Αυτόνομο αμεσοδημοκρατικό κοινωνικό δίκτυο βασισμένο σε τεχνολογίες αποκέντρωσης

Νικολαΐδης Παναγιώτης[1] και Φανάκης Απόστολος[2]

[1]nkpanagi@auth.gr, 7491
[2]apostolof@auth.gr, 8261

Επιβλέπων Χρήστος Ε. Δημάκης

Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Πολυτεχνική Σχολή

Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης

Θεσσαλονίκη 2021

Some text and the a cite[**einstein**].
And another cite[**latexcompanion**].
This is a list:

- item 1
- item 2
- item 3

This is some vertical space

This is a numbered list:

α) asdf

β) fdas

1

```
This is monospace
```

[1]Here is a footnote

Decentralized και τα σχετικά.
Don't forget the keywords.

Ευχαριστούμε η Αθήνα. Ευχαριστούμε η Ελλάδα.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

1.1 Γενικά

1.2 Ορισμός του προβλήματος

Στις μέρες μας τα περισσότερα δεδομένα των χρηστών βρίσκονται υπό τον έλεγχο συγκεντρωτικών συστημάτων. Σε τέτοια συστήματα οι χρήστες δεν είναι κύριοι των δεδομένων τους, δεν έχουν εγγύηση για την αυθεντικότητα αυτών που βλέπουν και υπόκεινται σε λογοκρισία, ενώ τα συστήματα αυτά δεν είναι ασφαλή και μπορεί να σταματήσουν να λειτουργούν προσωρινά ή μόνιμα για τεχνικούς/οικονομικούς/νομικούς λόγους.

Οι περισσότερες διαδεδομένες, συγκεντρωτικές μορφές πλατφόρμας επικοινωνίας (mailing list, forum, κοινωνικά δίκτυα και άλλες) χρειάζονται, τυπικά, τουλάχιστον τις εξής τεχνολογίες:

- μία πηγή επεξεργαστικής ισχύος (processing)
- μία βάση δεδομένων
- ένα πρωτόκολλο επικοινωνίας

Η επεξεργαστική ισχύς είναι αναγκαία για την περάτωση των λειτουργιών οι οποίες υλοποιούν τις υπηρεσίες της πλατφόρμας. Τις περισσότερες φορές η πηγή αυτή είναι ένας server ή μία cloud υπηρεσία.

Η βάση δεδομένων είναι απαραίτητη για την αποθήκευση της πληροφορίας. Σε μικρότερες εφαρμογές η βάση βρίσκεται στο ίδιο σύστημα που γίνεται και το processing, ενώ σε μεγαλύτερες ενδέχεται να υπάρχει για λόγους ασφάλειας ένα ξεχωριστό σύστημα αφιερωμένο στη βάση δεδομένων.

Το πρωτόκολλο επικοινωνίας αναλαμβάνει τη μετάδοση και ανάκτηση της πληροφορίας. Το πρωτόκολλό που χρησιμοποιείται σήμερα στη συντριπτική πλοιοψηφία των εφαρμογών είναι το HTTP.

Κάθε ένα από τα παραπάνω μέρη, εισάγει την ανάγκη ύπαρξης κεντρικών αρχών που τα διαχειρίζονται και τα συντηρούν. Η αρχή αυτή είναι συνήθως ο πάροχος της υπηρεσίας που διαχειρίζεται το processing και τη βάση δεδομένων, έχοντας έτσι πρόσβαση σε όλα τα δεδομένα που υπάρχουν στο σύστημα.

1.3 Προτεινόμενη λύση

Το Concordia είναι η εφαρμογή η οποία αναπτύσσουμε εμείς και στοχεύει να διορθώσει αυτά τα προβλήματα, επαναφέροντας στους χρήστες την κυριότητα των δεδομένων τους, εξασφαλίζοντας την πλήρη ελευθερία του λόγου και την αυθεντικότητα, ανοίγοντας τον δρόμο για αξιόπιστες ψηφοφορίες Όλα αυτά μέσα από δημόσιες, αποκεντρωτικές διαδικασίες.

1.3.1 Απαιτήσεις

1.3.2 Αποκέντρωση

Αποκέντρωση του συστήματος σημαίνει πρακτικά ότι το processing και η αποθήκευση των δεδομένων δε θα γίνονται από κάποια κεντρική αρχή αλλά θα είναι κατανεμημένα στο σύνολο των χρηστών (nodes). Με αυτόν τον τρόπο δεν υπάρχει ανάγκη για μία κεντρική αρχή και τα δεδομένα δεν είναι ελέγξιμα από κανέναν ατομικά, παρά μόνο από τη συναίνεση (consensus) του δικτύου.

Τα συγκεντρωτικά συστήματα έχουν μερικά θετικά χαρακτηριστικά που λείπουν από τα αποκεντρωτικά συστήματα, όπως ευκολία ανάπτυξης, συντήρησης και αποσφαλμάτωσης των εφαρμογών. Πάσχουν ωστόσο σε ό,τι αφορά την σταθερότητα, την ασφάλεια, την επεκτασιμότητα και την εξέλιξη, τομείς όπου τα αποκεντρωτικά συστήματα είναι ιδιαίτερα αποτελεσματικά.

Η ανάγκη για αποκέντρωση των εφαρμογών, ειδικά στην επικοινωνία, είναι μεγάλη και πηγάζει από την ανάγκη για ελευθερία του λόγου, ανωνυμία και ιδιωτικότητα. Χρησιμοποιώντας τεχνικές για κατανομή του processing, μία διανεμημένη βάση δεδομένων και αλγόριθμους κρυπτογραφίας δημόσιου κλειδιού μπορούμε να προστατεύσουμε την ανωνυμία του χρήστη αλλά και να εγγυηθούμε την ταυτοποίησή του.

1.3.3 Αμεσοδημοκρατικές διαδικασίες και αυτοδιαχείριση

Για την πλήρη επίτευξη του στόχου απαιτείται επίσης ένα σύστημα διαχείρισης της πλατφόρμας αυτής καθ' αυτής αλλά και των περιεχομένων της. Το σύστημα που επιλέγουμε για αυτούς τους σκοπούς είναι αυτό της άμεσης δημοκρατίας και αυτοδιαχείρισης. Αυτό σημαίνει ότι οι αποφάσεις θα παίρνονται μέσα από ψηφοφορίες στις οποίες θα μπορούν να συμμετέχουν όσα μέλη έχουν δικαίωμα ψήφου. Έτσι, λόγω της αποκέντρωσης και άρα της έλλειψης διοικούσας αρχής, η πλατφόρμα μπορεί να χρησιμοποιηθεί σαν μία εγγυημένα αμερόληπτη αρχή για ψηφοφορίες πάνω σε θέματα που αφορούν τη φοιτητική ζωή και όχι μόνο.

1.4 Στόχος

Στόχος του project είναι η δημιουργία μιας κοινωνικής πλατφόρμας, η οποία, βασιζόμενη σε τεχνολογίες αποκέντρωσης, αφενός θα παρέχει ελευθερία λόγου, εργαλεία αυτοδιαχείρισης και αμεσοδημοκρατικές διαδικασίες, αφετέρου θα διασφαλίζει την κυριότητα των δεδομένων του χρήστη από τον ίδιο και την ανεξαρτητοποίηση του συστήματος από κεντρικές οντότητες. Παράλληλα, θα παρέχει στους επαληθευμένους χρήστες του ΑΠΘ μια πλατφόρμα για ανώνυμες και αυθεντικές ψηφοφορίες, εν δυνάμει ικανών να αποτελέσουν ένα έγκυρο, έμπιστο και άμεσα δημοκρατικό βήμα λήψης αποφάσεων.

1.5 Μεθοδολογία ανάπτυξης

Για την επίτευξη των στόχων που ορίστηκαν και την οργάνωση της απαραίτητης δουλειάς 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 σύχρονη 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 αναπτύσει 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 σχεδιάστηκε η χρήση του μοντέλου που έχει αναπτυχθεί από την εταιρία Github, Flow. Το μοντέλο αυτό ορίζει ότι κάθε προγραμματιστής θα ανοίγει ένα νέο branch για τη ανάπτυξη ενός νέου χαρακτηριστικού της εφαρμογής ή την 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/η επιμελητής/επιμελήτρια 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 διακρούς επικοινωνίας με τα υπόλοιπα μέλη. Οι στόχοι είναι ορισμένοι, σαφής και χωρισμένοι σε διαχειρίσιμα μέρη τα οποία δεν καταβάλουν τα μέλη. Ταυτόχρονα, έχοντας ως έδρα καθιερομένα πρότυπα ανάπτυξης, παρέχεται φορμαλισμός και έτοιμες μέθοδοι επίλυσης προβλημάτων, γεγονός που λειτουργεί καταλυτικά και βοηθά στην αποφυγεί τελμάτων κατά τη συγγραφή του κώδικα.

1.6 Οργάνωση κεφαλαίων

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.

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:

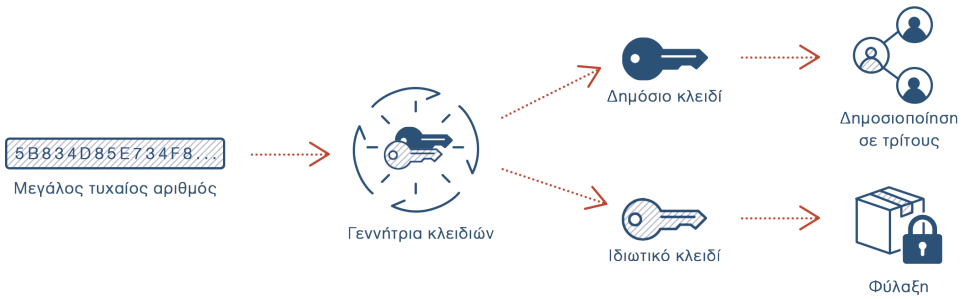
- Είναι ντετερμινιστική, δηλαδή η ίδια είσοδος παράγει πάντα την ίδια έξοδο.
- Είναι μη αντιστρέψιμη, δηλαδή είναι πρακτικά ανέφικτο να υπολογιστεί η είσοδος δεδομένης μιας εξόδου.
- Είναι αμφιμονοσήμαντη (1-1), δηλαδή σε δύο διαφορετικές εισόδους αντιστοιχούν πάντα δύο εντελώς διαφορετικές έξοδοι.
-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

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 2.1: Παραγωγή ασύμμετρου ζεύγους κλειδιών

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

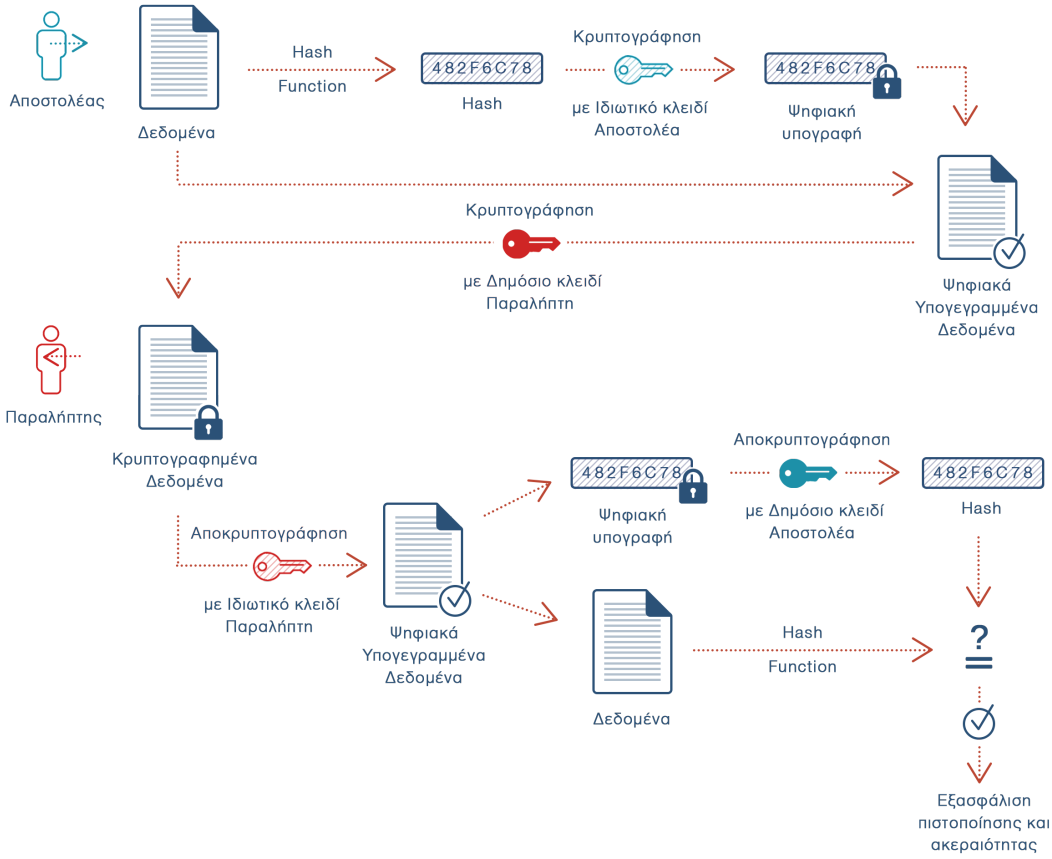
α) Για να αποκρυπτογραφήσει μηνύματα άλλων χρηστών, οι οποίοι τα κρυπτογράφησαν χρησιμοποιώντας το δημόσιο κλειδί του. Με αυτόν τον τρόπο εξασφαλίζεται η *εμπιστευτικότητα* (confidentiality).

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 2.2: Κρυπτογράφηση απ' άκρη σ' άκρη

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 το λεγόμενο root hash.

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.

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 σύνολου, χωρίς να χρειαστεί να αποκαλυφθεί το περιεχόμενο οποιουδήποτε εκ των δύο.

2.4 Δίκτυα Ομότιμων Κόμβων

Τα δίκτυα ομότιμων κόμβων ή Peer-to-Peer (P2P) networks αποτελούν μία κατανεμημένη αρχιτεκτονική δικτύων, οι συμμετέχοντες (κόμβοι) της οποίας μοιράζονται ένα τμήμα των πόρων τους, με στόχο την παροχή κάποιας υπηρεσίας (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.

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.

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).[]

Ως προς την κυριότητα επί αυτού, το blockchain συνήθως* 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.

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.

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

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.

2.6 Ethereum

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).

Με απλά λόγια, τα smart contracts αποτελούν αυτόνομα κομμάτια κώδικα τα οποία είναι αποθηκευμένα στο blockchain και ενεργοποιούνται μέσω συναλλαγών. Μπορούν να διαβάζουν και να γράφουν δεδομένα επί του blockchain, κληρονομώντας ιδιότητες όπως τη διαφάνεια (transparency), την εγκυρότητα (validability) και την αμεταβλητότητα (immutability).

Ένα παράδειγμα της καθημερινότητας που μπορεί να παρομοιασθεί λειτουργικά με smart contract είναι ο αυτόματος πωλητής . Ένας αυτόματος πωλητής ορίζεται ως ένα αυτόνομο μηχάνημα που διανέμει αγαθά ή παρέχει υπηρεσίες όταν εισάγονται σε αυτόν κέρματα ή κάποια ηλεκτρονική πληρωμή. 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 ποικίλων αποκεντρωμένων εφαρμογών. Οι εφαρμογές αυτές μπορούν να χωριστούν σε τρεις κατηγορίες:

- Οικονομικές εφαρμογές, οι οποίες παρέχοντας στους χρήστες ισχυρότερους τρόπους διαχείρισης και σύναψης συμβάσεων χρησιμοποιώντας τα χρήματά τους. Αυτό περιλαμβάνει υπο-νομίσματα, χρηματοοικονομικά παράγωγα, συμβάσεις αντιστάθμισης κινδύνου, πορτοφόλια αποταμίευσης, διαθήκες, και, τελικά, ακόμη και ορισμένες κατηγορίες συμβάσεων εργασίας πλήρους κλίμακας.

- 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).

- 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.

2.7 Αποκεντρωτική αποθήκευση δεδομένων (βάση δεδομένων)

Distributed databases - τι είναι; - ποιες είναι οι διαφορές από το blockchain; - γιατί τις χρειαζόμαστε; ποιο πρόβλημα λύνουν; - πόσες, ποιες υπάρχουν; παραδείγματα/διαφορές - τεχνική ανάλυση (προτερήματα, drawbacks)

Κεφάλαιο 3

Σχεδίαση εφαρμογής

3.1 Λογικά μέρη

Η πλατφόρμα μπορεί να διαχωριστεί σε δύο λογικά μέρη:

1) Το πρώτο μέρος αποτελεί μία αυτοτελή και πλήρως αποκεντρωτική πλατφόρμα που στόχος της είναι να παρέχει τη δυνατότητα ελευθερίας λόγου απρόσβλητου σε λογοκρισία και διαγραφή από κεντρικές οντότητες εξουσίας. Στην ουσία εδώ θα μπορεί - σε μια απλοποιημένη εκδοχή - οποιοσδήποτε να δημιουργήσει topics ή να απαντήσει σε άλλα. Επεξεργαστικός πυρήνας θα είναι ένα smart contract το οποίο θα δέχεται από τους χρήστες transactions και θα τα εγγράφει στο Storage Layer:

Το μειονέκτημα αυτού του κομματιού είναι πως για να λειτουργήσει απαιτεί για κάθε transaction οι χρήστες να καταβάλουν κάποιο τέλος για τα fees. Αν και υπάρχουν σχέδια από την ομάδα ανάπτυξης του Ethereum για τη μείωσή τους στο μέλλον (έως και 10-2), τα fees στη χρήση της EVM θα είναι αναπόφευκτα. Ωστόσο θα πρέπει να σημειωθεί ότι αφενός παρέχουν μια μορφή προστασίας απέναντι σε κακόβουλους χρήστες που θα πλημμύριζαν την εφαρμογή με ανεπιθύμητο ποσοτικά/ποιοτικά περιεχόμενο (θα τους ήταν οικονομικά ασύμφορη μια τέτοια επίθεση), αφετέρου υπάρχουν κάποια workarounds για 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 (από οποιονδήποτε) με Ethereum ή οι χρήστες (βλ. κατηγορίες χρηστών) να καταβάλουν τα δικά τους έξοδα.

2) Το δεύτερο μέρος αποτελεί μια μερικώς αποκεντρωτική και μη αυτοτελή πλατφόρμα που έρχεται να λειτουργήσει επιπρόσθετα 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. Με λίγα λόγια, θα δημιουργούνται θέματα προς ψηφοφορία (στο πρώτο κομμάτι), πάνω στα οποία θα ψηφίζουν όσοι έχουν το δικαίωμα (αυτοί θα ορίζονται με την κατοχή ενός ανάλογου token στο Ethereum).

Ο χρήστης μέσω ενός Frontend (μιας κλασικής ιστοσελίδας ουσιαστικά) θα μπορεί να πιστοποιήσει μέσω login στο it.auth.gr* την ακαδημαϊκή του ταυτότητα. Στη συνέχεια το TDS (Token Distribution Service, ελέγχοντας το admin account των tokens θα παρέχει στο χρήστη δύο tokens. Ένα το οποίο θα του δίνει voting rights (verified user) και ένα που θα κάνει τη πλατφόρμα να του επιστρέφει τα τέλη τα οποία πληρώνουν σε κάθε post τους (trusted user).

*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 σημαίνει ότι οι χρήστες δε θα χρειάζεται να εμπιστευτούν τον UAS με τα it credential τους.

3.2 Κατηγορίες χρηστών

3.2.1 Πρώτο μέρος

Όπως προειπώθηκε, το πρώτο μέρος της πλατφόρμας θα είναι ανοιχτό σε όλους. Ωστόσο, οι χρήστες του μπορούν να διακριθούν στις εξής δύο κατηγορίες:

- Έμπιστα μέλη του δικτύου (trusted users)
- Μη έμπιστα μέλη (untrusted users)

Βασική διαφορά των δύο κατηγοριών είναι πως ενώ οι trusted users θα αποζημιώνονται αυτόματα από το (ενν. φορτισμένο) smart contract και άρα θα είναι απαλλαγμένοι από τέλη, οι δεύτεροι θα πρέπει να καταβάλουν μόνοι τους τα τέλη τους (fees) για κάθε ενέργεια (π.χ. posting).

Η εμπιστοσύνη ενός χρήστη (trust) μπορεί να οριστεί ως ένας ακέραιος αριθμός με κάποιο κατώφλι, πάνω από το οποίο ο χρήστης θα θεωρείται trusted. Το trust θα μπορεί να αυξομειώνεται ανά πάσα στιγμή, με τους χρήστες να δίνουν και να παίρνουν βαθμούς trust σε/από άλλους.

Αξίζει να σημειωθεί επίσης ότι επειδή όλες οι συναλλαγές καταγράφονται, είναι δυνατό να υπολογιστεί το συνολικό ποσό του Ethereum που έχει ξοδέψει ένας common user μέχρι να γίνει trusted και έτσι μπορεί σταδιακά να του επιστραφεί μέσω του contract. Αυτό δίνει κίνητρο στους χρήστες να διατηρούν σωστή συμπεριφορά και να συμβάλλουν θετικά στην πλατφόρμα.

3.2.2 Δεύτερο μέρος

Για το δεύτερο μέρος της πλατφόρμας, οι χρήστες του μπορούν να διακριθούν στις εξής κατηγορίες:

- Πιστοποιημένα μέλη του Α.Π.Θ. (verified users)
- Μη πιστοποιημένα μέλη του Α.Π.Θ. (untrusted users)

Σχετικά με το δικαίωμα ψήφου για αυθεντικές δημοκρατικές αποφάσεις σχετικές με το ΑΠΘ, αυτό θα το έχουν μόνο οι verified χρήστες του δικτύου. Οι verified χρήστες θα μπορούν επιπλέον να αλληλεπιδρούν με την πλατφόρμα εξαρχής χωρίς την καταβολή τελών (θα ξεκινάνε ως trusted), πράγμα που βέβαια δε σημαίνει ότι χάνοντας trust δε θα μπορούν να χάσουν αυτό το προνόμιο.

3.2.3 Σύνοψη χρηστών

Συμπερασματικά προκύπτουν τέσσερις διακριτές κατηγορίες χρηστών με ξεχωριστά δικαιώματα που φαίνονται στο παρακάτω διάγραμμα:

3.3 Σενάρια χρήσης

3.4 Τεχνολογίες

3.4.1 Ethereum

Ξεκινώντας την σχεδίαση της πλατφόρμας πραγματοποιήσαμε έρευνα ώστε να ανακαλύψουμε τις πιθανές επιλογές για το κομμάτι της διανεμημένης επεξεργασίας (distributed computing). Αναλογιστήκαμε τα προτερήματα και μειονεκτήματα διάφορων επιλογών, συμπεριλαμβανομένων των ...

Επιλέξαμε να προχωρήσουμε με το Ethereum και όχι κάποια άλλη πλατφόρμα επειδή ...

Το Ethereum είναι ... Παρέχει Smart Contracts ακολουθώντας το μοντέλο ... Proof of work είναι ... Ο τρόπος που υπολογίζεται και πληρώνεται η καταναλώμενη επεξεργαστική ισχύς είναι ... Αυτά εισάγουν τους εξής περιορισμούς που πρέπει να ληφθούν υπόψιν κατά την υλοποίηση ...

Προχωρώντας την τεχνολογία του blockchain ένα βήμα παραπέρα, ξεκίνησαν να δημιουργούνται προγραμματιστικές πλατφόρμες για την ανάπτυξη αποκεντρωτικών εφαρμογών (Decentralized Applications ή DApps). Η πρώτη και, μέχρι τώρα, πιο δημοφιλής, ισχυρή και λειτουργική πλατφόρμα είναι το Ethereum.

Στο Ethereum υπάρχουν δύο είδη λογαριασμών: οι Externally Owned Accounts και οι Contracts Accounts. Η διαφορά τους είναι ότι ενώ οι πρώτοι ελέγχονται από τους χρήστες, οι δεύτεροι διαθέτουν ένα αμετάβλητο (immutable) κομμάτι κώδικα το οποίο αποτελεί ένα Smart Contract. Όταν μια συναλλαγή σταλεί σε ένα Smart Contract, ο συσχετιζόμενος κώδικας εκτελείται από την "Ethereum Virtual Machine (EVM)" σε κάθε κόμβο (και εν τέλει όλοι έρχονται σε consensus). Φυσικά, για την εκτέλεση των operations στην EVM (όπως και για τα απλά transactions) χρειάζεται να δοθούν κάποια fees στους miners ως ανταμοιβή για την εργασία τους.

3.4.2 IPFS, OrbitDB

Όπως η επιλογή του Blockchain, που περιγράφηκε στο προηγούμενο κεφάλαιο (insert reference), ομοίως και η επιλογή του λογισμικού που θα χρησιμοποιηθεί για την κατανεμημένη αποθήκευση δεδομένων ξεκίνησε με μία έρευνα των επιλογών που υπάρχουν. Αναλογιστήκαμε τα προτερήματα και μειονεκτήματα διάφορων επιλογών, συμπεριλαμβανομένων των ...

Επιλέξαμε να προχωρήσουμε με το IPFS και την OrbitDB έναντι άλλων λύσεων επειδή ...

Το IPFS είναι ... Παρέχει ... με τον εξής τρόπο ... Δωρεάν ... Αυτά τα χαρακτηριστικά εισάγουν τους εξής περιορισμούς που πρέπει να ληφθούν υπόψιν κατά την υλοποίηση ...

Η OrbitDB είναι ... και χρησιμοποιεί το IPFS για να καταφέρει τα εξής χαρακτηριστικά ... Περιορισμοί πάλι κλπ ...

Ένα από τα προβλήματα που προκύπτουν με την αποκέντρωση εφαρμογών είναι αυτό της εύρεσης των resources που χρειαζόμαστε. Το πρόβλημα έγκειται στο γεγονός ότι δεν υπάρχει ένας server και άρα μία μοναδική διεύθυνση IP από την οποία μπορούμε να πάρουμε το αντικείμενο που ψάχνουμε, διότι όλα είναι διανεμημένα στο δίκτυο. Επιπλέον η αποθήκευση μεγάλου όγκου πληροφοριών στο Ethereum on-chain έχει απαγορευτικά μεγάλο κόστος οπότε απορρίπτεται.

Το πρόβλημα ανάγεται σε αυτό της επικοινωνίας μεταξύ των κόμβων. Αν καθοριστεί ένα πρότυπο επικοινωνίας μεταξύ των κόμβων τότε τα αντικείμενα μπορούν να βρεθούν ζητώντας τα από τους γειτονικούς κόμβους, οι οποίοι με τη σειρά τους θα τα ζητήσουν από τους δικούς τους γείτονες και ου το κάθε εξής, μέχρι το αντικείμενο να βρεθεί και να σταλεί στον κόμβο που αρχικά το ζήτησε.

Το IPFS είναι ένα νέο πρωτόκολλο μεταφοράς υπερκειμένου που βρίσκεται ακόμα υπό ανάπτυξη. Όπως το γνωστό πρωτόκολλο HTTP, για συγκεντρωτικά συστήματα, έτσι και το IPFS, για αποκεντρωτικά συστήματα, καθορίζει το πρότυπο το οποίο θα χρησιμοποιούν τα τερματικά του δικτύου για να επικοινωνούν μεταξύ τους. Χρησιμοποιεί κρυπτογραφικές τεχνικές, όπως αυτές που είδαμε παραπάνω, καθώς και διάφορες άλλες τεχνολογίες για να:

- συντονίσει τη παράδοση περιεχομένου
- υλοποιήσει στρώμα σύνδεσης μέσω οποιουδήποτε πρωτοκόλλου δικτύου
- ορίσει ένα σύστημα ονομάτων τομέων (DNS)
- υλοποιήσει στρώμα δρομολόγησης
- διαμοιράσει αρχεία με peer-to-peer (P2P) τεχνικές

Έτσι το IPFS ορίζει ένα νέο δίκτυο υπολογιστών που συμπληρώνει τα ήδη υπάρχοντα (www, Tor, .bit) διατηρώντας πλήρως αποκεντρωμένη αρχιτεκτονική και κανένα κεντρικό σημείο αποτυχίας.

Συνοπτικά, δηλαδή, στο IPFS αποθηκεύονται διευθυνσιοδοτημένα βάσει περιεχομένου (content-addressable) αρχεία, τα οποία ανακτώνται βάσει του hash των περιεχομένων τους (αντί για την τοποθεσία τους), ενώ ανακαλύπτονται και διαμοιράζονται μέσω του παρεχόμενου P2P network layer. Αξίζει, ωστόσο, να σημειωθεί πως το layer αυτό δεν εγγυάται από μόνο του το hosting των αρχείων και το διαθέσιμο bandwidth για την ανάκτηση τους, πράγμα που σημαίνει ότι θα πρέπει να γίνει παροχή υποδομής από τους χρήστες ικανής να υποστηρίξει έναν ελάχιστο αριθμό κόμβων αποθήκευσης.

Πρόκειται για συμπληρωματικές τεχνολογίες στις παραπάνω που στόχο έχουν την οργάνωση των αποθηκευμένων πληροφοριών σε μορφή βάσεων δεδομένων.

3.5 Προδιαγραφή μεθόδου υλοποίησης και χρονοπρογραμματισμός

3.5.1 Προδιαγραφή κύκλων

Εποπτικά, η διαδικασία της υλοποίησης περιγράφεται ως εξής:

3.5.2 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.

3.5.3 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.

3.5.4 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.

3.5.5 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.

3.6 Αρχιτεκτονική

Κεφάλαιο 4

Υλοποίηση εφαρμογής

4.1 Χαρακτηριστικά που υλοποιήθηκαν

4.2 Μεθοδολογία υλοποίησης

4.3 Τεχνολογίες υλοποίησης

4.4 Αρχιτεκτονική υλοποίησης

Κεφάλαιο 5

Συμπεράσματα

5.1 Προβλήματα ανάπτυξης

5.2 Διαφορές σχεδιασμού-υλοποίησης

5.3 Ανοιχτά θέματα

5.4 Επίλογος