ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

ΤΕΧΝΟΛΟΓΙΕΣ BLOCKCHAIN ΚΑΙ ΑΝΑΠΤΥΞΗ ΕΞΥΠΝΩΝ ΣΥΜΒΟΛΑΙΩΝ

Επιμέλεια εργασίας

Φοιτητές: **Αποστόλου Αθανάσιος (mpsp----),**

Μπιρμπάκος Γεώργιος (mpsp2220)

Ημερομηνία: **30/07/2023**

Εισαγωγή - Σκοπός

Ο **σκοπός** της εργασίας είναι να παρουσιάσει και να εξηγήσει τον σχεδιασμό ενός Έξυπνου Συμβολαίου με το όνομα "SupplyChain" που υλοποιεί μια εφοδιαστική αλυσίδα χρησιμοποιώντας την τεχνολογία blockchain. Η εφοδιαστική αλυσίδα είναι μια σειρά διαδικασιών και δραστηριοτήτων που συνδέονται μεταξύ τους και απαιτούνται για την κατασκευή και τη διανομή ενός προϊόντος ή υπηρεσίας από τον προμηθευτή έως τον τελικό καταναλωτή.

Το Έξυπνο Συμβόλαιο που παρουσιάζεται στην εργασία παρέχει μια απλή αλλά αποτελεσματική δομή που καταγράφει πληροφορίες σχετικά με προϊόντα, υποψηφίους και μεταφορές στο blockchain. Κάθε πληροφορία που προστίθεται είναι ανεξίτηλη και ασφαλής καθώς αποθηκεύεται σε μπλοκ που συνδέονται μεταξύ τους με κρυπτογραφικά συνδέσμους.

Ο σκοπός του Έξυπνου Συμβολαίου αυτού είναι να προσφέρει μια διαφανή, αποτελεσματική και ασφαλή λύση για την εφοδιαστική αλυσίδα. Οι ενέργειες προσθήκης προϊόντων, υποψηφίων και μεταφορών καθώς και η μεταβίβαση ιδιοκτησίας υποστηρίζονται από τις κατάλληλες συναρτήσεις του συμβολαίου. Η ιχνηλασιμότητα των προϊόντων και η καταγραφή των μεταφορών διασφαλίζεται από το blockchain, δίνοντας τη δυνατότητα στους εμπλεκόμενους φορείς να παρακολουθούν τη διαδρομή των προϊόντων και να επαληθεύουν την ακεραιότητα των δεδομένων.

Συνολικά, ο σκοπός της εργασίας είναι να δείξει πώς η τεχνολογία blockchain και τα Έξυπνα Συμβόλαια μπορούν να συμβάλουν στην ενίσχυση της εφοδιαστικής αλυσίδας, προσφέροντας αυξημένη διαφάνεια, ασφάλεια και αξιοπιστία στις διαδικασίες και τις δραστηριότητές της.

Προαπαιτούμενα

Για την ανάπτυξη και τον έλεγχο του Έξυπνου Συμβολαίου που θα παρουσιαστεί, είναι απαραίτητα ορισμένα προαπαιτούμενα εργαλεία και τεχνολογίες, όπως :

1. **Truffle**: Το Truffle είναι ένα πλαίσιο ανάπτυξης για το Ethereum που διευκολύνει τη δημιουργία, τη δοκιμή και τη διαχείριση Έξυπνων Συμβολαίων. Επιτρέπει την εύκολη ανάπτυξη και αναδρομική δοκιμή του συμβολαίου με δυνατότητα αυτοματοποίησης των διαδικασιών.

2. **Ganache**: Το Ganache είναι ένα προσομοιωτής του Ethereum blockchain που δημιουργεί ιδιωτικό δίκτυο για ανάπτυξη και δοκιμές συμβολαίων. Επιτρέπει τη δημιουργία τυχαίων λογαριασμών για δοκιμαστικούς σκοπούς και παρέχει ευέλικτο περιβάλλον για τον έλεγχο και την παρατήρηση των συμβολαίων.

3. **Metamask**: Το Metamask είναι μια επέκταση φυλλομετρητή για το Google Chrome που λειτουργεί ως πορτοφόλι Ethereum και δίνει στους χρήστες τη δυνατότητα να διαχειρίζονται τους λογαριασμούς τους και να υπογράφουν συναλλαγές μέσω του προγράμματος περιήγησής τους. Αυτό είναι ιδιαίτερα χρήσιμο κατά την ανάπτυξη και τη δοκιμή Έξυπνων Συμβολαίων, καθώς επιτρέπει εύκολη αλληλεπίδραση με την blockchain.

4. **Custom RPC Network**: Το Ganache παρέχει μια τοπική αλυσίδα blockchain που λειτουργεί σε ένα ιδιωτικό περιβάλλον δοκιμών. Για να επικοινωνήσουμε με το Ganache από το Metamask, δημιουργήσαμε ένα προσαρμοσμένο δίκτυο RPC. Το προσαρμοσμένο δίκτυο RPC λειτουργεί ως μια γέφυρα μεταξύ του Metamask και του Ganache, διευκολύνοντας τη σύνδεση του περιηγητή με το τοπικό δίκτυο που δημιουργήσαμε μέσω του Ganache. Τα στοιχεία σύνδεσης, όπως η διεύθυνση RPC και ο αριθμός πόρτας που παρέχει το Ganache, προστέθηκαν στις ρυθμίσεις του Metamask. Κατόπιν, το Metamask μπορεί να επικοινωνεί με το δίκτυο RPC, επιτρέποντας τη χρήση των λογαριασμών που δημιουργήσαμε στο Ganache για την υπογραφή συναλλαγών και τον έλεγχο του Έξυπνου Συμβολαίου που αναπτύχθηκε.

5. **Δήλωση λογαριασμών Ganache στο Metamask**: Στη συγκεκριμένη υλοποίηση, όπου χρησιμοποιούμε το Ganache σε συνδυασμό με το Metamask, ήταν απαραίτητο να δηλώσουμε τους λογαριασμούς του Ganache στο Metamask. Οι λογαριασμοί που δημιουργήθηκαν στο Ganache συνόδευαν τοπική αλυσίδα blockchain με προσομοιωμένα Ether (ETH) για τις δοκιμές. Κάθε λογαριασμός που δημιουργήθηκε στο Ganache είχε μια αρχική υπόληψη 100 Ether. Στο Metamask, προσθέσαμε χειροκίνητα αυτούς τους λογαριασμούς μέσω των ιδιωτικών κλειδιών, χρησιμοποιώντας τις διευθύνσεις που παρέχονται από το Ganache.Μετά την προσθήκη των λογαριασμών στο Metamask, ήταν δυνατό να διαχειριστούμε αυτούς τους λογαριασμούς και να τους χρησιμοποιήσουμε για την εκτέλεση συναλλαγών με το Έξυπνο Συμβόλαιο που αναπτύχθηκε στην εφοδιαστική αλυσίδα.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

Οδηγίες Χρήσης Εφαρμογής

Αφού ανέβει ο server *, ανοίγει ο localhost:3000, όπου βρίσκεται το βασικό UI χρήσης της εφαρμογής. Στη σελίδα αυτή, παρουσιάζονται δύο πίνακες. Ο πρώτος πίνακας εμφανίζει τα στοιχεία των λογαριασμών του Ganache, μαζί με την αντίστοιχη δραστηριότητά τους, ενώ ο δεύτερος πίνακας παρουσιάζει τις συναλλαγές που έχουν πραγματοποιηθεί.

Για να ξεκινήσει η ροή μεταφοράς προϊόντος, πρέπει να συνδεθούμε στο Metamask χρησιμοποιώντας τον πρώτο λογαριασμό του Ganache, που έχει καθοριστεί ως κάτοχος του συμβολαίου (contract owner). Έτσι, επιλέγοντας αυτόν τον λογαριασμό στο Metamask, μπορούμε να ξεκινήσουμε τη ροή.

Ο κάτοχος έχει τη δυνατότητα να εισάγει ένα νέο προϊόν και να ορίσει τις σχετικές παραμέτρους του. Αφού ορίσει το προϊόν και τις παραμέτρους (πατώντας το κουμπί "SET VALUES"), μπορεί να επιλέξει τον υποψήφιο που θα λάβει το προϊόν και, τελικά, να πατήσει το κουμπί "TRANSFER" για να μεταφερθεί το προϊόν. Αυτόματα, η σελίδα ανανεώνεται, και ο χρήστης δεν έχει, πλέον, δυνατότητα ενεργειών.

Τα δικαιώματα έχουν μεταβιβαστεί στον υποψήφιο που επιλέχθηκε, ο οποίος μπορεί να επεξεργαστεί μόνο τις παραμέτρους του προϊόντος (δηλαδή δεν μπορεί να εισάγει νέο προϊόν, ούτε να επιλέξει άλλο προϊόν). Συνδεόμενοι στο Metamask με τον λογαριασμό του νέου υποψηφίου, συνεχίζεται η ροή της εφοδιαστικής αλυσίδας εκ νέου.

* *Εντολές στο GITBASH προκειμένου να τρέξουμε την εφαρμογή* :

1. `cd supplyChain`
2. `truffle compile`
3. `truffle migrate --reset --network development`
4. `truffle development`
5. `SupplyChain.deployed().then(function(instance) { app = instance; });`
6. `Ctrl+C`
7. `npm run dev`

Δομές και λειτουργίες -Σχεδιασμός του Έξυπνου Συμβολαίου (Smart Contract):

Το Έξυπνο Συμβόλαιο με το όνομα "SupplyChain" είναι ένα συμβόλαιο που υλοποιεί μια εφοδιαστική αλυσίδα με τη χρήση της τεχνολογίας blockchain. Ας αναλύσουμε τη δομή και τις λειτουργίες του:

Δομή:

1. **Μεταβλητές**: Το συμβόλαιο περιέχει τις παρακάτω μεταβλητές:
   - Μεταβλητή "**contractOwner**": Η διεύθυνση του κατόχου του συμβολαίου.
   - Μεταβλητή "**senders**": Ένα mapping που αποθηκεύει τις διευθύνσεις των αποστολέων και δείχνει αν έχουν ήδη κάνει μια μεταφορά.
   - Μεταβλητή "**owners**": Ένα mapping που αποθηκεύει τις διευθύνσεις των ιδιοκτητών και δείχνει αν είναι ιδιοκτήτες του συμβολαίου.
   - Μεταβλητές "**chainCount**", "**candidatesCount**", "**transferShipmentsCount**" και "**productsCount**" που χρησιμοποιούνται σαν μετρητές για τον αριθμό των αντίστοιχων στοιχείων που προστίθενται.

2. **Δομές**: Το συμβόλαιο περιέχει τρείς δομές (structs) :
   - Δομή "**Candidate**": Περιέχει τα στοιχεία ενός υποψήφιου στην εφοδιαστική αλυσίδα, όπως το αναγνωριστικό του (id), η διεύθυνση του λογαριασμού (Account), ο αριθμός αλυσίδας (chainSeqNo) και αν είναι ιδιοκτήτης (isOwner).
   - Δομή "**transferShipment**": Περιέχει τα στοιχεία μιας μεταφοράς από τον προμηθευτή στον προορισμό, όπως το αναγνωριστικό της μεταφοράς (transferId), οι διευθύνσεις του προμηθευτή (origin) και του προορισμού (destination), το προϊόν που μεταφέρεται (product), το ποσό (amount), η ημερομηνία αναχώρησης (departureDate), η ημερομηνία άφιξης (arrivalDate) και μια περιγραφή (description).
   - Δομή "**Product**": Περιέχει τα στοιχεία ενός προϊόντος, όπως το αναγνωριστικό του (productId) και το όνομά του (name).

3. **Συναρτήσεις**: Το συμβόλαιο παρέχει διάφορες συναρτήσεις για την προσθήκη υποψηφίων, προϊόντων και μεταφορών, καθώς και για τη μεταφορά της ιδιοκτησίας σε νέους υποψηφίους. Οι κύριες συναρτήσεις περιλαμβάνουν:

   - Συναρτήσεις **προσθήκης**: "**addProduct**", "**addCandidate**" και "**addTransferShipment**".

   - Συναρτήσεις **μεταφοράς**: "**transfer**", όπου ο τρέχων ιδιοκτήτης μπορεί να μεταφέρει την ιδιοκτησία του συμβολαίου σε έναν νέο υποψήφιο, υπό την προϋπόθεση ότι ο νέος υποψήφιος δεν είναι ήδη ιδιοκτήτης και ότι υπάρχει ένας εγγεγραμμένος υποψήφιος με τη συγκεκριμένη διεύθυνση.

Επιπλέον, το συμβόλαιο μπορεί να παρέχει και λειτουργίες, όπως:

Λειτουργία "**getOwner**": Επιστρέφει τη διεύθυνση του τρέχοντος ιδιοκτήτη του συμβολαίου.

Λειτουργία "**getCandidatesCount**" και "**getTransferShipmentsCount**": Επιστρέφει τον αριθμό των υποψηφίων και των μεταφορών που έχουν προστεθεί στην εφοδιαστική αλυσίδα.

Λειτουργία "**getCandidateById**" και "**getTransferShipmentById**": Επιστρέφει τα στοιχεία ενός υποψήφιου και μιας μεταφοράς, αντίστοιχα, βάσει του αναγνωριστικού τους.

Με τον παραπάνω σχεδιασμό του Έξυπνου Συμβολαίου "SupplyChain", επιτυγχάνεται η αυτοματοποίηση και η διαφάνεια των διαδικασιών της εφοδιαστικής αλυσίδας. Κάθε ενέργεια, όπως η προσθήκη προϊόντων, υποψηφίων ή μεταφορών, και η μεταβίβαση ιδιοκτησίας, καταγράφεται στο blockchain και είναι διαθέσιμη για επαλήθευση από όλους τους συμμετέχοντες στο δίκτυο. Αυτό εξασφαλίζει την ασφάλεια, την εμπιστοσύνη και την ακεραιότητα των δεδομένων και των διαδικασιών στην εφοδιαστική αλυσίδα.

Συμβολή της Blockchain Τεχνολογίας στην ιχνηλασιμότητα εμπορευμάτων στη εφοδιαστική αλυσίδα

Η τεχνολογία blockchain μπορεί να συμβάλλει σημαντικά στην ιχνηλασιμότητα των εμπορευμάτων στην εφοδιαστική αλυσίδα, παρέχοντας ένα αξιόπιστο και αδιαμφισβήτητο κατανεμημένο καταγραφικό σύστημα. Ορισμένοι τρόποι που αυτό επιτυγχάνεται είναι οι ακόλουθοι:

1. **Αναγνωρισιμότητα και πιστοποίηση**: Κάθε προϊόν που προστίθεται στην εφοδιαστική αλυσίδα μπορεί να λάβει μοναδικό αναγνωριστικό ή "υπογραφή" που το πιστοποιεί ως γνήσιο. Αυτό μπορεί να συμβάλει στην αποτροπή της παραχάραξης και της πειρατείας.

2. **Διαφάνεια**: Όλες οι συναλλαγές και οι κινήσεις προϊόντων καταγράφονται στο κατανεμημένο καταγραφικό βιβλίο του blockchain, το οποίο είναι προσβάσιμο από όλους τους ενδιαφερόμενους με τα κατάλληλα δικαιώματα πρόσβασης. Αυτό εξασφαλίζει τη διαφάνεια σε όλη την αλυσίδα προμηθειών και επιτρέπει στους εμπλεκόμενους να παρακολουθούν την πρόοδο και την κατάσταση των προϊόντων καθ' όλη τη διάρκεια της μεταφοράς.

3. **Ασφάλεια δεδομένων**: Οι πληροφορίες σχετικά με την προέλευση, τις συνθήκες μεταφοράς και άλλες σημαντικές πληροφορίες αποθηκεύονται κρυπτογραφημένες στο blockchain. Μόνο όσοι έχουν τα αναγκαία δικαιώματα πρόσβασης μπορούν να

αποκρυπτογραφήσουν και να διαβάσουν τις πληροφορίες, προστατεύοντας τα δεδομένα από ανεπιθύμητη πρόσβαση.

4. **Ανιχνευσιμότητα**: Εφόσον κάθε μεταφορά και κάθε μεταβολή στην κατάσταση του προϊόντος καταγράφεται στο blockchain, είναι εύκολο να ανιχνευτεί η τρέχουσα θέση και κατάσταση του προϊόντος. Αυτό μπορεί να βοηθήσει στην αποτροπή των χαμένων παρτίδων προϊόντων και στην αντίδραση σε περιστατικά ατυχημάτων ή προβλημάτων κατά τη διάρκεια της μεταφοράς. Οι ενδιαφερόμενοι μπορούν να εντοπίσουν πού και πότε συνέβη ένα πρόβλημα και να ανιχνεύσουν τον αντίστοιχο υπεύθυνο.

5. **Εξάλλειψη ενδιάμεσων**: Η τεχνολογία blockchain επιτρέπει την απευθείας ανταλλαγή πληροφοριών και προϊόντων ανάμεσα στους λογαριασμούς που συμμετέχουν στην αλυσίδα προμηθειών. Αυτό μπορεί να μειώσει την ανάγκη για ενδιάμεσους ή διαμεσολαβητές, μειώνοντας τα κόστη και αυξάνοντας την αποτελεσματικότητα του συστήματος.

6. **Επιβεβαίωση πιστοποιήσεων και προέλευσης**: Οι πληροφορίες που καταγράφονται στο blockchain μπορούν να πιστοποιήσουν την προέλευση των προϊόντων και την συμμόρφωσή τους προς ορισμένες προδιαγραφές. Αυτό είναι ιδιαίτερα σημαντικό σε κάποιες βιομηχανίες, όπως η διατροφή και η φαρμακευτική, όπου οι καταναλωτές θέλουν να γνωρίζουν την προέλευση και την ποιότητα των προϊόντων που αγοράζουν.

Συνολικά, η τεχνολογία blockchain παρέχει ένα αξιόπιστο, διαφανές και ασφαλές σύστημα για την ιχνηλασιμότητα των εμπορευμάτων στην εφοδιαστική αλυσίδα. Μειώνει τον κίνδυνο απάτης, παραχάραξης και καθυστερήσεων, ενώ παράλληλα βελτιώνει την αποτελεσματικότητα, την εμπιστοσύνη και την διαφάνεια σε όλη τη διαδικασία παραγωγής και διακίνησης των προϊόντων.