



Αυτόνομο αμεσοδημοκρατικό 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

Σύνοψη

Decentralized και τα σχετικά.

Abstract

Don't forget the keywords.

Ευχαριστίες

Ευχαριστούμε η Αθήνα. Ευχαριστούμε η Ελλάδα.

Περιεχόμενα

Σύνοψη	2
Abstract	3
Ευχαριστίες	4
1 Εισαγωγή	7
1.1 Ορισμός του προβλήματος	7
1.2 Αποκέντρωση	8
1.3 Στόχος της διπλωματικής	9
1.4 Μεθοδολογία ανάπτυξης	9
1.5 Οργάνωση κεφαλαίων	10
2 Θεωρητικό υπόβαθρο	11
2.1 Συναρτήσεις κατακερματισμού	11
2.2 Ασύμμετρη κρυπτογραφία	11
2.3 Δένδρα Merkle	13
2.4 Δίκτυα Ομότιμων Κόμβων	14
2.5 Blockchain	14
2.6 Ethereum	15
2.6.1 Smart Contracts & DApps	15
2.6.2 EVM	16
2.7 IPFS	17
2.8 OrbitDB	18
3 Σχεδίαση εφαρμογής	20
3.1 Λογικά μέρη	20
3.2 Κατηγορίες χρηστών	21
3.2.1 Πρώτο μέρος	21
3.2.2 Δεύτερο μέρος	21
3.2.3 Σύνοψη χρηστών	21
3.3 Σενάρια χρήσης	21
3.4 Τεχνολογίες	21
3.4.1 Ethereum	21
3.4.2 IPFS, OrbitDB	22
3.5 Προδιαγραφή μεθόδου υλοποίησης και χρονοπρογραμματισμός	23
3.5.1 Προδιαγραφή κύκλων	23
3.5.2 Πρώτη φάση	23
3.5.3 Δεύτερη φάση	23

3.5.4	Τρίτη φάση	23
3.5.5	Τέταρτη φάση	24
3.6	Αρχιτεκτονική	24
4	Υλοποίηση εφαρμογής	25
4.1	Χαρακτηριστικά που υλοποιήθηκαν	25
4.2	Μεθοδολογία υλοποίησης	25
4.3	Τεχνολογίες υλοποίησης	25
4.4	Αρχιτεκτονική υλοποίησης	25
5	Συμπεράσματα	26
5.1	Προβλήματα ανάπτυξης	26
5.2	Διαφορές σχεδιασμού-υλοποίησης	26
5.3	Ανοιχτά θέματα	26
5.4	Επίλογος	26

Κεφάλαιο 1

Εισαγωγή

1.1 Ορισμός του προβλήματος

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).

Από την άλλη πλευρά, η κεντροποιημένη λογική ενός τέτοιου συστήματος αφενός συνοδεύεται από ποικίλα μειονεκτήματα τεχνικής φύσεως, αφετέρου εγείρει σοβαρούς προβληματισμούς σχετικά με τη διαχείριση των προσωπικών δεδομένων των χρηστών από κεντρικές αρχές. Τα βασικότερα από τα παραπάνω θα μπορούσαν να συνοψιστούν ως εξής:

- 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 κανένα 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 υποχρεώσεών τους ως προς τρίτους.
- 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.

1.2 Αποκέντρωση

Αν και ο όρος "αποκέντρωση" χρησιμοποιείται ευρέως στην επιστήμη των υπολογιστών και στα κρυπτοοικονομικά¹ (cryptoeconomics), συνήθως ορίζεται αρκετά ασαφώς[2]. Στην πραγματικότητα η αποκέντρωση 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 εμπιστεύονται 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 επίτευξη πολιτικής αποκέντρωσης. Αυτό πηγάζει τόσο από την ανάγκη προάσπισης των αρχών

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]

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 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.).

1.4 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 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 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

² Αλγοκρατία (algoracry) ή αλγοκρατική διακυβέρνηση είναι μία εναλλακτική μορφή διακυβέρνησης που βασίζεται στη χρήση αλγορίθμων.[3]

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

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, σαφής 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 τελμάτων κατά τη συγγραφή του κώδικα.

1.5 Οργάνωση κεφαλαίων

Στο δεύτερο κεφάλαιο γίνεται παρουσίαση του θεωρητικού υπόβαθρου...

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:

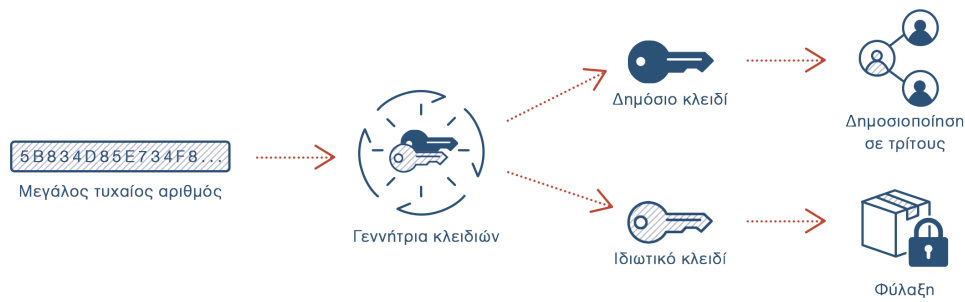
- Είναι ντετερμινιστική, δηλαδή η ίδια είσοδος παράγει πάντα την ίδια έξοδο.
- Είναι μη αντιστρέψιμη, δηλαδή είναι πρακτικά ανέφικτο να υπολογιστεί η είσοδος δεδομένης μιας εξόδου.
- Είναι αμφιμονοσήμαντη (1-1), δηλαδή σε δύο διαφορετικές εισόδους αντιστοιχούν πάντα δύο εντελώς διαφορετικές έξοδοι.
- 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
- Ότι 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.

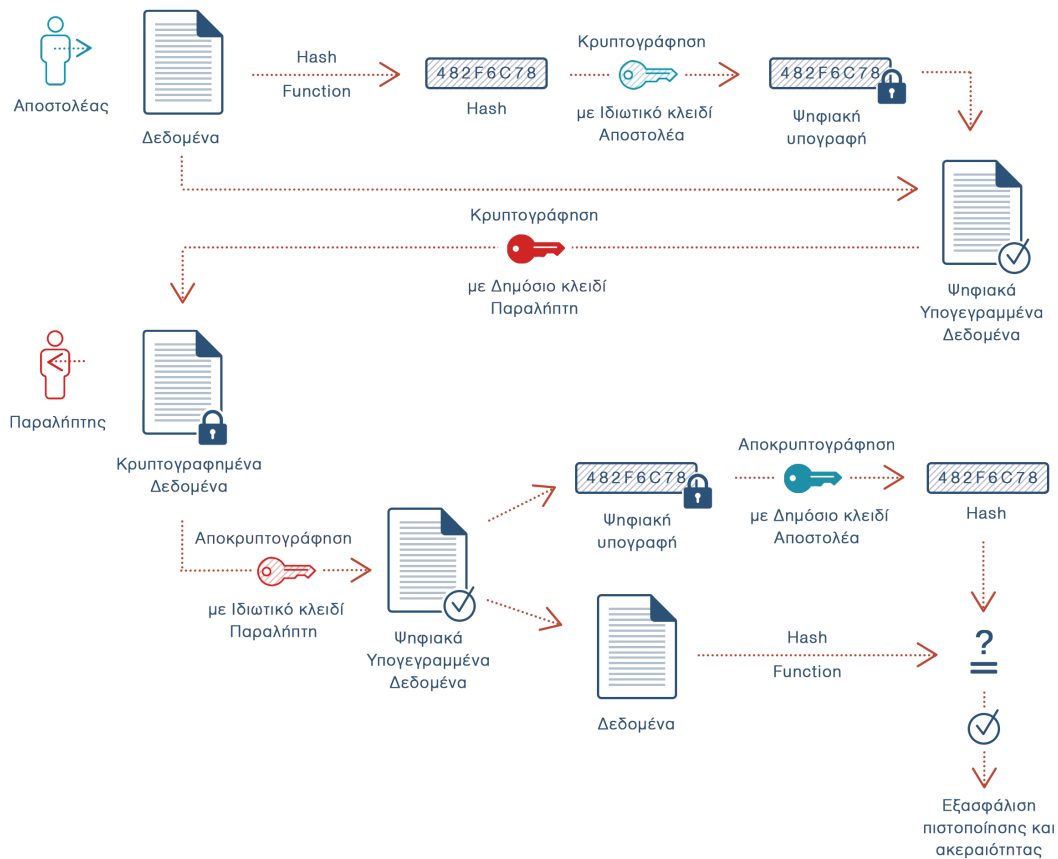


Σχήμα 2.1: Παραγωγή ασύμμετρου ζεύγους κλειδιών

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[4].

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 συνόλου, χωρίς να χρειαστεί να αποκαλυφθεί το περιεχόμενο οποιουδήποτε εκ των δύο[5].

2.4 Δίκτυα Ομότιμων Κόμβων

Τα δίκτυα ομότιμων κόμβων ή Peer-to-Peer (P2P) networks αποτελούν μία καταναμημένη 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.[6]

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.[7]

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).[8]

Ως προς την κυριότητα επί αυτού, το blockchain συνήθως¹ 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

¹Υπάρχουν και κάποιες υλοποιήσεις ιδιωτικών blockchain που, όμως, δε θα μας απασχολήσουν.

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.

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



Σχήμα 2.3: 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).[9]

2.6.1 Smart Contracts & DApps

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[10]. Ένας αυτόματος πωλητής ορίζεται ως ένα αυτόνομο μηχανήμα 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 παρέχουν 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. Bitcoin).
- 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.[9]

2.6.2 EVM

Τα smart contracts εκτελούνται από την εικονική μηχανή του Ethereum (Ethereum Virtual Machine ή EVM). Η EVM αποτελεί μία quasi²-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, που είναι διαθέσιμα κατά την εκτέλεση.[11]

²"quasi" 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.

2.7 IPFS

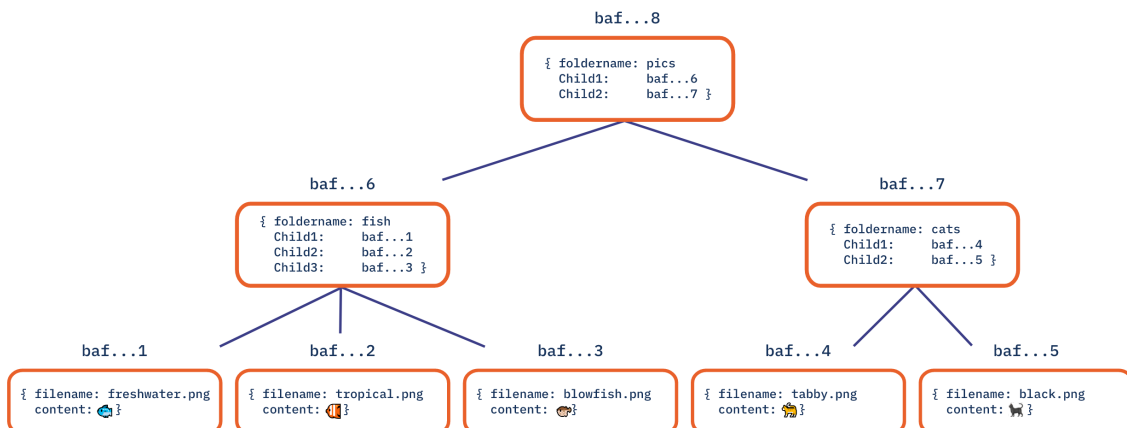


Σχήμα 2.4: IPFS logo

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.[12] 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.[13]

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 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 2.5: Merkle DAG[14]

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 κατακερματισμένων πινάκων κατακερματισμού (Distributed Hash Tables ή DHTs).** Ο DHT είναι ένα κατακερματισμένο 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.

2.8 OrbitDB



Σχήμα 2.6: 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 μία 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.[15]

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 κατανεμημένα 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, ενώ το DATABASE_NAME είναι το όνομα της βάσης[16]. 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 εξής (βλ. και <https://github.com/orbitdb/orbit-db-identity-provider>):

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

Σχήμα 2.7: OrbitDB Identity

- **Access Control:** Κατά τη δημιουργία μίας βάσης μπορούν να οριστούν όσοι θα έχουν δικαίωμα να γράψουν σε αυτήν 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.

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 εξ αρχής 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

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] Wikipedia. *Merkle tree*. URL: https://en.wikipedia.org/wiki/Merkle_tree.
- [5] Belavadi Prahalad. *Merkle proofs Explained*. 7 Ιαν. 2018. URL: <https://medium.com/crypto-0-nite/merkle-proofs-explained-6dd429623dc5>.
- [6] 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.
- [7] Satoshi Nakamoto. «Bitcoin: A Peer-to-Peer Electronic Cash System». Στο: *Cryptography Mailing list at https://metzdowd.com* (Μαρ. 2009).
- [8] Wikipedia. *Blockchain*. URL: <https://en.wikipedia.org/wiki/Blockchain>.
- [9] Vitalik Buterin. *Ethereum Whitepaper*. 2013. URL: <https://ethereum.org/en/whitepaper> (επίσκεψη 28/06/2021).
- [10] Alexander Savelyev. «Contract law 2.0: ‘Smart’ contracts as the beginning of the end of classic contract law». Στο: *Information & Communications Technology Law* 26 (Απρ. 2017), σσ. 1–19. DOI: 10.1080/13600834.2017.1301036.
- [11] Gavin Wood Andreas M Antonopoulos. *Mastering Ethereum: Building Smart Contracts and DApps*. O'Reilly Media, 2018. ISBN: 1491971940.
- [12] *IPFS*. URL: <https://ipfs.io/>.
- [13] *IPFS documentation*. URL: <https://docs.ipfs.io/>.
- [14] ProtoSchool. *Merkle DAGs: Structuring Data for the Distributed Web*. URL: <https://proto.school/merkle-dags/>.
- [15] *OrbitDB*. URL: <https://orbitdb.org>.
- [16] *Getting Started with OrbitDB*. URL: <https://github.com/orbitdb/orbit-db/blob/main/GUIDE.md>.