ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ
ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Ανάπτυξη έξυπνου συμβολαίου για την υποστήριξη συμπεριφορικής εξοικονόμησης ενέργειας μέσω ψηφιακών ενεργειακών νομισμάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Άρης Πρεβέντης

Επιβλέπων : Χρυσόστομος (Χάρης) Δούκας

Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2023

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ
ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Ανάπτυξη έξυπνου συμβολαίου για την υποστήριξη συμπεριφορικής εξοικονόμησης ενέργειας μέσω ψηφιακών ενεργειακών νομισμάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Άρης Πρεβέντης

Επιβλέπων : Χρυσόστομος (Χάρης) Δούκας

Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 12η Ιουλίου 2023.

.....	.....	.....
Χρυσόστομος Δούκας	Ιωάννης Ψαρράς	Δημήτριος Ασκούνης
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2023

.....

Άρης Πρεβέντης

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Ο μετριασμός της κλιματικής αλλαγής θεωρείται υψηλή προτεραιότητα διεθνώς και τοποθετείται στην κορυφή της ατζέντας για τους περισσότερους φορείς χάραξης πολιτικής και υπεύθυνους λήψης αποφάσεων. Για την επίτευξη αυτού του στόχου δεν αρκεί μόνο η μετάβαση σε ανανεώσιμες πηγές ενέργειας, αλλά είναι επίσης απαραίτητη μια στροφή προς την ενεργειακά αποδοτικότερη συμπεριφορά των καταναλωτών.

Η τεχνολογία blockchain, που χαρακτηρίζεται από τον αποκεντρωμένο και διαφανή χαρακτήρα της, προσφέρει μια πολλά υποσχόμενη προσέγγιση για την αντιμετώπιση των προκλήσεων που θέτονται. Παρέχοντας μια ασφαλή και αμετάβλητη πλατφόρμα για την καταγραφή και την επαλήθευση των συναλλαγών, το blockchain καθίσταται ιδανική υποδομή για την ανάπτυξη ψηφιακών ενεργειακών νομισμάτων τα οποία μπορούν να χρησιμοποιηθούν από τις τοπικές αρχές ή τους παρόχους ενέργειας για την παροχή χρηματικών κινήτρων στους χρήστες που επιτυγχάνουν καλύτερη ενεργειακή αποδοτικότητα. Επιπρόσθετα, μέσω της καινοτόμας τεχνολογίας των έξυπνων συμβολαίων, τα οποία είναι αυτόματα εκτελούμενα κομμάτια κώδικα με καθορισμένους εκ των προτέρων όρους και κανόνες, γίνεται δυνατή η ενσωμάτωση των απαραίτητων αυτών κανόνων και περιορισμών για την εύρυθμη λειτουργία του συστήματος των ενεργειακών νομισμάτων.

Ο στόχος της παρούσας διπλωματικής εργασίας είναι να διερευνήσει τις δυνατότητες και τις προκλήσεις που περιβάλλουν την ενσωμάτωση της τεχνολογίας blockchain, των έξυπνων συμβολαίων και των ψηφιακών νομισμάτων στη σφαίρα της εξοικονόμησης ενέργειας και της αποδοτικότητας. Για τον σκοπό αυτό αναπτύσσεται και παρουσιάζεται, ένα καινοτόμο πλαίσιο, που αποτελείται από ένα σύνολο αποκεντρωμένων εφαρμογών, που συνδέει τα ψηφιακά ενεργειακά νομίσματα με την εξοικονόμηση ενέργειας και σχετικά προγράμματα επιβράβευσης, και το οποίο ενθαρρύνει τους καταναλωτές να συμμετάσχουν σε δράσεις εξοικονόμησης ενέργειας ανταμείβοντάς τους οικονομικά με ενεργειακά νομίσματα για την εξοικονομούμενη ενέργεια που επιτυγχάνουν. Το πλαίσιο εφαρμογών πλαισιώνεται από ένα ιδιωτικό blockchain τεχνολογίας Ethereum, από τη διεπαφή χρήστη της εφαρμογής και από ένα βοηθητικό κεντρικό server.

Στο πλαίσιο της εργασίας αναλύθηκαν διεξοδικά οι έννοιες και οι λειτουργίες του Blockchain, των αλγορίθμων συναίνεσης και των έξυπνων συμβολάιων καθώς και οι δυσκολίες και περιορισμοί που συναντήθηκαν κατά τη δημιουργία της εφαρμογής.

Λέξεις Κλειδιά: Blockchain, Ethereum, Έξυπνα Συμβόλαια, Ψηφιακά Ενεργειακά Νομίσματα, Ενεργειακή Αποδοτικότητα, Ιδιωτικό Δίκτυο Blockchain, Αποκεντρωμένη Εφαρμογή

Abstract

Climate change mitigation is considered a high priority internationally and is placed at the top of the agenda for most policymakers and decision makers. To achieve this goal, it is not just enough to switch to renewable energy sources, but a shift towards more energy efficient consumer behavior is also necessary.

Blockchain technology, characterized by its decentralized and transparent nature, offers a promising approach to address the challenges posed. By providing a secure and immutable platform for recording and verifying transactions, blockchain becomes an ideal infrastructure for the development of digital energy currencies that can be used by local authorities or energy providers to provide monetary incentives to users who achieve better energy efficiency. In addition, through the innovative technology of smart contracts, which are automatically executed pieces of code with predefined terms and rules that are determined in advance, it becomes possible to incorporate the necessary rules and restrictions for the smooth functioning of the energy currency system.

The aim of this thesis is to explore the possibilities and challenges surrounding the integration of blockchain technology, smart contracts and digital currencies in the sphere of energy conservation and efficiency. For this purpose, it develops and presents an innovative framework based on a set of decentralized applications that connects digital energy coins with energy saving and the corresponding reward programs, which encourages consumers to participate in energy saving actions by rewarding them with energy coins for the saved energy they achieve. The decentralized framework of applications is framed by a private Ethereum blockchain, the user interface of the application and an auxiliary central server.

In the framework of the work, the concepts and functions of Blockchain, consensus algorithms and smart contracts as well as the difficulties and limitations encountered during the creation of the application were thoroughly analyzed.

Keywords: Blockchain, Ethereum, Smart Contracts, Digital Energy Currencies, Energy Efficiency, Private Blockchain Network, Decentralized Application

Ευχαριστίες

Η παρούσα διπλωματική εκπονήθηκε κατά το ακαδημαϊκό έτος 2022-2023 στον Τομέα Ηλεκτρικών Βιομηχανικών Διατάξεων και Συστημάτων Αποφάσεων στα πλαίσια των ερευνητικών δραστηριοτήτων του Εργαστηρίου Συστημάτων Αποφάσεων και Διοίκησης της σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου.

Με την ευκαιρία της ολοκλήρωσης της διπλωματικής μου εργασίας, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στον επιβλέποντα της, Αναπληρωτή Καθηγητή κ. Χάρη Δούκα για την ανάθεση ενός τόσο ενδιαφέροντος θέματος και για δυνατότητα που μου παρείχε να εργαστώ ερευνητικά στον τομέα του Blockchain.

Θα ήθελα επίσης να ευχαριστήσω τον κ. Κωνσταντίνο Κοασίδη, για το συνεχές του ενδιαφέρον, την καθοδήγηση, τις χρήσιμες συμβουλές και τις διορατικές παρατηρήσεις, την ενθάρρυνση και την υπομονή του σε όλα τα στάδια της εργασίας.

Τέλος, θα ήθελα να εκφράσω την ευγνωμοσύνη μου προς την οικογένεια μου που μου έδειξε άνευ όρων υποστήριξη κατά τη διάρκεια των σπουδών μου.

Πίνακας Περιεχομένων

Ευρετήριο Εικόνων

Ευρετήριο Πινάκων

Κεφάλαιο 1 Εισαγωγή

1.1 Αντικείμενο - Σκοπός

Η κλιματική αλλαγή είναι μια από τις πιο σύνθετες προκλήσεις που αντιμετωπίζει η ανθρωπότητα σήμερα. Η διαρκώς αυξανόμενη εκπομπή αερίων του θερμοκηπίου, κυρίως λόγω της κατανάλωσης ορυκτών καυσίμων, απειλεί να μετατρέψει αμετάκλητα το παγκόσμιο κλίμα με σοβαρές επιπτώσεις για τον ανθρώπινο πολιτισμό και τα φυσικά οικοσυστήματα [1].

Μια από τις προτεραιότητες στην πάλη κατά της κλιματικής αλλαγής είναι η μείωση της ενεργειακής κατανάλωσης και η προώθηση της ενεργειακής αποδοτικότητας. Εκτός από τις συμβατικές παρεμβάσεις, οι οποίες κυριαρχούν στις δράσεις μετριασμού από την πλευρά της ζήτησης, η αλλαγή συμπεριφοράς αποτελεί βασική πτυχή της ενεργειακής απόδοσης, καθώς οι αλλαγές στα πρότυπα κατανάλωσης μπορούν να οδηγήσουν σε ευρύτερες αλλαγές στον τρόπο ζωής και τις συνήθειες των τελικών χρηστών [2]. Προηγούμενες έρευνες έχουν υπογραμμίσει ότι ένα νοικοκυριό θα μπορούσε να εξοικονομήσει έως και το 20% της συνολικής του ενεργειακής κατανάλωσης αλλάζοντας τις καθημερινές συνήθειες των μελών του [3].

Ωστόσο, η προώθηση της ενεργειακής αποδοτικότητας απαιτεί περισσότερο από την απλή ενημέρωση των καταναλωτών. Απαιτείται η ανάπτυξη καινοτόμων λύσεων που θα παρέχουν κίνητρα για την ενεργειακή αποδοτικότητα και θα διευκολύνουν την παρακολούθηση και την ανταλλαγή ενεργειακών δεδομένων.

Η τεχνολογία του blockchain προσφέρει μια υποσχόμενη προοπτική σε αυτό το πεδίο. Μέσω της ασφάλειας, της διαφάνειας και της αποκεντρωμένης φύσης του blockchain, μπορούμε να δημιουργήσουμε πλατφόρμες που ενθαρρύνουν την ενεργειακή αποδοτικότητα μέσω της δημιουργίας ψηφιακών ενεργειακών νομισμάτων. Η χρήση της ενέργειας ως νομισματική μονάδα μέσα σε ένα πλαίσιο κινητροδότησης των καταναλωτών που βασίζεται στην έννοια των ενεργειακών νομισμάτων μπορεί να επιτύχει σημαντική μείωση της ενεργειακής κατανάλωσης μιας κοινότητας [4].

Σε αυτή τη διπλωματική εργασία, θα διερευνήσουμε τη χρήση της τεχνολογίας του blockchain για την προώθηση της ενεργειακής αποδοτικότητας. Θα αναπτύξουμε μια αποκεντρωμένη εφαρμογή με χρήση τεχνολογιών της οικογένειας του Ethereum που θα διασυνδέσει το blockchain με την ατομική ενεργειακή αποδοτικότητα, μέσω ενός ψηφιακού ενεργειακού νομίσματος που θα επιβραβεύει τους χρήστες, όταν αυτοί γίνονται περισσότερο ενεργειακά αποδοτικοί και καταναλώνουν μικρότερες ποσότητες ενέργειας.

Στόχος είναι η προτεινόμενη εφαρμογή να συμβάλει στην πάλη κατά της κλιματικής αλλαγής περιορίζοντας την σπατάλη ενέργειας στις επιμέρους κοινότητες, ώστε να επιτευχθεί μια συνολικότερη μείωση του ενεργειακού αποτυπώματος συνολικά.

1.2 Οργάνωση τόμου

Η εργασία αποτελείται από 6 κεφάλαια.

Το παρόν Κεφάλαιο 1 αποτελεί εισαγωγικό κομμάτι. Γίνεται μία εισαγωγή ως προς το πρόβλημα της κλιματικής αλλαγής και την κατεύθυνση που η εργασία προτείνει για τον περιορισμό της.

Στο Κεφάλαιο 2 γίνεται μία αναλυτικότερη παρουσίαση της τεχνολογίας του Blockchain με μία εμβάθυνση στις τεχνολογίες του Ethereum Blockchain που αποτελεί και το περιβάλλον πάνω στο οποίο αναπτύχθηκε η αποκεντρωμένη εφαρμογή. Γίνεται επίσης μία ανασκόπηση των ενεργειακών εφαρμογών στο Blockchain.

Το Κεφάλαιο 3 εισάγει το Atomcoin, την ιδέα πίσω από το ενεργειακό ψηφιακό νόμισμα που υλοποιήθηκε και περιγράφονται οι προδιαγραφές του. Επίσης γίνεται μία περιγραφή της αρχιτεκτονικής του συστήματος που σχεδιάστηκε με κέντρο την αποκεντρωμένη εφαρμογή του ψηφιακού νομίσματος.

Στο Κεφάλαιο 4 αναλύεται η διαδικασία που ακολουθήθηκε για την ανάπτυξη του συστήματος. Δίνεται μία περιγραφή των τεχνολογιών που χρησιμοποιήθηκαν και γίνεται μία ανάλυση της επιχειρηματικής λογικής του συστήματος και των επιμέρους εξαρτημάτων του με πυρήνα το έξυπνο συμβόλαιο. Αναλύεται επίσης η υποδομή που χρησιμοποιήθηκε για την ανάπτυξη της εφαρμογής.

Στο Κεφάλαιο 5 αναλύεται η λειτουργία της αποκεντρωμένης εφαρμογής. Περιγράφονται αναλυτικά οι επιμέρους περιπτώσεις χρήσης της εφαρμογής μέσω της διεπαφής χρήστη με τη βοήθεια στιγμιοτύπων.

Τέλος στο Κεφάλαιο 6 γίνεται μία αποτίμηση του συνόλου της εργασίας και προτείνονται μερικές κατευθύνσεις για επεκτάσεις της προτεινόμενης εφαρμογής.

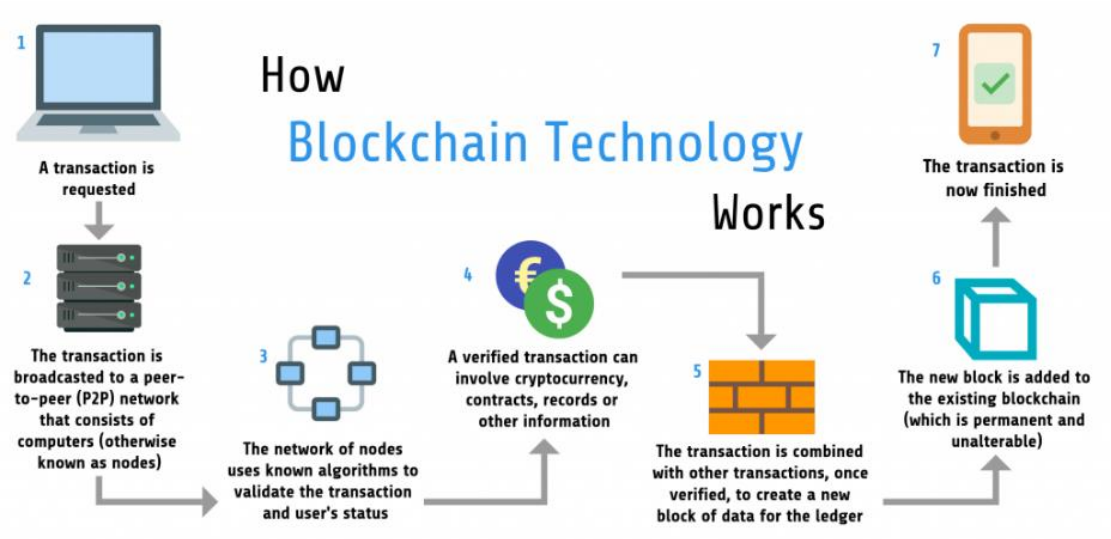
Κεφάλαιο 2 Ανασκόπηση της τεχνολογίας Blockchain

2.1 Εισαγωγή στο blockchain

Η έννοια της τεχνολογίας blockchain εισήχθη για πρώτη φορά το 2008 από το άτομο ή ομάδα ανθρώπων που χρησιμοποίησε το ψευδώνυμο Satoshi Nakamoto, σε ένα έγγραφο με τίτλο "Bitcoin: A Peer-to-Peer Electronic Cash System" [5]. Ο πρωταρχικός στόχος του blockchain ήταν να επιτρέψει τη δημιουργία ενός αποκεντρωμένου ψηφιακού νομίσματος, του Bitcoin, το οποίο θα μπορούσε να διευκολύνει ασφαλείς και αξιόπιστες συναλλαγές χωρίς την ανάγκη μιας κεντρικής αρχής, όπως μια τράπεζα ή ένα χρηματοπιστωτικό ίδρυμα.

Το blockchain είναι ένα κατανεμημένο ψηφιακό βιβλίο που αποθηκεύει πληροφορίες με τη μορφή μπλοκ, τα οποία συνδέονται χρονολογικά μεταξύ τους χρησιμοποιώντας κρυπτογραφικές τεχνικές. Κάθε μπλοκ περιέχει μια λίστα συναλλαγών ή άλλων δεδομένων και συνδέεται κρυπτογραφικά με το προηγούμενο μπλοκ στην αλυσίδα, δημιουργώντας μια αδιάσπαστη και διαφανή εγγραφή όλων των συναλλαγών ή των δεδομένων που είναι αποθηκευμένα στην αλυσίδα μπλοκ.

Σε αυτήν την ενότητα, θα εμβαθύνουμε στα βασικά στοιχεία και τους μηχανισμούς που συνθέτουν ένα blockchain, όπως τα κατανεμημένα λογιστικά βιβλία (distributed ledgers), οι κρυπτογραφικές τεχνικές, οι μηχανισμοί συναίνεσης και οι κόμβοι. Η κατανόηση αυτών των εννοιών είναι ζωτικής σημασίας για την κατανόηση των δυνατοτήτων και των περιορισμών της τεχνολογίας blockchain σε διάφορες εφαρμογές, συμπεριλαμβανομένου του ενεργειακού τομέα και του ψηφιακού ενεργειακού νομίσματος που θα παρουσιάσουμε.

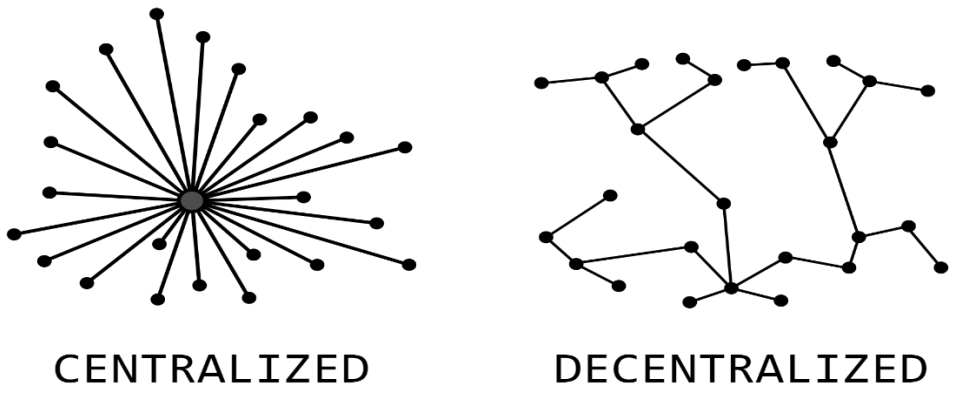


Εικόνα 2-1 Πως μεταδίδεται μία συναλλαγή στο blockchain
Πηγή: https://medium.com/@ipspecialist/how-blockchain-technology-works-e6109c033034

2.1.1 Κατανεμημένα Ledger

Ένα κατανεμημένο ledger είναι μια βάση δεδομένων που μοιράζεται, αναπαράγεται και συγχρονίζεται σε πολλούς κόμβους ή συμμετέχοντες σε ένα δίκτυο. Σε αντίθεση με τις παραδοσιακές κεντρικές βάσεις δεδομένων, όπου μια μεμονωμένη οντότητα ελέγχει τα δεδομένα και την πρόσβαση σε αυτά, τα κατανεμημένα ledger παρέχουν αποκεντρωμένο έλεγχο και διαχείριση των δεδομένων. Κάθε κόμβος στο δίκτυο διατηρεί ένα αντίγραφο του ledger και τυχόν ενημερώσεις του διαδίδονται σε όλο το δίκτυο, διασφαλίζοντας ότι όλοι οι κόμβοι έχουν τις ίδιες πληροφορίες.

Η αποκεντρωμένη φύση των κατανεμημένων ledger προσφέρει πολλά πλεονεκτήματα σε σχέση με τις παραδοσιακές κεντρικές βάσεις δεδομένων, όπως αυξημένη ασφάλεια, διαφάνεια και μειωμένο κίνδυνο χειραγώγησης δεδομένων ή μεμονωμένα σημεία αστοχίας. Στο πλαίσιο του blockchain, το κατανεμημένο ledger χρησιμεύει ως το θεμέλιο πάνω στο οποίο οικοδομείται το δίκτυο blockchain, αποθηκεύοντας τις πληροφορίες με τη μορφή μπλοκ που συνδέονται μεταξύ τους χρησιμοποιώντας κρυπτογραφικές τεχνικές.



Εικόνα 2-2 Διαφορά κεντροποιημένου και αποκεντρωμένου συστήματος.
Πηγή: https://en.wikipedia.org/wiki/Decentralised_system

2.1.2 Κρυπτογραφικές τεχνικές

Η κρυπτογραφία παίζει ζωτικό ρόλο στην ασφάλεια και τη λειτουργικότητα της τεχνολογίας blockchain. Χρησιμοποιείται για την ασφάλεια των δεδομένων που είναι αποθηκευμένα στο blockchain, για την επαλήθευση της αυθεντικότητας των συναλλαγών και για τη διατήρηση της ακεραιότητας του κατανεμημένου ledger. Μερικές από τις βασικές κρυπτογραφικές τεχνικές που χρησιμοποιούνται στην τεχνολογία blockchain περιλαμβάνουν:

- **Συναρτήσεις κατακερματισμού (Hash functions):** Μια συνάρτηση κατακερματισμού είναι ένας μαθηματικός αλγόριθμος που λαμβάνει μια είσοδο (ή "μήνυμα") και επιστρέφει μια συμβολοσειρά byte σταθερού

μεγέθους, συνήθως μια τιμή κατακερματισμού (hash value). Η έξοδος είναι μοναδική για κάθε μοναδική είσοδο, που σημαίνει ότι ακόμη και μια μικρή αλλαγή στην είσοδο θα έχει ως αποτέλεσμα μια εντελώς διαφορετική έξοδο. Στο πλαίσιο του blockchain, οι συναρτήσεις κατακερματισμού χρησιμοποιούνται για τη δημιουργία ενός μοναδικού αναγνωριστικού για κάθε μπλοκ και για τη σύνδεση των μπλοκ μεταξύ τους με τρόπο που δεν παραβιάζεται [6].

- **Κρυπτογράφηση δημόσιου κλειδιού (Public key cryptography):** Γνωστή και ως ασύμμετρη κρυπτογράφηση, η κρυπτογράφηση δημόσιου κλειδιού είναι ένα κρυπτογραφικό σύστημα που χρησιμοποιεί δύο κλειδιά, ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί, τα οποία σχετίζονται μαθηματικά αλλά δεν είναι υπολογιστικά εφικτό να προκύψουν το ένα από το άλλο. Σε ένα blockchain, η κρυπτογραφία δημόσιου κλειδιού χρησιμοποιείται για την ασφάλεια των συναλλαγών επιτρέποντας στους χρήστες να υπογράφουν ψηφιακά τις συναλλαγές τους με το ιδιωτικό τους κλειδί, το οποίο στη συνέχεια μπορεί να επαληθευτεί από οποιονδήποτε χρησιμοποιεί το αντίστοιχο δημόσιο κλειδί [7].

- **Δέντρα Merkle (Merkle trees)**: Ένα δέντρο Merkle είναι μια δομή δεδομένων που χρησιμοποιείται στην κρυπτογραφία που οργανώνει και κατακερματίζει δεδομένα με ιεραρχικό τρόπο, δημιουργώντας μια ενιαία τιμή κατακερματισμού, γνωστή ως ρίζα Merkle, η οποία αντιπροσωπεύει ολόκληρο το σύνολο δεδομένων. Στο πλαίσιο του blockchain, τα δέντρα Merkle χρησιμοποιούνται για την αποτελεσματική αποθήκευση και επαλήθευση των συναλλαγών μέσα σε ένα μπλοκ, καθώς και για τη μείωση του όγκου των δεδομένων που απαιτούνται για τους κόμβους για τη διατήρηση του blockchain [8].

Αυτές οι κρυπτογραφικές τεχνικές, μαζί με άλλες, παρέχουν τη βάση για την ασφάλεια, τη διαφάνεια και την αντοχή στην παραβίαση της τεχνολογίας blockchain, διασφαλίζοντας την ακεραιότητα και την αξιοπιστία του κατανεμημένου ledger.

2.1.3 Μηχανισμοί συναίνεσης

Οι μηχανισμοί συναίνεσης είναι μια ουσιαστική πτυχή της τεχνολογίας blockchain, καθώς επιτρέπουν στο δίκτυο να συμφωνεί για την εγκυρότητα των συναλλαγών και να διατηρεί μια συνεπή κατάσταση του κατανεμημένου ledger σε όλους τους κόμβους. Διάφοροι μηχανισμοί συναίνεσης έχουν αναπτυχθεί για την αντιμετώπιση των μοναδικών απαιτήσεων και προκλήσεων διαφορετικών δικτύων blockchain, αλλά οι πιο συνηθισμένοι είναι το **Proof of Work (PoW)** και το **Proof of Stake (PoS)**.

Proof of Work (PoW): Το PoW είναι ο συναινετικός αλγόριθμος που χρησιμοποιείται στην αρχική αλυσίδα blockchain του Bitcoin [5]. Στο PoW, οι κόμβοι, γνωστοί και ως

miners, ανταγωνίζονται για να λύσουν ένα πολύπλοκο μαθηματικό πρόβλημα. Ο πρώτος κόμβος που θα λύσει το πρόβλημα έχει το δικαίωμα να προσθέσει το επόμενο μπλοκ στο blockchain και ανταμείβεται με νέα νομίσματα και χρεώσεις συναλλαγών. Το PoW διασφαλίζει ότι το δίκτυο παραμένει ασφαλές και ανθεκτικό σε επιθέσεις, καθώς απαιτεί σημαντικούς υπολογιστικούς πόρους για την εξόρυξη ενός μπλοκ και τον χειρισμό του blockchain. Ωστόσο, το PoW έχει επικριθεί για την υψηλή κατανάλωση ενέργειας και την πιθανή συγκέντρωση λόγω της αυξανόμενης κυριαρχίας των μεγάλων εργασιών εξόρυξης.

Proof of Stake (PoS): Το PoS είναι ένας εναλλακτικός μηχανισμός συναίνεσης που αντιμετωπίζει ορισμένους από τους περιορισμούς του PoW, όπως η υψηλή κατανάλωση ενέργειας και η πιθανή συγκέντρωση [9]. Στο PoS, οι επικυρωτές επιλέγονται για τη δημιουργία νέων μπλοκ και την επικύρωση συναλλαγών με βάση το μερίδιο τους στο δίκτυο, το οποίο συνήθως καθορίζεται από το ποσό του εγγενούς κρυπτονομίσματος που κατέχουν και είναι πρόθυμοι να «ποντάρουν» ως εγγύηση. Το PoS θεωρείται γενικά πιο ενεργειακά αποδοτικό και αποκεντρωμένο από το PoW, καθώς δεν απαιτεί σημαντικούς υπολογιστικούς πόρους για τη συμμετοχή στη διαδικασία συναίνεσης.

Στον πίνακα 1 παρουσιάζονται συνοπτικά τα βασικά χαρακτηριστικά των δύο αλγόριθμων συναίνεσης που παρουσιάστηκαν καθώς και του αλγόριθμου **Proof of Authority (PoA)** που χρησιμοποιείται κυρίως σε δοκιμαστικά περιβάλλοντα λόγω της κεντροποίησης του.

Πίνακας 1 Σύγκριση Αλγορίθμων Συναίνεσης

Αλγόριθμοι Συναίνεσης	**Κύρια Ιδέα**	**Κατανάλωση Ενέργειας**	**Επίπεδο Κεντροποίησης**
Proof-of-Work (PoW)	Η υπολογιστική ισχύς καθορίζει την πιθανότητα προσθήκης νέου μπλοκ	Υψηλή	Χαμηλό
Proof-Of-Stake (PoS)	Τα κρυπτονομίσματα που ποντάρονται καθορίζουν την πιθανότητα προσθήκης νέου μπλοκ	Χαμηλή	Μέτριο
Proof-Of Authority (PoA)	Μόνο ορισμένοι εξουσιοδοτημένοι κόμβοι έχουν τη δυνατότητα να προσθέσουν ένα νέο μπλοκ	Χαμηλή	Υψηλό

2.2 Ethereum

Το Ethereum είναι μια αποκεντρωμένη πλατφόρμα blockchain ανοιχτού κώδικα που εισήχθη το 2014 από τον ιδρυτή της, Vitalik Buterin [9]. Σε αντίθεση με το Bitcoin, το οποίο σχεδιάστηκε κυρίως για τη διευκόλυνση ασφαλών και αξιόπιστων οικονομικών

συναλλαγών, το Ethereum σχεδιάστηκε ως μια πλατφόρμα για τη δημιουργία και την ανάπτυξη **αποκεντρωμένων εφαρμογών (dApps)** χρησιμοποιώντας **έξυπνα συμβόλαια (smart contracts).** Τα έξυπνα συμβόλαια είναι αυτοεκτελούμενες συμφωνίες με τους όρους της σύμβασης απευθείας γραμμένους σε κώδικα, επιτρέποντας αυξημένη αυτοματοποίηση, διαφάνεια και αποτελεσματικότητα σε ένα ευρύ φάσμα εφαρμογών.

Το όραμα του Ethereum ήταν να δημιουργήσει έναν «παγκόσμιο υπολογιστή» – μια παγκόσμια, αποκεντρωμένη και ανθεκτική στη λογοκρισία πλατφόρμα που θα μπορούσε να επιτρέψει στους προγραμματιστές να δημιουργήσουν και να αναπτύξουν dApps χωρίς την ανάγκη για μεσάζοντες ή κεντρικό έλεγχο [10]. Αυτή η επαναστατική ιδέα υποσχέθηκε να διαταράξει διάφορους κλάδους και τομείς, συμπεριλαμβανομένων των χρηματοοικονομικών, της διαχείρισης της εφοδιαστικής αλυσίδας, της διακυβέρνησης και του ενεργειακού τομέα, παρέχοντας έναν πιο ασφαλή, διαφανή και αποτελεσματικό τρόπο διαχείρισης και εκτέλεσης συναλλαγών και συμφωνιών.

Η πλατφόρμα Ethereum βασίζεται σε μια τροποποιημένη έκδοση του πρωτοκόλλου Bitcoin, με πολλές βασικές βελτιώσεις και καινοτομίες, όπως η **εικονική μηχανή Ethereum (EVM),** η οποία χρησιμεύει ως περιβάλλον εκτέλεσης για έξυπνα συμβόλαια και ένα εγγενές κρυπτονόμισμα που ονομάζεται **Ether (ETH)** που χρησιμοποιείται για την πληρωμή τελών συναλλαγών και υπολογιστικών υπηρεσιών στο δίκτυο. Το Ethereum εισήγαγε επίσης έναν νέο αλγόριθμο συναίνεσης, που ονομάζεται Ethash, ο οποίος έχει σχεδιαστεί για να είναι πιο ανθεκτικός σε εξειδικευμένο υλικό εξόρυξης, προωθώντας ένα πιο αποκεντρωμένο και ασφαλές δίκτυο. Από τις 15 Σεπτεμβρίου του 2022 το Ethereum προχώρησε σε έναν σημαντικό μετασχηματισμό με τη μετάβαση από τον υπερβολικά δαπανηρό ενεργειακά μηχανισμό συναίνεσης Proof of Work στον μηχανισμό Proof of Stake, μία μετάβαση που μείωσε τη ενεργειακή κατανάλωση του δικτύου Ethereum κατά ποσοστό 99,95% [11].

Σε αυτήν την ενότητα, θα παρέχουμε μια εις βάθος επισκόπηση της πλατφόρμας Ethereum, συζητώντας τα βασικά της στοιχεία, τις καινοτομίες και την υποκείμενη τεχνολογία που επιτρέπει την δημιουργία και την ανάπτυξη dApps και έξυπνων συμβολαίων. Θα διερευνήσουμε επίσης τη σημασία του προτύπου κρυπτονομισμάτων ERC-20, το οποίο έχει γίνει ευρέως διαδεδομένο πρότυπο για τη δημιουργία και τη διαχείριση ψηφιακών νομισμάτων στο δίκτυο Ethereum.

2.2.1 Ethereum Virtual Machine (EVM)

Η εικονική μηχανή Ethereum (EVM) είναι ένα βασικό στοιχείο του Ethereum, που χρησιμεύει ως περιβάλλον εκτέλεσης για την ανάπτυξη έξυπνων συμβολαίων (smart contracts) [12]. Είναι μια εικονική μηχανή Turing-complete, που επιτρέπει στους προγραμματιστές να δημιουργούν και να αναπτύσσουν έξυπνα συμβόλαια χρησιμοποιώντας τη γλώσσα προγραμματισμού υψηλού επιπέδου Solidity. Το EVM μεταφράζει τον κώδικα υψηλού επιπέδου σε bytecode χαμηλού επιπέδου, ο οποίος

στη συνέχεια εκτελείται στους κόμβους Ethereum, διασφαλίζοντας τη συνεπή εκτέλεση έξυπνων συμβολαίων σε όλο το δίκτυο.

Ως μια Turing-complete μηχανή, το EVM είναι ικανό να εκτελεί οποιονδήποτε υπολογισμό, λαμβάνοντας επαρκείς πόρους, οι οποίοι επιτρέπουν στους προγραμματιστές να δημιουργούν πολύπλοκες και πλούσιες σε χαρακτηριστικά εφαρμογές στην πλατφόρμα Ethereum. Ωστόσο, για να αποτρέψει άπειρους βρόχους ή υπερβολική κατανάλωση πόρων, το EVM χρησιμοποιεί ένα σύστημα «αερίου» (gas), το οποίο λειτουργεί ως μέτρο της υπολογιστικής προσπάθειας που απαιτείται για την εκτέλεση μιας συγκεκριμένης λειτουργίας. Κάθε λειτουργία στο πλαίσιο ενός έξυπνου συμβολαίου καταναλώνει μια συγκεκριμένη ποσότητα gas και οι χρήστες υποχρεούνται να πληρώσουν αυτό το κόστος χρησιμοποιώντας Ether. Αυτό όχι μόνο διασφαλίζει ότι οι πόροι του δικτύου χρησιμοποιούνται αποτελεσματικά, αλλά και δίνει κίνητρα στους προγραμματιστές να βελτιστοποιήσουν τα έξυπνα συμβόλαιά τους για ελάχιστη κατανάλωση αερίου.

Το EVM διαδραματίζει κρίσιμο ρόλο στην ασφάλεια, την επεκτασιμότητα και τη διαλειτουργικότητα της πλατφόρμας Ethereum, καθώς απομονώνει τα έξυπνα συμβόλαια από το υποκείμενο υλικό και λογισμικό, διασφαλίζοντας ότι τυχόν ευπάθειες ή σφάλματα σε ένα έξυπνο συμβόλαιο δεν θέτουν σε κίνδυνο ολόκληρο το δίκτυο. Επιπλέον, το EVM επιτρέπει την απρόσκοπτη ενσωμάτωση διαφόρων **ψηφιακών νομισμάτων (tokens)** που βασίζονται στο Ethereum, όπως τα ERC-20 tokens, καθώς μπορούν όλα να εκτελεστούν στο ίδιο περιβάλλον εκτέλεσης.

2.2.2 Smart Contracts

Τα έξυπνα συμβόλαια είναι αυτοεκτελούμενες συμφωνίες με τους όρους της σύμβασης γραμμένους απευθείας σε κώδικα [13]. Αποτελούν ουσιαστικό συστατικό του οικοσυστήματος του Ethereum, καθώς επιτρέπουν τη δημιουργία αποκεντρωμένων εφαρμογών και την εκτέλεση σύνθετης λογικής στο blockchain. Τα έξυπνα συμβόλαια αποθηκεύονται και εκτελούνται στο EVM.

Η ιδέα πίσω από τα έξυπνα συμβόλαια είναι να επιτραπεί η αξιόπιστη, διαφανής και αυτοματοποιημένη εκτέλεση συμβατικών συμφωνιών χωρίς την ανάγκη μεσαζόντων, όπως δικηγόροι ή συμβολαιογράφοι. Μόλις αναπτυχθεί ένα έξυπνο συμβόλαιο στο blockchain, δεν μπορεί να τροποποιηθεί ή να αφαιρεθεί, διασφαλίζοντας το αμετάβλητο και την αξιοπιστία των συμφωνιών που κωδικοποιούνται σε αυτό.

Τα έξυπνα συμβόλαια γράφονται σε γλώσσες προγραμματισμού υψηλού επιπέδου, στην περίπτωση του Ethereum σε Solidity, οι οποίες στη συνέχεια μεταγλωττίζονται σε bytecode για εκτέλεση στο EVM. Μπορούν να αλληλεπιδρούν με άλλα συμβόλαια, να αποθηκεύουν και να διαχειρίζονται δεδομένα και να ενεργοποιούν προκαθορισμένες ενέργειες με βάση συγκεκριμένες συνθήκες ή συμβάντα (events). Μπορούν επίσης να εκπέμπουν events για να ειδοποιούν εξωτερικές οντότητες για συγκεκριμένα περιστατικά ή να αναφέρουν αλλαγές στο πλαίσιο της σύμβασης.

Παραδείγματα περιπτώσεων χρήσης έξυπνων συμβολαίων περιλαμβάνουν εφαρμογές αποκεντρωμένης χρηματοδότησης (DeFi), συμβολοποίηση περιουσιακών στοιχείων, διαχείριση αλυσίδας εφοδιασμού, συστήματα ψηφοφορίας και άλλα.

Στο πλαίσιο της παρούσας εργασίας, τα έξυπνα συμβόλαια χρησιμεύουν ως η ραχοκοκαλιά για την εφαρμογή του συστήματος ανταμοιβής για την ενεργειακή απόδοση και τη διαχείριση της διανομής και της ανταλλαγής του ψηφιακού νομίσματος.

2.2.3 Tokens

Τα Ethereum tokens είναι ψηφιακά περιουσιακά στοιχεία που δημιουργούνται και διαχειρίζονται στο Ethereum blockchain, αξιοποιώντας τη δύναμη των έξυπνων συμβολαίων. Τα tokens είναι προγραμματιζόμενα, προσαρμόσιμα και μπορούν να σχεδιαστούν για να αντιπροσωπεύουν διάφορους τύπους αξίας ή χρησιμότητας, όπως νομίσματα, περιουσιακά στοιχεία, δικαιώματα ψήφου ή πρόσβαση σε υπηρεσίες.

Ένα από τα πιο δημοφιλή πρότυπα διακριτικών στο Ethereum είναι το πρότυπο **ERC-20**, το οποίο ορίζει ένα σύνολο κανόνων και λειτουργιών για τη δημιουργία και τη διαχείριση των διακριτικών με τυποποιημένο, διαλειτουργικό τρόπο [14]. Το πρότυπο ERC-20 έχει διευκολύνει την ταχεία ανάπτυξη του οικοσυστήματος tokens στο Ethereum, επιτρέποντας στα projects να δημιουργούν και να αναπτύσσουν εύκολα tokens για διάφορους σκοπούς, όπως η συγκέντρωση χρημάτων μέσω αρχικών προσφορών νομισμάτων (ICO), οι εφαρμογές αποκεντρωμένης χρηματοδότησης (DeFi) και τα μη ανταλλάξιμα tokens (NFTs).

2.3 Μειονεκτήματα του Ethereum

Ενώ το Ethereum υπήρξε επαναστατικό στον κόσμο της τεχνολογίας blockchain, δεν είναι χωρίς τα μειονεκτήματά του. Σε αυτήν την ενότητα, θα συζητήσουμε μερικά από τα βασικά μειονεκτήματα του Ethereum, τα οποία είναι απαραίτητο να ληφθούν υπόψη κατά την αξιολόγηση της καταλληλότητάς του για το έργο του ψηφιακού ενεργειακού νομίσματός μας ή οποιαδήποτε άλλης εφαρμογής.

2.3.1 Scalability

Μία από τις πιο σημαντικές προκλήσεις που αντιμετωπίζει το Ethereum είναι η περιορισμένη κλιμακωσιμότητά του [15]. Το δίκτυο Ethereum μπορεί επί του παρόντος να χειριστεί περίπου 30 συναλλαγές ανά δευτερόλεπτο (tps) , το οποίο είναι σημαντικά χαμηλότερο από τα παραδοσιακά συστήματα πληρωμών όπως η Visa, ικανά να επεξεργαστούν χιλιάδες tps. Αυτός ο περιορισμός οδηγεί σε

συμφόρηση δικτύου σε περιόδους υψηλής ζήτησης, με αποτέλεσμα αργούς χρόνους συναλλαγών και αυξημένα gas fees.

Η κοινότητα του Ethereum εργάζεται ενεργά για την αντιμετώπιση αυτού του ζητήματος μέσω διαφόρων λύσεων κλιμάκωσης, όπως το Ethereum 2.0 (που εισήγαγε το Proof-of-Stake) και τις τεχνολογίες κλιμάκωσης του επιπέδου 2, όπως τα Optimistic Rollups και τα ZK-Rollups. Ωστόσο, αυτές οι λύσεις είναι ακόμη υπό ανάπτυξη και ο πλήρης αντίκτυπός τους στην κλιμκωσιμότητα του Ethereum μένει να φανεί.

2.3.2 Υψηλά Κόστη Συναλλαγών

Όπως αναφέρθηκε προηγουμένως, η περιορισμένη κλιμακωσιμότητα του Ethereum οδηγεί σε υψηλές χρεώσεις αερίου σε περιόδους συμφόρησης δικτύου. Αυτές οι χρεώσεις είναι απαραίτητες για να δοθούν κίνητρα στους miners (και στο Ethereum 2.0, τους validators) να συμπεριλάβουν συναλλαγές στο blockchain. Ωστόσο, μπορεί να είναι απαγορευτικά ακριβά για τους χρήστες, ιδιαίτερα για εκείνους που εμπλέκονται σε πολύπλοκες αλληλεπιδράσεις έξυπνων συμβολαίων, όπως οι εφαρμογές DeFi.

Τα υψηλά κόστη συναλλαγών μπορούν να περιορίσουν την προσβασιμότητα και την υιοθέτηση εφαρμογών που βασίζονται στο Ethereum.. Αν και η μετάβαση του Ethereum στο Proof-of-Stake στο Ethereum 2.0 αναμένεται σταδιακά να μειώσει τα κόστη συναλλαγών [16], εξακολουθεί να είναι αβέβαιο πώς αυτό θα επηρεάσει τα κόστη συναλλαγών μακροπρόθεσμα.

2.3.3 Ευαλωτότητα Smart Contracts

Τα έξυπνα συμβόλαια του Ethereum, αν και ισχυρά και ευέλικτα, μπορεί να είναι επιρρεπή σε τρωτά σημεία και εκμεταλλεύσεις εάν δεν σχεδιαστούν και δεν ελεγχθούν σωστά. Υπήρξαν αρκετά περιστατικά όπου έξυπνα συμβόλαια με κακή σχεδίαση ή εφαρμογή οδήγησαν σε σημαντικές απώλειες κεφαλαίων. Για παράδειγμα, το hack του DAO το 2016 είχε ως αποτέλεσμα την απώλεια Ether αξίας περίπου 60 εκατομμυρίων δολαρίων λόγω ελαττώματος στο έξυπνο συμβόλαιο [17].

Για να μετριαστεί ο κίνδυνος ευπάθειας των έξυπνων συμβολαίων, είναι σημαντικό να ακολουθούνται οι βέλτιστες πρακτικές για την ανάπτυξή του, όπως η διεξαγωγή ενδελεχών ελέγχων, η εφαρμογή επίσημης επαλήθευσης και η χρήση καθιερωμένων βιβλιοθηκών έξυπνων συμβολαίων. Ωστόσο, ακόμη και με αυτές τις προφυλάξεις, ο κίνδυνος τρωτών σημείων παραμένει ανησυχητικός για τα έργα που βασίζονται στο Ethereum.

2.4 Ιδιωτικά Blockchain

Ένα ιδιωτικό blockchain, γνωστό και ως permissioned blockchain, είναι ένας συγκεκριμένος τύπος δικτύου blockchain που λειτουργεί υπό περιορισμούς πρόσβασης. Σε αντίθεση με τα δημόσια όπως το Bitcoin ή το Ethereum, όπου οποιοσδήποτε χρήστης μπορεί να συμμετέχει σε διαδικασίες επαλήθευσης συναλλαγών και συναίνεσης, τα ιδιωτικά blockchain απαιτούν ρητή άδεια συμμετοχής.

2.4.1 Δομή και Λειτουργία

Σε ένα ιδιωτικό blockchain, ο έλεγχος της συμμετοχής ασκείται από μια ενιαία οντότητα ή μια κοινοπραξία οντοτήτων. Αποφασίζουν για τους συμμετέχοντες στο δίκτυο και τη διαδικασία επικύρωσης των συναλλαγών. Έτσι, ένα ιδιωτικό blockchain αποτελείται από ένα δίκτυο προεπιλεγμένων κόμβων, όπου κάθε κόμβος αντιπροσωπεύει έναν χρήστη ή μια ομάδα χρηστών με την εξουσία να επικυρώνει τις συναλλαγές.

2.4.2 Πλεονεκτήματα

Οι ιδιωτικές αλυσίδες μπλοκ προσφέρουν πολλά πλεονεκτήματα, κυρίως όσον αφορά την ιδιωτικότητα, την αποτελεσματικότητα και τον έλεγχο. Μπορούν να διατηρήσουν το απόρρητο των συναλλαγών, καθιστώντας τα ιδανικά για επιχειρηματικές δραστηριότητες που απαιτούν υψηλά επίπεδα απορρήτου. Επιπλέον, καθώς λιγότεροι κόμβοι συμμετέχουν στη διαδικασία συναίνεσης, οι ιδιωτικές αλυσίδες μπλοκ μπορούν να χειριστούν περισσότερες συναλλαγές ανά δευτερόλεπτο, ενισχύοντας την κλιμακωσιμότητα τους.

Το ελεγχόμενο περιβάλλον επιτρέπει επίσης την ευελιξία και την προσαρμογή, επιτρέποντας στο δίκτυο να προσαρμόζεται σύμφωνα με συγκεκριμένες οργανωτικές ανάγκες. Επιπλέον, η κανονιστική συμμόρφωση μπορεί να διαχειρίζεται καλύτερα σε ιδιωτικές αλυσίδες μπλοκ, καθιστώντας τις κατάλληλες για ρυθμιζόμενες βιομηχανίες.

2.4.3 Μειονεκτήματα

Ενώ τα ιδιωτικά blockchain φέρνουν πολλά οφέλη, έρχονται επίσης με περιορισμούς. Η πιο σημαντική ανησυχία είναι η αντιστάθμιση μεταξύ ελέγχου και αποκέντρωσης. Από τη φύση τους, οι ιδιωτικές αλυσίδες μπλοκ είναι συγκεντρωμένες σε κάποιο βαθμό, γεγονός που μπορεί να οδηγήσει σε κινδύνους εάν οι οντότητες που ελέγχουν παραβιαστούν.

Δεύτερον, ενώ το απόρρητο ενισχύεται στις ιδιωτικές αλυσίδες μπλοκ, αυτό μπορεί να περιορίσει τη διαφάνεια, η οποία αποτελεί βασικό χαρακτηριστικό της τεχνολογίας blockchain. Η μειωμένη διαφάνεια θα μπορούσε ενδεχομένως να επιτρέψει στις δόλιες δραστηριότητες να μην εντοπιστούν, ιδιαίτερα εάν η ελεγκτική οντότητα δεν είναι πλήρως αξιόπιστη.

Τέλος, οι ιδιωτικές αλυσίδες μπλοκ μπορεί να μην είναι τόσο ασφαλείς όσο οι δημόσιες. Καθώς ο αριθμός των κόμβων στο δίκτυο είναι μικρότερος, το δίκτυο είναι πιο επιρρεπές σε επιθέσεις συμπαιγνίας, όπου η πλειονότητα των κόμβων συμπαιγνύουν για να επικυρώσουν δόλιες συναλλαγές (51% attack).

Συμπερασματικά, ενώ τα ιδιωτικά blockchain παρέχουν μια πολλά υποσχόμενη λύση για πολλές επιχειρήσεις και οργανισμούς, πρέπει να ληφθούν προσεκτικά υπόψη τα πιθανά μειονεκτήματά τους.

Στον πίνακα 2 παρουσιάζονται συνοπτικά οι κυριότερες διαφοροποιήσεις ενός δημόσιου με ένα ιδιωτικό blockchain

Πίνακας 2 Σύγκριση δημόσιου με ιδιωτικό blockchain

Δημόσιο Blockchain	Ιδιωτικό Blockchain
Ανοιχτό σε όλους	Οι συμμετέχοντες προεπιλέγονται
Απαιτείται κάποιο κρυπτονόμισμα για τη λειτουργία του	Το κρυπτονόμισμα δεν είναι απαραίτητο
Υψηλή αποκεντροποίηση	Χαμηλή αποκεντροποιήση
Χαμηλή διεκπεραιωτικότητα συναλλαγών	Υψηλή διεκπεραιωτικότητα συναλλαγών
Υποχρεωτική κοστολόγηση συναλλαγών	Προαιρετική κοστολόγηση συναλλαγών

2.4.4 Παραδείγματα Ιδιωτικών Blockchains

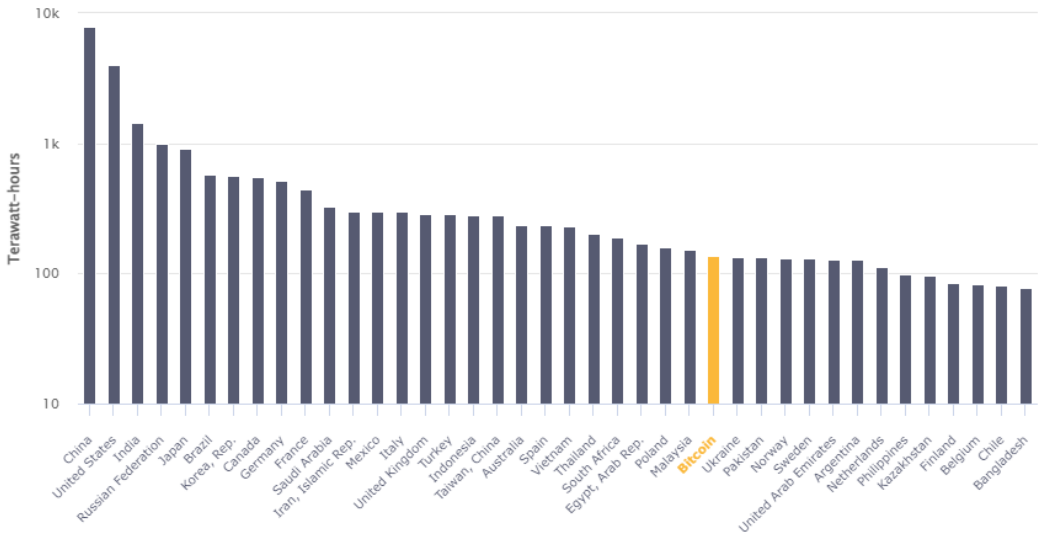
Εξέχοντα παραδείγματα ιδιωτικών πλατφορμών blockchain περιλαμβάνουν το Hyperledger Fabric και το Corda της R3. Το Hyperledger Fabric, που φιλοξενείται από το The Linux Foundation, προσφέρει modular αρχιτεκτονική, επιτρέποντας σε στοιχεία όπως η συναίνεση και οι υπηρεσίες συνδρομής να είναι plug-and-play [18]. Το Corda της R3, από την άλλη πλευρά, έχει σχεδιαστεί ειδικά για οικονομικές συμφωνίες, δίνοντας έμφαση στη διαλειτουργικότητα, την ασφάλεια και το απόρρητο [19].

Συμπερασματικά, τα ιδιωτικά blockchain αντιπροσωπεύουν μια κρίσιμη πτυχή της τεχνολογίας blockchain, προσφέροντας μια ελεγχόμενη, αποτελεσματική και προσαρμόσιμη λύση για οργανισμούς που επιδιώκουν να αξιοποιήσουν τα οφέλη του blockchain διατηρώντας τα απαραίτητα ρυθμιστικά πρότυπα και πρότυπα απορρήτου.

2.5 Το Blockchain στην ενέργεια

Η ενσωμάτωση της τεχνολογίας blockchain στον τομέα της ενέργειας γίνεται γρήγορα ένας πολλά υποσχόμενος τομέας καινοτομίας. Οι βασικές αρχές του blockchain - αποκέντρωση, διαφάνεια και ασφάλεια - είναι κατάλληλες για την αντιμετώπιση διαφόρων προκλήσεων που αντιμετωπίζει ο ενεργειακός τομέας. Αυτά περιλαμβάνουν τη βελτίωση της απόδοσης, τη δυνατότητα ανταλλαγής ενέργειας από ομοτίμους και τη διευκόλυνση της επιτυχούς ενσωμάτωσης ανανεώσιμων πηγών ενέργειας.

Ωστόσο, πριν ερευνήσουμε τις διάφορες εφαρμογές του blockchain στον ενεργειακό τομέα, είναι σημαντικό να αναλογιστούμε το περιβαλλοντικό αποτύπωμα της ίδιας της τεχνολογίας blockchain. Για παράδειγμα, ο συναινετικός μηχανισμός Proof-of-Work (PoW) του Bitcoin έχει επικριθεί ευρέως για τη σημαντική κατανάλωση ενέργειας του. Σύμφωνα με το Cambridge Center for Alternative Finance, η ετήσια κατανάλωση ηλεκτρικής ενέργειας του Bitcoin στις αρχές του 2023 προσέγγιζε τη Μαλαισία (Εικόνα 2-3), κατατάσσοντάς την μεταξύ των 30 κορυφαίων καταναλωτών ηλεκτρικής ενέργειας παγκοσμίως, αν ήταν χώρα. Αυτή η σημαντική χρήση ενέργειας και οι σχετικές εκπομπές άνθρακα αποτελούν σοβαρή πρόκληση για τις παγκόσμιες προσπάθειες βιωσιμότητας.



Εικόνα 2-3 Η θέση του Bitcoin στην κατάταξη των χωρών στην ετήσια κατανάλωση ενέργειας. Πηγή: https://ccaf.io/cbnsi/cbeci/comparisons

Από την άλλη πλευρά, το Ethereum, έχει αναγνωρίσει αυτές τις περιβαλλοντικές ανησυχίες και μετέβη από το PoW σε έναν συναινετικό μηχανισμό Proof-of-Stake (PoS) μέσω της αναβάθμισής του Ethereum 2.0. Το PoS είναι σημαντικά πιο ενεργειακά αποδοτικό και φιλικό προς το περιβάλλον, θέτοντας θετικό προηγούμενο για άλλα έργα blockchain.

Έχοντας αυτές τις σκέψεις κατά νου, αυτό το κεφάλαιο θα διερευνήσει διαφορετικές εφαρμογές της τεχνολογίας blockchain στον ενεργειακό τομέα, που κυμαίνονται από τη βελτίωση της διαχείρισης του δικτύου, τη διευκόλυνση του εμπορίου ενέργειας έως την προώθηση πρωτοβουλιών πράσινης ενέργειας.

2.5.1 Ενεργειακές εφαρμογές στο Blockchain

Η εμφάνιση της τεχνολογίας blockchain άνοιξε το δρόμο για καινοτόμες λύσεις σε διάφορους κλάδους, συμπεριλαμβανομένου του ενεργειακού τομέα, καθώς προσφέρει μια αποκεντρωμένη, διαφανή και ασφαλή μέθοδο καταγραφής συναλλαγών, με πολλά υποσχόμενες συνέπειες για την εμπορία ενέργειας, τη διαχείριση του δικτύου και την παρακολούθηση των εκπομπών άνθρακα [20].

Οι δυνατότητες του blockchain απεικονίζονται έντονα στο peer-to-peer (P2P) εμπόριο ενέργειας, όπου μπορεί να επιτρέψει άμεσες συναλλαγές ενέργειας μεταξύ των χρηστών. Το project Brooklyn Microgrid στη Νέα Υόρκη αποτελεί παράδειγμα αυτής της εφαρμογής. Εδώ, οι τοπικοί παραγωγοί ενέργειας ανταλλάσσουν την πλεονάζουσα ηλιακή ενέργεια με τους γείτονές τους χρησιμοποιώντας την πλατφόρμα Exergy, μία πλατφόρμα ιδιωτικού blockchain αναπτυγμένη από την LO3 Energy, ενισχύοντας έτσι την τοπική χρήση ανανεώσιμων πηγών ενέργειας και μειώνοντας την εξάρτηση από τις παραδοσιακές υπηρεσίες κοινής ωφέλειας [21].

Μια άλλη αξιοσημείωτη εφαρμογή έγκειται στην παρακολούθηση και επαλήθευση των εκπομπών άνθρακα. Το blockchain παρέχει ένα αξιόπιστο σύστημα για την παρακολούθηση αυτών των εκπομπών, υποστηρίζοντας έτσι τις προσπάθειες μετριασμού της κλιματικής αλλαγής. Ένα απτό παράδειγμα είναι το Energy Web Chain, μια παγκόσμια πλατφόρμα blockchain ανοιχτού κώδικα που έχει σχεδιαστεί για τον ενεργειακό τομέα. Παρέχει ένα σύστημα που δεν παραβιάζεται για την παρακολούθηση των εκπομπών άνθρακα, βοηθώντας έτσι την εμπορία άνθρακα και τη συμμόρφωση με τις πολιτικές για την κλιματική αλλαγή [22].

2.5.2 Ενεργειακά νομίσματα

Κάποιες από τις οντότητες που έχουν αναπτύξει ενεργειακά projects στο blockchain έχουν αναπτύξει και τα δικά τους νομίσματα χρησιμοποιώντας κατά κύριο λόγο το πρότυπο ERC-20. Παρακάτω παρουσιάζονται τα κυριότερα τέτοια νομίσματα και η χρησιμότητα η οποία έχε δοθεί σε αυτά.

- *Powerledger*

Το Powerledger είναι ένα project με βάση την Αυστραλία που χρησιμοποιεί τεχνολογία blockchain για να διευκολύνει το εμπόριο ενέργειας P2P. Το εγγενές κρυπτονόμισμα του Powerledger, POWR, χρησιμοποιείται για πρόσβαση και χρήση

της πλατφόρμας, ενώ ένα δευτερεύον token, το Sparkz, χρησιμοποιείται για συναλλαγές ενέργειας εντός της εφαρμογής. Οι κάτοχοι νομισμάτων POWR μπορούν να δημιουργήσουν tokens Sparkz, τα οποία είναι συνδεδεμένα με την τιμή του τοπικού νομίσματος. Αυτό το διπλό σύστημα επιτρέπει μια ασφαλή και αποτελεσματική αγορά για εμπορία ενέργειας και δίνει τη δυνατότητα στους καταναλωτές να νομισματοποιούν τις επενδύσεις τους σε ανανεώσιμες πηγές ενέργειας [23].

- *Energy Web Token*

Το Energy Web Chain, που αναπτύχθηκε από το Energy Web Foundation, είναι μια πλατφόρμα blockchain ανοιχτού κώδικα, επεκτάσιμη, σχεδιασμένη ειδικά για τις ρυθμιστικές, λειτουργικές ανάγκες και τις ανάγκες της αγοράς του ενεργειακού τομέα. Το εγγενές νόμισμά του, Energy Web Token (EWT), χρησιμοποιείται για την πρόσβαση και τη χρήση του δικτύου, την πληρωμή τελών συναλλαγών και τη διασφάλιση της ασφάλειας του δικτύου. Το Energy Web Chain στοχεύει να τυποποιήσει και να απλοποιήσει την εφαρμογή ενεργειακών εφαρμογών που βασίζονται σε blockchain, ενισχύοντας ένα οικοσύστημα αποκεντρωμένων ενεργειακών πόρων [22].

- *Efforce*

Το Efforce είναι μια πλατφόρμα βασισμένη στο Ethereum με συνιδρυτή τον Steve Wozniak της Apple. Στοχεύει στον εκδημοκρατισμό της πρόσβασης σε έργα και επενδύσεις ενεργειακής απόδοσης μέσω του token του, WOZX. Το Efforce επιτρέπει στους συνεισφέροντες να επενδύουν σε έργα ενεργειακής απόδοσης και να λαμβάνουν νομίσματα που αντιπροσωπεύουν την εξοικονόμηση ενέργειας που επιτυγχάνεται. Για το σκοπό αυτό χρησιμοποιείται ένα άλλο token, το mWOZ, το οποίο αντιστοιχεί σε 1$ εξοικονόμησης ενέργειας. Αυτά τα νομίσματα μπορούν να χρησιμοποιηθούν ή να πωληθούν στην πλατφόρμα, παρέχοντας έναν νέο τρόπο σε ιδιώτες και εταιρείες νομισματοποίησης της εξοικονόμησης ενέργειας και την προώθηση της ενεργειακής απόδοσης [24].

Κεφάλαιο 3 Ανάλυση και Σχεδίαση του Atomcoin

3.1 Ενεργειακό νόμισμα Atomcoin

3.1.1 Παρουσίαση Atomcoin

Στόχος της παρούσας διπλωματικής εργασίας είναι η ανάπτυξη μιας αποκεντρωμένης εφαρμογής (dapp) που θα ενθαρρύνει τους καταναλωτές ενέργειας ενός οικοσυστήματος να υιοθετήσουν περισσότερο ενεργειακά αποδοτικές πρακτικές. Σε αυτή την προσέγγιση επιλέχθηκε η ανάπτυξη του **Atomcoin**, ενός ενεργειακού νομίσματος, βασισμένου σε τεχνολογία blockchain που παρουσιάζεται αρχικά στο [4]. Μία βελτίωση του αρχικού μοντέλου παρουσιάστηκε το 2020 [25], ενώ η τελική μορφή η οποία είναι και αυτή που θα υλοποιηθεί σε αυτή την εργασία και στην οποία πραγματοποιείται ο υπολογισμός της επιβράβευσης σε ωριαία βάση παρουσιάζεται στο [2].

Οι συμμετέχοντες στο πρόγραμμα κερδίζουν 1 Atomcoin για κάθε κιλοβατώρα (kWh) που εξοικονομούν σε σύγκριση με την προβλεπόμενη κατανάλωσή τους.

Η ουσία του Atomcoin έγκειται στη δυνατότητά του να παρέχει κίνητρα για εξοικονόμηση ενέργειας σε ατομικό επίπεδο, υποκινώντας έτσι μια αλλαγή παραδείγματος προς μια κουλτούρα με περισσότερη ενεργειακή συνείδηση σε ολόκληρο το οικοσύστημα. Ως ψηφιακό νόμισμα, το Atomcoin θα κατανεμηθεί στους καταναλωτές ανάλογα με την ποσότητα ενέργειας που θα εξοικονομήσουν, αποδίδοντας έτσι μια απτή και χρηματοοικονομική αξία στην ενεργειακή απόδοση.

3.1.2 Καθορισμός Rate

Ο υπολογισμός της ημερήσιας τιμής (rate) του νομίσματος προκύπτει από την παρακάτω εξίσωση:

$$C_k = p_{kWh} * \mathrm{reg} * \left(0.5 * \frac{\sum_{i=1}^{k} \left\{ \sum_{j=1}^{N} \left[ES_{ij} - (cc-cb)_{i-1} \right] \right\}}{\sum_{i=1}^{k} \left[B_i + \mathrm{reg} * e - \mathrm{ratio}_{i-1} * (cc-cb)_{i-1} \right]} + 0.5 * \frac{\sum_{i=k-520}^{k} \sum_{j=1}^{N} ES_{ij}}{\sum_{i=k-5 \geq 0}^{k} B_i} \right) \quad (3.1)$$

όπου:

- pkWh: κόστος κιλοβατώρας (€/kWh),
- k: ημέρα προγράμματος,
- j: συμμετέχων,
- N: συνολικός αριθμός συμμετεχόντων,
- Bi: διαθέσιμο χρηματικό ποσό για τη μέρα i,
- ESij: ενέργεια που εξοικονομήθηκε την ημέρα i από τον συμμετέχων j,
- e: υπερκατανάλωση ενέργειας που ξεπέρασε το στόχο, προκειμένου να επιβληθεί ποινή,
- cc: νομίσματα που εξαργυρώθηκαν,
- cb: νομίσματα που αγοράστηκαν,

- reg: σταθερά.

Η τιμή reg στην παραπάνω εξίσωση ορίζεται ως εξής:

$$reg = \frac{B_T}{EST}\left(\frac{€}{kWh}\right) \qquad (3.2),$$

όπου:

- BT: συνολικό διαθέσιμο ποσό για τη δράση.
- EST: συνολικός στόχος εξοικονόμησης ενέργειας.

Η τιμή της μεταβλητής reg είναι σταθερή και καθορίζεται στην αρχή του προγράμματος από την αρχή που το χρησιμοποιεί. Αυτή η τιμή εκφράζει έναν στόχο που αφορά το ποσοστό εξοικονόμησης που αναμένεται να επιτευχθεί σε σχέση με το διαθέσιμο ποσό που δαπανάται. Παράλληλα, η τιμή του reg λειτουργεί και ως μια πρόβλεψη για το επίπεδο εξοικονόμησης που μπορούν να επιτύχουν οι χρήστες βάσει των διαθέσιμων κινήτρων.

Παρακάτω παρουσιάζεται η εξίσωση υπολογισμού του rate του νομίσματος σε ωριαία βάση:

$$C_k = p_{kWh} * reg * \left(0.5 * \frac{\sum_{j=1}^{N}\left\{\sum_{i=1}^{k}\left[\left(\sum_{l=1}^{24} ES_{ijl}\right)-(cc-cb)_{i-1}\right]\right\}}{\sum_{i=1}^{k}\left[\sum_{l=1}^{24} B_{il}+reg*e-\text{ ratio }_{i-1}*(cc-cb)_{i-1}\right]} + 0.5 * \frac{\sum_{j=1}^{N}\sum_{i=k-5\geq 0}^{k}\sum_{l=1}^{24} ES_{ijl}}{\sum_{i=k-5\geq 0}^{k}\sum_{l=1}^{24} B_{il}}\right) \quad (3.3)$$

όπου:

- l: ώρα προγράμματος.
- $Bil = Bi$ 24 , λόγω ισόποσης κατανομής του ημερήσιου διαθέσιμου χρηματικού ποσού στις 24 ώρες της ημέρας.

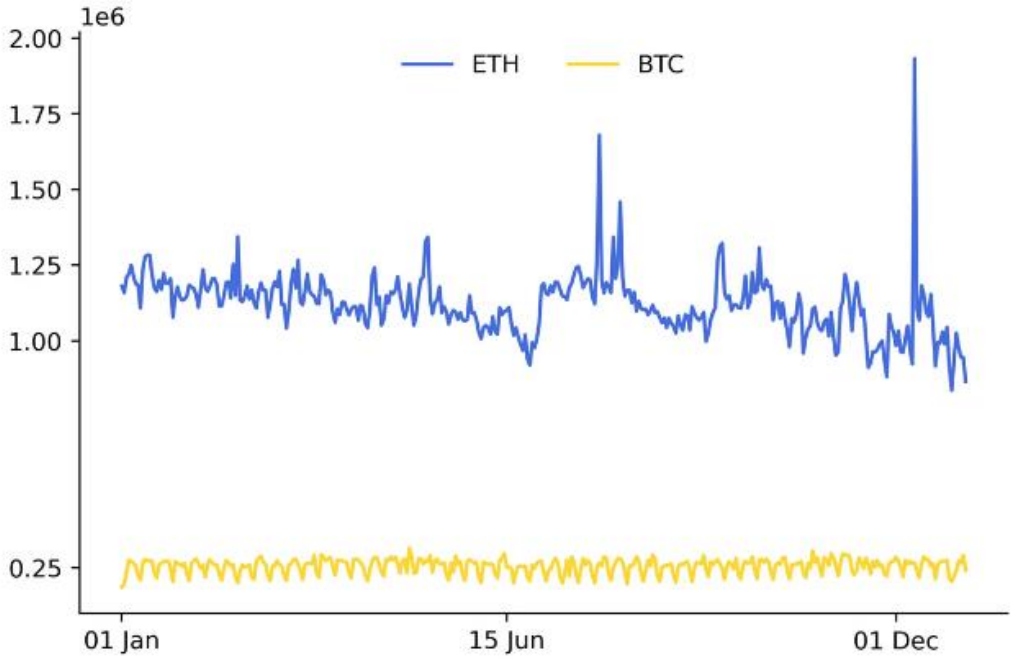
Με βάση τη συγκεκριμένη εξίσωση θεμελιώνεται ένα σαφές πλαίσιο προγράμματος επιβράβευσης στηριγμένο πάνω σε ένα ψηφιακό νόμισμα. Συγκεκριμένα η μεταβλητή pkwh έρχεται να λειτουργήσει ως μονάδα αναφοράς για το νόμισμα καθώς αγνοώντας τους υπόλοιπους όρους τότε το νόμισμα θα έχει σταθερό rate και ίσο με την αντίστοιχη τιμή πώλησης της κιλοβατώρας στον καταναλωτή. Με αυτό τον τρόπο επιτυγχάνεται να υπάρχει μεταβολή την οποία θα αναλύσουμε από τους υπόλοιπους παράγοντες, ωστόσο η αξία του νομίσματος θα παραμένει κοντά στην αξία της κιλοβατώρας στην οποία εξάλλου αντιστοιχεί και το κάθε νόμισμα.

3.2 Ανάλυση της ιδέας

Από την παρουσίαση του ενεργειακού νομίσματος Atomcoin εξάγονται κάποια βασικά συμπεράσματα που καθορίζουν τις λειτουργίες που απαιτούνται στην αποκεντρωμένη εφαρμογή που θα αναπτύξουμε. Αυτά τα συμπεράσματα παρουσιάζονται σε αυτή την ενότητα.

3.2.1 EVM συμβατό blockchain

Αρχικά θα επιλέξουμε να αναπτύξουμε το ψηφιακό μας νόμισμα σε ένα blockchain τεχνολογίας Ethereum καθώς αυτό μπορεί να αποφέρει πολλά οφέλη στο νόμισμά μας. Το Ethereum είναι το blockchain με τον μεγαλύτερο αριθμό συναλλαγών ξεπερνώντας ακόμα και το Bitcoin [26]. Όσον αφορά μάλιστα τα blockchain που υποστηρίζουν smart contracts το Ethereum είναι με διαφορά το πιο διαδεδομένο blockchain, γεγονός που επιτρέπει στο ενεργειακό μας νόμισμα να έχει μία ευρεία βάση πιθανών χρηστών, ήδη γνώριμων με την πλατφόρμα, αλλά και να μπορεί να αλληλεπιδρά με μια ευρεία ποικιλία εφαρμογών και υπηρεσιών στο οικοσύστημα.



Εικόνα 3-1 Ο αριθμός συναλλαγών σε Ethereum και σε Bitcoin το 2022.
Πηγή: https://cointelegraph.com/news/ethereum-transactions-338-higher-in-2022-but-bitcoin-remains-most-popular

3.2.2 ERC-20 Standard

Το Atomcoin θα ακολουθεί το πρότυπο υλοποίησης token ERC-20. Έτσι θα του επιτραπεί η συμβατότητα με ήδη υπάρχοντες υποδομές όπως πορτοφόλια κρυπτονομισμάτων και άλλες εφαρμογές, αλλά θα είναι και ευκολότερο για τους δημιουργούς να αλληλεπιδρούν μαζί του.

3.2.3 Ρόλοι εφαρμογής

Από την περιγραφή της εφαρμογής καθορίζονται 2 τουλάχιστον διαφορετικοί ρόλοι που θα αλληλεπιδρούν με την εφαρμογή:

- Οι απλοί χρήστες, οι οποίοι είναι οι συμμετέχοντες στο πρόγραμμα επιβράβευσης και θα μπορούν να χρησιμοποιήσουν το νόμισμα όπως οποιοδήποτε άλλο νόμισμα, δηλαδή μεταφέροντας το και επιτρέποντας τη χρήση του σε έξυπνα συμβόλαια,
- Οι διαχειριστές, οι οποίοι έχουν την ευθύνη της ενημέρωσης των δεδομένων κατανάλωσης των χρηστών, της εξουσιοδότησης των χρηστών που μπορούν να λάβουν το νόμισμα και του καθορισμού της τιμής του νομίσματος.

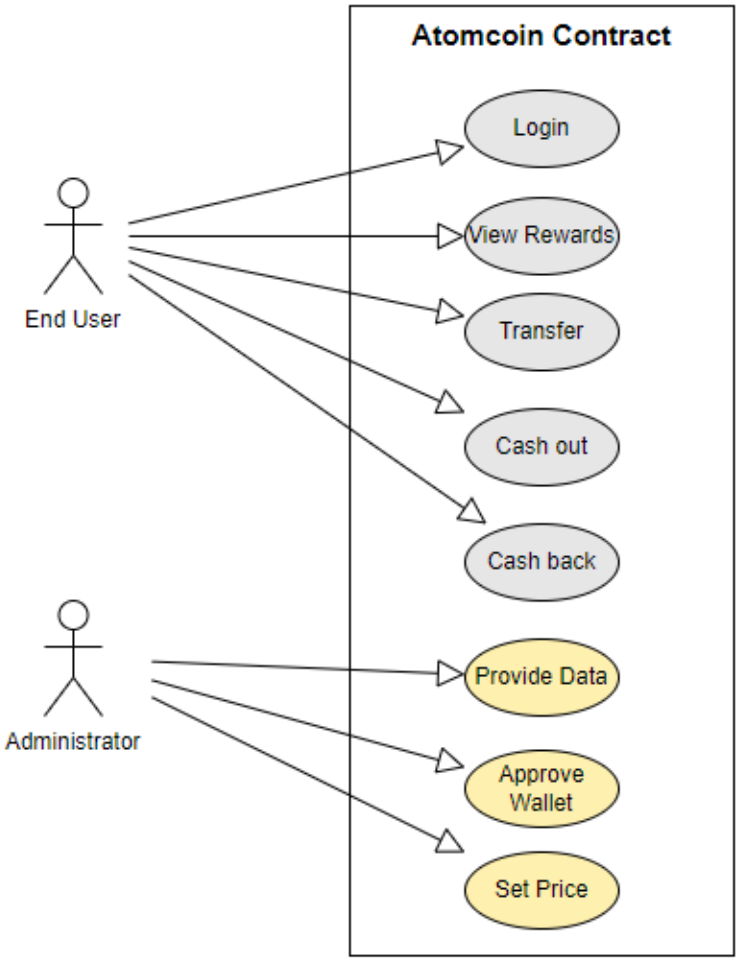
3.2.4 Αποτροπή ελεύθερης συναλλαγής νομίσματος

Από τη στιγμή που η τιμή του νομίσματος θα καθορίζεται από την εκδίδουσα αρχή σύμφωνα με τον τύπο (3.3), όπως παρουσιάστηκε παραπάνω, θα πρέπει να αποτρέπεται η ελεύθερη μεταφορά του νομίσματος από τους χρήστες, καθώς κάτι τέτοιο θα επέτρεπε τον καθορισμό μια διαφορετικής τιμής του νομίσματος η οποία θα καθοριζόταν από τη συμφωνηθείσα μεταξύ τους τιμή. Ένας τρόπος να αποφευχθεί αυτό είναι να ορίζονται στον κώδικα του smart contract οι διευθύνσεις των πορτοφολιών που μπορούν να λάβουν το νόμισμα, άλλα και να μπορεί να επαναστραφεί ο ορισμός μιας διεύθυνσης σε περίπτωση που παραβιάζει τους προβλεπόμενους κανόνες.

3.2.5 Ενημέρωση δεδομένων

Η εφαρμογή θα πρέπει να ενημερώνεται σε τακτικά και συχνά χρονικά διαστήματα με τα δεδομένα κατανάλωσης των χρηστών, ώστε να υπολογίζονται και να μοιράζονται τα νέα νομίσματα που θα αντιστοιχούν στις επιβραβεύσεις, καθώς και να υπολογίζεται και να αποθηκεύεται η ωρίαια τιμή του νομίσματος.

Στην εικόνα 3-2 παρουσιάζονται οι βασικές περιπτώσεις χρήσης που καλείται να ικανοποιήσει η εφαρμογή.



Εικόνα 3-2 Use Case Diagram της αποκεντρωμένης εφαρμογής

3.3 Αρχιτεκτονική Συστήματος

Για την πλήρη λειτουργία του συστήματος του Atomcoin εκτός του έξυπνου συμβολαίου είναι απαραίτητα και άλλα components, μια σύντομη περιγραφή τους παρουσιάζεται παρακάτω

User Interface

Το User Interface (UI) είναι βασικό κομμάτι του συστήματος. Συνδεόμενο με το έξυπνο συμβόλαιο μέσω της εφαρμογής πορτοφολιού Ethereum, Metamask, ή και άλλων αντίστοιχων εφαρμογών δίνει τη δυνατότητα στον χρήστη να αλληλεπιδρά με

την εφαρμογή και να διαχειρίζεται τα νομίσματά του και να παρακολουθεί το ιστορικό των κινήσεων του και των επιβραβεύσεών του, ώστε να προσαρμόζει την ενεργειακή του συμπεριφορά αναλόγως. Το UI , εκτός του smart contract, πρέπει να συνδέεται και με ένα backend server που θα χειρίζεται το παραδοσιακό κεντροποιημένο κομμάτι του συστήματος, δηλαδή τις αλληλεπιδράσεις των χρηστών που περιέχουν μεταβολές στο υπόλοιπο συμβατικών χρημάτων τους.

Backend Server

Για την ολοκληρωμένη λειτουργία της εφαρμογής είναι αναγκαία και η χρήση ενός backend το οποίο θα αναλαμβάνει κυρίως τη διεκπεραίωση λειτουργιών που μεταβάλλουν το υπόλοιπο συμβατικού συναλλάγματος του χρήστη, κατά την εξαργύρωση ή επιπλέον αγορά Atomcoin. Στα πλαίσια της παρούσας εργασίας έχει υλοποιηθεί ένας περιορισμένων δυνατοτήτων server που χρησιμοποιείται για τις λειτουργίες cash back και cash out της εφαρμογής.

Oracle

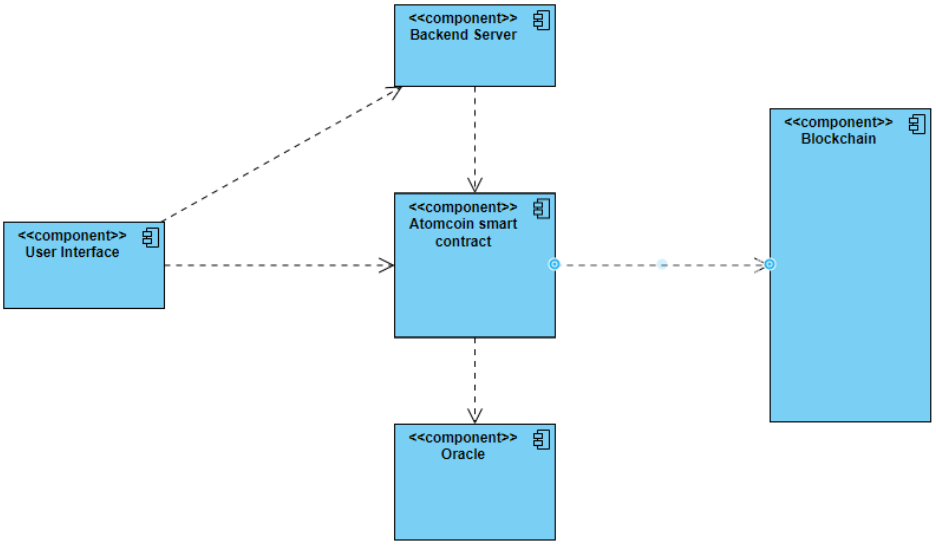
Μία κοινή δυσκολία που συναντιέται στην ανάπτυξη smart contracts είναι ο περιορισμός της επικοινωνίας τους με δεδομένα εκτός του blockchain. Ο μόνος τρόπος αντιμετώπισης αυτού του προβλήματος μέχρι στιγμής είναι η χρήση **oracles** τα οποία λειτουργούν ως γέφυρες μεταξύ του πραγματικού κόσμου και του blockchain. Τα oracles είναι υπηρεσίες οι οποίες γράφουν δεδομένα του πραγματικού κόσμου στο blockchain ώστε αυτά να γίνονται προσβάσιμα εντός του δικτύου. Από αυτό το γεγονός προκύπτει το πρόβλημα που είναι γνωστό ως «oracle problem» και αναφέρεται στο γεγονός ότι αυτές οι πηγές δεδομένων μπορούν να αποτελέσουν σημείο αποτυχίας στα κατά τα άλλα ντετερμινιστικά και απαραβίαστα smart contracts αφού πρέπει να εμπιστευτούν τα oracles ότι εισάγουν τα σωστά δεδομένα [27]. Στην εφαρμογή μας χρησιμοποιούμε oracle που εισάγει σε ωριαία βάση τα δεδομένα της κατανάλωσης των χρηστών στο smart contract ώστε αυτό να υπολογίσει το ποσό της επιβράβευσης ή ποινής του χρήστη.

Smart Contract

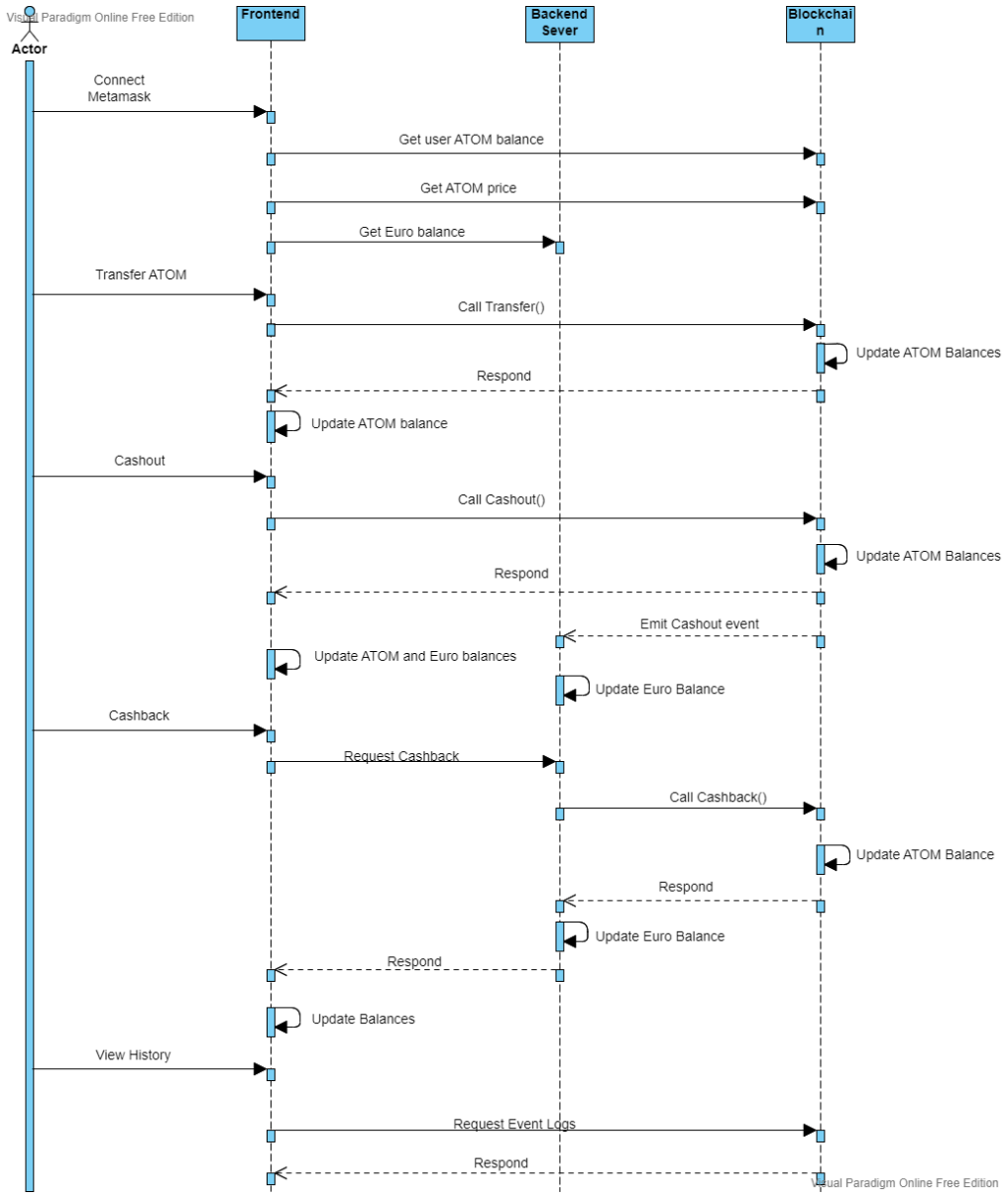
Το κυριότερο κομμάτι της εφαρμογής μας είναι βεβαίως το smart contract. Το smart contract συνδέεται με όλα τα παραπάνω συστατικά της εφαρμογής μας και αποτελεί τον πυρήνα της αποκεντρωμένης εφαρμογής μας. Στο smart contract υλοποιούνται όλες οι βασικές λειτουργίες του Atomcoin όπως αυτό παρουσιάζεται από τους Marinakis et al. Ως ένα αμετάβλητο σύνολο συναρτήσεων που ζει στο blockchain εγγυάται τη διαφάνεια, την εμπιστοσύνη και την ασφάλεια που προσφέρει η τεχνολογία blockchain.

Το component diagram της εικόνας 3-3 απεικονίζει τα βασικά components της εφαρμογής που θα υλοποιηθούν καθώς και την αλληλεπίδραση μεταξύ τους.

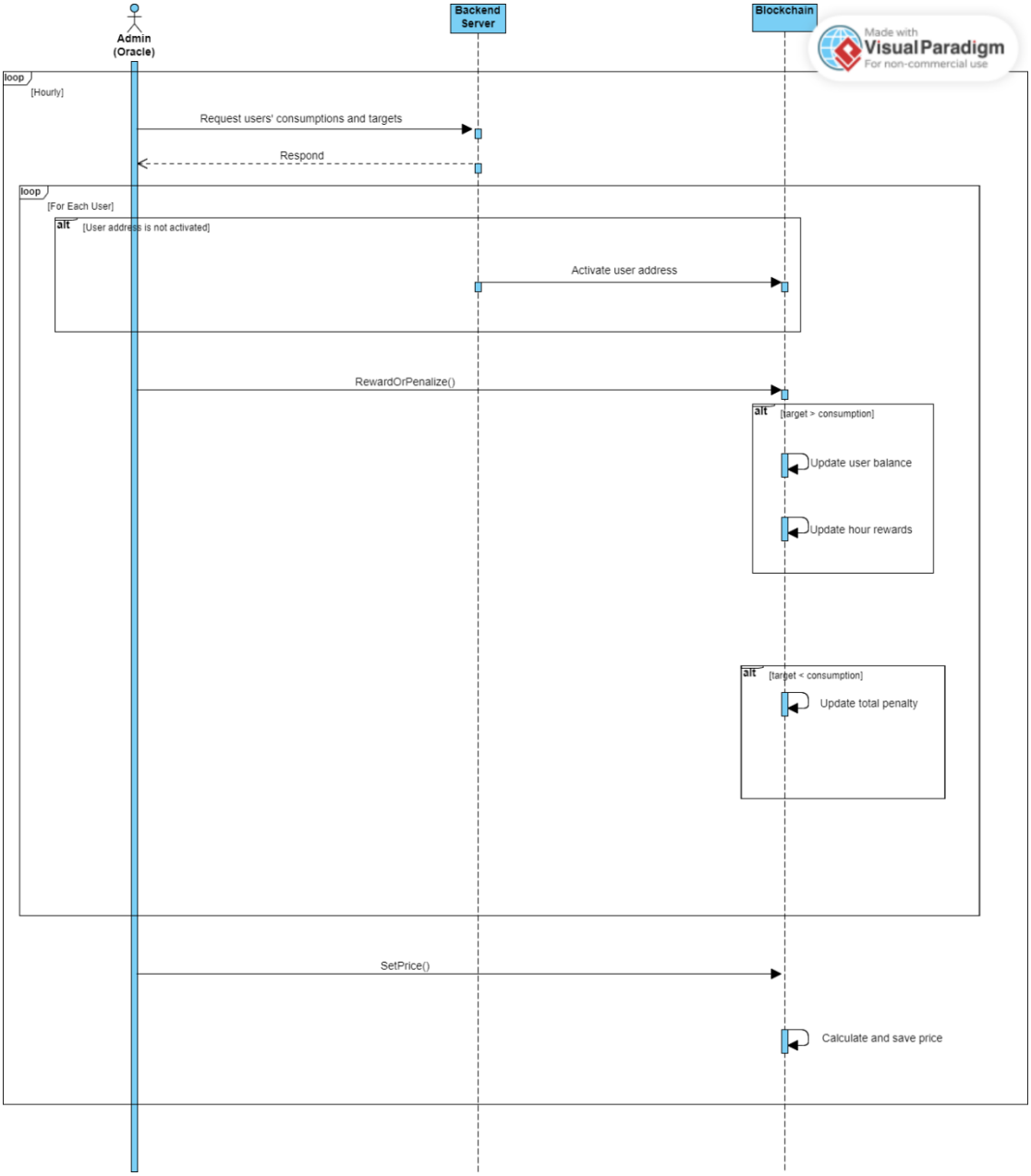
Τα sequence diagrams στις εικόνες 3-4 και 3-5 παρουσιάζουν την πλήρη αλληλεπίδραση χρήστη-components σε κάθε περίπτωση χρήσης.



Εικόνα 3-3 Το UML Component Diagram της εφαρμογής



Εικόνα 3-4 UML Sequence Diagram απλού χρήστη



Εικόνα 3-5 UML Sequence Diagram Oracle

Κεφάλαιο 4 Υλοποίηση της Εφαρμογής

4.1 Εργαλεία που χρησιμοποιήθηκαν

Κατά την ανάπτυξη της αποκεντρωμένης εφαρμογής του Atomcoin χρησιμοποιήθηκε μία ποικιλία εργαλείων και τεχνολογιών με σκοπό να διασφαλίζουν μια ασφαλή και φιλική προς το χρήστη πλατφόρμα. Τα εργαλεία που επιλέχθηκαν καλύπτουν όλο το φάσμα των απαιτούμενων λειτουργιών, από την αλληλεπίδραση με το blockchain μέχρι το σχεδιασμό του UI και τη διαχείριση του backend.

Παρακάτω θα εμβαθύνουμε στις ιδιαιτερότητες καθενός από αυτά τα εργαλεία, τους λόγους πίσω από την επιλογή τους και τον τρόπο με τον οποίο χρησιμοποιήθηκαν στη διαδικασία ανάπτυξης.

4.1.1 Geth (Go Ethereum)

Το Geth (Go Ethereum) είναι μία από τις τρεις αρχικές υλοποιήσεις (μαζί με τη C++ και την Python) του πρωτοκόλλου Ethereum [28]. Είναι γραμμένο στη γλώσσα προγραμματισμού Go και είναι το πιο δημοφιλές και ευρέως χρησιμοποιούμενο πρόγραμμα για τη διαχείριση κόμβων Ethereum. Προσφέρει μια ποικιλία χαρακτηριστικών, συμπεριλαμβανομένης της δυνατότητας δημιουργίας ιδιωτικών blockchain, κάτι που αξιοποιήσαμε για το έργο μας στο Atomcoin. Χρησιμοποιώντας το Geth στήθηκε ένα ιδιωτικό δίκτυο EVM με αλγόριθμο συναίνεσης Proof-of-Authority (PoA) και δύο κόμβους (nodes). Ο αλγόριθμος συναίνεσης PoA εξασφαλίζει γρήγορους χρόνους δημιουργίας block, ρυθμισμένο σε 1 block ανά 5 δευτερόλεπτα στην περίπτωσή μας, γεγονός που τον καθιστά κατάλληλο για περιβάλλον δοκιμών.

4.1.2 Remix IDE

Το Remix είναι ένα ισχυρό εργαλείο ανοιχτού κώδικα που βοηθά στη σύνταξη smart contracts γραμμένων σε Solidity απευθείας από το πρόγραμμα περιήγησής [29]. Διαθέτει ενσωματωμένο περιβάλλον εντοπισμού σφαλμάτων και δοκιμών και μπορεί να αλληλεπιδράσει άμεσα με το blockchain Ethereum, γεγονός που το καθιστά εξαιρετικό εργαλείο τόσο για αρχάριους που μαθαίνουν το Solidity όσο και για έμπειρους προγραμματιστές. Στο project μας χρησιμοποιήθηκε για την ανάπτυξη του smart contract του Atomcoin.

4.1.3 Truffle

Το Truffle είναι ένα περιβάλλον ανάπτυξης και πλαίσιο δοκιμών για το Ethereum, καθιστώντας το μια ολοκληρωμένη σουίτα για προγραμματιστές Ethereum [30]. Επιτρέπει στους προγραμματιστές να συντάσσουν, να αναπτύσσουν και να μεταγλωττίζουν (compile) και να εγκαθιστούν (deploy) έξυπνα συμβόλαια τόσο σε τοπικά όσο και σε δημόσια δίκτυα Ethereum. Στην παρούσα εργασία το Truffle

χρησιμοποιήθηκε για να εγκατασταθεί το smart contract που αναπτύχθηκε στο δοκιμαστικό blockchain.

```
module.exports = {

  networks: {
    development: {
      host: "127.0.0.1",     // Localhost (default: none)
      port: 8545,            // Standard Ethereum port (default: none)
      network_id: "14333",       // Any network (default: none)
      from: "0x6Ce4B585168b5016376FD1944aA8263D4D8c03e3",
      gas: 4600000,
      gasPrice: 0
    }
  },

  contracts_build_directory: "./../frontend/src/contracts",

  // Configure your compilers
  compilers: {
    solc: {
      version: "0.8.10",    // Fetch exact version from solc-bin (default: truffle's version)
    }
  },
};
```

Εικόνα 4-1 Η παραμετροποίηση του Truffle για σύνδεση στο τοπικό δίκτυο Ethereum

4.1.3 React.js

Η React.js, που συχνά αναφέρεται απλώς ως React, είναι μια ισχυρή βιβλιοθήκη JavaScript ανοιχτού κώδικα για την ανάπτυξη περιβάλλοντος διεπαφών χρήστη (user interfaces), ιδιαίτερα εφαρμογών μιας σελίδας [31]. Αναπτύχθηκε από το Facebook, το React επιτρέπει στους προγραμματιστές να δημιουργούν μεγάλες εφαρμογές Ιστού που μπορούν να αλλάξουν δεδομένα, χωρίς να φορτώσουν ξανά τη σελίδα. Στο πλαίσιο της παρούσας διπλωματικής η React χρησιμοποιήθηκε για την ανάπτυξη του user interface, για τη σύνδεση δηλαδή του χρήστη της εφαρμογής με το smart contract.

4.1.4 Metamask

Το MetaMask είναι ένα λογισμικό πορτοφολιού κρυπτονομισμάτων που χρησιμοποιείται για την αλληλεπίδραση με το Ethereum [32]. Επιτρέπει στους χρήστες να έχουν πρόσβαση στο πορτοφόλι Ethereum μέσω μιας επέκτασης προγράμματος περιήγησης (browser extension) ή μιας εφαρμογής για κινητά, δίνοντάς τους τη δυνατότητα να αποθηκεύουν, να στέλνουν και να λαμβάνουν Ether και ERC-20 νομίσματα. Επιτρέπει επίσης στο χρήστη να συνδεθεί με το δίκτυο Ethereum μέσω του browser του και με αυτόν τον τρόπο να αλληλεπιδράσει με το smart contract του Atomcoin απευθείας μέσω του UI.

4.1.5 Node.js

Το Node.js είναι ένα περιβάλλον εκτέλεσης JavaScript ανοιχτού κώδικα, που εκτελείται στη μηχανή V8 και εκτελεί κώδικα JavaScript εκτός προγράμματος περιήγησης [33]. Χρησιμοποιείται κυρίως για τη δημιουργία web servers, εργαλείων δικτύωσης και εφαρμογών σε πραγματικό χρόνο λόγω της non-blocking αρχιτεκτονικής. Το Node.js χρησιμοποιήθηκε στην ανάπτυξη της εφαρμογής μας σε 2 περιπτώσεις:

- Χρησιμοποιήθηκε για τη δημιουργία του backend server ο οποίος όπως εξηγήθηκε παραπάνω έχει συμμετοχή στις λειτουργίες cash back και cash out του smart contract.
- Χρησιμοποιήθηκε επίσης για τη δημιουργία του Oracle που φορτώνει τα νέα δεδομένα στο blockchain ώστε να υπολογίζεται το ποσό επιβράβευσης των χρηστών.

4.1.6 Express.js

Το Express.js είναι ένα γρήγορο, ανεπιτήδευτο και μινιμαλιστικό πλαίσιο ιστού για το Node.js [34]. Χρησιμοποιείται ευρέως για την κατασκευή ιστοσελίδων και APIs λόγω της απλότητας, ευελιξίας και κλιμακωσιμότητάς του. Στο πλαίσιο της εφαρμογής του Atomcoin χρησιμοποιήθηκε για τη δημιουργία του API στο backend server που διαχειρίζεται την αίτηση ενός χρήστη για cash back.

4.1.7 Web3.js

Το Web3.js είναι μια συλλογή βιβλιοθηκών που επιτρέπουν την αλληλεπίδραση με έναν τοπικό ή απομακρυσμένο κόμβο Ethereum χρησιμοποιώντας HTTP, IPC ή WebSocket [35]. Διαδραματίζει κρίσιμο ρόλο στο οικοσύστημα Ethereum, καθώς επιτρέπει στους προγραμματιστές να χρησιμοποιούν JavaScript καιν να μπορούν να αλληλεπιδρούν με έξυπνα συμβόλαια και να έχουν πρόσβαση σε δεδομένα στο blockchain. Στην ανάπτυξη της εφαρμογής το Web3.js χρησιμοποιήθηκε τόσο στο UI όσο και στο Backend server και στο Oracle για την επικοινωνία των προγραμμάτων με το smart contract του Atomcoin.

4.1.7 Visual Paradigm

Το Visual Paradigm είναι μια ολοκληρωμένη λύση λογισμικού που παρέχει ένα πλήρες φάσμα εργαλείων για το σχεδιασμό, την τεκμηρίωση και την κατασκευή συστημάτων λογισμικού [36]. Τα χαρακτηριστικά του περιλαμβάνουν μοντελοποίηση Unified Modeling Language (UML), Modeling Business Process (BPMN), μοντελοποίηση δεδομένων και άλλα. Στο πλαίσιο του Atomcoin το Visual Paradigm χρησιμοποιήθηκε για τη δημιουργία των διαγραμμάτων που χρησιμοποιούνται για την επεξήγηση της λειτουργίας της εφαρμογής στο παρόν έγγραφο.

4.2 Ανάλυση Έξυπνου Συμβολαίου

Σε αυτήν την ενότητα, εμβαθύνουμε στα θεμέλια του βασικού μας έξυπνου συμβολαίου, του Atomcoin. Αυτό το smart contract, γραμμένο σε Solidity αποτελεί τον πυρήνα της αποκεντρωμένης εφαρμογής μας.

Παρακάτω θα αναφέρουμε λεπτομερώς τις κυριότερες λειτουργίες και μεταβλητές που περιλαμβάνονται στο συμβόλαιο Atomcoin, παρέχοντας μια ολοκληρωμένη κατανόηση των εσωτερικών λειτουργιών του.

4.2.1 Βασικές μεταβλητές

- ***uint256 public TOTAL_BUDGET;***
  uint256 public TOTAL_TARGET;
  uint256 public TOTAL_HOURS;

Οι παραπάνω μεταβλητές ορίζονται κατά τη δημιουργία του smart contract και θεωρούνται σταθερές κατά τη διάρκεια ζωής του προγράμματος. Αντιπροσωπεύουν αντίστοιχα το συνολικό χρηματικό ποσό που θα διατεθεί στο πρόγραμμα, τις συνολικές μονάδες ενέργειας σε kwh που έχει ως στόχο το πρόγραμμα να εξοικονομηθούν και τέλος το συνολικό αριθμό ωρών ζωής του προγράμματος.

- ***uint256 public KWH_PRICE;***

Η μεταβλητή KWH_PRICE ορίζεται επίσης κατά τη δημιουργία του smart contract και δίνεται η δυνατότητα στους διαχειριστές της εφαρμογής να τη μεταβάλουν μέσω της συνάρτησης updateEnergyPrice.

- ***mapping(address => bool) public approved;***

Το παραπάνω mapping αντιστοιχίζει μια διεύθυνση πορτοφολιού τύπου Ethereum σε μία Boolean τιμή που υποδεικνύει αν η εν λόγω διεύθυνση είναι εξουσιοδοτημένη να λαμβάνει Atomcoin.

- ***mapping(uint256 => uint256) public priceHistory;***

Το mapping priceHistory χρησιμοποιείται για την αποθήκευση της τιμής του νομίσματος κάθε ώρα. Σαν key δίνεται η ώρα λειτουργίας του προγράμματος και σαν value ή αντίστοιχη τιμή που έχει υπολογιστεί για τη συγκεκριμένη ώρα.

- ***mapping(uint256 => uint256) public hourCashOuts;***
  mapping(uint256 => uint256) public hourCashBacks;
  mapping(uint256 => uint256) public hourRewards;

Τα παραπάνω mappings, στην ίδια λογική με την ωριαία τιμή, κρατάνε τα δεδομένα για τα cash backs, τα cash outs και τα rewards που δόθηκαν συνολικά, ανά ώρα προγράμματος. Σαν key του mapping λοιπόν δίνεται η ώρα προγράμματος και σαν value το συνολικό ποσό κάθε περίπτωσης.

- ***uint256 public totalPenalty;***

Η τιμή totalPenalty κρατάει το συνολικό αριθμό μονάδων ενέργειας που έχουν ξεπεράσει τους επιμέρους στόχους κατανάλωσης όλοι οι χρήστες από την αρχή του προγράμματος.

Οι μεταβλητές που παρουσιάστηκαν παραπάνω είναι εκείνες που χρειάζονται στο smart contract για τον υπολογισμό της τιμής σε κάθε χρονική στιγμή, όπως είδαμε και από τον τύπο υπολογισμού της τιμής στο προηγούμενο κεφάλαιο.

4.2.2 Βασικές συναρτήσεις

- ***constructor(uint256 _totalBudget, uint256 _totalTarget, uint256 _totalHours, uint256 _kwhPrice) ERC20("Atomcoin", "ATOM")***

Η συνάρτηση του constructor αρχικοποιεί την κατάσταση του smart contract όταν αυτό δημιουργείται στο blockchain. Σε αυτή τη συνάρτηση δηλώνουμε ότι το smart contract μας είναι ένα ERC-20 token χρησιμοποιώντας τη βιβλιοθήκη ERC20.sol [37] του OpenZeppelin [38] και δηλώνουμε την ονομασία του νομίσματος και το διακριτικό του. Στο σώμα της συνάρτησης αρχικοποιούμε τις μεταβλητές TOTAL_BUDGET, TOTAL_TARGET, TOTAL_HOURS, KWH_PRICE με τις τιμές που δίνει ο χρήστης κατά τη δημιουργία του smart contract. Επίσης δίνουμε στον δημιουργό τον ρόλο Admin χρησιμοποιώντας τη βιβλιοθήκη AccesControl.sol [39] πάλι του OpenZeppelin.

- ***function approveWallet(address account) public onlyAdmin***

Η συνάρτηση αυτή καλείται μόνο από κάποιον χρήστη που έχει ρόλο ‘Admin’ και ενεργοποιεί τη διεύθυνση που δίνεται ως όρισμα ώστε να μπορεί να λάβει Atomcoin. Πρέπει να κληθεί για κάθε διεύθυνση πριν τη μεταφορά του νομίσματος για πρώτη φορά σε αυτή τη διεύθυνση. Στην ίδια λογική υπάρχει και η αντίθετή της, η revokeApproval για να μπλοκάρει κάποιο πορτοφόλι από το να μπορεί να λάβει το νόμισμα.

- ***function transfer(address recipient, uint256 amount) public onlyApproved(msg.sender) onlyApproved(recipient) override returns (bool)***

Η συνάρτηση transfer που δίνεται από το ERC20 πρότυπο για τη μεταφορά του νομίσματος τροποποιείται ώστε να επιτρέπεται μόνο όταν τόσο ο αποδέκτης όσο και ο αποστολέας είναι εγκεκριμένοι χρήστες. Το ίδιο ισχύει και για την transferFrom.

- ***function rewardOrPenalise(address recipient, uint256 limit, uint256 consumption) public onlyAdmin onlyActiveHours returns (uint256)***

Αφού δίνονται σαν ορίσματα από το Oracle τα δεδομένα που αφορούν την κατανάλωση και το όριο κατανάλωσης ενός χρήστη, το σώμα της συνάρτησης αυτής ελέγχει εάν ο χρήστης πέτυχε εξοικονόμηση ενέργειας. Σε περίπτωση που η κατανάλωση του είναι κάτω από το όριο, ενημερώνεται η τιμή του hourRewards για τη συγκεκριμένη ώρα και δημιουργούνται νέα νομίσματα Atomcoin που αποστέλονται στον χρήστη. Εάν η κατανάλωση του χρήστη υπερβαίνει το όριο που του έχει δοθεί αυξάνεται η μεταβλητή totalPenalty κατά το ποσό της υπέρβασης.

Σε περίπτωση επιβράβευσης δημιουργείται από το smart contract ένα event Reward και σε περίπτωση ποινής ένα event Penalty.

- ***function cashOut(uint256 amount) public onlyApproved(msg.sender) onlyActiveHours***

Αυτό το κομμάτι εκτελείται όταν ένας χρήστης εξαργυρώνει νομίσματα. Με το όρισμα amount αναφέρεται ο αριθμός νομισμάτων που ο χρήστης εξαργυρώνει.

Τα νομίσματα αυτά «καίγονται», δηλαδή αποσύρονται από την κυκλοφορία και η μεταβλητή hourCashOuts της συγκεκριμένης ώρας αυξάνεται κατά αυτό το ποσό.

Τέλος δημιουργείται από το smart contract ένα νέο event Cash Out.

- ***function cashBack(address recipient, uint256 fiatAmount) public onlyAdmin***

Αντίστοιχα αυτή η συνάρτηση εκτελείται όταν ένας χρήστης κάνει αγοράζει νέα νομίσματα. Αυτή η ενέργεια γίνεται μέσω του backend server αφού απαιτεί τη δημιουργία νέων νομισμάτων και τη μεταφορά τους στον χρήστη ενέργειες που επιτρέπονται μόνο από έναν Admin. Υπολογίζεται λοιπόν εντός της συνάρτηση ο αριθμός νομισμάτων που ο χρήστης δικαιούται, με βάση την τιμή του νομίσματος, και νέα νομίσματα δημιουργούνται και μεταφέρονται στον χρήστη. Ενημερώνεται η ωριαία τιμή των cash backs και τέλος δημιουργείται ένα event CashBack.

- ***function setPrice() public onlyAdmin onlyActiveHours***

Με βάση τις τιμές των μεταβλητών και τον τύπο (3.3) του προηγούμενου κεφαλαίου υπολογίζεται και αποθηκεύεται η ωριαία τιμή του νομίσματος αφού το Oracle

καλέσει τη συνάρτηση setPrice. Ο λόγος που απαιτείται η αποθήκευση της ωριαίας τιμής είναι ότι πρέπει να χρησιμοποιηθεί για τον υπολογισμό της τιμής της επόμενης ώρας. Διαφορετικά θα χρειαζόταν να υπολογιστεί αναδρομικά, γεγονός που θα καθιστούσε απαγορευτικό τον υπολογισμό, λόγω του κόστους που θα κατανάλωνε.

```
function setPrice() public onlyAdmin onlyActiveHours {
    _currentHour = getCurrentHour();
    _currentDay = getCurrentDay();
    _commonFactor = (KWH_PRICE.mul(TOTAL_BUDGET)).div(TOTAL_TARGET).div(2);
    _firstNumerator = 0;
    _firstDenominator = 0;
    _secondNumerator = 0;
    _secondDenominator = 0;

    uint256 reg = TOTAL_BUDGET.mul(totalPenalty).div(TOTAL_TARGET);

    for (uint256 i = 0; i < _currentHour; i = i.add(1)) {
        uint256 prevHourCashOuts = i > 0 ? hourCashOuts[i.sub(1)] : 0;
        uint256 prevHourCashBacks = i > 0 ? hourCashBacks[i.sub(1)] : 0;
        uint256 thisHourRewards = hourRewards[i];

        uint256 prevHourPrice = i > 0 ? getPrice(i.sub(1)) : KWH_PRICE;
        uint256 fac = prevHourCashOuts > prevHourCashBacks ? (prevHourPrice.mul(prevHourCashOuts.sub(prevHourCashBacks))).div(10 ** decimals()) : 0;

        if (_firstNumerator.add(thisHourRewards).add(prevHourCashBacks) > prevHourCashOuts) {
            _firstNumerator = _firstNumerator.add(thisHourRewards).add(prevHourCashBacks).sub(prevHourCashOuts);
        }
        if (_firstDenominator.add(HOUR_BUDGET).add(reg) > fac) {
            _firstDenominator = _firstDenominator.add(HOUR_BUDGET).add(reg).sub(fac);
        }
    }

    uint256 limit = _currentHour > 120 ? 120 : _currentHour;
    uint256 start = _currentHour > 1 ? _currentHour.sub(1) : 1;

    for (uint256 i = start; i > _currentHour.sub(limit); i = i.sub(1)) {
        _secondNumerator = _secondNumerator.add(hourRewards[i]);
        _secondDenominator = _secondDenominator.add(HOUR_BUDGET);
    }

    uint256 firstAddend = (_commonFactor.mul(_firstNumerator)).div(_firstDenominator);
    uint256 secondAddend = (_commonFactor.mul(_secondNumerator)).div(_secondDenominator);

    uint256 price = firstAddend.add(secondAddend);
    priceHistory[_currentHour] = price;

    emit PriceSet(price, block.timestamp.div(60), block.timestamp);
}
```

Εικόνα 4-2 Η συνάρτηση υπολογισμού της τιμής

4.3 Υλοποίηση Backend Server και Oracle

Σε αυτή την ενότητα θα εμβαθύνουμε στο διπλή λειτουργία του κομματιού του συστήματος που δημιουργήθηκε σε περιβάλλον Node.js και αφορά τις λειτουργίες του backend server και του oracle.

4.3.1 Backend

Ο backend server αποτελεί ένα σημαντικό μέρος του συστήματος που δημιουργήθηκε για να διευκολύνει κάποιες βασικές αλληλεπιδράσεις μεταξύ του frontend που χειρίζεται ο χρήστης και του έξυπνου συμβολαίου που βρίσκεται στο

blockchain Ethereum. Με τη χρήση της βιβλιοθήκης Express.js στήθηκε ένα RESTful API που συντίθεται από 2 βασικά endpoints για την εξυπηρέτηση δύο λειτουργιών της εφαρμογής:

1. **User Cashback Endpoint:** Αυτό το endpoint απευθύνεται σε χρήστες που θέλουν να χρησιμοποιήσουν την επιλογή Cash back του έξυπνου συμβολαίου και να αγοράσουν περισσότερα νομίσματα. Όταν λαμβάνεται από το frontend ένα αίτημα POST που περιέχει στο σώμα το ποσό σε Ευρώ που θέλει ο χρήστης να ξοδέψει σε νέα νομίσματα και τη διεύθυνση πορτοφολιού του χρήστη, γίνεται από το backend μία κλήση της συνάρτησης cashback του smart contract. Η κλήση αυτή γίνεται με τη χρήση της βιβλιοθήκης web3.js και χρησιμοποιείται μία διεύθυνση πορτοφολιού με δικαιώματα Admin στο smart contract. Στο τέλος επιστρέφεται απάντηση στο frontend με το αποτέλεσμα της συναλλαγής.
2. **Data Upload Endpoint:** Αυτό το endpoint έχει υλοποιηθεί για χρήση από το frontend ενός χρήστη με δικαιώματα Admin. Επιτρέπει σε έναν διαχειριστή να ανεβάσει ένα αρχείο Excel, κάθε σειρά του οποίου περιέχει συγκεκριμένα δεδομένα χρήστη, όπως τη διεύθυνση πορτοφολιού του χρήστη, την αναμενόμενη κατανάλωση ενέργειας και την πραγματική κατανάλωση ενέργειας. Κατά τη μεταφόρτωση, ο διακομιστής αναλύει αυτά τα δεδομένα και επαναλαμβάνει για κάθε σειρά κλήση της συνάρτησης rewardOrPenalize του smart contract . Αυτό το τελικό σημείο επιτρέπει ουσιαστικά την αποτελεσματική ομαδική επεξεργασία ανταμοιβών ή κυρώσεων για πολλούς χρήστες σε μία μόνο λειτουργία.

4.3.2 Oracle

Το τρίτο κρίσιμο κομμάτι του συστήματος είναι το Oracle. Όπως περιγράφηκε προηγουμένως, η λειτουργία ενός Oracle στα πλαίσια του blockchain είναι να επιτελεί το ρόλο μιας γέφυρας δεδομένων μεταξύ του εξωτερικού κόσμου και του κόσμου του blockchain. Αντίστοιχη είναι και η λειτουργία του στην εφαρμογή μας. Ανά διαστήματα μίας ώρας με τη χρήση της βιβλιοθήκης web3.js και μέσω του ίδιου πορτοφολιού διαχειριστή που χρησιμοποιείται και στο backend καλούνται οι εξής συναρτήσεις του smart contract:

1. **setPrice:** Όπως εξηγήθηκε νωρίτερα στο κεφάλαιο η ωριαία τιμή του Atomcoin πρέπει να αποθηκεύεται διότι χρησιμοποείται σε μελλοντικούς υπολογισμούς της τιμής του, και για να γίνει αυτή η αποθήκευση πρέπει να ξεκινήσει ένα transaction που θα καλεί τη συνάρτηση του smart contract.

2. **rewardOrPenalize:** Το Oracle διαβάζει τα δεδομένα κατανάλωσης των χρηστών και τα εισάγει στο smart contract καλώντας τη συνάρτηση rewardOrPenalize για να υπολογιστούν και να διανεμηθούν οι αντίστοιχες επιβραβεύσεις ή ποινές.

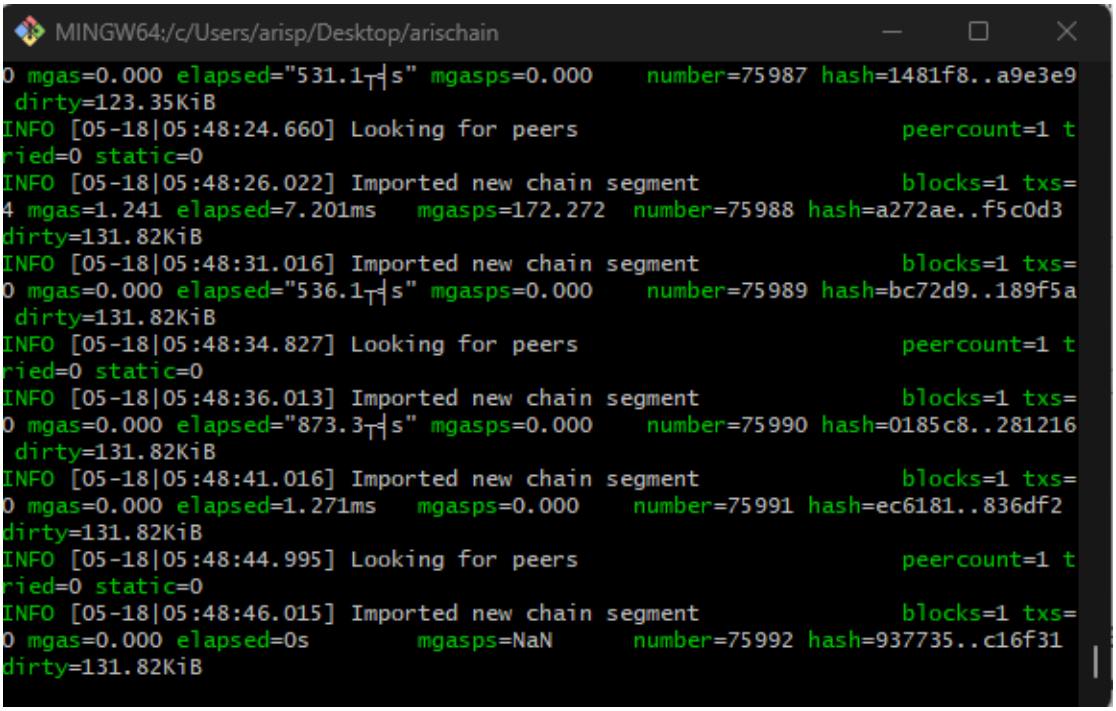
4.4 Τοπικό δίκτυο Ethereum Blockchain

Η εφαρμογή αναπτύχθηκε χρησιμοποιώντας ένα ιδιωτικό Ethereum blockchain. Ένα ιδιωτικό blockchain είναι ένα απομονωμένο δίκτυο κόμβων Ethereum που δεν είναι συνδεδεμένο στο κύριο δίκτυο Ethereum. Οι κόμβοι σε ένα ιδιωτικό δίκτυο επεξεργάζονται μόνο συναλλαγές και smart contracts εντός του δικτύου, το οποίο παρέχει ένα ασφαλές και ελεγχόμενο περιβάλλον που είναι ιδανικό για ανάπτυξη και δοκιμή.

Η δημιουργία ενός ιδιωτικού blockchain για την ανάπτυξη εφαρμογών έχει πολλά πλεονεκτήματα. Επιτρέπει γρήγορες επαναλήψεις, εντοπισμό σφαλμάτων και δοκιμές χωρίς το κόστος που σχετίζεται με την ανάπτυξη και την εκτέλεση συμβολαίων στο δημόσιο δίκτυο Ethereum. Επιπλέον, δεδομένου ότι το δίκτυο είναι ιδιωτικό, ο προγραμματιστής της εφαρμογής έχει τον πλήρη έλεγχο των συνθηκών δικτύου.

Στην περίπτωση αυτής της εφαρμογής, το ιδιωτικό blockchain δημιουργήθηκε χρησιμοποιώντας το Go Ethereum (Geth), μία από τις τρεις αρχικές υλοποιήσεις του πρωτοκόλλου Ethereum. Το Geth χρησιμοποιείται ευρέως για τη δημιουργία ιδιωτικών blockchains επειδή είναι ανοιχτού κώδικα, διαθέτει ισχυρή τεκμηρίωση και μια ισχυρή κοινότητα προγραμματιστών.

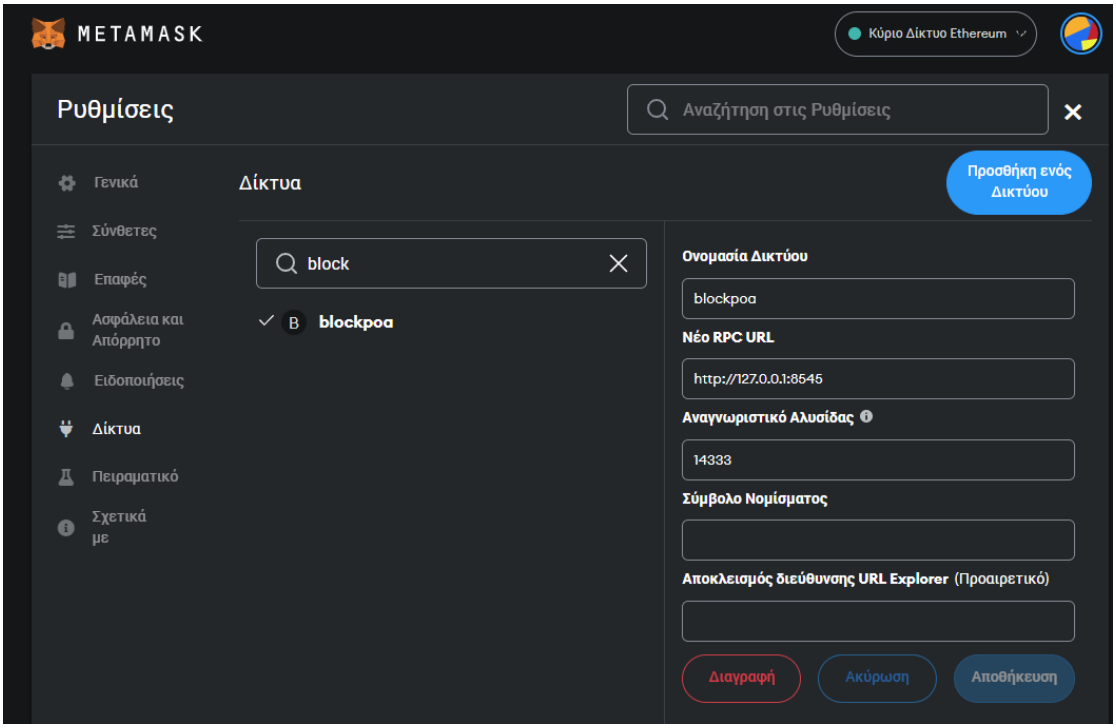
Το δίκτυο δημιουργήθηκε με δύο κόμβους Ethereum, στον καθένα από τους οποίους εκχωρήθηκε ένα μοναδικό αναγνωριστικό δικτύου και αριθμός θύρας. Οι κόμβοι επικοινωνούσαν μεταξύ τους μέσω ενός bootnode, ενός κόμβου που διευκολύνει την ανακάλυψη άλλων κόμβων στο δίκτυο. Ένας από τους κόμβους ρυθμίστηκε επίσης για εξόρυξη blocks, γεγονός που εξασφάλιζε ότι οι συναλλαγές που αποστέλλονταν στο δίκτυο επιβεβαιώθηκαν και προστέθηκαν στην αλυσίδα block.



Εικόνα 4-3 Παράδειγμα Logs του κόμβου που κάνει εξόρυξη block

Στο ιδιωτικό δίκτυο Ethereum, ο μηχανισμός συναίνεσης που επιλέχθηκε ήταν το Proof of Authority (PoA). Σε αντίθεση με το Proof of Work ή το Proof of Stake, το PoA δεν απαιτεί κόμβους για να λύσουν σύνθετα μαθηματικά προβλήματα ή να ποντάρουν ένα συγκεκριμένο ποσό Ether. Αντίθετα, σε μια συναίνεση PoA, οι συναλλαγές και τα μπλοκ επικυρώνονται από εγκεκριμένους λογαριασμούς, γνωστούς ως validators. Αυτός ο συμβιβασμός γίνεται για να προσφερθεί στον προγραμματιστή ένα περιβάλλον γρήγορης δημιουργίας block, στην περίπτωση μας ορίστηκε χρόνος ανά block 5 sec.

Στην εικόνα 4-4 φαίνεται η εισαγωγή του δοκιμαστικού τοπικού δικτύου στο πορτοφόλι Metamask ενώ στην εικόνα 4-5 δίνεται η παραμετροποίηση που χρησιμοποιήθηκε για τη δημιουργία του δικτύου.



Εικόνα 4-4 Η εισαγωγή του ιδιωτικού δικτύου στο Metamask

```
{
  "config": {
    "chainId": 14333,
    "homesteadBlock": 0,
    "eip150Block": 0,
    "eip150Hash": "0x0000000000000000000000000000000000000000000000000000000000000000",
    "eip155Block": 0,
    "eip158Block": 0,
    "byzantiumBlock": 0,
    "constantinopleBlock": 0,
    "petersburgBlock": 0,
    "istanbulBlock": 0,
    "clique": {
      "period": 5,
      "epoch": 30000
    }
  },
  "nonce": "0x0",
  "timestamp": "0x61bfe2fe",
  "extraData":
"0x0000000000000000000000000000000000000000000000000000000000000000006ce4b585168b5016376fd
1944aa8263d4d8c03e3000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000",
  "gasLimit": "0x47b760",
  "difficulty": "0x1",
  "mixHash": "0x0000000000000000000000000000000000000000000000000000000000000000",
  "coinbase": "0x0000000000000000000000000000000000000000",
  "alloc": {
    "6ce4b585168b5016376fd1944aa8263d4d8c03e3": {
      "balance": "0x200000000000000000000000000000000000000000000000000000000000000000"
    },
    "ff874cf65e0982349a14f09d64eabcaad841e1a0": {
      "balance": "0x200000000000000000000000000000000000000000000000000000000000000000"
    }
  },
  "number": "0x0",
  "gasUsed": "0x0",
  "parentHash": "0x0000000000000000000000000000000000000000000000000000000000000000",
  "baseFeePerGas": null
}
```


Εικόνα 4-5 Παραμετροποίηση του ιδιωτικού δικτύου Ethereum

Κεφάλαιο 5 Λειτουργία της Εφαρμογής

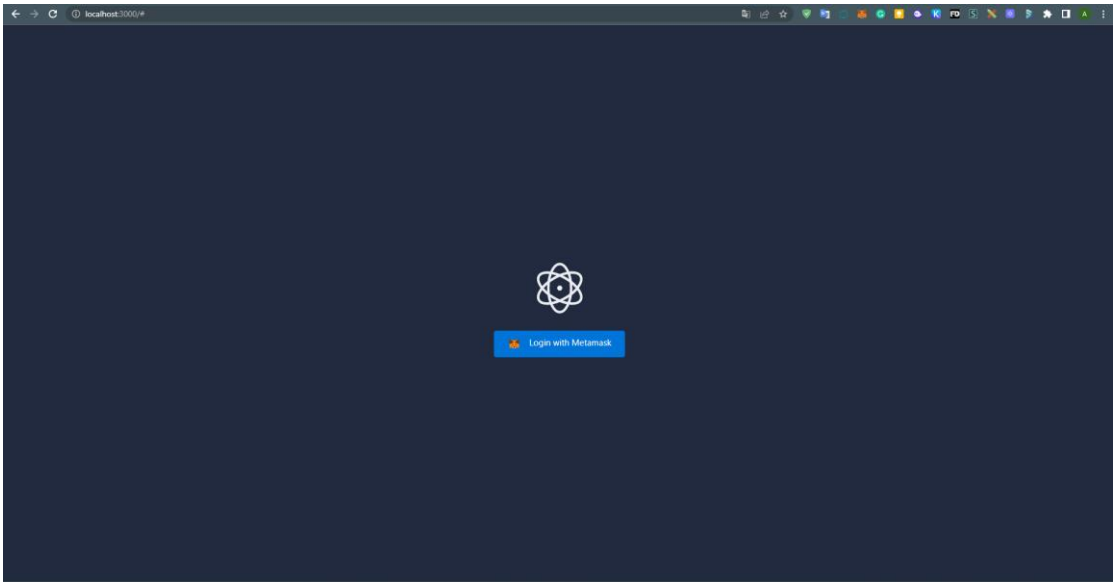
5.1 Εισαγωγή

Στο κεφάλαιο αυτό θα γίνει μια παρουσίαση της λειτουργίας της εφαρμογής κατά την περίοδο ενός προγράμματος επιβράβευσης, με τη βοήθεια του user interface που δημιουργήθηκε στα πλαίσια της διπλωματικής με χρήση της βιβλιοθήκης ReactJS. Το frontend της εφαρμογής συνδέεται τόσο με το έξυπνο συμβόλαιο του Atomcoin με τη χρήση του πορτοφολιού Metamask, με το οποίο ο χρήστης μπορεί να υπογράψει συναλλαγές με το έξυπνο συμβόλαιο, όσο και με τον backend εξυπηρετητή του συστήματος με τη χρήση του API που αυτός παρέχει.

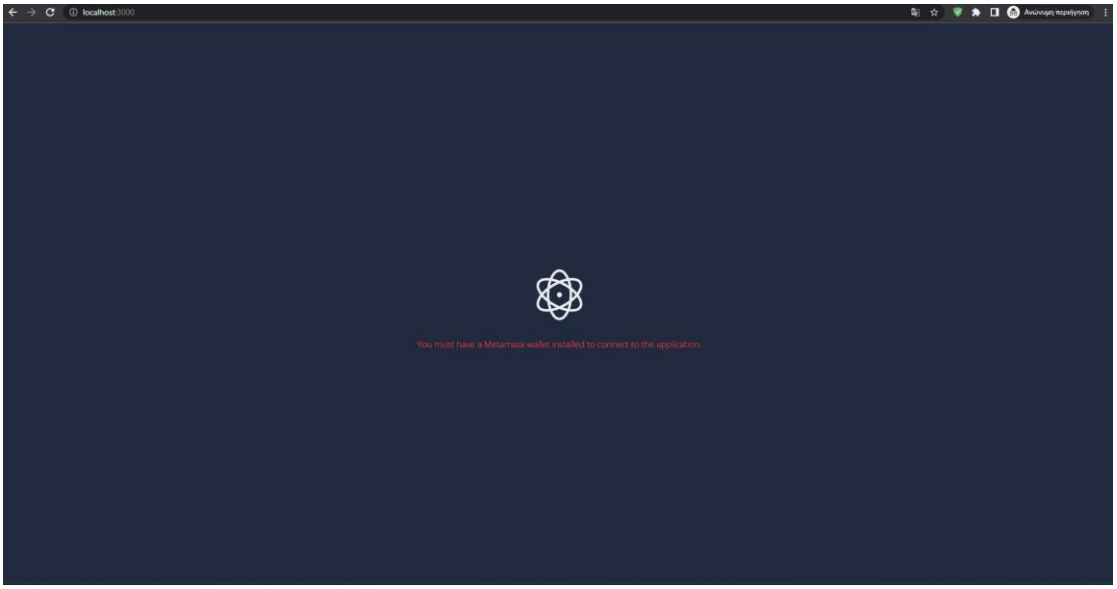
5.2 Λειτουργία απλού χρήστη

5.2.1 Σελίδα Login

Κατά την πρώτη επίσκεψη του χρήστη στην εφαρμογή του ζητείται να συνδεθεί σε αυτή (Εικόνα 5-1), με τη χρήση του πορτοφολιού Metamask εάν αυτό βρίσκεται εγκατεστημένο στον browser του, αλλιώς του εμφανίζεται ένα μήνυμα που εξηγεί ότι είναι απαραίτητη η χρήση του Metamask για να συνεχίσει (Εικόνα 5-2).

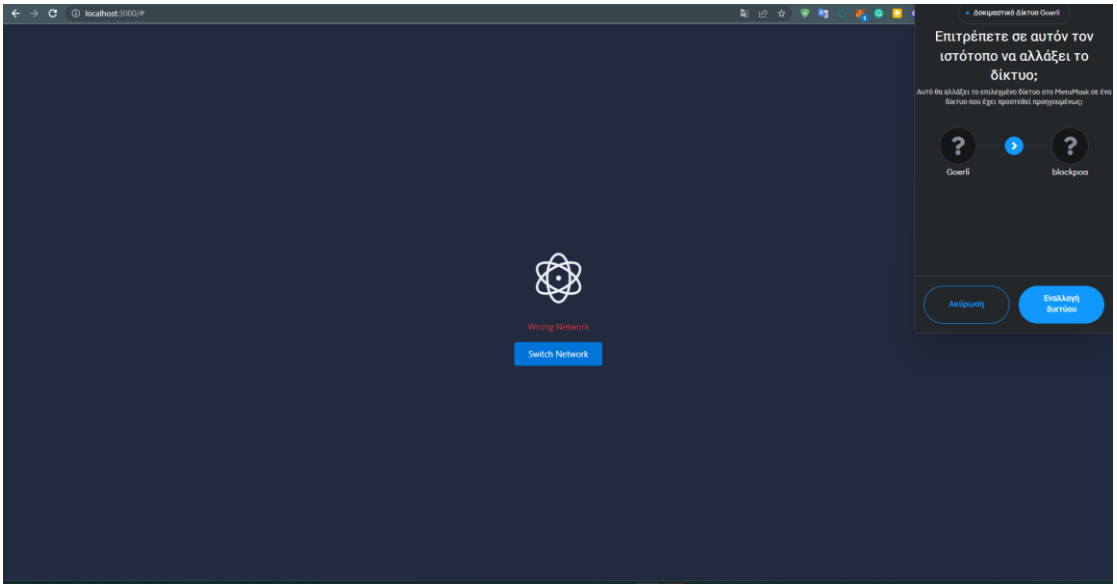


Εικόνα 5-1 Σελίδα Login



Εικόνα 5-2 Είσοδος στη σελίδα χωρίς εγκατεστημένο πορτοφόλι Metamask

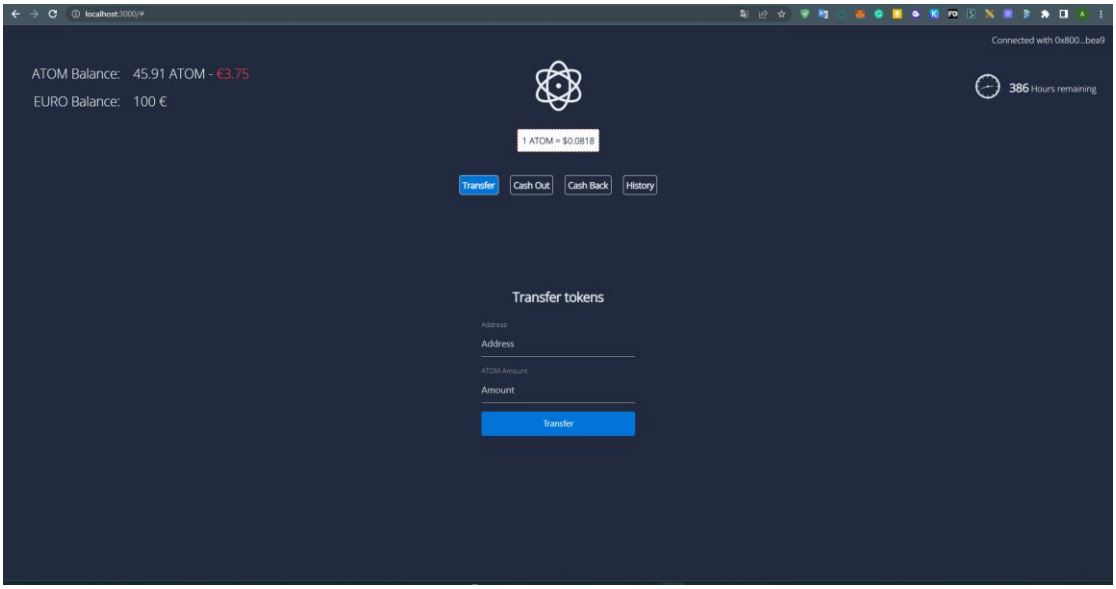
Σε περίπτωση που το πορτοφόλι Metamask του χρήστη είναι συνδεδεμένο σε κάποιο άλλο EVM δίκτυο το UI τον προτρέπει να συνδεθεί στο δίκτυο Ethereum της εφαρμογής και με το πάτημα ενός κουμπιού το Metamask ζητάει επιβεβαίωση για σύνδεση στο δίκτυο (Εικόνα 5-3).



Εικόνα 5-3 Ειδοποίηση Metamask για σύνδεση στο σωστό δίκτυο

5.2.2 Αρχική Σελίδα

Αφού λοιπόν ο χρήστης συνδέσει τον λογαριασμό του στο UI, εισέρχεται στην αρχική σελίδα της εφαρμογής (Εικόνα 5-4). Η αρχική σελίδα χωρίζεται σε 3 μέρη.



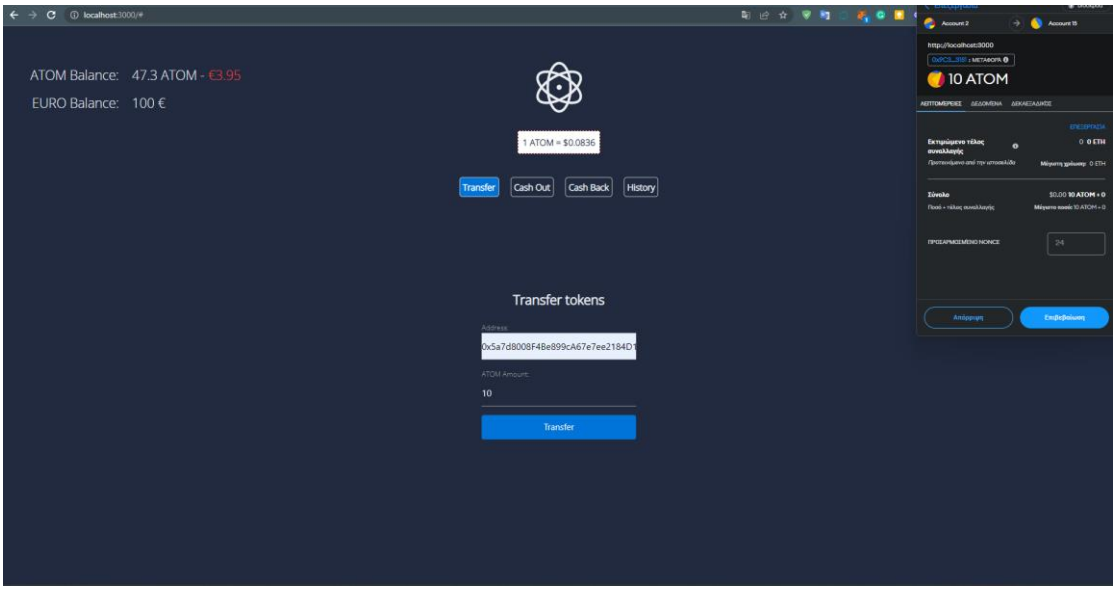
Εικόνα 5-4 Αρχική Σελίδα Απλού Χρήστη

Αριστερά ο χρήστης βλέπει το υπόλοιπο του σε Atomcoin και το υπόλοιπο του σε ευρώ (στα πλαίσια του παραδείγματος ορίζεται ένα εικονικό ποσό κατά τη σύνδεση του χρήστη).

Στο κέντρο της σελίδας εμφανίζεται η τιμή του Atomcoin όπως αυτή λαμβάνεται από το smart contract. Κάτω από την τιμή βρίσκονται οι πράξεις που μπορεί να επιλέξει να πραγματοποιήσει ο χρήστης μέσω της εφαρμογής.

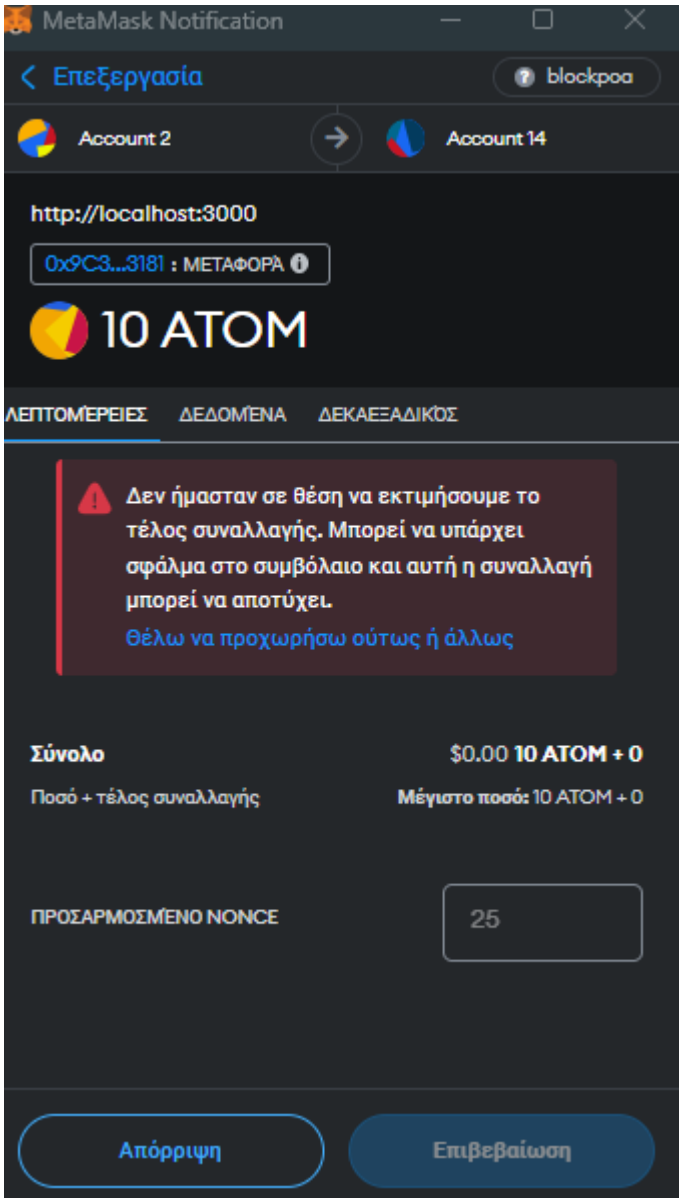
Αυτές είναι:

- Transfer, για τη μεταφορά νομισμάτων ATOM σε κάποια άλλη διεύθυνση. Η μεταφορά γίνεται μέσω του Metamask, αφού πρώτα ο χρήστης εισάγει τη διεύθυνση που θέλει να στείλει νομίσματα και την ποσότητα, καλώντας τη συνάρτηση transfer του smart contract (Εικόνα 5-5).



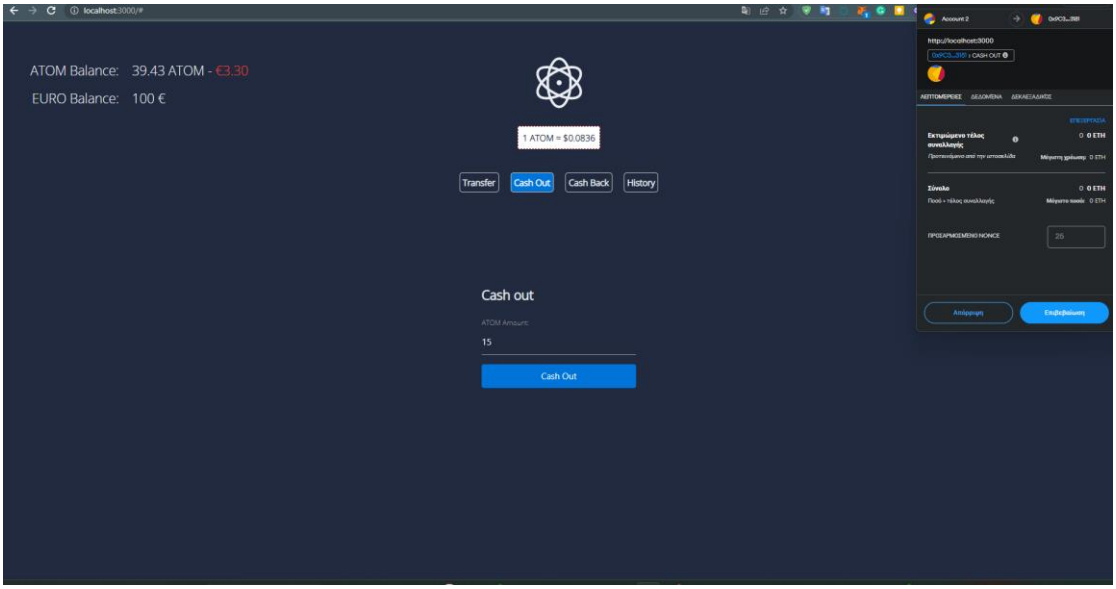
Εικόνα 5-5 Παράδειγμα Transfer

Στην περίπτωση που ο χρήστης προσπαθήσει να στείλει σε κάποιον λογαριασμό που δεν έχει εγκριθεί από κάποιον διαχειριστή βλέπει στο Metamask ένα μήνυμα που τον προειδοποιεί ότι η συναλλαγή θα αποτύχει (Εικόνα 5-6).



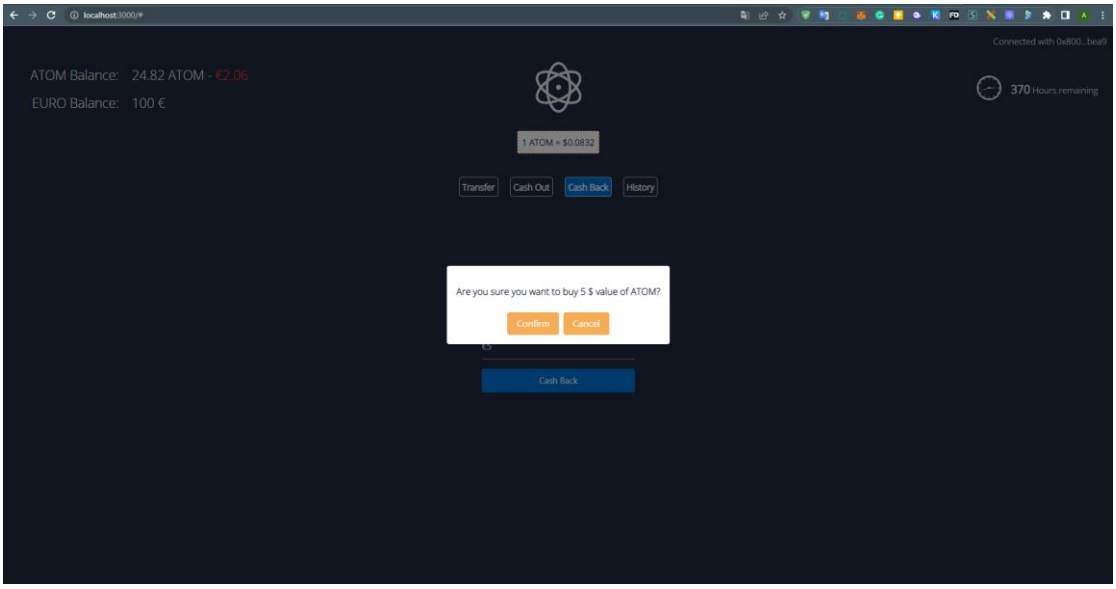
Εικόνα 5-6 Μήνυμα Metamask που προειδοποιεί ότι η μεταφορά προς μη εξουσιοδοτημένο χρήστη θα αποτύχει

- Cash Out, για εξαργύρωση νομισμάτων ATOM. Και εδώ η πράξη γίνεται μέσω Metamask. Ο χρήστης εισάγει τον αριθμό νομισμάτων που θέλει να εξαργυρώσει και καλεί τη συνάρτηση cashOut του smart contract (Εικόνα 5-7).



Εικόνα 5-7 Παράδειγμα Cash out

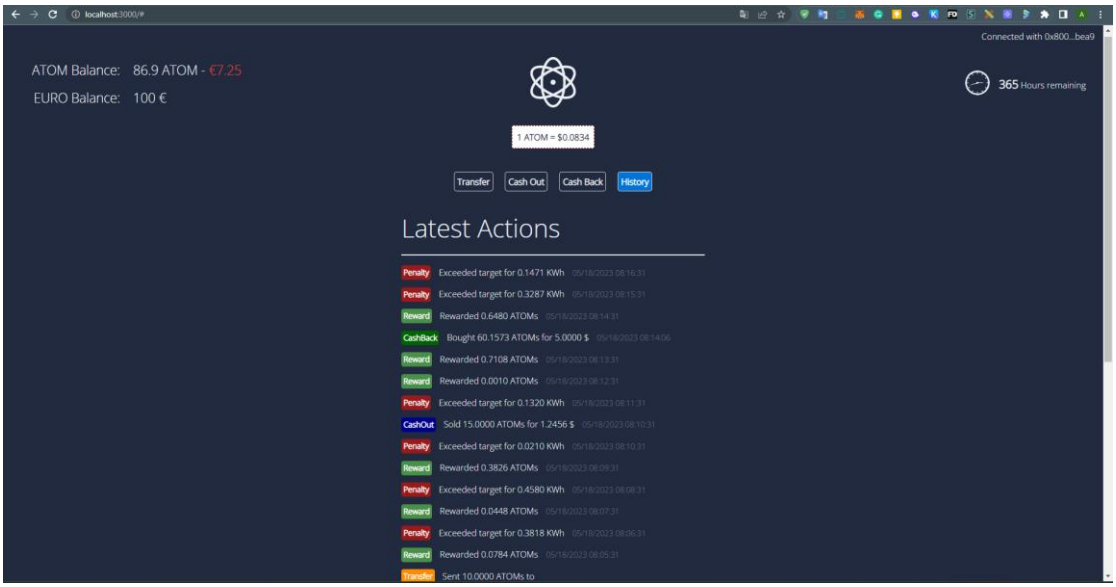
- Cash Back, για αγορά επιπλέον νομισμάτων ATOM. Εδώ ο χρήστης εισάγει το ποσό σε Ευρώ που θέλει να δαπανήσει. Στη συνέχεια και αφού πατήσει το κουμπί Cash Back εμφανίζεται ένα παράθυρο που του ζητάει να επιβεβαιώσει την αγορά του (Εικόνα 5-8). Αν η απάντηση είναι θετική, στέλνεται ένα request στο API του βοηθητικού server της εφαρμογής απ' όπου εκκινείται ένα transaction ώστε να ενημερωθεί το smart contract. Αν όλα κυλήσουν ομαλά ενημερώνεται το υπόλοιπο του χρήστη σε Ευρώ και ATOM.



Εικόνα 5-8 Παράδειγμα Cash Back

- History. Εδώ παρουσιάζονται συνοπτικά οι τελευταίες κινήσεις που αφορούν τον χρήστη (Εικόνα 5-9). Το σύνολο των γεγονότων που μπορεί να εμφανιστούν είναι:
  1. Transfer
  2. Cash Out

3. Cash Back
4. Reward
5. Penalty

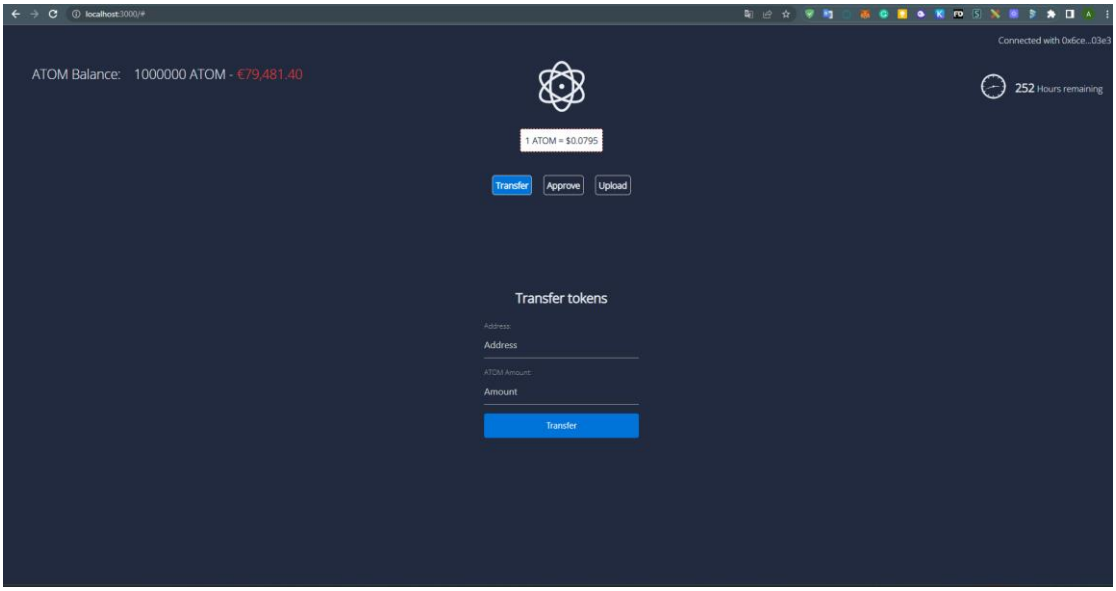


Εικόνα 5-9 Η σελίδα History

Δεξιά στην οθόνη του, ο χρήστης μπορεί να δει τον αριθμό των ωρών που απομένουν για τη λήξη του προγράμματος.

5.3 Λειτουργία Διαχειριστή

Όταν ένας χρήστης με δικαιώματα διαχειριστή εισέρχεται στο UI συναντά μία αρχική σελίδα αντίστοιχη με του απλού χρήστη, αλλά με διαφορά στις λειτουργίες που μπορεί να εκτελέσει (Εικόνα 5-10).

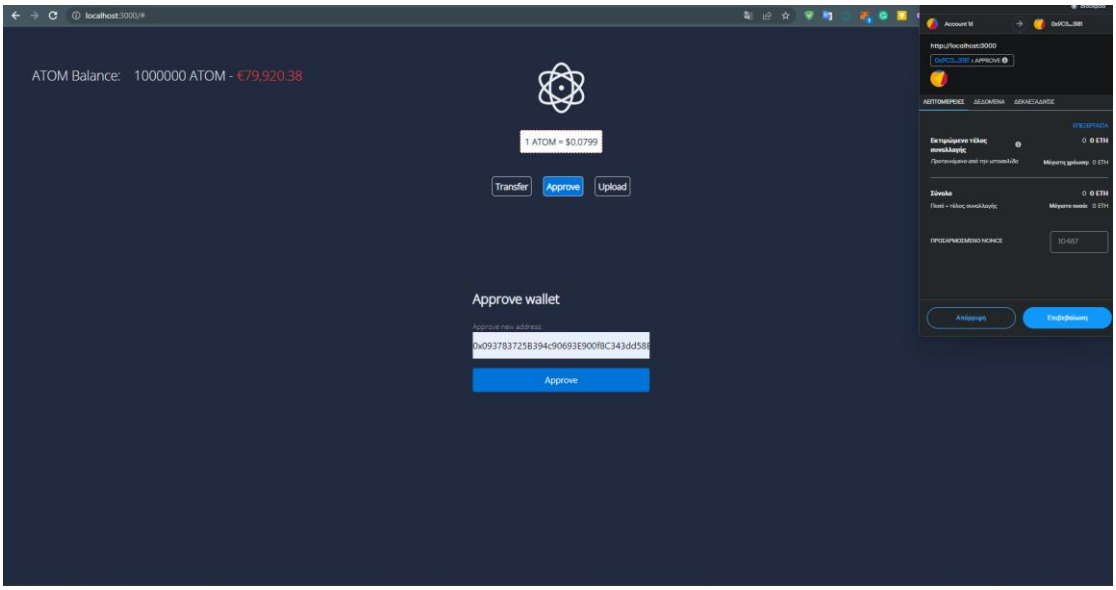


Εικόνα 5-10 Αρχική Σελίδα Διαχειριστή

Οι 3 λειτουργίες που προσφέρονται στη λειτουργία διαχειριστή είναι:

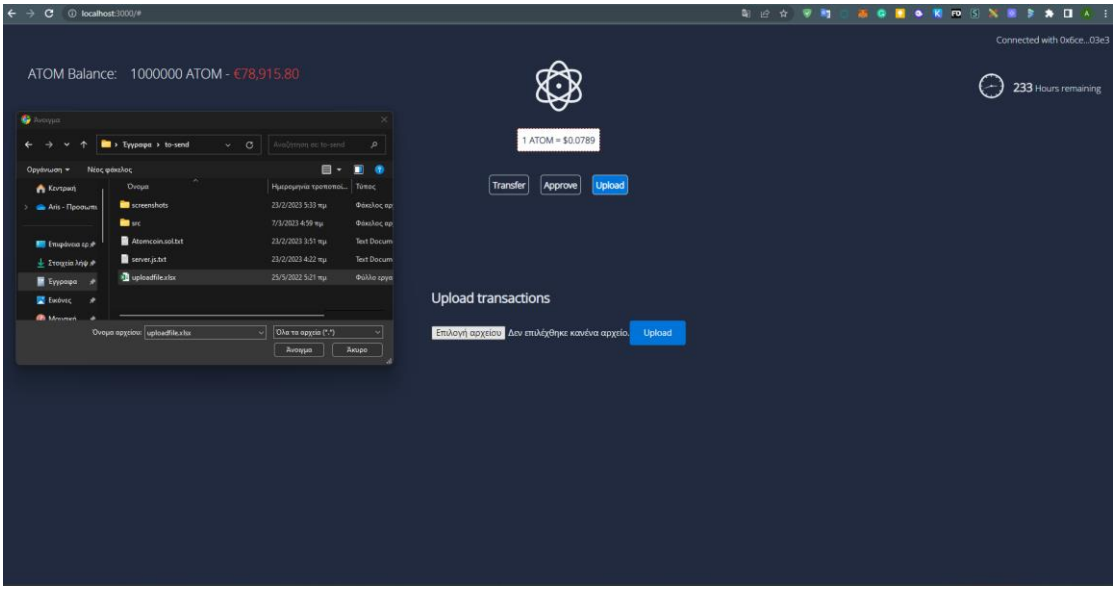
- Transfer, λειτουργία αντίστοιχη με του κοινού χρήστη. Όπως περιγράφηκε προηγουμένως ο χρήστης μπορεί να στείλει νομίσματα ATOM σε άλλες διευθύνσεις, Η διαδικασία είναι η ίδια με του κοινού χρήστη, όπως φαινεται στην εικόνα 5-5.

- Approve. Ο διαχειριστής μπορεί να εξουσιοδοτήσει άλλες διευθύνσεις ώστε να μπορούν να λάβουν ATOM. Αυτό γίνεται αφού εισάγει τη διεύθυνση που θέλει να εξουσιοδοτήσει, στο πεδίο “Address”. Επιβεβαιώνοντας τη συναλλαγή στο Metamask καλείται η συνάρτηση approve του smart contract με όρισμα τη διεύθυνση που δόθηκε (Εικόνα 5-11). Αν επιτύχει η συναλλαγή αυτή η διεύθυνση θα μπορεί να λάβει πλέον ATOM.



Εικόνα 5-11 Παράδειγμα Approve

- Upload File. Ο διαχειριστής μπορεί μέσω του frontend να ανεβάσει στον server, μέσω του API, ένα αρχείο Excel που περιέχει δεδομένα κατανάλωσης χρηστών (Εικόνα 5-12). Από το backend καλείται η συνάρτηση rewardOrPenalize του smart contract για κάθε γραμμή αυτού του αρχείου. Ένα παράδειγμα της μορφής αυτών των δεδομένων δίνεται στην εικόνα 5-13.



Εικόνα 5-12 Παράδειγμα Upload

	A	B	C	D	E	F	G	H
1	id	target	actual	address				
2	1	2,2	1	0x5a7d8008F4Be899cA67e7ee2184D1877A6Db0607				
3	2	1,72	0,68	0x773714A45d3495EAe1Da6fB077d04303b0B81B6c				
4	3	2,94	0,8	0xb9c0AA0684e4ee27255c66539ABc1132E6d9d500				
5	4	4,69	0,71	0x6600a823ecb0f25a8C031ac8c354a7941382feC3				

Εικόνα 5-13 Παράδειγμα δεδομένων κατανάλωσης αρχείου Excel

Κεφάλαιο 6 Επίλογος

6.1 Συμπεράσματα

Στην παρούσα εργασία εξετάστηκε η χρήση της τεχνολογίας blockchain, και πιο συγκεκριμένα του Ethereum για την παροχή κινήτρων στους καταναλωτές ενέργειας για μια πιο βιώσιμη και ενεργειακά αποδοτική κατανάλωση. Πιο συγκεκριμένα εξετάστηκε η δημιουργία ενός ψηφιακού ενεργειακού νομίσματος, του Atomcoin, όπως αυτό περιγράφεται από τους Marinakis et Al. [25]. Το νόμισμα αυτό δίνεται στα πλαίσια ενός προγράμματος επιβράβευσης στους χρήστες που πετυχαίνουν εξοικονόμηση ενέργειας, με αντιστοιχία 1 νόμισμα / kWh εξοικονόμησης.

Η υλοποίηση του νομίσματος βασίστηκε στη δημιουργία ενός έξυπνου συμβολαίου σε γλώσσα Solidity, και με μία επέκταση του προτύπου ERC-20 ώστε να καλυφθούν όλες οι ιδιαιτερότητες του συγκεκριμένου νομίσματος. Αυτές δημιουργούνται από το γεγονός ότι η τιμή του νομίσματος καθορίζεται δυναμικά από έναν μαθηματικό τύπο που βασίζεται στον βαθμό αποδοτικότητας των χρηστών και στα δεδομένα χρησιμοποίησης του νομίσματος, αντί να καθορίζεται από την αγορά. Αυτή η προϋπόθεση οδηγεί στην ανάγκη περιορισμού της αποστολής νομισμάτων εκτός του οικοσυστήματος. Για την πλήρη λειτουργία του συστήματος του Atomcoin εκτός του έξυπνου συμβολαίου δημιουργήθηκαν δύο ακόμα βοηθητικά εργαλεία, μία υπηρεσία Oracle για την των δεδομένων στο έξυπνο συμβόλαιο και μια υπηρεσία API για τη διεκπεραίωση αιτημάτων χρηστών της εφαρμογής που απαιτούνταν η διαμεσολάβηση διαχειριστή.

Ο ολοκληρωμένος κώδικας που υλοποιήθηκε βρίσκεται αναρτημένος στο GitHub στον εξής σύνδεσμο: https://github.com/arisprv/energy-coin.

6.2 Πιθανές μελλοντικές προεκτάσεις

Με βάση τα θεμέλια που τέθηκαν σε αυτή τη διπλωματική, υπάρχουν πολλές ενδιαφέρουσες κατευθύνσεις για μελλοντική εργασία που πρέπει να ληφθούν υπόψη.

1. **Αποκεντρωμένα δίκτυα Oracle:** Όπως αναφέρθηκε προηγουμένως η λύση oracle που χρησιμοποιήθηκε στην εργασία είναι κεντρωμένη και αποτελεί πιθανό σημείο αποτυχίας για. Θα ήταν χρήσιμο να διερευνηθεί η υλοποίηση και χρήση αποκεντρωμένων δικτύων oracle όπως το Chainlink[1], για τη βελτίωση της αξιοπιστίας των ροών δεδομένων.
2. **Δεδομένα πραγματικού κόσμου:** Η δοκιμή σε αυτή τη μελέτη χρησιμοποίησε προσομοιωμένα δεδομένα για την κατανάλωση ενέργειας. Μελλοντικές

[1] https://chain.link/

μελέτες θα μπορούσαν να ενσωματώσουν δεδομένα ενέργειας του πραγματικού κόσμου για να λάβουν μια πιο ακριβή αναπαράσταση του τρόπου με τον οποίο μπορεί να αποδώσει το σύστημα σε ζωντανό περιβάλλον. Αυτό θα συνεπαγόταν τη συνεργασία με παρόχους ενέργειας ή εταιρείες κοινής ωφέλειας για την πρόσβαση και τη χρήση πραγματικών δεδομένων κατανάλωσης ενέργειας.

3. **Λύσεις Ethereum Layer 2:** Αν και στην εργασία χρησιμοποιήθηκε ένα ιδιωτικό δοκιμαστικό δίκτυο Ethereum όπου τα κόστη συναλλαγών μπορούσαν να ελεγχθούν, σε μία εφαρμογή πραγματικού κόσμου στο κύριο δίκτυο Ethereum, και με δεδομένες τις συχνές συναλλαγές που η εφαρμογή χρειάζεται για ανανέωση των δεδομένων αυτά τα κόστη θα ήταν αρκετά μεγάλα. Μία λύση σε αυτό το πρόβλημα θα ήταν η χρησιμοποίηση ενός ιδιωτικού δικτύου και στην τελική μορφή της εφαρμογής, κάτι όμως που θα της στερούσε αρκετά από τα πλεονεκτήματα του blockchain όπως η αποκεντροποίηση. Μία άλλη λύση θα ήταν η εξέταση χρήσης λύσεων Layer 2, όπως Optimistic Rollups ή ZK-rollups, οι οποίες στοχεύουν στην κλιμάκωση του Ethereum με το χειρισμό συναλλαγών εκτός της κύριας αλυσίδας Ethereum. Αυτές οι λύσεις μπορούν να αυξήσουν δραματικά τη διεκπεραίωση των συναλλαγών και να μειώσουν το κόστος, καθιστώντας τις μια πολλά υποσχόμενη αναβάθμιση για ένα σύστημα που στοχεύει να χειριστεί αποτελεσματικά μεγάλο αριθμό συναλλαγών χρηστών [40].
4. **Επέκταση User Interface:** Ενώ ο κύριος στόχος αυτής της εργασίας ήταν η υποκείμενη τεχνολογία blockchain και έξυπνων συμβολαίων, η μελλοντική εργασία θα μπορούσε να επικεντρωθεί στην επέκταση και τη βελτίωση της διεπαφής χρήστη. Αυτό θα μπορούσε να περιλαμβάνει την επέκταση του web UI αλλά και την ανάπτυξη μίας εφαρμογής για κινητές συσκευές.

Βιβλιογραφία

[1] IPCC, "Global Warming of 1.5 ºC," 2018. [Online]. Available: https://www.ipcc.ch/sr15/.

[2] K. Koasidis, V. Marinakis, A. Nikas, K. Chira, A. Flamos and H. Doukas, "Monetising behavioural change as a policy measure to support energy management in the residential sector: A case study in Greece," 2022.

[3] T. Dietz, G. Gardner, J. Gilligan, P. Stern and M. Vandenbergh, "Household actions can provide a behavioral wedge to rapidly reduce US carbon emissions," 2009.

[4] V. Marinakis, C. Nikolopoulou and H. Doukas, "Digitizing Energy Savings in Sustainable Smart Cities: Introducing a Virtual Energy-Currency Approach," 2018.

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[6] R. Sobti and G. Geetha, "Cryptographic hash functions: a review.," 2012.

[7] A. Braeken, "Public key versus symmetric key cryptography in client–server authentication protocols," 2021.

[8] R. Zhang, R. Xue and L. Liu, "Security and Privacy on Blockchain," 2019.

[9] V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.," 2014. [Online]. Available: https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf.

[10] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," 2014. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf.

[11] Ethereum, "The Merge," [Online]. Available: https://ethereum.org/en/roadmap/merge/.

[12] A. Antonopoulos and G. Wood, Mastering Ethereum : building smart contracts and DApps, 2018.

[13] N. Szabo, "Formalizing and Securing Relationships on Public Networks," 1997. [Online]. Available: https://doi.org/10.5210/fm.v2i9.548.

[14] F. Vogelsteller and V. Buterin, "ERC-20: Token Standard," 2015. [Online]. Available: https://eips.ethereum.org/EIPS/eip-20.

[15] M. Bez, G. Fornari and T. Vardanega, "The scalability challenge of ethereum: An initial quantitative analysis," 2019.

[16] Cointelegraph, "Will the Ethereum 2.0 update reduce high gas fees?," [Online]. Available: https://cointelegraph.com/explained/will-the-ethereum-20-update-reduce-high-gas-fees.

[17] Coindesk, "Coindesk," 2023. [Online]. Available: https://www.coindesk.com/consensus-magazine/2023/05/09/coindesk-turns-10-how-the-dao-hack-changed-ethereum-and-crypto/.

[18] "Hyperledger Fabric," [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.5/.

[19] "Corda," [Online]. Available: https://corda.net/.

[20] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," 2019.

[21] A. Freier, "Blockchain in the energy sector. An analysis of the Brooklyn case.," 2022.

[22] "Energy Web," [Online]. Available: https://www.energyweb.org/.

[23] "Power Ledger Whitepaper," 2017. [Online]. Available: https://www.powerledger.io/company/power-ledger-whitepaper.

[24] "Efforce," [Online]. Available: https://efforce.io/.

[25] V. Marinakis, H. Doukas, K. Koasidis and H. Albuflasa, "From Intelligent Energy Management to Value Economy through a Digital Energy Currency: Bahrain City Case Study," 2020.

[26] "Cointelegraph," [Online]. Available: https://cointelegraph.com/news/ethereum-transactions-338-higher-in-2022-but-bitcoin-remains-most-popular.

[27] "Scholarly Community Encyclopedia," [Online]. Available: https://encyclopedia.pub/entry/2959.

[28] "Geth," [Online]. Available: https://geth.ethereum.org/.

[29] "Remix IDE," [Online]. Available: https://remix.ethereum.org/.

[30] "Truffle Suite," [Online]. Available: https://trufflesuite.com/.

[31] "React," [Online]. Available: https://react.dev/.

[32] "Metamask," [Online]. Available: https://metamask.io/.

[33] "Node.js," [Online]. Available: https://nodejs.org/.

[34] "Express," [Online]. Available: https://expressjs.com/.

[35] "Web3.js," [Online]. Available: https://web3js.org/.

[36] "Visual Paradigm," [Online]. Available: https://www.visual-paradigm.com/.

[37] "OpenZeppelin ERC20," [Online]. Available: https://docs.openzeppelin.com/contracts/4.x/erc20.

[38] "OpenZeppelin," [Online]. Available: https://www.openzeppelin.com/.

[39] "OpenZeppelin Acces Control," [Online]. Available: https://docs.openzeppelin.com/contracts/4.x/api/access.

[40] "Ethereum Layer 2," [Online]. Available: https://ethereum.org/en/layer-2/.