ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

Ανάπτυξη Ευφυών Συμβολαίων σε Περιβάλλον Blockchain για Ευφυή Ηλεκτρικά Δίκτυα (Smartgrids)

Development of Smart Contracts in a Blockchain Environment for Smart Electric Grids (Smartgrids)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΔΕΣΠΟΙΝΑ ΣΑΒΒΙΔΗ - (ge18098)

ΕΠΙΒΛΕΠΟΝΤΕΣ:
Αριστείδης Παγουρτζής, Καθηγητής ΕΜΠ
Πέτρος Ποτίκας, Ε.Δι.Π.

Αθήνα, Ιούνιος 2024

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

Ανάπτυξη Ευφυών Συμβολαίων σε Περιβάλλον Blockchain για Ευφυή Ηλεκτρικά Δίκτυα (Smartgrids)

Development of Smart Contracts in a Blockchain Environment for Smart Electric Grids (Smartgrids)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΔΕΣΠΟΙΝΑ ΣΑΒΒΙΔΗ - (ge18098)

ΕΠΙΒΛΕΠΟΝΤΕΣ:

Αριστείδης Παγουρτζής, Καθηγητής ΕΜΠ

Πέτρος Ποτίκας, Ε.Δι.Π.

ΤΡΙΜΕΛΗΣ ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ:

Αριστείδης Παγουρτζής, Καθηγητής ΕΜΠ Βασίλειος Βεσκούκης, Καθηγητής ΕΜΠ

Πέτρος Στεφανέας, Αναπληρωτής Καθηγητής ΕΜΠ

Αθήνα, Ιούνιος 2024

.....
Δέσποινα Σαββίδη
Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών Ε.Μ.Π.

Περίληψη

Η ανάπτυξη ευφυών συμβολαίων σε περιβάλλον Blockchain αναδεικνύεται ως κρίσιμη προσέγγιση για την εξέλιξη των ευφυών ηλεκτρικών δικτύων (Smartgrids). Η παρούσα διπλωματική διερευνά την έννοια της Blockchain τεχνολογίας και τη συνέπειά της στον τομέα της ενέργειας. Εστιάζοντας στη δημιουργία ευφυών συμβολαίων, προτείνεται ένα πλαίσιο εργασίας για την ανάπτυξη ευφυών συμβολαίων που εκτελούνται σε περιβάλλον Blockchain. Η εργασία αναλύει την αρχιτεκτονική και τις λειτουργικές αρχές των ευφυών συμβολαίων, επικεντρώνοντας στην αυτονομία, τη διαφάνεια και την ασφάλεια των συναλλαγών. Στη συνέχεια, παρουσιάζονται οι εφαρμογές των ευφυών συμβολαίων στα ευφυή ηλεκτρικά δίκτυα, προτείνοντας το «Energy Market System» συμβόλαιο για την αγοραπωλησία ενέργειας. Αυτό το συμβόλαιο αναπτύσσεται ως μέρος της διαδικασίας δημιουργίας ενός έξυπνου συμβολαίου που είναι ικανό να ανταποκριθεί στις ανάγκες ενός ευφυούς ηλεκτρικού δικτύου. Η εν λόγω διπλωματική εργασία αποτελεί προσπάθεια να επιλυθούν πρακτικά προβλήματα που αντιμετωπίζονται στον τομέα της ενέργειας μέσω της ενσωμάτωσης της τεχνολογίας Blockchain και των έξυπνων συμβολαίων.

Λέξεις Κλειδιά: Blockchain, Έξυπνα Συμβόλαια, Ευφυή Δίκτυα Ηλεκτρικής Ενέργειας (Smartgrids), Τεχνολογία Ενέργειας, Κρυπτογραφία, Μπλοκ, Κατακερματισμός.

Abstract

The development of smart contracts in a Blockchain environment emerges as a critical approach for the evolution of smart grids. This thesis explores the concept of Blockchain technology and its implications in the energy sector. Focusing on the creation of smart contracts, a framework is proposed for developing smart contracts executed in a Blockchain environment. The work analyzes the architecture and operational principles of smart contracts, with a focus on autonomy, transparency, and transaction security. Subsequently, the applications of smart contracts in smart grids are presented, proposing an ≪Energy Market System≫ contract for energy trading. This contract is developed as part of the process of creating a smart contract capable of meeting the needs of a smart grid. This thesis represents an effort to address practical problems encountered in the energy sector through the integration of Blockchain technology and smart contracts.

Keywords: Blockchain, Smart Contracts, Smart Grids, Energy Technology, Cryptography, Blocks, Hashing.

Ευχαριστίες

Με την ολοκλήρωση αυτής της διπλωματικής εργασίας, θα ήθελα να εκφράσω την ειλικρινή μου ευγνωμοσύνη σε όλους όσους με υποστήριξαν και συνέβαλαν καθοριστικά σε αυτήν την προσπάθεια.

Πρώτα απ΄ όλα, ευχαριστώ τον επιβλέποντα καθηγητή μου, κύριο Αριστείδη Παγουρτζή, αλλά και τον κύριο Πέτρο Ποτίκα (Ε.Δι.Π.) για την καθοδήγηση και τις πολύτιμες συμβουλές που μου παρείχαν καθ΄ όλη τη διάρκεια της εργασίας.

Επίσης, θα ήθελα να ευχαριστήσω την οικογένειά μου για την αμέριστη υποστήριξη και κατανόηση τους, καθώς και τους φίλους και συναδέλφους μου για την ενθάρρυνση και τη βοήθειά τους στις δύσκολες στιγμές.

Τέλος, εκφράζω τις ευχαριστίες μου προς όλους όσους συνέβαλαν έμμεσα ή άμεσα στη συγγραφή αυτής της εργασίας, για τη συνεργασία και την εμπιστοσύνη τους.

Περιεχόμενα

1 Εισαγωγή

1.1 Τα κίνητρα και οι στόχοι της Εργασίας

Η παρούσα διπλωματική εργασία επιθυμεί να εξετάσει και να αναλύσει την επίδραση της τεχνολογίας Blockchain και των έξυπνων συμβολαίων στον τομέα της ενέργειας, με έμφαση στα έξυπνα δίκτυα ηλεκτρικής ενέργειας (Smartgrids). Τα κίνητρα που καθοδήγησαν αυτήν την επιλογή περιλαμβάνουν την αυξανόμενη ανάγκη για αποτελεσματική διαχείριση της ενέργειας, την ανάδειξη του Blockchain ως τεχνολογία με δυνατότητες εφαρμογής στον τομέα της ενέργειας, καθώς και την επιδίωξη για αυτόνομα, διαφανή και ασφαλή ηλεκτρικά δίκτυα. Οι στόχοι της έρευνας περιλαμβάνουν την κατανόηση της αρχιτεκτονικής και των λειτουργικών αρχών των έξυπνων συμβολαίων, καθώς και την ανάδειξη της αξίας και των δυνατοτήτων τους στο πλαίσιο της ενεργειακής βιομηχανίας. Τέλος, ένας σημαντικός στόχος είναι η αναλυτική παρουσίαση δημιουργίας ενός συγκεκριμένου παραδείγματος έξυπνου συμβολαίου, του «Energy Market System», το οποίο είναι σχεδιασμένο για την αγοραπωλησία ενέργειας μέσω έξυπνων συμβολαίων. Με αυτούς τους στόχους, η διπλωματική εργασία αποσκοπεί στην ανάπτυξη καινοτόμων λύσεων που θα ενισχύσουν την απόδοση και τη διαφάνεια στον τομέα της ενέργειας.

1.2 Η δομή της Εργασίας

Η δομή αυτής της διπλωματικής περιλαμβάνει τα ακόλουθα κεφάλαια. Το πρώτο κεφάλαιο αναλύει την τεχνολογία του Blockchain, παρουσιάζοντας τις βασικές έννοιες και λειτουργίες του. Εξετάζονται οι διάφορες μορφές Blockchain, η αρχιτεκτονική τους και ο τρόπος λειτουργίας τους. Επιπλέον, εξετάζονται οι ασφάλεια και οι προκλήσεις που σχετίζονται με τη χρήση της τεχνολογίας Blockchain. Στο δεύτερο κεφάλαιο γίνεται μια ανασκόπηση των έξυπνων συμβολαίων και των δυνατοτήτων τους σε ένα περιβάλλον Blockchain. Παρουσιάζονται οι βασικές έννοιες των έξυπνων συμβολαίων, καθώς και παραδείγματα εφαρμογών τους σε διάφορους τομείς. Το τρίτο κεφάλαιο εστιάζει στα ευφυή ηλεκτρικά δίκτυα και τις προκλήσεις που αντιμετωπίζουν, καθώς και τον τρόπο με τον οποίο τα έξυπνα συμβόλαια μπορούν να συμβάλουν στη βελτίωση της λειτουργίας τους. Το τέταρτο και τελευταίο κεφάλαιο αφορά τη δημιουργία ενός «Energy Market System» συμβολαίου για την αγοραπωλησία ενέργειας. Εδώ, παρουσιάζεται η διαδικασία ανάπτυξης του συμβολαίου, καθώς και η ανάλυση των λειτουργιών του σε σχέση με τις ανάγκες του ευφυούς ηλεκτρικού δικτύου. Επίσης, γίνεται αξιολόγηση των πλεονεκτημάτων και των πιθανών προκλήσεων που προκύπτουν από την εφαρμογή του συμβολαίου σε πραγματικές συνθήκες.

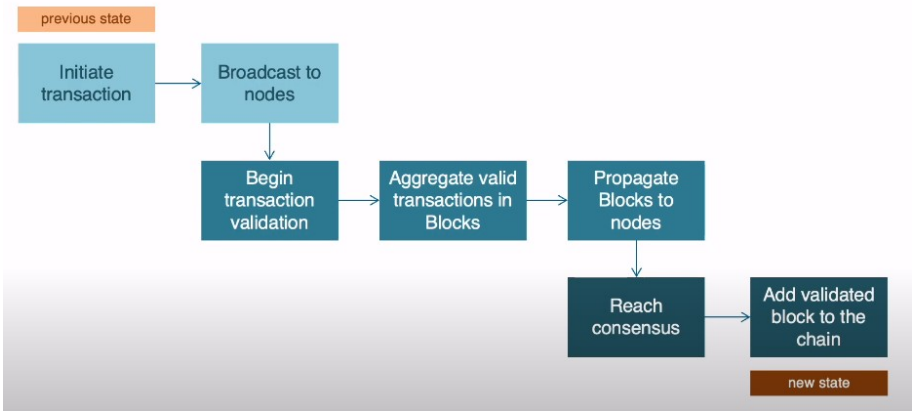
2 Τεχνολογία Blockchain

2.1 Τι είναι το Blockchain

Το Blockchain είναι μια τεχνολογία κατανεμημένου «βιβλίου» - distributed ledger technology (DLT). Επιτρέπει σε ένα σύνολο ισότιμων συμμετεχόντων να συνεργάζονται για να δημιουργήσουν ένα ενοποιημένο και αποκεντρωμένο δίκτυο. Χρησιμοποιεί μεθόδους συναίνεσης (consensus methods) για να επιτρέπει στους συμμετέχοντες να επικοινωνούν καθώς και να μοιράζονται πληροφορίες ή δεδομένα. Δεν υπάρχει ανάγκη για μια κεντρική αρχή, γεγονός που καθιστά ολόκληρο το δίκτυο πιο αξιόπιστο από άλλα δίκτυα. Το σύστημα είναι αδιαπέραστο, ασφαλές και διαφανές.

Ο όρος Blockchain αρχικά χρησιμοποιήθηκε για να περιγραφεί το κατανεμημένο ledger, δηλαδή το «βιβλίο» συναλλαγών, του Bitcoin. Συνεπώς, ένα Blockchain συγκεντρώνει το ιστορικό συναλλαγών και ομαδοποιεί τα δεδομένα κατάλληλα σε blocks, τα οποία μόλις γεμίσουν σε χώρο, επιβεβαιώνονται ως προς την εγκυρότητα τους από τους miners και πλέον ως έγκυρα συνδέονται με το προηγούμενο (χρονικά) block σχηματίζοντας μία ατέρμονη αλυσίδα με πληροφορίες.

Το βασικότερο χαρακτηριστικό που μοιράζονται όλα τα Blockchain είναι η χρήση ενός peer-to-peer δικτύου. Εν συνεχεία, κρίνεται αδήριτη η ανάγκη ύπαρξης ενός μηχανισμού συναίνεσης, ώστε οι όλοι οι κόμβοι του συστήματος να συναινούν με τα κοινόχρηστα δεδομένα. Αναλυτικότερα, η συμφωνία αυτή επιτυγχάνεται με κανόνες ενσωματωμένους στον κώδικα του λογισμικού που εκτελείται από τους κόμβους. Με τους κανόνες αυτούς οι κόμβοι του αποκεντρωμένου δικτύου παραμένουν συγχρονισμένοι και συναινούν με τα κοινόχρηστα δεδομένα.



Εικόνα 1: Ο Κύκλος Ζωής ενός block στο Blockchain του Bitcoin.

Ουσιαστικά, μια συναλλαγή δημιουργείται όταν ένας συμμετέχων στέλνει πληροφορίες σε έναν άλλο. Αφού δημιουργηθούν οι συναλλαγές, πρέπει να επικυρωθούν με τη χρήση αλγορίθμων συναίνεσης (consensus algorithms), διασφαλίζοντας ότι μόνο γνήσιες συναλλαγές προστίθενται στην αλυσίδα block. Τα block είναι τα δομικά στοιχεία της αλυσίδας block και χρησιμοποιούνται για την αποθήκευση συναλλαγών και δεδομένων που απαιτούνται για την επιτυχή λειτουργία της αλυσίδας block. [1]

2.2 Σύγκριση Blockchain με μια Βάση Δεδομένων (Database)

Οι τεχνολογίες Blockchain και Βάσεων Δεδομένων έχουν πολλές ομοιότητες και διαφορές και συχνά συγκρίνονται μεταξύ τους. Ενώ οι δύο τεχνολογίες μπορούν να εξυπηρετήσουν παρόμοιους σκοπούς και να χρησιμοποιηθούν μαζί, λειτουργούν με διαφορετικούς τρόπους.

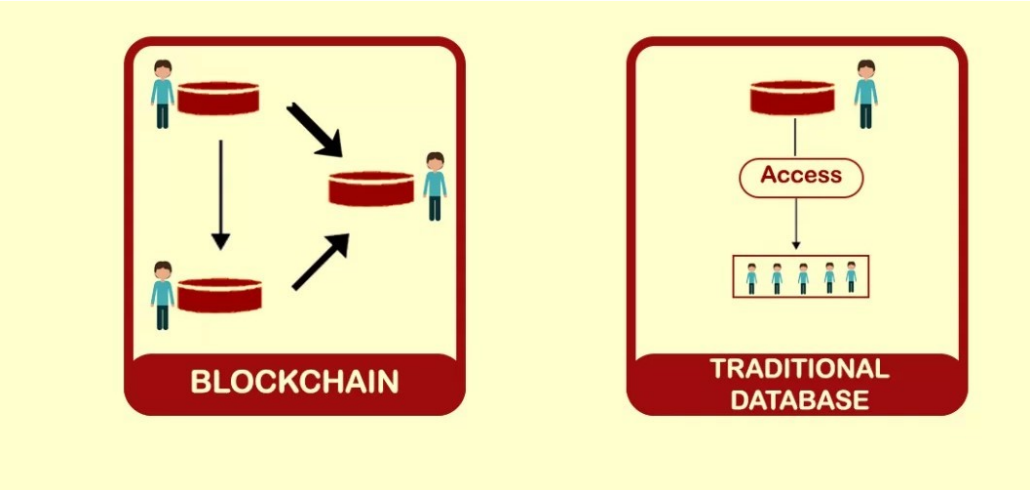
Οι βασικές διαφορές μεταξύ Blockchain και μιας Βάσης Δεδομένων είναι:

Blockchain	**Βάση Δεδομένων**
Αποκεντρωμένη αποθήκευση δεδομένων.	Κεντρική αποθήκευση δεδομένων.
Δεν υπάρχει διαχειριστής.	Χρειάζεται διαχειριστής βάσης δεδομένων.
Η τροποποίηση δεδομένων δεν απαιτεί άδεια. Οι χρήστες έχουν ένα αντίγραφο των δεδομένων και με την τροποποίηση των αντιγράφων δεν επηρεάζει το κύριο αντίγραφο των δεδομένων.	Η τροποποίηση δεδομένων απαιτεί άδεια από τον διαχειριστή της βάσης δεδομένων.
Διατηρεί τις τρέχουσες πληροφορίες καθώς και τις προηγούμενες πληροφορίες που έχουν αποθηκευτεί στο παρελθόν.	Διατηρεί πληροφορίες που είναι ενημερωμένες σε μια συγκεκριμένη στιγμή.
Χρησιμοποιεί λειτουργίες ανάγνωσης και εγγραφής.	Υποστηρίζει CRUD (Δημιουργία, Ανάγνωση, Ενημέρωση και Διαγραφή).
Χρησιμοποιεί ένα κατανεμημένο δίκτυο για αρχιτεκτονική.	Χρησιμοποιεί μια αρχιτεκτονική πελάτη - διακομιστή.
Τα δεδομένα υποστηρίζουν την ακεραιότητα.	Κακόβουλοι παράγοντες μπορούν να αλλάξουν τα δεδομένα της βάσης.
Περιορίζεται από τις μεθόδους επαλήθευσης και συναίνεσης.	Είναι εξαιρετικά γρήγορες, προσφέρουν μεγάλη επεκτασιμότητα.
Προσφέρει διαφάνεια.	Δεν είναι διαφανής. Μόνο ο διαχειριστής αποφασίζει ποιο κοινό μπορεί να έχει πρόσβαση στα δεδομένα.

Η βάση δεδομένων είναι μια συγκεντρωτική δομή δεδομένων που έχει τη δυνατότητα ανάγνωσης, εγγραφής και διαχείρισης. Έχει τη δυνατότητα να αποθηκεύει πολλά αντίγραφα των ίδιων δεδομένων καθώς και το ιστορικό αυτών των δεδομένων. Οι χρήστες με εξουσιοδοτημένη

πρόσβαση μπορούν να διαβάζουν και να γράφουν δεδομένα. Χαρακτηριστικό των βάσεων δεδομένων είναι η εύκολη και γρήγορη πρόσβαση. Η αποθήκευση των δεδομένων είναι απλή και γρήγορη. Ωστόσο, υπάρχουν ορισμένα μειονεκτήματα, το σημαντικότερο από τα οποία είναι η πιθανότητα αλλοίωσης των δεδομένων. Ο διαχειριστής έχει τον πλήρη έλεγχο. Η βάση δεδομένων αποθηκεύει πληροφορίες χρησιμοποιώντας δομή δεδομένων. Η γλώσσα δομημένων ερωτήσεων (SQL) μπορεί να χρησιμοποιηθεί για την υποβολή ερωτημάτων στα αποθηκευμένα δεδομένα. Οι πίνακες χρησιμοποιούνται για την αποθήκευση των στοιχείων δεδομένων.

Η βασική αξία ενός Blockchain είναι η δυνατότητα ενός αρχείου να μοιράζεται απευθείας μέσα στα όρια εμπιστοσύνης (Boundary of Trust), χωρίς να απαιτείται κεντρικός διαχειριστής ή όπου χρειάζεται ο διαμοιρασμός των δεδομένων να αποθηκευτούν στο Blockchain. Επίσης, μπορούν να αποθηκευτούν τα δεδομένα που προκύπτουν από διάφορες συσκευές IoT τα οποία μπορούν να κοινοποιηθούν σε πολλούς φορείς χρησιμοποιώντας το Blockchain.

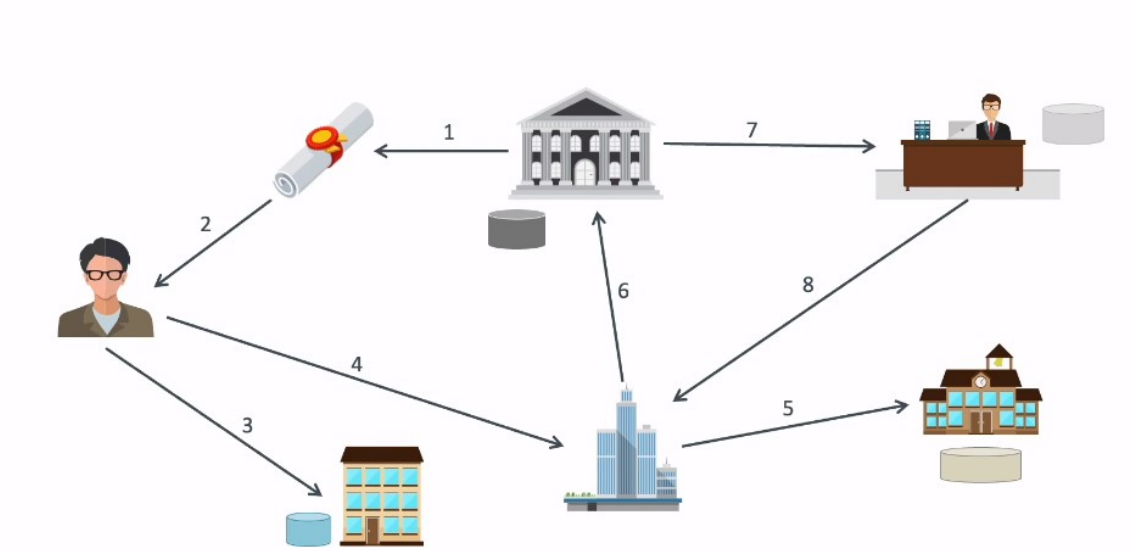


Εικόνα 2: Διαφορά Αποκεντρωμένου και Μη Συστήματος.

Παρακάτω παρουσιάζεται ένα παράδειγμα, όπου οι δύο τεχνολογίες που αναφέρθηκαν εξυπηρετούν τον ίδιο σκοπό, αλλά η χρήση Blockchain είναι προτιμότερη.

Παράδειγμα:
Ο Μπομπ κατέχει πτυχίο από μια πανεπιστημιακή σχολή, ας πούμε το Πανεπιστήμιο Χ′, και προσεγγίζει έναν υπεύθυνο πρόσληψης Ψ′ για να υποβάλει αίτηση για μια συγκεκριμένη εργασιακή θέση με βάση τα τρέχοντα εκπαιδευτικά του προσόντα. Για τον υπεύθυνο πρόσληψης, η διαδικασία επιβεβαίωσης της ταυτότητας φαίνεται πιο περίπλοκη. Ο υπεύθυνος πρόσληψης

πρέπει να πραγματοποιήσει πολλές γραπτές εργασίες και ακόμη κάποιες τηλεφωνικές κλήσεις για να επιβεβαιώσει την αυθεντικότητα της ακαδημαϊκής του εκπαίδευσης. Οι περισσότεροι υπεύθυνοι πρόσληψηςυποβάλλονταιι σε χρονοβόρες διαδικασίες επιβεβαίωσης. Γι΄ αυτό το λόγο, πολλοί από αυτούς αγνοούν συχνά αυτήν τη διαδικασία επαλήθευσης, γεγονός που μπορεί να προκαλέσει σοβαρά προβλήματα και να δημιουργήσει ανεπιθύμητες συνέπειες



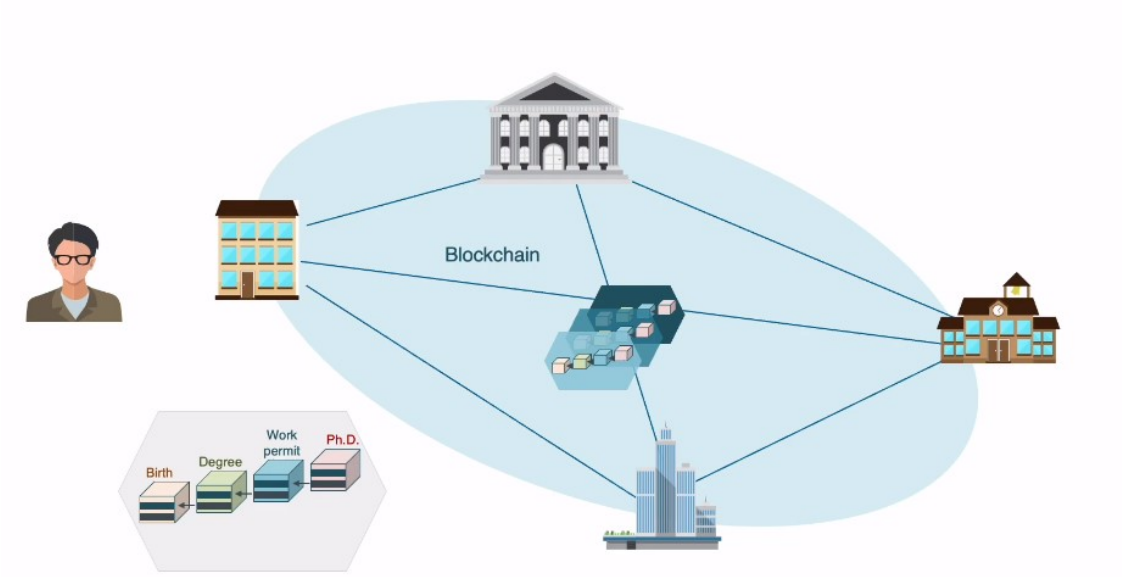
Εικόνα 3: Επαλήθεσυση Εγκυρότητας Πτυχίων με Database.

Επεξήγηση Σχήματος (Εικ.3): Ο Μπομπ (πτυχιούχος Πανεπιστημίου Χ΄) θέλει να πάρει το βαθμό του πτυχίου του για να τον προσκομίσει σε ένα φορέα. Αρχικά, πάει στο Πανεπιστήμιο και παίρνει το πτυχίο του (θέση (1) του Σχήματος), το στέλνει σε ένα φορέα Α (θέση (3) του Σχήματος) που του το ζήτησε και αυτός με τη σειρά του το δρομολογεί στο φορέα Β και Γ (θέση (4), (5) του Σχήματος). Οι φορείς για να ελέγξουν την εγκυρότητα του πτυχίου θα πρέπει πάλι να απευθυνθούν στην έκδουσα αρχή και εκείνη στον αρμόδιο του τμήματος (θέση (7) του Σχήματος).

Έστω τώρα, ότι ο Μπομπ προέρχεται από ένα Πανεπιστήμιο που παρέχει πιστοποιητικό που είναι επαληθεύσιμο μέσω **Blockchain**, η παραπάνω διαδικασία μπορεί να απλοποιηθεί και να ολοκληρωθεί με έναν μόνο κλικ από την πλευρά του υπεύθυνου πρόσληψης. Το μόνο που χρειάζεται να κάνει ο υπεύθυνος πρόσληψης είναι να επιβεβαιώσει ποιος είναι ο εκδότης ενός

συγκεκριμένου εγγράφου, και η αναλλοίωτη βάση δεδομένων Blockchain θα παράσχει τα επαληθεύσιμα ακαδημαϊκά δικαιολογητικά στον υπεύθυνο πρόσληψης που τα χρειάζεται.

Με την ενσωμάτωση των ακαδημαϊκών δικαιολογητικών στο Blockchain, το πανεπιστήμιο επιβεβαιώνει ότι παραχωρεί στους αποφοίτους του μια συγκεκριμένη εξουσία, δηλαδή μια επαληθευμένη ταυτότητα. Με την εφαρμογή αυτής της τεχνολογίας, παρέχεται μια απόδειξη Know Your Customer (KYC), ενισχύοντας τη διαδικασία επαλήθευσης της ταυτότητας των αποφοίτων. Με αυτόν τον τρόπο, δημιουργείται μια αξιόπιστη μέθοδος για τον έλεγχο των πτυχίων και την επιβεβαίωση της ταυτότητας των αποφοίτων, προσφέροντας ένα ασφαλές και αξιόπιστο σύστημα πιστοποίησης.



Εικόνα 4: Επαλήθεσυση Εγκυρότητας Πτυχίων με Blockchain.

2.3 Το Πρόβλημα των Βυζαντινών Στρατηγών

Το Πρόβλημα των Βυζαντινών Στρατηγών είναι ένα θεμελιώδες ζήτημα στη σφαίρα των κατανεμημένων συστημάτων, που περικλείει τις προκλήσεις για την επίτευξη συναίνεσης σε ένα αποκεντρωμένο δίκτυο. Αυτό το πρόβλημα, που προέρχεται από τη θεωρία παιγνίων, είναι ζωτικής σημασίας για την κατανόηση της δυναμικής της λήψης αποφάσεων όπου οι συμμετέχοντες δεν μπορούν να επαληθεύσουν την ταυτότητα ή την ακεραιότητα άλλων σε ένα περιβάλλον που χαρακτηρίζεται από αναξιόπιστα κανάλια επικοινωνίας.

Ένα κατανεμημένο δίκτυο κόμβων υπολογιστών μπορεί να συμφωνήσει σε μια απόφαση, παρότι ορισμένοι από τους κόμβους είναι πιθανό να αποτύχουν ή να ενεργήσουν ανέντιμα. Αυτό είναι το θεμελιώδες ερώτημα που θέτει το Πρόβλημα Βυζαντινών Στρατηγών, το οποίο γέννησε την έννοια «Ανοχή Βυζαντινών Σφαλμάτων».

Επινοήθηκε το 1982 ως ένα λογικό δίλημμα που δείχνει πώς μια ομάδα Βυζαντινών Στρατηγών μπορεί να έχει προβλήματα επικοινωνίας όταν προσπαθεί να συμφωνήσει για την επόμενη κίνησή της.

Το δίλημμα προϋποθέτει ότι κάθε στρατηγός έχει τον δικό του στρατό και ότι κάθε ομάδα βρίσκεται σε διαφορετικές τοποθεσίες γύρω από την πόλη στην οποία σκοπεύουν να επιτεθούν. Οι στρατηγοί πρέπει να συμφωνήσουν είτε να επιτεθούν είτε να αποχωρήσουν. Δεν έχει σημασία αν θα επιτεθούν ή θα υποχωρήσουν, αρκεί όλοι οι στρατηγοί να συμφωνήσουν σε μια κοινή απόφαση, προκειμένου να την εκτελέσουν συντονισμένα.

Επομένως, μπορούμε να σκεφτούμε τις εξής απαιτήσεις:

- Κάθε στρατηγός πρέπει να αποφασίσει: επίθεση ή υποχώρηση (ναι ή όχι).
- Αφού η απόφαση ληφθεί, δεν μπορεί να αλλάξει.
- Όλοι οι στρατηγοί πρέπει να συμφωνήσουν για την ίδια απόφαση και να την εκτελέσουν με συγχρονισμένο τρόπο.

Τα προαναφερθέντα προβλήματα επικοινωνίας σχετίζονται με το γεγονός ότι ένας στρατηγός μπορεί να επικοινωνήσει με έναν άλλο μόνο μέσω μηνυμάτων, τα οποία παραδίδονται από έναν αγγελιοφόρο. Κατά συνέπεια, η κεντρική πρόκληση του προβλήματος των βυζαντινών στρατηγών είναι ότι ενδέχεται τα μηνύματα με κάποιο τρόπο να καθυστερήσουν, να καταστραφούν ή να χαθούν.

Επιπλέον, ακόμη και αν ένα μήνυμα παραδοθεί με επιτυχία, ένας ή περισσότεροι στρατηγοί μπορούν να επιλέξουν (για οποιονδήποτε λόγο) να ενεργήσουν κακόβουλα και να στείλουν ένα δόλιο μήνυμα, ώστε να μπερδέψουν τους άλλους στρατηγούς, οδηγώντας σε πλήρη αποτυχία.

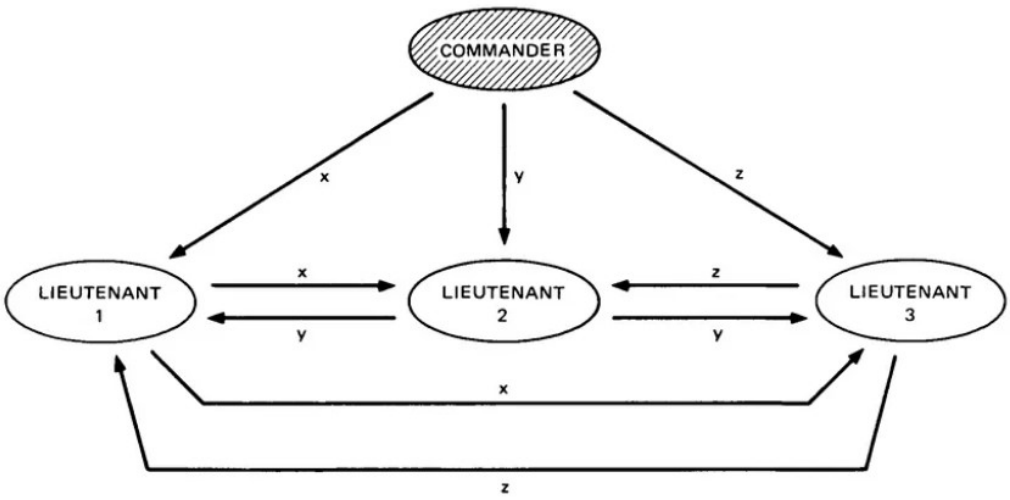
Εάν εφαρμόσουμε το δίλημμα στο πλαίσιο των Blockchain, κάθε στρατηγός αντιπροσωπεύει έναν κόμβο δικτύου και οι κόμβοι πρέπει να επιτύχουν ομοφωνία όσον αφορά την τρέχουσα κατάσταση του συστήματος. Με άλλα λόγια, η πλειοψηφία των συμμετεχόντων σε ένα κατανεμημένο δίκτυο πρέπει να συμφωνήσει και να εκτελέσει την ίδια ενέργεια για να αποφευχθεί η πλήρης αποτυχία.

Ο μόνος τρόπος για να επιτευχθεί ομοφωνία σε αυτούς τους τύπους κατανεμημένων συστημάτων είναι τουλάχιστον 2/3 από τους κόμβους του δικτύου να είναι οι αξιόπιστοι και ειλικρινείς. Αυτό

σημαίνει ότι εάν η πλειοψηφία του δικτύου αποφασίσει να ενεργήσει κακόβουλα, το σύστημα είναι επιρρεπές σε αστοχίες και επιθέσεις.

Τα προηγούμενα γίνονται πιο σαφή με ένα οπτικό παράδειγμα. Εξετάζεται η περίπτωση του διοικητή που είναι προδότης.

Έστω C ο Διοικητής και Li ο Υπολοχαγός i:



Εικόνα 5: Ο Διοικητής είναι Προδότης.
(Aamna Tariq, Hina Binte Haq, Syed Taha Ali, (14 December, 2019).
Cerberus: A Blockchain-Based Accreditation and Degree Verification System) [3]

Βήματα:
Ο L1 στέλνει x στον L2, L3.
Ο L2 στέλνει y στον L1, L3 .
Ο L3 στέλνει z στον L1, L2.
L1 ← majority(x,y,z) — L2 ← majority(x,y,z) — L3 ← majority(x,y,z).

Όλοι έχουν την ίδια τιμή και έτσι επιτυγχάνεται συναίνεση. Ακόμα και αν τα x, y, z είναι όλα διαφορετικά η τιμή της πλειοψηφίας (x, y, z) είναι η ίδια και για τους 3 υπολοχαγούς. Στην

περίπτωση που τα x,y,z είναι εντελώς διαφορετικές εντολές, μπορούμε να υποθέσουμε ότι ενεργούν στην προεπιλεγμένη επιλογή για υποχώρηση.

Εάν εφαρμόσουμε το δίλημμα στο πλαίσιο του Blockchain, κάθε στρατηγός αντιπροσωπεύει έναν κόμβο (node) δικτύου. Οι κόμβοι πρέπει να επιτύχουν συναίνεση στην τρέχουσα κατάσταση του συστήματος. Με άλλο λόγια, η πλειοψηφία των συμμετεχόντων σε ένα κατανεμημένο δίκτυο, πρέπει να συμφωνήσει και να εκτελέσει την ίδια ενέργεια. Στόχος, να αποφευχθεί η πλήρης αποτυχία.

Επομένως, ο μόνος τρόπος για να επιτευχθεί συναίνεση σε αυτούς τους τύπους κατανεμημένου συστήματος είναι να έχουμε τουλάχιστον 2/3 αξιόπιστους και ειλικρινείς κόμβους δικτύου. Αυτό σημαίνει ότι εάν η πλειονότητα του δικτύου αποφασίσει να δράσει κακόβουλα, το σύστημα είναι ευαίσθητο σε αποτυχίες και επιθέσεις.

Με λίγα λόγια, η **Ανοχή Βυζαντινών Σφαλμάτων - Byzantine Fault Tolerance (BFT)** είναι ιδιότητα ενός συστήματος που είναι σε θέση να αντισταθεί στην κατηγορία των αποτυχιών, που προέρχονται από το πρόβλημα των Βυζαντινών Στρατηγών. Αυτό σημαίνει ότι ένα σύστημα BFT είναι σε θέση να συνεχίσει να λειτουργεί ακόμη και αν ορισμένοι από τους κόμβους αποτύχουν ή ενεργούν κακόβουλα.

Υπάρχουν περισσότερες από μία πιθανές λύσεις στο πρόβλημα των Βυζαντινών Στρατηγών και, ως εκ τούτου, πολλοί τρόποι δημιουργίας ενός συστήματος BFT. Ομοίως, υπάρχουν διαφορετικές προσεγγίσεις για ένα Blockchain, για την επίτευξη Ανοχής Βυζαντινών Σφαλμάτων. Αυτό μας οδηγεί στους λεγόμενους αλγορίθμους συναίνεσης. [5]

2.4 Proof of Work (PoW)

Ο αλγόριθμος Proof of Work είναι ο πιο δημοφιλής αλγόριθμος συναίνεσης που χρησιμοποιείται από κρυπτονομίσματα όπως το Bitcoin και το Ethereum. Στο Proof of Work, προκειμένου να προστεθεί ένα block στο Blockchain, πρέπει ένας υπολογιστής να βρει μια λύση σε ένα συγκεκριμένο μαθηματικό πρόβλημα.

Κάθε φορά που εξορύσσεται ένα νέο block, αυτός ο εξορύκτης ανταμείβεται με κάποιο νόμισμα και έτσι δίνεται κίνητρο να συνεχίσει την εξόρυξη. Στο Proof of Work, άλλοι κόμβοι επαληθεύουν την εγκυρότητα του block ελέγχοντας ότι ο κατακερματισμός των δεδομένων του block είναι μικρότερος από έναν προκαθορισμένο αριθμό, σύμφωνα με τον παρακάτω τύπο:

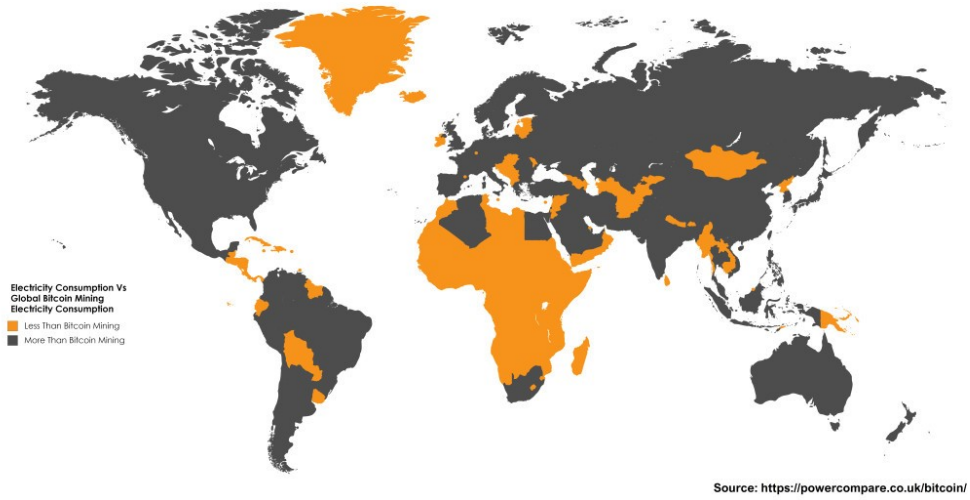
$$H(\textbf{data} + \textbf{nonce}) < \textbf{target}, \text{ όπου:}$$

Συνάρτηση Κατακερματισμού (H): Αναπαριστά τη συνάρτηση που παράγει το hash των δεδομένων του block και του nonce. Συμβολίζεται ως $H(\text{data} + \text{nonce})$.
Δεδομένα Block ($data$): Είναι οι πληροφορίες που περιέχονται στο block, όπως συναλλαγές, χρονικά στοιχεία και άλλα στοιχεία.
Nonce ($nonce$): Είναι ένας ακέραιος αριθμός που προσαρτάται στα δεδομένα του block και τροποποιείται μέχρις ότου το hash να πληροί τη συγκεκριμένη δυσκολία.

Στόχος (*target*): Είναι ο προκαθορισμένος αριθμός που καθορίζει το επίπεδο δυσκολίας. Το hash πρέπει να είναι μικρότερο από τον στόχο για να θεωρείται έγκυρο.

Λόγω της περιορισμένης παροχής υπολογιστικής ισχύος, οι miners έχουν επίσης κίνητρα να μην εξαπατήσουν. Η επίθεση στο δίκτυο θα κόστιζε πολύ λόγω του υψηλού κόστους του υλικού, της ενέργειας και των πιθανών κερδών εξόρυξης που χάνονται.

Το Proof of Work παρέχει την απαιτούμενη ασφάλεια και έχει αποδειχθεί ότι λειτουργεί αρκετά καλά μέχρι στιγμής. Ωστόσο, είναι πολύ ενεργοβόρο. [6]



The map above shows which countries consume less electricity than the amount consumed by global bitcoin mining

Εικόνα 6: Σχεδόν όλες οι αφρικανικές χώρες (ξεχωριστά) καταναλώνουν λιγότερη ηλεκτρική ενέργεια από τη βιομηχανία εξόρυξης Bitcoin.

Επεξήγηση Σχήματος (Εικ.6): Η συνολική ετήσια κατανάλωση ενέργειας του Bitcoin είναι ισοδύναμη με το 0,13% της συνολικής ετήσιας κατανάλωσης ενέργειας σε ολόκληρο τον κόσμο. Οι χώρες με το πορτοκαλί στον χάρτη είναι εκείνες που κάθε μία από αυτές χρησιμοποιεί λιγότερο ηλεκτρικό ρεύμα ετησίως από ό,τι χρειάζεται για να τροφοδοτήσει το Bitcoin. Πράγματι, αν το Bitcoin ήταν χώρα, θα κατατάσσονταν 61η στον κόσμο όσον αφορά την κατανάλωση ηλεκτρικής ενέργειας.)

2.5 Proof of Stake (PoS)

Ο αλγόριθμος Proof of Stake είναι ένας σχετικά διαφορετικός και νέος τρόπος να δημιουργηθούν block μέσα σε ένα Blockchain (mining), διαφορετικό από αυτό του αλγορίθμου Proof of Work. Η διασφάλιση της συνέπειας στο Proof of Stake βασίζεται στην οικονομική κατάσταση ενός κόμβου του Blockchain δικτύου. Όλοι οι κόμβοι ή αλλιώς «επικυρωτές» (validators) κατέχουν ένα σύνολο ψηφιακών κερμάτων (Bitcoins) και ανάλογα με την ποσότητα κερμάτων (stake), που απαιτείται να έχουν για συγκεκριμένο χρονικό διάστημα, μπορούν να συμμετέχουν στη διαδικασία επικύρωσης. Με άλλα λόγια οι πιθανότητες εκλογής ενός κόμβου ως validator του επόμενου block είναι ανάλογες με το ποσό πονταρίσματος που έχει διαθέσει. Έτσι, οι κόμβοι πάλι έχουν να λύσουν ένα κρυπτογραφικό πρόβλημα, αλλά το κλειδί στη λύση είναι το ποσό του στοιχήματος που έχει διαθέσει ο κόμβος και το χρονικό διάστημα που έχει παρέλθει από το ποντάρισμα.

Η διαδικασία mining σε PoS δεν είναι η προσαρμογή του nonce στην σωστή απάντηση κι έτσι δεν απαιτείται υπολογιστική δύναμη, εξοικονομώντας ενέργεια καθώς αξιοποιεί το νομισματικό κίνητρο (Stake) που διαθέτει. Επιπλέον, ο αλγόριθμος PoS είναι απρόσβλητος σε μια επίθεση κατά 51%, λόγω των προστίμων που επιβάλλονται στους validators για οποιαδήποτε ψευδή διαδικασία επαλήθευσης. Ο επιτιθέμενος πρέπει επίσης να κρατήσει αρκετά Bitcoins για πολύ καιρό πριν επιτεθεί στο δίκτυο, αυξάνοντας έτσι τη δυσκολία της επίθεσης.

Γίνεται αναλογία της εκλογής αρχηγού (αυτού που θα επιλέξει το επόμενο block) με μια λαχειοφόρο αγορά:
Σε μια λοταρία, πιθανολογικά, αν ο Μπομπ έχει περισσότερους λαχνούς από την Αλίκη, είναι πιο πιθανό να κερδίσει. Με έναν πολύ παρόμοιο τρόπο, στο Proof of Work, αν ο Μπομπ έχει περισσότερη υπολογιστική ισχύ και ενέργεια από την Αλίκη - και επομένως μπορεί να παράγει περισσότερη εργασία - είναι πιο πιθανό να κερδίσει («εξορύξει» το επόμενο block). Στο Proof of Stake, αν ο Bob έχει μεγαλύτερο ποντάρισμα από την Alice, είναι πιο πιθανό να κερδίσει («εξορύξει» το επόμενο block). [7]

2.6 Proof of Authority (PoA)

Σύμφωνα με τον Proof of Authority (PoA) αλγόριθμο, υπάρχουν προεπιλεγμένοι κόμβοι οι οποίοι είναι υπεύθυνοι για την επικύρωση των συναλλαγών και την δημιουργία νέων block. Σε αντιστοιχία με τους άλλους αλγόριθμους ο κόμβος που θέλει να δημιουργήσει το νέο block παρουσιάζει την «ταυτότητα» του και όχι τα tokens που έχει ποντάρει, την υπολογιστική του δύναμη. Αυτός ο αλγόριθμος είναι πολύ αποδοτικός αφού μόνο συγκεκριμένοι κόμβοι μπορούν δημιουργήσουν block και οι συναλλαγές γίνονται πολύ γρήγορα. Ακόμη εξουδετερώνει τον κίνδυνο της «51%» επίθεσης, αφού θα έπρεπε ο κακόβουλος χρήστης να είχε στον έλεγχο του πάνω από 50% των κόμβων που έχουν προεπιλεγεί ως συμμετέχοντες. Αυτός ο αλγόριθμος βρίσκει εφαρμογή κυρίως σε private ή permissioned Blockchains.[7]

2.7 Κρυπτογραφικά Θεμελιώδη Στοιχεία στο Blockchain

Οι κρυπτογραφικές πρωταρχικές διαδικασίες (cryptographic primitives) είναι οι βασικές διαδικασίες ενός πρωτοκόλλου ή ενός συστήματος ασφαλείας. Μπορούν να διακριθούν σε τρεις βασικές κατηγορίες: α) στις διαδικασίες χωρίς κλειδί, β) στις διαδικασίες συμμετρικού κλειδιού και γ) στις διαδικασίες δημοσίου κλειδιού. Για την παρούσα διπλωματική όμως είναι σημαντικό να κατανοηθούν έννοιες όπως των hash functions (συναρτήσεις κατακερματισμού), homomorphic encryption (ομομορφική κρυπτογράφηση), ανωνυμία, ψηφιακές υπογραφές και ελλειπτικές καμπύλες.

- **Hash functions (Συναρτήσεις κατακερματισμού)**
  Μια συνάρτηση κατακερματισμού είναι μια μαθηματική συνάρτηση η οποία μπορεί να αντιστοιχεί δεδομένα τυχαίου μεγέθους (που ονομάζεται «μήνυμα») σε δεδομένα σταθερού μεγέθους (ονομάζεται τιμή κατακερματισμού ή απλά κατακερματισμός).

  Βασικά σημεία:

  1. Μια συνάρτηση κατακερματισμού είναι μια μαθηματική συνάρτηση που μετατρέπει οποιαδήποτε ψηφιακά δεδομένα σε μια συμβολοσειρά εξόδου με σταθερό αριθμό χαρακτήρων.
  2. Ο κατακερματισμός είναι χρήσιμος για τη διασφάλιση της αυθεντικότητας ενός τμήματος δεδομένων και ότι δεν έχει παραβιαστεί, καθώς ακόμη και μια μικρή αλλαγή στο μήνυμα θα δημιουργήσει έναν εντελώς διαφορετικό κατακερματισμό.
  3. Οι συναρτήσεις κατακερματισμού είναι τα βασικά εργαλεία της σύγχρονης κρυπτογραφίας που χρησιμοποιούνται στην ασφάλεια πληροφοριών για τον έλεγχο ταυτότητας συναλλαγών, μηνυμάτων και ψηφιακών υπογραφών.

  Επομένως, ο κατακερματισμός είναι η εκτέλεση μιας εισόδου σε έναν τύπο που τη μετατρέπει σε μήνυμα εξόδου σταθερού μήκους. Ανεξάρτητα από το πόσοι χαρακτήρες είναι η είσοδος, η έξοδος θα είναι πάντα η ίδια ως προς τον αριθμό των δεκαεξαδικών (γράμματα και αριθμοί) χαρακτήρων.

  Ουσιαστικά, όταν κατακερματίζεται ένα μήνυμα, παίρνει το αρχείο ή το μήνυμά οποιουδήποτε μεγέθους, το τρέχει μέσω ενός μαθηματικού αλγόριθμου και βγάζει μια έξοδο σταθερού μήκους. Μια συνάρτηση κατακερματισμού εξαρτάται από τον αλγόριθμο, αλλά γενικά, για να ληφθεί η τιμή κατακερματισμού ενός καθορισμένου μήκους, πρέπει πρώτα να διαιρεθούν τα δεδομένα εισόδου σε block σταθερού μεγέθους, τα οποία ονομάζονται block δεδομένων. Στη συνέχεια, η συνάρτηση κατακερματισμού επαναλαμβάνεται όσες φορές είναι ο αριθμός των block δεδομένων. Οι hash functions πρέπει να είναι ντετερμινιστικές – που σημαίνει ότι κάθε φορά που εισάγετε την ίδια είσοδο, θα δημιουργεί πάντα την ίδια έξοδο. Με άλλα λόγια, η έξοδος ή η τιμή κατακερματισμού πρέπει να είναι μοναδική για την ακριβή είσοδο. Δεν θα πρέπει να υπάρχει καμία πιθανότητα ότι δύο διαφορετικές είσοδοι μηνυμάτων δημιουργούν τον ίδιο κατακερματισμό εξόδου.

  Μια συνάρτηση κατακερματισμού που είναι collision-resistant (ανθεκτική σε συγκρούσεις) δηλώνει ότι είναι δύσκολο να βρεθούν δύο διαφορετικά μηνύματα που παράγουν τον ίδιο κατακερματισμό. Αυτό είναι σημαντικό για την ασφάλεια, καθώς αποτρέπει ανεπιθύμητες

συγκρούσεις που θα μπορούσαν να οδηγήσουν σε προβλήματα ασφαλείας, όπως η παραβίαση κρυπτογραφικών συστημάτων.

Επίσης, η διαδικασία του κατακερματισμού πρέπει να είναι ανεξάρτητη και να παράγει αποτελέσματα που φαίνονται τυχαία. Αυτό ενισχύει τον χαρακτήρα της τυχαιότητας στον τομέα της κρυπτογραφίας, καθιστώντας δύσκολη την πρόβλεψη των αποτελεσμάτων. Η τυχαιότητα σε αυτό το πλαίσιο προσθέτει ένα επιπλέον επίπεδο πολυπλοκότητας, καθιστώντας δύσκολη την αντίληψη των προτύπων ή των επαναλαμβανόμενων συμπεριφορών, ενισχύοντας έτσι την ασφάλεια της διαδικασίας.

Ειδικότερα, το blockchain του Ethereum χρησιμοποιεί το Keccak-256. Ο Keccak-256 είναι ένας αλγόριθμος κατακερματισμού. Με το Keccak-256 είναι δυνατή η μετατροπή μιας εισόδου σε έξοδο κατακερματισμού. Αυτή η έξοδος είναι πάντα σταθερού μήκους: αποτελείται από 256 bit (bytes 32). Το Keccak-256 είναι μια μονόδρομη συνάρτηση κατακερματισμού. Αυτό σημαίνει ότι ο κατακερματισμός λειτουργεί μόνο με έναν τρόπο. Έτσι, μπορείτε να μετατρέψετε την είσοδο σε κατακερματισμό, αλλά δεν είναι δυνατός ο προσδιορισμός του περιεχομένου με βάση τον κατακερματισμό. Ο κατακερματισμός δεν δημιουργείται χρησιμοποιώντας κλειδιά. Όταν τα δεδομένα είναι ασφαλισμένα με δημόσιο και ιδιωτικό κλειδί, μιλάμε για κρυπτογράφηση ή κρυπτογραφία. Η κρυπτογραφία συχνά συγχέεται με τον κατακερματισμό. Ωστόσο, και οι δύο τεχνικές χρησιμοποιούνται για κρυπτονομίσματα. Επίσης όταν εκτελούμε μια συναλλαγή στο blockchain, την υπογράφουμε με ψηφιακή υπογραφή. Για μια τέτοια ψηφιακή υπογραφή χρειάζεται ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί. Συνδυάζοντας αυτά το ένα με το άλλο, δημιουργείται ένα νέο αποτέλεσμα. Αυτό το αποτέλεσμα διασφαλίζεται με το Keccak-256. Ο αλγόριθμος αυτός λοιπόν έχει πολύ σημαντικό ρόλο στην εκτέλεση των συναλλαγών.[8]

- **Ελλειπτικές Καμπύλες και Ψηφιακές υπογραφές**

  Η κρυπτογραφία ελλειπτικής καμπύλης (ECC) είναι ένας τύπος κρυπτογραφικού συστήματος δημόσιου κλειδιού. Αυτή η κατηγορία συστημάτων βασίζεται σε απαιτητικά «μονόδρομα» (one-way) μαθηματικά προβλήματα - που είναι εύκολο να υπολογιστούν, δύσκολο να αντιστραφούν. Μερικές φορές αυτά αποκαλούνται trapdoor (καταπακτή): για να λύσει κάποιος εύκολα το πρόβλημα, πρέπει να γνωρίζει κάποιο μυστικό.

  Για παράδειγμα, το σύστημα RSA χρησιμοποιεί μια κατηγορία «μονόδρομων» προβλημάτων που αφορούν την παραγοντοποίηση. Κάθε αριθμός έχει μια μοναδική παραγοντοποίηση πρώτων αριθμών. Για παράδειγμα, το 8 μπορεί να εκφραστεί ως 2^3 και το 30 είναι

  $$2 \cdot 3 \cdot 5.$$

  Αν ζητηθεί να λυθεί (με αριθμομηχανή) το

  $$13 \cdot 19,$$

  γρήγορα προκύπτει ότι είναι 247. Ωστόσο, αν ζητηθεί η άλλη πλευρά και να λυθεί την παραγοντοποίηση του 247 σε πρώτους αριθμούς, θα ήταν πιο δύσκολο (ακόμη και με υπολογιστή).

Το ECC δεν βασίζεται στην παραγοντοποίηση, αλλά αντίθετα λύνει εξισώσεις (ελλειπτικές καμπύλες) της μορφής:

$$y^2 = x^3 + ax + b.$$

Βασίζεται στο γεγονός ότι μπορεί να προσδιοριστεί ένα τρίτο σημείο, λαμβάνοντας υπόψη δύο σημεία στη γραμμή. Στην Εικόνα 7 φαίνεται η γραφική εξίσωση με τα σημεία P, Q και R.
Οι ελλειπτικές καμπύλες έχουν μερικές μοναδικές ιδιότητες. Το πιο σημαντικό είναι ότι μπορεί να οριστεί ένα είδος πράξης στην καμπύλη – μια πράξη που ικανοποιεί μαθηματικά ένα σύνολο κριτηρίων που ονομάζεται ομάδα. Θα χρησιμοποιήσουμε το + «τελεστή» και μπορείτε να το σκεφτείτε ως έναν τύπο προσθήκης.

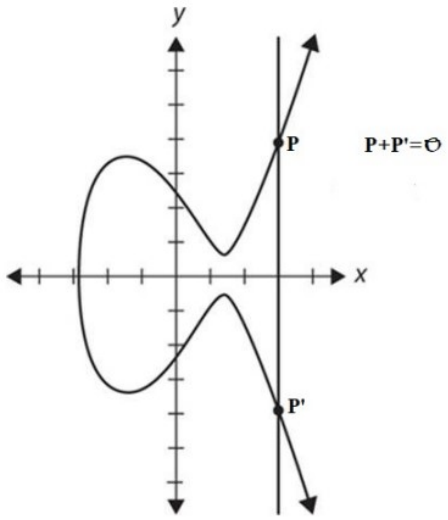
Για μια ευθεία που τέμνει τρία σημεία, $P + Q + R = 0$, που σημαίνει ότι $P + Q = -R$. Το σημείο 0 ορίζεται ως ένα «σημείο στο άπειρο» – ένας εύκολος τρόπος να σκεφτεί κανείς αυτό το σημείο είναι να σκεφτεί παράλληλες σιδηροδρομικές γραμμές που φαίνονται να τέμνονται στον ορίζοντα. Ορίζεται αντίστροφα ως το σημείο που αναστρέφεται πάνω από την οριζόντια γραμμή συμμετρίας. Η εναλλαξιμότητα μπορεί εύκολα να αποδειχθεί, δηλαδή, $P + Q = Q + P$. Η συσχέτιση δεν είναι τόσο προφανής αλλά ισχύει επίσης, δηλαδή $P + (Q + R) = (P + Q) + R$. Το στοιχείο ταυτότητας (ένα στοιχείο που μπορεί να εφαρμοστεί σε οποιοδήποτε άλλο στοιχείο και αφήνει αυτό το στοιχείο αμετάβλητο, π.χ. το 0) είναι το σημείο στο άπειρο.

Στην κρυπτογραφία ελλειπτικής καμπύλης (ECC), το εύκολο πρόβλημα είναι η επίλυση του «προβλήματος του διακριτού λογαρίθμου» (DLP - Discrete Logarithm Problem) σε έναν πεπερασμένο πεδίο. Αντίθετα, το δύσκολο πρόβλημα στην ECC είναι η αποκρυπτογράφηση με βάση το «πρόβλημα του διακριτού λογαρίθμου» (DLP). Δηλαδή, είναι εύκολο να υπολογιστεί ένα διακριτικό λογάριθμο σε μια ελλειπτική καμπύλη, αλλά είναι δύσκολο να αντιστραφεί, δηλαδή να βρεθεί το αντίστροφο.

Το «Discrete Logarithm Problem (DLP)» στο πλαίσιο των ελλειπτικών καμπυλών αναφέρεται στη δυσκολία του υπολογισμού του λογαρίθμου μιας συγκεκριμένης τιμής σε σχέση με ένα δεδομένο βάση, μέσα σε ένα πεπερασμένο πεδίο.

Αν σκεφτούμε μια ελλειπτική καμπύλη, η οποία είναι μια καμπύλη πάνω σε ένα πεπερασμένο σώμα, τότε το πρόβλημα αυτό αναφέρεται στο να βρεθεί ο λογάριθμος μιας τιμής (σημείου) σε σχέση με μια άλλη τιμή που λειτουργεί ως βάση. Στην περίπτωση των ελλειπτικών καμπυλών, το DLP είναι το μαθηματικό πρόβλημα που βασίζεται στη δυσκολία του υπολογισμού του παραπάνω λογαρίθμου.

Για παράδειγμα, έστω μια ελλειπτική καμπύλη και ένα σημείο P που βρίσκεται σε αυτήν, τότε το DLP θα είναι η δυσκολία του να βρεθεί ο ακέραιος k τέτοιος ώστε $P = kG$, όπου G είναι ένα σταθερό σημείο που λειτουργεί ως βάση. Αυτή η δυσκολία είναι η ουσία της κρυπτογραφίας ελλειπτικής καμπύλης και χρησιμοποιείται για την ασφαλή υλοποίηση διάφορων πρωτοκόλλων κρυπτογραφίας, όπως οι ψηφιακές υπογραφές.



Εικόνα 7: Ελλειπτικές Καμπύλες.
(Verma, Sharad Ojha, Badri. (2012). A Discussion on Elliptic Curve Cryptography and Its Applications. International Journal of Computer Science Issues. [10]

Η κρυπτογραφία ελλειπτικής καμπύλης (ECC) είναι ένα βασικό συστατικό του blockchain Ethereum και παρέχει την υποκείμενη ασφάλεια για τις ψηφιακές υπογραφές και την κρυπτογράφηση δημόσιου κλειδιού. Το ECC βασίζεται στην άλγεβρα των ελλειπτικών καμπυλών για τη δημιουργία ζευγών δημόσιων και ιδιωτικών κλειδιών που χρησιμοποιούνται για την επαλήθευση υπογραφών και την κρυπτογράφηση/αποκρυπτογράφηση μηνυμάτων. Το Ethereum χρησιμοποιεί τις παραμέτρους της ελλειπτικής καμπύλης secp256k1 που σχεδιάστηκαν αρχικά για το Bitcoin. Η καμπύλη secp256k1 ορίζεται σε ένα πεπερασμένο πεδίο 256 bit και παρέχει 128 bit ασφάλειας, πράγμα που σημαίνει ότι ένας εισβολέας θα πρέπει να εκτελέσει 2^{128} λειτουργίες για να την σπάσει. Αυτός ο αριθμός είναι τεράστιος και υπερβαίνει τις σημερινές υπολογιστικές δυνατότητες, καθιστώντας μια τέτοια επίθεση (brute force) ανέφικτη από πρακτική άποψη.

Μια επίθεση brute force συνίσταται στο να δοκιμάζει κάθε δυνατή πιθανότητα για το κλειδί μέχρι να βρει το σωστό. Συνδέεται με την ασφάλεια των κρυπτοσυστημάτων, όπως η

καμπύλη secp256k1 που χρησιμοποιείται στο Bitcoin, γιατί εάν το κλειδί είναι απλά ένας αριθμός, μπορεί κάποιος να δοκιμάσει κάθε δυνατό αριθμητικό συνδυασμό για να βρει το σωστό κλειδί. Η δυσκολία του προβλήματος είναι ουσιαστικά ο αριθμός των πιθανών συνδυασμών που πρέπει να δοκιμαστούν.

Ένας εισβολέας που εφαρμόζει επίθεση brute force θα δοκίμαζε σειριακά όλες τις πιθανές τιμές αυτού του αριθμού μέχρι να βρει τη σωστή. Η ασφάλεια του συστήματος κρυπτογραφίας συνήθως εξασφαλίζεται από το μεγάλο μήκος αυτού του κλειδιού, καθιστώντας την ανέφικτη λόγω του υπερβολικού αριθμού πιθανών τιμών προς δοκιμή.

Κάθε λογαριασμός Ethereum έχει ένα ιδιωτικό κλειδί που προέρχεται από έναν τυχαία δημιουργημένο αριθμό 256 bit. Το ιδιωτικό κλειδί χρησιμοποιείται στη συνέχεια για τη δημιουργία ενός δημόσιου κλειδιού μέσω ενός πολλαπλασιασμού σημείου ελλειπτικής καμπύλης. Το δημόσιο κλειδί προκύπτει πολλαπλασιάζοντας το ιδιωτικό κλειδί με το σημείο παραγωγής G της καμπύλης. Για να δημιουργήσει μια ψηφιακή υπογραφή, ο υπογράφων υπολογίζει τον κατακερματισμό του μηνύματος και στη συνέχεια υπογράφει τον κατακερματισμό με το ιδιωτικό του κλειδί χρησιμοποιώντας έναν αλγόριθμο ελλειπτικής καμπύλης όπως ο Elliptic Curve Digital Signature Algorithm. Η υπογραφή που προκύπτει περιέχει δύο αριθμούς 256-bit που αναφέρονται ως r και s.

Το Ethereum χρησιμοποιεί επίσης μια πρόσθετη v μεταβλητή (αναγνωριστικό ανάκτησης). Η υπογραφή μπορεί να σημειωθεί ως r, s, v.

Για να δημιουργήσετε μια υπογραφή χρειάζονται το μήνυμα για υπογραφή και το ιδιωτικό κλειδί (d_a) για να υπογραφεί. Η «απλοποιημένη» διαδικασία υπογραφής μοιάζει κάπως έτσι:

1. Υπολογίζεται ένας κατακερματισμός (e) από το μήνυμα προς υπογραφή.

2. Δημιουργείται μια ασφαλής τυχαία τιμή για το k.

3. Υπολογίζεται το σημείο (x_1, y_1) της ελλειπτικής καμπύλης πολλαπλασιάζοντας k με τη G σταθερά της ελλειπτικής καμπύλης.

4. Υπολογίζεται

$$r = x_1 \bmod n.$$

Αν r ισούται με μηδέν, επιστροφή στο βήμα 2.

5. Υπολογίζεται $s = k^{-1}(e + rd_a) \bmod n$. Αν s ισούται με μηδέν, επιστροφή στο βήμα 2.

Επειδή χρησιμοποιείται μια τυχαία τιμή για το k, η υπογραφή θα είναι διαφορετική κάθε φορά.

Η r, s, v υπογραφή μπορεί να συνδυαστεί σε μια ακολουθία μήκους 65 byte: 32 byte για r, 32 byte για s, και ένα byte για v. Αν κωδικοποιηθεί ως δεκαεξαδική συμβολοσειρά, καταλήγει σε μια συμβολοσειρά μήκους 130 χαρακτήρων, η οποία χρησιμοποιείται από τα περισσότερα πορτοφόλια και διεπαφές.

Το v είναι το τελευταίο byte της υπογραφής. Αυτό το αναγνωριστικό είναι σημαντικό σε ελλειπτικές καμπύλες πολλά σημεία στην καμπύλη μπορούν να υπολογιστούν από το r και s μόνα τους. Αυτό θα είχε ως αποτέλεσμα δύο διαφορετικά δημόσια κλειδιά (άρα διευθύνσεις) να μπορούν να ανακτηθούν. Το v ουσιαστικά υποδεικνύει ποιο από αυτά τα σημεία να χρησιμοποιήσετε.

Το ECC (elliptic curve cryptography) παρέχει στο Ethereum έναν τρόπο ψηφιακής υπογραφής συναλλαγών με ασφαλή και αποτελεσματικό τρόπο. Τα μαθηματικά της ελλειπτικής καμπύλης διασφαλίζουν ότι είναι υπολογιστικά ανέφικτο για έναν εισβολέα να αντλήσει το ιδιωτικό κλειδί από το δημόσιο κλειδί. Αυτό επιτρέπει την ελεύθερη κοινή χρήση διευθύνσεων δημόσιων κλειδιών, διασφαλίζοντας παράλληλα ότι τα ιδιωτικά κλειδιά παραμένουν μυστικά.

Στο κεφάλαιο 5.7 της παρούσας διπλωματικής γίνεται περαιτέρω αναφορά στη χρήση ψηφιακών υπογραφών στα Έξυπνα Συμβόλαια.

- **Homomorphic encryption (Ομομορφική κρυπτογράφηση)**
  Η τεχνολογία κρυπτογράφησης είναι εξαιρετικά σημαντική. Αποτελεί τη βάση του Διαδικτύου, βρίσκεται στην καρδιά του Web3 και επιτρέπει στα άτομα να προστατεύουν τα προσωπικά τους δεδομένα. Ωστόσο, οι παραδοσιακές μεθόδοι κρυπτογράφησης έχουν ένα σημαντικό περιορισμό: τα δεδομένα πρέπει να αποκρυπτογραφηθούν πριν από την ανάλυση και τον υπολογισμό τους. Φυσικά, η αποκρυπτογράφηση προσωπικών δεδομένων και η έκθεσή τους σε τρίτους υπονομεύει τους λόγους για τους οποίους τα δεδομένα κρυπτογραφούνται αρχικά.

  Η ομομορφική κρυπτογράφηση ξεπερνά αυτόν τον περιορισμό επιτρέποντας στα κρυπτογραφημένα δεδομένα να υπολογίζονται. Αυτό σημαίνει ότι μπορούν οι παροχείς υπηρεσιών στο cloud ή web-based υπηρεσίες να υπολογίσουν δεδομένα χωρίς να χρειαστεί να αποκαλυφθούν τα αρχικά δεδομένα σε αυτούς. Η ομομορφική κρυπτογράφηση είναι μια κρυπτογραφική τεχνική που επιτρέπει την εκτέλεση υπολογισμών σε κρυπτογραφημένα δεδομένα χωρίς την ανάγκη αποκρυπτογράφησής τους. Αυτό σημαίνει ότι τα αρχικά δεδομένα παραμένουν πλήρως κρυπτογραφημένα κατά τη διάρκεια επεξεργασίας και εκτέλεσης διάφορων αλγορίθμων και αναλύσεων. Αυτό επιτρέπει στα δεδομένα να παρεμένουν ιδιωτικά ενώ τα μοιράζονται με τρίτους για επεξεργασία.

  Παρότι η ομομορφική κρυπτογράφηση είχε σχεδιαστεί από τους Rivest, Adleman και Dertouzos το 1978, δεν ολοκληρώθηκε πλήρως μέχρι το 2009. Αυτό επετεύχθη από τον λαμπρό επιστήμονα των υπολογιστών Craig Gentry, που έλαβε το Βραβείο MacArthur. Ο Gentry περιέγραψε την ομομορφική κρυπτογράφηση, παρομοιάζοντάς την με τη χρήση ειδικών γαντιών που επιτρέπουν τον χειρισμό των αντικειμένων που είναι κλειδωμένα μέσα σε ένα μαύρο κουτί:

  «Οποιοσδήποτε μπορεί να έρθει και να βάλει τα χέρια του μέσα στα γάντια και να χειρίζεται ό,τι υπάρχει μέσα στο κλειδωμένο κουτί. Δεν μπορούν να τα βγάλουν έξω από το κουτί, αλλά μπορούν να τα χειριστούν, δηλαδή να τα επεξεργαστούν... Μετά τελειώνουν και το

άτομο με το μυστικό κλειδί πρέπει να έρθει και να το ανοίξει—και μόνο αυτό μπορεί να εξάγει το τελικό προϊόν από εκεί». [11]

Για ευαίσθητα δεδομένα, όπως πληροφορίες υγειονομικής περίθαλψης, μπορεί να χρησιμοποιηθεί ομομορφική κρυπτογράφηση για την ενεργοποίηση νέων υπηρεσιών καταργώντας τα εμπόδια απορρήτου που εμποδίζουν την κοινή χρήση δεδομένων ή αυξάνοντας την ασφάλεια των υπαρχουσών υπηρεσιών. Για παράδειγμα, η προγνωστική ανάλυση στην υγειονομική περίθαλψη μπορεί να είναι δύσκολο να εφαρμοστεί μέσω τρίτου παρόχου υπηρεσιών λόγω ανησυχιών σχετικά με το απόρρητο των ιατρικών δεδομένων, αλλά εάν ο πάροχος υπηρεσιών προγνωστικών αναλυτικών στοιχείων λειτουργήσει σε κρυπτογραφημένα δεδομένα, αυτές οι ανησυχίες για το απόρρητο μειώνονται. Επιπλέον, ακόμη και αν το σύστημα του παρόχου υπηρεσιών παραβιαστεί, τα δεδομένα θα παραμείνουν ασφαλή.

- **Anonymity (Ανωνυμία) και Privacy (Ιδιωτικότητα)**
  Στη συνεχώς εξελισσόμενη βιομηχανία κρυπτονομισμάτων, το Ethereum έχει αναδειχθεί ως μια πρωτοποριακή δύναμη, λόγω της επαναστατικής προσέγγισής του στα έξυπνα συμβόλαια και στις αποκεντρωμένες εφαρμογές (dApps). Ωστόσο, μέσα σε όλες τις πρωτοποριακές καινοτομίες, το Ethereum αντιμετωπίζει μια σοβαρή ανησυχία που θα μπορούσε να υπονομεύσει τις δυνατότητές του: την ιδιωτικότητα.

  Η έννοια της ιδιωτικότητας στο πλαίσιο της τεχνολογίας blockchain είναι πολύπλοκη. Ακόμη και ο ιδρυτής του Ethereum, Vitalik Buterin, υποστηρίζει ότι το απόρρητο είναι μια από τις μεγαλύτερες προκλήσεις για το δίκτυο. Το απόρρητο στο Ethereum είναι ένα πολύπλευρο ζήτημα που περιλαμβάνει πολλές αρχές, όχι απλώς να κρατά κρυφά τα δεδομένα χρήστη. Αυτά περιλαμβάνουν έλεγχο και συναίνεση χρήστη, ελάχιστη αποκάλυψη, διασφάλιση ασφάλειας , προστασία ταυτότητας και επικύρωση χωρίς εμπιστοσύνη. Κάθε μία από αυτές τις αρχές παρουσιάζει το δικό της σύνολο προκλήσεων στην τρέχουσα δομή του Ethereum.

  Κάθε υπολογιστής που είναι συνδεδεμένος στο Διαδίκτυο έχει μια διεύθυνση IP. Αυτή η διεύθυνση, μεταξύ άλλων, μπορεί να παρέχει πληροφορίες σχετικά με την τοποθεσία του χρήστη. Όταν οι χρήστες ασχολούνται με το δίκτυο Ethereum, το σύστημα θα μπορούσε να αποκαλύψει τη διεύθυνση IP τους. Αυτό περιπλέκει περαιτέρω τις προκλήσεις απορρήτου του Ethereum. Η έκθεση των διευθύνσεων IP δεν είναι απλώς μια θεωρητική ανησυχία, αλλά ένα πραγματικό ζήτημα που πρέπει να αντιμετωπίσουν οι χρήστες του Ethereum. Η ανοιχτή φύση του blockchain Ethereum σημαίνει ότι οποιοσδήποτε διαθέτει την τεχνογνωσία μπορεί ενδεχομένως να παρακολουθεί τις συναλλαγές ενός χρήστη και να τους συνδέσει με τη διεύθυνση IP του. Αυτό αντιπροσωπεύει σοβαρό κίνδυνο απορρήτου, καθώς θα μπορούσε να επιτρέψει σε κακόβουλους παράγοντες να στοχεύουν χρήστες.

  Αν και οι διευθύνσεις Ethereum είναι ψευδώνυμες, δεν είναι εντελώς ανώνυμες. Ένας αποφασισμένος παρατηρητής θα μπορούσε, θεωρητικά, να συνδέσει τις συναλλαγές με συγκεκριμένες διευθύνσεις και ενδεχομένως να εντοπίσει τους χρήστες πίσω από αυτές. Η μονιμότητα των συναλλαγών στο δίκτυο Ethereum επιδεινώνει αυτό το ζήτημα, καθώς το δίκτυο καταγράφει κάθε συναλλαγή στο blockchain επ΄ αόριστον. Εάν ένα άτομο είναι

συνδεδεμένο με μια διεύθυνση, καθίσταται δυνατός ο εντοπισμός όλων των συναλλαγών από αυτήν τη διεύθυνση πίσω σε αυτόν.

Τα έξυπνα συμβόλαια, ένα από τα καθοριστικά χαρακτηριστικά του Ethereum, παίζουν επίσης ρόλο σε αυτό το περίπλοκο δίλημμα προστασίας της ιδιωτικής ζωής. Από τη φύση τους, τα έξυπνα συμβόλαια είναι διαφανή και αμετάβλητα. Μόλις αναπτυχθεί στο δίκτυο Ethereum, ένα έξυπνο συμβόλαιο αποκαλύπτει τους όρους και τις προϋποθέσεις του σε όλους. Αυτή η έλλειψη απορρήτου μπορεί να είναι προβληματική σε περιπτώσεις όπου το έξυπνο συμβόλαιο περιλαμβάνει ευαίσθητες πληροφορίες. Επιπλέον, τα έξυπνα συμβόλαια παραμένουν αμετάβλητα μόλις αναπτυχθούν και δεν μπορούν να υποστούν τροποποιήσεις. Αυτό θα μπορούσε δυνητικά να οδηγήσει σε μια κατάσταση όπου ένα συμβόλαιο που συνδέεται με ένα άτομο συνεχίζει να διακυβεύει το απόρρητό του, ακόμη και πολύ καιρό αφού έχει σταματήσει να το χρησιμοποιεί.

Δεδομένων αυτών των ανησυχιών για το απόρρητο, γίνονται προσπάθειες για να γίνει το Ethereum πιο ισχυρό προς το απόρρητο. Ωστόσο, η βελτίωση του απορρήτου στο Ethereum δεν είναι εύκολη υπόθεση. Είναι ένα περίπλοκο εγχείρημα που απαιτεί εξισορρόπηση της ανάγκης για διαφάνεια, που είναι ζωτικής σημασίας για την εμπιστοσύνη και την ασφάλεια, με την ανάγκη για ιδιωτικότητα. Συγκεκριμένα, το Ethereum 2.0 έχει τη δυνατότητα βελτίωσης του απορρήτου. Η αναβάθμιση θα εισαγάγει μια μέθοδο κατάτμησης του δικτύου Ethereum σε μικρότερα κομμάτια ή shards. Κάθε θραύσμα θα μπορεί να επεξεργάζεται τις δικές του συναλλαγές και έξυπνα συμβόλαια, αυξάνοντας το απόρρητο αυτών των συναλλαγών. Βέβαια, δεν είναι σαφές πως θα αλληλεπιδράσει με άλλες τεχνολογίες που ενισχύουν το απόρρητο και αν θα είναι αρκετό για την αντιμετώπιση όλων των ανησυχιών του Ethereum σχετικά με το απόρρητο.

Η διαφορική ιδιωτικότητα (differential privacy) στο blockchain αναφέρεται σε μια τεχνική που χρησιμοποιείται για να προστατεύσει την ιδιωτικότητα των δεδομένων που αποθηκεύονται στο blockchain. Η ιδέα είναι να επιτραπεί η ανάλυση των δεδομένων για στατιστικούς σκοπούς χωρίς να αποκαλύπτονται ακριβείς πληροφορίες για συγκεκριμένα άτομα.

Οι τεχνικές differential privacy επιτρέπουν την εκτέλεση στατιστικών ερωτημάτων στο blockchain χωρίς να αποκαλύπτουν ευαίσθητες πληροφορίες. Αυτό επιτυγχάνεται με την εισαγωγή noise ή distortion στα δεδομένα, καθιστώντας δυσκολότερο για κακόβουλους χρήστες να αναγνωρίσουν τις πραγματικές τιμές. Συγκεκριμένα, προστίθεται τυχαίος θόρυβος (noise) στα δεδομένα πριν από τη δημοσίευσή τους και καθιστά δυσκολότερο για τους επιτιθέμενους να εξάγουν ακριβείς πληροφορίες από τα δεδομένα ή τα δεδομένα παραμορφώνονται χωρίς να επηρεάζεται η χρησιμότητα των δεδομένων αλλά καθιστώντας δυσκολότερο τον αντίστοιχο εντοπισμό προσωπικών πληροφοριών.

Η differential privacy μπορεί να εφαρμοστεί σε διάφορες πτυχές του blockchain, συμπεριλαμβανομένης της εκτέλεσης ερωτημάτων στατιστικών, της πρόσβασης σε ιδιωτικές βάσεις δεδομένων και της προστασίας της ιδιωτικότητας των χρηστών. Ο στόχος είναι να διατηρηθεί η χρησιμότητα των δεδομένων για στατιστικούς σκοπούς ενώ ταυτόχρονα προστατεύεται η ιδιωτικότητα των συμμετεχόντων.

3 Έξυπνα Συμβόλαια (Smart Contracts)

3.1 Τι είναι το Έξυπνο Συμβόλαιο

Τα έξυπνα συμβόλαια προτάθηκαν για πρώτη φορά το 1994 από τον Nick Szabo, έναν Αμερικανό επιστήμονα υπολογιστών ο οποίος εφηύρε και ένα εικονικό νόμισμα που ονομάζεται «Bit Gold» το 1998, 10 χρόνια πριν από την εισαγωγή του Bitcoin. Στην πραγματικότητα, ο Szabo φημολογείται ότι είναι ο πραγματικός Satoshi Nakamoto, ο ανώνυμος εφευρέτης του Bitcoin, κάτι που ο ίδιος έχει αρνηθεί.

Ο Szabo όρισε τα έξυπνα συμβόλαια ως ηλεκτρονικά πρωτόκολλα συναλλαγών που εκτελούν τους όρους μιας σύμβασης. Ήθελε να επεκτείνει τη λειτουργικότητα των μεθόδων ηλεκτρονικών συναλλαγών, όπως το POS (σημείο πώλησης) στην ψηφιακή σφαίρα.

Έτσι μια σημαντική επέκταση στην λειτουργικότητα που παρέχει ένα δίκτυο Blockchain, έρχεται με τα έξυπνα συμβόλαια. Ένα έξυπνο συμβόλαιο είναι ουσιαστικά ένα πρόγραμμα που είναι αποθηκευμένο σε ένα δίκτυο Blockchain και τρέχει όταν συντρέξουν κάποιες προκαθορισμένες συνθήκες. Χρησιμοποιούνται για την εκτέλεση συγκεκριμένων συναλλαγών και την διεκπεραίωση συμφωνιών χωρίς την ανάγκη ύπαρξης κάποιας κεντρικής αρχής. Ουσιαστικά εξασφαλίζουν στα συνεργαζόμενα μέρη ότι μπορούν να επικοινωνούν σύμφωνα με τους αρχικά συμφωνημένους όρους, που έχουν αποτυπωθεί σε κώδικα και κανείς δεν έχει την εξουσία να τους αλλάξει αφού το συμβόλαιο είναι αποθηκευμένο και εκτελείται μέσα στο Blockchain.

Το αμετάβλητο και διαφανές ledger του Blockchain διασφαλίζει ότι όλες οι πληροφορίες για τον υπολογισμό των δικαιωμάτων, οι κινήσεις των κεφαλαίων και οι πληρωμές καταγράφονται με τρόπο που δεν παραβιάζεται και είναι διαθέσιμες σε όλους. Αυτή η διαφάνεια αλλάζει τα μέχρι τώρα δεδομένα, καθώς δίνει τη δυνατότητα στους δημιουργούς να παρακολουθούν εύκολα και επακριβώς όλη τη διαδικασία.

Η λογική με την οποία θα υπολογίζονται και θα γίνονται οι πληρωμές θα είναι συμφωνημένη από πριν και προγραμματισμένη στο έξυπνο συμβόλαιο. Εφόσον το έξυπνο συμβόλαιο είναι αυτοεκτελούμενος κώδικας στο Blockchain, εισάγει πλέον την αυτοματοποίηση στη διανομή δικαιωμάτων και δεν χρειάζονται πλέον οι μεσάζοντες που εισήγαγαν και το θέμα της εμπιστοσύνης.

Η εξάλειψη των χειροκίνητων διεργασιών και όλων των μεσαζόντων μειώνει τον κίνδυνο σφαλμάτων, μειώνει το κόστος και ενισχύει την αποτελεσματικότητα. Τα χρήματα δεν είναι ανάγκη να περνούν μέσα από τράπεζες και άλλους οργανισμούς, αλλά βρίσκονται σε πορτοφόλια πάνω στο Blockchain. Οι πληρωμές εκτελούνται άμεσα και αυτόματα από το συμβόλαιο, ελαχιστοποιώντας τις καθυστερήσεις και τις χρεώσεις, με αποτέλεσμα οι δημιουργοί να έχουν γρήγορη πρόσβαση σε μεγαλύτερο μέρος των κερδών.

Η αποκεντρωμένη φύση του Blockchain επίσης, δεν δεσμεύεται από γεωγραφικά όρια. Άνθρωποι από όλες τις γωνιές του πλανήτη μπορούν να συμμετέχουν στην ψηφιακή οικονομία με ευκολία.

Τέλος, οι ισχυροί μηχανισμοί ασφάλειας του Blockchain προστατεύουν τις πληρωμές δικαιωμάτων από απειλές στον κυβερνοχώρο και μη εξουσιοδοτημένες κακόβουλες ενέργειες. Μόλις καταγραφούν στο Blockchain, οι συναλλαγές είναι ανθεκτικές στην παραποίηση και την απάτη, ενισχύοντας τη συνολική ασφάλεια του οικοσυστήματος συναλλαγών.[14]

3.2 Δημιουργία Έξυπνου Συμβολαίου

Τα έξυπνα συμβόλαια και τα παράγωγά τους είναι βασικά στοιχεία του χώρου Web3. Καθώς υπάρχουν πολλά Blockchain, η παρούσα διπλωματική θα επικεντρωθεί στη δημιουργία έξυπνων συμβολαίων στο Ethereum. Η καινοτομία του Ethereum σε σχέση με το Bitcoin, είναι πως το Ethereum αποτελεί μία πιο ευέλικτη και προσαρμόσιμη πλατφόρμα, πάνω στην οποία μπορούν να δημιουργηθούν και να λειτουργήσουν με ασφάλεια αποκεντρωμένες εφαρμογές, ενώ το Bitcoin παρέχει κυρίως την δυνατότητα (οικονομικών) συναλλαγών του κρυπτονομίσματος (Bitcoin).

Το Blockchain του Ethereum είναι μια Turing complete κατανεμημένη υπολογιστική αρχιτεκτονική, στην οποία κάθε κόμβος του δικτύου εκτελεί και καταγράφει τις ίδιες συναλλαγές, οι οποίες οργανώνονται σε block και προστίθενται στο Blockchain. Μόνο ένα block μπορεί να προστεθεί κάθε φορά και κάθε block περιέχει ως μέθοδο συναίνεσης (Proof of Work), αν και λόγω προβλημάτων που έχουν προκύψει (μεγάλη κατανάλωση ισχύος) συζητείται η μετάβαση από το Proof of Work στο Proof of Stake. Οι κόμβοι που συντηρούν το δίκτυο, δηλαδή αυτοί που δημιουργούν τα block ονομάζονται miners.

Στην ενότητα 2 του κεφαλαίου 5 της παρούσας διπλωματικής πραγματοποιείται λεπτομερής ανάλυση των σταδίων που απαιτούνται για τη δημιουργία ενός έξυπνου συμβολαίου, καθώς και των εργαλείων που χρησιμοποιήθηκαν.

3.2.1 Πώς το Ethereum αποθηκεύει και εκτελεί έξυπνα συμβόλαια

Η εκτέλεση έξυπνων συμβολαίων στο blockchain Ethereum δεν είναι δωρεάν και απαιτεί από τους χρήστες να ξοδεύουν Ether, το εγγενές νόμισμα του Ethereum, για την ανάπτυξη και εκτέλεση έξυπνων συμβολαίων. Η μονάδα εκτέλεσης κώδικα Ethereum ονομάζεται αέριο και μετριέται σε gwei.

Σημείωση: εκτός από το κρυπτονόμισμα Ether, το Ethereum διαθέτει επίσης gwei και wei. Ένα Ether αντιστοιχεί σε 10^9 gwei και 10^{18} wei.

Εικόνα 8: Σύμβολο Ethereum.

Το οικοσύστημα Ethereum διαθέτει δύο είδη δικτύων: mainnet και testnet. Το πρώτο χρησιμοποιείται για πραγματικές συναλλαγές και το δεύτερο είναι ένας προσομοιωτής για τη δοκιμή των συμβολαίων σε πραγματικό περιβάλλον.

Τα έξυπνα συμβόλαια Ethereum μπορούν να χρησιμοποιηθούν για κάθε είδους σκοπούς, όπως αποστολή και αποθήκευση χρημάτων σε μορφή Ether. Είναι λειτουργικά αδρανείς στο blockchain

έως ότου εξωτερικοί λογαριασμοί ή άλλα έξυπνα συμβόλαια καλέσουν τις λειτουργίες τους. Ο κώδικας συμβολαίου Ethereum Smart εκτελείται σε ένα περιβάλλον εκτέλεσης που ονομάζεται εικονική μηχανή Ethereum (EVM).

Το EVM αναγνωρίζει μόνο bytecode, επομένως πρέπει να μεταγλωττιστεί ένα έξυπνο συμβόλαιο πριν αναπτυχθεί στο κύριο δίκτυο. Η εκτέλεση κώδικα έξυπνων συμβολαίων που αλλάζει την κατάσταση της αλυσίδας block Ethereum απαιτεί πληρωμή του κόστους αερίου σε gwei. [11]

3.2.2 Έξυπνα συμβόλαια στο blockchain του Ethereum

Η κύρια γλώσσα προγραμματισμού που χρησιμοποιείται για την ανάπτυξη έξυπνων συμβολαίων Ethereum είναι η Solidity η οποία μοιράζεται πολλά στοιχεία με άλλες, πιο οικείες αντικειμενοστρεφείς γλώσσες προγραμματισμού. Η Solidity χρησιμοποιεί τα συμβάντα για να ειδοποιεί τις διεπαφές των εφαρμογών σχετικά με αλλαγές κατάστασης στο blockchain.

3.2.3 Διαφορές μεταξύ Ethereum και Ethereum 2.0

Το Ethereum είναι η πιο διαδεδομένη πλατφόρμα έξυπνων συμβολαίων. Ακριβώς αυτή η υπέρογκη χρήση της πλατφόρμας προκαλεί συχνά συμφόρηση του δικτύου, αυξάνοντας εκθετικά το κόστος συναλλαγής και τη κατανάλωση της ηλεκτρικής ενέργειας του δικτύου. Παράλληλα, ελλοχεύει ο κίνδυνος πλήρους απώλειας μιας συναλλαγής, δηλαδή να μην συμπεριληφθεί ποτέ σε block, να λήξει και να θεωρηθεί άκυρη, ενώ δαπανήθηκαν τέλη συναλλαγής, πολλές φορές μεγαλύτερα σε αριθμό από το ποσό που η ίδια μεταφέρει.

Το Ethereum 2.0 είναι η μεγαλύτερη και πολύ-αναμενόμενη αναβάθμιση του δικτύου του Ethereum που σκοπεύει να επιλύσει όλες τις αρνητικές πτυχές του. Συγκεκριμένα, στοχεύει να μεγιστοποιήσει την ταχύτητα και την απόδοση (network throughput), διατηρώντας τα υψηλά επίπεδα ασφαλείας και ελαχιστοποιώντας το ενεργειακό αντίκτυπο. Χαρακτηριστικό της αναβάθμισης είναι η ριζική αλλαγή του μηχανισμού συναίνεσης του δικτύου, μία κίνηση τολμηρή και δύσκολη, αφού ο μηχανισμός συναίνεσης είναι το σημαντικότερο χαρακτηριστικό ενός αποκεντρωμένου συστήματος. Αναλυτικότερα, ο αλγόριθμος συναίνεσης Proof-of Work (PoW) θα αντικατασταθεί από τον αλγόριθμο Proof-of-Stake (PoS), ο οποίος είναι σημαντικά ταχύτερος, πιο οικονομικός και δίχως (θεωρητικά τουλάχιστον) να θυσιάζεται η ασφάλεια του δικτύου.

Ο αλγόριθμος συναίνεσης PoS δεν συναντάται μόνο στην αναβάθμιση του δικτύου του Ethereum αλλά και σε πολλά κρυπτονομίσματα τρίτης γενιάς, καθώς τον προτιμούν από τον PoW αλγόριθμο. Με τον αλγόριθμο αυτόν αντικαθίστανται ουσιαστικά οι miners, οι οποίοι δαπανούσαν υπολογιστική ισχύ προκειμένου να λύσουν πρώτοι το μαθηματικό πρόβλημα, με τους λεγόμενους επικυρωτές (validators), οι οποίοι κληρώνονται τυχαία να επιβεβαιώσουν τις συναλλαγές ενός block και να λάβουν την ανταμοιβή που αντιστοιχεί σε Ether.

Το Ethereum 2.0 έχει σίγουρα εισαγάγει τον κόσμο της κρυπτογράφησης με καλύτερες δυνατότητες, αλλά το κύριο πλεονέκτημα που έχει προσφέρει το Ethereum 2.0 είναι η επεκτασιμότητα. Το Ethereum 2.0 χρησιμοποιεί το διαμοιρασμό για να αυξήσει τον αριθμό των συναλλαγών που πραγματοποιούνται στο δίκτυο και να επαληθεύσει και να επικυρώσει

περισσότερες από 10.000 συναλλαγές σε ένα δευτερόλεπτο. Αυτή είναι η πιο σημαντική ιδιότητα που κάνει το Ethereum 2.0 πιο ισχυρό από το Ethereum.

Ο διαμοιρασμός είναι μια έννοια που προέρχεται από συστήματα διαχείρισης βάσεων δεδομένων στη δεκαετία του 1980. Στην πραγματικότητα, το SHARD ήταν μια συντομογραφία ενός προϊόντος βάσης δεδομένων της δεκαετίας του ΄80, System for Highly Available Replicated Data.

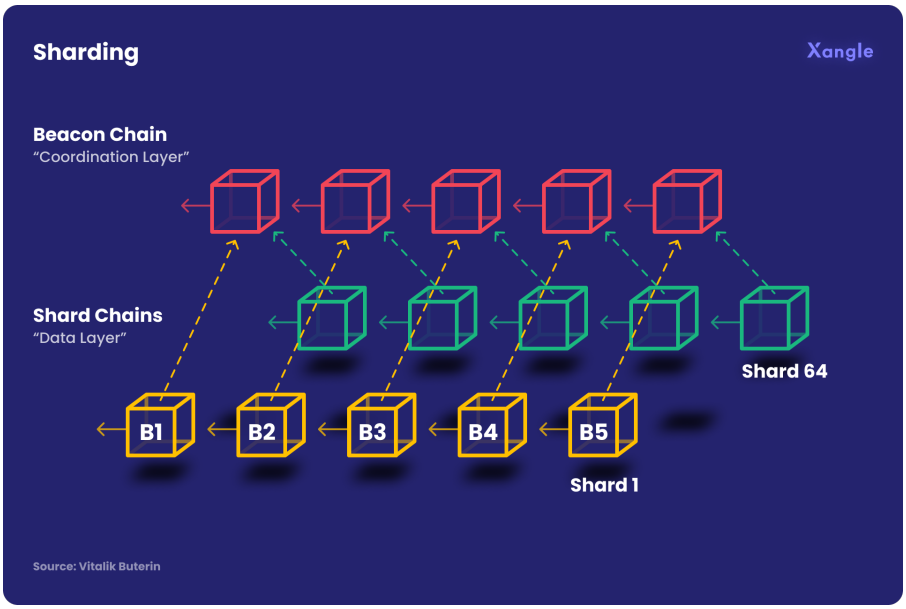
Συμπτωματικά, shard σημαίνει επίσης «ένα μικρό μέρος από κάτι μεγαλύτερο». Και αυτό ακριβώς στοχεύει ο διαμοιρασμός στην τεχνολογία Blockchain – να χωρίσει ένα δίκτυο Blockchain σε μικρότερα, διαχειρίσιμα κομμάτια που ονομάζονται θραύσματα. Κάθε θραύσμα έχει το δικό του μοναδικό υποσύνολο δεδομένων συναλλαγών και επεξεργάζεται συναλλαγές ταυτόχρονα στο δίκτυο.

Αυτή η διάσπαση ενός δικτύου Blockchain σε πολλαπλά θραύσματα επιτρέπει την παράλληλη επεξεργασία συναλλαγών, βελτιωμένη καθυστέρηση και αυξημένη επεκτασιμότητα. Η υπολογιστική επιβάρυνση στο δίκτυο μειώνεται και περισσότερες συναλλαγές μπορούν να διεκπεραιωθούν σε μια δεδομένη χρονική περίοδο. Στην περίπτωση του Ethereum, ο διαμοιρασμός θα βοηθήσει επίσης στην αντιμετώπιση των υψηλών τελών αερίου στο δίκτυο.

Απαραίτητη προϋπόθεση για την κατανόηση του διαμοιρασμού είναι η γνώση του πώς λειτουργούν οι κόμβοι σε ένα δίκτυο blockchain. Οι κόμβοι αναφέρονται στους υπολογιστές, σε ένα δίκτυο blockchain που αποθηκεύουν και μεταδίδουν δεδομένα συναλλαγών, διατηρώντας ουσιαστικά το δίκτυο σε λειτουργία.

Στον τρέχοντα μηχανισμό συναίνεσης PoW του Ethereum, όλοι οι κόμβοι επεξεργάζονται κάθε συναλλαγή στο δίκτυο. Αυτό μπορεί να οδηγήσει σε προβλήματα επεκτασιμότητας καθώς όλο και περισσότερες συναλλαγές προστίθενται στο δίκτυο.

Με τον διαμοιρασμό, οι κόμβοι στο δίκτυο χωρίζονται σε ομάδες που ονομάζονται αλυσίδες θραυσμάτων. Κάθε αλυσίδα θραυσμάτων είναι υπεύθυνη για την επεξεργασία ενός υποσυνόλου συναλλαγών στο δίκτυο. Αυτές οι αλυσίδες θραυσμάτων επικοινωνούν μεταξύ τους για να επιτευχθεί συναίνεση και να επικυρώσουν block δεδομένων συναλλαγών.



Εικόνα 9: Μοντέλο διαμοιρασμού Ethereum.

Επεξήγηση Σχήματος (Εικ.9): Η τεχνική Sharding χωρίζει το L1 blockchain σε αλυσίδες ή shards. Οι κόμβοι ομαδοποιούνται, και κάθε ομάδα αναλαμβάνει ένα shard. Κάθε επικυρωτής αποθηκεύει και διαχειρίζεται μόνο ένα shard αντί ολόκληρου του blockchain, μειώνοντας το έργο του.

Στο πλαίσιο του Ethereum, ωστόσο, θα υπάρχουν τεχνικά θραύσματα «blobs» αντί για αλυσίδες θραυσμάτων, λόγω της χρήσης του dankharding, μιας νεότερης προσέγγισης στο Sharding. Το κοινόχρηστο σύστημα του Ethereum θα αποτελείται από 64 συνδεδεμένες βάσεις δεδομένων και οι συναλλαγές θα υποβάλλονται σε επεξεργασία κάθε θραύσματος. Κάθε θραύσμα θα έχει μια «επιτροπή» που θα έχει 128 επικυρωτές. Αυτές οι επιτροπές θα είναι υπεύθυνες για την πρόταση και την επικύρωση κάθε block κάθε 12 δευτερόλεπτα.

Το Ethereum 2.0 έχει αναπτυχθεί για να παρέχει περισσότερη ασφάλεια σε συναλλαγές που δεν ήταν δυνατές με τη μέθοδο PoW. [13]

3.3 Τομείς Εφαρμογής Έξυπνων Συμβολαίων

Παραδείγματα εφαρμογών έξυπνων συμβολαίων περιλαμβάνουν οικονομικούς σκοπούς όπως εμπορικές συναλλαγές, επενδύσεις, και δανεισμό. Μπορούν να χρησιμοποιηθούν για εφαρμογές σε παιχνίδια, υγειονομική περίθαλψη, ακίνητα και μπορούν ακόμη και να χρησιμοποιηθούν για τη διαμόρφωση ολόκληρων εταιρικών δομών. Μερικά από τα πραγματικά παραδείγματα έξυπνων συμβολαίων είναι:

- **Στα Οικονομικά**
  Οι dApps αποκεντρωμένης χρηματοδότησης (DeFi) αντιπροσωπεύουν μια τρομερή εναλλακτική λύση στις παραδοσιακές χρηματοπιστωτικές υπηρεσίες και αυξάνονται σε δημοτικότητα χάρη στα αξιόπιστα, αμετάβλητα και διαφανή χαρακτηριστικά της τεχνολογίας Blockchain και έξυπνων συμβολαίων. Τα DeFi dApps παρέχουν παράλληλες υπηρεσίες στον κλάδο των τραπεζικών και χρηματοοικονομικών υπηρεσιών —όπως δανεισμός, διαπραγμάτευση και πλήθος άλλων χρηματοοικονομικών υπηρεσιών— μαζί με εντελώς νέους τύπους προϊόντων και αποκεντρωμένα επιχειρηματικά μοντέλα που μπορούν να προσφέρουν σημαντικό όφελος και χρησιμότητα στους χρήστες. Με την αυξημένη διαφάνεια που παρέχεται από τα έξυπνα συμβόλαια (μαζί με τη λειτουργικότητα 24/7 και το μειωμένο κόστος), οι dApps έχουν τη δυνατότητα να μειώσουν τα εμπόδια εισόδου στην αρένα των χρηματοοικονομικών υπηρεσιών για ανθρώπους σε όλο τον κόσμο.

- **Στο Gaming**
  Η παγκόσμια βιομηχανία τυχερών παιχνιδιών είναι ένα οικοσύστημα εκατοντάδων δισεκατομμυρίων δολαρίων που συνεχίζει να αναπτύσσεται γρήγορα, αλλά ο τρόπος με τον οποίο δημιουργείται και διανέμεται η αξία σε ολόκληρο τον κλάδο μπορεί να είναι άδικος. Οι προγραμματιστές δημιουργούν και κυκλοφορούν παιχνίδια και οι παίκτες πληρώνουν για να παίξουν και να αλληλεπιδράσουν με αυτά τα παιχνίδια. Αυτό διαιωνίζει μια μονόδρομη ροή αξίας, όπου οι παίκτες ξοδεύουν χρήματα για να ξεκλειδώσουν την πρόσβαση σε στοιχεία και διαμορφώσεις παιχνιδιού εντός του παιχνιδιού. Αντίθετα, η τεχνολογία Blockchain στο gaming μπορεί να επιτρέψει στους παίκτες να αποτυπώσουν τη χρησιμότητα και την αξία των αγορών εντός του παιχνιδιού και των αποκτήσεων περιουσιακών στοιχείων πιο αποτελεσματικά.

- **Στον Νομικό Κλάδο**
  Ίσως μια από τις πιο πολλά υποσχόμενες περιπτώσεις χρήσης έξυπνων συμβολαίων στον πραγματικό κόσμο είναι η δυνατότητά τους να λειτουργούν ως νομικά δεσμευτικές συμβάσεις. Τα έξυπνα συμβόλαια ενδέχεται σύντομα να αποτελέσουν επιλογή για την εκτέλεση νομικών συμφωνιών, μειώνοντας πιθανώς το κόστος που προκύπτει από τη χρήση δικηγόρων και άλλων διαμεσολαβητών. Ορισμένες πολιτείες των ΗΠΑ έχουν αρχίσει να επιτρέπουν τη χρήση έξυπνων συμβολαίων και blockchain στη νομική βιομηχανία σε ορισμένα πλαίσια. Για παράδειγμα, η Αριζόνα επιτρέπει τη δημιουργία εκτελεστών νομικών συμφωνιών μέσω έξυπνων συμβολαίων και η Καλιφόρνια επιτρέπει την έκδοση αδειών γάμου μέσω τεχνολογίας blockchain.

- **Στο Real Estate**
  Μέσω του tokenization, τα έξυπνα συμβόλαια προάγουν την κλασματική ιδιοκτησία περιουσιακών στοιχείων και έτσι μειώνουν το εμπόδιο εισόδου για επενδύσεις για πολλούς με τη συγχώνευση συναλλαγών blockchain και ακινήτων. Η κλασματική ιδιοκτησία κατοικίας είναι ένα μοντέλο ακινήτων όπου πολλά άτομα ή οντότητες κατέχουν συλλογικά και μοιράζονται δικαιώματα ιδιοκτησίας σε ένα μόνο ακίνητο. Οποιοσδήποτε έχει αγοράσει ένα σπίτι ή άλλο ακίνητο πιθανότατα γνωρίζει την πιθανότητα κρυφών δαπανών που σχετίζονται με προμήθειες κλεισίματος, μεταφορές τίτλων και αμοιβές μεσίτη. Πρόκειται για κόστη που ενδέχεται να μειωθούν ή και να εξαλειφθούν με την αυτόματη εκτέλεση

έξυπνων συμβολαίων που λειτουργούν χωρίς μεσάζοντες. Ουσιαστικά, μεγάλο μέρος της απαιτούμενης τήρησης αρχείων μπορεί να πραγματοποιηθεί μέσω σχετικών έξυπνων συμβολαίων, τα οποία μπορούν να εξοικονομήσουν χρόνο και χρήμα στα συνεργαζόμενα μέλη. Με τη χρήση έξυπνων συμβολαίων και Blockchain στην ακίνητη περιουσία, η ανάγκη για νομικούς συμβούλους ή άλλες συμβουλευτικές υπηρεσίες γίνεται λιγότερο κρίσιμη, μειώνοντας πιθανώς το κόστος σε όλο το φάσμα.

- **Σε Εταιρικές Δομές: Κατασκευή DAO**
  Το 2017, το Ντέλαγουερ πέρασε το νομοσχέδιο 69 της Γερουσίας, το οποίο επιτρέπει στις επιχειρήσεις να ενσωματώσουν και να χρησιμοποιούν τεχνολογία Blockchain. Αυτό το νομοσχέδιο άνοιξε την πόρτα στη διάδοση των αποκεντρωμένων αυτόνομων οργανισμών (DAO), οι οποίοι λειτουργούν ως εταιρείες όπου η ιδιοκτησία και η αποζημίωση μπορούν να ενσωματωθούν σε έξυπνα συμβόλαια. Οι DAO χρησιμοποιώντας έξυπνα συμβόλαια για την κωδικοποίηση εταιρικών δομών, μπορούν να ενεργοποιήσουν αυτόματες λειτουργίες μέσα σε ένα εταιρικό πλαίσιο. Οι DAO μπορούν επίσης να εξοικονομήσουν διοικητικά έξοδα, συμπεριλαμβανομένων των χώρων γραφείου, των προσλήψεων και της μισθοδοσίας μέσω λειτουργιών που ενδέχεται να μην περιλαμβάνουν επίσημες συμβάσεις εργασίας.

- **Στην Υγειονομική Περίθαλψη**
  Η ανταλλαγή δεδομένων μεταξύ ιδρυμάτων είναι ζωτικής σημασίας για αποτελεσματικές κλινικές δοκιμές. Με την υποστήριξη έξυπνων συμβολαίων, οι επαγγελματίες μπορούν να μοιράζονται απρόσκοπτα δεδομένα σε ολόκληρο τον κλάδο. Η τεχνολογία Blockchain μπορεί επίσης να βοηθήσει στον έλεγχο ταυτότητας των δεδομένων για να διασφαλιστεί ότι είναι ακριβή.

- **Στην Μουσική Βιομηχανία**
  Οι εφαρμογές έξυπνων συμβολαίων μπορούν να διευκολύνουν τις πληρωμές των δημιουργών. Για παράδειγμα, αυτά τα συμβόλαια μπορούν να περιλαμβάνουν το ποσοστό των εσόδων από δικαιώματα που πηγαίνει στη δισκογραφική και στον καλλιτέχνη. Αυτές οι πληρωμές μπορούν να πραγματοποιηθούν άμεσα, κάτι που αποτελεί σημαντική νίκη για όλα τα εμπλεκόμενα μέρη.

- **Σε Ψηφοφορία στις εκλογές**
  Τα έξυπνα συμβόλαια θα μπορούσαν να δημιουργήσουν ένα ασφαλές περιβάλλον για ψηφοφορίες, μειώνοντας τον κίνδυνο πιθανής χειραγώγησης των ψηφοφόρων. Κάθε ψήφος που χρησιμοποιεί ένα έξυπνο συμβόλαιο προστατεύεται από το ledger του blockchain. Λόγω της κρυπτογράφησης, είναι απίστευτα δύσκολο να αποκωδικοποιηθούν. Τα έξυπνα συμβόλαια θα μπορούσαν επίσης να αυξήσουν τη συμμετοχή των ψηφοφόρων. Με ένα διαδικτυακό σύστημα που τροφοδοτείται από έξυπνα συμβόλαια, δεν χρειάζεται να μετακινηθεί κάποιος σε εκλογικό κέντρο.

- **Στον Ασφαλιστικό Κλάδο**

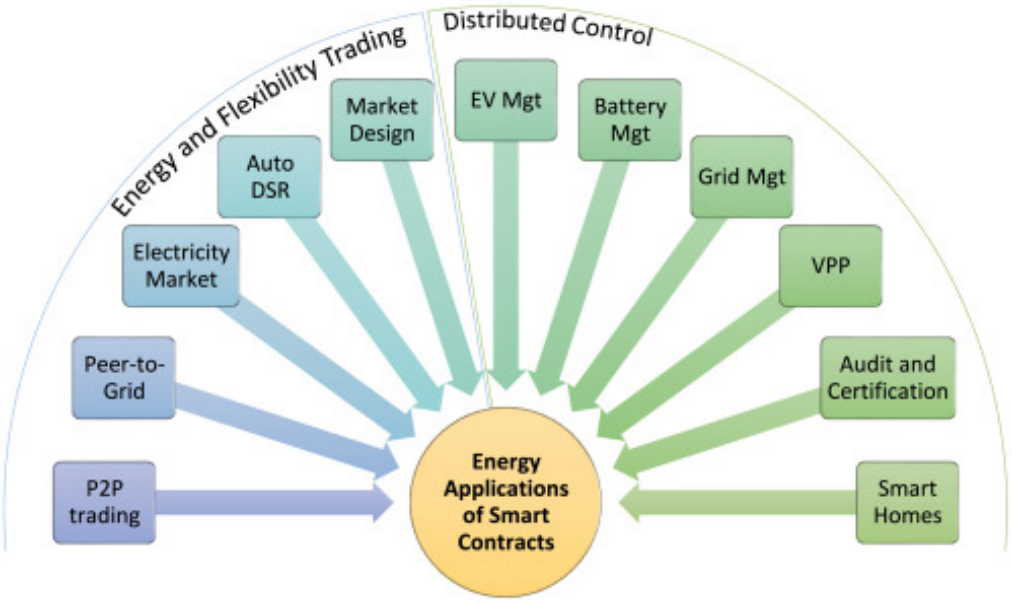
Τα έξυπνα συμβόλαια βοηθούν στη μείωση του κόστους των ασφαλιστών και να οδηγούν σε χαμηλότερα ασφάλιστρα. Με τις αυτοματοποιημένες διαδικασίες πληρωμής αξιώσεων που υποστηρίζονται από την τεχνολογία έξυπνων συμβολαίων, οι αντισυμβαλλόμενοι μπορούν να πληρωθούν πιο γρήγορα από ό,τι μέσω των τρεχουσών μη αυτόματων διαδικασιών.

- **Στη Διανομή Ενέργειας**
  Αξιοποιώντας την τεχνολογία Blockchain, ο ενεργειακός τομέας μπορεί να στοχεύσει στην αποκέντρωση, απομακρύνοντας τον παραδοσιακό κεντρικό έλεγχο. Αυτό επιτρέπει μεγαλύτερη αυτονομία και δίνει τη δυνατότητα σε διάφορους ενδιαφερόμενους φορείς —συμπεριλαμβανομένων των καταναλωτών, των παραγωγών και των διαχειριστών δικτύου— να συμμετέχουν ενεργά στις ενεργειακές συναλλαγές και στις διαδικασίες λήψης αποφάσεων. [15]

3.4 Έξυπνα Συμβόλαια στον Ενεργειακό Τομέα

Η παρούσα διπλωματική εργασία επικεντρώνεται στην κατανόηση, δημιουργία και εφαρμογή έξυπνων συμβολαίων στο τομέα της ενέργειας.

Το είδος των εφαρμογών των έξυπνων συμβολαίων στον ενεργειακό τομέα μπορεί να κατηγοριοποιηθεί σε δύο κύριες κατηγορίες: (α) παραγωγή ενέργειας και (β) κατανεμημένο έλεγχο. Οι διαφορετικοί τομείς ενεργειακών εφαρμογών απεικονίζονται στο παρακάτω σχήμα.



Εικόνα 10: Εφαρμογή έξυπνων συμβολαίων στον ενεργειακό τομέα. Κάθε εφαρμογή εξετάζεται σε μία από τις δύο κύριες κατηγορίες εφαρμογών που

προσδιορίζονται, οι οποίες είναι (α) η παραγωγή ενέργειας και (β) ο κατανεμημένος έλεγχος.
(Desen Kirli, Benoit Couraud, Valentin Robu, Marcelo Salgado-Bravo, Sonam Norbu, Merlinda Andoni, Ioannis Antonopoulos, Matias Negrete-Pincetic, David Flynn, Aristides Kiprakis, (April, 2022). Renewable and Sustainable Energy Reviews - Smart contracts in energy systems: A systematic review of fundamental approaches and implementations.) [16]

3.4.1 Παραγωγή ενέργειας

Καθώς τα έξυπνα συμβόλαια τρέχουν σε μια αλυσίδα block που είχε αρχικά σχεδιαστεί για την αποθήκευση χρηματοοικονομικών συναλλαγών, η πιο συχνή εφαρμογή των έξυπνων συμβολαίων αντιστοιχεί σε συναλλαγές και πληρωμές μεταξύ δύο οντοτήτων. Ως αποτέλεσμα, στην έρευνα, τα έξυπνα συμβόλαια χρησιμοποιούνται κυρίως στο πλαίσιο εφαρμογών συναλλαγών ενέργειας. Σε αυτές τις εφαρμογές, ο κύριος στόχος του έξυπνου συμβολαίου είναι να διευκολύνει την αντιστοίχιση μεταξύ καταναλωτών και προμηθευτών, αλλά και να προτείνει έναν ασφαλή και αξιόπιστο μηχανισμό πληρωμής ή διακανονισμού. Τα έξυπνα συμβόλαια έχουν χρησιμοποιηθεί για τις ακόλουθες εφαρμογές:

- **Συναλλαγές peer-to-peer (P2P)**
  Τα έξυπνα συμβόλαια χρησιμοποιούνται συχνά για εφαρμογές συναλλαγών P2P. Τα έξυπνα συμβόλαια λαμβάνουν πρώτα τις προσφορές από τα διάφορα ενδιαφερόμενα μέρη (παραγωγούς, προμηθευτές και αγοραστές) και εν συνεχεία απαιτεί την κατάθεση από τους αγοραστές. Έπειτα για την αντιστοίχιση των αγοραστών (καταναλωτών) με τους πωλητές (παραγωγούς), χρησιμοποιούνται διαφορετικές προσεγγίσεις έξυπνων συβολαίων. Αυτή η αντιστοίχιση μπορεί να πραγματοποιηθεί συγκρίνοντας την ποσότητα ενέργειας και την τιμή των εισερχόμενων προσφορών. Μόλις το έξυπνο συμβόλαιο επικυρώσει μια συναλλαγή, η οποία αποτελείται από μια τιμή, μια ποσότητα ενέργειας και έναν χρόνο παράδοσης, το έξυπνο συμβόλαιο για συναλλαγές P2P μπορεί στη συνέχεια να χρησιμοποιηθεί για την ανάλυση της παρακολούθησης της πραγματικής κατανάλωσης και παραγωγής που προέρχεται από την υποδομή έξυπνης μέτρησης. Αυτή η ανάλυση μπορεί στη συνέχεια να ενεργοποιήσει αυτόματα τον διακανονισμό εντός του έξυπνου συμβολαίου, προκειμένου να κατανεμηθούν οι ανταμοιβές και οι ποινές σύμφωνα με τον όρο του συμβολαίου.

- **Λιανική αγορά**
  Τα έξυπνα συμβόλαια μπορούν επίσης να χρησιμοποιηθούν για εφαρμογές λιανικής αγοράς, για να επιτρέψουν στους καταναλωτές να επιλέξουν προμηθευτή, να υπογράψουν σύμβαση με τον προμηθευτή, αλλά και να αποθηκεύσουν με ασφάλεια χρονοσειρές από την υποδομή παρακολούθησης ενέργειας και να παρέχουν σχετικές υπηρεσίες τιμολόγησης. Τα έξυπνα συμβόλαια μπορούν να χρησιμοποιηθούν από κοινού με έξυπνους μετρητές για τη μέτρηση σε πραγματικό χρόνο της ποσότητας ενέργειας που παράγεται ή καταναλώνεται και να προσαρμόζουν αυτόματα τη ζήτηση και την προσφορά. Τα έξυπνα συμβόλαια μπορούν επίσης να βοηθήσουν στην υλοποίηση αυτοματοποιημένων δραστηριοτήτων, όπως ο καθορισμός του κόστους ηλεκτρικής ενέργειας για μια περίοδο, οι πολιτικές πληρωμής, οι

χρόνοι αγοράς και πώλησης ηλεκτρικής ενέργειας. Πράγματι, αξιοποιώντας τα χαρακτηριστικά των έξυπνων συμβολαίων, αυξάνεται η ταχύτητα, η αξιοπιστία, η επεκτασιμότητα και η ασφάλεια της αγοράς ενέργειας.

- **Ευελιξία στην πλευρά της ζήτησης στην αγορά ενέργειας**
  Στις τρέχουσες ρυθμίσεις της αγοράς, τα ενδιαφερόμενα μέλη μπορούν να συνάψουν συμβάσεις βοηθητικών υπηρεσιών για την επίτευξη ισορροπίας μεταξύ προσφοράς και ζήτησης ενέργειας. Για μείωση ή αύξηση της ζήτησης, απαιτείται από τους εγγεγραμμένους τελικούς χρήστες να πληρούν ένα δεδομένο προφίλ φορτίου. Επιπλέον, η κατάλληλη τιμολόγηση και πληρωμή μπορούν να δημιουργηθούν αυτόματα από ένα έξυπνο συμβόλαιο προκειμένου να επιβραβεύονται ή να τιμωρούνται οι καταναλωτές που πληρούν το στοχευμένο προφίλ φορτίου ή όχι αντίστοιχα.

- **Σχεδιασμός αγοράς**
  Τα έξυπνα συμβόλαια μπορούν να χρησιμοποιηθούν για να καθοριστούν οι τιμές των συναλλαγών ενέργειας. Σε αντίθεση με την κατηγορία peer-to-peer που αντιστοιχεί σε πλήρεις συναλλαγές peer-to-peer, στις οποίες ένας αγοραστής αγοράζει ενέργεια από έναν συγκεκριμένο πωλητή, σε αυτήν την κατηγορία, η εφαρμογή αντιστοιχεί σε υβριδικά peer-to-peer. Ουσιαστικά, το έξυπνο συμβόλαιο λαμβάνει την έγκυρη ζήτηση των καταναλωτών και καθορίζει την υψηλότερη προσφορά του καταναλωτή ως τη νικητήρια προσφορά. Το έξυπνο συμβόλαιο επαναλαμβάνεται έως ότου ικανοποιηθεί όλη η ζήτηση ή μέχρι να μην μείνει καθόλου ενέργεια.

3.4.2 Κατανεμημένος έλεγχος

- **Διαχείριση ηλεκτρικών οχημάτων (Electric Vehicle (EV))**
  Στον τομέα των συστημάτων φόρτισης ηλεκτρικών οχημάτων (EV), τα έξυπνα συμβόλαια μπορούν να χρησιμοποιηθούν για διαφορετικούς σκοπούς. Τα έξυπνα συμβόλαια μπορούν να εφαρμόσουν αλγόριθμους βελτιστοποίησης με μικροτέρη πολυκλότητα, όπως για παράδειγμα βέλτιστος τρόπος εξισορρόπησης της κατανομής των χρηστών EV μεταξύ των χώρων στάθμευσης, επιτυγχάνοντας παράλληλα δίκαιη κατανομή τους στις θέσεις φόρτισης EV.

- **Διαχείριση μπαταρίας**
  Στην περίπτωση ελέγχου μπαταριών, ένα έξυπνο συμβόλαιο μπορεί να χρησιμοποιηθεί για την αποθήκευση των πληροφοριών των διανεμημένων μπαταριών, όπως η κατάσταση φόρτισης ή κατάστασης υγείας και η αυτόματη αποστολή συστάσεων ελέγχου σε όλες τις μπαταρίες προκειμένου να συγχρονιστεί ή να δοθεί προτεραιότητα στη φόρτιση ή την αποφόρτιση των κατανεμημένων περιπτώσεων.

- **Διαχείριση δικτύου (Smart Grid)**
  Smart Grid ή αλλιώς έξυπνο δίκτυο, είναι ένα προηγμένο ηλεκτρικό δίκτυο που περιλαμβάνει ένα μεγάλο κομμάτι ενεργειακής τεχνολογίας, όπως ανανεώσιμες πηγές ενέργειας, έξυπνες συσκευές τεχνολογίας IoT και έξυπνους μετρητές. Στα πλεονεκτήματα του έξυπνου δικτύου ανήκουν η αυτόματη επαναφορά μετά από τεχνικές διαταραχές, η μειωμένη ζήτηση αιχμής, το μειωμένο λειτουργικό κόστος άρα και μειωμένο τελικό κόστος ως προς τους καταναλωτές, καθώς και τη γενικότερη αυξημένη αντοχή σε βλάβες. Τέλος, το έξυπνο δίκτυο είναι πιο ασφαλές όσον αφορά επιθέσεις και χάρη στους έξυπνους μετρητές του έχει διαρκώς τη συνεχή εποπτεία της ενεργειακής κατανάλωσης, βάσει IT (Information Technology) διαδικασιών.

- **Εικονικοί σταθμοί ηλεκτροπαραγωγής (Virtual Power Plant (VPP))**
  Η έννοια των εικονικών σταθμών παραγωγής ενέργειας (VPP) περιλαμβάνει τον χειριστή που παρακολουθεί την παραγωγή ή την κατανάλωση διαφορετικών στοιχείων προκειμένου να συντονίσει καλύτερα και να βελτιστοποιήσει τη συνολική παραγωγή.

- **Έλεγχος και πιστοποίηση εφοδιαστικής αλυσίδας**
  Τα έξυπνα συμβόλαια μπορούν επίσης να χρησιμοποιηθούν για τη δημιουργία μιας διαφανούς αλυσίδας εφοδιασμού. Μειώνουν το χρόνο και το κόστος και εξαλείφουν την ανάγκη για εξωτερικό έλεγχο, επιτρέποντας ταυτόχρονα στους παραγωγούς ενέργειας να αποκομίσουν άμεσα χρήματα από τις πιστώσεις.

- **Internet of Things (IoT)**
  Μια άλλη προτεινόμενη εφαρμογή για έξυπνα συμβόλαια στην ενέργεια είναι οι εφαρμογές IoT. Οι έννοιες του IoT χρησιμοποιούνται ευρέως στον ενεργειακό τομέα για την παρακολούθηση και τον έλεγχο έξυπνων πόλεων και απομακρυσμένων στοιχείων. Ωστόσο εγκυμονούν κινδύνους όσον αφορά τον έλεγχο και την ασφάλεια των δεδομένων που συλλέγονται από συσκευές IoT, ιδίως όταν αυτά διαχειρίζονται κεντρικά από ένα ενιαίο σύστημα. Σε ένα πλαίσιο IoT, το απόρρητο αποτελεί βασικό μέλημα για τα έξυπνα συμβόλαια, καθώς τα δεδομένα μπορούν να μεταφερθούν και να μοιραστούν μεταξύ διαφορετικών μερών για παρακολούθηση, υποβολή προσφορών ή άλλους σκοπούς. Αυτά τα δεδομένα μπορεί να περιλαμβάνουν τη γεωγραφική θέση ενός αγοραστή ή άλλες προσωπικές πληροφορίες που θα πρέπει να προστατεύονται.

- **Έξυπνα σπίτια και συστήματα διαχείρισης ενέργειας (Home Energy Management System (HEMS))**
  Έξυπνα συμβόλαια έχουν επίσης χρησιμοποιηθεί για συστήματα διαχείρισης ενέργειας στο σπίτι (HEMS) προκειμένου, για παράδειγμα, να συντονίζεται ο προγραμματισμός θέρμανσης και ψύξης σπιτιού. Επιπλέον, η ασφαλής φύση των έξυπνων συμβολαίων παίζει σημαντικό ρόλο στον συντονισμό των οικιακών συσκευών, έτσι ώστε να ελαχιστοποιηθούν οι λογαριασμοί ή να μειωθεί το αποτύπωμα άνθρακα του χρήστη. Η εφαρμογή της τεχνολογίας αυτής μπορεί να συμβάλει στη βελτίωση της βιωσιμότητας (sustainability). Αυτό συμβαίνει καθώς οι έξυπνες λύσεις μπορούν να βοηθήσουν στην αποτελεσματική χρήση ενέργειας και των πόρων, να μειώσουν τις εκπομπές αερίων του θερμοκηπίου και να

συμβάλουν στη μείωση του οικολογικού αποτυπώματος του χρήστη. Με την έξυπνη διαχείριση της ενέργειας και των συσκευών, μπορούμε να επιτύχουμε πιο βιώσιμες και φιλικές προς το περιβάλλον κοινότητες. Ταυτόχρονα, για εφαρμογές Smart Home, τα έξυπνα συμβόλαια χρησιμοποιούνται για την αυτόματη λήψη αποφάσεων ελέγχου (ενεργοποίηση ή απενεργοποίηση συσκευών) ανάλογα με την κατάσταση ορισμένων μεταβλητών, καθώς διασφαλίζουν ότι το κανάλι επικοινωνίας είναι ασφαλές.[16]

3.4.3 Υλοποιημένα έργα στον κλάδο της ενέργειας

Η δυνατότητα αυτόματης επεξεργασίας δεδομένων με αποκεντρωμένο και ασφαλή τρόπο χρησιμοποιώντας έξυπνα συμβόλαια έχει παρακινήσει τη δημιουργία μεγάλου αριθμού έργων που σχετίζονται με συστήματα ηλεκτρικής ενέργειας, όπως η αγορά ενέργειας, η αποθήκευση ενέργειας, η χρέωση ενέργειας και η ιχνηλασιμότητα του CO2. Ακολουθεί μια ενδεικτική λίστα έργων που δημιούργησαν αντίκτυπο στον κλάδο των έξυπνων συμβολαίων παρουσιάζοντας καινοτόμες εφαρμογές τους στην ευρύτερη βιομηχανία ενέργειας.

- **Energy Web Foundation (EWF)**
  Ο Energy Web Foundation (EWF) είναι ένας μη κερδοσκοπικός οργανισμός που ιδρύθηκε από το Grid Singularity και το Ινστιτούτο Rocky Mountain. Η αποστολή του EWF είναι να επιταχύνει την ενεργειακή μετάβαση σε χαμηλές εκπομπές άνθρακα με επίκεντρο τον πελάτη χρησιμοποιώντας blockchain για την ανάπτυξη αποκεντρωμένων εφαρμογών και τεχνολογιών. Το 2019 το EWF κυκλοφόρησε το Energy Web Chain (EWC), ένα δημόσιο, ανοιχτό κώδικα χρησιμοποιώντας μέθοδο συναίνεσης (PoA) και βασισμένο στην τεχνολογία blockchain Ethereum που υπόσχεται αύξηση της χωρητικότητας συναλλαγών κατά 30 φορές και μείωση της κατανάλωσης ενέργειας σε 2-3 τάξεις μεγέθους.

- **Power Ledger**
  Η Power Ledger είναι μια Αυστραλιανή εταιρεία που ιδρύθηκε το 2016 και επικεντρώθηκε στο peer-to-peer εμπόριο ενέργειας. Αναπτύσσει ένα οικοσύστημα που στοχεύει στη μείωση της κατανάλωσης ενέργειας και επιτρέπει στους συμμετέχοντες να διαχειρίζονται ένα μικροδίκτυο αγοράς ανανεώσιμων πηγών ενέργειας σε πραγματικό χρόνο.

- **LO3 Energy**
  Η LO3 Energy ιδρύθηκε το 2012 και θέλει να βελτιώσει την τοπική παραγωγή και ανταλλαγή ενέργειας στα πλαίσια μιας κοινότητας. Το Brooklyn Microgrid αναπτύχθηκε από την LO3 Energy ως μια απόδειξη της ιδέας peer-to-peer εμπορίας ενέργειας χρησιμοποιώντας την υπάρχουσα υποδομή δικτύου. Έτσι αναπτύχθηκε μια πλατφόρμα ανταλλαγής ενέργειας που ονομάζεται Exergy ως εξουσιοδοτημένη πλατφόρμα δεδομένων για συναλλαγές peer-to-peer και της πλατφόρμας Pando που μπορεί να χρησιμοποιηθεί για

τη συγκέντρωση τοπικών πόρων και τη δημιουργία μιας ενεργειακής αγοράς, βασισμένης σε πλειστηριασμούς μεταξύ επιχειρήσεων και αγοραστών. Τον Δεκέμβριο του 2019, η L03 Energy μαζί με την Green Mountain Power αναπτύσσουν μια πιλοτική ενεργειακή αγορά που ονομάζεται Vermont Green ως η πρώτη εξουσιοδοτημένη αγορά των ΗΠΑ.

- **Prosume.io**
  Το prosume.io ιδρύθηκε το 2016 και προτείνει μια πλατφόρμα που βασίζεται σε έξυπνα συμβόλαια και συσκευές IoT. Αναπτύσσει πολλαπλές εφαρμογές, όπως παραγωγή ενέργειας, έξυπνη χρέωση, εξισορρόπηση δικτύου και βελτιστοποίηση διαπραγμάτευσης ηλεκτρικής ενέργειας και φυσικού αερίου, σύμφωνα με την τοπική νομοθεσία σε κάθε χώρα.

- **IBM - Hyperledger Fabric**
  Σε συνεργασία με την IBM, το Energy Blockchain Lab δημιουργεί μια αποκεντρωμένη πλατφόρμα διαχείρισης αποτυπώματος άνθρακα στην Κίνα που αναμένεται να μειώσει μεταξύ 20%–50% τον μέσο κύκλο ανάπτυξης ενεργητικού άνθρακα 10 μηνών.

- **Share & Charge**
  Το Share & Charge είναι ένα γερμανικό ίδρυμα επικεντρωμένο στην ηλεκτροκίνηση. Το Share & Charge προωθεί το Open Charging Network (OCN) ως αποκεντρωμένη λύση για υπηρεσίες φόρτισης EV. Περιλαμβάνονται διάφορες υπηρεσίες για σταθμούς φόρτισης, όπως πράσινα πιστοποιητικά, άμεση πληρωμή και συμβόλαια eRoaming.

Εικόνα 11: Logo Βιομηχανιών και Έργων.

4 Ευφυή Ηλεκτρικά Δίκτυα (Smartgrids)

4.1 Τι είναι το Ευφυές Ηλεκτρικό Δίκτυο

Ένα ευφυές ηλεκτρικό δίκτυο είναι ένα ηλεκτρικό δίκτυο που περιλαμβάνει μια ποικιλία λειτουργιών και ενέργειας, όπως:

- Προηγμένη υποδομή μέτρησης (οι έξυπνοι μετρητές είναι μια γενική ονομασία για οποιαδήποτε βοηθητική συσκευή).
- Έξυπνοι πίνακες διανομής και διακόπτες κυκλώματος ενσωματωμένοι με οικιακό έλεγχο και απόκριση ζήτησης (έπεται του μετρητή από την άποψη της χρησιμότητας).
- Διακόπτες ελέγχου φορτίου και έξυπνες συσκευές.
- Ανανεώσιμες πηγές ενέργειας, συμπεριλαμβανομένης της ικανότητας φόρτισης μπαταριών σταθμευμένων (ηλεκτρικών οχημάτων) ή μεγαλύτερων σειρών μπαταριών που ανακυκλώνονται από αυτές ή άλλης αποθήκευσης ενέργειας.
- Κατανομή πλεονάσματος ηλεκτρικής ενέργειας με ηλεκτροφόρα καλώδια και αυτόματο έξυπνο διακόπτη.
- Η ηλεκτρονική ρύθμιση ισχύος και ο έλεγχος της παραγωγής και διανομής ηλεκτρικής ενέργειας είναι σημαντικές πτυχές του έξυπνου δικτύου.

Έχουν διατυπωθεί αρκετοί **ορισμοί** για το Έξυπνο Δικτύο, όπως οι παρακάτω:

Ο πρώτος επίσημος ορισμός του Έξυπνου Δικτύου παρέχεται από τον Νόμο για την Ενεργειακή Ανεξαρτησία και την Ασφάλεια του 2007 (EISA-2007), ο οποίος εγκρίθηκε από το Κογκρέσο των **ΗΠΑ** τον Ιανουάριο του 2007. Παρέχει μια περιγραφή, με δέκα χαρακτηριστικά, που μπορεί να θεωρηθεί ως ορισμός για το Smart Grid:

«Αποτελεί πολιτική των Ηνωμένων Πολιτειών να υποστηρίξουν τον εκσυγχρονισμό του συστήματος μεταφοράς και διανομής ηλεκτρικής ενέργειας του Έθνους για τη διατήρηση μιας αξιόπιστης και ασφαλούς υποδομής ηλεκτρικής ενέργειας που μπορεί να καλύψει τη μελλοντική αύξηση της ζήτησης και να επιτύχει καθένα από τα ακόλουθα, τα οποία μαζί χαρακτηρίζουν ένα Έξυπνο Δίκτυο:

(1) Αυξημένη χρήση της τεχνολογίας ψηφιακών πληροφοριών και ελέγχων για τη βελτίωση της αξιοπιστίας, της ασφάλειας και της αποτελεσματικότητας του ηλεκτρικού δικτύου.
(2) Δυναμική βελτιστοποίηση των λειτουργιών και των πόρων του δικτύου, με πλήρη ασφάλεια στον κυβερνοχώρο.
(3) Ανάπτυξη και ενοποίηση κατανεμημένων πόρων και παραγωγή, συμπεριλαμβανομένων των ανανεώσιμων πόρων.
(4) Ανάπτυξη και ενσωμάτωση ανταπόκρισης στη ζήτηση, πόρων από την πλευρά της ζήτησης και πόρων ενεργειακής απόδοσης.
(5) Ανάπτυξη «έξυπνων» τεχνολογιών (σε πραγματικό χρόνο, αυτοματοποιημένες, διαδραστικές τεχνολογίες που βελτιστοποιούν τη φυσική λειτουργία συσκευών και καταναλωτικών συσκευών)

για μέτρηση, επικοινωνίες σχετικά με τις λειτουργίες και την κατάσταση του δικτύου και αυτοματισμό διανομής.
(6) Ενοποίηση «έξυπνων» συσκευών και καταναλωτικών συσκευών.
(7) Ανάπτυξη και ενοποίηση προηγμένων τεχνολογιών αποθήκευσης ηλεκτρικής ενέργειας, συμπεριλαμβανομένων των plug-in ηλεκτρικών και υβριδικών ηλεκτρικών οχημάτων και κλιματισμού.
(8) Παροχή στους καταναλωτές έγκαιρης ενημέρωσης και επιλογών ελέγχου.
(9) Ανάπτυξη προτύπων επικοινωνίας και διαλειτουργικότητας συσκευών και εξοπλισμού που συνδέονται με το ηλεκτρικό δίκτυο, συμπεριλαμβανομένης της υποδομής που εξυπηρετεί το δίκτυο.
(10) Εντοπισμός και μείωση εμποδίων στην υιοθέτηση τεχνολογιών, πρακτικών και υπηρεσιών έξυπνων δικτύων.»

Η **Ευρωπαϊκή Ένωση** παρέχει επίσης τον ορισμό του έξυπνου δικτύου ως:

«Ένα Έξυπνο Δίκτυο είναι ένα δίκτυο ηλεκτρικής ενέργειας που μπορεί να ενσωματώσει οικονομικά αποδοτικά τη συμπεριφορά και τις ενέργειες όλων των χρηστών που είναι συνδεδεμένοι με αυτό –γεννητριών, καταναλωτών και εκείνων που κάνουν και τα δύο– προκειμένου να διασφαλιστεί οικονομικά αποδοτικό, βιώσιμο σύστημα ηλεκτρικής ενέργειας με χαμηλές απώλειες και υψηλά επίπεδα ποιότητας. Ένα έξυπνο δίκτυο χρησιμοποιεί καινοτόμα προϊόντα και υπηρεσίες σε συνδυασμό με έξυπνες τεχνολογίες παρακολούθησης, ελέγχου και επικοινωνίας προκειμένου:

(1) Την καλύτερη σύνδεση και λειτουργία γεννητριών όλων των μεγεθών και τεχνολογιών.
(2) Οι καταναλωτές να παίξουν ρόλο στη βελτιστοποίηση της λειτουργίας του συστήματος.
(3) Παροχή περισσότερων πληροφοριών και επιλογές για τον τρόπο με τον οποίο χρησιμοποιούν την προμήθεια τους οι καταναλωτές .
(4) Σημαντική μείωση των περιβαλλοντικών επιπτώσεων ολόκληρου του συστήματος παροχής ηλεκτρικής ενέργειας.
(5) Διατήρηση ή ακόμα και βελτίωση των υπάρχοντων υψηλών επιπέδων αξιοπιστίας, ποιότητας και ασφάλειας του συστήματος.
(6) Διατήρηση και βελτίωση της αποτελεσματικότητας των υπαρχουσών υπηρεσιών».

Η ροή δεδομένων και η διαχείριση πληροφοριών καθιστώνται θεμελιώδη στοιχεία στο έξυπνο δίκτυο, μέσω της εφαρμογής ψηφιακής επεξεργασίας και επικοινωνιών. Προκύπτουν διάφορες δυνατότητες από τη βαθιά ενοποιημένη χρήση της ψηφιακής τεχνολογίας με τα δίκτυα ενέργειας. [17]

4.2 Οφέλη Ευφυούς Ηλεκτρικού Δικτύου

Τα παλαιότερα δίκτυα ηλεκτρικής ενέργειας αντικαθίστανται από ευφυή και πιο αποδοτικά δίκτυα που συνοδεύονται από καλύτερη διαχείριση ενέργειας και παρακολούθηση πληροφοριών. Αντιπροσωπεύουν μια νέα εποχή στον ηλεκτρικό τομέα, καθώς περνάμε από τη στατική μονόδρομη διαχείριση στη δυναμική αμφίδρομη διαχείριση. Αυτό αυξάνει την απόδοση και την

εξοικονόμηση ενέργειας.Υπάρχουν πολλά οφέλη από την επένδυση στην τεχνολογία Smart Grid, όπως:

- **Εξοικονόμηση ενέργειας**
  Ένα από τα πλεονεκτήματα των έξυπνων δικτύων είναι ότι δείχνουν την κατανάλωση σε έναν μετρητή ενέργειας ανά πάσα στιγμή, έτσι ώστε οι χρήστες να ενημερώνονται καλύτερα για την πραγματική τους κατανάλωση. Επιπλέον, με καλύτερη παρακολούθηση της κατανάλωσης, η ενέργεια μπορεί να προσαρμοστεί για να καλύψει τις πραγματικές ανάγκες κάθε καταναλωτή.

- **Καλύτερη εξυπηρέτηση πελατών - Ακριβείς λογαριασμοί**
  Ένα άλλο βασικό πλεονέκτημα είναι η ακρίβεια των λογαριασμών. Αντικατοπτρίζουν πάντα την πραγματική κατανάλωση κάθε μήνα αντί για εκτιμήσεις, μειώνοντας το κόστος του παλιού συστήματος χειροκίνητων μετρητών ενέργειας. Εκτός από τη δυνατότητα απομακρυσμένης πρόσβασης σε πληροφορίες σχετικά με την εγκατάσταση, τα προβλήματα γίνονται ευκολότερα στη διάγνωση και ως εκ τούτου οι λύσεις μπορούν να εφαρμοστούν πιο γρήγορα, βελτιώνοντας την εξυπηρέτηση πελατών.

- **Ανίχνευση απάτης - Τεχνικές απώλειες**
  Ανιχνεύσουν την απάτη με πολύ μεγαλύτερη ακρίβεια, καθώς οι μονάδες δεν περιέχουν εξαρτήματα που υπόκεινται σε μηχανική φθορά. Επιπλέον, οι νέοι μετρητές ενέργειας μπορούν να στείλουν μια αυτόματη ειδοποίηση στους διαχειριστές του δικτύου προειδοποίησης για πιθανή απάτη.

- **Μειωμένο κόστος εξισορρόπησης**
  Συλλέγουν πολύ περισσότερα δεδομένα από το χειροκίνητο σύστημα ανάγνωσης μετρητών ενέργειας. Έτσι προκύπτουν ρεαλιστικές προβλέψεις κατανάλωσης καθώς λαμβάνονται υπόψη πολλές περισσότερες μεταβλητές. Στη συνέχεια, οι επιχειρήσεις κοινής ωφέλειας μπορούν να προσαρμόσουν καλύτερα την παραγωγή τους στην κατανάλωση (ισορροπία) και να μειώσουν τα πλεονάσματα ενέργειας.

- **Αυξημένος ανταγωνισμός**
  Οι εταιρείες μάρκετινγκ να προσαρμόσουν τις τιμές τους με βάση τη ζήτηση ενέργειας. Όταν οι εταιρείες μάρκετινγκ έχουν περισσότερα δεδομένα, μπορούν να κάνουν καλύτερες προσφορές που συνάδουν περισσότερο με την πραγματικότητα, αυξάνοντας, έτσι, τις ανταγωνιστικές επιλογές μέσω μεγαλύτερης ποικιλίας προσφορών (ωριαία τιμολόγια, ενεργειακά πακέτα κ.λπ.). Αυτό ωφελεί τους καταναλωτές καθώς ο περισσότερος ανταγωνισμός οδηγεί σε πιο ανταγωνιστικές τιμές.

- **Ισοπέδωση της καμπύλης ζήτησης (Μείωση αιχμής)**

Μέσω της χρήσης διαφορετικών προφίλ τιμολόγησης, οι επιχειρήσεις κοινής ωφέλειας μπορούν να ισοπεδώσουν την καμπύλη ημερήσιας ζήτησης για να μετατοπίσουν τις κορυφές κατανάλωσης σε περιόδους με χαμηλότερη ζήτηση, βελτιστοποιώντας τη χρήση του ηλεκτρικού δικτύου. Έτσι, οι πελάτες μπορούν σκόπιμα να καταναλώνουν ενέργεια σε ώρες εκτός αιχμής, όταν κάθε kWh είναι λιγότερο ακριβή. Για παράδειγμα: ένας πελάτης μπορεί να αποφασίσει να αλλάξει τις καταναλωτικές του συνήθειες χρησιμοποιώντας το πλυντήριο σε ώρες εκτός αιχμής, τη νύχτα, όταν κάθε kWh είναι πιο οικονομική, εξοικονομώντας χρήματα και βοηθώντας το δίκτυο να εξισορροπήσει την κατανάλωση.

- **Μείωση των εκπομπών άνθρακα**
  Όλα τα παραπάνω οφέλη περιλαμβάνουν τη μείωση της κατανάλωσης ενέργειας, η οποία συνοδεύεται με τη μείωση των εκπομπών CO2. Η μείωση εκπομπών άνθρακα οδηγεί σε ένα πιο βιώσιμο μέλλον.

Η μετάβαση από το Παραδοσιακό Ηλεκτρικό Δίκτυο στο Έξυπνο Δίκτυο απαιτεί την ύπαρξη τηλεπικοινωνιακών δικτύων για τη μετάδοση δεδομένων, καθώς και ευφυών δικτύων διανομής, μεταφοράς και αποθήκευσης. Αυτοί οι συνδυασμοί τεχνολογιών είναι ουσιώδεις για την προσαρμογή του δικτύου στις ανάγκες της σύγχρονης ενεργειακής αγοράς, προωθώντας την αποδοτικότητα, την αξιοπιστία και τη βιωσιμότητα.

4.3 Έξυπνοι Μετρητές

4.3.1 Τι είναι οι Έξυπνοι Μετρητές

Ένας έξυπνος μετρητής είναι μια ηλεκτρονική συσκευή που καταγράφει πληροφορίες, όπως η κατανάλωση ηλεκτρικής ενέργειας, τα επίπεδα τάσης, το ρεύμα και το συντελεστή ισχύος και έπειτα κοινοποιεί τις πληροφορίες στους καταναλωτές και στους προμηθευτές ηλεκτρικής ενέργειας. Οι καταναλωτές αποκτούν για μεγαλύτερη σαφήνεια για τη συμπεριφορά κατανάλωσης και οι προμηθευτές για την παρακολούθηση του συστήματος και την τιμολόγηση των πελατών. Οι έξυπνοι μετρητές καταγράφουν συνήθως ενέργεια σε πραγματικό χρόνο και την αναφέρουν ανά τακτά, μικρά διαστήματα κατά τη διάρκεια της ημέρας. Επιτρέπουν την αμφίδρομη επικοινωνία μεταξύ του μετρητή και του κεντρικού συστήματος. Αν και δεν αποτελούν οι ίδιοι ένα έξυπνο δίκτυο, μπορεί να αποτελούν μέρος του.

Οι εταιρείες κοινής ωφέλειας με τη χρήση έξυπνων μετρητών μπορούν να χρεώνουν διαφορετικές τιμές για την κατανάλωση ανάλογα με την ώρα της ημέρας και την εποχή. Μια ακαδημαϊκή μελέτη βασισμένη σε υπάρχουσες δοκιμές έδειξε ότι η κατανάλωση ηλεκτρικής ενέργειας των ιδιοκτητών σπιτιού μειώνεται κατά μέσο όρο κατά 3-5% όταν παρέχεται ανατροφοδότηση σε πραγματικό χρόνο. Οι έξυπνοι μετρητές είναι το κλειδί για την αύξηση της απορρόφησης της κατανεμημένης παραγωγής ηλεκτρικής ενέργειας, η οποία, εκτός από το ότι επιτρέπει στους

πελάτες να παράγουν τη δική τους ενέργεια, είναι καίριας σημασίας για τη μείωση του αποτυπώματος άνθρακα και την καταπολέμηση της υπερθέρμανσης του πλανήτη.

4.3.2 Διαφορές Συμβατικών και Έξυπνων Μετρητών

Σε αρκετές περιπτώσεις οι έξυπνοι μετρητές έχουν αντικαταστήσει τους παραδοσιακούς μετρητές. Σε αντίθεση με τους έξυπνους, οι παραδοσιακοί μετρητές ηλεκτρικής ενέργειας καταγράφουν μόνο την κατανάλωση ηλεκτρικής ενέργειας. Οι έξυπνοι μετρητές εκτός από την καταγραφή της ποσότητας ηλεκτρικής ενέργειας που εισέρχεται στον χρήστη, είναι επίσης δυνατή η καταγραφή της ποσότητας ηλεκτρικής ενέργειας που παρέχει ο χρήστης στο δίκτυο. Οι χρήστες έξυπνων μετρητών μπορούν να κατασκευάσουν εγκαταστάσεις παραγωγής ηλεκτρικής ενέργειας (για παράδειγμα από αιολική ή ηλιακή ενέργεια) και αν η παραγόμενη ενέργεια δεν μπορεί να εξαντληθεί, μπορούν να μεταδώσουν πλεονάζουσα ενέργεια στο δίκτυο ηλεκτρικής ενέργειας. Με αυτόν τον τρόπο επιτυγχάνεται εξοικονόμηση ενέργειας και προστασία του περιβάλλοντος με τη μείωση των εκπομπών διοξειδίου του άνθρακα.

Τα κύρια χαρακτηριστικά ενός παραδοσιακού και ενός έξυπνου μετρητή αποτελούν τις ειδοποιούς διαφορές τους. Συγκεκριμένα:

Στον Παραδοσιακό μετρητή:

- Δεν αποθηκεύονται δεδομένα.
- Οι μετρήσεις πρέπει να γίνονται χειροκίνητα.
- Ένας εκτιμώμενος λογαριασμός εκδίδεται όταν δεν παρέχεται ένδειξη του μετρητή.
- Η χρήση παρακολουθείται συνήθως σε μηνιαία ή τριμηνιαία βάση.
- Δεν υπάρχει απάντηση σε πραγματικό χρόνο σε προβλήματα με τον εφοδιασμό.
- Οι συνδέσεις και οι αποσυνδέσεις πρέπει να γίνονται χειροκίνητα.

Στον Έξυπνο μετρητή:

- Τα δεδομένα αποθηκεύονται κάθε μισή ώρα.
- Η κατανάλωση ενέργειας αποστέλλεται ψηφιακά στον προμηθευτή.
- Οι λογαριασμοί βασίζονται πάντα σε αυτό που έχει χρησιμοποιήσει ο καταναλωτής.
- Η κατανάλωση ενέργειας εμφανίζεται σχεδόν σε πραγματικό χρόνο, μέσα σε λίγα δευτερόλεπτα από τη χρήση.
- Ο προμηθευτής μπορεί να δει πότε υπάρχει πρόβλημα με την παροχή και να διορθώσει το πρόβλημα.
- Οι συνδέσεις και οι αποσυνδέσεις γίνονται εξ' αποστάσεως.

Αξιοσημείωτο είναι το γεγονός ότι περισσότερο από το 54% των μετρητών που χρησιμοποιούνται σήμερα σε όλη την Αγγλία, τη Σκωτία και την Ουαλία είναι έξυπνοι μετρητές και στόχος των κυβερνήσεων είναι να εγκατασταθούν σε όλα τα σπίτια έως το 2025. Στην Ελλάδα στις 7 Νοεμβρίου 2023 υπεγράφη η σύμβαση δανειοδότησης ενός φιλόδοξου επενδυτικού προγράμματος το οποίο αφορά στην εγκατάσταση 7,3 εκατομμυρίων έξυπνων μετρητών ηλεκτρικής ενέργειας σε όλα τα νοικοκυριά και τις επιχειρήσεις.

Η εγκατάσταση των έξυπνων μέτρητών θα αλλάξει πλήρως το σκηνικό της αγοράς ηλεκτρισμού τόσο για τους καταναλωτές όσο και για τους προμηθευτές. Παρακάτω παρουσιάζονται τα οφέλη χρήσης έξυπνων μετρητών και για τις δύο πλευρές.

Οφέλη για τους καταναλωτές:

- **Μεγιστοποίηση της διαφάνειας**: Ενισχύεται η εμπιστοσύνη του καταναλωτή προς τους παρόχους των υπηρεσιών ενέργειας. Τα δεδομένα κατανάλωσης ηλεκτρικής ενέργειας συλλέγονται, μεταφέρονται και διατηρούνται με ασφάλεια και έτσι αποφεύγονται προβλήματα από λάθη καταμέτρησης ή από δυσκολία στην κατανόηση των λογαριασμών ή την επιβεβαίωση των στοιχείων.

- **Δυνατότητα εξοικονόμησης**: Οι καταναλωτές ηλεκτρικής ενέργειας λαμβάνουν ανταγωνιστικές προσφορές για προϊόντα προμήθειας ηλεκτρικού ρεύματος προσαρμοσμένα στο προφίλ της κατανάλωσής τους και επιλέγουν οι ίδιοι αυτό που θεωρούν οικονομικότερο. Μάλιστα, τους δίνεται τεχνικά η δυνατότητα να αλλάζουν προμηθευτή ακόμα και στη διάρκεια της ημέρας ή η αλλαγή πακέτου ανάλογα με την περίοδο χρήσης, π.χ. ώρες αιχμής κατά τη διάρκεια της ημέρας, σαββατοκύριακο ή αργίες.

- **Υπηρεσίες προστιθέμενης αξίας από την αγορά**: Παρέχεται η δυνατότητα στους καταναλωτές να λαμβάνουν υπηρεσίες προστιθέμενης αξίας από την αγορά π.χ. ιστορικά δεδομένα, ανάλυση προφίλ κατανάλωσης, προτάσεις για εξοικονόμηση, νέες υπηρεσίες όπως απόκριση για τη διαχείριση της ζήτησης.

- **Καταναλωτές στο ρόλο του παρόχου**: Οι έξυπνοι μετρητές επιτρέπουν τη μέτρηση ενέργειας και προς τις δύο κατευθύνσεις και την καταγραφή της, με ανάλυση 15λέπτου, κάτι που μεταφράζεται στη δυνατότητα που δίνεται π.χ. σε μικροπαραγωγούς με φωτοβολταϊκά στέγης (που είναι επίσης και καταναλωτές ηλεκτρικής ενέργειας) να πωλούν ενέργεια αλλά και να την αποθηκεύουν και να την παρέχουν στο δίκτυο όταν οι συνθήκες αγοράς είναι οι ευνοϊκότερες.

Οφέλη για τους προμηθευτές:

- **Διαφάνεια στα στοιχεία καταμέτρησης**: Βελτιώνονται οι σχέσεις προμηθευτών - καταναλωτών, ιδίως λόγω του ότι αποφεύγονται λάθη καταμέτρησης και παράπονα για υπέρμετρες χρεώσεις και στους λογαριασμούς.

- **Καλύτερος οικονομικός προγραμματισμός**: Η συχνή μέτρηση και έκδοση λογαριασμών με μικρότερους χρόνους πληρωμής, η άμεση αποκοπή στις περιπτώσεις που προβλέπεται, ο περιορισμός της κατανάλωσης πάνω από ένα συγκεκριμένο όριο και το μικρότερο διαχειριστικό κόστος αλλά και ο απαιτούμενος χρόνος για την αντιμετώπιση τέτοιου είδους θεμάτων, οδηγεί σε βελτίωση του κόστους και στην μείωση του οικονομικού κινδύνου και των

συναφών επισφαλειών.

- **Επιχειρηματικά οφέλη**: Οι προμηθευτές ηλεκτρικής ενέργειας προβλέπουν με μεγαλύτερη ακρίβεια και ασφάλεια την καταναλωτική συμπεριφορά κάθε χρήστη ηλεκτρικής ενέργειας. Αυτό έχει ως αποτέλσματα να διαμορφώνουν περισσότερους, πιο ευέλικτους και πιο προσαρμοσμένους συνδυασμούς πακέτων και προσφορών για τους πελάτες τους, βελτιώνοντας τη θέση τους στην αγορά και τους οικονομικούς τους δείκτες. Έτσι υλοποιείται πολυζωνική τιμολόγηση που συνιστά απαραίτητο πλαίσιο ώστε να εισέλθει η δραστηριότητα προμήθειας ηλεκτρικής ενέργειας σε μία εποχή δυναμικής, ευέλικτης και κατάλληλα προσαρμοσμένης στον καταναλωτή τιμολόγησης.

- **Βελτιστοποίηση λειτουργίας της αγοράς**: Με χρήση των προβλέψεων τόσο για την παραγωγή όσο και για τη ζήτηση ηλεκτρικής ενέργειας, παρατηρούνται εξελικτικά βήματα στο συνολικό τρόπο λειτουργίας της αγοράς ηλεκτρικής ενέργειας.

- **Αναβάθμιση της αγοράς**: Εφαρμόζονται νέα επιχειρηματικά μοντέλα και προσφορές καινοτόμων υπηρεσιών όπως π.χ. η φόρτιση ηλεκτρικών οχημάτων, η έξυπνη φόρτιση και η ενεργειακή αποδοτικότητα.

- **Αξιόπιστη διαχείρηση δεδομένων**: Με την επεξεργάσια των δεδομένων δημιουργούνται νέοι επιχειρηματικοί σκοποί και δίνεται η ευκαιρία διαμόρφωσης νέων πεδίων δραστηριοποίησης στο ευρύτερο τεχνολογικό οικοσύστημα, όπως της ανάλυσης δεδομένων και του Internet of Things. [18], [19]

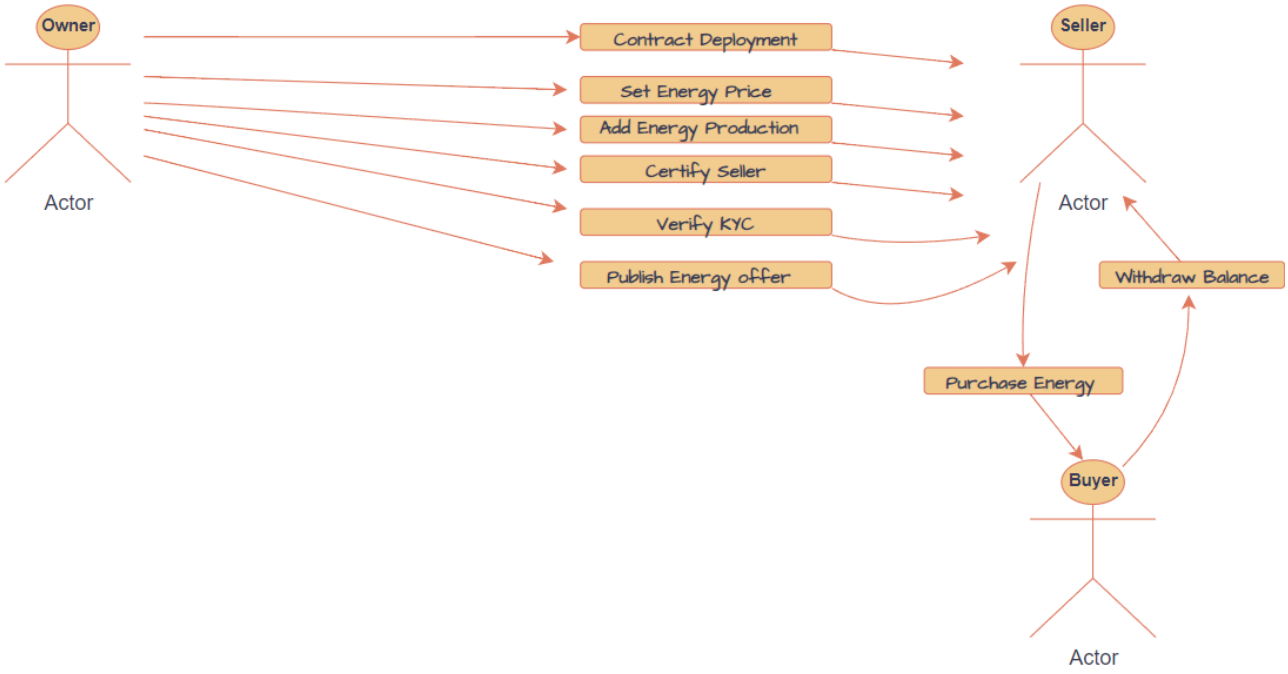
5 Υλοποίηση του Energy Market System

5.1 Στόχος του Energy Market System

Στόχος της παρούσας Διπλωματικής Εργασίας είναι η δημιουργία ενός αυτόνομου, αποκεντρωμένου συστήματος διαχείρισης ενέργειας μέσω του Ethereum Blockchain. Έτσι, δημιούργησα το Energy Market System που επιτρέπει σε μια ομάδα ατόμων ή σε μια κοινότητα να ανταλλάσσει ηλεκτρική ενέργεια χωρίς την ανάγκη ενδιάμεσων οντοτήτων. Με αυτόν τρόπο, επιτυγχάνεται η αποκεντρωμένη παραγωγή και διαχείριση ηλεκτρικής ενέργειας.

Το Energy Market System διευκολύνει τη διαδικασία αγοραπωλησίας ενέργειας σε ένα ανοιχτό και διαφανές περιβάλλον. Είναι κατάλληλο για μια σύγχρονη τεχνολογικά και περιβαλλοντικά συνειδητή κοινότητα που επενδύει σε αποκεντρωμένες, διαφανείς και οικονομικά ωφέλιμες συναλλαγές ενέργειας μεταξύ των μελών της. Συμβαδίζει με τις αρχές της βιωσιμότητας, της ενεργού συμμετοχής όλων των μελών της κοινότητας και της τεχνολογικής καινοτομίας στον τομέα της ενέργειας. Είναι ένα λειτουργικό περιβάλλον αγοράς και πώλησης ενέργειας με μηχανισμούς ελέγχου και ασφαλείας.

Με χρήση uml εργαλείων προκύπτει το διάγραμμα αλληλεπιδράσεων μεταξύ των διαφορετικών παραγόντων του συμβολαίου (ιδιοκτήτη, πωλητές και αγοραστές ενέργειας).



Εικόνα 12: Sequence Diagram.

5.2 Βήματα για τη Δημιουργία Έξυπνου Συμβολαίου

Αφού το συμβόλαιο θα αναπτυχθεί στο δίκτυο του Ethereum θα χρησιμοποιηθεί η γλώσσα Solidity. Παρακάτω παρατίθενται τα βασικά βήματα για τη δημιουργία αυτού του έξυπνου συμβολαίου αλλά και κάθε άλλου σε γλώσσα επιλογής του προγραμματιστή:

1. **Εγκατάσταση ενός Solidity συντάκτη (compiler)**: Εγκατάσταση ενός Solidity συντάκτη στον υπολογιστή. Εξαιρετικά φιλικό για προγραμματιστές λόγω απλότητας και αποτελεσματικότητας είναι το Remix Project και το IDE (Integrated Development Environment) που προσφέρει το Remix Ethereum.

   Μέσω αυτού θα γίνει τόσο η συγγραφή όσο και η μεταγλώττιση του συμβολαίου. Επιπρόσθετα, από το ίδιο το Remix IDE μπορεί να γίνει και το "deployment" στο δίκτυο του Ethereum αρκεί ο χρήστης και σύντομα ιδιοκτήτης του συμβολαίου να έχει δημιουργήσει πορτοφόλι κρυπτονομισμάτων στο Metamask διαθέτοντας επαρκή κρυπτονομίσματα για να καλύψει το τέλος συναλλαγής.

2. **Δημιουργία αρχείου Solidity**: Δημιουργία ενός νέου αρχείου με κατάληξη *.sol* για να συγγραφή του κώδικα του συμβολαίου.

3. **Ορισμός του** *pragma*: Στην αρχή του αρχείου Solidity, ορίζεται η έκδοση Solidity που θα χρησιμοποιηθεί. Για παράδειγμα: *pragmasolidity* 0.8.7. Η δήλωση της έκδοσης του μεταγλωττιστή Solidity που θα χρησιμοποιηθεί βοηθά στην αποφυγή προβλημάτων με μελλοντικές εκδόσεις μεταγλωττιστή που εισάγουν αλλαγές που ενδέχεται να εμποδίσουν τον κώδικά σας.

4. **Ορισμός του συμβολαίου**: Συνήθως, το συμβόλαιο ξεκινά με τη δήλωση της λέξης-κλειδιού *contract* ακολουθούμενη από το όνομα του συμβολαίου. Για παράδειγμα: $contractMyContract$ ... .

5. **Ορισμός μεταβλητών**: Δήλωση μεταβλητών στο σώμα του συμβολαίου. Για παράδειγμα: $uint256publicmyVariable$;.

6. **Ορισμός του κατασκευαστή** (*constructor*): Ορισμός συνάρτησης με το ίδιο όνομα με το συμβόλαιο, η οποία θα εκτελείται κατά τη δημιουργία του συμβολαίου. Αυτή η συνάρτηση χρησιμοποιείται για την αρχικοποίηση των μεταβλητών. Για παράδειγμα: $constructor()$ ... .

7. **Ορισμός συναρτήσεων**: Δυνατότητα ορισμού πρόσθετων συναρτήσεων που θα εκτελούνται από το συμβόλαιο. Για παράδειγμα: $functionmyFunction()public$ ... .

8. **Μεταγλώττιση του συμβολαίου**: Χρήση του Solidity συντάκτη για μεταγλώττιση του συμβολαίου.

9. **Καταχώρηση του συμβολαίου στο blockchain**: Καταχώρηση του συμβολαίου στο blockchain της επιλογής σας. Αυτό μπορεί να γίνει μέσω της εντολής συναλλαγής (transaction) σε ένα blockchain δοκιμαστικού περιβάλλοντος, όπως το Ganache, ή μέσω μιας διεπαφής που προσφέρεται από μια blockchain πλατφόρμα όπως το Ethereum.

10. **Διεπαφή χρήστη**: Ανάλογα με τον τρόπο ανάπτυξης του συμβολαίου, δημιουργείται μια διεπαφή χρήστη (UI) για αλληλεπίδραση με το συμβόλαιο. Αυτό μπορεί να γίνει με την ανάπτυξη μιας δικής μας εφαρμογής ή χρησιμοποιώντας μια υπάρχουσα πλατφόρμα αλληλεπίδρασης με τα έξυπνα συμβόλαια, όπως το Metamask.

Αυτά τα 10 βήματα αποτελούν τη διαδικασία δημιουργίας ενός έξυπνου συμβολαίου σε γλώσσα Solidity.

5.3 Κώδικας για το Energy Market System

Παρακάτω, παρατίθεται ο κώδικας του συμβολαίου:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract EnergyMarket {
    address public owner; // Contract owner
    uint256 public energyPrice; // Price per unit of energy in wei (1 Ether = 1e18 wei)
    uint256 public totalEnergyProduced; // Total energy produced by all sellers

    struct EnergyOffer {
        address seller;
        uint256 energyAmount;
        uint256 price;
        uint256 startTime;
        uint256 endTime;
        bool isActive;
        bytes32 smartMeterId; // Smart meter identifier
   }

    struct EnergyProducedData {
        uint256 energyProduced;
        bytes32 encryptedSmartMeterId; // Encrypted smart meter identifier
    }
    mapping(address => EnergyProducedData) private energyProducedData;

    EnergyOffer[] public energyOffers;

    mapping(address => uint256) public energyBalances; // Energy balances for each neighbor
    mapping(address => bool) public isCertifiedSeller; // Certification status of sellers
    mapping(address => bool) public isKYCVerified; // KYC verification status

    function reportEnergyProduced(
    uint256 _energyProduced,
    bytes32 _encryptedSmartMeterId,
    uint8 v,
    bytes32 r,
    bytes32 s
) public {
    require(isCertifiedSeller[msg.sender], "Sender is not a certified smart meter");

    // Verify the signature
    bytes32 messageHash = keccak256(abi.encodePacked(msg.sender, _energyProduced, _encryptedSmartMeterId));
    address recoveredAddress = ecrecover(messageHash, v, r, s);
    require(recoveredAddress == msg.sender, "Invalid signature");

    // Store encrypted data off-chain
    energyProducedData[msg.sender] = EnergyProducedData({
        energyProduced: _energyProduced,
        encryptedSmartMeterId: _encryptedSmartMeterId
```

```
49      });
50
51      // Emit an event without sensitive data
52      emit EnergyProduced(msg.sender);
53  }
54
55
56      function getEnergyProducedData() public view returns (uint256, bytes32) {
57          require(isCertifiedSeller[msg.sender], "Sender is not a certified smart meter");
58
59          // Retrieve encrypted data
60          EnergyProducedData storage data = energyProducedData[msg.sender];
61          return (data.energyProduced, data.encryptedSmartMeterId);
62      }
63
64       event EnergyProduced(address indexed smartMeter);
65       event EnergyOfferPublished(
66          uint256 indexed offerId,
67          address indexed seller,
68          uint256 energyAmount,
69          uint256 price,
70          uint256 startTime,
71          uint256 endTime,
72          bytes32 smartMeterId // Include smart meter ID in the event
73
74      );
75      event EnergyPurchased(
76          address indexed buyer,
77          uint256 indexed offerId,
78          uint256 energyAmount,
79          uint256 totalPrice
80      );
81
82      constructor(uint256 _initialEnergyPrice) {
83          owner = msg.sender;
84          energyPrice = _initialEnergyPrice;
85      }
86
87      modifier onlyOwner() {
88          require(msg.sender == owner, "Only the contract owner can call this function");
89          _;
90      }
91
92      function setEnergyPrice(uint256 _newPrice) public onlyOwner {
93          energyPrice = _newPrice;
94      }
95
96
97
98      function certifySeller(address _seller) public onlyOwner {
99          isCertifiedSeller[_seller] = true;
100     }
101
```

```
102     function verifyKYC(address _user) public onlyOwner {
103         isKYCVerified[_user] = true;
104     }
105 
106     function publishEnergyOffer(
107         uint256 _energyAmount,
108         uint256 _price,
109         uint256 _durationHours,
110         bytes32 _smartMeterId // New parameter for smart meter ID
111     ) public {
112         require(isCertifiedSeller[msg.sender], "Seller is not certified");
113         require(isKYCVerified[msg.sender], "Seller is not KYC verified");
114         require(_energyAmount > 0, "Energy amount must be greater than zero");
115         require(_price > 0, "Price must be greater than zero");
116         require(_durationHours > 0, "Duration must be greater than zero");
117 
118         uint256 startTime = block.timestamp;
119         uint256 endTime = startTime + (_durationHours * 1 hours);
120 
121         energyOffers.push(
122             EnergyOffer({
123                 seller: msg.sender,
124                 energyAmount: _energyAmount,
125                 price: _price,
126                 startTime: startTime,
127                 endTime: endTime,
128                 isActive: true,
129                 smartMeterId: _smartMeterId // Set the smart meter ID
130             })
131         );
132 
133         emit EnergyOfferPublished(
134             energyOffers.length - 1,
135             msg.sender,
136             _energyAmount,
137             _price,
138             startTime,
139             endTime,
140             _smartMeterId // Emit smart meter ID in the event
141         );
142     }
143 
144     function purchaseEnergy(uint256 _offerId, uint256 _energyAmount) public payable {
145         require(_offerId < energyOffers.length, "Invalid offer ID");
146         EnergyOffer storage offer = energyOffers[_offerId];
147 
148         require(offer.isActive, "The offer is no longer active");
149         require(_energyAmount > 0, "Energy amount must be greater than zero");
150         require(
151             block.timestamp >= offer.startTime && block.timestamp <= offer.endTime,
152             "The offer is not available at the moment"
153         );
154 
```

```
155         uint256 totalPrice = (offer.price * _energyAmount);
156         require(msg.value >= totalPrice, "Insufficient funds to purchase energy");
157 
158         energyBalances[msg.sender] += _energyAmount;
159         energyBalances[offer.seller] -= _energyAmount;
160 
161         // Transfer payment to the seller
162         payable(offer.seller).transfer(totalPrice);
163 
164         // Deactivate the offer if the energy quantity is fully purchased
165         if (_energyAmount == offer.energyAmount) {
166             offer.isActive = false;
167         }
168 
169         emit EnergyPurchased(msg.sender, _offerId, _energyAmount, totalPrice);
170     }
171 
172     function withdrawBalance() public {
173         uint256 balance = energyBalances[msg.sender];
174         require(balance > 0, "No balance to withdraw");
175 
176         energyBalances[msg.sender] = 0;
177         payable(msg.sender).transfer(balance);
178     }
179 }
```

5.4 Ανάλυση της Λειτουργίας του Energy Market System

Το Energy Market System είναι ένα ρεαλιστικό και νομικά συμμορφομένο έξυπνο συμβόλαιο. Έχει χαρακτηριστικά που λαμβάνουν υπόψη την ταυτότητα των χρηστών Know Your Customer (KYC), την πιστοποίηση ενέργειας και τη συμμόρφωση με νομικά πρότυπα. Η διαδικάσια Know Your Customer (KYC) αναφέρεται σε ένα σύνολο διαδικασιών που εφαρμόζονται από επιχειρήσεις και οργανισμούς για να αναγνωρίσουν και να επαληθεύσουν την ταυτότητα των πελατών τους μέσω της συλλογής διαφόρων πληροφοριών και εγγράφων των πελατών, όπως αναγνωριστικά, διευθύνσεις, φωτογραφίες και άλλα στοιχεία που μπορούν να χρησιμοποιηθούν για να επαληθευτεί η ταυτότητά τους. Παρακάτω εξηγείται λεπτομερώς ο κώδικας του συμβολαίου:

```
1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.0;
```

Αυτές οι γραμμές περιέχουν τη δήλωση άδειας χρήσης (license) για το συμβόλαιο, που σε αυτήν την περίπτωση είναι η MIT License. Αυτό δείχνει ότι το συμβόλαιο υπόκειται σε αυτήν την άδεια

χρήσης. Το *pragmasolidity* 0.8.0 δηλώνει την έκδοση της γλώσσας Solidity που χρησιμοποιείται και ορίζει ότι το συμβόλαιο πρέπει να συμμορφώνεται με τις εκδόσεις Solidity από 0.8.0 και μετά.

```
contract EnergyMarket {
```

Ορισμός του συμβολαίου με τη δήλωση *contract*. Το συμβόλαιο ονομάζεται EnergyMarket.

```
address public owner; // Contract owner
uint256 public energyPrice; // Price per unit of energy in wei (1 Ether = 1e18 wei)
uint256 public totalEnergyProduced; // Total energy produced by all sellers
```

Αυτές οι γραμμές δηλώνουν τις δημόσιες μεταβλητές (public variables) που χρησιμοποιούνται στο συμβόλαιο.

- Η μεταβλητή *owner* είναι η διεύθυνση του ιδιοκτήτη του συμβολαίου.
- Η $energyPrice$ είναι η τρέχουσα τιμή ανά μονάδα ενέργειας σε wei (η μονάδα του Ethereum).
- Η $totalEnergyProduced$ είναι το συνολικό ποσό ενέργειας που έχει παραχθεί από όλους τους πωλητές.

```
struct EnergyOffer {
        address seller;
        uint256 energyAmount;
        uint256 price;
        uint256 startTime;
        uint256 endTime;
        bool isActive;
        bytes32 smartMeterId; // Smart meter identifier
    }
```

Αυτή η δήλωση ορίζει μια δομή (struct) με το όνομα $EnergyOffer$. Μια δομή είναι ένα προσαρμόσιμο δεδομένο που μπορεί να περιλαμβάνει διάφορα στοιχεία. Στην περίπτωση αυτή, η δομή $EnergyOffer$ περιέχει τα παρακάτω στοιχεία για κάθε προσφορά ενέργειας:

- *seller*: Η διεύθυνση του πωλητή.
- $energyAmount$: Η ποσότητα της ενέργειας που προσφέρεται.
- *price*: Η τιμή ανά μονάδα ενέργειας.
- $startTime$: Ο χρόνος έναρξης της προσφοράς.
- $endTime$: Ο χρόνος λήξης της προσφοράς.
- $isActive$: Ένα boolean πεδίο που υποδηλώνει εάν η προσφορά ενέργειας είναι ενεργή ή όχι.
- $smartMeterId$: Αναγνωριστικό του έξυπνου μετρητή που σχετίζεται με αυτήν την προσφορά ενέργειας.

```
    struct EnergyProducedData {
     uint256 energyProduced;
     bytes32 encryptedSmartMeterId; // Encrypted smart meter identifier
}
mapping(address => EnergyProducedData) private energyProducedData;
```

Αυτή είναι μια άλλη δομή με το όνομα $EnergyProducedData$, που περιέχει δύο μέλη δεδομένων:
• $uint256 energyProduced$;: Ένας ακέραιος που χρησιμοποιείται για την αποθήκευση της ποσότητας ενέργειας που παράχθηκε.
• $bytes32 encryptedSmartMeterId$;: Ένας hashed κωδικοποιημένος αριθμός που χρησιμοποιείται για την αποθήκευση του κρυπτογραφημένου αναγνωριστικού του smart meter.

Το $mapping(address => EnergyProducedData) private energyProducedData$;: Δηλώνει ένα mapping με το όνομα $energyProducedData$, όπου κλειδιά είναι διευθύνσεις (address) και οι τιμές είναι δομές τύπου $EnergyProducedData$. Χρησιμοποιείται για να αποθηκεύσει δεδομένα σχετικά με την παραγωγή ενέργειας από κάθε πωλητή.

```
EnergyOffer[] public energyOffers;

mapping(address => uint256) public energyBalances; // Energy balances for each neighbor
mapping(address => bool) public isCertifiedSeller; // Certification status of sellers
mapping(address => bool) public isKYCVerified; // KYC verification status
```

Αυτή η γραμμή δηλώνει έναν δημόσιο πίνακα (array) με στοιχεία τύπου EnergyOffer που θα χρησιμοποιηθεί για την αποθήκευση των προσφορών ενέργειας. Ο πίνακας αυτός θα είναι προσβάσιμος από τον καθένα για ανάγνωση (public).

Αυτές οι γραμμές δηλώνουν τρία δημόσια (public) χαρτοφυλάκια (mappings) που θα χρησιμοποιηθούν για την αποθήκευση δεδομένων:

• Ο $energyBalances$ αντιστοιχεί τις διευθύνσεις των χρηστών στα υπόλοιπά τους ενέργειας.
• Ο $isCertifiedSeller$ αντιστοιχεί τις διευθύνσεις των πωλητών στην κατάσταση πιστοποίησης.
• Ο $isKYCVerified$ αντιστοιχεί τις διευθύνσεις των χρηστών στην κατάσταση επαλήθευσης KYC (γνώρισέ τον πελάτη σου).

```
    function reportEnergyProduced(
    uint256 _energyProduced,
    bytes32 _encryptedSmartMeterId,
    uint8 v,
    bytes32 r,
    bytes32 s
) public {
    require(isCertifiedSeller[msg.sender], "Sender is not a certified smart meter");

    // Verify the signature
```

```
11      bytes32 messageHash = keccak256(abi.encodePacked(msg.sender, _energyProduced, _encryptedSmartMeterId));
12      address recoveredAddress = ecrecover(messageHash, v, r, s);
13      require(recoveredAddress == msg.sender, "Invalid signature");
14
15      // Store encrypted data off-chain
16      energyProducedData[msg.sender] = EnergyProducedData({
17          energyProduced: _energyProduced,
18          encryptedSmartMeterId: _encryptedSmartMeterId
19      });
20
21      // Emit an event without sensitive data
22      emit EnergyProduced(msg.sender);
23  }
24
```

Η συνάρτηση $reportEnergyProduced$ λαμβάνει τα εξής ορίσματα:

- $uint256$ $\_energyProduced$: Η ποσότητα ενέργειας που παράχθηκε.
- $bytes32$ $\_encryptedSmartMeterId$: Το κρυπτογραφημένο αναγνωριστικό του smart meter.
- $uint8 v$: Η v συνιστώσα της υπογραφής.
- $bytes32 r$: Η r συνιστώσα της υπογραφής.
- $bytes32 s$: Η s συνιστώσα της υπογραφής.
- $require(isCertifiedSeller[msg.sender], "Senderisnotacertifiedsmartmeter")$;: Ελέγχει αν ο αποστολέας της συνάρτησης είναι πιστοποιημένος πωλητής. Η πιστοποίηση αυτή πιθανώς να έχει γίνει εκ των προτέρων από κάποιον εξωτερικό μηχανισμό.

Επικύρωση υπογραφής:
- $bytes32 messageHash = keccak256(abi.encodePacked(msg.sender, \_energyProduced, \_encryptedSmartMeterId))$;:
Δημιουργεί ένα μοναδικό $hash$ μηνύματος συνδυάζοντας τη διεύθυνση του αποστολέα, την ποσότητα ενέργειας και το κρυπτογραφημένο αναγνωριστικό του $smartmeter$.

- $address recoveredAddress = ecrecover(messageHash, v, r, s)$;:
Εκτελεί την ανάκτηση της διεύθυνσης που υπογράφει το μήνυμα, χρησιμοποιώντας τις συνιστώσες υπογραφής (v, r, s) και το $hash$ του μηνύματος.

- $require(recoveredAddress == msg.sender, "Invalidsignature")$;:
Επιβεβαιώνει ότι η διεύθυνση που ανακτήθηκε είναι ίδια με τη διεύθυνση του αποστολέα του μηνύματος, διασφαλίζοντας έτσι την έγκυρη υπογραφή.

Αποθήκευση δεδομένων:
- $energyProducedData[msg.sender] = EnergyProducedData(energyProduced: \_energyProduced, encryptedSmartMeterId: \_encryptedSmartMeterId)$;:
Αποθηκεύει τα δεδομένα παραγωγής ενέργειας (ποσότητα και κρυπτογραφημένο αναγνωριστικό) στο $mappingenergyProducedData$, χρησιμοποιώντας τη διεύθυνση του αποστολέα ως κλειδί.

- $emitEnergyProduced(msg.sender)$;:
Εκπέμπει ένα γεγονός ($EnergyProduced$) που μεταδίδει τη διεύθυνση του αποστολέα. Αυτό το γεγονός μπορεί να ακολουθηθεί από άλλες εφαρμογές που παρακολουθούν το συμβόλαιο.

Η συνάρτηση χρησιμοποιείται για την καταχώρηση ποσοτήτων ενέργειας που παράγονται από πιστοποιημένους πωλητές, με υπογραφή για επαλήθευση και ασφαλή αποθήκευση των δεδομένων.

```
function getEnergyProducedData() public view returns (uint256, bytes32) {
       require(isCertifiedSeller[msg.sender], "Sender is not a certified smart meter");

       // Retrieve encrypted data
       EnergyProducedData storage data = energyProducedData[msg.sender];
       return (data.energyProduced, data.encryptedSmartMeterId);
   }
```

Η συνάρτηση $getEnergyProducedData$ είναι δημόσια (public), δεν αλλάζει καταστάσεις (view), και επιστρέφει δύο τιμές: έναν ακέραιο ($uint256$) και ένα $bytes32$.

- $require(isCertifiedSeller[msg.sender], "Senderisnotacertifiedsmartmeter");$
Ελέγχει αν ο αποστολέας της συνάρτησης είναι πιστοποιημένος πωλητής. Αν δεν είναι, η συνάρτηση θα αποτύχει και θα εμφανίσει ένα μήνυμα λάθους.

- $EnergyProducedDatastoragedata = energyProducedData[msg.sender];:$
Δημιουργεί μια αναφορά ($storagereference$) στην αποθηκευμένη δομή $EnergyProducedData$ που αντιστοιχεί στη διεύθυνση του αποστολέα. Η δομή αυτή περιέχει τα δεδομένα παραγωγής ενέργειας για τον συγκεκριμένο πωλητή.

- $return(data.energyProduced, data.encryptedSmartMeterId);:$ Επιστρέφει τις δύο τιμές από τη δομή $EnergyProducedData$. Συγκεκριμένα, επιστρέφει την ποσότητα ενέργειας ($data.energyProduced$) και το κρυπτογραφημένο αναγνωριστικό του $smartmeter(data.encryptedSmartMeterId)$.

Η συνάρτηση αυτή είναι σχεδιασμένη για να επιτρέπει σε πιστοποιημένους πωλητές να ανακτούν τα δεδομένα παραγωγής ενέργειας που έχουν καταχωρηθεί για τον εαυτό τους. Επιστρέφει αυτά τα δεδομένα με τη χρήση μιας αναφοράς στην αποθηκευμένη δομή $EnergyProducedData$.

```
event EnergyProduced(address indexed seller, uint256 energyProduced);
    event EnergyOfferPublished(
        uint256 indexed offerId,
        address indexed seller,
        uint256 energyAmount,
        uint256 price,
        uint256 startTime,
        uint256 endTime,
        bytes32 smartMeterId // Include smart meter ID in the event

    );
    event EnergyPurchased(
        address indexed buyer,
        uint256 indexed offerId,
        uint256 energyAmount,
```

```
16          uint256 totalPrice
17      );
18
```

Αυτές οι γραμμές δηλώνουν τρία δημόσια γεγονότα (events) που θα χρησιμοποιηθούν για να καταγράψουν σημαντικά γεγονότα στο συμβόλαιο. Τα γεγονότα αυτά είναι η παραγωγή ενέργειας, η δημοσίευση προσφοράς ενέργειας και η αγορά ενέργειας αντίστοιχα. Τα events είναι σημαντικά για την παρακολούθηση των δραστηριοτήτων του συμβολαίου από την εξωτερική εφαρμογή.

Αυτό είναι το πρώτο μέρος του συμβολαίου, που περιέχει τις βασικές δηλώσεις, μεταβλητές και δομές. Στη συνέχεια, εξηγούνται οι υπόλοιπες γραμμές του κώδικα.

```
1  constructor(uint256 _initialEnergyPrice) {
2          owner = msg.sender;
3          energyPrice = _initialEnergyPrice;
4      }
```

Αυτή η συνάρτηση είναι ο *constructor* του συμβολαίου και εκτελείται μόλις το συμβόλαιο δημιουργηθεί. Στον *constructor*, ο ιδιοκτήτης του συμβολαίου (*owner*) ορίζεται ως η διεύθυνση του ατόμου που δημιούργησε το συμβόλαιο και η τιμή αρχικής ενέργειας (*energyPrice*) ορίζεται ως *_initialEnergyPrice* που παρέχεται ως όρισμα κατά τη δημιουργία του συμβολαίου.

```
1  modifier onlyOwner() {
2       require(msg.sender == owner, "Only the contract owner can call this function");
3       _;
4   }
```

Είναι ένας ειδικός ελέγχος (modifier) που ελέγχει αν ο καλώντας μιας συνάρτησης είναι ο ιδιοκτήτης του συμβολαίου. Εάν δεν είναι, η εκτέλεση της συνάρτησης δεν θα συνεχιστεί. Αυτό χρησιμοποιείται για να εξασφαλίσει ότι μόνο ο ιδιοκτήτης μπορεί να καλέσει ορισμένες λειτουργίες.

```
1      function setEnergyPrice(uint256 _newPrice) public onlyOwner {
2      energyPrice = _newPrice;
3  }
```

Η συνάρτηση $setEnergyPrice$ μπορεί να κληθεί μόνο από τον ιδιοκτήτη ($onlyOwnermodifier$), επιτρέπει στον ιδιοκτήτη να αλλάξει την τιμή της ενέργειας ($energyPrice$).

```
  function addEnergyProduced(uint256 _energyProduced) public onlyOwner {
    totalEnergyProduced += _energyProduced;
    emit EnergyProduced(msg.sender, _energyProduced);
}
```

Η συνάρτηση $addEnergyProduced$ επιτρέπει στον ιδιοκτήτη να προσθέσει την ποσότητα παραγόμενης ενέργειας ($\_energyProduced$) στο συνολικό ποσό ενέργειας που έχει παραχθεί ($totalEnergyProduced$). Επίσης, αποστέλλει ένα γεγονός ($EnergyProduced$) για να καταγράψει την παραγωγή ενέργειας αυτού του ποσού.

```
     function certifySeller(address _seller) public onlyOwner {
    isCertifiedSeller[_seller] = true;
}
```

Η συνάρτηση $certifySeller$ επιτρέπει στον ιδιοκτήτη να πιστοποιήσει έναν πωλητή ($\_seller$) ως πιστοποιημένο, ορίζοντας την τιμή true στο χαρτοφυλάκιο $isCertifiedSeller$ για αυτόν τον πωλητή. Αυτό σημαίνει ότι ο πωλητής έχει πλέον επισημανθεί ως πιστοποιημένος από τον ιδιοκτήτη του συμβολαίου, ύστερα από την επιτυχή ολοκλήρωση της διαδικασίας Know Your Customer (KYC). Αυτή η πιστοποίηση μπορεί να χρησιμοποιηθεί στο συμβόλαιο για να ελέγχεται η πρόσβαση σε συγκεκριμένες λειτουργίες ή υπηρεσίες, ή για να προβάλλεται η αξιοπιστία του πωλητή στους χρήστες του συμβολαίου.

```
    function verifyKYC(address _user) public onlyOwner {
    isKYCVerified[_user] = true;
}
```

Η συνάρτηση $verifyKYC$ επιτρέπει στον ιδιοκτήτη να επαληθεύσει την ταυτότητα ενός χρήστη ($\_user$) ως επαληθευμένη, ορίζοντας την τιμή $true$ στον χαρτοφυλάκιο $isKYCVerified$ για αυτόν τον χρήστη.

Αυτό είναι το δεύτερο μέρος του συμβολαίου, που περιέχει τις συναρτήσεις που εκτελούν διάφορες λειτουργίες και ελέγχους.

```
    function publishEnergyOffer(
    uint256 _energyAmount,
    uint256 _price,
    uint256 _durationHours,
    bytes32 _smartMeterId // New parameter for smart meter ID
) public {
```

Η συνάρτηση $publishEnergyOffer$ είναι υπεύθυνη για τη δημοσίευση προσφοράς ενέργειας από έναν πωλητή. Λαμβάνει τρία όρισματα: την ποσότητα ενέργειας $\_energyAmount$, την τιμή ανά μονάδα ενέργειας $\_price$, τη διάρκεια σε ώρες $\_durationHour$ και την ταυτοτητα του μετρητή $\_smartMeterId$.

```
require(isCertifiedSeller[msg.sender], "Seller is not certified");
require(isKYCVerified[msg.sender], "Seller is not KYC verified");
require(_energyAmount > 0, "Energy amount must be greater than zero");
require(_price > 0, "Price must be greater than zero");
require(_durationHours > 0, "Duration must be greater than zero");

```

Οι δύο πρώτες γραμμές ελέγχουν αν ο πωλητής που καλεί τη συνάρτηση είναι πιστοποιημένος ($isCertifiedSeller$) και έχει επαληθευτεί μέσω της διαδικασίας $KYC(isKYCVerified)$. Αν αυτοί οι έλεγχοι δεν περάσουν, η συνάρτηση θα αποτύχει και δεν θα δημοσιεύσει την προσφορά ενέργειας. Οι υπόλοιπες γραμμές ελέγχουν ότι οι τιμές των ορισμάτων $\_energyAmount$, $\_price$, και $\_durationHours$ είναι όλες μεγαλύτερες από μηδέν. Αν οποιαδήποτε από αυτές οι συνθήκες δεν ισχύουν, η συνάρτηση θα αποτύχει.

```
uint256 startTime = block.timestamp;
uint256 endTime = startTime + (_durationHours * 1 hours);
```

Αυτές οι γραμμές υπολογίζουν τον χρόνο έναρξης ($startTime$) και τον χρόνο λήξης ($endTime$) της προσφοράς ενέργειας. Ο $block.timestamp$ είναι ο τρέχων χρόνος στο blockchain.

```
    energyOffers.push(
       EnergyOffer({
           seller: msg.sender,
           energyAmount: _energyAmount,
           price: _price,
           startTime: startTime,
           endTime: endTime,
           isActive: true,
           smartMeterId: _smartMeterId // Set the smart meter ID
    })
);
```

Αυτές οι γραμμές προσθέτουν μια νέα προσφορά ενέργειας στον πίνακα $energyOffers$. Η προσφορά αυτή περιέχει τα στοιχεία του πωλητή ($msg.sender$), την ποσότητα ενέργειας ($\_energyAmount$), την τιμή ανά μονάδα ενέργειας ($\_price$), τον χρόνο έναρξης ($startTime$), τον χρόνο λήξης ($endTime$), ένα boolean πεδίο (isActive) που υποδηλώνει ότι η προσφορά είναι ενεργή και τον έξυπνο μετρητή ($\_smartMeterId$).

```
        emit EnergyOfferPublished(
        energyOffers.length - 1,
        msg.sender,
        _energyAmount,
        _price,
        startTime,
        endTime,
        _smartMeterId
    );
}
```

Αυτή η γραμμή εκπέμπει ένα γεγονός ($EnergyOfferPublished$) που δείχνει ότι η προσφορά ενέργειας έχει δημοσιευτεί. Το γεγονός αυτό καταγράφει το μήνυμα αυτό, την ποσότητα ενέργειας, την τιμή, και τους χρόνους έναρξης και λήξης και τον έξυπνο μετρητή.

```
function purchaseEnergy(uint256 _offerId, uint256 _energyAmount) public payable {
require(_offerId < energyOffers.length, "Invalid offer ID");
EnergyOffer storage offer = energyOffers[_offerId];

require(offer.isActive, "The offer is no longer active");
require(_energyAmount > 0, "Energy amount must be greater than zero");
require(block.timestamp >= offer.startTime && block.timestamp <= offer.endTime,
"The offer is not available at the moment");
```

Αυτή η συνάρτηση επιτρέπει σε έναν αγοραστή να αγοράσει ενέργεια από έναν πωλητή. Παίρνει δύο ορίσματα: $\_offerId$, το αναγνωριστικό της προσφοράς ενέργειας που αγοράζεται, και $\_energyAmount$, το ποσό της ενέργειας που αγοράζεται. Πραγματοποιούνται έλεγχοι για να διασφαλίσουν ότι το $\_offerId$ που παρέχει ο αγοραστής είναι έγκυρο και αντιστοιχεί σε μια υπάρχουσα προσφορά ενέργειας στον πίνακα $energyOffers$. Αν το $\_offerId$ δεν είναι έγκυρο, η συνάρτηση αποτυγχάνει. Έπειτα ελέγχει εάν η προσφορά ενέργειας που αγοράζεται είναι ακόμα ενεργή. Εάν η προσφορά δεν είναι πλέον ενεργή, π.χ. αν έχει ήδη αγοραστεί πλήρως ή έχει λήξει, η συνάρτηση αποτυγχάνει και ελέγχει εάν το $\_energyAmount$ που αγοράζεται είναι μεγαλύτερο από το μηδέν. Διασφαλίζει ότι ο αγοραστής προσπαθεί να αγοράσει θετική ποσότητα ενέργειας. Η τελευταία γραμμή ελέγχει ελέγξει αν η τρέχουσα χρονική στιγμή ($timestamp$) του μπλοκ ($block.timestamp$) βρίσκεται μεταξύ του χρόνου έναρξης ($offer.startTime$) και του χρόνου λήξης ($offer.endTime$) της προσφοράς ενέργειας. Αυτό διασφαλίζει ότι η προσφορά είναι διαθέσιμη για αγορά αυτή τη στιγμή.

```
uint256 totalPrice = (offer.price * _energyAmount);
require(msg.value >= totalPrice, "Insufficient funds to purchase energy");
```

Αυτές οι γραμμές υπολογίζουν το συνολικό ποσό ($totalPrice$) της πληρωμής για την ενέργεια που αγοράζεται, βασισμένο στην τιμή της ενέργειας ($offer.price$) και την ποσότητα ενέργειας

που αγοράζεται (*_energyAmount*). Στη συνέχεια, ελέγχει αν το ποσό Ether που αποστέλλεται από τον αγοραστή (*msg.value*) είναι μεγαλύτερο ή ίσο με το συνολικό ποσό πληρωμής. Εάν ο αγοραστής δεν στέλνει αρκετό Ether, η συνάρτηση αποτυγχάνει.

```
energyBalances[msg.sender] += _energyAmount;
energyBalances[offer.seller] -= _energyAmount;
```

Αυτές οι γραμμές ενημερώνουν τα υπόλοιπα ενέργειας του αγοραστή και του πωλητή. Το υπόλοιπο ενέργειας του αγοραστή αυξάνεται κατά το *_energyAmount* μονάδες, ενώ του πωλητή μειώνεται κατά το ίδιο ποσό.

```
// Transfer payment to the seller
    payable(offer.seller).transfer(totalPrice);

    // Deactivate the offer if the energy quantity is fully purchased
    if (_energyAmount == offer.energyAmount) {
        offer.isActive = false;
    }
```

Μεταφέρει το συνολικό ποσό πληρωμής (σε Ether) στη διεύθυνση του πωλητή. Η λέξη-κλειδί *payable* χρησιμοποιείται για να καθορίσει ότι η διεύθυνση του πωλητή μπορεί να λάβει Ether. Η συνθήκη ελέγχει αν ολόκληρη η ποσότητα ενέργειας που προσφέρεται ($offer.energyAmount$) έχει αγοραστεί πλήρως. Αν έχει, η προσφορά σημειώνεται ως ανενεργή (αποκλείοντας περαιτέρω αγορές από αυτήν την προσφορά).

```
emit EnergyPurchased(msg.sender, _offerId, _energyAmount, totalPrice);
    }
```

Αυτή η γραμμή εκπέμπει ένα γεγονός (*EnergyPurchased*) για να καταγράψει την αγορά ενέργειας. Περιλαμβάνει πληροφορίες για τον αγοραστή, το αναγνωριστικό της προσφοράς, το ποσό ενέργειας που αγοράστηκε και το συνολικό ποσό που πληρώθηκε.

```
    function withdrawBalance() public {
        uint256 balance = energyBalances[msg.sender];
        require(balance > 0, "No balance to withdraw");

        energyBalances[msg.sender] = 0;
        payable(msg.sender).transfer(balance);
    }
}
```

Αυτή η συνάρτηση ονομάζεται *withdrawBalance* και είναι δημόσια (*public*), που σημαίνει ότι οποιοσδήποτε μπορεί να την καλέσει. Δηλώνεται μια μεταβλητή με το όνομα *balance* τύπου *uint*256 (ακέραιος). Αυτή η μεταβλητή αντιστοιχεί στο υπόλοιπο ενέργειας του αποστολέα της συναρτήσης, δηλαδή του ατόμου που καλεί τη συνάρτηση. Το υπόλοιπο αυτό προέρχεται από τον πίνακα $energyBalances$ και αντιπροσωπεύει την ποσότητα ενέργειας που το άτομο έχει διαθέσιμη για ανάληψη.
Γίνεται ένας έλεγχος που εξετάζει εάν το υπόλοιπο ενέργειας (*balance*) του αποστολέα είναι μεγαλύτερο από μηδέν. Αν το υπόλοιπο είναι μηδέν, η συνάρτηση θα αποτύχει και δεν θα επιτρέψει την ανάληψη ενέργειας.
Το υπόλοιπο ενέργειας του αποστολέα (*msg.sender*) θέτεται σε μηδέν. Αυτό σημαίνει ότι ο αποστολέας έχει λάβει όλη τη διαθέσιμη ενέργειά του.
Στην τελευταία γραμμή, χρησιμοποιείται η *payable* λέξη-κλειδί για να δηλωθεί ότι η διεύθυνση *msg.sender* είναι δυνατόν να δέχεται Ether. Έπειτα, το υπόλοιπο (*balance*) του αποστολέα μεταφέρεται σε αυτήν τη διεύθυνση με τη χρήση της $transfer(balance)$. Αυτό σημαίνει ότι ο αποστολέας λαμβάνει το υπόλοιπό του σε Ether.

5.5 Δεδομένα και Έξυπνο Συμβόλαιο

Για την καλύτερη κατανόηση του συμβολαίου χρειάζεται να δοθεί έμφαση στο κομμάτι των δεδομένων και στο ρόλο που αυτά έχουν σε ένα έξυπνο συμβόλαιο. Τα δεδομένα είναι ουσιώδη για τη λειτουργία του έξυπνου συμβολαίου, καθώς καθορίζουν τις συνθήκες υπό τις οποίες θα εκτελεστεί το συμβόλαιο και ποιες ενέργειες θα πραγματοποιηθούν. Επίσης, είναι σημαντικό να γίνεται καλή διαχείριση τους για να διασφαλίζεται η ασφάλεια και η αξιοπιστία του συμβολαίου. Σε αυτό το έξυπνο συμβόλαιο οι έξυπνοι μετρητές αλληλεπιδρούν με αυτό. Η συνάρτηση $reportEnergyProduced$ είναι υπεύθυνη για αυτήν την αλληλεπίδραση. Συγκεκριμένα:

Λαμβάνει ως παραμέτρους:
$\_energyProduced$: Η ποσότητα ενέργειας που παράγεται από τον έξυπνο μετρητή.
$\_encryptedSmartMeterId$: Το κρυπτογραφημένο αναγνωριστικό έξυπνου μετρητή. Αυτό παρέχει ένα επίπεδο απορρήτου για την ταυτότητα του έξυπνου μετρητή.

Επαληθεύει την υπογραφή ECDSA:
v, r, s: Αυτές οι παράμετροι χρησιμοποιούνται για την επαλήθευση υπογραφής ECDSA. Ο έξυπνος μετρητής υπογράφει τα δεδομένα (διεύθυνση αποστολέα, παραγόμενη ενέργεια και κρυπτογραφημένο αναγνωριστικό έξυπνου μετρητή) και το συμβόλαιο επαληθεύει την υπογραφή για να διασφαλίσει την αυθεντικότητα των αναφερόμενων δεδομένων.

Βήματα επαλήθευσης:
Ελέγχει εάν ο αποστολέας (*msg.sender*) είναι πιστοποιημένος έξυπνος μετρητής $isCertifiedSeller$. Επαληθεύει την υπογραφή για να διασφαλίσει ότι τα αναφερόμενα δεδομένα δεν έχουν παραβιαστεί και ότι όντως στάλθηκαν από τον ισχυριζόμενο έξυπνο μετρητή.

Αποθήκευση κρυπτογραφημένων δεδομένων:
Η σύμβαση αποθηκεύει τα αναφερόμενα δεδομένα. Αυτό περιλαμβάνει την παραγόμενη ενέργεια ($\_energyProduced$) και το κρυπτογραφημένο αναγνωριστικό έξυπνου μετρητή ($\_encryptedSmartMeterId$). Τα έξυπνα συμβόλαια στο Ετηερευμ αποθηκεύουν δεδομένα στην αλυσίδα (on-chain) χρησιμοποιώντας μεταβλητές κατάστασης. Ωστόσο, το να αποθηκεύουν κρυπτογραφημένα δεδομένα εκτός αλυσίδας, όπως σε κεντρικές βάσεις δεδομένων είναι μια προσέγγιση που έχει συχνά χρησιμοποιηθεί για την προστασία της ιδιωτικότητας των δεδομένων.

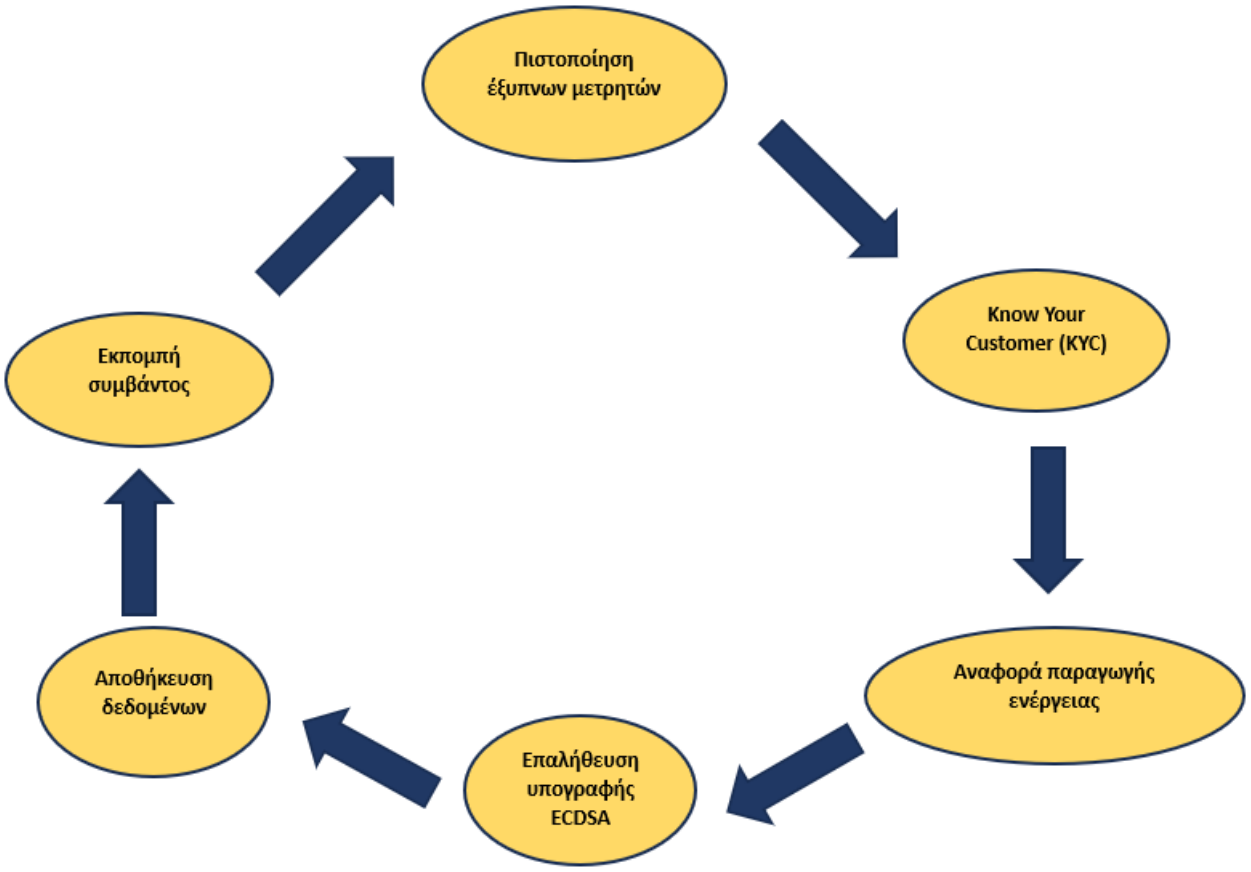
Εκπομπή συμβάντος:
Το συμβάν *energyProduced* εκπέμπεται μετά από επιτυχή επαλήθευση. Αυτό το συμβάν περιλαμβάνει την παράμετρο smartMeter, παρέχοντας μια αναφορά στη διεύθυνση του έξυπνου μετρητή που ανέφερε την παραγωγή ενέργειας.

Συνοπτικά, οι έξυπνοι μετρητές στέλνουν πληροφορίες σχετικά με την ποσότητα ενέργειας που έχουν παραγάγει (*_energyProduced*), την κρυπτογραφημένη ταυτότητά τους (*_encryptedSmartMeterId*) και μια κρυπτογραφική υπογραφή για να επαληθεύσουν την αυθεντικότητα των αναφερόμενων δεδομένων. Στη συνέχεια, αυτές οι πληροφορίες αποθηκεύονται στο έξυπνο συμβόλαιο και εκπέμπεται ένα συμβάν για την καταγραφή της αναφερόμενης παραγωγής ενέργειας.

Ο κύκλος αλληλεπίδρασης μεταξύ των έξυπνων μετρητών και του έξυπνου συμβολαίου ξεκινά με την πιστοποίηση των έξυπνων μετρητών από τον ιδιοκτήτη του συμβολαίου μέσω της λειτουργίας certifySeller, εξακριβώνοντας τη νομιμότητά τους. Στη συνέχεια, οι έξυπνοι μετρητές υποβάλλονται σε επαλήθευση Know Your Customer (KYC) χρησιμοποιώντας τη λειτουργία verifyKYC για να διασφαλιστεί η επικύρωση ταυτότητας χρήστη.

Οι πιστοποιημένοι και επαληθευμένοι έξυπνοι μετρητές KYC αναφέρουν την παραγωγή ενέργειας τους στο έξυπνο συμβόλαιο μέσω της λειτουργίας *reportEnergyProduced*, όπου τα αναφερόμενα δεδομένα, συμπεριλαμβανομένης της ποσότητας ενέργειας και του κρυπτογραφημένου αναγνωριστικού έξυπνου μετρητή, υποβάλλονται σε επαλήθευση υπογραφής ECDSA για επιβεβαίωση της γνησιότητας.

Στη συνέχεια, το έξυπνο συμβόλαιο αποθηκεύει αυτά τα δεδομένα εκτός αλυσίδας και εκπέμπει ένα συμβάν *EnergyProduced*. Αυτός ο κύκλος αλληλεπίδρασης επιτρέπει στους έξυπνους μετρητές να συμμετέχουν στην αποκεντρωμένη αγορά ενέργειας που διευκολύνεται από το έξυπνο συμβόλαιο συμβάλλοντας στις ενεργειακές συναλλαγές.



Εικόνα 13: Κύκλος Αλληλεπίδρασης.

5.6 Συναλλαγές και Έξυπνο συμβόλαιο

Όπως έχει αναφερθεί κάθε block έχει σταθερή χωρητικότητα αποθήκευσης και όταν γεμίσει συνδέεται με το προηγούμενο block της αλυσίδας. Οι νέες πληροφορίες που έρχονται μετά το block που προστέθηκε τελευταία μεταγλωττίζονται σε ένα νέο block και στη συνέχεια προστίθενται στην αλυσίδα, μόλις φτάσει στη μέγιστη χωρητικότητα αποθήκευσης. Το blockchain μοιράζεται μεταξύ των κόμβων του δικτύου υπολογιστών, με κάθε κόμβο να έχει ένα αντίγραφο του blockchain ή των συναλλαγών που γίνονται στο δίκτυο. Μια συναλλαγή αναφέρεται σε μια σύμβαση, συμφωνία, μεταβίβαση ή ανταλλαγή περιουσιακών στοιχείων μεταξύ δύο ή περισσότερων μερών. Το περιουσιακό στοιχείο είναι συνήθως μετρητά ή περιουσία. Ομοίως, μια συναλλαγή blockchain δεν είναι παρά μετάδοση δεδομένων μέσω του δικτύου υπολογιστών σε ένα σύστημα blockchain. Το δίκτυο υπολογιστών σε μια αλυσίδα block αποθηκεύει τα δεδομένα συναλλαγών ως αντίγραφα που καταγράφονται στο ledger.

Οι συναλλαγές είναι υπογεγραμμένα μηνύματα που προέρχονται από έναν εξωτερικό λογαριασμό (EOA-Externally Owned Account), μεταδίδονται από το δίκτυο Ethereum και καταγράφονται

στο blockchain Ethereum. Αυτός ο βασικός ορισμός κρύβει πολλές λεπτομέρειες. Τα συμβόλαια δεν λειτουργούν από μόνα τους. Το Ethereum δεν λειτουργεί αυτόνομα. Όλα ξεκινούν με μια συναλλαγή.

Αρχικά, η βασική δομή μιας συναλλαγής είναι σειριακή και μεταδίδεται στο δίκτυο Ethereum. Κάθε πελάτης και εφαρμογή που λαμβάνει μια σειριακή συναλλαγή θα την αποθηκεύσει στη μνήμη χρησιμοποιώντας τη δική της εσωτερική δομή δεδομένων, ίσως εμπλουτισμένη με μεταδεδομένα που δεν υπάρχουν στην ίδια τη σειριακή συναλλαγή του δικτύου. Μια συναλλαγή είναι ένα σειριακό δυαδικό μήνυμα που περιέχει τα ακόλουθα δεδομένα:

- **Nonce**
  Είναι ένα μοναδικό αναγνωριστικό που προστίθεται σε κάθε συναλλαγή για να διασφαλιστεί ότι μπορεί να υποβληθεί σε επεξεργασία μόνο μία φορά. Ουσιαστικά, μια κλιμακωτή τιμή ίση με τον αριθμό των συναλλαγών που αποστέλλονται από αυτήν τη διεύθυνση ή, στην περίπτωση λογαριασμών με συσχετισμένο κωδικό, με τον αριθμό των συμβάσεων-δημιουργιών που έγιναν από αυτόν τον λογαριασμό. Το nonce είναι ένα χαρακτηριστικό της διεύθυνσης προέλευσης, δηλαδή έχει νόημα μόνο στο πλαίσιο της διεύθυνσης αποστολής. Ωστόσο, δεν αποθηκεύεται ως μέρος της κατάστασης ενός λογαριασμού στο blockchain. Αντίθετα, υπολογίζεται δυναμικά, μετρώντας τον αριθμό των επιβεβαιωμένων συναλλαγών που έχουν προέλθει από μια διεύθυνση.

  Υπάρχουν δύο σενάρια όπου η ύπαρξη του nonce είναι σημαντική: η δυνατότητα οι συναλλαγές να περιλαμβάνονται σύμφωνα με τη σειρά δημιουργίας τους και η προστασία από την αντιγραφή των συναλλαγών. Ας δούμε ένα παράδειγμα για κάθε σενάριο:

  (1) Έστω ότι κάποιος θέλει να κάνει δύο συναλλαγές. Έχει να κάνει μια σημαντική πληρωμή με 6 Ether, καθώς και μια άλλη πληρωμή 8 Ether. Υπογράφει πρώτα τη συναλλαγή 6 Ether, επειδή είναι η πιο σημαντική, και μετά υπογράφει και μεταδίδει τη δεύτερη συναλλαγή με 8 Ether. Δυστυχώς, έχει παραβλέψει το γεγονός ότι ο λογαριασμός του περιέχει μόνο 10 Ether, επομένως το δίκτυο δεν μπορεί να δεχτεί και τις δύο συναλλαγές: μία από αυτές θα αποτύχει. Επειδή έστειλε πρώτα την πιο σημαντική (6 Ether), λογικά περιμένει ότι αυτή θα περάσει και η 8 Ether θα απορριφθεί. Ωστόσο, σε ένα αποκεντρωμένο σύστημα όπως το Ethereum, οι κόμβοι μπορούν να λαμβάνουν τις συναλλαγές με οποιαδήποτε σειρά. Δεν υπάρχει καμία εγγύηση ότι ένας συγκεκριμένος κόμβος θα έχει τη μία συναλλαγή να διαδοθεί σε αυτόν πριν από την άλλη. Ως εκ τούτου, είναι σχεδόν βέβαιο ότι ορισμένοι κόμβοι λαμβάνουν πρώτα τη συναλλαγή 6 Ether και άλλοι λαμβάνουν πρώτα τη συναλλαγή 8 Ether. Χωρίς το nonce, θα ήταν τυχαίο το ποιος γίνεται δεκτός και ποιος απορρίπτεται. Ωστόσο, με το nonce να περιλαμβάνεται, η πρώτη συναλλαγή που έστειλε θα έχει nonce, ας πούμε, 3, ενώ η συναλλαγή με 8 Ether έχει την επόμενη τιμή nonce (δηλαδή 4). Έτσι, αυτή η συναλλαγή θα αγνοηθεί έως ότου υποβληθούν σε επεξεργασία οι συναλλαγές με nonces από το 0 έως το 3, ακόμη και αν ληφθεί πρώτη.

  (2) Έστω ότι κάποιος έχει έναν λογαριασμό με 100 Ether και θέλει να πραγματοποιήσει μια αγορά. Στέλνει 2 Ether στον πωλητή και το αγοράζει. Για να πραγματοποιήσει αυτήν την πληρωμή 2 Ether, υπογράφει μια συναλλαγή που στέλνει 2 Ether από τον λογαριασμό του στον λογαριασμό του πωητή και, στη συνέχεια, τη μεταδίδει στο δίκτυο Ethereum για επαλήθευση και καταγραφή στο blockchain. Τώρα, χωρίς μια τιμή nonce στη συναλλαγή, μια δεύτερη συναλλαγή που στέλνει 2 Ether στην ίδια διεύθυνση για δεύτερη φορά θα μοιάζει ακριβώς με την πρώτη συναλλαγή. Αυτό σημαίνει ότι οποιοσδήποτε βλέπει τη

συναλλαγή σου στο δίκτυο Ethereum (που σημαίνει ότι όλοι, συμπεριλαμβανομένου του παραλήπτη ή των εχθρών του) μπορούν να αναπαράγουν τη συναλλαγή ξανά και ξανά έως ότου εξαφανιστεί όλη η ποσότητα Ether του απλά αντιγράφοντας και επικολλώντας την αρχική σου συναλλαγή και στέλνοντάς την ξανά στο δίκτυο. Μια τέτοια επίθεση ονομάζεται replay attack (επαναληπτική επίθεση) και είναι ένα είδος κακόβουλης επίθεσης, όταν κάποιος κακόβουλος χρήστης επαναλαμβάνει μια ήδη εκτελεσμένη συναλλαγή στο δίκτυο, αξιοποιώντας την ίδια υπογραφή και παραμένοντας έτσι ανεπηρέαστος από τυχόν αλλαγές στις συνθήκες που είχαν αρχικά περικλείσει τη συναλλαγή. Ωστόσο, με την τιμή nonce που περιλαμβάνεται στα δεδομένα συναλλαγής, κάθε μεμονωμένη συναλλαγή είναι μοναδική, ακόμη και όταν αποστέλλεται η ίδια ποσότητα Ether στην ίδια διεύθυνση παραλήπτη πολλές φορές. Έτσι, έχοντας το αυξανόμενο nonce ως μέρος της συναλλαγής, απλά δεν είναι δυνατό για κανέναν να «αντιγράψει» μια πληρωμή που έχει κάνει.

- **Τιμή αερίου**
  Η ποσότητα Ether (σε wei) που είναι διατεθειμένος να πληρώσει ο δημιουργός για κάθε μονάδα αερίου. Το αέριο (gas) είναι το καύσιμο του Ethereum. Το gas δεν είναι Ether—είναι ένα ξεχωριστό εικονικό νόμισμα με τη δική του ισοτιμία έναντι του Ether. Το Ethereum χρησιμοποιεί gas για να ελέγχει την ποσότητα των πόρων που μπορεί να χρησιμοποιήσει μια συναλλαγή, καθώς θα υποβληθεί σε επεξεργασία σε χιλιάδες υπολογιστές σε όλο τον κόσμο.

- **Όριο αερίου**
  Η μέγιστη ποσότητα αερίου που είναι διατεθειμένος να αγοράσει ο εντολέας για αυτήν τη συναλλαγή.

- **Παραλήπτης**
  Η διεύθυνση Ethereum που προορίζεται η συναλλαγή. Οποιαδήποτε τιμή 20 byte θεωρείται έγκυρη. Εάν η τιμή των 20 byte αντιστοιχεί σε μια διεύθυνση χωρίς αντίστοιχο ιδιωτικό κλειδί ή χωρίς αντίστοιχο συμβόλαιο, η συναλλαγή εξακολουθεί να είναι έγκυρη. Το Ethereum δεν έχει κανέναν τρόπο να γνωρίζει εάν μια διεύθυνση προήλθε σωστά από ένα δημόσιο κλειδί (και επομένως από ένα ιδιωτικό κλειδί) που υπάρχει.

- **Τιμή**
  Η ποσότητα του Ether (σε wei) για αποστολή στον παραλήπτη.

- **Δεδομένα**
  Το ωφέλιμο φορτίο δυαδικών δεδομένων μεταβλητού μήκους.

- **v,r,s**
  Τα τρία στοιχεία μιας ψηφιακής υπογραφής ECDSA του αρχικού EOA

Χρησιμοποιώντας αυτές τις τεχνικές, οι προγραμματιστές μπορούν να ασφαλίσουν τις συναλλαγές στη Solidity, παρέχοντας την ασφάλεια και την εμπιστοσύνη που απαιτούνται για τη λειτουργία ψηφιακών συμφωνιών και συναλλαγών σε ένα αποκεντρωμένο δίκτυο blockchain.

Βήματα της Διαδικασίας Συναλλαγών blockchain:

Μια συναλλαγή blockchain πρέπει να υποβληθεί σε πολλά βήματα προτού γίνει μέρος της αλυσίδας block. Παρακάτω επισημαίνονται τα βήματα που περιλαμβάνονται σε μια συναλλαγή blockchain μέσω ενός παραδείγματος:
Ο Μπιλ και η Άλις είναι δύο χρήστες bitcoin . Ο Μπιλ θέλει να στείλει 1 bitcoin στην Άλις.

1. Ο Μπιλ λαμβάνει τη διεύθυνση πορτοφολιού της Άλις (ένα πορτοφόλι στο blockchain είναι ένα ψηφιακό πορτοφόλι που επιτρέπει στους χρήστες να διαχειρίζονται τις συναλλαγές τους). Χρησιμοποιώντας αυτές τις πληροφορίες, δημιουργεί μια νέα συναλλαγή για 1 bitcoin από το πορτοφόλι του και περιλαμβάνει μια προμήθεια συναλλαγής 0,003 bitcoin.
2. Επαληθεύει τις πληροφορίες και στέλνει τη συναλλαγή. Κάθε συναλλαγή που ξεκινά υπογράφεται από μια ψηφιακή υπογραφή του αποστολέα που είναι το ιδιωτικό κλειδί του αποστολέα. Αυτό γίνεται για να είναι πιο ασφαλής η συναλλαγή και να αποτραπεί οποιαδήποτε απάτη.
3. Το πορτοφόλι του Μπιλ ξεκινά τον αλγόριθμο υπογραφής συναλλαγής που υπογράφει τη συναλλαγή του χρησιμοποιώντας το ιδιωτικό του κλειδί.
4. Η συναλλαγή μεταδίδεται τώρα στη δεξαμενή μνήμης (memory pool) εντός του δικτύου.
5. Αυτή η συναλλαγή γίνεται τελικά αποδεκτή από τους miners. Οι εξορύκτες, καταγράφουν αυτήν τη συναλλαγή σε ένα block και εκχωρούν σε αυτό το block μια τιμή κατακερματισμού που θα αντιστοιχιστεί στην αλυσίδα block.
6. Αυτό το block τοποθετείται τώρα στο blockchain.
7. Καθώς αυτό το block επιβεβαιώνεται, γίνεται αποδεκτό ως έγκυρη συναλλαγή στο δίκτυο.
8. Μόλις γίνει αποδεκτή αυτή η συναλλαγή, η Άλις παίρνει τελικά το bitcoin που της έστειλε ο Μπιλ.

Στο έξυπνο συμβόλαιο της παρούσας διπλωματικής, οι έξυπνοι μετρητές συνδέονται με το έξυπνο συμβόλαιο μέσω συναλλαγών Ethereum. Οι συναλλαγές σχετικές με την παραγωγή ενέργειας και την πώλησή της εισέρχονται στο blockchain του Ethereum. Οι συναλλαγές στο Ethereum είναι δημόσιες και αποθηκεύονται στο (ledger) του blockchain. Στο Energy Market, οι εξής συναλλαγές μπορεί να καταγραφούν στο blockchain:

- **Πιστοποίηση Έξυπνων Μετρητών (Smart Meter Certification):**
  Οι συναλλαγές που πιστοποιούν τους έξυπνους μετρητές από τον ιδιοκτήτη του συμβολαίου.
- **Έλεγχος Ταυτότητας (KYC Verification):**
  Οι συναλλαγές που επιβεβαιώνουν την ταυτότητα των χρηστών (έξυπνων μετρητών) μέσω του Know Your Customer (KYC).
- **Αναφορά Παραγωγής Ενέργειας (Energy Production Reporting):** Οι συναλλαγές που αναφέρουν την παραγωγή ενέργειας από τους έξυπνους μετρητές.
- **Δημοσίευση Προσφοράς Ενέργειας (Energy Offer Publication):** Οι συναλλαγές που δημοσιεύουν προσφορές ενέργειας από τους πιστοποιημένους και επαληθευμένους χρήστες.
- **Αγορά Ενέργειας (Energy Purchase):** Οι συναλλαγές που πραγματοποιούνται όταν κάποιος αγοράζει ενέργεια από μια προσφορά, ενεργοποιώντας τη μεταφορά χρημάτων και ενημερώνοντας τους λογαριασμούς ενέργειας.

Ουσιαστικά, όταν κάποιος χρήστης κάνει μια κλήση σε μια συνάρτηση του έξυπνου συμβολαίου, προκειμένου να εκτελέσει μια λειτουργία, αυτή η κλήση καταγράφεται στο blockchain. Για παράδειγμα, όταν ένας έξυπνος μετρητής αναφέρει την παραγωγή ενέργειας στο συμβόλαιο, αυτή η ενέργεια καταγράφεται ως μια συναλλαγή στο Ethereum blockchain. Επίσης, όταν το έξυπνο συμβόλαιο εκπέμπει ένα γεγονός (event), αυτό το γεγονός επίσης καταγράφεται στο blockchain. Για παράδειγμα, όταν δημοσιεύεται μια προσφορά ενέργειας, το γεγονός EnergyOfferPublished καταγράφεται και μπορεί να παρακολουθηθεί από τους χρήστες του συμβολαίου.

Κατά τη διάρκεια αυτών των ενεργειών, που ουσιαστικά είναι συναλλαγές με το συμβόλαιο, εκτελείται κώδικας του συμβολαίου, η κατάσταση του συμβολαίου αλλάζει, και αυτές οι αλλαγές καταγράφονται στο blockchain του Ethereum. Η δημοσίευση συναλλαγών και γεγονότων στο blockchain διασφαλίζει τη διαφάνεια και την αναστολή της δραστηριότητας του συμβολαίου.

Όλες αυτές οι συναλλαγές, μαζί με την κατάσταση του συμβολαίου και τα events που εκπέμπονται, αποθηκεύονται δημόσια στο blockchain του Ethereum. Για επιβεβαίωση οτι μια συναλλαγή έχει πραγματοποιηθεί και έχει καταγραφεί στο blockchain του Ethereum, μπορείτε να χρησιμοποιήσετε blockchain explorers. Οι blockchain explorers είναι διαδικτυακά εργαλεία που επιτρέπουν την παρακολούθηση της κατάστασης του blockchain, την προβολή συναλλαγών και την εξερεύνηση διαφόρων λεπτομερειών. Στην παρούσα διπλωματική έχει χρησιμοποιηθεί ο Etherscan, όπου με την εισαγωγή του hash της εκάστοτε συναλλαγής στη μπάρα αναζήτησης παρουσιάζονται λεπτομέρειες της συναλλαγής.

Οι συμμετέχοντες μπορούν να χρησιμοποιήσουν έναν blockchain explorer, ένα διαδικτυακό εργαλείο για την εξερεύνηση δεδομένων blockchain, για να προβάλουν προσφορές ενέργειας στο έξυπνο συμβόλαιο EnergyMarket. Αναζητώντας τη διεύθυνση έξυπνου συμβολαίου στην αναζήτηση, οι συμμετέχοντες έχουν πρόσβαση σε λεπτομέρειες σχετικά με την κατάσταση του συμβολαίου, συμπεριλαμβανομένης και του $nergyOffers$ που περιέχει πληροφορίες σχετικά με τις ενεργές προσφορές. Μπορούν να ελέγξουν λεπτομέρειες όπως τη διεύθυνση του πωλητή, την ποσότητα ενέργειας, την τιμή, την ώρα έναρξης, την ώρα λήξης και το αναγνωριστικό έξυπνου μετρητή για κάθε ενεργή προσφορά. Επιπλέον, οι συμμετέχοντες μπορούν να εξερευνήσουν το ιστορικό συναλλαγών και τα συμβάντα που εκπέμπονται από τη σύμβαση για να αποκτήσουν πληροφορίες για τις αλληλεπιδράσεις μεταξύ των χρηστών και της σύμβασης, παρέχοντας μια διαφανή και φιλική προς τον χρήστη διεπαφή για την παρακολούθηση των δραστηριοτήτων της αγοράς ενέργειας στο blockchain.

5.6.1 Προστασία δεδομένων στο Energy Market System

Τα έξυπνα συμβόλαια γίνονται όλο και πιο δημοφιλή τα τελευταία χρόνια, παρέχοντας έναν ασφαλή και αποκεντρωμένο τρόπο εκτέλεσης συναλλαγών και συμφωνιών. Η κρυπτογραφία διαδραματίζει κρίσιμο ρόλο στη διασφάλιση της ασφάλειας και του απορρήτου αυτών των συναλλαγών. Η κρυπτογραφία παρέχει την ασφάλεια και το απόρρητο που απαιτούνται για να διασφαλιστεί ότι αυτές οι συμφωνίες και οι συναλλαγές είναι στεγανές και ανθεκτικές σε κακόβουλες επιθέσεις. Η κρυπτογραφία επιτρέπει την ασφαλή επικοινωνία μεταξύ των μερών, διασφαλίζοντας ότι τα δεδομένα και οι πληροφορίες που κοινοποιούνται σε ένα έξυπνο συμβόλαιο προστατεύονται από υποκλοπές.

Στο Energy Market System το απόρρητο διασφαλίζεται με τη χρήση κατακερματισμένων τιμών και μια διαδικασία επαλήθευσης υπογραφής. Συγκεκριμένα, χρησιμοποιεί τη συνάρτηση ecrecover του Ethereum για τον έλεγχο της υπογραφής. Στη Solidity, αυτή η συνάρτηση είναι μια ενσωματωμένη κρυπτογραφική μέθοδος που επιτρέπει την ανάκτηση της διεύθυνσης του υπογράφοντος ενός μηνύματος που έχει υπογραφεί χρησιμοποιώντας το ιδιωτικό του κλειδί. Αυτή η λειτουργία χρησιμοποιείται συχνά σε έξυπνα συμβόλαια Ethereum για την επαλήθευση της αυθεντικότητας των μηνυμάτων χρήστη.

Συγκεκριμένα, η συνάρτηση ecrecover χρησιμοποιείται για την επαναφορά (recovery) της διεύθυνσης (address) που υπογράφει ένα μήνυμα σε συνδυασμό με μια υπογραφή ECDSA (Elliptic Curve Digital Signature Algorithm).
Δέχεται τα εξής ορίσματα:

- $bytes32hash$: Το μήνυμα που υπογράφεται, σε μορφή $bytes32$.
- $uint8v$: Το κομμάτι της υπογραφής που αναπαριστά το $recoveryid$.
- $bytes32r$: Το κομμάτι της υπογραφής που αναπαριστά το r.
- $bytes32s$: Το κομμάτι της υπογραφής που αναπαριστά το s.

Η συνάρτηση επιστρέφει τη διεύθυνση (address) που υπογράφει το μήνυμα. Η υπογραφή ECDSA περιλαμβάνει δύο μέρη, τα r και s, που συνδυάζονται για να δημιουργήσουν την υπογραφή. Το v (recovery id) χρησιμοποιείται για να ανακτηθεί η σωστή διεύθυνση από τον υπογράφων.

Ανάλυση ελέγχου υπογραφής στο συμβόλαιο

1. Συνάρτηση Ελέγχου Υπογραφής:

```
    function reportEnergyProduced(
    uint256 _energyProduced,
    bytes32 _encryptedSmartMeterId,
    uint8 v,
    bytes32 r,
    bytes32 s
) public {
    require(isCertifiedSeller[msg.sender], "Sender is not a certified smart meter");

    // Verify the signature
    bytes32 messageHash = keccak256(abi.encodePacked(msg.sender, _energyProduced, _encryptedSmartMeterId));
    address recoveredAddress = ecrecover(messageHash, v, r, s);
    require(recoveredAddress == msg.sender, "Invalid signature");
    // ...
}
```

2. Υπολογισμός *hash* μηνύματος:

Πριν από το $ecrecover$, το συμβόλαιο υπολογίζει ένα κατακερματισμένο μήνυμα που περιλαμβάνει τη διεύθυνση του αποστολέα ($msg.sender$), την αναφερόμενη παραγωγή ενέργειας ($\_energyProduced$), και τον κατακερματισμένο αναγνωριστικό έξυπνου μετρητή ($\_encryptedSmartMeterId$). Η συνάρτηση $keccak256$ χρησιμοποιείται για τον υπολογισμό του κατακερματισμένου μηνύματος.

3. Συστατικά της Υπογραφής (v, r, s):

Η συνάρτηση περιέχει τρεις επιπλέον παραμέτρους v, r, s. Αυτά τα στοιχεία αποτελούν την κρυπτογραφική υπογραφή.

4. Σύγκριση Διευθύνσεων:

Η ανακτημένη διεύθυνση ($recoveredAddress$) συγκρίνεται στη συνέχεια με τη διεύθυνση του αποστολέα ($msg.sender$) για να διασφαλιστεί ότι η υπογραφή είναι έγκυρη και αντιστοιχεί στον αναμενόμενο υπογράφοντα. Εάν η σύγκριση αποτύχει, η συνάρτηση εμφανίζει ένα σφάλμα που δηλώνει 'Άκυρη υπογραφή' και η συναλλαγή ανατρέπεται.

5. Επαλήθευση υπογραφής:
Αυτή η διαδικασία διασφαλίζει ότι η παραγώμενη ενέργεια και το αναγνωριστικό έξυπνου μετρητή συσχετίζονται νόμιμα με τη διεύθυνση που πραγματοποίησε τη συναλλαγή. Αποτρέπει κακόβουλους παράγοντες από την υποβολή ψευδών ή παραποιημένων δεδομένων στη σύμβαση. Η επαλήθευση της υπογραφής είναι ιδιαίτερα σημαντική στο πλαίσιο της αναφοράς παραγωγώμενης ενέργειας, όπου μόνο οι πιστοποιημένοι έξυπνοι μετρητές επιτρέπεται να υποβάλλουν δεδομένα.

5.7 Ψηφιακές υπογραφές

Ο αλγόριθμος ψηφιακής υπογραφής που χρησιμοποιείται στο Ethereum είναι ο αλγόριθμος ψηφιακής υπογραφής Elliptic Curve (ECDSA). Βασίζεται σε ζεύγη ιδιωτικών-δημόσιων κλειδιών ελλειπτικής καμπύλης. Μια ψηφιακή υπογραφή εξυπηρετεί τρεις σκοπούς στο Ethereum: πρώτον, η υπογραφή αποδεικνύει ότι ο κάτοχος του ιδιωτικού κλειδιού, ο οποίος είναι έμμεσα ο κάτοχος ενός λογαριασμού Ethereum, έχει εξουσιοδοτήσει τη δαπάνη Ether ή την εκτέλεση ενός συμβολαίου, δεύτερον, εγγυάται τη μη απόρριψη: η απόδειξη της εξουσιοδότησης είναι αδιαμφισβήτητη και τρίτον, η υπογραφή αποδεικνύει ότι τα δεδομένα συναλλαγής δεν τροποποιήθηκαν και δεν μπορούν να τροποποιηθούν από κανέναν μετά την υπογραφή της συναλλαγής.

Ορισμός ψηφιακής υπογραφής:
Είναι ένα μαθηματικό σχήμα για την παρουσίαση της αυθεντικότητας ψηφιακών μηνυμάτων ή εγγράφων. Μια έγκυρη ψηφιακή υπογραφή δίνει στον παραλήπτη λόγο να πιστεύει ότι το μήνυμα δημιουργήθηκε από γνωστό αποστολέα (έλεγχος ταυτότητας), ότι ο αποστολέας δεν μπορεί να αρνηθεί ότι έστειλε το μήνυμα (μη απόρριψη) και ότι το μήνυμα δεν άλλαξε κατά τη μεταφορά (ακεραιότητα).

Έννοια ψηφιακής υπογραφής:
Οι ψηφιακές υπογραφές είναι συνώνυμες με τις παραδοσιακές υπογραφές. Είναι απλώς ένας τρόπος εξουσιοδότησης μιας συναλλαγής ή ενός μηνύματος στο διαδίκτυο. Κάθε υπογεγραμμένη συναλλαγή περιέχει μια ψηφιακή υπογραφή και η υπογραφή αποτελεί απόδειξη της εγκυρότητας αυτού του μηνύματος.

Οι ψηφιακές υπογραφές είναι πολύ σημαντικές επειδή παρέχουν μια απόδειξη του λογαριασμού από τον οποίο προέρχεται μια συναλλαγή και ο υπογράφων μιας τέτοιας συναλλαγής δεν μπορεί να αρνηθεί ότι η υπογραφή προήλθε από τον λογαριασμό του. Οι ψηφιακές υπογραφές παρέχουν επίσης απόδειξη ότι το περιεχόμενο ενός μηνύματος ή συναλλαγής δεν έχει παραβιαστεί, επειδή οποιαδήποτε αλλαγή στο περιεχόμενο του μηνύματος θα παράγει μια υπογραφή εντελώς διαφορετική από την αρχική.

Δημιουργία ψηφιακών υπογραφών:
Οι ψηφιακές υπογραφές δημιουργούνται από τον αλγόριθμο ψηφιακής υπογραφής ελλειπτικής καμπύλης (ECDSA) και αυτός ο αλγόριθμος αποτελείται από δύο μέρη. Το πρώτο μέρος είναι ο αλγόριθμος δημιουργίας υπογραφών, ενώ το δεύτερο μέρος είναι ο αλγόριθμος επαλήθευσης υπογραφής.

Οι ψηφιακές υπογραφές δημιουργούνται όταν ένα ιδιωτικό κλειδί υπογράφει μια συναλλαγή. Στην πραγματικότητα, η συναλλαγή εδώ είναι ο κατακερματισμός Keccak256 του κωδικοποιημένου μηνύματος. Η μαθηματική συνάρτηση για την υπογραφή συναλλαγής είναι:

S i g = Fsig(Fkeccak256(m), k), όπου: k = το ιδιωτικό κλειδί υπογραφής

m= το κωδικοποιημένο μήνυμα RLP

Fkeccak256 = Συνάρτηση κατακερματισμού Keccak256

Fsig = ο αλγόριθμος υπογραφής

Sig = η υπογραφή που προκύπτει

Η συνάρτηση $Fsig$ παράγει μια υπογραφή (Sig)rs, : S i g = r, s.

Μια λεπτομερή και χρήσιμη εξήγηση είναι η εξής:
«Ο αλγόριθμος υπογραφής ECDSA λαμβάνει ως είσοδο ένα μήνυμα msg+ ένα ιδιωτικό κλειδί privKey **** και παράγει ως έξοδο μια υπογραφή , η οποία αποτελείται από ένα ζεύγος ακεραίων αριθμών {r, s}. Η υπογραφή που υπολογίσθηκε {r, s} είναι ένα ζεύγος ακεραίων, ο καθένας στην περιοχή $[1 \dots n-1]$. Κωδικοποιεί το τυχαίο σημείο R, μαζί με μια απόδειξη s, επιβεβαιώνοντας ότι ο υπογράφων γνωρίζει το μήνυμα h και το ιδιωτικό κλειδί privKey. Η απόδειξη είναι εξ αρχής επαληθεύσιμη χρησιμοποιώντας το αντίστοιχο pubKey.»

Επαλήθευση υπογραφών:
Ο αλγόριθμος επαλήθευσης μιας υπογραφής ECDSA λαμβάνει ως είσοδο το υπογεγραμμένο μήνυμα msg, την υπογραφή $\{r, s\}$ που παράγεται από τον αλγόριθμο υπογραφής, και το δημόσιο κλειδί pubKey που αντιστοιχεί στο ιδιωτικό κλειδί του υπογράφοντος. Η έξοδος είναι μια λογική τιμή: έγκυρη ή μη έγκυρη υπογραφή. Ο αλγόριθμος επαλήθευσης υπογραφής ECDSA λειτουργεί ως εξής (με μικρές απλοποιήσεις):

1. Υπολογισμός του $hash$ του μηνύματος, με την ίδια κρυπτογραφική συνάρτηση $hash$ που χρησιμοποιήθηκε κατά την υπογραφή: $h = hash(msg)$.

2. Υπολογισμός του αντίστροφου του υπογραφικού αποδεικτικού: $s_1 = s^{-1} \bmod n$.

3. Επαναφορά του τυχαίου σημείου που χρησιμοποιήθηκε κατά την υπογραφή:
$R' = (hs_1)G + (rs_1)pubKey$.

4. Εξαγωγή της x-συντεταγμένης του R' : $r' = R'x$.

5. Υπολογισμός του αποτελέσματος επαλήθευσης της υπογραφής συγκρίνοντας εάν $r' == r$

Η γενική ιδέα της επαλήθευσης της υπογραφής είναι να ανακτηθεί το σημείο R' χρησιμοποιώντας το δημόσιο κλειδί και να ελεγχθεί εάν είναι το ίδιο σημείο R που δημιουργήθηκε τυχαία κατά τη διαδικασία υπογραφής.

Ουσιαστικά, η υπογραφή ECDSA {r, s} έχει την ακόλουθη απλή εξήγηση:

- Η υπογραφή κωδικοποιεί ένα τυχαίο σημείο R (αναπαριστώμενο από την x-συντεταγμένη του μόνο) μέσω μετασχηματισμών στην ελλειπτική καμπύλη χρησιμοποιώντας το ιδιωτικό κλειδί privKey και το κατακερματισμένο μήνυμα h σε έναν αριθμό s. Αυτός ο αριθμός s αποτελεί την απόδειξη ότι ο υπογράφων του μηνύματος γνωρίζει το ιδιωτικό κλειδί privKey. Η υπογραφή {r, s} δεν μπορεί να αποκαλύψει το ιδιωτικό κλειδί.
- Η επαλήθευση της υπογραφής αποκωδικοποιεί τον αριθμό απόδειξης s από την υπογραφή πίσω στο αρχικό του σημείο R, χρησιμοποιώντας το δημόσιο κλειδί pubKey και το κατακερματισμένο μήνυμα h, και συγκρίνει την x-συντεταγμένη του ανακατακερματισμένου R με την τιμή r από την υπογραφή.

Ο αλγόριθμος υπογραφής αρχικά δημιουργεί ένα προσωρινό ιδιωτικό κλειδί με κρυπτογραφικά ασφαλή τρόπο. Αυτό το προσωρινό κλειδί χρησιμοποιείται για τον υπολογισμό των τιμών r και s για να διασφαλιστεί ότι το πραγματικό ιδιωτικό κλειδί του αποστολέα δεν μπορεί να υπολογιστεί από εισβολείς που παρακολουθούν υπογεγραμμένες συναλλαγές στο δίκτυο Ethereum.

Το προσωρινό ιδιωτικό κλειδί χρησιμοποιείται για την παραγωγή του αντίστοιχου (προσωρινού) δημόσιου κλειδιού, οπότε έχουμε:

- Ένας κρυπτογραφικά ασφαλής τυχαίος αριθμός q , ο οποίος χρησιμοποιείται ως το προσωρινό ιδιωτικό κλειδί.
- Το αντίστοιχο προσωρινό δημόσιο κλειδί Q, που δημιουργήθηκε από το q και το σημείο γεννήτριας ελλειπτικής καμπύλης G.

Η τιμή r της ψηφιακής υπογραφής είναι τότε η συντεταγμένη x του προσωρινού δημόσιου κλειδιού Q. Από εκεί, ο αλγόριθμος υπολογίζει την τιμή s της υπογραφής, έτσι ώστε:

$$s = q - 1(Keccak256(m) + rk)(\mathrm{mod} p), \text{που:}$$

- Το q είναι το προσωρινό ιδιωτικό κλειδί.
- Το r είναι η συντεταγμένη x του προσωρινού δημόσιου κλειδιού.
- Το k είναι το ιδιωτικό κλειδί υπογραφής (κατόχου EOA).
- Το m είναι τα δεδομένα συναλλαγής.
- Το p είναι η τάξη της ελλειπτικής καμπύλης.

Η επαλήθευση είναι το αντίστροφο της συνάρτησης δημιουργίας υπογραφής, χρησιμοποιώντας τις τιμές r και s και το δημόσιο κλειδί του αποστολέα για τον υπολογισμό μιας τιμής Q , η οποία

είναι ένα σημείο στην ελλειπτική καμπύλη (το προσωρινό δημόσιο κλειδί που χρησιμοποιείται στη δημιουργία υπογραφής).

Τα βήματα είναι τα εξής:
1. Έλεγχος ότι όλες οι είσοδοι έχουν διαμορφωθεί σωστά

2. Υπολογισμός του $w = s^{-1} \bmod p$

3. Υπολογισμός του $u1 = Keccak256(m)w \bmod p$

4. Υπολογίσμός του $u2 = rw \bmod p$

5. Τέλος, υπολογισμός του σημείου στην ελλειπτική καμπύλη $Q = u1G + u2K \bmod p$ που:

- r και s είναι οι τιμές υπογραφής.
- k είναι το δημόσιο κλειδί του υπογράφοντος (κατόχου EOA).
- m είναι τα δεδομένα συναλλαγής που υπογράφηκαν.
- G είναι σημείο της ελλειπτικής καμπύλης.
- p είναι η τάξη της ελλειπτικής καμπύλης.

Εάν η συντεταγμένη x του υπολογιζόμενου σημείου Q είναι ίση με r, τότε ο επαληθευτής μπορεί να συμπεράνει ότι η υπογραφή είναι έγκυρη. Κατά την επαλήθευση της υπογραφής, το ιδιωτικό κλειδί δεν είναι ούτε γνωστό ούτε αποκαλύπτεται.

Τι γίνεται με το v:

Όπως έχει ήδη εξηγηθεί, στη δημιουργία δημόσιου κλειδιού με χρήση κρυπτογραφίας ελλειπτικής καμπύλης, δημιουργούνται δύο πιθανά δημόσια κλειδιά σε κάθε περίπτωση. Αυτό συμβαίνει επειδή ο αλγόριθμος της ελλειπτικής καμπύλης έχει συμμετρία κατά μήκος του άξονα x, έτσι για οποιαδήποτε τιμή του x που παράγεται, υπάρχουν δύο πιθανές τιμές που ταιριάζουν στην καμπύλη, ένα σε κάθε πλευρά του άξονα x. Το ερώτημα τώρα είναι, πώς αυτός ο αλγόριθμος επιλέγει τη σωστή τιμή του x για να ενωθεί με την τιμή y. Εδώ μπαίνει το v.

Η υπογραφή συναλλαγής περιλαμβάνει μια τιμή προθέματος v, η οποία μας λέει ποια από τις δύο πιθανές τιμές R είναι το προσωρινό δημόσιο κλειδί. Το v προστίθεται στη συνάρτηση επαλήθευσης υπογραφής για να βοηθήσει στον εντοπισμό της σωστής τιμής του r μεταξύ των δύο πιθανών παραγόμενων τιμών R και R'. Αν το v είναι άρτιο, το R είναι η σωστή τιμή, αν το v είναι περιττό, τότε το R'.

Επομένως, η ψηφιακή υπογραφή είναι ένας αποτελεσματικός τρόπος όχι μόνο για την παρακολούθηση της προέλευσης των συναλλαγών, αλλά και για να διασφαλιστεί ότι οι συναλλαγές δεν διακυβεύονται μετά την υπογραφή και τη μετάδοσή τους. [23], [24], [25]

Στο κεφάλαιο 2.7 της παρούσας Διπλωματικής έχει γίνει και επιπλέον επεξήγηση των ψηφιακών υπογραφών.

5.8 Ανάπτυξη του Energy Market System

Το παραπάνω έξυπνο συμβόλαιο γράφτηκε στη γλώσσα προγραμματισμού Solidity, η οποία είναι η δημοφιλέστερη και η πιο ευρέως χρησιμοποιούμενη γλώσσα για smart contracts. Είναι αντικειμενοστραφής, με τα συμβόλαια να ορίζονται ως αντικείμενα, και υψηλού επιπέδου γλώσσα. Τέλος, είναι πολύ σημαντικό η υλοποίηση να γίνει όσο πιο αποδοτικά και ποιοτικά γίνεται για να μειωθεί όσο περισσότερο γίνεται το κόστος.

Κάθε "deployment" στο blockchain, καθώς και κάθε κλήση συνάρτησης κοστίζει "gas fees" στο δίκτυο του Ethereum. Για το λόγο αυτό, κρίνεται απαραίτητο η υλοποίηση να γίνει με τέτοιο τρόπο ώστε το κόστος να ελαχιστοποιείται.

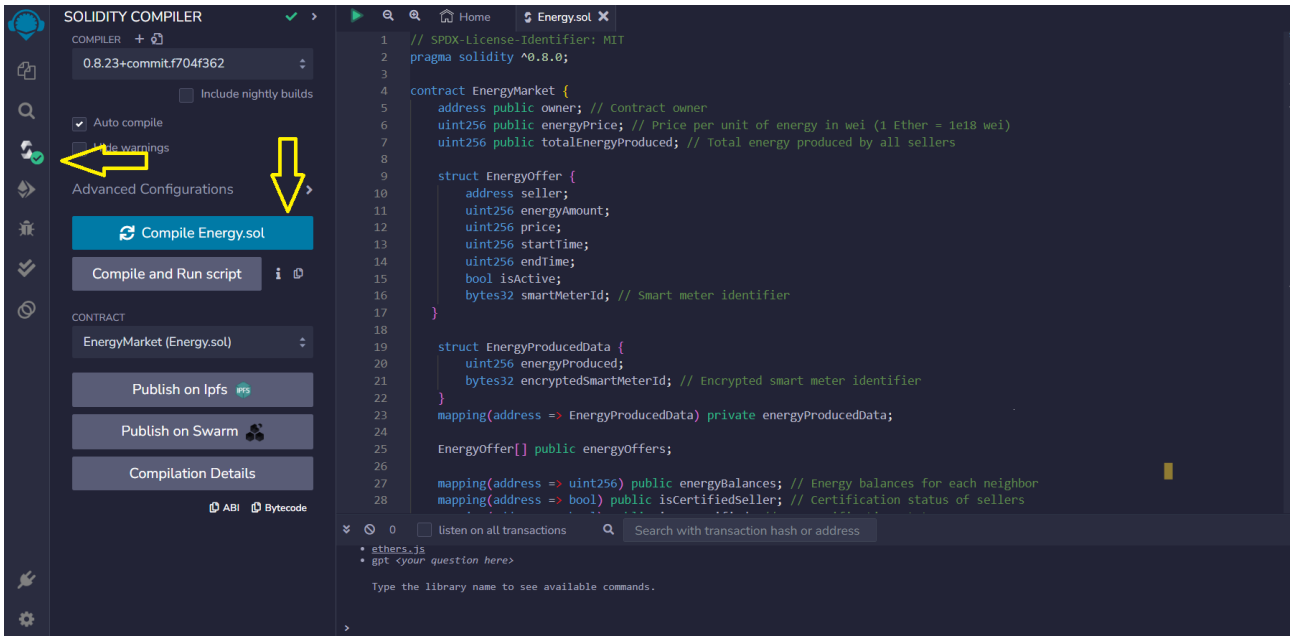
Ο παραπάνω κώδικας γράφτηκε στο Remix. Μέσω του Remix έγινε και η μεταγλώττιση του συμβολαίου.

Το Remix IDE είναι ένα ολοκληρωμένο περιβάλλον ανάπτυξης ανοιχτού κώδικα (IDE) ειδικά σχεδιασμένο για προγραμματισμό, δοκιμή και ανάπτυξη έξυπνων συμβολαίων στο blockchain Ethereum και στα διάφορα δοκιμαστικά δίκτυά του. Είναι ένα δημοφιλές εργαλείο μεταξύ των προγραμματιστών του web 3, ιδιαίτερα εκείνων που εργάζονται με το Ethereum, καθώς προσφέρει ένα φιλικό προς τον χρήστη και πλούσιο σε δυνατότητες περιβάλλον για τη σύνταξη και τη διαχείριση έξυπνων συμβολαίων. Το Remix IDE προσφέρει ένα πρόγραμμα συγγραφής και επεξεργασίας κώδικα (code editor) με δυνατότητες επισήμανσης σύνταξης και αυτόματης συμπλήρωσης για τη σύνταξη έξυπνων συμβολαίων στο Ethereum.

Συνοδεύεται επίσης, από έναν ενσωματωμένο μεταγλωττιστή Solidity που επιτρέπει στους προγραμματιστές να μεταγλωττίζουν τα έξυπνα συμβόλαιά τους απευθείας μέσα στο IDE. Επιπρόσθετα, παρέχει λεπτομερή μηνύματα σφάλματος και προειδοποιήσεις για να βοηθήσει τους προγραμματιστές να εντοπίσουν και να διορθώσουν προβλήματα στον κώδικά τους. Ένα πολύ σημαντικό χαρακτηριστικό του είναι ότι προσφέρει ανάλυση στατικού κώδικα για τον εντοπισμό πιθανών τρωτών σημείων ή κινδύνων ασφαλείας. Το εργαλείο συνοδεύεται και από ένα ενσωματωμένο πρόγραμμα εντοπισμού σφαλμάτων (debugger) που επιτρέπει στους προγραμματιστές να επιθεωρήσουν τον κώδικα, τις μεταβλητές και να κατανοήσουν πώς συμπεριφέρεται το συμβόλαιο κατά την εκτέλεση.

Μία ακόμα εξαιρετική διευκόλυνση είναι ότι οι προγραμματιστές μπορούν να γράφουν και να εκτελούν τεστ για τα έξυπνα συμβόλαιά τους απευθείας μέσα στο Remix. Για την συγγραφή των τεστ υποστηρίζει JavaScript και Solidity. Είναι κρίσιμο να επισημανθεί ότι το Remix προσφέρει και εργαλεία για την δημοσίευση (deployment) έξυπνων συμβολαίων στα διάφορα δίκτυα του Ethereum, συμπεριλαμβανομένων του mainnet και των δοκιμαστικών δικτύων. Υποστηρίζει επίσης ενσωμάτωση με δημοφιλείς εφαρμογές πορτοφολιού Ethereum όπως το MetaMask για τη διαχείριση λογαριασμών και συναλλαγών. Τέλος, για ακόμα μεγαλύτερη ευκολία, το IDE είναι διαθέσιμο από browser, οπότε δεν είναι αναγκαία η εγκατάσταση κάποιου λογισμικού. [26]

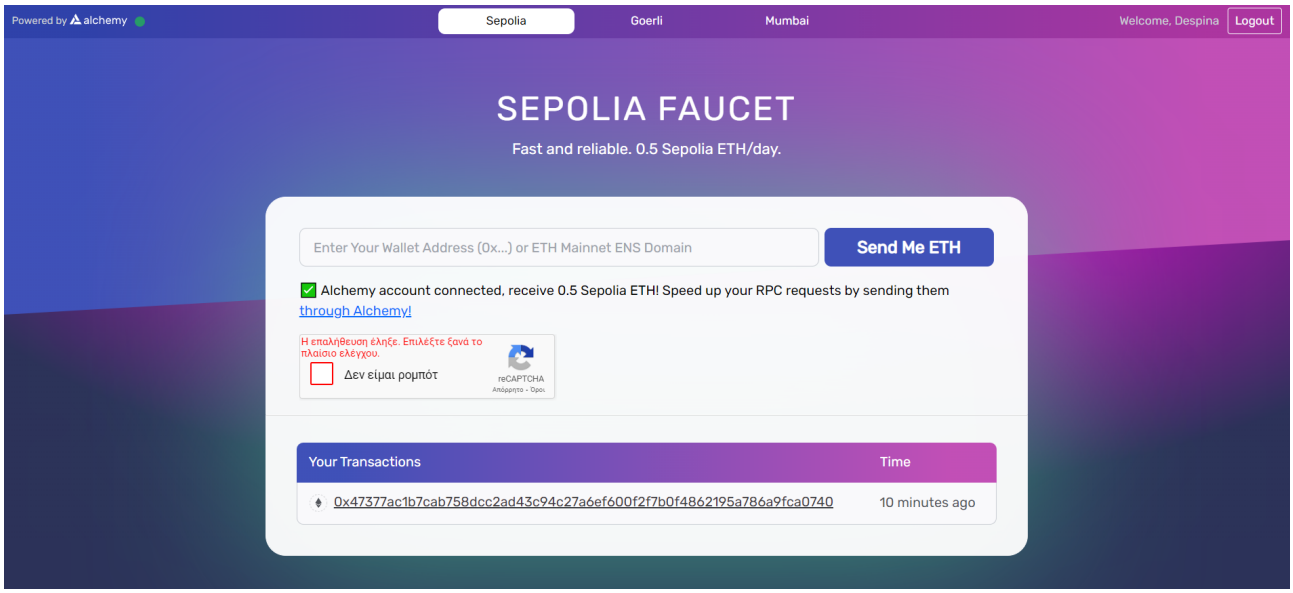
Ουσιαστικά, από το ίδιο το Remix IDE μπορεί να γίνει και το "deployment" στο δίκτυο του Ethereum αρκεί ο χρήστης και σύντομα ιδιοκτήτης του συμβολαίου να έχει δημιουργήσει πορτοφόλι κρυπτονομισμάτων στο Metamask και να διαθέτει επαρκή κρυπτονομίσματα να καλύψει το τέλος συναλλαγής.



Εικόνα 14: Μεταγλώτισση Συμβολαίου μέσω Remix IDE (Compile Energy.sol).

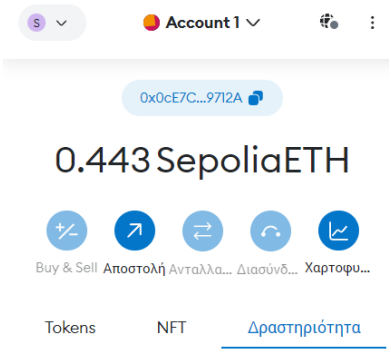
Το Metamask δεν είναι η μοναδική και κατ' επέκταση ούτε η υποχρεωτική επιλογή πορτοφολιού. Είναι, ωστόσο, πολύ βολικό και φιλικό πορτοφόλι κρυπτονομισμάτων που ικανοποιεί πλήρως τις όποιες ανάγκες του συστήματος. Στα πλεονεκτήματα του συγκαταλέγονται μεταξύ άλλων η εύκολη πρόσβαση και σύνδεση σε αποκεντρωμένες εφαρμογές, η ευρεία υιοθέτηση του από την κοινότητα του Ethereum (που συνεπάγεται εύκολη επιλογή σύνδεσης σε πιθανές front-end υλοποιήσεις), το λιτό και συγχρόνως πλήρες UI (User Interface) και η δυνατότητα αλληλεπίδρασης με το δίκτυο του Ethereum χωρίς την ανάγκη εκτέλεσης πλήρες κόμβου στον υπολογιστή του χρήστη. Πέρα από την προφανή απώλεια κεφαλαίου που θα υποστεί ο χρήστης σε περίπτωση μη διαφύλαξης της φράσης και μη δυνατότητας επαναφοράς του πορτοφολιού, θα χάσει και την πρόσβαση του ως ιδιοκτήτη στο συμβόλαιο που έχει δημιουργήσει.

Εφόσον, ο χρήστης έχει δημιουργήσει ένα πορτοφόλι θα πρέπει να προμηθευτεί δοκιμαστικά Ether από κατάλληλη παροχή (Ethereum faucet). Εδώ έγινε χρήση του GOERLI FAUCET.



Εικόνα 15: Ethereum faucet.

Και έτσι, αφού επιλεγεί το δίτυο «Sepolia» στο Metamask,το πορτοφόλι δεν είναι πλέον άδειο, έχει Ether.



Εικόνα 16: Ether στο πορτοφόλι.

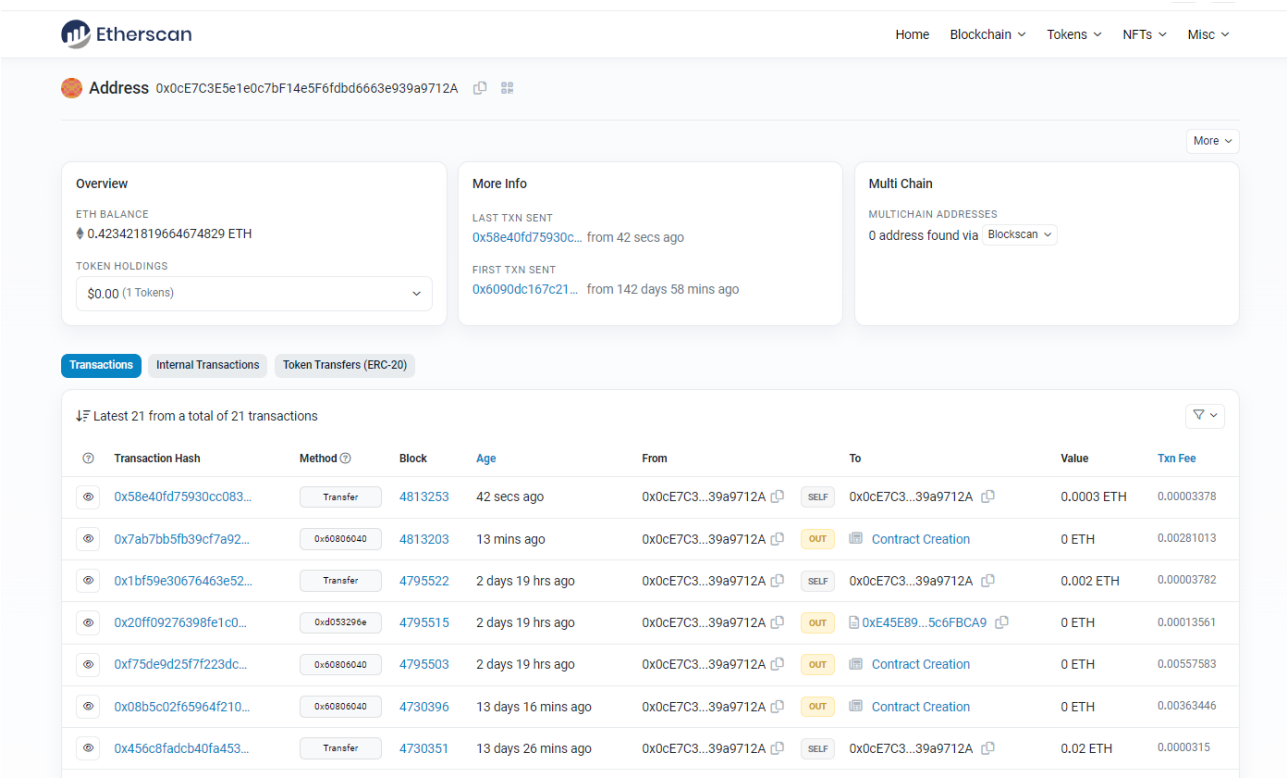
Ως ιδιοκτήτες του συμβολαίου, έχουμε πλέον το μοναδικό δεκαεξαδικό (hex) αναγνωριστικό του συμβολαίου (0x0cE7C3E5e1e0c7bF14e5F6fdbd6663e939a9712A) και συνεχίζουμε επιβεβαιώνοντας τον πηγαίο κώδικα στο Etherscan και συγκεκριμένα στο Etherscan Sepolia.

Αν δεν γίνει επιβεβαίωση του πηγαίου κώδικα καθίσταται αδύνατη η αλληλεπίδραση με το συμβόλαιο μέσω του Etherscan. Άπαξ και γίνει επιβεβαίωση του πηγαίου κώδικα, ταυτόχρονα

αυτός γίνεται δημόσιος και μπορεί να μελετηθεί από όλους τους χρήστες του δικτύου. Ουσιαστικά, ο πηγαίος κώδικας ελέγχεται για να διαπιστωθεί ότι είναι γνήσιος και δεν έχει αλλοιωθεί από κακόβουλους τρίτους και ότι συμμορφώνεται με τις προδιαγραφές και τις απαιτήσεις που έχουν θέσει οι προγραμματιστές και οι χρήστες. Μετά την επιβεβαίωση, ο πηγαίος κώδικας δημοσιοποιείται, δηλαδή γίνεται προσβάσιμος σε όλους τους ενδιαφερόμενους μέσω διαφόρων μέσων, όπως το GitHub ή το Etherscan. Αυτό δίνει τη δυνατότητα σε κάθε χρήστη να ελέγξει τον κώδικα και να εξασφαλίσει ότι είναι ασφαλής και αξιόπιστος.

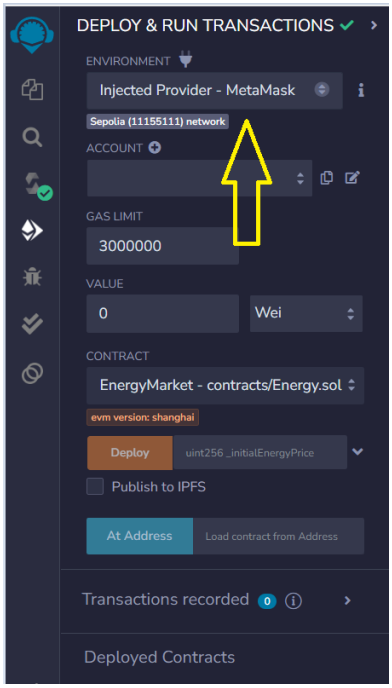
Άπαξ και καταχωρηθεί το έξυπνο συμβόλαιο στο δίκτυο του Ethereum, μπορούμε να αλληλεπιδράσουμε μαζί του τόσο εμείς όσο και οποιοσδήποτε άλλος (εξ' ου και το νόημα του αποκεντρωμένου συστήματος) και να παρατηρήσουμε όλες τις συναλλαγές που σχετίζονται με αυτό με χρήση του Etherscan. Το Etherscan (χωρίς πάλι να αποτελεί υποχρεωτική επιλογή) είναι ένας βολικός εξερευνητής (Blockchain Explorer) του δικτύου του Ethereum που καταγράφει όλες τις συναλλαγές που πραγματοποιούνται στο δίκτυο. Επιτρέπει επίσης με βολικό τρόπο την σύνδεση σε Dapps μέσω του πορτοφολιού Metamask και την αλληλεπίδραση με έξυπνα συμβόλαια.

Το Etherscan είναι μια ευρέως χρησιμοποιούμενη πλατφόρμα εξερεύνησης και ανάλυσης για το blockchain Ethereum. Είναι ένας «block explorer» γιατί όπως λέει και το όνομά του μας φανερώνει τα δεδομένα που υπάρχουν στα blocks του Ethereum blockchain. Παρέχει στους χρήστες ένα ευρύ φάσμα εργαλείων και λειτουργιών για την εξερεύνηση, την παρακολούθηση και την ανάλυση συναλλαγών Ethereum, έξυπνων συμβολαίων, διευθύνσεων κλπ. Το Etherscan χρησιμεύει για τους προγραμματιστές όσο και για τους λάτρεις του Ethereum και τους επενδυτές, προσφέροντας πληροφορίες για τις δραστηριότητες και τα δεδομένα του δικτύου.



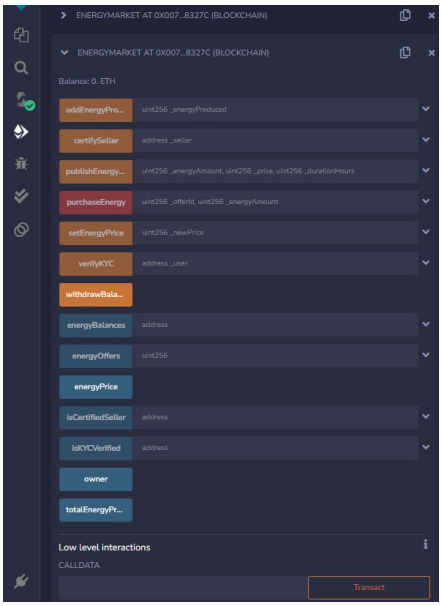
Εικόνα 17: Επιβεβαίωση του πηγαίου κώδικα.

Επίσης, θα πρέπει να γίνει αλλαγή στο ENVIRONMENT και να επιλεγεί Injected Provider MetaMask για να συνδέσει το Remix ID με το πορτοφόλι MetaMask.



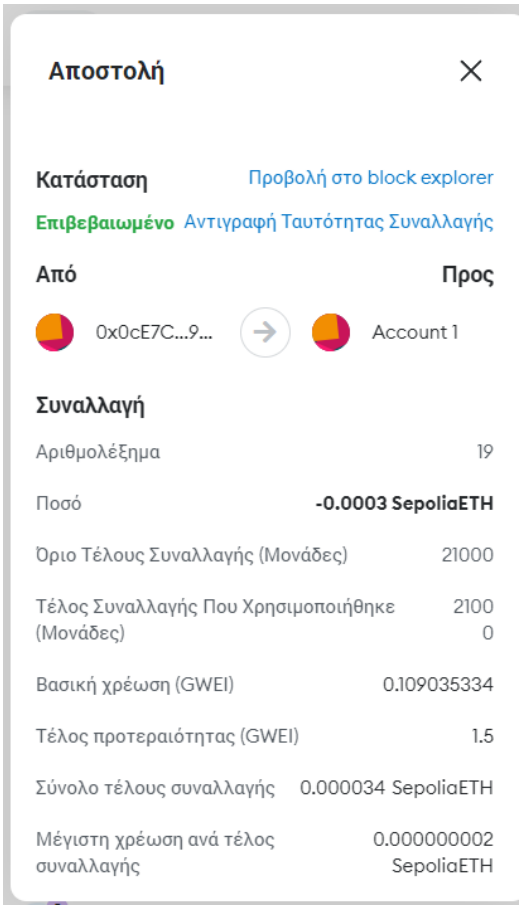
Εικόνα 18: Αλλαγή στο ENVIRONMENT.

Άρα με τον ενσωματωμένο μεταγλωττιστή γίνεται compile στον κώδικα. Στη συνέχεια deployment στο συμβόλαιο σε ένα ειδικό blockchain για τεστάρισμα που δημιουργεί τοπικά το remix και παρουσιάζει ίδια συμπεριφορά με τα αληθινά. Τέλος, οι συναρτήσεις μπορούν να τρέξουν με διάφορα δεδομένα και να ελεγχθεί αν η συμπεριφορά τους ήταν η επιθυμητή.



Εικόνα 19: Deployment.

Έτσι, πραγματοποείται το deployment του συμβολαίου και διάφορες συναλλαγές. Ενδεικτικά μια συναλλαγή:



Εικόνα 20: Παράδειγμα συναλλαγής.

Κάθε συναλλαγή που πραγματοποιείται καταγράφεται στο blockchain και μπορεί να αναζητηθεί μέσω του Etherscan.

Διευκρίνιση: Αν το έξυπνο συμβόλαιο έχει ήδη δημιουργηθεί και είναι σε λειτουργία στο blockchain Ethereum, τότε ένας πιθανός αγοραστής μπορεί να αγοράσει ενέργεια χρησιμοποιώντας κάποιο εργαλείο που επικοινωνεί με το συμβόλαιο. Θα μπορούσε να χρησιμοποιήσει ένα blockchain explorer όπως το Etherscan για να παρακολουθήσει τις συναλλαγές και την κατάσταση του συμβολαίου. Ωστόσο, το Etherscan δεν παρέχει τη δυνατότητα εκτέλεσης συναλλαγών. Για να αγοράσει ενέργεια, θα πρέπει να χρησιμοποιήσει ένα

Ethereum wallet, όπως το MetaMask, για να εκτελέσει τη συνάρτηση purchaseEnergy του έξυπνου συμβολαίου. Μπορεί να χρησιμοποιήσει το Remix για να συνδεθεί με το wallet του και να εκτελέσει τη συναλλαγή. Κατά την εκτέλεση, θα πρέπει να παρέχει τα απαραίτητα ορίσματα όπως το ID της προσφοράς ενέργειας και την επιθυμητή ποσότητα ενέργειας. Συνοψίζοντας, θα χρησιμοποιήσει ένα Ethereum wallet για να αλληλεπιδράσει με το έξυπνο συμβόλαιο μέσω του Remix ή άλλου εργαλείου που υποστηρίζει την εκτέλεση συναλλαγών. [27], [28]

6 Συμπεράσματα, τρόποι επέκτασης και εφαρμογές

6.1 Ανακεφαλαίωση

Σκοπός της διπλωματικής εργασίας ήταν να εξετάσει την εφαρμογή της τεχνολογίας Blockchain και των έξυπνων συμβολαίων στον τομέα των ευφυών ηλεκτρικών δικτύων. Αρχικά, παρουσιάστηκε η τεχνολογία του Blockchain και οι βασικές της λειτουργίες. Στη συνέχεια, εξετάζονται τα έξυπνα συμβόλαια και ο ρόλος τους στο περιβάλλον του Blockchain. Έπειτα, αναλύονται τα ευφυή ηλεκτρικά δίκτυα και η δυνατότητα ενσωμάτωσης της τεχνολογίας Blockchain στη λειτουργία τους. Τέλος, παρουσιάζεται η δημιουργία του «Energy Market System» συμβολαίου για την αγοραπωλησία ενέργειας σε ένα έξυπνο ηλεκτρικό δίκτυο. Αναλύονται οι λειτουργίες και οι προκλήσεις που αντιμετωπίζονται, καθώς και οι πλεονεκτήματα που προκύπτουν από την εφαρμογή του συμβολαίου.

6.2 Εφαρμογή του συμβολαίου σε ρεαλιστικά σενάρια

Υπάρχουν διάφορα ρεαλιστικά σενάρια εφαρμογής του συμβολαίου σε πραγματικό περιβάλλον. Ανάμεσά τους η αυτόματη διαχείριση ενέργειας. Μπορεί να χρησιμοποιηθεί για τη διαχείριση και την αυτόματη εκτέλεση συμφωνιών μεταξύ παραγωγών ενέργειας (όπως ηλιακά φωτοβολταϊκά ή αιολικά πάρκα) και εταιρειών διανομής ενέργειας. Ακόμα, μπορεί να χρησιμοποιηθεί για τη διαχείριση του φορτίου ενέργειας, με την αυτόματη προμήθεια ενέργειας ανάλογα με τη ζήτηση και τις συνθήκες προσφοράς ή στη διαχείριση αυτόνομων συστημάτων παραγωγής και αποθήκευσης ενέργειας, όπως τα οικιακά ηλιακά πάνελ.

6.3 Τρόποι επέκτασης του συμβολαίου

Οι τρόποι επέκτασης του συμβολαίου μπορούν να προσφέρουν ευελιξία και να προσαρμόζουν τη λειτουργία του σε νέες ανάγκες και συνθήκες. Μερικοί τρόποι επέκτασης περιλαμβάνουν την προσθήκη νέων λειτουργιών που να ανταποκρίνονται σε επιπλέον ανάγκες, τη βελτίωση απόδοσης και ασφάλειας ή ακόμα και τη διερεύνηση του πεδίου εφαρμογής του συμβολαίου για να καλύψει νέες κατηγορίες χρηστών ή να υποστηρίξει νέους τύπους συναλλαγών.

Σαν μελλοντική δουλειά μπορούμε να εξετάσουμε την ενσωμάτωση ειδικών υπογραφών που παρέχουν αυξημένη ανωνυμία. [30], [31]

Στην κατεύθυνση αυτή παρουσιάζουν ιδιαίτερο ενδιαφέρον και οι τεχνικές αέναης ανωνυμίας που έχουν αναπτυχθεί στο πλαίσιο συστημάτων e-voting.[32], [33], [34]

7 Βιβλιογραφία

[1] Zheng, Zibin Xie, Shaoan Dai, Hong-Ning Chen, Xiangping Wang, Huaimin. (2017). *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.*

[2] Geeksforgeeks, (11 May, 2022). *Difference Between Blockchain and a Database.*: `https://www.geeksforgeeks.org/difference-between-blockchain-and-a-database/`

[3] Aamna Tariq, Hina Binte Haq, Syed Taha Ali, (14 December, 2019). *Cerberus: A Blockchain-Based Accreditation and Degree Verification System.*: `https://arxiv.org/pdf/1912.06812.pdf`

[4] Akshara Srivastava, (August 25, 2021). *What Should a Startup Choose Between Blockchain and a Traditional Database?.*: `https://hashstudioz.com/blog/what-should-a-startup-choose-between-blockchain-and-a-traditional-database/`

[5] The Byzantine Generals Problem. *LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE.*

[6] Satoshi Nakamoto *Bitcoin: A Peer-to-Peer Electronic Cash System.*

[7] Sriman, B. Kumar, s Prabakaran, Shamili. (2020). *Blockchain Technology: Consensus Protocol Proof of Work and Proof of Stake.*

[8] Macharia, Wahome. (2021). *Cryptographic Hash Functions.*

[9] Matt Rickard,(Mar 27, 2022). *Elliptic Curve Cryptography.*: `https://matt-rickard.com/elliptic-curve-cryptography`

[10] Verma, Sharad Ojha, Badri. (2012). *A Discussion on Elliptic Curve Cryptography and Its Applications. International Journal of Computer Science Issues.*

[11] Gaid, Michael Salloum, Said. (2021). *Homomorphic Encryption.*

[12] Huang, Qichen. (2023). *Ethereum: Introduction, Expectation, and Implementation. Highlights in Science, Engineering and Technology.*

[13] THE INVESTOPEDIA TEAM,(Mar 15, 2024). *What Is Sharding? Purpose, How It Works, Security, and Benefits.*: `https://www.investopedia.com/terms/s/sharding.asp`

[14] Mohanta, Bhabendu Panda, Soumyashree Jena, Debasish. (2018). *An Overview of Smart Contract and Use Cases in Blockchain Technology.*

[15] *Smart Contract Use Cases.*: `https://hedera.com/learning/smart-contracts/smart-contract-use-cases`

[16] Desen Kirli, Benoit Couraud, Valentin Robu, Marcelo Salgado-Bravo, Sonam Norbu, Merlinda Andoni, Ioannis Antonopoulos, Matias Negrete-Pincetic, David Flynn, Aristides Kiprakis, (April, 2022). *Renewable and Sustainable Energy Reviews - Smart contracts in energy systems: A systematic review of fundamental approaches and implementations.*

[17] Dmitry Baimel, Saad Tapuchi, Nina Baimel, (August 2, 2016) *Smart Grid Communication Technologies.*: `https://file.scirp.org/Html/1-1770243_69361.htm`

[18] *Distribution Intelligence in Smart Grids.*:
https://www.smartgrid.gov/the_smart_grid/distribution_intelligence.html

[19] Geeksforgeeks, (07 Oct, 2022). *Smart Contracts and IoT.*:
https://www.geeksforgeeks.org/smart-contracts-and-iot/

[20] Journal of Physics: Conference Series, (2021). *Energy Storage Technology Used in Smart Grid.*:
https://iopscience.iop.org/article/10.1088/1742-6596/2083/3/032067/pdf

[21] *Compressed Air Energy Storage (CAES).*:
https://www.ctc-n.org/technologies/compressed-air-energy-storage-caes

[22] *Smart Versus Traditional: The Low Down on Energy Meters.*:
https://www.exceptional.com/homes/home-improvement/
smart-versus-traditional-the-low-down-on-energy-meters/

[23] Okoli Evans, (Jun 11, 2023). *Understanding Digital Signatures: The Role of V, R, S in Cryptographic Security and Signature.*: https://coinsbench.com/
understanding-digital-signatures-the-role-of-v-r-s-in-cryptographic-security-and-/
signature-b9d2b89bbc0c

[24] *Digital Signatures in Cryptography: ECDSA Sign and Verify Messages.*:
https://cryptobook.nakov.com/digital-signatures/ecdsa-sign-verify-messages

[25] *Digital Signatures in Ethereum.*: https://github.com/ethereumbook/ethereumbook/
blob/develop/06transactions.asciidoc#digital-signatures

[26] Brady Werkheiser, (2022). *Overview of Rinkeby Testnet.*:
https://www.alchemy.com/overviews/rinkeby-testnet

[27] Author Name, *What is Blockchain Transaction?.*:
https://www.upgrad.com/blog/what-is-blockchain-transaction/

[28] Pavan Vadapalli. *Blockchain Transaction Life Cycle.*:
https://www.geeksforgeeks.org/blockchain-transaction-life-cycle/

[29] Efstathios Zachos, Aristidis Pagourtzis, Panagiotis Grontas, (2015). *Computational Cryptography.*: https://repository.kallipos.gr/handle/11419/5439?locale=el

[30] Pourandokht Behrouz, Panagiotis Grontas, Vangelis Konstantakatos, Aris Pagourtzis, and Marianna Spyrakou, *Designated-Verifier Linkable Ring Signatures*, 24th International Conference on Information Security and Cryptology - ICISC 2021, LNCS, vol. 13218, pp. 51–70, 2022. https://doi.org/10.1007/978-3-031-08896-4_3.

[31] Danai Balla, Pourandokht Behrouz, Panagiotis Grontas, Aris Pagourtzis, Marianna Spyrakou, and Giannis Vrettos, *Designated-Verifier Linkable Ring Signatures with Unconditional Anonymity*, 9th International Conference on Algebraic Informatics, CAI 2022, LNCS, vol. 13706, pp. 55–68, 2022. https://doi.org/10.1007/978-3-031-19685-0_5.

[32] Panagiotis Grontas, Aris Pagourtzis, and Alexandros Zacharakis, *Coercion Resistance in a Practical Secret Voting Scheme for Large Scale Elections*, ISPAN-FCST-ISCC 2017, Exeter, United Kingdom, June 21-23, 2017, pp. 514–519, IEEE Computer Society, 2017. https://doi.org/10.1109/ISPAN-FCST-ISCC.2017.79.

[33] Panagiotis Grontas, Aris Pagourtzis, Alexandros Zacharakis, and Bingsheng Zhang, *Towards Everlasting Privacy and Efficient Coercion Resistance in Remote Electronic Voting*, Financial Cryptography and Data Security - FC 2018 International Workshops, BITCOIN, VOTING, and WTSC, Revised Selected Papers, LNCS, vol. 10958, pp. 210–231, Springer, 2018. https://doi.org/10.1007/978-3-662-58820-8_15.

[34] Panagiotis Grontas and Aris Pagourtzis, *Anonymity and Everlasting Privacy in Electronic Voting*, International Journal of Information Security, vol. 22, no. 4, pp. 819–832, 2023. https://doi.org/10.1007/S10207-023-00666-2.