**ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ**
**ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ**
**ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ & ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ**

**Διπλωματική Εργασία**

# Υποστήριξη Συστήματος Αξιολόγησης Χρηστών σε ένα Παιχνίδι με Εφαρμογή Μοναδικών Χαρακτηριστικών (NFTs) σε ένα δίκτυο Blockchain


**Φοιτητής: Μιχαήλ Κουκής**
**ΑΜ: 50107058**

**Επιβλέπων/ουσα Καθηγητής/τρια**

**Δημήτριος Γ. Κόγιας, Ph.D**
**Ακαδημαϊκός Υπότροφος / Εντεταλμένος Διδάσκων**

**ΑΘΗΝΑ-ΑΙΓΑΛΕΩ, (Δεκέμβριος) (2023)**

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

# Diploma Thesis

## An NFT-based User Reputation System for an online Blockchain-based Game


**Student: Michail Koukis**
**Registration Number: 50107058**

**Supervisor**

**Dimitrios G. Kogias, Ph.D**
**Adjunct Academic Staf**

**ATHENS-EGALEO, (December) (2023)**

Η Διπλωματική Εργασία έγινε αποδεκτή και βαθμολογήθηκε από την εξής τριμελή επιτροπή:

| Κόγιας Δημήτριος, Ακαδημαϊκός Υπότροφος / Εντεταλμένος Διδάσκων | Πατρικάκης Χαράλαμπος, Καθηγητής | Παπαδόπουλος Περικλής, Καθηγητής |
|---|---|---|
| Dimitrios Kogias Digitally signed by Dimitrios Kogias Date: 2024.04.10 16:42:46 +03'00' | Digitally signed by Charalampos Patrikakis Date: 2024.04.15 11:53:18 +03'00' | Periklis Papadopoulos Digitally signed by Periklis Papadopoulos Date: 2024.04.13 14:48:44 +03'00' |
| (Υπογραφή) | (Υπογραφή) | (Υπογραφή) |

## ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο/η κάτωθι υπογεγραμμένος Μιχαήλ Κουκής του Δημητρίου, με αριθμό μητρώου 50107058 φοιτητής του Πανεπιστημίου Δυτικής Αττικής της Σχολής ΜΗΧΑΝΙΚΩΝ του Τμήματος ΗΛΕΚΤΡΟΛΟΓΩΝ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ,

**δηλώνω υπεύθυνα ότι:**

«Είμαι συγγραφέας αυτής της διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.
Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του διπλώματός μου.
Επιθυμώ την απαγόρευση πρόσβασης στο πλήρες κείμενο της εργασίας μου μέχρι …… και έπειτα από αίτησή μου στη Βιβλιοθήκη και έγκριση του επιβλέποντος καθηγητή.»

Ο Δηλών
Μιχαήλ Κουκής

## Αφιερώσεις

Δίχως πολλά λογία την διπλωματική εργασία την αφιερώνω στην γιαγιά μου την Βικτωρία.

## Ευχαριστίες

Θα ήθελα πρώτα από όλα να ευχαριστήσω τον Κύριο Ιησού Χριστό και Θεό μου που ήταν μαζί μου σε όλη τη διάρκεια της ζωής μου. Το χέρι Του ήταν φανερό και σε όλη τη διάρκεια των σπουδών μου. Με στήριξε, μου έφερε ανθρώπους και σχέσεις που δεν θα υπήρχαν αν δεν ήταν Αυτός. Για αυτό και θα ήθελα πάρα πολύ να ευχαριστήσω αυτούς τους ανθρώπους, τους γονείς, τον αδερφό μου και τον θείο μου με την οικογένεια του (ο θείος ήταν μεγάλη βοήθεια σε όλα αυτά τα χρόνια). Θα ήθελα επίσης, να ευχαριστήσω τους φίλους και τα αδέρφια μου από την εκκλησία αλλά και τους συμφοιτητές μου. Σημαντική θέση κατέχει ο καθηγητής μου Δημήτρης Κόγιας, για την καθοδήγηση, τη στήριξη, την υπομονή και τον χρόνο που με πολλή όρεξη και αγάπη διέθεσε - από τα μαθήματα που τον είχα μέχρι και τη διπλωματική εργασία. Μου έδωσε θάρρος και όρεξη να δω έναν νέο τομέα, τον τομέα του blockchain, κάτι που δίχως τον κ. Κόγια δεν θα γινόταν. Μα πάνω από όλα είμαι ευγνώμων για τη σχέση και τη φιλία που καλλιεργήθηκε κατά το διάστημα αυτό. Τέλος, δεν θα ήθελα να παραλείψω τον Δημήτρη Σταματάκη και τον Γιάννη Χρηστίδη που με βοήθησαν στη διπλωματική εργασία.

## Περίληψη

Σε μια εποχή όπου υπάρχει πληθώρα ψηφιοποιημένων αγαθών, ~~και~~ η ιδιοκτησία τους είναι κρίσιμη, είτε αυτά αντιπροσωπεύουν αντικείμενα στον πραγματικό κόσμο, η ιδιοκτησία ενός σπιτιού λόγου χάρη, είτε στον ψηφιακό, όπως η ιδιοκτησία ενός παίχτη σε ένα παιχνίδι. Αυτό ισχύει και στον τομέα του αθλητισμού, στα φανταστικά παιχνίδια. Η τεχνολογία του blockchain προσπαθεί να αντιμετωπίσει το πρόβλημα της πραγματικής ιδιοκτησίας με διαχείρισή της μέσω των NFTs. Ειδικότερα, η χρήση των NFTs ως εμβλήματα για την κατάταξη των χρηστών αναδεικνύει έναν καινοτόμο τρόπο ανταμοιβής και αναγνώρισης των επιδόσεων σε ένα εικονικό παιχνίδι. Τα NFTs δεν αποτελούν απλώς ψηφιακά διακριτικά σε ένα σύστημα αξιολόγησης. Αντιθέτως, λειτουργούν ως μοναδικές και αυθεντικές ψηφιακές ιδιοκτησίες που αναδεικνύουν τις ικανότητες και τα επιτεύγματα των χρηστών. Με αυτό τον τρόπο, δίνεται έμφαση στην αξία και τη σημασία της εικονικής κοινότητας του παιχνιδιού, αναδεικνύοντας τις ικανότητες και τα επιτεύγματα των χρηστών. Συνοψίζοντας, η εργασία εξετάζει την εφαρμογή της τεχνολογίας blockchain και των NFTs στα φανταστικά παιχνίδια, παρουσιάζοντας έναν τρόπο αξιολόγησης και αναγνώρισης των χρηστών μέσα σε αυτόν τον εικονικό αθλητικό κόσμο.

## Λέξεις – κλειδιά

Αλυσίδα Συστοιχιών, Ethereum,, Έξυπνα Συμβόλαια, Αποκεντρωμένες Εφαρμογές, Μη Ανταλλάξιμο Διακριτικό, ERC-721. Διαδίκτυο 3.0, Φανταστικά αθλητικά παιχνίδια

## Abstract

In the age of digitised goods, ownership is critical, whether they represent objects in the real world, such as the ownership of a house, or in the digital world, such as the ownership of a player in a game. This is also true in the field of sports, in fantasy games. The blockchain technology is trying to address the problem of real ownership and manage them through NFTs. In particular, the use of NFTs as badges to rank users highlights an innovative way of rewarding and recognising performance in a virtual game. NFTs are not just digital Tokens in a rating system. Rather, they function as unique and authentic digital properties that showcase users' abilities and achievements. This emphasizes the value and importance of the virtual game community by highlighting the skills and achievements of users. In summary, the paper examines the application of blockchain technology and NFTs to fantasy games, presenting a way of evaluating and identifying users within this virtual sporting world

## Keywords

Blockchain, Ethereum, Smart Contracts, DApps, NFTs, ERC-721, Web 3.0, Fantasy sports games

## Περιεχόμενα

## Κατάλογος Πινάκων



## Κατάλογος Εικόνων

## Αλφαβητικό Ευρετήριο

NFT: Non-Fungible Tokens

dApps: Decentralized Application

P2P: Peer to Peer

EVM: Ethereum Virtual Machine (EVM)

ETH: Ether

CID: Content Identifier

IPFS: Inter Planetary File System

ERC: Ethereum Request for Comments

# ΕΙΣΑΓΩΓΗ

Πολλοί άνθρωποι είναι θαυμαστές των αθλημάτων, είτε παρακολουθώντας κάποιο άθλημα, είτε ως ενεργοί αθλητές. Μερικοί μπορεί να έχουν και εμφανίσεις των αγαπημένων τους παιχτών ή κάποιας ομάδας ή ακόμα να στοιχηματίζουν σε διάφορους αγώνες και παίχτες. Μερικοί απολαμβάνουν το άθλημα παίζοντας το σε κάποια ηλεκτρονική παιχνιδομηχανή και κάποιοι άλλοι δημιουργούν ομάδες βασισμένοι σε πραγματικούς παίχτες, με αληθινά στατιστικά από τους αγώνες που γίνονται στην καθημερινότητά μας, τα γνωστά και ως παιχνίδια φαντασίας (fantasy game). Το θέμα της διπλωματικής αφορά στην χρήση της τεχνολογίας του blockchain στην κατάταξη των χρηστών που συμμετέχουν στα παιχνίδια φαντασίας. Σε κάθε συμμετέχοντα χρήστη απονέμεται ένα έμβλημα επιτυχίας ανάλογα με τα στατιστικά του στοιχεία στο παιχνίδι. Η χρήση του blockchain σε παιχνίδια φαντασίας ανοίγει νέους ορίζοντες για τη διαφάνεια, την ασφάλεια και την αξιοπιστία στη διαχείριση των στατιστικών στοιχείων και των επιδόσεων των χρηστών. Αυτή η πρωτοποριακή προσέγγιση συνδυάζει την αγάπη για τον αθλητισμό με την καινοτομία του blockchain, δημιουργώντας ένα νέο πεδίο εξερεύνησης και απολαυστικής συμμετοχής στον κόσμο των αθλητικών παιχνιδιών.

## Αντικείμενο της διπλωματικής εργασίας

Το αντικείμενο της διπλωματικής αφορά τη δημιουργία μιας εφαρμογής που λειτουργεί στο διαδίκτυο και χρησιμοποιεί ένα δίκτυο κατανεμημένων κόμβων, όπως είναι το blockchain και το δίκτυο του Ethereum, αντί για έναν κεντρικό διακομιστή (server). Η λειτουργία των εφαρμογών γίνεται με προγράμματα που εκτελούνται αυτόματα και ελέγχουν την εκτέλεση συμφωνιών ή συμβολαίων μεταξύ δύο ή περισσότερων μερών χωρίς την ανάγκη ενδιάμεσων. Αυτά τα προγράμματα καλούνται Έξυπνα Συμβόλαια (Smart Contracts). Ο φοιτητής κλήθηκε να δημιουργήσει ένα Έξυπνο Συμβόλαιο το οποίο να αντιπροσωπεύει τα εμβλήματα (Badges) που αποκτούν οι χρήστες ανάλογα με της επιδόσεις του στο φανταστικό παιχνίδι. Για την απονομή των Badges δημιουργήθηκε ένα σύστημα αξιολόγησης των χρηστών που συμμετέχουν ως παράδειγμα της εφαρμογής, καθώς κάθε εταιρία έχει τα δικά της κριτήρια αξιολόγησης. Η τεχνολογία αυτή δυσκολεύει τυχόν προσπάθειες εισβολής στο παιχνίδι με κακόβουλους σκοπούς καθιστώντας το ασφαλές από απάτες και παράνομες επεμβάσεις, λόγω των προνομίων που προσφέρει το blockchain.

## Σκοπός και στόχοι

Ο σκοπός της εργασίας είναι να γίνει η πρώτη επαφή του αναγνώστη και του φοιτητή με τη νέα τεχνολογία blockchain, τη μελέτη των βασικών χαρακτηριστικών που προσφέρει και την εκμάθηση για τη δημιουργία των Έξυπνων Συμβολαίων και των αποκεντρωμένων εφαρμογών που λειτουργούν στο δίκτυο του Ethereum.

Ο βασικός στόχος είναι η ολοκλήρωση μια αποκεντρωμένης εφαρμογής με προτεραιότητα τη δημιουργία ενός Έξυπνου Συμβολαίου που θα διαχειρίζεται την απονομή εμβλημάτων σε χρήστες των φανταστικών παιχνιδιών. Ταυτόχρονα, χρησιμοποιήθηκαν τεχνολογίες κατάλληλες για τη

δημιουργία ιστοσελίδων, για παράδειγμα μία βάση δεδομένων, όπως γίνεται στο σημερινό διαδίκτυο.

Για την υλοποίηση της εργασίας αυτής χρειάστηκε να αποσαφηνιστούν τα εξής ερωτήματα:

- Τι είναι το blockchain και το web 3.0;
- Πώς συνδέεται με το διαδίκτυο του web 2.0;
- Πώς το blockchain βοηθάει το φανταστικό παιχνίδι;
- Τι τεχνολογίες υπάρχουν και ποιες από αυτές χρειάζονται για την υλοποίηση της αποκεντρωμένης εφαρμογής;
- Πώς γίνεται η υλοποίηση ενός Έξυπνου Συμβολαίου;
- Πώς υλοποιούνται εφαρμογές στο σημερινό διαδίκτυο;

Με την ολοκλήρωση της θα έχει γίνει η δημιουργία της αποκεντρωμένης εφαρμογής (Decentralized Application - dApp), όπου θα αποθηκεύει σε μια βάση δεδομένων τους χρήστες με τα στατιστικά τους στοιχεία κατά την εγγραφή τους στην πλατφόρμα. Θα αποκτούν εμβλήματα (Badges) υπό την μορφή ενός Έξυπνου Συμβολαίου. Η πλατφόρμα θα ανανεώνει τα στατιστικά που υπάρχουν στη βάση δεδομένων και μετά την ανανέωσή της, οι χρήστες θα μπορούν στο τέλος της Αθλητικής Χρονιάς να παραλάβουν το Badge τους ανάλογα με τα κριτήρια αξιολόγησης.

## Μεθοδολογία

Η μεθοδολογία που ακολουθήθηκε είχε τέσσερα στάδια:

1) Εκμάθηση με σκοπό την κατανόηση της τεχνολογίας blockchain για την δημιουργία του Έξυπνου Συμβολαίου
2) Υλοποίηση του Έξυπνου Συμβολαίου
3) Εκμάθηση των τεχνολογιών του web 2.0
4) Υλοποίηση της εφαρμογής με χρήση όλων των τεχνολογιών ώστε να ολοκληρωθεί η αποκεντρωμένη εφαρμογή.

## Καινοτομία

Μια από τις χρήσεις της τεχνολογίας του blockchain στο δίκτυο του Ethereum είναι η δημιουργία των NFTs (Non-Fungible Tokens). Τα NFTs είναι Έξυπνα Συμβόλαια όπου έχουν προγραμματιστεί ώστε να ξεχωρίζουν για τη μοναδικότητα τους. Ένα NFT αντιπροσωπεύει μια μοναδική ψηφιακή περιουσία όπως ένα ψηφιακό έργο τέχνης, ένα βίντεο ή ένα αρχείο. Το blockchain εξασφαλίζει ότι κάθε NFT είναι μοναδικό και αδιαίρετο καθιστώντας αδύνατον για κάποιον άλλον να αντιγράψει ή να παραποιήσει την ιδιοκτησία του. Οι ιδιοκτήτες των NFTs έχουν τον έλεγχο της αυθεντικότητας και της ιστορίας του ψηφιακού αγαθού. Το Έξυπνο Συμβόλαιο που δημιουργήθηκε για τη διπλωματική είχε ως σκοπό τα NFTs να αντιπροσωπεύουν τα εμβλήματα (Badges) που αποκτούν οι χρήστες. Πιο συγκεκριμένα, κάθε χρήστης που αποκτά ένα Badge στο παιχνίδι φαντασίας έχει στην ιδιοκτησία του ένα μοναδικό NFT, αναπαριστώντας μια πραγματική και μη επαναλαμβανόμενη αξία στον εικονικό κόσμο του παιχνιδιού. Το Badge αντιπροσωπεύει την κατάταξη του χρήστη σε ένα σύστημα αξιολόγησης που δημιουργήθηκε σαν παράδειγμα της χρήσης αυτής της τεχνολογίας. Μέσα από αυτήν την προσέγγιση, το παιχνίδι αποκτά ασφαλή φύση, ενθαρρύνοντας τους παίκτες

να επενδύουν χρόνο και πόρους στον εικονικό κόσμο του, ενώ παράλληλα προσφέρει στην εταιρία ένα αξιόπιστο περιβάλλον λειτουργίας.

## Δομή

Αρχικά, στο 1ο Κεφάλαιο παρουσιάζεται το Blockchain, ξεκινώντας με μια εισαγωγή και τα βασικά χαρακτηριστικά του. Στο κεφάλαιο αυτό δίνεται έμφαση στο Ethereum καθώς σε αυτό το δίκτυο υλοποιήθηκε η διπλωματική. Αναπτύσσονται με λίγα λόγια οι τρόποι και τι απαιτείται για την αλληλεπίδραση με το δίκτυο του Ethereum, όπως τι είναι τα πορτοφόλια (wallets), το νόμισμα του Ethereum -το Ether- σε συνδυασμό με το Gas, ενώ δίνεται έμφαση στις αποκεντρωμένες εφαρμογές (dApps) και στο Web 3.0 με τη χρήση Έξυπνων Συμβολαίων (Smart Contracts). Επίσης, γίνεται μια παρουσίαση των βασικών Tokens και των χαρακτηριστικών τους, καθώς χρησιμοποιήθηκε ένα από αυτά για την εκπόνηση της διπλωματικής εργασίας. Ολοκληρώνοντας το κεφάλαιο ο αναγνώστης θα έχει μια γενική ιδέα και τις απαραίτητες γνώσεις για να κατανοήσει την εφαρμογή.

Προχωρώντας στο 2ο Κεφάλαιο, γίνεται η παρουσίαση της εφαρμογής, αναπτύσσεται τι είναι τα φανταστικά παιχνίδια (fantasy games) και παρουσιάζονται τα διάφορα είδη παιχνιδιών που υπάρχουν. Το κεφάλαιο συνεχίζει με την ανάλυση κάποιων κριτηρίων που χρησιμοποιήθηκαν για τη δημιουργία του συστήματος αξιολόγησης των χρηστών έχοντας ως βάση έναν από τους τύπους παιχνιδιών που προαναφέρθηκαν. Για καλύτερη κατανόηση δίνεται ένα παράδειγμα όπου συμμετέχουν κάποιοι χρήστες, το οποίο είναι βασισμένο στον τύπο του παιχνιδιού και στα κριτήρια αξιολόγησης, με σκοπό να εφαρμοστεί το σύστημα αξιολόγησης και οι χρήστες να ανταμειφθούν με ένα έμβλημα. Έτσι, με το παράδειγμα γίνεται κατανοητή η χρήση των NFTs που χρησιμοποιούνται ως απονομή εμβλημάτων.

Έπειτα, στο 3ο Κεφάλαιο παρουσιάζονται τα εργαλεία που χρησιμοποιήθηκαν για την υλοποίηση του dApp. Συγκεκριμένα, αναφέρονται η Open Zeppelin και το Remix για την υλοποίηση του Έξυπνου Συμβολαίου (Smart Contract). Επίσης, χρησιμοποιήθηκε η αρχιτεκτονική MERN Stack για την υλοποίησή του front end και του υπολοίπου back end. Παράλληλα, αναφέρονται μερικά λόγια για την τεχνολογία Hardhat καθώς είναι αναγκαία για την υλοποίηση του dApp. Για κάθε εργαλείο δίνονται επαρκείς λεπτομέρειες, ώστε ο αναγνώστης να έχει μια πλήρη εικόνα για τον σκοπό επιλογής του κάθε εργαλείου στην εφαρμογή. Η εφαρμογή αποτελείται από διάφορες τεχνολογίες, για τις οποίες δίνονται οι απαιτούμενες πληροφορίες.

Στο 4ο Κεφάλαιο παρουσιάζεται η υλοποίηση της εφαρμογής. Εκεί δίνονται διευκρινήσεις για τη λειτουργία της εφαρμογής με το ενδιαφέρον να εστιάζεται στη λογική και όχι στον τρόπο δημιουργίας της από προγραμματιστική σκοπιά. Κατά την ανάλυση της εφαρμογής γίνεται χρήση του παραδείγματος που αναπτύχθηκε στο 2ο Κεφάλαιο. Η αρχή γίνεται με την ανάλυση του Έξυπνου Συμβολαίου, δηλαδή του NFT. Αυτό σημαίνει ότι αναφέρονται τόσο οι σημαντικές συναρτήσεις, όπως είναι η απόκτηση ενός Badge, αλλά και η αποθήκευση των εικόνων μέσω του IPFS στην Pinata. Έπειτα, το κεφάλαιο συνεχίζει με την υλοποίηση του MERN Stack δηλαδή της βάσης δεδομένων, του Server για το back end και το front end που αλληλεπιδρά με το Έξυπνο Συμβόλαιο (Smart Contract) και του server με τη βάση δεδομένων. Ταυτόχρονα, στην υλοποίηση του front end δίνεται ένα παράδειγμα της ολοκληρωμένης αποκεντρωμένης εφαρμογής ώστε ο χρήστης να έχει πλήρη εικόνα για το πώς χρησιμοποιείται η εφαρμογή.

Ολοκληρώνοντας, στον επίλογο παρουσιάζονται τα συμπεράσματα της διπλωματικής εργασίας και επιπλέον προσθήκες και αλλαγές που μπορούν να γίνουν στην εφαρμογή μελλοντικά.

# 1 ΚΕΦΑΛΑΙΟ 1ο : Τεχνολογία blockchain

Το 2008 δημιουργήθηκε το (πρωτόκολλο) Bitcoin, ένα ψηφιακό νόμισμα, από τον Satoshi Nakamoto [12]. Στη δημοσίευσή του αναφέρεται με ποιόν τρόπο στο Bitcoin γίνονται συναλλαγές σε ένα κατανεμημένο δίκτυο ομότιμων κόμβων (Peer to Peer, P2P). Άλλα σημαντικά χαρακτηριστικά του δικτύου αυτού είναι η κρυπτογραφία και η αποκεντροποίηση. Αυτή ήταν η αρχή της χρήσης τεχνολογίας του blockchain. Μετά από μερικά χρονιά (2013) δημιουργήθηκε το (πρωτόκολλο) Ethereum [13] από τον Vitalik Buterin οπού χρησιμοποιεί την τεχνολογία αυτή (blockchain) με κάποια ακόμα χαρακτηριστικά. Οι χρήστες μπορούν να κάνουν όχι μόνο αποκεντροποιημένες συναλλαγές αλλά και αποκεντροποιημένες συμφωνίες (Smart Contracts). Στη συνέχεια θα αναπτυχθούν τα χαρακτηριστικά του blockchain και θα δοθούν περισσότερες λεπτομέρειες σχετικά με το Ethereum.

## 1.1 Χαρακτηριστικά του blockchain

- Αποκεντροποίηση (Decentralization): Η λειτουργία του είναι χωρίς κάποια κεντρική αρχή ελέγχου. Όλες οι συναλλαγές που γίνονται επιβεβαιώνονται και αποθηκεύονται στο δίκτυο κόμβων (nodes). Όπως αναφέρθηκε στην εισαγωγή είναι ένα P2P δίκτυο.
- Συναίνεση (Consensus): Είναι η διαδικασία που γίνεται μεταξύ των κόμβων για την εγκυρότητα της συναλλαγής.
- Διαφάνεια (Transparency): Οι συναλλαγές στο δίκτυο είναι δημόσιες. Με αυτό μπορούμε να διασφαλίσουμε την εγκυρότητα τους καθώς γίνεται η συναίνεση / επιβεβαίωση. Όλοι έχουν την ίδια πληροφορία καθώς και την ίδια εικόνα
- Μοναδικότητα, Μονιμότητα (Immutable): Όταν γίνουν οι συναλλαγές και κατοχυρωθούν στο blockchain, είναι αδύνατον να αλλάξουν ή να τροποποιηθούν. Αυτό εξασφαλίζεται από τη χρήση κρυπτογραφίας και τη μη δυνατότητα αναίρεσης των επιβεβαιωμένων συναλλαγών.
- Ασφάλεια: Είτε από την οπτική γωνία των συναλλαγών που είναι κρυπτογραφημένες και αδιαλείπτως αποθηκευμένες (ledger), είτε ως προς την λειτουργία του δικτύου, καθώς σε ενδεχόμενο πτώσης ενός κόμβου, το δίκτυο συνεχίζει να λειτουργεί κανονικά ή σε περίπτωση που κάποιος θα ήθελε να πάρει τον έλεγχο του blockchain, θα χρειαζόταν να έχει υπό τον έλεγχο του τους μίσους και περισσοτέρους nodes.

Στον κόσμο των οικονομικών το μέρος όπου καταγράφονται όλες οι συναλλαγές ονομάζεται κεντρικό λογιστικό βιβλίο. Επίσης, ελέγχεται από μια κεντρική αρχή, λόγου χάρη μια τράπεζα. Στο blockchain, όπως αναφερθήκαμε, δεν υπάρχει αυτή η οντότητα καθώς είναι αποκεντρωμένο. Παρόλα αυτά, όλες οι συναλλαγές που γίνονται καταγράφονται. Το λογιστικό φίλο στο blockchain λέγεται ledger. Στο Ledger είναι κοινές όλες οι συναλλαγές για όλους τους χρήστες. Δηλαδή κάθε χρήστης έχει το δικό του αντίγραφο το οποίο ενημερώνεται συνεχώς με κάθε νέα συναλλαγή. Οι κόμβοι στο blockchain χρησιμοποιούν τις τεχνικές της κατανεμημένης συναίνεσης για να επαληθεύουν και να ενημερώνουν το ledger με τις νέες συναλλαγές.

Οι εκτελούμενες συναλλαγές διαχωρίζονται χρονολογικά και συλλέγονται σε ομάδες που ονομάζονται blocks. Στη συνέχεια, αυτές οι ομάδες συναλλαγών συνδέονται μεταξύ τους με

κρυπτογραφικό τρόπο για να δημιουργήσουν μια αλυσίδα. Κάθε νέο block προστίθεται στην αλυσίδα χωρίς δυνατότητα μελλοντικής αφαίρεσης. Επομένως, ό,τι προστεθεί στο blockchain δεν μπορεί να αφαιρεθεί, ενώ κάθε προσθήκη γίνεται σε συγκεκριμένο χρόνο και πάντα καταλήγει στο τέλος της αλυσίδας [11].

Για την πραγματοποίηση μια συναλλαγής απαιτείται η χρήση ενός πορτοφολιού. Το πορτοφόλι έχει μια διεύθυνση και ένα ιδιωτικό κλειδί. Η διεύθυνση είναι φανερή σε όλους του χρήστες και με αυτή γίνονται οι συναλλαγές. Όμως, το ιδιωτικό κλειδί πρέπει να παραμένει απολυτό μυστικό από τους υπόλοιπους χρήστες καθώς χρησιμοποιείται για να υπογραφούν οι συναλλαγές επιβεβαιώνοντας την ιδιοκτησία των ψηφιακών περιουσιακών στοιχείων. Περαιτέρω ανάλυση θα γίνει σε άλλη παράγραφο.

Συνεπώς, ως ορισμός του blockchain θα μπορούσε να δοθεί ότι είναι ένας αποκεντρωμένος αποθηκευτικός και δημόσιος καταμερισμός δεδομένων που χρησιμοποιεί κρυπτογραφία για την εξασφάλιση της ασφάλειας των συναλλαγών. Συγκεντρώνει τις συναλλαγές σε block και δημιουργεί μια αλυσίδα των εν λόγω block έχοντας ένα αναλλοίωτο ιστορικό από όλες τις εκτελεσθείσες συναλλαγές.

Παρόλα αυτά υπάρχουν και κάποια μειονεκτήματα στην τεχνολογία που αξίζει να αναφερθούν.

- Κόστος. Τόσο αυτό που αφορά στην υλοποίηση του Blockchain ως δίκτυο με τις υποδομές του, όσο και αυτό που αναφέρεται στις συναλλαγές με τους υπολογιστικούς πόρους και την ενέργεια που χρειάζονται.
- Ιδιωτικά κλειδιά. Σε περίπτωση απώλειάς τους μπορεί να χαθεί και η πρόσβαση στο πορτοφόλι του χρήστη.

## 1.2 Ethereum

Στην διπλωματική αυτή ως blockchain χρησιμοποιήθηκε το Ethereum. Για αυτόν τον λόγο δεν θα γίνει ανάλυση του Bitcoin και θα αναπτυχθούν κυρίως τα χαρακτηριστικά του Ethereum.

### 1.2.1 Εισαγωγή

Ο σκοπός της δημιουργίας του Ethereum είναι να δημιουργήσει ένα αποκεντρωμένο υπολογιστικό περιβάλλον γενικού σκοπού όπου δίνει τη δυνατότητα εκτέλεσης προγραμμάτων ή αλλιώς Έξυπνων Συμβολαίων (Smart Contracts) και τη δημιουργία αποκεντρωμένων εφαρμογών (Decentralized Applications - DApps). Η εκτέλεση των Smart Contracts και η δημιουργία των DApps γίνεται χωρίς την ανάγκη ενδιάμεσων. Για την επίτευξη του σκοπού αυτού, για την παρακολούθηση και τη διατήρηση της συνολικής κατάστασης του χρησιμοποιείται η τεχνολογία blockchain.

Για να γίνει αυτό απαιτείται η συμφωνία και ο συγχρονισμός όλων των μελών του δικτύου σχετικά με την τρέχουσα κατάσταση, την επαλήθευση και την αποθήκευση των αλλαγών κατάστασης μέσω της τεχνολογίας blockchain και του κρυπτονομίσματος ether.

Έτσι, το Ethereum διαχειρίζεται τις καταστάσεις καθώς αποθηκεύονται οι συναλλαγές στα διαδοχικά blocks. Με τη χρήση του ether εκτελούνται τα Smart Contracts και στις ανταλλαγές μεταξύ των μελών του δικτύου. Με τη διαδικασία αυτή καταγράφονται οι αλλαγές στις καταστάσεις και μπορούν να επαληθευθούν από όλα τα μέλη του δικτύου.

Η μηχανή αυτή λέγεται Ethereum Virtual Machine (EVM).

### 1.2.2 Ethereum Virtual Machine (EVM)

Όπως προαναφέρθηκε, το Ethereum Virtual Machine (EVM) είναι μηχανή που παρακολουθεί, επιβεβαιώνει τις αλλαγές στην κατάσταση του συστήματος στο δίκτυο και είναι ενεργό σε πολλούς κόμβους ταυτόχρονα. Σε αυτό γίνεται η εκτέλεση των Smart Contracts. Συγκεκριμένα, γίνεται η μετατροπή του κώδικα σε μορφή bytecodes ώστε να μπορεί να εκτελεστεί. Η μορφή αυτή επιτρέπει σε όλους του κόμβους του δικτύου να μπορούν να εκτελέσουν το Smart Contract και να επαληθεύουν τις ενέργειές του, χωρίς να απαιτείται εμπιστοσύνη σε ένα κεντρικό κόμβο ή αρχή.

### 1.2.3 Smart Contracts

Τα Smart Contracts είναι ένα σύνολο εντολών που εκτελούνται με αποκεντρωμένο τρόπο χωρίς την ανάγκη κεντρικού ή τρίτου διαμεσολαβητή.

Αν μπορεί να συγκριθεί με κάτι στον πραγματικό κόσμο, αυτό θα ήταν τα συμβόλαια που λογίζονται ως υποσχέσεις αδύνατον να καταπατηθούν. Η διαφορά είναι ότι αντί να γίνουν εγγράφως, γίνονται μέσω μιας υψηλού επιπέδου γλώσσας προγραμματισμού. Η πιο διαδεδομένη τέτοια γλώσσα ονομάζεται Solidity καθώς έχει δημιουργηθεί για τον σκοπό αυτό. Άλλες γλώσσες προγραμματισμού που μπορούν να γράψουν Smart Contracts είναι η Rust, JavaScript, Viper και Yul. Στη διπλωματική αυτή η συγγραφή του Smart Contract έγινε με τη χρήση της Solidity.

Όταν ένα Smart Contract αναρτηθεί στο δίκτυο του blockchain δεν μπορεί να τροποποιηθεί (είναι αμετάβλητο, immutable), εκτελείται αυτόματα και όλοι μπορούν να δουν τους ορούς της συμφωνίας. Μόλις ενταχθούν στο δίκτυο αποκτούν μια διεύθυνση. Κάθε Smart Contract έχει την δική του διεύθυνση η οποία είναι διαφορετική σε κάθε δίκτυο.

Παρόλο που τα Smart Contracts έχουν διεύθυνση δεν μπορούν να κάνουν συναλλαγές. Η χρήση της διεύθυνσης είναι είτε για την αποστολή και αποθήκευση χρήματων σε αυτό, είτε για να καλούνται συναρτήσεις. Επίσης τα Smart Contracts έχουν την ικανότητα να επικοινωνήσουν και να εκτελέσουν συναρτήσεις από αλλά Smart Contracts. Αυτό είναι ένα από τα χαρακτηριστικά που χρησιμοποιήθηκαν στη δημιουργία του Smart Contract και θα γίνει η αναφορά στο κεφάλαιο 4.

Όπως αναφέρθηκε, όταν το Smart Contract ενταχθεί στο δίκτυο δεν μπορεί να αλλάξει το περιεχόμενο του. Αυτό σημαίνει πως σε οποιαδήποτε περίπτωση που χρειάζεται να γίνει αλλαγή στο Smart Contract θα χρειαστεί να γίνει από την αρχή η διαδικασία. Όταν ολοκληρωθούν οι αλλαγές στο Smart Contract και αναρτηθεί στο δίκτυο, τότε αποκτά νέα διεύθυνση οπότε απαιτείται να ρυθμιστούν όλες οι αποκεντρωμένες εφαρμογές που αναφέρονταν στην παλιά διεύθυνση και να παραπέμπουν στη νέα διεύθυνση.

Κάθε Smart Contract για να μπει σε οποιοδήποτε δίκτυο (είτε είναι δίκτυο δοκιμών είτε είναι κύριο δίκτυο) χρειάζεται ο ιδιοκτήτης του Smart Contract να πληρώσει ένα ποσό gas με τη χρήση των ethers (είναι το κρυπτονόμισμα στο δίκτυο του Ethereum). Αν δεν πληρωθεί το ποσό, τότε δεν θα γίνει η ανάρτηση του Smart Contract στο δίκτυο. Εκτός από την ανάρτηση του Smart Contract, πρέπει να γίνει πάλι η πληρωμή ενός ποσού από τον χρήστη στην εφαρμογή όταν καλείται μια συνάρτηση που γράφεται στο blockchain.

Στη συνέχεια του κεφαλαίου θα αναπτυχθούν οι λόγοι που χρειάζεται το gas και στο κεφάλαιο 4 θα γίνει κατανοητή η διαφορά, καθώς επίσης και σε ποιες συναρτήσεις χρειάζεται ο χρήστης να πληρώσει και σε ποιες όχι.

### 1.2.4 Ether και GAS

Το νόμισμα στο δίκτυο του Ethereum είναι το Ether με συντομογραφία ETH.

Εκτός από τη χρήση που αναφέρθηκε για το gas, χρησιμοποιείται σε συναλλαγές μεταξύ των χρηστών αλλά και για την αγορά NFTs.

Στην Εικόνα 1 [1] παρουσιάζεται το Eth με τις διάφορες υποδιαιρέσεις του.

| Τιμή (σε Wei) | Εκθέτης | Ονομασία | Ονομασία σε SI |
|---|---|---|---|
| 1 | 1 | Wei | Wei |
| 1.000 | $10^3$ | Babbage | Kilo Wei |
| 1.000.000 | $10^6$ | Lovelace | Mega Wei |
| 1.000.000.000 | $10^9$ | Shannon | Giga Wei |
| 1.000.000.000.000 | $10^{12}$ | Szabo | Microether |
| 1.000.000.000.000.000 | $10^{15}$ | Finney | Milliether |
| 1.000.000.000.000.000.000 | $10^{18}$ | Ether | Ether |
| 1.000.000.000.000.000.000.000 | $10^{21}$ | Grand | Kiloether |
| 1.000.000.000.000.000.000.000.000 | $10^{24}$ | - | Megaether |

**Εικόνα 1 Οι υποδιαιρέσεις του ether (ETH).**

Για την πιο εύκολη κατανόηση του gas, αυτό μπορεί να συγκριθεί με τη βενζίνη που χρειάζεται το αυτοκίνητο για να κινηθεί. Αν δεν έχει βενζίνη, τότε ο οδηγός οφείλει να αγοράσει βενζίνη για να κινηθεί. Αυτό ακριβώς συμβαίνει και στο Ethereum, όσο ο χρήστης έχει ETH για να πληρώνει gas τόσο θα μπορεί να κάνει ενέργειες στο δίκτυο.

Άρα, το gas είναι ένα μέτρο υπολογιστικού κόστους που απαιτείται για να εκτελεστεί μια ενέργεια ή μια συναλλαγή. Αντιπροσωπεύει την ποσότητα επεξεργαστικής ισχύος, μνήμης και χρόνου που απαιτούνται για να ολοκληρωθεί μια ενέργεια στο δίκτυο.

Οι λόγοι που χρειάζεται το gas:

- Για τη δυνατότητα διακοπής εκτέλεσης ενός προγράμματος που βρίσκεται σε ατέρμονα βρόγχο επανάληψης.
- Για οικονομική διαχείριση του δικτύου. Όπως αναφέρθηκε, κάθε ενέργεια που εκτελείται κοστίζει ETH και οι χρήστες χρειάζεται να πληρώσουν gas. Αυτό δημιουργεί ένα οικονομικό κίνητρο για την αποφυγή της σπατάλης πόρων του δικτύου.

### 1.2.5 Wallets

Για να περιηγηθεί ένας χρήστης στο δίκτυο απαιτείται να έχει ένα πορτοφόλι. Αυτό περιλαμβάνει μια διεύθυνση και ένα ζευγάρι ιδιωτικού/δημόσιου κλειδιού τα οποία φυλάσσονται ασφαλώς στα πορτοφόλια. Το δημόσιο κλειδί είναι γνωστό σε όλους και χρησιμοποιείται για τη δημιουργία της διεύθυνσης του πορτοφολιού. Με τη διεύθυνση του πορτοφολιού γίνεται η λήψη ETH. Αντιθέτως, το ιδιωτικό κλειδί είναι απολυτά μυστικό και χρησιμοποιείται για την υπογραφή συναλλαγών.

Η δημιουργία τους είναι σημαντική γιατί:

1)Αποθηκεύουν και διαχειρίζονται το Eth.

2)Γίνεται η αλληλεπίδραση με τα Smart Contracts.

Τα κύρια χαρακτηριστικά των πορτοφολιών στο Ethereum είναι τα εξής:

- Είναι σχεδιασμένα για να είναι χρηστικά και φιλικά προς τον χρήστη
- Το ιδιωτικό κλειδί είναι απαραίτητο για την υπογραφή συναλλαγών και πρέπει να προστατεύεται προσεκτικά.

- Οι συναλλαγές στο Ethereum είναι γρήγορες και μπορούν να πραγματοποιηθούν ανά πάσα στιγμή.
- Τα κόστη συναλλαγής στο Ethereum είναι συνήθως χαμηλά σε σύγκριση με παραδοσιακά χρηματοοικονομικά συστήματα.
- Κάποια πορτοφόλια επιτρέπουν την πρόσβαση και τη διαχείριση πολλών κρυπτονομισμάτων και δικτύων blockchain.

Ένα από τα πιο διαδομένα πορτοφόλια στο δίκτυο του Ethereum είναι το Metamask [2] με το οποίο και έγινε η αλληλεπίδραση με το Smart Contract.

Αξίζει να σημειωθεί πως στο Metamask, εκτός από το κυρίως δίκτυο του Ethereum, υπάρχουν και δοκιμαστικά δίκτυα. Στο πλαίσιο της διπλωματικής έγινε μέσω του τοπικού δικτύου που παρέχει το Hardhat, για το οποίο θα δοθούν περισσότερες λεπτομέρειες στο κεφάλαιο της υλοποίησης.

## 1.3 Web 2.0, Web 3.0 και DApps.

### 1.3.1 Web 2.0

Το Web 2.0 και Web 3.0 είναι όροι που περιγράφουν διάφορα επίπεδα εξέλιξης του internet.

Το Web 2.0 είναι η παρούσα εκδοχή του internet όπου χαρακτηρίζεται από την κεντρική αρχιτεκτονική και τις κεντρικές υπηρεσίες καθώς σε αυτές αποθηκεύονται τα δεδομένα. Είναι η έκδοση του διαδικτύου που εστιάζει στην αλληλεπίδραση, τη συνεργασία και την κινητικότητα των χρηστών. Έχει επιφέρει σημαντικές αλλαγές στην εφαρμογή, το περιεχόμενο και τη χρήση του. Σημαντικά παραδείγματα είναι το Facebook και το Twitter.

Τα κύρια χαρακτηριστικά που το απαρτίζουν είναι τα εξής:

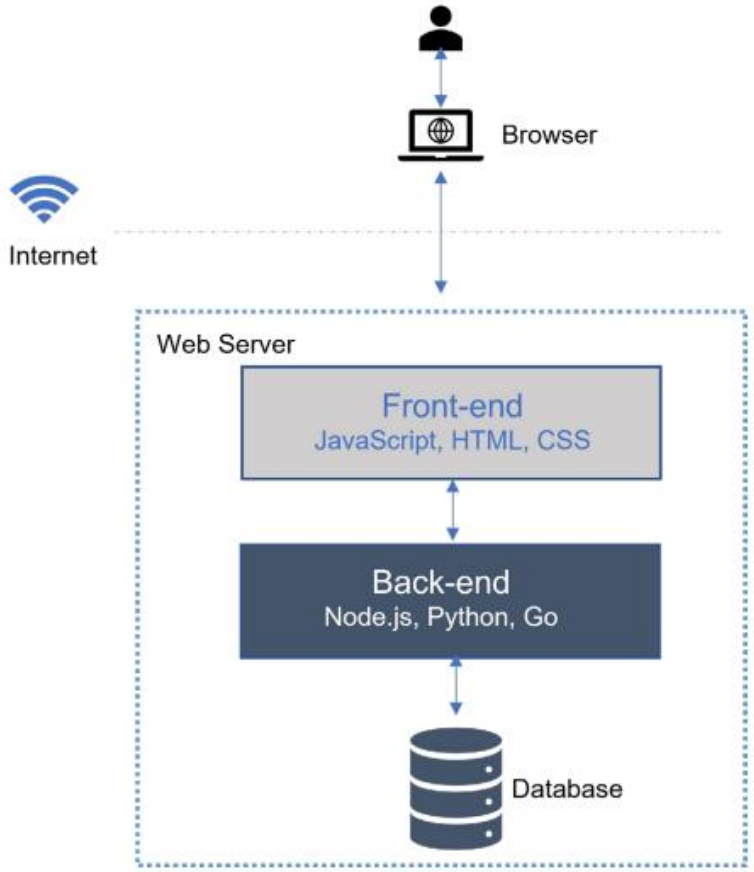
- Το περιεχόμενο δεν είναι στατικές σελίδες. Αντιθέτως, οι χρήστες μπορούν να συμμετέχουν ενεργά, να αλληλεπιδρούν με το περιεχόμενο και να δημιουργούν περιεχόμενο.
- Τα μέσα κοινωνικής δικτύωσης αποτέλεσαν ένα από τα μεγαλύτερα άλματα στο Web 2.0, με χαρακτηριστικό το παράδειγμα του Facebook. Οι χρήστες έχουν τη δυνατότητα σύνδεσης, επικοινωνίας και διαμοιρασμού πληροφορίας μεταξύ τους.
- Οι χρήστες μπορούν επίσης να δημιουργούν, να επεξεργάζονται και να μοιράζονται περιεχόμενο στο διαδίκτυο. Αυτό περιλαμβάνει βίντεο, φωτογραφίες, κριτικές και άλλα.
- Εμφανίστηκαν νέες υπηρεσίες και εφαρμογές που εκμεταλλεύονται την αλληλεπίδραση των χρηστών συλλέγοντας δεδομένα από αυτούς για να προσφέρουν προσαρμοσμένο περιεχόμενο, όπως προτάσεις για αγορές, επιλογές μέσων ενημέρωσης και πολλά άλλα.

Η δημιουργία τέτοιων εφαρμογών πραγματοποιείται μέσα από γλώσσες προγραμματισμού. Χωρίζονται σε δυο στάδια: το back-end και το front-end. Το front-end είναι υπεύθυνο για το περιβάλλον που αλληλεπιδρά ο χρήστης καθώς λειτουργεί ως διεπαφή μεταξύ αυτού και του λογισμικού. Περιλαμβάνει τα γραφικά, τον σχεδιασμό, τα κουμπιά, τις φόρμες και άλλα στοιχεία που ο χρήστης βλέπει και χρησιμοποιεί. Μερικές από τις βασικές γλώσσες προγραμματισμού είναι η HTML ως «σκελετός», η CSS ως αρμόδια για την εμφάνιση, η JavaScript που χρησιμοποιείται για τη διαδραστικότητα, η React η οποία αποτελεί το πιο διαδεδομένο framework που υλοποιήθηκε από την Facebook και αντίστοιχα η Angular από την Google.

Από την άλλη, το back-end είναι το μέρος της εφαρμογής που δεν είναι ορατό για τον τελικό χρήστη. Περιλαμβάνει τον διακομιστή (server), τη βάση δεδομένων (DB), τη λογική της εφαρμογής και τη διαχείριση των δεδομένων. Αναλαμβάνει την επεξεργασία των αιτημάτων των χρηστών, την

αποθήκευση και τη διαχείριση των δεδομένων στη βάση δεδομένων, την εκτέλεση της λογικής και την αποστολή αποτελεσμάτων πίσω στο front-end. Συνήθως, η γλώσσα προγραμματισμού που χρησιμοποιείται είναι μία από τις Node.js, Python ή JAVA και η πρόσβαση στα δεδομένα συνήθως γίνεται μέσω πρωτοκόλλων όπως το HTTP (Hypertext Transfer Protocol).

Στην Εικόνα 2 [1] παρουσιάζεται η αρχιτεκτονική μιας εφαρμογής στο Web2.0 καθώς και η σειρά εκτέλεσης κάθε φορά που ο χρήστης αλληλεπιδρά μαζί της.




**Εικόνα 2: Η αρχιτεκτονική μιας Web 2.0 εφαρμογής.**

Κάποια μειονεκτήματα που εμφανίζει αυτή η αρχιτεκτονική και βασικά χαρακτηριστικά του Web 2.0 είναι ο κίνδυνος απώλειας δεδομένων, η περιορισμένη ανθεκτικότητα σε αποτυχίες και η εξάρτηση από εταιρείες παροχής υπηρεσιών.

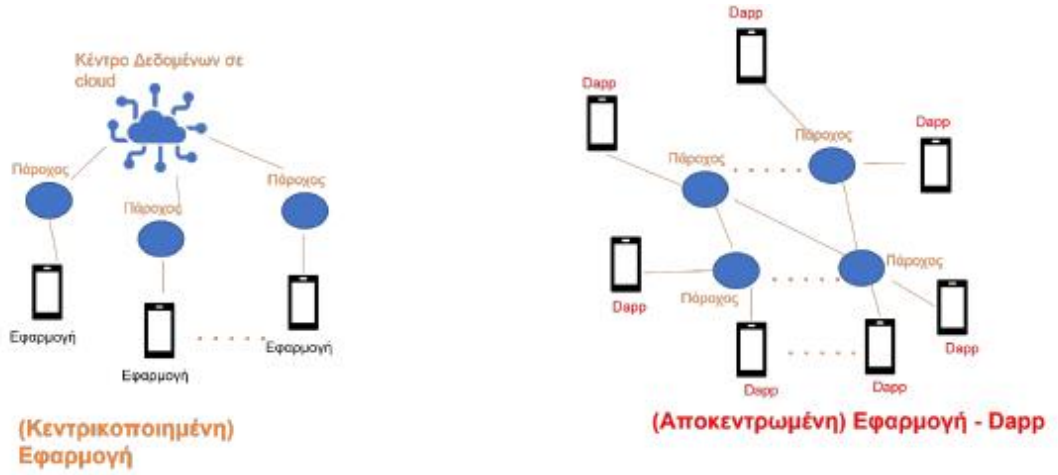
### 1.3.2 Web 3.0

Το Web 3.0 από την άλλη στοχεύει στη δημιουργία ενός αποκεντρωμένου και πιο ανοικτού διαδικτύου με χρήση της τεχνολογίας blockchain και άλλων αποκεντρωμένων τεχνολογιών. Στο Web 3.0 τα δεδομένα και οι λειτουργίες αποθηκεύονται και εκτελούνται από διακομιστές που βασίζονται σε blockchain και κόμβους. Λόγω της τεχνολογίας blockchain, τα δεδομένα είναι ανοικτά και δημοσίως επαληθεύσιμα, αφενός μειώνοντας τον κίνδυνο απάτης και αφετέρου αυξάνοντας την εμπιστοσύνη. Το γεγονός αυτό αποτελεί μια σημαντική διαφορά σε σχέση με το Web 2.0 όπου εκεί, οι χρήστες παραχωρούν τα δεδομένα τους σε μεγάλες εταιρείες έχοντας

περιορισμένο έλεγχο. Στο Web 3.0, οι χρήστες διατηρούν τον έλεγχο των προσωπικών τους δεδομένων και μπορούν να ανακτούν την ιδιοκτησία τους. Μια καινοτομία του Web 3.0 είναι η εισαγωγή των κρυπτονομισμάτων και των NFTs , επιτρέποντας τη δημιουργία ψηφιακών περιουσιακών στοιχείων και την ανταλλαγή τους μεταξύ χρηστών. Επίσης, είναι το μέρος χρήσης των Smart Contracts που εκτελούν αυτόματα συμφωνίες και συναλλαγές, χωρίς την ανάγκη ενδιάμεσων μεσολαβητών. Υπάρχουν και έτερα χαρακτηριστικά του Web 3.0, όμως η έμφαση θα δοθεί στις αποκεντρωμένες εφαρμογές (Decentralized Applications – DApps) και τα NFTs.

### 1.3.3 Decentralized Applications

Οι αποκεντρωμένες εφαρμογές (Decentralized Applications – DApps) είναι εφαρμογές που λειτουργούν πάνω σε ένα blockchain, στην προκειμένη περίπτωση στο Ethereum, αντί να βασίζονται και να βρίσκονται σε κεντρικούς διακομιστές (Εικόνα 3 [1]).




**Εικόνα 3: Σύγκριση μια εφαρμογής στο Web 2.0 με μια εφαρμογή στο Web 3.0**

Αυτές οι εφαρμογές αξιοποιούν την τεχνολογία blockchain για παροχή διαφάνειας, καθώς οι συναλλαγές και οι ενέργειες στο DApp είναι διαθέσιμες προς έλεγχο και επιβεβαίωση στο blockchain. Επίσης, επιτυγχάνεται ασφάλεια και αποκεντρωμένος έλεγχο για τους χρήστες μιας και ο κώδικας και τα δεδομένα αποθηκεύονται στο blockchain και όχι σε κεντρικούς υπολογιστές.

Ο χρήστης αλληλεπιδρά με μια DApp μέσω front-end που δημιουργείται με μια από τις ήδη υπάρχουσες γλώσσες στο Web 2.0 (HTM, CSS, JavaScript). Για την επίτευξη σύνδεσης με το δίκτυο του Ethereum και το Smart Contract απαιτείται η βιβλιοθήκη ether.js ή web3.js (στην παρούσα διπλωματική έγινε χρήση της ether.js). Το Smart Contract θεωρείται το back-end καθώς σε αυτό υλοποιείται η εφαρμογή και ανεβαίνει στο δίκτυο κατόπιν πληρωμής του gas.

Η βασική διαφορά στο Web 3.0 βρίσκεται στο back-end της αρχιτεκτονικής, όπου τα δεδομένα δεν αποθηκεύονται πλέον σε έναν κεντρικό διακομιστή, αλλά σε ένα σύνολο από κόμβους που συμμετέχουν εξίσου στο δίκτυο. Αυτή η αποκέντρωση εξαλείφει τον κεντρικό διακομιστή ως ενδιάμεσο παράγοντα, ενώ η επικοινωνία γίνεται απευθείας με το δίκτυο του blockchain.

Στο πλαίσιο του Web 3.0, η μηχανή Ethereum Virtual Machine (EVM) είναι κρίσιμης σημασίας, καθώς χρειάζεται για την αποθήκευση αλλαγών στα Smart Contracts. Τα Smart Contracts αποτελούν τον πυρήνα του back-end, υλοποιώντας ενέργειες από το front-end. Κάθε κόμβος

αναλαμβάνει την αποθήκευση των Smart Contracts, με αυστηρούς κανόνες συναίνεσης στο κατανεμημένο δίκτυο.

Ο χρήστης αλληλεπιδρά με το Smart Contract μέσω ενός πορτοφολιού, όπως το Metamask [2]. Όταν ο χρήστης καλεί ένα Smart Contract, η εφαρμογή συνδέεται σε έναν κόμβο, ο οποίος εκτελεί την ενέργεια και ενημερώνει τους υπόλοιπους κόμβους. Η επικοινωνία μπορεί να γίνει μέσω υπηρεσιών τρίτων (π.χ., Alchemy [3]) ή με τη δημιουργία και στήριξη ενός κόμβου που ανήκει στον χρήστη.

Η αλληλεπίδραση μεταξύ χρήστη και κόμβου γίνεται μέσω του παρόχου (provider), ενώ το Metamask διαδραματίζει καίριο ρόλο ως πορτοφόλι και, ενδεχομένως, ως πάροχος.

Στο Web 3.0, η αποθήκευση δεδομένων γίνεται σε αποκεντρωμένα συστήματα όπως το IPFS και το blockchain. Τα δεδομένα αποθηκεύονται στο ledger, αλλά η συνεχής αύξηση του μεγέθους του επηρεάζει την απόδοση του δικτύου. Ως λύση, χρησιμοποιείται το IPFS, το οποίο διατηρεί μόνο τη θέση των δεδομένων, ενώ τα ίδια αποθηκεύονται εκτός blockchain με χρήση μοναδικού αναγνωριστικού περιεχομένου (CID).

### 1.3.4 IPFS

Το IPFS [4] είναι ένα αποκεντρωμένο πρωτόκολλο αποθήκευσης και διανομής αρχείων που έχει σχεδιαστεί για να αντικαταστήσει το παραδοσιακό μοντέλο HTTP του διαδικτύου. Σε αυτό επιτρέπεται η αποθήκευση και η διανομή αρχείων σε ένα αποκεντρωμένο δίκτυο κόμβων. Αυτό είναι ιδιαιτέρως χρήσιμο για την αποθήκευση και την ανταλλαγή δεδομένων, όπως κειμένων, εικόνων, βίντεο και άλλων αρχείων, χωρίς την ανάγκη κεντρικών διακομιστών. Τα αρχεία αναγνωρίζονται με μοναδικά προσδιοριστικά CID (Content Identifier) που εξαρτώνται από το περιεχόμενο και όχι την τοποθεσία του αρχείου, και χρησιμοποιείται για την ταυτοποίηση, την ανάκτηση, την εύρεση και την παραλαβή του αρχείου. Αυτό σημαίνει ότι τα αρχεία παραμένουν διαθέσιμα ανεξάρτητα από το αν οι αρχικοί κόμβοι που τα ανέβασαν είναι online. Αυτή η τεχνολογία αποτελεί ουσιαστικό μέρος του Web 3.0, επιτρέποντας την αποθήκευση και τη διανομή δεδομένων με αποτελεσματικό και ανθεκτικό τρόπο.

Το IPFS είναι ανθεκτικό σε αποτυχίες και επιτρέπει την εξαγωγή δεδομένων μεταξύ κόμβων. Κάτι τέτοιο καθιστά δύσκολη την απώλεια δεδομένων και παρέχει διαφάνεια στη διανομή τους. Επίσης, είναι ένα ανοικτό πρότυπο, που σημαίνει ότι οποιοσδήποτε μπορεί να το «υιοθετήσει» και να συνεισφέρει στην ανάπτυξή του. Αυτό το καθιστά προβιβάσιμο και επεκτάσιμο.

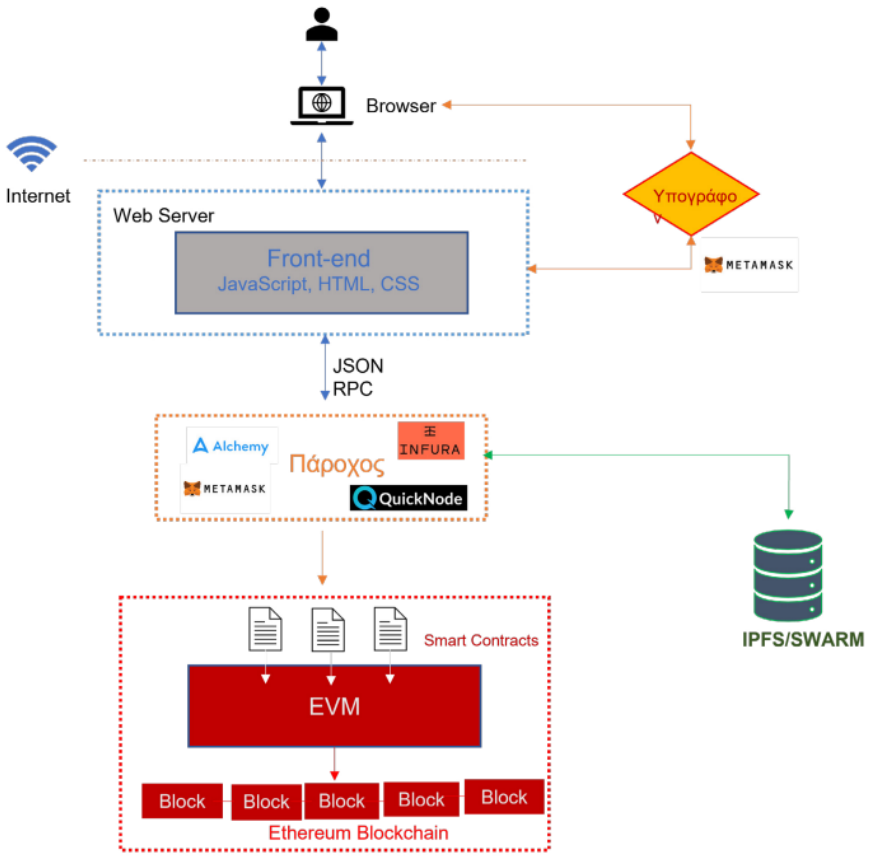
Ένα σημαντικότατο χαρακτηριστικό του είναι η συνεργασία του με τα DApps, καθώς παρέχει τη δομή αποθήκευσης και διανομής δεδομένων που χρειάζονται αυτές οι τεχνολογίες. Τα DApps μπορούν να χρησιμοποιούν το IPFS για την αποθήκευση του κώδικά τους και των αρχείων τους.

Υπάρχουν online υπηρεσίες για την υλοποίηση του κόμβου στο IPFS, όπως είναι η Pinata [5] , η Filebase [6], η NFT Storage[7] και η Infura[8]. Στην παρούσα διπλωματική έγινε χρήση του Pinata όπου αποθηκευτήκαν οι εικόνες και τα metadata του NFT. Ένα όμως μειονέκτημα των κεντρικών αυτών υπηρεσιών είναι το pinning, δηλαδή η δυνατότητα απόφασης που παρέχεται στις εταιρίες για αφαίρεση του περιεχομένου.

Αυτός ο τρόπος λειτουργίας επιτρέπει στο blockchain να παρέχει την απαραίτητη αξιοπιστία και ασφάλεια για τα δεδομένα που δεν αποθηκεύονται απευθείας σε αυτό. Προστατεύει την ακεραιότητά τους και επιτρέπει τη γρήγορη επιβεβαίωση της εγκυρότητάς τους, όταν αυτό είναι απαραίτητο.

Τέλος, ο πάροχος του δικτύου blockchain αναλαμβάνει τον ρόλο της σύνδεσης προς το κατανεμημένο δίκτυο κόμβων, το οποίο χρησιμοποιείται για την αποθήκευση των δεδομένων εκτός του blockchain, γνωστών ως δεδομένα off-chain. Αυτή η σύνδεση είναι σημαντική, διότι αφορά την ασφάλεια και την ακεραιότητα των δεδομένων. Συγκεκριμένα, συνήθως το αναγνωριστικό περιεχομένου (CID) που παράγεται από τα δεδομένα πριν αποθηκευτούν στο IPFS εισάγεται στο blockchain και στο ledger. Με αυτόν τον τρόπο, διασφαλίζεται ότι, ακόμη και όταν τα δεδομένα είναι εκτός του blockchain, δεν έχουν υποστεί αλλοίωση.

Στην Εικόνα 4 [1] παρουσιάζεται η αρχιτεκτονική μιας εφαρμογής στο Web 3.0.




**Εικόνα 4: Η αρχιτεκτονική μιας Web 3.0 εφαρμογής**

## 1.4 Tokens

Βασικό χαρακτηριστικό στην τεχνολογία του blockchain και συγκεκριμένα στο Ethereum είναι τα Tokens.

Τα Tokens στον κόσμο του blockchain έχουν ποικίλες εφαρμογές. Δύνανται να αντιπροσωπεύουν κρυπτονομίσματα ή άλλα περιουσιακά στοιχεία, να αντιπροσωπεύουν την ψήφο σε μια διαδικασία εκλογής ή τα δικαιώματα του χρήστη. Επίσης, μπορεί να χρησιμοποιούνται για την πρόσβαση σε υπηρεσίες ή λειτουργίες σε μια εφαρμογή ή πλατφόρμα.

Ενώ υπάρχουν περιπτώσεις που τα Tokens αντιπροσωπεύουν κάποια ιδιοκτησία του χρήστη στον πραγματικό κόσμο, άλλοτε η ιδιοκτησία αυτή είναι μόνο στον ψηφιακό κόσμο. Οι εφαρμογές των Tokens είναι πολλές.

Επομένως, τα Tokens είναι ψηφιακά αντικείμενα που λειτουργούν βάσει συγκεκριμένων κανόνων, που ονομάζονται πρότυπα (standards).

Τα Tokens μπορεί να διαφέρουν ανάλογα με τη χρήση τους πλην όμως έχουν κάποια κοινά χαρακτηριστικά:

- Ανάλογα με τον τύπο των Tokens, μπορεί να είναι ανταλλάξιμα με άλλα Tokens ή μη ανταλλάξιμα.
- Πολλά Tokens είναι μοναδικά και διακριτά, δηλαδή δεν υπάρχουν παρόμοια Tokens με τα ίδια χαρακτηριστικά.
- Τα περισσότερα Tokens είναι μεταβιβάσιμα, δηλαδή μπορούν να μεταφερθούν από έναν κάτοχο σε έναν άλλο.
- Χρησιμοποιούνται για να αναγνωρίσουν την ιδιοκτησία ενός αντικειμένου ή κάποιας αξίας στον ψηφιακό χώρο.

Στις εφαρμογές που τα Tokens δεν είναι μοναδικά, όπως τα κρυπτονομίσματα, μπορούν πολύ εύκολα να ανταλλαχθούν, ενώ όταν έχουν όλα τα χαρακτηριστικά τους ίδια τότε είναι ισοδύναμα. Στον πραγματικό κόσμο μπορούν να είναι τα χρήματα της οικονομίας ή τα χρήματα ενός παιχνιδιού ή οι μάρκες ενός παιχνιδιού. Αυτά τα Tokens που είναι ανταλλάξιμα ονομάζονται Fungible.

Τα Tokens που διακρίνονται για τη μοναδικότητα τους και δεν είναι αντικαταστάσιμα από άλλα ονομάζονται Non-Fungible Tokens (NFTs). Κάθε NFT έχει το δικό του μοναδικό αναγνωριστικό (ID), που το διακρίνει εντός του blockchain. Αντίθετα, μπορεί να μετακινηθεί σε συναλλαγές όπου οι κάτοχοι μεταφέρουν τα δικαιώματα του Token σε άλλους χρήστες, συνήθως με οικονομική ανταλλαγή. Παρ' όλα αυτά, είναι αδύνατο να δημιουργηθεί ένα εντελώς ίδιο Token που να ανήκει πάλι στον αρχικό κάτοχο.

Τα Tokens (τόσο τα NFTs όσο και τα FTs) αποτελούν ήδη Smart Contract στον ψηφιακό κόσμο του blockchain. Κάθε Token αποτελεί ένα ξεχωριστό Smart Contract με προκαθορισμένες ιδιότητες και λειτουργίες, και οι δυνατότητες του καθορίζονται από το πρότυπο στο οποίο ανήκει. Συγκεκριμένα, στο δίκτυο Ethereum, έχουν αναπτυχθεί πρότυπα όπως τα ERC-20 για τα FTs και τα ERC-721 για τα NFTs, τα οποία ορίζουν τον τρόπο δημιουργίας, μεταφοράς και χρήσης των Tokens. Αυτά τα πρότυπα διευκόλυναν την ανάπτυξη εφαρμογών που αλληλεπιδρούν με τα Tokens και άνοιξαν τον δρόμο για τη δημιουργία πλήθους ψηφιακών ενεργητικών εφαρμογών που τα χρησιμοποιούν. Στην Εικόνα 5 [9] φαίνεται ένα παράδειγμα της διαφοράς των FTs με τα NFTs χρησιμοποιώντας το ERC-20 και το ERC-721.


**Εικόνα 5: ERC-20 VS ERC-721**

Το "ERC" αναφέρεται σε "Ethereum Request for Comments" και αποτελεί το πρότυπο ανοικτού κώδικα που έχει θεσπίσει η κοινότητα του Ethereum για την εφαρμογή και την ανάπτυξη Έξυπνων Συμβολαίων και των Tokens στο δίκτυο Ethereum. Τα "Ethereum Request for Comments" είναι προτάσεις, προδιαγραφές και πρότυπα που έχουν δημοσιευθεί ώστε να οριστεί πώς πρέπει να λειτουργούν τα Έξυπνα Συμβόλαια και τα Tokens στο πλαίσιο του δικτύου Ethereum. Υπάρχουν πολλά πρότυπα ERC στον ψηφιακό κόσμο του Ethereum. Κάθε ERC αντιπροσωπεύει ένα συγκεκριμένο τύπο Smart Contract ή Token με συγκεκριμένες λειτουργίες και αριθμούνται σε αύξουσα σειρά. Τα πιο γνωστά και χρησιμοποιούμενα από αυτά είναι το ERC-20, το ERC-721 και το ERC-1155.

Στη συνέχεια θα γίνει μια παρουσίαση των προτύπων ERC-20, ERC-721 και ERC-1155 δίχως όμως την εμφάνιση τους στο προγραμματιστικό τομέα. Αυτό θα συντελέσει στην καλύτερη κατανόηση των χαρακτηριστικών, των πλεονεκτημάτων και των μειονεκτημάτων καθενός από αυτά, ώστε στο τέλος να εξηγηθεί ο λόγος χρησιμοποίησης του προτύπου ERC-721 για την υλοποίηση της διπλωματικής, καθώς και το πως σχετίζεται με το θέμα της εργασίας μας.

### 1.4.1 ERC-20

Το πρότυπο ERC-20 αποτελεί ένα από τα πιο δημοφιλή πρότυπα στον ψηφιακό κόσμο του Ethereum και είναι σχεδιασμένο για τη δημιουργία Fungible Tokens, δηλαδή Tokens που είναι ανταλλάξιμα μεταξύ τους. Τα βασικά χαρακτηριστικά και σημεία ενδιαφέροντος του ERC-20 είναι τα κάτωθι:

- Δημιουργία Tokens: Το ERC-20 ορίζει πώς να δημιουργούνται Tokens στο δίκτυο του Ethereum. Αυτό επιτρέπει σε οποιονδήποτε να δημιουργήσει τα δικά του κρυπτονομίσματα ή Tokens με βάση το πρότυπο.
- Ανταλλαγή Tokens: Οι κάτοχοι ERC-20 Tokens μπορούν να ανταλλάξουν αυτά τα Tokens μεταξύ τους.
- Συμβατότητα: Όλα τα ERC-20 Tokens ακολουθούν ένα κοινό πρότυπο, καθιστώντας τα συμβατά με διάφορες εφαρμογές και πορτοφόλια.
- Εύκολη Μεταφορά: Τα ERC-20 Tokens είναι εύκολα μεταφερόμενα μεταξύ διαφόρων πορτοφολιών και ανταλλακτηρίων.

- Κατοχή και οικονομική κατάσταση: Το ERC-20 προσδιορίζει πώς υπολογίζεται και διατηρείται η οικονομική κατάσταση του κάθε κατόχου για κάθε Token.

Ο κύριος σκοπός του ERC-20 είναι να δημιουργήσει ένα κοινό πρότυπο για την έκδοση και τη διαχείριση Fungible Tokens στο δίκτυο του Ethereum. Αυτό διευκολύνει τους αναπτυσσόμενους και τους επιχειρηματίες να δημιουργήσουν δικά τους Tokens και να τα ενσωματώσουν σε εφαρμογές, πορτοφόλια, ανταλλακτήρια, παιχνίδια και άλλες ψηφιακές υπηρεσίες χωρίς προβλήματα. Είναι σημαντικό να σημειωθεί ότι το ERC-20 αφήνει ανοικτό το θέμα της ποσότητας των Tokens που θα δημιουργηθούν. Δηλαδή, κάθε δημιουργός μπορεί να αποφασίσει πόσα Tokens θα εκδώσει. Συνοψίζοντας, το ERC-20 προσφέρει ένα ευέλικτο πλαίσιο για τη δημιουργία και την αλληλεπίδραση με Fungible Tokens στο δίκτυο του Ethereum, ενισχύοντας την ευκολία χρήσης, τη συμβατότητα και την επαναχρησιμοποίηση σε διάφορες εφαρμογές.

### 1.4.2 ERC-721

Το πρότυπο ERC-721 αφορά στη δημιουργία και διαχείριση των Non-Fungible Tokens (NFTs) προσφέροντας ένα σταθερό πλαίσιο για την αναπαράσταση μοναδικών ψηφιακών αντικειμένων στο blockchain του Ethereum. Παρακάτω, παρουσιάζουμε τα κύρια χαρακτηριστικά του ERC-721 και πώς αυτό αποτελεί ένα βήμα προς την εξέλιξη σε σχέση με το ERC-20, που αφορά τη δημιουργία Fungible Tokens.

- Μοναδικότητα: Τα ERC-721 Tokens είναι απολύτως μοναδικά. Κάθε ένα από αυτά διαθέτει ένα μοναδικό αναγνωριστικό (ID) που το καθιστά μοναδικό και αναγνωρίσιμο από όλα τα υπόλοιπα. Αυτό τα καθιστά ιδανικά για την αναπαράσταση ψηφιακών αντικειμένων που πρέπει να είναι αναμφίβολα μοναδικά.
- Δικαιώματα Κατοχής: Κάθε κάτοχος ενός ERC-721 Token έχει αποκλειστικά δικαιώματα κατοχής επί του συγκεκριμένου ψηφιακού αντικειμένου που το αντιπροσωπεύει το Token. Αυτά τα δικαιώματα είναι απολύτως καθορισμένα και προστατεύονται από την τεχνολογία blockchain.
- Ανταλλαγή και Μεταφορά: Τα ERC-721 Tokens μπορούν να ανταλλαχθούν μεταξύ διαφορετικών κατόχων μέσω συναλλαγών, καθώς και να μετακινηθούν από έναν κάτοχο σε έναν νέο.
- Ποικιλία Χρήσεων: Τα NFTs έχουν εφαρμογές σε πολλούς τομείς, συμπεριλαμβανομένων των τεχνών, των παιχνιδιών, της ψηφιακής αναπαράστασης ακινήτων και του ψηφιακού συλλεκτικού. Τα ERC-721 Tokens δίνουν τη δυνατότητα στους δημιουργούς να αντιπροσωπεύσουν ψηφιακά αντικείμενα και αξίες με μεγάλη ακρίβεια και ασφάλεια.

Ο βασικός στόχος του ERC-721 είναι να δημιουργήσει ένα πρότυπο για την αναπαράσταση NFTs εντός του οικοσυστήματος του Ethereum. Αυτό το πρότυπο επιτρέπει στους δημιουργούς να δημιουργήσουν NFTs που αντιπροσωπεύουν ο,τιδήποτε, από ψηφιακές τέχνες και εικονικά ακίνητα έως παιχνίδια και ψηφιακά συλλεκτικά.

Το ERC-721 πρότυπο προσφέρει την απαραίτητη δομή και λειτουργικότητα για τη δημιουργία, τη διακίνηση και τη διαχείριση των NFTs. Συνδυάζοντας τη μοναδικότητά τους με τα δικαιώματα των κατόχων τους, το ERC-721 δημιουργεί ένα πρότυπο που ενθαρρύνει την ανάπτυξη του ψηφιακού κόσμου και τη δημιουργία ψηφιακών αξιών.

Επιπρόσθετα, το ERC-721 περιλαμβάνει δύο προαιρετικές επεκτάσεις που μπορούν να ενισχύσουν τη λειτουργικότητα και την πληροφορία των NFTs.

Η προαιρετική επέκταση Metadata προσφέρει τη δυνατότητα απόδοσης ονόματος και συντομογραφίας σε κάθε NFT, μαζί με το αναγνωριστικό του (Token ID). Αυτό επιτρέπει στους δημιουργούς να παρέχουν περισσότερες πληροφορίες σχετικά με κάθε NFT, ενισχύοντας την κατανόηση και την αξία τους.

Επίσης, η προαιρετική επέκταση Enumeration προσφέρει τη δυνατότητα καταμέτρησης των NFTs στο δίκτυο, αν και συνήθως δεν συμπεριλαμβάνεται λόγω της αυξημένης χρήσης του δικτύου που απαιτεί. Αυτή η επέκταση επιτρέπει την αποτελεσματική καταμέτρηση και ανίχνευση των NFTs στο Ethereum.

Συνοψίζοντας, το ERC-721 επιτρέπει την έκδοση των Non-Fungible Tokens στο Ethereum και δημιουργεί ένα πρότυπο που επιτρέπει τη δημιουργία μοναδικών ψηφιακών αντικειμένων με δικαιώματα κατοχής και ανταλλαγής, ενισχύοντας παράλληλα την πληροφορία και την αντίληψη για κάθε NFT μέσω των προαιρετικών επεκτάσεών του.

### 1.4.3 ERC-1155

Το πρότυπο ERC-1155, γνωστό και ως το πρότυπο πολλών ειδών Token (multi-Token standard), εισήγαγε μια πρότυπη διεπαφή στον χώρο των blockchain που επιτρέπει τη δημιουργία πολλών ειδών Token σε ένα μόνο συμβόλαιο. Αυτό το συμβόλαιο μπορεί να διαχειριστεί τόσο Fungible όσο και Non-Fungible Tokens, αλλά και οποιονδήποτε άλλο συνδυασμό τους. Επομένως, το ERC-1155 μπορεί να αντικαταστήσει τα πρότυπα ERC-20 και ERC-721, αλλά και να τα συνδυάσει και να βελτιώσει την απόδοσή τους.

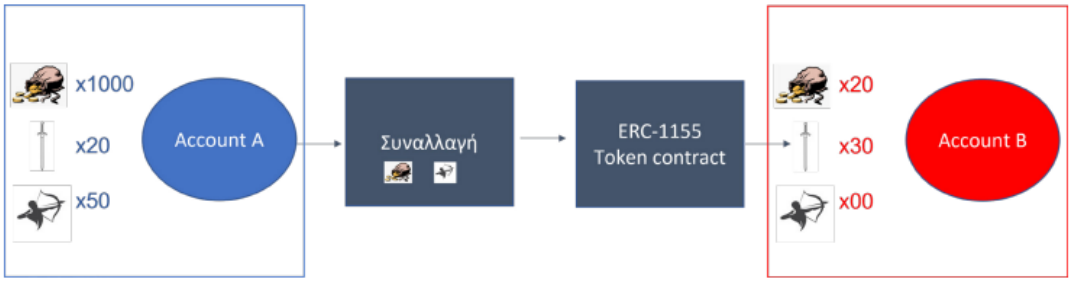
Λόγοι για την ανάπτυξη του ERC-1155 περιλαμβάνουν την ανάγκη για αποδοτικότητα στο Ethereum blockchain, καθώς η χρήση πολλαπλών ξεχωριστών συμβολαίων για τα διάφορα είδη Token προκαλεί υψηλά κόστη σε gas fees και αυξημένη πολυπλοκότητα Το ERC-1155 είναι ευέλικτο και επιτρέπει τη δημιουργία πολλών διαφορετικών ειδών Token σε ένα συμβόλαιο. Η χρήση ενός μόνο συμβολαίου για τη διαχείριση πολλαπλών ειδών Token μειώνει την πολυπλοκότητα και το κόστος σε gas fees.

Τα χαρακτηριστικά του ERC-1155 είναι:

- Επιτρέπει τη διαχείριση πολλαπλών Token σε μία μόνο συναλλαγή, χρησιμοποιώντας το id για να αναγνωρίσει το εκάστοτε Token.
- Η ευκολία στη χρήση καθώς οι χρήστες μπορούν να ανταλλάσσουν και να διαχειρίζονται διάφορα είδη Token χρησιμοποιώντας την ίδια διεπαφή.
- Η αποδοτικότητα αυξάνεται καθώς οι εφαρμογές μπορούν να χρησιμοποιούν ένα μόνο συμβόλαιο για πολλαπλά είδη Token.

Συνεπώς, σκοπός του ERC-1155 είναι να βελτιώσει την απόδοση και την αποδοτικότητα στον τομέα των Token στο Ethereum, παρέχοντας μια ευέλικτη και ενιαία διεπαφή για τη δημιουργία και διαχείριση πολλών ειδών Token με τη χρήση ενός μόνο Έξυπνου Συμβολαίου. Αυτό επιτρέπει στις αποκεντρωμένες εφαρμογές να είναι πιο αποδοτικές και ευέλικτες στην υποστήριξη διάφορων ειδών Token, ενώ ταυτόχρονα εξοικονομεί gas.

Στην Εικόνα 6 [1] παρουσιάζεται ένα παράδειγμα στο οποίο χρήστες συμμετέχουν σε ένα παιχνίδι. Σε αυτό το παιχνίδι, κάθε χρήστης έχει στην ιδιοκτησία του διάφορα αντικείμενα με διαφορετικά χαρακτηριστικά. Επειδή τα Tokens αυτά υποστηρίζουν το πρότυπο ERC-1155, είναι δυνατή η μεταφορά αντικειμένων από τον λογαριασμό Α στον λογαριασμό Β.




**Εικόνα 6: Παράδειγμα παιχνιδιού**

### 1.4.4 Συμπερασματικά

Τέλος, στην Εικόνα 7 [1] παρουσιάζονται συγκεντρωτικά οι διαφορές των χαρακτηριστικών των τριών προτύπων ERC-20, ERC-721, ERC-1155.

| Τεχνικές Προδιαγραφές | ERC-20 | ERC-721 | ERC-1155 |
|---|---|---|---|
| *Ευκολία στη χρήση* | Μια ενέργεια ανά συναλλαγή. | Μια ενέργεια ανά συναλλαγή. Νέο contract για κάθε τύπο token. | Πολλαπλές ενέργειες ανά συναλλαγή. Ένα συμβόλαιο για κάθε τύπο. |
| *Λειτουργίες burn και mint* | Δεν ενσωματώνει υλοποίηση. Επιλογή του χρήστη. | Διαθέτει. | Διαθέτει. |
| *Τύπος token που υποστηρίζεται* | Fungible | NFT | Fungible + NFTs |
| *Smart Contracts* | Χρήση 1 smart contract. | Χρήση νέου contract για κάθε τύπο token. | Χρήση 1 smart contract για όλους τους τύπους token. |
| *Αποτελεσματικότητα* | Χρειάζεται περισσότερο αποθηκευτικό χώρο. | Μπορεί να χρειαστεί περισσότερο αποθηκευτικό χώρο. | Χρειάζεται λιγότερο αποθηκευτικό χώρο. |
| *Μεταφορά tokens* | Μεταφορά 1 token σε κάθε συναλλαγή. | Μεταφορά 1 token σε κάθε συναλλαγή. | Μεταφορά πολλών tokens σε κάθε συναλλαγή. |
| *Τύπους Μεταφοράς* | Μεταφορά αξίας ανάμεσα σε χρήστες. | Μεταφορά δικαιωμάτων ιδιοκτησίας. | Μεταφορά αξίας ή δικαιωμάτων. |
| *Παραδείγματα Χρήσης* | Binance Coin, OmiseGo. | *Decentraland, Cryptokitties.* | Εξαγοράσιμα κουπόνια αγορών. |

**Εικόνα 7: Χαρακτηριστικά των τριών προτύπων**

# 2 ΚΕΦΑΛΑΙΟ 2ο : Εφαρμογή συστήματος αξιολόγησης χρηστών σε φανταστικό παιχνίδι

Στο 2ο Κεφάλαιο παρουσιάζεται η εφαρμογή της Διπλωματικής Εργασίας. Αρχικά, στην 1η ενότητα γίνεται μια περιληπτική ανάλυση των φανταστικών παιχνιδιών (fantasy games) που υπάρχουν ενώ στην 2η περιγράφεται το σύστημα αξιολόγησης που θα χρησιμοποιηθεί. Έπειτα, επιλέγεται ένας τύπος παιχνιδιού από αυτούς που αναφέρθηκαν και με συνδυασμό του συστήματος αξιολόγησης δημιουργείται ένα παράδειγμα με σκοπό την εφαρμογή του πρότυπου ERC-721 ως και την απονομή ενός Badge.

## 2.1 Φανταστικά Παιχνίδια

Τα Φανταστικά Παιχνίδια (fantasy sports games) είναι ένα είδος αθλητικών παιχνιδιών που έχουν επηρεάσει τον τρόπο που οι θαυμαστές αντιλαμβάνονται και παρακολουθούν τον αθλητισμό. Η ιδέα πίσω από αυτά τα παιχνίδια προήλθε από την επιθυμία των φανατικών θαυμαστών να αναλάβουν τον ρόλο του Γενικού Διευθυντή (General Manager - GM) ενός αθλητικού συλλόγου. Οι συμμετέχοντες δημιουργούν φανταστικές ή εικονικές ομάδες που αποτελούνται από υποκατάστατα πραγματικών παικτών ενός επαγγελματικού αθλήματος. Οι ομάδες αυτές ανταγωνίζονται με βάση τις στατιστικές επιδόσεις αυτών των παικτών σε πραγματικούς αγώνες. Οι επιδόσεις αυτές μετατρέπονται σε πόντους που συγκεντρώνονται και αθροίζονται σύμφωνα με έναν κατάλογο, μια λίστα που επιλέγεται από τον ιδιοκτήτη και GM της κάθε φανταστικής ομάδας. Αυτά τα συστήματα πόντων μπορεί να είναι αρκετά απλά ώστε να υπολογίζονται χειροκίνητα από έναν "επίτροπο πρωταθλήματος (league commissioner)" που συντονίζει και διαχειρίζεται το συνολικό πρωτάθλημα, ή οι πόντοι μπορούν να συγκεντρώνονται και να υπολογίζονται με τη χρήση υπολογιστών που παρακολουθούν τα πραγματικά αποτελέσματα του επαγγελματικού αθλήματος. Στα φανταστικά αθλήματα, όπως και στα πραγματικά αθλήματα, οι ιδιοκτήτες των ομάδων επιλέγουν, ανταλλάσσουν και κόβουν (αποδεσμεύουν) παίκτες. Στον πυρήνα του παιχνιδιού, οι συμμετέχοντες δημιουργούν τις δικές τους ομάδες επιλέγοντας παίκτες μέσω του "draft" για τη αθλητική χρονιά. Στη συνέχεια κερδίζουν ή χάνουν βάσει των στατιστικών επιδόσεων των παικτών τους σε πραγματικό χρόνο. Το υπέροχο και ενδιφέρον σε αυτά τα παιχνίδια είναι ότι υπάρχει πληθώρα αθλημάτων και πρωταθλημάτων που μπορεί κάποιος να επιλέξει να συμμετέχει, καθιστώντας τα πράγματι εθιστικά για όσους τους αρέσει ο αθλητισμός και η ανταγωνιστικότητα.

Για να γίνει κατανοητό το μέγεθος επιρροής των fantasy games, παρακάτω παρουσιάζονται μερικά στατιστικά στοιχεία που προέρχονται από την Fantasy Sports & Gaming Association[10]. Η FS&GA είναι ο μοναδικός εθνικός οργανισμός που εκπροσωπεί τα φανταστικά αθλήματα και τις εταιρίες παιχνιδιών. Αντιπροσωπεύει 60 εκατομμύρια παικτών φανταστικών αθλημάτων στις Ηνωμένες Πολιτείες και τον Καναδά, καθώς και των εταιρειών που παρέχουν υπηρεσίες, ειδήσεις, πληροφορίες και ανταγωνισμό για την υποστήριξη αυτού του αναπτυσσόμενου κλάδου. Έχουν σκοπό να παρέχουν βασικές έρευνες και δεδομένα, ευκαιρίες δικτύωσης και συλλογικής δράσης για την περαιτέρω αξιοποίηση των δυνατοτήτων τους.

Χρήστες που παίζουν φανταστικά παιχνίδια:

- 65% είναι άντρες και 35% είναι γυναίκες.

- 48% είναι μεταξύ ηλικιών 18 και 34.
- 84% έχουν προπτυχιακό ή μεγαλύτερο επίπεδο σπουδών.

Αθλήματα που παίζουν οι περισσότεροι χρήστες:

- 79% Αμερικανικό Ποδόσφαιρο (NFL).
- 32% Basketball (NBA).
- 22% Baseball (MLB).
- 12% Hockey (NHL).
- 11% Soccer, Ευρωπαϊκό ποδόσφαιρο.
- 11% Κολεγιακό Αμερικάνικο Ποδόσφαιρο (NCAA Football).

Το 2022, υπήρχαν 62,5 εκατομμύρια άνθρωποι που έπαιζαν φανταστικά αθλήματα στις ΗΠΑ και στον Καναδά.

Μερικές ενδεικτικές πλατφόρμες που ασχολούνται με τα φανταστικά αθλήματα είναι η ESPN Fantasy [14 ], η Fantrax [15] και η Yahoo sport [16].

Για το υπόλοιπο της διπλωματικής το NBA θα αποτελεί το άθλημα-σημείο αναφοράς.

Κατόπιν επιλογής του αθλήματος και εγγραφής του χρήστη στην πλατφόρμα του παιχνιδιού, το επόμενο βήμα είναι η είσοδος σε ένα Πρωτάθλημα (League) ώστε να ξεκινήσει η αθλητική χρονιά του. Το πρωτάθλημα ξεκινάει με τους χρήστες να επιλέγουν τους παίχτες που θέλουν να έχουν στην ομάδα τους μέσα από μια λίστα παιχτών, όπου όταν ένας παίχτης επιλεγεί από έναν χρήστη, τότε κανένας άλλος δεν μπορεί να τον επιλέξει. Οι χρήστες μπορούν να συμμετέχουν σε παραπάνω από ένα πρωταθλήματα ακόμα και αν είναι διαφορετικού τύπου από την αρχική τους επιλογή.

Ένα πρωτάθλημα αποτελείται από τις συμμετέχουσες ομάδες, τον τρόπο επιλογής παιχτών για την ομάδα του εκάστοτε χρήστη, καθώς και τον τρόπο υπολογισμού των πόντων.

Ο αριθμός των συμμετεχουσών ομάδων μπορεί να ποικίλλει, όμως 10 ή 12 ομάδες είναι ένας συνήθης και λογικός αριθμός ομάδων ώστε να αποκτά περισσότερο ενδιαφέρον και ανταγωνιστικότητα το εν λόγω πρωτάθλημα.

Εν συνεχεία, υπάρχει ο κλασικός τρόπος επιλογής παιχτών, όπου οι χρήστες επιλέγουν με τη σειρά τους τον παίχτη που επιθυμούν να εντάξουν στην ομάδα τους. Υπάρχει όμως και το Salary Cap, το οποίο είναι ένα ανώτατο επιτρεπτό όριο χρημάτων που μπορεί να δαπανήσει μια ομάδα για τις αμοιβές των παιχτών της. Τέλος, η σειρά επιλογής των παιχτών από τις ομάδες μπορεί να είναι είτε τυχαία είτε καθορισμένη ή ακόμα και τα δύο.

Για τον υπολογισμό των πόντων υπάρχουν διάφοροι τρόποι, οι επικρατέστεροι από τους οποίους παρουσιάζονται παρακάτω.

- Αντίπαλοι με πόντους: Κάθε εβδομάδα, επιτυγχάνονται περισσότεροι πόντοι από τον αντίπαλό σας.
- Αντίπαλοι σε κάθε κατηγορία: Ερχόμενοι αντιμέτωποι, υπολογίζεται μία νίκη ή ήττα με βάση κάθε κατηγορία στατιστικών στοιχείων.
- Αντίπαλοι σε περισσότερες κατηγορίες: Μια νίκη κατακτάται όταν κερδίζονται οι περισσότερες κατηγορίες στατιστικών.
- Rotisserie: Πόντοι αποκτώνται καταλαμβάνοντας την υψηλότερη θέση ανά κατηγορία στατιστικών σε σύγκριση με τους υπόλοιπους παίκτες.

- Βαθμοί σεζόν: Συγκεντρώνονται όσο το δυνατόν περισσότεροι πόντοι κατά τη διάρκεια ολόκληρης της σεζόν σε σύγκριση πάντα με τους υπόλοιπους παίκτες.

Καθώς διαφέρει ο τρόπος υπολογισμού πόντων, έτσι διαφέρει και ο τρόπος κατάταξης των χρηστών, τόσο στα πρωταθλήματα που συμμετέχουν όσο και στην γενική κατάταξη της πλατφόρμας. Για αυτό το λόγο, η συνέχεια του κεφαλαίου καθώς και το παράδειγμα και η υλοποίηση της εφαρμογής θα αφορούν σε συγκεκριμένο τύπο πρωταθλήματος.

Συγκεκριμένα, στον εν λόγω τύπο πρωταθλήματος οι χρήστες θα είναι αντίπαλοι ανά κατηγορία στατιστικών στοιχειών.

Στο τέλος της αθλητικής χρονιάς υπολογίζεται η κατάταξη των χρηστών με βάση δυο κριτήρια. Το 1$^{ο}$ είναι οι νίκες που έχει ο χρήστης και το 2$^{ο}$ είναι το ποσοστό νικών που έχει ο χρήστης. Με βάση αυτά τα δυο κριτήρια αξιολογείται η θέση κατάταξης του κάθε χρήστη καθώς και η άνοδος ή πτώση του σε αυτήν.

Όπως ο τύπος του πρωταθλήματος ορίστηκε στο παράδειγμα, έτσι χρειάζεται να οριστούν και οι ομάδες κατάταξης. Αρχικά, ο σκοπός ήταν να λαμβάνονται τα στοιχεία από την ίδια εταιρία με το δικό της σύστημα αξιολόγησης των χρηστών, ήτοι το σύνολο των κριτηρίων και κανόνων για την πιθανή άνοδο, κάθοδο ή παραμονή του παίχτη στο ίδιο επίπεδο. Παρόλα αυτά, το σύστημα αξιολόγησης των χρηστών για το συγκεκριμένο παράδειγμα θα αναλυθεί καθώς είναι η βάση αξιολόγησης του χρήστη για να πάρει το έμβλημα (Badge) που του αξίζει.

## 2.2 Σύστημα Αξιολόγησης Χρηστών

Για την αξιολόγηση των χρηστών χρειάζονται κάποια βασικά κριτήρια και ένας πίνακας κατάταξης. Στο συγκεκριμένο παράδειγμα ο Πίνακας 1 ορίζει ποιο Badge θα αποκτήσει ο χρήστης ανάλογα με την εκπλήρωση των κριτήριων. Το Badge δεν θα αφορά το κάθε πρωτάθλημα στο οποίο έχει λάβει μέρος ο χρήστης αλλά ολόκληρη την αθλητική χρονιά.

Τα κριτήρια στην εφαρμογή αυτή είναι δυο:

1. Οι συνολικές νίκες του χρήστη μετά το τέλος της αθλητικής χρονιάς, συμπεριλαμβανομένων και των προηγούμενων αθλητικών χρονιών.
2. Το ποσοστό νικών που έχει στις αθλητικές χρονιές.

Στη συνέχεια, αναπτύσσονται λεπτομερώς τα Κριτήρια και ο Πίνακας, ενώ στην Ενότητα 2.4 δίνεται ένα πλήρες παράδειγμα πάνω στην εφαρμογή.

### 2.2.1 Πίνακας

Στην πρώτη στήλη του Πίνακα αναφέρονται τα Badge με το Bronze να είναι το συνηθέστερο, καθώς είναι το πρώτο που αποκτάται από τους χρήστες, και το Gold που είναι το πλέον δύσκολο να αποκτηθεί. Στη δεύτερη και στην τρίτη στήλη φαίνονται τα περιθώρια εντός των οποίων ανήκει το κάθε Badge. Με βάση τα κριτήρια οι χρήστες αποκτούν και το κατάλληλο Badge. Για να λάβουν όμως Badge, θα πρέπει να εκπληρώνονται και τα δυο κριτήρια στις αντίστοιχε κατηγορίες. Αν ανήκουν σε διαφορετικές κατηγορίες, τότε ο χρήστης λαμβάνει το Badge που που εκπληρώνει και τα δυο κριτήρια μαζί. Για την καλύτερη κατανόηση, μπορεί να παρομοιαστεί με δυο στήλες όπου η κοινή τομή είναι το Badge που αποκτάται. Ακολουθεί ένα μικρό παράδειγμα για την εφαρμογή του πίνακα.

- Αν κάποιος χρήστης έχει 300 Νίκες και 50% Ποσοστό τότε αποκτά Silver. Στο παράδειγμα αυτό και τα δυο στατιστικά του χρήστη ανήκουν στην ομάδα του Silver

- Αν έχει 200 Νίκες και 35% Ποσοστό τότε το Badge που αποκτά είναι Bronze. Στο παράδειγμα αυτό οι Νίκες του ανήκουν στην κατηγορία που θα έδινε στον χρήστη το Silver Badge ενώ το Ποσοστό του ανήκει στην κατηγορία που θα έδινε στον χρήστη το Bronze. Θα αποκτήσει το Bronze Badge διότι είναι η κοινή κατηγορία, εκεί που εκπληρώνονται και τα δυο κριτήρια

- Αν έχει 80 Νίκες και 60% Ποσοστό τότε το Badge που αποκτά είναι Bronze. Οι Νίκες ανήκουν στην Bronze κατηγορία, έτσι παρόλο που το Ποσοστό ανήκει στη Silver κατηγορία, η κοινή κατηγορία είναι στο Bronze

| **Badge** | **Εικόνα** | **Νίκες** | **Ποσοστό** |
|---|---|---|---|
| Bronze |  | 0 – 100 | 0% – <40% |
| Silver |  | 101 – 500 | 40% – <70% |
| Gold |  | 501 και πάνω | 70% και πάνω |

**Πίνακας 1: Διάταξη Badge**

### 2.2.2 1ο Κριτήριο: ΝΙΚΕΣ

Κάθε αθλητική χρονιά αποτελείται από τουλάχιστον ένα πρωτάθλημα (League) και κάθε χρήστης μπορεί να λάβει μέρος σε όσα πρωταθλήματα επιθυμεί. Κάθε πρωτάθλημα αποτελείται από Χ βδομάδες κατά τις οποίες γίνονται αγώνες μεταξύ τον χρηστών. Για κάθε μια εβδομάδα αντιστοιχεί ένας αγώνας. Οι αγώνες γίνονται σε ΚΑΠΟΙΕΣ κατηγορίες, όπως αναφέρθηκε στον τύπο του πρωταθλήματος. Ο κάθε χρήστης βλέπει πόσες Νίκες, πόσες Ήττες και πόσες Ισοπαλίες έχει καταφέρει (Ν-Η-Ι) στους αγώνες.

Στο τέλος της βδομάδας, αρά στο τέλος του αγώνα το άθροισμα των Νικών, Ηττών και Ισοπαλιών θα είναι όσες και οι κατηγορίες που πραγματοποιείται ο αγώνας. Δηλαδή: Νίκες + Ήττες + Ισοπαλίες = Αριθμός Κατηγοριών.

Άρα στο τέλος του κάθε πρωταθλήματος θα υπάρχει ένα συνολικό αποτέλεσμα επίδοσης του χρήστη σε αυτή την αγωνιστική. Δηλαδή Σύνολο Νικών – Σύνολο Ηττών – Σύνολο Ισοπαλιών (ΣΝ – ΣΗ – ΣΙ). Αυτό ισχύει για κάθε πρωτάθλημα ξεχωριστά και στο τέλος της αθλητικής χρονιάς θα υπάρχει μια σειρά αθροισμάτων όλων των πρωταθλημάτων.

Αυτό επαναλαμβάνεται για κάθε αθλητική χρονιά.

Έτσι, με την πάροδο των χρόνων, δηλαδή των αθλητικών χρονιών, ο κάθε χρήστης θα έχει συγκεντρώσει ένα άθροισμα από Ν – Η – Ι από το οποίο και θα προκύψει το 1ο κριτήριο, καθώς

αυτό είναι το άθροισμα των Νικών όλων αθλητικών χρόνων. Αυτό ισχύει από την αρχή, δηλαδή εγγραφή του και την 1η συμμέτοχη του σε κάποιο πρωτάθλημα, έως και την τελευταία χρονιά που συμμετοχής του.

### 2.2.3 2ο Κριτήριο: Ποσοστό

Όπως αναφέρθηκε στο 1ο κριτήριο υπάρχει ένα άθροισμα κατηγοριών.

N – H – I όπου στο σύνολο κάθε πρωταθλήματος μεταφράζεται ως Κατηγόριες επί (*) Εβδομάδες. Αυτός ο ορός είναι ο παρονομαστής στο κλάσμα που θα χρησιμοποιηθεί για να βρεθεί το ποσοστό στο συγκεκριμένο πρωτάθλημα.

Ο αριθμητής υπολογίζεται από την Εξίσωση(1):

$$(N*1)+(I*0,5) \tag{1}$$

Το ίδιο σκεπτικό ισχύει και για τη συνολική αθλητική χρονιά με τα πολλαπλά πρωταθλήματα στα οποία μπορεί να συμμετέχει ο χρήστης.

Δηλαδή, στην Εξίσωση (2) δίνεται ο υπολογισμός του ποσοστού για την αθλητική χρονιά:

$$\frac{\sum((N*1)+(I*0,5))}{(\text{Κατηγορίες} * \text{Εβδομάδες})*\sum \text{Πρωταθλήμα τα}} \tag{2}$$

Το ίδιο ακριβώς ισχύει για όλες τις αθλητικές χρονιές ξεχωριστά.

Έτσι, με την πάροδο των ετών, οι αθλητικές χρονιές συγκεντρωτικά αλλά και η κάθε αθλητική χρονιά επηρεάζουν τις επόμενες που έρχονται.

Σε αντίθεση με το 1ο κριτήριο, στο οποίο οι αριθμοί - σε συνάρτηση πάντα με τη συμμετοχή σε πληθώρα πρωταθλημάτων - μόνο αυξάνονταν καθώς οι αθλητικές χρονιές προχωρούσαν, στο 2ο κριτήριο το ποσοστό είναι σχεδόν απίθανο να παραμένει αμετάβλητο καθώς επηρεάζεται από πολλούς παράγοντες.

Το τελικό ποσοστό λοιπόν, είναι ένα κλάσμα όπου στον αριθμητή του υπάρχει η κάθε αθλητική χρονιά, δηλαδή η Εξίσωση (3):

$$\sum_{\text{ΑθλητικήΧρονιά}} \left( \sum_{\text{Πρωταθλήματα}} \left( \sum N*1 + \sum I*0,5 \right) \right) \tag{3}$$

Ενώ ο παρονομαστής έχει την Εξίσωση (4) :

$$\sum_{\text{ΑθλητικήΧρονιά}} \left( \sum_{\text{Πρωταθλήματα}} \left( \sum \text{Κατηγορίες} * \text{Εβδομάδες} \right) \right) \tag{4}$$

Άρα, από την Εξίσωση(5) προκύπτει το ποσοστό για όλες τις αθλητικές χρονιές και τα πρωταθλήματα που έχει συμμετάσχει ο χρήστης:

$$\frac{\sum_{\text{ΑθλητικήΧρονιά}}\left(\sum_{\text{Πρωτάθλημα}}\left(\sum \text{N}*1+\sum \text{I}*0{,}5\right)\right)}{\sum_{\text{ΑθλητικήΧρονιά}}\left(\sum_{\text{Πρωτάθλημα}}\left(\sum \text{Κατηγορίες}*\text{Εβδομάδες}\right)\right)} \quad (5)$$

Με το παράδειγμα που ακολουθεί θα γίνει καλυτέρα κατανοητή η όλη διαδικασία ώστε να παρουσιαστεί ο τελικός σκοπός, δηλαδή η απονομή badge στους χρήστες με βάση τα κριτήρια αυτά.

## 2.3 Επιλογή προτύπου για την διπλωματική

Στην παρούσα διπλωματική έγινε η χρήση του πρότυπου ERC-721. Λόγω όλων των προαναφερθέντων, το ERC-20 απορρίφθηκε καθώς σε αυτό τα Tokens έχουν την ιδιότητα να είναι ισότιμα, δηλαδή είναι fungible, γεγονός μη επιθυμητό για την εφαρμογή αυτή. Αντιθέτως, απαιτείται να ξεχωρίζουν, να μην είναι ισότιμα. Οπότε μένουν τα πρότυπα ERC-1155 και το ERC-721 με τα οποία θα μπορούσε εξίσου να υλοποιηθεί η διπλωματική. Όμως, για λόγους ευκολίας της συγκεκριμένης υλοποίησης επιλέχθηκε το πρότυπο ERC-721, μιας και στην συγκεκριμένη εφαρμογή έγινε χρήση ενός μόνο Smart Contract για την υλοποίηση του NFT.

Ο τρόπος υλοποίησης του ERC-721 είναι να δίνει στον χρήστη το κατάλληλο NFT, δηλαδή το αντίστοιχο Badge και κάθε φορά που είναι να πάρει το ίδιο Badge, θα προσαυξάνεται ο υπάρχων μετρητής. Ο μετρητής υποδηλώνει πόσες φορές έχει λάβει ο χρήστης το εν λόγω Badge.

Ο τρόπος υλοποίησης βοηθάει ώστε να μην δημιουργούνται περισσότερα NFTs από όσα χρειάζονται. Έτσι, με τη χρήση του μετρητή αποφεύγεται η επιβάρυνση του συστήματος.

Όπως παρουσιάστηκε, ο αριθμός των χρηστών δεν είναι σταθερός. Εκτός αυτού, στις συγκεκριμένες εφαρμογές είναι σημαντικό να φαίνεται η μοναδικότητα και πως το εκάστοτε συγκεκριμένο NFT το έχει κάποιος συγκεκριμένος χρήστης και όχι κάποιος άλλος. Επιπροσθέτως, η δυνατότητα ανταλλαγής ή πώλησης του NFT είναι απενεργοποιημένη. Επομένως, το ERC-721 κρίθηκε ως το πλέον κατάλληλο καθώς αντιπροσωπεύει τη μοναδικότητα όπου κάθε αντικείμενο έχει τη δική του αξία.

## 2.4 Παράδειγμα Εφαρμογής

Στην ενότητα αυτή θα γίνει η παρουσίαση της εφαρμογής με τη χρήση ενός παραδείγματος. Εφαρμόζονται και αναπτύσσονται πλήρως τα κριτήρια και ο πίνακας για το σύστημα αξιολόγησης των χρηστών, με τελικό σκοπό την απονομή των Badge.

Αρχικά, οι χρήστες με την εγγραφή τους στην εφαρμογή αποκτούν το 1ο τους Badge που είναι το Bronze καθώς δεν έχουν συμμετάσχει σε κάποιο πρωτάθλημα και είναι η αρχή τους. Στη συνέχεια οι χρήστες επιλέγουν τους παίχτες που θέλουν στην ομάδα τους, παίρνουν μέρος σε πρωτάθλημα και στο τέλος της αθλητικής χρονιάς μπορούν να παραλάβουν το Badge τους.

Εν συνεχεία, δημιουργηθήκαν μερικές αθλητικές χρονιές ώστε να γίνει κατανοητό πώς αποκτούν το Badge μετά την ολοκλήρωση των αθλητικών χρόνων τους όπως φαίνεται στους Πίνακες 2 και 3.

| | | |
|---|---|---|
| 1ος Χρήστης<br>1η Αθλητική Χρονιά | 1ο Πρωτάθλημα | Ποσοστό 1ου πρωταθλήματος |
| | 19 25 1 | 43,67% |
| | 2ο Πρωτάθλημα | Ποσοστό 2ου πρωταθλήματος |
| | 24 20 1 | 54,44% |
| | Συνολική Αθλητική Χρονιά | Ποσοστό Αθλητικής Χρονιάς |
| | 43 45 2 | 48,89% |

**Πίνακας 2: 1ος Χρήστης με την 1η Αθλητική Χρονιά**

| | | |
|---|---|---|
| 2ος Χρήστης<br>1η Αθλητική Χρονιά | 1ο Πρωτάθλημα | Ποσοστό 1ου πρωταθλήματος |
| | 22 21 2 | 51,11% |
| | 2ου Πρωτάθλημα | Ποσοστό 2ου πρωταθλήματος |
| | 24 21 0 | 53,33% |
| | Συνολική Αθλητική Χρονιά | Ποσοστό Αθλητικής Χρονιάς |
| | 46 42 2 | 52,22% |

**Πίνακας 3: 2ος Χρήστης με την 1η Αθλητική Χρονιά**

Στο παράδειγμα συμμετέχουν δύο χρήστες. Στην πρώτη αθλητική χρονιά και οι δυο χρήστες συμμετέχουν σε δυο πρωταθλήματα. Κάθε πρωτάθλημα του παραδείγματος αποτελείται από 5 βδομάδες με 9 κατηγορίες. Άρα, 5 πολλαπλασιασμένο με το 9 ισούται με 45, όπου τόσες είναι συνολικά όλες οι συγκρίσεις. Όπως αναφέρθηκε στην εξήγηση των κριτηρίων, το άθροισμα των Νικών, των Ηττών και των Ισοπαλιών ισούται με 45. Ενώ το ποσοστό υπολογίζεται με τον τύπο που αναφέρθηκε προηγουμένως στα κριτήρια. Στον παρανομαστή είναι ο αριθμός των παιχνιδιών του πρωταθλήματος. Δηλαδή, το ένα πρωτάθλημα έχει 45, τα δυο πρωταθλήματα έχουν 45*2 = 90 και όσα περισσότερα πρωταθλήματα, τόσα περισσότερα και τα παιχνίδια. Όσο για τον αριθμητή υπάρχει η Εξίσωση (1).

Άρα για τον 1ο χρήστη και το 1ο πρωτάθλημα:

$$\frac{19*1+0,5}{45} = 43,67\%$$

Παρόμοια υπολογίζεται και το 2ο πρωτάθλημα.

Άρα στο τέλος της πρώτης αθλητικής χρονιάς από την Εξίσωση (5) ο 1ος χρήστης έχει:

$$\frac{(19*1+1*0,5)+(24*1+1*0,5)}{45*2} = 48,89\%$$

Στην αθλητική χρονιά αναφέρεται το πόσες είναι συνολικά οι Νίκες, οι Ήττες και οι Ισοπαλίες σε όλα τα πρωταθλήματα.

Άρα ο 1ος χρήστης στην 1η αθλητική χρονιά είχε 43 νίκες και το ποσοστό του ήταν 48,89%

Αντίστοιχη διαδικασία είναι και για τον 2ο χρήστη όπου στο τέλος της 1η αθλητικής χρονιάς είχε 46 Νίκες συνολικά και το ποσοστό υπολογίστηκε ως εξής:

$$\frac{(22*1+2*0,5)+(24*1+0*0,5)}{45*2}=52,22\%$$

Εφόσον υπάρχουν τα δυο κριτήρια που χρειάζονται και με βάση τον πίνακα που παρουσιάστηκε, ολοκληρώνεται το σύστημα αξιολόγησης των χρηστών, σύμφωνα με το οποίο οι δυο χρήστες στο τέλος της αθλητικής χρονιάς αποκτούν το ίδιο Badge που είναι Bronze. Όμως, λόγω της διαφορετικής τεχνολογίας του blockchain και συγκεκριμένα του ERC-721 που χρησιμοποιείται σαν NFT, τα Badge παρόλο που μοιάζουν ίδια, δεν είναι ίδια. Ο κάθε χρήστης κατέχει το δικό του Badge.

Άρα ο αυτό που βλέπουν οι χρήστες φαίνεται στον Πίνακα 4:

| Badges | Κατοχές | Εικόνα |
|---|---|---|
| Bronze | 2 |  |
| Silver | 0 | |
| Gold | 0 | |

**Πίνακας 4: Αποτέλεσμα χρηστών**

Προχωρώντας στη δεύτερη χρονιά, προχωράμε και στη δεύτερη αθλητική χρονιά. Τα στατιστικά στοιχεία των χρηστών παρουσιάζονται στους Πίνακες 5 και 6

| | | |
|---|---|---|
| 1ος Χρήστης<br>2η Αθλητική Χρονιά | 1ο Πρωτάθλημα | Ποσοστό 1ου πρωταθλήματος |
| | 25 - 16 - 4 | 60% |
| | 2ο Πρωτάθλημα | Ποσοστό 2ου πρωταθλήματος |
| | 26 18 1 | 58,89% |
| | 3ο Πρωτάθλημα | Ποσοστό 3ου πρωταθλήματος |
| | 20 - 22 - 3 | 47,78% |
| | Συνολική Αθλητική Χρονιά | Ποσοστό Αθλητικής Χρονιάς |
| | 71 56 8 | 55,56% |

**Πίνακας 5: 1ος Χρήστης με την 2η Αθλητική Χρονιά**

| | | |
|---|---|---|
| 2ος Χρήστης<br>2η Αθλητική Χρονιά | 1ο Πρωτάθλημα | Ποσοστό 1ου πρωταθλήματος |
| | 17 26 2 | 40% |
| | 2ο Πρωτάθλημα | Ποσοστό 2ου πρωταθλήματος |
| | 16 27 2 | 37,78% |
| | 3ο Πρωτάθλημα | Ποσοστό 3ου πρωταθλήματος |
| | 18 26 1 | 41,11% |
| | Συνολική Αθλητική Χρονιά | Ποσοστό Αθλητικής Χρονιάς |
| | 51 79 5 | 39,63% |

**Πίνακας 6: 2ος Χρήστης με την 2η Αθλητική Χρονιά**

Οι χρήστες αποφάσισαν να συμμετάσχουν σε 3 πρωταθλήματα αυτήν τη φορά.

Έχοντας κρατήσει την κατάταξη από την προηγουμένη αθλητική χρονιά και το σκεπτικό υπολογισμού των δυο κριτηρίων, προκύπτει το αποτέλεσμα (ποσοστό) για τον 1ο Χρήστη στη 2η Αθλητική Χρονιά με χρήση της Εξίσωσης (5):

$$\frac{(25*1+4*0,5)+(26*1+0*0,5)+(20*1+3*0,5)}{45*3}=55,56\%$$

Και αυτό έχοντας 71 νίκες συνολικά.

Για τον 2ο χρήστη οι νίκες ήταν 51 και το ποσοστό για αυτή την αθλητική χρονιά που προκύπτει με χρήση της Εξίσωσης (5) είναι:

$$\frac{(17*1+2*0,5)+(16*1+2*0,5)+(18*1+1*0,5)}{45*3}=39,63\%$$

Στον πίνακα 7 παρουσιάζονται τα συνολικά στοιχεία των χρηστών που απαιτούνται για την απόκτηση του Badge που τους αναλογεί, λαμβάνοντας πάντα υπ'όψη τις προηγούμενες αθλητικές χρονιές. Η προηγούμενη αθλητική χρονιά θεωρείται η αρχή της αλυσίδας την οποία ακολουθεί η δεύτερη αθλητική χρονιά. Στο τέλος κάθε αθλητικής χρονιάς απονέμεται το ανάλογο Badge, το οποίο αποτελεί ένδειξη της γενικής κατάταξης του χρήστη, καθώς επηρεάζεται και από τις προηγούμενες αθλητικές χρονιές.

| **Χρήστες** | 1η Αθλητική Χρονιά | | 2η Αθλητική Χρονιά | |
|---|---|---|---|---|
| | Νίκες | Ποσοστό | Νίκες | Ποσοστό |
| U1 | 0 + 43 | 0 + 48.89% | 43+71 = 114 | 48.89% + 55,56 % = 52.89% |
| U2 | 0 + 46 | 0 + 52.22% | 46+51 = 97 | 52.22% + 39.63% = 45.33% |

**Πίνακας 7: Συνολικά στοιχεία χρηστών.**

Άρα, με βάση τον Πίνακα 1 , τα νέα Badge που αντιστοιχούν στον 1ο και 2ο Χρήστη είναι Silver και Bronze αντίστοιχα. Αυτό φαίνεται στους Πίνακες 8 και 9 για τον κάθε χρήστη ξεχωριστά.

Αυτό που οι χρήστες θα βλέπουν τελικά είναι:

| | Badge | Κατοχές | Εικόνα του Badge |
|---|---|---|---|
| 1ος Χρήστης | Bronze | 2 |  |
| | Silver | 1 | |
| | Gold | 0 | |

**Πίνακας 8: Συνολικά Badge 1ου χρήστη.**

| | Badge | Κατοχές | Εικόνα του Badge |
|---|---|---|---|
| 2ος Χρήστης | Bronze | 3 |  |
| | Silver | 0 | |
| | Gold | 0 | |

**Πίνακας 9: Συνολικά Badge 2ου χρήστη.**

Παρατηρείται πως ο 2ος χρήστης ανταμείφθηκε με το Bronze, καθώς με βάση τον πίνακα μπορεί ναι μεν το ποσοστό του να ανήκει στην κατηγορία που θα το έδινε το Silver, αλλά οι νίκες του δεν το επιτρέπουν. Επειδή δεν εκπληρώνονται και τα δυο κριτήρια, τότε στον 2ος χρήστη απονέμεται το Bronze για το οποίο πληρούνται και τα δυο κριτήρια.

Στον Πίνακα 10 παρουσιάζεται αναλυτικά για την κάθε αθλητική χρονιά, το Badge που βλέπουν οι χρήστες ξεκινώντας από την εγγραφή τους, διατηρώντας πάντα τις προηγούμενες χρονιές.

| Χρήστες/ Αθλητικές χρονιές | Εγγραφή | | 1η Αθλητική Χρονιά | | 2η Αθλητική Χρονιά | |
|---|---|---|---|---|---|---|
| 1ος Χρήστης | Bronze |  | Bronze |  | Silver |  |
| 2ος Χρήστης | Bronze |  | Bronze |  | Bronze |  |

**Πίνακας 10: Badge χρηστών σε κάθε Αθλητική Χρονιά**

## 2.5 Συμπεράσματα παραδείγματος

Ολοκληρώνοντας το παράδειγμα της εφαρμογής, υπάρχει πλέον πλήρης κατανόηση τόσο του συστήματος αξιολόγησης που χρησιμοποιείται στο φανταστικό παιχνίδι, όσο και του πώς αποκτούν οι χρήστες το Badge που τους αντιστοιχεί ανάλογα με την αθλητική τους χρονιά. Με την προσθήκη της χρήσης του blockchain και συγκεκριμένα του NFT, δίδεται η δυνατότητα στους χρήστες να γνωρίζουν τι ακριβώς τους αναλογεί, αφού κάθε NFT είναι μοναδικό. Έτσι, γνωρίζουν ποιο είναι το Badge τους και πόσες φορές έχουν περάσει από αυτήν την κατηγορία. Στο 4ο κεφάλαιο θα παρουσιαστεί η υλοποίηση του Badge, το ERC-721, του πώς γίνεται ενώ ο χρήστης λαμβάνει το

ίδιο Badge στην ουσία να είναι διαφορετικό, και πώς γίνεται διαφορετικοί χρήστες να αποκτούν το ίδιο Badge. Επίσης, θα παρουσιαστεί ο τρόπος υλοποίησης της θεωρίας του ERC-721 στο συγκεκριμένο παράδειγμα. Στο σημείο αυτό είναι σημαντικό να υπενθυμίσουμε ότι κάθε εταιρία έχει το δικό της σύστημα αξιολόγησης, άρα και τη δική της υλοποίηση για το ERC-721. Αυτό με το οποίο θα ασχοληθούμε είναι ένα παράδειγμα εφαρμογής και δεν βασίζεται σε πραγματική εταιρία.

# 3 ΚΕΦΑΛΑΙΟ 3ο : Εργαλεία για τη δημιουργία dApp

Στο κεφάλαιο αυτό, παρουσιάζονται τα εργαλεία που χρησιμοποιήθηκαν για την υλοποίηση της διπλωματικής εργασίας. Όπως προαναφέρθηκε, η εφαρμογή έχει χαρακτηριστικά τόσο του Web 3.0 όσο και από το Web 2.0, ξεκινώντας με το back-end του Web 3.0, το blockchain. Αρχικά, το πρότυπο του ERC-721 δημιουργήθηκε από την Open Zeppelin [17] και έπειτα τροποποιήθηκε μέσω του Remix [18] μέχρι την τελική του μορφή. Ένα ακόμα εργαλείο που χρησιμοποιήθηκε από το Web 3.0 είναι το IPFS για την αποθήκευση εικόνων και metadata. Από τη στιγμή της ολοκλήρωσης του Smart Contract, κεντρική και μόνιμη προγραμματιστική εφαρμογή καθίσταται το Visual Studio Code [19]. Πάνω στο VS Code προστίθεται το Smart Contract που υλοποιήθηκε στο Remix ώστε να μπορεί να γίνει η αλληλεπίδραση με το front-end. Για την υλοποίηση της υπόλοιπης εφαρμογής χρησιμοποιήθηκε το MERN Stack, το οποίο είναι ταυτόχρονα η βάση δεδομένων για την αποθήκευση των χρηστών με τα στατιστικά τους στοιχεία, ο server και το front-end. Στη συγκεκριμένη περίπτωση της εφαρμογής, το front-end είναι κοινό τόσο για το blockchain όσο και για τη βάση δεδομένων. Στη συνέχεια αναπτύσσονται τα βασικά χαρακτηριστικά των εργαλείων αυτών ώστε να γίνει κατανοητός ο σκοπός τους στη διπλωματική εργασία.

## 3.1 Open Zeppelin και REMIX

Η OpenZeppelin [20], ως εταιρεία και κοινότητα, εξειδικεύεται στη δημιουργία εργαλείων, πλατφορμών και προτύπων για την ασφαλή ανάπτυξη εφαρμογών blockchain. Με κύριο ενδιαφέρον στο περιβάλλον του Ethereum, παρέχει έτοιμα Έξυπνα Συμβόλαια και βιβλιοθήκες, τα οποία χαρακτηρίζονται από την επαναχρησιμοποίηση και την ασφάλεια. Καθώς προσφέρει ένα πλαίσιο ανοικτού κώδικα για την κατασκευή ασφαλών Smart Contracts, παρέχει επίσης μια ολοκληρωμένη γκάμα προϊόντων ασφαλείας και υπηρεσιών ελέγχου για τη διαχείριση, ανάπτυξη και επιθεώρηση όλων των πτυχών της ανάπτυξης λογισμικού και της λειτουργίας για αποκεντρωμένες εφαρμογές. Ο σκοπός της Open Zeppelin ήταν να θέσει τις βάσεις για το NFT μέσω του προτύπου ERC-721.

Προχωρώντας, το REMIX είναι ένα ολοκληρωμένο περιβάλλον ανάπτυξης για τα Smart Contracts στο πλαίσιο της πλατφόρμας Ethereum. Παρέχει ένα φιλικό περιβάλλον για τον προγραμματισμό και τον χειρισμό των Smart Contracts. Σημαντικό χαρακτηριστικό του είναι ότι παρέχει ένα δοκιμαστικό περιβάλλον που επιτρέπει στους προγραμματιστές τη δοκιμή των Smart Contracts τους χωρίς την ανάγκη δημιουργίας ή σύνδεσης με ένα πραγματικό blockchain. Σε αυτό περιλαμβάνεται επίσης η δυνατότητα σύνταξης και επεξεργασίας του κώδικα της Solidity.

Ένα από τα πλεονεκτήματα του REMIX είναι ότι ενώ διατίθεται σε ιστοσελίδα, υπάρχει και ως λογισμικό με δυνατότητα εγκατάστασης. Στην περίπτωση αυτή, η χρήση του internet μετά την εγκατάσταση δεν είναι υποχρεωτική σε αντίθεση με την ιστοσελίδα.

## 3.2 Pinata

Για την τεχνολογία του IPFS χρησιμοποιήθηκε η υπηρεσία της Pinata. Η Pinata είναι μια υπηρεσία που «καρφιτσώνει» και κρατάει τα αρχεία καρφιτσωμένα. Με την προσθήκη των αρχείων, λαμβάνεται το CID και οποιοσδήποτε μπορεί να αποκτήσει το αρχείο, ανεξάρτητα από το αν ο

υπολογιστής είναι συνδεδεμένος ή όχι, αρκεί να έχει το CID. Εκεί λοιπόν, καρφιτσώθηκαν και αποθηκεύτηκαν οι εικόνες και τα metadata των Badge.

## 3.3 Visual Studio Code

Όπως αναφέρθηκε στην εισαγωγή, μετά την υλοποίηση του Smart Contract στο REMIX, το VS Code γίνεται το μόνιμο λογισμικό για την υλοποίηση της εφαρμογής. Εδώ γράφεται όλο το κομμάτι του back-end και του front-end. Στο back-end είναι το blockchain, ο server και η βάση δεδομένων ενώ στο front-end είναι το user interface, δηλαδή αυτό που βλέπει ο χρήστης και με το οποίο έχει άμεση αλληλεπίδραση στην εφαρμογή.

Το VS Code είναι ένας δωρεάν και ανοιχτού κώδικα επεξεργαστής κειμένου. Είναι ένα εργαλείο που χρησιμοποιείται κυρίως για την ανάπτυξη κώδικα και παρέχει πολλές δυνατότητες που καθιστούν ευκολότερη τη διαδικασία ανάπτυξης λογισμικού.

Μερικά από τα χαρακτηριστικά του είναι η υποστήριξη πολλαπλών γλωσσών προγραμματισμού, όπως η JavaScript και η Solidity που θα χρησιμοποιηθούν. Αναφορικά, άλλες γλώσσες είναι η Python και η C++. Οι επεκτάσεις που εγκαθίστανται βελτιώνουν τη λειτουργικότητά του. Παρέχει προηγμένα εργαλεία αναζήτησης και αντικατάστασης κειμένου, καθώς και λειτουργίες εντοπισμού σφαλμάτων.

### 3.3.1 Hardhat

Η ανάγκη για δημιουργία ενός περιβάλλοντος ανάπτυξης που να υποστηρίζει το Ethereum για το dApp, εξασφαλίζεται με το εργαλείο που ονομάζεται Hardhat [21]. Αυτό το περιβάλλον ανάπτυξης χρησιμοποιείται για τη μεταγλώττιση, τη δοκιμή, την ανάπτυξη, την επαλήθευση και την ανίχνευση σφαλμάτων των Smart Contracts. Άρα, είναι συμβατό με τη Solidity, τη γλώσσα που χρησιμοποιήθηκε για τη δημιουργία του ERC-721.

Ένα από τα ιδιαίτερα χαρακτηριστικά του Hardhat είναι η αυτοματοποίηση βασικών βημάτων της ανάπτυξης, καθιστώντας το ιδιαίτερα χρήσιμο. Επιπλέον, συνοδεύεται από ένα ήδη κατασκευασμένο τοπικό δίκτυο Ethereum blockchain για δοκιμές, επιτρέποντας την ανάπτυξη και τον έλεγχο χωρίς την ανάγκη σύνδεσης στο κύριο δίκτυο του Ethereum.

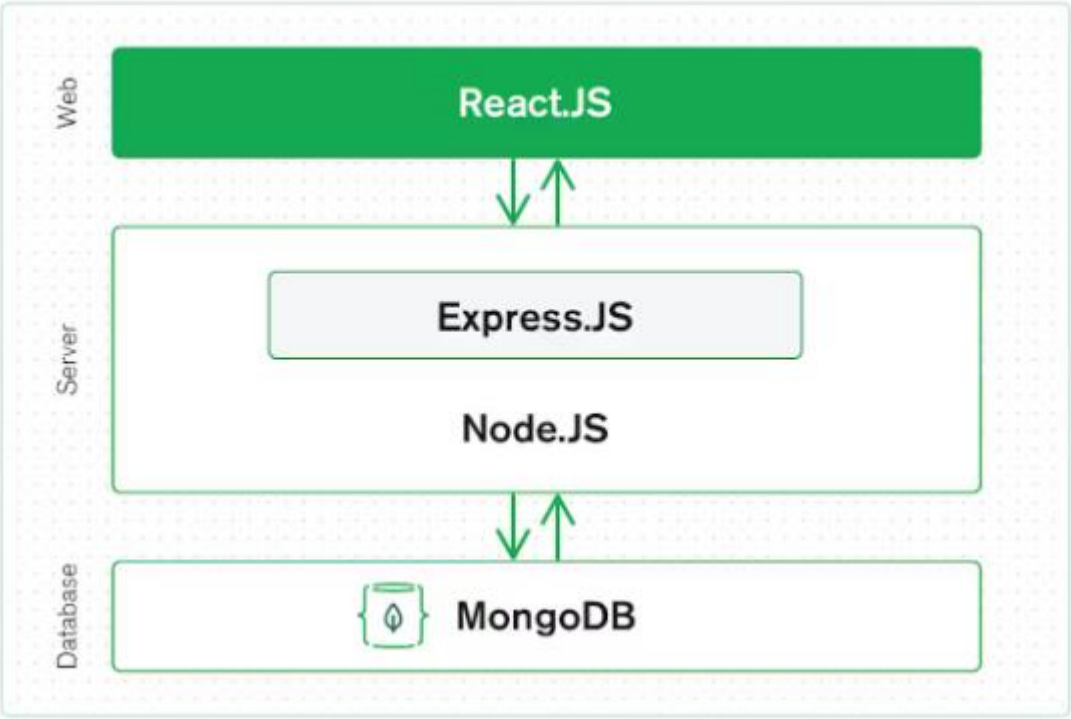
Ένα αξιοσημείωτο χαρακτηριστικό του Hardhat είναι η δυνατότητα παροχής ξεκάθαρων ενδείξεων και ιχνών στοίβας σε περίπτωση πιθανών προβλημάτων ή σφαλμάτων κατά τη διάρκεια της διαδικασίας ανάπτυξης. Αυτό επιτρέπει την ταχεία αναγνώριση και αποτελεσματική διόρθωση πιθανών προβλημάτων.

Συνολικά, το Hardhat αναδεικνύεται ως ένα ολοκληρωμένο, ευέλικτο, και αποτελεσματικό εργαλείο ανάπτυξης, παρέχοντας ταυτόχρονα φιλικό περιβάλλον και ξεκάθαρες λύσεις στη διαδικασία ανάπτυξης ενός dApp και διάφορων Smart Contracts στο δίκτυο του Ethereum.

### 3.3.2 MERN Stack

Ο όρος MERN [22] είναι ακρωνύμιο των όρων MongoDb, Express, React και Node. Όταν αυτές οι τέσσερις τεχνολογίες συνδυάζονται, δημιουργούν μια ολοκληρωμένη διαδικτυακή εφαρμογή, ήτοι μια full stack web application.

Στην Εικόνα 8 φαίνεται η γενική εικόνα του τρόπου συνδυασμού των τεχνολογιών αυτών.




**Εικόνα 8: Συνδεσμολογία MERN Stack [22]**

Η React είναι μια βιβλιοθήκη που ανήκει στη μεγάλη οικογένεια της JavaScript και είναι JavaScript που τρέχει στο πρόγραμμα περιήγησης. Αυτή είναι υπεύθυνη για την πλευρά του πελάτη (client), για την πλευρά του προγράμματος περιήγησης, για το τι βλέπει ο χρήστης, καθώς και την παρουσίαση και το περιβάλλον εργασίας χρήστη (ui). Άρα, με τη χρήση της React.js θα δημιουργηθεί η διαδικτυακή εφαρμογή που είναι υπεύθυνη για το front-end. Επίσης, είναι υπεύθυνη για τον τρόπο που απεικονίζονται τα στοιχεία στην οθόνη και το πώς ανταποκρίνεται κάθε φορά που κάτι αλλάζει, ενημερώνοντας δυναμικά το περιβάλλον του χρήστη για μια βέλτιστη εμπειρία. Ωστόσο, η React μόνη της έχει ορισμένους περιορισμούς. Δεν είναι σε θέση να εκτελέσει λογική στον διακομιστή (server), και αυτό περιορίζει τη δυνατότητά μας να εκτελούμε οποιαδήποτε λογική εκτός του προγράμματος περιήγησης. Τα δεδομένα που είναι εκτός blockchain χρειάζεται να αποθηκεύονται σε έναν μόνιμο αποθηκευτικό χώρο, πράγμα αδύνατο στο πρόγραμμα περιήγησης διότι αφενός οι χρήστες έχουν τη δυνατότητα εκκαθάρισης δεδομένων εκεί, αφετέρου τα δεδομένα διαγράφονται αυτομάτως εάν εξαντληθεί ο αποθηκευτικός χώρος του προγράμματος περιήγησης και τέλος, οι αλλαγές που γίνονται σε ένα πρόγραμμα περιήγησης δεν είναι προσβάσιμες σε όλους. Επίσης για να γίνει η αλληλεπίδραση της React με το blockchain χρειάζεται μια συγκεκριμένη βιβλιοθήκη. Αυτή μπορεί να είναι η web3.js ή ethers.js. Στην παρούσα διπλωματική έγινε η χρήση της ethers.js.

Στο κεφάλαιο της υλοποίησης θα δοθούν περισσότερες λεπτομέρειες σχετικά με το τι χρειάζεται για να επικοινωνήσει το Smart Contract με το front-end.

Για αυτούς τους λογούς απαιτούνται και οι υπόλοιπες τεχνολογίες, χρειάζεται το back-end, δηλαδή η πλευρά του διακομιστή, του server.

Η διαδικτυακή εφαρμογή τρέχει σε ένα συγκεκριμένο μηχάνημα, σε έναν server, μπορεί να βρίσκεται οπουδήποτε στο internet και να είναι προσβάσιμο από οποιονδήποτε χρήστη. Ο server δημιουργείται και τρέχει με τη Node.js και με το πλαίσιο (framework) της Node την Express.js. Με τη χρήση των δύο αυτών τεχνολογιών και γράφοντας JavaScripts, υλοποιείται ο server ο οποίος είναι ανεξάρτητος από τον client (πελάτη) και από το πρόγραμμα περιήγησης. Εκεί, δημιουργείται οποιαδήποτε λογική που δεν είναι απαραίτητο να γνωρίζουν οι χρήστες. Επίσης, μέσω των τεχνολογιών αυτών επιτυγχάνεται και η αποθήκευση αρχείων.

Η επικοινωνία μεταξύ ενός client και ενός server γίνεται μέσω πρωτοκόλλων, όμως δεν θα αναπτυχθούν περαιτέρω, καθώς δεν αφορά το θέμα της διπλωματικής εργασίας. Γενικά, η βασική αρχή είναι ότι ο client στέλνει ένα αίτημα στον server για μια συγκεκριμένη υπηρεσία ή πόρο, όταν αλληλεπιδρά με το περιβάλλον. Ο server λαμβάνει το αίτημα και με τη σειρά του ανταποκρίνεται με τα απαραίτητα δεδομένα ή αναφορά στο αίτημα του client. Η πιο διαδεδομένη μεταφορά δεδομένων πραγματοποιείται με το HTTP και τα δεδομένα που χρησιμοποιήθηκαν ήταν σε μορφή JSON.

Ο σκοπός του server στην εφαρμογή αυτή είναι να μεταφέρει τις διευθύνσεις των χρηστών από το πορτοφόλι τους σε ένα μόνιμο αποθηκευτικό χώρο, κατά την εγγραφή τους στην πλατφόρμα του fantasy game. Η διαχείριση των στατιστικών στοιχείων του κάθε χρήστη, είτε αυτά αφορούν την παραλαβή του αντίστοιχου Badge είτε την ενημέρωση των στατιστικών τους στοιχείων, γίνεται από τον server.

Για τον μόνιμο αποθηκευτικό χώρο χρησιμοποιείται η τεχνολογία MongoDB. Στην MongoDB υπάρχει ένας server για την βάση δεδομένων (data base, db) το οποίο μπορεί να τρέχει, είτε στο ίδιο μηχάνημα που βρίσκεται ο Express server, είτε σε εντελώς διαφορετικό μηχάνημα. Να σημειωθεί ότι ο Express server είναι ο server που επιτρέπει την επικοινωνία μεταξύ της React και της MongoDB. Ο server επ' ωφελεία της MongoDB χρησιμοποιείται μόνο για την αποθήκευση δεδομένων και όχι αρχείων. Για την αποθήκευση αρχείων χρησιμοποιείται η υπηρεσία Pinata. Συγκεκριμένα, εκεί αποθηκεύτηκαν οι εικόνες των Badge και τα metadata τους για το ERC-721. Δεν θα δοθούν περισσότερες λεπτομέρειες για την υπηρεσία Pinata και το IPFS, καθώς έχει αναπτυχθεί στην ενότητα του blockchain. Όσο για την MongoDB και τον σκοπό της στην παρούσα διπλωματική, δεν είναι άλλος από την καταχώρηση των διευθύνσεων των χρηστών με τα στατιστικά τους στοιχεία.

Τέλος, η εγκατάσταση, η διαχείριση και ο έλεγχος όλων των πακέτων και τον εξαρτημάτων (dependencies) έγινε με την χρήση του εργαλείου npm (Node Package Manager) και yarn.

# 4 ΚΕΦΑΛΑΙΟ 4ο : Υλοποίηση DApp

Στο κεφάλαιο αυτό παρουσιάζεται η υλοποίηση της εφαρμογής. Όπως αναφέρθηκε στην εισαγωγή, δεν θα γίνει ανάλυση σε προγραμματιστικό επίπεδο. Αρχικά, θα γίνει παρουσίαση των τεχνικών μερών του Smart Contract, εν συνεχεία και για καλύτερη κατανόηση του σκοπού θα παρουσιαστεί μέσω παραδείγματος και σε συνδυασμό με τη διαδικασία που εκτελούν οι χρήστες κατά τη συμμετοχή τους στην πλατφόρμα.

Η παρουσίαση του Smart Contract περιλαμβάνει την εγγραφή των χρηστών και την απονομή των Badge, δηλαδή τη δημιουργία των NFTs. Παράλληλα, οι χρήστες έχουν συνεχώς εις γνώση τους το είδος και των αριθμό των Badge που κατέχουν από κάθε κατηγορία. Συνεχίζοντας με τη χρήση του παραδείγματος, γίνεται η παρουσίαση του MERN Stack, με τη διαφορά ότι στην υλοποίηση αναφέρεται και η πλευρά της πλατφόρμας, κάτι που στο παράδειγμα δεν υπήρχε. Αρχικός σκοπός ήταν να λαμβάνονται τα στοιχεία από κάποια πλατφόρμα (όπως το ESPN Fantasy [14], η Fantrax [15] και η Yahoo sport [16]) αλλά αυτό δεν υλοποιήθηκε. Για αυτό τον λόγο, τον ρόλο της πλατφόρμας τον έχει ο ιδιοκτήτης του Smart Contract, ήτοι αυτός που το ανέβασε στο δίκτυο. Αυτός είναι ο μόνος που μπορεί να ανανεώνει τα στατιστικά στοιχεία για κάθε χρήστη που συνδέεται στην εφαρμογή.

Αυτό σημαίνει ότι θα αναφερθούν τα σημαντικά κομμάτια των συνδεσμολογιών τόσο για τη επικοινωνία του Smart Contract με το front-end, όσο και της βάσης δεδομένων με τον server και το front-end.

## 4.1 Υλοποίηση NFT

Η αφετηρία για την υλοποίηση του Smart Contract ήταν η Open Zeppelin, καθώς από εκεί εισάχθηκαν οι βάσεις για το πρότυπο του ERC-721. Το REMIX όμως, διαδραμάτισε το βασικό ρόλο στη δημιουργία, στην προσομοίωση και στις τροποποιήσεις του ERC-721. Είναι σημαντικό να αναφερθούμε σε μια τροποποίηση που έχει γίνει και είναι η εξής: όταν ο χρήστης αποκτά ένα Badge, αυτό δεν μπορεί να ανταλλαχθεί ούτε με κάποιο χρηματικό ποσό σε ETH ούτε με το Badge κάποιο άλλου χρήστη. Το Badge μόνο απονέμεται, δεν αγοράζεται ούτε ανταλλάζεται.

Το Smart Contract αποτελείται από δυο στάδια. Τις συναρτήσεις που γράφουν στο blockchain, εκτελούν συναλλαγές δηλαδή, και τις συναρτήσεις που ο χρήστης διαβάζει από το blockchain, βλέπει τι υπάρχει. Αυτές οι συναρτήσεις με τις οποίες βλέπουν τι υπάρχει γραμμένο στο blockchain, ονομάζονται view ή pure. Παρακάτω αναλύεται ο σκοπός των συναρτήσεων στην εφαρμογή.

### 4.1.1 Υλοποίηση συναρτήσεων. Δημιουργία Badge

Οι συναρτήσεις που γράφουν στο blockchain, δηλαδή αυτές που γίνονται συναλλαγές, είναι δύο ειδών, καθώς ο σκοπός τους είναι η απονομή του αναλογούντος Badge στον χρήστη.

Για την απονομή ενός Badge απαιτείται η εγγραφή του χρήστη στην πλατφόρμα. Η εγγραφή του στην πλατφόρμα, λοιπόν, αποτελεί την πρώτη συνάρτηση που πρέπει να εκτελέσει ο χρήστης γιατί αλλιώς δεν θα μπορέσει ποτέ να πάρει κάποιο άλλο Badge. Η υλοποίηση της συνάρτησης αυτής έχει γίνει με τέτοιο τρόπο ώστε να μην επιτρέπει την απόκτηση Badge από μη καταχωρημένο στην πλατφόρμα χρήστη, και ταυτόχρονα να μην έχει τη δυνατότητα επανεγγραφής σε περίπτωση που το

έχει ξεχάσει. Κατά την εγγραφή του, απονέμεται το πρώτο το πρώτο Badge, το bronze, όπως έχει παρουσιαστεί στο παράδειγμα και φαίνεται στις Εικόνες 17, 20 και 21 με το παράδειγμα του front-end.

Μετά την εγγραφή και ολοκλήρωση της πρώτης αθλητικής χρονιάς στην πλατφόρμα, απονέμεται το αντίστοιχο με τις επιδόσεις του χρήστη, Badge.

Στη δεύτερη συνάρτηση, δημιουργείται ένα νέο NFT, σε περίπτωση που ο χρήστης δεν κατέχει Badge από προηγουμένη αθλητική χρονιά, και επικαιροποιεί τον συνολικό αριθμό απονομών του συγκεκριμένου Badge.

Συγκεκριμένα, η δημιουργία ενός νέου Badge γίνεται μέσω της συνάρτησης mint, η οποία έχει ήδη υλοποιηθεί από το από το πρότυπο του ERC 721 που εισήχθη μέσω της Open Zeppelin. Η συνάρτηση mint ενεργοποιείται μόνο για τη δημιουργία νέου Badge (bronze, silver, gold), καθώς υπάρχει το NFT, όπως για παράδειγμα συμβαίνει κατά την εγγραφή νέου χρήστη στον οποίο και απονέμεται ένα bronze Badge. Σε περίπτωση που με το τέλος της αθλητικής χρονιάς ο χρήστης δεν έχει καταφέρει να αποκτήσει νέο και διαφορετικό Badge αλλά παραμένει, λόγου χάρη, στο bronze, τότε αφενός η mint δεν ενεργοποιείται, και αφετέρου αυξάνεται κατά μία μονάδα ο μετρητής.

Η λογική της εφαρμογής ναι μεν παρουσιάζεται με έναν μετρητή, αλλά προγραμματιστικά δεν γίνεται μόνο με έναν μετρητή, καθώς υπάρχει το πρόβλημα ότι ο χρήστης μπορεί να ξεχωρίζει πόσα και ποια Badge κατέχει κάποιος. Το πρόβλημα λύνεται με τη συνθήκη που καλείται mapping. Για καλύτερη κατανόηση, μπορεί να προσομοιαστεί με ένα πίνακα που αντιστοιχεί στον συγκεκριμένο χρήστη και κάθε χρήστης έχει τον δικό του πίνακα των Badge.

Τέλος, είναι σημαντικό να αναφερθεί μια παρατήρηση. Κανονικά, οι χρήστες θα μπορούσαν να ενεργοποιήσουν τη δεύτερη συνάρτηση μια φορά ετησίως, ώστε να αποτρέπει τους χρήστες να παίρνουν το Badge όποτε επιθυμούν. Αυτό πραγματοποιείται με την εντολή block.timestamp + 365 days (μέρες).

### 4.1.2 View συναρτήσεις

Οι συναρτήσεις αυτές έχουν σκοπό να διαβάζουν τι έχει γραφτεί στο blockchain. Είναι συναρτήσεις που δεν κοστίζουν gas όταν ενεργοποιούνται, καθώς δεν γίνεται κάποια συναλλαγή. Οι συναρτήσεις αυτές δείχνουν τα εξής:

- Πόσα και τι είδους Badge κατέχει ο χρήστης συνολικά
- Το Badge και το URI του που έχει τη συγκεκριμένη χρονική περίοδο

Έτσι, ο χρήστης παραμένει πλήρως ενημερωμένος ακόμα και σε περίπτωση που επιθυμεί να δει λεπτομέρειες, τα metadata και πληροφορίες σχετικά με το κατεχόμενο Badge όπως φαίνεται στις Εικόνες 20, 21 και 22 στο παράδειγμα του front-end.

## 4.2 Metadata και Pinata

Η σύνδεση με το IPFS και η δημιουργία των URI για τα metadata γίνεται εφικτή με δυο τρόπους: είτε ανεβαίνουν προγραμματιστικά στην υπηρεσία με τη χρήση των API (Application Programming Interface), είτε με την ιστοσελίδα της υπηρεσίας Pinata. Όποια διαδικασία και αν επιλέξουμε, το αποτέλεσμα παραμένει ίδιο. Συγκεκριμένα, πρώτα απαιτείται η αποθήκευση των εικόνων στην υπηρεσία, όπου με τη διαδικασία αυτή δημιουργούνται και τα CID τους. Όπως αναφέρθηκε και στη θεωρία, κάθε εικόνα έχει το δικό της CID. Στην παρούσα διπλωματική οι εικόνες είναι τρεις,

όσα και τα Badge. Για να εμφανιστεί όμως η εικόνα του Badge πρέπει να γραφτούν τα αρχικά: https://ipfs.io/ipfs/CID.

Τα Metadata δεν αποτελούνται μόνο από την εικόνα αλλά και από ένα JSON αρχείο που περιγράφει και περιέχει την εικόνα. Επομένως, στο JSON αρχείο χρειάζεται να υπάρχει η τοποθεσία της εικόνας, δηλαδή το https με το CID, ώστε όταν ο χρήστης επιθυμεί να μπορεί να δει την εικόνα του Badge. Τα υπόλοιπα αφορούν στην πλατφόρμα καθώς και το τι επιθυμούν εκείνοι να αναφέρουν στο αρχείο τους. Ένα ακόμα πιθανό χαρακτηριστικό είναι η ονομασία του Badge και το τι δηλώνει το Badge αυτό. Όπως οι εικόνες έχουν το δικό τους CID, έτσι και τα JSON αρχεία όταν ανέβουν στην υπηρεσία θα έχουν το δικό τους CID. Για να βρεθεί το JSON αρχείο, όπως στις εικόνες έτσι και στα αρχεία αυτά χρειάζονται τα αρχικά https://ipfs.io/ipfs/CID. Μόνο που το CID είναι του αρχείου JSON που ανέβηκε. Με την ολοκλήρωση τη διαδικασίας τα URI τοποθετούνται στον constructor του ERC-721. Αν στο μέλλον προστεθούν νέα Badge ή γίνει αλλαγή των εικόνων, τότε η διαδικασία πρέπει να γίνει εξ αρχής και το Smart Contract να ανεβεί εκ νέου στο δίκτυο, αφού το CID είναι μοναδικό. Στην Εικόνα 22 παρουσιάζονται τα Metadata εντός του παραδείγματος στο front-end.

## 4.3 Υλοποίηση MERN STACK

Έχοντας ολοκληρώσει την υλοποίηση του Smart Contract στο REMIX, έφτασε η στιγμή να γίνει η εγκατάσταση του Hardhat, μαζί με όλες τις απαιτούμενες εξαρτήσεις, στο VS Code για την ανάπτυξη του Smart Contract. Στο VS Code, η σειρά υλοποιήσεων της εφαρμογής με χρήση της MERN Stack δεν έχει σημασία, καθώς όλες οι απαραίτητες τεχνολογίες πρέπει να είναι ενεργοποιημένες και να εκτελούνται ταυτόχρονα για την λειτουργία του dApp.. Σημαντικό να σημειωθεί πως η υλοποίηση πραγματοποιήθηκε βασιζόμενη στο παράδειγμα που παρουσιάστηκε στο 2ο Κεφάλαιο. Όπως στο Hardhat έτσι και στο MERN Stack χρειάζεται να προστεθούν τα καταλληλά dependencies για να υλοποιηθεί η εφαρμογή.

### 4.3.1 Βάση Δεδομένων

Για την υλοποίηση της βάσης δεδομένων, παρόλο που μπορεί να γίνει από την πλατφόρμα της MongoDB, επιλέχθηκε να γίνει προγραμματιστικά.

Με την εγγραφή του χρήστη στην πλατφόρμα και την απόκτηση του πρώτο του Badge, καταχωρείται ταυτόχρονα και στη βάση δεδομένων (dB). Συγκεκριμένα, η dB λαμβάνει την διεύθυνση του από το Metamask, αφού ολοκληρωθεί η συναλλαγή (transaction) και την καταχωρεί μαζί με το ποσοστό και τις νίκες που έχει. Συγκεκριμένα και στις δυο κατηγορίες είναι μηδενική τιμή (0) γιατί δεν έχει ολοκληρώσει καμία αθλητική χρονιά ακόμη.

Όταν ολοκληρωθεί η πρώτη αθλητική χρονιά, τότε ο υπεύθυνος της πλατφόρμας, της εφαρμογής, ανανεώνει τα στατιστικά στοιχεία για κάθε διεύθυνση.

Στις Εικόνες 19 και 24 παρουσιάζονται οι ενέργειες που γίνονται καθώς εξελίσσεται το παράδειγμα.

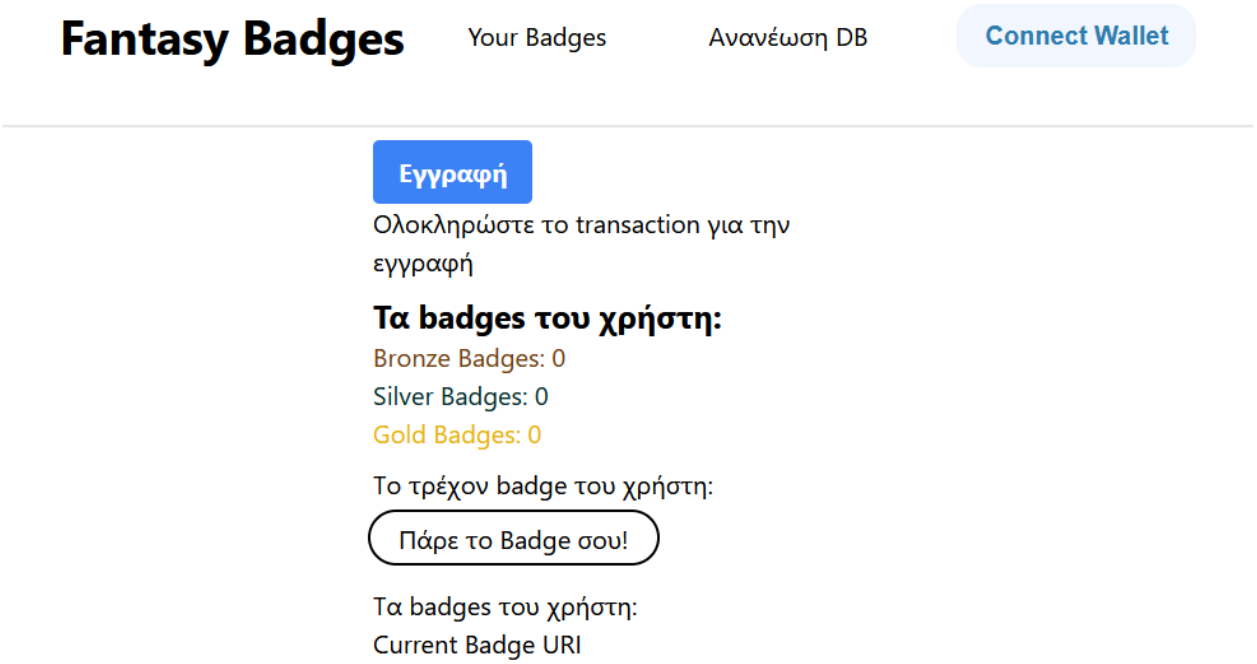
Άρα, το σχήμα της βάσης περιλαμβάνει ένα αλφαριθμητικό, ένα string που αποθηκεύει την διεύθυνση του χρήστη από το Metamask και δυο αριθμούς που αντιπροσωπεύουν τις νίκες και το ποσοστό.

### 4.3.2 Server

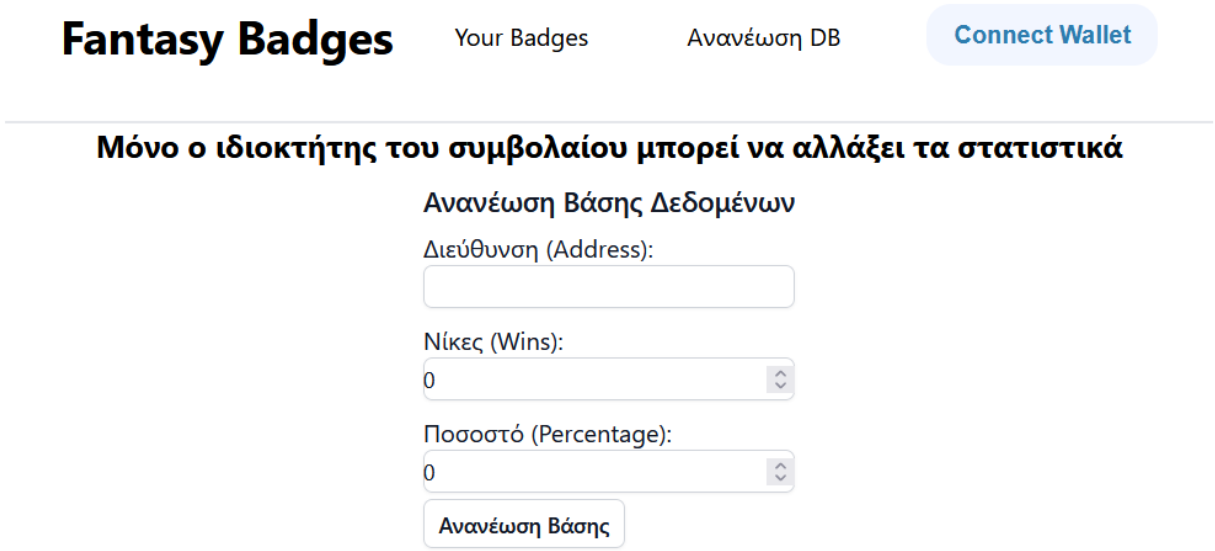
Η υλοποίηση του server δεν μπορεί να παραληφθεί καθώς είναι υπεύθυνος για την επικοινωνία με το front-end και την πλατφόρμα της MongoDB για τη βάση δεδομένων. Δίχως τον server δεν μπορεί να γίνει η αποθήκευση του χρήστη στη βάση, ούτε η ανανέωση της βάσης από τους υπεύθυνους της εφαρμογής και ούτε μπορεί ο χρήστης να πάρει κάποιο Badge μετά την πρώτη αθλητική χρονιά. Μπορεί στο παράδειγμα της εφαρμογής να μη διαδραματίζει μεγάλο ρόλο στην υλοποίηση αλλά η υλοποίηση του είναι απαραίτητη.

### 4.3.3 Front End

Το front-end, όπως έχει ειπωθεί, είναι το μέρος που αλληλεπιδρά ο χρήστης αλλά και η ίδια η εταιρία. Για να γίνει κατανοητή η υλοποίηση του, θα παρουσιαστεί η διαδικασία, όπως γίνεται με το παράδειγμα, και θα δοθούν εξηγήσεις καθώς εξελίσσεται η διαδικασία. Διαφορετικά, υπάρχει ο κίνδυνος να μην γίνει κατανοητή η υλοποίηση και η σειρά με την οποία πρέπει να γίνει. Ταυτόχρονα, θα αναφερθούν αποτελέσματα από την υλοποίηση των Metadata και της βάσης δεδομένων. Η παρουσίαση του παραδείγματος θα γίνει σε τρεις φάσεις και σε δυο ιστοσελίδες. Στην Εικόνα 9 φαίνεται η αλληλεπίδραση με το Smart Contract και η Εικόνα 10 αφορά μόνο στην εταιρία, δηλαδή τον ιδιοκτήτη του Smart Contract.

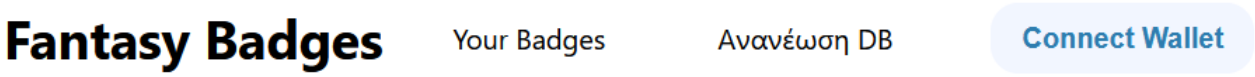



**Εικόνα 9: Η Ιστοσελίδα που αφορά το Smart Contract και όλους τους χρήστες πριν την εγγραφή τους στην πλατφόρμα.**

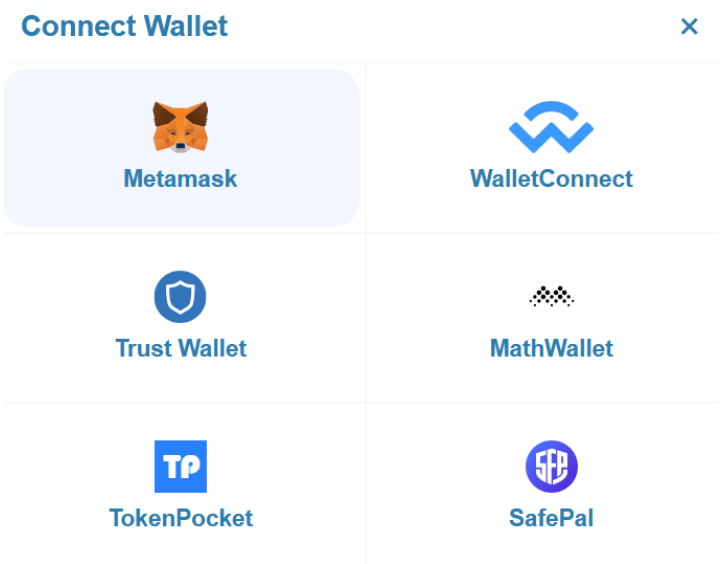



**Εικόνα 10: Η Ιστοσελίδα που αφορά μόνο τον deployer, την πλατφόρμα.**

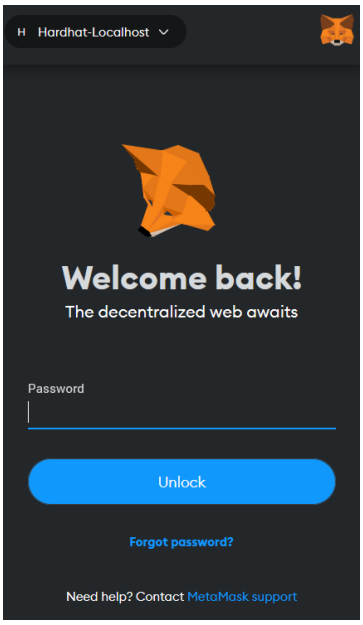
Αρχικά, στην πρώτη φάση και πριν απαιτηθεί η σύνδεση του χρήστη στην πλατφόρμα, απαιτείται η σύνδεση με τον πορτοφόλι του. Το πορτοφόλι που χρησιμοποιήθηκε είναι το Metamask και στις Εικόνες 11 μέχρις και 14 παρουσιάζεται η διαδικασία με την οποία γίνεται.




**Εικόνα 11: Η Κεντρική σελίδα, στο αριστερό μέρος της οποίας είναι το όνομα της εφαρμογής μαζί με το Badge, μετά είναι η ανανέωση της βάσης δεδομένων της πλατφόρμας και, τέλος, στα δεξιά είναι η σύνδεση του πορτοφολιού.**

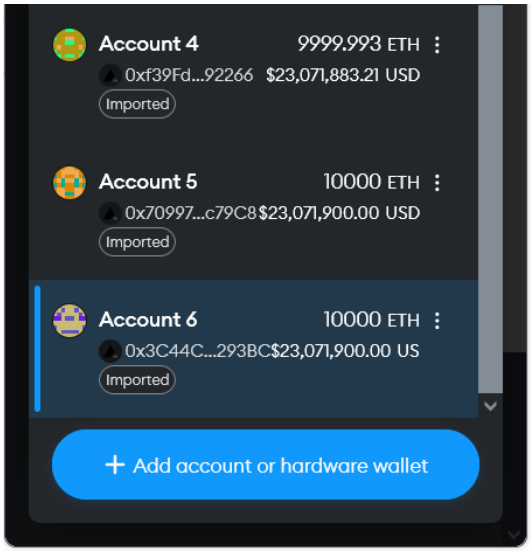



**Εικόνα 12: Επιλέγεται το Metamask ως βασικό πορτοφόλι.**

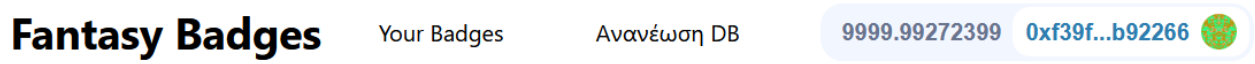



**Εικόνα 13: Συνδέεται ο χρήστης στον λογαριασμό του και, όπως φαίνεται, βρίσκεται ήδη στο δίκτυο του Hardhat όπως αναγράφεται πάνω αριστερά.**

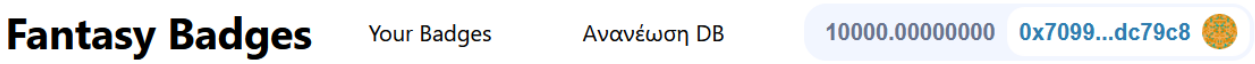
Το Hardhat με το τοπικό εξοπλισμένο δίκτυο προσφέρει 20 λογαριασμούς, δηλαδή 20 διευθύνσεις και 20 κλειδιά. Σε κάθε διεύθυνση παρέχεται το δικό της κρυφό κλειδί και σε κάθε λογαριασμό δίνονται 100 ψεύτικα eth για να γίνονται οι αλληλεπιδράσεις με το Smart Contract. Συνίσταται να χρησιμοποιούνται αυτοί οι λογαριασμοί μόνο για εκπαιδευτικούς σκοπούς. Στο Metamask έχουν ήδη περαστεί 3 λογαριασμοί, ένας εκ των οποίων πέρα από τον ρόλο του χρήστη, έχει και τον ρόλο της πλατφόρμας [23]. Επίσης έχει περαστεί το δίκτυο του Hardhat [24].




**Εικόνα 14: Οι λογαριασμοί που έχουν συνδεθεί στο Metamask και χρησιμοποιήθηκαν σε όλη τη διάρκεια της υλοποίησης.**

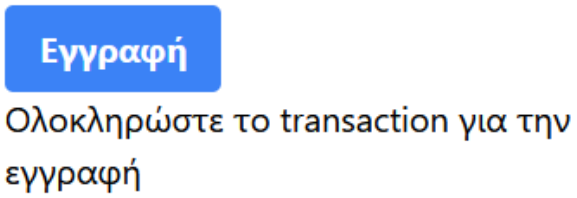



**Εικόνα 15: Η Διεύθυνση 0xf39f...b92266 είναι η διεύθυνση που ανέβασε το Smart Contract, είναι ο owner και έχει τον ρόλο της πλατφόρμας. Για αυτό δεν του έχουν δοθεί τα 100 Eth.**

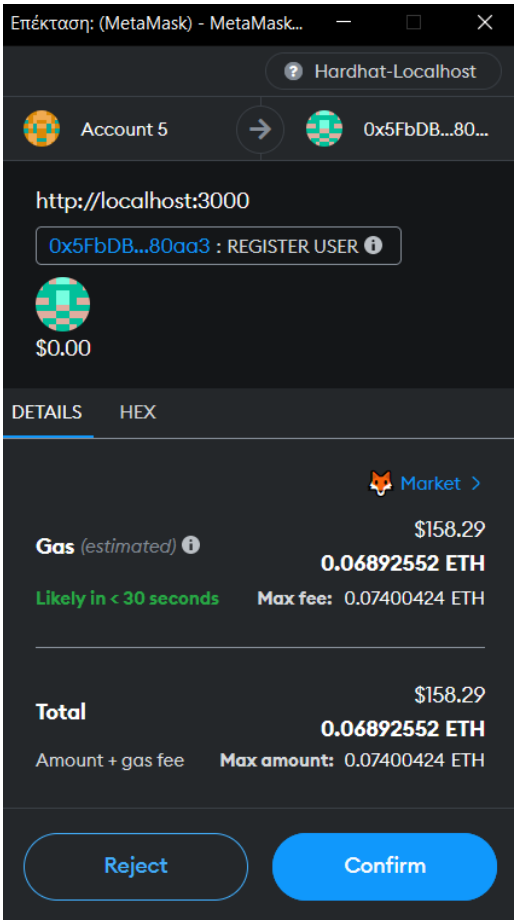



**Εικόνα 16: Η Διεύθυνση 0x7099...dc79c8 έχει τον ρόλο ενός απλού χρήστη, γι' αυτό και έχει 100 eth τα οποία δίνονται από το HardHat.**

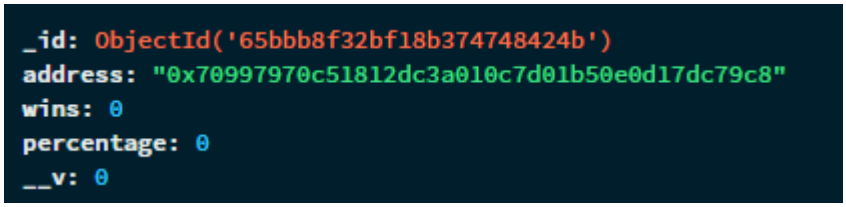
Αφού συνδεθούν οι απαιτούμενοι λογαριασμοί για το παράδειγμα της εφαρμογής, επιλέγεται ο χρήστης με τη διεύθυνση 0x7099…dc79c8 (ο χρήστης στην Εικόνα 16) και ακολουθεί η εγγραφή του στην πλατφόρμα. Θα είναι ,δηλαδή, το πρώτο κουμπί που χρειάζεται να πατήσει ο χρήστης και όπως ειπώθηκε στην υλοποίηση του Smart Contract και της βάσης δεδομένων, ο χρήστης λαμβάνει το πρώτο του Badge και στην οθόνη του γίνεται άμεσα ανανέωση και εμφάνιση της εικόνας του. Ταυτόχρονα και χωρίς εκείνος να το δει, κατοχυρώνεται και στη βάση δεδομένων (Άρα, στην πρώτη φάση του Smart Contract γίνεται η πρώτη συναλλαγή, ενεργοποιείται η πρώτη συνάρτηση που αναγράφεται στο blockchain. Με το που ολοκληρωθεί η συναλλαγή, ο χρήστης μπορεί να δει το είδος και τον αριθμό των Badge που κατέχει. Τα ανωτέρω φαίνονται στις Εικόνες 17 και 21.



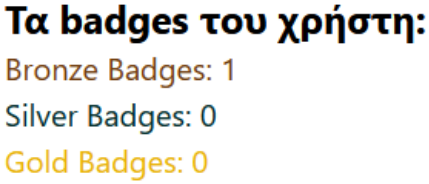

**Εικόνα 17: Το κουμπί που χρειάζεται να πατηθεί για να εγγραφή στην πλατφόρμα.**




**Εικόνα 18: Η συναλλαγή χρειάζεται να ολοκληρωθεί για να γίνει εγγραφή στην πλατφόρμα.**




**Εικόνα 19: Ο χρήστης κατοχυρώνεται στην βάση μετά την ολοκλήρωση της συναλλαγής.**



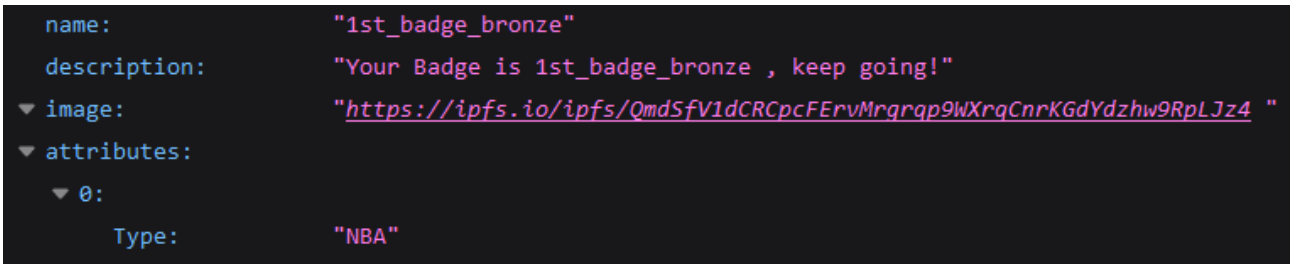

**Εικόνα 20: Η εγγραφή ολοκληρώθηκε από τον χρήστη και του απονεμήθηκε το πρώτο του Badge, το Bronze.**


**Εικόνα 21: Το Badge που απεικονίζεται στον χρήστη.**

Στις λεπτομέρειες που αναγράφονται κάτω από την εικόνα του Badge, αν ο χρήστης επιθυμεί, μπορεί να δει τις περισσότερες πληροφορίες σχετικά με την εικόνα. Εκεί βρίσκονται τα Metadata, που είναι αρχείο JSON. Στο παράδειγμα γράφονται μόνο τα βασικά στοιχεία του Badge.
Αυτά είναι:

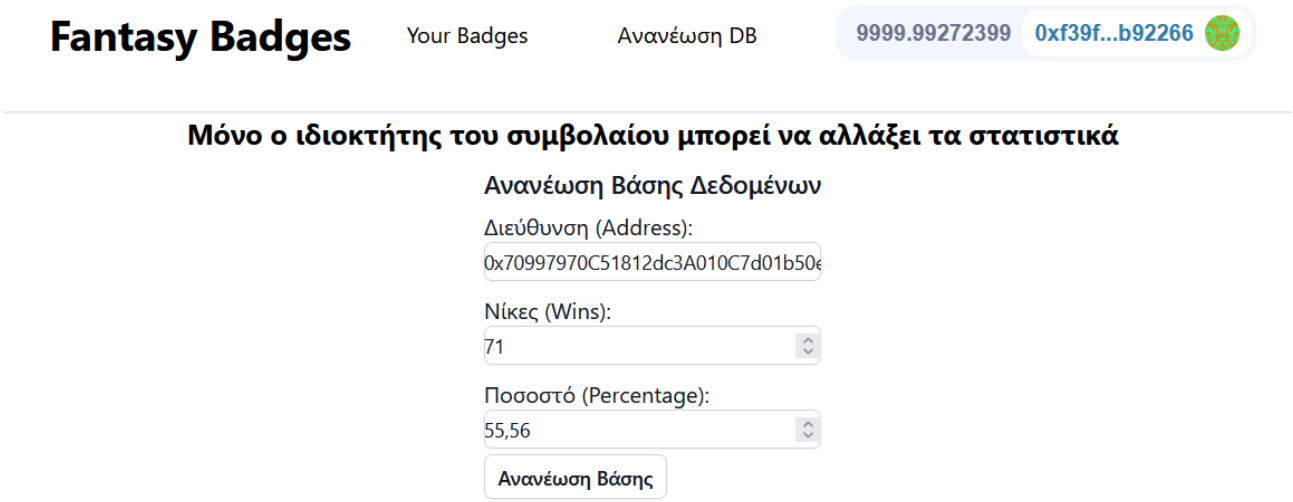
- Το όνομα του Badge.
- Το URI της εικόνας.
- Το άθλημα που αφορά.

Οι πληροφορίες κάθε εταιρίας θα αντιστοιχούν στα δικά της Metadata.

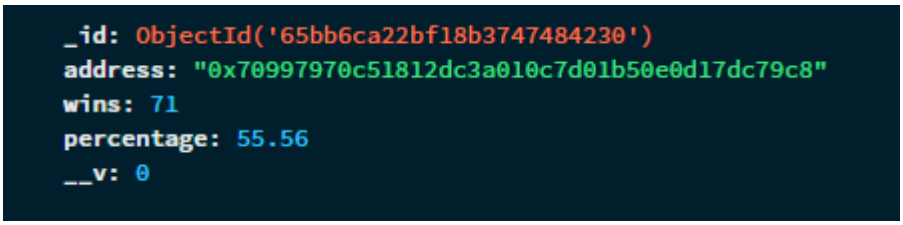



**Εικόνα 22: Τα Metadata του συγκεκριμένου Badge.**

Προχωρώντας η δεύτερη φάση που αφορά την ανανέωση της βάσης δεδομένων, γίνεται στην Εικόνα 10. Για τη διαδικασία αυτή είναι υπεύθυνη η πλατφόρμα καθώς εκείνη έχει την ιδιοκτησία του Smart Contract, αφού το ανέβασε στο blockchain. Καμία άλλη διεύθυνση ή άλλος χρήστης δεν μπορεί να αλλάξει τη βάση δεδομένων πάρα μόνο ο ιδιοκτήτης του Smart Contract. Αν προσπαθήσει κάποιος άλλος χρήστης να αλλάξει τα στατιστικά στοιχεία των παιχτών, τότε δεν θα του επιτραπεί η πρόσβαση για την οποιαδήποτε αλλαγή. Όπως έχει αναφερθεί, ο ρόλος της πλατφόρμας έχει αναληφθεί από τον λογαριασμό με τη διεύθυνση 0xf3f…b92266, όπως φαίνεται και στην Εικόνα 14. Αφού γίνει η αλλαγή των στατιστικών στοιχείων των χρηστών τότε ακολουθεί η επόμενη φάση. Στις Εικόνες 22 και 23 παρουσιάζεται η αλλαγή αυτή.



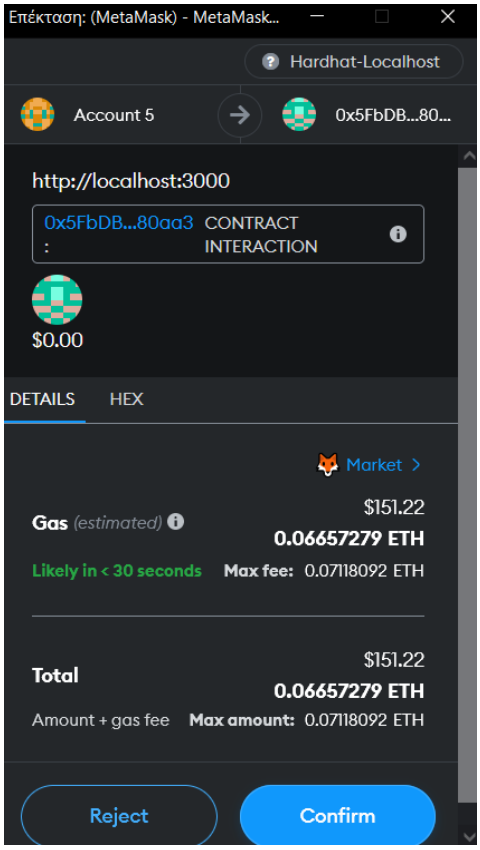

**Εικόνα 23: Είναι συνδεδεμένος ο λογαριασμός που έχει το ρόλο της πλατφόρμας (πάνω δεξιά), έχει βάλει την διεύθυνση του χρήστη που θα γίνει η αλλαγή των στατιστικών στοιχείων και έχουν προστεθεί τα νέα στατιστικά στοιχεία που αφορούν την αθλητική χρονιά.**



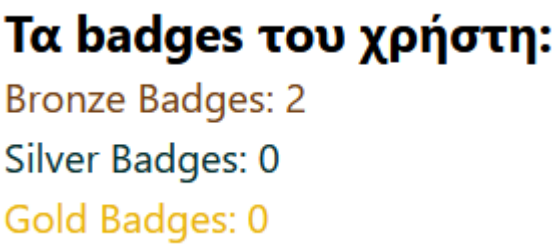

**Εικόνα 24: Η ανανέωση στη βάση δεδομένων**

Στην τρίτη φάση, υλοποιείται η απόκτηση των νέων Badge μετά την αλλαγή των στατιστικών στοιχείων των χρηστών. Οι χρήστες απαιτείται να ζητήσουν τη λήψη του νέου Badge με τη χρήση ενός κουμπιού. Όταν πατηθεί το κουμπί, λαμβάνονται τα στατιστικά στοιχεία που υπάρχουν στη βάση δεδομένων για τον χρήστη που πάτησε το κουμπί. Με βάση τον Πίνακα 1 που έχει δοθεί στο παράδειγμα του 2$^{ου}$ Κεφαλαίου, γίνεται η σύγκριση των στατιστικών στοιχείων για να δοθεί από το Smart Contract το κατάλληλο Badge. Με την απόκτηση του νέου Badge, ανανεώνεται αυτόματα το URI όπου ανήκει στο Badge που μόλις απέκτησε ο χρήστης καθώς και το πόσα Badge έχει συνολικά από το κάθε είδος. Στις Εικόνες 24 μέχρι 27 παρουσιάζεται η απόκτηση του νέου Badge.


**Εικόνα 25: Το κουμπί που χρειάζεται να πατηθεί ώστε να πάρει το Badge του ο χρήστης**




**Εικόνα 26: Χρειάζεται να ολοκληρωθεί η συναλλαγή για να αποικηθεί το Badge.**




**Εικόνα 27: Συνολικά ποσά Badge κατέχει ο χρήστης μετά την εγγραφή του.**


**Εικόνα 28: Η εικόνα του NFT και το URI**

Για λόγους συντομίας παραλείπεται το υπόλοιπο παράδειγμα αλλά η διαδικασία παραμένει ίδια.

Όσον αφορά την επικοινωνία του Smart Contract, γίνεται μέσω της βιβλιοθήκης ether.js όπως έχει αναφερθεί στα εργαλεία. Ταυτόχρονα, όμως, χρειάζεται το abi (Application Binary Interface) και τη διεύθυνση του Smart Contract για να γίνει οποιαδήποτε αλληλεπίδραση. Αυτά γίνονται γνωστά όταν ανέβει το Smart Contract στο δίκτυο.

## 4.4 Παράδειγμα διαφόρων τυχαίων στατιστικών στοιχείων από το front-end

Εφόσον έχει γίνει κατανοητή η διαδικασία αλλαγής στατιστικών στοιχείων και η απόκτηση νέου Badge, παραλείπεται η λεπτομερής περιγραφή και δίνεται το τελικό αποτέλεσμα ώστε να καλυφθούν όλες οι περιπτώσεις που υπάρχουν στο σύστημα αξιολόγησης. Στον Πίνακα 10 αναπτύσσονται οι διάφοροι συνδυασμοί που υπάρχουν με τυχαία νούμερα, καθώς ο βασικός σκοπός του παραδείγματος αυτού είναι η κατανόηση από τον χρήστη για το τι θα βλέπει στην ιστοσελίδα του με την πάροδο των αθλητικών χρονιών.

| Τυχαίοι συνδυασμοί | Συνολικά Badge του χρήστη στο front-end | Εικόνα του Badge για την συγκεκριμένο παράδειγμα |
|---|---|---|
| Εγγραφή του χρήστη.<br>Νίκες: 0<br>Ποσοστό 0% | Bronze Badges: 1<br>Silver Badges: 0<br>Gold Badges: 0 |  |
| Νίκες: 0 – 100 πχ 40<br>Ποσοστό: 40% - 70% πχ 50% | Bronze Badges: 2<br>Silver Badges: 0<br>Gold Badges: 0 |  |
| Νίκες: 101 – 500 πχ 117<br>Ποσοστό: 0% - 40% πχ 35% | Bronze Badges: 3<br>Silver Badges: 0<br>Gold Badges: 0 |  |
| Νίκες: 101 – 500 πχ 250<br>Ποσοστό: 40% - 70% πχ 45% | Bronze Badges: 3<br>Silver Badges: 1<br>Gold Badges: 0 |  |

| | | |
|---|---|---|
| Νίκες: 501 και πάνω πχ 510<br>Ποσοστό: 40% - 70% πχ 42% | Bronze Badges: 3<br>Silver Badges: 2<br>Gold Badges: 0 |  |
| Νίκες: 501 και πάνω πχ 600<br>Ποσοστό: 70% και πάνω πχ 70% | Bronze Badges: 3<br>Silver Badges: 2<br>Gold Badges: 1 |  |
| Νίκες: 501 και πάνω πχ 685<br>Ποσοστό: 40% - 70% πχ 60% | Bronze Badges: 3<br>Silver Badges: 3<br>Gold Badges: 1 |  |
| Νίκες: 501 και πάνω πχ 710<br>Ποσοστό: 40% - 70% πχ 40% | Bronze Badges: 3<br>Silver Badges: 4<br>Gold Badges: 1 |  |
| Νίκες: 501 και πάνω πχ 795<br>Ποσοστό: 0% - 40% πχ 38.9% | Bronze Badges: 4<br>Silver Badges: 4<br>Gold Badges: 1 |  |

**Πίνακας 11: Παράδειγμα τυχαίων στατιστικών στοιχείων.**

## 4.5 Συμπεράσματα υλοποίησης

Μετά την ολοκλήρωση των υλοποιήσεων κάθε κομματιού, παρατηρείται ότι υπάρχουν τρεις φάκελοι στον VS Code. Ο πρώτος φάκελος αφορά το blockchain, όπου το hardhat εκτελείται και ο node είναι ενεργός. Ο δεύτερος φάκελος αφορά το back-end, όπου υπάρχει η βάση δεδομένων και ο server. Ο τρίτος φάκελος είναι το front-end. Για τη χρήση της εφαρμογής, απαιτείται η λειτουργία και των τριών κομματιών. Αυτό περιλαμβάνει την εκτέλεση του node με το blockchain, την ενεργοποίηση του server της βάσης δεδομένων, τον τοπικό server που επικοινωνεί με τη βάση δεδομένων, και την ενεργοποίηση του front-end για τις αλληλεπιδράσεις με τους χρήστες στο UI. Η διαδικασία απόκτησης κάποιου Badge θεωρείται εύκολη, καθώς έχει υλοποιηθεί με τρόπο που να είναι ξεκάθαρη για όλους τους χρήστες. Ο πλήρης έλεγχος της διαδικασίας για την αλλαγή των στατιστικών στοιχείων, έχει αναληφθεί από τη διεύθυνση της πλατφόρμας, ενώ η απόκτηση ενός Badge δεν επιτρέπεται σε κανέναν χρήστη παρά μόνον εάν έχει ολοκληρωθεί η εγγραφή του.

Τέλος, με τη χρήση του NFT, παρόλο που τα Badge έχουν ίδια ακριβώς εικόνα, στην ουσία κανένα από αυτά δεν είναι ίδιο και έτσι, ο κάθε χρήστης έχει τα δικά του Badge μόνο.

# 5 ΣΥΜΠΕΡΑΣΜΑΤΑ- ΜΕΛΛΟΝΤΙΚΕΣ ΠΡΟΟΠΤΙΚΕΣ

Έχοντας ολοκληρώσει τη διπλωματική εργασία σε ένα νέο αντικείμενο για τον φοιτητή, εξήχθη το συμπέρασμα ότι η εφαρμογή θεωρείται το κατάλληλο ξεκίνημα για ένα αρχάριο επίπεδο. Το ενδιαφέρον κεντρίζεται ανεξαρτήτως των γνώσεων που προϋπήρχαν, δημιουργώντας κίνητρο για περαιτέρω εμβάθυνση στον τομέα του blockchain και του web development. Επιπλέον, κατανοήθηκε από τον φοιτητή, πώς λειτουργεί μια web εφαρμογή για το Web 2.0 και το Web 3.0. Ταυτόχρονα, λόγω της δημιουργίας του dApp, χρησιμοποιήθηκαν πολλαπλές τεχνολογίες, αποκτώντας έτσι βασική κατανόηση της αρχιτεκτονικής MERN Stack, του IPFS και των Metadata, αλλά και σφαιρική γνώση στον τομέα του blockchain, κυρίως όμως στα NFTs. Τα NFTs έχουν τη δυνατότητα ανταλλαγής ή πώλησης αλλά στη συγκεκριμένη εφαρμογή δεν γίνεται επιτρεπτό. Έτσι, αυξάνεται η αίσθηση της επίτευξης στόχου και της μοναδικότητας στο παιχνίδι όταν αποκτάται κάποιο Badge. Παρόλο που η εφαρμογή τέθηκε σε αρχάριο επίπεδο για εκπαιδευτικούς λόγους, ο σκοπός της παραμένει σημαντικός, καθώς μελλοντικά θα μπορούσε να χρησιμοποιηθεί από πραγματικές εταιρίες, είτε παιχνιδιών είτε στοιχηματικές. Σε αυτή την περίπτωση, το Smart Contract θα έπρεπε να τροποποιηθεί για να είναι στα πλαίσια που απαιτούνται από κάθε εταιρία, είτε έχει να κάνει με το πόσα Badge θα ήθελε η εταιρία να διαθέτει, είτε με την αντιστοιχία των Badge. Ακόμα, αν η εταιρία ήθελε να παρέχει περισσότερη ασφάλεια και εμπιστοσύνη στους πελάτες της, τότε θα μπορούσαν τα κριτήριά της να υλοποιηθούν στο blockchain. Έτσι, θα υπήρχε μόνο η βάση δεδομένων με τα στατιστικά στοιχεία. Επιπλέον, μια ακόμα μελλοντική αναβάθμιση θα ήταν η υλοποίηση με το πρότυπο του ERC-1155, ώστε να διαχειρίζεται πολλούς περισσότερους χρήστες και περισσότερα Badge. Επίσης, μια τροποποίηση στο πλαίσιο της διπλωματικής θα ήταν τα στατιστικά στοιχεία να εισέρχονται απευθείας από μια πλατφόρμα με τη χρήση API και όχι να δίνονται τυπογραφικά, όπως ήταν ο αρχικός σκοπός.

## Βιβλιογραφία – Αναφορές - Διαδικτυακές Πηγές

[1] Αλυσίδες Συστοιχιών (Blockchain) (2023), Πατρικάκης, Χ., Λελίγκου, Ε., & Κόγιας, Δ., Online πηγή: https://repository.kallipos.gr/handle/11419/9130 [Τελευταία πρόσβαση: Δεκέμβριος 2023].
[2] Metamask website (2023). Online πηγή: https://metamask.io/
[Τελευταία πρόσβαση: Δεκέμβριος 2023].
[3] Alchemy website (2023). Online πηγή: https://ipfs.tech/
[Τελευταία πρόσβαση: Δεκέμβριος 2023].
[4] IPFS website (2023). Online πηγή: https://ipfs.tech/
[Τελευταία πρόσβαση: Δεκέμβριος 2023].
[5] Pinata website (2023). Online πηγή: https://www.pinata.cloud/
[Τελευταία πρόσβαση: Δεκέμβριος 2023].
[6] Filebase website (2023). Online πηγή: https://filebase.com/
[Τελευταία πρόσβαση: Δεκέμβριος 2023].
[7] NFT Storage website (2023). Online πηγή: https://nft.storage/
[Τελευταία πρόσβαση: Δεκέμβριος 2023].
[8] Infura website (2023). Online πηγή: https://www.infura.io/
[Τελευταία πρόσβαση: Δεκέμβριος 2023].
[9] ERC-20 vs ERC-721 website (2023). Online πηγή: https://info.etherscan.com/what-is-erc721/
[10] Fantasy Sports & Gaming Association website (2023). Online πηγή: https://thefsga.org/industry-demographics/ [Τελευταία πρόσβαση: Δεκέμβριος 2023].
[11] What is blockchain technology? How does it work? Website (2023). Online πηγή: https://cointelegraph.com/learn/how-does-blockchain-work-everything-there-is-to-know
[Τελευταία πρόσβαση: Δεκέμβριος 2023].
[12] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Πηγή: https://bitcoin.org/bitcoin.pdf [Τελευταία πρόσβαση: Δεκέμβριος 2023].
[13] Buterin, V. (2013). Ethereum. White paper. Online πηγή: https://ethereum.org/en/whitepaper
[Τελευταία πρόσβαση: Δεκέμβριος 2023].
[14] ESPN Fantasy (2023). Online πηγή: https://www.espn.com/fantasy/mens-basketball/
[Τελευταία πρόσβαση: Δεκέμβριος 2023].
[15] Fantrax (2023). Online πηγή: https://www.fantrax.com/home
[Τελευταία πρόσβαση: Δεκέμβριος 2023].
[16] Yahoo sport (2023). Online πηγε: https://sports.yahoo.com/fantasy/
[Τελευταία πρόσβαση: Δεκέμβριος 2023].
[17] OpenZeppelin ERC721 (2023). Online πηγή: https://wizard.openzeppelin.com/#erc721
[Τελευταία πρόσβαση: Δεκέμβριος 2023].
[18] Remix (2023). Online πηγή:https://remix.ethereum.org/
[Τελευταία πρόσβαση: Δεκέμβριος 2023].
[19] Visual Studio Code (2023). Online πηγή: https://code.visualstudio.com/
[Τελευταία πρόσβαση: Δεκέμβριος 2023].
[20] OpenZeppelin (2023). Online πηγή: https://www.openzeppelin.com/
[Τελευταία πρόσβαση: Δεκέμβριος 2023].
[21] Hardhat (2023). Online πηγή: https://hardhat.org/

[Τελευταία πρόσβαση: Δεκέμβριος 2023].
[22] MERN Stack (2023). Online πηγή: https://www.mongodb.com/mern-stack
[Τελευταία πρόσβαση: Δεκέμβριος 2023].
[23] Προσθήκη λογαριασμών από το Hardhat (2023). Online πηγή: https://support.metamask.io/hc/en-us/articles/360015489331-How-to-import-an-account
[Τελευταία πρόσβαση: Δεκέμβριος 2023].
[23] Προσθήκη δικτύου στο Metamask (2023). Online πηγη: https://support.metamask.io/hc/en-us/articles/360043227612-How-to-add-a-custom-network-RPC
[Τελευταία πρόσβαση: Δεκέμβριος 2023].

## Παράρτημα Α : Κώδικας του Smart Contract

Οι δυο συναρτήσεις που γράφουν στο blockchain, οι συναρτήσεις που γίνεται συναλλαγή.

1)Συνάρτηση εγγραφής των χρηστών και η απόκτηση του πρώτου Badge:

```
function registerUser() external {
        if (userBronzeBadges[msg.sender] != 0) {
            revert Exei_kanei_ergafi();
        }
        receiveBadge[BadgeType.Silver] = false;
        receiveBadge[BadgeType.Gold] = false;

        s_TokenCounter = s_TokenCounter + 1;

        s_players.push(msg.sender);
        userBadge[msg.sender] = BadgeType.Bronze;
        userBronzeBadges[msg.sender] = 1;
        currentBadge = BadgeType.Bronze;
        emit UserRegistered(msg.sender);
        emit BadgeAwarded(msg.sender, currentBadge);
        _safeMint(msg.sender, s_TokenCounter);

    }
```

2)Συνάρτηση δημιουργίας νέων Badge:

```
function CreateBadge(uint256 badgeType) public {
        require(
            badgeType >= uint256(BadgeType.Bronze) && badgeType <=
uint256(BadgeType.Gold),
            "Invalid badge type"
        );
        // Ελέγχεται αν έχει περάσει ο κατάλληλος χρόνος από την τελευταία κλήση
της συνάρτησης
    require(block.timestamp >= endTime, "Not enough time has passed");
        if (userBronzeBadges[msg.sender] < 1) {
            revert Den_exeis_kanei_EGRAFI();
        }
        if (badgeType == 1) {
            if (receiveBadge[BadgeType.Silver] == false) {
                s_TokenCounter = s_TokenCounter + 1;
                userBadge[msg.sender] = BadgeType.Silver;
                userSilverBadges[msg.sender] = 1;
                currentBadge = BadgeType.Silver;
                emit BadgeAwarded(msg.sender, currentBadge);
                _safeMint(msg.sender, s_TokenCounter);
                receiveBadge[BadgeType.Silver] = true;
```

```
            } else {
                userBadge[msg.sender] = BadgeType.Silver;
                userSilverBadges[msg.sender] += 1;
                currentBadge = BadgeType.Silver;
                emit BadgeAwarded(msg.sender, currentBadge);
            }
            endTime = block.timestamp + 10; //365 days για να περάσει ένας χρόνος
από την δημιουργία του Badge
        } else if (badgeType == 2) {
            if (userBadge[msg.sender] != BadgeType.Gold) {
                s_TokenCounter = s_TokenCounter + 1;
                userBadge[msg.sender] = BadgeType.Gold;
                userGoldBadges[msg.sender] = 1;
                currentBadge = BadgeType.Gold;
                emit BadgeAwarded(msg.sender, currentBadge);
                _safeMint(msg.sender, s_TokenCounter);
                receiveBadge[BadgeType.Gold] = true;
            } else {
                userBadge[msg.sender] = BadgeType.Gold;
                userGoldBadges[msg.sender] += 1;
                currentBadge = BadgeType.Gold;
                emit BadgeAwarded(msg.sender, currentBadge);
            }
            endTime = block.timestamp + 10; //365 days για να περάσει ένας χρόνος
από την δημιουργία του Badge
        }
        else if (badgeType == 0) {
            userBadge[msg.sender] = BadgeType.Bronze;
            currentBadge = BadgeType.Bronze;
            userBronzeBadges[msg.sender] += 1;
            emit BadgeAwarded(msg.sender, currentBadge);
            endTime = block.timestamp + 10; //365 days για να περάσει ένας χρόνος
από την δημιουργία του Badge
        } else {
            revert("Invalid badge type");
        }
        emit UserRegistered(msg.sender);
    }
```

Οι συναρτήσεις που διαβάζουν από το block chain:

1) Η ποσότητα των Bronze Badge που κατέχονται από τον χρήστη

```
function getBronzeBadge() public view returns (uint256) {
        return userBronzeBadges[msg.sender];
}
```

2) Η ποσότητα των Silver Badge που κατέχονται από τον χρήστη

```
    function getSilverBadge() public view returns (uint256) {
```

```
        return userSilverBadges[msg.sender];
    }
```

3) Η ποσότητα των Gold Badge που κατέχονται από τον χρήστη

```
function getGoldBadge() public view returns (uint256) {
        return userGoldBadges[msg.sender];
}
```

4) Οι συναρτήσεις που χρησιμοποιούνται για τη φανέρωση της εικόνας του Badge και το URI

```
function getUserBadge() public view returns (BadgeType) {
     return userBadge[msg.sender];
}
function getCurrentBadgeURI() public view returns (string memory) {
     if (userBronzeBadges[msg.sender] < 1) {
          revert Den_exeis_kanei_EGRAFI();
     }

     if (userBadge[msg.sender] == BadgeType.Bronze) {
          return s_BadgesUris[uint256(BadgeType.Bronze)];
     } else if (userBadge[msg.sender] == BadgeType.Silver) {
          return s_BadgesUris[uint256(BadgeType.Silver)];
     } else if (userBadge[msg.sender] == BadgeType.Gold) {
          return s_BadgesUris[uint256(BadgeType.Gold)];
     } else {
          revert("Invalid badge type");
     }
}
```

Ο πλήρης κώδικας του Smart Contract

```
// SPDX-License-Identifier: MIT

pragma solidity ^0.8.8;

import "@openzeppelin/Smart
Contracts/Token/ERC721/extensions/ERC721URIStorage.sol";

error Den_exeis_kanei_EGRAFI();
error Exei_kanei_ergafi();

Smart Contract Badge is ERC721URIStorage {
    enum BadgeType {
        Bronze,
        Silver,
        Gold
    }

    mapping(address => BadgeType) public userBadge;
```

```
    mapping(BadgeType => bool) public receiveBadge;
    mapping(address => uint256) public userBronzeBadges;
    mapping(address => uint256) public userSilverBadges;
    mapping(address => uint256) public userGoldBadges;

    address[] private s_players;
    BadgeType private currentBadge
    uint256 private s_TokenCounter;
    string[] internal s_BadgesUris;

    uint256 public endTime;

    event UserRegistered(address indexed user);
    event BadgeAwarded(address indexed user, BadgeType badge);
    event LogMessage(string message);



    constructor() ERC721("Badge NFTs", "BG") {
        s_BadgesUris.push(
https://ipfs.io/ipfs/QmRJxSofVHmH9M7cqHDpreMYHATJbxekdDUQ7USnAqFPNe"
        );
        s_BadgesUris.push(
https://ipfs.io/ipfs/QmQ7NUNcHWFNbj3hZJMNhC53dgfrStvaVvcBVC5YnAp8wq"
        );
        s_BadgesUris.push(
           https://ipfs.io/ipfs/QmYWwqEdnFSiJxS3etcVssdKMpdCurFyBKSEG98mACaf3n"
        );
    }

    function registerUser() external {
        // Ελέγχεται αν ο χρήστης έχει ήδη το Bronze Badge
        if (userBronzeBadges[msg.sender] != 0) {
            revert Exei_kanei_ergafi();
        }
        receiveBadge[BadgeType.Silver] = false;
        receiveBadge[BadgeType.Gold] = false;

        s_TokenCounter = s_TokenCounter + 1;

        s_players.push(msg.sender);
        userBadge[msg.sender] = BadgeType.Bronze;
        userBronzeBadges[msg.sender] = 1;
        currentBadge = BadgeType.Bronze;
        emit UserRegistered(msg.sender);
        emit BadgeAwarded(msg.sender, currentBadge);
        emit LogMessage("done");
        _safeMint(msg.sender, s_TokenCounter);
    }
```

```
    function CreateBadge(uint256 badgeType) public {
        require(
            badgeType >= uint256(BadgeType.Bronze) && badgeType <=
uint256(BadgeType.Gold),
            "Invalid badge type"
        );
        // Ελέγχεται αν έχει περάσει ο κατάλληλος χρόνος από την τελευταία
δημιουργία του Badge
    require(block.timestamp >= endTime, "Not enough time has passed");
        if (userBronzeBadges[msg.sender] < 1) {
            revert Den_exeis_kanei_EGRAFI();
        }
        if (badgeType == 1) {
            if (receiveBadge[BadgeType.Silver] == false) {
                s_TokenCounter = s_TokenCounter + 1;
                userBadge[msg.sender] = BadgeType.Silver;
                userSilverBadges[msg.sender] = 1;
                currentBadge = BadgeType.Silver;
                emit BadgeAwarded(msg.sender, currentBadge);
                _safeMint(msg.sender, s_TokenCounter);
                receiveBadge[BadgeType.Silver] = true;
            } else {
                userBadge[msg.sender] = BadgeType.Silver;
                userSilverBadges[msg.sender] += 1;
                currentBadge = BadgeType.Silver;
                emit BadgeAwarded(msg.sender, currentBadge);
            }
            endTime = block.timestamp + 10; //365 days για να περάσει ένας χρόνος
από την δημιουργία του Badge
        } else if (badgeType == 2) {
            if (userBadge[msg.sender] != BadgeType.Gold) {
                s_TokenCounter = s_TokenCounter + 1;
                userBadge[msg.sender] = BadgeType.Gold;
                userGoldBadges[msg.sender] = 1;
                currentBadge = BadgeType.Gold;
                emit BadgeAwarded(msg.sender, currentBadge);
                _safeMint(msg.sender, s_TokenCounter);
                receiveBadge[BadgeType.Gold] = true;
            } else {
                userBadge[msg.sender] = BadgeType.Gold;
                userGoldBadges[msg.sender] += 1;
                currentBadge = BadgeType.Gold;
                emit BadgeAwarded(msg.sender, currentBadge);
            }
            endTime = block.timestamp + 10; //365 days για να περάσει ένας χρόνος
από την δημιουργία του Badge
        }
        else if (badgeType == 0) {
```

```
            userBadge[msg.sender] = BadgeType.Bronze;
            currentBadge = BadgeType.Bronze;
            userBronzeBadges[msg.sender] += 1;
            emit BadgeAwarded(msg.sender, currentBadge);
            endTime = block.timestamp + 10; //365 days για να περάσει ένας χρόνος
από την δημιουργία του Badge
        } else {
            revert("Invalid badge type");
        }
        emit UserRegistered(msg.sender);
    }



    function getSilverState() public view returns (bool) {
        return receiveBadge[BadgeType.Silver];
    }

    function getGoldState() public view returns (bool) {
        return receiveBadge[BadgeType.Gold];
    }

    function getUserBadge() public view returns (BadgeType) {
        return userBadge[msg.sender];
    }

    function getBronzeBadge() public view returns (uint256) {
        return userBronzeBadges[msg.sender];
    }

    function getSilverBadge() public view returns (uint256) {
        return userSilverBadges[msg.sender];
    }

    function getGoldBadge() public view returns (uint256) {
        return userGoldBadges[msg.sender];
    }

    function getCurrentBadgeURI() public view returns (string memory) {
        if (userBronzeBadges[msg.sender] < 1) {
            revert Den_exeis_kanei_EGRAFI();
        }

        if (userBadge[msg.sender] == BadgeType.Bronze) {
            return s_BadgesUris[uint256(BadgeType.Bronze)];
        } else if (userBadge[msg.sender] == BadgeType.Silver) {
            return s_BadgesUris[uint256(BadgeType.Silver)];
        } else if (userBadge[msg.sender] == BadgeType.Gold) {
            return s_BadgesUris[uint256(BadgeType.Gold)];
```

```
        } else {
            revert("Invalid badge type");
        }
    }

//Τροποποιούνται οι συναρτήσεις της μεταφοράς των NFTs ώστε να μην μπορούν να ανταλλαχτούν ή να πουληθούν τα Badge

    function transferFrom(
    address from,
    address to,
    uint256 TokenId
) public override {
    require(false, "you cont do that");
}

function safeTransferFrom(
    address from,
    address to,
    uint256 TokenId
) public override {
    require(false, "you cont do that boy");
}

}
```