Πανεπιστήμιο Δυτικής Αττικής
Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών

Διπλωματική Εργασία

Αυθεντικοποίηση συσκευών IoT με χρήση έξυπνων συμβολαίων.

Χρήστος Τασατζής
(711161043)

Εισηγητής

Μπόγρης Αντώνιος,
Καθηγητής

Αθήνα-Αιγάλεω, 2023

Πανεπιστήμιο Δυτικής Αττικής, Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών

Χρήστος Τασατζής

University of West Attica
Faculty of Engineering
Department of Informatics and Computer Engineering

Diploma Thesis

IoT device authentication using smart contracts

Christos Tasatzis
(711161043)

Supervisor

Bogris Antonios,
Professor

Athens-Egaleo, 2023

University of West Attica, Department of Informatics and Computer Engineering

Christos Tasatzis

Διπλωματική Εργασία

Αυθεντικοποίηση συσκευών IoT με χρήση έξυπνων συμβολαίων.

Χρήστος Τασατζής
(711161043)

Εισηγητής:

Αντώνιος Μπόγρης, Καθηγητής

Antonios Bogris
Digitally signed by Antonios Bogris
Date: 2023.07.26 07:26:58 +02'00'

Εξεταστική Επιτροπή:

Ιωάννα Καντζάβελου, Επίκουρη Καθηγήτρια

Ioanna Kantzavelou
Digitally signed by Ioanna Kantzavelou
Date: 2023.07.26 12:04:22 +03'00'

Παναγιώτης Καρκαζής, Αναπληρωτής Καθηγητής

Panagiotis Karkazis
Digitally signed by Panagiotis Karkazis
Date: 2023.07.26 10:12:05 +03'00'

Ημερομηνία εξέτασης 10/7/2023

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Χρήστος Τασατζής του Ελευθερίου, με αριθμό μητρώου 711160143 φοιτητής του Προγράμματος Προπτυχιακών Σπουδών του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Είμαι συγγραφέας αυτής της προπτυχιακής 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 πτυχίου μου».

Ο δηλών,

Χρήστος Τασατζής

ΕΥΧΑΡΙΣΤΊΕΣ

Η παρούσα διπλωματική εργασία ολοκληρώθηκε μετά από επίμονες προσπάθειες, σε ένα ενδιαφέρον γνωστικό αντικείμενο, όπως αυτό της τεχνολογίας του Blockchain. Την προσπάθειά μου αυτή υποστήριξε ο επιβλέπων καθηγητής μου, τον οποίο θα ήθελα να ευχαριστήσω.

Ακόμα θα ήθελα να ευχαριστήσω την οικογένειά μου για τη συμπαράσταση κατά τη διάρκεια των σπουδών μου.

Περίληψη

Η ταχεία εξάπλωση των συσκευών του Internet of Things (IoT) έχει δημιουργήσει πολυάριθμες ευκαιρίες για καινοτομία και ευκολία. Ωστόσο, τα εγγενή τρωτά σημεία των οικοσυστημάτων IoT δημιουργούν σημαντικές προκλήσεις, ιδίως στον τομέα της αυθεντικοποίησης και της ασφάλειας των δεδομένων. Η παρούσα εργασία διερευνά τις δυνατότητες των έξυπνων συμβολαίων, που τροφοδοτούνται από την τεχνολογία του blockchain, ως μέσο για την αυθεντικοποίηση και την επικοινωνία μεταξύ των συσκευών IoT. Οι παραδοσιακοί μηχανισμοί αυθεντικοποίησης δυσκολεύονται να αντιμετωπίσουν τις μοναδικές απαιτήσεις των περιβαλλόντων IoT. Η δυναμική και αποκεντρωμένη φύση των δικτύων IoT απαιτεί μια λύση αυθεντικοποίησης που να είναι ασφαλής, διαφανής και ικανή να χειριστεί την κλίμακα και την πολυπλοκότητα των διασυνδεδεμένων συσκευών. Τα έξυπνα συμβόλαια προσφέρουν μια συναρπαστική προσέγγιση για την αντιμετώπιση αυτών των προκλήσεων, αξιοποιώντας τις βασικές αρχές του blockchain, δηλαδή την αμεταβλητότητα, την αποκέντρωση και τη διαφάνεια.

Η παρούσα εργασία διερευνά τα θεωρητικά θεμέλια της αυθεντικοποίησης του IoT και τις θεμελιώδεις έννοιες των έξυπνων συμβολαίων. Αναλύει τους υφιστάμενους μηχανισμούς ελέγχου ταυτότητας, επισημαίνοντας τους περιορισμούς και τις ευπάθειές τους στο πλαίσιο των συστημάτων IoT. Εισάγοντας τις έξυπνες συμβάσεις ως ασφαλές μέσο επικοινωνίας, η εργασία αυτή προτείνει ένα νέο πλαίσιο για την επίτευξη ισχυρής αυθεντικοποίησης και ακεραιότητας δεδομένων σε οικοσυστήματα IoT. Μέσω της έρευνας και ανάλυσης, η παρούσα εργασία έχει ως στόχο να συμβάλει στον αυξανόμενο όγκο γνώσεων στον τομέα των συστημάτων IoT με δυνατότητές αξιοποίησης του blockchain, καταδεικνύοντας τις δυνατότητες των έξυπνων συμβολαίων για την αυθεντικοποίηση, την ακεραιότητα των δεδομένων και την αποκεντρωμένη επικοινωνία. Ταυτόχρονα παρουσιάζει τις προκλήσεις που θα πρέπει να ερευνηθούν περαιτέρω στο μέλλον.

Λέξεις Κλειδιά

Internet of Things, Blockchain, Έξυπνα Συμβόλαια, Κρυπτογραφία

Abstract

The rapid growth of Internet of Things (IoT) devices has created numerous opportunities for innovation and convenience. However, the inherent vulnerabilities of IoT ecosystems create significant challenges, particularly in the area of authentication and data security. This thesis explores the potential of smart contracts, powered by blockchain technology, as a means for authentication and communication between IoT devices. Traditional authentication mechanisms struggle to address the unique requirements of IoT environments. The dynamic and decentralized nature of IoT networks requires an authentication solution that is secure, transparent, and capable of handling the scale and complexity of interconnected devices. Smart contracts offer a compelling approach to address these challenges by leveraging the core principles of blockchain, namely immutability, decentralization and transparency.

This thesis explores the theoretical foundations of IoT authentication and the fundamental concepts of smart contracts. It analyses existing authentication mechanisms, highlighting their limitations and vulnerabilities in the context of IoT systems. By introducing smart contracts as a secure communication medium, the thesis proposes a new framework for achieving strong authentication and data integrity in IoT ecosystems. Through research and analysis, this thesis aims to contribute to the growing body of knowledge in the field of blockchain-enabled IoT systems. By demonstrating the potential of smart contracts for authentication, data integrity and decentralized communication. At the same time, it presents challenges that will need to be further researched in the future.

Keywords

Internet of Things, Blockchain, Smart Contracts, Cryptography

Πίνακας Περιεχομένων

Κατάλογος Πινάκων

Κατάλογος Σχημάτων

Κατάλογος Συντομογραφιών

AES	Advanced Encryption Standard
RSA	Rivest Shamir Adleman
ECC	Elliptic Curve Cryptography
CA	Certificate Authority – Αρχή Πιστοποιητικών
RA	Reservation Authority – Αρχή Κρατήσεων
IoT	Internet of Things – Διαδίκτυο των Αντικειμένων
RFID	Radio-frequency Identification – Ταυτοποίηση Ραδιοσυχνοτήτων
IaaS	Infrastructure as a Service (Υποδομή ως υπηρεσία)
PaaS	Platform as a Service (Πλατφόρμα ως υπηρεσία)
SaaS	Software as a Service (Λογισμικό ως υπηρεσία)
PoW	Proof of Work
PoS	Proof of Stake
DPoS	Delegated Proof of Stake
ABI	Application Binary Interface

ΣΚ	Συμμετρική Κρυπτογράφηση
ΑΚ	Ασύμμετρη Κρυπτογράφηση
ΓΨΑ	Γεννήτρια Ψευδοτυχαίων Αριθμών
ΓΤΑ	Γεννήτρια Τυχαίων Αριθμών
ΚΣΚ	Κρυπτογραφική Συνάρτηση Κατακερματισμού – Hash Functions
ΕΣ	Έξυπνο Συμβόλαιο

Κεφάλαιο 1: Εισαγωγή

1.1 Πρόλογος

Σε μια εποχή που χαρακτηρίζεται από τη ραγδαία εξέλιξη της τεχνολογίας, το **Internet of Things** (IoT) έχει αναδειχθεί ως μια επαναστατική έννοια, η οποία επιτρέπει την ομαλή ενσωμάτωση φυσικών συσκευών στον διασυνδεδεμένο ψηφιακό κόσμο. Καθώς ο αριθμός των συσκευών IoT συνεχίζει να πολλαπλασιάζεται, η ανάγκη για ισχυρούς και ασφαλείς μηχανισμούς αυθεντικοποίησης γίνεται όλο και πιο σημαντική. Οι παραδοσιακές μέθοδοι αυθεντικοποίησης είναι συχνά ανεπαρκείς για την αντιμετώπιση των μοναδικών προκλήσεων που θέτει η δυναμική και αποκεντρωμένη φύση των οικοσυστημάτων IoT.

Η έλευση της τεχνολογίας **blockchain**, ιδίως η έννοια των **έξυπνων συμβολαίων** (ΕΣ), προσφέρει μια πολλά υποσχόμενη λύση για την αντιμετώπιση των προβλημάτων αυθεντικοποίησης που ταλανίζουν το τοπίο του IoT. Τα ΕΣ, που εκτελούνται σε κατανεμημένα και αμετάβλητα δίκτυα blockchain, παρέχουν ένα ασφαλές και διαφανές μέσο επικοινωνίας μεταξύ των συσκευών IoT. Αξιοποιώντας τα εγγενή χαρακτηριστικά του blockchain, όπως η αμεταβλητότητα, η αποκέντρωση και η διαφάνεια, τα ΕΣ προσφέρουν μια νέα προσέγγιση για την επίτευξη αυθεντικοποίησης δεδομένων σε συστήματα IoT.

1.2 Στόχος εργασίας

Ο πρωταρχικός στόχος της παρούσας εργασίας είναι να διερευνήσει τις δυνατότητες των ΕΣ ως μέσο για την αυθεντικοποίηση και την επικοινωνία σε δίκτυα IoT. Αξιοποιώντας τη δύναμη της τεχνολογίας **blockchain**, επιδιώκεται η ενίσχυση της ασφάλειας, της αξιοπιστίας και της διαφάνειας των οικοσυστημάτων IoT. Η παρούσα εργασία προτείνει μια λύση που αξιοποιεί τα ΕΣ για την επίτευξη της ασφαλούς και αποτελεσματικής επικοινωνίας μεταξύ συσκευών IoT, διασφαλίζοντας ταυτόχρονα την ακεραιότητα και την αυθεντικοποίηση των δεδομένων.

1.3 Διάρθρωση κεφαλαίων

Τα επόμενα κεφάλαια θα εμβαθύνουν στα θεωρητικά θεμέλια της αυθεντικοποίησης του IoT, στις θεμελιώδεις έννοιες της **κρυπτογραφίας**, του **IoT** και των ΕΣ καθώς και στη δυνατότητα εφαρμογής τους στα συστήματα IoT. Θα εξεταστούν οι υπάρχοντες μηχανισμοί ελέγχου **αυθεντικοποίησης** και οι περιορισμοί τους, ανοίγοντας το δρόμο για την εισαγωγή των έξυπνων συμβολαίων ως βιώσιμης εναλλακτικής λύσης. Επιπλέον, η παρούσα εργασία θα παρουσιάσει μια υλοποιημένη λύση για το πρόβλημα της αυθεντικοποίησης IoT συσκευών με τη χρήση έξυπνων συμβολαίων. Τέλος θα αναλύσει τα δυνητικά **οφέλη** και τις **προκλήσεις** που συνδέονται με την υιοθέτηση έξυπνων συμβολαίων για την αυθεντικοποίηση του IoT.

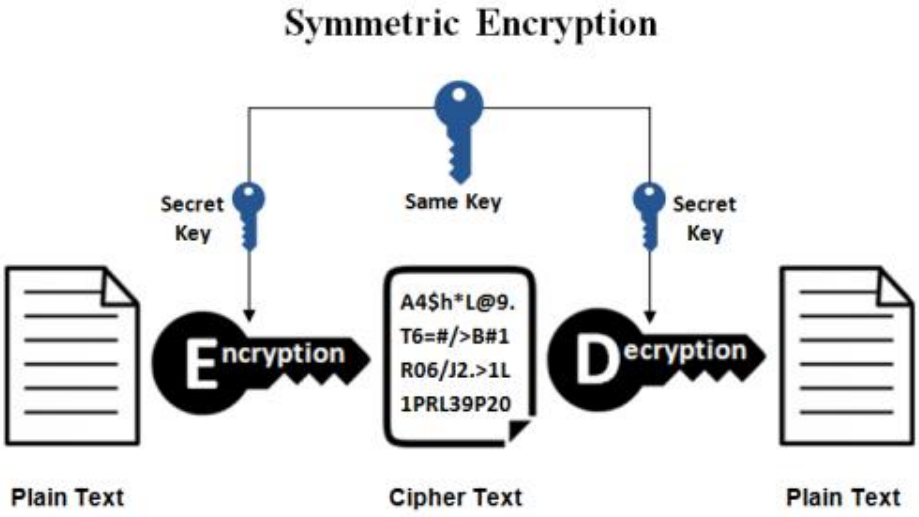
Κεφάλαιο 2: Κρυπτογραφία

2.1 Εισαγωγή

Η **κρυπτογραφία** συμβάλλει σημαντικά στη διασφάλιση της **εμπιστευτικότητας**, της **ακεραιότητας** και της **αυθεντικότητας** των δεδομένων που ανταλλάσσονται μεταξύ συσκευών και συστημάτων IoT. Στο πλαίσιο του IoT, όπου ένας τεράστιος αριθμός διασυνδεδεμένων συσκευών λειτουργεί σε ποικίλα και δυναμικά περιβάλλοντα, η χρήση της κρυπτογραφίας είναι απαραίτητη για την εξασφάλιση της ασφάλειας αυτών των συσκευών που συχνά έχουν περιορισμένους πόρους. Σε αυτό το κεφάλαιο, θα δοθεί μια επισκόπηση των διαφόρων κρυπτογραφικών αλγορίθμων που μπορούν να χρησιμοποιηθούν για την αυθεντικοποίηση συσκευών IoT, συμπεριλαμβανομένων των **συμμετρικών** και **ασύμμετρων** αλγορίθμων, καθώς και των **κρυπτογραφικών συναρτήσεων κατακερματισμού**. Επιπλέον, θα συζητηθεί η σημασία των πρακτικών διαχείρισης κλειδιών και των εκτιμήσεων ασφαλείας για τη διασφάλιση της αποτελεσματικότητας των κρυπτογραφικών μηχανισμών σε περιβάλλοντα IoT. Μέχρι το τέλος αυτού του κεφαλαίου, θα έχει αποκτηθεί καλύτερη κατανόηση των θεμελιωδών εννοιών της κρυπτογραφίας και του τρόπου με τον οποίο μπορούν να χρησιμοποιηθούν για την ασφάλεια συσκευών και συστημάτων IoT, επιτρέποντας τη λήψη τεκμηριωμένων αποφάσεων σχετικά με την επιλογή κατάλληλων κρυπτογραφικών μηχανισμών για εφαρμογές IoT.

2.2 Συμμετρική κρυπτογράφηση

Η **ΣΚ** είναι ένας τύπος κρυπτογράφησης στον οποίο το ίδιο κλειδί χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των δεδομένων. Αναφέρεται επίσης ως κρυπτογράφηση με κοινό μυστικό (shared secret cryptography), δεδομένου ότι τόσο ο αποστολέας όσο και ο παραλήπτης μοιράζονται το **ίδιο κλειδί**. Σε αυτή την ενότητα θα συζητηθούν οι βασικές αρχές της συμμετρικής κρυπτογράφησης, τους τύπους συμμετρικών αλγορίθμων, καθώς και τα πλεονεκτήματα και τους περιορισμούς τους στην αυθεντικοποίηση συσκευών IoT.



Εικόνα 1 Ροή Συμμετρικής Κρυπτογράφησης

2.2.1 Ορισμός

Η ΣΚ είναι ένας τύπος κρυπτογράφησης που χρησιμοποιεί ένα μόνο μυστικό κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση δεδομένων. Αυτό σημαίνει ότι το ίδιο κλειδί χρησιμοποιείται τόσο από τον αποστολέα όσο και από τον παραλήπτη, και πρέπει και οι δύο να γνωρίζουν και να χρησιμοποιούν το ίδιο κλειδί για να επικοινωνούν με ασφάλεια [1]. Κατά τη διαδικασία αυτή, το απλό κείμενο μετατρέπεται σε κρυπτογραφημένο κείμενο χρησιμοποιώντας έναν αλγόριθμο, το οποίο μπορεί να αποκρυπτογραφηθεί πίσω στο αρχικό απλό κείμενο μόνο με το ίδιο μυστικό κλειδί.

2.2.2 Τύποι συμμετρικών αλγορίθμων

Οι συμμετρικοί κρυπτογραφικοί αλγόριθμοι χωρίζονται σε δύο βασικές κατηγορίες, στους κρυπτογράφους μπλοκ και στους κρυπτογράφους ροής.

2.2.2.1 Κρυπτογράφοι μπλοκ

Οι **κρυπτογράφοι μπλοκ** είναι αλγόριθμοι συμμετρικής κρυπτογράφησης που διαιρούν το απλό κείμενο σε μπλοκ **σταθερού μεγέθους** και κρυπτογραφούν κάθε μπλοκ ξεχωριστά χρησιμοποιώντας το ίδιο κλειδί. Ο πιο ευρέως χρησιμοποιούμενος κρυπτογράφος μπλοκ είναι το AES, ο οποίος είναι ένας κρυπτογράφος μπλοκ 128 bit με μεγέθη κλειδιού 128, 192 ή 256 bit [1].

2.2.2.2 Κρυπτογράφοι ροής

Οι **κρυπτογράφοι ροής** είναι αλγόριθμοι συμμετρικής κρυπτογράφησης που κρυπτογραφούν το απλό κείμενο **ένα bit ή byte κάθε φορά**, παράγοντας μια ροή κρυπτογραφήματος. Οι πιο διαδεδομένοι κρυπτογράφοι ροής παράγουν το κρυπτογράφημα είτε χρησιμοποιώντας τα τελευταία n bit της ακολουθίας των δεδομένων, είτε χρησιμοποιώντας μια κοινή συνάρτηση κατά την κρυπτογράφηση και την αποκρυπτογράφηση [1]. Ο πιο ευρέως χρησιμοποιούμενος κρυπτογράφος ροής είναι ο αλγόριθμος RC4, ο οποίος είναι δημοφιλής στις ασύρματες επικοινωνίες και στις συσκευές IoT λόγω της απλότητας και της αποτελεσματικότητάς του.

2.2.3 Πλεονεκτήματα/μειονεκτήματα

Ένα πλεονέκτημα της συμμετρικής κρυπτογραφίας είναι η ταχύτητα και η αποτελεσματικότητά της, γεγονός που την καθιστά κατάλληλη για συσκευές IoT με περιορισμένους πόρους. Οι λειτουργίες κρυπτογράφησης και αποκρυπτογράφησης είναι **υπολογιστικά απλές** και τα κλειδιά είναι μικρότερα σε σύγκριση με εκείνα που χρησιμοποιούνται στην ασύμμετρη κρυπτογραφία. Ωστόσο, το κύριο μειονέκτημα της συμμετρικής κρυπτογραφίας είναι η **ανάγκη για ασφαλή διανομή κλειδιών**, καθώς το ίδιο κλειδί χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Οποιαδήποτε παραβίαση του κλειδιού θα μπορούσε να οδηγήσει σε παραβίαση όλων των κρυπτογραφημένων δεδομένων, καθιστώντας τη διαχείριση του κλειδιού μια κρίσιμη πτυχή της συμμετρικής κρυπτογραφίας [2].

2.2.4 Δημιουργία και διανομή συμμετρικού κλειδιού

Τα συμμετρικά κλειδιά μπορούν να παραχθούν με χρήση **γεννήτριας ψευδοτυχαίων αριθμών (ΓΨΑ)** ή με χρήση **γεννήτριας τυχαίων αριθμών (ΓΤΑ)** που βασίζεται σε υλικό. Η διανομή κλειδιών είναι μια κρίσιμη πτυχή της συμμετρικής κρυπτογραφίας και υπάρχουν διάφορες μέθοδοι για την ασφαλή

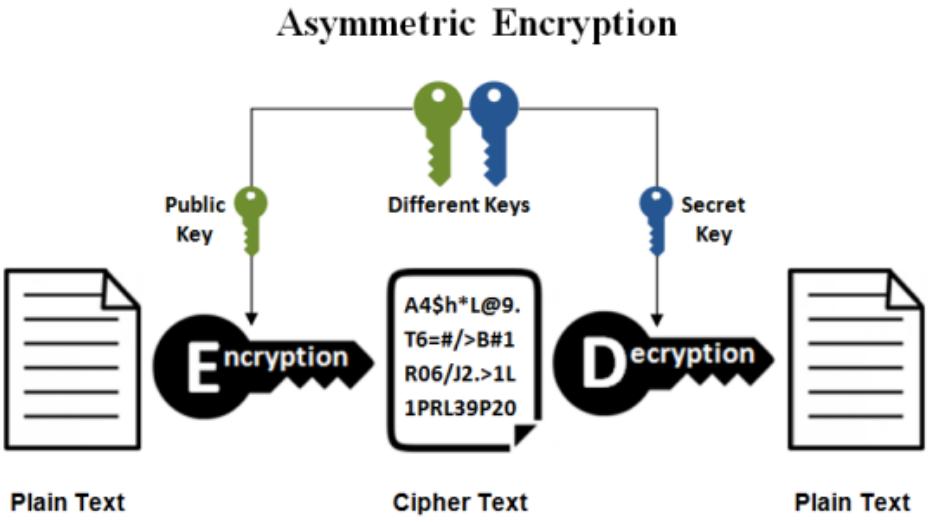
διανομή κλειδιών, όπως τα πρωτόκολλα ανταλλαγής κλειδιών και η διανομή κλειδιών από έμπιστους τρίτους.

2.2.5 Παραδείγματα χρήσης στην αυθεντικοποίηση συσκευών IoT

Αρκετοί συμμετρικοί αλγόριθμοι χρησιμοποιούνται στην αυθεντικοποίηση συσκευών IoT, όπως οι AES, RC4 και Blowfish. Αυτοί οι αλγόριθμοι παρέχουν εμπιστευτικότητα, ακεραιότητα και αυθεντικότητα των δεδομένων που μεταδίδονται μεταξύ συσκευών IoT.

2.3 Ασύμμετρη κρυπτογράφηση

Η **ΑΚ**, επίσης γνωστή ως κρυπτογράφηση δημόσιου κλειδιού, είναι ένας τύπος κρυπτογράφησης που χρησιμοποιεί ένα **ζεύγος κλειδιών** - ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί - για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων. Σε αυτή την ενότητα, θα αναλυθούν οι βασικές αρχές της ασύμμετρης κρυπτογραφίας, τους τύπους ασύμμετρων αλγορίθμων, καθώς και τα πλεονεκτήματα και τους περιορισμούς τους στην αυθεντικοποίηση συσκευών IoT.



Εικόνα 2 Ροή Ασύμμετρης Κρυπτογράφησης

2.3.1 Ορισμός

Η **ΑΚ** χρησιμοποιεί δύο διαφορετικά κλειδιά - ένα **δημόσιο κλειδί** και ένα **ιδιωτικό κλειδί** - για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων. Το δημόσιο κλειδί είναι ελεύθερα διαθέσιμο σε οποιονδήποτε, ενώ το ιδιωτικό κλειδί παραμένει μυστικό. Τα δεδομένα που κρυπτογραφούνται με το δημόσιο κλειδί μπορούν να αποκρυπτογραφηθούν μόνο με το αντίστοιχο ιδιωτικό κλειδί και το αντίστροφο 71[1]. Οι πιο ευρέως χρησιμοποιούμενοι ασύμμετροι αλγόριθμοι είναι ο RSA, ο Diffie-Hellman και η ECC.

2.3.2 Τύποι ασύμμετρων αλγορίθμων

Σε αυτό το κεφάλαιο θα αναλυθούν οι δημοφιλέστεροι αλγόριθμοι ασύμμετρης κρυπτογράφησης. Συγκεκριμένα θα αναλυθούν οι **RSA**, **Diffie-Hellman** και **ECC**.

2.3.2.1 RSA

Ο **RSA** είναι ένας ευρέως χρησιμοποιούμενος ασύμμετρος αλγόριθμος που χρησιμοποιεί έναν μεγάλο πρώτο αριθμό για τη δημιουργία του δημόσιου και του ιδιωτικού κλειδιού. Το δημόσιο κλειδί προκύπτει από το **γινόμενο δύο μεγάλων πρώτων αριθμών**, ενώ το ιδιωτικό κλειδί προκύπτει από τους **πρώτους παράγοντες** του δημόσιου κλειδιού. Ο RSA χρησιμοποιείται ευρέως σε ψηφιακές υπογραφές και πρωτόκολλα ανταλλαγής κλειδιών.

2.3.2.2 Diffie-Hellman

Ο **Diffie-Hellman** είναι ένας ασύμμετρος αλγόριθμος που χρησιμοποιείται για πρωτόκολλα ανταλλαγής κλειδιών. Επιτρέπει σε δύο μέρη να ανταλλάσσουν με ασφάλεια ένα κοινό μυστικό κλειδί χωρίς την ανάγκη ενός έμπιστου τρίτου μέρους. Ο αλγόριθμος χρησιμοποιεί **αριθμητική υπολοίπων** για τη δημιουργία ενός κοινού μυστικού κλειδιού που είναι γνωστό μόνο στα δύο εμπλεκόμενα μέρη.

2.3.2.3 Κρυπτογραφία ελλειπτικής καμπύλης (ECC)

Η **ECC** είναι ένας τύπος ασύμμετρου αλγορίθμου που χρησιμοποιεί τα μαθηματικά των **ελλειπτικών καμπυλών** για τη δημιουργία του δημόσιου και του ιδιωτικού κλειδιού. Χρησιμοποιείται ευρέως σε συσκευές IoT λόγω του υψηλού επιπέδου ασφάλειας και της αποτελεσματικότητάς του, καθιστώντας τον κατάλληλο για συσκευές με περιορισμένους πόρους.

2.3.3 Πλεονεκτήματα/μειονεκτήματα

Το κύριο πλεονέκτημα της ασύμμετρης κρυπτογραφίας είναι η δυνατότητα ασφαλούς ανταλλαγής κλειδιών **χωρίς** την ανάγκη ενός **αξιόπιστου τρίτου μέρους**. Παρέχει επίσης καλύτερη ασφάλεια σε σύγκριση με τη συμμετρική κρυπτογραφία, καθώς το ιδιωτικό κλειδί δεν μοιράζεται και το δημόσιο κλειδί μπορεί να διανεμηθεί ελεύθερα. Ωστόσο, το κύριο μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η υπολογιστική της **πολυπλοκότητα**, γεγονός που την καθιστά λιγότερο κατάλληλη για συσκευές με περιορισμένους πόρους [2].

2.3.4 Δημιουργία και διανομή κλειδιών

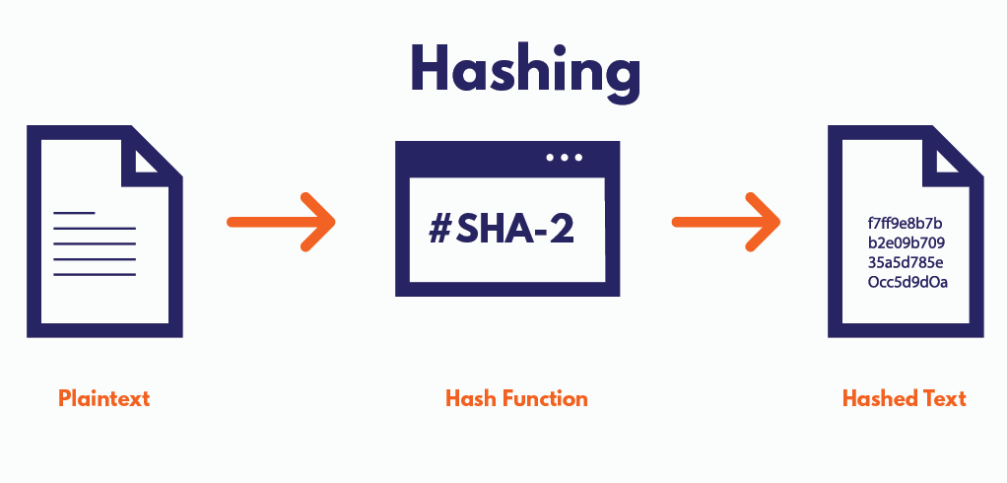
Τα ασύμμετρα κλειδιά παράγονται με χρήση ΓΤΑ και το ιδιωτικό κλειδί παραμένει μυστικό, ενώ το δημόσιο κλειδί είναι ελεύθερα διαθέσιμο. Τα δημόσια κλειδιά διανέμονται με τη χρήση ψηφιακών πιστοποιητικών, τα οποία υπογράφονται από ένα αξιόπιστο τρίτο μέρος, γνωστό ως Αρχή Πιστοποιητικών (CA).

2.3.5 Παραδείγματα χρήσης στην αυθεντικοποίηση συσκευών IoT

Στην αυθεντικοποίηση συσκευών IoT χρησιμοποιούνται διάφοροι ασύμμετροι αλγόριθμοι, όπως οι RSA, Diffie-Hellman και ECC. Αυτοί οι αλγόριθμοι παρέχουν εμπιστευτικότητα, ακεραιότητα και αυθεντικότητα των δεδομένων που μεταδίδονται μεταξύ των συσκευών IoT.

2.4 Κρυπτογραφικές συναρτήσεις κατακερματισμού

Οι **κρυπτογραφικές συναρτήσεις κατακερματισμού (ΚΣΚ)** αποτελούν βασικό συστατικό της σύγχρονης κρυπτογραφίας που χρησιμοποιείται στην αυθεντικοποίηση συσκευών IoT και στην τεχνολογία **blockchain**. Σε αυτή την ενότητα θα συζητηθούν οι βασικές αρχές των ΚΣΚ, οι ιδιότητές τους και οι εφαρμογές τους στην αυθεντικοποίηση συσκευών IoT.



Εικόνα 3 Ροή χρήσης κρυπτογραφικών συναρτήσεων κατακερματισμού

2.4.1 Ορισμός

Μια ΚΣΚ είναι ένας μαθηματικός αλγόριθμος που λαμβάνει δεδομένα **εισόδου αυθαίρετου μεγέθους** και παράγει μια **έξοδο σταθερού μεγέθους**, γνωστή ως κατακερματισμός ή χώνεψη μηνύματος. Η έξοδος είναι μοναδική σε σχέση με τα δεδομένα εισόδου, πράγμα που σημαίνει ότι ακόμη και μια μικρή αλλαγή στα δεδομένα εισόδου θα οδηγήσει σε μια εντελώς διαφορετική τιμή κατακερματισμού [3]. Οι ΚΣΚ έχουν σχεδιαστεί για να είναι **μονόδρομες** συναρτήσεις, πράγμα που σημαίνει ότι είναι υπολογιστικά ανέφικτο να εξαχθούν τα αρχικά δεδομένα εισόδου από την τιμή κατακερματισμού.

2.4.2 Ιδιότητες

Οι κρυπτογραφικές συναρτήσεις κατακερματισμού διαθέτουν αρκετές σημαντικές ιδιότητες [3], μεταξύ των οποίων:

- **Αντοχή σε συγκρούσεις**: Είναι υπολογιστικά ανέφικτο να βρεθούν δύο διαφορετικές τιμές εισόδου που παράγουν την ίδια τιμή κατακερματισμού.
- **Αντίσταση στην προαντίληψη**: Δεδομένης μιας τιμής κατακερματισμού, είναι υπολογιστικά ανέφικτο να βρεθεί οποιαδήποτε τιμή εισόδου που παράγει την ίδια τιμή κατακερματισμού.
- **Αντίσταση στην προαντίληψη (2)**: Δεδομένης μιας τιμής εισόδου, είναι υπολογιστικά ανέφικτο να βρεθεί μια άλλη τιμή εισόδου που παράγει την ίδια τιμή κατακερματισμού.
- **Ντετερμινισμός**: Η ίδια τιμή εισόδου παράγει πάντα την ίδια τιμή κατακερματισμού.
- **Μη αντιστρεψιμότητα**: Είναι υπολογιστικά ανέφικτο να προκύψουν τα αρχικά δεδομένα εισόδου από την τιμή κατακερματισμού.

2.4.3 Παραδείγματα χρήσης στην αυθεντικοποίηση συσκευών IoT

Οι ΚΣΚ χρησιμοποιούνται ευρέως στην αυθεντικοποίηση συσκευών IoT για τη διασφάλιση της ακεραιότητας των δεδομένων που μεταδίδονται μεταξύ συσκευών. Οι τιμές κατακερματισμού μπορούν να χρησιμοποιηθούν για την ανίχνευση τυχόν μη εξουσιοδοτημένων αλλαγών στα δεδομένα, όπως παραποίηση ή αλλοίωση.

2.4.4 Χρήση στην τεχνολογία blockchain

Οι ΚΣΚ αποτελούν κρίσιμο στοιχείο της τεχνολογίας **blockchain**, όπου χρησιμοποιούνται για τη δημιουργία των ασφαλών συνδέσμων μεταξύ των μπλοκ σε μια αλυσίδα μπλοκ. Ο κατακερματισμός κάθε μπλοκ περιλαμβάνεται στο επόμενο μπλοκ, σχηματίζοντας μια αλυσίδα μπλοκ που είναι ανθεκτική στην παραποίηση ή την τροποποίηση. Η χρήση ΚΣΚ εξασφαλίζει την ακεραιότητα και την αμεταβλητότητα της αλυσίδας μπλοκ.

2.5 Διαχείριση κλειδιών

Η διαχείριση κλειδιών αναφέρεται στις διεργασίες και τις διαδικασίες που χρησιμοποιούνται για τη διαχείριση των κρυπτογραφικών κλειδιών που χρησιμοποιούνται από τους εκάστοτε κρυπτογραφικούς αλγορίθμους. Περιλαμβάνει τη δημιουργία, τη διανομή, την αποθήκευση και την ανάκληση κλειδιών. Η αποτελεσματική διαχείριση κλειδιών είναι ζωτικής σημασίας για τη διασφάλιση της ασφάλειας, της ακεραιότητας και της αυθεντικοποίησης.

2.5.1 Βέλτιστες πρακτικές

Η αποτελεσματική διαχείριση κλειδιών απαιτεί την τήρηση βέλτιστων πρακτικών, όπως:

- **Παραγωγή κλειδιών**: Θα πρέπει να δημιουργούνται κλειδιά με τη χρήση ασφαλούς ΓΤΑ.
- **Διανομή κλειδιών**: Τα κλειδιά πρέπει να διανέμονται με ασφάλεια χρησιμοποιώντας έναν αξιόπιστο μηχανισμό διανομής.
- **Αποθήκευση κλειδιών**: Τα κλειδιά πρέπει να αποθηκεύονται με ασφάλεια, χρησιμοποιώντας κατάλληλους μηχανισμούς κρυπτογράφησης και ελέγχου πρόσβασης.
- **Ανάκληση κλειδιών**: Τα κλειδιά θα πρέπει να ανακαλούνται αμέσως εάν παραβιάζονται ή δεν χρειάζονται πλέον.
- **Εναλλαγή κλειδιών**: Τα κλειδιά πρέπει να εναλλάσσονται περιοδικά για να διασφαλίζεται η ασφάλεια και η ακεραιότητά τους.

2.6 Παραβίαση κρυπτογραφικών συστημάτων

Η μελέτη της παραβίασης κρυπτογραφικών συστημάτων αποκαλείται **κρυπτανάλυση**. Περιλαμβάνει την ανάλυση της ασφάλειας των κρυπτογραφικών συστημάτων και την ανάπτυξη τεχνικών για την παραβίασή τους. Η κρυπτανάλυση αποτελεί ένα σημαντικό εργαλείο για την εύρεση πιθανών αδυναμιών στους κρυπτογραφικούς αλγόριθμους. Η κρυπτανάλυση είναι επίσης πολύ σημαντική για την επιλογή του κατάλληλου κρυπτογραφικού αλγορίθμου, ώστε να προσφέρεται η μέγιστη δυνατή ασφάλεια στην εκάστοτε εφαρμογή. Η κρυπτανάλυση μπορεί να χωριστεί σε δύο κατηγορίες: συμμετρική κρυπτανάλυση και ασύμμετρη κρυπτανάλυση.

2.6.1 Συμμετρική κρυπτανάλυση

Η **συμμετρική κρυπτανάλυση** περιλαμβάνει την ανάλυση και την παραβίαση συμμετρικών κρυπτογραφικών συστημάτων, όπως οι κρυπτογραφήσεις μπλοκ και οι κρυπτογραφήσεις ροής. Υπάρχουν διάφορες τεχνικές που χρησιμοποιούνται στη συμμετρική κρυπτανάλυση [4], όπως:

2.6.1.1 Επιθέσεις ωμής βίας

Οι **επιθέσεις ωμής βίας** περιλαμβάνουν τη δοκιμή όλων των πιθανών κλειδιών για την αποκρυπτογράφηση ενός κρυπτογραφημένου κειμένου. Οι επιθέσεις ωμής βίας είναι συνήθως πρακτικές μόνο για μικρά μεγέθη κλειδιών.

2.6.1.2 Επιθέσεις γνωστού κειμένου

Οι **επιθέσεις γνωστού κειμένου** περιλαμβάνουν την ανάλυση του κρυπτογραφημένου κειμένου και του αντίστοιχου απλού κειμένου για την εξαγωγή πληροφοριών σχετικά με το κλειδί.

2.6.1.3 Διαφορική κρυπτανάλυση

Η **Διαφορική κρυπτανάλυση** πρόκειται για μια στατιστική μέθοδο που χρησιμοποιείται για την ανάλυση της συμπεριφοράς ενός κρυπτογραφικού συστήματος. Περιλαμβάνει την εύρεση ζευγών εισόδων που παράγουν μια διαφορά στην έξοδο και στη συνέχεια την ανάλυση του τρόπου με τον οποίο η διαφορά διαδίδεται μέσω του συστήματος.

2.6.1.4 Γραμμική κρυπτανάλυση

Η **Γραμμική κρυπτανάλυση** πρόκειται για μια άλλη στατιστική μέθοδο που χρησιμοποιείται για την ανάλυση της συμπεριφοράς ενός κρυπτογραφικού συστήματος. Περιλαμβάνει την εύρεση γραμμικών σχέσεων μεταξύ της εισόδου, της εξόδου και του κλειδιού ενός κρυπτογραφικού συστήματος.

2.6.2 Ασύμμετρη κρυπτανάλυση

Η **ασύμμετρη κρυπτανάλυση** περιλαμβάνει την ανάλυση και την παραβίαση ασύμμετρων κρυπτογραφικών συστημάτων, όπως η κρυπτογράφηση δημόσιου κλειδιού και οι ψηφιακές υπογραφές. Η ασύμμετρη κρυπτανάλυση είναι γενικά πιο δύσκολη από τη συμμετρική κρυπτανάλυση, καθώς τα μεγέθη κλειδιών που χρησιμοποιούνται στα ασύμμετρα συστήματα είναι συνήθως πολύ μεγαλύτερα. Υπάρχουν διάφορες τεχνικές που χρησιμοποιούνται στην ασύμμετρη κρυπτανάλυση [4], μεταξύ των οποίων:

2.6.2.1 Επιθέσεις παραγοντοποίησης

Οι **επιθέσεις παραγοντοποίησης** περιλαμβάνουν την παραβίαση του υποκείμενου μαθηματικού προβλήματος που χρησιμοποιείται σε ορισμένα ασύμμετρα κρυπτογραφικά συστήματα, όπως το RSA. Οι επιθέσεις παραγοντοποίησης είναι γενικά πρακτικές μόνο για μικρά μεγέθη κλειδιών.

2.6.2.2 Επιθέσεις διακριτού λογαρίθμου

Οι **επιθέσεις διακριτού λογαρίθμου** περιλαμβάνουν την παραβίαση του υποκείμενου μαθηματικού προβλήματος που χρησιμοποιείται σε ορισμένα ασύμμετρα κρυπτογραφικά συστήματα, όπως ο Diffie-Hellman και ορισμένα κρυπτογραφικά συστήματα ελλειπτικών καμπυλών.

2.6.2.3 Επιθέσεις πλευρικού καναλιού

Οι **επιθέσεις πλευρικού καναλιού** περιλαμβάνουν την ανάλυση της φυσικής υλοποίησης ενός κρυπτογραφικού συστήματος για την εξαγωγή πληροφοριών σχετικά με το κλειδί. Οι επιθέσεις πλευρικού καναλιού μπορεί να περιλαμβάνουν ανάλυση ισχύος, ανάλυση χρονισμού και ηλεκτρομαγνητική ανάλυση.

2.7 Σύνοψη

Συνοψίζοντας, η κρυπτογραφία αποτελεί ζωτική πτυχή της ασφαλούς επικοινωνίας και της προστασίας των δεδομένων. Η συμμετρική, η ασύμμετρη και η κρυπτογραφία συναρτήσεων κατακερματισμού χρησιμοποιούνται για διαφορετικούς σκοπούς, ενώ η διαχείριση των κλειδιών είναι απαραίτητη σε όλες τις περιπτώσεις. Η κρυπτανάλυση χρησιμοποιείται για τον έλεγχο της ασφάλειας των κρυπτογραφικών συστημάτων και είναι ένας συνεχώς εξελισσόμενος τομέας. Η κρυπτογραφία είναι απαραίτητη για τη διασφάλιση ευαίσθητων πληροφοριών και αποτελεί μια από τις τεχνολογίες που καθιστούν εφικτή την ύπαρξη του IoT.

Κεφάλαιο 3: IoT

3.1 Εισαγωγή

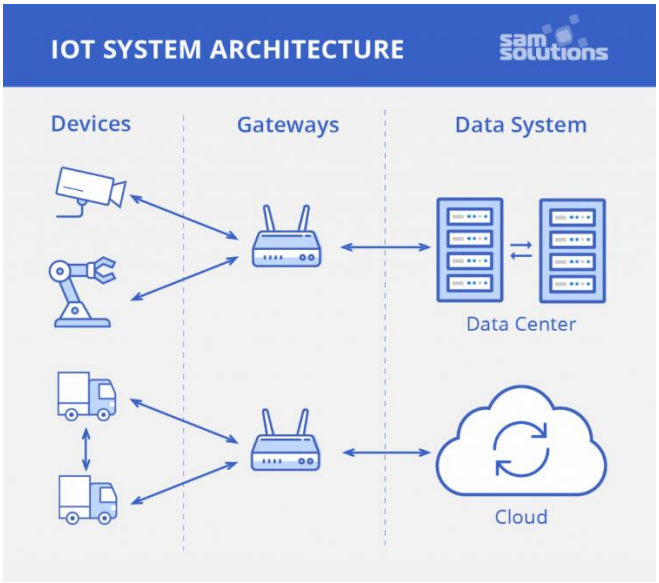
Το Internet of Things (IoT) είναι μια αναδυόμενη τεχνολογία που έχει κερδίσει μεγάλη προσοχή τα τελευταία χρόνια. Η έννοια του IoT αναφέρεται στο **δίκτυο φυσικών συσκευών**, οχημάτων και άλλων αντικειμένων που είναι εξοπλισμένα με αισθητήρες, λογισμικό και συνδεσιμότητα δικτύου, επιτρέποντάς τους να συλλέγουν και να ανταλλάσσουν δεδομένα. Το IoT έχει τη δυνατότητα να φέρει επανάσταση στον τρόπο με τον οποίο ζούμε, εργαζόμαστε και αλληλεπιδρούμε με την τεχνολογία. Σε αυτό το κεφάλαιο, θα γίνει μια επισκόπηση της αρχιτεκτονικής του IoT, των συστατικών στοιχείων, των παραδειγμάτων συσκευών και εφαρμογών, καθώς και των πλεονεκτημάτων και των προκλήσεων που σχετίζονται με την τεχνολογία.

3.1.1 Ορισμός

Ο όρος " Internet of Things " (Διαδίκτυο των αντικειμένων) επινοήθηκε για πρώτη φορά από τον **Kevin Ashton**, έναν Βρετανό πρωτοπόρο της τεχνολογίας, το 1999. Το IoT μπορεί να οριστεί ως ένα δίκτυο φυσικών συσκευών, οχημάτων και άλλων αντικειμένων που είναι ενσωματωμένα με αισθητήρες, λογισμικό και συνδεσιμότητα δικτύου, επιτρέποντάς τους να συλλέγουν και να ανταλλάσσουν δεδομένα. Το δίκτυο αυτό χαρακτηρίζεται από την ικανότητά του να επικοινωνεί με άλλες συσκευές και συστήματα μέσω του διαδικτύου, επιτρέποντας την αυτοματοποίηση διαφόρων διαδικασιών [5].

3.1.2 Αρχιτεκτονική

Η αρχιτεκτονική του IoT αποτελείται από διάφορα στοιχεία, όπως αισθητήρες, ενεργοποιητές, πύλες, υπηρεσίες cloud και συσκευές τελικού χρήστη. Οι αισθητήρες και οι ενεργοποιητές είναι υπεύθυνοι για τη συλλογή και την επεξεργασία δεδομένων, ενώ οι πύλες και οι υπηρεσίες cloud χρησιμοποιούνται για την αποθήκευση και την ανάλυση δεδομένων. Οι συσκευές τελικού χρήστη χρησιμοποιούνται για την εμφάνιση των πληροφοριών που συλλέγονται από τις συσκευές IoT. Η ροή δεδομένων στο IoT διευκολύνεται από διάφορα πρωτόκολλα επικοινωνίας, όπως Wi-Fi και Bluetooth.



Εικόνα 4 Αρχιτεκτονική συτήματος IoT [26]

3.1.3 Παραδείγματα συσκευών και εφαρμογών IoT

Το IoT έχει ένα ευρύ φάσμα εφαρμογών, από έξυπνα σπίτια μέχρι wearables, έξυπνες πόλεις και βιομηχανικό IoT. Τα έξυπνα σπίτια χρησιμοποιούν συσκευές IoT για τον έλεγχο των οικιακών συσκευών, του φωτισμού και των συστημάτων ασφαλείας. Οι φορητές συσκευές IoT, όπως οι συσκευές παρακολούθησης φυσικής κατάστασης (fitness trackers) και τα έξυπνα ρολόγια, χρησιμοποιούνται για την παρακολούθηση της υγείας και της φυσικής κατάστασης. Οι έξυπνες πόλεις χρησιμοποιούν συσκευές IoT για τη διαχείριση της κυκλοφορίας, της δημόσιας ασφάλειας και της διαχείρισης αποβλήτων. Το βιομηχανικό IoT χρησιμοποιείται για την παρακολούθηση και τη βελτιστοποίηση διαφόρων βιομηχανικών διαδικασιών, όπως η παραγωγή, τα logistics και η διαχείριση της εφοδιαστικής αλυσίδας.

3.1.4 Οφέλη και προκλήσεις

Το IoT έχει πολλά οφέλη, όπως η αυτοματοποίηση, η αποδοτικότητα και η ευκολία. Για παράδειγμα, η χρήση συσκευών IoT μπορεί να αυτοματοποιήσει διάφορες διαδικασίες, μειώνοντας την ανάγκη για ανθρώπινη παρέμβαση. Το IoT μπορεί επίσης να βελτιώσει την **αποδοτικότητα** παρέχοντας δεδομένα και αναλύσεις σε πραγματικό χρόνο που μπορούν να χρησιμοποιηθούν για τη βελτιστοποίηση των διαδικασιών. Ωστόσο, το IoT παρουσιάζει επίσης διάφορες προκλήσεις, όπως η ασφάλεια, η προστασία της ιδιωτικότητας και η διαλειτουργικότητα. Η χρήση συσκευών IoT μπορεί να δημιουργήσει νέους κινδύνους για την **ασφάλεια** και την προστασία της ιδιωτικότητας, ενώ η **έλλειψη τυποποίησης** μπορεί να δυσχεράνει την επικοινωνία διαφορετικών συσκευών και συστημάτων μεταξύ τους.

3.1.5 Σύνοψη

Συμπερασματικά, το IoT είναι μια ταχέως αναπτυσσόμενη τεχνολογία που έχει τη δυνατότητα να μεταμορφώσει τον τρόπο με τον οποίο ζούμε, εργαζόμαστε και αλληλεπιδρούμε με την τεχνολογία. Σε αυτό το κεφάλαιο θα αναλυθεί το IoT, οι πιθανές χρήσεις του, οι βασικές τεχνολογίες που καθιστούν δυνατή την ύπαρξη του, καθώς και οι υφιστάμενες προκλήσεις ασφαλείας.

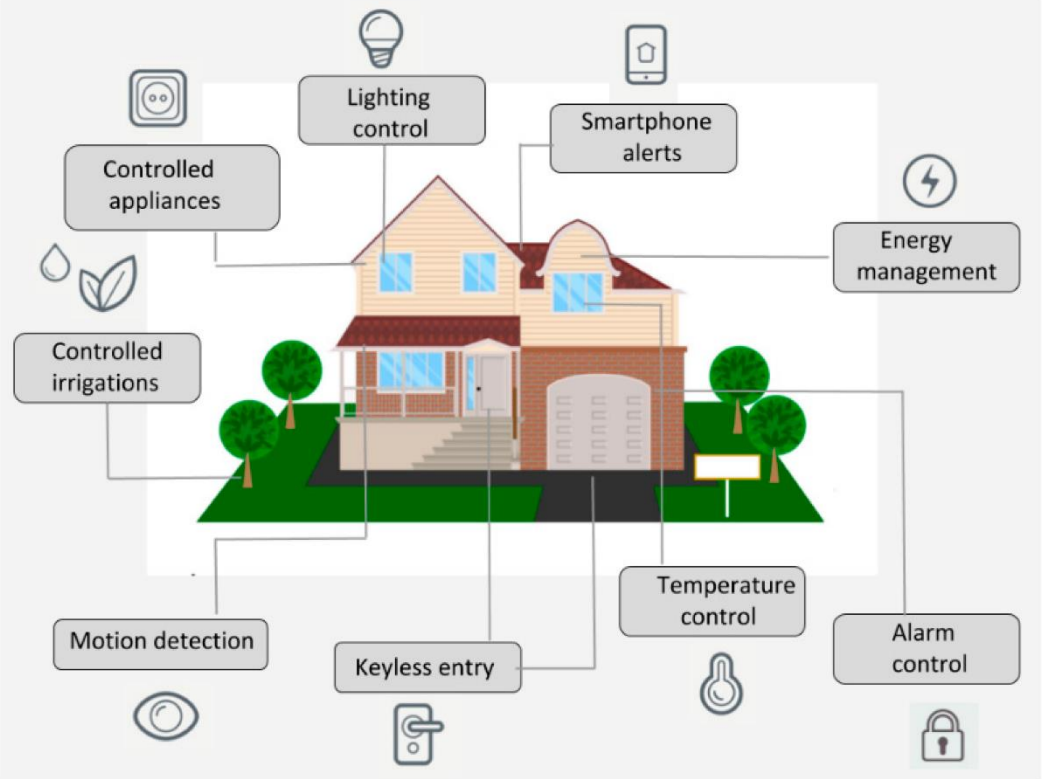
3.2 Εφαρμογές

Το Internet of Things (IoT) χρησιμοποιείται για να μεταμορφώσει ένα ευρύ φάσμα κλάδων, από τη βιομηχανία και την υγειονομική περίθαλψη έως τις μεταφορές και τη γεωργία. Σε αυτό το κεφάλαιο, θα διερευνηθούν ορισμένες από τις πιο συνηθισμένες περιπτώσεις χρήσης του IoT και πώς χρησιμοποιείται για την προώθηση της καινοτομίας και τη βελτίωση της αποδοτικότητας.

3.2.1 Έξυπνο Σπίτι

Τα τελευταία χρόνια υπάρχει αυξημένη προσφορά και ζήτηση για έξυπνες οικιακές συσκευές. Το επόμενο στάδιο στην αυτοματοποίηση των οικιακών διαδικασιών είναι η επικοινωνία μεταξύ των έξυπνων οικιακών συσκευών και η αυτόνομη διαχείριση του σπιτιού. Για να επιτευχθεί αυτό αρχικά χρειάζονται διάφορες **συσκευές/αισθητήρες** που θα αναλαμβάνουν την λήψη δεδομένων από το σπίτι (αισθητήρες φωτός, κίνησης, υγρασίας). Επίσης χρειάζεται μια υπηρεσία που θα μαζεύει όλα τα παραπάνω δεδομένα και μέσω αλγορίθμων θα λαμβάνει τις αποφάσεις και τις πράξεις που θα πρέπει να συμβούν. Στη συνέχεια θα πρέπει να υπάρχουν οι έξυπνες συσκευές που θα εκτελούν τις αποφάσεις αυτές (π.χ. κλειδαριά, θερμοστάτης, λάμπα κ.λπ.). Τέλος πρέπει να υπάρχει και μια διεπαφή χρήστη (web app), όπου

ο ιδιοκτήτης θα μπορεί να ορίζει την συμπεριφορά του έξυπνου σπιτιού και να ρυθμίζει τις παραμέτρους [6].



Εικόνα 5 Έξυπνο Σπίτι [27]

3.2.2 Γεωργία

Ο κλάδος της γεωργίας έχει εξελιχθεί αρκετά τις τελευταίες δεκαετίες με την ενσωμάτωση της τεχνολογίας στις γεωργικές διαδικασίες (λιπάσματα, γεωργικά μηχανήματα, GMOs). Το επόμενο βήμα στην εξέλιξη των γεωργικών διαδικασιών είναι η ενσωμάτωση του IoT και του Big Data. Συγκεκριμένα αυτό θα επέλθει με τη χρήση αισθητήρων για τη συλλογή γεωλογικών δεδομένων (σύσταση χώματος, υγρασία, θερμοκρασία κ.α.) Στη συνέχεια θα γίνεται η επεξεργασία αυτών των δεδομένων και συνδυαστικά με άλλα συστήματα (π.χ. μετεωρολογικές προβλέψεις) θα λαμβάνονται οι αποφάσεις σχετικά με τις γεωργικές διαδικασίες. Το παραπάνω μπορεί να βοηθήσει με πολλαπλούς τρόπους την βελτίωση των γεωργικών διαδικασιών. Για παράδειγμα η συλλογή δεδομένων μπορεί να βοηθήσει στη συσχέτιση κακής σοδιάς με τις παραμέτρους που επικρατούν. Άλλος ένας τρόπος που μπορεί να βοηθήσει το IoT τη γεωργία είναι μέσω της παρακολούθησης των καλλιεργειών σε πραγματικό χρόνο και την άμεση αντιμετώπιση προβλημάτων. Τέλος το IoT μπορεί να βοηθήσει μικρούς γεωργούς να μεγιστοποιήσουν την παραγωγή και τα κέρδη τους χωρίς την ανάγκη πρόσληψης ειδικών για συμβουλευτικές υπηρεσίες [7].

3.2.3 Υγεία

Η εξέλιξη της ιατρικής έχει φέρει ως αποτέλεσμα την σημαντική αύξηση του προσδόκιμου ζωής. Αυτό έχει ως αποτέλεσμα την ανάγκη για δημιουργία συστημάτων παρακολούθησης υγείας κυρίως για άτομα που ανήκουν σε ευπαθείς ομάδες. Η χρήση του IoT για τη δημιουργία ενός τέτοιου συστήματος θα είχε πολλαπλά οφέλη. Ένα από αυτά είναι η αυτόματη παρακολούθηση σε πραγματικό χρόνο των ζωτικών δεδομένων ενός ατόμου, έτσι μπορούν να προληφθούν προβλήματα υγείας χωρίς να χρειαστεί ο ασθενής να νιώσει συμπτώματα και να επισκεφθεί ένα γιατρό. Άλλο ένα από αυτά τα οφέλη η συλλογή δεδομένων ασθενών που μπορούν να χρησιμοποιηθούν για να εκπαιδευτούν μοντέλα τεχνητής νοημοσύνης για την έγκαιρη πρόβλεψη ασθενειών. Τέλος όπως απέδειξε και η πρόσφατη επιδημία του ιού Covid-19, θα ήταν χρήσιμο να υπήρχαν συστήματα που να αναγνωρίζουν σε πραγματικό χρόνο την πιθανή νόσηση και να σταματούν τη διασπορά [8].

3.2.4 Αυτόνομη Οδήγηση

Οι δύο πιο σημαντικές τεχνολογικές εξελίξεις στην αυτοκινητιστική βιομηχανία είναι αναμφισβήτητα η ηλεκτροκίνηση και η αυτόνομη οδήγηση. Η αυτόνομη οδήγηση ενθυλακώνει τόσο την ημιαυτόνομη κίνηση, όπου τα αυτοκίνητα έχουν τη δυνατότητα να επιταχύνουν, να επιβραδύνουν και να αλλάζουν κατεύθυνση, αλλά η παρουσία του οδηγού είναι ακόμα αναγκαία, όσο και την πλήρη αυτόνομη κίνηση, όπου τα αυτοκίνητα μπορούν να μετακινούνται από το ένα σημείο στο άλλο χωρίς ανθρώπινη παρέμβαση. Η τεχνολογία του IoT εμπλέκεται περισσότερο με τη δεύτερη κατηγορία, όπου μέσα από ένα σύστημα επικοινωνίας τα αυτοκίνητα έχουν την δυνατότητα να επικοινωνούν μεταξύ τους. Αυτό έχει ως αποτέλεσμα την αύξηση της ασφάλειας στους δρόμους με την εξάλειψη του ανθρωπίνου λάθους. Άλλο ένα αποτέλεσμα είναι η οικονομία στα καύσιμα και στις θέσεις στάθμευσης, καθώς η επικοινωνία μεταξύ των οχημάτων θα είναι αποδοτικότερη, με αποτέλεσμα να γίνουν οι πόλεις μας καθαρότερες και λιγότερο συμφορημένες. Τέλος η αυτόνομη οδήγηση θα προσφέρει αυτονομία κίνησης σε όλους τους ανθρώπους ανεξαρτήτως ικανότητας απόκτησης διπλώματος οδήγησης [9].

3.2.5 Βιομηχανία (Industry 4.0)

Η ανθρωπότητα έχει αναπτυχθεί με ραγδαίους ρυθμούς τους τελευταίους αιώνες και ένας από τους σημαντικότερους παράγοντες αποτελεί η βιομηχανική επανάσταση. Συγκεκριμένα η βιομηχανική επανάσταση μπορεί να χωριστεί σε 4 φάσεις. Η πρώτη ήρθε με την ανακάλυψη και η μαζική όρυξη γαιανθράκων, καθώς και η αξιοποίηση τους από τις ατμομηχανές. Η δεύτερη βιομηχανική επανάσταση συνέβη με την εφεύρεση του ηλεκτρικού ρεύματος και την χρήση του σε διάφορες εφευρέσεις (ηλεκτροκινητήρας, τηλέφωνο, ηλεκτρικός λαμπτήρας) καθώς και την ανακάλυψη του πετρελαίου. Η τρίτη βιομηχανική επανάσταση επήλθε με τις εξελίξεις στον τομέα της ηλεκτρονικής, των τηλεπικοινωνιών καθώς και της πληροφορικής, παράλληλα με την αξιοποίηση την πυρηνικής ενέργειας. Η πιο πρόσφατη βιομηχανική επανάσταση (Industry 4.0) αφορά την αξιοποίηση των ανανεώσιμων πηγών ενέργειας, αλλά και κυρίως τη χρήση του διαδικτύου. Στο πλαίσιο αυτό εμπλέκεται η χρήση του IoT στην παραγωγική διαδικασία. Συγκεκριμένα σκοπός είναι η χρήση μηχανών που θα επικοινωνούν μεταξύ τους ώστε να αυτοματοποιηθεί η παραγωγική διαδικασία. Επίσης η χρήση IoT μπορεί να προσφέρει την άντληση δεδομένων από την παραγωγική διαδικασία ώστε να γίνει πιο αποδοτική [10].

3.2.6 Σύνοψη

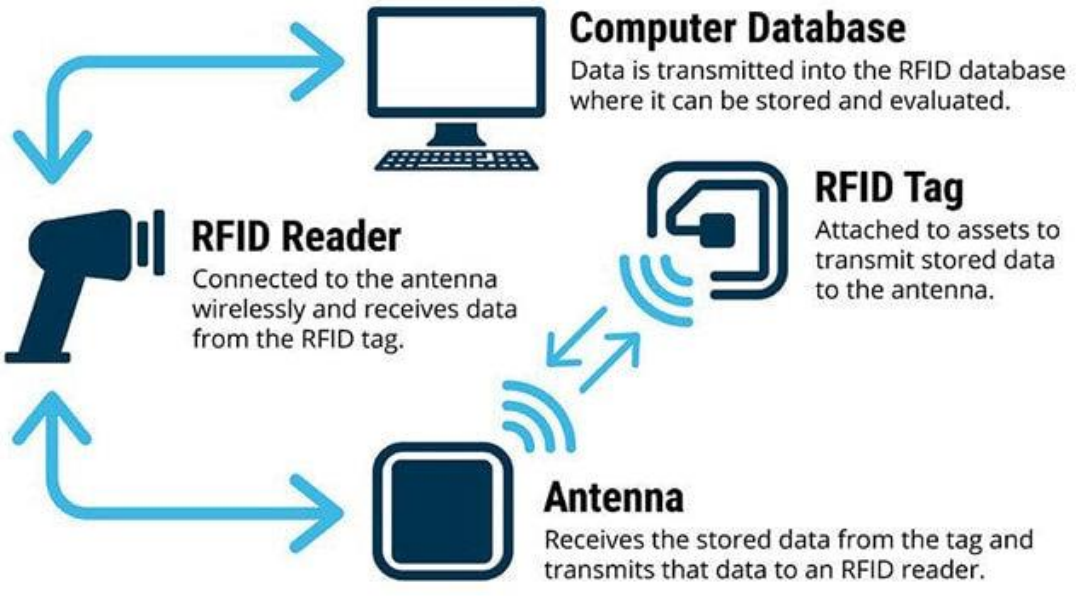
Συνοψίζοντας, το IoT χρησιμοποιείται για να μεταμορφώσει ένα ευρύ φάσμα τομέων, από τα έξυπνα σπίτια μέχρι την υγειονομική περίθαλψη και τη γεωργία. Τα οφέλη του IoT περιλαμβάνουν τη βελτίωση της αποδοτικότητας, τη μείωση του κόστους και την ενίσχυση της ασφάλειας και της προστασίας. Καθώς το IoT συνεχίζει να εξελίσσεται, αναμένεται να υπάρξουν ακόμη πιο καινοτόμες περιπτώσεις χρήσης και εφαρμογές. Στο επόμενο κεφάλαιο, θα αναλυθούν οι απαραίτητες τεχνολογίες που επιτρέπουν την ύπαρξη του IoT.

3.3 Βασικές τεχνολογίες για το IoT

Το IoT βασίζεται σε μια σειρά από βασικές τεχνολογίες που επιτρέπουν τη συλλογή, την επεξεργασία και την ανταλλαγή δεδομένων. Σε αυτό το κεφάλαιο, θα γίνει μια επισκόπηση των βασικών τεχνολογιών που υποστηρίζουν το IoT, συμπεριλαμβανομένων των τεχνολογιών ασύρματης επικοινωνίας, των αισθητήρων, του υπολογιστικού νέφους και της ανάλυσης δεδομένων [11].

3.3.1 RFID

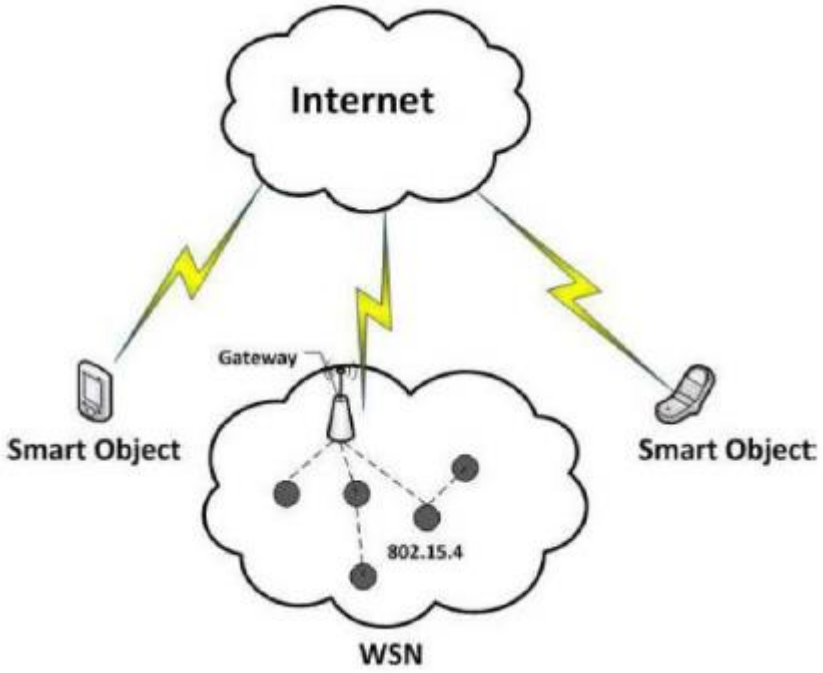
Το RFID είναι μια από τις πλέον διαδεδομένες τεχνολογίες ταυτοποίησης συσκευών και αποτελεί την εξέλιξη του barcode. Τα συστήματα RFID λειτουργούν με τη συνεργασία δύο οντοτήτων, των ετικετών (tags) και των αναγνωστών (readers). Οι ετικέτες χωρίζονται σε 3 κατηγορίες. Συγκεκριμένα υπάρχουν οι **παθητικές**, οι **ημι-παθητικές** και οι **ενεργές ετικέτες**. Οι **παθητικές** ετικέτες λειτουργούν με τη χρήση της ενέργειας που υπάρχει στα ραδιοκύματα, με αποτέλεσμα να μπορούν να επικοινωνούν με τους αναγνώστες χωρίς την ανάγκη χρήσης μπαταρίας και χρησιμοποιούνται κυρίως για την αναγνώριση αντικειμένων μέσω ενός μοναδικού κωδικού. Αντιθέτως οι **ημι-παθητικές** και οι **ενεργές** ετικέτες χρησιμοποιούν μπαταρίες και χρησιμοποιούνται όποτε είναι αναγκαίο οι ετικέτες να μεταδίδουν δεδομένα είτε ανά τακτά χρονικά διαστήματα (beacons) είτε κατόπιν αιτήματος (transponders). Οι ενεργές και οι ημι-παθητικές ετικέτες κοστίζουν περισσότερο από τις παθητικές, ενώ είναι και αναλώσιμες καθώς οι μπαταρίες τους δεν αντικαθίστανται [11].



Εικόνα 6 Ροή δεδομένων σε IoT σύστημα με χρήση RFID ετικετών [28]

3.3.2 WSN

Τα **Ασύρματα Δίκτυα Αισθητήρων (Wireless Sensor Networks - WSN)** είναι ένας τύπος δικτύου που αποτελείται από μικρές αυτόνομες συσκευές που ονομάζονται κόμβοι και είναι εξοπλισμένοι με αισθητήρες, επεξεργαστές και τη δυνατότητα ασύρματης επικοινωνίας. Αυτοί οι κόμβοι μπορούν να τοποθετηθούν σε διάφορα περιβάλλοντα για να παρακολουθούν φυσικές ή περιβαλλοντικές συνθήκες, όπως θερμοκρασία, υγρασία, πίεση, ήχος και κίνηση. Οι κόμβοι επικοινωνούν μεταξύ τους ασύρματα, δημιουργώντας ένα δίκτυο, και μπορούν να συνδεθούν στο Διαδίκτυο. Τα WSN χρησιμοποιούν διάφορα πρωτόκολλα επικοινωνίας για να διατηρούν την επικοινωνία μεταξύ των κόμβων, και τεχνικές διαχείρισης ισχύος χρησιμοποιούνται για την εξοικονόμηση ενέργειας. Τα δεδομένα που συλλέγονται από τους κόμβους μπορούν να αναλυθούν χρησιμοποιώντας διάφορες τεχνικές, όπως τη μηχανική μάθηση και τη στατιστική ανάλυση, για την εξαγωγή συμπερασμάτων [11]. Τα WSN αποτελούν μια ισχυρή τεχνολογία για τη συλλογή και ανάλυση δεδομένων σε πραγματικό χρόνο.



Εικόνα 7 Τοπολογία WSN στο διαδίκτυο [29]

3.3.3 Big Data

Η **ανάλυση δεδομένων μεγάλης κλίμακας** είναι η διαδικασία εξαγωγής συμπερασμάτων και γνώσης από μεγάλα και πολύπλοκα σύνολα δεδομένων. Περιλαμβάνει τη χρήση προηγμένων αναλυτικών τεχνικών, όπως μηχανική μάθηση, εξόρυξη δεδομένων και προβλεπτική ανάλυση, για την αναγνώριση προτύπων, τάσεων και σχέσεων στα δεδομένα. Η ανάλυση δεδομένων μεγάλης κλίμακας είναι ουσιώδης για τους οργανισμούς που συλλέγουν και αποθηκεύουν μαζικές ποσότητες δεδομένων, όπως πλατφόρμες κοινωνικών μέσων, ισότοποι ηλεκτρονικού εμπορίου και πάροχοι υπηρεσιών υγείας. Αναλύοντας τα δεδομένα, οι οργανισμοί μπορούν να αποκτήσουν σημαντικές ενδείξεις για τη συμπεριφορά των πελατών, τις τάσεις της αγοράς, την απόδοση των προϊόντων και άλλες βασικές επιχειρησιακές μετρήσεις [11]. Η ανάλυση δεδομένων μεγάλης κλίμακας απαιτεί ειδικά εργαλεία και τεχνολογίες, όπως κατανεμημένα συστήματα αρχείων, παράλληλη επεξεργασία και οπτικοποίηση δεδομένων, για να αντιμετωπίσει τον όγκο, την ταχύτητα και την ποικιλία των μεγάλων δεδομένων.

3.3.4 Cloud Computing

Η τεχνολογία του **cloud computing** είναι ένα μοντέλο υπολογισμού που παρέχει πρόσβαση σε ένα κοινόχρηστο πιστοποιημένο σύνολο υπολογιστικών πόρων, όπως διακομιστές, αποθηκευτικό χώρο, εφαρμογές και υπηρεσίες, μέσω του Διαδικτύου. Αυτό εξαλείφει την ανάγκη για οργανισμούς να επενδύσουν στη δική τους φυσική υποδομή και να τη διαχειρίζονται, επιτρέποντας τους να κλιμακώσουν δυναμικά τους υπολογιστικούς τους πόρους πάνω ή κάτω, ανάλογα με τις ανάγκες τους [11]. Η τεχνολογία του cloud computing μπορεί να κατηγοριοποιηθεί σε τρεις βασικές κατηγορίες: **υποδομή ως υπηρεσία (IaaS), πλατφόρμα ως υπηρεσία (PaaS)** και **λογισμικό ως υπηρεσία (SaaS)**. Η τεχνολογία του cloud computing προσφέρει αρκετά πλεονεκτήματα, συμπεριλαμβανομένης της κλιμακωσιμότητας, της ευελιξίας, της προσβασιμότητας, της αξιοπιστίας και της ασφάλειας.

3.3.5 Σύνοψη

Όλες οι παραπάνω τεχνολογίες συμβάλουν στην εκπλήρωση των απαιτήσεων για την λειτουργία της τεχνολογίας του IoT. Συγκεκριμένα το **RFID** αποτελεί την τεχνολογία που επιτρέπει την ταυτοποίηση των αισθητήρων. Τα **WSN** αποτελούν τη γέφυρα που επιτρέπει την επικοινωνία των αισθητήρων είτε μεταξύ τους είτε με κάποια δομή για την αποθήκευση και την επεξεργασία των παραγόμενων δεδομένων. Το **Cloud Computing** παρέχει τις υποδομές για τη συλλογή και την επεξεργασία αυτών των δεδομένων. Τέλος η **Big Data** ανάλυση παρέχει τις πρακτικές για εξαγωγή χρήσιμων συμπερασμάτων από τα δεδομένα αυτά. Συνοψίζοντας γίνεται κατανοητό πως η τεχνολογία του IoT δε θα ήταν εφικτή χωρίς την ανάπτυξη οποιασδήποτε από τις παραπάνω τεχνολογίες.

3.4 Προκλήσεις ασφαλείας IoT

Το IoT έχει τη δυνατότητα να μεταμορφώσει τον τρόπο με τον οποίο ζούμε και εργαζόμαστε, αλλά παρουσιάζει επίσης μοναδικές προκλήσεις ασφαλείας. Σε αυτό το κεφάλαιο, θα εξεταστούν ορισμένες από τις σημαντικότερες προκλήσεις ασφαλείας που σχετίζονται με το IoT και τη σημασία της αυθεντικοποίησης συσκευών [12].

3.4.1 Κλιμακωσιμότητα

Μία από τις μεγαλύτερες προκλήσεις της ασφάλειας του IoT είναι η μεγάλη κλίμακα και η πολυπλοκότητα του δικτύου. Με δισεκατομμύρια συσκευές συνδεδεμένες στο διαδίκτυο, μπορεί να είναι δύσκολο να παρακολουθηθούν όλες οι πιθανές ευπάθειες. Επιπλέον, η ποικιλομορφία των συσκευών και των πρωτοκόλλων που χρησιμοποιούνται στο IoT αποτελεί πρόκληση για την τυποποίηση των μέτρων ασφαλείας.

3.4.2 Έλλειψη τυποποίησης

Το IoT δεν διαθέτει ένα καθολικό πρότυπο για την ασφάλεια, πράγμα που σημαίνει ότι οι συσκευές ενδέχεται να μην έχουν σχεδιαστεί με γνώμονα την ασφάλεια. Αυτό μπορεί να οδηγήσει σε ευπάθειες που μπορούν να αξιοποιηθούν σε κακόβουλες επιθέσεις. Επιπλέον, η έλλειψη τυποποίησης καθιστά δύσκολο για τους χρήστες να γνωρίζουν ποια μέτρα ασφαλείας υπάρχουν και πώς να ασφαλίζουν σωστά τις συσκευές τους.

3.4.3 Απόρρητο δεδομένων

Το IoT παράγει τεράστιες ποσότητες δεδομένων, πολλά από τα οποία είναι ευαίσθητα ή προσωπικά στη φύση τους. Η διασφάλιση του απορρήτου και της ασφάλειας αυτών των δεδομένων είναι απαραίτητη για τη διατήρηση της εμπιστοσύνης των χρηστών στις συσκευές IoT. Οι παραβιάσεις δεδομένων μπορεί να έχουν σοβαρές συνέπειες, όπως κλοπή ταυτότητας, οικονομικές απώλειες και βλάβη της φήμης.

3.4.4 Αυθεντικοποίηση συσκευών

Ο έλεγχος ταυτότητας συσκευής είναι απαραίτητος για την ασφάλεια του IoT. Περιλαμβάνει την επαλήθευση της ταυτότητας των συσκευών και τη διασφάλιση ότι μόνο εξουσιοδοτημένες συσκευές μπορούν να έχουν πρόσβαση στο δίκτυο. Χωρίς τον κατάλληλο έλεγχο ταυτότητας, μπορούν να σχεδιαστούν επιθέσεις που χρησιμοποιούν ψεύτικες συσκευές για να αποκτήσουν πρόσβαση στο δίκτυο και να κλέψουν δεδομένα, να παράξουν πλαστά δεδομένα ή να εξαπολύσουν επιθέσεις.

3.4.5 Σύνοψη

Συνοψίζοντας, οι προκλήσεις ασφαλείας που σχετίζονται με το IoT είναι σημαντικές, αλλά μπορούν να αντιμετωπιστούν με τα κατάλληλα μέτρα. Η τυποποίηση, το απόρρητο των δεδομένων και ο έλεγχος ταυτότητας των συσκευών είναι απαραίτητα για την ασφάλεια του IoT.

3.5 Συμπεράσματα

Σε αυτό το κεφάλαιο διερευνήθηκαν οι βασικές τεχνολογίες που καθιστούν εφικτό το Διαδίκτυο των πραγμάτων (IoT). Συζητήθηκε ο τρόπος με τον οποίο οι αισθητήρες, τα ασύρματα δίκτυα και το υπολογιστικό νέφος συνεργάζονται για τη συλλογή και ανάλυση δεδομένων σε πραγματικό χρόνο και πώς μπορούν να χρησιμοποιηθούν για τη δημιουργία ενός ευρέος φάσματος εφαρμογών και υπηρεσιών. Επιπλέον, διερευνήθηκαν ορισμένες από τις πιο υποσχόμενες περιπτώσεις χρήσης του IoT, από τα έξυπνα σπίτια και τις πόλεις έως την υγειονομική περίθαλψη και τη γεωργία. Αυτές οι περιπτώσεις χρήσης καταδεικνύουν τις δυνατότητες του IoT να μεταμορφώσει τον τρόπο με τον οποίο ζούμε και εργαζόμαστε και να δημιουργήσει νέες ευκαιρίες για καινοτομία και ανάπτυξη. Ωστόσο, έχει επίσης αποδειχθεί ότι το IoT παρουσιάζει μοναδικές προκλήσεις στον τομέα της ασφάλειας, όπως αναλύεται στην ενότητα σχετικά με τις προκλήσεις στον τομέα της ασφάλειας του IoT και τη σημασία της πιστοποίησης της ταυτότητας των συσκευών. Η διασφάλιση του απορρήτου και της ασφάλειας των τεράστιων ποσοτήτων δεδομένων που παράγονται από το IoT είναι απαραίτητη για τη διατήρηση της εμπιστοσύνης των χρηστών στις συσκευές IoT. Συνολικά, το IoT είναι ένας πολύπλοκος και ταχέως εξελισσόμενος τομέας με τεράστιες δυνατότητες καινοτομίας και ανάπτυξης. Ωστόσο, η αξιοποίηση αυτών των δυνατοτήτων θα απαιτήσει συνεργασία και συντονισμό μεταξύ κατασκευαστών, προγραμματιστών και χρηστών. Συνεργαζόμενοι και δίνοντας προτεραιότητα στην ασφάλεια, μπορεί να δημιουργηθεί ένα IoT που θα είναι αξιόπιστο και ασφαλές για όλους τους χρήστες και θα ωφελεί την κοινωνία στο σύνολό της. Στα επόμενα κεφάλαια θα αναλυθεί η πρόταση μιας λύσης σε ένα από τα σημαντικότερα προβλήματα ασφαλείας του IoT, την αυθεντικοποίηση.

Κεφάλαιο 4: Blockchain

4.1 Εισαγωγή

Το blockchain είναι μια τεχνολογία που επιτρέπει την αποθήκευση δεδομένων με **αποκεντρωμένο** και **ασφαλή** τρόπο. Πρωτοεμφανίστηκε το 2008 [13] ως η βασική τεχνολογία πίσω από το ψηφιακό νόμισμα **Bitcoin**. Από τότε, έχει εφαρμοστεί σε διάφορους τομείς, συμπεριλαμβανομένων των οικονομικών, της διαχείρισης αλυσίδας εφοδιασμού και της υγείας. Σε ένα σύστημα blockchain, τα δεδομένα αποθηκεύονται σε μια αλυσίδα μπλοκ που συνδέονται μεταξύ τους σε χρονολογική σειρά. Κάθε μπλοκ περιέχει ένα σύνολο συναλλαγών και μόλις ένα μπλοκ προστίθεται στην αλυσίδα, δεν μπορεί να τροποποιηθεί ή διαγραφεί. Αυτό εξασφαλίζει την **ακεραιότητα** και την **αμετάβλητη φύση** των δεδομένων που αποθηκεύονται στο blockchain. Η αποκεντρωμένη φύση του blockchain σημαίνει ότι δεν υπάρχει κεντρική αρχή που ελέγχει το δίκτυο. Αντίθετα, το δίκτυο διατηρείται από ένα σύνολο κόμβων που επικυρώνουν και προσθέτουν νέα μπλοκ στην αλυσίδα. Αυτό καθιστά δύσκολη την παραποίηση ή τη διαφθορά των δεδομένων που αποθηκεύονται στο blockchain. Η ασφάλεια του blockchain επιτυγχάνεται μέσω της χρήσης κρυπτογραφικών τεχνικών, όπως **ψηφιακές υπογραφές** και **κατακερματισμός** (hashing). Κάθε συναλλαγή επαληθεύεται από το δίκτυο και προστίθεται στο blockchain μόνο αν πληροί ορισμένα κριτήρια, όπως το να έχει τη σωστή ψηφιακή υπογραφή και να πληροί τους **κανόνες συναίνεσης (consensus rules)** του δικτύου. Καταλήγοντας, το blockchain έχει τη δυνατότητα να επαναστατικοποιήσει τον τρόπο με τον οποίο αποθηκεύουμε και διαχειριζόμαστε δεδομένα, επιτρέποντας μεγαλύτερη **ασφάλεια**, **διαφάνεια** και **αποδοτικότητα** σε διάφορους τομείς.

4.2 Ιστορική αναδρομή

Σε αυτό το κεφάλαιο, θα εξεταστεί η ιστορία της τεχνολογίας blockchain, ξεκινώντας από την προέλευσή της στα πρώτα **ψηφιακά νομίσματα** της δεκαετίας του 1990 και την εξέλιξή της ώστε να συμπεριλάβει **ΕΣ** και άλλες λειτουργίες. Θα μελετηθεί επίσης η ανάγκη για ένα αποκεντρωμένο σύστημα για την οποία δημιουργήθηκε η τεχνολογία blockchain και η εμφάνιση των altcoins και άλλων έργων που βασίζονται στην τεχνολογία blockchain.

4.2.1 Πρώιμα ψηφιακά νομίσματα

Στις πρώτες ημέρες του διαδικτύου, δημιουργήθηκαν ψηφιακά νομίσματα για να διευκολύνουν τις διαδικτυακές συναλλαγές [14]. Αυτά τα νομίσματα, όπως το **DigiCash** και το **eCash**, ήταν συγκεντρωτικά συστήματα που βασίζονταν σε ένα **αξιόπιστο τρίτο μέρος** για τη διευκόλυνση των συναλλαγών και τη διατήρηση της ακεραιότητας του νομίσματος. Ωστόσο, αυτό το συγκεντρωτικό μοντέλο είχε αρκετά μειονεκτήματα, όπως η έλλειψη διαφάνειας και η πιθανότητα απάτης.

4.2.2 Bitcoin Whitepaper

Το 2008, ο Satoshi Nakamoto δημοσίευσε ένα Whitepaper με τίτλο **"Bitcoin: A Peer-to-Peer Electronic Cash System"** [13]. Αυτό το έγγραφο περιέγραφε ένα νέο αποκεντρωμένο σύστημα που θα επέτρεπε ασφαλείς, ανώνυμες συναλλαγές χωρίς την ανάγκη ενός αξιόπιστου τρίτου μέρους. Το σύστημα, το οποίο έγινε γνωστό ως blockchain, χρησιμοποιούσε κρυπτογραφία για να διασφαλίζει την ακεραιότητα των συναλλαγών και να διατηρεί την ακεραιότητα του νομίσματος.

4.2.3 Ανάδυση των Altcoins

Το Bitcoin ήταν το πρώτο έργο βασισμένο στο blockchain, αλλά σύντομα το ακολούθησαν και άλλα κρυπτονομίσματα, γνωστά ως **altcoins**. Αυτά τα altcoins, όπως το **Litecoin** και το **Ripple**, προσπάθησαν να βελτιώσουν το μοντέλο του Bitcoin αντιμετωπίζοντας ορισμένους από τους περιορισμούς του, όπως η επεκτασιμότητα και η ταχύτητα των συναλλαγών. Εκτός από τα altcoins, εμφανίστηκαν και άλλα έργα βασισμένα στο blockchain, όπως πλατφόρμες βασισμένες στο blockchain για την επαλήθευση ψηφιακών ταυτοτήτων, τη διαχείριση της εφοδιαστικής αλυσίδας και τα συστήματα ψηφοφορίας. Τα έργα αυτά κατέδειξαν την ευελιξία της τεχνολογίας blockchain και τη δυνατότητά της να φέρει επανάσταση σε διάφορους κλάδους.

4.2.4 Εμφάνιση έξυπνων συμβολαίων

Καθώς η τεχνολογία blockchain ωρίμαζε, εξελίχθηκε ώστε να περιλαμβάνει ΕΣ και άλλες λειτουργικότητες. Τα ΕΣ είναι αυτοεκτελούμενα συμβόλαια με τους όρους της συμφωνίας μεταξύ αγοραστή και πωλητή να γράφονται απευθείας σε γραμμές κώδικα [15]. Επιτρέπουν την **αυτοματοποιημένη** και αποκεντρωμένη **εκτέλεση** των συμβολαίων, μειώνοντας δυνητικά την ανάγκη για μεσάζοντες. Άλλες λειτουργίες που έχουν προστεθεί στην τεχνολογία blockchain περιλαμβάνουν αποκεντρωμένη αποθήκευση αρχείων, αποκεντρωμένα συστήματα διακυβέρνησης και αποκεντρωμένα ανταλλακτήρια για τη διαπραγμάτευση κρυπτονομισμάτων. Αυτές οι πρόσθετες λειτουργικότητες έχουν επεκτείνει περαιτέρω τις πιθανές χρήσεις της τεχνολογίας blockchain πέρα από τα ψηφιακά νομίσματα.

4.3 Βασικά χαρακτηριστικά

Σε αυτό το κεφάλαιο θα εξεταστούν τα βασικά χαρακτηριστικά της τεχνολογίας blockchain, συμπεριλαμβανομένων της **αποκέντρωσης**, της **αμεταβλητότητας**, της **διαφάνειας** και της **ασφάλειας** .

4.3.1 Αποκέντρωση

Ένα από τα καθοριστικά χαρακτηριστικά της τεχνολογίας blockchain είναι ο **αποκεντρωμένος χαρακτήρας** της. Σε αντίθεση με τα παραδοσιακά συστήματα, τα οποία βασίζονται σε μια **κεντρική αρχή** για την επαλήθευση και τη διεκπεραίωση των συναλλαγών, το blockchain χρησιμοποιεί ένα δίκτυο ομότιμων κόμβων για την επικύρωση και την αποθήκευση δεδομένων. Αυτό σημαίνει ότι δεν υπάρχει ενιαίο σημείο αποτυχίας ή ελέγχου και οι συναλλαγές μπορούν να διεκπεραιώνονται με ασφάλεια και διαφάνεια χωρίς την ανάγκη ενδιάμεσων.

4.3.2 Αμεταβλητότητα

Ένα άλλο σημαντικό χαρακτηριστικό της τεχνολογίας blockchain είναι η **αμεταβλητότητα**. Μόλις μια συναλλαγή καταγραφεί στο blockchain, δεν μπορεί να **τροποποιηθεί** ή να **διαγραφεί**. Αυτό οφείλεται στο γεγονός ότι κάθε μπλοκ στην αλυσίδα περιέχει ένα κρυπτογραφικό κατακερματισμό (hash) του προηγούμενου μπλοκ, δημιουργώντας μια αλυσίδα μπλοκ που είναι απαραβίαστη. Αυτή η αμεταβλητότητα παρέχει υψηλό επίπεδο ακεραιότητας και ασφάλειας για τις συναλλαγές που καταγράφονται στο blockchain.

4.3.3 Διαφάνεια

Η τεχνολογία blockchain είναι επίσης γνωστή για τη **διαφάνειά** της. Επειδή οι συναλλαγές καταγράφονται σε ένα δημόσιο «βιβλίο» που είναι **προσβάσιμο από οποιονδήποτε**, όλοι οι συμμετέχοντες στο δίκτυο μπορούν να δουν το ιστορικό των συναλλαγών και να επαληθεύσουν την ακρίβειά τους. Αυτή η διαφάνεια προάγει την εμπιστοσύνη και τη λογοδοσία στις συναλλαγές και μπορεί επίσης να βοηθήσει στην πρόληψη της απάτης και της διαφθοράς.

4.3.4 Ασφάλεια

Η τεχνολογία blockchain έχει σχεδιαστεί για να είναι **εξαιρετικά ασφαλής**. Επειδή κάθε μπλοκ στην αλυσίδα περιέχει έναν κρυπτογραφικό **κατακερματισμό** του **προηγούμενου μπλοκ**, οποιαδήποτε προσπάθεια τροποποίησης ενός μπλοκ στην αλυσίδα θα απαιτούσε την τροποποίηση όλων των επόμενων μπλοκ, καθιστώντας υπολογιστικά **ανέφικτη** την **αλλοίωση** της αλυσίδας μπλοκ. Επιπλέον, η χρήση κρυπτογραφίας δημόσιου κλειδιού διασφαλίζει ότι μόνο ο κάτοχος ενός ιδιωτικού κλειδιού μπορεί να εξουσιοδοτήσει συναλλαγές, παρέχοντας ένα πρόσθετο επίπεδο ασφάλειας.

4.4 Εφαρμογές

Όπως και η τεχνολογία του IoT έτσι και το blockchain αποτελεί μια πολύ πρώιμη τεχνολογία. Παρόλα αυτά υπάρχουν ήδη για την χρησιμότητα της. Συγκεκριμένα έχουν βρεθεί ήδη αρκετοί τομείς στους οποίους μπορεί να εφαρμοστεί (ή εφαρμόζεται ήδη). Μερικά παραδείγματα είναι τα παρακάτω.

4.4.1 Ψηφιακά νομίσματα

Η τεχνολογία της blockchain μπορεί να χρησιμοποιηθεί για τη δημιουργία αποκεντρωμένων ψηφιακών νομισμάτων, όπως το Bitcoin [13] και το Ethereum [15]. Αυτά τα νομίσματα λειτουργούν σε ένα αποκεντρωμένο δίκτυο υπολογιστών που καταγράφουν και επαληθεύουν **συναλλαγές**, καθιστώντας τις **διαφανείς**, **ασφαλείς** και **ανθεκτικές** στην παρέμβαση. Τα ψηφιακά νομίσματα μπορούν να χρησιμοποιηθούν για μια μεγάλη ποικιλία εφαρμογών, συμπεριλαμβανομένων των ηλεκτρονικών αγορών, των αποστολών χρημάτων και των χρηματικών επενδύσεων.

4.4.2 Αλυσίδα εφοδιασμού

Η τεχνολογία του blockchain μπορεί να χρησιμοποιηθεί για τη δημιουργία μιας ασφαλούς και διαφανούς καταγραφής κάθε σταδίου του ταξιδιού ενός προϊόντος στην αλυσίδα. Αυτό μπορεί να βοηθήσει στη μείωση της απάτης, στην αύξηση της αποδοτικότητας και στη βελτίωση της διαφάνειας. Για παράδειγμα, η **Walmart** χρησιμοποιεί την τεχνολογία blockchain για να καταγράφει την προέλευση των τροφίμων, βοηθώντας στη διασφάλιση της ασφάλειας και ποιότητας τους [16].

4.4.3 Συστήματα ταυτοποίησης

Η τεχνολογία του blockchain μπορεί να χρησιμοποιηθεί για τη δημιουργία ενός αποκεντρωμένου, ασφαλούς και αμετάβλητου συστήματος ταυτοποίησης της ταυτότητας ενός ατόμου χωρίς την ανάγκη για κεντρική αρχή. Αυτό μπορεί να είναι χρήσιμο σε μια ποικιλία εφαρμογών, όπως χρηματοπιστωτικές υπηρεσίες και υγειονομική περίθαλψη.

4.4.4 Συστήματα ψηφοφορίας

Η τεχνολογία της blockchain μπορεί να χρησιμοποιηθεί για τη δημιουργία ενός ασφαλούς και διαφανούς συστήματος ψηφοφορίας που είναι ανθεκτικό στις κακόβουλες επιθέσεις. Χρησιμοποιώντας ένα αποκεντρωμένο δίκτυο υπολογιστών για την καταγραφή και τον έλεγχο των ψήφων, η τεχνολογία της blockchain μπορεί να βοηθήσει στη διασφάλιση δίκαιων και διαφανών εκλογών.

4.4.5 Αποκεντρωμένες αγορές

Η τεχνολογία του blockchain μπορεί να χρησιμοποιηθεί για τη δημιουργία αποκεντρωμένων αγορών όπου οι αγοραστές και οι πωλητές μπορούν να διεξάγουν συναλλαγές απευθείας μεταξύ τους, χωρίς την ανάγκη μεσαζόντων. Αυτές οι αγορές μπορούν να χρησιμοποιηθούν για μια ποικιλία εφαρμογών, όπως online αγορές για αγαθά και υπηρεσίες, πλατφόρμες δανεισμού από άτομο σε άτομο και πλατφόρμες μαζικής χρηματοδότησης.

4.5 Τύποι Blockchain

Η τεχνολογία blockchain έχει αποκτήσει αυξανόμενη δημοτικότητα από την εμφάνιση του. Έκτοτε έχει εφαρμοστεί σε διάφορες βιομηχανίες και τομείς, όπως η χρηματοδότηση, η υγειονομική περίθαλψη, η διαχείριση της εφοδιαστικής αλυσίδας και άλλα. Καθώς η τεχνολογία συνεχίζει να εξελίσσεται, έχουν εμφανιστεί διάφοροι τύποι blockchain. Σε αυτό το κεφάλαιο, θα εξερευνήσουμε τους τρεις κύριους τύπους blockchain: το **δημόσιο**, το **ιδιωτικό** και το **υβριδικό** [17].

4.5.1 Δημόσια Blockchain

Ένα **δημόσιο** blockchain είναι ένα αποκεντρωμένο δίκτυο που είναι ανοιχτό σε όποιον θέλει να συμμετάσχει. Είναι ο πιο γνωστός τύπος blockchain και συνδέεται συχνά με κρυπτονομίσματα όπως το Bitcoin και το Ethereum. Σε ένα δημόσιο blockchain, ο καθένας μπορεί να διαβάσει, να γράψει ή να συμμετάσχει στο δίκτυο και οι συναλλαγές επικυρώνονται από έναν **μηχανισμό συναίνεσης**, συνήθως Proof of Work (**PoW**) ή Proof of Stake (**PoS**). Τα δημόσια blockchain παρέχουν διαφάνεια, ασφάλεια και αμεταβλητότητα, καθιστώντας δύσκολη τη χειραγώγηση των δεδομένων στο blockchain από κακούς παράγοντες. Ωστόσο, τα δημόσια blockchain δεν είναι χωρίς τους περιορισμούς τους. Μία από τις σημαντικότερες ανησυχίες με τα δημόσια blockchain είναι η **επεκτασιμότητα**. Καθώς αυξάνεται ο αριθμός των συναλλαγών στο δίκτυο, αυξάνεται και ο χρόνος επεξεργασίας για κάθε συναλλαγή, με αποτέλεσμα μεγαλύτερους χρόνους συναλλαγών και υψηλότερα τέλη συναλλαγών.

4.5.2 Ιδιωτικά Blockchain

Ένα **ιδιωτικό** blockchain είναι ένα blockchain που ελέγχεται από έναν μόνο οργανισμό ή ομάδα οργανισμών. Σε αντίθεση με τα δημόσια blockchain, η πρόσβαση σε ένα ιδιωτικό blockchain είναι περιορισμένη και η συμμετοχή περιορίζεται μόνο σε **εξουσιοδοτημένα** μέλη. Τα ιδιωτικά blockchain χρησιμοποιούνται συνήθως για επιχειρηματικές εφαρμογές, όπου οι συμμετέχοντες πρέπει να μοιράζονται ευαίσθητα δεδομένα με ασφάλεια και ιδιωτικότητα. Παραδείγματα ιδιωτικών blockchain περιλαμβάνουν τις **Hyperledger Fabric**, **R3 Corda** και **Quorum**. Τα ιδιωτικά blockchain παρέχουν αρκετά πλεονεκτήματα έναντι των δημόσιων blockchain. Πρώτον, προσφέρουν υψηλότερη απόδοση συναλλαγών και χαμηλότερη καθυστέρηση, καθιστώντας τις πιο κατάλληλες για επιχειρηματικές εφαρμογές. Επιπλέον, τα ιδιωτικά blockchain μπλοκ επιτρέπουν στους συμμετέχοντες να διατηρούν τον έλεγχο

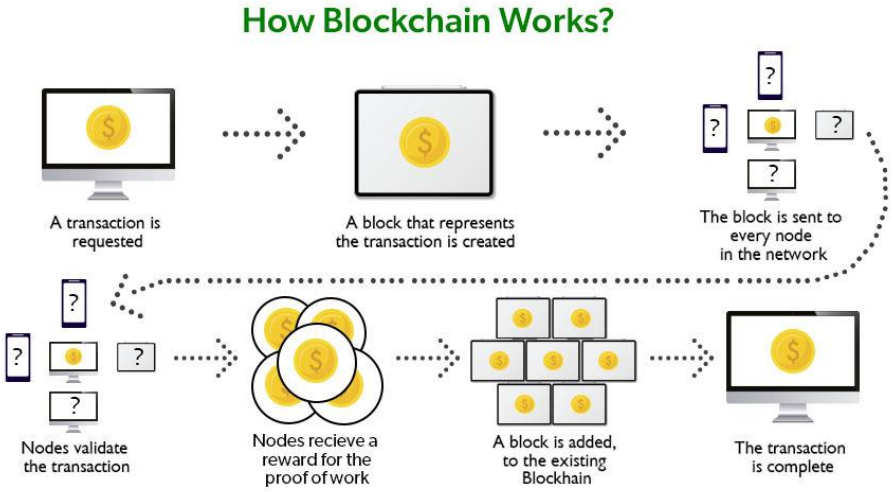
των δεδομένων τους και να διασφαλίζουν τη συμμόρφωση με τους κανονισμούς και τις νομικές απαιτήσεις. Ωστόσο, τα ιδιωτικά blockchain έχουν επίσης τους περιορισμούς τους. Είναι λιγότερο αποκεντρωμένα από τα δημόσια blockchain, γεγονός που μπορεί να οδηγήσει σε ανησυχίες σχετικά με την ασφάλεια και το αμετάβλητο των δεδομένων στο blockchain. Επιπλέον, ο κλειστός χαρακτήρας των ιδιωτικών blockchain μπορεί να περιορίσει τις δυνατότητές τους για καινοτομία και ανάπτυξη.

4.5.3 Υβριδικά Blockchain

Ένα **υβριδικό** blockchain συνδυάζει τα χαρακτηριστικά τόσο των δημόσιων όσο και των ιδιωτικών blockchain. Πρόκειται για ένα blockchain που επιτρέπει τόσο **δημόσιες** όσο και **ιδιωτικές συναλλαγές**, ανάλογα με το επίπεδο πρόσβασης που παρέχεται στους συμμετέχοντες. Σε ένα υβριδικό blockchain, ένα δημόσιο blockchain χρησιμοποιείται για την καταγραφή των δημόσιων συναλλαγών, ενώ τα ιδιωτικά blockchain χρησιμοποιούνται για ευαίσθητες ή εμπιστευτικές συναλλαγές. Τα υβριδικά blockchain παρέχουν τα πλεονεκτήματα τόσο των δημόσιων όσο και των ιδιωτικών blockchain. Προσφέρουν διαφάνεια και ασφάλεια για τις δημόσιες συναλλαγές, ενώ παρέχουν ιδιωτικότητα και έλεγχο για τις ιδιωτικές συναλλαγές. Τα υβριδικά blockchain είναι κατάλληλα για κλάδους όπως η υγειονομική περίθαλψη και τα χρηματοοικονομικά, όπου ορισμένες συναλλαγές πρέπει να είναι δημόσιες ενώ άλλες πρέπει να είναι ιδιωτικές. Ωστόσο, τα υβριδικά blockchain έχουν επίσης τους περιορισμούς τους. Είναι πιο **πολύπλοκα** από τα δημόσια ή τα ιδιωτικά blockchain, απαιτώντας μια πιο εξελιγμένη αρχιτεκτονική για τη διαχείριση των διαφορετικών τύπων συναλλαγών. Επιπλέον, τα υβριδικά blockchain μπορεί να υπόκεινται σε κανονιστικές και νομικές προκλήσεις, καθώς πρέπει να συμμορφώνονται με τους κανονισμούς που ισχύουν τόσο για τα δημόσια όσο και για τα ιδιωτικά blockchain.

4.6 Αρχιτεκτονική

Η τεχνολογία blockchain είναι μια καινοτόμος προσέγγιση στα κατανεμημένα συστήματα που επιτρέπει την ασφαλή και διαφανή τήρηση αρχείων. Στον πυρήνα της, το blockchain είναι μια αποκεντρωμένη βάση δεδομένων που αποθηκεύει τις συναλλαγές με ασφαλή και απαραβίαστο τρόπο. Σε αυτό το κεφάλαιο, θα συζητηθούν τα βασικά στοιχεία μιας αρχιτεκτονικής blockchain, συμπεριλαμβανομένων των κόμβων και της **τοπολογίας δικτύου**, των μπλοκ και των συναλλαγών, της εξόρυξης και της **επικύρωσης μπλοκ**, του **κατακερματισμού** και της **κρυπτογραφίας**, καθώς και των **μηχανισμών συναίνεσης**.



Εικόνα 8 Ροή προσθήκης συναλλαγής σε blockchain [30]

4.6.1 Κόμβοι και τοπολογία δικτύου

Οι **κόμβοι** είναι τα θεμελιώδη δομικά στοιχεία ενός δικτύου blockchain. Κάθε κόμβος είναι ένας υπολογιστής ή μια συσκευή που συμμετέχει στο δίκτυο επικυρώνοντας και μεταδίδοντας συναλλαγές σε άλλους κόμβους. Οι κόμβοι μπορούν να ταξινομηθούν σε δύο κατηγορίες: **πλήρεις** κόμβοι και **ελαφροί** κόμβοι. Οι πλήρεις κόμβοι διατηρούν ένα πλήρες αντίγραφο του βιβλίου blockchain και συμμετέχουν ενεργά στην επικύρωση των συναλλαγών και των μπλοκ. Οι ελαφροί κόμβοι, από την άλλη πλευρά, δεν διατηρούν πλήρες αντίγραφο του blockchain και βασίζονται στους πλήρεις κόμβους για την επικύρωση των συναλλαγών. Η τοπολογία δικτύου blockchain αναφέρεται στη δομή του δικτύου και στον τρόπο με τον οποίο οι κόμβοι συνδέονται μεταξύ τους. Οι συνήθεις τοπολογίες δικτύου περιλαμβάνουν τα ομότιμα (P2P), τα ιεραρχικά και τα δίκτυα πλέγματος.

4.6.2 Μπλοκ και συναλλαγές

Τα **μπλοκ** είναι οι δομές δεδομένων που αποθηκεύουν τις συναλλαγές στο blockchain. Κάθε μπλοκ περιέχει ένα **σύνολο συναλλαγών**, μια **χρονοσφραγίδα** και μια αναφορά στο **προηγούμενο** μπλοκ της αλυσίδας. Οι συναλλαγές είναι οι μονάδες δεδομένων που αντιπροσωπεύουν τη μετακίνηση ψηφιακών περιουσιακών στοιχείων ή πληροφοριών μεταξύ χρηστών στο blockchain. Κάθε συναλλαγή περιλαμβάνει έναν αποστολέα, έναν παραλήπτη, μια αξία και μια ψηφιακή υπογραφή που επαληθεύει τη γνησιότητά της [19].

4.6.3 Εξόρυξη και επικύρωση μπλοκ

Η **εξόρυξη** είναι η διαδικασία με την οποία προστίθενται νέα μπλοκ στο blockchain. Περιλαμβάνει την επίλυση ενός κρυπτογραφικού γρίφου που απαιτεί σημαντική υπολογιστική ισχύ και πόρους (PoW) ή τον στοιχιμαστισμό των κρυπτονομισμάτων (PoS). Οι **εξορυκτές** που επικυρώνουν επιτυχώς μια συναλλαγή λαμβάνουν μια **ανταμοιβή** και **τέλη συναλλαγών**. Η επικύρωση μπλοκ είναι η διαδικασία με την οποία οι κόμβοι του δικτύου επαληθεύουν τη γνησιότητα ενός μπλοκ πριν το προσθέσουν στην αλυσίδα μπλοκ. Η επικύρωση ενός μπλοκ περιλαμβάνει την επαλήθευση της εγκυρότητας των συναλλαγών του, της κρυπτογραφικής υπογραφής του και της συμμόρφωσής του με τους κανόνες συναίνεσης του δικτύου [19].

4.6.4 Κατακερματισμός και κρυπτογραφία

Ο **κατακερματισμός** και η **κρυπτογραφία** είναι οι βασικές τεχνολογίες που επιτρέπουν την ασφάλεια και την ακεραιότητα ενός blockchain. Ο κατακερματισμός, όπως αναλύθηκε, είναι η διαδικασία μετατροπής δεδομένων εισόδου σε έξοδο σταθερού μήκους που αντιπροσωπεύει τα αρχικά δεδομένα. Σε ένα blockchain, ο κατακερματισμός και η κρυπτογραφία χρησιμοποιούνται για την ασφάλεια των συναλλαγών, των μπλοκ και ολόκληρου του δικτύου.

4.6.5 Μηχανισμοί συναίνεσης

Οι **μηχανισμοί συναίνεσης** είναι οι κανόνες με τους οποίους οι κόμβοι σε ένα δίκτυο blockchain συμφωνούν σχετικά με την κατάσταση του blockchain. Καθορίζουν πώς προστίθενται νέα μπλοκ στην αλυσίδα μπλοκ, πώς επιλύονται οι συγκρούσεις και πώς επικυρώνονται οι συναλλαγές. Ορισμένοι κοινοί μηχανισμοί συναίνεσης που χρησιμοποιούνται σε δίκτυα blockchain περιλαμβάνουν το **PoW**, **PoS** και το **DPoS**.

4.6.5.1 Proof of Work

Ο αλγόριθμος **Proof of Work** είναι ο αρχικός και πιο γνωστός αλγόριθμος συναίνεσης που χρησιμοποιείται στα δίκτυα blockchain. Παρουσιάστηκε για πρώτη φορά από τον Satoshi Nakamoto στο whitepaper του Bitcoin [13]. Σε ένα σύστημα PoW, οι εξορυκτές ανταγωνίζονται για την επίλυση ενός κρυπτογραφικού **γρίφου** χρησιμοποιώντας **υπολογιστική ισχύ**. Ο πρώτος εξορυκτής που θα λύσει τον γρίφο και θα επικυρώσει ένα νέο μπλοκ συναλλαγών ανταμείβεται με μια ανταμοιβή μπλοκ και τέλη συναλλαγής [18][17]. Η διαδικασία επίλυσης του γρίφου ονομάζεται **εξόρυξη**. Το PoW είναι γνωστό ότι είναι ασφαλές και αξιόπιστο, αλλά απαιτεί σημαντικούς υπολογιστικούς πόρους και καταναλώνει πολλή ενέργεια.

4.6.5.2 Proof of Stake

Ο αλγόριθμος **Proof of Stake** είναι ένας νεότερος αλγόριθμος συναίνεσης που αποσκοπεί στην αντιμετώπιση ορισμένων από τους περιορισμούς του PoW. Σε ένα σύστημα PoS, οι επικυρωτές επιλέγονται για να επικυρώσουν νέα μπλοκ με βάση το ποσό του κρυπτονομίσματος που κατέχουν ή "**στοιχηματίζουν**" στο δίκτυο. Οι επικυρωτές έχουν κίνητρο να ενεργούν προς το συμφέρον του δικτύου, καθώς μπορούν να χάσουν το μερίδιό τους εάν επικυρώσουν δόλιες συναλλαγές [18]. Το PoS θεωρείται **ενεργειακά αποδοτικότερο** από το PoW, αλλά έχει επικριθεί ότι ευνοεί τους πλούσιους επικυρωτές και ενδεχομένως οδηγεί σε **συγκεντρωτισμό**.

4.6.5.3 Delegated Proof of Stake

Το **Delegated Proof of Stake** είναι μια παραλλαγή του PoS που εισάγει έναν μηχανισμό για την **εκλογή** μιας μικρότερης **ομάδας επικυρωτών** για την επικύρωση συναλλαγών εκ μέρους ολόκληρου του δικτύου. Οι κάτοχοι token μπορούν να ψηφίσουν τους επικυρωτές της προτίμησής τους, οι οποίοι στη συνέχεια είναι υπεύθυνοι για τη συντήρηση του δικτύου και την επικύρωση νέων μπλοκ [18]. Το DPoS έχει σχεδιαστεί για να είναι πιο αποτελεσματικό από το PoW και το PoS, καθώς μειώνει τον αριθμό των επικυρωτών που απαιτούνται για την επίτευξη συναίνεσης. Ωστόσο, έχει επικριθεί για το γεγονός ότι ενδέχεται να οδηγήσει σε συγκεντρωτισμό και να δώσει υπερβολική εξουσία σε μια μικρή ομάδα επικυρωτών.

4.6.6 Σύνοψη

Συμπερασματικά, η αρχιτεκτονική blockchain αποτελείται από διάφορα κρίσιμα στοιχεία που συνεργάζονται για να διασφαλίσουν την ασφάλεια και την ακεραιότητα του δικτύου. Οι κόμβοι, τα μπλοκ, οι συναλλαγές, η εξόρυξη, ο κατακερματισμός, η κρυπτογραφία και οι μηχανισμοί συναίνεσης διαδραματίζουν όλοι ζωτικό ρόλο στην ενεργοποίηση της αποκεντρωμένης και χωρίς εμπιστοσύνη φύσης της τεχνολογίας blockchain. Η κατανόηση αυτών των στοιχείων είναι ζωτικής σημασίας για τον σχεδιασμό και την εφαρμογή αποτελεσματικών λύσεων blockchain.

4.7 Έξυπνα συμβόλαια

Τα τελευταία χρόνια, η έλευση της τεχνολογίας blockchain έχει φέρει επανάσταση στον τρόπο με τον οποίο πραγματοποιούμε συναλλαγές και εγκαθιδρύουμε εμπιστοσύνη σε διάφορους κλάδους. Στο επίκεντρο αυτής της επανάστασης βρίσκεται η έννοια των ΕΣ. Τα ΕΣ είναι **αυτοεκτελούμενες συμφωνίες** με τους **όρους** και τις **προϋποθέσεις** της συμφωνίας απευθείας γραμμένες στον **κώδικα**. Λειτουργούν σε δίκτυα blockchain, εξασφαλίζοντας διαφάνεια, αμεταβλητότητα και αυτοματοποίηση των συμβατικών υποχρεώσεων.

4.7.1 Ορισμός

Ένα ΕΣ μπορεί να οριστεί ως ένα πρόγραμμα υπολογιστή που διευκολύνει, επαληθεύει και επιβάλλει τη διαπραγμάτευση και την εκτέλεση μιας συμφωνίας μεταξύ των μερών. Αυτά τα συμβόλαια κωδικοποιούνται με αποκεντρωμένο τρόπο σε ένα blockchain, όπου οι **όροι** του συμβολαίου είναι **προκαθορισμένοι** και η **εκτέλεση** του συμβολαίου ενεργοποιείται **αυτόματα** όταν πληρούνται οι καθορισμένες προϋποθέσεις. Οι συμβατικοί όροι, η επιχειρηματική λογική και τα αποτελέσματα είναι όλα ενσωματωμένα στον κώδικα, παρέχοντας μια αξιόπιστη και ανθεκτική στην παραποίηση μέθοδο για τη διενέργεια συναλλαγών.

4.7.2 Ιστορική αναδρομή

Η έννοια των ΕΣ προτάθηκε για πρώτη φορά από τον επιστήμονα πληροφορικής **Nick Szabo** το 1994 [20], πολύ πριν από την εμφάνιση της τεχνολογίας blockchain. Ο Szabo οραματίστηκε αυτοεκτελούμενα συμβόλαια βασισμένα σε πρωτόκολλα υπολογιστών, όπου οι συμβατικές ρήτρες και υποχρεώσεις θα γράφονταν απευθείας στον κώδικα. Ωστόσο, μόνο με την έλευση της τεχνολογίας blockchain, ιδίως με την εισαγωγή του **Ethereum** το 2015, τα ΕΣ έγιναν ευρέως εφαρμόσιμα και προσβάσιμα.

4.7.3 Πλεονεκτήματα

Τα ΕΣ προσφέρουν πολλά πλεονεκτήματα σε σχέση με τα παραδοσιακές συμβατικά συμβόλαια. Ορισμένα βασικά πλεονεκτήματα περιλαμβάνουν [20]:

4.7.3.1 Αποτελεσματικότητα

Τα ΕΣ αυτοματοποιούν την εκτέλεση των συμβάσεων, καταργώντας την ανάγκη για μεσάζοντες και χειροκίνητη επεξεργασία. Αυτό μειώνει το κόστος, επιταχύνει τις συναλλαγές και εξαλείφει τα ανθρώπινα λάθη.

4.7.3.2 Διαφάνεια

Η αποκεντρωμένη φύση του blockchain εξασφαλίζει διαφάνεια, καθώς ο κώδικας και το ιστορικό των συναλλαγών είναι ορατά σε όλους τους συμμετέχοντες. Αυτό ενισχύει την εμπιστοσύνη, καθώς τα μέρη μπορούν να επαληθεύουν ανεξάρτητα τους όρους και την εκτέλεση της σύμβασης.

4.7.3.3 Αυτοματοποίηση

Τα ΕΣ επιτρέπουν την αυτοματοποιημένη εκτέλεση βάσει προκαθορισμένων συνθηκών. Αυτό επιτρέπει την αυτοεπιβεβαίωση των συμφωνιών, μειώνοντας την εξάρτηση από τη χειροκίνητη παρέμβαση και ενισχύοντας την αποτελεσματικότητα των διαδικασιών.

4.7.3.4 Ασφάλεια

Αξιοποιώντας τεχνικές κρυπτογράφησης, τα ΕΣ παρέχουν υψηλό επίπεδο ασφάλειας και ακεραιότητας. Η αμεταβλητότητα του blockchain διασφαλίζει ότι μόλις αναπτυχθεί ένα ΕΣ, δεν μπορεί να τροποποιηθεί, παρέχοντας ένα ανθεκτικό στην αλλοίωση και ελέγξιμο αρχείο συναλλαγών.

4.7.4 Λειτουργία

Η κατανόηση των αρχών λειτουργίας των ΕΣ είναι απαραίτητη για την κατανόηση της διαδικασίας εκτέλεσης και επικύρωσής τους. Σε αυτή την ενότητα, θα εξεταστεί ο τρόπος εκτέλεσης και επικύρωσης των ΕΣ και ο ρόλος των ανθρακωρύχων/επικυρωτών.

4.7.4.1 Διαδικασία εκτέλεσης και επικύρωσης

Η εκτέλεση ενός ΕΣ περιλαμβάνει διάφορα βήματα:

4.7.4.1.1 ***Ανάπτυξη***

Ένα ΕΣ αναπτύσσεται σε ένα δίκτυο blockchain με τη δημιουργία μιας συναλλαγής που περιέχει τον κώδικα του συμβολαίου και τυχόν αρχικές παραμέτρους ή τιμές.

4.7.4.1.2 ***Ενεργοποίηση***

Αφού αναπτυχθεί, ένα ΕΣ μπορεί να ενεργοποιηθεί από ένα συγκεκριμένο γεγονός ή συνθήκη. Το γεγονός αυτό μπορεί να είναι μια συναλλαγή, ένας συγκεκριμένος χρόνος ή μια εξωτερική είσοδος.

4.7.4.1.3 ***Επαλήθευση***

Όταν συμβεί ένα συμβάν ενεργοποίησης, εκτελείται ο κώδικας του ΕΣ και επικυρώνεται η λογική του. Αυτή η επαλήθευση διασφαλίζει ότι πληρούνται οι συνθήκες και οι απαιτήσεις που ορίζονται στο συμβόλαιο.

4.7.4.1.4 ***Μετάβαση κατάστασης***

Με βάση τα αποτελέσματα της εκτέλεσης και της επαλήθευσης, η κατάσταση του ΕΣ μπορεί να αλλάξει. Για παράδειγμα, μπορεί να μεταφερθούν κεφάλαια, να ενημερωθούν δεδομένα ή να δημιουργηθούν νέα συμβόλαια.

4.7.4.1.5 ***Καταγραφή***

Οι λεπτομέρειες της εκτέλεσης του ΕΣ και οι επακόλουθες αλλαγές της κατάστασής του καταγράφονται στο blockchain, δημιουργώντας ένα αμετάβλητο και διαφανές αρχείο της συναλλαγής.

4.7.4.2 **Ρόλος εξορυκτών/επικυρωτών**

Στα δίκτυα blockchain που χρησιμοποιούν έναν μηχανισμό συναίνεσης όπως το PoW ή το PoS, οι εξορυκτές ή οι επικυρωτές παίζουν καθοριστικό ρόλο στην εκτέλεση και επικύρωση ΕΣ. Οι εξορυκτές (στο PoW) ή οι επικυρωτές (στο PoS) ανταγωνίζονται για την επίλυση πολύπλοκων μαθηματικών γρίφων ή στοιχηματίζουν τα κρυπτονομίσματα που κατέχουν για να αποκτήσουν το δικαίωμα να επικυρώνουν συναλλαγές και να τις προσθέτουν στο blockchain. Η εκτέλεση και η επικύρωση ΕΣ αποτελούν μέρος αυτής της διαδικασίας. Οι εξορυκτές/επικυρωτές διασφαλίζουν ότι ο **κώδικας** του ΕΣ **εκτελείται σωστά** και τα αποτελέσματα είναι συνεπή σε όλο το δίκτυο. Επαληθεύουν επίσης τη **γνησιότητα** των **ψηφιακών υπογραφών** και διασφαλίζουν ότι πληρούνται οι όροι του συμβολαίου πριν επιτρέψουν αλλαγές κατάστασης.

4.7.5 Έξυπνα συμβόλαια Ethereum

Το **Ethereum** αποτελεί την πιο διαδεδομένη και ώριμη πλατφόρμα ανάπτυξης ΕΣ. Υλοποιημένα με τη χρήση της γλώσσας προγραμματισμού Solidity, τα ΕΣ του Ethereum αξιοποιούν την εικονική μηχανή του Ethereum (EVM) για την εκτέλεση κώδικα με ασφαλή και ντετερμινιστικό τρόπο. Οι δυνατότητες ΕΣ του Ethereum έχουν διαδραματίσει καθοριστικό ρόλο στην ανάπτυξη του οικοσυστήματος blockchain, δίνοντας τη δυνατότητα στους προγραμματιστές να δημιουργήσουν καινοτόμες και αποκεντρωμένες λύσεις σε ένα ευρύ φάσμα βιομηχανιών.

4.7.5.1 Solidity (Ethereum)

Η **Solidity** είναι μια γλώσσα προγραμματισμού υψηλού επιπέδου ειδικά σχεδιασμένη για τη συγγραφή ΕΣ στην πλατφόρμα Ethereum. Είναι στατικά τυποποιημένη και υποστηρίζει κληρονομικότητα, βιβλιοθήκες και σύνθετους τύπους που ορίζονται από τον χρήστη. Ο κώδικας Solidity μεταγλωττίζεται σε bytecode που μπορεί να εκτελεστεί στην εικονική μηχανή Ethereum (EVM).

Το Solidity παρέχει διάφορα χαρακτηριστικά και εργαλεία για τον ορισμό της λογικής ενός ΕΣ, όπως:

- **State variables**: Μεταβλητές για την αποθήκευση και τη διατήρηση της κατάστασης του συμβολαίου.
- **Functions**: Μπλοκ κώδικα που καθορίζουν τη συμπεριφορά και τις ενέργειες του συμβολαίου.
- **Events**: Μηχανισμοί για την εκπομπή και την καταγραφή συμβάντων που συμβαίνουν στο πλαίσιο του συμβολαίου.
- **Modifiers**: Προκαθορισμένες συνθήκες που μπορούν να εφαρμοστούν σε συναρτήσεις για έλεγχο πρόσβασης ή επικύρωση.
- **Libraries**: Επαναχρησιμοποιήσιμα στοιχεία κώδικα που μπορούν να εισαχθούν και να χρησιμοποιηθούν από πολλαπλές συμβάσεις.

4.7.6 Σύνοψη

Εν κατακλείδι, τα ΕΣ παρουσιάζουν μια εξαιρετικά αποτελεσματική λύση για την αντιμετώπιση των προκλήσεων αυθεντικοποίησης των συσκευών IoT, αξιοποιώντας τα πλεονεκτήματα ασφάλειας της τεχνολογίας blockchain, σε συνδυασμό με την ευελιξία και τη λειτουργικότητα που παρέχουν οι παραδοσιακές γλώσσες προγραμματισμού. Η εκτεταμένη κοινότητα προγραμματιστών, η ολοκληρωμένη τεκμηρίωση και οι άφθονοι πόροι που σχετίζονται με το Solidity το καθιστούν ως τη βέλτιστη επιλογή για την ανάπτυξη ΕΣ.

Κεφάλαιο 5: Αυθεντικοποίηση IoT συσκευών

5.1 Εισαγωγή

Η αυθεντικοποίηση των IoT συσκευών αποτελεί ένα κρίσιμο ζήτημα λόγω του μεγάλου αριθμού των συσκευών και της ποικιλίας των πρωτοκόλλων επικοινωνίας που χρησιμοποιούνται στα συστήματα IoT. Πολλές συσκευές IoT εγκαθίστανται σε ανοικτά περιβάλλοντα, καθιστώντας τις ευάλωτες σε επιθέσεις από μη εξουσιοδοτημένους χρήστες ή κακόβουλα προγράμματα.

5.2 Το πρόβλημα της αυθεντικοποίησης

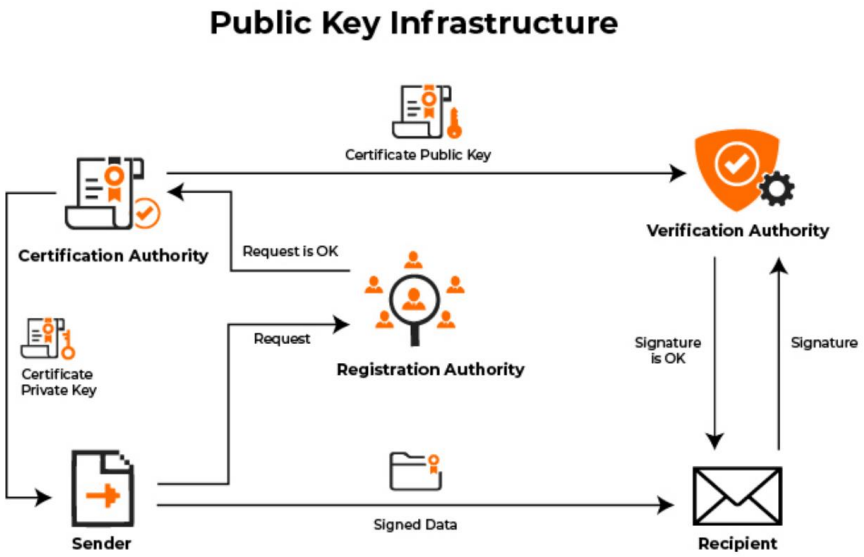
Το κύριο πρόβλημα με την αυθεντικοποίηση στα συστήματα IoT είναι ότι πολλές συσκευές IoT δεν διαθέτουν την απαραίτητη επεξεργαστική ισχύ και μνήμη για να υποστηρίξουν προηγμένα χαρακτηριστικά ασφαλείας, όπως η ισχυρή κρυπτογράφηση και οι ψηφιακές πιστοποιήσεις. Επιπλέον, οι συσκευές IoT συχνά χρησιμοποιούν ελαφριά πρωτόκολλα επικοινωνίας που δεν έχουν σχεδιαστεί για να χειρίζονται περίπλοκους μηχανισμούς ασφαλείας. Ένα άλλο πρόβλημα είναι ότι πολλές συσκευές IoT σχεδιάζονται για να λειτουργούν για μεγάλα χρονικά διαστήματα χωρίς συντήρηση ή ενημερώσεις, καθιστώντας τις ευάλωτες σε προβλήματα ασφάλειας που μπορεί να παραμείνουν ανεντόπιστα για μεγάλα χρονικά διαστήματα. Επιπλέον, πολλές συσκευές IoT είναι εγκατεστημένες σε ανασφαλή δίκτυα, καθιστώντας τις εύκολους στόχους σε επιθέσεις που μπορούν να εκμεταλλευτούν τους αδύναμους μηχανισμούς πιστοποίησης για να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα ή να αναλάβουν τον έλεγχο της συσκευής.

5.3 Εναλλακτικές λύσεις

Το πρόβλημα της αυθεντικοποίησης έχει απασχολήσει εδώ και χρόνια την ερευνητική κοινότητα και υπάρχουν ήδη αρκετές λύσεις. Μερικές από αυτές δύνανται να χρησιμοποιηθούν και στο πρόβλημα της αυθεντικοποίησης IoT συσκευών. Οι σημαντικότερες εκ των οποίων είναι οι εξής:

5.3.1 Public Key Infrastructure (PKI)

Το **Public Key Infrastructure (PKI)** είναι ένα πρωτόκολλο ασφάλειας που χρησιμοποιείται για να ασφαλίσει την ψηφιακή επικοινωνία μέσω δικτύων, όπως το Διαδίκτυο. Το PKI καθιστά δυνατή την ασφαλή επικοινωνία με τη χρήση ενός συνδυασμού δημόσιων και ιδιωτικών κλειδιών, ψηφιακών πιστοποιητικών, και μιας αξιόπιστης τρίτης αρχής που ονομάζεται Αρχή Πιστοποίησης (Certificate Authority - CA) [21]. Ο κύκλος ζωής της αυθεντικοποίησης επικοινωνίας με τη χρήση του PKI είναι ο εξής:



Εικόνα 9 Ροή μεταφοράς δεδομένων με χρήση PKI [31]

5.3.1.1 **Δημιουργία Κλειδιών**

Το πρώτο βήμα στο πρωτόκολλο PKI είναι η δημιουργία ενός ζεύγους δημόσιων και ιδιωτικών κλειδιών. Ο χρήστης διατηρεί το ιδιωτικό κλειδί μυστικό, και το δημόσιο κλειδί διανέμεται ελεύθερα.

5.3.1.2 **Αίτηση Ψηφιακού Πιστοποιητικού**

Όταν ένας χρήστης επιθυμεί να συμμετάσχει σε μια ασφαλή επικοινωνία, ζητά ένα ψηφιακό πιστοποιητικό από μια αξιόπιστη CA. Η ταυτότητα του χρήστη επαληθεύεται από την CA, και αν η επαλήθευση είναι επιτυχής, η CA εκδίδει ένα ψηφιακό πιστοποιητικό που περιλαμβάνει το δημόσιο κλειδί του χρήστη, καθώς και πληροφορίες για το χρήστη.

5.3.1.3 **Διανομή Ψηφιακού Πιστοποιητικού**

Ο χρήστης λαμβάνει το ψηφιακό πιστοποιητικό από την CA και το διανέμει στα μέρη με τα οποία επιθυμεί να επικοινωνήσει.

5.3.1.4 **Ασφαλής Επικοινωνία**

Όταν δύο μέρη θέλουν να επικοινωνήσουν ασφαλώς, ανταλλάσσουν τα ψηφιακά πιστοποιητικά τους. Κάθε μέρος επαληθεύει το ψηφιακό πιστοποιητικό του άλλου χρησιμοποιώντας το δημόσιο κλειδί της CA. Έπειτα χρησιμοποιούν τα δημόσια κλειδιά του ενός άλλου για να κρυπτογραφήσουν τα δεδομένα, τα οποία μπορούν να αποκρυπτογραφηθούν μόνο από τον αποδέκτη χρησιμοποιώντας το ιδιωτικό κλειδί του.

5.3.1.5 **Ανάκληση Πιστοποιητικού**

Εάν το ιδιωτικό κλειδί ενός χρήστη διαρρεύσει, η CA μπορεί να ανακαλέσει το ψηφιακό του πιστοποιητικό, καθιστώντας το άκυρο. Η CA δημοσιεύει μια λίστα ανακλήσεων πιστοποιητικών, η οποία ονομάζεται Λίστα Ανάκλησης Πιστοποιητικών (CRL), και ενημερώνεται περιοδικά από τους πελάτες για να ελέγχουν τα ανακληθέντα πιστοποιητικά.

Το PKI αποτελεί ένα από τα πιο διαδεδομένα πρωτόκολλα αυθεντικοποίησης, ωστόσο η χρήση του στο IoT παρουσιάζει κάποιες προκλήσεις. Συγκεκριμένα το PKI βασίζεται στην CA για την επικύρωση τον ψηφιακών πιστοποιητικών και σε συνδυασμό με τον μεγάλο αριθμό συσκευών που προϋποθέτει το IoT δημιουργούνται σημαντικά προβλήματα. Ένα πρόβλημα αποτελεί το αυξημένο κόστος σε υπολογιστικούς και αποθηκευτικούς πόρους για την σωστή λειτουργία της CA. Προβληματικό επίσης αποτελεί το κόστος διαχείρισης των ψηφιακών πιστοποιητικών (συχνή δημιουργία, ανάκληση). Τέλος πρόβλημα αποτελεί το γεγονός πως οι IoT συσκευές συνήθως δεν έχουν τους απαραίτητους υπολογιστικούς πόρους για να εκτελέσουν τα πρωτόκολλα του PKI σε εύλογο χρονικό διάστημα.

5.3.2 Token Based Authentication

Η **αυθεντικοποίηση βασιζόμενη σε tokens (Token Based Authentication)** είναι ένα μηχανισμός που χρησιμοποιείται ευρέως για την ασφαλή πιστοποίηση συσκευών IoT. Απαιτεί τη χρήση tokens, τα οποία είναι μοναδικές και τυχαία δημιουργημένες συμβολοσειρές που λειτουργούν ως ψηφιακά κλειδιά για την πρόσβαση στη συσκευή IoT. Η επίτευξη της διαδικασίας της αυθεντικοποίησης προϋποθέτει την ύπαρξη μιας **Αρχής Κρατήσεων** (RA) που είναι υπεύθυνη για τη **δημιουργία** και το **διαμοιρασμό** των tokens [22]. Η διαδικασία της αυθεντικοποίησης βασιζόμενη σε tokens είναι η εξής:

Εικόνα 10 Ροή ασφαλούς επικοινωνίας με Token Based Authentication [32]

5.3.2.1 **Πιστοποίηση χρήστη**

Ο χρήστης πρώτα πιστοποιείται με την RA χρησιμοποιώντας τα στοιχεία σύνδεσής του και ζητά την πρόσβαση σε κάποιο πόρο.

5.3.2.2 **Δημιουργία token**

Μετά την επιτυχή πιστοποίηση, ο διακομιστής δημιουργεί ένα μοναδικό token που δίνει πρόσβαση στον χρήστη στον πόρο που έχει ζητήσει και το επιστρέφει στον χρήστη.

5.3.2.3 **Μετάδοση token**

Ο διακομιστής στέλνει στη συνέχεια το token στη συσκευή IoT (που παρέχει τον ζητηθέντα πόρο) συνήθως μέσω κάποιου ασφαλούς καναλιού.

5.3.2.4 **Αποθήκευση token**
Η συσκευή IoT αποθηκεύει το token με ασφάλεια.

5.3.2.5 **Χρήση token**
Όταν ο χρήστης θέλει να έχει πρόσβαση στον πόρο (της IoT συσκευής), παρουσιάζει το token στη συσκευή. Η συσκευή επιβεβαιώνει στη συνέχεια το token έναντι του αποθηκευμένου token και επιτρέπει την πρόσβαση αν τα κλειδιά ταιριάζουν.

5.3.2.6 **Λήξη και ανανέωση token**
Τα token έχουν περιορισμένη ισχύ. Μόλις λήξει το token, ο χρήστης χρειάζεται να επαναπιστοποιηθεί για να δημιουργηθεί ένα καινούριο token που θα του επιτρέψει εκ νέου την πρόσβαση στον πόρο.

Η διαδικασία της αυθεντικοποίησης με τη χρήση tokens λειτουργεί με διαφορετικό τρόπο από το PKI. Συγκεκριμένα, αντί να γίνεται υπογραφή και εκπομπή των δεδομένων από την IoT συσκευή, η συσκευή μεταδίδει τα δεδομένα κατά παραγγελία. Αυτό λύνει σε κάποιο βαθμό το πρόβλημα της κλιμακωσιμότητας καθώς η διαχείριση (δημιουργία, διαμοιρασμός και αποθήκευση) των tokens θα λαμβάνει μέρος αποκλειστικά όταν κάποιος αιτηθεί πρόσβαση στον συγκεκριμένο πόρο. Ωστόσο και αυτή η λύση ακολουθείται από μειονεκτήματα. Συγκεκριμένα αυξάνονται σημαντικά οι απαιτήσεις σε υπολογιστική ισχύ αλλά και αποθηκευτικό χώρο στις IoT συσκευές που διαμοιράζουν δεδομένα που πρέπει να υπάρχει πρόσβαση από πολλούς χρήστες, καθώς υπάρχει η ανάγκη διαχείρισης του αυξημένου όγκου token. Επίσης καθώς τα tokens έχουν συγκεκριμένη διάρκεια ζωής προστίθεται το κόστος ανανέωσης τους. Τέλος ο διαμοιρασμός των δεδομένων δεν γίνεται με εκπομπή (broadcast) οι IoT συσκευές είναι πιθανό να μην έχουν τη δυνατότητα να εξυπηρετήσουν την αίτηση για παροχή δεδομένων όταν υπάρχει αυξημένη κίνηση.

Κεφάλαιο 6: Πρόταση με χρήση έξυπνων συμβολαίων

6.1 Εισαγωγή

Όπως αναπτύχθηκε και στο προηγούμενο κεφάλαιο, είναι επιφανές πως η αυθεντικοποίηση IoT συσκευών αποτελεί ένα αρκετά κρίσιμο πρόβλημα και πως οι υπάρχουσες λύσεις στο πρόβλημα παρουσιάζουν δυσκολίες στην ευρεία υιοθέτηση τους. Συγκεκριμένα αποτελούν λύσεις που έχουν αποδειχθεί χρήσιμες και αποδοτικές. Ωστόσο ο τρόπος λειτουργίας τους, τις περιορίζει στις αυξημένες ανάγκες του IoT για κλιμακωσιμότητα.

6.2 Πρόταση λύσης

Γνωρίζοντας πως η χρήση της τεχνολογίας του blockchain για την αυθεντικοποίηση των IoT συσκευών αποτελεί μια αρκετά υποσχόμενη λύση στο πρόβλημα. Συγκεκριμένα η χρήση του blockchain προσφέρει ασφάλεια σε ένα σύστημα με τους παρακάτω τρόπους:

Αποκέντρωση: Το blockchain είναι ένα κατανεμημένο σύστημα που αποτελείται από ένα μεγάλο αριθμό κόμβων σε ένα αποκεντρωμένο δίκτυο. Αυτό καθιστά δυσκολότερο για επιτιθέμενους να παραβιάσουν το δίκτυο, καθώς δεν υπάρχει καμία μοναδική αδύναμη στιγμή που μπορεί να επιτεθεί.

Αμεταβλητότητα: Μόλις τα δεδομένα προστίθενται στο blockchain, δεν μπορούν να τροποποιηθούν ή να διαγραφούν χωρίς ανίχνευση. Αυτό καθιστά το blockchain ένα ιδανικό σύστημα για την καταγραφή και την αποθήκευση πληροφοριών που χρειάζονται ανθεκτικότητα στην παραβίαση.

Αλγόριθμοι συναίνεσης: Το blockchain χρησιμοποιεί αλγόριθμους συναίνεσης για να διασφαλίσει ότι όλοι οι κόμβοι στο δίκτυο συμφωνούν στην κατάσταση των δεδομένων. Αυτό καθιστά δυσκολότερο για επιτιθέμενους να επηρεάσουν το blockchain καθώς θα ήταν αναγκαίο να έχουν στη διάθεση τους την πλειοψηφία των πόρων του δικτύου κόμβων.

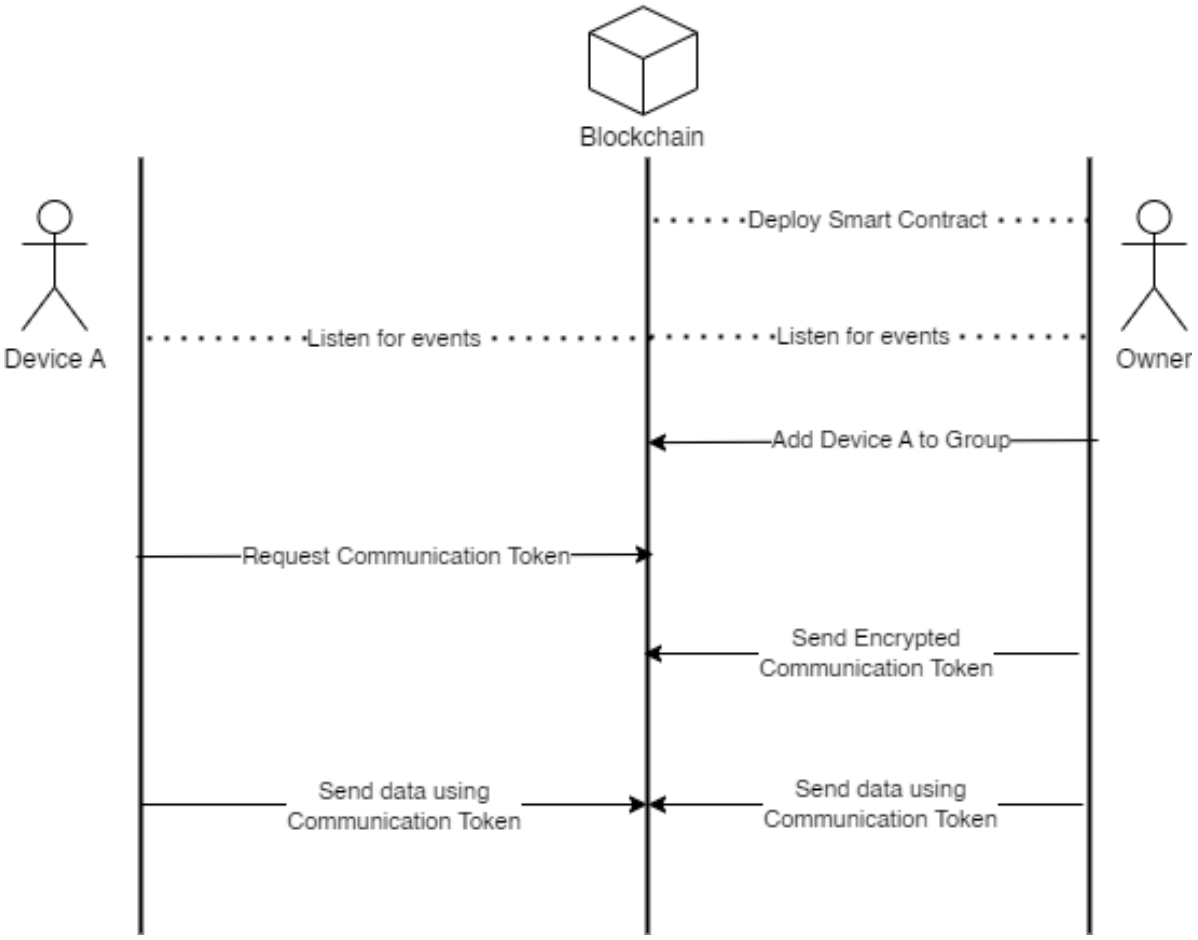
Κρυπτογραφία: Οι συναλλαγές στο blockchain υπογράφονται με τη χρήση ασύμμετρης κρυπτογράφησης επικυρώνοντας την ταυτότητα των χρηστών του δικτύου. Αυτό δίνει τη δυνατότητα ταυτοποίησης της γνησιότητας των δεδομένων που περιέχονται σε μία συναλλαγή.

Όπως γίνεται αντιληπτό το blockchain μέσω των εγγενών ιδιοτήτων του είναι σε θέση να λύσει το πρόβλημα της αυθεντικοποίησης των IoT συσκευών παρέχοντας τη δυνατότητα για ασφαλή διαμοιρασμό και αποθήκευση των δεδομένων που παράγουν οι IoT συσκευές. Άλλο ένα πλεονέκτημα που απορρέει από τις εγγενής ιδιότητες του blockchain είναι αυτό της κλιμακωσιμότητας λόγω της αποκεντρωμένης φύσης του, καθιστώντας ιδανικό για την αποθήκευση της ογκώδους ποσότητας πληροφορίας που παράγεται από τα συστήματα IoT.

Μια ακόμη ιδιότητα του blockchain είναι πως τα δεδομένα που είναι αποθηκευμένα σε αυτό με τη μορφή συναλλαγών είναι δημοσίως διαθέσιμα. Αυτό σημαίνει πως με τη χρήση του blockchain δίδεται μεν η δυνατότητα για την αυθεντικοποίηση των IoT συσκευών, αλλά χάνεται η δυνατότητα για τη διαχείριση της πρόσβασης στα δεδομένα αυτά. Η παρακάτω λύση έχει ως σκοπό την επαναφορά της δυνατότητας διαμοιρασμού πληροφοριών με ελεγχόμενο τρόπο.

Για να υπάρξει η δυνατότητα ασφαλή διαμοιρασμού δεδομένων θα δημιουργηθούν ομάδες που θα έχουν τη δυνατότητα να επικοινωνούν με ασφαλή τρόπο σε ένα ιδιωτικό κανάλι επικοινωνίας. Ο τρόπος δημιουργίας και χρήσης του ιδιωτικού καναλιού είναι ο παρακάτω:

- Ένας κόμβος δημιουργεί το κανάλι επικοινωνίας ανεβάζοντας το ΕΣ στο blockchain (πιθανότατα ο κόμβος αυτός να μην αποτελεί μια IoT συσκευή). Ο κόμβος αυτός είναι ο Ιδιοκτήτης.
- Ο Ιδιοκτήτης έχει τη δυνατότητα να προσθέτει άλλους κόμβους στο κανάλι επικοινωνίας. Έτσι προσθέτει στο κανάλι τη συσκευή Α.
- Η συσκευή Α αιτείται από τον Ιδιοκτήτη το token επικοινωνίας.
- Ο Ιδιοκτήτης κρυπτογραφεί το token επικοινωνίας με το δημόσιο κλειδί της συσκευής Α που αιτήθηκε το token και το στέλνει στη συσκευή (η αποστολή γίνεται μέσω του ίδιου του δικτύου blockchain).
- Η συσκευή Α λαμβάνει το token επικοινωνίας και το αποκρυπτογραφεί χρησιμοποιώντας το ιδιωτικό κλειδί της.
- Τόσο ο Ιδιοκτήτης, όσο και η συσκευή Α έχουν τη δυνατότητα αποστολής δεδομένων κρυπτογραφώντας τα δεδομένα με κάποιον συμμετρικό αλγόριθμο κρυπτογράφησης και το token επικοινωνίας.



Σχήμα 1Ροή ασφαλούς επικοινωνίας με χρήση blockchain

Η παραπάνω λύση δίνει τη δυνατότητα εκμετάλλευσης των πλεονεκτημάτων ασφαλείας του blockchain, ενώ παράλληλα δίδεται η δυνατότητα για ασφαλή διαμοιρασμό πληροφοριών σε μια αυστηρώς ορισμένη ομάδα παραληπτών.

6.3 Τεχνολογίες και εργαλεία που χρησιμοποιήθηκαν

Για την υλοποίηση της παραπάνω λύσης στο πρόβλημα της αυθεντικοποίησης IoT συσκευών θα γίνει χρήση διαφόρων τεχνολογιών και εργαλείων. Στο κεφάλαιο αυτό θα αναλυθούν τα εργαλεία και οι τεχνολογίες αυτές.

6.3.1 Ethereum

Το **Ethereum** είναι μια αποκεντρωμένη πλατφόρμα blockchain που επιτρέπει τη δημιουργία και εκτέλεση ΕΣ. Παρουσιάστηκε το 2013 από τον **Gavin Wood** [15], το Ethereum έφερε επανάσταση στον κόσμο της τεχνολογίας blockchain επεκτείνοντας τις δυνατότητές του πέρα από ένα απλό ψηφιακό νόμισμα. Βασισμένο στις αρχές της διαφάνειας, της ασφάλειας και της αμεταβλητότητας, το Ethereum προσφέρει μια αποκεντρωμένη εικονική μηχανή που ονομάζεται Ethereum Virtual Machine (EVM) και επιτρέπει στους προγραμματιστές να δημιουργούν και να αναπτύσσουν αποκεντρωμένες εφαρμογές (dApps) στην πλατφόρμα του. Το Ethereum εισήγαγε το εγγενές κρυπτονόμισμα που ονομάζεται **Ether** (ETH), το οποίο χρησιμεύει τόσο ως ψηφιακό νόμισμα όσο και ως μάρκα χρησιμότητας στο δίκτυο Ethereum.

6.3.2 Ganache

Το **Ganache** είναι ένα λογισμικό που χρησιμοποιείται για την ανάπτυξη, τον έλεγχο και την αποσφαλμάτωση εφαρμογών blockchain του Ethereum. Παρέχει ένα περιβάλλον **τοπικού blockchain** που προσομοιώνει τη συμπεριφορά ενός πραγματικού δικτύου Ethereum, επιτρέποντας στους προγραμματιστές να δημιουργήσουν και να δοκιμάσουν τα ΕΣ και τις αποκεντρωμένες εφαρμογές τους σε ένα ασφαλές και ελεγχόμενο περιβάλλον. Στην υλοποίηση θα χρησιμοποιηθεί ως ένα εικονικό δίκτυο blockchain για την ανάπτυξη και τον έλεγχο λειτουργίας του ΕΣ.

6.3.3 Metamask

Το **MetaMask** είναι ένα λογισμικό που χρησιμοποιείται για την πλοήγηση στον κόσμο των blockchain. Είναι ένα πρόσθετο πρόγραμμα περιηγητή που συνδέει τον χρήστη με τα διάφορα blockchain δίκτυα, όπως το Ethereum. Με το Metamask, οι χρήστες μπορούν να διαχειρίζονται τα κρυπτονομίσματά τους και να αλληλεπιδρούν με διάφορα ΕΣ. Στην παρούσα υλοποίηση θα χρησιμοποιηθεί για την **προσομοίωση** της **αλληλεπίδρασης** των IoT συσκευών με το ΕΣ.

6.3.4 Solidity

Η **Solidity** είναι μια αντικειμενοστραφής **γλώσσα προγραμματισμού** που χρησιμοποιείται για τη δημιουργία ΕΣ στο blockchain του Ethereum. Η γλώσσα αυτή επιτρέπει τη δημιουργία ΕΣ προσφέροντας δυνατότητες, όπως κληρονομικότητα, στατικούς τύπους δεδομένων και events. Η Solidity θα χρησιμοποιηθεί για την σύνταξη του ΕΣ που θα υλοποιήσει τη λύση που έχει προταθεί.

6.3.5 OpenZeppelin

Το **OpenZeppelin** είναι μια open-source **βιβλιοθήκη** που χρησιμοποιείται για τη σύνταξη ΕΣ. Η βιβλιοθήκη αυτή προσφέρει εργαλεία και λύσεις για συχνά προβλήματα που αντιμετωπίζονται κατά την ανάπτυξη ΕΣ. Στην παρακάτω λύση θα χρησιμοποιηθεί για την απλοποίηση του ΕΣ, παρέχοντας ταυτόχρονα επαυξημένη ασφάλεια, ως μέρος μιας ευρέως χρησιμοποιούμενης βιβλιοθήκης.

6.3.6 Truffle Suite

Το **Truffle Suite** είναι ένα **framework** που χρησιμοποιείται για τη δημιουργία αποκεντρωμένων εφαρμογών. Το Truffle Suite θα χρησιμοποιηθεί για την **ανάπτυξη** μιας εφαρμογής **προσομοίωσης χρήσης** του ΕΣ, καθώς και για το deployment του έξυπνου συμβολαίου στο blockchain.

6.4 Υλοποίηση

Η υλοποίησης της προταθείσας λύσης αποτελείται από τρία σκέλη. Στο πρώτο σκέλος θα αναλυθεί η διαδικασία **συγγραφής** του ΕΣ. Έπειτα θα αναλυθεί η διαδικασία **deployment** του ΕΣ σε ένα δίκτυο Ethereum. Στη συνέχεια θα γίνει **ανάπτυξη** μίας **αποκεντρωμένης εφαρμογής** που θα είναι σε θέση αλληλεπιδράσει με το ΕΣ επιτυγχάνοντας τον τελικό σκοπό. Τέλος θα γίνει μια ανάλυση κόστους λειτουργίας του ΕΣ.

6.4.1 Ανάπτυξη έξυπνου συμβολαίου

Για την ανάπτυξη του ΕΣ θα γίνει χρήση της γλώσσας προγραμματισμού Solidity, η οποία επιτρέπει τη συγγραφή ΕΣ που είναι σε θέση να γίνουν deploy στο δίκτυο του Ethereum.

Η υλοποίηση του ΕΣ ακολουθεί την αντικειμενοστραφή προσέγγιση ως μεθοδολογία ανάπτυξης. Το βασικό στοιχείο (αντιστοιχία της κλάσης) αποτελεί η οντότητα **contract** η οποία μπορεί να αποκτήσει λειτουργικότητα χρησιμοποιώντας το λεκτικό is με τον ίδιο τρόπο που λειτουργεί και η έννοια της κληρονομικότητας στον αντικειμενοστραφή προγραμματισμό.

Για το δεδομένο συμβόλαιο θα γίνει χρήση του συμβολαίου **Ownable** από τη βιβλιοθήκη OpenZeppellin που αναπτύχθηκε παραπάνω ως συμβόλαιο «Πατέρας» με σκοπό τη δημιουργία ενός ΕΣ που θα παρέχει επαυξημένες δυνατότητες σε ένα συγκεκριμένο λογαριασμό Ethereum, ο οποίος θεωρείται και ο ιδιοκτήτης του συμβολαίου.

Για την επίτευξη της ζητούμενης λειτουργικότητας θα χρειαστούν και δυο συλλογές που θα αποθηκεύεται η πληροφορία για του λογαριασμούς που:

a. είναι μέλη του συμβολαίου
b. έχουν ζητήσει το Token επικοινωνίας

Οι συλλογές αυτές στη Solidity αποκαλούνται **mapping**, είναι παρόμοιες με συλλογές που σε πιο γνωστές γλώσσες προγραμματισμού αποκαλούνται Dictionaries ή και Hashsets και διατηρούν την πληροφορία σε ζεύγη κλειδιού-τιμής. Στη δεδομένη χρήση το κλειδί θα είναι το public key των εκάστοτε λογαριασμών Ethereum και η τιμή μια Boolean τιμή που αντιστοιχεί στο ενδεχόμενο ο λογαριασμός να είναι μέλος ή να έχει λάβει το token.

Το συμβόλαιο ολοκληρώνεται με τις τέσσερις παρακάτω μεθόδους που υλοποιούν την επιθυμητή λειτουργικότητα:

6.4.1.1 **addMember**

Αυτή η μέθοδος υλοποιεί το πρώτο βήμα της διαδικασίας, την προσθήκη ενός λογαριασμού Ethereum στη λίστα με τους λογαριασμούς που είναι σε θέση να ζητήσουν το token επικοινωνίας. Η μέθοδος καλείται αποκλειστικά από τον ιδιοκτήτη του ΕΣ. Με αυτόν τον τρόπο επιτυγχάνεται ο κατά βούληση διαμοιρασμός του token και εν συνεχεία η αποκρυπτογράφηση των μηνυμάτων από συγκεκριμένους λογαριασμούς και μόνο.

6.4.1.2 **requestToken**

Η μέθοδος requestToken υλοποιεί το δεύτερο βήμα της διαδικασίας. Η κλήση πραγματοποιείται από λογαριασμούς Ethereum που έχουν ήδη προστεθεί στη λίστα με τα μέλη από τον ιδιοκτήτη του ΕΣ και περιλαμβάνει ένα δημόσιο κλειδί ασύμμετρης κρυπτογραφίας, με το οποίο θα κρυπτογραφηθεί το token επικοινωνίας πριν την αποστολή του. Με την ολοκλήρωση της μεθόδου παράγεται ένα event με τον λογαριασμό Ethereum του αιτούντα και το δημόσιο κλειδί με το οποίο θα κρυπτογραφηθεί το token επικοινωνίας. Το event αυτό αποσκοπεί στην ενημέρωση του ιδιοκτήτη του ΕΣ πως ένας συγκεκριμένος λογαριασμός έχει ζητήσει την παραλαβή του token επικοινωνίας με σκοπό του επόμενου σταδίου της διαδικασίας, την αποστολή του token επικοινωνίας.

6.4.1.3 **sendToken**

Η μέθοδος sendToken, αποτελεί ακόμα μια μέθοδο στην οποία έχει δικαίωμα εκτέλεσης μόνο ο ιδιοκτήτης του ΕΣ. Η εκτέλεση της πραγματοποιείται αφότου κάποιο μέλος έχει επιτυχημένα ζητήσει το token. Για να γίνει η εκτέλεση της μεθόδου, ο ιδιοκτήτης του ΕΣ λαμβάνει το δημόσιο κλειδί του αιτούντα από το παραχθέν event και, χρησιμοποιώντας κάποιον ασύμμετρο κρυπτογραφικό αλγόριθμο, κρυπτογραφεί το token επικοινωνίας, έτσι ώστε να μπορεί να το αποκρυπτογραφήσει μόνο ο αιτών με το ιδιωτικό κλειδί του. Αφού κρυπτογραφηθεί με επιτυχία το token επικοινωνίας, ξεκινά η εκτέλεση της μεθόδου. Το πρώτο βήμα είναι η προσθήκη του αιτούντα στη συλλογή με τους λογαριασμούς που έχουν λάβει το token επικοινωνίας, επιτρέποντας τη χρήση της τελευταίας μεθόδου για την επίτευξη της ασφαλούς επικοινωνίας. Τέλος παράγεται ένα event που περιέχει το κρυπτογραφημένο token επικοινωνίας καθώς και το λογαριασμό του αιτούντα με σκοπό την ενημέρωση του αιτούντα για την πρόοδο της αίτησης του.

6.4.1.4 **communicate**

Η τελευταία μέθοδος του ΕΣ, communicate, υλοποιεί την επικοινωνία. Χρησιμοποιείται αποκλειστικά αφού ένα μέλος έχει γίνει μέλος και έχει ζητήσει το token επικοινωνίας. Παράμετρος της μεθόδου αποτελεί το μήνυμα, το οποίο έχει κρυπτογραφηθεί από το token επικοινωνίας. Με την ολοκλήρωση της μεθόδου παράγεται ένα event που αποσκοπεί στην ενημέρωση όλων των μελών για τη δημιουργία ενός νέου μηνύματος, στο οποίο μπορούν να αποκτήσουν πρόσβαση αποκρυπτογραφώντας το με το token επικοινωνίας.

Το ΕΣ που περιγράφηκε υλοποιείται με τον παρακάτω κώδικα Solidity:

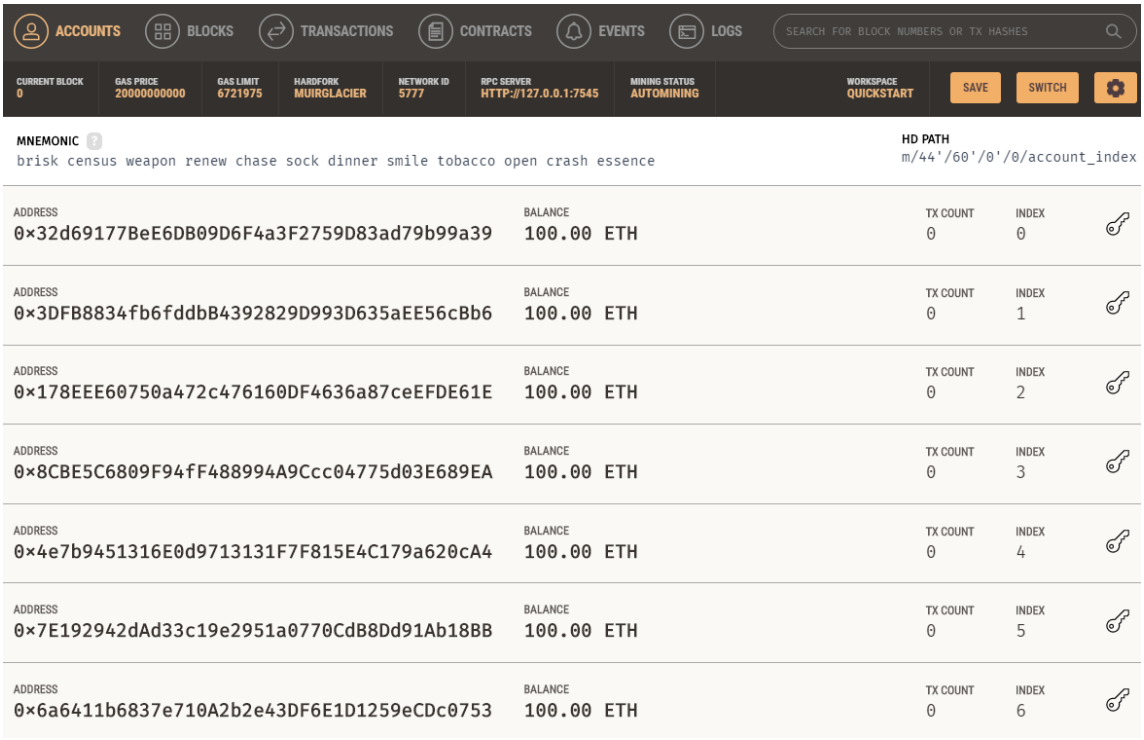
```
pragma solidity >=0.8.0 <0.9.0;

import "@openzeppelin/contracts/access/Ownable.sol";

contract trustedGroup is Ownable {
    mapping(address => bool) private members;
    mapping(address => bool) private hasToken;

    event ReqToken(address _from, string _key);
    event SToken(address _to, string _encToken);
    event Comm(address indexed _from, string _encMessage);

    constructor() {
        members[msg.sender] = true;
        hasToken[msg.sender] = true;
    }

    function addMember(address member) public onlyOwner {
        require(members[member] != true, "Member already exists");
        members[member] = true;
    }

    function requestToken(string calldata publicKey) public {
        require(members[msg.sender] == true, "Not a member");
        emit ReqToken(msg.sender, publicKey);
    }

    function sendToken(string calldata EncryptedToken, address receiver)
        public
        onlyOwner
    {
        hasToken[receiver] = true;
        emit SToken(receiver, EncryptedToken);
    }

    function communicate(string calldata encMessage) public {
        require(members[msg.sender] == true, "Not a member");
        require(hasToken[msg.sender] == true, "Member doesn't have the Token");
        emit Comm(msg.sender, encMessage);
    }
}
```

6.4.2 Deployment έξυπνου συμβολαίου

Το deployment του ΕΣ είναι η διαδικασία κατά την οποία ο κώδικας solidity που αναπτύχθηκε παραπάνω μεταφράζεται σε **πηγαίο κώδικα** και γίνεται upload στο υφιστάμενο Ethereum δίκτυο με σκοπό την αλληλεπίδραση μαζί του από τις εκάστοτε συσκευές. Για την υλοποίηση αυτής της διπλωματικής εργασίας το deployment του ΕΣ αποτελείται από τα παρακάτω βήματα:

6.4.2.1 Δημιουργία τοπικού δικτύου Ethereum

Για την ανάπτυξη και το testing του ΕΣ θα γίνει χρήση ενός τοπικού δικτύου Ethereum, όπου μπορεί να παρατηρηθεί η συμπεριφορά ενός έξυπνου συμβολαίου χωρίς την ανάγκη αλληλεπίδρασης με το κύριο δίκτυο Ethereum. Για τη δημιουργία του τοπικού δικτύου Ethereum θα γίνει χρήση του εργαλείου **Ganache**.



Εικόνα 11 Περιβάλλον τοπικού δικτύου Ethereum

Στην Εικόνα 11 φαίνεται το περιβάλλον που δημιουργείται από το εργαλείο Ganache.

Αρχικά στην οριζόντια μπάρα εμφανίζονται τα χαρακτηριστικά που ορίζουν το δίκτυο:

- **Mnemonic**: Μια αλληλουχία λέξεων που χρησιμοποιείται ως seed για τη δημιουργία των Ethereum λογαριασμών του δικτύου.
- **Current Block**: Ο αριθμός των block που έχουν γίνει mine από το δίκτυο
- **Gas Price**: Η τιμή του gas σε Wei
- **Gas Limit**: Το όριο του gas που μπορεί να συμπεριληφθεί σε ένα block
- **Network Id**: Ο μοναδικός κωδικός του δικτύου
- **RPC Server**: Η http διεύθυνση στην οποία θα δέχεται συνδέσεις το δίκτυο

Έπειτα υπάρχουν οι παρακάτω καρτέλες:

- **Accounts**: Η καρτέλα στην οποία φαίνονται οι λογαριασμοί Ethereum (τα δημόσια κλειδιά τους, το υπόλοιπο τους σε ETH και άλλες χρήσιμες πληροφορίες).
- **Blocks**: Η καρτέλα που εμφανίζονται τα blocks που γίνονται mine στο δίκτυο.
- **Transactions**: Η καρτέλα που εμφανίζονται οι συναλλαγές που βρίσκονται στα blocks που έχουν γίνει mine.
- **Contracts**: Η λίστα με τα ΕΣ που έχουν γίνει migrate στο δίκτυο.
- **Events**: Η λίστα με τα events που έχουν γίνει emit από τις συναλλαγές που έχουν γίνει mine στο δίκτυο.

6.4.2.2 Μεταγλώττιση του έξυπνου συμβολαίου

Για την διαδικασία του **compilation**, αλλά και του deployment του ΕΣ θα γίνει χρήση του εργαλείου Truffle Suite. Το Truffle Suite παρέχει μήτρες για τη δημιουργία και αλληλοεπίδραση με ΕΣ. Αφού γίνει η επιλογή της εκάστοτε μήτρας, δημιουργείται η δομή που επιτρέπει την ανάπτυξη του λογισμικού.

Στο τρέχον βήμα θα γίνει η προσθήκη του ΕΣ που αναπτύχθηκε παραπάνω στον φάκελο contracts που παράχθηκε από τη μήτρα.

Στη συνέχεια με την εκτέλεση της παρακάτω εντολής, γίνεται η μεταγλώττιση των ΕΣ και η παραγωγή των **ABI**, τα οποία θα χρησιμοποιηθούν από το λογισμικό για την αλληλεπίδραση με το ΕΣ.

```
> truffle compile
```

6.4.2.3 Migration του έξυπνου συμβολαίου στο τοπικό δίκτυο Ethereum

Σε αυτό το βήμα θα γίνει το migration του ΕΣ στο τοπικό δίκτυο Ethereum που δημιουργήθηκε παραπάνω. Για να επιτευχθεί αυτό θα χρειαστεί να γίνει η προσθήκη του δικτύου στο αρχείο "truffle-config.js" που έχει παραχθεί από τη μήτρα. Συγκεκριμένα θα χρειαστεί να προστεθεί το δίκτυο στη λίστα με τα δίκτυα.

Για τον ορισμό του δικτύου χρειάζεται:

- το **Mnemonic** του δικτύου
- η http διεύθυνση του **RPC Server** του δικτύου
- ο αύξων αριθμός του λογαριασμού Ethereum που θα αναλάβει το migration (θα είναι **owner** και θα υποστεί τις κυρώσεις του migration σε gas)
- ο μοναδικός αριθμός του Ethereum δικτύου

Στην περίπτωση του τοπικού δικτύου ο ορισμός του δικτύου γίνεται με τον παρακάτω κώδικα.

```
    ganache_local: {
      provider: function () {
        return new HDWalletProvider(process.env.MNEMONIC,
          "http://127.0.0.1:7545", AccountIndex)
      },
      network_id: 5777
    }
```

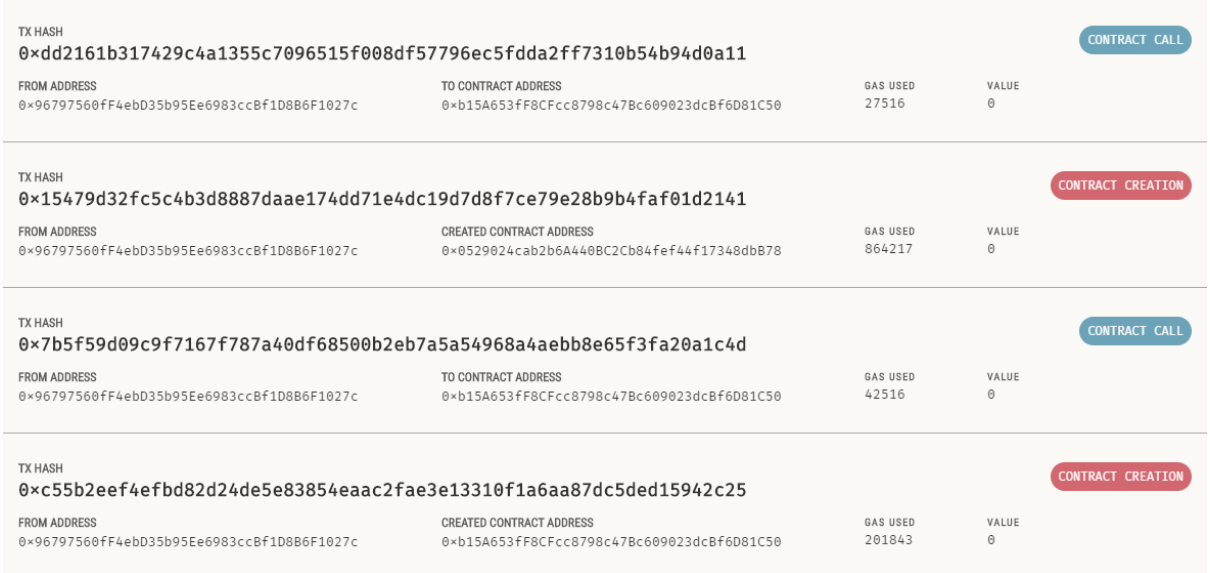
Με τον ορισμό του δικτύου έτοιμο με την παρακάτω εντολή επιτυγχάνεται το migration:

```
> truffle migrate --network ganache_local
```

Με την εκτέλεση της εντολής εμφανίζονται τα συμβόλαια στην καρτέλα contracts:

Εικόνα 12 Έξυπνα συμβόλαια στο Ganache

Επίσης στην καρτέλα Transactions φαίνονται και οι συναλλαγές που εκτελέστηκαν για την δημιουργία του ΕΣ.



Εικόνα 13 Συναλλαγές deployment έξυπνου συμβολαίου

Από την παραπάνω εικόνα υπολογίζεται το συνολικό κόστος του deployment σε 1.136.092 gas.

6.4.3 Ανάπτυξη αποκεντρωμένης εφαρμογής

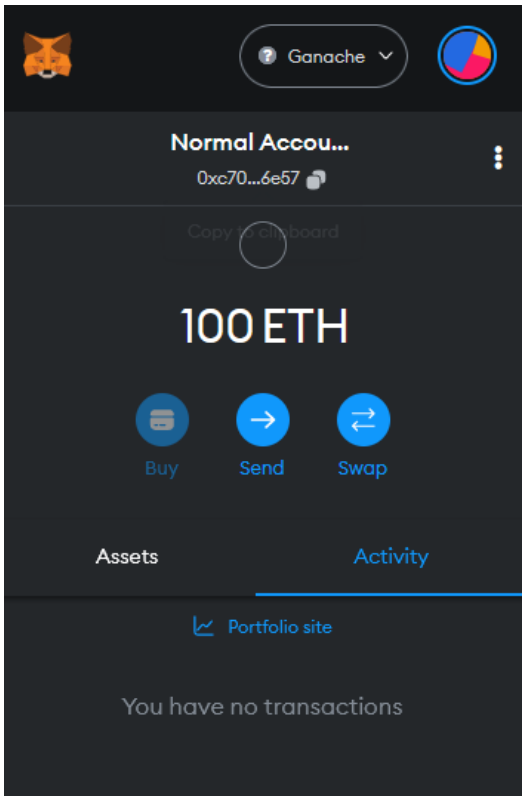
Με το ΕΣ να είναι deployed στο τοπικό δίκτυο Ethereum, το επόμενο βήμα είναι η δημιουργία μιας αποκεντρωμένης εφαρμογής που θα αλληλοεπιδρά με το ΕΣ και θα υλοποιεί τις απαραίτητες λειτουργίες.

Η εφαρμογή υλοποιεί τις παρακάτω λειτουργίες:

6.4.3.1 Ανάκτηση Ethereum λογαριασμών του χρήστη

Για την αλληλεπίδραση του χρήστη με το ΕΣ, θα χρειαστεί να έχει γίνει εισαγωγή ενός λογαριασμού (από αυτούς που δημιουργήθηκαν κατά τη δημιουργία του τοπικού δικτύου Ethereum) στο πορτοφόλι του χρήστη. Για αυτόν τον σκοπό θα χρησιμοποιηθεί το εργαλείο Metamask.

Η εισαγωγή γίνεται με την προμήθεια του ιδιωτικού κλειδιού του λογαριασμού Ethereum. Παρακάτω φαίνεται το πορτοφόλι μετά την εισαγωγή του λογαριασμού.



Εικόνα 14 Λογαριασμός Ethereum σε πορτοφόλι Metamask

6.4.3.2 Ανάκτηση instance έξυπνου συμβολαίου

Με τον αύξων αριθμό του δικτύου Ethereum και το ABI που παράχθηκε κατά το compilation του ΕΣ παράγεται ένα instance, με το οποίο καθίσταται εφικτή η αλληλεπίδραση με το ΕΣ.

6.4.3.3 Έλεγχος ιδιοκτησίας συμβολαίου

Με τη χρήση του instance από το προηγούμενο βήμα, γίνεται κλήση στην μέθοδο owner που παρέχει η βιβλιοθήκη OpenZeppellin, η οποία επιστρέφει τον ιδιοκτήτη του συμβολαίου. Με αυτόν τον τρόπο αναγνωρίζεται αν ο λογαριασμός του πορτοφολιού Metamask είναι ιδιοκτήτης του συμβολαίου, ώστε να προστεθεί η απαραίτητη λειτουργικότητα που είναι χρήσιμη μόνο στον ιδιοκτήτη.

6.4.3.4 Προσθήκη ακροατών για events
Όπως αναλύθηκε, το ΕΣ δύναται να κάνει emit κάποια events.

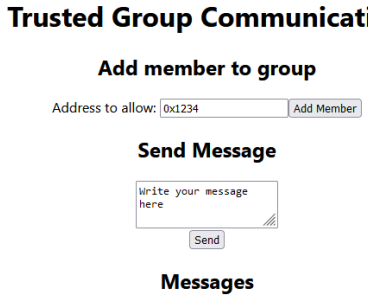
Τα events αυτά είναι:

- Το event αίτησης token (ReqToken)
- Το event αποστολής token (SToken)
- Το event μετάδοσης μηνύματος (Comm)

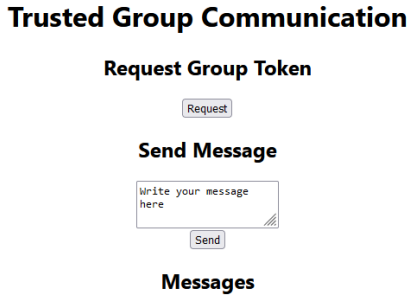
Η προσθήκη ακροατή για το πρώτο είναι αναγκαία μόνο από τον ιδιοκτήτη (καθώς πρέπει να απαντήσει στο event καλώντας τη μέθοδο sendToken για να στείλει το κρυπτογραφημένο token επικοινωνίας), ενώ η προσθήκη ακροατή για τα άλλα δύο event γίνεται από όλους.

6.4.3.5 Υλοποίηση διεπαφής χρήστη
Η διεπαφή χρήστη θα πρέπει να παρέχει τη δυνατότητα στον Ιδιοκτήτη του ΕΣ να προσθέσει μέλη, στα μέλη να αιτηθούν το token επικοινωνίας και σε όλους τη δυνατότητα να στείλουν ένα μήνυμα μέσω του ΕΣ.

Παρακάτω φαίνονται οι διεπαφές χρήστη για τον ιδιοκτήτη και τον απλό χρήστη αντίστοιχα:



Εικόνα 15 Διεπαφή χρήστη ιδιοκτήτη



Εικόνα 16 Διεπαφή απλού χρήστη

6.4.3.6 Υλοποίηση λειτουργικότητας
Για την ολοκλήρωση της ανάπτυξης της αποκεντρωμένης εφαρμογής πρέπει να υλοποιηθεί η λειτουργικότητα των κουμπιών (Add member, Request (Token) και Send (Message)), καθώς και τον ακροατών που προστέθηκαν παραπάνω.

6.4.3.6.1 ***Προσθήκη μέλους***
Η υλοποίηση της μεθόδου αυτής αποτελείται από την κλήση της μεθόδου addMember του ΕΣ, η οποία θα προσθέσει τον λογαριασμό Ethereum (που έχει συμπληρωθεί στο textbox) στη λίστα με τα μέλη.

6.4.3.6.2 ***Αίτηση token επικοινωνίας***
Η υλοποίηση της μεθόδου αυτής αποτελείται από την κλήση της μεθόδου requestToken του ΕΣ (περνώντας ως παράμετρο ένα δημόσιο κλειδί κάποιου ασύμμετρου κρυπτογραφικού αλγορίθμου), η οποία θα κάνει emit το event ReqToken.

6.4.3.6.3 ***Αποστολή token επικοινωνίας***
Η αποστολή του token επικοινωνίας εκτελείται όταν κάποιος χρήστης έχει αιτηθεί επιτυχημένα το token επικοινωνίας, επομένως εκτελείται από τον ακροατή ReqToken που υπάρχει όταν ο συνδεδεμένος λογαριασμός Ethereum είναι ο ιδιοκτήτης του συμβολαίου. Για την υλοποίηση της αποστολής token επικοινωνίας κρυπτογραφείται το token επικοινωνίας (που έχει ο ιδιοκτήτης) με το δημόσιο κλειδί που υπάρχει στον event και στη συνέχεια γίνεται κλήση της μεθόδου sendToken του ΕΣ με παραμέτρους το κρυπτογραφημένο token και τον λογαριασμό Ethereum του αιτούντα.

6.4.3.6.4 ***Παραλαβή token επικοινωνίας***
Η παραλαβή του token επικοινωνίας εκτελείται όταν έχει γίνει επιτυχημένα αποστολή του token από τον ιδιοκτήτη με αποτέλεσμα να έχει γίνει emit το event SToken. Επομένως αυτή η λειτουργία εκτελείται από τον ακροατή για το event SToken. Η υλοποίηση της λειτουργικότητας αποτελείται από την αποκρυπτογράφηση του token (εφόσον η διεύθυνση του παραλήπτη του event ταυτίζεται με τον συνδεδεμένο λογαριασμό Ethereum) με τη χρήση του ιδιωτικού κλειδιού και την αποθήκευση του token επικοινωνίας για μετέπειτα χρήση για την αποστολή μηνυμάτων.

6.4.3.6.5 ***Αποστολή μηνυμάτων***
Η υλοποίηση της αποστολής μηνυμάτων αποτελείται από τη ΣΚ του εκάστοτε μηνύματος με τη χρήση του token επικοινωνίας και η κλήση της communicate μεθόδου του ΕΣ για την μετάδοση του κρυπτογραφημένου μηνύματος.

6.4.3.6.6 ***Παραλαβή μηνυμάτων***
Η παραλαβή των μηνυμάτων είναι συνέπεια του ακροατή των Comm event που γίνονται emit από το ΕΣ. Για την υλοποίηση της παραλαβής αρκεί η αποκρυπτογράφηση του μηνύματος με τη χρήση του token επικοινωνίας (αν είναι διαθέσιμο) και η προσθήκη των μηνυμάτων στη λίστα με τα μηνύματα που έχουν μεταδοθεί.

Με την υλοποίηση όλων των παραπάνω ολοκληρώνεται και η υλοποίηση της ροής, παρέχοντας τη δυνατότητα ασφαλούς μεταφοράς του token επικοινωνίας και την ασφαλή επικοινωνία μέσω του ΕΣ συμβολαίου.

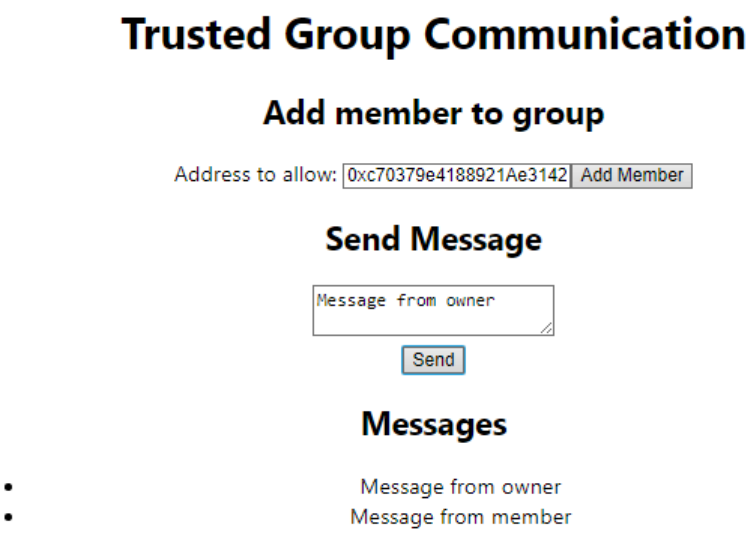
6.4.3.7 Παράδειγμα λειτουργίας του έξυπνου συμβολαίου
Για την επίδειξη της λειτουργίας του ΕΣ θα χρειαστούν 3 λογαριασμοί:

- Ο ιδιοκτήτης
- Ένα μέλος (θα προστεθεί στην διάρκεια της ροής)
- Ένα μη μέλος

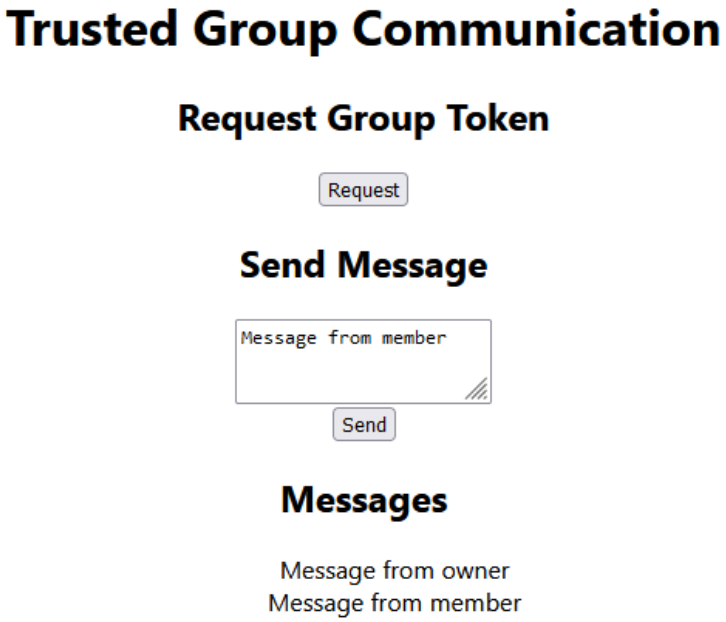
Η ροή που θα ακολουθηθεί είναι η εξής:

- Προσθήκη του μέλους
- Αίτηση του token επικοινωνίας από το μέλος
- Αποστολή μηνύματος από τον ιδιοκτήτη
- Αποστολή μηνύματος από το μέλος

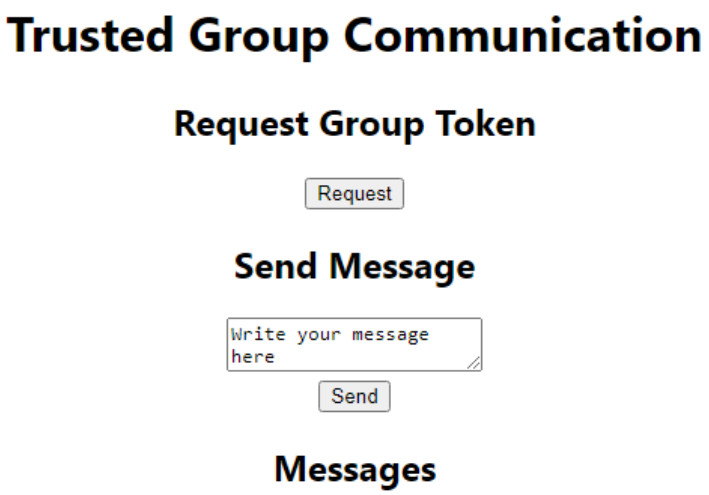
Οι διεπαφές χρήστη μετά την εκτέλεση της παραπάνω ροής είναι οι εξής:



Εικόνα 17 Διεπαφή ιδιοκτήτη μετά τη ροή



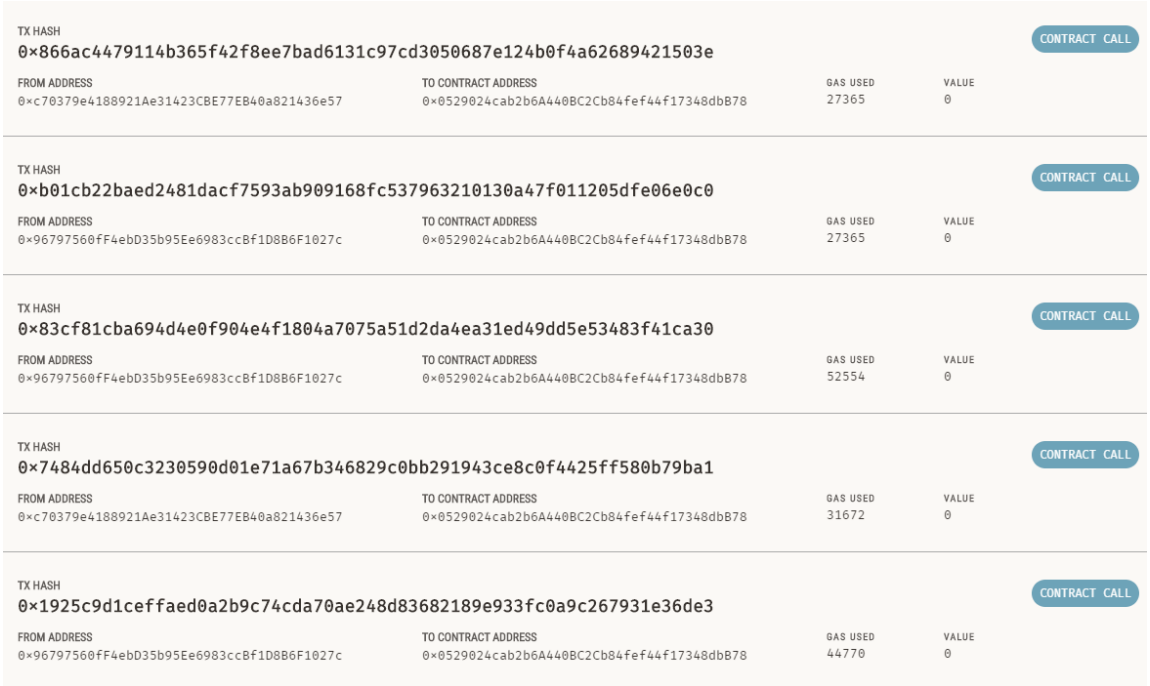
Εικόνα 18 Διεπαφή μέλους μετά τη ροή



Εικόνα 19 Διεπαφή μη μέλους μετά τη ροή

Οι συναλλαγές που εκτελέστηκαν είναι οι παρακάτω πέντε και είναι κατά σειρά οι κλήσεις:

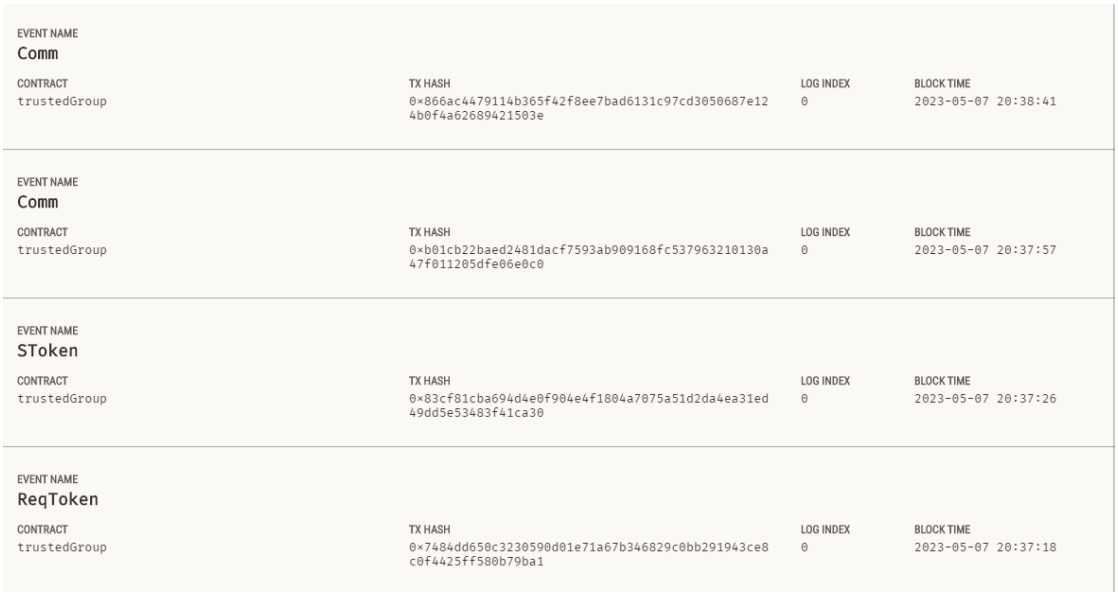
- addMember (από τον ιδιοκτήτη)
- requestToken (από το μέλος)
- sendToken (από τον ιδιοκτήτη)
- communicate (από τον ιδιοκτήτη)
- communicate (από το μέλος)



Εικόνα 20 Συναλλαγές που εισήχθησαν στο δίκτυο κατά τη ροή

Τέλος τα event που έγιναν emit είναι τα παρακάτω:

- ReqToken (από το μέλος)
- SendToken (από τον ιδιοκτήτη)
- Comm (από τον ιδιοκτήτη)
- Comm (από το μέλος)



Εικόνα 21 Event που έγιναν emit κατά τη ροή

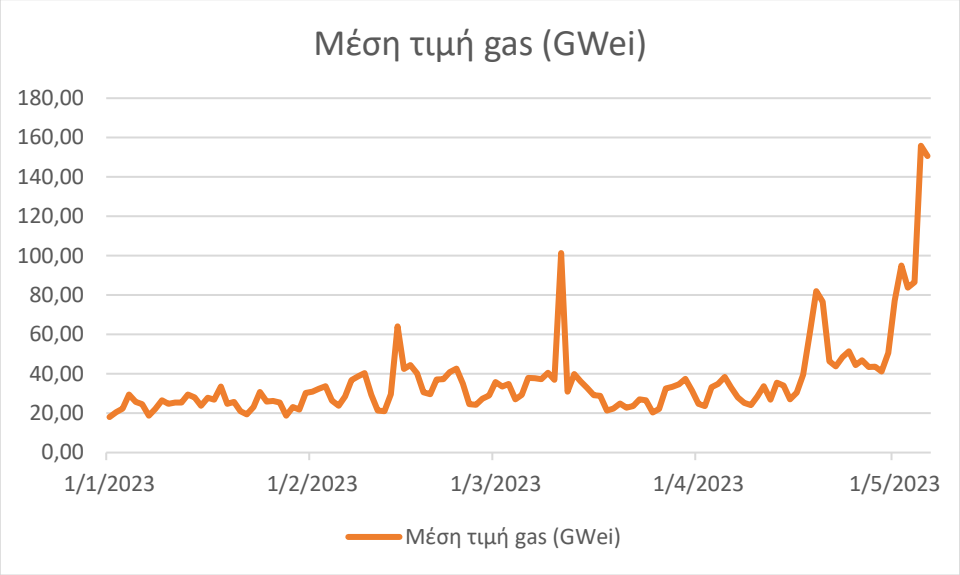
Το αποτέλεσμα της παραπάνω ροής είναι η ασφαλής μεταφορά μηνυμάτων δεδομένων μέσω του ΕΣ. Η διαδικασία ολοκληρώθηκε με πέντε συναλλαγές από τις οποίες οι τρείς αποσκοπούσαν στον ασφαλή διαμοιρασμό του token επικοινωνίας με συνολικό κόστος **128.986 gas** και 2 συναλλαγές για την αποστολή μηνυμάτων με κόστος **27365 gas ανά μήνυμα**.

6.4.4 Ανάλυση κόστους λειτουργίας

Για τη λειτουργία όπως αναλύθηκε παραπάνω είναι αναγκαίο να γίνονται κλήσεις στο ΕΣ. Συγκεκριμένα χρειάζονται οι κλήσεις addMember, requestToken και sendToken για την ασφαλή μεταβίβαση του token επικοινωνίας, και η κλήση communicate για την αποστολή μηνυμάτων.

Η τιμή του gas δεν είναι σταθερή και εξαρτάται από την κίνηση που υπάρχει στο δίκτυο (όσο μεγαλύτερη η κίνηση τόσο μεγαλύτερο είναι το gas price, με σκοπό να δοθεί κίνητρο στους miners να επιλέξουν την δεδομένη συναλλαγή στις συναλλαγές που θα συμπεριλάβουν στο block τους.

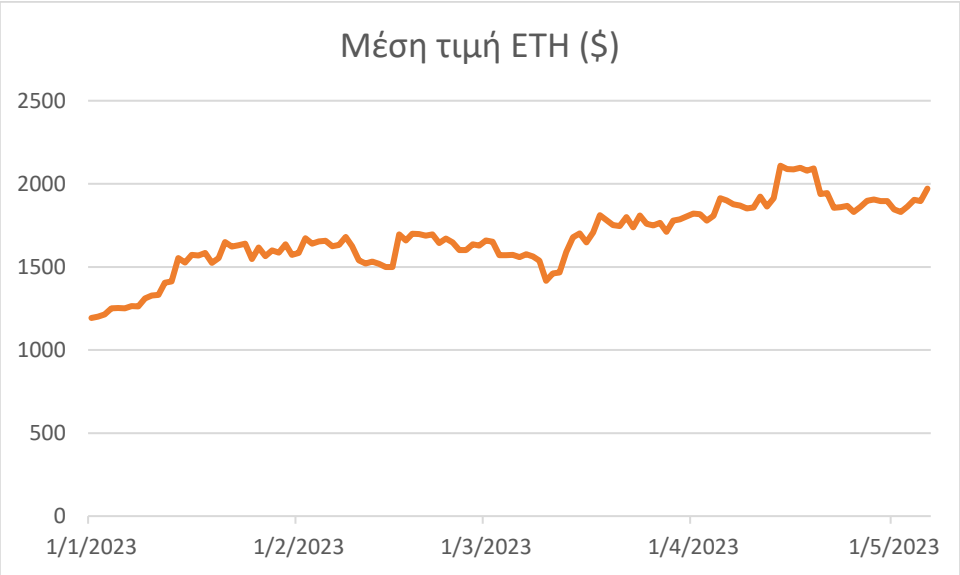
Παρακάτω φαίνεται η μέση ημερήσια τιμή του gas για το έτος 2023 (μέχρι στιγμής) [23]:



Εικόνα 22 Μέση ημερήσια τιμή gas στο Ethereum MainNet για το έτος 2023

Επομένως το **μέσο κόστος** gas για το 2023 είναι **126 GWei**.

Παρακάτω φαίνεται η μέση ημερήσια τιμή του ETH για το έτος 2023 (μέχρι στιγμής) [24]:



Εικόνα 23 Μέση ημερήσια τιμή ETH στο Ethereum MainNet για το έτος 2023

Συνεπώς το **μέσο κόστος** του **ETH** για το έτος 2023 είναι **1676.088** $.

Συνοψίζοντας σύμφωνα με τα δεδομένα από την εκτέλεσης της ροής του παραπάνω κεφαλαίου το κόστος της λειτουργίας του ΕΣ είναι το παρακάτω, την μέση τιμή gas και την μέση τιμή ETH καταλήγουμε στα παρακάτω αποτελέσματα :

	Προσθήκη μέλους	Αίτηση token	Αποστολή token	Συνολικό κόστος μεταφοράς token	Κόστος μηνύματος
Gas	44.770	31.672	52.544	128.986	27365
GWei	5.641.020	3.990.672	6.620.544	16.252.236	3.447.990
Dollar	9.45	6.69	11.10	27.24	5.78

Πίνακας 1 Κόστη εκτέλεσης έξυπνου συμβολαίου

6.5 Πλεονεκτήματα πρότασης

Στο παρόν κεφάλαιο θα συζητηθούν τα πλεονεκτήματα από τη χρήση ΕΣ για την επικοινωνία του IoT συσκευών. Τα πλεονεκτήματα αυτά αποτελούν κατά κύριο λόγο, εγγενείς ιδιότητες της τεχνολογίας Blockchain. Η επιλογή της επιλογής του Blockchain ως μέσο αυθεντικοποίησης έγινε καθώς η χρήση του προσφέρει επαυξημένη ασφάλεια με τους παρακάτω τρόπους.

6.5.1 Ανθεκτικότητα δεδομένων

Στα παραδοσιακά κανάλια επικοινωνίας, υπάρχει πάντα ο κίνδυνος να αλλοιωθούν ή να τροποποιηθούν τα δεδομένα κατά τη μετάδοση. Αυτό μπορεί να οδηγήσει σε σοβαρές συνέπειες, ιδίως σε εφαρμογές όπου η ακρίβεια των δεδομένων είναι κρίσιμη, όπως στην υγειονομική περίθαλψη ή τη βιομηχανική παρακολούθηση. Με τη χρήση της τεχνολογίας blockchain και των ΕΣ, ωστόσο, τα δεδομένα μπορούν να καταγράφονται με τρόπο **απαραβίαστο** και **αμετάβλητο**, καθώς οι συναλλαγές που εισέρχονται στο blockchain είναι απαράλλακτες, μειώνοντας τον κίνδυνο χειραγώγησης των δεδομένων και παρέχοντας ένα πιο ασφαλές και αξιόπιστο κανάλι επικοινωνίας μεταξύ των συσκευών IoT.

6.5.2 Διαφάνεια δεδομένων

Η διαφάνεια που παρέχει η τεχνολογία blockchain, είναι αποτέλεσμα του γεγονότος πως το σύνολο των συναλλαγών σε ένα blockchain είναι **δημόσια** κοινοποιημένες και προσβάσιμες μέσω του δικτύου. Αυτό σημαίνει ότι όλα τα μέρη που εμπλέκονται στην επικοινωνία IoT μπορούν να **βλέπουν** και να **επαληθεύουν** τα δεδομένα σε **πραγματικό χρόνο**. Αυτό μπορεί να βελτιώσει την εμπιστοσύνη και τη λογοδοσία μεταξύ των μερών και να μειώσει το ενδεχόμενο διαφορών ή παρεξηγήσεων. Επιπλέον, η χρήση της τεχνολογίας blockchain μπορεί να διευκολύνει την παρακολούθηση της ροής των δεδομένων μεταξύ των συσκευών IoT, παρέχοντας μια πιο πλήρη και ακριβή εικόνα της διαδικασίας επικοινωνίας.

6.5.3 Ιχνηλασιμότητα δεδομένων

Η χρήση της τεχνολογίας blockchain μπορεί να παρέχει ένα πλήρες και ελέγξιμο αρχείο όλων των συναλλαγών μεταξύ των συσκευών IoT, καθιστώντας δυνατή την ανίχνευση της πηγής και του ιστορικού των δεδομένων. Αυτό το χαρακτηριστικό μπορεί να είναι ιδιαίτερα χρήσιμο σε εφαρμογές όπως η διαχείριση της αλυσίδας εφοδιασμού ή τα logistics, όπου η παρακολούθηση της κίνησης των εμπορευμάτων ή των περιουσιακών στοιχείων είναι κρίσιμη. Παρέχοντας ένα **διαφανές** και **ανιχνεύσιμο αρχείο δεδομένων**, τα ΕΣ μπορούν να συμβάλουν στη βελτίωση της λογοδοσίας και στη μείωση του κινδύνου σφαλμάτων ή απάτης.

6.5.4 Αυθεντικότητα δεδομένων

Η χρήση ΕΣ στην τεχνολογία blockchain μπορεί να παρέχει υψηλότερο επίπεδο ασφάλειας για την επικοινωνία του IoT με την αξιοποίηση κρυπτογραφικών αλγορίθμων και ψηφιακών υπογραφών. Κάθε συναλλαγή στο blockchain **πιστοποιείται** από μια **ψηφιακή υπογραφή**, η οποία παρέχει έναν ασφαλή και απαραβίαστο τρόπο επαλήθευσης της **αυθεντικότητας** των δεδομένων. Αυτό εξακριβώνει την αυθεντικότητα των δεδομένων, μειώνοντας τον κίνδυνο τροποποίησης, η εμπλουτισμού των δεδομένων. Επιπλέον, η χρήση ψηφιακών υπογραφών διασφαλίζει επίσης την ακεραιότητα των δεδομένων, καθιστώντας το κανάλι επικοινωνίας μεταξύ των συσκευών IoT αξιόπιστο.

Συνολικά, η χρήση ΕΣ για την επικοινωνία IoT συσκευών παρέχει έναν ασφαλή τρόπο αλληλεπίδρασης και αξιοποίησης των τεραστίων ποσοτήτων των δεδομένων που παράγονται από συσκευές IoT. Με τη δημιουργία ενός πιο ασφαλούς, αποτελεσματικού και αξιόπιστου καναλιού επικοινωνίας, τα ΕΣ είναι σε θέση να βρουν εφαρμογή σε εφαρμογές με επαυξημένες απαιτήσεις ασφαλείας.

6.6 Μειονεκτήματα πρότασης

Παρόλο που τα ΕΣ και η τεχνολογία blockchain προσφέρουν πολλά πιθανά οφέλη για την ασφαλή και αξιόπιστη επικοινωνία μεταξύ συσκευών IoT, υπάρχουν επίσης αρκετές προκλήσεις και μειονεκτήματα που πρέπει να ληφθούν υπόψη. Σε αυτό το κεφάλαιο, θα διερευνηθούν τα πιθανά μειονεκτήματα της χρήσης ΕΣ και της τεχνολογίας blockchain για επικοινωνίες IoT. Με την ενδελεχή εξέταση των προκλήσεων, καθίσταται δυνατή η καλύτερη κατανόηση των περιορισμών και των αντισταθμιστικών οφελών της χρήσης ΕΣ και της τεχνολογίας blockchain για την επικοινωνία IoT συσκευών. Αναλυτικότερα τα μειονεκτήματα –προκλήσεις της προταθείσας λύσης είναι τα παρακάτω.

6.6.1 Ευπάθεια σε επιθέσεις

Ένα πιθανό μειονέκτημα της χρήσης ΕΣ και token κρυπτογράφησης για την επικοινωνία IoT είναι η ευπάθεια των δεδομένων σε επιθέσεις. Καθώς τα δεδομένα αποθηκεύονται **μόνιμα** στο blockchain, το **token** επικοινωνίας που χρησιμοποιείται για την κρυπτογράφηση των δεδομένων αποτελεί ευάλωτο σημείο της λύσης. Αυτό έχει ως αποτέλεσμα μια πιθανή διαρροή ή κάποιας επίθεσης (π.χ. brute force) προς το token επικοινωνίας να καθιστά δυνατή την πρόσβαση στα δεδομένα από οποιονδήποτε. Η ανθεκτικότητα των δεδομένων στο blockchain καθιστά ένα τέτοιο σενάριο ακόμη πιο επώδυνο, καθώς δεν υπάρχει η δυνατότητα διαγραφής των δεδομένων με σκοπό την απόκρυψη τους. Αυτή η πρόκληση θα μπορούσε να αντιμετωπισθεί με την συστηματική αλλαγή token επικοινωνίας με σκοπό την ελάττωση της προκληθείσας ζημιάς σε περίπτωση κάποιου τέτοιου συμβάντος, με μειονεκτήματα αντίστοιχα την αύξηση της πολυπλοκότητας του συστήματος και την αύξηση των απαιτούμενων συναλλαγών και συνεπώς και του κόστους λειτουργίας.

6.6.2 Υψηλό κόστος λειτουργίας

Ένα ακόμα πιθανό μειονέκτημα της προτεινόμενης λύσης είναι το υψηλό κόστος της. Σύμφωνα με υπολογισμούς του προηγούμενου κεφαλαίου η χρήση του υλοποιημένου ΕΣ κοστίζει περίπου **6 δολάρια ανά μήνυμα**, το οποίο είναι απαγορευτικά ακριβό για την πλειοψηφία των εφαρμογών IoT που παράγουν μεγάλες ποσότητες δεδομένων. Το υψηλό κόστος χρήσης της προτεινόμενης λύσης, τη δεδομένη στιγμή, περιορίζει σημαντικά τις πιθανές εφαρμογές της, περιορίζοντας τη σε εφαρμογές όπου η ροή της πληροφορίας είναι περιορισμένη ή το κόστος αμελητέο. Η τεχνολογία του blockchain ωστόσο, βρίσκεται ακόμη σε αρκετά **πρώιμα** στάδια, έτσι βελτιώσεις στην τεχνολογία, όπως η χρήση

του PoS για την εξακρίβωση τον μπλοκ συναλλαγών, έναντι του PoW, πιθανότατα να επηρεάσουν σημαντικά το κόστος των συναλλαγών στο δίκτυο blockchain, καθιστώντας την προταθείσα λύση πιο εφικτή.

6.6.3 Αργοί χρόνοι συναλλαγών

Η επιλογή του δικτύου Ethereum για την προτεινόμενη λύση είναι ένα άλλο πιθανό μειονέκτημα, καθώς η **εισροή νέων συναλλαγών** στο δίκτυο γίνεται περίπου κάθε **12 δευτερόλεπτα** [25]. Ενώ αυτό μπορεί να είναι αποδεκτό για ορισμένες εφαρμογές, δεν είναι ιδανικό για εφαρμογές πραγματικού χρόνου που απαιτούν σχεδόν άμεση μετάδοση δεδομένων. Οι αργοί χρόνοι συναλλαγών μπορεί να οδηγήσουν σε καθυστερήσεις στη μετάδοση δεδομένων, γεγονός που μπορεί να προκαλέσει προβλήματα σε εφαρμογές που απαιτούν δεδομένα σε πραγματικό χρόνο. Επιπλέον, καθώς αυξάνεται ο αριθμός των συσκευών IoT, αυξάνεται και ο όγκος των δεδομένων που παράγονται, γεγονός που δυνητικά υπερφορτώνει το δίκτυο blockchain και οδηγεί σε πιο αργούς χρόνους συναλλαγών.

6.6.4 Υπολογιστική επιβάρυνση

Ένα άλλο πιθανό μειονέκτημα της χρήσης ΕΣ και της τεχνολογίας blockchain για την αξιόπιστη επικοινωνία μεταξύ συσκευών IoT είναι η υπολογιστική επιβάρυνση που απαιτείται για την κρυπτογράφηση και την αποκρυπτογράφηση. Για την κρυπτογράφηση δεδομένων πριν από τη δημοσίευσή τους στο blockchain, οι συσκευές IoT θα πρέπει να εκτελούν βαριούς αλγορίθμους κρυπτογράφησης που μπορεί να επιβαρύνουν τις περιορισμένες δυνατότητες επεξεργασίας τους. Πολλές συσκευές IoT έχουν πολύ ελάχιστες προδιαγραφές για εξοικονόμηση ενέργειας και κόστους, γεγονός που καθιστά δύσκολη την αποτελεσματική διαχείριση της κρυπτογράφησης και από- κρυπτογράφησης δεδομένων. Αυτό μπορεί να έχει ως αποτέλεσμα βραδύτερη απόδοση και αυξημένη καθυστέρηση, γεγονός που μπορεί να αποβεί επιζήμιο για τις ευαίσθητες στον χρόνο εφαρμογές. Επιπλέον, η υπολογιστική επιβάρυνση που απαιτείται για την κρυπτογράφηση μπορεί να οδηγήσει σε αυξημένη κατανάλωση ενέργειας, η οποία αποτελεί σημαντική ανησυχία για τις συσκευές IoT που λειτουργούν με μπαταρία. Συνεπώς, είναι σημαντικό η επιλογή των αλγορίθμων κρυπτογράφησης να συνάδει με τις υπολογιστικές δυνατότητες των εκάστοτε συσκευών.

6.6.5 Πολυπλοκότητα

Η εφαρμογή της προτεινόμενης λύσης απαιτεί σημαντική τεχνική εμπειρογνωμοσύνη και πόρους, οι οποίοι ενδέχεται να μην είναι άμεσα διαθέσιμοι σε όλους τους οργανισμούς. Επιπλέον, η χρήση κωδικών κρυπτογράφησης προσθέτει ένα επιπλέον επίπεδο πολυπλοκότητας, καθιστώντας ενδεχομένως πιο δύσκολη τη διαχείριση και την αντιμετώπιση προβλημάτων του συστήματος. Η πολυπλοκότητα της προτεινόμενης λύσης θα μπορούσε να περιορίσει την υιοθέτησή της και να την καταστήσει ακατάλληλη για οργανισμούς που δεν διαθέτουν την απαραίτητη τεχνική εμπειρογνωμοσύνη και τους απαραίτητους πόρους.

6.6.6 Νομικές και κανονιστικές προκλήσεις

Η χρήση της τεχνολογίας blockchain εγείρει διάφορες νομικές και ρυθμιστικές προκλήσεις, όπως η προστασία της ιδιωτικής ζωής των δεδομένων, η πνευματική ιδιοκτησία και ζητήματα δικαιοδοσίας. Η αντιμετώπιση αυτών των προκλήσεων μπορεί να είναι χρονοβόρα και δαπανηρή, περιορίζοντας ενδεχομένως την ευρεία υιοθέτηση της προτεινόμενης λύσης. Επιπλέον, οι νομικές και κανονιστικές προκλήσεις που σχετίζονται με τη χρήση της τεχνολογίας blockchain εξελίσσονται συνεχώς, γεγονός που

καθιστά δύσκολο για τους οργανισμούς να παραμένουν ενήμεροι με τους πιο πρόσφατους κανονισμούς και τις απαιτήσεις συμμόρφωσης.

6.6.7 Κατανάλωση ενέργειας

Η διαδικασία εξόρυξης στο δίκτυο blockchain απαιτεί σημαντική ποσότητα ενέργειας, συμβάλλοντας στο συνολικό αποτύπωμα άνθρακα της προτεινόμενης λύσης. Αυτό θα μπορούσε ενδεχομένως να καταστήσει την προτεινόμενη λύση λιγότερο φιλική προς το περιβάλλον και κοινωνικά υπεύθυνη. Καθώς οι οργανισμοί εστιάζουν όλο και περισσότερο στη βιωσιμότητα και την κοινωνική ευθύνη, η κατανάλωση ενέργειας της προτεινόμενης λύσης θα μπορούσε να περιορίσει την υιοθέτησή της και να την καταστήσει ακατάλληλη για οργανισμούς που θέτουν ως προτεραιότητα την περιβαλλοντική και κοινωνική βιωσιμότητα.

Συνοψίζοντας, η παρουσία προκλήσεων στην υλοποίηση της προταθείσας λύσης είναι εμφανής. Συνεπώς, για να αξιοποιηθούν πλήρως οι δυνατότητες των ΕΣ και της τεχνολογίας blockchain για τις επικοινωνίες IoT, είναι ζωτικής σημασίας να σταθμιστούν προσεκτικά τα οφέλη και τα μειονεκτήματα και να αναπτυχθούν στρατηγικές για τον μετριασμό των περιορισμών.

Κεφάλαιο 7: Συμπεράσματα

Η παρούσα εργασία είχε ως στόχο να διερευνήσει τις δυνατότητες χρήσης της τεχνολογίας blockchain για την αυθεντικοποίηση των IoT συσκευών. Ύστερα από μελέτη των υπάρχουσων λύσεων, που επιλύουν το συγκεκριμένο πρόβλημα, παρατηρήθηκε το γεγονός πως υπάρχουν αρκετές προκλήσεις που εμπίπτουν από τη χρήση των λύσεων αυτών, όπως η μειωμένη ασφάλεια, η έλλειψη διαφάνειας, η κλιμακωσιμότητα κ.α. Η τεχνολογία του Blockchain επιλέχθηκε ως ο βασικός πυλώνας για την ανάπτυξη μιας λύσης σε αυτές τις προκλήσεις λόγω των εγγενών ιδιοτήτων τής (ασφάλεια, διαφάνεια, αμεταβλητότητα κ.λπ.). Μέσα από την έρευνα και την ανάπτυξη της λύσης βρέθηκαν και παρουσιάστηκαν τόσο οι δυνατότητες, που είναι σε θέση να προσφέρει η αυθεντικοποίηση IoT συσκευών με τη χρήση ΕΣ, όσο και οι προκλήσεις που παρουσιάζονται και θα χρειαστεί να αντιμετωπισθούν.

Συνολικά, η παρούσα εργασία συνεισφέρει στον τομέα με τους παρακάτω τρόπους. Πρώτον, παρέχει μια ολοκληρωμένη επισκόπηση της τρέχουσας κατάστασης της έρευνας σχετικά με την αυθεντικοποίηση του IoT και την τεχνολογία blockchain. Δεύτερον, παρουσιάζει μιας λύση στο πρόβλημα της αυθεντικοποίησης των IoT συσκευών με τη χρήση των ΕΣ, η οποία μπορεί να χρησιμεύσει ως πρότυπο για άλλους ερευνητές και επαγγελματίες. Τρίτον, προσδιορίζει διάφορες προκλήσεις και ευκαιρίες για μελλοντική έρευνα, όπως η διερεύνηση εναλλακτικών πλατφορμών blockchain, η ανάπτυξη τεχνικών για την αποδοτικότερη κρυπτογράφηση και αποκρυπτογράφηση δεδομένων από συσκευές χαμηλών προδιαγραφών κ.α.

Εν κατακλείδι, η παρούσα εργασία μας έδειξε ότι η χρήση της τεχνολογίας blockchain για την αυθεντικοποίηση του IoT συσκευών έχει σημαντικά πλεονεκτήματα, όπως η αυξημένη ασφάλεια, η ιδιωτικότητα και η διαφάνεια. Ωστόσο, οι προκλήσεις της επεκτασιμότητας, του κόστους συναλλαγών και της εξειδικευμένης τεχνογνωσίας καθιστούν δύσκολη την εφαρμογή λύσεων που βασίζονται στο blockchain σε πολλά σενάρια του πραγματικού κόσμου. Ενώ αυτές οι προκλήσεις καθιστούν δύσκολο για τις λύσεις που βασίζονται στο blockchain να είναι βιώσιμες για τις περισσότερες εφαρμογές, θεωρώ ότι η τεχνολογία blockchain βρίσκεται ακόμη σε πρώιμο στάδιο και εξελίσσεται με ταχείς ρυθμούς. Καθώς η τεχνολογία συνεχίζει να βελτιώνεται, αναπτύσσονται νέοι αλγόριθμοι συναίνεσης και λύσεις κλιμάκωσης που μπορούν να βοηθήσουν στην αντιμετώπιση ορισμένων από τα προβλήματα κλιμάκωσης, ενώ το κόστος χρήσης του blockchain μπορεί να μειωθεί, καθιστώντας την πιο εφικτή για εφαρμογές IoT. Ενώ η εργασία υπογραμμίζει τις σημαντικές προκλήσεις που πρέπει να ξεπεραστούν προτού οι λύσεις που βασίζονται στο blockchain για την αυθεντικοποίηση του IoT γίνουν βιώσιμες, η τεχνολογία αυτή υπόσχεται πολλά για το μέλλον. Η μελλοντική έρευνα θα πρέπει να επικεντρωθεί στην αντιμετώπιση των υπόλοιπων προκλήσεων και στη διερεύνηση νέων περιπτώσεων χρήσης της τεχνολογίας blockchain στο χώρο του IoT.

Βιβλιογραφία

[1] Kessler, G.C. (2003) An Overview of Cryptography.
[2] Chandra, S. et al. (2014) A comparative survey of Symmetric and Asymmetric Key Cryptography.
[3] Sobti, R. (2012) "Cryptographic Hash Functions: A Review," International Journal of Computer Science Issues (IJSCE), 9.2.
[4] Kendhe, A.K. and Agrawal, H. (2013) "A Survey Report on Various Cryptanalysis Techniques," International Journal of Soft Computing and Engineering (IJSCE), 3.2
[5] Khan, J.Y. and Yuce, M.R. (2019) Internet of Things (IoT): Systems and Applications. CRC Press.
[6] Patru, I.-I. et al. (2016) Smart home IoT system.
[7] Jaiganesh, S., Gunaseelan, K. and Ellappan, V. (2017) IOT agriculture to improve food and farming technology.
[8] Nguyen, H.L. et al. (2017) A review on IoT healthcare monitoring applications and a vision for transforming sensor data into real-time clinical feedback.
[9] Krasniqi, X. and Hajrizi, E. (2016) "Use of IoT Technology to Drive the Automotive Industry from Connected to Full Autonomous Vehicles," IFAC-PapersOnLine, 49(29), pp. 269–274.
[10] Manavalan, E. and Sultan, M.T.H. (2019) "A review of Internet of Things (IoT) embedded sustainable supply chain for industry 4.0 requirements," Computers & Industrial Engineering, 127, pp. 925–953.
[11] Lee, I. and Lee, K. (2015) "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," Business Horizons, 58(4), pp. 431–440.
[12] Van Kranenburg, R. and Bassi, A. (2012) "IoT Challenges," Communications in Mobile Computing, 1(1).
[13] Nakamoto, S. (2008) Bitcoin, a Peer-to-peer Electronic Cash System.
[14] Grinberg, R. (2012) "Bitcoin: An Innovative Alternative Digital Currency," Astings Science & Technology Law Journal, 4(1), p. 159.
[15] Wood, G. (2013) "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Project Yellow Paper.
[16] Kamath, R. (2018) "Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM," The Journal of the British Blockchain Association, 1(1), pp. 1–12.
[17] GeeksforGeeks (2022) "Types of Blockchain," GeeksforGeeks [Preprint]. Available at: https://www.geeksforgeeks.org/types-of-blockchain/.
[18] Zhang, S. and Lee, J.-H. (2020) "Analysis of the main consensus protocols of blockchain," ICT Express, 6(2), pp. 93–97.
[19] Zheng, Z. et al. (2017) An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.
[20] Mohanta, B.K., Panda, S.S. and Jena, D. (2018) An Overview of Smart Contract and Use Cases in Blockchain Technology.
[21] Höglund, J. et al. (2020) "PKI4IoT: Towards public key infrastructure for the Internet of Things," Computers & Security, 89, p. 101658.
[22] Dammak, M. et al. (2019) Token-Based Lightweight Authentication to Secure IoT Networks.
[23] Ethereum Average Gas Price Chart (no date). Available at: https://etherscan.io/chart/gasprice.
[24] Ethereum (ETH) Historical Prices | Nasdaq (no date). Available at: https://www.nasdaq.com/market-activity/cryptocurrency/eth/historical.
[25] Etherscan (no date). Available at: https://etherscan.io.
[26] Sakovich, N. (2023) "Internet of Things (IoT) Protocols and Connectivity Options: An Overview," SaM Solutions [Preprint]. Available at: https://www.sam-solutions.com/blog/internet-of-things-iot-protocols-and-connectivity-options-an-overview/.
[27] Stolojescu-Crisan, C., Crisan, C. and Butunoi, B.-P. (2021) "An IoT-Based Smart Home Automation System," Sensors, 21(11), p. 3784. Available at: https://doi.org/10.3390/s21113784.

[28] Electronics, T. (2020) RFID: The Technology Making Industries Smarter. Available at: https://blog.ttelectronics.com/rfid-technology.
[29] View of an Empirical Investigation of Securing Internet of Things Data in Wireless Sensor Network| Journal of Asian Scientific Research (no date). Available at: https://archive.aessweb.com/index.php/5003/article/view/3920/6552.
[30] Implementing a Blockchain with JavaScript (no date). Available at: https://www.devlane.com/blog/implementing-a-blockchain-with-javascript.
[31] Gopi, A. (2020) 5 Steps Towards Securing your Certificate Infrastructure - Security Boulevard. Available at: https://securityboulevard.com/2020/12/5-steps-towards-securing-your-certificate-infrastructure/.
[32] What Is Token-Based Authentication? - Okta SG (no date). Available at: https://www.okta.com/sg/identity-101/what-is-token-based-authentication/.