Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων
Τομεας Τεχνολογιας Πληροφορικης και Υπολογιστων

Δημιουργία συστήματος πώλησης δεδομένων χρηστών μέσω του δικτύου Cardano

Διπλωματικη Εργασια

του

ΜΑΡΚΟΥ ΓΚΕΡΓΚΕΣ

Επιβλέπων: Νεκτάριος Κοζύρης
Καθηγητής Ε.Μ.Π.

Αθήνα, Νοέμβριος 2023

Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων
Τομεας Τεχνολογιας Πληροφορικης και Υπολογιστων

Δημιουργία συστήματος πώλησης δεδομένων χρηστών μέσω του δικτύου Cardano

Διπλωματικη Εργασια

του

ΜΑΡΚΟΥ ΓΚΕΡΓΚΕΣ

Επιβλέπων: Νεκτάριος Κοζύρης
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 21η Νοεμβρίου 2023.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Νεκτάριος Κοζύρης	Άγγελος Κιαγιάς	Αριστείδης Παγουρτζής
Καθηγητής Ε.Μ.Π.	Καθηγητής Πανεπιστήμιο του Εδιμβούργου	Καθηγητής Ε.Μ.Π.

Αθήνα, Νοέμβριος 2023

Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων
Τομεας Τεχνολογιας Πληροφορικης και Υπολογιστων

ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ενυπογράφως ότι είμαι αποκλειστικός συγγραφέας της παρούσας Πτυχιακής Εργασίας, για την ολοκλήρωση της οποίας κάθε βοήθεια είναι πλήρως αναγνωρισμένη και αναφέρεται λεπτομερώς στην εργασία αυτή. Έχω αναφέρει πλήρως και με σαφείς αναφορές, όλες τις πηγές χρήσης δεδομένων, απόψεων, θέσεων και προτάσεων, ιδεών και λεκτικών αναφορών, είτε κατά κυριολεξία είτε βάσει επιστημονικής παράφρασης. Αναλαμβάνω την προσωπική και ατομική ευθύνη ότι σε περίπτωση αποτυχίας στην υλοποίηση των ανωτέρω δηλωθέντων στοιχείων, είμαι υπόλογος έναντι λογοκλοπής, γεγονός που σημαίνει αποτυχία στην Πτυχιακή μου Εργασία και κατά συνέπεια αποτυχία απόκτησης του Τίτλου Σπουδών, πέραν των λοιπών συνεπειών του νόμου περί πνευματικών δικαιωμάτων. Δηλώνω, συνεπώς, ότι αυτή η Πτυχιακή Εργασία προετοιμάστηκε και ολοκληρώθηκε από εμένα προσωπικά και αποκλειστικά και ότι, αναλαμβάνω πλήρως όλες τις συνέπειες του νόμου στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής άλλης πνευματικής ιδιοκτησίας.

(Υπογραφή)

.....
Μάρκος Γκέργκες

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

21 Νοεμβρίου 2023

Περίληψη

Σε μια εποχή όπου τα δεδομένα περιγράφονται συχνά ως ο νέος «χρυσός», ο έλεγχος και η νομισματοποίηση των προσωπικών δεδομένων βρίσκονται σε μεγάλο βαθμό στα χέρια κεντρικών οντοτήτων. Η παρούσα διπλωματική παρουσιάζει μια αποκεντρωμένη αγορά δεδομένων που βασίζεται στην αλυσίδα μπλοκ Cardano, αξιοποιώντας τα έξυπνα συμβόλαια για την αυτοματοποίηση της διαδικασίας ανταλλαγής δεδομένων μεταξύ αγοραστών και πωλητών. Χρησιμοποιώντας τη Haskell και το Plutus για την ανάπτυξη έξυπνων συμβολαίων και μια επέκταση του προγράμματος περιήγησης για τη συλλογή δεδομένων, το σύστημα στοχεύει στην επιστροφή του ελέγχου των προσωπικών δεδομένων στο άτομο.

Χρησιμοποιώντας το μοντέλο Extended UTXO (EUTxO) του Cardano και τα έξυπνα συμβόλαια, η αγορά επιτρέπει στους χρήστες να συμβολαιοποιήσουν τα δεδομένα τους, μετατρέποντάς τα έτσι σε εμπορεύσιμα περιουσιακά στοιχεία. Το σύστημα ενσωματώνει μια επέκταση προγράμματος περιήγησης για τη συλλογή δεδομένων, IPFS για αποκεντρωμένη αποθήκευση δεδομένων και κρυπτογραφικές τεχνικές για ασφαλή μετάδοση δεδομένων και επαλήθευση ταυτότητας. Για την επίδειξη των μηχανισμών πώλησης και αγοράς δεδομένων χρησιμοποιούνται δύο πρωταρχικές ροές, ¨Ask(Ζήτηση)¨ και ¨Bid(Προσφορά)¨.

Η παρούσα διπλωματική εργασία έχει ως στόχο να υποδείξει τις δυνατότητες της τεχνολογίας blockchain και των έξυπνων συμβολαίων στην αυτοματοποίηση πολύπλοκων διαδικασιών, προσφέροντας έτσι μια ευέλικτη λύση στο καθολικό πρόβλημα της ιδιοκτησίας και της νομισματοποίησης των δεδομένων. Η παρούσα εργασία χρησιμεύει ως εφαλτήριο για περαιτέρω έρευνα στην αξιοποίηση της τεχνολογίας blockchain για πρακτικές, ασφαλείς και διαφανείς λύσεις διαχείρισης δεδομένων.

Λέξεις Κλειδιά

Blockchain, Έξυπνα Συμβόλαια, Cardano

Abstract

In an era where data is often described as the new oil, the control and monetization of personal data have largely been in the hands of centralized entities. This thesis presents a decentralized data marketplace built on the Cardano blockchain, leveraging smart contracts to automate the process of data exchange between buyers and sellers. Utilizing Haskell and Plutus for smart contract development, and a browser extension for data collection, the system aims to return control of personal data to the individual.

Utilizing Cardano's Extended UTXO (EUTxO) model and smart contracts, the marketplace enables users to tokenize their data, thereby converting it into tradable assets. The system incorporates a browser extension for data collection, IPFS for decentralized data storage, and cryptographic techniques for secure data transmission and identity verification. Two primary workflows, "Ask" and "Bid", are elaborated to demonstrate the data sale and purchase mechanisms.

This diploma thesis aims to indicate the potential of blockchain technology and smart contracts in automating complex processes, thereby offering a versatile solution to the universal problem of data ownership and monetization. This work serves as a stepping stone for further research in leveraging blockchain technology for practical, secure, and transparent data management solutions.

Keywords

Blockchain, Smart Contracts, Cardano, Decentrilized Data Marketplace, Data Ownership, Haskell, Plutus, IPFS

στους γονείς μου

Ευχαριστίες

Θα ήθελα να ευχαριστήσω πρώτα απ' όλα τον καθηγητή κ. Κοζύρη για την επίβλεψη αυτής της διπλωματικής και για την ευκαιρία που μου έδωσε να την εκπονήσω στο Εργαστήριο Υπολογιστικών Συστημάτων. Επίσης ευχαριστώ ιδιαίτερα την Δρ. Δόκα και τον κ. Κατσιγιάννη για την καθοδήγηση και την άριστη συνεργασία που είχαμε. Είμαι επίσης ευγνώμων για τη χρηματοδότηση που μου παρείχε το IOG, η οποία υποστήριξε τις ερευνητικές μου προσπάθειες. Τέλος, θα ήθελα να ευχαριστήσω τους γονείς μου για την καθοδήγηση και την ηθική υποστήριξη που μου έχουν προσφέρει όλα αυτά τα χρόνια.

Αθήνα, Νοέμβριος 2023

Μάρκος Γκέργκες

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Πρόλογος

Στην ψηφιακή εποχή, τα δεδομένα έχουν γίνει ένα από τα πιο πολύτιμα αγαθά. Ωστόσο, τα άτομα που παράγουν αυτά τα δεδομένα έχουν συχνά ελάχιστο έλεγχο του τρόπου με τον οποίο χρησιμοποιούνται, αξιοποιούνται ή ακόμη και διασφαλίζονται. Αυτή η ανισορροπία δύναμης μεταξύ των παραγωγών δεδομένων και των υπευθύνων επεξεργασίας δεδομένων έχει οδηγήσει σε αμέτρητες ανησυχίες ηθικής και προστασίας της ιδιωτικής ζωής που είναι ολοένα και πιο δύσκολο να αγνοηθούν. Ταυτόχρονα, η άνοδος της τεχνολογίας blockchain έχει δείξει ότι υπόσχεται την απομάκρυνση των κεντρικών αρχών και την ενδυνάμωση των ατόμων, προσφέροντας μια πιθανή λύση σε αυτό το πιεστικό ζήτημα.

Το ενδιαφέρον μου στον κόσμο της τεχνολογίας blockchain παρακινήθηκε περαιτέρω από τη γοητεία που μου ασκούσαν οι δυνατότητες των έξυπνων συμβολαίων για την αυτοματοποίηση και την ασφάλεια πολύπλοκων διαδικασιών. Ενώ το απόρρητο των δεδομένων είναι μια σημαντική πτυχή, ο πρωταρχικός στόχος αυτής της διπλωματικής είναι να παρουσιάσει πώς τα έξυπνα συμβόλαια μπορούν να εφαρμοστούν πρακτικά για την επίλυση καθολικών προβλημάτων -στην προκειμένη περίπτωση, το ζήτημα της ιδιοκτησίας και της νομισματοποίησης των δεδομένων.

Καθώς θα διαβάζετε τις σελίδες που ακολουθούν, θα βρείτε μια ολοκληρωμένη διερεύνηση μιας αποκεντρωμένης αγοράς δεδομένων που βασίζεται στην αλυσίδα μπλοκ(blockchain) Cardano. Αυτή η αγορά αξιοποιεί τα έξυπνα συμβόλαια για να δώσει στα άτομα μεγαλύτερο έλεγχο των προσωπικών τους δεδομένων, επιτρέποντάς τους να τα αξιοποιήσουν οικονομικά με τους δικούς τους όρους, ενώ παράλληλα αυτοματοποιεί τη διαδικασία συναλλαγής δεδομένων και ενισχύει την ασφάλεια. Παρόλο που η εφαρμογή είναι συγκεκριμένη για το οικοσύστημα Cardano, οι αρχές και οι μεθοδολογίες μπορούν να προσαρμοστούν σε άλλες πλατφόρμες blockchain, προσφέροντας μια ευέλικτη λύση σε ένα καθολικό πρόβλημα.

Ελπίζω η εργασία αυτή να αποτελέσει έμπνευση για περαιτέρω έρευνα και ανάπτυξη στην αξιοποίηση των έξυπνων συμβολαίων για πρακτικές λύσεις. Είτε είστε φοιτητής, είτε ερευνητής, είτε απλά κάποιος που σας ιντριγκάρει η μετασχηματιστική δυνατότητα των έξυπνων συμβολαίων να αυτοματοποιήσουν και να διασφαλίσουν ένα ευρύ φάσμα εφαρμογών, πιστεύω ότι η παρούσα διπλωματική εργασία έχει πολύτιμες γνώσεις να σας προσφέρει.

Σας ευχαριστώ που αφιερώσατε χρόνο για να ασχοληθείτε με αυτή την εργασία. Ανυπομονώ για τις συζητήσεις και τις εξελίξεις που μπορεί να πυροδοτήσει.

Κεφάλαιο 1

Εισαγωγή

Στη σύγχρονη εποχή, τα δεδομένα έχουν γίνει ένα από τα πιο πολύτιμα αγαθά. Καθοδηγούν τη λήψη αποφάσεων σε διάφορους τομείς, από την υγειονομική περίθαλψη και τη χρηματοδότηση έως το μάρκετινγκ και τη δημόσια πολιτική. Ωστόσο, τα τρέχοντα μοντέλα συλλογής και νομισματοποίησης δεδομένων συχνά αφήνουν στους μεμονωμένους χρήστες ελάχιστο έλεγχο των προσωπικών τους πληροφοριών. Αυτή η συγκεντρωτική προσέγγιση έχει οδηγήσει σε αυξανόμενες ανησυχίες σχετικά με το απόρρητο των δεδομένων, την ασφάλεια και την ιδιοκτησία. Η άνοδος της τεχνολογίας blockchain και των έξυπνων συμβολαίων προσφέρει μια μετασχηματιστική λύση σε αυτές τις προκλήσεις, επιτρέποντας ένα αποκεντρωμένο, διαφανές και ασφαλές πλαίσιο για τη διαχείριση δεδομένων.

Ενώ τα υπάρχοντα συστήματα προσφέρουν κάποιο επίπεδο προστασίας των δεδομένων, συχνά βασίζονται σε κεντρικούς μεσάζοντες, γεγονός που τα καθιστά ευάλωτα σε κινδύνους ασφαλείας και περιορίζει τον έλεγχο των χρηστών. Επιπλέον, οι χρήστες σπάνια λαμβάνουν απτά οφέλη για τη συνεισφορά των δεδομένων τους, δημιουργώντας μια ανισορροπία στην οικονομία των δεδομένων.

Ο πρωταρχικός στόχος της παρούσας διπλωματικής είναι να διερευνήσει τις δυνατότητες της τεχνολογίας blockchain, συγκεκριμένα μέσω της χρήσης έξυπνων συμβολαίων στο δίκτυο Cardano, για τη δημιουργία μιας αποκεντρωμένης αγοράς δεδομένων. Αυτή η αγορά έχει ως στόχο να:

1. Να ενδυναμώσει τους χρήστες δίνοντάς τους τον έλεγχο των δεδομένων τους και άμεσο όφελος από την πώληση τους.

2. Να παρέχει ένα διαφανές και δίκαιο σύστημα της πώλησης των δεδομένων, εξαλείφοντας την ανάγκη για κεντρικούς μεσάζοντες, μέσω της αυτοματοποίησης που προσφέρουν τα έξυπνα συμβολαία.

3. Εξασφαλίση την ασφάλειας αξιοποιώντας τα κρυπτογραφικά χαρακτηριστικά της τεχνολογίας blockchain.

Ερωτήσεις έρευνας

1. Πώς μπορεί να αξιοποιηθεί η τεχνολογία blockchain για τη δημιουργία μιας αποκεντρωμένης αγοράς δεδομένων;

2. Ποιες είναι οι τεχνικές προκλήσεις και λύσεις στην υλοποίηση μιας τέτοιας αγοράς;

3. Πώς μπορούν τα έξυπνα συμβόλαια να διασφαλίσουν την ιδιωτικότητα και την ασφάλεια των δεδομένων;

Η παρούσα διπλωματική εργασία επικεντρώνεται στο σχεδιασμό και την υλοποίηση μιας αποκεντρωμένης αγοράς δεδομένων με τη χρήση της πλατφόρμας έξυπνων συμβολαίων του Cardano, Plutus. Καλύπτει τις τεχνικές πτυχές, συμπεριλαμβανομένης της ανάπτυξης front-end και back-end, της υλοποίησης έξυπνων συμβολαίων και των λύσεων αποθήκευσης δεδομένων μέσω του πρωτόκολλου IPFS. Επιπρόσθετα, πραγματοποιείται ανάλυση των ηθικών διαστάσεων που αφορούν την ιδιωτικότητα και την κυριότητα των δεδομένων σε ένα πλαίσιο ενεργοποιημένο από την τεχνολογία blockchain.

Περίγραμμα

1. Εισαγωγή: Παρέχει μια επισκόπηση του έργου, συμπεριλαμβανομένης της δήλωσης του προβλήματος, των στόχων, των ερευνητικών ερωτημάτων και του πεδίου εφαρμογής της μελέτης.

2. Θεωρητικό Μέρος: Διερευνά τα θεωρητικά θεμέλια, συμπεριλαμβανομένης της τεχνολογίας blockchain, των έξυπνων συμβολαίων και των αποκεντρωμένων εφαρμογών.

3. Μεθοδολογία και υλοποίηση: Περιγράφει λεπτομερώς την αρχιτεκτονική του συστήματος και τη διαδικασία υλοποίησης.

4. Αποτελέσματα και συζήτηση: Αναλύει τα τεχνικά επιτεύγματα, τις προκλήσεις και τις μελλοντικές κατευθύνσεις.

5. Δεοντολογικές εκτιμήσεις: Διερευνά τις ηθικές προεκτάσεις του έργου.

6. Επίλογος: Αναστοχασμός σχετικά με τον ευρύτερο αντίκτυπο και τις δυνατότητες για μελλοντικές εργασίες.

Με την εξέταση των προκλήσεων και των ευκαιριών για τη δημιουργία μιας αποκεντρωμένης αγοράς δεδομένων, η παρούσα διπλωματική έχει ως στόχο να συμβάλει στη συνεχιζόμενη συζήτηση σχετικά με την προστασία της ιδιωτικής ζωής, την ασφάλεια των δεδομένων, και την ιδιοκτησία. Χρησιμεύει ως σκαλοπάτι προς ένα μέλλον όπου η τεχνολογία blockchain και τα έξυπνα συμβόλαια δίνουν στα άτομα τη δυνατότητα μεγαλύτερου ελέγχου των προσωπικών τους δεδομένων, προωθώντας έτσι μια πιο διαφανή και δίκαιη οικονομία δεδομένων.

Μέρος Ι

Θεωρητικό Μέρος

Κεφάλαιο 2

Βιβλιογραφική ανασκόπηση

2.1 Τεχνολογία Blockchain

Η τεχνολογία Blockchain έχει αναδειχθεί ως μια πρωτοποριακή τεχνολογία, τόσο στον ακαδημαϊκό όσο και στον επιχειρηματικό κόσμο , αλλάζοντας ριζικά τον τρόπο με τον οποίο αντιλαμβανόμαστε τις ψηφιακές συναλλαγές και την αποθήκευση δεδομένων. Απέκτησε αρχική προβολή μέσω της πρώτης εφαρμογής της σε κρυπτονομίσματα όπως το Bitcoin [1]. Η τεχνολογία χαρακτηρίζεται από την αποκέντρωση, τη διαφάνεια και τους ισχυρούς μηχανισμούς ασφαλείας [2].

Ωστόσο, η τεχνολογία Blockchain έχει βρει εφαρμογές πολύ πέρα από τα κρυπτονομίσματα, επεκτεινόμενη σε τομείς όπως η υγειονομική περίθαλψη, η διαχείριση της εφοδιαστικής αλυσίδας και η διακυβέρνηση [3]. Στον τομέα της υγειονομικής περίθαλψης, για παράδειγμα, η τεχνολογία blockchain χρησιμοποιείται για τη διασφάλιση του απορρήτου και της ασφάλειας των δεδομένων, ειδικά όταν πρόκειται για ευαίσθητα δεδομένα ασθενών [3]. Ο αποκεντρωμένος μηχανισμός αποθήκευσης της αλυσίδας μπλοκ εξασφαλίζει ότι τα δεδομένα είναι όχι μόνο ασφαλή αλλά και εύκολα επαληθεύσιμα, γεγονός που προσθέτει ένα επιπλέον επίπεδο εμπιστοσύνης και λογοδοσίας.

Η αλυσίδα μπλοκ, στον πυρήνα της, λειτουργεί ως ένα λογιστικό βιβλίο, σκοπός του οποίου είναι η καταγραφή των συναλλαγών σε ένα δίκτυο κατανεμημένων υπολογιστικών συστημάτων. Αυτή η μοναδική αρχιτεκτονική παρέχει ασφάλεια, διαφάνεια και ακεραιότητα δεδομένων. Για να επιτευχθεί αυτό, οι συναλλαγές ομαδοποιούνται σε μπλοκ και στη συνέχεια συνδέονται με διαδοχικό τρόπο για τη δημιουργία μιας δομής που μοιάζει με αλυσίδα και ονομάζεται ¨blockchain¨. Σε αντίθεση με τα συνηθισμένα συστήματα, το blockchain δεν βασίζεται σε μια κεντρική αρχή για τον έλεγχο, καθιστώντας το πιο δημοκρατικό. Η αυθεντικότητα των συναλλαγών επαληθεύεται από τους κόμβους του δικτύου με τη χρήση κρυπτογραφικών τεχνικών και αλγορίθμων συναίνεσης, γεγονός που ενισχύει το δίκτυο έναντι αλλαγών και εξασφαλίζει την αξιοπιστία του.

2.1.1 Το μοντέλο UTXO

Το Bitcoin, το διαμάντι του στέμματος των κρυπτονομισμάτων, λειτουργεί σε ένα μοντέλο λογιστικού βιβλίου που έχει τις ρίζες του στην έννοια των Unspent Transaction Outputs (UTxOs) [4]. Σε αυτό το μοντέλο, οι μεμονωμένες συναλλαγές δεν είναι απλά γραμμικά γεγονότα- είναι σύνθετες οντότητες που περιλαμβάνουν τόσο εισόδους όσο και εξόδους. Αυ-

τές οι έξοδοι χρησιμεύουν ως τοποτηρητές αξίας, αντιπροσωπεύοντας συγκεκριμένα ποσά κρυπτονομισμάτων που είναι έτοιμα να χρησιμοποιηθούν σε μελλοντικές συναλλαγές.

Είναι σημαντικό να σημειωθεί ότι κάθε έξοδος προορίζεται να συνδεθεί με ακριβώς μία είσοδο σε μια επόμενη συναλλαγή. Πρόκειται για ένα σχολαστικά δομημένο σύστημα, χωρίς να επιτρέπονται κύκλοι και διπλές δαπάνες. Αυτό διασφαλίζει ότι οι συναλλαγές σχηματίζουν ένα κατευθυνόμενο ακυκλικό γράφο (Directed Acyclic Graph - DAG), ένα γράφο οικονομικών αλληλεπιδράσεων όπου κάθε συναλλαγή -που χαρακτηρίζεται από "m" εισόδους και "n" εξόδους - εμφανίζεται ως ένας μοναδικός κόμβος, πλήρης με το δικό του σύνολο ακμών εισόδου και εξόδου. Μια έξοδος μπορεί στη συνέχεια να χρησιμεύσει ως πιθανή είσοδος για επόμενες συναλλαγές, συμβάλλοντας έτσι στη συνεχή κατασκευή της αλυσίδας μπλοκ.

Το μοντέλο επιβάλλει επίσης έναν νόμο διατήρησης, παρόμοιο με τους φυσικούς νόμους που διέπουν το σύμπαν μας. Η συνολική αξία που απορροφάται από τις εισροές μιας συναλλαγής πρέπει να βρίσκεται σε τέλεια ισορροπία με τη συνολική αξία που εκπέμπεται από τις εκροές της. Στην ουσία, η αξία ούτε δημιουργείται ούτε καταστρέφεται- διατηρείται σχολαστικά.

Μια σημαντική λεπτομέρεια που πρέπει να σημειωθεί είναι: κάθε έξοδος είναι μια οντότητα μιας χρήσης. Μόλις μια έξοδος χρησιμοποιηθεί ως είσοδος σε μια επόμενη συναλλαγή, μετατρέπεται από ¨μη δαπανημένη¨ σε ¨δαπανημένη¨. Αυτό σημαίνει ότι δεν μπορεί πλέον να επαναχρησιμοποιηθεί ως είσοδος για μελλοντικές συναλλαγές. Αυτός ο χαρακτήρας της εφάπαξ χρήσης των εξόδων είναι που τους δίνει την ετικέτα ¨μη δαπανημένες έξοδοι συναλλαγών¨(UTxO) μέχρι να δαπανηθούν πραγματικά. Πρόκειται για ένα ενσωματωμένο χαρακτηριστικό ασφαλείας που αποτρέπει τη διπλή δαπάνη και διασφαλίζει την ακεραιότητα του ιστορικού συναλλαγών.

2.2 Έξυπνα συμβόλαια

2.2.1 Το Extended UTXO μοντέλο

Το μοντέλο ledger του Cardano είναι το EUTxO [5]. Το μοντέλο Extended UTxO (EUTxO) είναι μια επέκταση του μοντέλου UTxO του Bitcoin που υποστηρίζει μια πιο εκφραστική μορφή σεναρίων επικύρωσης. Σε αυτό το εκτεταμένο μοντέλο, μια έξοδος μπορεί να δαπανηθεί, να χρησιμοποιηθεί ως είσοδος μιας επόμενης συναλλαγής, μόνο εάν ικανοποιεί μια συνάρτηση ν. Αυτή η συνάρτηση είναι γνωστή ως validator(επικυρωτής) της εξόδου. Εδώ έρχεται η έννοια του redeemer(εξαργυρωτή). Μια συναλλαγή αποδεικνύει την επιλεξιμότητά της να ξοδέψει μια έξοδο παρέχοντας μια τιμή redeemer ρ, τέτοια ώστε ν(ρ) = αληθής.

Ας εξετάσουμε την απλούστερη δυνατή περίπτωση, όπου ένας ιδιοκτήτης πορτοφολιού προσπαθεί να ξοδέψει ένα από τα δικά του UTxO. Σε ένα βασικό μοντέλο UTXO, μπορεί κανείς να αντιληφθεί ότι ο redeemer είναι ο κρυπτογραφικός κατακερματισμός της συναλλαγής δαπάνης υπογεγραμμένος από το ιδιωτικό κλειδί αυτού του πορτοφολιού και η λειτουργία επικύρωσης ως ένα σταθερό script(σενάριο) που επαληθεύει, αν αυτός ο κατακερματισμός είναι πράγματι υπογεγραμμένος από τον ιδιοκτήτη των εισόδων της συναλλαγής.

Από την άλλη πλευρά, στο μοντέλο Extended UTxO (EUTxO), η έννοια του redeemer δεν περιορίζεται σε μια συγκεκριμένη αξία- μπορεί ουσιαστικά να είναι οποιαδήποτε αξία,

η οποία επιλέγεται και αποστέλλεται από τη συναλλαγή που αποσκοπεί στην κατανάλωση του UTxO. Επιπλέον, η συνάρτηση επικυρωτή(validator) ν δεν είναι αμετάβλητη- μπορεί να αντικατασταθεί με οποιαδήποτε λογική έξυπνου συμβολαίου που ταιριάζει στις ανάγκες της εφαρμογής.

Το μοντέλο EUTxO αναβαθμίζει την παραδοσιακή έξοδο UTxO από ένα απλό ζεύγος ενός επικυρωτή ν και μιας αξίας κρυπτονομίσματος σε ένα πιο περίπλοκο τρίπτυχο -(ν, αξία, δ). Εδώ, το δ είναι ένα Datum(δεδομένο) που περιέχει δεδομένα ειδικά για το συμβόλαιο, προσθέτοντας άλλο ένα επίπεδο πολυπλοκότητας και χρησιμότητας στο μοντέλο. Στην εφαρμογή της Cardano, τα έξυπνα συμβόλαια γνωρίζουν επίσης ολόκληρο το πλαίσιο της συναλλαγής δαπάνης που προσπαθεί να καταναλώσει το UTxO. Αυτή η ολοκληρωμένη πρόσβαση δίνει τη δυνατότητα στους validators να επιβάλλουν απρόσκοπτα τη συνέχεια των συμβολαίων.

Πολλαπλοί validators μπορούν να συντονιστούν για τη δημιουργία σύνθετων συστημάτων. Συνοψίζοντας, για μια είσοδο με redeemer ρ που αποτελεί μέρος της συναλλαγής tx, το σύστημα επαληθεύει το δικαίωμά του να δαπανήσει μια έξοδο (ν, αξία, δ) εξασφαλίζοντας ότι

$$\nu(\text{αξία}, \delta, \rho, \text{tx}) = \text{αληθές}.$$

Σε μια προσπάθεια να συνοψίσουμε την ουσία του μοντέλου Extended UTxO (EUTxO) και τον ρόλο του στα έξυπνα συμβόλαια του Cardano, ας συνοψίσουμε τα βασικά συστατικά του:

- Datum: Δεν πρόκειται για ένα οποιοδήποτε κομμάτι δεδομένων, αλλά για ένα ωφέλιμο φορτίο που μεταφέρεται στο πλαίσιο μιας εξόδου συναλλαγής. Καθορισμένο από τη συναλλαγή που γεννά την έξοδο, το δεδομένο είναι αμετάβλητο. Όταν μια έξοδος πρόκειται να μεταβεί σε κατάσταση ¨spent¨, αυτό το δεδομένο μεταβιβάζεται στη συνάρτηση validator, η οποία στη συνέχεια αποφασίζει αν θα δώσει το πράσινο φως για τη δαπάνη της. Αυτός ο μηχανισμός παρέχει σε κάθε κλειδωμένη έξοδο έναν ορισμένο βαθμό κατάστασης(state).

- Πλαίσιο: Ο validator δεν είναι απομονωμένος· Λαμβάνει πλούσιες πληροφορίες σχετικά με τη συναλλαγή δαπανών. Αυτό περιλαμβάνει όλες τις εισόδους της συναλλαγής και, κυρίως, πρόσβαση σε όλες τις εξόδους της. Αυτό ανοίγει την πόρτα σε ενδιαφέροντα σενάρια όπου πολλαπλοί validators μπορούν να συνεργαστούν συντονισμένα για να ενορχηστρώσουν σύνθετες λογικές λειτουργίες.

- Redeemer: Αυτή είναι η τιμή μπαλαντέρ που μεταβιβάζεται στον επικυρωτή από τη συναλλαγή που προσπαθεί να δαπανήσει την έξοδο. Είναι ένα ευέλικτο εργαλείο, ειδικά όταν πολλοί φορείς επιθυμούν να επικαλεστούν τον ίδιο validator. Ο validator μπορεί να εφαρμόζει διαφορετικούς κανόνες σε κάθε φορέα ή ακόμη και να επιτρέπει σε έναν μόνο φορέα να εκτελεί ποικίλες λειτουργίες.

2.2.2 Cardano και Plutus

Το Cardano χρησιμοποιεί το Plutus ως εγγενή γλώσσα προγραμματισμού για έξυπνα συμβόλαια, ένα ισχυρό εργαλείο βασισμένο στη Haskell, το οποίο αξιοποιεί το ισχυρό σύστημα τύπων της Haskell και τις αρχές του συναρτησιακού προγραμματισμού. Στην πράξη,

τα έξυπνα συμβόλαια αναπτύσσονται σε Haskell, η οποία στη συνέχεια μεταγλωττίζεται στο Plutus Core χρησιμοποιώντας το πρόσθετο Plutus Tx GHC. Σε αντίθεση με τη Solidity του Etherium, το Plutus δίνει μεγάλη προτεραιότητα στην ασφάλεια. Αυτή η ενότητα καταδύεται σε μερικλά δυνατά σημεία του Plutus και σε ορισμένα από τα πλεονεκτήματά του έναντι της Solidity, όπως τονίζεται στο έγγραφο "UTxO- vs account-based smart contract blockchain programming paradigms" των Brünjes, Gabbay και άλλων (Brünjes et al., 2020) [6].

Ενισχυμένη προγραμματισιμότητα Το Plutus επιβαρύνει περισσότερο τους προγραμματιστές, αλλά συνδυάζεται με ισχυρές μαθηματικές ιδιότητες που ενισχύουν την προγραμματισιμότητα, όπως τα Monads [6]. Αυτή η μαθηματική έμφαση παρέχει μια ισχυρή βάση για την ανάπτυξη πιο σύνθετων και ασφαλών έξυπνων συμβολαίων.

Έλεγχος από τον χρήστη - Ντετερμινισμός Ένα από τα ιδιαίτερα χαρακτηριστικά του Plutus είναι το επίπεδο ελέγχου που προσφέρει στους χρήστες. Στο Plutus, ο καταναλωτής ενός συμβολαίου μπορεί να δημιουργήσει μια συναλλαγή και να αποφανθεί εκ των προτέρων τις εισόδους και τις εξόδους της. Αυτό επιτρέπει στους χρήστες να προφυλάσσονται από πιθανά σφάλματα ή επιθέσεις ανεξάρτητα από τον σχεδιαστή του συμβολαίου [6]. Κάθε φορά που μια συναλλαγή γίνεται αποδεκτή, θα έχει προβλέψιμες επιπτώσεις στην κατάσταση του Ledger. Διασφαλίζοντας ότι μια δέσμη ενεργειών θα τερματίζει πάντα(βλ. Halting Problem [7]) και ότι θα επιστρέφει το ίδιο αποτέλεσμα αν εφαρμοστούν τα ίδια ορίσματα, όπως μια καθαρή συνάρτηση, παρέχεται ντετερμινιστική αξιολόγηση του αποτελέσματος. Οι καταναλωτές μπορούν να εκτελέσουν τοπικά την πιθανή συναλλαγή τους και να προβλέψουν πόσο θα κοστίσουν τα τέλη, αν η συναλλαγή θα γίνει αποδεκτή και τι αντίκτυπο θα έχει στο Ledger. Έτσι, οι χρήστες που ενεργούν με καλή πίστη δεν θα έχουν απροσδόκητες παρενέργειες και δεν θα χάσουν ποτέ κατά λάθος κανένα collateral(ενέχυρο).

Κρίσιμος αντίκτυπος Κρίσιμος αντίκτυπος Το έγγραφο επισημαίνει ότι το Ethereum μπορεί να είναι "αναμφισβήτητα buggy", ένα φαινόμενο που προέρχεται από τα υποκείμενα προγραμματιστικά θεμέλια της Solidity. Το Plutus αποφεύγει τέτοιους κινδύνους, καθιστώντας το πιο αξιόπιστο για εφαρμογές κρίσιμης σημασίας [6]. Εκτός από τη μαθηματική αυστηρότητα και το σχεδιασμό με επίκεντρο τον χρήστη, το Plutus κληρονομεί επίσης την έμφαση της Haskell στην αμετάβλητη λειτουργία. Αυτό το χαρακτηριστικό δεν είναι απλώς μια θεωρητική λεπτομέρεια, αλλά ένα πρακτικό χαρακτηριστικό που ενισχύει την ασφάλεια και την ευρωστία των έξυπνων συμβολαίων. Η αμεταβλητότητα απομακρύνει ένα ευρύ φάσμα σφαλμάτων που σχετίζονται με τη μεταβλητή κατάσταση, καθιστώντας ευκολότερο να συνάγουμε συμπέρασμα ως προς τη συμπεριφορά των έξυπνων συμβολαίων κατά την ανάπτυξή τους και διασφαλίζοντας ότι μόλις αναπτυχθούν, οι κανόνες του συμβολαίου θα συμπεριφέρονται όπως αναμένεται. Αυτό ευθυγραμμίζεται καλά με την αμετάβλητη φύση της τεχνολογίας blockchain , ένα βασικό χαρακτηριστικό που είναι υπεύθυνο για την ασφάλεια και την αξιοπιστία της.

2.2.3 Validators και Minting Policies

Μέχρι στιγμής έχουμε συζητήσει τα έξυπνα συμβόλαια επικυρωτών(validators) και αναφέραμε ότι κάθε φορά που επιχειρείται να δαπανηθεί ένα UTxO που έχει κλειδωθεί από μια διεύθυνση έξυπνου συμβολαίου validator, θα εκτελεστεί το αντίστοιχο έξυπνο συμβόλαιο validator, με 3 εισόδους, το Datum (από το UTxO), τον Redeemer (από την είσοδο) και το Πλαίσιο Συναλλαγής(Transaction Context).

Ωστόσο, ένα έξυπνο συμβόλαιο, εκτός από το σκοπό του validator, μπορεί επίσης να έχει και σκοπό Minting(νομισματοκοπίας). Αυτά τα έξυπνα συμβόλαια ονομάζονται Minting Policies και δίνουν τη δυνατότητα να κόβουν native tokens Cardano, τα οποία μπορούν να εξυπηρετήσουν πολλαπλούς σκοπούς στο οικοσύστημα blockchain.

Τα tokens μπορούν να χρησιμοποιηθούν για την αντιπροσώπευση συγκεκριμένων ρόλων για τους χρήστες που αλληλεπιδρούν με τα έξυπνα συμβόλαια [8]. Για παράδειγμα, ένα token θα μπορούσε να αντιπροσωπεύει το ρόλο ενός πιστωτή σε μια σύμβαση που βασίζεται σε συμφέροντα. Δεδομένου ότι ένα token μπορεί να έχει ένα μοναδικό αναγνωριστικό, τα Datums έξυπνων συμβολαίων μπορούν να δείχνουν σε αυτά, δημιουργώντας σύνθετες συνθήκες βασισμένες σε ρόλους, χωρίς να απαιτείται ένας σκληρά κωδικοποιημένος κατάλογος στοιχείων μέσα στο ίδιο το συμβόλαιο. Δεδομένου ότι τα ίδια τα token είναι πόροι στο λογιστικό βιβλίο, μπορούν να ανταλλάσσονται, επιτρέποντας ουσιαστικά την ανταλλαγή ρόλων [8]. Για παράδειγμα, ένας αγοραστής θα μπορούσε να αποκτήσει ένα token πωλητή, όπως θα αποδειχθεί στην επερχόμενη υλοποίηση. Τα tokens μπορούν να διασφαλίσουν ότι όλοι οι συμμετέχοντες σε μια συμφωνία, όπως η αρχική προσφορά νομισμάτων, έχουν συμμετάσχει. Με την έκδοση tokens συμμετοχής, το δικαίωμα συμμετοχής γίνεται εμπορεύσιμο περιουσιακό στοιχείο, διασφαλίζοντας ότι κανένας συμμετέχων δεν μπορεί να παραλειφθεί αθέμιτα [8].

Όσον αφορά το πλαίσιο εκτέλεσής τους, τα Minting Policies εκτελούνται κάθε φορά που κάποιος προσπαθεί να κόψει ή να κάψει ένα token (νομισματικό σύμβολο) που έχουν ορίσει. Λαμβάνουν 2 εισόδους, τον Redeemer και το Πλαίσιο Συναλλαγής. Δεν επικυρώνουν το ξεκλείδωμα κάποιου UTxO, οπότε δεν υπάρχει Datum, σε αντίθεση με τα Validator scripts.

2.2.4 Παραμετροποιημένα scripts

Μέχρι στιγμής έχουμε συζητήσει τα validator έξυπνα συμβολαία, τα οποία έχουν μια διεύθυνση στο blockchain και κλειδώνουν τα UTxOs που αποστέλλονται στη διεύθυνσή αυτή. Αντί να ορίσουμε ένα script, με μια μοναδική διεύθυνση, με όλα τα UTxOs να βρίσκονται στην ίδια διεύθυνση, μπορούμε να ορίσουμε μια οικογένεια από Validator έξυπνα συμβόλαια που παραμετροποιούνται από μια δεδομένη παράμετρο [9]. Αυτά ονομάζονται παραμετροποιημένα σενάρια(Parameterized Scripts). Ένα Parameterized Script, αφού του δοθούν πραγματικές συγκεκριμένες τιμές παραμέτρων, μπορεί να λάβει την διεύθυνση του όπως κάνουν τα απλά μη παραμετροποιημένα σενάρια. Αυτή η ικανότητα, εγείρει το ερώτημα, αν θα πρέπει μερικές φορές να βάζουμε ένα κομμάτι της κατάστασης που θέλουμε στο δεδομένο ή στις παραμέτρους ενός σεναρίου.

Όταν προσθέτουμε τα δεδομένα στο Datum και επιμένουμε σε μη παραμετροποιημένο σενάριο, έχουμε 1 διεύθυνση σεναρίου. Έτσι, όλα τα UTxO και τα Datums για ένα μη πα-

ραμετροποιημένο σενάριο βρίσκονται στην ίδια διεύθυνση σεναρίου, πράγμα που σημαίνει ότι είναι εύκολα ανιχνεύσιμα.

Από την άλλη πλευρά, αν χρησιμοποιήσουμε ένα παραμετροποιημένο σενάριο, για κάθε διαφορετική επιλογή παραμέτρων, θα έχουμε ένα διαφορετικό σενάριο, με εντελώς διαφορετικό hash και επομένως μια εντελώς διαφορετική διεύθυνση. Κατά συνέπεια, είναι πολύ πιο δύσκολο να τα βρει κάποιος που θα ήθελε να τα ανακαλύψει. Θα πρέπει να γνωρίζει ποιες παραμέτρους πρέπει να αναζητήσει για να υπολογίσει τη διεύθυνση του σεναρίου. Έτσι, συνολικά η επιλογή μεταξύ των δύο μπορεί να εξαρτηθεί από τους ακόλουθους παράγοντες:

1. Τύπος δεδομένων: Εάν τα δεδομένα με τα οποία ασχολείστε είναι δυναμικά και αναμένεται να αλλάζουν συχνά κατά τη διάρκεια της λειτουργίας της σύμβασης, τότε μπορεί να είναι καταλληλότερο να αποθηκεύσετε τα δεδομένα αυτά στο Datum. Το Datum έχει σχεδιαστεί για να διατηρεί την κατάσταση της σύμβασης ανά πάσα στιγμή, και έτσι είναι κατάλληλο για δεδομένα που αλλάζουν συχνά. Από την άλλη πλευρά, εάν τα δεδομένα είναι πιο στατικά και ορίζονται όταν το συμβόλαιο αναπτύσσεται για πρώτη φορά(όπως μια συγκεκριμένη αναλογία για ένα αποκεντρωμένο χρηματιστήριο), τότε ίσως είναι προτιμότερο να χρησιμοποιήσετε ένα παραμετροποιημένο σενάριο.

2. Ευελιξία Συμβολαίου: Τα παραμετροποιημένα συμβόλαια προσφέρουν μεγαλύτερη ευελιξία. Μπορούν να είναι διαφορετικά ανάλογα με τις παραμέτρους με τις οποίες αρχικοποιούνται. Αν θέλετε να επαναχρησιμοποιήσετε τη λογική του συμβολαίου σε διαφορετικές περιπτώσεις με ελαφρώς διαφορετικές συμπεριφορές, τότε ένα παραμετροποιημένο συμβόλαιο μπορεί να είναι μια καλή επιλογή. Ωστόσο, εάν η λογική σας είναι στενά συνδεδεμένη με την κατάσταση του συμβολαίου και η κατάσταση αλλάζει συχνά, η χρήση του Datum για την αποθήκευση της κατάστασης μπορεί να είναι μια καλύτερη προσέγγιση.

3. Μέγεθος και πολυπλοκότητα: Η πολυπλοκότητα και το μέγεθος των δεδομένων μπορεί επίσης να επηρεάσουν αυτή την απόφαση. Εάν τα δεδομένα είναι μεγάλα ή πολύπλοκα, η αποθήκευση στο Datum μπορεί να είναι πιο εύχρηστη και αποτελεσματική.

Σε γενικές γραμμές, αυτές οι αποφάσεις θα λαμβάνονται συχνά με βάση τις συγκεκριμένες απαιτήσεις του έξυπνου συμβολαίου και δεν υπάρχει μία απάντηση που να ταιριάζει σε όλες τις συνθήκες. Η κατανόηση του τομέα(domain) του συμβολαίου, καθώς και των διαφορών και των συμβιβασμών κάθε επιλογής είναι ζωτικής σημασίας για την καθοδήγηση της απόφασής.

Τα Minting Policies κάνουν μεγάλη χρήση των παραμετροποιημένων scripts. Με την παραμετροποίηση ενός Minting Policy με το αναγνωριστικό του συγκεκριμένου UTxO ενός χρήστη και, στη συνέχεια, με την απαίτηση ότι κάθε συναλλαγή που χρησιμοποιεί αυτό το Minting Policy πρέπει να καταναλώνει ως είσοδο το συγκεκριμένο UTxO, μπορούν να κοπούν πραγματικά μοναδικά tokens. Ένα UTxO μπορεί να ξοδευτεί μόνο μία φορά, με βάση το μοντέλο UTXO, οπότε αυτό διασφαλίζει ότι μόνο ο ιδιοκτήτης της παραμέτρου UTxO θα μπορεί να κόψει το token, και μάλιστα μόνο μία φορά. Αυτή η προσέγγιση επιτρέπει με έξυπνο τρόπο τη δημιουργία αυθεντικών non-fungible tokens (NFTs) στο οικοσύστημα Cardano.

2.2.5 Κώδικας off-chain vs on-chain

Ο κώδικας Plutus Core λειτουργεί σε δύο διαφορετικά πεδία: το περιβάλλον εντός(on-chain) και εκτός(off-chain) αλυσίδας, το καθένα με τους δικούς του κανόνες και στόχους.

Όταν μιλάμε για on-chain, αναφερόμαστε στην υπολογιστική λογική που αξιολογεί τις συναλλαγές απευθείας στην αλυσίδα μπλοκ. Αυτός ο κώδικας εκτελείται κάθε φορά που προτείνεται μια συναλλαγή, διασφαλίζοντας την εγκυρότητά της. Αν η συναλλαγή περάσει, είναι πολύ πιθανό να ενσωματωθεί στην αλυσίδα μπλοκ. Αλλά αυτή η υπολογιστική επικύρωση δεν είναι δωρεάν, εισπράττονται τέλη συναλλαγών για να αποτρέπονται οι κακόβουλοι φορείς από το να κατακλύζουν το δίκτυο και να καταλαμβάνουν άσκοπα τους κόμβους της αλυσίδας μπλοκ [10], διασφαλίζοντας έτσι τη λειτουργική ακεραιότητα της αλυσίδας μπλοκ.

Από την άλλη πλευρά, ο off-chain κώδικας έχει διαφορετική αποστολή. Χρησιμεύει ως αρχιτέκτονας των συναλλαγών, διαμορφώνοντάς τες για υποβολή στην αλυσίδα μπλοκ. Φανταστείτε ότι είστε απορροφημένοι σε μια ηλεκτρονική δημοπρασία που φιλοξενείται στο Cardano. Για να κάνετε μια προσφορά, θα πρέπει να αποστείλετε συγκεκριμένα δεδομένα στο έξυπνο συμβόλαιο της δημοπρασίας -όπως ένα αναγνωριστικό και την προσφορά σας σε Ada(το νόμισμα του Cardano). Εδώ, ο off-chain κώδικας αναλαμβάνει τα ηνία, κατασκευάζοντας τη συναλλαγή, εκτελώντας προκαταρκτικές επικυρώσεις για να αποφευχθεί η σπατάλη τελών και υπολογίζοντας τα τέλη της συναλλαγής πριν την αποστείλει στην αλυσίδας μπλοκ.

Πρώτον, θεωρήστε ότι ένας χρήστης κλειδώνει ένα UTXO σε μια συγκεκριμένη διεύθυνση Validator. Όταν έρθει η στιγμή να ξοδευτεί αυτό το UTXO, καλείται ο Validator. Αλλά εδώ είναι η παγίδα: αυτή η διαδικασία επικύρωσης πραγματοποιείται αρχικά εκτός αλυσίδας. Γιατί; Για να μετριαστεί η υπολογιστική επιβάρυνση των κόμβων της αλυσίδας μπλοκ. Αυτή η επικύρωση εκτός αλυσίδας χρησιμεύει ως ένα αρχικό φίλτρο, διασφαλίζοντας ότι μόνο οι συναλλαγές με υψηλή πιθανότητα επιτυχίας προχωρούν στο στάδιο επικύρωσης εντός αλυσίδας. Πρόκειται για έναν αποδοτικό σε πόρους μηχανισμό που αποτρέπει το δίκτυο από το να κατακλύζεται από αποτυχημένες συναλλαγές.

Σε περίπτωση που μια συναλλαγή παρακάμψει τους ελέγχους εκτός αλυσίδας -ίσως εξαιτίας ενός κακόβουλου χρήστη που προσπαθεί να κάνει κατάχρηση του συστήματος- δεν θα μπορεί να παρακάμψει τους ελέγχους εντός αλυσίδας. Κάθε συναλλαγή που περιλαμβάνει επικύρωση έξυπνων συμβολαίων απαιτείται να περιλαμβάνει ένα ενέχυρο(collateral) UTxO [11]. Σε περίπτωση που η συναλλαγή αποτύχει στην επικύρωση εντός της αλυσίδας, αυτό το ενέχυρο UTxO χάνεται. Πρόκειται για μια οικονομική εγγύηση που προσθέτει ένα ακόμη επίπεδο ασφάλειας, διασφαλίζοντας ότι οι κακόβουλοι φορείς θα το σκεφτούν δύο φορές πριν επιχειρήσουν να πλημμυρίσουν το δίκτυο με άκυρες συναλλαγές.

Ανάπτυξη έξυπνων συμβολαίων Όταν αλληλεπιδράτε με έξυπνα συμβόλαια, υπάρχουν δύο επιλογές: είτε να ενσωματώσετε ολόκληρο το έξυπνο συμβόλαιο σε κάθε συναλλαγή είτε να το αναπτύξετε(deploy) μία φορά και να το αναφέρετε σε επόμενες συναλλαγές, χρησιμοποιώντας ένα UTxO εισόδου αναφοράς(reference input). Η τελευταία προσέγγιση, που θυμίζει τις καλές πρακτικές στον σχεδιασμό λογισμικού, ελαχιστοποιεί τον πλεονασμό, αποθηκεύοντας το σενάριο επικύρωσης μία φορά στην αλυσίδα μπλοκ και στη συνέχεια ανατρέχοντας σε αυτό όταν χρειάζεται. Ενώ αυτό απαιτεί ένα αρχικό κόστος για την ανάπτυξη, αποφέρει

μακροπρόθεσμα εξοικονόμηση σε υπολογιστικούς πόρους και αποθήκευση, καθιστώντας την προτιμώμενη στρατηγική για συχνά χρησιμοποιούμενα συμβόλαια. Από την άλλη πλευρά, τα Minting Polcies που προορίζονται να εκτελεστούν μόνο μία φορά μπορούν να ενσωματωθούν στη συναλλαγή που εξαργυρώνει το token και στη συνέχεια να απορριφθούν, καθώς δεν χρειάζονται πλέον.

Συνοπτικά, το μοντέλο Extended UTxO προσφέρει ένα ισχυρό πλαίσιο για την επικύρωση συναλλαγών, την ανάπτυξη έξυπνων συμβολαίων Validator και Minting Polcies, βελτιστοποιώντας τόσο την υπολογιστική αποδοτικότητα όσο και την αποθήκευση. Πρόκειται για ένα παράδειγμα που ευθυγραμμίζεται καλά με τις αρχές των κλιμακούμενων, ασφαλών και αποδοτικών συστημάτων blockchain.

2.3 Αποκεντρωμένες εφαρμογές(dApps)

Τι είναι τα dApps; Οι αποκεντρωμένες εφαρμογές, κοινώς γνωστές ως dApps, είναι μια πρωτοποριακή μορφή συστημάτων λογισμικού που ενισχύονται από την τεχνολογία blockchain. Σε αντίθεση με τις παραδοσιακές εφαρμογές που εκτελούνται σε κεντρικούς διακομιστές, τα dApps λειτουργούν σε ένα δίκτυο peer-to-peer (P2P). Αυτή η αποκέντρωση δεν είναι απλώς μια τεχνική αλλαγή, είναι ένας τρόπος που επαναπροσδιορίζει τον τρόπο με τον οποίο δομούνται και λειτουργούν οι εφαρμογές. Το χαρακτηριστικό της αμετάβλητης λειτουργίας της αλυσίδας μπλοκ είναι θεμελιώδες για αυτές τις εφαρμογές. Αυτή η αμεταβλητότητα διασφαλίζει ότι μόλις καταγραφούν τα δεδομένα, δεν μπορούν να τροποποιηθούν χωρίς να τροποποιηθούν όλα τα επόμενα μπλοκ, παρέχοντας έτσι ένα ισχυρό επίπεδο ασφάλειας.

Ενώ η αρχική εφαρμογή-φαινόμενο της αλυσίδας μπλοκ ήταν, αναμφίβολα, τα κρυπτονομίσματα, οι πραγματικές δυνατότητες της τεχνολογίας αλυσίδας μπλοκ βρίσκονται πολύ πέρα από τα ψηφιακά νομίσματα. Οι αποκεντρωμένες εφαρμογές προσφέρουν ένα πιο ασφαλές, διαφανές και ανοικτού κώδικα περιβάλλον για τους χρήστες. Εξυπηρετούν πολλαπλούς σκοπούς, από τις χρηματοοικονομικές συναλλαγές και τα έξυπνα συμβόλαια έως τους αποκεντρωμένους αυτόνομους οργανισμούς (DAOs) και πέραν αυτών.

Θα πρέπει να σημειωθεί ότι οι αποκεντρωμένες εφαρμογές έχουν επίσης τις δικές τους προκλήσεις και τρωτά σημεία. Ένα τέτοιο ζήτημα περιλαμβάνει το πρόβλημα των Βυζαντινών Στρατηγών, ένα πρόβλημα συγχρονισμού δεδομένων σε κατανεμημένα συστήματα [12], όταν προσπαθούν να επιτύχουν συναίνεση μεταξύ δυνητικά αναξιόπιστων ή κακόβουλων κόμβων του δικτύου. Θα πρέπει να σημειωθεί, ωστόσο, ότι τα περισσότερα πρωτόκολλα blockchain εφαρμόζουν αλγόριθμους συναίνεσης που έχουν σχεδιαστεί για να μετριάσουν αυτό ακριβώς το πρόβλημα.

2.4 Πρωτόκολλο IPFS

Καθώς όλο και περισσότερα dApps αναδύονται, η ανάγκη για αποθήκευση δεδομένων εκτός αλυσίδας είναι ένα επαναλαμβανόμενο θέμα. Ενώ η αλυσίδα μπλοκ υπερέχει στη διασφάλιση της ακεραιότητας των δεδομένων μέσω της αρχής της αμεταβλητότητας και της εδραίωσης της εμπιστοσύνης, δεν είναι κατάλληλο μέρος για την αποθήκευση μεγάλου όγκου δεδομένων. Σε αυτό το σημείο μπαίνει στο παιχνίδι το Διαπλανητικό Σύστημα Αρχείων

(IPFS) [13], το οποίο προσφέρει μια ισχυρή λύση που ευθυγραμμίζεται καλά με την αποκεντρωμένη φύση της αλυσίδας μπλοκ

Το IPFS, το οποίο σχεδιάστηκε από τον Juan Benet, είναι ένα κατανεμημένο σύστημα αρχείων peer-to-peer (P2P) που στοχεύει στη σύνδεση όλων των υπολογιστικών συσκευών με ένα ενιαίο, εκσυγχρονισμένο σύστημα αρχείων. Σε αντίθεση με το γνωστό πρωτόκολλο HTTP, όπου ένα όνομα τομέα(domain name) αντιστοιχίζεται ουσιαστικά σε μια συγκεκριμένη διεύθυνση IP που φιλοξενεί το επιθυμητό περιεχόμενο, καθιστώντας το εστιασμένο στην τοποθεσία, το IPFS υιοθετεί μια προσέγγιση εστιασμένη στο περιεχόμενο. Στο IPFS οι χρήστες αναζητούν ένα μοναδικό αναγνωριστικό περιεχομένου, συνήθως συντομογραφημένο ως CID, το οποίο ουσιαστικά είναι ένας κατακερματισμός του εν λόγω περιεχομένου. Αντί να δείχνει σε μια συγκεκριμένη διεύθυνση, το περιεχόμενο είναι αποκεντρωμένο και διανέμεται στους ομότιμους του δικτύου. Κάθε μέλος του δικτύου διατηρεί έναν κατανεμημένο πίνακα κατακερματισμού(DHT), ο οποίος απαριθμεί τις προσβάσιμες τοποθεσίες για κάθε CID. Αυτοί οι υπερσύνδεσμοι (CIDs) και τα δεδομένα στα οποία παραπέμπουν σχηματίζουν ένα Merkle DAG, μια δομή δεδομένων που επιτρέπει την αποτελεσματική αποθήκευση και ανάκτηση δεδομένων σε ένα αποκεντρωμένο δίκτυο [13].

Γιατί χρησιμοποιείται το IPFS στα δΑππς; Το IPFS (InterPlanetary File System) είναι κάτι περισσότερο από ένα απλό σύστημα διανομής αρχείων σε πολλούς υπολογιστές, συνδυάζει πολλά προηγμένα χαρακτηριστικά για να δημιουργήσει μια ισχυρή και ευέλικτη πλατφόρμα για την αποκεντρωμένη αποθήκευση και ανάκτηση δεδομένων. Τα στοιχεία του διασφαλίζουν ότι το IPFS είναι ανθεκτικό σε μεμονωμένα σημεία αποτυχίας και εξαλείφουν την ανάγκη να εμπιστεύονται οι κόμβοι ο ένας τον άλλον. Πρόκειται για ένα στιβαρό σύστημα που έχει ήδη βρει εφαρμογές σε διάφορους τομείς, συμπεριλαμβανομένης της τεχνολογίας blockchain [14].

Κεφάλαιο 3

Σχετική εργασία

3.1 Book.io

Το Book.io παρουσιάζει μια συναρπαστική μελέτη περίπτωσης για την εφαρμογή της τεχνολογίας blockchain στην ιδιοκτησία ψηφιακών περιουσιακών στοιχείων, συγκεκριμένα στο πεδίο των ψηφιακών βιβλίων (eBooks και Audiobooks) [15]. Σε αντίθεση με τις παραδοσιακές πλατφόρμες ψηφιακών βιβλίων, όπου οι καταναλωτές αγοράζουν μια ¨άδεια πρόσβασης στο περιεχόμενο¨ αντί να κατέχουν το πραγματικό περιεχόμενο, το Book.io εισάγει την έννοια των αποκεντρωμένων κρυπτογραφημένων περιουσιακών στοιχείων (DEAs). Αυτά τα DEAs παραχωρούν πραγματική κυριότητα των ψηφιακών βιβλίων στους καταναλωτές, επιτρέποντάς τους να πωλούν, να δανείζουν ή να χαρίζουν τα ψηφιακά τους βιβλία. Η πλατφόρμα τους χρησιμοποιεί μια τεχνολογική αρχιτεκτονική δύο επιπέδων:

- Το αποκρυπτογραφημένο κρυπτογραφημένο περιουσιακό στοιχείο (DEA), το οποίο αντιπροσωπεύει το πραγματικό κρυπτογραφημένο ψηφιακό βιβλίο
- Το $BOOK Token, το οποίο χρησιμεύει ως μάρκα χρησιμοποίησης και πιστότητας του οικοσυστήματος.

Τα DEAs αποτελούν σημαντική πρόοδο σε σχέση με τα παραδοσιακά Non-Fungible Tokens (NFTs). Σε αντίθεση με τα βασικά NFTs που απλώς παραπέμπουν σε μια εικόνα ή ένα αρχείο, τα DEAs στο Book.io είναι πλήρως κρυπτογραφημένα και αποθηκεύονται σε αποκεντρωμένο χώρο αποθήκευσης, διασφαλίζοντας ότι μόνο ο ιδιοκτήτης μπορεί να έχει πρόσβαση στο περιεχόμενο. Αυτό το χαρακτηριστικό ευθυγραμμίζεται στενά με τις πτυχές της ιδιοκτησίας δεδομένων και της κρυπτογράφησης της αγοράς μας για την πώληση δεδομένων, αν και εφαρμόζεται σε διαφορετικό τομέα. Επιπλέον, το Book.io εισάγει ένα native token $BOOK για να δώσει κίνητρα για ανάγνωση, προσφέροντας μια μοναδική προοπτική για το πώς τα tokens μπορούν να προωθήσουν τη δέσμευση των χρηστών και να προσθέσουν αξία στα ψηφιακά περιουσιακά στοιχεία. Αυτός ο μηχανισμός κινήτρων που βασίζεται σε τοκεν θα μπορούσε να προσφέρει ιδέες για την ενίσχυση της συμμετοχής των χρηστών σε αγορές πώλησης δεδομένων.

Συνοψίζοντας, το Book.io αποτελεί ένα διδακτικό παράδειγμα για το πώς η τεχνολογία blockchain μπορεί να φέρει επανάσταση στην ιδιοκτησία ψηφιακών περιουσιακών στοιχείων και στην κινητοποίηση των χρηστών. Η καινοτόμος χρήση των DEAs και των κινήτρων που

βασίζονται σε tokens παρέχει πολύτιμα διδάγματα για την ανάπτυξη και την τελειοποίηση των αγορών πώλησης δεδομένων που βασίζονται στην αλυσίδα μπλοκ.

3.2 JPG Store

Το JPG Store αναδεικνύεται ως μια πρωτοποριακή αγορά για Non-Fungible Tokens (NFTs) στην αλυσίδα μπλοκ Cardano, εισάγοντας καινοτόμα χαρακτηριστικά που παιχνιδοποιούν τις αλληλεπιδράσεις των χρηστών και τις συναλλαγές τους. Η πλατφόρμα είναι ένα οικοσύστημα που καλύπτει ένα ευρύ φάσμα ψηφιακών έργων τέχνης και δημιουργιών, το οποίο ανταμείβει την ενεργό συμμετοχή μέσω των Πόντων Εμπειρίας (XP) και του native token τους $JPG.

Το token $JPG εξυπηρετεί πολλαπλούς σκοπούς εντός του οικοσυστήματος. Λειτουργεί ως ανταμοιβή για τους πιστούς χρήστες και προσφέρει διάφορα οφέλη, όπως μειωμένα τέλη συναλλαγών και προτεραιότητα στην κοπή. Αυτό το token πολλαπλών χρήσεων θα μπορούσε να παρέχει πληροφορίες για το πώς θα μπορούσε να εφαρμοστεί ένα παρόμοιο token σε μια αγορά πώλησης δεδομένων για την παροχή κινήτρων στους παρόχους και τους καταναλωτές δεδομένων.

Το JPG Store έχει επίσης υποβληθεί σε πολλαπλές αναβαθμίσεις έξυπνων συμβολαίων για τη βελτίωση της εμπειρίας των χρηστών και της ασφάλειας. Η πιο πρόσφατη αναβάθμιση επικεντρώνεται στις επιδόσεις, επιτρέποντας μαζικές αγορές έως και 52 περιουσιακών στοιχείων σε μία μόνο συναλλαγή. Αυτό είναι ιδιαίτερα σημαντικό για την αγορά πώλησης δεδομένων, όπου οι αποτελεσματικές και ασφαλείς συναλλαγές είναι ζωτικής σημασίας.

Το JPG Store χρησιμοποιεί επίσης ένα σύστημα διπλής επικύρωσης για το χειρισμό των ¨αιτήσεων¨ και των ¨προσφορών¨, όροι δανεισμένοι από την παραδοσιακή χρηματοδότηση. Το σύστημα διπλού επικυρωτή στο JPG Store έχει σχεδιαστεί για τη βελτιστοποίηση της αποτελεσματικότητας και της ασφάλειας των συναλλαγών. Αυτή η τεχνολογία θα μπορούσε να προσφέρει πολύτιμες γνώσεις για την αγορά μας, όπου υπάρχουν παρόμοιες προκλήσεις σχετικά με την ταχύτητα και την ασφάλεια των συναλλαγών.

Συνοπτικά, τα καινοτόμα χαρακτηριστικά και οι μηχανισμοί του παρέχουν πολύτιμες πληροφορίες που θα μπορούσαν να εφαρμοστούν για την ενίσχυση της δέσμευσης των χρηστών και της αποτελεσματικότητας των συναλλαγών σε αγορές πώλησης δεδομένων με βάση την αλυσίδα μπλοκ.

Μέρος II

Μεθολογία και Υλοποίηση

Κεφάλαιο 4

Μεθοδολογία και αρχιτεκτονική συστήματος

Η αρχιτεκτονική αυτού του έργου είναι μια ενορχήστρωση διαφόρων στοιχείων: μια επέκταση του προγράμματος περιήγησης, ένα dApp Next.js με δυνατότητες τόσο στο front-end όσο και στο back-end και τρεια έξυπνα συμβόλαια Plutus - δύο Validators και ένα Minting Policy. Επιπλέον, το InterPlanetary File System (IPFS) χρησιμοποιείται για την αποθήκευση των δεδομένων και μία βάση δεδομένων ζεύγους κλειδιού-τιμής(Redis) χρησιμοποιείται από το back-end.

4.1 Επισκόπηση του δΑπп

Το σύστημα φιλοξενεί δύο τύπους φορέων: Πωλητές και Αγοραστές. Ο Πωλητής είναι ένα άτομο που έχει ως στόχο να εκμεταλλευτεί τα δεδομένα περιήγησής του και τα προσωπικά του δεδομένα πουλώντας τα. Από την άλλη πλευρά, ένας αγοραστής είναι μια οντότητα ή ένα άτομο που ενδιαφέρεται να αγοράσει τέτοια δεδομένα για αναλυτικούς ή άλλους σκοπούς.

Στην αρχιτεκτονική αυτής της αποκεντρωμένης αγοράς, υπάρχουν δύο πρωταρχικοί μηχανισμοί συναλλαγών που διευκολύνουν την ανταλλαγή μεταξύ ενός πωλητή και ενός αγοραστή: οι ροές "Ask" και "Bid".

1. Ask Flow: Σε αυτό το μοντέλο, ο πωλητής αναλαμβάνει την πρωτοβουλία κλειδώνοντας ένα συγκεκριμένο token σε ένα έξυπνο συμβόλαιο. Το token ουσιαστικά "εισάγεται" με μια προκαθορισμένη τιμή μέσα στο Datum του. Αυτό θέτει τις βάσεις για τους αγοραστές να ανταποκριθούν σε αυτή την τιμή προκειμένου να ξεκλειδώσουν και να αποκτήσουν το token. Το έξυπνο συμβόλαιο DataListing validator διασφαλίζει ότι το token κρατείται με ασφάλεια μέχρι να επιτευχθεί η ζητούμενη τιμή, οπότε το token μεταβιβάζεται στον αγοραστή και το συμφωνηθέν ποσό αποστέλλεται στον πωλητή.

2. Bid Flow: Σε αντίθεση με τη ροή ζήτησης, στο μοντέλο προσφορών οι αγοραστές δίνουν το έναυσμα. Εδώ, οι αγοραστές μπορούν να υποβάλλουν προσφορές για τα tokens που τους ενδιαφέρουν. Η προσφορά αποτελείται από ένα συγκεκριμένο ποσό ADA που ο αγοραστής είναι διατεθειμένος να πληρώσει για το token. Οι πωλητές μπορούν να περιηγηθούν σε αυτές τις προσφορές που γίνονται για τα token τους και να επιλέξουν να αποδεχτούν όσες ανταποκρίνονται στην αποτίμησή τους για το token. Μετά την αποδοχή, το έξυπνο συμβόλαιο εγγυάται την άμεση ανταλλαγή του token και του ποσού της προσφοράς μεταξύ του πωλητή και του αγοραστή.

Και οι δύο ροές προσφέρουν μοναδικά πλεονεκτήματα και απευθύνονται σε διαφορετικές εμπορικές προτιμήσεις, δημιουργώντας έτσι μια ευέλικτη και δυναμική αγορά.

Στοιχεία του συστήματος:

1. Επέκταση προγράμματος περιήγησης: Αυτή η επέκταση καταγράφει τα δεδομένα περιήγησης του χρήστη. Ο χρήστης εισάγει τη διεύθυνση του πορτοφολιού του και επιλέγει τη διάρκεια για την οποία θέλει να καταγράψει το ιστορικό περιήγησής του. Επί του παρόντος, τα δεδομένα που συλλαμβάνονται περιορίζονται σε άμεσες επισκέψεις - URLs που έχουν εισαχθεί ρητά από τον χρήστη. Ωστόσο, το API του Chrome προσφέρει την ευελιξία να καταγράψει ένα πιο πλούσιο σύνολο δεδομένων στο μέλλον.

2. Έξυπνα συμβόλαια: Το σύστημα χρησιμοποιεί τρία έξυπνα συμβόλαια. Το πρώτο είναι ένα Minting Policy για τη δημιουργία μοναδικών token "DataToken". Το δεύτερο και η τρίτο είναι έξυπνα συμβόλαια Validators, ένα για το χειρισμό των Asks(DataListing) και το άλλο για τα Bids. Αυτά τα συμβόλαια εξασφαλίζουν ασφαλείς και δίκαιες συναλλαγές μεταξύ Πωλητών και Αγοραστών και περιλαμβάνουν επίσης έναν μηχανισμό ¨Ακύρωσης¨ και για τα δύο μέρη.

3. Back-end Server: (NodeJS), ο back-end διακομιστής της αγοράς κατασκευάζεται χρησιμοποιώντας το API του Next.js. Κρυπτογραφεί τα δεδομένα που λαμβάνονται από την επέκταση και τα αποθηκεύει στο δίκτυο IPFS. Χειρίζεται επίσης τα μεταδεδομένα του token, τα οποία είναι ζωτικής σημασίας για την ανάκτηση δεδομένων και την αποκρυπτογράφηση για τον αγοραστή.

4. Η διεπαφή χρήστη είναι επίσης γραμμένη σε TypeScript, αναπτύσσεται με τη χρήση του Next.js και διαμορφώνεται με το Tailwind CSS. Χρησιμεύει ως κόμβος για όλο τον εκτός αλυσίδας κώδικα, τον χειρισμό συναλλαγών, τον εντοπισμό των απαραίτητων UTxOs και tokens, και την υποβολή συναλλαγών στο δίκτυο. Η βιβλιοθήκη lucid-cardano χρησιμοποιείται για τη διευκόλυνση αυτών των λειτουργιών. Η διεπαφή χωρίζεται σε 2 πρωταρχικές προβολές, η μία σχεδιασμένη για τον πωλητή και η άλλη για τον αγοραστή.

Με την ενσωμάτωση αυτών των στοιχείων, το σύστημα προσφέρει μια ολοκληρωμένη λύση για την ασφαλή και αποτελεσματική αγορά και πώληση δεδομένων χρηστών.

4.2 Επέκταση προγράμματος περιήγησης

Μια επέκταση προγράμματος περιήγησης γράφεται ουσιαστικά με τις ίδιες τεχνολογίες ιστού που χρησιμοποιούνται για τη δημιουργία μιας εφαρμογής ιστού, όπως η HTML, η CSS και η JavaScript. Ωστόσο, αυτό που την κάνει να ξεχωρίζει είναι η ικανότητά της να έχει πρόσβαση σε εξειδικευμένα API του προγράμματος περιήγησης, όπως το API του Chrome για την επέκταση Google Chrome.

Επιπλέον, η Πολιτική Ασφάλειας Περιεχομένου (CSP) στις επεκτάσεις του προγράμματος περιήγησης προσθέτει ένα επιπλέον επίπεδο πολυπλοκότητας σε σύγκριση με την παραδοσιακή ανάπτυξη ιστοσελίδων [16]. Για παράδειγμα, η προεπιλεγμένη CSP περιορίζει τις

επεκτάσεις να φορτώνουν μόνο τοπικά σενάρια και αντικείμενα, απαγορεύοντας την inline JavaScript και την αξιολόγηση συμβολοσειρών ως εκτελέσιμο κώδικα. Αυτό σημαίνει ότι κοινές λειτουργίες JavaScript όπως η eval() είναι εκτός ορίων, και το ίδιο ισχύει και για οποιεσδήποτε βιβλιοθήκες που βασίζονται σε τέτοιες λειτουργίες. Αυτοί οι περιορισμοί έχουν σχεδιαστεί για να ενισχύσουν την ασφάλεια, αλλά μπορεί να δημιουργήσουν προκλήσεις κατά την ανάπτυξη, απαιτώντας μια πιο προσεκτική προσέγγιση για την ενσωμάτωση και την εκτέλεση σεναρίων. Τα πιο βασικά συστατικά μιας επέκτασης προγράμματος περιήγησης [17, 18] είναι:

1. Το manifest: Ο ακρογωνιαίος λίθος οποιασδήποτε επέκτασης είναι το αρχείο manifest, το οποίο ονομάζεται βολικά manifest.json. Τοποθετημένο στο ριζικό φάκελο, αυτό το αρχείο χρησιμεύει ως το σχέδιο για την επέκταση, με λεπτομερή περιγραφή των μεταδεδομένων της, των δικαιωμάτων και των αρχείων που χρειάζεται για να εκτελεστεί τόσο στο παρασκήνιο όσο και σε ιστοσελίδες. Πρόκειται ουσιαστικά για ένα αρχείο ρυθμίσεων που καθορίζει την αρχιτεκτονική και τα στοιχεία μιας επέκτασης.

2. Service worker: Ενεργώντας ως διαχειριστής συμβάντων της επέκτασης, ο Service worker ακούει για διάφορα συμβάντα του προγράμματος περιήγησης, όπως η δημιουργία καρτελών ή η αφαίρεση σελιδοδεικτών. Παρόλο που μπορεί να αξιοποιήσει όλα τα API του Chrome, δεν μπορεί να χειριστεί άμεσα το περιεχόμενο της ιστοσελίδας.

3. Content Scripts: Αυτά τα σενάρια εκτελούν JavaScript στο πλαίσιο οποιασδήποτε ιστοσελίδας που επισκέπτονται, επιτρέποντάς τους να διαβάζουν και να τροποποιούν το DOM. Παρόλο που μπορούν να χρησιμοποιήσουν μόνο ένα υποσύνολο των API του Chrome, μπορούν να έχουν έμμεση πρόσβαση σε όλο το φάσμα ανταλλάσσοντας μηνύματα με τον εργάτη υπηρεσίας.

4. Popup και άλλες σελίδες HTML: Οι επεκτάσεις μπορούν να περιλαμβάνουν διάφορα αρχεία HTML, όπως το Popup ή η σελίδα ρυθμίσεων της. Αυτές χρησιμεύουν ως η κύρια διεπαφή χρήστη για την αλληλεπίδραση με την επέκταση και μπορούν να έχουν πρόσβαση σε μερικά API του Chrome.

Manifest V3 Το Manifest V3 χρησιμεύει ως το πιο ενημερωμένο πλαίσιο για επεκτάσεις του Chrome, προσφέροντας βελτιώσεις στην ασφάλεια, το απόρρητο και την απόδοση. Επιτρέπει επίσης τη χρήση σύγχρονων τεχνολογιών ιστού, όπως service workers και promises. Το αρχείο manifest είναι καθοριστικής σημασίας, καθώς περιγράφει τις δυνατότητες και τα απαιτούμενα δικαιώματα της επέκτασης, τα οποία παρουσιάζονται στον χρήστη κατά την εγκατάσταση. Οι επεκτάσεις λειτουργούν σε περιβάλλον sandboxed, περιορίζοντας την πρόσβαση μόνο στους απαραίτητους πόρους.

Το αναδυόμενο στοιχείο(Popup) ενεργεί ως η κύρια διεπαφή χρήστη και εμφανίζεται όταν γίνεται κλικ στο εικονίδιο της επέκτασης. Είναι περιορισμένο, καθώς δεν μπορεί να συνεργαστεί με το DOM της ιστοσελίδαςή να αλληλεπιδράσει με άλλες επεκτάσεις.

Από την άλλη πλευρά, το Content Script έχει τη δυνατότητα χειρισμού του περιεχομένου μιας ιστοσελίδας, αλλά δεν έχει πρόσβαση στο API του Chrome.

Οι service workers λειτουργούν ως σενάρια παρασκηνίου, ενορχηστρώνουν διάφορες δραστηριότητες επέκτασης και ανταποκρίνονται σε συμβάντα του προγράμματος περιήγησης. Αν και δεν μπορούν να αλληλεπιδράσουν με το DOM, χρησιμεύουν ως διαχειριστής συμβάντων της επέκτασης, ακούγοντας συμβάντα όπως η δημιουργία νέας καρτέλας, η προσθήκη σελιδοδεικτών ή τα κλικ στο εικονίδιο της επέκτασης.

Κάθε συστατικό της επέκτασης έχει τα δικά του πλεονεκτήματα και μειονεκτήματα. Για την πλήρη αξιοποίηση των δυνατοτήτων και των λειτουργιών της επέκτασης, αυτά τα συστατικά πρέπει να αλληλεπιδρούν συντονισμένα μεταξύ τους. Αυτή η αλληλεπίδραση ενορχηστρώνεται μέσω της διακίνησης μηνυμάτων, που απηχεί στις αρχές μιας αρχιτεκτονικής που βασίζεται σε γεγονότα(event-driven). Το αναδυόμενο παράθυρο, για παράδειγμα, μπορεί να συλλάβει ένα γεγονός που ενεργοποιείται από τον χρήστη και να μεταδώσει ένα αντίστοιχο μήνυμα. Αυτό το μήνυμα μπορεί στη συνέχεια να υποκλαπεί από έναν service worker για σκοπούς αποθήκευσης δεδομένων ή από ένα Content Script για την τροποποίηση του περιεχομένου της ιστοσελίδας.

4.3 NextJS dApp

Καθώς ο κόσμος των αποκεντρωμένων εφαρμογών (dApps) συνεχίζει να εξελίσσεται, η ανάγκη για ευέλικτα και κλιμακούμενα πλαίσια γίνεται ολοένα και πιο εμφανής. Το Next.js, ένα κορυφαίο πλαίσιο απόδοσης από την πλευρά του διακομιστή (SSR) για τη React που προσφέρει μια συναρπαστική λύση για την ανάπτυξη dApp.

Ενοποιημένη βάση κώδικα Ένα από τα ιδιαίτερα χαρακτηριστικά του Next.js είναι η ικανότητά του να φιλοξενεί τη λογική τόσο του frontend όσο και του backend στην ίδια βάση κώδικα. Αυτή η συνεγκατάσταση απλοποιεί τις ροές εργασίας ανάπτυξης και βελτιώνει τη συντηρησιμότητα του κώδικα. Επιτρέπει στους προγραμματιστές να γράφουν διαδρομές API και συναρτήσεις από την πλευρά του διακομιστή παράλληλα με τα στοιχεία της React, βελτιώνοντας τη διαδικασία ανάπτυξης και μειώνοντας την εναλλαγή περιβάλλοντος.

Τεχνολογίες frontend Το frontend του dApp έχει κατασκευαστεί με τη χρήση της React, μιας δημοφιλούς βιβλιοθήκης για την κατασκευή διεπαφών χρήστη. Διαμορφώνεται με τη χρήση του Tailwind CSS, ενός πλαισίου CSS με γνώμονα τη χρησιμότητα, το οποίο παρέχει έτοιμες προς χρήση κλάσεις css. Η διαχείριση της κατάστασης και του πλαισίου γίνεται με το ενσωματωμένο Context API του React, εξασφαλίζοντας αποτελεσματική ροή δεδομένων και χειρισμό της κατάστασης σε όλα τα στοιχεία.

Δρομολόγια API στο backend Το backend είναι δομημένο ως ένα σύνολο δρομολογίων API, καθένα από τα οποία εξυπηρετεί μια συγκεκριμένη λειτουργία. Αυτές οι διαδρομές έχουν τη δυνατότητα να αλληλεπιδρούν με διάφορες υπηρεσίες, συμπεριλαμβανομένου του IPFS για αποκεντρωμένη αποθήκευση και ενός συστήματος αποθήκευσης για τα μεταδεδομένα των token.

Μηχανισμοί εξουσιοδότησης Η ασφάλεια αποτελεί ύψιστο μέλημα, ειδικά στο πλαίσιο των dApps. Οι διαδρομές API του backend χρησιμοποιούν διάφορους μηχανισμούς εξουσιοδότησης για την επικύρωση των αιτήσεων που προέρχονται από την πλευρά του πελάτη. Αυτό διασφαλίζει ότι μόνο πιστοποιημένοι χρήστες μπορούν να εκτελέσουν ορισμένες ενέργειες, προσθέτοντας ένα επιπλέον επίπεδο ασφάλειας στο σύστημα.

Server-Side Rendering και React Το Next.js πηγαίνει τη δύναμη της React ένα βήμα παραπέρα, προσφέροντας server-side rendering. Αυτό το χαρακτηριστικό ενισχύει την απόδοση και το SEO των εφαρμογών ιστού, μια κρίσιμη πτυχή που συχνά παραβλέπεται στο πεδίο των dApps. Με το SSR, το αρχικό περιεχόμενο HTML δημιουργείται στον διακομιστή, μειώνοντας τον χρόνο για το "first paint" και βελτιώνοντας την εμπειρία του χρήστη

Υποστήριξη της TypeScript Η TypeScript, ένα υπερσύνολο της JavaScript, προσθέτει στατικούς τύπους στη γλώσσα, διευκολύνοντας τον εντοπισμό σφαλμάτων κατά τη διάρκεια της ανάπτυξης και όχι κατά την εκτέλεση. Η ενσωμάτωση της TypeScript σε ένα έργο Next.js είναι απρόσκοπτη, απαιτώντας μόνο ένα απλό αρχείο ρυθμίσεων.

Με την υιοθέτηση αυτής της αρχιτεκτονικής, το dApp του Next.js επιτυγχάνει ένα αρμονικό μείγμα ικανότητας κλιμάκωσης, επιδόσεων και ασφάλειας, καθιστώντας την κατάλληλη για σύγχρονες αποκεντρωμένες εφαρμογές.

4.4 Έξυπνα συμβόλαια Plutus

Η αρχιτεκτονική των έξυπνων συμβολαίων έχει σχεδιαστεί με ακρίβεια και σκοπιμότητα, ενσωματώνοντας τη βασική λογική και τις αλληλεπιδράσεις που λαμβάνουν χώρα στην αγορά.

Data Token Minting Policy Πρόκειται για ένα παραμετροποιημένο έξυπνο συμβόλαιο κοπής, το οποίο, όπως υποδηλώνει ο τύπος του έξυπνου συμβολαίου, είναι υπεύθυνο για την κοπή των "DataTokens", που χρησιμοποιούνται για την αναπαράσταση και τη μετέπειτα πρόσβαση στα αποθηκευμένα δεδομένα ιστορικού περιήγησης ενός χρήστη. Μόλις παραμετροποιηθεί με ένα από τα διαθέσιμα UTxO του πωλητή, το συμβόλαιο παράγει μια συγκεκριμένη διεύθυνση Minting Policy, παραχωρώντας αποκλειστικά δικαιώματα νομισματοκοπίας στον συγκεκριμένο πωλητή. Σημαντικό είναι ότι πρόκειται για μια εφάπαξ λειτουργία- μετά την αρχική νομισματοκοπία, το UTXO εξαντλείται, καθιστώντας το άχρηστο για μελλοντική νομισματοκοπία.

Έξυπνο συμβόλαιο DataListing Το έξυπνο συμβόλαιο DataListing validator υλοποιεί τη ροή "Ask" στο μοντέλο προσφοράς-ζήτησης της αγοράς. Ορίζει μια δομή Datum που κωδικοποιεί τον κατακερματισμό του δημόσιου κλειδιού του πωλητή (PubKeyHash) και τη ζητούμενη τιμή σε lovelaces. Το συμβόλαιο αναγνωρίζει επίσης δύο τιμές redeemer: "Purchase" και "Redeem". Ο redeemer "Purchase" προορίζεται να χρησιμοποιηθεί από ενδιαφερόμενους δυνητικούς αγοραστές, ενώ ο redeemer "Redeem" επιτρέπει στους πωλητές να αποσύρουν την καταχώριση του DataToken τους. Τα πεδία PubKeyHash και τιμή του Datum είναι

καθοριστικά για την επικύρωση της ακεραιότητας της συναλλαγής, διασφαλίζοντας ότι ο αγοραστής έχει εκπληρώσει τις απαιτήσεις της πληρωμής.

Έξυπνο συμβόλαιο Bid Το έξυπνο συμβόλαιο επικύρωσης προσφορών είναι υπεύθυνο για τη ροή "Bid" και παραμετροποιείται από το μοναδικό αναγνωριστικό (Asset Class) ενός token. Αυτή η σχεδιαστική επιλογή ενισχύει την δυνατότητα εντοπισμού των προσφορών τόσο για τους αγοραστές όσο και για τους πωλητές, δημιουργώντας ξεχωριστές διευθύνσεις έξυπνων συμβολαίων για κάθε token. Παρακάμπτει τις υλικοτεχνικές επιπλοκές που θα προέκυπταν από ένα μονολιθικό συμβόλαιο που θα χειριζόταν όλες τις πιθανές προσφορές για όλα τα tokens. Το Datum σε αυτό το συμβόλαιο περιέχει το PubKeyHash του αγοραστή, το οποίο είναι απαραίτητο για την επαλήθευση ότι ο πωλητής μεταφέρει το token κατά τη διεκδίκηση της προσφοράς. Παρόμοια με το συμβόλαιο DataListing, το συμβόλαιο Bid έχει επίσης δύο redeemers: "Sell" και "Redeem". Ο redeemer "Sell" χρησιμοποιείται αποκλειστικά από τον ιδιοκτήτη του token (τον πωλητή), ενώ ο redeemer "Redeem" προορίζεται για τον αγοραστή.

Μέτρα ασφαλείας Κάθε έξυπνο συμβόλαιο επικυρωτή ενσωματώνει ισχυρά μέτρα ασφαλείας, συμπεριλαμβανομένης της επαλήθευσης υπογραφής, για να διασφαλιστεί ότι οι συναλλαγές έχουν εγκριθεί από τα κατάλληλα μέρη. Αυτό προσθέτει το απαραίτητο επίπεδο εμπιστοσύνης και αξιοπιστίας στην αποκεντρωμένη αρχιτεκτονική της αγοράς .

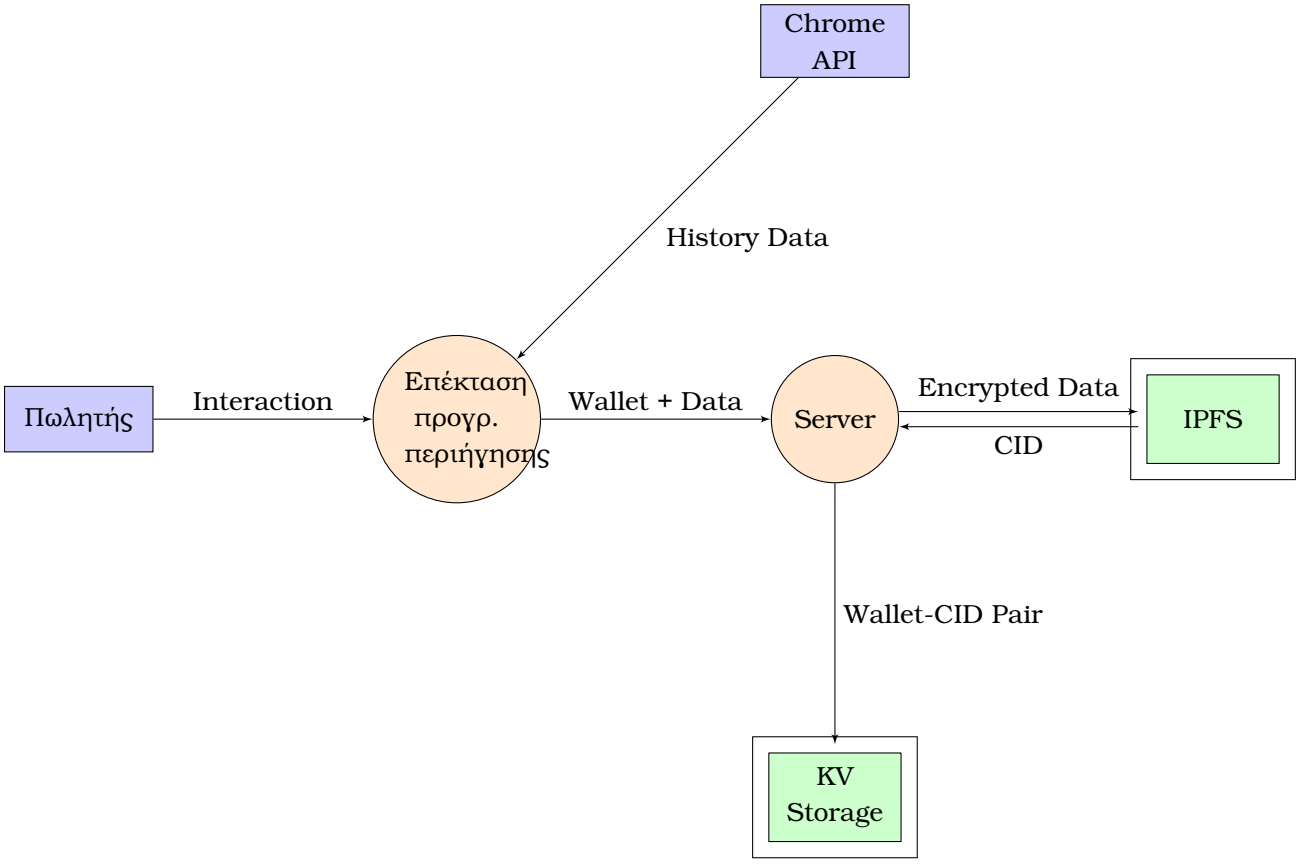
4.5 Διαγράμματα ροής δεδομένων

Τα διαγράμματα ροής δεδομένων έγιναν δημοφιλή τη δεκαετία του '70, επειδή παρέχουν έναν απλό τρόπο απεικόνισης της ροής των δεδομένων μέσω ενός συστήματος. Σε ένα DFD, υπάρχουν τέσσερα κύρια στοιχεία:

- Εξωτερική οντότητα: Αυτό το στοιχείο που αναπαρίσταται από ένα ορθογώνιο, αναφέρεται στην πηγή ή τον προορισμό των δεδομένων. Στην αρχιτεκτονική αυτού του συστήματος, οι εξωτερικές οντότητες είναι ο Πωλητής και ο Αγοραστής.
- Διαδικασία: Το στοιχείο αυτό, που αναπαρίσταται με έναν κύκλο, αναφέρεται σε μια δραστηριότητα που μετατρέπει την εισερχόμενη ροή δεδομένων σε εξερχόμενη ροή δεδομένων. Συνήθως οι διεργασίες ξεκινούν από την πάνω αριστερή πλευρά του DFD και τελειώνουν κάτω δεξιά.
- Αποθήκευση δεδομένων: Το στοιχείο αυτό, που αναπαρίσταται από δύο παράλληλες γραμμές, αναφέρεται στα δεδομένα που αποθηκεύονται στο σύστημα. Σε αυτή την αρχιτεκτονική του συστήματος, η αποθήκη δεδομένων είναι το δίκτυο IPFS και ο αποθηκευτικός χώρος key-value(KV) του διακομιστή. Θα χρησιμοποιήσουμε πράσινο χρώμα για να το αναπαραστήσουμε.
- Ροή δεδομένων: Το στοιχείο αυτό, που αναπαρίσταται με ένα βέλος, αναφέρεται στην κίνηση των δεδομένων μεταξύ εξωτερικών οντοτήτων, διεργασιών και αποθηκών δεδομένων. Οι ετικέτες περιγράφουν τον τύπο των δεδομένων που ρέουν. Ωστόσο, σε πολλά

συστήματα, ιδίως σε εκείνα που περιλαμβάνουν ανθρώπινες αλληλεπιδράσεις, όπως οι διεπαφές χρήστη, τα "δεδομένα" που μεταφέρονται μπορεί επίσης να είναι μια ενέργεια ή ένα γεγονός. Αυτό ισχύει ιδιαίτερα για τα DFD υψηλού επιπέδου (επίπεδο 0 ή επίπεδο 1), όπου οι διεργασίες μπορεί να είναι πιο αφηρημένες.

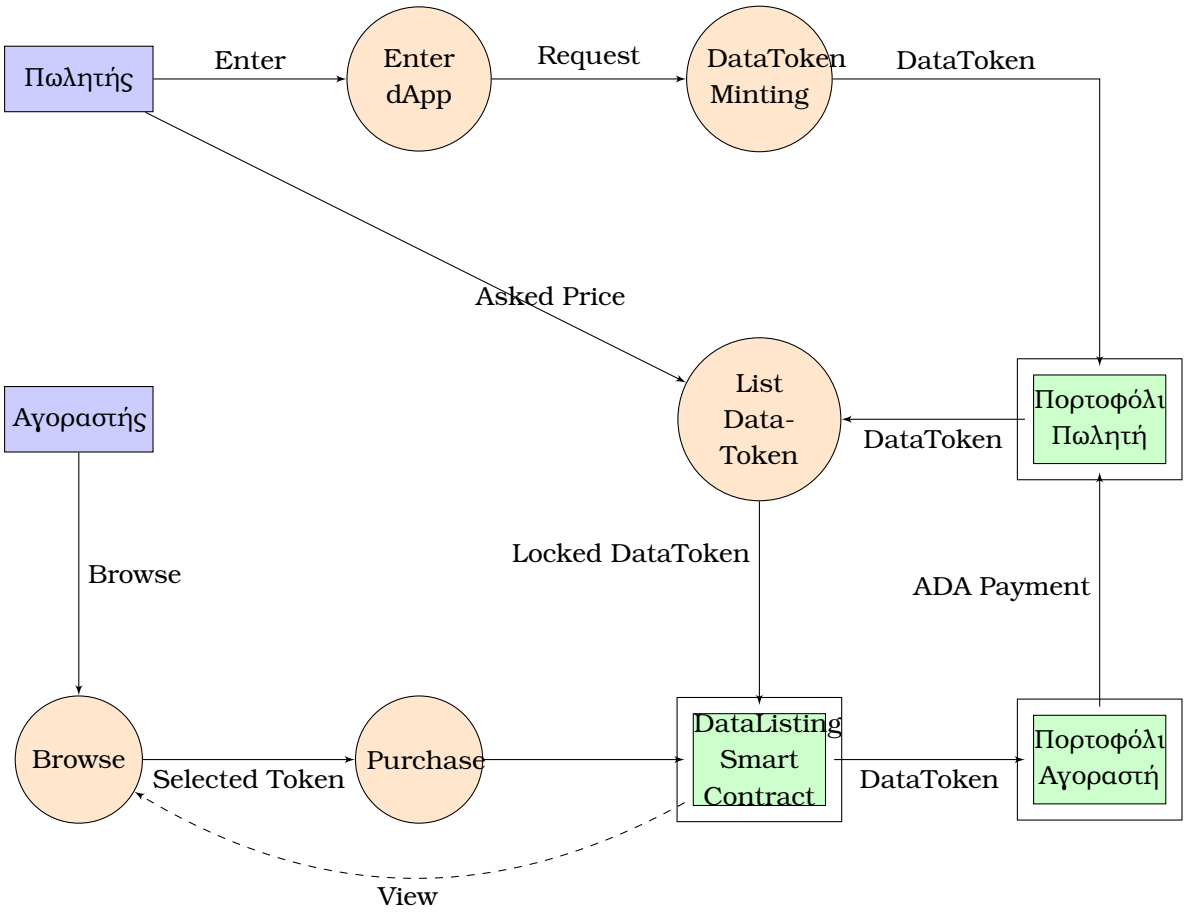
Αλληλεπίδραση του πωλητή με την επέκταση περιήγησης Στο Διάγραμμα 4.1 παρουσιάζεται η αλληλεπίδραση ενός πωλητή με την επέκταση περιήγησης και τον διακομιστή, προκειμένου να αποθηκεύσει τα δεδομένα ιστορικού περιήγησης στο IPFS. Η διεύθυνση πορτοφολιού του Πωλητή χρησιμοποιείται ως κλειδί για την αποθήκευση του CID των δεδομένων στην αποθήκη KV(Key Value) του Διακομιστή.



Σχήμα 4.1: *Διάγραμμα ροής δεδομένων της αλληλεπίδρασης ενός πωλητή με την επέκταση περιήγησης.*

Και για τις δύο ροές, ο Πωλητής εισέρχεται στη συνέχεια στο dApp και δημιουργεί ένα DataToken, το οποίο κόβεται χρησιμοποιώντας την πολιτική κοπής DataToken.

Ask Flow Στη ροή Ask Flow(Διάγραμμα 4.2), ο Πωλητής παραθέτει το DataToken προς πώληση, κλειδώνοντάς το στο πλαίσιο του έξυπνου συμβολαίου DataListing. Ο αγοραστής μπορεί να περιηγηθεί στα κλειδωμένα token και να αγοράσει όποιο τον ενδιαφέρει. Κατά την αγορά, το έξυπνο συμβόλαιο διευκολύνει την άμεση ανταλλαγή του token και της ζητούμενης τιμής μεταξύ του πωλητή και του αγοραστή.

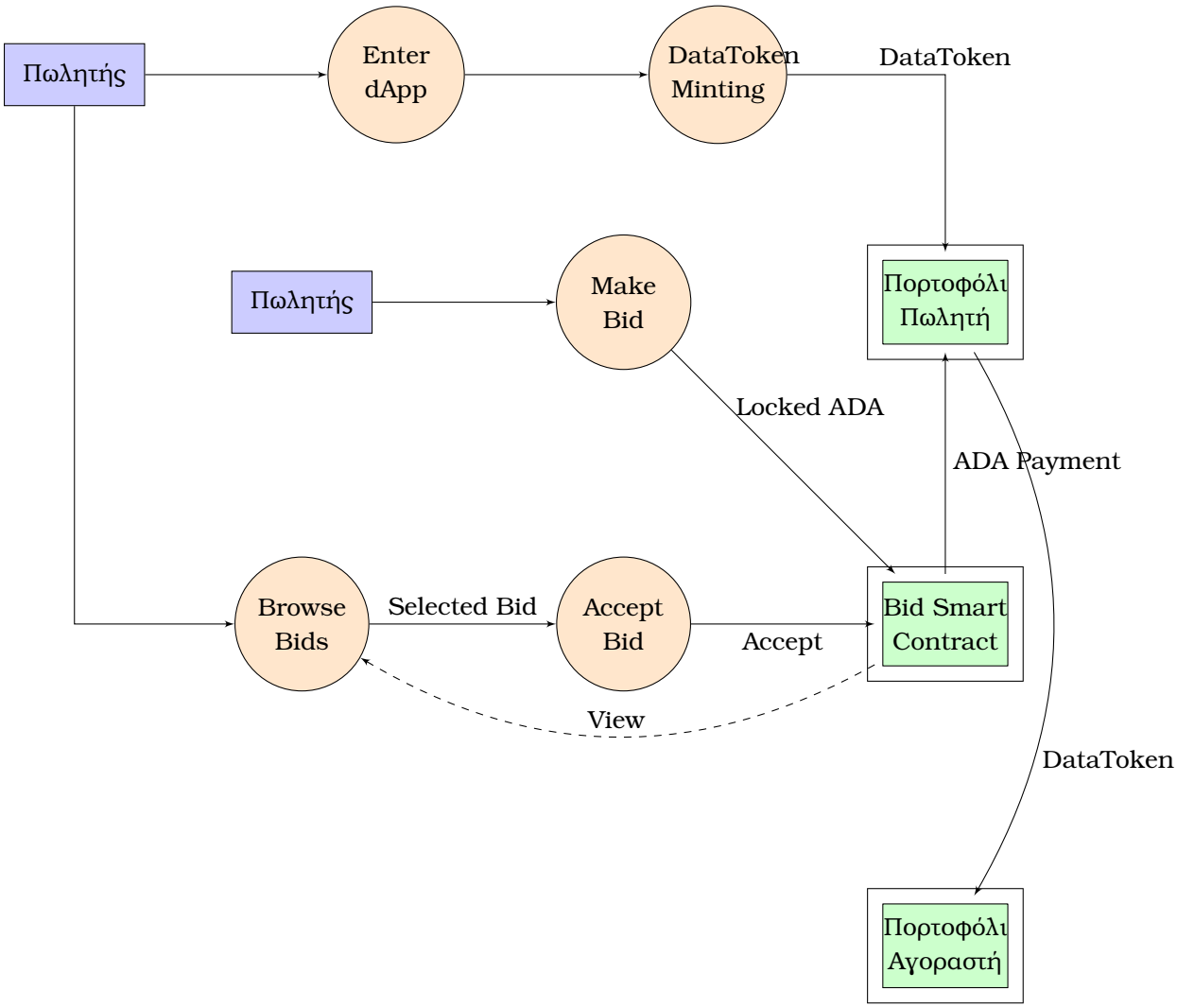


Σχήμα 4.2: *Ask Flow διαδικασία που απεικονίζει την καταχώριση και αγορά DataTokens μέσω του έξυπνου συμβολαίου DataListing.*

Bid Flow Στη ροή προσφορών Bid Flow(Διάγραμμα 4.3), ο αγοραστής μπορεί να κάνει προσφορές σε μάρκες που έχουν κοπεί από πωλητές, κλειδώνοντας την προσφορά ADA στο πλαίσιο του έξυπνου συμβολαίου προσφορών. Ο Πωλητής μπορεί να περιηγηθεί στις προσφορές που γίνονται για το DataToken του και να αποδεχτεί όποια ανταποκρίνεται στην αποτίμησή του για το token. Μετά την αποδοχή, το έξυπνο συμβόλαιο διευκολύνει την άμεση ανταλλαγή του token και του ποσού της προσφοράς μεταξύ του πωλητή και του αγοραστή. Μια σημαντική διαφορά εδώ είναι ότι το token δεν κλειδώνεται ποτέ στο πλαίσιο του έξυπνου συμβολαίου, βρίσκεται συνεχώς στην κατοχή του πωλητή, μέχρι τη στιγμή της ανταλλαγής.

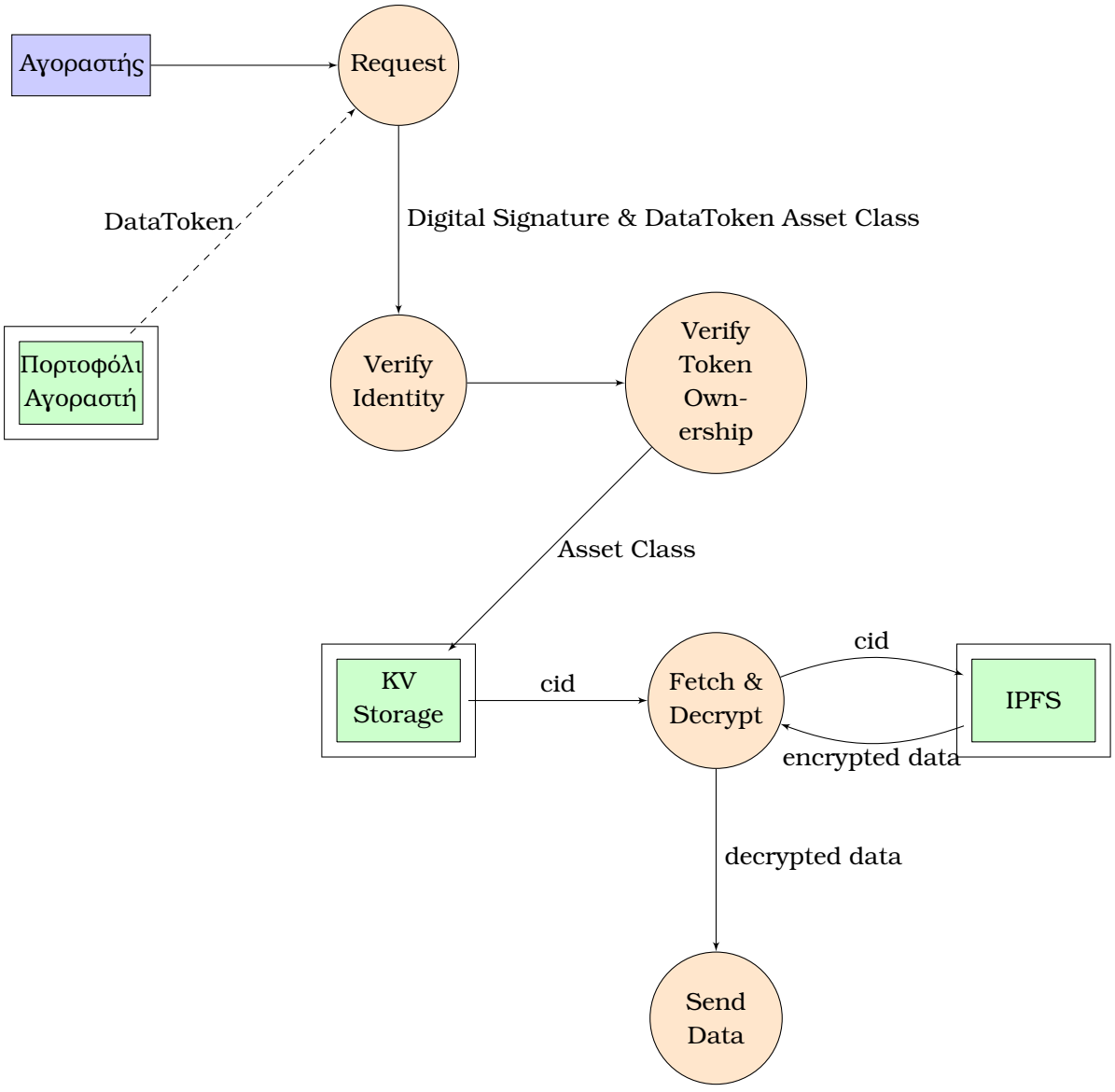
Μια λεπτή λεπτομέρεια που δεν απεικονίζεται στα διαγράμματα, είναι η δημιουργία των μεταδεδομένων εκτός αλυσίδας για κάθε κουπόνι κατά την κοπή του κουπονιού, στο KV Storage του διακομιστή. Αυτά τα μεταδεδομένα είναι ζωτικής σημασίας για να μπορεί ο αγοραστής να ανακτήσει και να αποκρυπτογραφήσει τα δεδομένα που είναι αποθηκευμένα στο IPFS, στη φάση μετά την αγορά.

Μετά την αγορά Και στις δύο ροές, ο αγοραστής που έχει αγοράσει το κουπόνι, μπορεί να προχωρήσει στη λήψη των δεδομένων που σχετίζονται με αυτό το κουπόνι.Πρέπει να στείλει μια ψηφιακή υπογραφή στον κεντρικό διακομιστή, προκειμένου να επαληθεύσει την ταυτότητά του. Στη συνέχεια, ο διακομιστής αντλεί τα κρυπτογραφημένα δεδομένα από το



Σχήμα 4.3: *Bid Flow διάγραμμα που δείχνει τη διαδικασία υποβολής προσφορών από τον αγοραστή, την αποδοχή από τον πωλητή και το ρόλο του έξυπνου συμβολαίου Bid στην ανταλλαγή DataTokens και ADA.*

IPFS, τα αποκρυπτογραφεί και τα αποστέλλει στον αγοραστή. (Διάγραμμα 4.4)



Σχήμα 4.4: *Διαδικασία μετά την αγορά που απεικονίζει τα βήματα επαλήθευσης και ανάκτησης δεδομένων του αγοραστή μετά την απόκτηση ενός DataToken.*

Κεφάλαιο 5

Υλοποίηση

5.1 Front-end Ανάπτυξη

Στην καρδιά της αρχιτεκτονικής του front-end βρίσκεται η βιβλιοθήκη lucid-cardano, ένα κεντρικό στοιχείο που διευκολύνει τις αλληλεπιδράσεις με το πορτοφόλι. Με τη συγκατάθεση του χρήστη, αυτή η βιβλιοθήκη μπορεί να έχει πρόσβαση στις πληροφορίες του πορτοφολιού και να εκτελεί συναλλαγές για λογαριασμό του χρήστη. Ενώ το πορτοφόλι Nami χρησιμεύει ως το κύριο πορτοφόλι για την παρούσα υλοποίηση, το σύστημα έχει σχεδιαστεί ώστε να είναι συμβατό με οποιοδήποτε πορτοφόλι που τηρεί το πρότυπο CIP-0030, όπως το Yoroi, το Lace ή το Eternl.

Εκτός από τις αλληλεπιδράσεις των πορτοφολιών, το Blockfrost λειτουργεί ως πάροχος υπηρεσιών blockchain. Χρησιμεύει ως μια ισχυρή εναλλακτική λύση στη λειτουργία ενός αποκλειστικού κόμβου blockchain, προσφέροντας λειτουργίες όπως η αναζήτηση συναλλαγών, η παρακολούθηση UTXO και η ανάκτηση περιεχομένου πορτοφολιού. Το Blockfrost βοηθά επίσης στην υπογραφή και κατάθεση συναλλαγών, εξαλείφοντας έτσι την ανάγκη για συνεχή συγχρονισμό ενός δικού μας κόμβου με το δίκτυο blockchain.

Το front-end χωρίζεται σε δύο κύριες διεπαφές: τη διεπαφή του πωλητή και τη διεπαφή του αγοραστή. Κάθε διεπαφή αποσκοπεί στη διευκόλυνση των δύο κύριων ροών συναλλαγών - ¨Ζήτηση¨ και ¨Προσφορά¨ - από τη σκοπιά του Πωλητή και του Αγοραστή, αντίστοιχα. Ωστόσο, πριν εμβαθύνουμε σε αυτές τις διεπαφές, είναι ζωτικής σημασίας να κατανοήσουμε τον ρόλο της επέκτασης του προγράμματος περιήγησης, που χρησιμοποιείται αποκλειστικά από τους πωλητές.

5.1.1 Επέκταση προγράμματος περιήγησης

Όσον αφορά την επέκταση του προγράμματος περιήγησης, έχει αναπτυχθεί χρησιμοποιώντας Create React App και Typescript. Δεδομένου ότι οι επεκτάσεις προγράμματος περιήγησης απαιτούν μια έξοδο δημιουργίας που περιλαμβάνει απλά αρχεία HTML, CSS και JavaScript, χρησιμοποιείται το Webpack ως bundler για την ικανοποίηση αυτής της απαίτησης. Η επέκταση ρυθμίζεται μέσω ενός αρχείου Manifest V3 JSON, το οποίο περιγράφει διάφορα σημεία εισόδου. Το πιο κρίσιμο σημείο εισόδου για αυτή τη συγκεκριμένη περίπτωση χρήσης είναι το αναδυόμενο στοιχείο, με άλλα στοιχεία όπως το contentScript, το service-worker και η σελίδα επιλογών να μην χρησιμοποιούνται ενεργά για την απαιτούμενη λειτουργικότητα της επέκτασης

Το αναδυόμενο στοιχείο διαθέτει μια φόρμα με δύο πεδία εισόδου. Το πρώτο πεδίο προορίζεται για τη διεύθυνση πορτοφολιού του χρήστη, την οποία πρέπει να εισάγει ο πωλητής για να ανακτήσει και να πουλήσει αργότερα τα δεδομένα του. Το δεύτερο πεδίο καθορίζει το χρονικό διάστημα, σε ημέρες, για το οποίο ο πωλητής επιθυμεί να συλλέξει δεδομένα ιστορικού περιήγησης- η προεπιλεγμένη ρύθμιση για αυτό είναι επτά ημέρες. Με το πάτημα του κουμπιού ¨Συλλογή¨, μια μέθοδος εντός του αναδυόμενου στοιχείου καλεί την chrome.history.search API για να συγκεντρώσει όλους τους άμεσους συνδέσμους που εισήγαγε ο χρήστης εντός του καθορισμένου χρονικού πλαισίου. Μετά από αυτή τη συλλογή δεδομένων, ο χρήστης μπορεί να κάνει κλικ στο κουμπί Ὑποβολή¨, ενεργοποιώντας την κρυπτογράφηση των δεδομένων και τη μετέπειτα αποθήκευση στο δίκτυο IPFS.

5.1.2 dApp Διεπαφή Χρήστη

Παραγωγή Τοκεν

Κατά την είσοδο στο dApp, ο πωλητής έχει τη δυνατότητα να αντλήσει όλα τα δεδομένα που σχετίζονται με το πορτοφόλι του και είναι αποθηκευμένα στο δίκτυο IPFS. Εάν δεν βρεθούν δεδομένα, μια προτροπή συμβουλεύει τον Πωλητή να χρησιμοποιήσει πρώτα την επέκταση του προγράμματος περιήγησης για τη λήψη δεδομένων. Διαφορετικά, ο Πωλητής μπορεί να προχωρήσει στην κοπή του DataToken του. Αυτή η διαδικασία δημιουργεί επίσης μεταδεδομένα εκτός αλυσίδας στον διακομιστή, τα οποία περιλαμβάνουν το CID των δεδομένων στο δίκτυο IPFS. Πρόσθετα μεταδεδομένα θα μπορούσαν να προστεθούν στο μέλλον για να παρέχουν μεγαλύτερο πλαίσιο στον αγοραστή, όπως ο τύπος των δεδομένων και ο αριθμός των ημερών που καλύπτουν.

Για την κοπή του DataToken, το UI σαρώνει το πορτοφόλι του χρήστη για ένα διαθέσιμο UTxO και το χρησιμοποιεί για την παραμετροποίηση της πολιτικής κοπής. Η προκύπτουσα τελική πολιτική κοπής(finalPolicy) χρησιμοποιείται στη συνέχεια σε μια νέα συναλλαγή για τη δημιουργία ενός μοναδικού DataToken. Μετά τη λήψη της finalPolicy, μπορούμε επίσης να λάβουμε το μοναδικό αναγνωριστικό πολιτικής της, χρησιμοποιώντας το 'lucid.utils.mintingPolicyToId(finalMintingPolicy);' Αυτό είναι ουσιαστικά το hash της τελικής παραμετροποιημένης πολιτικής νομισματοκοπίας. Συνδέοντας το Policy ID με το όνομα του token('DataToken'), λαμβάνουμε τελικά την Asset Class του token. Αυτή η μοναδική Asset Class λειτουργεί ως αναγνωριστικό για το παραγόμενο τοκεν.

Αξίζει να σημειωθεί ότι τα έξυπνα συμβόλαια Plutus σειριοποιούνται σε bytes (σε δεκαεξαδική μορφή) για να χρησιμοποιηθούν σε κώδικα εκτός αλυσίδας και να συνδεθούν με συναλλαγές.

Ask Flow

Πωλητής Αφού κόψει το DataToken του, ο Πωλητής μπορεί να το διαθέσει προς πώληση δημιουργώντας μια μεταβίβαση στη διεύθυνση συμβολαίου DataListing. Το σειριοποιημένο έξυπνο συμβόλαιο DataListing αποθηκεύεται στο React context και η διεύθυνσή του ανακτάται χρησιμοποιώντας το lucid.utils. Στη συνέχεια, ο Πωλητής δημιουργεί μια συναλλαγή με ένα δεδομένο που αποτελείται από τον κατακερματισμό του δημόσιου κλειδιού του και

τη ζητούμενη τιμή, κλειδώνοντας το DataToken του ως τιμή.

Αγοραστής Ο αγοραστής μπορεί να δει έναν πίνακα με όλα τα κουπόνια που είναι κλειδωμένα στη διεύθυνση DataListing χρησιμοποιώντας τη μέθοδο utxosAt του lucid. Δεδομένου ότι οποιοσδήποτε μπορεί να κλειδώσει τιμές με αυθαίρετα Datums στη διεύθυνση ενός έξυπνου συμβολαίου, ορισμένα UTxOs ενδέχεται να είναι άκυρα. Μετά το φιλτράρισμα των άκυρων UTXOs, παραμένουν μόνο αυτά που τηρούν το πραγματικό Datum του έξυπνου συμβολαίου μας. Ο αγοραστής μπορεί να επιλέξει ένα τοκεν από ένα από αυτά και να προχωρήσει στην αγορά.

Το UTxO περιέχει το PubKeyHash του πωλητή, το οποίο χρησιμοποιείται για λόγους επικύρωσης. Μπορούμε εύκολα να λάβουμε τη διεύθυνση του πωλητή, ζητώντας πληροφορίες από τον πάροχο Blockfrost και χρησιμοποιώντας το hash της συναλλαγής που δημιούργησε το UTxO, να βρούμε τη διεύθυνση που δημιούργησε το UTxO και ταιριάζει με αυτό το PubKeyHash. Η συναλλαγή πληρώνει το απαιτούμενο ποσό στη διεύθυνση του Πωλητή, ενώ παράλληλα συλλέγει το κλειδωμένο token.

Όταν προσπαθείτε να ξοδέψετε ένα UTXO που είναι κλειδωμένο από έναν επικυρωτή, είναι απαραίτητο να επισυνάψετε τον σειριοποιημένο επικυρωτή στη συναλλαγή. Αυτό γίνεται με τη χρήση της μεθόδου 'attachSpendingValidator'. Αυτός ο έλεγχος εκτός αλυσίδας διασφαλίζει ότι ο επικυρωτής θα ξεκλειδώσει επιτυχώς το UTXO πριν από την υποβολή της συναλλαγής στο δίκτυο blockchain.

Μόλις η συναλλαγή πληροί όλες τις προϋποθέσεις, συμπεριλαμβανομένης της καταβολής του απαιτούμενου ποσού στον Πωλητή, θα διεκπεραιωθεί επιτυχώς. Αυτό έχει ως αποτέλεσμα ο Αγοραστής να αποκτήσει το DataToken και ο Πωλητής να λάβει το καθορισμένο ποσό σε ADA.

Μετά την επιτυχή συναλλαγή, ο αγοραστής μπορεί στη συνέχεια να ζητήσει τα δεδομένα που σχετίζονται με το DataToken από τον διακομιστή. Για να γίνει αυτό, ο Αγοραστής δημιουργεί μια ψηφιακή υπογραφή χρησιμοποιώντας τη μέθοδο lucid.wallet.signMessage. Ο διακομιστής επαληθεύει αυτή την υπογραφή, αποκρυπτογραφεί τα αντίστοιχα δεδομένα από το IPFS και τα επιστρέφει στον πελάτη για λήψη.

Η διαδικασία αυτή εξασφαλίζει μια ασφαλή και διαφανή συναλλαγή, επιτρέποντας τόσο στον Αγοραστή όσο και στον Πωλητή να επιτύχουν τους στόχους τους, διατηρώντας παράλληλα την ακεραιότητα των σχετικών δεδομένων.

Bid Flow

Το μοτίβο Bid αντιμετωπίζει μια κοινή ανησυχία μεταξύ των χρηστών που διστάζουν να παραχωρήσουν προσωρινά τον έλεγχο των tokens τους, όπως απαιτείται στο μοτίβο Ask. Στο μοτίβο προσφοράς, ο πωλητής διατηρεί την κατοχή του token μέχρι τη στιγμή που θα αποζημιωθεί πλήρως.

Αγοραστής Υποθέτοντας ότι ένας Πωλητής έχει ήδη κόψει ένα DataToken, το μοτίβο προσφοράς ξεκινά από τον Αγοραστή που εκφράζει ενδιαφέρον για ένα συγκεκριμένο token. Μέσα από τη διεπαφή αγοραστή, μπορούν να προβληθούν όλα τα token που έχουν κοπε-

ί από τους πωλητές. Είναι σημαντικό να σημειωθεί ότι αυτά τα token εξακολουθούν να βρίσκονται στα πορτοφόλια των Πωλητών και δεν είναι κλειδωμένα στο πλαίσιο του συμβολαίου DataListing.

Ο Αγοραστής επιλέγει το κουπόνι που τον ενδιαφέρει και υποβάλλει προσφορά. Για να γίνει αυτό, το έξυπνο συμβόλαιο Bid παραμετροποιείται χρησιμοποιώντας την κατηγορία περιουσιακών στοιχείων του token, δημιουργώντας μια τελική σειριακή μορφή και, κατά συνέπεια, μια μοναδική διεύθυνση έξυπνου συμβολαίου. Στη συνέχεια, ο αγοραστής κλειδώνει ένα UTxO κάτω από αυτή τη διεύθυνση , θέτοντας ως τιμή το ποσό της προσφοράς. Το ποσό αυτό αντιπροσωπεύει αυτό που θα λάβει ο Πωλητής κατά τη διεκδίκηση της προσφοράς. Ο κατακερματισμός του δημόσιου κλειδιού του Αγοραστή ορίζεται ως Datum για να επιβεβαιωθεί αργότερα ότι ο Αγοραστής λαμβάνει το token για το οποίο πλειοδότησε. Στη συνέχεια, η συναλλαγή υπογράφεται και υποβάλλεται στο δίκτυο.

Στο ίδιο περιβάλλον εργασίας, ο Αγοραστής μπορεί να δει όλες τις ενεργές προσφορές που έχει κάνει και δεν έχουν ακόμη διεκδικηθεί από τους Πωλητές. Αυτό του δίνει τη δυνατότητα να εξαργυρώσει τα ΑΔΑ του, αν επιλέξει να αποσύρει την προσφορά του. Για να γίνει αυτό, υποβάλλεται μια συναλλαγή για την είσπραξη του UTxO, χρησιμοποιώντας ως τιμή redeemer "Redeem". Ο Validator script του έξυπνου συμβολαίου Bid πρέπει να επισυνάπτεται στη συναλλαγή και η συναλλαγή να υπογράφεται ώστε να ταιριάζει με το hash του δημόσιου κλειδιού του Αγοραστή στο datum, απελευθερώνοντας έτσι το κλειδωμένο ποσό ADA.

Πωλητής Εάν ένας ή περισσότεροι Αγοραστές έχουν υποβάλει προσφορές για ένα συγκεκριμένο κουπόνι, ο Πωλητής μπορεί να επιλέξει ποια προσφορά θα διεκδικήσει. Για να το κάνει αυτό, ο Πωλητής παραμετροποιεί τον Validator με την Asset Class του token του, δημιουργώντας μια μοναδική διεύθυνση έξυπνου συμβολαίου όπου μπορεί να δει όλες τις τις προσφορές που έγιναν για το συγκεκριμένο token. Στη συνέχεια, ο Πωλητής επιλέγει το UTXO (προσφορά) που επιθυμεί να διεκδικήσει. Ο redeemer επισυνάπτεται στη συναλλαγή και "Sell" χρησιμοποιείται ως τιμή. Είναι καθοριστικό η συναλλαγή αυτή να μεταφέρει επίσης το DataToken στο πορτοφόλι του Αγοραστή, διαφορετικά η συναλλαγή θα αποτύχει. Εάν πληρούνται όλες οι προϋποθέσεις, ο Πωλητής λαμβάνει το ποσό της προσφοράς σε ADA και ο Αγοραστής αποκτά στην κατοχή του το DataToken.

Αξίζει να σημειωθεί ότι εάν ένας Πωλητής προσπαθήσει να διεκδικήσει πολλαπλές προσφορές, η συναλλαγή θα αποτύχει. Το έξυπνο συμβόλαιο διασφαλίζει ότι κάθε Αγοραστής λαμβάνει το συγκεκριμένο token, και δεδομένου ότι ο Πωλητής μπορεί να κατέχει μόνο μία μονάδα του συγκεκριμένου token, πολλαπλές διεκδικήσεις δεν είναι δυνατές.

Μετά τη συναλλαγή, ο Αγοραστής μπορεί να σαρώσει το πορτοφόλι του για νέα tokens χρησιμοποιώντας τη διεπαφή αγοραστή. Μόλις εντοπιστεί το νέο token, η διεπαφή χρήστη παρέχει τη δυνατότητα λήψης των σχετικών δεδομένων. Παρόμοια με το μοτίβο Ask, ο αγοραστής υπογράφει το αίτημα διακομιστή για να επικυρώσει την κυριότητα του τοκεν. Μετά την επικύρωση, τα δεδομένα αποκρυπτογραφούνται και αποστέλλονται πίσω στον Αγοραστή για λήψη.

Αυτό το μοτίβο προσφοράς προσφέρει μια εναλλακτική ροή συναλλαγών που αντιμετωπίζει τις ανησυχίες των χρηστών που προτιμούν να διατηρούν τον έλεγχο των tokens τους μέχρι τη στιγμή της πώλησης, εξασφαλίζοντας μια ασφαλή και διαφανή διαδικασία και για

τα δύο μέρη.

5.2 Ανάπτυξη έξυπνων συμβολαίων

5.2.1 Minting Policy DataToken

Το DataToken Minting Policy είναι το πρώτο από τα τρία έξυπνα συμβόλαια που χρησιμοποιούνται σε αυτή την αποκεντρωμένη εφαρμογή. Σε αντίθεση με τα τυπικά έξυπνα συμβόλαια, η πολιτική κοπής νομισμάτων είναι εξειδικευμένη για να διέπει τη δημιουργία νέων token. Από προεπιλογή, μια πολιτική κοπής λαμβάνει ως ορίσματα τον redeemer και το πλαίσιο της συναλλαγής. Ωστόσο, η συγκεκριμένη πολιτική κοπής παραμετροποιείται περαιτέρω με το (UTxO) ενός χρήστη, το οποίο οποίο αναπαρίσταται με ένα όρισμα TxOutRef.

Κάθε συναλλαγή blockchain έχει ένα μοναδικό αναγνωριστικό συναλλαγής, το οποίο προκύπτει από το hash της. Επιπλέον, κάθε συναλλαγή μπορεί να έχει πολλαπλές εξόδους, γνωστές ως UTxOs, καθεμία από τις οποίες έχει ξεχωριστό δείκτη εξόδου. Ως εκ τούτου, ένα ΥΤξΟ μπορεί να αναγνωριστεί μοναδικά εντός της αλυσίδας μπλοκ χρησιμοποιώντας τη μορφή `txHash#outputIndex`.

Παρακάτων είναι ο βασικός κώδικας για αυτή την πολιτική νομισματοκοπίας:

```
1
2  mkDataTokenPolicy :: TxOutRef -> TokenName -> () -> ScriptContext -> Bool
3  mkDataTokenPolicy utxo tn () ctx = traceIfFalse "UTxO not consumed" consumesUtxo &&
4                                     traceIfFalse "Wrong amount minted" mintsExactlyOneToken
5      where
6          info :: TxInfo
7          info = scriptContextTxInfo ctx
8
9          transactionInputs :: [TxInInfo]
10         transactionInputs = txInfoInputs info
11
12         consumesUtxo :: Bool
13         consumesUtxo = any (\i -> txInInfoOutRef i == utxo) transactionInputs
14
15         valueMinted :: Value
16         valueMinted = txInfoMint info
17
18         mintsExactlyOneToken :: Bool
19         mintsExactlyOneToken = case flattenValue valueMinted of
20             -- we ignore currencySymbol
21             [(_, tn', amt)] -> tn' == tn && amt == 1
22             _               -> False
```

Η πολιτική νομισματοκοπίας DataToken έχει σχεδιαστεί για να επιβάλλει δύο κρίσιμους κανόνες:

1. Κατανάλωση UTxO: Η πολιτική νομισματοκοπίας επαληθεύει ότι η συναλλαγή καταναλώνει το συγκεκριμένο UTxO με το οποίο παραμετροποιήθηκε η πολιτική. Αυτό διασφαλίζει ότι μόνο ο κάτοχος αυτού του UTxO μπορεί να κόψει ένα νέο DataToken.

Αυτό είναι ζωτικής σημασίας για τη διατήρηση της ακεραιότητας και της μοναδικότητας κάθε νομισματοδέκτη που έχει κοπεί.

2. Κοπή ενιαίου token: Η πολιτική ελέγχει επίσης ότι στη συναλλαγή κόβεται μόνο ένα DataToken. Αυτός είναι ένας κανόνας ειδικού τομέα(domain) για το dApp μας, που διασφαλίζει ότι κάθε DataToken αντιπροσωπεύει ένα μοναδικό σύνολο δεδομένων και διατηρεί την ατομική του αξία.

5.2.2 Έξυπνο συμβόλαιο DataListing για τη ροή Ask

Το έξυπνο συμβόλαιο DataListing χρησιμεύει ως επικυρωτής για τη ροή Ask, όπου ένας πωλητής κλειδώνει το DataToken του και θέτει μια ζητούμενη τιμή γι' αυτό. Αυτό το έξυπνο συμβόλαιο είναι ένας επικυρωτής, πράγμα που σημαίνει ότι δέχεται τρία ορίσματα: τον redeemer, το πλαίσιο συναλλαγής και το Datum.

```
data DataListDatum = DataListDatum
    {
     dataSeller  :: PubKeyHash
    , price      :: Integer
    } deriving Prelude.Show

data DataListingRedeemer = Redeem | Purchase


mkValidator :: DataListDatum -> DataListingRedeemer -> ScriptContext -> Bool
mkValidator dat r ctx = case r of
    Purchase -> traceIfFalse "Amount required not paid to owner" buyerHasPaidSeller &&
          traceIfFalse "You must consume only one utxo" consumesOnlyOneUtxo
    Redeem   -> traceIfFalse "data seller's signature missing" checkSignedBySeller

  where

    info :: TxInfo
    info = scriptContextTxInfo ctx

    -- In lovelaces
    dataPrice :: Integer
    dataPrice = price dat

    valuePaidToSeller :: Value
    valuePaidToSeller = valuePaidTo info (dataSeller dat)

    pricePaidToSeller :: Integer
    pricePaidToSeller = valueOf valuePaidToSeller adaSymbol adaToken

    buyerHasPaidSeller :: Bool
    buyerHasPaidSeller = pricePaidToSeller >= dataPrice

```

```
34  consumesOnlyOneUtxo = length consumedInputsOfThisScript == 1
35      where
36      scriptAddress :: ValidatorHash
37      scriptAddress = ownHash ctx
38
39      -- The credentials that are required to unlock each input, can be either PubKeyHash,
40      -- which means they belong to a user, and they unlock them by signing with their pk,
41      -- or ScriptCredentials, that require the script to be included, and validated
42      inputScriptCredentials :: [Credential]
43      inputScriptCredentials = map (addressCredential . txOutAddress . txInInfoResolved) $ txInfoInputs info
44
45      consumedInputsOfThisScript = filter protectedByThisScript inputScriptCredentials
46          where
47          protectedByThisScript :: Credential -> Bool
48          protectedByThisScript c = case c of
49              PubKeyCredential _ -> False
50              ScriptCredential vh -> vh == scriptAddress
51
52  checkSignedBySeller :: Bool
53  checkSignedBySeller = txSignedBy info $ dataSeller dat
```

Δυνατότητες του Redeemer Το έξυπνο συμβόλαιο DataListing έχει σχεδιαστεί για να φιλοξενεί δύο διαφορετικούς φορείς:

1. Ο αγοραστής: Ο οποίος επιθυμεί να αγοράσει το DataToken.

2. Ο πωλητής: Ο οποίος μπορεί να θέλει να ακυρώσει την καταχώριση δεδομένων και να ανακτήσει το DataToken του.

Όταν καλείται ο εξαργυρωτής ¨Αγορά¨, ο επικυρωτής εκτελεί δύο κρίσιμους ελέγχους:

1. Επαλήθευση πληρωμής: Επαληθεύει ότι ο αγοραστής έχει καταβάλει στον πωλητή το συμφωνηθέν ποσό, όπως ορίζεται στο Datum. Αυτό διασφαλίζει ότι η συναλλαγή είναι δίκαιη και ευθυγραμμίζεται με την τιμή που ζητά ο πωλητής.

2. Ξεκλείδωμα με ένα μόνο Token: Ελέγχει ότι η συναλλαγή δαπάνης επιχειρεί να ξεκλειδώσει μόνο ένα DataToken. Αυτό είναι ένα κρίσιμο μέτρο ασφαλείας για την αποτροπή πιθανών ευπαθειών.

    - Επιπτώσεις στην ασφάλεια: Χωρίς αυτόν τον έλεγχο, θα μπορούσε να προκύψει ευπάθεια. Σκεφτείτε ένα σενάριο όπου δύο DataTokens από τον ίδιο πωλητή είναι κλειδωμένα στο πλαίσιο αυτού του έξυπνου συμβολαίου, και τα δύο απαιτούν την ίδια τιμή (π.χ. 40 ADA) στο Datum. Ένας κακόβουλος αγοραστής θα μπορούσε να δημιουργήσει μια συναλλαγή που πληρώνει τον πωλητή 40 ADA, αλλά επιχειρεί να ξεκλειδώσει και τα δύο tokens. Αυτός ο έλεγχος μετριάζει αποτελεσματικά τέτοιους κινδύνους.

5.2.3 Έξυπνο συμβόλαιο προσφοράς για τη ροή προσφορών

Το έξυπνο συμβόλαιο Bid χρησιμεύει ως η ραχοκοκαλιά για τη ροή Bid, όπου ένας αγοραστής υποβάλλει μια προσφορά για ένα DataToken. Πρόκειται για έναν παραμετροποιημένο επικυρωτή, που σημαίνει ότι δέχεται τέσσερα ορίσματα: το τοκεν με το οποίο έχει παραμετροποιηθεί, το Datum, τον Redeemer και το Script Context.

```
data BidParams = BidParams
    {
     dataTokenNFT :: AssetClass
    }

data BidDatum = BidDatum
    {
     dataBuyer   :: PubKeyHash
    } deriving Prelude.Show


data BidRedeemer = Redeem | Sell

mkValidator :: BidParams -> BidDatum -> BidRedeemer -> ScriptContext -> Bool
mkValidator p dat r ctx = case r of
          Sell     -> traceIfFalse "token not given to buyer" buyerGetsToken
          Redeem -> traceIfFalse "buyer's signature missing" checkSignedByBuyer

  where
    info :: TxInfo
    info = scriptContextTxInfo ctx

    checkSignedByBuyer :: Bool
    checkSignedByBuyer = txSignedBy info $ dataBuyer dat

    valuePaidToBuyer :: Value
    valuePaidToBuyer = valuePaidTo info $ dataBuyer dat

    buyerGetsToken :: Bool
    buyerGetsToken = assetClassValueOf valuePaidToBuyer (dataTokenNFT p) == 1
```

Έλεγχοι και περιορισμοί Το έξυπνο συμβόλαιο Bid εκτελεί ελέγχους που είναι εννοιολογικά παρόμοιοι με εκείνους του συμβολαίου DataListing, αλλά με κάποιες μικρές διαφορές:

1. Όχι διπλές δαπάνες: Δεδομένου ότι κάθε DataToken μπορεί να κοπεί μόνο μία φορά, δεν υπάρχει κίνδυνος διπλών δαπανών στο πλαίσιο αυτό. Αυτό απλοποιεί τη λογική επικύρωσης σε σύγκριση με το συμβόλαιο DataListing.

2. Μία προσφορά ανά Token: Το συμβόλαιο έχει σχεδιαστεί έτσι ώστε ένας αγοραστής να μην μπορεί να κάνει πολλαπλές προσφορές για το ίδιο DataToken. Εάν ένας αγοραστής επιθυμεί να αλλάξει την προσφορά του, θα πρέπει πρώτα να εξαργυρώσει την υπάρχουσα προσφορά του πριν τοποθετήσει νέα.

- Σημείωση για την ασφάλεια: Εάν προκύψει ένα σενάριο όπου είναι επιθυμητή η τοποθέτηση πολλαπλών προσφορών, θα μπορούσε να εφαρμοστεί ένας πρόσθετος έλεγχος για να διασφαλιστεί ότι μόνο ένα UTxO θα διεκδικηθεί από τον Πωλητή. Αυτό θα βοηθούσε στην αποφυγή πιθανών τρωτών σημείων διπλής δαπάνης.

Έτσι ολοκληρώνεται η επισκόπηση των τριών έξυπνων συμβολαίων που τροφοδοτούν το dApp: DataToken Minting Policy, DataListing και Bid. Κάθε ένα έχει το δικό του σύνολο ελέγχων και περιορισμών για να διασφαλίσει ασφαλείς και δίκαιες συναλλαγές στην αγορά.

5.3 Βαςκ-ενδ ανάπτυξη

Το βαςκενδ παίζει σημαντικό ρόλο στην κρυπτογράφηση και αποθήκευση των δεδομένων του χρήστη, καθώς και στην αποθήκευση μεταδεδομένων εκτός αλυσίδας για τα tokens, τα οποία μπορούν στη συνέχεια να χρησιμοποιηθούν από τους αγοραστές για να ανακτήσουν τα περιουσιακά στοιχεία που αγόρασαν. Διαθέτει επίσης ορισμένους μηχανισμούς επικύρωσης για την επικύρωση των αιτημάτων και την επαλήθευση των ιδιοκτητών των token που κάνουν τα αιτήματα. Αυτό διασφαλίζει ότι μόνο οι κάτοχοι των token μπορούν να αποκρυπτογραφήσουν και να κατεβάσουν τα δεδομένα περιήγησης. Αλληλεπιδρά επίσης με το δίκτυο IPFS, όπου τα δεδομένα αποθηκεύονται σε κρυπτογραφημένη μορφή.

5.3.1 API Routes

Διαδρομή για Συσχετισμό Token & Data

`saveHistory` Διαδρομή

Endpoint: `/api/saveHistory`

Σκοπός: Αυτή είναι η πρώτη διαδρομή που συνήθως καλείται στη ροή του χρήστη. Ενεργοποιείται από την επέκταση του προγράμματος περιήγησης και λαμβάνει τη διεύθυνση πορτοφολιού του χρήστη και τα δεδομένα περιήγησης στο σώμα της αίτησης.

Λειτουργικότητα: Ο διακομιστής κρυπτογραφεί τα λαμβανόμενα δεδομένα περιήγησης και τα αποθηκεύει στο δίκτυο IPFS. Στη συνέχεια συσχετίζει το επιστρεφόμενο CID (Content Identifier) με τη διεύθυνση πορτοφολιού του χρήστη. Μια βάση δεδομένων κλειδιών-τιμών χρησιμοποιείται τόσο για τον έλεγχο ταυτότητας όσο και για την αποθήκευση μεταδεδομένων τοκεν.

Επικύρωση: Ο διακομιστής επικυρώνει το σώμα της αίτησης για να διασφαλίσει ότι περιέχει έγκυρη διεύθυνση πορτοφολιού και δεδομένα περιήγησης.

Στη συνέχεια, όταν ο χρήστης εισέρχεται στην εφαρμογή dApp, η οποία χρησιμοποιεί το Lucid για να συνδεθεί με το πορτοφόλι του χρήστη, υποβάλλει αίτημα στον διακομιστή για να ανακτήσει τυχόν δεδομένα που σχετίζονται με αυτό το πορτοφόλι.

`retrieveHistory` Διαδρομή

Endpoint: `/api/retrieveHistory`

Σκοπός: Αυτή η διαδρομή καλείται όταν ο χρήστης αποκτά πρόσβαση στην δΑπп, η οποία συνδέεται με το πορτοφόλι του χρήστη χρησιμοποιώντας τη βιβλιοθήκη Lucid.

Λειτουργικότητα: Ο διακομιστής ανακτά όλα τα δεδομένα που σχετίζονται με το πορτοφόλι του χρήστη.

Επικύρωση: Μια ψηφιακή υπογραφή χρησιμοποιείται για να επικυρώσει ότι το αίτημα υποβάλλεται πράγματι από τον ιδιοκτήτη του πορτοφολιού.

`associateDataWithToken` Διαδρομή

Endpoint: `/api/associateDataWithToken`

Σκοπός: Αυτή η διαδρομή είναι υπεύθυνη για τη συσχέτιση της κατηγορίας περιουσιακών στοιχείων ενός νεοδημιουργηθέντος token με το προηγουμένως αποθηκευμένο CID, δημιουργώντας ουσιαστικά μεταδεδομένα εκτός αλυσίδας για το token.

Λειτουργικότητα:

- Συνδέει το CID με την κατηγορία περιουσιακών στοιχείων του νέου κουπονιού.
- Διαγράφει την προηγούμενη συσχέτιση του CID με το πορτοφόλι του χρήστη.
- Δημιουργεί μια λίστα TokenListing για μάρκες που είναι διαθέσιμες αλλά δεν έχουν ακόμη κλειδωθεί στο πλαίσιο μιας λίστας ΔαταΛιστινγ.

Επικύρωση:

- Επαληθεύει ότι η κατηγορία περιουσιακών στοιχείων και το CID του κουπονιού είναι έγκυρα.
- Διασφαλίζει ότι το προηγούμενο πορτοφόλι κατέχει το νέο κουπόνι.

Διαδρομές για την ενημέρωση των καταχωρίσεων και των ενεργών προσφορών των tokens Η αρχιτεκτονική του βαςκενδ έχει σχεδιαστεί όχι μόνο για τη διαχείριση των tokens και των σχετικών δεδομένων τους, αλλά και των καταχωρίσεων και των ενεργών προσφορών για αυτά τα tokens. Παρακάτω παρουσιάζονται οι βασικές διαδρομές και λειτουργίες για τη διαχείριση των καταχωρίσεων και των ενεργών προσφορών των token:

Καταχωρίσεις Token

Οι λίστες token δημιουργούνται για τα token που είναι διαθέσιμα προς αγορά αλλά δεν έχουν κλειδωθεί στο πλαίσιο ενός συμβολαίου DataListing. Η λειτουργία τους είναι να επιτρέπουν στους αγοραστές να περιηγηθούν στα διαθέσιμα μάρκες και να υποβάλουν προσφορές για αυτές που τους ενδιαφέρουν.

`fetchAll` Διαδρομή

Endpoint: `/api/tokenListing/fetchAll`

Σκοπός: Ανάκτηση όλων των διαθέσιμων καταχωρίσεων tokens, ώστε οι πλειοδότες να μπορούν να περιηγηθούν σε αυτές.

Λειτουργικότητα: Επιστρέφει μια λίστα με όλα τα tokens που είναι διαθέσιμα αλλά δεν έχουν ακόμη κλειδωθεί στο πλαίσιο ενός συμβολαίου DataListing

`deleteTokenListing` Διαδρομή

Endpoint: `/api/tokenListing/delete`

Σκοπός: Διαγραφή μιας καταχώρισης token μόλις εγκριθεί μια προσφορά και το token δεν είναι πλέον διαθέσιμο προς πώληση

Λειτουργικότητα: Διαγράφει τη συγκεκριμένη καταχώριση token με βάση το μοναδικό αναγνωριστικό της.

Ενεργές προσφορές

Οι ενεργές προσφορές δημιουργούνται όταν οι αγοραστές υποβάλλουν προσφορές για τις διαθέσιμες λίστες tokens. Το back-end διαχειρίζεται αυτές τις προσφορές μέχρι να εξαργυρωθούν ή να εκπληρωθούν.

`createActiveBid` Διαδρομή

Endpoint: `/api/activeBid/create`

Σκοπός: Δημιουργία μιας νέας ενεργής προσφοράς όταν ένας αγοραστής την τοποθετεί

Λειτουργικότητα: Προσθέτει μια νέα καταχώρηση στη συλλογή των ενεργών προσφορών, αποθηκεύοντας βασικές πληροφορίες, όπως το hash της συναλλαγής, το ποσό, την Asset Class του token και την ημερομηνία.

`deleteActiveBid` Διαδρομή

Endpoint: `/api/activeBid/delete`

Σκοπός: Αφαίρεση μιας ενεργής προσφοράς, συνήθως όταν έχει εξαργυρωθεί ή εκπληρωθεί.

Λειτουργικότητα: Διαγράφει τη συγκεκριμένη ενεργή προσφορά με βάση το μοναδικό αναγνωριστικό της.

`fetchActiveBidsByWallet` Διαδρομή

Endpoint: `/api/activeBid/fetchByWallet`

Σκοπός: : Ανάκτηση όλων των ενεργών προσφορών που σχετίζονται με ένα συγκεκριμένο πορτοφόλι

Φυνστιοναλιτψ: Επιστρέφει μια λίστα με όλες τις ενεργές προσφορές που συνδέονται με ένα συγκεκριμένο πορτοφόλι.

5.3.2 Διαχείριση δεδομένων με το IPFS

Το διαπλανητικό σύστημα αρχείων (IPFS) χρησιμεύει ως επίπεδο αποθήκευσης δεδομένων για την dApp, ειδικά για την αποθήκευση κρυπτογραφημένου ιστορικού περιήγησης των χρηστών. Το IPFS προσφέρει μια αποκεντρωμένη προσέγγιση στην αποθήκευση δεδομένων, καθιστώντας το ιδανικό για την εφαρμογή αυτή.

Χρήση του Blockfrost ως πύλη IPFS

Ενώ είναι δυνατή η ανάπτυξη και διαχείριση ενός προσαρμοσμένου κόμβου IPFS, η αξιοποίηση ενός παρόχου υπηρεσιών όπως η Blockfrost απλοποιεί τη διαδικασία. Η Blockfrost, που χρησιμοποιείται ήδη ως πάροχος blockchain, μπορεί επίσης να λειτουργήσει ως πύλη IPFS, χειριζόμενη τις πολυπλοκότητες της αποθήκευσης και ανάκτησης δεδομένων.
Ακολουθεί ένα απλοποιημένο παράδειγμα για το πώς μπορεί να επιτευχθεί αυτό στο Νοδεθς με τη χρήση Τψπεσςριπτ.

```
import { BlockFrostIPFS } from '@blockfrost/blockfrost-js';

const IPFS = new BlockFrostIPFS({
      projectId: ipfsProjectId,
    });
const added = await IPFS.add(tmpFilePath);

// Pin the data to ensure it remains accessible
const pinned = await IPFS.pin(added.ipfs_hash);
const cid = pinned.ipfs_hash;
```

Listing 5.1: Store data in IPFS using Blockfrost

Μηχανισμός καρφίτσωσης(pinning) Η καρφίτσωση είναι ένα κρίσιμο χαρακτηριστικό του IPFS που εξασφαλίζει τη μόνιμη αποθήκευση των αντικειμένων δεδομένων. Όταν τα δεδομένα μεταφορτώνονται για πρώτη φορά στο IPFS μέσω του Blockfrost, θα πρέπει να καρφιτσωθούν για να διασφαλιστεί ότι παραμένουν προσβάσιμα και δεν υπόκεινται σε συλλογή σκουπιδιών. Αυτό πρέπει να γίνεται συχνά για να αποφεύγεται η συλλογή σκουπιδιών. Σε μια πιο προηγμένη υλοποίηση, θα μπορούσε να ρυθμιστεί μια εργασία cron για την τακτική επανασύνδεση των δεδομένων, εξασφαλίζοντας έτσι τη μακροπρόθεσμη διαθεσιμότητά τους.

Με την ενσωμάτωση του IPFS και τη χρήση του Blockfrost ως πύλης, η αρχιτεκτονική του backend επιτυγχάνει μια ισχυρή, αποκεντρωμένη λύση αποθήκευσης δεδομένων. Αυτή η

ρύθμιση όχι μόνο ευθυγραμμίζεται με την αποκεντρωμένη φύση της δΑπп, αλλά προσφέρει επίσης έναν κλιμακούμενο και ασφαλή τρόπο διαχείρισης των δεδομένων των χρηστών.

Χρησιμοποιώντας αυτές τις διαδρομές και τους σχετικούς μηχανισμούς επικύρωσής τους, το backend διασφαλίζει την ασφαλή και αποτελεσματική διαχείριση των μαρκών και των σχετικών δεδομένων τους.

5.4 Μηχανισμοί εξουσιοδότησης

5.4.1 Ψηφιακή υπογραφή για επαλήθευση ταυτότητας

Στον κόσμο των dApps που βασίζονται στην αλυσίδα μπλοκ, οι ψηφιακές υπογραφές είναι κρίσιμες για την επαλήθευση της ταυτότητας ενός χρήστη. Η διαδικασία αυτή χρησιμοποιεί ασύμμετρη κρυπτογραφία, όπου κάθε χρήστης διαθέτει ένα ζεύγος κλειδιών: ένα δημόσιο κλειδί που μοιράζεται δημόσια και ένα ιδιωτικό κλειδί που παραμένει εμπιστευτικό. Όταν ένας χρήστης επιθυμεί να στείλει ένα μήνυμα ή να πραγματοποιήσει μια συναλλαγή, το υπογράφει με το ιδιωτικό του κλειδί. Αυτή η υπογραφή χρησιμεύει ως μόνιμη αμετάβλητη σφραγίδα της ταυτότητάς του.

Δημιουργία υπογραφής Ο χρήστης χρησιμοποιεί το ιδιωτικό του κλειδί για να δημιουργήσει μια ψηφιακή υπογραφή στα δεδομένα ή το μήνυμα. Αυτό γίνεται συνήθως με τη λήψη ενός κατακερματισμού του μηνύματος και την κρυπτογράφηση χρησιμοποιώντας το ιδιωτικό κλειδί. Στη συνέχεια, η ψηφιακή υπογραφή προσαρτάται στο μήνυμα. Στην παρούσα δΑπп, αυτό επιτυγχάνεται από την πλευρά του πελάτη με τη χρήση της βιβλιοθήκης `lucid-cardano` ως εξής:

```
1 const signature = lucid.wallet.signMessage(wallet, hexPayload);
```

Listing 5.2: Signature Generation

Επαλήθευση υπογραφής Για να επαληθεύσει την ταυτότητα του αποστολέα, ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για να αποκρυπτογραφήσει τη συνημμένη ψηφιακή υπογραφή. Στη συνέχεια, κατακερματίζει το ληφθέν μήνυμα και το συγκρίνει με την αποκρυπτογραφημένη κατακερματισμένη μορφή. Εάν και οι δύο κατακερματισμοί ταιριάζουν, επιβεβαιώνεται ότι το μήνυμα δεν έχει παραποιηθεί και προέρχεται πράγματι από τον κάτοχο του δημόσιου κλειδιού. Αυτή η επαλήθευση γίνεται από την πλευρά του διακομιστή, χρησιμοποιώντας επίσης τη βιβλιοθήκη `lucid-cardano`:

```
1 const signatureIsValid = lucid.verifyMessage(wallet, hexPayload, signature);
```

Listing 5.3: Signature Verification

Αυτός ο μηχανισμός διασφαλίζει τόσο την ακεραιότητα όσο και την προέλευση του μηνύματος, αποτελώντας θεμελιώδες στοιχείο για ασφαλείς και χωρίς εμπιστοσύνη(trustless) επικοινωνίες εντός της dApp.

Χρονοσφράγιση στις ψηφιακές υπογραφές Η προσθήκη μιας χρονοσφραγίδας σε μια ψηφιακή υπογραφή είναι μια κοινή πρακτική, η τεχνική αυτή είναι γνωστή ως ¨χρονοσφράγιση¨ και εξυπηρετεί πολλαπλούς σκοπούς:

- Λήξη: Μπορούμε να ορίσουμε ένα χρόνο λήξης για την ψηφιακή υπογραφή, καθιστώντας την άκυρη μετά από ένα συγκεκριμένο χρονικό διάστημα. Αυτό μπορεί να είναι χρήσιμο για προσωρινές εξουσιοδοτήσεις ή συναλλαγές που είναι ευαίσθητες στο χρόνο.
- Μη αποκήρυξη: Αυτό μπορεί να είναι ύψιστης σημασίας σε νομικές και οικονομικές εφαρμογές.
- Ασφάλεια: Η χρονοσφραγίδα μπορεί να βοηθήσει στον περιορισμό του χρονικού πλαισίου κατά το οποίο το παραβιασμένο κλειδί χρησιμοποιήθηκε για την υπογραφή εγγράφων, βοηθώντας στον έλεγχο και περιορισμό των ζημιών.

5.4.2 Εξουσιοδότηση πωλητή

Ροές ζήτησης και προσφοράς Ο πωλητής ξεκινά τη διαδικασία συλλογής δεδομένων μέσω μιας επέκτασης του προγράμματος περιήγησης, όπου απαιτείται η εισαγωγή της διεύθυνσης του πορτοφολιού Cardano. Στη συνέχεια, τα δεδομένα που συλλέγονται αποστέλλονται στο backend, κρυπτογραφούνται και αποθηκεύονται στο IPFS.

Επιπλέον, μια συσχέτιση μεταξύ της διεύθυνσης πορτοφολιού ή της κατηγορίας περιουσιακού στοιχείου(Asset Class) token και του αναγνωριστικού περιεχομένου IPFS CID (Content Identifier) αποθηκεύεται στη βάση δεδομένων κλειδιών-τιμών του διακομιστή. Αυτή η προσέγγιση είναι παρόμοια με την προσάρτηση μεταδεδομένων on-chain στο τοκεν, συμπεριλαμβάνοντας μεταδεδομένα σχετικά με τη συναλλαγή που έκοψε το τοκεν.

Κατά την είσοδο στην εφαρμογή Next.js dApp, η εφαρμογή συνδέεται με το πορτοφόλι του πωλητή χρησιμοποιώντας τη βιβλιοθήκη `lucid-cardano`. Στη συνέχεια, η dApp αντλεί όλα τα δεδομένα που σχετίζονται με το πορτοφόλι του πωλητή από τον διακομιστή και αποδεικνύει την ταυτότητα του χρήστη στέλνοντας επίσης μια ψηφιακή υπογραφή. Ο διακομιστής επαληθεύει αυτή την υπογραφή και επιστρέφει τα δεδομένα στον πωλητή για επιθεώρηση και κοπή του "Data Token".

5.4.3 Εξουσιοδότηση αγοραστή

Ο αγοραστής ξεκινάει ένα αίτημα προς τον διακομιστή με σκοπό να αποκρυπτογραφήσει και να κατεβάσει τα δεδομένα που συνδέονται με ένα συγκεκριμένο token που έχει αγοράσει. Για να το κάνει αυτό, ο αγοραστής αποστέλλει τόσο την Asset Class του token όσο και τη δική του διεύθυνση πορτοφολιού. Στη συνέχεια, ο διακομιστής προχωρά σε μια διαδικασία επαλήθευσης δύο βημάτων:

1. Επαλήθευση ταυτότητας: Παρόμοια με τον μηχανισμό που χρησιμοποιείται για τον Πωλητή, ο διακομιστής επιβεβαιώνει πρώτα ότι το αίτημα προέρχεται πραγματικά από τον ιδιοκτήτη της παρεχόμενης διεύθυνσης πορτοφολιού. Αυτό επιτυγχάνεται μέσω της επαλήθευσης της ψηφιακής υπογραφής.

2. Επαλήθευση ιδιοκτησίας token: Χρησιμοποιώντας τον πάροχο Blockfrost, ο διακομιστής ελέγχει ότι το εν λόγω πορτοφόλι κατέχει πράγματι τουλάχιστον ένα UTxO που σχετίζεται με την καθορισμένη Asset Class του token.

Αν ο διακομιστής παρακάμψει αυτά τα βήματα επαλήθευσης, θα ανοίξει την πόρτα για πιθανούς κινδύνους ασφαλείας. Συγκεκριμένα, οποιοσδήποτε χρήστης που γνωρίζει την Asset Class ενός τοκεν θα μπορούσε να ισχυριστεί ψευδώς ότι είναι ιδιοκτήτης και να ζητήσει πρόσβαση στα δεδομένα. Αυτό θα υπονόμευε θεμελιωδώς την εμπιστοσύνη και την ακεραιότητα ολόκληρου του συστήματος.

Μηχανισμοί εξουσιοδότησης των ΤοκενΛιστινγς και ΑχτιεΒιδς

Ενώ η επικύρωση πορτοφολιού θα μπορούσε επίσης να χρησιμοποιηθεί για αυτές τις διαδρομές, ένας εναλλακτικός και ενδεχομένως πιο αποτελεσματικός τρόπος για την εξουσιοδότηση αυτών των αιτημάτων θα μπορούσε να είναι η αποστολή του αντίστοιχου κατακερματισμού συναλλαγής που σχετίζεται με κάθε ενέργεια. Ο διακομιστής θα μπορούσε στη συνέχεια να το επικυρώσει χρησιμοποιώντας έναν πάροχο blockchain για να διασφαλίσει ότι τα δεδομένα εισόδου είναι σωστά. Για παράδειγμα, ένα αίτημα δημιουργίας ενεργής προσφοράς θα πρέπει να στείλει το τξΗαση της συναλλαγής που κλείδωσε το UTxO κάτω από τη διεύθυνση Bid.

5.5 Έλεγχος στο Plutus: Ακεραιότητα έξυπνων συμβολαίων

Στη σφαίρα των αποκεντρωμένων εφαρμογών (dApps), ο ρόλος των δοκιμών δεν είναι απλώς μια βέλτιστη πρακτική, αλλά μια επιτακτική ανάγκη. Δεδομένης της αμετάβλητης φύσης των συναλλαγών blockchain, τα σφάλματα και τα τρωτά σημεία μπορούν να έχουν μη αναστρέψιμες συνέπειες. Στην παρούσα ενότητα αναφέρονται κοινές μεθοδολογίες δοκιμών που χρησιμοποιούνται στο Plutus, για να διασφαλιστεί η ακεραιότητα και η ευρωστία των έξυπνων συμβολαίων.

5.5.1 Δοκιμές μονάδας: Η πρώτη γραμμή άμυνας

Η δοκιμή μονάδας(unit testing) είναι μια τεχνική δοκιμής λογισμικού όπου μεμονωμένες μονάδες ή στοιχεία ενός λογισμικού δοκιμάζονται μεμονωμένα για να διασφαλιστεί ότι λειτουργούν όπως προβλέπεται, επομένως είναι πολύ χρήσιμες για τη δοκιμή έξυπνων συμβολαίων.

Η βιβλιοθήκη Simple Model Plutus είναι ειδικά σχεδιασμένη για δοκιμές μονάδας και χρησιμοποιεί μονάδες κατάστασης για την προσομοίωση του περιβάλλοντος blockchain. Η state monad χρησιμεύει ως ένα περιτύλιγμα γύρω από την κατάσταση της αλυσίδας μπλοκ, επιτρέποντας τη δοκιμή μιας ακολουθίας συναλλαγών ως προς την εγκυρότητά τους. Αυτό είναι ιδιαίτερα χρήσιμο για τη δοκιμή διαφόρων σεναρίων δαπανών, συμπεριλαμβανομένων των κανονικών δαπανών και των προσπαθειών διπλής δαπάνης.

Ακολουθεί ένα απόσπασμα από τις δοκιμές μονάδας του DataListing, το οποίο έχει σχεδιαστεί για να πιάνει την ευπάθεια διπλών δαπανών που συζητήθηκε προηγουμένως κατά την ανάλυση των έξυπνων συμβολαίων:

```
doubleSpending :: Run ()
doubleSpending = do
  (u1,u2) <- setupUsers

  -- Lock 2 tokens utxos, asking for 400 each
  let token = fakeValue scToken 1
  sp1 <- spend u1 token
  submitTx u1 $ lockingTx u1 400 sp1 token

  sp2 <- spend u1 token
  submitTx u1 $ lockingTx u1 400 sp2 token
  --
  -- Get the locked utxos
  scriptsUtxos <- utxoAt dataListingScript
  let ((ref1, out1), (ref2, out2)) = scriptsUtxos

  let buyerPaying = adaValue 400
  u2_sp <- spend u2 buyerPaying
  submitTx u2 $ doubleConsumingTx u2 u1 u2_sp buyerPaying (ref1,ref2) (txOutValue out1) (OnChain.DataListDatum u1 400)

  (v1,v2) <- mapM valueAt (u1,u2)
  -- If user 1 has only 400, this succeeds(logError does not run), and since it's a bad test, it will fail
  unless (v1 == adaValue 400 &&
    v2 == adaValue 600 <> fakeValue scToken 2)
    $ logError $ "Error occured. Received values: " ++ show (fmap flattenValue (v1,v2))
```

Σε αυτή τη δοκιμή, η λειτουργία doubleSpending έχει σχεδιαστεί για να προσομοιώνει ένα σενάριο όπου ένας πονηρός αγοραστής προσπαθεί να κάνει διπλά έξοδα αγοράζοντας 2 tokens, ενώ πληρώνει μόνο για 1. Σε αυτό το σενάριο ο Πωλητής(u1) έχει κάποια tokens και ο Αγοραστής(u2) έχει 1000 ΑΔΑ. Ο πωλητής προχωρά στη διάθεση των 2 tokens του για 400 ΑΔΑ το καθένα. Ο καταχραστής θα προσπαθήσει να καταναλώσει και τα δύο για 400 ΑΔΑ αντί για 800, οπότε αν τα καταφέρει, αναμένει ότι ο χρήστης1 θα έχει 400 ΑΔΑ, ενώ αυτός θα έχει 600 ΑΔΑ και 2 tokens. Έτσι, γράφουμε τη μέθοδο από την οπτική γωνία του καταχραστή και αργότερα ορίζουμε αυτή την περίπτωση δοκιμής ως ¨κακή¨, αναμένοντας να αποτύχει και να καταγράψει ένα σφάλμα, προκειμένου να περάσει η δοκιμή μας.

Αυτού του είδους οι δοκιμές διασφαλίζουν ότι η λογική του έξυπνου συμβολαίου αναγνωρίζει σωστά και προλαμβάνει αυτή την κακόβουλη δραστηριότητα, διασφαλίζοντας έτσι την ακεραιότητα των συναλλαγών.

Property Testing Αν και οι δοκιμές μονάδας είναι εξαιρετικές για τον εντοπισμό ειδικών σφαλμάτων, δεν επαρκούν για την απόδειξη της συνολικής αξιοπιστίας ενός έξυπνου συμβολαίου. Το Plutus υποστηρίζει επίσης δοκιμές ιδιοτήτων μέσω της βιβλιοθήκης QuickCheck της Haskell, η οποία παράγει αυτόματα περιπτώσεις δοκιμών για την επικύρωση των ιδιοτήτων του έξυπνου συμβολαίου. Αυτό προσθέτει ένα πρόσθετο επίπεδο διασφάλισης ότι το συμβόλαιο συμπεριφέρεται όπως αναμένεται σε ένα ευρύ φάσμα συνθηκών.

Οι δοκιμές αποτελούν απαραίτητο στοιχείο του κύκλου ζωής της ανάπτυξης των έξυπνων

συμβολαίων Plutus. Μέσω ενός συνδυασμού δοκιμών μονάδας και δοκιμών ιδιοτήτων, οι προγραμματιστές μπορούν να διασφαλίσουν ότι τα έξυπνα συμβόλαια είναι τόσο ασφαλή όσο και λειτουργικά, ενισχύοντας έτσι την εμπιστοσύνη και την αξιοπιστία στις dApps που είναι χτισμένες στην αλυσίδα μπλοκ Cardano.

Μέρος III

Ανάλυση

Κεφάλαιο 6

Αποτελέσματα και συζήτηση

6.1 Το μετασχηματιστικό δυναμικό των έξυπνων συμβολαίων

Μία από τις πιο εντυπωσιακές αποκαλύψεις κατά τη διάρκεια του έργου αυτού ήταν η αξιοσημείωτη ευελιξία και η μετασχηματιστική δυνατότητα των έξυπνων συμβολαίων. Στα παραδοσιακά συστήματα, η διαδικασία ανταλλαγής δεδομένων και οικονομικών συναλλαγών βασίζεται συχνά σε κεντρικούς μεσάζοντες, οι οποίοι μπορεί να είναι τόσο δαπανηροί όσο και λιγότερο ασφαλείς. Τα έξυπνα συμβόλαια, ωστόσο, προσφέρουν μια θεμελιώδη αλλαγή στον τρόπο με τον οποίο μπορούμε να αυτοματοποιήσουμε αυτές τις διαδικασίες σε ένα αποκεντρωμένο, χωρίς ανάγκης για εμπιστοσύνη περιβάλλον.

Στο πλαίσιο αυτού του έργου, τα έξυπνα συμβόλαια ανέλαβαν τον έλεγχο της διαδικασίας πληρωμών, εξαλείφοντας ουσιαστικά την ανάγκη για ένα έμπιστο τρίτο μέρος για την επίβλεψη των συναλλαγών. Αυτό όχι μόνο μειώνει τον κίνδυνο απάτης, αλλά και εξορθολογίζει την όλη διαδικασία, καθιστώντας την πιο αποτελεσματική και διαφανή.

Η αξιοπιστία των έξυπνων συμβολαίων είναι ιδιαίτερα επαναστατική. Γράφοντας με κώδικα τους κανόνες της συναλλαγής μέσα στο ίδιο το συμβόλαιο, μπορούμε να δημιουργήσουμε μια αυτοεκτελούμενη και αυτοεπιβεβαιούμενη συμφωνία, την οποία κανένα μέρος δεν μπορεί να αλλοιώσει μόλις αναπτυχθεί. Αυτό έχει βαθιές επιπτώσεις σε ένα ευρύ φάσμα εφαρμογών πέρα από τις αγορές δεδομένων, από τη διαχείριση της αλυσίδας εφοδιασμού έως την αποκεντρωμένη χρηματοδότηση (DeFi).

Το έργο αυτό χρησιμεύει ως απόδειξη ορισμένων από τις δυνατότητες των έξυπνων συμβολαίων και ανοίγει την πόρτα για να επανεξετάσουμε τον τρόπο με τον οποίο προσεγγίζουμε όχι μόνο τις συναλλαγές δεδομένων, αλλά και ένα πλήθος διαδικασιών που μπορούν να επωφεληθούν από την αποκέντρωση και την αυτοματοποίηση χωρίς να θυσιάζεται η ασφάλεια.

6.1.1 Τεχνικά επιτεύγματα και προκλήσεις

Mastery of Haskell and Plutus Ένα από τα πιο σημαντικά ορόσημα αυτού του έργου ήταν η απόκτηση άνεσης στην Haskell και το Plutus. Ενώ έχω ισχυρό υπόβαθρο σε γλώσσες λειτουργικού προγραμματισμού όπως η Standard ML (SML), η Haskell παρουσίασε μοναδικές προκλήσεις, ιδίως στην κατανόηση προηγμένων εννοιών όπως οι Μοναδς. Το πρόγραμμα Πλυτυς Πιονεερ Προγραμ από το IOHK ήταν καθοριστικό για τη γεφύρωση αυτού του χάσματος, παρέχοντας ουσιαστικές γνώσεις για την ανάπτυξη στο δίκτυο ἄρδανο. Πόροι όπως το βιβλίο "Learn You a Haskell for Great Good!", το οποίο διάβασα τουλάχιστον δύο φορές,

βοήθησαν σημαντικά στη μείωση της απότομης καμπύλης εκμάθησης της Haskell.

Ανάπτυξη επέκτασης προγράμματος περιήγησης Το αρχικό μου σχέδιο για την ενσωμάτωση ολόκληρης της αγοράς σε μια επέκταση προγράμματος περιήγησης έπρεπε να αναθεωρηθεί λόγω των περιορισμών του. Αυτοί οι περιορισμοί έγιναν εμφανείς κατά τη διάρκεια της ανάπτυξης, καθώς κατανόησα καλύτερα την αρχιτεκτονική και τα μέτρα ασφαλείας που υπαγορεύουν τις επεκτάσεις του προγράμματος περιήγησης. Ο ρόλος της επέκτασης περιορίστηκε στη συλλογή δεδομένων, καθιστώντας το σύστημα πιο ισχυρό και εστιασμένο.

Ασφάλεια έξυπνων συμβολαίων Η εφαρμογή και η δοκιμή των έξυπνων συμβολαίων ήταν καθοριστική για τη διασφάλιση της ακεραιότητας της αγοράς. Ο εντοπισμός ευπαθειών και η επιβεβαίωση του μετριασμού τους σε ζωντανά σενάρια, όπως η περίπτωση διπλής δαπάνης, ήταν σημαντικά επιτεύγματα.

6.1.2 Μελλοντικές κατευθύνσεις

Ενισχυμένη συλλογή δεδομένων Η τρέχουσα συλλογή δεδομένων αποτελεί απόδειξη της έννοιας και μπορεί να εμπλουτιστεί σημαντικά. Με την ενσωμάτωση βιβλιοθηκών ανάλυσης και τη συγκατάθεση των χρηστών, το σύστημα θα μπορούσε να καταγράφει πιο διαφοροποιημένα δεδομένα, όπως μοτίβα πλοήγησης των χρηστών και θερμικούς χάρτες πλοήγησης(Heat Maps).

Βελτιώσεις των έξυπνων συμβολαίων Αρκετές επεκτάσεις μπορούν να γίνουν στα έξυπνα συμβόλαια, όπως η ανάπτυξη επαναχρησιμοποιήσιμων scrips για τη μείωση του κόστους των τελών ανά συναλλαγή και η προσθήκη χρονικών συνθηκών για πιο σύνθετες αλληλεπιδράσεις. Επιπλέον, η τρέχουσα εφαρμογή περιορίζεται σε ένα μόνο token ανά συναλλαγή, το οποίο θα μπορούσε να βελτιστοποιηθεί ώστε να επιτρέπει πολλαπλά tokens ανά συναλλαγή.

Ενημερώσεις σε πραγματικό χρόνο στην dApp Η dApp θα μπορούσε να γίνει πιο δυναμική ενσωματώνοντας ενημερώσεις σε πραγματικό χρόνο μέσω web sockets ή συμβάντων που αποστέλλονται από τον διακομιστή(sse).

Κρυπτογράφηση από την πλευρά του πελάτη Η διερεύνηση της κρυπτογράφησης των δεδομένων που συλλέγονται από την πλευρά του πελάτη θα μπορούσε να αποκεντρώσει περαιτέρω την dApp. Ωστόσο, αυτό δημιουργεί προκλήσεις, καθώς η αποθήκευση μυστικών στην αλυσίδα μπλοκ δεν ενδείκνυται. Αυτό παραμένει ένας τομέας για μελλοντική έρευνα.

Βελτιστοποίηση των τελών Η τρέχουσα εφαρμογή θα μπορούσε να διδαχθεί από τη ροή προσφορών του JPG Store, η οποία επιτρέπει περισσότερες μεταφορές περιουσιακών στοιχείων ανά συναλλαγή, βελτιστοποιώντας την αμοιβή ανά καταβαλλόμενο περιουσιακό στοιχείο δεδομένων.

Αυτή η εφαρμογή έχει τη δυνατότητα να φέρει επανάσταση στον τρόπο με τον οποίο τα δεδομένα των χρηστών καταγράφονται και αξιολογούνται στον ιστό. Επί του παρόντος, οι χρήστες έχουν ελάχιστα κίνητρα για να συμφωνούν με τις συναινέσεις cookie- το σύστημα

αυτό θα μπορούσε να τους παρέχει απτά οφέλη, αλλάζοντας έτσι τη δυναμική της συγκατάθεσης και της συλλογής δεδομένων

Κεφάλαιο 7

Δεοντολογικές εκτιμήσεις

Το απόρρητο των δεδομένων αποτελεί κρίσιμο ζήτημα κατά την ανάπτυξη και την εξάπλωση αποκεντρωμένων εφαρμογών (dApps), ιδίως εκείνων που διαχειρίζονται ευαίσθητες πληροφορίες χρηστών. Η παρούσα ενότητα διερευνά τις ηθικές εκτιμήσεις που αφορούν την προστασία της ιδιωτικής ζωής των δεδομένων στο πλαίσιο των dApps, με έμφαση στη συγκεκριμένη περίπτωση μιας δΑπп που αποθηκεύει και πωλεί κρυπτογραφημένα δεδομένα πωλητών στο Διαπλανητικό Σύστημα Αρχείων (IPFS).

Ενημερωμένη συγκατάθεση Πριν από την αποθήκευση οποιωνδήποτε δεδομένων πωλητή, είναι ζωτικής σημασίας να λαμβάνεται ενημερωμένη συγκατάθεση από τους χρήστες. Η επέκταση του προγράμματος περιήγησης θα ήταν το ιδανικό μέρος για την απόκτηση συγκατάθεσης μετά από ενημέρωση, ιδίως επειδή είναι το σημείο αλληλεπίδρασης όπου γίνεται η αρχική καταγραφή των δεδομένων. Όταν ο χρήστης εγκαθιστά την επέκταση ή όταν χρησιμοποιεί για πρώτη φορά τη λειτουργία που καταγράφει το ιστορικό του προγράμματος περιήγησης, θα πρέπει να εμφανίζεται μια σαφής και εύκολα κατανοητή φόρμα συγκατάθεσης.

Σύμφωνα με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (ΓΚΠΔ), η συγκατάθεση ορίζεται ως ¨κάθε ελεύθερα δοθείσα, συγκεκριμένη, ενημερωμένη και σαφής ένδειξη της επιθυμίας του υποκειμένου των δεδομένων, με την οποία το υποκείμενο, με δήλωση ή με σαφή θετική ενέργεια, δηλώνει ότι συμφωνεί με την επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν¨ [19]. Αυτό περιλαμβάνει τη σαφή εξήγηση των δεδομένων που θα αποθηκευτούν, του τρόπου χρήσης τους και του ποιος θα έχει πρόσβαση σε αυτά. Η συγκατάθεση μετά από ενημέρωση δεν αποτελεί απλώς μια ηθική απαίτηση, αλλά και μια νομική απαίτηση βάσει κανονισμών όπως ο ΓΚΠΔ.

Κρυπτογράφηση Η κρυπτογράφηση των δεδομένων πριν από την αποθήκευσή τους στο IPFS προσθέτει ένα επιπλέον επίπεδο ασφάλειας, καθιστώντας δύσκολη την πρόσβαση στις πληροφορίες από μη εξουσιοδοτημένους χρήστες. Ωστόσο, η κρυπτογράφηση δεν είναι μια ασημένια σφαίρα και θα πρέπει να αποτελεί μέρος μιας ευρύτερης στρατηγικής προστασίας δεδομένων. Ευπάθειες μπορεί να προκύψουν από αδύναμους αλγορίθμους, κακή διαχείριση κλειδιών, ανθρώπινα λάθη και επιθέσεις ωμής βίας [20].

Ανωνυμοποίηση Όποτε είναι δυνατόν, η αποθήκευση των δεδομένων ανωνυμοποιημένων στο δίκτυο IPFS είναι μια καλή πρακτική για την προστασία της ταυτότητας των εμπλεκόμενων ατόμων.

Πολιτική διατήρησης δεδομένων Θα πρέπει να υπάρχει σαφής πολιτική διατήρησης δεδομένων, η οποία θα καθορίζει πόσο καιρό θα αποθηκεύονται τα δεδομένα και τι θα συμβαίνει με αυτά μετά την περίοδο αυτή. Αυτό είναι ιδιαίτερα σημαντικό για τη συμμόρφωση με το ¨δικαίωμα στη λήθη¨ σύμφωνα με το άρθρο 17 του ΓΚΠΔ

IPFS και απόρρητο δεδομένων Η αποθήκευση δεδομένων σε IPFS συνεπάγεται τις δικές της προκλήσεις και ευκαιρίες. Από τη μία πλευρά, η αποκεντρωμένη φύση του IPFS εξαλείφει τους κινδύνους που συνδέονται με τα κεντρικά συστήματα αποθήκευσης δεδομένων. Από την άλλη πλευρά, από τη στιγμή που τα δεδομένα βρίσκονται στο IPFS, παραμένουν εκεί μόνιμα, εκτός αν ληφθούν μέτρα για να καταστεί δυνατή η αφαίρεσή τους. Αξίζει να σημειωθεί ότι τα δεδομένα που δεν καρφιτσώνονται τακτικά μπορούν να υπόκεινται σε συλλογή σκουπιδιών σύμφωνα με το πρωτόκολλο IPFS. Αυτό σημαίνει ότι αν θέλετε να εξασφαλίσετε τη μακροζωία των δεδομένων σας, πρέπει να διαχειρίζεστε ενεργά την καρφίτσωσή τους. Αντίθετα, το ρητό ξεκαρφίτσωμα μπορεί να είναι μια μέθοδος για τη διευκόλυνση της αφαίρεσης δεδομένων, αν και αυτό δεν εγγυάται ότι άλλοι κόμβοι δεν έχουν ήδη αναπαράγει τα δεδομένα

Το απόρρητο των δεδομένων είναι ένα πολυσύνθετο ζήτημα που απαιτεί μια ολοκληρωμένη προσέγγιση, η οποία περιλαμβάνει συγκατάθεση μετά από ενημέρωση, κρυπτογράφηση, ανωνυμοποίηση και σαφή πολιτική διατήρησης δεδομένων. Ειδικές εκτιμήσεις απαιτούνται όταν χρησιμοποιούνται τεχνολογίες όπως η IPFS, οι οποίες έχουν τα δικά τους πλεονεκτήματα και μειονεκτήματα.

Μέρος IV

Επίλογος

Καθώς ολοκληρώνω αυτή τη διπλωματική, αξίζει να αφιερώσω λίγο χρόνο για να αναλογιστώ το ταξίδι που οδήγησε στην ολοκλήρωσή της. Η διαδικασία ανάπτυξης μιας αποκεντρωμένης εφαρμογής για την αγορά δεδομένων ήταν τόσο προκλητική όσο και διαφωτιστική, προσφέροντας πολυάριθμα μαθήματα που επεκτείνονται πέρα από το τεχνικό πεδίο.

Η εργασία που παρουσιάζεται στην παρούσα διπλωματική δεν είναι απλώς μια τεχνική άσκηση, αλλά ένα βήμα προς την επανεξέταση του τρόπου με τον οποίο προσεγγίζουμε την ιδιωτικότητα και την ιδιοκτησία των δεδομένων στην ψηφιακή εποχή. Αξιοποιώντας την τεχνολογία blockchain και τα έξυπνα συμβόλαια, μπορούμε να οραματιστούμε ένα μέλλον όπου ο έλεγχος των προσωπικών δεδομένων επιστρέφει στο άτομο, διαταράσσοντας τα παραδοσιακά μοντέλα χρηματικοποίησης δεδομένων και συναίνεσης.

Οι προκλήσεις που αντιμετωπίστηκαν κατά τη διάρκεια αυτού του έργου, από την εκμάθηση της Haskell και του Plutus μέχρι την πλοήγηση στις πολυπλοκότητες των αποκεντρωμένων συστημάτων, ήταν ανεκτίμητες εμπειρίες μάθησης. Δεν τελειοποίησαν μόνο τις τεχνικές μου δεξιότητες, αλλά και εμβάθυναν την κατανόηση των ηθικών και κοινωνικών διαστάσεων της τεχνολογίας.

Για όποιον ξεκινάει ένα παρόμοιο ταξίδι, η συμβουλή μου θα ήταν να αγκαλιάσει τις προκλήσεις ως ευκαιρίες για ανάπτυξη. Το ταχέως εξελισσόμενο τοπίο της τεχνολογίας blockchain προσφέρει ένα γόνιμο έδαφος για καινοτομία, αλλά απαιτεί επίσης προθυμία προσαρμογής και συνεχούς μάθησης.

Σε έναν κόσμο που καθοδηγείται όλο και περισσότερο από τα δεδομένα, η ανάγκη για ασφαλή, διαφανή και δίκαια συστήματα ανταλλαγής δεδομένων είναι πιο επιτακτική από ποτέ. Η παρούσα διπλωματική χρησιμεύει ως απόδειξη των δυνατοτήτων που προκύπτουν όταν η τεχνολογία ευθυγραμμίζεται με αυτές τις αρχές. Παρόλο που υπάρχει ακόμη πολλή δουλειά να γίνει, τόσο για τη βελτίωση του τρέχοντος συστήματος όσο και για τη διερεύνηση νέων εφαρμογών, η πορεία προς τα εμπρός είναι πολλά υποσχόμενη.

Παραρτήματα

Παράρτημα Α΄

Κώδικας

Ο κώδικας που αναπτύχθηκε για την υλοποίηση της παρούσας διπλωματικής εργασίας είναι διαθέσιμος στον παρακάτω σύνδεσμο: https://github.com/varagos/data-sail.

Βιβλιογραφία

[1] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. Available online.

[2] M. N. Bhutta, A. Khwaja, A. Nadeem, H. F. Ahmad, M. Khan, M. Hanif, H. Song, M. A. Alshamari και Y. Cao. *A Survey on Blockchain Technology: Evolution, Architecture and Security*. *IEEE Access*, 2021. Available as PDF.

[3] H. Liu, R. G. Crespo και O. S. Martínez. *Enhancing Privacy and Data Security across Healthcare Applications Using Blockchain and Distributed Ledger Concepts*. 2020.

[4] Nicola Atzei, Massimo Bartoletti, Stefano Lande και Roberto Zunino. *A formal model of Bitcoin transactions*, 2017. Paper 2017/1124.

[5] M. M. T. Chakravarty, J. Chapman, K. MacKenzie, O. Melkonian, M. Peyton Jones και P. Wadler. *The Extended UTXO Model*. 2020.

[6] L. Brünjes, M. Gabbay και others. *UTxO- vs account-based smart contract blockchain programming paradigms*. 2020.

[7] Wikipedia. *Halting problem*. https://en.wikipedia.org/wiki/Halting_problem. Accessed: 18-10-2023.

[8] M. M. T. Chakravarty, J. Chapman, K. MacKenzie, O. Melkonian, J. Müller, M. Peyton Jones, P. Vinogradova και P. Wadler. *Native Custom Tokens in the Extended UTXO Model*.

[9] *Plutus Documentation - Parameterized contracts*. https://plutus-pioneer-program.readthedocs.io/en/latest/pioneer/week3.html#example-2-parameterized-contract. Accessed: 18-10-2023.

[10] IOHK. *The Plutus Platform Technical Report*. https://ci.iog.io/build/1231235/download/1/plutus.pdf. Accessed: 13-10-2023.

[11] Cardano Documentation. *Collateral Mechanism*. https://docs.cardano.org/plutus/collateral-mechanism/. Accessed: 13-10-2023.

[12] M. M. Wachs, M. Hoque και M. Vukolić. *Decentralized Applications: The Blockchain-Empowered Software System*. 2018.

[13] J. Benet. *IPFS - Content Addressed, Versioned, P2P File System*. Original IPFS white paper.

[14] D. Trautwein, A. Raman, G. Tyson, I. Castro, W. Scott, M. Schubotz, B. Gipp και Y. Psaras. *Design and Evaluation of IPFS: A Storage Layer for the Decentralized Web*. *Association for Computing Machinery*, 2022.

[15] Joshua Stone. *Book.io Whitepaper*, 2023. Available online.

[16] Google. *Content Security Policy (CSP)*. https://developer.chrome.com/docs/extensions/mv3/manifest/content_security_policy/. Accessed: 13-10-2023.

[17] Google. *Extensions 101*. https://developer.chrome.com/docs/extensions/mv3/getstarted/extensions-101/. Accessed: 17-10-2023.

[18] Google. *Architecture overview*. https://developer.chrome.com/docs/extensions/mv3/architecture-overview/.

[19] European Union. *GDPR Article 4(11)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679, 2016.

[20] M. Mohan, M. Devi και V. Prakash. *Security Analysis and Modification of Classical Encryption Scheme*. https://www.ijstr.org/final-print/apr2015/Security-Analysis-And-Modification-Of-Classical-Encryption-Scheme.pdf, 2015.

Συντομογραφίες - Αρκτικόλεξα - Ακρωνύμια

Απόδοση ξενόγλωσσων όρων

Απόδοση	Ξενόγλωσσος όρος