ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ & ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ

Διπλωματική Εργασία

ΑΝΑΠΤΥΞΗ ΕΝΟΣ ΙΔΙΩΤΙΚΟΥ ΔΙΚΤΥΟΥ ΑΛΥΣΙΔΑΣ ΣΥΣΤΟΙΧΙΩΝ ΒΑΣΙΣΜΕΝΟ ΣΤΗΝ ΠΛΑΤΦΟΡΜΑ ΤΟΥ ETHEREUM

Φοιτητής: ΚΟΡΟΜΗΛΑΣ ΠΑΝΑΓΙΩΤΗΣ
ΑΜ: 50106683

Επιβλέπων Καθηγητής

ΚΟΓΙΑΣ ΔΗΜΗΤΡΙΟΣ
Ακαδημαϊκός Υπότροφος/ ΕΣΠΑ

ΑΘΗΝΑ-ΑΙΓΑΛΕΩ, (ΔΕΚΕΜΒΡΙΟΣ) (2020)

UNIVERSITY OF WEST ATTICA
FACULTY OF ENGINEERING
DEPARTMENT OF ELECTRICAL & ELECTRONICS ENGINEERING

Diploma Thesis

DEVELOPMENT OF A PRIVATE ETHEREUM BLOCKCHAIN NETWORK

Student: KOROMILAS PANAGIOTIS
Registration Number: 50106683

Supervisor

KOGIAS DIMITRIOS
Academic Scholar/ ESPA

ATHENS-EGALEO, (DECEMBER) (2020)

ΔΗΛΩΣΗ ΠΕΡΙ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ ΚΑΙ ΛΟΓΟΚΛΟΠΗΣ

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ενυπόγραφα ότι η παρούσα εργασία προετοιμάστηκε και ολοκληρώθηκε από εμένα αποκλειστικά και ότι είμαι ο αποκλειστικός συγγραφέας του κειμένου της.

Η εργασία μου δεν προσβάλλει οποιασδήποτε μορφής δικαιώματα πνευματικής ιδιοκτησίας, προσωπικότητας ή προσωπικών δεδομένων τρίτων, δεν περιέχει έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής ή λογοκλοπής.

Κάθε βοήθεια που έλαβα για την ολοκλήρωση της εργασίας είναι αναγνωρισμένη και αναφέρεται λεπτομερώς στο κείμενό της. Ειδικότερα, έχω αναφέρει ευδιάκριτα μέσα στο κείμενο και με την κατάλληλη παραπομπή όλες τις πηγές δεδομένων, κώδικα προγραμματισμού Η/Υ, απόψεων, θέσεων και προτάσεων, ιδεών και λεκτικών αναφορών που χρησιμοποιήθηκαν, είτε κατά κυριολεξία είτε βάσει επιστημονικής παράφρασης, και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Επιπλέον, όλες οι πηγές που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον και πληρούν τους κανόνες της επιστημονικής παράθεσης κατά τα διεθνή πρότυπα.

Τέλος δηλώνω ενυπόγραφα ότι αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της είναι προϊόν λογοκλοπής.

Ημερομηνία _____

Παναγιώτης Κορομηλάς

(Υπογραφή)

ΑΦΙΕΡΩΣΗ

Την Διπλωματική Εργασία την αφιερώνω στους γονείς μου για την απεριόριστη βοήθεια και υποστήριξη που μου παρείχαν κατά την διάρκεια των σπουδών μου.

ΕΥΧΑΡΙΣΤΙΕΣ

Με την περάτωση της Διπλωματικής εργασίας μου, θα ήθελα να ευχαριστήσω την Πολυχρονάκη Μαρία, τον Ξευγένη Μιχαήλ και όλους όσους βοήθησαν στην εκπόνηση της.
Ιδιαίτερα επιθυμώ να ευχαριστήσω τον κύριο Κόγια Δημήτριο, για την καθοδήγηση που μου παρείχε στην εκπόνηση της παρούσας Διπλωματικής εργασίας και για όλες τις συμβουλές και γνώσεις που αποκόμισα από αυτόν κατά την διάρκεια των σπουδών μου.
Ακόμα, θα ήθελα να ευχαριστήσω τον Καρσλίδη Δημήτριο, για την συνεργασία μας, τις ανταλλαγές απόψεων και την σημαντική βοήθεια που πρόσφερε σε όλα τα στάδια της εργασίας.

Περίληψη

Η διπλωματική εργασία αποτελείται από δύο μέρη, το πρακτικό και το θεωρητικό μέρος. Στο πρακτικό μέρος παρουσιάζεται η δημιουργία ενός ιδιωτικού Blockchain Ethereum δικτύου και η επιτυχής σύνδεση του με μία αποκεντρωμένη εφαρμογή. Το δίκτυο αποτελείται από τρεις κόμβους, δηλαδή τρείς εικονικές μηχανές, οι οποίες υπάρχουν στον Okeanos Cloud και παρέχονται από την GRNET. Επίσης, παρουσιάζονται οι υπολογιστικές απαιτήσεις που χρειάζονται για την ομαλή λειτουργία του δικτύου και οι απαραίτητες ενέργειες και εντολές που πρέπει να εκτελεστούν για την σωστή ρύθμιση των κόμβων, αλλά και του Metamask, που είναι ένα πορτοφόλι με την μορφή μιας επέκτασης στο πρόγραμμα περιήγησης, ώστε να χρησιμοποιηθεί για να ανέβει με επιτυχία μια αποκεντρωμένη εφαρμογή στο ιδιωτικό δίκτυο.

Στο θεωρητικό μέρος εξηγούνται, αρχικά, βασικές έννοιες σχετικά με την τεχνολογία του Blockchain. Για παράδειγμα, γιατί ονομάζεται Blockchain και ποιος είναι ο ρόλος του στο ιδιωτικό δίκτυο, τι είναι η συναίνεση μεταξύ των χρηστών του και γιατί είναι σημαντικό η επίτευξη της. Επιπλέον, γίνεται μια αναφορά σχετικά με τις πιο γνωστές Blockchain πλατφόρμες, αλλά και για παραδείγματα συναίνεσης αλγορίθμων που υπάρχουν.

Στη συνέχεια, ακολουθεί το Ethereum που αποτελεί την πλατφόρμα εκείνη που έχει επιλεχθεί για μελέτη στην παρούσα Διπλωματική. Αναλύεται η αρχιτεκτονική του Ethereum, η οποία περιλαμβάνει το είδος των δικτύων στα οποία ο χρήστης μπορεί να συνδεθεί. Ακόμα, εξηγούνται οι λόγοι που καθιστούν μια εφαρμογή αποκεντρωμένη και τα μέρη που την αποτελούν. Επιπλέον, γίνεται μια αναφορά σχετικά με τον αλγόριθμο συναίνεσης που χρησιμοποιεί το Ethereum, τι είδος λογαριασμών υπάρχουν και τις δυνατότητες που παρέχουν τα πορτοφόλια, όπως το Metamask.

Λέξεις – κλειδιά

Έξυπνο Συμβόλαιο, Αποκεντρωμένη εφαρμογή, Κόμβος, Εικονική Μηχανή, Metamask, Συναίνεση, Αλγόριθμοι συναίνεσης, Λογαριασμός, Κρυπτονόμισμα

Abstract

The dissertation consists of two parts, the practical and the theoretical one. The practical part presents the creation of a private Blockchain Ethereum network and its successful connection to a decentralized application. The network consists of three nodes, i.e. three virtual machines, which exist in the Okeanos Cloud and are provided by GRNET. It also presents the computational requirements which are needed for the smooth operation of the network and the necessary actions and commands that must be performed for the correct configuration of the nodes, but also of Metamask, which is a browser extension wallet that runs in your browser, so the decentralized application is successfully uploaded in the private network.

In the theoretical part are explained, at first, basic concepts about Blockchain technology. For example, why it is called Blockchain and what its role in the private network is, what the consensus between its users is and why it is important to achieve that. In addition to, the most well-known Blockchain platforms and also examples of consensus algorithms are reported.

Afterward, Ethereum follows which is the platform that has been selected for this particular Diploma study. The Ethereum architecture is analyzed, which includes the type of networks that the user can connect. Also, are explained the reasons that make an application decentralized and the parts that make it up. In addition, there is a report on the consent algorithm used by Ethereum, what type of accounts there are and the features are provided by wallets, such as Metamask.

Keywords

Smart Contract, D-App, Node, Virtual Machine – VM, Metamask, Consensus, Consensus Algorithm, Account, Cryptocurrency

Περιεχόμενα

Κατάλογος Εικόνων

ΕΙΣΑΓΩΓΗ

Το κυρίως θέμα της διπλωματικής εργασίας αφορά την δημιουργία ενός ιδιωτικού Blockchain δικτύου. Αρχικά, ένα Blockchain δίκτυο είναι ένα μεγάλο κατανεμημένο δίκτυο υπολογιστών το οποίο λειτουργεί χωρίς την ανάγκη για μεσάζοντες και καταγράφει στο σύνολο του όλες τις συναλλαγές μεταξύ των συμμετεχόντων σε αυτό. Για να έχει κάποιος πρόσβαση σε ένα ιδιωτικό Blockchain δίκτυο, θα πρέπει να έχει προσκληθεί σε αυτό, σε αντίθεση με ένα δημόσιο Blockchain δίκτυο που έχει πρόσβαση ο καθένας. Ο έλεγχος στο δίκτυο γίνεται από ένα σύνολο κανόνων στους οποίους έχουν συμφωνήσει όλοι οι συμμετέχοντες. Η χρήση ενός ιδιωτικού δικτύου γίνεται κυρίως από άτομα εμπιστευτικά, τα οποία ανταλλάζουν σημαντικά δεδομένα για αυτούς.

Τα περισσότερα ιδιωτικά δίκτυα δεν χρησιμοποιούν κρυπτογράφηση και δεν παρέχουν την ίδια ασφάλεια που παρέχει ένα αποκεντρωμένο δίκτυο. Η χωρητικότητα αποθήκευσης δεδομένων του δικτύου μπορεί να είναι απεριόριστη.

Τα ιδιωτικά Blockchain δίκτυα είναι ιδανικά για προγραμματιστές , στους οποίους επιτρέπει να πραγματοποιήσουν τις ιδέες τους χωρίς να πληρώσουν τα κόστη που συνοδεύουν την πραγματοποίηση της λύσης τους σε ένα δημόσιο Blockchain δίκτυο μέσω της χρήσης κάποιου κρυπτονομίσματος, ανάλογα με την πλατφόρμας της επιλογής. Οι μεγάλες επιχειρήσεις μπορούν να αξιοποιήσουν την ασφάλεια που παρέχει η τεχνολογία Blockchain και οι συναλλαγές τους να είναι ορατές στους συμμετέχοντες του δικτύου, και μόνο σε αυτούς. (Laurence, 2019)

Αντικείμενο της διπλωματικής εργασίας

Το κύριο θέμα της εργασίας είναι η δημιουργία ενός κατανεμημένου δικτύου, στο οποίο θα υπάρχει εμπιστοσύνη και ασφάλεια μεταξύ των συναλλαγών των συμμετεχόντων χωρίς να χρειάζεται παραπάνω ενέργειες από τους ίδιους. Το δίκτυο θα το ασφαλίσει αυτό με την επίτευξη της συναίνεσης. Με αυτό τον τρόπο, οι συναλλαγές εκτελούνται πιο γρήγορα σε σύγκριση με τον κλασικό τρόπο εκτέλεσης των συναλλαγών, όπως μιας τράπεζας, όπου τις περισσότερες φορές αναγκάζεται η συναλλαγή να εγκριθεί από τρίτους και έτσι καθυστερείτε η εκτέλεση της συναλλαγής. Τα παραπάνω επιτυγχάνονται με την δημιουργία ενός Blockchain δικτύου, το οποίο είναι και ο κύριος στόχος της παρούσας διπλωματικής.

1.2 Σκοπός και στόχοι

Ο σκοπός της εργασίας είναι η δημιουργία ενός ιδιωτικού Blockchain Ethereum δικτύου και η επίδειξη της λειτουργίας του με χρήση μιας αποκεντρωμένης εφαρμογής. Ο στόχος του δικτύου είναι η ευκολότερη και η γρηγορότερη πραγματοποίηση των συναλλαγών, χωρίς ενδιάμεσους, που στην τελική ωφελεί τους συμμετέχοντες του δικτύου.

1.3 Μεθοδολογία

Η μεθοδολογία που ακολουθήθηκε ήταν η εξής.

- Αναζήτηση πληροφοριών για το Blockchain
- Κατανόηση τρόπου λειτουργίας του Ethereum
- Αναζήτηση πληροφοριών για δημιουργία ιδιωτικού δικτύου για το Ethereum
- Εύρεση πόρων για τη δημιουργία του δικτύου στον ΩΚΕΑΝΟ

1.4 Καινοτομία

Τα στοιχεία της διπλωματικής εργασίας που είναι καινοτομικά είναι το Blockchain, και ιδιαίτερα η πλατφόρμα του Ethereum. Στο Blockchain, κάθε συναλλαγή που πραγματοποιείται, αποθηκεύεται σε αυτό. Βοηθάει στην εύκολη και γρηγορότερη εκτέλεση των συναλλαγών, δίχως προβλήματα, όπως είναι το "μαγείρεμα" των τιμών. Στην ουσία, το Blockchain λειτουργεί ως ένα καθολικό βιβλίο που παρακολουθεί και καταγράφει τα πάντα που τρέχουν σε αυτό. Από την άλλη, το Ethereum, παρέχει την δυνατότητα δημιουργίας αποκεντρωμένων εφαρμογών και έξυπνων συμβολαίων. Ένα έξυπνο συμβόλαιο αποτελείται από υπολογιστικό κώδικα, ο οποίος εκτελείται αυτόματα όταν πληρούνται κάποιες προϋποθέσεις. Στην αποκεντρωμένη εφαρμογή κανείς δεν έχει τον κύριο έλεγχο και όλα τρέχουν αυτόματα, με βάση τον κώδικα που αποτελεί ένα έξυπνο συμβόλαιο. Με αυτό τον τρόπο, οι συναλλαγές εκτελούνται γρήγορα και με ασφάλεια, ανώνυμα χωρίς κάποιος να κατέχει τον κύριο έλεγχο του δικτύου.

1.5 Δομή

Η δομή της διπλωματικής εργασίας αποτελείται κυρίως από την εισαγωγή που αναφέρεται το αντικείμενο της διπλωματικής εργασίας και τέσσερα κεφάλαια. Ακολουθεί το Κεφάλαιο 2, στο οποίο αναφέρονται εισαγωγικές έννοιες για την τεχνολογία του Blockchain. Στο Κεφάλαιο 3, εξηγούνται βασικές έννοιες για το Ethereum, την αρχιτεκτονική του και τη λειτουργία του. Στο Κεφάλαιο 4, παρουσιάζεται η υλοποίηση του πρακτικού μέρους της διπλωματική εργασίας, δηλαδή η δημιουργία ενός ιδιωτικού Blockchain Ethereum δικτύου. Τέλος στο Κεφάλαιο 5, περιέχονται τα συμπεράσματα που εξάχθηκαν από την ανάλυση την διπλωματικής εργασίας.

2 Εισαγωγικές Έννοιες για την Τεχνολογία του Blockchain

2.1 Η τεχνολογία Blockchain

Η ανάγκη του ανθρώπου να εξεύρει αξιόπιστα εργαλεία για την διασφάλιση της αξίας των συναλλαγών και την προστασία των ατόμων που εμπλέκονται σε αυτές συνεχώς και αυξάνεται. Σε αρκετές συναλλαγές εμπλέκονται ενδιάμεσοι, ενώ η συναλλαγή παραμένει σε αναμονή μέχρι την έγκριση της. Αυτό σημαίνει ότι η ταχύτητα πραγματοποίησης των συναλλαγών μειώνεται λόγω των ενδιάμεσων. Στη συνέχεια, χάρη στην κοινωνική και τεχνολογική εξέλιξη, σπουδαίες εφευρέσεις, όπως το ίντερνετ και οι τηλεφωνικές γραμμές βελτίωσαν τις συναλλαγές μειώνοντας την απόσταση μεταξύ του πωλητή και του αγοραστή, αυξάνοντας την ταχύτητα και την αποδοτικότητα τους.

Ωστόσο, παρά τη διευκόλυνση που παρείχαν τα παραπάνω, αρκετές συναλλαγές, ιδίως επιχειρησιακές, παρέμειναν ευάλωτες, καθώς αντιμετωπίζουν τους παρακάτω περιορισμούς:

- Η μακρά διάρκεια των συναλλαγών.
- Επιθέσεις στο κυβερνοχώρο και απάτες μειώνουν την αποδοτικότητα των επιχειρήσεων, με αποτέλεσμα την μείωση κερδών ακόμα και την έκθεση των συμμετεχόντων που ανήκουν στο δίκτυο τους.
- Πάνω από το μισό ποσοστό του παγκόσμιου πληθυσμού, δεν έχουν τραπεζικό λογαριασμό και αναζητούν παράλληλους τρόπους συστημάτων πληρωμής για να καλύψουν τις συναλλαγές τους.

Με την από μέρα σε μέρα εκθετική αύξηση των συναλλαγών, αυξάνεται επίσης η πολυπλοκότητα και επιβραδύνεται η λειτουργία των τωρινών συστημάτων συναλλαγών. Για την κάλυψη αυτών των αναγκών ο κόσμος χρειάζεται δίκτυα συναλλαγών, όπου θα παρέχονται μηχανισμοί που θα εξασφαλίσουν την ασφάλεια και την αξιοπιστία κάθε συναλλαγής.

Μια λύση στο πρόβλημα που εξηγήθηκε παραπάνω είναι το Bitcoin. (Gupta, 2020)

Πρόκειται για ένα ψηφιακό νόμισμα όπου δημιουργήθηκε το 2009 από έναν άγνωστο με το όνομα ονόματι Satoshi Nakamoto. Το Bitcoin δεν ελέγχεται από κανέναν σε αντίθεση με τις παραδοσιακές τράπεζες. Τα Bitcoin δεν εκτυπώνονται αλλά γίνονται “mined” από ανθρώπους που χρησιμοποιούν υπολογιστές σε όλο το κόσμο με την λύση μαθηματικών προβλημάτων. Όπως, μια επιχείρηση έχει τα λογιστικά βιβλία καταγραφής των συναλλαγών της, το Blockchain υπηρετεί το Bitcoin ως ένα «καθολικό βιβλίο» με όλες τις πληροφορίες των συναλλαγών που πραγματοποιούνται, διαθέσιμο για όλους του χρήστες του Blockchain δικτύου.

Συγκεκριμένα, το Blockchain συνιστά ένα κοινό βιβλίο όπου καταγράφονται συναλλαγές και τα περιουσιακά στοιχεία των ατόμων που συμμετέχουν σε ένα Blockchain δίκτυο. Το Bitcoin και το Blockchain δεν είναι το ίδιο. Το Blockchain παρέχει τα μέσα που χρειάζονται για την καταγραφή και αποθήκευση των Bitcoin συναλλαγών. Το Bitcoin είναι η πρώτη περίπτωση χρήσης του Blockchain.

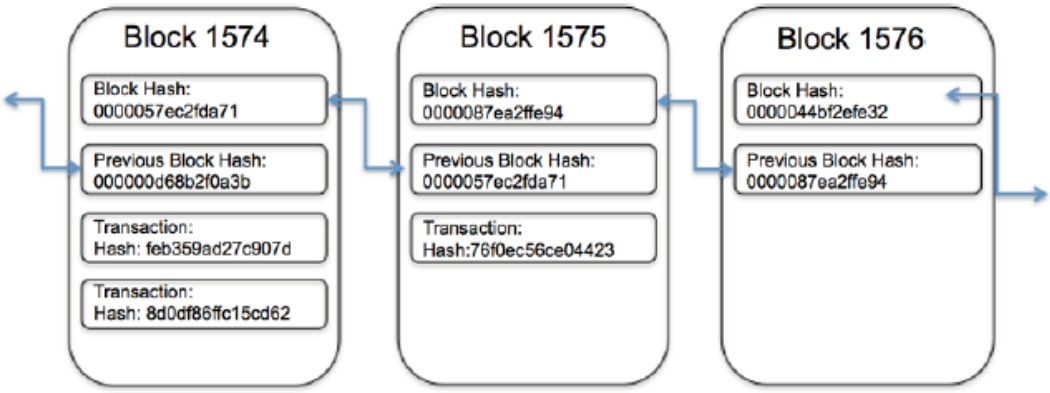
Με τις παραδοσιακές μεθόδους για καταγραφή συναλλαγών και παρακολούθηση των περιουσιακών στοιχείων οι συμμετέχοντες του δικτύου πρέπει να έχουν τα δικά τους βιβλία. Το πρόβλημα που δημιουργείται, είναι ότι αυτή η μέθοδος μπορεί να είναι ιδιαίτερα κοστοβόρα, διότι περιλαμβάνει μεσάζοντες οι οποίοι χρεώνουν τέλη για τις υπηρεσίες τους αλλά και αναξιόπιστη γιατί δεν μπορεί να αποκλείσει κανείς την παραποίηση των βιβλίων.

Το Blockchain δίνει στους χρήστες του την ικανότητα να μοιράζονται ένα κοινό βιβλίο το οποίο ενημερώνεται διαρκώς, μέσω ενός δικτύου ομότιμων κόμβων (peer to peer, P2P) κάθε φορά που μια συναλλαγή πραγματοποιείται. Οι συμμετέχοντες στο δίκτυο ονομάζονται αλλιώς και «κόμβοι», καθώς μπορούν να λάβουν και να στείλουν συναλλαγές σε άλλους κόμβους και οι πληροφορίες που περιέχουν οι συναλλαγές συγχρονίζονται και μεταφέρονται σε όλο το δίκτυο. Το Blockchain δίκτυο είναι αποδοτικό, διότι μειώνει την ανάγκη για μεσάζοντες, δηλαδή είναι λιγότερο δαπανηρό, ενώ γίνεται λιγότερο τρωτό επειδή χρησιμοποιεί μοντέλα κοινής συναίνεσης για να επικυρώσει τις πληροφορίες του. Συνεπώς, οι συναλλαγές είναι ασφαλείς και επικυρωμένες.

Οι συμμετέχοντες και στις δύο περιπτώσεις είναι ίδιοι, με μόνη διαφορά ότι τώρα το βιβλίο όπου περιέχει τις πληροφορίες για τις συναλλαγές και τα περιουσιακά στοιχεία είναι κοινό και διαθέσιμο για όλους. Ένα δίκτυο Blockchain έχει τα παρακάτω χαρακτηριστικά:

- Για την επικύρωση μιας συναλλαγής πρέπει η πλειοψηφία των συμμετεχόντων να συμφωνούν για την εγκυρότητα της.
- Οι συμμετέχοντες γνωρίζουν από που προήλθαν τα περιουσιακά στοιχεία και πως άλλαξαν ιδιοκτησία.
- Κανένας δεν μπορεί να τροποποιήσει τις συναλλαγές από την στιγμή που έχουν καταχωρηθεί στο καθολικό βιβλίο.

Το Blockchain χρωστάει το όνομα του στο τρόπο το οποίο αποθηκεύει τα δεδομένα από τις συναλλαγές δηλαδή σε block τα οποία είναι συνδεδεμένα μεταξύ τους σχηματίζοντας μία αλυσίδα (chain). Καθώς μεγαλώνει ο αριθμός των συναλλαγών, μεγαλώνει και το μέγεθος της αλυσίδας. Τα blocks καταγράφουν τη σειρά των συναλλαγών σε ένα δίκτυο όπου κυβερνάται από ένα σύνολο κανόνων που έχει αποφασιστεί μεταξύ των συμμετέχων του.



Εικόνα 1: Φαίνεται μια σειρά από Blocks, αποθηκευμένη στο Blockchain. Επίσης, κάθε block περιέχει το hash του προηγούμενου και του επόμενου block από αυτόν. Με αυτό τον τρόπο δημιουργείται η αλυσίδα των block, ένα Blockchain. (Manav, 2020)

Κάθε block περιέχει ένα hash, ένα ψηφιακό δαχτυλικό αποτύπωμα ενός block, και το hash του προηγούμενου block. Κάθε block είναι συνδεδεμένο με το προηγούμενο και επόμενο block πάνω στην αλυσίδα. Με αυτόν τον τρόπο κάθε block δυναμώνει την επαλήθευση του προηγούμενου του block, δυναμώνοντας ολόκληρο το Blockchain. Χρησιμοποιώντας την μέθοδο αυτή εμποδίζεται η εισαγωγή ενός block ανάμεσα σε άλλα δύο και η τροποποίηση του.

Σημαντικές για την κατανόηση της έννοιας του Blockchain είναι οι παρακάτω έννοιες.

- Το καθολικό βιβλίο καταγράφει κάθε συναλλαγή στο δίκτυο, μια πηγή αλήθειας. Μοιράζεται σε όλους τους συμμετέχοντες στο δίκτυο και ο καθένας τους έχει ένα αντίγραφο από αυτό. Ακόμα οι συμμετέχοντες έχουν την άδεια να παρατηρήσουν οποιαδήποτε συναλλαγή στην οποία έχουν εξουσιοδότηση.
- Το Blockchain μπορεί να είναι προσβάσιμο μέσω άδειας (permissioned) ή ελεύθερο (permissionless). Στο permissioned Blockchain κάθε χρήστης έχει μια μοναδική ταυτότητα όπου επιτρέπει τη χρήση πολιτικών για τον περιορισμό της συμμετοχής στο δίκτυο και πρόσβαση στις λεπτομέρειες των συναλλαγών. Με την ικανότητα του περιορισμού πρόσβασης στις συναλλαγές έχει ως αποτέλεσμα περισσότερες πληροφορίες συναλλαγών να αποθηκεύονται στο Blockchain και κάθε συμμετέχων έχει την ικανότητα να ορίσει ο ίδιος ποιες πληροφορίες από τις συναλλαγές επιτρέπεται να βλέπουν οι υπόλοιποι συμμετέχοντες.
- Σε μια επιχείρηση οι συμμετέχοντες είναι γνωστοί μεταξύ τους και υπάρχει εμπιστοσύνη. Οι συναλλαγές μπορούν να πραγματοποιηθούν και να επαληθευθούν μέσω συμφωνίας.
- Ένα έξυπνο συμβόλαιο είναι μια συμφωνία ή ένα σύνολο κανόνων όπου κυβερνά μια συναλλαγή. Αποθηκεύεται στο Blockchain και εκτελείται ως αναπόσπαστο μέρος της συναλλαγής.

Γενικά παρατηρείται ότι το Blockchain είναι αξιόπιστο, καθώς ενισχύει την σχέση εμπιστοσύνης μεταξύ των συμμετεχόντων. Η εμπιστοσύνη αυτή επιτυγχάνεται σύμφωνα με τα παρακάτω:

- Το καθολικό βιβλίο είναι κοινό για όλους και ενημερώνεται με κάθε συναλλαγή. Η ύπαρξη του Blockchain δεν εξαρτάται από καμία οντότητα.
- Οι συμμετέχοντες έχουν πρόσβαση στις ίδιες καταγραφές, μπορούν να επικυρώσουν συναλλαγές και να επαληθεύσουν τις ταυτότητες ή τις ιδιοκτησίες χωρίς την εμπλοκή τρίτων μεσαζόντων.

Τέλος κάθε συμμετέχων πρέπει να συμφωνήσει στην επικύρωση μιας συναλλαγής. Αυτό επιτυγχάνεται με τη χρήση αλγορίθμων συναίνεσης. (Gupta, 2020)

2.2 Οι πιο γνωστές Blockchain πλατφόρμες

Μία από τις πιο γνωστές πλατφόρμες στο ευρύ κοινό είναι το Bitcoin. Η σημασία που κατέχει για το Blockchain είναι τόσο μεγάλη όσο και η σπουδαιότητα που έχει ένα νόμισμα για ένα κράτος. Είναι το χρυσό πρότυπο των ψηφιακών περιουσιακών στοιχείων. Η κρυφή αλήθεια είναι ότι δύσκολα χρησιμοποιείται ως ψηφιακό νόμισμα. Με την αύξηση της διασημότητας του Bitcoin, αυξήθηκε η δυσκολία αγοράς πραγμάτων και με τις συχνές μεταβολές των τιμών του δεν συστήνεται να χρησιμοποιηθεί υπό την μορφή μετρητών. (Hargrave, 2019)

Πέρα από τη χρήση του ως ψηφιακό νόμισμα για αγορές, το Bitcoin Blockchain είναι ένα καθολικό βιβλίο, το οποίο καταγράφει τις συναλλαγές που πραγματοποιούνται στο Bitcoin δίκτυο. Τα Bitcoins μεταφέρονται από τον τρέχοντα κάτοχο τους, που υπογράφει μια συναλλαγή, όπου μεταφέρει μια αξία, σε νέο ιδιοκτήτη. Ο νέος ιδιοκτήτης επαναλαμβάνει την ίδια διαδικασία για να μεταφέρει τα Bitcoins σε επόμενους χρήστες. (Liu-Thorrold, et al., 2017)

Επίσης, το Hyperledger Fabric συνιστά θεμέλιο για την ανάπτυξη των περισσότερων blockchain εφαρμογών. Το Fabric είναι μοναδικό, διότι επιτρέπει στους προγραμματιστές να χρησιμοποιούν κομμάτια του Fabric χωρίς να δεσμεύονται σε όλη του τη λειτουργικότητα. Ακόμα, το Fabric μπορεί να δημιουργήσει έξυπνα συμβόλαια τα οποία ονομάζονται «Chaincode».

Το Fabric είναι permissioned blockchain και δεν χρησιμοποιεί κρυπτονόμισμα. Αυτό σημαίνει, ότι όλοι οι συμμετέχοντες είναι γνωστοί μεταξύ τους σε αντίθεση με ένα τυπικό δημόσιο Blockchain, στο οποίο όλοι οι συμμετέχοντες είναι ανώνυμοι από προεπιλογή. Το Fabric λειτουργεί όπως τα περισσότερα Blockchains, δηλαδή καταγράφει τα ψηφιακά γεγονότα σε ένα βιβλίο. Τα γεγονότα είναι δομημένα ως συναλλαγές και μοιράζονται στους συμμετέχοντες. Οι συναλλαγές εκτελούνται δίχως κρυπτονομίσματα.

Όλες οι συναλλαγές είναι ασφαλείς και ιδιωτικές. Το Fabric διατηρεί την ακεραιότητα του, επιτρέποντας ενημερώσεις με την συναίνεση των συμμετεχόντων. Από την στιγμή που ένα γεγονός έχει καταγραφεί, δεν μπορεί να αλλοιωθεί.

Αξίζει, επιπλέον να αναφερθούμε στο Ethereum, μία από τις δημοφιλέστερες Blockchain πλατφόρμες που αποτελεί και βασικό αντικείμενο μελέτης της εργασίας αυτής.. Είναι μία αποκεντρωμένη πλατφόρμα που χρησιμοποιεί «Turing-complete» γλώσσα για την συγγραφή και εφαρμογή έξυπνων συμβολαίων. Η δυνατότητα του Ethereum να δημιουργεί έξυπνα συμβόλαια επιτρέπει σε περίπλοκες εφαρμογές, όπως χρηματοοικονομικές συναλλαγές, να εκτελούνται στην αποκεντρωμένη πλατφόρμα.

Το Ethereum είναι σίγουρα το καλύτερο μέρος για την ανάπτυξη μιας αποκεντρωμένης εφαρμογής. Έχει γρήγορη ανάπτυξη, παρέχει ασφάλεια -για μικρές εφαρμογές- και την ικανότητα για τις εφαρμογές να αλληλοεπιδρούν μεταξύ τους.

Οι γλώσσες προγραμματισμού «Turing-complete» είναι το κύριο χαρακτηριστικό που κάνει το Ethereum Blockchain πιο ισχυρό από το Bitcoin Blockchain στη δημιουργία νέων προγραμμάτων. Η προγραμματιστική γλώσσα του Ethereum δίνει την δυνατότητα δημιουργίας εφαρμογών με ελάχιστες γραμμές κώδικα και τις καθιστά αρκετά ασφαλείς.

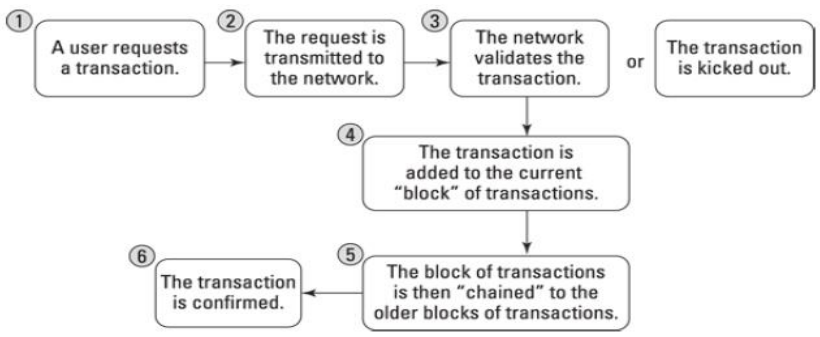
Το Ethereum δημιούργησε ένα εντελώς άλλο είδος εφαρμογών. Η πλατφόρμα του Ethereum χρησιμοποιείται για την καταγραφή ψηφιακών περιουσιακών στοιχείων (πχ Bitcoin token), ιδιοκτησίας (πχ κομμάτι γης) και την διαχείριση αποκεντρωμένων αυτόνομων οργανισμών (DAOs). Το Ethereum άνοιξε ένα νέο δρόμο στην οργάνωση των επιχειρήσεων και των κυβερνήσεων. Έχει καταφέρει να κρατήσει, να μοιράσει και να ανταλλάξει αξία χωρίς συναντήσεις μεταξύ ομάδων. Συνεπώς, ο κώδικας κάνει όλη τη δουλειά.

Όμως, για την εύκολη διαχείριση των παραπάνω, το Ethereum μας δίνει την δυνατότητα δημιουργίας αποκεντρωμένων εφαρμογών, των D-Apps. Τα D-Apps δημιουργήθηκαν για να αντικαταστήσουν την κεντρική διοίκηση των περιουσιακών στοιχείων και των οργανισμών. Αυτή η δομή έχει μεγάλη έφεση, επειδή πολλοί άνθρωποι πιστεύουν ότι η απόλυτη δύναμη προκαλεί διαφθορά. Επομένως, για αυτούς που φοβούνται να χάσουν τον έλεγχο, αυτός ο τύπος δομής έχει μεγάλες επιπτώσεις. (Laurence, 2019)

2.3 Ο σημαντικός ρόλος του Consensus

Το Blockchain είναι ισχυρό επειδή δημιουργεί συστήματα που αυτο-διορθώνουν, χωρίς την ανάγκη τρίτου να επιβάλλει τους κανόνες. Αντιθέτως, επιτυγχάνουν την επιβολή των κανόνων μέσω του αλγόριθμου της συναίνεσης.

Στο κόσμο του blockchain, «consensus» ή «συναίνεση» είναι η διαδικασία ανάπτυξης μιας συμφωνίας, μεταξύ μιας ομάδας που αποτελείται από δύσπιστους μετόχους. Αυτοί είναι οι «Πλήρεις Κόμβοι» στο δίκτυο, οι οποίοι μπορούν να επικυρώσουν συναλλαγές που εισάγονται στο δίκτυο και καταγράφονται στο καθολικό βιβλίο.



Εικόνα 2: Παρουσιάζονται τα στάδια που περνάει μια συναλλαγή μέχρι να εγκριθεί ή να απορριφθεί. (Laurence, 2019)

Κάθε Blockchain έχει τους δικούς του αλγόριθμους, για την δημιουργία συμφωνίας εντός του δικτύου του και για τις καταχωρήσεις που προστίθενται. Υπάρχουν αρκετά διαφορετικά μοντέλα για την δημιουργία συναίνεσης επειδή κάθε Blockchain δημιουργεί διαφορετικά είδη καταγραφών. Μερικά Blockchains ανταλλάζουν αξία, ενώ άλλα αποθηκεύουν δεδομένα και άλλα χρησιμοποιούνται για την ασφάλεια των συστημάτων και των συμβολαίων.

Το Bitcoin, για παράδειγμα, ανταλλάζει την αξία των tokens του μεταξύ των συμμετεχόντων στο δίκτυο του. Τα tokens αυτά έχουν εμπορική αξία, οπότε οι απαιτήσεις που σχετίζονται με την απόδοση, επεκτασιμότητα και την σταθερότητα είναι υψηλές. Το bitcoin λειτουργεί υπό την προϋπόθεση, ότι ένας κακόβουλος εισβολέας μπορεί να θέλει να καταστρέψει το ιστορικό των συναλλαγών, με σκοπό να κλέψει τα tokens. Το Bitcoin εμποδίζει την παραπάνω ενέργεια χρησιμοποιώντας το μοντέλο συναίνεσης "Proof of Work" (POW), το οποίο λύνει και το πρόβλημα των βυζαντινών στρατηγών. (Küfner, 2018)

Τα περισσότερα Blockchains λειτουργούν υπό την προϋπόθεση, ότι θα δεχτούν επιθέσεις από εξωτερικές δυνάμεις ή από χρήστες του συστήματος. Η αναμενόμενη απειλή και ο βαθμός εμπιστοσύνης που το δίκτυο έχει στους κόμβους που χειρίζονται το Blockchain, καθορίζει τον τύπο του αλγόριθμου συναίνεσης που θα χρησιμοποιηθεί για την ασφάλεια του καθολικού βιβλίου. Για παράδειγμα, το Bitcoin και το Ethereum προσδοκούν μεγάλο βαθμό απειλής και χρησιμοποιούν έναν δυνατό αλγόριθμο συναίνεσης, ο οποίος ονομάζεται Proof of Work.

Στα Blockchains που χρησιμοποιούνται για την καταγραφή οικονομικών συναλλαγών μεταξύ γνωστών συμμετεχόντων μπορούν να χρησιμοποιήσουν μια γρήγορη και ελαφριά συναίνεση. Η ανάγκη τους για γρήγορες συναλλαγές είναι πολύ σημαντική. Ο αλγόριθμος συναίνεσης Proof of work είναι αργός και δαπανηρός για αυτούς, λόγω των λίγων συμμετεχόντων στο δίκτυο και την άμεση ανάγκη που υπάρχει για κάθε συναλλαγή. Επίσης, δεν χρειάζονται token ή κρυπτονόμισμα για να ενθαρρύνει την επεξεργασία συναλλαγών. Οπότε, εξαφανίζουν τα παραπάνω από το σύστημα τους και τρέχουν γρηγορότερα και φθηνότερα από τα POW συστήματα όπως είναι το Hashcash. (Laurence, 2019)

2.4 Παραδείγματα Consensus Αλγορίθμων

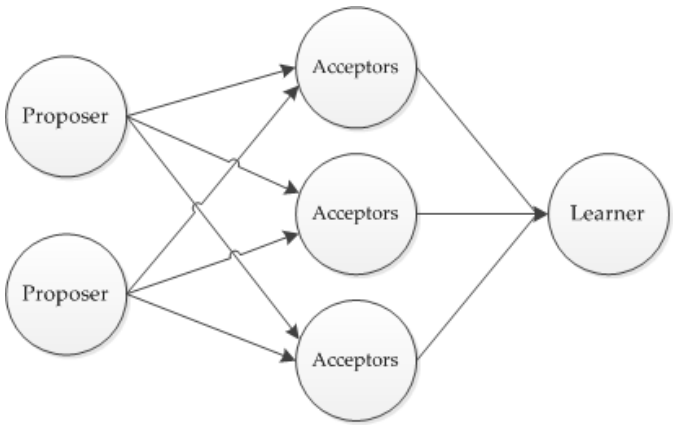
Το Blockchain είναι ένα κατανεμημένο δίκτυο που παρέχει ιδιωτικότητα και ασφάλεια. Δεν υπάρχει κεντρική αρχή για την επικύρωση και την επαλήθευση των συναλλαγών, ωστόσο κάθε συναλλαγή στο Blockchain θεωρείται ότι είναι πλήρως ασφαλής και επαληθευμένη. Αυτό είναι δυνατό μόνο χρησιμοποιώντας ένα πρωτόκολλο συναίνεσης που αποτελεί βασικό μέρος οποιουδήποτε δικτύου Blockchain.

Ο αλγόριθμος για την επίτευξη της συναίνεσης είναι μια διαδικασία μέσω της οποίας όλοι οι συμμετέχοντες ενός κατανεμημένου δικτύου, π.χ., ενός δικτύου Blockchain, καταλήγουν σε μια κοινή συμφωνία σχετικά με το δίκτυο και στην περίπτωση του Blockchain, αφορά την τρέχουσα κατάσταση του καθολικού βιβλίου. Οι αλγόριθμοι συναίνεσης προδίδουν αξιοπιστία στο Blockchain δίκτυο και δημιουργούν εμπιστοσύνη μεταξύ κόμβων σε ένα κατανεμημένο δίκτυο. Ουσιαστικά, διασφαλίζει ότι κάθε νέο μπλοκ που προστίθεται στο Blockchain είναι η μοναδική έκδοση της αλήθειας που συμφωνείται από όλους τους κόμβους του Blockchain. (Patel, 2020)

-Paxos

Ο αλγόριθμος Paxos εντάσσεται στους αλγόριθμους συναίνεσης και λειτουργεί ως αλγόριθμος ψηφοφορίας. Ο αλγόριθμος Paxos έχει τρείς οντότητες:

- **Proposers:** Δέχονται τιμές από τους Clients και προσπαθούνε να πείσουνε τους acceptors να δεχτούν τις προτεινόμενες τιμές τους. Ο client εκδίδει ένα αίτημα στο κατανεμημένο σύστημα και περιμένει μια απάντηση.
- **Acceptors:** Αποδέχονται ορισμένες προτεινόμενες τιμές από τους Proposers και τους ενημερώνει εάν κάτι άλλο έγινε αποδεκτό. Η απάντηση ενός αποδέκτη αντιπροσωπεύει μια ψήφο για μια συγκεκριμένη πρόταση.
- **Learners:** Ανακοινώνουν το αποτέλεσμα.



Εικόνα 3: Τρόπος λειτουργίας του Paxos. Οι proposers υποβάλλουν προτάσεις στους acceptors. Όταν ένας acceptor αποδέχεται μια τιμή, στέλνει το αποτέλεσμα στους κόμβους - learners. (Macdonald, 2018)

Ο αλγόριθμος Paxos είναι ένα πρωτόκολλο στο οποίο κερδίζει η πλειοψηφία. Ένας client στέλνει ένα αίτημα σε οποιονδήποτε proposer του Paxos. Στη συνέχεια, ο proposer εκτελεί ένα πρωτόκολλο δύο φάσεων με τους acceptors. Αυτό σημαίνει ότι οι proposers αλληλοεπιδρούν δύο φορές με τους acceptors. Παρακάτω περιγράφονται οι δύο φάσεις:

- **Φάση 1:** Ένας proposer ρωτά όλους τους acceptors εάν κάποιος έχει ήδη λάβει μια πρόταση. Εάν η απάντηση είναι όχι, προτείνει μια τιμή.
- **Φάση 2:** Εάν η πλειοψηφία των acceptors συμφωνεί με αυτήν την τιμή, τότε αυτή είναι η συναίνεσή μας.

Όταν ένας proposer λαμβάνει από τον client ένα αίτημα για να επιτύχει συναίνεση σχετικά με μια τιμή, ο proposer πρέπει να δημιουργήσει μια πρόταση με έναν αριθμό. Αυτός ο αριθμός πρέπει να έχει δύο ιδιότητες:

- Πρέπει να είναι μοναδικός. Κανένας proposer δεν μπορεί να προτείνει τον ίδιο αριθμό.

- Πρέπει να είναι μεγαλύτερος από οποιοδήποτε άλλο αναγνωριστικό που χρησιμοποιήθηκε στο δίκτυο. Ένας proposer μπορεί να χρησιμοποιήσει έναν αυξανόμενο μετρητή ή να χρησιμοποιήσει μια χρονική σήμανση επιπέδου νανοδευτερόλεπτου για να το επιτύχει. Εάν ο αριθμός δεν είναι μεγαλύτερος από αυτόν που χρησιμοποιήθηκε προηγουμένως, ο proposer θα το ανακαλύψει απορρίπτοντας την πρότασή του και θα πρέπει να προσπαθήσει ξανά. (Krzyzanowski, 2018)

Λόγω της πολυπλοκότητας του Paxos, ο Ongaro παρουσίασε έναν απλούστερο αλγόριθμο που λέγεται Raft. Το Raft σχεδιάστηκε για καλύτερη κατανόηση του πώς μπορεί να επιτευχθεί η συναίνεση. Πριν από το Raft, το Paxos θεωρούνταν το ιερό δισκοπότηρο για την επίτευξη συναίνεσης.

Ο αλγόριθμος Raft είναι ένα ασύμμετρο μοντέλο βασισμένο σε ηγέτες. Ένας κόμβος σε ένα σύστημα μπορεί να βρίσκεται μόνο σε μία από τις τρεις καταστάσεις ανά πάσα στιγμή:

- Ηγέτης: Μόνο ο κόμβος που έχει εκλεγεί ως ηγέτης μπορεί να αλληλοεπιδράσει με τον client. Όλοι οι άλλοι κόμβοι συγχρονίζονται με τον ηγέτη. Σε οποιαδήποτε στιγμή, μπορεί να υπάρχει το πολύ ένας ηγέτης.
- Ακόλουθος: Οι οπαδοί-κόμβοι συγχρονίζουν το αντίγραφο των δεδομένων τους με αυτό του ηγέτη μετά από κάποιο χρονικό διάστημα. Όταν ο κόμβος-ηγέτης «πέφτει» για οποιονδήποτε λόγο, ένας από τους οπαδούς μπορεί να διεξάγει εκλογές και να γίνει ηγέτης.
- Υποψήφιος: Κατά τη στιγμή της διεξαγωγής εκλογών για την επιλογή του κόμβου-ηγέτη, οι κόμβοι μπορούν να ζητήσουν ψήφους από άλλους κόμβους. Ως εκ τούτου, καλούνται υποψήφιοι όταν έχουν ζητήσει ψήφους. Αρχικά, όλοι οι κόμβοι βρίσκονται στην κατάσταση υποψηφίων. (Hooda, 2018)

Στο αρχικό στάδιο, όλοι οι κόμβοι είναι ακόλουθοι. Για να γίνει ένας ακόλουθος (κόμβος) ηγέτης, πρέπει να γίνει υποψήφιος και να ξεκινήσει έναν γύρο εκλογικών ψήφων. Εάν ο κόμβος δεν λάβει αρκετές ψήφους, ο κόμβος γίνεται ακόλουθος ξανά. Ωστόσο, εάν λάβει την πλειοψηφία των ψήφων, ο κόμβος γίνεται ηγέτης. Εάν ο ηγέτης αντιμετωπίσει δυσκολίες στην λειτουργία του, θα αντικατασταθεί από νέο ηγέτη. Ο αρχικός ηγέτης επιστρέφει αυτόματα στην κατάσταση των ακόλουθων αφού ανακάμψει από τις αποτυχίες.

Επίσης, ο εκλεγμένος ηγέτης για να διατηρήσει την εξουσία του, θα πρέπει να στέλνει συνεχώς ένα πακέτο στους άλλους κόμβους του δικτύου όπου θα τους ενημερώνει για την λειτουργία του. Εάν ένας ακόλουθος δεν λάβει το πακέτο κατά τη διάρκεια ενός συγκεκριμένου χρονικού που έχει αποφασιστεί, ο ηγέτης θεωρείται ότι έχει καταρρεύσει και ο ακόλουθος αλλάζει την κατάστασή του σε υποψήφιο και ξεκινά η εκλογή ενός νέου ηγέτη.

Η διανομή του αρχείου καταγραφής των συναλλαγών εφαρμόζεται μέσω ισχυρής ηγεσίας. Ο ηγέτης λαμβάνει το αίτημα του client, το προσαρτά στο αρχείο καταγραφής και επαναλαμβάνει το

αρχείο καταγραφής σε άλλους ακόλουθους. Το Raft διασφαλίζει την ασφάλεια επιτρέποντας μόνο σε έναν ηγέτη να αποφασίσει αν θα δημιουργήσει ένα αρχείο καταγραφής.

Ωστόσο, παρόλο που ο μηχανισμός του Raft δεν είναι ακριβώς ο ίδιος με του Paxos, τα προβλήματα που επιλύουν και οι αντισταθμιστικές πολιτικές που υιοθετούν μπορούν να θεωρηθούν παρόμοια. Δηλαδή, το Raft μπορεί να αντιμετωπίσει προβλήματα, όπως όταν ένας κόμβος ενδέχεται να διακόψει την λειτουργία του ανά πάσα στιγμή ή να σταματήσει να λειτουργεί για ένα μικρό χρονικό διάστημα και να ανακάμψει αργότερα. Ακόμα το δίκτυο ενδέχεται να διακοπεί ανά πάσα στιγμή. Αυτά τα προβλήματα ονομάζονται «crash fault» και είναι ο πιο βασικός και κοινός τύπος σφαλμάτων που πρέπει να επιλυθούν σε κατανεμημένα συστήματα. (vic, 2019)

3 Η πλατφόρμα του Ethereum

3.1 Αρχιτεκτονική

Το Ethereum είναι μια πλατφόρμα ανοιχτού κώδικα, που χρησιμοποιεί την τεχνολογία Blockchain για να δημιουργήσει αποκεντρωμένες ψηφιακές εφαρμογές, γνωστές και ως "D-app" (Decentralized Applications). Αυτές οι εφαρμογές επιτρέπουν στους χρήστες να συνάπτουν συμφωνίες και συναλλαγές απευθείας μεταξύ τους για να αγοράζουν, να πωλούν και να εμπορεύονται αγαθά και υπηρεσίες χωρίς μεσάζοντα. Επίσης, το Ethereum λειτουργεί μέσω ενός παγκόσμιου δικτύου υπολογιστών που συνεργάζονται. Το δίκτυο συγκεντρώνει και εκτελεί έξυπνα συμβόλαια που θεωρητικά είναι ανεξάρτητα από τυχόν παρεμβολές τρίτων, καθώς το Blockchain είναι ανθεκτικό σε παραβιάσεις. Τα έξυπνα συμβόλαια λειτουργούν ακριβώς όπως έχουν προγραμματιστεί, μειώνοντας σημαντικά τον κίνδυνο απάτης και αυτο-εκτελούνται, όπως ένα μηχάνημα αυτόματης πώλησης που εκτελεί τους όρους της σύμβασης ψηφιακά. Όταν αποδειχθεί ότι πληρούνται ορισμένες προϋποθέσεις, όπως η μεταφορά μιας πληρωμής, τότε τα εμπορεύματα μεταφέρονται ή καθίστανται προσβάσιμα στον αγοραστή.

3.1.1 Δίκτυο

Υπάρχει μια ποικιλία δικτύων που βασίζονται στο Ethereum. Μεταξύ αυτών των δικτύων είναι τα Ethereum, Ethereum Classic, Ella, Expanse, Ubiq, Musicoin και πολλά άλλα. Αυτά τα δίκτυα έχουν ανάγκη από προγραμματιστές του Ethereum Client για να κάνουν μικρές αλλαγές προκειμένου να υποστηρίξουν κάθε δίκτυο.

Υπάρχουν έξι κύριες υλοποιήσεις του πρωτοκόλλου του Ethereum, γραμμένες σε έξι διαφορετικές γλώσσες:

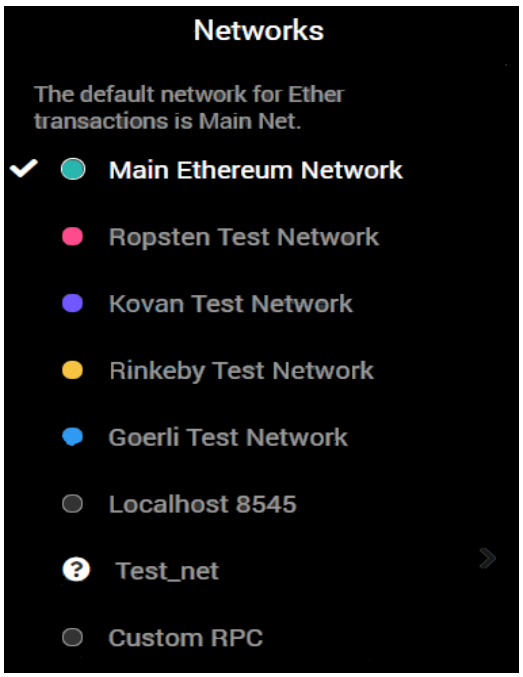
- Parity, γραμμένη σε Rust
- Geth, γραμμένη σε Go
- cpp-Ethereum, γραμμένη σε C++
- pyEthereum, γραμμένη σε Python
- Mantis, γραμμένη σε Scala
- Harmony, γραμμένη σε Java

Για να υπάρχει μια επιτυχής σύνδεση στο δίκτυο του Ethereum, αρχικά χρειάζεται ένα πορτοφόλι όπως είναι το Metamask. Αυτό μας παρέχει την δυνατότητα σύνδεσης σε πολλά δίκτυα του Ethereum. Το Metamask από προεπιλογή θα προσπαθήσει να συνδεθεί στο κύριο δίκτυο (main net) του Ethereum. Οι υπόλοιπες επιλογές είναι δημόσια τεστ δίκτυα (testnet), κόμβοι του Ethereum της επιλογής μας και κόμβοι που τρέχουν τοπικά στον υπολογιστή μας. Τα δημόσια τεστ δίκτυα

χρησιμοποιούνται για την δοκιμή εφαρμογών πριν ανέβουν στο κύριο δίκτυο του Ethereum. Το κύριο δίκτυο του Ethereum ή αλλιώς Main Ethereum Network είναι το κύριο δημόσιο Ethereum Blockchain και περιέχει πραγματικά ETH, με πραγματικές αξίες και συνέπειες. Επίσης, υπάρχει το Ropsten όπου σε αυτό τα ETH δεν έχουν καμία αξία. Είναι ένα δημόσιο Ethereum test Blockchain και τρέχει το ίδιο πρωτόκολλο με το Ethereum. Ακόμα, υπάρχει το Kovan, το οποίο είναι ένα δημόσιο Ethereum test Blockchain. Τα ETH δεν έχουν καμία αξία και υποστηρίζεται από το Parity μόνο. Το Parity είναι ένα λογισμικό ανοιχτού κώδικα που επιτρέπει σε ένα χρήστη να τρέχει έναν κόμβο στο δημόσιο Ethereum ή σε οποιοδήποτε άλλο δίκτυο Blockchain που χρησιμοποιεί Ethereum πρωτόκολλο.

Επιπλέον, ένα δημόσιο Ethereum Blockchain και δίκτυο που υπάρχει είναι το Rinkeby όπου και εκεί τα ETH δεν έχουν αξία. Εκτός από τα παραπάνω που αναφέρθηκαν, υπάρχει ακόμα η σύνδεση με χρήση του localhost 8545 και Custom RPC. Το localhost 8545 επιτρέπει την σύνδεση ενός κόμβου με έναν υπολογιστή, όπου ο κόμβος μπορεί να είναι μέρος ενός δημόσιου Blockchain ή ιδιωτικού. Τέλος, το Custom RPC επιτρέπει την σύνδεση με οποιοδήποτε κόμβο που χρησιμοποιεί Geth. Το geth είναι μία διεπαφή γραμμής εντολών που παρέχει την δυνατότητα ανάπτυξης ενός Ethereum κόμβου σε ένα δίκτυο. (Wood & Antonopoulos, 2019)

Στην παρακάτω εικόνα φαίνονται τα δίκτυα του Ethereum στο Metamask. Το Test_net είναι ένα δίκτυο και έχει δημιουργηθεί για την επίτευξη του στόχου της διπλωματικής εργασίας. Η σύνδεση μεταξύ του υπολογιστή και του δικτύου έχει γίνει με την βοήθεια του Metamask χρησιμοποιώντας Custom Rpc.



Εικόνα 4: Δίκτυα του Ethereum μέσα από το Metamask

3.1.2 Άλλες Πλατφόρμες που βασίζονται στο Ethereum

Το EOS είναι μία από τις πολλές εναλλακτικές λύσεις του Ethereum. Είναι ένα ολοκαίνουργιο Blockchain project, όπου ξεκίνησε το 2017, που μπορεί να χειριστεί έξυπνα συμβόλαια. Ο απώτερος στόχος του EOS είναι ο γρήγορος και φθηνός χειρισμός των έξυπνων συμβολαίων σε όλο το κόσμο. Το Blockchain του EOS είναι επίσης δημόσιο, που σημαίνει ότι δεν ελέγχεται από κανένα άτομο ή οντότητα. Με έναν παρόμοιο τρόπο με το Ethereum, οι συναλλαγές επαληθεύονται από την κοινότητα.

Ο κεντρικός στόχος του EOS είναι τα D-apps. Το Ethereum χειρίζεται 15 συναλλαγές το δευτερόλεπτο ενώ το EOS σχεδιάζει να αυξήσει τις δυνατότητες του και να χειρίζεται εκατομμύριες συναλλαγές το δευτερόλεπτο. Σύμφωνα με το EOS δεν θα υπάρχει καμία χρέωση συναλλαγής για πληρωμή κατά την αποστολή και τη λήψη χρημάτων.

Για να υπάρχει συναίνεση το Ethereum χρησιμοποιεί το Proof of Work. Ο μηχανισμός συναίνεσης που χρησιμοποιεί το EOS για να υποστηρίζει το δίκτυο ονομάζεται Delegated Proof of Stake (DPoS). Για να διευκρινιστεί, τον αλγόριθμο Proof of Stake που χρησιμοποιεί το Ethereum επιτρέπει σε οποιονδήποτε έχει ένα συγκεκριμένο ποσό νομισμάτων να βοηθήσει στην επαλήθευση συναλλαγών στο δίκτυο. Από την άλλη πλευρά, στο DPoS, η κατοχή νομισμάτων δεν επιτρέπει την επικύρωση συναλλαγών. Ωστόσο, επιτρέπει να ψηφιστεί "ποιος" πρέπει να επαληθεύσει τις συναλλαγές. Τα άτομα που μπορούν να ψηφιστούν ονομάζονται "Block Producers". Εάν δεν κάνουν την δουλειά τους σωστά, τότε θα αντικατασταθούν από άλλο Block Producer που περιμένουν τη σειρά τους. (Laura, 2020)

Άλλη μία πλατφόρμα που αξίζει να σημειωθεί είναι το Quorum. Ο στόχος του είναι η δημιουργία μιας εφαρμογής του Ethereum που να υποστηρίζει τις συναλλαγές και το απόρρητο των συμβολαίων.

Η λειτουργία του Quorum είναι παρόμοια με το Ethereum, αλλά με μερικές διαφορές. Το δίκτυο του Quorum δεν είναι ανοιχτό για όλους. Μόνο τα επικυρωμένα και εξουσιοδοτημένα άτομα μπορούν να είναι μέρος αυτού του δικτύου. Επίσης, οι δημόσιες συναλλαγές είναι παρόμοιες με του Ethereum, αλλά όταν πρόκειται για μια ιδιωτική συναλλαγή τότε είναι εμπιστευτική και δεν εκτίθεται στο κοινό.

Το Quorum βασίζεται σε έναν μηχανισμό συναίνεσης ψηφοφορίας, ο οποίος είναι γνωστός ως QuorumChain. Η λειτουργία του μηχανισμού είναι πολύ απλή, εκχωρεί δικαιώματα ψήφου σε άλλους. Για να εκχωρήσει δικαιώματα ψήφου, κάνει χρήση των έξυπνων συμβολαίων. Δεν εκχωρεί μόνο δικαιώματα ψήφου, αλλά ταυτόχρονα παρακολουθεί την κατάσταση όλων των κόμβων που ψηφίζουν.

Όταν πρόκειται για την ταχύτητα που πραγματοποιούνται οι συναλλαγές στο Quorum, σύμφωνα με την ομάδα ανάπτυξης, το σύστημα μπορεί εύκολα να χειριστεί 100 συναλλαγές το δευτερόλεπτο. Ο

λόγος που οι συναλλαγές γίνονται τόσο γρήγορα, είναι λόγω του μηχανισμού συναίνεσης που επιτρέπει ταχύτερες συναλλαγές.

Λαμβάνοντας υπόψη όλες τις δυνατότητες του Quorum, τότε είναι ένα εξαιρετικό εργαλείο για τις τραπεζικές εταιρείες. Αν και λειτουργεί με περιοριστικό μηχανισμό συναίνεσης, αυτό μειώνει τα ζητήματα εμπιστοσύνης που έχουν τα τραπεζικά και χρηματοπιστωτικά ιδρύματα. (Sharma, n.d.)

3.1.3 Συναίνεση στο Ethereum Blockchain

Για να επιτύχουμε συναίνεση σε ένα σύστημα θα πρέπει οι συμμετέχοντες να ακολουθήσουν κάποιους κανόνες ,έτσι ώστε το σύστημα να λειτουργεί με αποκεντρωμένο, αλλά με ντετερμινιστικό τρόπο. Όταν όλοι οι συμμετέχοντες σε ένα κατανεμημένο σύστημα συμφωνούν, τότε αυτό ονομάζεται «επίτευξη συναίνεσης».

Όσο αφορά τη βασική λειτουργία της αποκέντρωσης, μπορεί να γίνει προβληματική, το να βασίζεται το δίκτυο μόνο στην εμπιστοσύνη για να διασφαλίσει συναίνεση μεταξύ όλων των συμμετεχόντων. Αυτή η πρόκληση είναι ιδιαίτερα έντονη σε αποκεντρωμένα δίκτυα επειδή δεν υπάρχει έλεγχος από μια κεντρική οντότητα.

Στο Blockchain, η συναίνεση είναι μια ιδιότητα του συστήματος. Καθώς από το αποτέλεσμα αυτής, διακυβεύονται χρήματα. Συναίνεση είναι να είναι ικανό το Blockchain να φτάσει σε μια κοινή κατάσταση, διατηρώντας παράλληλα την αποκέντρωση του. Με άλλα λόγια, η συναίνεση προορίζεται να παράγει ένα σύστημα αυστηρών κανόνων, που τηρούνται από όλους τους συμμετέχοντες, χωρίς την ύπαρξη ενός κυβερνήτη.

Η επίτευξη της συναίνεσης σε ένα κατανεμημένο δίκτυο χωρίς κεντρικό έλεγχο, είναι η βασική αρχή όλων των δημόσιων Blockchain. Οι αλγόριθμοι συναίνεσης είναι ένας μηχανισμός, που χρησιμοποιείται για την τήρηση της ασφάλειας και της αποκέντρωσης. Οι δύο κυριότεροι αλγόριθμοι συναίνεσης είναι ο Proof of Work και ο Proof of Stake, όπου θα αναλυθούν παρακάτω. (Wood & Antonopoulos, 2019)

Στο Ethereum για να επικυρωθεί μια συναλλαγή, χρησιμοποιείται το PoW. Είναι ένας τρόπος που βοηθάει στην επικύρωση μιας συναλλαγής με αποκεντρωμένο τρόπο, χωρίς να υπάρχει μια κεντρική αρχή. Στο PoW, οι miners, χρησιμοποιούν την ισχύ από εξαρτήματα του υπολογιστή, όπως είναι ο επεξεργαστής και η κάρτα γραφικών, και επιλύουν πολύπλοκα μαθηματικά προβλήματα ώστε να επικυρώσουν τις συναλλαγές στο δίκτυο. Για την προσπάθεια τους ανταμείβονται με ETH. Στο PoS, οι miners ή επικυρωτές, για να επικυρώσουν συναλλαγές ποντάρουν τα κρυπτονομίσματα τους ως εγγύηση για το δικαίωμα επαλήθευσης των συναλλαγών.

Το PoW χρειάζεται αρκετή ενέργεια να για επικυρώσει τις συναλλαγές ενώ το PoS δεν απαιτεί τόση ενέργεια για επικύρωση των συναλλαγών. Οπότε, το PoS θα ήταν καλύτερο περιβάλλον για την επικύρωση των συναλλαγών, από την στιγμή που τα κρυπτο-δίκτυα θα μεγαλώνουν και θα απαιτούν περισσότερη ενέργεια. (Won, 2020)

Casper είναι το όνομα που έχει δοθεί για τον αλγόριθμο συναίνεσης του Ethereum PoS. Στην ουσία, είναι η μετατροπή του PoW σε PoS. Το Casper αναπτύσσεται σε δύο μέρη.

- Casper FFG: "The Friendly Finality Gadget"
- Casper CBC: "The Friendly GHOST/Correct-by-Construction"

(Wood & Antonopoulos, 2019)

Η έκδοση CBC προτάθηκε αρχικά από τον ερευνητή του ιδρύματος Ethereum, Vlad Zamfir. Παρόλο που η έρευνα για την CBC επικεντρώθηκε αρχικά σε πρωτόκολλα PoS για δημόσια Blockchain, έχει εξελιχθεί από τότε σε ένα ευρύτερο πεδίο σπουδών, που περιλαμβάνει μια οικογένεια μοντέλων PoS.

Η έρευνα για την FFG Casper διευθύνεται από τον συνιδρυτή της Ethereum Vitalik Buterin. Η αρχική πρόταση συνίστατο σε ένα υβριδικό σύστημα PoW / PoS, αλλά η εφαρμογή εξακολουθεί να αποτελεί αντικείμενο συζήτησης, και νέες προτάσεις ενδέχεται τελικά να την αντικαταστήσουν με ένα καθαρό μοντέλο PoS.

Η μετάβαση από το Ethereum 1.0 σε 2.0 αποκαλείται "αναβάθμιση Serenity". Θα αποτελείται από τρεις διαφορετικές φάσεις. Στην αρχική φάση (Φάση 0), θα ξεκινήσει ένα νέο Blockchain που ονομάζεται Beacon Chain. Οι κανόνες FFG του Casper θα οδηγήσουν τον μηχανισμό συναίνεσης αυτού του νέου Blockchain με βάση το PoS. Σε αντίθεση με το mining PoW, όπου οι miners τρέχουν δαπανηρές και εξειδικευμένες μηχανές για να δημιουργήσουν και να επικυρώσουν τμήματα συναλλαγών, το Casper θα καταργήσει τη διαδικασία mining από το Ethereum.

Εναλλακτικά, η επαλήθευση και η επικύρωση νέων τμημάτων συναλλαγών θα γίνει με επικυρωτές block, οι οποίες θα επιλεγούν ανάλογα με το μερίδιό τους. Η ισχύς ψηφοφορίας κάθε επικύρωσης θα καθορίζεται από το ποσό του ETH που διακυβεύεται. Για παράδειγμα, κάποιος που έχει καταθέσει 64 ETH θα έχει το διπλάσιο το βάρος ψήφου από κάποιον που κατέθεσε το ελάχιστο ποσό πονταρίσματος. (Peaster, n.d.)

Ακόμα επιλύει τα εξής προβλήματα:

- Λογοκρισία: Εάν ένας Bitcoin miner χάσει ένα block του, τότε κάθε άλλος miner που είναι ανταγωνιστής του επωφελείται αναλόγως. Το PoS του Ethereum θα αλλάξει το δίκτυο σε ένα «συντονισμένο παιχνίδι», όπου όλοι θα επωφεληθούν εάν όλα τα block των miners συμπεριληφθούν στο Blockchain.
- Έξοδα: Μέσω του τρέχοντος πρωτοκόλλου PoW του Ethereum, η ασφάλεια μπορεί να διατηρηθεί μόνο μέσω υψηλών λειτουργικών εξόδων. Το Casper θα διευκολύνει τους ειλικρινείς επικυρωτές με φθηνές επικυρώσεις ενώ τα έξοδα των επιτιθέμενων θα είναι εξαιρετικά ακριβά. (Dale, 2017)

3.1.4 Έξυπνα συμβόλαια

Ο όρος έξυπνο συμβόλαιο χρησιμοποιείται με την πάροδο του χρόνου για να περιγράψει μια μεγάλη ποικιλία διαφορετικών πραγμάτων. Ο Nick Szabo επινόησε τον όρο και τον καθόρισε ως ένα σύνολο υποσχέσεων, που καθορίζονται σε ψηφιακή μορφή. Από τότε η έννοια των έξυπνων συμβολαίων έχει εξελιχθεί, ειδικά μετά την εισαγωγή αποκεντρωμένων πλατφορμών του Blockchain.

Έξυπνα συμβόλαια ονομάζουμε τα αμετάβλητα προγράμματα υπολογιστών που εκτελούνται από την εικονική μηχανή του Ethereum (EVM) ως μέρος του πρωτοκόλλου δικτύου του Ethereum. (Wood & Antonopoulos, 2019)

3.1.5 Λογαριασμοί Χρηστών

Μία από τις θεμελιώδεις τεχνολογίες του Ethereum είναι η κρυπτογραφία, που χρησιμοποιείται για την ασφάλεια των συναλλαγών. Η κρυπτογραφία μπορεί να χρησιμοποιηθεί για να αποδειχθεί η γνώση ενός μυστικού χωρίς να αποκαλυφθεί το μυστικό ή για να αποδειχθεί η αυθεντικότητα των δεδομένων. Η κρυπτογραφία είναι κρίσιμο εργαλείο για την λειτουργία της πλατφόρμας του Ethereum και χρησιμοποιείται εκτενώς σε εφαρμογές του Ethereum.

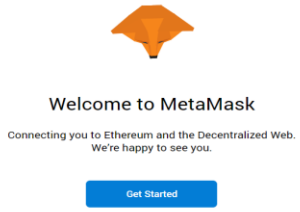
Τη στιγμή της δημοσίευσης, κανένα μέρος του πρωτοκόλλου του Ethereum δεν είναι κρυπτογραφημένο, δηλαδή όλες οι επικοινωνίες με την πλατφόρμα του Ethereum και μεταξύ των κόμβων δεν είναι κρυπτογραφημένα και μπορούν να διαβαστούν από τον καθένα. Αυτό γίνεται έτσι ώστε να μπορούν όλοι να επαληθεύσουν την ορθότητα των ενημερώσεων κατάστασης και να επιτευχθεί η συναίνεση. (Wood & Antonopoulos, 2019)

Οι λογαριασμοί που χρησιμοποιεί το Ethereum χωρίζονται σε δύο κατηγορίες, σε λογαριασμούς συμβολαίων (contract accounts) και σε λογαριασμούς χρηστών (user accounts). Η κύρια διαφορά τους είναι ότι όλη η δράση στο Blockchain του Ethereum υπάρχει στις συναλλαγές που πραγματοποιούνται από τους user account ενώ όταν ένα έξυπνο συμβόλαιο παραλάβει μία συναλλαγή, ο κώδικας του εκτελείται σύμφωνα με τις παραμέτρους εισαγωγής, που αποστέλλονται ως μέρος της συναλλαγής. Οι συναλλαγές μπορούν να ενεργοποιηθούν και από τους δύο τύπους λογαριασμών, αν και τα συμβόλαια ενεργοποιούν μόνο τις συναλλαγές ως απόκριση σε άλλες συναλλαγές που έχουν λάβει. Επομένως, όλες οι ενέργειες σε ένα Ethereum Blockchain ξεκινούν από συναλλαγές που προέρχονται από εξωτερικά ελεγχόμενους λογαριασμούς ή αλλιώς user accounts.

Ένας user account περιέχει ένα υπόλοιπο από Ether, μπορεί να λάβει ή να στείλει συναλλαγές και ελέγχεται από ένα ιδιωτικό κλειδί, που το γνωρίζει μόνο ο χρήστης, μοναδικό για κάθε λογαριασμό. Το ιδιωτικό κλειδί έχει τον ρόλο της υπογραφής, που με αυτό τον τρόπο μπορεί να εγκριθεί μια συναλλαγή. Η συναλλαγή "υπογράφτηκε" και η υπογραφή δημιουργήθηκε με την βοήθεια του ιδιωτικού κλειδιού.

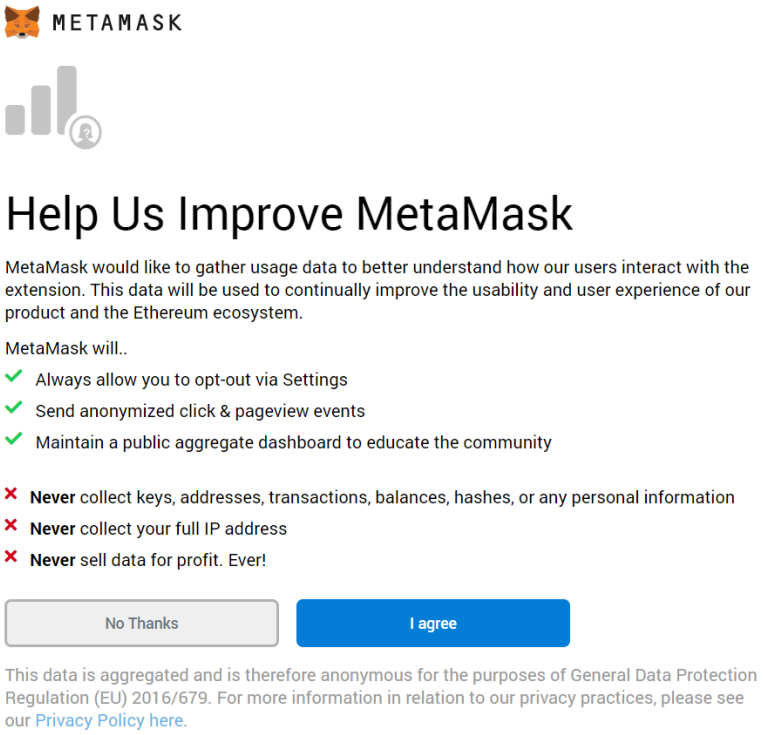
Το contract account περιέχει ένα υπόλοιπο από Ether για να μπορούν να αποθηκεύσουν, να στείλουν και να λάβουν Ether, όπως ένας user account. Αυτό και μόνο δηλώνει ότι χρειάζεται να είναι λογαριασμός και όχι συναλλαγή. Ένας contract account περιέχει τον δικό του κώδικα και ελέγχεται από κώδικα.

Για την δημιουργία ενός user account θα χρειαστεί ένα πορτοφόλι όπως είναι το Metamask. Όταν γίνει η εγκατάσταση της επέκτασης του Metamask στο toolbar του φυλλομετρητή θα υπάρχει ένα εικονίδιο του Metamask. Πατώντας το εμφανίζει την παρακάτω εικόνα.



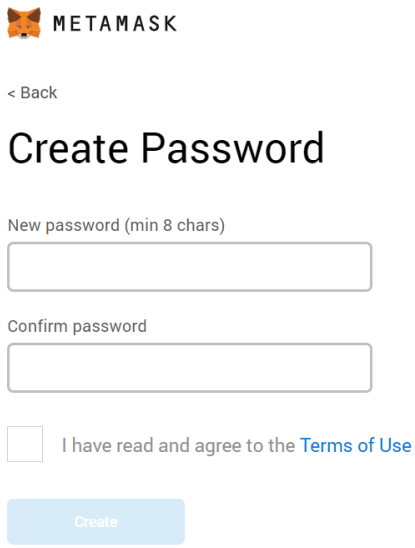
Εικόνα 5: Δημιουργία ενός User account

Πατώντας το get started, το Metamask παρέχει την επιλογή για την εισαγωγή ενός λογαριασμού εάν υπάρχει ήδη και την επιλογή δημιουργίας καινούργιου λογαριασμού. Επιλέγοντας την δημιουργία καινούργιου λογαριασμού, γίνεται μια συμφωνία μεταξύ του χρήστη και του Metamask, στην οποία το Metamask αναφέρει τις δυνατότητες που θα παρέχει στο χρήστη.



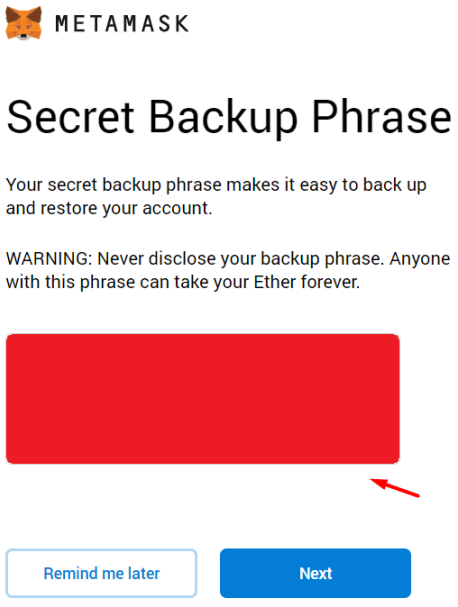
Εικόνα 6: Δημιουργία ενός User account

Στη συνέχεια το Metamask μεταφέρεται στην επόμενη σελίδα, όπου εκεί ο χρήστης επιλέγει τον κωδικό που θα έχει στο λογαριασμό του.



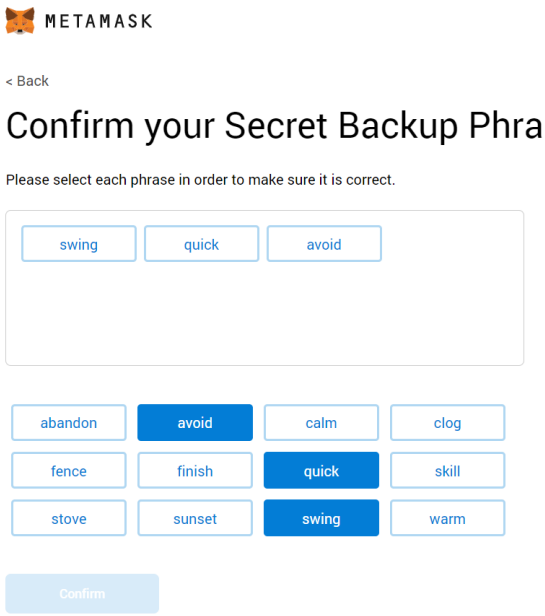
Εικόνα 7: Δημιουργία ενός User account

Στη συνέχεια εμφανίζει το Metamask τις λέξεις ασφαλείας, οι οποίες χρησιμοποιούνται για την επαναφορά του λογαριασμού στο Metamask. Είναι πολύ σημαντικό και πρέπει να σημειωθεί ότι πρέπει να γίνει η αποθήκευση τους σε κατάλληλο μέρος, όπως είναι το Dropbox ή σε ένα εξωτερικό σκληρό δίσκο, ώστε να μην χαθούν. Σε περίπτωση απώλειας του κωδικού του λογαριασμού, δεν είναι δυνατή η επαναφορά του λογαριασμού χωρίς αυτές. Αυτό σημαίνει ότι χάθηκαν τα περιεχόμενα του λογαριασμού, για παράδειγμα τα Ether , και δεν επαναφέρονται. Οι λέξεις βρίσκονται στο κόκκινο κουτί.



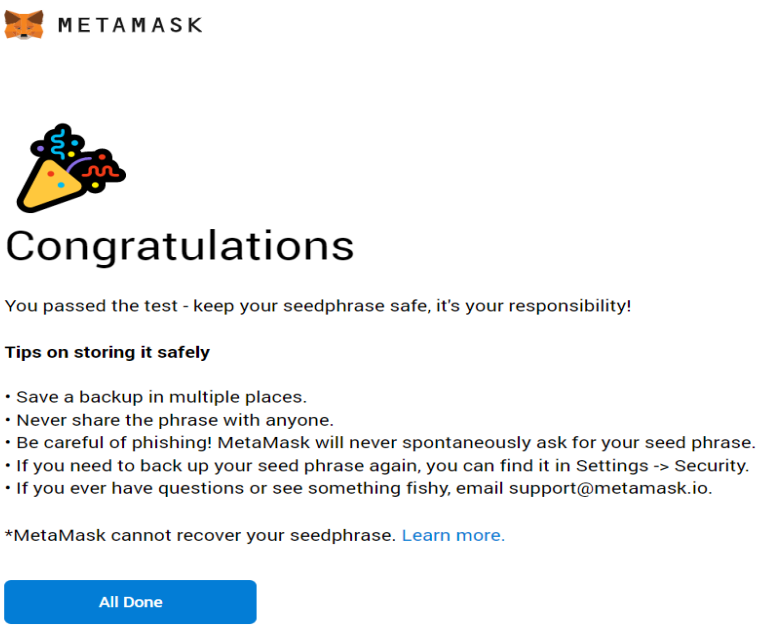
Εικόνα 8: Δημιουργία ενός User account

Γίνεται επανάληψη των παραπάνω λέξεων, ώστε να επιβεβαιωθεί το Metamask ότι ο χρήστης έλαβε τις λέξεις.



Εικόνα 9: Δημιουργία ενός User account

Τέλος, ο λογαριασμός δημιουργήθηκε και από αυτή τη στιγμή ο χρήστης έχει ένα User account.



Εικόνα 10: Δημιουργία ενός User account

3.1.6 Πορτοφόλια

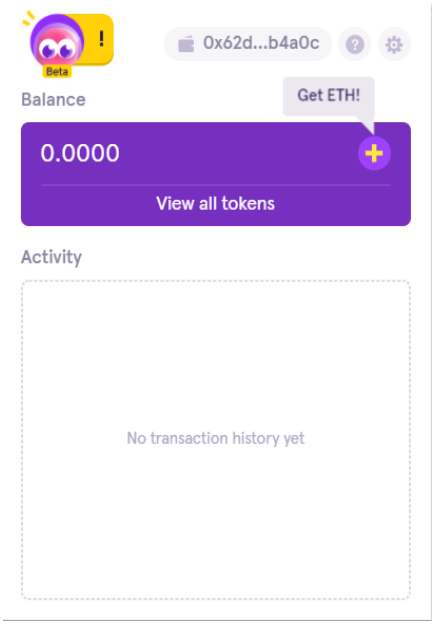
Η λέξη "πορτοφόλι" χρησιμοποιείται για να περιγράψει αρκετά διαφορετικά πράγματα στο Ethereum. Ένα πορτοφόλι είναι μια εφαρμογή που χρησιμεύει ως η κύρια επαφή του χρήστη με το Ethereum. Το πορτοφόλι ελέγχει την πρόσβαση στα χρήματα ενός χρήστη, στα κλειδιά διαχείρισης και διευθύνσεων, παρακολούθηση του υπολοίπου και δημιουργία συναλλαγών. Επίσης, ορισμένα πορτοφόλια μπορούν να αλληλεπιδράσουν με συμβόλαια.

Από την οπτική γωνία ενός προγραμματιστή, η λέξη "πορτοφόλι" αναφέρεται στο σύστημα που χρησιμοποιείται για την αποθήκευση και διαχείριση των κλειδιών ενός χρήστη. Άλλα πορτοφόλια είναι διεπαφές μεταξύ των εφαρμογών του Ethereum και των προγραμμάτων περιήγησης. (Wood & Antonopoulos, 2019)

Το Metamask είναι μια επέκταση πορτοφολιού του φυλλομετρητή, όπως είναι το Chrome και το Firefox, και είναι το πιο γνωστό πορτοφόλι για το Ethereum. Είναι εύκολο στην χρήση, μπορεί να συνδεθεί σε κόμβους του Ethereum και να δοκιμάσει Blockchains. Επίσης, επιτρέπει τη σύνδεση σε D-apps, όπου οι χρήστες μπορούν να ξοδέψουν τα νομίσματα τους σε παιχνίδια, εφαρμογές τζόγου ή να τα ανταλλάξουν.

Ακόμα, το Metamask επιτρέπει την αποστολή, λήψη και αποθήκευση των Ether, απλά τρέχοντας μια απλή επέκταση του φυλλομετρητή. Το πλεονέκτημα που παρέχει το Metamask είναι ότι ένας χρήστης για να τρέξει ένα D-app θα έπρεπε να τρέξει όλα τα λογισμικά του Ethereum που χρειάζονται ενώ με το Metamask τα τρέχει στους Servers του.

Επίσης, ένα ακόμα γνωστό πορτοφλόλι είναι το Dapper. Το Dapper είναι ένα πορτοφόλι έξυπνου συμβολαίου λόγω της αποκέντρωσης του, που σχεδιάστηκε για ανθρώπους, έτσι ώστε να παρέχει χρησιμότητα και ασφάλεια χωρίς συμβιβασμούς. Το Dapper προσφέρει ένα συνδυασμό χρησιμότητας και ασφάλειας, όπου αυτός ο συνδυασμός είναι ένα μεγάλο πλεονέκτημα στην αποκέντρωση. Το μυστικό του Dapper είναι ότι η δύναμη του πηγάζει από τα έξυπνα συμβόλαια. Το Dapper παρέχει ασφάλεια, όπως ανάκτηση λογαριασμού και προστασία από απάτες. Ακόμα, μπορεί να παρακολουθεί παράξενες ενέργειες, όπως αποστολή μεγάλων ποσών σε παράξενες διευθύνσεις και ασυνήθιστες δραστηριότητες.



Εικόνα 11: Dapper

3.1.7 Αποκεντρωμένες Εφαρμογές (D-Apps)

Ένα D-app είναι μια εφαρμογή όπου είναι αποκεντρωμένη. Παρακάτω φαίνονται όλες οι πιθανές πτυχές μια εφαρμογής που μπορούν να αποκεντρωθούν:

- Backend λογισμικό
- Frontend λογισμικό
- Αποθήκευση δεδομένων
- Επικοινωνία μηνυμάτων
- Ανάλυση ονομάτων (Name resolution)

Καθένα από αυτά μπορεί να είναι κάπως συγκεντρωτικό ή κάπως αποκεντρωμένο. Για παράδειγμα, το frontend μπορεί να αναπτυχθεί ως μια ιστοσελίδα που λειτουργεί σε κεντρικό διακομιστή ή ως εφαρμογή για κινητά που εκτελείται σε μια συσκευή. Το backend και ο αποθηκευτικός χώρος μπορεί να είναι σε ιδιωτικούς διακομιστές ή μπορεί να χρησιμοποιηθεί ένα έξυπνο συμβόλαιο και αποθήκευση P2P. Το backend παρέχει έναν αποτελεσματικό και αξιόπιστο τρόπο επικοινωνίας με το δίκτυο του Ethereum.

Στην ουσία, το backend ενός D-app είναι ένα έξυπνο συμβόλαιο, το οποίο καλείται από τον κώδικα του frontend.

Τα πλεονεκτήματα που παρέχει ένα D-app είναι αρκετά σε σύγκριση με μια τυπική κεντρική αρχιτεκτονική. Αρχικά, το D-app παρέχει:

- Ανθεκτικότητα (Resiliency) : Επειδή η επιχειρηματική λογική ελέγχεται από ένα έξυπνο συμβόλαιο, το Backend ενός D-app διανέμεται και διαχειρίζεται από την πλατφόρμα του Blockchain. Αντιθέτως, μια εφαρμογή που έχει ανέβει σε έναν κεντρικό διακομιστή, το D-app δεν θα έχει χρόνο διακοπής (downtime) και θα συνεχίζει να είναι διαθέσιμο όσο η πλατφόρμα εξακολουθεί να λειτουργεί.
- Διαφάνεια (Transparency): Η φύση ενός D-app επιτρέπει σε όλους να ελέγχουν τον κώδικα και να είναι περισσότερο σίγουροι για την λειτουργία του. Οποιαδήποτε αλληλεπίδραση με το D-app θα αποθηκεύεται για πάντα στο Blockchain.
- Αντίσταση λογοκρισίας (Censorship Resistance): Από την στιγμή που ένας χρήστης έχει πρόσβαση σε ένα κόμβο του Ethereum, θα μπορεί να αλληλεπιδρά με το D-app χωρίς καμία παρέμβαση από οποιονδήποτε κεντρικό έλεγχο. Κανένας πάροχος υπηρεσιών ή ακόμη και ο κάτοχος του έξυπνου συμβολαίου, μπορεί να αλλάξει τον κώδικα μόλις αυτός ανέβει στο δίκτυο. (Wood & Antonopoulos, 2019)

Τα D-apps ,όπως προαναφέρθηκε παραπάνω, είναι αποκεντρωμένες εφαρμογές που δεν ελέγχονται από κανέναν. Αυτές οι εφαρμογές χωρίζονται σε διάφορες κατηγορίες, οι κυριότερες είναι φαίνονται παρακάτω.

- Τύπου 1 : D-apps που έχουν το δικό τους Blockchain.
- Τύπου 2 : D-apps που χρησιμοποιούν τα D-apps του τύπου 2, επειδή αυτά τα D-apps είναι πρωτόκολλα και χρειάζονται tokens για να λειτουργήσουν.
- Τύπου 3 : D-apps που χρησιμοποιούν τα πρωτόκολλα του τύπου 2, αλλά επίσης είναι πρωτόκολλα που χρειάζονται tokens. (HBUS, 2018)

Ένα από τα πιο γνωστά D-apps είναι το Splinterlands. Το splinterlands είναι ένα ψηφιακό παιχνίδι, στο οποίο συλλέγεις κάρτες. Κάθε κάρτα είναι ένα μοναδικό token, το οποίο ανήκει στον χρήστη. Ένας χρήστης μπορεί να αγοράσει, πουλήσει και να ανταλλάξει κάρτες.

Επίσης, το Cryptokitties είναι ένα ψηφιακό παιχνίδι, το οποίο παρέχει την δυνατότητα αγοράς, συλλογής και αναπαραγωγής νέων τύπου εικονικών γατιών. Κάθε γάτα έχει τα δικά της μοναδικά χαρακτηριστικά. Οπότε συνδυάζοντας την με μία άλλη γάτα, δημιουργείται μια γάτα με μοναδικά χαρακτηριστικά, με μοναδική εμφάνιση, η οποία είναι σπάνια. Κάθε παίχτης μπορεί να ανταλλάξει, να αγοράσει και να πουλήσει τις γάτες του, οι οποίες είναι ψηφιακά κεφάλαια στην ουσία.

Ακόμα, το Axie Infinity είναι ένα γνωστό παιχνίδι, το οποίο είναι η πρώτη Blockchain εφαρμογή κινητού. Στο κόσμο του Axie Infinity οι παίκτες έχουν στην κατοχή τους κατοικίδια, τα οποία μπορούν να τα δυναμώσουν και να πολεμήσουν μεταξύ τους, όπως και να τα ανταλλάξουν.

Οι παραπάνω εφαρμογές, όπως και πολλές άλλες μπορούν να βρεθούν σε μια ιστοσελίδα που ονομάζεται State of the D-apps. Η ιστοσελίδα περιέχει αρκετές εφαρμογές που μπορεί ο καθένας να τις χρησιμοποιήσει. Ακόμα, περιέχει εφαρμογές για κάθε πλατφόρμα, όπως είναι το Ethereum, EOS και Gochain. Τα D-apps που υπάρχουν χωρίζονται σε κατηγορίες όπως είναι τα ψηφιακά παιχνίδια, εφαρμογές που σχετίζονται με την αποθήκευση, ασφάλεια, κοινωνικότητα, υγεία κ.ά.

3.2 Proof of Stake

Ο δημιουργός του Bitcoin δημιούργησε τον αλγόριθμο συναίνεσης Proof of Work (PoW). Ο συνηθισμένος όρος που χρησιμοποιείται για το PoW είναι το “mining”, όπου δημιουργεί μια παρανόηση για τον πρωταρχικό σκοπό της συναίνεσης. Συχνά οι άνθρωποι υποθέτουν ότι ο σκοπός του mining είναι η δημιουργία ενός καινούργιου νομίσματος, καθώς ο σκοπός του mining στον πραγματικό κόσμο είναι η εξόρυξη πολύτιμων μετάλλων ή άλλως πόρων. Ο πραγματικός σκοπός του mining και άλλως μοντέλων συναίνεσης στο Blockchain είναι η διατήρηση της ασφάλειας του Blockchain. Στο PoW η ανταμοιβή του νομίσματος που έγινε mined αποτελεί κίνητρο για όσους συνεισφέρουν στην ασφάλεια του συστήματος. Στο PoW υπάρχει και η “τιμωρία”, που είναι το κόστος της ενέργειας που απαιτείται για το mining. Εάν οι συμμετέχοντες δεν ακολουθούν τους κανόνες, ρισκάρουν τα χρήματα που έχουν δαπανηθεί για ηλεκτρική ενέργεια κατά τη διάρκεια του mining. Οπότε, το Proof of Work ελέγχει την ισορροπία μεταξύ ρίσκου και ανταμοιβής που ωθεί τους συμμετέχοντες να συμπεριφέρονται ειλικρινά από συμφέρον.

Το Ethereum είναι επί του παρόντος ένα PoW Blockchain, καθώς ο κύριος στόχος του είναι η εξασφάλιση του αποκεντρωμένου ελέγχου στο Blockchain. Ο αλγόριθμος PoW του Ethereum είναι ελαφρώς διαφορετικός από τον Bitcoin και ονομάζεται Ethash.

Το PoW δεν ήταν ο πρώτος αλγόριθμος συναίνεσης που προτάθηκε. Αρκετοί ερευνητές είχαν προτείνει μια παραλλαγή της συναίνεσης που βασίζεται στα χρηματοοικονομικά. Πλέον αυτός ο αλγόριθμος συναίνεσης λέγεται Proof of Stake (PoS). Το PoW επινοήθηκε ως εναλλακτική λύση για το PoS. Λόγω της επιτυχίας του Bitcoin, πολλά Blockchains χρησιμοποιούν το PoW. Από την αρχή, οι ιδρυτές του Ethereum ήλπιζαν μεταβούν από τον αλγόριθμο συναίνεσης PoW σε PoS. Το Ethereum εξακολουθεί να χρησιμοποιεί το PoW, αλλά η συνεχόμενη έρευνα έχει βοηθήσει στην δημιουργία ενός νέου αλγόριθμου συναίνεσης για το Ethereum με βάση τα χρηματοοικονομικά που ονομάζεται Casper. Όμως, η αντικατάσταση του Pow σε PoS έχει αναβληθεί αρκετές φορές τα τελευταία χρόνια.

Γενικά ένας αλγόριθμος PoS λειτουργεί ως εξής. Το Blockchain παρακολουθεί ένα σύνολο επικυρωτών και οποιοσδήποτε έχει στη κατοχή του κρυπτονομίσματα μπορεί να γίνει επικυρωτής στέλνοντας έναν ειδικό τύπο συναλλαγής που κλειδώνει τα Ether τους σε μια κατάθεση. Οι επικυρωτές διαδοχικά ψηφίζουν στο επόμενο έγκυρο Block και το βάρος της ψήφου που έχει κάθε επικυρωτής εξαρτάται από το μέγεθος της κατάθεσης. Ένας επικυρωτής ρισκάρει να χάσει την κατάθεση του εάν το Block που ψηφίζει απορρίπτεται από την πλειοψηφία των επικυρωτών. Οι επικυρωτές κερδίζουν μια μικρή ανταμοιβή, ανάλογη με το ποντάρισμα τους, για κάθε Block που γίνεται αποδεκτό από την πλειοψηφία. Έτσι, το PoS αναγκάζει τους επικυρωτές να ενεργούν με ειλικρίνεια και να ακολουθούν τους κανόνες τις συναίνεσης, με ένα σύστημα ανταμοιβής και τιμωρίας. (Wood & Antonopoulos, 2019)

3.3 Δημιουργία Έξυπνων Συμβολαίων στο Ethereum

Τα έξυπνα συμβόλαια γράφονται σε υψηλές γλώσσες προγραμματισμού, μία από αυτές τις γλώσσες είναι η Solidity. Είναι μια αντικειμενοστραφής γλώσσα προγραμματισμού για τη σύνταξη έξυπνων συμβολαίων και χρησιμοποιείται για την εφαρμογή έξυπνων συμβάσεων σε διάφορες πλατφόρμες, κυρίως του Ethereum.

Ο μεταγλωττιστής που χρησιμοποιεί η Solidity, Solc, μετατρέπει τα προγράμματα που γράφτηκαν με Solidity σε EVM bytecode. Ακόμα διαχειρίζεται το Application Binary Interface (ABI) για τα έξυπνα συμβόλαια του Ethereum. Κάθε έκδοση του μεταγλωττιστή της Solidity αντιστοιχείται σε μια συγκεκριμένη έκδοση της γλώσσα προγραμματισμού Solidity.

Όταν ένα έξυπνο συμβόλαιο δημιουργείται με την χρήση της Solidity, για να "τρέξει" πρέπει να μεταγλωττιστεί σε χαμηλό επίπεδο Bytecode για να εκτελεστεί στο Ethereum Virtual Machine (EVM). Όταν μεταγλωττιστεί το έξυπνο συμβόλαιο, "ανεβαίνει" στην πλατφόρμα του Ethereum χρησιμοποιώντας μια ειδική συναλλαγή. Κάθε συναλλαγή αντιστοιχείται σε μια διεύθυνση του

Ethereum, η οποία προέρχεται από την συναλλαγή της δημιουργίας του συμβολαίου. Η Ethereum διεύθυνση ενός συμβολαίου μπορεί να χρησιμοποιηθεί σε μια συναλλαγή ως παραλήπτης και να καλέσουν συναρτήσεις που υπάρχουν στο έξυπνο συμβόλαιο.

Τα έξυπνα συμβόλαια εκτελούνται μόνο εάν κληθούν μέσω συναλλαγής. Ένα συμβόλαιο μπορεί να καλέσει άλλο συμβόλαιο που μπορεί να καλέσει άλλο συμβόλαιο, και ούτω καθεξής, αλλά το πρώτο συμβόλαιο σε μια τέτοια αλυσίδα εκτέλεσης θα έχει κληθεί πάντα από μια συναλλαγή από έναν EOA. Τα συμβόλαια δεν εκτελούνται ποτέ «μόνα τους» ή «στο παρασκήνιο».

Οι συναλλαγές είναι ατομικές, ανεξάρτητα από το πόσα συμβόλαια καλούν ή τι πραγματοποιούν όταν αυτά καλούνται. Οι συναλλαγές εκτελούνται στο σύνολό τους, με τυχόν αλλαγές στο δίκτυο να καταγράφονται μόνο εάν ολοκληρωθεί η εκτέλεση επιτυχώς. Ο επιτυχής τερματισμός σημαίνει ότι το πρόγραμμα εκτελέστηκε χωρίς σφάλμα και έφτασε στο τέλος της εκτέλεσης. Εάν η εκτέλεση αποτύχει λόγω σφάλματος, όλες αυτές οι αλλαγές επαναφέρονται σαν να μην εκτελέστηκε ποτέ η συναλλαγή. Μια αποτυχημένη συναλλαγή καταγράφεται ως προσπάθεια και τα Ether που δαπανήθηκαν για gas για την εκτέλεση αφαιρούνται από τον αρχικό λογαριασμό, αλλά διαφορετικά δεν έχει άλλες επιπτώσεις στο συμβόλαιο ή στην κατάσταση του λογαριασμού.

Ο κώδικας ενός συμβολαίου δεν μπορεί να αλλάξει. Ωστόσο, ένα συμβόλαιο μπορεί να διαγραφεί, αφαιρώντας τον κωδικό του και την εσωτερική του κατάσταση (αποθηκευτικός χώρος) από την διεύθυνση της αφήνοντας έναν κενό λογαριασμό. Τυχόν συναλλαγές που αποστέλλονται σε αυτή την διεύθυνση λογαριασμού, μετά τη διαγραφή του συμβολαίου δεν οδηγεί σε εκτέλεση κώδικα, γιατί δεν υπάρχει πλέον κώδικας να εκτελεστεί. (Wood & Antonopoulos, 2019)

Παρακάτω φαίνεται ένα συμβόλαιο γραμμένο σε Solidity όπου ονομάζεται SimpleStorage. Δηλώνει μια μεταβλητή με όνομα storedData, της οποίας ο τύπος είναι ακέραιος. Επίσης, αποτελείται από δύο συναρτήσεις, την set και την get. Όταν καλείται η set περιμένει μια ακέραια τιμή ως είσοδο στην μεταβλητή storedData και η συνάρτηση get επιστρέφει την τιμή που περιέχει η μεταβλητή storedData. Να σημειωθεί η έκδοση της Solidity που χρησιμοποιήθηκε είναι η 0.4.0 .

```
pragma solidity ^0.4.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public returns (uint) {
        return storedData;
    }
}
```

Εικόνα 12: Έξυπνο συμβόλαιο σε Solidity

Για την εγκατάσταση ενός έξυπνου συμβολαίου σε ένα Ethereum δίκτυο, θα χρειαστούμε ένα εργαλείο που ονομάζεται Truffle. Το Truffle είναι ένα αναπτυξιακό περιβάλλον για έξυπνα συμβόλαια. Συνιστάται κυρίως για προγραμματιστές που θέλουν να δημιουργήσουν projects χρησιμοποιώντας javascript, τα οποία είναι βασισμένα πάνω στα έξυπνα συμβόλαια όπως τα D-apps. Το Truffle μας παρέχει προσομοίωση ενός πραγματικού Blockchain περιβάλλοντος. Οπότε, δημιουργώντας ένα έξυπνο συμβόλαιο με το Truffle, δημιουργούνται οι παρακάτω φάκελοι. Σε κάθε φάκελο δίπλα έχει σημειωθεί και η χρήση του.

- **contracts/**: Directory for Solidity contracts
- **migrations/**: Directory for scriptable deployment
- **test/**: Directory for test files for testing your application and contracts
- **truffle-config.js**: Truffle configuration file

Εικόνα 13: Φάκελοι που δημιουργήθηκαν μέσω του Truffle

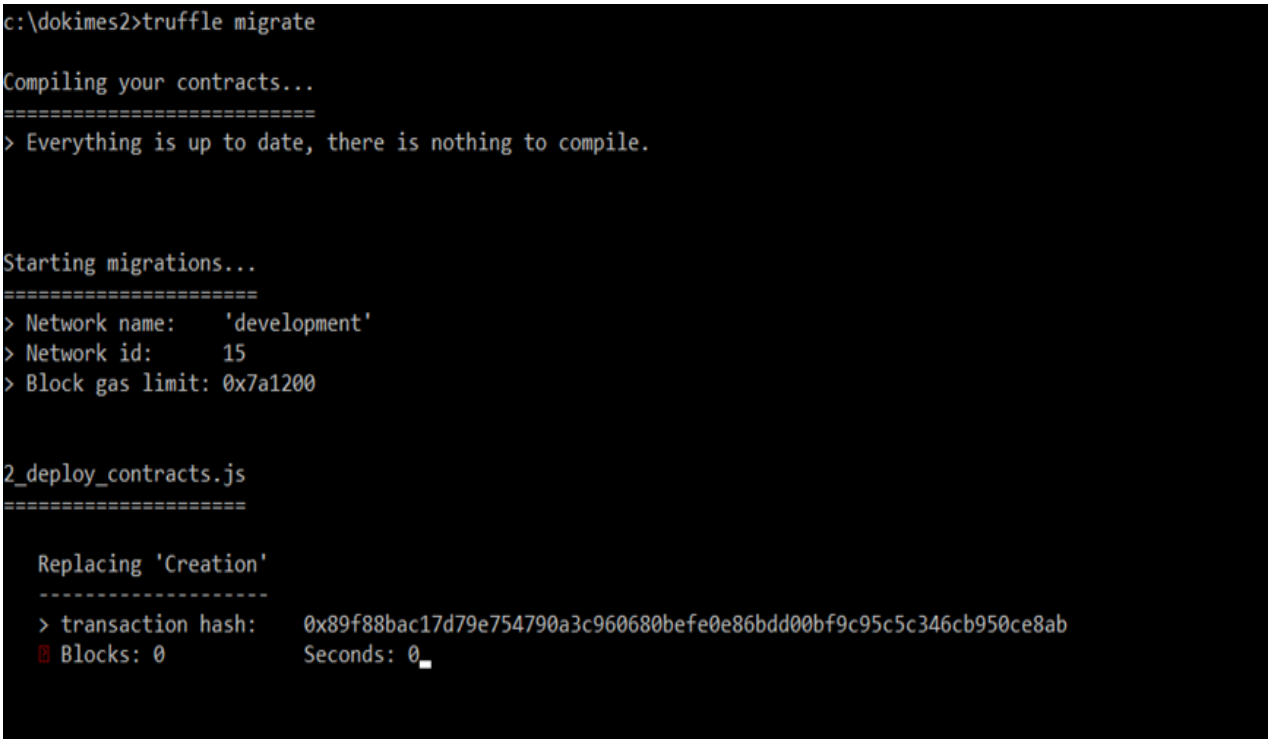
Όταν το έξυπνο συμβόλαιο δημιουργηθεί, στο φάκελο contracts, μπορεί να εγκατασταθεί στο δίκτυο. Στο φάκελο migration, ο χρήστης δημιουργεί ένας αρχείο, όπου περιέχει κώδικα, ο οποίος βοηθάει το έξυπνο συμβόλαιο στην εγκατάσταση του στο δίκτυο. Στο φάκελο test περιέχονται αρχεία, τα οποία τεστάρουν τα έξυπνα συμβόλαια. Στο αρχείο truffle-config.js συμπληρώνονται τα πεδία, τα οποία δείχνουν σε πιο δίκτυο θα εγκατασταθεί στο έξυπνο συμβόλαιο.

```
module.exports = {
  networks: {
    development: {
      host: "127.0.0.1",
      port: 8545,
      network_id: "*"
    }
  },

  mocha: {
  },

  compilers: {
    solc: {
      version: "0.5.3",
      docker: false
    }
  }
}
```

Εικόνα 14: Φαίνεται ο κώδικας που περιέχεται στο αρχείο truffle-config.js. Σε αυτή την περίπτωση το έξυπνο συμβόλαιο εγκαθίσταται σε τοπικό δίκτυο.

Στην τελική, έχοντας το έξυπνο συμβόλαιο εγκατασταθεί στο δίκτυο, θα εμφανίσει την

παρακάτω εικόνα. Το Truffle παρέχει πληροφορίες σχετικά με την εγκατάσταση του έξυπνου συμβολαίου όπως σε πιο δίκτυο εγκαταστάθηκε, εάν η εγκατάσταση ήταν επιτυχής και πληροφορίες της συναλλαγής.



Εικόνα 15: Πληροφορίες σχετικά με την εγκατάσταση του έξυπνου συμβολαίου σε ένα δίκτυο

Παρακάτω υπάρχουν σημαντικές συναρτήσεις, οι οποίες χρησιμοποιούνται στο Truffle.

- truffle init: Δημιουργία φακέλων που περιέχουν αρχεία απαραίτητα για την δημιουργία του D-app.
- truffle compile: Έλεγχος του κώδικα του έξυπνου συμβολαίου, μη τυχόν υπάρχει κάποιο λάθος.
- truffle migrate -network development: Εγκατάσταση του έξυπνου συμβολαίου στο δίκτυο, όπου το development είναι το όνομα του δικτύου που το έχουμε σημειώσει στο αρχείο truffle-config.js (Benemerito, 2019)

4 Υλοποίηση: Δημιουργία ενός ιδιωτικού δικτύου Ethereum

Ένα ιδιωτικό δίκτυο του Ethereum είναι ένα ιδιωτικό Blockchain, εντελώς απομονωμένο από το κύριο δίκτυο του Ethereum. Μόνο οι κόμβοι με τα κατάλληλα δικαιώματα θα έχουν πρόσβαση στο ιδιωτικό δίκτυο. Ένα ιδιωτικό Ethereum δίκτυο χρησιμοποιείται κυρίως από οργανώσεις που θέλουν να αποθηκεύσουν ιδιωτικά δεδομένα, τα οποία δεν πρέπει να είναι ορατά για τους ανθρώπους που δεν είναι μέρος της οργάνωσης. Επίσης, ένα ιδιωτικό Ethereum δίκτυο χρησιμοποιείται πειραματικούς σκοπούς πάνω στο Blockchain, στην περίπτωση που η χρήση του κύριου δικτύου του Blockchain δεν είναι επιθυμητή.

Σε αυτή την ενότητα περιέχονται τα βήματα που χρειάζονται να γίνουν για τη δημιουργία ενός Ethereum ιδιωτικού Blockchain δικτύου. Το δίκτυο αποτελείται από τρείς κόμβους, όπου μπορούν να αυξηθούν στη πορεία. Η ανάπτυξη των κόμβων γίνεται σε VMs στον Okeanos Cloud που παρέχεται από την GRNET. Οι κόμβοι αυτού του δικτύου δεν είναι συνδεδεμένοι στο ΄κύριο δίκτυο του Ethereum.

4.1 Υπολογιστικές Απαιτήσεις

Στο δίκτυο θα υπάρχουν τρείς κόμβοι, δηλαδή τρία VMs τα οποία θα τρέχουν σε Ubuntu 16.04 LTS server image και το καθένα θα έχει τους παρακάτω πόρους:

- 2 CPUs
- 4GB RAM
- 30GB Boot disk,150GB πρόσθετη αποθήκευση
- 1 public ip

4.2 Βήματα υλοποίησης

Στη συνέχεια, περιγράφεται η διαδικασία που χρειάζεται για την δημιουργία ενός ιδιωτικού δικτύου και ο τρόπος που θα χρησιμοποιηθεί για το ανέβασμα ενός D-app σε αυτό το δίκτυο. Θα γίνει αναφορά σε εντολές και εικόνες, όπου θα κάνουν την διαδικασία να γίνει πιο εύκολα κατανοητή.

- Στο βήμα 1: Δημιουργία του Blockchain στο δίκτυο.
- Στο βήμα 2: Δημιουργία λογαριασμών.
- Στο βήμα 3: Έναρξη και διακοπή του mining.
- Στο βήμα 4: Πραγματοποίηση σύνδεσης μεταξύ κόμβων.
- Στο βήμα 5: Πραγματοποίηση συναλλαγής μεταξύ δύο κόμβων.
- Στο βήμα 6: Σύνδεση του Metamask με το ιδιωτικό δίκτυο.

- Στο βήμα 7: Απόκτηση ιδιωτικού κλειδιού ενός λογαριασμού και η αποθήκευση του σε αρχείο JSON.
- Στο βήμα 8: Ανέβασμα έξυπνου συμβολαίου στο δίκτυο.
- Στο βήμα 9: Τελικό τρέξιμο του D-app στον φυλλομετρητή.

4.3 Περιγραφή βημάτων

- Βήμα 1: Δημιουργία του Blockchain στο δίκτυο.

Κάθε VMs περιέχει τα βασικά που χρειάζεται για να λειτουργήσει αλλά πρέπει να προστεθούν επιπλέον εξαρτήματα και εργαλεία που απαιτούνται για να υποστηρίξει ο κόμβος το Ethereum. Αυτό πραγματοποιείται χρησιμοποιώντας τις παρακάτω εντολές.

- sudo apt-get install software-properties-common
- sudo add-apt-repository -y ppa:Ethereum/Ethereum
- sudo apt-get update
- sudo apt-get -y install Ethereum
- which geth
- mkdir ~/.Ethereum
- mkdir ~/.Ethereum/privatenet
- mkdir ~/.private_Ether
- nano ~/.private_Ether/genesis.json

Με αυτές εγκαθίσταται το Ethereum στον κόμβο και δημιουργείται ένας φάκελος με το όνομα Ethereum, όπου εκεί αποθηκεύονται τα απαραίτητα αρχεία του blockchain. Ακόμα δημιουργείται ο φάκελος private_Ether, που περιέχει το genesis αρχείο για τη δημιουργία των block.

Παρακάτω φαίνεται το Genesis Block. Είναι το πρώτο ή το αρχικό κομμάτι ενός ιδιωτικού δικτύου στο Ethereum. Περιέχει όλες τις απαραίτητες πληροφορίες για τη διαμόρφωση του δικτύου. Είναι ένα απλό JSON αρχείο όπου περιέχει κάποιες παραμέτρους. Παρακάτω αναλύονται οι παράμετροι που συμπεριλαμβάνονται στο αρχείο.

- Config: Το αρχείο ξεκινάει με το block "config", το οποίο περιέχει όλες τις παραμέτρους config και τα «κατώφλια», που ελέγχουν τις βασικές λειτουργίες του δικτύου.
- chainId: Προστατεύει το δίκτυο από μια επίθεση επανάληψης. Λειτουργεί ως αντιστάθμιση προκειμένου να αποτρέψει τους επιτιθέμενους από την αποκρυπτογράφηση συνεχών τιμών στο δίκτυο.
- homesteadBlock: Είναι η δεύτερη σημαντική κυκλοφορία του Ethereum. Η τιμή μηδέν (0) σημαίνει ότι χρησιμοποιείται αυτή η έκδοση.
- Difficulty: Είναι ο βαθμός δυσκολίας του mining στο δίκτυο.

- gasLimit: Ορίζει το όριο του κόστους του gas ανά block.
- nonce & mixhash: Είναι τιμές οι οποίες, όταν συνδυάζονται, επαληθεύουν ότι ένα block έχει πράγματι εξαχθεί κρυπτογραφικά και επομένως είναι έγκυρο.
- alloc: Επιτρέπει τον καθορισμό μιας λίστας «προγεμισμένων» πορτοφολιών.

Τα περιεχόμενα του Genesis αρχείου φαίνονται στην Εικόνα 21 παρακάτω.


```
{
"config":{
"chainId":15,
"homesteadBlock":0,
"eip155Block":0,
"eip158Block":0
},
"nonce":"0x0000000000000042",
"mixhash":"0x00000000000000000000000000000000000000000000000000
0000000000
0000000",
"difficulty":"0x200",
"alloc": {},
"coinbase": "0x0000000000000000000000000000000000000000",
"timestamp": "0x00",
"parentHash":"0x00000000000000000000000000000000000000000000000000
00000000000
000000000",
"gasLimit":"0xffffffff",
"alloc":{
}
}
}
```


Εικόνα 16: Περιεχόμενα του Genesis αρχείου.

Από την στιγμή που ο κόμβος είναι έτοιμος εκτελούνται οι παρακάτω εντολές.

- get--datadir~/.Ethereum/privatenet/ init ~/.private_Ether/genesis.json
- geth --datadir="consert" --networkid 15 --rpc --rpcport "8545" --rpcaddr "localhost" --rpccorsdomain "*" -rpcapi"eth,net,web3,miner,debug,personal,rpc" –nodiscover console 2>> eth.log

Οι παραπάνω εντολές βοηθάνε στην αρχικοποίηση του δικτύου με βάση το genesis αρχείο, ξεκινάει το geth και αποθηκεύονται τα αρχεία καταγραφής. Με την εντολή «tail -F /home/user/eth.log» εμφανίζονται τα παρεχόμενα του αρχείου καταγραφής eth.log.

```
INFO [01-15|18:50:22.542] Maximum peer count                       ETH=25 LES=0
total=25
INFO [01-15|18:50:22.542] Allocated cache and file handles         database=/hom
e/user/.ethereum/privatenet/geth/chaindata cache=16 handles=16
INFO [01-15|18:50:22.560] Persisted trie from memory database      nodes=0 size=
0.00B time=2.335µs gcnodes=0 gcsize=0.00B gctime=0s livenodes=1 livesize=0.00B
INFO [01-15|18:50:22.561] Successfully wrote genesis state         database=chai
ndata                                     hash=8da729…3e3e9f
INFO [01-15|18:50:22.561] Allocated cache and file handles         database=/hom
e/user/.ethereum/privatenet/geth/lightchaindata cache=16 handles=16
INFO [01-15|18:50:22.578] Persisted trie from memory database      nodes=0 size=
0.00B time=2.334µs gcnodes=0 gcsize=0.00B gctime=0s livenodes=1 livesize=0.00B
INFO [01-15|18:50:22.579] Successfully wrote genesis state         database=ligh
tchaindata                                    hash=8da729…3e3e9f
user@snf-8003:~$ the network based on the genesis file
```

Εικόνα 17: Αρχικοποίηση δικτύου με βάση το genesis

- Βήμα 2

Εφόσον έχει τελειώσει η διαμόρφωση του Ethereum κόμβου στο VM τότε, πρέπει να συνεχιστεί η διαδικασία και να δημιουργηθούν λογαριασμοί, όπου θα αποθηκεύονται εκεί τα Ether από το mining που θα εκτελεί ο κόμβος. Το βήμα αυτό πραγματοποιείται σε κάθε κόμβο, για κάθε λογαριασμό που υπάρχει σε αυτόν.

- personal.newAccount() #Δημιουργία λογαριασμού, όπου μέσα στις παρενθέσεις σε εισαγωγικά εισάγετε ένας κωδικός για τον λογαριασμό.
- eth.getBalance(eth.accounts[0])])# Εμφανίζεται το υπόλοιπο Ether του λογαριασμού.

```
["0x664e8fde1351d8e91d03cd34b652eb910067971e",
> eth.getBalance(eth.accounts[0])
4.82406916205523e+22
```

Εικόνα 18: Εμφάνιση ενός λογαριασμού και το υπόλοιπο του σε Ether

- Βήμα 3

Εκτελώντας τις παρακάτω εντολές στο geth σε κάθε κόμβο, ρυθμίζονται οο λογαριασμοί ως Etherbase/coinbase, έτσι ώστε να λαμβάνουν τα Ether από το mining. Με τη πρώτη εντολή ξεκινά το mining και με την δεύτερη το διακόπτει, όπου μετά από μερικά λεπτά εάν ελεγχθεί τα υπόλοιπα των λογαριασμών, αυτά θα έχουν αυξηθεί.

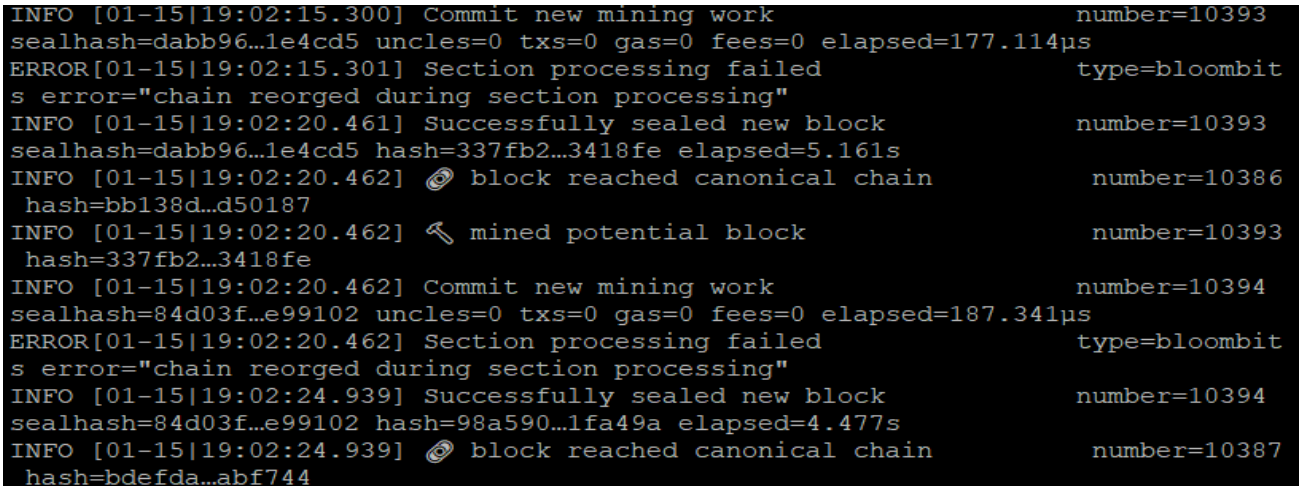
- miner.start() # Ξεκινάει το mining.
- miner.stop() # Διακόπτει το mining.

```
> miner.start()
null
> miner.stop()
null
```

Εικόνα 19: Έναρξη και διακοπή του mining

Για να βεβαιωθεί ο χρήστης ότι το mining έχει ξεκινήσει, αρκεί να παρατηρήσει το αρχείο eth.log, όπου καταγράφει οτιδήποτε γίνεται στο blockchain. Παρακάτω, φαίνεται το αρχείο καταγραφής,

στο οποίο παρατηρείται η πορεία του mining των block από τον συγκεκριμένο λογαριασμό. Επίσης, φένεται ότι ο κόμβος έχει κάνει mining ένα block **(mined potential block)** και συνεχίζει να κάνει mining τα επόμενα blocks **(commit new mining work).** Η διαδικασία αυτή επαναλαμβάνεται μέχρις ότου να διακοπεί το mining.



Εικόνα 20: Mining του block-eth.log

Πλέον, στο τέλος της διαδικασίας δημιουργίας ενός κόμβου με Ether, ο κόμβος περιέχει έναν λογαριασμό, ο οποίος μπορεί τόσο να στείλει, όσο και να λάβει Ether. Για τη δημιουργία περισσότερων κόμβων πραγματοποιείται η ίδια διαδικασία από την αρχή σε ξεχωριστό VMs.

- Βήμα 4

Σε αυτό το σημείο, οι κόμβοι είναι έτοιμοι να στείλουν και να λάβουν Ether, αλλά κανένας κόμβος δεν βλέπει τον άλλον, διότι δεν είναι συνδεδεμένοι μεταξύ τους ακόμα. Οπότε πρέπει να αλληλοσυνδεθούν. Συνεπώς, το αποτέλεσμα σε αυτό το βήμα θα είναι η δημιουργία ενός ιδιωτικού Ethereum δικτύου.

Για την αλληλοσύνδεση τους, χρειάζεται ένας κόμβος «διαχειριστής» ή αλλιώς bootstrap κόμβος. Αρχικά πρέπει να βρεθεί η διεύθυνση του bootstrap κόμβου, η οποία εμφανίζεται ως εξής:

«enode://c2036b8e20e0582f7f0835270cb7bb64049bfd014a2927a14ca05ef6e6a82bfae1acf8450a4cd15265361ff60dfc3eb0b7256f5b25345bd66a63ce309da5c588@83.212.75.112:30303?discport=0'»

Με μια συγκεκριμένη εντολή, επιτυγχάνεται η εισαγωγή της διεύθυνσης του «διαχειριστή» κόμβου και εν συνεχεία, εκτελείται στον άλλο κόμβο. Μετά παρατηρείται, ότι πλέον ο ένας κόμβος είναι αλληλοσυνδεμένος με τον άλλον. Σε αυτό το σημείο ο bootstrap κόμβος γνωρίζει ότι υπάρχει ένας κόμβος πέρα από αυτόν στο δίκτυο. Για τον τρίτο κόμβο επαναλαμβάνεται εκ νέου το προηγούμενο βήμα.

- admin.peers # Δείχει τον κόμβο διαχειριστή εάν υπάρχει.
- admin.nodeInfo.enode # Η διεύθυνση του κόμβου διαχειριστή.
- admin.addPeer #(“ εισάγεται το admin.nodeInfo.enode ”).

```
> admin.addPeer('enode://c2036b8e20e0582f7f0835270cb7bb64049bfd014a2927a14ca05ef
6e6a82bfae1acf8450a4cd15265361ff60dfc3eb0b7256f5b25345bd66a63ce309da5c588@83.212
.75.112:30303?discport=0')
true
```

Εικόνα 21: Έγκριση δημιουργίας του κόμβου διαχειριστή. Αυτό φαίνεται από την απάντηση true που εμφανίστηκε.

Εικόνα 22: Σύνδεση μεταξύ δύο κόμβων. Στο caps και enode φαίνεται ποιοι κόμβοι είναι συνδεμένοι μεταξύ τους. Επίσης, φαίνονται και οι διευθύνσεις τους.

- Βήμα 5

Για να γίνει μια συναλλαγή μεταξύ των δύο κόμβων, χρειάζονται οι διευθύνσεις του αποστολέα και του παραλήπτη, όπως και να ξεκλειδωθεί ο λογαριασμός του αποστολέα. Η εντολή eth.accounts εμφανίζει τις διευθύνσεις που βρίσκονται στο κόμβο, δίνοντας μας τη δυνατότητα στο χρήστη να διαλέξει τον αποστολέα και τον παραλήπτη. Η personal.unlockAccount(eth.coinbase) ξεκλειδώνει τον λογαριασμό και το eth.coinbase είναι η διεύθυνση, από την οποία θα στείλουμε τα Ether.

```
> personal.unlockAccount("0xc27f8f7309816cab19bf130b4b81593cf124f965")
Unlock account 0xc27f8f7309816cab19bf130b4b81593cf124f965
Passphrase:
true
```

Εικόνα 23: Ξεκλείδωμα λογαριασμού

Χρησιμοποιώντας την παρακάτω εντολή εμφανίζονται τα Ether του λογαριασμού: web3.fromWei(web3.eth.getBalance(web3.eth.coinbase),” Ether”).

```
> web3.fromWei(web3.eth.getBalance(web3.eth.coinbase), 'ether')
49095.691620523
```

Εικόνα 24: Τα Ether του κόμβου

Στη συνέχεια, με τη χρήση της eth.sendTransaction({from: eth.coinbase, to: “address” value: web3.toWei(10,“Ether”)}) πραγματοποιείται μια συναλλαγή, όπου στέλνονται 10 Ether σε μια άλλη διεύθυνση.

```
> eth.sendTransaction({from: "0xc27f8f7309816cab19bf130b4b81593cf124f965", to: "
0xe723052c126ecbe2b9427944b3435cb29c42f38e"
......  values: web3.toWei(10,'ether')})
"0x88f5e8b15a133ff897690e4d2ba2315a2f8e2f64f5a93fb41c66c095bbb7538b"
```

Εικόνα 25: Αρχικοποίηση συναλλαγής

Με την eth.pendingTransactions εμφανίζονται οι συναλλαγές, οι οποίες εκκρεμούν και δεν έχουν ακόμη ολοκληρωθεί.

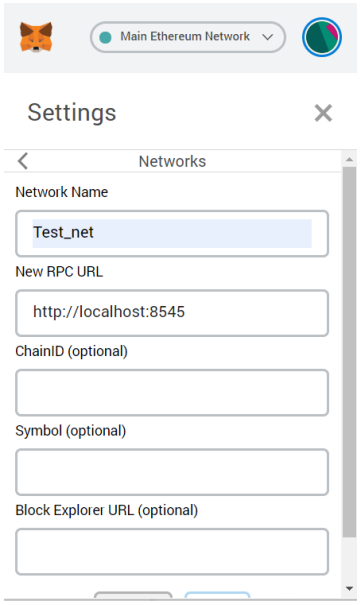

```
blockHash: null,
blockNumber: null,
from: "0xa39ac7083c84d94f242d1b9e7fdc0416e0172d4b",
gas: 21000,
gasPrice: 1000000000,
hash: "0x7abf7f9630c76952c5302396c1a331a2acaf0acf84c6704b13d27d02f632793e",
input: "0x",
nonce: 4,
r: "0x45108100eaa1f48c7dc069e52cf6172a562c129b1f04fb382a3cd8f2ed7140a3",
s: "0x1c0a490c13772b29d824040ef8949bf1f38f95f658e7c37af77a58fe94946cb2",
to: "0xe723052c126ecbe2b9427944b3435cb29c42f38e",
transactionIndex: null,
v: "0x42",
value: 10000000000000000000
```


Εικόνα 26: Συναλλαγή σε εκκρεμότητα μεταξύ δύο λογαριασμών σε ξεχωριστούς κόμβους

Απαραίτητη προϋπόθεση για να ολοκληρωθεί μια συναλλαγή, συνιστάται η πραγματοποίηση του mining από τον παραλήπτη.

- Βήμα 6

Για να συνδεθεί κάποιος στο ιδιωτικό Ethereum Δίκτυο με χρήση του Metamask, θα πρέπει αρχικά να είναι το Rpc ενεργοποιημένο στο δίκτυο καθώς και να γνωρίζει την διεύθυνση του Blockchain κόμβου. Στο Metamask επιλέγει ο χρήστης custom RPC, το δίκτυο που θέλει να συνδεθεί και εισάγει στις προχωρημένες ρυθμίσεις τα δεδομένα, όπως το όνομα και τη διεύθυνση του Blockchain. Για να υπάρχει επιτυχής σύνδεση του Metamask με το ιδιωτικό δίκτυο θα πρέπει το RPC να είναι ενεργοποιημένο και στο ιδιωτικό δίκτυο. Τα υπόλοιπα στοιχεία είναι απλώς προαιρετικά.



Εικόνα 27: Εισαγωγή στοιχείων για σύνδεση στο ιδιωτικό δίκτυο μέσω Metamask

- Βήμα 7

Από τη στιγμή που υπάρχει σύνδεση μεταξύ του Metamask και του ιδιωτικού δικτύου απαιτείται η εισαγωγή ενός λογαριασμού. Για να γίνει αυτό, χρειάζεται το ιδιωτικό κλειδί του λογαριασμού. Το αρχείο έχει όνομα "UTC-….", βρίσκεται αποθηκευμένο σε αυτό το μονοπάτι:

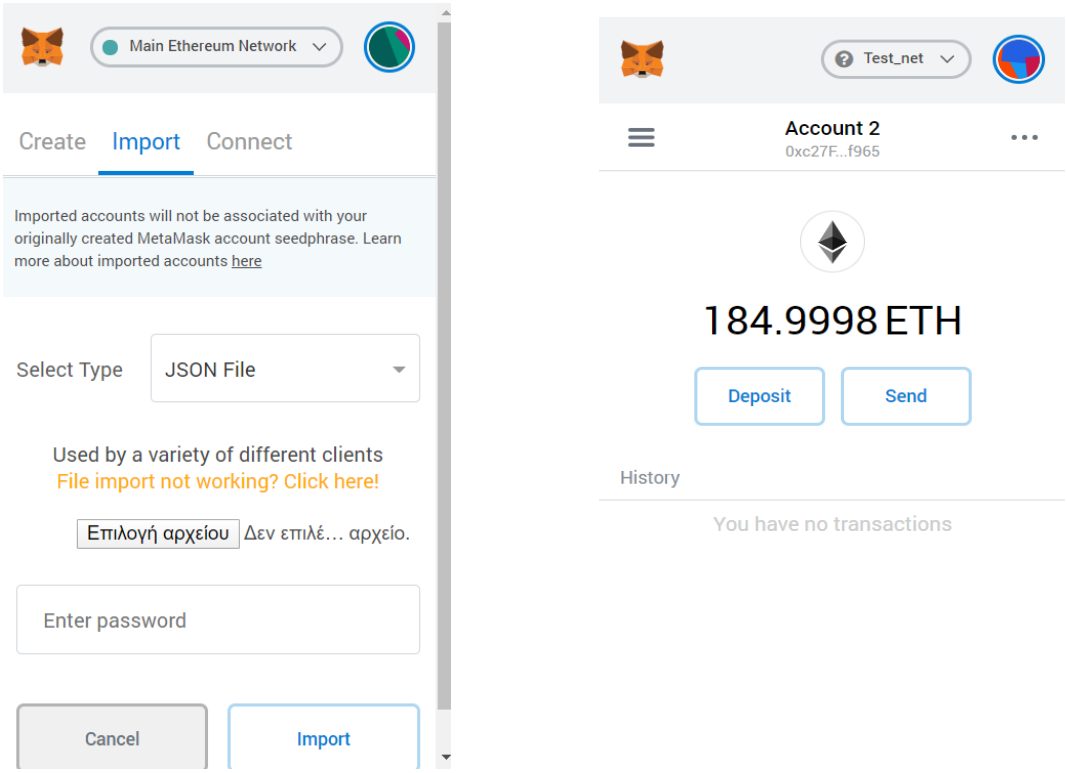
«path :/home/user/.Ethereum/privatenet/keystore»

Περιέχει διάφορα πεδία που αποτελούν το ιδιωτικό κλειδί του λογαριασμού.


```
{"address":"c27f8f7309816cab19bf130b4b81593cf124f965",
"crypto":{"cipher":"aes-128-ctr",
"ciphertext":"8d40a309de494f740cc1a41d861458997a7a5dc9ebdcc03c1b74a8fe805c16e4",
"cipherparams":{"iv":"0a6ffcdc6ceff998d01a67e1e772c566"},
"kdf":"scrypt",
"kdfparams":{"dklen":32,
"n":262144,
"p":1,
"r":8,
"salt":"e388ac6d889bf9b8bda25421bf7d44b314b7db851ebcee15fe88f07afc675443"},
"mac":"b862c6867818f206eb2112a4b6866b6d3e6047a8a0a8fca19df6359d88122877"},
"id":"92499787-311e-4f45-ac5d-bf90a11d130f",
"version":3}
```


Εικόνα 28: Τα περιεχόμενα ενός ιδιωτικού κλειδιού

Κάθε λογαριασμός έχει ένα μοναδικό κλειδί. Αφού βρεθεί, για να γίνει η εισαγωγή του στο Metamask και να το αναγνωρίζει, πρέπει πρώτα τα περιεχόμενα του κλειδιού να αποθηκευτούν σε ένα αρχείο JSON.



Εικόνα 29: Εισαγωγή κλειδιού στο Metamask

Από τη στιγμή που το κλειδί εισαχθεί με επιτυχία στο Metamask, φαίνεται ότι πλέον το συγκεκριμένο δίκτυο που συνδέθηκε με το Metamask περιέχει τον λογαριασμό με τα Ether που υπάρχουν σε αυτόν.

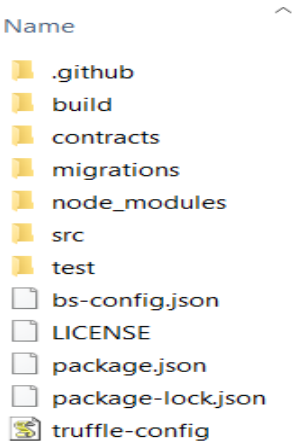
- Βήμα 8

Έχοντας έτοιμο το ιδιωτικό δίκτυο και έχει εισαχθεί ο λογαριασμός σε αυτό, η διαδικασία για το ανέβασμα ενός Dapp στο δίκτυο συνεχίζεται.

Για το ανέβασμα ενός Dapp χρειάζεται να εγκαταστήσουμε στον υπολογιστή μας τα εξής:

- το Node Package Manager (NPM)
- το Truffle Framework.

Συγκεκριμένα, το Dapp αποτελείται από τα παρακάτω αρχεία.



Εικόνα 30: Τα αρχεία που αποτελείται ένα D-App

Το Dapp αποτελείται από διάφορα αρχεία, όπως τα έξυπνα συμβόλαια, που βρίσκονται στον φάκελο «contracts» και το front-end του Dapp, που βρίσκεται στο φάκελο «src». Αναγκαίο για να συνεχίσει ομαλά η διαδικασία, είναι να γίνουν οι κατάλληλες αλλαγές στο φάκελο truffle-config, έτσι ώστε να γνωρίζει την διεύθυνση του κόμβου που χρειάζεται για να συνδεθεί το Metamask και την θύρα του. Όπως φαίνεται στην παρακάτω εικόνα, υπάρχουν πεδία στα οποία θα εισάγουμε τα παραπάνω στοιχεία, όπως επίσης και την έκδοση της γλώσσας που χρησιμοποιήθηκε για την ανάπτυξη των έξυπνων συμβολαίων.

```
module.exports = {
  // See <http://truffleframework.com/docs/advanced/configuration>
  // for more about customizing your Truffle configuration!
  networks: {
    development: {
      host: "83.212.74.223",
      port: 8545,
      network_id: "*" // Match any network id
    }
  },
  compilers: {
    solc: {
      version: '0.4.25',
      optimizer: {
        enabled: true,
        runs: 200
      }
    }
  }
};
```

Εικόνα 31: Περιεχόμενα του αρχείου Truffle-config

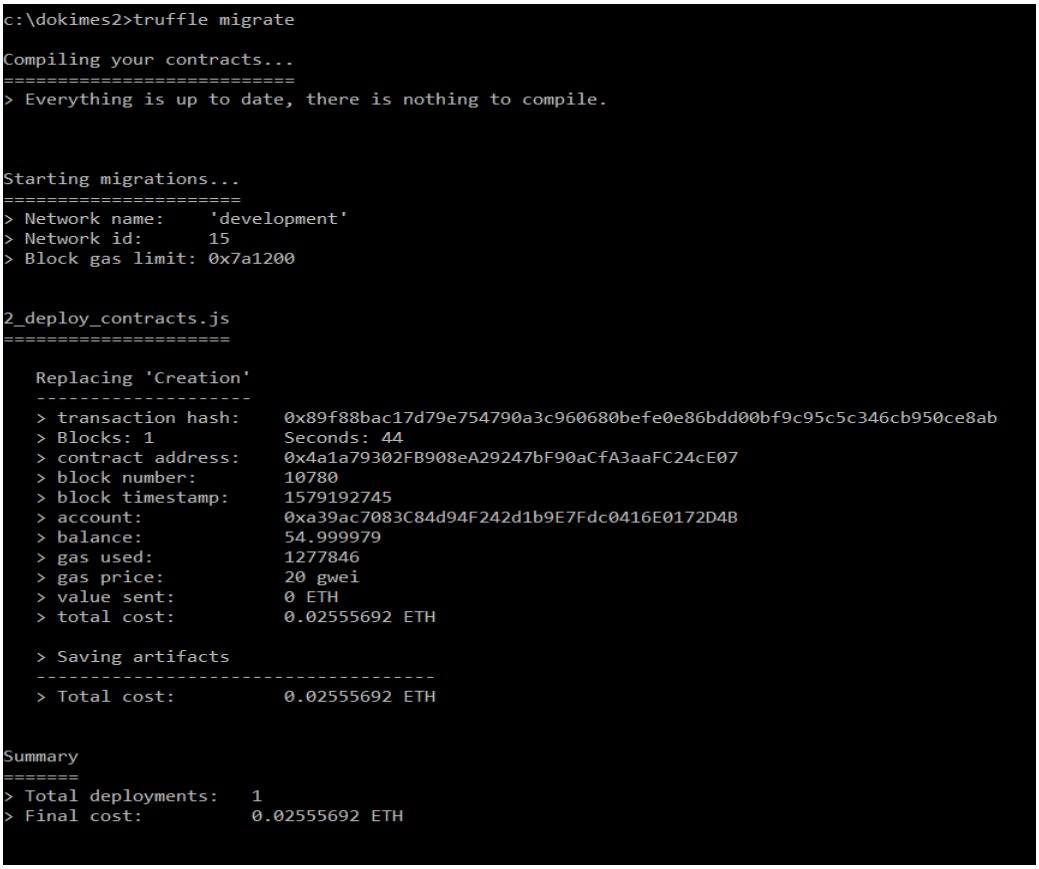
Σε αυτό σημείο γίνεται χρήση του cmd με δικαιώματα «διαχειριστή» ,για την αποφυγή τυχόν προβλημάτων, και πηγαίνουμε στο φάκελο όπου έχει αποθηκευτεί το Dapp με τη χρήση της εντολής CD. Με τη βοήθεια συγκεκριμένων εντολών του truffle, όπως είναι η εντολή truffle migrate, θα πραγματοποιήσει το ανέβασμα του έξυπνου συμβολαίου στο δίκτυο. Επίσης, όπως αναφέρθηκε σε προηγούμενη ενότητα, θα πρέπει να έχει ξεκλειδωθεί ο λογαριασμός που υπάρχει στον κόμβο για να συνεχιστεί η διαδικασία, με την χρήση της εντολής:

personal.unlockAccount(eth.coinbase)

```
c:\dokimes2>truffle migrate

Compiling your contracts...
===========================
> Everything is up to date, there is nothing to compile.



Starting migrations...
======================
> Network name:    'development'
> Network id:      15
> Block gas limit: 0x7a1200


2_deploy_contracts.js
=====================

   Replacing 'Creation'
   --------------------
   > transaction hash:    0x89f88bac17d79e754790a3c960680befe0e86bdd00bf9c95c5c346cb950ce8ab
   > Blocks: 0            Seconds: 0
```

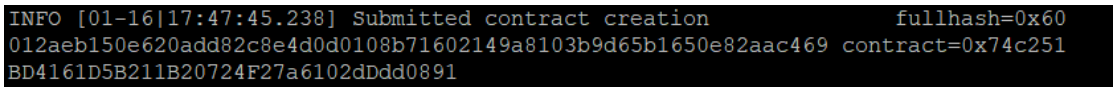
Εικόνα 32: Ανέβασμα έξυπνου συμβολαίου στο ιδιωτικό δίκτυο

Τώρα, για να συνεχιστεί αυτή η ενέργεια θα πρέπει ο κόμβος να αρχίσει τη διαδικασία του mining έτσι ώστε να εγκριθεί το συμβόλαιο και να ανέβει επιτυχώς στο δίκτυο , όπως συνέβη και με τις συναλλαγές που υπήρχαν σε προηγούμενο παράδειγμα.



Εικόνα 33: Επιτυχές ανέβασμα του έξυπνου συμβολαίου στο ιδιωτικό δίκτυο

Πλέον διαπιστώνεται ότι ανέβηκε το έξυπνο συμβόλαιο στο δίκτυο και από το αρχείο eth.log, που καταγράφει οτιδήποτε γίνεται στο Blockchain, στην παρακάτω εικόνα. Επίσης, αυτό φαίνεται και στην εικόνα 31, που περιέχει πληροφορίες σχετικά με το δίκτυο που ανέβηκε το έξυπνο συμβόλαιο, αλλά και το τελικό ποσό σε Ether που πρέπει να πληρωθεί για να ανέβει το έξυπνο συμβόλαιο στο δίκτυο. Ακόμα, αναφέρει την ποσότητα των έξυπνων συμβολαίων που ανέβηκαν.

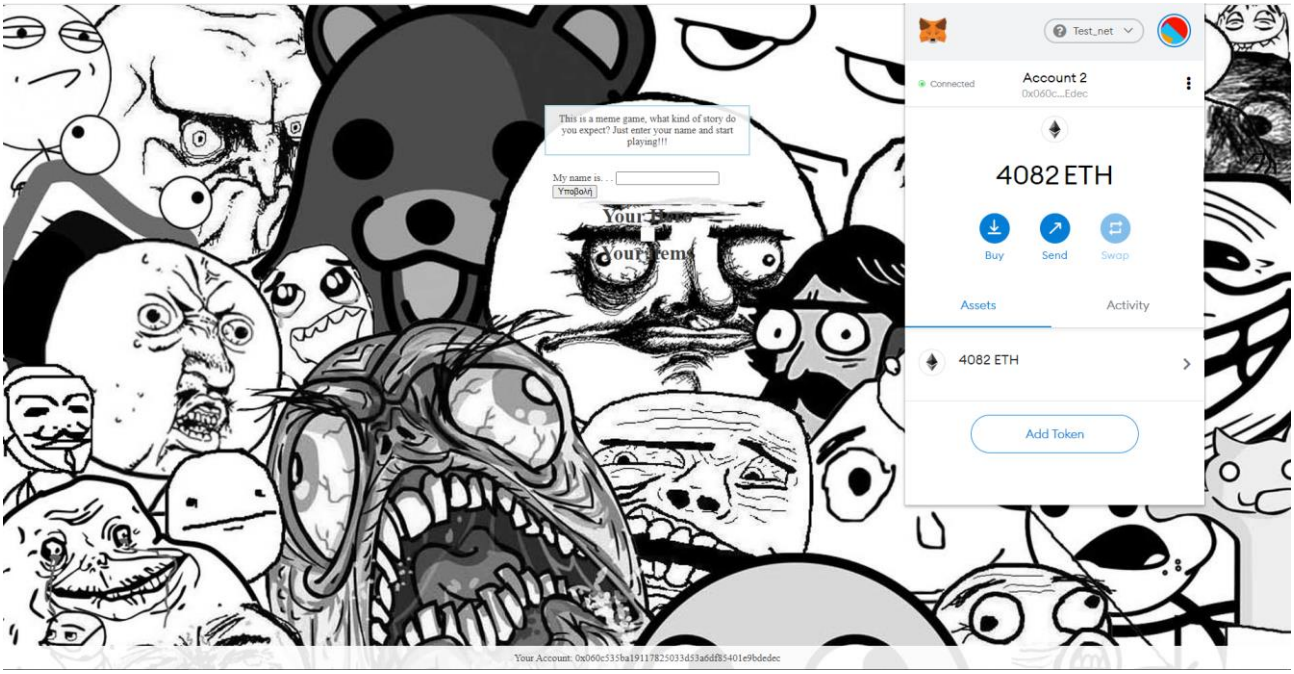


Εικόνα 34: Ενημέρωση του eth.log σχετικά με το ανέβασμα ενός συμβολαίου στο δίκτυο

- Βήμα 9

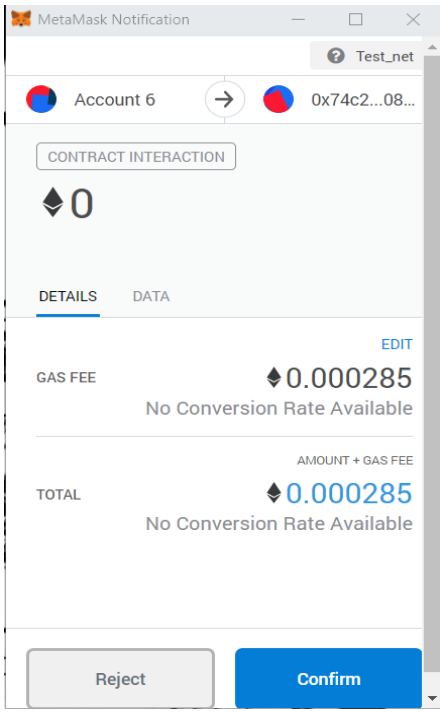
Από τη στιγμή που το συμβόλαιο έχει ανέβει στο δίκτυο, μένει μόνο να γίνει χρήση της εντολή npm run dev, όπου θα λειτουργήσει ο υπολογιστής ως server και θα φιλοξενήσει το Dapp, το οποίο θα τρέξει στον φυλλομετρητή. Στην παρακάτω εικόνα, φαίνεται το Dapp και το Metamask να είναι συνδεδεμένα στο δίκτυο και να υπάρχει ο λογαριασμός που εισήχθη με τα Ether.

Σχετικά με το D-app, είναι ένα παιχνίδι arcade, στα πλαίσια του οποίου δημιουργεί ο κάθε παίχτης τον δικό του χαρακτήρα, έχοντας ως αποστολή την εξόντωση εχθρών - τεράτων, κερδίζοντας σε κάθε αναμέτρηση πόντους εμπειρίας, ξεκλειδώνοντας νέα ανώτερα επίπεδα «levels».



Εικόνα 35: Εμφάνιση του D-app στον φυλλομετρητή

Αρχικά ο χρήστης επιλέγει όνομα και πατάει υποβολή, καλείται το έξυπνο συμβόλαιο το οποίο δημιουργεί τον χαρακτήρα και χρησιμοποιούνται τα Ether που έχει στο λογαριασμό του για να εκπληρωθεί αυτή η ενέργεια.



Εικόνα 36: Κάλεσμα μιας συνάρτηση που περιέχεται στο έξυπνο συμβόλαιο, δηλαδή πραγματοποιείται μια συναλλαγή μεταξύ του έξυπνου συμβολαίου και του χρήστη

Ο χαρακτήρας δημιουργήθηκε και ο χρήστης είναι έτοιμος να ξεκινήσει την περιπέτεια του.

Εικόνα 37: Αρχή μιας περιπέτειας

5 ΣΥΜΠΕΡΑΣΜΑΤΑ

Κατά την πραγματοποίηση της διπλωματικής εργασίας εξήχθησαν τα παρακάτω συμπεράσματα. Οι συναλλαγές σε ένα ιδιωτικό Blockchain δίκτυο πραγματοποιούνται πιο γρήγορα σε σχέση με ένα δημόσιο διότι τα μέλη που συμμετέχουν στο ιδιωτικό δίκτυο είναι λιγότερα και χρειάζεται λιγότερος χρόνος για την επίτευξη της συναίνεσης μεταξύ τους. Ακόμα, αυξάνεται η ασφάλεια και η εμπιστοσύνη μεταξύ των συμμετεχόντων διότι τα μέλη που έχουν πρόσβαση στο δίκτυο είναι συγκεκριμένα και έχουν προσκληθεί από τον δημιουργό του δικτύου.

Ένα ιδιωτικό Blockchain Ethereum δίκτυο παρέχει αρκετές δυνατότητες, όχι μόνο σε επιχειρήσεις αλλά και σε προσωπικό επίπεδο. Ο δημιουργός του ιδιωτικού δίκτυο μπορεί να κάνει mine το πρώτο Block. Με αυτό τον τρόπο, αποκτά τα δικά του Ether και του παρέχεται η δυνατότητα δοκιμής των D-App του, χωρίς την ανάγκη για πληρωμή πραγματικών Ether. Με αυτό τον τρόπο, μπορεί να τις δοκιμάζει μέχρι να τις ανεβάσει στο κύριο δίκτυο του Ethereum. Επίσης, για τις επιχειρήσεις, τα πλεονεκτήματα που παρέχουν είναι ασφαλής καταγραφή των συναλλαγών και προστασία από κακόβουλες επιθέσεις, από την στιγμή που κάθε συναλλαγή καταγράφεται στο καθολικό βιβλίο. Για την ακρίβεια, μπορούν να μοιράζονται πληροφορίες σχετικά με συγκεκριμένες συναλλαγές, που επιτρέπεται να γνωρίζουν μόνο συγκεκριμένα άτομα σε έναν ιδιωτικό κόμβο.

Η λειτουργία των D-App γίνεται αρκετά εύκολη, από την στιγμή που λειτουργεί σύμφωνα με ένα σύνολο κανόνων που εκτελείται αυτόματα και κάθε συναλλαγή εκτελείται γρήγορα, χωρίς καθυστερήσεις και ενδιάμεσους. Τα Dapp μπορούν να χρησιμοποιηθούν σε τράπεζες και επιχειρήσεις ως μέθοδοι πληρωμής συναλλαγών. Επίσης, ένα Dapp με την χρήση των έξυπνων συμβολαίων παρέχει σε κάθε χρήστη διαφάνεια και αυξάνεται η αποδοτικότητα του δικτύου, διότι οι όροι και οι προϋποθέσεις του συμβολαίου είναι ορατά μόνο σε αυτούς. Με την ακρίβεια και την ταχύτητα που εκτελούνται οι συναλλαγές, έχουν ως αποτέλεσμα την αύξηση των συναλλαγών που πραγματοποιούνται.

Με την πάροδο του χρόνου πραγματοποιήθηκαν αρκετά βήματα που οδήγησαν στην τεχνολογία του σήμερα. Κάθε μέρα που περνάει, η τεχνολογία εξελίσσεται και επιλύει προβλήματα που σε παλαιότερα χρόνια θα ήταν αδύνατη η επίλυση τους. Επίσης, σπουδαία άτομα, όπως ο Vitalik και ο Σατόσι Νακαμότο, άλλαξαν την εικόνα του ίντερνετ και καθώς ο χρόνος κυλάει, όλο και περισσότερες ενέργειες γίνονται για την ανακάλυψη νέων τεχνολογιών και την καλυτέρευση της ζωής του ανθρώπου.

Βιβλιογραφία – Αναφορές - Διαδικτυακές Πηγές

Benemerito, S., 2019. Deploying Smart Contracts with Truffle. [Ηλεκτρονικό]
Available at: https://medium.com/openberry/deploying-smart-contracts-with-truffle-1c056b452cde
[Πρόσβαση 3 Οκτώμβριος 2020].

Dale, O., 2017. Beginner's Guide to Ethereum Casper Hardfork: What You Need to Know. [Ηλεκτρονικό]
Available at: https://blockonomi.com/ethereum-casper/
[Πρόσβαση 3 Οκτώμβριος 2020].

Hargrave, J., 2019. BLOCKCHAIN FOR EVERYONE. New York: Simon & Schuster, Inc..

HBUS, 2018. What is a DApp?. [Ηλεκτρονικό]
Available at: https://medium.com/hbus-official/what-is-a-dapp-eec896a4bbbf
[Πρόσβαση 3 Οκτώμβριος 2020].

Hooda, P., 2018. Raft Consensus Algorithm. [Ηλεκτρονικό]
Available at: https://www.geeksforgeeks.org/raft-consensus-algorithm/
[Πρόσβαση 2 Οκτώμβριος 2020].

Krzyzanowski, P., 2018. Understanding Paxos. [Ηλεκτρονικό]
Available at: https://www.cs.rutgers.edu/~pxk/417/notes/paxos.html
[Πρόσβαση 1 Οκτώμβριος 2020].

Küfner, R., 2018. The Byzantine Generals Problem. [Ηλεκτρονικό]
Available at: http://cgi.di.uoa.gr/~mema/courses/m120/byzantineGenerals.pdf
[Πρόσβαση 4 Οκτώμβριος 2020].

Laura, M., 2020. EOS vs Ethereum - What's the Better Alternative?. [Ηλεκτρονικό]
Available at: https://www.bitdegree.org/crypto/tutorials/eos-vs-ethereum#strongeosstrong
[Πρόσβαση 8 Οκτώμβριος 2020].

Laurence, T., 2019. Blockchain for dummies. 2η Έκδοση επιμ. New Jersey: John Wiley & Sons, Inc.,.

Liu-Thorrold, L., Macdonald, M. & Julien, R., 2017. The Blockchain: A Comparison of Platforms and Their Uses Beyond Bitcoin. [Ηλεκτρονικό]
Available at: https://www.researchgate.net/profile/Lisa_Liu-Thorrold/publication/313249614_The_Blockchain_A_Comparison_of_Platforms_and_Their_Uses_Beyond_Bitcoin/links/5894447baca27231daf63689/The-Blockchain-A-Comparison-of-Platforms-and-Their-Uses-Beyond-Bitcoin.pdf
[Πρόσβαση 6 Οκτώμβριος 2020].

Macdonald, A., 2018. Paxos By Example. [Ηλεκτρονικό]
Available at: https://medium.com/@angusmacdonald/paxos-by-example-66d934e18522
[Πρόσβαση 5 Οκτώμβριος 2020].

Manav, G., 2020. Blockchain for dummies. 3η Έκδοση επιμ. New Jersey: John Wiley & Sons, Inc..

Patel, M., 2020. Consensus Algorithms in Blockchain. [Ηλεκτρονικό]
Available at: https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/
[Πρόσβαση 5 Οκτώμβριος 2020].

Peaster, W. M., χ.χ. Ethereum Casper Explained. [Ηλεκτρονικό]
Available at: https://academy.binance.com/blockchain/ethereum-casper-explained
[Πρόσβαση 2 Οκτώμβριος 2020].

Sharma, T., χ.χ. WHAT IS QUORUM BLOCKCHAIN?. [Ηλεκτρονικό]
Available at: https://www.blockchain-council.org/blockchain/what-is-quorum-how-is-it-different-from-other-blockchain/
[Πρόσβαση 3 Οκτώμβριος 2020].

vic, 2019. From Distributed Consensus Algorithms to the Blockchain Consensus Mechanism. [Ηλεκτρονικό]
Available at: https://www.alibabacloud.com/blog/from-distributed-consensus-algorithms-to-the-blockchain-consensus-mechanism_595315
[Πρόσβαση 7 Οκτώμβριος 2020].

Won, D., 2020. Ethereum Proof of Stake Date: Date + What You Need to Know. [Ηλεκτρονικό]
Available at: https://www.exodus.io/blog/ethereum-proof-of-stake-date/
[Πρόσβαση 9 Οκτώμβριος 2020].

Wood, G. & Antonopoulos, A., 2019. Mastering Ethereum. Sebastopol: O'Reilly Media, Inc..