ΣΥΣΤΗΜΑ ΤΑΥΤΟΠΟΙΗΣΗ ΑΡΧΕΙΩΝ

με την χρήση της τεχνολογίας Ethereum Blockchain

Περίληψη

Το σύστημα επιτρέπει την επαλήθευση της ακεραιότητας, της αυθεντικότητας, της ύπαρξης και της κατοχής ενός οποιουδήποτε τύπου αρχείου μέσω των τεχνολογιών Ethereum Blockchain, IPFS και της κρυπτογράφησης SHA-256.

develodio

http://proof.develodio.com

Περιεχόμενα

Εισαγωγή

Τί είναι το blockchain;

Πρόκειται για ένα δημόσιο ψηφιακό λογιστικό βιβλίο που έχει σχεδιαστεί ούτως ώστε να είναι αδιαπέραστο από τους hacker. Παρόλο που χρησιμοποιείται κυρίως ως τρόπος παρακολούθησης και επαλήθευσης των νομισματικών συναλλαγών, μπορεί επίσης να εντοπίζει και να ελέγχει σχεδόν οποιοδήποτε είδος δεδομένων, καθιστώντας την μια απίστευτα ασφαλή πλατφόρμα που έχει τη δυνατότητα να αλλάξει ολόκληρο το διαδίκτυο.

Κάθε χρονολογική αλλαγή στο βιβλίο αναφέρεται ως block (μπλοκ), ενώ μια μεγαλύτερη σειρά αλλαγών ονομάζεται αλυσίδα, Blockchain.

Αυτό που κάνει το blockchain τόσο ασφαλές είναι ο distributed (διανεμημένο, χωρίς έδρα) χαρακτήρας του. Δεν υπάρχει σε κανένα διακομιστή, Master Ledger (κυρίαρχο λογιστικό βιβλίο), αντίθετα, υπάρχει στον υπολογιστή του καθενός ταυτόχρονα! Αυτό σημαίνει ότι κάθε φορά που ενημερώνεται με νέες πληροφορίες, κάθε υπολογιστής που χρησιμοποιεί την πλατφόρμα, πρέπει να συμφωνεί ότι η αλλαγή είναι έγκυρη.

Αυτό σημαίνει ότι αν κάποιος θέλησε να παραποιήσει τα αρχεία στην blockchain, θα χρειαζόταν να «μπει» (hack) σε κάθε έναν από αυτούς τους υπολογιστές ταυτόχρονα, σε αντίθεση με μια ενιαία κεντρική (centralised) βάση δεδομένων.

Ο καθένας έχει πρόσβαση στο βιβλίο ανά πάσα στιγμή, αλλά χωρίς χαρακτηριστικά αναγνώρισης.

Το blockchain μπορεί να ελέγξει με ασφάλεια τις συναλλαγές μεταξύ δύο μερών ενώ μειώνει αποτελεσματικά την ανάγκη για μεσάζοντα.

Τι είναι το Ethereum Project;

Το 2013, μια ομάδα προγραμματιστών ανακοίνωσε ότι εργάζονται πάνω σε ένα project που θα επιτρέπει την δημιουργία χρηματοοικονομικών εφαρμογών χωρίς την ανάγκη κάποιας τράπεζας ή μεσάζοντα.

Δύο χρόνια αργότερα εμφανίστηκε το Ethereum. Πρόκειται για ένα ψηφιακό νόμισμα αλλά και μια ανοικτού κώδικα πλατφόρμα blockchain με προγραμματιζόμενη λειτουργία συναλλαγών.

Η τεχνολογία του blockchain είναι η κύρια διαφορά του Ethereum από το Bitcoin. Το blockchain του Ethereum δίνει την δυνατότητα να αναπτύξουμε διαφορετικές, ανεξάρτητες εφαρμογές που τρέχουν μέσω του δικτύου του.

Στο δίκτυο του Ethereum, οι εφαρμογές λέγονται Smart Contracts. Κατασκευάζονται κυρίως με την γλώσσα προγραμματισμού Solidity. Για κάθε εφαρμογή, ο δημιουργός θα πρέπει να καταβάλλει ένα αντίτιμο στο νόμισμα του δικτύου, το Ether.

Ουσιαστικά, το Ethereum είναι μια παγκόσμια υπολογιστική μηχανή. Αποτελείται από τους δεκάδες χιλιάδες υπολογιστές που συνδέονται στο δίκτυο για να σφραγίσουν συναλλαγές και οι πόροι τους τρέχουν τις εφαρμογές που δημιουργούμε.

Τί είναι το IPFS;

Το IPFS είναι διανεμημένο σύστημα αρχείων peer-to-peer που επιδιώκει να συνδέσει όλες τις υπολογιστικές συσκευές με το ίδιο σύστημα αρχείων. Κατά κάποιο τρόπο, το IPFS είναι παρόμοιο με το World Wide Web, αλλά το IPFS, θα μπορούσε να θεωρηθεί ως ενιαίο σμήνος BitTorrent, ανταλλάσσοντας αντικείμενα μέσα σε αποθετήριο Git. Με άλλα λόγια το IPFS παρέχει υψηλής απόδοσης, διευθετημένο σε περιεχόμενο μοντέλο μπλοκ αποθήκευσης, με διευθετημένες σε περιεχόμενο υπερσυνδέσεις.

Τί είναι το Metamask;

Το Metamask είναι ένα plugin που συνδέει το Google Chrome ή το Firefox στο δίκτυο του Ethereum. Το Metamask είναι εύκολο στη χρήση, πάντα προσβάσιμο και αποθηκεύει τα πάντα μέσα στον υπολογιστή και όχι στο διαδίκτυο.

Κρυπτογράφηση SHA-256

Ο αλγόριθμος SHA-256 (Ασφαλής Αλγόριθμος Κατακερματισμού 256-bit) χρησιμοποιείται για κρυπτογραφική ασφάλεια.

Η συνάρτηση είναι μία από τις συναρτήσεις που ανήκουν στην κατηγορία SHA-2. Έχει σχεδιαστεί από την Υπηρεσία Εθνικής Ασφάλειας των ΗΠΑ (NSA) και δημοσιεύθηκε επίσημα το 2002 από τη NIST ως ένα FIPS.

Οι αλγόριθμοι κρυπτογραφικού κατακερματισμού παράγουν μη αναστρέψιμους και μοναδικούς κατακερματισμούς. Όσο μεγαλύτερος είναι ο αριθμός των πιθανών κατακερματισμών, τόσο μικρότερη είναι η πιθανότητα δημιουργίας του ίδιου κατακερματισμού από δύο τιμές.

Περιγραφή

Με χρήση των προαναφερθέντων τεχνολογιών το Σύστημα Ταυτοποίησης Αρχείων (**http://proof.develodio.com**) διασφαλίζει την απόδειξη ύπαρξης, αυθεντικοποίησης, ακεραιότητας και κατοχής ενός οποιουδήποτε ηλεκτρονικού αρχείου.

Μέσα από την πλατφόρμα ο χρήστης μπορεί να ταυτοποιήσει ένα αρχείο, να καταχωρήσει ένα νέο, να προσθέσει ή να αφαιρέσει έναν κάτοχο του αρχείου.

Το σύστημα για κάθε αρχείο δημιουργεί ένα μοναδικό αναγνωριστικό κλειδί (SHA-256 hash). Το μοναδικό αυτό αναγνωριστικό κλειδί αντιπροσωπεύει την ακεραιότητα του αρχείου. Δεν υπάρχει άλλο αρχείο με το ίδιο αναγνωριστικό κλειδί. Οποιαδήποτε αλλαγή στο περιεχόμενο του αρχείου θα επιφέρει αλλαγή στο αναγνωριστικό κλειδί και θα χαθεί η αυθεντικότητα και η ακεραιότητα του αρχείου. Για τον λόγο αυτό **ο χρήστης θα πρέπει να φυλάξει το συγκεκριμένο αρχείο στην μορφή που το υπέβαλε στο σύστημα και να μην το τροποποιήσει**. Το αρχείο, αν επιθυμεί ο χρήστης, μπορεί να γίνει δημόσιο, αποθηκεύοντάς το στο IPFS.

Το σύστημα προσθέτει το μοναδικό αυτό αναγνωριστικό κλειδί μαζί με τις πρόσθετες πληροφορίες που συνοδεύουν το αρχείο και την χρονική στιγμή υποβολής στο Ethereum Blockchain. Από την στιγμή που οριστικοποιηθεί η προσθήκη στο Ethereum Blockchain, τα δεδομένα αυτά είναι αμετάβλητα και ακέραια για πάντα.

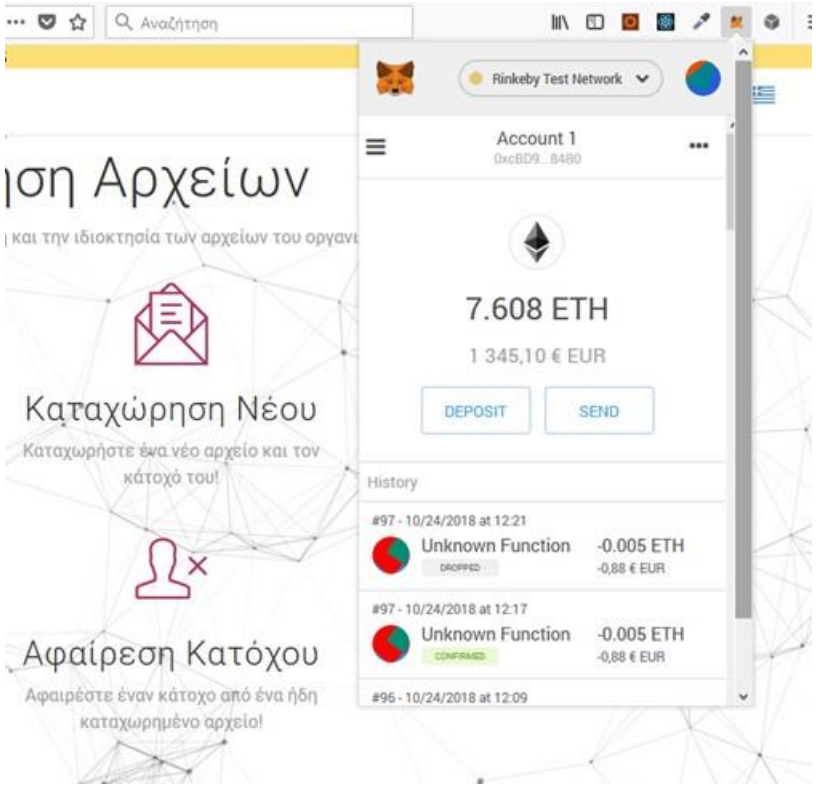
Λαμβάνοντας αυτές τις πληροφορίες από το Ethereum Blockchain, το σύστημα αποδεικνύει την απόδειξη ύπαρξης και κατοχής για το συγκεκριμένο αρχείο την συγκεκριμένη χρονική στιγμή.

Ταυτότητα Αρχείου

Παράμετρος Ταυτοποίησης	Τιμή
Block Timestamp #	22/10/2018, 11:09:51 π.μ.
Block Number #	3204493
Block Hash #	0xac99516c9cbd94737cbfe2bdf56944f7c3ea774894d364cf1ee8ffb61b8ba76a
Transaction Hash #	0x5e72f32228acadea3c0f90d572de25e8b452b0e5307422019d68735ae5a2cb26
From Address #	0xcbd985a1ef0cfe641e8ef9847d11e50e879984b0
File Hash #	3c1b657969707c7b82a184087602baef05dd74e8
File IPFS Hash #	QmYTVykF1R6i3YT8Z2hYn8AAtf3dzbFpFCmBEviTyyYgjE

Όλες οι μορφές και τα μεγέθη αρχείων είναι αποδεκτά.

Για την εκτέλεση κάποιας συναλλαγής απαιτείται η σύνδεση στο δίκτυο Rinkeyby Testnet του Ethernet μέσω του Metamask.



Προσοχή: Αυτή την στιγμή το σύστημα λειτουργεί δοκιμαστικά στο δίκτυο Rinkeby Testnet και δεν πρέπει να χρησιμοποιηθεί επιχειρησιακά!

Η τελική έκδοση του συστήματος θα εγκατασταθεί στο Main Ethereum Network. Το σύστημα μπορεί να εγκατασταθεί και σε Private Ethereum Network.

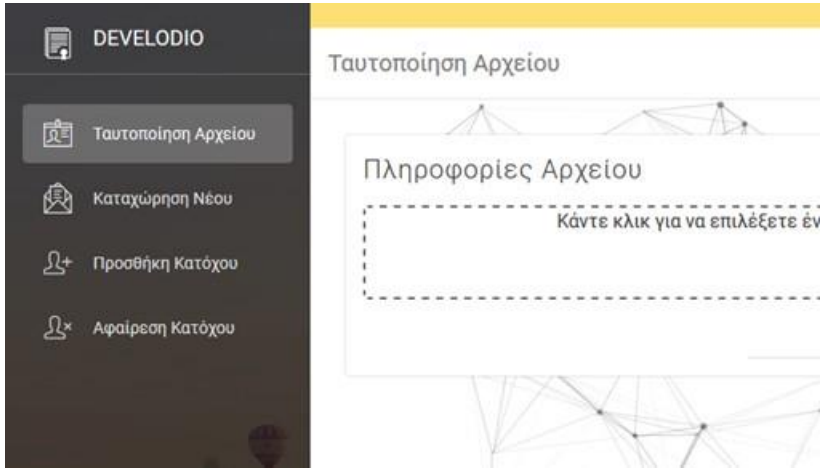
Το κόστος κάθε συναλλαγής του συστήματος έχει οριστεί σε 0.005 Ether (0.898€ τιμή 24/10/2018) συν το GAS Fee[1].

[1] Το ποσό που πρέπει να δοθεί ως ανταμοιβή στους «miners» για την επαλήθευση της συναλλαγής και την προσθήκη των δεδομένων στο Ethereum Network.

Ταυτοποίηση Αρχείου

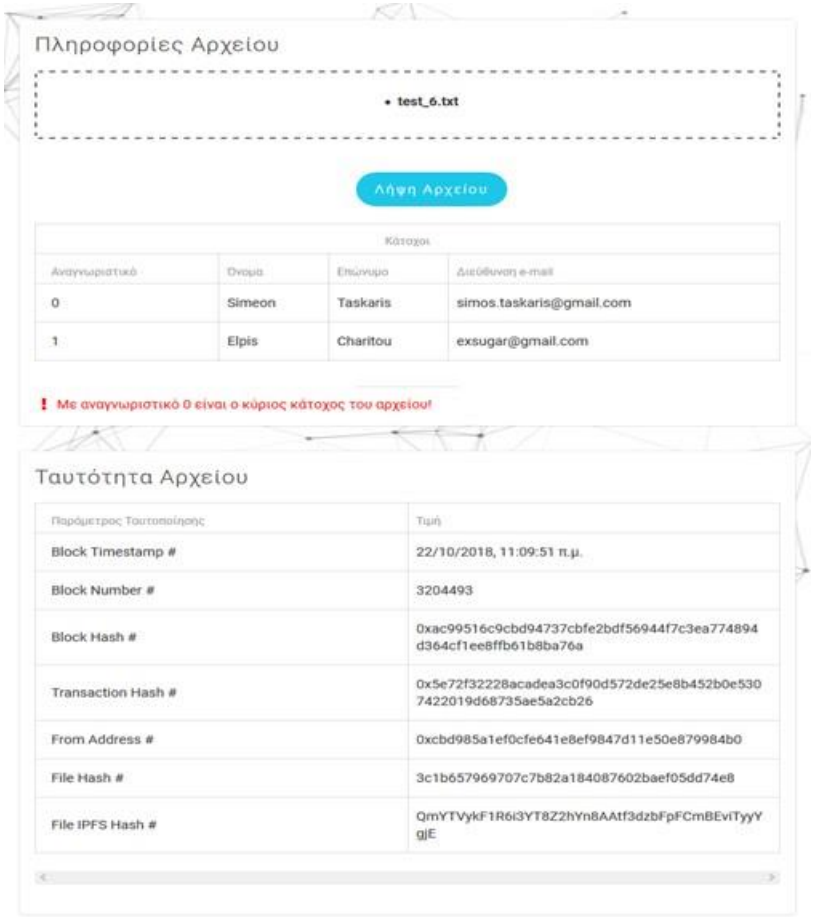
Για να ταυτοποιήσετε ένα αρχείο:

1. Επιλέξτε «Ταυτοποίηση Αρχείου» στο μενού αριστερά του συστήματος.



2. Στην περιοχή «Πληροφορίες Αρχείου» κάντε κλικ για να επιλέξετε ή σύρετε στην περιοχή αυτή από τον υπολογιστή σας το αρχείο.

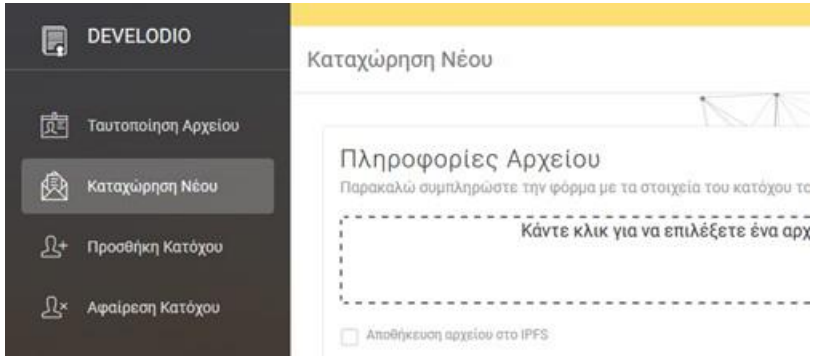
3. Η ταυτότητα του αρχείου θα εμφανιστεί. Σε περίπτωση που το αρχείο δεν είναι καταχωρημένο στο σύστημα, θα εμφανιστεί προειδοποίηση μη καταχώρησης στο σύστημα.



Καταχώρηση Αρχείου

Για να καταχωρήσετε ένα νέο αρχείο:

1. Επιλέξτε «Καταχώρηση Αρχείου» στο μενού αριστερά του συστήματος.

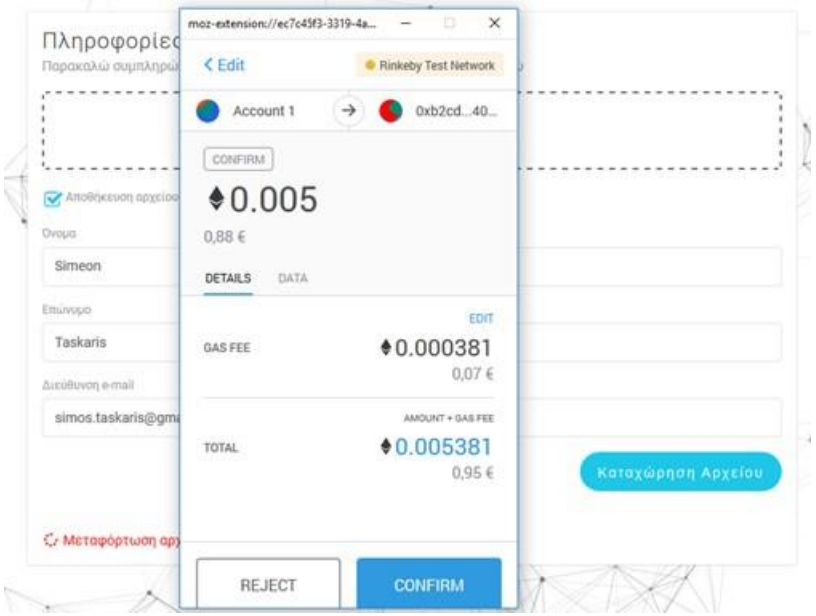


2. Στην περιοχή «Πληροφορίες Αρχείου» κάντε κλικ για να επιλέξετε ή σύρετε στην περιοχή αυτή από τον υπολογιστή σας το αρχείο που θέλετε να καταχωρήσετε στο σύστημα.

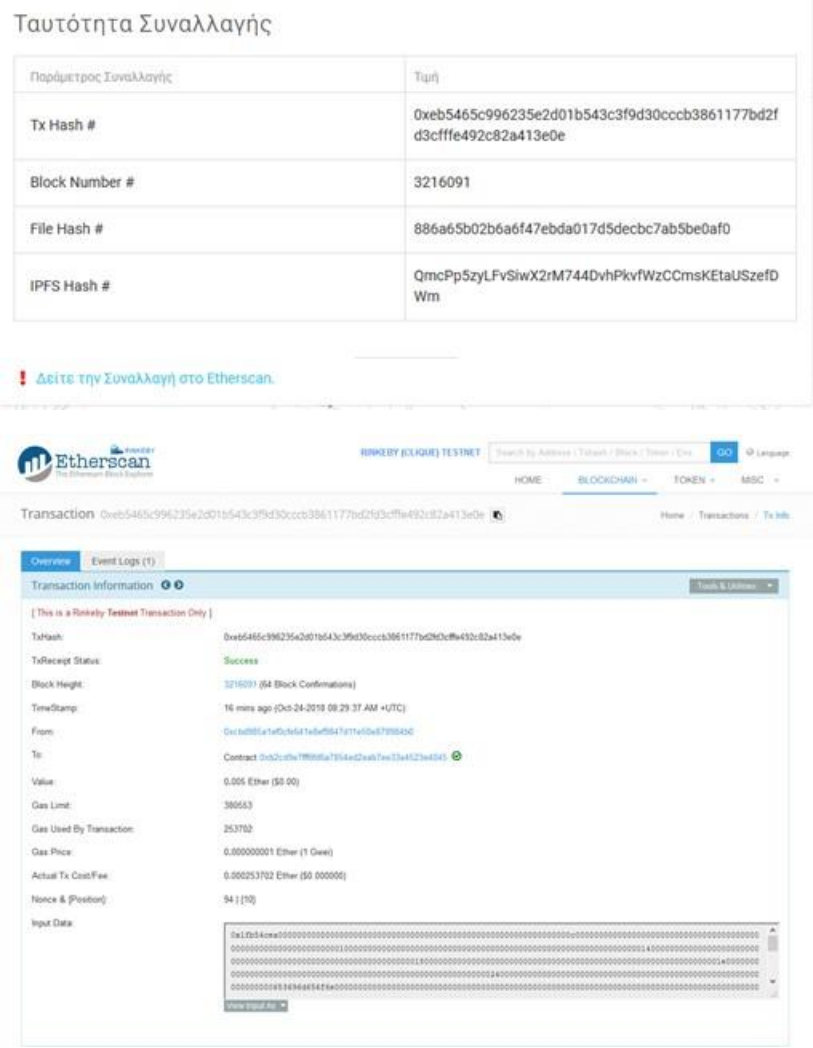
3. Συμπληρώστε τα στοιχεία του κυρίου κατόχου του αρχείου. Αφού καταχωρήστε το αρχείο στο σύστημα στην συνέχεια μπορείτε να προσθέσετε και άλλους κατόχους στην περίπτωση που το αρχείο έχει και άλλους. Σε περίπτωση που θέλετε να ανεβάσετε το αρχείο στο IPSF τσεκάρετε το «Αποθήκευση αρχείου στο IPFS».

4. Πατήσετε «Καταχώρηση Αρχείου» για να καταχωρηθεί το αρχείο στο σύστημα.

5. Επιβεβαιώστε την πληρωμή του αντιτίμου στο Metamask για την καταχώρηση του αρχείου στο σύστημα.



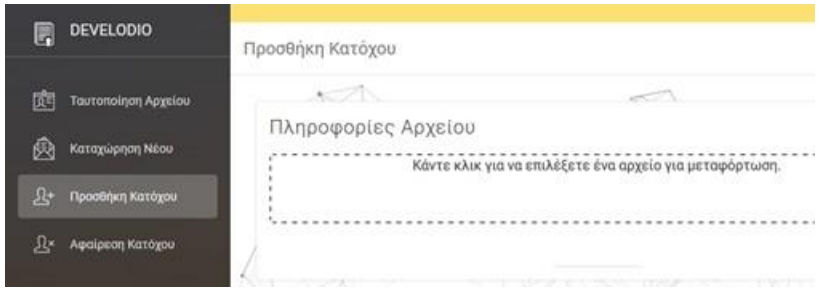
6. Μετά την επιτυχή καταχώρηση του αρχείου στο σύστημα, θα εμφανιστεί η ταυτότητα της συναλλαγής. Επίσης, μπορείτε να δείτε την συναλλαγή και στο Etherscan.



Προσθήκη Κατόχου[2]

Για να προσθέσετε έναν κάτοχο σε ένα υπάρχον καταχωρημένο αρχείο στο σύστημα:

1. Επιλέξτε «Προσθήκη Κατόχου» στο μενού αριστερά του συστήματος.

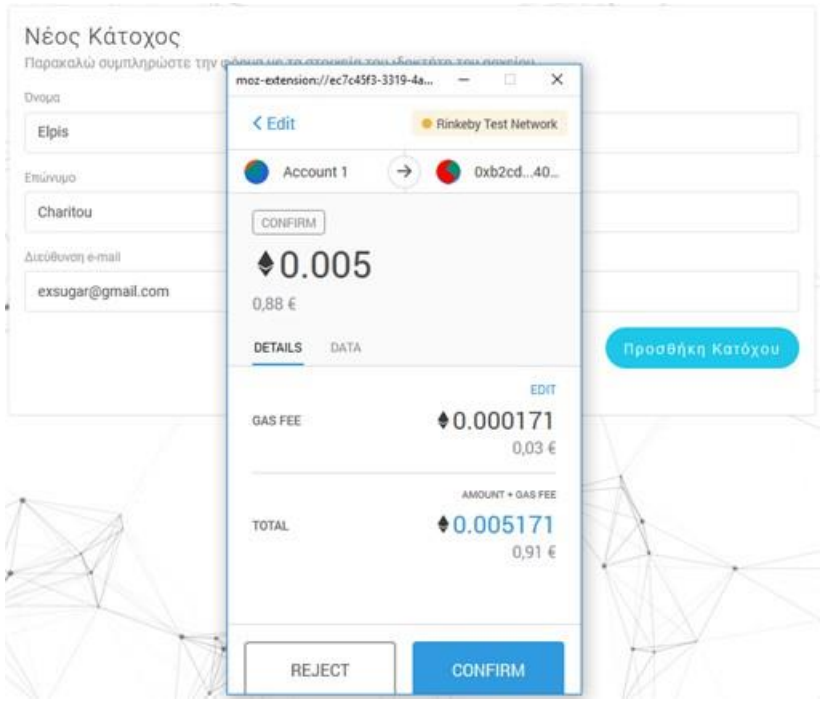


2. Στην περιοχή «Πληροφορίες Αρχείου» κάντε κλικ για να επιλέξετε ή σύρετε στην περιοχή αυτή από τον υπολογιστή σας το αρχείο στο οποίο θέλετε να προσθέσετε έναν νέο κάτοχο. Στις «Πληροφορίες Αρχείου» θα εμφανιστούν οι υπάρχοντες κάτοχοι του αρχείου.

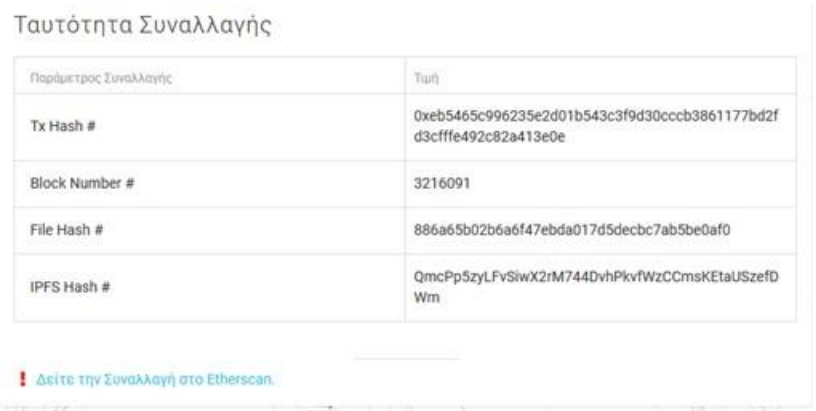
3. Στην περιοχή «Νέος Κάτοχος» συμπληρώστε τα στοιχεία του νέου κατόχου και πατήστε «Προσθήκη Κατόχου».

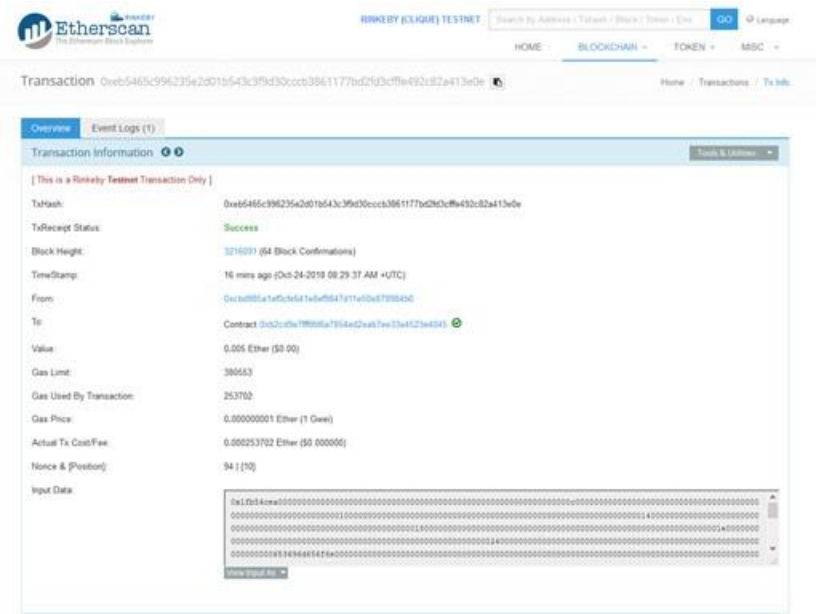
[2] Η ενέργεια αυτή μπορεί να πραγματοποιηθεί μόνο από τον κύριο κάτοχο του αρχείου και από την διεύθυνση λογαριασμού στο Metamask από την οποία καταχωρήθηκε το αρχείο.

4. Επιβεβαιώστε την πληρωμή του αντιτίμου στο Metamask για την καταχώρηση του κατόχου του αρχείου στο σύστημα.



5. Μετά την επιτυχή καταχώρηση του κατόχου του αρχείου στο σύστημα, θα εμφανιστεί η ταυτότητα της συναλλαγής. Επίσης, μπορείτε να δείτε την συναλλαγή και στο Etherscan.

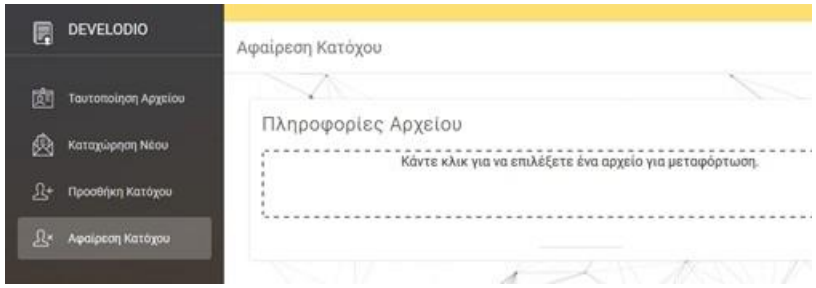




Αφαίρεση Κατόχου[3]

Για να αφαιρέσετε έναν κάτοχο από ένα υπάρχον καταχωρημένο αρχείο στο σύστημα:

1. Επιλέξτε «Αφαίρεση Κατόχου» στο μενού αριστερά του συστήματος.



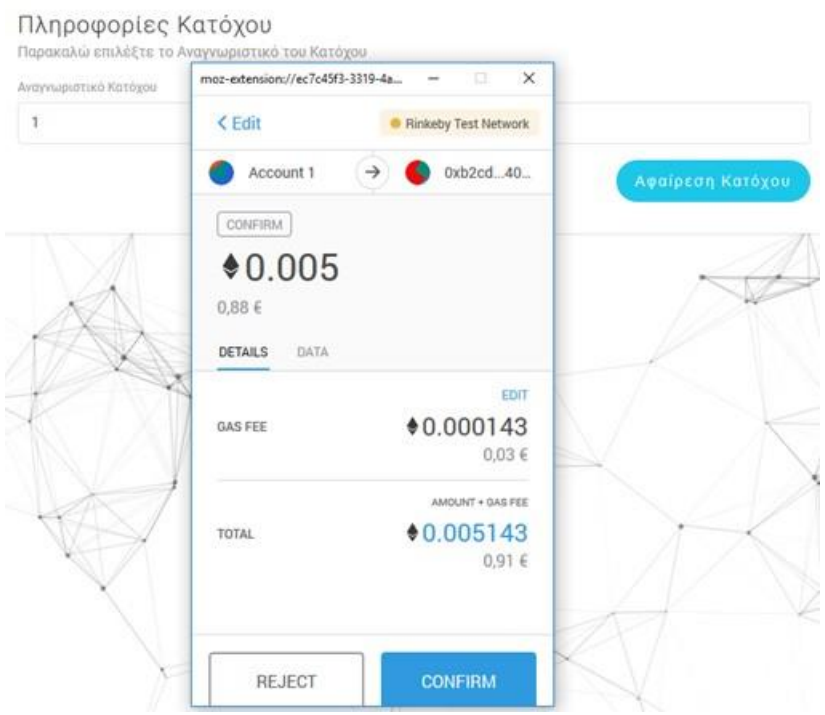
2. Στην περιοχή «Πληροφορίες Αρχείου» κάντε κλικ για να επιλέξετε ή σύρετε στην περιοχή αυτή από τον υπολογιστή σας το αρχείο στο οποίο θέλετε να προσθέσετε έναν νέο κάτοχο. Στις «Πληροφορίες Αρχείου» θα εμφανιστούν οι υπάρχοντες κάτοχοι του αρχείου.

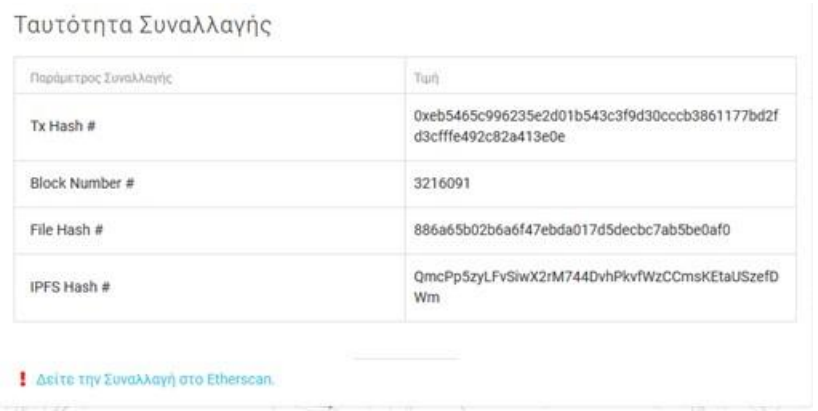
3. Στην περιοχή « Πληροφορίες Κατόχου» συμπληρώστε το αναγνωριστικό του κατόχου που θέλετε να αφαιρέστε και πατήστε «Αφαίρεση Κατόχου».[4]

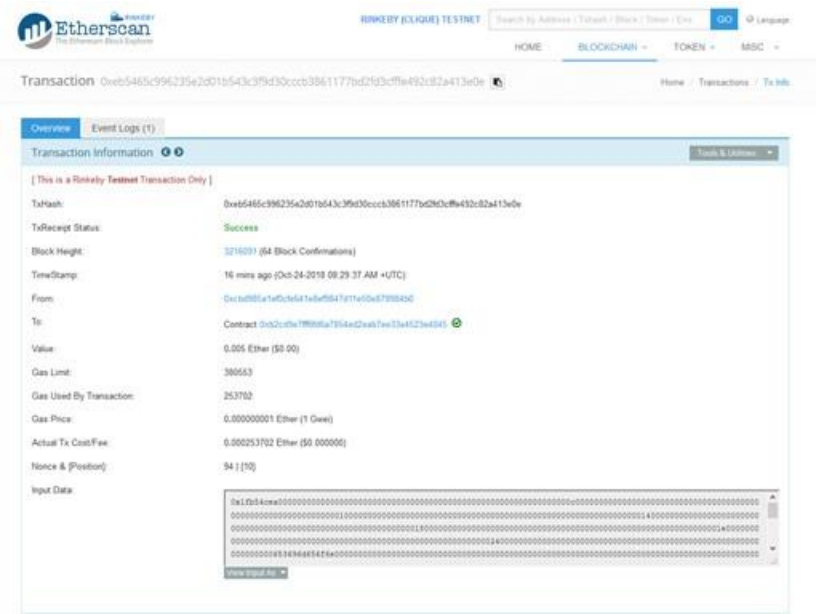
4. Επιβεβαιώστε την πληρωμή του αντιτίμου στο Metamask για την καταχώρηση του κατόχου του αρχείου στο σύστημα.

[3] Η ενέργεια αυτή μπορεί να πραγματοποιηθεί μόνο από τον κύριο κάτοχο του αρχείου και από την διεύθυνση λογαριασμού στο Metamask από την οποία καταχωρήθηκε το αρχείο.

[4] Ο κύριος κάτοχος του αρχείου δεν μπορεί να αφαιρεθεί.







5. Μετά την επιτυχή αφαίρεση του κατόχου του αρχείου στο σύστημα, θα εμφανιστεί η ταυτότητα της συναλλαγής. Επίσης, μπορείτε να δείτε την συναλλαγή και στο Etherscan.