



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

**Δημιουργία web interface με χρήση τεχνολογιών cloud computing για την εξακρίβωση γνησιότητας εγγράφων, αξιοποιώντας APIs βασισμένα σε Blockchain**

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΔΑΜΙΑΝΟΣ ΠΑΠΠΑΣ

**Επιβλέπων :** Ασκούνης Δημήτριος

Καθηγητής Ε.Μ.Π.

Αθήνα, Νοέμβριος 2021





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

**Δημιουργία web interface με χρήση τεχνολογιών cloud computing για την εξακρίβωση γνησιότητας εγγράφων, αξιοποιώντας APIs βασισμένα σε Blockchain**

**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

**ΔΑΜΙΑΝΟΣ ΠΑΠΠΑΣ**

**Επιβλέπων : Ασκούνης Δημήτριος**

**Καθηγητής Ε.Μ.Π.**

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 5<sup>η</sup> Νοεμβρίου 2021.

*(Υπογραφή)*

.....  
Ασκούνης Δημήτριος  
Καθηγητής Ε.Μ.Π.

*(Υπογραφή)*

.....  
Ιωάννης Ψαρά  
Καθηγητής Ε.Μ.Π.

*(Υπογραφή)*

.....  
Χάρης Δούκας  
Καθηγητής Ε.Μ.Π.

Αθήνα, Νοέμβριος 2021

(Υπογραφή)

.....  
**ΔΑΜΙΑΝΟΣ ΠΑΠΠΑΣ**

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

Copyright © Damianos Pappas,2021.

Με επιφύλαξη παντός δικαιώματος.All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα. Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού Μετσόβιου Πολυτεχνείου.

## Περίληψη

Ο μέσος άνθρωπος στις μέρες μας αλλάζει 12 διαφορετικές θέσεις εργασίας κατά μέσο όρο στην διάρκεια της καριέρας του σύμφωνα με έρευνες. Αυτό σημαίνει πως θα μπει σίγουρα στην διαδικασία διεκδίκησης μιας θέσης, με ό,τι συνεπάγεται αυτό. Ο recruiter από την πλευρά του θα πρέπει να φροντίσει να πιστοποιήσει την γνησιότητα των εγγράφων κάθε υποψηφίου, διαδικασία που με τα μέχρι τώρα δεδομένα, είναι απίστευτα χρονοβόρα, πολυέξοδη και όχι τόσο ασφαλής.

Μια λύση στο πρόβλημα αυτό μπορεί να δώσει μια αποκεντρωμένη τεχνολογία, που όλοι είναι ομότιμοι στο δίκτυο της και οι συναλλαγές σε αυτό δεν μπορούν να μεταποιηθούν μετά την καταχώρηση τους, η τεχνολογία του blockchain. Με αυτόν το τρόπο η επικύρωση και η πιστοποίηση εγγράφων γίνεται γρήγορα και με ασφάλεια χωρίς την μεσολάβηση μεσαζόντων.

Στα πλαίσια αυτής της διπλωματικής, γίνεται έρευνα και χρήση προηγμένων τεχνολογιών και εργαλείων στον τομέα της ανάπτυξης εφαρμογών, με στόχο την δημιουργία μιας διαδικτυακής εφαρμογής που λύνει το παραπάνω πρόβλημα. Δηλαδή δίνει την δυνατότητα στον χρήστη να πιστοποιήσει την γνησιότητα έγγραφων με την χρήση APIs που βασίζονται στην τεχνολογία blockchain για επικύρωση και πιστοποίηση δικαιολογητικών.

Ακόμη μελετάται η τεχνολογία «cloud computing» όπως και τα πλεονεκτήματα που παρέχουν οι υπηρεσίες «cloud» σε μια εφαρμογή. Στις μέρες μας παρατηρείται η τάση του τεχνολογικού κόσμου να μεταφέρεται σε αυτό με σκοπό την εκμετάλλευση των πλεονεκτημάτων που παρέχει. Έτσι λοιπόν με την σειρά μας, κάνουμε χρήση των υπηρεσιών «cloud» για της ανάγκες της εφαρμογής μέσω της πλατφόρμας του Azure Microsoft, διασφαλίζοντας μελλοντική επεκτασιμότητα, ελαστικότητα, προσαρμοστικότητα και ασφάλεια της λύσης που προτείνουμε.

**Λέξεις Κλειδιά:** <<Blockchain, πιστοποίηση εγγράφων, επικύρωση εγγράφων, Smart Contracts, ανάπτυξη εφαρμογών, web-app Java, Spring, MVC, Maven, Cloud, Cloud Computing, Microsoft Azure>>



## **Abstract**

Nowadays, according to research, the average person changes 12 different jobs on average during his career. This means that he will enter the process of claiming a job position at least once in his lifetime. The recruiter for his part should make sure to certify the authenticity of the documents each candidate provides, a process that so far, is incredibly time consuming, costly, and not safe.

A solution to this problem can be a decentralized technology, with peer-to-peer network and the transactions in the network cannot be processed after their registration, this is the blockchain technology. With blockchain, the validation and certification of documents is fast and safe, without the mediation of intermediaries.

In this diploma thesis, are being studied and used advanced technologies and tools in the field of software development, with the aim of creating a web application that solves the above problem. The web application gives to the user the opportunity to certify the authenticity of documents using APIs based on blockchain technology for validation and certification.

Cloud computing technology is also being studied, as well as the benefits that cloud services provide to an application. Nowadays there is a tendency of the technological world to migrate to the "cloud" to take advantage of the possibilities it provides. For this reason, we use the "cloud" services to fulfil the needs of our application through the Azure Microsoft platform, ensuring future scalability, adaptability, elasticity, and security of the solution we propose.

**Keywords:** << Blockchain, documents validation, documents certification, Smart Contracts, web development, web-app, Java, Spring, MVC, Maven, Cloud, Cloud Computing, Microsoft Azure >>





## Ευχαριστίες

Ξεκινώντας, θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα μου, τον Καθηγητή κ. Δημήτριο Ασκούνη για την εμπιστοσύνη και την ευκαιρία που μου έδωσε να ασχοληθώ με την παρούσα εργασία. Εν συνεχεία, δεν θα μπορούσα να μην ευχαριστήσω τον διδακτορικό κ. Παναγιώτη Ζαραφίδη τόσο για την καθοδήγηση του όσο και για την εξαιρετικής σημασίας βοήθεια και στήριξη που μου παρείχε καθ' όλη τη διάρκεια εκπόνησης της παρούσας εργασίας. Οι συμβουλές και οι υποδείξεις του κ. Παναγιώτη ήταν καθοριστικές για την τελική μορφή της εργασίας και χωρίς την πολύτιμη συμβολή του, δεν θα έφτανα σε αυτό το σημείο. Από τον κύκλο των ευχαριστιών μου, δε θα μπορούσαν να λείπουν τα εναπομείναντα δύο μέλη της Τριμελούς Εξεταστικής Επιτροπής, ο κ. Χάρης Δούκας, Αναπληρωτής Καθηγητής του Ε.Μ.Π., και ο κ. Ιωάννης Ψαράς, Καθηγητής Ε.Μ.Π., τόσο γιατί δέχτηκαν να απαρτίσουν την Επιτροπή της διπλωματικής αυτής εργασίας, όσο και για το ενδιαφέρον που έδειξαν. Θα ήθελα ακόμη, να ευχαριστήσω όλους τους κοντινούς μου ανθρώπους και φίλους που στάθηκαν δίπλα μου σε αυτό το μεγάλο ταξίδι και με βοήθησαν, ο καθένας με τον τρόπο του. Ένα μεγάλο ευχαριστώ οφείλω στην αγαπημένη μου οικογένεια και ειδικά στους γονείς μου για την στήριξη και την εμπιστοσύνη τους, όντας πάντα στο πλευρό μου όλα αυτά τα χρόνια.

Δαμιανός Παπιάς  
Αθήνα, 5<sup>η</sup> Νοεμβρίου 2021

*“The value of an idea lies in the using of it.”  
Thomas Edison*



# Περιεχόμενα

<b>Ευρετήριο Εικόνων .....</b>	<b>1</b>
<b>Κεφάλαιο 1: Εισαγωγή.....</b>	<b>1</b>
1.1 Ορισμός Προβλήματος .....	1
1.2 Το Blockchain ως λύση.....	1
1.3 Ανάπτυξη τεχνολογικά προηγμένης web εφαρμογής .....	2
1.4 Οργάνωση Κειμένου.....	2
<b>Κεφάλαιο 2: Blockchain και Πιστοποίηση .....</b>	<b>3</b>
2.1 Η αρχή του Blockchain .....	3
2.2 Η εξέλιξη του Blockchain από ένα κρυπτονόμισμα .....	3
2.3 Θεμελιώδεις έννοιες του Blockchain .....	4
2.4 Πως λειτουργεί το Blockchain .....	5
2.4.1 Αποκεντρωμένο σύστημα.....	5
2.4.2 Nodes.....	6
2.4.3 Applications and Network.....	6
2.4.4 Smart Contracts.....	7
2.4.5 Distributed ledger technology.....	7
2.5 Τύποι Blockchain.....	8
2.5.1 Permissionless (χωρίς άδεια) .....	8
2.5.2 Permissioned(με άδεια) .....	9
2.6 Πλατφόρμες Blockchain .....	10
2.6.1 Ethereum .....	10
2.6.1 Bitcoin.....	11
2.6.3 Ripple .....	11
2.7 Πιστοποίηση μέσω Blockchain .....	11
<b>Κεφάλαιο 3: Blockchain APIs για Πιστοποίηση Εγγράφων .....</b>	<b>13</b>
3.1 Έρευνα για Blockchain Εφαρμογές Πιστοποίησης Εγγράφων .....	13
3.1.1 OpenCerts.....	13
3.1.2 SmartDegrees.....	14
3.1.3 BlockSign.....	14
3.1.4 BTCert.....	14
3.1.5 EduCtx.....	15
3.1.6 Blockcerts.....	16
3.1.7 Qualichain.....	16
3.2 Blockchain API που προσπαθήσαμε να υλοποιήσουμε.....	18

3.2.1 Qualichain API .....	18
3.2.2 Blockcerts API.....	18
<b>Κεφάλαιο 4: Τεχνολογίες και Λειτουργίες της εφαρμογής.....</b>	<b>20</b>
4.1 Πλατφόρμες και εργαλεία ανάπτυξης.....	20
4.1.1 Βάση Δεδομένων .....	20
4.1.2 Back-End .....	21
4.1.3 Front-End.....	22
4.1.4 Other technologies .....	23
4.2 Λειτουργικότητες της Εφαρμογής.....	24
4.2.1 Βασικές Λειτουργικότητες Απλού Χρήστη.....	25
4.2.2 Άλλες Λειτουργικότητες .....	26
4.2.3 Αποκλειστικές Λειτουργικότητες του απλού Χρήστη-Recruiter.....	26
4.2.4 Αποκλειστικές Λειτουργικότητες του Διαχειριστή (root user).....	27
4.3 Λειτουργικότητα για την πιστοποίηση εγγράφων .....	28
4.3.1 Κύρια λειτουργικότητα στην εφαρμογή.....	28
4.3.2 Πως γίνεται η πιστοποίηση από τα blockchain apis.....	29
<b>Κεφάλαιο 5: Ανάπτυξη της Εφαρμογής.....</b>	<b>30</b>
5.1 Business Model.....	30
5.1.1 Πρόβλημα που καλούμαστε να λύσουμε.....	30
5.1.2 Ομάδες Χρηστών .....	30
5.1.3 Blockchain APIs .....	31
5.1.4 Αλληλεπίδραση και Επεκτασιμότητα .....	31
5.2 Αρχιτεκτονική.....	32
5.2.1 MVC framework.....	32
5.2.2 Σχεδιασμός και Υλοποίηση .....	33
5.2.3 Δέντρο Κλάσεων.....	34
5.2.4 Σχεσιακό διάγραμμα οντοτήτων .....	35
5.3 Guide how to use the web-app.....	36
5.3.1 Χρήστης.....	36
5.3.2 Διαχειριστής (root user) .....	45
5.3.3 Mobile .....	48
5.4 Εγκατάσταση εφαρμογής και GitHub .....	49
5.4.1 GitHub.....	49
5.4.1 Εγκατάσταση Εφαρμογής.....	49
<b>Κεφάλαιο 6: Cloud Computing και η εφαρμογή του(AZURE).....</b>	<b>50</b>
6.1 Τι είναι το Cloud Computing .....	50
6.2 Ιστορία πίσω από το Cloud Computing .....	51

6.3 Από τι διακρίνεται το cloud computing .....	53
6.4 Πλεονεκτήματα του Cloud (Azure) .....	53
6.5 Ποια είναι τα μοντέλα cloud service;.....	54
6.5.1 Software as a Service – (SaaS) .....	54
6.5.2 Platform as a Service – (PaaS).....	55
6.5.3 Infrastructure as a Service – (IaaS) .....	55
6.6 Σύγκριση μεταξύ των μοντέλων cloud service.....	56
6.6.1. SaaS.....	56
6.6.2. PaaS.....	56
6.6.3. IaaS.....	57
6.7 Διαφορετικοί τύποι μοντέλων cloud.....	58
6.7.1 Δημόσιο νέφος (Public Cloud) .....	58
6.7.2 Ιδιωτικό νέφος (Private Cloud).....	58
6.7.3 Υβριδικό νέφος (Hybrid Cloud) .....	59
Bonus Κοινοτικό νέφος (Community Cloud) .....	59
6.7 Εισαγωγή στο Microsoft Azure .....	60
6.8 Υπηρεσίες και εργαλεία που προσφέρει το Microsoft Azure.....	60
6.8.1 Υπηρεσίες και εργαλεία .....	60
6.8.2 Τιμολογιακές πολιτικές του Microsoft Azure.....	62
6.9 Χρήση του Azure για το deployment του web-app στο cloud .....	64
6.9.1 Δημιουργία λογαριασμού στο Microsoft Azure .....	64
6.9.2 Δημιουργία Resource Group στο Azure.....	66
6.9.3 Δημιουργία της βάσης δεδομένων στο cloud .....	66
6.9.4 Δημιουργία Web App Service .....	72
6.9.5 Code Deployment μέσω του IntelliJ IDEA .....	76
6.9.6 Επιτυχής μετάβαση στο “cloud” .....	79
<b>Κεφάλαιο 7: Σύνοψη και Συμπεράσματα .....</b>	<b>80</b>
7.1 Σύνοψη.....	80
7.2 Συμπεράσματα και μελλοντικές επεκτάσεις.....	81
<b>Βιβλιογραφία .....</b>	<b>83</b>

# Ευρετήριο Εικόνων

Εικόνα 1: Ιστορία του Blockchain .....	3
Εικόνα 2: Blockchain Programming Context .....	4
Εικόνα 3: Blockchain node and application stack.....	6
Εικόνα 4: Δίκτυο κόμβων στο Blockchain .....	7
Εικόνα 5: Από τα μηνύματα της εφαρμογής στο TxS .....	7
Εικόνα 6: Συναλλαγές σε blocks.....	8
Εικόνα 7: Blockchain Networks Logos .....	11
Εικόνα 8: Έκδοση Certificate .....	15
Εικόνα 9:Blockcerts Certificate life cycle .....	16
Εικόνα 10: Qualichain Use Case diagram .....	17
Εικόνα 11: Διαδικασία πιστοποίησης στο blockchain .....	29
Εικόνα 12: Equal hashes blockchain verification.....	29
Εικόνα 13: MVC model.....	32
Εικόνα 14: How MVC works .....	33
Εικόνα 15: Application code diagram .....	34
Εικόνα 16: Database Entity-Relations diagram .....	35
Εικόνα 17: Register(matching passwords) .....	36
Εικόνα 18: Register (password does not match).....	36
Εικόνα 19: Successful Registration.....	36
Εικόνα 20: Fail to Register .....	37
Εικόνα 21: Login(user).....	37
Εικόνα 22: Fail to Login.....	37
Εικόνα 23: User main page (Blockcerts).....	38
Εικόνα 24: User main page (Qualichain).....	38
Εικόνα 25: Verified Successful in Blockcerts.....	38
Εικόνα 26: Successful information message.....	38
Εικόνα 27: Verification Faillure.....	39
Εικόνα 28: verification Faillure (information message).....	39
Εικόνα 29:My Account (user).....	39
Εικόνα 30: Update User Credentials failure .....	40
Εικόνα 31: Successful Update User Credentials .....	40
Εικόνα 32: My Documents(user) .....	40
Εικόνα 33:Confirmation message for deleting document.....	41
Εικόνα 34:Confirmation message for clear all history .....	41
Εικόνα 35: Contact tab .....	41
Εικόνα 36: Logout message.....	42
Εικόνα 37: Error page.....	42
Εικόνα 38: Fail to send email for restting password .....	43
Εικόνα 39: Message sent for resetting password .....	43
Εικόνα 40: Reset Password email .....	43
Εικόνα 41: Reset passwords(matching).....	43
Εικόνα 42: Reset passwords(not matching).....	43
Εικόνα 43: Password reset successfully .....	44
Εικόνα 44: Invalid URL token message .....	44
Εικόνα 45: About tab.....	44
Εικόνα 46: Login (root user).....	45
Εικόνα 47: Main page (root user).....	45

Εικόνα 48: All Users page (root) .....	45
Εικόνα 49: Update Users Credentials (root) .....	46
Εικόνα 50: Update User (wrong credentials).....	46
Εικόνα 51: User Successfully updated(root).....	46
Εικόνα 52: Failed to update user credentials(root).....	46
Εικόνα 53: Confirmation message for deleting user (root).....	47
Εικόνα 54: All users documents (root).....	47
Εικόνα 55: My Account mobile (user Azure).....	48
Εικόνα 56: Mobile friendly menu (user Azure) .....	48
Εικόνα 57: Mobile friendly main page (root local).....	48
Εικόνα 58: Mobile friendly menu (root local) .....	48
Εικόνα 59: SaaS, PaaS, IaaS .....	55
Εικόνα 60: Comparison between models .....	57
Εικόνα 61: Public, Private, Hybrid Cloud .....	59
Εικόνα 62: Azure Cost Policies .....	63
Εικόνα 63: Azure Sign In with University Account.....	64
Εικόνα 64: Azure Student Account.....	65
Εικόνα 65: Azure Portal main Page .....	65
Εικόνα 66: Resource Groups .....	66
Εικόνα 67: Create a Resource Group .....	66
Εικόνα 68: Azure marketplace.....	67
Εικόνα 69: Azure Database for MySQL.....	67
Εικόνα 70: Create MySQL server .....	68
Εικόνα 71: MySQL deployment options .....	68
Εικόνα 72: MySQL server preview.....	69
Εικόνα 73: MySQL pricing tier .....	69
Εικόνα 74: mysqlcertified database created.....	70
Εικόνα 75: Configure database security (firewall).....	70
Εικόνα 76: Connect through MySQL Workbench to Azure Database .....	71
Εικόνα 77: Create new scheme in Azure database .....	71
Εικόνα 78: WebApp in Azure marketplace .....	72
Εικόνα 79: Create a WebApp form .....	73
Εικόνα 80: Configure WebApp characteristics.....	73
Εικόνα 81: WebApp deployment complete .....	74
Εικόνα 82: Create WebApp preview .....	74
Εικόνα 83: Azure WebApp main page.....	74
Εικόνα 84: Configure database security (add WebApp ip).....	75
Εικόνα 85: Azure toolkit for IntelliJ.....	76
Εικόνα 86: Add Azure Subscriptios(IntelliJ).....	76
Εικόνα 87 IntelliJ select subscription.....	76
Εικόνα 88: Reload Maven Projects .....	77
Εικόνα 89: Deploy to Azure WebApps .....	77
Εικόνα 90: WebApp service (IntelliJ).....	78
Εικόνα 91: Successful WebApp Deployment.....	78
Εικόνα 92: WebApp on cloud (mobile version).....	79
Εικόνα 93: WebApp on cloud (pc version).....	79





# 1.Εισαγωγή

## 1.1 Ορισμός Προβλήματος

Η αναζήτηση εργασίας είναι κάτι που απασχολεί τον κάθε άνθρωπο στον πλανήτη προκειμένου να μπορέσει να βιοποριστεί. Η συνήθεις διαδικασίες που ακολουθούνται σήμερα για την πρόσληψη υπαλλήλων περιλαμβάνουν και την αποστολή εγγράφων από τους υποψήφιους εργαζομένους για να δικαιολογήσουν και να επισημάνουν όλα τα προσόντα και τις γνώσεις που απέκτησαν κατά την διάρκεια των σπουδών τους, παλιότερων εργασιακών εμπειριών η ακόμα και σεμιναρίων η δράσεις οργανισμών στις οποίες έλαβαν μέρος. Ποιος μπορεί να εγγυηθεί όμως ότι αυτά τα έγγραφα είναι γνήσια και επικυρωμένα από τους αρμόδιους φορείς και αντικατοπτρίζουν πλήρως το προφίλ του ενδιαφερόμενου;

Οι διαδικασίες πιστοποίησής των εγγράφων αυτών από τα αρμόδια ιδρύματα είναι πολύ χρονοβόρες αφού χρειάζεται πάντα η διαμεσολάβηση κάποιου μεσάζοντα που θα αναλάβει να επικυρώσει την γνησιότητα του κάθε εγγράφου από την αρχή ή ίδρυμα η οποία το έκδωσε. Πιο συγκεκριμένα στον ελληνικό δημόσιο τομέα, έχει ανακοινωθεί ότι, η επαλήθευση της γνησιότητας και της εγκυρότητας ενός πιστοποιητικού, που εκδίδεται από ελληνικό ΑΕΙ, μπορεί να πάρει πέντε έως τριάντα ημέρες, ανάλογα με την ανταπόκριση του ΑΕΙ. Στην περίπτωση των πιστοποιητικών που εκδίδονται από μη ελληνικά ΑΕΙ ,όπου μερικές φορές είναι απαραίτητη η παρέμβαση της πρεσβείας, η καθυστέρηση, σύμφωνα με πληροφορίες, έχει παραταθεί σε πέντε μήνες (αν και πρόσφατα μειώθηκε σε τρεις μήνες). Στην περίπτωση τίτλων ξένων γλωσσών (δηλαδή, που εκδίδονται από αντίστοιχα ινστιτούτα) ο εκτιμώμενος χρόνος επικύρωσης είναι είκοσι ημέρες και μπορεί να επιφέρει επιπλέον κόστος για τον υποψήφιο. Επιπλέον, όταν η επικύρωση αποτύχει για οποιονδήποτε λόγο, η ίδια η διαδικασία αντικατάστασης είναι επίσης χρονοβόρα και συνδέεται με άμεσο και έμμεσο κόστος .[1]

Αναμφισβήτητα λοιπόν οι τεχνικές και οι ήδη υπάρχουσες διαδικασίες για την επικύρωση της γνησιότητας εγγράφων είναι μη αποτελεσματικές και αποτελούν μη βιώσιμη λύση αφού απαιτούν χρόνο, κόστος και απασχολούν σημαντικό ποσοστό ανθρώπινου δυναμικού. Αν λάβουμε υπόψη ότι τα πιστοποιητικά αυτά έρχονται πάντα σε έντυπη μορφή τότε εισάγονται στην εξίσωση και άλλα εμπόδια όπως η εύαλωτη φύση τους σε φθορές, απώλειες ή ακόμα και καταδολιεύσεις, που κάνουν το έργο των recruiters και των υποψήφιων εργαζομένων ακόμα δυσκολότερο.

## 1.2 Το Blockchain ως λύση

Λύση σε αυτό το πρόβλημα έρχεται να δώσει μια τεχνολογία που ανακαλύφθηκε το 2008 για να εξυπηρετήσει κυρίως χρηματοοικονομικά ζητήματα αλλά και στο να χτίσει εμπιστοσύνη ανάμεσα στους συμμετέχοντες αυτών των συστημάτων. Η ευρέως διαδεδομένη ονομασία αυτού, τεχνολογία Blockchain. Πρώτες αναφορές τις έγιναν το 2008 με την δημοσίευση του paper με τίτλο «Bitcoin: A Peer-to-Peer Electronic Cash System» σε ένα περιοδικό από τον μέχρι σήμερα μυστήριο ιδρυτή του bitcoin Satoshi Nakamoto.[2]

Η τεχνολογία Blockchain επιτρέπει τη δημιουργία ενός αποκεντρωμένου περιβάλλοντος όπου οι συναλλαγές και τα δεδομένα δεν βρίσκονται υπό τον έλεγχο κανενός τρίτου οργανισμού. Κάθε συναλλαγή που έχει ολοκληρωθεί καταγράφεται σε ένα δημόσιο βιβλίο (distributed ledger) μόνιμα και με τρόπο που μπορεί να επικυρωθεί. Η λύση με την βοήθεια της τεχνολογίας του blockchain υπόσχεται να προσφέρει καλύτερη υποστήριξη για όλες αυτές τις διαδικασίες, διανέμοντας ακαδημαϊκά αρχεία μέσω μιας αποκεντρωμένης προσέγγισης. Αυτό σημαίνει ότι οι φοιτητές, τα ιδρύματα, οι κυβερνητικές

οντότητες και οι εργοδότες θα αποκτήσουν κυριαρχία στις ανακλήσεις , τους ελέγχους εγκυρότητας και την γρήγορη έκδοση εγγράφων και πιστοποιητικών.[3]

### ***1.3 Ανάπτυξη τεχνολογικά προηγμένης web εφαρμογής***

Στην παρούσα διπλωματική μελετώνται τεχνολογίες cloud computing και APIs που αξιοποιούν το blockchain για την αποθήκευση και την επικύρωση εγγράφων με απώτερο στόχο την δημιουργία μιας τεχνολογικά προηγμένης εφαρμογής που θα εκμεταλλεύεται τις τεχνολογίες αυτές για την πιστοποίησή τη γνησιότητας εγγράφων .Σημαντικό χαρακτηριστικό της έρευνας και της υλοποίησης αυτής της εφαρμογής είναι η χρήση και η εκμετάλλευση εργαλείων και πλατφόρμων που αποτελούν την αιχμή της τεχνολογίας πάνω στην ανάπτυξη εφαρμογών κάνοντας έτσι δυνατή την πιθανή επεκτασιμότητα της εφαρμογής μας για χρήση της από το ευρύ κοινό. Η εφαρμογή αναπτύσσεται με Java MVC αρχιτεκτονική πάνω στην πλατφόρμα spring boot με χρήση του Azure Portal για το deploy της στο «νέφος» και την υλοποίηση δύο blockchain based APIs καθώς και άλλων εργαλείων που θα αναφερθούν εκτενέστερα στα επόμενα κεφάλαια.

### ***1.4 Οργάνωση Κειμένου***

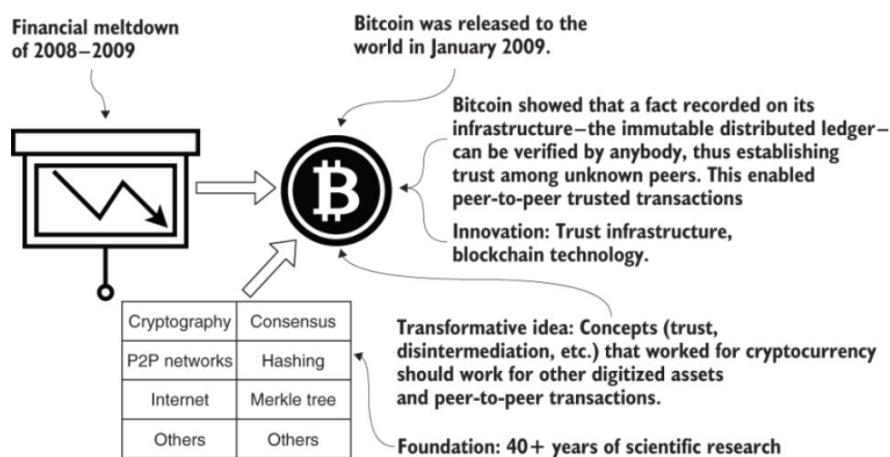
Η διπλωματική εργασία αποτελείται από επτά κεφάλαια. Στο Κεφάλαιο 1 ( Εισαγωγή) γίνεται αναφορά του προβλήματος και μια περιληπτική επεξήγηση στο θέμα που πραγματεύεται η διπλωματική. Στο Κεφάλαιο 2 (Blockchain και Πιστοποίηση) περιγράφεται ο όρος blockchain και πως γίνεται η πιστοποίηση με αυτό. Στο Κεφάλαιο 3 (Blockchain APIs για Πιστοποίηση Εγγράφων) παραθέτουμε την έρευνα που διεξάχθηκε γύρω από APIs που χρησιμοποιούν την τεχνολογία blockchain για αποθήκευση και επικύρωση της γνησιότητας εγγράφων καθώς και ποια APIs χρησιμοποιήσαμε εμείς στην υλοποίησή μας. Ακολουθώντας στο Κεφάλαιο 4 (Τεχνολογίες και Λειτουργίες της εφαρμογής) περιγράφουμε τις τεχνολογίες και τα εργαλεία που χρησιμοποιήθηκαν για την ανάπτυξη της εφαρμογής καθώς και τις λειτουργικότητες του web-app. Στο Κεφάλαιο 5 (Ανάπτυξη της Εφαρμογής) παρατίθενται τα βήματα ανάπτυξης της εφαρμογής μαζί με έναν οδηγό χρήσης που υποδεικνύει όλες τις λειτουργικότητες που αναφερθήκαν στο προηγούμενο κεφάλαιο. Στη συνέχεια στο Κεφάλαιο 6 (Cloud Computing και η εφαρμογή του AZURE ) γίνεται αναφορά στο cloud computing περιγράφοντας τον ορισμό και τα χαρακτηριστικά του και παρατίθεται ο τρόπος που χρησιμοποιήθηκε η πλατφόρμα Azure για την μετάβαση της εφαρμογής μας από την τοπική κατάσταση στο «νέφος». Τέλος στο Κεφάλαιο 7 (Σύνοψη και Συμπεράσματα) ανακεφαλαιώνουμε με τα τελικά μας συμπεράσματα από το μοντέλο που υλοποιήσαμε και παρουσιάζουμε τον τρόπο με τον οποίο θα μπορούσε να κατευθυνθεί η μελλοντική έρευνα μέσω της συγκεκριμένης διπλωματικής.

## 2. Blockchain και Πιστοποίηση

### 2.1 Η αρχή του Blockchain

Στα τέλη του 2008 και στις αρχές του 2009, τα συγκεντρωτικά συστήματα των χρηματοπιστωτικών αγορών του κόσμου, ενεργοποιημένα από μεγάλους μεσάζοντες όπως τράπεζες και εταιρείες επενδύσεων, απέτυχαν και άρχισαν να καταρρέουν. Η εμπιστοσύνη σε αυτά τα συστήματα διαβρώθηκε και ο πανικός επικράτησε σε όλο τον κόσμο με την κατάρρευση των χρηματοπιστωτικών αγορών. Σε αυτή τη συγκυρία, ένα μυστηριώδες πρόσωπο ή πρόσωπα παρουσίασαν στον κόσμο ένα μοντέλο εργασίας ενός αποκεντρωμένου συστήματος ψηφιακών νομισμάτων από ομότιμους χρήστες (χωρίς κεντρική αρχή ή διοίκηση), που ονομάζεται Bitcoin. Η διαμεσολάβηση εμπιστοσύνης σε αυτό το σύστημα πραγματοποιήθηκε μέσω λογισμικού που αργότερα θα ονομαστεί blockchain. Το Blockchain παρέχει τα βασικά στοιχεία επαλήθευσης, επικύρωσης, καταγραφής και ακεραιότητας για μεταφορές νομισμάτων.[2][4]

Παρόλο που το Bitcoin φάνηκε να ξεκίνησε ξαφνικά το 2009, η ιδέα ενός λειτουργικού ψηφιακού νομίσματος ήταν μια αναζήτηση από την αυγή του υπολογισμού. Πιο συγκεκριμένα η τεχνολογία Blockchain παρουσιάστηκε για πρώτη φορά το 1991 από τους Stuart Haber και W. Scott Stornetta, δύο ερευνητές που ήθελαν να εφαρμόσουν ένα σύστημα όπου οι χρονικές σφραγίδες εγγράφων δεν θα μπορούσαν να παραβιαστούν, και έγινε ευρέως γνωστή με την πρώτη ουσιαστική εφαρμογή της στο Bitcoin. Η τεχνολογία blockchain του Bitcoin βασίζεται σε μια ισχυρή βάση περισσότερων από 40 ετών επιστημονικής έρευνας στην κρυπτογραφία, το hashing, τα δίκτυα peer-to-peer και τα πρωτόκολλα συναίνεσης. Το Σχήμα 1 παρέχει μια σύντομη ιστορία του blockchain, της καινοτομίας και της ισχυρής επιστημονικής του βάσης, καθώς και της επίδραση του στα σύγχρονα δικτυωμένα συστήματα



Εικόνα 1: Ιστορία του Blockchain

### 2.2 Η εξέλιξη του Blockchain από ένα κρυπτονόμισμα

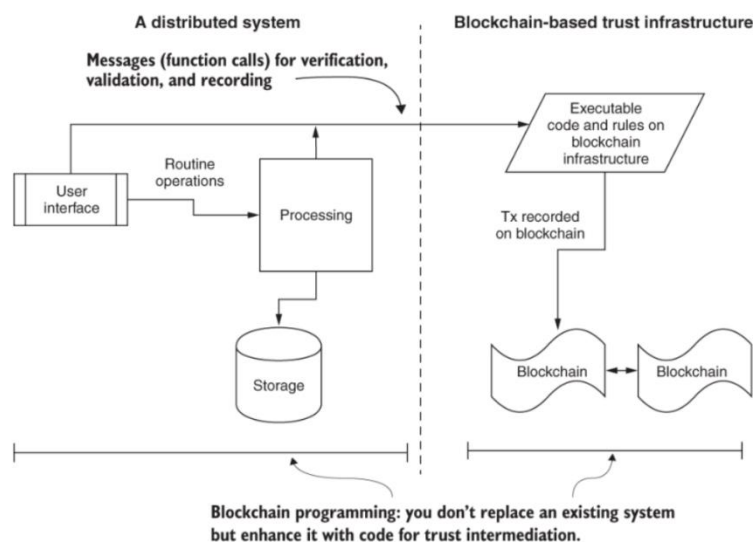
Ο αρχικός ενθουσιασμός για την τεχνολογία blockchain αφορούσε τη δυνατότητα μεταφοράς ψηφιακών νομισμάτων από ένα άτομο σε οποιονδήποτε στον κόσμο, διασχίζοντας τα όρια που δημιουργήθηκαν από τον άνθρωπο (όπως τα σύνορα χωρών) χωρίς μεσάζοντες όπως οι τράπεζες. Αυτός ο ενθουσιασμός αυξήθηκε περαιτέρω από τη συνειδητοποίηση ότι αυτή η δυνατότητα peer-to-

peer(ομοτίμων) θα μπορούσε να εφαρμοστεί σε άλλους τύπους συναλλαγών εκτός τις νομισματικές. Αυτές οι συναλλαγές περιλαμβάνουν περιουσιακά στοιχεία, όπως τίτλοι, έργα, μουσική και τέχνη, μυστικοί κωδικοί, συμβάσεις μεταξύ επιχειρήσεων, αποφάσεις αυτόνομων οδηγών και τεχνουργήματα που προκύπτουν από πολλές καθημερινές ανθρώπινες προσπάθειες.[2] Μια συναλλαγή μπορεί να περιέχει πολλές άλλες λεπτομέρειες βασισμένες στο πρωτόκολλο blockchain και την εφαρμογή του.

Το Bitcoin λειτουργεί συνεχώς από την έναρξή του. Τη στιγμή που γράφεται αυτό, σύμφωνα με τα Blockchain Charts (<https://www.blockchain.com/en/charts>), πραγματοποιεί περισσότερες από 250.000 συναλλαγές την ημέρα. Μετά την αρχική του επιτυχία, οι άνθρωποι άρχισαν να ρωτούν: "Εάν μπορεί να πραγματοποιήσει συναλλαγές ψηφιακού νομίσματος, γιατί όχι και άλλα ψηφιακά περιουσιακά στοιχεία;" Αυτή η ερώτηση απαντήθηκε γύρω στο 2013 με την προσθήκη ενός περιβάλλοντος για εκτέλεση κώδικα σε ένα άλλο δημοφιλές blockchain, το Ethereum (<https://ethereum.org>).[4] Η καινοτομία ήταν ότι η επαλήθευση, η επικύρωση και η καταγραφή θα μπορούσαν να επεκταθούν σε άλλα ψηφιακά περιουσιακά στοιχεία και σε συναφείς συναλλαγές και συστήματα. Επομένως, το blockchain μπορεί να διαδραματίσει καθοριστικό ρόλο στην εφαρμογή αποκεντρωμένων συστημάτων, παρέχοντας διαμεσολάβηση βάσει λογισμικού σε άλλες (μη νομισματικές) συναλλαγές των χρηστών.

### 2.3 Θεμελιώδεις έννοιες του Blockchain

Το blockchain είναι μια τεχνολογία που επιτρέπει την εμπιστοσύνη σε ένα αποκεντρωμένο σύστημα συναλλαγών στους χρήστες του. Ο σκοπός ενός blockchain είναι να επαληθεύσει και να επικυρώσει ή να απορρίψει μια συναλλαγή που ξεκίνησε ένας συμμετέχων, και στη συνέχεια να εκτελέσει τη συναλλαγή και να καταγράψει την απόδειξη αυτών των ενεργειών με τη συναίνεση των υπόλοιπων συμμετεχόντων-χρηστών. Όπως φαίνεται στο σχήμα 2, η υποδομή εμπιστοσύνης που βασίζεται στο blockchain υπάρχει σε ένα μεγαλύτερο σύστημα. Η υποδομή Blockchain περιέχει λογισμικό για συγκεκριμένο σκοπό: διαμεσολάβηση εμπιστοσύνης μεταξύ μεγάλου αριθμού (τυπικά άγνωστων) ομοτίμων συμμετεχόντων. Στην αριστερή πλευρά του σχήματος 2 είναι ένα καταναμημένο σύστημα (πελάτης/διακομιστής) που εκτελεί τις συνήθεις λειτουργίες. Αυτό το σύστημα μπορεί να στείλει μηνύματα που περιέχουν δεδομένα προς επαλήθευση, επικύρωση και εγγραφή στο blockchain (στα δεξιά) για να εδραιωθεί η εμπιστοσύνη σε αυτό το μεγαλύτερο σύστημα. Άξιο αναφοράς είναι το γεγονός ότι στον προγραμματισμό blockchain, δεν αντικαθίσταται ένα υπάρχον σύστημα, αλλά βελτιώνεται με κώδικα για την ενίσχυση της εμπιστοσύνης μέσω επικύρωσης και επαλήθευσης.[4][5]



Εικόνα 2: Blockchain Programming Context

Παρακάτω θα αναφέρουμε κάποιες χαρακτηριστικές έννοιες που συνδέονται με το blockchain:[6]

- Συναλλαγή (transaction): Είναι η μικρότερη αυτοτελής μονάδα πληροφορίας που ανταλλάσσεται σε ένα σύστημα Blockchain. Μια συναλλαγή που καταγράφεται σε ένα blockchain περιέχει ένα μήνυμα peer-to-peer που καθορίζει τις λειτουργίες που εκτελούνται, τις παραμέτρους δεδομένων που χρησιμοποιούνται για την εκτέλεση των λειτουργιών, τον αποστολέα και τον παραλήπτη του μηνύματος, το τέλος συναλλαγής και τη χρονική σήμανση της εγγραφής του.
- Κόμβος (node) : Το Node είναι η ονομασία που περιγράφει το λογισμικό του blockchain ,όπως και τα μηχανήματα ή το υλικό στα οποία είναι εγκατεστημένο για τους συμμετέχοντες σε ένα αποκεντρωμένο σύστημα. Το δίκτυο είναι peer-to-peer, επομένως κάθε κόμβος συμμετέχει ισότιμα διατηρώντας ένα πλήρες ή μερικό αντίγραφο του ledger και εφαρμόζοντας την πολιτική συναίνεσης του συστήματος.
- Ledger: Η καταγραφή των συναλλαγών, που διατηρείται κατανεμημένα με αντίγραφα σε κάθε κόμβο. Οι συναλλαγές του ledger είναι οριστικές και αναλλοίωτες. Ο στόχος του συστήματος Blockchain είναι να διασφαλίσει μέσω πρωτοκόλλου ότι τα ledger που διατηρούνται σε κάθε κόμβο είναι πανομοιότυπα, ώστε να αντικατοπτρίζουν την ίδια κατάσταση
- Account: Ένας λογαριασμός αντιπροσωπεύει μια μοναδική ταυτότητα για μια οντότητα συναλλαγής. Για την διεκπεραίωση μιας συναλλαγής απαιτείται ο λογαριασμός
- Συναίνεση (consensus): Ονομάζεται ο αλγόριθμος με τον οποίο οι κόμβοι ενός συστήματος Blockchain συμφωνούν ότι μία συναλλαγή είναι έγκυρη και καταλήγουν σε μία κοινή κατάσταση του ledger με το ίδιο σύνολο συναλλαγών και την ίδια ταξινόμησή τους.
- Dapps: Τα Dapps είναι διαδικτυακές ή εταιρικές εφαρμογές που περιλαμβάνουν λογική εφαρμογών για την επίκληση λειτουργιών blockchain που υλοποιούνται για την μεσολάβηση εμπιστοσύνης.
- Smart contract: Ένα έξυπνο συμβόλαιο είναι ένας αμετάβλητος εκτελέσιμος κώδικας που αντιπροσωπεύει τη λογική ενός Dapp. Οι μεταβλητές δεδομένων και οι λειτουργίες που ορίζονται σε ένα έξυπνο συμβόλαιο αντιπροσωπεύουν συλλογικά την κατάσταση και τις λειτουργίες για την επιβολή των κανόνων μιας εφαρμογής (Dapp) για επαλήθευση, επικύρωση και εγγραφή στο blockchain. Ουσιαστικά είναι οποιοδήποτε πρόγραμμα μπορεί να καταχωρηθεί σε ένα σύστημα Blockchain, να εκτελεστεί από τους κόμβους και να καταγράψει τα αποτελέσματά του στο ledger. Ο κώδικάς του παραμένει αναλλοίωτος.

## ***2.4 Πως λειτουργεί το Blockchain***

### ***2.4.1 Αποκεντρωμένο σύστημα***

Τι είναι ένα αποκεντρωμένο σύστημα; Ένα αποκεντρωμένο σύστημα είναι ένας τύπος κατανεμημένου συστήματος στο οποίο:

- Οι συμμετέχοντες επικοινωνούν μεταξύ τους ισότιμα (peer to peer).
- Οι συμμετέχοντες έχουν τον έλεγχο των περιουσιακών τους στοιχείων, ψηφιακών ή άλλων.

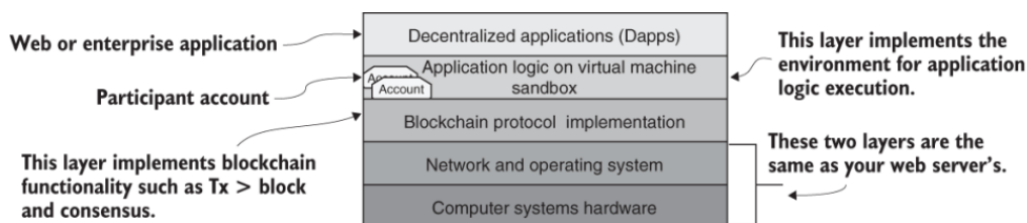
- Οι συμμετέχοντες μπορούν να συμμετάσχουν και να εγκαταλείψουν το σύστημα, όποτε το επιθυμούν.
- Οι συμμετέχοντες λειτουργούν πέρα από τα τυπικά όρια εμπιστοσύνης.
- Οι αποφάσεις λαμβάνονται από τους συμμετέχοντες και όχι από οποιαδήποτε κεντρική αρχή.
- Η διαμεσολάβηση μεταξύ συμμετεχόντων επιτυγχάνεται με τη χρήση αυτοματοποιημένου λογισμικού, όπως ένα blockchain.[5]

### 2.4.2 Nodes

Παίρνουμε ως παράδειγμα την εναέρια κυκλοφορία όπου πτήσεις έχουν προέλευση και προορισμούς, ενώ τα ενδιάμεσα αεροδρόμια και τα σημεία αναφοράς αποτελούν τα δίκτυα των αεροπορικών εταιρειών. Ομοίως, οι κόμβοι blockchain, φιλοξενούν το υπολογιστικό περιβάλλον που χρησιμεύει ως καταληκτικά σημεία συναλλαγών και εκτελεί επίσης άλλες λειτουργίες, όπως συναλλαγές αναμετάδοσης και μετάδοσης.

Το σχήμα 3 δείχνει τη λογική αρχιτεκτονική ενός μεμονωμένου κόμβου blockchain. Ένας κόμβος μπορεί να υποστηρίξει πολλούς λογαριασμούς για να αντιπροσωπεύει τις ταυτότητες των ομότιμων συμμετεχόντων στο αποκεντρωμένο δίκτυο. Ένας κόμβος blockchain φιλοξενεί τα στοιχεία που αντιπροσωπεύονται από τη στοιβή στο σχήμα 3. Χρησιμεύει ως βάση για την ανάπτυξη εφαρμογών blockchain.

Ας ξεκινήσουμε από κάτω και προχωράμε προς τα πάνω. Τα δύο χαμηλότερα επίπεδα είναι το τυπικό υλικό και λογισμικό των περισσότερων υπολογιστικών συστημάτων. Το επόμενο επίπεδο είναι το επίπεδο πρωτοκόλλου blockchain, το οποίο φιλοξενεί τα στοιχεία του blockchain. Το αμέσως μετά επίπεδο φιλοξενεί τη λογική της εφαρμογής. Σ' αυτό το επίπεδο επιλύονται προβλήματα, όπως έλεγχος πρόσβασης σε δεδομένα και λειτουργίες κώδικα για επικύρωση, επαλήθευση και εγγραφή. Το επάνω επίπεδο είναι η διεπαφή που βλέπει ο χρήστης, όπου γίνεται προγραμματισμός ιστού με HTML, JavaScript και άλλα συναφή εργαλεία και γλώσσες προγραμματισμού. Αυτά τα στοιχεία αποτελούν το επίπεδο Dapp και τη διεπαφή χρήστη (UI).



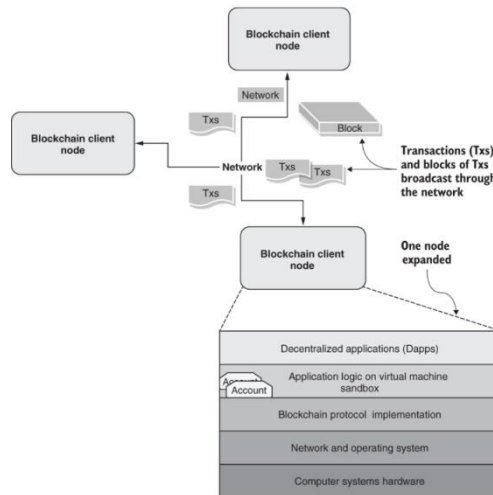
Εικόνα 3: Blockchain node and application stack

### 2.4.3 Applications and Network

Μια εφαρμογή blockchain δεν είναι μια εφαρμογή ενός χρήστη, σε αντίθεση με ένα φορητό παιχνίδι ή κάποιο άλλο λογισμικό. Συνήθως συνδέει μεγάλο αριθμό συμμετεχόντων μέσω του δικτύου κόμβων του. Κάθε κόμβος μπορεί να φιλοξενήσει πολλούς λογαριασμούς για να προσδιορίσει τους διαφορετικούς πελάτες που εξυπηρετεί. Ένας κόμβος μπορεί επίσης να φιλοξενήσει περισσότερους από έναν Dapp, όπως έναν για αποκεντρωμένο σύστημα διαχείρισης της αλυσίδας εφοδιασμού και έναν άλλο για ένα αποκεντρωμένο σύστημα πληρωμών. Το σχήμα 4 δείχνει ένα δίκτυο τριών κόμβων που συνδέονται με ένα δίκτυο. Το δίκτυο διευκολύνει τη μετάδοση των συναλλαγών που ξεκινούν από μπλοκ χρηστών που σχηματίζονται από τις συναλλαγές.

Αυτές οι συναλλαγές και τα μπλοκ αποτελούν το ωφέλιμο φορτίο του δικτύου και, τελικά, μετά από επαλήθευση και επικύρωση, καταγράφονται στο ledger.[4]

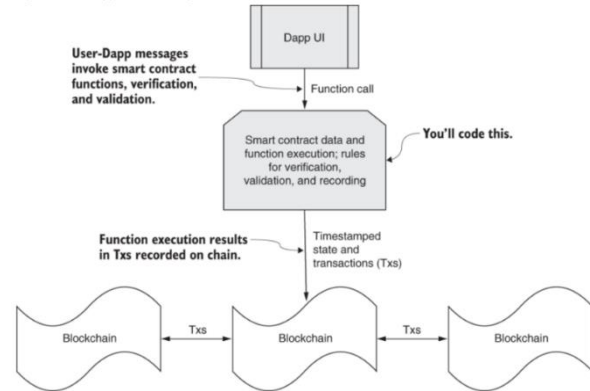
Ένα αναγνωριστικό δικτύου προσδιορίζει ένα δίκτυο κόμβων blockchain. Το αναγνωριστικό δικτύου #1, για παράδειγμα, είναι το κύριο δημόσιο δίκτυο Ethereum. Το αναγνωριστικό δικτύου #4 είναι ένα δημόσιο δίκτυο που ονομάζεται Rinkeby (<https://www.rinkeby.io>) και ούτω καθεξής. Θα πρέπει να υποδειχθεί το δίκτυο, χρησιμοποιώντας το αναγνωριστικό του, κατά την ανάπτυξη μιας έξυπνης σύμβασης στο δίκτυο. Οι συμμετέχοντες σε ένα δεδομένο δίκτυο θα μοιραστούν ένα ενοποιημένο ledger για την καταγραφή των στοιχείων της συναλλαγής τους.



Εικόνα 4: Δίκτυο κόμβων στο Blockchain

#### 2.4.4 Smart Contracts

Τα έξυπνα συμβόλαια αναπτύσσονται σε περιβάλλον sandbox, όπως μια εικονική μηχανή (VM) που φιλοξενείται από έναν κόμβο blockchain.[8] Η σύνταξη ενός έξυπνου συμβολαίου είναι παρόμοια με μια κλάση σε μια γλώσσα ΟΟ (αντικειμενοστραφής). Περιέχει δεδομένα, συναρτήσεις και κανόνες για την εκτέλεση συναρτήσεων. Η κλήση ή η επίκληση μιας λειτουργίας έξυπνης σύμβασης δημιουργεί τις συναλλαγές που καταγράφονται στο blockchain, όπως φαίνεται στο σχήμα 5. Εάν κάποιος από τους κανόνες επαλήθευσης και επικύρωσης αποτύχει, η κλήση της λειτουργίας επιστρέφει. Εάν όμως η εκτέλεση είναι επιτυχής, οι δημιουργούμενες συναλλαγές (Tx) μεταδίδονται στο δίκτυο για εγγραφή, όπως φαίνεται στο σχήμα 5.



Εικόνα 5: Από τα μηνύματα της εφαρμογής στο Tx

#### 2.4.5 Distributed ledger technology

Η τεχνολογία που βασίζεται και υποστηρίζει την υποδομή του blockchain, που αναφέραμε πιο πάνω, (nodes,application,networks, smart contracts) ονομάζεται Distributed ledger technology(DLT). Αποτελείται από τις συναλλαγές, τα blocks και την αλυσίδα.

Συναλλαγές(transactions):

Οι εφαρμογές ξεκινούν τις συναλλαγές και την εκτέλεση έξυπνου κώδικα συμβολαίου. Μια απλή μεταφορά κρυπτονομίσματος μεταξύ λογαριασμών, για παράδειγμα, δημιουργεί μια συναλλαγή "αποστολής". Οι συναλλαγές που δημιουργούνται μεταδίδονται μέσω του δικτύου blockchain και στη συνέχεια συγκεντρώνονται και καταγράφονται στο ledger.[7]

## Blocks και Αλυσίδα:

Ένα σύνολο συναλλαγών κάνει ένα μπλοκ και ένα σύνολο μπλοκ κάνει ένα blockchain, όπως φαίνεται στο σχήμα 6. Η διαδικασία έχει ως εξής:

-Οι συναλλαγές στο δίκτυο επαληθεύονται, συλλέγονται και συγκεντρώνονται. Οι κόμβοι επιλέγουν ένα σύνολο συναλλαγών από την ομάδα για να δημιουργήσουν ένα μπλοκ.

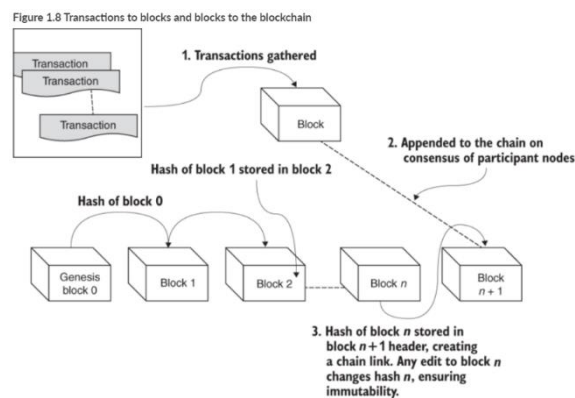
-Οι συμμετέχοντες κόμβοι χρησιμοποιούν έναν αλγόριθμο συναίνεσης για να συμφωνήσουν συλλογικά ή να καταλήξουν σε συναίνεση σε ένα ενιαίο συνεπές μπλοκ συναλλαγών που θα προσαρτηθεί στην υπάρχουσα αλυσίδα.

-Ένας κατακερματισμός (hash) ή μια αντιπροσωπευτική τιμή του τρέχοντος μπλοκ της αλυσίδας προστίθεται στο πρόσφατα προσαρτημένο μπλοκ, δημιουργώντας έναν κρίκο αλυσίδας.

Όπως δείχνει το σχήμα 6, η δημιουργία του blockchain ξεκινά με ένα μόνο μπλοκ που ονομάζεται μπλοκ γένεσης. Κάθε κόμβος ενός ενδιαφερόμενου μέρους στο blockchain έχει ένα πανομοιότυπο αντίγραφο του blockchain, ξεκινώντας από τον κόμβο γένεσης. Ένα blockchain DLT, επομένως, είναι:

- Distributed (μπορεί να διανεμηθεί): Επειδή το πρωτόκολλο blockchain διασφαλίζει ότι κάθε διανεμημένος κόμβος που εμπλέκεται έχει ένα πανομοιότυπο αντίγραφο της αλυσίδας των μπλοκ.
- Immutable (Αμετάβλητο): Επειδή κάθε νεοσύστατο μπλοκ συνδέεται με το υπάρχον blockchain με την τιμή κατακερματισμού της τρέχουσας κεφαλής του blockchain, όπως φαίνεται στο σχήμα 6.[4][5]

Σε αυτό το σημείο, αρκεί να γνωρίζουμε ότι μια αντιπροσωπευτική τιμή υπογραφής του μπλοκ  $n$  αποθηκεύεται στο μπλοκ  $n+1$ , για να διασφαλιστεί η μη μεταβλητότητα του blockchain. Οποιαδήποτε ακούσια ή σκόπιμη αλλαγή στα δεδομένα ενός μπλοκ σε έναν κόμβο θα αλλάξει την τιμή κατακερματισμού του μπλοκ και θα καταστήσει την αλυσίδα αυτού του κόμβου άκυρη.



Εικόνα 6: Συναλλαγές σε blocks

## 2.5 Τύποι Blockchain

### 2.5.1 Permissionless (χωρίς άδεια)

Τα Permissionless blockchains είναι blockchains που δεν απαιτούν άδεια για να συνδεθείτε και να αλληλοεπιδράσετε μέσα σε αυτά, αφού θεωρούνται συστήματα ανοικτού τύπου. Είναι επίσης γνωστά ως δημόσια blockchains. Τις περισσότερες φορές, το blockchain χωρίς άδεια είναι ιδανικό για τη λειτουργία και τη διαχείριση ψηφιακών νομισμάτων. Σε ένα blockchain χωρίς άδεια, ένας χρήστης μπορεί να δημιουργήσει μια προσωπική διεύθυνση και στη συνέχεια να αλληλοεπιδράσει με το δίκτυο είτε βοηθώντας το δίκτυο να επικυρώσει συναλλαγές είτε απλά να στείλει συναλλαγές σε άλλον χρήστη στο δίκτυο. Η διακυβέρνηση τέτοιων συστημάτων στηρίζεται στην ύπαρξη ενός κοινού νομίσματος που μέσω κρυπτοοικονομικών μηχανισμών και οικονομικών κινήτρων δημιουργείται, ανταλλάσσεται



και χρησιμοποιείται για να ενθαρρύνει μία ομάδα ατόμων χωρίς εμπιστοσύνη μεταξύ τους να συμμετέχουν σε ένα δίκτυο Blockchain και να διατηρήσουν ένα κοινό ledger, χωρίς την ανάγκη ύπαρξης κεντρικών αρχών.[7][10]

Ο πρώτος τύπος blockchain χωρίς άδεια είναι το Bitcoin. Έδωσε τη δυνατότητα στους χρήστες να μεταφέρουν ψηφιακά νομίσματα μεταξύ τους. Επίσης, οι χρήστες μπορούν να αλληλεπιδράσουν με το δίκτυο συμμετέχοντας στη διαδικασία εξόρυξης. Είναι μια διαδικασία επίλυσης σύνθετων μαθηματικών εξισώσεων και στη συνέχεια χρήσης της για την επικύρωση συναλλαγών. Ο αλγόριθμος συναίνεσης που χρησιμοποιείται από το bitcoin είναι το Proof-of-Work (PoW). Υπάρχουν επίσης και άλλα blockchains που είναι χωρίς άδεια. Το Ethereum (ETH) είναι ένας άλλος δημοφιλής δημόσιος τύπος χωρίς άδεια που χρησιμοποιεί προσπαθεί να μεταβεί σε μια άλλη μέθοδο συναίνεσης την Proof-of-Stake (PoS). [61]

Χαρακτηριστικά των Permissionless blockchain[5][7][9]

- Πραγματικά αποκεντρωμένα
- Ανωνυμία : Το Permissionless blockchain είναι ανοιχτό σε όλους. Ωστόσο, αυτό δεν σημαίνει ότι δεν είναι ανώνυμο. Όποιος συμμετέχει στο δίκτυο μπορεί να παραμείνει ανώνυμος καθώς δεν θα χρειαστεί ένα KYC(know your consumer) για να συνδεθεί και να προηγηθεί στο δίκτυο.
- Διαφάνεια :Οι δημόσιοι κόμβοι μπορούν να δουν τις συναλλαγές, καθιστώντας το δίκτυο διαφανές.
- Εμπιστοσύνη : Μπορείτε να εντοπίσετε ή να διαβάσετε τις συναλλαγές. Έτσι, μπορείτε να εμπιστευτείτε αυτά τα blockchains χωρίς άδεια(Permissionless blockchain) περισσότερο από ένα κλειστό ή εξουσιοδοτημένο blockchain (Permissioned blockchain).
- Αμετάβλητο : Κάθε μεμονωμένο στοιχείο στην πλατφόρμα είναι αμετάβλητο, πράγμα που σημαίνει ότι δεν μπορεί κάποιος να αλλάξει κάτι που καταχωρήθηκε στην αλυσίδα.
- Ενισχυμένη ασφάλεια : Η κρυπτογραφία και άλλες παράμετροι ασφάλειας καθιστούν τα Permissionless blockchain ασφαλή.[8]

### 2.5.2 Permissioned(με άδεια)

Τα permissioned blockchains είναι εντελώς αντίθετα από τα permissionless. Ένας τρόπος να αποδώσουμε την ετυμολογία τους είναι να τα φανταστούμε ως ιδιωτικά blockchains. Η μεγαλύτερη διαφορά τους με τα permissionless blockchain είναι ότι δεν μπορούν να είναι όλοι συμμετέχοντες στο permissioned blockchain, αφού απαιτείται ειδική άδεια από τον διαχειριστή του δικτύου ή τον κάτοχο για να υπάρξει πρόσβαση στο δίκτυο. Γιατί όμως χρειάζεται ένα τέτοιο blockchain; Ο μοναδικός σκοπός δημιουργίας του είναι για δημιουργηθεί ένα δίκτυο blockchain που θα είναι αποκομμένο από το κοινό. Δεν χρειάζεται όλα τα blockchains να είναι δημόσια και οι οργανισμοί απλά δεν έχουν την πολυτέλεια να δημοσιοποιούν τις διαδικασίες ή τα δεδομένα τους. Αυτό είναι όπου το blockchain με άδεια είναι πολύ χρήσιμο ακόμη και όταν μετακινείται ελαφρώς από το βασικό χαρακτηριστικό του blockchain, δηλαδή την αποκέντρωση[7][9]. Παραδείγματα οργανισμών που θα μπορούσαν να χρησιμοποιήσουν αυτού του είδους blockchain είναι οι τράπεζες οι εταιρείες ή και άλλα ιδρύματα ή οργανισμοί που θέλουν να προστατεύσουν τα δεδομένα τους.[10]

Στα permissioned blockchain δίκτυα η ταυτότητα του κάθε κόμβου είναι γνωστή, έτσι προστατεύονται απο τυχόν μαζικές επιθέσεις οι οποίες στοχεύουν στον να επηρεάσουν το δίκτυο με την δημιουργία πολλαπλών ψευδή λογαριασμών. Ο κάθε κόμβος έχει απαρτίζεται από μια συγκεκριμένη ταυτότητα και δικαιώματα, πράγμα που αυξάνει τον βαθμό εμπιστοσύνης που προσφέρει το Blockchain. Με αυτόν τον τρόπο, τα permissioned συστήματα μπορούν να επιτύχουν μεγαλύτερη αποδοτικότητα καθώς και ιδιωτικότητα των δεδομένων τους, αφού αυτά είναι προσβάσιμα μόνο εντός του δικτύου και από γνωστούς κόμβους. Αυτά τα δίκτυα επιτρέπουν την ευκολότερη παραμετροποίηση τους για την κάλυψη των αναγκών των συμμετεχόντων (πχ επιλογή αλγόριθμου συναίνεσης) λόγω του ότι είναι κλειστά.[9]

Χαρακτηριστικά των Permissioned blockchains:[7][9]

- **Ενναλακτική αποκέντρωση:**

Αν νομίζατε ότι η αποκέντρωση μπορεί να γίνει μόνο με έναν τρόπο, τότε κάνετε λάθος. Μπορείτε να επιτύχετε αποκέντρωση μέσω πολλών και διαφόρων τρόπων, όπως η διατήρηση του ενδιαφέροντος του ιδιοκτήτη, αλλά η εξασφάλιση μερικών βασικών χαρακτηριστικών που ταιριάζουν με την τεχνολογία blockchain. Μπορούμε να τα σκεφτούμε ως επίπεδα αποκέντρωσης. Στην περίπτωση ενός δημόσιου δικτύου, έχουμε πλήρη αποκέντρωση καθώς ταιριάζει με τη φιλοσοφία του ίδιου του δικτύου. Τώρα, κάθε οντότητα δεν μπορεί να κάνει πλήρη αποκέντρωση για αυτό πρέπει να προσαρμοστεί σε μια ελαφρύτερη έκδοση αποκέντρωσης, όπου μια κεντρική αρχή εγκρίνει ποιος συμμετέχει και ποιος όχι. Η αποκέντρωση που χρησιμοποιείται από permissioned blockchains είναι επίσης πιο ευέλικτη, καθώς τα ιδιωτικά δίκτυα είναι ελεύθερα να χρησιμοποιούν αλγόριθμους συναίνεσης της επιλογής τους.

- **Διακυβέρνηση εκ των έσω:**

Τα permissioned δίκτυα διαχειρίζονται από τον εκάστοτε οργανισμό έτσι, οι οργανισμοί ορίζουν μέλη για το επιχειρηματικό δίκτυο και διασφαλίζουν ότι το μεγαλύτερο μέρος του δικτύου έχει αποκεντρωμένη φύση με κάποιο κεντρικό έλεγχο επίσης. Σε αυτά τα δίκτυα ο οργανισμός αποφασίζει αν θα συμπεριλάβει τον (τους) κόμβο (-ους) επικύρωσης για την επικύρωση συναλλαγών.

- **Προσαρμοστικότητα:**

Οι οργανισμοί μπορούν να προσαρμόσουν τα δίκτυα με βάση τις απαιτήσεις τους.

- **Αποτελεσματικότητα:**

Τα permissioned blockchains δίκτυα είναι αποτελεσματικά όταν πρόκειται για την ταχύτητα και την επεκτασιμότητα των συναλλαγών

- **Ανωνυμία και διαφάνεια:**

Τα ιδιωτικά blockchains είναι γνωστά για τη διαφάνεια. Μπορούν να επιλέξουν να είναι διαφανή διασφαλίζοντας ότι υπάρχει εμπιστοσύνη εντός του οργανισμού. Όσον αφορά το απόρρητο, κάθε μεμονωμένη ταυτότητα προστατεύεται, χρησιμοποιώντας κρυπτογραφία. Μόνο η κεντρική οντότητα γνωρίζει για το άτομο, καθώς πρέπει να κάνει ένα KYC(know your consumer-customer) όταν εντάσσεται στο δίκτυο.[9]

## 2.6 Πλατφόρμες Blockchain

### 2.6.1 Ethereum

Το Ethereum κατατάσσεται στα permissionless συστήματα Blockchain. Χαρακτηρίζεται από το περιβάλλον εκτέλεσής του, Ethereum Virtual Machine (EVM), όπου εκτελούνται τα smart contracts, γραμμένα στην Turing-complete γλώσσα προγραμματισμού Solidity, που δημιουργήθηκε για τις ανάγκες του Ethereum. Το Ethereum είναι μια πλατφόρμα που επιτρέπει σε οποιονδήποτε να δημιουργήσει και να χρησιμοποιήσει αποκεντρωμένες εφαρμογές, που βασίζονται σε έξυπνα συμβόλαια και λειτουργούν με τεχνολογία blockchain. Το Ethereum επικεντρώνεται στην ικανότητα αυτόματης διαχείρισης ψηφιακών περιουσιακών στοιχείων και, για να το κάνει αυτό, υποστηρίζει έξυπνες συμβάσεις ή ιδιότητες, καθιστώντας τη δημιουργία προγραμμάτων διαχείρισης περιουσιακών στοιχείων ευκολότερη από ό,τι όταν χρησιμοποιείτε τη γλώσσα δέσμης ενεργειών(script) στο Bitcoin Blockchain. Το Ethereum προσαρμόζει επίσης το πρωτόκολλο συναίνεσης PoW (Proof-of-work) και έχει επιτρέψει την υλοποίηση καινοτόμων ιδεών που αφορούν από αγορές τέχνης μέχρι χρηματοοικονομικές λύσεις (decentralized finance, DeFi) , π.χ. για δανεισμό , ή για δημιουργία αποκεντρωμένων εταιρειών (Decentralized Autonomous Organizations, DAOs)[11]

### 2.6.1 Bitcoin

Το Bitcoin, το πρώτο γνωστό και ευρέως διαδεδομένο κρυπτονόμισμα, λειτουργεί ένα δίκτυο peer-to-peer χωρίς κεντρική αρχή ή τράπεζες από πίσω να το στηρίζουν και εισήγαγε την τεχνολογία και την πλατφόρμα blockchain στον κόσμο. Η διαχείριση των συναλλαγών και η έκδοση νομισμάτων πραγματοποιούνται συλλογικά από το δίκτυο blockchain. Το Bitcoin χρησιμοποιεί το PoW (Proof-of-work) ως πρωτόκολλο συναίνεσης για την επαλήθευση των συναλλαγών και έτσι καταναλώνει πολλή ενέργεια. Λόγω της επιτυχίας του Bitcoin, πολλά άλλα εναλλακτικά κρυπτονομίσματα και πρωτόκολλα συναίνεσης προτάθηκαν και αναπτύχθηκαν.[2][11]

### 2.6.3 Ripple

Το Ripple είναι ένα δίκτυο blockchain χαμηλής καθυστέρησης που ρυθμίζει ατομικά και καταγράφει συναλλαγές σε μια ασφαλή κατανεμημένη βάση δεδομένων, το Ripple Consensus Ledger. Το Ripple εφαρμόζει το Ripple Consensus Protocol Algorithm, έναν εναλλακτικό αλγόριθμο στο υψηλής καθυστέρησης Bitcoin Blockchain PoW, για τον χειρισμό του «Βυζαντινού Προβλήματος» και του «Sybil Attack». Τα μπλοκ επικυρώνονται μόνο από τους σχετικά λίγους «Επιλεγμένους επικυρωτές» για να επιτρέψουν συναλλαγές χαμηλής καθυστέρησης. Ενώ επιτυγχάνεται συναίνεση, το τρέχον distributed ledger είναι "κλειστό" και θεωρείται το πιο πρόσφατο. Επίσης, τα νομίσματα Ripple είναι «προ-εξορυχθέντα» και δεν μπορούν να δημιουργηθούν κατά τη διαδικασία συναίνεσης. Και πάλι, αν σκεφτούμε ότι οι περισσότερες εφαρμογές υγειονομικής περίθαλψης θα χρησιμοποιούν δίκτυα με άδεια(permissioned networks), τα πλεονεκτήματα της χρήσης εναλλακτικών πρωτοκόλλων συναίνεσης μειώνονται.[11]



Εικόνα 7: Blockchain Networks Logos

## 2.7 Πιστοποίηση μέσω Blockchain

Το Blockchain είναι ένα δημόσιο εργαλείο που χρησιμοποιείται για την καταγραφή όλης της συναλλαγής σε ένα αποκεντρωμένο αρχείο καταγραφής δεδομένων και όχι σε ένα φυσικό μέσο ή μια ενιαία βάση δεδομένων. Ενώ η τεχνολογία blockchain χρησιμοποιήθηκε αρχικά για τη δημιουργία κρυπτονομισμάτων, στις μέρες μας το blockchain προωθείται σε διαφορετικούς τομείς, όπως συναλλαγές, αποθήκευση αρχείων, υπηρεσίες πληρωμών, διαχείριση ταυτότητας, οικονομικές ανταλλαγές, διαχείριση ιατρικών αρχείων, εκπαίδευση και άλλα.[12]

Δυστυχώς, στον σημερινό κόσμο, τα πλαστά έγγραφα αποτελούν «επιδημία» στην κοινωνία και όπως οι περισσότεροι από εσάς γνωρίζετε, είναι πολύ εύκολο η απόκτηση πλαστών εγγράφων. Καθώς τα πλαστά έγγραφα μοιάζουν ακριβώς με τα πρωτότυπα, είναι δύσκολο για έναν μη καταρτισμένο άνθρωπο να προσδιορίσει το πραγματικό και το ψεύτικο. Οι Πάροχοι υπηρεσιών πρέπει να δαπανήσουν εκατομμύρια για να επαληθεύσουν τα έγγραφα των υποψηφίων. Ωστόσο, το blockchain βρίσκει επίσης την εφαρμογή του στις διαδικασίες επαλήθευσης εγγράφων. Ένα ψηφιακό πιστοποιητικό υπό το φως της τεχνολογίας blockchain θα μπορούσε να αντιμετωπίσει το παραπάνω ζήτημα όπως εξηγούμε παρακάτω.[13][14]

1. Η επαλήθευση εγγράφων με την τεχνολογία blockchain εξαλείφει τον μεσάζοντα περιορίζοντας έτσι το κόστος συναλλαγής στο δίκτυο, αρά ουσιαστικά εξοικονομείται κόστος.
2. Τα πιστοποιητικά τοποθετούνται σε ένα distributed ledger, έτσι ώστε οι άνθρωποι να έχουν πρόσβαση σε πληροφορίες οποιαδήποτε στιγμή, οπουδήποτε. Στο blockchain, τα έγγραφα ανεβαίνουν με ασφάλεια, στα οποία μόνο εξουσιοδοτημένο άτομο μπορεί να έχει πρόσβαση χρησιμοποιώντας τα ιδιωτικά του κλειδιά.

3. Η τεχνολογία Blockchain αποθηκεύει δεδομένα σε μορφή που δεν μπορεί να τροποποιηθεί. Αυτό γίνεται μέσω της επιστήμης της κρυπτογραφίας που περιλαμβάνει κρυπτογράφηση δεδομένων χρησιμοποιώντας μια λειτουργία κατακερματισμού. Έτσι, τα δεδομένα γίνονται αμετάβλητα και είναι πρακτικά αδύνατο κάποιος επιτήδειος να τα κλέψει.
4. Δεν θα υπάρχει πλέον ζήτημα επεκτασιμότητας, καθώς ο χρόνος συναλλαγής που απαιτείται θα μπορούσε να είναι πολύ γρήγορος, της κλάσης των μερικών δευτερολέπτων. Με αυτόν τον τρόπο, τα έγγραφα που επαληθεύονται στο blockchain επιτρέπουν τη γρήγορη παράδοση της υπηρεσίας.

## ***3. Blockchain APIs για Πιστοποίηση Εγγράφων***

### ***3.1 Έρευνα για Blockchain Εφαρμογές Πιστοποίησης Εγγράφων***

Βάσει όσων ειπώθηκαν προηγουμένως, η πιστοποίηση εγγράφων με την χρήση του blockchain αποτελεί έναν αξιόπιστο και γρήγορο τρόπο πιστοποίησης εγγράφων, αφού είναι αδιάβλητος. Το κάθε στοιχείο στην αλυσίδα του blockchain είναι αμετάβλητο και δεν μπορεί να παρακάμψει κάποιος την αρχή η οποία εξέδωσε και επικύρωσε το κάθε έγγραφο. Γι' αυτό τον λόγο προσπαθήσαμε να βρούμε και να χρησιμοποιήσουμε ήδη υπάρχοντα APIs, τα οποία χρησιμοποιούνται από blockchain εφαρμογές, έτσι ώστε να τα ενσωματώσουμε στην εφαρμογή μας για την επίτευξη της πιστοποίησης εγγράφων. Αυτά τα APIs αποθηκεύουν, επικυρώνουν και πιστοποιούν έγγραφα, κάποια από αυτά είναι το BlockCerts, το Qualichain, το OpenCerts, το BtCerts κ.α.[15]

#### ***3.1.1 OpenCerts***

Το OpenCerts χρησιμοποιεί blockchain για να παρέχει έναν εύκολο και αξιόπιστο τρόπο έκδοσης και επικύρωσης πιστοποιητικών προστασίας από παραβίαση. Με την υποστήριξη του Ethereum, ενός δικτύου blockchain, γνωστού και ως DLT(distributed ledger technology), το OpenCerts αντιμετωπίζει το εμπόδιο της πιστοποίησης εγγράφων με την δημοσίευσης κρυπτογραφικά προστατευμένων εκπαιδευτικών διαπιστευτηρίων. Παρέχει μία ενιαία πλατφόρμα για όλα τα άτομα, από φοιτητές έως εργοδότες, για την επαλήθευση των πιστοποιητικών που έχουν εκδοθεί από οποιοδήποτε ίδρυμα. Σχεδιάστηκε για πρώτη φορά σε συνεργασία με το Ngee Ann Polytechnic (NP) τον Νοέμβριο του 2017 και τώρα υιοθετείται από εκπαιδευτικά ιδρύματα στο πλαίσιο του OpenCerts Consortium. Μέσω του OpenCerts, τα άτομα μπορούν να δουν τα πιστοποιητικά τους, να ελέγξουν ότι δεν έχουν παραποιηθεί.[16]

Το OpenCerts το διαχειρίζεται η SkillsFuture Singapore (SSG), είναι μέρος της πρωτοβουλίας Smart Nation της Σιγκαπούρης, και επιτρέπει την έκδοση και την επικύρωση ακαδημαϊκών πιστοποιητικών, ανθεκτικών σε παραβιάσεις με βολικό και αξιόπιστο τρόπο. Το OpenAttestation είναι ένα πρότυπο που βοηθά στη δημιουργία επαληθεύσιμων εγγράφων. Ακόμα το OpenCerts αποτελεί μια συγκεκριμένη εφαρμογή, η οποία χρησιμοποιεί το OpenAttestation, για να παρέχει στα ιδρύματα έναν τρόπο δημιουργίας επαληθεύσιμων πιστοποιητικών.[17]

Το OpenCerts χρησιμοποιείται για υπηρεσίες της κυβέρνησης της Σιγκαπούρης και έχει τα παρακάτω χαρακτηριστικά:

- Ένα σχήμα ανοιχτού κώδικα για τη δημοσίευση εκπαιδευτικών διαπιστευτηρίων.
- Ένα σύνολο εργαλείων για τη δημιουργία κρυπτογραφικών προστασιών για εκπαιδευτικά διαπιστευτήρια.
- Ο διαδικτυακός ιστότοπος OpenCerts για την επαλήθευση της γνησιότητας των αρχείων OpenCerts.

Με το OpenCerts έχουν να κερδίσουν τόσο οι μαθητές όσο και τα εκπαιδευτικά ιδρύματα. Τα εκπαιδευτικά ιδρύματα μπορούν να επωφεληθούν από την εξοικονόμηση κόστους και το μειωμένο χρονικό διάστημα για την επαλήθευση των εκδοθέντων πιστοποιητικών, ενώ οι μαθητές μπορούν εύκολα να αποκτήσουν τα πιστοποιητικά τους και να τα στείλουν σε μελλοντικούς εργοδότες, οι οποίοι στη συνέχεια μπορούν επίσης να χρησιμοποιήσουν την πλατφόρμα για να ελέγξουν την αυθεντικότητα του πιστοποιητικού.[18]

### **3.1.2 SmartDegrees**

Το SmartDegrees είναι μια πλατφόρμα για την εγγραφή, επικύρωση και πιστοποίηση διπλωμάτων και ακαδημαϊκών πιστοποιητικών, με συναφείς υπηρεσίες, που επιτρέπει την τοποθέτηση της αξίας τους στην αγορά εργασίας και στην κοινωνία, ενώ ταυτόχρονα τα καθιστά αμετάβλητα, διασφαλίζοντας την ισχύ τους επ' αόριστον.[19]

Χρησιμοποιεί distributed ledger technology (DLT) βασισμένη σε blockchain, η οποία ανοίγει τεράστιες δυνατότητες στους αποφοίτους, τα πανεπιστήμια, τις πλατφόρμες εργασίας και τους recruiters. Τα διπλώματα και τα πιστοποιητικά εξελίσσονται από το να αποτελούν ένα στατικό στοιχείο που υποστηρίζεται σε χαρτί ή ψηφιακά υπογεγραμμένο αρχείο και αποτελούν ασφαλή ψηφιακά στοιχεία. Ως εκ τούτου, ο απόφοιτος έχει τον αποκλειστικό έλεγχο στην διαχείριση των εγγράφων του.

Η σημερινή βιομηχανία τριτοβάθμιας εκπαίδευσης συγκαταλέγεται στους τομείς της ταχύτερα αναπτυσσόμενης εκπαίδευσης. Ωστόσο, οι πρόσφατες τεχνολογικές εξελίξεις όπως τα διαδικτυακά και τα εταιρικά πανεπιστήμια αντιπροσωπεύουν νέες προκλήσεις που συμβάλλουν στο να καταστούν τα παραδοσιακά πανεπιστήμια μη βιώσιμα. Τα ακαδημαϊκά πτυχία σε έντυπη μορφή, για παράδειγμα, περιορίζουν την πρόσβαση του χρήστη στην αγορά εργασίας, που εξαρτάται από την ψηφιακή τεχνολογία. Το έργο SmartDegrees, που χρηματοδοτείται από την ΕΕ και είναι ένα έργο που εξελίχθηκε στην Ισπανία προτείνει μια καινοτόμο και πρωτοποριακή λύση, βασισμένη στην τεχνολογία blockchain, που αυξάνει την ψηφιακή υποστήριξη, προσθέτει την ψηφιακή αναγνώριση του χρήστη και επιτρέπει την επέκταση σε άλλους τομείς, όπως η υγειονομική περίθαλψη. Η πρωτοποριακή πλατφόρμα SmartDegrees εισάγει ένα νέο επιχειρηματικό μοντέλο, που εξασφαλίζει αξιόπιστη εγγραφή και πιστοποίηση ακαδημαϊκών πτυχίων, μετατρέποντάς τα σε δυναμικά ψηφιακά στοιχεία.[20]

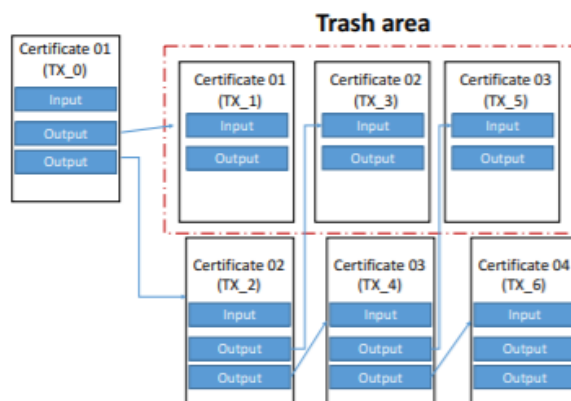
### **3.1.3 BlockSign**

Το Blocksign είναι μια άλλη υπηρεσία που βασίζεται σε blockchain για τη νόμιμη υπογραφή οποιουδήποτε εγγράφου, συμβολαίου ή συμφωνίας. Ουσιαστικά κατακερματίζει (hash) το έγγραφο και το αποθηκεύει σε blockchain. Αλλά σε ένα τέτοιο σύστημα, η επαλήθευση ενός εγγράφου αμέσως μετά την υπογραφή δεν είναι δυνατή, επειδή η προσθήκη μιας συναλλαγής σε ένα blockchain πρέπει να περάσει από διάφορα στάδια.[14] Για να επιτευχθεί η αυθεντικότητα, το Blocksign αποθηκεύει στοιχεία λογαριασμού χρήστη, όπως διεύθυνση ηλεκτρονικού ταχυδρομείου μαζί με τον κρυπτογραφικό κατακερματισμό. Η γνησιότητα του εγγράφου επιτυγχάνεται, συγκρίνοντας τις τιμές κατακερματισμού στη διαδικασία επαλήθευσης. Οι διαδικτυακές εφαρμογές, όπως το "ProofOfExistence", λειτουργούν επίσης με βάση την παραπάνω αρχή.[21]

### **3.1.4 BTCert**

Το BTCert είναι μια πρωτοβουλία του Πανεπιστημίου του Μπέρμιγγαμ του Ηνωμένου Βασιλείου, εμπνευσμένο από το έργο που αναπτύχθηκε στο Ινστιτούτο Τεχνολογίας της Μασαχουσέτης (MIT), Blockcerts. Η προσέγγιση προτείνει την επίλυση ορισμένων αδυναμιών που εντοπίζονται στη λύση του MIT, όπως η ανάκληση. Η ανάκληση ενός πιστοποιητικού συνεπάγεται την αποστολή μιας πληρωμής (π.χ. σε Bitcoin) στη διεύθυνση ανάκλησης του εκδότη, η οποία είναι ενσωματωμένη στο ψηφιακό δίπλωμα. Κάθε ανακληθείσα εγγραφή δημιουργεί έτσι μια νέα συναλλαγή.

Στο σχήμα, η εγγραφή που δημιουργείται κατά την έκδοση ενός πιστοποιητικού πρέπει πάντα να δημιουργεί μια συναλλαγή του κατανεμημένου τύπου, η οποία έχει πάντα μια είσοδο και δύο εξόδους. Σε μια έξοδο, υπάρχουν οι πιστώσεις της δημόσιας διεύθυνσης του πανεπιστημίου, έτοιμες να χρησιμοποιηθούν σε έκδοση, ενώ στην άλλη έξοδο, μια μικρή πίστωση είναι διαθέσιμη για μεταφορά στη δημόσια διεύθυνση της ανάκλησης.[22]



Εικόνα 8: Έκδοση Certificate

Η πίστωση ανάκλησης παραμένει σε κατάσταση αναμονής, έτοιμη να χρησιμοποιηθεί σε περίπτωση ακύρωσης. Όταν πρέπει να ανακληθεί ένα πιστοποιητικό, εκτελείται μια λειτουργία μεταφοράς από τη διεύθυνση έκδοσης στην ανακληθείσα διεύθυνση. Το σύνολο των εγγράφων που φαίνεται στη εικόνα 7 προήλθε από αυτές τις λειτουργίες, σχηματίζοντας μια περιοχή απορριμμάτων. Σημειώστε ότι αν και σε ένα blockchain οι χρεώσεις συναλλαγής είναι δυναμικές, ανάλογα με το ποσό του νομίσματος που απομένει να δημιουργηθεί, υποθέτουμε εδώ ότι τα τέλη ανάκλησης είναι σταθερά. Η διαδικασία ελέγχου λειτουργεί αντίστροφα, που σημαίνει ότι λειτουργεί από την είσοδο στην έξοδο. Τα μπλοκ σχετίζονται με τις συναλλαγές τους από την είσοδο στην προηγούμενη έξοδο. Με αυτόν τον τρόπο, η BTCert προτείνει τον εντοπισμό ενός ανακληθέντος πιστοποιητικού, ερωτώντας τη διεύθυνση που είναι ενσωματωμένη στο ψηφιακό δίπλωμα, ελέγχοντας αν υπάρχει κίνηση στις προηγούμενες εξόδους, χρησιμοποιώντας τη διεύθυνση ανάκλησης. Εάν ναι, για λόγους ασφάλειας, γίνεται ένας δεύτερος έλεγχος, ο έλεγχος αν αυτή η διεύθυνση είναι πραγματική και ανήκει στο πανεπιστήμιο.[23]

### 3.1.5 EduCtx

Το Ευρωπαϊκό Σύστημα Μεταφοράς και Συνσώρευσης Πιστώσεων (ECTS) που αναπτύχθηκε το 1989 από την Ευρωπαϊκή Επιτροπή και υιοθετήθηκε από τα μέλη της Ευρωπαϊκής Ένωσης (ΕΕ) και άλλες χώρες του κόσμου, είναι μια πρωτοβουλία τριτοβάθμιας εκπαίδευσης που αποτελεί τη βασική υποστήριξη του προγράμματος κινητικότητας φοιτητών Erasmus. [24]Το EduCTX , είναι μια πλατφόρμα που δημιουργήθηκε για να μετατρέψει το ECTS σε ψηφιακή μορφή. Το έργο ξεκίνησε χρησιμοποιώντας ένα blockchain ανοιχτού κώδικα, που ονομάζεται Ark , και λειτουργεί σε δίκτυο τύπου κοινοπραξίας (consortium network).[3] Για την επίλυση του προβλήματος της εξουσιοδότησης από όλα τα εμπλεκόμενα μέρη, το σύστημα προτείνει τη χρήση πολλαπλών υπογραφών, διασφαλίζοντας ότι και τα δύο ενδιαφερόμενα μέρη, ο εκδότης και ο παραλήπτης, εξουσιοδοτούν μια πράξη. Το πρωτόκολλο πολλαπλών υπογραφών είναι μια έννοια γνωστή στον κόσμο της κρυπτογραφίας δημόσιου κλειδιού η οποία επιτρέπει στα μέρη να υπογράφουν ψηφιακά ένα συμφωνημένο μήνυμα μαζί, χρησιμοποιώντας τα δικά τους ιδιωτικά κλειδιά . Μια τέτοια έννοια είναι ήδη μια κοινή πρακτική στον κόσμο των κρυπτονομισμάτων και μπορούν να δημιουργηθούν πορτοφόλια blockchain M-to-N , στα οποία το M αντιπροσωπεύει τον ελάχιστο αριθμό υπογραφών και το N το μέγιστο αριθμό δημόσιων διευθύνσεων.[22]

Το EduCTX επιτρέπει σε δύο έως οκτώ συμμετέχοντες να συσχετιστούν και έτσι διασφαλίζει ότι η λειτουργικότητα συνεχίζει να λειτουργεί, ακόμη και αν χαθεί ένα από τα κλειδιά. Με αυτόν τον τρόπο το σύστημα θα είναι πιο ανθεκτικό εάν ένα από τα μέρη καθίσταται μη λειτουργικό. Για παράδειγμα, ένα πανεπιστήμιο μπορεί να κλείσει τις λειτουργίες του, αλλά η κυβέρνηση μπορεί να πάρει από εκεί και να χειριστεί τη διαδικασία πιστοποίησης για λογαριασμό τους. Αυτή η προσέγγιση έχει μεγαλύτερο έλεγχο στη δράση της ανάκλησης, αλλά ανάλογα με τον τρόπο που έχει συσταθεί το σύστημα, μπορεί να θέσει σε κίνδυνο την κυριαρχία του ιδρύματος. Η ασφάλεια του ιδιωτικού κλειδιού επιβάλλεται με

τη χρήση ενός πορτοφολιού κρυπτογραφημένου με κωδικό πρόσβασης ή ενσωματωμένου στο πορτοφόλι Nano HW7 (είναι ένα crypto hardware wallet που προσφέρει offline αποθηκευτικό χώρο για αποθήκευση κρυπτονομισμάτων). Ακόμα, στο πρωτότυπο, δεν υπάρχουν πληροφορίες σχετικά με λειτουργίες που εφαρμόζουν πρόσθετες πληροφορίες για ανάκληση.

### 3.1.6 Blockcerts

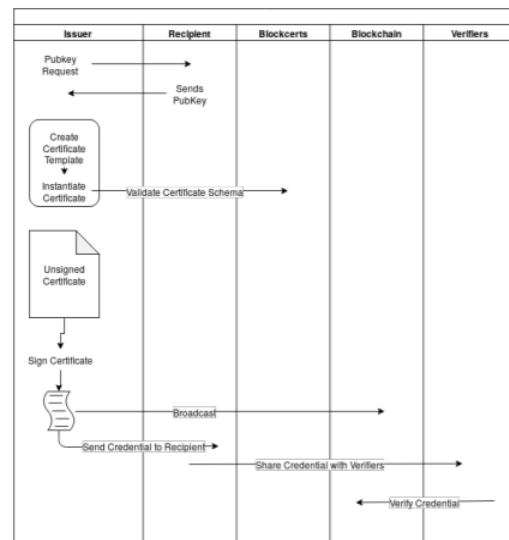
Με στόχο την ύπαρξη ενός παγκόσμιου συστήματος για την επαλήθευση των ακαδημαϊκών αρχείων, η ανάπτυξη των Blockcerts ξεκίνησε το 2015 ως μέρος ενός ερευνητικού έργου από το MIT Media Lab σε συνεργασία με το Learning Machine. [22][26] Το έργο Blockcerts εκμεταλλεύεται την πλατφόρμα Open Badges από κοινού με την τεχνολογία blockchain, προκειμένου να υλοποιήσει ένα παγκόσμιο, αποκεντρωμένο εργαλείο για επικύρωση και πιστοποίηση εγγράφων, με τα ακόλουθα χαρακτηριστικά

- i) Αποδείξεις οποιασδήποτε παραβίασης (tampered evidence)
- ii) Ιδιοκτησία εκδότη και παραλήπτη
- iii) Ευέλικτη μορφή εγγράφων
- iv) Διαδικτυακή και offline κοινή χρήση με επαλήθευση
- v) Ανεξάρτητη επαλήθευση

Το έργο εγκαινιάστηκε επίσημα το 2016 και όλες οι βιβλιοθήκες αναφοράς δημοσιεύθηκαν με άδεια ανοικτού κώδικα MIT, καθιστώντας τον κώδικα εύκολα προσβάσιμο και δωρεάν. Ως εκ τούτου, το Blockcerts ορίζεται ως ένα ανοιχτό πρότυπο για τη δημιουργία, έκδοση, προβολή και επαλήθευση πιστοποιητικών που βασίζονται σε blockchain.[3][25]

Βασικά, ο εκδότης μπορεί να δημιουργήσει αυτόνομα ένα δομημένο πιστοποιητικό Blockcerts, να το υπογράψει και να πιστοποιήσει την ακεραιότητά του, αποθηκεύοντας ένα hash digest του πιστοποιητικού μέσα σε μια συναλλαγή blockchain.

Στη συνέχεια, ο εκδότης μπορεί να στείλει στον παραλήπτη ένα αντίγραφο του υπογεγραμμένου πιστοποιητικού Blockcerts που μπορεί να μοιραστεί σε κοινωνικά δίκτυα, μέσω e-mail κ.λπ. Όποιος έχει πρόσβαση στο πιστοποιητικό, μπορεί να επαληθεύσει την γνησιότητα του, χρησιμοποιώντας μια ανοιχτή πλατφόρμα, που ονομάζεται Blockcerts Universal Verifier, η οποία εκτελεί έλεγχο που βασίζεται σε blockchain. Ολόκληρος ο κύκλος ζωής ενός πιστοποιητικού που βασίζεται σε Blockcerts περιγράφεται στο σχήμα 8. Αφού ολοκληρώσει επιτυχώς τις σπουδές του, ο φοιτητής καλείται από το ακαδημαϊκό ίδρυμα να δώσει μια δημόσια διεύθυνση blockchain. Για το σκοπό αυτό, ο μαθητής δημιουργεί ένα ιδιωτικό/δημόσιο κλειδί για το χρησιμοποιούμενο blockchain και στη συνέχεια υπολογίζει τη δημόσια διεύθυνσή του ως έξοδο μιας μονόδρομης συνάρτησης που εφαρμόζεται στο δημόσιο κλειδί του. Ταυτόχρονα (ή πριν) δημιουργείται από το ίδρυμα έκδοσης ένα πρότυπο πιστοποιητικού συμβατό με Blockcerts. Στη συνέχεια, εκδίδεται ένα νέο πιστοποιητικό και αποστέλλεται στον φοιτητή, μαζί με μια συναλλαγή blockchain στη δημόσια διεύθυνση του, που επιτρέπει την επαλήθευση του εκδοθέντος πιστοποιητικού.[27][28]



Εικόνα 9: Blockcerts Certificate life cycle

### 3.1.7 QualiChain

Το QualiChain είναι ένα ερευνητικό πρόγραμμα χρηματοδοτούμενο από την ΕΕ που στοχεύει στη δημιουργία, την πιλοτική και αξιολόγηση μιας αποκεντρωμένης πλατφόρμας για την αποθήκευση, την ανταλλαγή και την επαλήθευση των προσόντων εκπαίδευσης και απασχόλησης και επικεντρώνεται

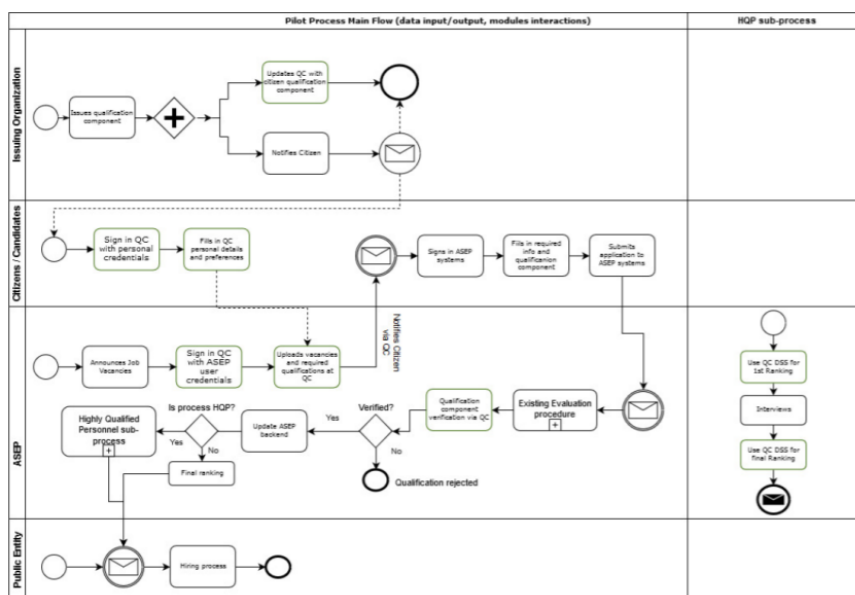


στην εκτίμηση του δυναμικού της τεχνολογίας blockchain, των αλγοριθμικών τεχνικών και της υπολογιστικής νοημοσύνης στον τομέα της δημόσιας εκπαίδευσης, καθώς και της διασύνδεσής της με την ιδιωτική εκπαίδευση, την αγορά εργασίας, τις διοικητικές διαδικασίες του δημόσιου τομέα και τις ευρύτερες κοινωνικοοικονομικές εξελίξεις.

Στην περίπτωση του πιλοτικού έργου του ΑΣΕΠ οι υπηρεσίες πρόσληψης και διαχείρισης ικανοτήτων με το QualiChain θα αξιοποιηθούν για να βελτιώσουν όχι μόνο τον έλεγχο των δηλωθέντων προσόντων των υποψηφίων, αλλά και τον έλεγχο του ποιοι προπορεύονται άλλων σε στοιχεία ομαδικότητας και ηγετικών ικανοτήτων, οδηγώντας σε μια σύντομη λίστα με εκείνους που θα πάρουν συνέντευξη και τελικά στον εντοπισμό του καλύτερου δυνατού υποψηφίου για το ρόλο. Οι χαρακτηριστικές απαιτήσεις από αυτό το πιλοτικό πρόγραμμα είναι:[1][63]

- Παροχή εξατομικευμένων ειδοποιήσεων υποψηφίων για κενές θέσεις εργασίας με αντιστοίχιση μεμονωμένων προφίλ με διαθέσιμες θέσεις εργασίας στον πολιτικό τομέα
- Χρήση του ψηφιακού ledger της λύσης με βάση το Blockchain, προκειμένου να επιτευχθεί η επικύρωσή(δηλ. Επιβεβαίωση της γνησιότητας) τυπικών ακαδημαϊκών προσόντων μεμονωμένων υποψηφίων, απαλλάσσοντας έτσι τον δημόσιο τομέα από τη σχετική γραφειοκρατική επιβάρυνση. Φυσικά, αυτή η λειτουργικότητα μπορεί να επεκταθεί στο μέλλον σε άλλα προσόντα (επαγγελματικά προσόντα, άτυπα ακαδημαϊκά, κλπ). Σε κάθε περίπτωση, το αναμενόμενο όφελος έναντι του τρέχοντος συστήματος είναι σημαντικό αφού οι καθυστερήσεις αναμένεται να μειωθούν σημαντικά, δηλαδή από ημέρες/μήνες σε λεπτά.

#### ΑΣΕΠ Use Case Flow του Qualichain για πιστοποίηση εγγράφων\*



Εικόνα 10: QualiChain Use Case diagram

## 3.2 Blockchain API που προσπαθήσαμε να υλοποιήσουμε

Τα δύο blockchain APIs που προσπαθήσαμε να καλέσουμε από το front end της εφαρμογής μας για να γίνει η πιστοποίηση στο αρχείο που ανεβάζει ο χρήστης είναι το QualiChain και το BlockCerts. Παρακάτω θα παρουσιάσουμε κάποια τεχνικά χαρακτηριστικά των APIs.

### 3.2.1 QualiChain API

Η διαδικασία επαλήθευσης είναι ένα ουσιαστικό στοιχείο στην αρχιτεκτονική και ένας από τους ακρογωνιαίους λίθους της πλατφόρμας QualiChain. Για την επαλήθευση της γνησιότητας ο recruiter του οργανισμού ή της αρχής πρόσληψης λαμβάνει από τον υποψήφιο ένα έγγραφο σε μορφή pdf το οποίο αποτελεί το δίπλωμα για πιστοποίηση. Αυτού του είδους τα έγγραφα φέρουν το IssuerID και το CivilID τα οποία σε συνδυασμό αποτελούν την ταυτότητα του εγγράφου. Έπειτα ανεβάζει πιστοποιεί το έγγραφο στην πλατφόρμα βάζοντας ως είσοδο το pdf αρχείο ,το IssuerId και το CivilID. Το hash του διπλώματος υπολογίζεται. Στη συνέχεια, λαμβάνεται το αντίστοιχο hash του διπλώματος που είναι καταχωρημένο στο δίκτυο (Ropsten) Ethereum, μέσω του παρεχόμενου αναγνωριστικού (Diploma ID). Σε περίπτωση που το υπολογισμένο hash του διπλώματος ταιριάζει με τη hash του παρεχόμενου PDF, το δίπλωμα είναι έγκυρο, δηλαδή είναι αυθεντικό και δεν έχει τροποποιηθεί. Διαφορετικά, η ταυτοποίηση είναι άκυρη.

Το IssuerID προσδιορίζει το ΑΕΙ που εξέδωσε το δίπλωμα. Δεν χρειάζεται να καταχωρίσετε τη διεύθυνση της σύμβασης (contract) του ΑΕΙ, επειδή το QualiChain Recruiting module (βρίσκεται στο παρακάτω github repository) την παίρνει από το έξυπνο συμβόλαιο (smart-contract) του QualiChain Consortium.

Για την χρήση του QualiChain API συμβουλευτήκαμε το repository στο GitHub<sup>1</sup> του API.

### 3.2.2 Blockcerts API

Τα βασικά στοιχεία από τα οποία αποτελείται η διαδικασία της επαλήθευσης στο BlockCerts API είναι το πιστοποιητικό (certificate) blockchain, η συναλλαγή (transaction), η ταυτότητα εκδότη (Issuers Id), και τα στοιχεία ανάκλησης (revoked details) στο blockchain

- **Πιστοποιητικό Blockchain**

Το πιστοποιητικό Blockchain περιέχει:

- το προς επαλήθευση περιεχόμενο
- τη θέση των εισόδων που απαιτούνται για επαλήθευση

- **Συναλλαγή Blockchain**

Ένα πιστοποιητικό Blockchain πρέπει να έχει ένα πεδίο certificate.signature.anchors, το οποίο πρέπει να περιέχει τουλάχιστον μία άγκυρα σε μια συναλλαγή blockchain.

- **Ταυτότητα εκδότη**

Το πεδίο badge.issuer.id στο Πιστοποιητικό Blockchain λέει πού μπορείτε να βρείτε τις τρέχουσες πληροφορίες του εκδότη για τα κλειδιά που είναι έγκυρα. Προς το παρόν, πρόκειται για ένα HTTP URI (αν και το σχήμα επιτρέπει άλλες υλοποιήσεις), το οποίο (όταν παραπέμπει) περιέχει μια σειρά από δημόσια κλειδιά που έκδωσε ο εκδότης. Αυτές οι πληροφορίες απαιτούνται για διασταύρωση των δημόσιων κλειδιών που αξιώνει ο εκδότης με τις πληροφορίες από τη συναλλαγή blockchain.

- **Στοιχεία ανάκλησης εκδότη**

Το πεδίο badge.issuer.revocationList στο Πιστοποιητικό Blockchain αναφέρει πού μπορείτε να λάβετε τη λίστα ανακληθέντων πιστοποιητικών του εκδότη (γνωστός και ως ισχυρισμοί). Το Blockcerts χρησιμοποιεί ένα HTTP URI, σύμφωνα με την προδιαγραφή Open Badges. Όταν

---

<sup>1</sup> <https://github.com/QualiChain/consortium>

παραπέμπεται, αυτό το URI παρέχει μια σειρά ανακληθέντων ισχυρισμών. Το σχήμα Blockcerts επιτρέπει άλλες εφαρμογές ανάκλησης, ανάλογα με τις εφαρμογές που επιτρέπονται από το blockchain και την ακαταλληλότητα domain/εκδότη.

### **Verification Process**

Η διαδικασία πιστοποίησης ενός εγγράφου απαρτίζεται από τα παρακάτω βήματα.

#### **Έλεγχος της ακεραιότητας του πιστοποιητικού**

Ο έλεγχος της ακεραιότητας του πιστοποιητικού διασφαλίζει ότι το πιστοποιητικό δεν έχει παραποιηθεί. Αυτό αποτελείται από 3 βήματα:

- Επικύρωση της απόδειξη Merkle στο πιστοποιητικό.
- Σύγκριση του hash του τοπικού πιστοποιητικού με την τιμή στην απόδειξη.
- Σύγκριση της τιμή merkleRoot στο πιστοποιητικό με την τιμή στη συναλλαγή blockchain.

#### **Έλεγχος την αυθεντικότητας του πιστοποιητικού**

Αυτό το βήμα επαληθεύει ότι το πιστοποιητικό συντάχθηκε από τον εκδότη. Αυτό επαληθεύεται διασφαλίζοντας ότι ο εκδότης διεκδικεί πράγματι το κλειδί υπογραφής για τη συναλλαγή blockchain και ότι το κλειδί ήταν έγκυρο τη στιγμή που εκδόθηκε η συναλλαγή.

Αυτό αποκλείει εξαιρετικές (και πιθανώς δόλιες) περιπτώσεις, όπως:

- το δημόσιο κλειδί δεν αξιώνεται(εκδίδεται) από τον εκδότη
- συναλλαγή εκδόθηκε μετά την ανάκληση ή λήξη του δημόσιου κλειδιού

Η λήξη κλειδιού διαφέρει από τη λήξη πιστοποιητικού, αφού τα κλειδιά λήξης είναι μια καλή πρακτική ασφάλειας για τους εκδότες.

#### **Έλεγχος εάν δεν έχει ανακληθεί από τον εκδότη**

Η είσοδος που λαμβάνεται από τις "Πληροφορίες ανάκλησης εκδότη" περιέχει τη λίστα των ανακληθέντων πιστοποιητικών (ή "ισχυρισμών"). Για "Open Badges" συμβατά με Blockcerts, ένα πιστοποιητικό θεωρείται ότι έχει ανακληθεί εάν οποιαδήποτε καταχώριση αναγνωριστικού στον πίνακα ανακληθέντων αποθέσεων περιέχει το αναγνωριστικό του πιστοποιητικού. Το αναγνωριστικό πιστοποιητικού είναι διαθέσιμο στο πεδίο (id) του πιστοποιητικού Blockchain. Εάν το πιστοποιητικό έχει ανακληθεί, η εντολή "revocationReason" ενδέχεται να παρέχει περισσότερες πληροφορίες σχετικά με τους λόγους ανάκλησης του πιστοποιητικού.

#### **Έλεγχος εάν το πιστοποιητικό δεν έχει λήξει**

Το πιστοποιητικό μπορεί να περιέχει ημερομηνία λήξης. Εάν υπάρχει, η επαλήθευση πρέπει να συγκρίνει αυτήν την τιμή, η οποία είναι διαθέσιμη στο πεδίο λήξης, με την τρέχουσα ώρα.

### **Εφαρμογή της επαλήθευσης**

1. Ανεβάζει ο χρήστης το αρχείο που θέλει να επαλήθευση την γνησιότητα
2. Με την βοήθεια της βιβλιοθήκης cert-verifier-js που παρέχει το Blockcerts μετατρέπουμε το αρχείο αυτό σε «Certificate» - *new Certificate (certificateDefinition, options)* . Και ο constructor κατασκευάζει αυτόματα ένα πιστοποιητικό με κάποιες συγκεκριμένες ιδιότητες.
3. Εφαρμόζεται η εντολή της επαλήθευσης *,verify(stepCallback)* , όπου επιστρέφει την επαλήθευση του πιστοποιητικού που δημιουργήσαμε στο προηγούμενο βήμα.
4. Τέλος λαμβάνουμε την κατάσταση της επαλήθευσης στην μορφή (*{code, status, message}*), που με την σειρά μας τα εμφανίζουμε στον χρήστη.

Για την χρήση του BlockCerts API συμβουλευτήκαμε το repository στο GitHub<sup>2</sup> του API.

---

<sup>2</sup> <https://github.com/blockchain-certificates/cert-verifier-js>

## 4. Τεχνολογίες και Λειτουργίες της εφαρμογής

### 4.1 Πλατφόρμες και εργαλεία ανάπτυξης

Στόχος μας κατά τον σχεδιασμό και την ανάπτυξη της εφαρμογής ήταν να εκμεταλλευτούμε και να αξιοποιήσουμε τα πιο σύγχρονα και τεχνολογικά προηγμένα εργαλεία που υπάρχουν στην αγορά του software development, έτσι ώστε να θέσουμε γερές βάσεις για μια ποιοτική και υψηλά ανταγωνιστική εφαρμογή. Απώτερος σκοπός ήταν η δημιουργία μιας εφαρμογής που δεν θα είχε να ζηλέψει τίποτα από άλλες ήδη υπάρχουσες εφαρμογές και θα παρείχε μια φιλική και προσιτή εμπειρία στον χρήστη. Έχοντας τα παραπάνω στο μυαλό, θα προσπαθήσουμε να συμβαδίσουμε με την τεχνολογική ανάπτυξη της εποχής που ζούμε, ειδικότερα στον τομέα της ανάπτυξης λογισμικού.

Αρχικά, μοντελοποιήσαμε την διεπαφή χρήστη (ui) της εφαρμογής στο εργαλείο σχεδιασμού της Adobe το AdobeXD, έπειτα η ανάπτυξη του λογισμικού της εφαρμογής έγινε στην πλατφόρμα επεξεργασίας κώδικα IntelliJ (IDEA) ως ένα maven project. Η εφαρμογή χτίστηκε εξ ολοκλήρου στην πλατφόρμα Spring ως ένα SpringBoot web-app με την java στο back-end ως κύρια γλώσσα προγραμματισμού. Για την ανάπτυξη της διεπαφής χρήστη ή αλλιώς front-end έγινε χρήση της HTML για την διαμόρφωση της σελίδας, CSS για την επεξεργασία των γραφιστικών και JavaScript για τους αλγορίθμους και τα animation, τα οποία τρέχουνε στο client κομμάτι της εφαρμογής. Για την επικοινωνία μεταξύ back-end και front-end χρησιμοποιήθηκε το εργαλείο thymeleaf. Τέλος, για την βάση δεδομένων αξιοποιήθηκαν γνώσεις από μαθήματα της σχολής (Βάσεις Δεδομένων, Προηγμένα Συστήματα Βάσεων Δεδομένων) και στήθηκε στο εργαλείο MySQL Workbench.

Όλα αυτά αποτελούν μια συνοπτική και περιγραφική παρουσίαση των εργαλείων και των τεχνολογιών που αξιοποιήθηκαν. Θα αναπτύξουμε περαιτέρω περί του θέματος στα ακόλουθα υποκεφάλαια, που θα γίνει η πλήρης καταγραφή και επεξήγηση όλων των σύγχρονων εργαλείων και πλατφόρμων που συνέβαλαν στην υλοποίηση της εφαρμογής. Για χάρην ευκολίας της ανάγνωσης, τα εργαλεία θα ταξινομηθούν ανάλογα σε πιο μέρος της εφαρμογής χρησιμοποιήθηκαν (database, back-end, front-end).

#### 4.1.1 Βάση Δεδομένων

- **MySQL Workbench:**

Είναι ένα σύγχρονο εργαλείο σχεδίασης βάσεων δεδομένων με φιλική προς τον χρήστη διεπαφή (user interface), που ενσωματώνει σε ένα ενιαίο και ολοκληρωμένο περιβάλλον, την ανάπτυξη, διαχείριση, δημιουργία και συντήρηση βάσεων MySQL.[29]

- **Hibernate Framework:**

Το Hibernate είναι Java framework που απλοποιεί την ανάπτυξη μιας εφαρμογής Java όσον αφορά την αλληλεπίδραση με τη βάση δεδομένων. Είναι ένα ανοιχτού κώδικα, μη απαιτητικό, εργαλείο ORM (Object Relational Mapping). Το Hibernate εφαρμόζει τις προδιαγραφές του JPA (Java Persistence API) για την διαχείριση, αποθήκευση και το πέρασμα δεδομένων. Τώρα το εργαλείο ORM απλοποιεί τη δημιουργία δεδομένων, τον χειρισμό δεδομένων και την πρόσβαση στα δεδομένα. Είναι μια τεχνική προγραμματισμού που αντιστοιχίζει το αντικείμενο στα δεδομένα που είναι αποθηκευμένα στη βάση δεδομένων και κάνει χρήση του JDBC API για να επικοινωνεί και να αλληλοεπιδρά με την βάση δεδομένων.[30]

#### 4.1.2 Back-End

- **Maven:**

Το Maven είναι ένα ισχυρό εργαλείο διαχείρισης projects που βασίζεται σε POM (project object model). Χρησιμοποιείται κυρίως για την ανάπτυξη, την τεκμηρίωση και την συγγραφή των εξαρτήσεων ενός project. Απλοποιεί τη διαδικασία κατασκευής, όπως το ANT αλλά είναι πολύ πιο ισχυρό από αυτό. Με λίγα λόγια μπορούμε να πούμε ότι το maven είναι ένα εργαλείο που μπορεί να χρησιμοποιηθεί για την κατασκευή και τη διαχείριση οποιουδήποτε έργου που βασίζεται σε Java. Το maven διευκολύνει την καθημερινή εργασία των προγραμματιστών Java και γενικά βοηθά στην κατανόηση οποιουδήποτε έργου που βασίζεται σε Java.[34][35]

- **Spring Boot:**

Το Spring Boot παρέχει μια καλή πλατφόρμα για τους προγραμματιστές Java για να αναπτύξουν μια αυτόνομη και παραγωγική εφαρμογή Spring, που μπορεί απλά να τρέξει με το πάτημα ενός κουμπιού. Δίνει την δυνατότητα στον προγραμματιστή να ξεκινήσει το χτίσιμο μιας εφαρμογής με ελάχιστες αρχικές ρυθμίσεις και χωρίς να χρειαστεί να εγκαταστήσει ολόκληρη την πλατφόρμα του Spring για να τρέξει μια εφαρμογή. Τα θετικά αυτής της πλατφόρμας και οι λόγοι που μας ώθησαν στο να την επιλέξουμε ήταν πως είναι εύκολη στην κατανόηση και στην ανάπτυξη Spring εφαρμογών, αυξάνει δραστικά την παραγωγικότητα, αφού ελαττώνει τον χρόνο που θα χρειαστεί μια εφαρμογή για να ολοκληρωθεί και τέλος σου δίνει την δυνατότητα να επιλέξεις μόνο τα εργαλεία και τις παραμέτρους που χρειάζεται το δικό σου πρόγραμμα, όπως για παράδειγμα το Spring Security dependency.[36]

- **Spring Security:**

Το Spring Security είναι μια πλατφόρμα- εργαλείο του Spring που είναι πολύ ισχυρή και εξαιρετικά προσαρμόσιμη με βάση τις ανάγκες της κάθε εφαρμογής, και παρέχει ένα πλαίσιο ελέγχου ταυτότητας και ελέγχου πρόσβασης στη εφαρμογή. Είναι το de-facto πρότυπο για τη διασφάλιση εφαρμογών που βασίζονται στο Spring.

Η Spring Security είναι μια πλατφόρμα που επικεντρώνεται στην παροχή ελέγχου ταυτότητας και εξουσιοδότησης σε εφαρμογές Java. Όπως όλα τα έργα του Spring, η πραγματική δύναμη του Spring Security κρύβεται στο πόσο εύκολα και γρήγορα είναι επεκτάσιμο, με σκοπό να ικανοποιήσει τις προσαρμοσμένες απαιτήσεις της εκάστοτε εφαρμογής. Κάποια από τα κύρια χαρακτηριστικά της πλατφόρμας αυτής είναι τα ακόλουθα:[37]

1. LDAP (Lightweight Directory Access Protocol)
2. Single sign-on
3. JAAS (Java Authentication and Authorization Service) Login Module
4. Basic Access Authentication
5. Digest Access Authentication
6. Remember-me
7. Web Form Authentication
8. Authorization
9. Software Localization
10. HTTP Authorization

Στην εφαρμογή που φτιάξαμε εμείς πιο συγκεκριμένα χρησιμοποιήσαμε τα χαρακτηριστικά 2,3,4,7 και 8 κυρίως για την εγγραφή και την σύνδεση του χρήστη στον λογαριασμό του όπως και για την λειτουργία forgot my password, με απώτερο στόχο να αυξήσουμε την ασφάλεια της εφαρμογής.[38][39]

- **Bcrypt:**

Όλοι γνωρίζουν και καταλαβαίνουν ότι η αποθήκευση του κωδικού πρόσβασης ως απλό κείμενο στη βάση δεδομένων είναι μια κίνηση αφελής αλλά συγχρόνως καθόλου ασφαλή. Ωστόσο, αρκετοί προγραμματιστές το κάνουν, επειδή καθιστά ευκολότερη την ανάκτηση κωδικού από την βάση δεδομένων, όπως επίσης διευκολύνει κατά ένα μεγάλο βαθμό και την διαδικασία του testing. Αυτό όμως κάνει πιο ευάλωτη την εφαρμογή σε επιθέσεις από κακόβουλα προγράμματα ή χάκερς, που στόχο έχουν την υποκλοπή προσωπικών στοιχείων των χρηστών. [40]Γι' αυτό τον λόγο κάνουμε χρήση του εργαλείου bcrypt κατά την αποθήκευση του κωδικού και άλλων ευαίσθητων στοιχείων του χρήστη. Το bcrypt, με λίγα λόγια είναι μια τεχνική κατακερματισμού κωδικού πρόσβασης που χρησιμοποιείται για τη την ασφάλεια της εφαρμογής και του κωδικού πρόσβασης. Χρησιμοποιείται για την προστασία του κωδικού πρόσβασης από επιθέσεις χάκερ, επειδή ο κωδικός πρόσβασης είναι αποθηκευμένος σε κρυπτογραφημένη μορφή.

- **Gmail SMTP Server**

Ο διακομιστής Gmail SMTP της Google είναι μια δωρεάν υπηρεσία SMTP, την οποία όποιος έχει λογαριασμό Gmail, μπορεί να χρησιμοποιήσει για την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου. Μπορεί να χρησιμοποιηθεί με προσωπικά μηνύματα ηλεκτρονικού ταχυδρομείου ή ακόμη και σε ιστοσελίδες και εφαρμογές, εάν σκοπός είναι να σταλούν αυτόματα μηνύματα ηλεκτρονικού ταχυδρομείου για πράγματα, όπως φόρμες επικοινωνίας, ειδοποιήσεις κ.α. Στην δική μας περίπτωση αυτό το δωρεάν εργαλείο μας έδωσε την δυνατότητα να στέλνουμε προσωπικά emails στον κάθε χρήστη ξεχωριστά, ο οποίος θέλει να ανακτήσει τον κωδικό του και έκανε χρήση της λειτουργίας forgot my password. Πιο συγκεκριμένα, μετά από το αίτημα του χρήστη, λαμβάνει ο ίδιος ένα email το οποίο περιέχει ένα URL προς την σελίδα επαναφοράς κωδικού. Σε αυτό το URL link υπάρχει εμφωλευμένο το hash token του χρήστη που αυτό του δίνει την δυνατότητα μόνο σε αυτόν να έχει πρόσβαση στο link. Αν το link χρησιμοποιηθεί, τότε δεν μπορεί να ξαναχρησιμοποιηθεί από τον οποιοδήποτε, ούτε ακόμα και από τον ίδιο τον χρήστη, αφού το hash token θα έχει λήξει.

### 4.1.3 Front-End

- **Thymeleaf**

Το Thymeleaf είναι μια σύγχρονη μηχανή Java templates από την πλευρά του διακομιστή τόσο για ιστό όσο και για αυτόνομα περιβάλλοντα. Ο κύριος στόχος του Thymeleaf είναι να φέρει κομψά φυσικά templates στη ροή εργασίας ανάπτυξης - HTML η οποία θα πρέπει να μπορεί να εμφανιστεί σωστά στα προγράμματα περιήγησης και επίσης να λειτουργήσει ως στατικά πρωτότυπα, επιτρέποντας ισχυρότερη συνεργασία σε ομάδες ανάπτυξης. Με λίγα λόγια είναι μια βιβλιοθήκη της Java που μπορεί να χαρακτηριστεί και ως μηχανή δημιουργίας template και την χρησιμοποιούμε για να κάνουμε μετατροπές στα αρχεία template, με απώτερο σκοπό να εμφανίζουμε στον χρήστη δεδομένα και κείμενο που παράγονται από την κύρια εφαρμογή μας. Στην δική μας εφαρμογή χρησιμοποιείται κυρίως για την επικοινωνία του front με το back-end.[41]

- **Bootstrap**

Το Bootstrap είναι μια ισχυρή εργαλειοθήκη - μια συλλογή εργαλείων HTML, CSS και JavaScript για τη δημιουργία ιστοσελίδων και διαδικτυακών εφαρμογών. Είναι ένα δωρεάν έργο που κατατάσσεται στην κατηγορία των projects ανοιχτού κώδικα, φιλοξενείται στο GitHub και δημιουργήθηκε αρχικά από (και για) το Twitter.

Μετά την κυκλοφορία ανοιχτού κώδικα το 2011, το Bootstrap έγινε δημοφιλές πολύ γρήγορα, και αυτό γιατί άρεσε πολύ στους σχεδιαστές ιστοσελίδων και στους προγραμματιστές, αφού ήταν μια σωτήρια λύση για αυτούς λόγω του ότι είναι εύελικτο και εύκολο στην χρήση του.

[42]Τα κύρια πλεονεκτήματά του είναι η ανταπόκριση σχεδιασμού (responsive design), διατηρεί ευρεία συμβατότητα με προγράμματα περιήγησης, προσφέρει σταθερό σχεδιασμό χρησιμοποιώντας επαναχρησιμοποιήσιμα εξαρτήματα και είναι πολύ εύκολο στη χρήση και γρήγορο στην εκμάθηση. Προσφέρει πλούσια επεκτασιμότητα χρησιμοποιώντας JavaScript, συνοδευόμενη από ενσωματωμένη υποστήριξη για πρόσθετα jQuery και API JavaScript μέσω προγραμματισμού. Το Bootstrap μπορεί να χρησιμοποιηθεί με οποιοδήποτε IDE ή πρόγραμμα επεξεργασίας και οποιαδήποτε τεχνολογία και γλώσσα διακομιστή, από ASP.NET έως PHP έως Ruby on Rails.

Με το Bootstrap, οι προγραμματιστές ιστού μπορούν να επικεντρωθούν στο έργο ανάπτυξης, χωρίς να ανησυχούν για το σχεδιασμό αφού θα είναι σε θέση να αναπτύξουν γρήγορα έναν ωραίο αισθητικά ιστότοπο. Αυτό γιατί δίνει στους σχεδιαστές ιστοσελίδων ένα στερεό θεμέλιο για τη δημιουργία ενδιαφερόντων θεμάτων Bootstrap.

#### 4.1.4 Other technologies

- **MVC αρχιτεκτονική στην Java:**

Τα μοντέλα τα οποία βασίζονται στην αρχιτεκτονική MVC(Model View Controller) ακολουθούν ένα συγκεκριμένο μοτίβο και διαχωρίζουν τη λογική της εφαρμογής από την διεπαφή χρήστη κατά τον σχεδιασμό τους, Όπως εύκολα καταλαβαίνουμε και από την ονομασία η αρχιτεκτονική αυτή αποτελείται από 3 κύρια επίπεδα, τα οποία είναι:[31]

1. Το μοντέλο(model): Το οποίο αντιπροσωπεύει το επιχειρηματικό επίπεδο της εφαρμογής
2. Η προβολή (view): Η οποία ορίζει το πως παρουσιάζεται στον χρήστη η εφαρμογή
3. Τον ελεγκτή(controller): Ο οποίος διαχειρίζεται τη ροή της εφαρμογής[33]

Στο πλαίσιο προγραμματισμού Java, το μοντέλο αποτελείται από απλές κλάσεις Java, το View εμφανίζει τα δεδομένα στον χρήστη και το Controller αποτελείται από servlets.[32] Αυτός ο διαχωρισμός έχει ως αποτέλεσμα την επεξεργασία των αιτημάτων των χρηστών ως εξής:

1. Το πρόγραμμα περιήγησης στον υπολογιστή -πελάτη στέλνει ένα αίτημα για μια σελίδα στον ελεγκτή που υπάρχει στον διακομιστή
2. Ο ελεγκτής εκτελεί τη διαδικασία της επίκλησης του μοντέλου, ανακτώντας έτσι τα δεδομένα που χρειάζεται σε απάντηση του αιτήματος
3. Στη συνέχεια, ο ελεγκτής δίνει τα δεδομένα που ανακτήθηκαν στην προβολή
4. Γίνεται επεξεργασία της απάντησης αυτής και εκτελούνται οι κατάλληλες διαδικασίες για την σωστή προβολή της και έπειτα αποστέλλεται πίσω στον πελάτη για εμφάνιση του προγράμματος περιήγησης.

Οι λόγοι που επιλέξαμε να χρησιμοποιήσουμε την παραπάνω αρχιτεκτονική σχεδιασμού της εφαρμογής, πέρα από το ότι αποτελεί την πιο σύγχρονη επιλογή για πολλές εφαρμογές μεγάλου βεληνεκούς, είναι:

- 1.Η ευκολία στην επέκταση της εφαρμογής εισάγοντας περισσότερους προγραμματιστές οι οποίοι θα μπορούν να δουλεύουν και στα 3 επίπεδα ταυτόχρονα
- 2.Είναι επίσης ευκολότερη και η συντήρηση του κώδικα, αφού τα επίπεδα αυτά δεν εξαρτώνται το ένα από το άλλο.
- 3.Ένα μοντέλο μπορεί να επαναχρησιμοποιηθεί όσες φορές χρειάζεται από πολλά μοντέλα ταυτόχρονα.
- 4.Ευκολότερος έλεγχος της εφαρμογής.
- 5.Κάνει την εφαρμογή πιο κατανοητή στους προγραμματιστές αφού υπάρχει ο ξεκάθαρος διαχωρισμός των επιπέδων.

- **GitHub**

Το GitHub είναι μια πλατφόρμα που βασίζεται στο ιντερνέτ και χρησιμοποιεί το Git (λογισμικό ελέγχου έκδοσης ανοιχτού κώδικα, που επιτρέπει σε πολλούς χρήστες να κάνουν ξεχωριστές

αλλαγές σε ιστοσελίδες ή projects κώδικα ταυτόχρονα). Επειδή επιτρέπει τη συνεργασία σε πραγματικό χρόνο, το GitHub ενθαρρύνει τις ομάδες να συνεργαστούν για τη δημιουργία και την επεξεργασία του περιεχομένου του ιστότοπού τους και οποιουδήποτε άλλου project. Ο κάθε developer μπορεί να συνεισφέρει στον κώδικα από όπου κι αν βρίσκεται, κάνοντας απλά αιτήματα pull και push στα διάφορα branches του κώδικα. Έτσι γίνεται το κάθε project άμεσα και εύκολα επεκτάσιμο, επειδή μπορούν να συνεργαστούν πολλοί developers ταυτόχρονα.

- **Azure Portal**

Το Azure Portal είναι μια cloud computing πλατφόρμα, η οποία είναι συνδεδεμένη με τον κυβερνοχώρο και δίνει την δυνατότητα στον χρήστη να έχει πρόσβαση, καθώς και να διαχειρίζεται υπηρεσίες και πόρους «νέφους» («cloud» services), τις οποίες παρέχει, στην περίπτωση του Azure, η Microsoft. Κάποιες από αυτές τις υπηρεσίες μπορεί να είναι η αποθήκευση μεγάλου όγκου δεδομένων, όπως επίσης και υπηρεσίες deployment ενός web app σαν και αυτή που χρησιμοποιήσαμε στην δική μας περίπτωση.[48]

- **Adobe XD**

Το Adobe XD είναι το εργαλείο της Adobe το οποίο βοηθάει στο σχεδιασμό της διεπαφής χρήστη για την αλληλεπίδρασή του με μια εφαρμογή όπως και για τον σχεδιασμό της όλης εμπειρίας του χρήστη με την εφαρμογή. Οι δυνατότητες του Adobe XD χρησιμοποιούνται για τη δημιουργία mockups, πρωτοτύπων για ψηφιακά προϊόντα, όπως ιστότοπους και εφαρμογές για κινητά.

## 4.2 Λειτουργικότητες της Εφαρμογής

Καταρχάς, η κύρια λειτουργία που προσπαθήσαμε να υλοποιήσουμε στην εφαρμογή μας ήταν η πιστοποίηση δικαιολογητικών μέσα από διαφορετικά Blockchain APIs, πράγμα που θα καθιστούσε την εφαρμογή μας ένα πρότυπο πλατφόρμας που κάτω από αυτή στο μέλλον θα υπάρχει η δυνατότητα να στεγαστούν πολλαπλά blockchain APIs, τα οποία αποθηκεύουν και πιστοποιούν έγγραφα. Πέρα από αυτό όμως στόχος μας κατά την ανάπτυξη της εφαρμογής ήταν να την κάνουμε όσο γίνεται πιο ολοκληρωμένη με έμφαση στην καλή εμπειρία του χρήστη, για να μπορεί να είναι εύκολα διαχειρίσιμη από τον καθένα. Έτσι, συμπεριλάβαμε στην εφαρμογή αρκετές βασικές λειτουργίες, όπως την εγγραφή νέου χρήστη βάσει του email του, την σύνδεσή του στην εφαρμογή με τα στοιχεία που αυτός δήλωσε, την διαχείριση και την αλλαγή των στοιχείων του λογαριασμού που δήλωσε αρχικά από την σελίδα του προφίλ του, όπως επίσης και λειτουργία “ξέχασα τον κωδικό μου” (forgot my password) για τις περιπτώσεις χρηστών, που δεν μπορούν να συνδεθούν στον λογαριασμό τους. Έπειτα προσθέσαμε κάποιες λειτουργίες, οι οποίες συμπληρώνουν την κύρια λειτουργικότητα που είναι η πιστοποίηση των εγγράφων, με απώτερο σκοπό να φτιάξουμε μια πιο ολοκληρωμένη εμπειρία για τον χρήστη. Αυτές οι λειτουργίες είναι η αποθήκευση του εγγράφου, εάν αυτό πιστοποιηθεί επιτυχώς, η δυνατότητα ταξινόμησης των εγγράφων των οποίων αποθήκευσε ο χρήστης, όπως η διαγραφή τους ή ακόμα και το κατέβασμά τους σε περίπτωση που ο χρήστης δεν έχει εύκαιρο το αρχικό έγγραφο κ.α. Τέλος, προσθέσαμε στην εφαρμογή λειτουργίες που ενδυναμώνουν την αλληλεπίδραση του χρήστη με εμάς τους δημιουργούς της εφαρμογής. Ένα παράδειγμα αυτού είναι η καρτέλα contact που επιτρέπει στον χρήστη να επικοινωνήσει άμεσα με τον developer της εφαρμογής. Αναλυτικότερα, θα εξηγήσουμε τις λειτουργίες αυτές, όπως και άλλες που δεν έχουν αναφερθεί παρακάτω.

Το σύστημά μας απευθύνεται σε δύο διαφορετικές ομάδες χρηστών. Η πρώτη είναι οι απλοί χρήστες και η δεύτερη είναι ο root user ή αλλιώς διαχειριστής του συστήματος. Αυτές οι δύο ομάδες έχουν κάποιες ίδιες λειτουργικότητες αλλά και κάποιες εντελώς διαφορετικές. Αρχικά, θα αναλύσουμε τις κοινές λειτουργικότητες των χρηστών μας και μετέπειτα θα διαχωρίσουμε τις δυο ομάδες, αναλύοντας



τις μοναδικές λειτουργικότητες της κάθε μιας ξεχωριστά. Περισσότερα πίσω για το business model της εφαρμογής θα πούμε στο επόμενο κεφάλαιο.

#### 4.2.1 Βασικές Λειτουργικότητες Απλού Χρήστη

- **Register (εγγραφή νέου χρήστη)**

Όλοι οι χρήστες της εφαρμογής έχουν την δυνατότητα να εγγραφούν σε αυτήν, δημιουργώντας ένα λογαριασμό για να μπορούν έπειτα να συνδεθούν σε αυτόν. Κατά την διάρκεια της εγγραφής ο χρήστης πρέπει να εισάγει κάποια απαραίτητα στοιχεία στα αντίστοιχα πεδία. Αυτά τα στοιχεία είναι το FirstName (Όνομα), LastName (επίθετο), email, καθώς και το password (κωδικός χρήστη). Η εφαρμογή απαιτεί από τον χρήστη να πληκτρολογήσει ξανά τον κωδικό, για να τον επιβεβαιώσει, ελέγχοντας συγχρόνως αν οι δύο κωδικοί που συμπλήρωσε ο χρήστης συμφωνούν. Αν ναι, του επιτρέπει να εγγραφεί. Αν όχι, εμφανίζεται μήνυμα στον χρήστη πως οι κωδικοί δεν είναι ίδιοι και τον αφήνει να τους διορθώσει. Επίσης, η εφαρμογή ελέγχει αν ο χρήστης έχει δώσει έγκυρο και σωστής μορφής email, όπως και τα μεγέθη του ονόματος, του επιθέτου και του κωδικού να είναι στα επιτρεπτά όρια. Αν κάτι από τα παραπάνω συμπληρωθεί λανθασμένα, η εφαρμογή ενημερώνει τον χρήστη με ένα μήνυμα και του δίνει το περιθώριο να τα διορθώσει. Αλλιώς, αν είναι όλα τα πεδία σωστά, γίνεται επιτυχής η εγγραφή του χρήστη και με ένα παράθυρο του δίνεται η επιλογή να επιστρέψει στην σελίδα του login.

- **Login (σύνδεση χρήστη)**

Εφόσον ένας χρήστης είναι εγγεγραμμένος στην εφαρμογή, θα έχει την δυνατότητα να συνδεθεί σε αυτήν, εισάγοντας τα στοιχεία του email, που λειτουργεί σαν primary key (μοναδικό κλειδί: είναι το αναγνωριστικό του κάθε χρήστη και με βάση αυτό ξεχωρίζει από τους υπόλοιπους, μιας και δεν γίνεται να υπάρχουν δυο ίδια email στην βάση δεδομένων), και τον κωδικό του, στην σελίδα του login. Αν τα στοιχεία που συμπλήρωσε είναι σωστά, τότε γίνεται επιτυχής η σύνδεση και μεταφέρεται στην κύρια σελίδα της εφαρμογής στην οποία βρίσκεται και κύρια λειτουργικότητα (πιστοποίηση εγγράφων). Αν πάλι κάποιο από τα στοιχεία που εισήγαγε ο χρήστης είναι λανθασμένο (κωδικός η email), η εφαρμογή του εμφανίζει μήνυμα πως κάτι πήγε λάθος με την εισαγωγή στοιχείων και δίνει την επιλογή στον χρήστη να προσπαθήσει ξανά να συνδεθεί. Εσκεμμένα δεν επιλέγουμε να εμφανίσουμε στον χρήστη μήνυμα με το ποιο στοιχείο ακριβώς δεν συμπλήρωσε σωστά, ως ένα από τα μέτρα προστασίας των δεδομένων των χρηστών μας από κακόβουλες ενέργειες, αφού έτσι εύκολα θα μπορούσε κάποιος να δει ποια email είναι εγγεγραμμένα στην εφαρμογή μας και βρίσκονται στην βάση μας.

- **Forgot my Password (ξέχασα τον κωδικό μου)**

Αυτή η λειτουργικότητα δίνει την δυνατότητα στον χρήστη τον οποίο ξέχασε τον κωδικό του να τον ανακτήσει. Αν ο χρήστης πατήσει στην επιλογή forgot my password κατευθύνεται σε μια σελίδα που του ζητάει να πληκτρολογήσει την διεύθυνση email του. Γίνεται έλεγχος από την εφαρμογή αν η διεύθυνση που εισήγαγε ο χρήστης ανήκει σε κάποιον χρήστη που είναι καταχωρημένος στην βάση δεδομένων. Αν η διεύθυνση δεν βρεθεί στην βάση, τότε εμφανίζεται το αντίστοιχο μήνυμα στον χρήστη και αυτός καλείται να συμπληρώσει ξανά το πεδίο με σωστό email αυτή την φορά. Στην περίπτωση που ο χρήστης συμπληρώσει επιτυχημένα στο email του, του εμφανίζεται μήνυμα πως η εφαρμογή έστειλε προσωπικό email στην διεύθυνση στην οποία εισήγαγε ο ίδιος. Η εφαρμογή δημιουργεί ένα μοναδικό token για τον χρήστη, το οποίο το στέλνει εμφωλευμένο στο URL της σελίδας ανάκτησης κωδικού. Αυτό το URL είναι προσβάσιμο μόνο από τον συγκεκριμένο χρήστη και είναι μιας χρήσης, αφού δεν μπορεί να χρησιμοποιηθεί ξανά. Κι αυτό γιατί μόλις χρησιμοποιηθεί από τον χρήστη, τότε διαγράφεται το token του χρήστη από την βάση δεδομένων και δεν μπορεί να γίνει η

ταυτοποίηση. Αν περάσει μεγάλο χρονικό διάστημα ή αν το URL που στάλθηκε έχει χρησιμοποιηθεί, τότε εμφανίζεται στον χρήστη το μήνυμα «token expired», αλλιώς κατευθύνεται στην σελίδα αλλαγής του κωδικού. Εκεί ζητείται από τον χρήστη να πληκτρολογήσει τον νέο του κωδικό και να τον επιβεβαιώσει. Το πρόγραμμα ελέγχει αν ο χρήστης εισήγαγε σωστά τον κωδικό, αν όλα είναι εντάξει εμφανίζεται το μήνυμα επιτυχίας αλλαγής κωδικού και ο χρήστης επιστρέφει στην σελίδα του login, αλλιώς εμφανίζεται μήνυμα λάθους και του δίνεται η ευκαιρία να συμπληρώσει σωστά το κωδικό.

#### 4.2.2 Άλλες Λειτουργικότητες

- **My account**

Μέσα από την καρτέλα MyAccount ο χρήστης έχει την δυνατότητα να δει τα στοιχεία που συμπλήρωσε ο ίδιος κατά την διαδικασία της εγγραφής του. Αλλά και να τα ανανεώσει, αν αυτό θελήσει. Και εδώ το πρόγραμμα ελέγχει τις εισόδους που συμπληρώνει ο χρήστης στα ανάλογα πεδία και, αν κάτι δεν πληροί τις προϋποθέσεις, του εμφανίζει το αντίστοιχο μήνυμα. Αν όλα τα πεδία έχουν τιμές που να συμφωνούν με τις προϋποθέσεις του προγράμματος, τότε ο χρήστης λαμβάνει το μήνυμα επιτυχίας ανανέωσης των προσωπικών του δεδομένων.

- **Search and sort My Documents (ταξινόμηση και αναζήτηση εγγράφων)**

Ο απλός χρήστης καθώς και ο διαχειριστής της σελίδας έχουν την δυνατότητα να ταξινομήσουν τα έγγραφα τα οποία πιστοποιήσαν και μετά αποθηκεύσαν. Πιο συγκεκριμένα, στην καρτέλα My Documents και των δύο χρηστών μπορούν οι χρήστες να ταξινομήσουν τα αποθηκευμένα τους έγγραφα βάσει του ID του εγγράφου ή του ονόματος, καθώς και της ημερομηνίας και της ώρας που το αποθήκευσαν. Επίσης, στην ίδια καρτέλα δίνεται η δυνατότητα στον χρήστη να αναζητήσει λέξεις κλειδιά, ακόμα και αριθμούς που να σχετίζονται με το έγγραφό του από το πλαίσιο της αναζήτησης στην σελίδα.

- **Clear History**

Αυτή η λειτουργικότητα επιτρέπει στον χρήστη να διαγράψει με το πάτημα ενός κουμπιού ολόκληρο το ιστορικό εγγράφων, τα οποία ο ίδιος έχει πιστοποιήσει και αποθηκεύσει. Με το πάτημα του κουμπιού εμφανίζεται ένα μήνυμα, το οποίο ενημερώνει τον χρήστη αν είναι ενημερωμένος για τις συνέπειες αυτής της λειτουργικότητας και αν είναι βέβαιος για να προχωρήσει. Σε θετική απάντηση του χρήστη διαγράφεται το ιστορικό του από την βάση δεδομένων, αλλιώς δεν γίνεται τίποτα και ο χρήστης μεταφέρεται στην καρτέλα με τα έγγραφά του.

- **Download and Delete documents**

Ο χρήστης έχει τη δυνατότητα μέσα από την καρτέλα My Documents να κατεβάσει τα έγγραφα που αποθήκευσε σε περίπτωση που δεν τα έχει μαζί του και τα χρειαστεί ή ακόμα και να διαγράψει όποια αυτός θέλει από την βάση δεδομένων. Το πρόγραμμα, πριν προβεί σε οποιαδήποτε ενέργεια διαγραφής των εγγράφων, θα ρωτήσει τον χρήστη με ένα μήνυμα αν είναι σίγουρος για την διαγραφή του συγκεκριμένου εγγράφου.

- **Logout**

Επιλέγοντας το logout από το menu λειτουργικοτήτων, ο χρήστης αποσυνδέεται από την εφαρμογή και επιστρέφει στην αρχική σελίδα του login.

#### 4.2.3 Αποκλειστικές Λειτουργικότητες του απλού Χρήστη-Recruiter

Ο απλός χρήστης της εφαρμογής μπορεί να είναι ένας χρήστης ο οποίος θέλει να ελέγξει την γνησιότητα των εγγράφων του και έπειτα να τα αποθηκεύσει για να τα έχει κάπου μαζεμένα, αλλά μπορεί επίσης

να είναι και ένας recruiter που σκοπό έχει να ελέγξει την γνησιότητα των εγγράφων που του έχουν αποσταλεί για την κάλυψη μιας θέσης εργασίας η οτιδήποτε άλλο.

*\*Περισσότερα για το business κομμάτι της εφαρμογής θα αναπτυχθούν αναλυτικότερα στο επόμενο κεφάλαιο*

- **About**

Στο μενού λειτουργικότητας ο απλός χρήστης μπορεί να βρει την καρτέλα about. Στην καρτέλα αυτή αναγράφονται ορισμένες πληροφορίες με το project γενικότερα, όπως επίσης γίνεται και αναφορά για τα συγκεκριμένα Blockchain APIs που χρησιμοποιήσαμε για την υλοποίηση της εφαρμογής. Επίσης, σε αυτή την σελίδα ο χρήστης μπορεί να συναντήσει και ένα μικρό αλλά περιεκτικό εγχειρίδιο χρήσης για το πως μπορεί να πιστοποιήσει στα δύο APIs τα έγγραφα του και στην συνέχεια, αν είναι γνήσια, να τα αποθηκεύσει, έτσι ώστε να τα βρει στην καρτέλα My Documents.

- **Contact**

Σε μια προσπάθειά μας να φέρουμε πιο κοντά τον χρήστη σε εμάς τους δημιουργούς της εφαρμογής, με απώτερο σκοπό να πετύχουμε μια πιο άμεση αλληλεπίδραση χρήστη-developer, δημιουργήσαμε την καρτέλα contact. Αυτή η λειτουργικότητα δίνει την ευκαιρία στον χρήστη να έρθει σε επαφή με εμάς τους developers, στέλνοντάς μας μήνυμα για ότι τον προβληματίζει, πιθανά bugs που βρήκε στην εφαρμογή και χρειάζονται άμεση διόρθωση, ακόμα και να μας δώσει τα συγχαρητήριά του για την πολύ καλή δουλειά την οποία κάναμε. Αυτό μπορεί να το πετύχει συμπληρώνοντας στα κατάλληλα πεδία το θέμα και το περιεχόμενο του μηνύματος που θα ήθελε να στείλει σε εμάς. Πατώντας το κουμπί send, θα ανακατευθυνθεί στον προσωπικό του λογαριασμό email και αυτόματα θα συμπληρωθεί το μήνυμα που θέλει να αποστείλει. Το μόνο που μένει από την πλευρά του είναι να επιβεβαιώσει την αποστολή. Επίσης, ο χρήστης στην σελίδα contact θα συναντήσει και άλλους τρόπους επικοινωνίας με τους δημιουργούς της εφαρμογής, όπως Instagram, Facebook, LinkedIn.

#### **4.2.4 Αποκλειστικές Λειτουργικότητες του Διαχειριστή (root user)**

Ο διαχειριστής μοιράζεται τις ίδιες λειτουργικότητες με τον απλό χρήστη όσον αφορά την κύρια λειτουργικότητα πιστοποίησης εγγράφων, όπως και τις λειτουργικότητες ταξινόμησης, αναζήτησης, κατέβασμα και διαγραφή των εγγράφων που έχει αποθηκεύσει ο ίδιος. Πέρα όμως από αυτές τις βασικές λειτουργίες του έχουν ανατεθεί επιρόσθετες που τον βοηθούν να ανταπεξέλθει στον διαχειριστικό ρόλο που έχει.

*\*Περισσότερα για το business κομμάτι της εφαρμογής θα αναπτυχθούν αναλυτικότερα στο επόμενο κεφάλαιο*

- **Users Accounts**

Μέσα από την καρτέλα ο διαχειριστής έχει την δυνατότητα να προσθέσει κάποιο καινούργιο χρήστη. Για να το κάνει αυτό με το πάτημα του κουμπιού add new user κατευθύνεται σε μία νέα σελίδα, όπου του ζητείται να συμπληρώσει τα στοιχεία του νέου χρήστη: αυτά είναι το όνομα, το επίθετο, η διεύθυνση ηλεκτρονικού ταχυδρομείου, καθώς και ο κωδικός. Αυτά όλα τα στοιχεία ελέγχονται για την ορθότητά τους από το πρόγραμμα, όπως αντίστοιχα γίνεται και κατά την εγγραφή του χρήστη (registration). Σε περίπτωση που όλα τα στοιχεία που εισήγαγε ο διαχειριστής πληρούν τις προϋποθέσεις, εμφανίζεται μήνυμα επιτυχίας και προστίθεται κανονικά ο νέος χρήστης στην βάση δεδομένων. Διαφορετικά εμφανίζεται μήνυμα με το συγκεκριμένο λάθος, αδειάζει όλη η φόρμα και δίνεται στον διαχειριστή η ευκαιρία να συμπληρώσει ξανά τα στοιχεία του νέου χρήστη.

Στην ίδια καρτέλα ο διαχειριστής μπορεί να δει στοιχεία από όλους τους εγγεγραμμένους χρήστες της πλατφόρμας, καθώς και να τους ταξινομήσει σύμφωνα με το όνομά τους, το επίθετό τους και την διεύθυνση ηλεκτρονικού ταχυδρομείου.

Ακόμα, ο διαχειριστής έχει την δυνατότητα να ανανεώσει τα στοιχεία ενός συγκεκριμένου χρήστη, πατώντας στο κουμπί update, το οποίο τον κατευθύνει στην σελίδα ανανέωσης στοιχείων, εκεί πρέπει να συμπληρώσει τα νέα στοιχεία και αντίστοιχα με προηγούμενως γίνεται έλεγχος ορθότητας και ανανεώνονται τα δεδομένα του χρήστη.

Τέλος, ο διαχειριστής, εφόσον χρειαστεί μπορεί να διαγράψει κάποιον χρήστη από την βάση δεδομένων. Με το πάτημα του κουμπιού delete εμφανίζεται ένα μήνυμα στο χρήστη που ζητάει επιβεβαίωση για την ενέργειά του. Στην περίπτωση που ο διαχειριστής επιβεβαιώσει την διαγραφή ενός χρήστη, τότε ο χρήστης διαγράφεται από την βάση δεδομένων και μαζί του διαγράφονται και όλα τα δεδομένα τα οποία αποθήκευσε αυτός ο χρήστης (προσωπικά στοιχεία, αποθηκευμένα έγγραφα κ.α.).

- **Users Documents**

Εδώ ο διαχειριστής μπορεί να δει όλα τα αρχεία που αποθηκεύτηκαν από τους χρήστες της πλατφόρμας. Επίσης, μπορεί να ταξινομήσει αυτά τα έγγραφα βάσει του id τους, του χρήστη του οποίου τα αποθήκευσε, του ονόματος του αρχείου και τέλος της ημερομηνίας και της ώρας την οποία αποθηκεύτηκαν. Μέσω του κουτιού της αναζήτησης δίνεται η δυνατότητα στον διαχειριστή να ψάξει οποιαδήποτε λέξη ή αριθμό κλειδί θέλει ανάμεσα στα δεδομένα των αρχείων. Επιπρόσθετα, η λειτουργικότητα show entries διευκολύνει τον διαχειριστή, αφού του δίνει την δυνατότητα να επιλέξει πόσες καταχωρήσεις εγγράφων θέλει να βλέπει σε κάθε σελίδα.

Τέλος, προσθέσαμε και την επιλογή download για να κατεβάζει ο διαχειριστής τα αρχεία των χρηστών (\*αυτό συμβαίνει σε ειδικές περιπτώσεις που το σύστημα απευθύνεται σε πολυεθνικές εταιρείες και είναι σύστημα on-premise που αξιοποιείται και διαχειρίζεται έγγραφα της εταιρείας, διαφορετικά η ύπαρξη του κουμπιού θα αναιρούσε την χρήση του blockchain και θα παραβιάζαμε τα προσωπικά δεδομένα των χρηστών )

*\*Περαιτέρω για το business κομμάτι της εφαρμογής θα αναπτυχθούν αναλυτικότερα στο επόμενο κεφάλαιο*

## **4.3 Λειτουργικότητα για την πιστοποίηση εγγράφων**

### **4.3.1 Κύρια λειτουργικότητα στην εφαρμογή**

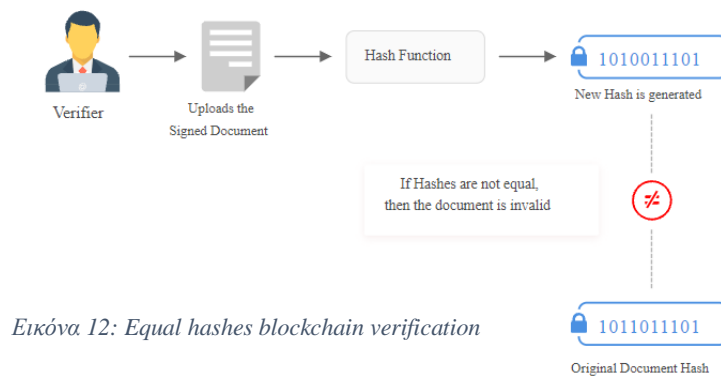
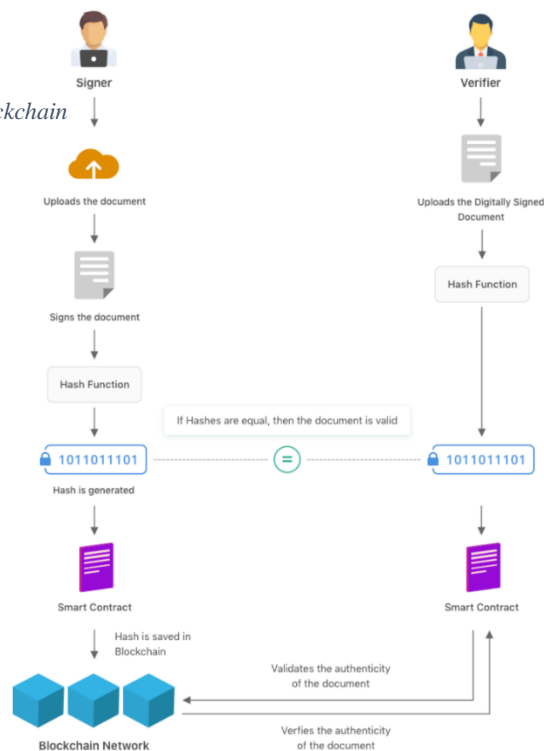
Η κύρια λειτουργικότητα της εφαρμογής μας είναι η πιστοποίηση εγγράφων που θα ανεβάζει ο χρήστης μέσω ενός Blockchain APIs. Αυτή την λειτουργικότητα την μοιράζονται όλες οι ομάδες χρηστών μας και ο απλός χρήστης- recruiter και διαχειριστής του συστήματος. Ο χρήστης αρχικά πρέπει να επιλέξει από το dropdown list πιο blockchain API θέλει να χρησιμοποιήσει. Η εφαρμογή μας προς το παρόν του δίνει 2 επιλογές με τις οποίες δουλέψαμε και προσπαθήσαμε να υλοποιήσουμε, αλλά μελλοντικά στόχος μας είναι να αποτελέσει σπίτι για μεγαλύτερο αριθμό APIs που βασίζονται στο blockchain. Αν διαλέξει το Qualichain ως το API που θα ήθελε να γίνει η πιστοποίηση, τότε εμφανίζονται 2 επιπρόσθετα πεδία για να συμπληρώσει το πεδίο IssuerId και το πεδίο CivilId, αφού συμπληρώσει αυτά ο χρήστης σωστά, τότε ανεβάζει και το έγγραφο που θα ήθελε να πιστοποιήσει. Η άλλη περίπτωση είναι να διαλέξει από το drop down list το πεδίο Blockcerts για να χρησιμοποιήσει αυτό το API για την πιστοποίηση του εγγράφου του. Σε αυτή την περίπτωση ο χρήστης θα πρέπει να ανεβάσει το json αρχείο που θα περιέχει το έγγραφο, καθώς και τα στοιχεία του εγγράφου που θα ήθελε να πιστοποιήσει. Όταν ολοκληρώσει τα παραπάνω βήματα, θα είναι έτοιμος να πατήσει το κουμπί verify. Αν το αρχείο του είναι γνήσιο, σε κάποιο από τα δυο APIs θα εμφανιστεί μήνυμα στην οθόνη του χρήστη που θα τον ενημερώνει για την γνησιότητα του εγγράφου και σε πιο Blockchain API βρέθηκε ακριβώς, έπειτα θα του δοθεί η επιλογή εάν θέλει να αποθηκεύσει το έγγραφο για να μπορεί να το βρει ευκολά αργότερα στην καρτέλα My Documents. Αν το έγγραφο δεν πιστοποιηθεί, τότε η εφαρμογή θα εμφανίσει μήνυμα

αποτυχίας, καθώς επίσης θα τον συμβουλευσει να αλλάξει την επιλογή του Blockchain API που θέλει να χρησιμοποιηθεί. Σε αυτή την περίπτωση το έγγραφο δεν μπορεί να αποθηκευτεί, αφού δεν έχει πιστοποιηθεί ως γνήσιο, γι' αυτό τον λόγο και η επιλογή αποθήκευσης του εγγράφου είναι κλειδωμένη.

### 4.3.2 Πως γίνεται η πιστοποίηση από τα blockchain APIs

Αφού το έγγραφο υπογραφεί από όλες τις οντότητες, δημιουργείται ένα hash στο blockchain. Κάθε χρήστης με το υπογεγραμμένο έγγραφο μπορεί να ελέγξει την αυθεντικότητα του εγγράφου στην πλατφόρμα. Οι χρήστες μπορούν να ανεβάσουν το υπογεγραμμένο έγγραφο στην πλατφόρμα. Εάν ο κατακερματισμός (hash) είναι ο ίδιος μετά τη μεταφόρτωση ενός υπογεγραμμένου εγγράφου με αυτόν του κατακερματισμού που δημιουργήθηκε κατά την υπογραφή, τότε το έγγραφο θα επικυρωθεί ως γνήσιο. Ουσιαστικά ο αλγόριθμος μας ελέγχει αν το hash του εγγράφου που θα ανεβάσει ο χρήστης είναι το ίδιο με το hash που υπάρχει στο blockchain API και δημιουργήθηκε κατά την υπογραφή του εγγράφου. Αν είναι ίδια, τότε το έγγραφο πιστοποιείται ως γνήσιο.[23][25]

Εικόνα 11: Διαδικασία πιστοποίησης στο blockchain



Εικόνα 12: Equal hashes blockchain verification

## 5. Ανάπτυξη της Εφαρμογής

### 5.1 Business Model

Πριν ξεκινήσουμε ακόμα την ανάπτυξη της εφαρμογής, είχαμε προτεραιότητα να θεσπίσουμε ένα business model, για να εργαστούμε μεθοδικά και με κάποιο στόχο. Έπρεπε πρωταρχικά να βρούμε σε ποιο πρόβλημα θα έδινε λύση η εφαρμογή μας και πόση αξία θα είχε για τον χρήστη. Έπειτα έπρεπε να καταλάβουμε σε τι κοινό απευθυνόμαστε και πιο συγκεκριμένα ποιες ομάδες χρηστών θα μπορούσαν να χρησιμοποιήσουν την εφαρμογή μας. Ακολούθως ερευνήσαμε ποιοι θα ήταν οι συνεργάτες μας σε αυτό το εγχείρημα, στην δική μας περίπτωση ποια blockchain APIs θα χρησιμοποιούσαμε. Τέλος, έπρεπε να λάβουμε υπόψη την αλληλεπίδραση με τον χρήστη και την εύκολη επεκτασιμότητα της εφαρμογής, για να είναι σε θέση να καλύψει μια μεγαλύτερη ομάδα χρηστών.[43]

#### 5.1.1 Πρόβλημα που καλούμαστε να λύσουμε

Το πρόβλημα που κληθήκαμε να λύσουμε ως developers είναι η πιστοποίηση της γνησιότητας εγγράφων γρήγορα και αποδοτικά. Ωστόσο, ο τρόπος με τον οποίο πραγματοποιείται μέχρι και σήμερα η επικύρωση, όσο και η διαχείριση εγγράφων, παρουσιάζει πολλά μειονεκτήματα. Τα κυριότερα αφορούν στη διάθεση των πιστοποιητικών σε μορφές εύαλωτες σε απώλεια, φθορά ή και καταδολίευση, στην εξάρτηση από τους ίδιους τους οργανισμούς ή τρίτους φορείς για την έκδοση και επικύρωσή τους αλλά και τις ίδιες τις χρονοβόρες διαδικασίες, όπως και την ύπαρξη κάποιου μεσάζοντα για την πιστοποίηση της γνησιότητας των εγγράφων από τους φορείς και τις αρμόδιες αρχές τις οποίες τα εξέδωσαν.

Στόχος της εφαρμογής μας είναι η αυτόματη επικύρωση εγγράφων γρήγορα και άκοπα μέσω blockchain APIs σε ένα περιβάλλον φιλικό και εύκολο στην χρήση του, χωρίς να προϋπάρχει κάποια γνώση σε πληροφοριακά συστήματα από τον χρήστη.

#### 5.1.2 Ομάδες Χρηστών

Η υλοποίηση της εφαρμογής μας εξυπηρετεί δυο κύριους χρήστες τον απλό χρήστη και τον διαχειριστή της πλατφόρμας. Αυτό το μοντέλο χρηστών που χρησιμοποιήσαμε καλύπτει αρκετά σενάρια του πραγματικού κόσμου και είναι πλήρως παραμετροποιήσιμο στις εκάστοτε ανάγκες του πελάτη.

- Εταιρική Χρήση (on-premises)

Η πρώτη περίπτωση χρήσης είναι η εταιρική, δηλαδή την πλατφόρμα και την εφαρμογή να την χρησιμοποιούν αυστηρά μόνο εταιρείες ή οργανισμοί για να εξυπηρετούν τις ανάγκες τους σε τοπικό επίπεδο με χρήση δικών τους servers. Σε αυτή την περίπτωση οι recruiters είναι οι απλοί χρήστες ως υπάλληλοι της εταιρείας και ο διαχειριστής μπορεί να θεωρηθεί ο επικεφαλής του τμήματος ανθρώπινου δυναμικού. Έτσι θα μπορεί να προσθέσει μαζικά πολλούς χρήστες στην πλατφόρμα που θα αντιπροσωπεύονται από τους recruiters της εταιρείας όπως επίσης θα δίνεται στην εταιρεία η ευκαιρία να έχει κάπου μαζεμένα όλα τα αρχεία που πιστοποιήθηκαν από τους recruiters και θα μπορεί να τα κατεβάζει.

- Online χρήση

Η δεύτερη περίπτωση χρήσης είναι αυτή που οι χρήστες δεν ανήκουν σε μια εταιρεία ή οργανισμό και η εφαρμογή είναι ευρέως προσβάσιμη από τον καθένα σε κάποια «cloud» υπηρεσία. Σε αυτή την περίπτωση ο απλός μας χρήστης μπορεί να είναι κάποιος ανεξάρτητος recruiter που θέλει να ελέγξει την γνησιότητα εγγράφων των υποψηφίων ή ακόμα και κάποιος απλός χρήστης που το μόνο που θέλει είναι να έχει μαζεμένους όλους τους πιστοποιημένους τίτλους σπουδών του. Έχοντας αυτό στο μυαλό είναι εύκολα αντιληπτό ότι ο διαχειριστής σαν εξωτερικός παράγοντας δεν πρέπει να έχει πρόσβαση στα προσωπικά στοιχεία των χρηστών, πόσο μάλλον στο να έχει την δύναμη να κατεβάσει τα πιστοποιημένα έγγραφα τους. Για αυτό οι λειτουργικότητες που παραβιάζουν τα προσωπικά δεδομένα του χρήστη, μπορούν εύκολα να απενεργοποιηθούν, όταν ισχύει αυτή η περίπτωση χρήσης.

### **5.1.3 Blockchain APIs**

Σημαντικής σημασίας ήταν η εύρεση APIS βασισμένα στο blockchain που θα μπορούσαν να χρησιμοποιηθούν στην εφαρμογή. Τελικά επιλέξαμε το Qualichain, το οποίο είναι ένα project συνεργασίας πολλών πανεπιστημίων, συμπεριλαμβανομένου και του Εθνικού Μετσόβιου Πολυτεχνείου, και το Blockcerts που είναι έργο ανοικτού κώδικα και χρησιμοποιείται από μεγάλα εκπαιδευτικά ιδρύματα, όπως το MIT. Κατά την προσπάθειά μας να εντοπίσουμε πιθανά APIS, που θα μπορούσαν να χρησιμοποιηθούν στην εφαρμογή, επικοινωνήσαμε με διάφορους οργανισμούς, ήρθαμε σε επαφή με κοινότητες σε διάφορα φόρουμ αλλά στείλαμε και προσωπικά μηνύματα σε ιδρυτές start-up που βασίζονται στο blockchain. Περισσότερα για τα blockchain APIs που χρησιμοποιήσαμε και προσεγγίσαμε θα βρείτε στο κεφάλαιο 3.

### **5.1.4 Αλληλεπίδραση και Επεκτασιμότητα**

Ένας άλλος σημαντικός στόχος κατά την ανάπτυξη της εφαρμογής ήταν να είναι φιλική και εύκολη στην χρήση για τον μέσο χρήστη. Έτσι λοιπόν χρησιμοποιήσαμε εργαλεία προσομοίωσης λειτουργικότητας των εφαρμογών, όπως το Adobe XD (mock-up tools) για την σχεδίαση διεπαφής χρήστη. Με αυτή μας την κίνηση πετύχαμε να προσομοιώσουμε την εφαρμογή πριν την υλοποιήσουμε και να εντοπίσουμε πιθανά λάθη και δυσκολίες στην χρήση από την πλευρά του χρήστη. Επιπρόσθετα, φροντίσαμε η εφαρμογή μετά την υλοποίησή της να είναι συμβατή με όλες τις ηλεκτρονικές συσκευές (smartphones, laptop, pc ,tablet), με απώτερο σκοπό να βελτιώσουμε την εμπειρία και την αλληλεπίδραση του χρήστη με αυτήν.

Σημαντικός πυλώνας για την επιτυχία μιας εφαρμογής που βασίζεται στο διαδίκτυο είναι το πόσο εύκολα επεκτάσιμη είναι, αν μπορεί να διαχειριστεί άμεσα βλάβες τους συστήματος και το αν είναι ευέλικτη. Για αυτό, λοιπόν, και εμείς προνοήσαμε και αναπτύξαμε την εφαρμογή μας με την βοήθεια cloud services, πιο συγκεκριμένα την βοήθεια του Azure Portal της Microsoft. Με αυτό πετύχαμε την εύκολη επεκτασιμότητα της εφαρμογής, αφού στο μέλλον στόχος είναι να φιλοξενεί μεγαλύτερο αριθμό blockchain API, στα οποία θα γίνεται η πιστοποίηση των εγγράφων. Συνεπακόλουθο αυτού είναι και ο μεγαλύτερος αριθμός χρηστών.

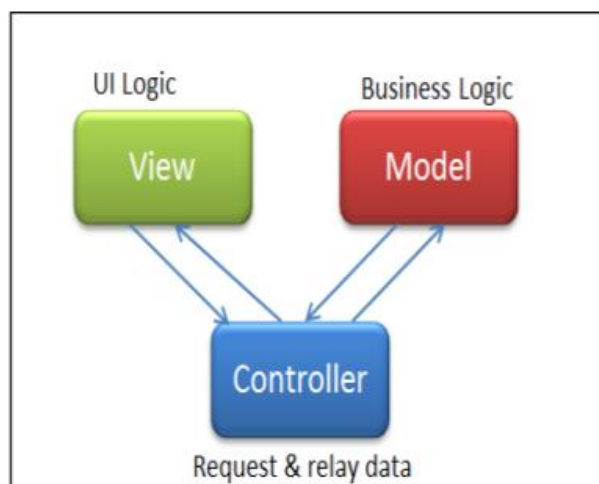
## 5.2 Αρχιτεκτονική

### 5.2.1 MVC framework

Γενικά, το λογισμικό εφαρμογών περιέχει κυρίως τρεις μεγάλες ενότητες, αυτές είναι η διεπαφή, η επιχειρησιακή λογική και τα δεδομένα. Στις παραδοσιακές εφαρμογές, οι συνδέσεις μεταξύ αυτών ήταν πολύ στενές, έτσι στα πρώτα χρόνια της ανάπτυξης λογισμικού, οι προγραμματιστές έπρεπε να γράψουν όλο τον κώδικα για την παραγωγή οποιασδήποτε εφαρμογής. Τώρα, η εμφάνιση του μοντέλου MVC, ήρθε για να λύσει το παραπάνω πρόβλημα.[31]

Το MVC (Model-View-Controller) είναι μια έννοια αρχιτεκτονικής λογισμικού, που θεωρείται ως αρχιτεκτονικό πρότυπο στη μηχανική λογισμικού. Αποτελείται από τρία συστατικά το Model, το View και τον Controller και διαχωρίζει την είσοδο της εφαρμογής, τη λογική της εκτέλεσης και την έξοδο, σύμφωνα με το Model, View και τον Controller. Το MVC έχει αποδείξει τα οφέλη του ειδικότερα στις διαδραστικές εφαρμογές, που επιτρέπουν πολλαπλές αναπαραστάσεις παρόμοιων πληροφοριών, προωθώντας την επαναχρησιμοποίηση κώδικα και βοηθώντας τους προγραμματιστές να εστιάσουν σε μια συγκεκριμένη λειτουργία εφαρμογής. Το MVC framework έχει γίνει ευρέως το πρότυπο για την σύγχρονη ανάπτυξη λογισμικού. Η κατάλληλη επαναχρησιμοποίηση κώδικα που εφαρμόζεται στο στρώμα μοντέλου, το επίπεδο προβολής και το επίπεδο ελέγχου που εφαρμόζεται μπορεί όχι μόνο να επιφέρει τον διαχωρισμό της υποκείμενης επιχειρησιακής λογικής, του ελέγχου διαδικασίας, και της προβολής, αλλά μπορεί επίσης να βελτιώσει σημαντικά την επεκτασιμότητα και τη δυνατότητα συντήρησης του λογισμικού, αφού η επαναχρησιμοποίηση κώδικα, είναι μια από τις πιο κοινές μορφές αντικειμενοστραφούς επαναχρησιμοποίησης. Κατά την ανάπτυξη μιας μονάδας λογισμικού, οι εσωτερικές ενότητες θα πρέπει να επαναχρησιμοποιηθούν όσο το δυνατόν περισσότερο, έτσι ώστε όχι μόνο να επιτευχθεί σημαντικά η ταχύτητα ανάπτυξης της εφαρμογής και να μειωθεί το κόστος της επένδυσης, αλλά μπορεί επίσης να βελτιώσει την ποιότητα του συστήματος, για να διευκολύνει τον εντοπισμό και την αντιμετώπιση προβλημάτων στο στάδιο της δοκιμής-ελέγχου.[44]

Σε ένα framework MVC, η προβολή και ο ελεγκτής ανήκουν στη διεπαφή χρήστη. Στην αρχή, ο χρήστης στέλνει ένα αίτημα σε έναν ελεγκτή μέσω μιας γραφικής διεπαφής χρήστη (GUI). Στη συνέχεια, το μοντέλο πρόσβασης του ελεγκτή δίνει τα δεδομένα, σύμφωνα με το αίτημα του χρήστη. Μετά από αυτό, το μοντέλο επιστρέφει τα δεδομένα στον ελεγκτή και ο ελεγκτής παρουσιάζει τα δεδομένα μέσω της καθορισμένης προβολής.[45] Χρησιμοποιούμε επίσης βάση δεδομένων για την αποθήκευση δεδομένων και την παροχή αρχικής προέλευσης δεδομένων στο σύστημά μας.



Εικόνα 13: MVC model



Συνοψίζουμε, λοιπόν, με τα ακόλουθα στοιχεία:

- **Model:** Το μοντέλο αντιπροσωπεύει ένα αντικείμενο (object) ή δεδομένα που μεταφέρονται στην Java. Μπορεί επίσης να έχει λογική ενημέρωσης του ελεγκτή εάν αλλάζουν τα δεδομένα του.
- **View:** Η προβολή αντιπροσωπεύει την οπτικοποίηση των δεδομένων που περιέχει το μοντέλο.
- **Controller:** Ο ελεγκτής λειτουργεί τόσο στο μοντέλο όσο και στην προβολή. Ελέγχει τη ροή δεδομένων στο αντικείμενο μοντέλου και ενημερώνει την προβολή κάθε φορά που αλλάζουν δεδομένα. Διατηρεί το View και το Model ξεχωριστά.

### 5.2.2 Σχεδιασμός και Υλοποίηση

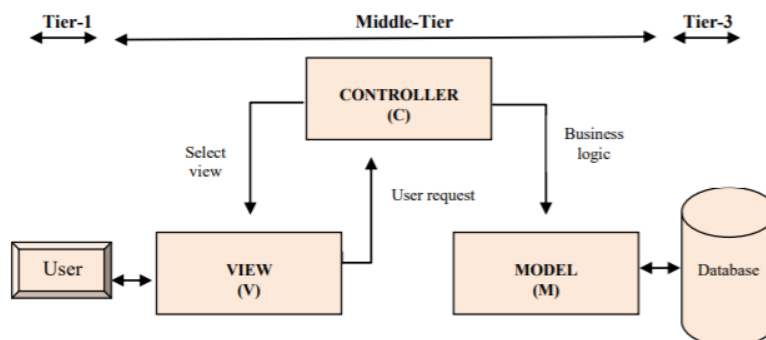
Σε αυτήν την ενότητα, εξηγούμε εν συντομία την αρχιτεκτονική σχεδιασμού και τη λειτουργία του μοντέλου. Πρόκειται για ένα πλαίσιο τριών επιπέδων που οργανώνεται σε τρία μεγάλα μέρη. Τα τρία μέρη είναι:

- Χρήστες
- MVC components
- Βάση Δεδομένων

Η πρώτη βαθμίδα αποτελείται μόνο από χρήστες. Ο χρήστης μπορεί να στείλει αίτημα και να λάβει απάντηση από τα στοιχεία της "Προβολή" της μεσαίας βαθμίδας. Δεύτερον, η μεσαία βαθμίδα αποτελείται από το MVC. Αυτά τα στοιχεία μπορούν να επικοινωνούν και να επεξεργάζονται μεταξύ τους. Τέλος, η τρίτη βαθμίδα περιέχει μόνο μια βάση δεδομένων όπου τα δεδομένα αποθηκεύονται μόνιμα.

Οι λειτουργίες περιγράφονται στα ακόλουθα βήματα:

- Η είσοδος του χρήστη γίνεται αποδεκτή από το στοιχείο "Προβολή" μέσω γραφικού περιβάλλοντος χρήστη (GUI). Οι αλληλεπιδράσεις μεταξύ του χρήστη και της διεπαφής γίνονται με πάτημα κουμπιών, ανέβασμα αρχείων και συμπλήρωση κειμένου.
- Ο "Ελεγκτής" επεξεργάζεται τα αιτήματα των χρηστών. Με βάση το αίτημα χρήστη, ο ελεγκτής καλεί μεθόδους στην προβολή και το μοντέλο για να πραγματοποιήσει την απαιτούμενη ενέργεια. Ένας καθαρός ελεγκτής GUI δέχεται την είσοδο από το χρήστη και δίνει εντολή στο μοντέλο και στο παράθυρο προβολής να εκτελέσουν ενέργειες με βάση αυτήν την είσοδο. Ο ελεγκτής προσαρμόζει το αίτημα στο μοντέλο. Το μοντέλο αντιπροσωπεύει ή ενσωματώνει την επιχειρησιακή λογική ή κατάσταση μιας εφαρμογής.
- Η προβολή είναι υπεύθυνη για την έξοδο του μοντέλου. Μια καθαρή προβολή GUI προσαρτάται σε ένα μοντέλο και αποδίδει τα περιεχόμενά του στην επιφάνεια της οθόνης.

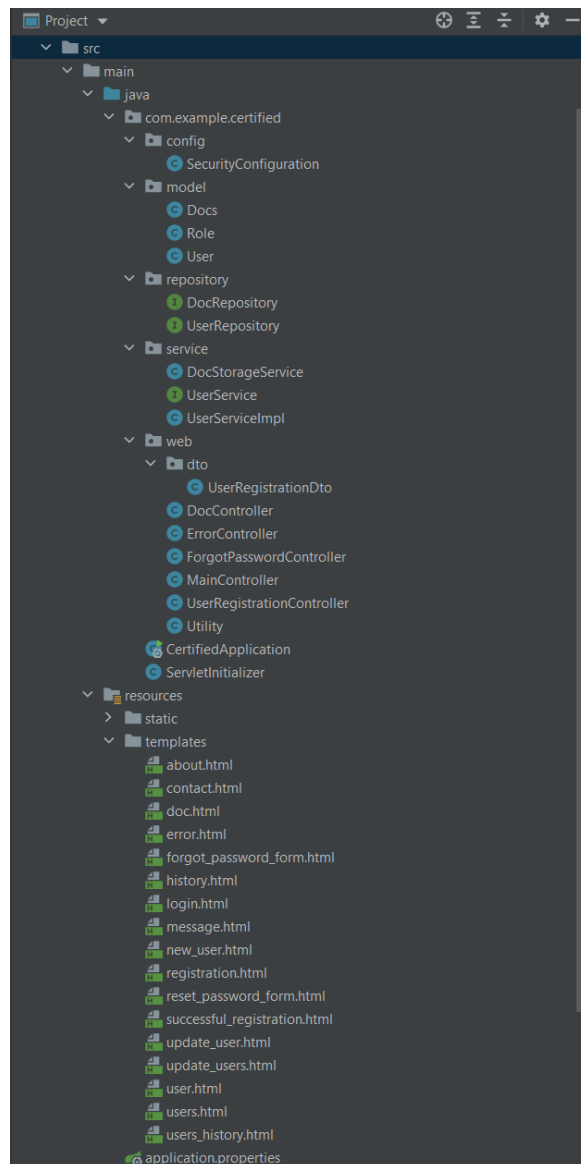


Εικόνα 14: How MVC works

### 5.2.3 Δέντρο Κλάσεων

Παρακάτω βλέπουμε το δέντρο κλάσεων της εφαρμογής μας. Είναι ομαδοποιημένο ανά πακέτα τα οποία χωρίζουν τις κλάσεις ανάλογα με την λειτουργία τους σύμφωνα με το μοντέλο MVC αρχιτεκτονικής. Αρχικά έχουμε την κλάση SecurityConfiguration (στο πακέτο config) όπου ρυθμίζει ό,τι έχει σχέση με την ασφάλεια της εφαρμογής (login,register κλπ.) . Έπειτα έχουμε το πακέτο model που περιέχει τις κλάσεις για το πέρασμα όλων των πεδίων των μοντέλων του χρήστη, του ρόλου του χρήστη και των εγγράφων. Επόμενο στην σειρά είναι το πακέτο repository που περιέχει κλάσεις για την διαχείριση των στοιχείων των μοντέλων της εφαρμογής. Ακολούθως βλέπουμε το πακέτο service που φιλοξενεί όλες τις κλάσεις που έχουν να κάνουν με τις υπηρεσίες και τις λειτουργικότητες τις εφαρμογής μας. Κάποιες από αυτές είναι η αποθήκευση δεδομένων , η εγγραφή χρήστη, η ταξινόμηση λιστών κ.α. Τέλος στο Java κομμάτι του δέντρου βρίσκουμε το πακέτο web που περιέχει όλες τις κλάσεις που λειτουργούν σαν controllers, και διαχειρίζονται τα διάφορα end-points της εφαρμογής.

Κάτω από την κατηγορία resources θα βρούμε το πακέτο static που αποτελείται από όλα τα βοηθητικά αρχεία JavaScript και CSS που υποστηρίζουν τα κύρια templates μας. Και στο πακέτο templates βρίσκονται όλες οι επιμέρους html σελίδες της εφαρμογής.



Εικόνα 15: Application code diagram

#### 5.2.4 Σχεσιακό διάγραμμα οντοτήτων

Για την δημιουργία της βάσης αρχικά έπρεπε να φτιάξουμε ένα scheme στο MySQL Workbench που αυτό με την σειρά του θα γέμιζε αυτόματα με τα παρακάτω πεδία και σχέσεις μεταξύ των οντοτήτων, χάρη στο εργαλείο JPA hibernate που φτιάχνει τους πίνακες, σύμφωνα με τα μοντέλα των κλάσεων που αναπτύξαμε στον κώδικά μας.

Στην βάση μας έχουμε έναν πίνακα που αποθηκεύουμε τα προσωπικά στοιχεία των χρηστών (όνομα, επίθετο, κωδικό,email). Ο κωδικός αποθηκεύεται σε κρυπτογραφημένη μορφή για την ασφάλεια των δεδομένων και ένα πεδίο που εκεί αποθηκεύεται το κατακερματισμένο token του χρήστη το οποίο χρησιμεύει για την ανάκτηση του κωδικού πρόσβασης. Επίσης, υπάρχουν και οι πίνακες roles και user\_roles για τον καθορισμό του ρόλου του κάθε χρήστη (απλός χρήστης ή διαχειριστής)

Τέλος, έχουμε και τον πίνακα με τα έγγραφα των χρηστών που αποθηκεύει τα αναγνωριστικά στοιχεία των εγγράφων, καθώς και τον χρήστη του οποίου βρίσκεται στην κατοχή το κάθε έγγραφο.



Εικόνα 16: Database Entity-Relations diagram

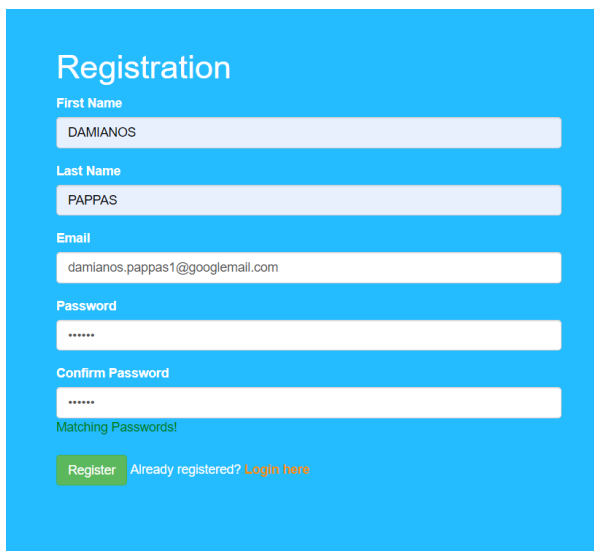
## 5.3 Guide how to use the web-app

Παρακάτω θα αναλύσουμε το πώς δουλεύει η εφαρμογή και θα δούμε τις λειτουργικότητες που εξηγήσαμε στο προηγούμενο πως αντικατοπτρίζονται στην διεπαφή χρήστη. Θα χωρίσουμε τις λειτουργικότητες της κάθε ομάδας χρηστών.

### 5.3.1 Χρήστης

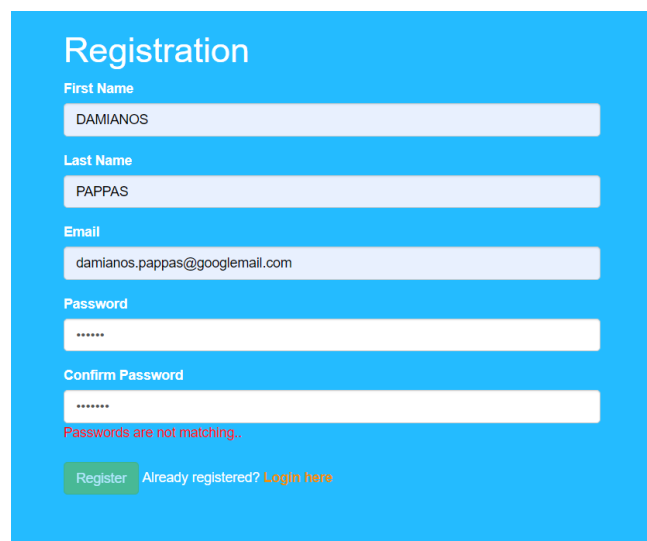
#### 5.3.1.1 Register

Ο απλός χρήστης μπορεί να εγγραφεί στην εφαρμογή, δηλώνοντας σωστά τα προσωπικά του στοιχεία. Αν οι κωδικοί που συμπληρώσει ο χρήστης δεν συμπίπτουν, τότε η εφαρμογή τον ενημερώνει, όπως επίσης και όταν πληκτρολογήσει λάθος μορφής στοιχεία. Πιο συγκεκριμένα, διεύθυνση email λάθος που να μην είναι έγκυρη ή όνομα και επίθετο μικρότερο των 2 χαρακτήρων.



The screenshot shows a registration form on a blue background. The form has the following fields: First Name (DAMIANOS), Last Name (PAPPAS), Email (damianos.pappas1@googlemail.com), Password (masked with dots), and Confirm Password (masked with dots). Below the Confirm Password field, there is a green message: "Matching Passwords!". At the bottom, there is a green "Register" button, a link "Already registered? Login here", and a "Back to Login" button.

Εικόνα 17: Register(matching passwords)



The screenshot shows the same registration form as in Figure 17, but with a red error message: "Passwords are not matching..". The "Register" button is disabled, and the "Back to Login" button is visible.

Εικόνα 18: Register (password does not match)

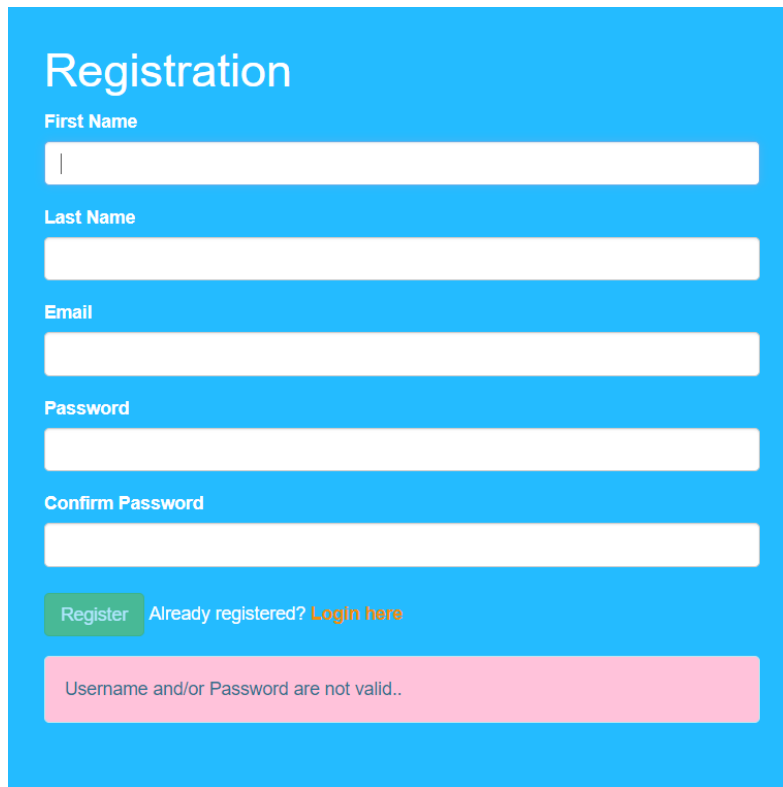
Αν συμπληρώσει τα παραπάνω πεδία σωστά τότε θα γίνει επιτυχής εγγραφή και θα του δοθεί η επιλογή να επιστρέψει στην σελίδα του login για να συνδεθεί στον νέο του λογαριασμό.



The screenshot shows a green success message: "Success! You've successfully registered!". Below the message is a blue "Back to Login" button.

Εικόνα 19: Successful Registration

Σε διαφορετική περίπτωση, αν δηλαδή ο χρήστης συμπληρώσει email που υπάρχει ήδη, παίρνει την ακόλουθη απάντηση και αδειάζει η φόρμα, δίνοντάς του την ευκαιρία να προσπαθήσει ξανά.

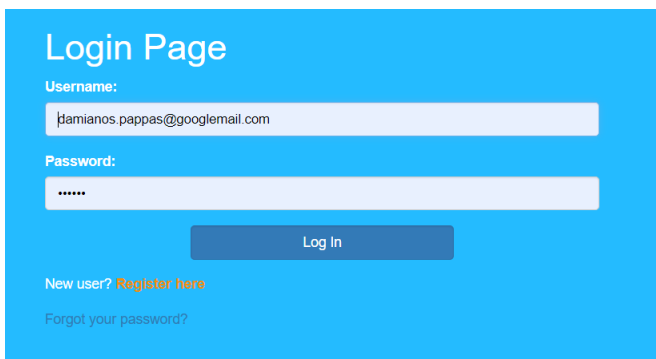


The image shows a registration form on a blue background. The form has five input fields: 'First Name', 'Last Name', 'Email', 'Password', and 'Confirm Password'. Below the fields is a green 'Register' button and a link 'Already registered? Login here'. At the bottom, a pink error message box displays the text 'Username and/or Password are not valid..'.

Εικόνα 20: Fail to Register

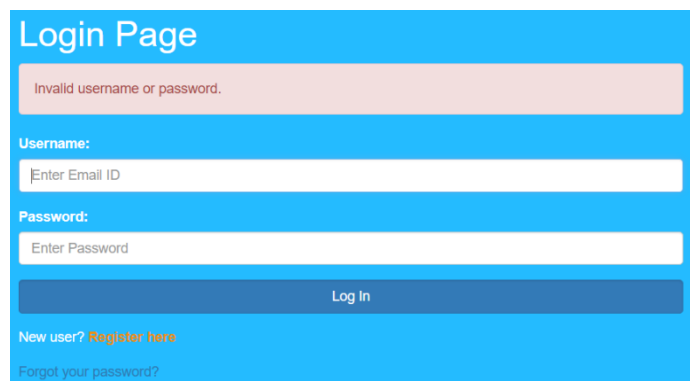
### 5.3.1.2 Login

Όταν ο χρήστης εγγραφεί, θα έχει το δικαίωμα να συνδεθεί στην εφαρμογή. Αν πληκτρολογήσει λάθος κωδικό ή email, θα του εμφανιστεί μήνυμα αποτυχίας.



The image shows a login page on a blue background. It has two input fields: 'Username:' with the value 'jamianos.pappas@googlemail.com' and 'Password:' with masked characters '.....'. Below the fields is a dark blue 'Log In' button. At the bottom, there are links for 'New user? Register here' and 'Forgot your password?'.

Εικόνα 21: Login(user)

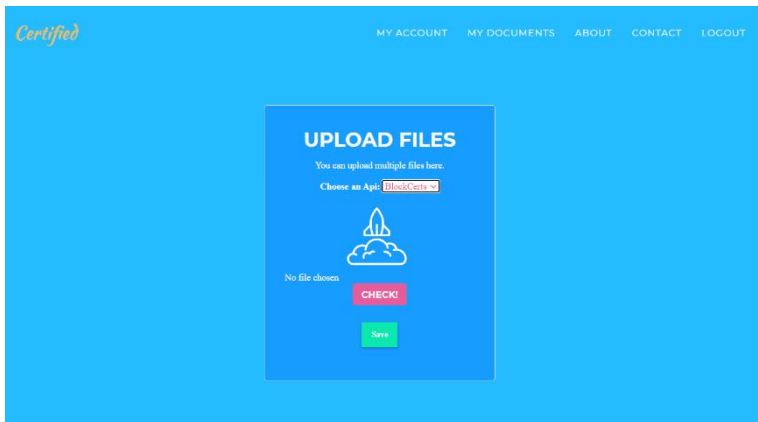


The image shows a login page on a blue background. At the top, a light pink error message box displays the text 'Invalid username or password.'. Below this are two input fields: 'Username:' with the placeholder 'Enter Email ID' and 'Password:' with the placeholder 'Enter Password'. Below the fields is a dark blue 'Log In' button. At the bottom, there are links for 'New user? Register here' and 'Forgot your password?'.

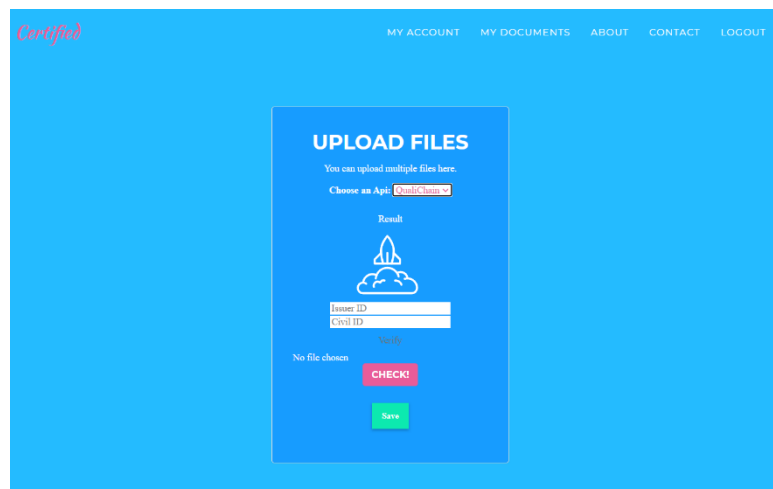
Εικόνα 22: Fail to Login

### 5.3.1.3 Main

Όταν ο χρήστης συνδεθεί θα αντικρίσει πρώτα την κύρια σελίδα που του δίνει την επιλογή να διαλέξει ποιο API θέλει να χρησιμοποιήσει για την επικύρωση των εγγράφων του.

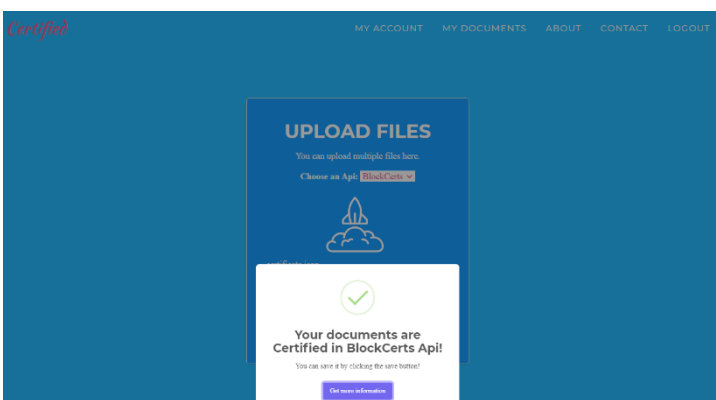


Εικόνα 23: User main page (Blockcerts)

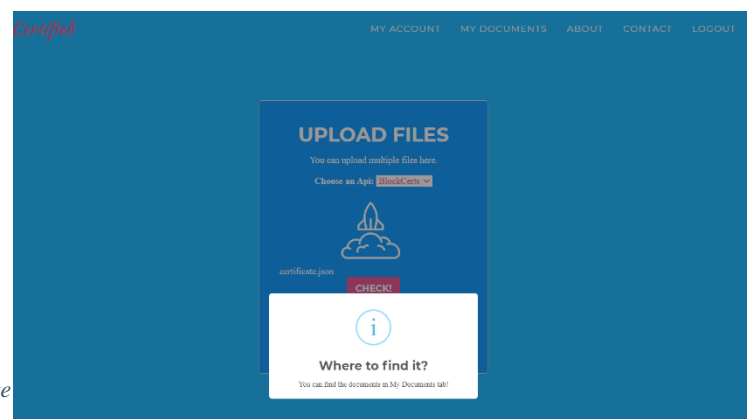


Εικόνα 24: User main page (Qualichain)

Αν το έγγραφο είναι γνήσιο του εμφανίζεται το ανάλογο μήνυμα και η δυνατότητα να το αποθηκεύσει.

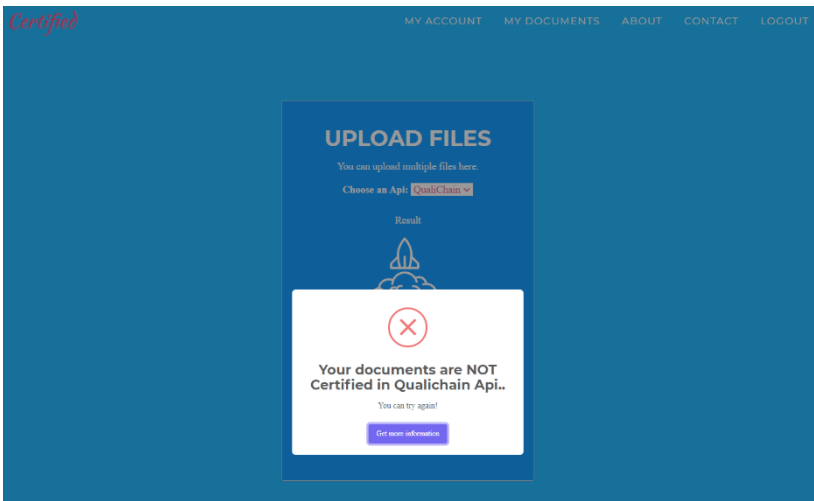


Εικόνα 25: Verified Successful in Blockcerts

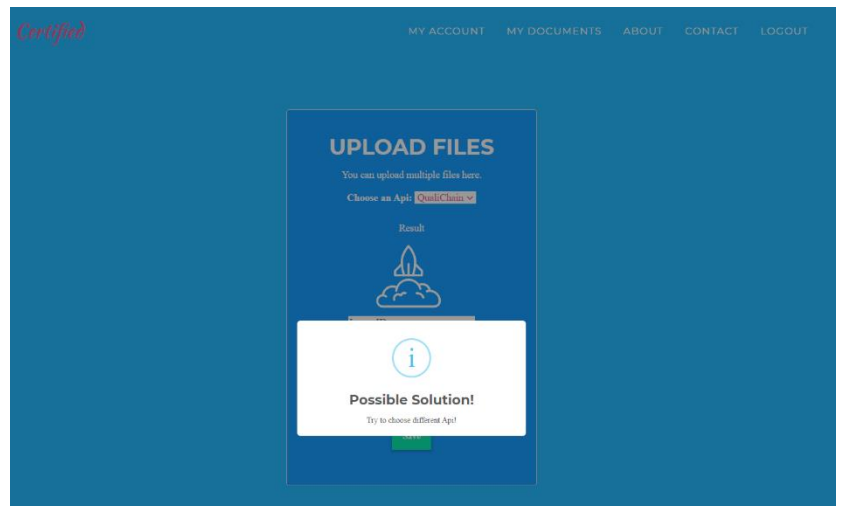


Εικόνα 26: Successful information message

Αν το έγγραφο δεν είναι γνήσιο του εμφανίζεται μήνυμα που διευκρινίζει σε ποιο API έγινε η αναζήτηση και τον συμβουλεύει να αλλάξει την επιλογή του API.



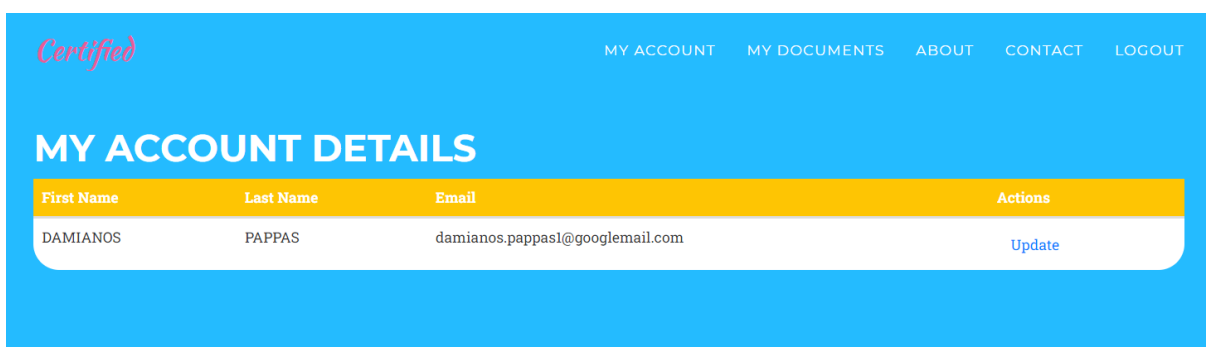
Εικόνα 27: Verification Faillure



Εικόνα 28: verification Faillure (information message)

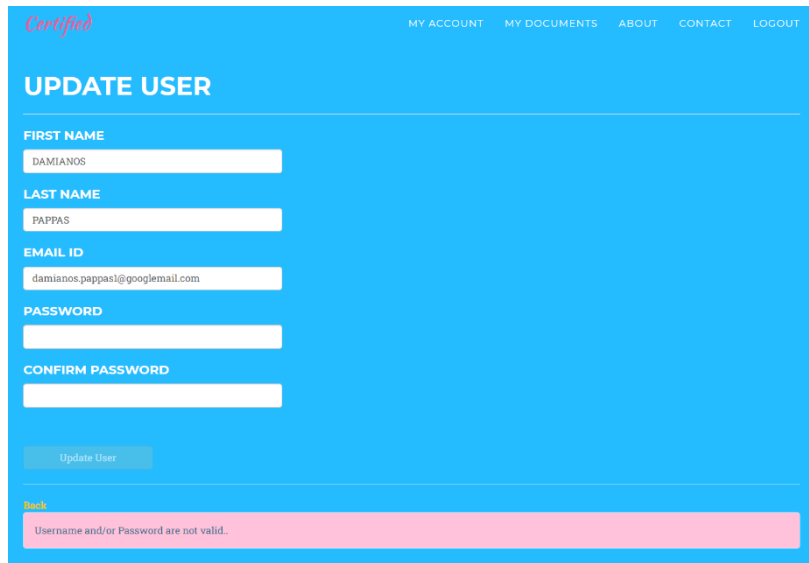
#### 5.3.1.4 My Account

Ο χρήστης σε αυτή την καρτέλα έχει την δυνατότητα να δει στοιχεία του λογαριασμού του, καθώς και να ενημερώσει κάποια από αυτά, αν το επιθυμεί φυσικά και ο ίδιος.



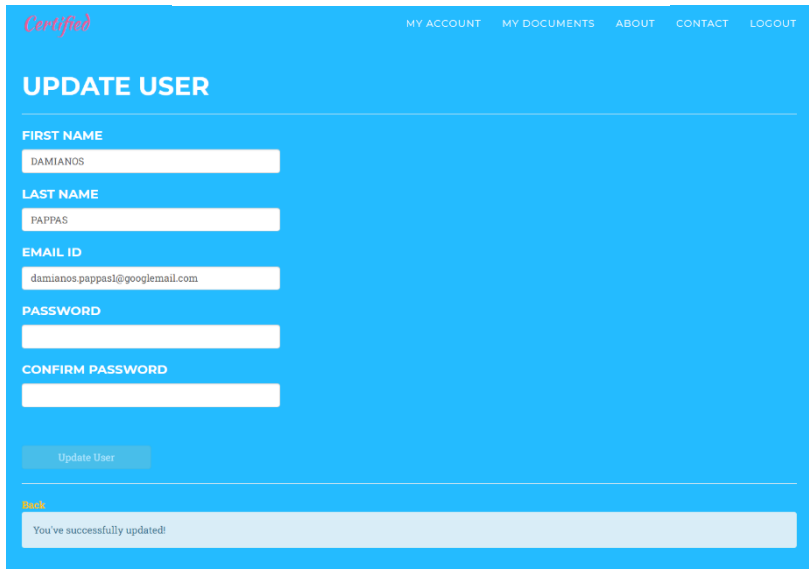
Εικόνα 29: My Account (user)

Αν κατά την ενημέρωση τα στοιχεία που θα συμπληρώσει είναι σωστά, θα λάβει επιτυχές μήνυμα και θα ενημερωθούν αυτόματα, αλλιώς θα αδειάσει η φόρμα και θα λάβει μήνυμα αποτυχίας.



The screenshot shows the 'UPDATE USER' form with the following fields filled: FIRST NAME (DAMIANOS), LAST NAME (PAPPAS), EMAIL ID (damianos.pappas1@googlemail.com), and two empty password fields. A red error message at the bottom states: 'Username and/or Password are not valid.'

Εικόνα 30: Update User Credentials failure

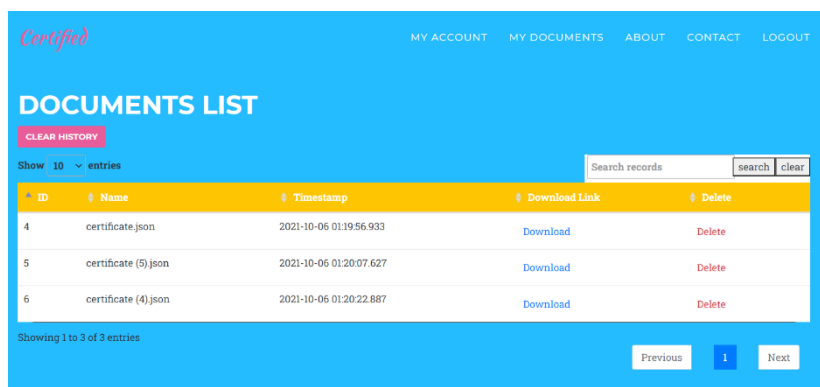


The screenshot shows the 'UPDATE USER' form with the same fields as in the previous image. A green success message at the bottom states: 'You've successfully updated!'

Εικόνα 31: Successful Update User Credentials

### 5.3.1.5 My Documents

Σε αυτή την καρτέλα ο χρήστης έχει την δυνατότητα να δει, να ταξινομήσει, να αναζητήσει τα έγγραφα που ο ίδιος έχει επικυρώσει και αποθηκεύσει, όπως επίσης να τα κατεβάσει τοπικά στην συσκευή του, καθώς και να διαγράψει ένα ή και όλα τα έγγραφα μαζί.



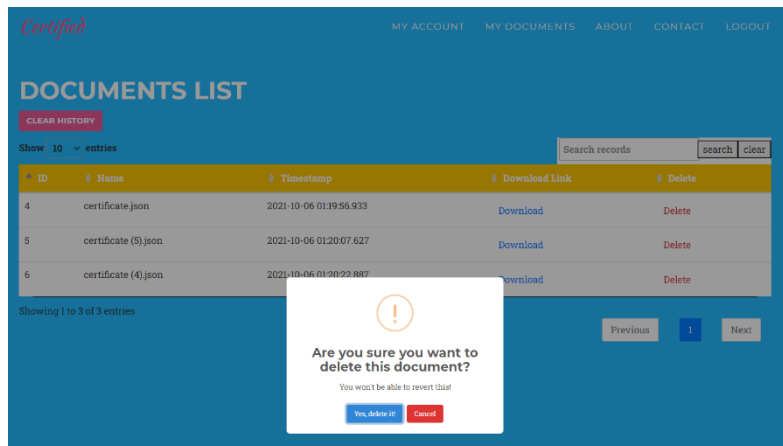
The screenshot shows the 'DOCUMENTS LIST' page with a table of documents. The table has columns for ID, Name, Timestamp, Download Link, and Delete. There are three rows of data.

ID	Name	Timestamp	Download Link	Delete
4	certificate.json	2021-10-06 01:19:56.933	<a href="#">Download</a>	<a href="#">Delete</a>
5	certificate (5).json	2021-10-06 01:20:07.627	<a href="#">Download</a>	<a href="#">Delete</a>
6	certificate (4).json	2021-10-06 01:20:22.887	<a href="#">Download</a>	<a href="#">Delete</a>

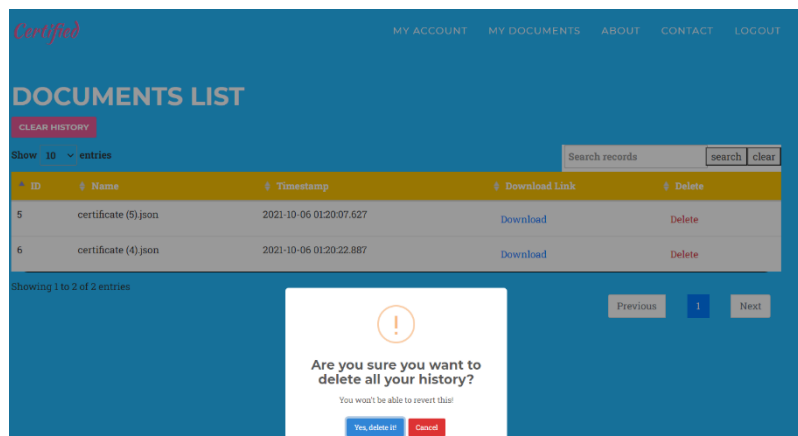
Εικόνα 32: My Documents(user)



Αν ο χρήστης θελήσει να διαγράψει κάποιο έγγραφο ή να καθαρίσει ολόκληρο το ιστορικό του, του εμφανίζεται μήνυμα επιβεβαίωσης πριν να εκτελεστεί η λειτουργικότητα για πιθανή αποφυγή λάθους.



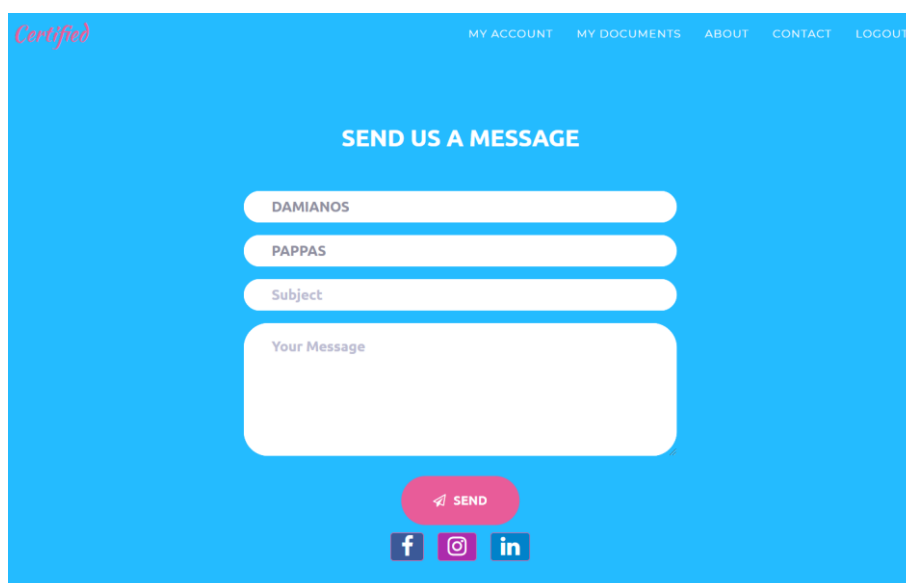
Εικόνα 33: Confirmation message for deleting document



Εικόνα 34: Confirmation message for clear all history

### 5.3.1.6 Contact

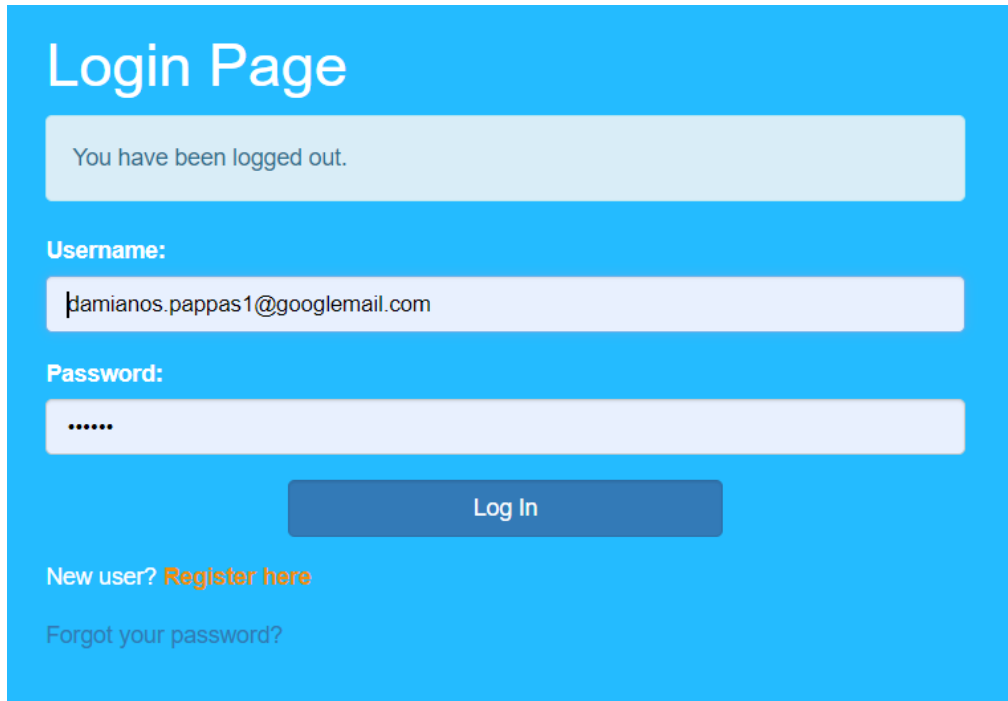
Δίνουμε την δυνατότητα ο χρήστης να έρθει σε επαφή με εμάς για οτιδήποτε τον προβληματίζει μέσω email, Instagram, Facebook και LinkedIn με την βοήθεια της καρτέλας contact.



Εικόνα 35: Contact tab

### 5.3.1.7 Logout

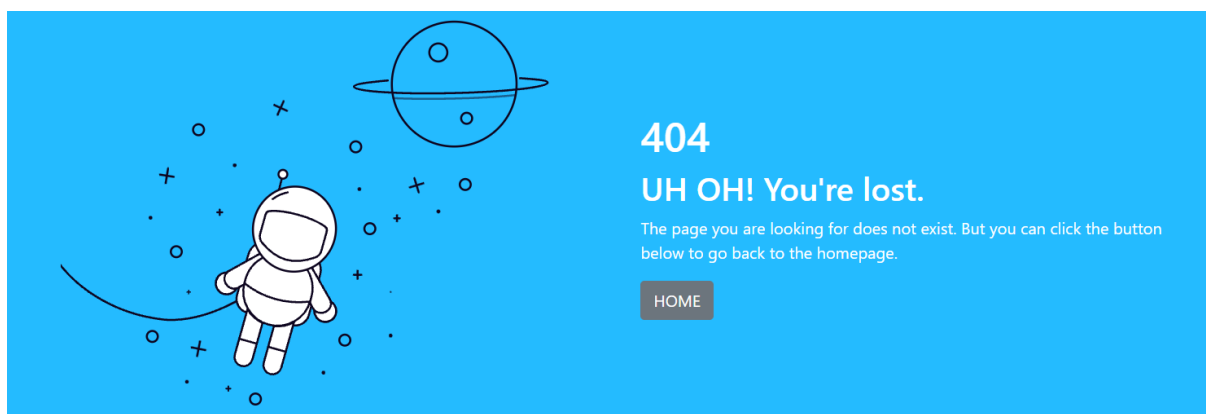
Όταν αποσυνδεθεί ο χρήστης από την εφαρμογή, το spring security διαγράφει το session του και του εμφανίζεται μήνυμα επιτυχίας αποσύνδεσης.



Εικόνα 36: Logout message

### 5.3.1.8 Error Page

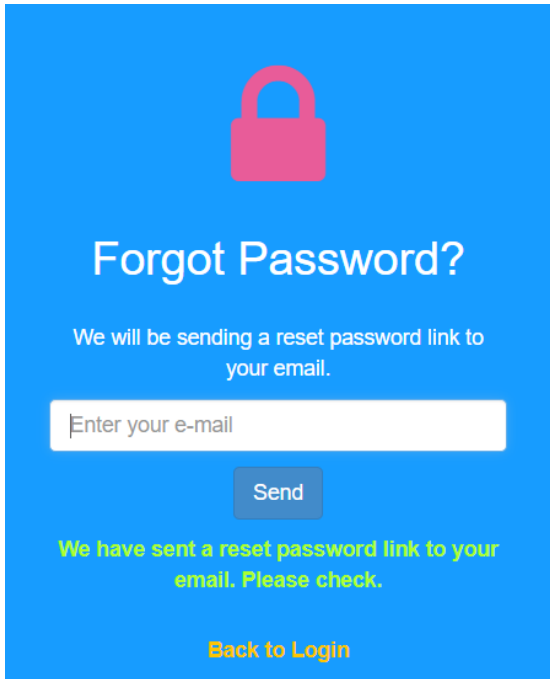
Αν κάποιος χρήστης προσπαθήσει να μεταβεί σε endpoint που δεν είναι διαθέσιμο στην εφαρμογή μας τότε ο controller διαχειρίζεται την ενέργεια του ως λάθος και του επιστρέφει συγκεκριμένο view που φτιάξαμε για τα λάθη.



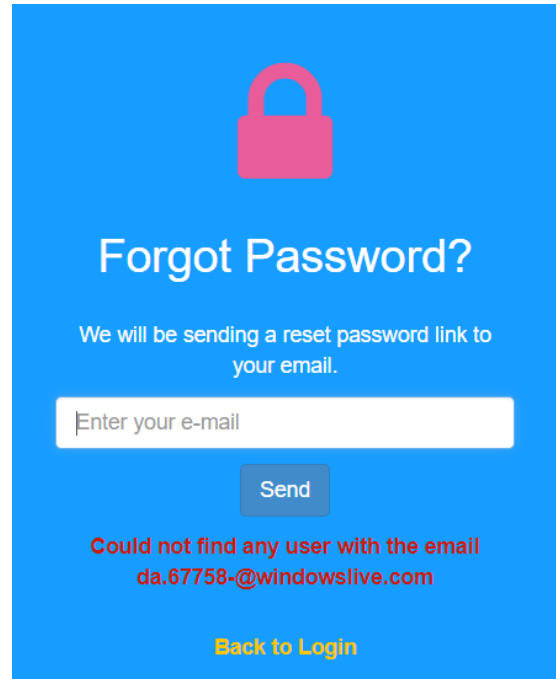
Εικόνα 37: Error page

### 5.3.1.9 Forgot my Password

Σε περίπτωση που κάποιος χρήστης ξεχάσει τον κωδικό του έχει την επιλογή να τον επανακτήσει συμπληρώνοντας στην φόρμα το email με το οποίο είναι εγγεγραμμένος στην εφαρμογή. Αν συμπληρώσει το σωστό email υπάρχει στην βάση τότε του αποστέλλεται στην διεύθυνση αυτή url ανάκτησης του κωδικού του διαφορετικά εμφανίζεται μήνυμα αδυναμίας εύρεσης του χρήστη, αδειάζει η φόρμα και έχει την δυνατότητα να την συμπληρώσει ξανά.

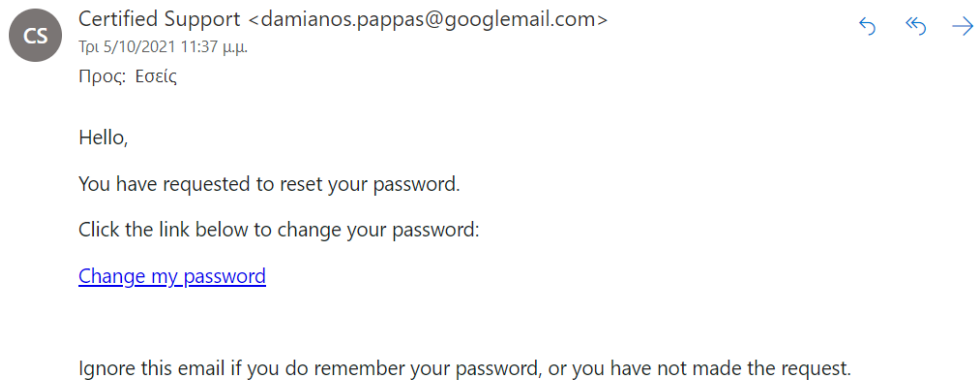


Εικόνα 39: Message sent for resetting password



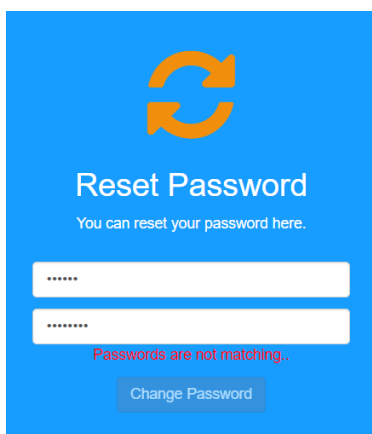
Εικόνα 38: Fail to send email for resetting password

Αν ο χρήστης ακολούθησε σωστά τα βήματα μέχρι εδώ, θα έχει λάβει στο email του ένα αντίστοιχο μήνυμα με το παρακάτω που περιέχει το url με το token του χρήστη.

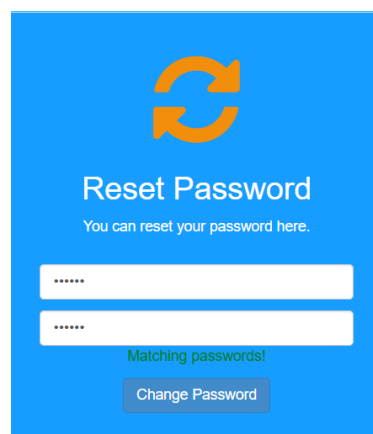


Εικόνα 40: Reset Password email

Ακολουθώντας το url θα μπορεί να αλλάξει τον κωδικό του εφόσον τον επιβεβαιώσει επιτυχημένα.

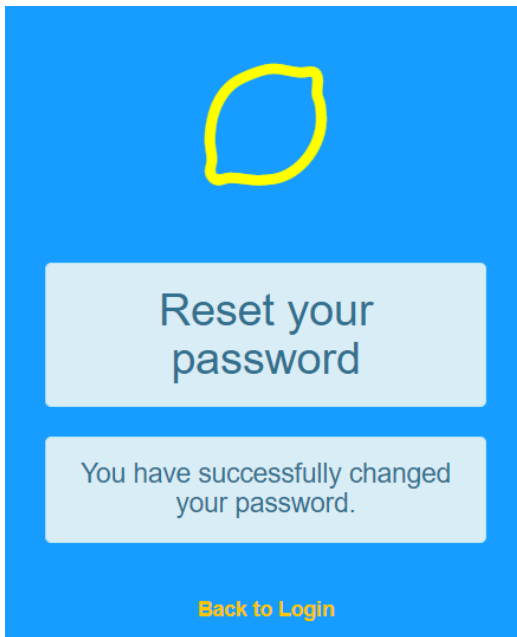


Εικόνα 42: Reset passwords(not matching)

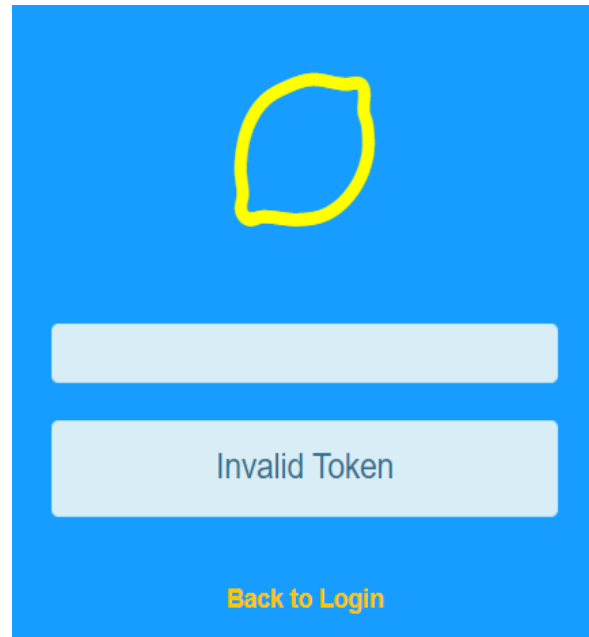


Εικόνα 41: Reset passwords(matching)

Εφόσον το url που του έχει σταλεί δεν έχει λήξει(ισχύει μέχρι και 2 ώρες) ή δεν έχει χρησιμοποιηθεί τότε έχει την δυνατότητα να αλλάξει τον κωδικό με επιτυχία, αλλιώς του εμφανίζεται μήνυμα πως το token του χρήστη δεν είναι έγκυρο.



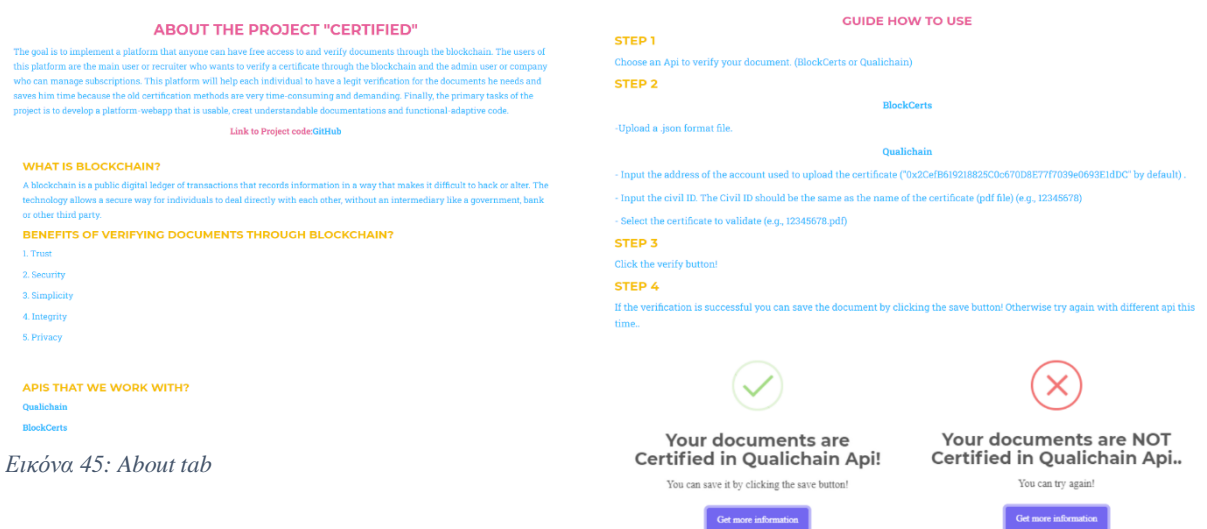
Εικόνα 43: Password reset successfully



Εικόνα 44: Invalid URL token message

### 5.3.1.10 About

Σε αυτή την καρτέλα ο χρήστης μπορεί να βρει πληροφορίες για όλη την εργασία, links στα APIs που χρησιμοποιήθηκαν καθώς και το link του repository του κώδικα στο Github. Επίσης σε αυτή την σελίδα υπάρχουν οδηγίες για την χρήση της εφαρμογής



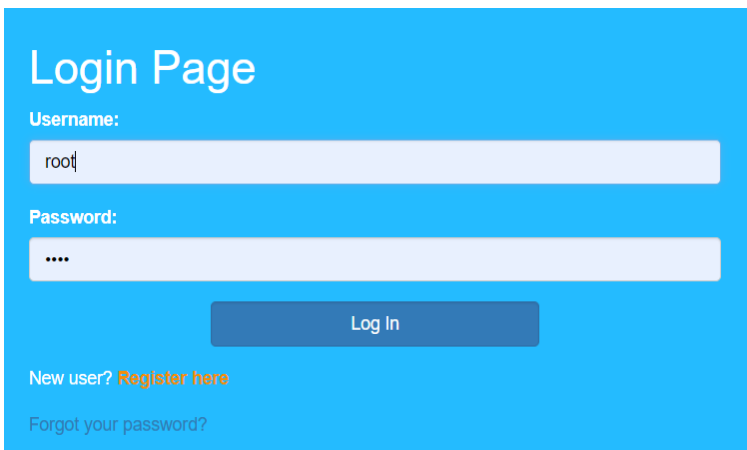
Εικόνα 45: About tab

### 5.3.2 Διαχειριστής (root user)

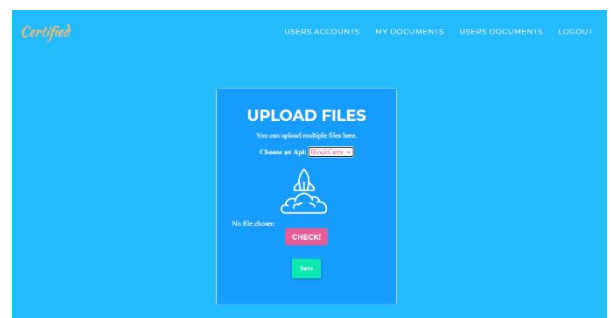
Ο Διαχειριστής της εφαρμογής έχει κάποιες μοναδικές λειτουργικότητες πέραν από τις κοινές με τον απλό χρήστη (My Documents, Main, My Account). Σε αυτές συμπεριλαμβάνεται η διαχείριση χρηστών μέσω του Users Accounts και η πρόσβαση σε αποθηκευμένα έγγραφα.

#### 5.3.2.1 Login/Main

Ο διαχειριστής συνδέεται στην εφαρμογή με διαφορετικά στοιχεία από τους υπόλοιπους χρήστες που δεν ακολουθούν την μορφή του μοντέλου του χρήστη και έχει την ίδια κύρια λειτουργικότητα με τον απλό χρήστη. Ο διαχειριστής δεν έχει την έγκριση για οποιαδήποτε αλλαγή των στοιχείων σύνδεσης του.



Εικόνα 46: Login (root user)



Εικόνα 47: Main page (root user)

#### 5.3.2.2 Users Accounts

Εδώ δίνεται η δυνατότητα στον διαχειριστή να ταξινομήσει τους χρήστες βάση των στοιχείων τους να διαγράψει, να προσθέσει η ακόμα και να ενημερώσει τα στοιχεία κάποιου χρήστη.

User First Name	User Last Name	User Email	Actions
charalampos	rossidis	xrossides@gmail.com	<a href="#">Update</a> <a href="#">Delete</a>
Chris	PAPPAS	A@gmail.com	<a href="#">Update</a> <a href="#">Delete</a>
Christos	Pappas	damianos.pappas@gmail	<a href="#">Update</a> <a href="#">Delete</a>
DAMIANOS	PAPPAS	damianos.pappas@goolemail.com	<a href="#">Update</a> <a href="#">Delete</a>
DAMIANOS	PAPPAS	da.67-@windowslive.com	<a href="#">Update</a> <a href="#">Delete</a>
DAMIANOS	PAPPAS	damianos.pappas1@goolemail.com	<a href="#">Update</a> <a href="#">Delete</a>
root	root	root	<a href="#">Update</a> <a href="#">Delete</a>
Sang	Sou	artsias@gmail.com	<a href="#">Update</a> <a href="#">Delete</a>
Yiota	Pappa	yiotapappa@gmail.com	<a href="#">Update</a> <a href="#">Delete</a>

Εικόνα 48: All Users page (root)

Για την λειτουργικότητα προσθήκης νέου χρήστη ο διαχειριστής πρέπει να συμπληρώσει σωστά τα πεδία με τα στοιχεία του χρήστη που θα ήθελε να προσθέσει, αλλιώς θα το εμφανιστεί μήνυμα λάθους.

USER MANAGEMENT SYSTEM

### NEW USER

Giorgos

Georgiou

giorgos@gmail.com

\*\*\*\*\*

\*\*\*\*\*

Matching Passwords!

Save User

[Back to Users List](#)

Εικόνα 49: Update Users Credentials (root)

USER MANAGEMENT SYSTEM

### NEW USER

DAMIANOS

PAPPAS

asdas

must be a well-formed email address

User Password

Confirm Password

Save User

[Back to Users List](#)

Εικόνα 50: Update User (wrong credentials)

Αν ο διαχειριστής συμπληρώσει σωστά τα στοιχεία θα λάβει μήνυμα επιτυχίας, εάν όμως πληκτρολογήσει email που είδη υπάρχει στην βάση θα του εμφανιστεί μήνυμα λάθους.

USER MANAGEMENT SYSTEM

### NEW USER

User First Name

User Last Name

User Email

User Password

Confirm Password

Save User

[Back to Users List](#)

You've successfully registered new user!

Εικόνα 51: User Successfully updated(root)

USER MANAGEMENT SYSTEM

### NEW USER

User First Name

User Last Name

User Email

User Password

Confirm Password

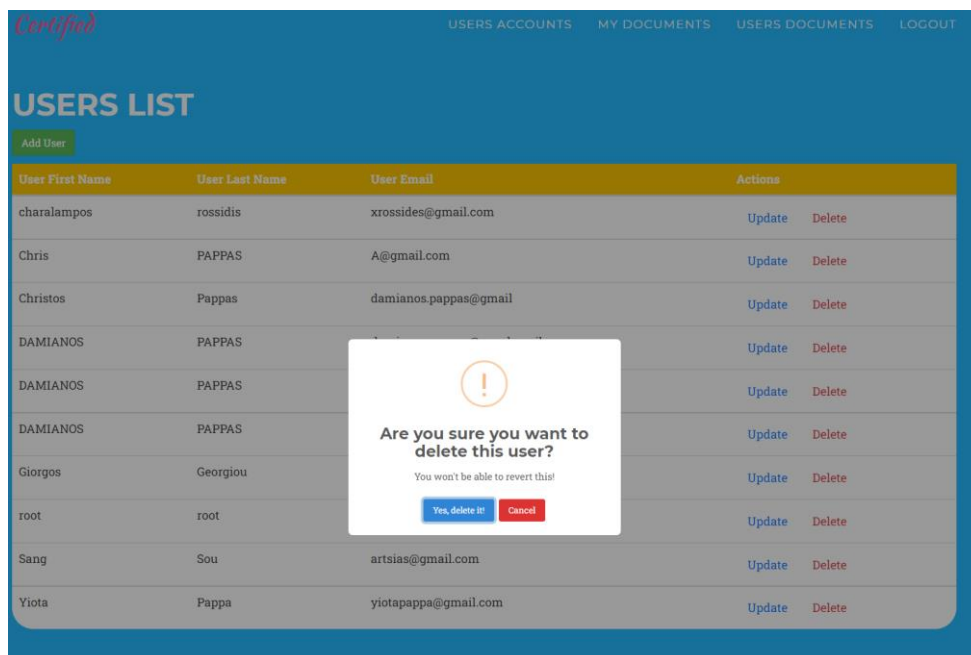
Save User

[Back to Users List](#)

Username and/or Password are not valid.

Εικόνα 52: Failed to update user credentials(root)

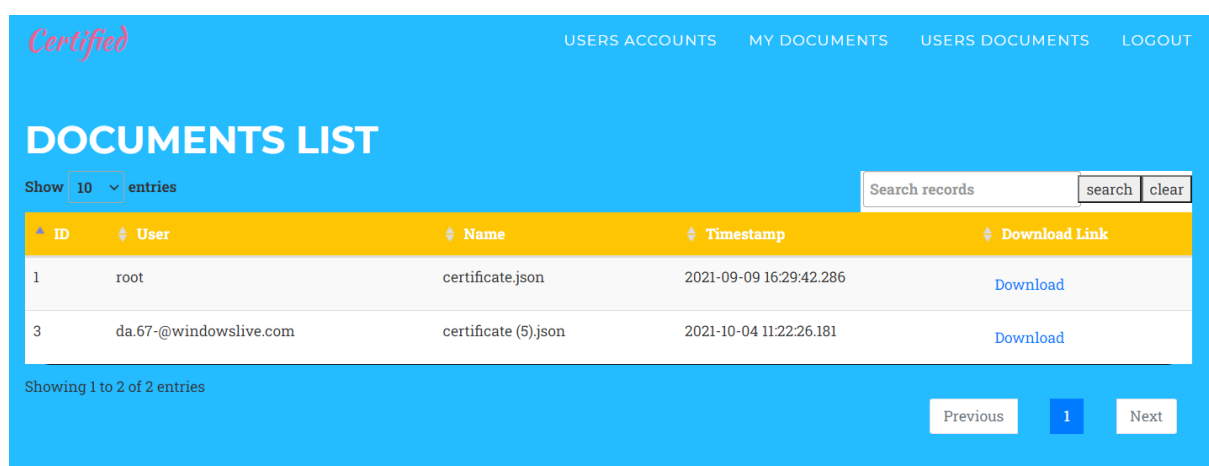
Για την λειτουργικότητα διαγραφής χρήστη ο διαχειριστής πρέπει να επιβεβαιώσει την ενέργεια αυτή στο μήνυμα επιβεβαίωσης που θα εμφανιστεί για την αποφυγή κάποιου λάθους, αφού αυτή η λειτουργικότητα είναι μη αναστρέψιμη.



Εικόνα 53: Confirmation message for deleting user (root)

### 5.3.2.3 Users Documents

Στην καρτέλα Users Documents ο διαχειριστής μπορεί να δει την λίστα με τα αποθηκευμένα έγγραφα των χρηστών, όπου εκεί του δίνεται η δυνατότητα να τα ταξινομήσει ή να κάνει οποιαδήποτε αναζήτηση σε αυτά. Επίσης ένα άλλο προνόμιο του σε ειδικές περιπτώσεις (το αναλύσαμε περαιτέρω στο υποκεφάλαιο με το επιχειρησιακό μοντέλο) είναι να κατεβάσει τοπικά τα έγγραφα στην συσκευή του.

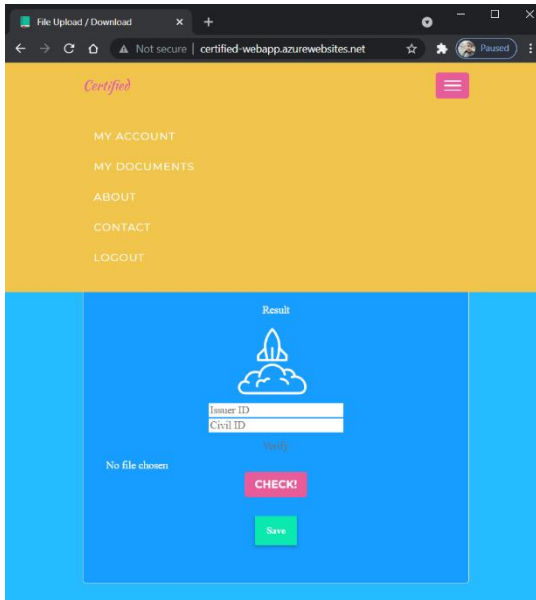


Εικόνα 54: All users documents (root)

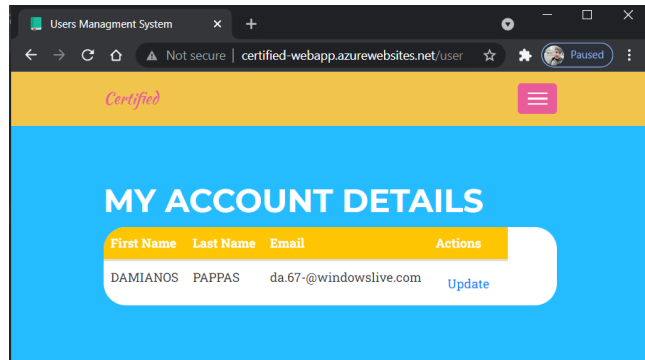
### 5.3.3 Mobile

Κύριο μέλημα μας ήταν η εφαρμογή να είναι ευχάριστη και εύκολη στην χρήση από όλες τις ομάδες χριστών και σε όλες τις συσκευές. Έτσι χρησιμοποιήσαμε εργαλεία που φτιάχνουν mobile friendly εφαρμογές, αλλάζοντας την όψη τους ανάλογα σε τι είδους συσκευή χρησιμοποιούνται. Η εφαρμογή μας είναι φιλική προς τον χρήστη που χρησιμοποιεί το κινητό του τηλέφωνο τόσο σε online μορφή στο cloud του azure πόσο μάλλον όταν τρέχει τοπικά.

#### 5.3.3.1 User

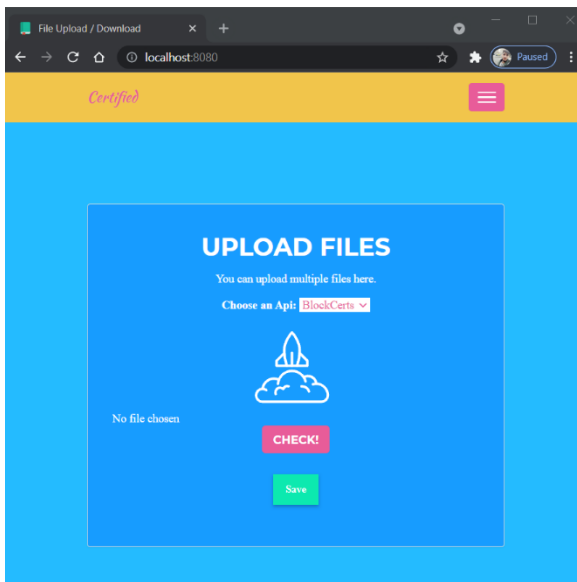


Εικόνα 56: Mobile friendly menu (user Azure)

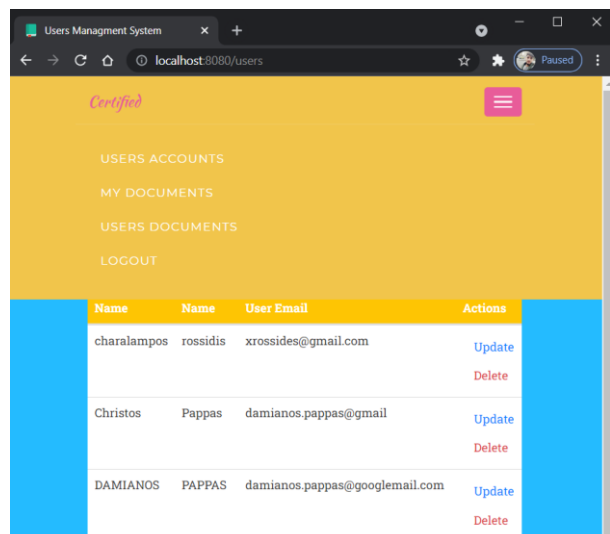


Εικόνα 55: My Account mobile (user Azure)

#### 5.3.3.2 Root



Εικόνα 57: Mobile friendly main page (root local)



Εικόνα 58: Mobile friendly menu (root local)



## 5.4 Εγκατάσταση εφαρμογής και GitHub

### 5.4.1 GitHub

Για να κατανοήσουμε το GitHub, πρέπει πρώτα να κατανοήσουμε τι είναι το Git. Το Git είναι ένα σύστημα ελέγχου έκδοσης ανοιχτού κώδικα που ξεκίνησε από τον Linus Torvalds - το ίδιο άτομο που δημιούργησε το Linux. Το Git είναι παρόμοιο με άλλα συστήματα ελέγχου εκδόσεων - Subversion, CVS και Mercurial για να αναφέρουμε μερικά. Έτσι, το Git είναι ένα σύστημα ελέγχου εκδόσεων, αλλά τι σημαίνει αυτό; Όταν οι προγραμματιστές δημιουργούν κάτι (για παράδειγμα μια εφαρμογή), πραγματοποιούν συνεχείς αλλαγές στον κώδικα, απελευθερώνοντας νέες εκδόσεις έως και μετά την πρώτη επίσημη κυκλοφορία (χωρίς beta). Τα συστήματα ελέγχου έκδοσης διατηρούν αυτές τις αναθεωρήσεις ευθείες, αποθηκεύοντας τις τροποποιήσεις σε ένα κεντρικό αποθετήριο. Αυτό επιτρέπει στους προγραμματιστές να συνεργάζονται εύκολα, καθώς μπορούν να κατεβάσουν μια νέα έκδοση του λογισμικού, να κάνουν αλλαγές και να ανεβάσουν τη νεότερη αναθεώρηση. Κάθε προγραμματιστής μπορεί να δει αυτές τις νέες αλλαγές, να τις κατεβάσει και να συνεισφέρει. Ομοίως, άτομα που δεν έχουν καμία σχέση με την ανάπτυξη ενός έργου μπορούν ακόμα να κατεβάσουν τα αρχεία και να τα χρησιμοποιήσουν.

Το Git είναι το προτιμώμενο σύστημα ελέγχου έκδοσης των περισσότερων προγραμματιστών, καθώς έχει πολλαπλά πλεονεκτήματα σε σχέση με τα άλλα διαθέσιμα συστήματα. Αποθηκεύει τις αλλαγές αρχείων πιο αποτελεσματικά και εξασφαλίζει καλύτερη ακεραιότητα αρχείων. Τι κάνει όμως το GitHub τόσο ξεχωριστό; Το Git είναι ένα εργαλείο γραμμής εντολών, αλλά το κέντρο γύρω από το οποίο περιστρέφονται όλα τα πράγματα που αφορούν το Git είναι ο κόμβος - το GitHub.com - όπου οι προγραμματιστές αποθηκεύουν τα έργα τους και το δίκτυό τους με άλλα άτομα.

Για αυτό και εμείς λοιπόν επιλέξαμε να αναπτύξουμε τον κώδικα μας στο GitHub κάνοντας commit και push στο δικό μας repository (αποθήκη), ολόκληρα κομμάτια κώδικα που τα ομαδοποιήσουμε κατά λειτουργικότητες κατά την ανάπτυξη της εφαρμογής μας.

### 5.4.1 Εγκατάσταση Εφαρμογής

Για την εγκατάσταση της εφαρμογής τόσο τοπικά όσο και στο cloud θα βρείτε αναλυτικά τα βήματα στο README.md του repository<sup>3</sup> της εφαρμογής.

Αρχικά θα πρέπει να κατεβάσετε ολόκληρο το project τοπικά στον υπολογιστή σας. Έπειτα θα εγκαταστήσετε το IntelliJ IDEA και το MySQL Workbench (μόνο αν θέλετε να χρησιμοποιήσετε βάση τοπικά). Η εφαρμογή θα τρέχει στο url: <http://localhost:8080/>

#### Τοπική εγκατάσταση:

- Δημιουργώ έναν localhost στο MySQL Workbench με κωδικό και username «root»
- Μέσα στον server που δημιουργήσαμε φτιάχνουμε ένα scheme με ονομασία «cerified» που θα γεμίσει αυτόματα αργότερα
- Ανοίγω το project με το IntelliJ IDEA
- Στο tab του maven επιλέγω το profile “Local” και τρέχω την εντολή “Reload All Maven Projects”
- Τέλος τρέχω την εφαρμογή πατώντας δεξί κλικ στο αρχείο CertifiedApplication.java
- Η εφαρμογή θα τρέχει στην πιο πάνω διεύθυνση με την τοπική βάση που δημιουργήσαμε.

#### Τοπική εγκατάσταση με cloud database:

- Ανοίγω το project με το IntelliJ IDEA
- Στο tab του maven επιλέγω το profile “Azure” και τρέχω την εντολή “Reload All Maven Projects”
- Τέλος τρέχω την εφαρμογή πατώντας δεξί κλικ στο αρχείο CertifiedApplication.java
- Η εφαρμογή θα τρέχει στην πιο πάνω διεύθυνση με την cloud database.

---

<sup>3</sup> <https://github.com/damianosp7/Certified>

## 6. Cloud Computing και η εφαρμογή του(AZURE)

### 6.1 Τι είναι το Cloud Computing

Το «Cloud Computing» ή αλλιώς «Υπολογιστικό Νέφος» στα νέα ελληνικά είναι η παροχή υπηρεσιών και η διάθεση υπολογιστικών πόρων μέσω του διαδικτύου. Αυτοί οι υπολογιστικοί πόροι πολλές φορές βρίσκονται σε απομακρυσμένες γεωγραφικές περιοχές από τον χρήστη και διασκορπισμένοι σε όλα τα μήκη και πλάτη του πλανήτη, με απώτερο σκοπό να εξυπηρετήσουν τον πελάτη, αυτοματοποιώντας διαδικασίες και παρέχοντας ευελιξία σύνδεσης. Πιο απλά θα λέγαμε πως το «Cloud Computing» δίνει την δυνατότητα παροχής υπηρεσιών υπολογιστών-διακομιστών, αποθηκευτικών χώρων, βάσεων δεδομένων, δικτύωσης, λογισμικού, αναλυτικών στοιχείων και άλλων πολλών υπηρεσιών που ο χρήστης μπορεί να αξιοποιήσει και να έχει πρόσβαση σε αυτές εξ αποστάσεως μέσω του σύννεφου ('cloud').[46]

Το «Cloud Computing» ονομάστηκε έτσι γιατί ο καθένας μπορεί να έχει πρόσβαση στην πληροφορία που παρέχεται εξ αποστάσεως μέσω ενός cloud ή κάποιου εικονικού αποθηκευτικού χώρου. Τα cloud services δίνουν την ελευθερία στον χρήστη να αποθηκεύσει οτιδήποτε αυτός θέλει σε servers και virtual spaces ανά τον κόσμο και να έχει άμεση πρόσβαση σε αυτή την πληροφορία από όπου και να βρίσκεται, φτάνει να ισχύει η προϋπόθεση πως υπάρχει μια σύνδεση στον παγκόσμιο ιστό. Με λίγα λόγια το «Cloud Computing» αναλαμβάνει όλη την σκληρή δουλειά που αφορά την επεξεργασία και αποθήκευση δεδομένων μακριά από την συσκευή σας και τα μεταφέρει σε μεγάλα και υπερσύγχρονα υπολογιστικά συστήματα που βρίσκονται σε απομακρυσμένα μέρη του πλανήτη, δίνοντας την ελευθερία στον πελάτη να μην ανησυχήσει ποτέ αν το υπολογιστικό του σύστημα έχει αρκετή δύναμη ώστε να σηκώσει μια εφαρμογή στο web, ή αν υπάρχει αρκετός αποθηκευτικός χώρος ή ακόμα να έχει στο μυαλό του τη συντήρηση της υποδομής και του εξοπλισμού που έχει στην κατοχή του.[47] Όλα αυτά και άλλα πολλά ακόμη είναι βάρη, που έρχεται το «Cloud Computing» να πάρει από τους ώμους του χρήστη, πάντα με το αντίστοιχο τίμημα.

Το «Cloud Computing» έφερε μια μεγάλη αλλαγή σχετικά με τον παραδοσιακό τρόπο που οι επιχειρήσεις σκέφτονται για τους πόρους πληροφορικής. Το «Cloud Computing» έχει σημαντικά οφέλη, καθώς οι οργανισμοί που το χρησιμοποιούν διανέμουν τους πόρους τους πιο ευέλικτα και το πιο σημαντικό είναι ότι, όταν δεν χρησιμοποιούνται, επαναφέρονται ή απελευθερώνονται. Σημαντικός λόγος για τον οποίο οι οργανισμοί στρέφονται στις υπηρεσίες «Cloud Computing» είναι το κόστος. Επίσης, εξαλείφει το κόστος κεφαλαίου για την αγορά υλικού και λογισμικού, παρέχει ταχύτητα και καλύτερη παραγωγικότητα, καθώς και μεγαλύτερη απόδοση και αξιοπιστία. Και, ως συνήθως, στις τιμολογιακές πολιτικές των εταιρειών που παρέχουν cloud solutions εφαρμόζεται το “pay as you go πλάνο”, αυτό σημαίνει πως πληρώνεις ανάλογα τους υπολογιστικούς πόρους που χρησιμοποιείς και την κίνηση στο δίκτυό σου.

## 6.2 Ιστορία πίσω από το Cloud Computing

Η έννοια του «Υπολογιστικού Νέφους» («Cloud Computing») γεννήθηκε το 1963, όταν ο αμυντικός οργανισμός προηγμένων ερευνητικών έργων ή αλλιώς DARPA έδωσε επιχορήγηση στο MIT, ύψους 2 εκατομμυρίων δολαρίων, για την ανάπτυξη του λεγόμενου Project MAC. Σε αυτό το Project υπήρχαν απαιτήσεις που προέβλεπαν την δημιουργία και ανάπτυξη τεχνολογίας που θα καθιστούσε δυνατόν ένας υπολογιστής να χρησιμοποιείται από δύο άτομα ταυτόχρονα! Αποτέλεσμα αυτού ήταν η γέννηση του όρου που έχει γίνει πλέον συλλογικά γνωστό ως «Cloud Computing», με πρόδρομό του έναν από αυτούς τους γιγαντιαίους, αρχαίους υπολογιστές που χρησιμοποιούσαν κυλίνδρους μαγνητικής ταινίας για τη μνήμη.[48]

Αυτό το σύστημα λειτούργησε ως ένα πρωτόγονο «cloud» με δύο ή τρία άτομα να έχουν ταυτόχρονη πρόσβαση σε αυτό. Ο όρος, που χρησιμοποιήθηκε αρχικά για να περιγράψει αυτή την πρωτόγονη για τα τότε δεδομένα διαδικασία, ήταν αυτός του “Virtualization” (“Εικονοποίηση”), αν και αργότερα η σημασία αυτής της λέξης επεκτάθηκε.

Η μέχρι τότε επικρατούσα έννοια της «Εικονοποίησης» (“Virtualization”), που χρησιμοποιούνταν για να περιγράψει το πρώιμο «Cloud Computing», άρχισε να παίρνει διαφορετική σημασία κατά τη δεκαετία του 1970 με την εμφάνιση του διαδικτύου (“Internet”). Πλέον περιγράφει τη δημιουργία μιας εικονικής μηχανής, που λειτουργεί σαν πραγματικός υπολογιστής, με ένα πλήρως λειτουργικό σύστημα. Αυτή η έννοια εξελίχθηκε και εδραιώθηκε κυρίως λόγω των επιχειρήσεων που άρχισαν να προσφέρουν «εικονικά» ιδιωτικά δίκτυα ως υπηρεσία ενοικίασης. Τότε είναι που εισήχθησαν στο παιχνίδι η IBM και η Google και αποφάσισαν να συνεργαστούν στο συγκεκριμένο τεχνολογικό πεδίο. Αρχικά, η IBM παρουσίασε το λειτουργικό σύστημα εικονικών μηχανών (VM operating system), το οποίο παρείχε τη δυνατότητα να εργάζονται πολλές εικονικές μηχανές (virtual machines) στο ίδιο μηχάνημα. Κάθε εικονική μηχανή είναι μία αυτοτελής οντότητα που εκτελεί το δικό της λειτουργικό σύστημα και παρέχει υπολογιστικούς πόρους, όπως τη μια κεντρική μονάδα επεξεργασίας, μνήμης και μονάδες εισόδου-εξόδου.[49]

Το «Cloud Computing» απέκτησε δημοσιότητα γύρω στο 1999, καθώς οι εταιρείες έχτιζαν μια καλύτερη κατανόηση και γνώση γύρω από τον όρο αυτό. Ένα καλό παράδειγμα σωστής χρήσης του «Cloud Computing» ήταν η εταιρεία Salesforce, που το 1999 το χρησιμοποίησαν και πρωτοστάτησαν με την ιδέα της εκμετάλλευσης του διαδικτύου για την παράδοση προγραμμάτων λογισμικού στους χρήστες. Με αυτόν τον τρόπο θα μπορούσε ο καθένας να έχει πρόσβαση στα προγράμματα ή στο λογισμικό μέσω του διαδικτύου και θα του δινόταν η δυνατότητα να τα κατεβάσει τοπικά στον υπολογιστή του. Έτσι, το μόνο που θα χρειαζόταν κάποιος για να έχει πρόσβαση σε αυτά τα προγράμματα θα ήταν η σύνδεση στο διαδίκτυο και οι επιχειρήσεις θα μπορούσαν να αγοράσουν το λογισμικό κατά παραγγελία, γρήγορα οικονομικά και άμεσα χωρίς μεσάζοντες και χωρίς να κουνηθεί κανείς από τα γραφεία, πράγμα που αποτελούσε επανάσταση για τα δεδομένα της εποχής.

Το 2002, η Amazon παρουσίασε στο κοινό υπηρεσίες που βασίζονται στο διαδίκτυο (“web-based services”) και ήταν η πρώτη μεγάλη επιχείρηση που σκέφτηκε να χρησιμοποιήσει μόνο το 10% της χωρητικότητας που είχε στην κατοχή της, πράγμα περίεργο για τα τότε δεδομένα αφού οι υπόλοιπες επιχειρήσεις χρησιμοποιούσαν μεγαλύτερα ποσοστά. Αυτό το έβλεπαν, γιατί το μοντέλο που σχεδίασαν για τις υποδομές του «Cloud Computing» τους έδινε την ελαστικότητα να χρησιμοποιούν την υπολογιστική χωρητικότητα που είχαν στην διάθεσή τους πολύ πιο αποτελεσματικά. Αποτέλεσμα αυτής της επαναστατικής αρχιτεκτονικής των υποδομών τους ήταν να ακολουθήσουν το παράδειγμά τους και οι υπόλοιποι μεγάλοι οργανισμοί.[50]

Το 2006, η Amazon ξεκίνησε τις υπηρεσίες Web Amazon, οι οποίες προσφέρουν διαδικτυακές υπηρεσίες σε άλλους ιστότοπους ή πελάτες. Ένας από τους ιστότοπους της Amazon Web Services, που ονομάζεται Amazon Mechanical Turk, παρέχει μια ποικιλία υπηρεσιών (web-services) που βασίζονται στο Cloud, συμπεριλαμβανομένης της αποθήκευσης δεδομένων, του υπολογισμού πράξεων και

αλγορίθμων και της «ανθρώπινης νοημοσύνης» (human intelligence). Ένας άλλος ιστότοπος του Amazon Web Services είναι το Elastic Compute Cloud (EC2), που επιτρέπει στα άτομα να νοικιάζουν εικονικούς υπολογιστές και να χρησιμοποιούν τα δικά τους προγράμματα και εφαρμογές.

Την ίδια χρονιά, η Google ξεκίνησε τις υπηρεσίες των Google Docs. Τα Google Docs βασίστηκαν αρχικά σε δύο ξεχωριστά προϊόντα, το Google Spreadsheets και το Writely. Η Google αγόρασε το Writely, το οποίο προσφέρει στους ενοικιαστές τη δυνατότητα να αποθηκεύουν έγγραφα, να επεξεργάζονται έγγραφα και να τα μεταφέρουν σε συστήματα blog (ιστολογίου). Τα Google Spreadsheets είναι ένα πρόγραμμα που βασίζεται στο Διαδίκτυο και επιτρέπει στους χρήστες να αναπτύσσουν, να ενημερώνουν και να επεξεργάζονται υπολογιστικά φύλλα και να μοιράζονται τα δεδομένα στο διαδίκτυο.

Το 2007, η IBM, η Google και πολλά Πανεπιστήμια ένωσαν τις δυνάμεις τους για να αναπτύξουν ένα server farm για ερευνητικά έργα που χρειάζονται τόσο γρήγορους επεξεργαστές όσο και τεράστια σύνολα δεδομένων. Το Πανεπιστήμιο της Ουάσιγκτον ήταν το πρώτο που εγγράφηκε και χρησιμοποίησε πόρους που παρείχαν η IBM και η Google. Έπειτα και άλλα μεγάλα και καταξιωμένα Πανεπιστήμια ακολούθησαν γρήγορα το παράδειγμά τους. Τα Πανεπιστήμια συνειδητοποίησαν αμέσως ότι τα υπολογιστικά πειράματά τους μπορούν να γίνουν γρηγορότερα και με λιγότερα χρήματα, εάν η IBM και η Google υποστήριζαν την έρευνά τους με τις τεχνολογίες «Cloud Computing» που τους πρόσφεραν. Το 2007 ήταν επίσης η χρονιά κατά την οποία το Netflix ξεκίνησε την υπηρεσία streaming ταινιών και σειρών (streaming video service), χρησιμοποιώντας το «Cloud».

Το 2011, η IBM παρουσίασε το framework IBM SmartCloud για την υποστήριξη του Smarter Planet (ένα έργο πολιτιστικού χαρακτήρα). Στη συνέχεια, η Apple κυκλοφόρησε το iCloud, το οποίο επικεντρώνεται στην αποθήκευση προσωπικών πληροφοριών (φωτογραφίες, μουσική, βίντεο κ.λπ.). Επίσης, κατά τη διάρκεια αυτού του έτους, η Microsoft άρχισε να διαφημίζει το «Cloud» στην τηλεόραση, κάνοντας το ευρύ κοινό να γνωρίζει την ικανότητά του να αποθηκεύει φωτογραφίες ή βίντεο, με εύκολη πρόσβαση. Επίσης, η Oracle παρουσίασε το Oracle Cloud το 2012, προσφέροντας τους 3 βασικούς πυλώνες για τις επιχειρήσεις, το IaaS (Infrastructure-as-a-Service), το PaaS (Platform-as-a-Service) και το SAAS (Software-as-a-Service). Τα υπόλοιπα αποτελούν ιστορία μιας και σήμερα ολοένα και περισσότερες εταιρείες στρέφονται στο «Cloud Computing» σε μια προσπάθεια να συμβαδίσουν με το κύμα της τεχνολογικής ανάπτυξης της εποχής, έτσι ώστε να παραμείνουν ανταγωνιστικοί και επίκαιροι.[51]

### 6.3 Από τι διακρίνεται το cloud computing

- **Κατανομή ζήτησης (on-demand self service)**  
Οι πελάτες μπορούν αυτόματα να εκμεταλλεύονται υπολογιστικές δυνατότητες παροχής και τους πόρους για τη δική τους ασφάλεια, όταν χρειάζεται, χωρίς να απαιτείται οποιαδήποτε ανθρώπινη παρέμβαση.[47][48]
- **Διαθεσιμότητα των πόρων (Resource Pooling)**  
Ένας μεγάλος αριθμός πελατών είναι δυνατόν να χρησιμοποιούν την ίδια χρονική στιγμή το ίδιο σύνολο υπολογιστικών πόρων[46]. Η δυνατότητα αυτή είναι γνωστή ως διαθεσιμότητα πόρων (resource pooling). Η ιδέα είναι ότι ο πάροχος επιτρέπει στους πελάτες / χρήστες, οι οποίοι είναι διατεθειμένοι να πληρώσουν γι' αυτή την υπηρεσία, πρόσβαση σε μια μεγάλη κοινή δεξαμενή υπολογιστικών πόρων, φροντίζοντας ταυτόχρονα η απόδοση να ικανοποιεί τις απαιτήσεις τους.
- **Ευελιξία επεκτασιμότητας (Rapid Elasticity)**  
Η ευελιξία, όσον αφορά την ταχύτητα δέσμευσης / αποδέσμευσης πόρων με αποτέλεσμα την δυναμική προσαρμογή των πληροφοριακών συστημάτων στις εκάστοτε ανάγκες, είναι μια από τις θεμελιώδεις ευκολίες της υπολογιστικής νέφους. Στο μυαλό του πελάτη καταναλωτή οι δυνατότητες του σύννεφου είναι απεριόριστες, ενώ οι πόροι που διαθέτει τείνουν στο άπειρο. Επιπλέον είναι πάντοτε διαθέσιμες και ο πελάτης μπορεί να προμηθευτεί κάθε φορά όσες ακριβώς χρειάζεται. Η ταχύτητα που κάθε φορά ο πάροχος Cloud Computing προσαρμόζεται στις απαιτήσεις του πελάτη εξαρτάται από τις συμβάσεις (SLA's – Service Level Agreements) που έχει συνάψει μαζί του.
- **Τιμολόγηση βάση χρήσης (Measured Service)**  
Μια ακόμα καινοτομία που φέρνει το cloud computing είναι η εισαγωγή ενός διαφορετικού μοντέλου τιμολόγησης. Ο πελάτης δηλαδή πληρώνει ανάλογα με την χρήση των πόρων που ζητά να χρησιμοποιήσει. Το ακριβές μοντέλο τιμολόγησης μπορεί να διαφέρει από υπηρεσία σε υπηρεσία ή και από πάροχο σε πάροχο. Η χρήση των υπολογιστικών πόρων καταμετράται, ελέγχεται και αποτυπώνεται σε αναφορές (reports) παρέχοντας σαφή στοιχεία στα συναλλασσόμενα μέρη (πάροχος – πελάτης). Έτσι ο πάροχος μπορεί να τιμολογεί με απόλυτη διαφάνεια και ακρίβεια τον πελάτη του για τις υπηρεσίες που χρησιμοποίησε και ο πελάτης μπορεί να ελέγχει τι καλείται να πληρώσει ακριβώς, για ποιες υπηρεσίες και τότε τις χρησιμοποίησε.

### 6.4 Πλεονεκτήματα του Cloud (Azure)

- **Υψηλή διαθεσιμότητα (High Availability):**  
Ανάλογα με το Service-level agreement (SLA) που επιλέγετε, οι εφαρμογές σας που βασίζονται στο «Cloud» μπορούν να παρέχουν μια συνεχόμενη εμπειρία χρήστη χωρίς καμιά διακοπή λειτουργίας, ακόμη και όταν τα πράγματα πάνε στραβά.
- **Επεκτασιμότητα (Scalability):**  
Οι εφαρμογές στο «Cloud» μπορούν να κλιμακώνονται κάθετα και οριζόντια:
  - Η κάθετη κλιμάκωση αυξάνει την υπολογιστική δυνατότητα (compute capacity), προσθέτοντας RAM ή CPU σε μια εικονική μηχανή (virtual machine).
  - Η οριζόντια κλιμάκωση αυξάνει την υπολογιστική δυνατότητα (compute capacity), προσθέτοντας υπολογιστικούς πόρους. Ένα παράδειγμα είναι η προσθήκη περισσότερων εικονικών μηχανών (virtual machines) κατά την διαμόρφωση της εφαρμογής.
- **Ελαστικότητα (Elasticity):**  
Η δυνατότητα της διαμόρφωσης των εφαρμογών που βασίζονται στο «σύννεφο» («Cloud»), έτσι ώστε να επωφεληθούν από την υπηρεσία της αυτόματης επέκτασης πόρων σε περίπτωση απότομης αύξησης της ζήτησης σε resources (auto-scaling), που αυτό έχει ως αποτέλεσμα οι εφαρμογές σας να έχουν πάντα τους πόρους που χρειάζονται.

- **Ευελιξία (Agility):**  
Γρήγορη ανάπτυξη και διαμόρφωση πόρων που βασίζονται στο «σύννεφο», καθώς αλλάζουν οι απαιτήσεις της εφαρμογής σας.
- **Γεωδιανομή (Geo-distribution):**  
Μπορούν να αναπτυχθούν εφαρμογές και δεδομένα σε κέντρα δεδομένων (data-centers) τα οποία είναι χωρισμένα σε περιφέρειες (regions) και βρίσκονται σε όλο τον κόσμο, διασφαλίζοντας έτσι ότι οι πελάτες έχουν πάντα την καλύτερη απόδοση στην περιοχή τους.
- **Αποκατάσταση καταστροφών (Disaster Recovery):**  
Εκμεταλλεύόμενοι τις υπηρεσίες δημιουργίας αντιγράφων ασφαλείας που βασίζονται στο «σύννεφο», την αναπαραγωγή δεδομένων και τη γεωδιανομή, μπορούμε να αναπτύξουμε εφαρμογές έχοντας την εμπιστοσύνη ότι τα δεδομένα είναι ασφαλή σε περίπτωση βλάβης των υποδομών.[52][51]

## 6.5 Ποια είναι τα μοντέλα cloud service;

Κάποιος ο οποίος ασχολείται με το «Cloud computing» σίγουρα θα είχε συναντήσει κάποτε μπροστά του τα ακρωνύμια Paas, Iaas, Saas, τα οποία περιγράφουν τα διάφορα cloud service models (μοντέλα υπηρεσιών ‘Σύννεφου’). Αυτά τα τρία μοντέλα ορίζουν τα διαφορετικά επίπεδα κοινής ευθύνης που υπάρχουν μεταξύ του παρόχου Cloud, που προσφέρει τα Cloud services και του ενοικιαστή του Cloud ή αλλιώς του πελάτη.[48][53]Παρακάτω θα αναλύσουμε αυτά τα 3 μοντέλα παραθέτοντας τα χαρακτηριστικά τους.

### 6.5.1 Software as a Service – (SaaS)

Η ιδέα είναι ότι ένας πάροχος είναι δυνατόν να προσφέρει στους τελικούς χρήστες πρόσβαση σε διάφορες εφαρμογές λογισμικού. Οι εφαρμογές είναι προσβάσιμες από διάφορες συσκευές με χρήση απλών διεπαφών πελάτη, π.χ. ένα web browser, ο οποίος επιτρέπει την πρόσβαση στον διακομιστή (server) των λογισμικών. Τα λογισμικά αποτελούν ιδιοκτησία του παρόχου. Ως αντάλλαγμα των παραπάνω διευκολύνσεων, ο τελικός χρήστης καλείται να καταβάλει μίσθωμα για την χρήση τους. [54]

Στο μοντέλο αυτό δεν υπάρχει ανάγκη ο τελικός χρήστης να προβεί σε σχεδίαση και ανάπτυξη λογισμικού. Η μόνη εργασία που χρειάζεται να γίνει είναι παραμετροποίηση του λογισμικού, ώστε να ικανοποιήσει με τον καλύτερο δυνατό τρόπο τις ανάγκες. Δεν υπάρχει καμία πράξη αγοροπωλησίας software, ενώ η αμοιβή που ο τελικός χρήστης υποχρεούται να καταβάλει στον πάροχο αφορά μονάχα την χρήση του λογισμικού και την αποθήκευση των εγγραφών του.

Ένας SaaS πάροχος κανονικά φιλοξενεί και διαχειρίζεται ένα ή περισσότερα λογισμικά χρησιμοποιώντας ιδιόκτητες υποδομές, ενώ ταυτόχρονα διασφαλίζει την απρόσκοπτη διαθεσιμότητα σε πολλαπλούς χρήστες μέσω του διαδικτύου.

Γνωστά παραδείγματα υπηρεσιών αυτού του τύπου είναι το Microsoft Dynamics CRM Online της Microsoft, το Gmail, το Facebook, κλπ. Είναι προφανές από την απήχηση και μόνο των συγκεκριμένων εφαρμογών ότι πρόκειται για την περισσότερο διαδεδομένη εκδοχή χρήσης της υπολογιστικής νέφους. Τέλος δεν είναι λίγες οι φορές που ένα πάροχος SaaS χρησιμοποιεί υπηρεσίες Platform as a service (PaaS) ή και Infrastructure as a service (IaaS) τις οποίες προσφέρουν άλλοι Cloud Providers.

### 6.5.2 Platform as a Service – (PaaS)

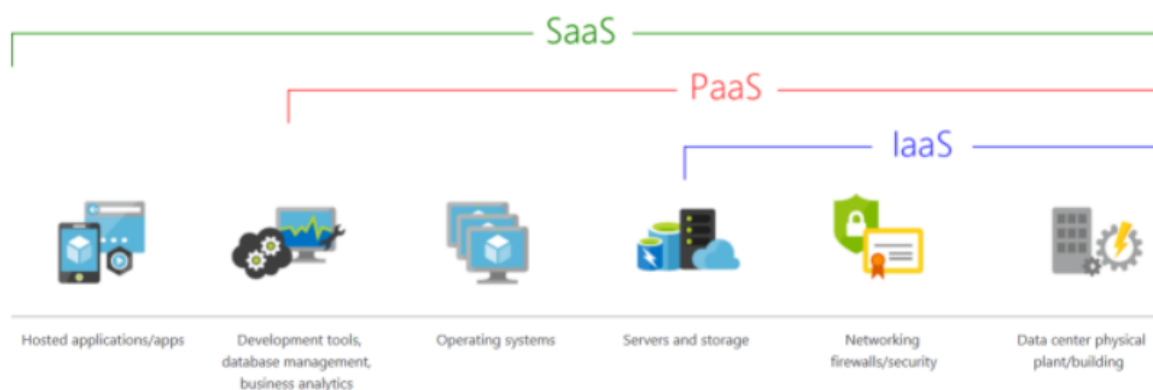
Η ιδέα είναι ότι ένας πάροχος είναι δυνατόν να προσφέρει την υλικοτεχνική υποδομή (IaaS) καθώς και συγκεκριμένης κατηγορίας software, όπως ολοκληρωμένα περιβάλλοντα ανάπτυξης λογισμικού, γλώσσες προγραμματισμού, βάσεις δεδομένων και λοιπά εργαλεία ανάπτυξης με την βοήθεια των οποίων ο τελικός χρήστης μπορεί να αναπτύξει το δικό του λογισμικό. Το μοντέλο Platform as a Service (PaaS) είναι ένα περιβάλλον ανάπτυξης, εγκατάστασης και διανομής λογισμικού και παρέχεται ως υπηρεσία σε προγραμματιστές μέσω του διαδικτύου. Διευκολύνει την ανάπτυξη του λογισμικού και τον διαμοιρασμό του απαλλαγμένο από το κόστος και την πολυπλοκότητα της αγοράς και της διαχείρισης της αναγκαίας υποδομής, ενώ ταυτόχρονα παρέχει όλες τις διευκολύνσεις που απαιτούνται για την υποστήριξη του κύκλου ζωής του λογισμικού [54]. Με το μοντέλο PaaS οι προγραμματιστές μπορούν να δημιουργούν εφαρμογές διαδικτύου (web applications) χωρίς να χρειάζεται να εγκαταστήσουν κανένα «εργαλείο» τοπικά στον υπολογιστή τους ενώ μπορούν να διανείμουν τα λογισμικά που παράγουν χωρίς χρήση κανενός ιδιαίτερου εργαλείου διαχείρισης.

Η Microsoft τα τελευταία χρόνια διαθέτει το Microsoft Azure, το οποίο είναι μια από τις πιο δημοφιλείς εκδοχές του PaaS. Επαγγελματίες της Πληροφορικής μπορούν να έχουν πρόσβαση σε εργαλεία τελευταίας γενιάς και να αναπτύξουν λογισμικό απευθείας στο «Σύννεφο».

### 6.5.3 Infrastructure as a Service – (IaaS)

Infrastructure as a Service είναι η υπηρεσία διάθεσης υλικοτεχνικής υποδομής, (hardware), όπως διακομιστές (servers), αποθηκευτικά μέσα (storage), υποδομές δικτύου (network) και σχετικού με αυτά λογισμικό, όπως λειτουργικά συστήματα (operating systems), τεχνολογίες εξομοίωσης (virtualization technology) και συστήματα διαχείρισης αρχείων (file systems). Πρόκειται για μια εξέλιξη του μοντέλου της παραδοσιακής φιλοξενίας αρχείων, η οποία όμως στην νέα της μορφή δεν απαιτεί μακροχρόνιες συμβάσεις, ενώ επιπλέον επιτρέπει στους τελικούς χρήστες να δεσμεύουν και να χρησιμοποιούν δυναμικά τις υποδομές ανάλογα με την ζήτηση. Στο μοντέλο αυτό ο πάροχος IaaS εκτελεί πολύ λίγες εργασίες υποστήριξης και οι τελικοί χρήστες πρέπει να διαμοιράσουν και να διαχειριστούν τις υπηρεσίες με τον ίδιο ακριβώς τρόπο, όπως θα έκαναν αν οι υποδομές ήταν στο δικό τους data center. [54].

Το μοντέλο Infrastructure as a Service είναι μια μορφή φιλοξενίας (hosting). Περιλαμβάνει πρόσβαση στο δίκτυο, καθώς και υπηρεσίες δρομολόγησης και αποθήκευσης δεδομένων. Ο πάροχος IaaS σε γενικές γραμμές συντηρεί το υλικό και διαχειρίζεται τις υπηρεσίες (services), που είναι αναγκαίες για να «τρέξουν» τα λογισμικά. Η δυναμική αυξομείωση του εύρους ζώνης (bandwidth), της μνήμης και του αποθηκευτικού χώρου είναι ένα από τα κύρια χαρακτηριστικά του μοντέλου. Η ταχύτητα της δυναμικής προσαρμογής και η τιμολόγησή της αποτελεί πεδίο ισχυρού ανταγωνισμού μεταξύ των παρόχων υπηρεσιών IaaS.



Εικόνα 59: SaaS, PaaS, IaaS

Δεκάδες εκατοντάδες εφαρμογές που υποστηρίζουν παράλληλη χρήση σε διάφορες συσκευές (smart phones, tablets, desktop applications) εμπίπτουν στην κατηγορία αυτή. Τα δεδομένα τους είναι

αποθηκευμένα σε υποδομές του Cloud και γίνονται διαθέσιμα προς χρήση στην τελευταία τους μορφή από όποια συσκευή και αν ζητηθούν.

## 6.6 Σύγκριση μεταξύ των μοντέλων cloud service

### 6.6.1. SaaS

SaaS είναι το λογισμικό που φιλοξενείται κεντρικά στην εταιρεία που παρέχει το cloud και μπορεί κάποιος να το διαχειριστεί προς όφελος του ιδίου αλλά καθώς και για τους χρήστες ή τους πελάτες του. Συνήθως μία έκδοση της εφαρμογής χρησιμοποιείται για όλους τους πελάτες και έχει άδεια μέσω μηνιαίας ή ετήσιας συνδρομής.

Το SaaS παρέχει τα ίδια οφέλη κατά κύριο λόγο με το IaaS, αλλά υπάρχουν και κάποια επιπρόσθετα οφέλη που είναι άξια αναφοράς.

#### Πλεονεκτήματα:

- **No CapEx:** Οι χρήστες δεν έχουν προκαταρκτικό κόστος.
- **Agility:** Οι χρήστες μπορούν να παρέχουν στο προσωπικό πρόσβαση στο πιο πρόσφατο λογισμικό γρήγορα και εύκολα.
- **Pay as you go τιμολογιακή πολιτική:** Οι χρήστες πληρώνουν για το λογισμικό που χρησιμοποιούν σε συνδρομητικό μοντέλο, συνήθως μηνιαία ή ετήσια, ανεξάρτητα από το πόσο χρησιμοποιούν το λογισμικό.
- **Skills:** Δεν απαιτούνται πολύ εξειδικευμένες τεχνικές δεξιότητες για την ανάπτυξη, τη χρήση και την απόκτηση του SaaS
- **Elasticity:** Οι χρήστες μπορούν να έχουν πρόσβαση στα ίδια δεδομένα εφαρμογής από οπουδήποτε.

#### Μειονέκτημα :

- **Software Limitations.**

Μπορεί να υπάρχουν ορισμένοι περιορισμοί σε κάποια εφαρμογή που προσφέρει το SaaS που μπορεί να επηρεάσουν τον τρόπο με τον οποίο οι χρήστες θα ήθελαν να το χρησιμοποιήσουν. Επειδή χρησιμοποιείται έτοιμο λογισμικό, ο χρήστης-πελάτης δεν έχει τον άμεσο έλεγχο των λειτουργιών, έτσι δεν μπορεί ο ίδιος να κάνει αλλαγές οι οποίες θα χρειαζόνταν, για να φέρει στα μέτρα του την εφαρμογή. Γι' αυτό, πριν μια εταιρεία χρησιμοποιήσει κάποια πλατφόρμα SaaS πρέπει πρώτα να αξιολογήσει της ανάγκες της και να λάβει υπόψιν τον οποιοδήποτε περιορισμό λόγω λογισμικού μπορεί να προκύψει.[48]

### 6.6.2. PaaS

#### Πλεονεκτήματα:

- **No CapEx:** Οι χρήστες δεν έχουν προκαταρκτικό κόστος.
- **Agility:** Το PaaS είναι πιο ευέλικτο από το IaaS και οι χρήστες δεν χρειάζεται να διαμορφώσουν διακομιστές(servers) για εκτέλεση εφαρμογών.
- **Consumption-based model:** Οι χρήστες πληρώνουν μόνο για αυτό που χρησιμοποιούν και λειτουργούν με μοντέλο τιμολογιακής πολιτικής OpEx.
- **Skills:** Δεν απαιτούνται εξειδικευμένες τεχνικές δεξιότητες για την ανάπτυξη, τη χρήση και την απόκτηση των πλεονεκτημάτων του PaaS.
- **Cloud benefits:** Οι χρήστες μπορούν να επωφεληθούν από τις δεξιότητες και την τεχνογνωσία του παρόχου cloud για να διασφαλίσουν ότι τα projects τους θα είναι ασφαλή και διαθέσιμα ανά πάσα ώρα και στιγμή (availability). Επιπλέον, οι χρήστες μπορούν να αποκτήσουν πρόσβαση σε περισσότερα εκσυγχρονισμένα εργαλεία τελευταίας τεχνολογίας. Στη συνέχεια, μπορούν να χρησιμοποιήσουν αυτά τα εργαλεία σε ολόκληρο τον κύκλο ζωής μιας εφαρμογής.



- **Productivity:** Οι χρήστες μπορούν να επικεντρωθούν στην ανάπτυξη εφαρμογών μόνο, επειδή ο πάροχος cloud διαχειρίζεται όλα όσα έχουν να κάνουν με την σωστή λειτουργία της πλατφόρμας. Η συνεργασία με καταναμημένες ομάδες ως υπηρεσίες είναι ευκολότερη επειδή η πλατφόρμα είναι προσβάσιμη μέσω διαδικτύου. Μπορείτε να κάνετε την πλατφόρμα διαθέσιμη παγκοσμίως πιο εύκολα.

#### Μειονέκτημα :

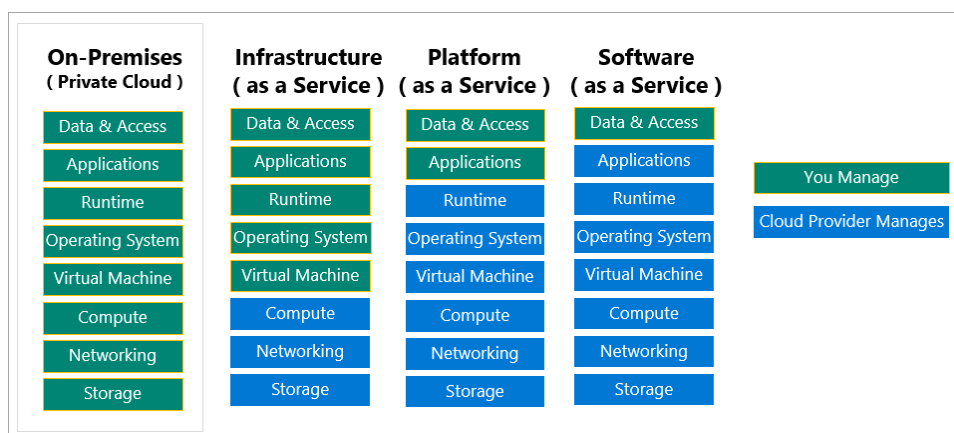
Μπορεί να υπάρχουν ορισμένοι περιορισμοί σε μια πλατφόρμα cloud που ενδέχεται να επηρεάσουν τον τρόπο λειτουργίας μιας εφαρμογής. Όταν αξιολογείται ποια πλατφόρμα PaaS είναι η πιο κατάλληλη για μια συγκεκριμένη εφαρμογή, πρέπει να λαμβάνονται υπόψη τυχόν περιορισμοί σε αυτόν τον τομέα.

### 6.6.3. IaaS

Το IaaS είναι το πιο ελαστικό μοντέλο από τα τρία, αφού έχει στόχο να δώσει στον χρήστη τον πλήρη έλεγχο του hardware πάνω στο οποίο τρέχει η εκάστοτε εφαρμογή. Έρχεται να αντικαταστήσει την αγορά hardware εξοπλισμού, αφού με το μοντέλο αυτό ενοικιάζεις τον εξοπλισμό από τους παρόχους cloud services.[54]

#### Πλεονεκτήματα:

- **No CapEx:** Οι χρήστες δεν έχουν προκαταρκτικό κόστος.
- **Consumption-based model:** Οι χρήστες πληρώνουν μόνο για αυτό που χρησιμοποιούν και λειτουργούν με μοντέλο τιμολογιακής πολιτικής OpEx
- **Skills:** Δεν απαιτούνται εξειδικευμένες τεχνικές δεξιότητες για την ανάπτυξη, τη χρήση και την απόκτηση των πλεονεκτημάτων του IaaS.
- **Cloud benefits:** Οι χρήστες μπορούν να επωφεληθούν από τις δεξιότητες και την τεχνογνωσία του παρόχου cloud για να διασφαλίσουν ότι τα projects τους θα είναι ασφαλή και διαθέσιμα ανά πάσα ώρα και στιγμή (availability).
- **Flexibility:** Το IaaS είναι η πιο ευέλικτη υπηρεσία cloud επειδή ο πελάτης έχει τον έλεγχο για τη διαμόρφωση και τη διαχείριση του hardware που εκτελεί την εφαρμογή. Από τα παραπάνω συμπεραίνουμε πως το IaaS μοντέλο έχει την μεγαλύτερη ευελιξία από τα τρία γιατί ο χρήστης μπορεί να διαχειριστεί και να ρυθμίσει το hardware. Το PaaS είναι ένα μοντέλο το οποίο επικεντρώνεται στην δημιουργία και ανάπτυξη των εφαρμογών και η διαχείριση της πλατφόρμας στην οποία βρίσκεται η εφαρμογή γίνεται από τον πάροχο υπηρεσιών cloud. Τέλος, στο SaaS μοντέλο εφαρμόζεται η pay-as-you-go τιμολογιακή πολιτική και ο χρήστης πληρώνει την χρήση λογισμικών προγραμμάτων μέσα από την εγγραφή του.



Εικόνα 60: Comparison between models

## 6.7 Διαφορετικοί τύποι μοντέλων cloud

Σήμερα στην βιομηχανία της τεχνολογίας είναι επικρατέστερα τρία μοντέλα ανάπτυξης cloud computing τα οποία ουσιαστικά περιγράφουν το πώς κατανέμονται οι υπολογιστικοί πόροι και ποιος μπορεί να τους χρησιμοποιήσει, ανάμεσα στον πάροχο του «cloud computing» και τον χρήστη. Αυτά τα τρία μοντέλα είναι το δημόσιο νέφος (public cloud) το ιδιωτικό νέφος (private cloud) και το υβριδικό νέφος (hybrid cloud). [55]

### 6.7.1 Δημόσιο νέφος (Public Cloud)

Το δημόσιο νέφος είναι ο πιο συνηθισμένος αλλά και διαδεδομένος τρόπος ανάπτυξης «Cloud computing». Οι υπολογιστικοί πόροι (servers, data centers κ.α.) του νέφους βρίσκονται υπό την κατοχή του παρόχου «Cloud computing», ο οποίος τους λειτουργεί, τους διαχειρίζεται και προσφέρει τα cloud services στον πελάτη μέσω του διαδικτύου. Με το μοντέλο του δημόσιου νέφους (public cloud) όλο το λογισμικό, το hardware, όπως και διάφορες άλλες υποδομές ανήκουν και διαχειρίζονται από τον πάροχο των cloud services. Ένα καλό παράδειγμα αυτού του μοντέλου αποτελεί και το Microsoft Azure. Στο δημόσιο νέφος ο κάθε οργανισμός, επιχείρηση ή ακόμα και αυτόνομος πελάτης ο οποίος το χρησιμοποιεί, μοιράζεται τους πόρους (υλικό, χώρο αποθήκευσης και συσκευές δικτύου) με τους υπολοίπους «ενοικιαστές» του νέφους, έχοντας πρόσβαση μέσω ενός προγράμματος περιήγησης ιστού (web-browser). Οι δημόσιες εφαρμογές «Cloud» χρησιμοποιούνται συχνά για την παροχή και χρήση ηλεκτρονικού ταχυδρομείου (web-based email), διαδικτυακών εφαρμογών, οι οποίες χρησιμοποιούνται σε γραφεία, χώρους αποθήκευσης και εικονικού περιβάλλοντος δοκιμών και ανάπτυξης νέων εφαρμογών.

Πλεονεκτήματα των δημόσιων cloud:

- Χαμηλότερο κόστος - δεν χρειάζεται αγορά υλικού ή λογισμικού, ο πελάτης πληρώνει μόνο για την υπηρεσία που χρησιμοποιεί.
- Χωρίς συντήρηση - ο πάροχος υπηρεσιών «Cloud» παρέχει τη συντήρηση.
- Σχεδόν απεριόριστη επεκτασιμότητα - διατίθενται πόροι κατά παραγγελία για να καλύψουν τις ανάγκες της κάθε επιχείρησης ή του κάθε πελάτη.
- Υψηλή αξιοπιστία - ένα τεράστιο δίκτυο διακομιστών (servers) διασφαλίζει την προστασία από οποιαδήποτε βλάβη του συστήματος.

### 6.7.2 Ιδιωτικό νέφος (Private Cloud)

Ένα ιδιωτικό σύννεφο αποτελείται από υπολογιστικούς πόρους «cloud» που χρησιμοποιούνται αποκλειστικά από μία επιχείρηση ή οργανισμό. Το ιδιωτικό σύννεφο μπορεί να βρίσκεται φυσικά στο κέντρο δεδομένων του οργανισμού ή να φιλοξενείται από τρίτο πάροχο υπηρεσιών. Αλλά σε ένα ιδιωτικό σύννεφο, οι υπηρεσίες και η υποδομή διατηρούνται πάντα σε ένα ιδιωτικό δίκτυο και το υλικό και το λογισμικό είναι αφιερωμένα αποκλειστικά στον εκάστοτε οργανισμό.

Με αυτόν τον τρόπο, ένα ιδιωτικό «cloud» μπορεί να διευκολύνει έναν οργανισμό να προσαρμόσει τους πόρους του ώστε να πληροί συγκεκριμένες απαιτήσεις. Τα ιδιωτικά σύννεφα χρησιμοποιούνται συχνά από κυβερνητικές υπηρεσίες, χρηματοπιστωτικά ιδρύματα, οποιοσδήποτε άλλες οργανώσεις μεσαίου έως μεγάλου μεγέθους με επιχειρηματικές δραστηριότητες κρίσιμες που επιδιώκουν επιπρόσθετο έλεγχο του περιβάλλοντός τους.

### Πλεονεκτήματα ενός ιδιωτικού cloud:

- Μεγαλύτερη ευελιξία - ο οργανισμός μπορεί να προσαρμόσει το περιβάλλον «cloud» του για να καλύψει συγκεκριμένες επιχειρηματικές ανάγκες.
- Περισσότερος έλεγχος - οι πόροι δεν μοιράζονται με άλλους, επομένως είναι δυνατά υψηλότερα επίπεδα ελέγχου και ιδιωτικότητας.
- Μεγαλύτερη επεκτασιμότητα-τα ιδιωτικά σύννεφα συχνά προσφέρουν μεγαλύτερη δυνατότητα κλιμάκωσης σε σύγκριση με την εσωτερική υποδομή (on-premises infrastructure).

### **6.7.3 Υβριδικό νέφος (Hybrid Cloud)**

Μια υβριδική πλατφόρμα cloud παρέχει στους οργανισμούς πολλά πλεονεκτήματα - όπως μεγαλύτερη ευελιξία, περισσότερες επιλογές ανάπτυξης, ασφάλεια, συμβατότητα με όλα τα συστήματα και το όφελος να αξιοποιούν στο μέγιστο την υπάρχουσα υποδομή του δίνοντας της έτσι μεγαλύτερη αξία. Όταν η ζήτηση και η επεξεργασία των cloud services αυξομειώνεται, το υβριδικό νέφος (μέσω εσωτερικού συστήματος αυτόματου υπολογισμού ζήτησης) δίνει στις επιχειρήσεις τη δυνατότητα να ανεβάσουν γρήγορα και άκοπα την εσωτερική τους υποδομή (on-premises infrastructure) στο δημόσιο σύννεφο έτσι ώστε να είναι σε θέση να διαχειριστεί τυχόν υπερχείλιση-χωρίς να δώσει πρόσβαση στο σύνολο των δεδομένων τους ,σε κέντρα δεδομένων τρίτων παρόχων. Οι οργανισμοί αποκτούν την ευελιξία και την καινοτομία που παρέχει το δημόσιο «cloud» εκτελώντας συγκεκριμένο φόρτο εργασίας στο «cloud» διατηρώντας ταυτόχρονα τα εξαιρετικά ευαίσθητα δεδομένα στο δικό τους κέντρο δεδομένων για να καλύψουν τις ανάγκες του πελάτη ή τις οποιοσδήποτε απαιτήσεις προκύψουν.

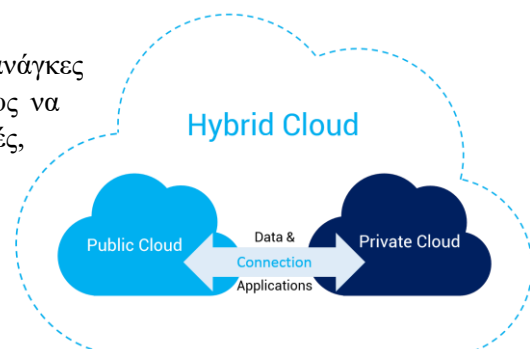
Αυτό όχι μόνο επιτρέπει στις εταιρείες να κλιμακώσουν τους υπολογιστικούς πόρους-εξαλείφει επίσης την ανάγκη να γίνουν μαζικές δαπάνες κεφαλαίου για τον χειρισμό βραχυπρόθεσμων αυξήσεων της ζήτησης, καθώς και όταν η επιχείρηση χρειάζεται να ελευθερώσει τοπικούς πόρους για πιο ευαίσθητα δεδομένα ή εφαρμογές. Οι εταιρείες θα πληρώσουν μόνο για πόρους που χρησιμοποιούν προσωρινά αντί να χρειαστεί να αγοράσουν, να προγραμματίσουν και να διατηρήσουν πρόσθετους πόρους και εξοπλισμό που θα μπορούσαν να παραμείνουν αδρανείς για μεγάλα χρονικά διαστήματα.

### Πλεονεκτήματα του υβριδικού νέφους:

- Έλεγχος - ο οργανισμός σας μπορεί να διατηρήσει μια ιδιωτική υποδομή για ευαίσθητα περιουσιακά στοιχεία ή εργασίες που απαιτούν χαμηλή καθυστέρηση.
- Ευελιξία – ο οργανισμός μπορεί να επωφεληθεί από πόρους στο δημόσιο «cloud» όταν τους χρειαστεί.
- Οικονομική αποδοτικότητα- η δυνατότητα κλιμάκωσης στο δημόσιο «cloud» δίνει την ευκολία στον χρήστη να πληρώνει για επιπλέον υπολογιστική ισχύ μόνο όταν αυτή χρειάζεται.
- Ευκολία - η μετάβαση στο σύννεφο δεν χρειάζεται να είναι μαζική και αμέσως, αυτό επειδή ο εκάστοτε οργανισμός μπορεί να μεταβεί σταδιακά – με το να προγραμματίσει σε φάσεις την μετάβαση στο «cloud» με την πάροδο του χρόνου.

### **Bonus Κοινοτικό νέφος (Community Cloud)**

Στην περίπτωση που κάποιοι πελάτες με παρόμοιες ανάγκες αποφασίζουν για λόγους οικονομίας κλίμακας ή άλλους να μοιραστούν κοινές υλικοτεχνικές υποδομές, εγκαταστάσεις, παραμετροποιήσεις αλλά και την ευθύνη της διαχείρισης του Cloud, τότε έχουμε το κοινοτικό υπολογιστικό σύννεφο. Η διαχείριση του Cloud στην περίπτωση αυτή μπορεί να γίνεται είτε από τα μέλη της κοινότητας είτε από εξουσιοδοτημένο τρίτο μέλος εκτός κοινότητας[56]



Εικόνα 61: Public, Private, Hybrid Cloud

## 6.7 Εισαγωγή στο Microsoft Azure

Το Microsoft Azure, γνωστό παλιότερα και ως Windows Azure, είναι η δημόσια πλατφόρμα υπολογιστικού νέφους της Microsoft. Παρέχει μια σειρά από υπηρεσίες «Cloud», συμπεριλαμβανομένων compute, analytics, storage και networking. Οι χρήστες μπορούν να επιλέξουν και να χρησιμοποιήσουν οποιαδήποτε από αυτές τις υπηρεσίες, για να αναπτύξουν και να κλιμακώσουν σε μεγαλύτερο βαθμό νέες εφαρμογές ή να τρέξουν ήδη υπάρχουσες εφαρμογές στο δημόσιο cloud (public clouds). Αυτό παρέχει στους χρήστες την ευελιξία να χρησιμοποιούν τα εργαλεία και τις τεχνολογίες που προτιμούν, αφού το Azure περιέχει μια γκάμα από εργαλεία και τεχνολογίες που μπορούν να ικανοποιήσουν κάθε λογής απαιτήσεις από εταιρείες που δραστηριοποιούνται στο ηλεκτρονικό εμπόριο και τα οικονομικά, μέχρι και εταιρείες που ανήκουν στις top 500, σύμφωνα με τα χρηματιστηριακά δεδομένα. Επιπλέον, το Azure προσφέρει 4 διαφορετικές μορφές cloud computing: υποδομή ως υπηρεσία (IaaS), πλατφόρμα ως υπηρεσία (PaaS), λογισμικό ως υπηρεσία (SaaS) και serverless computing.[57]

Επίσης, η πλατφόρμα cloud Azure αποτελείται από περισσότερα από 200 προϊόντα και υπηρεσίες cloud που έχουν σχεδιαστεί για να βοηθήσουν να δοθούν νέες λύσεις στους οργανισμούς και τις επιχειρήσεις έτσι ώστε να καταφέρουν να δημιουργήσουν να τρέξουν και να διαχειριστούν εφαρμογές σε διαφορετικά «νέφη» («clouds»), σε on-promises υποδομές ακόμα και σε συνδυασμό των δύο με εργαλεία και πλατφόρμες που βρίσκονται στην αιχμή της τεχνολογίας. Τέλος, η Microsoft χρεώνει το Azure με pay-as-you-go τιμολογιακή πολιτική, πράγμα που σημαίνει ότι οι συνδρομητές λαμβάνουν έναν λογαριασμό κάθε μήνα που τους χρεώνει μόνο για τους συγκεκριμένους πόρους που έχουν χρησιμοποιήσει κατά την περίοδο αυτή.[58]

## 6.8 Υπηρεσίες και εργαλεία που προσφέρει το Microsoft Azure

Επειδή το Microsoft Azure αποτελείται από πολλές υπηρεσίες και εργαλεία, οι περιπτώσεις χρήσης τους μπορούν να είναι εξαιρετικά διαφορετικές μεταξύ τους. Η πιο διαδεδομένη χρήση του Azure είναι για την εκτέλεση και την χρήση εικονικών μηχανημάτων (virtual machines) και containers. Άλλα παραδείγματα χρήσης του Microsoft Azure είναι η δημιουργία βάσεων δεδομένων, οι οποίες φιλοξενούνται στο cloud, όπως επίσης η χρήση του «νέφους» για να γίνονται backup εφαρμογές ακόμα και αρχεία εταιρειών για την διασφάλιση της προστασίας και της ακεραιότητας τους σε περίπτωση βλάβης των on-premises υποδομών. Αυτά είναι κάποια από τα εργαλεία που θα αναλυθούν εκτενέστερα παρακάτω και τα προσφέρει η πλατφόρμα του Microsoft Azure στους χρήστες.[57]

### 6.8.1 Υπηρεσίες και εργαλεία

**Compute:** Αυτές οι υπηρεσίες δίνουν τη δυνατότητα σε έναν χρήστη να αναπτύξει και να διαχειριστεί εικονικά μηχανήματα, κοντέινερ και batch jobs, καθώς και υποστήριξη απομακρυσμένης πρόσβασης σε εφαρμογές. Οι υπολογιστικοί πόροι που δημιουργούνται στο Azure cloud μπορούν να διαμορφωθούν είτε με δημόσιες διευθύνσεις IP είτε με ιδιωτικές διευθύνσεις IP, ανάλογα με το αν ο πόρος πρέπει να είναι προσβάσιμος σε εξωτερικούς παράγοντες.

**Mobile:** Αυτά τα προϊόντα βοηθούν τους προγραμματιστές να δημιουργήσουν εφαρμογές cloud για κινητές συσκευές, παρέχοντας υπηρεσίες ειδοποιήσεων, υποστήριξη για εργασίες back-end, εργαλεία για τη δημιουργία διεπαφών προγράμματος εφαρμογών (API).

**Web:** Αυτές οι υπηρεσίες υποστηρίζουν την ανάπτυξη και το deployments εφαρμογών Ιστού. Προσφέρουν επίσης δυνατότητες για αναζήτηση, παράδοση περιεχομένου, διαχείριση API, ειδοποιήσεις και αναφορά κατάστασης (reporting).

**Storage:** Αυτή η κατηγορία υπηρεσιών παρέχει κλιμακούμενη αποθήκευση στο cloud για δομημένα και μη δομημένα δεδομένα. Υποστηρίζει επίσης μεγάλα έργα δεδομένων (big data projects with data lakes and blobs), persistent storage και αρχειοθέτηση (archival storage).

**Analytics:** Αυτές οι υπηρεσίες παρέχουν καταναεμημένη ανάλυση και αποθήκευση, καθώς και λειτουργίες για αναλύσεις σε πραγματικό χρόνο, ανάλυση μεγάλων δεδομένων (big data analysis), λίμνες δεδομένων (data lakes), μηχανική μάθηση (ML), επιχειρηματική ευφυΐα (BI), internet of things (IoT) και αποθήκευση δεδομένων.

**Networking:** Αυτή η ομάδα περιλαμβάνει εικονικά δίκτυα, αποκλειστικές συνδέσεις και gateways, καθώς και υπηρεσίες διαχείρισης και διάγνωσης κυκλοφοριακής συμφόρησης στο δίκτυο, εξισορρόπησης φορτίου, DNS hosting και προστασίας δικτύου από επιθέσεις τύπου distributed denial-of-service (DDoS).

**Media and content delivery network (CDN):** Αυτές οι υπηρεσίες CDN παρέχουν on-demand streaming, προστασία ψηφιακών δικαιωμάτων, κωδικοποίηση και αναπαραγωγή πολυμέσων καθώς και ευρετήριο πολυμέσων.

**Integration:** Αυτές είναι υπηρεσίες για δημιουργία αντιγράφων ασφαλείας διακομιστή (server), ανάκτηση ιστότοπου και σύνδεση ιδιωτικών και δημόσιων cloud.

**Identity:** Αυτή η υπηρεσία προσφέρει την δυνατότητα της διασφάλισης ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση στις υπηρεσίες Azure και προστατεύουν τα κρυπτογραφημένα κλειδιά (encryption keys) και άλλες ευαίσθητες πληροφορίες στο cloud. Οι υπηρεσίες περιλαμβάνουν υποστήριξη για το Azure Active Directory και έλεγχο ταυτότητας με πολλούς διαφορετικούς τρόπους (MFA-multifactor authentication).

**Internet of things:** Αυτές οι υπηρεσίες βοηθούν τους χρήστες να καταγράφουν, να παρακολουθούν και να αναλύουν δεδομένα IoT από αισθητήρες και άλλες συσκευές. Στις υπηρεσίες αυτές περιλαμβάνονται και οι ειδοποιήσεις, analytics, monitoring και τεχνική υποστήριξη για ό,τι αφορά τον κώδικα και την εκτέλεση των εφαρμογών.

**DevOps:** Αυτή η ομάδα υπηρεσιών παρέχει εργαλεία για την προώθηση της συνεργασίας σε ένα έργο, όπως το Azure DevOps - πρώην Visual Studio Team Services - που διευκολύνουν τις διαδικασίες ανάπτυξης λογισμικού DevOps. Προσφέρει επίσης χαρακτηριστικά για τη διάγνωση εφαρμογών, εργαλεία integration του DevOps και εργαστήρια δοκιμών (test labs) για δοκιμές κατασκευής και πειραματισμούς πάνω σε εφαρμογές πριν το deployment.

**Development:** Αυτές οι υπηρεσίες βοηθούν τους προγραμματιστές εφαρμογών να μοιράζονται κώδικα, να δοκιμάζουν εφαρμογές και να παρακολουθούν πιθανά προβλήματα. Το Azure υποστηρίζει μια σειρά από γλώσσες προγραμματισμού εφαρμογών, όπως JavaScript, Python, .NET και Node.js. Τα εργαλεία αυτής της κατηγορίας περιλαμβάνουν επίσης τεχνική υποστήριξη για Azure DevOps, πακέτο ανάπτυξης λογισμικού (SDK- Software Development kits) και blockchain.

**Security:** Αυτά τα προϊόντα παρέχουν δυνατότητες αναγνώρισης και προστασίας από απειλές που θέτουν σε κίνδυνο την ασφάλεια στο cloud, καθώς και διαχείριση κλειδιών κρυπτογράφησης (encryption keys) και άλλων ευαίσθητων στοιχείων.

**Artificial intelligence (AI) και μηχανική μάθηση (ML):** Πρόκειται για ένα ευρύ φάσμα υπηρεσιών που ένας προγραμματιστής μπορεί να χρησιμοποιήσει για να εισάγει την τεχνητή νοημοσύνη, την μηχανική μάθηση και ικανότητες γνωστικού υπολογισμού (cognitive computing capabilities) σε εφαρμογές και σύνολα δεδομένων.

**Containers:** Αυτές οι υπηρεσίες βοηθούν μια επιχείρηση να δημιουργήσει, να καταχωρήσει, να ενορχηστρώσει και να διαχειριστεί τεράστιους όγκους κοντέινερ στο cloud Azure, χρησιμοποιώντας πλατφόρμες όπως το Docker και το Kubernetes.

**Databases:** Αυτή η κατηγορία περιλαμβάνει υπηρεσίες Database as a Service (DBaaS) για SQL και NoSQL, καθώς και άλλες περιπτώσεις βάσεων δεδομένων - όπως Azure Cosmos DB και Azure Database για PostgreSQL. Περιλαμβάνει επίσης τεχνική υποστήριξη Azure SQL Data Warehouse, λειτουργία προσωρινής αποθήκευσης (caching) και υβριδικής βάσης δεδομένων (hybrid database integration) και data migration χαρακτηριστικά. Το Azure SQL είναι η κορυφαία υπηρεσία βάσης δεδομένων της πλατφόρμας. Είναι μια σχεσιακή βάση δεδομένων που παρέχει λειτουργικότητα SQL χωρίς την ανάγκη ανάπτυξης ενός διακομιστή (server) SQL.

**Migration:** Αυτή η σειρά εργαλείων βοηθά έναν οργανισμό να εκτιμήσει το κόστος μετακίνησης του στο cloud και να πραγματοποιήσει την μετεγκατάσταση του από τα τοπικά κέντρα δεδομένων στο cloud Azure.

**Management and governance:** Αυτές οι υπηρεσίες παρέχουν μια σειρά από εργαλεία δημιουργίας αντιγράφων ασφαλείας, ανάκτησης (recovery), compliance, αυτοματοποίησης, προγραμματισμού και παρακολούθησης που μπορούν να βοηθήσουν έναν cloud administrator manager να διαχειριστεί ένα deployment στο Azure.

**Mixed reality:** Αυτές οι υπηρεσίες έχουν σχεδιαστεί για να βοηθούν τους προγραμματιστές να δημιουργούν περιεχόμενο για το περιβάλλον των Windows Mixed Reality.

**Blockchain:** Η υπηρεσία Azure Blockchain σας επιτρέπει να συμμετάσχετε σε μια κοινοπραξία blockchain (consortium) ή να δημιουργήσετε τη δική σας.

**Intune:** Το Microsoft Intune μπορεί να χρησιμοποιηθεί για την εγγραφή συσκευών χρήστη, καθιστώντας έτσι δυνατή την προώθηση πολιτικών ασφαλείας και εφαρμογών για κινητά σε αυτές τις συσκευές. Οι εφαρμογές για κινητά μπορούν να αναπτυχθούν είτε σε ομάδες χρηστών είτε σε μια συλλογή συσκευών. Το Intune παρέχει επίσης εργαλεία για την παρακολούθηση των εφαρμογών που χρησιμοποιούνται. Μια λειτουργία διαγραφής δεδομένων από απόσταση η αλλιώς «σκουπίσματος από μακριά» («remote wipe») επιτρέπει την ασφαλή αφαίρεση των δεδομένων του οργανισμού από τις συσκευές χωρίς την διαγραφή άλλων εφαρμογών για κινητά ενός χρήστη κατά τη διαδικασία.

### **6.8.2 Τιμολογιακές πολιτικές του Microsoft Azure**

Μια συνδρομή Azure παρέχει πρόσβαση σε πόρους Azure, όπως εικονικές μηχανές (VM), χώρο αποθήκευσης και βάσεις δεδομένων. Μόλις οι πελάτες εγγραφούν στο Azure, έχουν πρόσβαση σε όλες τις υπηρεσίες που περιλαμβάνονται στην πύλη Azure. Οι συνδρομητές μπορούν να χρησιμοποιήσουν αυτές τις υπηρεσίες για να δημιουργήσουν πόρους που βασίζονται στο cloud, όπως εικονικές μηχανές (VM) και βάσεις δεδομένων. Οι τύποι πόρων που χρησιμοποιείτε επηρεάζουν τον μηνιαίο λογαριασμό σας.[59]Το Azure προσφέρει δωρεάν αλλά και συνδρομητικές επιλογές subscription για να ταιριάζει στις ανάγκες και τις απαιτήσεις του εκάστοτε χρήστη. Αυτές είναι οι ακόλουθες:

#### **Free trial**

Μια δωρεάν δοκιμαστική συνδρομή παρέχει στον χρήστη 12 μήνες δημοφιλών δωρεάν υπηρεσιών, πίστωση για να εξερευνήσει οποιαδήποτε υπηρεσία Azure για 30 ημέρες και περισσότερες από 25 υπηρεσίες που είναι πάντα δωρεάν. Οι υπηρεσίες Azure απενεργοποιούνται όταν λήξει η δοκιμαστική περίοδος ή όταν λήξει η πίστωση (περίπου στα 250 ευρώ) για προϊόντα επί πληρωμή, εκτός εάν κάνετε αναβάθμιση σε συνδρομή επί πληρωμή.

## Pay-as-you-go

Μια συνδρομή pay-as-you-go δίνει τη δυνατότητα στον χρήστη να πληρώσει για αυτούς τους πόρους που χρησιμοποιεί, αλλά συνδέοντας μια πιστωτική ή χρεωστική κάρτα στο λογαριασμό του. Οι οργανισμοί μπορούν να υποβάλουν αίτηση για μαζικές εταιρικές εκπτώσεις και προπληρωμένη τιμολόγηση.

## Member offers

Τα member offers τα δικαιούνται χρήστες που έχουν πληρώσει άλλες συνδρομητικές υπηρεσίες η προϊόντα που σχετίζονται με την Microsoft. Κάποια παραδείγματα προϊόντων που τα μέλη τους έχουν την ευκαιρία προσφοράς στο Azure είναι τα μέλη του Visual Studio, στα μέλη του Microsoft Partner Network, στα μέλη της Microsoft for Startups και στα μέλη της Microsoft Imagine.

Εκτός από τις υπηρεσίες που προσφέρει η Microsoft μέσω της πύλης Azure (Azure Portal), ένας αριθμός τρίτων προμηθευτών καθιστά επίσης άμεσα διαθέσιμο το λογισμικό του μέσω του Azure. Το κόστος που χρεώνεται για εφαρμογές τρίτων ποικίλλει, αλλά κάποιες φορές μπορεί να περιλαμβάνει την πληρωμή συνδρομής για την εφαρμογή, καθώς και το τέλος χρήσης για την υποδομή που χρησιμοποιείται για τη φιλοξενία της εφαρμογής.

Η Microsoft παρέχει πέντε διαφορετικές επιλογές υποστήριξης πελατών για το Azure:

- Basic
- Developer
- Standard
- Professional Direct
- Premier

Αυτά τα σχέδια υποστήριξης πελατών διαφέρουν ως προς το εύρος και την τιμή. Η βασική υποστήριξη είναι διαθέσιμη σε όλους τους λογαριασμούς Azure, αλλά η Microsoft χρεώνει ένα ποσό για τις άλλες επιπρόσθετες υπηρεσίες υποστήριξης. Αναλυτικά τα κόστη όπως και οι υπηρεσίες που προσφέρονται για κάθε βαθμίδα φαίνονται στο παρακάτω γράφημα:

	Basic	DEVELOPER	STANDARD	PROFESSIONAL DIRECT
	<a href="#">Request support</a>	<a href="#">Purchase support</a>	<a href="#">Purchase support</a>	<a href="#">Purchase support</a>
Price	Included for all Azure customers	\$29 per month	\$100 per month	\$1,000 per month
Scope	Included for all Azure customers	Trial and non-production environments	Production workload environments	Business-critical dependence
Billing and subscription management support	✓	✓	✓	✓
24/7 self-help resources, including <a href="#">Microsoft Learn</a> , <a href="#">Azure portal how-to videos</a> , <a href="#">documentation</a> , and <a href="#">community support</a>	✓	✓	✓	✓
Ability to submit as many support tickets as you need	✓	✓	✓	✓
<a href="#">Azure Advisor</a> —your free, personalized guide to Azure best practices	✓	✓	✓	✓
<a href="#">Azure health status and notifications</a>	✓	✓	✓	✓
Third-party software support with interoperability and configuration guidance and troubleshooting		✓	✓	✓
24/7 access to technical support by email and phone after a support request is submitted		Available during business hours by email only.	✓	✓
<a href="#">Case severity and response time</a>		Minimal business impact (Sev C): Within eight business hours <sup>1</sup>	Minimal business impact (Sev C): Within eight business hours <sup>2</sup> Moderate business impact (Sev B): Within four hours Critical business impact (Sev A): Within one hour	Minimal business impact (Sev C): Within four business hours <sup>3</sup> Moderate business impact (Sev B): Within two hours Critical business impact (Sev A): Within one hour

Εικόνα 62: Azure Cost Policies

## 6.9 Χρήση του Azure για το deployment του web-app στο cloud

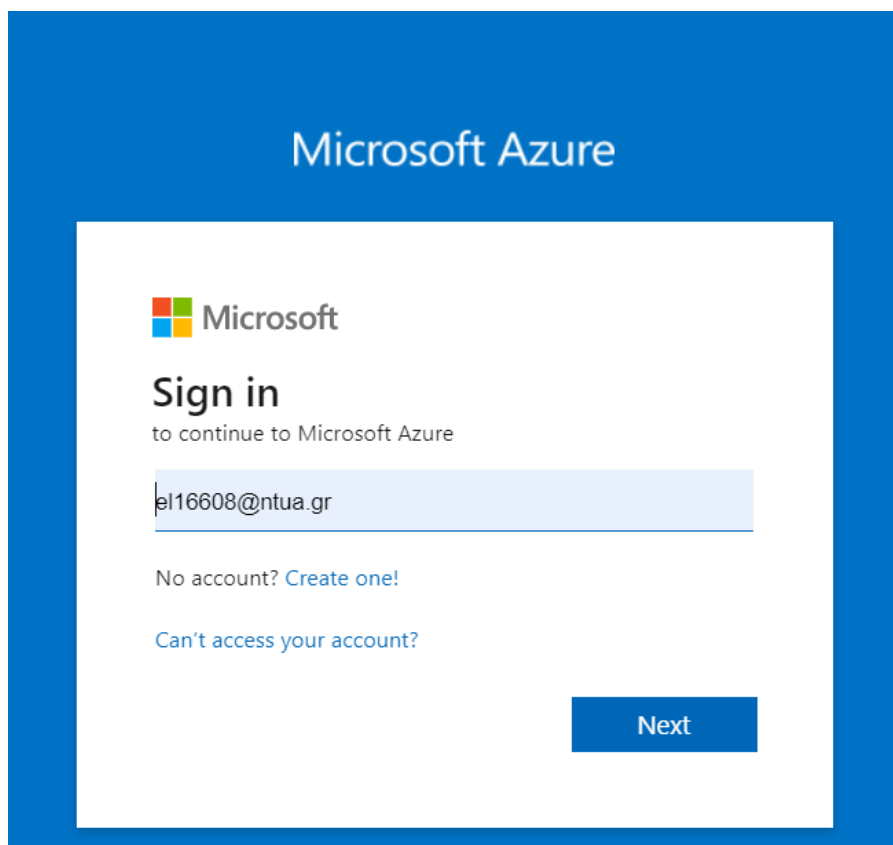
Λαμβάνοντας υπόψιν την έρευνα, που παρέθεσα συνοπτικά στα προηγούμενα κεφάλαια, γύρω από το cloud computing και τις υπηρεσίες που προσφέρει η Microsoft με την πλατφόρμα του Azure ήταν αναπόφευκτο το επόμενο βήμα στην διπλωματική μου εργασία να ήταν το ολικό migration του web-app (“Certified”), που ανέπτυξα, στο cloud του Azure.[60][61]

Έτσι, η λύση που προτείνουμε με αυτή την εφαρμογή, για την πιστοποίηση δικαιολογητικών και εγγράφων μέσω APIs, που βασίζονται στην τεχνολογία του blockchain, γίνεται πλέον πιο σύγχρονη, χρησιμοποιώντας εργαλεία και υπηρεσίες ανάπτυξης λύσεων στο “Cloud”, τα οποία αποτελούν τεχνολογική αιχμή, επιτυγχάνοντας έτσι να μεταφέρουμε την εφαρμογή από τον τοπικό μας υπολογιστή (on-premises infrastructure) στο «Νέφος» και ακολουθώντας το κύμα της τεχνολογικής πρόοδου του παρόντος.

### 6.9.1 Δημιουργία λογαριασμού στο Microsoft Azure

Αρχικά, έπρεπε να εγγραφούμε στην πλατφόρμα του Azure Portal για να μπορέσουμε να χρησιμοποιήσουμε τις υπηρεσίες του. Η Microsoft γενικότερα προωθεί τα προϊόντα της στους φοιτητές και μαθητές, προσφέροντάς τους ελκυστικές τιμές, εκπτώσεις πάνω στα προϊόντα της ή πολλές φορές δίνει ακόμα και δωρεάν πρόσβαση σε αυτά.

- Έτσι και εμείς εκμεταλλευτήκαμε το γεγονός αυτό και εγγραφήκαμε στο Azure Portal με τον ιδρυματικό μας λογαριασμό.

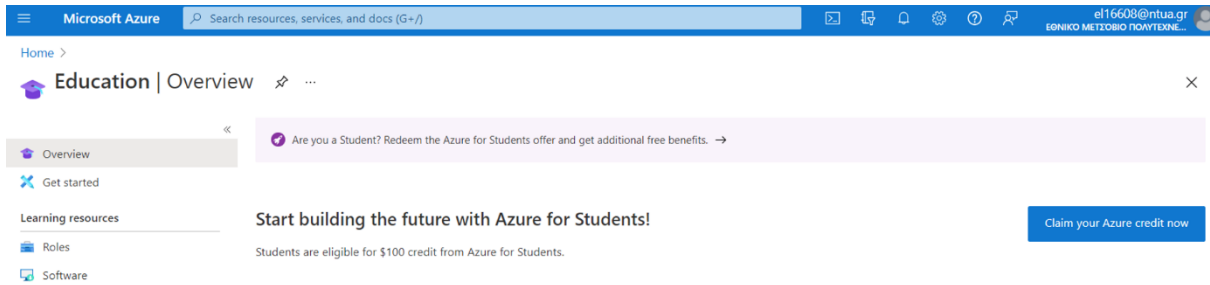


Εικόνα 63: Azure Sign In with University Account



-Έπειτα γίνεται η ταυτοποίηση μέσω του διακομιστή του Εθνικού Μετσόβιου Πολυτεχνείου και έχουμε πρόσβαση στο Azure Portal σαν φοιτητές.

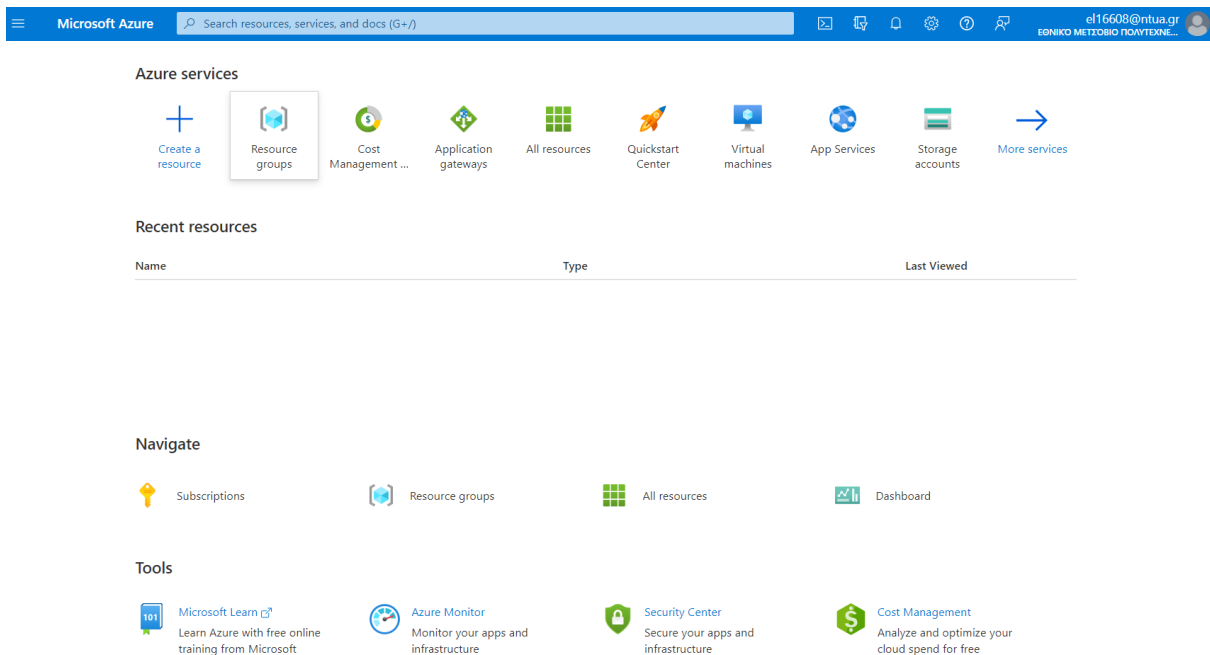
-Αυτό μας δίνει το δικαίωμα να αποκτήσουμε κάποια free credits (100 ευρώ περίπου) από την Microsoft με σκοπό να τα ξοδέψουμε στις υπηρεσίες και τα εργαλεία του Azure.



Εικόνα 64: Azure Student Account

-Αυτό το πακέτο συνδρομής που χρησιμοποιήσαμε συγκαταλέγεται μέσα στην pay-as-you-go τιμολογιακή πολιτική αφού όταν τελειώσει το free credit που έχουμε δικαίωμα ως φοιτητές θα πρέπει να πληρώνουμε ανάλογα την χρήση των πόρων που χρησιμοποιούμε.

-Όταν συνδεθούμε με τον ιδρυματικό λογαριασμό έχουμε πρόσβαση στο Azure Portal και όλες τις υπηρεσίες και τα εργαλεία που προσφέρει.

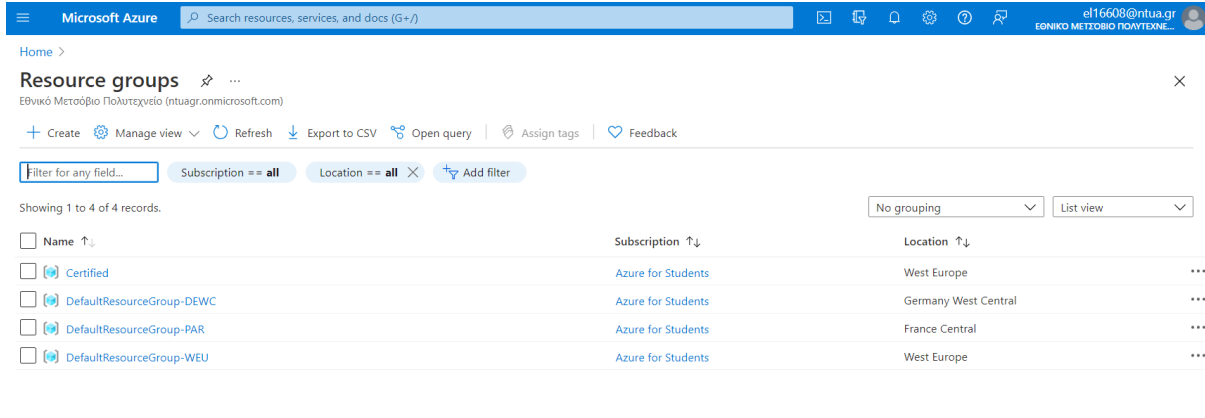


Εικόνα 65: Azure Portal main Page

## 6.9.2 Δημιουργία Resource Group στο Azure

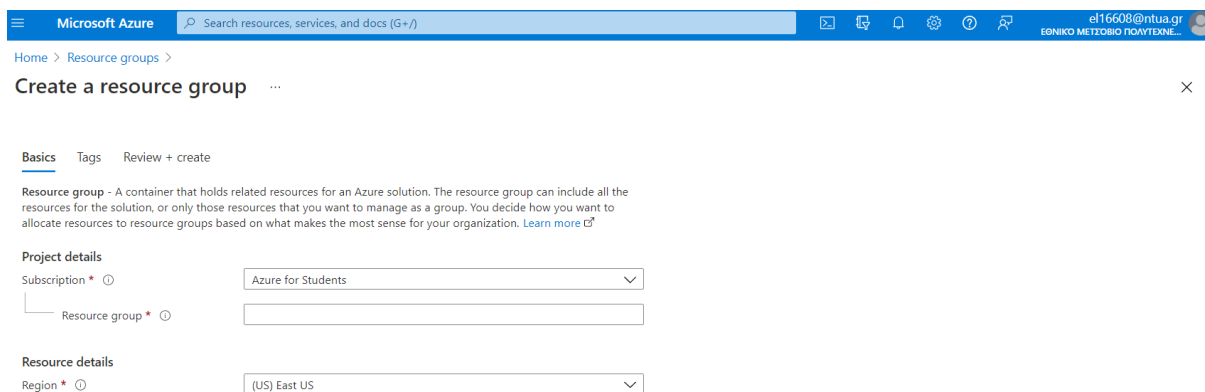
-Αρχικά, πριν κάνουμε οτιδήποτε άλλο πρέπει να δημιουργήσουμε ένα Resource Group στο Azure Portal ή αλλιώς μια ομάδα που θα φιλοξενήσει όλους τους πόρους που θα χρειαστούμε για το deployment του web-app.

-Από την κεντρική οθόνη του Azure Portal επιλέγουμε τα Resource Groups.



Εικόνα 66: Resource Groups

-Και έπειτα το κουμπί Create a Group για να δημιουργήσουμε το δικό μας Resource Group.



Εικόνα 67: Create a Resource Group

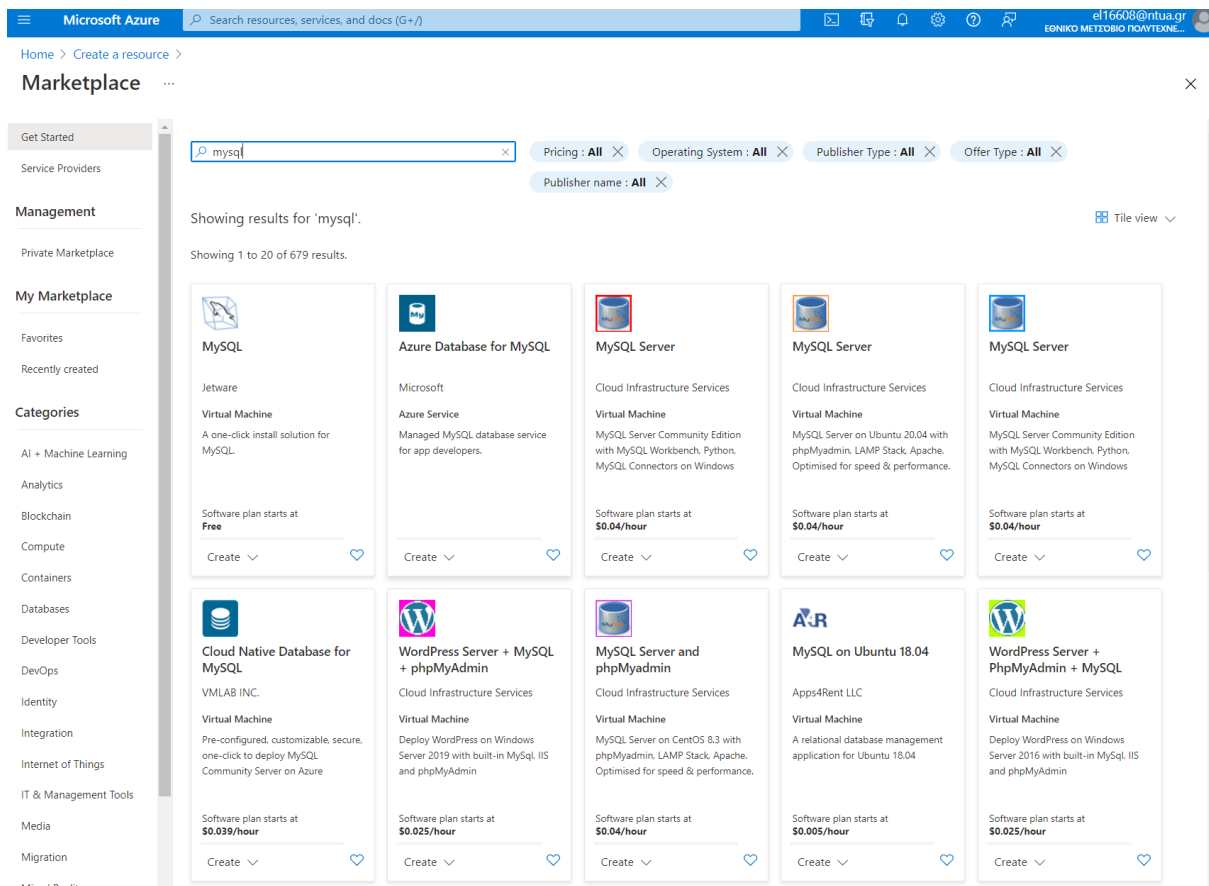
-Συμπληρώνουμε τα στοιχεία της φόρμας βάζοντας το Student Subscriptions για το οποίο έχουμε πρόσβαση, ένα όνομα μοναδικό για το γκρουπ που θα δημιουργήσουμε καθώς και την περιφέρεια στην οποία ανήκει η χώρα μας (για να βρει διακομιστές όσο το δυνατόν πιο κοντά σε εμάς).

-Η δημιουργία του Resource Group θα μας βοηθήσει στο να επεξεργαζόμαστε και να αξιοποιούμε τους πόρους σαν σύνολο αφού θα έχουν άμεση σχέση μεταξύ τους.

## 6.9.3 Δημιουργία της βάσης δεδομένων στο cloud

-Για να έχουμε πλήρη ανάπτυξη της εφαρμογής μας στο «νέφος» θα πρέπει να μεταφέρουμε αρχικά την βάση δεδομένων στο cloud.

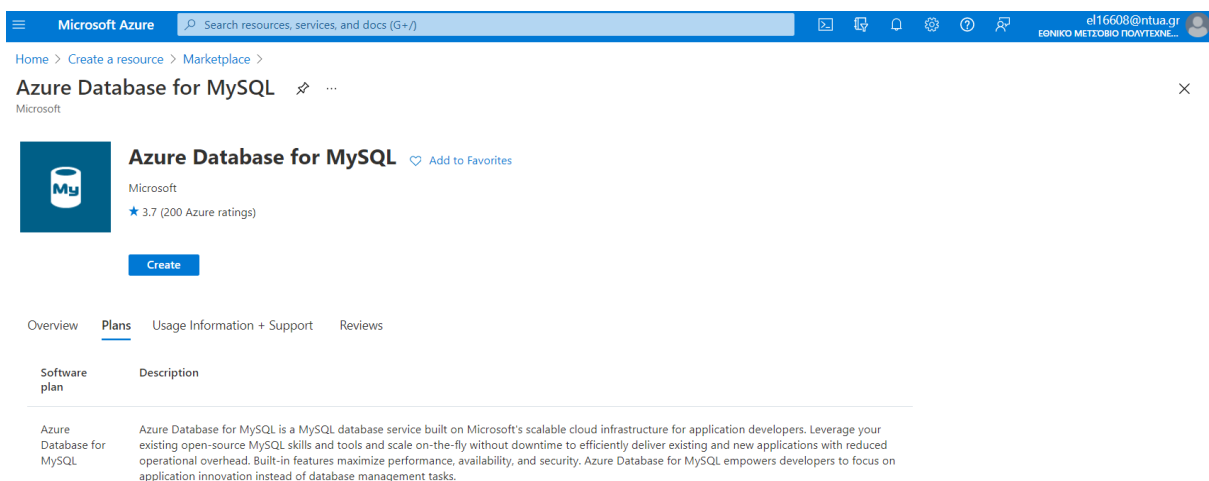
-Από την αρχική οθόνη του Azure Portal επιλέγουμε το κουμπί create a resource το οποίο μας κατευθύνει στο market place της πλατφόρμας.



Εικόνα 68: Azure marketplace

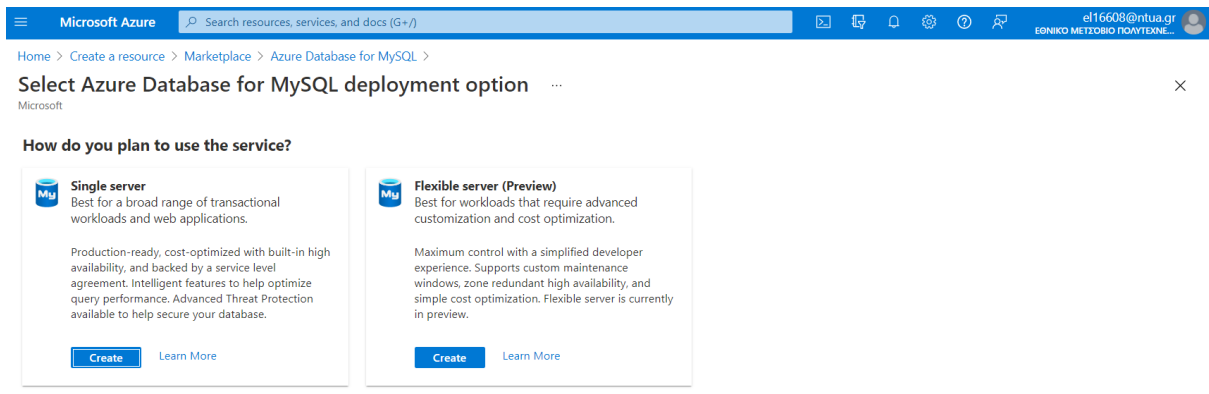
-Στο market place θα ψάξουμε για υπηρεσία του azure που θα μας προσφέρει πρόσβαση σε MySQL βάση δεδομένων αφού και την εφαρμογή μας την αναπτύξαμε με MySQL database τοπικά χρησιμοποιώντας το MySQL Workbench.

-Επιλέγουμε την υπηρεσία Azure Database for MySQL και στην συνέχεια θα δημιουργήσουμε έναν SQL server που θα φιλοξενήσει την βάση μας.



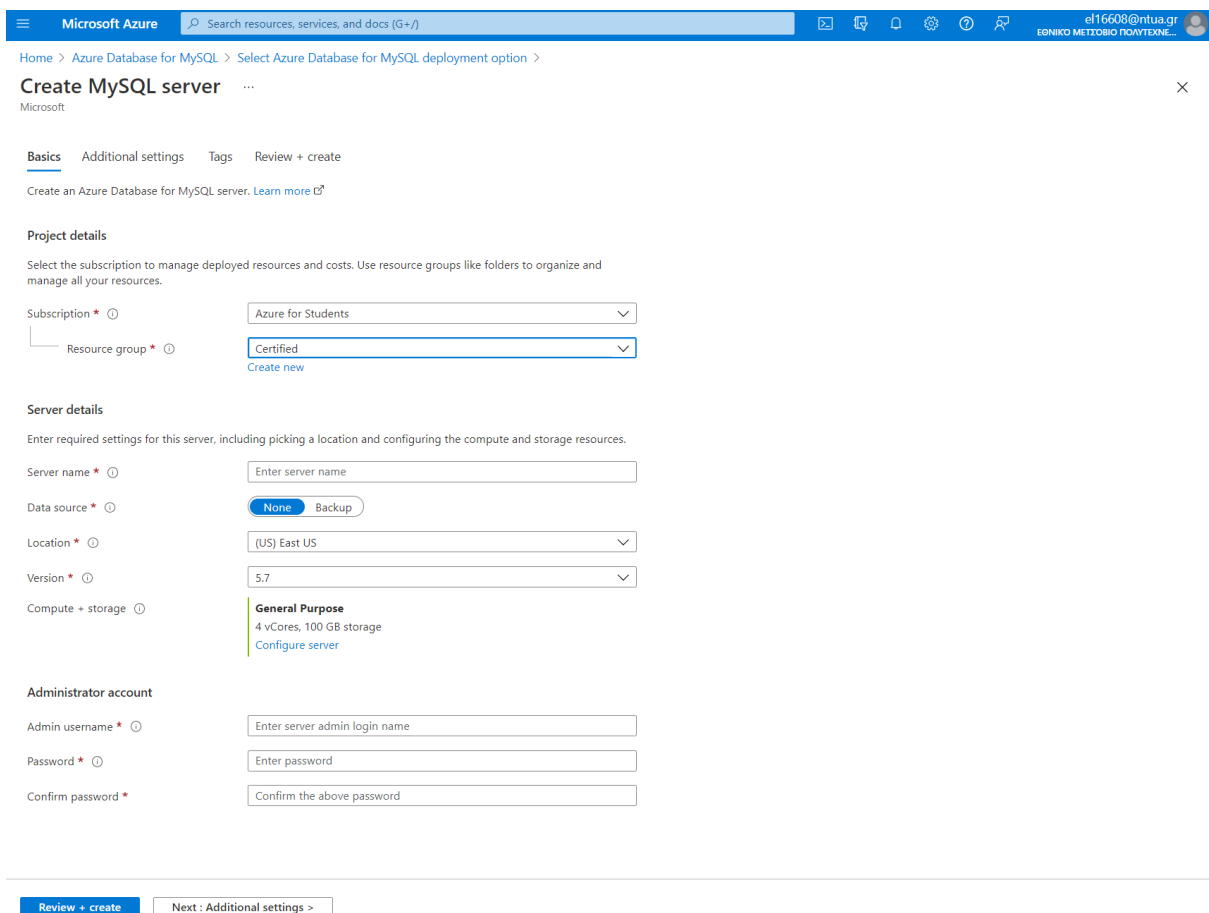
Εικόνα 69: Azure Database for MySQL

-Στη συνέχεια μας δίνεται η δυνατότητα να επιλέξουμε τον τύπο server θέλουμε να χρησιμοποιήσουμε για να ανεβάσουμε την βάση μας. Επιλέγουμε τον μονό server γιατί δεν έχουμε απαιτητικές διαδικασίες στην βάση μας που θα χρειαστούν ένα πιο ευέλικτο server για να διαχειρίζεται το workload.



Εικόνα 71: MySQL deployment options

-Έπειτα συμπληρώνουμε την φόρμα για την δημιουργία του MySQL server με τα απαραίτητα στοιχεία (όνομα server, admin username και password, το Resource Group που δημιουργήσαμε προηγουμένως, το region που θέλουμε να βρίσκεται ο server).



Εικόνα 70: Create MySQL server

-Το αμέσως επόμενο βήμα είναι να καθορίσουμε την τιμολογιακή πολιτική που θα θέλαμε βάση των πόρων που υπολογίζουμε πως θα χρησιμοποιήσουμε (configure server) . Βλέπουμε πως η πρόβλεψη κόστους του server που θα ανεβάσουμε είναι περίπου στα 25 ευρώ τον μήνα με τα χαρακτηριστικά που φαίνονται στην παρακάτω εικόνα.

The screenshot displays the 'Pricing tier' configuration page in the Azure portal. It features three columns for different compute tiers: Basic (up to 2 vCores), General Purpose (up to 64 vCores), and Memory Optimized (up to 32 memory optimized vCores). The 'Basic' tier is selected. Below the tiers, there are several configuration sections: 'Compute Generation' with 'Gen 5' selected; 'vCore' with a slider set to '1 vCore'; 'Storage' with a slider set to '5 GB'; 'Storage Auto-growth' with 'Yes' selected; 'Backup Retention Period' with a slider set to '7 Days'; and 'Backup Redundancy Options' with 'Locally Redundant' selected. A 'PRICE SUMMARY' box on the right indicates a total 'EST. MONTHLY COST' of 24.96. An 'OK' button is at the bottom left.

Εικόνα 73: MySQL pricing tier

-Μας δίνεται η δυνατότητα να δούμε μια προεπισκόπηση του server πριν τον ανεβάσουμε online. Με την επιλογή create ο server της βάση μας πλέον είναι διαθέσιμος.

The screenshot shows the 'Create MySQL server' page in the Azure portal, specifically the 'Review + create' step. The page includes a navigation bar with 'Basics', 'Additional settings', 'Tags', and 'Review + create'. Under 'Product details', it lists 'Azure Database for MySQL by Microsoft' with an 'Estimated cost per month' of 24.96 EUR. Below this, there are 'Terms' and 'Basics' sections. The 'Basics' section contains a table of configuration details:

Subscription	Azure for Students
Resource group	Certified
Server name	mysqlcertified
Data source	None
Server admin login name	dampap
Location	West Europe
Version	8.0
Compute + storage	Basic, Gen5, 1 vCores, 5 GB Storage
Backup retention period	7 day(s)
Backup redundancy	Locally redundant
Storage Auto Grow	Enabled

Εικόνα 72: MySQL server preview

-Μπορούμε να τροποποιήσουμε και να διαχειριστούμε το οτιδήποτε θέλουμε στον server μέσω της διεπαφής χρήστη της υπηρεσίας Azure Database for MySQL. Εκεί θα βρούμε πολλά εργαλεία και

τεχνολογίες που βοηθούν στην διαχείριση, παρακολούθηση, επίλυση προβλημάτων, ανάλυση στατιστικών, τιμολογιακής πολιτικής και άλλα πολλά που έχουν να κάνουν με τον server που σηκώσαμε.

The screenshot shows the Azure portal interface for a MySQL server named 'mysqlcertified'. The left sidebar contains navigation options like Overview, Activity log, Access control, and Settings. The main content area is divided into 'Essentials' (server details), 'Resource utilization' (a line graph showing CPU and storage usage), and 'Features' (Intelligent Performance and Read replicas, both currently not configured).

Εικόνα 74: mysqlcertified database created

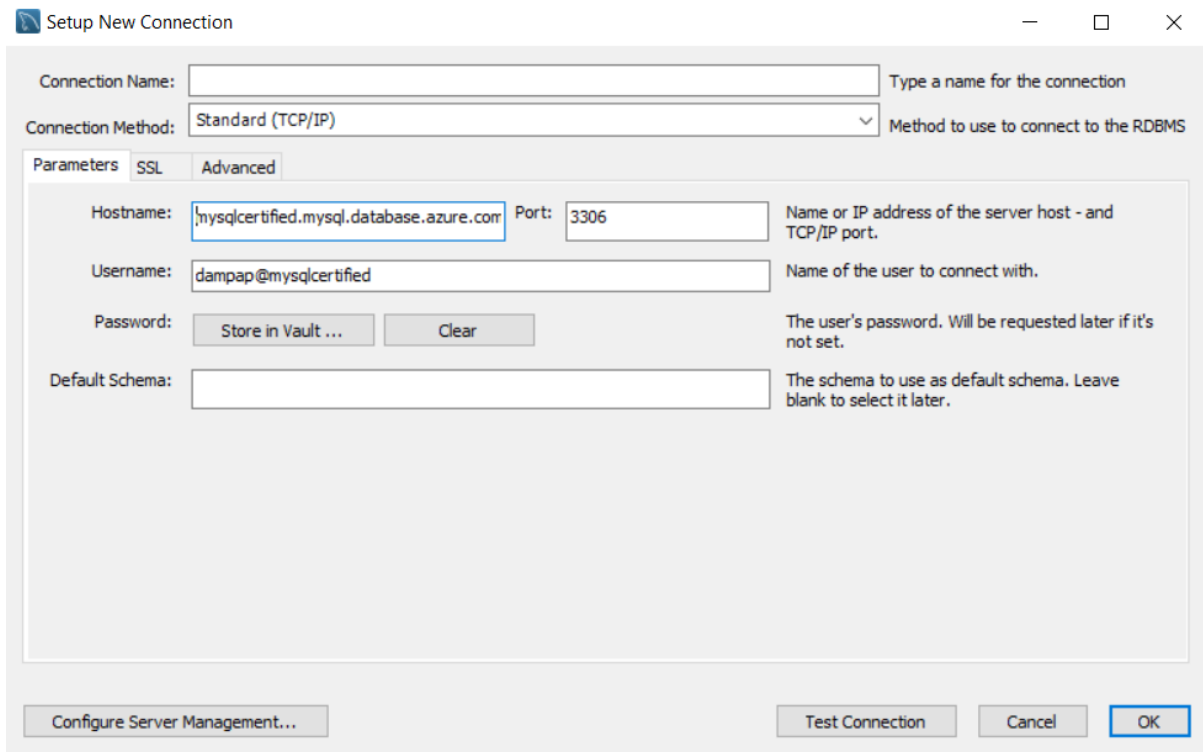
-Το επόμενο βήμα είναι ίσως και το σημαντικότερο. Με την χρήση του εργαλείου Security δίνουμε πρόσβαση στην διεύθυνση IP του υπολογιστή μας έτσι ώστε να μην μας σταματήσει το firewall του server που στήσαμε από το να κάνουμε login σε αυτόν και να διαχειριστούμε την βάση μας.

The screenshot displays the 'Connection security' configuration page for the 'mysqlcertified' database. It features a 'Firewall rules' section with a table listing existing rules. Below this, there are 'SSL settings' and 'TLS setting' sections, both with configuration options like 'ENABLED/DISABLED' buttons and dropdown menus.

Firewall rule name	Start IP	End IP
ClientIPAddress_2021-9-9_15-44-16	79.129.176.90	79.129.176.90

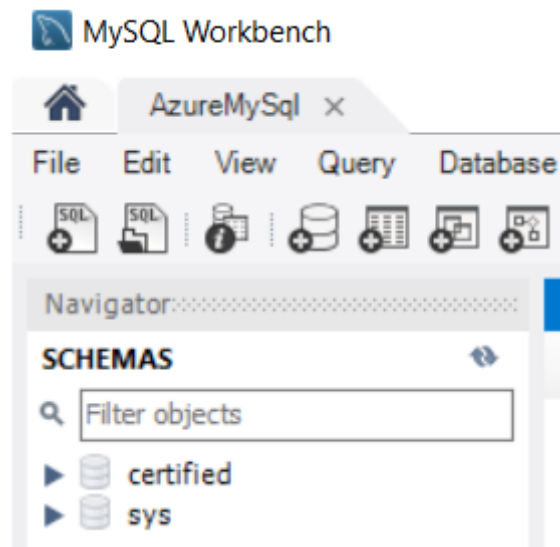
Εικόνα 75: Configure database security (firewall)

-Ακολουθώντας συνδεόμαστε στον MySQL server που τώρα βρίσκεται online με τα στοιχεία τα οποία δηλώσαμε κατά την δημιουργία του.



Εικόνα 76: Connect through MySQL Workbench to Azure Database

-Τέλος δημιουργούμε μια βάση δεδομένων στον server μας με το όνομα “certified” η οποία θα γεμίσει αυτόματα με τα απαραίτητα στοιχεία και πίνακες όταν θα τρέξουμε την εφαρμογή μας .



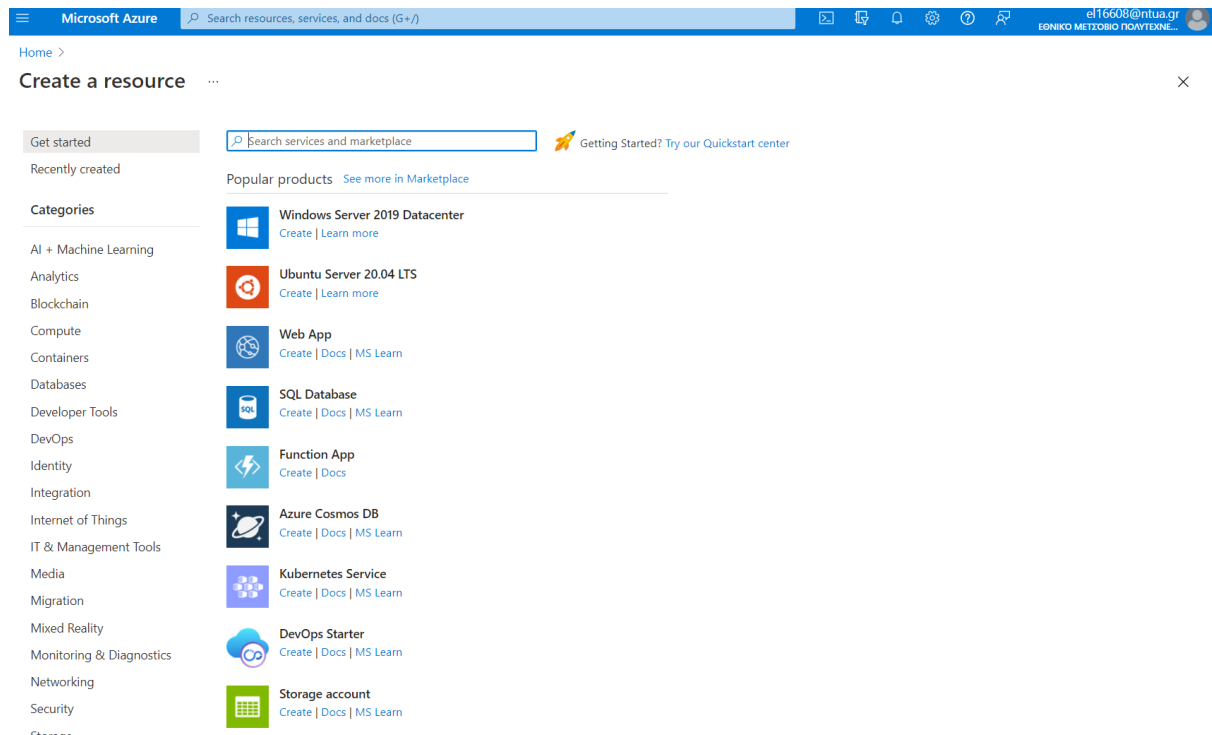
Εικόνα 77: Create new scheme in Azure database

### 6.9.4 Δημιουργία Web App Service

-Στην υπηρεσία Web App θα κάνουμε deploy τον κώδικα της εφαρμογής μας έτσι ώστε να ολοκληρωθεί η μετάβαση στο «νέφος».

-Με παρόμοιο τρόπο (με τον τρόπο που αναφέραμε προηγούμενος για την δημιουργία της βάσης δεδομένων) από την αρχική οθόνη του Azure Portal επιλέγουμε το κουμπί create a resource, το οποίο μας κατευθύνει στο market place της πλατφόρμας.

-Στο market place θα ψάξουμε για υπηρεσία Web App του Azure και θα επιλέξουμε create.



Εικόνα 78: WebApp in Azure marketplace

-Στη συνέχεια συμπληρώνουμε την φόρμα για την δημιουργία της υπηρεσίας Web App. Το Resource Group που δημιουργήσαμε και περιέχει και τον server της βάσης μας, το μοναδικό όνομα της εφαρμογής μας, την γλώσσα του κώδικα που είναι γραμμένο η εφαρμογή που θέλουμε να κάνουμε deploy, το λειτουργικό σύστημα, την περιφέρεια που θέλουμε να τρέχει ο διακομιστής μας καθώς και τον τύπο server που θα τρέχει πάνω η εφαρμογή.

-Εμείς επιλέξαμε Java SE στο πεδίο Java web server stack που ουσιαστικά είναι ο ενσωματωμένος διακομιστής στον ιστό. Αυτό το κάναμε γιατί γλιτώνουμε περιττά βήματα, αφού ο ενσωματωμένος server επικοινωνεί απευθείας με την εφαρμογή μας. Αν επιλέγαμε κάποιον άλλο server, για παράδειγμα έναν Tomcat, τότε θα εισάγαμε στην διαδικασία περιττή πολυπλοκότητα, αφού ο ενσωματωμένος διακομιστής θα επικοινωνούσε με τον Tomcat και ο Tomcat μετέπειτα με την εφαρμογή μας. Αυτή η μέθοδος που χρησιμοποιήσαμε θεωρείται η πιο σύγχρονη, αφού μεγάλες εφαρμογές γίνονται deploy στο «Cloud» μέσω του embed server, αποφεύγοντας το stacking άλλου διακομιστή πάνω στον ενσωματωμένο.



Microsoft Azure Search resources, services, and docs (G+)

Home > Create a resource >

## Create Web App

App Service Web Apps lets you quickly build, deploy, and scale enterprise-grade web, mobile, and API apps running on any platform. Meet rigorous performance, scalability, security and compliance requirements while using a fully managed platform to perform infrastructure maintenance. [Learn more](#)

**Project Details**

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*

Resource Group \*  [Create new](#)

**Instance Details**

Need a database? Try the new Web + Database experience.

Name \*  .azurewebsites.net

Publish \*  Code  Docker Container

Runtime stack \*

Java web server stack \*

Operating System \*  Linux  Windows

Region \*    
 [Not finding your App Service Plan? Try a different region.](#)

**App Service Plan**

App Service plan pricing tier determines the location, features, cost and compute resources associated with your app. [Learn more](#)


Linux Plan (West Europe) \*  [Create new](#)

Skus and size \* **Basic B1**  
100 total ACU, 1.75 GB memory


Εικόνα 79: Create a WebApp form

-Αμέσως επόμενο βήμα είναι να επιλέξουμε τα χαρακτηριστικά της εφαρμογής μας. Επιλέγουμε ένα πακέτο που απευθύνεται σε Dev/Test, αφού δεν έχουμε μια απαιτητική εφαρμογή, δηλαδή με αυξημένη κίνηση και φόρτο εργασίας.


### Spec Picker



**Dev / Test**  
For less demanding workloads



**Production**  
For most production workloads



**Isolated**  
Advanced networking and scale

**i** The first Basic (B1) core for Linux is free for the first 30 days!

**Recommended pricing tiers**

**F1**

1 GB memory  
60 minutes/day compute  
Free

**B1**

100 total ACU  
1.75 GB memory  
A-Series compute equivalent  
12.31 EUR/Month (Estimated)

[See additional options](#)

**Included features**

Every app hosted on this App Service plan will have access to these features:

- Custom domains / SSL**  
Configure and purchase custom domains with SNI SSL bindings
- Manual scale**  
Up to 3 instances. Subject to availability.

**Included hardware**

Every instance of your App Service plan will include the following hardware configuration:

- Azure Compute Units (ACU)**  
Dedicated compute resources used to run applications deployed in the App Service Plan. [Learn more](#)
- Memory**  
Memory per instance available to run applications deployed and running in the App Service plan.
- Storage**  
10 GB disk storage shared by all apps deployed in the App Service plan.

Εικόνα 80: Configure WebApp characteristics

-Πατώντας create μας εμφανίζεται μια προεπισκόπηση της υπηρεσίας που ρυθμίσαμε και τελικά έχουμε online το Web App service μας.

## Create Web App

Basics Deployment Monitoring Tags **Review + create**

Summary

**Web App**  
by Microsoft

Details

Subscription: ac014411-180e-4a2e-86ab-1297906e67b7  
 Resource Group: Certified  
 Name: certified-web-app  
 Publish: Code  
 Runtime stack: Java 8  
 Java web server stack: Java SE (Embedded Web Server)

App Service Plan

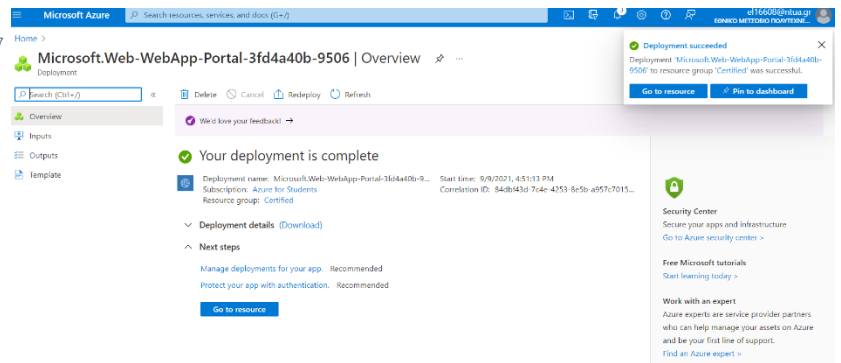
Name: certified-webapp  
 Operating System: Linux  
 Region: West Europe  
 SKU: Basic  
 Size: Small  
 ACU: 100 total ACU  
 Memory: 1.75 GB memory

Monitoring

Application Insights: Not enabled

Deployment

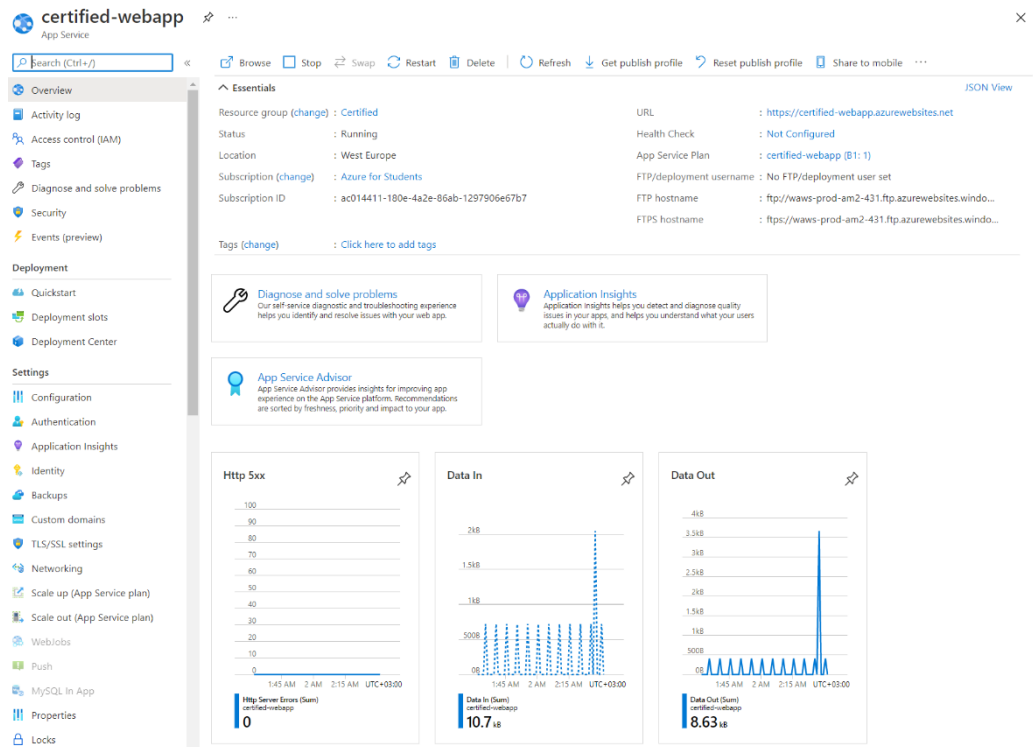
Continuous deployment: Not enabled / Set up after app creation



Εικόνα 81: WebApp deployment complete

## Εικόνα 82: Create WebApp preview

-Από την διεπαφή χρήστη της υπηρεσίας μπορούμε να βρούμε πολλά εργαλεία που βοηθούν στην διαχείριση του web app.



Εικόνα 83: Azure WebApp main page

-Αυτό είναι το σημαντικότερο βήμα για να πετύχει το deployment της εφαρμογής μας. Το group των servers, που βρίσκεται πίσω από την υπηρεσία web app, θα χρειαστεί να πάρει πληροφορίες και δεδομένα από την βάση δεδομένων που στήσαμε στο «Νέφος» προηγουμένως. Όπως ξέρουμε ήδη ο κάθε διακομιστής χαρακτηρίζεται από την μοναδική του διεύθυνση IP. Αυτές οι διευθύνσεις IP στην προσπάθειά τους να χτυπήσουν στην βάση, θα κόβονται από το firewall του διακομιστή της βάσης που στήσαμε, γιατί πολύ απλά δεν θα τις αναγνωρίζει. Για αυτόν τον λόγο εμείς, με την βοήθεια του εργαλείου security της υπηρεσίας Azure Database for MySQL, θα προσθέσουμε τις IP διευθύνσεις των server του App Service.

mysqlcertified | Connection security ...

Azure Database for MySQL server

Search (Ctrl+/) << Save Discard + Add client IP

Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems

Settings

Connection security  
Connection strings  
Server parameters  
Active Directory admin  
Pricing tier  
Properties  
Locks

Intelligent Performance

Query Performance Insight  
Performance recommendations

Monitoring

Alerts  
Metrics  
Diagnostic settings

Firewall rules

Some network environments may not report the actual public-facing IP address needed to access your server. Contact your network administrator if adding your IP address does not allow access to your server.

Allow access to Azure services  No  Yes

+ Add current client IP address (79.129.181.38) + Add 0.0.0.0 - 255.255.255.255

Firewall rule name	Start IP	End IP
AllowAll_2021-9-10_12-9-18	0.0.0.0	255.255.255.255
ClientIPAddress_2021-9-9_15-44-16	79.129.176.90	79.129.176.90

Firewall rule name Start IP End IP

SSL settings

Enforcing SSL connections on your server may require additional configuration to your applications connecting to the server. [Learn more](#)

Enforce SSL connection  ENABLED  DISABLED

TLS setting

Select the minimum TLS version supported by the server which may require additional configuration to your application connecting to the server. Click here to [Learn more](#)

Minimum TLS version  1.0  1.1  1.2

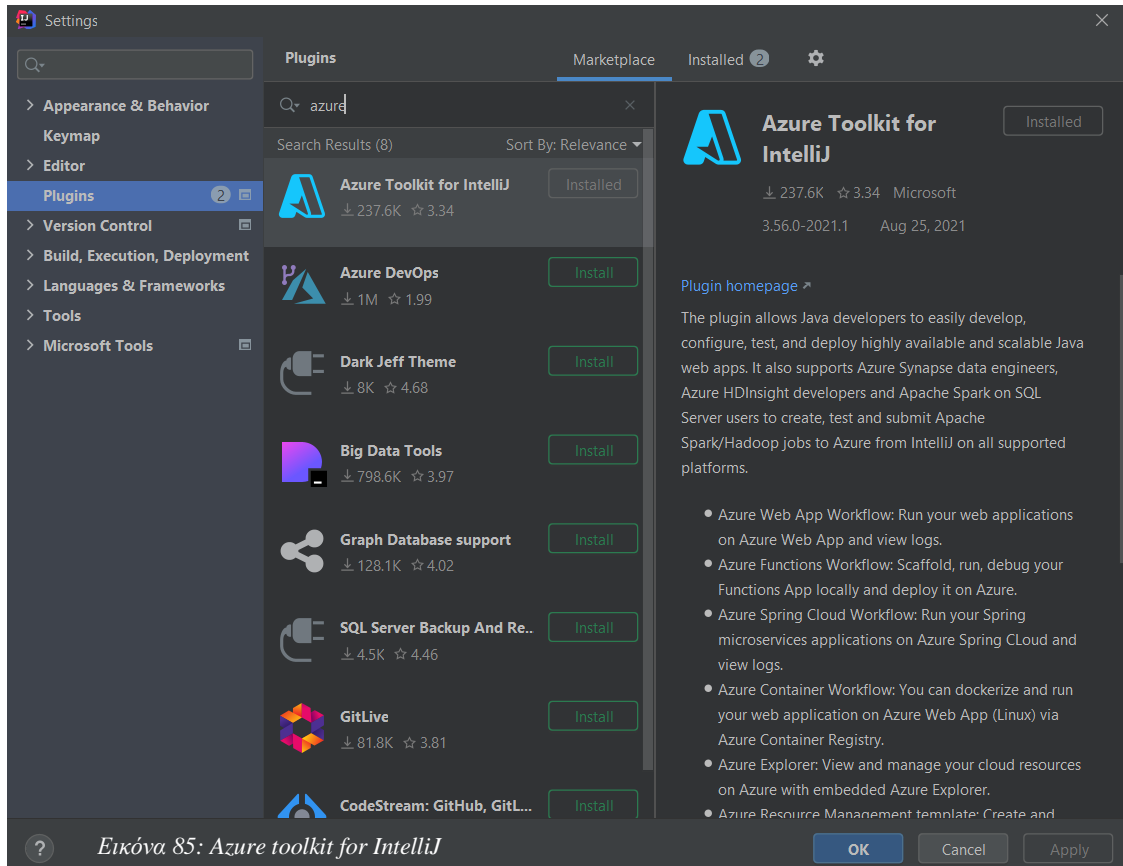
Εικόνα 84: Configure database security (add WebApp ip)

-Η υπηρεσία web app είναι έτοιμη και το μόνο που απομένει για να έχουμε μια επιτυχή μετάβαση της εφαρμογής μας στο «Cloud» είναι το deployment του κώδικα στην υπηρεσία που μόλις δημιουργήσαμε. Μόλις γίνει αυτό, η εφαρμογή μας θα είναι διαθέσιμη προς όλο το κοινό μέσω του URL link, το οποίο δημιουργήθηκε αυτόματα από την υπηρεσία του Azure.

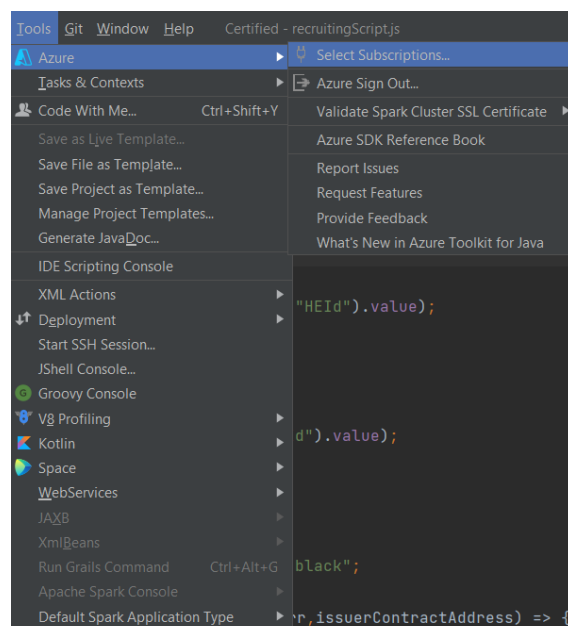
- Για να έχει πρόσβαση σε αυτό κάποιος, το μόνο που αρκεί είναι πρόσβαση στο διαδίκτυο, άλλωστε για αυτόν τον λόγο δημιουργήθηκε και το cloud computing.

### 6.9.5 Code Deployment μέσω του IntelliJ IDEA

-Αρχικά, για να μπορέσουμε να ανεβάσουμε τον κώδικα της εφαρμογής στο Azure και να μπορέσει να γίνει σωστά η μεταφορά στο cloud μέσω του IntelliJ IDEA θα χρειαστεί να εγκαταστήσουμε στην πλατφόρμα το plugin “Azure Toolkit for IntelliJ”. Αυτό θα γίνει μέσω του marketplace του IDE (shift+windows+s).

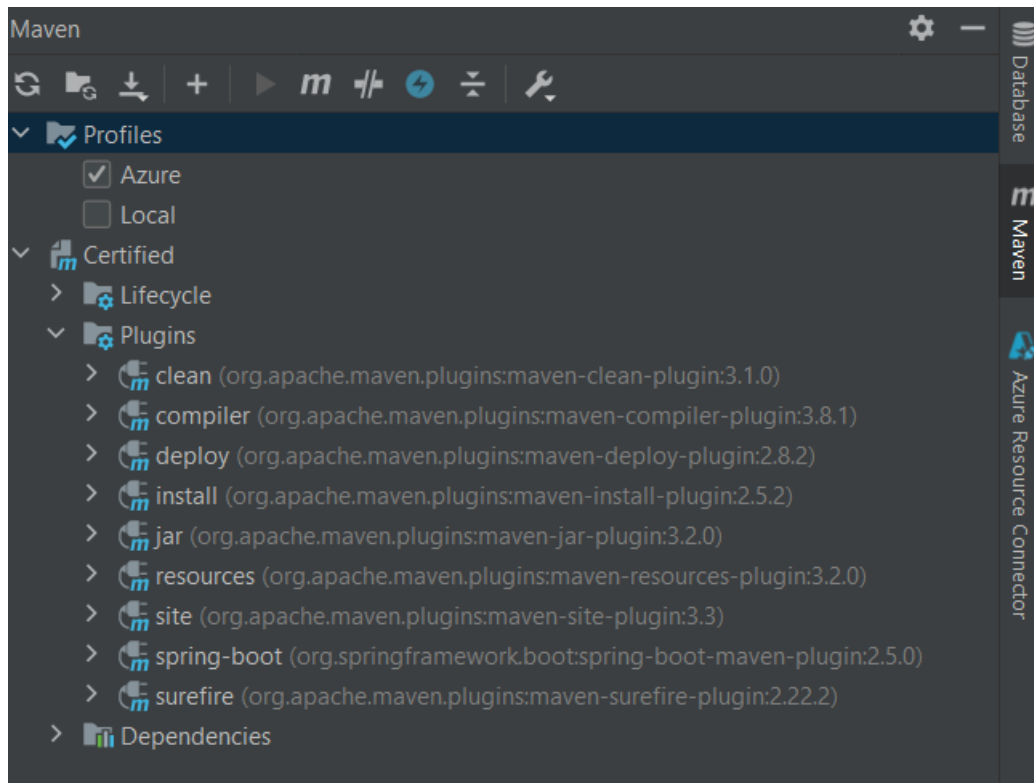


-Έπειτα από τα tools της πλατφόρμας θα βρούμε το Azure και θα συνδεθούμε στον λογαριασμό που δημιουργήσαμε επιλέγοντας το κατάλληλο subscription.



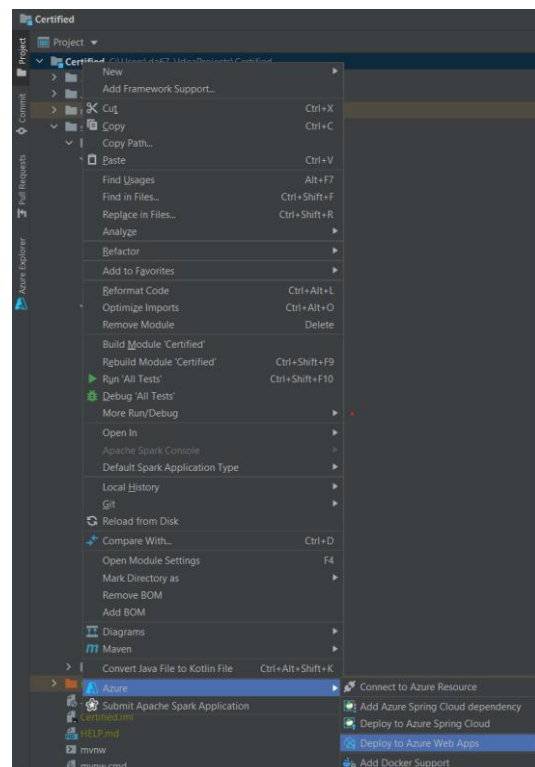
Εικόνα 87 IntelliJ select subscription

-Στην συνέχεια ανοίγουμε το tab του Maven από την καρτέλα profiles επιλέγουμε το προφίλ Azure (φροντίζουμε το local να μην είναι επιλεγμένο) και εκτελούμε την εντολή reload all maven dependencies για να ενημερωθεί η νέα σύνδεση στην βάση που φτιάξαμε στο cloud.



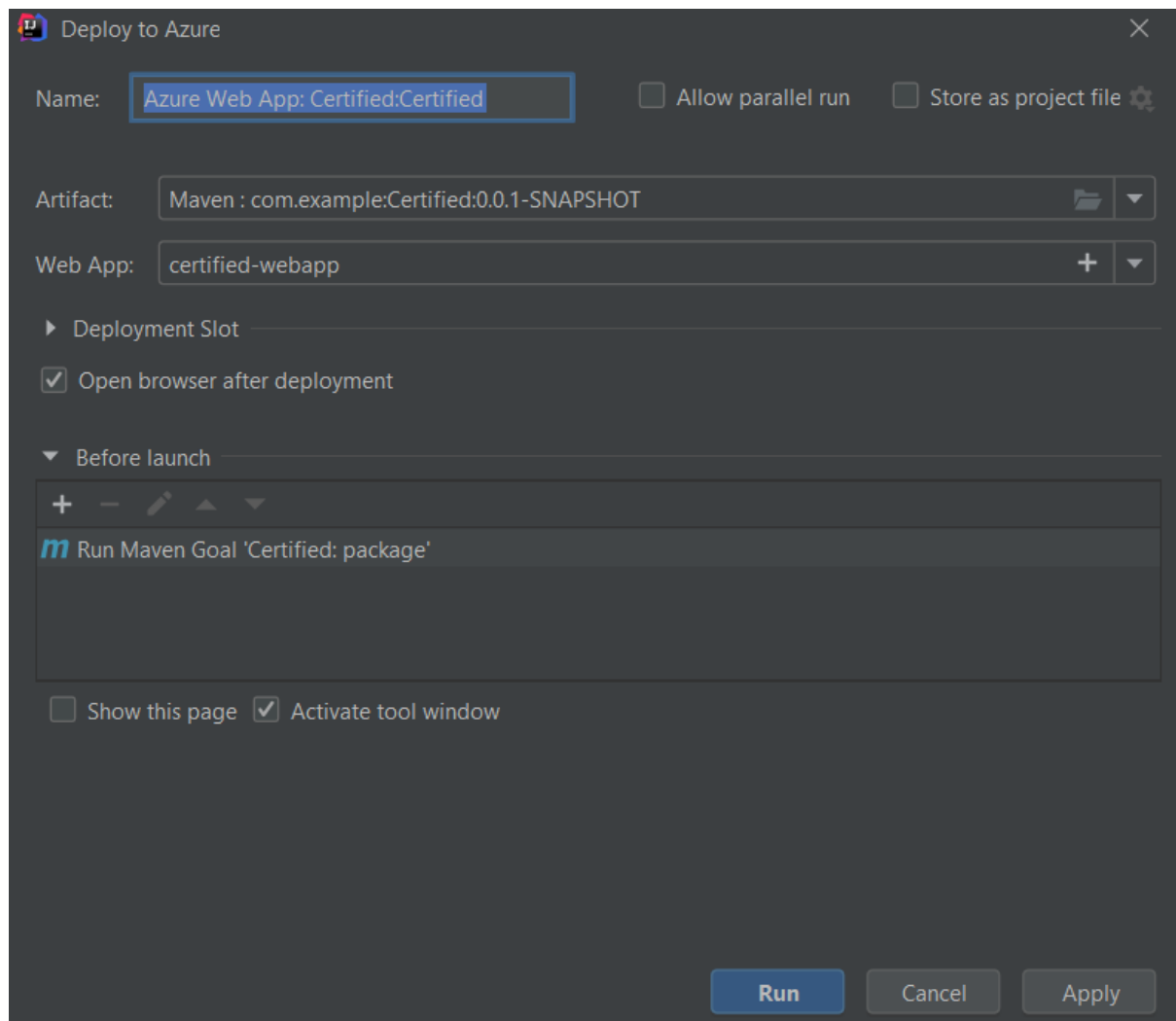
Εικόνα 88: Reload Maven Projects

-Αμέσως μετά με δεξί κλικ στο project βρίσκουμε το εικονίδιο του Azure και επιλέγουμε το κουμπί “Deploy to Azure Web Apps” το οποίο θα μας ανοίξει ένα παράθυρο για να ρυθμίσουμε το πώς θα γίνει το deployment του κώδικα σαν web app service στο “νέφος”.



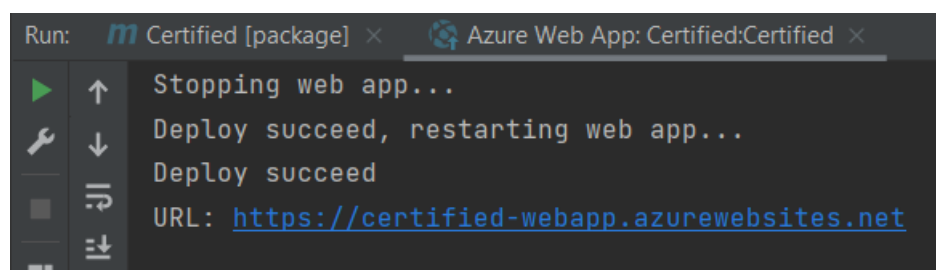
Εικόνα 89: Deploy to Azure WebApps

-Τέλος, στο παράθυρο που μας εμφανίζεται στο πεδίο web app, βρίσκουμε την υπηρεσία που δημιουργήσαμε προηγουμένως και τρέχουμε την εφαρμογή μας.



Εικόνα 90: WebApp service (IntelliJ)

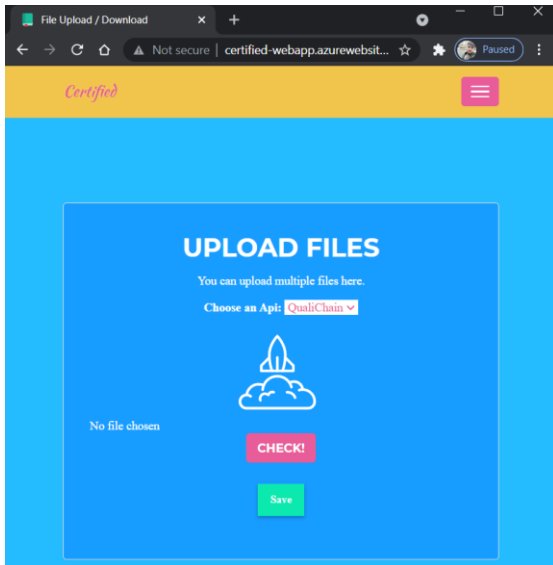
-Αν όλα τα βήματα γίνανε σωστά, το IntelliJ IDEA θα «πακετάρει» την εφαρμογή σαν αρχείο jar (αυτό τον τύπο αρχείου διαβάζει ο embedded web server, αν χρησιμοποιούσαμε tomcat πάνω από τον ενσωματωμένο server, θα έπρεπε να κάνουμε deploy τον κώδικα σαν war αρχείο που με την σειρά του ο Tomcat θα έστελνε την πληροφορία στον ενσωματωμένο διακομιστή), θα το ανεβάσει στο web app service, που δημιουργήσαμε, και τέλος θα τρέξει την εφαρμογή.



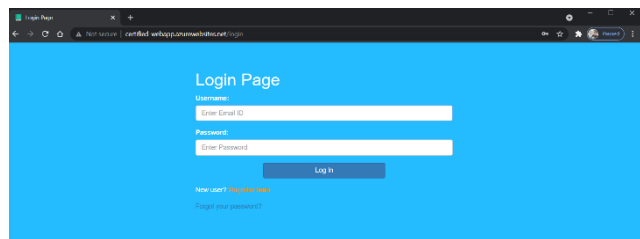
Εικόνα 91: Successful WebApp Deployment

### 6.9.6 Επιτυχής μετάβαση στο “cloud”

-Μετά από όλα αυτά τα βήματα που αναλύθηκαν πιο πάνω η εφαρμογή μας έκανε μια ομαλή μετάβαση από εφαρμογή που έτρεχε τοπικά στον ηλεκτρονικό υπολογιστή, σε εφαρμογή που τρέχει στο «νέφος» του Azure και πλέον σε αυτήν μπορεί να έχει πρόσβαση ο οποιασδήποτε σε όλα τα μήκη και πλάτη του πλανήτη.



Εικόνα 92: WebApp on cloud (mobile version)



Εικόνα 93: WebApp on cloud (pc version)

-Έτσι διασφαλίσαμε την προσβασιμότητα σε αυτήν εύκολα και γρήγορα από όλα τα μέρη του πλανήτη αφού έχει το πλεονέκτημα να κάνει χρήση διακομιστών που βρίσκονται διασκορπισμένοι παντού στον κόσμο, είναι πλέον ευέλικτη και μπορεί να διαχειριστεί μεγάλες αυξομειώσεις του work load ή αλλιώς της κυκλοφοριακής συμφόρησης της εφαρμογής. Δεν αποτελεί πλέον πρόβλημα η επέκταση και η κλιμάκωση της εφαρμογής για να εξυπηρετεί μεγαλύτερο κοινό, αφού αυτό μπορεί να γίνει αυτόματα με το πάτημα ενός κουμπιού. Και τέλος μας παρέχει ασφάλεια πως η εφαρμογή θα είναι online και θα τρέχει ακόμα και σε περίπτωση βλάβης των υποδομών, αφού υπάρχουν αντίγραφα ασφαλείας σε διάφορους διακομιστές (servers) και κέντρα δεδομένων (data centers) στην περιφέρειά μας.

-Η εφαρμογή μας θα βρίσκεται στην διεύθυνση: **http://certified-webapp.azurewebsites.net/**

## 7.Σύννοψη και Συμπεράσματα

### 7.1 Σύννοψη

Στην παρούσα διπλωματική στόχος μας ήταν να αναπτύξουμε μια διαδικτυακή εφαρμογή, που θα εκμεταλλευόταν τεχνολογίες “cloud computing” για να πιστοποιήσει την γνησιότητα εγγράφων η δικαιολογητικών μέσω APIS βασισμένα στην τεχνολογία blockchain. Αρχικά μελετήσαμε την τεχνολογία του blockchain και πως θα μπορούσε αυτή να συμβάλει καθοριστικά στην πιστοποίηση και επικύρωση εγγράφων. Ακολούθως κάναμε μια έρευνα για να βρούμε υπάρχοντα APIs που βασίζονται στην τεχνολογία blockchain για επικύρωση και πιστοποίηση εγγράφων, τίτλων σπουδών, πιστοποιητικών κ.α. Αμέσως επόμενο στάδιο ήταν ο σχεδιασμός και η ανάπτυξη της εφαρμογής μας. Αφού σχεδιάσαμε το επιχειρηματικό σχέδιο που θα ακολουθούσαμε και αναγνωρίσαμε τους κύριους ενδιαφερόμενους μιας τέτοιας εφαρμογής, σειρά είχε η υλοποίηση της.

Για την ανάπτυξη της εφαρμογής αρχικά χρησιμοποιήθηκε το εργαλείο AdobeXD, όπου με την βοήθεια του μοντελοποιήσαμε την διεπαφή χρήστη για να καταλήξουμε στις κύριες και δευτερεύουσες λειτουργικότητες που θα θέλαμε ιδανικά να ικανοποιεί το λογισμικό (back-end, front-end). Έπειτα με την βοήθεια σύγχρονων τεχνολογιών και εργαλείων τόσο στο back-end όσο και στο front-end αναπτύξαμε σε τοπικό επίπεδο την εφαρμογή. Πιο συγκεκριμένα η εφαρμογή μας βασίζεται σε Java MVC αρχιτεκτονική. Με την βοήθεια της πλατφόρμας Spring την χτίσαμε ως ένα Maven project ,όπου το front-end αποτελείται από html pages ,τα οποία υποστηρίζονται με JavaScript ,CSS και Bootstrap, και η σύνδεση του με το back-end γίνεται μέσω της πλατφόρμας ThymeLeaf. Η επικοινωνία της βάσης δεδομένων (τοπικής ή στο «cloud») με τον πυρήνα του προγράμματος ,το back-end, γίνεται με την βοήθεια του εργαλείου JPA-Hibernate.

Μετά την ανάπτυξη του «κορμού» της εφαρμογής κύριο μέλημα μας ήταν η εύρεση των κατάλληλων APIs που βασίζονται στο blockchain, για να τα χρησιμοποιήσουμε έτσι ώστε η εφαρμογή να πιστοποιεί την γνησιότητα εγγράφων. Μέσα από την έρευνα μας καταλήξαμε στα APIs ανοικτού κώδικα, Blockcerts και Qualichain, όπου και προσπαθήσαμε να τα υλοποιήσουμε καλώντας τα στο front-end της εφαρμογής μας. Το επόμενο βήμα ήταν να τρέξουμε την εφαρμογή τοπικά, και αυτό έγινε μέσω του ενσωματωμένου tomcat server στο maven project που δημιουργήσαμε. Παράλληλα με την ανάπτυξη της εφαρμογής χρησιμοποιήθηκε και το GitHub λόγο της ομαλής διαχείρισης του κώδικα που προσφέρει καθώς και για πιθανή ευκολότερη επεκτασιμότητα της εφαρμογής, μετέπειτα από μια μεγαλύτερη ομάδα developer.

Το επόμενο βήμα στην εκπόνηση αυτής της διπλωματικής ήταν η μεταφορά της εφαρμογής από το τοπικό επίπεδο στο “cloud”. Κατανοήσαμε αρχικά τα οφέλη που μπορούν να προσφέρουν γενικότερα τα “cloud” services και αφού αντιληφθήκαμε την τάση μεγάλων εταιρειών στην μεταφορά των online υπηρεσιών στο «νέφος», αποφασίσαμε με την σειρά μας να την ακολουθήσουμε , αφού μόνο θετικά θα επηρέαζε την ανάπτυξη της εφαρμογής μας. Έτσι λοιπόν μετά από έρευνα για πιθανούς παρόχους υπηρεσιών “cloud” που θα μπορούσαν να φιλοξενήσουν την εφαρμογή, καταλήξαμε στην υιοθέτηση μιας λύσης που βασίζεται στις υπηρεσίες «νέφους» που παρέχει η Microsoft μέσω του Azure Portal. Με την βοήθεια των documentation της Microsoft ,καταφέραμε να μάθουμε πολλά για την αρχιτεκτονική στο «cloud» ,και τελικά να ανεβάσουμε την εφαρμογή μας online ως ένα App Service, το οποίο υποστηρίζεται από μια MySQL βάση δεδομένων που τρέχει σε έναν Azure server για MySQL.



## 7.2 Συμπεράσματα και μελλοντικές επεκτάσεις

Στην σύγχρονη εποχή στην οποία ζούμε, όπου τα πάντα είναι σε ψηφιακή μορφή και η καθημερινότητα του μέσου ανθρώπου εξαρτάται σε μεγάλο βαθμό από τα διαδικτυο, προβάλλει επιτακτική η ανάγκη του εκσυγχρονισμού της διαδικασίας επικύρωσης και πιστοποίησης εγγράφων, που προέρχονται από πανεπιστημιακά ιδρύματα, κρατικές αρχές ή άλλους οργανισμούς. Όχι μόνο γιατί οι συμβατικές μέθοδοι πιστοποίησης της γνησιότητας εγγράφων κρίνονται ως χρονοβόρες, αφού για να διεκπεραιωθούν χρειάζονται μεσάζοντες, αλλά γιατί δεν αποπνέουν εμπιστοσύνη ούτε ασφάλεια στο άτομο που καλείται να προβεί σε αυτή την διαδικασία. Αυτό ισχύει εφόσον τα έγγραφα συνήθως είναι σε έντυπη μορφή, η οποία είναι εύκολο να καταδολιευθεί από επιτήδειους η ακόμα και να παραποιηθεί με ψευδή στοιχεία.

Συμπέρασμα των πιο πάνω είναι πως η τεχνολογία του blockchain μπορεί να αποτελέσει μια ασφαλή, γρήγορη και έμπιστη μέθοδο για την πιστοποίηση της γνησιότητας εγγράφων. Αυτό είναι εφικτό γιατί η τεχνολογία αυτή από την φύση της δεν μπορεί να υποπέσει σε οποιαδήποτε μορφής απάτη. Η αρμόδια αρχή η οποία εκδίδει ένα έγγραφο, ένα πιστοποιητικό ή έναν τίτλο σπουδών, το ανεβάζει μόνιμα στο blockchain σε μορφή κατακερματισμένου τόκεν (hash), οπότε, όταν ένας recruiter θέλει να πιστοποιήσει την γνησιότητα ενός εγγράφου που το έχει σε ηλεκτρονικά υπογραμμένη μορφή, το μόνο που πρέπει να κάνει είναι να επιβεβαιώσει το έγγραφο αξιοποιώντας κάποιο API που βασίζεται στο blockchain. Αυτό με την σειρά του θα κατακερματίσει το έγγραφο και αν το hash του είναι ίδιο με κάποιο επικυρωμένο έγγραφο τότε το έγγραφο είναι γνήσιο. Τόσο εύκολα ,απλά και γρήγορα μπορεί κάποιος να πιστοποιήσει την γνησιότητα ενός εγγράφου με την χρήση του blockchain, αντικαθιστώντας τους μεσάζοντες με την τεχνολογία των Smart Contracts.

Επίσης η χρήση των υπηρεσιών “cloud” για την ολική μετάβαση της εφαρμογής στο «νέφος», βοηθούν την οποιαδήποτε μελλοντική επεκτασιμότητα της, με απώτερο σκοπό να καλύψει ανάγκες ενός ευρύτερου κοινού. Τα πλεονεκτήματα αυτής της επιλογής μας θα είναι πιο εμφανή με την κλιμάκωση και την επέκταση της εφαρμογής. Αφού η αξιοποίηση πόρων και υπηρεσιών του “cloud” θα συνδράμουν στην υψηλή διαθεσιμότητα της, την εύκολη επεκτασιμότητα, την ελαστικότητα και την ευελιξία της καθώς και για την άμεση αποκατάσταση της σε περιπτώσεις βλάβης υποδομών.

### Πιθανές Μελλοντικές Επεκτάσεις της διπλωματικής”

Κατά την ανάπτυξη της εφαρμογής είχαμε κατά νου την πιθανή μελλοντική επέκταση της εφαρμογής, έτσι ώστε να καλύπτει ένα μεγαλύτερο κοινό εξυπηρετώντας όλες τις ανάγκες του. Γι’ αυτό το λόγο χρησιμοποιήσαμε τις τεχνολογίες του «cloud computing» και του GitHub αφού κάνουν την επεκτασιμότητα μιας εφαρμογής ζήτημα μερικών λεπτών.

-Μια πιθανή επέκταση της εφαρμογής είναι η στέγαση περισσότερων API που βασίζονται στο blockchain και αποθηκεύουν επικυρωμένα έγγραφα. Έτσι θα καταφέρουμε να καλύψουμε μια πιο ευρεία γκάμα επικυρωμένων εγγράφων από πανεπιστημιακά ιδρύματα, αρμόδιες αρχές και άλλους οργανισμούς, δίνοντας την δυνατότητα στον χρήστη να μπορεί να πιστοποιήσει οποιοδήποτε του έγγραφο. Στο κεφάλαιο 3 αναφέραμε κάποια αξιολογία projects που βασίζονται στο blockchain και θα μπορούσαν να χρησιμοποιηθούν μελλοντικά στην εφαρμογή. Άξιο αναφοράς αποτελεί το γεγονός ότι μέρα με την μέρα ολοένα και περισσότερα πανεπιστημιακά ιδρύματα επικυρώνουν τους τίτλους σπουδών τους στο blockchain κάποια παραδείγματα αυτών είναι το Massachusetts Institute of Technology (MIT), το Cornell University, το University of Oxford, όπως και το Κυπριακό ιδιωτικό ίδρυμα , το University of Nicosia. Άρα μια πλατφόρμα που να στεγάζει όλα αυτά τα APIs θα αποτελούσε κάτι το ιδανικό για τους χρήστες και ειδικότερα για τους recruiters.

Σύμμαχος μας σε αυτή την μεγάλη επέκταση της εφαρμογής θα αποτελέσουν τα «cloud services», αφού θα καταστήσουν δυνατή την κλιμάκωση της διατηρώντας την ευελιξία, την ελαστικότητα και την άμεση αποκατάσταση πιθανών βλαβών στις υλικοτεχνικές υποδομές. Ενώ συγχρόνως θα μπορούμε να εγγυηθούμε την αξιοπιστία και τους χαμηλούς χρόνους απόκρισης της εφαρμογής, τροποποιώντας τα

πακέτα των “cloud services” που χρησιμοποιούμε, με απώτερο σκοπό να καλύψουμε οποιοσδήποτε ανάγκες προκύψουν όσο αφορά τους πόρους και την διαχείριση αυξημένου φόρτου εργασίας.

-Ένα δεύτερο εναλλακτικό σενάριο επεκτασιμότητας αυτού του project, είναι η προσθήκη μιας καινούριας λειτουργικότητας που θα εξυπηρετεί πανεπιστημιακά ιδρύματα και άλλες αρμόδιες αρχές, που εκδίδουν πιστοποιητικά, διπλώματα και άλλα επίσημα έγγραφα. Η λειτουργικότητα αυτή θα δίνει την δυνατότητα σε αυτούς τους φορείς να επικυρώνουν τα έγγραφα τα οποία εκδίδουν σε blockchain APIs της επιλογής τους και θα στέλνουν στον ενδιαφερόμενο το ηλεκτρονικά υπογραμμένο αντίγραφο του εγγράφου του. Με αυτό τον τρόπο θα γίνει ευκολότερη η μετάβαση των επικυρωμένων εγγράφων στο blockchain από οργανισμούς που δεν είχαν τα μέσα και την ευκαιρία να το πράξουν και να το υιοθετήσουν νωρίτερα. Για να γίνει αυτό ίσως χρειαστεί η επικοινωνία με τα υπάρχοντα blockchain APIs για να δώσουν την έγκριση (αναγνώριση γνησιότητας εκδότριας αρχής)να επικυρώνονται έγγραφα μέσω της εφαρμογής μας από αναγνωρισμένα ιδρύματα και οργανισμούς.

-Μια τρίτη ιδέα για διεύρυνση του θέματος της εφαρμογής είναι η περίπτωση χρήσης του σε εφαρμογές τρίτων σαν εξωτερικό web-service που να κουμπώνει σε αυτές, με άλλα λόγια σαν ένα plugin. Ένα παράδειγμα εφαρμογής που θα μπορούσε να χρησιμοποιηθεί εύκολα η υπηρεσία αυτή είναι το LinkedIn. Το LinkedIn αποτελεί μια πλατφόρμα κοινωνικής δικτύωσης επαγγελματικού προσανατολισμού. Εκεί ο χρήστης έχει την δυνατότητα να ανεβάσει τα προσόντα του, τις γνώσεις και τα επιτεύγματα του καθώς και πιθανά έγγραφα η πιστοποιητικά τα οποία αποδεικνύουν τους ισχυρισμούς του. Απώτερο στόχο αυτής της διαδικασίας είναι να έρθει σε επικοινωνία με recruiters, που αργότερα θα του προσφέρουν μια θέση εργασίας. Το πρόβλημα όμως, είναι πως κανένας δεν μπορεί να εγγυηθεί την γνησιότητα των εγγράφων που ανεβάζει ο κάθε χρήστης. Εδώ έρχεται λοιπόν να κουμπώσει μια πιθανή επέκταση της εφαρμογής ως plugin, τα έγγραφα αυτά που θα ανεβάζει ο χρήστης θα πιστοποιούνται από το plugin της εφαρμογής και αν είναι γνήσια το έγγραφο θα κερδίζει το αντίστοιχο badge. Αποτέλεσμα αυτού είναι ο recruiter να γνωρίζει αν τα έγγραφα κάποιου ενδιαφερόμενου είναι γνήσια.

-Τέλος μελλοντική επέκταση της εφαρμογής μας θα μπορούσε να είναι μια εθνική πολιτική αντίστοιχη της πρωτοβουλίας της κυβέρνησης της Σιγκαπούρης με την δράση του SkillsFuture και την χρήση του OpenCerts. Δηλαδή η εφαρμογή μας να αποτελέσει μια πλατφόρμα βασισμένη στο blockchain που θα μπορεί ο κάθε εργοδότης στο ελληνικό κράτος να πιστοποιήσει την γνησιότητα των εγγράφων του υποψήφιου εργοδοτούμενου. Αντίστοιχα τα ελληνικά πανεπιστήμια και οι αρμόδιοι φορείς που έχουν την δυνατότητα να εκδίδουν πιστοποιητικά θα μπορούν να επικυρώσουν την γνησιότητα τους στην πλατφόρμα μας με την χρήση blockchain.

# Βιβλιογραφία

- [1] Dimitrios Askounis, Panagiotis Zarafidis, Konstantinos Siassiakos, Dimitrios Strotos, Panayiotis Deriziotis, "Blockchain in Recruitment – Greek Public Sector Analysis and the QualiChain Solution", 2020
- [2] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2007. Available: <https://bitcoin.org/bitcoin.pdf>
- [3] Fernando Richter Vidal, Feliz Gouveia, Christophe Soares, "Blockchain Application in Higher Education Diploma Management and Results Analysis", 2020, [Online]. Available: [https://www.researchgate.net/publication/346647984\\_Blockchain\\_Application\\_in\\_Higher\\_Education\\_Diploma\\_Management\\_and\\_Results\\_Analysis](https://www.researchgate.net/publication/346647984_Blockchain_Application_in_Higher_Education_Diploma_Management_and_Results_Analysis)
- [4] B. Ramamurthy, Blockchain in action. 2020 [Online]. Available: <https://www.manning.com/books/blockchain-in-action>
- [5] Melanie Swan, "Blockchain for Business: Next-Generation Enterprise Artificial Intelligence Systems", 4 May 2018. Available: <https://www.sciencedirect.com/science/article/pii/S0065245818300287>
- [6] "BLOCKCHAIN GLOSSARY OF TERMS: 128 BLOCKCHAIN TERMS AND THEIR DEFINITIONS", [online] Available: <https://objectcomputing.com/expertise/blockchain/glossary>
- [7] Wattana Viriyasitavat, Danupol Hoonsopon, "Blockchain characteristics and consensus in modern business processes", 29 July 2018. Available: <https://www.sciencedirect.com/science/article/pii/S2452414X18300815>
- [8] Karim Sultan<sup>1</sup>, Umar Ruhi<sup>1</sup> and Rubina Lakhani<sup>2</sup>, "CONCEPTUALIZING BLOCKCHAINS: CHARACTERISTICS & APPLICATIONS", 2018. Available: <https://arxiv.org/ftp/arxiv/papers/1806/1806.03693.pdf>
- [9] Julien Polge, Jérémy Robert, Yves Le Traon, "Permissioned blockchain frameworks in the industry: A comparison", 12 September 2020. Available: <https://www.sciencedirect.com/science/article/pii/S2405959520301909>
- [10] Siamak Solat, P. Calvez, "Permissioned vs. Permissionless Blockchain: How and Why There Is Only One Right Choice", December 2020. Available: [https://www.researchgate.net/publication/349537863\\_Permissioned\\_vs\\_Permissionless\\_Blockchain\\_How\\_and\\_Why\\_There\\_Is\\_Only\\_One\\_Right\\_Choice](https://www.researchgate.net/publication/349537863_Permissioned_vs_Permissionless_Blockchain_How_and_Why_There_Is_Only_One_Right_Choice)
- [11] Tsung-Ting Kuo, Hugo Zavaleta Rojas, Lucila Ohno-Machado, "Comparison of blockchain platforms: a systematic review and healthcare examples", 25 March 2019. Available: <https://academic.oup.com/jamia/article/26/5/462/5419321#219598681>
- [12] Martin Stellnberger, "Document Certification Through the Blockchain", 2016-12-05. [online] Available: [https://www.martinstellnberger.co/document-certification-through-the-blockchain?fbclid=IwAR29Mf9vGzXr2\\_7GF90zZX-mTBGfLPdtGDqsF7R9dW3blW71sqAfH9QgS7Q](https://www.martinstellnberger.co/document-certification-through-the-blockchain?fbclid=IwAR29Mf9vGzXr2_7GF90zZX-mTBGfLPdtGDqsF7R9dW3blW71sqAfH9QgS7Q)
- [13] Blockchain Experts, "Document Verification Using Blockchain", Nov 3, 2018. [online] Available: <https://medium.com/blockchainexpert-blog/document-verification-using-blockchain-a02c059ed97b>
- [14] Chanaka Lakmal, Sachithra Dangalla, Chandu Herath, Chamin Wickramarathna, Gihan Dias, Shantha Fernando, "IDStack - The Common Protocol for Document Verification built on Digital Signatures", 2019. Available: <https://arxiv.org/ftp/arxiv/papers/1901/1901.01883.pdf>
- [15] Ibrahim Alnafrh, Suliman Mouselli, "Revitalizing blockchain technology potentials for smooth academic records management and verification in low-income countries", 9

- July 2021. Available:  
<https://www.sciencedirect.com/science/article/pii/S0738059321001139#abs0010>
- [16] Opencerts. [online] Available: <https://www.opencerts.io/faq> ,  
<https://github.com/OpenCerts>
- [17] "OpenCerts - An Easy Way to Check and Verify Your Certificates", Singapore Government ,18 August 2021. [online] Available:  
<https://www.developer.tech.gov.sg/technologies/blockchain/opencerts>
- [18] Government Technology Agency (GovTech), Ngee Ann Polytechnic, SkillsFuture Singapore and Ministry of Education, "Opencerts". [online] Available:  
<https://www.tech.gov.sg/scewc2019/opencerts>
- [19] "First anti-fraud platform for the registration and certification of diplomas and academic certificates based in blockchain "[online] Available:  
<https://cordis.europa.eu/project/id/887349>
- [20] SmartDegrees Website," SmartDegrees". [online] Available:  
<https://www.smartdegrees.es/en/home-en/>
- [21] KEVIN CRUZ," BLOCKSIGN: SIGNING DOCUMENTS ON THE BLOCKCHAIN", NOV 20, 2014. [online] Available:  
<https://bitcoinmagazine.com/business/blocksign-signing-documents-on-the-blockchain-1416508388>
- [22] Fernando Richter Vidal, Feliz Ribeiro Gouveia , Christophe Pinto de Almeida Soares, "Revocation Mechanisms for Academic Certificates Stored on a Blockchain", April 2020. Available:  
[https://www.researchgate.net/publication/340536611\\_Revocation\\_Mechanisms\\_for\\_Academic\\_Certificates\\_Stored\\_on\\_a\\_Blockchain](https://www.researchgate.net/publication/340536611_Revocation_Mechanisms_for_Academic_Certificates_Stored_on_a_Blockchain)
- [23] Rujia Li, Dr. David Galindo," Better Security Over Blockcerts", September 2017. Available: <https://dgalindo.es/mscprojects/rujia.pdf>
- [24] M. Turkanovic, M. Holbl, K. Kopic, M. Hericko, A. Kamisalic, "EduCTX: A blockchain-based higher education credit platform," IEEE. Available:  
<https://arxiv.org/pdf/1710.09918.pdf>
- [25] Marco Baldi, Franco Chiaraluce, Migelan Kodra and Luca Spalazzi," Security analysis of a blockchain-based protocol for the certification of academic credentials", 10 October 2019. Available: <https://arxiv.org/pdf/1910.04622.pdf>
- [26] "Introducing Smart Contracts to BlockCerts", Blockcerts Community, February 2020. Available: <https://community.blockcerts.org/t/introducing-smart-contracts-to-blockcerts/2362>
- [27] A. Ronning, W. W. Chung, "Blockcerts V3 Proposal," 2019. Available:  
<https://nbviewer.org/github/WebOfTrustInfo/rwot9-prague/blob/master/final-documents/BlockcertsV3.pdf>
- [28] M. L. MIT Media Lab, "Blockcerts-An Open Infrastructure for Academic Credentials on the Blockchain," 2016. Available: <https://medium.com/mit-media-lab/blockcerts-an-open-infrastructure-for-academic-credentials-on-the-blockchain-899a6b880b2f>
- [29] Wikipedia, "MySQL Workbench",January 2010. [online] Available:  
[https://en.wikipedia.org/wiki/MySQL\\_Workbench](https://en.wikipedia.org/wiki/MySQL_Workbench)
- [30] JavaTPoint," Hibernate Framework". [online] Available:  
<https://www.javatpoint.com/hibernate-tutorial>
- [31] Iqbal H. Sarker, Khalid Ibn Zinnah Apu, "MVC Architecture Driven Design and Implementation of Java Framework for Developing Desktop Application", September 2014. Available:  
[https://www.researchgate.net/publication/291098214\\_MVC\\_Architecture\\_Driven\\_Design\\_and\\_Implementation\\_of\\_Java\\_Framework\\_for\\_Developing\\_Desktop\\_Application](https://www.researchgate.net/publication/291098214_MVC_Architecture_Driven_Design_and_Implementation_of_Java_Framework_for_Developing_Desktop_Application)

- [32] Tutorials Point, “MVC Framework - Introduction”. [online] Available: [https://www.tutorialspoint.com/mvc\\_framework/mvc\\_framework\\_introduction.htm](https://www.tutorialspoint.com/mvc_framework/mvc_framework_introduction.htm)
- [33] Archana Choudary, “How to Implement MVC Architecture in Java?”, Jun 2021. [online] Available: <https://www.edureka.co/blog/mvc-architecture-in-java/>
- [34] GeeksforGeeks, “Introduction to Apache Maven | A build automation tool for Java projects”, 30 Dec 2019. [online] Available: <https://www.geeksforgeeks.org/introduction-apache-maven-build-automation-tool-java-projects/>
- [35] Apache Maven.” Apache Maven Project”, 2021-10-04. [online] Available: <https://maven.apache.org/>
- [36] Tutorials Point,” Spring Boot - Introduction”. [online] Available: [https://www.tutorialspoint.com/spring\\_boot/spring\\_boot\\_introduction.htm](https://www.tutorialspoint.com/spring_boot/spring_boot_introduction.htm)
- [37] Spring,”Spring Security”. [online] Available: <https://spring.io/projects/spring-security>
- [38] Javatpoint, “Spring Security Features”. [online] Available: <https://www.javatpoint.com/spring-security-features>
- [39] Spring Docs,” Spring Security Reference”. [online] Available: <https://docs.spring.io/spring-security/site/docs/current/reference/html5/>
- [40] Dan Arias, “Hashing in Action: Understanding bcrypt”, February 25, 2021. [online] Available: <https://auth0.com/blog/hashing-in-action-understanding-bcrypt/>
- [41] Thyme leaf main page, “Thymeleaf”. [online] Available: <https://www.thymeleaf.org/>
- [42] Tomislav Bacinger,” What is Bootstrap? A Short Bootstrap Tutorial on the What, Why, and How”, 2015 [online] Available: <https://www.toptal.com/front-end/what-is-bootstrap-a-short-tutorial-on-the-what-why-and-how>
- [43] KEMEL,” Business Model Canvas, Δυναμικό Εργαλείο Επιχειρηματικότητας”, Ιούλιος 2014. [online] Available: <https://www.kemel.gr/library/business-model-canvas-dynamiko-ergaleio-epicheirimatikotitas>
- [44] Abdul Majeed1 and Ibtisam Rauf,” MVC Architecture: A Detailed Insight to the Modern Web Applications Development”, September 26, 2018. Available: <https://crimsonpublishers.com/prsp/pdf/PRSP.000505.pdf>
- [45] Ralph F. Grove and Eray Ozkan,” THE MVC-WEB DESIGN PATTERN”,2011. Available: <https://www.scitepress.org/Papers/2011/32969/32969.pdf>
- [46] M.G.Avrar, “Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective”, 15 January 2014. Available: <https://www.sciencedirect.com/science/article/pii/S221201731300710X>
- [47] Peter Mell Timothy Grance, “The NIST Definition of Cloud Computing”, September 2011. Available: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf>
- [48] JAKE FRANKENFIELD, “Cloud Computing”, uly 28, 2020. [online] Available: <https://www.investopedia.com/terms/c/cloud-computing.asp>
- [49] Scality, “The history of cloud computing”. [online] Available: <https://www.scality.com/solved/the-history-of-cloud-computing/>
- [50] Keith D. Foote , “A Brief History of Cloud Computing”,June 22, 2017. [online] Available: <https://www.dataversity.net/brief-history-cloud-computing/>
- [51] Kalliopi Kanaki , “ΥΠΟΛΟΓΙΣΤΙΚΟ ΝΕΦΟΣ”, April 2015. Available: [https://www.researchgate.net/publication/302873104\\_YPOLOGISTIKO\\_NEPHOS](https://www.researchgate.net/publication/302873104_YPOLOGISTIKO_NEPHOS)
- [52] Microsoft Docs, “Describe cloud benefits and considerations”. Available: <https://docs.microsoft.com/en-us/learn/modules/fundamental-azure-concepts/benefits-of-cloud-computing>
- [53] Microsoft Docs, “Describe different cloud services”. Available: <https://docs.microsoft.com/en-us/learn/modules/fundamental-azure-concepts/categories-of-cloud-services>

- [54] Shshil B., Leena J., Sandeep J., "Cloud Computing: A study of infrastructure as a service (IaaS)"; 2010. Available:  
[https://www.academia.edu/1181740/Cloud\\_computing\\_A\\_study\\_of\\_infrastructure\\_as\\_a\\_service\\_IAAS\\_](https://www.academia.edu/1181740/Cloud_computing_A_study_of_infrastructure_as_a_service_IAAS_)
- [55] Microsoft Forum, "What are public, private, and hybrid clouds?". Available:  
<https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/?fbclid=IwAR0y--OkLJzoQPdaJeeYwXQaOkYHNiaH2cuyWTfopGMfYMmLwVEoBSiQYSo#overview>
- [56] DEJAN TUCAKOV, "What is Community Cloud? Benefits & Examples with Use Cases", JUNE 18,2020. [online] Available:  
<HTTPS://PHOENIXNAP.COM/BLOG/COMMUNITY-CLOUD>
- [57] George Carutasu , "Cloud Computing and Windows Azure", June 2016. Available:  
[https://www.researchgate.net/publication/305725698\\_Cloud\\_Computing\\_and\\_Windows\\_Azure](https://www.researchgate.net/publication/305725698_Cloud_Computing_and_Windows_Azure)
- [58] Stephen J. Bigelow, "Microsoft Azure". [online] Available:  
<https://searchcloudcomputing.techtarget.com/definition/Windows-Azure>
- [59] Microsoft Docs, "Describe Azure cost management and service level agreements", Available: <https://docs.microsoft.com/en-us/learn/paths/az-900-describe-azure-cost-management-service-level-agreements/>
- [60] Microsoft Docs," Host a web application with Azure App Service". Available:  
<https://docs.microsoft.com/en-us/learn/modules/host-a-web-app-with-azure-app-service/>
- [61] Microsoft Docs," Deploy a website to Azure with Azure App Service" Available:  
<https://docs.microsoft.com/en-us/learn/paths/deploy-a-website-with-azure-app-service/>
- [62] Ethereum Docs, "Proof-of-Stake". [online] Available:  
<https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/>
- [63] Niaz Chowdhury (OU), Allan Third (OU), Ahmad Mehrbod (KBZ), Vagelis Karakolis, Christos Kontzinos, Christos Botsikas (NTUA), Simon Scerri (IAIS), Ingo Keck (TIB), Nadia Politou (ATOS), Miguel Correia (INESC), "Qualichain", October 2019