ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ
ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Σχεδιασμός και Ανάπτυξη Εφαρμογής Έξυπνων Συμβολαίων (Smart Contracts) με χρήση Non-Fungible Tokens

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Γεώργιος Χ. Λαγός

Επιβλέπων : Γρηγόρης Μέντζας
Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2022

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ
ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Σχεδιασμός και Ανάπτυξη Εφαρμογής Έξυπνων Συμβολαίων (Smart Contracts) με χρήση Non-Fungible Tokens

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Γεώργιος Χ. Λαγός

Επιβλέπων : Γρηγόρης Μέντζας
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 12η Οκτωβρίου 2022.

.....	.....	.....
Γρηγόρης Μέντζας	Ιωάννης Ψαρράς	Δημήτριος Ασκούνης
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2022

.....
Γεώργιος Χ. Λαγός

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Αποτελεί αδιαμφισβήτητο γεγονός η ραγδαία τόσο ανάπτυξη όσο και υιοθέτηση των αποκεντρωμένων τεχνολογιών (Blockchain). Όλα ξεκίνησαν το έτος 2008 όπου δημοσιεύτηκε από τον δημιουργό του Bitcoin το επίσημο έγγραφο (Whitepaper) που περιέγραφε τον τρόπο λειτουργίας του επαναστατικού ψηφιακού χρυσού. Το Bitcoin αποτελεί σήμερα περισσότερο από ποτέ αποθήκευση αξίας (store of value) και μέσο συναλλαγής. Εύκολα διαπιστώνει κανείς πως χρειάστηκαν πολλά χρόνια για να σχηματιστεί εμπιστοσύνη στις αποκεντρωμένες αυτές τεχνολογίες, αφού μόλις τα τελευταία χρόνια έχουν εισέλθει στον χώρο των κρυπτονομισμάτων τόσο τεχνολογικοί όσο και οικονομικοί κολοσσοί, ακόμα και κράτη.

Το Bitcoin αποτελεί την γενέτειρα τεχνολογία στον αποκεντρωμένο χώρο και συγκαταλέγεται ως κρυπτονόμισμα πρώτης γενιάς. Αρκετά χρόνια αργότερα και με βάση την τεχνολογία του Bitcoin αναδύονται τα κρυπτονομίσματα δεύτερης και τρίτης γενιάς που εξέλιξαν περαιτέρω την αποκεντρωμένη τεχνολογία με χρήση έξυπνων συμβολαίων και πλέον συγκρίνονται με πολλές παραδοσιακές υπηρεσίες στον χώρο της οικονομίας. Η μεγαλύτερη αποκεντρωμένη πλατφόρμα που υποστηρίζει έξυπνα συμβόλαια είναι το Ethereum και συγκαταλέγεται στα κρυπτονομίσματα δεύτερης γενιάς. Το Ethereum αποτέλεσε επαναστατική επέκταση των δυνατοτήτων του αποκεντρωμένου τομέα και τα τελευταία χρόνια έχει γνωρίσει εκθετική υιοθέτηση, καθώς πληθώρα προγραμματιστών το αξιοποιεί προκειμένου να δημιουργήσει αποκεντρωμένες εφαρμογές (decentralized applications - Dapps).

Ο σκοπός της παρούσας διπλωματικής εργασίας είναι η ανάπτυξη μίας αποκεντρωμένης εφαρμογής στο δίκτυο του Ethereum που θα δημιουργεί και θα επαληθεύει την εγκυρότητα ψηφιακών εισιτηρίων τα οποία θα επιτρέπουν την πρόσβαση σε κατάλληλο περιεχόμενο.

Η εν λόγω αποκεντρωμένη εφαρμογή δύναται να αξιοποιηθεί από οποιονδήποτε, είτε πρόκειται για άτομο είτε για οργανισμό που επιθυμεί να πραγματοποιεί οποιουδήποτε είδους ψηφιακές εκδηλώσεις, ανεξαρτήτως περιεχομένου, και επιβάλει ως προϋπόθεση συμμετοχής εισιτήριο εισόδου. Οι κάτοχοι των εισιτηρίων θα έχουν την πλήρη κυριότητα των ειστηρίων τους, τα οποία θα είναι Non-Fungible Tokens (NFT) και θα μπορούν να μεταβούν σε μεταπώληση τους σε περίπτωση που το επιθυμούν.

Στο πλαίσιο της εργασίας αναλύθηκαν διεξοδικά οι έννοιες και οι λειτουργίες του Blockchain, των αλγορίθμων συναίνεσης και των έξυπνων συμβολάιων. Επιπρόσθετα, έγινε εκτεταμένη αναφορά στην επιλογή χρήσης Non-Fungible Tokens και των ευεργετικών επιδράσεων που αυτά επιφέρουν σε σύγκριση με τη παραδοσιακή μορφή εισιτηρίων.

Λέξεις κλειδιά: Blockchain, Ethereum, NFT, Εξύπνα συμβόλαια, Αποκεντρωμένη εφαρμογή (Dapp).

Abstract

The rapid development and adoption of decentralized technologies (Blockchain) is an indisputable fact. It all started back in the year 2008 when the creator of Bitcoin published the official document (Whitepaper) that described how the revolutionary digital gold works. Bitcoin is now more than ever a store of value and a medium of exchange. It took many years for people to build trust in these decentralized technologies, since it was not until recent years that both technological and economic giants and even states entered the cryptocurrency sector.
Bitcoin paved the way to the decentralized space and is considered a first generation cryptocurrency. Several years later, based on Bitcoin's technology, second and third generation cryptocurrencies emerged that further evolved decentralized technology using smart contracts and can now compete with many traditional financial services. The largest decentralized platform that supports smart contracts is Ethereum and is one of the second generation cryptocurrencies. Ethereum has revolutionized the capabilities of the decentralized sector and has recently seen exponential adoption, as a plethora of developers use it to create decentralized applications (Dapps).
The purpose of my thesis is to develop a decentralized application on the Ethereum network that will create and verify the validity of digital tickets that will allow access to locked content. This decentralized application can be used by anyone, whether it is an individual or an organization that wishes to hold any kind of digital events, regardless of content, and imposes an entry ticket as a condition of participation. Ticket holders will have full ownership of their tickets, which will be Non-Fungible Tokens (NFT) and will be allowed at all times to resale them if they wish.
In my thesis I also analyze in detail the concepts and utilities of Blockchain technology, consent algorithms and smart contracts. In addition, extensive analysis was made to support the choice of use of Non-Fungible Tokens and the beneficial effects that they offer compared to the traditional form of tickets.

Keywords: Blockchain, Ethereum, NFT, Smart Contracts, Decentralized Application (Dapp).

Ευχαριστίες

Με την παρούσα διπλωματική εργασία δεν ολοκληρώνεται μόνο ο κύκλος σπουδών μου στο Ε.Μ.Π. αλλά και η πολύχρονη και γεμάτη κόπο προσπάθεια μου να αποκτήσω πνευματικά εφόδια που θα μου εξασφαλίσουν ένα μέλλον πιθανοτικά καλύτερο, ίσως και λαμπρό.
Τίποτα δεν θα είχε πραγματοποιηθεί δίχως την οικογένεια μου που πάντα προσπαθούσε να με οδηγεί στο σωστό μονοπάτι και που μου παρείχε πάντα περισσότερα από όσα χρειαζόμουν.
Ακόμη, είμαι ευγνώμων τόσο για τους φίλους που σχημάτισα εντός σχολής, χωρίς την συνεργασία των οποίων δεν θα είχα ολοκληρώσει τις σπουδές μου, όσο και για τους εξωσχολικούς μου φίλους που παραμείναμε κοντά.
Τέλος, είμαι πολύ χαρούμενος για την εργασία μου, την οποία διεκπεραίωσα με απόλυτη χαρά, καθώς το θέμα βρισκόταν σε πλήρη ταύτιση με τα ενδιαφέροντα μου, ενώ η συνεργασία που ανέπτυξα με τον κ. Γρηγόρη Μέντζα και τους κ. Ιωάννη Βεργινάδη και κ. Φώτη Παρασκευόπουλο ήταν καλύτερη από ό,τι θα μπουρούσα ποτέ να φανταστώ.

Περιεχόμενα

Περίληψη 6
Abstract 8
Ευχαριστίες 10
Περιεχόμενα 12
Πίνακας σχημάτων 14
Κεφάλαιο 1: Εισαγωγή 16
1.1 Κίνητρο 16
1.2 Σκοπός 16
1.3 Οργάνωση του τόμου σε κεφάλαια 17
Κεφάλαιο 2: Γενικές πληροφορίες για το Blockchain 19
2.1 Εισαγωγή 19
2.2 Τι είναι το Blockchain 19
2.3 Γιατί είναι σημαντική η αποκέντρωση και παραδείγματα αξιοποίησης 21
2.4 Πορτοφόλι κρυπτονομισμάτων 22
2.5 Τι είναι τα Έξυπνα Συμβόλαια, τα Dapps και το DeFi 22
2.6 Τι είναι το Ethereum 23
2.7 Μειονεκτήματα του Ethereum και το Ethereum 2.0 24
2.8 Τι είναι τα NFTs 25
2.9 Γιατί τα NFTs προσελκύουν χρήστες 25
Κεφάλαιο 3: Υλοποίηση του NFT Ticketing System 28
3.1 Εννοιολογική ανάπτυξη της αποκεντρωμένης εφαρμογής 28
3.2 Εργαλεία ανάπτυξης της αποκεντρωμένης εφαρμογής 29
3.3 Το έξυπνο συμβόλαιο της εφαρμογής 32
Κεφάλαιο 4: Λειτουργία της αποκεντρωμένης εφαρμογής 39
4.1 Καταχώρηση του συμβολαίου, επιβεβαίωση του πηγαίου κώδικα και αρχικοποίηση του συστήματος ως διοργανωτές 39
4.2 Αλληλεπίδραση με το συμβόλαιο ως attendees 41
4.3 Επέμβαση του διοργανωτή για θεμιτές τροποποιήσεις και συλλογή εσόδων 47
4.4 Αλληλεπίδραση και χρήση του συστήματος από front-end 49
Κεφάλαιο 5: Συμπεράσματα, τρόποι επέκτασης και εφαρμογές 55
5.1 Ανακεφαλαίωση 55
5.2 Εφαρμογή του συστήματος σε ρεαλιστικά σενάρια 55
5.3 Τρόποι επέκτασης του συστήματος 56
5.4 Σχετικά με τους επικριτές της τεχνολογίας Blockchain και των κρυπτονομισμάτων 56
Βιβλιογραφία 60

Πίνακας σχημάτων

Εικόνα 1: Ο κύκλος ζωής ενός block στο Blockchain του Bitcoin. 20
Εικόνα 2: Διαφορά αποκεντρωμένου και μη συστήματος… 221
Εικόνα 3: Ethereum sharding model 25
Εικόνα 4: Παράδειγμα λειτουργίας του συστήματος 29
Εικόνα 5: Δομή της αποκεντρωμένης εφαρμογής 29
Εικόνα 6: Παράδειγμα ανάπτυξης συμβολαίου στο Remix IDE 30
Εικόνα 7: Το πορτοφόλι κρυπτονομισμάτων Metamask.....31
Εικόνα 8: Στιγμιότυπο από πλοήγηση στο συμβόλαιο στο Etherscan 32
Εικόνα 9: Υπογραφή συναλλαγής δημιουργίας του έξυπνου συμβολαίου. 39
Εικόνα 10: Επιβεβαίωση του πηγαίου κώδικα του συμβολαίου.....40
Εικόνα 11: Απεικόνιση ενός επιβεβαιωμένου συμβολαίου με δυνατότητες αλληλεπίδρασης Read/Write.....40
Εικόνα 12: Αρχικοποίηση πρώτου event 41
Εικόνα 13: Ενεργοποίηση των πωλήσεων 4141
Εικόνα 14: Δεδομένα που αντλεί ο ενδιαφερόμενος από το ίδιο το συμβόλαιο 42
Εικόνα 15: Αγορά ενός εισιτηρίου απευθείας από το έξυπνο συμβόλαιο 43
Εικόνα 16: Αναζήτηση και προβολή του NFT που μόλις αγοράσαμε. 43
Εικόνα 17: Προειδοποιητικό μήνυμα - Υπάρχει σφάλμα. 44
Εικόνα 18: Αδυναμία εκτέλεσης της συναλλαγής λόγω γνωστού λάθους.....45
Εικόνα 19: Εξουσιοδότηση του συμβολαίου. 45
Εικόνα 20: Ανάρτηση πώλησης του εισιτηρίου. 45
Εικόνα 21: Λήψη τιμής εισιτηρίου προς πώληση απευθείας από το συμβόλαιο.....46
Εικόνα 22: Λήψη κατάστασης εισιτηρίου απευθείας από το συμβόλαιο.....46
Εικόνα 23: Αγορά εισιτηρίου από secondary market μέσω του συμβολαίου. 47
Εικόνα 24: Η συναλλαγή αγοραπωλησίας και μεταφοράς κυριότητας. 47
Εικόνα 25: Τυχαία χρονική στιγμή με έσοδα στο συμβόλαιο 48
Εικόνα 26: Συλλογή εσόδων από το συμβόλαιο. 48
Εικόνα 27: Ο διοργανωτής μπορεί να θέσει ένα εισιτήριο ως χρησιμοποιημένο. 48
Εικόνα 28: Παράδειγμα ABI έξυπνου συμβολαίου. 49
Εικόνα 29: Αρχική σελίδα του frontend. 50
Εικόνα 30: Εμφάνιση στατιστικών εκδήλωσης. 51
Εικόνα 31: Αδυναμία πρόσβασης στην εκδήλωση δίχως NFT εισιτήριο. 51
Εικόνα 32: Αγορά εισιτηρίου με το κλικ κουμπιού. 52
Εικόνα 33: Πρόσβαση στο κλειδωμένο περιεχόμενο.....52

Κεφάλαιο 1: Εισαγωγή

1.1 Κίνητρο

Τάσσομαι ιδιαίτερα υπέρ της τεχνολογίας του Blockchain και θεωρώ ότι ο κλάδος είναι ακόμα σε ιδιαίτερα πρώιμο στάδιο, με αποτέλεσμα η ενασχόληση και η δημιουργία στον τομέα να είναι εντυπωσιακή και ενδιαφέρουσα, αφού ακόμα ερευνώνται οι δυνατότητες που δύναται να προσφέρει. Πιστεύω ακράδαντα ότι στα επόμενα χρόνια ο τομέας θα αξιοποιείται με τρόπους που την παρούσα στιγμή δεν είμαστε σε θέση να φανταστούμε.
Είναι πράγματι, όμως, τόσο επαναστατικό αυτό που επέφερε η εφεύρεση του Bitcoin; Το σύστημα που επέφερε το Bitcoin είναι πλήρως αποκεντρωμένο. Ο αποκεντρωμένος τομέας, ή αλλιώς Web 3.0, αποτελεί φυσική εξέλιξη του σημερινού οικοσυστήματος του διαδικτύου, εξασφαλίζοντας χαρακτηριστικά διαφάνειας, εμπιστοσύνης που δεν βασίζεται σε πρόσωπα ή οργανισμούς και ανθεκτικότητας σε λογοκρισία και έλεγχο. Ο καλύτερος χαρακτηρισμός που βρήκα για το σύστημα του Blockchain είναι «Decentralized Brain», ένας αποκεντρωμένος δηλαδή και πλήρως αυτοτελής εγκέφαλος.
Το Bitcoin κατάφερε να κάνει το έως τότε αδύνατο δυνατό, κατάφερε να επιτρέψει στο άτομο Α να στείλει χρηματική αξία στο άτομο Β απευθείας, δίχως δηλαδή να χρειαστεί να μεσολαβήσει έλεγχος ή οποιουδήποτε είδους μεσάζοντας (τράπεζα). Το Bitcoin ως τεχνολογία μπορεί να προασπίσει τους ανθρώπους από ατασθαλίες κρατών, από υποτιμήσεις νομισμάτων, από φαινόμενα υπερπληθωρισμού. Το τελευταίο ισχύει επειδή ο μέγιστος συνολικός αριθμός Bitcoin είναι προκαθορισμένος σε αντίθεση με λόγου χάρη το δολάριο που η συνολική του ποσότητα εμπίπτει στην κρίση των κυβερνητών της Αμερικής.
Όλα τα παραπάνω μου κέντρισαν το ενδιαφέρουν και ήταν η αφορμή να αναζητήσω περισσότερες πληροφορίες και να αντλήσω γνώση για τον τομέα. Έτσι, θέλω να εκφράσω την ευγνωμοσύνη μου που μου δόθηκε η δυνατότητα να αναπτύξω το συγκεκριμένο θέμα που βασίζεται στις ευεργετικές επιδράσεις της αποκεντρωμένης τεχνολογίας καθώς μου διεύρυνε έμπρακτα τις θεωρητικές γνώσεις, τις οποίες χρησιμοποίησα για να δημιουργήσω ένα πλήρως αποκεντρωμένο σύστημα.

1.2 Σκοπός

Σκοπός της παρούσας διπλωματικής εργασίας είναι η δημιουργία μιας αποκεντρωμένης εφαρμογής που θα ικανοποιεί την πώληση εισιτηρίων πρόσβασης σε εκδηλώσεις. Μέσω της εφαρμογής αυτής οι χρήστες θα δύνανται σε επίπεδο peer-to-peer, χωρίς δηλαδή την ανάγκη ύπαρξης μεσάζοντα, να αγοράζουν καθώς και να πωλούν εισιτήρια πρόσβασης τα οποία θα έχουν την μορφή Non-Fungible Token (NFT).
Η εφαρμογή και η όποια αλληλεπίδραση μαζί της θα χαρακτηρίζεται από αμεσότητα και εμπιστοσύνη, αφού οι χρήστες θα μπορούν να μελετήσουν τον κώδικα που την απαρτίζει και να γνωρίζουν από πριν το αποτέλεσμα που θα συμβεί με κάθε αλληλεπίδραση. Η αμεσότητα και η εμπιστοσύνη θα διασφαλιστεί με χρήση του αποκεντρωμένου δικτύου του Ethereum, πάνω στο οποίο θα δημιουργηθεί και εκτελεστεί η εφαρμογή.

1.3 Οργάνωση του τόμου σε κεφάλαια

Η διπλωματική εργασία οργανώνεται σε ακριβώς 5 κεφάλαια. Το πρώτο κεφάλαιο αποτελεί εισαγωγικό κομμάτι και μία πρώτη επαφή με τον συγγραφέα, την κοσμοθεωρία του και τις φιλοδοξίες του όσον αφορά το τι επιχειρεί να καταφέρει με την εργασία. Στο δεύτερο κεφάλαιο αναλύονται θεωρητικές έννοιες γύρω από τα κρυπτονομίσματα και την τεχνολογία Blockchain, προκειμένου ο αναγνώστης να αποκτήσει τα απαραίτητα εφόδια και να είναι σε θέση να εμπεδώσει εις βάθος το τελικό δημιούργημα. Στο τρίτο κεφάλαιο αναλύονται ενδελεχώς οι οντότητες της εφαρμογής, ο κώδικας που τις απαρτίζει και τα εργαλεία που χρησιμοποιήθηκαν για την δημιουργία της. Στο τέταρτο κεφάλαιο παρουσιάζονται στιγμιότυπα πρακτικής χρήσης της εφαρμογής, τόσο με απευθείας αλληλεπίδραση με το αποκεντρωμένο δίκτυο όσο και μέσω front-end εφαρμογής. Στο πέμπτο και τελευταίο κεφάλαιο γίνεται αναφορά στα συμπεράσματα που απορρέουν από την ανάπτυξη της εν λόγω αποκεντρωμένης εφαρμογής, σε μελλοντικές επεκτάσεις της και σε περιπτώσεις που θα μπορούσε η εφαρμογή να αξιοποιηθεί στον πραγματικό κόσμο.

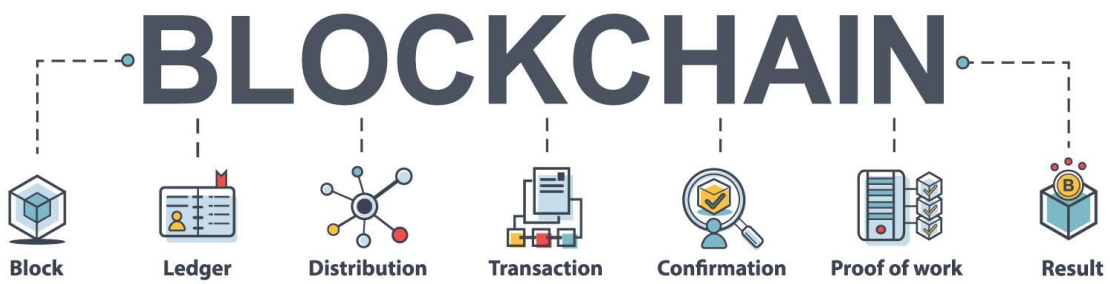
Κεφάλαιο 2: Γενικές πληροφορίες για το Blockchain

2.1 Εισαγωγή

Τα κρυπτονομίσματα είναι ψηφιακά νομίσματα που εξασφαλίζουν την ακεραιότητα τους με χρήση κρυπτογραφίας. Αναλυτικότερα, τα κρυπτονομίσματα είναι αποκεντρωμένα, δηλαδή δεν ελέγχονται από καμία κεντρική αρχή και έτσι θεωρούνται ασφαλή από κυβερνητικές χειραγωγήσεις ενώ ταυτόχρονα παραμένει αδύνατη τόσο η πλαστογράφηση τους όσο και το double spending problem (Να αποσταλεί δηλαδή δύο φορές το ίδιο ποσό ενώ εξαντλήθηκε από την πρώτη συναλλαγή).
Το Bitcoin είναι το πρώτο, πραγματικά αποκεντρωμένο και ανοιχτού κώδικα κρυπτονόμισμα που έλυσε το περιβόητο "double spending problem" χωρίς την ανάγκη τρίτου μεσάζοντα. Η επαναστατική μέθοδος που βασίστηκε το Bitcoin είναι η διανομή του απαραίτητου Ledger («βιβλίου» συναλλαγών) σε όλους τους χρήστες του δικτύου. Το δίκτυο του Bitcoin είναι peer-to-peer (ομότιμο), δηλαδή επιτρέπει σε πολλούς υπολογιστές να μοιράζονται τους πόρους ισοδύναμα και κάθε συναλλαγή πάνω του καταγράφεται στο δημόσιο Ledger που καλείται Blockchain. Όλες οι νέες συναλλαγές αφού ελεγχθούν ότι ικανοποιούν τις προϋποθέσεις (δηλαδή ότι υπάρχουν τα διαθέσιμα Bitcoin που πρόκειται να αποσταλλούν) επικυρώνονται από τους miners και εισάγονται στο Blockchain. Οι miners είναι αυτοί οι οποίοι αποτελούν μια αποκεντρωμένη αρχή που διασφαλίζει την ασφάλεια και την αξιοπιστία του δικτύου του Bitcoin.
Τα κρυπτονομίσματα επιτρέπουν απευθείας ψηφιακές συναλλαγές, καταργώντας την ανάγκη μεσάζοντα και κάθε χρονικό περιορισμό. Βέβαια, όπως θα δούμε και στη συνέχεια, η χρήση τους δεν περιορίζεται μόνο σε αυτό. Η ανάγκη για μεσάζοντα στην μεταφορά αξίας από ένα άτομο σε ένα άλλο εξαλείφεται αφού για οποιαδήποτε μεταφορά αρκεί ο ίδιος ο αποστολέας χρήστης να εγκρίνει ή αλλιώς «υπογράψει» την συναλλαγή με χρήση κρυπτογραφίας (sign the transaction). Αυτή η υπογραφή λαμβάνεται ως έγκυρη χάρη στο ιδιωτικό κλειδί του πορτοφολιού που γνωρίζει μόνο ο χρήστης που την πραγματοποιεί και έτσι κάθε χρήστης και μόνο αυτός έχει πλήρη έλεγχο των κρυπτονομισμάτων του. Είναι αδύνατο να γίνει οποιαδήποτε εξωτερική παρέμβαση τρίτου δίχως το ιδιωτικό κλειδί.
Αυτή η ειδοποιός διαφορά του οικονομικού συστήματος των κρυπτονομισμάτων είναι ύψιστης σημασίας σε χώρες όπου οι πολίτες δεν μπορούν να εμπιστευτούν τις κυβερνήσεις και τα χρηματοπιστωτικά ιδρύματα τους. Παρ' όλα αυτά, η απουσία μεσάζοντα πέρα από την εξάλειψη του κινδύνου σφετερισμού των περιουσιακών στοιχείων, μειώνει επίσης σε μεγάλο βαθμό το κόστος αποστολής μίας συναλλαγής ενώ σε κρυπτονομίσματα που υποστηρίζουν τα λεγόμενα έξυπνα συμβόλαια προσφέρονται πολύ ελκυστικές επιστροφές σε προσφορά (δανεισμό) κεφαλαίου επειδή ακριβώς το κόστος συντήρησης του πρωτοκόλλου είναι αμελητέο και ο κάθε συμμετέχων καρπώνεται όλο το κέρδος που στις παραδοσιακές υπηρεσίες θα το συσσώρευαν οι οικονομικοί κολοσσοί (τράπεζες).

2.2 Τι είναι το Blockchain

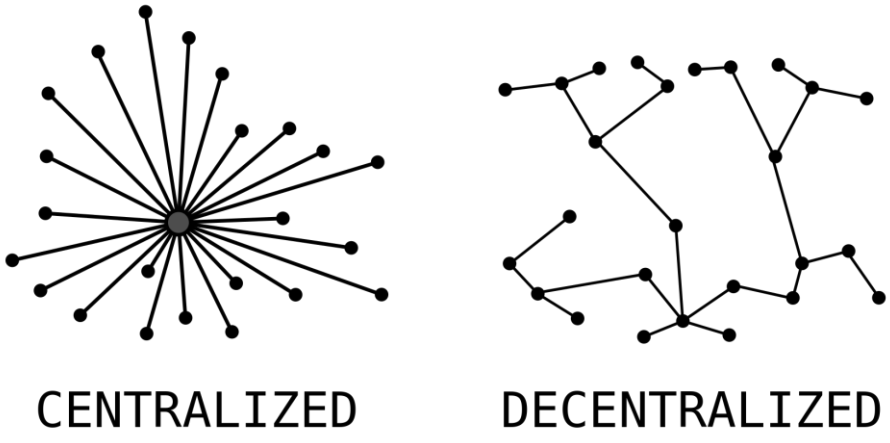
Ο όρος Blockchain αρχικά χρησιμοποιήθηκε για να περιγραφεί το κατανεμημένο Ledger, δηλαδή το «βιβλίο» συναλλαγών, του Bitcoin. Συνεπώς, ένα Blockchain συγκεντρώνει το ιστορικό συναλλαγών και ομαδοποιεί τα δεδομένα κατάλληλα σε Blocks, τα οποία μόλις γεμίσουν σε χώρο, επιβεβαιώνονται ως προς την εγκυρότητα τους από τους miners και πλέον ως έγκυρα συνδέονται με το προηγούμενο (χρονικά) Block σχηματίζοντας μία ατέρμονη αλυσίδα με πληροφορίες. Πολλές μετέπειτα αποκεντρωμένες τεχνολογίες που βασίστηκαν στο μοντέλο του Bitcoin, χρησιμοποιήσαν βιβλίο συναλλαγών με αποτέλεσμα η έννοια «Blockchain» να διευρυνθεί, διατηρώντας ωστόσο συγκεκριμένα χαρακτηριστικά κοινά.
Το βασικότερο χαρακτηριστικό που μοιράζονται όλα τα Blockchain είναι η χρήση ενός peer-to-peer (ομότιμου) δικτύου. Εν συνεχεία, κρίνεται αδήριτη η ανάγκη ύπαρξης ενός μηχανισμού συναίνεσης, ώστε οι όλοι οι κόμβοι του συστήματος να συναινούν με τα κοινόχρηστα δεδομένα. Αναλυτικότερα, η συμφωνία αυτή επιτυγχάνεται με κανόνες ενσωματωμένους στον κώδικα του λογισμικού που εκτελείται από τους κόμβους. Με τους κανόνες αυτούς οι κόμβοι του αποκεντρωμένου δικτύου παραμένουν συγχρονισμένοι και συναινούν με τα κοινόχρηστα δεδομένα. Με τον όρο κοινόχρηστα δεδομένα αναφερόμαστε στα δεδομένα που αποθηκεύονται εντός του Blockchain, τα οποία έχουν επαληθευτεί ως προς την εγκυρότητα. Τα δεδομένα αυτά απαρτίζονται από όλες τις συναλλαγές που έχουν πραγματοποιηθεί στο δίκτυο. Χαρακτηριστικό κάθε Blockchain είναι πως κάθε μεταγενέστερη εγγραφή δεδομένων συνδέεται άρρηκτα με χρονικά προγενέστερη (δημιουργία συνδεδεμένης αλυσίδας).
Η ασφάλεια του συστήματος έγκειται στο γεγονός πως οποιαδήποτε τροποποίηση προγενέστερης εγγραφής συνεπάγεται και την αλλαγή κάθε χρονικά μεταγενέστερης εγγραφής, αλλιώς θα υπάρξουν αναντιστοιχίες στις ψηφιακές υπογραφές που είναι ενσωματωμένες στα δεδομένα. Τα Blockchain είναι αποκεντρωμένα αλλά όχι πλήρως αμετάβλητα. Για να εφαρμοστεί οποιαδήποτε μεταβολή στην δομή δεδομένων ενός Blockchain πρέπει η πλειονότητα των κόμβων να την αποδεχτεί προκειμένου να καθιερωθεί ως η νέα πραγματικότητα (το ακριβές ποσοστό πλειοψηφίας που απαιτείται διαφέρει από Blockchain δίκτυο σε Blockchain δίκτυο).
Όλα τα παραπάνω χαρακτηριστικά εντοπίζονται στο Blockchain του Bitcoin. Μερικές διαφορές που παρατηρούνται σε νεότερα μοντέλα Blockchain είναι στον μηχανισμό συναίνεσης, λόγου χάρη αν επιτρέπεται σε οποιονδήποτε χρήστη να μετέχει ενεργά στην επαλήθευση της αλυσίδας ή αν ο έλεγχος γίνεται μόνο από επιλεγμένους χρήστες.



Εικόνα 1: Ο κύκλος ζωής ενός block στο Blockchain του Bitcoin.

2.3 Γιατί είναι σημαντική η αποκέντρωση και παραδείγματα αξιοποίησης

Χάρη στα αποκεντρωμένα συστήματα καταργείται τόσο η ύπαρξη ενός ενιαίου μέρους αποθήκευσης των δεδομένων όσο και η αποκλειστική ευθύνη του συστήματος σε έναν μόνο οργανισμό. Τα κρυπτονομίσματα αποτελούν την πρώτη και έως σήμερα μοναδική μορφή αποκεντρωμένης χρηματικής αξίας. Ωστόσο, ενώ η πλειονότητα των κρυπτονομισμάτων είναι αποκεντρωμένα δεν είναι κανόνας ότι κάθε κρυπτονόμισμα είναι αποκεντρωμένο.
Αναγκαία συνθήκη για την αποκέντρωση ενός κρυπτονομίσματος είναι η χρήση της τεχνολογίας Blockchain, δηλαδή ενός αποκεντρωμένου δικτύου, όπου χρήστες από όλη την υφήλιο δύνανται να μετέχουν ενεργά και να επικυρώνουν τα δεδομένα του. Με τα κρυπτονομίσματα οι άνθρωποι για πρώτη φορά έχουν πλήρη ιδιοκτησία και ελευθερία διαχείρισης των χρημάτων τους ενώ η ασφάλεια του δικτύου έγκειται στο ότι είναι αδύνατη η αποτελεσματική επίθεση σε ένα σημείο/κόμβο αφού το σύστημα δεν έχει κανένα μεμονωμένο τρωτό σημείο.
Αποτελεί αδιαμφισβήτητο γεγονός ότι ο χώρος των κρυπτονομισμάτων διαρκώς εξελίσσεται, διευρύνεται και ικανοποιεί ολοένα και περισσότερες ανθρώπινες ανάγκες βέλτιστα και αποτελεσματικά. Ειδικότερα, δίχως την ανάγκη για ακριβή εμπιστοσύνη και ασφάλεια και σε συνδυασμό με την απόλυτη διαφάνεια των συναλλαγών στο δίκτυο τα κρυπτονομίσματα ενδείκνυνται για παροχή φιλανθρωπικής υποστήριξης, πόσο μάλλον σε περιόδους παγκόσμιων συρράξεων και περιορισμών. Όμοια οφέλη μπορούν να παρατηρηθούν στην εφοδιαστική αλυσίδα όπου η εμπιστοσύνη αποτελεί αδήριτη ανάγκη και δεν είναι εύκολο να επιβεβαιωθεί. Η τεχνολογία Blockchain είναι εφικτό να διαχειρίζεται όλη την διαδικασία εφοδιασμού, από την δημιουργία, τη διανομή έως και την τελική παράδοση των αγαθών. Εν συνεχεία, τα χαρακτηριστικά της αποκεντρωμένης τεχνολογίας ευνοούν και άλλες πτυχές του ανθρώπινου βίου, όπως διακυβερνητικές λειτουργίες, εξασφαλίζοντας το αναλλοίωτο εκλογών, την εγκυρότητα ταυτότητας καθώς και δικαιώματα πρόσβασης (εξάλειψη πειρατείας).



Εικόνα 2: Διαφορά αποκεντρωμένου και μη συστήματος.

2.4 Πορτοφόλι κρυπτονομισμάτων

Τα κρυπτονομίσματα αποθηκεύονται σε ειδικά πορτοφόλια και όχι σε κεντρικά ανταλλακτήρια (centralized exchanges). Ειδικότερα, αυτά τα πορτοφόλια είναι ψηφιακά, βρίσκονται πάνω στο Blockchain και είναι προσβάσιμα από κάθε συσκευή με πρόσβαση στο διαδίκτυο, εξασφαλίζουν την ασφάλεια των συναλλαγών με χρήση κρυπτογραφίας και διατηρούν «κρυφό» το απόρρητο του χρήστη.
Η δημιουργία ενός αποκεντρωμένου πορτοφολιού ήταν, είναι και θα παραμείνει δωρεάν. Κατά τη δημιουργία σχηματίζονται για κάθε πορτοφόλι ένα δημόσιο και ένα ιδιωτικό κλειδί (public & private key). Το δημόσιο κλειδί είναι το αναγνωριστικό του πορτοφολιού, αυτό δηλαδή το οποίο θα χρησιμοποιηθεί για να γίνει οποιαδήποτε αποστολή κρυπτονομισμάτων προς τον χρήστη ή να αναζητηθεί το ιστορικό συναλλαγών του. Από την άλλη πλευρά, το ιδιωτικό κλειδί είναι αυστηρά απόρρητο, αφού η γνωστοποίηση του επιτρέπει την επέμβαση ξένου χρήστη και τον σφετερισμό των περιεχομένων του πορτοφολιού. Σε αυτό το σημείο πρέπει να τονιστεί ότι εφόσον το πορτοφόλι βρίσκεται αποκλειστικά πάνω στο Blockchain, είναι προσβάσιμο και ανακτήσιμο ανά πάσα στιγμή από μία σειρά (αυστηρή) απλών λέξεων (είθισται να είναι από 12 έως 24 λέξεις) που ονομάζεται “seed phrase”. Από αυτές ακριβώς τις λέξεις (οι οποίες δεν είναι κάτι άλλο από μία αναπαράσταση τυχαίων αριθμών) προκύπτει και το ιδιωτικό κλειδί του πορτοφολιού που είναι απαραίτητο για οποιαδήποτε εξερχόμενη συναλλαγή.

2.5 Τι είναι τα Έξυπνα Συμβόλαια, τα Dapps και το DeFi

Η εφεύρεση του Bitcoin ήταν επαναστατική και προλείανε το έδαφος για τεχνολογικά θαύματα στον αποκεντρωμένο χώρο. Ένα από αυτά ήταν η ιδέα και υλοποίηση των έξυπνων συμβολαίων, αρχικά από το Ethereum. Με τα έξυπνα συμβόλαια τα κρυπτονομίσματα επαλήθευσαν και καθιέρωσαν πως δεν αποτελούν ένα απλό μέσο συναλλαγής αλλά ότι είναι εγγενώς προγραμματίσιμο χρήμα.
Τα έξυπνα συμβόλαια (smart contracts) είναι σύνθετες συναλλαγές και λειτουργούν διότι όλα τα στοιχεία της επιμέρους συναλλαγής είναι πλήρως ψηφιοποιημένα, αποθηκευμένα και επαληθεύσιμα από το Blockchain. Επειδή τα Smart Contracts είναι όσο σωστά όσο ο κώδικας που τα διέπει, τα προγραμματιστικά σφάλματα μπορούν να αποβούν καταστρεπτικά αλλά και αντιστρόφως ο ορθός κώδικας εγγυάται το ζητούμενο αποτέλεσμα κάθε φορά.
Τα έξυπνα συμβόλαια χρησιμοποιούν ψηφιακές υποσχέσεις πάνω στο αποκεντρωμένο πρωτόκολλο και έτσι δύνανται να επιτελέσουν τόσο οικονομικές λειτουργίες όσο και λειτουργίες περί εφαρμογής κανόνων, ταυτοποίησης και ενοικίασης. Με τα έξυπνα συμβόλαια προέκυψε ένα νέο είδος αξιοποίησης της προγραμματίσιμης αποκεντρωμένης τεχνολογίας, τα Dapps (Decentralized Applications). Οι αποκεντρωμένες εφαρμογές (Dapps) σε αντίθεση με τις παραδοσιακές εφαρμογές του διαδικτύου υποστηρίζονται από αποκεντρωμένα και αμετάβλητα δίκτυα Blockchain. Αυτή η ουσιαστική διαφορά σε σχέση με τις παραδοσιακές εφαρμογές είναι που καθιστά τις αποκεντρωμένες ασταμάτητες, ανεμπόδιστες και ανεπηρέαστες. Οι αποκεντρωμένες εφαρμογές είθισται να είναι ανοικτού κώδικα (open source), προκειμένου να εμπνέουν εμπιστοσύνη στους

χρήστες μιας και οι συναλλαγές στο Blockchain είναι μη αναστρέψιμες και με αυτόν τον τρόπο δίδεται στον χρήστη η δυνατότητα να μελετήσει τον κώδικα της εφαρμογής προτού προβεί στην χρήση της. Υπάρχουν πολλών ειδών αποκεντρωμένες εφαρμογές, ιδιαίτερο ενδιαφέρον δε παρουσιάζουν οι αποκεντρωμένες εφαρμογές οικονομικών (Decentralized Finance).
Η αποκεντρωμένη οικονομία αποσκοπεί στην δίκαιη και αμερόληπτη διαχείριση των οικονομικών, καταργώντας τις κεντροποιημένες και αισχροκερδείς παραδοσιακές υπηρεσίες. Με βάση την peer-to-peer εμπιστοσύνη των αποκεντρωμένων συστημάτων καθίστανται εφικτές όλων των ειδών οι χρηματοοικονομικές υπηρεσίες: Από απλές συναλλαγές μεταφοράς αξίας, χρήση δανείων με υποθήκη κρυπτονομίσματα, προσφορά κεφαλαίου για επιτόκια δανεισμού έως και πιο σύνθετες οικονομικές συμφωνίες.

2.6 Τι είναι το Ethereum

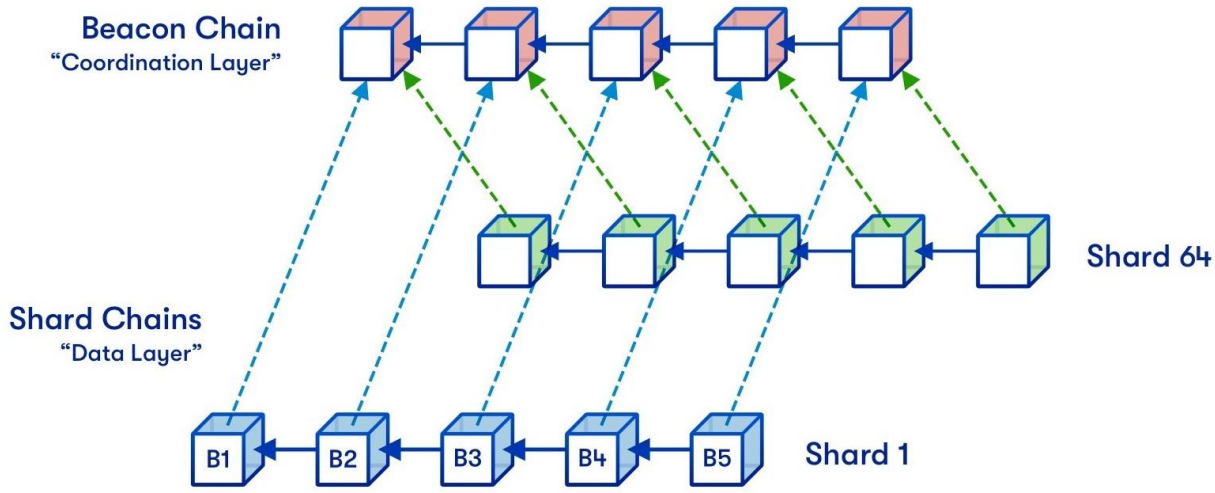
Το Ethereum αποτελεί το δεύτερο μεγαλύτερο σε κεφαλαιοποίηση κρυπτονόμισμα, δημιουργήθηκε το 2015 και σε αντίθεση με το Bitcoin δεν αποτελεί μόνο μορφή ψηφιακού χρήματος. Αναλυτικότερα, οι ιδρυτές του Ethereum αποσκοπούσαν στη δημιουργία μίας παγκόσμιας αποκεντρωμένης πλατφόρμας που να καρπώνεται τα οφέλη και την ασφάλεια της τεχνολογίας Blockchain. Πράγματι, μπορεί σήμερα ο οποιοσδήποτε να χρησιμοποιήσει το Ethereum, του οποίου το λογισμικό είναι ανοικτού κώδικα, για να δημιουργήσει οτιδήποτε κωδικοποιημένο, ασφαλές και αποκεντρωμένο.
Ενώ το Ethereum αποτελεί δημοφιλή επένδυση και μέσο αποθήκευσης αξίας, επαναστατικό χαρακτηριστικό του αποτελεί η δυνατότητα δημιουργίας έξυπνων συμβολαίων και κατ' επέκταση εφαρμογών σε αυτό. Ειδικότερα, κάθε χρήστης του δικτύου μπορεί με προγραμματισμό να αναπτύξει σύνθετες εφαρμογές για τις οποίες είναι βέβαιος ότι θα λειτουργούν ακριβώς όπως τις προγραμμάτισε δίχως να ελλοχεύει ο κίνδυνος διακοπής λειτουργίας ή παρέμβασης. Σε αυτό κρίνεται επιτακτική η ανάγκη διαχωρισμού του Ethereum και του Ether (ticker: ETH). Με τον όρο Ethereum αναφερόμαστε στο ίδιο το αποκεντρωμένο δίκτυο που είναι προγραμματίσιμο και υποστηρίζει την πληθώρα λειτουργιών που έχουμε ήδη επισημάνει. Από την άλλη πλευρά, το Ether (ελληνικά: αιθέρας) είναι το νόμισμα που χρησιμοποιείται στο δίκτυο για την διενέργεια οποιασδήποτε συναλλαγής. Ο αιθέρας ως μέσο συναλλαγής και αποθήκευσης αξίας λειτουργεί όμοια με το Bitcoin. Η ειδοποιός διαφορά εντοπίζεται στην χρήση του ως κινητήριο καύσιμο των έξυπνων συμβολαίων και κατ' επέκταση ολόκληρου του δικτύου, αφού όλες οι πληρωμές γίνονται με αυτό. Η προστασία των συναλλαγών με αιθέρα διασφαλίζεται από το δίκτυο του Ethereum, όπως ακριβώς διασφαλίζονται και οι συναλλαγές με Bitcoin στο δικό του δίκτυο, με τεράστια ποσά υπολογιστικής ισχύος που δαπανούνται συνολικά από τους κόμβους που επαληθεύουν την εγκυρότητα των συναλλαγών.
Ενώ το δίκτυο του Ethereum θεωρείται ασφαλές λόγω του λογισμικού ανοικτού κώδικα, όπου τυχόν τρωτά σημεία θα είχαν ανακαλυφθεί, οι εφαρμογές που εκτελούνται πάνω στο δίκτυο του δεν έχουν σε καμία περίπτωση συγκρίσιμο βαθμό ασφαλείας παρόλο που μπορεί είναι ανοικτού κώδικα και αυτό οφείλεται στον σημαντικά μικρότερο βαθμό μελέτης και επαλήθευσης λειτουργίας του κώδικα που τις διέπει. Μάλιστα, το πρωτόκολλο του δικτύου του Ethereum διαρκώς εξελίσσεται και έχουν δρομολογηθεί ριζικές αλλαγές (Ethereum 2.0) προκειμένου να

εξασφαλίσουν ένα ασφαλέστερο, τάχιστο και οικονομικό αποκεντρωμένο δίκτυο. Ενώ το Blockchain του Bitcoin παρομοιάζεται με ένα λογιστικό βιβλίο, το Blockchain του Ethereum είναι ασύγκριτα πιο προγραμματίσιμο και ικανό να υποστηρίξει πληθώρα καινοτόμων υπηρεσιών.
Αυτό καθίσταται εφικτό επειδή το Ethereum χρησιμοποιεί μία εικονική μηχανή (Ethereum Virtual Machine ή EVM) για να εξασφαλίσει την προγραμματισιμότητα του. Θα παρομοιάζαμε το EVM με έναν γιγάντιο και παγκόσμιο υπολογιστή που απαρτίζεται από πλήθος μεμονωμένων υπολογιστών με κοινό παρονομαστή τους το ίδιο λογισμικό του Ethereum.

2.7 Μειονεκτήματα του Ethereum και το Ethereum 2.0

Το Ethereum είναι, κατά τη στιγμή συγγραφής του τόμου, με διαφορά η πιο διαδεδομένη πλατφόρμα έξυπνων συμβολαίων. Ακριβώς αυτή η υπέρογκη χρήση της πλατφόρμας προκαλεί συχνά συμφόρηση του δικτύου, αυξάνοντας εκθετικά το κόστος συναλλαγής και τη κατανάλωση της ηλεκτρικής ενέργειας του δικτύου. Παράλληλα, ελλοχεύει ο κίνδυνος πλήρους απώλειας μιας συναλλαγής, δηλαδή να μην συμπεριληφθεί ποτέ σε Block, να λήξει και να θεωρηθεί άκυρη, ενώ δαπανήθηκαν τέλη συναλλαγής, πολλές φορές μεγαλύτερα σε αριθμό από το ποσό που η ίδια μεταφέρει.
Το Ethereum 2.0 είναι η μεγαλύτερη και πολύ-αναμενόμενη αναβάθμιση του δικτύου του Ethereum που σκοπεύει να επιλύσει όλες τις αρνητικές πτυχές του. Συγκεκριμένα, στοχεύει να μεγιστοποιήσει την ταχύτητα και την απόδοση (network throughput), διατηρώντας τα υψηλά επίπεδα ασφαλείας και ελαχιστοποιώντας τον ενεργειακό αντίκτυπο. Χαρακτηριστικό της αναβάθμισης είναι η ριζική αλλαγή του μηχανισμού συναίνεσης του δικτύου, μία κίνηση τολμηρή και δύσκολη, αφού ο μηχανισμός συναίνεσης είναι το σημαντικότερο χαρακτηριστικό ενός αποκεντρωμένου συστήματος. Αναλυτικότερα, ο αλγόριθμος συναίνεσης Proof-of-Work (PoW) θα αντικατασταθεί από τον αλγόριθμο Proof-of-Stake (PoS), ο οποίος είναι σημαντικά ταχύτερος, απίστευτα πιο οικονομικός και δίχως (θεωρητικά τουλάχιστον) να θυσιάζεται η ασφάλεια του δικτύου.
Ο αλγόριθμος συναίνεσης PoS δεν συναντάται μόνο στην αναβάθμιση του δικτύου του Ethereum αλλά και σε πολλά κρυπτονομίσματα τρίτης γενιάς, καθώς τον προτιμούν από τον PoW αλγόριθμο. Με τον αλγόριθμο αυτόν αντικαθίστανται ουσιαστικά οι miners, οι οποίοι δαπανούσαν υπολογιστική ισχύ προκειμένου να λύσουν πρώτοι το μαθηματικό πρόβλημα, με τους λεγόμενους επικυρωτές (validators), οι οποίοι κληρώνονται τυχαία να επιβεβαιώσουν τις συναλλαγές ενός Block και να λάβουν την ανταμοιβή που αντιστοιχεί σε Ether.
Στην πραγματικότητα, το Ethereum 2.0 υπάρχει ήδη από τις αρχές του 2021 και λειτουργεί παράλληλα με το κύριο δίκτυο (Beacon Chain). Φυσικά, δεν είναι έτοιμο αλλά όταν ολοκληρωθεί και δοκιμαστεί εκτενώς τα δύο υπάρχοντα blockchain θα συγχωνευτούν σε ένα ενιαίο (Merge). Άπαξ και ολοκληρωθεί η διαδικασία συνένωσης των δύο αλυσίδων και έχει επιτυχώς αλλάξει ο αλγόριθμος συναίνεσης σε PoS, μεγάλο ενδιαφέρον παρουσιάζει το επόμενο βήμα αναβάθμισης που ονομάζεται «θρυμματισμός» (Sharding).
Το Sharding αποτελεί δημοφιλή λύση (επιπέδου 1) στο πρόβλημα της κλιμακωσιμότητας ενός αποκεντρωμένου δικτύου. Με την τεχνική του Sharding, όπως προδίδει και το όνομα, ο έλεγχος και η επιβεβαίωση των συναλλαγών ανατίθεται σε πολλά μικρότερα κομμάτια, πετυχαίνοντας κατ’ αυτόν τον τρόπο

κατανομή του φορτίου σε περισσότερη (συνολικά) υπολογιστική ισχύ. Συγκεκριμένα, το Ethereum δίκτυο θα χωριστεί σε συνολικά εξήντα τέσσερις (64) αλυσίδες θραύσματα, με την κάθε μία να μπορεί να λειτουργεί ανεξάρτητα (σε ένα βαθμό), αφού θα έχει τοπικά αποθηκευμένα πλήθος των συνολικών δεδομένων.



Εικόνα 3: Ethereum sharding model.

2.8 Τι είναι τα NFTs

Ως Non-Fungible Token, ή αλλιώς NFT (ελληνικά: Μη εναλλάξιμο Κρυπτοπαραστατικό) ορίζεται οποιοδήποτε κρυπτογραφημένο στοιχείο που βασίζεται σε δίκτυο Blockchain και έχει μοναδικούς κωδικούς αναγνώρισης. Ενώ τα NFT στην σημερινή εποχή έχουν κυρίως συσχετιστεί αποκλειστικά με φωτογραφίες, στην πραγματικότητα τα κρυπτοπαραστατικά μπορεί να είναι οποιουδήποτε είδους ψηφιακό αρχείο και να παρέχουν ποικίλες λειτουργίες σε κατόχους λόγω των μεταδεδομένων που περιέχουν που τα καθιστούν πλήρως διαφοροποιήσιμα μεταξύ τους.
Η ιδιοκτησία ενός μη εναλλάξιμου κρυπτοπαραστατικού επαληθεύεται μοναδικά από το δίκτυο Blockchain στο οποίο δημιουργήθηκε. Ειδοποιός διαφορά μεταξύ των παραδοσιακών κρυπτονομισμάτων και των κρυπτοπαραστατικών είναι ότι τα πρώτα διαθέτουν δικό τους αυτόνομο Blockchain ενώ τα δεύτερα δημιουργούνται σε υπάρχον αποκεντρωμένο δίκτυο. Απαραίτητη προϋπόθεση ενός Blockchain για να μπορεί να υποστηρίξει την δημιουργία κρυπτοπαραστατικών είναι η προγραμματισιμότητα του. Απαιτείται δηλαδή το δίκτυο να υποστηρίζει τα λεγόμενα έξυπνα συμβόλαια (smart contracts) ή να δύνανται να δημιουργηθούν νομίσματα (εναλλάξιμα ή μη) πάνω του με εγγενή τρόπο.

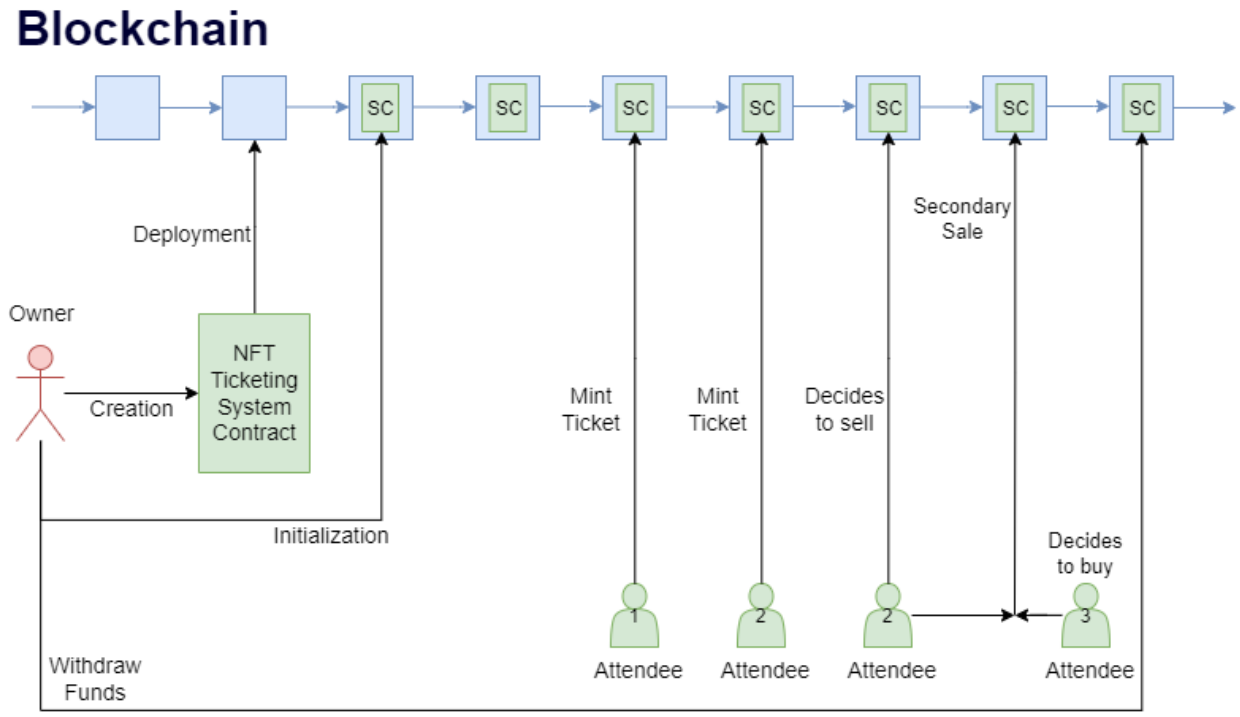
2.9 Γιατί τα NFTs προσελκύουν χρήστες

Η επαναστατική μορφή ιδιοκτησίας ψηφιακής τέχνης έχει προσελκύσει πλήθος νέων χρηστών. Τα αίτια της διαρκώς αυξανόμενης υιοθέτησης κρυπτοπαραστατικών είναι ποικίλα. Ιδιαίτερη έμφαση δίνεται, όμως, στην αναθεώρηση της έννοιας «ιδιοκτησία». Ειδικότερα, χάρη στην φύση των δικτύων Blockchain, ο ιδιοκτήτης ενός οποιουδήποτε NFT μπορεί πολύ εύκολα να αποδείξει ότι είναι ο πραγματικός ιδιοκτήτης ενός αυθεντικού κρυπτοπαραστατικού. Ακόμα, οι ιδιοκτήτες κρυπτοπαραστατικών μπορούν με ευκολία είτε να μεταφέρουν είτε να πουλήσουν οποιοδήποτε NFT τους ανήκει χρησιμοποιώντας αγορές (marketplaces) πάνω στο αποκεντρωμένο δίκτυο. Μάλιστα, μερικά marketplaces υποστηρίζουν και μεθόδους δημοπρασίας (auction houses) που καθιστούν την διαδικασία πώλησης πιο ενδιαφέρουσα.
Επειδή ακριβώς οποιαδήποτε συναλλαγή ενός NFT λαμβάνει χώρα πάνω στο Blockchain είναι και καθ' όλα διαφανής σαν διαδικασία, επαληθεύσιμη από όλους ενώ λόγω των μοναδικών κωδικών αναγνώρισης κάθε NFT μπορεί ο χρήστης με απλούς κανόνες να προστατευθεί από απομιμήσεις. Επιπρόσθετα, τα NFTs είναι επί το πλείστων εξ' ολοκλήρου αμετάβλητα, δηλαδή τα μεταδεδομένα που τα συνοδεύουν καθώς και η φωτογραφία που τα συνοδεύει είναι αδύνατο να επηρεαστούν ή τροποποιηθούν από κάποιον (ούτε από τον ίδιο τον δημιουργό).

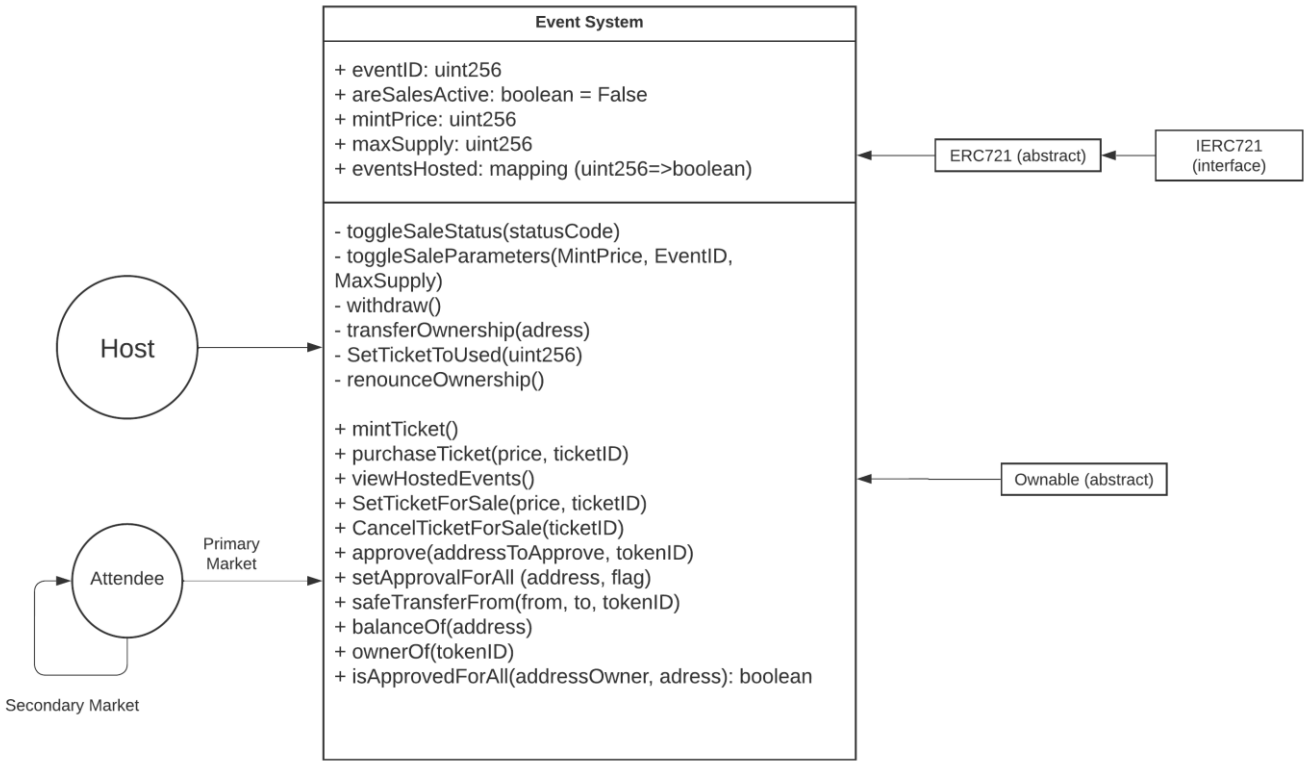
Κεφάλαιο 3: Υλοποίηση του NFT Ticketing System

3.1 Εννοιολογική ανάπτυξη της αποκεντρωμένης εφαρμογής

Στόχος μου είναι να δημιουργήσω μία πλήρη υποδομή αποκεντρωμένου Ticketing System που θα κάνει χρήση Non-Fungible Tokens, τα οποία θα αποτελούν εισιτήρια πρόσβασης για το εκάστοτε περιεχόμενο του διοργανωτή. Όντας NFT, το εισιτήριο κάθε πελάτη/attendee εφόσον αγοραστεί (γίνει "minted") από το έξυπνο συμβόλαιο θα ανήκει στον αγοραστή, ο οποίος θα διατηρεί πλήρη κυριότητα των δικαιώματων του για όσο το έχει στην κατοχή του. Συγχρόνως, λόγω της μοναδικότητας και της ευκολίας επαλήθευσης της εγκυρότητας ενός NFT είναι ιδιαίτερα απλή διαδικασία η πιστοποίηση των ατόμων που δικαιούνται πρόσβαση στο κλειδωμένο περιέχομενο του διοργανωτή. Ωστόσο, το έξυπνο συμβόλαιο δεν θα περιορίζεται μόνο στη δημιουργία NFT εισιτηρίων και την επικύρωση τους αλλά θα προσφέρει την δυνατότητα δευτερεύουσων πωλήσεων (secondary market sales), ασφαλείς μεταφορές εισιτηρίων (safe transfer), σύνθετη λογική (χρησιμοποιημένα ή όχι εισιτήρια, αύξων αριθμός εισιτηρίου και εκδήλωση που αναφέρονται), τροποποίηση κατάστασης πωλήσεων και αυτόματα και από τον διοργανωτή (αν το έξυπνο συμβόλαιο δρα αποκλειστικά για δευτερεύουσες πωλήσεις ή όχι, αν είναι ενεργό ή ανενεργό).



Εικόνα 4: Παράδειγμα λειτουργίας του συστήματος



Εικόνα 5: Δομή της αποκεντρωμένης εφαρμογής.

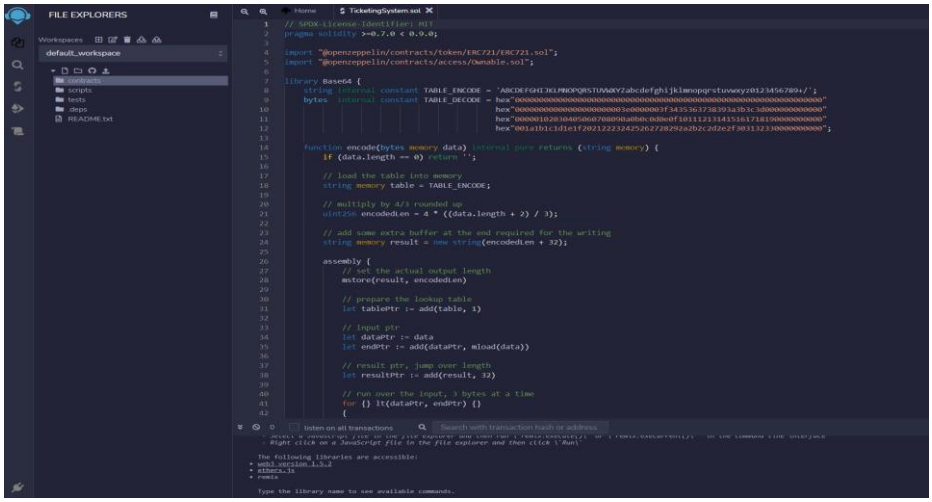
3.2 Εργαλεία ανάπτυξης της αποκεντρωμένης εφαρμογής

Το σύστημα θα είναι πλήρως αποκεντρωμένο και θα βασίζεται εξ' ολοκλήρου στην εγκυρότητα που διασφαλίζει η τεχνολογία του Blockchain. Συνεπώς, η λειτουργία της εφαρμογής θα είναι απρόσκοπτη από εξωγενείς παράγοντες και σε λογικά πλαίσια τροποποιήσιμη μόνο από τον διοργανωτή και ιδιοκτήτη του συμβολαίου, προκειμένου να υπάρχει εμπιστοσύνη και ασφάλεια των δικαιωμάτων κυριότητας των συμμετεχόντων.

Εφόσον η αποκεντρωμένη εφαρμογή θα αναπτυχθεί πάνω στο δίκτυο του Ethereum, κρίνεται απαραίτητη η εξοικείωση και χρήση της γλώσσας πρωγραμματισμού του. Αυτή ονομάζεται Solidity και είναι μία αντικειμενοστραφής και υψηλού επιπέδου γλώσσα προγραμματισμού. Μέσω αυτής θα προγραματίσουμε το ζητούμενο έξυπνο συμβόλαιο που θα αποτελέσει την «καρδιά» της αποκεντρωμένης και ασταμάτητης εφαρμογής. Στην Solidity ως αντικείμενα ορίζονται ολόκληρα τα έξυπνα συμβόλαια, ενώ είναι εξαιρετικής σημασίας η χρήση μόνο του ικανού και αναγκαίου κώδικα, καθώς προγραμμαστική περίσσεια συνεπάγεται αυξημένο κόστος καυσίμου για κάθε εκτέλεση λειτουργίας του συμβολαίου. Εν ολίγοις, δεν αρκεί μόνο η εφαρμογή να λειτουργεί ορθά αλλά και βέλτιστα, διότι χαρακτηριστικό ενός ικανού μηχανικού στον τομέα του Web 3.0 (δηλαδή του αποκεντρωμένου τομέα) είναι να εξασφαλίζει πρωτίστως εγκυρότητα αλλά και οικονομία στο κόστος εκτέλεσης των συμβολαίων του δικτύου.

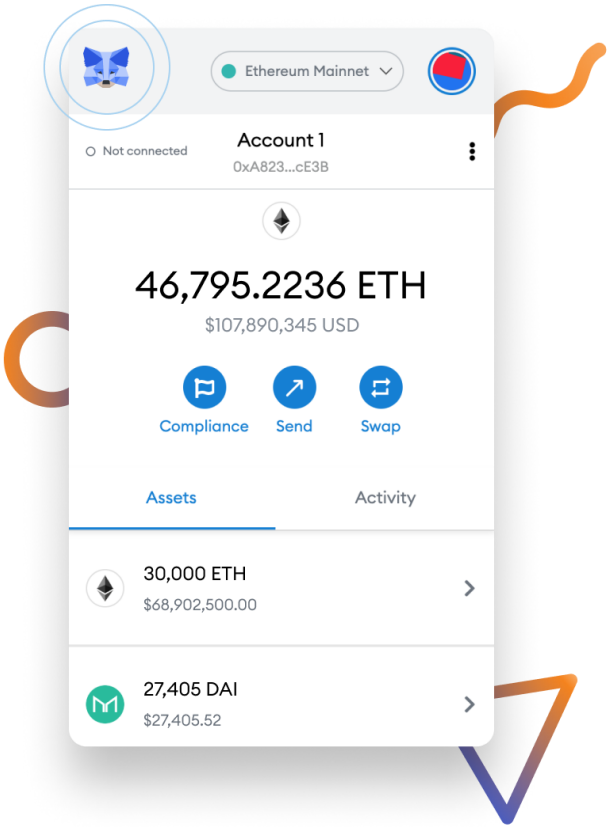
Αφού εξασφαλιστεί η εξοικείωση της γλώσσας προγραμματισμού του Ethereum και η συγγραφή του έξυπνου συμβολαίου, απομένει το τελικό βήμα του "deployment"

στο δίκτυο του Ethereum, δηλαδή της καταχώρησης του συμβολαίου στο Blockchain, όπου θα μείνει μόνιμα. Εξαιρετικά φιλικό για προγραμματιστές λόγω απλότητας και αποτελεσματικότητας είναι το Remix Project και το IDE (Integrated Development Environment) που προσφέρει. Μέσω αυτού θα γίνει τόσο η συγγραφή όσο και η μεταγλώττιση του συμβολαίου της εφαρμογής. Επιπρόσθετα, από το ίδιο το Remix IDE μπορεί να γίνει και το "deployment" στο δίκτυο του Ethereum αρκεί ο χρήστης και σύντομα ιδιοκτήτης του συμβολαίου να έχει δημιουργήσει πορτοφόλι κρυπτονομισμάτων στο Metamask και να διαθέτει επαρκή κρυπτονομίσματα να καλύψει το τέλος συναλλαγής.



Εικόνα 6: Στιγμιότυπο ανάπτυξης συμβολαίου στο Remix IDE.

Το Metamask δεν είναι η μοναδική και κατ' επέκταση ούτε η υποχρεωτική επιλογή πορτοφολιού. Είναι, ωστόσο, πολύ βολικό και φιλικό πορτοφόλι κρυπτονομισμάτων που ικανοποιεί πλήρως τις όποιες ανάγκες του συστήματος. Στα πλεονεκτήματα του συγκαταλέγονται μεταξύ άλλων η εύκολη πρόσβαση και σύνδεση σε αποκεντρωμένες εφαρμογές, η ευρεία υιοθέτηση του από την κοινότητα του Ethereum (που συνεπάγεται εύκολη επιλογή σύνδεσης σε πιθανές front-end υλοποιήσεις), το λιτό και συγχρόνως πλήρες UI (User Interface) και η δυνατότητα αλληλεπίδρασης με το δίκτυο του Ethereum χωρίς την ανάγκη εκτέλεσης πλήρες κόμβου στον υπολογιστή του χρήστη. Το Metamask αποτελεί plugin και η εγκατάσταση του μπορεί να γίνει σε όλους τους δημοφιλείς φυλλομετρητές ιστού. Δεν μπορεί να το τονιστεί αρκετά η σημασία της ασφαλούς διαφύλαξης του "seed phrase" κατά τη δημιουργία του/ενός πορτοφολιού. Πέρα από την προφανή απώλεια κεφαλαίου που θα υποστεί ο χρήστης σε περίπτωση μη διαφύλαξης της φράσης και μη δυνατότητας επαναφοράς του πορτοφολιού, θα χάσει και την πρόσβαση του ως ιδιοκτήτη στο συμβόλαιο που έχει δημιουργήσει.

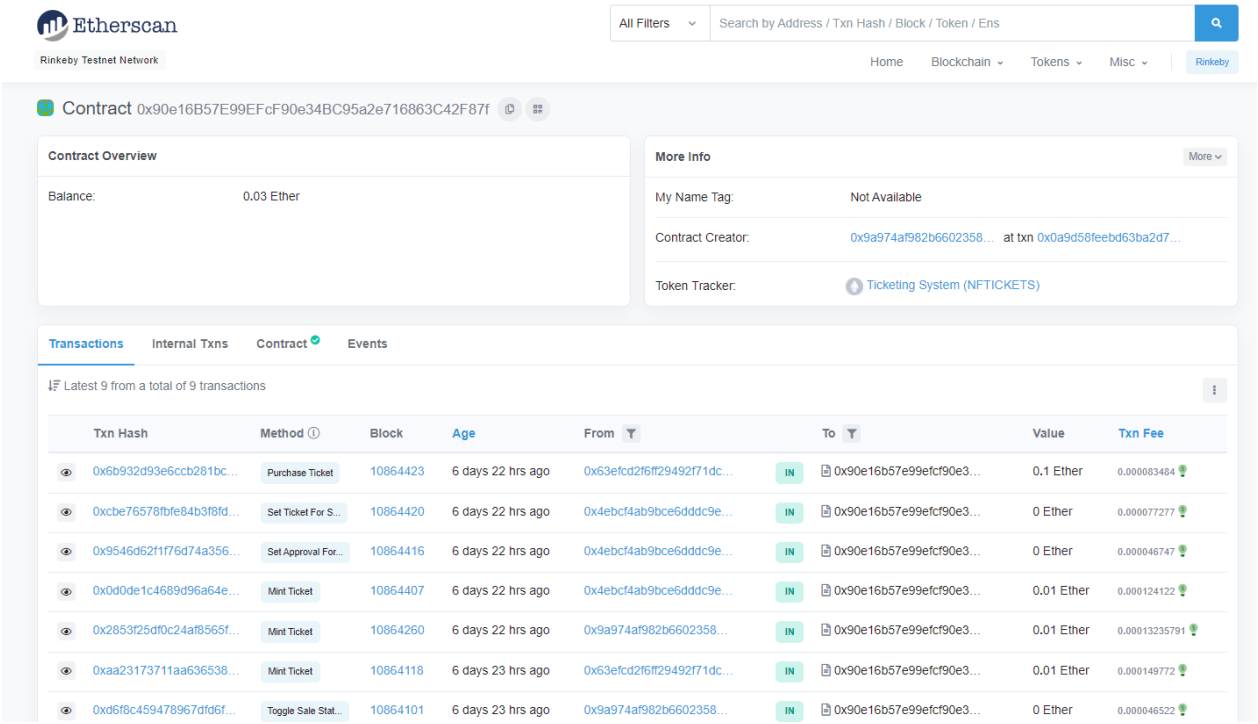


Εικόνα 7: Το πορτοφόλι κρυπτονομισμάτων Metamask.

Άπαξ και καταχωρηθεί το έξυπνο συμβόλαιο στο δίκτυο του Ethereum, μπορούμε να αλληλεπιδράσουμε μαζί του τόσο εμείς όσο και οποιοσδήποτε άλλος (εξ' ου και το νόημα του αποκεντρωμένου συστήματος) και να παρατηρήσουμε όλες τις συναλλαγές που σχετίζονται με αυτό με χρήση του Etherscan. Το Etherscan (χωρίς πάλι να αποτελεί υποχρεωτική επιλογή) είναι ένας βολικός εξερευνητής (Blockchain Explorer) του δικτύου του Ethereum που καταγράφει όλες τις συναλλαγές που πραγματοποιούνται στο δίκτυο. Επιτρέπει επίσης με βολικό τρόπο την σύνδεση σε Dapps μέσω του πορτοφολιού Metamask και την αλληλεπίδραση με έξυπνα συμβόλαια.

Αποτελεί πολύ καλή και ασφαλή τακτική η αλληλεπίδραση με έξυπνα συμβόλαια μέσω του Etherscan, διότι ενώ αρχικά μπορεί να μοιάζει πιο σύνθετη διαδικασία (από μερικά κλικ σε ένα έτοιμο και σίγουρα πιο εμφανίσιμο front-end) παρέχει στο χρήστη απαράμιλλη σιγουριά ότι αλληλεπιδρά με το σωστό έξυπνο συμβόλαιο, του οποίου μπορεί να επιβεβαιώσει τον κώδικα πρωτού προβεί σε οποιαδήποτε αλληλεπίδραση. Με λίγα λόγια, ο χρήστης πρωτού υπογράψει την όποια συναλλαγή, ως απόρροια αλληλεπίδρασης με κάποια συνάρτηση του συμβολαίου, μπορεί πρώτα να μελετήσει των κώδικα της. Όταν ένας χρήστης αλληλεπιδρά μέσω front-end όλη αυτή η διαδικασία είθισται να παραλείπεται και απλά να συναινεί με την υπογραφή του, θεωρώντας πως δεν θα υπάρξει θύμα εξαπάτησης. Ωστόσο, θυμίζουμε ότι όλες οι συναλλαγές σε ένα αποκεντρωμένο Blockchain είναι μη αναστρέψιμες, αφού δεν υπάρχει κάποια κεντρική αρχή να ανατρέξει το θύμα για υποστήριξη. Το παραπάνω αποτελεί κίνητρο για πολλούς κακόβολους και για αυτό γρήγορες και απερίσκεπτες αλληλεπιδράσεις στο δίκτυο οποιουδήποτε Blockchain δεν θα πρέπει να λαμβάνουν χώρα σε καμία περίπτωση και υπό καμία συνθήκη, όσο άξια εμπιστοσύνης και αν

είναι η ιστοσελίδα ή ο αρμόδιος φορεάς, διότι μέχρι και αυτές/αυτοί μπορούν να παραβιαστούν (όπως έχει συμβεί πολλές φορές στο παρελθόν).



Εικόνα 8: Στιγμιότυπο από πλοήγηση στο συμβόλαιο στο Etherscan.

3.3 Το έξυπνο συμβόλαιο της εφαρμογής

Σε αυτό το σημείο θα αναλύσουμε διεξοδικά τις κύριες συναρτήσεις και μεταβλητές που απαρτίζουν το έξυπνο συμβόλαιο του συστήματος μας. Φυσικά, όλο το συμβόλαιο και κατ' επέκταση και οτιδήποτε θα συμπεριληφθεί στο συγκεκριμένο σκέλος της διπλωματικής βρίσκονται αναρτημένα στο δίκτυο του Ethereum και συνεπώς είναι προσβάσιμα από οποιονδήποτε με πρόσβαση στο διαδίκτυο ανά πάσα στιγμή.

Α) Ξεκινώντας από τον διοργανωτή και ιδιοκτήτη του συμβολαίου:

Μόλις το συμβόλαιο γίνει deployed στο δίκτυο του Ethereum είναι ανενεργό, εφόσον η αρχικοποίηση του δεν θα έπρεπε να είναι υποχρεωτική μιας και εκπροσωπεί σύστημα εκδηλώσεων και όχι μία μεμονωμένη εκδήλωση. Όταν, λοιπόν, ο διοργανωτής το αποφασίσει δύναται να προβεί στην ενεργοποίηση του συμβολαίου, δηλαδή στην αρχικοποίηση των χαρακτηριστηκών της πρώτης εκδήλωσης (event). Η συνάρτηση που οφείλει να καλέσει είναι η toggleSaleParameters(), η οποία δέχεται ακριβώς τέσσερα ορίσματα: Αναγνωριστικό εκδήλωσης (Event ID), Πλήθος εισιτηρίων (Max Supply), Τιμή εισιτηρίου (Mint Price) και υπερσύνδεσμο εικόνας (Image URL, αφορά την ψηφιακή εικόνα που θα έχει το εισιτήριο).

```
function toggleSaleParameters(uint256 MintPrice_, uint256 Event_ID_, uint256 MaxSupply_, string memory ImageURL_) external onlyOwner {

    require(!areSalesActive, 'Can not change sale parameters on an active sale.');
    require(!EventsHosted[Event_ID_], 'An event with such an ID has already been hosted.');
    require(MaxSupply_ > 0, 'Please define an acceptable MaxSupply');
    require(Event_ID_ >= 0, 'Please define an acceptable Event ID');

    MintPrice = MintPrice_;
    Event_ID =  Event_ID_;
    MaxSupply = MaxSupply_;
    PrimarySale_SoldOut = false;
    EventsHosted[Event_ID_]=true;
    ImageURL= ImageURL_;
    counter_minted_per_event = 0;

}
```

Εύκολα διαπιστώνει κανείς την απανωτή χρήση της εντολής “require” τόσο στην συγκεκριμένη συνάρτηση όσο και σε σχεδόν κάθε συνάρτηση του συμβολαίου. Η εντολή κρίνεται απαραίτητη αφού ελέγχει αν ισχύει η εκάστοτε συνθήκη που της δίδεται ως όρισμα και μόνον τότε επιτρέπει την συνέχεια στην σειριακή εκτέλεση του κώδικα. Μάλιστα, σε περίπτωση που δεν τηρείται η συνθήκη θα επιστρέψει “error”, ο υπόλοιπος κώδικας δεν θα εκτελεστεί και η συναλλαγή θα γίνει “revert”.
Εν συνεχεία, αφού ο διοργανωτής θέσει τις απαραίτητες τιμές προκειμένου να οριστεί ορθά ένα event, μπορεί να ενεργοποιήσει τις πωλήσεις του συμβολαίου. Η συνάρτηση που οφείλει να καλέσει είναι η toggleSaleStatus(), η οποία δέχεται ακριβώς ένα όρισμα, έναν ακέραιο αριθμό που αποτελεί κωδικοποίηση κατάστασης. Για χάριν ευκολίας, για να ενεργοποιηθούν όλες οι πωλήσεις πρέπει να θέσει ως όρισμα τον αριθμό ένα (1). Κλήση της συνάρτησης με όρισμα τον αριθμό μηδέν (0) συνεπάγεται απενεργοποίηση του συμβολαίου ενώ κλήση με όρισμα τον αριθμό δύο (2) ή τρία (3) συνεπάγεται επέμβαση για αποκλειστικά δευτερογενείς πωλήσεις ή προσωρινή παύση των πωλήσεων του συμβολαίου αντίστοιχα.

```
function toggleSaleStatus(uint256 _StatusCode) external onlyOwner {

    require(_StatusCode >= 0 && _StatusCode < 4, 'No such state has been encoded');
    if (_StatusCode == 0) areSalesActive = false;
    else if (_StatusCode == 1) {
        areSalesActive = true;
        OnPause = false;
    }
    else if (_StatusCode == 2)  PrimarySale_SoldOut = true;
    else if (_StatusCode == 3) {
    OnPause = !OnPause;
    if (OnPause) areSalesActive = false;
    }

}
```

Επιπρόσθετα, ο διοργανωτής και μόνο αυτός έχει την δυνατότητα να θέσει κάποιο εισιτήριο σε χρησιμοποιημένο (used), αρκεί φυσικά να έχει δημιουργηθεί τέτοιο εισιτήριο καθώς και να πραγματοποιήσει ανάληψη (withdraw) των πληρωμών σε μορφή Ether που έχει συλλέξει το συμβόλαιο.

```
function SetTicketToUsed(uint256 tickedID_) external onlyOwner {

   require (tickedID_ < Event_ID*1000 + counter_minted_per_event, 'This ticket has not been minted!');
   UsedTickets[tickedID_]=true;

}
```

Παρατηρούμε στην συνθήκη ελέγχου την εξίσωση *Event_ID*1000 + counter_minted_per_event* που επαληθεύει αν το εκάστοτε εισιτήριο έχει δημιουργηθεί. Αυτό δεν είναι τίποτα παραπάνω από σχεδιαστική προτίμηση. Συγκεκριμένα, λειτουργεί ορθά αν τα Event ID είναι αύξοντα, δηλαδή Event 0, Event 1,…, Event 500, … και αν και μόνο αν ο μέγιστος αριθμός εισιτηρίων ανά event δεν μπορεί να υπερβεί τα 1000 (φυσικά αυτό προσαρμόζεται πολύ εύκολα). Για παράδειγμα το πρώτο εισιτήριο του πρώτου event είναι το 0 ενώ το πρώτο του δεύτερου event είναι το 1000.

```
function withdraw() public payable onlyOwner {

   (bool success, ) = payable(msg.sender).call{value: address(this).balance}("");
   require(success);

 }
```

Β) Συνεχίζοντας ως ενδιαφερόμενος που επιθυμεί να συμμετάσχει στην εκδήλωση:

Προκειμένου να μπορεί κάποιος να συμμετάσχει στην εκδήλωση, δηλαδή να αλληλεπιδράσει με το έξυπνο συμβόλαιο για να αγοράσει εισιτήριο επιβάλλεται να έχει μεριμνήσει ο διοργανωτής να αρχικοποιήσει το event και να έχει ενεργοποιήσει τις πωλήσεις. Δεδομένου ότι αυτές οι προϋποθέσεις ισχύουν, ο ενδιαφερόμενος μπορεί, εφόσον δεν έχουν εξαντληθεί τα εισιτήρια, να αγοράσει το εισιτήριο του απευθείας από το έξυπνο συμβόλαιο. Η συνάρτηση που οφείλει να καλέσει είναι η mintTicket(). Η συνάρτηση είναι “payable”, δηλαδή αναμένει να λάβει ποσότητα Ether. Το έξυπνο συμβόλαιο θα περιμένει να λάβει ακριβώς την ποσότητα που πρέπει, δηλαδή όσο κοστίζει το εισιτήριο, προκειμένου να θεωρήσει έγκυρη την συναλλαγή. Τέλος, το έξυπνο συμβόλαιο μέσω αυτής της συνάρτησης θα ενημερώσει αυτόματα σε περίπτωση που τα εισιτήρια έχουν εξαντληθεί και θα υπάρχει μόνο η δυνατότητα δευτερογενών πωλήσεων.

```
function mintTicket() external payable {

   require(areSalesActive, 'Can not purchase a ticket. Sale has not yet started!');
   require(msg.value == MintPrice, 'Trying to pay a wrong ticket price!');
   require (counter_minted_per_event < MaxSupply, 'SOLD OUT');
   _mint(msg.sender, Event_ID*1000 + counter_minted_per_event);
   counter_minted_per_event++;
   if (counter_minted_per_event == MaxSupply) PrimarySale_SoldOut = true;
}
```

Σε περίπτωση που εξαντλήθηκαν οι πρωτεύοντες πωλήσεις (primary sales), το έξυπνο συμβόλαιο είναι αδύνατον να παράγει επιπλέον εισιτήρια. Δύναται, όμως, να

υποστηρίξει πλήρως δευτερογενείς πωλήσεις (secondary sales). Λέγοντας πλήρης υποστήριξη δευτερογενών πωλήσεων, αναφερόμαστε στην ανάρτηση ενός εισιτηρίου για πώληση σε τιμή αρέσκειας του πωλητή, την δυνατότητα ακύρωσης μίας ανάρτησης πώλησης καθώς και την δυνατότητα αγοράς από ενδιαφερόμενο αγοραστή όσο η ανάρτηση έχει ισχύ. Κατ' αρχάς, κάθε χρήστης μπορεί εύκολα να επιβεβαιώσει την κατάσταση ενός εισιτηρίου, όσον αφορά αν έχει χρησιμοποιηθεί ή όχι. Η συνάρτηση που οφείλει να καλέσει είναι η IsTicketUsed(), η οποία δέχεται ακριβώς ένα όρισμα, έναν ακέραιο αριθμό, την αύξουσα κωδικοποίηση του εισιτηρίου (π.χ. 50) και επιστρέφει αληθές ή ψευδές.

```
function IsTicketUsed(uint256 Ticketid) external view returns (bool used)  {

    require (Ticketid < Event_ID*1000 + counter_minted_per_event, 'This ticket has not been minted!');
     used = UsedTickets[Ticketid];

}
```

Ακόμη, με κλήση της συνάρτησης IsTicketForSale() με μοναδικό όρισμα την αύξουσα κωδικοποίηση του εισιτηρίου μπορεί κάποιος να ενημερωθεί άμεσα αν ένα εισιτήριο είναι προς πώληση και φυσικά σε ποια τιμή. Προσοχή αυτή η τιμή θα επιστραφεί σε Wei και όχι σε Ether.

```
function IsTicketForSale(uint256 Ticketid) external view returns (bool forsale, uint256 price) {

    require (Ticketid <= Event_ID*1000 + counter_minted_per_event, 'This ticket has not been minted!');
    if (tickets_for_sale[Ticketid].price > 0 ) {
       forsale = true;
       price = tickets_for_sale[Ticketid].price;
       }
    else {
       forsale = false;
       price = 0;
    }

}
```

Αποτελεί σχεδιαστική επιλογή, σε περίπτωση που το εν λόγω εισιτήριο δεν είναι προς πώληση να επιστρέφεται ως τιμή μηδέν (0), φυσικά μαζί με "False" στο ερώτημα αν είναι προς πώληση.
Με τις παραπάνω συναρτήσεις είδαμε πως μπορεί κάποιος να χρησιμοποιήσει το έξυπνο συμβόλαιο για να ενημερωθεί για την κατάσταση ενός εισιτηρίου. Στη συνέχεια θα δούμε πως κάποιος μπορεί να θέσει ένα εισιτήριο για πώληση (και να ακυρώσει την πώληση του αντίστοιχα) και πως μπορεί ένας ενδιαφερόμενος να αγοράσει ένα εισιτήριο που διατίθεται προς πώληση.
Απαραίτητη προϋπόθεση για να μπορέσει να θέσει ένας κάτοχος εισιτηρίου το εισιτήριο του προς πώληση είναι να εξουσιοδοτήσει το ίδιο το συμβόλαιο προκειμένου να μπορεί το συμβόλαιο, αυτόματα, σε περίπτωση πώλησης να μεταφέρει την κυριότητα από τον πωλητή στον αγοραστή. Δίχως αυτήν την εξουσιοδότηση το έξυπνο συμβόλαιο δεν επιτρέπει να τεθεί ένα εισιτήριο προς πώληση. Ο πιο εύκολος τρόπος να εξουσιοδοτηθεί το έξυπνο συμβόλαιο είναι μέσω της συνάρτησης setApprovalForAll() η οποία αναμένει δύο ορίσματα. Το δε πρώτο

είναι η διεύθυνση που εξουσιοδοτείται, δηλαδή του συμβολαίου και το δεύτερο όρισμα είναι μία τιμή είτε Αληθής είτε Ψευδής ανάλογα με το αν εξουσιοδοτείται το συμβόλαιο ή διακόπτεται η υπάρχουσα εξουσιοδότηση του. Άπαξ και ο πωλητής εξουσιοδοτήσει το συμβόλαιο δύναται να θέσει προς πώληση το εισιτήριο που κατέχει καλώντας την συνάρτηση setTicketForSale() η οποία αναμένει δύο ορίσματα: το αναγνωριστικό του εισιτηρίου που θέλει να θέσει σε πώληση και φυσικά την τιμή πώλησης.

```
function setTicketForSale (uint256 price, uint256 tokenID_) public {

   require(this.ownerOf(tokenID_) == msg.sender, 'You do not own the ticket you are trying to set for sale!');
   require(this.isApprovedForAll(msg.sender,(address(this))),'You need to approve the contract to be able to transfer the token in case of sale!');
   tickets_for_sale[tokenID_] = TicketListing(price,UsedTickets[tokenID_],msg.sender);

}
```

Σε περίπτωση που ο πωλητής αποφασίσει να ακυρώσει την ανάρτηση πώλησης ενός εισιτηρίου μπορεί να προβεί σε κλήση της συνάρτησης cancelTicketForSale() δίνοντας ως όρισμα το αναγνωριστικό του εισιτήριου. Προφανώς, απαιτείται το εισιτήριο να είναι ήδη αναρτημένο προς πώληση διαφορετικά δεν μπορεί να εκτελεστεί η συνάρτηση.

```
function cancelTicketForSale (uint256 tokenID_) public {

   require (tokenID_ < Event_ID*1000 + counter_minted_per_event, 'This ticket has not been minted!');
   require (tickets_for_sale[tokenID_].price > 0, 'This ticket is not for sale!');
   require(this.ownerOf(tokenID_) == msg.sender, 'You do not own the ticket you are trying to cancel for sale!');

   delete tickets_for_sale[tokenID_];

}
```

Σε αυτό το σημείο απομένει να αναλύσουμε την συνάρτηση με την οποία δύναται ένας ενδιαφερόμενος αγοραστής να προβεί στην αγορά του εισιτηρίου. Όπως προαναφέραμε, ο αγοραστής μπορεί να επιβεβαιώσει ότι το εκάστοτε εισιτήριο που επιθυμεί είναι όντως προς πώληση και σε ποια τιμή. Εφόσον επιτελέσει τα βήματα αυτά μπορεί να καλέσει την συνάρτηση purchaseTicket() με όρισμα το αναγνωριστικό του εισιτηρίου που επιθυμεί και αφού καταβάλλει την απαραίτητη πληρωμή (payable συνάρτηση) θα συμβεί ταυτόχρονα τόσο η μεταφορά της κυριότητας του εισιτηρίου που αγόρασε όσο και η πληρωμή σε Ether του πωλητή.

```
function purchaseTicket(uint256 tokenID_) public payable {

require (tokenID_ < Event_ID*1000 + counter_minted_per_event, 'This ticket has not been minted!');
require (tickets_for_sale[tokenID_].price > 0, 'This ticket is not for sale!');

TicketListing memory ticket = tickets_for_sale[tokenID_];

require (msg.value == ticket.price, 'Insuffiecient funds');
```

```
this.safeTransferFrom(ticket.seller,msg.sender,tokenID_);
address payable addr = payable(ticket.seller);

addr.transfer(ticket.price);

delete tickets_for_sale[tokenID_];
sold_secondary = sold_secondary + 1;

}
```

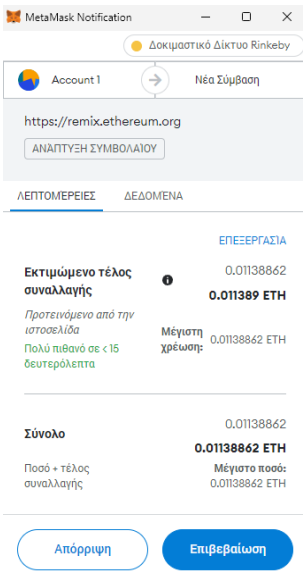
Όλες οι παραπάνω συναρτήσεις δοκιμάστηκαν και λειτουργούν ορθά, ενώ όλο το συμβόλαιο εμπνέει εμπιστοσύνη στους χρήστες, αφού βασίζεται, στις πασίγνωστες και πολύ δοκιμασμένες για τον χώρο του Ethereum, βιβλιοθήκες του OpenZeppelin. Συγκεκριμένα, κάνει χρήση του προτύπου ERC721 που είναι η κυρίαρχη μορφή για την δημιουργία Non-Fungible Tokens στο δίκτυο του Ethereum και του προτύπου Ownable που εξασφαλίζει αποκλειστική πρόσβαση στον διοργανωτή σε θέματα διαχείρισης.
Επιπρόσθετα, λόγω της δυνατότητας που παρέχεται στον διοργανωτή να προσθέσει εικόνα στο εισιτήριο της διοργάνωσης, έγινε χρήση και γνωστής συνάρτησης κωδικοποίησης και αποκωδικοποίησης σε μορφή Base64. Αυτό είναι απαραίτητο διότι προς ευκολία χρήσης, ο διοργανωτής παρέχει υπερσύνδεσμο για την εικόνα και όχι την δυαδική αναπαράσταση της εικόνας και πρέπει ο σύνδεσμος αυτός να προστεθεί στα μεταδεδομένα του NFT, αυστηρά σε δυαδική μορφή, ώστε να είναι ορατή η εικόνα σε όλες τις μεγάλες πλατφόρμες που υποστηρίζουν NFT. Ουσιαστικά, κάνουμε override την έτοιμη συνάρτηση της βιβλιοθήκης ERC721 tokenURI(), καθώς δεν παρέχει την δυνατότητα σύνθετων μεταδεδομένων, παρεμποδίζοντας την αισθητική βελτίωση της μορφής του εισιτηρίου. Ως σχεδιαστική επιλογή προστέθηκαν μερικά επιπλέον στοιχεία στα μεταδεδομένα που ο συγγραφέας έκρινε σημαντικά (όνομα και χαρακτηριστικά εισιτηρίου).

```
function tokenURI(uint256 tokenId) override(ERC721) public view returns (string memory) {

    string memory json = Base64.encode(
        bytes(string(
            abi.encodePacked(
                '{"name": "Access Ticket",',
                 '"image": "',ImageURL,'",',
                '"attributes": [{"trait_type": "Event ID", "value": ', uint2str(Event_ID), '},',
                '{"trait_type": "Ticket ID", "value": ', uint2str(tokenId), '}]}'
            )
        ))
    );
    return string(abi.encodePacked('data:application/json;base64,', json));

}
```

Κεφάλαιο 4: Λειτουργία της αποκεντρωμένης εφαρμογής

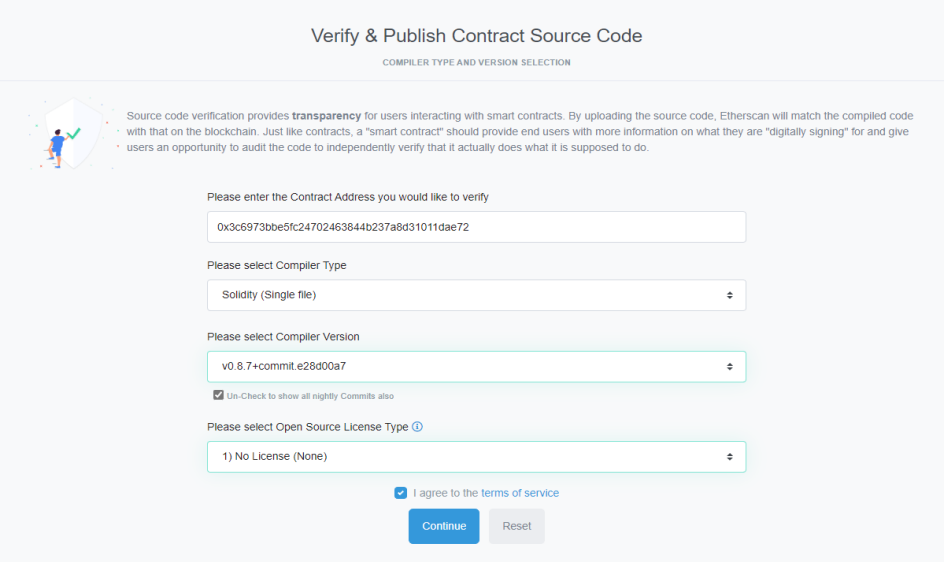
4.1 Καταχώρηση του συμβολαίου, επιβεβαίωση του πηγαίου κώδικα και αρχικοποίηση του συστήματος ως διοργανωτές

Όλες οι συναλλαγές λαμβάνουν μέρος στο δοκιμαστικό δίκτυο Rinkeby, αφού πρώτα προμηθευτούμε δοκιμαστικά Ether από κατάλληλη παροχή (Ethereum faucet).



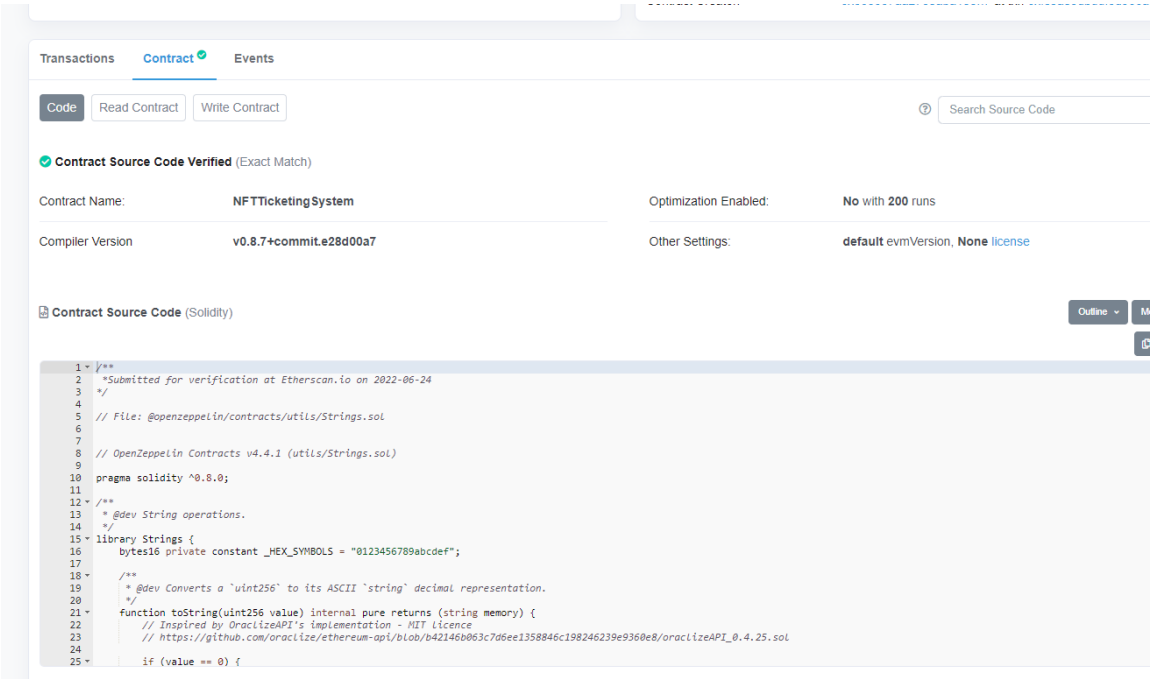
Εικόνα 9: Υπογραφή συναλλαγής δημιουργίας του έξυπνου συμβολαίου.

Κατευθείαν λαμβάνουμε επιβεβαίωση ότι η συναλλαγή έχει συμπεριληφθεί σε Block και είναι επικυρωμένη. Ως ιδιοκτήτες του συμβολαίου, έχουμε πλέον το μοναδικό δεκαεξαδικό (hex) αναγνωριστικό του συμβολαίου (0x3C6973Bbe5FC24702463844b237A8D31011DAE72) και συνεχίζουμε επιβεβαιώνοντας τον πηγαίο κώδικα στο Etherscan (ιδιαίτερα χρήσιμο plugin του Remix IDE για τη διαδικασία αυτή είναι το “Flattener”). Φυσικά δεν είναι αναγκαία η χρήση του plugin γιατί ο πηγαίος κώδικας είναι ήδη γνωστός. Ωστόσο, σε συμβόλαια που κάνουν import βιβλιοθήκες (όπως και σε αυτό της εργασίας) πρέπει να συμπεριληφθεί και ο κώδικας των βιβλιοθηκών. Το plugin αυτό μεριμνά για την συγκεκριμένη λεπτομέρεια και προσφέρει απευθείας όλο τον πηγαίο κώδικα.



Εικόνα 10: Επιβεβαίωση του πηγαίου κώδικα του συμβολαίου.

Αν δεν γίνει επιβεβαίωση του πηγαίου κώδικα καθίσταται αδύνατη η αλληλεπίδραση με το συμβόλαιο μέσω του Etherscan. Άπαξ και γίνει επιβεβαίωση του πηγαίου κώδικα, ταυτόχρονα αυτός γίνεται δημόσιος και μπορεί να μελετηθεί από όλους τους χρήστες του δικτύου.

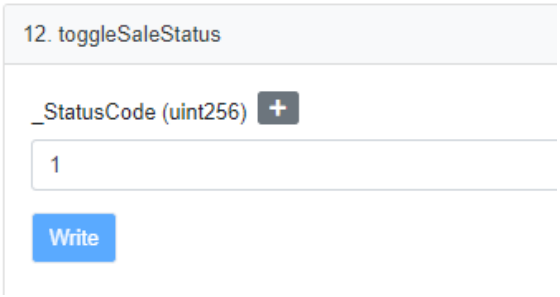


Εικόνα 11: Απεικόνιση ενός επιβεβαιωμένου συμβολαίου με δυνατότητες αλληλεπίδρασης Read/Write.

Προκειμένου να ενεργοποιηθεί το συμβόλαιο για να υποστηρίξει πωλήσεις πρέπει να αρχικοποιήσει ο διοργανωτής το πρώτο event.

Εικόνα 12: Αρχικοποίηση του πρώτου event από τον διοργανωτή.

Είναι πολύ καλή συνήθεια η εικόνα που αντιπροσωπεύει ένα NFT να είναι "immutable", δηλαδή να μην μπορεί να αλλοιωθεί. Θέτοντας ως Image URL μία εικόνα που έχει ανεβεί στο IPFS εμπνέουμε εμπιστοσύνη στους ενδιαφερόμενους. Αυτό οφείλεται στην φύση του IPFS που είναι πρωτόκολλο peer-to-peer και χρησιμοποιεί κατανεμημένο σύστημα αρχείων, με αποτέλεσμα να μην γίνεται να απολεσθεί ποτέ η εικόνα. Η χρήση του είναι δωρεάν.
Επίσης βλέπουμε ότι το Mint Price περιέχει πληθώρα μηδενικών. Συγκεκριμένα, έχει δεκαοκτώ (17) μηδενικά και αυτό γιατί η μικρότερη υποδιαίρεση ενός πλήρους Ether είναι το ένα Wei και ισχύει πως 1 Ether = 10^{18} Wei. Θέσαμε, δηλαδή, τιμή 0.1 Ether ανά εισιτήριο.

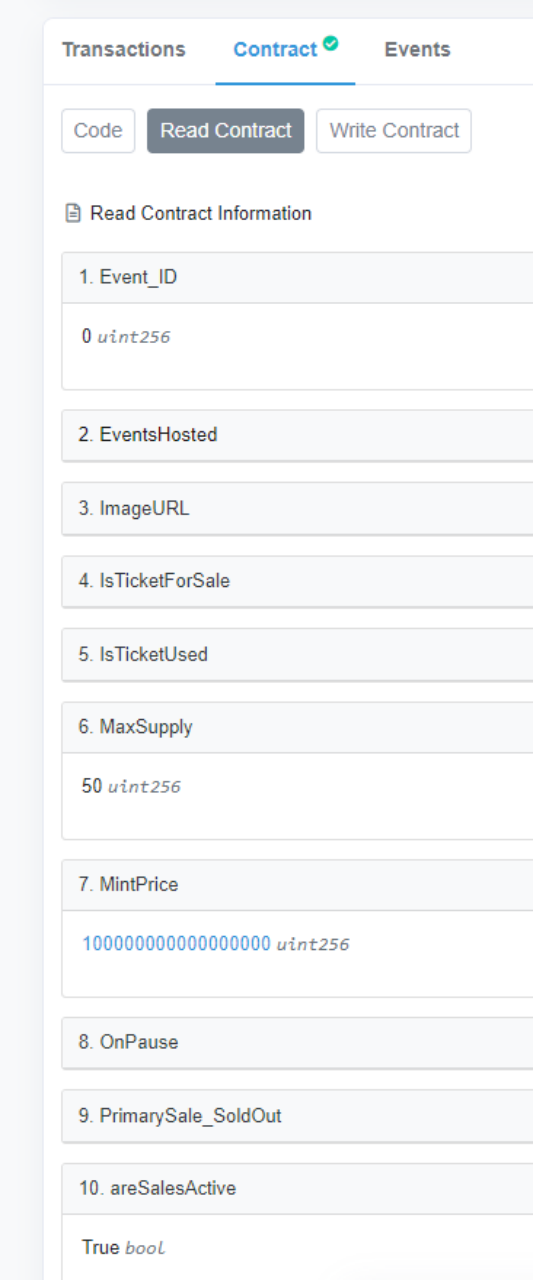


Εικόνα 13: Ενεργοποίηση των πωλήσεων από τον διοργανωτή.

Πλέον το σύστημα έχει ενεργοποιηθεί. Είναι σειρά των ενδιαφερόμενων να αγοράσουν εισιτήριο.

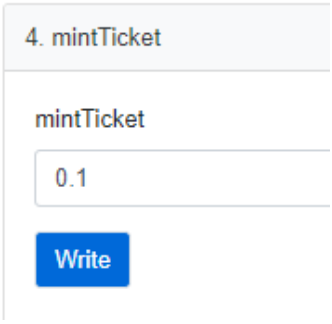
4.2 Αλληλεπίδραση με το συμβόλαιο ως attendees

Για να γίνουμε attendees αρκεί απλά να αλλάξουμε πορτοφόλι. Μόνο από την αλλαγή έχουμε χάσει τα δικαιώματα διοργανωτή. Προσεγγίζοντας, λοιπόν, το συμβόλαιο ως ενδιαφερόμενοι να παρακολουθήσουμε την διοργάνωση είμαστε σε θέση να αντλήσουμε όλες τις σημαντικές πληροφορίες όπως: Ποιος είναι ο τρέχον αύξων αριθμός εκδήλωσης (Event ID), Ποια είναι η τιμή του εισιτηρίου (Mint Price), Ποια είναι η μέγιστη ποσότητα εισιτηρίων (Max Supply), Αν το συμβόλαιο είναι ενεργό, αν εξυπηρετεί μόνο δευτερογενείς πωλήσεις ή αν για κάποιο λόγο βρίσκεται σε προσωρινή παύση. Οι υπόλοιπες συναρτήσεις ενώ μπορούν να κληθούν κανονικότατα κρίνονται τετριμμένες, αφού προέχει να δημιουργηθούν πρώτα μερικά εισιτήρια.



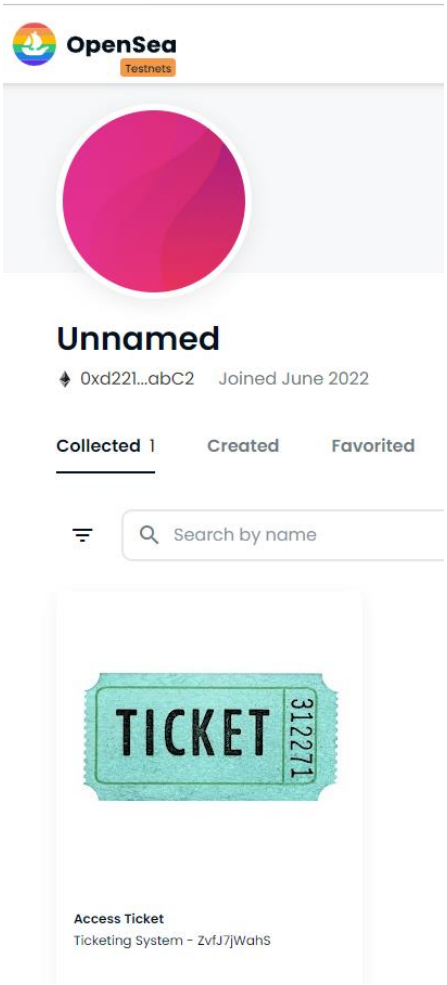
Εικόνα 14: Δεδομένα που αντλεί ο ενδιαφερόμενος από το ίδιο το συμβόλαιο.

Στο σημείο αυτό είμαστε σε θέση να προχωρήσουμε στην αγορά ενός εισιτηρίου. Καλούμε, λοιπόν, την συνάρτηση MintTicket() αφού θέσουμε ως τιμή 0.1 Ether.



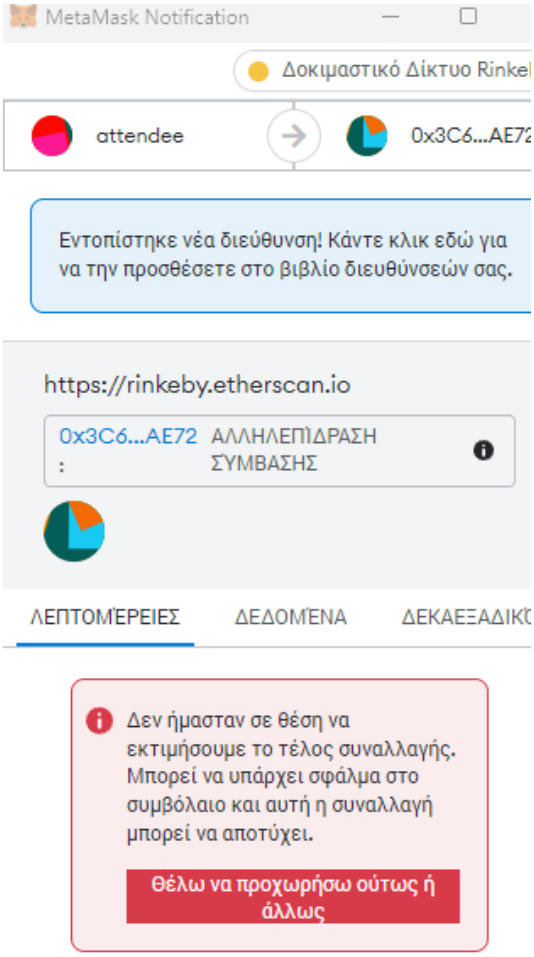
Εικόνα 15: Αγορά ενός εισιτηρίου απευθείας από το έξυπνο συμβόλαιο.

Μόλις η συναλλαγή ενταχθεί σε Block και επικυρωθεί διαθέτουμε στην κατοχή μας ένα εισιτήριο σε μορφή NFT. Μπορούμε να δούμε το NFT μας με ευκολία στην μεγαλύτερη πλατφόρμα για NFTs στο Ethereum, την Opensea (προσοχή: Στο δοκιμαστικό δίκτυο Rinkeby).



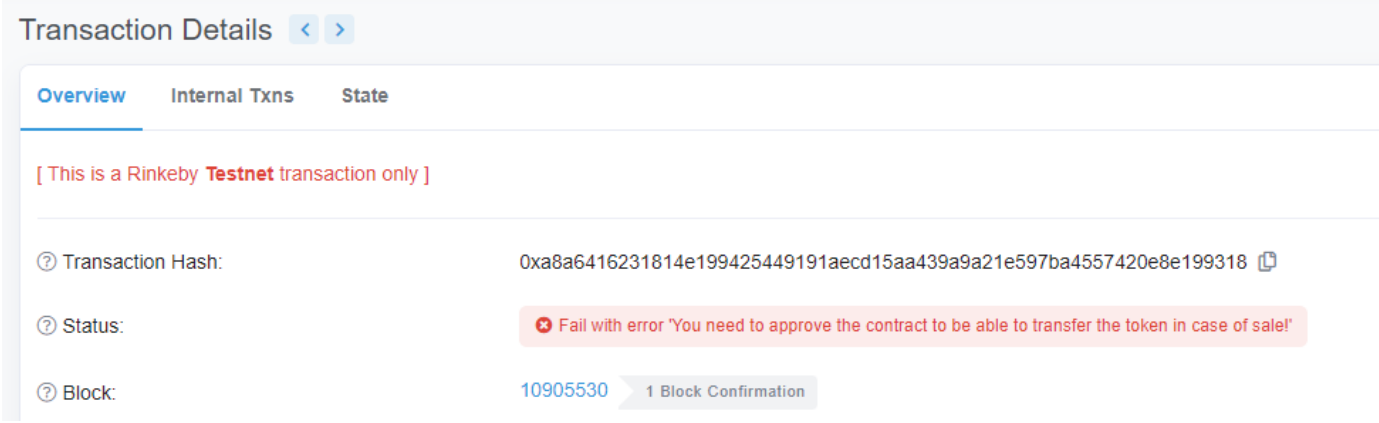
Εικόνα 16: Αναζήτηση και προβολή του NFT που μόλις αγοράσαμε.

Πλέον διαθέτουμε ένα αχρησιμοποίητο εισιτήριου εισόδου για μία εκδήλωση που μας ενδιαφέρει. Μπορούμε να προβούμε οποιαδήποτε στιγμή σε πώληση του NFT. Εδώ έχουμε πολλές επιλογές. Θα μπορούσαμε να το πουλήσουμε στην ίδια την Opensea ή στο δικό μας συμβόλαιο. Ενώ υπό πραγματικές συνθήκες ο τυχαίος χρήστης θα χρησιμοποιούσε την Opensea, εμείς θα χρησιμοποιήσουμε το δικό μας συμβόλαιο για να δείξουμε την λειτουργία του.
Είχαμε τονίσει ότι για να γίνει η διαδικασία πώλησης, οφείλει ο πωλητής πρώτα να εξουσιοδοτήσει το συμβόλαιο. Μάλιστα, αν αποπειραθεί να επιχειρήσει να αναρτήσει για πώληση το εισιτήριο του χωρίς πρώτα να έχει εξουσιοδοτήσει το συμβόλαιο λαμβάνει το ακόλουθο προειδοποιητικό μήνυμα:



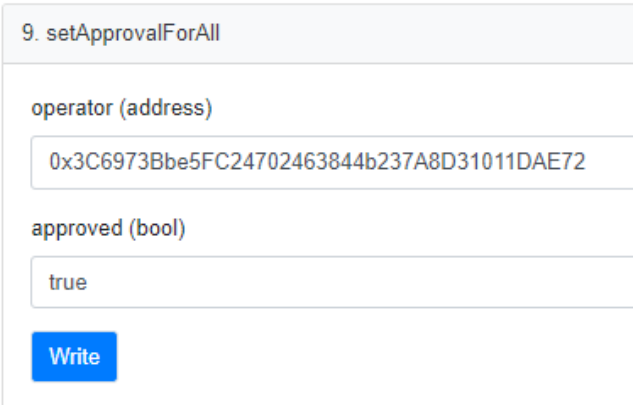
Εικόνα 17: Προειδοποιητικό μήνυμα - Υπάρχει σφάλμα.

Βρισκόμαστε σε αποκεντρωμένο δίκτυο και κατά επέκταση ο χρήστης μπορεί να αποφασίσει να αγνοήσει το μήνυμα και να προβεί σε απόπειρα εκτέλεσης της συναλλαγής. Ως συνέπεια, βλέπουμε την συναλλαγή να αποτυχαίνει και την αιτία αποτυχίας της. Ο χρήστης δεν έχασε κάτι πέρα από το τέλος συναλλαγής, δηλαδή το transaction fee αφού έγινε απόπειρα να μπεί σε Block.



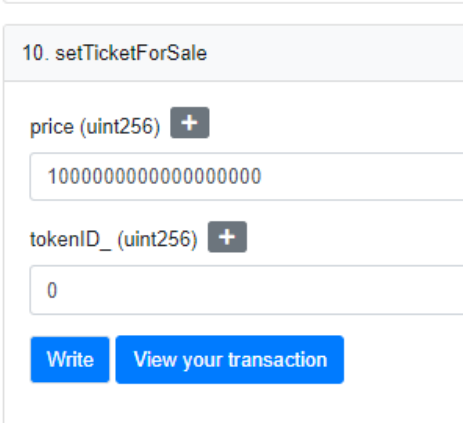
Εικόνα 18: Αδυναμία εκτέλεσης της συναλλαγής λόγω αναμενόμενου σφάλματος.

Ας γίνει, τώρα, η διαδικασία με την ορθή και έγκυρη σειρά. Ξεκινάμε εξουσιοδοτώντας το έξυπνο συμβόλαιο.



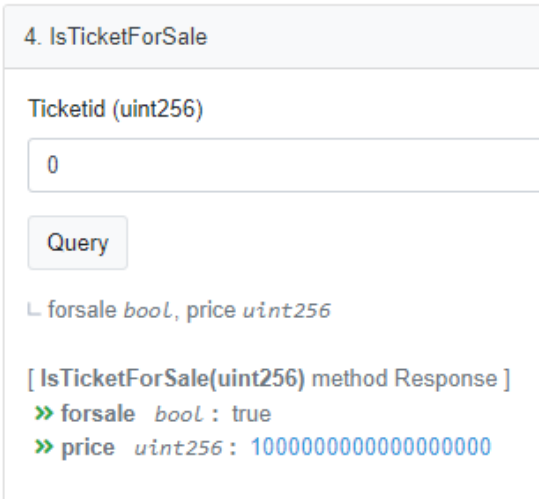
Εικόνα 19: Εξουσιοδότηση του συμβολαίου.

Μόλις επιβεβαιωθεί η συναλλαγή εξουσιοδότησης, προχωρούμε στην ανάρτηση πώλησης του εισιτηρίου που αγοράσαμε (αναγνωριστικό εισιτηρίου 0). Ορίζουμε ως τιμή πώλησης 1 Ether.

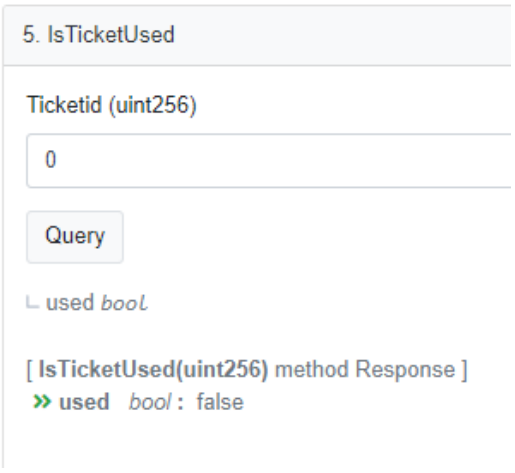


Εικόνα 20: Ανάρτηση πώλησης του εισιτηρίου.

Έστω, λοιπόν, ότι βρίσκεται ενδιαφερόμενος αγοραστής του συγκεκριμένου εισιτηρίου (σε σενάριο που εξαντλήθηκαν τα εισιτήρια και γίνεται πλέον μόνο αγορά από secondary market). Ο αγοραστής πληροφορείται ότι το εισιτήριο με αναγνωριστικό μηδέν (0) διατίθεται προς πώληση και αποφασίζει να μάθει την κατάσταση και επίσημη τιμή του. Πλοηγείται στο συμβόλαιο και αλληλεπιδρά μαζί του. Επιβεβαιώνει αν το εισιτήριο είναι όντως προς πώληση, σε ποια τιμή και αν είναι χρησιμοποιημένο ή όχι.

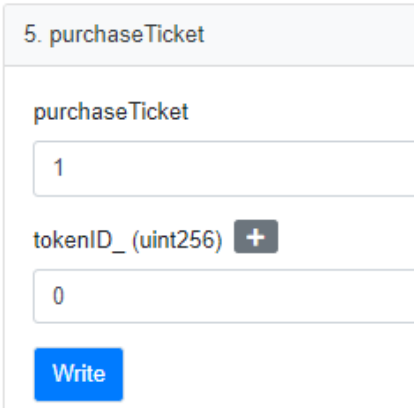


Εικόνα 21: Λήψη τιμής εισιτηρίου προς πώληση απευθείας από το συμβόλαιο.



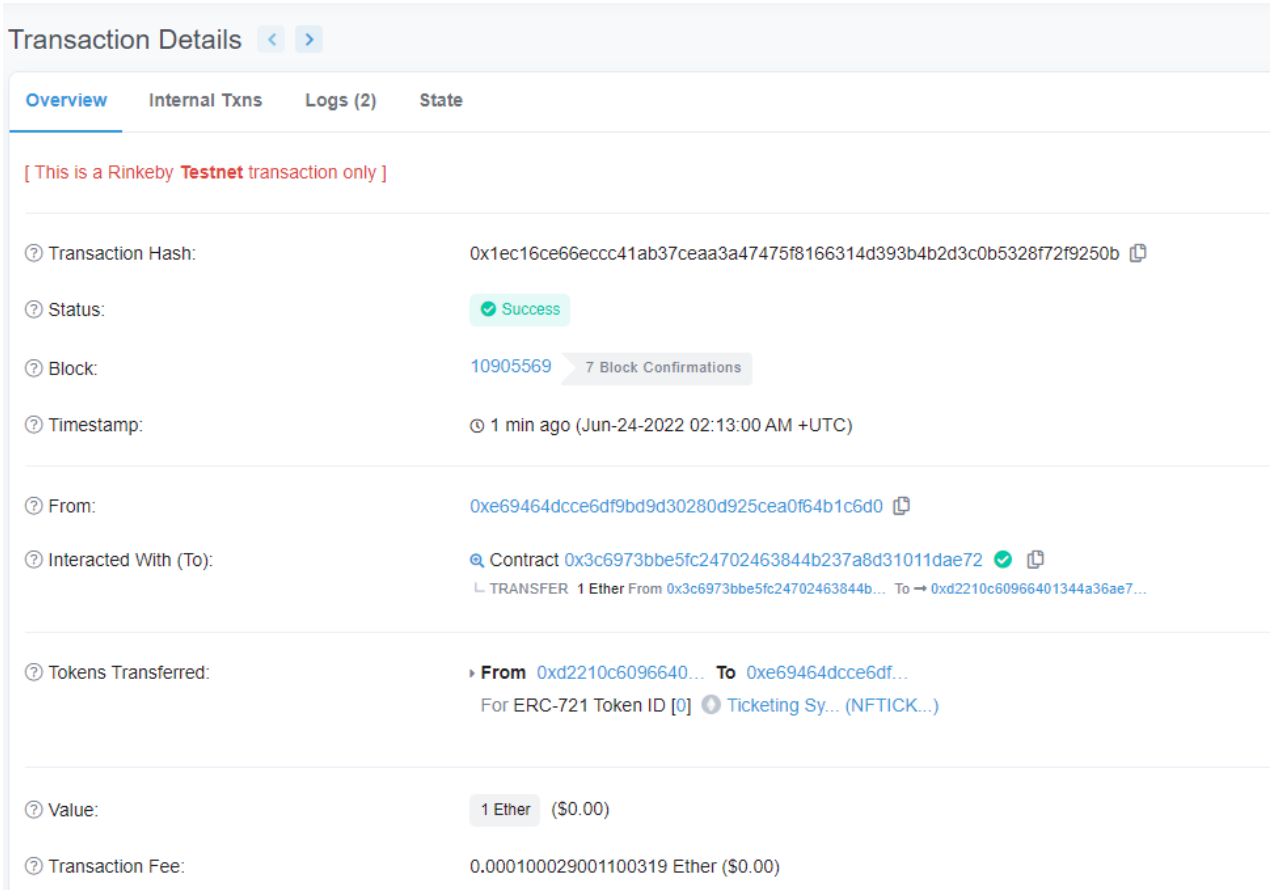
Εικόνα 22: Λήψη κατάστασης εισιτηρίου απευθείας από το συμβόλαιο.

Ο αγοραστής αποφασίζει να προβεί στην αγορά του εισιτηρίου, θέτοντας τις σωστές παραμέτρους στην κλήση της συνάρτησης purchaseTicket().



Εικόνα 23: Αγορά εισιτηρίου από secondary market μέσω του συμβολαίου.

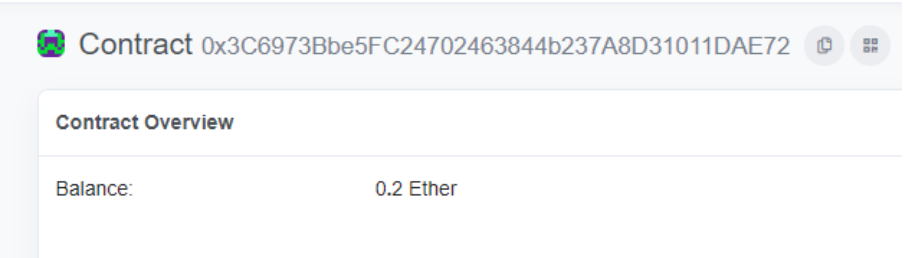
Η συναλλαγή επιβεβαιώνεται. Ο αγοραστής διαθέτει πλέον ένα (1) NFT εισιτήριο και ο πωλητής εισέπραξε 1 Ether στο πορτοφόλι του.



Εικόνα 24: Η συναλλαγή αγοραπωλησίας και μεταφοράς κυριότητας του εισιτηρίου.

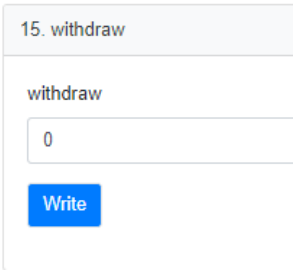
4.3 Επέμβαση του διοργανωτή για θεμιτές τροποποιήσεις και συλλογή εσόδων

Έστω χρονική στιγμή που έχουν δημιουργηθεί δύο εισιτήρια από το συμβόλαιο και έχει ανταλλαχθεί ένα σε δευτερογενή αγορά. Τότε το συμβόλαιο θα έχει συλλέξει ακριβώς 0.2 Ether (δηλαδή τιμή ίση με το κόστος των δύο εισιτήριών, αφού για δευτερογενείς πωλήσεις δεν έχει εφαρμοστεί κάποιου είδους προμήθεια).



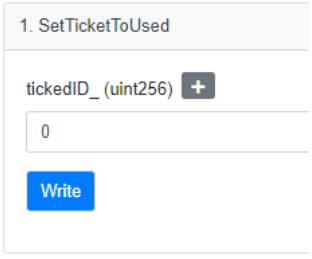
Εικόνα 25: Τυχαία χρονική στιγμή με συγκεντρωμένα έσοδα στο συμβόλαιο.

Τότε ο διοργανωτής και μόνο αυτός μπορεί να αλληλεπιδράσει με το έξυπνο συμβόλαιο (από το πορτοφόλι που το καταχώρησε στο δίκτυο) και να συλλέξει τα έσοδα.



Εικόνα 26: Συλλογή εσόδων από το συμβόλαιο.

Η συνάρτηση αυτή πρέπει να είναι “payable”. Μόνο έτσι δύναται μια συνάρτηση να μπορεί να αποστείλει (ή και να λάβει) Ether. Επειδή ακριβώς δεν γίνεται το σύστημα να γνωρίζει τι ακριβώς κάνει η συνάρτηση αναμένει να τοποθετηθεί μια τιμή από Ether, αν πρόκειται για αποστολή χρημάτων. Θέτοντας εκεί μηδέν (0), η συνάρτηση καλείται ορθά και η συναλλαγή εκτελείται. Ο διοργανωτής μπορεί ακόμη να θέσει ένα εισιτήριο ως “used”.

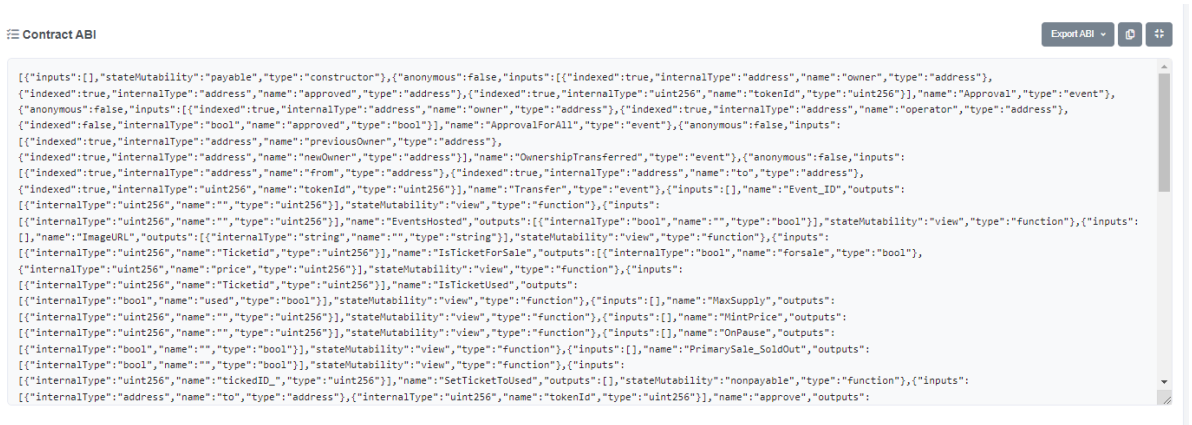


Εικόνα 27: Ο διοργανωτής μπορεί να θέσει ένα εισιτήριο ως χρησιμοποιημένο.

4.4 Αλληλεπίδραση και χρήση του συστήματος από front-end

Προκειμένου να δειχθεί έμπρακτα ότι τα συγκεκριμένα NFT θα συντελέσουν εισιτήρια εισόδου σε κλειδωμένο περιεχόμενο, έγινε κατασκευή front-end σε react που επιτρέπεται την πρόσβαση μόνο στους έχοντες εισιτηρίου (ανεξάρτητα αν αυτό αγοράστηκε από το συμβόλαιο ή από άλλον πωλητή). Ο χρήστης θα κληθεί να επισκεφθεί την ιστοσελίδα και να συνδέσει το πορτοφόλι του. Προσοχή. Η σύνδεση του πορτοφολιού συνεπάγεται ΜΟΝΟ ότι η ιστοσελίδα μπορεί να δει την διεύθυνση του πορτοφολιού και να αντλήσει πληθώρα πληροφοριών, καθώς να σχηματίσει πιθανές συναλλαγές τις οποίες θα ζητήσει από τον χρήστη να υπογράψει. Ουδεμία κακόβουλη πράξη μπορεί να λάβει μέρος από την σύνδεση πορτοφολιού. Παρ' όλα αυτά, εξυπακούεται ότι επιβάλλεται ύψιστη προσοχή στις συναλλαγές που η ιστοσελίδα θέτει προς υπογραφή, αφού αυτές εν τέλει μπορεί να είναι οι κακόβουλες.

Εξαιρετικά χρήσιμη βιβλιοθήκη για την σύνδεση front-end εφαρμογής με το δίκτυο του Ethereum είναι η ether.js. Η βιβλιοθήκη αυτή είναι πλήρης και ικανοποιεί με αποτελεσματικότητα την όποια αλληλεπίδραση με έξυπνο συμβόλαιο μέσω του πορτοφολιού Metamask. Ωστόσο, δεν αρκεί μόνο η βιβλιοθήκη αυτή για την αλληλεπίδραση με έξυπνο συμβόλαιο στο δίκτυο του Ethereum.
Χρειάζεται, ακόμη, το ABI (Application Binary Interface) του επιθυμητού έξυπνου συμβολαίου. Μόνο έτσι είναι εφικτή η πρόσβαση και κλήση σε συναρτήσεις του συμβολαίου από γλώσσες υψηλού επιπέδου, αφού το έξυπνο συμβόλαιο δεν είναι τίποτα παραπάνω από αλληλουχία bytes και επιβάλλεται να γίνει μετάφραση ονομάτων και ορισμάτων σε αναπαράσταση από bytes. Το ABI ενός επαληθευμένου έξυπνου συμβολαίου είναι ορατό προς όλους στο Etherscan και συνεπώς οποιοσδήποτε μπορεί να το χρησιμοποιήσει για σύνδεση σε front-end εφαρμογή.

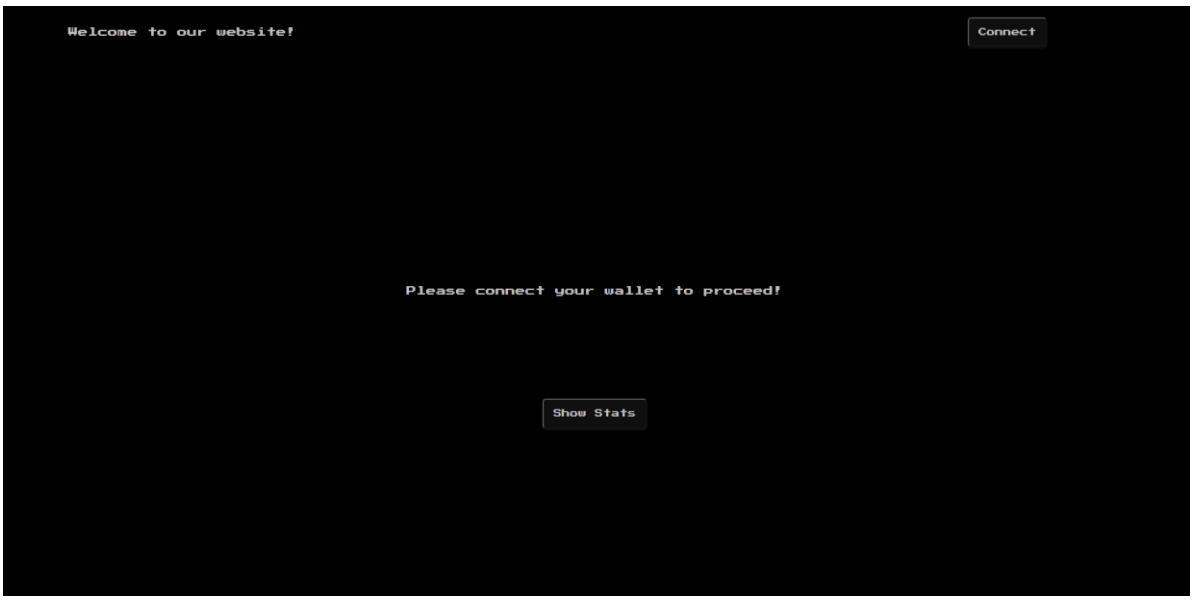


Εικόνα 28: Παράδειγμα ABI έξυπνου συμβολαίου.

Με την παρακάτω συνάρτηση γίνεται κλήση της συνάρτησης mintTicket() του έξυπνου συμβολαίου. Όπως βλέπουμε, αναμένει πρώτα να γίνει σύνδεση του πορτοφολιού του χρήστη. Εν συνεχεία, γίνεται διάβασμα των δεδομένων του συμβολαίου, λαμβάνεται η τιμή μονάδας εισιτηρίου και προετοιμάζεται η συναλλαγή που θα χρειαστεί την υπογραφή του χρήστη προκειμένου να εκτελεστεί.

```
async function handleMint () {

   if (window.ethereum) {
      const provide = new ethers.providers.Web3Provider(window.ethereum); //Connect to the blockchain
      const signer = (provide.getSigner());


      const contract = new ethers.Contract(ContractAddress, ticketingsystem, signer);
      try {
         //MintPrice
         const Price = await contract.MintPrice();
         const options = {value: Price};
         const response = await contract.mintTicket(options);

         console.log('response: ', response);
      }
       catch(err) {
         console.log("error: ", err);
      }
   }

}
```

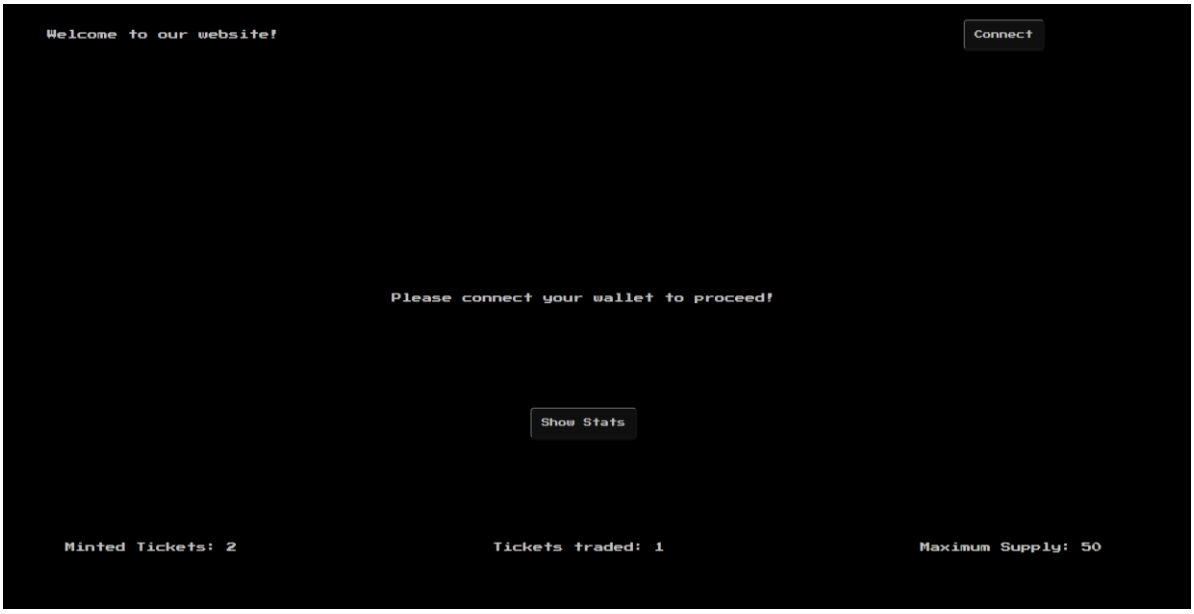
Στην συνέχεια κάνουμε χρήση της front-end εφαρμογής σαν χρήστης που ενδιαφέρεται για την εκδήλωση.



Εικόνα 29: Αρχική σελίδα του frontend.

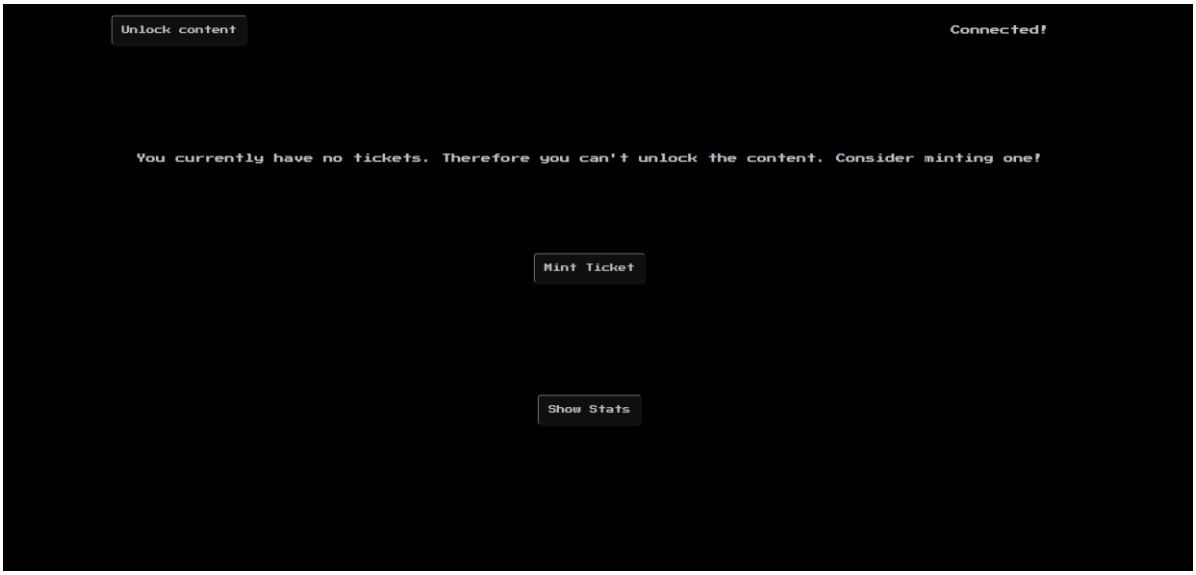
Παρατηρούμε ότι ο χρήστης μπορεί και χωρίς να συνδέσει το πορτοφόλι του (όπως άλλωστε θα έπρεπε) να δει πληροφορίες για την τρέχουσα κατάσταση της εκδήλωσης, δηλαδή πόσα εισιτήρια έχουν αγοραστεί, πόσα έχουν μεταπωληθεί σε δευτερογενή αγορά και πόσα είναι συνολικά διαθέσιμα. Επιλέγοντας Show Stats, αφού πρώτα έχουμε δημιουργήσει δύο (2) εισιτήρια και μεταπωλήσει ένα (1) και

ύστερα από μία μικρή καθυστέρηση, μιας και τα δεδομένα είναι τα τρέχοντα (οι πληροφορίες λαμβάνονται κατευθείαν από το συμβόλαιο):



Εικόνα 30: Εμφάνιση στατιστικών εκδήλωσης.

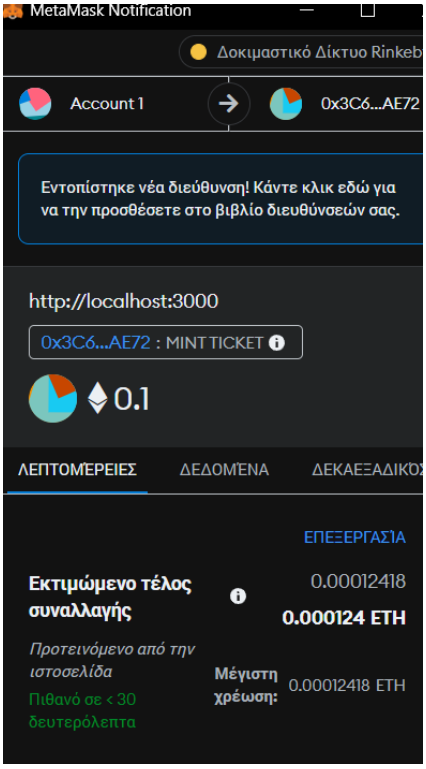
Σε περίπτωση που ο χρήστης συνδέσει το πορτοφόλι του και αποπειραθεί να ξεκλειδώσει το περιεχόμενο της εκδήλωσης δίχως να διαθέτει κατάλληλο NFT εισιτήριο εισόδου, παρατηρούμε μήνυμα που περιγράφει την κατάσταση και τον παροτρύνει να προβεί σε αγορά εισιτηρίου.



Εικόνα 31: Αδυναμία πρόσβασης στην εκδήλωση δίχως NFT εισιτήριο.

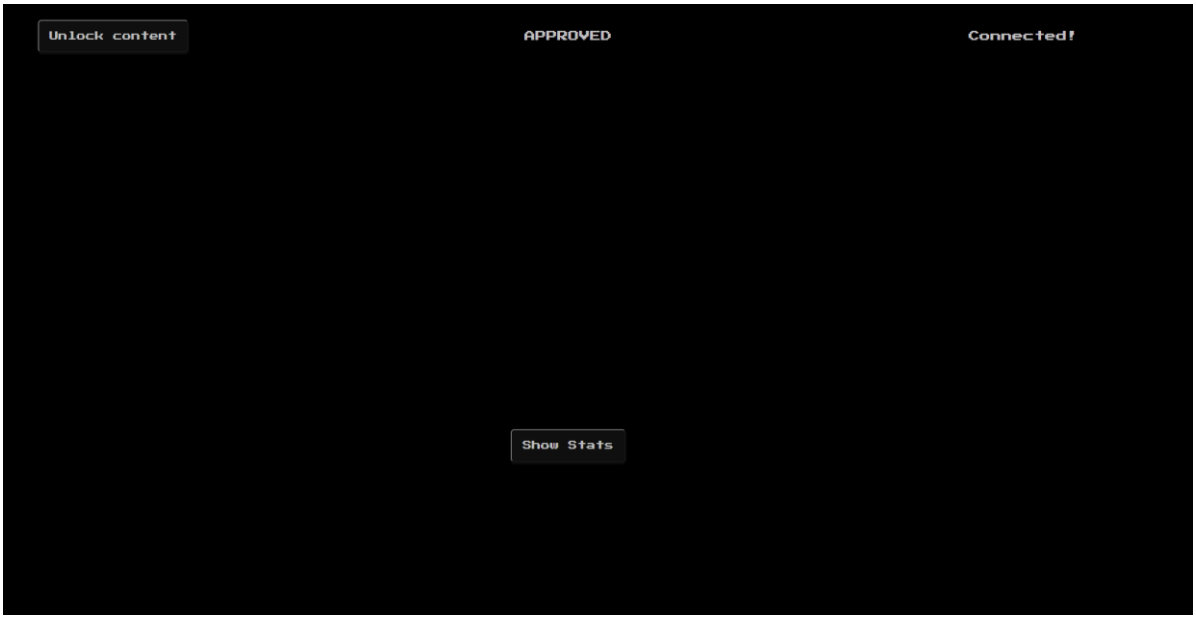
Επιλέγοντας Mint Ticket προκύπτει αναδυόμενο παράθυρο του Metamask πορτοφολιού, όπου μπορούμε να δούμε ότι γίνεται κλήση της συνάρτησης

MintTicket() καθώς και το συμβόλαιο, το οποίο μπορούμε με κλικ να δούμε στο Etherscan και να το μελετήσουμε προτού προβούμε σε υπογραφή της συναλλαγής. Ακόμα, βλέπουμε ότι αυτόματα τέθηκε η σωστή τιμή εισιτηρίου και ίση με 0.1 Ether.



Εικόνα 32: Αγορά εισιτηρίου με χρήση κουμπιού.

Μόλις επιβεβαιωθεί η συναλλαγή και με εκ νέου προσπάθεια για πρόσβαση στο κλειδωμένο περιεχόμενο λαμβάνουμε θετική ανταπόκριση (“APPROVED”).



Εικόνα 33: Πρόσβαση στο κλειδωμένο περιεχόμενο.

Η συνάρτηση που ελέγχει αν ο χρήστης έχει στην κατοχή του εισιτήριο υπό τη μορφή NFT κάνει κλήση της συνάρτησης balanceOf() του έξυπνου συμβολαίου που έχει εισαχθεί από το πρότυπο ERC721 της βιβλιοθήκης του OpenZeppelin.

```
async function Check() {

      if (window.ethereum) {
      const provide = new ethers.providers.Web3Provider(window.ethereum); //Connect to the blockchain
      const signer = (provide.getSigner());


      const contract = new ethers.Contract(ContractAddress, ticketingsystem, signer);
      try {
         const owned_tickets = await contract.balanceOf(accounts[0]);
      if (owned_tickets > 0) {
         HasTicket = true;
      }

      }
       catch(err) {
         console.log("error: ", err);
      }
   }

}
```

Κεφάλαιο 5: Συμπεράσματα, τρόποι επέκτασης και εφαρμογές

5.1 Ανακεφαλαίωση

Στη παρούσα διπλωματική εργασία είδαμε βήμα-βήμα την ανάπτυξη και την λειτουργία μιας πλήρως αποκεντρωμένης εφαρμογής για την άμεση, ασφαλή και αξιόπιστη αγορά εισιτηρίων πρόσβασης σε ψηφιακή εκδήλωση. Όλα πραγματοποιούνται μέσω επαληθεύσιμου έξυπνου συμβολαίου που υποστηρίζει και δευτερογενείς πωλήσεις.
Αναλυτικότερα, επιτρέπεται συγκεκριμένη πρόσβαση στον διοργανωτή, ο οποίος έχει περιορισμένα δικαιώματα διαχειριστή στο σύστημα, ενώ σε καμία περίπτωση δεν μπορεί να σφετεριστεί ή να ακυρώσει κυριότητα αγορασμένου εισιτηρίου. Συγκεκριμένα, ο διοργανωτής μπορεί να ενεργοποιήσει και να απενεργοποιήσει το συμβόλαιο, να θέσει εισιτήρια ως χρησιμοποιημένα και να ελέγχει κάθε πότε και για πόσο θα τεθεί σε ισχύ μία νέα εκδήλωση και φυσικά τα επιμέρους χαρακτηριστικά της. Μπορεί, ακόμα, ανά πάσα στιγμή να κάνει ανάληψη των εσόδων του συμβολαίου που δικαιωματικά του ανήκουν.
Από την άλλη πλευρά, ο ενδιαφερόμενος για την εκδήλωση χρήστης δύναται να μελετήσει όλα τα χαρακτηριστικά της εκδήλωσης (τιμή, συνολικός αριθμός εισιτηρίων, διαθέσιμα εισιτήρια, κατάσταση συμβολαίου, κατάσταση δευτερογενών πωλήσεων) και να αποφασίσει αν θέλει πράγματι να λάβει μέρος. Μόλις αγοράσει ένα εισιτήριο, είτε από πρωτογενή είτε από δευτερογενή αγορά, διαθέτει πλήρη κυριότητα, με την μορφή NFT, του εισιτηρίου του και έχει πρόσβαση σε πλήθος νέων συναρτήσεων που αφορούν την διαχείριση του εισιτηρίου του.
Η λειτουργία του συμβολαίου είναι απρόσκοπτη από εξωγενείς παράγοντες, αφού έχει καταχωρηθεί στο δίκτυο του Ethereum. Ο κώδικας του έξυπνου συμβολαίου έχει αναρτηθεί στο GitHub: https://github.com/giorgos208/NFTTicketingSystem

5.2 Εφαρμογή του συστήματος σε ρεαλιστικά σενάρια

Το σύστημα που δημιουργήθηκε μπορεί να αξιοποιηθεί στα ακόλουθα σενάρια (και όχι μόνο):

- Διεξαγωγή online σεμιναρίων με συγκεκριμένο θέμα. Παρέχεται πρόσβαση σε όσους διαθέτουν το κατάλληλο NFT εισόδου. Κάθε εβδομάδα μπορεί να λαμβάνει χώρα διαφορετική θεματική ενότητα και να απαιτείται διαφορετικό εισιτήριο (Διαφορετικό Event ID).
- Διεξαγωγή συναυλίας ή οποιασδήποτε καλλιτεχνικής δραστηριότητας. Ένας καλλιτέχνης μπορεί να χρησιμοποιεί επ' αόριστο το ίδιο έξυπνο συμβόλαιο, αφού αποτελεί σύστημα εκδηλώσεων και όχι μεμονωμένο γεγονός.
- Πραγματικού χρόνου δικαίωμα συμμετοχής σε βιντεοκλήση με στόχο τη γνωριμία και ομιλία με διάσημες προσωπικότητες που επιθυμούν να αναπτύξουν συζήτηση (meet and greet) με τους υποστηρικτές τους.

- Κάθε είδους συνδρομητική υπηρεσία με εβδομαδιαία, μηνιαία ή ετήσια ανανέωση.

5.3 Τρόποι επέκτασης του συστήματος

Το σύστημα δύναται να επεκταθεί προκειμένου να γίνει πιο ελκυστικό και κατ' επέκταση επιθυμητό για αξιοποίηση τόσο από την πλευρά ενός διοργανωτή όσο και ενός συμμετέχοντα.

Α) Για την βελτίωση της εμπειρίας και τη μεγιστοποίηση του πιθανού κέρδους ενός διοργανωτή:

- Είναι δυνατόν να επιβάλει ποσοστό φόρου σε όλες τις δευτερογενείς πωλήσεις. Το ύψος του ποσοστού ποικίλλει ανάλογα το είδος των εκδηλώσεων. Για παράδειγμα, αν το NFT εισιτήριο παρέχει μόνιμη πρόσβαση σε εβδομαδιαίες υπηρεσίες το ποσοστό φόρου θα μπορούσε να είναι μέχρι και πενήντα τοις εκατό (50%) ή και περισσότερο.
- Είναι δυνατόν ο διοργανωτής να επιθυμεί να προσφέρει ειδικές προσφορές σε όσους έχουν ήδη συμμετάσχει σε μία εκδήλωση (δηλαδή έχουν αγοράσει ήδη εισιτήριο) και πρόκειται να λάβουν μέρος και σε επόμενη. Μάλιστα, θα μπορούσαν να υπάρχουν ειδικές εκπτώσεις για απανωτές συμμετοχές.
- Είναι δυνατόν όλα τα εισιτήρια να μην έχουν την ίδια βαρύτητα και άρα ούτε την ίδια τιμή πώλησης.

Β) Για τη βελτίωση της εμπειρίας των συμμετεχόντων:

- Είναι δυνατόν οι χρήστες να μπορούν να κάνουν προσφορά (bid) για την διεκδίκηση κάποιου εισιτηρίου ακόμα και αν το εν λόγω εισιτήριο δεν έχει αναρτηθεί προς πώληση. Ο ιδιοκτήτης του εισιτηρίου θα μπορούσε να δεχτεί την προσφορά και να συμβεί δευτερογενής αγοραπωλησία ή να αρνηθεί την προσφορά.

5.4 Σχετικά με τους επικριτές της τεχνολογίας Blockchain και των κρυπτονομισμάτων

Δυστυχώς σήμερα περισσότερο από ποτέ κυριαρχεί σε πολλούς η νοοτροπία της ήσσονος προσπάθειας. Επειδή ο κόσμος των κρυπτονομισμάτων είναι σχετικά νέος και μέρα με την μέρα συμβάλουν στην κεφαλαιοποίηση του όλο και περισσότεροι άνθρωποι (αγοράζοντας κάποιο κρυπτονόμισμα) συχνά δημιουργούνται υπερ-αποδόσεις για αυτούς που εισήχθησαν νωρίτερα. Το παραπάνω σε συνδυασμό με την ύπαρξη είτε κακόβουλων είτε ανούσιων project έχει ως αποτέλεσμα πολλά άτομα να βρίσκονται στον κόσμο των κρυπτονομισμάτων αποκλειστικά για το γρήγορο κέρδος. Αγοράζουν κρυπτονομίσματα ενός μη γνωστού νομίσματος, αναμένουν να γίνει δημοφιλές συχνά εξαπατώντας πιο αρχάριους στον τομέα χρήστες και στη συνέχεια ρευστοποιούν τις θέσεις του έχοντας καρπωθεί σε κέρδος την απώλεια των νεοεισερχόμενων. Αυτό το γεγονός, πέραν του ότι αντιβαίνει σε μέγιστο βαθμό το

όραμα που προσπαθεί να φέρει αυτή η τεχνολογία, στηλιτεύει εξωφρενικά την εικόνα των κρυπτονομισμάτων στον έξω κόσμο και δημιουργεί την ιδέα ότι όλο το σύστημα είναι μια απάτη. Βέβαια, η απληστία του γρήγορου κέρδους είναι ιδιαίτερα επικίνδυνη, γιατί αυτά τα άτομα έχουν περιορισμένη επιτυχία αφού μετά από ένα σημείο θα εγκλωβιστούν σε κάποιο νόμισμα γιατί νόμιζαν ότι τοποθετήθηκαν νωρίς εντός αγοράς αλλά εν τέλει αγόρασαν ακριβώς πριν την πτώση.
Μοναδική αντιμετώπιση του παρόντος θέματος είναι η εκπαίδευση των νεοεισερχόμενων ώστε να αποφύγουν τέτοιες παγίδες γιατί τα κρυπτονομίσματα δεν είναι χρηματιστήριο, είναι κάτι ανώτερο. Σαν μηχανικός υπολογιστών μου ήταν ευκολότερο να διαπιστώσω την μοναδική φύση των κρυπτονομισμάτων και τον εκ νέου ορισμό της εμπιστοσύνης σε υπηρεσίες οικονομίας. Θεωρώ ότι οι επικριτές της τεχνολογίας του Blockchain εστιάζουν μονομερώς σε αρνητικά συμβάντα και αδυνατούν να παρατηρήσουν το γενικότερο καλό που μπορούν να προσφέρουν αυτές οι νέες τεχνολογίες. Ενδεικτικά, τριτοκοσμικές χώρες που πλήττονται από ατασθαλίες κρατών και πλαστογραφίες κάθε είδους μπορούν να εξασφαλίσουν ένα καλύτερο μέλλον, χάρη στην πλήρη διαφάνεια που συνεπάγεται η υιοθέτηση της αποκεντρωμένης τεχνολογίας. Παραδείγματα ευεργετικών χρήσεων είναι η τέλεση εκλογών με επαληθεύσιμη και μοναδική συμμετοχή, η καταμέτρηση ψήφων καθώς και η δημιουργία ταυτοτήτων πάνω σε δίκτυο Blockchain.
Εν συνεχεία, ένα άλλο τρανό επιχείρημα κατά των κρυπτονομισμάτων και ιδιαίτερα κατά του Bitcoin και του Ethereum είναι η συνολική ενεργειακή δαπάνη των δικτύων τους που σε ετήσια βάση ξεπερνά αυτή ολόκληρων χωρών. Πράγματι, η ενεργειακή δαπάνη και των δύο είναι αδιαμφισβήτητα υπέρογκη. Ωστόσο, εκτιμάται ότι ποσοστό άνω του εβδομήντα τοις εκατό (70%) προκύπτει από ανανεώσιμες πηγές ενέργειες (ηλιακή, αιολική και άλλες). Συνεπώς, οι θιασώτες του κατεστημένου τάσσονται κατά, σκεπτόμενοι μόνο έναν απόλυτο αριθμό και όχι πως αυτός πραγματικά προκύπτει. Μάλιστα, σχεδόν όλα τα νέα κρυπτονομίσματα ως βελτιωμένα έχουν ελαττώσει δραματικά την κατανάλωση ενέργειας, κυρίως γιατί αρκετά χρόνια αργότερα αποδείχθηκε με μαθηματικό υπόβαθρο, ασφαλής τρόπος για την δημιουργία των Blocks καταργώντας πλήρως τους miners, οι πράξεις των οποίων ήταν ουσιαστικά η αιτία της τεράστιας υπολογιστικής ισχύος. Γίνεται γενικότερη (όχι μόνο το Ethereum) μετάβαση από το Proof-of-Work (PoW) στο Proof-of-Stake (PoS). Άρα, είναι τελικά η ενεργειακή κατανάλωση του συστήματος ορθό αντεπιχείρημα;
Τα NFTs είναι αποτέλεσμα αξιοποίησης της τεχνολογίας Blockchain. Η διαφάνεια, η εγκυρότητα και η δυνατότητα επαλήθευσης που προσφέρει η τεχνολογία αυτή καθιστά τα NFT ριζική επανάσταση, καθώς και αναθεώρηση και γενίκευση της έννοιας της ιδιοκτησίας. Μέσω του Blockchain ανταλλάσσεται πλέον κάθε μορφή αξίας, όχι μόνο χρηματικής. Τα NFT εξασφαλίζουν απρόσκοπτη κυριότητα και δύνανται να ικανοποιήσουν πληθώρα αναγκών που έως τώρα κρινόταν απαραίτητη η συμμετοχή παραδοσιακών υπηρεσιών. Στο σύστημα που δημιουργήσαμε, ο διοργανωτής μπορεί κατά βούληση να ξεκινήσει μία εκδήλωση χωρίς να ανησυχεί για την εκπλήρωση καθηκόντων από τρίτους φορείς. Επιπροσθέτως, παύει να προβληματίζεται για πιθανά κωλύματα που δεν ελέγχει ο ίδιος, αφού το έξυπνο συμβόλαιο, άπαξ και ελεγχθεί εκτενώς, προσφέρει εγγυημένη ασφάλεια σε κάθε εκτέλεση. Ειδικότερα στο θέμα των εισιτηρίων, με επιβολή προμήθειας σε

δευτερογενείς πωλήσεις ο ίδιος ο διοργανωτής αποδέχεται μετά χαράς τις πωλήσεις μεταξύ τρίτων. Ο εμπλεκόμενος αγοραστής είναι βέβαιος για την εγκυρότητα του εισιτηρίου που αγοράζει, ενώ η πώληση μπορεί να γίνει άμεσα δίχως καθυστερήσεις ή πρόσθετη πληρωμή μεσαζόντων, οποιαδήποτε στιγμή της ημέρας και οποιαδήποτε ημέρα της εβδομάδας.

Η τεχνολογία πίσω από τα NFTs και οι δυνατότητες που παρέχουν τείνουν στη σημερινή εποχή να επισκιάζονται από την κοινή γνώμη που εστιάζει αποκλειστικά σε αρνητικά συμβάντα που επέφεραν εφήμερες φάσεις υπερ-απληστίας στον τομέα. Για όλους τους παραπάνω λόγους, θεωρώ ενδιαφέρουσα και ωφέλιμη την ενασχόληση μου, ως μηχανικός υπολογιστών, με τον υπό ανάπτυξη τομέα των κρυπτονομισμάτων και της τεχνολογίας τους. Πιστεύω πως με αντιπροσωπεύουν οι φιλελεύθερες ιδέες της αποκέντρωσης και πως μπορώ να δραστηριοποιηθώ και να παράξω ωφέλιμο έργο στον κλάδο.

Βιβλιογραφία

S. Nakamoto, (2008). “Bitcoin: A Peer-to-Peer Electronic Cash System.” [Ηλεκτρονική μορφή]
Σύνδεσμος: https://bitcoin.org/bitcoin.pdf.

V. Buterin, (2015). “Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.” [Ηλεκτρονική μορφή]
Σύνδεσμος: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Lacity, M. C., & Treiblmaier, H. (Eds.). (2022). *Blockchains and the Token Economy: Theory and Practice*. Springer Nature. [Ηλεκτρονική μορφή]
Σύνδεσμος: https://link.springer.com/book/10.1007/978-3-030-95108-5

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, *151*(2014), 1-32.

Regner, F., Urbach, N., & Schweizer, A. (2019). NFTs in practice–non-fungible tokens as core component of a blockchain-based event ticketing application.

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International journal of web and grid services*, *14*(4), 352-375.

Gupta, S. S. (2017). Blockchain. *IBM Onlone (http://www. IBM. COM)*.

Farell, R. (2015). An analysis of the cryptocurrency industry.

U. W. Chohan, (2017). “The Double Spending Problem and Cryptocurrencies.” [Ηλεκτρονική μορφή]
Σύνδεσμος: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174

Goyal S., (2018). “Centralized vs. Decentralized? The New Decentralized Internet Networks.” [Ηλεκτρονική μορφή]
Σύνδεσμος: https://101blockchains.com/centralized-vs-decentralized-internet-networks/

McMillan, C. (2016). “Secondary ticketing: the problem and possible solutions, explained.”
Σύνδεσμος: https://inews.co.uk/culture/music/secondary-ticketing-problems-solutions/

Jake Frankenfield, (2021). “Decentralized Applications.” [Ηλεκτρονική μορφή]
Σύνδεσμος: https://www.investopedia.com/terms/d/decentralized-applications-dapps.asp

Allie Grace Garnett, (2022). “Pros and Cons of Investing in NFTs.” [Ηλεκτρονική μορφή]
Σύνδεσμος: https://www.investopedia.com/pros-and-cons-of-investing-in-nfts-5220290

Griffin, J. (2018). “Software licences as non-fungible tokens.” [Ηλεκτρονική μορφή]

Σύνδεσμος: https://medium.com/atchai/software-licences-as-non-fungible-tokens-1f0635913e41

Ethereum [Ηλεκτρονική μορφή]
Σύνδεσμος: https://ethereum.org/en/

Jake Frankenfield, (2022). "Ethereum." [Ηλεκτρονική μορφή]
Σύνδεσμος: https://www.investopedia.com/terms/e/ethereum.asp

Etherscan, (2018). [Ηλεκτρονική μορφή]
Σύνδεσμος: https://etherscan.io/

Ethers [Ηλεκτρονική μορφή]
Σύνδεσμος: https://docs.ethers.io/v5/

Non-fungible Token, (2022). [Ηλεκτρονική μορφή]
Σύνδεσμος: https://en.wikipedia.org/wiki/Non-fungible_token

Solidity [Ηλεκτρονική μορφή]
Σύνδεσμος: https://docs.soliditylang.org/en/v0.8.15/

Metamask [Ηλεκτρονική μορφή]
Σύνδεσμος: https://metamask.io/

Consensus Algorithms, (2018). [Ηλεκτρονική μορφή]
Σύνδεσμος: https://medium.com/coinbundle/consensus-algorithms-dfa4f355259d#a76e

Ethereum Merge [Ηλεκτρονική μορφή]
Σύνδεσμος: https://ethereum.org/en/upgrades/merge/

Ethereum Sharding [Ηλεκτρονική μορφή]
Σύνδεσμος: https://ethereum.org/en/upgrades/sharding/

Decentralised application [Ηλεκτρονική μορφή]
Σύνδεσμος: https://en.wikipedia.org/wiki/Decentralized_application

Rinkeby Ether Faucet [Ηλεκτρονική μορφή]
Σύνδεσμος: https://rinkebyfaucet.com/

OpenSea (2019) [Ηλεκτρονική μορφή]
Σύνδεσμος: https://opensea.io/

OpenZeppelin (2019) [Ηλεκτρονική μορφή]
Σύνδεσμος: https://openzeppelin.org/

Βασίλης Παζόπουλος, (2022). «Το επενδυτικό εγχειρίδιο του Bitcoin.» [Χειρόγραφη μορφή]

Greepto, (2021). «Τι είναι το Blockchain.» [Ηλεκτρονική μορφή]
Σύνδεσμος: https://greepto.gr/education/docs/blockchain/ti-einai-blockchain/

Solidity Contract ABI (2021) [Ηλεκτρονική μορφή]
Σύνδεσμος: https://www.quicknode.com/guides/solidity/what-is-an-abi

Remix [Ηλεκτρονική μορφή]
Σύνδεσμος: https://remix-project.org/