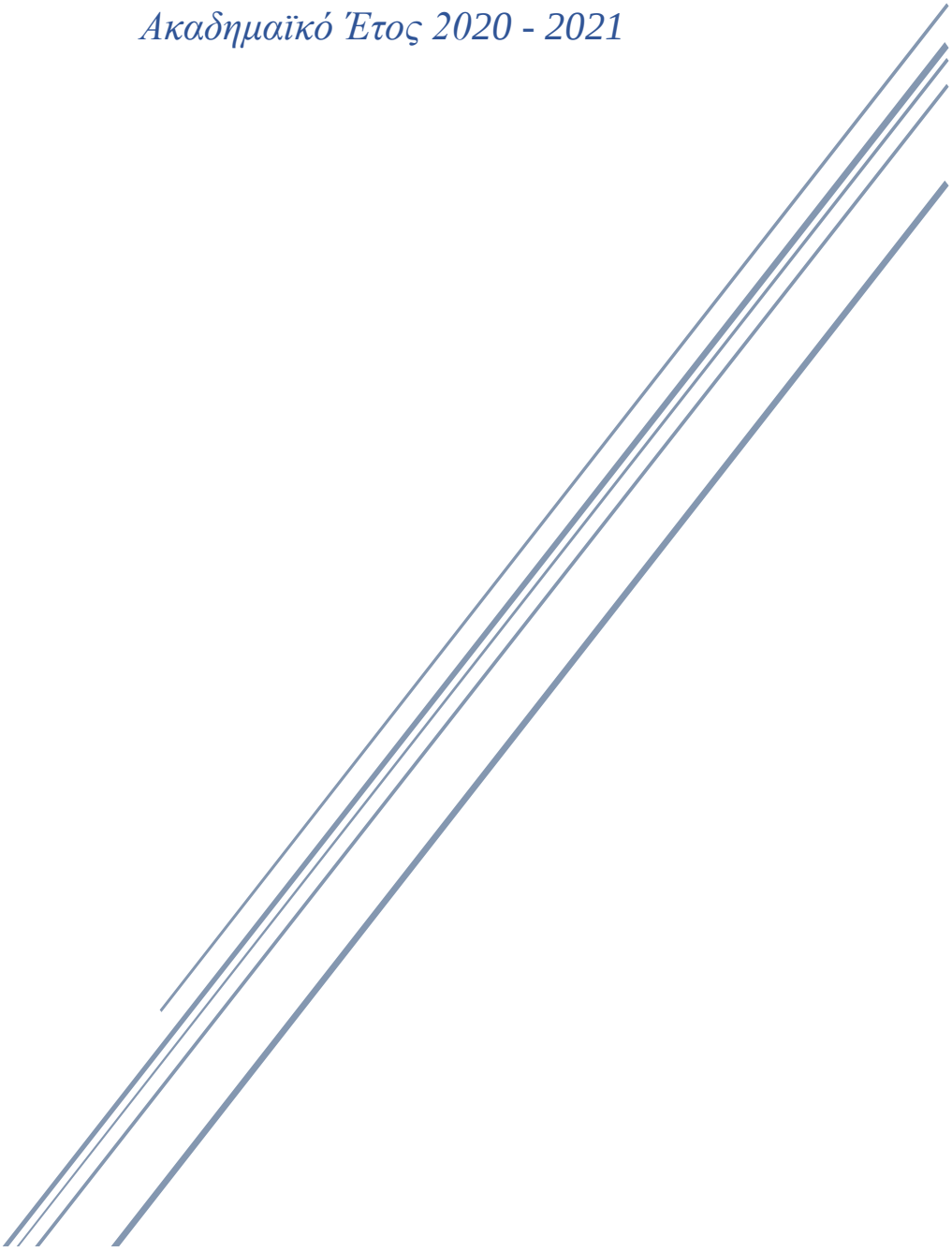
Τεχνολογία Blockchain και Εφαρμογές

Εργασία Μαθήματος

Ακαδημαϊκό Έτος 2020 - 2021



Δημήτρης Ματσαγγάνης, Π17068
Παύλος Ρουμελιώτης, Π17112

Περιεχόμενα

Εκφώνηση Εργασίας

Οδηγίες εκπόνησης εργασίας Blockchain

Η εκπόνηση της εργασίας περιλαμβάνει:

- Την ανάπτυξη ενός πλήρους λειτουργικού Έξυπνου Συμβολαίου (Smart Contract) με τη χρήση του Remix. Χρησιμοποιώντας την πλατφόρμα Remix, οι φοιτητές καλούνται να αναπτύξουν ένα Έξυπνο Συμβόλαιο της αρεσκείας τους, το οποίο θα πρέπει να περιλαμβάνει τουλάχιστον πέντε (5) functions.
- Την καταγραφή (documentation) όλης της διαδικασίας ανάπτυξης (deployment) του Έξυπνου Συμβολαίου και την παρουσίαση των σχετικών screenshots. Στην καταγραφή θα πρέπει να γίνεται και αναφορά στα σχετικά functions που εκτελούνται.

Κεντρική Ιδέα Εφαρμογής

Η εφαρμογή που να αναπτύχθηκε μέσω της Solidity, ως κύριο σκοπό της έχει τη συλλογή και διαχείριση κεφαλαίων που θα γίνονται μέσα από δωρεές, είτε από οργανισμούς, είτε από μεμονωμένα άτομα.

Ειδικότερα, ένας διαχειριστής θα δημιουργεί ένα νέο πρότζεκτ, που σκοπό θα έχει τη συγκέντρωση ενός ποσού για ένα φιλανθρωπικό ίδρυμα. Το ποσό αυτό θα θέτεται ως στόχος του πρότζεκτ και στη περίπτωση που δεν επιτευχθεί μέχρι την ημερομηνία λήξης, θα δίνεται η δυνατότητα επιστροφής χρημάτων σε όποιον από τους συμμετέχοντες το ζητήσει.

Επιπλέον, σε περίπτωση που συμπληρωθεί ή υπερκαλυφθεί το ποσό στόχος, ο διαχειριστής του πρότζεκτ μπορεί να μεταφέρει το ποσό, είτε ολόκληρο, είτε μέρος του στο ίδρυμα για κάποια συγκεκριμένη ενεργεία αφού το θέσει σε ψηφοφορία των συμμετεχόντων, όπου θα χρειάζεται πλειοψηφία (50% + 1). Αυτή η ψηφοφορία σκοπό έχει την επιβεβαίωση ότι τα συγκεντρωμένα χρήματα θα μεταφερθούν σε λογαριασμό του ιδρύματος ή για κάποια άλλη ανάγκη του και θα περιορίζει την πιθανότητα κατάχρησης των χρημάτων από το διαχειριστή, προσφέροντας διαφάνεια στην εφαρμογή.

Τέλος, μέσω της εφαρμογής προσφέρονται οι ακόλουθες δυνατότητες. Πιο συγκεκριμένα, ο κάθε χρήστης θα μπορεί να δει το ποσό που έχει συλλεχθεί μέχρι εκείνη τη χρονική στιγμή, τον αριθμό των συμμετεχόντων, την ημερομηνία λήξης του πρότζεκτ, το ποιος είναι διαχειριστής και την διεύθυνσή του, το ποσό ελάχιστης συμμετοχής στο πρότζεκτ και το ποσό που έχει οριστεί σαν στόχος.

Συναρτήσεις

Σε αυτή την ενότητα θα περιγραφούν εκτενώς οι συναρτήσεις που χρησιμοποιήθηκαν στην υλοποίηση της εφαρμογής. Αρχικά, η έκδοση της Solidity που χρησιμοποιήθηκε είναι η 0.4.25 .

Συνάρτηση contribute()

Η συνάρτηση contribute, είναι η συνάρτηση μέσα από την οποία μπορεί κάποιος χρήστης ή οργανισμός να συμμετάσχει σε ένα πρότζεκτ μέσω δωρεών.

Ειδικότερα, ως απαραίτητες προϋποθέσεις θέτονται το ποσό της δωρεάς να είναι μεγαλύτερο του ελάχιστου ποσού δωρεάς και να μην έχει περάσει η ημερομηνία λήξης του πρότζεκτ. Έπειτα, και αφού πληρούνται οι παραπάνω προϋποθέσεις θα αυξάνεται ο αριθμός των συμμετεχόντων και θα προστίθεται στον πίνακα που συσχετίζει τον κάθε μέτοχο με το ποσό που συνείσφερε στο πρότζεκτ.

Συνάρτηση refund()

Η συνάρτηση refund, είναι η συνάρτηση, η οποία είναι υπεύθυνη για την επιστροφή χρημάτων στους μετέχοντες στη περίπτωση που λήξει το πρότζεκτ και το συγκεντρωμένο ποσό χρημάτων δεν ικανοποιεί τον αρχικό στόχο.

Στη συνέχεια, εφόσον ικανοποιούνται οι παραπάνω προϋποθέσεις θα μειώνεται ο αριθμός των συμμετεχόντων και θα εκμηδενίζεται η συνεισφορά στον πίνακα που συσχετίζει τον κάθε μέτοχο με το ποσό που συνείσφερε στο πρότζεκτ.

Συνάρτηση vote()

Μέσα από αυτή τη συνάρτηση ο κάθε μετέχων έχει τη δυνατότητα ψήφου σε κάποιο ενδεχόμενο αίτημα μεταφοράς χρημάτων από τον διαχειριστή.

Πιο αναλυτικά, ως απαραίτητες προϋποθέσεις θέτονται το συγκεντρωμένο ποσό να είναι μεγαλύτερο του ορισμένου στόχου και ο χρήστης να έχει συμμετάσχει στο πρότζεκτ. Έπειτα, και αφού πληρούνται οι παραπάνω προϋποθέσεις ο χρήστης θα έχει τη δυνατότητα να ψηφίσει.

Συνάρτηση startSpending()

Η παρούσα συνάρτηση είναι υπεύθυνη για τη δημιουργία ενός αιτήματος μεταφοράς χρημάτων από τον διαχειριστή. Το αίτημα αυτό θα τεθεί υπό τη ψηφοφορία των μετόχων και για να ολοκληρωθεί η μεταφορά χρειάζεται την απόλυτη πλειοψηφία των ψήφων (50% +1).

Για να είναι σε θέση ο διαχειριστής να υλοποιήσει ένα αίτημα μεταφοράς θα πρέπει το ποσό να έχει καλύψει ή υπερκαλύψει τον ορισμένο στόχο και ο χρήστης που θέλει να το υλοποιήσει να είναι ο διαχειριστής του πρότζεκτ.

Τέλος, ο διαχειριστής ορίζει την περιγραφή του στόχου, το ποσό και τη διεύθυνση του παραλήπτη των χρημάτων.

Συνάρτηση makePayment()

Συνδικάστηκα με την παραπάνω συνάρτηση, η παρούσα είναι υπεύθυνη για την επικύρωση του αιτήματος του διαχειριστή για τη μεταφορά ενός ποσού με τη διαδικασία που περιγράφεται στην προηγούμενη ενότητα.

Αυτό δύναται να υλοποιηθεί στη περίπτωση που έχει μαζευτεί το ποσό στόχος, ο χρήστης είναι ο διαχειριστής, να έχει την πλειοψηφία των ψήφων και δεν έχει ορισθεί ως ολοκληρωμένη, μέχρι εκείνη τη χρονική στιγμή, η προτεινόμενη μεταφορά.

Συνάρτηση getMoneyRaised()

Η συνάρτηση getMoneyRaised δείχνει σε κάθε χρήστη, ανεξάρτητα από το εάν είναι μέτοχος ή όχι, το συγκεντρωμένο ποσό που θα δωρισθεί στο εκάστοτε ίδρυμα για την παρούσα χρονική στιγμή.

Συνάρτηση getNumOfContributors()

Η συνάρτηση getNumOfContributors, όπως και η προηγούμενη, δείχνει σε κάθε χρήστη, ανεξάρτητα από το εάν είναι μέτοχος ή όχι, τον αριθμό των συμμετεχόντων του πρότζεκτ για την παρούσα χρονική στιγμή.

Συνάρτηση getGoal()

Η συνάρτηση getGoal δείχνει στον κάθε χρήστη το ποσό που έχει ορισθεί ως στόχος από τον διαχειριστή κατά τη δημιουργία του πρότζεκτ.

Συνάρτηση getMinAmount()

Η συνάρτηση getMinAmount δείχνει στον κάθε χρήστη το ποσό που έχει ορισθεί ως ποσό ελάχιστης συμμετοχή στο πρότζεκτ.

Συνάρτηση getEndDate()

Η συνάρτηση getEndDate δείχνει στον κάθε χρήστη την ημερομηνία λήξης του πρότζεκτ. Αυτή την ημερομηνία την έθεσε ο διαχειριστής κατά τη δημιουργία του πρότζεκτ.

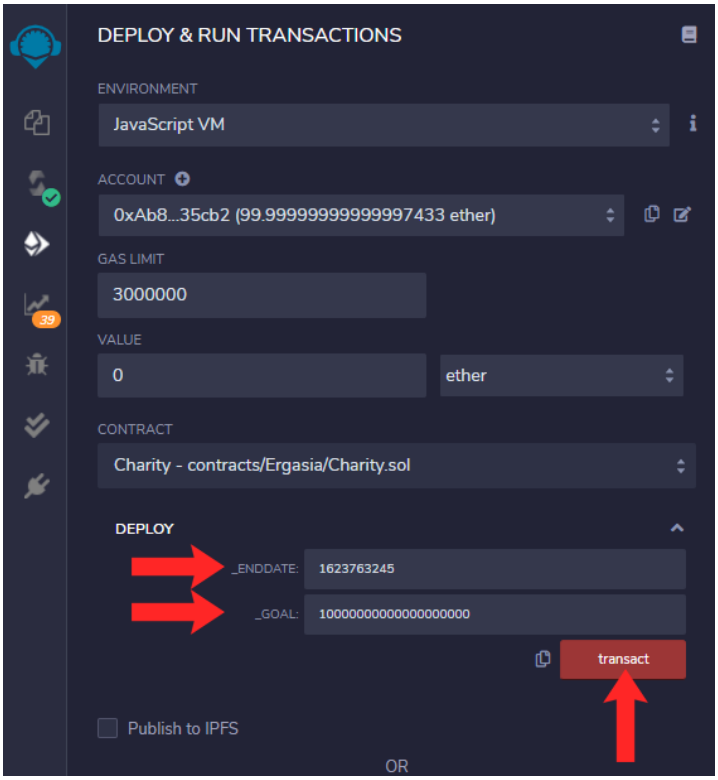
Συνάρτηση getAdminAddress()

Η συνάρτηση getAdminAddress δείχνει στον κάθε χρήστη τη διεύθυνση του διαχειριστή του πρότζεκτ.

Οδηγίες χρήσης

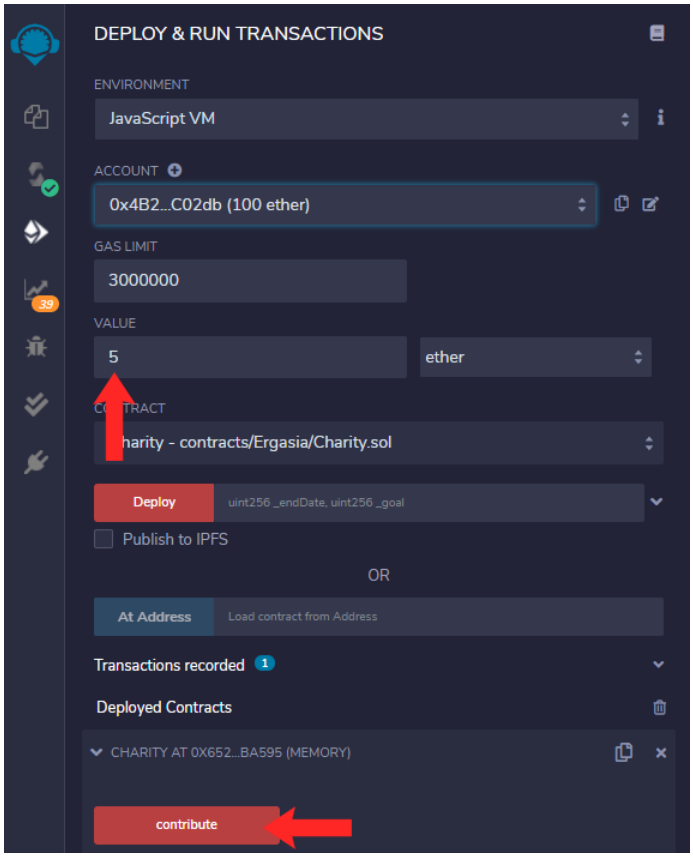
Σε αυτή την ενότητα θα παρουσιαστούν οι οδηγίες χρήσης της εφαρμογής για την πλήρη κατανόηση των κουμπιών της.

Αρχικά ο διαχειριστής δημιουργεί το πρότζεκτ θέτοντας την ημερομηνία λήξης, το ποσό στόχο και πατώντας το κουμπί «transact».



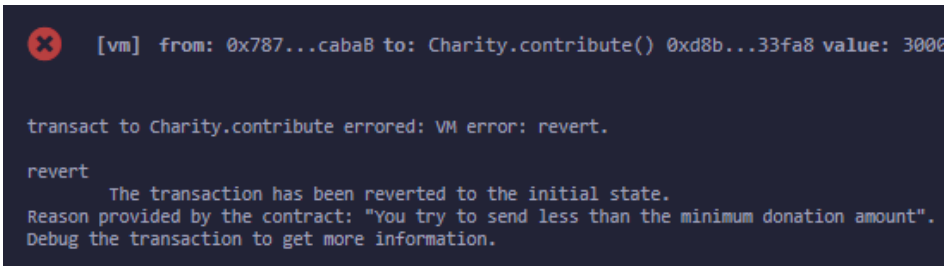
Εικόνα 1 – Δημιουργία πρότζεκτ

Στην συνέχεια οι χρήστες πραγματοποιούν την δωρεά τους εισάγοντας το ποσό και πατώντας το κουμπί «contribute».



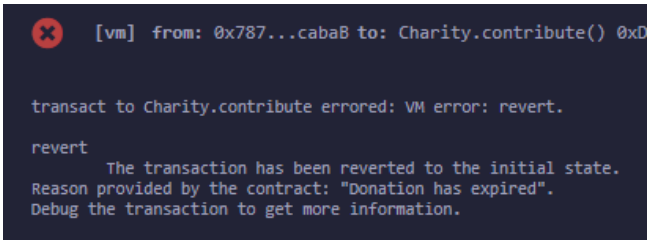
Εικόνα 2 – Πραγματοποίηση δωρεάς

Στην περίπτωση που ο χρήστης εισάγει ποσό μικρότερο από το ελάχιστο επιτρεπτό, δέχεται το παρακάτω μήνυμα.



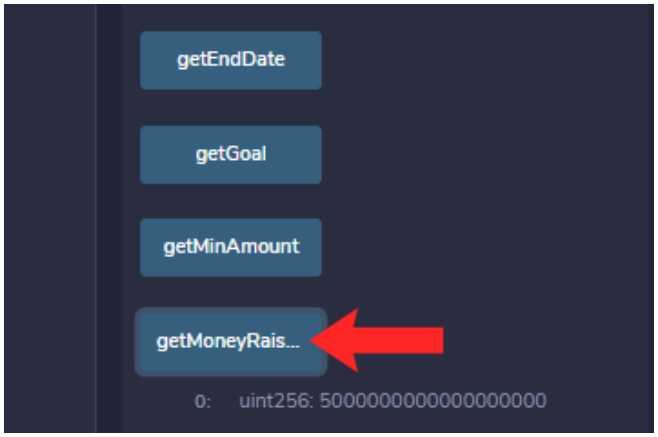
Εικόνα 3 – Ποσό χαμηλότερο από το ελάχιστο

Ενώ αν έχει περάσει η ημερομηνία λήξης, δέχεται αντίστοιχο μήνυμα.



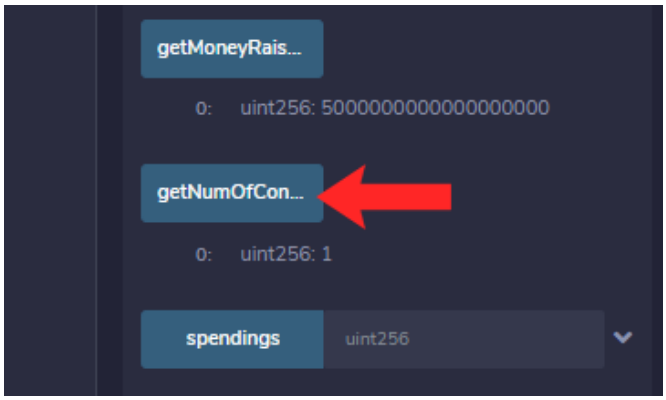
Εικόνα 4 – Το πρότζεκτ έχει λήξει

Για να δει κάποιος χρήστης το ποσό που έχει συλλεχθεί από τις δωρεές, πρέπει να πατήσει το κουμπί «getRaisedMoney».



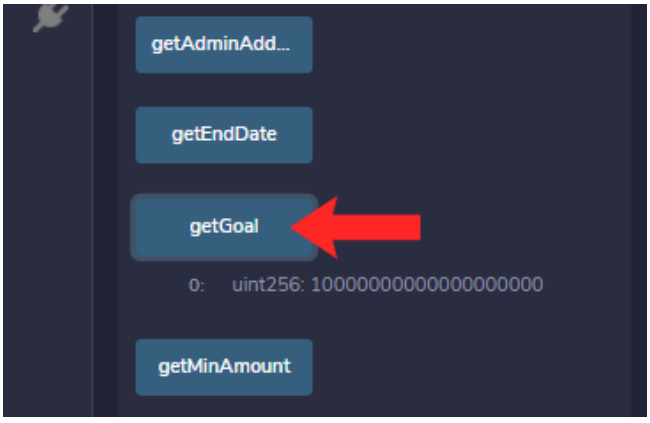
Εικόνα 5 – Συνάρτηση getMoneyRaised

Για να δει ένας χρήστης τον αριθμό των χρηστών που έχουν πραγματοποιήσει δωρεές, πρέπει να πατήσει το κουμπί «getNumOfContributors»



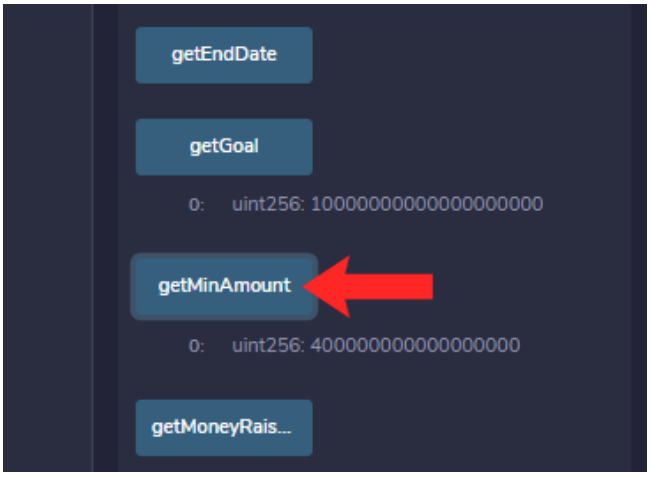
Εικόνα 6 – Συνάρτηση getNumOfContributors

Αν θελήσει ένας χρήστης να δει το ποσό στόχο, πρέπει να πατήσει το κουμπί «getGoal»



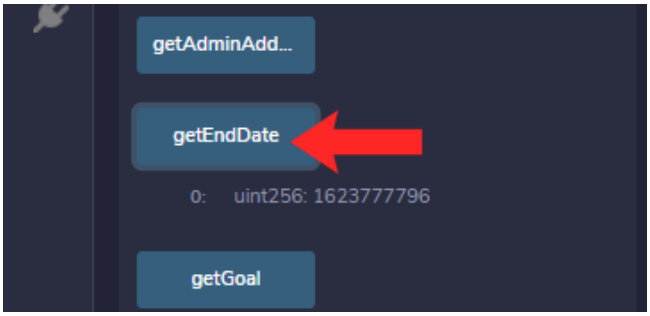
Εικόνα 7 – Συνάρτηση getGoal

Για το ελάχιστο ποσό συμμετοχής, ο χρήστης πρέπει να πατήσει το κουμπί «getMinAmount».



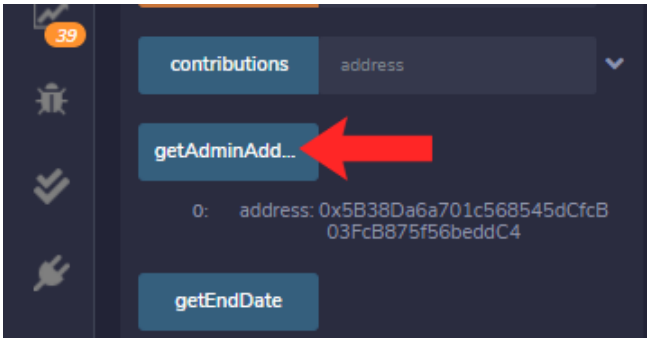
Εικόνα 8 – Συνάρτηση getMinAmount

Στην περίπτωση που ένας χρήστης θέλει να δει κάποιος την ημερομηνία λήξης του πρότζεκτ, πρέπει να πατήσει το κουμπί «getEndDate».



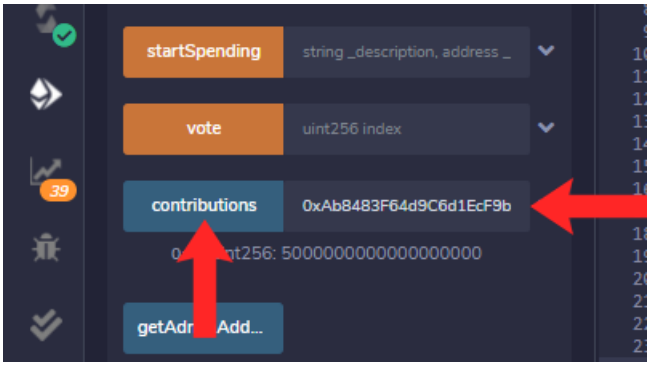
Εικόνα 9 – Συνάρτηση getEndDate

Επίσης για τη διεύθυνση του διαχειριστή του πρότζεκτ, ο χρήστης πρέπει να πατήσει το κουμπί «getAdminAddress».



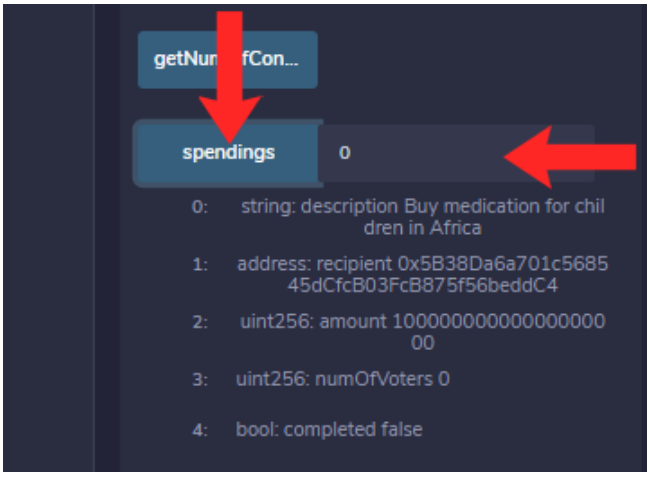
Εικόνα 10 – Συνάρτηση getAdminAddress

Επίσης υπάρχει η δυνατότητα να προβληθεί το συνολικό ποσό που έχει καταβάλει ένας χρήστης. Αυτό γίνεται εισάγοντας την διεύθυνση του χρήστη και πατώντας το κουμπί «contributions».



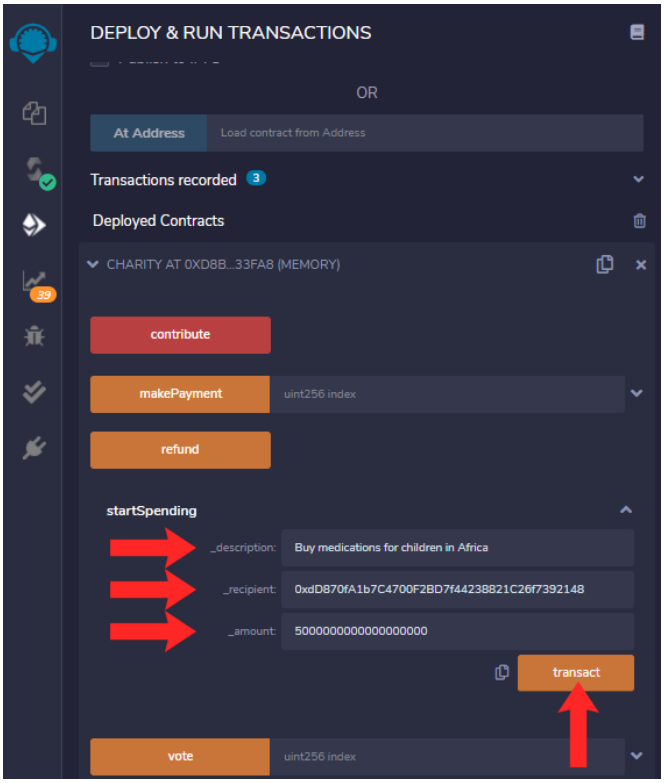
Εικόνα 11 – Contributions mapping

Τέλος, για να λάβει πληροφορίες ένας χρήστης για τα αιτήματα μεταφοράς του διαχειριστή, πρέπει να εισάγει τον αριθμό δείκτη (η αρίθμηση ξεκινά από το 0) και να πατήσει το κουμπί spendings.



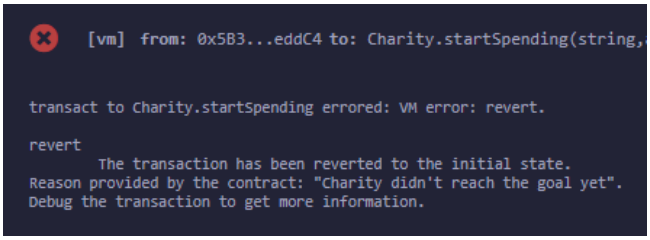
Εικόνα 12 – Λίστα με τα αιτήματα μεταφοράς

Από την στιγμή που καλυφθεί το επιθυμητό ποσό, ο διαχειριστής μπορεί να δημιουργήσει αίτημα για μεταφορά χρημάτων δημιουργώντας έτσι μια ψηφοφορία. Για την επιτυχημένη δημιουργία, ο διαχειριστής πρέπει να συμπληρώσει τα απαραίτητα πεδία και να πατήσει το κουμπί «transact».



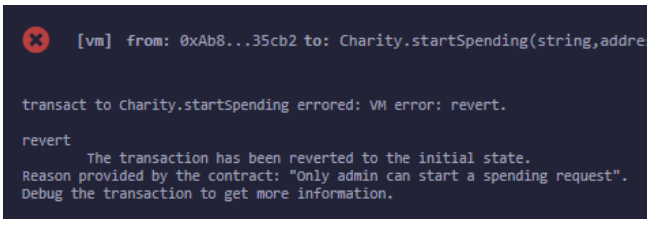
Εικόνα 13 – Αίτημα μεταφοράς χρημάτων

Αν δεν έχει καλυφθεί το ποσό στόχος, εμφανίζεται το παρακάτω μήνυμα.



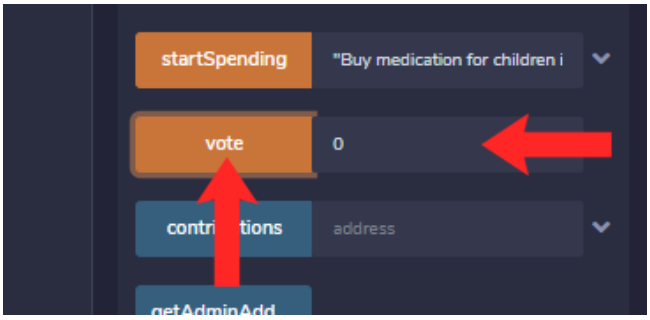
Εικόνα 14 – Δεν έχει καλυφθεί το ποσό στόχος

Αν δεν πραγματοποιηθεί το αίτημα από τον διαχειριστή, εμφανίζεται το αντίστοιχο μήνυμα.



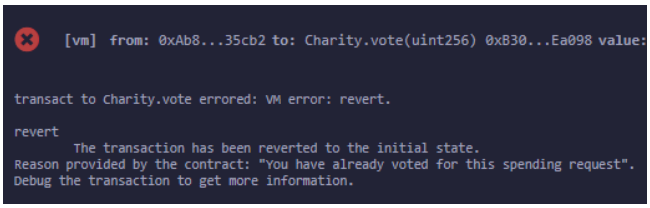
Εικόνα 15 – Μόνο ο διαχειριστής μπορεί να κάνει αίτημα μεταφοράς

Στην συνέχεια οι χρήστες από την μεριά τους μπορούν να ψηφίσουν για το αν συμφωνούν με το αίτημα του διαχειριστή. Για να ψηφίσουν θετικά πρέπει να εισάγουν τον αριθμό δείκτη του αιτήματος (η αρίθμηση ξεκινά από το 0) και να πατήσουν το κουμπί «vote».



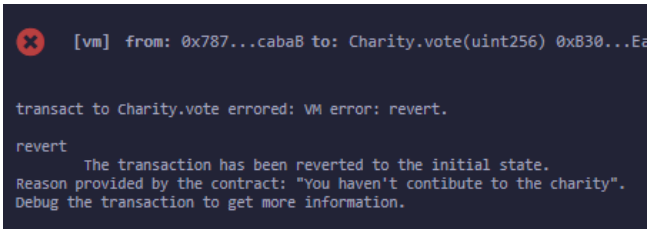
Εικόνα 16 – Θετική ψήφος σε αίτημα μεταφοράς

Αν ο χρήστης έχει ήδη ψηφίσει θετικά, τότε εμφανίζεται το παρακάτω μήνυμα.



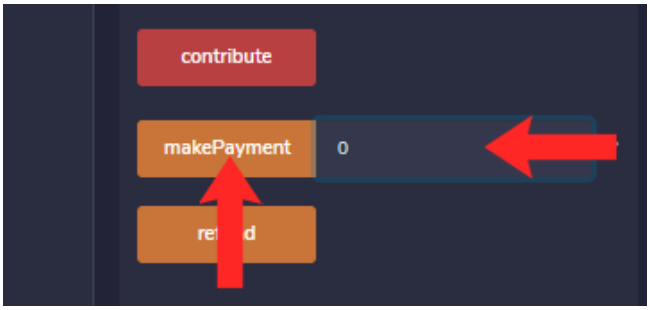
Εικόνα 17 – Ο χρήστης έχει ήδη ψηφίσει

Αν ο χρήστης δεν έχει κάνει κάποια δωρεά πριν ψηφίσει, τότε εμφανίζεται το αντίστοιχο μήνυμα.



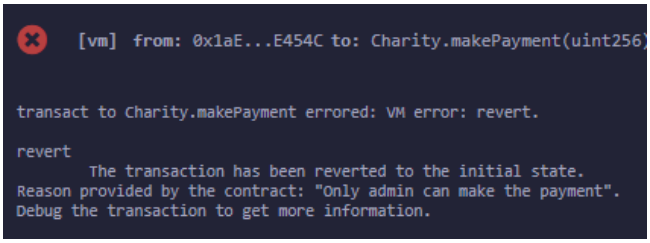
Εικόνα 18 – Ο χρήστης δεν έχει κάνει κάποια δωρεά

Τέλος ο διαχειριστής μπορεί να προχωρήσει στην πραγματοποίηση της μεταφοράς. Για την επίτευξη αυτής της διαδικασίας πρέπει ο διαχειριστής να εισάγει τον αριθμό δείκτη του αιτήματος (η αρίθμηση ξεκινά από το 0) και να πατήσει το κουμπί «makePayment».



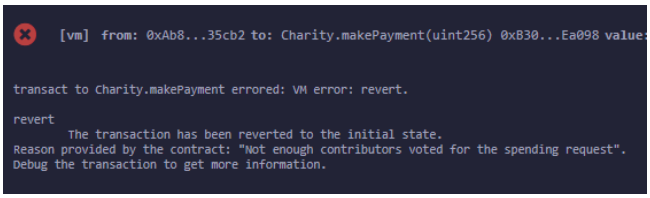
Εικόνα 19 – Πραγματοποίηση μεταφοράς ποσού

Αν δεν πραγματοποιηθεί η μεταφορά από τον διαχειριστή, εμφανίζεται το αντίστοιχο μήνυμα.



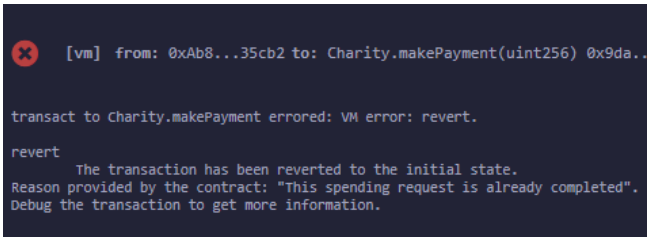
Εικόνα 20 - Μόνο ο διαχειριστής μπορεί να πραγματοποιήσει την μεταφορά

Αν κάτω από το 50% των χρηστών που συμμετέχουν ψήφισε θετικά, τότε εμφανίζεται το παρακάτω μήνυμα.



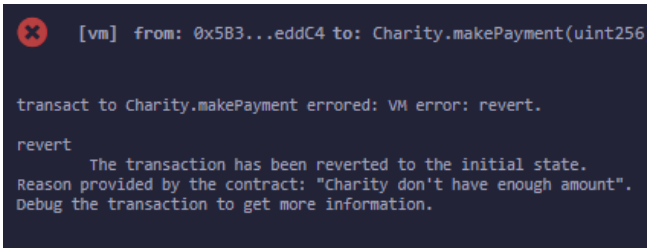
Εικόνα 21 – Δεν έχουν ψηφίσει θετικά αρκετοί χρήστες

Αν το αίτημα μεταφοράς του ποσού έχει ήδη ολοκληρωθεί, τότε εμφανίζεται το αντίστοιχο μήνυμα.



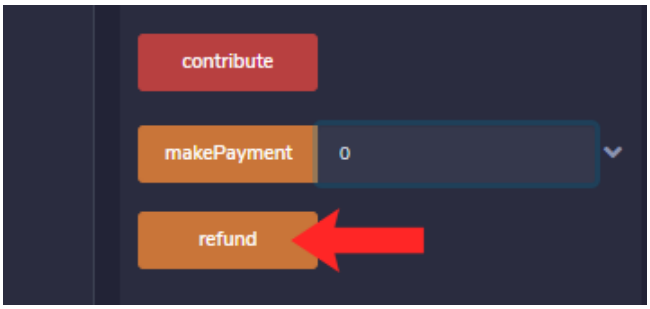
Εικόνα 22 – Η μεταφορά έχει ήδη ολοκληρωθεί

Αν έχει καλυφθεί το ποσό στόχος αλλά το ποσό που ορίζεται στο αίτημα μεταφοράς είναι μεγαλύτερο από το ποσό που έχει συλλεχθεί μέχρι στιγμής από τις δωρεές, εμφανίζεται το παρακάτω μήνυμα.



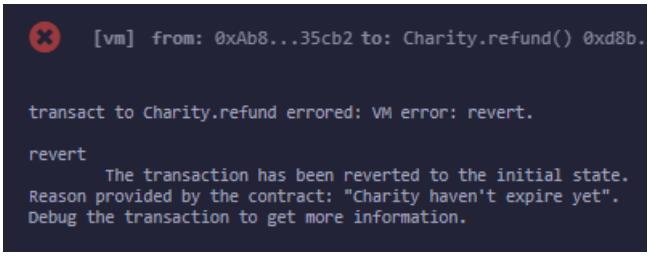
Εικόνα 23 – Το ποσό στο αίτημα είναι μεγαλύτερο από αυτό που έχει συλλεχθεί

Από την στιγμή που λήξει η προθεσμία του πρότζεκτ και δεν έχει καλυφθεί το επιθυμητό ποσό, ο κάθε χρήστης έχει το δικαίωμα επιστροφής των χρημάτων που έχει κάνει δωρεά. Για πραγματοποίηση της επιστροφής χρημάτων, οι χρήστες πρέπει να πατήσουν το κουμπί «refund».



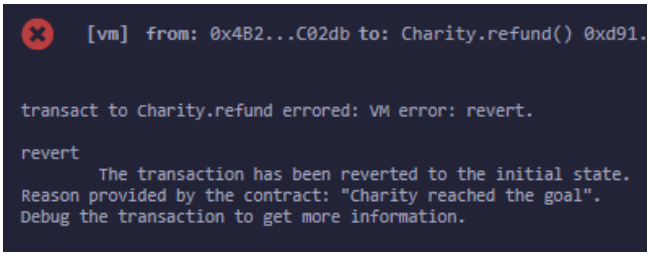
Εικόνα 24 – Επιστροφή χρημάτων χρήστη

Αν δεν έχει λήξει ακόμα η προθεσμία του πρότζεκτ, τότε εμφανίζεται το παρακάτω μήνυμα.



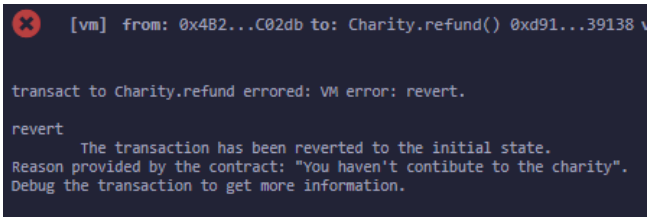
Εικόνα 25 – Η προθεσμία δεν έχει λήξει ακόμα

Αν έχει καλυφθεί το ποσό στόχος, τότε εμφανίζεται το αντίστοιχο μήνυμα.



Εικόνα 26 – Το ποσό στόχος έχει καλυφθεί

Αν ο χρήστης δεν έχει κάνει δωρεά, εμφανίζεται το παρακάτω μήνυμα.



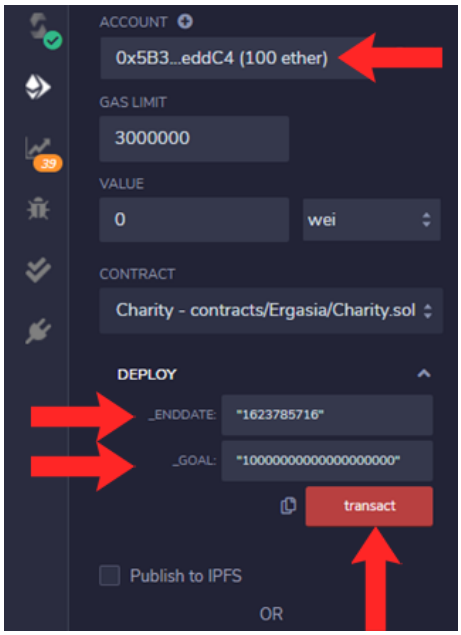
Εικόνα 27 – Ο χρήστης δεν έχει κάνει δωρεά

Σενάρια

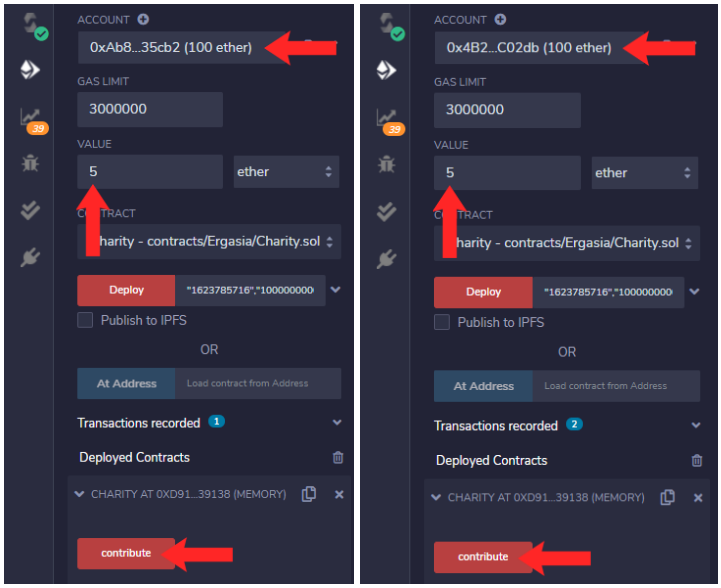
Σε αυτή την ενότητα θα παρουσιαστούν ενδεικτικά σενάρια χρήσης με απώτερο σκοπό να παρουσιαστούν οι δυνατότητες της παρούσας εφαρμογής.

Σενάριο 1

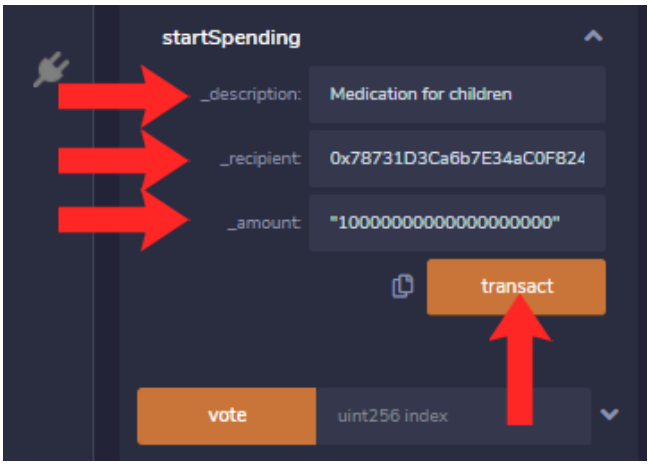
Ο χρήστης με διεύθυνση 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 δημιουργεί ένα πρότζεκτ με ποσό στόχο 10 ether και ημερομηνία λήξης 1623785716 και επομένως γίνεται διαχειριστής του πρότζεκτ.



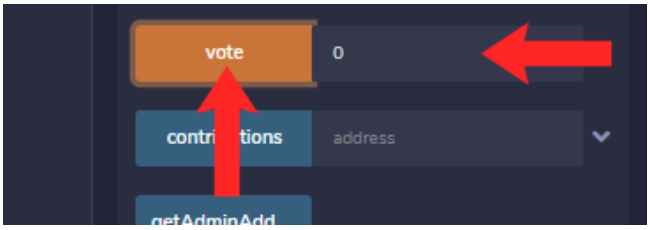
Στην συνέχεια χρήστες με διευθύνσεις 0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2 και 0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db κάνουν δωρεά 5 ether ο καθένας.



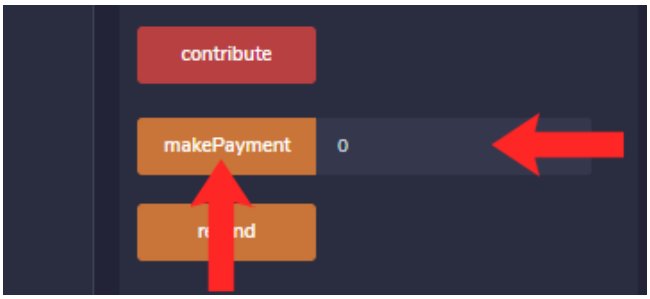
Αφού συμπληρώθηκε το ποσό στόχος που όρισε ο διαχειριστής, εκείνος συμπληρώνει ένα αίτημα μεταφοράς 10 ether για φάρμακα στον χρήστη με διεύθυνση 0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB .



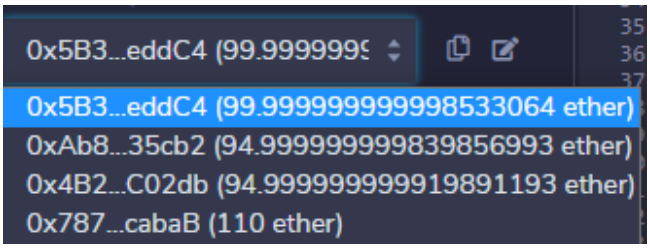
Οι δυο χρήστες ψηφίζουν θετικά στο πρώτο αίτημα του διαχειριστή.



Έπειτα ο διαχειριστής πραγματοποιεί την μεταφορά αποστέλλοντας το ποσό από την διεύθυνση του φιλανθρωπικού ιδρύματος στην διεύθυνση που είχε ορίσει ο διαχειριστής στο αίτημα.

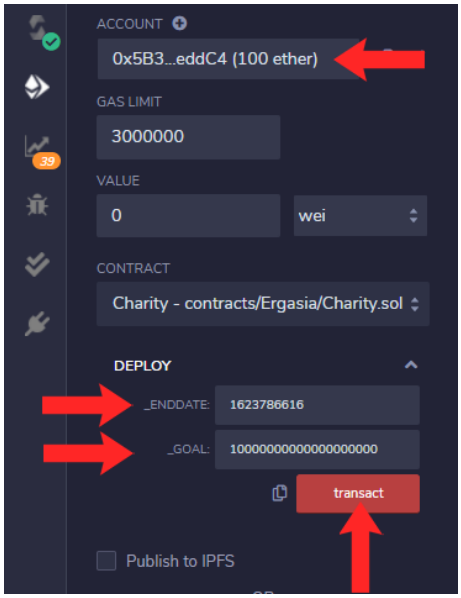


Όπως φαίνεται στην παρακάτω εικόνα ο πρώτος λογαριασμός που είναι του διαχειριστή έχει χάσει μερικά Wei για την δημιουργία του πρότζεκτ. Οι επόμενοι δυο έχουν χάσει 5 ether ο καθένας τα οποία δώρισαν, ενώ ο τέταρτος λογαριασμός παρέλαβε τα 10 ether από το φιλανθρωπικό ίδρυμα.

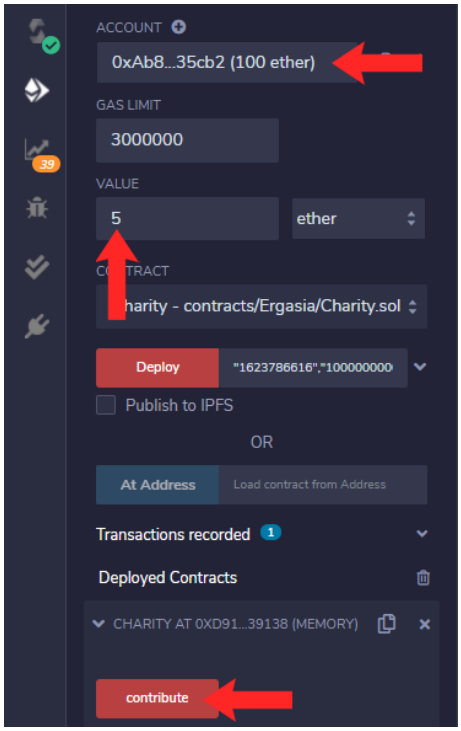


Σενάριο 2

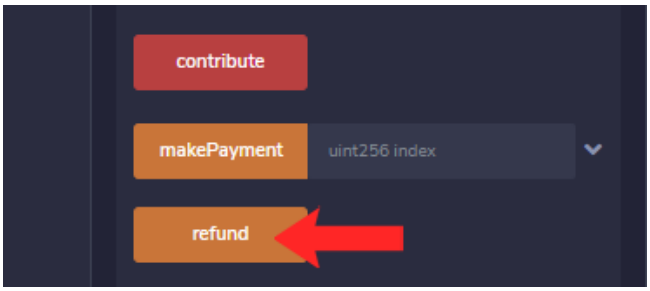
Ο χρήστης με διεύθυνση 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 δημιουργεί ένα πρότζεκτ με ποσό στόχο 10 ether και ημερομηνία λήξης 1623786616 και επομένως γίνεται διαχειριστής του πρότζεκτ.

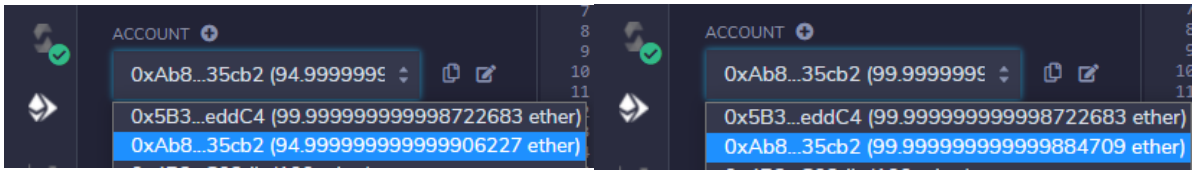


Στην συνέχεια ο χρήστης με διεύθυνση 0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2 κάνει δωρεά 5 ether.



Η προθεσμία του πρότζεκτ έχει πλέον λήξει και το ποσό στόχος δεν έχει καλυφθεί επομένως ο χρήστης με διεύθυνση 0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2 έχει πλέον δικαίωμα για επιστροφή χρημάτων.





Βιβλιογραφία

Σε αυτή την ενότητα παραθέτονται όλες οι πηγές που ωφέλησαν στην δημιουργία της παρούσας εφαρμογής.

1. Documentation Solidity v0.4.25 (τελευταία προσπέλαση 14/06/2021)
2. Documentation Remix (τελευταία προσπέλαση 05/06/2021)
3. Payable Function (τελευταία προσπέλαση 09/06/2021)
4. Payable Function 2 (τελευταία προσπέλαση 10/06/2021)
5. Mapping Address to uint (τελευταία προσπέλαση 14/06/2021)
6. Block Timestamp (τελευταία προσπέλαση 09/06/2021)
7. Return Struct Data (τελευταία προσπέλαση 08/06/2021)