



Αυτόνομο κοινωνικό δίκτυο βασισμένο σε τεχνολογίες αποκέντρωσης

Νικολαΐδης Παναγιώτης¹ και Φανάκης Απόστολος²

¹nkpanagi@auth.gr, 7491

²apostolof@auth.gr, 8261

Επιβλέπων Χρήστος Ε. Δημάκης

Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Πολυτεχνική Σχολή

Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης

Θεσσαλονίκη 2021

Περίληψη

Τις τελευταίες δεκαετίες, η ραγδαία ανάπτυξη του διαδικτύου μετέβαλε ριζικά τις ανθρωπίνες κοινωνίες, μέσω μίας πληθώρας ψηφιακών εφαρμογών, οι οποίες, στη συντριπτική τους πλειοψηφία, προσφέρονται από παρόχους υπηρεσιών υπολογιστικού νέφους, ακολουθώντας την αρχιτεκτονική πελάτη-εξυπηρετητή.

Μολονότι αυτό το μοντέλο υλοποίησης έχει αποδειχθεί ιδιαίτερα λειτουργικό και έχει βελτιωθεί αξιοσημείωτα ανά τα χρόνια, η συγκεντρωτική του λογική συνοδεύεται από μία σειρά προβλημάτων. Πρώτα απ' όλα, ο χρήστης καλείται να εμπιστευθεί τα προσωπικά του δεδομένα σε μία εξωτερική οντότητα. Εκείνη, διατηρώντας τον πλήρη έλεγχο επί αυτών, διαθέτει τη δυνατότητα να τα επεξεργάζεται, να τα διαμοιράζεται και να τα λογοκρίνει, είτε για να εξυπηρετήσει τα συμφέροντά της, είτε για να συμμορφωθεί με άλλες αρχές που της ασκούν εξουσία. Επιπλέον, απουσιάζει η εγγύηση της διαθεσιμότητας των δεδομένων, καθώς, ανά πάσα στιγμή, ο εξυπηρετητής μπορεί να αποσυνδεθεί για αόριστο χρονικό διάστημα και λόγω ποικίλων αιτιών, όπως κάποιας κυβερνοεπίθεσης ή κάποιας φυσικής καταστροφής.

Αυτοί είναι μερικοί βασικοί λόγοι που συνετέλεσαν στην ταχεία ανάπτυξη ενός συνόλου λογισμικών ανοιχτού κώδικα, όπως του Ethereum blockchain και του IPFS, τα οποία, αν και βρίσκονται σε σχετικά πρώιμο στάδιο, αποτελούν ήδη ικανά εργαλεία δημιουργίας κατακεντρωμένων και αποκεντρωμένων εφαρμογών.

Στόχος της παρούσας διπλωματικής εργασίας είναι η υλοποίηση μίας αυτόνομης κοινωνικής πλατφόρμας, η οποία, αξιοποιώντας τεχνολογίες αποκέντρωσης, αφενός θα επιστρέφει την κυριότητα των προσωπικών δεδομένων στον χρήστη, αφετέρου θα παρέχει τη δυνατότητα διενέργειας διαφανών δημοκρατικών ψηφοφοριών. Αυτά μέσα σε ένα πλαίσιο ανθεκτικό, τόσο σε σφάλματα και επιθέσεις, όσο και σε απόπειρες λογοκρισίας και παραποίησης.

Λέξεις-Κλειδιά: Αποκεντροποίηση, Ethereum, Blockchain, Έξυπνο Συμβόλαιο, Αποκεντρωμένη Εφαρμογή, IPFS, OrbitDB, React, Redux, Jenkins

Abstract

Don't forget the keywords.

Ευχαριστίες

Ευχαριστούμε η Αθήνα. Ευχαριστούμε η Ελλάδα.

Περιεχόμενα

Περίληψη	2
Abstract	3
Ευχαριστίες	4
1 Εισαγωγή	7
1.1 Γενικά	7
1.2 Περί αποκέντρωσης	8
1.3 Ορισμός του προβλήματος	9
1.4 Στόχος της διπλωματικής	10
1.5 Μεθοδολογία της διπλωματικής	10
1.6 Οργάνωση κεφαλαίων	10
2 Θεωρητικό υπόβαθρο	11
2.1 Συναρτήσεις κατακερματισμού	11
2.2 Ασύμμετρη κρυπτογραφία	12
2.3 Δένδρα Merkle	14
2.4 Δίκτυα Ομότιμων Κόμβων	16
2.5 Blockchain	16
2.6 Ethereum	17
2.6.1 Λογαριασμοί	17
2.6.2 Smart Contracts	18
2.6.3 DApps	19
2.6.4 Tokens	20
2.6.5 EVM	21
2.7 IPFS	21
3 Σχεδίαση εφαρμογής	24
3.1 Σύλληψη της ιδέας	24
3.2 Τεχνολογική στοίβα	25
3.3 Μεθοδολογία σχεδίασης	26
3.4 Κατηγορίες χρηστών	26
3.4.1 Ενεργοί χρήστες	26
3.4.2 Παθητικοί χρήστες	26
3.4.3 Σύνοψη χρηστών	27
3.5 Απαιτήσεις λογισμικού	27
3.6 Σενάρια χρήσης	31
3.6.1 Σενάριο χρήσης 1: Εγγραφή χρήστη	32

3.6.2	Σενάριο χρήσης 2: Σύνδεση χρήστη	34
3.6.3	Σενάριο χρήσης 3: Δημιουργία νέου θέματος	36
3.6.4	Σενάριο χρήσης 4: Ανάκτηση θέματος	38
3.6.5	Σενάριο χρήσης 5: Δημιουργία νέου μηνύματος	42
3.6.6	Σενάριο χρήσης 6: Τροποποίηση μηνύματος	44
3.6.7	Σενάριο χρήσης 7: Ψήφιση σε ψηφοφορία	46
3.6.8	Σενάριο χρήσης 8: Ψήφιση μηνύματος	47
3.6.9	Σενάριο χρήσης 9: Διαγραφή τοπικών δεδομένων	48
3.7	Αρχιτεκτονική σχεδίαση	49
3.7.1	Πρώτο μέρος	49
3.7.2	Δεύτερο μέρος	50
3.8	Προδιαγραφή μεθόδου υλοποίησης και χρονοπρογραμματισμός	51
3.8.1	Προδιαγραφή κύκλων	51
3.8.2	Πρώτη φάση	51
3.8.3	Δεύτερη φάση	51
3.8.4	Τρίτη φάση	51
3.8.5	Τέταρτη φάση	51
4	Υλοποίηση εφαρμογής	52
4.1	Χαρακτηριστικά που υλοποιήθηκαν	52
4.2	Μεθοδολογία υλοποίησης	52
4.3	Τεχνολογίες υλοποίησης	53
4.3.1	OrbitDB	53
4.4	Αρχιτεκτονική υλοποίησης	54
4.4.1	Αρθρώματα	56
4.4.2	Concordia Application	58
4.4.3	Concordia Contracts Migrator	60
4.4.4	Concordia Pinner	60
4.4.5	Concordia Contracts Provider	61
4.4.6	Ganache	62
4.4.7	Rendezvous Server	63
4.4.8	Διασύνδεση υπηρεσιών	63
4.4.9	Ροή πληροφορίας	64
5	Συμπεράσματα	67
5.1	Προβλήματα ανάπτυξης	67
5.2	Διαφορές σχεδιασμού-υλοποίησης	67
5.3	Ανοιχτά θέματα	67
5.4	Επίλογος	67

Κεφάλαιο 1

Εισαγωγή

1.1 Γενικά

Η αλματώδης ανάπτυξη του διαδικτύου διαμόρφωσε ένα ολοκαίνουργιο τοπίο σε κάθε τομέα της ανθρώπινης δραστηριότητας, παρέχοντας ένα αναρίθμητο πλήθος εφαρμογών και υπηρεσιών. Τα μέσα κοινωνικής δικτύωσης, το ηλεκτρονικό ταχυδρομείο, η ψηφιακή ειδησεογραφία, ο διαμοιρασμός αρχείων και οι υπηρεσίες πολυμέσων ροής, αποτελούν ορισμένα από τα σημαντικότερα - και πλέον αναπόσπαστα - κομμάτια, που συνθέτουν την ψηφιακή πτυχή της σύγχρονης καθημερινότητας.

Κατά κύριο λόγο, το μοντέλο που ακολουθούν οι παραπάνω τεχνολογίες είναι αυτό της αρχιτεκτονικής πελάτη-εξυπηρετητή (client-server architecture) και προσφέρονται από παρόχους υπηρεσιών υπολογιστικού νέφους (cloud computing service providers). Αυτό σημαίνει ότι οι απαραίτητες λειτουργίες τους, δηλαδή η επεξεργασία (processing), η αποθήκευση των δεδομένων (storage) και το πρωτόκολλο επικοινωνίας (communication protocol) υλοποιούνται επί ενός συγκεντρωτικού (centralized) πλαισίου, κάτι που τους προσδίδει ορισμένα αξιοσημείωτα πλεονεκτήματα (π.χ. ευκολία ανάπτυξης, συντήρησης και αποσφαλμάτωσης).

Στις μέρες μας, ωστόσο, παρατηρείται παράλληλα μία τάση δημιουργίας εφαρμογών που ακολουθούν αποκεντρωτικά μοντέλα λειτουργίας, στα οποία το processing και το storage κατανέμονται σε ένα σύνολο κόμβων που επικοινωνούν ομοτίμα. Εντός, λοιπόν, αυτής της τάσης, αναπτύσσονται με ταχείς ρυθμούς διάφορα λογισμικά, τα οποία συνθέτουν ένα νέο, αποκεντρωτικό οικοσύστημα. Αυτό περιλαμβάνει (μεταξύ άλλων) τόσο καινοτόμα πρωτόκολλα αποθήκευσης δεδομένων (π.χ. IPFS), όσο και πλατφόρμες ανάπτυξης και εκτέλεσης αποκεντρωμένων εφαρμογών (π.χ. Ethereum blockchain).

1.2 Περί αποκέντρωσης

Αν και ο όρος «αποκέντρωση» χρησιμοποιείται ευρέως στην επιστήμη των υπολογιστών και στα κρυπτοοικονομικά¹ (cryptoeconomics), συνήθως ορίζεται αρκετά ασαφώς[2]. Στην πραγματικότητα η αποκέντρωση (ή, αντίστοιχα, ο συγκεντρωτισμός) μπορεί να τοποθετηθεί πάνω σε τρεις ξεχωριστούς άξονες, οι οποίοι είναι σε γενικές γραμμές ανεξάρτητοι ο ένας από τον άλλον. Αυτοί έχουν ως εξής:

- α) **Αρχιτεκτονική** αποκέντρωση: Από πόσους φυσικούς υπολογιστές αποτελείται ένα σύστημα; Πόσοι από αυτούς μπορούν, ανά πάσα στιγμή, να χαλάσουν και εκείνο να αντέξει;
- β) **Πολιτική** αποκέντρωση: Πόσα άτομα ή οργανισμοί ελέγχουν τους υπολογιστές από τους οποίους αποτελείται το σύστημα;
- γ) **Λογική** αποκέντρωση: Η διεπαφή και οι δομές δεδομένων του συστήματος μοιάζουν περισσότερο με ένα μονολιθικό αντικείμενο ή ένα άμορφο σμήνος; Αν, δηλαδή, το σύστημα (συμπεριλαμβανομένων των παρόχων και των χρηστών) «κοπεί στη μέση», θα συνεχίσουν τα δύο μισά να λειτουργούν πλήρως ως ανεξάρτητες μονάδες;

Για παράδειγμα, το BitTorrent είναι αποκεντρωτικό ως προς όλους τους άξονες, ενώ ένα CDN (Content Delivery Network), είναι μόνο αρχιτεκτονικά και λογικά, αφού ελέγχεται από κάποια εταιρεία. Φυσικά, η έννοια μπορεί να γενικευθεί και να μιλάμε για αποκέντρωση μίας επιχείρησης (συνήθως πλήρως συγκεντρωτική) ή μίας γλώσσας (συνήθως πλήρως αποκεντρωτική).

Η επιλογή της δομής ενός συστήματος ως προς την αποκέντρωσή του βασίζεται στις εκάστοτε ανάγκες και στους στόχους του. Μερικά ισχυρά πλεονεκτήματα που διατυπώνονται συχνά για τα αποκεντρωτικά συστήματα είναι τα εξής:

- **Ανοχή σε σφάλματα:** Τα αρχιτεκτονικά αποκεντρωμένα συστήματα είναι λιγότερο πιθανό να αποτύχουν τυχαία, επειδή βασίζονται σε πολλά ξεχωριστά στοιχεία που είναι απίθανο να παρουσιάσουν σφάλματα ταυτόχρονα.
- **Αντοχή σε επιθέσεις:** Το κόστος μίας επίθεσης, που έχει ως στόχο την καταστροφή ή τον χειρισμό ενός αποκεντρωτικού συστήματος, είναι πολύ ακριβό. Αυτό συμβαίνει επειδή δεν υπάρχει κάποιο ευαίσθητο κεντρικό σημείο στο οποίο να μπορεί να πραγματοποιηθεί μία επίθεση, η οποία να έχει κόστος πολύ χαμηλότερο από το οικονομικό μέγεθος του περιβάλλοντος συστήματος.
- **Απουσία ανάγκης εκχώρησης εμπιστοσύνης:** Σε ένα ιδανικό πολιτικά αποκεντρωμένο σύστημα οι χρήστες δε χρειάζεται να εμπιστευονται κάποια κεντρική αρχή για την επεξεργασία και την αποθήκευση των δεδομένων.
- **Αντίσταση σε συμπαιγνίες:** είναι πολύ πιο δύσκολο για τους συμμετέχοντες σε αποκεντρωμένα συστήματα να συνεργαστούν για να ενεργήσουν με τρόπο που τους ωφελεί σε βάρος άλλων συμμετεχόντων.

Ιδιαίτερα τα τελευταία χρόνια, παρατηρείται μία έντονη ανάγκη υλοποίησης αποκεντρωμένων εφαρμογών (decentralized applications), οι οποίες, πέρα από τα αρχιτεκτονικά πλεονεκτήματα που τις χαρακτηρίζουν (π.χ. σταθερότητα, ασφάλεια, επεκτασιμότητα), αποσκοπούν στην

¹Τα «κρυπτοοικονομικά» είναι η πρακτική επιστήμη της δημιουργίας κατανεμημένων συστημάτων, οι ιδιότητες των οποίων εξασφαλίζονται με οικονομικά κίνητρα, ενώ οι οικονομικοί τους μηχανισμοί είναι κρυπτογραφικά εγγυημένοι.[1]

επίτευξη πολιτικής αποκέντρωσης. Αυτό πηγάζει τόσο από την ανάγκη προάσπισης των αρχών που καταστρατηγούνται όταν τα δεδομένα υπάγονται στον έλεγχο κάποιας κεντρικής διαχείρισης (π.χ. της ελευθερίας του λόγου, της ανωνυμίας και της ιδιωτικότητας του χρήστη), όσο και από την ανάγκη δημιουργίας διαδικασιών που απαιτούν εγκυρότητα και αυθεντικότητα, όπως όσων σχετίζονται με την αυτοδιαχείριση και την άμεση δημοκρατία. Ως απόγειο των παραπάνω, μπορούν να θεωρηθούν οι λεγόμενες *αποκεντρωτικές αυτόνομες οργανώσεις* (decentralized autonomous organizations ή DAOs), οι οποίες αποτελούν μία μορφή αλγοκρατικής² οργάνωσης βασισμένης σε τεχνολογίες αποκέντρωσης και, κυρίως, στο blockchain.

1.3 Ορισμός του προβλήματος

Οι περισσότερες διαδεδομένες πλατφόρμες επικοινωνίας (κοινωνικά δίκτυα, mailing lists, forums κ.ά.) είναι ως επί το πλείστον συγκεντρωτικής μορφής, πράγμα το οποίο καθιστά αναγκαία την ύπαρξη κεντρικών αρχών που να τις διαχειρίζονται και να τις συντηρούν.

Παρά τα θετικά της χαρακτηριστικά, η κεντροποιημένη λογική ενός τέτοιου συστήματος αφενός συνοδεύεται από ποικίλα μειονεκτήματα τεχνικής φύσεως (αρχιτεκτονικός συγκεντρωτισμός), αφετέρου εγείρει σοβαρούς προβληματισμούς σχετικά με τη διαχείριση των προσωπικών δεδομένων των χρηστών από τις κεντρικές αρχές (πολιτικός συγκεντρωτισμός). Τα βασικότερα από τα παραπάνω θα μπορούσαν να συνοψιστούν ως εξής:

- **Έλλειψη ασφάλειας:** Τα προσωπικά δεδομένα των χρηστών μπορεί να υποκλαπούν εξαιτίας κάποιας κυβερνοεπίθεσης.
- **Έλλειψη διαθεσιμότητας:** Το σύστημα μπορεί να σταματήσει να λειτουργεί προσωρινά ή μόνιμα για τεχνικούς, οικονομικούς ή νομικούς λόγους.
- **Έλλειψη εμπιστοσύνης:** Οι κεντρικές αρχές έχουν τη δυνατότητα να παρακολουθούν τους χρήστες, να διαβάζουν, ή ακόμα και να διαρρέουν τα προσωπικά τους δεδομένα εν αγνοία των τελευταίων. Οι δε χρήστες δε διαθέτουν κανέναν τρόπο με τον οποίον να μπορούν να τις εμπιστευθούν με βεβαιότητα.
- **Έλλειψη εγγύησης της αυθεντικότητας** των δεδομένων: Οι κεντρικές αρχές έχουν τη δυνατότητα να τροποποιούν τα δεδομένα κατά βούληση κάτι που έχει ως αποτέλεσμα να μην υπάρχει εγγύηση ως προς την αυθεντικότητα όσων βλέπουν οι χρήστες.
- **Έλλειψη εγγύησης της ελευθερίας του λόγου:** Οι κεντρικές αρχές έχουν τη δυνατότητα να λογοκρίνουν τα δεδομένα, είτε βάσει των συμφερόντων τους, είτε βάσει υποχρεώσεων τους προς τρίτους.

Επιπλέον, όπως γίνεται φανερό, οι αδυναμίες του συστήματος ως προς τον πολιτικό άξονα το καθιστούν ακατάλληλο να παρέχει στους χρήστες αυθεντικές και επικυρώσιμες δημοκρατικές διαδικασίες. Τέτοιου είδους διαδικασίες θα μπορούσε να ήταν από απλές ψηφοφορίες, μέχρι σύνθετες διαδικασίες αυτοδιαχείρισης της πλατφόρμας.

²Ο όρος «αλγοκρατία» (algoracry) αναφέρεται σε εναλλακτικές μορφές διακυβέρνησης που βασίζονται στη χρήση αλγορίθμων.[3]

1.4 Στόχος της διπλωματικής

Στόχος της παρούσας διπλωματικής εργασίας είναι η δημιουργία μίας αυτόνομης κοινωνικής πλατφόρμας, η οποία, βασιζόμενη σε τεχνολογίες αποκέντρωσης, θα λειτουργεί ανεξάρτητα από κεντρικές αρχές, παρέχοντας στους χρήστες της πλήρη ελευθερία του λόγου και κυριότητα επί των δεδομένων τους. Παράλληλα, θα παρέχει μία πλατφόρμα για ανώνυμες και αυθεντικές ψηφοφορίες, εν δυνάμει ικανών να αποτελέσουν ένα έγκυρο, έμπιστο και άμεσα δημοκρατικό βήμα λήψης αποφάσεων.

Η proof of concept (PoC) εφαρμογή που αναπτύχθηκε για την επίτευξη του παραπάνω στόχου ονομάζεται Concordia³ και λειτουργεί μέσω ενός συνδυασμού αποκεντρωτικών τεχνολογιών. Πιο συγκεκριμένα, στον επεξεργαστικό πυρήνα της και σαν σημείο αναφοράς αξιοποιεί το Ethereum blockchain, ενώ για την αποθήκευση του μεγαλύτερου όγκου των δεδομένων χρησιμοποιεί το IPFS μέσω της OrbitDB . Η δε διεπαφή του χρήστη υλοποιείται με σύγχρονες μεθόδους web development σε Javascript (React, Redux κ.ά.).

1.5 Μεθοδολογία της διπλωματικής

Η παρούσα διπλωματική είχε έμπνευση τις συζητήσεις μας με τον Δημάκη.

Αρχικά, πραγματοποιήθηκε έρευνα του χώρου των αποκετρωμένων τεχνολογιών με στόχο την κατανόηση των επιπλοκών αυτών των τεχνολογιών τόσο στην ανάπτυξη του κώδικα όσο και στην χρήση...

Στα πρώτα στάδια της έρευνας εξοικειωθήκαμε με τον χώρο

Έπειτα, έγιναν μερικές πρώτες προσπάθειες για τη δημιουργία ενός proof of concept application...

1.6 Οργάνωση κεφαλαίων

Η παρούσα διπλωματική εργασία οργανώνεται σε κεφάλαια, ενότητες και υποενότητες, όπως αυτά παρατίθενται στα Περιεχόμενα. Πιο συγκεκριμένα:

- Στο Κεφάλαιο 1
- Στο Κεφάλαιο 2
- Στο Κεφάλαιο 3
- Στο Κεφάλαιο 4
- Στο Κεφάλαιο 5

³Η Concordia είναι η θεά της αρχαίας Ρωμαϊκής θρησκείας που προσωποποιεί την ομόνοια. Στην ελληνική μυθολογία ταυτίζεται με τη θεότητα Ομόνοια ή τη θεά Αρμονία.

Κεφάλαιο 2

Θεωρητικό υπόβαθρο

2.1 Συναρτήσεις κατακερματισμού

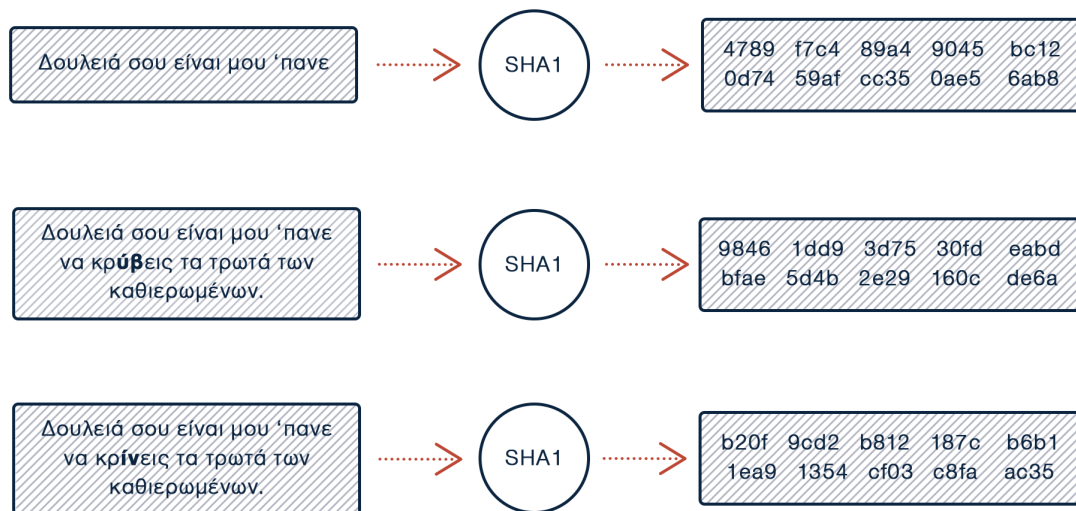
Οι κρυπτογραφικές συναρτήσεις κατακερματισμού (cryptographic hash functions) είναι ειδική κατηγορία συναρτήσεων κατακερματισμού σχεδιασμένες για χρήση στην κρυπτογραφία. Αποτελούν μαθηματικές συναρτήσεις που δέχονται ως είσοδο δεδομένα τυχαίου μεγέθους και επιστρέφουν συμβολοσειρές σταθερού μήκους.



Σχήμα 2.1: Λειτουργία συνάρτησης κατακερματισμού

Οι τιμές που επιστρέφει η συνάρτηση κατακερματισμού ονομάζονται τιμές κατακερματισμού (hash values, digests ή απλά hashes). Μία ιδανική κρυπτογραφική συνάρτηση κατακερματισμού έχει τις εξής βασικές ιδιότητες:

- Είναι ντετερμινιστική, δηλαδή η ίδια είσοδος παράγει πάντα την ίδια έξοδο.
- Είναι μη αντιστρέψιμη, δηλαδή είναι πρακτικά ανέφικτο να υπολογιστεί η είσοδος δεδομένης μιας εξόδου.
- Είναι αμφιμονοσήμαντη (1-1), δηλαδή σε δύο διαφορετικές εισόδους αντιστοιχούν πάντα δύο εντελώς διαφορετικές εξοδοί.
- Είναι αποδοτική, δηλαδή ο υπολογισμός του hash οποιασδήποτε εισόδου είναι γρήγορος.



Σχήμα 2.2: Παράδειγμα λειτουργίας συνάρτησης κατακερματισμού

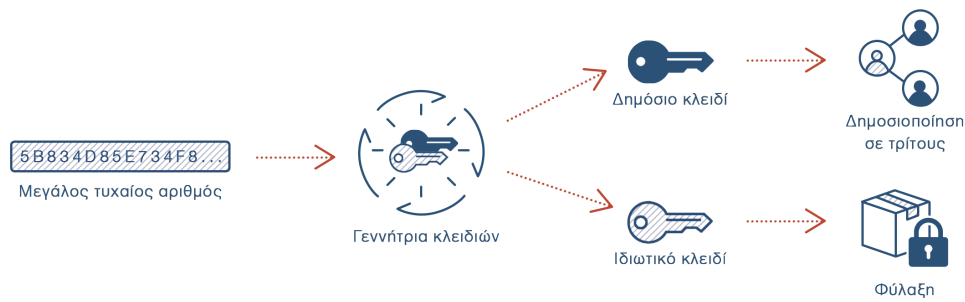
Μία από τις δημοφιλέστερες οικογένειες κρυπτογραφικών αλγορίθμων κατακερματισμού είναι αυτή των Secure Hash Algorithms (SHA), η οποία περιλαμβάνει τους SHA-0, SHA-1, SHA-2 και SHA-3.

2.2 Ασύμμετρη κρυπτογραφία

Η ασύμμετρη κρυπτογραφία (asymmetric cryptography) ή κρυπτογραφία δημόσιου κλειδιού (public-key cryptography) αποτελεί κρυπτογραφικό σύστημα που βασίζεται στη χρήση ενός ζεύγους κλειδιών (key pair), του δημόσιου (public key) και του ιδιωτικού (private key). Αυτά τα κλειδιά είναι μαθηματικά συνδεδεμένα ως εξής:

- Το ιδιωτικό κλειδί δε μπορεί να προκύψει γνωρίζοντας το δημόσιό του
- Ό,τι κρυπτογραφηθεί από το ένα μπορεί να αποκρυπτογραφηθεί μόνο από το άλλο

Η δημιουργία ενός ζεύγους κλειδιών επιτυγχάνεται μέσω μιας γεννήτριας κλειδιών (key generation function), η οποία χρησιμοποιεί ειδικούς αλγορίθμους (π.χ. RSA), δεχόμενη ως είσοδο έναν τυχαίο αριθμό. Από τα παραχθέντα κλειδιά, το δημόσιο γνωστοποιείται σε τρίτους, ενώ το ιδιωτικό παραμένει μυστικό.

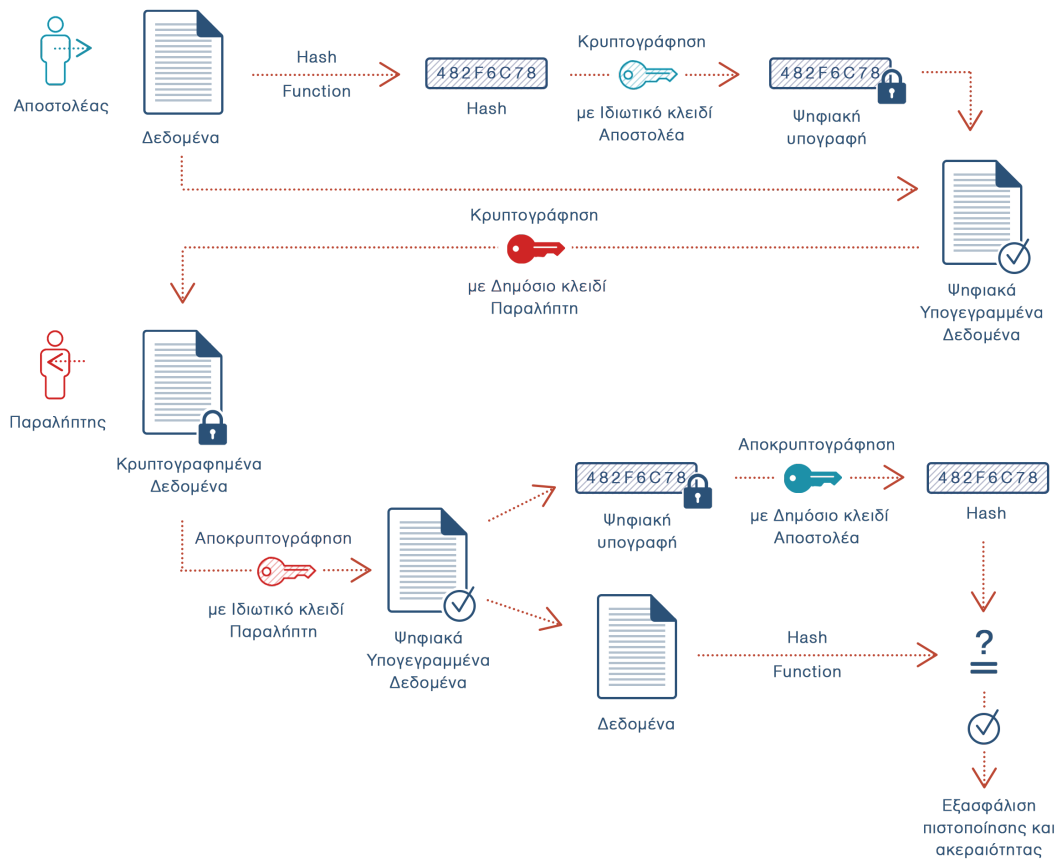


Σχήμα 2.3: Παραγωγή ασύμμετρου ζεύγους κλειδιών

Ο χρήστης μπορεί να χρησιμοποιήσει τα κλειδιά για δύο βασικούς σκοπούς:

- α) Για να αποκρυπτογραφήσει μηνύματα άλλων χρηστών, οι οποίοι τα κρυπτογράφησαν χρησιμοποιώντας το δημόσιο κλειδί του. Με αυτόν τον τρόπο εξασφαλίζεται η *εμπιστευτικότητα* (confidentiality).
- β) Για να υπογράψει ψηφιακά ένα μήνυμα, κρυπτογραφώντας το hash των δεδομένων του με το ιδιωτικό του κλειδί. Έτσι, ο παραλήπτης του μηνύματος μπορεί μέσω της ληφθείσας *ψηφιακής υπογραφής* (digital signature):
 - i. Να επαληθεύσει την ταυτότητα του αποστολέα, αποκρυπτογραφώντας επιτυχώς την ψηφιακή υπογραφή με το δημόσιο κλειδί του τελευταίου. Εξασφαλίζεται έτσι η *πιστοποίηση* (authenticity) της προέλευσης των δεδομένων.
 - ii. Να επιβεβαιώσει ότι το μήνυμα έφτασε αναλλοίωτο, εφόσον το hash των δεδομένων συμπίπτει με το hash εντός της ψηφιακής υπογραφής. Με αυτόν τον τρόπο εξασφαλίζεται η *ακεραιότητα* (integrity) των δεδομένων.

Με τον συνδυασμό των παραπάνω, λέμε ότι δύο χρήστες μπορούν να επικοινωνούν μεταξύ τους με *κρυπτογράφηση απ' άκρη σ' άκρη* (end to end encryption).



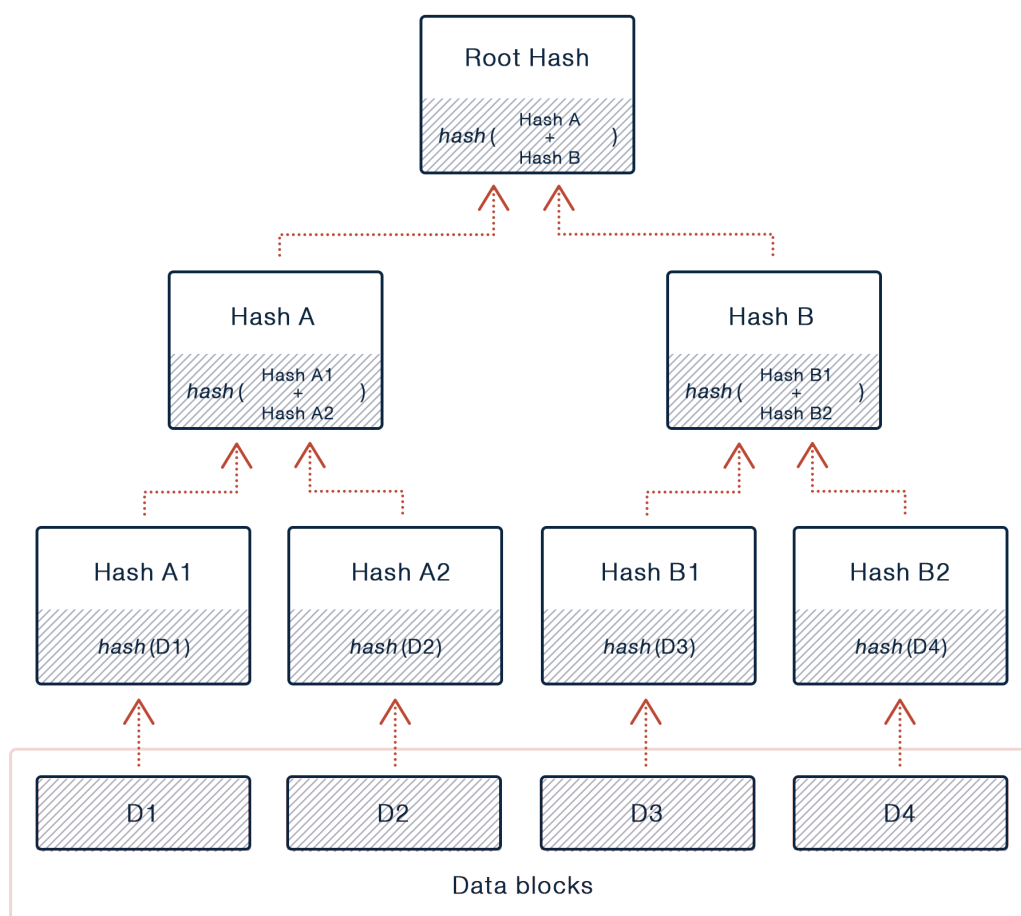
Σχήμα 2.4: Κρυπτογράφηση απ' άκρη σ' άκρη

Μία προσέγγιση στην κρυπτογραφία δημόσιου κλειδιού είναι η κρυπτογραφία ελλειπτικής καμπύλης (Elliptic-Curve Cryptography ή ECC). Η ECC βασίζεται στην αλγεβρική δομή των ελλειπτικών καμπυλών σε πεπερασμένα πεδία και υπερέχει της non-EC κρυπτογραφίας, καθώς επιτρέπει τη δημιουργία μικρότερων κλειδιών με ισοδύναμη ασφάλεια. Ένα από τα πρωτόκολλα της είναι ο Elliptic Curve Digital Signature Algorithm (ECDSA), ο οποίος χρησιμοποιείται για την ψηφιακή υπογραφή δεδομένων και αποτελεί το EC-ανάλογο του DSA (Digital Signature Algorithm).[4]

2.3 Δένδρα Merkle

Ένα δένδρο Merkle (Merkle tree ή hash tree) είναι μία δενδρική δομή δεδομένων, η οποία απαρτίζεται από φύλλα (leaf nodes), που περιέχουν hashes από blocks δεδομένων, και από άλλους κόμβους (non-leaf nodes), οι οποίοι περιέχουν τα hashes των θυγατρικών τους. Στην κορυφή του δένδρου βρίσκεται ο ριζικός κόμβος με το λεγόμενο root hash.[5]

Η πιο συνηθισμένη υλοποίηση είναι το δυαδικό (binary) δένδρο Merkle, το οποίο περιλαμβάνει δύο θυγατρικούς κόμβους (child nodes) κάτω από κάθε γονικό non-leaf κόμβο, και είναι αυτό που αναλύεται στη συνέχεια.



Σχήμα 2.5: Παράδειγμα δυαδικού δένδρου Merkle

Τα Merkle trees επιτρέπουν την αποδοτική και ασφαλή επαλήθευση των περιεχομένων που ανήκουν σε σετ δεδομένων μεγάλου μεγέθους. Η βασική ιδιότητα είναι ότι για κάθε σετ δεδομένων υπάρχει ακριβώς ένα πιθανό δένδρο, το οποίο δε γίνεται να τροποποιηθεί χωρίς να αλλάξει ταυτόχρονα και το root hash.

Έτσι, μέσω των λεγόμενων Merkle proofs, μπορούμε:

- Να αποφανθούμε εάν κάποια δεδομένα ανήκουν στο δένδρο (με τον αριθμό των hashes που θα πρέπει να υπολογιστούν να είναι ανάλογος του λογαρίθμου του αριθμού των leaf nodes).
- Να αποδείξουμε συνοπτικά την εγκυρότητα ενός τμήματος κάποιου σετ δεδομένων, χωρίς να χρειαστεί να αποθηκεύσουμε ολόκληρο το σύνολο δεδομένων.
- Να διασφαλίσουμε την εγκυρότητα ενός συγκεκριμένου συνόλου δεδομένων εντός ενός μεγαλύτερου συνόλου, χωρίς να χρειαστεί να αποκαλυφθεί το περιεχόμενο οποιουδήποτε εκ των δύο.[6]

2.4 Δίκτυα Ομότιμων Κόμβων

Τα δίκτυα ομότιμων κόμβων ή Peer-to-Peer (P2P) networks αποτελούν μία κατακεντρωμένη αρχιτεκτονική δικτύων, οι συμμετέχοντες (κόμβοι) της οποίας μοιράζονται ένα τμήμα των πόρων τους, με στόχο την παροχή κάποιων υπηρεσιών (π.χ. τον διαμοιρασμό περιεχομένου). Εν αντιθέσει με συγκεντρωτικά δίκτυα τύπου client/server, οι κόμβοι (nodes) έχουν απευθείας πρόσβαση στους πόρους, χωρίς τη διαμεσολάβηση ενδιάμεσων οντοτήτων. Οι συμμετέχοντες ενός τέτοιου δικτύου είναι, δηλαδή, ταυτόχρονα, τόσο πάροχοι, όσο και αιτούντες των πόρων και της παρεχόμενης υπηρεσίας.[7]

Τα P2P networks μπορούν να χωριστούν σε δύο κατηγορίες:

- Στα «Καθαρά» (Pure) P2P networks, στα οποία ισχύει ότι η αφαίρεση ενός τυχαίου κόμβου από το δίκτυο δεν προκαλεί κάποιο πρόβλημα σε αυτό.
- Στα «Υβριδικά» (Hybrid) P2P networks, στα οποία συμμετέχουν επιπλέον και κεντρικές οντότητες, παρέχοντας απαραίτητα τμήματα των προσφερόμενων υπηρεσιών.

Από εδώ και στο εξής, εάν δεν αναφέρεται ρητά η κατηγορία κάποιου P2P network, θα εννοείται ότι ανήκει στην πρώτη.

2.5 Blockchain

Το blockchain αποτελεί μία διανεμημένη δημόσια σειρά δεδομένων, που διατηρεί έναν αμετάβλητο ως προς το ιστορικό του κατάλογο (immutable ledger) ψηφιακών συναλλαγών (digital transactions) ενός αγαθού (asset), π.χ. ενός νομίσματος (token). Περιγράφηκε για πρώτη φορά το 2008 από ένα άτομο (ή μία ομάδα ανθρώπων) γνωστό ως Satoshi Nakamoto, αποτελώντας τη βάση του κρυπτονομίσματος (cryptocurrency) Bitcoin.[8]

Δομικό στοιχείο του blockchain είναι το μπλοκ (block), το οποίο περιέχει μία ομάδα έγκυρων συναλλαγών που έχουν κατακερματιστεί και κωδικοποιηθεί σε ένα δένδρο Merkle, το hash του προηγούμενου μπλοκ και μερικά ακόμα μεταδεδομένα (π.χ. nonce, timestamp). Έτσι, κάθε νέο μπλοκ «δείχνει» στο προηγούμενό του μέσω του hash, επιβεβαιώνοντας την ακεραιότητά του, με τα διαδεχόμενα μπλοκ να σχηματίζουν τελικά μία αλυσίδα, μέχρι το αρχικό μπλοκ, το οποίο είναι γνωστό ως το μπλοκ γένεσης (genesis block).[9]

Ως προς την κυριότητα επί αυτού, το blockchain συνήθως⁴ δεν ελέγχεται από κάποια κεντρική οντότητα, αλλά διατηρείται από ένα δημόσιο P2P δίκτυο. Οι κόμβοι (nodes) του δικτύου συμμορφώνονται συλλογικά με ένα πρωτόκολλο συναίνεσης (consensus) για την επικοινωνία και την επικύρωση νέων μπλοκ. Για παράδειγμα, στο Bitcoin, το consensus επιτυγχάνεται μέσω ενός Proof of Work (PoW) αλγορίθμου, όπου οι κόμβοι (miners) ανταγωνίζονται ο ένας τον άλλον για το ποιος θα λύσει πρώτος ένα σύνθετο αλγοριθμικό πρόβλημα που συσχετίζεται με το εκάστοτε block. Αυτός που θα τα καταφέρει επιβραβεύεται για την επεξεργαστική ισχύ που δαπάνησε με ένα ποσό από bitcoin. Εκείνα είναι εν μέρει νέα νομίσματα που κόβονται ή «εξορύσσονται» εκείνη τη στιγμή (όπως ορίζεται από το πρωτόκολλο), αλλά και όσα τέλη (fees) κατέβαλαν οι κόμβοι για να πραγματοποιήσουν τις συναλλαγές του μπλοκ. Αξίζει να σημειωθεί πως δεν είναι αναγκαίο να διαθέτει κανείς ολόκληρο το blockchain (το οποίο είναι ογκώδες) - δηλαδή έναν πλήρη κόμβο - για να επικοινωνήσει με το δίκτυο, αλλά αρκεί ένας light node που απλά αναμεταδίδει την συναλλαγή που επιθυμεί να πραγματοποιήσει ο χρήστης.

⁴Υπάρχουν και κάποιες υλοποιήσεις ιδιωτικών blockchain που, όμως, δε θα μας απασχολήσουν.

Η διευθυνσιοδότηση σε ένα blockchain επιτυγχάνεται αξιοποιώντας την κρυπτογραφία δημόσιου κλειδιού. Το πρωτόκολλο του εκάστοτε blockchain ορίζει έναν αλγόριθμο για την παραγωγή ζευγών κλειδιών (π.χ. ECDSA στο Bitcoin). Το δημόσιο από αυτά ορίζει τη διεύθυνση, ενώ το ιδιωτικό παραμένει μυστικό, υπό την κατοχή του χρήστη. Με αυτό τον τρόπο προκύπτει ένα πρακτικά ανεξάντλητο πλήθος πιθανών έγκυρων δημόσιων διευθύνσεων (π.χ. 2^{160} για το Bitcoin), στις οποίες οι χρήστες μπορούν να στέλνουν και να λαμβάνουν ποσά του εκάστοτε κρυπτονομίσματος. Για την αποστολή ενός ποσού, δηλώνουν το fee που επιθυμούν να καταβάλουν και υπογράφουν την επιθυμητή συναλλαγή με το ιδιωτικό τους κλειδί. Η συναλλαγή αναμεταδίδεται στο δίκτυο και παραμένει στο transaction pool μέχρις ότου να γίνει αποδεκτή και να συμπεριληφθεί στο επόμενο block.

Από τεχνική σκοπιά, το blockchain μπορεί να θεωρηθεί ως μία μηχανή καταστάσεων βασισμένη σε συναλλαγές (transaction-based state machine). Δηλαδή, ξεκινάει από μία αρχική κατάσταση (genesis state), η οποία τροποποιείται σταδιακά με κάθε block, και περιλαμβάνει ανά πάσα στιγμή τις διευθύνσεις με τα ποσά των νομισμάτων που τις αντιστοιχούν.

Σύμφωνα με την ανάλυση της ενότητας 1.2, το blockchain είναι αρχιτεκτονικά και πολιτικά αποκεντρωτικό, καθώς δεν διαθέτει δοκιμικά κάποιο κεντρικό σημείο αποτυχίας, ούτε ελέγχεται από κάποιον. Ωστόσο, είναι λογικά συγκεντρωτικό, αφού υπάρχει μία κοινά αποδεκτή κατάσταση και το σύστημα συμπεριφέρεται μακροσκοπικά ως ένας ενιαίος υπολογιστής.

2.6 Ethereum



Σχήμα 2.6: Ethereum logo

Το Ethereum είναι ένα δημόσιο blockchain ανοιχτού κώδικα με εγγενές κρυπτονόμισμα το Ether (ETH). Παρέχει μία προγραμματιστική πλατφόρμα με ενσωματωμένη μία Turing-complete γλώσσα προγραμματισμού, που μπορεί να χρησιμοποιηθεί για τη δημιουργία αποκεντρωμένων εφαρμογών (Decentralized Applications ή DApps) μέσω της χρήσης «έξυπνων συμβολαίων» (smart contracts).[10]

2.6.1 Λογαριασμοί

Στο Ethereum blockchain οι λογαριασμοί αποτελούν οντότητες οι οποίες μπορούν να δέχονται, να κρατούν και να στέλνουν ETH και tokens, καθώς και να αλληλεπιδρούν με smart contracts.[11] Χωρίζονται σε δύο κατηγορίες: στους λογαριασμούς εξωτερικής κατοχής (externally owned accounts ή EOAs) και στους λογαριασμούς συμβολαίων (contract accounts).

Οι λογαριασμοί εξωτερικής κατοχής δημιουργούνται χωρίς κόστος και ελέγχονται μέσω ιδιωτικών κλειδιών. Μπορούν να πραγματοποιούν μόνο συναλλαγές μεταφοράς ETH ή κάποιου token.

Από την άλλη, οι λογαριασμοί συμβολαίων απαιτούν κάποιο κόστος δημιουργίας, καθώς χρησιμοποιούν αποθηκευτικό χώρο επί του blockchain, ενώ ελέγχονται αποκλειστικά από τον κώδικά τους. Οι συναλλαγές που πραγματοποιούν προς άλλους λογαριασμούς είναι μόνο σαν αντίδραση σε μία εισερχόμενη συναλλαγή, όπως ορίζει ο κώδικας του smart contract τους.

Πιο αναλυτικά, τα πεδία που διαθέτουν οι λογαριασμοί στο Ethereum είναι τα εξής:

- Το **nonce**: ένας μετρητής που υποδεικνύει τον αριθμό των απεσταλμένων συναλλαγών του λογαριασμού. Αυτό διασφαλίζει ότι οι συναλλαγές διεκπεραιώνονται μόνο μία φορά. Σε έναν λογαριασμό συμβολαίου, αυτός ο αριθμός αντιπροσωπεύει τον αριθμό των συμβολαίων που δημιουργήθηκαν από εκείνον.
- Το **balance**: το ποσό σε ETH που διαθέτει ο λογαριασμός, μετρημένο σε wei (1 ETH = 10^{18} wei).
- Το **codeHash**: ένα hash που αναφέρεται στον κώδικα του λογαριασμού (contract code). Είναι χαρακτηριστικό των λογαριασμών συμβολαίων (στους λογαριασμούς εξωτερικής κατοχής είναι hash μίας κενής συμβολοσειράς) και, σε αντίθεση με τα άλλα πεδία, αφότου οριστεί παραμένει αμετάβλητο.
- Το **storageRoot**: το root hash του δένδρου Merkle των αποθηκευμένων δεδομένων του smart contract, εφόσον πρόκειται για έναν λογαριασμό συμβολαίου (δε χρησιμοποιείται σε λογαριασμούς εξωτερικής κατοχής).

Η δημιουργία των λογαριασμών επιτυγχάνεται μέσω της παραγωγής ενός ζεύγους κλειδιών, αξιοποιώντας τον ECDSA (βλ. ενότητα 2.2). Έτσι, το ιδιωτικό κλειδί χρησιμοποιείται για να υπογράφονται ψηφιακά οι συναλλαγές, ενώ το δημόσιο ορίζει τη δημόσια διεύθυνση του λογαριασμού (είναι της μορφής «0x + τα 20 τελευταία bytes του Keccak-256⁵ hash του δημόσιου κλειδιού»).

Κατά κύριο λόγο, οι χρήστες παράγουν και διαχειρίζονται τα ιδιωτικά κλειδιά των λογαριασμών εξωτερικής κατοχής μέσω ενός πορτοφολιού (wallet). Τα wallets αποτελούν εφαρμογές, οι οποίες δείχνουν το balance του λογαριασμού και παρέχουν τη δυνατότητα αποστολής/λήψης ETH και tokens από/σε αυτόν. Ορισμένα προτοφόλια προσφέρουν περαιτέρω λειτουργίες, σημαντικότερη εκ των οποίων είναι η διασύνδεση του λογαριασμού με αποκεντρωμένες εφαρμογές. Επί του παρόντος, το πιο διαδεδομένο πορτοφόλι τέτοιου τύπου είναι το MetaMask⁶.

2.6.2 Smart Contracts

Με λίγα λόγια, τα smart contracts αποτελούν αυτόνομα κομμάτια κώδικα, τα οποία είναι αποθηκευμένα στο blockchain και ενεργοποιούνται μέσω συναλλαγών. Κληρονομούν ιδιότητες του blockchain, όπως τη διαφάνεια (transparency), την επαληθευστικότητα (verifiability) και την αμεταβλητότητα (immutability).

Ένα παράδειγμα της καθημερινότητας που μπορεί να παρομοιασθεί λειτουργικά με smart contract είναι ο αυτόματος πωλητής.[12] Ένας αυτόματος πωλητής ορίζεται ως ένα αυτόνομο μηχανήμα που διανέμει αγαθά ή παρέχει υπηρεσίες, όταν εισαχθεί σε αυτόν κάποιο χρηματικό ποσό και επιλεγθεί ένα διαθέσιμο προϊόν. Οι αυτόματοι πωλητές είναι προγραμματισμένοι να εκτελούν συγκεκριμένους κανόνες που θα μπορούσαν να οριστούν σε ένα συμβόλαιο. Με όμοιο τρόπο, σε ένα smart contract μπορούν να κωδικοποιηθούν αυθαίρετες συναρτήσεις μετάβασης, επιτρέποντας τη δημιουργία μίας πληθώρας αποκεντρωμένων εφαρμογών.

Όπως προαναφέρθηκε στην υποενότητα 2.6.1, τα smart contracts εντάσσονται σε contract accounts και απαιτούν την καταβολή τελών για τη δημιουργία τους, αφού χρειάζεται να εγγραφούν επί του blockchain τον κώδικα και τα αρχικά δεδομένα τους.

Επιπλέον, ο κώδικάς τους ενεργοποιείται μονάχα όταν δεχθούν μία έγκυρη συναλλαγή από κάποιον άλλον λογαριασμό (είτε εξωτερικής κατοχής, είτε συμβολαίου). Η συναλλαγή αυτή

⁵Ο Keccak-256 αποτελεί τον κρυπτογραφικό αλγόριθμο κατακερματισμού που χρησιμοποιείται στο Ethereum. Πρόκειται για τον αλγόριθμο SHA3-256 πριν την τυποποίησή του από το NIST.

⁶Επίσημος ιστότοπος: <https://metamask.io/>

εμπεριέχει, πέρα από το απαιτούμενο fee, ένα συνοδευτικό μήνυμα με πληροφορίες σχετικές με τη συνάρτηση που πρέπει να εκτελεστεί. Η δε συνάρτηση μπορεί να πραγματοποιεί ποικίλες διαφορετικές ενέργειες, όπως την ανάγνωση και την εγγραφή στην εσωτερική αποθήκευση, την πραγματοποίηση νέων συναλλαγών, ή, ακόμα, τη δημιουργία νέων συμβολαίων.

Η σύνταξη των smart contracts γίνεται κατά βάση σε γλώσσες υψηλού επιπέδου και, συγκεκριμένα, στις Solidity και Vyper. Πριν την εγγραφή τους στο blockchain, μεταγλωττίζονται σε εμμενέσιμο από την EVM bytecode, η οποία είναι υπεύθυνη για την αποθήκευση και την εκτέλεσή του (βλ. υποενότητα 2.6.5).

2.6.3 DApps

Οι DApps στο οικοσύστημα του Ethereum είναι εφαρμογές οι οποίες συνδυάζουν smart contracts και frontend UIs. Είναι ντετερμινιστικές, Turing-complete και εκτελούνται απομονωμένα στην EVM.[11]

Πέρα από τα θετικά χαρακτηριστικά των DApps που αναλύθηκαν στην ενότητα 1.2 (ανοχή σε σφάλματα, αντοχή σε επιθέσεις, απουσία ανάγκης εκχώρησης εμπιστοσύνης, αντίσταση σε συμπαιγνίες), τα Ethereum DApps διαθέτουν επιπλέον όλα τα πλεονεκτήματα των blockchain και των smart contract, όπως μηδενικό downtime, πλήρη ακεραιότητα δεδομένων και επαληθεύσιμη συμπεριφορά.

Ωστόσο, χαρακτηρίζονται και από μία σειρά αξιοσημείωτων μειονεκτημάτων, όπως τα παρακάτω:

- Δυσκολία συντήρησης: Συντηρούνται δυσκολότερα από τις συγκεντρωτικές εφαρμογές, εξαιτίας της αμεταβλητότητας του κώδικα και των δεδομένων επί του blockchain.
- Επιβάρυνση απόδοσης: Υπάρχει τεράστια επιβάρυνση απόδοσης (performance overhead) και η κλιμάκωση (scaling) είναι πολύ δύσκολη, καθώς απαιτείται όλοι οι κόμβοι να εκτελούν και να αποθηκεύουν όλες τις συναλλαγές.
- Συμφόρηση δικτύου: Επί του παρόντος, το δίκτυο μπορεί να επεξεργαστεί μόνο περίπου 10-15 συναλλαγές ανά δευτερόλεπτο. Εάν οι συναλλαγές αποστέλλονται με ταχύτερο ρυθμό από αυτόν, θα αυξάνονται παράλληλα και οι μη επιβεβαιωμένες συναλλαγές που αναμένουν να εκτελεστούν.
- Κακή εμπειρία χρήστη: Επί του παρόντος, είναι δύσκολο για τον μέσο τελικό χρήστη να αλληλεπιδράσει με το blockchain με ευκολία και ασφάλεια, καθώς απαιτούνται ενέργειες όπως η εγκατάσταση ειδικών εργαλείων για τη διασύνδεση με αυτό, η δημιουργία wallet, η διαφύλαξη του ιδιωτικού του κλειδιού και η προσθήκη ETH για την εξόφληση των τελών.

Παρ' όλα τα μειονεκτήματα, τα οποία μετριαζονται με τον καιρό μέσω συνεχών αναβαθμίσεων της πλατφόρμας, υπάρχει ήδη ένα ευρύ φάσμα εφαρμογών που μπορούν να υλοποιηθούν στο Ethereum, αξιοποιώντας τα ισχυρά του πλεονεκτήματα. Οι εφαρμογές αυτές μπορούν να διακριθούν σε τρεις κατηγορίες:

- α) Οικονομικές εφαρμογές, οι οποίες παρέχουν στους χρήστες ισχυρούς τρόπους διαχείρισης και σύναψης συμβάσεων χρησιμοποιώντας τα χρήματά τους. Αυτό περιλαμβάνει υπονομίσματα, χρηματοοικονομικά παράγωγα, συμβάσεις αντιστάθμισης κινδύνου, πορτοφόλια αποταμίευσης, διαθήκες και ακόμα και ορισμένες κατηγορίες συμβάσεων εργασίας πλήρους κλίμακας.

- β) Ημι-οικονομικές εφαρμογές, όπου εμπλέκονται χρήματα, αλλά η λειτουργία τους εμπεριέχει παράλληλα και μία αξιοσημείωτη μη νομισματική πλευρά. Ένα τέτοιο παράδειγμα είναι οι αυτόματες πληρωμές για λύσεις σε υπολογιστικά προβλήματα (βλ. Gitcoin).
- γ) Μη οικονομικές εφαρμογές, όπως η αποκεντρωμένη αποθήκευση δεδομένων, συστήματα ταυτότητας (identity) και φήμης (reputation), διαδικτυακές ψηφοφορίες και αποκεντρωμένη διακυβέρνηση. Οι τελευταίες εισάγουν και την έννοια των Αποκεντρωμένων Αυτόνομων Οργανώσεων (Decentralized Autonomous Organizations ή DAOs), οντοτήτων που ενεργούν αυτόνομα, χωρίς την ανάγκη διαμεσολάβησης κάποιας συγκεντρωτικής (centralized) αρχής.[10]

2.6.4 Tokens

Η λέξη «token» προέρχεται από τη λέξη «tācen» των Παλαιών Αγγλικών και σημαίνει σημάδι ή σύμβολο. Στην καθημερινότητα, ο όρος χρησιμοποιείται, κατά κύριο λόγο, για την περιγραφή αντικειμένων ειδικού σκοπού, τα οποία μοιάζουν με κέρματα και έχουν ασήμαντη εγγενή αξία (π.χ. μάρκες παιχνιδιών). Συνήθως, η χρήση των tokens περιορίζεται σε συγκεκριμένες επιχειρήσεις, οργανισμούς ή τοποθεσίες, πράγμα το οποίο σημαίνει ότι δεν ανταλλάσσονται εύκολα και τυπικά έχουν μόνο μία λειτουργία.[13]

Ωστόσο, στο Ethereum blockchain η έννοια των tokens επεκτείνεται και επαναπροσδιορίζεται. Πλέον δεν υπάρχουν περιορισμοί χρήσης και ιδιοκτησίας, ενώ η αξία τους ποικίλει, ανάλογα με το τι αντιπροσωπεύουν (π.χ. νομίσματα, περιουσιακά στοιχεία, ή δικαιώματα πρόσβασης). Μπορούν, δε, να ανταλλαχθούν σε παγκόσμιο επίπεδο, για άλλα tokens ή για άλλα νομίσματα.

Τα tokens που ορίζονται σε Ethereum smart contracts μπορούν να έχουν μία ή περισσότερες από τις παρακάτω χρήσεις:

- Νόμισμα (currency)
- Πόρος (resource), π.χ. για το διαμοιρασμό CPU ή storage εντός ενός δικτύου
- Περιουσιακό στοιχείο (asset), εγγενούς ή εξωγενούς, υλικού ή άυλου (π.χ. χρυσός, πετρέλαιο, ενέργεια, ακίνητο)
- Πρόσβαση (access), ψηφιακή ή φυσική (π.χ. forum, δωμάτιο ξενοδοχείου)
- Μετοχικό κεφάλαιο (equity) ενός ψηφιακού οργανισμού (π.χ. μίας DAO) ή μίας νομικής οντότητας (π.χ. μίας εταιρείας)
- Ψηφοφορία (voting), παρέχοντας δικαιώματα ψήφου σε ένα ψηφιακό ή νομικό σύστημα
- Συλλεκτικό (collectible), ψηφιακό ή φυσικό
- Ταυτότητα (identity), ψηφιακής ή νομικής φύσεως
- Πιστοποίηση (attestation), π.χ. πτυχίο, πιστοποιητικό γέννησης
- Χρησιμότητα (utility), για πρόσβαση ή πληρωμή μίας υπηρεσίας

Ένα σημαντικό κριτήριο κατηγοριοποίησης των tokens είναι η εναλλαξιμότητα (fungibility) τους. Ένα token είναι εναλλάξιμο όταν οποιαδήποτε μονάδα του μπορεί να αντικατασταθεί με μία άλλη χωρίς καμία διαφορά στην αξία ή τη λειτουργία του. Από την άλλη πλευρά, ένα non-fungible token (NFT) αντιπροσωπεύει ένα μοναδικό υλικό ή άυλο στοιχείο και, επομένως, είναι μη εναλλάξιμο.

Τέλος, τα tokens συχνά ακολουθούν κάποια καθορισμένα standards στην υλοποίησή τους. Τα δημοφιλέστερα από αυτά είναι τα ERC-20 και ERC-777 (για fungible tokens), το ERC-721 (για NFTs) και το ERC-1155 (για semi-fungible tokens ή SFTs).

2.6.5 EVM

Τα smart contracts (και, κατ' επέκταση, οι DApps) εκτελούνται από την εικονική μηχανή του Ethereum (Ethereum Virtual Machine ή EVM). Η EVM αποτελεί μία quasi⁷-Turing-complete μηχανή καταστάσεων αρχιτεκτονικής βασισμένης σε στοίβα (stack-based architecture). Σε υψηλό επίπεδο, η EVM μπορεί να θεωρηθεί ως ένας παγκόσμιος αποκεντρωμένος υπολογιστής που περιέχει εκατομμύρια εκτελέσιμα αντικείμενα, το καθένα με τη δική του μόνιμη αποθήκη δεδομένων.

Η EVM αποθηκεύει όλες τις τιμές της μνήμης σε μια στοίβα και λειτουργεί με μέγεθος λέξης 256 bit, κυρίως για τη διευκόλυνση των εγγενών λειτουργιών κατακερματισμού και ελλειπτικής καμπύλης. Διαθέτει ένα σύνολο διευθυνσιοδοτήσιμων στοιχείων δεδομένων:

- Έναν αμετάβλητο κώδικα προγράμματος σε εικονική μνήμη ROM, φορτωμένο με τον bytecode του smart contract προς εκτέλεση.
- Μία πτητική (volatile) μνήμη, με κάθε θέση ρητά αρχικοποιημένη στο μηδέν.
- Ένας χώρος μόνιμης αποθήκευσης, που είναι μέρος του Ethereum state, επίσης αρχικά μηδενισμένος.

Υπάρχει, επίσης, ένα σύνολο μεταβλητών περιβάλλοντος και δεδομένων, τα οποία είναι διαθέσιμα κατά την εκτέλεση.[13]

2.7 IPFS



Σχήμα 2.7: IPFS logo

Το IPFS (InterPlanetary File System) είναι ένα P2P πρωτόκολλο υπερμέσων, σχεδιασμένο για να διατηρήσει και να αυξήσει τη γνώση της ανθρωπότητας κάνοντας το διαδίκτυο αναβαθμισμένο, ανθεκτικό και πιο ανοιχτό.[14] Πρακτικά πρόκειται για ένα κατακερματισμένο σύστημα για αποθήκευση και πρόσβαση σε αρχεία, ιστότοπους, εφαρμογές και δεδομένα. Το περιεχόμενο είναι προσβάσιμο μέσω ενός δικτύου ομότιμων κόμβων που βρίσκονται οπουδήποτε στον κόσμο, οι οποίοι ενδέχεται να αποθηκεύουν πληροφορία, να τη μεταφέρουν (relay nodes) ή και τα δύο.[15]

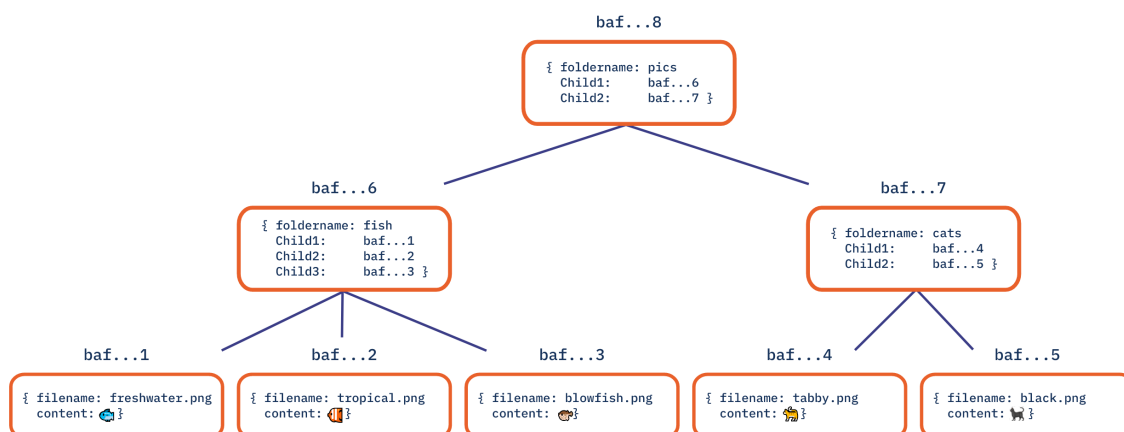
Ο τρόπος λειτουργίας του IPFS βασίζεται στα εξής:

- **Μοναδική ταυτοποίηση μέσω διευθυνσιοδότησης περιεχομένου (content addressing).** Το περιεχόμενο δεν προσδιορίζεται από την τοποθεσία του (π.χ. <https://...>), αλλά από το

⁷«Quasi» («σχεδόν») επειδή όλες οι διαδικασίες εκτέλεσης περιορίζονται σε έναν πεπερασμένο αριθμό υπολογιστικών βημάτων από την ποσότητα gas που είναι διαθέσιμη για οποιαδήποτε εκτέλεση ενός smart contract.

τι περιλαμβάνει. Κάθε κομμάτι περιεχομένου έχει ένα μοναδικό αναγνωριστικό (Content ID ή CID), το οποίο είναι το hash του σε μορφή multihash (<https://multiformats.io/multihash/>).

- **Σύνδεση περιεχομένου μέσω κατευθυνόμενων άκυκλων γράφων (Directed Acyclic Graphs ή DAGs).** Το IPFS αξιοποιεί DAGs (και συγκεκριμένα Merkle DAGs), μίας δομής δεδομένων της οποίας κάθε κόμβος έχει ως μοναδικό αναγνωριστικό το hash του περιεχομένου του (το CID).



Σχήμα 2.8: Merkle DAG[16]

Στο παραπάνω Merkle DAG τα baf...i αποτελούν τα CID των αρχείων και των φακέλων. Το δένδρο δημιουργείται από κάτω προς τα πάνω, υπολογίζοντας κάθε φορά τα κατάλληλα hashes/CIDs. Σε περίπτωση που το περιεχόμενο ενός κόμβου αλλάξει, τότε αλλάζει τόσο το CID του, όσο και τα CIDs όλων των προγόνων του.

- **Ανακάλυψη περιεχομένου μέσω καταναμημένων πινάκων κατακερματισμού (Distributed Hash Tables ή DHTs).** Ο DHT είναι ένα καταναμημένο σύστημα για την αντιστοίχιση κλειδιών σε τιμές. Στο IPFS αποτελεί το θεμελιώδες συστατικό του συστήματος δρομολόγησης περιεχομένου και λειτουργεί ως διασταύρωση μεταξύ καταλόγου και συστήματος πλοήγησης. Πρακτικά πρόκειται για ένα πίνακα που αποθηκεύει ποιος έχει ποια δεδομένα και, μέσω του οποίου, ο χρήστης βρίσκει τον peer που έχει αποθηκευμένο το επιθυμητό περιεχόμενο.

Κάτι που θα πρέπει να σημειωθεί είναι πως, σαν προεπιλογή, οι IPFS κόμβοι αντιμετωπίζουν τα αποθηκευμένα δεδομένα ως προσωρινή μνήμη (cache), πράγμα που σημαίνει ότι δεν υπάρχει καμία εγγύηση ότι εκείνα θα συνεχίσουν να παραμένουν αποθηκευμένα σε αυτούς. Για την αποφυγή της διαγραφής τους από τον garbage collector, τα δεδομένα θα πρέπει να σημανθούν ως σημαντικά, μέσω του «καρφιτσώματος» (pinning). Έτσι, για την ομαλή λειτουργία π.χ. μίας DApp που βασίζεται στο IPFS, θα πρέπει το περιεχόμενό της να είναι pinned από αρκετούς peers και/ή να γίνεται χρήση κάποιου pinning service, ώστε να εξασφαλίζεται διαθεσιμότητά του.

Βασικό πλεονέκτημα του IPFS είναι ότι ο αποκεντρωτικός του χαρακτήρας δίνει τη δυνατότητα να παρέχεται το περιεχόμενο από πολλούς κόμβους, οι οποίοι βρίσκονται σε διαφορετικές τοποθεσίες και δεν υπάγονται σε κάποια συγκεκριμένη κεντρική αρχή. Με αυτόν τον τρόπο, τα δεδομένα είναι πιο ανθεκτικά τόσο από άποψη διαθεσιμότητας (αν ένας κόμβος αποσυνδεθεί, θα υπάρχει κάποιος άλλος), όσο και από άποψη αντοχής στη λογοκρισία. Μπορεί, επίσης, να

ανακτώνται γρηγορότερα, εφόσον τα διαθέτουν κάποιοι κοντινοί peers, πράγμα ιδιαίτερα πολύτιμο εάν για κοινότητες που είναι καλά δικτυωμένες τοπικά αλλά δεν έχουν καλή σύνδεση με το ευρύτερο διαδίκτυο.

Κεφάλαιο 3

Σχεδίαση εφαρμογής

3.1 Σύλληψη της ιδέας

Η σύλληψη της ιδέας για τη δημιουργία της εφαρμογής της παρούσας διπλωματικής εργασίας είχε ως εφαλτήριο την αναγνώριση ενός διδιάστατου προβλήματος.

Η πρώτη διάσταση εστιάζει στον χώρο των μέσων κοινωνικής δικτύωσης. Εκεί παρατηρείται αδιαμφισβήτη επικράτηση πλατφορμών επικοινωνίας συγκεντρωτικής μορφής (π.χ. Facebook, Twitter, Instagram), ενώ προσπάθειες δημιουργίας αντίστοιχων αποκεντρωτικών εφαρμογών βρίσκονται σε πρώιμα στάδια, τόσο ανάπτυξης, όσο και υιοθέτησης από το ευρύ κοινό. Όπως αναλύθηκε και στην ενότητα 1.3, η τρέχουσα αυτή κατάσταση θέτει αξιοσημείωτα προβλήματα τεχνικής φύσεως (έλλειψη ασφάλειας και διαθεσιμότητας) και, κυρίως, πολιτικής (έλλειψη εμπιστοσύνης, εγγύησης της αυθεντικότητας των δεδομένων και της ελευθερίας του λόγου).

Η δεύτερη διάσταση εστιάζει στον χώρο της ψηφιακής δημοκρατίας (digital democracy). Συγκεκριμένα, παρατηρείται έλλειψη εργαλείων, ικανών να παρέχουν τη δυνατότητα διενέργειας αυθεντικών δημοκρατικών διαδικασιών. Ψηφοφορίες και αυτοδιαχείριση εντός συστημάτων κεντροποιημένης λογικής αδυνατούν, για αρχιτεκτονικούς λόγους, να εξασφαλίσουν τις απαραίτητες θεμελιώδεις ιδιότητες τέτοιων διαδικασιών, δηλαδή της ανωνυμίας και της επαληθευσιμότητας.

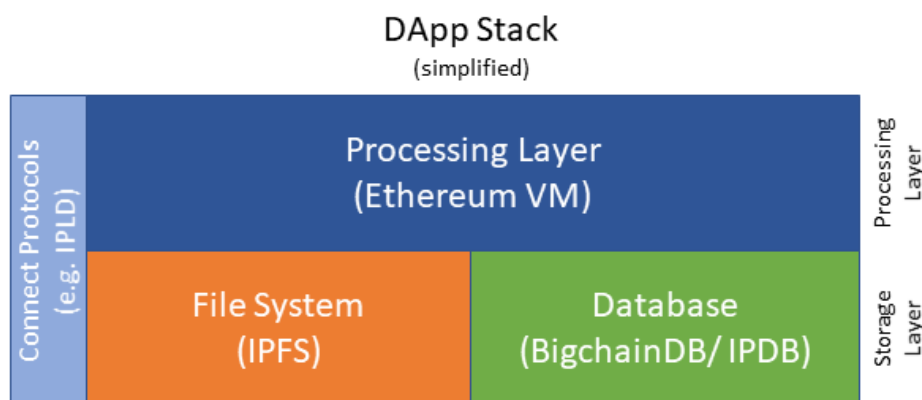
Βάσει των παραπάνω, γεννήθηκε η ιδέα δημιουργίας μίας εφαρμογής, η οποία, μέσω ενός προτεινόμενου συνδυασμού αποκεντρωτικών τεχνολογιών, να ορίσει έναν ψηφιακό χώρο που θα έρθει αντιμέτωπος με τα παραπάνω. Έτσι, κεντρικός στόχος της πιλοτικής εφαρμογής Concordia, είναι να αποτελέσει μία αυτόνομη κοινωνική πλατφόρμα, που θα κατοχυρώνει στους χρήστες της ελευθερία του λόγου και πλήρη κυριότητα επί των δεδομένων τους. Επιπλέον, θα παρέχει τη δυνατότητα διενέργειας αυθεντικών, ανώνυμων ψηφοφοριών, κάτι που θα την καθιστά ένα αξιόπιστο δημοκρατικό βήμα για τη λήψη αποφάσεων εντός αυτοδιαχειριζόμενων κοινοτήτων της.

3.2 Τεχνολογική στοίβα

Ξεκινώντας τη σχεδίαση της πλατφόρμας, πραγματοποιήθηκε έρευνα για την επιλογή της τεχνολογικής της στοίβας (technology stack). Αυτή αποφασίστηκε να ακολουθήσει μία προσαρμοσμένη για τα δεδομένα μορφή τριμερούς διάταξης⁸ και να χωριστεί σε τρία λογικά επίπεδα (tiers):

- α) **Presentation tier:** Αποτελεί τη διεπαφή του χρήστη (user interface ή UI), μέσω της οποίας ο τελευταίος αλληλεπιδρά με την εφαρμογή. Για την εκπλήρωση των προδιαγραφών, το μοναδικό απαραίτητο χαρακτηριστικό αυτού του τμήματος είναι να μπορεί να εκτελείται αυτούσιο από τη συσκευή του τελικού χρήστη, δηλαδή να μην απαιτείται η ύπαρξη κάποιου εξυπηρετητή για τη λειτουργία του. Λαμβάνοντας, επιπροσθέτως, υπόψιν τις ανάγκες και τους περιορισμούς των λογισμικών των άλλων δύο επιπέδων, το παρόν κομμάτι αποφασίστηκε να σχεδιαστεί ως μία client-side web application σε HTML/CSS/JS.
- β) **Application tier:** Πρόκειται για το επίπεδο που πραγματοποιεί την επεξεργασία (processing) της εφαρμογής. Εδώ επιλέχθηκαν το blockchain και τα smart contracts, καθώς τα θετικά τους χαρακτηριστικά, όπως αυτά περιγράφηκαν στο κεφάλαιο 2, ταίριαζαν απόλυτα με τις ιδιαίτερες απαιτήσεις της εφαρμογής. Συγκεκριμένα, επιλέχθηκε η πλατφόρμα του Ethereum, καθώς αποτελεί τον πρωτοπόρο στο χώρο, με λειτουργικές εφαρμογές και την ισχυρότερη κοινότητα.
- γ) **Data tier:** Το τμήμα αυτό είναι υπεύθυνο για την αποθήκευση των δεδομένων (storage). Για την επίτευξη πλήρους αρχιτεκτονικής αποκέντρωσης των δεδομένων επιλέχθηκε το IPFS (ενότητα 2.7), το οποίο διανέμει το περιεχόμενο της εφαρμογής στους peers που συμμετέχουν σε αυτήν.

Τελικά, με τη διασύνδεση των προαναφερθέντων τεχνολογιών, προκύπτει σχηματικά η ακόλουθη διάταξη:



Σχήμα 3.1: Τεχνολογική στοίβα

⁸Η τριμερής διάταξη (three-tier architecture) διαχωρίζει μία εφαρμογή σε τρία ανεξάρτητα λειτουργικά επίπεδα και αποτελεί την κυρίαρχη επιλογή για διατάξεις παραδοσιακών εφαρμογών πελάτη-εξυπηρετητή.

3.3 Μεθολογία σχεδίασης

3.4 Κατηγορίες χρηστών

Οι χρήστες (actors) της πλατφόρμας χωρίζονται σε πρωτεύοντες ή ενεργούς και δευτερεύοντες ή παθητικούς. Πρωτεύοντες χρήστες είναι εκείνοι που εκκινούν διεργασίες στο σύστημα. Δευτερεύοντες είναι οι χρήστες με τους οποίους αλληλεπιδρά το σύστημα, αλλά οι ίδιοι δεν εκκινούν διεργασίες σε αυτό. Συνολικά οι χρήστες που συμμετέχουν στο σύστημα είναι οι:

- Επισκέπτες
- Εγγεγραμμένα μέλη
- Δημιουργοί κοινοτήτων
- Συμβόλαια κοινοτήτων

3.4.1 Ενεργοί χρήστες

Οι ενεργοί χρήστες στο σύστημα είναι οι επισκέπτες, τα εγγεγραμμένα μέλη και οι δημιουργοί κοινοτήτων.

Όλοι οι χρήστες στο σύστημα είναι αρχικά επισκέπτες. Οι επισκέπτες έχουν τη δυνατότητα να βλέπουν το περιεχόμενο της κοινότητας, αλλά δε μπορούν να συμμετέχουν δημιουργώντας νέο περιεχόμενο (δημοσιεύοντας νέα θέματα ή μηνύματα). Επίσης, δε μπορούν να συμμετέχουν στις ψηφοφορίες της κοινότητας ή να ψηφίσουν τα μηνύματα.

Όταν ένας επισκέπτης εγγράφεται στο σύστημα, αποκτά έναν μοναδικό, αύξοντα αριθμό χρήστη και αποτελεί πλέον εγγεγραμμένο μέλος της κοινότητας. Τα εγγεγραμμένα μέλη έχουν τα δικαιώματα των επισκεπτών και μπορούν επιπλέον να προσθέσουν περιεχόμενο στην πλατφόρμα μέσω της δημιουργίας νέων θεμάτων, της δημοσίευσης μηνυμάτων και της ψήφισης στις ψηφοφορίες στις οποίες έχουν δικαίωμα.

Οι δημιουργοί κοινοτήτων είναι οι χρήστες οι οποίοι χρησιμοποιούν την δυνατότητα του συστήματος να δημιουργήσει κοινότητες, τα μέλη των οποίων διαφοροποιούνται βάσει ενός εξωτερικού token. Το token που ορίζει τα μέλη μίας κοινότητας προέρχεται από ένα έξυπνο συμβόλαιο το οποίο ορίζεται κατά τη δημιουργία της κοινότητας. Οι δημιουργοί κοινοτήτων πρέπει να είναι εγγεγραμμένα μέλη της κοινότητας. Ένας δημιουργός κοινότητας δεν έχει παραπάνω δικαιώματα από αυτά των απλών εγγεγραμμένων χρηστών.

3.4.2 Παθητικοί χρήστες

Παθητικοί χρήστες τους συστήματος είναι τα συμβόλαια των κοινοτήτων. Τα συμβόλαια αυτά δεν εκκινούν διεργασίες στο σύστημα και δεν αλληλεπιδρούν με αυτό άμεσα. Αποτελούν αυτόνομες εξωτερικές οντότητες, οι οποίες ορίζουν τους χρήστες κοινοτήτων μέσω της διάθεσης αναγνωριστικών token στα μέλη τους. Συγκεκριμένα, μέσω του διαμοιρασμού των token, καθορίζουν ποιοι χρήστες της πλατφόρμας έχουν δικαίωμα ψήφου στις ψηφοφορίες που αφορούν την κοινότητα.

3.4.3 Σύνοψη χρηστών

Συμπερασματικά προκύπτουν τρεις διακριτές κατηγορίες ενεργών χρηστών με ξεχωριστά δικαιώματα όπως φαίνεται στο παρακάτω σχήμα:

Κατηγορία χρήστη	Δικαιώματα								
	Προβολή θεμάτων	Προβολή μηνυμάτων	Προβολή ψηφοφοριών	Προβολή ψήφων μηνυμάτων	Δημιουργία θεμάτων	Δημιουργία μηνυμάτων	Δημιουργία ψηφοφοριών	Ψήφιση σε ψηφοφορίες	Ψήφιση μηνυμάτων
Επισκέπτες	✓	✓	✓	✓	✗	✗	✗	✗	✗
Εγγεγραμμένα μέλη	✓	✓	✓	✓	✓	✓	✓*	✓*	✓
Δημιουργοί κοινοτήτων	✓	✓	✓	✓	✓	✓	✓*	✓*	✓

* Μόνο στις υποκοινότητες στις οποίες κατέχει το αντίστοιχο token και σε αυτές οι οποίες δεν έχουν ορισμένο token.

Πίνακας 3.1: Δικαιώματα χρήσης ανά κατηγορία χρήστη

3.5 Απαιτήσεις λογισμικού

Στην παρούσα ενότητα περιγράφονται οι βασικές απαιτήσεις λογισμικού (software requirements) της εφαρμογής.

Η πρώτη κατηγορία είναι αυτή των Λειτουργικών Απαιτήσεων (ΛΑ), η οποία αναφέρεται στη συμπεριφορά του συστήματος, δηλαδή στον τρόπο που θα αντιδρά και στις εξόδους που θα παράγει ανάλογα με τις εισόδους.

<ΛΑ-1> Ο χρήστης πρέπει να μπορεί να εγγραφεί στην εφαρμογή με τον Ethereum λογαριασμό του.

Περιγραφή: Ο χρήστης πρέπει να μπορεί να εγγραφεί στην εφαρμογή, πατώντας το κουμπί «Sign Up» και συμπληρώνοντας τα απαραίτητα πεδία σύμφωνα με τις οδηγίες. Το πεδίο «Username» είναι υποχρεωτικό να συμπληρωθεί και ορίζεται με μοναδικό τρόπο. Σε περίπτωση που ο χρήστης εισάγει μη διαθέσιμο Username, το σύστημα θα πρέπει να μην επιτρέπει στον χρήστη να συνεχίσει και να προβάλει αντίστοιχο μήνυμα λάθους. Τα πεδία «Profile picture URL» και «Location» είναι προαιρετικά.

User Priority (5/5): Η απαίτηση είναι ύψιστης προτεραιότητας για τους επισκέπτες καθώς μόνο μέσω της εγγραφής μπορούν να χρησιμοποιήσουν τα υπόλοιπα χαρακτηριστικά της εφαρμογής.

Technical Priority (5/5): Η απαίτηση αυτή είναι ύψιστης σημασίας για το σύστημα επειδή επηρεάζει τη λειτουργικότητά του.

<ΛΑ-2> Ο χρήστης πρέπει να συνδέεται αυτόματα, εφόσον είναι εγγεγραμμένος.

Περιγραφή: Το σύστημα πρέπει να διαπιστώνει αυτόματα εάν το τρέχον Ethereum address έχει λογαριασμό στην εφαρμογή και εάν ναι, να συνδέει να τον χρήστη, ανακτώντας το Username του από το blockchain και προβάλλοντας το στο μενού.

User Priority (5/5): Η απαίτηση είναι ύψιστης προτεραιότητας για τους επισκέπτες καθώς μέσω της σύνδεσης ενεργοποιούνται τα χαρακτηριστικά της δημιουργίας θεμάτων και δημοσίευσης μηνυμάτων.

Technical Priority (1/5): Η σύνδεση αφορά μόνο τη γραφική διεπαφή του χρήστη με την πλατφόρμα και δεν αποτελεί στοιχείο που επιδρά στο υπόλοιπο σύστημα.

<ΛΑ-3> Το σύστημα πρέπει να δημιουργεί τις βάσεις δεδομένων του χρήστη.

Περιγραφή: Το σύστημα πρέπει να δημιουργεί τις βάσεις δεδομένων του χρήστη, εάν αυτές δεν υπάρχουν ήδη τοπικά. Όταν ο χρήστης ξεκλειδώσει τον Ethereum λογαριασμό του, το σύστημα θα πρέπει να τον προτρέπει να υπογράψει με το ιδιωτικό του κλειδί μία συναλλαγή που θα εξασφαλίζει τη γνησιότητα των βάσεων του και των δεδομένων που αυτές θα εμπεριέχουν.

User Priority (5/5): Η απαίτηση αυτή είναι υψηλής σημασίας για τον χρήστη καθώς η δημιουργία των βάσεων είναι απαραίτητη για την διατήρηση των δεδομένων που δημοσιοποιεί.

Technical Priority (5/5): Η απαίτηση αυτή είναι υψηλής σημασίας για το σύστημα για τους ίδιους λόγους.

<ΛΑ-4> Ο εγγεγραμμένος χρήστης πρέπει να μπορεί να δημιουργεί θέματα (topics).

Περιγραφή: Ο εγγεγραμμένος χρήστης πρέπει να μπορεί να δημιουργεί νέα θέματα. Αυτό το επιτυγχάνει πατώντας το κουμπί «New Topic», συμπληρώνοντας τα υποχρεωτικά πεδία της φόρμας («Topic subject» και «First post content»), πατώντας το κουμπί «Create Topic» και επιβεβαιώνοντας τη συναλλαγή στο Ethereum.

User Priority (5/5): Η απαίτηση αυτή είναι υψηλής σημασίας καθώς επιτελεί έναν από τους βασικούς στόχους της πλατφόρμας.

Technical Priority (5/5): Η απαίτηση αυτή είναι υψηλής σημασίας για τον ίδιο λόγο.

<ΛΑ-5> Ο χρήστης πρέπει να μπορεί να περιηγείται σε θέματα.

Περιγραφή: Το σύστημα πρέπει να μπορεί να προβάλλει τα θέματα που έχουν δημιουργηθεί στην αρχική οθόνη. Ο χρήστης πρέπει να μπορεί να περιηγείται σε αυτά πατώντας πάνω τους και, έπειτα, χρησιμοποιώντας τα βέλη, να περιηγηθεί στο ιστορικό των μηνυμάτων του θέματος.

User Priority (5/5): Η απαίτηση αυτή είναι υψηλής σημασίας επειδή επιτρέπει στους επισκέπτες να έχουν πρόσβαση στο υλικό που είναι δημοσιευμένο στην πλατφόρμα.

Technical Priority (5/5): Η απαίτηση αυτή είναι υψηλής σημασίας επειδή αποτελεί βασικό χαρακτηριστικό της πλατφόρμας για την χρηστικότητά της.

<ΛΑ-6> Ο εγγεγραμμένος χρήστης πρέπει να μπορεί να δημιουργεί μηνύματα (posts).

Περιγραφή: Ο εγγεγραμμένος χρήστης πρέπει να μπορεί να δημιουργεί μηνύματα στο θέμα που επιθυμεί. Αυτό επιτυγχάνεται συμπληρώνοντας το πεδίο νέου μηνύματος στην οθόνη του θέματος, πατώντας το κουμπί «Post» και επιβεβαιώνοντας τη συναλλαγή στο Ethereum.

User Priority (5/5): Η απαίτηση αυτή είναι ύψιστης σημασίας για τους χρήστες επειδή αποτελεί ένα από τα βασικότερα χαρακτηριστικά της πλατφόρμας.

Technical Priority (5/5): Η απαίτηση αυτή είναι υψίστης σημασίας για το σύστημα καθώς αποτελεί θεμελιώδες κομμάτι για την επίτευξη του βασικότερου στόχου της, αυτού της δημιουργίας διαλόγου.

<ΛΑ-7> Ο χρήστης πρέπει να μπορεί να τροποποιεί τα μηνύματά του.

Περιγραφή: Ο χρήστης πρέπει να μπορεί να τροποποιεί τα μηνύματά του. Αυτό το επιτυγχάνει πατώντας το κουμπί επεξεργασίας στο εκάστοτε μήνυμα, τροποποιώντας το μήνυμα και πατώντας το κουμπί επιβεβαίωσης. Στη συνέχεια, το σύστημα τροποποιεί το περιεχόμενο του μηνύματος στη βάση δεδομένων του χρήστη ανάλογα. Σε περίπτωση που ο χρήστης αλλάξει γνώμη κατά τη διάρκεια της διαδικασίας της επεξεργασίας, μπορεί να πατήσει το κουμπί ακύρωσης και να αναιρέσει τις αλλαγές που πραγματοποίησε.

User Priority (4/5): Η απαίτηση αυτή αποτελεί σημαντικό χαρακτηριστικό που απευθύνεται κυρίως στην χρηστικότητα της πλατφόρμας.

Technical Priority (3/5): Η απαίτηση αυτή είναι μέτριας σημαντικότητας για το σύστημα επειδή αυτό θα μπορούσε να είναι λειτουργικό χωρίς το χαρακτηριστικό της επεξεργασίας μηνυμάτων.

<ΛΑ-8> Ο εγγεγραμμένος χρήστης πρέπει να μπορεί να ψηφίζει σε μηνύματα άλλων χρηστών.

Περιγραφή: Ο εγγεγραμμένος χρήστης πρέπει να μπορεί να υπερψηφίζει ή να καταψηφίζει μηνύματα άλλων χρηστών. Αυτό το επιτυγχάνει πατώντας τα παρακείμενα κουμπιά «+» ή «-» αντίστοιχα και επιβεβαιώνοντας τη συναλλαγή στο Ethereum (οι ψήφοι αποθηκεύονται εκεί). Η διαδικασία ισχύει και για την τροποποίηση ή την αφαίρεση μίας ψήφου από τον χρήστη.

User Priority (3/5): Η απαίτηση αυτή είναι μέτριας σημασίας για τους χρήστες καθώς αποτελεί ένα χρήσιμο αλλά όχι απαραίτητο χαρακτηριστικό.

Technical Priority (4/5): Η απαίτηση αυτή είναι μεγάλης σημασίας για το σύστημα επειδή δημιουργεί δεδομένα τα οποία είναι χρήσιμα για τον υπολογισμό της εμπιστοσύνης των χρηστών.

<ΛΑ-9> Ο εγγεγραμμένος χρήστης πρέπει να μπορεί να δημιουργεί ψηφοφορίες (polls).

Περιγραφή: Ο εγγεγραμμένος χρήστης πρέπει να μπορεί να δημιουργεί ψηφοφορίες. Αυτό το επιτυγχάνει πατώντας «Add Poll» στην οθόνη δημιουργία θέματος και συμπληρώνοντας τα απαραίτητα πεδία.

User Priority (5/5): Η απαίτηση αυτή είναι ύψιστης σημασίας για τους χρήστες καθώς οι αμεσοδημοκρατικές διαδικασίες αποτελούν μία από τις κυριότερες χρήσεις της πλατφόρμας

Technical Priority (5/5): Η απαίτηση αυτή είναι μεγάλης σημασίας για το σύστημα επειδή αποτελεί βασική προδιαγραφή του.

<ΛΑ-10> Ο εγγεγραμμένος χρήστης πρέπει να μπορεί να ψηφίζει σε ψηφοφορίες.

Περιγραφή: Ο εγγεγραμμένος χρήστης πρέπει να μπορεί να ψηφίζει σε ψηφοφορίες, σύμφωνα με τους εκάστοτε κανόνες.

User Priority (5/5): Η απαίτηση αυτή είναι ύψιστης σημασίας για τους χρήστες καθώς αποτελεί μία από τις -- insert same as above

Technical Priority (5/5): Η απαίτηση αυτή είναι υψηλής σημασίας για το σύστημα καθώς αποτελεί σημαντικό χαρακτηριστικό του.

<ΛΑ-11> Ο χρήστης πρέπει να μπορεί να διαγράφει τα τοπικά δεδομένα.

Περιγραφή: Ο χρήστης πρέπει να μπορεί να διαγράφει τα τοπικά δεδομένα. Αυτό το επιτυγχάνει πατώντας στο κουμπί «Clear databases» του μενού και επιβεβαιώνοντας τη διαγραφή μέσω ενός pop-up διαλόγου.

User Priority (2/5): Η απαίτηση αυτή είναι χαμηλής σημασία για τους χρήστες, διότι αποτελεί απλά μία διευκόλυνση για τη διαγραφή των δεδομένων που έχουν αποθηκεύσει τοπικά.

Technical Priority (3/5): Η απαίτηση αυτή είναι μέτριας σημασίας για το σύστημα καθώς συνάδει με την φιλοσοφία της πλατφόρμας σχετικά με την κυριότητα των δεδομένων από τους χρήστες.

<ΛΑ-12> Ο χρήστης πρέπει να μπορεί να δημιουργεί κοινότητες.

Περιγραφή: Ο χρήστης πρέπει να μπορεί να δημιουργεί κοινότητες, μέσω κουμπιού της αρχικής οθόνης.

User Priority (4/5): Η απαίτηση αυτή είναι μεγάλης σημασίας για τους χρήστες καθώς παρέχει την ευελιξία της δημιουργίας κοινοτήτων.

Technical Priority (4/5): Η απαίτηση αυτή είναι μεγάλης σημασίας για την πλατφόρμα επειδή θα γενικεύσει τη χρήση της σε περισσότερες κοινότητες προσελκύοντας μεγαλύτερο αριθμό χρηστών.

<ΛΑ-13> Κατά τη δημιουργία κοινότητας, ο χρήστης πρέπει να έχει τη δυνατότητα να ορίσει ένα contract που θα παρέχει προσαρμοσμένα tokens για αυτήν.

Περιγραφή: Κατά τη δημιουργία κοινότητας, ο χρήστης πρέπει να έχει τη δυνατότητα να ορίσει ένα contract που θα παρέχει προσαρμοσμένα tokens για αυτήν. Τα tokens αυτά θα διαμοιράζονται με τον τρόπο που επιθυμεί η κοινότητα και θα είναι εκείνα τα οποία θα καθορίζουν τους έγκυρους ψηφοφόρους της.

User Priority (4/5): Η απαίτηση αυτή είναι μεγάλης σημασίας καθώς παρέχει στις κοινότητες τη δυνατότητα διενέργειας ανώνυμων ψηφοφοριών.

Technical Priority (4/5): Η απαίτηση αυτή είναι μεγάλης σημασίας για το σύστημα διότι θα παρέχει στις κοινότητες την απαιτούμενη αυτονομία στον ορισμό των διαδικασιών της κοινότητας.

Η δεύτερη κατηγορία είναι αυτή των Μη Λειτουργικών Απαιτήσεων (ΜΛΑ). Περιλαμβάνει απαιτήσεις αρχιτεκτονικής σημασίας, οι οποίες καθορίζουν κριτήρια ή περιορισμούς του τρόπου λειτουργίας του συστήματος και σχετίζονται με χαρακτηριστικά όπως η αποδοτικότητα, η αξιοπιστία και η ευχρηστία του.

<ΜΛΑ-1> Η πλατφόρμα πρέπει να είναι κατά το δυνατόν αρχιτεκτονικά αποκεντρωμένη.

Περιγραφή: Οι τεχνολογίες στις οποίες βασίζεται η πλατφόρμα πρέπει ιδανικά να μη δημιουργούν κεντρικά σημεία. Επιπλέον, ο κώδικας και η δημόσια διάθεση του πρέπει να γίνονται με αποκεντρωμένο τρόπο.

User Priority (5/5): Η αρχιτεκτονική αποκέντρωση της πλατφόρμας αποτελεί απαίτηση υψηλής σημασίας για τον χρήστη, καθώς διασφαλίζει την ελευθερία του λόγου του κτλ –κεφ 1.2

Technical Priority (5/5): Η αρχιτεκτονική αποκέντρωση της πλατφόρμας αποτελεί απαίτηση υψηλής σημασίας για το σύστημα, καθώς το καθιστά ασφαλές σε επιθέσεις κτλ –κεφ 1.2

<ΜΛΑ-2> Τα fees για τη χρήση του Ethereum blockchain πρέπει να ελαχιστοποιούνται.

Περιγραφή: Τα fees που πρέπει να καταβάλλονται για τη χρήση του Ethereum blockchain εξαρτώνται άμεσα τόσο από τον όγκο των δεδομένων προς αποθήκευση, όσο και από τους κύκλους επεξεργασίας των smart contracts της εφαρμογής. Ως προς τα δεδομένα, οι προγραμματιστές θα πρέπει να μεριμνούν ώστε ο κύριος όγκος τους να αποθηκεύεται επί του IPFS, ενώ επί του blockchain να αποθηκεύονται μόνο όσα πραγματικά χρειάζονται. Ως προς την απαιτούμενη επεξεργαστική ισχύ, πρέπει να βελτιστοποιείται ο κώδικας των smart contracts, έτσι ώστε οι διάφορες λειτουργίες τους να εκτελούνται με τους λιγότερους δυνατούς επεξεργαστικούς κύκλους.

User Priority (4/5): Η απαίτηση αυτή είναι μεγάλης σημασίας για τους χρήστες καθώς και δεν είναι απαραίτητη για τη χρήση της αλλά είναι ιδιαίτερα σημαντική για την ένταξη χρηστών με χαμηλότερες οικονομικές δυνατότητες.

Technical Priority (5/5): Η απαίτηση αυτή είναι μεγάλης σημασίας για το σύστημα διότι αποτελεί σημαντικό παράγοντα που επιδρά στην προσέλκυση και διατήρηση ενεργών χρηστών.

<ΜΛΑ-3> Τα contracts της εφαρμογής πρέπει να είναι αναβαθμισμα.

Περιγραφή: Τα contracts της εφαρμογής πρέπει μπορούν να αναβαθμιστούν, έτσι ώστε να μπορούν να προστίθενται λειτουργίες και να διορθώνονται σφάλματα. Η αναβαθμισσιμότητά τους θα πρέπει να επιτυγχάνεται με μεθόδους που να μην υπονομεύουν τη λειτουργικότητα των προηγούμενων εκδόσεων.

User Priority (2/5): Η απαίτηση αυτή είναι χαμηλής σημασίας για τους χρήστες καθώς αφορά την ανάπτυξη και όχι τη χρήση της.

Technical Priority (5/5): Η απαίτηση αυτή είναι υψηλής σημασίας για το σύστημα επειδή προσφέρει τη δυνατότητα εξέλιξης και υλοποίησης νέων χαρακτηριστικών.

3.6 Σενάρια χρήσης

Βασικό μέρος της σχεδίασης της πλατφόρμας ήταν η καταγραφή των απαιτήσεων η οποία έγινε στην προηγούμενη ενότητα (3.5) καθώς και η σχεδίαση και ανάπτυξη των σεναρίων χρήσης. Τα σενάρια χρήσης αντιστοιχίζουν πιθανές ενέργειες των χρηστών με αποκρίσεις του συστήματος. Μέσω της αντιστοίχισης αυτής παρουσιάζεται η λειτουργικότητα του συστήματος

και περιγράφονται τόσο οι λειτουργικές όσο και οι μη λειτουργικές απαιτήσεις του συστήματος.

Παρατίθενται εδώ τα σενάρια χρήσης που δίνουν τις απαραίτητες πληροφορίες για την κατανόηση της λειτουργίας του συστήματος.

3.6.1 Σενάριο χρήσης 1: Εγγραφή χρήστη

Το σενάριο χρήσης 1, <ΣΧ-1>, περιγράφει τις διαδοχικές ενέργειες που εκτελούνται για την εγγραφή ενός χρήστη στο σύστημα. Στους πίνακες 3.2 και 3.3 παρατίθενται οι βασικές πληροφορίες του <ΣΧ-1> και οι ενέργειες της βασικής ροής αντίστοιχα, ενώ στο σχήμα 3.2 φαίνεται το διάγραμμα της βασικής ροής.

Εγγράφομαι στο σύστημα	
Σύντομη περιγραφή	Στόχος του σεναρίου χρήσης είναι ο επισκέπτης να μπορεί να εγγραφεί στο σύστημα ως χρήστης.
Αναφορά ΛΑ	<ΛΑ-1>, <ΛΑ-3>
Αναφορά ΜΛΑ	<ΜΛΑ-2>
Πυροδότηση δραστηριότητας	Ο επισκέπτης πατάει το κουμπί εγγραφή.
Προϋπόθεση	Ο επισκέπτης πρέπει να έχει ανοίξει την σελίδα της εφαρμογής.

Πίνακας 3.2: Σενάριο χρήσης 1, εγγραφή χρήστη στο σύστημα.

Βασική ροή		
Γραμμή	Ενέργεια χρήστη συστήματος	Απάντηση Συστήματος
1	Ο χρήστης πατάει το κουμπί εγγραφή.	Το σύστημα εμφανίζει την φόρμα “Εγγραφή Χρήστη”.
2	Ο χρήστης συμπληρώνει τα πεδία και πατάει το κουμπί “Υποβολή”.	Το σύστημα εισάγει νέο χρήστη στο blockchain.
3	-	Το σύστημα δημιουργεί τις προσωπικές βάσεις βάσεις δεδομένων OrbitDb του χρήστη.
4	-	Το σύστημα εμφανίζει την φόρμα “Πληροφορίες Χρήστη”.
5	Ο χρήστης συμπληρώνει τις προσωπικές του πληροφορίες και πατάει το κουμπί “Υποβολή”.	Το σύστημα εισάγει τις πληροφορίες χρήστη στην προσωπική του βάση OrbitDb.
Μετάπειτα κατάσταση:	Το σύστημα μεταβαίνει στην αρχική σελίδα της εφαρμογής.	

Πίνακας 3.3: Σενάριο χρήσης 1 - Βασική ροή



Σχήμα 3.2: Σενάριο χρήσης 1 - Διάγραμμα βασικής ροής

Το <ΣΧ-1> περιέχει επίσης τρεις εναλλακτικές ροές που μπορεί να προκύψουν βάσει των επιλογών του χρήστη και οι οποίες περιγράφονται στους πίνακες 3.4, 3.5 και 3.6.

Εναλλακτική ροή 1: Τα στοιχεία χρήστη είναι λανθασμένα.

Εφόσον ο χρήστης στη γραμμή 2 δεν συμπληρώσει το πεδίο ονόματος χρήστη ή συμπληρώσει ένα όνομα χρήστη το οποίο είναι ήδη σε χρήση στο σύστημα, το σύστημα πρέπει να επιστρέψει σχετικό μήνυμα σφάλματος.

Γραμμή	Ενέργεια χρήστη συστήματος	Απάντηση Συστήματος
1	-	Το σύστημα εμφανίζει μήνυμα σφάλματος.

Το σύστημα επιστρέφει στη γραμμή 1 της βασικής ροής.

Πίνακας 3.4: Σενάριο χρήσης 1 - Εναλλακτική ροή 1

Εναλλακτική ροή 2: Ο χρήστης πατάει το κουμπί “Άκυρο”.

Εφόσον ο χρήστης στη γραμμή 2 της Βασικής Ροής επιλέξει “Άκυρο” το σύστημα επιστρέφει στην αρχική σελίδα της εφαρμογής.

Γραμμή	Ενέργεια χρήστη συστήματος	Απάντηση Συστήματος
1	Ο χρήστης πατάει το κουμπί “Άκυρο”	Το σύστημα επιστρέφει στην αρχική σελίδα της εφαρμογής.

Το σενάριο χρήσης τερματίζεται.

Πίνακας 3.5: Σενάριο χρήσης 1 - Εναλλακτική ροή 2

Εναλλακτική ροή 3: Ο χρήστης πατάει το κουμπί “Παράληψη”.

Εφόσον ο χρήστης στη γραμμή 5 της Βασικής Ροής επιλέξει “Παράληψη” το σύστημα επιστρέφει στην αρχική σελίδα της εφαρμογής.

Γραμμή	Ενέργεια χρήστη συστήματος	Απάντηση Συστήματος
1	Ο χρήστης πατάει το κουμπί “Παράληψη”	Το σύστημα επιστρέφει στην αρχική σελίδα της εφαρμογής.

Το σενάριο χρήσης τερματίζεται.

Πίνακας 3.6: Σενάριο χρήσης 1 - Εναλλακτική ροή 3

3.6.2 Σενάριο χρήσης 2: Σύνδεση χρήστη

Το σενάριο χρήσης 2, <ΣΧ-2>, περιγράφει τις διαδοχικές ενέργειες που εκτελούνται για την σύνδεση ενός χρήστη στο σύστημα. Στους πίνακες 3.7 και 3.8 παρατίθενται οι βασικές πληρο-

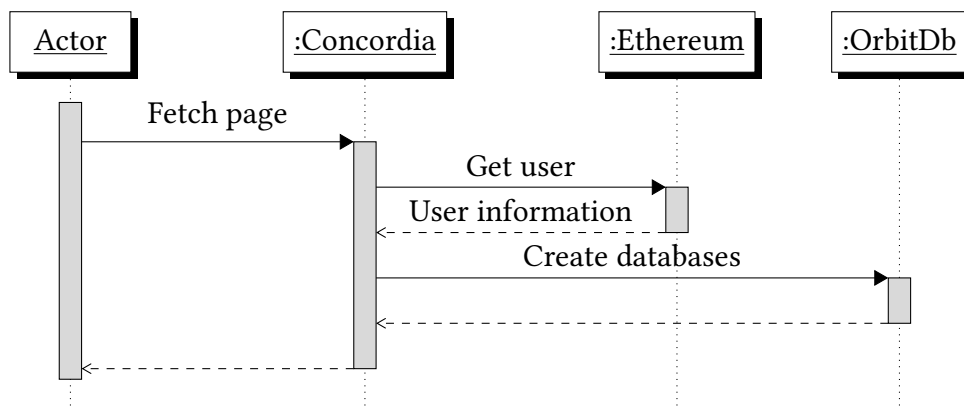
φορίες του <ΣΧ-2> και οι ενέργειες της βασικής ροής αντίστοιχα, ενώ στο σχήμα 3.3 φαίνεται το διάγραμμα της βασικής ροής.

Συνδέομαι στο σύστημα	
Σύντομη περιγραφή	Στόχος του σεναρίου χρήσης είναι ο χρήστης να συνδέεται αυτόματα στο σύστημα.
Αναφορά ΛΑ	<ΛΑ-2>
Αναφορά ΜΛΑ	-
Πυροδότηση δραστηριότητας	-
Προϋπόθεση	Ο χρήστης πρέπει να έχει ανοίξει την σελίδα της εφαρμογής.

Πίνακας 3.7: Σενάριο χρήσης 2, σύνδεση χρήστη στο σύστημα.

Βασική ροή		
Γραμμή	Ενέργεια χρήστη συστήματος	Απάντηση Συστήματος
1	-	Το σύστημα ανακτά τις πληροφορίες του χρήστη από το blockchain.
2	-	Το σύστημα δημιουργεί τις προσωπικές βάσεις δεδομένων OrbitDb του χρήστη.
Μετέπειτα κατάσταση:		Το σύστημα παραμένει στην αρχική σελίδα της εφαρμογής.

Πίνακας 3.8: Σενάριο χρήσης 2 - Βασική ροή



Σχήμα 3.3: Σενάριο χρήσης 2 - Διάγραμμα βασικής ροής

3.6.3 Σενάριο χρήσης 3: Δημιουργία νέου θέματος

Το σενάριο χρήσης 3, <ΣΧ-3>, περιγράφει τις διαδοχικές ενέργειες που εκτελούνται για την δημιουργία ενός θέματος. Στους πίνακες 3.9 και 3.10 παρατίθενται οι βασικές πληροφορίες του <ΣΧ-3> και οι ενέργειες της βασικής ροής αντίστοιχα, ενώ στο σχήμα 3.4 φαίνεται το διάγραμμα της βασικής ροής.

Δημιουργώ νέο θέμα	
Σύντομη περιγραφή	Στόχος του σεναρίου χρήσης είναι ο χρήστης να μπορεί να δημιουργήσει νέο θέμα.
Αναφορά ΛΑ	<ΛΑ-4>, <ΛΑ-9>
Αναφορά ΜΛΑ	<ΜΛΑ-2>
Πυροδότηση δραστηριότητας	Ο χρήστης πατάει το κουμπί δημιουργίας νέου θέματος.
Προϋπόθεση	Ο χρήστης να έχει συνδεθεί στην εφαρμογή και να βρίσκεται στην αρχική σελίδα.

Πίνακας 3.9: Σενάριο χρήσης 3, δημιουργία νέου θέματος.

Βασική ροή		
Γραμμή	Ενέργεια χρήστη συστήματος	Απάντηση Συστήματος
1	Ο χρήστης πατάει το κουμπί δημιουργίας νέου θέματος.	Το σύστημα εμφανίζει την φόρμα “Δημιουργία Θέματος”.
2	Ο χρήστης συμπληρώνει τα πεδία και πατάει το κουμπί “Υποβολή”.	Το σύστημα εισάγει νέο θέμα στο blockchain.
3	-	Το σύστημα εισάγει τις πληροφορίες του θέματος στην προσωπική βάση OrbitDb του χρήστη.
Μετέπειτα κατάσταση:	Το σύστημα μεταβαίνει στην σελίδα του νέου θέματος.	

Πίνακας 3.10: Σενάριο χρήσης 3 - Βασική ροή



Σχήμα 3.4: Σενάριο χρήσης 3 - Διάγραμμα βασικής ροής

Το <ΣΧ-3> περιέχει επίσης δύο εναλλακτικές ροές που μπορεί να προκύψουν βάσει των επιλογών του χρήστη και οι οποίες περιγράφονται στους πίνακες 3.11 και 3.12. Η εναλλακτική ροή 1 φαίνεται επίσης στο σχήμα 3.5 όπου παρουσιάζεται το διάγραμμα ροής της.

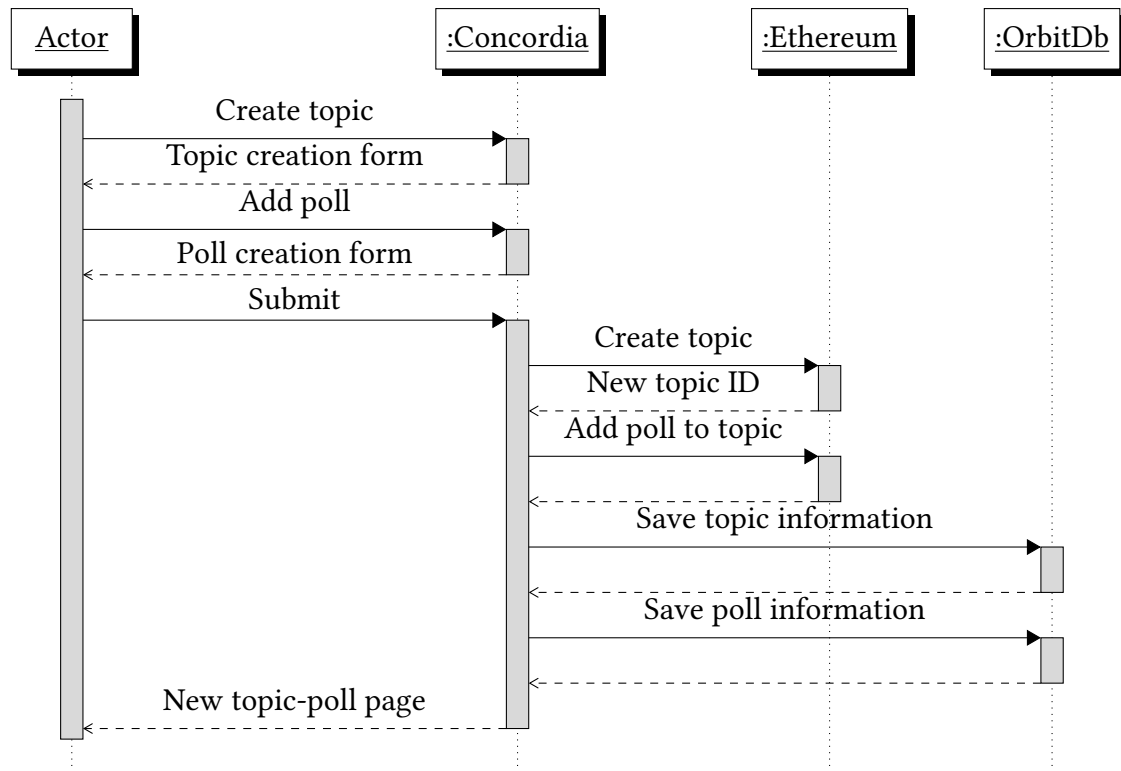
Εναλλακτική ροή 1: Ο χρήστης δημιουργεί ψηφοφορία.

Εφόσον ο χρήστης στη γραμμή 2 της Βασικής Ροής επιλέξει “Προσθήκη Ψηφοφορίας” το σύστημα ανανεώνει την σελίδα προσθέτοντας τα επιπλέον πεδία της φόρμας “Δημιουργία Ψηφοφορίας”.

Γραμμή	Ενέργεια χρήστη συστήματος	Απάντηση Συστήματος
1	Ο χρήστης, αφού συμπληρώσει τη φόρμα “Δημιουργία Θέματος”, πατάει το κουμπί “Προσθήκη ψηφοφορίας”	Το σύστημα ανανεώνει τη σελίδα με τα πεδία της φόρμας “Δημιουργία Ψηφοφορίας”.
2	Ο χρήστης συμπληρώνει τα πεδία και πατάει το κουμπί “Υποβολή”.	Το σύστημα εισάγει το νέο θέμα καθώς και τη νέα ψηφοφορία στο blockchain.
3	-	Το σύστημα εισάγει τις πληροφορίες του θέματος και της ψηφοφορίας στις προσωπικές βάσεις OrbitDb του χρήστη.

Το σύστημα μεταβαίνει στην σελίδα του νέου θέματος.

Πίνακας 3.11: Σενάριο χρήσης 3 - Εναλλακτική ροή 1



Σχήμα 3.5: Σενάριο χρήσης 3 - Διάγραμμα εναλλακτικής ροής 1

Εναλλακτική ροή 2: Ο χρήστης πατάει το κουμπί “Άκυρο”.

Εφόσον ο χρήστης στη γραμμή 2 της Βασικής Ροής ή στη γραμμή 2 της Εναλλακτικής Ροής 1 επιλέξει “Άκυρο” το σύστημα επιστρέφει στην αρχική σελίδα της εφαρμογής.

Γραμμή	Ενέργεια χρήστη συστήματος	Απάντηση Συστήματος
1	Ο χρήστης πατάει το κουμπί “Άκυρο”	Το σύστημα επιστρέφει στην αρχική σελίδα της εφαρμογής.

Το σενάριο χρήσης τερματίζεται.

Πίνακας 3.12: Σενάριο χρήσης 3 - Εναλλακτική ροή 2

3.6.4 Σενάριο χρήσης 4: Ανάκτηση θέματος

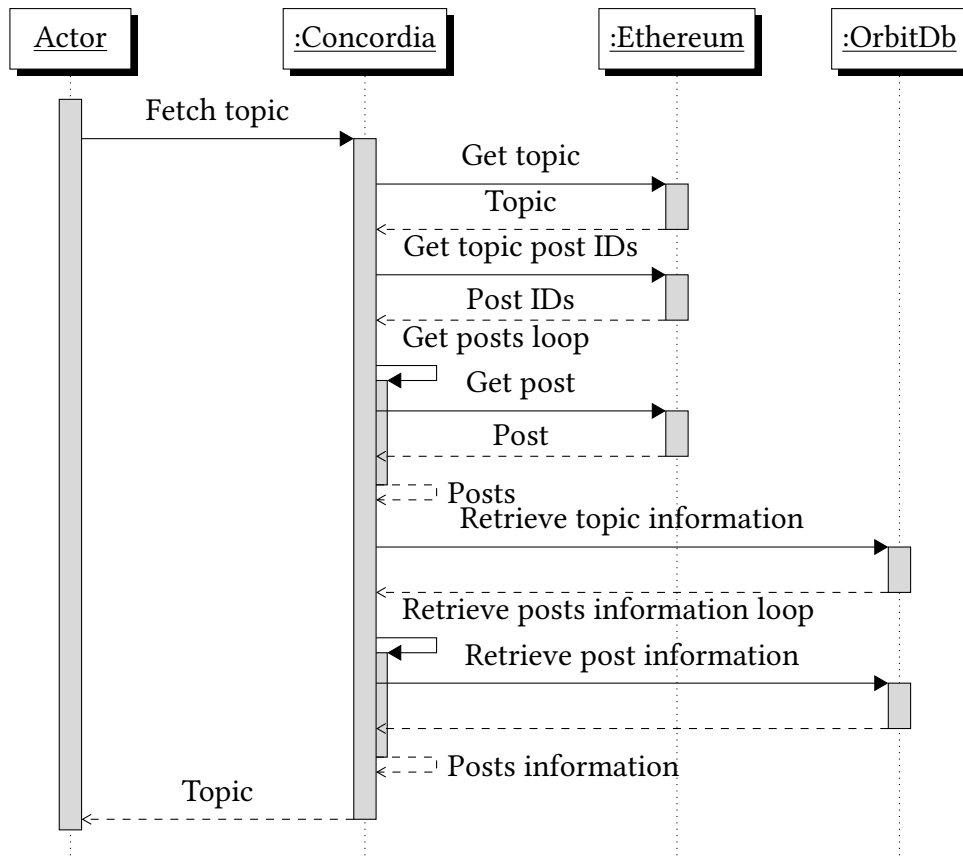
Το σενάριο χρήσης 4, <ΣΧ-4>, περιγράφει τις διαδοχικές ενέργειες που εκτελούνται για την ανάκτηση ενός θέματος. Στους πίνακες 3.13 και 3.14 παρατίθενται οι βασικές πληροφορίες του <ΣΧ-4> και οι ενέργειες της βασικής ροής αντίστοιχα, ενώ στο σχήμα 3.6 φαίνεται το διάγραμμα της βασικής ροής.

Ανακτώ ένα θέμα	
Σύντομη περιγραφή	Στόχος του σεναρίου χρήσης είναι ο επισκέπτης ή ο χρήστης να μπορεί να ανακτήσει ένα θέμα.
Αναφορά ΛΑ	<ΛΑ-5>
Αναφορά ΜΛΑ	-
Πυροδότηση δραστηριότητας	Ο επισκέπτης ή χρήστης πατάει σε ένα από τα θέματα.
Προϋπόθεση	Ο επισκέπτης ή χρήστης πρέπει να έχει ανοίξει την σελίδα της εφαρμογής.

Πίνακας 3.13: Σενάριο χρήσης 4, ανάκτηση θέματος.

Βασική ροή		
Γραμμή	Ενέργεια χρήστη συστήματος	Απάντηση Συστήματος
1	Ο χρήστης πατάει σε ένα από τα θέματα της λίστας.	Το σύστημα ανακτά τις πληροφορίες του θέματος από το blockchain.
2	-	Το σύστημα ανακτά τα μηνύματα του θέματος αντιγράφοντας τις προσωπικές βάσεις OrbitDb των συγγραφέων.
Μετέπειτα κατάσταση:	Το σύστημα μεταβαίνει στην σελίδα του θέματος.	

Πίνακας 3.14: Σενάριο χρήσης 4 - Βασική ροή



Σχήμα 3.6: Σενάριο χρήσης 4 - Διάγραμμα βασικής ροής

Το <ΣΧ-4> περιέχει επίσης μία εναλλακτική ροή που μπορεί να προκύψει βάσει των επιλογών του χρήστη και η οποία περιγράφεται στον πίνακα 3.15. Η εναλλακτική ροή 1 φαίνεται επίσης στο σχήμα 3.7 όπου παρουσιάζεται το διάγραμμα ροής της.

Εναλλακτική ροή 1: Το θέμα περιέχει ψηφοφορία.

Εφόσον το θέμα που ανακτήθηκε στη γραμμή 1 της Βασικής Ροής περιέχει ψηφοφορία ανακτώνται οι πληροφορίες της.

Γραμμή	Ενέργεια χρήστη συστήματος	Απάντηση Συστήματος
1	-	Το σύστημα ανακτά τα μηνύματα του θέματος αντιγράφοντας τις προσωπικές βάσεις OrbitDb των συγγραφέων.
2	-	Το σύστημα ανακτά την ψηφοφορία από το blockchain.
3	-	Το σύστημα ανακτά τις πληροφορίες της ψηφοφορίας αντιγράφοντας την προσωπική βάση OrbitDb του συγγραφέα.
4	-	Το σύστημα επιβεβαιώνει τις πληροφορίες της ψηφοφορίας με βάση το hash που έχει ανακτηθεί από το blockchain.

Το σενάριο χρήσης τερματίζεται.

Πίνακας 3.15: Σενάριο χρήσης 4 - Εναλλακτική ροή 1



Σχήμα 3.7: Σενάριο χρήσης 4 - Διάγραμμα εναλλακτικής ροής 1

3.6.5 Σενάριο χρήσης 5: Δημιουργία νέου μηνύματος

Το σενάριο χρήσης 5, <ΣΧ-5>, περιγράφει τις διαδοχικές ενέργειες που εκτελούνται για την δημιουργία ενός μηνύματος. Στους πίνακες 3.16 και 3.17 παρατίθενται οι βασικές πληροφορίες του <ΣΧ-5> και οι ενέργειες της βασικής ροής αντίστοιχα, ενώ στο σχήμα 3.8 φαίνεται το διάγραμμα της βασικής ροής.

Δημιουργώ νέο μήνυμα

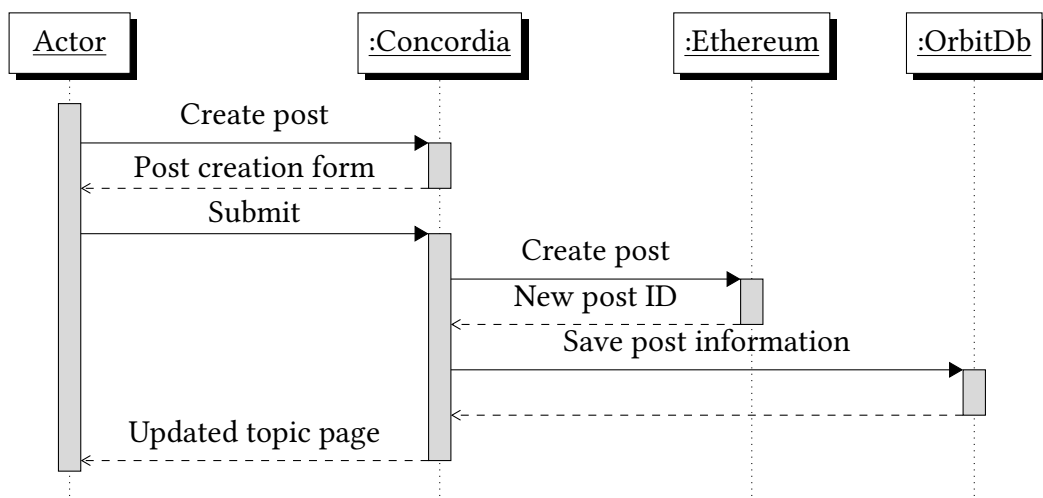
Σύντομη περιγραφή	Στόχος του σεναρίου χρήσης είναι ο χρήστης να μπορεί να δημιουργήσει νέο μήνυμα.
Αναφορά ΛΑ	<ΛΑ-6>
Αναφορά ΜΛΑ	<ΜΛΑ-2>
Πυροδότηση δραστηριότητας	Ο χρήστης πατάει το κουμπί δημιουργίας νέου μηνύματος.
Προϋπόθεση	Ο χρήστης να έχει συνδεθεί στην εφαρμογή και να βρίσκεται στην σελίδα ενός θέματος.

Πίνακας 3.16: Σενάριο χρήσης 5, δημιουργία νέου μηνύματος.

Βασική ροή

Γραμμή	Ενέργεια χρήστη συστήματος	Απάντηση Συστήματος
1	Ο χρήστης πατάει το κουμπί δημιουργίας νέου μηνύματος.	Το σύστημα εμφανίζει την φόρμα “Δημιουργία Μηνύματος”.
2	Ο χρήστης συμπληρώνει τα πεδία και πατάει το κουμπί “Υποβολή”.	Το σύστημα εισάγει νέο μήνυμα στο blockchain.
3	-	Το σύστημα εισάγει τις πληροφορίες του μηνύματος στην προσωπική βάση OrbitDb του χρήστη.
Μετέπειτα κατάσταση:	Το σύστημα παραμένει στη σελίδα του θέματος εμφανίζοντας το νέο μήνυμα.	

Πίνακας 3.17: Σενάριο χρήσης 5 - Βασική ροή



Σχήμα 3.8: Σενάριο χρήσης 5 - Διάγραμμα βασικής ροής

Το <ΣΧ-5> περιέχει επίσης μία εναλλακτική ροή που μπορεί να προκύψει βάσει των επιλογών του χρήστη και η οποία περιγράφεται στον πίνακα 3.18.

Εναλλακτική ροή 1: Ο χρήστης πατάει το κουμπί “Άκυρο”.		
Εφόσον ο χρήστης στη γραμμή 2 της Βασικής Ροής επιλέξει “Άκυρο” το σύστημα επιστρέφει στη σελίδα του θέματος.		
Γραμμή	Ενέργεια χρήστη συστήματος	Απάντηση Συστήματος
1	Ο χρήστης πατάει το κουμπί “Άκυρο”	Το σύστημα επιστρέφει στη σελίδα του θέματος.
Το σενάριο χρήσης τερματίζεται.		

Πίνακας 3.18: Σενάριο χρήσης 5 - Εναλλακτική ροή 1

3.6.6 Σενάριο χρήσης 6: Τροποποίηση μηνύματος

Το σενάριο χρήσης 6, <ΣΧ-6>, περιγράφει τις διαδοχικές ενέργειες που εκτελούνται για τη τροποποίηση ενός μηνύματος. Στους πίνακες 3.19 και 3.20 παρατίθενται οι βασικές πληροφορίες του <ΣΧ-6> και οι ενέργειες της βασικής ροής αντίστοιχα, ενώ στο σχήμα 3.9 φαίνεται το διάγραμμα της βασικής ροής.

Τροποποιώ ένα μήνυμα	
Σύντομη περιγραφή	Στόχος του σεναρίου χρήσης είναι ο χρήστης να μπορεί να τροποποιήσει τα μηνύματά του.
Αναφορά ΛΑ	<ΛΑ-7>
Αναφορά ΜΛΑ	-
Πυροδότηση δραστηριότητας	Ο χρήστης πατάει το κουμπί τροποποίησης του μηνύματος.
Προϋπόθεση	Ο χρήστης να έχει συνδεθεί στην εφαρμογή και να βρίσκεται στην σελίδα του θέματος που περιέχει το μήνυμά του.

Πίνακας 3.19: Σενάριο χρήσης 6, τροποποίηση μηνύματος.

Βασική ροή		
Γραμμή	Ενέργεια χρήστη συστήματος	Απάντηση Συστήματος
1	Ο χρήστης πατάει το κουμπί τροποποίησης του μηνύματος.	Το σύστημα εμφανίζει την φόρμα “Τροποποίηση Μηνύματος”.
2	Ο χρήστης συμπληρώνει τα πεδία και πατάει το κουμπί “Υποβολή”.	Το σύστημα τροποποιεί τις πληροφορίες του μηνύματος στην προσωπική βάση OrbitDb του χρήστη.
Μετέπειτα κατάσταση:	Το σύστημα παραμένει στη σελίδα του θέματος εμφανίζοντας το τροποποιημένο μήνυμα.	

Πίνακας 3.20: Σενάριο χρήσης 6 - Βασική ροή



Σχήμα 3.9: Σενάριο χρήσης 6 - Διάγραμμα βασικής ροής

Το <ΣΧ-6> περιέχει επίσης μία εναλλακτική ροή που μπορεί να προκύψει βάσει των επιλογών του χρήστη και η οποία περιγράφεται στον πίνακα 3.21.

Εναλλακτική ροή 1: Ο χρήστης πατάει το κουμπί “Άκυρο”.		
Εφόσον ο χρήστης στη γραμμή 2 της Βασικής Ροής επιλέξει “Άκυρο” το σύστημα επιστρέφει στη σελίδα του θέματος.		
Γραμμή	Ενέργεια χρήστη συστήματος	Απάντηση Συστήματος
1	Ο χρήστης πατάει το κουμπί “Άκυρο”	Το σύστημα επιστρέφει στη σελίδα του θέματος.
Το σενάριο χρήσης τερματίζεται.		

Πίνακας 3.21: Σενάριο χρήσης 6 - Εναλλακτική ροή 1

3.6.7 Σενάριο χρήσης 7: Ψήφιση σε ψηφοφορία

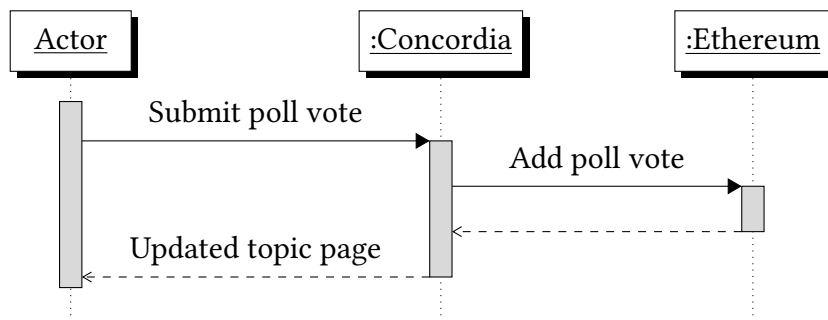
Το σενάριο χρήσης 7, <ΣΧ-7>, περιγράφει τις διαδοχικές ενέργειες που εκτελούνται για την ψήφιση σε μία ψηφοφορία. Στους πίνακες 3.22 και 3.23 παρατίθενται οι βασικές πληροφορίες του <ΣΧ-7> και οι ενέργειες της βασικής ροής αντίστοιχα, ενώ στο σχήμα 3.10 φαίνεται το διάγραμμα της βασικής ροής.

Ψηφίζω σε ψηφοφορία	
Σύντομη περιγραφή	Στόχος του σεναρίου χρήσης είναι ο χρήστης να μπορεί να ψηφίσει σε μία ψηφοφορία.
Αναφορά ΛΑ	<ΛΑ-10>
Αναφορά ΜΛΑ	<ΜΛΑ-2>
Πυροδότηση δραστηριότητας	Ο χρήστης πατάει το κουμπί ψηφοφορίας.
Προϋπόθεση	Ο χρήστης να έχει συνδεθεί στην εφαρμογή και να βρίσκεται στην σελίδα ενός θέματος το οποίο περιλαμβάνει ψηφοφορία.

Πίνακας 3.22: Σενάριο χρήσης 7, ψήφιση σε ψηφοφορία.

Βασική ροή		
Γραμμή	Ενέργεια χρήστη συστήματος	Απάντηση Συστήματος
1	Ο χρήστης πατάει το κουμπί της επιλογής που επιθυμεί να ψηφίσει και πατάει το κουμπί “Υποβολή”.	Το σύστημα εισάγει νέα ψήφο στο blockchain.
Μετέπειτα κατάσταση:	Το σύστημα ανανεώνει τις πληροφορίες της ψηφοφορίας.	

Πίνακας 3.23: Σενάριο χρήσης 7 - Βασική ροή



Σχήμα 3.10: Σενάριο χρήσης 7 - Διάγραμμα βασικής ροής

3.6.8 Σενάριο χρήσης 8: Ψήφιση μηνύματος

Το σενάριο χρήσης 8, <ΣΧ-8>, περιγράφει τις διαδοχικές ενέργειες που εκτελούνται για την ψήφιση σε ένα μήνυμα. Στους πίνακες 3.24 και 3.25 παρατίθενται οι βασικές πληροφορίες του <ΣΧ-8> και οι ενέργειες της βασικής ροής αντίστοιχα, ενώ στο σχήμα 3.11 φαίνεται το διάγραμμα της βασικής ροής.

Ψηφίζω σε μήνυμα	
Σύντομη περιγραφή	Στόχος του σεναρίου χρήσης είναι ο χρήστης να μπορεί να υπερψηφίσει ή καταψηφίσει ένα μήνυμα.
Αναφορά ΛΑ	<ΛΑ-8>
Αναφορά ΜΛΑ	<ΜΛΑ-2>
Πυροδότηση δραστηριότητας	Ο επισκέπτης πατάει το κουμπί υπερψηφίσης ή καταψηφίσης.
Προϋπόθεση	Ο χρήστης να έχει συνδεθεί στην εφαρμογή και να βρίσκεται στην σελίδα ενός θέματος το οποίο περιλαμβάνει τουλάχιστον ένα μήνυμα το οποίο δεν έχει δημιουργήσει ο ίδιος.

Πίνακας 3.24: Σενάριο χρήσης 8, ψήφιση μηνύματος.

Βασική ροή		
Γραμμή	Ενέργεια χρήστη συστήματος	Απάντηση Συστήματος
1	Ο χρήστης πατάει στο κουμπί υπερψηφίσης μηνύματος.	Το σύστημα εισάγει νέα ψήφο μηνύματος στο blockchain.
Μετάπειτα κατάσταση:	Το σύστημα ανανεώνει τις ψήφους του μηνύματος.	

Πίνακας 3.25: Σενάριο χρήσης 8 - Βασική ροή



Σχήμα 3.11: Σενάριο χρήσης 8 - Διάγραμμα βασικής ροής

3.6.9 Σενάριο χρήσης 9: Διαγραφή τοπικών δεδομένων

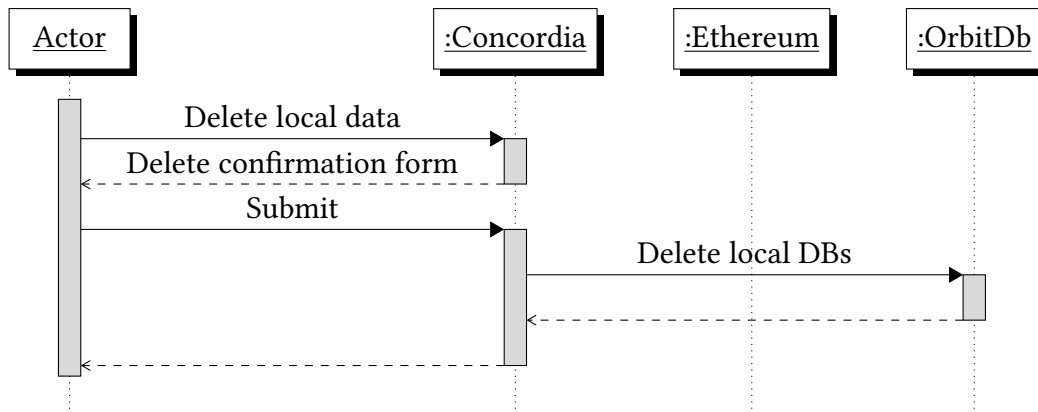
Το σενάριο χρήσης 9, <ΣΧ-9>, περιγράφει τις διαδοχικές ενέργειες που εκτελούνται για τη διαγραφή των τοπικών δεδομένων. Στους πίνακες 3.26 και 3.27 παρατίθενται οι βασικές πληροφορίες του <ΣΧ-9> και οι ενέργειες της βασικής ροής αντίστοιχα, ενώ στο σχήμα 3.12 φαίνεται το διάγραμμα της βασικής ροής.

Διαγράψω τα τοπικά δεδομένα	
Σύντομη περιγραφή	Στόχος του σεναρίου χρήσης είναι ο επισκέπτης να μπορεί να διαγράψει τα τοπικά δεδομένα που αποθηκεύονται στο σύστημά του από την εφαρμογή.
Αναφορά ΛΑ	<ΛΑ-11>
Αναφορά ΜΛΑ	-
Πυροδότηση δραστηριότητας	Ο επισκέπτης πατάει το κουμπί διαγραφής των τοπικών δεδομένων.
Προϋπόθεση	Ο επισκέπτης πρέπει να έχει ανοίξει την σελίδα της εφαρμογής.

Πίνακας 3.26: Σενάριο χρήσης 9, διαγραφή τοπικών δεδομένων.

Βασική ροή		
Γραμμή	Ενέργεια χρήστη συστήματος	Απάντηση Συστήματος
1	Ο επισκέπτης πατάει το κουμπί διαγραφής των τοπικών δεδομένων.	Το σύστημα εμφανίζει την φόρμα “Επιβεβαίωση Διαγραφής Τοπικών Δεδομένων”.
2	Ο επισκέπτης συμπληρώνει το πεδίο και πατάει το κουμπί “Υποβολή”.	Το σύστημα διαγράφει όλες τις τοπικές βάσεις OrbitDb που χρησιμοποιούνται από την εφαρμογή.
Μετάπειτα κατάσταση:	Το σύστημα παραμένει πραγματοποιεί ανανέωση της σελίδας.	

Πίνακας 3.27: Σενάριο χρήσης 9 - Βασική ροή



Σχήμα 3.12: Σενάριο χρήσης 9 - Διάγραμμα βασικής ροής

3.7 Αρχιτεκτονική σχεδίαση

Στο κεφάλαιο αυτό θα περιγραφεί η αρχιτεκτονική του συστήματος, όπως αυτό σχεδιάστηκε αρχικά. Η αρχιτεκτονική αυτή είναι πρώιμη και δεν αποτελεί την τελική υλοποίηση της πλατφόρμας στο σύνολό της. Μέρη της πρώιμης αρχιτεκτονικής είναι διαφορετικά από αυτά της τελικής η οποία περιγράφεται σε επόμενο κεφάλαιο.

Η πλατφόρμα χωρίζεται σε δύο λογικά μέρη τα οποία θα αναλυθούν σε λεπτομέρεια στα επόμενα κεφάλαια:

- α) μία αυτοτελή και πλήρως αποκεντρωτική πλατφόρμα επικοινωνίας γενικής χρήσης
- β) μία μερικώς αποκεντρωτική και μη αυτοτελή επέκταση του πρώτου μέρους στοχευμένη για χρήση από μέλη του ΑΠΘ

3.7.1 Πρώτο μέρος

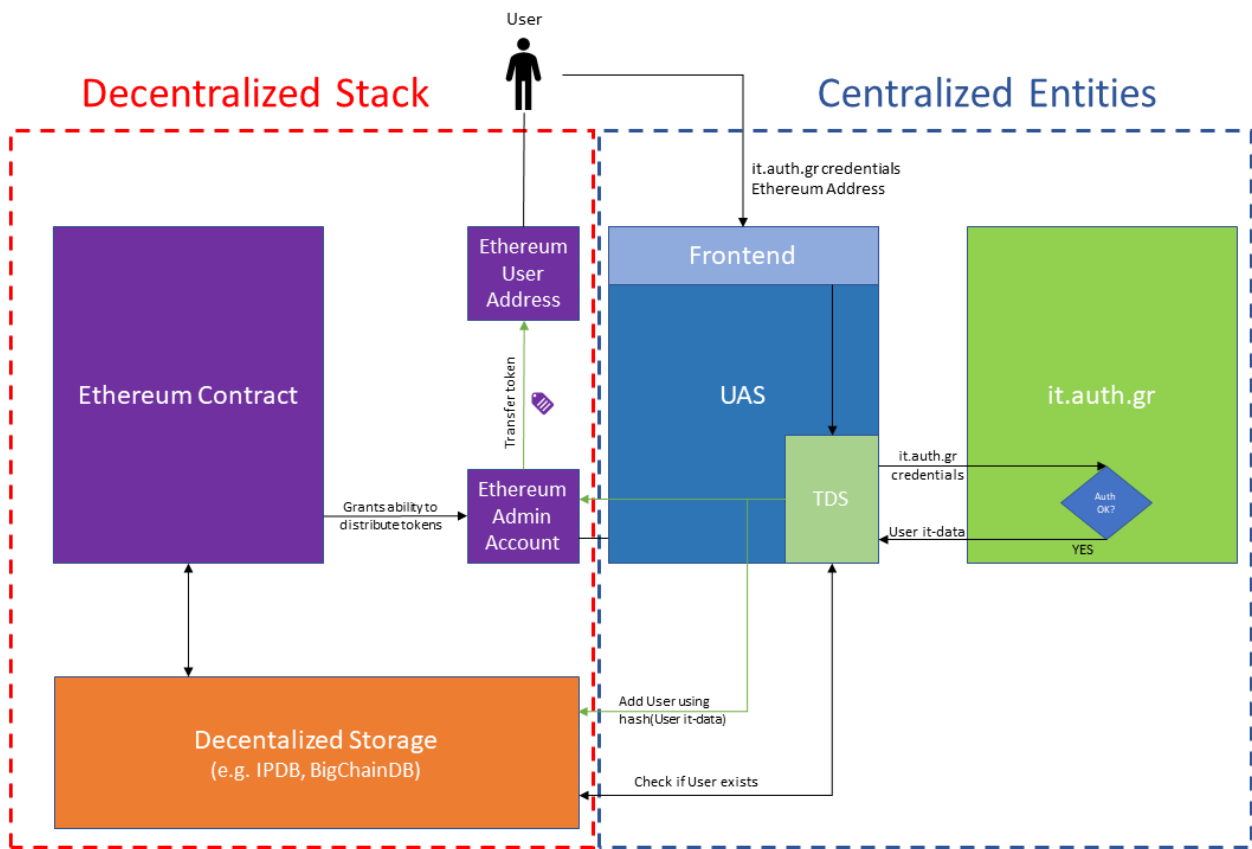
Το πρώτο μέρος αποτελεί μία αυτοτελή και πλήρως αποκεντρωτική πλατφόρμα. Στόχος της πλατφόρμας είναι να παρέχει τη δυνατότητα ελευθερίας λόγου, απρόσβλητου σε λογοκρισία από κεντρικές οντότητες εξουσίας. Στην πλατφόρμα αυτή θα μπορεί οποιοσδήποτε να δημιουργήσει θέματα (topics) ή να απαντήσει σε άλλα. Η επεξεργασία των πληροφοριών που παράγονται και η οποία είναι αναγκαία για τη λειτουργία της πλατφόρμας θα παρέχεται από το Ethereum μέσω των smart contracts τα οποία θα υλοποιηθούν στο πλαίσιο αυτής της διπλωματικής. Τα contracts αποτελούν ανοιχτό λογισμικό από τη φύση τους, κάτι το οποίο ενισχύει την διαφάνεια των διαδικασιών κάνοντας το επιχείρημα της ισότητας του λόγου πιο δυνατό. Τα contracts αυτά θα δέχονται transactions από τους χρήστες και θα εγγράφουν τα αποτελέσματα στο Storage Layer του blockchain:

Το πρόβλημα αυτής της προσέγγισης είναι πως, για τη λειτουργία της, απαιτείται για κάθε συναλλαγή (transaction) οι χρήστες να καταβάλουν ένα τέλος. Το τέλος αυτό αφορά τα fees που είναι αναγκαία για την περάτωση των συναλλαγών. Παρόλο που υπάρχουν σχέδια από την ομάδα ανάπτυξης του Ethereum για τη μείωσή αυτών των fees στο μέλλον, θα είναι πάντα αναπόφευκτα για τη χρήση του EVM. Ωστόσο, πρέπει να σημειωθούν δύο πράγματα. Αφενός τα τέλη παρέχουν μια μορφή προστασίας απέναντι σε κακόβουλους χρήστες που θα πλημμύριζαν την εφαρμογή με ανεπιθύμητο ποσοτικά ή ποιοτικά περιεχόμενο καθώς θα τους ήταν οικονομικά ασύμφορη μια τέτοια επίθεση. Αφετέρου υπάρχουν κάποιες εναλλακτικές ώστε να μειωθεί δραστικά η εμπλοκή του χρήστη με την καταβολή τελών, κάτι που περιγράφεται παρακάτω στις κατηγορίες χρηστών.

Τα παραπάνω πρακτικά σημαίνουν ότι το Smart Contract θα πρέπει ανά διαστήματα να φορτίζεται με Ether ή οι χρήστες να καταβάλουν τα δικά τους έξοδα.

3.7.2 Δεύτερο μέρος

Το δεύτερο μέρος αποτελεί μια μερικώς αποκεντρωτική και μη αυτοτελή πλατφόρμα που λειτουργεί προσθετικά στην πρώτη. Το κομμάτι αυτό απευθύνεται αποκλειστικά σε επικυρωμένα μέλη του ΑΠΘ και συνιστά ένα αμεσοδημοκρατικό σύστημα ψηφοφορίας που θα εγγυάται σε υψηλό βαθμό την εγκυρότητα και την ανωνυμία των διαδικασιών του. Στο πρώτο μέρος, το οποίο αναλύθηκε προηγουμένως, θα παρέχεται η δυνατότητα δημιουργίας θεμάτων προς ψηφοφορία. Πάνω στα θέματα αυτά θα ψηφίζουν όσοι έχουν δικαίωμα, ενώ το δικαίωμα στην ψήφο θα ορίζεται με την κατοχή ενός ανάλογου token στο Ethereum.



Σχήμα 3.13: Ethereum logo

Ο χρήστης, μέσω ενός frontend με τη μορφή ιστοσελίδας, θα μπορεί να πιστοποιήσει μέσω login στο it.auth.gr την ακαδημαϊκή του ταυτότητα. Στη συνέχεια η Υπηρεσία Διανομής Token (Token Distribution Service - TDS), όντως ο ιδιοκτήτης (owner) του contract που δινέ- μαι τα tokens θα παρέχει στο χρήστη δύο tokens. Το πρώτο token θα δίνει στον χρήστη το δικαίωμα ψήφου (verified user token) και το δεύτερο θα σηματοδοτεί στη πλατφόρμα ότι πρέπει του επιστρέφει τα τέλη (fees) τα οποία πληρώνει (trusted user token).

*Ιδανικά, με τη συνεργασία του ΑΠΘ, το UAS θα αποτελεί υπηρεσία συνεργαζόμενη με την Υποδομή πιστοποίησης και εξουσιοδότησης (βλ. <https://it.auth.gr/el/infrastructure/aai>). Αυτό ση- μαίνει ότι οι χρήστες δε θα χρειάζεται να εμπιστευτούν τον UAS με τα it credential τους.

3.8 Προδιαγραφή μεθόδου υλοποίησης και χρονοπρογραμματισμός

3.8.1 Προδιαγραφή κύκλων

Εποπτικά, η διαδικασία της υλοποίησης περιγράφεται ως εξής:

3.8.2 Πρώτη φάση

Στήνεται ένα Ethereum Private Network ως βάση πάνω στην οποία θα δουλέψουμε. Πάνω σε αυτό γράφουμε τα contracts που θα είναι υπεύθυνα για διεκπεραίωση ή μη των posts. Στη συνέχεια αναπτύσσεται ο απαραίτητος κώδικας που υλοποιεί το posting χρησιμοποιώντας τις βιβλιοθήκες που δίνονται από το IPFS για την επικοινωνία μεταξύ των κόμβων του δικτύου και αυτές που δίνονται από τη BigChainDB για την αποθήκευση των πληροφοριών με διανεμημένο τρόπο. Γίνονται δοκιμές για την εξακρίβωση της σωστής λειτουργίας του αποτελέσματος και διορθώνονται τυχόν λάθη στο κώδικα.

3.8.3 Δεύτερη φάση

Υλοποιείται το δικαίωμα ψήφου και posting χωρίς fees. Αυτό γίνεται μέσω δύο contracts που θα δημιουργούν δύο διαφορετικά tokens (voting token, feeless token) και θα τα αποδίδουν στον εκάστοτε χρήστη που πρέπει να πάρει το δικαίωμα. Αναπτύσσεται κώδικας που να υλοποιεί τη διαδικασία ψηφοφορίας. Γίνονται δοκιμές για την εξακρίβωση της σωστής λειτουργίας του αποτελέσματος και διορθώνονται τυχόν λάθη στο κώδικα. Σε αυτή τη φάση η απόδοση των tokens θα γίνει χειροκίνητα για το σκοπό της δοκιμής.

3.8.4 Τρίτη φάση

Υλοποιείται ένα σύστημα απόδοσης εμπιστοσύνης (ΣΑΠ). Αναπτύσσονται τα contracts που είναι απαραίτητα για τη λειτουργία του ΣΑΠ καθώς και για την αυτόματη απόδοση feeless token στους trusted χρήστες. Γίνονται δοκιμές για την εξακρίβωση της σωστής λειτουργίας του αποτελέσματος και διορθώνονται τυχόν λάθη στο κώδικα. Εφόσον η εφαρμογή περάσει το στάδιο των δοκιμών είναι έτοιμη για alpha deployment, είναι δηλαδή έτοιμη για χρήση από το κοινό, υπολείπονται όμως χαρακτηριστικά που είναι ιδιαίτερα θεμιτά αλλά όχι απαραίτητα για τη λειτουργία.

3.8.5 Τέταρτη φάση

Αναπτύσσεται ο κώδικας του (μοναδικού) συγκεντρωτικού τμήματος του συστήματος το οποίο ανήκει στο δεύτερο κομμάτι - του UAS: Έτσι αυτοματοποιείται η διαδικασία απόδοσης των token, που στην προηγούμενη φάση έγινε χειροκίνητα. Γίνονται δοκιμές για την εξακρίβωση της σωστής λειτουργίας του αποτελέσματος και διορθώνονται τυχόν λάθη στο κώδικα. Εφόσον η εφαρμογή περάσει το στάδιο των δοκιμών είναι έτοιμη για ένα beta deployment, ώστε να γίνει πιο ευρύς έλεγχος από μία ομάδα δοκιμών και να παρθεί feedback για την εμπειρία χρήστη.

Για το τελικό deployment θα μπορούσε να τεθεί ως στόχος η κατά το δυνατόν μείωση των τελών για τη λειτουργία της πλατφόρμας, ανεπτυγμένα χαρακτηριστικά επικοινωνίας όπως δόμηση των συζητήσεων σε κατηγορίες, προφίλ χρηστών και άλλα χαρακτηριστικά ευκολίας χρήσης.

Κεφάλαιο 4

Υλοποίηση εφαρμογής

4.1 Χαρακτηριστικά που υλοποιήθηκαν

TODO: move to last, add diagram with colors
TODO: add references to use cases implemented with screenshots of application
TODO: add unimplemented parts like serve (front and contracts) thru IPFS, upgradability
TODO: add differences in architecture

4.2 Μεθοδολογία υλοποίησης

Για την επίτευξη των στόχων που ορίστηκαν και την οργάνωση της εργασίας που απαιτείται σε διαχειρίσιμα μέρη, σχεδιάστηκε η χρήση διάφορων εργαλείων και μεθόδων ανάπτυξης λογισμικού, όπως το σύστημα ελέγχου εκδόσεων (version control system) Git και η μέθοδος οργάνωσης Scrum. Τα εργαλεία αυτά είναι δοκιμασμένα και έχουν εδραιωθεί στη σύγχρονη ανάπτυξη λογισμικού.

Το Git είναι δωρεάν λογισμικό ανοιχτού κώδικα το οποίο επιτρέπει και επικουρεί την απρόσκοπτη ανάπτυξη λογισμικού από πολλαπλά μέλη μίας ομάδας, ταυτόχρονα και διανεμημένα. Αυτό επιτυγχάνεται παρέχοντας ένα πλαίσιο από εργαλεία τα οποία βοηθούν την διαχείριση και ενσωμάτωση των διαφορετικών εκδόσεων του κώδικα τις οποίες αναπτύσσει κάθε μέλος της ομάδας ξεχωριστά. Υπάρχουν διάφορα μοντέλα χρήσης του Git και πιο συγκεκριμένα της δυνατότητας που δίνει για δημιουργία, ανάπτυξη και ένωση κλαδιών (branches). Για τους σκοπούς της παρούσας διπλωματικής χρησιμοποιήθηκε το μοντέλο GitHub flow[17]. Το μοντέλο αυτό ορίζει ότι κάθε προγραμματιστής θα ανοίγει ένα νέο branch για τη ανάπτυξη ενός νέου χαρακτηριστικού της εφαρμογής ή τη διόρθωση ενός μέρους του κώδικα. Έπειτα, όταν η δουλειά έχει ολοκληρωθεί, το branch ενώνεται (merge) με το βασικό branch της εφαρμογής.

Το Scrum είναι μία μέθοδος οργάνωσης στην οποία ο επιμελητής του Scrum (Scrum master) διαχωρίζει τα ανεξάρτητα μέρη εργασίας (tasks) που πρέπει να υλοποιηθούν για την ολοκλήρωση των στόχων ενός project. Τα μέρη αυτά περιγράφονται αναλυτικά μαζί με τις απαιτήσεις τους και κατατίθενται σε μία λίστα εργασιών (backlog). Έπειτα, μέσα από συσκέψεις (meetings), επιλέγεται ένας αριθμός από μέρη εργασίας τα οποία θα αποτελέσουν το επόμενο Sprint. Κάθε μέρος εργασίας ανατίθεται σε κάποιο μέλος για υλοποίηση και ορίζεται για το Sprint μία χρονική διάρκεια, στόχος της οποίας είναι η περάτωση όλων των μερών εργασίας πριν τη λήξη της. Στο τέλος προθεσμίας που ορίστηκε για το Sprint τα μέλη της ομάδας αποτιμούν τα αποτελέσματα και ορίζουν το επόμενο Sprint. Η διαδικασία επαναλαμβάνεται έως ότου το έργο ολοκληρωθεί.

Μέσα από την χρήση των παραπάνω εργαλείων επιτυγχάνεται η ομαλή συνεργασία στην ανάπτυξη του λογισμικού. Κάθε μέλος της ομάδας δύναται να εργαστεί ανεξάρτητα και χωρίς την ανάγκη διαρκούς επικοινωνίας με τα υπόλοιπα μέλη. Οι στόχοι είναι ορισμένοι, σαφείς και

χωρισμένοι σε διαχειρίσιμα μέρη τα οποία δεν καταβάλουν τα μέλη. Ταυτόχρονα, έχοντας ως έδρα καθιερωμένα πρότυπα ανάπτυξης, παρέχεται φορμαλισμός και έτοιμες μέθοδοι επίλυσης προβλημάτων, γεγονός που λειτουργεί καταλυτικά και βοηθά στην αποφυγή τελεμάτων κατά τη συγγραφή του κώδικα.

TODO: add continuous integration

4.3 Τεχνολογίες υλοποίησης

TODO: add ganache, truffle TODO: add additional technologies like react, redux, sagas, express, nodejs, docker TODO: add jenkins, janus and build steps diagram

4.3.1 OrbitDB



Σχήμα 4.1: OrbitDB logo

Η OrbitDB είναι μία P2P βάση δεδομένων ανοιχτού κώδικα. Χρησιμοποιεί το IPFS για την αποθήκευση των δεδομένων και το IPFS Pubsub για τον αυτόματο συγχρονισμό των βάσεων δεδομένων μεταξύ των peers. Είναι τελικά συνεπής (eventually consistent) και χρησιμοποιεί CRDTs (Conflict-Free Replicated Data Types) για συγχωνεύσεις βάσεων δεδομένων χωρίς συγκρούσεις, πράγμα που την καθιστά εξαιρετική επιλογή για DApps και offline-first web applications.[18]

Κάποια Βασικά χαρακτηριστικά της είναι τα εξής:

- **Stores:** Η OrbitDB παρέχει διάφορους τύπους βάσεων (stores) για διαφορετικά μοντέλα δεδομένων και περιπτώσεις χρήσης:
 - **log:** ένα αμετάβλητο (μόνο για προσάρτηση) ημερολόγιο με ανιχνεύσιμο ιστορικό.
 - **feed:** ένα μεταβλητό αρχείο καταγραφής με ανιχνεύσιμο ιστορικό, του οποίου οι καταχωρήσεις μπορούν να προστεθούν και να αφαιρεθούν.
 - **keyvalue:** μία βάση δεδομένων κλειδιών-τιμών.
 - **docs:** μία βάση δεδομένων εγγράφων στην οποία μπορούν να αρχειοθετηθούν έγγραφα JSON με ένα καθορισμένο κλειδί.
 - **counter:** μία βάση δεδομένων για καταμέτρηση συμβάντων.

Όλα τα stores υλοποιούνται πάνω στο `ipfs-log`, μία αμετάβλητη, operation-based CRDT για καταναμημένα συστήματα, ενώ υπάρχει και η δυνατότητα δημιουργίας προσαρμοσμένων stores ανάλογα με την περίπτωση.

- **Address:** Κάθε βάση δεδομένων λαμβάνει κατά τη δημιουργία της μία διεύθυνση της μορφής `/orbitdb/CID/DATABASE_NAME`, όπου CID είναι το IPFS multihash του μανιφέστου της και DATABASE_NAME το όνομα της βάσης.[19] Το μανιφέστο είναι ένα IPFS object που περιέχει πληροφορίες της βάσης όπως το όνομα, τον τύπο και έναν δείκτη στον ελεγκτή πρόσβασης (access controller).

- **Identity:** Κάθε φορά που προστίθεται μία εγγραφή στη βάση υπογράφεται από τον δημιουργό της, ο οποίος προσδιορίζεται από μία ταυτότητα (identity). Το Identity object, πέρα από τον προεπιλεγμένο τρόπο λειτουργίας, μπορεί να προσαρμοστεί έτσι ώστε να συνδέεται με κάποιο εξωτερικό αναγνωριστικό. Η μορφή του έχει ως εξής⁹:

```
{
  _id: '<the ID of the external identity>',
  // Auto-generated by OrbitDB
  _publicKey: '<signing key used to sign OrbitDB entries>',
  signatures: {
    //Allows the owner of id to prove they own the private key
    //associated with publicKey
    id: '<signature of _id signed using publicKey>',
    //This links the two ids
    publicKey: '<signature of signatures.id + _publicKey using
      _id>'
  },
  type: 'orbitdb'
}
```

Σχήμα 4.2: OrbitDB Identity

- **Access Control:** Κατά τη δημιουργία μίας βάσης μπορούν να οριστούν όσοι θα έχουν δικαίωμα να γράψουν σε αυτή μέσω ενός ελεγκτή πρόσβασης (access controller). Ο ελεγκτής θα περιλαμβάνει τα public keys τους, τα οποία μπορούν να ανακτηθούν από το identity του καθενός. Από προεπιλογή και αν δεν ορίζεται διαφορετικά, δίνεται πρόσβαση εγγραφής μόνο στον δημιουργό της βάσης.

4.4 Αρχιτεκτονική υλοποίησης

Το σύστημα υλοποιήθηκε χρησιμοποιώντας το μοντέλο αρχιτεκτονικής των μικροϋπηρεσιών. Το μοντέλο των μικροϋπηρεσιών βασίζεται στην αποδόμηση του συστήματος σε μικρές μονάδες, οι οποίες συνεργάζονται ώστε να προσφέρουν ένα ενιαίο αποτέλεσμα. Η προσέγγιση αυτή έχει πολλά πλεονεκτήματα σε σύγκριση με την ανάπτυξη μονολιθικών εφαρμογών. Ο βασικός λόγος για τον οποίο επιλέχθηκε η αρχιτεκτονική μικροϋπηρεσιών είναι η ευκολία που προσφέρει στη γρήγορη ανάπτυξη καινούριων χαρακτηριστικών, ταυτόχρονα από διαφορετικά μέλη μίας ομάδας, ασύγχρονα και χωρίς την ανάγκη συνεχής επικοινωνίας και συνεννόησης μεταξύ τους. Αυτό συμβαίνει επειδή κάθε μέρος του συστήματος (υπηρεσία) είναι αυτόνομο και η ανάπτυξή του είναι διαχωρισμένη από το υπόλοιπο σύστημα με το οποίο είναι αδύναμα συνδεδεμένο (loosely coupled).

Το σύστημα συντίθεται από διάφορες μικροϋπηρεσίες, κάποιες από τις οποίες αναπτύχθηκαν στα πλαίσια αυτής της εργασίας ενώ άλλες αποτελούν δωρεάν λογισμικό ανοιχτού κώδικα. Οι μικροϋπηρεσίες αυτές συνοψίζονται στον παρακάτω πίνακα (πίνακας 4.1).

⁹Βλ. και <https://github.com/orbitdb/orbit-db-identity-provider>

Μικροϋπηρεσία	Σύντομη περιγραφή - Αντικείμενο/Στόχος
Concordia Application	Υπηρεσία με την οποία αλληλεπιδρούν οι χρήστες.
Concordia Contracts Migrator	Υπηρεσία μεταφόρτωσης των συμβολαίων (contracts) στο blockchain.
Concordia Pinner	Υπηρεσία καρφισώματος δεδομένων.
Concordia Contracts Provider	Υπηρεσία διαμοιρασμού των contract artifacts μέσω HTTP.
Ganache	Τοπικό, ιδιωτικό Ethereum blockchain.
Rendezvous Server	Υπηρεσία εύρεσης ομότιμων χρηστών.

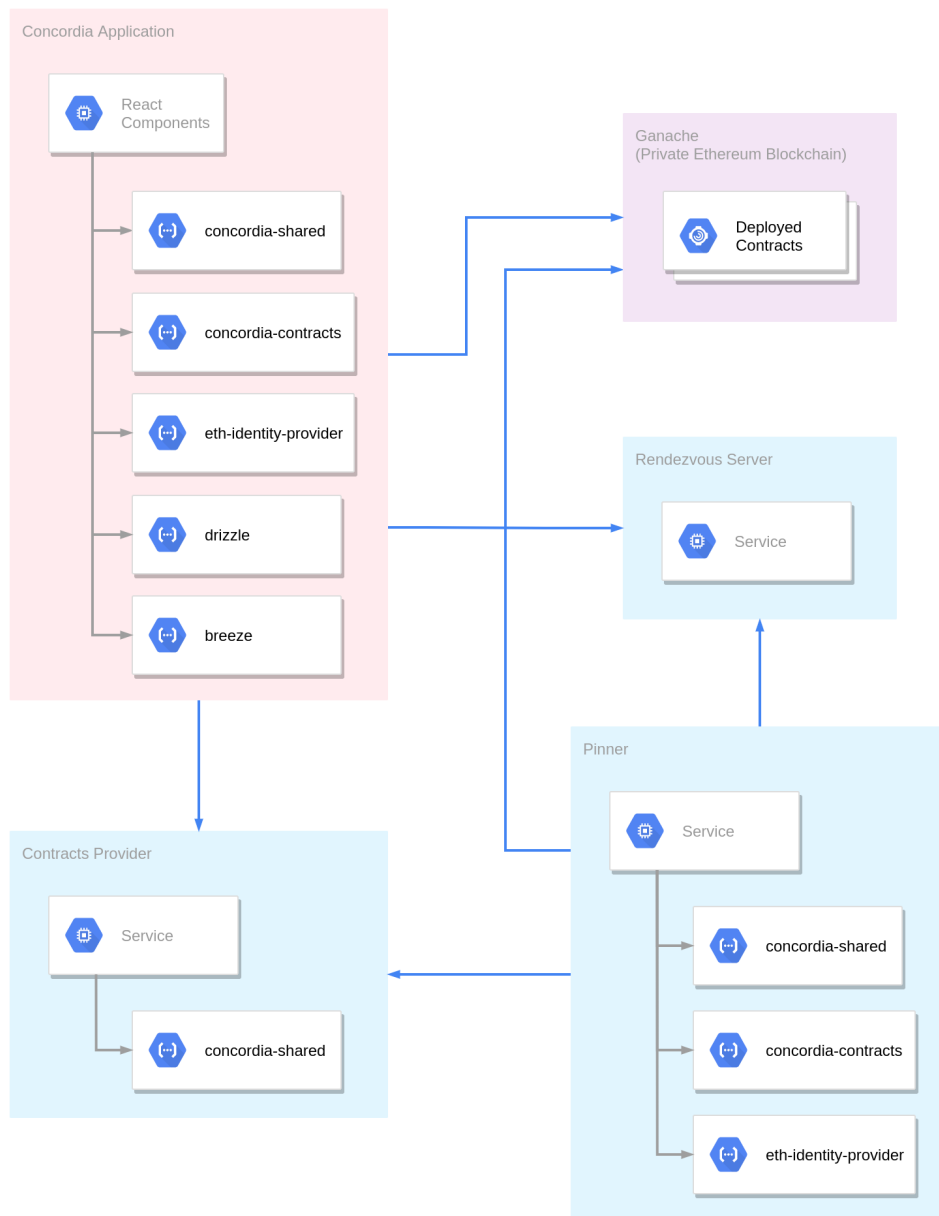
Πίνακας 4.1: Σύντομη περιγραφή υπηρεσιών συστήματος.

Στα πλαίσια της εργασίας αναπτύχθηκαν επίσης διάφορα αρθρώματα, κυρίως με τη μορφή βιβλιοθηκών Javascript. Τα αρθρώματα χρησιμοποιούνται από τις υπηρεσίες για την επίτευξη των επιμέρους εργασιών. Η ανάπτυξη του λογισμικού σε ξεχωριστά αρθρώματα επιτρέπει την εύκολη επαναχρησιμοποίηση του κώδικα καθώς και τον διαχωρισμό των αυτόνομων τμημάτων κώδικα. Τα αρθρώματα συνοψίζονται στον παρακάτω πίνακα (πίνακας 4.2).

Άρθρωμα	Σύντομη περιγραφή - Αντικείμενο/Στόχος
Άρθρωμα concordia-shared	Χρήσιμα εργαλεία και σταθερές συστήματος.
Άρθρωμα concordia-contracts	Μεταγλώττιση των contracts και διάθεση των artifacts.
Άρθρωμα eth-identity-provider	Δημιουργία μοναδικού αναγνωριστικού χρήστη για τη βάση OrbitDB.
Άρθρωμα drizzle	Βελτιωμένη προγραμματιστική διεπαφή επικοινωνίας με το blockchain.
Άρθρωμα breeze	Βελτιωμένη προγραμματιστική διεπαφή χρήσης της βάσης OrbitDB.

Πίνακας 4.2: Σύντομη περιγραφή αρθρωμάτων συστήματος.

Τα αρθρώματα και οι υπηρεσίες θα περιγραφούν σε μεγαλύτερη ανάλυση στα επόμενα κεφάλαια. Στο παρακάτω σχήμα (σχήμα 4.3) φαίνεται η συνολική αρχιτεκτονική του συστήματος.



Σχήμα 4.3: Διάγραμμα αρχιτεκτονικής συστήματος

4.4.1 Αρθρώματα

Στο κεφάλαιο αυτό θα περιγραφούν με μεγαλύτερη λεπτομέρεια τα αρθρώματα που αναπτύχθηκαν.

Άρθρωμα concordia-shared

Το άρθρωμα concordia-shared αποτελεί μία βιβλιοθήκη χρήσιμων εργαλείων και σταθερών. Εδώ περιέχεται όλο το λογισμικό το οποίο πρέπει ή είναι επιθυμητό να συμπεριφέρεται με τον ίδιο τρόπο συνολικά στο σύστημα, όπως για παράδειγμα μέθοδοι παραμετροποίησης των υπηρεσιών και μέθοδοι καταγραφής (logging). Το άρθρωμα αυτό χρησιμοποιείται από το άρθρωμα concordia-contracts καθώς και από τις υπηρεσίες Concordia Application, Concordia Pinner και Concordia Contracts Provider.

Το άρθρωμα αυτό γίνεται διαθέσιμο για χρήση με τη μορφή τοπικής βιβλιοθήκης με τη χρήση της βιβλιοθήκης διαχείρισης μοναδικού αποθετηρίου κώδικα (monorepo) lerna.

Άρθρωμα concordia-contracts

Το άρθρωμα αυτό επιτελεί δύο ενέργειες. Αρχικά, είναι το άρθρωμα στο οποίο αναπτύσσονται τα contracts που χρησιμοποιούνται από την εφαρμογή. Το άρθρωμα αυτό αναλαμβάνει τη μεταγλώττιση των contracts από κώδικα γλώσσας Solidity, στην κατάλληλη τελική μορφή JSON. Παρέχονται επίσης σενάρια ενεργειών (scripts) ώστε τα contracts να μεταφορτωθούν σε blockchain καθώς και στην υπηρεσία Concordia Contracts Provider. Αποτελεί επίσης βιβλιοθήκη η οποία μετά τη μεταγλώττιση και μεταφόρτωση των contracts σε blockchain παρέχει τα contract artifacts. Χρησιμοποιείται από τις υπηρεσίες Concordia Application και Concordia Pinner.

Το άρθρωμα αυτό γίνεται διαθέσιμο για χρήση με τη μορφή τοπικής βιβλιοθήκης με τη χρήση της βιβλιοθήκης διαχείρισης `monorepo lerna`.

Άρθρωμα eth-identity-provider

Η λειτουργία της βάση OrbitDB απαιτεί τη δημιουργία ενός μοναδικού αναγνωριστικού χρήστη (identity). Για την εύκολη εξαγωγή ενός αναγνωριστικού χρήστη το οποίο να είναι μοναδικό αλλά να είναι δυνατός ο επανυπολογισμός, χρησιμοποιήθηκε ο συνδυασμός της διεύθυνσης του χρήστη στο δίκτυο Ethereum με τη διεύθυνση του βασικού contract που χρησιμοποιεί η εφαρμογή. Ο υπολογισμός του συνδυασμού αυτού υλοποιείται από αυτό το άρθρωμα.

Το άρθρωμα αυτό γίνεται διαθέσιμο για χρήση με τη μορφή βιβλιοθήκης μέσω του αποθετηρίου λογισμικού `npm`.

Άρθρωμα drizzle

Το άρθρωμα `drizzle` που χρησιμοποιείται στην υπηρεσία Concordia Application είναι μία τροποποιημένη έκδοση της Javascript βιβλιοθήκης `Drizzle` που προσφέρεται από τη σουίτα εργαλείων `Truffle`. Η τροποποιημένη βιβλιοθήκη αναπτύχθηκε στα πλαίσια της διπλωματικής με στόχο τη διευκόλυνση της χρήσης του `Drizzle` και την επιδιόρθωση προβληματικών σημείων της πρωτότυπης βιβλιοθήκης.

Το άρθρωμα `drizzle` υλοποιεί τις προγραμματιστικές διεπαφές μέσω των οποίων πραγματοποιείται η επικοινωνία της εφαρμογής με το blockchain. Για την επίτευξη της επικοινωνίας αυτής, η βιβλιοθήκη χρησιμοποιεί τη συλλογή βιβλιοθηκών `web3.js` η οποία αποτελεί τον πιο διαδεδομένο τρόπο διεπαφής με το blockchain σε αποκεντρωτικές εφαρμογές.

Το άρθρωμα αυτό γίνεται διαθέσιμο για χρήση με τη μορφή βιβλιοθήκης μέσω του αποθετηρίου λογισμικού `npm`.

Άρθρωμα breeze

Το άρθρωμα αυτό αποτελεί μία βιβλιοθήκη περίβλημα (wrapper) της βιβλιοθήκης OrbitDB. Η OrbitDB είναι μία βιβλιοθήκη η οποία προσφέρει τις απαραίτητες προγραμματιστικές διεπαφές για τη χρήση της βάσης δεδομένων με το ίδιο όνομα. Μέσα από τη χρήση των βιβλιοθηκών που προσφέρονται από το IPFS για την αποθήκευση δεδομένων, η OrbitDB καταφέρνει να υλοποιήσει μία αποκεντρωμένη βάση δεδομένων.

Το άρθρωμα `breeze` κάνει χρήση της βιβλιοθήκης OrbitDB, προσφέρει ωστόσο συγκεκριμένες προγραμματιστικές διεπαφές που διευκολύνουν τόσο την παραμετροποίηση της βάσης όσο και τη χρήση της, ενώ όπως και στο άρθρωμα `drizzle` το άρθρωμα `breeze` αναλαμβάνει να διορθώσει ορισμένα προβλήματα της πρωτότυπης βιβλιοθήκης.

Το άρθρωμα αυτό γίνεται διαθέσιμο για χρήση με τη μορφή βιβλιοθήκης μέσω του αποθετηρίου λογισμικού `npm`.

4.4.2 Concordia Application

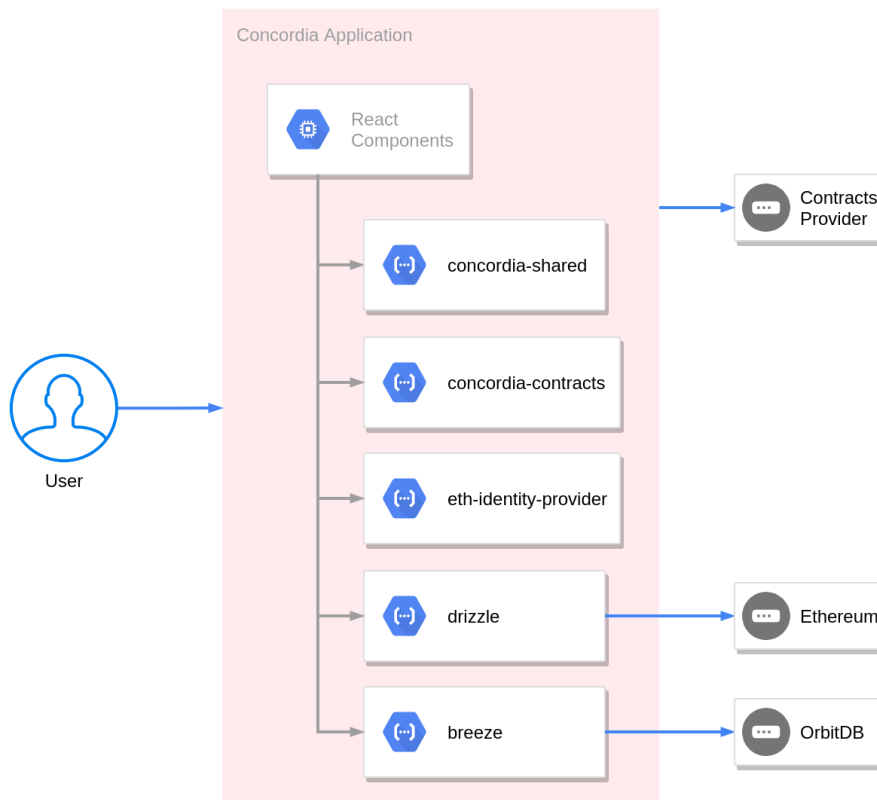
Περιγραφή - Στόχοι υπηρεσίας

Η εφαρμογή Concordia (Concordia Application) εκθέτει τις γραφικές διεπαφές μέσω των οποίων αλληλεπιδρούν οι χρήστες με το σύστημα. Αποτελεί τον δίαυλο επικοινωνίας του τελικού χρήστη με το blockchain και με τη βάση OrbitDB. Η αρχιτεκτονική της υπηρεσίας φαίνεται στο σχήμα 4.4. Μέσω της εφαρμογής Concordia οι χρήστες μπορούν να:

- περιηγηθούν και διαβάσουν το περιεχόμενο της πλατφόρμας
- δημιουργήσουν λογαριασμό χρήστη
- δημοσιεύσουν και τροποποιήσουν προσωπικές τους πληροφορίες όπως η τοποθεσία και η εικόνα προφίλ
- δημιουργήσουν θέματα (topics)
- δημιουργήσουν ψηφοφορίες (polls), καθώς και να ψηφίσουν σε αυτές
- δημιουργήσουν και τροποποιήσουν μηνύματα (posts)
- υπερψηφίσουν (up-vote) ή καταψηφίσουν (down-vote) μηνύματα άλλων χρηστών

Η υπηρεσία αποτελείται από κώδικα γραμμένο σε Javascript ο οποίος γίνεται διαθέσιμος στους τελικούς χρήστες με τη μορφή εφαρμογής διαδικτύου (web application) μέσω ενός διακομιστή (server). Παρόλο που η υπηρεσία προσφέρει τη γραφική διεπαφή χρήστη μόνο στην αγγλική γλώσσα, έχει παραμετροποιηθεί ώστε να είναι δυνατή η εύκολη μεταγλώττιση της χωρίς την ανάγκη πραγματοποίησης μεγάλων αλλαγών στον κώδικα.

Χρησιμοποιείται η βιβλιοθήκη React για την οργάνωση και ανάπτυξη των συνθετικών τμημάτων (components) του γραφικού περιβάλλοντος. Για το γραφικό περιβάλλον γίνεται χρήση του framework της Semantic UI. Χρησιμοποιείται η βιβλιοθήκη Redux για τη διαχείριση κατάστασης της εφαρμογής (state management), καθώς και η βιβλιοθήκη Redux-Saga για τη διαχείριση ασύγχρονων παράπλευρων ενεργειών (side-effects) σε ένα σύστημα βασισμένο σε συμβάντα (event-based). Άλλες βιβλιοθήκες χρησιμοποιούνται για διάφορα μέρη της υπηρεσίας, ενώ χρησιμοποιούνται επίσης τα αρθρώματα που περιγράφηκαν προηγουμένως για την επίτευξη διαφορετικών στόχων. Ο πλήρης κατάλογος των βιβλιοθηκών και αρθρωμάτων μπορεί να βρεθεί στον κώδικα της υπηρεσίας στο παράρτημα.



Σχήμα 4.4: Αρχιτεκτονική υπηρεσίας Concordia Application

Για τη λειτουργία της υπηρεσίας Concordia Application είναι απαραίτητα τα αντικείμενα (artifacts) που προκύπτουν από τη μεταγλώττιση των contracts και τη μεταφόρτωση/δημοσίευσή τους στο blockchain. Για την εισαγωγή των artifacts στην υπηρεσία έχουν αναπτυχθεί δύο μέθοδοι.

Η πρώτη μέθοδος είναι η μεταγλώττιση και μεταφόρτωση των contracts πριν την παραγωγή του πακέτου λογισμικού της υπηρεσίας για τελική χρήση (production build). Με αυτό τον τρόπο η υπηρεσία θα έχει πρόσβαση στα artifacts μέσω της βιβλιοθήκης που παράγεται από το άρθρωμα concordia-contracts. Αυτή η μέθοδος έχει το μειονέκτημα ότι το τελικό πακέτο λογισμικού (production build) “δένεται” με όποια συγκεκριμένη έκδοση των contracts είναι διαθέσιμη κατά τη δημιουργία του πακέτου. Αυτό σημαίνει ότι σε ενδεχόμενη ενημέρωση των contracts πρέπει αναγκαστικά να δημιουργηθεί και νέα έκδοση του πακέτου λογισμικού της υπηρεσίας Concordia Application.

Για την αποφυγή του παραπάνω προβλήματος αναπτύχθηκε η δεύτερη μέθοδος προσκόμισης των contract artifacts, η οποία είναι η λήψη τους (download) από μία άλλη τοποθεσία στο διαδίκτυο. Σε αυτή τη μέθοδο, η εφαρμογή κατά την εκκίνησή της πραγματοποιεί ένα HTTP αίτημα (HTTP request) σε διεύθυνση η οποία δίνεται ως μεταβλητή περιβάλλοντος (environment variable). Η απάντηση του αιτήματος αναμένεται να περιέχει τα artifacts ώστε η εφαρμογή να τα χρησιμοποιήσει.

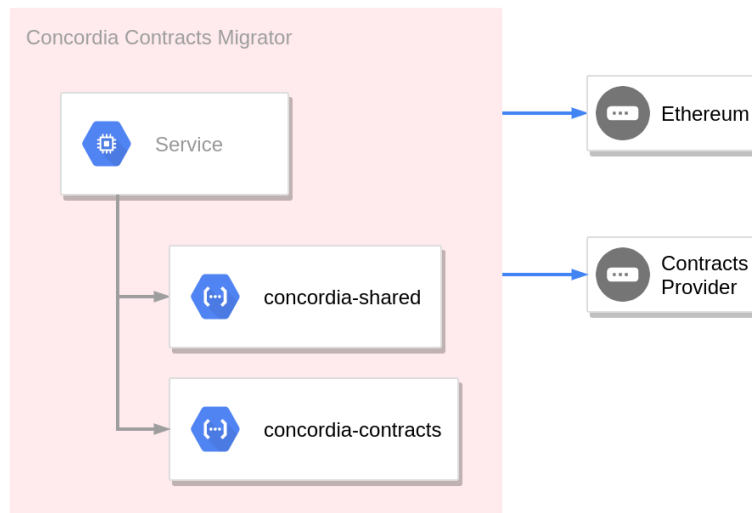
Διανομή

Η υπηρεσία Concordia Application πακετάρεται μαζί με τον διακομιστή nginx και γίνεται διαθέσιμη για χρήση ως εικόνα docker (docker image) μέσω του αποθετηρίου εικόνων dockerhub. Κατά την εκτέλεση της εικόνας οι χρήστες μπορούν μέσω μεταβλητών περιβάλλοντος να ορίσουν παραμέτρους της εκτέλεσης όπως η διεύθυνση του εξυπηρετητή (host location) της εφαρμογής και οι τοποθεσίες των υπηρεσιών Rendezvous Server και Contracts Provider.

4.4.3 Concordia Contracts Migrator

Περιγραφή - Στόχοι υπηρεσίας

Η υπηρεσία αυτή αποτελείται από ένα εκτελέσιμο πρόγραμμα γραμμής εντολών βασισμένο στο άρθρωμα concordia-contracts που αναλύθηκε σε προηγούμενη υποενότητα (4.4.1). Το πρόγραμμα, κατά την εκτέλεσή του, μεταγλωττίζει τα contracts και έπειτα τα μεταφορτώνει στο blockchain το οποίο είναι ορισμένο με χρήση μεταβλητών περιβάλλοντος. Τέλος, αν οι κατάλληλες μεταβλητές περιβάλλοντος είναι ορισμένες, το πρόγραμμα μεταφορτώνει τα τελικά artifacts σε αποθετήριο Concordia Contracts Provider. Η αρχιτεκτονική της υπηρεσίας φαίνεται στο παρακάτω σχήμα (σχήμα 4.5).



Σχήμα 4.5: Αρχιτεκτονική υπηρεσίας Concordia Contracts Migrator

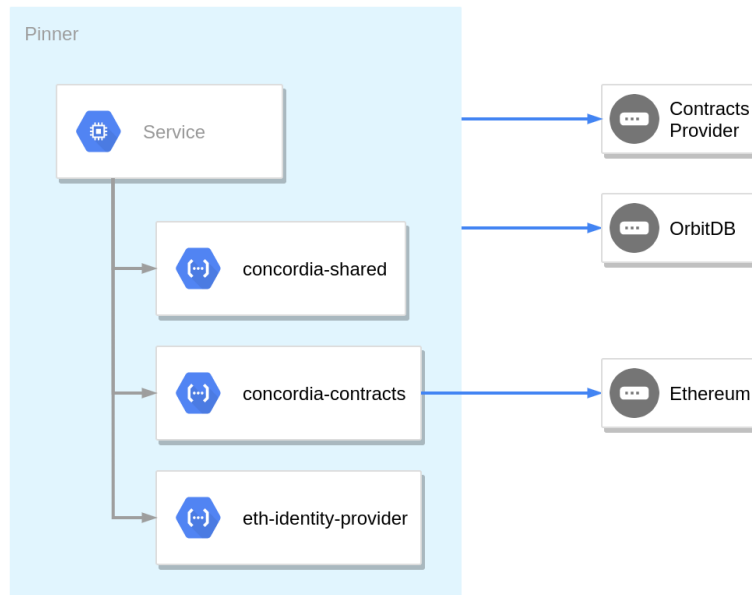
Διανομή

Η υπηρεσία αυτή γίνεται διαθέσιμη για χρήση ως docker image μέσω του αποθετηρίου εικόνων dockerhub. Οι χρήστες μπορούν χρησιμοποιώντας μεταβλητές περιβάλλοντος να αλλάξουν τη διεύθυνση του blockchain και την τοποθεσία της υπηρεσίας Contracts Provider στην οποία το πρόγραμμα θα μεταφορτώσει τα contracts και τα artifacts.

4.4.4 Concordia Pinner

Περιγραφή - Στόχοι υπηρεσίας

Η υπηρεσία καρφίτσωματος περιεχομένου (Concordia Pinner) αποτελεί μία εφαρμογή τερματικού (terminal application/cmd application) η οποία στοχεύει στο καρφίτσωμα (pinning) του περιεχομένου που αποθηκεύεται στο IPFS μέσω της βάσης OrbitDB. Η υπηρεσία είναι γραμμένη στη γλώσσα προγραμματισμού Javascript. Η αρχιτεκτονική της υπηρεσίας φαίνεται το σχήμα 4.6.



Σχήμα 4.6: Αρχιτεκτονική υπηρεσίας Concordia Pinner

Η υπηρεσία αυτή υλοποιήθηκε για να εγγυηθεί η διαθεσιμότητα του περιεχομένου του συστήματος που αποθηκεύεται στο IPFS (τίτλοι θεμάτων, περιεχόμενο μηνυμάτων και άλλα). Λόγω του τρόπου λειτουργίας του IPFS, το περιεχόμενο που αναρτούν οι χρήστες πρέπει να καρφιτσώνεται από άλλους χρήστες ή αυτόνομες εφαρμογές, όπως η υπηρεσία Concordia Pinner, ώστε να είναι διαθέσιμο. Αν το περιεχόμενο δεν καρφιτσωθεί, τότε θα είναι διαθέσιμο στους υπόλοιπους χρήστες μόνο από τον/τη δημιουργό, έτσι αν αυτός/αυτή δεν είναι ενεργός/ενεργή στο δίκτυο, το περιεχόμενο θα είναι αδύνατο να βρεθεί.

Η υπηρεσία συνδέεται στο blockchain από όπου παρακολουθεί την κατάσταση του συστήματος και “ακούει” για νέους χρήστες, θέματα και μηνύματα. Η υπηρεσία συνδέεται επίσης στο IPFS, έτσι όταν δημιουργηθεί νέο περιεχόμενο στο σύστημα το καρφιτσώνει αυτόματα. Με αυτό τον τρόπο, διατηρώντας την υπηρεσία πάντα διαθέσιμη, για παράδειγμα εκτελώντας τη σε περιβάλλον διακομιστή (server), διαβεβαιώνεται η διαθεσιμότητα του περιεχομένου.

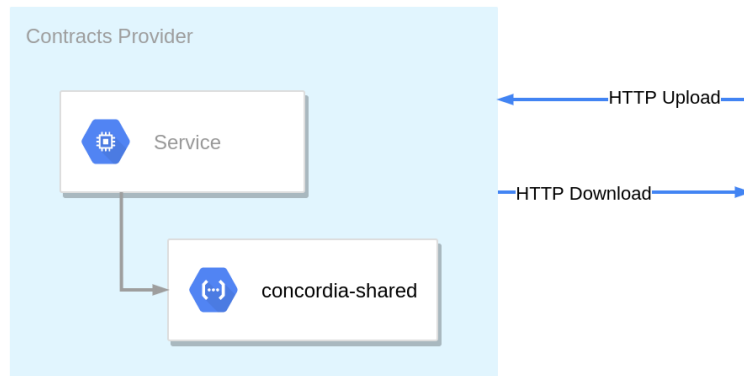
Διανομή

Η υπηρεσία αυτή γίνεται διαθέσιμη για χρήση ως docker image μέσω του αποθετηρίου εικόνων dockerhub. Κατά την εκτέλεση της εικόνας οι χρήστες μπορούν μέσω μεταβλητών περιβάλλοντος να ορίσουν παραμέτρους της υπηρεσίας όπως τη διεύθυνση του εξυπηρετητή (host location), τη διεύθυνση του blockchain, τις διαδρομές αποθήκευσης των δεδομένων στο σύστημα και τις τοποθεσίες των υπηρεσιών Rendezvous Server και Contracts Provider.

4.4.5 Concordia Contracts Provider

Περιγραφή - Στόχοι υπηρεσίας

Η υπηρεσία Contracts Provider αποτελεί μία βοηθητική υπηρεσία η οποία υλοποιεί ένα απλό αποθετήριο για τα contract artifacts. Είναι γραμμένη σε Javascript και διαθέτει δύο HTTP endpoints, ένα για τη μεταφόρτωση (upload) των artifacts προς την υπηρεσία και ένα για τη λήψη (download) από την υπηρεσία. Η υπηρεσία υποστηρίζει επίσης την επισύναψη ετικετών στα artifacts, όπως η έκδοση (version) ή το κλαδί ανάπτυξης (branch, για παράδειγμα master/develop). Η αρχιτεκτονική της υπηρεσίας φαίνεται το σχήμα 4.7.



Σχήμα 4.7: Αρχιτεκτονική υπηρεσίας Concordia Contracts Provider

Η υπηρεσία χρησιμοποιείται σε μία προσπάθεια αποσύνδεσης της βασικής εφαρμογής που υλοποιεί η υπηρεσία Concordia Application από μία συγκεκριμένη έκδοση των contracts. Οι λόγοι που αυτό είναι επιθυμητό αναπτύχθηκαν στην περιγραφή της υπηρεσίας Concordia Application (υποενότητα 4.4.2). Ωστόσο, η υπηρεσία Contracts Provider αποτελεί σημείο κεντροποίησης του συστήματος, για το λόγο αυτό θεωρείται προσωρινή λύση η οποία θα μπορούσε να αντικατασταθεί από αποκεντρωτικές λύσεις όπως η μεταφόρτωση των artifacts στο IPFS και ο διαμοιρασμός τους από εκεί.

Διανομή

Η υπηρεσία αυτή γίνεται διαθέσιμη για χρήση ως docker image μέσω του αποθετηρίου εικόνων dockerhub. Οι χρήστες μπορούν χρησιμοποιώντας μεταβλητές περιβάλλοντος να αλλάξουν παραμέτρους της εκτέλεσης όπως η διαδρομή αποθήκευσης των μεταφορτωμένων contract artifacts.

4.4.6 Ganache

Περιγραφή - Στόχοι υπηρεσίας

Η υπηρεσία Ganache αποτελεί μία εφαρμογή τερματικού η οποία είναι μέρος της δωρεάν σουίτας ανοιχτού λογισμικού Truffle. Η εφαρμογή δημιουργεί ένα τοπικό, ιδιωτικό blockchain το οποίο ακολουθεί το πρότυπο του Ethereum. Επίσης, η εφαρμογή δρα ως minner στο δίκτυο, διεκπεραιώνοντας όλες τις συναλλαγές.

Διανομή

Για τη χρήση της υπηρεσίας αυτής αναπτύχθηκε μία νέα εικόνα docker που βασίζεται στην επίσημη εικόνα που διατίθεται από τη σουίτα και προσθέτει μερικές χρήσιμες λειτουργικότητες όπως η δυνατότητα αποκάλυψης των κλειδιών που δημιουργούνται κατά την εκτέλεση. Η υπηρεσία γίνεται διαθέσιμη για χρήση ως docker image μέσω του αποθετηρίου εικόνων dockerhub. Η εικόνα παρέχει τη δυνατότητα τροποποίησης των παραμέτρων εκτέλεσης με χρήση μεταβλητών περιβάλλοντος. Με αυτό τον τρόπο οι χρήστες μπορούν να αλλάξουν τον αριθμό των λογαριασμών που θα δημιουργηθούν, το ποσό του Ether που θα λάβει κάθε λογαριασμός καθώς και άλλες μεταβλητές.

4.4.7 Rendezvous Server

Περιγραφή - Στόχοι υπηρεσίας

Η υπηρεσία Rendezvous Server αποτελεί δωρεάν λογισμικό ανοιχτού κώδικα το οποίο χρησιμοποιήθηκε (αλλά δεν αναπτύχθηκε) στα πλαίσια της διπλωματικής και υλοποιεί το πρωτόκολλο rendezvous για την εύρεση ομότιμων χρηστών (peers). Η υπηρεσία είναι απαραίτητη για τη λειτουργία του IPFS, ώστε οι ομότιμοι χρήστες (peers) να μπορούν να ανακαλύψουν τις διευθύνσεις των υπόλοιπων χρηστών του δικτύου.

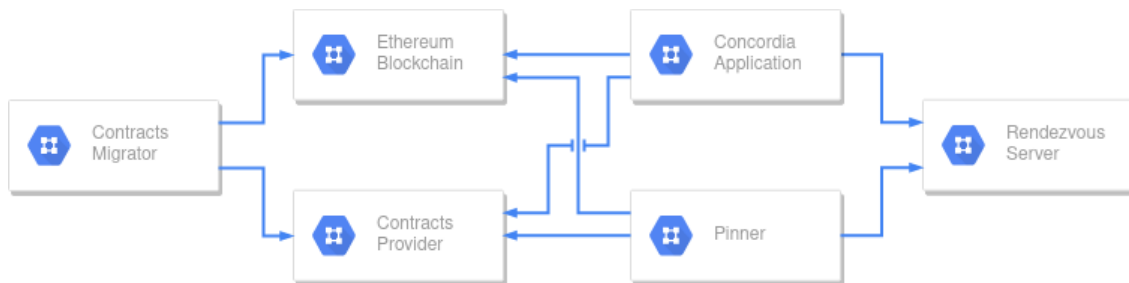
Διανομή

Η υπηρεσία αυτή είναι διαθέσιμη για χρήση από τους δημιουργούς της τόσο ως εφαρμογή μέσω του αποθετηρίου λογισμικού npm αλλά και ως docker image μέσω του αποθετηρίου εικόνων dockerhub.

4.4.8 Διασύνδεση υπηρεσιών

Στο μοντέλο των μικροϋπηρεσιών, βασικό χαρακτηριστικό είναι η επικοινωνία των ξεχωριστών υπηρεσιών και η ανταλλαγή μηνυμάτων για την επίτευξη των λειτουργικοτήτων του συστήματος. Σε αυτήν την υποενότητα θα αναλυθεί ο τρόπος με τον οποίο οι μικροϋπηρεσίες επικοινωνούν μεταξύ τους καθώς και η φύση και το περιεχόμενο των μηνυμάτων που ανταλλάσσουν.

Στο παρακάτω σχήμα (σχήμα 4.8) φαίνεται ο γράφος που οπτικοποιεί τα κανάλια επικοινωνίας μεταξύ των μικροϋπηρεσιών, καθώς και τα κανάλια επικοινωνίας των μικροϋπηρεσιών με το blockchain.



Σχήμα 4.8: Γράφος οπτικοποίησης των καναλιών επικοινωνίας των μικροϋπηρεσιών

Εδώ αναλύεται η επικοινωνία κάθε μικροϋπηρεσίας:

- **Contracts Migrator:** η υπηρεσία εκτελεί αίτημα HTTP κατά την μεταφόρτωση των contracts στο Ethereum blockchain, επίσης εκτελεί αίτημα HTTP για την μεταφόρτωση των contract artifacts στην υπηρεσία Contracts Provider
- **Concordia Application:** η υπηρεσία εκτελεί αίτημα HTTP για την λήψη των contract artifacts από την υπηρεσία Contracts Provider, εκτελεί αιτήματα HTTP για την διενέργεια συναλλαγών στο Ethereum blockchain και τέλος δημιουργεί κανάλι UDP επικοινωνίας με την υπηρεσία Rendezvous Server για την ανακάλυψη ομότιμων χρηστών (peers) στο δίκτυο IPFS
- **Pinner:** η υπηρεσία εκτελεί αίτημα HTTP για την λήψη των contract artifacts από την υπηρεσία Contracts Provider, εκτελεί αιτήματα HTTP για την ανανέωση και παρατήρηση

της κατάστασης του contract στο Ethereum blockchain και τέλος δημιουργεί κανάλι UDP επικοινωνίας με την υπηρεσία Rendezvous Server για την ανακάλυψη peers στο δίκτυο IPFS

- **Rendezvous Server:** η υπηρεσία διατηρεί ανοιχτά κανάλια UDP επικοινωνίας με τους ομότιμους χρήστες μέσω των οποίων ενημερώνει την λίστα των διαθέσιμων, ενεργών χρηστών
- **Contracts Provider:** η υπηρεσία δεν υποκινεί καμία επικοινωνία παρά μόνο απαντά σε αιτήματα επικοινωνία από άλλες υπηρεσίες

4.4.9 Ροή πληροφορίας

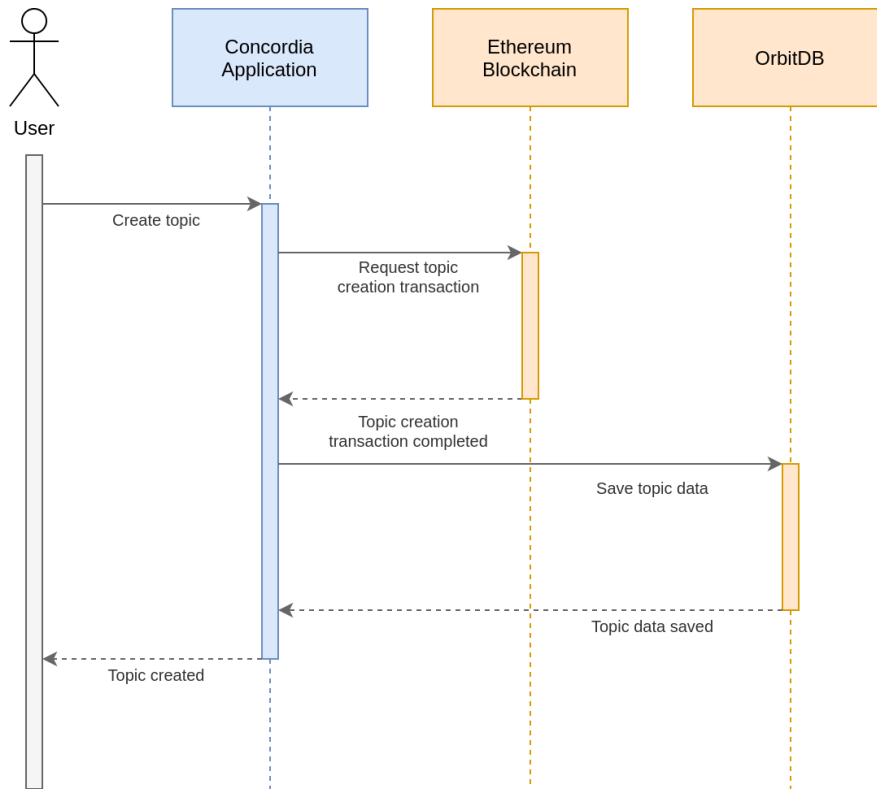
Στην παρούσα υποενότητα θα αναλυθεί η ροή της πληροφορίας στο σύστημα. Λόγω των πολλαπλών υπηρεσιών, της κατάτμησης της πληροφορίας και των διαφορετικών σημείων αποθήκευσης της, η ροή της πληροφορίας στο σύστημα ακολουθεί ένα σχετικά περίπλοκο μονοπάτι (σε σχέση με κλασσικές, μονολιθικές, κεντροποιημένες εφαρμογές).

Αρχικά θα γίνει αναφορά στη διαδικασία αποθήκευσης των νέων πληροφοριών. Η μοναδική πηγή παραγωγής δεδομένων στο σύστημα είναι οι χρήστες και κατ' επέκταση η υπηρεσία Concordia Application, εφόσον είναι η μοναδική υπηρεσία με την οποία αυτοί αλληλεπιδρούν. Τα δεδομένα που δημιουργούν οι χρήστες (πληροφορίες χρηστών, τίτλοι θεμάτων και περιεχόμενο μηνυμάτων) κατατμήζονται πριν αποθηκευτούν. Η πληροφορία που εισάγεται στο σύστημα κατατμήζεται σε δύο μέρη. Στο blockchain αποθηκεύεται ένας δείκτης προς τα δεδομένα, ενώ τα πραγματικά δεδομένα αποθηκεύονται στη βάση OrbitDB. Ο δείκτης εκτός από την άμεση χρησιμότητα στην εύρεση των δεδομένων, παρέχει και την έμμεση λειτουργικότητα της δημιουργίας απαραίτητων μεταδομένων όπως ο αριθμός των θεμάτων στο σύστημα ή των μηνυμάτων σε ένα θέμα.

Από την πλευρά της εύρεσης των πληροφοριών στο σύστημα, η ροή είναι ως εξής. Αρχικά, είναι απαραίτητη η αναζήτηση στο blockchain για την εύρεση του δείκτη προς τα δεδομένα. Έπειτα, τα δεδομένα μπορούν να ανακτηθούν μέσω του IPFS από τον εκάστοτε χρήστη ή από κάποιον Pinner.

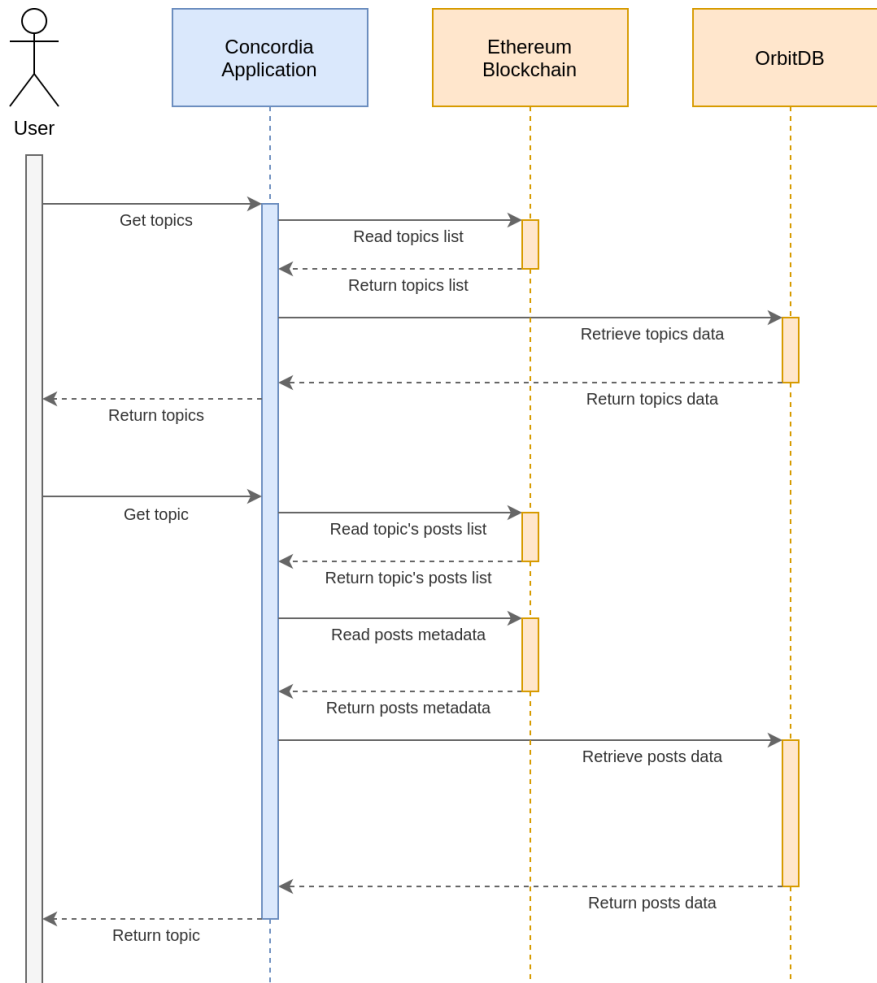
Τέλος, παρακάτω δίνεται ένα παράδειγμα εισαγωγής πληροφορίας στο σύστημα και έπειτα ανάκτησης της ίδιας πληροφορίας.

Έστω, χρήστης που δημιουργεί νέο θέμα. Τα δεδομένα που παράγονται είναι ο τίτλος του θέματος και το περιεχόμενο του πρώτου μηνύματος. Μεταδεδομένα της δημιουργίας είναι η διεύθυνση του/της δημιουργού του θέματος. Για την αποθήκευση του θέματος στο σύστημα δημιουργείται πρώτα συναλλαγή στο blockchain ώστε να δημιουργηθεί μία νέα εγγραφή στον πίνακα των θεμάτων. Η εγγραφή αυτή δεν περιέχει τίποτα παρά μόνο τη διεύθυνση του/της δημιουργού χρήστη. Αν η συναλλαγή είναι επιτυχής, θα επιστραφεί ο αύξων αριθμός του νέου θέματος. Έπειτα, στην προσωπική βάση OrbitDB του/της χρήστη και στον πίνακα των θεμάτων θα προστεθεί εγγραφή με αναγνωριστικό τον αύξων αριθμό του θέματος όπου θα αποθηκευτούν τα δεδομένα του τίτλου και πρώτου μηνύματος. Στο σχήμα 4.9 παρουσιάζεται γραφικά η διαδικασία.



Σχήμα 4.9: Διάγραμμα ακολουθίας δημιουργίας θέματος

Έστω, χρήστης που επιθυμεί να διαβάσει το προηγούμενο μήνυμα. Αρχικά, πρέπει να διαβαστεί ο πίνακας θεμάτων από το blockchain. Η πληροφορία αυτή εμπλουτίζεται από τα δεδομένα του κάθε θέματος, τα οποία ανακτώνται από τις προσωπικές βάσεις Orbit κάθε χρήστη. Έπειτα, εφόσον το θέμα βρεθεί και ο αύξων αριθμός του είναι γνωστός, πρέπει να διαβαστούν από το blockchain τα μεταδομένα των μηνυμάτων του θέματος και συγκεκριμένα η διευθύνσεις των δημιουργών τους. Τέλος, μέσω του IPFS πρέπει να γίνει αντιγραφή των προσωπικών βάσεων των δημιουργών του κάθε μηνύματος και να αναζητηθούν σε αυτές τα εκάστοτε μηνύματα. Στο σχήμα 4.10 φαίνεται το διάγραμμα ροής της πληροφορίας κατά την ανάκτηση πληροφοριών από το σύστημα.



Σχήμα 4.10: Διάγραμμα ακολουθίας εύρεσης και ανάκτησης θέματος

Κεφάλαιο 5

Συμπεράσματα

5.1 Προβλήματα ανάπτυξης

5.2 Διαφορές σχεδιασμού-υλοποίησης

5.3 Ανοιχτά θέματα

TODO: add 1. feeless 2. reputation system 3. voting types 4. token distribution 5. ethereum, ipfs, move to proof of stake, remove of rendezvous server

5.4 Επίλογος

Βιβλιογραφία

- [1] *Μάθετε για το Ethereum*. URL: <https://ethereum.org/el/learn/> (επίσκεψη 16/03/2021).
- [2] Vitalik Buterin. *The Meaning of Decentralization*. 6 Φεβ. 2017. URL: <https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274>.
- [3] A. Aneesh. *Virtual Migration*. 2006.
- [4] Don Johnson, Alfred Menezes και Scott Vanstone. «The Elliptic Curve Digital Signature Algorithm (ECDSA)». Στο: *International Journal of Information Security* (Αύγ. 2001). DOI: 10.1007/s102070100002. URL: <https://doi.org/10.1007/s102070100002>.
- [5] Wikipedia. *Merkle tree*. URL: https://en.wikipedia.org/wiki/Merkle_tree.
- [6] Belavadi Prahalad. *Merkle proofs Explained*. 7 Ιαν. 2018. URL: <https://medium.com/crypto-0-nite/merkle-proofs-explained-6dd429623dc5>.
- [7] R. Schollmeier. «A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications». Στο: *Proceedings First International Conference on Peer-to-Peer Computing*. 2001, σσ. 101–102. DOI: 10.1109/P2P.2001.990434.
- [8] Satoshi Nakamoto. «Bitcoin: A Peer-to-Peer Electronic Cash System». Στο: *Cryptography Mailing list at https://metzdowd.com* (31 Οκτ. 2008).
- [9] Wikipedia. *Blockchain*. URL: <https://en.wikipedia.org/wiki/Blockchain>.
- [10] Vitalik Buterin. *Ethereum Whitepaper*. 2013. URL: <https://ethereum.org/en/whitepaper> (επίσκεψη 28/06/2021).
- [11] Ethereum community. *Ethereum documentation*. URL: <https://ethereum.org/en/developers/docs/> (επίσκεψη 05/09/2021).
- [12] Nick Szabo. «Formalizing and Securing Relationships on Public Networks». Στο: *First Monday* 2.9 (Σεπτ. 1997). DOI: 10.5210/fm.v2i9.548. URL: <https://journals.uic.edu/ojs/index.php/fm/article/view/548>.
- [13] Gavin Wood Andreas M Antonopoulos. *Mastering Ethereum: Building Smart Contracts and DApps*. O'Reilly Media, 2018. ISBN: 1491971940.
- [14] *IPFS*. URL: <https://ipfs.io/>.
- [15] *IPFS documentation*. URL: <https://docs.ipfs.io/>.
- [16] ProtoSchool. *Merkle DAGs: Structuring Data for the Distributed Web*. URL: <https://proto.school/merkle-dags/>.
- [17] GitHub Guides. *Understanding the GitHub flow*. URL: <https://guides.github.com/introduction/flow/>.
- [18] *OrbitDB*. URL: <https://orbitdb.org>.

[19] *Getting Started with OrbitDB*. URL: <https://github.com/orbitdb/orbit-db/blob/main/GUIDE.md>.