθούν για τη γρήγορη και εύκολη κατασκευή έργων. Επιπλέον, είναι συμβατό με διάφορους αισθητήρες, shields και modules, επιτρέποντας στους χρήστες να επεκτείνουν τα έργα και τις δυνατότητές τους.

4.2 Τι είναι το ESP32 και ο αισθητήρας DHT22 και πως συνδέονται

Το ESP32 είναι ένας ευέλικτος μικροελεγκτής που προσφέρει συνδεσιμότητα Wi-Fi και Bluetooth, καθιστώντας το ιδανικό για μια ευρεία γκάμα εφαρμογών IoT (Internet of Things). Ο αισθητήρας DHT22, από την άλλη πλευρά, είναι μια δημοφιλής επιλογή για τη μέτρηση της θερμοκρασίας και

της υγρασίας σε διάφορα περιβάλλοντα. Η κατανόηση του τρόπου λειτουργίας αυτών των δύο στοιχείων είναι σημαντική για την κατασκευή έργων IoT που αφορούν την παρακολούθηση του περιβάλλοντος, την αυτοματοποίηση του σπιτιού και πολλά άλλα.

4.2.1 ESP32

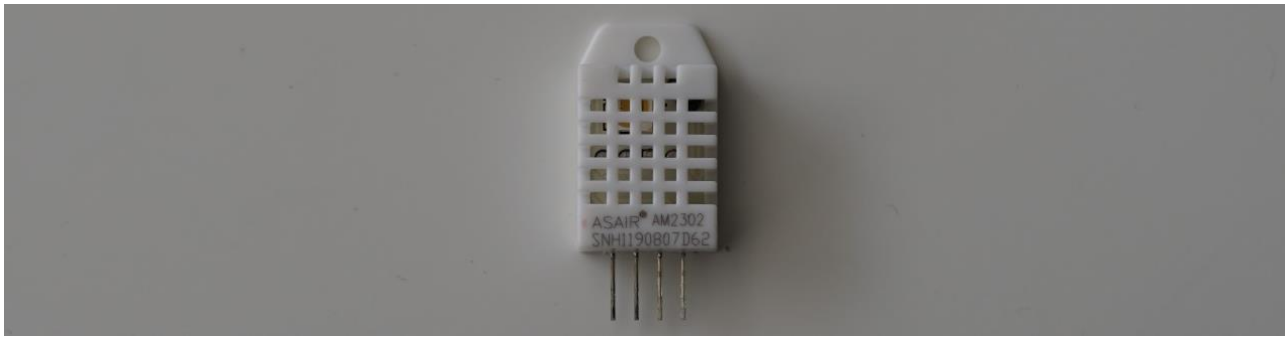


Εικόνα 4.2: ESP-WROOM32 module

Το ESP32 είναι ένας μικροελεγκτής χαμηλής κατανάλωσης που σχεδιάστηκε από την εταιρεία Espressif Systems. Βασίζεται στο σύστημα ενσωματωμένου κυκλώματος ESP32 (SoC) και προσφέρει μια ισχυρή υπολογιστική πλατφόρμα για εφαρμογές IoT. Το ESP32 διαθέτει διπλοπύρηνο επεξεργαστή, διάφορες περιφερειακές μονάδες και ενσωματωμένη συνδεσιμότητα Wi-Fi και Bluetooth, επιτρέποντας την αλληλεπίδρασή του με άλλες συσκευές και την επικοινωνία μέσω του διαδικτύου.

Το ESP32 υποστηρίζει διάφορες γλώσσες προγραμματισμού και πλαίσια ανάπτυξης, συμπεριλαμβανομένων του Arduino IDE, του MicroPython και του ESP-IDF (ESP32 IoT Development Framework) που παρέχεται από την Espressif. Αυτή η ευελιξία το καθιστά προσβάσιμο τόσο για αρχάριους όσο και για έμπειρους προγραμματιστές. Το ESP-IDF παρέχει χαμηλού επιπέδου έλεγχο και πρόσβαση στα χαρακτηριστικά του υλικού, επιτρέποντας τον μέγιστο βαθμό προσαρμογής και βελτιστοποίησης.

4.2.2 Κατανόηση του Αισθητήρα DHT22



Εικόνα 4.3: Αισθητήριο DHT22

Ο αισθητήρας DHT22, είναι ένας ψηφιακός αισθητήρας που μετρά τη θερμοκρασία και την υγρασία. Χρησιμοποιεί έναν αισθητήρα υγρασίας και έναν θερμίστορ για την ακριβή ανίχνευση αυτών των

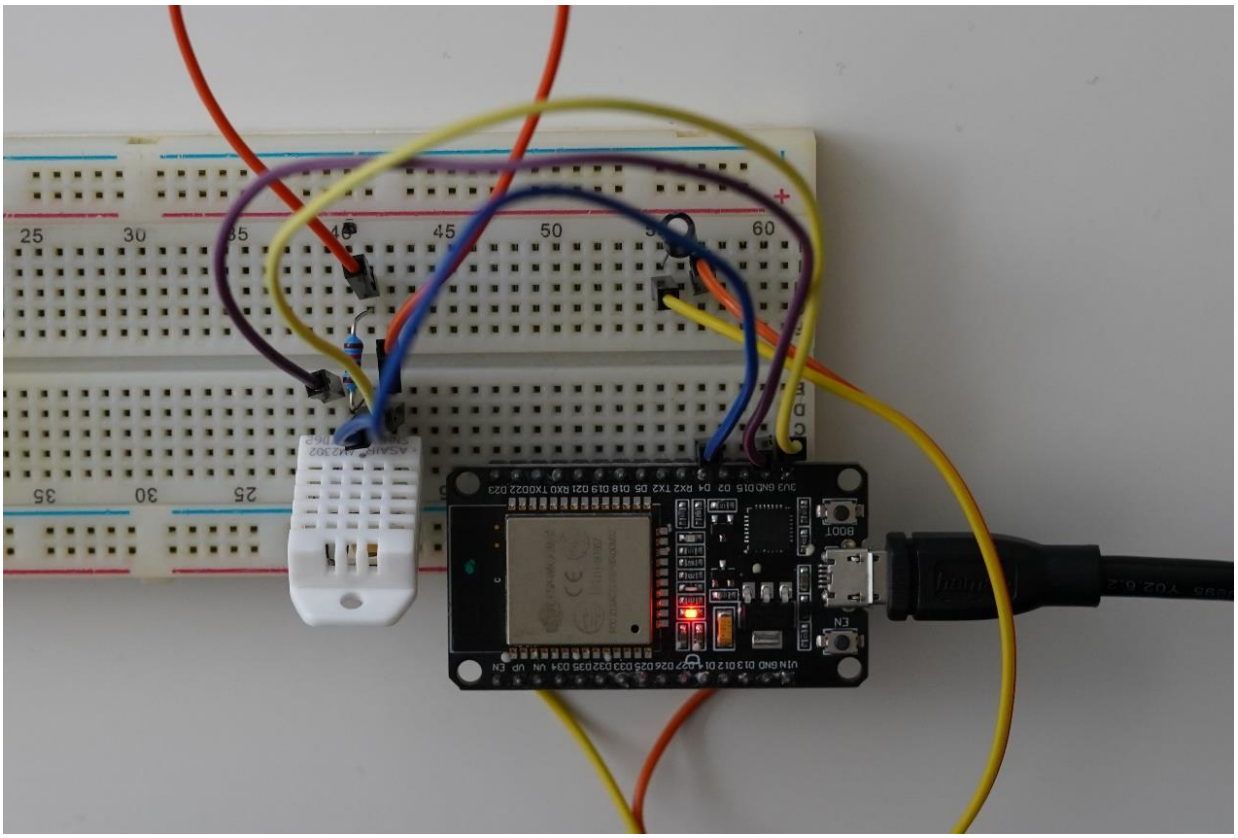
περιβαλλοντικών παραμέτρων. Ο αισθητήρας DHT22 είναι αξιόπιστος, οικονομικός και ευρέως χρησιμοποιείται σε έργα DIY και εμπορικές εφαρμογές.

Ο αισθητήρας DHT22 επικοινωνεί χρησιμοποιώντας ένα μονόκλωνο ψηφιακό πρωτόκολλο που ονομάζεται "One-Wire" ή "DHT πρωτόκολλο". Αυτό το πρωτόκολλο επιτρέπει στον αισθητήρα να αποστέλλει δεδομένα θερμοκρασίας και υγρασίας στο μικροελεγκτή με έναν απλό και αποτελεσματικό τρόπο. Τα δεδομένα μεταδίδονται ως ένα ψηφιακό σήμα 40-bit, το οποίο περιλαμβάνει 16 bit για την τιμή υγρασίας, 16 bit για την τιμή θερμοκρασίας και έναν έλεγχο ακεραιότητας δεδομένων.

4.2.3 Σύνδεση του ESP32 με τον Αισθητήρα DHT22

Για να συνδεθεί το ESP32 με τον αισθητήρα DHT22, θα χρειαστούν τα παρακάτω στοιχεία:

- ESP32 development board ή module
- Αισθητήρας DHT22
- Πλακέτα breadboard
- Καλώδια
- Αντίσταση 10KΩ



Εικόνα 4.4: Σύνδεση ESP32 με το αισθητήριο DHT22

Η διαδικασία σύνδεσης περιλαμβάνει τα εξής βήματα:

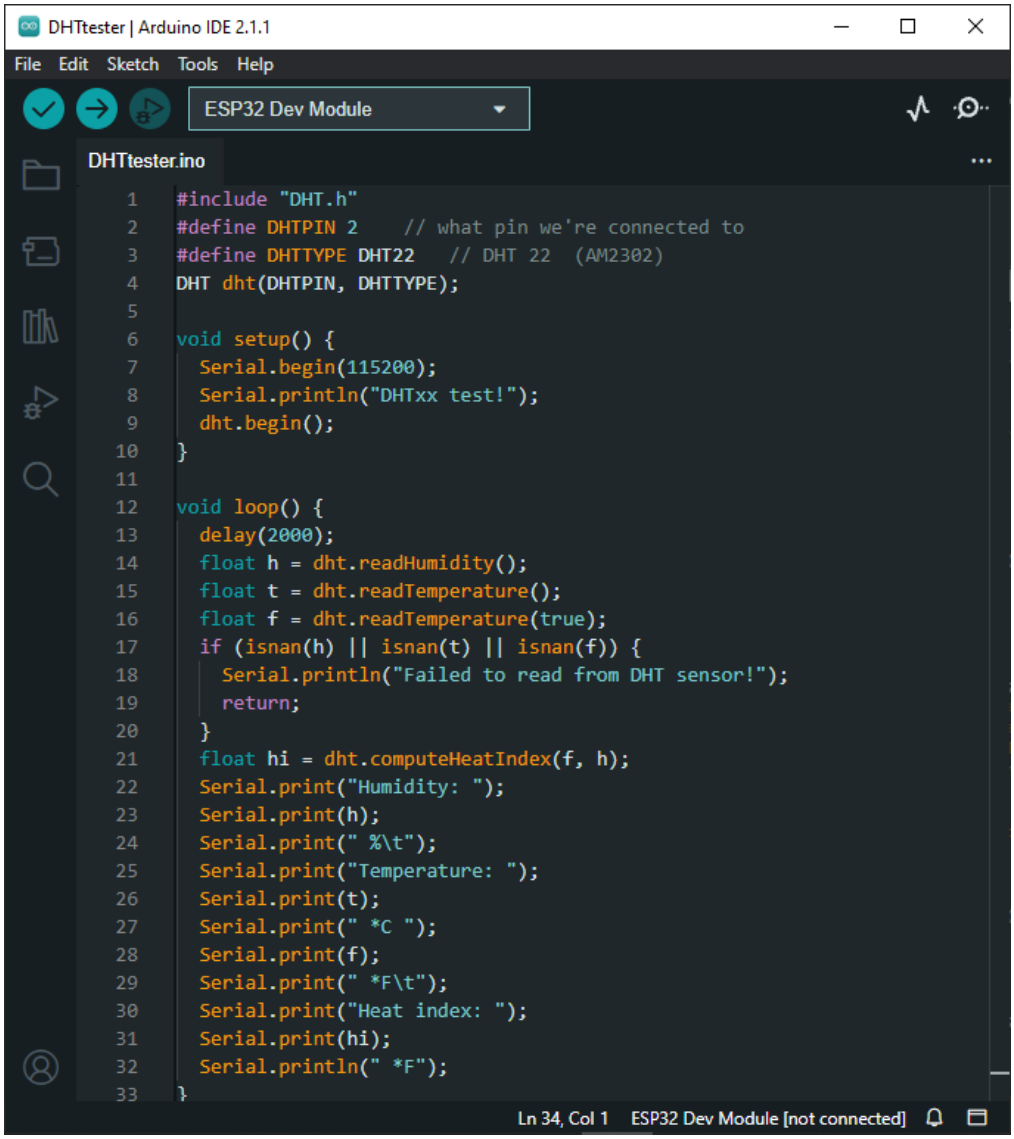
Σύνδεση στην παροχή ισχύος: Παρέχεται στο ESP32 μια σταθερή παροχή ισχύος συνδέοντας τα pin VCC και GND του ESP32 με τις αντίστοιχες γραμμές στο breadboard.

Σύνδεση της γραμμή δεδομένων: Σύνδεση του ακροδέκτη δεδομένων (Data) του αισθητήρα DHT22 σε οποιοδήποτε ψηφιακό ακροδέκτη GPIO στο ESP32. Χρησιμοποιείται μια αντίσταση τύπου pull-up (10kΩ) μεταξύ της γραμμής δεδομένων και του ακροδέκτη VCC για την εξασφάλιση της σταθερότητας του σήματος. Η αντίσταση pull-up αποτρέπει την ελεύθερη κίνηση της γραμμής δεδομένων όταν ο αισθητήρας δεν μεταδίδει δεδομένα.

Δημιουργία επικοινωνίας: Για την ενεργοποίηση της επικοινωνίας μεταξύ του ESP32 και του αισθητήρα DHT22, πρέπει να γίνει η εγκατάσταση των απαραίτητων βιβλιοθηκών. Για το Arduino IDE, είναι η "DHT.h" για τη σύνδεση με τον αισθητήρα DHT22.

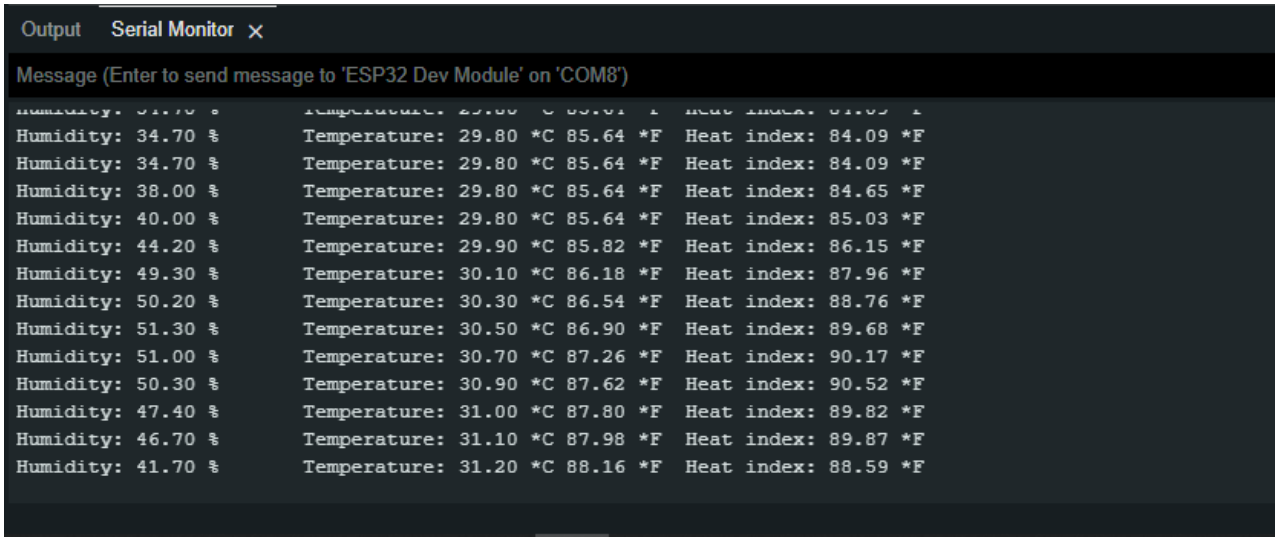
Αρχικοποίηση του αισθητήρα: Στον κώδικα, γίνεται αρχικοποίηση του αισθητήρα δηλώνοντας τον ακροδέκτη GPIO στον οποίο είναι συνδεδεμένη η γραμμή δεδομένων του αισθητήρα. Αυτό το βήμα εξασφαλίζει ότι ο μικροελεγκτής αναγνωρίζει τον αισθητήρα και είναι έτοιμος να λάβει δεδομένα.

Ανάγνωση δεδομένων από τον αισθητήρα: Χρησιμοποιούνται οι κατάλληλες λειτουργίες της βιβλιοθήκης για να διαβαστούν τα δεδομένα θερμοκρασίας και υγρασίας από τον αισθητήρα DHT22. Η βιβλιοθήκη θα αναλάβει το χαμηλού επιπέδου πρωτόκολλο επικοινωνίας και την αποκωδικοποίηση του ληφθέντος σήματος.



Εικόνα 4.5: Κώδικας που χρησιμοποιήθηκε στο παράδειγμα

Επεξεργασία και χρήση των δεδομένων: Μόλις ληφθούν τα δεδομένα από τον αισθητήρα, μπορεί να γίνει περαιτέρω επεξεργασία, να εφαρμοστεί βαθμονόμηση εάν είναι απαραίτητο και να τα χρησιμοποιηθούν για την επιθυμητή εφαρμογή. Αυτό μπορεί να περιλαμβάνει την εμφάνιση των δεδομένων σε ένα LCD, την ασύρματη μετάδοσή τους ή την αποθήκευσή τους σε μια βάση δεδομένων για ανάλυση.



Εικόνα 4.6: Δεδομένα από τη σύνδεση του ESP32 με τον αισθητήρα DHT22 στο Serial Monitor του Arduino

Συμπέρασμα:

Το μοντέλο ESP32, με τις ισχυρές του δυνατότητες και την ενσωματωμένη τεχνολογία Wi-Fi και Bluetooth, παρέχει ένα αξιόπιστο και ευέλικτο πλαίσιο για τα έργα IoT. Συνδέοντας το ESP32 με έναν αισθητήρα DHT22, γίνεται εύκολη η παρακολούθηση της θερμοκρασίας και της υγρασίας σε πραγματικό χρόνο, ανοίγοντας προοπτικές για εφαρμογές όπως η αυτοματοποίηση του σπιτιού, οι μετεωρολογικοί σταθμοί και η έξυπνη γεωργία. Η κατανόηση των λεπτομερειών και της άριστης ενσωμάτωσης αυτών των εξαρτημάτων είναι ουσιώδης για την αξιοποίηση της πλήρους δυνατότητας του μοντέλου ESP32 και του αισθητήρα DHT22 στα έργα IoT.

4.3 Τι είναι η Solidity

Η Solidity είναι μια γλώσσα υψηλού επιπέδου που χρησιμοποιείται για την εγγραφή έξυπνων συμβολαίων στο Ethereum blockchain. Είναι μια γλώσσα προσανατολισμένη στα συμβόλαια που σχεδιάστηκε για να υποστηρίξει τη δημιουργία, την ανάπτυξη και την εκτέλεση συμβολαίων στην Ethereum Virtual Machine (EVM).

Η Solidity είναι παρόμοια με τη σύνταξη της JavaScript και δημιουργήθηκε από το Ίδρυμα Ethereum το 2014. Έκτοτε έχει γίνει η πιο δημοφιλής γλώσσα προγραμματισμού για την ανάπτυξη έξυπνων συμβολαίων στο δίκτυο Ethereum.

Μερικά από τα χαρακτηριστικά είναι:

- Προγραμματισμός Contract-oriented: η Solidity έχει σχεδιαστεί για να υποστηρίζει τη δημιουργία έξυπνων συμβολαίων που μπορούν να εκτελεστούν στο δίκτυο Ethereum.

- Ασφάλεια: η Solidity έχει σχεδιαστεί με γνώμονα την ασφάλεια και έχει ενσωματωμένα χαρακτηριστικά ασφαλείας για την πρόληψη κοινών σφαλμάτων προγραμματισμού που θα μπορούσαν να οδηγήσουν σε ευπάθειες.

- Στατική πληκτρολόγηση: η Solidity είναι μια στατικά πληκτρολογούμενη γλώσσα, που σημαίνει ότι οι τύποι μεταβλητών ελέγχονται κατά το χρόνο μεταγλώττισης, καθιστώντας πιο εύκολο τον εντοπισμό σφαλμάτων πριν την εκτέλεση.

- Προγραμματισμός βάσει συμβάντων: η Solidity υποστηρίζει προγραμματισμό με γνώμονα τα συμβάντα, το οποίο επιτρέπει στα συμβόλαια να αντιδρούν σε αλλαγές στην κατάσταση της αλυσίδας μπλοκ.

- Βιβλιοθήκες: η Solidity υποστηρίζει τη χρήση εξωτερικών βιβλιοθηκών, καθιστώντας πιο εύκολη την επαναχρησιμοποίηση του κώδικα και την αποφυγή αντιγραφής λειτουργιών.

Η Solidity είναι μια δημοφιλής γλώσσα μεταξύ των προγραμματιστών blockchain και εξελίσσεται συνεχώς για να καλύψει τις ανάγκες του οικοσυστήματος Ethereum. Υπάρχουν πολλοί διαθέσιμοι πόροι για την εκμάθηση του Solidity, συμπεριλαμβανομένων των διαδικτυακών σεμιναρίων, διάφορων εγγράφων και των κοινοτήτων προγραμματιστών.

Στο παράρτημα Α παρουσιάζεται ένα παράδειγμα έξυπνου συμβολαίου που μπορεί να χρησιμοποιηθεί για το σκοπό αυτής της διπλωματικής

Το συμβόλαιο Αισθητήρα Δεδομένων (SensorData contract) καθορίζει ένα struct που ονομάζεται Reading και περιλαμβάνει δύο τιμές uint για τη θερμοκρασία και την υγρασία. Ορίζει επίσης έναν χάρτη (mapping) που ονομάζεται readings και αντιστοιχεί τις διευθύνσεις Ethereum των συσκευών στα Reading structs. Τέλος, ορίζει μια συνάρτηση που ονομάζεται addReading, η οποία λαμβάνει δύο τιμές uint για τη θερμοκρασία και την υγρασία ως ορίσματα και τις αποθηκεύει στον χάρτη readings χρησιμοποιώντας τη διεύθυνση Ethereum της συσκευής ως κλειδί.

Μόλις οριστεί το smart contract, μπορούμε να χρησιμοποιήσουμε τη βιβλιοθήκη web3 στο περιβάλλον Arduino για να αλληλοεπιδράσει με το Ethereum blockchain και να εκτελεστεί η συνάρτηση addReading στο smart contract. Η βιβλιοθήκη web3 παρέχει έναν βολικό τρόπο για την αποστολή συναλλαγών στο blockchain χρησιμοποιώντας τη συνάρτηση eth_sendTransaction.

Στο παράρτημα Β παρουσιάζεται ένα παράδειγμα για το πως χρησιμοποιείται η βιβλιοθήκη web3 για να σταλθεί μια συναλλαγή στην συνάρτηση addReading στο SensorData συμβόλαιο

Η συνάρτηση eth_sendTransaction παίρνει ένα JSON αντικείμενο που καθορίζει τη διεύθυνση αποστολέα (from), τη διεύθυνση σύμβασης (to) και τα δεδομένα που θα αποσταλούν (data). Η συνάρτηση keccak256 χρησιμοποιείται για τον υπολογισμό της υπογραφής της συνάρτησης addReading, και οι τιμές θερμοκρασίας και υγρασίας κωδικοποιούνται ως δεκαεξαδικές συμβολοσειρές και συνενώνονται με την υπογραφή της συνάρτησης για να δημιουργηθούν τα ορίσματα δεδομένων για τη συναλλαγή.

Χρησιμοποιώντας μια συνδυασμένη προσέγγιση Solidity smart contracts και τη βιβλιοθήκη web3, μπορούμε να δημιουργήσουμε έναν απλό και αποτελεσματικό τρόπο για να αποθηκεύουμε και να διαχειριζόμαστε τα δεδομένα θερμοκρασίας και υγρασίας από συσκευές IoT στο δίκτυο του Ethereum blockchain.

Αυτό το κεφάλαιο περιγράφει τη μεθοδολογία που χρησιμοποιήθηκε στο έργο, εστιάζοντας στη ρύθμιση υλικού και λογισμικού καθώς και στις βασικές λειτουργίες που χρησιμοποιούνται στην υλοποίηση του κώδικα.

Η ρύθμιση υλικού περιλαμβάνει τη χρήση του μικροελεγκτή ESP32, που είναι γνωστός για τις δυνατότητες του IoT και τις εκτεταμένες επιλογές συνδεσιμότητας.

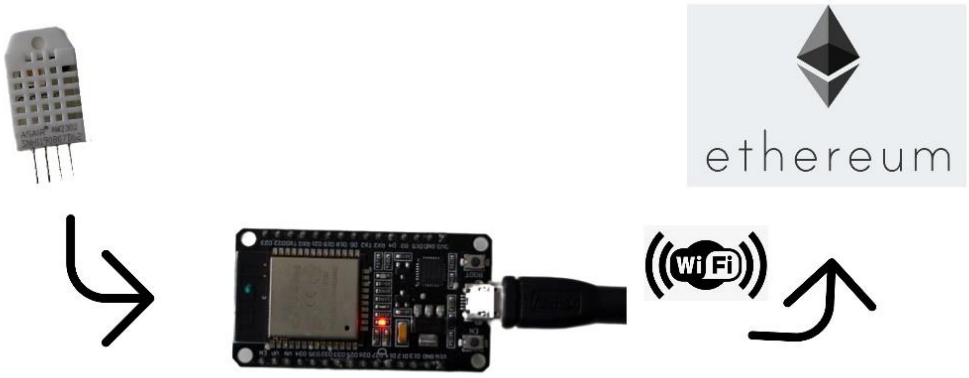
Ο κώδικας για το ESP32 σε περιβάλλον Arduino βρίσκεται στο Παράρτημα Γ.

Οι απαιτούμενες βιβλιοθήκες, συγκεκριμένα WiFi.h και Web3.h, εισάγονται για να ενεργοποιηθεί η λειτουργία Wi-Fi και Ethereum. Το SSID και ο κωδικός πρόσβασης, καθορίζονται για τη δημιουργία ασφαλούς σύνδεσης με το τοπικό δίκτυο Wi-Fi. Επιπλέον, η διεύθυνση URL του κόμβου Ethereum, η διεύθυνση του συμβολαίου και το ιδιωτικό κλειδί παρέχονται για σύνδεση στο δίκτυο Ethereum και αλληλεπίδραση με το αντίστοιχο έξυπνο συμβόλαιο. Το Web3 εγκαθίσταται και αρχικοποιείται με τη διεύθυνση URL του κόμβου Ethereum για διευκόλυνση της επικοινωνίας.

Η συνάρτηση εγκατάστασης (setup()) εκτελείται μία φορά στην αρχή του προγράμματος. Ξεκινά τη σειριακή επικοινωνία για να διευκολύνει τον εντοπισμό σφαλμάτων και την αλληλεπίδραση με τη σειριακή οθόνη. Το ESP32 δημιουργεί μια σύνδεση με το καθορισμένο δίκτυο Wi-Fi χρησιμοποιώντας τα παρεχόμενα διαπιστευτήρια, διασφαλίζοντας απρόσκοπτη συνδεσιμότητα δικτύου. Μόλις συνδεθεί, το αντικείμενο web3 διαμορφώνεται ώστε να συνδέεται με τον κόμβο Ethereum μέσω της συνάρτησης setProvider(). Επιπλέον, το ιδιωτικό κλειδί που σχετίζεται με τον λογαριασμό Ethereum εισάγεται χρησιμοποιώντας τη συνάρτηση personal.importPrivateKey(), επιτρέποντας την ασφαλή υπογραφή συναλλαγής.

Η συνάρτηση κύριου βρόχου (loop()) εκτελείται επανειλημμένα μετά τη συνάρτηση εγκατάστασης. Εντός του βρόχου, λαμβάνονται δεδομένα αισθητήρα, ειδικά μετρήσεις θερμοκρασίας και υγρασίας. Αν και σε αυτό το παράδειγμα οι τιμές είναι κωδικοποιημένες, σε πρακτικά σενάρια, θα αποκτώνται από πραγματικούς αισθητήρες. Η συνάρτηση web3.eth.sendTransaction() καλείται να στείλει μια συναλλαγή στο δίκτυο Ethereum και να αλληλεπιδράσει με το αναπτυγμένο έξυπνο συμβόλαιο. Συγκεκριμένα, καλείται η συνάρτηση addReading, περνώντας ως ορίσματα τις τιμές θερμοκρασίας και υγρασίας. Αυτό διασφαλίζει την αποθήκευση των αναγνώσεων αισθητήρων στο blockchain για παρακολούθηση και διαχείριση σε πραγματικό χρόνο. Μια καθυστέρηση καθορισμένης διάρκειας ενσωματώνεται μεταξύ των μετρήσεων χρησιμοποιώντας τη συνάρτηση delay(), που ρυθμίζει τη συχνότητα των ενημερώσεων δεδομένων αισθητήρα.

Ακολουθώντας αυτή τη μεθοδολογία, ο μικροελεγκτής ESP32 ρυθμίζεται αποτελεσματικά και ενσωματώνεται με τις απαραίτητες βιβλιοθήκες, επιτρέποντας αδιάλειπτη σύνδεση με το Wi-Fi και το δίκτυο Ethereum. Ο κύριος βρόχος εξασφαλίζει τη συνεχή απόκτηση και μετάδοση δεδομένων αισθητήρων στο έξυπνο συμβόλαιο Ethereum, διευκολύνοντας την αποκεντρωμένη και ασφαλή αποθήκευση.



Εικόνα 4.7: Σύνδεση του συστήματος με το Ethereum Blockchain μέσω WiFi

4.4 Πειραματική διάταξη

Η διαμόρφωση υλικού αποτελείται από τον μικροελεγκτή ESP32, που είναι γνωστός για τις δυνατότητές του σε εφαρμογές IoT, καθώς και από τον αισθητήρα DHT22 που χρησιμοποιείται για τη συλλογή δεδομένων. Το περιβάλλον λογισμικού περιλαμβάνει το ολοκληρωμένο περιβάλλον ανάπτυξης Arduino (IDE), που διευκολύνει τη λειτουργικότητα του Wi-Fi και του Ethereum. Επιπλέον, το έξυπνο συμβόλαιο αναπτύχθηκε στο δίκτυο Ethereum όμως η λειτουργικότητά του δεν επαληθεύτηκε για να διασφαλιστεί η ακριβής αποθήκευση και ανάκτηση δεδομένων.

4.5 Συμπέρασμα και μελλοντική εργασία

4.5.1 Περίληψη

Συμπερασματικά, η παρούσα διπλωματική εργασία παρουσίασε μια λύση για τη διασύνδεση του μικροελεγκτή ESP32 με ένα έξυπνο συμβόλαιο Ethereum για τη διαχείριση δεδομένων αισθητήρα. Οι ερευνητικοί στόχοι, που είχαν ως στόχο την ανάπτυξη ενός πρακτικού και αποτελεσματικού συστήματος για αποκεντρωμένη και ασφαλή αποθήκευση δεδομένων, έχουν επιτευχθεί με εξαίρεση τη μη επαλήθευση της λειτουργικότητας του έξυπνου συμβολαίου. Με την ενσωμάτωση του ESP32 με το δίκτυο Ethereum, τα δεδομένα του αισθητήρα θα μπορούσαν να μεταδοθούν και να αποθηκευτούν με ασφάλεια στο blockchain, διασφαλίζοντας αμεταβλητότητα και διαφάνεια.

4.5.2 Μελλοντική εργασία

Υπάρχουν αρκετοί δρόμοι για μελλοντική εργασία και βελτίωση. Μια πιθανή κατεύθυνση είναι να επεκταθούν οι δυνατότητες του συστήματος ενσωματώνοντας πρόσθετους τύπους αισθητήρων και ενσωματώνοντας προηγμένα χαρακτηριστικά όπως ανάλυση δεδομένων ή πολύπλοκες αλληλεπιδράσεις έξυπνων συμβολαίων. Αυτό θα επέτρεπε πιο εξελιγμένη επεξεργασία και ανάλυση δεδομένων απευθείας στο blockchain Ethereum.

Ένας άλλος τομέας για μελλοντική εξερεύνηση είναι η βελτιστοποίηση των πρωτοκόλλων μετάδοσης δεδομένων για τη βελτίωση της αποτελεσματικότητας και της επεκτασιμότητας του συστήματος. Η διερεύνηση τεχνικών για τη συμπίεση και την κρυπτογράφηση δεδομένων αισθητήρων κατά τη μετάδοση μπορεί να βελτιώσει τη χρήση του εύρους ζώνης και να ενισχύσει την ασφάλεια των δεδομένων. Επιπλέον, η αντιμετώπιση προκλήσεων επεκτασιμότητας, όπως η εξερεύνηση λύσεων για τη διαχείριση μεγάλου όγκου δεδομένων αισθητήρων στο blockchain, μπορεί να ενισχύσει περαιτέρω την εφαρμογή του συστήματος σε σενάρια πραγματικού κόσμου.

Επιπλέον, υπάρχει χώρος για έρευνα για τη βελτίωση της διεπαφής χρήστη και της προσβασιμότητας του συστήματος. Η ανάπτυξη ευανάγνωστων πινάκων ελέγχου ή εργαλείων οπτικοποίησης που επιτρέπουν στους χρήστες να παρακολουθούν και αναλύουν εύκολα τα δεδομένα αισθητήρων που αποθηκεύονται στο blockchain μπορεί να ενισχύσει τη χρηστικότητα και την πρακτικότητα της λύσης.

Τέλος, είναι απαραίτητο να διεξαχθούν περαιτέρω αξιολογήσεις απόδοσης και δοκιμές συγκριτικής αξιολόγησης για την αξιολόγηση των δυνατοτήτων του συστήματος κάτω από διαφορετικά σενάρια και φόρτους εργασίας. Αυτό θα βοηθήσει στον εντοπισμό πιθανών σημείων συμφόρησης και στη βελτιστοποίηση των παραμέτρων του συστήματος για βέλτιστη απόδοση.

Επιδιώκοντας αυτές τις οδούς για μελλοντικές εργασίες, η προτεινόμενη λύση μπορεί να βελτιωθεί και να επεκταθεί για να αντιμετωπίσει τις αναδυόμενες προκλήσεις και απαιτήσεις στον τομέα της διαχείρισης δεδομένων αισθητήρων. Ο πιθανός αντίκτυπος αυτής της έρευνας καλύπτει διάφορους τομείς, συμπεριλαμβανομένης της περιβαλλοντικής παρακολούθησης, των βιομηχανικών συστημάτων και των εφαρμογών IoT, όπου η ασφαλής και αποκεντρωμένη διαχείριση δεδομένων είναι ζωτικής σημασίας.

Βιβλιογραφία – Αναφορές - Διαδικτυακές Πηγές

1. Alharby, M., Moorsel, A. (2017). Blockchain Based Smart Contracts: A Systematic Mapping Study. Computer Science & Information Technology (CS & IT). doi: 10.5121/csit.2017.71011

2. Prusty, N. (2017). Building Blockchain projects. Packt Publishing Ltd

3. Bauerle, N. (2020). Blockchain 101 - CoinDesk. Accessed 20 February 2022, from https://www.coindesk.com/learn/what-is-a-distributed-ledger/

4. Bashir, I. (2018). MASTERING BLOCKCHAIN (2nd ed.). [Place of publication not identified]: PACKT Publishing

5. Iredale, G. (2020). History of Blockchain Technology: A detailed Guide. Accessed 12 February 2022, from https://101blockchains.com/history-of-blockchain-timeline/

6. Unknown author (n.d.). History of Blockchain. Accessed 12 February 2022, from https://www.javatpoint.com/history-of-blockchain

7. Yaga, D., Mell, P., Roby, N., Scarfone, K. (2018). Blockchain Technology Overview. Accessed 5 March 2022, from https://doi.org/10.6028/NIST.IR.8202

8. Stark, J. (2016). Making Sense of Blockchain Smart Contracts. Accessed 24 March 2022, from https://www.coindesk.com/markets/2016/06/04/making-sense-of-blockchain-smart-contracts/

9. Hertig, A. (2020). What is an Oracle? Accessed 2 April 2022, from https://www.coindesk.com/tech/2020/12/22/what-is-an-oracle/

10. Hertig, A. (2021). What is Ethereum? Accessed 9 April 2022, from https://www.coindesk.com/learn/what-is-ethereum/

11. Wu, K., Ma, Y., Huang, G., Liu, X. (2019). A first look at blockchain-based decentralized applications. Wiley online library, https://doi.org/10.1002/spe.2751

12. Reyna, A., Martin, C., Chen, J., Soler, E., Diaz, M., (2018). On blockchain and its integration with IoT. Challenges and opportunities. Accessed 8 May 2022, from https://doi.org/10.1016/j.future.2018.05.046

13. Lao, L., Li, Z., Hou, S., Xiao, B., Guo, S., Yang, Y. (2020). A survey of IoT applications in blockchain systems: Architecture, consensus and traffic modeling. Accessed 22 December 2022, from https://dl.acm.org/doi/abs/10.1145/3372136

14. Dorri, A., Kanhere, S., Jurdakk, R., Gauravaram, P. (2019). A lightweight scalable Blockchain for IoT security and anonymity. Accessed 22 December 2022, from https://www.sciencedirect.com/science/article/pii/S0743731518307688

15. Blockdata website. Proclaimed bio for Exergy token. Accessed 14 January 2023, from https://www.blockdata.tech/tokens/exergy

16. Sagirlar, G., Carminati, B., Ferrari, E., Sheehan, J.D., Ragnoli, E. (2018). Hybrid-IoT: Hybrid Blockchain Architecture for Internet of things – PoW Sub-Blockchains. Accessed 21 January 2023, from https://arxiv.org/abs/1804.03903

17. Bahga, A., Madisetti, V.K., (2016). Blockchain Platform for Industrial Internet of Things. Journal of Software Engineering and Applications, 9, 533- 546. Accessed 21 January 2023, from http://dx.doi.org/10.4236/jsea.2016.910036

18. JD. (2018) The JD. Accessed 21 January 2023, from https://ledger.jd.com/

19. Liu, B., Yu, X.L., Chen, S., Xu, X., Zhu, L. (2017). Blockchain based data integrity service framework for IoT data. Accessed 21 January 2023, from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8029796&tag=1

20. Alphand, O., Amoretti, M., Claeys, T., Dall'Asta, S., Duda, A., et al. (2018). IoTChain: A Blockchain Security Architecture for Internet of things. Accessed 26 January 2023, from https://hal.science/hal-01705455

21. Vučinić, M., Tourancheau, B., Rousseau, F., Duda, A., Damon, L., Guizzetti, R. (2015). OSCAR: Object Security Architecture for the Internet of Things. Accessed 26 January 2023, from https://www.sciencedirect.com/science/article/pii/S1570870514003126

22. Seitz, L., Selander, G., Wahlstroem, E., Erdtman, S., Tschofenig, H. (2017). Authentication and authorization for constrained environments (ACE). Accessed 26 January 2023, from https://datatracker.ietf.org/doc/rfc9200/

23. Geroni, D. (2020). What Is A Public Blockchain? Beginner's Guide. Accessed 18 July 2023, from https://101blockchains.com/public-blockchain/

24. Rishi, A. (2022). The Ultimate guide to Ethereum Blocks. Accessed 20 July 2023, from https://blog.cryptostars.is/the-ultimate-guide-to-ethereum-blocks-98da8e2c1697

25. Malviya, H., (2016). How Blockchain will Defend IOT. Accessed 8 May 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2883711

26. Khan M. A., Salah K., (2017). IoT security: Review, blockchain solutions, and open challenges. Accessed 8 May 2022, from https://www.sciencedirect.com/science/article/pii/S0167739X17315765

27. Prisco, G., (2015). Slock.It To introduce smart locks linked to smart ethereum contracts, decentralize the sharing economy. Accessed 8 May 2022, from https://bitcoinmagazine.com/technical/slock-it-to-introduce-smart-locks-linked-to-smart-ethereum-contracts-decentralize-the-sharing-economy-1446746719

28. Diaz, M., Martin, C., Rubio, B., (2016). State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. Accessed 8 May 2022, from https://www.sciencedirect.com/science/article/pii/S108480451600028X

29. Roman, R., Zhou, J., Lopez, J., (2013). On the features and challenges of security and privacy in distributed internet of things. Accessed 8 May 2022, from https://www.sciencedirect.com/science/article/pii/S1389128613000054

30. Chakraborty, B.(2022). Cryptographic primitives in blockchain. Accessed 20 July 2023, from https://www.analyticsvidhya.com/blog/2022/07/cryptographic-primitives-in-blockchain/

31. Buterin, V., (2013) Ethereum white paper. Accessed 8 May 2022, from https://github.com/ethereum/wiki/wiki/White-Paper

32. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C.,Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., et al. (2018). Hyperledger fabric: A distributed operating system for permissioned blockchains. Accessed 8 May 2022, from https://arxiv.org/abs/1801.10228

33. Litecoin Website. Accessed 8 May 2022, from https://litecoin.org/

34. Lisk website. Accessed 8 May 2022, from https://lisk.com/documentation/

35. Naidu, R., Irrera, A., (2017). Nestle, Unilever, Tyson and others team with IBM on blockchain. Accessed 8 May 2022, from https://www.reuters.com/article/us-ibm-retailers-blockchain/nestle-unilever-tyson-and-others-team-with-ibm-on-blockchain-idUSKCN1B21B1

36. Pradeep, (2017). Renault partners with Microsoft for blockchain-based digital car maintenance book. Accessed 8 May 2022, from https://mspoweruser.com/renault-partners-microsoft-blockchain-based-digital-car-maintenance-book/

Παράρτημα Α

```
pragma solidity ^0.8.0;

contract SensorData {

   struct Reading {

      uint temperature;

      uint humidity;

   }

   mapping(address => Reading) public readings;

   function addReading(uint _temperature, uint _humidity) public {

      readings[msg.sender] = Reading(_temperature, _humidity);

   }

}
```

Παράρτημα Β

```
String transactionHash = web3.eth_sendTransaction("{\"from\": \"0xYourAccountAddress\", \"to\": \"0xYourSmartContractAddress\", \"data\": \"0x" + String(keccak256("addReading(uint256,uint256)")).substring(0, 8) + String(temperature, HEX) + String(humidity, HEX) + "\"}");
```

Παράρτημα Γ

```
#include <WiFi.h>

#include <Web3.h>


#define DHTTYPE DHT22

uint8_t DHTPin = 4;

DHT dht(DHTPin, DHTTYPE);

float Temperature;

float Humidity;
```

```
// Replace with network credentials
const char* ssid = "Your_SSID";
const char* password = "Your_PASSWORD";

// Replace with Ethereum node information
const char* ethNodeURL = "http://your_ethereum_node_url:8545";
const char* contractAddress = "0x123456789abcdef";
const char* privateKey = "Your_PRIVATE_KEY";
Web3 web3(ethNodeURL);
void setup() {
  Serial.begin(115200);
  delay(1000)
  // Connect to Wi-Fi
  WiFi.begin(ssid, password);
  while (WiFi.status() != WL_CONNECTED) {
    delay(1000);
    Serial.println("Connecting to WiFi...");
  }
  Serial.println("Connected to WiFi");
  // Connect to Ethereum node
  web3.setProvider(ethNodeURL);
  // Import private key
  web3.personal.importPrivateKey(privateKey);
}
void loop() {
  // Read sensor data
  Temperature = dht.readTemperature();  // temperature reading
  Humidity = dht.readHumidity();     // humidity reading
  // Call the smart contract's addReading function
  web3.eth.sendTransaction(contractAddress, "addReading(uint256,uint256)", temperature,
humidity);
  delay(5000);  // Delay between readings
}
```