Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων
Τομεας Ηλεκτρικων Βιομηχανικων Διαταξεων και Συστηματων Αποφασεων

Αξιοποίηση της τεχνολογίας Blockchain για τη δημιουργία ενός Αποκεντρωμένου Αυτόνομου Οργανισμού

Διπλωματικη Εργασια

της

ΠΕΓΕΙΩΤΗ ΝΑΤΑΛΥ

Επιβλέπων: Μέντζας Γρηγόρης
Καθηγητής Ε.Μ.Π

Αθήνα, Μάρτιος 2023

Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων
Τομεας Ηλεκτρικων Βιομηχανικων Διαταξεων και Συστηματων Αποφασεων

Αξιοποίηση της τεχνολογίας Blockchain για τη δημιουργία ενός Αποκεντρωμένου Αυτόνομου Οργανισμού

Διπλωματικη Εργασια

της

ΠΕΓΕΙΩΤΗ ΝΑΤΑΛΥ

Επιβλέπων: Μέντζας Γρηγόρης
Καθηγητής Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 9η Μαρτίου 2023.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Μέντζας Γρηγόρης	Ψαρράς Ιωάννης	Ασκούνης Δημήτριος
Καθηγητής Ε.Μ.Π	Καθηγητής Ε.Μ.Π	Καθηγητής Ε.Μ.Π

Αθήνα, Μάρτιος 2023

Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων
Τομεας Ηλεκτρικων Βιομηχανικων Διαταξεων και Συστηματων Αποφασεων

(Υπογραφή)

.....
Πεγειώτη Νάταλυ

Μάρτιος 2023

Περίληψη

Στο χώρο της ψηφιακής τεχνολογίας κάνουν την εμφάνιση τους, κατά καιρούς, ορισμένες τεχνολογίες οι οποίες δημιουργούν πολύ ¨θόρυβο¨, άλλες δικαίως, ενώ άλλες όχι. Μια από τις πολυσυζητημένες τεχνολογίες των τελευταίων χρόνων που όπως φαίνεται ανταποκρίνεται στις εξαιρετικά υψηλές προσδοκίες που δημιουργούνται γύρω από αυτή, είναι το Blockchain.

Η πρώτη αναφορά στη συγκεκριμένη τεχνολογία έγινε το 2008 με τη δημιουργία του Bitcoin. Έκ τοτε έχει πραγματοποιηθεί μεγάλη επέκταση των δυνατοτήτων του blockchain και τα τελευταία χρόνια έχει γνωρίσει εκθετική υιοθέτηση, καθώς πληθώρα προγραμματιστών το αξιοποιεί για τη δημιουργία αποκεντρωμένων εφαρμογών.

Ο ενθουσιασμός που επικρατεί για τη νέα τεχνολογία, τα πλεονεκτήματα και τις δυνατότητες εφαρμογής της κάνουν πολλούς να μιλούν για επανάσταση αντίστοιχη με εκείνη του διαδικτύου, η οποία μέσα στα επόμενα χρόνια θα αλλάξει ριζικά τις δομές, τον τρόπο οργάνωσης και τη λειτουργία των σύγχρονων κοινωνιών. Ήδη οι εφαρμογές της τεχνολογίας blockchain καλύπτουν όλα σχεδόν τα πεδία της οικονομίας, ενώ ολοένα και περισσότερες εταιρείες, οργανισμοί και δημόσιες αρχές επενδύουν σημαντικούς πόρους προκειμένου να εφαρμόσουν τη νέα τεχνολογία.

Στόχος της παρούσας διπλωματικής εργασίας είναι η μελέτη του blockchain και πως αυτό μπορεί να βελτιώσει τη σημερινή δομή των φιλανθρωπικών οργανώσεων. Με την εκμετάλλευση αυτής της σπουδαίας καινοτομίας της τεχνολογίας, γίνεται εφικτή η υπερπήδηση πολλών εμποδίων που καθιστούν αναξιόπιστες τις φιλανθρωπικές πρωτοβουλίες, με την μεχρι τώρα δομή τους, και αποτελούν τροχοπέδη για τον πολίτη της κοινωνίας που θέλει να προσφέρει βοήθεια.

Απόσταγμα της έρευνας που διεξήχθη, είναι η δημιουργία ενός Αποκεντρωμένου Αυτόνομου Οργανισμού με φιλανθρωπικό χαρακτήρα, του «Charity DAO». Πρόκειται για έναν οργανισμό, χτισμένο εξ ολοκλήρου στο blockchain, ώστε να μπορεί να εκμεταλλευτεί όλα τα πλεονεκτήματα που προσφέρει η εν λόγω τεχνολογία.

Στο πλαίσιο της εργασίας ερευνούνται οι έννοιες του Blockchain, των αλγορίθμων συναίνεσης και των έξυπνων συμβολαίων. Επιπλέον, αναλύεται η έννοια του Decentralized Autonomous Organization (DAO) και των πλεονεκτημάτων που προσφέρει σε σύγκριση με την παραδοσιακή μορφή ενός οργανισμού.

Λέξεις Κλειδιά

Blockchain, Bitcoin, Ethereum, Έξυπνο Συμβόλαιο, Πρωτόκολλο Συναίνεσης, Αποκεντρωμένος Αυτόνομος Οργανισμός, Φιλανθρωπία

Abstract

In the field of digital technology, certain technologies occasionally emerge that create a lot of noise, some rightfully so, while others not. One of the most talked-about technologies in recent years, that seems to live up to the extremely high expectations surrounding it, is Blockchain.

The first reference to this particular technology was made in 2008 with the creation of Bitcoin. Since then, there has been a significant expansion of blockchain capabilities, and in recent years it has experienced exponential adoption, as a multitude of programmers leverage it to create decentralized applications.

The enthusiasm surrounding the new technology, its advantages and application possibilities, has led many to talk about a revolution similar to that of the Internet, which in the coming years will radically change the structures, organization and operation of modern societies. Already, blockchain technology applications cover almost all areas of the economy, while more and more companies, organizations and public authorities are investing significant resources in order to implement the new technology.

The aim of this thesis is to study blockchain technology and how it can improve the current structure of charitable organizations. By leveraging this significant innovation of technology, it becomes possible to overcome many obstacles that make charitable initiatives unreliable, given their current structure, and act as a hindrance to citizens who want to offer help.

The result of the research conducted is the creation of a Decentralized Autonomous Organization with philanthropic character, the "Charity DAO". This organization is built entirely on the blockchain in order to take advantage of all the benefits offered by this technology.

The concepts of Blockchain, consensus algorithms, and smart contracts are being investigated in the context of the thesis. Additionally, the concept of Decentralized Autonomous Organization (DAO) is analyzed, along with the advantages it offers compared to the traditional form of an organization.

Keywords

Blockchain, Bitcoin, Ethereum, Smart Contract, Consensus Protocol, Decentralized Autonomous Organization, Charity

στη μαμά μου

Ευχαριστίες

Με την ολοκλήρωση της διπλωματικής μου εργασίας και των προπτυχιακών μου σπουδών θα ήθελα να ευχαριστήσω τους ανθρώπους που με βοήθησαν και με στήριξαν σε αυτή μου την προσπάθεια.

Αρχικά θα ήθελα να εκφράσω τις ευχαριστίες μου στον καθηγητή κ.Γρηγόρη Μέντζα για την εμπιστοσύνη που μου έδειξε και που μου επέτρεψε να μετατρέψω ένα ζήτημα που με απασχολεί προσωπικά σε θέμα της διπλωματικής μου εργασίας. Επιπλέον θα ήθελα να ευχαριστήσω τον διδακτορικό ερευνητή Φώτη Παρασκευόπουλο για την καθοδήγηση και την ενθάρρυνση που μου παρείχε καθ' όλη τη διάρκεια της εκπόνησης της εργασίας αυτής.

Τέλος, ένα μεγάλο ευχαριστώ σε όλους τους ανθρώπους που ήταν δίπλα μου στη φοιτητική μου πορεία.

Αθήνα, Μάρτιος 2023

Πεγειώτη Νάταλυ

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

1.1 Πρόλογος - Κίνητρο

Μετά από ένα ταξίδι εθελοντικού σκοπού, και ζώντας για ένα μήνα σε μια μικρή πόλη της Κένυας, βιώνοντας την καθημερινότητα των ντόπιων ανθρώπων, συνειδητοποίησα περισσότερο από πότε, το μέγεθος της ανάγκης που υπάρχει εκεί έξω.

Συζητώντας με τους ανθρώπους εκεί για τα προβλήματα που αντιμετωπίζουν, ακούγοντας από τους άμεσα εμπλεκόμενους για την εκμετάλλευση που υπάρχει στον χώρο της φιλανθρωπίας, για το πόσο μικρή είναι η βοήθεια που προσφέρεται, κι αυτή για συγκεκριμένες ομάδες πληθυσμού, αντιλήφθηκα ότι το πρόβλημα είναι στην πραγματικότητα πολύ μεγαλύτερο απ'όσο πίστευα.

Δυστυχώς, στις μέρες μας, η φιλανθρωπία έχει προδοθεί από συλλόγους που καταχρώνται την πίστη του κοινού. Υπάρχουν πάρα πολλοί που διστάζουν να προσφέρουν βοήθεια με αφορμή το σκεπτικό που επικρατεί, πως ¨μόνο ένα μικρό ποσό των χρημάτων πηγαίνει τελικά στους άπορους¨, και έχουν δίκαιο. Αποτέλεσμα αυτού, οι άνθρωποι τείνουν να εγκαταλείψουν τη φιλανθρωπία εντελώς.

Η φτώχεια και τα προβλήματα υγειονομικού χαρακτήρα που συνάντησα κατά την παραμονή μου εκεί με προβληματίσαν ιδιαίτερα, και δυστυχώς αυτά είναι μόνο δύο από τα πολλά ζητήματα που υπάρχουν. Η αντιμετώπιση προβλημάτων που προκύπτουν από ασθένειες, πολέμους, φυσικές καταστροφές, δικτατορικά καθεστώτα, χρειάζεται να γίνει μέγιστη προτεραιότητα όλων όσων από τύχη δεν βρίσκονται κάτω υπό τέτοιες συνθήκες. Επιπλέον η προώθηση της εκπαίδευσης, η εκπλήρωση των ονείρων ατόμων που αδυνατούν να τα καταφέρουν, η προσφορά διάφορων ευκαιριών σε αυτούς που δεν τις έχουν, πρέπει επίσης να γίνουν σκοπός μας.

Για καλή μου τύχη έχω γεννηθεί και μεγαλώσει με όλα όσα χρειάζεται και δικαιούται ένας άνθρωπος στη ζωή του. Μεγαλώνοντας στα χρόνια της τεχνολογικής προόδου και αντιλαμβανόμενη τις ευκολίες και τις δυνατότητες που η τεχνολογία μπορεί να προσφέρει στη ζωή των ανθρώπων αποφάσισα να ακολουθήσω και την αντίστοιχη εκπαίδευση, με αποτέλεσμα να καταλήξω στη σχολή από την οποία προσπαθώ σήμερα να αποφοιτήσω.

Για την διπλωματική μου εργασία και την ολοκλήρωση των σπουδών μου, αποφάσισα να παντρέψω τα δύο αυτά θέματα που με ενδιαφέρουν και με απασχολούν, την φιλανθρωπία και την τεχνολογία.

Με κίνητρο δηλαδή την επιθυμία μου να βρω λύσεις και να βελτιώσω τον κόσμο μας,

και έχοντας το κατάλληλο τεχνολογικό υπόβαθρο προέκυψε η ιδέα της δημιουργίας της υλοποίησης που θα εξεταστεί στην συνέχεια, η οποία θέλω να πιστεύω ότι με δουλειά και βελτιώσεις μπορεί όντως να έχει ένα θετικό αντίκτυπο στον κόσμο μας.

Κι αν ένα τέτοιο σενάριο είναι ουτοπικό, αν μια τέτοια προσπάθεια δεν είναι αρκετή, πιστεύω παρ'όλάυτά, ότι η τεχνολογία μπορεί πράγματι να φέρει την αλλαγή στον κόσμο της φιλανθρωπίας.

1.2 Οργάνωση του τόμου

Η εργασία αυτή είναι οργανωμένη σε επτά (7) κεφάλαια εκ των οποίων τα έξι (6) περιλαμβάνονται σε τρία (3) βασικά μέρη:

Το **Κεφάλαιο 1** αποτελεί εισαγωγικό κομμάτι. Είναι μία πρώτη επαφή με τον συγγραφέα, το αντικείμενο της διπλωματικής εργασίας και το κίνητρο που οδήγησε στην επιλογή του συγκεκριμένου θέματος. Περιλαμβάνει επίσης πληροφορίες για την οργάνωση του τόμου.

Το πρώτο βασικό μέρος του συγγράμματος περιλαμβάνει τα Κεφάλαια 2 και 3, στα οποία περιέχεται όλο το απαραίτητο **Θεωρητικό Υπόβαθρο** για την κατανόηση των βασικών τεχνολογιών που σχετίζονται με τη διπλωματική, καθώς και μια προσέγγιση της βασικής ιδέας του δημιουργήματος.

Συγκεκριμένα στο **Κεφάλαιο 2** γίνεται μια εισαγωγή στο bitcoin, μια συλλογή εννοιών και τεχνολογιών που σχηματίζουν τη βάση ενός οικοσυστήματος ψηφιακών χρημάτων. Αναλύεται η έννοια του blockchain, της επαναστατικής μεθόδου στην οποία στηρίχτηκε το bitcoin καθώς και οι αλγόριθμοι συναίνεσης. Περιγράφεται το Ethereum blockchain καθώς και οι επιπλέον δυνατότητες που προσφέρει σε σύγκριση με το bitcoin, μέσω των έξυπνων συμβολαίων. Τέλος δίνεται μια επεξήγηση για το τι είναι ένα DAO, που είναι και το βασικό αντικείμενο της διπλωματική εργασίας.

Στο **Κεφάλαιο 3** περιγράφεται η ιδέα στην οποία βασίστηκε η εργασία. Πρόκειται για το ζήτημα της φιλανθρωπίας. Αναλύεται η μέχρι σήμερα μορφή της και κατά πόσο έχει θετικό αντίκτυπο στην κοινωνία, σε συνάρτηση με όλα τα προβλήματα που προκύπτουν από αυτή. Παρατίθεται η ανάγκη για τη δημιουργία on chain charities και ποια ζητήματα λύνονται με αυτή τη νέα προσέγγιση.

Το δεύτερο κύριο μέρος του συγγράμματος περιλαμβάνει το κομμάτι της **Περίπτωσης Χρήσης**, τα Κεφάλαια 4, 5 και 6. Αρχικά, δίνεται η κεντρική ιδέα του δημιουργήματος ενώ ακολούθως παρουσιάζεται μια αναλυτική περιγραφή της σχεδίασης του Charity DAO, η διαδικασία της υλοποίησης καθώς επίσης και η λειτουργία του.

Αναλυτικά, στο **Κεφάλαιο 4** δίνεται μια πρώτη εικόνα της υλοποίησης που ακολουθεί. Περιγράφεται η δομή του αποκεντρομένου αυτόνομου οργανισμού και ο τρόπος λειτουργίας του. Αναλύονται ενδελεχώς οι οντότητες και οι δυνατές λειτουργικότητες της εφαρμογής ενώ φανερώνεται ο σχεδιασμός και η αρχιτεκτονική του δημιουργήματος.

Στο **Κεφάλαιο 5** παρατίθενται όλα τα εργαλεία που χρησιμοποιήθηκαν για την ανάπτυξη της εφαρμογής και επεξηγείται η χρήση τους. Επιπλέον γίνεται η ανάλυση της επιχειρη-

ματικής λογικής του DAO μέσω του έξυπνου συμβολαίου, δηλαδή του βασικού πυρήνα, με την επεξήγηση των κύριων συναρτήσεών του. Γίνεται αναφορά στη δημιουργία του τοπικού δικτύου Ethereum καθώς και της διεπαφής χρήστη ενώ τέλος φαίνεται ο τρόπος σύνδεσής τους για τη δημιουργία ενός ολοκληρωμένου και λειτουργικού Αποκεντρωμένου Αυτόνομου Οργανισμού.

Στο **Κεφάλαιο 6** γίνεται η παρουσίαση του Charity DAO. Περιγράφεται αναλυτικά και βήμα-βήμα ο τρόπος χρήσης της εφαρμογής μέσω της διεπαφής χρήστη. Για την αποδοτικότερη ανάλυση και καλύτερη κατανόηση της λειτουργίας παρατίθενται στιγμιότυπα οθόνης με ξεκάθαρη επεξήγηση του εκάστοτε σεναρίου χρήσης.

Το τρίτο και τελευταίο μέρος του συγγράμματος περιλαμβάνει τον **Επίλογο** της εργασίας.

Στο **Κεφάλαιο 7** αποδίδεται η συνεισφορά αυτής της διπλωματικής εργασίας, καθώς και μελλοντικές επεκτάσεις της. Συλλέγονται τα συμπεράσματα της εργασίας που αφορούν τους Αποκεντρωμένους Αυτόνομους Οργανισμούς αλλά και γενικότερα την τεχνολογία blockchain. Συζητούνται τα συμπεράσματα που απορρέουν από την ανάπτυξη της εν λόγω αποκεντρωμένης εφαρμογής και η σημαντικότητα της αξιοποίησής της στον πραγματικό κόσμο.

Μέρος I

Θεωρητικό Υπόβαθρο

Κεφάλαιο 2

Βασικές Έννοιες

Στο κεφάλαιο αυτό γίνεται μια εισαγωγή στο bitcoin, μια συλλογή εννοιών και τεχνολογιών που σχηματίζουν τη βάση ενός οικοσυστήματος ψηφιακών χρημάτων. Αναλύεται η έννοια του blockchain, της επαναστατικής μεθόδου στην οποία στηρίχτηκε το bitcoin καθώς και οι αλγόριθμοι συναίνεσης. Περιγράφεται το Ethereum blockchain καθώς και οι επιπλέον δυνατότητες που προσφέρει σε σύγκριση με το bitcoin, μέσω των έξυπνων συμβολαίων. Τέλος δίνεται μια επεξήγηση για το τι είναι ένα DAO, που είναι και το βασικό αντικείμενο της διπλωματική εργασίας.

2.1 Bitcoin

2.1.1 Ιστορική Αναδρομή

Το bitcoin επινοήθηκε το 2008 με τη δημοσίευση ενός εγγράφου με τίτλο «Bitcoin: Ένα peer-to-peer ηλεκτρονικό σύστημα μετρητών» (Bitcoin: A Peer-to-Peer Electronic Cash System) [1], γραμμένο με το ψευδώνυμο Satoshi Nakamoto, η ταυτότητα του οποίου δεν έχει ακόμη εξακριβωθεί.

Η παγκόσμια οικονομική ύφεση της τότε εποχής η οποία προκάλεσε τη δυσπιστία των ανθρώπων για τις τράπεζες και τα κεντρικά συστήματα διαχείρισης, ευνόησε την πρόοδο του εν λόγω καινοτόμου δημιουργήματος.

Ο Nakamoto συνδύασε αρκετές προηγούμενες εφευρέσεις για τη δημιουργία ενός εντελώς αποκεντρωμένου ηλεκτρονικού συστήματος μετρητών που δεν βασίζεται σε μια κεντρική αρχή για την έκδοση νομίσματος ή την επίλυση και επαλήθευση των συναλλαγών.

Στις αρχές του 2009 κυκλοφόρησε η πρώτη έκδοση λογισμικού του bitcoin μέσω του οποίου δημιουργήθηκε το δίκτυο, καθώς και το συνάλλαγμα που ονομάστηκε επίσης bitcoin (BTC). Έκτοτε το λογισμικό αναθεωρήθηκε και αναθεωρείται μέχρι σήμερα από πολλους προγραμματιστές.

Ο δημιουργός συνέχισε να συμβάλλει στην ανάπτυξη του λογισμικού, σε συνεργασία με άλλους προγραμματιστές. Η παρουσία του Satoshi Nakamoto άρχισε να ξεθωριάζει στα μέσα του 2010, ενώ λίγο αργότερα παρέδωσε τον έλεγχο του πηγαίου κώδικα του λογισμικού και της ιστοσελίδας Bitcoin.org σε εξέχοντα μέλη της κοινότητας Bitcoin. Αποσύρθηκε από τα κοινά τον Απρίλιο του 2011, αφήνοντας την ευθύνη ανάπτυξης του κώδικα και του δικτύου σε μια ακμάζουσα ομάδα εθελοντών. Ωστόσο, ούτε ο ίδιος ούτε οποιοσδήποτε άλλος ασκεί έλεγ-

χο στο σύστημα του bitcoin, το οποίο λειτουργεί με βάση απόλυτα διαφανείς μαθηματικές αρχές.

Η εφεύρεση από μόνη της είναι πρωτοποριακή και έχει γεννήσει νέα πεδία γνώσης στην επιστήμη των κατανεμημένων συστημάτων πληροφορικής και της οικονομίας.

2.1.2 Τι είναι το bitcoin

Το bitcoin [2] [3] [4] είναι μια συλλογή εννοιών και τεχνολογιών που σχηματίζουν τη βάση ενός οικοσυστήματος ψηφιακών χρημάτων. Μονάδες του νομίσματος BTC χρησιμοποιούνται για την αποθήκευση και τη μετάδοση αξίας μεταξύ των συμμετεχόντων στο δίκτυο του bitcoin. Πρόκειται για ένα ανοιχτού κώδικα λογισμικό που μπορεί να τρέξει σε ένα ευρύ φάσμα υπολογιστικών συσκευών, συμπεριλαμβανομένων των φορητών υπολογιστών και των κινητών τηλεφώνων, καθιστώντας την τεχνολογία εύκολα προσβάσιμη.

Οι χρήστες μπορούν εκτελούν οποιαδήποτε συναλλαγή γίνεται και με συμβατικά νομίσματα, μεταφέροντας bitcoin (BTC) μέσω του δικτύου. Τα BTC μπορούν να αγοραστούν, πωληθούν και ανταλλαχθούν με άλλα νομίσματα σε εξειδικευμένα ανταλλακτήρια νομισμάτων.

Το bitcoin φαίνεται να είναι η τέλεια μορφή χρήματος για το Διαδίκτυο, διότι είναι γρήγορη, ασφαλής και χωρίς σύνορα. Προσφέρει στους ιδιοκτήτες του την αμεσότητα που παρέχουν οι συναλλαγές με μετρητά εξαλείφοντας την ανάγκη του τρίτου φορέα, κάποιας κεντρικής αρχής δηλαδή, η οποία εποπτεύει κάθε συναλλαγή τους.

Η ιδέα του αποκεντρωμένου άυλου ψηφιακού νομίσματος δεν ήταν τόσο καινοτόμα καθώς επιχειρήθηκε και προηγουμένως, ωστόσο το bitcoin ήταν η πρώτη ολοκληρωμένη πρόταση που δεν απαιτούσε κανενός είδους κεντρική εξουσία, κανέναν που να ελέγχει και να διαχειρίζεται το σύστημα. Το τρωτό σημείο των προηγούμενων αντίστοιχων προτάσεων ήταν οι επιθέσεις από κακόβουλους χρήστες που καταλάμβαναν τον έλεγχο του δικτύου (Sybil Attacks). Η πραγματική καινοτομία του συγκεκριμένου εγχειρήματος ήταν ο τρόπος με τον οποίο αντιμετωπίστηκαν οι συγκεκριμένες επιθέσεις.

Την επανάσταση στην τεχνολογία έχει φέρει το bitcoin πρωτόκολλο, ένα δίκτυο και μία καινοτομία στα κατανεμημένα υπολογιστικά συστήματα. Το νόμισμα bitcoin (BTC) είναι στην πραγματικότητα μόνο η πρώτη εφαρμογή αυτής της σπουδαίας εφεύρεσης.

2.1.3 Πώς λειτουργεί το bitcoin

Σε αντίθεση με τα παραδοσιακά νομίσματα, τα bitcoin είναι εξ ολοκλήρου εικονικά. Τα νομίσματα, υπονοείται στις συναλλαγές ότι, μεταφέρουν αξία από τον αποστολέα στον παραλήπτη.

Οι χρήστες του bitcoin κατέχουν κλειδιά, με τα οποία τους επιτρέπεται να αποδεικνύουν την κυριότητα των συναλλαγών τους στο δίκτυο bitcoin, ξεκλειδώνοντας την αξία για να τη ξοδέψουν και να τη μεταφέρουν σε νέο παραλήπτη. Αυτά τα κλειδιά αποθηκεύονται συχνά σε ένα ψηφιακό πορτοφόλι, και η κατοχή τους είναι η μόνη προϋπόθεση για το ξόδεμα bitcoin, αφήνοντας έτσι τον απόλυτο έλεγχο στα χέρια του κάθε χρήστη.

Το bitcoin είναι ένα κατανεμημένο peer-to-peer (ομότιμου-προς-ομότιμο) σύστημα, πράγμα που σημαίνει ότι δεν υπάρχει κάποιο κέντρο ελέγχου.

Τα bitcoin (BTC) [5] δημιουργούνται μέσω μιας διαδικασίας που ονομάζεται «εξόρυξη» (mining), η οποία αφορά τον ανταγωνισμό για εύρεση λύσεων σε ένα μαθηματικό πρόβλημα κατά την επεξεργασία των συναλλαγών bitcoin. Κάθε χρήστης του δίκτυο bitcoin έχει τη δυνατότητα να λειτουργήσει ως εξορύκτης (miner), χρησιμοποιώντας την επεξεργαστική ισχύ του υπολογιστή του προκειμένου να επαληθεύει και να καταγράφει τις συναλλαγές. Κάθε περίπου 10 λεπτά κάποιος miner καταφέρνει να επικυρώσει ένα μπλοκ, που περιέχει τις συναλλαγές των τελευταίων λεπτών, το οποίο τοποθετείται σε μια αλυσίδα με όλα τα προηγούμενα μπλοκ που έχουν επικυρωθεί. Για αυτή του την επίτευξη ανταμείβεται με καινούρια bitcoin. Αυτή λοιπόν είναι η διαδικασία δημιουργίας νέων νομισμάτων.

Το πρωτόκολλο bitcoin περιλαμβάνει ενσωματωμένους αλγορίθμους που ρυθμίζουν τη λειτουργία της εξόρυξης σε όλο το δίκτυο. Κάθε τέσσερα χρόνια, το πρωτόκολλο μειώνει το ρυθμό με τον οποίο τα νέα bitcoin δημιουργούνται στο μισό, ενώ ταυτόχρονα περιορίζει τον συνολικό αριθμό που θα εκδοθούν σε συνολικά 21 εκατομμύρια νομίσματα. Έτσι υπολογίζεται ότι η διαδικασία της δημιουργίας των bitcoin θα ολοκληρωθεί κατά το έτος 2140. Επιπλέον, το bitcoin δεν μπορεί να πληθωριστεί από «εκτύπωση» νέου χρήματος πέρα από τον αναμενόμενο ρυθμό έκδοσης.

Για να λειτουργήσει όμως σωστά και με ασφάλεια ένα σύστημα αποκεντρωμένου ψηφιακού νομίσματος πρέπει να ληφθεί υπόψη το γεγονός ότι οι χρήστες δεν γνωρίζουν και δεν εμπιστεύονται ο ένας τον άλλο. Είναι επιτακτική η ανάγκη ύπαρξης ενός Πρωτοκόλλου Συναίνεσης (Consensus Protocol) σύμφωνα με το οποίο η κατάσταση του δικτύου, τουτέστιν η αξία νομισμάτων που έχει κάθε χρήστης στην κατοχή του, να είναι μοναδική και αποδεκτή από όλους τους χρήστες.

Για να επιτυχνάνεται αυτό, το bitcoin συνδιάζει τον μηχανισμό συναίνεσης με την αποθήκευση των στοιχείων των συναλλαγών σε μία αλυσιδωτή δομή δεδομένων. Η κατάσταση του δικτύου βασίζεται αυστηρά στη χρονολογική σειρά με την οποία πραγματοποιούνται οι συναλλαγές.

2.2 Blockchain

2.2.1 Κρυπτογραφία Δημοσίου Κλειδιού

Η κρυπτογραφία δημοσίου κλειδιού [6] (ή αλλιως ασύμμετρη κρυπτογραφία) ανακαλύφθηκε στη δεκαετία του 1970 και είναι το θεμέλιο από τα μαθηματικά για την ασφάλεια των υπολογιστών και των πληροφοριών. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί όπως στην περίπτωση της συμμετρικής κρυπτογράφησης, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.

Συγκεκριμένα κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: το ένα ονομάζεται ιδιωτικό κλειδί (private key) και το άλλο δημόσιο κλειδί (public key). Το ιδιωτικό κλειδί πρέπει ο κάθε χρήστης να το προφυλάσσει και να το κρατάει κρυφό, ενώ αντιθέτως το δημόσιο κλειδί μπορεί να το κοινοποιεί σε όλη τη διαδικτυακή κοινότητα ή σε συγκεκριμένους παραλήπτες.

Τα δύο αυτά κλειδιά (ιδιωτικό και δημόσιο) έχουν μαθηματική σχέση μεταξύ τους. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης.

2.2.2 Συνάρτηση Κατακερματισμού / Hash Function

Από την εφεύρεση της κρυπτογραφίας δημοσίου κλειδιού και έπειτα, έχουν ανακαλυφθεί αρκετές ακόμα μαθηματικές λειτουργίες, όπως η εκθετικότητα πρώτων αριθμών και η κρυπτογραφία ελλειπτικών καμπυλών [7]. Αυτές οι μαθηματικές λειτουργίες είναι πρακτικά μη-αναστρέψιμες, που σημαίνει ότι είναι εύκολος ο υπολογισμός προς μία κατεύθυνση και ανέφικτος προς την αντίθετη.

Συνάρτηση κατακερματισμού καλείται μια συνάρτηση η οποία παίρνει ως είσοδο ένα σύνολο χαρακτήρων αυθαίρετου μεγέθους M και παράγει ως έξοδο ένα σύνολο χαρακτήρων σταθερού και προκαθορισμένου μεγέθους H(M). Οποιαδήποτε μεταβολή στην είσοδο της συνάρτησης κατακερματισμού αλλάζει άρδην την έξοδο.

Για να είναι έγκυρη μια συνάρτηση κατακερματισμού πρέπει να πληρούνται τα δύο εξής κριτήρια:

1. Ο υπολογισμός της εξόδου H(M) δεδομένης μια εισόδου M πρέπει να υπολογιστικά εύκολος

2. Ο υπολογισμός της εισόδου M δεδομένη της εξόδου H(M) πρέπει να είναι υπολογιστικά αδύνατος

2.2.2.1 Κρυπτογραφική συνάρτηση κατακερματισμού

Για να θεωρηθεί κρυπτογραφική μια Hash Function πρέπει να πληροί και τις ακόλουθες επιπρόσθετες προϋποθέσεις:

1. Ανθεκτικότητα σε προεικόνες (preimage resistance)
   Δεδομένης της συνάρτησης H( ) και για κάθε έξοδο y να είναι υπολογιστικά αδύνατη η εύρεση τιμής x τέτοια ώστε H(x) = y

2. Ανθεκτικότητα σε δεύτερες προεικόνες (second preimage resistance) ή ασθενής ανθεκτικότητα σε συγκρούσεις (weak collision resistance)
   Δεδομένης της συνάρτησης H( ) και για κάθε είσοδο x να είναι υπολογιστικά αδύνατη η εύρεση τιμής x' τέτοια ώστε H(x') = H(x)

3. Ανθεκτικότητα σε συγκρούσεις (collision resistance) ή ισχυρή ανθεκτικότητα σε συγκρούσεις (strong collision resistance)
   Δεδομένης της συνάρτησης H( ) να είναι υπολογιστικά αδύνατη η εύρεση ζεύγους x, x' τέτοιο ώστε H(x) = H(x')

2.2.3 Συναλλαγές

Μία συναλλαγή είναι η μεταφορά κάποιας χρηματικής αξίας από τον κάτοχό της σε κάποιον άλλο παραλήπτη. Σε ένα δίκτυο όπως το bitcoin, μια συναλλαγή λέει στο δίκτυο ότι ο ιδιοκτήτης ενός αριθμού νομισμάτων, επιτρέπει τη μεταφορά ορισμένων από αυτά σε κάποιον άλλο χρήστη. Ο νέος ιδιοκτήτης μπορεί έπειτα να ξοδέψει αυτά τα νομίσματα δημιουργώντας μια νέα συναλλαγή που επιτρέπει τη μεταφορά σε άλλον ιδιοκτήτη και ούτω καθεξής.

Οι συναλλαγές μεταφέρουν αξία από τις εισόδους της συναλλαγής στις εξόδους της συναλλαγής. Κάθε συναλλαγή μπορεί να περιέχει μία ή περισσότερες εισόδους, όπως επίσης και μία ή περισσότερες εξόδους. Μια είσοδος είναι εκεί από όπου η αξία του νομίσματος προέρχεται, συνήθως η έξοδος μιας προηγούμενης συναλλαγής.

Μια έξοδος συναλλαγής συνδέεται με ένα δημόσιο κλειδί που αντιστοιχεί στη διεύθυνση του παραλήπτη και νέου ιδιοκτήτη. Για τη μεταφορά αυτής της αξίας ο νέος κάτοχος πρέπει να «υπογράψει» με το ιδιωτικό του κλειδί (το οποίο αντιστοιχεί στο δημόσιο κλειδί που συνδέεται με τη συγκεκριμένη αξία), ότι εγκρίνει τη συναλλαγή που πρόκειται να πραγματοποιηθεί.

Κάθε συναλλαγή πραγματοποιείται με τον τρόπο που αναλύεται πιο πάνω αλλά δεν γίνεται απευθείας μέρος του κοινού αρχείου συναλλαγών του δικτύου. Μέχρι τότε ορίζεται σαν «αίτημα συναλλαγής». Κάθε τέτοιο αίτημα συναλλαγής αναμεταδίδεται σε όλο το δίκτυο.

2.2.4 Block

Οι miners συλλέγουν τα αιτήματα συναλλαγών και αφού επιβεβαιώσουν την εγκυρότητά τους τα τοποθετούν σε ένα μπλοκ. Η σειρά με την οποία ο miner τοποθετεί τις συναλλαγές στο μπλοκ είναι σημαντική αφού οι εξόδοι μίας συναλλαγής μπορεί να χρησιμοποιούνται ως εισόδοι για μια άλλη συναλλαγή.

Εκτός από τα αιτήματα των συναλλαγών, κάθε μπλοκ πρέπει να περιέχει μια αναφορά (hash) στο τελευταίο μπλοκ που έχει «εξορυχθεί» και έχει γίνει μέρος του αρχείου του δικτύου αλλά και μία χρονοσφραγίδα.

Έδω αρχίζει ένας αγώνας μεταξύ των miners για το ποιος θα επιτύχει να λύσει γρηγορότερα ένα μαθηματικό πρόβλημα. Αυτό το πρόβλημα είναι ο μηχανισμός συναίνεσης που αναφέρθηκε προηγουμένως και παράγει μια κρυπτογραφική σύνδεση μεταξύ του τρέχοντος και του προηγούμενου μπλοκ. Κάθε μπλοκ περνά από συνάρτηση κατακερματισμού hash function η έξοδος hash της οποίας, είναι αυτή που χαρακτηρίζει το μπλοκ.

Μόλις κάποιος miner καταφέρει να λύσει το εν λόγω μαθηματικό πρόβλημα, να παράξει δηλαδή ένα έγκυρο μπλοκ, το μεταδίδει στο δίκτυο. Τότε οι υπόλοιποι miners οφείλουν να επικυρώσουν την εγκυρότητά του. Η διαδικασία που ακολουθείται είναι η εξής:

1. Επαληθεύεται ότι το μπλοκ στο οποίο γίνεται αναφορά ως προηγούμενο υπάρχει και είναι έγκυρο

2. Επαληθεύεται ότι η χρονοσφραγίδα του μπλοκ έπεται χρονικά της χρονοσφραγίδας του προηγούμενου μπλοκ

3. Επαληθεύεται ότι οι συναλλαγές που περιέχονται στο μπλοκ είναι έγκυρες και συμβατές με την κατάσταση που δημιουργήθηκε μετά την καταχώρηση του προηγούμενου μπλοκ

4. Επαληθεύεται ότι το μαθηματικό πρόβλημα έχει λυθεί σωστά

2.2.5 Αλυσίδα Block / Blockchain

Το Blockchain [8] [9] είναι ένα κατανεμημένο σύστημα που μπορεί να αποθηκεύσει πληροφορίες με τρόπο που καθιστά αδύνατη την τροποποίησή τους. Πρόκειται για ένα καθολικό (ledger), το οποίο αντιγράφεται και μοιράζεται σε όλο το δίκτυο. Ανά πάσα στιγμή όλοι οι χρήστες του δικτύου κατέχουν ακριβώς το ίδιο αντίγραφο του ledger το οποίο περιέχει την κατάσταση του δικτύου τη συγκεκριμένη χρονική στιγμή.

Όπως φανερώνει και η ονομασία του, δεν είναι άλλο από μια αλυσίδα από μπλοκς. Εφόσον κάθε μπλοκ περιλαμβάνει στα δεδομένα του το hash του προηγούμενου έγκυρου μπλοκ, η σειρά τοποθέτησής τους είναι καθορισμένη. Κάθε μπλοκ που κρίνεται έγκυρο, σύμφωνα με τη διαδικασία που αναφέρθηκε στην προηγούμενη ενότητα, προστίθεται στο τέλος της αλυσίδας.

Λόγω της αμετάβλητης κρυπτογραφικής υπογραφής hash του κάθε μπλοκ η οποιαδήποτε αλλοίωση στο καθολικό, γίνεται αμέσως αντιληπτή. Αναλυτικότερα, εφόσον κάθε μπλοκ περνά από μια συνάρτηση κατακερματισμού, οποιαδήποτε ελάχιστη αλλαγή στο περιεχόμενο κάποιου μπλοκ (ακόμα και σε μία μόνο συναλλαγή), αλλάζει ολοκληρωτικά το hash του μπλοκ. Από τη στιγμή που το κάθε μπλοκ περιλαμβάνει στα δεδομένα του και το hash του προηγούμενου έγκυρου μπλοκ αλλά και μια χρονοσφραγίδα, δεν είναι δυνατή ούτε η μετατόπιση των μπλοκς στην αλυσίδα.

Με αυτό τον τρόπο εξασφαλίζεται ότι τα δεδομένα που καταχωρούνται στο Βλοσκσηαιν δεν μπορούν ούτε να διαγραφούν αλλά ούτε και να παραποιηθούν, επομένως η ακεραιότητα των δεδομένων που μοιράζονται είναι εγγυημένη.

Σε περίπτωση που κάποιος κακόβουλος χρήστης προσπαθήσει να αλλοιώσει το δικό του αντίγραφο του Blockchain, η διαφορά των εξόδων κατακερματισμού σε σχέση με όλα τα αντίγραφα που διατηρούν οι υπόλοιποι χρήστες είναι εύκολα εντοπίσιμη.

2.2.6 Πρωτόκολλο Συναίνεσης / Consensus Protocol

Τα πρωτοκολλα συναίνεσης [10] (γνωστά και ως μηχανισμοί συναίνεσης ή αλγόριθμοι συναίνεσης) είναι ο ασφαλής τρόπος συνεργασίας των υπολογιστών που αποτελούν μέρος ενός δικτύου, που ανήκουν δηλαδή σε ένα κατανεμημένο σύστημα. Αυτού του είδους οι μηχανισμοί χρησιμοποιούνται εδώ και δεκαετίες για την επίτευξη συναίνεσης σε εταιρικές υποδομές.

Τα τελευταία χρόνια, νέοι μηχανισμοί συναίνεσης έχουν δημιουργηθεί και εφαρμοστεί στα Blockchains για να εξυπηρετούν κρυπτοοικονομικά συστήματα και να συμφωνούν για την κατάσταση του δικτύου, που σημαίνει όλοι οι χρήστες να κατέχουν το ίδιο ακριβώς αντίγραφο του ledger.

Ο μόνος τρόπος να τεθεί σε κίνδυνο η συναίνεση, να υπερισχύσει δηλαδή μια παραποιημένη αλυσίδα Blockchain αντί της πραγματικής, είναι ο κακόβουλος χρήστης να αποκτήσει πρόσβαση σε ποσοστό τουλάχιστον 51% [11] της συνολικής υπολογιστικής ισχύος του δικτύου, κάτι που είναι πρακτικά αδύνατο με τον τρόπο που έχουν σχεδιαστεί οι μηχανισμοί.

Υπάρχουν διάφοροι μηχανισμοί συναίνεσης που επινοήθηκαν για χρήση σε κρυπτοοικονομικά συστήματα blockchain με δημοφιλέστερους του εξής δύο:

2.2.6.1 Proof of Work - PoW

Το PoW είναι το πρωτόκολλο που προτάθηκε αρχικά από τον Satoshi Nakamoto για την εξασφάλιση της συναίνεσης στο bitcoin blockchain. Σήμερα χρησιμοποιείται και για πολλά άλλα κρυπτοοικονομικά συστήματα blockchain όπως για παράδειγμα το Ethereum.

Πρόκειται για ένα περίπλοκο υπολογιστικό πρόβλημα η λύση του οποίου δεν μπορεί να βρεθεί με συστηματικό τρόπο αλλά μόνο με τυχαίες δοκιμές. Υπεύθυνοι για την επίλυση του προβλήματος αυτού είναι οι miners.

Όπως εξηγήθηκε σε προηγούμενη ενότητα, κάθε νέο μπλοκ περιλαμβάνει μεταξύ άλλων συναλλαγές, μία χρονοσφραγίδα και το hash του προηγούμενου μπλοκ. Με αυτά και επιπλέον ένα τυχαίο νούμερο σαν είσοδο σε μια συνάρτηση κατακερματισμού οι miners προσπαθούν να καταλήξουν σε μία έξοδο της συνάρτησης η οποία θα αρχίζει με έναν συγκεκριμένο αριθμό μηδενικών. Η δυσκολία επίλυσης αυτού του προβλήματος είναι εκθετική συναρτήσει του μήκους των μηδενικών που απαιτούνται.

Ο miner που θα καταφέρει πρώτος να επικυρώσει το νέο μπλοκ, επιβραβεύεται με τα νέα νομίσματα που δημιουργούνται.

2.2.6.2 Proof of Stake - PoS

Στην περίπτωση του PoS δεν υπάρχουν εξορύκτες (miners) αλλά επικυρωτές (validators). Ανάμεσα σε αυτούς επιλέγεται τυχαία ένας, ο οποίος πρέπει να δημιουργήσει το επόμενο μπλοκ. Για να έχουν τη δυνατότητα να επιλεγούν, οι επικυρωτές θέτουν ως εγγύηση ένα μέρος του κεφαλαίου τους (των κρυπτονομισμάτων τους). Όσο μεγαλύτερη εγγύηση έχει θέσει ένας επικυρωτής, τόσο μεγαλύτερη η πιθανότητα να επιλεγεί για τη δημιουργία του επόμενου μπλοκ.

Κάθε validator οφείλει να επικυρώνει τα μπλοκς που έχουν προταθεί από άλλους επικυρωτές. Αν δεν είναι συνεπής σε αυτή την υποχρέωση, μπορεί να του αφαιρεθεί μέρος της εγγύησης που έχει καταβάλει.

Για να θεωρηθεί μια κατάσταση του δικτύου ως έγκυρη πρέπει να συμφωνήσουν τα 2/3 των επικυρωτών.

Βάσει αυτού του μηχανισμού συναίνεσης η αμοιβή του επικυρωτή προέρχεται από τα τέλη συναλλαγών που περιλαμβάνονται στα μπλοκς.

Το Ethereum blockchain αναμένεται να αντικαταστήσει τον μηχανισμό συναίνεσης PoW με το πρωτόκολλο PoS.

2.3 Ethereum

2.3.1 Ιστορική Αναδρομή

Το Ethereum [12] περιγράφηκε αρχικά, στα τέλη του 2013, από τον Vitalik Buterin, ως αποτέλεσμα της έρευνας και της εμπλοκής του με την κοινότητα του Bitcoin. Στη συνέχεια, ο Vitalik δημοσίευσε το white paper του Ετηερευμ, όπου περιγράφεται με λεπτομέρεια τόσο ο σχεδιασμός σε τεχνικό επίπεδο, όσο και οι σκοποί που εξυπηρετεί το πρωτόκολλο του Ethereum.

Τον Ιανουάριο του 2014, ο Vitalik ανακοίνωσε επίσημα το εγχείρημα Ethereum στο συνέδριο του Bitcoin της Βόρειας Αμερικής.

Την ίδια περίοδο, ο Vitalik ξεκίνησε τη συνεργασία του με τον Gavin Wood και μαζί ιδρύσανε το Ethereum. Τον Απρίλιο του 2014, ο Gavin δημοσίευσε επιστημονική εργασία για το Ethereum, περιγράφοντας λεπτομερώς τις τεχνικές προδιαγραφές για την ανάπτυξη του Ethereum Virtual Machine (EVM), το οποίο θα αναλυθεί στη συνέχεια.

Το 2015, σε συνεργασία με τους Charles Hoskinson, Anthony Di Iorio και Joseph Lubin έθεσαν το σύστημα Ethereum σε λειτουργία.

Το 2016, ως αποτέλεσμα της κατάρρευσης ενός εγχειρήματος, το Ethereum χωρίστηκε σε δύο ξεχωριστά blockchains. Η νέα ξεχωριστή έκδοση είναι το σημερινό Ethereum και η αρχική συνεχιζόμενη έκδοση έγινε γνωστή ως Ethereum Classic.

2.3.2 Τι είναι το Ethereum

Βασισμένο στην καινοτομία του bitcoin, αποτελεί μια αναβαθμισμένη έκδοση blockchain με προηγμένα χαρακτηριστικά.

Αντίστοιχα με το bitcoin, το Ethereum [13] κατέχει το δικό του ψηφιακό νόμισμα που καλείται Ether (ETH). Ενώ και τα δύο blockchains επιτρέπουν τη χρήση ψηφιακού χρήματος χωρίς παρόχους, το Ethereum ξεφεύγει από ένα καθαρά χρηματοοικονομικό σύστημα, καθώς είναι προγραμματιζόμενο. Τι σημαίνει αυτο; Ότι μπορεί να κάνει οτιδήποτε.

Η καινοτομία στην περίπτωση του Ethereum είναι ότι υποστηρίζει μία Turing Complete γλώσσα προγραμματισμού σε μορφή έξυπνων συμβολαίων. Κάθε χρήστης του δικτύου μπορεί με προγραμματισμό να αναπτύξει σύνθετες εφαρμογές.

Αποτελεί την απαρχή μιας νέας εποχής στο διαδίκτυο, γνωστής ως Web3.

Η πρώτη εποχή του διαδικτύου, γνωστή ως Web1 περιελάμβανε στατικές ιστοσελίδες οι οποίες παρέχονταν στο χρήστη από κάποιο διακομιστή (server) και η αλληλεπίδραση του χρήστη με αυτές ήταν μονόδρομη. Το 2004 έγινε η μετάβαση στην Web2 εποχή με την ανάπτυξη δυναμικών και διαδραστικών ιστοσελίδων με τις οποίες ο χρήστης είχε πλέον αμφίδρομη αλληλεπίδραση. Το κοινό χαρακτηριστικό των δύο αυτών εποχών ήταν η εξάρτηση από κάποιο κεντρικό σύστημα.

Η σημερινή Web3 εποχή, βασίζεται στην αποκέντρωση.

Με το Ethereum γίνεται ένα βήμα μπροστά σε επίπεδο τεχνολογίας, αφού πέραν της καταγραφής δεδομένων στους κόμβους του δικτύου, γίνεται δυνατή και η παράλληλη εκτέλεση υπολογιστικού κώδικα σε πολυάριθμους υπολογιστές, που βρίσκονται σε διαφορετικά σημεία του πλανήτη.

Πρόκειται για μια παγκόσμια αποκεντρωμένη πλατφόρμα που να καρπώνεται τα οφέλη και την ασφάλεια της τεχνολογίας blockchain. Οι εφαρμογές δεν έχουν ένα μοναδικό σημείο αποτυχίας στην υποδομή τους (single point of failure) όπως ένας κεντρικός διακομιστής ενώ παράλληλα δεν υπάρχει ανάγκη για κάποιο κεντρικό σύστημα για την εκτέλεση των συναλλαγών των χρηστών. Δεν υπάρχει η έννοια της εξουσιοδότησης και οι χρήστες είναι ελεύθεροι να συμμετέχουν στο δίκτυο κατά βούληση, ενώ παράλληλα κατέχουν την κυριότητα των ψηφιακών τους περιουσιακών στοιχείων.

2.3.3 Smart Contract/Έξυπνα συμβόλαια

Τα έξυπνα συμβόλαια [14] (γνωστά και ως έξυπνες συμβάσεις) είναι απλά προγράμματα υπολογιστών που ζουν στο blockchain Ethereum.

Η βασική ιδέα πίσω από τα έξυπνα συμβόλαια είναι πως όροι συμβολαίων διαφόρων ειδών, όπως οινοκομικές συμφωνίες, εγγυήσεις, δικαιώματα ιδιοκτησίας κ.α. μπορούν να ενσωματωθούν σε λογισμικό, με τρόπο ώστε να καθίσταται δύσκολη ή και αδύνατη η αλλοίωση του περιεχόμενου τους. Ζώντας στο blockchain, καθίσταται σαφές, σύμφωνα με τα όσα επεξηγήθηκαν σε προηγούμενες ενότητες, ότι η ιδέα αυτή είναι πλέον ρεαλιστική.

Από τη στιγμή που θα δημοσιευτεί ένα έξυπνο συμβόλαιο στο Ethereum, θα είναι ονλινε και λειτουργικό για όσο διάστημα υπάρχει το Ethereum. Ούτε ο ίδιος ο συγγραφέας δεν μπορεί να το τροποποιήσει ή να το κατεβάσει. Δεδομένου ότι τα έξυπνα συμβόλαια είναι αυτοματοποιημένα, δεν κάνουν διακρίσεις σε βάρος κανενός χρήστη και είναι πάντα έτοιμα για χρήση. Εκτελούνται μόνο όταν ενεργοποιηθούν μέσω μιας συναλλαγής από έναν χρήστη ή κάποιο άλλο έξυπνο συμβόλαιο.

Γράφονται σε κάποια συμβατή γλώσσα προγραμματισμού με πιο διαδεδομένη τη γλώσσα Solidity. Η δομή των contracts μοιάζει με κλάσεις (classes) σε αντικειμενοστραφείς γλώσσες προγραμματισμού (object-oriented languages). Μπορούν να περιέχουν σταθερές, μεταβλητές, συναρτήσεις, σύνθετες δομές δεδομένων κ.λπ. Μπορούν επίσης να κληρωνόμουν άλλα contracts ή να χρησιμοποιούνται ως βιβλιοθήκες.

Παρά τη μεγάλη ευελιξία τους, τα smart contracts υπόκεινται σε κάποιους περιορισμούς όπως για παράδειγμα το μέγεθος που μπορούν να φτάσουν και το ότι δεν έχουν τη δυνατότητα να αντλήσουν πληροφορίες για τον πραγματικό κόσμο εξ αιτίας του ότι δεν μπορούν να στείλουν αιτήματα HTTP (HTTP requests).

2.3.4 Ψηφιακή Μηχανή Ethereum / EVM

Το Ethereum Virtual Machine (EVM) [15] είναι μια ισχυρή, εικονική μηχανή που υπάρχει ως μια ενιαία οντότητα που διατηρείται από χιλιάδες συνδεδεμένους υπολογιστές του δικτύου Ethereum και είναι υπεύθυνη για την εκτέλεση των smart contracts. Τα contracts αυτά μεταγλωττίζονται σε EVM bytecode και εκτελούνται πάνω στο EVM το οποίο είναι Turing complete, επομένως ικανό να εκτελέσει οποιοδήποτε λογικό βήμα μιας υπολογιστικής συνάρτησης.

Το περιβάλλον είναι σαφώς ορισμένο και πλήρως απομονωμένο, αφού ο κώδικας που εκτελείται στο EVM δεν έχει πρόσβαση στο δίκτυο, αλλά ούτε στα αρχεία συστήματος του

υπολογιστή ή οποιασδήποτε άλλης διαδικασίας εκτελείται παράλληλα. Ακόμη και ανάμεσα σε δύο έξυπνα συμβόλαια, η πρόσβαση είναι περιορισμένη.

Το EVM είναι απαραίτητο για το πρωτόκολλο του Ethereum και είναι καθοριστικό για τον μηχανισμό συναίνεσης του. Επιτρέπει σε οποιονδήποτε να εκτελέσει τον κώδικα σε ένα οικοσύστημα που είναι trustless, και στο οποίο μπορεί να διασφαλιστεί το αποτέλεσμα μιας ενέργειας.

Για κάθε εντολή που εκτελείται στο EVM, ένα σύστημα που παρακολουθεί το κόστος της εκτέλεσης, αναθέτει στην εντολή αυτή ένα σχετικό κόστος (gas). Όταν ένας χρήστης θέλει να εκτελέσει μια εντολή, διατηρεί και δεσμεύει το ποσό Ether που ισοδυναμεί με το gas, το οποίο πρέπει να πληρώσει για την εκτέλεση της εντολής.

Το EVM είναι στην ουσία μια μηχανή καταστάσεων που ορίζει την παρούσα κατάσταση του δικτύου με την οποία τα αντίγραφα όλων των χρηστών πρέπει να συμφωνούν. Για κάθε μπλοκ του Ethereum Blockchain υπάρχει μία μόνο κατάσταση. Το EVM καθορίζει επίσης του κανόνες της μετάβασης από μία έγκυρη κατάσταση σε μία άλλη.

Η ανάγκη ύπαρξης του EVM προκύπτει από το γεγονός ότι το Ethereum επιτρέπει να εκτελεστούν στο Blockchain πολύ σύνθετες λειτουργίες.

2.3.5 Λογαριασμοί / Accounts

Ένας λογαριασμός ethereum [16] είναι μια οντότητα η οποία κατέχει ένα πορτοφόλι με κάποιο υπόλοιπο ETH και έχει τη δυνατότητα να εκτελεί συναλλαγές στο δίκτυο.

Στο Ethereum υπάρχουν δύο τύποι λογαριασμού, όπου και οι δύο έχουν τη δυνατότητα να κατέχουν, στέλνουν και δέχονται ETH καθώς και να αλληλεπιδρούν με smart contracts.

Οι δύο τύποι λογαριασμών και οι διαφορές τους παρατίθενται πιο κάτω:

1. Ιδιωτικοί Λογαριασμοί / Externally-owned account (EOA)
   Είναι user-controlled λογαριασμοί, που σημαίνει ότι ελέγχονται από κάποιο χρήστη του δικτύου. Η δημιουργία τους έχει μηδενικό κόστος και ακολουθεί την πρακτική της ασύμμετρης κρυπτογραφίας, του ζεύγους δημοσίου-ιδιωτικού κλειδιού. Οποιοσδήποτε κατέχει το ιδιωτικό κλειδί ενός λογαριασμού έχει στα χέρια του τον έλεγχο των δραστηριοτήτων του λογαριασμού. Κάθε EOAλογαριασμός έχει τη δυνατότητα να αρχικοποιήσει κάποια συναλλαγή, ενώ κάθε συναλλαγή μεταξύ τέτοιου είδους λογαριασμών είναι καθαρά για την μεταβίβαση αξίας ETH.

2. Έξυπνα Συμβόλαια / Smart Contracts
   Είναι code-controlled λογαριασμοί, δηλαδή δεν ελέγχονται από κάποιο χρήστη αλλά από κώδικα. Δεν προσδιορίζονται από κάποιο ζεύγος κλειδιών, αλλά από τη λογική με την οποία έχουν προγραμματιστεί. Η δημιουργία τους συνεπάγεται κάποιο κόστος καθώς χρειάζονται χώρο στο δίκτυο για την αποθήκευσή τους. Μπορούν να εκτελέσουν μια συναλλαγή μόνο ως απάντηση στη λήψη μιας άλλης συναλλαγής. Οι συναλλαγές από έναν EOA σε έναν smart contract λογαριασμό μπορούν να περιλαμβάνουν τη μεταβίβαση ETH, την ενεργοποίηση συναρτήσεων του κώδικα του smart contract ή ακομά και τη δημιουργία ενός νέου contract.

2.4 Αποκεντρωμένος Αυτόνομος Οργανισμός / DAO

2.4.1 Τι είναι DAO

Με πηγή έμπνευσης την αποκέντρωση των κρυπτονομισμάτων, προέκυψε και η ιδέα της αποκέντρωσης ενός οργανισμού, έννοια της οποίας είναι η κατανεμημένη επίβλεψη και διαχείριση μιας οντότητας παρόμοιας με μια εταιρεία.

Αποκεντρωμένος Αυτόνομος Οργανισμός (Decentralized Autonomous Organization) [17] [18] καλείται μια αυτόνομη οντότητα που ζει στο blockchain και του οποίου η διαχείριση γίνεται συλλογικά από τα μέλη του, που μπορεί να είναι είτε άτομα, είτε οργανισμοί.

Ένα DAO διαφέρει από έναν παραδοσιακό οργανισμό που διοικείται από συμβούλια, επιτροπές και στελέχη. Πρόκειται για μια κοινότητα από μέλη, χωρίς κεντρική ηγεσία. Αντί να διοικείται από μια περιορισμένη ομάδα, χρησιμοποιεί ένα σύνολο κανόνων, γραμμένων σε κώδικα, που επιβάλλεται από το δίκτυο υπολογιστών λόγω της εκτέλεσης ενός κοινόχρηστου λογισμικού.

Έχει ενσωματωμένο θησαυροφυλάκιο (treasury) στο οποίο κανείς δεν έχει την εξουσία να έχει πρόσβαση χωρίς την έγκριση της ομάδας. Οι αποφάσεις διέπονται από προτάσεις και ψηφοφορία για να διασφαλιστεί ότι όλοι στον οργανισμό έχουν φωνή και ότι όλα γίνονται με διαφάνεια στο δίκτυο του blockchain. Ο κώδικας είναι αυτός που ορίζει πώς λειτουργεί ο οργανισμός και πώς δαπανόνται τα κεφάλαια.

Πρόκειται για έναν συλλογικό οργανισμό βασισμένο στην καινοτομία του blockchain, που επιτρέπει τη συνεργασία χρηστών από όλο τον κόσμο που εργάζονται για μια κοινή αποστολή. Παρ'όλη την αποκέντρωση και την αυτονομία εξακολουθεί να απαιτεί έντονη συμμετοχή από ανθρώπους που αλληλεπιδρούν συγκεκριμένα, σύμφωνα με το πρωτόκολλο που ορίζεται από το DAO, προκειμένου να λειτουργήσει.

2.4.2 Πώς λειτουργεί

Η ραχοκοκαλιά ενός DAO είναι το έξυπνο συμβόλαιό του. Το συμβόλαιο ορίζει τους κανόνες του οργανισμού και διαχειρίζεται τις λειτουργίες του. Μόλις το συμβόλαιο τεθεί σε λειτουργία, κανείς δεν μπορεί να αλλάξει τους κανόνες παρά μόνο με ψηφοφορία. Αν κάποιος προσπαθήσει να κάνει κάποια ενέργεια που δεν καλύπτεται από τους κανόνες και τη λογική του κώδικα, θα αποτύχει.

Η ομάδα λαμβάνει αποφάσεις συλλογικά και οι λειτουργίες εξουσιοδοτούνται αυτόματα όταν υπολογιστούν οι ψήφοι. Αυτό είναι δυνατό επειδή τα έξυπνα συμβόλαια είναι αμετάβλητα από τη στιγμή που ενεργοποιηθούν. Ένα μέλος, δεν μπορεί απλώς να τροποποιήσει τον κώδικα (τους κανόνες) του DAO χωρίς να το αντιληφθούν τα υπόλοιπα μέλη, επειδή όλα είναι δημόσια και διαφανή.

Για να γίνουν μέλη ενός DAO, οι χρήστες πρέπει να είναι κάτοχοι του κρυπτονόμισματος που χρησιμοποιεί το DAO. Η κατοχή του κρυπτονομίσματος δίνει γενικά στους χρήστες τη δυνατότητα να ψηφίσουν για προτάσεις και ενημερώσεις/αναβαθμίσεις.Η διαδικασία ψηφοφορίας ενός αποκεντρομένου αυτόνομου οργανισμού δημοσιεύεται στο blockchain, καθιστώντας όλες τις ενέργειες των χρηστών δημόσια ορατές.

Τα δικαιώματα ψήφου, ή αλλιώς το βάρος της ψήφου ενός χρήστη, συχνά κατανέμεται με βάση τον αριθμό των διακριτικών που διαθέτει ο χρήστης. Με τον όρο διακριτικά εννοείται καθετί που μπορεί να ορίσει κάποιο DAO ως απαραίτητο για τη συμμετοχή του χρήστη στο πρωτόκολλο. Μπορεί να είναι το ποσό του κρυπτονομίσματος που κατέχει ο χρήστης, η αξία κάποιου περιουσιακού στοιχείου του DAO που κατέχει ο χρήστης, ή κάτι άλλο που ορίζεται από το πρωτόκολλο του κάθε DAO.

Τα έξυπνα συμβόλαια, αυτές οι λογικά κωδικοποιημένες συμφωνίες, υπαγορεύουν τη μεταγενέστερη λειτουργία του DAO σύμφωνα με την υποκείμενη δραστηριότητα στο δίκτυο του blockchain. Με βάση το αποτέλεσμα μιας ψηφοφορίας, λαμβάνεται η απόφαση, από την οποία εξαρτάται ποιο συγκεκριμένο μέρος του κώδικα (ποιες συναρτήσεις) θα εκτελεστεί, δηλαδή ποιες ενέργειες θα ακολουθήσει το πρωτόκολλο στη συνέχεια.

2.4.3 Σε τι χρησιμεύει

Για τη δημιουργία ενός οργανισμού, απαιτείται η επίδειξη μεγάλης εμπιστοσύνης στα άτομα με τα οποία πρόκειται να υπάρξει συνεργασία. Ιδιαίτερα σε περιπτώσεις που η συνεργασία περιλαμβάνει τη συνεισφορά χρημάτων, είναι πολύ δύσκολο να υπάρξει εμπιστοσύνη στο πρόσωπο κάποιου άλλου, πόσο μάλλον όταν ο άλλος είναι κάποιος άγνωστος.

Με ένα DAO δεν χρειάζεται εμπιστοσύνη σε κανέναν άλλον στην ομάδα, πέρα από τον κώδικα του έξυπνου συμβολαίου, ο οποίος είναι 100% διαφανής και επαληθεύσιμος από οποιονδήποτε. Αυτό δημιουργεί ευκαιρίες για παγκόσμιες συνεργασίες και συντονισμό αγνώστων, ή και γνωστών, μελών χωρίς κάποιον έμπιστο τρίτο φορέα.

Ένα DAO έχει σκοπό να βελτιώσει την παραδοσιακή δομή διαχείρισης πολλών οργανισμών και στοχεύει στη διόρθωση όλων όσων ήταν λανθασμένα με τον τρόπο λειτουργίας των σύγχρονων οργανισμών. Εκμεταλλεύεται την τεχνολογία του blockchain και επωφελείται από όλες τις δυνατότητες που αυτό μπορεί να προσφέρει.

2.4.4 Σύγκριση παραδοσιακού οργανισμού με DAO

Παραδοσιακός Οργανισμός	**Αποκεντρωμένος Αυτόνομος Οργανισμός**
Συνήθως ιεραρχικός	Συνήθως επίπεδος και πλήρως δημοκρατικός
Ανάλογα τη δομή, αλλαγές μπορεί να απαιτηθούν από ένα μέλος ή μπορεί να προσφέρεται ψηφοφορία	Απαιτείται ψηφοφορία για την υλοποίηση οποιασδήποτε αλλαγής
Εάν προσφέρεται ψηφοφορία, οι ψήφοι καταμετρούνται εσωτερικά και το αποτέλεσμα αντιμετωπίζεται χειροκίνητα	Οι ψήφοι καταμετρούνται και το αποτέλεσμα εφαρμόζεται αυτόματα χωρίς έμπιστο τρίτο φορέα
Απαιτεί ανθρώπινο χειρισμό ή κεντρικά ελεγχόμενο αυτοματισμό, επιρρεπής σε χειραγώγηση	Οι λειτουργίες του οργανισμού εκτελούνται αυτόματα
Η δραστηριότητα είναι συνήθως ιδιωτική και περιορισμένη στο κοινό	Κάθε δραστηριότητα είναι διαφανής και πλήρως δημόσια

Πίνακας 2.1: *Παραδοσιακός Οργασνισμός VS DAO*

Κεφάλαιο 3

DAOs και ΜΚΟ

Στο κεφάλαιο αυτό περιγράφεται η ιδέα στην οποία βασίστηκε η εργασία. Πρόκειται για το ζήτημα της φιλανθρωπίας. Αναλύεται η μέχρι σήμερα μορφή της και κατά πόσο έχει θετικό αντίκτυπο στην κοινωνία, σε συνάρτηση με όλα τα προβλήματα που προκύπτουν από αυτή. Παρατίθεται η ανάγκη για τη δημιουργία on chain charities και ποια ζητήματα λύνονται με αυτή τη νέα προσέγγιση.

3.1 Φιλανθρωπία

3.1.1 Τι είναι

Φιλανθρωπία είναι η πράξη που κάνει κάποιος ώστε να βοηθήσει άλλους ανθρώπους.

Ετυμολογικά σημαίνει «αγάπη για τον άνθρωπο», με την έννοια της φροντίδας για την θρέψη, την ανάπτυξη και την ενίσχυση δεινοπαθούντων συνανθρώπων.

Ο πιο συμβατικός σύγχρονος ορισμός είναι οι πρωτοβουλίες, για το κοινό καλό, με έμφαση στην ποιότητα της ζωής. Πρόκειται για πρωτοβουλίες ιδιωτών ή ιδρυμάτων που έχουν στόχο τη βελτίωση της ποιότητας ζωής ανθρώπων ή κοινοτήτων.

Στην αγγλόγλωσση βιβλιογραφία αναφέρεται ως «charity» και συνδέεται συνήθως με μεγάλες διεθνείς οργανώσεις, που αναλαμβάνουν δράσεις κυρίως σε χώρες όπου υπάρχει ανθρωπιστική κρίση.

Κατά τη φιλανθρωπία, διενεργούνται ενέργειες από κάποιον ή κάποιους ώστε να βοηθήσουν ευπαθείς ομάδες ανθρώπων που έχουν διάφορες ανάγκες. Συνήθως η πράξη αφορά στην προσφορά υλικών αγαθών (χρήματα, κτίρια, τρόφιμα κ.ά.) που παραχωρούνται χωρίς αμοιβή ή αντάλλαγμα.

Πρόκειται συνήθως για μια πράξη στιγμιαία και ευκαιριακή που στόχοι της είναι η παροχή βοήθειας και η ανακούφιση σε κάποια δύσκολη κατάσταση. Στις περισσότερες περιπτώσεις δεν δημιουργείται μια μόνιμη σχέση συμπαράστασης και αλληλεγγύης εκείνου που ασκεί τη φιλανθρωπία με τους επωφελούμενους.

3.1.2 Γιατί είναι καλό να γίνεται

Ο Αριστοτέλης είχε πει: ¨Η μόρφωση του μυαλού χωρίς τη μόρφωση της καρδιάς δεν είναι καθόλου μόρφωση¨.

Η προσέγγιση αυτή προσδιορίζει απόλυτα την ουσία της έννοιας της φιλανθρωπίας. Η φιλανθρωπία είναι μια άσκηση, μια εκπαίδευση που διαμορφώνει τον χαρακτήρα ώστε να σκέφτεται λιγότερο το «εγώ», αλλά περισσότερο το «εμείς».

Οι άνθρωποι που δεν συμμετέχουν σε κάποια φιλανθρωπική ή εθελοντική δράση χάνουν πολλά! Κερδίζει τεράστια ικανοποίηση όποιος γνωρίζει ότι έχει βοηθήσει άλλους ανθρώπους που το έχουν ανάγκη. Έτσι, κατά κάποιο τρόπο, η φιλανθρωπία είναι μια κατάσταση που κερδίζουν και οι δύο πλευρές. Νιώθεις καλά για τον εαυτό σου και βοηθάς και τους άλλους.

Σημαντικό είναι να κατανοήσουμε ότι η φιλανθρωπία εκφράζεται με πολλούς και διαφορετικούς τρόπους, όλοι εκ των οποίων είναι εξίσου σημαντικοί.

Η φροντίδα για τους συνανθρώπους μας είναι το στοιχείο που προσδίδει σε όλους μας την ανθρώπινή μας διάσταση. Είναι ο τρόπος να κάνουμε τον κόσμο καλύτερο για όλους. Και αν δεν μπορούμε να αλλάξουμε ολόκληρο τον κόσμο, μπορούμε τουλάχιστον να προσπαθήσουμε να αλλάξουμε τον κόσμο ενός ανθρώπου!

3.2 Οι φιλανθρωπικές οργανώσεις του σήμερα

3.2.1 Ποια προβλήματα προκύπτουν

Όταν αποφασίζουν να δωρίσουν κεφάλαια για φιλανθρωπικούς σκοπούς, πολλοί αναρωτιούνται εάν η συνεισφορά τους θα έχει αντίκτυπο ή όχι. Ποιο κάτω παρουσιάζονται κάποια από τα βασικότερα προβλήματα που αντιμετωπίζουν οι σύγχρονοι φιλανθρωπικοί οργανισμοί

3.2.1.1 Διαφάνεια / Transparency

Αρκετοί μη κερδοσκοπικοί οργανισμοί έχουν κλονίσει την εμπιστοσύνη των ανθρώπων στη φιλανθρωπία, και τους έχουν κάνει να αμφισβητούν την αξιοπιστία των φιλανθρωπικών πρωτοβουλιών, συμμετέχοντας σε σκιερά προγράμματα για την άντληση περισσότερων εσόδων. Η διαφάνεια είναι ένα από τα βασικά ζητήματα στον σημερινό φιλανθρωπικό κόσμο. Σε μεγάλες, κεντρικοποιημένες φιλανθρωπικές οργανώσεις, υπάρχει πάντα η πιθανότητα κάθε μεσάζοντας (που υπάρχουν πολλοί), να καταχραστεί μέρος των δωρεών.

3.2.1.2 Τρίτος Φορέας

Με τον όρο τρίτος φορέας υπονοείται μια οντότητα που εμπλέκεται με κάποιο τρόπο σε μια αλληλεπίδραση που είναι κυρίως μεταξύ δύο άλλων οντοτήτων. Στην περίπτωση ενός φιλανθρωπικού οργανισμού τρίτος φορέας μπορεί να θεωρηθεί και ο ίδιος ο οργανισμός, καθώς είναι ο μεσάζοντας ανάμεσα σε μια αλληλεπίδραση που στην ουσία γίνεται ανάμεσα στον δωρητή και τον δικαιούχο. Επίσης μια τράπεζα ή κάποιο άλλο χρηματοπιστωτικό ίδρυμα, είναι ο τρίτος φορέας ανάμεσα στον δωρητή και τον οργανισμό ή ανάμεσα στον οργανισμό και τον δικαιούχο. Τελικά, μια συναλλαγή που ουσιαστικά αφορά τον δωρητή και τον δικαιούχο, καταλήγει σε πολλαπλές συναλλαγές, στην καλύτερη περίπτωση, μεταξύ δωρητή-χρηματοπιστωτικού ιδρύματος-φιλανθρωπικού οργανισμού-χρηματοπιστωτικού ιδρύματος-δικαιούχου. Από μια συναλλαγή μεταξύ δύο οντοτήτων, προκύπτει ένας σιδηρόδρομος από τον οποίο πρέπει να εγκριθεί η συναλλαγή για να γίνει πραγματικότητα.

3.2.1.3 Ιδιωτικότητα / Privacy

Η δωρεά σε φιλανθρωπικές οργανώσεις περιλαμβάνει τις πλείστες φορές την αποκάλυψη της ταυτότητας του δωρητή στα χέρια της φιλανθρωπικής οργάνωσης, και κατ' επέκταση, σε πολλές άλλες άλλες οργανώσεις και φορείς. Ακόμη και αν μέσω της ίδιας της οργάνωσης διατηρηθεί η ανωνυμία του δωρητή, υπάρχουν πολλοί τρόποι να υπάρξει διαρροή μιας τέτοιας πληροφορίας, όπως για παράδειγμα μέσω κάποιας τραπεζικής συναλλαγής ή απλά από στόμα σε στόμα. Κάτι τέτοιο πολλές φορές δεν είναι επιθυμητό από τους δωρητές καθώς έτσι γίνεται φανερή η οικονομική τους κατάσταση, μπορεί να ενοχληθούν από άλλους φορείς ή οντότητες που ζητούν επίσης κάποια οικονομική στήριξη, ή μπορει ακόμα να βρεθούν και στο στόχαστρο κακόβουλων. Η ιδιωτικότητα και η ανωνυμία είναι στη σημερινή κοινωνία σημαντική για πολλούς δωρητές και μπορεί να γίνει η αιτία αποφυγής κάποιας φιλανθρωπικής πράξης.

3.2.1.4 Φόροι / Fees

Τα χρηματοπιστωτικά ιδρύματα, μέσω των οποίων πραγματοποιούνται οι μεταφορές κεφαλαίων, πολλές φορές και οι κυβερνήσεις επιβάλλουν τέλη για διεθνείς συναλλαγές, με αποτέλεσμα ένα σημαντικό ποσοστό μιας δωρεάς να χάνεται.

3.2.1.5 Χρόνος

Εξ αιτίας των μηχανισμών μεταφοράς κεφαλαίων μπορεί να χρειαστούν μέρες, ίσως και εβδομάδες για την έγκριση και μεταβίβαση κάποιου ποσού στο λογαριασμό κάποιου δικαιούχου.

3.2.1.6 Στελέχωση

Καθώς ο αριθμός των ανθρώπων που είναι πρόθυμοι να προσφέρουν εθελοντικά σε μη κερδοσκοπικούς οργανισμούς μειώνεται, οι οργανισμοί γεφυρώνουν αυτό το χάσμα προσλαμβάνοντας περισσότερους εργαζομένους. Έτσι, κεφάλαια που προορίζονται ως δωρεές μπορούν να διατεθούν προς την πληρωμή στελεχών και προσωπικού προκειμένου να διασφαλιστεί η ομαλή λειτουργία του φιλανθρωπικού ιδρύματος.

3.2.1.7 Συμμετοχή

Η σημερινή δομή των φιλανθρωπικών οργανισμών δεν επιτρέπει την ουσιαστική εμπλοκή των δωρητών στο έργο που εκτελούν. Οι δωρητές προσφέρουν τα χρήματά τους στους οργανισμούς χωρίς όμως να έχουν λόγο στο που θα καταλήξει η προσφορά τους. Ναι μεν πολλοί οργανισμοί έχουν κάποιο γενικό σύνολο στο οποίο στοχεύουν να βοηθήσουν και ο δωρητής γνωρίζει ότι η προσφορά του θα συμβάλει σε αυτόν τον τομέα, αλλά δεν μπορεί να εκφέρει πιο συγκεκριμένη άποψη για το πώς θέλει να χρησιμοποιηθεί η δωρεά του. Οι αποφάσεις για το πώς θα κατανεμηθούν τα κεφάλαια που διαθέτει ο οργανισμός, λαμβάνονται από επιτροπές και στελέχη του εκάστοτε οργανισμού.

3.2.2 Παραδείγματα

Πιο κάτω φαίνονται κάποια παραδείγματα Φιλανθρωπικών Οργανώσεων μέσω των οποίων γίνονται φανερά κάποια από τα προβλήματα που αναφέρονται στην προηγούμενη ενότητα.

1. National Children's Leukemia Foundation (America)
   Ένα παράδειγμα που αποκαλύπτει προβλήματα που αναφέρονται πιο πάνω είναι η περίπτωση του NCLF στην Αμερική, το οποίο συγκέντρωσε περίπου 9,7 εκατομμύρια δολάρια σε φιλανθρωπικές συνεισφορές, αλλά σύμφωνα με το CNN [19], δαπάνησε μόνο 57.000 δολάρια για βοήθεια σε ασθενείς με λευχαιμία. Περίπου 1,3 εκατομμύρια δολάρια, συν απολαβές, πήγαν κατευθείαν στην τσέπη του ιδρυτή του NCLF, ο οποίος ίδρυσε τον συγκεκριμένο οργανισμό έπειτα από τον χαμό του γιου του από λευχαιμία.

2. Alzheimer's Association
   Χωρίς να αμφισβητείται η προσφορά και η αξιοπιστία του συγκεκριμένου ιδρύματος, τα στατιστικά στοιχεία που αφορούν τις συνολικές δαπάνες του μπορούν να προβληματίσουν τους δωρητές. Σύμφωνα με έρευνες [20], 7.40% δαπανόνται σε διοικητικούς σκοπούς, 15.96% σε fundraising και το υπόλοιπο 76.63% για τον σκοπό του ιδρύματος. Για παράδειγμα, εάν κάποιος δωρίσει 1.000 ευρώ στο Alzheimer's Association, με βάση την ανάλυση του προϋπολογισμού τους, 74 ευρώ θα δαπανηθούν για την πληρωμή διοικητικών εξόδων, 160 ευρώ θα χρησιμοποιηθούν για τη συγκέντρωση πρόσθετων δωρεών και 766 ευρώ της δωρεάς θα δαπανηθούν για την αποστολή τους. Σίγουρα το ποσό που προσφέρεται για τον σκοπό της δωρεάς δεν είναι αμελητέο, αλλά μήπως θα μπορούσε να είναι ακόμη μεγαλύτερο;

3. Against Malaria Foundation
   Το AMF είναι μια φιλανθρωπική οργάνωση με έδρα το Ηνωμένο Βασίλειο που παρέχει βοήθεια σε πληθυσμούς υψηλού κινδύνου για ελονοσία, κυρίως στην Αφρική. Χωρίς αμφιβολία το έργο που επιτελεί είναι σπουδαίο και αξίζει τη στήριξη από όλο τον κόσμο. Υπάρχει μια λίστα από χώρες οι οποίες για να στείλουν τη δωρεά τους στον συγκεκριμένο οργανισμό δικαιούνται φοροαπαλλαγή. [21] Δυστυχώς η Ελλάδα και πολλές άλλες χώρες δεν χρήζουν αυτής της διευκόλυνσης. Σε περίπτωση που κάποιος Έλληνας για παράδειγμα πολίτης επιθυμεί να ενισχύσει οικονομικά το συγκεκριμένο ίδρυμα, θα πρέπει πέραν του ποσού που επιθυμεί να δωρίσει να πληρώσει έναν μη αμελητέο φόρο για την πραγματοποίηση της συναλλαγής. Αν ληφθούν υπόψην και οι μεταβολές των συναλλαγμάτων, η τελική αξία της δωρεάς μπορεί να είναι πολύ χαμηλότερη από την επιθυμητή.

Υπάρχουν εκατοντάδες άλλα παραδείγματα που μπορούν να παρατεθούν τα οποία παρουσιάζουν τα διάφορα προβλήματα που αντιμετωπίζουν οι σύγχρονες φιλανθρωπικές οργανώσεις. Τα πιο πάνω ήταν απλά ενδεικτικά. Επίσης, πολλά από τα προβλήματα που αναφέρονται πιο πάνω δεν εξαρτόνται από τις οργανώσεις αυτές καθάυτές αλλά από το οικονομικό σύστημα και διάφορα άλλα κοινωνικά ζητήματα.

3.3 On chain Charities

3.3.1 Ποια προβλήματα λύνονται

Πιο κάτω, παρατίθενται οι λύσεις που δύναται να προσφέρει ένα DAO και κατ' επέκταση το blockchain στα προβλήματα που αναφέρθηκαν στην προηγούμενη ενότητα.

3.3.1.1 Διαφάνεια / Transparency

Το Blockchain παρέχει μεγάλη διαφάνεια πίσω από τους μη κερδοσκοπικούς οργανισμούς. Δεδομένου ότι είναι ένα δημόσιο καθολικό που είναι ορατό από οποιονδήποτε, επιτρέπει εξαιρετικά ορατές και ανιχνεύσιμες συναλλαγές, και καθιστά δυνατή την παρακολούθησή τους από τους χορηγούς. Παρακολουθώντας ολόκληρη τη σειρά των συναλλαγών, οι χορηγοί μπορούν εύκολα να ανακαλύψουν εάν τα κεφάλαιά τους έφτασαν τον επιδιωκόμενο στόχο. Με την αμετάβλητη δομή του blockchain, οι δωρεές καταγράφονται μόνιμα και δεν μπορούν να παραποιηθούν, δίνοντας μεγαλύτερη ευθύνη στους δικαιούχους όσον αφορά τον τρόπο με τον οποίο δαπανώνται. Αποτέλεσμα της πλήρους διαφάνειας είναι ότι καθίσταται πολύ δύσκολη η διάπραξη απάτης.

3.3.1.2 Τρίτος Φορέας

Με τις συναλλαγές που πραγματοποιούνται σε δίκτυο blockchain, ο αριθμός των μεσαζόντων μεταξύ των δωρητών και εκείνων που θέλουν να βοηθήσουν μειώνεται στο ελάχιστο. Πλέον οι συναλλαγές αφορούν μόνο τους άμεσα εμπλεκόμενους, τον δωρητή και τον δικαιούχο και μπορούν να γίνονται άμεσα χωρίς της επίβλεψη και την έγκριση οποιουδήποτε τρίτου.

3.3.1.3 Ιδιωτικότητα / Privacy

Με το blockchain, το απόρρητο των δωρητών δεν θα παραβιάζεται, καθώς τα προσωπικά τους στοιχεία είναι κρυπτογραφημένα και μη ορατά στους χρήστες.

3.3.1.4 Φόροι / Fees

Οι πληρωμές που βασίζονται σε blockchain αποφέρουν φορολογικά οφέλη. Οι συναλλαγές με κρυπτονομίσματα, δεν προσελκύουν φόρους υπεραξίας. Επιπλέον, καθώς οι συναλλαγές μπορεί να προγρατοποιούνται σε παγκόσμια εμβέλεια, η επιβολή τελών για διεθνείς πληρωμές δεν θα είναι επίσης πρόβλημα, καθώς τα τέλη μεταφοράς κρυπτονομισμάτων είναι πολύ χαμηλότερα.

3.3.1.5 Χρόνος

Οι συναλλαγές που εκτελούνται σε blockchain μπορούν να φτάσουν στους παραλήπτες γρηγορότερα από ό,τι εάν πραγματοποιούνται μέσω άλλων μεθόδων συναλλαγής.

3.3.1.6 Στελέχωση

Όπως έχει εξηγηθεί και σε προηγούμενη ενότητα, ένα DAO είναι ένας αυτόνομος οργανισμός πράγμα που σημαίνει ότι η λειτουργία του δεν εξαρτάται από κάποιον διαχειριστή. Με βάση τους κανόνες που έχουν τεθεί κατά τη δημιουργία του εκτελεί τις κατάλληλες ενέργειες για την ορθή λειτουργία του οργανισμού. Αυτή η μορφή διαχείρισης προσφέρει χαμηλότερο κόστος σε σύγκριση με ένα παραδοσιακό οργανισμό, αφού αποφεύγονται τα έξοδα για τη στελέχωση του οργανισμού με προσωπικό, κάτι το οποίο σε άλλη περίπτωση θα ήταν απαραίτητο.

3.3.1.7 Συμμετοχή

Εφόσον ένα DAO διοικείται συλλογικά από όλα τα μέλη του, τότε όλες οι αποφάσεις λαμβάνονται από κοινού και με ψηφοφορία. Ο κάθε συμμετέχοντας έχει φωνή και μπορεί να εμπλεκεί ενεργά στις αποφάσεις εκφέροντας άποψη για το πώς θέλει να χρησιμοποιηθεί η δωρεά του.

3.3.2 Τι υπάρχει

Η πιο κοινή ενσωμάτωση της τεχνολογίας blockchain στη φιλανθρωπία αυτή τη στιγμή είναι οι δωρεές κρυπτονομισμάτων. Αρκετές φιλανθρωπικές οργανώσεις έχουν επιλέξει να λαμβάνουν δωρεές σε μορφή κρυπτονομισμάτων, ενώ έχουν δημιουργηθεί πολλές πλατφόρμες που προωθούν αυτές τις οργανώσεις. Επιπλέον έχουν γίνει κάποιες προσπάθειες για την ανάπτυξη κάποιων DAO με φιλανθρωπικό χαρακτήρα.

Ακολουθούν κάποια παραδείγματα ενεργών οργανώσεων τα οποία είναι ενδεικτικά παραδείγματα για το τι υπάρχει αυτή τη στιγμή στον χώρο.

1. The Giving Block

   Το Giving Block [22] διευκολύνει τη συγκέντρωση διαφόρων κρυπτονομισμάτων για μη κερδοσκοπικούς οργανισμούς. Στόχος του είναι η ενδυνάμωση οργανισμών, φιλανθρωπικών ιδρυμάτων, πανεπιστημίων και θρησκευτικών οργανισμών, όλων των μεγεθών, για να επιτύχουν την αποστολή τους.

   Με την ανοδική αγορά κρυπτονομισμάτων του 2017-2018, εκατομμύρια άνθρωποι σε όλο τον κόσμο έκαναν μια περιουσία επενδύοντας σε κρυπτονομίσματα όπως το Bitcoin και το Ether. Όμως, ενώ εκατοντάδες εκατομμύρια δολάρια σε μορφή κρυπτονομισμάτων διοχετεύτηκαν για φιλανθρωπικούς σκοπούς, λίγες μη κερδοσκοπικές οργανώσεις ήταν στην πραγματικότητα εξοπλισμένες για να δεχτούν αυτές τις δωρεές.

   Οι μη κερδοσκοπικοί οργανισμοί και οι δωρητές κρυπτονομισμάτων χρειάζονταν κάτι που δεν υπήρχε: έναν τρόπο να βρουν ο ένας τον άλλον εύκολα ώστε να μπορούν να αλλάξουν τον κόσμο μαζί. Αυτός ήταν και ο σκοπός της δημιουργίας του The Giving Block. Μία πλατφόρμα που δίνει στους μη κερδοσκοπικούς οργανισμούς τη δυνατότητα να αποδέχονται κρυπτονομίσματα και επιτρέπει στους δωρητές να εντοπίζουν εύκολα και γρήγορα τις οργανώσεις που μπορούν να γίνουν αποδέχτες.

Μέσα σε λίγα μόλις χρόνια, το The Giving Block έχει αυξηθεί αλματωδώς. Σήμερα, οι δωρητές μπορούν, μέσω της συγκεκριμένης πλατφόρμας, να διαλέξουν ανάμεσα σε χιλιάδες μη κερδοσκοπικούς οργανισμούς και είναι πιο εύκολο από ποτέ οι ΜΚΟ να αρχίσουν να δέχονται δωρεές κρυπτονομισμάτων.

2. Giveth
   Το Giveth [23], κυκλοφόρησε τον Μάρτιο του 2021, και προσφέρει έναν απλό και βελτιστοποιημένο τρόπο, για να κάνει κανείς δωρεές σε διάφορα έργα φιλανθρωπικού χαρακτήρα, μέσω του Ethereum Blockchain.

   Ο στόχος του Giveth είναι να γίνει η πύλη για μη κερδοσκοπικούς οργανισμούς στο web3.

   Προσφέρει μια ομαλή διαδικασία ενσωμάτωσης για δωρητές και έργα. Η δημιουργία ενός έργου μπορεί να γίνει σε λίγα λεπτά, ενώ η δωρεά μπορεί να γίνει σε δευτερόλεπτα. Η εύρεση ποιοτικών έργων για κοινωνική ή περιβαλλοντική αλλαγή είναι εύκολη.

   Οι κατασκευαστές μπορούν να δημιουργήσουν τα δικά τους έργα και να αρχίσουν να συγκεντρώνουν κεφάλαια, ενώ οι δωρητές μπορούν να χρησιμοποιήσουν την πλατφόρμα για να δώσουν δωρεές σε έναν σκοπό ή ένα έργο.

   Τα ποσά που δωρίζονται αποστέλλονται απευθείας στη διεύθυνση Ethereum του ιδιοκτήτη του έργου. Η Giveth δεν εισπράττει χρεώσεις από αλληλεπιδράσεις στην πλατφόρμα και το 100% των κεφαλαίων πηγαίνουν στον σκοπό που ο δωρητής σκόπευε να υποστηρίξει.

3. Endaoment
   Το Endaoment [24] είναι ένα ίδρυμα που δημιουργήθηκε για αποκεντρωμένη χρηματοδότηση φιλανθρωπικών οργανισμών. Πρόκειται για μια πλατφόρμα στην οποία παρουσιάζονται φιλανθρωπικές οργανώσεις (στην Αμερική) οι οποίες δέχονται δωρεές σε κρυπτονομίσματα μέσω DAF (Donor-advised Fund - Το DAF είναι, από μόνο του, ένας μη κερδοσκοπικός οργανισμός που λειτουργεί ως μεσάζων. Τα DAF δέχονται τη δωρεά κρυπτονομισμάτων και εξαργυρώνουν αμέσως για να επανεπενδύσουν τα χρήματα στον ζητούμενο μη κερδοσκοπικό οργανισμό).

   Μπορεί κανείς να κάνει τη δωρεά του απευθείας σε κάποιον από τους υπάρχοντες οργανισμούς ή να δώσει τα χρήματα σε κάποια Community Funds τα οποία αποφασίζουν για το που θα δοθούν τα χρήματα αυτά.

   Φαίνεται να υπάρχει η πρόθεση στο μέλλον να γίνει decentralized και να έχει την μορφή DAO.

4. The UNICEF CryptoFund Το UNICEF CryptoFund [25] είναι ένα ταμείο που δημιουργήθηκε από την UNICEF για να υποστηρίξει open-source projects που στοχεύουν να ωφελήσουν παιδιά και νέους ανθρώπους σε όλο τον κόσμο. Το ταμείο δέχεται συνεισφορές σε κρυπτονομίσματα, όπως το Bitcoin και το Ethereum, και τα χρησιμοποιεί για να επενδύει σε εταιρείες που βασίζονται στην τεχνολογία blockchain.

   Το UNICEF CryptoFund έχει σκοπό να βοηθήσει τη UNICEF να εξερευνήσει την τεχνολογία blockchain και να βρει νέους τρόπους για να υποστηρίξει παιδιά και νέους

ανθρώπους που έχουν ανάγκη. Τα έργα που υποστηρίζονται από το ταμείο επιλέγονται βάσει του δυναμικού τους να έχουν θετικό αντίκτυπο στη ζωή των παιδιών και τη συμμόρφωσή τους με την αποστολή και τις αξίες της UNICEF.

Είναι μέρος της ευρύτερης στρατηγικής καινοτομίας της UNICEF, η οποία αποσκοπεί στη χρήση αναδυόμενων τεχνολογιών για τη δημιουργία νέων λύσεων σε ορισμένα από τα πιο επείγοντα προβλήματα του κόσμου.

3.3.3 Πώς διαφοροποιείται η παρούσα υλοποίηση

Όπως έχει αναφερθεί και προηγουμένως, η πιο κοινή χρήση της τεχνολογίας του blockchain είναι η δωρεά σε κρυπτονομίσματα. Παρ'όλάυτά έχουν γίνει προσπάθειες διάφοροι οργανισμοί να χτίστουν εξ ολοκλήρου στο blockchain.

Δεν είναι λίγοι αυτοί που επιχείρησαν να δημιουργήσουν DAOs που έχουν να κάνουν με τη φιλανθρωπία. Πρόκειται για μία καινοτομία που όπως φαίνεται έχει μεγάλες προοπτικές στον συγκεκριμένο τομέα, και που όλα δείχνουν ότι ήρθε για να αλλάξει για πάντα την σημερινή δομή των οργανώσεων αυτών και όχι μόνο.

Πολλές από τις επιχειρήσεις αυτές έχουν αποτύχει ή έχουν πάψει να είναι ενεργές για διάφορους άλλους λόγους. Άλλες λειτουργούν κανονικά μέχρι σήμερα αλλά δεν πρεσβεύουν ακριβώς την έννοια ενός DAO και άλλες έχουν δημιουργηθεί κεντρικοποιημένα με σκοπό όμως στο μέλλον να αποκτήσουν πλήρη αποκέντρωση.

Σίγουρα για να πετύχει κάτι καινούριο χρειάζεται χρόνος και προσπάθειες, προσπάθειες αποτυχημένες, ή επιτυχημένες που χρήζουν βελτίωσης.

Στα πλαίσια της παρούσας διπλωματικής εργασίας έχει γίνει μια προσπάθεια για τη δημιουργία ενός MVP (minimum valuable product), δηλαδή ενός προϊόντος με τα ελάχιστα δυνατά χαρακτηριστικά για να είναι βιώσιμο και λειτουργικό, τηρώντας όλες τις απαραίτητες προϋποθέσεις, για να μπορεί να θεωρηθεί ένας Αποκεντρωμένος Αυτόνομος Οργανισμός.

Πρόκειται για έναν οργανισμό που στόχο έχει την απευθείας μεταβίβαση κάποιας αξίας συγκεκριμένα σε αυτόν που το έχει ζητήσει και το χρειάζεται και όχι για μια πλατφόρμα μέσω της οποίας ο χρήστης μπορεί να επιλέξει έναν ήδη υπάρχοντα οργανισμό για να πραγματοποιήσει την δωρεά του. Επιπλέον, η παραχώρηση χρηματοδότησης γίνεται ή πλήρως ή καθόλου με συλλογική απόφαση από τους χρήστες του οργανισμού, σε αντίθεση με υπάρχουσες οργανώσεις που επιτρέπουν στον κάθε χρήστη να προσφέρει στον σκοπό που επιθυμεί με κίνδυνο όμως κανένα από τα έργα που φιλοξενούνται να μην λάβει ποτέ το πλήρες ποσό που επιθυμεί.

Για την εν λόγω υλοποίηση, που είναι χτισμένη σε ένα τοπικό blockchain δίκτυο, με πλήρη διαφάνεια, αποκέντρωση και αυτοματισμό δεν μπορεί να αμφισβητηθεί η μορφή της ως DAO.

Αδιαμφισβήτητα, δεν μπορεί να συγκριθεί με τις προσπάθειες που έχουν αναφερθεί πιο πάνω και άλλες αντίστοιχες γιατί όπως είναι λογικό κατά την υλοποίηση ενός project σε ρεαλιστικά σενάρια τα δεδομένα αλλάζουν και ίσως γιάυτό να μην υπάρχει μέχρι σήμερα ένας 100% Decentralized Autonomous Organization φιλανθρωπικού χαρακτήρα.

Παρ'όλάυτά είναι μια αρχική υλοποίηση η οποία μπορεί να επεκταθεί και ίσως να επιτύχει.

Μέρος II

Μελέτη Περίπτωσης Χρήσης

Κεφάλαιο 4

Ανάλυση και σχεδίαση

Στο κεφάλαιο αυτό δίνεται μια πρώτη εικόνα της υλοποίησης που ακολουθεί. Περιγράφεται η δομή του αποκεντρομένου αυτόνομου οργανισμού και ο τρόπος λειτουργίας του. Αναλύονται ενδελεχώς οι οντότητες και οι δυνατές λειτουργικότητες της εφαρμογής ενώ φανερώνεται ο σχεδιασμός και η αρχιτεκτονική του δημιουργήματος.

4.1 Κεντρική Ιδέα

Στόχος της παρούσας διπλωματικής εργασίας ήταν η μελέτη του blockchain και πως αυτό μπορεί να βελτιώσει τη σημερινή δομή των φιλανθρωπικών οργανώσεων. Με την εκμετάλλευση αυτής της σπουδαίας καινοτομίας της τεχνολογίας, γίνεται εφικτή η υπερπήδηση πολλών εμποδίων που καθιστούν αναξιόπιστες τις φιλανθρωπικές πρωτοβουλίες, με την μεχρι τώρα δομή τους, και αποτελούν τροχοπέδη για τον πολίτη της κοινωνίας που θέλει να προσφέρει βοήθεια.

Απόσταγμα της έρευνας που διεξήχθη, ήταν η δημιουργία ενός Αποκεντρωμένου Αυτόνομου Οργανισμού με φιλανθρωπικό χαρακτήρα, του «Charity DAO».

Σκοπός ήταν η δημιουργία ενός οργανισμού στον οποίο δικαίωμα συμμετοχής έχει οποιοσδήποτε από οποιοδήποτε μέρος του κόσμου, με μόνη προϋπόθεση την πρόσβαση στο διαδίκτυο. Το Charity DAO ξεφεύγει από το πλαίσιο μιας φιλανθρωπικής οργάνωσης γενικού σκοπού και γίνεται το μέρος όπου κανείς μπορεί να ζητήσει βοήθεια για συγκεκριμένο σκοπό ανάλογα με τις δικές του ανάγκες.

Πιο συγκεκριμένα, το Charity DAO δεν έχει σαν κεντρικό στόχο την σύτιση των παιδιών στις τριτοκοσμικές χώρες της Αφρικής, ή την ιατρική περίθαλψη των πληγέντων του πολέμου στην Ουκρανία ή την προστασία και μόρφωση των Αφγανών γυναικών. Ωστόσο, όλοι αυτοί είναι τομείς τους οποίους το Charity DAO μπορεί να στηρίξει οικονομικά, αλλά όχι σε μόνιμη βάση. Οι τομείς αυτοί δεν χρειάζονται μόνο χρήματα αλλά ανθρώπους, χέρια που να προσφέρουν βοήθεια, γιατρούς και ψυχολόγους που να κλείνουν πληγές, πράγματα τα οποία δεν μπορεί να προσφέρει ένα πρόγραμμα υπολογιστή. Για την εκπλήρωση των πιο πάνω υπάρχουν φορείς και οργανώσεις, εθελοντές και μη, που μάχονται στην πρώτη γραμμή για το καλύτερο δυνατο αποτέλεσμα, και που καμία τεχνολογία δεν μπορεί να αντικαταστήσει. Αυτό που μπορεί να υποσχεθεί ένα DAO, είναι ότι δε θα υπάρξει εκμετάλλευση και απώλεια οικονομικής στήριξης στη διαδικασία της συλλογής χρημάτων από όλο τον κόσμο, μέχρι την αποστολή τους στους ανθρώπους αυτούς που αναλαμβάνουν ουσιαστικά τη δράση.

Το Charity DAO είναι αυτό που θα προσφέρει το απαραίτητο ποσό που χρειάζεται ένα χωριό της Κένυας για να αποκτήσει σύστημα ύδρευσης και να μη χρειάζεται πια οι κάτοικοι να πηγαίνουν καθημερινά μέχρι το ποτάμι. Είναι αυτό που θα διαθέσει τα χρήματα για να χτιστεί σε ένα σχολείο στην Ουγκάντα μια επιπλέον τάξη για να μην κάθονται τα παιδιά το ένα πάνω στο άλλο. Είναι αυτό που θα στηρίξει οικονομικά την ανάπτυξη ενός κέντρου υγείας στις φαβέλες της Βραζιλίας.

Η κεντρική ιδέα ήταν η δημιουργία μιας σελίδας όπου ο κάθε ενδιαφερόμενος μπορεί να καταθέση μία πρόταση με την οποία ζητά ένα συγκεκριμένο ποσό για την υλοποίηση ενός συγκεκριμένου σκοπού - έργου για το οποίο δίνει τις απαραίτητες πληροφορίες και εξηγήσεις.

Εάν η πρόταση αυτή θα εγκριθεί από τον οργανισμό, εξαρτάται από τα μέλη του. Οι αποφάσεις λαμβάνονται συλλογικά μετά από ψηφοφορία στην οποία μπορεί να συμμετέχει κανείς κάνοντας κάποια δωρεά. Υπάρχει ένα ελάχιστο ποσό το οποίο χρειάζεται κάποιος να προσφέρει για να αποκτήσει δικαίωμα ψήφου, και ανάλογα με το συνολικό ποσο που δωρίζει στον οργανισμό τότε τα δικαιώματα ψήφου του μπορούν να αυξηθούν.

Το ποιες προτάσεις θα εγκριθούν εξαρτάται όχι μόνο από την έκβαση της ψηφοφορίας αλλά και από το συνολικό ποσό που υπάρχει στο treasury του οργανισμού.

Οι δικαιούχοι των προτάσεων που εγκρίνονται λαμβάνουν αυτόματα, μέσω του smart contract, στους λογαριασμούς τους το αντίστοιχο ποσό.

Η λειτουργία πραγματοποιείται σε γύρους. Κάθε γύρος περιλαμβάνει τη διαδικασία της κατάθεσης προτάσεων και δωρεών και τη διαδικασία της ψηφοφορίας που θα έχει ως αποτέλεσμα τις νικηφόρες προτάσεις.

Οι λεπτομέρειες της λειτουργίας του οργανισμού αναλύονται στη συνέχεια.

4.2 Ανάλυση της ιδέας

4.2.1 Κόμβοι - Συμμετέχοντες

Στο DAO που αναπτύχθηκε υπάρχουν δύο τύποι συμμετεχόντων, οι οποίοι έχουν γίνει ήδη αντιληπτοί από τη σύντομη επεξήγηση της κεντρικής ιδέας. Πιο συγκεκριμένα, πρόκειται για τους ακόλουθους δύο:

4.2.1.1 Δωρητές

Οι δωρητές είναι ουσιαστικά τα στελέχη στα οποία βασίζεται η λειτουργία όλου του οργανισμού και χωρίς τους οποίους τίποτα δεν είναι εφικτό. Είναι αυτοί που προσφέρουν τα χρήματά τους στο treasury του DAO με σκοπό να τα χαρίσουν σε ανθρώπους που τα χρειάζονται για την υλοποίηση κάποιου σκοπού ή έργου. Είναι επίσης αυτοί που με τη ψήφο τους λαμβάνουν τις αποφάσεις για το πώς θα διανεμηθούν τα κεφάλαια του οργανισμού. Το δικαίωμα ψήφου δίνεται σε κάθε δωρητή που έχει προσφέρει στο treasury πάνω από ένα συγκεκριμένο ελάχιστο ποσό, και το βάρος της ψήφου μπορεί να αυξηθεί ανάλογα με τις συνολικές δωρεές προς τον οργανισμό. Υπάρχει βέβαια ένα πλαφόν, ένα μέγιστο ποσό συνολικών δωρεών που σε περίπτωση που ξεπεραστεί δεν αυξάνεται πλέον το βάρος της ψήφου,

έτσι ώστε κανείς να μην μπορεί να καταλάβει τόσο μεγάλο ποσοστό ψήφων που να μπορεί να καθορίζει τις αποφάσεις.

4.2.1.2 Επωφελούμενοι - Δικαιούχοι

Οι επωφελούμενοι (beneficiaries) είναι αυτοί που μέσω του Charity DAO ζητούν από τους δωρητές την οικονομική υποστήριξη για την πραγμάτωση κάποιου έργου. Οποιοσδήποτε, από οπουδήποτε και για οποιοδήποτε λόγο μπορεί να ζητήσει χρηματοδότηση μέσω του DAO για να εκπληρώσει τη δράση του. Αυτό που χρειάζεται είναι να καταθέσει την προτασή του και να πείσει τους δωρητές ότι αξίζει την στήριξη που αναζητά. Σε περίπτωση που η ψηφοφορία είναι υπέρ του και υπάρχει στο treasury του οργανισμού διαθέσιμο το ζητούμενο κεφάλαιο, τότε το λαμβάνει απευθείας στον λογαριασμό του χωρίς καθυστερήσεις και φορολογήσεις, και οφείλει να το χρησιμοποιήσει για τον επιδιωκόμενο στόχο.

4.2.2 Λειτουργικότητες

4.2.2.1 Δωρητές

1. Δωρεά
   Προσφορά χρημάτων στο treasury του DAO

2. Ψηφοφορία
   Επιλογή της επιθυμητής πρότασης για οικονομική στήριξη

3. Εκπροσώπηση
   Κάθε δωρητής έχει το δικαίωμα να μεταφέρει τα δικαιώματα ψήφου του σε κάποιον άλλο δωρητή, ο οποίος κατέχει και αυτός το δικαίωμα να ψηφίζει, για να τον εκπροσωπεί. Αντίστοιχα, μπορεί ανά πάσα στιγμή να ανακαλέσει και να έχει ξανά το δικαίωμα να ψηφίζει ο ίδιος.

4.2.2.2 Επωφελούμενοι

1. Πρόταση
   Παρουσίαση του επιθυμητού έργου - δράσης και του απαραίτητου ποσού που χρειάζεται για να υλοποιηθεί

4.2.2.3 Smart Contract

1. Διαχείριση Θησαυροφυλακίου
   Αποθηκεύει τις δωρεές και υπολογίζει το balance του DAO

2. Παρουσίαση προτάσεων
   Εμφάνιζει όλες τις υποψήφιες προτάσεις ώστε να μπορούν οι δωρητές να επιλεξουν εκείνη που προτιμούν

3. Υπολογισμός ύψους δωρεών
   Ανάλογα με το ποσό που υπάρχει στο treasury του DAO υπολογίζει το ποσό που μπορεί να δοθεί σαν δωρεά σε κάθε γύρο

4. Καταμέτρηση ψήφων
   Στο τέλος κάθε ψηφοφορίας ανακατατάσσει τις υποψήφιες προτάσεις ανάλογα με τις ψήφους προτίμησης που έχουν λάβει

5. Υπολογισμός αποτελεσμάτων
   Σύμφωνα με την κατάταξη της ψηφοφορίας και το ύψος των δωρεών που μπορούν να προσφερθούν, κρίνονται οι νικητές

6. Μεταβίβαση δωρεών
   Ανάλογα με την έκβαση του αποτελέσματος μεταβιβάζει στους δικαιούχους των νικηφόρων προτάσεων το αντίστοιχο ποσό

4.2.3 Περιοδικότητα

Όπως αναφέρθηκε και προηγουμένως, η λειτουργία του DAO πραγματοποιείται σε γύρους.

Η πρώτη φάση κάθε γύρου περιλαμβάνει την περίοδο κατά την οποία οι δωρητές μπορούν να πραγματοποιήσουν τις δωρεές τους και να μεταβιβάσουν τα δικαιώματα ψήφου τους, ενώ οι επωφελούμενοι μπορούν να καταθέσουν τις προτάσεις τους ζητώντας την απαραίτητη χορηγία.

Η δεύτερη φάση είναι η περίοδος της ψηφοφορίας όπου όλοι οι δωρητές με δικαιώματα ψήφου μπορούν να επιλέξουν την πρόταση που θεωρούν ότι αξίζει περισσότερο.

Μετά την ολοκλήρωση της ψηφοφορίας παρουσιάζονται τα αποτελέσματα του γύρου και είναι δυνατή η εκκίνηση ενός νέου γύρου υπό τις ίδιες συνθήκες.

Σε ένα ρεαλιστικό σενάριο κάθε γύρος θα μπορούσε να πραγματοποιείται σε μηνιαία βάση, με ένα περιθώριο ίσως τριών εβδομάδων για την πρώτη περίοδο και μιας εβδομάδας για την ψηφοφορία.

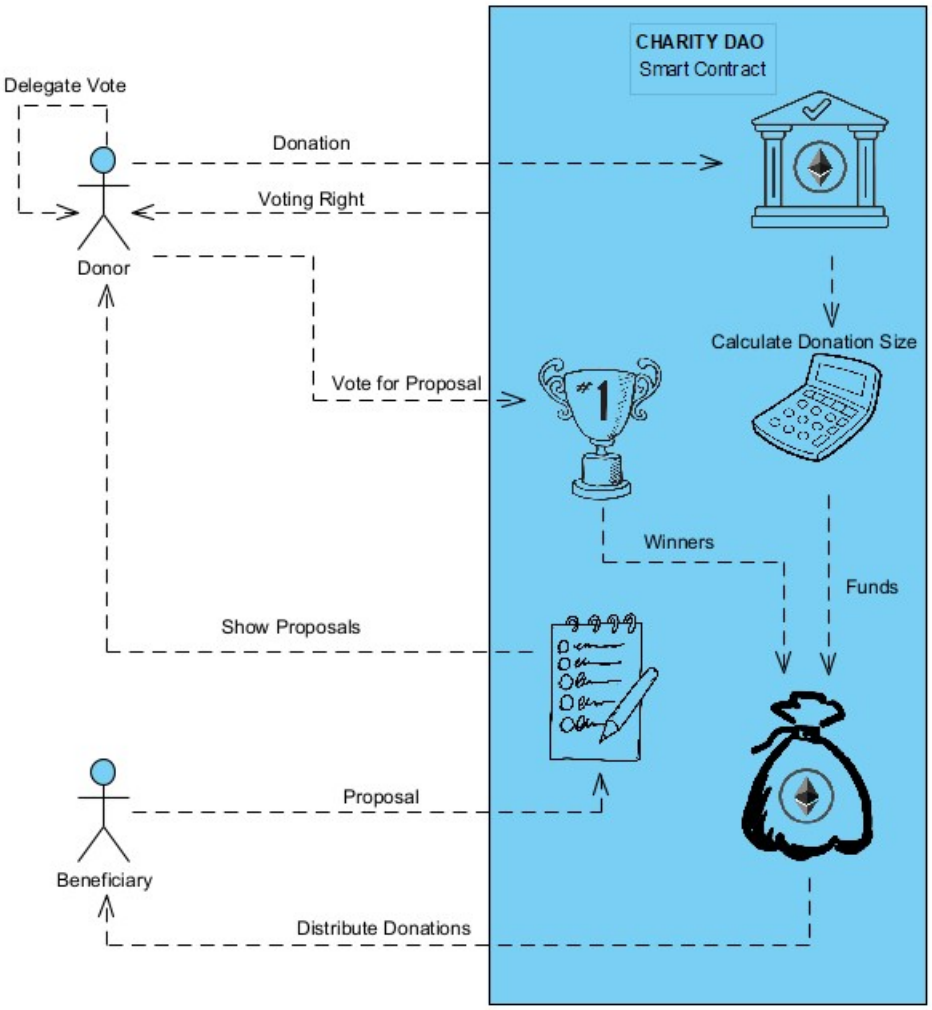
Στα πλαίσια της διπλωματικής, για να μπορεί να γίνει φανερή η λειτουργικότητα της εργασίας έχει δοθεί ένα περιθώριο μερικών λεπτών για την ολοκλήρωση κάθε φάσης.

4.3 Περιγραφή αρχιτεκτονικής

Στην ενότητα αυτή παρουσιάζονται τα απαραίτητα διαγράμματα για να γίνει κατανοητός ο τρόπος λειτουργίας του Charity DAO.

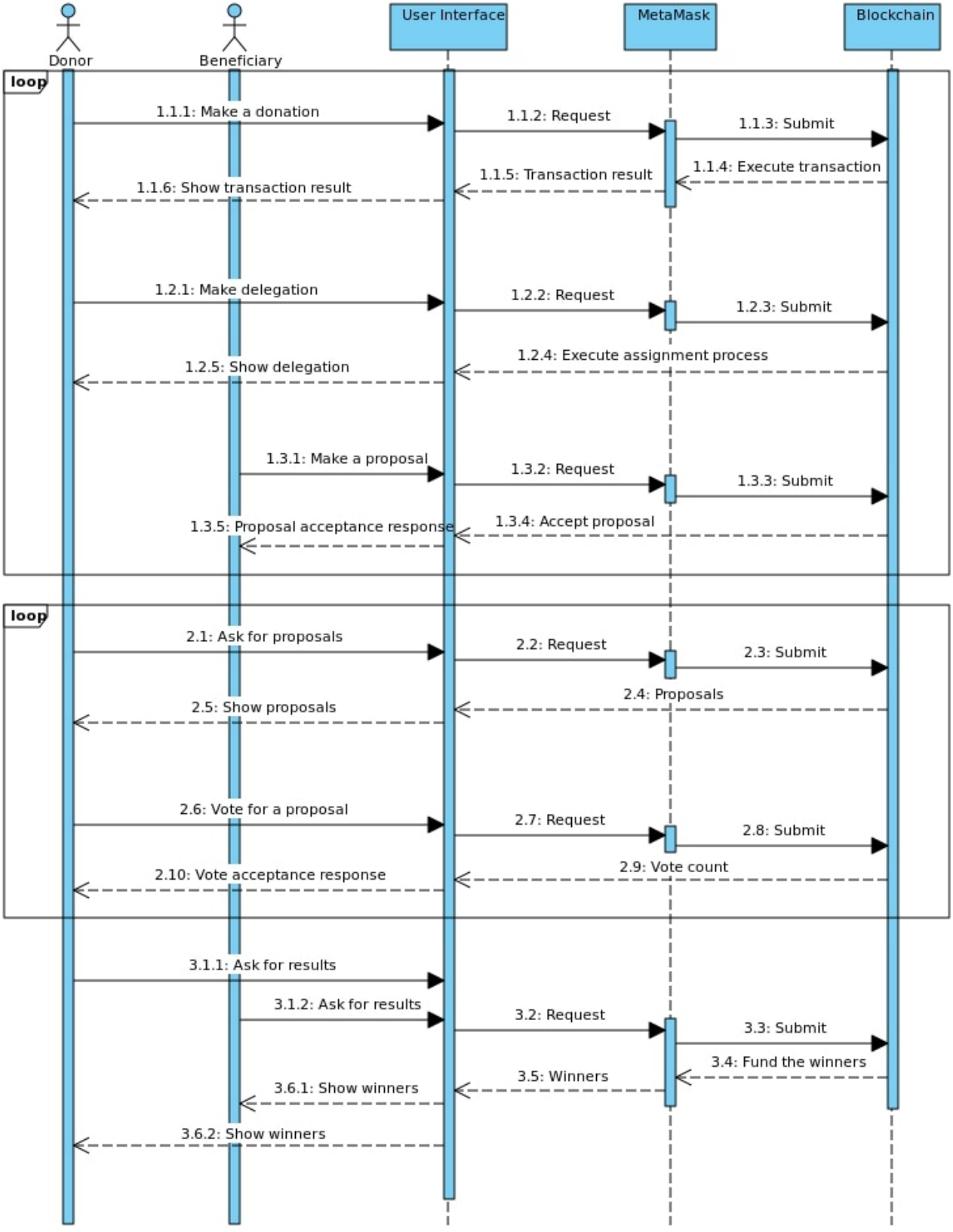
4.3.1 Use Case Diagram

Στο ακόλουθο διάγραμμα παρουσιάζεται η αλληλεπίδραση των οντοτήτων του Charity DAO με το smart contract του οργανισμού. Γίνονται φανερές όλες οι λειτουργικότητες που επεξηγήθηκαν στην προηγούμενη ενότητα και η μεταξύ τους αλληλεπίδραση.



Σχήμα 4.1: *Use Case Diagram*

4.3.2 Sequence Diagram



Σχήμα 4.2: *Sequence Diagram*

Στο διάγραμμα που φαίνεται πιο πάνω γίνεται ξεκάθαρη η λειτουργία ενός γύρου του Charity DAO.

Παρουσιάζεται το πώς οι χρήστες αλληλεπιδρούν με το User Interface του οργανισμού και μέσω του πορτοφολιού τους επικοινωνούν με το blockchain ενεργοποιώντας την κατάλληλη λειτουργία του smart contract.

Πιο κάτω αναλύεται, σύμφωνα με το διάγραμμα, ο τρόπος που έχει υλοποιηθεί το DAO, ώστε να γίνει απόλυτα κατανοητός.

Κάθε χρήστης μπορεί να αλληλεπιδράσει με το User Interface και να εκτελέσει την επιθυμητή ενέργεια. Μέσω του UI ενεργοποιείται ένα αίτημα στο πορτοφόλι του χρήστη και εφόσον γίνει έγκριση από τον χρήστη το αίτημα μεταβιβάζεται στο smart contract που είναι καταχωρημένο στο blockchain. Το smart contract εκτελεί όποια ενέργεια του ζητήθηκε και το αποτέλεσμα γίνεται αντιληπτό στον χρήστη μέσω του UI.

Συγκεκριμένα, στο πρώτο loop του διαγράμματος φαίνεται η πρώτη φάση ενός γύρου.

Οι δωρητές μπορούν να κάνουν ένα donation στο treasury του DAO. Στη συγκεκριμένη περίπτωση εφόσον από το smart contract εκτελείται κάποια συναλλαγή, παρατηρείται αμφίδρομη αλληλεπίδραση του πορτοφολιού του χρήστη με το blockchain, καθώς με την εκτέλεση της λειτουργίας από το smart contract αφαιρείται το ποσό της δωρεάς από το πορτοφόλι του χρήστη και μεταβιβάζεται στο treasury. Οι δωρητές μπορούν επίσης να μεταβιβάσουν τα δικαιώματα ψήφου τους εάν το επιθυμούν.

Οι επωφελούμενοι μέσω του UI καταθέτουν τις προτάσεις τους, και αφού εγκρίνουν την συναλλαγή μέσω του πορτοφολιού τους, οι προτάσεις καταγράφονται στο blockchain.

Στο δεύτερο loop του διαγράμματος επεικονίζεται η δεύτερη φάση του κύκλου. Πρόκειται για την περίοδο της ψηφοφορίας.

Οι δωτηρές μέσω του UI μπορούν να δουν όλες τις υποψήφιες προτάσεις και να καταχωρήσουν στο ίδιο σημείο την πρόταση που οι ίδιοι υποστηρίζουν. Οι ψήφοι καταχωρούνται στο blockchain και είναι αμετάβλητες.

Στο τελευταίο κομμάτι του διαγράμματος, μετά την ολοκλήρωση της περιόδου ψηφοφορίας, παρατηρείται και για τους δύο τύπους χρήστη η δυνατότητα να αιτηθούν τα αποτελέσματα του τρέχοντος γύρου. Μετά την εκτέλεση των απαραίτητων συναρτήσεων του smart contract, το ποσό των δωρεών μεταβιβάζεται στα πορτοφόλια των δικαιούχων και οι νικητήριες προτάσεις παρουσιάζονται στο UI.

Κεφάλαιο 5

Υλοποίηση

Στο κεφάλαιο αυτό παρατίθενται όλα τα εργαλεία που χρησιμοποιήθηκαν για την ανάπτυξη της εφαρμογής και επεξηγείται η χρήση τους. Επιπλέον γίνεται η ανάλυση της επιχειρηματικής λογικής του DAO μέσω του έξυπνου συμβολαίου, δηλαδή του βασικού πυρήνα, με την επεξήγηση των κύριων συναρτήσεών του. Γίνεται επίσης αναφορά στη δημιουργία του τοπικού δικτύου Ethereum.

5.1 Εργαλεία

Στην ενότητα αυτή παρουσιάζονται όλα τα εργαλεία τα οποία χρησιμοποιήθηκαν για την υλοποίηση του Charity DAO.

5.1.1 Remix IDE

Το Remix IDE [26] είναι ένα ανοικτού κώδικα περιβάλλον ανάπτυξης, το οποίο χρησιμοποιείται για την ανάπτυξη έξυπνων συμβολαίων smart contracts στο Ethereum Blockchain. Χρησιμοποιεί τη γλώσσα προγραμματισμού Solidity για την ανάπτυξη των smart contracts, ενώ υποστηρίζει επισης τη μεταγλώττιση και δοκιμή τους. Στο πλαίσιο της διπλωματικής εργασίας χρησιμοποιήθηκε για την ανάπτυξη του smart contract CharityDAO.sol. Το συμβόλαιο είναι αυτό που κάνει εφικτή την επικοινωνία του συστήματος με το Blockchain.

5.1.2 Truffle

Το Truffle [27] είναι ένα πλαίσιο λογισμικού (framework) για την ανάπτυξη εφαρμογών στο Ethereum χρησιμοποιώντας το EVM. Περιλαμβάνει χρήσιμες εντολές για τη δημιουργία ενός αρχικού περιγράμματος (template) με τους βασικούς φακέλους που χρειάζεται ο προγραμματιστής, εντολές για τη μεταγλώττιση των smart contracts, για την παράταξη (deployment) της εφαρμογής αλλά και για την εκτέλεση δοκιμών (testing). Στο πλαίσιο της διπλωματικής εργασίας χρησιμοποιήθηκε για την ανάπτυξη του Blockchain backend το ο-

ποίο περιέχεται στο φάκελο ςοντραςτς. Μεταξύ άλλων εκεί περιλαμβάνεται το συμβόλαιο CharityDAO.sol και η μεταγλώττισή του.

5.1.3 Ganache

Το Ganache [28] είναι ένα εργαλείο για την δημιουργία τοπικών Ethereum Blockchain δικτύων ώστε να δοκιμαστεί μία εφαρμογή πριν δημοσιευτεί στο δημόσιο δίκτυο του Ethereum. Προσφέρει τη δυνατότητα δημιουργίας εικονικών λογαριασμών Ethereum με τις δικές τους διευθύνσεις και υπόλοιπα λογαριασμών. Παράλληλα υποστηρίζει την παράταξη smart contracts σε κάποια διεύθυνση και οπτικοποιεί τα δεδομένα που περιέχουν. Στο πλαίσιο της διπλωματικής εργασίας χρησιμοποιήθηκε για τη δημιουργία ενός τοπικού Ethereum Blockchain για λόγους δοκιμών αλλά και επίδειξης.

5.1.4 Metamask

Το Metamask [29] είναι λογισμικό ηλεκτρονικού πορτοφολιού κρυπτονομισμάτων. Χρησιμοποιείται σε μορφή επέκτασης (extension) για προγράμματα περιήγησης (browsers) ή σε μορφή εφαρμογής. Προσφέρει στους χρήστες την ευκαιρία να αλληλεπιδράσουν με Web3 εφαρμογές χρησιμοποιώντας το Ethereum πορτοφόλι τους, στο οποίο φαίνονται διάφορα στοιχεία για τον κάθε λογαριασμό, όπως η διεύθυνση και το υπόλοιπό του. Στο πλαίσιο της διπλωματικής εργασίας χρησιμοποιήθηκε μέσω του frontend για να συνδέσει τους εικονικούς λογαριασμούς που δημιουργεί το Ganache local network με το Blockchain ώστε να εκτελούν οι χρήστες τις διάφορες συναλλαγές.

5.1.5 React.js

Η React.js [30] είναι μια frontend βιβλιοθήκη ανοικτού κώδικα (open-source library) για τη γλώσσα προγραμματισμού JavaScript. Χρησιμοποιείται για την ανάπτυξη περιβάλλοντος διεπαφής χρήστη (User Interfaces – UI). Στο πλαίσιο της διπλωματικής εργασίας χρησιμοποιήθηκε εντός ενός Next.js project για τη δημιουργία του frontend του Charity DAO, δηλαδή την ιστοσελίδα που χρησιμοποιεί ο χρήστης για να αλληλεπιδράσει με το σύστημα.

5.1.6 Next.js

Η Next.js [31] είναι ένα React.js πλαίσιο λογισμικού ανοικτού κώδικα (open-source framework) για την ανάπτυξη εφαρμογών. Είναι κατασκευασμένο επί της React.js επιτρέποντας έτσι τη συγγραφή κώδικα, που ακολουθεί την κανονική δομή της React.js, αλλά προσφέρει και κάποιες επιπλέον διευκολύνσεις στον προγραμματιστή. Στο πλαίσιο της διπλωματικής εργασίας χρησιμοποιήθηκε για την ανάπτυξη του frontend του Charity DAO. Ο σχετικός κώδικας βρίσκεται στο φάκελο client. Εκτός από το περιβάλλον διεπαφής (δλδ την

ιστοσελίδα) που χρησιμοποιεί ο χρήστης, χρησιμοποιήθηκε και για τη σύνδεση της εφαρμογής με το Smart Contract,δλδ για την αλληλεπίδραση με το Βλοσκσηαιν καθώς και με το πορτοφόλι του χρήστη μέσω του Metamask.

5.1.7 Visual Paradigm

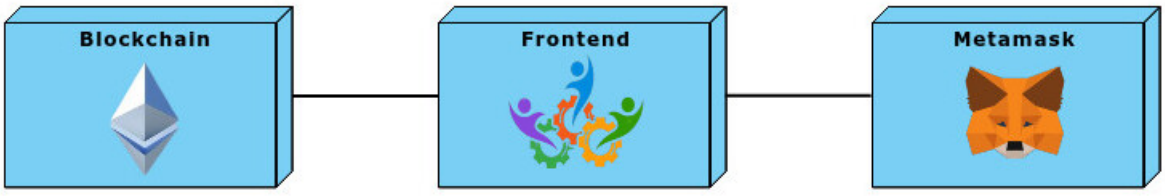
Το Visual Paradigm [32]είναι ένα εργαλείο για τη δημιουργία διαγραμμάτων διαφόρων τύπων. Στο πλαίσιο της διπλωματικής εργασίας χρησιμοποιήθηκε για τη δημιουργία των διαγραμμάτων που περιλαμβάνονται στο παρόν έγγραφο.

5.1.8 GitHub

Το GitHub [33] είναι ένα λογισμικό ανοικτού κώδικα (open-source software) για την αποθήκευση και το διαμοιρασμό λογισμικού. Υποστηρίζει τη διαχείριση αποθετηρίων git (git repositories) τα οποία είναι ένα σύστημα ελέγχου εκδόσεων (version control) λογισμικού. Στο πλαίσιο της διπλωματικής εργασίας χρησιμοποιήθηκε για την αποθήκευση της ίδιας της εργασίας σε διαδοχικές εκδόσεις. Ο τελικός κώδικας μαζί με όλα τα σχετικά έγγραφα και εγχειρίδια βρίσκονται αποθηκευμένα εκεί ώστε να υπάρχει δημόσια πρόσβαση σε αυτά.

5.2 Δομή Υλοποίησης

Το σύστημα του Charity DAO είναι δομημένο όπως φαίνεται στο ακόλουθο διάγραμμα. Την ραχοκοκαλιά του συστήματος αποτελεί το blockchain backend το οποίο συνδέεται με το πορτοφόλι του Metamask, δηλαδή τους χρήστες, μέσω του frontend.



Σχήμα 5.1: *Δομή υλοποίησης του συστήματος*

5.3 Το Smart Contract

Σε αυτή την ενότητα αναλύονται διεξοδικά οι κύριες συναρτήσεις και μεταβλητές που απαρτίζουν το έξυπνο συμβόλαιο του συστήματος. Εκτός από τις ακόλουθες, υπάρχουν διάφορες βοηθητικές συναρτήσεις και μεταβλητές οι οποίες όμως δεν αναλύονται, καθώς δεν είναι απαραίτητες για την κατανόηση της λειτουργίας του συστήματος.

5.3.1 Βασικές Δομές/Μεταβλητές

1. ***struct Donor{uint weight; uint256 totalDonation; bool votingRight; address delegate; uint proposalVoted;}***

   mapping(address => Donor) public donors;

   Τα δεδομένα των δωρητών καταχωρούνται στο mapping *donors* το οποίο έχει ως key μια διεύθυνση *address* και ως value μια δομή δεδομένων *Donor*.
   Η εν λόγω δομή δεδομένων περιλαμβάνει τις μεταβλητές που φαίνονται πιο πάνω και αναλύονται ακολούθως:

   - *totalDonation* - το συνολικό μέγεθος των δωρεών που έχει προσφέρει ο δωρητής στο treasury του DAO
   - *voting Right* - παίρνει την τιμή true/false ανάλογα με το αν ο δωρητής μπορεί να ψηφίσει ή οχι
   - *weight* - το πλήθος των δικαιωμάτων ψήφου, η τιμή του αναλογεί στο μέγεθος των συνολικών δωρεών του χρήστη και κυμαίνεται από 1 (για δωρεές άνω του ενός (1) Ether) μέχρι 5 (για δωρεές άνω των σαράντα (40) Ethers)
   - *delegate* - η διεύθυνση του εκπροσώπου του δωρητή, σε περίπτωση που επιλέξει κάποιον
   - *proposalVoted* - η πρόταση για την οποία ο δωρητής έχει ψηφίσει υπέρ (σε κάθε γύρο)

2. ***struct Proposal{uint proposalID; address proposer; address recipient; string title; string details; uint cost; uint votesFor;}***

   Proposal[] public proposal;

   Τα δεδομένα των προτάσεων καταχωρούνται στον πίνακα *proposal* με δομή δεδομένων *Proposal* η οποία αναλύεται ως εξής:

   - *proposalID* - το μοναδικό αναγνωριστικό μιας πρότασης (σε κάθε γύρο)
   - *proposer* - η διεύθυνση του beneficiary που έχει υποβάλει την συγκεκριμένη πρόταση
   - *recipient* - η διεύθυνση στην οποία θα καταχωρηθεί το ποσό σε περίπτωση που η πρόταση ψηφισθεί (συνήθως είναι ίδια με την διεύθυνση του proposer)
   - *title* - ο τίτλος της πρότασης
   - *details* - χρήσιμες πληροφορίες, επεξήγηση της πρότασης
   - *cost* - το κόστος για την υλοποίηση της πρότασης
   - *votesFor* - το πλήθος των ψήφων υπέρ της πρότασης

3. ***mapping(address => uint) public beneficiaries;***

   Οι διευθύνσεις *address* των beneficiaries αποτελούν το key σε ένα mapping με value το ID της πρότασης που έχει προτείνει ο αντίστοιχος δικαιούχος.

4. ***mapping(uint => Proposal[]) public history;*** Για την αποθήκευση του ιστορικού του συτήματος έχει δημιουργηθεί ένα mapping με key τον αριθμό κάθε γύρου και value τη δομή *Proposal* (η οποία έχει αναλυθεί προηγουμένως) για την αποθήκευση των νικηφόρων προτάσεων κάθε γύρου.

5.3.2 Βασικές Συναρτήσεις

1. ***function initializeRound() public {...}***

   Καλείται από οποιονδήποτε χρήστη του οργανισμού για την αρχικοποίηση ενός νέου γύρου. Προϋπόθεση για την εκτέλεση της συνάρτησης *initializeRound()* είναι να έχει ολοκληρωθεί ο προηγούμενος γύρος.

2. ***function calculateDonationSize() public view returns (uint256 amount) {...}***

   Το treasury του DAO περιέχει μόνο τα ethers που δίνονται ως δωρεές από τους δωρητές του οργανισμού και σε κάθε γύρο από αυτο μεταβιβάζεται το απαραίτητο ποσό στους δικαιούχους των νικηφόρων προτάσεων. Για να μπορεί ο οργανισμός να είναι λειτουργικός και κατά περιόδους όπου οι εισφορές δεν είναι ικανοποιητικές, σε κάθε γυρο είναι διαθέσιμο για να χορηγηθεί το 30% του συνόλου του θησαυροφυλακίου. Η συνάρτηση *calculateDonationSize()* υπολογίζει πριν από την ψηφοφορία των χρηστών το συνολικό ποσό, δηλαδή το 30% του balance του DAO, που μπορεί να αξιοποιηθεί σε κάθε γύρο.

3. ***function donate() external payable {...}***

   Για την εκτέλεση της συνάρτησης *donate()* δίνεται από τον χρήστη το ποσό (σε Ethers ή κάποια υποδιαίρεση) που επιθυμεί να δωρίσει στο treasury του DAO. Κατά την εκτέλεση της συνάρτησης μεταβιβάζεται το αντίστοιχο ποσό από την διεύθυνση του δωρητή στη διεύθυνση του DAO, ενώ παράλληλα υπολογίζεται το συνολικό ύψος των δωρεών του χρήστη σε περίπτωση που έχει πραγματοποιήσει κι άλλες εισφορές και το πλήθος των ψήφων που δικαιούται ο χρήστης ανάλογα με τις δωρεές του.

4. ***function delegation(address to) public {...}***

   Κύρια προϋπόθεση για την εκτέλεση αυτής της συνάρτησης είναι να καλεστεί σε περίοδο που είναι επιτρεπτές οι μεταβιβάσεις δικαιωμάτων (δηλαδή πριν από την περίοδο ψηφοφορίας). Σκοπός της συνάρτησης *delegation()* είναι να μεταβιβάσει τα δικαιώματα ψήφου του δωρητή που την καλεί στον δωρητή με τη διεύθυνση *to* η οποία δίνεται σαν όρισμα. Επιπλέον προϋποθέσεις για την εκτέλεση της συνάρτησης είναι ο δωρητής που την καλεί να έχει δικαιώματα ψήφου (δηλαδή να έχει δωρήσει πάνω από ένα (1) Ether στο DAO), να μην έχει ήδη μεταβιβάσει τα δικαιώματα ψήφου του σε άλλον δωρητή, και ο δωρητής στον οποίο θέλει να κάνει τη μεταβίβαση να έχει ήδη δικαιώματα ψήφου.

5. ***function revokeDelegation() public {...}***

   Προϋπόθεση για την εκτέλεση αυτής της συνάρτησης είναι να καλεστεί σε περίοδο που είναι επιτρεπτές οι μεταβιβάσεις δικαιωμάτων (δηλαδή πριν από την περίοδο ψηφοφορίας) καθώς επίσης και ο χρήστης να είναι δωρητής και να έχει μεταβιβάσει τα δικαιώματα ψήφου του σε κάποιον άλλο δωρητή. Σκοπός της συνάρτησης *revokeDelegation()* είναι να μεταβιβάσει εκ νέου τα δικαιώματα ψήφου στον προκάτοχό τους και να μειώσει το πλήθος των ψήφων του delegate στον αριθμό που αντιστοιχεί στις δικές του δωρεές.

6. ***function giveRightToVote(address donor, uint voteWeight) private {...}***

   Η συνάρτηση *giveRightToVote()* καλείται από την συνάρτηση *donate()* με παραμέτρους τη διεύθυνση του δωρητή *donor* και το πλήθος των δικαιωμάτων ψήφου *voteWeight* που του αναλογούν. Παραχωρεί τα δικαιώματα ψήφου στον ίδιο τον δωρητή ή τον επιλεγμένο από αυτόν εκπρόσωπο delegate που πιθανόν να έχει.

7. ***function propose(string memory title, string memory details, uint cost, address to) public {...}***

   Η συγκεκριμένη συνάρτηση καλείται από τους χρήστες του οργανισμού που θέλουν να συμμετέχουν σαν δικαιούχοι, κάνονας κάποια πρόταση η οποία θα μπορεί στη συνέχεια να ψηφιστεί και να λάβει το απαραίτητο χρηματικό ποσό για την υλοποίησή της. Η εκτέλεση της συνάρτησης *propose()* απαιτείται πριν από την περίοδο της ψηφοφορίας. Δέχεται σαν ορίσματα όλες τις απαραίτητες πλήροφορίες για να γίνει κατανοητός ο σκοπός για τον οποίο ζητούν τη στήριξη του οργανισμού. Ο χρήστης που επιθυμεί να πραγματοποιήσει μια πρόταση δίνει γιάυτήν έναν τίτλο *title*, κάποιες παραπάνω πληροφορίες για την καλύτερη κατανόηση της κατάστασης *details*, το εκτιμώμενο κόστος *cost* για την υλοποίηση του στόχου καθώς και την διεύθυνση *to* του δικαιούχου που θα λάβει την χρηματοδότηση σε περίπτωση που η πρόταση ψηφιστεί.

8. ***function vote(uint proposalID) public {...}***

   Η συνάρτηση *vote()* εκτελείται μόνο κατά την περίοδο της ψηφοφορίας κάθε γύρου και μόνον από τους δωρητές που κατέχουν δικαιώματα ψήφου. Δέχεται σαν παράμετρο έναν αριθμό *proposalID* ο οποίος εκφράζει την πρόταση του γύρου για την οποία ο χρήστης θέλει να ψηφίσει υπέρ. Για να γίνει αποδεκτό το αποτέλεσμα μιας ψηφοφορίας πρέπει τα δικαιώματα ψήφουν που έχουν ασκηθεί να ανέρχονται τουλάχιστον στο 50% του συνόλου.

9. ***function delegation(address to) public {...}***

   Κύρια προϋπόθεση για την εκτέλεση αυτής της συνάρτησης είναι να καλεστεί σε περίοδο που είναι επιτρεπτές οι μεταβιβάσεις δικαιωμάτων (δηλαδή πριν από την περίοδο ψηφοφορίας). Σκοπός της συνάρτησης *delegation()* είναι να μεταβιβάσει τα δικαιώματα ψήφου του δωρητή που την καλεί στον δωρητή με τη διεύθυνση *to* η οποία δίνεται σαν όρισμα. Επιπλέον προϋποθέσεις για την εκτέλεση της συνάρτησης είναι ο δωρητής που την καλεί να έχει δικαιώματα ψήφου (δηλαδή να έχει δωρήσει πάνω από ένα (1) Ether

στο DAO), να μην έχει ήδη μεταβιβάσει τα δικαιώματα ψήφου του σε άλλον δωρητή, και ο δωρητής στον οποίο θέλει να κάνει τη μεταβίβαση να έχει ήδη δικαιώματα ψήφου.

10. ***function revokeDelegation() public {...}***

    Προϋπόθεση για την εκτέλεση αυτής της συνάρτησης είναι να καλεστεί σε περίοδο που είναι επιτρεπτές οι μεταβιβάσεις δικαιωμάτων (δηλαδή πριν από την περίοδο ψηφοφορίας) καθώς επίσης και ο χρήστης να είναι δωρητής και να έχει μεταβιβάσει τα δικαιώματα ψήφου του σε κάποιον άλλο δωρητή. Σκοπός της συνάρτησης *revokeDelegation()* είναι να μεταβιβάσει εκ νέου τα δικαιώματα ψήφου στον προκάτοχό τους και να μειώσει το πλήθος των ψήφων του delegate στον αριθμό που αντιστοιχεί στις δικές του δωρεές.

11. ***function results() public payable {...}***

    Η συνάρτηση *results()* μπορεί να εκτελεστεί από οποιονδήποτε χρήστη του συστήματος αμέσως μετά τη λήξη της περιόδου ψηφοφορίας. Κατατάσσει τις προτάσεις σύμφωνα με τις ψήφους που έχουν λάβει και ανάλογα με το διαθέσιμο ποσό που μπορεί να δοθεί στον τρέχοντα γύρο υπολογίζει τις προτάσεις που θα λάβουν τη χορηγία που ζητούν. Παρουσιάζει τις νικηφόρες προτάσεις του γύρου και ενημερώνει το ιστορικό του συστήματος αναλόγως.

12. ***function fund(address payable toAddress, uint256 amountInWei) private {...}***

    Σαν πρώτη παράμετρος δίνεται η διεύθυνση *toAddress* ενός δικαιούχου και σαν δεύτερη παράμετρος ένα ποσό σε υποδιαίρεση WEI *amountInWei*. Η λειτουργία που πραγματοποιεί η συνάρτηση *fund()* είναι η μεταβίβαση του ποσού που δίνεται ως παράμετρος από το treasury του DAO στην αντίστοιχη διεύθυνση. Η συνάρτηση καλείται μέσω της συνάρτησης *results()* όσες φορές χρειαστεί σε κάθε γύρο, ανάλογα με τον αριθμό των προτάσεων που έχουν επιλεχθεί για να χορηγηθούν.

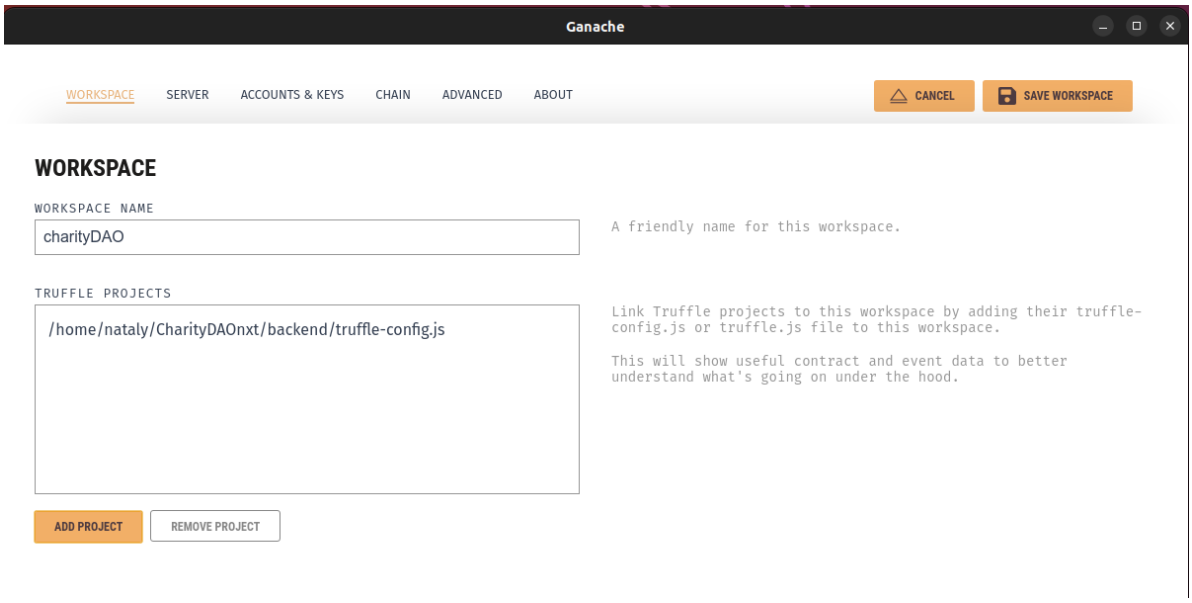
5.4 Τοπικό δίκτυο Blockchain

Το smart contract για να μπορεί να εκτελεστεί πρέπει να δημοσιευτεί σε ένα δίκτυο Blockchain ώστε να αποκτήσει μια διεύθυνση με την οποία μπορούν να αλληλεπιδρούν οι χρήστες. Στην περίπτωση του Charity DAO έχει δημιουργηθεί ένα τοπικό Ethereum Blockchain με τη βοήθεια του εργαλείου Ganache που περιγράφηκε προηγουμένως.

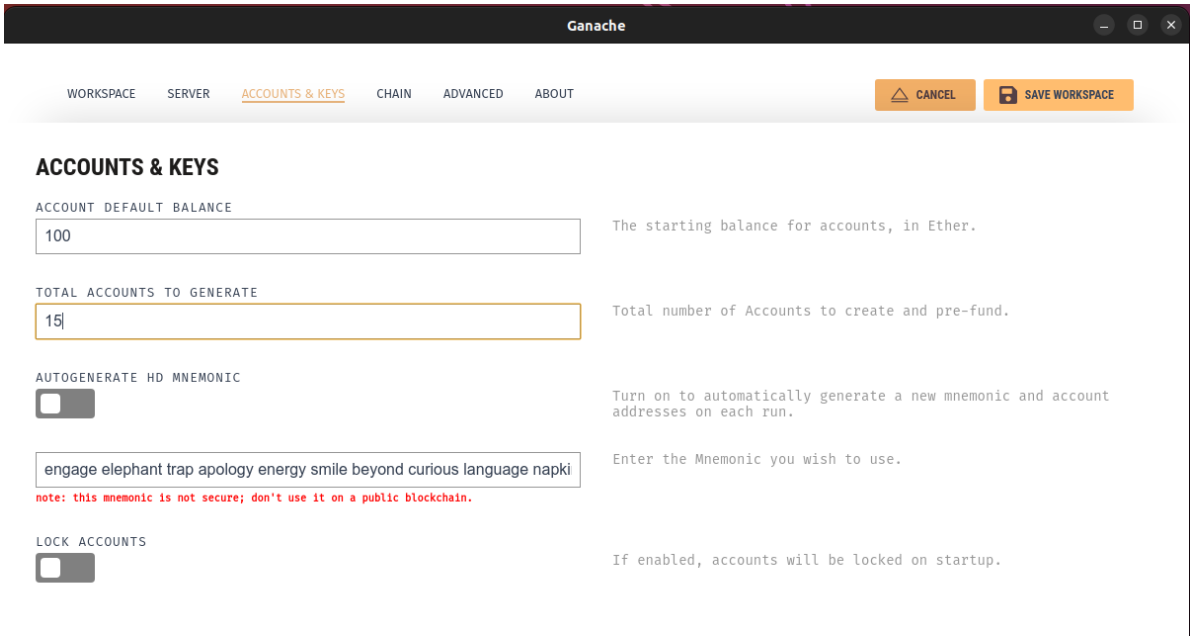
Το Ganache προσφέρει ευκολία στη δημιουργία ενός τοπικού Blockchain. Η αποθήκευση των δεδομένων σε blocks για τη δημιουργία του Blockchain γίνεται αυτόματα, χωρίς να χρειάζεται η δημιουργία της αλυσίδας των blocks από το μηδέν θέτοντας κόμβους-μεταλλωρύχους και δημιουργώντας το genesis block.

Επιπλέον, το Ganache παρουσιάζει σε γραφικό περιβάλλον απαραίτητες πληροφορίες για το blockchain αλλά και τα δεδομένα που είναι αποθηκευμένα σε αυτό.

Αρχικά το Ganache ρυθμίζεται χρησιμοποιώντας το αρχείο truffle-config.js και πραγματοποιώντας κάποιες ρυθμίσεις για το πλήθος των λογαριασμών και το αρχικό τους υπόλοιπο. Στην περίπτωση του Charity DAO δημιουργήθηκαν 15 λογαριασμοί με υπόλοιπο 100 ethers έκαστος.



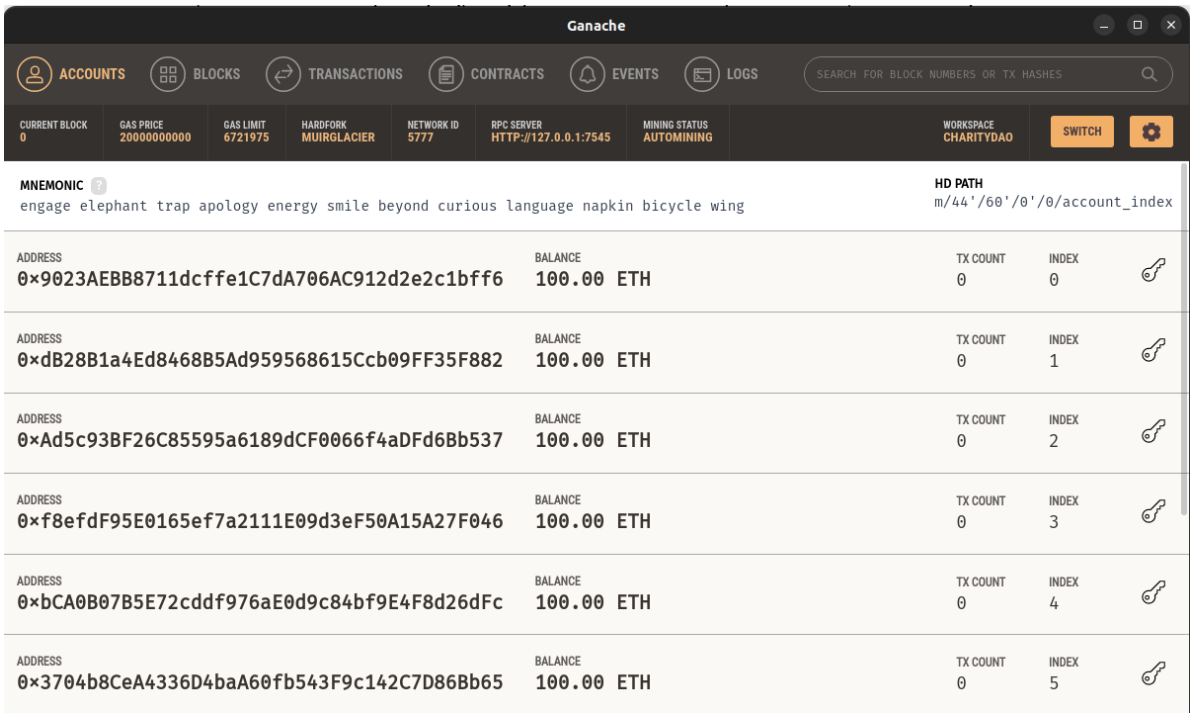
Σχήμα 5.2: *Δημιουργία του Local Ethereum Blockchain*



Σχήμα 5.3: *Δημιουργία των λογαριασμών*

Μετά τη δημιουργία του Blockchain παρουσιάζονται οι επιλογές του Ganache εκ των οποίων οι απαραίτητες συνοψίζονται ακολούθως:

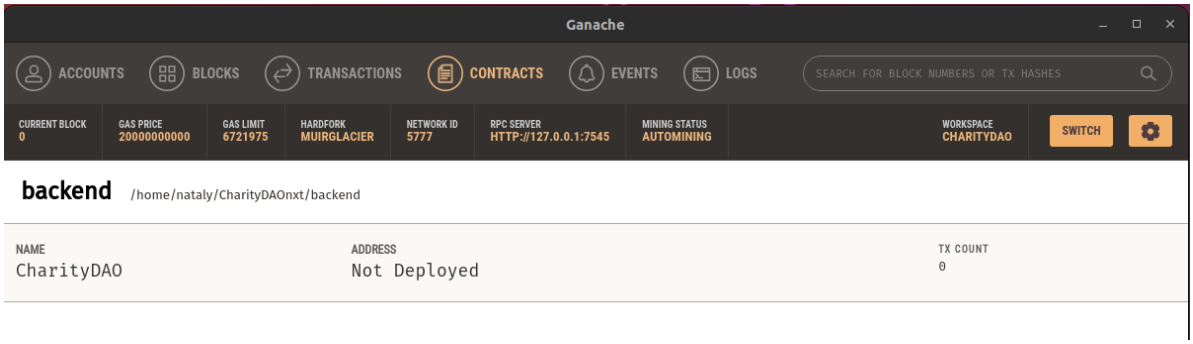
Στην καρτέλα ACCOUNTS υπάρχει μια σύνοψη για τους λογαριασμούς, τις διευθύνσεις τους, τα υπόλοιπά τους και διάφορες άλλες σχετικές πληροφορίες.



Σχήμα 5.4: *Καρτέλα Accounts*

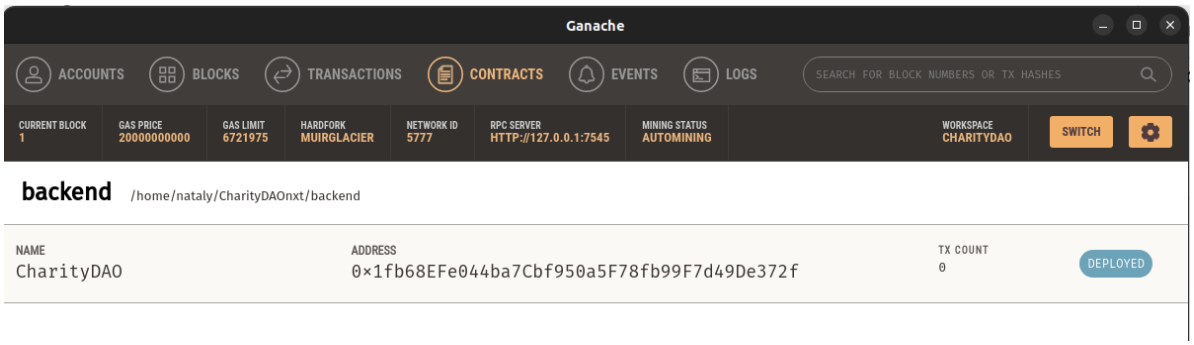
Κατά τη λειτουργία του DAO παρατηρείται αυτόματη μεταβολή στα υπόλοιπα των λογαριασμών, ανάλογα με τη δράση που εκτελείται.

Στην καρτέλα CONTRACTS παρατηρείται αρχικά η επιγραφή Not Deployed.



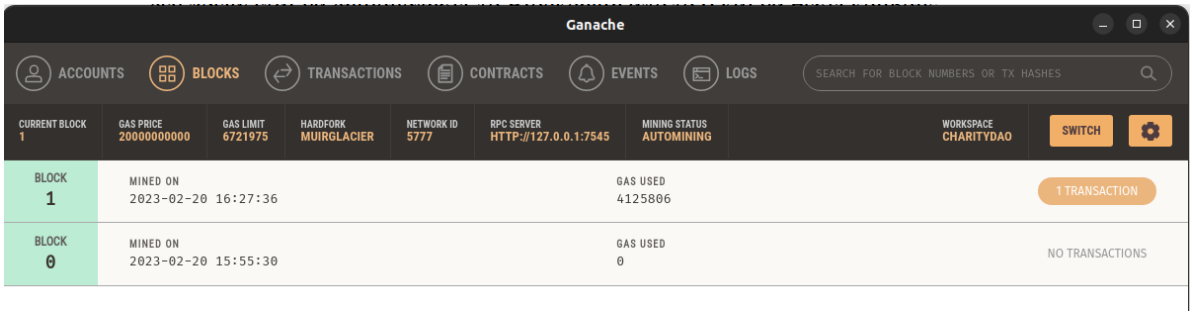
Σχήμα 5.5: *Καρτέλα Contracts*

Στη συνέχεια με χρήση της εντολής *truffle migrate* το smart contract δημοσιεύεται στο blockchain, αποκτά μια διεύθυνση και είναι πλέον λειτουργικό.



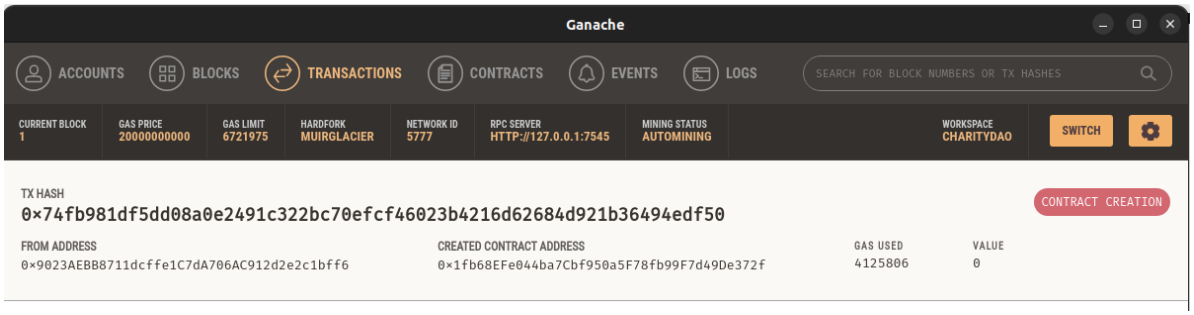
Σχήμα 5.6: *Καρτέλα Contracts*

Στην καρτέλα BLOCKS εμφανίζονται διαδοχικά τα blocks που έχουν δημιουργηθεί και αποτελούν το Blockchain. Επιλέγοντας κάποιο από τα blocks εμφανίζονται λεπτομέρειες σχετικά με τα δεδομένα του block και τις συναλλαγές που περιέχονται σε αυτό.



Σχήμα 5.7: *Καρτέλα Blocks*

Στην καρτέλα TRANSACTIONS φαίνονται όλες οι συναλλαγές που έχουν καταχωρηθεί. Επιλέγοντας κάποια από αυτές παρουσιάζονται λεπτομέρειες σχετικά με τα δεδομένα που περιέχει.

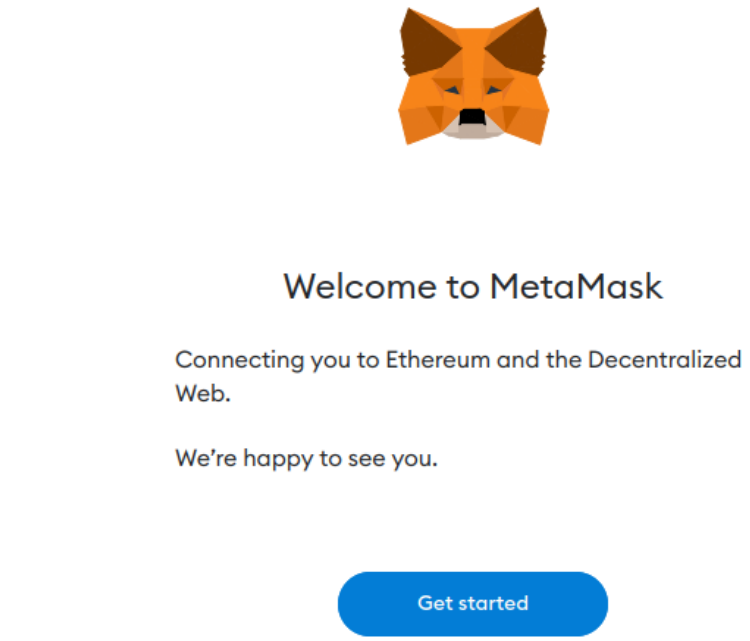


Σχήμα 5.8: *Καρτέλα Transactions*

Κατά τη λειτουργία του Charity DAO τα blocks και οι συναλλαγές αυξάνονται σύμφωνα με τα όσα εκτελούνται.

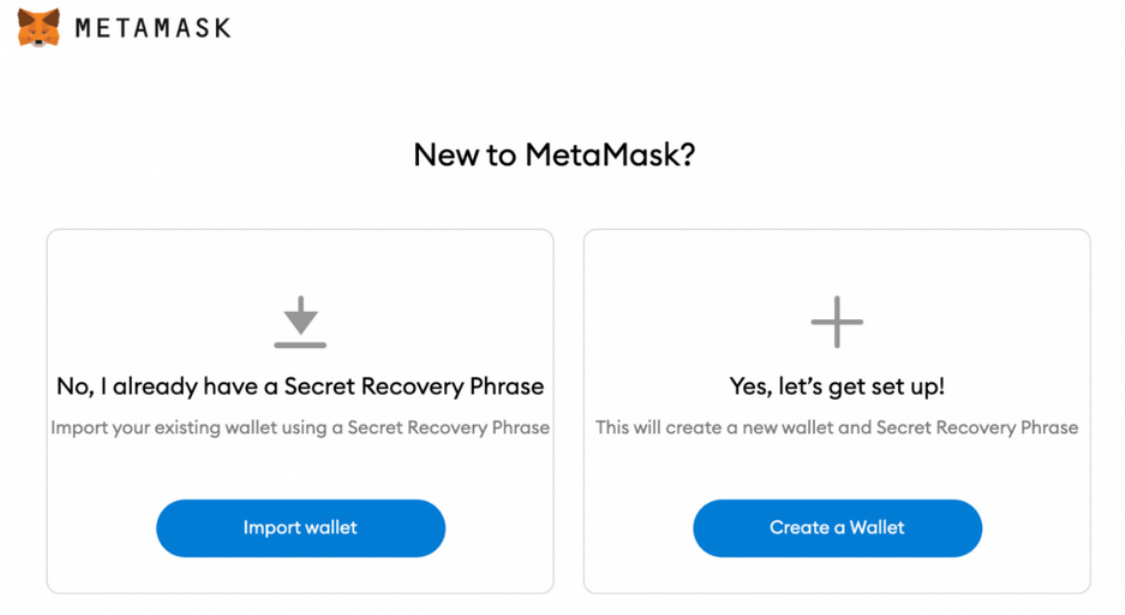
Για να είναι δυνατή η αλληλεπίδραση των χρηστών του Blockchain με το έξυπνο συμβόλαιο μέσω του front-end απαραίτητη προϋπόθεση είναι η εγκατάσταση του πορτοφολιού

Metamask και η σύνδεσή του με το τοπικό δίκτυο.

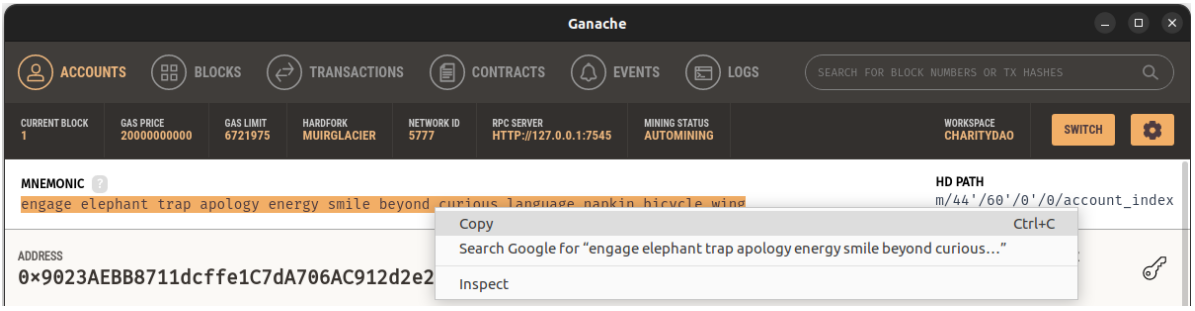


Σχήμα 5.9: *Εκκίνηση Metamask*

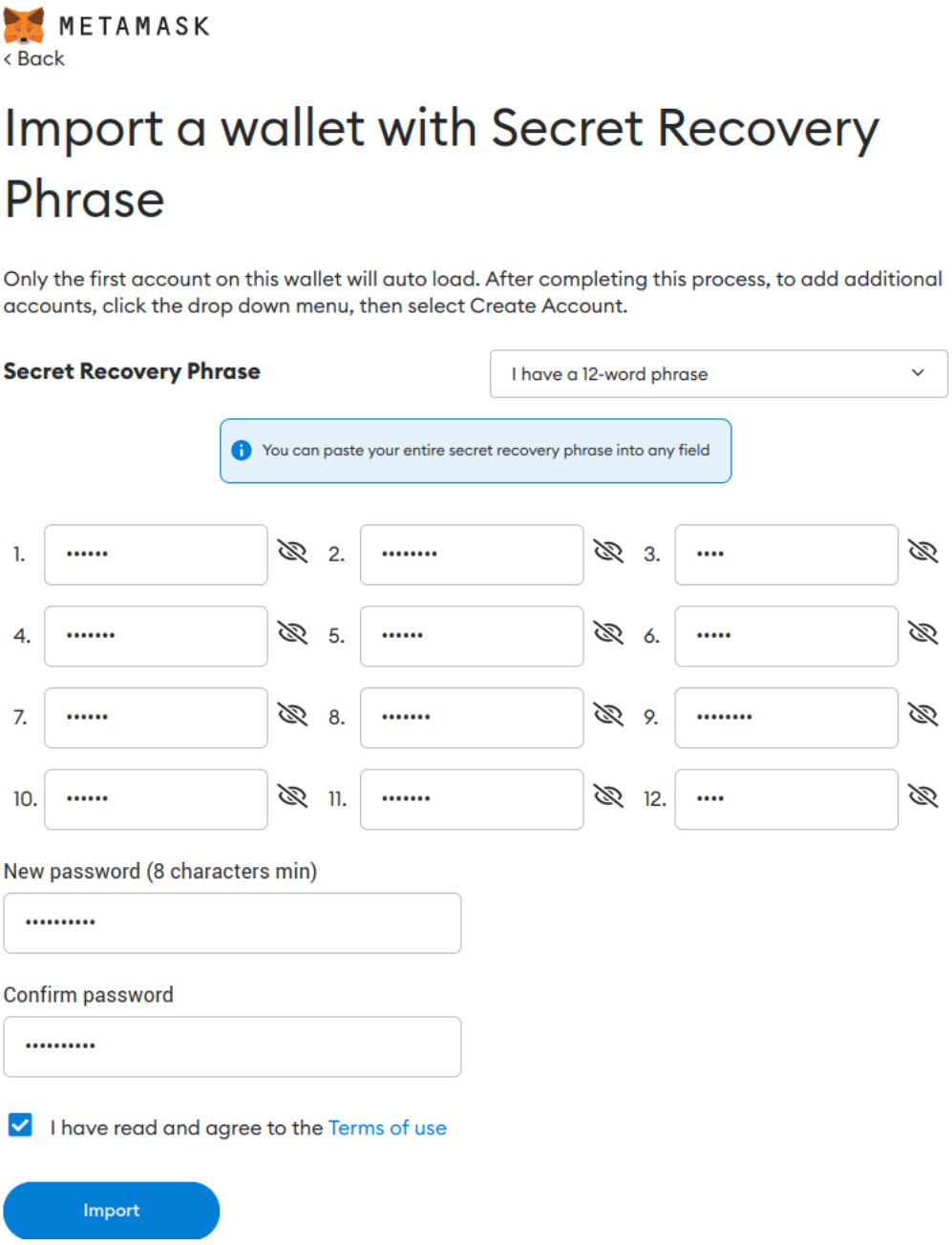
Στη συνέχεια μέσω της εντολής import wallet και με χρήση του mnemonic phrase από το ganache network και την προσθήκη ενός κωδικού καθίσταται δυνατή η χρήση του πορτοφολιού Metamask.



Σχήμα 5.10: *Import Wallet*

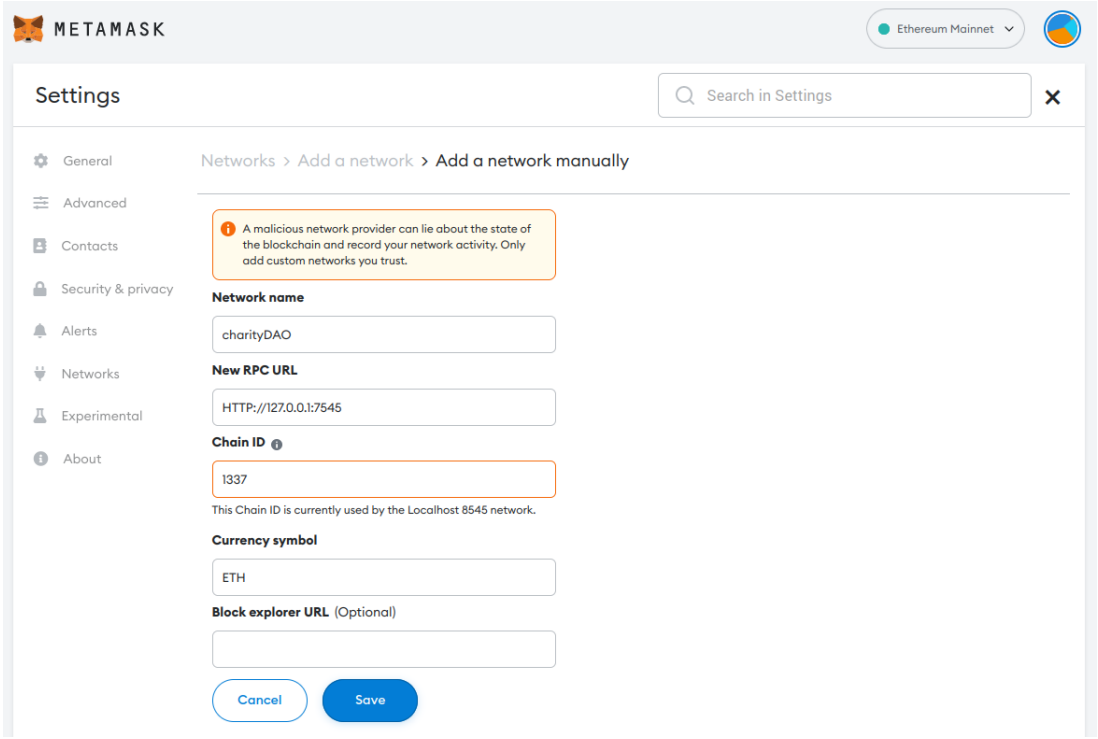


Σχήμα 5.11: *Αντιγραφή του mnemonic phrase*

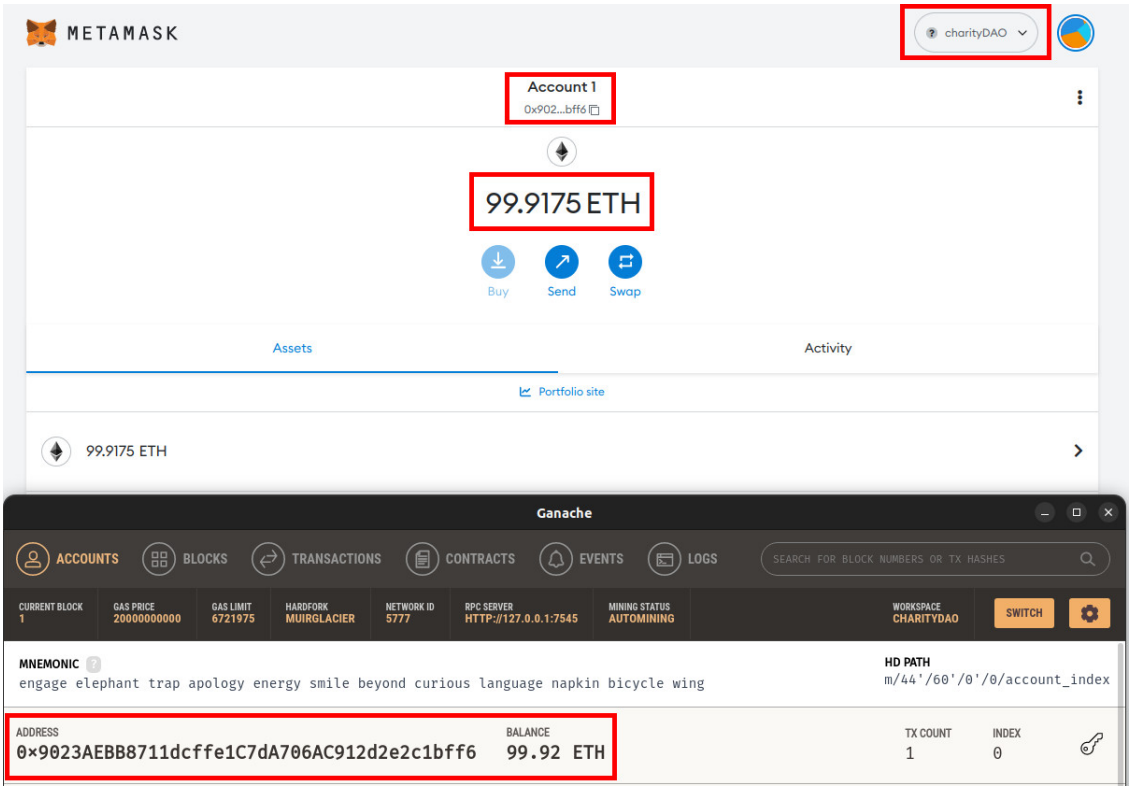


Σχήμα 5.12: *Ολοκλήρωση της προσθήκης πορτοφολιού*

Ακολούθως γίνεται η προσθήκη του τοπικού δικτύου στο Metamask.



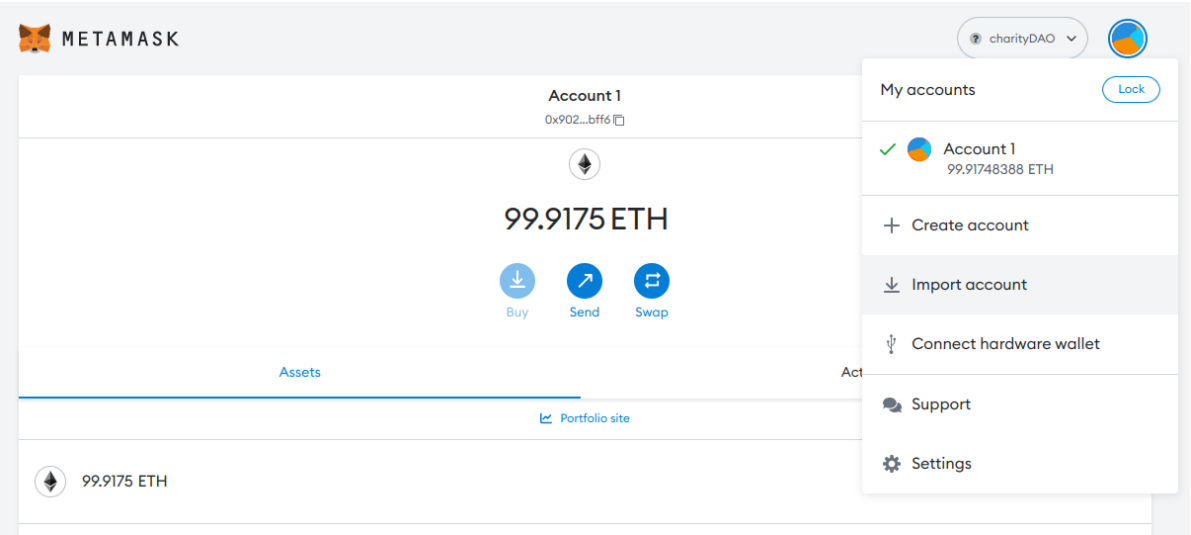
Σχήμα 5.13: *Δημιουργία τοπικού δικτύου*



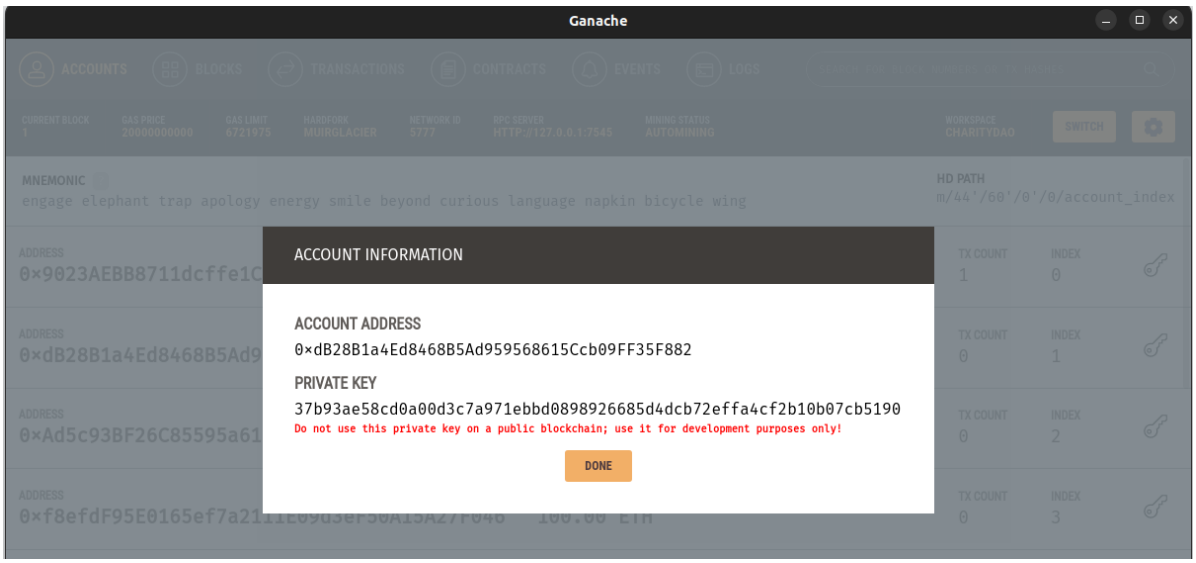
Σχήμα 5.14: *Χρήση του τοπικού δικτύου*

Το τοπικό δίκτυο έχει δημιουργηθεί στο Metamask και ο λογαριασμός ο οποίος έχει συνδεθεί σε αυτό είναι ο πρώτος λογαριασμός που υπάρχει στο Ganache.

Έπειτα είναι απαραίτητη η εισαγωγή στο Metamask και των υπόλοιπων λογαριασμών που έχουν δημιουργηθεί στο Ganache. Η διαδικασία που ακολουθείται είναι η εξής:

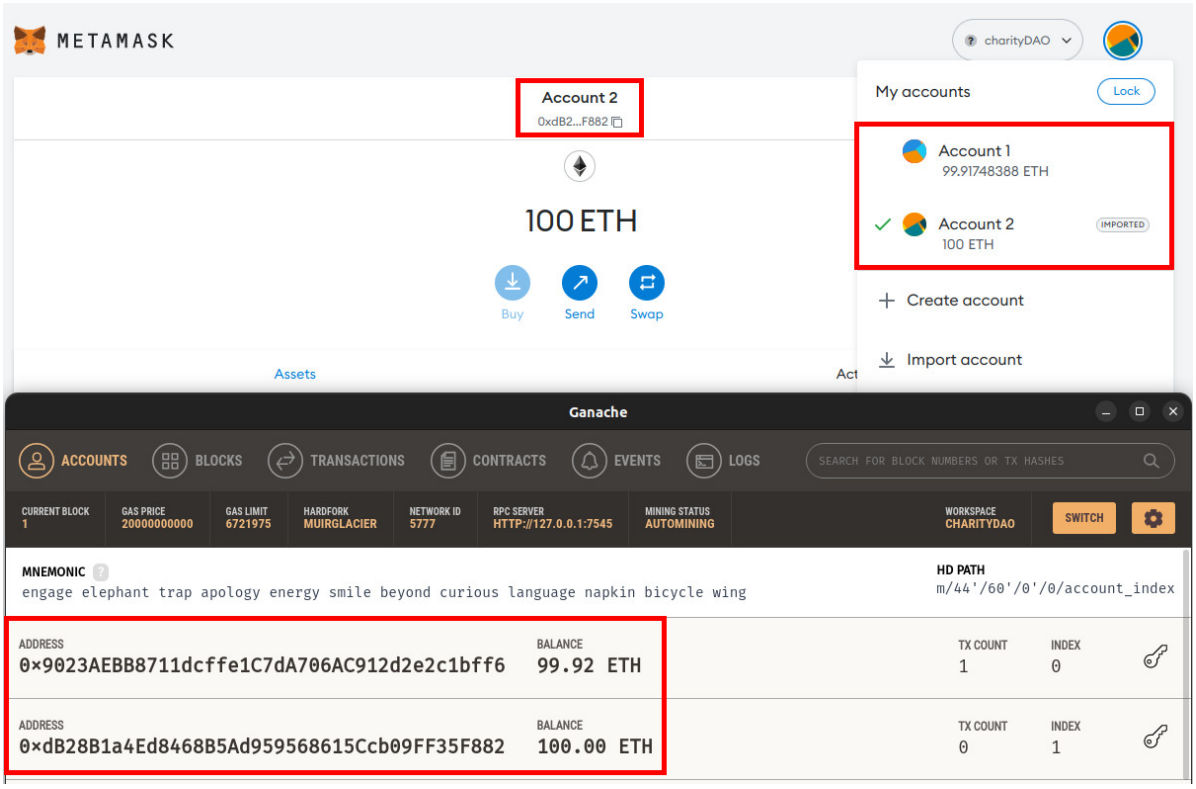


Σχήμα 5.15: *Εισαγωγή λογαριασμού στο Metamask*



Σχήμα 5.16: *Αντιγραφή του private key ενός λογαριασμού*

Ο δεύτερος λογαριασμός του Ganache έχει πλέον εισαχθεί στο Metamask.



Σχήμα 5.17: *Επίδειξη λογαριασμών Metamask*

Με την ίδια διαδικασία γίνεται η προσθήκη και των υπόλοιπων λογαριασμών.

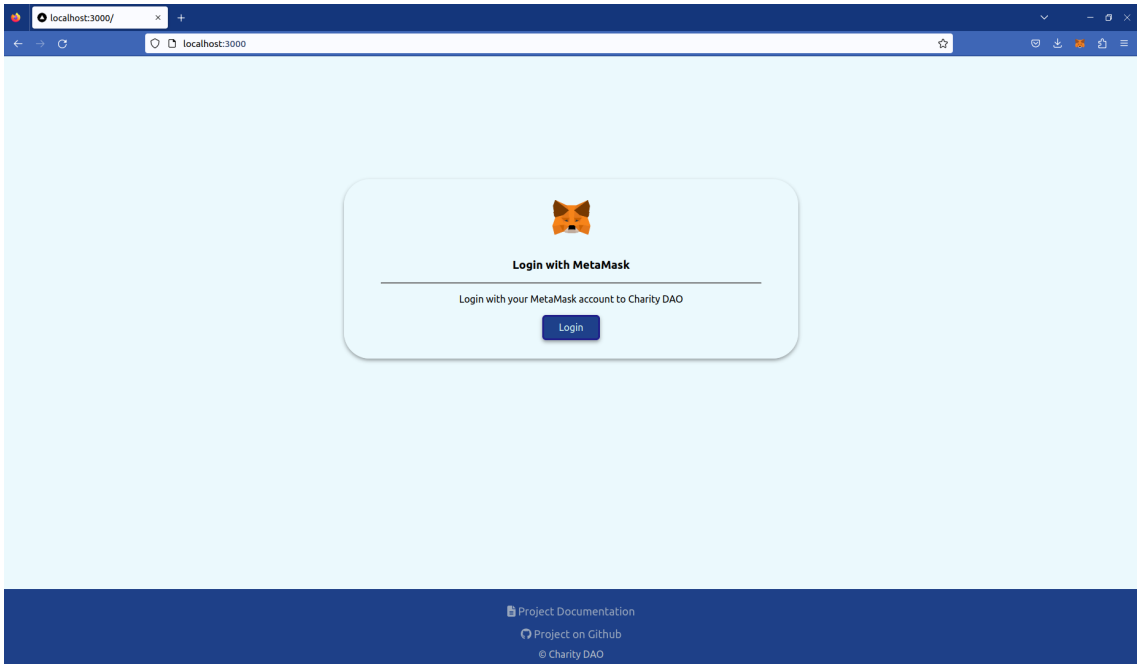
Κεφάλαιο 6

Επίδειξη Λειτουργίας

Στο κεφάλαιο αυτό γίνεται η επίδειξη της λειτουργίας του Charity DAO μέσω του user interface που έχει δημιουργηθεί. Το frontend έχει δημιουργηθεί με χρήση του πλαισίου λογισμικού Next.js, όπως έχει αναφερθεί και προηγουμένως. Πρόκειται ουσιαστικά για μια ιστοσελίδα στην οποία ο χρήστης συνδέεται με χρήση του Metamask πορτοφολιού του και μέσω αυτής μπορεί να αλληλεπιδράσει με το έξυπνο συμβόλαιο της εφαρμογής εκτελώντας διάφορες λειτουργίες.

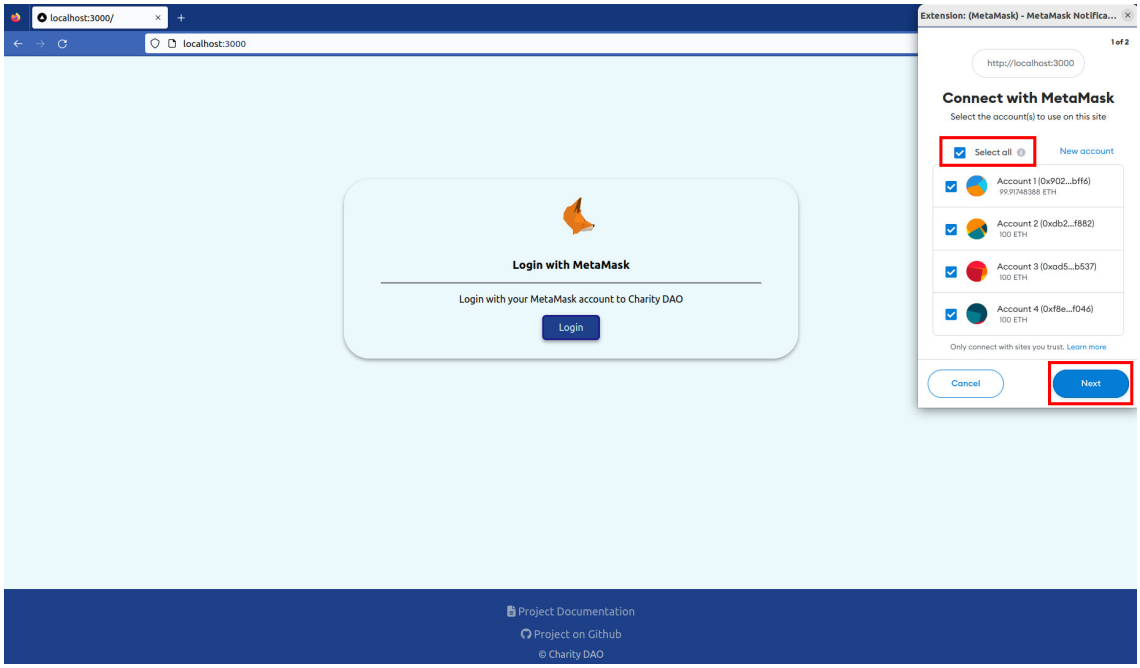
6.1 Σελίδα Login

Με χρήση της εντολής *npm run dev* ενεργοποιείται η σελίδα της εφαρμογής στο port 3000 του localhost. Η πρώτη σελίδα που εμφανίζεται με την ενεργοποίηση του URL είναι η σελίδα σύνδεσης Login η οποία φαίνεται ακολούθως.

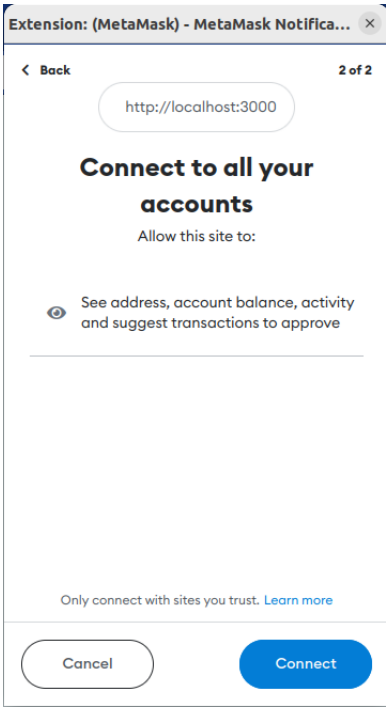


Σχήμα 6.1: *Σελίδα Login*

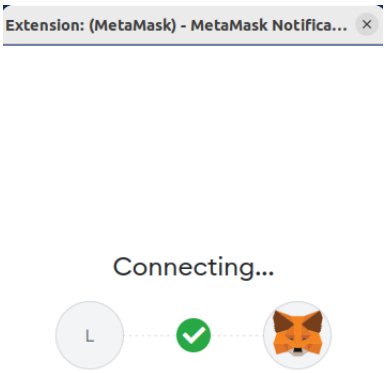
Ενεργοποιώντας την επιλογή login εμφανίζεται ένα παράθυρο του Metamask μέσω του οποίου γίνεται επιλογή για τους λογαριασμούς που θα συνδεθούν με το Charity DAO. Με την επιλογή Select all όλοι οι λογαριασμοί συνδέονται με το User Interface.



Σχήμα 6.2: *Επιλογή λογαριασμών για σύνδεση με το UI*



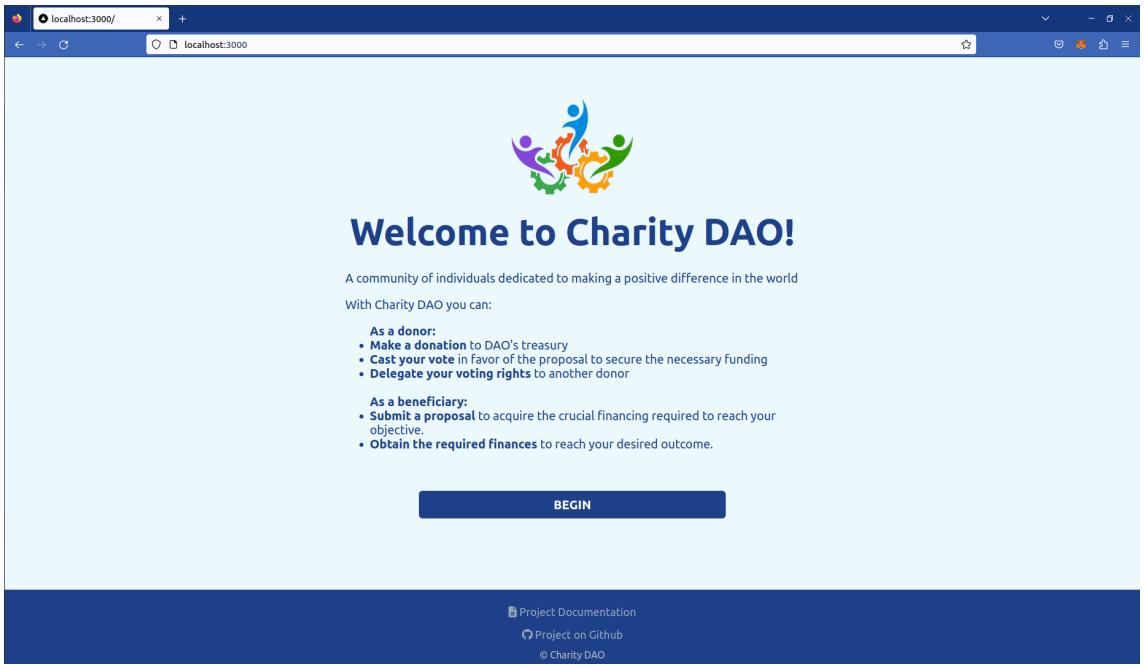
Σχήμα 6.3: *Έγκριση για σύνδεση των επιλεγμένων λογαριασμών*



Σχήμα 6.4: *Σύνδεση των λογαριασμών Metamask με το UI*

6.2 Αρχική Σελίδα

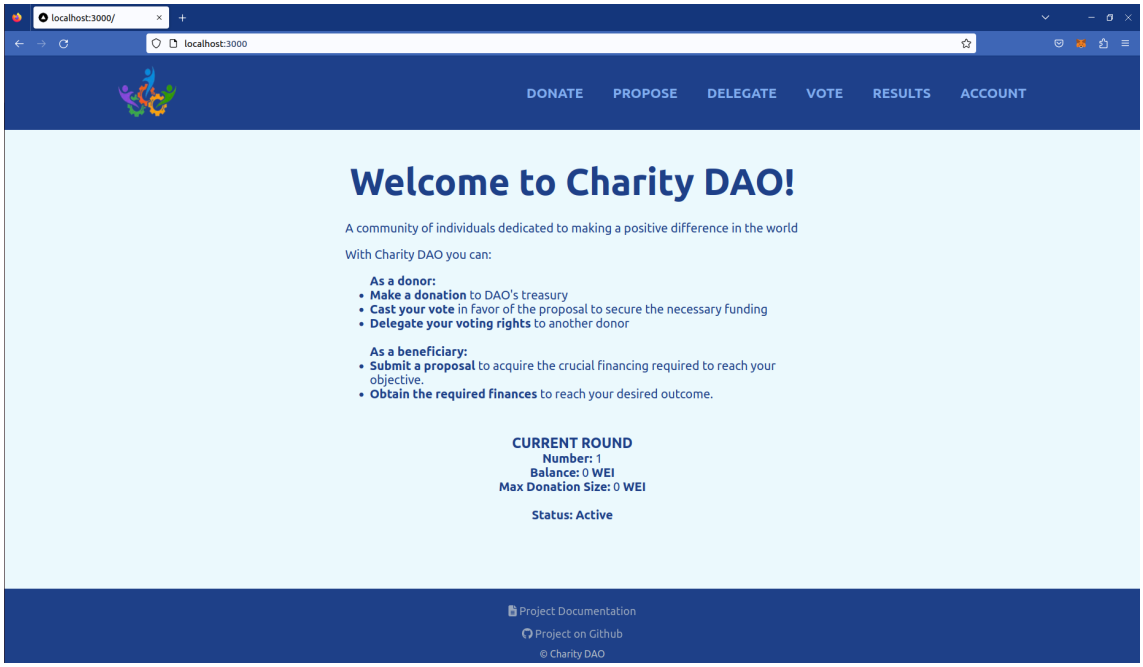
Έπειτα από στην σύνδεση των λογαριασμών εμφανίζεται η αρχική σελίδα του Charity DAO.



Σχήμα 6.5: *Αρχική σελίδα του Charity DAO*

Όπως έχει αναφερθεί νωρίτερα, το Charity DAO λειτουργεί σε γύρους. Η έναρξη του πρώτου γύρου γίνεται με το πάτημα του Begin button. Εμφανίζεται εκ νέου ένα παράθυρο του Metamask για την έγκριση της επιλογής. Από τη στιγμή της ενεργοποίησής του ξεκινά η αντίστροφη μέτρηση του πρώτου γύρου.

Η αρχική σελίδα μετατρέπεται ως ακολούθως.

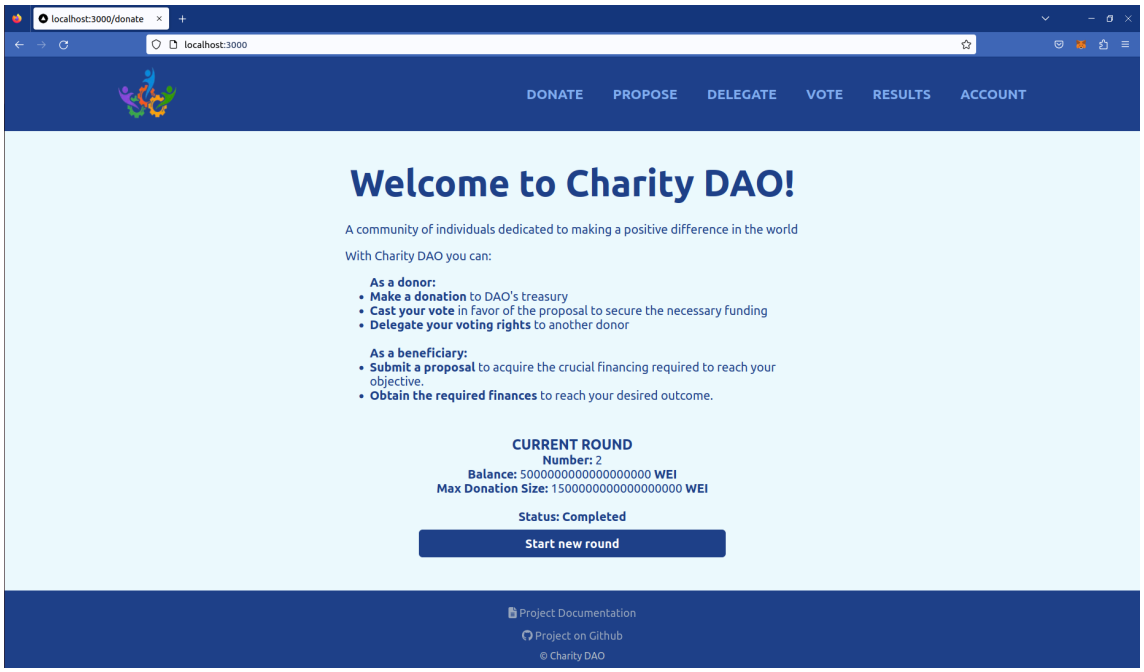


Σχήμα 6.6: *Αρχική σελίδα του Charity DAO μετά την έναρξη των γύρων*

Πλέον στην αρχική σελίδα εμφανίζεται ένα μενού επιλογών καθώς και πληροφορίες για τον τρέχοντα γύρο του Charity DAO οι οποίες ενημερώνονται ανάλογα με τις ενέργειες των χρηστών.

Η ετικέτα Number φανερώνει τον τρέχοντα γύρο, η ετικέτα Balance το υπόλοιπο του treasury του DAO ενώ η ετικέτα Status ενημερώνει τους χρήστες για την κατάσταση του γύρου, δηλαδή αν ένας γύρος είναι ενεργός ή έχει ολοκληρωθεί. Όπως έχει εξηγηθεί και προηγουμένως σε κάθε γύρο το Charity DAO μπορεί να διαθέσει το 30% του θησαυροφυλακίου του, έτσι ώστε να υπάρχει κάποιο περιθώριο για γύρους κατά τους οποίους δεν υπάρχουν πολλές εισφορές. Η ετικέτα Max Donation Size φανερώνει το συνολικό ποσό που μπορεί να διατεθεί στον τρέχοντα γύρο.

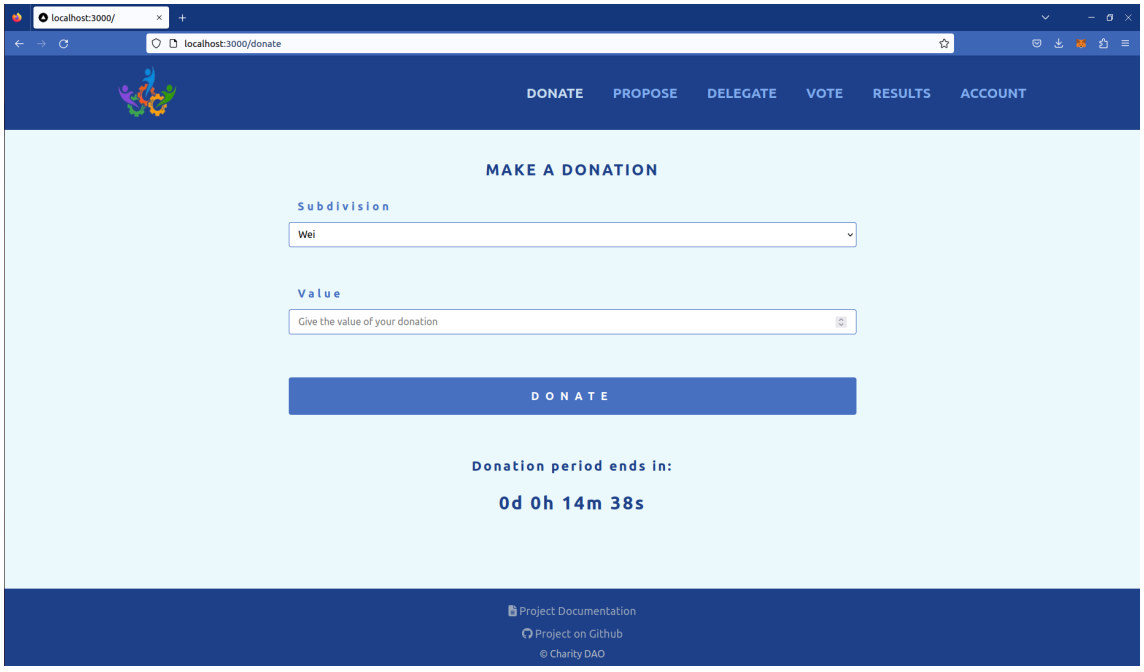
Όταν ένας γύρος ολοκληρωθεί το Status ενημερώνεται σε Completed και εμφανίζεται το κουμπί Start new round για την έναρξη του επόμενου γύρου.



Σχήμα 6.7: *Ολοκλήρωση γύρου*

6.3 Σελίδα Donate

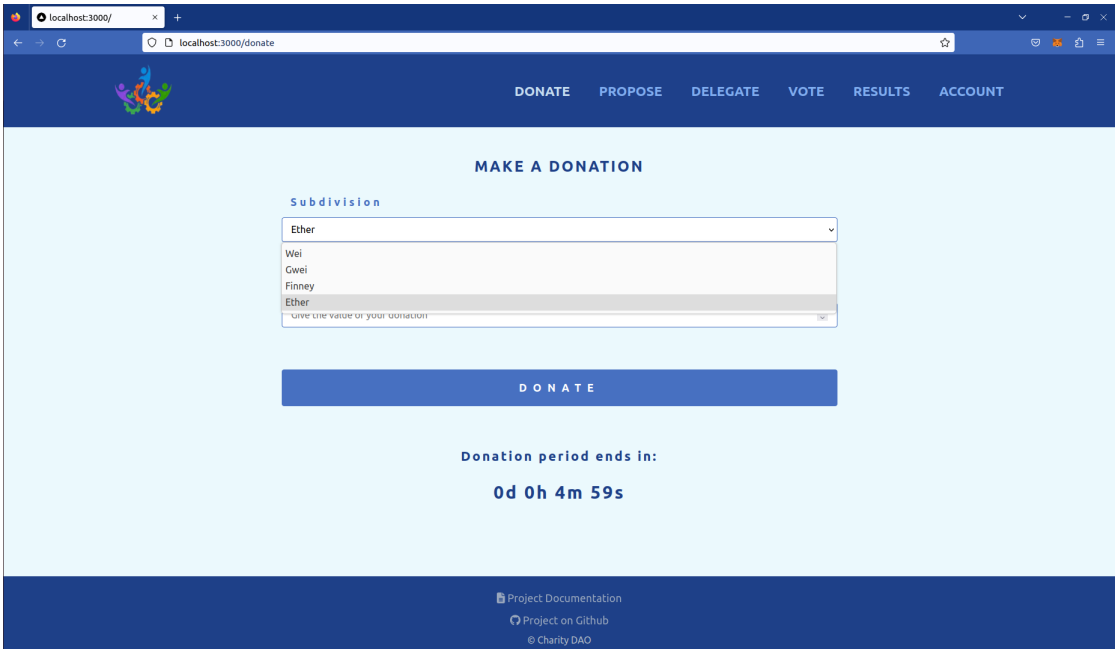
Από το Header Menu με την επιλογή Donate η σελίδα που εμφανίζεται είναι η εξής.



Σχήμα 6.8: *Σελίδα Donate*

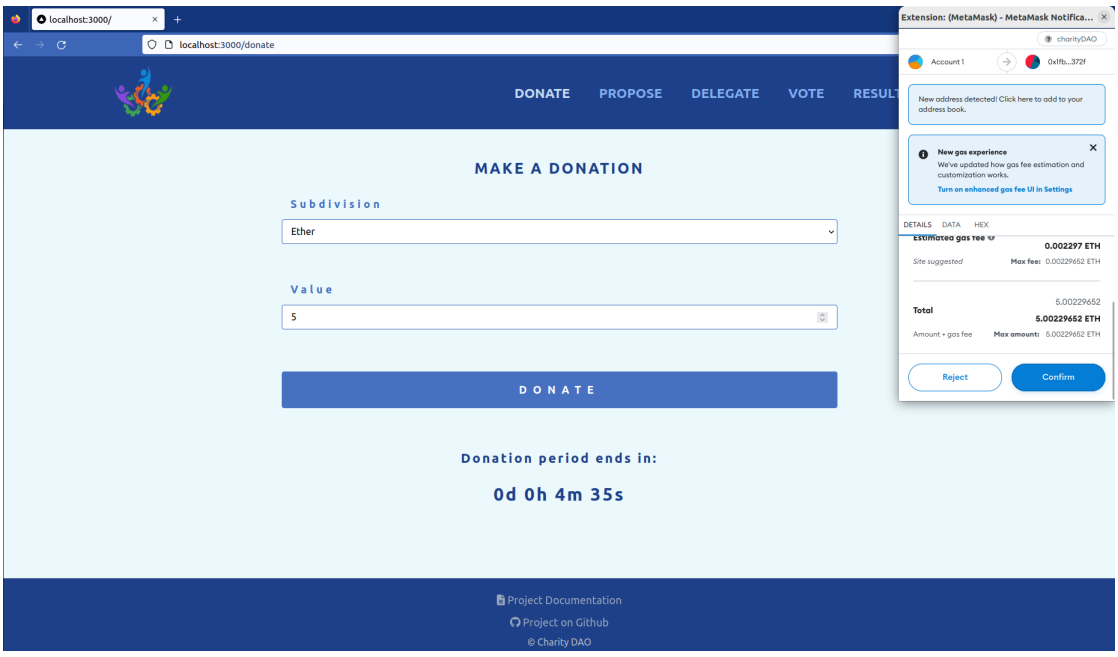
Στη σελίδα φαίνεται ο εναπομείναντας χρόνος μέχρι να ολοκληρωθεί η περίοδος των δωρεών.

Εδώ ένας χρήστης μπορεί να πραγματοποιήσει την δωρεά που επιθυμεί στο treasury του Charity DAO. Ο δωρητής επιλέγει από το Subdivision την υποδιαίρεση του κρυπτονομίσματος ανάμεσα σε Wei, Gwei, Finney και Ethers και πληκτρολογεί στο Value την τιμή που επιθυμεί.



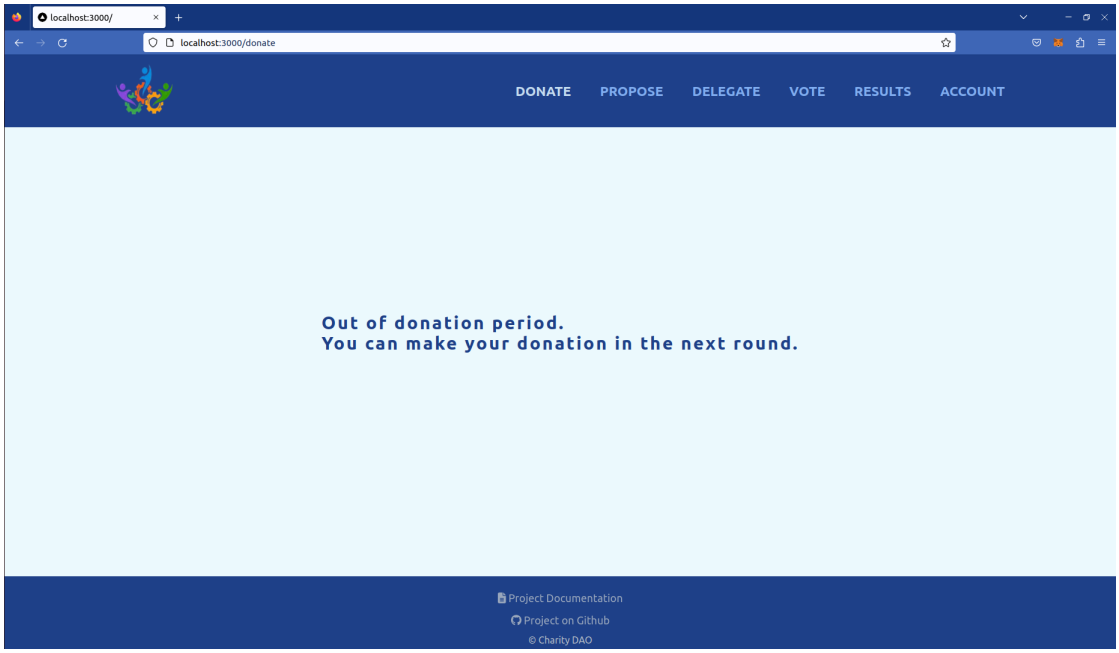
Σχήμα 6.9: *Επιλογή υποδιαίρεσης*

Με το πάτημα του Donate ένα παράθυρο του Metamask εμφανίζεται για την έγκριση της συναλλαγής και στη συνέχεια μέσω του smart contract πραγματοποιείται η μεταβίβαση του αντίστοιχου ποσού από το πορτοφόλι του δωρητή στο treasury του οργανισμού.



Σχήμα 6.10: *Έγκριση της δωρεάς του αντίστοιχου ποσού*

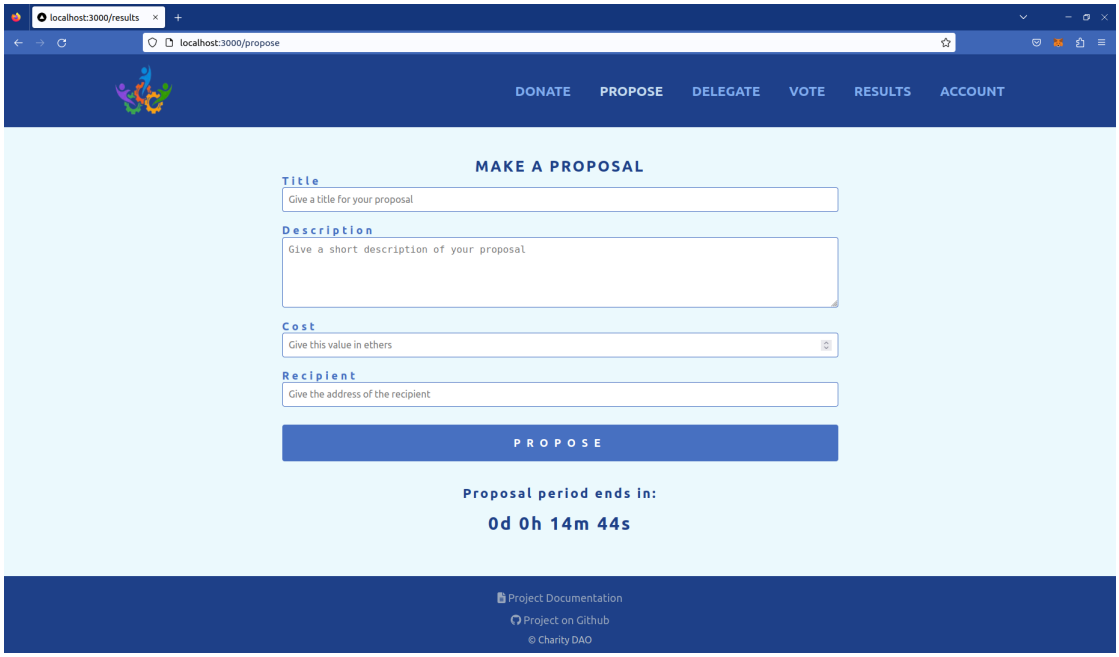
Μετά το πέρας της περιόδου δωρεών η φόρμα για τη συμπλήρωση των στοιχείων της δωρεάς απενεργοποιείται.



Σχήμα 6.11: *Ολοκλήρωση περιόδου δωρεών*

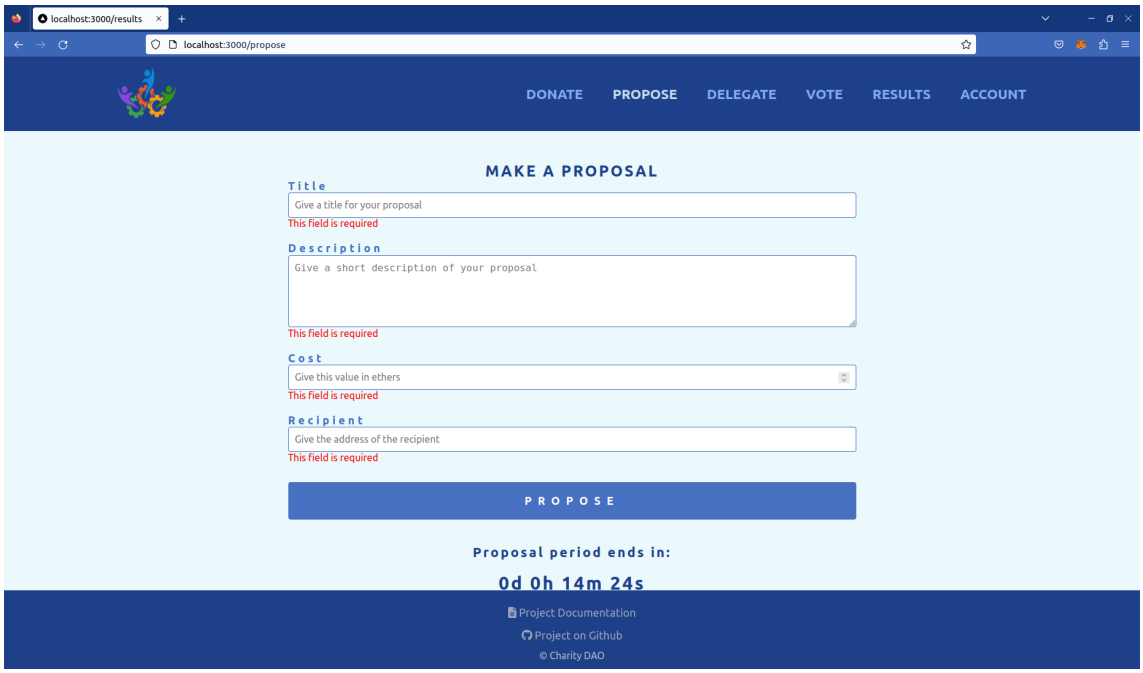
6.4 Σελίδα Propose

Η καρτέλα Propose του Header Menu οδηγεί στην ακόλουθη σελίδα.



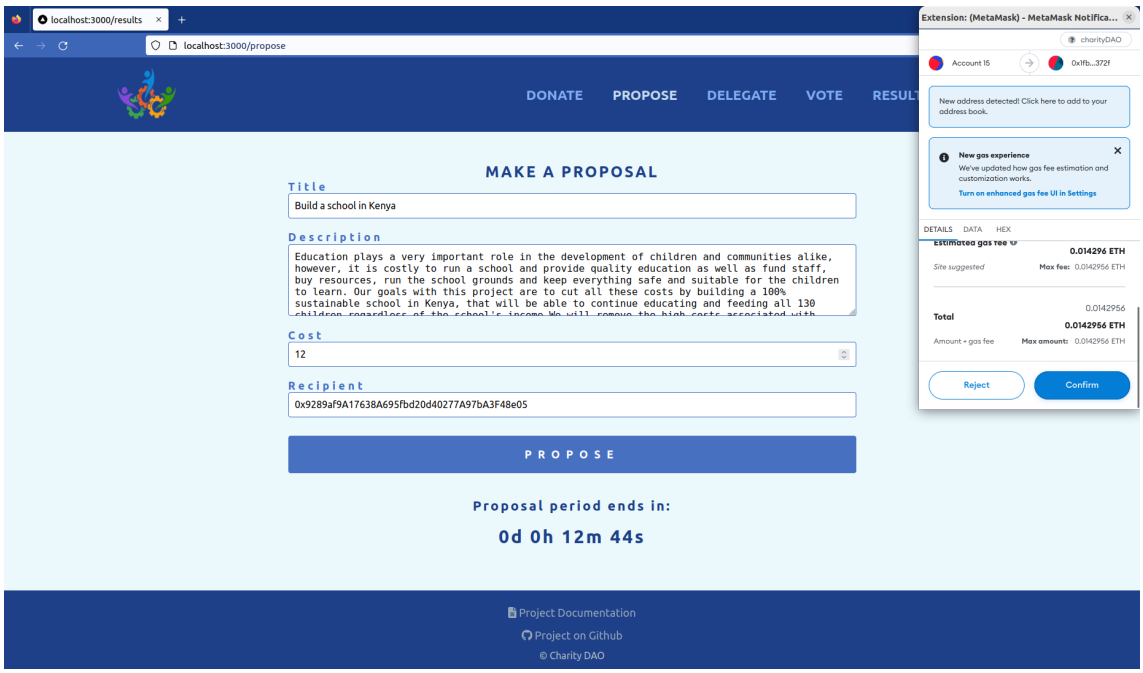
Σχήμα 6.12: *Σελίδα Propose*

Ο χρήστης που θέλει να κάνει κάποια πρόταση στον οργανισμό πρέπει να επιλέξει το κουμπί Propose πριν την λήξη του χρονικού διαστήματος που παρουσιάζεται στο κάτω μέρος της σελίδας και έχοντας συμπληρώσει όλα τα πεδία της φόρμας με τις απαραίτητες πληροφορίες.



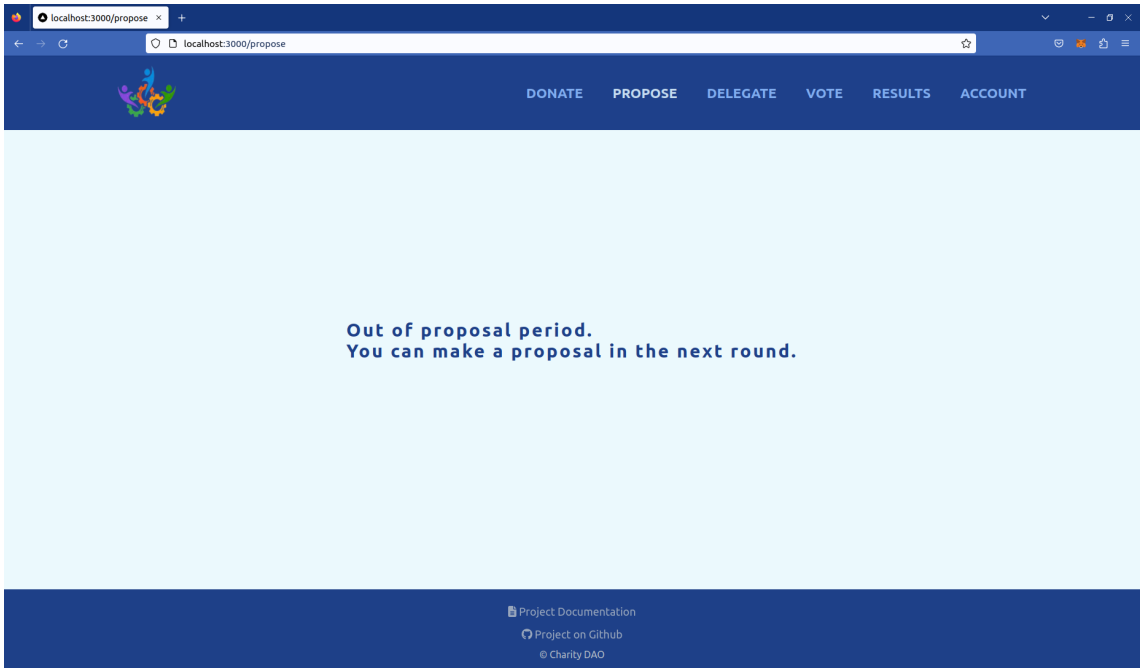
Σχήμα 6.13: *Απαραίτητα πεδία στην συμπλήρωση της φόρμας*

Εφόσον η φόρμα έχει συμπληρωθεί σωστά εμφανίζεται το γνωστό πλέον παράθυρο του Metamask και έπειτα από την έγκριση του χρήστη η πρότασή του καταχωρείται ως υποψήφια για τον τρέχοντα γύρο.



Σχήμα 6.14: *Πραγματοποίηση ενός proposal*

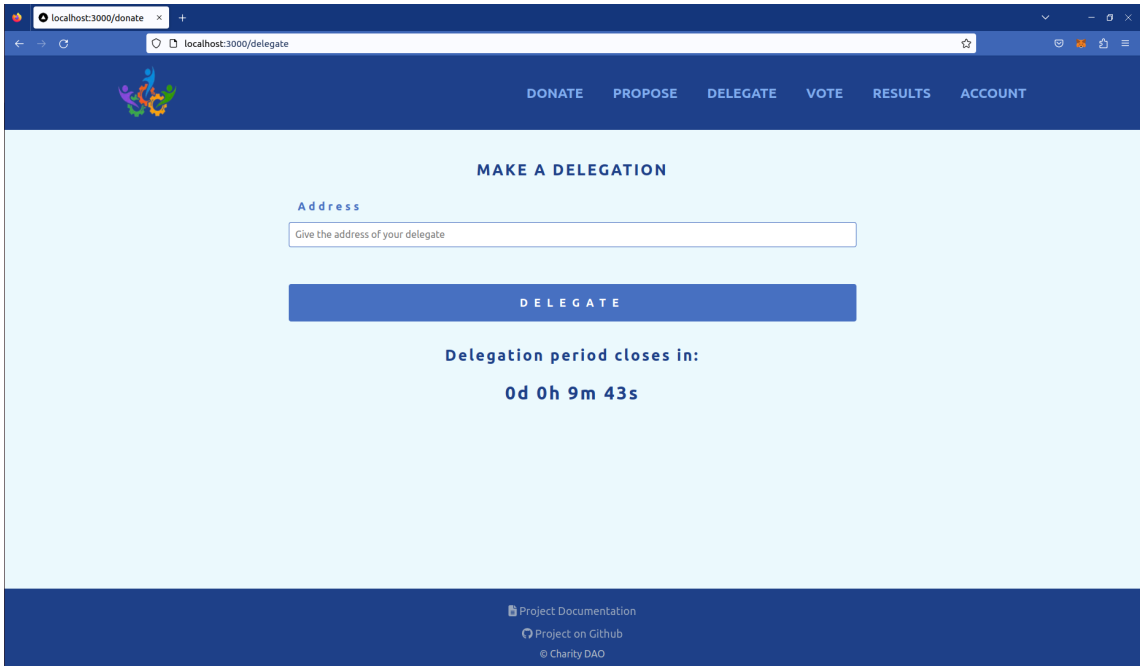
Μετά τη λήξη της περιόδου κατά την οποία επιτρέπονται οι υποβολές προτάσεων η σελίδα Propose μετατρέπεται ως εξής.



Σχήμα 6.15: *Ολοκλήρωση περιόδου υποβολής προτάσεων*

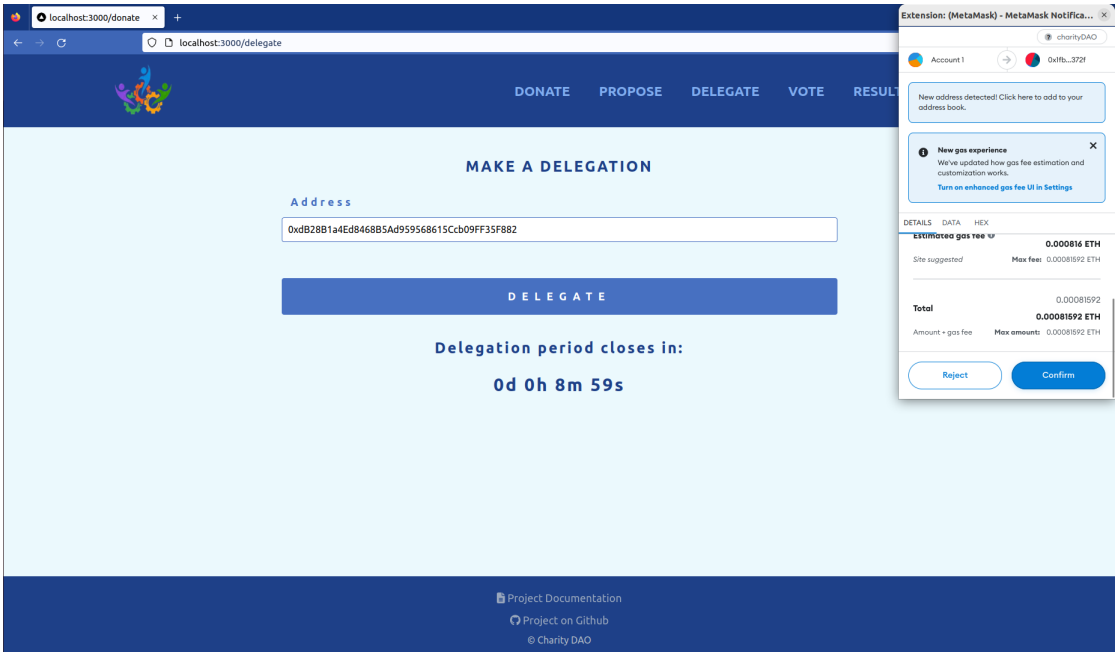
6.5 Σελίδα Delegate

Επιλέγοντας από το Μενού την καρτέλα Delegate εμφανίζεται η ακόλουθη σελίδα.



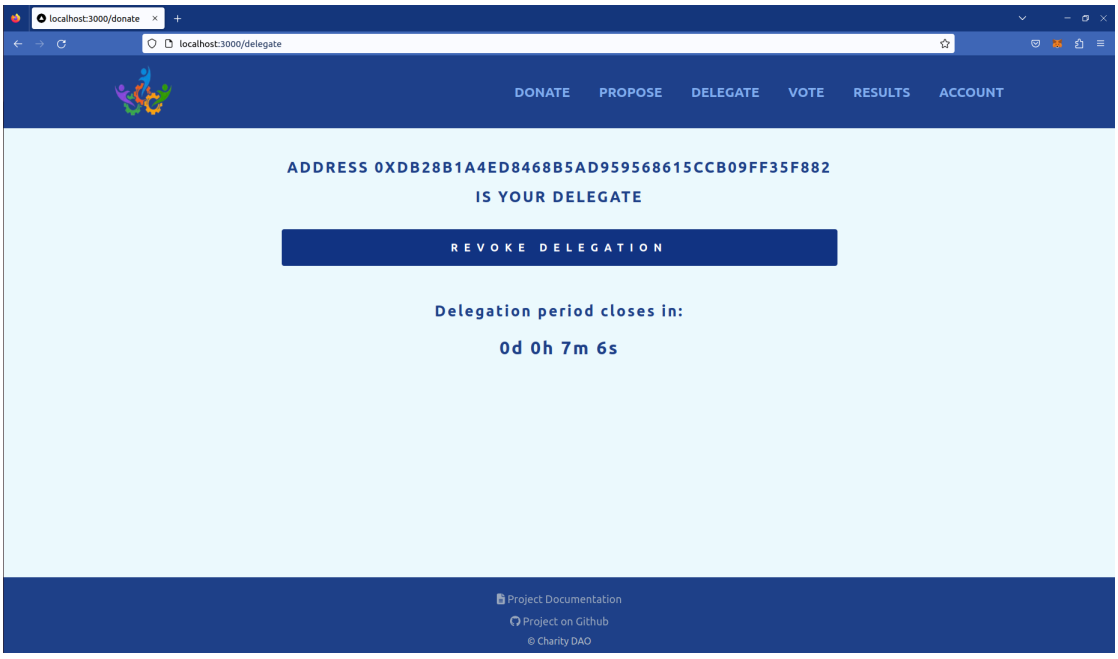
Σχήμα 6.16: *Σελίδα Delegate όταν δεν υπάρχει αντιπρόσωπος*

Σε περίπτωση που ο χρήστης θέλει να ορίσει κάποιον εκπρόσωπο, μεταβιβάζοντάς του τα δικαιώματα ψήφου του, προσδιορίζει την διεύθυνση του χρήστη που επιθυμεί και επιλέγει το κουμπί Delegate.
Το παράθυρο του Metamask εμφανίζεται για την έγκριση και έπειτα με εκτέλεση των κατάλληλων συναρτήσεων του smart contract πραγματοποιείται η μεταβίβαση των δικαιωμάτων.



Σχήμα 6.17: *Έγκριση της μεταβίβασης των δικαιωμάτων ψήφου*

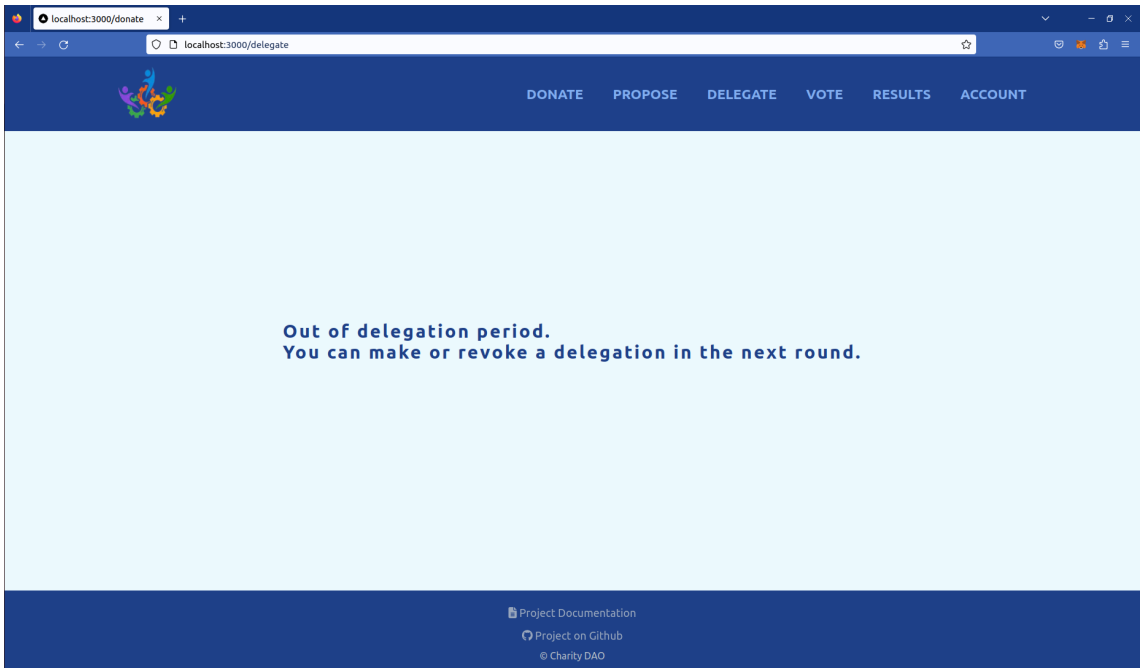
Πλέον ο χρήστης έχει έναν αντιπρόσωπο ο οποίος ψηφίζει εκ μέρους του. Σε αυτή την περίπτωση επιλέγοντας την καρτέλα Delegate εμφανίζεται η εξής σελίδα.



Σχήμα 6.18: *Σελίδα Delegate όταν υπάρχει αντιπρόσωπος*

Πατώντας το κουμπί Revoke ο χρήστης πάυει να έχει αντιπρόσωπο και επανακτά τα δικαιώματα ψήφου του. Φυσικά, όπως πάντα, χρειάζεται να γίνει έγκριση στο παράθυρο του Metamask που εμφανίζεται μετά το πάτημα του κουμπιού.

Η περίοδος κατά την οποία επιτρέπονται οι μεταβιβάσεις δικαιωμάτων ψήφου είναι συγκεκριμένη και ολοκληρώνεται πριν την περίοδο ψηφοφορίας. Στη σελίδα υπάρχει πάντα το χρονόμετρο που φανερώνει τον υπολοιπόμενο χρόνο κατά τον οποίο μπορούν να εκτελεστούν οι λειτουργίες που αφορούν τους αντιπροσώπους. Όταν η περίοδος αυτή ολοκληρωθεί η σελίδα Delegate έχει ως εξής.

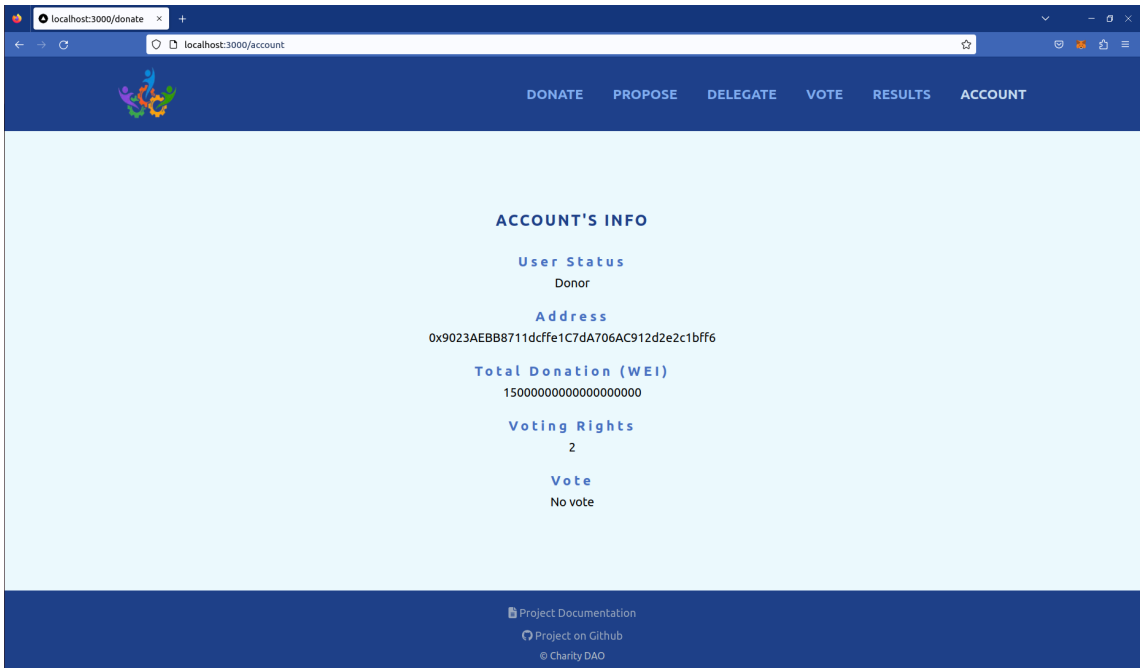


Σχήμα 6.19: *Ολοκλήρωση περιόδου μεταβίβασης δικαιωμάτων ψήφου*

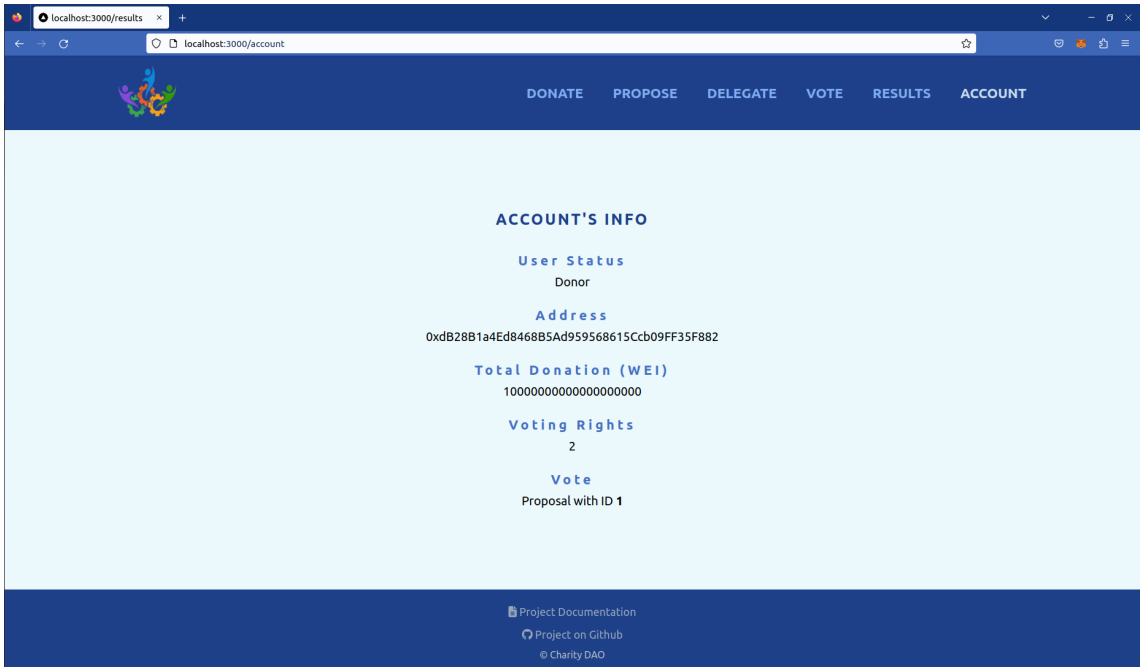
6.6 Σελίδα Account

Η καρτέλα Account του Header Menu εμφανίζει τις πληροφορίες του χρήστη. Πιο κάτω παρατίθενται δύο παραδείγματα.

Σε περίπτωση που ο χρήστης είναι δωρητής στο User Status εμφανίζεται η ένδειξη Donor και στην ετικέτα Address αναγράφεται η διεύθυνση του χρήστη. Η ετικέτα Total Donation φανερώνει το συνολικό ποσό σε Wei που έχει δωρίσει ο χρήστης στον οργανισμό από το οποίο εξαρτάται και το πλήθος των δικαιωμάτων ψήφου Voting Rights. Η ετικέτα Vote φανερώνει το ID της πρότασης που έχει ψηφίσει ο χρήστης ή σε περίπτωση που δεν έχει ακόμη ψηφίσει αναγράφεται η ένδειξη No Vote.

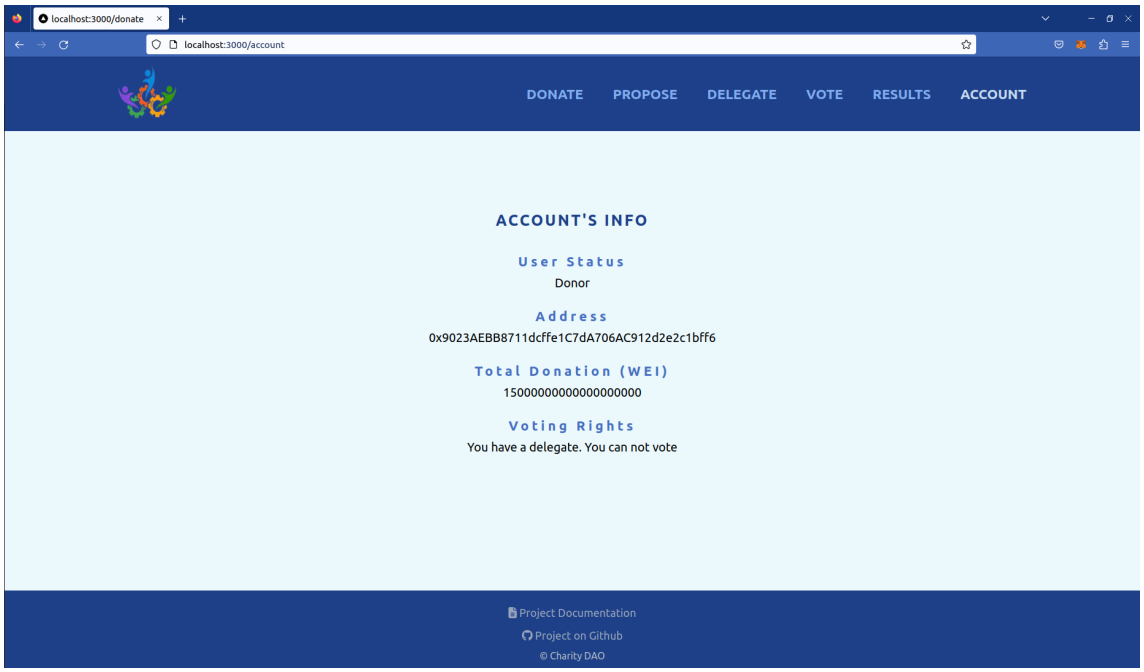


Σχήμα 6.20: *Πληροφορίες δωρητή 0x9023AEBB8711dcffe1C7dA706AC912d2e2c1bff6*



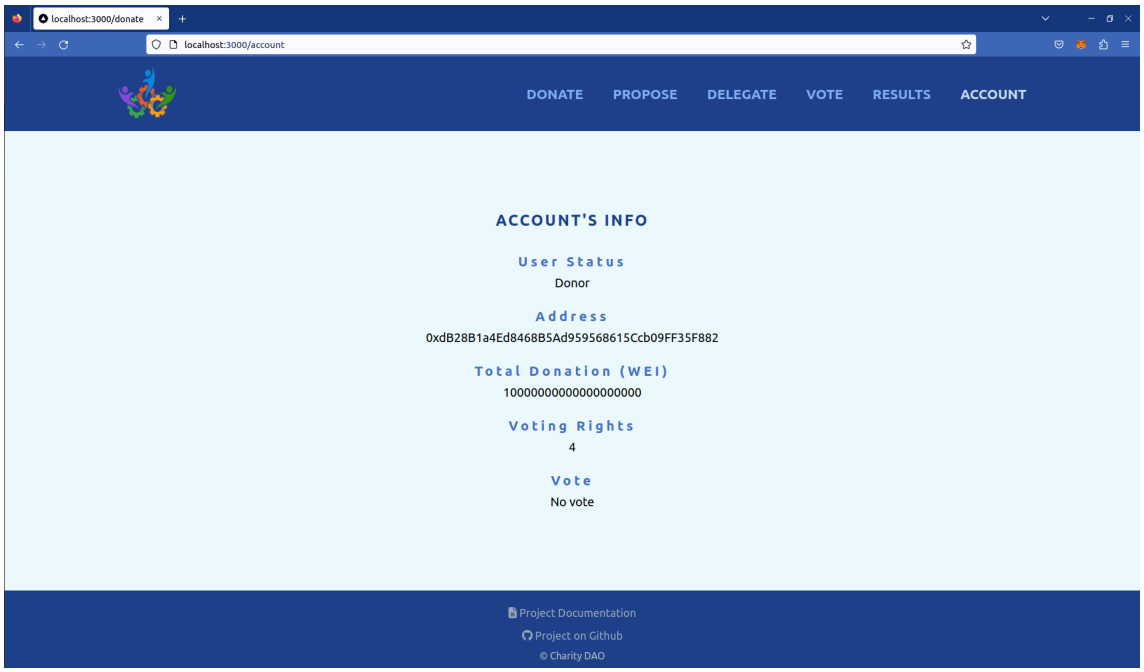
Σχήμα 6.21: *Πληροφορίες δωρητή 0xdB28B1a4Ed8468B5Ad959568615Ccb09FF35F882*

Εάν για παράδειγμα ο χρήστης 0x9023AEBB8711dcffe1C7dA706AC912d2e2c1bff6 είχε θέσει ως αντιπρόσωπό του τον χρήστη 0xdB28B1a4Ed8468B5Ad959568615Ccb09FF35F882 τότε τα προφίλ των χρηστών θα μετατρέπονταν ως εξής.



Σχήμα 6.22: *Πληροφορίες δωρητή 0x9023AEBB8711dcffe1C7dA706AC912d2e2c1bff6*

Στο προφίλ του χρήστη ο οποίος έχει θέσει τον αντιπρόσωπο στην ετικέτα Voting Rights αναγράφεται πλέον η ένδειξη *You have a delegate. You can not vote.* Επιπλέον η ετικέτα Vote έχει αφαιρεθεί από τη σελίδα εφόσον ο χρήστης δεν μπορεί να ψηφίσει.

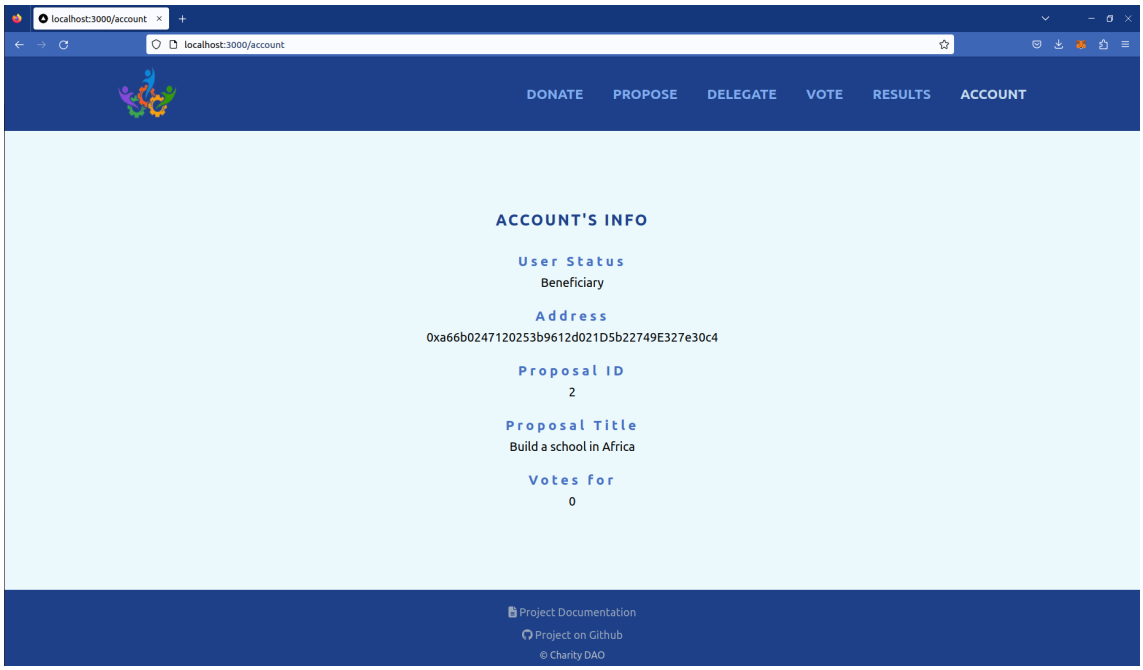


Σχήμα 6.23: *Πληροφορίες δωρητή 0xdB28B1a4Ed8468B5Ad959568615Ccb09FF35F882*

Στο προφίλ του αντιπροσώπου, ενώ σύμφωνα με το ποσό που έχει δώσει σαν δωρεά στον

οργανισμό θα έπρεπε να έχει δύο (2) δικαιώματα ψήφου, παρατηρείται η ένδειξη τέσσερα (4) στην ετικέτα Voting Rights. Αυτό οφείλεται στη μεταβίβαση των δικαιωμάτων ψήφου του χρήστη που τον έχει θέσει ως αντιπρόσωπο. Τα δικαιώματα που κατέχει πλέον το συγκεκριμένο προφίλ είναι το άθροισμα των δικαιωμάτων που έχει λάβει σύμφωνα με τις δωρεές που έχει πραγματοποιήσει και των δικαιωμάτων που του έχουν μεταβιβασει.

Σε περίπτωση που ο χρήστης είναι επωφελούμενος η σελίδα Account παρουσιάζει τις ακόλουθες πληροφορίες. Στο User Status αναγράφεται η ένδειξη Beneficiary. Η ετικέτα Proposal ID φανερώνει το μοναδικό αναγνωριστικό της πρότασης που έχει κάνει ο χρήστης ενώ η ετικέτα Proposal Title τον τίτλο της συγκεκριμένης πρότασης. Η ετικέτα Votes for παρουσιάζει τις ψήφους που έχει λάβει η πρόταση. Στο συγκεκριμένο παράδειγμα η πρόταση του χρήστη δεν έχει ψηφιστεί.

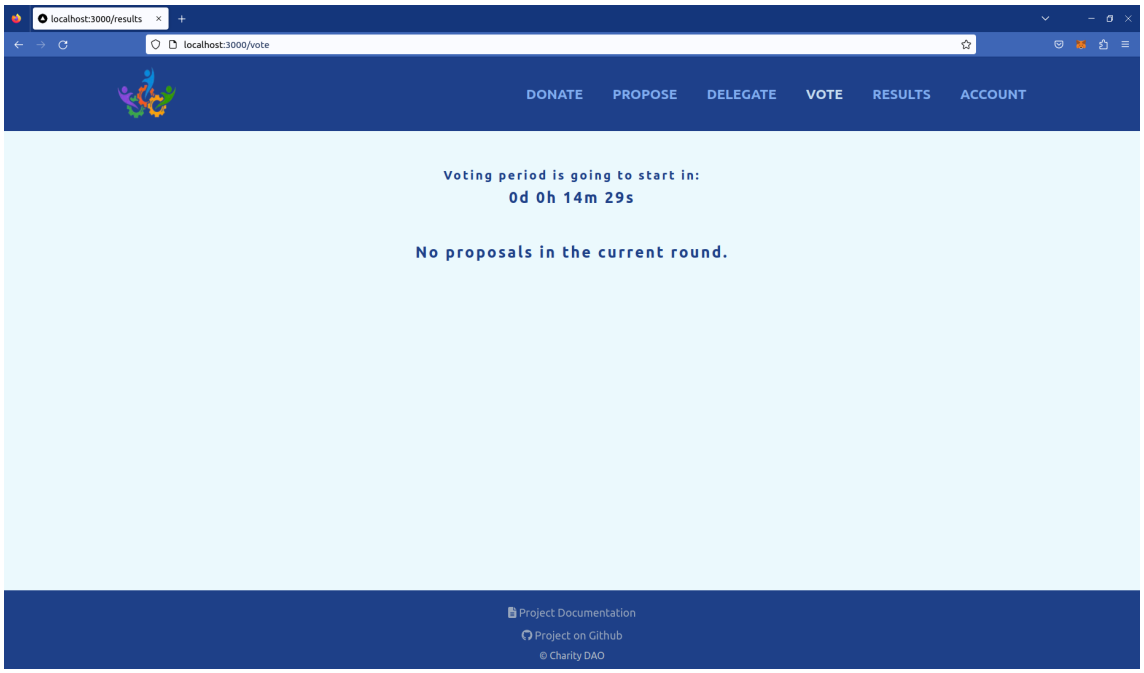


Σχήμα 6.24: *Πληροφορίες επωφελούμενου*

6.7 Σελίδα Vote

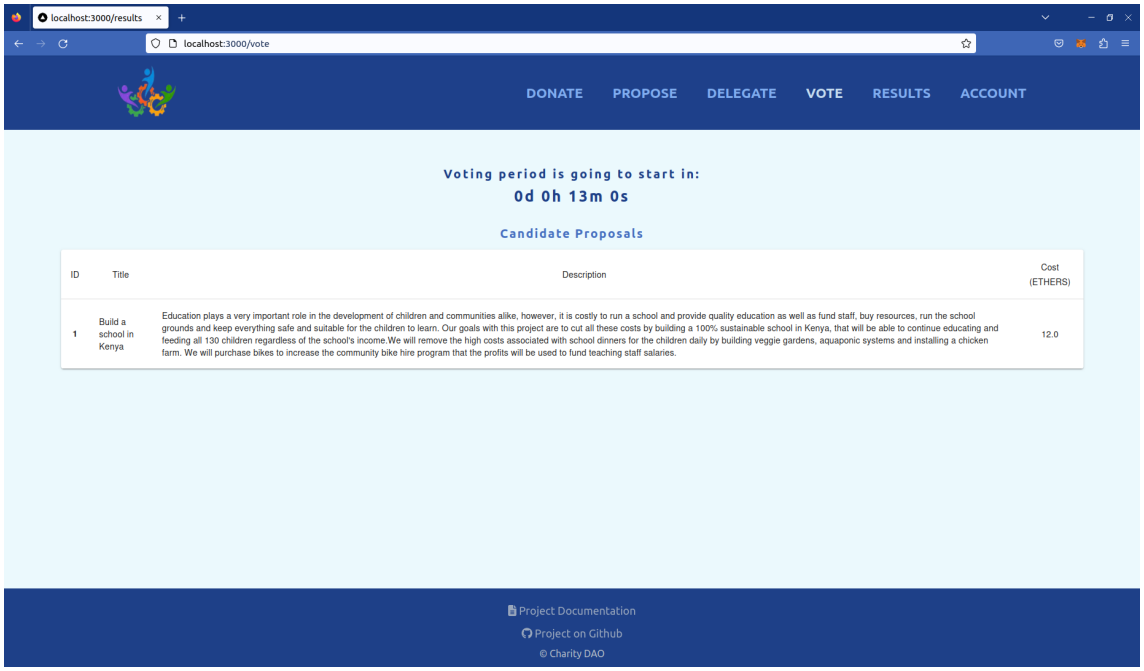
Η σελίδα Vote του Μενού διαφέρει ανάλογα με την περίοδο στην οποία βρίσκεται ο γύρος.

Σε περιόδους πριν την έναρξη της ψηφοφορίας ο χρήστης αντικρίζει αρχικά την ακόλουθη σελίδα.

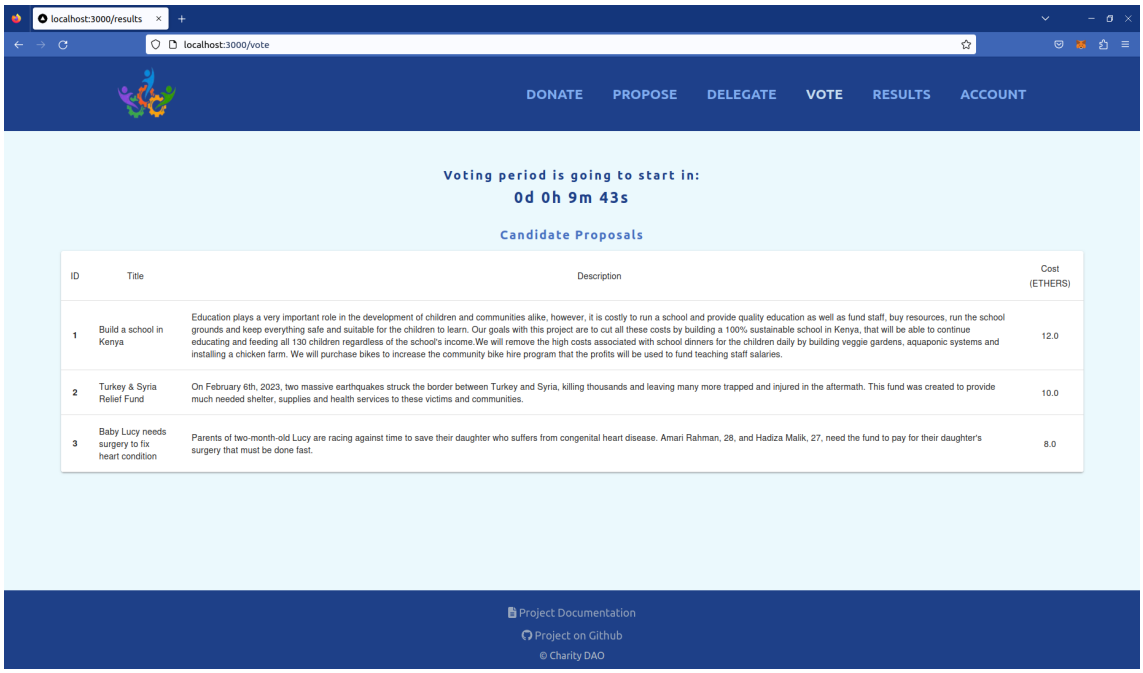


Σχήμα 6.25: *Σελίδα Vote πριν την περίοδο ψηφοφορίας χωρίς προτάσεις*

Όταν οι χρήστες αρχίσουν να πραγματοποιούν κάποια proposals για τον τρέχοντα γύρο αυτόματα οι προτάσεις που καταχωρούνται εμφανίζονται στη σελίδα Vote ώστε οι δωρητές που θα καλεστούν αργότερα να ψηφίσουν για τις προτάσεις αυτές να μπορούν να έχουν πρόσβαση και να παρακολουθούν τις υποψηφιότητες.

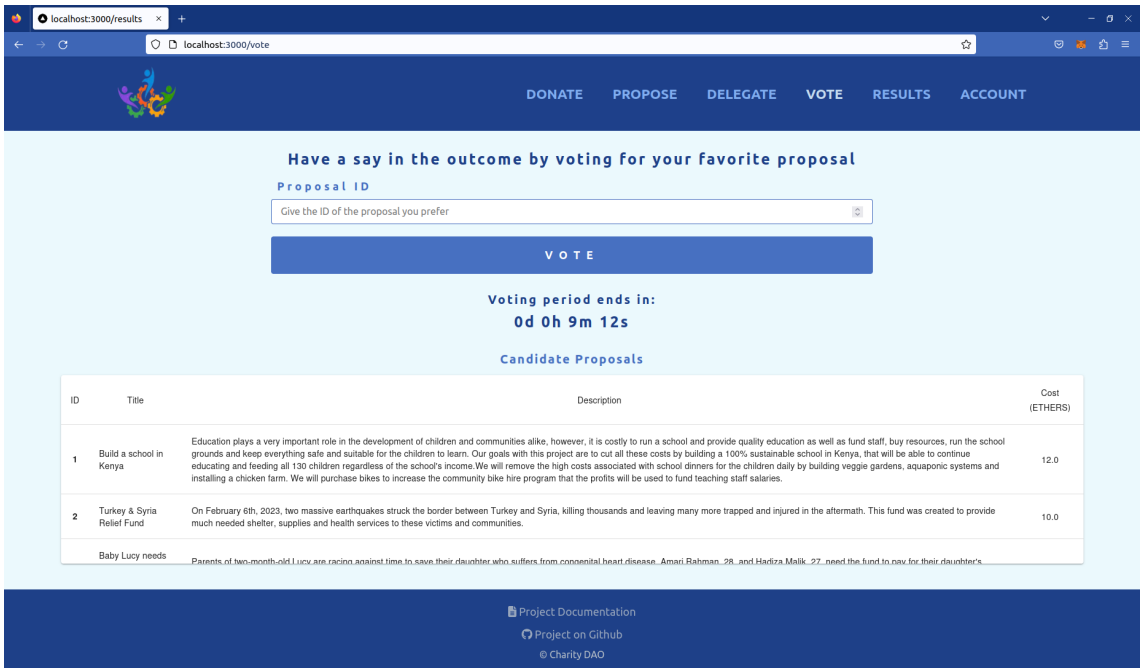


Σχήμα 6.26: *Σελίδα Vote πριν την περίοδο ψηφοφορίας με μία πρόταση*



Σχήμα 6.27: *Σελίδα Vote πριν την περίοδο ψηφοφορίας με τρεις προτάσεις*

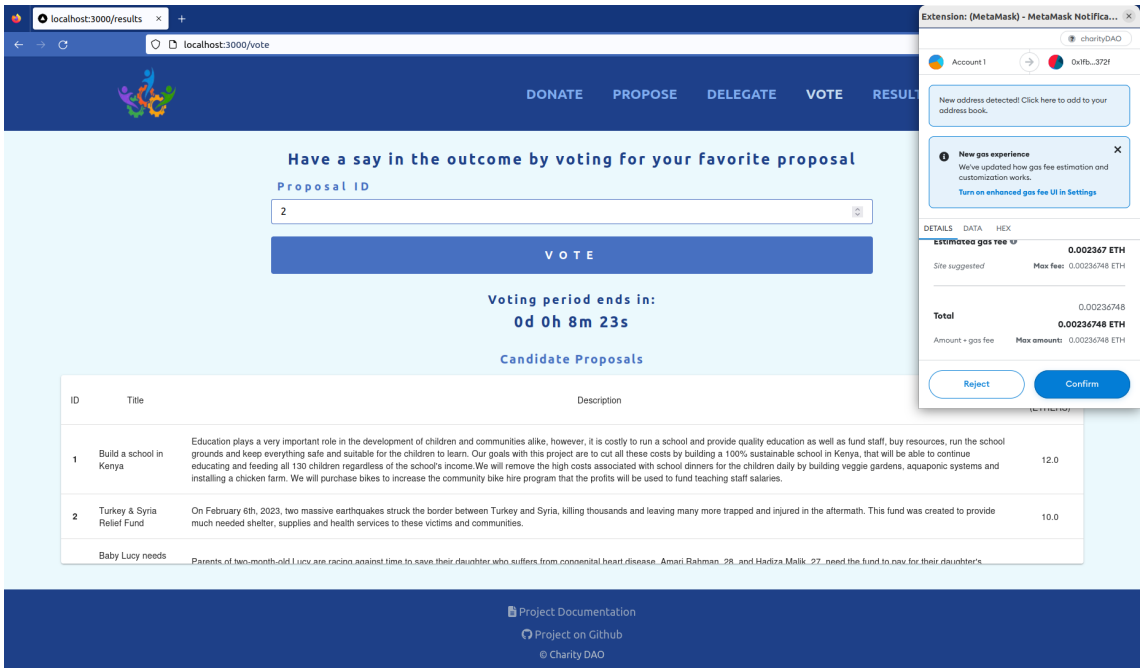
Μόλις ξεκινήσει η περίοδος ψηφοφορίας στη σελίδα Vote εμφανίζεται μία φόρμα μέσω της οποίας οι δωρητές μπορούν να επιλέξουν την πρόταση που θέλουν, ενώ ένα νέο χρονόμετρο που φανερώνει το χρονικό περιθώριο που υπάρχει για την ψηφοφορία αντικαθιστά το προηγούμενο.



Σχήμα 6.28: *Σελίδα Vote μετά την έναρξη της ψηφοφορίας*

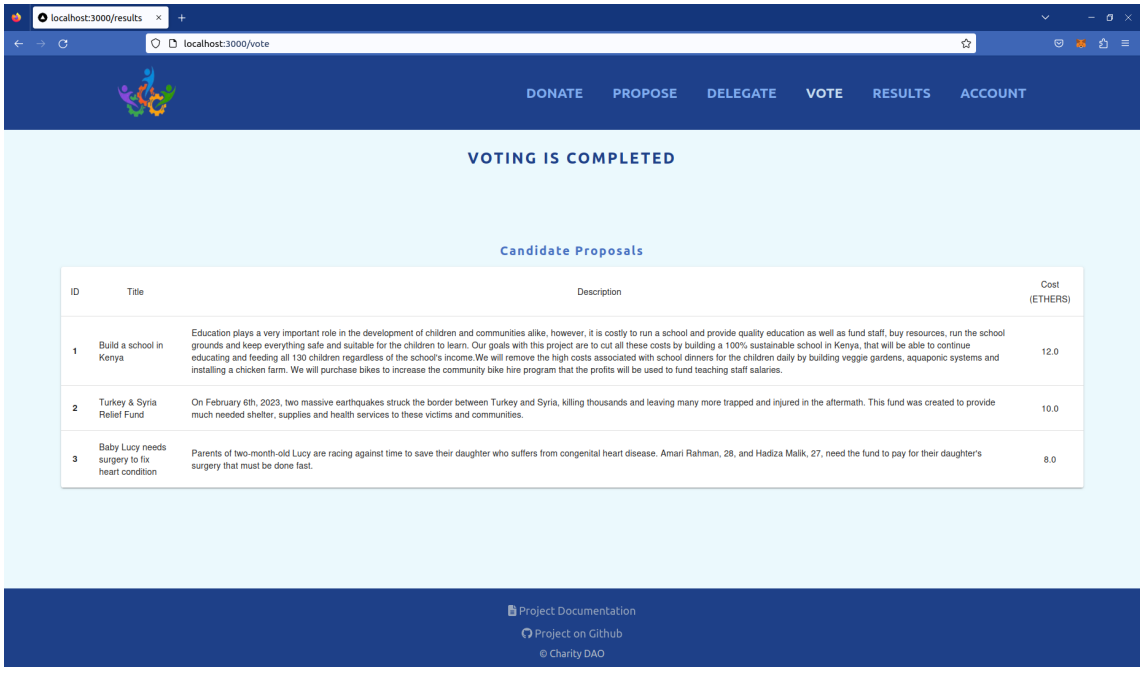
Ο scrollable πίνακας με τις υποψήφιες προτάσεις εξακολουθεί να φαίνεται στην οθόνη έτσι ώστε οι δωρητές να μπορούν να τις βλέπουν κατά τη διάρκεια της ψηφοφορίας.

Οι δωρητές επιλέγουν την επιθυμητή πρόταση και πληκτρολογούν στο πεδίο το μοναδικό αναγνωριστικό της. Πατώντας το κουμπί Vote το παράθυρο του Metamask εμφανίζεται και μετά από την έγκριση του χρήστη η ψήφος καταχωρείται.



Σχήμα 6.29: *Διαδικασία ψηφοφορίας*

Έπειτα από την ολοκλήρωση της περιόδου ψηφοφορίας η σελίδα μετατρέπεται ως ακολούθως.



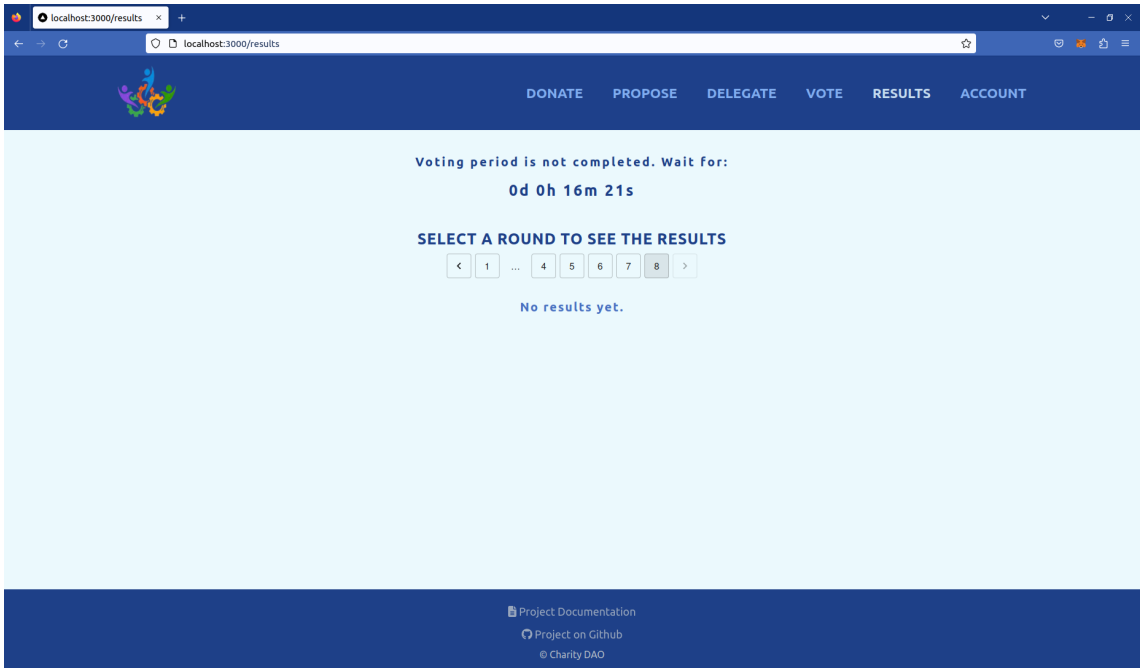
Σχήμα 6.30: *Ολοκλήρωση περιόδου ψηφοφορίας*

6.8 Σελίδα Results

Η καρτέλα Results του ιστότοπου είναι αυτή που φανερώνει όλο το έργο του οργανισμού. Παρουσιάζει τα αποτελέσματα του τρέχοντος γύρου όταν αυτά είναι διαθέσιμα όπως επίσης και τα αποτελέσματα όλων των προηγούμενων γύρων από την εκκίνηση του οργανισμού.

Σε περίοδο που η ψηφοφορία του τρέχοντος γύρου δεν έχει ολοκληρωθεί στη σελίδα φαίνεται η αντίστροφη μέτρηση για τον εναπομείναντα χρόνο κατά τον οποίο οι δωρητές μπορούν να καταθέσουν την ψήφο τους.

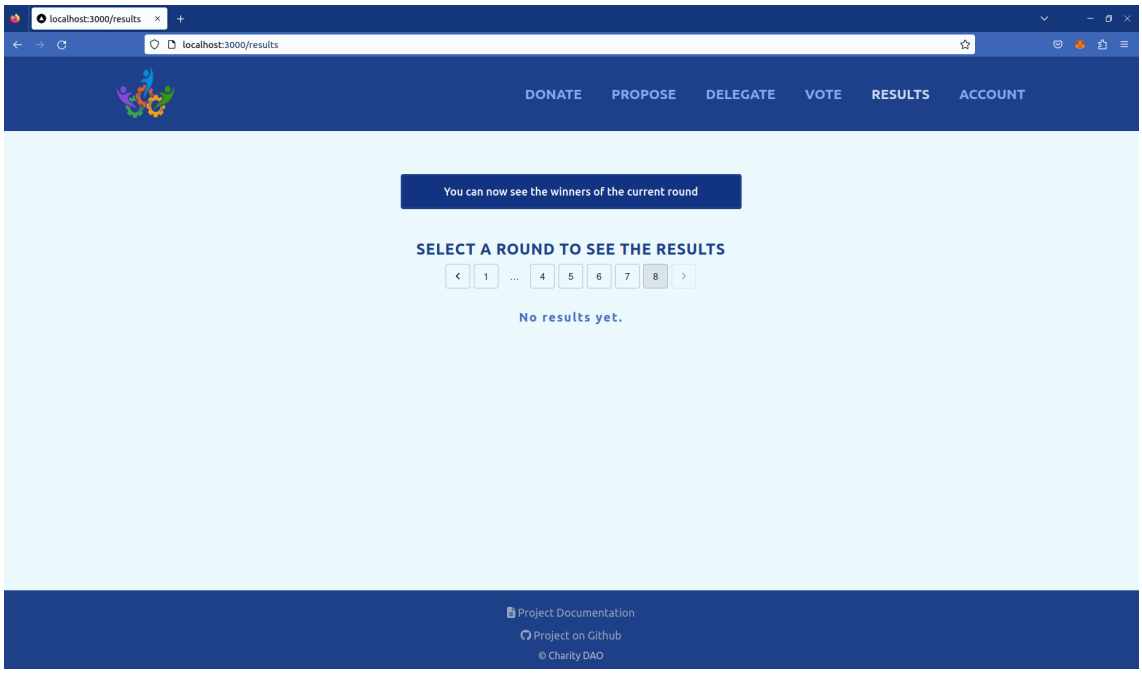
Επιπλέον υπάρχει μια σειρά από κουμπιά ισάριθμη με τους γύρους που έχουν μέχρι στιγμής πραγματοποιηθεί με τελευταίο τον τρέχοντα γύρο. Επιλέγοντας οποιονδήποτε γύρο επιθυμεί, ο χρήστης μπορεί πατώντας το αντίστοιχο κουμπί να δει τα αποτελέσματα του συγκεκριμένου γύρου, δηλαδή τις προτάσεις οι οποίες κέρδισαν στον εκάστοτε γύρο την χρηματοδότηση που ζητούσαν.



Σχήμα 6.31: *Σελίδα Results πριν από την ολοκλήρωση της ψηφοφορίας*

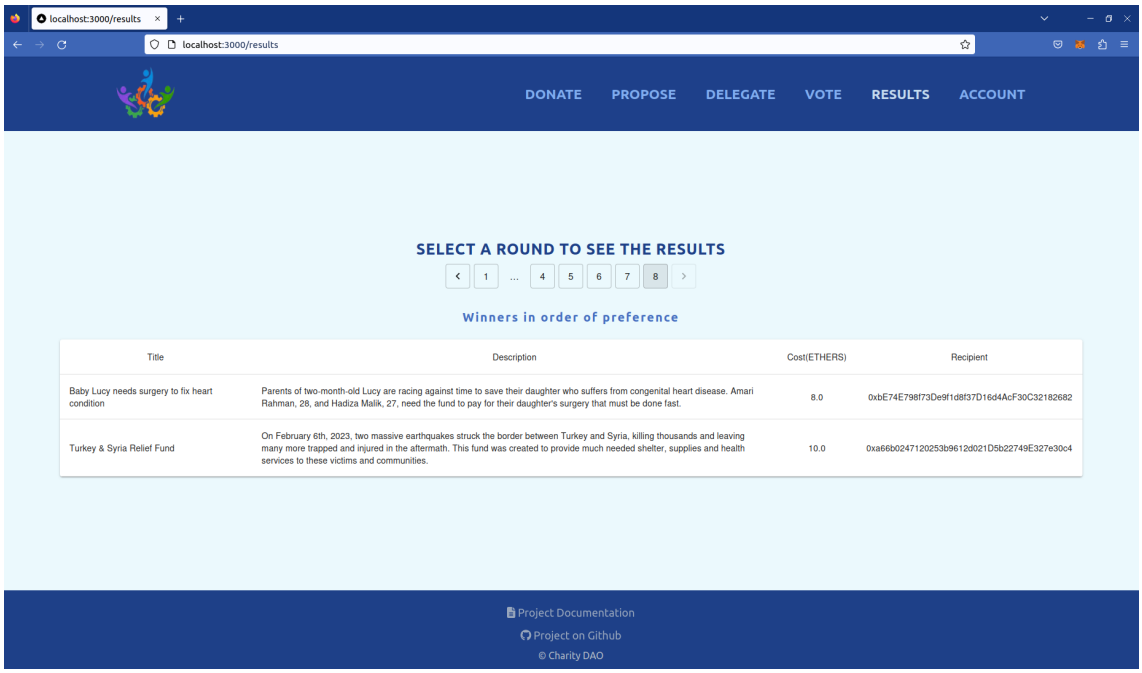
Στο στιγμιότυπο που φαίνεται πιο πάνω επιλεγμένος είναι ο τρέχοντας γύρος και σαν αποτέλεσμα φαίνεται η ένδειξη No results yet εφόσον δεν έχει ακόμη ολοκληρωθεί η διαδικασία της ψηφοφορίας.

Με τη λήξη της περιόδου ψηφοφορίας η αντίστροφη μέτρηση αντικαθίσταται από ένα κουμπί με την ετικέτα You can now see the winners of the current round.



Σχήμα 6.32: *Ολοκλήρωση της ψηφοφορίας*

Με το πάτημα του εν λόγω κουμπιού και την έγκριση του χρήστη στο παράθυρο του Metamask εκτελούνται στο smart contract όλες οι απαραίτητες ενέργειες για την ανάδειξη των νικητών, σύμφωνα πάντα με την ψήφο των δωρητών αλλά και το ποσό του treasury που είναι διαθέσιμο.

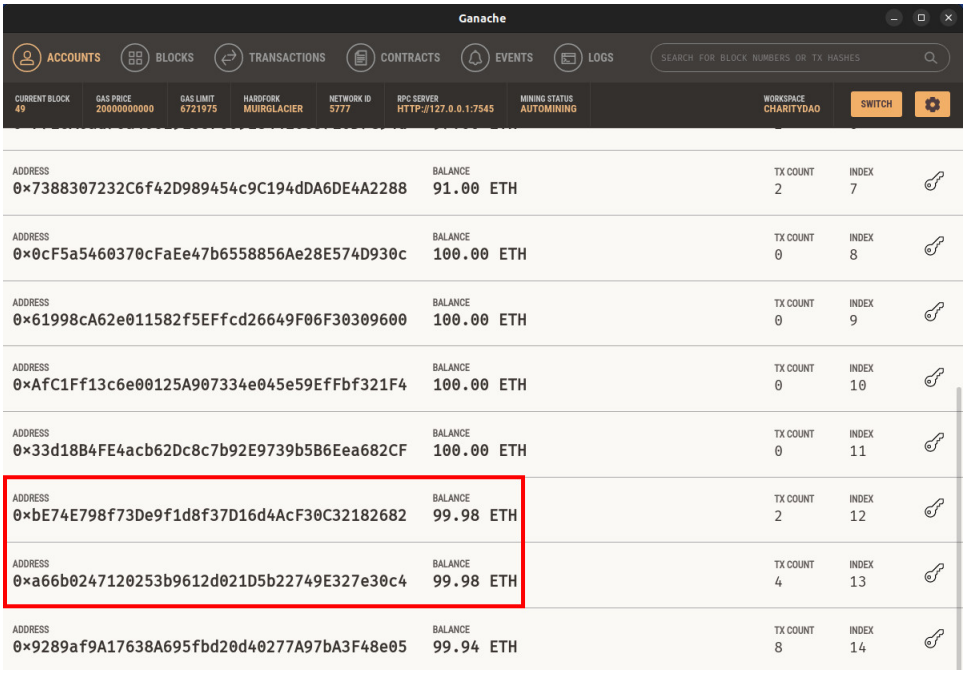


Σχήμα 6.33: *Παρουσίαση των αποτελεσμάτων*

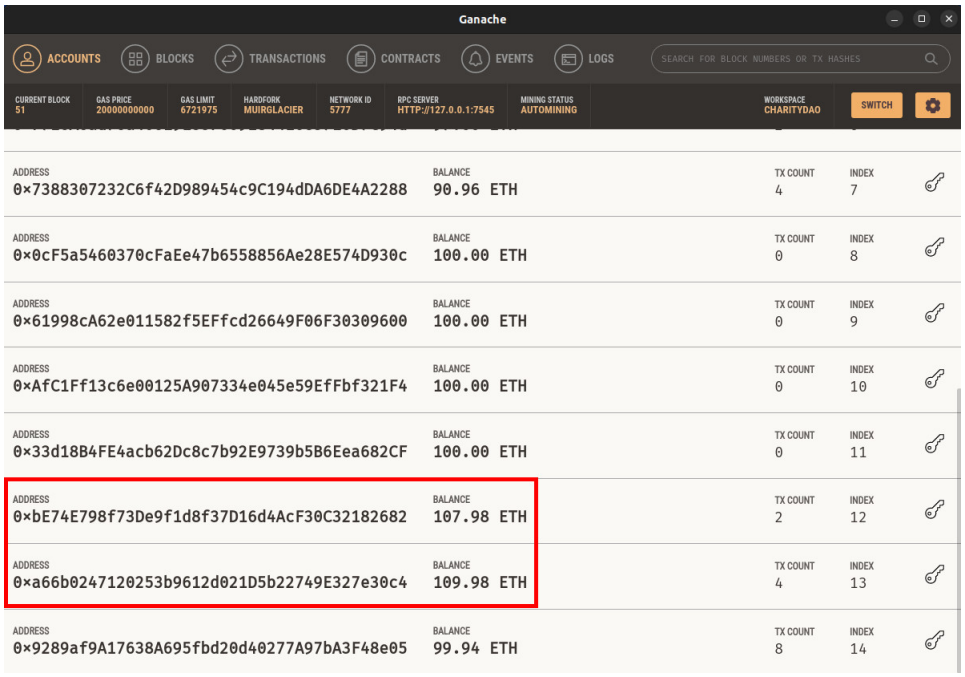
Αυτόματα, με την εκλογή των νικητήριων προτάσεων γίνεται και η μεταβίβαση του α-

ντίστοιχου ποσού στους δικαιούχους, χωρίς οποιαδήποτε επιπλέον διαδικασία ή έγκριση.

Πιο κάτω παρουσιάζονται στιγμιότυπα από το Ganache που φανερώνουν το υπόλοιπο των χρηστών μόλις πριν και αμέσως μετά την ανάδειξη των αποτελεσμάτων του τρέχοντος γύρου. Όπως γίνεται φανερό, οι δικαιούχοι των δύο νικηφόρων προτάσεων έλαβαν άμεσα στον λογαριασμό τους το ακριβές ποσό που είχε ζητηθεί.



Σχήμα 6.34: *Υπόλοιπα λογαριασμών μόλις πριν τα αποτελέσματα*



Σχήμα 6.35: *Υπόλοιπα λογαριασμών αμέσως μετά την ανάδειξη των νικητών*

Μέρος III

Επίλογος

Κεφάλαιο 7

Επίλογος

7.1 Ανακεφαλαίωση

Στην παρούσα διπλωματική εργασία εξετάστηκε η δημιουργία ενός Αποκεντρωμένου Αυτόνομου Οργανισμού (Decentralized Autonomous Organization - DAO) βασισμένου στην τεχνολογία Blockchain. Το DAO που δημιουργήθηκε είναι φιλανθρωπικού χαρακτήρα και χάρις στην τεχνολογία στην οποία στηρίζεται είναι ένα πλήρως αποκεντρωμένο σύστημα το οποίο μπορεί να προσφέρει αμεσότητα, ασφάλεια και αξιοπιστία σε αυτό τον τομέα που στις μέρες μας έχει τόσο αμφισβητηθεί.

Σκοπός ήταν η δημιουργία ενός οργανισμού στον οποίο δικαίωμα συμμετοχής έχει οποιοσδήποτε από οποιοδήποτε μέρος του κόσμου, με μόνη προϋπόθεση την πρόσβαση στο διαδίκτυο. Το Charity DAO ξεφεύγει από το πλαίσιο μιας φιλανθρωπικής οργάνωσης γενικού σκοπού και γίνεται το μέρος όπου κανείς μπορεί να ζητήσει βοήθεια για συγκεκριμένο σκοπό ανάλογα με τις δικές του ανάγκες.

Η κεντρική ιδέα ήταν η δημιουργία μιας σελίδας όπου ο κάθε ενδιαφερόμενος μπορεί να καταθέση μία πρόταση με την οποία ζητά ένα συγκεκριμένο ποσό για την υλοποίηση ενός συγκεκριμένου σκοπού - έργου για το οποίο δίνει τις απαραίτητες πληροφορίες και εξηγήσεις.

Εάν η πρόταση αυτή θα εγκριθεί από τον οργανισμό, εξαρτάται από τα μέλη του. Οι αποφάσεις λαμβάνονται συλλογικά μετά από ψηφοφορία στην οποία μπορεί να συμμετέχει κανείς κάνοντας κάποια δωρεά. Υπάρχει ένα ελάχιστο ποσό το οποίο χρειάζεται κάποιος να προσφέρει για να αποκτήσει δικαίωμα ψήφου, και ανάλογα με το συνολικό ποσο που δωρίζει στον οργανισμό τότε τα δικαιώματα ψήφου του μπορούν να αυξηθούν.

Το ποιες προτάσεις θα εγκριθούν εξαρτάται όχι μόνο από την έκβαση της ψηφοφορίας αλλά και από το συνολικό ποσό που υπάρχει στο treasury του οργανισμού. Οι δικαιούχοι των προτάσεων που εγκρίνονται λαμβάνουν αυτόματα, μέσω του smart contract, στους λογαριασμούς τους το αντίστοιχο ποσό.

Η λειτουργία πραγματοποιείται σε γύρους. Κάθε γύρος περιλαμβάνει τη διαδικασία

της κατάθεσης προτάσεων και δωρεών και τη διαδικασία της ψηφοφορίας που θα έχει ως αποτέλεσμα τις νικηφόρες προτάσεις.

7.2 Εφαρμογή του συστήματος σε ρεαλιστικά σενάρια

Δυστυχώς, στις μέρες μας, η φιλανθρωπία, με όλο το ευγενές της όραμα και την ιερή της αποστολή, έχει προδοθεί από συλλόγους που καταχρώνται την πίστη του κοινού. Στη σημερινή κοινωνία η αμφισβήτηση που υπάρχει στον συγκεκριμένο τομέα, εξαιτίας της έλλειψης διαφάνειας και της κακοδιαχείρισης κονδυλίων που παρατηρήθηκαν πολλές φορές, έχει προκαλέσει την αποχή του κόσμου.

Ο μεγάλος αριθμός των ανενεργών ΜΚΟ οφείλεται στο ότι οι περισσότερες από αυτές είτε εξαρτώνται από το κράτος για την οικονομική τους στήριξη είτε επιδιώκουν ειδικά συμφέροντα. Η συντριπτική πλειοψηφία από αυτές δεν διαθέτει την κατάλληλη οργάνωση, και τους μηχανισμούς παρακολούθησης και διαφάνειας για την κατανομή των πόρων. Λόγω αυτής της συνεχιζόμενης έλλειψης διαφάνειας μεγάλη μερίδα του πληθυσμού θεωρεί τις ΜΚΟ περιττές για την κοινωνία, και δεν τις εμπιστεύεται είτε σε σχέση με την πραγματοποίηση των σκοπών τους είτε σε σχέση με την επίτευξη των σύγχρονων προκλήσεων.

Για τους λίγους που επιμένουν να θέλουν να βοηθήσουν τίθενται κάποια πολύ βασικά ερωτήματα τα οποία πρέπει να απαντηθουν:
- Ποιους οργανισμούς θα πρέπει να εξετάσω ως υποψήφιους δωρεοδόχους;
- Πώς μπορώ να βεβαιωθώ ότι ένας οργανισμός είναι οικονομικά βιώσιμος;
- Έχει η δωρεά μου αποτελεσματικότητα;
- Πώς μπορώ να ξέρω ότι θα χρησιμοποιήσουν τη δωρεά μου με τον τρόπο που θέλω;

Το πιο σημαντικό είναι η αποκατάσταση της εμπιστοσύνη στο φιλανθρωπικό σύστημα και η εξασφάλιση ότι οι φιλανθρωπικές δωρεές έχουν το μεγαλύτερο δυνατό αποτέλεσμα, πράγμα ιδιαίτερα σημαντικό κατά τη διάρκεια της τρέχουσας κοινωνικής και οικονομικής κατάστασης. Η εμπιστοσύνη προς τις ΜΚΟ θα ανακτηθεί μόνο αν η λειτουργία τους διέπεται πλήρως από διαφανείς όρους και διαδικασίες.

Η συγκεκριμένη υλοποίηση η οποία έχει εκτελεστεί στα πλαίσια μιας διπλωματικής εργασίας είναι ένα παράδειγμα που αποδεικνύει ότι η φιλανθρωπία μπορεί να αποκτήσει ξανά την εμπιστοσύνη του κόσμου. Με την καινοτόμα τεχνολογία του Blockchain και όλα τα πλεονεκτήματα που μπορεί να προσφέρει ένα σύστημα όπως αυτό που εξετάστηκε στην παρούσα εργασία μπορεί να σταθεί στον πραγματικό κόσμο και να λειτουργήσει ιδανικά ικανοποιώντας τις προσδοκίες του κοινού και πείθοντάς τους αμέτοχους ότι αξίζει να συμμετέχουν χωρίς να φοβούνται.

Σήμερα υπάρχει πραγματικός χώρος για την επανένταξη της φιλανθρωπίας στην κοινωνία μας. Με χρήση της τεχνολογίας το πρόσωπο της φιλανθρωπίας μπορεί να αλλάξει,

αποκτώντας μια νέα αξιόπιστη μορφή.

Φυσικά, ενώ υπάρχουν κάποιες αχτίδες ελπίδας, υπάρχει ακόμη δρόμος μέχρι αυτή η καινοτομία να αγκαλιαστεί από την κοινωνία και να αντικαταστήσει το κατεστημένο σύστημα που υπάρχει.

7.3 Τρόποι επέκτασης του συστήματος

Για την εφαρμογή του συστήματος σε ρεαλιστικά σενάρια είναι προφανές ότι χρειάζονται σημαντικές επεκτάσεις οι οποίες δεν θα μπορούσαν να πραγματοποιηθούν στα πλαίσια μιας διπλωματικής εργασίας. Ακολουθούν κάποιες προτάσεις για μελλοντική βελτίωση του συστήματος.

1. Παράταξη του smart contract στο δημόσιο Blockchain
2. Βελτίωση του τρόπου αποθήκευσης και ανάκτησης δεδομένων από το Blockchain ώστε να μην καταναλώνονται τόσοι πόροι και να επιταχυνθούν οι διαδικασίες
3. Αλλαγές στο frontend ώστε να γίνει πιο φιλικό προς τον χρήστη
4. Τα fees που προκύπτουν από τις συναλλαγές να επιβαρύνουν το treasury του DAO και όχι τους χρήστες.
5. Φιλτράρισμα των προτάσεων σχετικά με τον τομέα που αφορούν ώστε να γίνεται πιο εύκολα η επιλογή της επιθυμητής πρότασης σε περίπτωση που οι προτάσεις είναι τόσες πολλές.
6. Να δίνονται δικαιώματα ψήφου, υπό κάποιες προϋποθέσεις, σε κόσμο που δεν μπορεί να προσφέρει οικονομική βοήθεια αλλά τον ενδιαφέρει η συμμετοχή.

7.4 Συμπεράσματα σχετικά με το Blockchain και τα DAOs

7.4.1 Blockchain

Το blockchain αποτελεί μια νέα πρωτοπόρα τεχνολογία αλλά δυστυχώς ξένη για την κοινωνία. Ο κόσμος των κρυπτονομισμάτων είναι σχετικά νέος και ως γνωστόν οι άνθρωποι φοβούνται το καινούριο, το διαφορετικό με αποτέλεσμα το μεγαλύτερο μέρος του πληθυσμού να μην έχει προσπαθήσει καν να κατανοήσει την προσφορά αυτής της καινοτομίας στον κόσμο. Σε συνδυασμό δε με την διάδοση διάφορων απατών που έχουν προκύψει στον συγκεκριμένο τομέα, καθίσταται πολλές φορές δύσκολο να πειστεί η κοινωνία για την αξία του blockchain και πολλοί είναι αυτοί που βρίσκονται εναντίον του.

Είναι αλήθεια ότι η απληστία του γρήγορου κέρδους είναι ιδιαίτερα επικίνδυνη και πολλοί κακόβουλοι τείνουν να εκμεταλλευτούν την άγνοια των πολιτών γύρω από τον τομέα.

Συχνά εξαπατώντας πιο αρχάριους χρήστες καταφέρνουν να καρπωθούν σε κέρδος την απώλεια των νεοεισερχόμενων. Τέτοια γεγονότα όχι μόνο δεν αντιπροσωπεύουν το όραμα αυτής της νέας τεχνολογίας αλλά στηλιτεύουν εξωφρενικά την εικόνα των κρυπτονομισμάτων και του blockchain στον κόσμο και προκαλούν την αντίληψη ότι όλο το σύστημα είναι μια απάτη.

Μοναδική αντιμετώπιση του παρόντος προβλήματος είναι η ενημέρωση του κόσμου και η εκπαίδευση των νεοεισερχόμενων ώστε να αποφύγουν πιθανές παγίδες. Δεν είναι η λειτουργία του blockchain που μπορεί να οδηγήσει κάποιον χρήστη σε μειονεκτική θέση, αλλά η διαχείριση που κάνει ο ίδιος.

Οι επικριτές της τεχνολογίας του Blockchain είτε δεν έχουν γνώση στο θέμα και δεν θέλουν να δώσουν την ευκαιρία σε κάτι καινούριο, είτε εστιάζουν μονομερώς σε αρνητικά συμβάντα και αδυνατούν να αντιληφθούν το γενικότερο καλό που μπορούν να προσφέρουν αυτές οι νέες τεχνολογίες. Κάποια από τα σημαντικότερα πλεονεκτήματα που προσφέρει το blockchain γενικά αλλά και που απορραίουν από την υλοποίηση της εργασίας αναφέρονται ακολούθως:

1. Ο χρήστης διατηρεί την ανωνυμία του καθώς το μόνο στοιχείο που χρειάζεται να δώσει είναι ο αριθμός του λογαριασμού του, που δεν είναι ευαίσθητη πληροφορία και δεν αποκαλύπτει στοιχεία για την ταυτότητά του

2. Εξασφαλίζεται η ακεραιότητα των δεδομένων εφόσον δεν μπορούν ούτε να διαγραφούν, ούτε να παραποιηθούν από κακόβουλους χρήστες.

3. Η δημιουργία των smart contracts είναι απλή και εφόσον σχεδιαστούν σωστά δεν υπάρχει περίπτωση να λειτουργήσουν με μη αναμενόμενο τρόπο αφού δεν μπορεί κάποιος να τα αλλάξει.

4. Ο κώδικας των smart contracts είναι open-source άρα μπορεί ο καθένας να δει πως λειτουργεί και να αποφασίσει αν συμφωνεί με τον τρόπο λειτουργίας του.

5. Μια Web 3 εφαρμογή δεν απαιτεί σύνδεση σε ηλεκτρονικό περιβάλλον τράπεζας για τις συναλλαγές σε αντίθεση με μια Web 2 εφαρμογή απαιτεί εμπιστοσύνη σε ένα κεντρικό σύστημα διαχείρισης. Με το blockchain ο χρήστης συνδέεται στην εφαρμογή με το πορτοφόλι του και μπορεί να αλληλεπιδράσει απευθείας με το smart contract.

6. Δεν μπορεί να απαγορευτεί η χρήση της εφαρμογής σε κανένα χρήστη (για παράδειγμα λόγω της τοποθεσίας που βρίσκεται)

Βεβαίως, παρ'όλα τα πλεονεκτήματα που υπάρχουν στη χρήση της τεχνολογίας του blockchain για τη δημιουργία διάφορων εφαρμογών και συστημάτων, υπάρχουν κάποια σημεία στα οποία ο προγραμματιστής οφείλει να δώσει ιδιαίτερη προσοχή για την καλύτερη και αποδοτικότερη λειτουργία τους.

1. Απαιτείται προσεκτικός σχεδιασμός των δομών δεδομένων που θα χρησιμοποιηθούν για την αποθήκευση των δεδομένων. Μη αποδοτικές δομές δεδομένων μπορούν να οδηγήσουν σε μεγάλες καθυστερήσεις κατά τη λειτουργία του συστήματος.

2. Το κόστος των transaction fees δεν είναι αμελητέο και είναι ανάλογο του όγκου των δεδομένων που αποθηκεύονται, οπότε είναι σημαντικό να αποθηκεύονται στο Blockchain μόνο τα απολύτως απαραίτητα, ενώ γίνεται σαφές ότι το κόστος αυτό δεν μπορεί να έχει μια σταθερή τιμή και λόγω του μεγέθους τους αλλά και ανάλογα με την προτεραιότητα που θέλει ο χρήστης να πραγματοποιήσει τη συναλλαγή του.

3. Παρ'όλο που οι υπολογισμοί στο Blockchain έχουν κόστος είναι αρχή της Τεχνολογίας Λογισμικού ότι δεν πρέπει να γίνονται πολλοί υπολογισμοί στο frontend μιας εφαρμογής γιατί ο κώδικας του είναι ευάλωτος, επομένως χρειάζεται μια ισορροπία μεταξύ των δύο.

Όπως κάθε τεχνολογία έτσι και το blockchain έχει τα υπέρ και τα κατά του. Είναι όμως προφανές ότι αυτή η επαναστατική καινοτομία έχει να προσφέρει πολλά περισσότερα θετικά παρά αρνητικά. Με τη σωστή εκμετάλλευσή της και την ορθή διαχείριση από τους χρήστες, το blockchain έχει τη δυνατότητα να αλλάξει τον κόσμο προς το καλύτερο.

7.4.2 Decentralized Autonomous Organizations

Τα DAOs είναι αποτέλεσμα αξιοποίησης της τεχνολογίας Blockchain.

Με πηγή έμπνευσης την αποκέντρωση των κρυπτονομισμάτων, προέκυψε και η ιδέα της αποκέντρωσης ενός οργανισμού, έννοια της οποίας είναι η κατανεμημένη επίβλεψη και διαχείριση μιας οντότητας παρόμοιας με μια εταιρεία. Η διαφάνεια, η εγκυρότητα και η συλλογικότητα καθιστούν τα DAOs ριζική επανάσταση, καθώς και αναθεώρηση της έννοιας της συνεργασίας.

Ο επίπεδος και πλήρως δημοκρατικός χαρακτήρας ενός Αποκεντρωμένου Αυτόνομου Οργανισμού έρχεται να αντικαταστήσει την ιεραρχική δομή των μέχρι σήμερα οργανισμών ενώ η αυτοματοποίηση στις λειτουργίες του μπορεί να εγγυηθεί τη μη χειραγώγηση και την αξιοκρατία σε ό,τι αφορά τον οργανισμό. Επιπλέον η αμεσότητα και η διακρατικότητα δίνει τη δυνατότητα σε κάθε άνθρωπο από οποιδήποτε σημείο του κόσμου να συμμετέχει.

Πέραν όμως από τον τομέα της φιλανθρωπίας ένα DAO μπορεί να υλοποιηθεί σε οποιοδήποτε άλλο τομέα απαιτεί συνεργασία και συνεπώς εμπιστοσύνη όπως για παράδειγμα επιχειρήσεις, εταιρείες, συλλογικές ιδιοκτησίες, κοινότητες κλπ.

Για όλους τους πιο πάνω λόγους, γίνεται αντιληπτό ότι ένας Αποκεντρωμένος Αυτόνομος Οργανισμός αποτελεί σπουδαία καινοτομία της τεχνολογίας η οποία έχει έρθει για να μείνει, και να επιλύσει τα προβλήματα που μπορεί να προκύπτουν σε ό,τι αφορά μια συνεργασία.

Βιβλιογραφία

[1] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. http://www.bitcoin.org/bitcoin.pdf, 2009.

[2] *Open source P2P money*. https://bitcoin.org/en/.

[3] Andreas M. Antonopoulos. *Mastering bitcoin: Programming The open blockchain*. Stanford Publishing, 2021.

[4] *A quick introduction to bitcoin: How do bitcoin and crypto work?: Get started with Bitcoin.com*. https://www.bitcoin.com/get-started/a-quick-introduction-to-bitcoin/.

[5] *How does bitcoin work?* https://learnmeabitcoin.com/.

[6] *Public key cryptography*. https://www.globalsign.com/en/ssl-information-center/what-is-public-key-cryptography.

[7] Lane Wagner. *Elliptic curve cryptography: A basic introduction*. https://blog.boot.dev/cryptography/elliptic-curve-cryptography/, 2020.

[8] *Blockchain Basics*. https://www.coursera.org/learn/blockchain-basics.

[9] *Blockchain*. https://builtin.com/blockchain.

[10] *Consensus mechanisms*. https://ethereum.org/en/developers/docs/consensus-mechanisms/.

[11] Binance Academy. *Sybil attacks explained*. https://academy.binance.com/en/articles/sybil-attacks-explained, 2023.

[12] https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf.

[13] *ethereum*. https://ethereum.org/en/.

[14] *Smart contracts*. https://www.coursera.org/learn/smarter-contracts.

[15] Murtuza Merchant. *What is an Ethereum Virtual Machine (EVM) and how does it work?* https://cointelegraph.com/news/what-is-an-ethereum-virtual-machine-evm-and-how-does-it-work, 2022.

[16] *Ethereum accounts*. https://ethereum.org/en/developers/docs/accounts/.

[17] *Decentralized Autonomous Organizations (DAOs)*. https://ethereum.org/en/dao/.

[18] Nathan Reiff. *Decentralized Autonomous Organization (DAO): Definition, purpose, and example*. https://www.investopedia.com/tech/what-dao/#toc-what-is-a-decentralized-autonomous-organization-dao, 2022.

[19] Tal Trachtman Alroy. *Children's Leukemia Foundation accused in $9.7 million fraud*. https://edition.cnn.com/2015/07/21/us/new-york-charity-fraud/index.html, 2015.

[20] *Big nonprofit spending: Where the dollars go*. https://onlinegrad.syracuse.edu/blog/big-non-profit-budgets-spending/, 2022.

[21] *Against Malaria Foundation*. https://www.againstmalaria.com/CharityStatus.aspx, journal=The Against Malaria Foundation.

[22] *The Giving Block*. https://thegivingblock.com/.

[23] *Giveth*. https://giveth.io/.

[24] *Endaoment*. https://endaoment.org/.

[25] *The UNICEF CryptoFund*. https://www.unicef.org/innovation/stories/unicef-cryptofund, 2020.

[26] *REMIX Ethereum IDE*. https://remix.ethereum.org/.

[27] *Truffle Suite*. https://trufflesuite.com/.

[28] *Ganache*. https://trufflesuite.com/ganache/.

[29] *Metamask | The crypto wallet for DeFi, Web3 DApps and NFTs*. https://metamask.io/.

[30] *React – a JavaScript library for building user interfaces*.

[31] *Next.js by Vercel - the REACT framework*. https://nextjs.org/.

[32] *Visual Paradigm | The #1 Development Tool Suite*. https://www.visual-paradigm.com/.

[33] *GitHub | Let's build from here*. https://github.com/.

[34] Δ. Κυριάκου. *Αξιοποίηση συστημάτων Blockchain για εκπαίδευση μοντέλων μηχανικής μάθησης*. Διπλωματική εργασία, Εθνικό Μετσόβιο Πολυτεχνείο, 2022.

[35] Χ. Χατζηχριστοφή. *Implementation of Blockchain Application for managing University grades*. Διπλωματική εργασία, Εθνικό Μετσόβιο Πολυτεχνείο, 2022.