



ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. «ΨΗΦΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΥΠΗΡΕΣΙΕΣ»

ΚΑΤΕΥΘΥΝΣΗ: ΠΡΟΗΓΜΕΝΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΗΛΕΚΤΡΟΝΙΚΗ ΠΛΑΤΦΟΡΜΑ ΓΙΑ ΤΗ
ΒΕΛΤΙΩΣΗ ΤΗΣ ΔΙΑΔΙΚΑΣΙΑΣ ΔΙΕΞΑΓΩΓΗΣ
ΕΡΕΥΝΩΝ ΜΕ ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ
BLOCKCHAIN

Επιβλέποντες Καθηγητές:
Κυριαζής Δημοσθένης, Μενύχτας Ανδρέας

Ιούνιος 2020

Αλεξανδρίδης Αλέξανδρος-Ραφαήλ (ΜΕ1739)
alexrafalexandridis@gmail.com

Πίνακας Περιεχομένων

1.	Εισαγωγή	8
2.	Περιγραφή προβλήματος, εισαγωγή στη λύση του.	9
3.	Επιστημονικό και Τεχνολογικό Υπόβαθρο	11
3.1	Διάγραμμα Gantt	11
3.2	Blockchain	12
3.2.1	Ιστορία του Blockchain	12
3.2.2	Τι είναι το Blockchain.....	13
3.2.3	Πως λειτουργεί το Blockchain	13
3.2.4	Δημόσιο και Ιδιωτικό Blockchain.....	14
3.3	Αποκεντρωμένες Εφαρμογές (Decentralized Applications DApps).....	16
3.3.1	Τι είναι τα DApps	16
3.3.2	Τύποι των DApps.....	17
3.3.3	Διάσημες Εφαρμογές DApps	17
3.3.4	Πλατφόρμες Ανάπτυξης DApps	18
3.4	Ethereum.....	19
3.4.1	Ethereum Accounts.....	20
3.4.2	Ethereum Currency	20
3.4.3	Ethereum Συναλλαγή (Transaction)	21
3.4.4	Ethereum Smart Contract.....	23
4.	Προδιαγραφές Συστήματος	24
4.1	Αρχιτεκτονική Συστήματος.....	24
4.2	Απαιτήσεις Συστήματος	28
4.3	Περιπτώσεις Χρήσης	29
5.	Ανάπτυξη Συστήματος.....	33
5.1	Solidity.....	33
5.2	Deploy Smart Contract στο Infura.....	37
5.3	Node.js & React.js	39
6.	Λειτουργικό Πρωτότυπο	41
7.	Μετρήσεις σε ένα Τυπικό σενάριο χρήσης.....	70
8.	Προοπτικές Επεκτασιμότητας	72

9. Βιβλιογραφία.....	73
----------------------	----

Πίνακας Εικόνων

Εικόνα 1: Διάγραμμα Γκαντ (Gantt).....	11
Εικόνα 2: Δημόσιο vs Ιδιωτικό Blockchain	16
Εικόνα 3: Σχεδιάγραμμα Ethereum	19
Εικόνα 4: Ether to Wei	21
Εικόνα 5: Ethereum.....	24
Εικόνα 6: Solidity.....	24
Εικόνα 7: Solidity Compiler	25
Εικόνα 8: MetaMask	25
Εικόνα 9: Infura	26
Εικόνα 10: Web3.js	26
Εικόνα 11: Διασύνδεση Εργαλείων	27
Εικόνα 12: React.js - Node.js.....	27
Εικόνα 13: Διάγραμμα Δραστηριοτήτων - Επόπτης	30
Εικόνα 14: Διάγραμμα Δραστηριοτήτων - Οργανισμός	31
Εικόνα 15: Διάγραμμα Δραστηριοτήτων - Επενυτής.....	32
Εικόνα 16: Rinkeby API Infura.....	38
Εικόνα 17: Etherscan.....	39
Εικόνα 18: Διάταξη Κώδικα	40
Εικόνα 19: Δημιουργία Έρευνας.....	41
Εικόνα 20: Ανάδραση με MetaMask	42
Εικόνα 21: Αναμονή απόκρισης.....	42
Εικόνα 22: Επαλήθευση Αλληλεπίδρασης	43
Εικόνα 23: Έρευνες	43
Εικόνα 24: Λεπτομέρειες Έρευνας.....	45
Εικόνα 25: Λεπτομέρειες Έρευνας.....	46
Εικόνα 26: Προσθήκη Οργανισμού από Επόπτη	46
Εικόνα 27: Προσθήκη Οργανισμού από Επόπτη	47
Εικόνα 28: Επιβεβαίωση.....	47
Εικόνα 29: Προσθήκη Οργανισμού από Επόπτη	48
Εικόνα 30: Λεπτομέρειες Έρευνας.....	48
Εικόνα 31: Πληροφορίες Activities	49
Εικόνα 32: Προσθήκη Activity.....	49
Εικόνα 33: Επιβεβαίωση.....	50
Εικόνα 34: Προσθήκη Activity	50
Εικόνα 35: Επιβεβαίωση.....	51
Εικόνα 36: Λίστα Με Activities	51
Εικόνα 37: Προσθήκη Ποσοστού Κάλυψης.....	52
Εικόνα 38: Επιβεβαίωση Προσθήκης Ποσοστού Κάλυψης.....	52
Εικόνα 39: Info - Ποσοστό Κάλυψης.....	53
Εικόνα 40: Επιπρόσθετα - Προσθήκη Ποσοστού Κάλυψης	53

Εικόνα 41: Ένδειξη Ποσοστού Κάλυψης.....	54
Εικόνα 42:Εμφάνιση Ποσοστού και Διαθέσιμου Ποσού	54
Εικόνα 43: Ένδειξη Ποσοστού Κάλυψης.....	55
Εικόνα 44: Πλήρης Εισαγωγή Activities.....	56
Εικόνα 45: Δήλωση Συμμετοχής Οργανισμού	56
Εικόνα 46: Επιβεβαίωση Εισαγωγής	57
Εικόνα 47: Δήλωση Συμμετοχής 2ου Οργανισμού.....	57
Εικόνα 48: Επιβεβαίωση.....	58
Εικόνα 49: Προβολή Συμμετεχόντων Οργανισμών	58
Εικόνα 50:Λεπτομέρειες Έρευνας	59
Εικόνα 51:Διαδικασία Επένδυσης από τον Επενδυτή.....	59
Εικόνα 52:Επιβεβαίωση Επένδυσης.....	60
Εικόνα 53:Λίστα με τους Επενδυτές.....	60
Εικόνα 54:Κατάσταση Δραστηριοτήτων.....	61
Εικόνα 55:Πληρωμή Πωλητή.....	61
Εικόνα 56:Κατάσταση Activity	62
Εικόνα 57:Πληρωμή Πωλητή.....	62
Εικόνα 58:Κατάσταση Activity	63
Εικόνα 59:Έλεγχος Activity.....	63
Εικόνα 60: Κατάσταση Activity	64
Εικόνα 61:Αλλαγή Κατάστασης από Επόπτη.....	64
Εικόνα 62:Επιβεβαίωση αλλαγής κατάστασης	65
Εικόνα 63: Πληροφορίες Activity.....	65
Εικόνα 64: Πληροφορίες Activity.....	66
Εικόνα 65: Πληροφορίες Πληρωμών.....	66
Εικόνα 66:Πληροφορίες Πληρωμών.....	67
Εικόνα 67:Προβολή κατάσταση Έρευνας.....	67
Εικόνα 68: Διαδικασία Αποπληρωμής.....	68
Εικόνα 69:Επιβεβαίωση Αποπληρωμής.....	68
Εικόνα 70: Τελικά κατάσταση Έρευνας.....	69
Εικόνα 71: Αποπληρωμή Απενεργοποιημένη	69

Ένα μεγάλο ευχαριστώ από καρδιάς σε όλη την οικογένειά μου και τους φίλους μου που με στήριξαν όλη αυτή την περίοδο! Επιπλέον θα ήθελα να ευχαριστήσω βαθύτατα τους καθηγητές μου κ. Ανδρέα Μενύχτα και κ. Δημοσθένη Κυριαζή για τις κατευθυντήριες γραμμές που μου έδωσαν και την υπομονή τους στην προσπάθειά μου να υλοποιήσω την συγκεκριμένη εργασία.

1. Εισαγωγή

Τα τελευταία χρόνια η ραγδαία ανάπτυξη της τεχνολογίας έχει δημιουργήσει ανάγκες που κάποτε τις θεωρούσαμε ανύπαρκτες. Η ανάπτυξη των υπολογιστών, η εισαγωγή τους σε κάθε χώρο εργασίας, διασκέδασης και γνώσης καθώς και η είσοδος του διαδικτύου έχουν ως αποτέλεσμα την εισαγωγή της τεχνολογίας στην καθημερινότητά μας.

Μέσα σε αυτή την ραγδαία εξέλιξη τα τελευταία χρόνια έχει αναπτυχθεί μία πραγματικά επαναστατική τεχνολογία. Η τεχνολογία του Blockchain. Όλοι έχουν ακούσει για τα ψηφιακά νομίσματα, όπως το Bitcoin. Πολλοί λιγότεροι όμως γνωρίζουν την τεχνολογία πάνω στην οποία βασίζονται, την τεχνολογία του Blockchain. Πρόκειται για μια τεχνολογία που επιτρέπει σε άτομα, επιχειρήσεις και οργανισμούς να πραγματοποιούν συναλλαγές μεταξύ τους χωρίς ενδιάμεσους. Αυτό επιτυγχάνεται μέσω μιας διαδικτυακής υποδομής, η οποία επιτρέπει την αποθήκευση πληροφοριών με τέτοιο τρόπο ώστε κανένα από τα συναλλασσόμενα μέρη να μην μπορεί να αμφισβητήσει, τροποποιήσει ή διαγράψει πληροφορίες που έχουν καταγραφεί σε ένα blockchain.

Ακούγοντας το σε πρώτη φάση φαίνεται αρκετά θεωρητικό. Εμβαθύνοντας όμως στην ουσία και στην υλοποίηση της τεχνολογίας κατανοούμε πως στην πραγματικότητα μας επιτρέπει να περάσουμε στην επόμενη φάση του Internet. Το Internet μετασχηματίζεται πλέον εκτός από ένα δίκτυο ανταλλαγής πληροφοριών και σε ένα δίκτυο ανταλλαγής χρηματικών αξιών. Στην πραγματικότητα, το blockchain επιτυγχάνει τη μετάβαση μίας από τις σημαντικότερες λειτουργίες του εμπορίου (αυτή της εμπιστοσύνης) από τους οργανισμούς στο διαδίκτυο.

Φανταστείτε πόσο άλλαξε τον κόσμο μας το διαδίκτυο τα τελευταία χρόνια και θα αρχίσετε να κατανοείται του πόσο περισσότερο μπορούν να αλλάξουν τα πράγματα αν μπορούμε στο μέλλον να χρησιμοποιούμε ψηφιακό χρήμα και να ανταλλάσσουμε κάθε είδους αξία χωρίς τους ενδιάμεσους που χρησιμοποιούμε σήμερα, όπως οι τράπεζες.

Πολλές κεντρικές τράπεζες προσανατολίζονται στη δημιουργία ψηφιακών νομισμάτων, εντός και εκτός τραπεζικού χώρου. Επιπροσθέτως αναπτύσσεται ως σημαντική καινοτομία σε τομείς όπως η υγεία, το εμπόριο, οι ασφάλειες, η ενέργεια, οι μεταφορές και αλλού.

Τα ψηφιακά νομίσματα και η τεχνολογία του Blockchain έχουν εισέλθει για τα καλά στην ζωή μας. Αποτέλεσμα αυτού είναι πολλές διαδικασίες που πραγματοποιούμε στην καθημερινότητάς μας να μπορούν να προσομοιώνονται πάνω σε αυτή την τεχνολογία προσφέροντάς μας ασφάλεια, ανωνυμία (εάν αυτή είναι απαραίτητη) και μη αποποίηση των πράξεων-συναλλαγών που έχουν διαπραχθεί.

2. Περιγραφή προβλήματος, εισαγωγή στη λύση του.

Πολλές έρευνες εξελίσσονται στην σημερινή εποχή. Έρευνες σε διάφορους κλάδους όπως στον κλάδο της οικονομίας, στον κλάδο της ιατρικής, στον κλάδο της τεχνολογία κ.α. Περισσότεροι αύξηση την δεδομένη στιγμή στην διαδικασία περάτωσης μιας έρευνας έχει εμφανιστεί στο κλάδο της υγείας. Λόγω του Covid-19 πολλές έρευνες ανά τον κόσμο βρίσκονται σε εξέλιξη ώστε να βρεθεί το φάρμακο και μέτρα αντιμετώπισης του Ιού.

Κατά την διεξαγωγή μιας έρευνας λαμβάνουν χώρα τρεις διαφορετικές κύριες ομάδες. Μπορούμε να τις ορίσουμε ως εξής:

- Οργανισμοί που πραγματοποιούν την Έρευνα: Στην ομάδα αυτή μπορούμε να κατατάξουμε όλες τις ομάδες ή τα άτομα που θα αποτελέσουν την ερευνητική ομάδα. Ο κάθε ένας έχει το δικό του ρόλο μέσα στο Project με αποτέλεσμα να χρειάζεται ένα χρηματικό ποσό ώστε να μπορέσει να αγοράσει και να χρησιμοποιήσει τον κατάλληλο εξοπλισμό για την περάτωση του έργου του.
- Επενδυτές που επενδύουν στην Έρευνα: Για να μπορέσει να διεξαχθεί μια έρευνα θα πρέπει να επενδύσουν κάποιοι οργανισμοί ή κάποια άτομα ένα χρηματικό ποσό. Ποσό το οποίο θα χρησιμοποιήσουν οι Οργανισμοί για την διεξαγωγή της έρευνας και μόνο γι' αυτό. Σκοπός των επενδυτών είναι είτε η πραγμάτωση της έρευνας για το κοινό καλό είτε να έχουν κάποιο κέρδος μετά την ολοκλήρωση της έρευνας με το αποτέλεσμα που θα παραχθεί.
- Επόπτης: Κατά την διαδικασία περάτωσης της έρευνας υπάρχει ένα άτομο το οποίο ασχολείται με τα διαδικαστικά της έρευνας, όπως εάν τα στάδιά της ολοκληρώνονται επιτυχώς, εάν τα χρήματα ξοδεύονται από τους οργανισμούς όπως έχει οριστεί κ.α.

Ο τρόπος λοιπόν που διεξάγεται στην σημερινή εποχή μια έρευνα είναι η Δημιουργία της έρευνας. Στην συνέχεια η κατάθεση των χρημάτων από τους Επενδυτές σε κάποιο τραπεζικό λογαριασμό. Η έναρξη της έρευνας σηματοδοτεί το δικαίωμα στους οργανισμούς να λάβουν τα χρήματα και να τα ξοδέψουν με υποτιθέμενο σκοπό την υλοποίηση των διαδικασιών.

Το πρόβλημα το οποίο δημιουργείται στην δεδομένη κατάσταση είναι η ανεξέλεγκτη χρήση των χρημάτων που έχουν καταβάλει οι Επενδυτές χωρίς την ύπαρξη ενός αδιάβλητου και ασφαλούς συστήματος καταγραφής συναλλαγών και διαδικασιών.

Με την παρούσας εργασία θα δημιουργήσουμε μία ηλεκτρονική πλατφόρμα με σκοπό την βελτίωση της διαδικασίας διεξαγωγής ερευνών με χρήση τεχνολογιών Blockchain.

Το σύστημα αυτό απευθύνεται:

- Σε όσους οργανισμούς θέλουν να δημιουργήσουν μια έρευνα ένα Project και θέλουν να παρέχουν την διαφάνεια και την ασφάλεια που πρέπει να παρέχετε πραγματοποιώντας ένα τέτοιο έργο.

- Μπορεί να χρησιμοποιηθεί από τους Επόπτες των ερευνών ώστε να τους διευκολύνει στο έργο του και να τους βοηθήσει κάνοντας ευκολότερο τον έλεγχο των διαδικασιών.
- Τέλος μπορεί να ζητηθεί η χρήση του από τους Επενδυτές ώστε να νιώθουν ασφάλεια για την επένδυσή τους.

Το συγκεκριμένο σύστημα μπορεί να χρησιμοποιηθεί σε όλους τους κλάδους είτε δημόσιους είτε ιδιωτικούς χωρίς περιορισμούς. Θα δούμε πως το στήσιμο του συγκεκριμένου συστήματος γίνεται εύκολα.

3. Επιστημονικό και Τεχνολογικό Υπόβαθρο

3.1 Διάγραμμα Gantt

Για την διεξαγωγή μιας έρευνας συνήθως γίνεται χρήση του διαγράμματος Γκαντ (Gantt chart). Το διάγραμμα Gantt είναι ένα οριζόντιο ιστόγραμμα που αναπτύχθηκε ως εργαλείο ελέγχου παραγωγής το 1917 από τον Henry Gantt. Το διάγραμμα Gantt παρέχει μια γραφική απεικόνιση ενός έργου που βοηθά το σχεδιασμό, τον συντονισμό και την εξειδίκευση των επιμέρους εργασιών μέσα σε ένα έργο. Η βασικότερη χρήση τους είναι η παρακολούθηση της προόδου ενός έργου. Μέσα από αυτά μπορούν να ελεγχθούν όλες οι δραστηριότητες οποιαδήποτε στιγμή και να λάβουν χώρα τυχόν απαραίτητες ενέργειες που μπορεί να χρειαστούν να γίνουν αν κάποια δραστηριότητα ξεφύγει από τα χρονικά της πλαίσια. Στην παρακάτω εικόνα εμφανίζεται ένα παράδειγμα υλοποίησης προγραμματισμού με την βοήθεια του διαγράμματος Gantt.

	Εβδομάδες									
Εργασία	1	2	3	4	5	6	7	8	9	10
Activity 1	■									
Activity 2		■								
Activity 3			■	■	■					
Activity 4				■	■	■				
Activity 5					■	■				
Activity 6						■	■	■	■	
Activity 7							■	■	■	
Activity 8								■	■	
Activity 9										■

Εικόνα 1: Διάγραμμα Γκαντ (Gantt)

Τα πλεονεκτήματα από την χρήση της συγκεκριμένης τεχνικής είναι η σαφής απεικόνιση της χρονικής διάρκειας και της αλληλουχίας των δράσεων, η εύκολη και γρήγορη κατασκευή του, αλλά και η ευκολία με την οποία μπορεί να κατανοήσει ακόμα και κάποιο μη εξειδικευμένο άτομο τις πληροφορίες που το διάγραμμα παρέχει στον χρήστη του.

Επενδυτές λοιπόν επενδύουν τα χρήματά του σε τέτοιες έρευνες με σκοπό την εξάλειψη του ιού και την δημιουργία ενός ασφαλέστερου μέλλοντος. Ποιος όμως εγγυάται στους επενδυτές ότι τα χρήματα που επενδύουν στις έρευνες πηγαίνουν εκεί που πρέπει και την χρονική στιγμή που

πρέπει; Μπορεί ο χρονικός περιορισμός να είναι καταγεγραμμένος στο διάγραμμα Gantt αλλά αυτό δεν αποτελεί απόδειξη της σωστής διεξαγωγής των δραστηριοτήτων της έρευνας. Επίσης δεν παρέχεται κάποια πληροφορία για τα ποσά που θα δαπανηθούν σε κάθε δραστηριότητα.

3.2 Blockchain

Ξεκινώντας να ξεκαθαρίσουμε πως δεν θα πρέπει να συγχέουμε την τεχνολογία Blockchain με το Bitcoin, πράγμα που γίνεται ευρέως. Πρόκειται για δύο εντελώς διαφορετικά πράγματα. Το σημαντικότερο είναι πως κανείς δεν μπορεί να γνωρίζει το μέλλον του Bitcoin και των υπόλοιπων κρυπτονομισμάτων, όμως εκτιμάται πως η τεχνολογία του blockchain θα φέρει δραστικές αλλαγές σε πολλούς κλάδους.

3.2.1 Ιστορία του Blockchain

Η ιδέα πίσω από την τεχνολογία blockchain περιγράφηκε ήδη από το 1991, όταν οι ερευνητές Stuart Haber και W. Scott Stornetta εισήγαγαν μια υπολογιστικά πρακτική λύση για χρονική σφράγιση ψηφιακών εγγράφων, ώστε να μην μπορούν να καθυστερήσουν ή να αλλοιωθούν.

Το σύστημα χρησιμοποίησε μια κρυπτογραφημένη ασφαλής αλυσίδα-block (blockchain) για να αποθηκεύσει τα χρονικά σφραγισμένα έγγραφα. Το 1992 τα «Merkle tree» ενσωματώθηκαν στο σχεδιασμό, καθιστώντας το πιο αποτελεσματικό επιτρέποντας τη συλλογή πολλών εγγράφων σε ένα block. Ωστόσο, αυτή η τεχνολογία δεν χρησιμοποιήθηκε.

Το 2004, ο Hal Finney (Harold Thomas Finney II) εισήγαγε ένα σύστημα που ονομάζεται RPoW (Reusable Proof Of Work). Το σύστημα λειτούργησε λαμβάνοντας ένα μη ανταλλάξιμο αποδεικτικό διακριτικό εργασίας με βάση το Hashcash. Σε αντάλλαγμα δημιούργησε ένα διακριτικό με υπογραφή RSA που θα μπορούσε στη συνέχεια να μεταφερθεί από άτομο σε άτομο.

Η RPoW έλυσε το πρόβλημα των διπλών δαπανών διατηρώντας την κατοχή των διακριτικών που είναι καταχωρημένα σε έναν αξιόπιστο διακομιστή που έχει σχεδιαστεί για να επιτρέπει στους χρήστες σε όλο τον κόσμο να επαληθεύουν την ορθότητα και την ακεραιότητά του σε πραγματικό χρόνο.

Το RPoW μπορεί να θεωρηθεί ως ένα πρώιμο πρωτότυπο και ένα σημαντικό πρώτο βήμα στην ιστορία των κρυπτονομισμάτων.

Στα τέλη του 2008 δημιουργήθηκε ένα σύστημα που εισήγαγε ένα αποκεντρωμένο σύστημα ηλεκτρονικών μετρητών peer-to-peer το οποίο ονομάζεται Bitcoin. Δημοσιεύτηκε σε μια λίστα αλληλογραφίας κρυπτογράφησης από ένα άτομο ή ομάδα χρησιμοποιώντας το ψευδώνυμο Satoshi Nakamoto.

Με βάση τον αλγόριθμο απόδειξης εργασίας Hashcash, αλλά αντί να χρησιμοποιεί μια αξιόπιστη υπολογιστική λειτουργία όπως το RPoW, η προστασία διπλών δαπανών στο Bitcoin παρέχεται

από ένα αποκεντρωμένο πρωτόκολλο peer-to-peer για παρακολούθηση και επαλήθευση των συναλλαγών. Με λίγα λόγια, τα Bitcoin "εξ ορύσσονται" για μια ανταμοιβή χρησιμοποιώντας τον μηχανισμό απόδειξης εργασίας από μεμονωμένους εξ ορυκτές και στη συνέχεια επαληθεύονται από τους αποκεντρωμένους κόμβους στο δίκτυο.

Στις 3 Ιανουαρίου 2009 δημιουργήθηκε το πρώτο block Bitcoin το οποίο εξόρυξε ο Satoshi Nakamoto με ανταμοιβή 50 Bitcoin. Ο πρώτος παραλήπτης του Bitcoin ήταν ο Hal Finney, έλαβε 10 Bitcoin από την Satoshi Nakamoto στην πρώτη συναλλαγή Bitcoin στον κόσμο στις 12 Ιανουαρίου 2009.

3.2.2 Τι είναι το Blockchain

Σε βασικό επίπεδο, το blockchain είναι κυριολεκτικά απλά μια «αλυσίδα block», αλλά όχι με την παραδοσιακή έννοια αυτών των λέξεων. Όταν λέμε τις λέξεις «block» και «αλυσίδα» σε αυτό το πλαίσιο, στην πραγματικότητα μιλάμε για ψηφιακές πληροφορίες («block») που είναι αποθηκευμένες σε μια δημόσια βάση δεδομένων («αλυσίδα»).

Τα «block» στο blockchain αποτελούνται από ψηφιακά κομμάτια πληροφοριών.

Συγκεκριμένα, στο Block αποθηκεύονται τρεις βασικές πληροφορίες:

- Πληροφορίες σχετικά με συναλλαγές, όπως την ημερομηνία, την ώρα και το ποσό του της συναλλαγής.
- Πληροφορίες σχετικά με το ποιος συμμετέχει σε συναλλαγές: Αντί να γίνεται χρήση του πραγματικού ονόματος, η αγορά καταγράφεται χωρίς καμία πληροφορία αναγνώρισης χρησιμοποιώντας μια μοναδική «ψηφιακή υπογραφή» όπως ένα όνομα χρήστη το οποίο είναι μοναδικό και αντιπροσωπεύει μόνο ένα άτομο – συναλλαγή – διεπαφή.
- Πληροφορίες που τις διακρίνουν από άλλα block|: Κάθε block αποθηκεύει έναν μοναδικό κωδικό που ονομάζεται «hash» που μας επιτρέπει να το ξεχωρίζουμε από κάθε άλλο block. Το hash δημιουργείται με βάση το περιεχόμενα του block. Εάν αλλάξει έστω ένα στοιχείο του block τότε αλλάζει και ο αναγνωριστικός αριθμός του block (Hash).

Στο σημείο αυτό αξίζει να σημειώσουμε πως σε ένα μόνο block στο blockchain μπορεί πραγματικά να αποθηκευθεί έως και 1 MB δεδομένων. Ανάλογα με το μέγεθος των συναλλαγών, αυτό σημαίνει ότι ένα μόνο block μπορεί να φιλοξενήσει μερικές χιλιάδες συναλλαγές.

3.2.3 Πως λειτουργεί το Blockchain

Το Blockchain, όπως βεβαίως υποδηλώνει το όνομά του, αποτελείται από πολλά block που συνδέονται μεταξύ τους. Όταν σε ένα block προθέτονται δεδομένα, τότε το block προστίθεται στο blockchain. Για να προστεθεί ένα block στο blockchain, ωστόσο, πρέπει να συμβούν τα παρακάτω τέσσερα πράγματα:

- Πρέπει να πραγματοποιηθεί μια συναλλαγή. Όπως αναφέρθηκε και παραπάνω, ένα block μπορεί να περιέχει πληροφορίες για χιλιάδες συναλλαγές.
- Αυτή η συναλλαγή πρέπει να επαληθευτεί. Αφού πραγματοποιηθεί μια συναλλαγή, αυτή η συναλλαγή σας πρέπει να επαληθευτεί. Η επαλήθευση δεν γίνεται από κάποιο κεντρικό φορέα ή κάποια τράπεζα. Με το blockchain η συναλλαγή παραμένει σε ένα δίκτυο υπολογιστών. Η επιβεβαίωση γίνεται με την επιβεβαίωση των λεπτομερειών της συναλλαγής, συμπεριλαμβανομένου του χρόνου συναλλαγής, του ποσού και των συμμετεχόντων. Εάν τα στοιχεία που έχουν δοθεί είναι αληθείς, το ποσό είναι διαθέσιμο με βάση τα προηγούμενα block που έχουν καταγραφεί τότε η συναλλαγή επιβεβαιώνεται και προχωράει στην διαδικασία της αποθήκευσης.
- Αυτή η συναλλαγή πρέπει να αποθηκευτεί σε ένα block. Μετά την επαλήθευση της συναλλαγής ως ακριβής, λαμβάνει το πράσινο φως. Όλες οι δοθείσες πληροφορίες αποθηκεύονται σε ένα block. Σε αυτό το block πρέπει να δοθεί ένας αριθμός hash. Ο μοναδικός αριθμός ο οποίος είναι και ο αναγνωριστικός αριθμός του block. Η δημιουργία του μοναδικού αυτού αριθμού παράγεται με βάση τα περιεχόμενα του block αλλά και του μοναδικού αναγνωριστικού αριθμού του προηγούμενου block. Μόλις γίνεται η παραπάνω διαδικασία, το block μπορεί να προστεθεί στο blockchain. Εκεί, η συναλλαγή γίνεται μέρος του blockchain.

Μετά την προσθήκη του νέου block στο blockchain, το block καθίσταται διαθέσιμο στο κοινό για να το βλέπει ο καθένας.

3.2.4 Δημόσιο και Ιδιωτικό Blockchain

3.2.4.1 Δημόσιο Blockchain

Κάνοντας χρήση του δημόσιου blockchain πρέπει να γνωρίζουμε πως όλες οι πληροφορίες είναι εμφανείς προς όλους. Οι χρήστες μπορούν επίσης να επιλέξουν να συνδέσουν τους υπολογιστές τους στο δημόσιο δίκτυο blockchain. Με αυτόν τον τρόπο, ο υπολογιστής τους λαμβάνει ένα αντίγραφο του blockchain που ενημερώνεται αυτόματα κάθε φορά που προστίθεται ένα νέο block.

Κάθε υπολογιστής στο δημόσιο δίκτυο blockchain έχει το δικό του αντίγραφο του blockchain, πράγμα που σημαίνει ότι υπάρχουν χιλιάδες, ή στην περίπτωση του Bitcoin, εκατομμύρια αντίγραφα του ίδιου blockchain. Αν και κάθε αντίγραφο του blockchain είναι πανομοιότυπο, η διάδοση αυτών των πληροφοριών σε ένα δίκτυο υπολογιστών καθιστά πιο δύσκολο να μεταβληθούν οι πληροφορίες κακόβουλα. Ένας εισβολέας θα χρειαστεί να αλλάξει κάθε αντίγραφο του δημόσιου blockchain. Αυτό σημαίνει ότι το blockchain είναι «κατανεμημένο» καθολικά και δύσκολο έως αδύνατον να «αλλοιωθεί».

Κάθε χρήστης, όπως αναφέρθηκε και παραπάνω, για να πραγματοποιήσει μια συναλλαγή κάνει χρήση της μοναδικής του «ψηφιακής υπογραφής». Η υπογραφή αυτή δεν αναφέρει κάποιο όνομα ή επωνυμία. Πράγμα που διατηρεί την ανωνυμία του συμμετέχοντος στην συναλλαγή.

Εάν ο συμμετέχων θέλει να δηλώσει σε κάποιο τρίτο τον μοναδικό του αριθμό μπορεί να το κάνει χωρίς φόβο να εκτεθεί σε κίνδυνο ο λογαριασμός του. Για να εκτεθεί σε κίνδυνο θα πρέπει να αναφέρει και το μοναδικό κλειδί που ενεργοποιεί την χρήση την «ψηφιακής υπογραφής» του.

Λόγω των παραπάνω καταλήγουμε στο συμπέρασμα πως το δημόσιο blockchain διακρίνεται από τα παρακάτω στοιχεία:

- Μεγαλύτερη ασφάλεια
- Ανοιχτό περιβάλλον
- Αωνυμία

3.2.4.2 *Ιδιωτικό Blockchain*

Τι είναι ένα ιδιωτικό blockchain; Ένα ιδιωτικό blockchain είναι ένας ειδικός τύπος της τεχνολογίας blockchain. Στην αλυσίδα αυτή έχει εξουσία μόνο ένας οργανισμός. Το δίκτυο δεν είναι ανοιχτό προς το κοινό για να συμμετάσχει σε αυτή την αλυσίδα.

Όλες οι ιδιωτικές λύσεις blockchain θα έχουν κάποια μορφή αναγνώρισης χρήστη ώστε να μπορούν συγκεκριμένα άτομα να εισέρχονται στο δίκτυο. Οι ιδιωτικές αυτές λύσεις blockchain αναπτύσσονται συνήθως σε πλατφόρμες για την χρήση στο εσωτερικό σύστημα δικτύωσης μιας εταιρείας.

Αποτέλεσμα αυτού είναι να υπάρχει εμπιστοσύνη μεταξύ των κόμβων. Χωρίς εμπιστοσύνη στους κόμβους, αυτό το μοντέλο δικτύου δεν θα λειτουργήσει. Έτσι, μόνο οι εργαζόμενοι μιας επιχείρησης μπορούν να έχουν πρόσβαση σε αυτήν.

Η εμπιστοσύνη χρειάζεται διότι ένα ιδιωτικό blockchain δεν είναι πλήρως αποκεντρωμένο όπως οι δημόσιες πλατφόρμες blockchain. Είναι περισσότερο μια εν μέρει αποκεντρωμένη κατάσταση.

Όλοι οι κόμβοι πρέπει να συμμορφώνονται με ορισμένους κανόνες για να διασφαλίσουν τη σωστή ροή μιας εταιρείας.

Παρόλο που το δημόσιο blockchain ήρθε πρώτο, τείνουν να στερούνται αναποτελεσματικότητας. Επειδή το δημόσιο δίκτυο είναι ανοιχτό προς το ευρύ κοινό έχει ως αποτέλεσμα, όταν περισσότερα άτομα προσπαθούν να χρησιμοποιήσουν τις λειτουργίες του να καταλαμβάνει πολλούς πόρους με αποτέλεσμα να επιβραδύνεται γρήγορα.

Από την άλλη πλευρά, το ιδιωτικό blockchain επιτρέπει μόνο λίγα άτομα στο δίκτυο. Σε πολλές περιπτώσεις, πρέπει ακόμα και να πραγματοποιηθούν ορισμένες εργασίες προτού ολοκληρωθεί το block. Έτσι, δεν υπάρχει τρόπος να καταληφθούν επιπλέον πόροι και να επιβραδυνθεί η διαδικασία ολοκλήρωσης ενός block οπότε δεν υπάρχει καμία μορφή καθυστέρησης ή φόρτου.

Επιπλέον, η χρέωση της επαλήθευσης του block στις ιδιωτικές αλυσίδες blockchain είναι σταθερή. Σε κάθε δίκτυο blockchain, δημόσιο ή ιδιωτικό πρέπει να καταβληθεί μια συγκεκριμένη χρέωση για να επαλειφθεί και να ολοκληρωθεί μια συναλλαγή. Σε δημόσιες πλατφόρμες, η χρέωση μπορεί να αυξηθεί σε μεγάλο βαθμό λόγω της πίεσης των κόμβων που ζητούν συναλλαγές. Αντίθετα στο ιδιωτικό blockchain το κόστος αυτό θα παραμείνει σταθερό.

Λόγω των παραπάνω καταλήγουμε στο συμπέρασμα πως το ιδιωτικό blockchain διακρίνεται από τα παρακάτω στοιχεία:

- Υψηλή απόδοση
- Σταθερότητα

3.2.4.3 Δημόσιο δίκτυο σε σύγκριση με το ιδιωτικό δίκτυο Blockchain

Παρακάτω παραθέτουμε μία εικόνα με τις βασικές διαφορές μεταξύ των δυο αυτών δικτύων Blockchain.



Εικόνα 2: Δημόσιο vs Ιδιωτικό Blockchain

3.3 Αποκεντρωμένες Εφαρμογές (Decentralized Applications DApps)

3.3.1 Τι είναι τα DApps

Στις μέρες μας, η μεγαλύτερη πλειοψηφία των εφαρμογών βασίζονται στο Internet. Έχοντας μία κεντρική αρχιτεκτονική, η σχέση μεταξύ του τελικού χρήστη και της εφαρμογής είναι η εφαρμογή να φιλοξενείται σε έναν κεντρικό υπολογιστή (διακομιστή) και μέσα από αυτόν οι χρήστες να έχουν πρόσβαση στην εφαρμογή.

Η εφαρμογή που βασίζεται σε ένα αποκεντρωμένο σύστημα ονομάζεται Decentralized Application - DApp. Οι αποκεντρωμένες εφαρμογές δεν χρειάζεται απαραίτητα να εκτελούνται πάνω από ένα δίκτυο blockchain. Τα BitTorrent, Porcorn Time, uTorrent, είναι παραδείγματα αποκεντρωμένων εφαρμογών που εκτελούνται σε δίκτυο Peer-To-Peer (P2P).

Το blockchain είναι ένα ειδικό είδος δικτύου P2P. Οι Αποκεντρωμένες Εφαρμογές (Decentralized Applications - DApps) πάνω σε ένα δίκτυο blockchain είναι ένας νέος τύπος εφαρμογών λογισμικού που δεν ανήκουν σε κάποια κεντρική αρχή. Από τα πιο σημαντικά τους χαρακτηριστικά είναι ότι δεν μπορούν να τερματιστούν από κανέναν και δεν υφίστανται διακοπή λειτουργίας. Πρόκειται για λογισμικό ανοιχτού κώδικα που χρησιμοποιεί έξυπνες συμβάσεις (Smart Contract) για την εκτέλεση συναλλαγών στην αλυσίδα του blockchain.

Εάν μία εφαρμογή πληροί τα παρακάτω κριτήρια τότε μπορεί να χαρακτηριστεί ως DApp

- Η εφαρμογή είναι εφαρμογή ανοιχτού κώδικα.
- Η εφαρμογή πρέπει να λειτουργεί αυτόνομα, καμία οντότητα δεν την ελέγχει.
- Τα δεδομένα και τα αρχεία της εφαρμογής αποθηκεύονται κρυπτογραφημένα σε ένα δημόσιο αποκεντρωμένο σύστημα.
- Η εφαρμογή πρέπει να χρησιμοποιεί ένα κρυπτογραφικό διακριτικό. Η συμβολοσειρά αυτή είναι απαραίτητη για την πρόσβαση στο αίτημα και μέσω του διακριτικού γίνεται και η οποιαδήποτε συνεισφορά σε αυτούς που θα επαληθεύσουν την συναλλαγή.

3.3.2 Τύποι των DApps

Με βάση το μοντέλο του Blockchain οι DApps μπορούν να ταξινομηθούν σε τρεις κατηγορίες:

- Κατηγορία 1: Στην συγκεκριμένη κατηγορία τα DApps έχουν το δικό τους blockchain. Παράδειγμα τέτοιου DApps είναι το Bitcoin.
- Κατηγορία 2: Στην συγκεκριμένη κατηγορία τα DApps κάνουν χρήση το δίκτυο blockchain των εφαρμογών DApps της κατηγορίας 1. Αυτές οι αποκεντρωμένες εφαρμογές είναι πρωτόκολλα και διαθέτουν τα απαραίτητα διακριτικά για τη λειτουργία τους.
- Κατηγορία 3: Η εφαρμογές DApps στην συγκεκριμένη κατηγορία κάνουν χρήση του πρωτοκόλλου της κατηγορίας 2.

3.3.3 Διάσημες Εφαρμογές DApps

Οι δημοφιλέστερες εφαρμογές στο κόσμο στις μέρες που σίγουρα όλοι τις έχουμε ακούσει είναι το Bitcoin και το Ethereum.

- Bitcoin: Το Bitcoin είναι ένα πρωτόκολλο, ένα ψηφιακό νόμισμα και μια πλατφόρμα μαζί. Ο συνδυασμός των τριών παραπάνω μας δημιουργεί το ψηφιακό νόμισμα bitcoin.
- Ethereum: Το Ethereum είναι μια αποκεντρωμένη πλατφόρμα, που επιτρέπει την εκτέλεση DApps από πάνω της. Το Ethereum έχει την δυνατότητα εκτέλεσης έξυπνων συμβολαίων (Smart Contract). Οι εφαρμογές εκτελούνται ακριβώς όπως έχουν

προγραμματιστεί. Δεν υπάρχει πιθανότητα διακοπής λειτουργίας, λογοκρισίας, απάτης ή τρίτου μέρους παρέμβασης, πράγμα που προσφέρει μέγιστη ασφάλεια.

Πολλές εφαρμογές έχουν κατασκευαστεί πάνω σε αυτές της δημόσιες αλυσίδες. Πολλές βέβαια εφαρμογές δημιουργούν την δική του αλυσίδα. Παρακάτω παραθέτουμε έναν πίνακα με τις πιο γνωστές εφαρμογές DApps στις μέρες μας, οι οποίες χρησιμοποιούν είτε το Blockchain του Bitcoin είτε του Ethereum.

ΕΦΑΡΜΟΓΗ DAPP	BLOCKCHAIN	ΚΑΤΗΓΟΡΙΑ DAPP	ΔΙΑΚΡΙΤΙΚΟ (TOKEN)	ΠΕΡΙΓΡΑΦΗ
THE SAFE NETWORK	Bitcoin	2	SafeCoin (SFE)	Αποθήκευση δεδομένων και επικοινωνία
AUGUR	Ethereum	2	Augur (REP)	Πλατφόρμα Αγορών
FACTOM	Ιδιωτικό	1	Factom (FCT)	Σύστημα τήρησης αρχείων
GOLEM	Ethereum	2	Golem (GNT)	Πρώτη παγκόσμια αγορά για αδράνεια υπολογιστή

Πίνακας 1: Διάσημα DApps Σήμερα

3.3.4 Πλατφόρμες Ανάπτυξης DApps

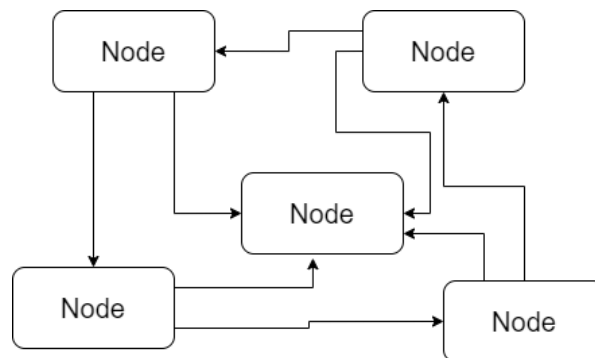
Οι πιο δημοφιλείς πλατφόρμες blockchain για την κατασκευή DApps σήμερα είναι Ethereum, EOS και TRON. Σε αυτήν την ενότητα, θα συζητήσουμε εν συντομία τα βασικά χαρακτηριστικά κάθε μιας από αυτές τις τρεις πλατφόρμες.

- **Ethereum (ETH):** Το Ethereum διακρίνεται για την διασφάλιση της ασφάλειας και την πραγματική αποκέντρωση. Παρόλα αυτά εάν κάποιος θέλει να δημιουργήσει μια εφαρμογή η οποία αργότερα θα πρέπει να επεκταθεί, τότε το Ethereum δεν είναι η καλύτερη λύση για τον προγραμματισμό και της υλοποίηση της DApps. Εάν πρώτο μέλημα της εφαρμογής είναι η ασφάλεια τότε άφοβα μπορεί να επιλέξει κάποιος την δημιουργία DApps πάνω στο δίκτυο του Ethereum. Ωστόσο εάν χρειάζεται να αναπτυχθεί μια εφαρμογή παραδείγματος χάριν τυχερών παιχνιδιών, όπου αργότερα σίγουρα θα δημιουργηθεί η ανάγκη της επεκτασιμότητας, τότε το ETH ίσως δεν είναι η καλύτερη επιλογή πλατφόρμας.
- **EOS:** Η EOS δεν είναι μια πραγματικά αποκεντρωμένη πλατφόρμα. Μέχρι σήμερα περιλαμβάνει 21 εξ ορυκτές οι οποίοι επαληθεύουν τις συναλλαγές με βάση τον αλγόριθμο «Proof of Stake». Η ασφάλεια της πλατφόρμας είναι ευμετάβλητη. Διάφοροι κόμβοι μπορεί να συνεργαστούν για να σαμποτάρουν το σύστημα.

- TRON: Είναι μια πλατφόρμα ανάπτυξης παρόμοια με την EOS. Το TRON λειτουργεί με τον αλγόριθμο «Proof of Stake». Επιλύει και εκείνο το πρόβλημα της επεκτασιμότητας.. Πάραυτα, και εκείνο δεν προστατεύεται πλήρως όπως θα ήταν μια πραγματικά αποκεντρωμένη πλατφόρμα. Οι χρήστες μπορούν ακόμα να κλειδωθούν εάν συνεργαστούν οι εξ ορυκτές.

3.4 Ethereum

Στο παρακάτω διάγραμμα βλέπουμε την δομή που έχει ένα δίκτυο Ethereum. Όλοι οι κόμβοι είναι συνδεδεμένοι μεταξύ τους. Η αλυσίδα blockchain βρίσκεται σε όλους τους κόμβους αυτούς.



Εικόνα 3: Σχεδιάγραμμα Ethereum

Το πρώτο πράγμα λοιπόν που πρέπει να κατανοήσουμε είναι πως δουλεύοντας με το Ethereum, δουλεύουμε με ένα network από κόμβους, Nodes. Μέσω αυτού του δικτύου μπορούμε να μεταφέρουμε χρήματα (Ethereum) μεταξύ διάφορων χρηστών και επιπλέον μπορούμε να αποθηκεύουμε δεδομένα. Με δεδομένες τις παραπάνω δυνατότητες, μέσω του Ethereum μπορούμε να δημιουργήσουμε εξαιρετικές εφαρμογές.

Θα πρέπει όμως να κατανοήσουμε ότι υπάρχουν πολλά και διαφορετικά Ethereum δίκτυα. Το κύριο όμως Ethereum δίκτυο είναι μοναδικό και το ονομάζουμε Main Network. Στο δίκτυο αυτό το κόστος του Ether είναι πραγματικό και η αξία του μπορεί να μετατραπεί σε πραγματικό χρήμα. Κάποια παραδείγματα από άλλα Ethereum δίκτυα είναι:

- Ropsten Network
- Kovan Network
- Δοκιμαστικό Rinkeby Network
- Δοκιμαστικό Goerli Network

Τα δυο τελευταία δίκτυα μπορούν να χρησιμοποιηθούν για δοκιμαστικούς σκοπούς. Σε αυτό το σημείο να τονίσουμε πως μπορεί κάποιος να δημιουργήσει και το δικό του ιδιωτικό Ethereum δίκτυο.

Οι κόμβοι που αναφέραμε παραπάνω είναι υπολογιστές όπως laptop ή σταθεροί υπολογιστές ή οποιαδήποτε μορφή υπολογιστή στους οποίους τρέχει η διαδικασία δημιουργία της αλυσίδας του Ethereum. Ο κάθε ένας έχει πρόσβαση σε αυτή την διαδικασία. Κάθε κόμβος για να λάβει χώρα στην διαδικασία θα πρέπει να έχει ένα πλήρες αντίγραφο της αλυσίδας του Ethereum. Την αλυσίδα του blockchain μπορούμε να την παρομοιάσουμε σαν μια βάση δεδομένων στην οποία γράφονται οι συναλλαγές που λαμβάνουν χώρα.

3.4.1 Ethereum Accounts

Για να μπορέσει κανείς να χρησιμοποιήσει το δίκτυο του Ethereum θα πρέπει να έχει ένα δικό του λογαριασμό, τον οποίο παραπάνω το περιγράψαμε ως username. Ο λογαριασμός αυτός είναι ο προσωπικός του Account. Πως δημιουργείται όμως αυτός ο λογαριασμός;

Για να δημιουργηθεί ο Λογαριασμός (Accounts) γίνεται χρήση τριών διαφορετικών κομματιών πληροφορίας. Αυτά είναι:

- Account Address: Μπορούμε να το σκεφτούμε σαν email. Είναι μοναδικό, μπορεί να μοιραστεί και να δηλωθεί ως κάτι που μας ανήκει.
- Public Key, Private Key: Τις συγκεκριμένες συμβολοσειρές μπόουμε να τις παρομοιάσουμε σαν το password. Είναι εκείνες που μπορούν να μας δώσουν της εξουσιοδότηση της χρήσης του Account Address. Συγκεκριμένα, το στοιχείο που πρέπει να κρατάμε καλά φυλαγμένο είναι το Private Key. Δεν πρέπει να το μοιραζόμαστε ή να το ξεχάσουμε.

Δημιουργώντας ένα λογαριασμό Ethereum, ο συγκεκριμένος λογαριασμός μπορεί να χρησιμοποιηθεί σε οποιαδήποτε αλυσίδα Ethereum, σε αντίθεση με το ποσό ETH που μπορεί να περιέχει μπορεί να χρησιμοποιηθεί στην αλυσίδα για την οποία δημιουργήθηκε το συγκεκριμένο ποσό.

3.4.2 Ethereum Currency

Όπως το Bitcoin έτσι και το Ethereum έχει και εκείνο ένα «φυσικό» νόμισμα το οποίο ονομάζεται Ether (ETH). Ρίχνοντας μια ματιά στο διαδίκτυο θα δούμε πως αναφέρεται και άλλο ένα νόμισμα το οποίο ονομάζεται Ether Classic (ETC).

Το Ethereum Classic (ETC) είναι το αρχικό νόμισμα του blockchain Ethereum. Το ETH και το ETC μοιράζονταν το ίδιο blockchain πριν από το λεγόμενο Hard Fork τον Ιούλιο 2016. Πριν απ' αυτό το γεγονός, ο αρχικός σχεδιασμός και η λειτουργικότητα αυτών των δύο ήταν ουσιαστικά ίδια. Το Hard Fork χώρισε το blockchain σε Ethereum Classic και Ethereum, χωρίζοντας την κοινότητα εκείνη την εποχή. Οι περισσότεροι προγραμματιστές επέλεξαν να «ακολουθήσουν» το νέο πρωτόκολλο Ethereum (ETH), περιορίζοντας το μέγεθος της κοινότητας ETC.

Όπως όλα τα νομίσματα έτσι και το ETH έχει της υποδιαιρέσεις του. Οι υποδιαιρέσεις του ETH παρουσιάζονται στην παρακάτω εικόνα.

Unit	Wei Value	Wei
wei	1 wei	1
Kwei (babbage)	1e3 wei	1,000
Mwei (lovelace)	1e6 wei	1,000,000
Gwei (shannon)	1e9 wei	1,000,000,000
microether (szabo)	1e12 wei	1,000,000,000,000
milliether (finney)	1e15 wei	1,000,000,000,000,000
ether	1e18 wei	1,000,000,000,000,000,000

Εικόνα 4: Ether to Wei

3.4.3 Ethereum Συναλλαγή (Transaction)

Ως συναλλαγή (transaction) μπορεί να οριστεί ως μία εγγραφή – block το οποίο περιγράφει την προσπάθεια ενός λογαριασμού να στείλει χρήματα σε άλλον ή σε κάποια Smart Contract. Η εγγραφή μπορεί να ποικίλει και να περιέχει κάποια από τα στοιχεία που εμφανίζονται στον παρακάτω πίνακα.

nonce	Αριθμός Συναλλαγής
to	Διεύθυνση την οποία θα αποσταλούν τα Ether
value	Το ποσό των Ether που θα σταλεί σε κάποιο λογαριασμό ή σε κάποιο Smart Contract
gasPrice	Το ποσό των Ether που πρέπει να πληρώσει ο αποστολέας για να πραγματοποιηθεί η συναλλαγή
startGas/gasLimit	Το υπολογιζόμενο στο περίπου ποσό Ether που μπορεί να καταναλώσει η συγκεκριμένη συναλλαγή.
v	Τα σημεία αυτά είναι κρυπτογραφημένα
r	κομμάτια τα οποία δημιουργήθηκαν
s	από το private key του αποστολέα.

Πίνακας 2: Πεδία Συναλλαγής Ethereum

Ο συνδυασμός εμφάνισης των παραπάνω στοιχείων μας δείχνει και τον σκοπό τον οποίο δημιουργήθηκε και το αντίστοιχο block.

Τα σημεία που είναι άξια λόγου για μια συναλλαγή είναι ότι αφορά στο GAS. Τί είναι λοιπόν το gas;

3.4.3.1 GasLimit

Ως GasLimit ονομάζεται μέγιστο ποσό μονάδων Ether που είστε διατεθειμένοι να ξοδέψετε σε μια συναλλαγή. Αυτό ορίζεται εξ αρχής της συναλλαγής έτσι ώστε να μην υπάρξει κάποιο σφάλμα κάπου σε ένα συμβόλαιο (Smart Contract) με αποτέλεσμα να ξοδευτούν περισσότερα ETH απ' ότι αναμενόταν.

Ωστόσο, το GasLimit είναι απαραίτητο για μια συναλλαγή. Καθορίζονται ήδη από των κώδικα που εκτελείται στο blockchain. Εάν δεν θέλετε να δαπανήσετε τόσο πολύ Gas, η μείωση του δεν θα βοηθήσει πολύ. Πρέπει να συμπεριλάβετε Gas σε μια συναλλαγή ώστε να καλύψετε τους υπολογιστικούς πόρους που χρησιμοποιείτε, διαφορετικά η συναλλαγή σας θα αποτύχει λόγω σφάλματος "Out of Gas".

Στο σημείο αυτό να σημειώσουμε πως το αχρησιμοποίητο Gas επιστρέφει στον λογαριασμό του χρήστη σε περίπτωση ολοκληρωμένης συναλλαγής. Σε περίπτωση μη ολοκληρωμένης συναλλαγής με μήνυμα λάθος "Out of Gas", το ποσό που είχε τοποθετηθεί ως GasLimit θα ξοδευτεί ολόκληρο.

3.4.3.2 GasPrice

Εάν κάποιος θέλει να δαπανήσει λιγότερα Gas για μια συναλλαγή, μπορεί να το πραγματοποιήσει μειώνοντας το ποσό που θα πληρώσει ανά μονάδα φυσικού αερίου. Ως συνέπεια αυτή της μείωσης η συναλλαγή θα εξορυχθεί πιο αργά.

Η αύξηση της τιμής του Gas σημαίνει και γρηγορότερη εξόρυξη. Το ποσό Gas πηγαίνει στο εξορυκτή του block σας. Όταν οι εξορυκτές εξορύσσουν ένα block, πρέπει να αποφασίσουν ποιες συναλλαγές θα συμπεριλάβουν. Μπορούν να επιλέξουν να μην περιλαμβάνουν συναλλαγές ή να επιλέγουν τυχαία επιλογή συναλλαγών. Για να ενθαρρύνει τους εξορυκτές να συμπεριλαμβάνουν την συναλλαγή στο block, καλό είναι οριστεί μια τιμή Gas η οποία να είναι αρκετά υψηλή για να τους κάνει να θέλουν να το συμπεριλάβουν (καθώς εξαρτάται αποκλειστικά από αυτούς).

Οι περισσότεροι εξορυκτές ακολουθούν την στρατηγική της ταξινόμησης. Ταξινομούν τις συναλλαγές από την υψηλότερη τιμή Gas προς την χαμηλότερη. Στη συνέχεια συμπεριλαμβάνουν τις συναλλαγές με υψηλό Gas έως ότου το block γεμίσει ή φτάσουν σε συναλλαγή με χαμηλή τιμή Gas.

3.4.4 Ethereum Smart Contract

Μπορούμε να φανταστούμε μια Έξυπνη Διεπαφή (Smart Contract) σαν ένα λογαριασμό (Account) αλλά αντί να την χειρίζεται κάποιος άνθρωπος την χειρίζεται κάποιος προγραμματισμένος κώδικας. Ο κώδικας αυτός, ο οποίος είναι υπεύθυνος για το πως θα συμπεριφέρεται η διεπαφή, έχει παραχθεί από τον προγραμματιστή (developer) της συγκεκριμένης διεπαφής. Μια διεπαφή μπορεί να έχει τα παρακάτω πεδία τα οποία απεικονίζονται στο παρακάτω πίνακα.

Πεδίο	Περιγραφή
balance	Το ποσό το οποίο περιλαμβάνεται μέσα στην Έξυπνη Διεπαφή (Smart Contract)
storage	Ο χώρος ο οποίος αποθηκεύονται τα δεδομένα της διεπαφής
Code	Ο κώδικας της διεπαφής

Πίνακας 3: Έξυπνη Διεπαφή (Smart Contract)

- **Balance:** Μια διεπαφή έχει την δυνατότητα να έχει πάνω της κάποιο ποσό από Ether.
- **Storage:** Τον χώρο σε μια διεπαφή μπορούμε να τον φανταστούμε σαν ένα μικρό ράφι στο οποίο μπορούμε να αποθηκεύουμε κάποια δεδομένα σχετικά με την διεπαφή μας. Αυτά μπορεί να είναι αριθμοί, λίστες, οποιαδήποτε τέτοια μορφή δεδομένα τα οποία είναι απαραίτητα για την λειτουργία της διεπαφής.
- **Code:** Αυτό το πεδίο περιέχει όλο τον κώδικα σε μορφή κώδικα μηχανής. Ουσιαστικά είναι ο κώδικας μετά την διαδικασία του compile. Γι' αυτό το λόγο η διεπαφή γνωρίζει ανά πάσα στιγμή τι πρέπει να κάνει, μιας και όλες οι οδηγίες που έχει λάβει από τον προγραμματιστή της βρίσκονται ενσωματωμένες μέσα σε αυτή.

Σε αντίθεση με τον Account του κάθε χρήστη στο οποίο αναφερθήκαμε παραπάνω, η έξυπνη διεπαφή δημιουργείται σε ένα συγκεκριμένο δίκτυο όπου και στο οποίο εκτελείται. Δεν μπορεί να εκτελεστεί σε κάποιο άλλο. Για να μπορέσει να εκτελεστεί σε κάποιο άλλο δίκτυο, η διεπαφή θα πρέπει να ξανά γίνει deploy σε αυτό το διαφορετικό δίκτυο.

4. Προδιαγραφές Συστήματος

Όπως αναφέραμε και στην αρχή του Paper στόχος της εργασία είναι η ανάπτυξη ενός συστήματος με την βοήθεια του blockchain το οποίο θα προσομοιάζει το διάγραμμα Γκαντ ώστε να χρησιμοποιηθεί στον τομέα της υγείας για την καλύτερη και σωστή παρακολούθηση των ερευνών.

4.1 Αρχιτεκτονική Συστήματος

Το σύστημα που θα δημιουργήσουμε θέλουμε να μας παρέχει ασφάλεια. Μεγάλα ποσά διακινούνται κατά την εξέλιξη μιας έρευνας. Αυτά τα ποσά δεν πρέπει να είναι προσβάσιμα σε όλους ή να πέσουν σε υποκλοπή. Επιπλέον τα άτομα – οργανισμοί που θα λάβουν χώρα δεν θα βρίσκονται υπό την αιγίδα ενός μεγάλου οργανισμού. Για τους παραπάνω λόγους η εφαρμογή DApps θα αναπτυχθεί με την βοήθεια του Main Ethereum.



Εικόνα 5: Ethereum

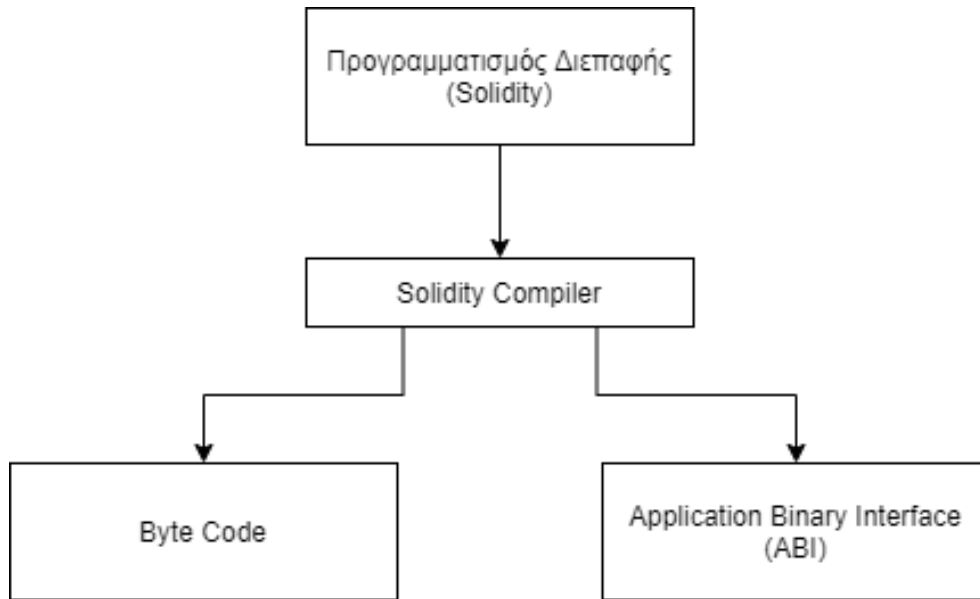
Στο κορμό της εφαρμογής θα λάβει χώρα ο κώδικας ο οποίος θα είναι γραμμένος στην γλώσσα που επικοινωνεί με το Ethereum Blockchain. Η γλώσσα αυτή είναι η Solidity.



Εικόνα 6: Solidity

Προγραμματίζοντας μία διεπαφή σε κάποιο IDE πρόγραμμα είναι εύκολο κάποιος να κατανοήσει τι ακριβώς κάνει μια διεπαφή. Τα δεδομένα τα οποία δεν μπορεί κανείς να διαβάσει είναι τα δεδομένα που παράγονται μετά το Compile της διεπαφής.

Κατά την διαδικασία του Compile παράγονται δύο αρχεία. Ο κώδικας σε μορφή Byte Code είναι εκείνος ο οποίος ενσωματώνεται στην διεπαφή. Από την άλλη μεριά ο κώδικας με την ονομασία Application Binary Interface (ABI) είναι εκείνος που μπορεί χρησιμοποιηθεί από διάφορα προγράμματα για να καλέσουν τις αντίστοιχες συναρτήσεις της διεπαφής.

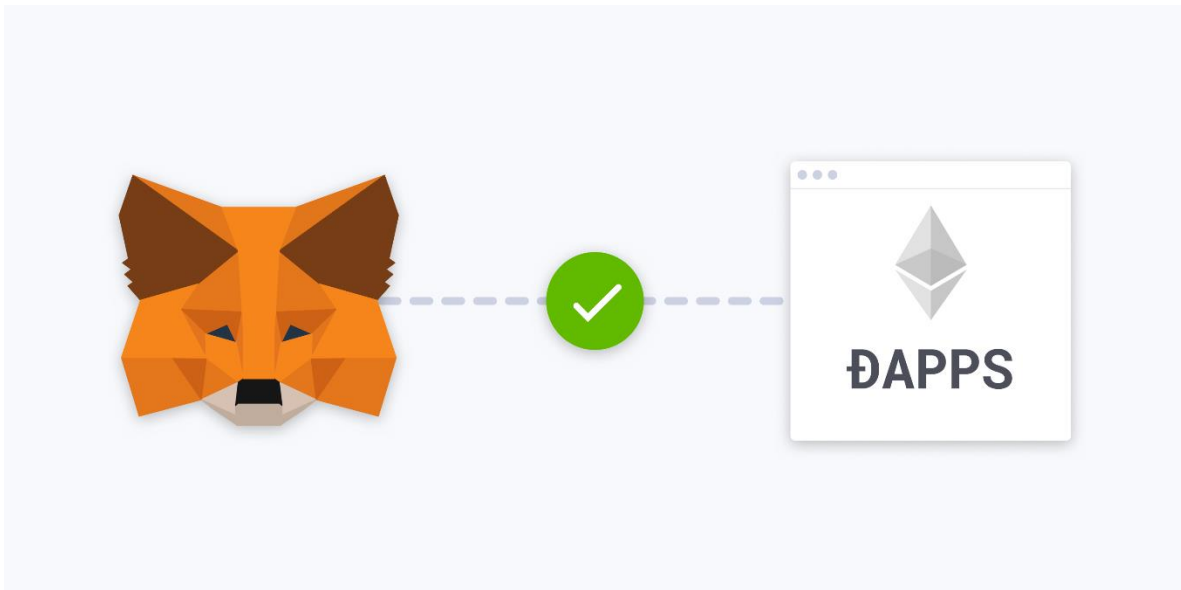


Εικόνα 7: Solidity Compiler

Να σημειώσουμε πως για τους σκοπούς της εργασίας θα χρησιμοποιήσουμε το δοκιμαστικό δίκτυο του Ethereum το οποίο ονομάζεται Rinkeby Network.

Δημιουργώντας λοιπόν την διεπαφή και κάνοντας την compile και deploy στο Rinkeby Network, οποιοσδήποτε που γνωρίζει την διεύθυνση, address, που έχει λάβει η διεπαφή μπορεί να πραγματοποιήσει συναλλαγή μαζί της σύμφωνα βέβαια με τον κώδικα του δημιουργού της.

Για να μπορέσει όμως κάποιος να έρθει εύκολα σε συναλλαγή με την διεπαφή θα δημιουργηθεί ένα περιβάλλον προσβάσιμο από Browser και συγκεκριμένα από τον Chrome με την βοήθεια του plug in MetaMask.



Εικόνα 8: MetaMask

Σε αυτό το σημείο καλό είναι να αναφέρουμε δύο λόγια για το MetaMask. Το MetaMask είναι μια γέφυρα που μας επιτρέπει να εκτελούμε Ethereum DApps απευθείας στο πρόγραμμα του περιηγητή μας χωρίς να χρειάζεται να εκτελέσουμε έναν πλήρη κόμβο στο μηχάνημά μας. Αντ' αυτού μας επιτρέπει να συνδεθούμε σε ένα κόμβο του Ethereum που ονομάζεται Infura και να εκτελούμε Smart Contract σε αυτό τον κόμβο. Το MetaMask διαχειρίζεται το πορτοφόλι μας στο Ethereum το οποίο περιέχει Ether και μας επιτρέπει να στέλνουμε χρήματα ή να λαμβάνουμε μέσω κάποιας DApps εφαρμογής.

Όπως λοιπόν κατανοούμε, το επόμενο αντικείμενο το οποίο θα χρησιμοποιήσουμε στην εργασία είναι το INFURA. Τί είναι όμως το INFURA;



Εικόνα 9: Infura

Το Infura είναι ένα φιλοξενούμενο σύμπλεγμα κόμβων Ethereum που επιτρέπει στους χρήστες της εφαρμογής να την εκτελούν χωρίς να απαιτείται να δημιουργήσουν τον δικό τους κόμβο ή πορτοφόλι Ethereum. Για λόγους ασφαλείας, το Infura δεν διαχειρίζεται τα ιδιωτικά κλειδιά, πράγμα που σημαίνει ότι η Infura δεν μπορεί να υπογράψει συναλλαγές εκ μέρους μας.

Ένα επιπλέον εργαλείο το οποίο θα χρειαστούμε για την σύνδεση της εφαρμογής μας με το περιβάλλον που θα χρησιμοποιεί ο χρήστης είναι το Web3.js.



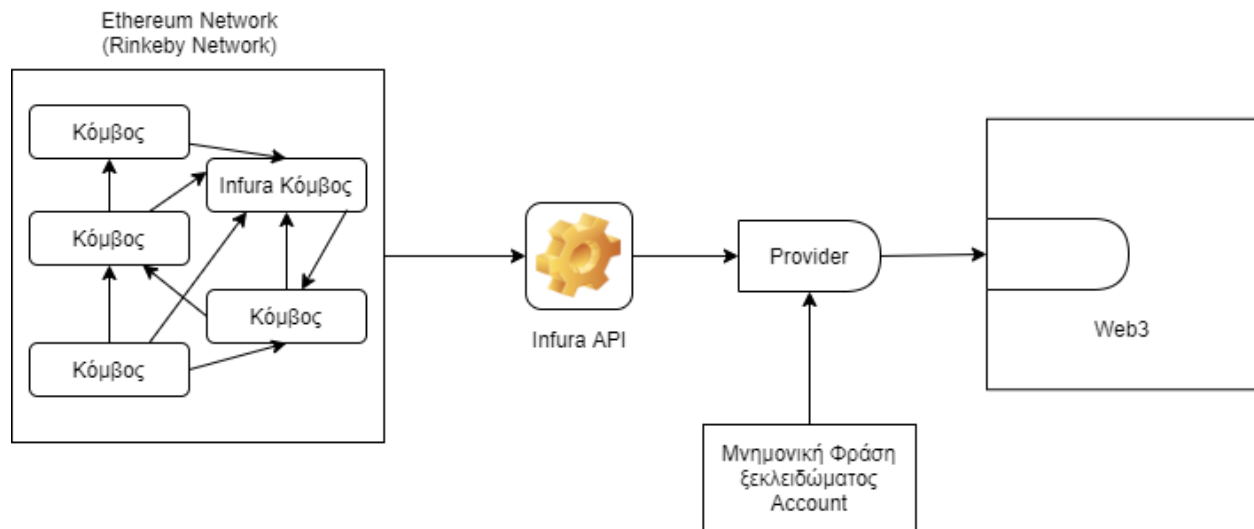
Εικόνα 10: Web3.js

Το Web3.js είναι μια συλλογή βιβλιοθηκών που μας επιτρέπουν να αλληλοεπιδρούμε με έναν τοπικό ή απομακρυσμένο κόμβο ethereum χρησιμοποιώντας HTTP, IPC ή WebSocket.

Μας παρέχει ένα API για χρήση, ώστε να μπορούμε εύκολα να συνεργαστούμε με το blockchain. Το Web3 λειτουργεί ως περιτύλιγμα για το JSON RPC για σύνδεση σε απομακρυσμένο ή τοπικό κόμβο Ethereum με σύνδεση HTTP ή IPC. Το Web3 είναι βασικά μια σύνδεση μεταξύ του Ethereum blockchain και του έξυπνου συμβολαίου σας.

Με τα παραπάνω αναφερόμενα εργαλεία μας δίνεται η δυνατότητα να δημιουργήσουμε την έξυπνη διεπαφή και την άμεση σύνδεσή της με κάποιο Interface (Επίπεδο προβολής) ώστε να μπορεί εύκολα ο χρήστης να χρησιμοποιεί την DApp που σχεδιάζουμε.

Ο τρόπος με τον οποίο διαγραμματικά συνδέονται όλα αυτά τα εργαλεία φαίνεται στην παρακάτω εικόνα.



Εικόνα 11: Διασύνδεση Εργαλείων

Ας δούμε όμως τώρα τα εργαλεία τα οποία θα χρησιμοποιήσουμε για να δημιουργήσουμε το Interface που θα έχουν πρόσβαση οι χρήστες.

Για την δημιουργία ενός ευχάριστου Interface το οποίο διαθέτει τα κατάλληλα εργαλεία και είναι συμβατό με τα παραπάνω ώστε να δημιουργηθεί μια ολοκληρωμένη εφαρμογή DApp θα κάνουμε χρήση της React.js και Node.js.



Εικόνα 12: React.js - Node.js

Η Node.js είναι ένα περιβάλλον εκτέλεσης JavaScript. Το περιβάλλον αυτό περιλαμβάνει όλα όσα χρειαζόμαστε για να εκτελεστεί ένα πρόγραμμα γραμμένο σε γλώσσα JavaScript.

Η React.js είναι μια βιβλιοθήκη JavaScript η οποία μας βοηθάει στην δημιουργία Interfaces.

Στοιχείο της React είναι ότι είναι αυτόνομη. Μας απεικονίζει μια κάποια έξοδα άμεσα. Μπορούμε εύκολα να δημιουργήσουμε στοιχεία διεπαφής όπως ένα κουμπί ή ένα πεδίο εισαγωγής ως στοιχείο React. Τα συστατικά είναι συνθέσιμα. Ένα στοιχείο μπορεί να περιλαμβάνει ένα ή περισσότερα άλλα στοιχεία στην έξοδο του.

Παρακάτω παρατίθενται όλα τα πακέτα package τα οποία έχουμε χρησιμοποιήσει κατά την διαδικασία δημιουργία της DApp.

```
},
"author": "",
"license": "ISC",
"dependencies": {
  "fs-extra": "^7.0.1",
  "ganache-cli": "^6.3.0",
  "mocha": "^6.0.0",
  "next": "^4.1.4",
  "next-routes": "^1.4.2",
  "react": "^16.13.1",
  "react-dom": "^16.13.1",
  "semantic-ui-css": "^2.4.1",
  "semantic-ui-react": "^0.88.2",
  "solc": "^0.4.22",
  "web3": "^1.0.0-beta.35"
},
"devDependencies": {
  "any-promise": "^1.3.0",
  "bindings": "^1.5.0",
  "truffle-hdwallet-provider": "^1.0.0-web3one.5"
}
```

4.2 Απαιτήσεις Συστήματος

Έχοντας εξηγήσει την αρχιτεκτονική του συστήματός μας και τα εργαλεία τα οποία θα χρησιμοποιήσουμε ως δούμε τις απαιτήσεις που χρειάζεται ένα σύστημα για να μπορέσει να υποστηρίξει μία τέτοια εφαρμογή.

Γνωρίζοντας ότι η εφαρμογή «τρέχει» πάνω στην αλυσίδα του Ethereum, ο βασικός κορμός της εφαρμογής θα τρέχει στο δίκτυο αυτό. Το πόσο γρήγορα θα εκτελείται μία συναλλαγή, όπως έχουμε εξηγήσει και σε προηγούμενο κεφάλαιο, εξαρτάται από το GasPrice που θα χρησιμοποιήσει ο εκάστοτε εκτελεστής της συναλλαγής.

Θα χρειαστεί όμως να στηθεί ένας Web Server στον οποίο θα τρέχουν τα εργαλεία για την δημιουργία του Interface. Θα χρειαστεί ένα μηχάνημα το οποίο να μπορεί να αντέχει πολλά Request εμφάνισης της ιστοσελίδας. Λόγω του ότι η εφαρμογή θα χρησιμοποιηθεί για την

βελτίωση της διαδικασίας της διαχείρισης των Ιατρικών Ερευνών, συγκεκριμένος αριθμός χρηστών θα κάνει χρήση της πλατφόρμας αυτής.

- Hardware Specifications για τον Web Server
- 100 GB of disk space for cache
- 8 CPU cores
- 16 GB RAM

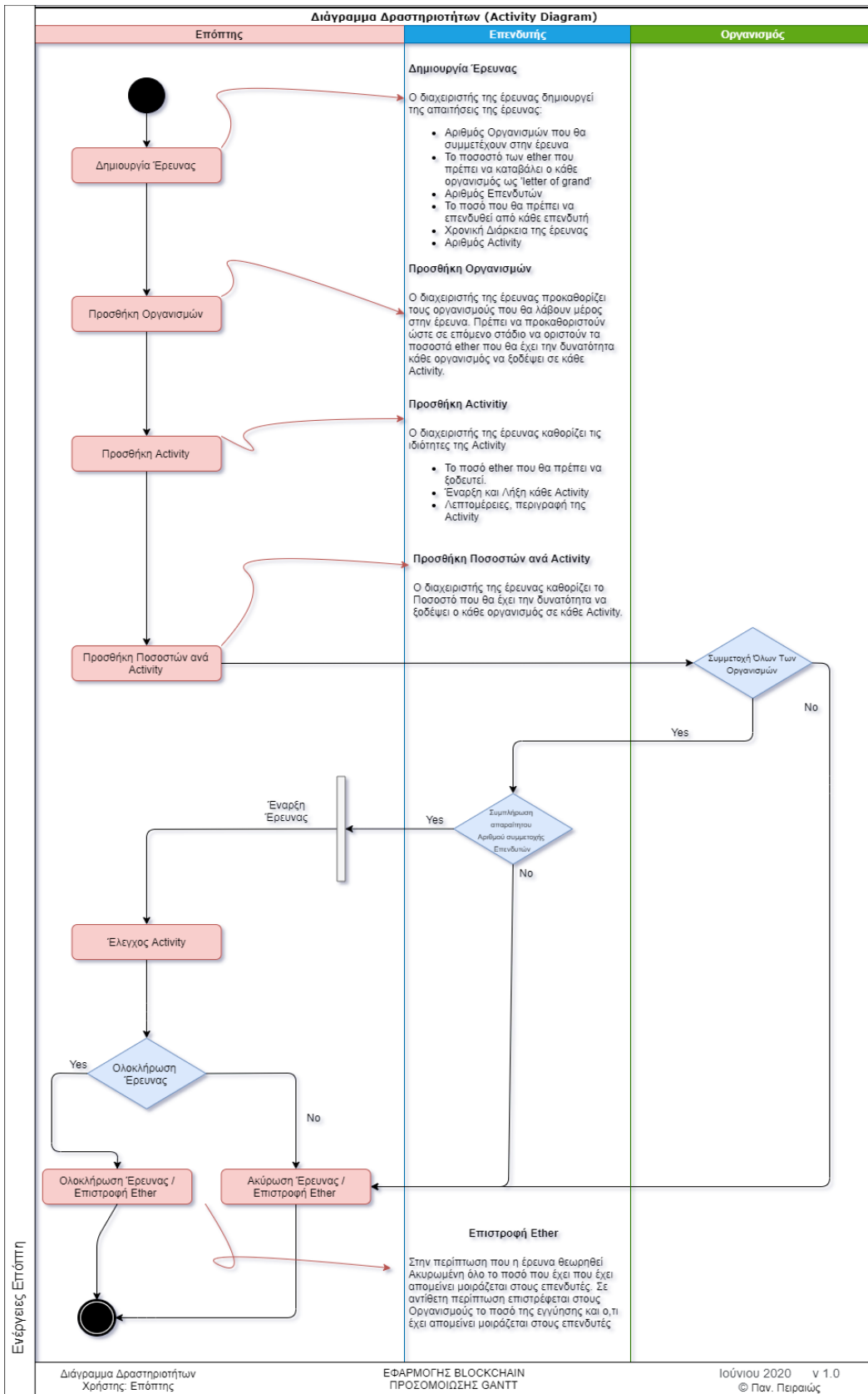
Από την μεριά του χρήστη, δεν χρειάζονται κάποιες εξειδικευμένες απαιτήσεις. Αυτό που χρειάζεται ένας χρήστης για να μπορέσει να χρησιμοποιήσει την εφαρμογή είναι ένας Browser, συνιστάται ο Google Chrome, ο οποίος να υποστηρίζει το πρόσθετο MetaMask.

Τέλος, ο χρήστης θα πρέπει να έχει ή να δημιουργήσει λογαριασμό Ethereum. Ο λογαριασμός Ethereum δημιουργείται είτε μέσω του MetaMask είτε εάν ήδη διαθέτει λογαριασμό, θα πρέπει να τον εισάγει στο πρόσθετο αυτό.

4.3 Περιπτώσεις Χρήσης

Επόπτης: Ο Επόπτης είναι εκείνος ο οποίος δημιουργεί την διαδικασία της Έρευνας στην εφαρμογή. Είναι άτομο αρμόδιο να ορίσει τις Activities της έρευνας, τα ποσά που πρέπει να καταθέσουν οι Οργανισμοί και οι Επενδυτές για να συμμετάσχουν στην έρευνα. Επιπλέον είναι εκείνος ο οποίος μπορεί και αξιολογεί τα στάδια της έρευνας. Κάθε στάδιο για να θεωρηθεί ολοκληρωμένο, και κατά συνέπεια να συνεχίσει να είναι ενεργή η έρευνα, πρέπει να αξιολογείται. Αξιολογούνται όλα τα παραδοτέα και οι αγορές που έχουν πραγματοποιήσει οι Οργανισμοί σε εκείνη την φάση. Ο επόπτης είναι εκείνος που θα κρίνει εάν μια δραστηριότητα έχει ολοκληρωθεί επιτυχώς ή όχι.

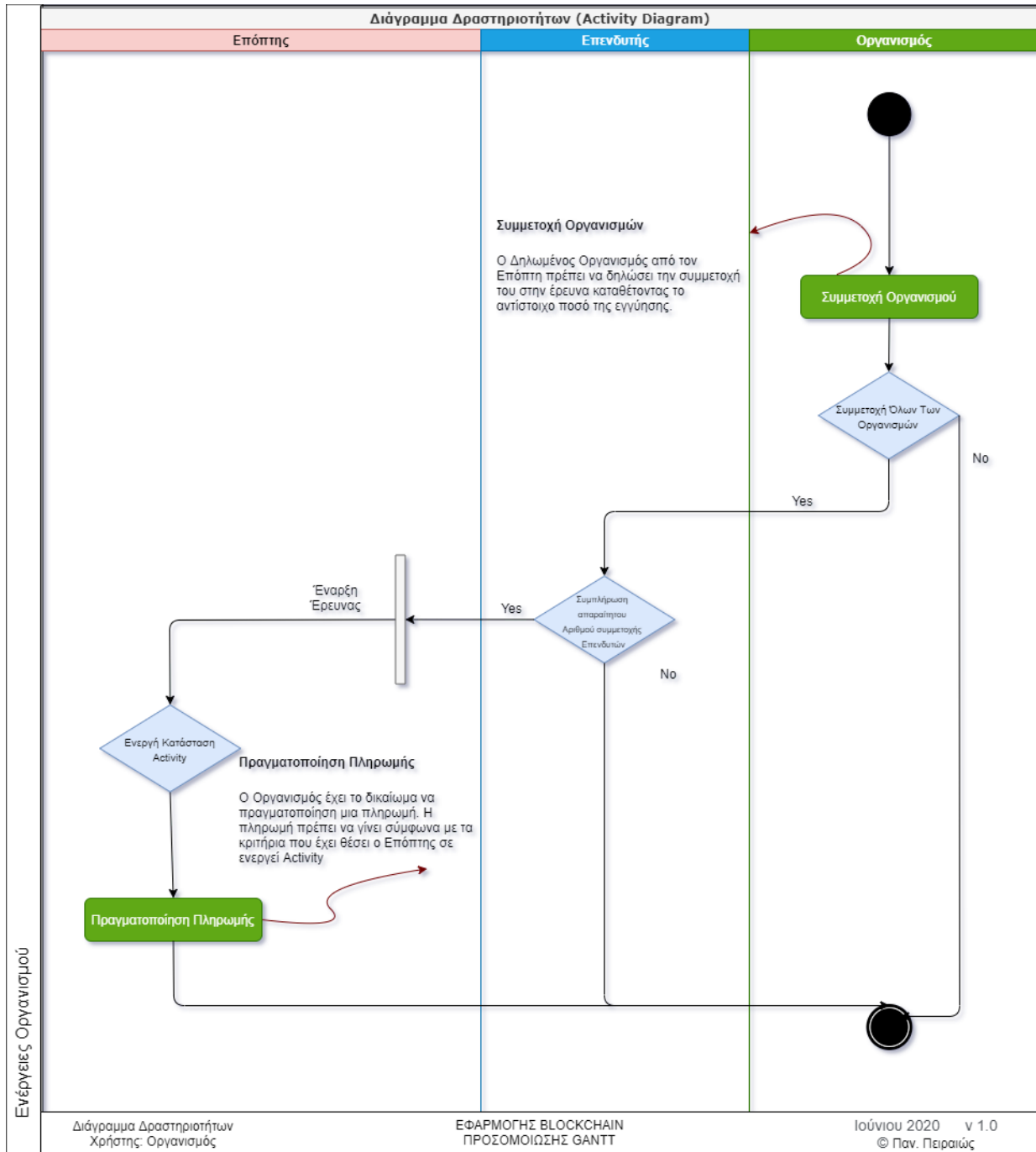
Στην παρακάτω εικόνα μπορούμε να δούμε το Διάγραμμα Δραστηριοτήτων για τον επόπτη.



Εικόνα 13: Διάγραμμα Δραστηριοτήτων - Επόπτης

Οργανισμοί: Ως Οργανισμούς αναφέρουμε τις ομάδες εκείνες που θα λάβουν μέρος στην έρευνα με σκοπό την περάτωσή της. Οι Οργανισμοί που θα λάβουν μέρος στην έρευνα είναι δηλωμένοι από την Επόπτη κατά την δημιουργία της Έρευνας.

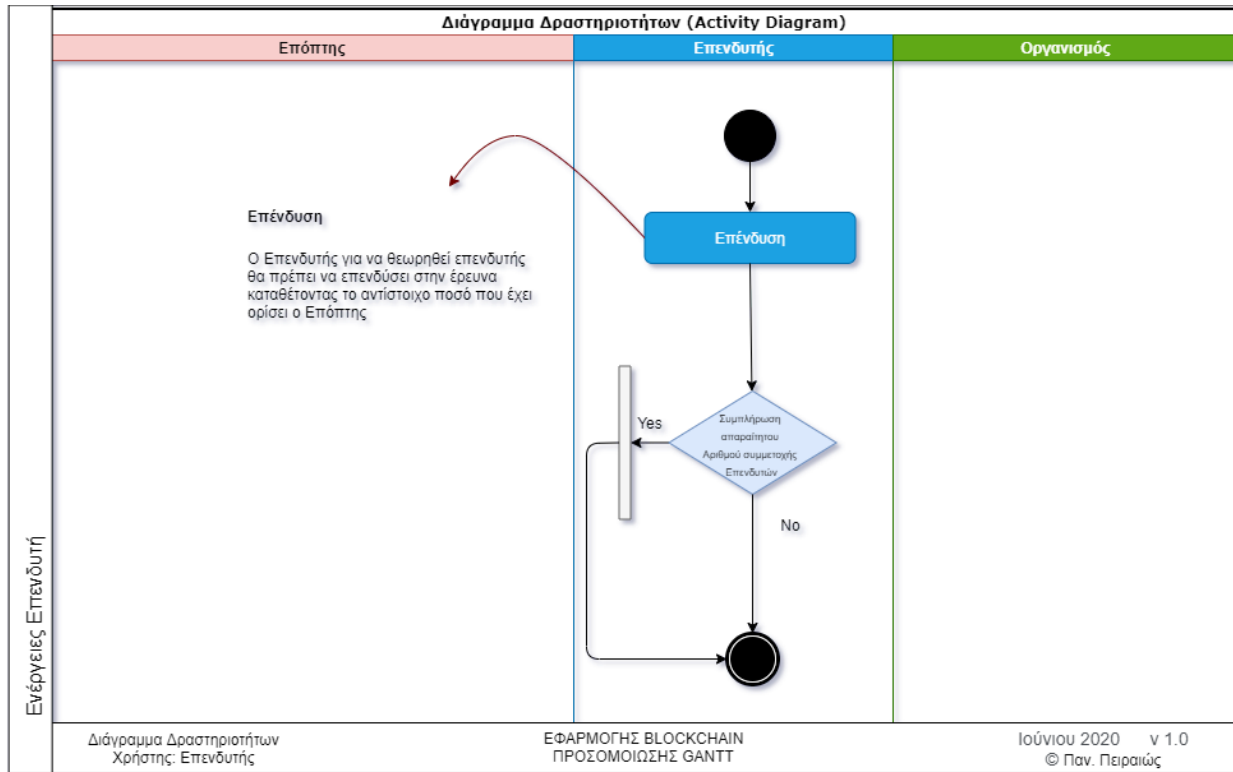
Στην παρακάτω εικόνα μπορούμε να δούμε το Διάγραμμα Δραστηριοτήτων για τους Οργανισμούς.



Εικόνα 14: Διάγραμμα Δραστηριοτήτων - Οργανισμός

Επενδυτές: Ως Επενδυτές αναφέρουμε τις ομάδες εκείνες που θα εμπιστευτούν στους Οργανισμούς ένα οικονομικό ποσό και θα γίνουν χρηματοδότες της έρευνας.

Στην παρακάτω εικόνα μπορούμε να δούμε το Διάγραμμα Δραστηριοτήτων για τους Επενδυτές.



Εικόνα 15: Διάγραμμα Δραστηριοτήτων - Επενυτής

5. Ανάπτυξη Συστήματος

Στο κεφάλαιο αυτό θα δούμε τα βήματα και κάποια σημεία του κώδικα σχετικά με την ανάπτυξη του συστήματός μας.

5.1 Solidity

Το πρώτο στάδιο της Ανάπτυξης του Συστήματος είναι η δημιουργία της Smart Contract με την βοήθεια της Solidity.

Η έκδοση του Solidity που θα χρησιμοποιήσουμε είναι η 0.4.22. Παρακάτω παρατίθενται οι βασικές συναρτήσεις από τον κώδικα του Solidity.

Ξεκινώντας να γράφουμε Solidity η πρώτη γραμμή πρέπει να αναγράφει ποια έκδοση θα χρησιμοποιήσουμε. Αυτή η έκδοση θα χρησιμοποιηθεί για να γίνει Compile και Deploy η Smart Contract.

```
pragma solidity ~0.4.22;
```

Παρατηρώντας τον κώδικα του Solidity έχουμε δημιουργήσει δύο Contract.

Το Contract Application καλείται την πρώτη φορά που δημιουργείται η Smart Contract από εκείνον που κάνει Deploy την εφαρμογή στο δίκτυο του Blockchain.

```
contract Application {...}
```

Το Contract Investment είναι εκείνο που καλείται κάθε φορά όταν ο Επόπτης δημιουργεί μία έρευνα και τις ιδιότητες αυτές.

```
contract Investment {...}
```

Στην συνέχεια ορίζονται οι μεταβλητές του συστήματος. Ουσιαστικά αυτές οι μεταβλητές είναι και ο αποθηκευτικός χώρος του Smart Contract. Κάθε φορά που καλείται κάποια συνάρτηση οι μεταβλητές είτε αλλάζουν είτε προστίθενται πράγματα.

```
address master;  
  
uint numOrganizations;  
uint numInvestors;  
  
uint contribution;  
uint contributionorganization;  
uint availableetherforactivities;
```

```

uint nowOrganizationsAddedDeclaireMaster;
uint nowOrganizationsAdded;
uint nowInvestorsAdded;

uint activities;

uint maxTimesOfProject = 0;
uint maxTimesOfProjectTemp;

State statusOfResearch;
uint numberOfCompletedActivities = 0;

mapping(address => bool) public organizationsmaster; // Mapping με τις
διευθύνσεις των οργανισμών όπως έχει δηλωθεί από τον master
address[] public organizationsaddressesdeclairemaster; // Λίστα με τις
διευθύνσεις των οργανισμών όπως έχει δηλωθεί από τον master
mapping(address => bool) public organizations; // Mapping με τις διευθύνσεις
των οργανισμών που έχουν συμμετάσχει στην έρευνα καταθέτοντας το ανάλογο ποσό
address[] public organizationsaddresses; // Λίστα με τις διευθύνσεις των
οργανισμών που έχουν συμμετάσχει στην έρευνα καταθέτοντας το ανάλογο ποσό
bool public organizationsaddresseslength = false;

mapping(uint => bool) public check_complete_activity;

mapping(address => bool) public investors;
address[] public investorsaddresses;
bool public investorsaddresslength = false;

enum State {Inactive, Active, Pending, Cancelled, Completed, InactiveClosed,
CancelledClosed, CompletedClosed}

DetailActivities[] public activitiesTable;
struct DetailActivities {
    uint value;
    uint leftvalue;
    uint timeSecStartActivity;
    uint timeSecStopActivity;
    uint timeStartActivity;
    uint timeStopActivity;
    string detail;
    uint perscentagecoverage;
    State statusActivity;
    mapping(address => uint) available_ether_to_spent_per_organization;
    mapping(address => uint) perscentage_per_organization;
}

DetailPurchase[] public detailPurchase;
struct DetailPurchase {
    uint activityNumber;
    uint value;
    string detail;
    address seller;
    address organizationmakepayment;
}

```

Σε επόμενο βήμα ορίζονται κάποιες από τις γενικές απαιτήσεις που πρέπει να έχουν οι συναρτήσεις της Smart Contract.

```
modifier requireToBeMaster() {  
    require(master == msg.sender);  
    _;  
}
```

Αυτές οι απαιτήσεις τοποθετούνται στις αντίστοιχες συναρτήσεις με αποτέλεσμα εάν δεν εκπληρώνεται η απαίτηση τότε η συνάρτηση να μην μπορεί να εκτελεστεί. Για παράδειγμα μία απαίτηση φαίνεται παραπάνω. Η συγκεκριμένη απαίτηση, όταν τοποθετηθεί σε κάποια μέθοδο, τότε η μέθοδος θα μπορεί να εκτελεστεί μόνο εάν ο καλών είναι ο Master – Επόπτης – Δημιουργός της Έρευνας.

Παρακάτω παραθέτουμε τα ονόματα των βασικών συναρτήσεων της Smart Contract.

```
constructor (uint _numOrganizations, uint _numInvestors, uint  
_maxTimesOfProject, uint _contribution, uint  
_contributionorganizationpercentage, uint _activities, address _master)
```

Ο Constructor είναι η συνάρτηση η οποία καλείται όταν ο Επόπτης δημιουργεί μία καινούργια έρευνα. Οι μεταβλητές που βρίσκονται μέσα στην παρένθεση είναι εκείνες που πρέπει να δηλωθούν από την Επόπτη κατά την δημιουργία της έρευνας.

Για μεγαλύτερη κατανόηση του κώδικα και της σειράς που πρέπει να εκτελούνται οι συναρτήσεις που αποτελούν την Smart Contract, μπροστά από κάθε συνάρτηση έχει προστεθεί ένα γράμμα της αγγλική αλφαβήτου. Η διαδικασία της εκτέλεσης των συναρτήσεων θα πρέπει να πραγματοποιείται με συγκεκριμένη σειρά.

```
function B AddOrganizations
```

Την συνάρτηση αυτή έχει δικαίωμα να την εκτελέσει μόνο ο Επόπτης. Κατά την εκτέλεση αυτής της συνάρτησης ο Επόπτης ουσιαστικά δηλώνει ποιοι Οργανισμοί θα λάβουν μέρος στην Έρευνα. Κανένας άλλος Οργανισμός δεν μπορεί συμμετέχει στην Έρευνα. Η δήλωση των Οργανισμών γίνεται με βάση το Account που διαθέτουν στο Ethereum Network.

```
function C AddActivity
```

Την συνάρτηση αυτή έχει δικαίωμα να την εκτελέσει μόνο ο Επόπτης. Με την εκτέλεση αυτής της συνάρτησης ο Επόπτης δηλώνει τα Activity που θα έχει η συγκεκριμένη έρευνα. Δηλώνει το ποσό που μπορεί να καταναλωθεί στην συγκεκριμένη Activity. Επίσης δηλώνει το πότε θα ξεκινήσει ουσιαστικά η Activity και πότε θα τελειώσει.

`function D_AddPercentageInActivity`

Την συνάρτηση αυτή έχει δικαίωμα να την εκτελέσει μόνο ο Επόπτης. Η εκτέλεση αυτή της συνάρτησης είναι προαιρετική. Εκτελώντας αυτή την συνάρτηση δηλώνεται το ποσοστό που μπορεί να ξοδέψει ο κάθε οργανισμός σε σχέση με τα χρήματα που είχε ορίσει από πριν για την συγκεκριμένη Activity. Το ποσοστό δεν πρέπει να ξεπερνάει αθροιστικά το 100% και επίσης μπορεί να είναι 0%. Όταν το ποσοστό είναι 0% τότε η Activity απλά εκτελείται χωρίς να μπορούν να πραγματοποιήσουν κάποια πληρωμή οι Οργανισμοί.

`function E_OrganizationsPayment`

Την συνάρτηση αυτή έχουν δικαίωμα να την εκτελέσουν μόνο οι Οργανισμοί που έχει δηλώσει ο Επόπτης και μόνο μια φορά. Ουσιαστικά με την εκτέλεση αυτής της συνάρτησης οι Οργανισμοί αποδέχονται τους όρους της Έρευνας. Εάν έχει οριστεί το ποσοστό το οποίο πρέπει να υποβάλουν οι οργανισμοί ως εγγύηση για να συμμετάσχουν στην έρευνα, στο στάδιο αυτό ο Account του Οργανισμού χρεώνεται με τον συγκεκριμένο ποσό. Το ποσό αυτό πηγαίνει ως απόθεμα στην Smart Contract.

`function F_MakeAppanage`

Την συνάρτηση αυτή έχουν δικαίωμα να την εκτελέσουν μόνο οι επενδυτές. Περιορισμός στο ποιος θα είναι επενδυτής δεν έχει οριστεί. Όπως θέλει να επενδύσει στην έρευνα επενδύει. Ο επόπτης έχει ορίσει το ποσό που πρέπει να υποβάλλει ο κάθε επενδυτής. Για να θεωρηθεί κάποιος Account ως επενδυτής εκτελεί αυτή την συνάρτηση και στο στάδιο αυτό ο Account του Επενδυτή χρεώνεται με τον αντίστοιχο ορισμένο ποσό. Το ποσό αυτό πηγαίνει ως απόθεμα στην Smart Contract.

`function G_checkStatusOfActivities`

Την συνάρτηση αυτή έχει δικαίωμα να την εκτελέσει οποιοσδήποτε. Δεν χρειάζεται να υπάρχει κάποιος περιορισμός για το ποιος θα εκτελέσει την συγκεκριμένη συνάρτηση με την Smart Contract. Ο ρόλος της συγκεκριμένης συνάρτησης είναι να ελέγχει τις Activities και να τους αλλάζει καταστάσεις. Παράδειγμα, εάν κάποια Activity έχει υπερβεί το χρονικό περιθώριο που της έχει ορίσει ο Επόπτης τότε η κατάστασή της γίνεται Pending μέχρι να αποφασίσει ο επόπτης εάν θεωρεί τη συγκεκριμένη Activity ολοκληρωμένη επιτυχώς ή όχι. Επιπλέον η συνάρτηση αυτή μετατρέπει μια Activity από Inactive (μη ενεργή) σε Active (ενεργή) όταν ο παρών χρόνος βρίσκεται στα όρια έναρξης και λήξης που έχει θέσει ο Επόπτης.

`function H_PaySeller`

Την συγκεκριμένη συνάρτηση έχει δικαίωμα να την εκτελέσει μόνο κάποιος Οργανισμός. Για να την εκτελέσει όμως θα πρέπει να έχει οριστεί από τον Επόπτη το ποσοστό Ether που μπορεί να ξοδέψει ο συγκεκριμένος οργανισμός στην συγκεκριμένη Activity. Η συνάρτηση αυτή εκτελείται μόνο όταν η Activity και η κατάσταση ολόκληρης της έρευνας είναι ενεργή.

```
function I_changeStatusOfActivity
```

Την συνάρτηση αυτή έχει δικαίωμα να την εκτελέσει μόνο ο Επόπτης. Η συγκεκριμένη συνάρτηση εκτελείται από τον επόπτη ώστε να αλλάξει κατάσταση σε μια Activity. Ο επόπτης έχει το δικαίωμα να θεωρήσει μια Activity επιτυχώς ολοκληρωμένη ή όχι.

```
function returnMoney()
```

Την συνάρτηση αυτή έχει δικαίωμα να την εκτελέσει μόνο ο Επόπτης και μόνο κάτω από συγκεκριμένες συνθήκες. Εκτελώντας αυτή την συνάρτηση όταν η κατάσταση της έρευνας είναι Completed ή Cancelled (ολοκληρωμένη ή μη) τα χρήματα που έχουν απομείνει στην Smart Contract περνάνε τους αντίστοιχους λογαριασμούς. Η επιστροφή χρημάτων γίνεται με τους παρακάτω τρόπους:

- Completed: Τα ether που δόθηκαν από τους οργανισμούς ως εγγύηση γυρνάνε σε αυτούς. Το υπόλοιπο, εάν υπάρχει, μοιράζεται στους επενδυτές.
- Cancelled: Όλο το ποσό που έχει απομείνει στην Smart Contract μοιράζεται στους επενδυτές.

5.2 Deploy Smart Contract στο Infura

Αφού δημιουργηθεί ο κώδικας της διεπαφής, επόμενο βήμα είναι το Deploy της Smart Contract μέσω του Infura στο δίκτυο του Ethereum (Rinkeby Network).

Παίρνοντας τον κώδικα Solidity, αυτός γίνεται Compile από τον παρακάτω κώδικα JavaScript (compile.js)

```
const path = require('path');
const solc = require('solc');
const fs = require('fs-extra');

const buildPath = path.resolve(__dirname, 'build');
fs.removeSync(buildPath);

const applicationPath =
path.resolve(__dirname, 'soliditycontract', 'Application.sol');
const source = fs.readFileSync(applicationPath, 'utf8');
const output = solc.compile(source, 1).contracts;

fs.ensureDirSync(buildPath);

for (let contract in output){
  fs.outputJsonSync(
    path.resolve(buildPath, contract.replace(':', '') + '.json'),
    output[contract]
  );
}
```

Το αποτέλεσμα του παραπάνω κώδικα είναι η δημιουργία δυο αρχείων ABI (γλώσσα μηχανής). Δημιουργούνται δύο αρχεία διότι όπως αναφέρθηκε παραπάνω το Smart Contract που δημιουργήσαμε αποτελείται από δυο Contract.

Αφού δημιουργηθούν τα δύο αυτά αρχεία, πρέπει να γίνει deploy ο κώδικα σε δίκτυο. Για να το επιτύχουμε αυτό χρησιμοποιούμε τον παρακάτω κώδικα (deploy.js)

```
const HDWalletProvider = require ('truffle-hdwallet-provider');
const Web3 = require('web3');
const compiledApplication = require('./build/Application.json');

const provider = new HDWalletProvider(
  'xxxxxxxxxxxxxxxxxxxxxxxx',
  'https://rinkeby.infura.io/v3/d5860a644ed34a38a59f4d5e58ed6a6c'
);

const web3 = new Web3(provider);

const deploy = async () => {
  const accounts = await web3.eth.getAccounts();

  console.log('Attempting to deploy from account', accounts[0]);

  const result = await new
web3.eth.Contract(JSON.parse(compiledApplication.interface))
  .deploy({data: '0x' + compiledApplication.bytecode})
  .send({ gas: '4712388', from: accounts[0] });

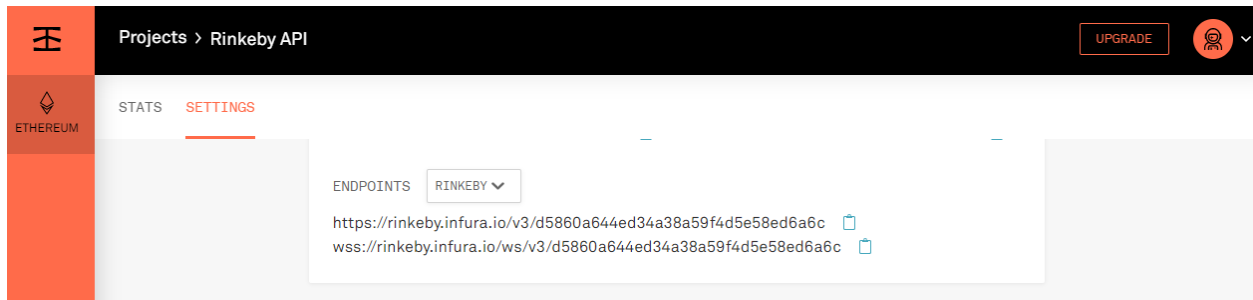
  console.log('Contract deployed to', result.options.address);
};

deploy();
```

Στο σημείο αυτό η συμβολοσειρά 'xxxxxxxxxxxxxxxxxxxxxxxx' που έχει ήδη τοποθετηθεί, θα πρέπει να αντικατασταθεί με την φράση κλειδί που ξεκλειδώνει ο λογαριασμός μας στο Ethereum. Χρειάζεται αυτή η φράση για να ενεργοποιηθεί ο λογαριασμός μας ο οποίος έχει συσχετιστεί με το αποκάτω URL.

Για λόγους ασφαλείας παρατίθεται με 'xxxxxxxxxxxxxxxxxxxxxxxx'.

Το URL έχει παραχθεί έχοντας δημιουργήσει λογαριασμό στο Infura και στην συνέχεια κάνοντας χρήση του Rinkeby API που μας παρέχεται.



Εικόνα 16: Rinkeby API Infura

Πραγματοποιούμε λοιπόν το Deploy εκτελώντας το παραπάνω αρχείο οπότε η Smart Contract πλέον αναρτάται στο Rinkeby Network. Κατανοούμε ότι έχει ολοκληρωθεί η διαδικασία

επιτυχώς όταν μας επιστρέφεται ένας δεκαεξαδικός μοναδικός αριθμός ο οποίος αναπαριστά την Smart Contract.

0xfE6f690496779D08dbc0a3758fe0d8D5638FAd92

Τον συγκεκριμένο μπορούμε να τον αναζητήσουμε στο Etherscan (Rinkeby Network).

The screenshot shows the Etherscan interface for the Rinkeby Testnet Network. The main heading is "Contract 0xfE6f690496779D08dbc0a3758fe0d8D5638FAd92". Below this, there are two panels: "Contract Overview" showing a balance of 0 Ether, and "More Info" showing "My Name Tag: Not Available" and "Contract Creator: 0x8264429f1720da4... at txn 0xf75058754700c98...".

Below the panels is a "Transactions" section with tabs for "Internal Txns", "Contract", and "Events". It shows "Latest 3 from a total of 3 transactions".

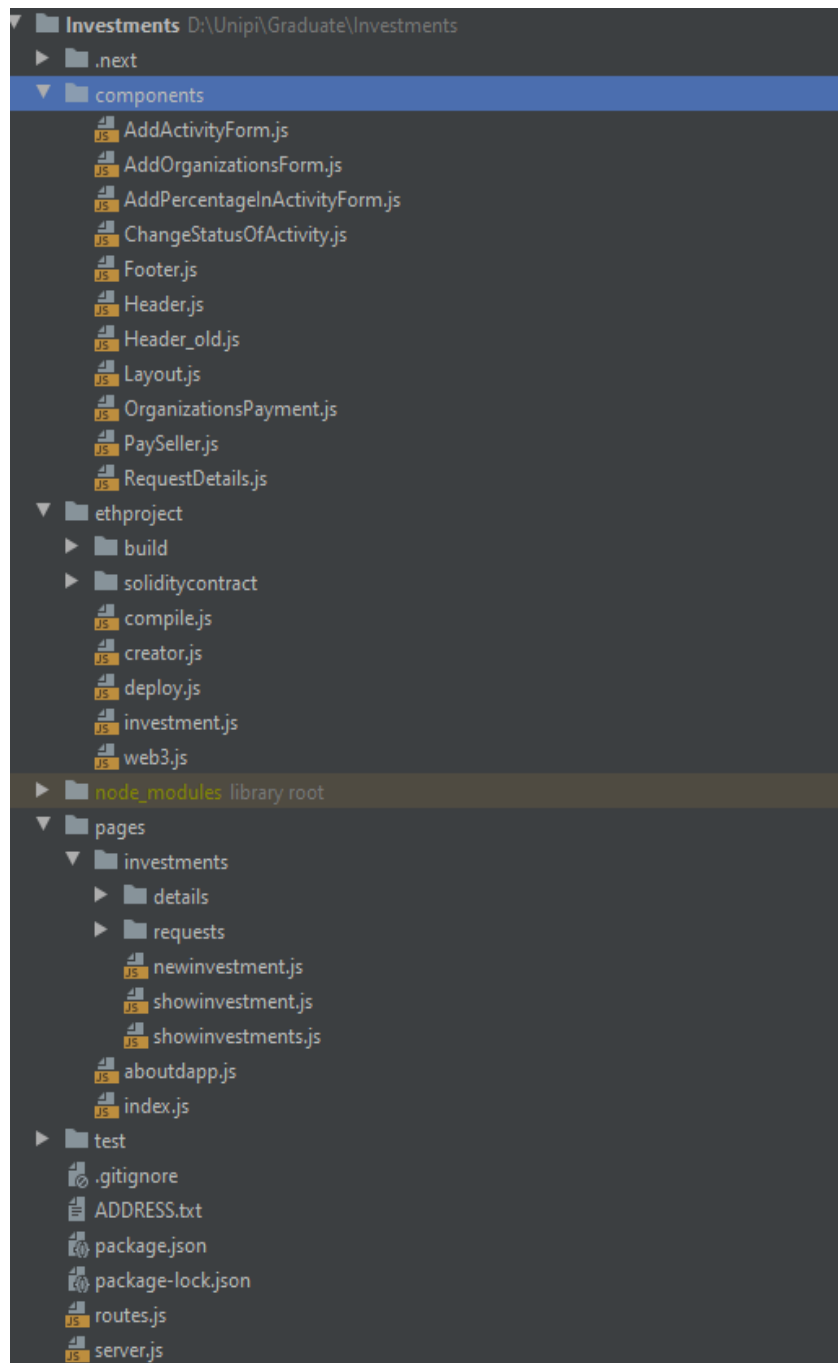
Txn Hash	Block	Age	From	To	Value	[Txn Fee]
0xdd0008378a6154...	6816477	3 days 18 hrs ago	0x8264429f1720da4...	IN 0xfe6f690496779d0...	0 Ether	0.002047015
0xd07fa64aac9e9d3...	6816338	3 days 19 hrs ago	0x8264429f1720da4...	IN 0xfe6f690496779d0...	0 Ether	0.002062015
0xf75058754700c98...	6816331	3 days 19 hrs ago	0x8264429f1720da4...	IN Contract Creation	0 Ether	0.002214192

[Download CSV Export]

Εικόνα 17: Etherscan

5.3 Node.js & React.js

Κάνοντας χρήση React και Node έχουν δημιουργηθεί κομμάτια κώδικα «Component» τα οποία βοηθάνε στην καλύτερη οργάνωση του κώδικα, την εύκολη αναπαράσταση συγκεκριμένων τμημάτων από σελίδα σε σελίδα και την καλύτερη διαχείριση των συναρτήσεων.



Εικόνα 18: Διάταξη Κώδικα

6. Λειτουργικό Πρωτότυπο

Στο παρόν κεφάλαιο θα παρουσιάσουμε ένα πρότυπο παράδειγμα δημιουργίας και διαχείρισης Έρευνας με την βοήθεια της DApp που δημιουργήσαμε.

Από το κεντρικό menu στο πάνω μέρος της σελίδας επιλέγουμε «Δημιουργία Έρευνας». Στην συνέχεια μας εμφανίζεται η παρακάτω εικόνα.

localhost:3000/investments/new x +

localhost:3000/investments/newinvestment

Home Έρευνες Δημιουργία Έρευνας Λεπτομέρειες Έρευνας About DApp

Δημιουργία καινούργιας Έρευνας

Αριθμός Συμμετεχόντων Οργανισμών
2 Αριθμός

Αριθμός Συμμετεχόντων Επενδυτών
2 Αριθμός

Μέγιστη Διάρκεια Έρευνας
3600 Δευτερόλεπτα

Συνεισφορά Επενδυτών ανά Επενδυτή
1 ether

Συνεισφορά Οργανισμών σε ποσοστό
50 Ποσοστό

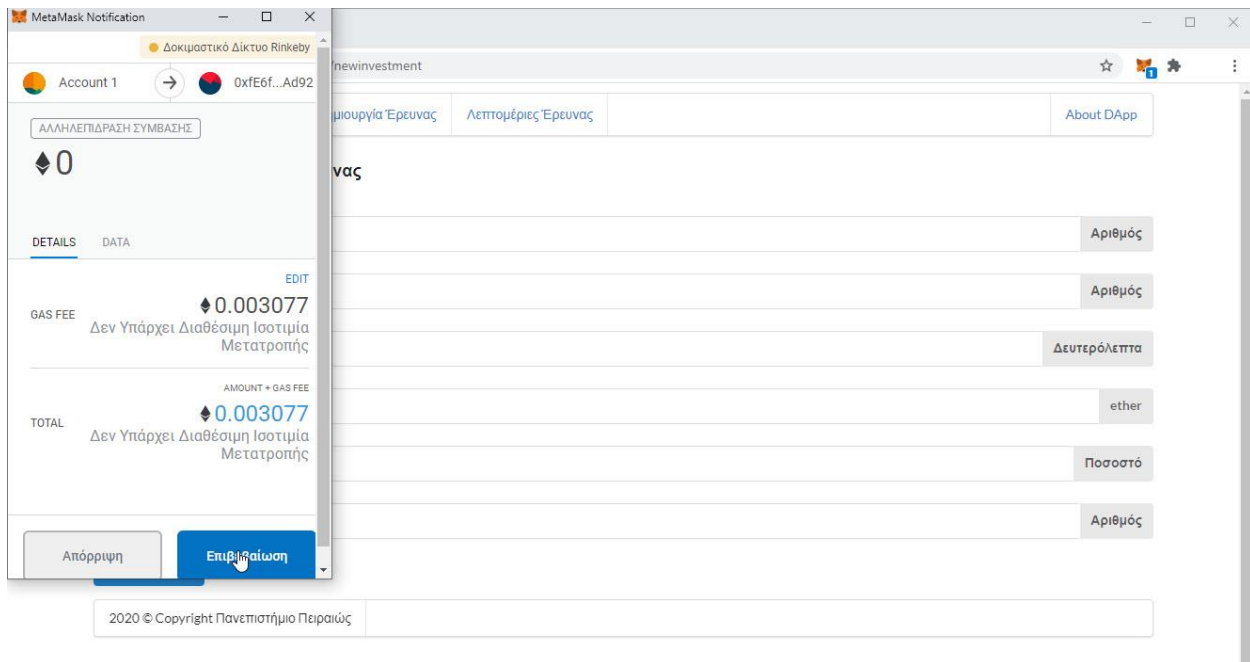
Αριθμός Activities της έρευνας
3 Αριθμός

Δημιουργία

2020 © Copyright Πανεπιστήμιο Πειραιώς

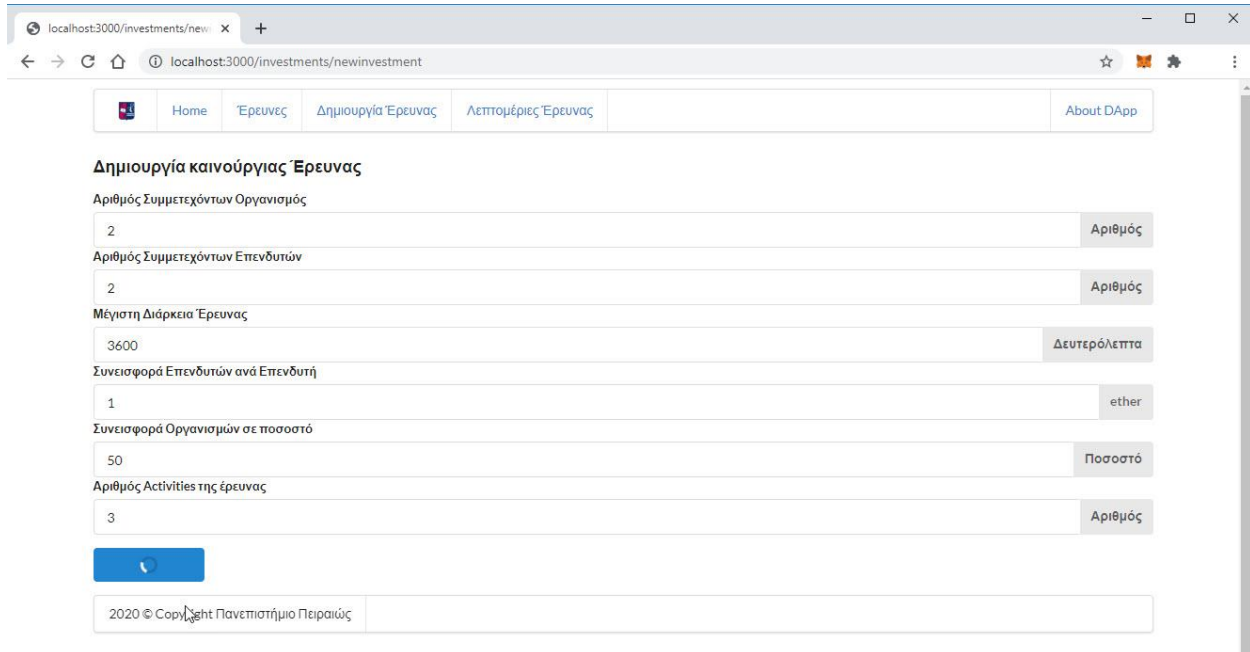
Εικόνα 19: Δημιουργία Έρευνας

Συμπληρώνουμε τα απαραίτητα στοιχεία της έρευνας και κάνουμε κλικ στο κουμπί «Δημιουργία». Το πρόσθετο MetaMask θα μας ζητήσει επιβεβαίωση αλληλεπίδρασης.

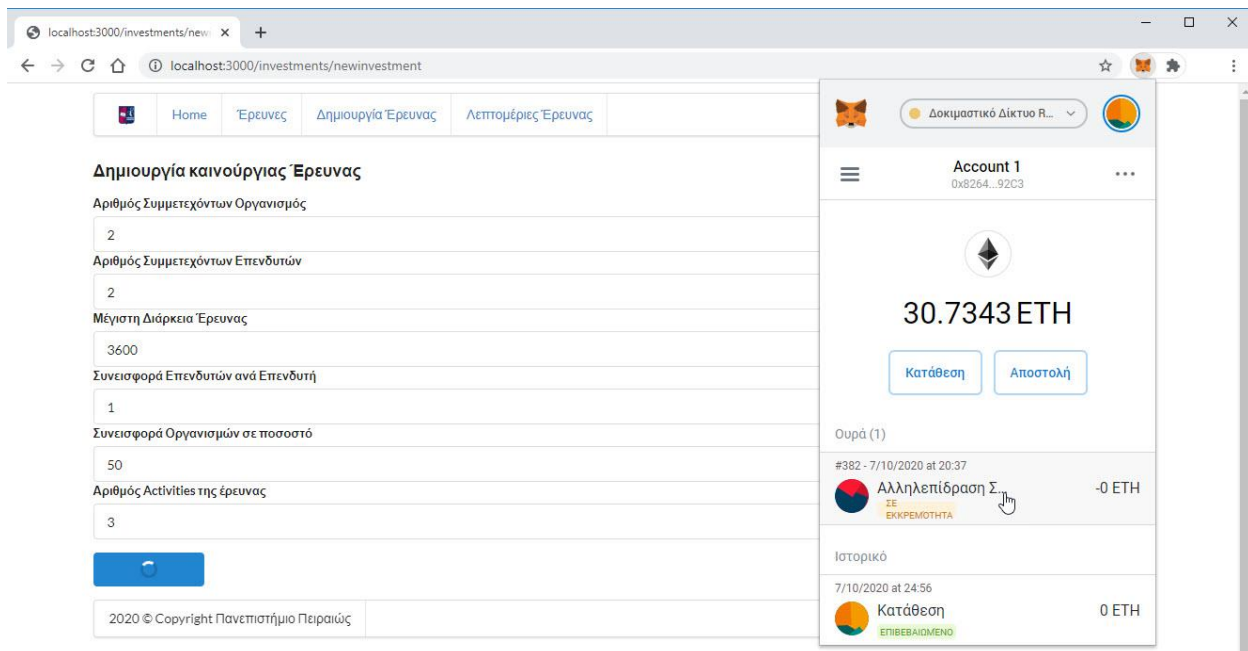


Εικόνα 20: Ανάδραση με MetaMask

Πατώντας το κουμπί «Επιβεβαίωση» αποδεχόμαστε το κόστος δημιουργίας και δημιουργούμε την έρευνα. Ο λογαριασμός ο οποίος δημιούργησε την έρευνα είναι πλέον ο Επόπτης της έρευνας.

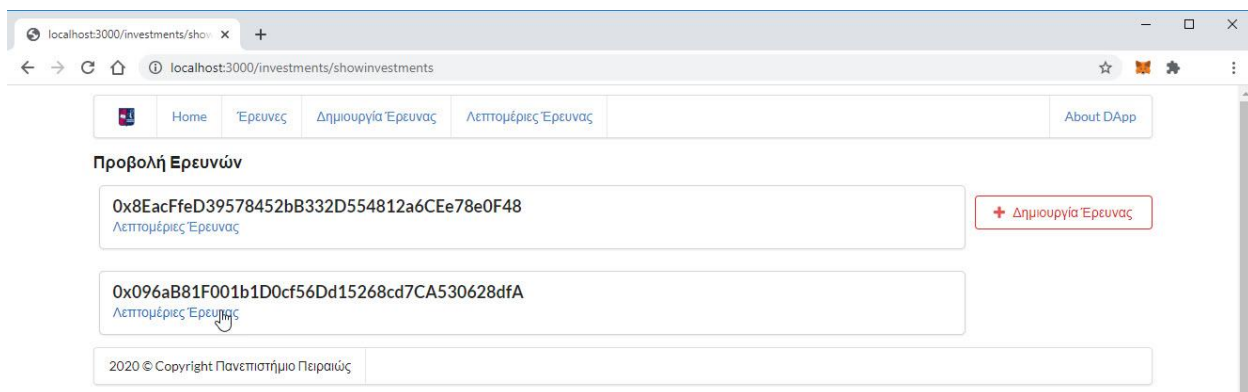


Εικόνα 21: Αναμονή απόκρισης



Εικόνα 22: Επαλήθευση Αλληλεπίδρασης

Αφού ολοκληρωθεί η διαδικασία και καταχωρηθεί η αλληλεπίδραση στο Rinkeby Network η εφαρμογή μας ανακατευθύνει στην σελίδα «Έρευνες». Στην σελίδα αυτή εμφανίζονται όλες οι έρευνες που έχουν δημιουργηθεί.



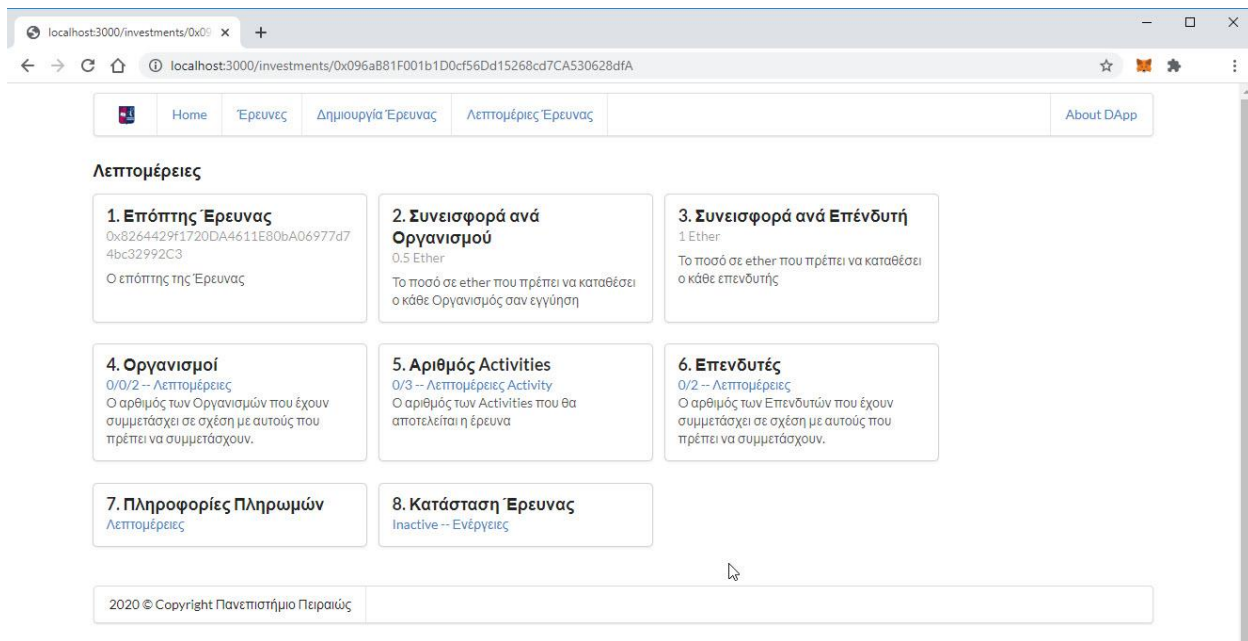
Εικόνα 23: Έρευνες

Κάνοντας κλικ στο κουμπί «Λεπτομέρειες Έρευνας» ανακατευθυνόμαστε στην σελίδα με τις πληροφορίες για την έρευνα που επιλέξαμε. Στην σελίδα αυτή θα δούμε 8 σημεία.

1. Επόπτης Έρευνας: μας εμφανίζει τον επόπτη της έρευνας.
2. Συνεισφορά ανά Οργανισμό: μας εμφανίζει το ποσό που πρέπει να προσφέρει ο κάθε οργανισμός ως εγγύηση ώστε να συμμετάσχει στην έρευνα.
3. Συνεισφορά ανά Επενδυτή : μας εμφανίζει το ποσό που πρέπει να προσφέρει ο επενδυτής ώστε να θεωρηθεί επενδυτής της έρευνας.
4. Οργανισμοί: Στο σημείο αυτό μπορούμε να ανακτήσουμε άμεσα πολύτιμες πληροφορίες για την έρευνα και τους οργανισμούς που θα συμμετέχουν σε αυτή. Στο παράδειγμά μας

εμφανίζονται οι αριθμοί 0/0/2. Το πρώτο 0 μας ενημερώνει πως ακόμα κανένας οργανισμός δεν έχει λάβει μέρος στην έρευνα. Το δεύτερο 0 μας ενημερώνει πως ο Επόπτης δεν έχει ορίσει κάποιον οργανισμό που θα λάβει μέρος στην έρευνα. Ο αριθμός 2 μας ενημερώνει για το πόσοι οργανισμοί θα λάβουν χώρα στην συγκεκριμένη έρευνα.

5. Αριθμός Activities: : Στο σημείο αυτό μπορούμε να ανακτήσουμε άμεσα πολύτιμες πληροφορίες σχετικά με τις Activities της έρευνας. Το 0 μας ενημερώνει πως καμία Activity δεν έχει δηλωθεί από τον Επόπτη ακόμα. Ο αριθμός 3 μας ενημερώνει πως η έρευνα αποτελείται από 3 Activities.
6. Επενδυτές: Στο σημείο αυτό μπορούμε να ανακτήσουμε άμεσα πολύτιμες πληροφορίες σχετικά με τους επενδυτές της έρευνας. Ο αριθμός 0 μας ενημερώνει πως κανένας επενδυτής δεν έχει επενδύσει στην έρευνα ενώ ο αριθμός 2 μας ενημερώνει πως ο Επόπτης έχει δημιουργήσει την έρευνα με απαραίτητα 2 επενδυτές.
7. Πληροφορίες Πληρωμών : Εσωτερικά της συγκεκριμένης πληροφορίας θα έχουμε την δυνατότητα να δούμε αναλυτικά της πληρωμές που πραγματοποιήθηκαν από τους οργανισμούς κατά της διάρκεια της έρευνας.
8. Κατάσταση Έρευνας: Σε αυτό το σημείο μας εμφανίζεται η κατάσταση της έρευνας. Οι καταστάσεις είναι οι παρακάτω:
 - **Inactive:** Στην κατάσταση αυτή η έρευνα δεν έχει ξεκινήσει ακόμα.
 - **Active:** Στην κατάσταση αυτή η έρευνα είναι σε εξέλιξη.
 - **Pending:** Στην κατάσταση αυτή η έρευνα έχει παγώσει και περιμένει κάποια ενέργεια από τον επόπτη.
 - **Cancelled:** Στην κατάσταση αυτή ο επόπτης έχει θεωρήσει κάποια Activity ακυρωμένη άρα και ολόκληρη την έρευνα. Η κατάσταση είναι αναστρέψιμη μόνο από τον επόπτη.
 - **Completed:** Στην κατάσταση αυτή ο επόπτης έχει θεωρήσει ολοκληρωμένη την έρευνα. Η κατάσταση είναι αναστρέψιμη μόνο από τον επόπτη.
 - **Cancelled Closed:** Στην κατάσταση αυτή ο επόπτης έχει θεωρήσει την έρευνα ακυρωμένη. Τα ποσά που απέμειναν στην έρευνα επιστρέφονται στους επενδυτές.
 - **Completed Closed:** Στην κατάσταση αυτή ο επόπτης έχει θεωρήσει την έρευνα ολοκληρωμένη. Οι οργανισμοί παίρνουν πίσω την εγγύηση που είχαν καταβάλει και οι επενδυτές τα χρήματα που ίσως περίσσεψαν.







Εικόνα 24: Λεπτομέρειες Έρευνας

Οι ενέργειες για να ξεκινήσει η έρευνα πρέπει να γίνουν με συγκεκριμένη σειρά.

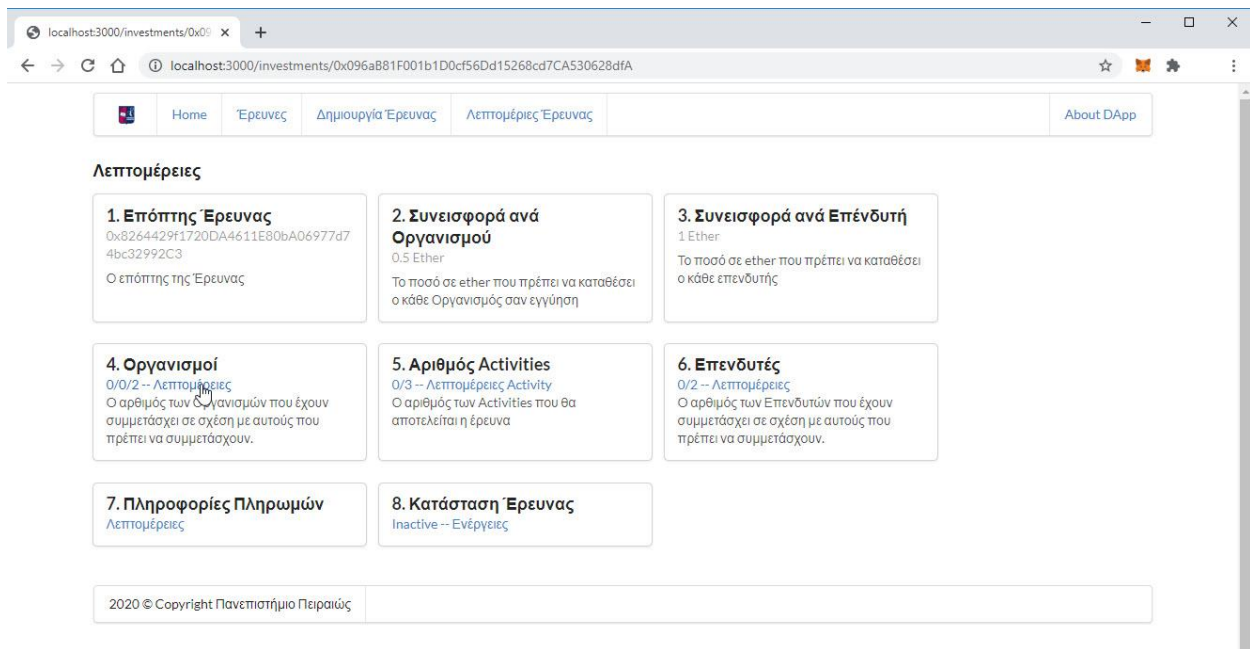
1. Ο επόπτης ορίζει ποιοι οργανισμοί θα συμμετέχουν στην έρευνα.
2. Ο επόπτης ορίζει τις Activities.
3. Ο επόπτης ορίζει τα ποσά που μπορούν να καταναλωθούν και από ποιόν οργανισμό σε κάθε Activity.
4. Οι Οργανισμοί συμμετέχουν στην έρευνα καταθέτοντας το αντίστοιχο ποσό.
5. Οι Επενδυτές επενδύουν στην έρευνα καταθέτοντας το αντίστοιχο ποσό.

Μετά την επένδυση και του τελευταίου επενδυτή η έρευνα γίνεται ενεργή και οι οργανισμοί μπορούν να πραγματοποιούν συναλλαγές σύμφωνα με τις προδιαγραφές που έχει ορίσει ο επόπτης στην κάθε Activity.

Να σημειωθεί πως στην εφαρμογή υπάρχουν Button με τέσσερα διαφορετικά χρώματα.

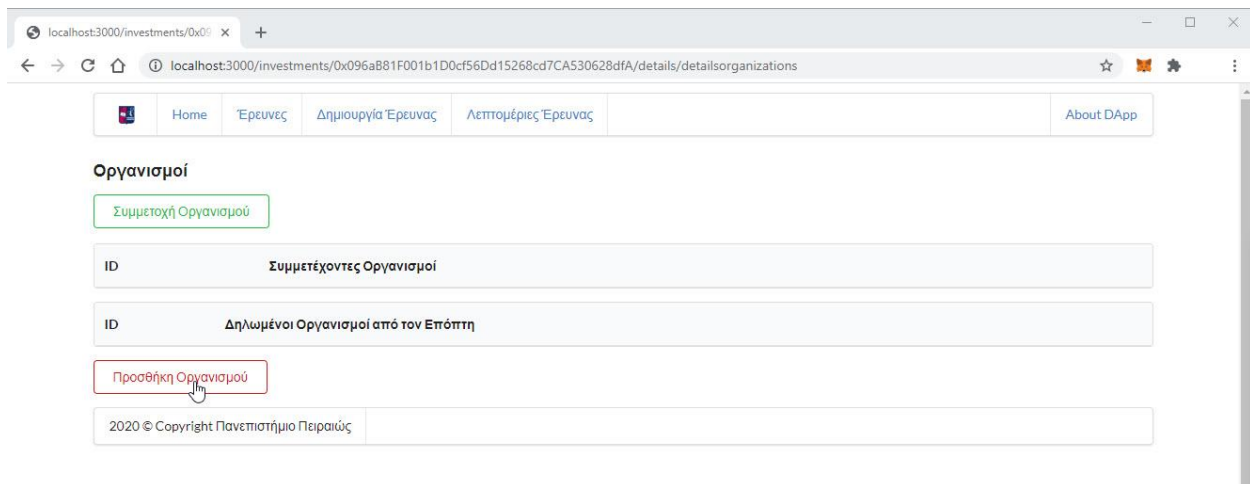
1.  : Η ενέργεια που εκτελείται πίσω από αυτό το κουμπί είναι ενέργεια που μπορεί να εκτελεστεί από όλους τους χρήστες.
2.  : Η ενέργεια που εκτελείται πίσω από αυτό το κουμπί είναι ενέργεια που μπορεί να εκτελεστεί μόνο από τον επόπτη της έρευνας.
3.  : Η ενέργεια που εκτελείται πίσω από αυτό το κουμπί είναι ενέργεια που μπορεί να εκτελεστεί μόνο από τους οργανισμούς της έρευνας.
4.  : Η ενέργεια που εκτελείται πίσω από αυτό το κουμπί είναι ενέργεια που μπορεί να εκτελεστεί μόνο από τους επενδυτές της έρευνας.

Επιλέγοντας «Λεπτομέρειες» κάτω από την επιλογή «4. Οργανισμοί»



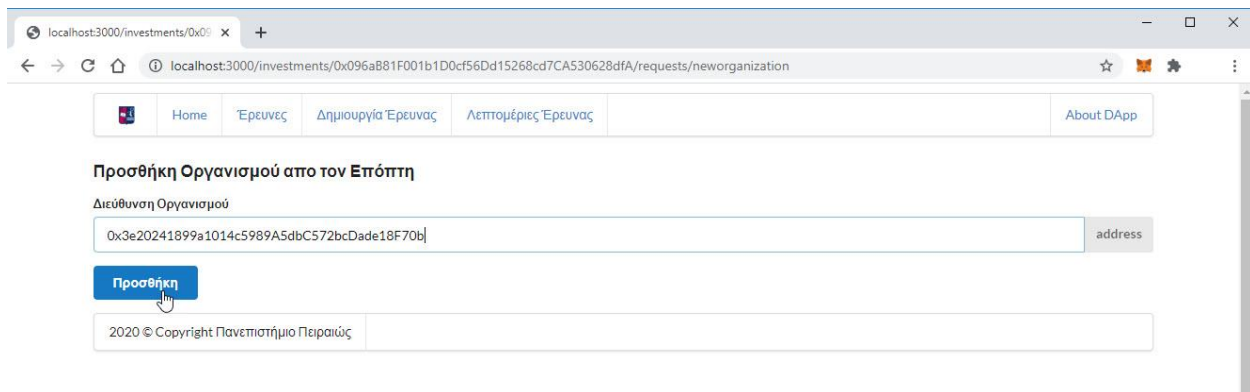
Εικόνα 25: Λεπτομέρειες Έρευνας

μεταφερόμαστε στην παρακάτω σελίδα. Στο σημείο αυτό ο επόπτης κάνοντας κλικ στο κουμπί «Προσθήκη Οργανισμού»



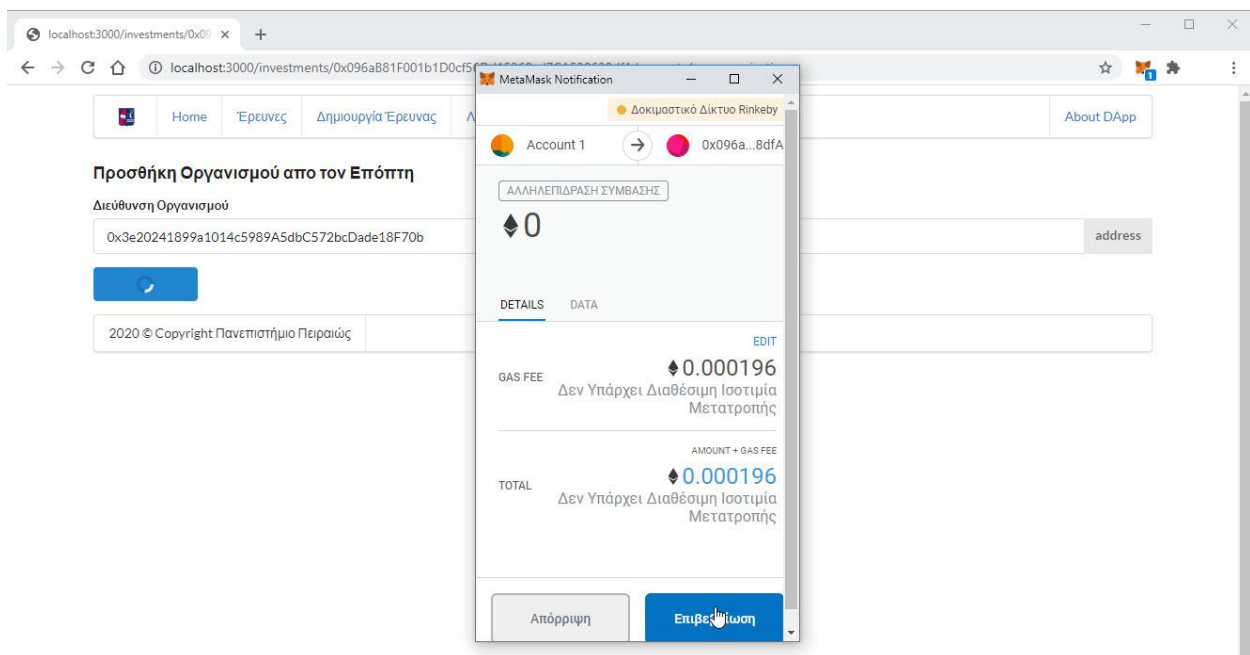
Εικόνα 26: Προσθήκη Οργανισμού από Επόπτη

μεταβαίνει στην παρακάτω σελίδα και προσθέτει την διεύθυνση του Οργανισμού που θα λάβει μέρος.



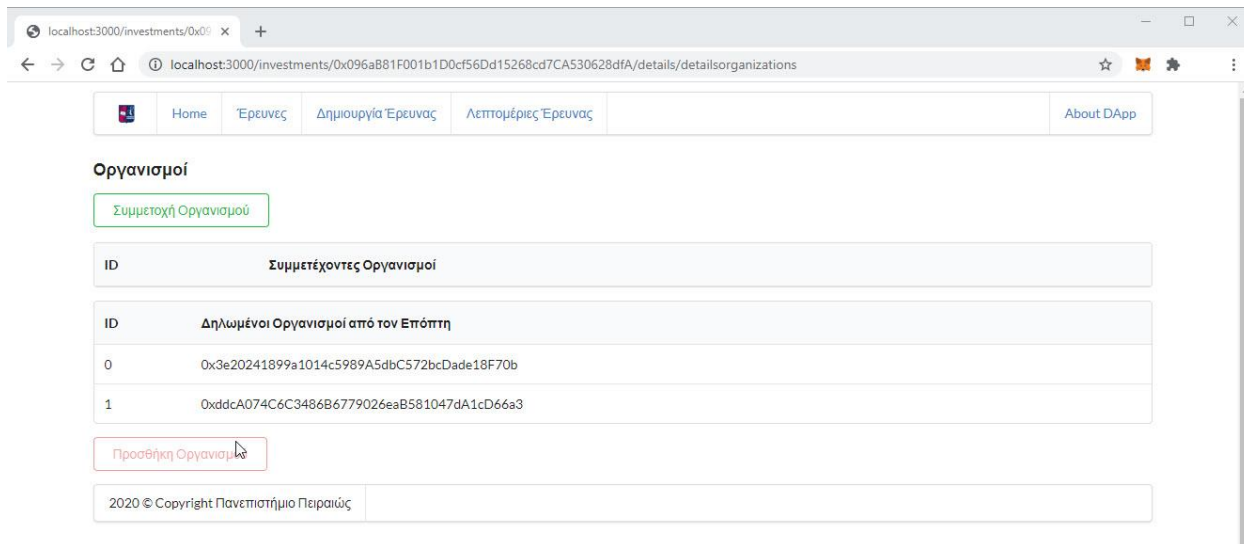
Εικόνα 27: Προσθήκη Οργανισμού από Επόπτη

Η προσθήκη λαμβάνει χώρα αφού πατήσει «Επιβεβαίωση» στην συναλλαγή από το πρόσθετο MetaMask το οποίο θα εμφανιστεί.



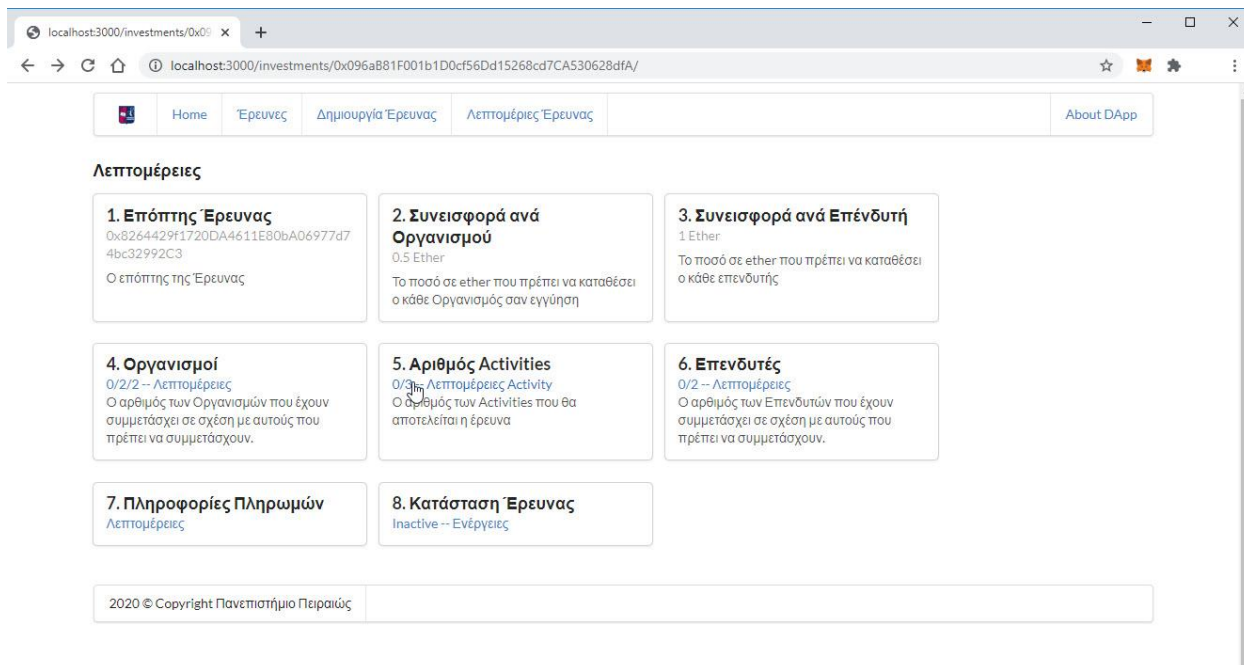
Εικόνα 28: Επιβεβαίωση

Τελειώνοντας την διαδικασία, μπορεί να δει στον δεύτερο πίνακα τους Οργανισμούς που έχει προσθέσει για την συγκεκριμένη έρευνα.



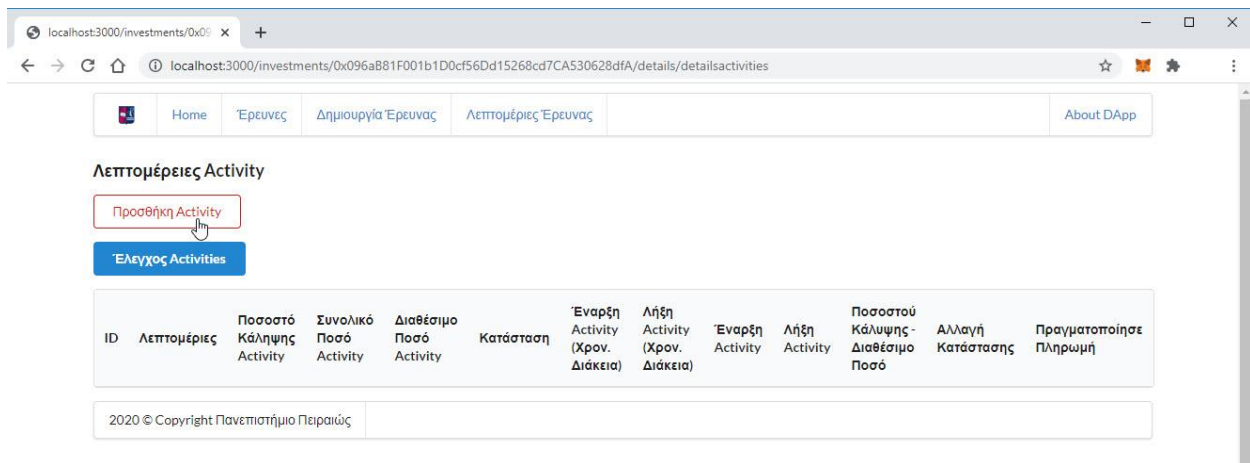
Εικόνα 29: Προσθήκη Οργανισμού από Επόπτη

Στην συνέχεια, ο επόπτης πρέπει να προσθέσει τις λεπτομέρειες των Activities επιλέγοντας «Λεπτομέρειες Activity» από το «5 Αριθμός Activities».



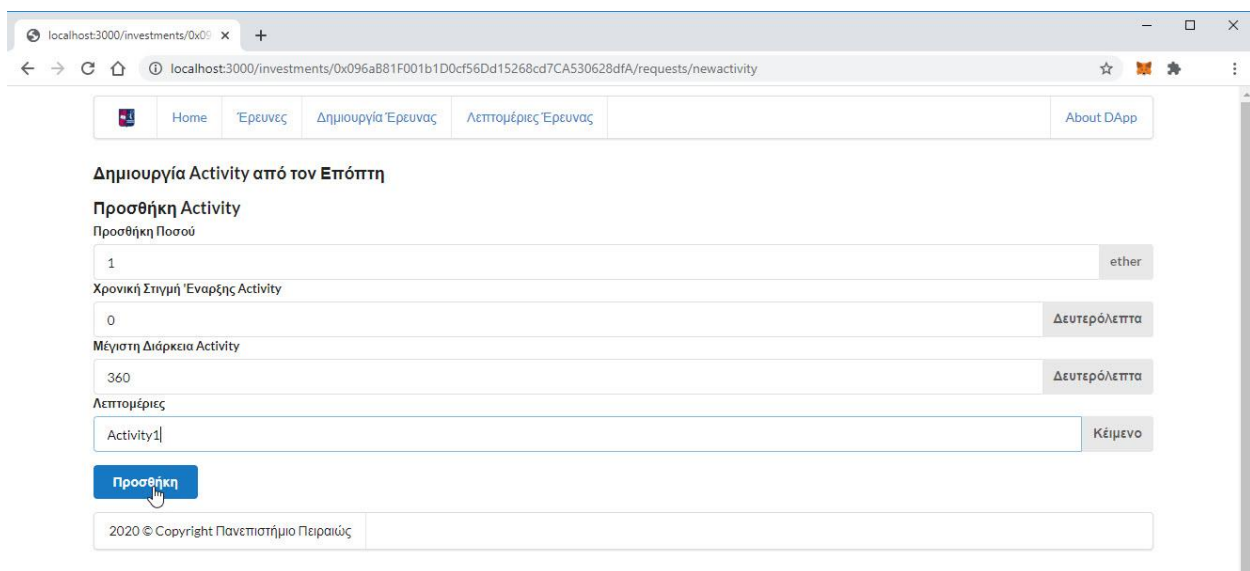
Εικόνα 30: Λεπτομέρειες Έρευνας

Αφού μεταβεί στην σελίδα με τις πληροφορίες των Activities κάνοντας κλικ στο κόκκινο κουμπί «Προσθήκη Activity»

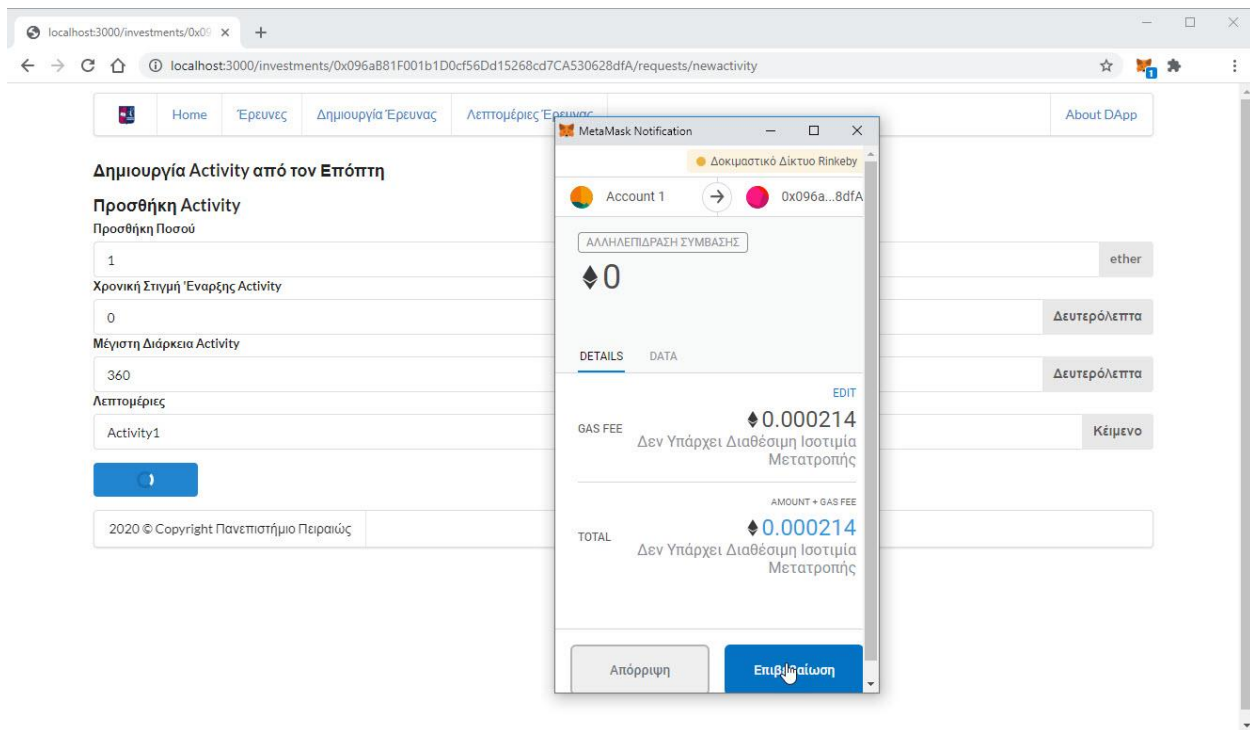


Εικόνα 31: Πληροφορίες Activities

μεταβαίνει στην φόρμα «Προσθήκη Activity». Το ποσό που θα χρησιμοποιηθεί δεν θα πρέπει να ξεπερνάει το δηλωθέν ποσό κατά την δημιουργία της έρευνας ή το διαθέσιμο ποσό εάν είμαστε σε διαδικασία δημιουργίας δεύτερης ή και τρίτης Activity. Σε αυτό το σημείο συμπληρώνει τα στοιχεία της Activity. Να σημειώσουμε πως η «Χρονική Στιγμή Έναρξης Activity» υπολογίζεται από την στιγμή που η έρευνα θεωρηθεί ως ενεργή.

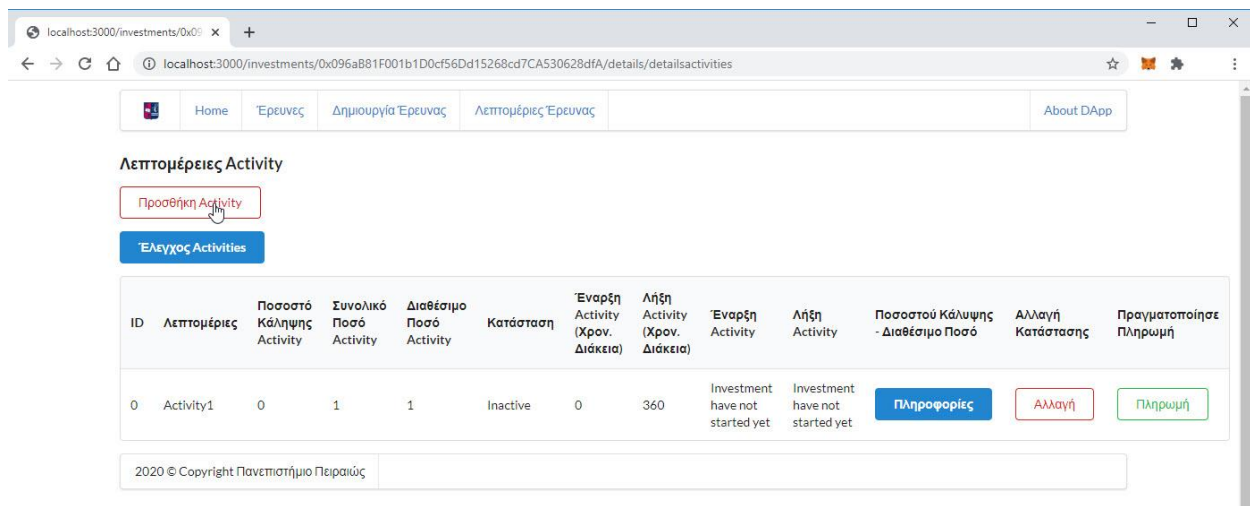


Εικόνα 32: Προσθήκη Activity

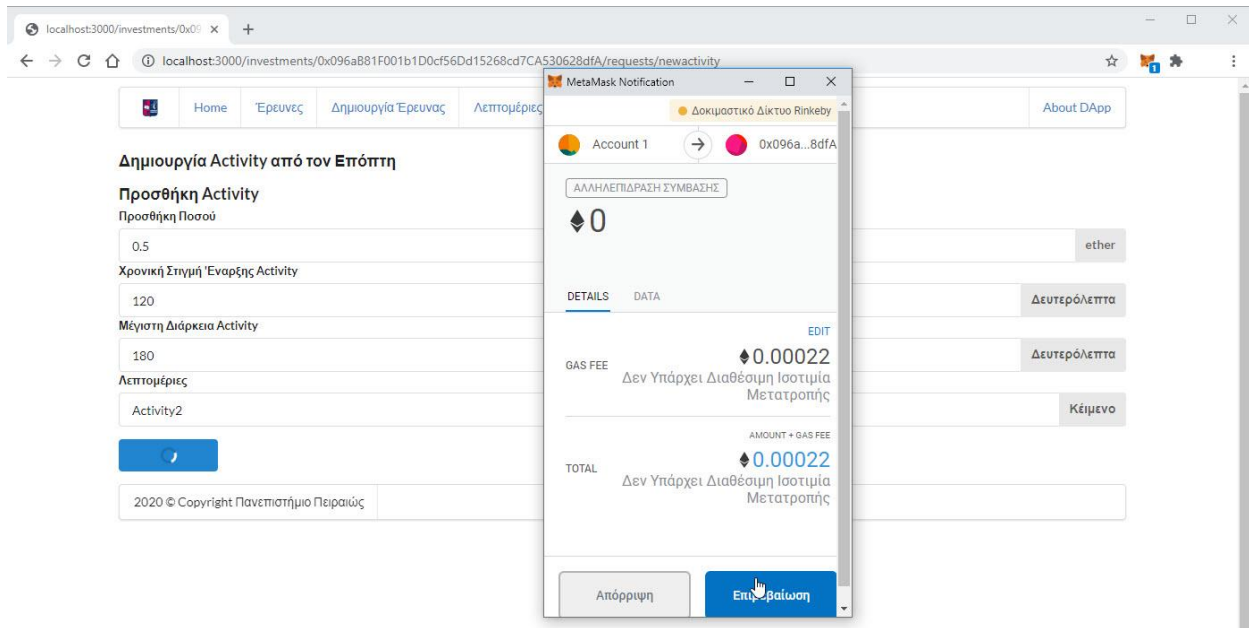


Εικόνα 33: Επιβεβαίωση

Στις παρακάτω εικόνες, πραγματοποιείται προσθήκη δύο ακόμα Activities, αφού για να συνεχίσουμε την διαδικασία της έρευνας πρέπει να έχουν δηλωθεί όλες οι Activities από τις οποίες αποτελείται η Έρευνα.

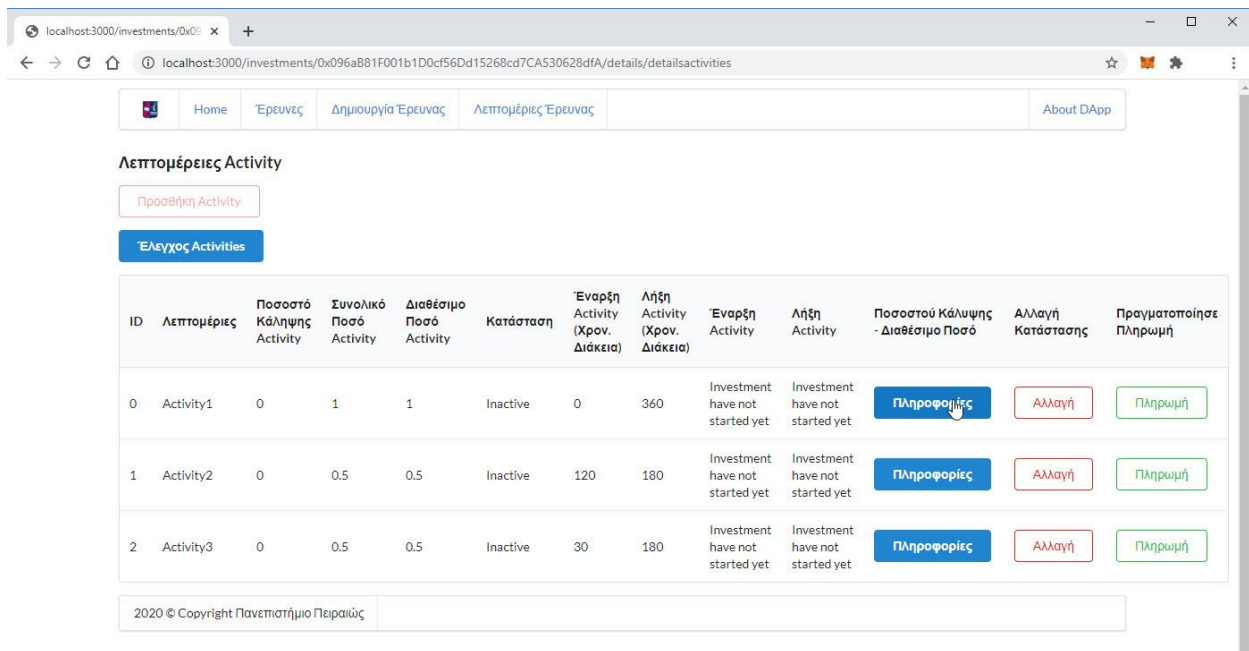


Εικόνα 34: Προσθήκη Activity



Εικόνα 35:Επιβεβαίωση

Επόμενο στάδιο είναι η κατανομή του ποσού που μπορεί να ξοδέψει ο κάθε οργανισμός στην συγκεκριμένη Activity. Κάνοντας κλικ στο κουμπί «Πληροφορίες»

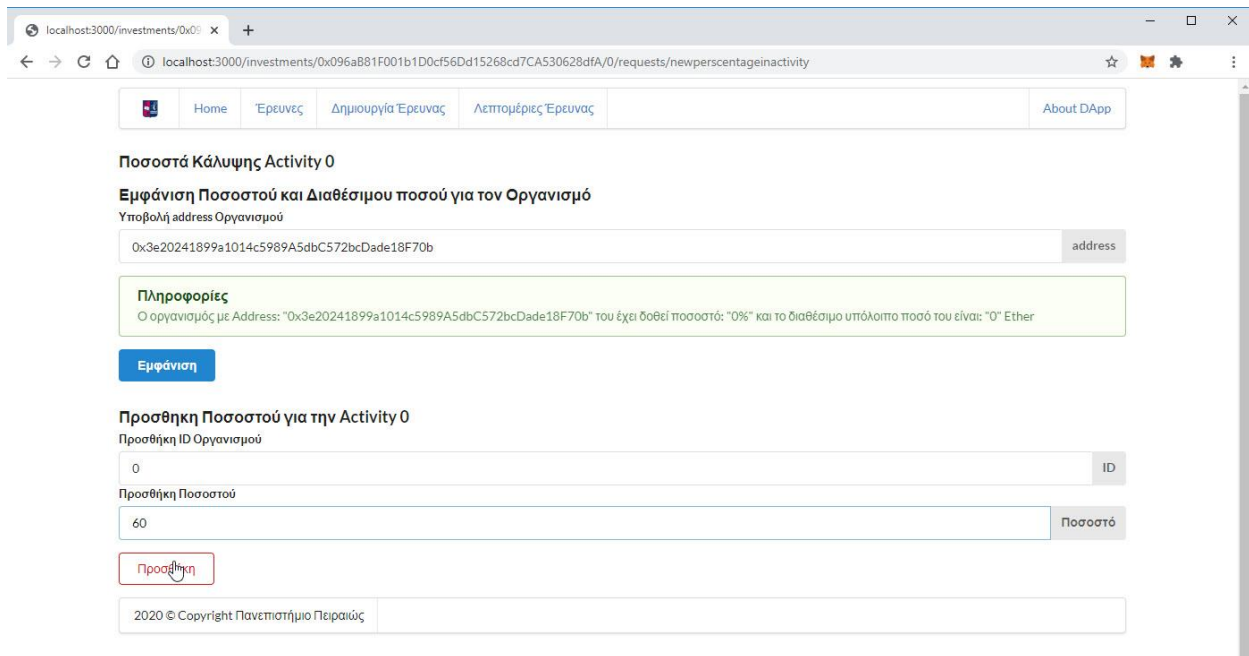


Εικόνα 36: Λίστα Με Activities

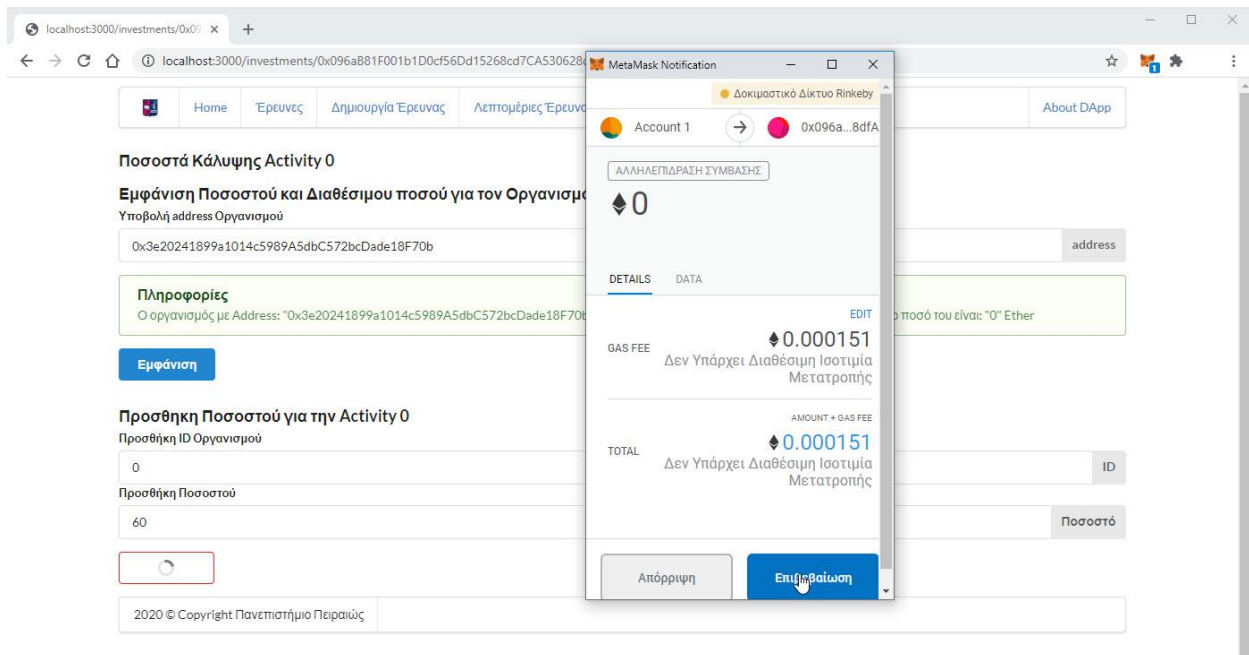
στο πάνω μέρος της σελίδας που μας φορτώνει, μπορεί οποιοσδήποτε να τοποθετήσει την διεύθυνση του Οργανισμού και να δει το ποσοστό που του έχει δοθεί αλλά και το διαθέσιμο υπόλοιπο προς κατανάλωση του Οργανισμού για αυτή την Activity.

Ακριβώς από κάτω υπάρχει η ενέργεια «Προσθήκη Ποσοστού» την οποία μπορεί να εκτελέσει μόνο ο Επόπτης και μόνο πριν την διαδικασία έναρξης της Έρευνας. Τοποθετώντας το ID του

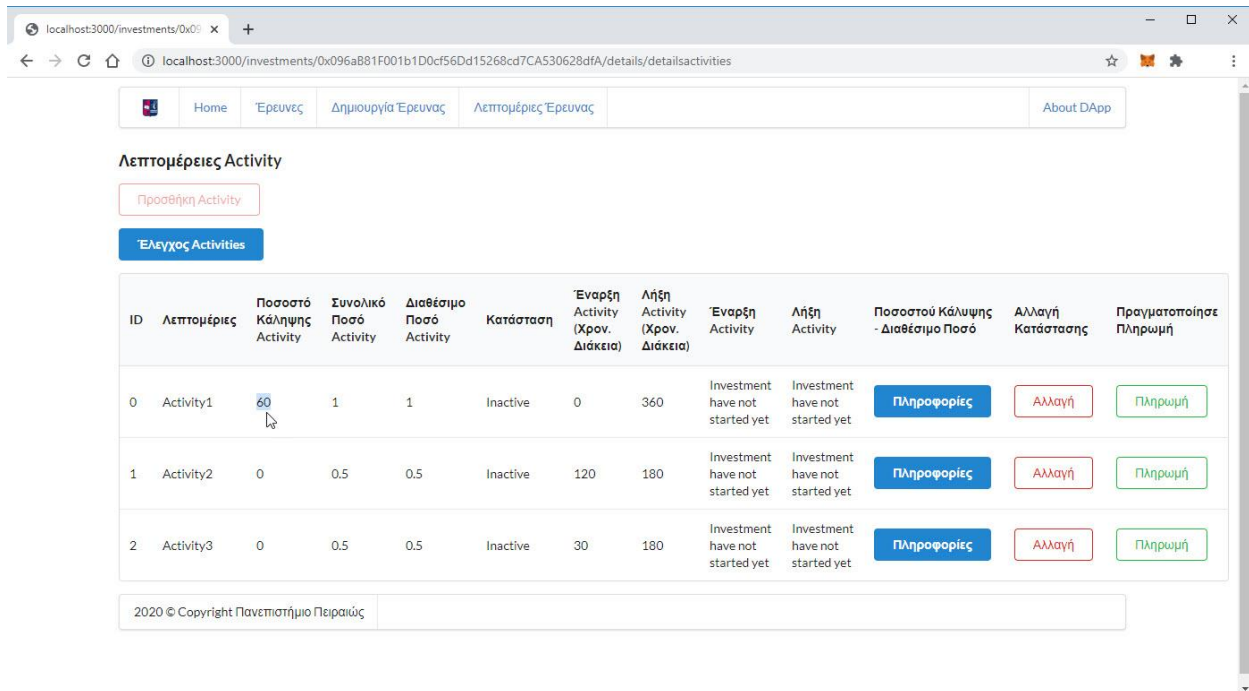
οργανισμού (το ID του οργανισμού μπορεί να το δει από τις λεπτομέρειες στο πεδίο «4.Οργανισμοί») και το ποσοστό που θέλει να του αντιστοιχίσει.



Εικόνα 37: Προσθήκη Ποσοστού Κάλυψης

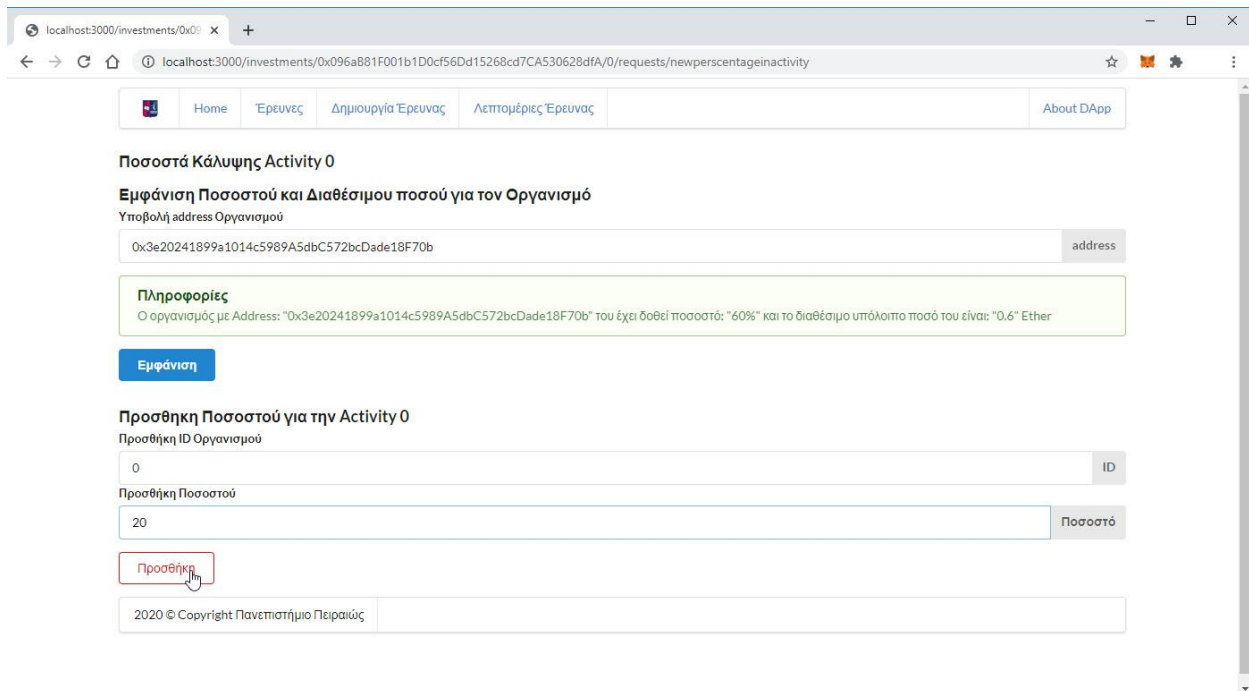


Εικόνα 38: Επιβεβαίωση Προσθήκης Ποσοστού Κάλυψης



Εικόνα 39: Info - Ποσοστό Κάλυψης

Η διαδικασία προσθήκης ποσοστού είναι προσθετική. Όπως και στο παράδειγμα ο επόπτης στην αρχή παραχώρησε δικαίωμα 60% στον οργανισμό με ID 0. Στην συνέχεια όμως του έδωσε επιπλέον ποσοστό 20% επί του αρχικού.



Εικόνα 40: Επιπρόσθετα - Προσθήκη Ποσοστού Κάλυψης

ID	Λεπτομέρειες	Ποσοστό Κάλυψης Activity	Συνολικό Ποσό Activity	Διαθέσιμο Ποσό Activity	Κατάσταση	Έναρξη Activity (Χρον. Διάκεια)	Λήξη Activity (Χρον. Διάκεια)	Έναρξη Activity	Λήξη Activity	Ποσοστό Κάλυψης - Διαθέσιμο Ποσό	Αλλαγή Κατάστασης	Πραγματοποίησης Πληρωμή
0	Activity1	80	1	1	Inactive	0	360	Investment have not started yet	Investment have not started yet	Πληροφορίες	Αλλαγή	Πληρωμή
1	Activity2	0	0.5	0.5	Inactive	120	180	Investment have not started yet	Investment have not started yet	Πληροφορίες	Αλλαγή	Πληρωμή
2	Activity3	0	0.5	0.5	Inactive	30	180	Investment have not started yet	Investment have not started yet	Πληροφορίες	Αλλαγή	Πληρωμή

Εικόνα 41: Ένδειξη Ποσοστού Κάλυψης

Το αποτέλεσμα είναι του οργανισμού με ID 0 να του έχει δοθεί ποσοστό 80%.

Ποσοστά Κάλυψης Activity 0

Εμφάνιση Ποσοστού και Διαθέσιμου ποσού για τον Οργανισμό

Υποβολή address Οργανισμού

0x3e20241899a1014c5989A5dbC572bcDade18F70b address

Πληροφορίες

Ο οργανισμός με Address: "0x3e20241899a1014c5989A5dbC572bcDade18F70b" του έχει δοθεί ποσοστό 80% και το διαθέσιμο υπόλοιπο ποσό του είναι: "0.8" Ether

Εμφάνιση

Προσθήκη Ποσοστού για την Activity 0

Προσθήκη ID Οργανισμού

Προσθήκη Ποσοστού

Προσθήκη

Εικόνα 42: Εμφάνιση Ποσοστού και Διαθέσιμου Ποσού

Στην συνέχεια δίνεται ποσοστό 10% στον οργανισμό με ID 1.

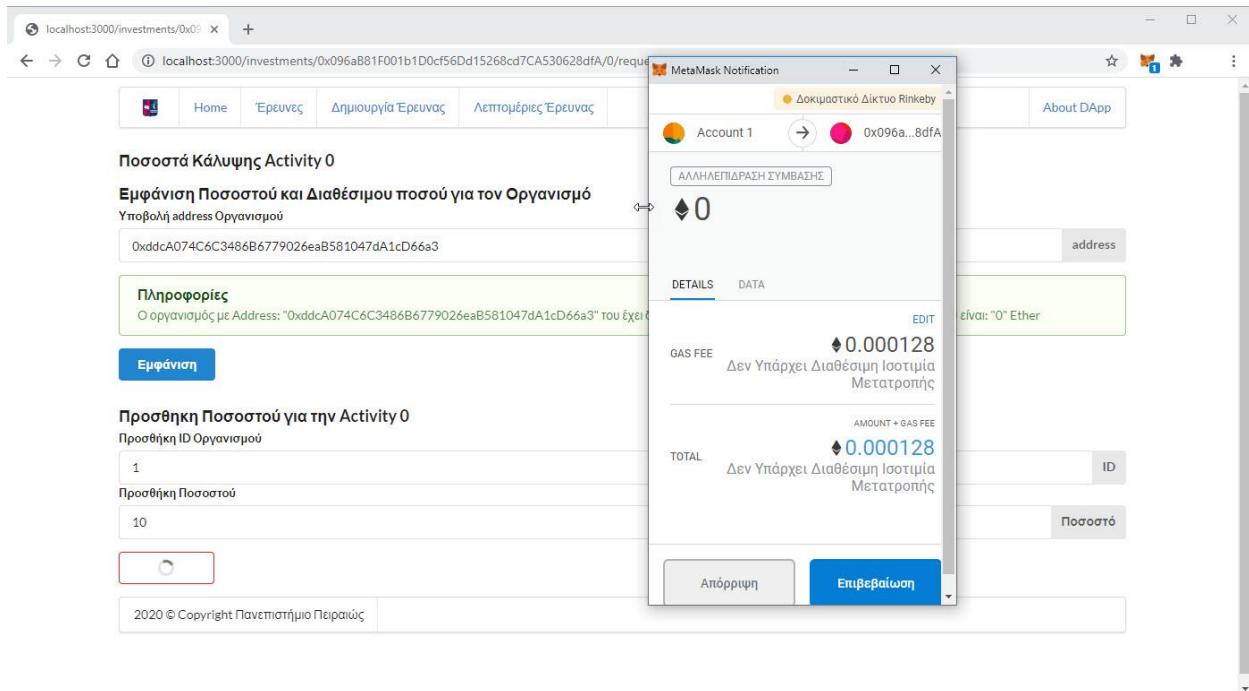
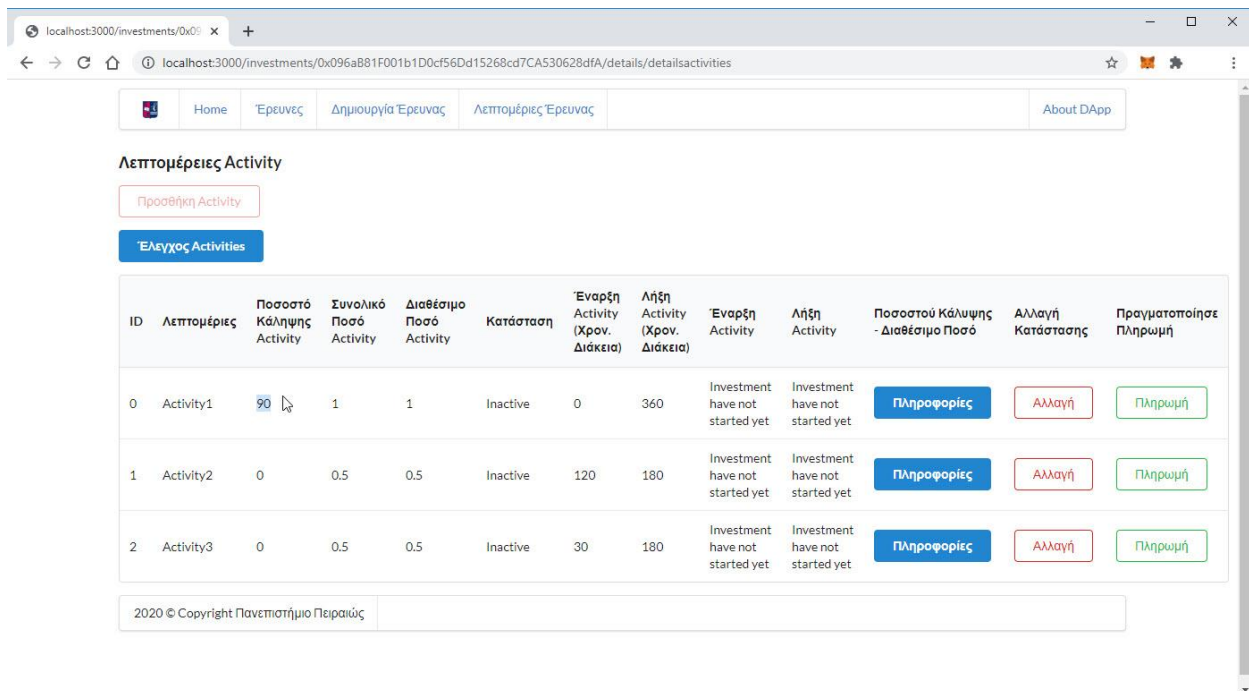


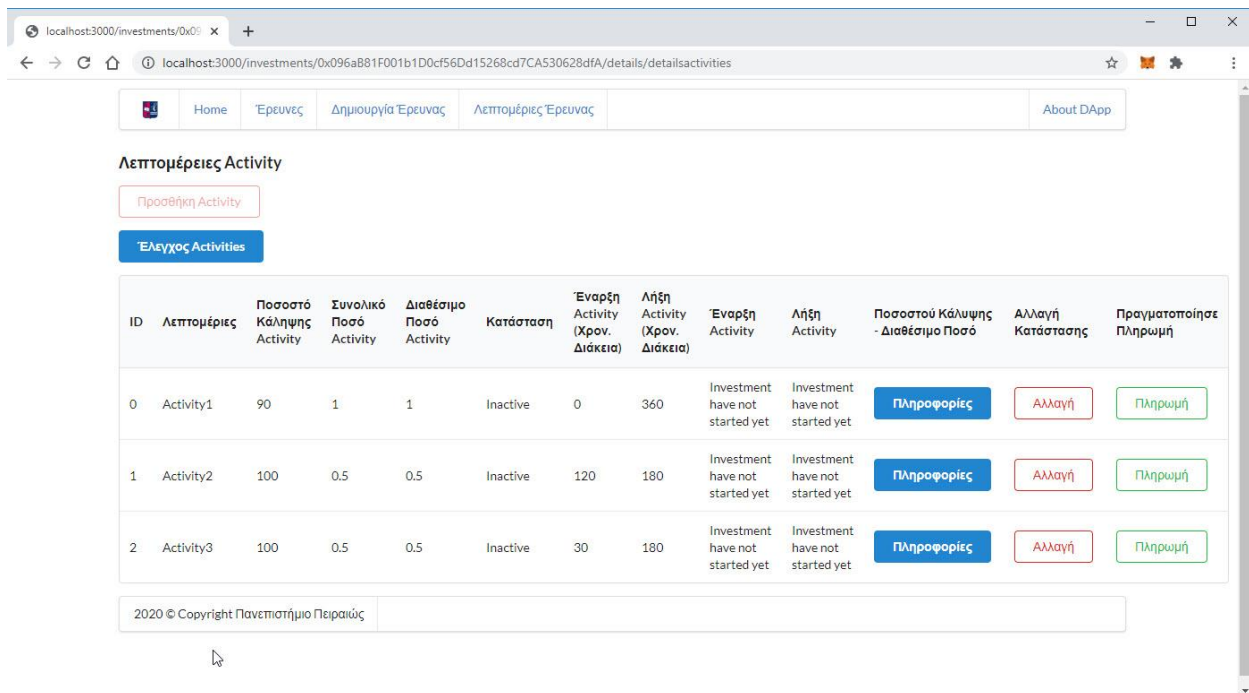
Figure 1

Το ποσοστό κάλυψης δεν είναι ανάγκη να φτάσει το 100%.



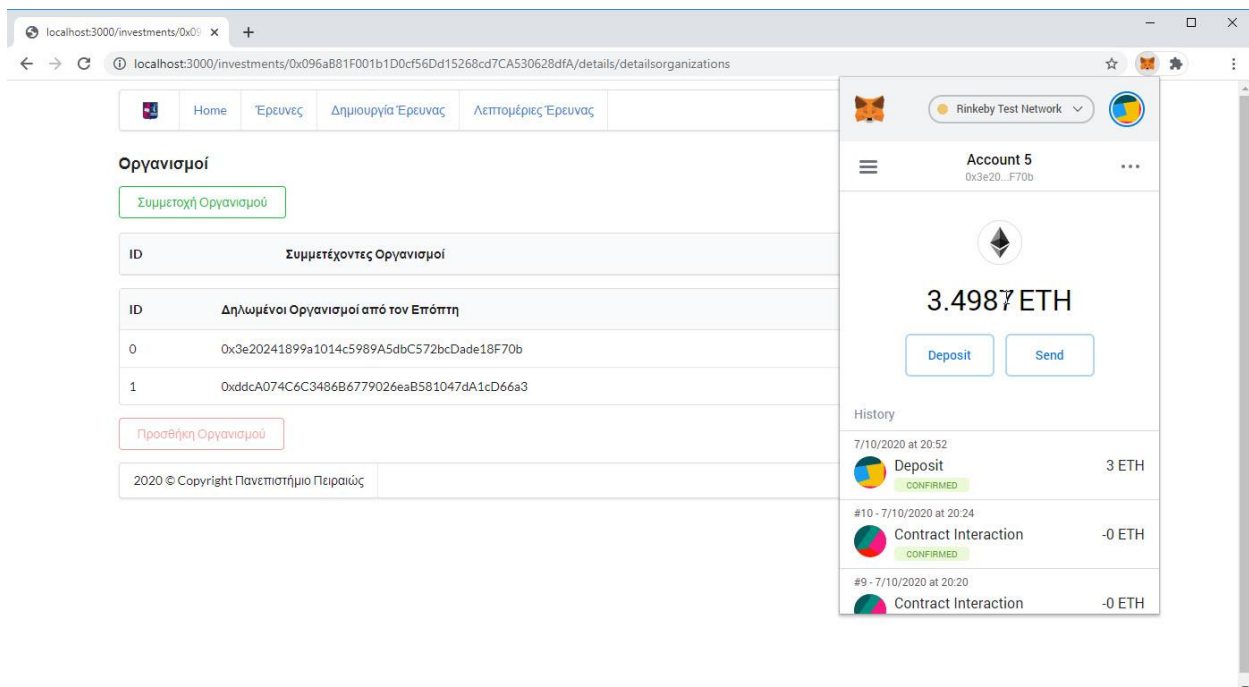
Εικόνα 43: Ένδειξη Ποσοστού Κάλυψης

Προσθέτοντας Ποσοστά Κάλυψης και στις επόμενες Activity με τον ίδιο τρόπο παίρνουμε ως αποτέλεσμα την παρακάτω εικόνα.



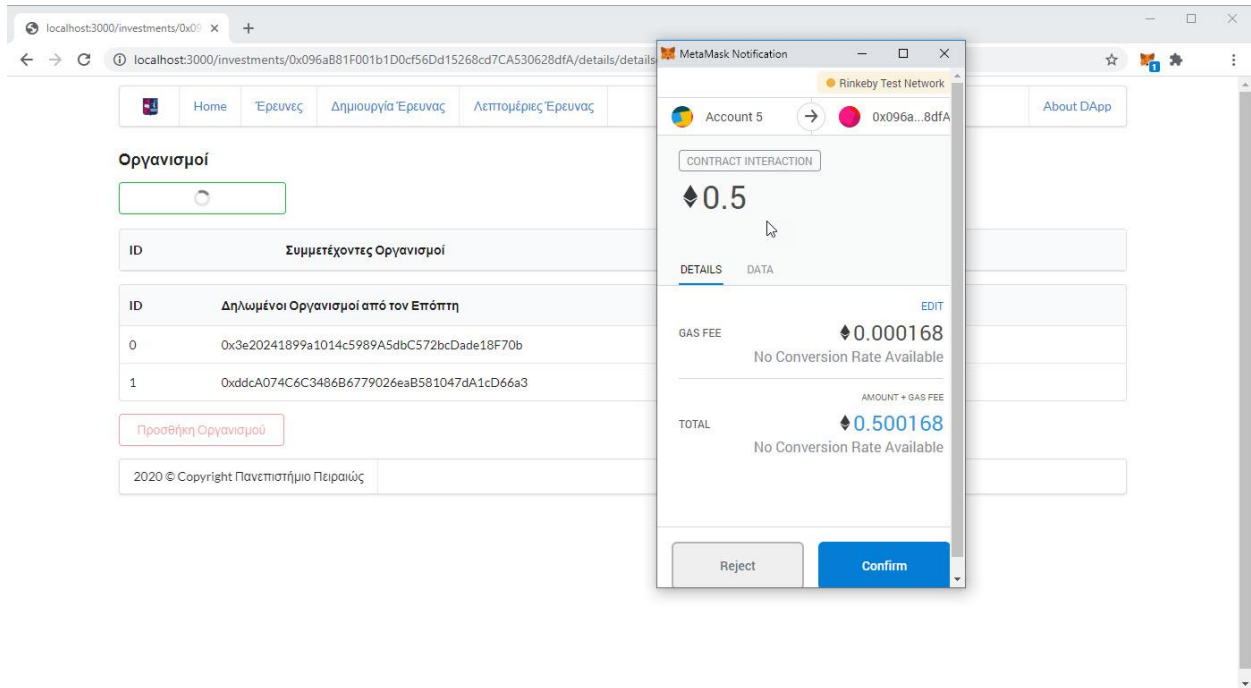
Εικόνα 44: Πλήρης Εισαγωγή Activities

Εν συνεχεία, θα πρέπει οι Οργανισμοί να δηλώσουν συμμετοχή και να καταβάλουν το αντίστοιχο ποσό. Πηγαίνοντας στο «4. Οργανισμοί» στην σελίδα που εμφανίζεται, κάθε δηλωμένος οργανισμός θα πρέπει να κάνει κλικ στο κουμπί «Συμμετοχή Οργανισμού» και να καταβάλει το αντίστοιχο ποσό.



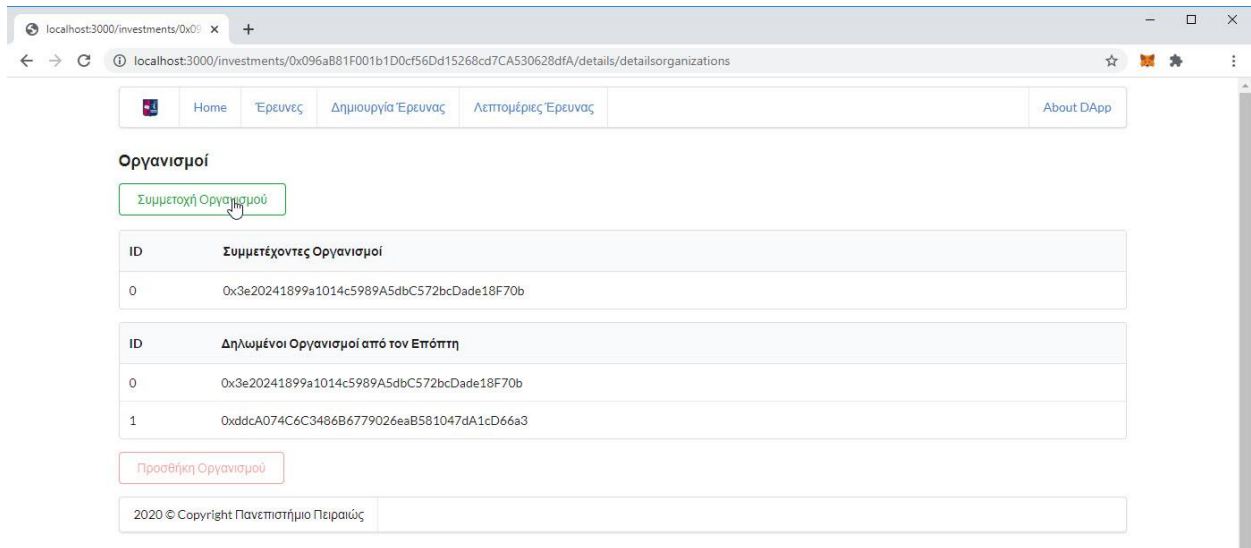
Εικόνα 45: Δήλωση Συμμετοχής Οργανισμού

Στο πρόσθετο του MetaMask του εμφανίζεται το ποσό που θα χρεωθεί ο λογαριασμός του. Επιβεβαιώνοντας την πράξη αυτή ο Οργανισμός λαμβάνει μέρος στην έρευνα.

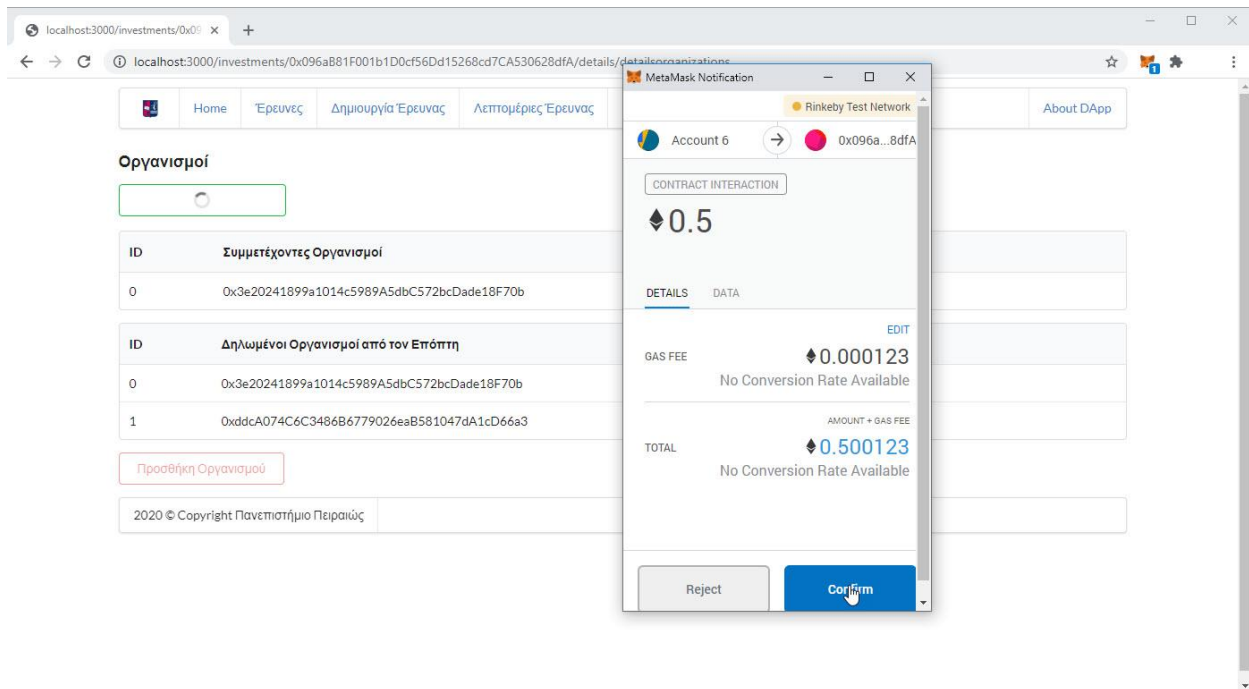


Εικόνα 46: Επιβεβαίωση Εισαγωγής

Επιβεβαιώνεται η συμμετοχή του βλέποντας τον αριθμό της διεύθυνσή του στο πρώτο πίνακα κάτω από το «Συμμετέχοντες Οργανισμοί».

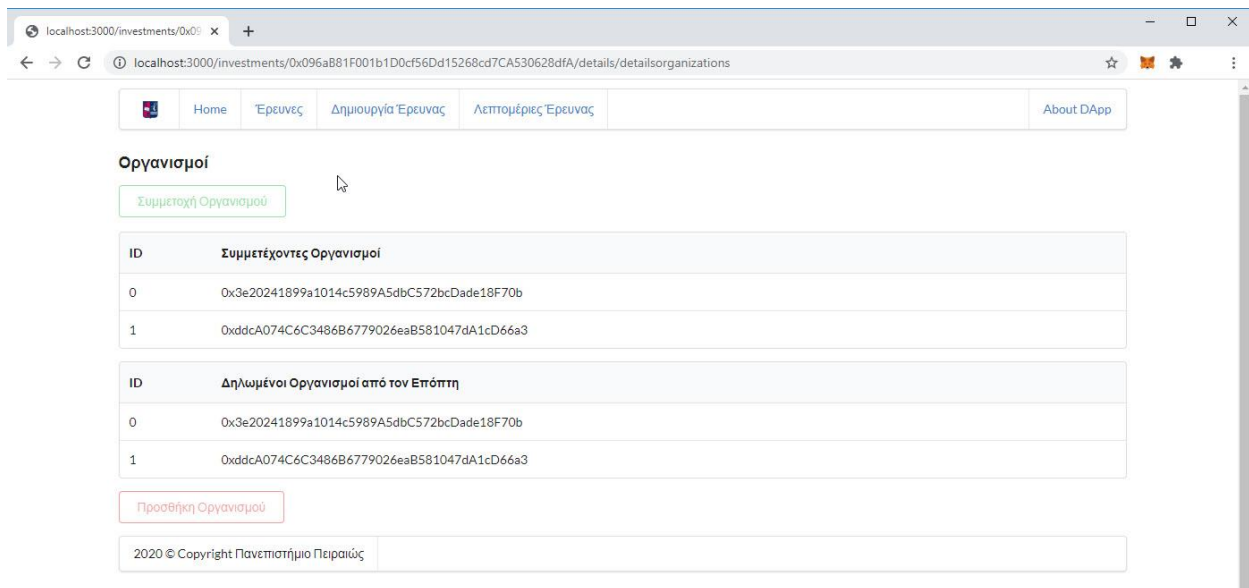


Εικόνα 47: Δήλωση Συμμετοχής 2ου Οργανισμού



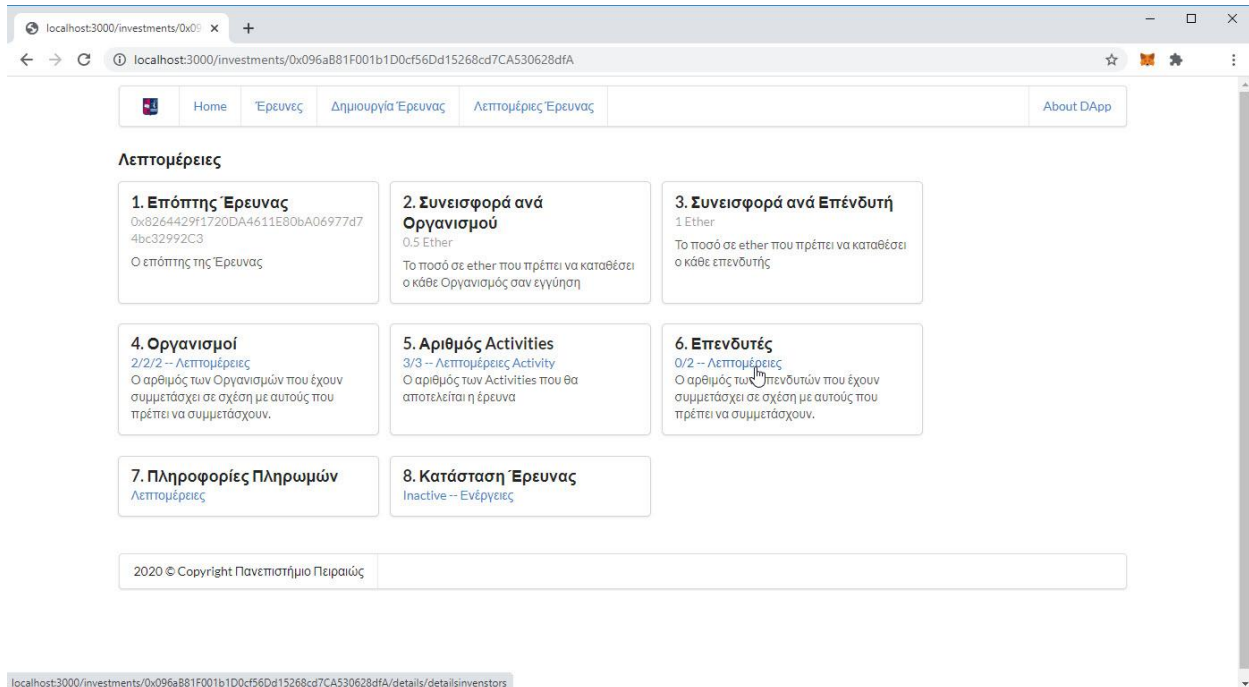
Εικόνα 48: Επιβεβαίωση

Αφού όλοι οι δηλωμένοι Οργανισμοί έχουν λάβει μέρος, τότε το αντίστοιχο κουμπί απενεργοποιείται.



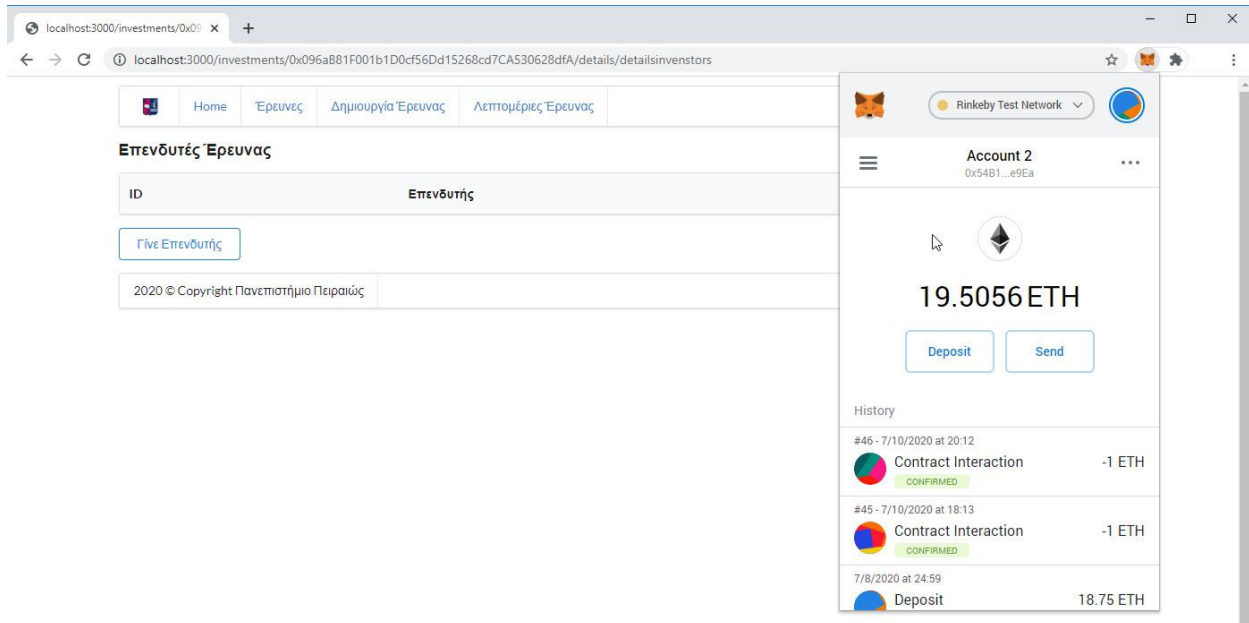
Εικόνα 49: Προβολή Συμμετεχόντων Οργανισμών

Στο τελευταίο στάδιο, για να θεωρηθεί η έρευνα ενεργή, θα πρέπει να βρεθούν οι επενδυτές και να συμμετάσχουν στην έρευνα καταθέτοντας το αντίστοιχο ποσό.

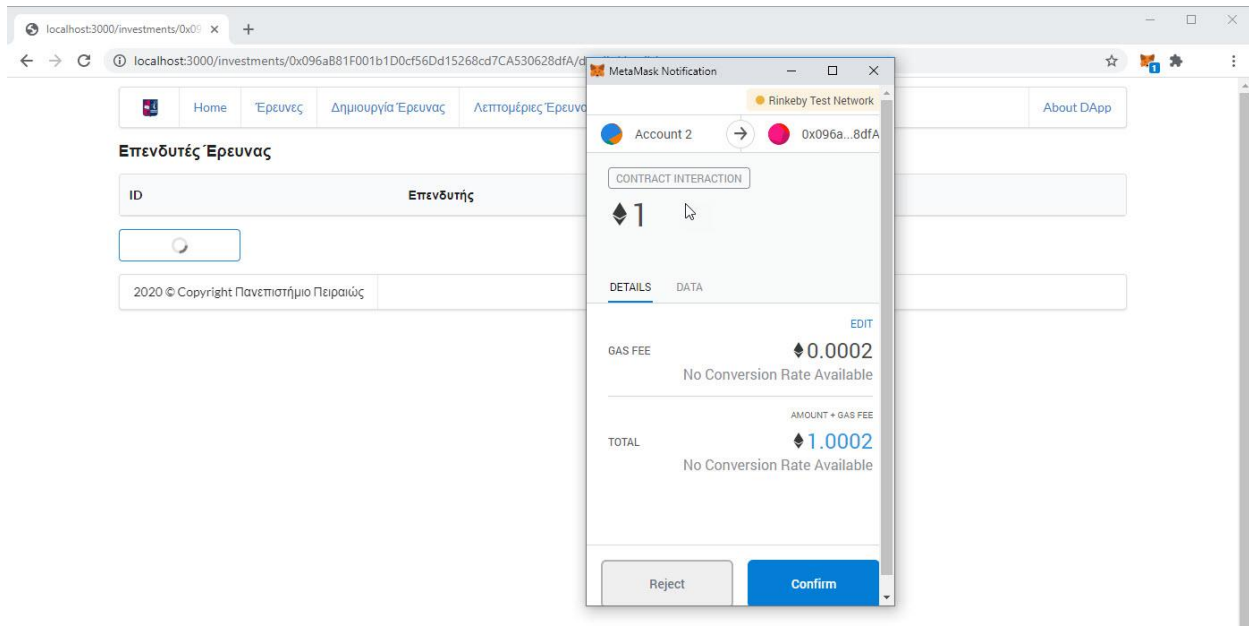


Εικόνα 50:Λεπτομέρειες Έρευνας

Ο Επενδυτής, κάνοντας κλικ στο κουμπί «Γίνε Επενδυτής» και αφού δώσει την επιβεβαίωση συναλλαγής μέσω του MetaMask, γίνεται επενδυτής κι έπειτα καταγράφεται το όνομα του στον παρακάτω πίνακα.



Εικόνα 51:Διαδικασία Επένδυσης από τον Επενδυτή



Εικόνα 52:Επιβεβαίωση Επένδυσης

Όταν συμπληρωθεί ο απαραίτητος αριθμός των επενδυτών η έρευνα αυτόματα θεωρείται ενεργή.

ID	Επενδυτής
0	0x54B155f3D8c1AF04f16246De45ad349bD3c6e9Ea
1	0xcC03d8A009eC277Eed0b64CE94FF322616956695

Εικόνα 53:Λίστα με τους Επενδυτές

Κατά την διάρκεια που η έρευνα είναι ενεργή, η κατάσταση της activity είναι ενεργή (Active) και ο τρέχων χρόνος είναι μέσα στα όρια της «Έναρξης Activity» και «Λήξης Activity». Για να θεωρηθεί η έρευνα ενεργή θα πρέπει να μην υπάρχει κάποιο Activity που να βρίσκεται σε κατάσταση Pending ή Cancelled, τότε ο οργανισμός μπορεί να πραγματοποιήσει πληρωμή.

Λεπτομέρειες Activity

Προσθήκη Activity

Έλεγχος Activities

ID	Λεπτομέρειες	Ποσοστό Κάλυψης Activity	Συνολικό Ποσό Activity	Διαθέσιμο Ποσό Activity	Κατάσταση	Έναρξη Activity (Χρον. Διάκεια)	Λήξη Activity (Χρον. Διάκεια)	Έναρξη Activity	Λήξη Activity	Ποσοστό Κάλυψης - Διαθέσιμο Ποσό	Αλλαγή Κατάστασης	Πραγματοποιήσε Πληρωμή	
0	Activity1	90	1	1	Active	0	360	Jul 10, 2020, 8:59:09 PM	Jul 10, 2020, 9:05:09 PM		Πληροφορίες	Αλλαγή	Πληρωμή
1	Activity2	100	0.5	0.5	Inactive	120	180	Jul 10, 2020, 9:01:09 PM	Jul 10, 2020, 9:04:09 PM		Πληροφορίες	Αλλαγή	Πληρωμή
2	Activity3	100	0.5	0.5	inactive	30	180	Jul 10, 2020, 8:59:39 PM	Jul 10, 2020, 9:02:39 PM		Πληροφορίες	Αλλαγή	Πληρωμή

2020 © Copyright Πανεπιστήμιο Πειραιώς

Εικόνα 54:Κατάσταση Δραστηριοτήτων

Επιλέγοντας το κουμπί «Πληρωμή» μεταβαίνει στην παρακάτω σελίδα. Στο πάνω μέρος μπορεί να ελέγξει το ποσό από το απομένει για να ξοδέψει στην συγκεκριμένη Activity. Στο κάτω μέρος πραγματοποιεί την πληρωμή επιλέγοντας το ποσό που θα αφαιρεθεί από την Έρευνα, το σχόλιο που θα τοποθετήσει και τον παραλήπτη – πωλητή.

Πληρωμή Πωλητή

Εμφάνιση Ποσοστού και Διαθέσιμου ποσού για τον Οργανισμό

Υποβολή address Οργανισμού

0x3e20241899a1014c5989A5dbC572bcDade18F70b

Πληροφορίες

Ο οργανισμός με Address: "0x3e20241899a1014c5989A5dbC572bcDade18F70b" του έχει δοθεί ποσό

Εμφάνιση

Πληρωμή Πωλητή για την Activity0

Προσθήκη Ποσού

0.5

Περιγραφή Ενέργειας

Οργανισμός_Πληρωμή1

Προσθήκη Διεύθυνσης Πωλητή

0x0E3e55b64307aa8953b87d91b63148Acd48Cb04b

2020 © Copyright Πανεπιστήμιο Πειραιώς

MetaMask Notification

Rinkeby Test Network

Account 5 → 0x096a...8dfA

CONTRACT INTERACTION

0

DETAILS DATA

GAS FEE 0.000382 No Conversion Rate Available

TOTAL 0.000382 No Conversion Rate Available

Reject Confirm

Εικόνα 55:Πληρωμή Πωλητή

localhost:3000/investments/0x0: x +

localhost:3000/investments/0x096aB81F001b1D0cf56Dd15268cd7CA530628dfA/details/detailsactivities

Home Έρευνες Δημιουργία Έρευνας Λεπτομέρειες Έρευνας About DApp

Λεπτομέρειες Activity

Προσθήκη Activity

Έλεγχος Activities

ID	Λεπτομέρειες	Ποσοστό Κάλυψης Activity	Συνολικό Ποσό Activity	Διαθέσιμο Ποσό Activity	Κατάσταση	Έναρξη Activity (Χρον. Διάκεια)	Λήξη Activity (Χρον. Διάκεια)	Έναρξη Activity	Λήξη Activity	Ποσοστό Κάλυψης - Διαθέσιμο Ποσό	Αλλαγή Κατάστασης	Πραγματοποίησης Πληρωμή	
0	Activity1	90	1	0.5	Active	0	360	Jul 10, 2020, 8:59:09 PM	Jul 10, 2020, 9:05:09 PM		Πληροφορίες	Αλλαγή	Πληρωμή
1	Activity2	100	0.5	0.5	Active	120	180	Jul 10, 2020, 9:01:09 PM	Jul 10, 2020, 9:04:09 PM		Πληροφορίες	Αλλαγή	Πληρωμή
2	Activity3	100	0.5	0.5	Active	30	180	Jul 10, 2020, 8:59:39 PM	Jul 10, 2020, 9:02:39 PM		Πληροφορίες	Αλλαγή	Πληρωμή

2020 © Copyright Πανεπιστήμιο Πειραιώς

Εικόνα 56:Κατάσταση Activity

localhost:3000/investments/0x0: x +

localhost:3000/investments/0x096aB81F001b1D0cf56Dd15268cd7CA530628dfA/2/requests/newpayment

Home Έρευνες Δημιουργία Έρευνας Λεπτομέρειες Έρευνας About DApp

Πληρωμή Πωλητή

Εμφάνιση Ποσοστού και Διαθέσιμου ποσού για τον Οργανισμό

Υποβολή address Οργανισμού

0x3e20241899a1014c5989A5dbC572bcDade18F70b address

Πληροφορίες
Ο οργανισμός με Address: "0x3e20241899a1014c5989A5dbC572bcDade18F70b" του έχει δοθεί ποσοστό: "100%" και το διαθέσιμο υπόλοιπο ποσό του είναι: "0.5" Ether

Εμφάνιση

Πληρωμή Πωλητή για την Activity2

Προσθήκη Ποσού

0.5 ether

Περιγραφή Ενέργειας

Οργανισμός_Πληρωμή2 κείμενο

Προσθήκη Διεύθυνσης Πωλητή

0x0E3e55b64307aa8953b87d91b63148AcD48Cb04b address

2020 © Copyright Πανεπιστήμιο Πειραιώς

Εικόνα 57:Πληρωμή Πωλητή

Ανά πάσα στιγμή, οποιοσδήποτε μπορεί να πραγματοποιήσει «Έλεγχο Activity». Κατά την διαδικασία αυτή γίνεται έλεγχος των Activities. Εάν κάποιος έχει φύγει από το χρονικό περιθώριο και ήταν σε κατάσταση Activity τότε αλλάζει η κατάσταση του σε κατάσταση Pending περιμένοντας ενέργεια από τον Επόπτη.

localhost:3000/investments/0x0: X +

localhost:3000/investments/0x096a881f001b1d0cf56Dd15268cd7CA530628dfA/details/detailsactivities

Home Έρευνες Δημιουργία Έρευνας Λεπτομέρειες Έρευνας About DApp

Λεπτομέρειες Activity

Προσθήκη Activity

Έλεγχος Activities

ID	Λεπτομέρειες	Ποσοστό Κάλυψης Activity	Συνολικό Ποσό Activity	Διαθέσιμο Ποσό Activity	Κατάσταση	Έναρξη Activity (Χρον. Διάκεια)	Λήξη Activity (Χρον. Διάκεια)	Έναρξη Activity	Λήξη Activity	Ποσοστό Κάλυψης - Διαθέσιμο Ποσό	Αλλαγή Κατάστασης	Πραγματοποιήσε Πληρωμή	
0	Activity1	90	1	0.5	Active	0	360	Jul 10, 2020, 8:59:09 PM	Jul 10, 2020, 9:05:09 PM		Πληροφορίες	Αλλαγή	Πληρωμή
1	Activity2	100	0.5	0.5	Active	120	180	Jul 10, 2020, 9:01:09 PM	Jul 10, 2020, 9:04:09 PM		Πληροφορίες	Αλλαγή	Πληρωμή
2	Activity3	100	0.5	0	Active	30	180	Jul 10, 2020, 8:59:39 PM	Jul 10, 2020, 9:02:39 PM		Πληροφορίες	Αλλαγή	Πληρωμή

2020 © Copyright Πανεπιστήμιο Πειραιώς

Εικόνα 58:Κατάσταση Activity

Σε περίπτωση που κάποια Activity θεωρηθεί Pending, η όλη έρευνα μπαίνει σε κατάσταση Pending και αναμένει κίνηση από τον επόπτη.

localhost:3000/investments/0x0: X +

localhost:3000/investments/0x096a881f001b1d0cf56Dd15268cd7CA530628dfA/details/detailsactivities

Home Έρευνες Δημιουργία Έρευνας Λεπτομέρειες Έρευνας About DApp

Λεπτομέρειες Activity

Προσθήκη Activity

Έλεγχος Activities

ID	Λεπτομέρειες	Ποσοστό Κάλυψης Activity	Συνολικό Ποσό Activity	Διαθέσιμο Ποσό Activity	Κατάσταση	Έναρξη Activity (Χρον. Διάκεια)	Λήξη Activity (Χρον. Διάκεια)	Έναρξη Activity	Λήξη Activity	Ποσοστό Κάλυψης - Διαθέσιμο Ποσό	Αλλαγή Κατάστασης	Πραγματοποιήσε Πληρωμή	
0	Activity1	90	1	0.5	Active	0	360	Jul 10, 2020, 8:59:09 PM	Jul 10, 2020, 9:05:09 PM		Πληροφορίες	Αλλαγή	Πληρωμή
1	Activity2	100	0.5	0.5	Active	120	180	Jul 10, 2020, 9:01:09 PM	Jul 10, 2020, 9:04:09 PM		Πληροφορίες	Αλλαγή	Πληρωμή
2	Activity3	100	0.5	0	Pending	30	180	Jul 10, 2020, 8:59:39 PM	Jul 10, 2020, 9:02:39 PM		Πληροφορίες	Αλλαγή	Πληρωμή

2020 © Copyright Πανεπιστήμιο Πειραιώς

Εικόνα 59:Έλεγχος Activity

Ο Επόπτης είναι ο μόνος που μπορεί να αλλάξει την κατάσταση της Activity και κατά συνέπεια και της έρευνας. Πατώντας το κουμπί «Αλλαγή» μεταφερόμαστε στην παρακάτω σελίδα.

Λεπτομέρειες Activity

Προσθήκη Activity

Έλεγχος Activities

ID	Λεπτομέρειες	Ποσοστό Κάλυψης Activity	Συνολικό Ποσό Activity	Διαθέσιμο Ποσό Activity	Κατάσταση	Έναρξη Activity (Χρον. Διάκεια)	Λήξη Activity (Χρον. Διάκεια)	Έναρξη Activity	Λήξη Activity	Ποσοστού Κάλυψης - Διαθέσιμο Ποσό	Αλλαγή Κατάστασης	Πραγματοποιήσε Πληρωμή	
0	Activity1	90	1	0.5	Active	0	360	Jul 10, 2020, 8:59:09 PM	Jul 10, 2020, 9:05:09 PM		Πληροφορίες	Αλλαγή	Πληρωμή
1	Activity2	100	0.5	0.5	Active	120	180	Jul 10, 2020, 9:01:09 PM	Jul 10, 2020, 9:04:09 PM		Πληροφορίες	Αλλαγή	Πληρωμή
2	Activity3	100	0.5	0	Pending	30	180	Jul 10, 2020, 8:59:39 PM	Jul 10, 2020, 9:02:39 PM		Πληροφορίες	Αλλαγή	Πληρωμή

2020 © Copyright Πανεπιστήμιο Πειραιώς

Εικόνα 60: Κατάσταση Activity

Σε αυτή την σελίδα ο επόπτης κρίνει εάν η Activity έχει Ολοκληρωθεί ή Ακυρωθεί.

Αλλαγή Κατάστασης

Αλλαγή κατάστασης για την Activity2

Για να "Ακυρώσει" επιλέξε 3 για "Ολοκλήρωση" επιλέξε 4

4

Αλλαγή

2020 © Copyright Πανεπιστήμιο Πειραιώς

Rinkeby Test Network

Account 1
0x8264...92C3

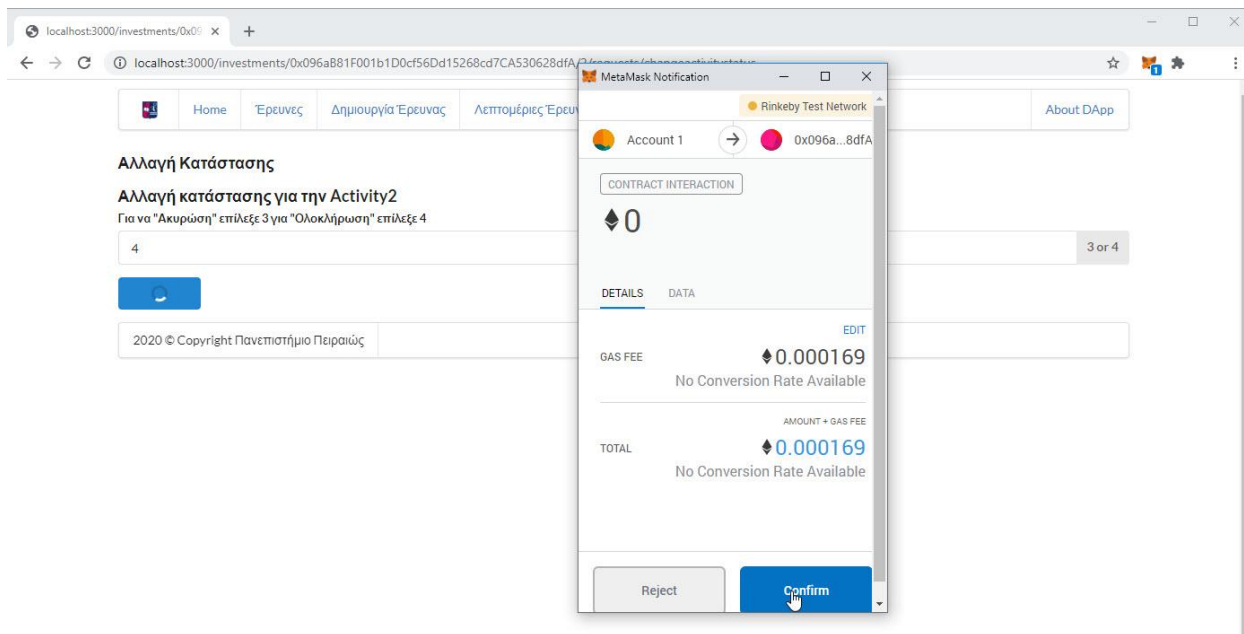
30.7311 ETH

Deposit Send

History

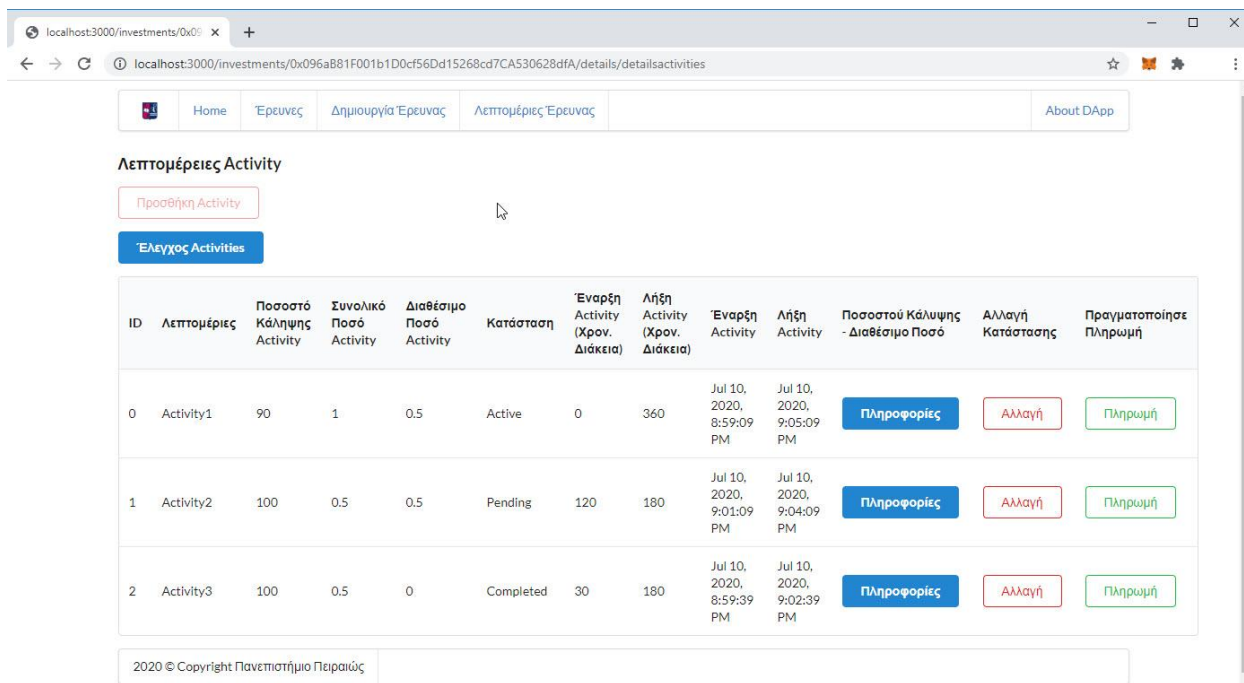
- #381 - 7/10/2020 at 20:26
Return Money -0 ETH
CONFIRMED
- #380 - 7/10/2020 at 20:26
Contract Interaction -0 ETH
CONFIRMED
- #379 - 7/10/2020 at 20:24
Contract Interaction -0 ETH

Εικόνα 61: Αλλαγή Κατάστασης από Επόπτη



Εικόνα 62: Επιβεβαίωση αλλαγής κατάστασης

Σε περίπτωση που η ενέργεια θεωρηθεί ολοκληρωμένη συνεχίζουμε πραγματοποιώντας αλλαγή κατάστασης σε όσες ενέργειες σταδιακά εμφανίζονται ως Pending.



Εικόνα 63: Πληροφορίες Activity

ID	Λεπτομέρειες	Ποσοστό Κάλυψης Activity	Συνολικό Ποσό Activity	Διαθέσιμο Ποσό Activity	Κατάσταση	Έναρξη Activity (Χρον. Διάκεια)	Λήξη Activity (Χρον. Διάκεια)	Έναρξη Activity	Λήξη Activity	Ποσοστό Κάλυψης - Διαθέσιμο Ποσό	Αλλαγή Κατάστασης	Πραγματοποιήσε Πληρωμή	
0	Activity1	90	1	0.5	Completed	0	360	Jul 10, 2020, 8:59:09 PM	Jul 10, 2020, 9:05:09 PM		Πληροφορίες	Αλλαγή	Πληρωμή
1	Activity2	100	0.5	0.5	Completed	120	180	Jul 10, 2020, 9:01:09 PM	Jul 10, 2020, 9:04:09 PM		Πληροφορίες	Αλλαγή	Πληρωμή
2	Activity3	100	0.5	0	Completed	30	180	Jul 10, 2020, 8:59:39 PM	Jul 10, 2020, 9:02:39 PM		Πληροφορίες	Αλλαγή	Πληρωμή

Εικόνα 64: Πληροφορίες Activity

Στο σημείο αυτό να σημειώσουμε πως όλες οι συναλλαγές των οργανισμών καταγράφονται.

Εικόνα 65: Πληροφορίες Πληρωμών

Στην σελίδα που μας εμφανίζεται κάνοντας κλικ στο κουμπί Λεπτομέρειες στο «7. Πληροφορίες Πληρωμών» μπορούμε να δούμε αναλυτικά τις πληρωμές που έχουν πραγματοποιηθεί, σε ποια Activity, από ποιόν Οργανισμό, το ποσό και προς ποιόν πωλητή πραγματοποιήθηκε.

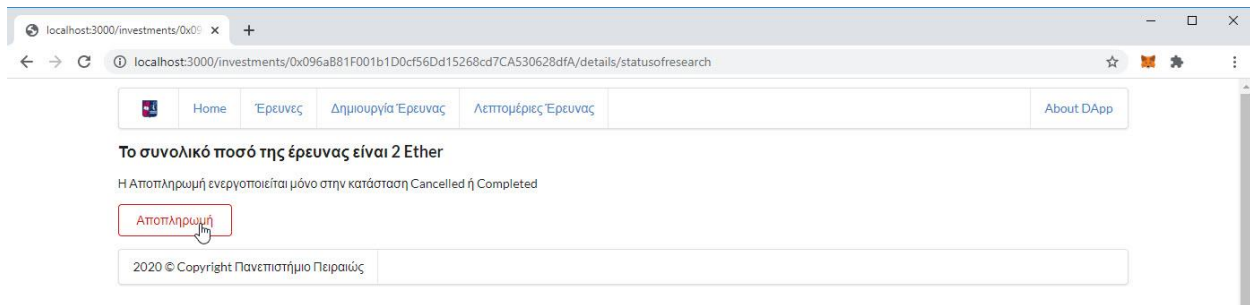
ID	Δραστηριότητα	Ποσό Πληρωμής(wei)	Λεπτομέρειες	Οργανισμός που πραγματοποίησε την πληρωμή	Πωλητής
0	0	0.5	Οργανισμός0_Πληρωμή1	0x3e20241899a1014c5989A5dbC572bcDade18F70b	0x0E3e55b64307aa8953b87d91b63148Ac448Cb04b
1	2	0.5	Οργανισμός0_Πληρωμή2	0x3e20241899a1014c5989A5dbC572bcDade18F70b	0x0E3e55b64307aa8953b87d91b63148Ac448Cb04b

Εικόνα 66:Πληροφορίες Πληρωμών

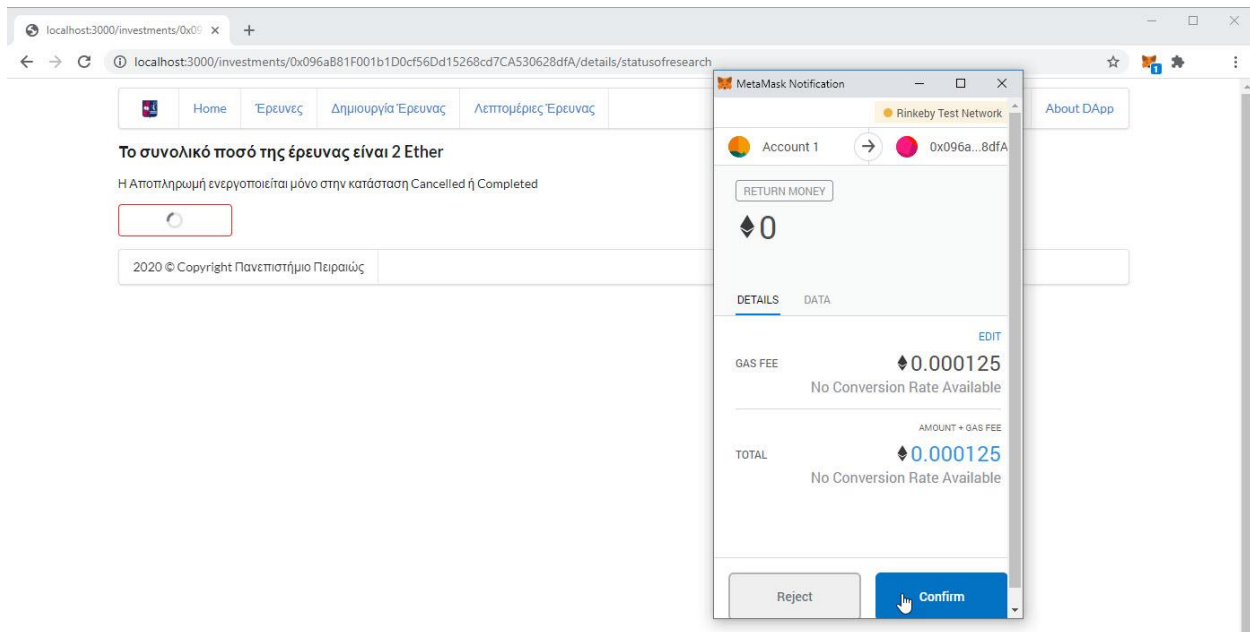
Τέλος, στο «8. Κατάσταση Έρευνας» μπορούμε να δούμε την κατάσταση της έρευνας ανά πάσα στιγμή.

Εικόνα 67:Προβολή κατάσταση Έρευνας

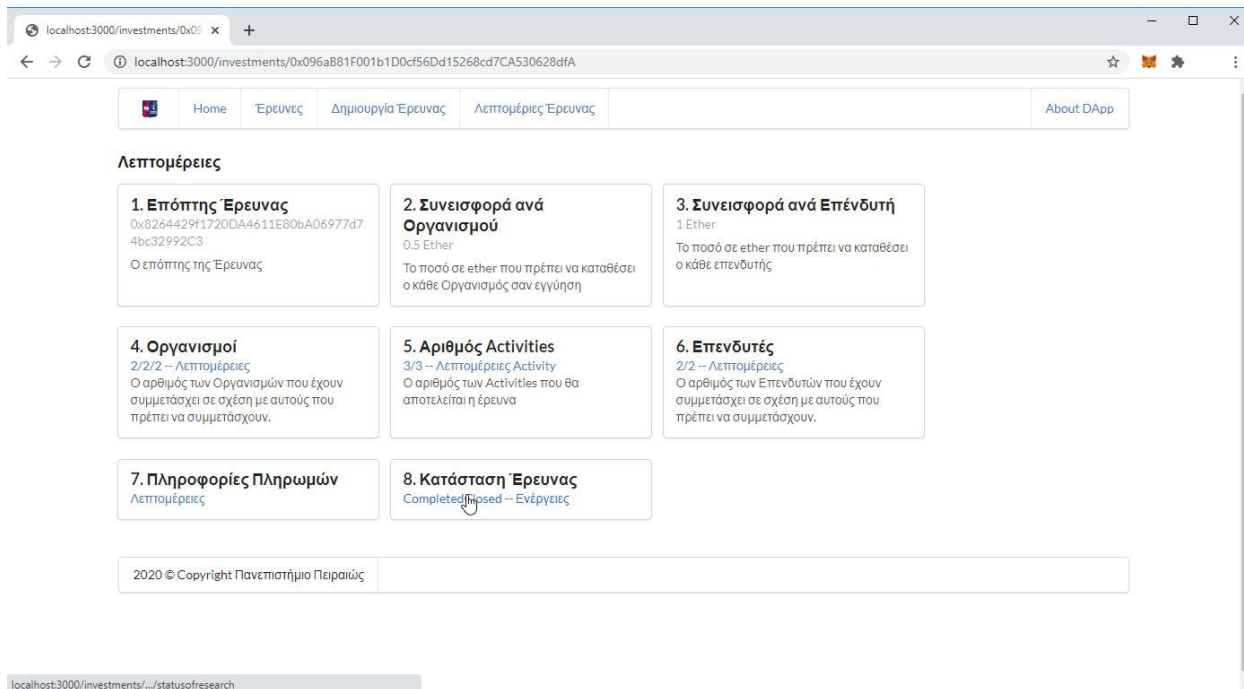
Εάν η έρευνα είναι σε κατάσταση Inactive ή Cancelled ή Completed τότε ο Επόπτης έχει το δικαίωμα να πραγματοποιήσει «Αποπληρωμή»



Εικόνα 68: Διαδικασία Αποπληρωμής



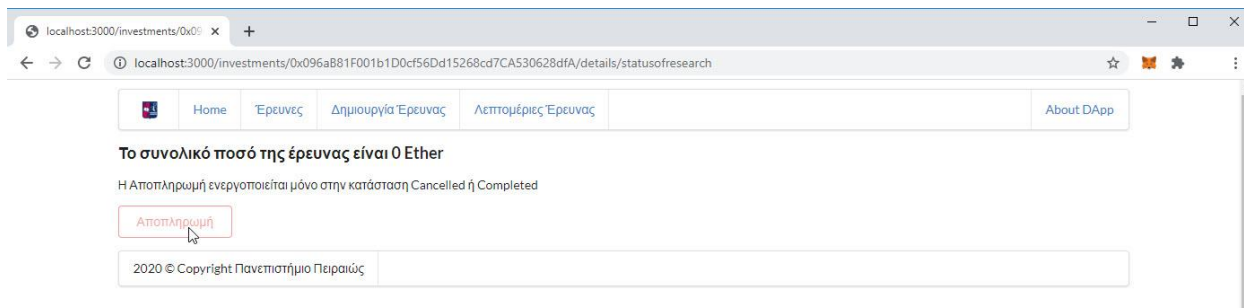
Εικόνα 69: Επιβεβαίωση Αποπληρωμής



Εικόνα 70: Τελικά κατάσταση Έρευνας

Η αποπληρωμή γίνεται με τους παρακάτω τρόπους:

- Εάν η κατάσταση της έρευνας είναι Inactive τότε το χρηματικό ποσό που έχει καταθέσει μέχρι τώρα ο κάθε οργανισμός και επενδυτής το λαμβάνει πίσω.
- Εάν η κατάσταση της έρευνας είναι Cancelled τότε το χρηματικό ποσό που υπάρχει στην έρευνα (Εναπομένουσα Συνεισφορά Επενδυτών μαζί με την Συνεισφορά Οργανισμών) μοιράζεται στους Επενδυτές.
- Εάν η κατάσταση της έρευνας είναι Completed τότε το χρηματικό επιστρέφεται το χρηματικό ποσό που είχαν βάλει οι Οργανισμοί στους Οργανισμούς και το ποσό που απέμεινε από την έρευνα επιστρέφεται στους επενδυτές.



Εικόνα 71: Αποπληρωμή Απενεργοποιημένη

7. Μετρήσεις σε ένα Τυπικό σενάριο χρήσης

Στο κεφάλαιο αυτό θα πραγματοποιήσουμε δυο μετρήσεις για το σύστημά μας.

- Κόστος ανάδρασης με το Blockchain. Στο κόστος αυτό δεν λάβουμε υπόψιν μας τα ether που θα χρειαστούν για να πραγματοποιηθεί η έρευνα (Συνεισφορά Οργανισμών & Επένδυση Επενδυτών) αλλά τα ether που θα ξοδευτούν σε επίπεδο εφαρμογής με γνώμονα την προσφορά του λιγότερου δυνατού Gas.
- Ταχύτητα εκτέλεσης από την δημιουργία της Έρευνας μέχρι και την ολοκλήρωση της. Η μέτρηση θα πραγματοποιηθεί με βάση το χρόνο που χρειάζεται κάθε ανάδραση Blockchain ώστε να πραγματοποιηθεί με το λιγότερο Gas. Θεωρούμε πως ο χρόνος απόκρισης των χρηστών είναι μηδενικός.

Οι μετρήσεις αυτές θα βασιστούν σε πάνω σε ένα τυπικό σενάριο χρήστη. Θα ξεκινήσουμε με την προϋπόθεση πως η Έρευνα που θέλουμε να δημιουργήσουμε θα έχει τα εξής χαρακτηριστικά:

- Δυο οργανισμοί θα λάβουν μέρος στην έρευνα
- Δυο επενδυτές θα λάβουν μέρος στην έρευνα
- Τρεις Activities όπου όλοι οι οργανισμοί θα λάβουν το 50% του ποσοστού σε κάθε Activity
- Μία πληρωμή θα λάβει χώρα κατά την διάρκεια της κάθε Activity
- Η έρευνα δεν θα ακυρωθεί. Θα ολοκληρωθούν επιτυχώς όλα τα Activities με αποτέλεσμα και η έρευνα να θεωρηθεί επιτυχώς ολοκληρωμένη.

Με βάση λοιπόν τις παραπάνω προϋποθέσεις από την δημιουργία της έρευνας μέχρι και την επιτυχής ολοκλήρωσή της πραγματοποιούνται οι παρακάτω ενέργειες αριθμητικά.

- Επόπτης: Δημιουργία Έρευνας , Προσθήκη Οργανισμών (2), Προσθήκη Activities (3), Προσθήκη Ποσοστών (3*2), Αλλαγή Κατάστασης Έρευνας (3), Αποπληρωμή (1) -> Σύνολο 16 Αναδράσεις με το Blockchain.
- Οργανισμός: Συμμετοχή στην Έρευνα (2), Πληρωμή (3) -> Σύνολο 5 Αναδράσεις με το Blockchain
- Επενδυτής: : Συμμετοχή στην Έρευνα (2) -> Σύνολο 2 Αναδράσεις με το Blockchain

Κάθε ανάδραση για να μπορέσει να πραγματοποιηθεί και να την επαληθεύσει κάποιος Node ώστε να μπορέσει να καταγραφεί στην αλυσίδα του Blockchain ως block χρειάζεται περίπου 10-15 δευτερόλεπτα.

Επιπλέον με κόστος Gas Price : 1 gwei και ένα μέσω όρο Gas Limit (Units) 174108 η συνολική χρέωση για κάθε επιτυχημένη ανάδραση είναι περίπου 0.000112 ETH. Με βάση την σημερινή τιμή μετατροπής του ETH σε Ευρώ το κόστος της κάθε ανάδρασης βγαίνει στα 0.023 Ευρώ

Το συνολικό λοιπόν κόστος για την διαδικασία μιας επιτυχημένης εκτέλεσης έρευνας με την βοήθεια της εφαρμογής DApps που δημιουργήσαμε είναι το παρακάτω:

- Συνολικό κόστος ανάδρασης με το Blockchain: Περίπου 0.5 Ευρώ
- Ταχύτητα εκτέλεσης: Περίπου 5 Λεπτά

8. Προοπτικές Επεκτασιμότητας

Στην παρούσα εργασία, υλοποιήσαμε μια DApp εφαρμογή με την οποία μπορεί κανείς να διαχειρίζεται τις έρευνες εξασφαλίζοντας στους Επενδυτές την αίσθηση της ασφάλειας και στους Οργανισμούς που πραγματοποιούν την έρευνα την αίσθηση ευθύνης της ολοκλήρωσης. Έχοντας δημιουργήσει μία τέτοια εφαρμογή πάνω στο Blockchain, το επόμενο βήμα θα ήταν να χρησιμοποιηθεί εσωτερικά σε κάποιον οργανισμό - επιχείρηση.

Πολλά προβλήματα εμφανίζονται σε διάφορους τομείς εσωτερικά μιας επιχείρησης λόγω μη σωστής οργάνωσης. Η παραπάνω εφαρμογή θα μπορούσε να χρησιμοποιηθεί στο εσωτερικό κομμάτι της κάθε επιχείρησης - οργανισμού και να εφαρμόζεται όχι μόνο για εσωτερικές έρευνες αλλά για όλα τα εσωτερικά project που θα μπορούσαν να τρέξουν.

Μιας και σε μια τέτοια εκδοχή οι χρήστες οι οποίοι θα χειρίζονταν την εφαρμογή θα ήταν συγκεκριμένοι χρήστες του οργανισμού θα μπορούσαμε αντί να κάνουμε χρήση ενός public δικτύου Ether, να δημιουργήσουμε ένα ιδιωτικό δίκτυο Ethereum.

Τέλος, ο τρόπος δημιουργία της εφαρμογής δεν περιορίζει το ενδεχόμενο να μπορέσει να προσαρμοστεί και να εφαρμοστεί και σε πολλούς κλάδους όπως σε οικονομικές έρευνες, σε μεγάλα έργα δημοσίου και άλλα Project, που μέχρι τώρα εφαρμοζόταν η μεθοδολογία του Gantt.

9. Βιβλιογραφία

Books

Bitcoin: What's in the whitepaper?

https://huobi-1253283450.cos.ap-beijing.myqcloud.com/1543476765952_lgOT7VVG04Vr3QUjymBa.pdf

BLOCKCHAIN: The foundation behind Bitcoin

<https://www.isical.ac.in/~debrup/slides/Bitcoin.pdf>

Ethereum: A secure decentralised generalised transaction ledger

<https://files.gitter.im/ethereum/yellowpaper/Vlyt/Paper.pdf>

Decentralization in bitcoin and ethereum networks

https://link.springer.com/chapter/10.1007/978-3-662-58387-6_24

MadMax: surviving out-of-gas conditions in Ethereum smart contracts

<https://dl.acm.org/doi/abs/10.1145/3276486>

Introducing Ethereum and solidity

<https://link.springer.com/content/pdf/bfm%253A978-1-4842-2535-6%252F1.pdf>

Smart contracts: security patterns in the ethereum ecosystem and solidity

<https://ieeexplore.ieee.org/abstract/document/8327565>

Site

Elearning E.K.Π.A - <https://elearningekpa.gr/>

Wikipedia - <https://el.wikipedia.org/>

Πανεπιστήμιο Λευκωσίας - <https://www.unic.ac.cy/>

Bitcoin Org - <https://bitcoin.org/>

OliveoilTimes - <https://www.oliveoiltimes.com/>

Survey - <https://survey.gr/>

Investopedia - <https://www.investopedia.com/>

101Blockchains - <https://101blockchains.com/>

Leewayhertz - <https://www.leewayhertz.com/>

OReilly - <https://www.oreilly.com/>

Blockgeeks - <https://blockgeeks.com/>

Udemy - <https://www.udemy.com/>

Etherscan - <https://etherscan.io/>

Onassis.org - <https://www.onassis.org/>