ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Εισαγωγή στις Αλυσίδες Συστοιχιών και σύγκριση δικτύων μικροπληρωμών

Των φοιτητών
Κάιντας Μάρτιν, Απόστολου Καλοβελώνη
Αρ. Μητρώου: 174957, 174915

Επιβλέποντες
Βλάχος Βασίλης, Αναπληρωτής Καθηγητής
Ηλιούδης Χρήστος, Καθηγητής

18 Σεπτεμβρίου 2023

Τίτλος Δ.Ε. Εισαγωγή στις Αλυσίδες Συστοιχιών και σύγκριση δικτύων μικροπληρωμών
Κωδικός Δ.Ε. 23136
Ονοματεπώνυμο φοιτητών Κάιντας Μάρτιν, Καλοβελώνης Απόστολος
Ονοματεπώνυμο εισηγητή Ηλιούδης Χρήστος
Ημερομηνία ανάληψης Δ.Ε. 12-03-2023
Ημερομηνία περάτωσης Δ.Ε. 17-09-2023

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Στους καθηγητές των φοιτητικών μας χρόνων

Πρόλογος

Το παρόν έργο είναι μια εισαγωγή στην τεχνολογία αλυσίδων συστοιχιών, εμβαθύνοντας τόσο στον τεχνικό όσο και στον πρακτικό τομέα, αποσαφηνίζοντας τις θεμελιώδεις της αρχές, τους μηχανισμούς και τις χρήσεις της. Λόγω των πολυάριθμων χρήσεων, οι αλυσίδες θεωρούνται ως μια τεχνολογική επανάσταση, όπως το διαδίκτυο, αναδιαμορφώνοντας τον τρόπο που αλληλεπιδρούμε και συναλλασόμαστε.

Περίληψη

Οι αλυσίδες μπλοκ μεταβάλλουν σχεδόν ολοκληρωτικά τις μέχρι τώρα δεδομένες μεθόδους συναλλαγών. Μέσω των μηχανισμών συναίνεσης, οι αλυσίδες καταφέρνουν να αντιμετωπίσουν με επιτυχία το πρόβλημα των βυζαντινών στρατηγών, αφαιρώντας την ανάγκη ύπαρξης ενός κεντροποιημένου τρίτου, όπως μια τράπεζα, που δρα ως η πηγή αλήθειας. Παράλληλα, η δημιουργία έξυπνων συμβολαίων δεν αναθεωρεί μόνο τα συστήματα συναλλαγών, αλλά τα πληροφοριακά συστήματα ως σύνολο, καθώς μια εφαρμογή μπορεί να εκτελεστεί στην ίδια την αλυσίδα και όχι σε κάποιο διακομιστή.

Στην δεύτερη ενότητα κάνουμε μια εισαγωγή στην τεχνολογία, την ορολογία, τα χαρακτηριστικά και τη δομή των αλυσίδων. Αναφέρουμε επίσης, τις δύο γνωστότερες μεθόδους συναίνεσης, την Απόδειξη-Εργασίας και Απόδειξη-Πονταρίσματος.

Στην τρίτη ενότητα αναφερόμαστε στο πρώτο και γνωστότερο κρυπτονόμισμα, το Bitcoin, τονίζοντας τόσο τα επιχειρήματα χρήσης αλλά και τις αδυναμίες. Έπειτα, στην τέταρτη ενότητα προχωρούμε με το Ethereum, το 2ο γνωστότερο κρυπτονόμισμα το οποίο έφερε την επανάσταση με τη χρήση Έξυπνων Συμβολαίων. Καθώς τα Έξυπνα Συμβόλαια δεν είναι χαρακτηριστικό μόνο του Ethereum, στην πέμπτη ενότητα εμβαθύνουμε στις δυνατότητες και τις χρήσεις τους, ανεξαρτήτως δικτύου.

Επειδή τα δίκτυα παρουσιάζουν δυσκολίες επέκτασης, στην έκτη ενότητα βρίσκονται οι διάφορες μέθοδοι αντιμετώπισης αυτού του προβλήματος. Στην έβδομη ενότητα κάνουμε μια εισαγωγή στα γνωστότερα δίκτυα μικροπληρωμών: Nano, Stellar και Lightning.

Στην όγδοη ενότητα εμβαθύνουμε στο δίκτυο μικροπληρωμών του Lightning και λίγο πριν το τέλος παρουσιάζουμε μια εφαρμογή μικροπληρωμών στο δίκτυο του αυτό, προσφέροντας μια εναλλακτική προσέγγιση στη σύγχρονη ηλεκτρονική ειδησιογραφία.

Τέλος, παρουσιάζουμε τα συμπεράσματά μας και πιθανές επεκτάσεις.

Introduction to Blockchain & micropayments network comparison

Martin Kaintas & Apostolos Kalovelonis

Abstract

Blockchains could completely change the way trade is conducted in our times. Through consensus mechanisms, the chains manage to successfully deal with the Byzantine generals problem by removing the need for a centralized third party, such as a bank, to act as the single source of truth. At the same time, the creation of smart contracts rethinks not only transaction systems, but information systems as a whole, as an application can be run on the blockchain itself rather than on a centralised server.

In the second section we introduce the technology, terminology, characteristics and structure of blockchains. We also mention the two best known consensus methods, Proof-of-Work and Proof-of-Stake.

In the third section we refer to the first and most well-known cryptocurrency, Bitcoin, highlighting both its advantages and weaknesses. Next, in the fourth section we move on to Ethereum, the second most known cryptocurrency that revolutionized the industry with the use of Smart Contracts. As Smart Contracts are not only a feature of Ethereum, in the fifth section we dive deeper into their capabilities and uses, regardless of the network they are on.

Most blockchain networks face difficulties in scalability, this is why the sixth section contains the various approaches that are used to deal with this problem. In the seventh section, we provide an introduction to the most widely known micropayment networks: Nano, Stellar and Lightning.

In the eighth section we delve into Lightning's micropayment network and shortly before the end we present a micropayment application using this network, offering an alternative approach to modern digital media.

Finally, we present our conclusions and possible future work that can be done on the subject.

Ευχαριστίες

Ευχαριστούμε τους καθηγητές μας για την καθοδήγηση και εκπαίδευση μας, όχι μόνο για την ολοκλήρωση της διπλωματικής εργασίας, αλλά και για τη διδασκαλία των προπτυχιακών μας χρόνων.

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Συντομογραφίες

Δ.Ε.	Διπλωματική Εργασία
ΔΙΠΑΕ	Διεθνές Πανεπιστήμιο Ελλάδος
Π.Ε.	Πτυχιακή Εργασία
PoW	Proof of Work
PoS	Proof of Stake
ECDSA	Elliptic Curve Digital Signature Algorithm
ORV	Open Representative Voting
HTLC	Hash Time Locked Contract

Κεφάλαιο 1ο: Εισαγωγή

Το αντικείμενο της εργασίας αυτής είναι η τεχνολογία του blockchain (αλυσίδες μπλοκ) καθώς και οι αλλαγές που μπορεί να φέρει στην καθημερινότητα του ανθρώπου. Θα εξερευνήσουμε αναλυτικά τις αλυσίδες μπλοκ και θα παρουσιάσουμε την εφαρμογή που αναπτύξαμε στα πλαίσια αυτής της εργασίας με σκοπό να αναδείξουμε το πώς η τεχνολογία των αλυσίδων μπλοκ μπορεί να ενταχθεί ομαλά στην καθημερινότητα μας.

Κίνητρο για την συγγραφή της εργασίας αποτελεί το πάθος μας για καινοτόμες τεχνολογίες και για την εξέλιξη της τεχνολογίας που εξυπηρετεί ευρύτερο κοινό. Πιστεύουμε ότι μέσω αλυσίδων συστοιχιών ο κόσμος μπορεί να επωφεληθεί σημαντικά, και να πετύχει πράγματα που χωρίς αυτό θα ήταν αδύνατα. Το blockchain σε συνδυασμό με εφαρμογές ανοιχτού κώδικα μπορούν να προσφέρουν ασυναγώνιστη διαφάνεια και εμπιστοσύνη στους χρήστες τους.

Οι αλυσίδες μπλοκ περιγράφονται συχνά ως μια επαναστατική τεχνολογία. Έχουν τη δυνατότητα να διαταράξουν τις υπάρχουσες βιομηχανίες και να δημιουργήσουν εντελώς νέες. Η εργασία αυτή συμβάλει στην κατανόηση του τρόπου με τον οποίο το blockchain μπορεί να προωθήσει την καινοτομία και να αναδιαμορφώσει επιχειρηματικά μοντέλα.

Οι αλυσίδες μπλοκ μεταβάλλουν σχεδόν ολοκληρωτικά τις μέχρι τώρα δεδομένες μεθόδους συναλλαγών. Μέσω των μηχανισμών συναίνεσης, οι αλυσίδες καταφέρνουν να αντιμετωπίσουν με επιτυχία το Βυζαντινό πρόβλημα των στρατηγών, αφαιρώντας την ανάγκη ύπαρξης ενός κεντροποιημένου τρίτου, όπως μια τράπεζα, που δρα ως η πηγή αλήθειας. Παράλληλα, η δημιουργία έξυπνων συμβολαίων δεν αναθεωρεί μόνο τα συστήματα συναλλαγών, αλλά τα πληροφοριακά συστήματα ως σύνολο, καθώς μια εφαρμογή μπορεί να εκτελεστεί στην ίδια την αλυσίδα και όχι σε κάποιο διακομιστή, αυξάνοντας έτσι την ασφάλεια και μειώνοντας την ανάγκη τυφλής εμπιστοσύνης του χρήστη σε κεντροποιημένα συστήματα.

Μέσω της διπλωματικής καταφέραμε να εμπλουτίσουμε τις γνώσεις μας γύρω από την τεχνολογία των αλυσίδων μπλοκ και ελπίζουμε η εργασία μας να αποτελέσει πηγή για άλλους που ενδιαφέρονται να κατανοήσουν ή και να εργαστούν με την τεχνολογία blockchain πιο αποτελεσματικά.

Στην δεύτερη ενότητα κάνουμε μια εισαγωγή στην τεχνολογία, την ορολογία, τα χαρακτηριστικά και τη δομή των αλυσίδων. Αναφέρουμε επίσης, τις 2 γνωστότερες μεθόδους συναίνεσης, την Απόδειξη-Εργασίας και Απόδειξη-Πονταρίσματος.

Στην τρίτη ενότητα αναφερόμαστε στο πρώτο και γνωστότερο κρυπτονόμισμα, το Bitcoin, τονίζοντας τόσο τα επιχειρήματα χρήσης αλλά και τις αδυναμίες. Έπειτα, στην τέταρτη ενότητα προχωρούμε με το Ethereum, το 2ο γνωστότερο κρυπτονόμισμα το οποίο έφερε την επανάσταση με τη χρήση Έξυπνων Συμβολαίων. Καθώς τα Έξυπνα Συμβόλαια δεν είναι χαρακτηριστικό μόνο του Ethereum, στην πέμπτη ενότητα εμβαθύνουμε στις δυνατότητες και τις χρήσεις τους, ανεξαρτήτως δικτύου.

Επειδή τα δίκτυα παρουσιάζουν δυσκολίες επέκτασης, στην έκτη ενότητα βρίσκονται οι διάφορες μέθοδοι αντιμετώπισης αυτού του προβλήματος. Στην έβδομη ενότητα κάνουμε μια εισαγωγή στα γνωστότερα δίκτυα μικροπληρωμών: Nano, Stellar και Lightning.

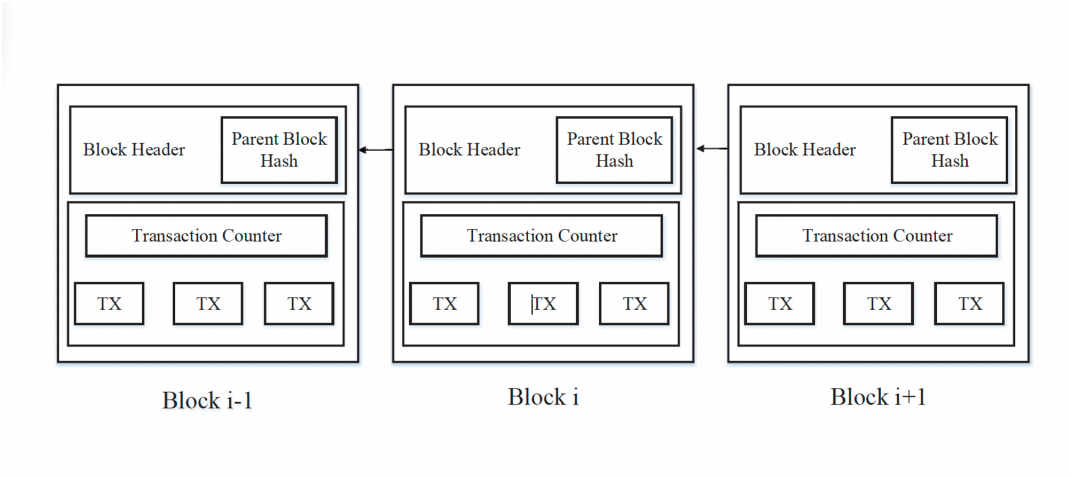
Στην όγδοη ενότητα εμβαθύνουμε στο δίκτυο μικροπληρωμών του Lightning και λίγο πριν το τέλος παρουσιάζουμε μια εφαρμογή μικροπληρωμών στο δίκτυο του αυτό, προσφέροντας μια εναλλακτική προσέγγιση στη σύγχρονη ηλεκτρονική ειδησιογραφία.

Τέλος, παρουσιάζουμε τα συμπεράσματά μας και πιθανές επεκτάσεις.

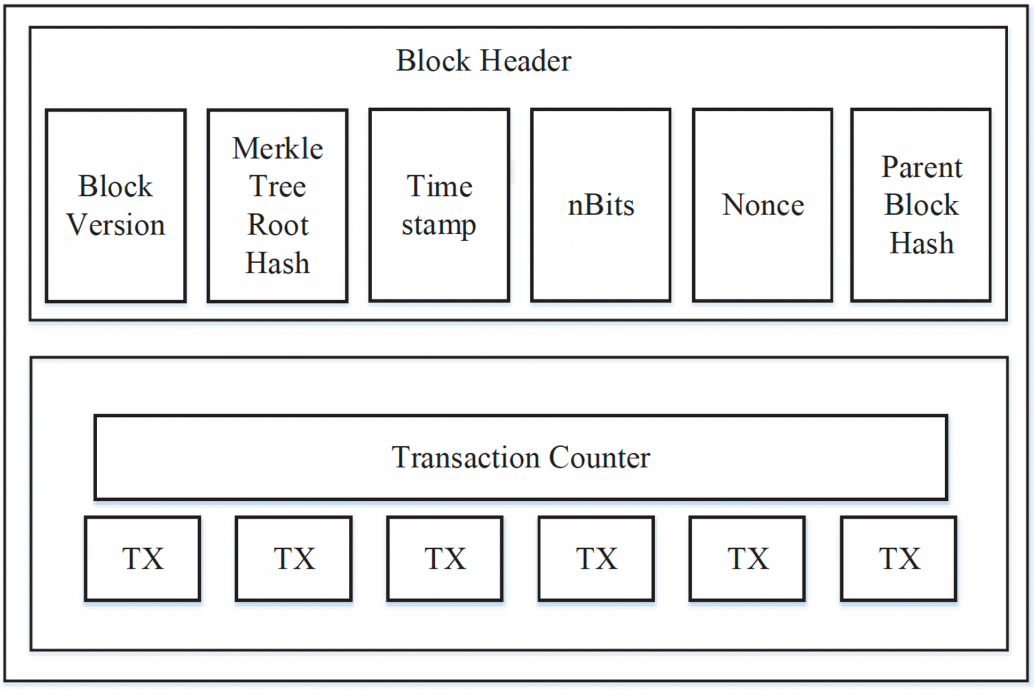
Κεφάλαιο 2ο: Εισαγωγή στις Αλυσίδες Συστοιχιών

Μια αλυσίδα συστοιχιών είναι ένα σύστημα κατανεμημένης λογιστικής που επιτρέπει διαφανείς και ασφαλείς συναλλαγές χωρίς την ανάγκη κάποιου κεντρικού μεσάζοντα. Ένας εναλλακτικός τρόπος παρουσίασης του είναι μια βάση δεδομένων που αποθηκεύει αμετάβλητα δεδομένα με ασφαλή και αποκεντρωμένο τρόπο.

Το κίνητρο πίσω από την τεχνολογία του είναι η δημιουργία ενός δικτύου από υπολογιστές **κόμβους** nodes που επικοινωνούν μεταξύ τους για την επαλήθευση και επικύρωση συναλλαγών. Κάθε μπλοκ στην αλυσίδα περιέχει ένα σύνολο συναλλαγών που έχουν επαληθευτεί από το ίδιο το δίκτυο. Όπως προαναφέρθηκε, μόλις προστεθεί ένα μπλοκ στην αλυσίδα, δεν μπορεί να παραμετροποιηθεί.



Σχήμα 2.1: Δείγμα αλυσίδας



Σχήμα 2.2: Δείγμα Block

Στο σχήμα 2.1 παρουσιάζεται μία αλυσίδα. Κάθε μπλοκ έχει μια κατακερματισμένη συμβολοσειρά (hash) η οποία χρησιμοποιείται ως αναγνωριστικό του. Συγκεκριμένα, κάθε επόμενο μπλοκ, έχει ως αναφορά στην επικεφαλίδα του (header) την κατακερματισμένη συμβολοσειρά του προηγούμενου (parent) block, παρόμοια με τη λειτουργία της δομής δεδομένων συνδεδεμένης λίστας. Το πρώτο μπλοκ μιας αλυσίδας ονομάζεται genesis καθώς δεν έχει αναφορά σας άλλο μπλοκ. Στη συνέχεια θα αναφερθούμε στα κομβικότερα στοιχεία μιας αλυσίδας.

2.1 Στοιχεία μιας αλυσίδας

Χρήστης Ως χρήστης ορίζεται μια οντότητα η οποία αλληλεπιδρά με το δίκτυο στέλνοντας ή λαμβάνοντας συναλλαγές. Κάθε χρήστης έχει ένα ψηφιακό πορτοφόλι, το οποίο αποτελείται από ένα κρυφό και ένα δημόσιο κλειδί, τα οποία χρησιμοποιούνται για την επαλήθευση συναλλαγών. Όπως εκμυστηρεύουν και οι τίτλοι τους, το ζεύγος κλειδιών είναι αντίστοιχο με το ζεύγος ονόματος χρήστη και κωδικού άλλων συστημάτων: Το δημόσιο κλειδί μπορεί να μοιραστεί ελεύθερα μεταξύ των χρηστών, ενώ αντίθετα, το κρυφό κλειδί, επιτρέποντας μεταβολές στην κατάσταση του πορτοφολιού, θα πρέπει να παραμένει μυστικό. Συγκεκριμένα, το δημόσιο κλειδί είναι το κύριο αναγνωριστικό του χρήστη, μέσω του οποίου μπορεί να επαληθευτεί η κατοχή μιας συναλλαγής. Αντίθετα, το κρυφό κλειδί χρησιμοποιείται για την υπογραφή συναλλαγών, αλλάζοντας την ιδιοκτησία τους. [6] Κάθε ψηφιακή υπογραφή αποτελείται από 2 φάσεις, τη φάση υπογραφής (signing phase) και τη φάση πιστοποίησης (verification phase). Λόγου χάρη, ο Γιάννης θέλει να στείλει στην Άννα ένα μήνυμα. Στην πρώτη φάση, ο Γιάννης θα κρυπτογραφήσει το μήνυμα του με το κρυφό του κλειδί, ενώ έπειτα θα στείλει στην Άννα το αρχικό μήνυμα αλλά και το κρυπτογραφημένο. Με αυτόν τον τρόπο, η Άννα μπορεί να επιβεβαιώσει ότι το μήνυμα δεν έχει αλλοιωθεί κατά την αποστολή του. Ο συχνότερος αλγόριθμος υπογραφής είναι ο ECDSA. [7]

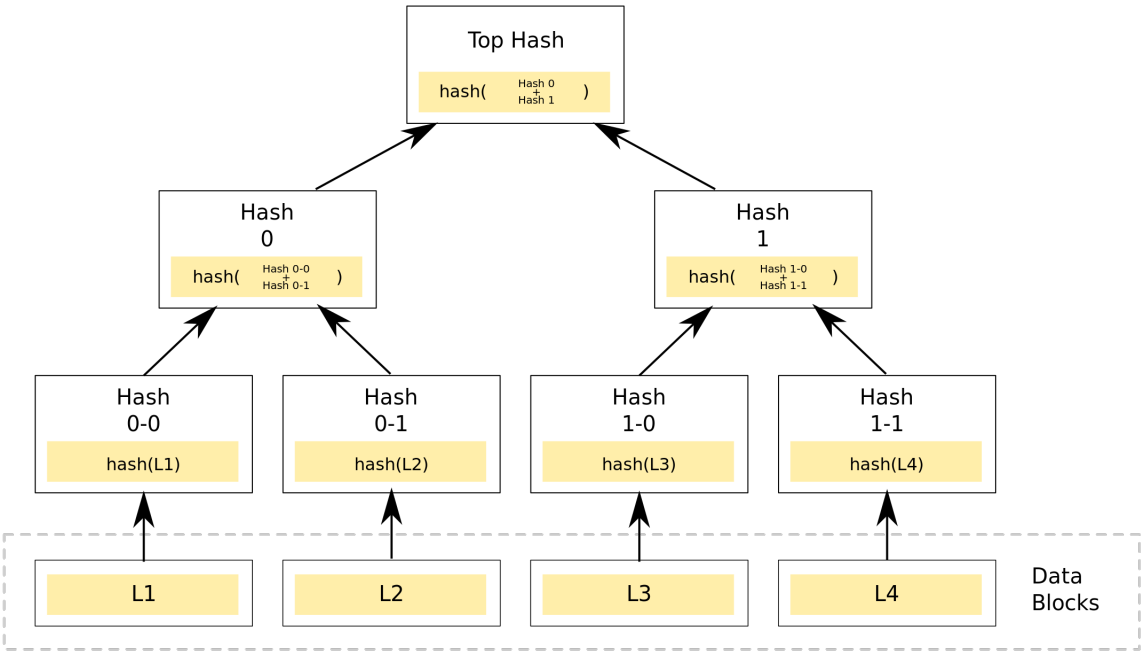
Κόμβος Ένας κόμβος (node) ειναι μια οντότητα που συμμετέχει σε ένα δίκτυο διατηρώντας ένα αντίγραφο της αλυσίδας, επαληθεύοντας συναλλαγές βασιζόμενη σε ένα σύνολο κοινών κανόνων. Σε σχέση με το χρήστη, ένας κόμβος μπορεί να θεωρηθεί ως το μέσο αλληλεπίδρασης με το δίκτυο. Οι κόμβοι επικοινωνούν μεταξύ τους με σκοπό την πάραξη νέων συναλλαγών αλλά και για την πιστοποίηση συναλλαγών. [6]

Συναλλαγή Μια συναλλαγή στα πλαίσια μιας αλυσίδας είναι η ψηφιακή μεταφορά μιας ιδιοκτησίας ή πληροφορίας η οποία μπορεί να πιστοποιηθεί μέσα από το δίκτυο. Κάθε συναλλαγή αναπαριστάται από ένα ξεχωριστικό αναγνωριστικό παραγώμενο από μια συνάρτηση κρυπτογράφησης. [6]

Μπλοκ Ένα μπλοκ, όπως και ένα πακέτο IP, αποτελείται από μια επικεφαλίδα και ένα σώμα. Το σώμα περιέχει τις συναλλαγές, ενώ η επικεφαλίδα ενός block περιέχει 6 σημαντικά στοιχεία.

1. **Έκδοση** καθορίζει τους κανόνες που πρέπει να ακολουθηθούν για την επικύρωση μιας συναλλαγής.

2. **Ριζική κατακερματισμένη συμβολοσειρά Merkle Δέντρου - Merkle tree root hash** Κάθε συναλλαγή ενός μπλοκ, περνάει από στρώματα κατακερματισμού. Κάθε στρώμα, έχει ν εισόδους και ν/2 εξόδους, μέχρις ότου η τελική έξοδος να έχει έναν κατακερματισμό, μειώνοντας σημαντικά το μέγεθος της πληροφορίας. Το τελικό αποτέλεσμα έχει την ισχύ ενός ψηφιακού ίχνους, επιτρέποντας την επαλήθευση συμπερίληψης μιας συναλλαγής. Η μεθοδολογία αυτή μπορεί να παρουσιαστεί με ένα δέντρο, για αυτό το λόγο η τελική έξοδος λέγεται και ρίζα του merkle δέντρου.



Σχήμα 2.3: Ένα Δέντρο Merkle

3. **Χρονοσφραγίδα** Δοθείσα χρονική στιγμή σε δευτερόλεπτα, σε σχέση με τη διεθνή ημερομηνία 1η Ιανουαρίου 1970
4. **nBits** Μέγεθος block hash
5. **Μετρητής (Nonce)** Ένας μετρητής 4 byte, που ξεκινάει με 0 και αυξάνεται με κάθε υπολογισμό hash. Δεν βρίσκεται στα δίκτυα Proof-of-Stake.
6. **Συμβολοσειρά block γονέα (Parent block hash)** Το αναγνωριστικό του προηγούμενου block

2.2 Χαρακτηριστικά Αλυσίδων συστοιχιών

Αποκεντροποιημένες Τα μέχρι σήμερα συστήματα συναλλαγών βασίζονται σε μια κεντροποιημένη μεθοδολογία για την επικαιροποίηση συναλλαγών, στηριζόμενα σε έναν κεντρικό πάροχο, λόγου χάρη μια κεντρική τράπεζα. Αντίθετα, στις αλυσίδες, η εξάρτηση από έναν έμπιστο πάροχο αφαιρείται καθώς κάθε συναλλαγή επαληθεύεται μέσω ενός συμφωνημένου αλγορίθμου από τους κόμβους του δικτύου.

Αμετάβλητες Κάθε συναλλαγή που έχει συμπεριληφθεί σε ένα μπλοκ δεν μπορεί να διαγραφεί, ενώ μπλοκ που έχουν μη έγκυρες συναλλαγές μπορούν άμεσα να απορριφθούν μέσω του συμφωνημένου αλγορίθμου.

Απαράβατες Όντας ως ένα δημόσιο βιβλίο προσβάσιμο από όλους, η ασφάλεια των συναλλαγών στηρίζεται από τους αλγορίθμους κρυπτογράφησης καθώς και στη δύναμη του συνόλου καθώς οι συναλλαγές επαληθεύονται από τους συμμετέχοντες. Άρα, μη έγκυρες συναλλαγές και μπλοκ εύκολα απορρίπτονται πριν συμπεριληφθούν στην αλυσίδα.

Ήμι-ανώνυμο Κάθε χρήστης μπορεί να αλληλεπιδράσει με μια αλυσίδα έχοντας μόνο ένα κρυφό και ένα δημόσιο κλειδί, χωρίς αυτά να αποκαλύπτουν την ταυτότητα του.

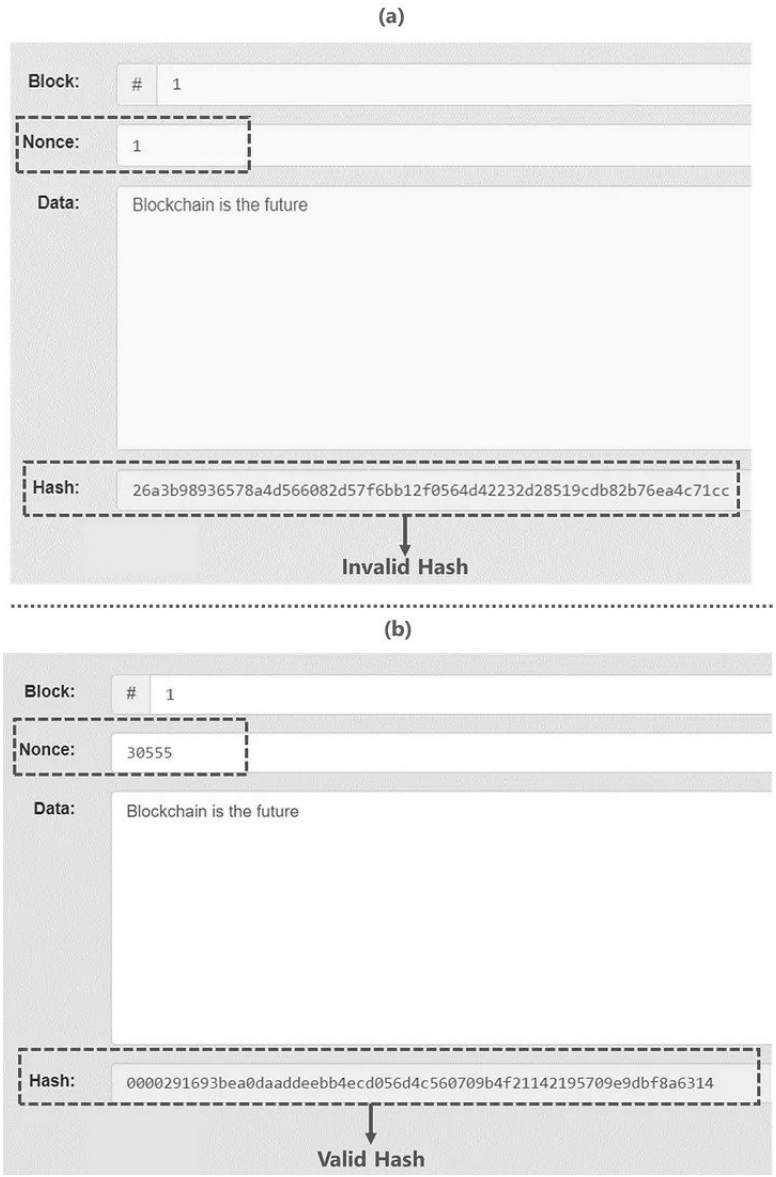
2.3 Αλγόριθμοι Πιστοποίησης

Ως αλγορίθμους πιστοποίησης ορίζουμε τη μεθοδολογία καθορισμού της κατάστασης μιας αλυσίδας η οποία αποδέχεται από όλους τους χρήστες της. Για παράδειγμα, μια κατάσταση είναι το περιεχόμενο των συναλλαγών ενός μπλοκ, τα ίδια τα μπλοκ, η αξία λογαριασμών των χρηστών. Σε αυτό το σημείο θα αναλύσουμε τους 2 γνωστότερους αλγορίθμους, Απόδειξη-Εργασίας (Proof-Of-Work) και Απόδειξη-Πονταρίσματος (Proof-Of-Stake)

2.3.1 Απόδειξη-Εργασίας

Όπως προ-αναφέρθηκε, κάθε μπλοκ έχει μια κατακερματισμένη συμβολοσειρά. Πριν κλείσει ένα μπλοκ, το κατακερματισμένο κείμενο του πρέπει να επικυρωθεί πριν ανοίξει ένα νέο. Με τη σημερινή τεχνολογία, ένας δεκαεξαδικός αριθμός 64 ψηφίων που είναι το hash, μπορεί να δημιουργηθεί σε χιλιοστά του δευτερολέπτου ακόμη και για δεδομένα υψηλού όγκου. Η τιμή του πρέπει να είναι μικρότερη ή ίση του στόχου (target). Στις αλυσίδες PoW, οι συμμετέχοντες (miners) στην ουσία προσπαθούν να μαντέψουν αυτήν την τιμή, εφόσον δεν υπάρχει κάποια πληροφορία που θα τους βοηθήσει στον υπολογισμό. Ο υπολογισμός αυτός απαιτεί αρκετούς υπολογιστικούς πόρους, αλλά αντιθέτως η επαλήθευση της τιμής είναι πολύ πιο απλή. Στην πράξη, οι miners προσπαθούν συνεχώς ξανά και ξανά κατακερματίζοντας τα δεδομένα της συναλλαγής προς πιστοποίηση με το **αριθμητή (nonce)**. Επειδή οι προσπάθειες είναι τυχαίες, το nonce είναι ένας αριθμός μιας χρήσης που αναφέρεται στο πλήθος των προσπαθειών. [8]

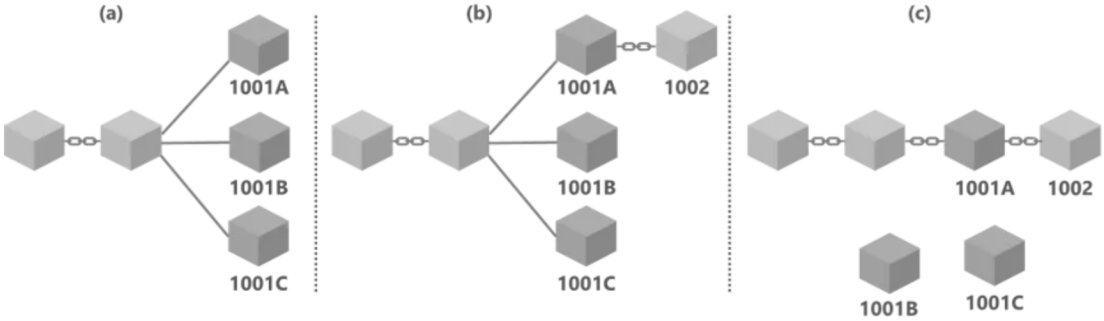
Δυσκολία Η δυσκολία υπολογισμού είναι δυναμική. Κάθε target ξεκινάει με ένα πλήθος 0 το οποίο μεταβάλλεται ανάλογα με το πόσο δύσκολος πρέπει να είναι ο υπολογισμός. Στο bitcoin, στόχος είναι ένα μπλοκ να κλείνει κάθε 10 λεπτά, συνεπώς το πλήθος των μηδενικών καθορίζεται ανάλογα με το μέσο όρο του απαιτούμενου χρόνου για την προσθήκη ενός νέου μπλοκ στην αλυσίδα. Καθώς η τεχνολογία εξελίσσεται, τόσο ευκολότερο είναι για τις μηχανές να υπολογίσουν το hash. Για αυτό το λόγο, στο Bitcoin, κάθε 2016 μπλοκ ή περίπου ανά 2 εβδομάδες μεταβάλλεται το πλήθος των 0 με σκοπό ο μέσος χρόνος νέου μπλοκ να είναι τα 10 λεπτά. [9]



Σχήμα 2.4: Έγκυρο και μη hash

Επιβράβευση Με την εισαγωγή ενός νέου block στην αλυσίδα, παράγονται νέα coins τα οποία δίνονται στον πρώτο miner που υπολογίζει το hash. Παράλληλα, επιβραβεύεται και με τους προπληρωμένους φόρους των συναλλαγών που περιέχονται. Το πλήθος των νέων νομισμάτων που δίνονται στον εξορύκτη είναι μεταβαλλόμενο και με την πάροδο του χρόνου μειώνεται. Αυτό συμβαίνει διότι με αυτόν τον τρόπο η αξία του νομίσματος αυξάνεται καθώς γίνεται σπανιότερη η απόκτηση του, ενώ παράλληλα γίνεται κίνητρο για περισσότερους εξορύκτες. Συγκεκριμένα, το δίκτυο του Bitcoin μειώνει στο μισό τα επιβραβευόμενα νομίσματα κάθε 210.000 blocks, δηλαδή περίπου 4 χρόνια. [10]

Η κυριαρχεία της μακρύτερης αλυσίδας Παρόλο που ο υπολογισμός ενός hash είναι δύσκολος, υπάρχει μια πιθανότητα 2 ή παραπάνω εξορύκτες να το βρουν. Αυτό θα προκαλέσει τη γέννηση 2 νέων κλαδιών της αλυσίδας. Για παράδειγμα, σε μια αλυσίδα μήκους 1000 block, 3



Σχήμα 2.5: Η κυριαρχεία της μακρύτερης αλυσίδας. το 1001A επιλέγεται ως το 1001ο block.

εξορύκτες υπολογίζουν το hash. Αυτό σημαίνει ότι θα υπάρξουν 4 1001α μπλοκ: 1001A, 1001B, 1001Γ. Η μέθοδος επιλογής block για να συνεχίσει να είναι έγκυρη η αλυσίδα, στηρίζεται στη γέννηση του επόμενου μπλοκ (502). Το κλαδί που θα στηριχθεί το επόμενο 1002ο μπλοκ, είναι αυτό που σφραγίζεται ως το 1001ο. Η μέθοδος αυτή ονομάζεται κυριαρχεία της **μακρύτερης αλυσίδας - longest chain rule**. [9]

Ομάδες Εξόρυξης Η διαδικασία εξόρυξης μπορεί να γίνει είτε ατομικά είτε σε ομάδα. Στο ατομικό, ο χρήστης πρέπει να εγγραφεί ως miner και έπειτα θα μπορεί να χρησιμοποιήσει τους υπολογιστικούς του πόρους για να μαντέψει το hash. Από την άλλη μεριά, μια ομάδα είναι μια συνεργατική προσπάθεια συλλογικών υπολογιστικών πόρων. Στην περίπτωση που μια ομάδα υπολογίσει το σωστό hash, τότε τα κέρδη διαμοιράζονται. Με την ομαδική προσέγγιση, χρήστες με πιο αδύναμους υπολογιστές αυξάνουν τις πιθανότητες τους να κερδίσουν. [11]

2.3.2 Απόδειξη Πονταρίσματος - proof of Stake

Στις αλυσίδες PoS, οι εξορύκτες ονομάζονται επικυρωτές και η πιθανότητα να επιλεχθούν δεν καθορίζεται από την υπολογιστική τους ισχύ. Αντιθέτως, οι εν δυνάμει επικυρωτές σφραγίζουν ένα πλήθος νομισμάτων το οποίο αναλογικά αυξάνει τις πιθανότητες να επιλεχθούν ως αυτοί που θα προσθέσουν το block στην αλυσίδα. Η σφράγιση του ποσού γίνεται μέσω ενός έξυπνου συμβολαίου, το οποίο σε περίπτωση που ο χρήστης πράξει κακόβουλα, θα τιμωρηθεί παίρνοντας του το κλειδωμένο ποσό. Το αν κάποιος πράξει κακόβουλα, καθορίζεται από τους υπόλοιπους επικυρωτές οι οποίοι πράττουν ως ελεγκτές. Ο κίνδυνος να σφάλουν οι υπόλοιποι επικυρωτές είναι περιορισμένος, καθώς ένα τέτοιο λάθος ισοδυναμεί με πλήγμα στο ίδιο το δίκτυο, άρα και στην αξία του ίδιου του νομίσματος. Ένα δίκτυο που υπολειτουργεί, σίγουρα δεν θα επιλεχθεί και για χρήση. [12]

Από πολλούς, το PoS χαρακτηρίζεται ως μια πολύ ισχυρότερη εναλλακτική του PoW. Μερικοί λόγοι είναι [13]:

Φιλικό προς το περιβάλλον Αφαιρώντας την εξάρτηση υπολογιστικής ισχύς, αυτός ο μηχανισμός είναι σημαντικά πιο φιλικός προς το περιβάλλον.

Λιγότερο ευάλωτο σε επιθέσεις Στα συστήματα PoW, το κόστος μιας επίθεσης είναι όλοι οι πόροι (κόστος ρεύματος) που καταναλώθηκαν για την επίθεση. Αντιθέτως, στα συστήματα PoS, το κόστος είναι πολύ ακριβότερο, καθώς μια αποτυχημένη επίθεση μπορεί να οδηγήσει στο χάσιμο ολόκληρης της κρυπτονομισματικής περιουσίας. Με όρους PoW, αυτό θα ήταν σαν να χανόταν ολόκληρο το μηχάνημα που χρησιμοποιείται για mining πέρα από το ρεύμα που απαιτεί. Συνεπώς, επιθέσεις 51% γίνονται πολύ πιο ακριβές άρα και πιο σπάνιες.

Αποκεντροποίηση Από τη στιγμή που δεν απαιτείται κάποιο μηχάνημα που θα τρέχει συνεχώς ακόμη και για να συμμετάσχει σε μια ομάδα mining, οι ομάδες πονταρίσματος είναι πολύ πιο προσβάσιμες.

Επεκτασιμότητα Η αρχιτεκτονική αυτών των συστημάτων επιτρέπουν τη χρήση ενός μηχανισμού που ονομάζεται **Τεμαχισμός (Sharding)**. Ο τεμαχισμός, είναι μιας μορφής βάσης δεδομένων, όπου μια αλυσίδα κομματιάζεται σε μικρότερες αλυσίδες, όπου κάθε μια μπορεί να γεμίσει με μπλοκ, κάτι που αυξάνει σημαντικά την ταχύτητα ενός δικτύου.

Ο τεμαχισμός δεν είναι εφικτό σε PoW, καθώς η ύπαρξη υπο-αλυσιδών θα απαιτούσε ευκολότερους υπολογισμούς hash, κάτι που θα αποδυνάμωνε την ασφάλεια του δικτύου.

Κεφάλαιο 3ο: Bitcoin

Σε αυτή την ενότητα αναφέρουμε την ανάγκη ενός συστήματος σαν το Bitcoin, καθώς και τις αδυναμίες του.

3.1 Επιχειρήματα υπέρ του Bitcoin

Επιχειρήματα που σχετίζονται με τα περισσότερα δίκτυα, όπως η αποκεντροποίηση και η ψευδοανωνυμότητα που αναφέρθηκαν σε προηγούμενες ενότητες, θεωρούνται δεδομένα.

3.1.1 Αντιμετώπιση ηλεκτρονικής απάτης

Εύκολα μπορούμε να συμπεράνουμε πως το ηλεκτρονικό εμπόριο στηρίζεται ολοκληρωτικά στα χρηματοπιστωτικά ιδρύματα, λόγου χάρη στην Εθνική Τράπεζα της Ελλάδος. Σαφέστατα αυτά τα συστήματα έχουν αποδείξει πως μπορούν να λειτουργήσουν αποτελεσματικά, παρόλα αυτά έχουν κάποιες σημαντικές αδυναμίες.

Για παράδειγμα, οι συναλλαγές στα τυπικά συστήματα είναι επί το πλείστον αναστρέψιμες. Με μια πρώτη ματιά η ιδέα των αναστρέψιμων συναλλαγών δεν παρουσιάζεται λανθασμένη, παρόλα αυτά, σύμφωνα με μια έρευμα της LexisNexis [14] το 2022, οι επιχείρησεις χάνουν κατά μέσο ώρο $3.75 για κάθε $1 αντίστροφων χρεώσεων. Ενώ, με την άνοδο των ηλεκτρονικών αγορών την εποχή του 2021 [15], οι επιχειρήσεις παρατήρησαν 75% αύξηση στις ηλεκτρονικές απάτες, με τη μεγαλύτερη αυτών την απάτη μέσω επιστροφής χρημάτων. [1] Σε ένα blockchain σύστημα όπως το Bitcoin, οι συναλλαγές δεν είναι αντιστρέψιμες, προστατεύοντας τους πωλητές από σχετικές.

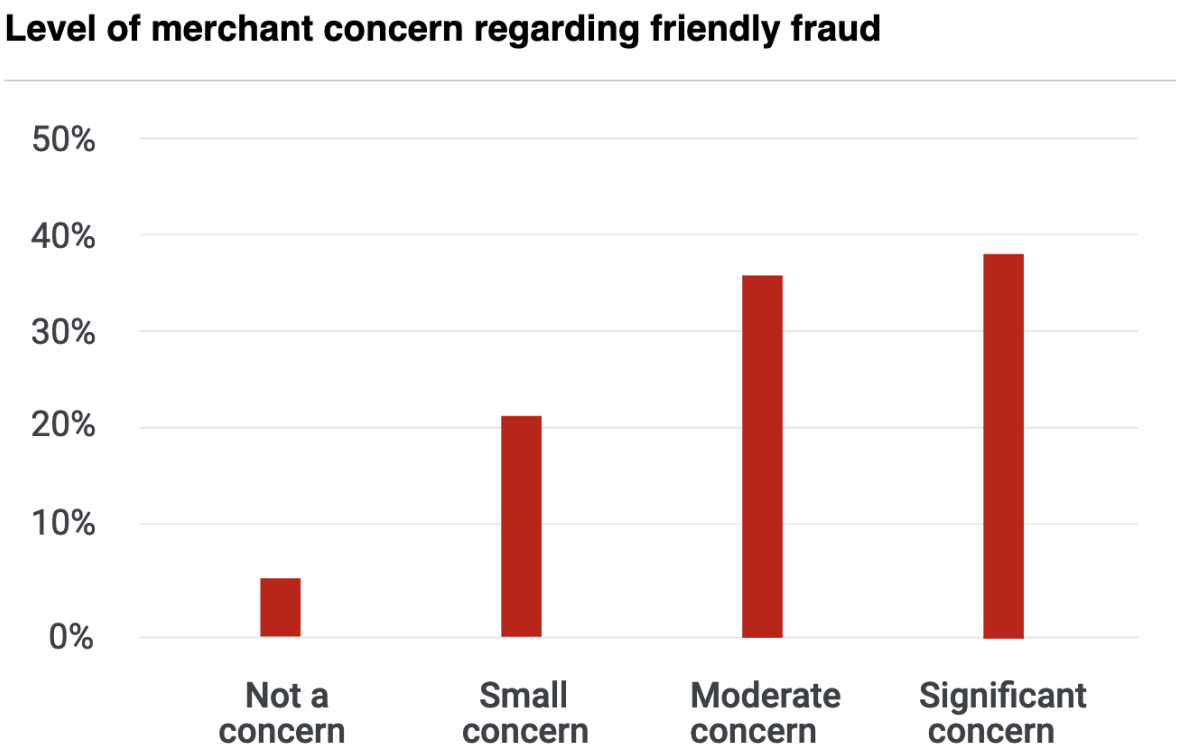
3.1.2 Προστασία από τον πληθωρισμό

Σε αντίθεση με άλλα νομίσματα, το Bitcoin έχει προκαθορισμένο πλήθος νομισμάτων που μπορούν να υπάρξουν. Ο αριθμός αυτός είναι 21.000.000, δίνοντας στο Bitcoin την προστασία απέναντι στον πληθωρισμό. Αυτή η ιδιότητα το έχει οδηγήσει να συγκρίνεται με το χρυσό, καθώς και ο χρυσός, λόγω της περιορισμένης εύρεσης του, είναι ένα εργαλείο κόντρα στον πληθωρισμό.

3.2 Αδυναμίες

3.2.1 Έλλειψη πληθωρισμού

Ένα μεγάλο πλήθος οικονομολόγων, υποστηρίζει πως για να αποδεχθεί ένα νόμισμα από την παγκόσμια αγορά, θα πρέπει να παρουσιάζει κάποιας μορφής πληθωρισμού. Το επιχείρημα είναι πως, όταν ένα νόμισμα προβλέπεται ότι θα χάσει την αξία του σε σχέση με τα προϊόντα που μπορεί να ανταλλαχθεί, ενισχύει την αγορά καθώς είναι μιας μορφής πίεσης της ροής του χρήματος. Αντιθέτως, όταν ένα νόμισμα δεν παρουσιάζει πληθωρισμό και προβλέπεται πως η αξία του θα αυξηθεί, λόγου χάρη όπως ο χρυσός, τότε η ροή του στην αγορά μειώνεται καθώς οι ιδιοκτήτες θεωρούν πως είναι πιο κερδοφόρο να περιμένουν την αύξηση της τιμής του. Συνεπώς, ενώ το Bitcoin είναι



Σχήμα 3.1: Επίπεδα ανησυχίας πωλητών σχετικά με τις απάτες επιστροφής χρημάτων. Παρατηρείται ότι πάνω από 35% θεωρεί πως είναι ένα σημαντικό πρόβλημα. [1]

ένα ισχυρό εργαλείο συγκρίσιμο με το χρυσό και το ασήμι, είναι αμφισβητήσιμη η ισχύ του στην καθημερινή αγορά.

3.2.2 Περιορισμένη επεκτασιμότητα

Περιορισμένο μέγεθος Block Το μέγεθος ενός block στο δίκτυο του Bitcoin είναι στο 1MB. Αυτό από μόνο του περιορίζει το πλήθος των συναλλαγών που μπορούν να συμπεριληφθούν, άρα και αργότερη επιβεβαίωση συναλλαγών σε περιόδους υψηλής ζήτησης. [16]

Υψηλή κατανάλωση ρεύματος Όντας ένα δίκτυο PoW, η εκλογή εξορύκτη γίνεται σε αντάλλαγμα με την κατανάλωση ρεύματος, η οποία είναι ακριβή. [16]

Υψηλό κόστος συναλλαγών Με την αύξηση της αξίας του Bitcoin, το υψηλό κόστος για την επιβεβαίωση μιας συναλλαγής καθιστά ακατάλληλο το Bitcoin για την ολοκλήρωση μικρο-αγορών. [16]

Κεφάλαιο 4ο: Ethereum

Το Ethereum είναι μια αποκεντροποιημένη πλατφόρμα αλυσίδων συστοιχιών ανοιχτού κώδικα, η οποία επιτρέπει την εκτέλεση προγραμματιστικών συναρτήσεων, γνωστά ως έξυπνα συμβόλαια (smart contracts). Προτάθηκε το 2013 από τον Vitalik Buterin και τέθηκε σε λειτουργία το 2015. Το κύριο κίνητρο του Ethereum είναι η ιδέα μιας προγραμματίσιμης αλυσίδας, όπου προγραμματιστές θα έχουν τη δυνατότητα να δημιουργούν αποκεντροποιημένες εφαρμογές οι οποίες μπορούν να εκτελεσθούν χωρίς κάποιο μεσάζοντα. [17]

Είναι ένα δίκτυο Proof-Of-Stake, το οποίο αρχικά ήταν Proof-Of-Work, όπως το Bitcoin. Το νόμισμα του είναι το Ether, με τη μικρότερη μονάδα να είναι το Wei. Ένα Ether, αντιστοιχεί σε 2î8 Wei. Μια ειδοποιός οικονομική διαφορά μεταξύ του Ethereum και το Bitcoin είναι πως το πρώτο παρουσιάζει πληθωρισμό, επιτρέποντας του καθημερινή χρήση. [17]

4.1 Δομή

Το δίκτυο απαρτίζεται από αντικείμενα που ονομάζομαι **λογαριασμοί (accounts)**, τα οποία περιέχουν μια διεύθυνση 20bytes. Πέρα από τη διεύθυνση, υπάρχει το nonce, ο μετρητής συναλλαγών, ο οποίος επιτρέπει την εκτέλεση συναλλαγών μια φορά. Υπάρχει επίσης το διαθέσιμο υπόλοιπο Ether (balance), καθώς και μια δομή ονόματι αποθήκη (storage), η οποία λειτουργεί ως μνήμη. Τέλος, υπάρχει ένα προαιρετικό πεδίο, κώδικας συμβολαίου (contract code), το οποίο αφορά λογαριασμούς που πρακτικά είναι συμβόλαια. [17]

Είναι σημαντικό να σημειωθεί πως τα συμβόλαια, είναι επίσης λογαριασμοί, δηλαδή έχουν το δικό τους υπόλοιπο Ether. Οι κλασικοί λογαριασμοί που έχουμε δει στο Bitcoin, λογαριασμοί δηλαδή που διαχειρίζονται με δημόσια και ιδιωτικά κλειδιά, ονομάζομαι εξωτερικοί (external) λογαριασμοί, ενώ τα συμβόλαια ονομάζομαι συμβολικοί (contract) λογαριασμοί, τα οποία διαχειρίζονται από τον κώδικα (contract code) τους. [17]

4.2 Συναλλαγές και Μηνύματα

4.2.1 Συναλλαγές

Οι συναλλαγές στο Ethereum είναι στην ουσία πακέτα τα οποία περιέχουν μια πληροφορία που αποστέλλεται από ένα εξωετερικό λογαριασμό. Συγκεκριμένα, περιέχουν

- Τη διεύθυνση του παραλήπτη - Την υπογραφή του αποστολέα - Το ποσό Ether προς αποστολή - Ένα προαιρετικό πεδίο δεδομένων (data field) - Ένα πεδίο 'STARTGAS' το οποίο συμβολίζει το μέγιστο αριθμό υπολογιστικών βημάτων που μπορεί να εκτελέσει η συναλλαγή - Ένα πεδίο 'GASPRICE' το οποίο συμβολίζει το κόστος σε Ether κάθε υπολογιστικού βήματος

Τα πεδία 2 τελευταία πεδία είναι κομβικά, καθώς προστατεύουν το δίκτυο από επιθέσεις anti-denial, καθώς και ατέρμωνους βρόγχους. Το κόστος ονομάζεται gas, δηλαδή καύσιμο, καθώς αυτό χρειάζεται για την εκτέλεση του κώδικα. Οι περισσότερες εντολές απαιτούν 1 gas, αλλά αυτό δεν

είναι σταθερό, καθώς εντολές που είναι πιο σύνθετες, έχουν και μεγαλύτερο κόστος. Υπάρχει επίσης, ένα κόστος αξίας 5 gas, για κάθε byte πληροφορίας που εμπεριέχεται σε μια συναλλαγή. Το κίνητρο του κόστους είναι η προστασία από επιθέσεις, καθώς οι κακόβουλοι χρήστες θα πρέπει να πληρώνουν για κάθε πόρο που καταναλώνουν. [17]

4.2.2 Μηνύματα

Αντιθέτως, οι συναλλαγές που παράγονται από συμβόλαια, ονομάζομαι μηνύματα. Τα πεδία είναι τα ίδια, με μόνη διαφορά την αφαίρεση του πεδίου 'GASPRICE'

4.3 Εισαγωγή στα Έξυπνα Συμβόλαια

Ο κώδικας των συμβολαίων συντάσσεται σε Solidity, μια αντικειμενοστρεφής γλώσσα προγραμματισμού υψηλού επιπέδου η οποία μεταγλωττίζεται σε γλώσσα EVM (Ethereum Virtual Machine), μια γλώσσα χαμηλού επιπέδου. Οι διαθέσιμες εντολές έχουν προσβάση σε 3 χώρους

- Το 'stack', ένας τελευταίος-μέσα-πρώτος-έξω (last-in-first-out) χώρος όπου τιμές μπορούν να εισαχθούν και να αφαιρεθούν - Τη μνήμη 'memory' , μορφής bytearray - Τον μακροχρόνιο αποθηκευτικό χώρο του συμβολαίου, ακολουθώντας τη δομή κλειδί/τιμή. Σε αντίθεση με τη μνήμη και την στάκα των οποίων η πληροφορία διαγράφεται με την ολοκλήρωση μιας εκτέλεσης, αυτός ο χώρος διατηρείται. [17]

Η εκτέλεση του κώδικα, από τη μεριά υποδομής, είναι αρκετά απλή. Ο κώδικας εκτελείται από κάθε κόμβο που επαληθεύει το μπλοκ που εμπεριέχεται το σχετικό μήνυμα.

4.3.1 Κουπόνια - Tokens

Η ευελιξία των συμβολαίων επιτρέπει τη δημιουργία πληθώρων εφαρμογών σε διάφορους τομείς, από ιατρικούς μέχρι χρηματιστηριακών. Η πιο χαρακτηριστική εφαρμογή είναι αυτή της ιδιοκτησίας όπως έχουμε δει με τα NFT (Non-Fungible Tokens), όπου μια πληροφορία (για παράδειγμα ένα ηλεκτρονικό έργο τέχνης) μπορεί να ανήκει σε ένα λογαριασμό. Τέτοια κουπόνια, μπορούν να είναι μέχρι μετοχές μιας εταιρίας, καθώς αυτή μπορεί να δημιουργήσει το δικό της νόμισμα, βασίζοντας στην ασφάλεια, το κύρος και την αποκεντροποίηση ενός δικτύου, όπως το Ethereum. Έτσι, συνήθως το νομίσματα ενός δικτύου αποτελούν ηλεκτρονική νομισματική αξία, τα tokens αντιθέτως μπορούν να αποτελούν ιδιοκτησία μιας πληροφορίας ή ενός δικαιώματος. Για παράδειγμα, κάτοχοι NFT της συλλογής bored apes, είχαν πρόσβαση σε ένα πάρτυ με βάρκες στην Αμερική. [18]

ERC-20 Πρωτόκολλο Καθώς κάποιες χρήσης κουπονιών επαναλαμβάνονται, δημιουργούνται μοτίβα στις σχετικές ανάγκες. Για αυτό το σκοπό, δημιουργήθηκε μια κοινή διεπαφή, το ERC-20 πρωτόκολλο, το οποίο είναι ένα σύνολο κανόνων (για παράδειγμα μέθοδοι συγκεκριμένων υπογραφών) που πρέπει να περιέχει ένα κουπόνι. [18]

```solidity
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.17;

// https://github.com/OpenZeppelin/openzeppelin-contracts/blob/v3.0.0/contracts/token/ERC20/IERC20.sol
interface IERC20 {
    function totalSupply() external view returns (uint);

    function balanceOf(address account) external view returns (uint);

    function transfer(address recipient, uint amount) external returns (bool);

    function allowance(address owner, address spender) external view returns (uint);

    function approve(address spender, uint amount) external returns (bool);

    function transferFrom(
        address sender,
        address recipient,
        uint amount
    ) external returns (bool);

    event Transfer(address indexed from, address indexed to, uint value);
    event Approval(address indexed owner, address indexed spender, uint value);
}
```

Σχήμα 4.1: ERC-20 Interface

Κεφάλαιο 5ο: Έξυπνα Συμβόλαια

Όπως είδαμε, τα έξυπνα συμβόλαια αποτελούν μια ισχυρή καινοτομία που αξιοποιεί τις δυνατότητες της τεχνολογίας αλυσίδων για τη δημιουργία αυτοεκτελούμενων, αδιάψευστων και διαφανών συμβολαίων, χωρίς την ανάγκη μεσάζοντες ή κεντρικού ελέγχου. Στον πυρήνα του, ένα έξυπνο συμβόλαιο είναι ένα κομμάτι κώδικα που εκτελεί αυτόματα και επιβάλλει τους όρους μιας συμφωνίας όταν πληρούνται προκαθορισμένες προϋποθέσεις. Αυτοί οι όροι κωδικοποιούνται στη σύμβαση και αφού ικανοποιηθούν, οι ενέργειες της σύμβασης ενεργοποιούνται χωρίς καμία χειροκίνητη παρέμβαση. Αυτός ο αυτοματισμός εξαλείφει την ανάγκη για παραδοσιακούς μεσάζοντες, όπως τράπεζες, δικηγόρους ή μεσίτες, μειώνοντας σημαντικά το σχετικό κόστος, τις καθυστερήσεις και την πιθανότητα ανθρώπινου λάθους. Αυτή η τεχνολογία έχει τη δυνατότητα να αναδιαμορφώσει τις βιομηχανίες, να εξορθολογίσει τις διαδικασίες και να ενισχύσει την εμπιστοσύνη σε διάφορους τομείς.

5.1 Βασικές αρχές

5.1.1 Εμπιστοσύνη και ασφάλεια

Η εμπιστοσύνη και η διαφάνεια είναι θεμελιώδεις πυλώνες των έξυπνων συμβολαίων, που διαδραματίζουν καθοριστικό ρόλο στην ευρεία υιοθέτησή τους και τον μετασχηματιστικό αντίκτυπό τους σε διάφορους κλάδους. Αυτές οι αρχές επιτυγχάνονται χάρη στα παρακάτω [17]

Αμετάβλητο Ιστορικό Μόλις αναπτυχθεί ένα έξυπνο συμβόλαιο, ο κώδικας και το ιστορικό εκτέλεσής του καταγράφονται στην αλυσίδα. Αυτό δημιουργεί ένα αμετάβλητο και αδιάψευστο αρχείο του κύκλου ζωής του συμβολαίου, καθιστώντας εξαιρετικά δύσκολη την αλλαγή ή τη χειραγώγηση προηγούμενων συναλλαγών. Αυτό το χαρακτηριστικό ενισχύει την εμπιστοσύνη διασφαλίζοντας ότι οι όροι της σύμβασης δεν μπορούν να αλλάξουν αφού έχουν συμφωνηθεί.

Δημόσια επαλήθευση Οι αλυσίδες είναι ανοιχτές και προσβάσιμες σε οποιονδήποτε. Αυτό σημαίνει ότι όλοι οι συμμετέχοντες σε ένα δίκτυο έξυπνων συμβολαίων μπορούν να επαληθεύσουν ανεξάρτητα τους όρους και την εκτέλεση μιας σύμβασης. Οι συναλλαγές είναι δημόσια ορατές, επιτρέποντας στα μέρη να παρακολουθούν τη ροή των περιουσιακών στοιχείων, τις αλλαγές στην ιδιοκτησία και άλλες σχετικές πληροφορίες. Αυτή η διαφάνεια ενισχύει την εμπιστοσύνη μεταξύ των συμμετεχόντων, καθώς καμία μεμονωμένη οντότητα δεν έχει τον αποκλειστικό έλεγχο των δεδομένων ή των αποτελεσμάτων.

Αποκεντροποίηση Οι παραδοσιακές εφαρμογές βασίζονται σε κεντρικούς μεσάζοντες για την επίβλεψη και την επιβολή των συμφωνιών. Τα έξυπνα συμβόλαια, από την άλλη πλευρά, λειτουργούν με αποκεντρωμένο τρόπο, χωρίς ενιαίο σημείο ελέγχου. Αυτή η αποκέντρωση εξαλείφει την ανάγκη εμπιστοσύνης σε μια ενιαία αρχή και μειώνει την πιθανότητα μεροληψίας ή χειραγώγησης.

Αυτοματοποιημένη Εκτέλεση Η αυτοματοποίηση των έξυπνων συμβολαίων διασφαλίζει ότι οι όροι μιας συμφωνίας εκτελούνται ακριβώς όπως έχουν προγραμματιστεί. Αυτό εξαλείφει την ανάγκη για χειροκίνητη επιβολή, μειώνοντας την πιθανότητα ανθρώπινου λάθους ή μεροληψίας. Τα μέρη μπορούν να εμπιστεύονται ότι η σύμβαση θα εκτελεστεί όπως προβλέπεται, χωρίς να βασίζονται στην υποκειμενική ερμηνεία ενός διαμεσολαβητή.

Πρωτόκολλα Πολλές πλατφόρμες αλυσιδών συμμορφώνονται με πρωτόκολλα για την ανάπτυξη και εκτέλεση έξυπνων συμβολαίων. Αυτά τα πρωτόκολλα διασφαλίζουν ότι οι συμβάσεις είναι ομοιόμορφες και διαλειτουργικές σε διαφορετικές πλατφόρμες, ενισχύοντας την εμπιστοσύνη παρέχοντας συνεπή συμπεριφορά και μειώνοντας την πιθανότητα απροσδόκητων αποτελεσμάτων.

5.1.2 Ακρίβεια

Προκαθορισμένοι και σαφείς όροι Τα έξυπνα συμβόλαια προγραμματίζονται με ακριβείς οδηγίες που δεν αφήνουν περιθώρια ερμηνείας ή ασάφειας. Οι όροι και οι προϋποθέσεις της σύμβασης ορίζονται με σαφήνεια στον κώδικα, διασφαλίζοντας ότι όλα τα εμπλεκόμενα μέρη έχουν κοινή κατανόηση του τι αναμένεται. Αυτό εξαλείφει την πιθανότητα παρεξηγήσεων που μπορεί να προκύψουν από ασαφή γλώσσα στις παραδοσιακές εφαρμογές.

Παρακολούθηση πραγματικού χρόνου Οι συμμετέχοντες μπορούν να παρακολουθούν την εκτέλεση της αποκεντροποιημένης εφαρμογής σε πραγματικό χρόνο. Αυτό επιτρέπει στα μέρη να παρακολουθούν την εκπλήρωση των όρων και την πρόοδο του συμβολαίου, ενισχύοντας τη διαφάνεια και διασφαλίζοντας ότι όλα τα μέρη γνωρίζουν την κατάσταση της σύμβασης ανά πάσα στιγμή.

Πρόληψη σφαλμάτων και επικύρωση Τα έξυπνα συμβόλαια περιλαμβάνουν μηχανισμούς επικύρωσης για να διασφαλίσουν ότι τα δεδομένα εισόδου πληρούν προκαθορισμένα κριτήρια πριν από

την εκτέλεση. Αυτό αποτρέπει την εκτέλεση της σύμβασης με μη έγκυρα ή εσφαλμένα δεδομένα, ενισχύοντας περαιτέρω την ακρίβεια. Για παράδειγμα, ένα έξυπνο συμβόλαιο για μια οικονομική συναλλαγή μπορεί να περιλαμβάνει ελέγχους για την επαλήθευση της διαθεσιμότητας υπολοίπου πριν ολοκληρωθεί.

Μειωμένος κίνδυνος διαμεσολάβησης Οι παραδοσιακές εφαρμογές συνήθως περιλαμβάνουν μεσάζοντες που επιβλέπουν και επικυρώνουν τους όρους και τις προϋποθέσεις. Αυτοί οι μεσάζοντες μπορούν να κάνουν λάθος ή να παρουσιάσουν αποτελέσματα με αποκλίσεις. Τα έξυπνα συμβόλαια ελαχιστοποιούν τη συμμετοχή των ενδιάμεσων, μειώνοντας την πιθανότητα σφαλμάτων που προκαλούνται από αλληλεπιδράσεις τρίτων.

Έξυπνα Μαντεία (Smart Oracles) Ορισμένα συμβόλαια χρησιμοποιούν εξωτερικές πηγές δεδομένων γνωστές ως μαντεία για να τροφοδοτήσουν πληροφορίες πραγματικού κόσμου και χρόνου στην εφαρμογλη. Αυτοί οι πάροχοι παρέχουν ακριβή και ενημερωμένα δεδομένα, διασφαλίζοντας ότι οι όροι της σύμβασης βασίζονται σε ακριβείς πληροφορίες από τον πραγματικό κόσμο. Αυτό ενισχύει την ακρίβεια της λήψης αποφάσεων στο πλαίσιο της σύμβασης.

5.1.3 Παγκόσμια προσβασιμότητα

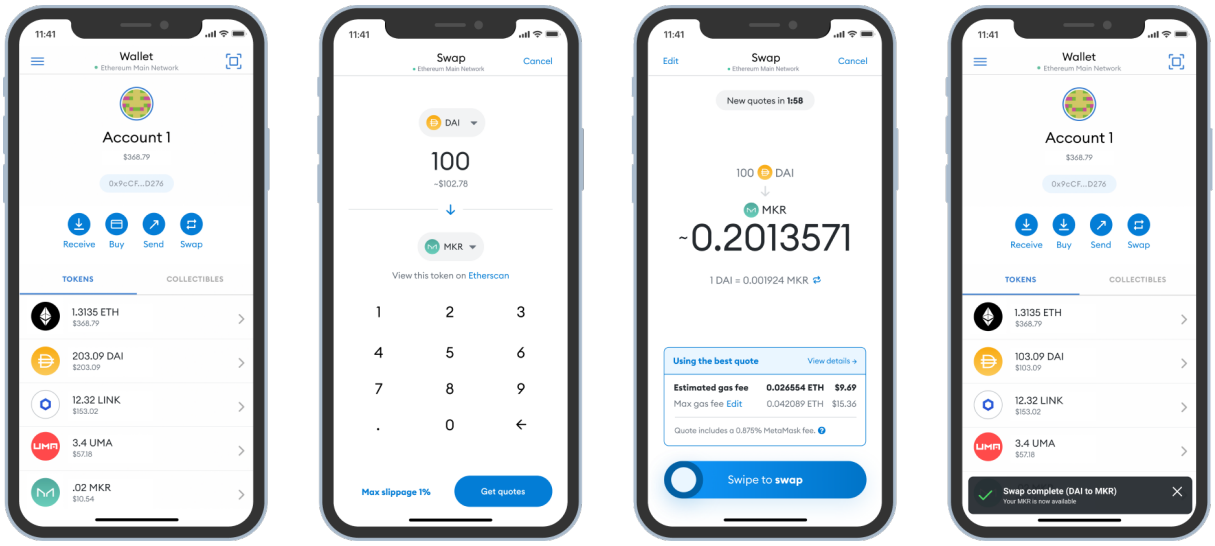
Οποιοσδήποτε έχει πρόσβαση στο διαδίκτυο, έχει πρόσβαση και στην εκτέλεση μιας αποκεντοποιημένης εφαρμογής. Έτσι επιτρέπεται η συνεργασία από διαφορετικά μέρη του κόσμου χωρίς γεωγραφικά εμπόδια. [7]

5.2 Καινοτομία και Επιχειρηματικά μοντέλα

5.2.1 Αποκεντροποιημένη Οικονομία - Decentralized Finance (DeFi)

Πλατφόρμες DeFi επιτρέπουν χρηματοοικονομικές υπηρεσίες, όπως δανεισμό και ανταλλαγή χωρίς την ανάγκη παραδοσιακών χρηματοοικονομικών ενδιάμεσων. Τα έξυπνα συμβόλαια αυτοματοποιούν τα πρωτόκολλα δανεισμού και δανεισμού και οι χρήστες μπορούν να συμμετέχουν σε χρηματοοικονομικές δραστηριότητες απευθείας από τα ψηφιακά τους πορτοφόλια, ανοίγοντας νέες ευκαιρίες για τη δημιουργία και τη διαχείριση πλούτου.

Metamask Το Metamask είναι ένα ψηφιακό πορτοφόλι που επιτρέπει στους χρήστες να αλληλεπιδρούν με το δίκτυο του Ethereum και τα συμβόλαια του. Πέρα από πορτοφόλι, υποστηρίζεται και ένα αποκεντροποιημένο ανταλλακτήριο (Decentralized Exchange - DEX) μέσω του οποίου ένας χρήστης μπορεί να ανταλλάξει νομίσματα ERC-20. Η ίδια εφαρμογή, αλληλεπιδρά με άλλα DEX του δικτύου έτσι ώστε να προτείνεται η καλύτερη δυνατή τιμή στο χρήστη. [2]



Σχήμα 5.1: Ανταλλαγή νομισμάτων στο Metamask [2]

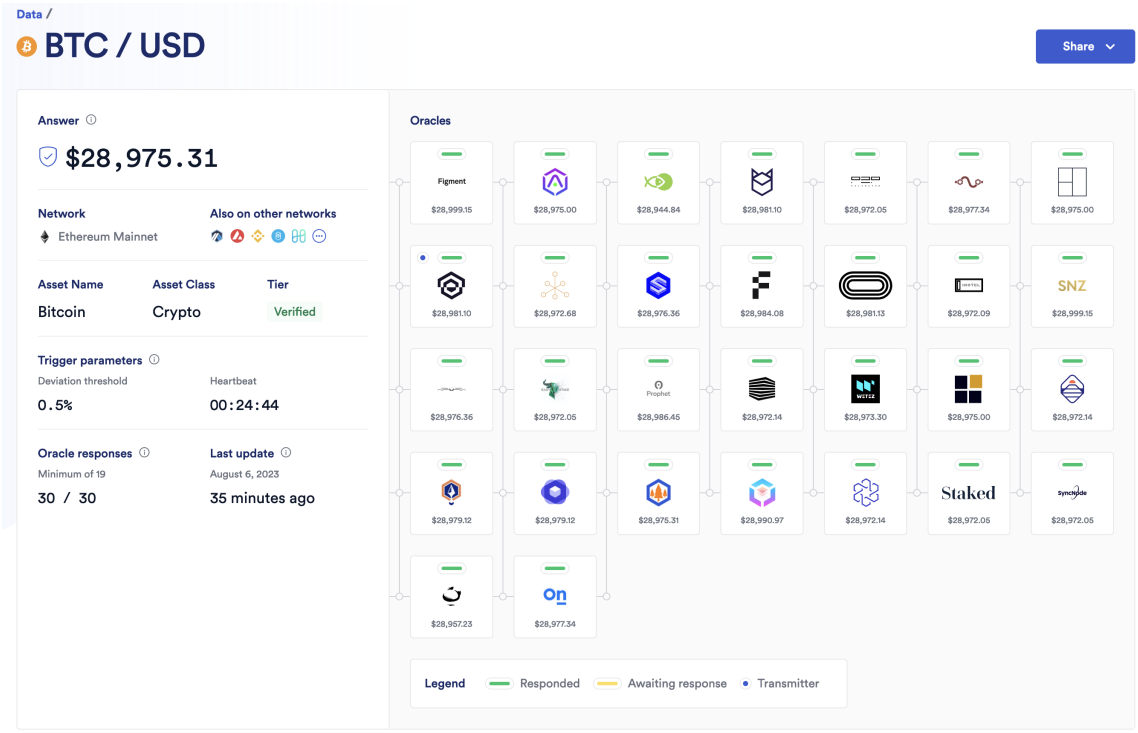
5.2.2 Έξυπνα Μαντεία (Oracles)

Καθώς τα συμβόλαια και σε προέκταση οι αλυσίδες δεν έχουν επικοινωνία με τον πραγματικό κόσμο, έχουν δημιουργηθεί κάποια ειδικά συμβόλαια που καλούνται μαντεία, στα οποία μπορεί να αποθηκευτεί πληροφορία ενώ η ανάγνωση τους είναι υπό πληρωμή, αμοίβοντας τον πάροχο της πληροφορίας. Αυτού του είδους η οικονομία, δίνει σε την ευκαιρία σε διάφορες εταιρίες αλλά και άτομα να νομισματοποιήσουν τις πληροφορίες τους και να αμοιφθούν για αυτές. Το ειδικό συμβόλαιο ακούει αιτήματα δεδομένων από άλλα συμβόλαια, αναμεταδίδει ερωτήματα δεδομένων σε κόμβους μαντείων και εκπέμπει δεδομένα που στέλνονται στους αιτούντες. [19]

Chainlink Το Chainlink είναι η δημοφιλέστερη πλατφόρμα μαντείων, η οποία γεφυρώνεται με διάφορα δίκτυα πέρα από το Ethereum, παρέχοντας πληροφορίες σε πολλαπλές αλυσίδες. Καθώς παρέχουν πολλά μαντεία, πλέον παρέχουν και μια ακόμη υπηρεσία, τις ροές δεδομένων, όπου μια πληροφορία, για παράδειγμα η τιμή του Bitcoin σε δολλάριο, υπολογίζεται από το μέσο όρο συγκεκριμένων μαντειών. Έτσι, σε περίπτωση που κάποιο μαντείο υπολογίσει λάθος τιμή, η έξοδος της ροής δεν θα αποκλίσει πολύ από την πραγματικότητα. Παράλληλα, παρέχεται και ένα σύστημα αξιολόγησης όπου διάφοροι πάροχοι μαντειών αξιολογούνται για την ακρίβεια των αποτελεσμάτων τους. [20]

5.2.3 Κουπόνια (Tokenization) και NFT

Τα έξυπνα συμβόλαια επέτρεψαν τη δημιουργία και τη διαχείριση μη ανταλλάξιμων κουπονιών (NFT), τα οποία αντιπροσωπεύουν την ιδιοκτησία μοναδικών ψηφιακών στοιχείων όπως έργα τέχνης, μουσική και τα εικονικά ακίνητα. Διαπραγματεύονται σε πλατφόρμες αλυσιδών, επιτρέποντας στους δημιουργούς να εισπράτουν έσοδα από τις ψηφιακές δημιουργίες τους και στους θαυμαστές να κατέχουν και να εμπορεύονται ψηφιακά στοιχεία με νέους και καινοτόμους τρόπους.



Σχήμα 5.2: Ροή δεδομένων ζεύγους BTC-USD, υπολογισμένο από 30 μαντεία

OpenSea το OpenSea είναι η μεγαλύτερη και μία από τις πιο γνωστές αποκεντρωμένες αγορές για αγορά, πώληση και διαπραγμάτευση μη ανταλλάξιμων κουπονιών (NFT).

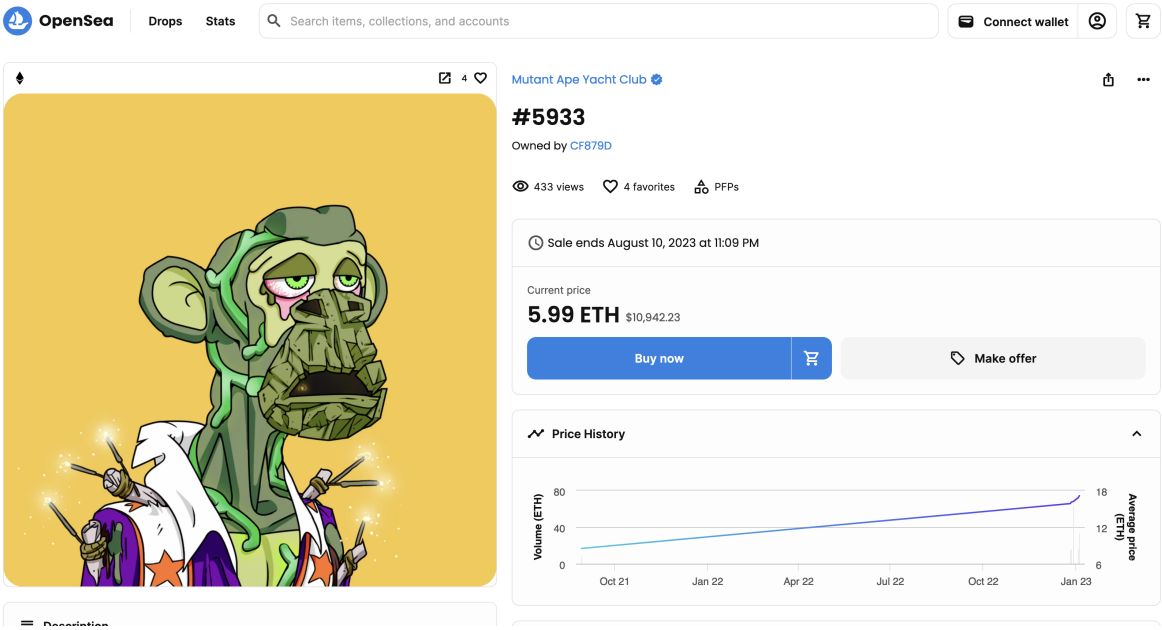
5.2.4 Αυτοματοποιημένες Εφοδιαστικές Αλυσίδες

Τα έξυπνα συμβόλαια μπορούν να χρησιμοποιηθούν για τη δημιουργία αυτοματοποιημένων συστημάτων διαχείρισης εφοδιαστικής αλυσίδας. Αυτά τα συστήματα επιτρέπουν την παρακολούθηση των αγαθών σε πραγματικό χρόνο και την αυτοματοποιημένη διαχείριση αποθεμάτων. Μέσω των συμβολαίων, μπορούν να ενεργοποιηθούν αυτόματα αιτήματα αναπαραγγελίας, ενώ παράλληλα μπορεί εύκολα να επαληθευτεί η αυθεντικότητα του προϊόντος χάρη στη διαφάνεια των αλυσιδών.

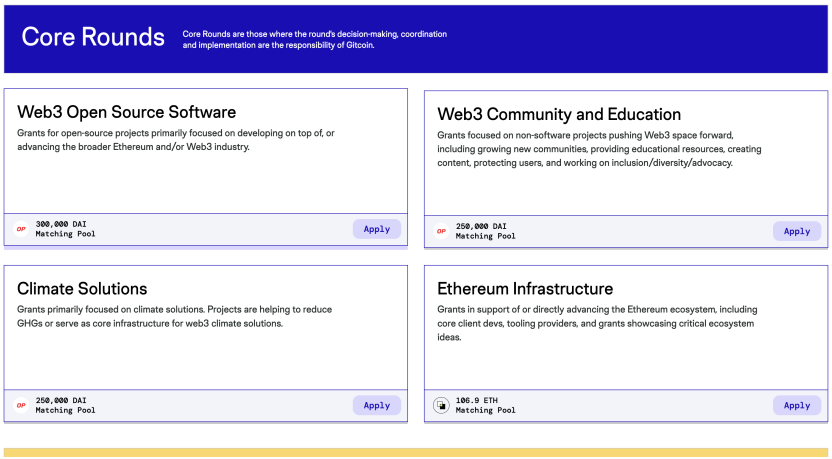
Αλυσίδα Αυτοματοποιημένων Εφοδίων της IBM Η εταιρία IBM ανέπτυξε μια πλατφόρμα αυτοματοποιημένων εφοδίων με βάση τις υποδομές των αλυσίδων συστοιχιών, την τεχνητή νοημοσύνη και το Διαδίκτυο των Πραγμάτων. Μέσω διεπαφών (API), διάφοροι πάροχοι μπορούν να συνδεθούν στην πλατφόρμα και να ανεβάσουν τα δεδομένα τους. [21]

5.2.5 Συλλογική χρηματοδότηση (Crowdfunding) και Αρχική Προσφορά Νομίσματος (Initial Coin Offering - ICO)

Νέες εταιρίες τύπου startups, μπορούν να παράξουν το δικό τους νόμισμα και να το προσφέρουν στους επενδυτές ως μετοχές.



Σχήμα 5.3: Ιστοσελίδα OpenSea

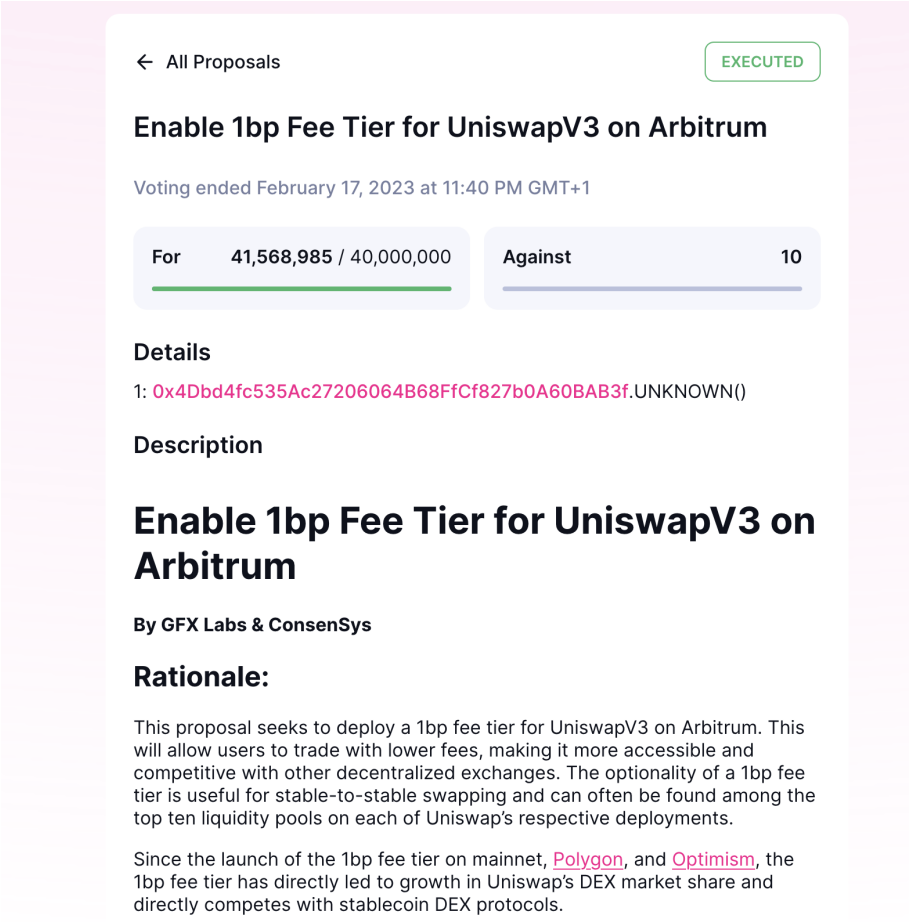


Σχήμα 5.4: Gitcoin Grants - https://grants.gitcoin.co

Gitcoin το Gitcoin είναι μια πλατφόρμα η οποία έχει σκοπό να φέρει κοντά εταιρίες, προγραμματιστές και σχεδιαστές στα πλαίσια του ανοιχτού κώδικα. Οι συντηρητές μιας εφαρμογής μπορούν να δημιουργήσουν αμοιβές σε όσους συνεισφέρουν, για παράδειγμα με την επίλυση ενός σφάλματος στον κώδικα. Επιπλέον, καθώς ο ανοιχτός κώδικας μπορεί να χρησιμοποιηθεί από οποιονδήποτε, οποιοσδήποτε μπορεί να χρηματοδοτήσει μια αμοιβή για την επίλυση ή επέκταση μιας εφαρμογής. Παράλληλα, υπάρχει μια ξεχωριστή εφαρμογή, η Gitcoin grants, στην οποία εταιρίες ανάπτυξης εφαρμογών αλυσίδων συστοιχειών μπορούν να κάνουν αίτηση για χρηματοδότηση.

5.2.6 Έξυπνες Μεσιτικές Ιδιοκτησίες

Οι συναλλαγές ακινήτων μπορούν να διευκολυνθούν μέσω έξυπνων συμβολαίων, επιτρέποντας αυτοματοποιημένες μεταβιβάσεις ακινήτων, συμφωνίες ενοικίασης, ακόμη και διαχείριση ακινήτων. Τα έξυπνα συμβόλαια μπορούν να βοηθήσουν στη μείωση της γραφειοκρατίας, στον εξορθολογισμό των



Σχήμα 5.5: Ψηφοφορία για την ύπαρξη φόρου

συναλλαγών ακινήτων και στην παροχή μεγαλύτερης διαφάνειας στις συμφωνίες ακινήτων.

5.2.7 Αποκεντροποιημένοι και Αυτόνομοι Οργανισμοι - Decentralized Autonomous Organizations (DAOs)

Τα DAO είναι οργανισμοί που διέπονται από έξυπνα συμβόλαια τα οποία επιτρέπουν την αποκεντρωμένη λήψη αποφάσεων, όπου οι συμμετέχοντες μπορούν να ψηφίσουν και να επηρεάσουν την κατεύθυνση του οργανισμού.

Uniswap Το Uniswap είναι ένα αποκεντροποιημένο ανταλλακτήριο το οποίο καθορίζεται από τους χρήστες του. Ιδιοκτήτες του UNI token, μπορούν να ψηφίσουν για το μέλλον του ανταλλακτηρίου. Για παράδειγμα, οι χρήστες μπορεί να ζητηθούν να ψηφίσουν για αλλαγές στους φόρους του δικτύου, δηλαδή στις επιβραβεύσεις.

5.2.8 Ασφαλής Επαλήθευση Ιδιοκτησίας - Secure Identity Verification

Τα έξυπνα συμβόλαια μπορούν να χρησιμοποιηθούν για ασφαλείς και επαληθεύσιμες λύσεις ψηφιακής ταυτότητας. Αυτό θα μπορούσε να φέρει επανάσταση σε κλάδους που απαιτούν ισχυρή επαλήθευση

ταυτότητας, όπως η ηλεκτρονική τραπεζική, η υγειονομική περίθαλψη και οι κρατικές υπηρεσίες, παρέχοντας στα άτομα τον έλεγχο των δεδομένων ταυτότητάς τους.

Chainlink Deco Το DECO είναι ένα πρωτόκολλο της Chainlink, μιας πλατφόρμας μαντειών το οποίο δίνει τη δυνατότητα σε έναν χρήστη να αποδείξει την αυθεντικότητα των δεδομένων χωρίς να αποκαλύψει τα ίδια τα δεδομένα. Η αυθεντικότητα, σε αυτό το πλαίσιο, σημαίνει ότι τα δεδομένα λαμβάνονται από έναν συγκεκριμένο διακομιστή ιστού μέσω του πρωτοκόλλου TLS. Για παράδειγμα, ένας χρήστης μπορεί να αποδείξει ότι έλαβε την οικονομική της αναφορά από την ιστοσελίδα της τράπεζάς της και ότι, σύμφωνα με αυτήν την αναφορά, το υπόλοιπο του λογαριασμού της υπερβαίνει ένα συγκεκριμένο ποσό. Ωστόσο, δεν αποκαλύπτει άλλες πληροφορίες που υπάρχουν στην αναφορά, όπως τον αριθμό λογαριασμού ή το ακριβές υπόλοιπό της. [22]

5.2.9 Προγραμματισμένα Κεφάλαια

Τα έξυπνα συμβόλαια επιτρέπουν προγραμματιζόμενα χρήματα, όπου τα κεφάλαια μπορούν να διανεμηθούν και να κατανεμηθούν αυτόματα βάσει προκαθορισμένων συνθηκών. Αυτό έχει εφαρμογές στις συνδρομητικές υπηρεσίες, στη μισθοδοσία των εργαζομένων και σε κάθε σενάριο όπου οι πληρωμές πρέπει να εκτελούνται σύμφωνα με συγκεκριμένους κανόνες ενεργοποίησης.

Οικονομία των Πραγμάτων - Economy of Things (EOT) Η Οικονομία των Πραγμάτων είναι μια αποκεντρωμένη δικτυακή οικονομία που χτίστηκε και ανήκει στους ανθρώπους και τις μηχανές που τη χρησιμοποιούν. Στην Οικονομία των Πραγμάτων, τα συνδεδεμένα συστήματα νομισματοποιούν την αξία που δημιουργούν, καθιστώντας ολοένα και πιο αυτόνομα και οικονομικά ανεξάρτητα. Η οικονομία των πραγμάτων στηρίζεται σε 3 τεχνολογίες:

- Διαδίκτυο των πραγμάτων: Επιτρέπεται η σύνδεση μικροσυσκευών στο διαδίκτυο
- Τεχνητή Νοημοσύνη: Αυτοματοποίηση
- Αλυσίδες συστοιχιών: Επιτρέπουν στα συστήματα να γίνουν οικονομικά ανεξάρτητα

Για παράδειγμα, τα αυτόνομα ηλεκτρονικά αυτοκίνητα θα οδηγούνται μόνα τους στο σταθμό φόρτισης, θα διαπραγματεύονται μια τιμή, θα φορτιστούν και στη συνέχεια θα πραγματοποιήσουν την πληρωμή. Η πληρωμή θα κατανεμηθεί απευθείας και θα μεταφερθεί σε όλα τα συμβαλλόμενα μέρη σύμφωνα με ένα προκαθορισμένο κλειδί. Λόγου χάρη, 70% στον πάροχο ηλεκτρικής ενέργειας και από 10% στον κατασκευαστή του σταθμού φόρτισης, στον χειριστή του πρατηρίου καυσίμων και στον κατασκευαστή του αυτοκινήτου.

Κεφάλαιο 6ο: Στρώματα Αλυσίδων

Για την επεκτασιμότητα των δικτύων, έχει εγκαθιδρυθεί η ορολογία των στρωμάτων. Η ιδέα στηρίζεται στο ότι μια αλυσίδα μπορεί να ξεκινάει από μια άλλη αλυσίδα, χρησιμοποιώντας την ασφάλεια της πρώτης όπου χρειάζεται (μέσω της μεγάλης αποκεντροποίησης) υιοθετώντας τον απαιτούμενο φόρτο μακρία από αυτήν, έτσι ώστε το συνολικό δίκτυο να γίνει γρηγορότερο αλλά και φθηνότερο. Στρώματα που είδαμε μέχρι τώρα, όπως το Bitcoin και το Ethereum, είναι στρώματα επιπέδου 1.

6.1 Στρώμα 2

Είδαμε πως ένα δίκτυο μπορεί να επεκταθεί με διάφορες ενημερώσεις, παρόλα αυτά η ταχύτητα αυτών των ενημερώσεων μπορεί να είναι αργή, ενώ κάποιοι περιορισμοί μπορεί να μην λύνονται τόσο εύκολα.

Η ύπαρξη των συμβολαίων, επιτρέπει τη γέννηση αλυσιδών μέσα σε μια αλυσίδα. Εικονικά, μπορούμε να φανταστούμε μια αλυσίδα η οποία αναπτύσσεται σε μια άλλη διάσταση, ή ένα άλλο στρώμα. Στην ουσία, οι αλυσίδες δευτέρου επιπέδου επιτρέπουν την επέκταση ενός δικτύου χωρίς τη παραμετροποίηση αυτού. Είναι συμβατά δηλαδή, με όλη την αρχιτεκτονική του δικτύου στο οποίο στηρίζονται.

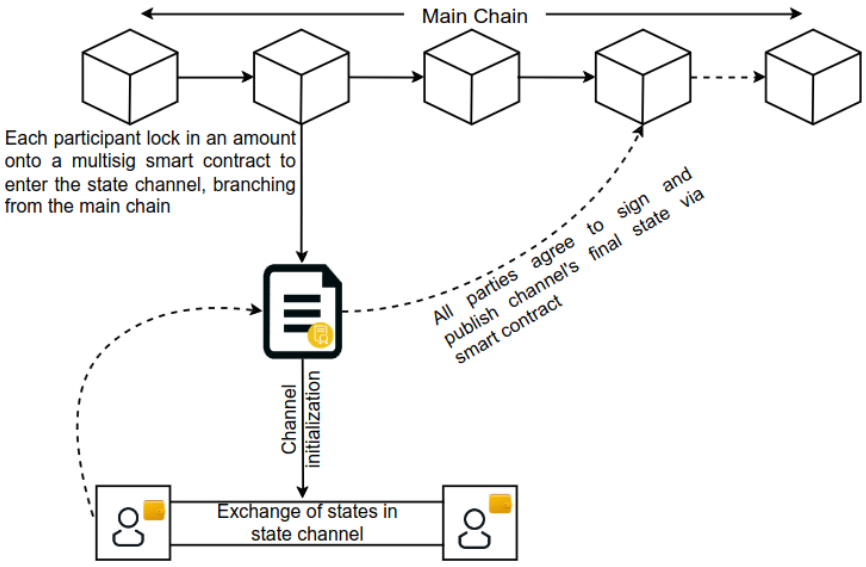
Το κύριο χαρακτηριστικό αυτών των δικτύων είναι πως δεν εκπέμπουν (broadcast) κάθε συναλλαγή στο κύριο δίκτυο, αλλά στην ουσία επιτρέπουν συναλλαγές εκτός αυτού (off-chain) μέσω ενός πιστοποιημένου συστήματος. Συνεπώς, ο φόρτος του πρώτου στρώματος μειώνεται σημαντικά. [3]

Σε αυτή την ενότητα θα παρουσιάσουμε τις 3 κύριες εναλλακτικές λύσεις επιπέδου 2.

6.1.1 Κανάλια - Channels

Τα κανάλια, είναι ένα είδος πρωτοκόλλου που επιτρέπουν 2 άκρες να επικοινωνήσουν με ένα ιδιωτικό κανάλι επικοινωνίας. Σκοπός είναι η αποφόρτωση του δικτύου με όσο το δυνατόν περισσότερη ασφάλεια. Για την επιτυχία του, ένα σύνολο κανόνων είναι ορισμένο πριν τη λειτουργία ενός τέτοιου καναλιού. Υπάρχουν 2 κύρια είδη καναλιών, σε πληρωμής (payment) και κατάστασης (state).

Κανάλια Κατάστασης - State Channels Σκοπό έχουν την εκτέλεση μιας εφαρμογής μεταξύ 2 ή περισσότερων ακρών, λόγου χάρη ενός συμβολαίου σε μειωμένο χρόνο με ελάχιστους φόρους. Συνήθως, ένα κανάλι χτίζεται πάνω σε υπογραφές κατωφλιού (threshold) - αλλιώς και multisig - καθώς επίσης συμπεριλαμβάνονται χρονικά κλειδώματα (timelocks) σε περίπτωση καθυστέρησης κάποιας άκρης. Κάθε άκρη υπογράφει κλειδώνοντας ένα ποσό, το οποίο, μέσω του έξυπνου συμβολαίου που στηρίζεται το δοθέν κανάλι, ενημερώνει τους λογαριασμούς κάθε μέλους ανάλογα με κάθε νέα κατάσταση. Η νέα κατάσταση μπορεί να προταθεί από οποιοδήποτε μέλος, όπου τα υπόλοιπα οφείλουν να επαληθεύσουν. Σε ένα ιδανικό σενάριο, υπάρχουν 2 φόροι που πρέπει να πληρωθούν, η λειτουργία ενός καναλιού καθώς ενημερώνει το κύριο δίκτυο ότι λειτουργεί με τους τάδε συμμετέχοντες, καθώς επίσης και το κλείσιμο ενός καναλιού, όπου η με τη λήξη του επιστρέφονται στα μέλη τα ποσά που τους αντιστοιχούν. [3]



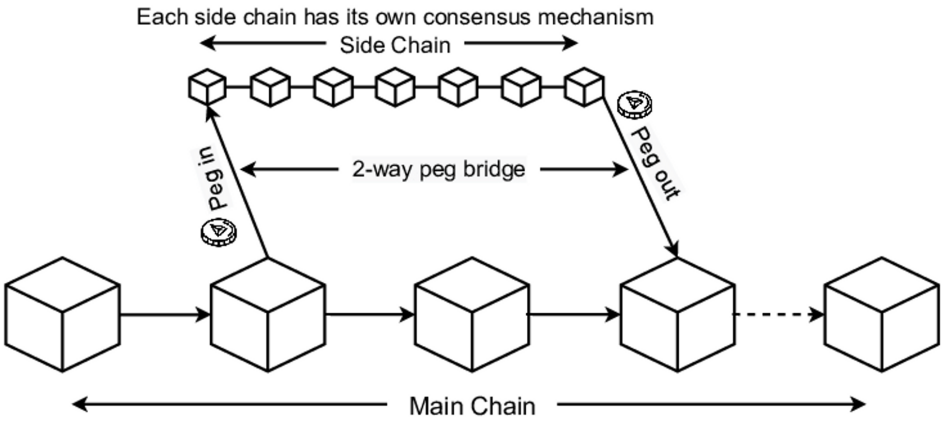
Σχήμα 6.1: κανάλι κατάστασης [3]

Ένα δίκτυο που επιτρέπει τα κανάλια κατάστασης, είναι το δίκτυο της Aeternity. Για παράδειγμα, μπορούμε να φανταστούμε το παιχνίδι πέτρα-ψαλίδι-χαρτί. Οι κανόνες του παιχνιδιού δομούνται σε ένα συμβόλαιο μέσα στο οποίο συμμετέχουν 2 πλευρές, όπου κάθε πλευρά κλειδώνει ένα ποσό. Το παιχνίδι κομματιάζεται σε φάσεις: Αρχή νέου γύρου, αναμονή για τις επιλογές των παιχτών καθώς και την εμφάνιση των αποτελεσμάτων. Για κάθε φάση υπάρχει και μια κατάσταση, για παράδειγμα το ποσό του στοιχήματος για το γύρο, την επιλογή του κάθε παίχτη και το νικητή. Σε οποιαδήποτε στιγμή ένας χρήστης μπορεί να προτείνει μια νέα κατάσταση, και σε περίπτωση που ο αντίπαλος θεωρεί πως ο άλλος έκλεψε, τότε για το γύρο μπορούν να μεταφερθούν on-chain, καταναλώνοντας ένα φόρο από το κλειδωμένο ποσό, επαληθεύοντας ή μη την απάτη. Το παιχνίδι παρουσιάζεται online μέσω ενός demo στο https://statechannel.aepps.com/ ενώ τον κώδικα του μπορούμε να τον βρούμε στο σύνδεσμο https://github.com/aeternity/state-channel-demo/blob/develop/contract/contracts/RockPaperScissors.aes.

Κανάλια Πληρωμών Σκοπό έχουν την εκτέλεση (μίκρο)-συναλλαγών σε μηδαμινό χρόνο και ελάχιστους φόρους. Έχουν την ίδια λογική με τα κανάλια κατάστασης, απλώς είναι σχεδιασμένα για συγκεκριμένες χρήσεις, δηλαδή αποκλειστικά για πληρωμές. Ένα τέτοιο δίκτυο είναι το Bitcoin Lightning network, πάνω στο οποίο έχει στηριχθεί το δικό μας παράδειγμα και αναλύεται παρακάτω.

6.1.2 Πλευρικές Αλυσίδες - Side Chains

Μια πλευρική αλυσίδα, είναι μια ανεξάρτητη αλυσίδα το οποίο λειτουργεί παράλληλα με το κύριο δίκτυο. Σκοπός του είναι να αναλαμβάνει όσο περισσότερο φόρτο, δηλαδή συνθετότερους υπολογισμούς, απελευθερώνοντας πόρους στο βασικό δίκτυο. Μια τέτοια αλυσίδα έχει συνήθως το δικό του μηχανισμό συναίνεσης, και χρησιμοποιούν μια γέφυρα διπλής διαδρομής με το κύριο δίκτυο, η οποία καλείται two-way peg. Μέσω αυτής μεταφέρονται κεφάλαια του κύριου δικτύου.



Σχήμα 6.2: Γεφύρωση [3]

Η κύρια κατηγορία των πλευρικών αλυσίδων είναι οι αλυσίδες Plasma, οι οποίες δημοσιοποιούν το root hash τους στο κύριο δίκτυο, Θα μπορούσαμε να φανταστούμε αυτή τη λογική ως μια δενδροποίηση του δικτύου, όπου ένα δίκτυο μπορεί να στηρίζεται σε ένα άλλο, όπου κάθε κλαδί είναι και ένα νέο δίκτυο.

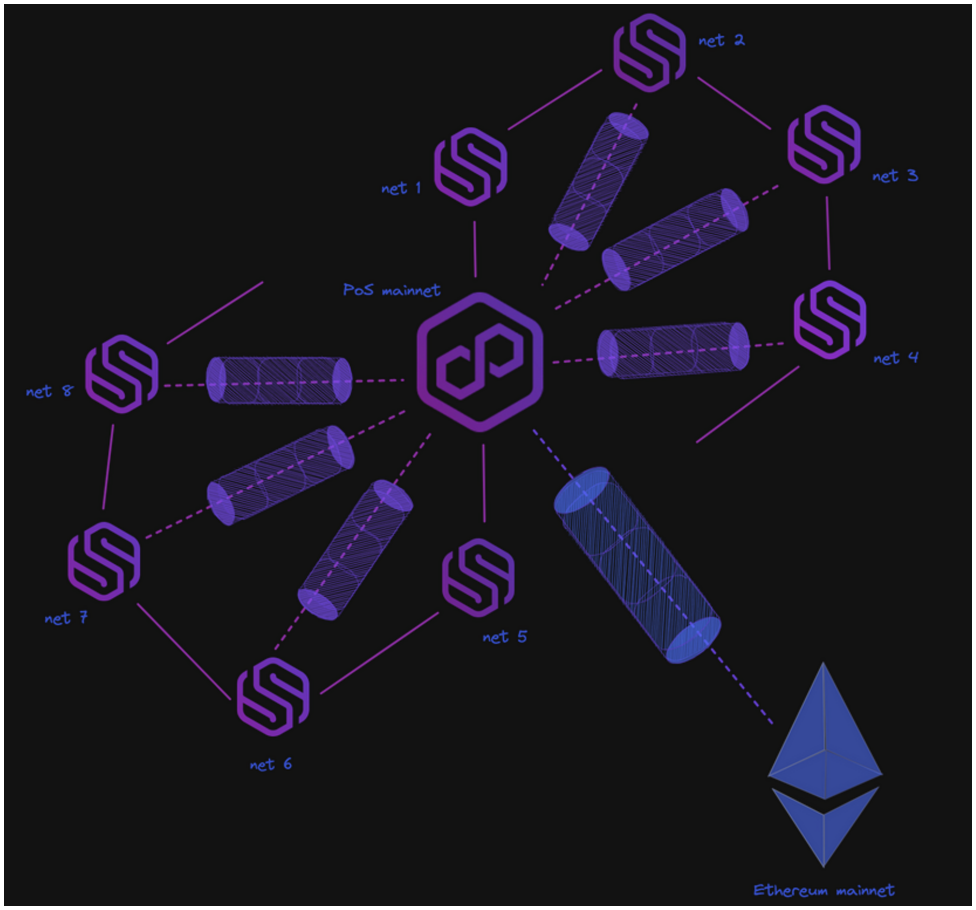
Polygon Το polygon, είναι το γνωστότερο δίκτυο 2ου επιπέδου που στηρίζεται στο Ethereum. Η αποδοχή του είναι τεράστια, καθώς πάνω του έχουν χτίσει εφαρμογές κολοσσοί εταιριών όπως η Nike, Adidas, Starbucks, Disney, Adobe και Facebook.

Ξεκίνησε ως μια πλευρική αλυσίδα και πλέον χαρακτηρίζεται ως ένα οικοσύστημα για τη δημιουργία διάφορων λύσεων. Πλέον, είναι ένα οικοσύστημα δυνατοτήτων, όπου παρακάτω επεκτεινόμαστε στις 2 κυριότερες.

Polygon PoS Ένα δίκτυο PoS πάνω στο Ethereum, προσφέροντας μια πιο αποδοτική και επεκτάσιμη λύση, επιτρέποντας γρηγορότερες συναλλαγές φτάνοντας στις 2400 ανά δευτερόλεπτο [23], ενώ, η ασφάλεια του εξασφαλίζεται από την ίδια του την ύπαρξη πάνω στην αποκεντροποίηση του Ethereum.

Υπερδίκτυα Polygon - Supernets Τα υπερδίκτυα είναι δίκτυα τα οποία ξεκινούν από το polygon PoS και υποστηρίζουν νέα δίκτυα που υλοποιούν συγκεκριμένες εφαρμογές. Κάθε Υπερδίκτυο είναι ένα νέο οικοσύστημα, μέσα στο οποίο υπάρχουν προμηθευτές υπηρεσιών για τη δημιουργία ρυθμιζόμενων εφαρμογών που καλύπτουν συγκεκριμένες νομοθεσίες. Συγκεκριμένα, τέτοιες υπηρεσίες είναι:

Προμηθευτές Κόμβων - Node Providers - Υποστήριξη μέσω υποδομών hardware για τη λειτουργία επαρκών κόμβων



Σχήμα 6.3: Υπερδίκτυα Polygon

Μαντεία - Oracles - Για την εισαγωγή πληροφοριών από τον έξω κόσμο μέσα στον κλειστό κόσμο των αποκεντροποιημένων εφαρμογών

Ανιχνευτές μπλοκ - Block Scanners - Ανάγνωση και πληροφόρηση συναλλαγών

KYC - Υπηρεσίες ταυτοποίηση χρηστών για την πιστοποίηση νόμιμων συναλλαγών και αποφυγή χρηματικού ξεπλύματος

6.1.3 Συναθροίσεις - Rollups

Τα συναθροιτικά δίκτυα ξεκινούν από το κύριο δίκτυο το οποίο χρησιμοποιούν για να επαληθεύουν συναλλαγές ενώ τα ίδια χρησιμοποιούν τεχνικές συμπίεσης για να αποφορτώνουν το πρώτο. Διατηρούν ελάχιστες πληροφορίες στο βασικό δίκτυο, για τις αλλαγές στην κατάσταση. Συγκεκριμένα, το έξυπνο συμβόλαιο διατηρεί τη ρίζα merkle, αλλά όχι τα υπόλοιπα κλαδιά (δέντρο merkle), μειώνοντας τον απαιτούμενο χώρο. Το root μπορεί να επαναυπολογισθεί από τα δεδομένα που βρίσκονται on-chain. Περιοδικά, υπολογίζεται ένα νέο merkle root, το οποίο είναι η νέα κατάσταση του δικτύου όπου περιέχονται τα ενημερωμένα balances βάσει των εκτελεσμένων συναλλαγών. Οποιοσδήποτε μπορεί να δημοσιεύσει την επόμενη ρίζα κατάστασης, αποστέλλοντας το συμπιεσμένο πλήθος συναλλαγών, την προηγούμενη καταστατική ρίζα καθώς και προφανώς, τη νέα.

Επειδή οποιοσδήποτε μπορεί να δημοσιεύσει τη νέα κατάσταση, υπάρχουν 2 κύρια πρωτόκολλα διαχείρισης απάτης.

Αισιόδοξες συναθροίσεις - Optimistic Rollups Έχουν μια φιλόδοξη προσέγγιση, καθώς θεωρούν πως κάθε συναλλαγή είναι σωστή εκτός και κάποιος θεωρήσει το αντίθετο. Συνεπώς, υπολογιστικοί πόροι δεν καταναλώνονται για την πιστοποίηση τους, αυξάνοντας σημαντικά την επεκτασιμότητα του δικτύου. Από την άλλη, το συμβόλαιο διατηρεί ιστορικό κάθε έκδοσης της καταστατικής ρίζας, καθώς επίσης και τις κατακερματισμένες συμβολοσειρές των συνόλων παραγωγής (batch). Για να εναντιωθεί κάποιος σε ένα σύνολο χρειάζεται η on-chain εκπομπή της απόδειξης λανθασμένων υπολογισμών, η οποία ονομάζεται απόδειξη απάτης - fraud proof, η οποία επαληθεύεται on-chain, από το ίδιο το συμβόλαιο, καθώς καταναλώνονται on-chain πόροι. Αν όντως το αποτέλεσμα είναι διαφορετικό, τότε το σύνολο ακυρώνεται καθώς και κάθε επακόλουθο του σύνολο.

Συναθροίσης Μηδενικής Γνώσης - Zero Knowledge Rollups Αντίθετα με τα αισιόδοξα, αυτά τα rollups υποπτεύονται κάθε συναλλαγή. Κάθε σύνολο συμπεριλαμβάνει μια κρυπτογραφημένη απόδειξη (validity proof), η οποία αποδεικνύει ότι η νέα καταστατική ρίζα πράγματι αντιστοιχεί στη σωστή έξοδο του συνόλου. Ο υπολογισμός των αποδείξεων είναι σύνθετος αλλά μπορεί να πιστοποιηθεί ταχύτατα on-chain.

6.2 Layer 0

Για να κατανοήσουμε την ύπαρξη των δικτύων μηδενικού επιπέδου, πρέπει να καταλάβουμε το κύριο πρόβλημα των δικτύων πρώτου επιπέδου. Το κύριο πρόβλημα, δομείται σε ένα τρίλημμα: Επεκτασιμότητα, Αποκεντροποίηση, Ασφάλεια. Αυτό που παρατηρείται είναι ότι οι περισσότερες λύσεις αποτελούνται από 2 από τα 3 χαρακτηριστικά, θυσιάζοντας τουλάχιστον 1. Για παράδειγμα, οι περισσότερες ηλεκτρονικές εφαρμογές του παρόντος διαδικτύου, θυσιάζουν την αποκεντροποίηση στα χέρια κάποιου τρίτου παρόχου, κερδίζοντας ταχύτητα. [24] Έτσι επίσης και το Bitcoin, ενώ έχει μεγάλη ασφάλεια λόγω της αποκεντροποίησης του, επεκτείνεται δυσκολότατα ενώ παράλληλα είναι σχετικά αργό.

Έτσι, δημιουργήθηκαν τα δίκτυα μηδενικού επιπέδου, πάνω στα οποία μπορούν να δημιουργηθούν δίκτυα πρώτου επιπέδου όπως το Bitcoin. Καθώς το δίκτυο L0 (Layer 0) στέκεται ως η βάση των υπολοίπων δικτύων, διαθεσιμότητα πληροφορίας μεταξύ δικτύων πρώτου επιπέδου γίνεται εφικτή. Παράλληλα, τα περισσότερα L0 δίκτυα παρέχουν σουίτες ανάπτυξης λογισμικού (SDK), διευκολύνοντας τους προγραμματιστές. 2 από τα γνωστότερα σχετικά δίκτυα είναι το Cosmos και το Polkadot.

Κεφάλαιο 7ο: Δίκτυα Μικροπληρωμών

Σε αυτό το κεφάλαιο παρουσιάζουμε 3 δίκτυα μιας σημαντικής χρήσης της τεχνολογίας αλυσίδων συστοιχιών, αυτή των μικρο-πληρωμών.

7.1 Nano

Το Nano είναι ένα ψηφιακό πρωτόκολλο πληρωμών σχεδιασμένο να είναι προσβάσιμο και ελαφρύ. Είναι από τα γνωστότερα δίκτυα για μίκρο-συναλλαγές, καθώς έχει μηδενικές χρεώσεις ενώ παράλληλα είναι φιλικό προς το περιβάλλον καθώς δεν υπάρχει μεγάλη κατανάλωση ρεύματος. [25] Σε αυτό το δίκτυο, κάθε λογαριασμός ελέγχει τη δική του αλυσίδα συστοιχιών. Αυτό επιτρέπει την γρήγορη προσθήκη μπλοκ, και την αποστολή του στην αλυσίδα για επιβεβαίωση. Οι συναλλαγές πραγματοποιούνται με δύο ξεχωριστές ενέργειες:

- Ο αποστολέας δημοσιεύει ένα μπλοκ χρεώνοντας τον δικό του λογαριασμό για το ποσό που θα σταλεί στον παραλήπτη
- παραλήπτης δημοσιεύει ένα αντίστοιχο μπλοκ πιστώνοντας τον δικό του λογαριασμό για το ποσό που αποστέλλεται

Μόλις επιβεβαιωθεί από το δίκτυο ένα μπλοκ αποστολής, η συναλλαγή μεταβαίνει σε **ΕΙΣΠΡΑΚΤΕΑ (RECEIVABLE)** κατάσταση και δεν μπορεί να αντιστραφεί. Ο παραλήπτης μπορεί να μην είναι συνδεδεμένος στο διαδίκτυο και να αφήσει με ασφάλεια τα χρήματα σε αυτήν την κατάσταση μέχρι να είναι έτοιμος να δημοσιεύσει ένα αντίστοιχο μπλοκ που λαμβάνει τα χρήματα στον λογαριασμό του. Κάθε μπλοκ περιέχει τα εξής δεδομένα για το λογαριασμό του:

- αναγνωριστικό λογαριασμού
- υπόλοιπο
- αντιπρόσωπο.

Κάθε μπλοκ πρέπει επίσης να περιέχει μια μικρή τιμή τύπου Απόδειξη-Εργασίας (PoW) που δημιουργείται από το χρήστη. Ο υπολογισμός PoW για μια συναλλαγή διαρκεί συνήθως μερικά δευτερόλεπτα σε ένα μοντέρνο CPU. Ο μηχανισμός συναίνεσης είναι πολυ διαφορετικός από τα υπόλοιπα δίκτυα, και ονομάζεται **Ανοιχτή Αντιπροσωπευτική ψηφοφορία, Open Representative Voting (ORV)**. Κάθε λογαριασμός μπορεί να επιλέξει έναν **Αντιπρόσωπο (Representative)** ανά πάσα στιγμή για να ψηφίσει εκ μέρους του, ακόμη και όταν ο ίδιος είναι εκτός σύνδεσης. Οι αντιπρόσωποι διαμορφώνονται σε κόμβους που παραμένουν συνδεδεμένοι και ψηφίζουν για την εγκυρότητα των συναλλαγών. Η ισχύς της ψήφου τους είναι το άθροισμα των υπολοίπων των λογαριασμών που τους έχουν επιλέξει ως αντιπροσώπους. Εάν έχουν αρκετή ισχύ, προάγονται σε **Κύριο Εκπρόσωπο (Principal Representative)**. Οι ψήφοι που στέλνουν αυτοί οι Κύριοι Εκπρόσωποι θα αναμεταδοθούν στη συνέχεια από άλλους κόμβους, επιταχύνοντας το δίκτυο. Καθώς αυτές οι ψήφοι μοιράζονται και αναμεταδίδονται μεταξύ των κόμβων, συγκρίνονται με την ψηφοφοριακή ισχύ στο διαδίκτυο.

Μόλις ένας κόμβος δει ένα μπλοκ να παίρνει αρκετές ψήφους για να φτάσει στην απαρτία (quorum), δηλαδή έχει τουλάχιστον 67% των ψήφων του δικτύου , αυτό το μπλοκ επιβεβαιώνεται. Λόγω της ελαφρότητας της αρχιτεκτονικής, το δίκτυο μπορεί να επιβεβαιώσει ταχύτατα συναλλαγές, συχνά σε λίγα δευτερόλεπτα. [25] Αυτός ο μηχανισμός θυμίζει το PoS, αλλά διαφέρει σημαντικά, καθώς στο Nano

- οι Κύριοι Εκπρόσωποι δεν δημιουργούν νέα block
- κάθε λογαριασμός έχει το δικό του blockchain όπου μόνο ο χρήστης μπορεί να παραμετροποιήσει
- κάθε μπλοκ δεν είναι ένα σύνολο συναλλαγών, αλλά μια συναλλαγή
- δεν κλειδώνονται ποσά
- δεν υπάρχουν φόροι

7.1.1 Ανησυχίες

Ενώ το σύστημα Κυρίων Αντιπροσώπων είναι ταχύτατο, παρουσιάζει κεντροποίηση, καθώς ψηφοφορική δύναμη πολώνεται σε ένα μικρότερο πλήθος κόμβων. Παράλληλα, ο ίδιος ο μηχανισμός είναι ευάλωτος σε σίβυλλες επιθέσεις. Μια τέτοια επίθεση μπορεί να πραγματοποιηθεί δημιουργώντας πάμπολλους λογαριασμούς, επηρεάζοντας την ψηφοφορία. Τέλος, καθώς οι συναλλαγές δεν έχουν φόρους, το δίκτυο είναι πιο ευάλωτο σε επιθέσεις άρνησης παροχής υπηρεσιών (Denial of Service), καθώς ένα κακόβουλος χρήστης θα μπορούσε να πλημμυρίσει το δίκτυο. Παρόλο που υπάρχουν προσεγγίσεις για να χειριστούν τα παραπάνω προβλήματα, παραμένουν όμως, ενεργοί κίνδυνοι.

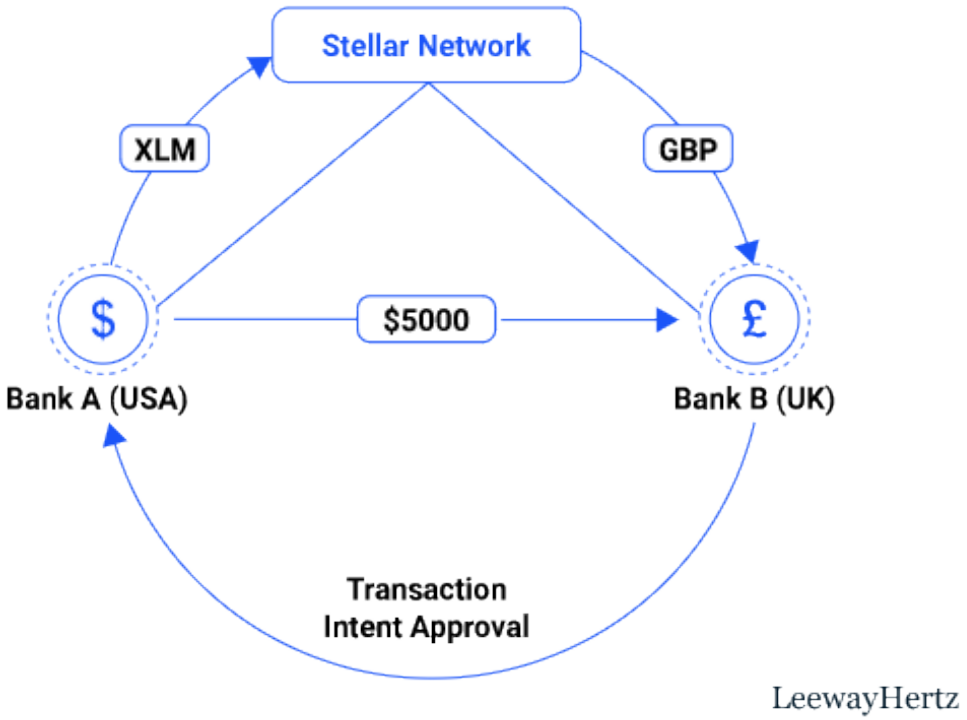
7.2 Stellar

Το Stellar είναι ένα δίκτυο σχεδιασμένο για διασυνοριακές συναλλαγές με χαμηλό κόστος. Κύριος σκοπός είναι η μετατροπή παραστατικού χρήματος όπως το δολλάριο σε ψηφιακά νομίσματα. Ιδρυτές ο Joyce Kim καθώς και ο Jed McCaleb, ο οποίος είναι συνειδρητής ενός άλλου γνωστού δικτύου, το Ripple. Το δίκτυο μπορεί να επεξεργαστεί χιλιάδες συναλλαγές ανά δευτερόλεπτο, ενώ η επιβεβαίωση μιας συναλλαγής διαρκεί μεταξύ 3 και 5 δευτερολέπτων. [4]

Το νόμισμα καλείται Lumens (XLM) και χρησιμοποιείται ως το μέσο που μετατροπής οποιουδήποτε υποστηριζόμενο νόμισμα του δικτύου σε άλλο. Το δίκτυο στηρίζεται σε ένα σύνολο έμπιστων οντοτήτων, οι οποίες καλούνται **Άγκυρες (Anchors)**. Οι άγκυρες συνήθως είναι τράπεζες, οι οποίες προμηθεύουν το δίκτυο με παραστατικό χρήμα αλλά και με ψηφιακό. Στην ουσία, γεφυρώνουν το κενό μεταξύ το παραδοσιακού οικονομικού συστήματος και του δικτύου του Stellar. Το νόμισμα παρουσιάζει περίπου 1% πληθωρισμό/χρόνο. [4]

7.2.1 Μηχανισμος Συναίνεσης

Ο μηχανισμός συναίνεσης ονομάζεται Πρωτόκολλο Συναίνεσης του Stellar - Stellar Consensus Protocol **(SCP)**. Κάθε κόμβος του δικτύου, επιβεβαιώνει συναλλαγές έχοντας ένα μικρό δίκτυο



Σχήμα 7.1: Stellar στην Πράξη [4]

εμπιστευμένων συμμετοχόντων. Αυτά τα δίκτυα καλούνται **Φέτες Απαρτίας - Quorum Slices**. Για τον αρχικό κόμβο, αυτή η φέτα θεωρείται ως ένα έμπιστο σύνολο κόμβων όπου το δίκτυο βασίζει την ασφάλεια του αλλά και την επικύρωση των συναλλαγών. Σε κάθε γύρο του μηχανισμού, οι κόμβοι ψηφίζουν για την επικυρώτητα των συναλλαγών. Στην πράξη, ψηφίζουν ποιες συναλλαγές θεωρούν σωστές, αλλά επίσης ψηφίζουν και ποιους κόμβους θεωρούν έμπιστους, δηλαδή θα ακολουθήσουν τους κανόνες του μχανισμού. Ο μηχανισμός έχει 3 κύριες φάσεις, **Προετοιμασία, Επιβεβαίωση, Εξωτερίκευση.** Στην πρώτη φάση, δηλαδή κατά την Προετοιμασία, οι κόμβοι ψηφίζουν και ανταλλάσουν πληροφορίες μεταξύ τους. Έπειτα, κατά την Επιβεβαίωση, οι κόμβοι καταλήγουν στις συναλλαγές προς επιβεβαίωση αλλά και στις φέτες του μηχανισμού. Τέλος, κατά την Εξωτερίκευση, κάθε κόμβος κλειδώνει τις επιλογές του και το αντίστοιχο σύνολο συναλλαγών σφραγίζεται στην αλυσίδα. Για τους κόμβους που επικυρώνουν συναλλαγές, δεν υπάρχει κάποιο κέρδος, όπως παρουσιάζεται σε άλλα δίκτυα. [26]

7.2.2 Παράδειγμα χρήσης

Έστω ότι ο Μιχάλης ζει στην Αμερική και θέλει να στείλει 5.000$ στον Κώστα που ζει στο Ηνωμένο Βασίλειο, μετατρέποντας το ποσό σε βρεατανική Στερλίνα. Ας θεωρήσουμε πως η τράπεζα το πρώτου είναι η Bank A και Bank B η τράπεζα του δεύτερου.

Αυτές οι 2 τράπεζες, είναι επίσης μέλη του δικτύου Stellar, ως Άγκυρες. Όταν ο Μιχάλης στείλει το

ποσό, ένα αντίστοιχο αίτημα στέλνεται στην τράπεζα Β έτσι ώστε να επιβεβαιωθεί η συναίνεση του δεύτερου. Όταν η Bank A λάβει την αποδοχή από την άλλη τράπεζα, τότε αφαιρούν το ποσό από το Μιχάλη, το οποίο μετατρέπεται σε XLM, στέλνεται στην άλλη τράπεζα, και μόλις το παραλάβει, το μετατρέπει στο επιθυμητό νόμισμα, δηλαδή Στερλίνα. [4]

7.2.3 Ανησυχίες

Όταν δημιουργήθηκε το δίκτυο, το **Ίδρυμα Ανάπτυξης το Stellar - Stellar Development Foundation** δημιούργησε 100 δις XLM για να χρηματοδοτήσει την ανάπτυξη του. Ένα μεγάλο ποσοστό αυτού του αριθμού υπάρχει ακόμη στην κατοχή του, όντας κεντροποιημένο. Στην ουσία, ο κίνδυνος που φοβίζει τον κόσμο είναι η πιθανότητα να πουληθεί αυτό το ποσό. Παράλληλα, για τη δημιουργία μιας Άγκυρας, πρέπει να αποδεχθεί από το ίδιο το Ίδρυμα. Συνεπώς, ακόμη και οι ίδιοι οι κόμβοι, είναι κεντροποιημένοι κάτω από το Ίδρυμα.

7.3 Lightning Network

Το Lightning Network, το οποίο θα αναλύσουμε με μεγαλύτερη λεπτομέρεια σε επόμενο κεφάλαιο, είναι ένα πρωτόκολλο δευτέρου επιπέδου βασισμένο στο πρωτόκολλο του Bitcoin, μέσω του οποίου μπορούμε να εκτελέσουμε άμεσες και με πολύ χαμηλό κόστος συναλλαγές. Όλες οι συναλλαγές γίνονται σε κανάλια πληρωμών μεταξύ ομότιμων και είναι έγκυρες συναλλαγές Bitcoin με μόνη διαφορά ότι δεν δημοσιεύονται στην αλυσίδα του Bitcoin παρά μόνο στην περίπτωση που κάποιος από τους ομότιμους θελήσει να διευθετήσει το υπόλοιπό του στην αλυσίδα. Τα κανάλια πληρωμών αποτελούν το δίκτυο του Lightning.

Σε περίπτωση που μια οντότητα θέλει να εκτελέσει μια πληρωμή προς μια οντότητα με την οποία δεν υπάρχει απευθείας σύνδεση με μεμονωμένο κανάλι τότε αρκεί να υπάρχει έμμεση διαδρομή πολλαπλών καναλιών μέσω της οποίας μπορεί δρομολογηθεί η πληρωμή. Στα ενδιάμεσα κανάλια, οι κόμβοι μπορούν να επιβάλουν ένα κόστος δρομολόγησης το οποίο πληρώνεται από την οντότητα που θέλει να εκτελέση την πληρωμή.

7.4 Σύγκριση

Δίκτυο	Επεξεργασία συν./δευτ.	Χρόνος Επιβεβαίωσης συναλλαγής	Φόροι
Nano	1200+	<1 s	0
Stellar	4000	3-5 s	0
Lightning	1000000	λίγα ms εώς και 1 λεπτό	0+

Πίνακας 7.1: Σύγκριση ποσοτικών χαρακτηριστικών δικτύων μικροπληρωμών

Δίκτυο	Πληθωρισμός	Έξυπνα Συμβόλαια	Μηχανισμός Συναίνεσης
Nano	-	-	ORV
Stellar	1%	δοκιμαστικά	SCP
Lightning	-	ναι	τοπικός (κανάλι πληρωμών)

Πίνακας 7.2: Σύγκριση γενικών χαρακτηριστικών δικτύων μικροπληρωμών

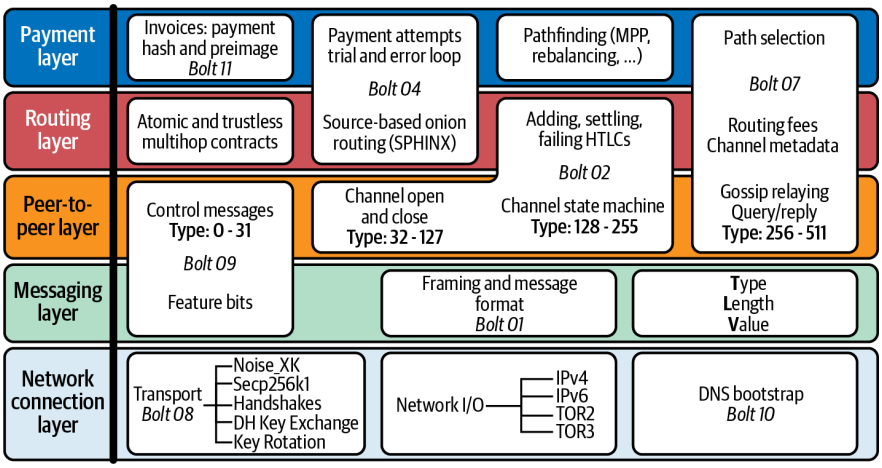
Κεφάλαιο 8ο: Το Lightnin Network

8.1 Εισαγωγή στο δίκτυο Lightning

Το δίκτυο Lightning είναι μια λύση κλιμάκωσης 2ου επιπέδου (layer-2 scalling solution) που βασίζεται στο πρωτόκολλο του Bitcoin. Είναι δηλαδή μια ξεχωριστή αλυσίδα που επεκτείνει το Bitcoin κληρονομώντας τις εγγυήσεις ασφαλείας του. Αποτελείται από κανάλια που επιτρέπουν σε οντότητες να διακινούν κεφάλαια μεταξύ τους χωρίς να χρειάζεται να χρησιμοποιήσουν το Bitcoin για την επαλήθευση των συναλλαγών τους. Στο Lightning οι μεταφορές οριστικοποιούνται εκτός της κύριας αλυσίδας [27], αυτό επιτρέπει στο δίκτυο να λειτουργεί πολύ πιο γρήγορα από ότι το Bitcoin με αποτέλεσμα να προσφέρει φθηνές και γρήγορες συναλλαγές μεταξύ οντοτήτων.

Η ανάγκη για μια λύση κλιμάκωσης 2ου επιπέδου προέρχεται από το γεγονός ότι το Bitcoin δεν μπορεί να διεκπεραιώσει αρκετές συναλλαγές ταυτόχρονα ώστε να επιτρέπει σε δισεκατομμύρια χρήστες να πραγματοποιούν συναλλαγές καθημερινά [28].

Τα πρωτόκολλα από τα οποία απαρτίζεται το Lightning μπορούν να ομαδοποιηθούν σε πέντε διακριτά επίπεδα, όπου κάθε επίπεδο βασίζεται και χρησιμοποιεί τα πρωτόκολλα του αμέσως προηγούμενου επιπέδου με τρόπο παρόμοιο των επιπέδων του TCP/IP.



Σχήμα 8.1: Η σουίτα πρωτοκόλλων του Lightning [5]

Επίπεδο σύνδεσης δικτύου Τα πρωτόκολλα σε αυτό το επίπεδο αλληλεπιδρούν άμεσα με τα βασικά πρωτόκολλα του διαδικτύου (TCP/IP), τα πρωτόκολλα Tor v2/v3 και υπηρεσίες διαδικτύου όπως το DNS. Αυτό το επίπεδο περιλαμβάνει επίσης τα κρυπτογραφικά πρωτόκολλα μεταφοράς που προστατεύουν τα μηνύματα του Lightning.

Επίπεδο μεταφοράς Σε αυτό το επίπεδο οι κόμβοι διαπραγματεύονται διαθέσιμες λειτουργίες, μορφοποιούν μηνύματα και κωδικοποιούν τα πεδία των μηνυμάτων.

Επίπεδο ομότιμων (P2P) Όλη η επικοινωνία μεταξύ των κόμβων πραγματοποιείται σε αυτό το επίπεδο.

Επίπεδο δρομολόγησης Αυτό το επίπεδο περιλαμβάνει τα πρωτόκολλα που χρησιμοποιούνται για τη δρομολόγηση των πληρωμών μεταξύ των κόμβων, από άκρο σε άκρο και ατομικά.

Επίπεδο πληρωμής Το υψηλότερο επίπεδο στο δίκτυο. Προσφέρει μια αξιόπιστη διεπαφή πληρωμών στις εφαρμογές.

8.2 Κανάλια πληρωμών

Ένα κανάλι πληρωμών είναι στην ουσία ένα συμβόλαιο πολλαπλών υπογραφών (multi-signature contract) μεταξύ ομότιμων το οποίο διατηρεί bitcoin. Οι πληρωμές που γίνονται μέσα σε ένα κανάλι μπορούν να διευθετηθούν στην αλυσίδα.

Το Lightning απαρτίζεται από χιλιάδες κανάλια πληρωμών όπου κάθε κανάλι αντιπροσωπεύει μια συναλλαγή που δεν έχει εξαργυρωθεί (unspent transaction output, UTXO) στην αλυσίδα του Bitcoin και ελέγχεται συνεργατικά από τους υπογράφοντες του συμβολαίου, οι οποίοι μπορούν να εκτελέσουν συναλλαγές μέσα από το κανάλι όσο συχνά επιθυμούν [29].

Παρόλο που το κεφάλαιο που διατηρείται στο κανάλι ελέγχεται συνεργατικά από τις δύο οντότητες από την οπτική του Bitcoin, στην πραγματικότητα σε κάθε οντότητα ανήκει ένα ποσοστό του. Κάθε οντότητα διατηρεί αρχείο αυτής της ιδιοκτησίας τοπικά.

Για να διασφαλιστεί ότι οι δύο οντότητες δεν χρειάζεται να εμπιστεύονται η μία την άλλη, τα κανάλια πληρωμών διασφαλίζονται από μια συναλλαγή δέσμευσης, η οποία υπογράφεται και από τις δύο οντότητες και τους επιτρέπει να αποχωρήσουν μονομερώς από τη συμφωνία τους ανά πάσα στιγμή. Αποστέλλοντας το αντίστοιχο μερίδιο των κεφαλαίων τους πίσω στο πορτοφόλι τους. Το γεγονός αυτό ονομάζεται "αναγκαστικό κλείσιμο".

8.2.1 Άνοιγμα καναλιού

Ας υποθέσουμε ότι δύο οντότητες, η Αλίκη και ο Κώστας, θέλουν να ανοίξουν ένα κανάλι μεταξύ τους.

Για να μπορεί οποιοσδήποτε να ανοίξει ένα κανάλι με την Αλίκη, ο κόμβος της θα πρέπει να είναι προσβάσιμος μέσο του internet. Η Αλίκη μπορεί επίσης να επιβάλει περιορισμούς όσον αφορά το ποιος μπορεί να ανοίξει νέα κανάλια μαζί της.

Για να ανοίξει το κανάλι, ο Κώστας θα πρέπει να κατέχει bitcoin. Κατόπιν εντολής του, ο κόμβος του θα συνδεθεί με την Αλίκη και θα της προσφέρει ένα κανάλι. Ο συνδυασμός των κλειδιών τους θα δημιουργήσει ένα συμβόλαιο πολλαπλών υπογραφών, το οποίο θα λειτουργεί επίσης ως διεύθυνση του καναλιού τους.

Για να διασφαλιστεί ότι σε καμία περίπτωση δεν θα κλειδωθεί το κεφάλαιο του Κώστα σε αυτό το συμβόλαιο, δημιουργεί την συναλλαγή χρηματοδότησης του χωρίς όμως να την μεταδώσει στο δίκτυο. Δημιουργεί επίσης μια επιπλέον συναλλαγή, την συναλλαγή δέσμευσης, η οποία επιστρέφει τα χρήματά πίσω σε αυτόν και ζητά από την Αλίκη να την συνυπογράψει.

Τώρα ο Κώστας δημοσιεύει την αρχική του συναλλαγή και μεταφέρει το κεφάλαιο στο κανάλι πληρωμών, κρατώντας την δεύτερη συναλλαγή που επιστρέφει το κεφάλαιο πίσω σε αυτόν στην μνήμη του υπολογιστή του. Η Αλίκη δεν μπορεί να πάρει το κεφάλαιο του χωρίς την συνεργασία του και σε περίπτωση που εκείνη σταματήσει να ανταποκρίνεται, εκείνος μπορεί να δημοσιεύσει την συναλλαγή δέσμευσης παίρνοντας πίσω τα χρήματά του. Αφού το χρηματοδοτήσει ο Κώστας, το κανάλι είναι ανοιχτό και διαθέσιμο για χρήση.

Κανάλια πληρωμών διπλής χρηματοδότησης Προς το παρόν τα κανάλια χρηματοδοτούνται μόνο από τον κόμβο που ξεκινάει το κανάλι (στο παράδειγμα μας, τον Κώστα). Έχει γίνει πρόταση να προστεθεί η δυνατότητα διπλής χρηματοδότησης αλλά επί του παρόντος δεν υποστηρίζεται στο Lightning. Σε ένα κανάλι διπλής χρηματοδότησης, και οι δύο κόμβοι συνεισφέρουν στην συναλλαγή χρηματοδότησης.

8.2.2 Αποστολή χρημάτων μέσω καναλιού πληρωμών

Οι συναλλαγές δέσμευσης αντικατοπτρίζουν την κατάσταση του καναλιού. Η τελευταία συναλλαγή δέσμευσης αντικατοπτρίζει πάντα τα τρέχοντα υπόλοιπα του καναλιού μεταξύ των δύο οντοτήτων. Οι οντότητες μπορούν να μεταφέρουν αυτό το υπόλοιπο μεταξύ τους ενημερώνοντας τη συναλλαγή δέσμευσής τους. Δεν υπάρχει όριο στο πόσο συχνά μπορούν να μεταφέρουν το υπόλοιπο μεταξύ τους, όπως δεν υπάρχει περιορισμός και στην κατεύθυνση και τον αριθμό των μεταφορών. Όσο οι συναλλαγές δεν δημοσιεύονται στην αλυσίδα το κεφάλαιο δεν μεταφέρεται ποτέ στην αλυσίδα, είναι γνωστό μόνο στις δύο οντότητες.

Με κάθε πληρωμή, όλες οι προηγούμενες συναλλαγές δέσμευσης ακυρώνονται, διασφαλίζοντας έτσι ότι μόνο η τελευταία συναλλαγή μπορεί να χρησιμοποιηθεί για την ανάκτηση του κεφαλαίου στην περίπτωση που το κανάλι οδηγηθεί σε αναγκαστικό κλείσιμο.

8.2.3 Κλείσιμο καναλιού

Όπως και το άνοιγμα ενός καναλιού, έτσι και το κλείσιμο ενός καναλιού είναι μια συναλλαγή στην αλυσίδα του Bitcoin. Συμβαίνει όταν έστω και μια από τις οντότητες θέλει να διευθετήσει το υπόλοιπο της πίσω στην αλυσίδα του Bitcoin.

Υπάρχουν δύο τρόποι να κλείσει ένα κανάλι: Συνεργατικά ή μη συνεργατικά. Και στις δύο περιπ-

τώσεις τα έξοδα της συναλλαγής πληρώνονται από την οντότητα που άνοιξε το κανάλι.

Συνεργατικά Σε ένα συνεργατικό κλείσιμο, και η Αλίκη και ο Κώστας είναι συνδεδεμένοι, συμφωνούν στα υπόλοιπα τους και στους όρους του κλεισίματος του καναλιού που έχουν προταθεί από τον καθένα. Υπογράφουν και οι δύο μια νέα συναλλαγή η οποία στέλνει άμεσα το υπόλοιπο του καθενός στο αντίστοιχο πορτοφόλι. Από αυτό το σημείο και έπειτα δεν γίνονται άλλες συναλλαγές στο κανάλι.

Τα κανάλια στο Lightning συνήθως κλείνουν συνεργατικά.

Μη συνεργατικά Ένα κανάλι κλείνει μη συνεργατικά όταν ένα από τα μέλη του καναλιού το κλείνει χωρίς την συγκατάθεση του άλλου. Υπάρχει περίπτωση ένα μέλος του καναλιού να μην είναι διαθέσιμο ή να αρνείται να υπογράψει την συναλλαγή κλεισίματος του καναλιού για οποιονδήποτε λόγο. Σε αντίστοιχη περίπτωση το μέλος που προσπαθεί να κλείσει το κανάλι θα πρέπει να δημοσιεύσει την συναλλαγή δέσμευσης που κρατάει στην μνήμη στην αλυσίδα. Αυτό οδηγεί το κανάλι σε μη συνεργατικό κλείσιμο ή αλλιώς αναγκαστικό κλείσιμο.

Οι συναλλαγές δέσμευσης είναι ασύμμετρες, διότι το υπόλοιπο της οντότητας που ξεκίνησε το αναγκαστικό κλείσιμο κλειδώνεται σε ένα συμβόλαιο για συγκεκριμένο χρονικό διάστημα, ενώ το υπόλοιπο της άλλης οντότητας στέλνεται κατευθείαν στο πορτοφόλι της. Αυτό επιτρέπει στην ανυποψίαστη οντότητα να επιστρέψει και να επιβεβαιώσει την κατάσταση του καναλιού. Αν δεν επιστρέψει, τότε η οντότητα που ξεκίνησε το κλείσιμο του καναλιού θα πάρει πίσω το κλειδωμένο της κεφάλαιο μετά το πέρας του χρόνου κλειδώματος (συνήθως δύο εβδομάδες) [28].

Σε περίπτωση που μια από τις οντότητες προσπαθήσει να κλέψει, δημοσιεύοντας μια προηγούμενη κατάσταση του καναλιού που τους ευνοεί, τότε η άλλη οντότητα μπορεί να χρησιμοποιήσει το μυστικό ακύρωσης που ανταλλάχθηκε προηγουμένως ώστε να εισπράξει και το υπόλοιπο της οντότητας που προσπάθησε να κλέψει. Αυτό αποτελεί ισχυρό κίνητρό για τις οντότητες να παραμείνουν ειλικρινείς και διασφαλίζει γενικότερα το δίκτυο.

8.3 Δρομολόγηση

Στο Lightning Network, η δρομολόγηση των πληρωμών περιγράφεται στο BOLT#4 και βασίζεται σε μια παραλλαγή της δρομολόγησης κρεμμυδιού (onion routing) που ονομάζεται SPHINX [30].

Η καινοτομία των δρομολογημένων καναλιών πληρωμών επιτρέπει σε δύο οντότητες να στέλνουν και να λαμβάνουν πληρωμές ακόμη και αν δεν είναι άμεσα συνδεδεμένες με ξεχωριστό κανάλι. Οι ενδιάμεση κόμβοι από τους οποίους θα περάσει η πληρωμή ονομάζονται κόμβοι δρομολόγησης και οποιοσδήποτε κόμβος Lightning είναι ικανός να λειτουργεί ως κόμβος δρομολόγησης. Οι κόμβοι δρομολόγησης είναι ανίκανοι να κλέψουν το ποσό της πληρωμής αλλά είναι επίσης αδύνατο να χάσουν χρήματα από την συμμετοχή τους στην διαδικασία της δρομολόγησης. Μπορούν επίσης να επιβάλουν ένα κόστος δρομολόγησης.

Χάρη στην δρομολόγηση κρεμμυδιού, οι κόμβοι δρομολόγησης γνωρίζουν μόνο τον προηγούμενο και τους επόμενο κόμβο τους. Δεν γνωρίζουν ούτε το μήκος της συνολικής διαδρομής καθώς ούτε και την θέση τους στην διαδρομή. Αυτό επιτρέπει στις οντότητες να στέλνουν χρήματα μεταξύ τους, χωρίς να διαρρέουν ιδιωτικές τους πληροφορίες.

Για την ορθή λειτουργεία της δρομολόγησης των πληρωμών, απαιτείται η ύπαρξη ενός πρωτοκόλλου δικαιοσύνης. Το πρωτόκολλο αυτό αντικαθιστά την ανάγκη εμπιστοσύνης σε τρίτους με ένα αξιόπιστο πρωτόκολλο το οποίο μπορούν όλοι να εμπιστευτούν. Το πρωτόκολλο εμπιστοσύνης πρέπει να έχει τις εξής ιδιότητες [5]:

1. **Λειτουργεία χωρίς την ανάγκη εμπιστοσύνης τρίτων** Οι οντότητες μιας δρομολόγησης είναι αναγκαίο να μην χρειάζεται να εμπιστεύονται ο ένας τον άλλον ή οποιονδήποτε μεσάζοντα. Αντιθέτως, εμπιστεύονται το πρωτόκολλο για την προστασία τους.
2. **Ατομικότητα** Στο Lighting ο όρος ατομικότητα αναφέρεται στο γεγονός ότι κάτι είτε διεκπεραιώνεται εξ ολοκλήρου είτε καθόλου. Έτσι και μια πληρωμή, είτε εκτελείται πλήρως, είτε αποτυγχάνει και επιστρέφονται τα χρήματα σε όλους τους κόμβους.
3. **Ασφάλεια από άρκο σε άκρο** Η ασφάλεια του συστήματος επεκτείνεται από άκρο σε άκρο έτσι ώστε ότι ακριβώς ισχύει για μια πληρωμή μεταξύ των οντοτήτων ενός ενιαίου καναλιού πληρωμών να ισχύει και για τις πληρωμές που δρομολογούνται μέσω πολλαπλών κόμβων.

Η υλοποίηση αυτού του πρωτοκόλλου στο Lightning γίνεται μέσω του Bitcoin Script. Το πρωτόκολλο δικαιοσύνης που χρησιμοποιείται σήμερα στο δίκτυο Lightning ονομάζεται συμβόλαιο με χρονικά κλειδωμένο κατακερματισμό (hash time-locked contract, HTLC). Τα HTLC χρησιμοποιούν μια προ-εικόνα κατακερματισμού ως το μυστικό που ξεκλειδώνει μια πληρωμή. Ο παραλήπτης μιας πληρωμής παράγει έναν τυχαίο μυστικό αριθμό και υπολογίζει το κατακερματισμό του. Το κατακερματισμένο μήνυμα γίνεται η συνθήκη της πληρωμής και μόλις αποκαλυφθεί το μυστικό, όλοι οι συμμετέχοντες μπορούν να εξαργυρώσουν τις εισερχόμενες πληρωμές τους. Τα HTLCs προσφέρουν όσα απαιτούνται για την διασφάλιση των ιδιοτήτων του πρωτοκόλλου δικαιοσύνης.

8.3.1 Πώς δουλεύουν τα συμβόλαια με χρονικά κλειδωμένο κατακερματισμό (HTLC);

Τα συμβόλαια αυτά χρησιμοποιούν κρυπτογραφικούς αλγόριθμους για την δημιουργία τυχαίων μυστικών. Μέσω του κρυπτογραφικού κατακερματισμού μπορούμε να διαβεβαιώσουμε ότι κανείς δεν μπορεί να μαντέψει το μυστικό αλλά όλοι μπορούν να το επαληθεύσουν.

Για την πραγματοποίηση μια πληρωμής, από την Αλίκη στον Κώστα παραδείγματος χάριν, ο Κώστας δημιουργεί μια απόδειξη (Lightning invoice) και την στέλνει στην Αλίκη. Μέσα στην απόδειξη ο Κώστας έχει ενσωματώσει το μήνυμα που κατακερματίστηκε με το μυστικό του.

Η χρήση της κρυπτογραφικής συνάρτησης κατακερματισμού εγγυάται τη λειτουργία χωρίς ανάγκη εμπιστοσύνης σε τρίτους.

Η ατομικότητα των πληρωμών επιτυγχάνετε μέσω του χρονικού κλειδώματος το οποίο σημαίνει ότι αν περάσει κάποιο χρονικό διάστημα και η συναλλαγή δεν έχει διεκπεραιωθεί τότε αποτυγχάνει εξ ολοκλήρου και επιστρέφονται τα χρήματα σε όλους τους συμμετέχοντες.

8.3.2 Δρομολόγηση κρεμμυδιού (Onion Routing)

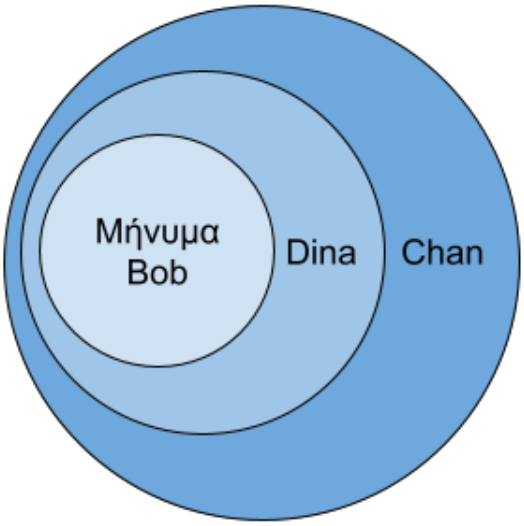
Στην δρομολόγηση κρεμμυδιού, όπως γίνεται φανερό και από την ονομασία, πρόκειται για δρομολόγηση στην οποία τα πακέτα καθώς μεταφέρονται από τον έναν κόμβο στον άλλο βρίσκονται το ένα μέσα στο άλλο σχηματίζοντας διαδοχικά εμφωλευμένα στρώματα. Κάθε κόμβος έχει πρόσβαση μόνο στο πρώτο επίπεδο του κρεμμυδιού που λαμβάνει και, αφού έχει λάβει τις απαραίτητες πληροφορίες από το στρώμα αυτό, το αφαιρεί από το κρεμμύδι και το προωθεί στον επόμενο κόμβο. Αυτό επαναλαμβάνεται για κάθε κόμβο ωσότου φτάσει το μήνυμα στον τελικό του προορισμό. Η δρομολόγηση κρεμμυδιού εξασφαλίζει ότι μόνο ο αποστολέας γνωρίζει τον παραλήπτη και τον αριθμό των ενδιάμεσων κόμβων. Παρέχει έτσι ανώνυμες συνδέσεις οι οποίες είναι εξαιρετικά ανθεκτικές τόσο στην υποκλοπή πληροφορίων όσο και στην ανάλυση κίνησης [31].

Στην παραλλαγή της δρομολόγησης κρεμμυδιού που χρησιμοποιείται στο Lightning η δρομολόγηση γίνεται στον αποστολέα (δρομολόγηση πηγής), πράγμα που σημαίνει ότι η διαδρομή που θα ακολουθήσει η πληρωμή καθορίζεται από τον αποστολέα και μόνο από τον αποστολέα. Η δρομολόγηση πηγής ενισχύει σημαντικά την ιδιωτικότητα του αποστολέα και του παραλήπτη.

Δημιουργία του κρεμμυδιού Ας θεωρήσουμε πάλι ότι η Αλίκη θέλει να στείλει μια πληρωμή στον Κώστα μόνο που αυτή την φορά δεν υπάρχει απευθείας κανάλι μεταξύ τους. Αντιθέτως, η πληρωμή μπορεί να ακολουθήσει την διαδρομή Αλίκη → Γιώργος → Ντίνα → Κώστας. Για να στείλει την πληρωμή, η Αλίκη αρχικά θα χτίσει το τελικό μήνυμα προς τον Κώστα και το κρυπτογραφεί με το δημόσιο κλειδί του Κώστα έτσι ώστε μόνο αυτός να μπορεί να το ανοίξει. Το κρυπτογραφημένο αυτό μήνυμα θα τοποθετηθεί μέσα σε ένα άλλο μήνυμα με παραλήπτη την Ντίνα. Μαζί με το κρυπτογραφημένο μήνυμα για τον Κώστα, η Ντίνα θα λάβει και κάποιες οδηγίες για το που να στείλει το μήνυμα που έλαβε. Ολόκληρο το μήνυμα με προορισμό την Ντίνα προέρχεται όμως από τον Γιώργο, οπότε εκείνος χρειάζεται επίσης ένα αντίστοιχο μήνυμα στο οποίο μέσα βρίσκονται οδηγίες και το κρυπτογραφημένο μήνυμα για την Ντίνα. Το τελευταίο είναι το μήνυμα που στέλνει η Αλίκη στον Γιώργο όπως φαίνεται στο σχήμα 8.2.

Ο Γιώργος λαμβάνει το μήνυμα από την Αλίκη, χωρίς να γνωρίζει αν η Αλίκη το δημιούργησε εξ αρχής ή αν και η Αλίκη είναι ένας από τους κόμβους δρομολόγησης που απλός προωθούν τα μηνύματα. Ο Γιώργος αποκρυπτογραφεί το μήνυμα, διαβάζει τις οδηγίες και προωθεί το μήνυμα που προορίζεται για την Ντίνα σε εκείνη. Το ίδιο σενάριο επαναλαμβάνεται για όλους τους ενδιάμεσους κόμβους μέχρι το μήνυμα να φτάσει στον τελικό του παραλήπτη. Ο τελικός παραλήπτης, ο Κώστας στο παράδειγμά μας, ανοίγει το μήνυμα που λαμβάνει από την Ντίνα αλλά, αντί από οδηγίες και κάποιο κρυπτογραφημένο μήνυμα, βρίσκει το μήνυμα της πληρωμής.

Κάθε ενδιάμεσος κόμβος μπορεί να ζητήσει κάποιο ποσό για την προώθηση ενός μηνύματος. Για κάθε κόμβο στον οποίο απαιτείται πληρωμή η Αλίκη κατά την δημιουργία του κρεμμυδιού τοποθετεί



Σχήμα 8.2: Το τελικό πακέτο που δημιουργεί η Αλίκη στον Γιώργο

μαζί με τις οδηγίες και την σχετική πληρωμή. Όταν η κύρια πληρωμή επιβεβαιωθεί από τον τελικό κόμβο, τότε όλοι οι ενδιάμεσοι κόμβοι μπορούν να εισπράξουν τις δικές τους πληρωμές.

8.4 Ατομικές πολυμερείς πληρωμές

Όταν πρώτο εμφανίστηκε το Lightning όλες οι πληρωμές αποτελούνταν από μία μεταφορά. Αν το κανάλι ή τα ενδιάμεσα κανάλια αδυνατούσαν να μεταφέρουν το ποσό της πληρωμής, ο χρήστης έπρεπε να σπάσει την πληρωμή σε μικρότερες, ανεξάρτητες, πληρωμές ή να στείλει την πληρωμή από διαφορετική διαδρομή. Το 2020 προστέθηκε στο Lightning η δυνατότητα ατομικών πολυμερών πληρωμών (atomic multi-part payments). Οι πολυμερείς πληρωμές επιτρέπουν την διάσπαση μιας πληρωμής σε πολλές μεταφορές οι οποίες μπορούν να ακολουθήσουν διαφορετικές διαδρομές από τον αποστολέα ως τον παραλήπτη, διατηρώντας όμως την ιδιότητα της ατομικότητας, δηλαδή η πληρωμή είτε επιτυγχάνει είτε αποτυγχάνει εξ ολοκλήρου. Από την προσθήκη των πολυμερών πληρωμών φαίνεται να έχει αυξηθεί η πιθανότητα μια πληρωμή να είναι επιτυχής [5].

8.4.1 Διατήρηση ατομικότητας

Για την διατήρηση της ιδιότητας της ατομικότητας ο αποστολέας δημιουργεί ένα μοναδικό μυστικό στο οποίο προστίθενται τυχαίες τιμές για κάθε ξεχωριστή μεταφορά [29]. Για εξαργυρώσει τις ξεχωριστές μεταφορές ο παραλήπτης, πρέπει να έχει λάβει όλες τις μεταφορές ώστε να υπολογίσει το αρχικό μοναδικό μυστικό του αποστολέα [32].

Ένα αρνητικό των ατομικών πολυμερών πληρωμών είναι ότι είναι πλέον αδύνατο για τον παραλήπτη να αποδείξει την επιτυχία της πληρωμής αφού ο αποστολέας γνωρίζει το αρχικό μυστικό εξ αρχής [32].

8.4.2 Εύρεση κατάλληλης διαδρομής

Το επόμενο ερώτημα που πρέπει να απαντηθεί είναι το πώς πρέπει να χωρίζονται οι πληρωμές και ποιος είναι ο ιδανικός αριθμός ξεχωριστών μεταφορών;

Όλα τα κανάλια στην διαδρομή που ακολουθεί η μεταφορά πρέπει να έχουν διαθέσιμη ρευστότητα τουλάχιστον ίση με το ποσό που απαιτείται από την μεταφορά. Η ακριβής ρευστότητα κάθε καναλιού δεν είναι γνωστοποιείται από τον κόμβο με αποτέλεσμα να χρειάζονται πολλαπλές προσπάθειες για την επιτυχία μιας μεταφοράς. Από τα παραπάνω μπορούμε να συμπεράνουμε ότι μικρότερες μεταφορές έχουν μεγαλύτερα ποσοστά επιτυχίας (αφού είναι πιο πιθανό ένα κανάλι να έχει αρκετή ρευστότητα) και ότι όσο περισσότερα κανάλια χρησιμοποιούνται για μία μεταφορά τόσο μικρότερα ποσοστά επιτυχίας έχει.

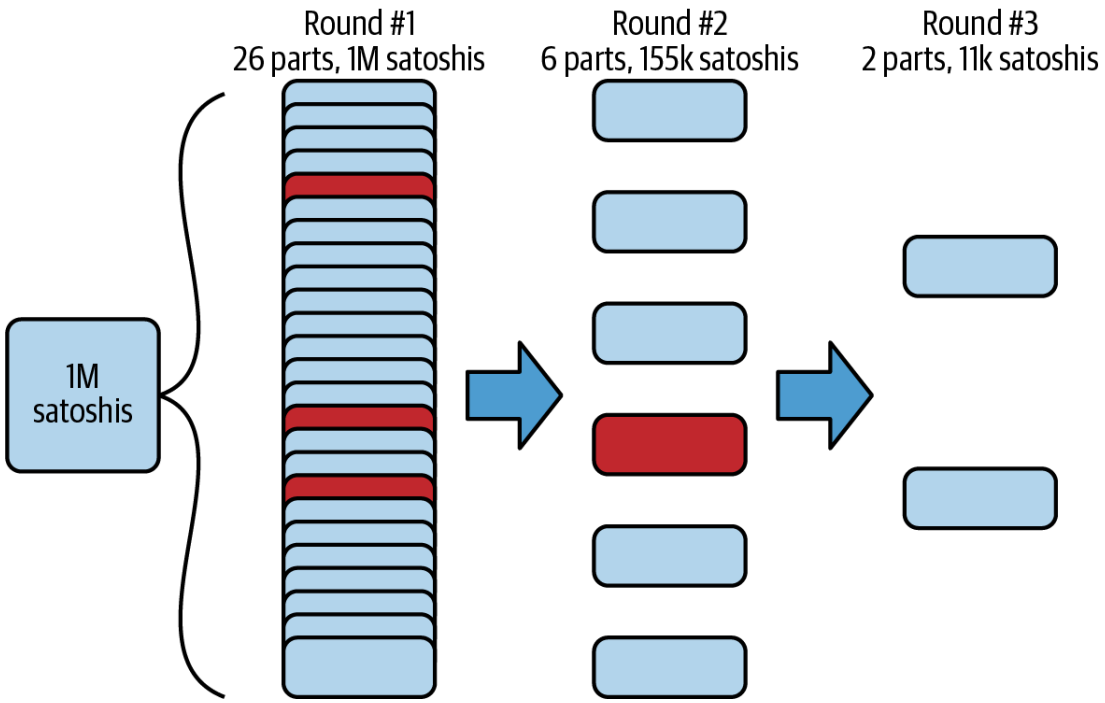
Η απάντηση στο ερώτημα "πώς πρέπει να χωρίζονται οι πληρωμές;" είναι αρκετά περίπλοκη. Πρόκειται για ένα πεδίο στο οποίο γίνονται ακόμη έρευνες και έχουν προταθεί διαφορετικές απαντήσεις. Στο [33] οι συγγραφείς περιγράφουν μια λύση που αναλύει τις πληρωμές σε προβλήματα ροής ελάχιστου κόστους (minimum cost flow problems). Λύση την οποία θεωρούν βέλτιστη. Μία άλλη μέθοδος για τον χωρισμό μια πληρωμής βασίζεται σε μια αρκετά πιο απλή στρατηγική, τον χωρισμό της πληρωμής σε 2, 4 και ούτω καθεξής μέρη.

Στις ατομικές πολυμερείς πληρωμές αν αποτύχει μια από τις μεταφορές ο αποστολέας μπορεί να την χωρίσει πάλι σε μικρότερες μεταφορές, διαλέγοντας διαφορετικά μονοπάτια, αυξάνοντας έτσι την πιθανότητα να φτάσουν στον παραλήπτη με επιτυχία. Στο σχήμα 8.3 βλέπουμε μια πληρωμή 1εκ shatoshis, που αρχικά χωρίζεται σε 26 αποστολές, 3 εκ των οποίων αποτυγχάνουν, με αποτέλεσμα 155 χιλιάδες shatoshis να χωρίζονται ξανά σε 6 αποστολές, μια εκ των οποίων αποτυγχάνει ξανά και χωρίζεται σε 2 αποστολές οι οποίες τελικά επιτυγχάνουν και ολοκληρώνουν έτσι την πληρωμή. Σε κάθε γύρω που υπάρχουν αποτυχημένες μεταφορές ο αποστολέας δρομολογεί εκ νέου το υπολειπόμενο ποσό.

8.5 Παρατηρητήρια

Όπως έχει ήδη αναφερθεί, μια οντότητα μπορεί να μην είναι διαθέσιμη για οποιονδήποτε λόγο. Ένας από τους λόγους μπορεί να είναι ότι κόπηκε η σύνδεσή της στο διαδίκτυο. Σε μια τέτοια περίπτωση η οντότητα είναι ευάλωτη και κινδυνεύει από κακούς πράκτορες που μπορούν να οδηγήσουν τα κανάλια που έχουν με την αρχική οντότητα σε αναγκαστικό κλείσιμο δημοσιεύοντας μια παλιά συναλλαγή δέσμευσης που να τους ευνοεί. Αν η οντότητα, της οποίας κόπηκε η σύνδεση, καταφέρει να επανασυνδεθεί και δει το αναγκαστικό κλείσιμο, τότε μπορεί να χρησιμοποιήσει το μυστικό ακύρωσης και να τιμωρήσει τον κακό πράκτορα, όπως αναφέρθηκε και σε προηγούμενο κεφάλαιο.

Τι γίνεται όμως αν δεν καταφέρει να επανασυνδεθεί μέσα στον χρόνο κλειδώματος; Μια λύση που προσφέρεται στο Lightning είναι η χρήση παρατηρητήριων [29]. Τα παρατηρητήρια είναι άλλοι κόμβοι του Lightning που ιδανικά λειτουργούν σε ξεχωριστό μηχάνημα και δίκτυο από τον κόμβο που επιβλέπουν έτσι ώστε να μην επηρεάζονται από τις ίδιες βλάβες. Ένα παρατηρητήριο απαιτείται να είναι σχεδόν πάντα συνδεδεμένο και να παρακολουθεί κάθε μπλοκ που εισέρχεται στο bitcoin για πιθανές παραβιάσεις. Για να μην χρειάζεται να βασιστεί σε μεσάζοντες, ένα παρατηρητήριο είναι



Σχήμα 8.3: Πληρωμή που χωρίζεται σταδιακά σε μικρότερες αποστολές μέχρι να σταλθεί ολόκληρη [5]

θεμιτό να τρέχει και τον δικό του κόμβο bitcoin, πράγμα που το καθιστά και πιο ασφαλές.

Για κάθε συναλλαγή δέσμευσης, οι κόμβοι των μελών του καναλιού δημιουργούν και μια συναλλαγή ακύρωσης και την στέλνουν, κρυπτογραφημένα με το αναγνωριστικό της συναλλαγής δέσμευσης, στα παρατηρητήριά τους μαζί με το πρώτο μισό του αναγνωριστικού της συναλλαγής. Έτσι τα παρατηρητήρια γνωρίζουν ποιες συναλλαγές χρειάζεται να επιβλέπουν χωρίς να έχουν πρόσβαση στην συναλλαγή δέσμευσης.

Όταν ένα παρατηρητήριο βρίσκει μια παραβίαση, τότε αποκρυπτογραφεί την συναλλαγή ακύρωσης και να τη δημοσιεύσει στην αλυσίδα του bitcoin. Ο κακός πράκτορας χάνει το κεφάλαιο που ήταν κλειδωμένο και το εισπράττει το άλλο μέλος του καναλιού.

Κεφάλαιο 9ο: Η εφαρμογή μας - Μια περίπτωση χρήσης

9.1 Εισαγωγή

Με σκοπό να αναδείξουμε τα πλεονεκτήματα της τεχνολογίας των αλυσίδων μπλοκ, και συγκεκριμένα του Lightning Network, αναπτύξαμε μια εφαρμογή μέσω της οποίας παρουσιάζεται ένας τρόπος για το πως μπορεί οποιοσδήποτε ιστότοπος με περιεχόμενο κειμένου να εκμεταλλευτεί το Lightning ως μέσο χρηματοδότησής του.

Σε αυτό το κεφάλαιο θα δούμε με ποιους τρόπους γίνεται η χρηματοδότηση ενός τέτοιου ιστότοπου χωρίς την χρήση αλυσίδων συστοιχιών, θα αναλύσουμε τα πλεονεκτήματα και τα μειονεκτήματα τους, καθώς και αυτά της χρηματοδότησης μέσω αλυσίδων, και τέλος θα παρουσιάσουμε την εφαρμογή που αναπτύξαμε.

9.2 Παραδοσιακοί τρόποι χρηματοδότησης ιστοτόπου

Πριν την εμφάνιση του διαδικτύου το πιο διαδεδομένο μέσω βασισμένο σε γραπτό κείμενο (πέραν των βιβλίων) ήταν οι εφημερίδες και τα περιοδικά. Για να μπορέσει κάποιος να διαβάσει κάτι από μια εφημερίδα ή από ένα περιοδικό έπρεπε να το αγοράσει, και μάλιστα ολόκληρο. Ο καταναλωτής είχε επίσης την επιλογή να κάνει συνδρομή σε μια εφημερίδα και να λαμβάνει κάθε νέα έκδοση πληρώνοντας την εκάστοτε συνδρομή.

Από την εμφάνιση του διαδικτύου και έπειτα, πολλές εφημερίδες άρχισαν να μεταφέρονται σε αυτό, είτε εξ ολοκλήρου είτε μερικώς. Το 2016 πάνω από το 65% των ατόμων ηλικίας 18 με 29 ενημερώνονται μέσω του διαδικτύου [34].

Στους ιστότοπους η χρηματοδότηση παίρνει άλλη μορφή καθώς η ανάγκη να αγοράσει κανείς ολόκληρη μια εφημερίδα εξαφανίζεται και το συνδρομητικό μοντέλο κάνει χώρο για άλλες πιο αποτελεσματικές μεθόδους.

9.2.1 Συνδρομητικό μοντέλο

Στο συνδρομητικό μοντέλο ο ιστότοπος επιβάλλει ένα ετήσιο ή μηνιαίο συνήθως κόστος στον καταναλωτή ώστε να έχει πρόσβαση στο περιεχόμενο.

Οι ιστότοποι που κρατούν το συνδρομητικό μοντέλο το κάνουν επειδή πιστεύουν ότι οι καταναλωτές πρέπει να πληρώνουν άμεσα για το υψηλό κόστος της δημοσιογραφίας. Το συνδρομητικό μοντέλο πετυχαίνει κυρίως σε περιπτώσεις που ο εκδότης γνωρίζει την ύπαρξη ενός κοινού το οποίο είναι πρόθυμο να πληρώσει για το συγκεκριμένο περιεχόμενο και χρησιμοποιείται συνήθως σε συνδυασμό με διαφημίσεις [34].

Ένα αρνητικό του συνδρομητικού μοντέλου είναι ότι ένας χρήστης δίχως συνδρομή δεν έχει πρόσβαση στα κείμενα του ιστότοπου και είτε πρέπει να αγοράσει ένα κείμενο μεμονωμένα, εφόσον αυτό υποστηρίζεται από τον ιστότοπο, είτε να κάνει συνδρομή παρόλο που ενδιαφέρεται μόνο για το μεμονωμένο κείμενο. Επίσης, χρήστες με συνδρομή μπορεί να μην ενδιαφέρονται για πολλές από

τις δημοσιεύσεις και έτσι να πληρώνουν ολόκληρη την συνδρομή ακόμη και αν διαβάζουν ελάχιστα κείμενα κάθε φορά.

Στα θετικά του συνδρομητικού μοντέλου βρίσκονται το γεγονός ότι αποτελεί ένα σχετικά σταθερό εισόδημα για τον ιστότοπο και το γεγονός ότι το συνδρομητικό κοινό είναι συνήθως συγκεκριμένο και έτσι ο ιστότοπος μπορεί να χρεώσει περισσότερο για στοχευμένες διαφημίσεις.

9.2.2 Διαφημίσεις

Οι διαφημίσεις είναι από τους πιο διαδεδομένους και πετυχημένους τρόπους χρηματοδότησης περιεχομένου στο διαδίκτυο.

Ένα από αρνητικά των διαφημίσεων είναι ότι οι χρήστες είναι πλέον τόσο συνηθισμένοι σε αυτές, που τείνουν να τις αγνοούν [34]. Ένα δεύτερο αρνητικό είναι ότι βλάπτουν την εμπειρία του χρήστη καθώς είναι συνήθως ενοχλητικές, βλάπτοντας έτσι την εικόνα του διαφημιστή αλλά και του ιστότοπου [35].

Τέλος, οι διαφημίσεις αποδίδουν καλύτερα σε ιστότοπους με πολύ κίνηση και πολλούς χρήστες. Αυτό σημαίνει ότι ιστότοποι με χαμηλό αριθμό επισκεπτών δεν μπορούν πάντα να βασίζονται μόνο σε διαφημίσεις και αναζητούν εναλλακτικές.

9.2.3 Εναλλακτικές

Οι διαφημίσεις από μόνες τους δεν μπορούν να παράγουν επαρκή έσοδα. Το συνδρομητικό μοντέλο είναι ασύμβατο με τον τρόπο με τον οποίο οι καταναλωτές καταναλώνουν κείμενα στο διαδίκτυο, αφού οι χρήστες διαβάζουν περιεχόμενο από πολλές πηγές και όχι μόνο από έναν ιστότοπο [36].

Υπάρχουν όμως και πολλοί άλλοι τρόποι, εκτός των συνηθισμένων διαφημίσεων και του συνδρομητικού μοντέλου, που μπορούν να χρησιμοποιηθούν για την χρηματοδότηση ενός ιστότοπου. Παρακάτω παρατίθενται ορισμένες εναλλακτικές λύσεις που χρησιμοποιούνται.

Χορηγούμενα άρθρα Ένα κείμενο θεωρείται χορηγούμενο, όταν για αυτό πληρώνει ένας διαφημιζόμενος. Συνήθως επισημαίνεται ως "Χορηγούμενο άρθρο", "Χορηγούμενο περιεχόμενο" ή μπορεί να υπάρχει μια υποσημείωση που εξηγεί ότι πρόκειται για χορηγία.

Ψηφιακά προϊόντα Πρόκειται για την πώληση ψηφιακών προϊόντων όπως φωτογραφίες, ψηφιακά βιβλία, 3D μοντέλα, σχέδια, μαθήματα κ.α. Τα προϊόντα συνήθως σχετίζονται με το κείμενο αλλά μπορεί να είναι και ανεξάρτητα.

Διαφημίσεις στα ενημερωτικά e-mail (newsletters) Μπορεί να χρησιμοποιηθεί για την μείωση διαφημίσεων στον ιστότοπο.

Freemium μοντέλο Στο freemium μοντέλο, οι χρήστες έχουν πρόσβαση στην δωρεάν/βασική έκδοση του ιστότοπου αλλά πρέπει να πληρώσουν ή να έχουν συνδρομή για να αποκτήσουν πρόσβαση σε κλειδωμένο περιεχόμενο [36]. Η λέξη freemium προέρχεται από την ένωση των λέξεων free (δωρεάν) και premium (που αναφέρεται στο κλειδωμένο περιεχόμενο).

Σύνδεσμοι συνεργατών (Affiliate Links) Ένας έμπορος παρέχει αμοιβή παραπομπής, που κυμαίνεται από 5 έως 20 τοις εκατό, ως ανταμοιβή για τις άμεσες πωλήσεις που αποδίδονται στον ιστότοπο.

Έρευνες αγοράς και αναλύσεις Στον κόσμο του ηλεκτρονικού εμπορίου, τα δεδομένα των καταναλωτών είναι χρυσορυχείο. Οι εταιρείες, ιδίως εκείνες που δραστηριοποιούνται σε εξειδικευμένες αγορές, θέλουν να γνωρίζουν τα πάντα για τους πιθανούς πελάτες τους, τι τους αρέσει και τι όχι, τις συνήθειες τους κ.α. Οι ιστότοποι μπορούν να αποκτήσουν πρόσβαση σε αυτά τα πολύτιμα δεδομένα με ερωτηματολόγια, δημοσκοπήσεις και αναλύοντας συνήθειες περιήγησης. Στη συνέχεια μπορούν να πουλήσουν αυτήν την έρευνα αγοράς και τις πληροφορίες των πελατών σε άλλες εταιρείες.

9.2.4 Μικροπληρωμές

Οι μικροπληρωμές είναι μια ακόμη εναλλακτική για την χρηματοδότηση ιστότοπων. Μέσω μικροπληρωμών ο καταναλωτής μπορεί να πληρώσει για συγκεκριμένα κείμενα, άρθρα κλπ. χωρίς να χρειάζεται κάποια συνδρομή. Με το μοντέλο των μικροπληρωμών το μέγεθος της πληροφορίας για την οποία πληρώνει ο καταναλωτής μπορεί να είναι όσο μικρό ή μεγάλο επιλέξει ο ιστότοπος. Παραδείγματος χάριν ο ιστότοπος μπορεί να προσφέρει το κείμενο ολόκληρο ή χωρισμένο σε ενότητες, κεφάλαια, παραγράφους ή ακόμα και προτάσεις. Αυτό δίνει στον καταναλωτή μεγαλύτερο έλεγχο πάνω στο πόσα χρήματα θα ξοδέψει σε ένα κείμενο που ίσως τελικά δεν τον ενδιαφέρει καθόλου ή που τελικά δεν έχει χρόνο να διαβάσει ολόκληρο.

Επιπρόσθετα, ένα σύστημα μικροπληρωμών ανοίγει την πόρτα στην ανάπτυξη επιπλέον λειτουργιών όπως ένα σύστημα επιβράβευσης, όπως περιγράφεται στο [36], όπου οι χρήστες που μοιράζονται τον σύνδεσμο του κειμένου με φίλους και γνωστούς τους επιβραβεύονται.

Περιορισμοί των μικροπληρωμών παραστατικού χρήματος Καθώς οι συναλλαγές σε ένα τέτοιο σύστημα είναι πολλές και μικρής αξίας, ο παραδοσιακός τρόπος πληρωμής μέσω παραστατικού χρήματος είναι ακατάλληλος αφού θα υπάρχουν παρακρατήσεις για κάθε συναλλαγή.

Μια λύση στο πρόβλημα αυτό είναι η δημιουργία και πώληση πόντων στους καταναλωτές. Αγοράζοντας πόντους ο καταναλωτής κάνει μόνο μια πραγματική συναλλαγή και έπειτα χρησιμοποιεί τους πόντους για περαιτέρω συναλλαγές στον ιστότοπο, χωρίς καμία χρέωση ούτε για τον ίδιο αλλά ούτε και για τον ιστότοπο. Οι ίδιοι πόντοι μπορούν να χρησιμοποιηθούν και για τυχών επιβραβεύσεις.

Ένα πρόβλημα με την χρήση πόντων είναι ότι ο χρήστης έχει χάσει πάλι τον έλεγχο στο πόσα

χρήματα θα δώσει στον ιστότοπο, αφού είναι υποχρεωμένος να αγοράσει πολλούς πόντους μαζί, ακόμη και αν δεν τους χρειαστεί όλους.

Στην συνέχεια θα δούμε πως μπορεί να λυθεί αυτό με την χρήση αλυσίδων μπλοκ.

Μικροπληρωμές μέσω αλυσίδων μπλοκ Όπως είδαμε σε προηγούμενο κεφάλαιο, τα εξειδικευμένα δίκτυα μικροπληρωμών έχουν πολύ χαμηλά ως και μηδενικά κόστη συναλλαγών και οι συναλλαγές διεκπεραιώνονται άμεσα.

Χρησιμοποιώντας τέτοιες αλυσίδες μπλοκ για τις μικροπληρωμές στους ιστότοπους δεν υπάρχει πλέον η ανάγκη αγοράς πόντων από τον καταναλωτή αφού μπορεί να πληρώσει κατευθείαν το ποσό, χωρίς να επιβαρυνθεί κανείς σημαντικά από τα έξοδα της συναλλαγής.

Περαιτέρω, κάποια δίκτυα μικροπληρωμών υποστηρίζουν και έξυπνα συμβόλαια μέσω των οποίων ο ιστότοπος μπορεί να προσθέσει ακόμα περισσότερες λειτουργίες, αντίστοιχες της επιβράβευσης των χρηστών.

9.3 Pay as you read demo blog

9.3.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα αναλύσουμε λεπτομερώς την εφαρμογή που αναπτύξαμε στα πλαίσια αυτής της διπλωματικής. Πρόκειται για ένα ιστολόγιο (blog) στο οποίο ο χρήστης έχει την δυνατότητα να διαβάσει κείμενα αγοράζοντας τα σε μέρη, χρησιμοποιώντας το δίκτυο του Lightning για την διεκπεραίωση των πληρωμών. Ο χρήστης πιστοποιεί την αυθεντικότητά του μέσω του ψηφιακού του πορτοφολιού και αποθηκεύει τα αγορασμένα κείμενα τοπικά ώστε να μπορεί να τα ξαναδιαβάσει όποτε επιθυμεί.

Όταν ο χρήστης αγοράζει ένα κομμάτι του κειμένου το λαμβάνει αμέσως μόλις επιβεβαιωθεί η πληρωμή του από τον διακομιστή. Χάρη στο Lightning αυτό συμβαίνει συνήθως άμεσα (μια μεταφορά μπορεί να αποτύχει για διάφορους λόγους, παραδείγματος χάριν ένα κανάλι από το οποίο έχει δρομολογηθεί να περάσει η μεταφορά μπορεί να μην έχει την χωρητικότητα να επεξεργαστεί την συγκεκριμένη μεταφορά. Σε περίπτωση αποτυχίας η αποστολή επαναλαμβάνεται έχοντας όμως πλέον καθυστερήσει).

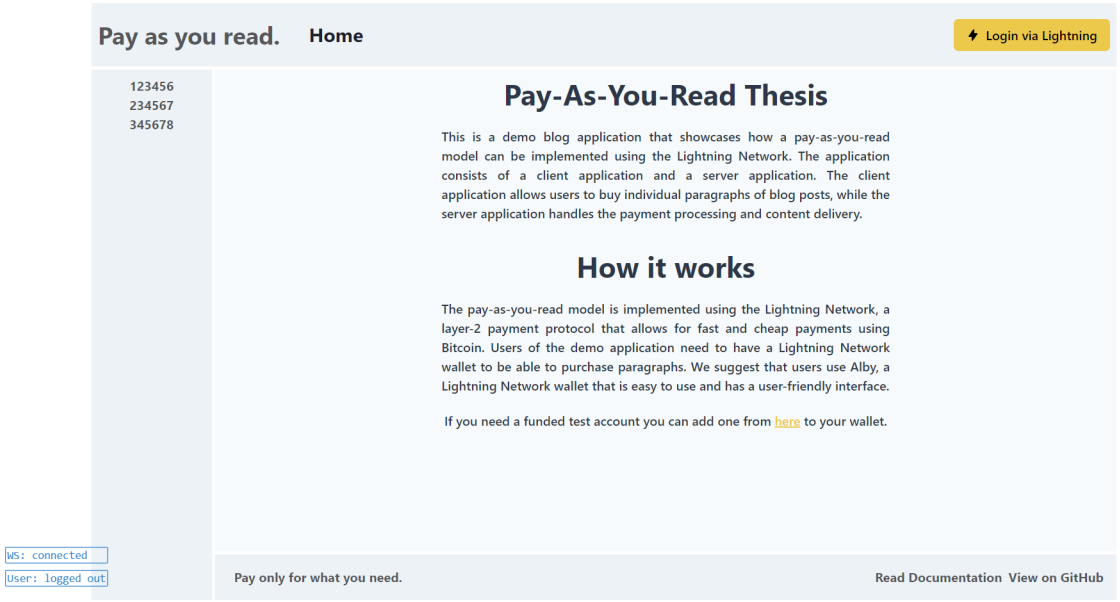
Οι κόμβοι Lightning του διακομιστή και του χρήστη δεν χρειάζεται να έχουν άμεση σύνδεση μέσω αποκλειστικού καναλιού, αρκεί να υπάρχει κάποια διαδρομή μέσω άλλων καναλιών που να τους συνδέει. Οι περισσότεροι κόμβοι στο Lightning είναι ευρέως διασυνδεδεμένοι με αποτέλεσμα να υπάρχει πάντα κάποια διαδρομή.

9.3.2 Τυπική ροή χρήσης της εφαρμογή

Συνεχίζοντας θα δούμε πως μπορεί αν αλληλοεπιδράσει ένας χρήστης με την εφαρμογή.

Όταν ο χρήστης επισκεφτεί το ιστολόγιο για πρώτη φορά θα αντικρίσει την αρχική σελίδα του ιστολόγιου όπως φαίνεται στην εικόνα 9.1

Διαβάζοντας την σελίδα από πάνω αριστερά προς τα κάτω δεξιά ο χρήστης βλέπει δει τίτλο του ιστολόγιου, ακριβώς δεξιά τον σύνδεσμο "Home" όπου όταν πατηθεί, επιστρέφει τον χρήστη στην συγκεκριμένη σελίδα και τέλος την πάνω δεξιά γωνία υπάρχει το κουμπί για την αυθεντικοποίηση του χρήστη μέσω του ψηφιακού πορτοφολιού του, το οποίο θα πρέπει να υποστηρίζει το Lightning.



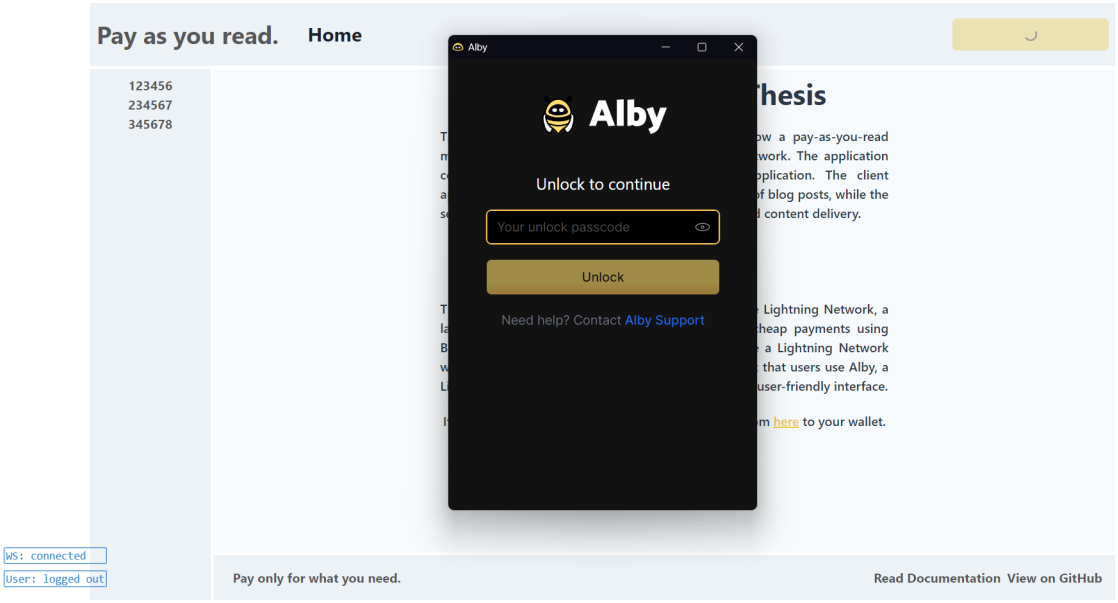
Σχήμα 9.1: Η αρχική σελίδα του ιστολόγιου

Στην εικόνα 9.2 φαίνεται το παράθυρο που ανοίγει όταν πατήσει ο χρήστης να το κουμπί για την αυθεντικοποίηση. Στο συγκεκριμένο παράδειγμα ο χρήστης χρησιμοποιεί το ψηφιακό πορτοφόλι Alby. Παραθέτουμε περισσότερες πληροφορίες για τα ψηφιακά πορτοφόλια και συγκεκριμένα για το Alby σε επόμενη ενότητα. Έπειτα από την επιτυχή αυθεντικοποίηση του χρήστη το κουμπί φεύγει ώστε να εμφανιστεί στην θέση του ένα καλωσόρισμα για τον χρήστη. Το καλωσόρισμα αποτελείται από την λέξη "Hello" και ακολουθείται από το ψευδώνυμο που έχει ορίσει ο χρήστης στο ψηφιακό του πορτοφόλι.

Συνεχίζοντας, η στήλη που καλύπτει το μεγαλύτερο μέρος της αριστερής πλευράς του ιστολόγιου, αποτελεί την λίστα των διαθέσιμων κειμένων που είναι διαθέσιμα προς ανάγνωση ή/και αγορά από τον χρήστη. Πατώντας σε ένα από τα αναγνωριστικά κειμένου από την λίστα ο χρήστης οδηγείται σε μια νέα σελίδα, την σελίδα του συγκεκριμένου όπως φαίνεται στην εικόνα 9.3. Στην νέα σελίδα ο χρήστης μπορεί να διαβάσει όλα τα κομμάτια του κειμένου που έχει αγοράσει καθώς και να αγοράσει τα υπόλοιπα χρησιμοποιώντας το κουμπί "Buy next paragraph".

Στην εικόνα 9.4 φαίνεται το παράθυρο που ανοίγει το ψηφιακό πορτοφόλι Alby όταν ο χρήστης θέλει να κάνει μια πληρωμή. Μόλις η πληρωμή επιβεβαιωθεί στην μεριά του διακομιστή, ο χρήστης θα λάβει το κομμάτι του κειμένου που μόλις αγόρασε.

Με την αγορά του τελευταίου κομματιού του κειμένου, ο διακομιστής ενημερώνει τον χρήστη ότι έχει αγοράσει ολόκληρο το κείμενο, εικόνα 9.5



Σχήμα 9.2: Οθόνη αυθεντικοποίησης μέσω Alby

Επιπλέον, ο χρήστης μπορεί να περιηγηθεί στον ιστότοπο όπως επιθυμεί και μπορεί να διαβάσει ή/και να αγοράσει επιπλέον μέρη από κείμενα.

9.3.3 Αρχιτεκτονική

Η αρχιτεκτονική που εφαρμόστηκε κατά την ανάπτυξη του ιστολόγιου ακολουθεί το μοντέλο πελάτη-εξυπηρετητή (client-server).

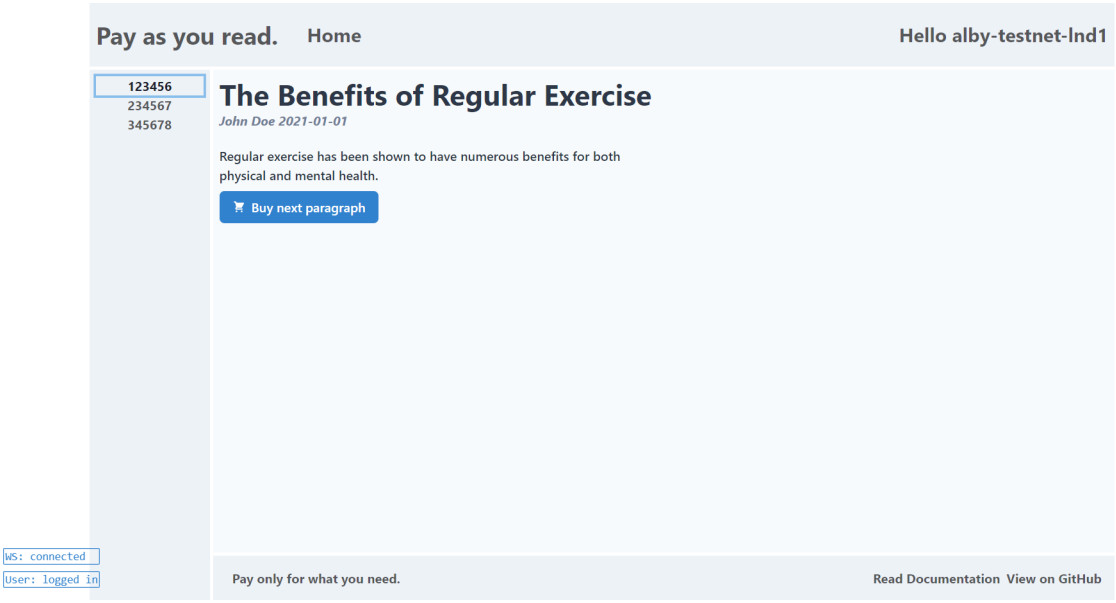
Στην αρχιτεκτονική πελάτη-εξυπηρετητή υπάρχει ένας εξυπηρετητής (συνήθως ένας αλλά μπορεί να είναι περισσότεροι) ο οποίος λαμβάνει και επεξεργάζεται αιτήματα, και πολλαπλοί πελάτες οι οποίοι δημιουργούν αυτά τα αιτήματα. Ένα αίτημα μπορεί να είναι η αρχική σελίδα ενός ιστότοπου, όπου ένας πελάτης στέλνει αίτημα σε έναν εξυπηρετητή ότι θέλει να δει την αρχική σελίδα του ιστότοπου που εξυπηρετεί ο συγκεκριμένος διακομιστής. Ο διακομιστής θα απαντήσει στον πελάτη στέλνοντάς του όποιες πληροφορίες χρειάζονται.

Η αρχιτεκτονική αυτή έχει αρκετά πλεονεκτήματα, μερικά από τα οποία παρουσιάζονται παρακάτω:

1. Κάθε οντότητα στο μοντέλο αυτό είναι ξεχωριστή, γεγονός που καθιστά την συντήρηση του συστήματος πολύ εύκολη. Η εύκολη συντήρηση είναι το κύριο πλεονέκτημα του μοντέλου πελάτη-εξυπηρετητή.

2. Η αρχιτεκτονική πελάτη-εξυπηρετητή ευνοεί την κλιμάκωση [37]. Η δυνατότητα κλιμάκωσης μιας εφαρμογής, καθώς αυξάνεται η ζήτηση και πληθαίνουν οι απαιτήσεις και οι λειτουργίες της, είναι απαραίτητη και αποτελεί ένα από τα σημαντικά πλεονεκτήματα της αρχιτεκτονικής.

3. Πολλαπλοί πελάτες μπορούν να έχουν πρόσβαση στην πληροφορία του εξυπηρετητή ταυτόχρονα και από διάφορες τοποθεσίες.



Σχήμα 9.3: Η σελίδα του άρθρου με αναγνωριστικό 123456

9.3.4 Γλώσσες προγραμματισμού

Η γλώσσα προγραμματισμού που χρησιμοποιήσαμε στην εφαρμογή είναι η TypeScript, η οποία είναι μια γλώσσα προγραμματισμού βασισμένη στην JavaScript.

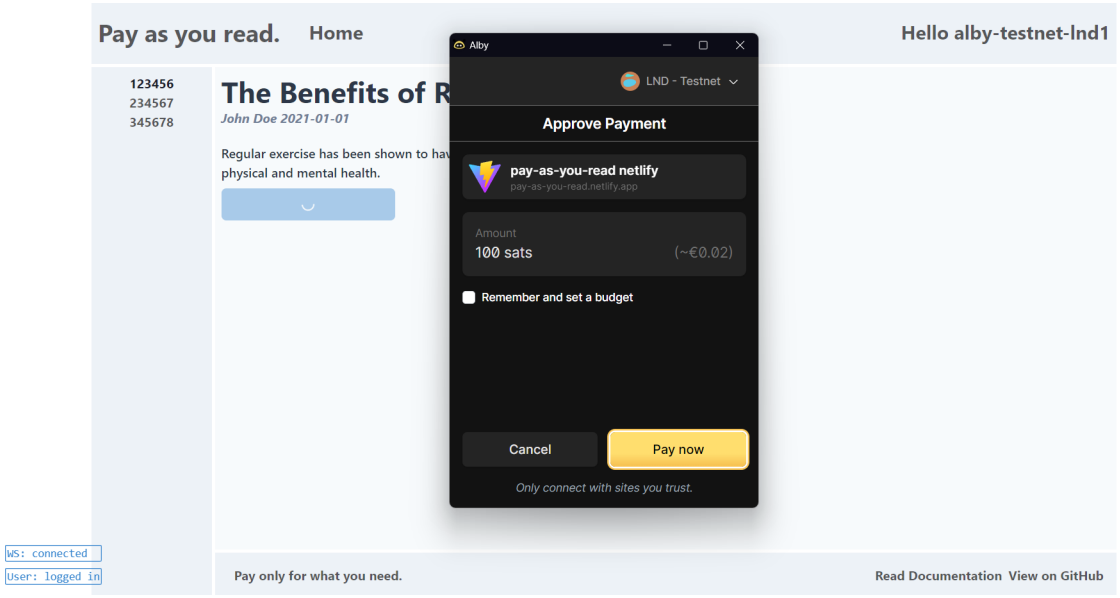
Η Typescript, μεταξύ άλλων, παρέχει πρόσθετη σύνταξη στη JavaScript για να υποστηρίξει μια στενότερη ενσωμάτωση με τα εργαλεία που χρησιμοποιούνται από τους προγραμματιστές κατά την διάρκεια της ανάπτυξης και της συντήρησης μίας εφαρμογής. Βοηθάει στον εντοπισμό σφαλμάτων στο στάδιο της ανάπτυξης, σε αντίθεση με την JavaScript, όπου πολλά σφάλματα εντοπίζονται αργά ή και καθόλου.

Όπως και το μοντέλο πελάτη-εξυπηρετητή έτσι και η Typescript ευνοεί σημαντικά την κλιμάκωση αφού ο κώδικας που παράγεται είναι πιο ευανάγνωστος, πιο σωστά δομημένος και διευκολύνει έτσι την συντήρηση και την προσθήκη επιπλέον λειτουργιών.

9.3.5 Εργαλεία

Κατά την ανάπτυξη της εφαρμογής χρησιμοποιήσαμε κάποια εργαλεία που μας βοήθησαν να την ολοκληρώσουμε πιο γρήγορα και με μεγαλύτερη ευκολία. Σε αυτή την ενότητα να αναφερθούμε στα εργαλεία αυτά.

GitHub Το GitHub είναι μια από τις πιο δημοφιλής πλατφόρμες Git hosting. Είναι μια πλατφόρμα η οποία βοηθάει προγραμματιστές να συνεργαστούν μεταξύ τους και να αναπτύξουν εφαρμογές. Έχει εξελιχθεί σε μια πλήρη σουίτα εφαρμογών που επιτρέπει σε προγραμματιστές αλλά και διάφορες οντότητες γύρω από μια εφαρμογή να αυτοματοποιούν εργασίες, να συντονίζονται, να παρουσιάζουν το έργο τους και πολλά άλλα. Προτιμάται από πολλές εφαρμογές ανοιχτού κώδικα.



Σχήμα 9.4: Το παράθυρο που ανοίγει μέσω του ψηφιακού πορτοφολιού Alby για την επιβεβαίωση πληρωμής

Netlify Χρησιμοποιήσαμε το Netlify για την φιλοξενία (hosting) της εφαρμογής πελάτη (ιστολόγιου).

Η Netlify είναι μια πλατφόρμα που βασίζεται στο cloud και απλοποιεί και βελτιώνει τη διαδικασία φιλοξενίας ιστότοπων και εφαρμογών ιστού. Προσφέρει μια ομαλή εμπειρία για τους προγραμματιστές, παρέχοντας χαρακτηριστικά όπως η συνεχής ενσωμάτωση και συνεχής ανάπτυξη (CI/CD), η αυτόματη κλιμάκωση και η εύκολη διαχείριση domain. Με τη διαισθητική διεπαφή του, οι προγραμματιστές μπορούν να συνδέσουν τα αποθετήρια του κώδικά τους (όπως το GitHub) με το Netlify, επιτρέποντας την αυτόματη ανανέωση του ιστότοπου κάθε φορά που γίνονται αλλαγές στον κώδικα. Αυτό δημιουργεί αποτελεσματικές ροές εργασίας και διασφαλίζει ότι η τελευταία έκδοση του ιστότοπου ή της εφαρμογής είναι πάντα διαθέσιμη στους χρήστες. Το Netlify υποστηρίζει επίσης μια πληθώρα άλλων χαρακτηριστικά όπως τον αυτόματο χειρισμό φορμών, καθιστώντας το μια ολοκληρωμένη λύση για τις σύγχρονες ανάγκες ανάπτυξης και φιλοξενίας ιστοσελίδων.

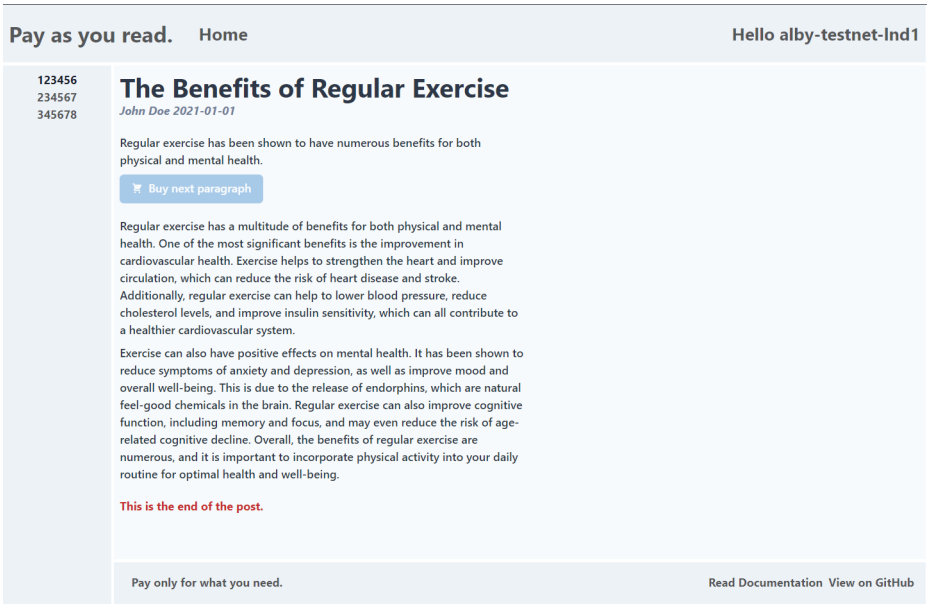
Render Για την φιλοξενία του εξυπηρετητή χρησιμοποιήσαμε το Render.

Το Render είναι μια πλατφόρμα φιλοξενίας εφαρμογών, υποστηρίζει εφαρμογές που τρέχουν σε JavaScript, Python, Ruby, Rust, Go, Elixir καθώς και Docker.

Όπως το Netlify έτσι και το Render, μεταξύ πολλών άλλων, προσφέρει και συνεχής ενσωμάτωση/συνεχής ανάπτυξη (CI/CD) μέσω Git.

Polar Κατά την αρχική ανάπτυξη της εφαρμογής χρησιμοποιήσαμε το Polar για την δημιουργία ενός εικονικού δικτύου Lightning.

Το Polar, όπως αναφέρεται και στην ιστοσελίδα τους, παρέχει "δίκτυα Bitcoin Lightning με ένα κλικ



Σχήμα 9.5: Παράδειγμα κειμένου το οποίο έχει αγοράσει εξ ολοκλήρου ο χρήστης

για τοπική ανάπτυξη και δοκιμή εφαρμογών" [38]. Μέσω του Polar στήσαμε διάφορα δοκιμαστικά δίκτυα Lightning τα οποία χρησιμοποιήσαμε για να αναπτύξουμε και να δοκιμάσουμε την εφαρμογή μας.

Alby Το Alby είναι ένα ψηφιακό πορτοφόλι για Bitcoin και υποστηρίζει και το δίκτυο του Lightning.

Κάθε χρήστης που θέλει να χρησιμοποιήσει την εφαρμογή μας, χρειάζεται ένα ψηφιακό πορτοφόλι που να υποστηρίζει και το δίκτυο Lightning ώστε να κάνει πληρωμές. Μέσω του Alby ο χρήστης μπορεί να εκτελέσει πληρωμές και να εξουσιοδοτήσει το πορτοφόλι του να κάνει πληρωμές χωρίς την άμεση συγκατάθεσή του για ένα προκαθορισμένο ποσό.

Στο Alby ο χρήστης μπορεί να έχει και να διαχειρίζεται πολλούς λογαριασμούς με ευκολία.

9.3.6 Τεχνολογίες

Επικοινωνία πελάτη εξυπηρετητή Η αλληλεπίδραση μεταξύ του πελάτη και του εξυπηρετητή στην εφαρμογή μας γίνεται μέσω ενός REST API και ενός WebSocket API. Στην συνέχεια αναλύουμε πώς λειτουργούν αυτές οι τεχνολογίες και πως τις έχουμε εκμεταλλευτεί στην εφαρμογή μας.

REST API Με βάση την IBM, τα REST APIs παρέχουν έναν ευέλικτο και ελαφρύ τρόπο για την ενσωμάτωση εφαρμογών και τη σύνδεση στοιχείων σε αρχιτεκτονικές μικρό-υπηρεσιών [39].

Τα REST APIs καθορίζουν ένα σύνολο αρχιτεκτονικών αρχών και περιορισμών για το σχεδιασμό ενός API αλλά και για την αλληλεπίδραση με αυτό. Παρέχουν έναν τυποποιημένο τρόπο επικοινωνίας μεταξύ διαφορετικών συστημάτων λογισμικού μέσω του διαδικτύου. Προσφέρουν ευελιξία,

επεκτασιμότητα και συμβατότητα, γεγονός που τα καθιστά δημοφιλή επιλογή για τη δημιουργία σύγχρονων εφαρμογών και υπηρεσιών ιστού.

Τα REST APIs χρησιμοποιούν μεθόδους HTTP για την εκτέλεση τυπικών λειτουργιών βάσης δεδομένων, όπως η δημιουργία (create), η ανάγνωση (read), η ενημέρωση (update) και η διαγραφή (delete) εγγραφών (γνωστή και ως CRUD) εντός ενός πόρου. Οι πιο συνηθισμένες μέθοδοι HTTP που χρησιμοποιούνται από τα REST APIs είναι οι εξής:

1. **GET:** Ανάκτηση δεδομένων από τον εξυπηρετητή.
2. **POST:** Δημιουργία δεδομένων στον εξυπηρετητή.
3. **PUT:** Ενημέρωση δεδομένων στον εξυπηρετητή.
4. **DELETE:** Διαγραφή δεδομένων από τον εξυπηρετητή.

Χάρη στην απλότητα της εφαρμογής μας, το REST API του εξυπηρετητή μας είναι σχετικά μικρό και απλό παρέχοντας μόνο δύο σημεία αλληλεπίδρασης (endpoints).

Το πρώτο επιστρέφει στον καλούντα τα αναγνωριστικά όλων των κειμένων (posts) που υπάρχουν στην στον εξυπηρετητή όπως φαίνεται στην εικόνα 9.6. Ο πελάτης μπορεί να το χρησιμοποιήσει κάνοντας ένα HTTP αίτημα τύπου GET στην τοποθεσία *https://<σύνδεσμος-εξυπηρετητή>/posts/*.

Το δεύτερο είναι διαθέσιμο στην τοποθεσία *https://<σύνδεσμος-εξυπηρετητή>/posts/:id* και, όταν κληθεί μέσω ενός αιτήματος τύπου GET, επιστρέφει στον καλούντα πληροφορίες για το κείμενο (post) με αναγνωριστικό *id*.

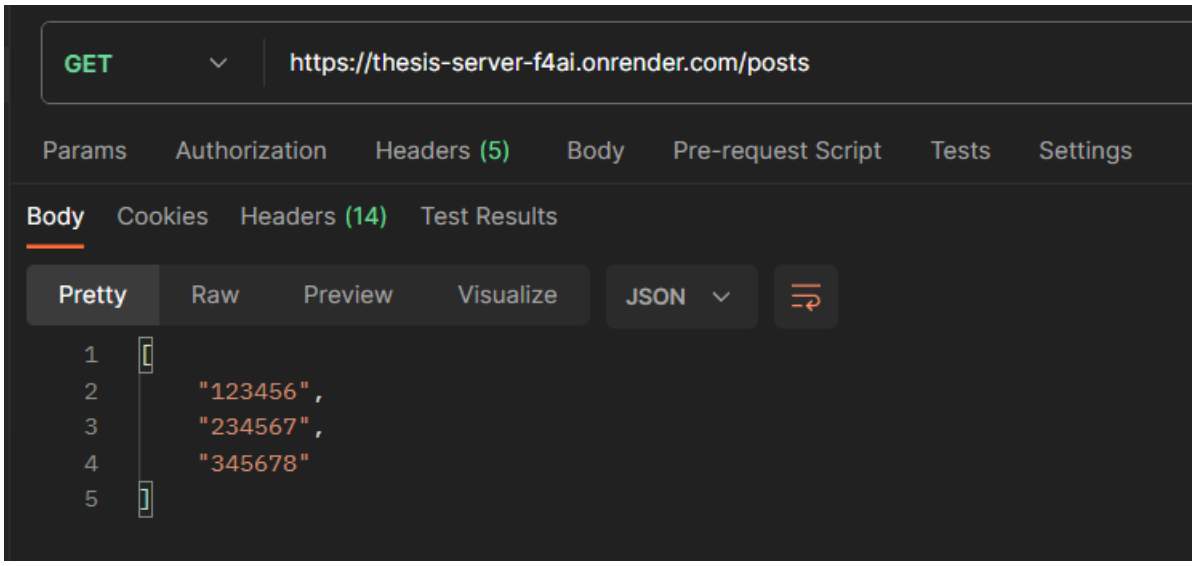
Οι πληροφορίες που επιστρέφουμε για το κείμενο είναι ο τίτλος του, η ημερομηνία, μια περίληψη, ο συγγραφέας και το αριθμός των παραγράφων από τις οποίες αποτελείται.

Αυτό που δεν επιστρέφει στον πελάτη σε καμία περίπτωση είναι το ίδιο το κείμενο, αφού αυτό παρέχεται στον πελάτη επί πληρωμή και μέσω του WebSocket API.

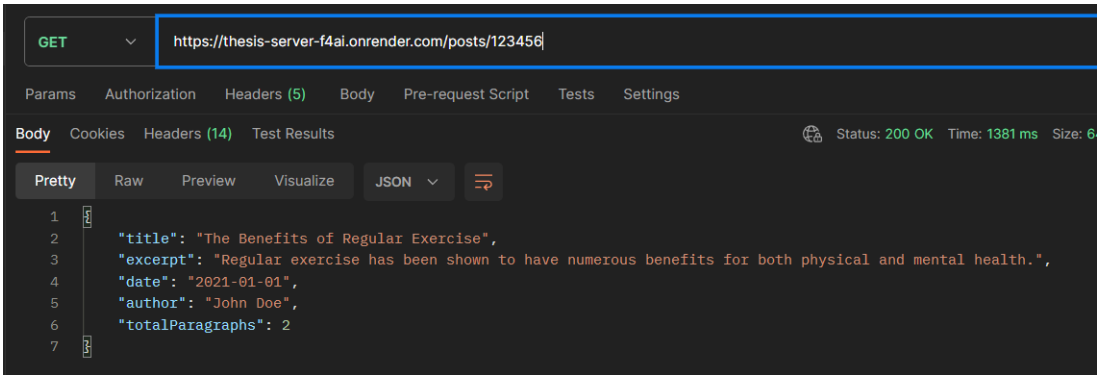
WebSocket API Πρόκειται για μια προηγμένη τεχνολογία που καθιστά δυνατή την έναρξη μιας αμφίδρομης διαδραστικής επικοινωνίας μεταξύ του προγράμματος περιήγησης του χρήστη και ενός εξυπηρετητή [40].

Σε αντίθεση με το παραδοσιακό πρωτόκολλο HTTP, το οποίο ακολουθεί ένα μοτίβο αιτήματος-απάντησης, το WebSocket επιτρέπει τόσο στον πελάτη όσο και στον διακομιστή να στέλνουν δεδομένα ο ένας στον άλλον ανεξάρτητα, χωρίς την ανάγκη επαναλαμβανόμενων αιτημάτων και απαντήσεων. Η επικοινωνία γίνεται μέσω αποστολής γεγονότων (events) στα οποία η λαμβάνουσα πλευρά μπορεί να αντιδράσει αντίστοιχα.

Ένα σημαντικό πλεονέκτημα του WebSocket είναι ότι επιτυγχάνει πολύ χαμηλές καθυστερήσεις (low-latency) στην επικοινωνία πελάτη-εξυπηρετητή. Σε αυτό το πλεονέκτημα βασίστηκε η επιλογή μας να χρησιμοποιήσουμε WebSocket για την αποστολή των κομματιών κειμένου από τον εξυπηρετητή στον πελάτη.



Σχήμα 9.6: Στιγμιότυπο από την εφαρμογή Postman, εφαρμογή για ανάπτυξη και έλεγχο λειτουργίας API, στο πάνω μέρος φαίνεται το αίτημα στο endpoint */posts/* που κάνει ο πελάτης και στο κάτω μέρος η απάντηση που δέχεται από τον εξυπηρετητή



Σχήμα 9.7: Στιγμιότυπο από την εφαρμογή Postman, εφαρμογή για ανάπτυξη και έλεγχο λειτουργίας API, στο πάνω μέρος φαίνεται το αίτημα στο endpoint */posts/:id* που κάνει ο πελάτης και στο κάτω μέρος η απάντηση που δέχεται από τον εξυπηρετητή

Στην εφαρμογή μας ο πελάτης έχει μόνο ένα διαθέσιμο γεγονός (πέρα από τα γεγονότα αρχικοποίησης και τερματισμού της σύνδεσης) που μπορεί να στείλει. Το γεγονός αυτό είναι το *buyParagraph* και ο χρήστης το στέλνει, μαζί με τον κωδικό ενός κειμένου στον διακομιστή, ενημερώνοντας τον ότι θέλει να αγοράσει το επόμενο κομμάτι του συγκεκριμένου κειμένου.

Ο εξυπηρετητής από την άλλη έχει έξι διαθέσιμα γεγονότα με τα οποία επικοινωνεί πληροφορίες στον πελάτη.

1. *unavailable* Σε περίπτωση που ο εξυπηρετητής δεν μπορεί να συνδεθεί με το Lightning και η υπηρεσία δημιουργίας αποδείξεων δεν είναι διαθέσιμη τότε ο εξυπηρετητής ενημερώνει τον πελάτη με το αντίστοιχο γεγονός.

2. *post-not-found* Στέλνεται στον πελάτη ως απάντηση όταν ο πελάτης στέλνει ένα γεγονός *buyParagraph* με κωδικό κειμένου που δεν υπάρχει.

3. *invoice* Μέσω αυτού το γεγονότος ο εξυπηρετητής στέλνει στον πελάτη την απόδειξη που πρέπει να πληρώσει για κάποιο αίτημα *buyParagraph*. Όταν ο πελάτης δέχεται ένα γεγονός 'invoice' ξεκινάει την διαδικασία πληρωμής μέσω του ψηφιακού του πορτοφολιού. Ο εξυπηρετητής παρακολουθεί την κατάσταση της απόδειξης και όταν δει ότι απόδειξη έχει πληρωθεί στέλνει, μέσω ενός νέου γεγονότος, το αντίστοιχο κομμάτι του κειμένου στον πελάτη.

4. *paragraph* Μέσο του γεγονότος αυτού ο εξυπηρετητής στέλνει στον πελάτη ένα κομμάτι κειμένου για το οποίο έχει επιβεβαιώσει την πληρωμή του.

5. *end-of-post* Το γεγονός αυτό ενημερώνει τον πελάτη ότι έχει αγοράσει όλα τα κομμάτια του συγκεκριμένου κειμένου.

6. *payment-timeout* Στον εξυπηρετητή υπάρχει ένα χρονικό όριο, μέσα στο οποίο πρέπει να έχει επιβεβαιωθεί η πληρωμή. Αν η πληρωμή δεν επιβεβαιωθεί εντός του χρονικού ορίου τότε θεωρείται αποτυχημένη και ο εξυπηρετητής ενημερώνει τον πελάτη. Παρ' όλ' αυτά η πληρωμή κατά πάσα πιθανότητα θα εκτελεστεί με ευτυχία σε μεταγενέστερο χρόνο και ο πελάτης θα χάσει χρήματα χωρίς να λάβει το κομμάτι για το οποίο πλήρωσε. Αυτό δεν είναι κάτι που μας απασχολεί ιδιαίτερα αφού πρόκειται για δοκιμαστική εφαρμογή και για χρήματα που χρησιμοποιούνται είναι ψεύτικα και δεν έχουν αξία. Σε κάποια μελλοντική έκδοση της εφαρμογής μπορεί να προστεθεί η λειτουργία επιστροφής των χρημάτων στον πελάτη σε τέτοιες περιπτώσεις.

Τεχνολογίες στον εξυπηρετητή

alby-tools Πρόκειται για μια βιβλιοθήκη που παρέχει χρήσιμα εργαλεία για τη ενσωμάτωση λειτουργιών του Lightning σε εφαρμογές ιστού. Μέσω του alby-tools ο εξυπηρετητής μπορεί να δημιουργήσει αποδείξεις και να επιβεβαιώσει την πληρωμή τους.

NodeJS Πρόκειται για ένα περιβάλλον εκτέλεσης JavaScript. Είναι ανοιχτού κώδικα και υποστηρίζει πολλές πλατφόρμες (cross-platform). Δημιουργήθηκε από τον Ryan Dahl και κυκλοφόρησε για πρώτη φορά το 2009. Την ανάπτυξης της NodeJS έχει πλέον αναλάβει το OpenJS Foundation. Σε αντίθεση με την παραδοσιακή JavaScript, η οποία χρησιμοποιείται κυρίως στους φυλλομετρητές ιστού για την ενίσχυση της διαδραστικότητας των ιστότοπων, η NodeJS επιτρέπει την εκτέλεση της JavaScript στην πλευρά του διακομιστή.

Η NodeJS χρησιμοποιείται συχνά σε διάφορους τύπους εφαρμογών, όπως διακομιστές, APIs, μικρόυπηρεσίες, εφαρμογές IoT και πολλά άλλα. Η ικανότητά της να χειρίζεται αποτελεσματικά ασύγχρονες λειτουργίες και το εκτεταμένο οικοσύστημα πακέτων που διαθέτει την καθιστούν μια δημοφιλή επιλογή για τη σύγχρονη ανάπτυξη εφαρμογών διακομιστή.

Τεχνολογίες στον πελάτη

WebLN Το WebLN είναι ένα πρωτόκολλο που γεφυρώνει το χάσμα μεταξύ των εφαρμογών ιστού και του δικτύου Lightning. Επιτρέπει την απρόσκοπτη ενσωμάτωση των λειτουργιών του δικτύου Lightning απευθείας σε εφαρμογές ιστού, επιτρέποντας στους χρήστες να κάνουν συναλλαγές Lightning χωρίς την ανάγκη πρόσθετων προγραμμάτων ή λογισμικού.

Η βιβλιοθήκη *webln* διευκολύνει την επικοινωνία μεταξύ των εφαρμογών και των κόμβων Lightning των χρηστών με ασφαλή τρόπο. Η βιβλιοθήκη παρέχει μια προγραμματιστική, εξουσιοδοτημένη διεπαφή μέσω της οποίας η εφαρμογή πελάτη μπορεί να ζητήσει από τον χρήστη να στείλει πληρωμές, να δημιουργήσει αποδείξεις για να λάβει πληρωμές και πολλά άλλα.

Μέσω της βιβλιοθήκης η εφαρμογή πελάτη ζητάει από τον χρήστη να συνδεθεί και να αυθεντικοποιήσει τον εαυτό του χρησιμοποιώντας το ψηφιακό πορτοφόλι του. Η εφαρμογή πελάτη έχει στην συνέχεια την δυνατότητα να λάβει πληροφορίες σχετικά με τον κόμβο Lightning του χρήστη και να στείλει αιτήματα στο πορτοφόλι του.

ReactJS Η κύρια βιβλιοθήκη που χρησιμοποιήσαμε στην ανάπτυξη της εφαρμογής πελάτη είναι η ReactJS.

Η ReactJS, που συχνά αναφέρεται και απλά ως React, είναι μια βιβλιοθήκη JavaScript ανοικτού κώδικα για την ανάπτυξη διεπαφών χρήστη (UIs) για εφαρμογές ιστού. Αναπτύχθηκε και συντηρείται από την Meta (πρώην Facebook) και έχει αποκτήσει ευρεία δημοτικότητα στην κοινότητα ανάπτυξης εφαρμογών ιστού λόγω της αποδοτικότητας, της σπονδυλωτής δομής και της αρχιτεκτονικής της που βασίζεται σε στοιχεία (component based architecture).

Κάποια κύρια χαρακτηριστικά της React είναι τα εξής:

1. **Αρχιτεκτονική βασισμένη σε στοιχεία** Στην React ο προγραμματιστής μπορεί να αναλύει τις διεπαφές χρήστη σε επαναχρησιμοποιήσιμα στοιχεία. Τα στοιχεία είναι αυτοτελείς μονάδες κώδικα που ενσωματώνουν τη δική τους λογική, δομή και στυλ. Αυτή η αρθρωτή προσέγγιση προωθεί την επαναχρησιμοποίηση του κώδικα, διευκολύνει την συντήρηση του κώδικα και τον διαχωρισμό των προβλημάτων.

2. **Εικονικός DOM** Μία από τις βασικές καινοτομίες της React είναι η χρήση ενός εικονικού DOM. Αντί να ενημερώνει απευθείας το πραγματικό DOM του προγράμματος περιήγησης, η React δημιουργεί μια ελαφριά εικονική αναπαράσταση του DOM στη μνήμη. Όταν υπάρχουν αλλαγές στα δεδομένα ή την κατάσταση ενός στοιχείου, η React υπολογίζει τον πιο αποτελεσματικό τρόπο ενημέρωσης του εικονικού DOM και στη συνέχεια συγχρονίζει το πραγματικό DOM με αυτές τις αλλαγές. Αυτή η προσέγγιση μειώνει τις περιττές αναδρομές και βελτιώνει τις σημαντικά τις επιδόσεις.

3. **Ροή δεδομένων μονής κατεύθυνσης** Αυτό σημαίνει ότι τα δεδομένα ρέουν προς μία μόνο κατεύθυνση από τα γονικά στοιχεία στα στοιχεία-παιδιά. Αυτό διευκολύνει την παρακολούθηση και τη διαχείριση της κατάστασης μιας ιεραρχίας συστατικών, καθώς οι αλλαγές σε ένα μέρος της εφαρμογής δεν μπορούν να οδηγήσουν σε απρόβλεπτες παρενέργειες σε άλλα μέρη.

4. **JSX** Το JSX είναι μια επέκταση της σύνταξης της JavaScript που επιτρέπει στους προγραμματιστές να γράφουν κώδικα που μοιάζει με HTML μέσα στη JavaScript. Αυτό επιτρέπει τη δημιουργία στοιχείων UI με πιο διαισθητικό τρόπο, συνδυάζοντας άψογα την HTML και τη JavaScript [41].

5. **Μέθοδοι κύκλου ζωής στοιχείων** Τα συστατικά στην React διαθέτουν μεθόδους κύκλου ζωής που επιτρέπουν στους προγραμματιστές να εκτελέσουν λειτουργίες σε συγκεκριμένες στιγμές κατά τη διάρκεια του κύκλου ζωής ενός συστατικού, όπως όταν αυτό δημιουργείται, ενημερώνεται ή καταστρέφεται. Αυτές οι μέθοδοι επιτρέπουν στους προγραμματιστές να εκτελούν ενέργειες όπως η άντληση δεδομένων (π.χ. κλήση API), οι ενημερώσεις κατάστασης και ο καθαρισμός (απελευθέρωση πόρων).

6. **Κατάσταση και ιδιότητες** Τα στοιχεία στην React μπορούν επίσης να διατηρούν τη δική τους τοπική κατάσταση, η οποία αντιπροσωπεύει τα δυναμικά δεδομένα που τυχόν αλλάζουν με την πάροδο του χρόνου. Επιπλέον, τα στοιχεία λαμβάνουν δεδομένα από τα γονικά τους στοιχεία μέσω των props (συντομογραφία των ιδιοτήτων (properties)). Τα props είναι αμετάβλητα, διασφαλίζοντας ότι τα στοιχεία-παιδιά δεν τροποποιούν άμεσα τα δεδομένα του γονέα τους.

7. **Διαχείριση του κατάστασης** Παρόλο που η ενσωματωμένες λειτουργίες διαχείρισης κατάστασης της React είναι κατάλληλες για μικρές και μεσαίου μεγέθους εφαρμογές, μεγαλύτερες εφαρμογές συνήθως θα επωφεληθούν από την ενσωμάτωση εξωτερικών βιβλιοθηκών διαχείρισης κατάστασης, όπως είναι το Redux ή το Zustand. Αυτές οι βιβλιοθήκες βοηθούν στην αποτελεσματικότερη διαχείριση πολύπλοκων καταστάσεων και ροής δεδομένων της εφαρμογής.

Η React δεν είναι ένα ολοκληρωμένο framework όπως η Angular, εστιάζει ειδικά στο επίπεδο UI. Για την δημιουργία μιας ολοκληρωμένης εφαρμογής ιστού, οι προγραμματιστές συχνά συνδυάζουν την React με άλλες βιβλιοθήκες και εργαλεία για λειτουργίες όπως η δρομολόγηση, τα αιτήματα HTTP και η διαχείριση κατάστασης. Δημοφιλείς επιλογές για αυτές τις συμπληρωματικές βιβλιοθήκες είναι οι React Router, Axios και Redux.

Εν κατακλείδι, η React είναι μια πολύ ισχυρή βιβλιοθήκη που έφερε την επανάσταση στον τρόπο ανάπτυξης εφαρμογών ιστού, εισάγοντας μια αρχιτεκτονική βασισμένη σε στοιχεία και τον εικονικό DOM. Έχει γίνει ο ακρογωνιαίος λίθος της σύγχρονης ανάπτυξης ιστοσελίδων, επιτρέποντας στους προγραμματιστές να δημιουργούν διαδραστικές και αποδοτικές διεπαφές χρήστη με ευκολία.

Η React αποτελεί επίσης έμπνευση για ανερχόμενες βιβλιοθήκες όπως η Vue, οι οποίες συνδυάζουν τις βέλτιστες πρακτικές της Reacts και προσθέτουν επιπλέον λειτουργικότητα και ευκολία χρήσης.

Chakra UI Το Chakra UI είναι μια απλή, αρθρωτή βιβλιοθήκη στοιχείων UI, η οποία δίνει έμφαση στην προσβασιμότητα και παρέχει στον προγραμματιστή τα δομικά στοιχεία που χρειάζεται για να δημιουργήσει εφαρμογές σε React.

Το Chakra UI παρέχει στον προγραμματιστή έτοιμα στοιχεία όπως κουμπιά, φόρμες, πίνακες και πολλά άλλα.

Στόχος του Chakra UI είναι να ενισχύσει την παραγωγικότητα των προγραμματιστών, διατηρώντας παράλληλα την έμφαση στην αισθητική, την προσαρμοστικότητα (responsiveness) και την εμπειρία του χρήστη.

Κεφάλαιο 10ο: Συμπεράσματα και προτάσεις βελτίωσης

Σε αυτήν την περιεκτική ανάλυση της τεχνολογίας αλυσίδων μπλοκ και των σημαντικότερων δικτύων της, συμπεριλαμβανομένων των Bitcoin, Ethereum, Chainlink, Polygon, Lightning Network και Nano, έχουμε διασχίσει ένα τοπίο καινοτομίας που αναδιαμορφώνει τον κόσμο μας με διάφορους τρόπους.

Αυτή η τεχνολογία έχει εγκαινιάσει μια νέα εποχή καινοτομίας, αλλάζοντας τον ίδιο τον παγκόσμιο ιστό. Στον πυρήνα του, το blockchain είναι κάτι περισσότερο από ένα απλό καθολικό. είναι μια επαναστατική έννοια που ξεπερνά τα παραδοσιακά όρια. Λειτουργεί ως ένα αποκεντρωμένο και αμετάβλητο καθολικό, φέρνοντας επανάσταση στον τρόπο με τον οποίο καταγράφουμε και μοιραζόμαστε δεδομένα. Παρέχοντας μια ασφαλή και ανθεκτική σε παραβιάσεις πλατφόρμα για συναλλαγές και διαχείριση δεδομένων, έχει επαναπροσδιορίσει τις δυνατότητες εμπιστοσύνης και ασφάλειας στην ψηφιακή εποχή.

Η ικανότητα της τεχνολογίας να αποκεντρώνει τον έλεγχο και να εξαλείφει την ανάγκη για μεσάζοντες έχει βαθιές επιπτώσεις για τις βιομηχανίες που μαστίζονται από αναποτελεσματικότητα και ευπάθειες. Πηγαίνει πέρα από την απλή καταγραφή συναλλαγών. δίνει τη δυνατότητα σε άτομα και οργανισμούς να ανακτήσουν τον έλεγχο των ψηφιακών τους αλληλεπιδράσεων.

Επιπλέον, η έννοια της ασφάλειας εκτείνεται πέρα από την προστασία δεδομένων. Ενσταλάζει μια αίσθηση ασφάλειας στις συναλλαγές, ενισχύοντας την εμπιστοσύνη στον ψηφιακό τομέα. Η αμεταβλητότητα των δεδομένων και η κρυπτογράφηση διασφαλίζουν ότι μόλις καταγραφούν τα δεδομένα, παραμένουν ασφαλή και αδιάψευστα. Αυτό το νέο επίπεδο ασφάλειας έχει τη δυνατότητα να εξαλείψει την απάτη, να μειώσει τις απειλές στον κυβερνοχώρο και να προστατεύσει ευαίσθητες πληροφορίες σε όλους τους κλάδους.

10.1 Προκλήσεις και κίνδυνοι

Ενώ οι αλυσίδες έχουν τεράστιες δυνατότητες, έχουν επίσης μερίδιο προκλήσεων, κινδύνων και σκεπτικισμού. Καθώς εξετάζουμε αυτό το πολύπλευρο τοπίο, γίνεται προφανές ότι το blockchain, όπως κάθε ανατρεπτική καινοτομία, δεν είναι απρόσβλητο από κριτική και πιθανές παγίδες.

Οι ρυθμιστικές προκλήσεις προσθέτουν άλλο ένα επίπεδο πολυπλοκότητας. Η αποκεντρωμένη φύση των αλυσίδων, αν και αποτελεί αναπόσπαστο στοιχείο της ελκυστικότητας του, μπορεί να είναι ένα δίκοπο μαχαίρι. Μπορεί να διευκολύνει παράνομες δραστηριότητες όπως το ξέπλυμα χρήματος και τη φοροδιαφυγή, θέτοντας ένα δίλημμα για τις ρυθμιστικές αρχές και τις κυβερνήσεις παγκοσμίως. Η δημιουργία κατάλληλων ρυθμιστικών πλαισίων είναι μια συνεχής διαδικασία.

Υπάρχουν επίσης τρωτά σημεία ασφαλείας. Παρά τη φήμη του για την ασφάλεια, το blockchain δεν είναι εντελώς αδιαπέραστο από απειλές. Τα ελαττώματα των έξυπνων συμβολαίων, δημιουργημένα από ανθρώπινο παράγοντα, για παράδειγμα, έχουν οδηγήσει σε σημαντικές οικονομικές απώλειες. Η περίπλοκη φύση ορισμένων υλοποιήσεων blockchain μπορεί να τις εκθέσει σε νέους φορείς επίθεσης.

Η τυποποίηση είναι ένα άλλο ζήτημα που μαστίζει τον χώρο. Η απουσία καθολικών προτύπων

περιπλέκει τη διαλειτουργικότητα μεταξύ διαφόρων δικτύων και πλατφορμών, εμποδίζοντας την ανάπτυξη εφαρμογών που μπορούν να αλληλεπιδρούν απρόσκοπτα με πολλαπλές αλυσίδες μπλοκ.

Παράλληλα, οι ανησυχίες για το απόρρητο παραμένουν. Ενώ οι συναλλαγές blockchain είναι ψευδώνυμες, η διαφάνεια αυτών των δικτύων σημαίνει ότι μόλις καταγραφούν πληροφορίες, δεν μπορούν να διαγραφούν. Αυτή η μακροπρόθεσμη αμετάβλητη μπορεί να εγείρει ανησυχίες σχετικά με την έκθεση ευαίσθητων δεδομένων.

Πέρα από αυτά τα τεχνικά ζητήματα, η διαφημιστική εκστρατεία και η κερδοσκοπία έχουν κυριαρχήσει στο χώρο των κρυπτονομισμάτων. Αυτό οδήγησε σε ακραία αστάθεια των τιμών και στην εμφάνιση έργων με αμφισβητήσιμες βάσεις. Τέτοιες εξελίξεις μπορεί να αποθαρρύνουν την επικρατούσα υιοθέτηση και να θέσουν αμφιβολίες για τη μακροπρόθεσμη βιωσιμότητα της τεχνολογίας blockchain.

Τέλος, η ίδια η υιοθεσία παρουσιάζει προκλήσεις. Η ενσωμάτωση της τεχνολογίας blockchain συχνά απαιτεί μια ουσιαστική αλλαγή στη νοοτροπία, την υποδομή και τις επιχειρηματικές διαδικασίες. Η αντίσταση στην αλλαγή, σε συνδυασμό με την αδράνεια των υφιστάμενων συστημάτων, δημιουργεί σημαντικά εμπόδια εισόδου.

10.2 Επόμενα βήματα και επεκτάσεις της εφαρμογής

Έχοντας δημιουργήσει μια απόδειξη της ιδέας (proof of concept), τα επόμενα βήματα στην εξέλιξη της ειδησιογραφικής πλατφόρμας στηρίζονται στη βελτίωση της εμπειρίας χρήστη, την επέκταση της λειτουργικότητας και την υπέρβαση των ορίων του δυνατού στο οικοσύστημα του Lightning Network.

Βελτιώσεις με επίκεντρο τον χρήστη Για να κάνουμε την εμπειρία ανάγνωσης ειδήσεων ακόμα πιο απρόσκοπτη, μπορούμε να επικεντρωθούμε σε βελτιώσεις με επίκεντρο τον χρήστη. Επεκτάσεις επηρεασμένες από υπάρχουσες πλατφόρμες όπως εξατομικευμένες συνδρομές ειδήσεων, σελιδοδείκτες και ειδοποιήσεις για νέα άρθρα μπορούν να ενισχύσουν την αφοσίωση και την ικανοποίηση των χρηστών.

Μικροπληρωμές και πληρωμή ανά μονάδα Αξιοποιώντας τις δυνατότητες μικροσυναλλαγών του Lightning, μπορούμε να εισαγάγουμε ένα μοντέλο πληρωμής ανά μονάδα επιλογής, όπως παράγραφο, άρθρο ή γραμμή.

Ενσωμάτωση έξυπνων συμβολαίων Με την πλατφόρμα RGB του Lightning Network για έξυπνα συμβόλαια, μπορούμε να εξερευνήσουμε καινοτόμους τρόπους για να δημιουργήσουμε συμφωνίες εμπιστοσύνης μεταξύ δημιουργών περιεχομένου και καταναλωτών. Τα έξυπνα συμβόλαια μπορούν να αυτοματοποιήσουν τη διανομή εσόδων, διασφαλίζοντας ότι οι δημιουργοί αμείβονται δίκαια για το έργο τους βάσει προκαθορισμένων συνθηκών, όπως πλήθος προβολών ή αξιολογήσεις χρηστών. Παράλληλα, μπορούμε να αναπτύξουμε ένα σύστημα αδειοδότησης περιεχομένου

που επιτρέπει στους δημιουργούς περιεχομένου να ορίζουν όρους και προϋποθέσεις για τη χρήση των άρθρων τους. Οι χρήστες μπορούν στη συνέχεια να πληρώσουν για συγκεκριμένα δικαιώματα χρήσης με αποκεντρωμένο και αυτοματοποιημένο τρόπο, απλοποιώντας τη δημιουργία εσόδων από περιεχόμενο και για τα δύο μέρη.

10.3 Εν κατακλείδι

Παρά τις προκλήσεις και τις αβεβαιότητες που αντιμετωπίζει η τεχνολογία, είναι σημαντικό να αναγνωρίσουμε ότι βρισκόμαστε ακόμη στα πρώτα στάδια της εξέλιξής της. Η δυναμική του εκτείνεται πολύ πέρα από τους τρέχοντες περιορισμούς και παγίδες του. Ακριβώς όπως το Διαδίκτυο αντιμετώπισε σκεπτικισμό και εμπόδια στις νεοφυείς μέρες του, έτσι και αυτή η τεχνολογία είναι έτοιμη να υποστεί μεταμορφωτικές αλλαγές και βελτιώσεις τα επόμενα χρόνια. Η ικανότητά των αλυσίδων να ενθαρρύνει την εμπιστοσύνη, τη διαφάνεια και την αποκέντρωση έχει ήδη αρχίσει να φέρνει επανάσταση στις βιομηχανίες και καθώς η τεχνολογία ωριμάζει, υπόσχεται να αντιμετωπίσει τις δικές της ελλείψεις. Με την καινοτομία, τη συνεργασία και την υπεύθυνη ανάπτυξη, το οικοσύστημα αυτό μπορεί να ξεπεράσει αυτά τα εμπόδια και να αναδειχθεί ως θεμελιώδης πυλώνας του ψηφιακού μας μέλλοντος. Το ταξίδι που ακολουθεί είναι προκλητικό, αλλά οι πιθανές ανταμοιβές ενός πιο περιεκτικού, ασφαλούς και αποτελεσματικού ψηφιακού κόσμου καθιστούν τη συνεχή εξερεύνηση της τεχνολογίας αναμφισβήτητα χρήσιμη.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Chargebacks911, "The 2023 chargeback field report." Available: `https://chargebacks911.com/chargeback-field-report/`, Jun 2023. [Online; accessed 20-07-2023].

[2] Consensys, "Swap crypto and exchange digital tokens." Available: `https://metamask.io/swaps`. [Online; accessed 20-07-2023].

[3] A. Gangwal, H. Gangavalli, and A. Thirupathi, "A survey of layer-two blockchain protocols," *Science Direct*, p. 22, 04 2022.

[4] A. Takyar, "What is stellar blockchain? a complete guide for beginners." Available: `https://www.leewayhertz.com/what-is-stellar-blockchain`, Mar 2023. [Online; accessed 20-07-2023].

[5] A. Antonopoulos, O. Osuntokun, and R. Pickhardt, *Mastering the Lightning Network*, pp. 39–65, 168, 185–207. O'Reilly Media, 12 2021.

[6] Y. Zou, T. Meng, P. Zhang, W. Zhang, and H. Li, "Focus on blockchain: A comprehensive survey on academic and application," *IEEE Access*, vol. 8, pp. 187182–187201, 01 2020.

[7] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*, 06 2017.

[8] B. Sriman, S. Kumar, and S. Prabakaran, *Blockchain Technology: Consensus Protocol Proof of Work and Proof of Stake*, pp. 395–406. Research Gate, 09 2020.

[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Cryptography Mailing list at https://metzdowd.com*, 03 2009.

[10] L. Conway, "What is bitcoin halving? definition, how it works, why it matters." Available: `http://aiweb.techfak.uni-bielefeld.de/content/bworld-robot-control-software/`, May 2023. [Online; accessed 20-07-2023].

[11] J. Frankenfield, "Mining pool: Definition, how it works, methods, and benefits." Available: `https://www.investopedia.com/terms/m/mining-pool.asp`, Oct 2022. [Online; accessed 20-07-2023].

[12] C. Nguyen, H. Dinh Thai, D. Nguyen, D. Niyato, H. Nguyen, and E. Dutkiewicz, "Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities," *IEEE Access*, vol. PP, pp. 1–1, 06 2019.

[13] Consensys, "What is proof of stake?." Available: `https://consensys.net/blog/blockchain-explained/what-is-proof-of-stake`, May 2020. [Online; accessed 20-07-2023].

[14] LexisNexis, "The true cost of fraudtm study." Available: `https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study`, 2022. [Online; accessed 20-07-2023].

[15] S. Chevalier, "Global covid-19 impact on fraud to e-merchants." Available: `https://www.statista.com/statistics/1295142/impact-covid19-pandemic-fraud-worldwide`, Apr 2023. [Online; accessed 20-07-2023].

[16] D. Khan, T. Low, and M. Hashmani, "Systematic literature review of challenges in blockchain scalability," *Applied Sciences*, vol. 11, p. 9372, 10 2021.

[17] V. Buterin, "Ethereum whitepaper." Available: `https://ethereum.org/en/whitepaper`. [Online; accessed 20-07-2023].

[18] F. Victor and B. Lüders, *Measuring Ethereum-Based ERC20 Token Networks*, pp. 113–129. Research Gate, 09 2019.

[19] K. Karvez, "Oracles." Available: `https://ethereum.org/en/developers/docs/oracles`, June 2023. [Online; accessed 20-07-2023].

[20] Chainlink, "Data feeds." Available: `https://docs.chain.link/data-feeds`. [Online; accessed 20-07-2023].

[21] IBM, "Ibm blockchain supply chain." Available: `https://www.ibm.com/blockchain-supply-chain`. [Online; accessed 20-07-2023].

[22] S. Hussain, "Deco research series 1: Introduction." Available: `https://blog.chain.link/deco-introduction`, Apr 2023. [Online; accessed 20-07-2023].

[23] P. Foundation, "Supernets." Available: https://wiki.polygon.technology/docs/supernets/operate/supernets-performance. [Online; accessed 20-07-2023].

[24] H. Academy, "Layer 0." Available: https://www.horizen.io/academy/layer-0. [Online; accessed 20-07-2023].

[25] N. Foundation, "Nano living paper."

[26] D. Mazière, "The stellar consensus protocol: A federated model for internet-level consensus," *The Stellar Consensus Protocol A federated model for Internet-level consensus*, Dec 2017.

[27] J. Poon and T. Dryja, "Lightning whitepaper." Available: https://lightning.network/lightning-network-paper.pdf, 1 2016. [Online; accessed 20-07-2023].

[28] "A beginners guide to the lightning network." Available: https://bitcoiner.guide/lightning. [Online; accessed 20-07-2023].

[29] B. Guide, "Lightning docs." Available: https://docs.lightning.engineering/the-lightning-network. [Online; accessed 20-07-2023].

[30] "Bolt #4: Onion routing protocol." Available: https://github.com/lightning/bolts/blob/master/04-onion-routing.md. [Online; accessed 20-07-2023].

[31] D. Goldschlag, M. Reed, and P. Syverson, "Onion routing for anonymous and private internet connections," *COMMUNICATIONS OF THE ACM*, vol. 42, 02 1999.

[32] Lorenzo, "Multipart payments – amp/mmp." Available: https://voltage.cloud/blog/lightning-network-faq/multipart-payments-on-lightning-network-break-down-amp-and-mmp, 2023. [Online; accessed 20-07-2023].

[33] R. Pickhardt and S. Richter, "Optimally reliable & cheap payment flows on the lightning network," 2021.

[34] D. Perell, "Models of internet monetization," *ELON JOURNAL OF UNDERGRADUATE RESEARCH IN COMMUNICATIONS*, vol. 7, 2016.

[35] O. Foulds, L. Azzopardi, and M. Halvey, "Investigating the influence of ads on user search performance, behaviour, and experience during information seeking," in *Proceedings of the 2021 Conference on Human Information Interaction and Retrieval*, CHIIR '21, (New York, NY, USA), p. 107–117, Association for Computing Machinery, 2021.

[36] J. Hayes and G. Graybeal, "Synergizing traditional media and the social web for monetization: A modified media micropayment model," *Journal of Media Business Studies*, vol. 8, no. 2, pp. 19–44, 2011.

[37] M. E. Rana and O. S. Saleh, "Chapter 15 - high assurance software architecture and design," in *System Assurances* (P. Johri, A. Anand, J. Vain, J. Singh, and M. Quasim, eds.), Emerging Methodologies and Applications in Modelling, pp. 271–285, Academic Press, 2022.

[38] Jamaljsr, "Regtest lightning networks, made easy." Available: https://lightningpolar.com. [Online; accessed 20-07-2023].

[39] IBM, "What is a rest api?." Available: https://www.ibm.com/topics/rest-apis. [Online; accessed 20-07-2023].

[40] MozDevNet, "The websocket api (websockets) - web apis: Mdn." Available: https://developer.mozilla.org/en-US/docs/Web/API/WebSockets_API. [Online; accessed 20-07-2023].

[41] Meta, "Writing markup with jsx." Available: https://react.dev/learn/writing-markup-with-jsx. [Online; accessed 20-07-2023].

ΠΑΡΑΡΤΗΜΑ Α Κώδικας Oracle στο δίκτυο του Ethereum

```
    pragma solidity >=0.4.21 <0.6.0;

contract Oracle {
  Request[] requests; //list of requests made to the contract
  uint currentId = 0; //increasing request id
  //minimum number of responses to receive before declaring final result
  uint minQuorum = 2;
  uint totalOracleCount = 3; // Hardcoded oracle count

  // defines a general api request
  struct Request {
    uint id;                          //request id
    string urlToQuery;                //API url
    string attributeToFetch;          //json attribute (key) to retrieve in the response
    string agreedValue;               //value from key
    mapping(uint => string) answers; //answers provided by the oracles
    // oracles which will query the answer
    // (1=oracle hasn't voted, 2=oracle has voted)
    mapping(address => uint) quorum;
  }

  //event that triggers oracle outside of the blockchain
  event NewRequest (
    uint id,
    string urlToQuery,
    string attributeToFetch
  );

  //triggered when there's a consensus on the final result
  event UpdatedRequest (
    uint id,
    string urlToQuery,
    string attributeToFetch,
    string agreedValue
  );

  function createRequest (
    string memory _urlToQuery,
    string memory _attributeToFetch
  )
  public
```

```
  {
    uint length = requests.push(Request(currentId, _urlToQuery, _attributeToFetch, ""));
    Request storage r = requests[length-1];

    // Hardcoded oracles address
    r.quorum[address(0x6c2339b46F41a06f09CA0051ddAD54D1e582bA77)] = 1;
    r.quorum[address(0xb5346CF224c02186606e5f89EACC21eC25398077)] = 1;
    r.quorum[address(0xa2997F1CA363D11a0a35bB1Ac0Ff7849bc13e914)] = 1;

    // launch an event to be detected by oracle outside of blockchain
    emit NewRequest (
      currentId,
      _urlToQuery,
      _attributeToFetch
    );

    // increase request id
    currentId++;
  }

  //called by the oracle to record its answer
  function updateRequest (
    uint _id,
    string memory _valueRetrieved
  ) public {

    Request storage currRequest = requests[_id];

    //check if oracle is in the list of trusted oracles
    //and if the oracle hasn't voted yet
    if(currRequest.quorum[address(msg.sender)] == 1){

      //marking that this address has voted
      currRequest.quorum[msg.sender] = 2;

      // iterate through "array" of answers until a
      // position if free and save the retrieved value
      uint tmpI = 0;
      bool found = false;
      while(!found) {
        //find first empty slot
        if(bytes(currRequest.answers[tmpI]).length == 0){
          found = true;
```

```
            currRequest.answers[tmpI] = _valueRetrieved;
          }
          tmpI++;
        }

        uint currentQuorum = 0;

        //iterate through oracle list and check if enough oracles(minimum quorum)
        //have voted the same answer has the current one
        for(uint i = 0; i < totalOracleCount; i++){
          bytes memory a = bytes(currRequest.answers[i]);
          bytes memory b = bytes(_valueRetrieved);

          if(keccak256(a) == keccak256(b)){
            currentQuorum++;
            if(currentQuorum >= minQuorum){
              currRequest.agreedValue = _valueRetrieved;
              emit UpdatedRequest (
                currRequest.id,
                currRequest.urlToQuery,
                currRequest.attributeToFetch,
                currRequest.agreedValue
              );
            }
          }
        }
      }
    }
}
```