Πανεπιστημιο Μακεδονιας

Σχολη Επιστημων Πληροφοριας

Τμημα Εφαρμοσμενης Πληροφορικης

Τίτλος

Επαλήθευση εγκυρότητας ακαδημαϊκών τίτλων με χρήση της τεχνολογίας **Blockchain**

Πτυχιακή Εργασία

Γεώργιος Μιχούλης

Επίβλεψη

Επίκουρη Καθηγήτρια, Σοφία Πετρίδου

Θεσσαλονίκη, 25 Οκτωβρίου 2020

Ευχαριστίες

Για την εκπόνηση αυτής της εργασίας θα ήθελα να ευχαριστήσω θερμά την επιβλέπουσα Καθηγήτρια μου κ. Πετρίδου Σοφία για την πολύτιμη βοήθεια της, τις συμβουλές της, την υπομονή και την υποστήριξη που επέδειξε σε όλο αυτό το διάστημα, καθώς και τον Καθηγητή κ. Βεργίδη Κωνσταντίνο, αφού η συμβολή του στην εκπόνηση και την τελική μορφή της παρούσας εργασίας ήταν πολύ βοηθητική και παραγωγική.

Επίσης, θα ήθελα να ευχαριστήσω την οικογένεια μου που με στήριξε σε όλες τις προσπάθειες μου όλα αυτά τα χρόνια.

Πρόλογος

Το ολοένα και αυξανόμενο ενδιαφέρον γύρω από τα θέματα ασφαλείας στο Διαδίκτυο, απασχολεί ολοένα και περισσότερο τον κόσμο, αλλά και η εξέλιξη της επιστήμης της κρυπτογραφίας που στρέφει το ενδιαφέρον των μελετητών για την διατήρηση της ασφάλειας, δημιούργησαν την τεχνολογία blockchain. Το 2008 ο Satoshi Nakamoto δημοσίευσε το άρθρο του Bitcoin για προτείνει ένα νέο τρόπο συναλλαγών, με συμμετέχοντες που δεν μπορεί να εμπιστευτεί ο ένας τον άλλον. Η ραγδαία ανάπτυξη των εφαρμογών του Διαδικτύου, ο τεράστιος όγκος δεδομένων και η επιτακτική ανάγκη της προστασίας και διαφύλαξης των συναλλαγών του χρήστη, κάνει πιο επιτακτική την ανάγκη για την χρήση του blockchain.

Η βασική διάρθρωση της παρούσας πτυχιακής εργασίας εστιάζει στην μελέτη της τεχνολογίας blockchain, με στόχο την κατανόηση της τόσο σε θεωρητικό, όσο και σε πρακτικό επίπεδο. Πιο συγκεκριμένα, η παρούσα εργασία έχει ως στόχο να κάνει κατανοητή με παραστατικό τρόπο την τεχνολογία blockchain και τον τρόπο που αυτήν λειτουργεί. Για αυτόν τον λόγο το Κεφάλαιο 2 περιγράφει το υπόβαθρο της κρυπτογραφίας του blockchain, ώστε να μελετηθούν τα μαθηματικά πίσω από αυτήν την τεχνολογία και αυτό επιτυγχάνεται με την πρακτική εφαρμογής τους στο λογισμικό ανοιχτού κώδικα Sage. Ακολουθεί το Κεφάλαιο 3, που περιγράφει την δομή του blockchain, το πως χρησιμοποιούνται τα κρυπτοσυστήματα του προηγούμενου κεφαλαίου και εισάγει έννοιες όπως οι συναλλαγές, αλλά παραθέτει και την δομή του μπλοκ, την αλυσιδωτή σύνδεση των μπλοκ και την έννοια της διακλάδωσης (forking). Επίσης, στόχος του συγκεκριμένου Κεφαλαίου είναι να οριοθετήσει την τεχνολογία του blockchain με το Bitcoin, παρόλο που το πρότυπο που περιγράφεται είναι το πρότυπο του blockchain το οποίο προέρχεται από το Bitcoin αλλά η τεχνολογία αυτή δεν περιορίζεται μόνο στον οικονομικό τομέα.

Στο Κεφάλαιο 4 περιγράφονται τα πιο γνωστά μοντέλα συναίνεσης και γίνεται μία σύγκριση μεταξύ τους, με σκοπό την έρευνα. Επειδή όμως, το Bitcoin δεν είναι το μοναδικό blockchain, το Κεφάλαιο 5 εστιάζει στο Ethereum, την δομή του και την αφαιρετική του σύγκριση με το Bitcoin, καθώς επίσης, παρατίθενται και η τεχνολογία των ψηφιακών πορτοφολιών, των έξυπνων συμβολαίων και μερικών παραδειγμάτων αποκεντρωμένων εφαρμογών.

Το πρόβλημα της πλαστογραφίας των ακαδημαϊκών τίτλων που ανησυχεί την σύγχρονη κοινωνία, σε συνδυασμό με τις παραπάνω γνώσεις, μας οδήγησαν στην δημιουργία του Κεφαλαίου 6, στο οποίο δημιουργείται και υλοποιείται η διαδικτυακή αποκεντρωμένη εφαρμογή Verde. Η συγκεκριμένη εφαρμογή λειτουργεί ως εργαλείο για την αντιμετώπιση της πλαστογράφησης των ακαδημαϊκών τίτλων με την χρήση του Ethereum blockchain. Έτσι, σε αυτό το Κεφάλαιο περιγράφεται η αρχιτεκτονική της εφαρμογής μας, ο τρόπος λειτουργίας της με την χρήση και υλοποίηση έξυπνων συμβολαίων, με την χρήση του ψηφιακού πορτοφολιού Metamask και με την υλοποίηση των δύο διεπαφών, α) της καταχώρησης των δεδομένων του φοιτητή και β) της επαλήθευσης των δεδομένων του φοιτητή. Το Κεφάλαιο καταλήγει με την σύγκριση της Verde με άλλες δέκα παρόμοιες εφαρμογές, αλλά επίσης, συγκρίνεται

και η ίδια πλατφόρμα του Ethereum, με την αντίστοιχη πλατφόρμα εκτέλεσης έξυπνων συμβολαίων του Bitcoin, RSK και αναλύεται ποια πλατφόρμα είναι καλύτερη για την ανάπτυξη της εφαρμογής Verde.

Συνοψίζοντας, η συνεισφορά της παρούσας πτυχιακής εντοπίζεται κατά κύριο λόγο τόσο στο επίπεδο της μελέτης της τεχνολογίας, όσο και στην έρευνα και την υλοποίηση μιας αποκεντρωμένης εφαρμογής που θα έχει ως απώτερο σκοπό την αποτροπή και αντιμετώπιση της πλαστογράφησης των ακαδημαϊκών τίτλων. Έτσι, η παρούσα μελέτη διαθέτει, βιβλιογραφική έρευνα, έρευνα με συγκριτική μέθοδο και επεκτείνεται στο επίπεδο προγραμματιστικής εφαρμογής.

Λέξεις κλειδιά: Blockchain, Bitcoin, Ethereum, Έξυπνα συμβόλαια, Συναρτήσεις Διασποράς, Ελλειπτικές Καμπύλες, Merkle Tree, Αποκεντρωμένες Εφαρμογές, Ψηφιακά Πορτοφόλια, Αντιμετώπιση Πλαστογράφησης Πτυχίων.

Abstract

The explosion of interest around internet security issues is increasing concern to the world, but also the evolution of cryptography science that increases the interest of scholars in maintaining security, created the technology blockchain. In 2008 Satoshi Nakamoto published the article of Bitcoin to propose a new way of trading, with participants who cannot trust each other. The rapid development of Internet applications, the huge amount of data and the imperative of protecting and safeguarding the user's transactions makes the need for the use of blockchain.

The structure of this thesis focuses on the study of blockchain, with the aim of understanding it both in theory and in practical terms. The reason we quote Chapter 2 with the background of cryptography of blockchain, so that to understanded the mathematics behind this technology and this is achieved by their practical application in open source software Sage. The Chapter 3 follows, which aims to understand the structure of blockchain and how the cryptosystems of the previous chapter are used. It introduces us to concepts such as transactions, but also lists us with the structure of the block, the blockchain and the concept of blockchain.

Chapter 4 describes the most well-known models of consent and a comparison is made with a view to researching and condensing knowledge. However, because Bitcoin is not the only blockchain, Chapter 5 focuses on Ethereum, its structure and abstract comparison with Bitcoin, as well as the technology of digital wallets, smart contracts and some examples of decentralized applications.

The problem of forgery of academic titles that conecerns modern society, combined with the above knowledge led us to the creation of Chapter 6, in which the web decentralized application Verde is created and implemented. This application acts as a tool to combat the spoofing of academic titles by using Ethereum blockchain. Thus, this Chapter describes the architecture of our application, the way it works by using and implementing smart contracts using the digital wallet Metamask and the implementation of the two interfaces, a) the registration of the student's data and b) the verification of the student's data. The Chapter concludes by comparing Verde with ten other similar applications, but also compares the same platform of Ethereum, with the corresponding platform for the execution of smart contracts of Bitcoin, RSK and analyzes which platform is best for the development of the Verde application.

To sum up, the contribution of this thesis is primarily identified both at the level of the study and education of the technology, as well as in the research and implementation of a decentralised implementation aimed to prevent and deterrence of the forgery of academic qualifications. Thus, this study has bibliographic research, comparative research and extends to the level of programming application.

Keywords: Blockchain, Bitcoin, Ethereum, Smart Contracts, Scatter Functions, El-

liptical Curves, Merkle Tree, Decentralized Applications, Digital Wallets, Face Forging Degree

Περιεχόμενα

Κατάλογος Πινάκων

Κατάλογος Σχημάτων

Κεφάλαιο 1

Εισαγωγή

Η παρούσα εργασία μελετά την τεχνολογία Blockchain, τα κρυπτοσυστήματα που σχετίζονται με αυτήν την τεχνολογία, με τη βοήθεια λογισμικού ανοιχτού κώδικα και τελικά αναπτύξαμε μια πρόταση για την αντιμετώπιση της πλαστογράφησης ακαδημαϊκών τίτλων με την χρήση της τεχνολογίας αυτής, δηλαδή την εφαρμογή Verde. Αρχικά, θα ορισθούν βασικές έννοιες της κρυπτογραφίας και του κατάλληλου μαθηματικού υπόβαθρου, στην συνέχεια θα εξηγήσουμε την δομή του blockchain, τα μοντέλα συναίνεσης κάτω από τα οποία λειτουργούν τα διαφορετικά blockchain και τέλος δημιουργήσαμε μια αποκεντρωμένη εφαρμογή και την συγκρίναμε με παρόμοιες μελέτες. Μετά από μια σύντομη αναφορά των σύγχρονων κρυπτοσυστημάτων που χρησιμοποιούνται από το blockchain, θα εστιάσουμε το ενδιαφέρον μας στην ίδια. Κύριο άξονα μελέτης θα αποτελέσει η αφαιρετική δομή του πρώτου blockchain, δηλαδή του Bitcoin. Στην συνέχεια θα συγκρίνουμε το μοντέλο συναίνεσης του με άλλα πιο πρόσφατα μοντέλα. Επίσης, υπάρχει η επεξήγηση του Ethereum blockchain και των έξυπνων συμβολαίων του, μια αφαιρετική σύγκριση με το πρώτο blockchain και η υλοποίηση της πρότασης μας στο blockchain αυτό.

Η ετυμολογική ανάλυση της λέξης blockchain προέρχεται από τις "σύνθετες" λέξεις "block" & "chain" και αποδίδει τη σημασία της έννοιας, δηλαδή μία άρρηκτη αλυσίδα από μπλοκ. Αυτό σημαίνει ότι τα μπλοκ τα οποία περιέχουν συναλλαγές, συνδέονται το ένα μπλοκ με το άλλο, με κρυπτογραφημένες πληροφορίες, οι οποίες είναι πολύ δύσκολο να παραβιαστούν, καθώς βασίζονται στις συναρτήσεις διασποράς (hash functions). Το blockchain είναι μια από τις τεχνολογίες που θα ανθίσουν στην 4η βιομηχανική επανάσταση. Η επιστήμη της Κρυπτογραφίας σχετίζεται με τη σπουδή μαθηματικών τεχνικών που έχουν σκοπό να εξασφαλίζουν την ασφαλή μετάδοση της πληροφορίας μέσω ανασφαλών διαύλων επικοινωνίας. Αυτός είναι και ο λόγος της ύπαρξης του αποκεντρωμένου χαρακτήρα που έχει το blockchain με τέτοιο τρόπο ώστε, να μην υπάρχει μια κεντρική αρχή για να ελέγχει τις συναλλαγές του. Ουσιαστικά το blockchain αποτελεί ένα αποκεντρωμένο δίκτυο κατάστιχων (decentralized ledgers) και οι κόμβοι επικοινωνούν μεταξύ τους ομότιμα peer-to-peer. Δεν υπάρχει κάποιο gateway μεταξύ των κόμβων και του blockchain καθώς, η επικοινωνία μεταξύ του δικτύου έχει την μορφή του torrent. Ο στόχος του blockchain είναι η επικοινω-

νία, η συναλλαγή και η αποθήκευση δεδομένων μεταξύ μη έμπιστων κόμβων που λειτουργεί αποκεντρωμένα, δηλαδή, δεν υπάρχει τρίτη οντότητα για να ελέγχει το δίκτυο.

Οι βασικές ιδέες αναφορικά με την τεχνολογία blockchain προέκυψαν στα τέλη της δεκαετίας του 1980 και στις αρχές της δεκαετίας του 1990. Το 1989, ο Leslie Lamport ανέπτυξε το πρωτόκολλο Paxos και το 1990 υπέβαλε το έγγραφο "Το Κοινοβούλιο μερικής απασχόλησης στις Συναλλαγές *ACM* για Συστήματα Υπολογιστών" [19], το οποίο έγγραφο δημοσιεύθηκε τελικά σε ένα τεύχος του 1998. Το έγγραφο περιγράφει ένα μοντέλο συναίνεσης για την επίτευξη συμφωνίας σχετικά με ένα αποτέλεσμα σε ένα δίκτυο υπολογιστών όπου οι υπολογιστές ή το ίδιο το δίκτυο μπορεί να είναι αναξιόπιστο. Το 1991, μια αλυσίδα πληροφοριών χρησιμοποιήθηκε ως ηλεκτρονικός κατάλογος για ψηφιακή υπογραφή εγγράφων με τρόπο που θα μπορούσε εύκολα να δείξει ότι κανένα από τα υπογεγραμμένα έγγραφα της συλλογής δεν είχε αλλάξει. Αυτές οι έννοιες συνδυάστηκαν και εφαρμόστηκαν στις ηλεκτρονικές πληρωμές το 2008 και περιγράφηκαν στο έγγραφο Bitcoin: Ένα Peer-to-Peer Ηλεκτρονικό Νομισματικό Σύστημα, το οποίο δημοσιεύθηκε (με ψευδώνυμο) από τον Satoshi Nakamoto, και αργότερα το 2008 με την ίδρυση του δικτύου κρυπτονομισμάτων Bitcoin blockchain [20].

Η ιδέα του Blockchain του Satoshi Nakamoto είναι και η λύση του Byzantine Generals Problem [21]. Το πρόβλημα των Στρατηγών θα γίνει πιο κατανοητό μέσα από ένα παράδειγμα: κάθε στρατηγός έχει το δικό του στρατό και βρίσκεται σε διαφορετικές τοποθεσίες γύρω από την πόλη που πολιορκούν. Οι στρατηγοί πρέπει να συμφωνήσουν είτε σε επίθεση, είτε σε υποχώρηση. Δεν έχει σημασία αν θα επιτεθούν ή υποχωρήσουν αρκεί όλοι οι στρατηγοί να καταλήξουν σε συναίνεση. Επομένως, επικοινωνούν δια αλληλογραφίας ο ένας με τον άλλον για να αποφασίσουν την επόμενη κίνηση τους, όμως δεν γνωρίζουν αν το μήνυμα που στέλνουν ή δέχονται είναι γνήσιο. Η λύση του Nakamoto χρησιμοποιεί τις συναρτήσεις διασποράς (hash functions) και την τυχαία τιμή μοναδικής χρήσης (nonce). Οπότε, ο Α στρατηγός θα στείλει στον Β ένα μήνυμα για επίθεση, το οποίο θα περιλαμβάνει το κείμενο (plaintext) και το κατάλληλο nonce, τέτοιο ώστε η σύνοψη των δύο (hash) να ικανοποιεί το κριτήριο (hash target) που έθεσε ο Β. Στη συνέχεια ο Β υπολογίζει την ίδια σύνοψη και εφόσον ικανοποιεί το κριτήριο που ίδιος έθεσε αποδέχεται το μήνυμα του Α ως αυθεντικό. Η διαδικασία που ακολουθεί ο Α στρατηγός ονομάζεται απόδειξη εργασίας (proof of work) [22] και απαιτεί μεγάλη υπολογιστική ισχύ. Στην περίπτωση που είχαμε πολλούς Α, οι Α θα εναπόθεταν τα μηνύματα τους σε ένα «μπλοκ» και θα έβρισκαν ένα μοναδικό nonce για όλο το μπλοκ που θα συνοψίσουν. Πριν την σύνοψη όμως ο Nakamoto πρότεινε να προστεθούν και άλλα στοιχεία στο μπλοκ για να γίνει πιο ισχυρή η επαλήθευσή του και δύσκολος ο υπολογισμός της σύνοψης, ένα από αυτά είναι η σύνοψη του προηγούμενου μπλοκ. Έτσι δημιουργείται μια αλυσίδα από μπλοκ, το blockchain, που δεν μπορεί να παραποιηθεί.

Έναν ελλιπή ορισμό που θα μπορούσαμε να δώσουμε στο blockchain είναι:

Το blockchain, είναι ένα κατανεμημένο σύστημα ομότιμων κόμβων που χρησιμοποιεί έναν αλγόριθμο, ο οποίος χειρίζεται τις πληροφορίες που

υπάρχουν μέσα σε ταξινομημένα και συνδεδεμένα μπλοκ δεδομένων με τη χρήση κρυπτογραφίας και της ασφάλειας υπολογιστών, έχοντας ως σκοπό την ακεραιότητα των πληροφοριών αυτών και την διατήρηση της [23].

Το blockchain είναι μια τεχνολογία με πολλές εφαρμογές σήμερα και είναι σημαντικό να αναφέρουμε τα κύρια δίκτυα που υπάρχουν σήμερα, αυτά είναι το Bitcoin, το Litecoin, το Ripple, το Ethereum, το Hyperledger.

Bitcoin Το Bitcoin είναι ένα ψηφιακό σύστημα χρημάτων και είναι το πρώτο σύστημα που χρησιμοποίησε τεχνολογία blockchain. Τα νέα μπλοκ δημιουργούνται περίπου μία φορά κάθε 10 λεπτά χρησιμοποιώντας τη συνάρτηση διασποράς τύπου SHA-256 για την μεταξύ τους σύνδεση. Χρησιμοποιεί το μοντέλο συναίνεσης PoW, όπου οι κόμβοι εξόρυξης miners πρέπει να βρουν μια τυχαία τιμή μοναδικής χρήσης (nonce) για να προσθέσουν στο νέο μπλοκ, έτσι ώστε η τιμή διασποράς του μπλοκ να είναι μικρότερη από κάποια προκαθορισμένη τιμή δυσκολίας. Η δυσκολία προσαρμόζεται προς τα πάνω ή προς τα κάτω, προκειμένου να επιτευχθεί ο στόχος των 10 λεπτών, για τη δημιουργία μπλοκ. Στο Bitcoin, η πληρωμή των φόρων από τις συναλλαγές είναι πολύ μικρή καθώς το μεγαλύτερο μέρος των κεφαλαίων τους το λαμβάνουν με τη δημοσίευση νέων μπλοκ. Αυτός ο φόρος έχει σχεδιαστεί για να χρεώνει ένα μικρό ποσό για κάθε συναλλαγή, που όμως ενδέχεται και να μεγαλώσει, εξαιτίας της καθυστέρησης των εκκρεμών συναλλαγών. Η πληρωμή υψηλότερου φόρου συναλλαγής μπορεί να δώσει μεγαλύτερη προτεραιότητα σε μία συναλλαγή για να προστεθεί στο blockchain. Αρχικά, οι κόμβοι εξόρυξης έπαιρναν 50 Bitcoin για κάθε μπλοκ. Τον Ιούλιο του 2016 το κόστος για την εξόρυξη ενός μπλοκ ήταν 12,5 Bitcoins και από τον Μάιο του 2020 είναι 6,5 Bitcoins λόγω του halving. Σύμφωνα με το πρωτόκολλο, αυτή η ανταμοιβή μειώνεται κατά το ήμισυ σε κάθε 210.000 μπλοκ (περίπου τέσσερα χρόνια) και θα μηδενιστεί μόλις δημιουργηθούν 21 εκατομμύρια Bitcoins. Η εξόρυξη Bitcoin θα συνεχιστεί σε αυτό το σημείο, αλλά η ανταμοιβή θα προέρχεται εξ ολοκλήρου από τα τέλη συναλλαγών. Τέλος, συναλλαγή Bitcoin περιέχει κώδικα γραμμένο σε γλώσσα Script. Οι συναλλαγές Bitcoin σήμερα χρησιμοποιούν μόνο ένα μικρό μέρος των διαθέσιμων λειτουργιών του Script. Πρακτικά οι περισσότερες συναλλαγές Bitcoin χρησιμοποιούν πολύ λίγο κώδικα Script για την κίνηση κεφαλαίων μεταξύ των μερών [1].

Litecoin Το Litecoin είναι παρόμοιο με το Bitcoin, αλλά έχει ως στόχο να παρέχει ταχύτερους χρόνους επιβεβαίωσης. Το Litecoin έχει εφαρμόσει το SegWit, διαιρώντας τις συναλλαγές σε δύο τμήματα και κρύβοντας ένα αυξημένο μέγεθος μπλοκ. Η υπογραφή ¨μάρτυρας' διαχωρίζεται από το δέντρο Merkle. Μια άλλη διαφορά μεταξύ του Bitcoin και του Litecoin είναι ότι το Litecoin χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης Script για τη διασπορά αντί του SHA-256. Ο αλγόριθμος Script είναι πιο δύσκολο να επιλυθεί από το SHA-256, επειδή χρησιμοποιεί περισσότερη μνήμη, γεγονός που καθιστά πιο δύσκολη την

ανάπτυξη ολοκληρωμένων κυκλωμάτων ειδικά προσαρμοσμένων στις εφαρμογές. Υπάρχει μεγαλύτερος αριθμός νομισμάτων που μπορούν να εξορύσσονται (84 εκατομμύρια Litecoins). Το Litecoin λειτουργεί συμπληρωματικά προς το Bitcoin, με μεγαλύτερους όγκους συναλλαγών και δεν έχει σχεδιαστεί για να το αντικαταστήσει [1] καθώς, αυτό αφορά καθημερινές συναλλαγές.

Ripple Ο στόχος του Ripple είναι η αξιοποίηση του Bitcoin και η ταυτόχρονη σύνδεση των διαφορετικών συστημάτων πληρωμών. Έχει σταθερή προσφορά 100 δισεκατομμυρίων XRP, από τα οποία τα μισά προορίζονται για κυκλοφορία. Οι πελάτες δεν χρειάζεται να κατεβάζουν ολόκληρο το blockchain, καθώς εύκολα μπορούν να συμμετάσχουν σε δευτερόλεπτα. Επιπλέον, δεν υπάρχει ανταμοιβή για την εξόρυξη, επειδή η συναλλαγή κοστίζει μια μικρή ποσότητα Ripple, παρόμοια με το αέριο Ethereum [1].

Ethereum Το Ethereum είναι μια πλατφόρμα που εστιάζει στην εκτέλεση έξυπνων συμβολαίων. Τα έξυπνα συμβόλαια είναι προγράμματα που υπάρχουν στο blockchain, στα οποία μπορούν να έχουν πρόσβαση οι χρήστες του Ethereum. Έχουν τη δυνατότητα τόσο να λαμβάνουν όσο και να στέλνουν κεφάλαια κατά την εκτέλεση υπολογισμών. Το συμβόλαιο μπορεί να λειτουργήσει ως ένας αξιόπιστος τρίτος στις συναλλαγές, καθώς ο κώδικας είναι δημόσιος. Επίσης, χρησιμοποιεί Turing complete γλώσσα προγραμματισμού (π.χ. Solidity). Οι κόμβοι λαμβάνουν ανταμοιβές μέσω των φόρων εξόρυξης αλλά και της συναλλαγής. Το Ethereum περιλαμβάνει επίσης μια έννοια που ονομάζεται ¨αέριο' - gas που χρησιμοποιείται ως ανταμοιβή για την πραγματοποίηση υπολογισμών για ένα συμβόλαιο. Υπάρχει ένα μέγιστο όριο αερίου ανά έξυπνο συμβόλαιο. Αυτό οφείλεται στο γεγονός ότι όλοι οι κόμβοι εξόρυξης πρέπει να εκτελούν τις συναλλαγές παράλληλα. Η κατάσταση που δημιουργείτε από την εκτέλεση του συμβολαίου αποθηκεύεται στο blockchain από το χρήστη που δημοσιεύει το επόμενο μπλοκ. Επίσης, το 2015, το Ethereum δέχτηκε ένα DAO hack, με αποτέλεσμα να γίνει ένα hard fork. Πολλοί χρήστες απέρριψαν το hard fork, με αποτέλεσμα να δημιουργηθεί μια νέα πλατφόρμα, το Ethereum Classic, που ουσιαστικά συνεχίζει να λειτουργεί την πλατφόρμα του Ethereum πριν αυτό ακόμα κάνει το fork.

Hyperledger Το Hyperledger συνιστά ομάδα έργων που αποσκοπούν στη δημιουργία κατανεμημένων κατάστιχων. Το Hyperledger φιλοξενείται και υποστηρίζεται από τη Linux Foundation. Υπάρχουν πολλές πλατφόρμες blockchain που χρησιμοποιούν Hyperledgerκαι το καθένα από αυτά επιλύει συγκεκριμένα προβλήματα. Υπάρχουν πολλών τύπων Hyperledger, όπως [1]

- Fabric. Πρόκειται για ένα permissioned blockchain που μπορεί να εκτελέσει έξυπνα συμβόλαια (chaincode). Δημιουργήθηκε από τη Digital Asset και την IBM.

- Sawtooth. Πρόκειται για ένα κατανεμημένο σύστημα που χρησιμοποιεί ως μοντέλο συναίνεσης το PoET. Κάθε συμμετέχων σε αυτό το σύστημα ζητά ένα χρόνο "αναμονής" από ένα υλικό,το οποίο κατανέμει τυχαία τις ώρες αναμονής. Όποιος συμμετέχων πετυχαίνει το συντομότερο χρονικό διάστημα, δημιουργεί το επόμενο μπλοκ στην αλυσίδα. Το Sawtooth το δημιούργησε η Intel.

- Iroha. Λειτουργεί ως υπηρεσία ταυτότητας "Know Your Customer" (KYC) χρησιμοποιώντας την τεχνολογία blockchain, η οποία επιτρέπει στα ιδρύματα να μοιράζονται δεδομένα και να διαχειρίζονται τις ταυτότητες. Δημιουργήθηκε από τους Soramitsu, Hitachi, NTT Data and Colu.

- Burrow. Είναι πλατφόρμα του τρέχει τα έξυπνα συμβόλαια. Αποδέχεται τον κώδικα των έξυπνων συμβολαίων του Ethereum. Δημιουργήθηκε από την Monax και συγχρηματοδοτήθηκε από την Intel.

- Indy. Πρόκειται για μια ανεξάρτητη πλατφόρμα που παρέχει στοιχεία για τις ασφαλείς συναλλαγές και ψηφιακές ταυτότητες. Υποστηρίζει τρεις σημαντικές λειτουργίες απορρήτου:, α) τα Αποκεντρωμένα αναγνωριστικά στοιχεία (DID), β) δείκτες σε πηγές εκτός κατάστιχου, έτσι ώστε να μην εγγράφονται προσωπικά δεδομένα στο κατάστιχο και τέλος γ) zero-knowledge-proofs.Δημιουργήθηκε από το Ίδρυμα Sovrin.

1.1 Στόχοι

Ο στόχος της παρούσας εργασίας είναι η μελέτη της τεχνολογίας blockchain και η υλοποίηση μιας αποκεντρωμένης εφαρμογής στο περιβάλλον της τεχνολογίας αυτής. Αυτό, αρχικά, περιλαμβάνει την κατανόηση του κρυπτογραφικού υπόβαθρου, της δομής του blockchain και τα μοντέλα συναίνεσης, καθώς και την έρευνα και την σύγκριση των τεχνολογιών αυτών. Έπειτα, θα γίνει κατανοητό πως το blockchain έχει εφαρμογή στα ακαδημαϊκά ιδρύματα, θα αναπτύξουμε μια εφαρμογή και θα συγκρίνουμε τόσο προς το blockchain που χρησιμοποιεί, όσο και προς τις παρόμοιες μελέτες που προϋπήρχαν. Η υλοποίηση της εφαρμογής Verde παρέχει μια εφαρμοσμένη απεικόνιση της δομής των αποκεντρωμένων εφαρμογών, τον τρόπο που αναπτύσσονται αλλά και την ικανοποιητική και άμεσα υλοποιήσιμη λύση που προσφέρει η ιδέα μας. Συνεπώς, η παρούσα εργασία μελετά την τεχνολογία blockchain τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο, αλλά και παρουσιάζει μία ερευνητική και ρεαλιστική πρόταση για την προτροπή της πλαστογραφίας των ακαδημαϊκών τίτλων.

1.2 Περιγραφή προβλήματος

Στις μέρες μας, αρκετά συχνά, δημοσιεύονται ειδήσεις για περιστατικά ανθρώπων που κατέχουν κρίσιμες θέσεις ιδιωτικού ή δημόσιου τομέα όντας κάτοχοι πλαστών ακαδημαϊκών

τίτλων. Ενδεικτικά παραδείγματα πλαστογράφησης πτυχίων περιλαμβάνουν διοικητικούς υπαλλήλους, εκπαιδευτικούς, ερευνητές, και ακόμη πιο ανησυχητικά, ιατρούς και χειρουργούς [24, 25, 26, 27]. Η ανησυχία όμως, για την ακεραιότητα των δεδομένων δεν βρίσκεται μόνο τον εκπαιδευτικό τομέα, αλλά σε όλους τους τομείς που αφορά την κοινωνία μας, ακόμα και στην ίδια την επιστήμη της Πληροφορικής, όπως για παράδειγμα τα ποικίλα ζητήματα σχετικά με τα θέματα ασφάλειας και ιδιωτικότητας που προκύπτουν από την τεχνολογία του Διαδικτύου των Αντικειμένων. Τα παραπάνω περιστατικά μας ώθησαν να σκεφτούμε τον τρόπο που η ψηφιακή τεχνολογία μπορεί να συνδράμει στην αντιμετώπιση του φαινομένου. Θεωρώντας ότι: (i) η απόκτηση ενός ακαδημαϊκού τίτλου αποτελεί μια «δημόσια συναλλαγή» μεταξύ ενός Ακαδημαϊκού Ιδρύματος και ενός τελειόφοιτου, (ii) υπάρχουν κοινότητες φορέων που ενδιαφέρονται να έχουν πρόσβαση στην καταγραφή αυτών των συναλλαγών, και (iii) κάθε συναλλαγή δε μπορεί να αλλοιωθεί από τη στιγμή της δημιουργίας της, οδηγηθήκαμε στο συμπέρασμα ότι το blockchain αποτελεί μια κατάλληλη λύση [20]. Επιπλέον χαρακτηριστικά, όπως η κατανεμημένη αποθήκευση της πληροφορίας και η απουσία κεντρικής αρχής την καθιστούν και ελκυστική σε επίπεδο υλοποίησης. Επίσης, η έλλειψη βιβλιογραφίας στα ελληνικά μας οδήγησε να δημιουργήσουμε την παρούσα μελέτη στην ελληνική γλώσσα.

1.3 Μεθοδολογία

Η παρούσα εργασία αποτελεί τόσο βιβλιογραφική ανασκόπηση όσο και ερευνητική. Τόσο η ανάλυση της τεχνολογίας blockchain, όσο και αυτή της Κρυπτογραφίας, βασίστηκε σε έγκυρη βιβλιογραφία. Πρώτα βασίστηκε σε βιβλιογραφική μελέτη για την κατανόηση του θεωρητικού υπόβαθρου του blockchain, αλλά και των εργαλείων που εφαρμόζονται στα συστήματα της. Στη συνέχεια, η πρόκληση ήταν να υλοποιηθούν μια σειρά από τεχνολογίες όπως, συγκεκριμένα κρυπτοσυστήματα και οι μαθηματικές πράξεις σε συστήματα υπολογιστικής άλγεβρας, την υλοποίηση της αποκεντρωμένης διαδικτυακής εφαρμογής και των διεπαφών με την χρήση γλωσσών προγραμματισμού αλλά και την ανάπτυξη των έξυπνων συμβολαίων. Συνεπώς, αφού υλοποιήθηκαν όλα τα παραπάνω σε περιβάλλον ανοιχτού κώδικα, τα αποτελέσματα καταγράφηκαν και παρουσιάζονται στην παρούσα εργασία. Το ερευνητικό κομμάτι έγκειται από την έρευνα, την μελέτη, την παρατήρηση και τελικά την σύγκριση των μοντέλων συναίνεσης, της πλατφόρμας ανάπτυξης της εφαρμογής Verde και των παρόμοιων προτάσεων με αυτήν.

1.4 Δομή

Το Κεφάλαιο 2 παρουσιάζει τα βασικά κρυπτογραφικά μοντέλα στα οποία βασίζεται η τεχνολογία blockchain. Στόχος του κεφαλαίου είναι να γίνουν κατανοητές οι έννοιες της θεωρίας των συναρτήσεων διασποράς, των ελλειπτικών καμπυλών και τη εφαρμογής τους

στην πράξη με την βοήθεια του ανοιχτού λογισμικού Sage. Κάθε ενότητα συνοδεύεται με κατάλληλα παραδείγματα και εφαρμογές της μαθηματικής θεωρίας στο Sage προκειμένου να γίνει κατανοητή η σημασία των σχετικών ορισμών, θεωρημάτων και πορισμάτων.

Το Κεφάλαιο 3 αναφέρεται στην αρχιτεκτονική του blockchain βάση το πρότυπο, δηλαδή του Bitcoin. Αρχικά, εισάγει τις έννοιες των επιπέδων του blockchain, τα ομότιμα συστήματα αλλά και την έννοια της ιδιοκτησίας. Στην συνέχεια, περιγράφεται αναλυτικά η έννοια των συναλλαγών, η δομή του μπλοκ και η αλυσίδα των μπλοκ · και ολοκληρώνεται με την σημασία του forking. Ο σκοπός του κεφαλαίου είναι να γίνει κατανοητή η τεχνολογία blockchain και κυρίως για τον τρόπο που λειτουργεί, μέσα από παραστατικές εικόνες και ανάλυση των παραπάνω εννοιών.

Στη συνέχεια, στο Κεφάλαιο 4 μελετώνται τα μοντέλα συναίνεσης. Αφορά ένα διαφορετικό επίπεδο του blockchain για αυτό και αποτελεί ξεχωριστό κεφάλαιο. Ο σκοπός του είναι να περιγράψει τα πιο γνωστά μοντέλα συναίνεσης με ευρεία χρήση και τελικά να τα συγκρίνει. Σε αυτό επίσης, γίνεται μια επισκόπηση στα υπάρχοντα μοντέλα.

Έπειτα ακολουθεί το Κεφάλαιο 5, όπου γίνεται μια παρουσίαση του Ethereum blockchain. Το Ethereum διαφέρει σε σχέση με το πρότυπο καθώς διαθέτει έννοιες όπως το EVM, smart contract και gas, αλλά διαφέρει τόσο στην δομή του μπλοκ όσο και στην αρχιτεκτονική του δικτύου. Στο Κεφάλαιο αυτό αναλύεται η σημασία των ψηφιακών πορτοφολιών και των αποκεντρωμένων εφαρμογών. Γίνεται η ενημέρωση για πιο τεχνικά θέματα του Ethereum και η ενημέρωση για εφαρμογές του ήδη βρίσκονται στο εμπόριο, κάνοντας έτσι μία εισήγηση στο επόμενο κεφάλαιο.

Στο Κεφάλαιο 6 περιγράφεται η αποκεντρωμένη διαδικτυακή εφαρμογή Verde, σύγκρισή της με παρόμοιες προτάσεις και ερευνάται η καλύτερη λύση στην χρήση της κατάλληλης πλατφόρμας blockchain. Ο στόχος είναι να παρουσιάσει την αποκεντρωμένη εφαρμογή VerDe (Verified Degrees), που βασίζεται στην τεχνολογία blockchain και στα έξυπνα συμβόλαια, προκείμενου να παρέχει επαλήθευση της εγκυρότητας ενός ακαδημαϊκού τίτλου. Η καινοτομία της εφαρμογής έγκειται στο γεγονός ότι, χρησιμοποιεί το Ethereum blockchain για την επαλήθευση και χρησιμοποιεί «ψευδό-κρυπτονομίσματα», ως τρόπο επαλήθευσης των ακαδημαϊκών τίτλων.

Τέλος, στο Κεφάλαιο 7 συγκεντρώνονται τα συμπεράσματα της παρούσας εργασίας ως προς την τεχνολογία blockchain και την εφαρμογή Verde, συμπεραίνονται και παρατίθενται μερικές σκέψεις για το blockchain και αναφέρεται η μελλοντική έρευνα και η επέκταση της εφαρμογής και του blockchain.

Για να ολοκληρωθεί η εργασία, στο Παράρτημα Α′ παρουσιάζεται ένας πίνακας-λεξικό, μέσα από το οποίο προτείνουμε μερικούς όρους στην ελληνική γλώσσα.

Κεφάλαιο 2

Υπόβαθρο Κρυπτογραφίας

Σε αυτήν την ενότητα θα μελετήσουμε τα κρυπτογραφικά συστήματα που χρησιμοποιούνται από το blockchain και θα δώσουμε μαθηματικά παραδείγματα με την χρήση του ανοιχτού λογισμικού Sage.

Η Κρυπτογραφία αποσκοπεί στη επίτευξη των παρακάτω στόχων ασφάλειας της επικοινωνίας που αποτελούν θεμέλιο λίθο της τόσο στη θεωρία, όσο και στην πράξη:

1. Εμπιστευτικότητα, η οποία διασφαλίζει το απόρρητο των δεδομένων και αποκρύπτει την πληροφορία από μη εξουσιοδοτημένους χρήστες. Ο όρος αυτός είναι στενά συνδεδεμένος και με την ιδιωτικότητα.

2. Μη - Απάρνηση, που στερεί τη δυνατότητα του αποστολέα να αρνηθεί ότι έστειλε ο ίδιος το μήνυμα και του παραλήπτη να αρνηθεί ότι το έλαβε.

3. Ιδιωτικότητα, που στοχεύει στη διατήρηση της πληροφορίας εμπιστευτική και έλεγχος πρόσβασης σε αυτή.

4. Αυθεντικότητα, η οποία επιβεβαιώνει τον παραλήπτη ότι το μήνυμα που έλαβε είναι πράγματι από τον αποστολέα που το έχει στείλει και όχι από κάποιο τρίτο.

5. Ακεραιότητα, που διασφαλίζει ότι η πληροφορία που μεταδίδεται δεν αλλοιώνεται.

Τα παρακάτω κρυπτογραφικά μοντέλα θα τα μελετήσουμε με την χρήση του εργαλείου Sage. Το Sage είναι δωρεάν λογισμικό μαθηματικών ανοιχτού κώδικα και δίνει έμφαση στη δυνατότητα συυνεργατικής ανάπτυξης και της δωρεάν πρόσβασης στον πηγαίο κώδικα. Το Sage υποστηρίζει την έρευνα και τη διδασκαλία στην κρυπτογραφία, τη θεωρία αριθμών, την άλγεβρα, τη γεωμετρία και άλλους συναφείς τομείς.

2.1 Συναρτήσεις Διασποράς

Στην κρυπτογραφία με τον όρο συναρτήσεις διασποράς εννοούμε την συνάρτηση H, που δέχεται ένα μήνυμα οποιουδήποτε μεγέθους και επιστρέφει μια συμβολοσειρά συγκεκρι-

μένου μήκους(128 ή 160 ή 256 ή 512 *bit*). Η έξοδος της συνάρτησης ονομάζεται *'δαχτυλικό αποτύπωμα ή σύνοψη'*. Η πιο σημαντική χρήση των συναρτήσεων διασποράς είναι η αυθεντικοποίηση του μηνύματος. Αν για παράδειγμα η Αλίκη θέλει να στείλει ένα μήνυμα στον Μπομπ σε ένα συμμετρικό κρυπτοσύστημα τότε:

1. Η Αλίκη διασπείρει το μήνυμα της m και παράγει ένα $y = H(m)$ και το κρυπτογραφεί χρησιμοποιώντας το κλειδί k για να πάρει το $e = E(y, k)$.

2. Τοποθετεί το e στο τέλος του μηνύματος και το στέλνει στον Μπομπ.

3. Ο Μπομπ διαχωρίζει το κρυπτοκείμενο από το μήνυμα που έλαβε(m'). Αποκρυπτογραφεί το μήνυμα για να παράξει το $y = D(e, k)$ και στην συνέχεια το ξανά κρυπτογραφεί το μήνυμα που έλαβε για να παράξει το $y' = H(m')$.

4. Αν το $y = y'$ τότε γνωρίζει ότι το μήνυμα που έλαβε είναι το γνήσιο.

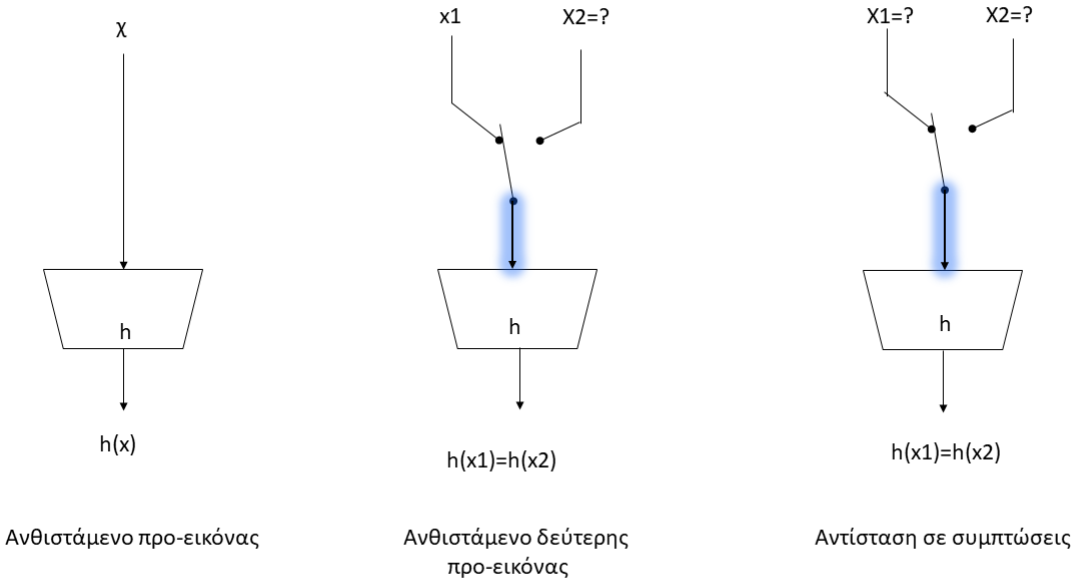
Η πιο συνηθισμένη εφαρμογή των κρυπτογραφικών συναρτήσεων διασποράς είναι η «κρυπτογράφηση» των κωδικών πρόσβασης (password) [28]. Όταν ένας χρήστης εισάγει τον κωδικό του pwd τότε, το σύστημα υπολογίζει την τιμή της διασποράς $h(pwd)$ και αποθηκεύει αυτήν την τιμή έναντι του ίδιου του κωδικού. Οπότε όταν ο χρήστης επαναλάβει τον κωδικό του στο σύστημα τότε αυτό ξανά υπολογίζει την τιμή της διασποράς και την συγκρίνει με την αποθηκευμένη. Μια συνάρτηση διασποράς πρέπει να είναι γρήγορη στον υπολογισμό αλλά και [29]:

- Να είναι ακατόρθωτο κάποιος να βρει το μήνυμα m για το οποίο ισχύει $H(m) = y$ [30].Δηλαδή να είναι μονόδρομη (ή ανθιστάμενη προ-Εικόνας) συνάρτηση: δοθείσης μιας τιμής $y \in 0, 1^n$.

- Να έχει την ιδιότητα: δοθέντος ενός μηνύματος m, είναι υπολογιστικά ανέφικτη η εύρεση ενός δεύτερου μηνύματος m' με $m' \neq m$ και $h(m') = h(m)$. Η ιδιότητα αυτή λέγεται αντίσταση δεύτερης προ-Εικόνας ή ασθενής αντίσταση (second pre-image resistance or weak collision resistance).

- Με ένα ζεύγος μηνυμάτων (m, m'), με $m \neq m'$ και $h(m) = h(m')$, λέγεται ότι είναι μια σύμπτωση ή σύγκρουση (collision) της h. Αν είναι υπολογιστικά ανέφικτη η εύρεση μιας σύμπτωσης (m, m') της h, τότε η h λέγεται ότι είναι ανθιστάμενη συμπτώσεων ή ισχυρή αντίσταση σε συμπτώσεις (strong collision resistant).

Μερικές φορές, οι ανθιστάμενες των συμπτώσεων συναρτήσεις διασποράς λέγονται ελεύθερες συμπτώσεων (collision free), αλλά κάτι τέτοιο είναι παραπλανητικό. Η συνάρτηση h είναι μια απεικόνιση από ένα σύνολο με άπειρο πλήθος στοιχείων σε ένα σύνολο με πεπερασμένο πλήθος στοιχείων. Άρα, υπάρχουν πολλές συμπτώσεις (στην πραγματικότητα, απείρως πολλές) [28]. Η αντίσταση σε συμπτώσεις απλά σημαίνει ότι αυτές είναι δύσκολο



Σχήμα 2.1: Οι κατηγορίες των συναρτήσεων διασποράς ως προς την αντίσταση τους

να βρεθούν. Μερικές φορές, συναρτήσεις διασποράς ανθιστάμενες συμπτώσεων λέγονται ελεύθερες συμπτώσεων (collision free), αλλά κάτι τέτοιο είναι παραπλανητικό. Η συνάρτηση η είναι μια απεικόνιση από ένα σύνολο με άπειρο πλήθος στοιχείων σε ένα σύνολο με πεπερασμένο πλήθος στοιχείων. Άρα, υπάρχουν πολλές συμπτώσεις (στην πραγματικότητα, απείρως πολλές). Η αντίσταση σε συμπτώσεις απλά σημαίνει ότι αυτές είναι δύσκολο να βρεθούν.

2.1.1 Κατασκευή συναρτήσεων διασποράς

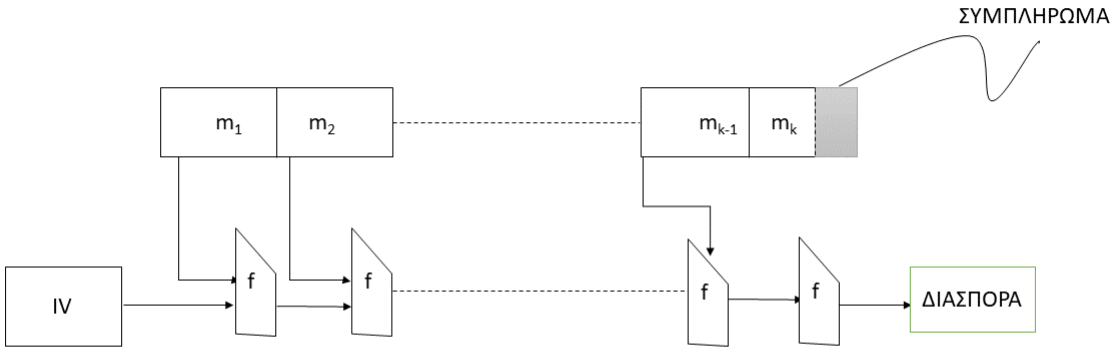
Μεσα από το παράδειγμα των Chaum, van Heijst,Pfitzman μπορούμε να κατανοήσουμε καλυτέρα την δομή μιας συνάρτησης διασποράς [28]. Έστω ότι ένας μεγάλος πρώτος αριθμός p τέτοιος ώστε ο $q = (p-1)/2$ να είναι πρώτος. Επίσης έστω ότι a και β δυο πρωτεύουσες ρίζες του p (γεννήτορες της $\mathbb{Z}_p^*$). Η τιμή $\log_\alpha \beta$ δεν είναι δημόσια και υποθέτουμε ότι είναι υπολογιστικά ανέφικτος ο υπολογισμός της. Η συνάρτηση διασποράς $h : 0, ..., q-1x0, ..., q-1 \to \mathbb{Z}_p^*$ και ορίζεται ως εξής:

$$h(x_1, x_2) = \alpha^{x_1}\beta^{x_2} \bmod \ p$$

Η συνάρτηση αυτή θα απεικονίζει τους ακεραίους $modq^2$ σε ακέραιους mod p. Συνεπώς, η σύνοψη μηνύματος θα αποτελείται από τα μισά περίπου bit από ότι το μήνυμα. Οπότε αν είναι αδύνατον να υπολογιστεί ο διακριτός λογάριθμος $\log_\alpha \beta$ στο $\mathbb{Z}_p^*$ τότε, η συνάρτηση είναι ανθισταμένη συμπτώσεων [28] [31].

2.1.2 Μέθοδος των Merkle και Damgård.

Ένας από τους πιο αποδοτικούς και πρακτικούς τρόπους κατασκευής κρυπτογραφικών συναρτήσεων διασποράς είναι των Merkle και Damgård ή μετα-μέθοδος του Merkle [28]. Η μέθοδος,*η οποία ονομάζεται και μέθοδος συμπίεσης*, ανάγει το πρόβλημα σχεδίασης μιας ανθιστάμενης συμπτώσεων συνάρτησης διασποράς $h : 0, 1^n \leftarrow 0, 1^n$ στο πρόβλημα κατασκευής μιας ανθιστάμενης συμπτώσεων συνάρτησης $f : 0, 1^{n+r} \leftarrow 0, 1n(r \in \mathbb{N}, r > 0)$ και πεπερασμένο πεδίο ορισμού $0, 1^{n+r}$. Ουσιαστικά το μήνυμα m μήκους $n + r$ ανάγεται σε μήνυμα συμπίεσης $f(m)$ με μήκος n οπού r ο βαθμός συμπίεσης. Στο σχήμα απεικονίζεται ο τρόπος που λειτουργεί αυτή η μέθοδος. Συγκεκριμένα το m είναι ένα μήνυμα οποιουδήποτε μήκους και η συνάρτηση διασποράς δουλεύει επαναληπτικά για τον υπολογισμού του $h(m)$. Το μήνυμα υποδιαιρείται σε τμήματα μήκους r. Το ένα τμήμα μετά το άλλο λαμβάνεται από το m, συνενώνεται με την τρέχουσα τιμή και συμπιέζεται από την f προκειμένου να προκύψει ένα νέο μήκος $n - bit$. Κάθε μήνυμα m συμπληρώνεται με μια τέτοια συμβολοσειρά $100\ldots0$, ακόμα και αν το μήκος του αρχικού μηνύματος m είναι ένα πολλαπλάσιο του r. Οπότε τα bit που προστίθενται κατά τη συμπλήρωση μπορούν να διακριθούν από τα βιτ του αρχικού μηνύματος και αρά μπορούν να αφαιρεθούν πιο ευκολά [31].



Σχήμα 2.2: Η κατασκευή του Merkle - Damgård

Μετά τη συμπλήρωση, γίνεται η αποσύνθεση $m = m_m||m_2||...||m_k, m_i \in 0, 1^r, 1 \leq i \leq k$, σε τμήματα m_i μήκους r. Τα εναπομείναντα bit του m_{k+1} πληρούνται με μηδενικά:

$$m = m_1||m_2||...||m_k||m_{k+1}$$

Αρχίζοντας με την αρχική τιμή $\upsilon_0 \in 0, 1^n$, θέτουμε αναδρομικά

$$\upsilon_i := f(\upsilon i - 1||m_i), 1 \leq i \leq k+1$$

Άρα $h(m) := \upsilon_{k+1}$

2.1.3 Επίθεση γενεθλίων

Στον τομέα της ασφάλειας των συναρτήσεων διασποράς ισχύει ότι, ο δείκτης ασφάλειας μετράται με βάση το πόσο δύσκολο είναι να βρεθεί μια σύγκρουση σε δυο διαφορετικά μηνύματα, τα οποία τελικά θα πράξουν την ίδια σύνοψη (τιμή διασποράς) [32] [28]. Η επίθεση γενεθλίων είναι μια πρωτόγονη επίθεση εναντίον της αντίστασης σε συμπτώσεις. Το πλήθος των ατόμων που πρέπει να βρεθούν στον ίδιο χώρο ώστε η πιθανότητα να είναι πάνω από 50% αυτά να είναι 23. Αυτό προκύπτει από την μαθηματική εξίσωση: [28]

$$\prod_{k-1}^{i=1} \frac{365-i}{365} = (1 - \frac{1}{365})(1 - \frac{2}{365})....(1 - \frac{k-1}{365})$$

Αυτό πρακτικά σημαίνει ότι έχουν ασφάλεια της τάξεως των $2^{n/2}$ δηλαδή 50% πιθανότητα να βρεθεί μια σύγκρουση. Αν για παράδειγμα επιλέγαμε μια συνάρτηση διασποράς της τάξεως των 128-*bit* αυτή θα είχε μόλις 64-*bit* ασφάλεια [28]. Όμως αυτό το ποσό είναι πολύ μικρό ειδικά στους σύγχρονους υπολογιστές καθώς τα 80-*bit* θεωρούνται το λιγότερο πόσο για μια μη αποτελεσματική πρωτόγονη επίθεση. Αρά οι συναρτήσεις διασποράς πρέπει όλες να μεγαλύτερες των 160-*bit* [32] [28].

2.1.4 Η οικογένεια MD

Πρόκειται για τις κρυπτογραφικές συναρτήσεις διασποράς MD2, MD4 και MD5. Η πλέον δημοφιλής είναι η MD5 και σχεδιάστηκε προκειμένου να διορθωθούν ατέλειες της προγενέστερης έκδοσής της, MD4 [32] [28]. Όμως, η εσωτερική της συνάρτηση συμπίεσης διαπιστώθηκε ότι έχει αδυναμίες κι ως εκ τούτου δεν είναι μια ασφαλής συνάρτηση. Επίσης MD5 διασπείρει σε τιμές 128-*bit*, που δεν θεωρούνται πλέον ικανοποιητικές τιμές για την ασφάλεια στις μέρες μας [32] [33]. Το **RIPEMD** (Research and Development in Advanced Communications Technologies in Europe = RACE +Integrity Primitives Evaluation = RIPE + Message Digest = RIPEMD) είναι η πιο μοντέρνα μορφή των συναρτήσεων διασποράς. Το RIPEMD-160 παράγει μια σύνοψη μεγέθους 160 –*bit*. Προέρχεται από την οικογένεια των MD4. Παρόλο που το MD4 θεωρείται πλέον ξεπερασμένη τεχνολογία, το RIPE θεωρείται ως μια από τις πιο σύγχρονες και δυνατές συναρτήσεις διασποράς. **SHA-1**. Ο Secure Hashing Algorithm αναπτύχθηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST – National Institute of Standards and Technology) από κοινού με την Εθνική Υπηρεσία Ασφαλείας (NSA) των ΗΠΑ. Παράγει τιμές 160-*bit* αλλά από τον Φεβρουάριο του 2005 έπαψε να θεωρείται ασφαλής [31] [28]. **SHA-2** (Secure Hash Algorithm 2), Πρόκειται για μια οικογένεια έξι κρυπτογραφικών συναρτήσεων διασποράς με τιμές

διασποράς 224, 256, 384 *or* 512 bit, αντίστοιχα:SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. Το Sage διαθετει βιβλιοθηκες για να παραξουμε συναρτήσεις διασποράς [31].

Sage:

```
sage: import hashlib
sage: hashlib.sha1('').hexdigest()
'da39a3ee5e6b4b0d3255bfef95601890afd80709'
sage: hashlib.sha1('a').hexdigest()
'86f7e437faa5a7fce15d1ddcb9eaeaea377667b8'
sage: hashlib.sha1('abc').hexdigest()
'a9993e364706816aba3e25717850c26c9cd0d89d'
sage: hashlib.sha1('abd').hexdigest()
'cb4cc28df0fdbe0ecf9d9662e294b118092a5735'
sage: hashlib.sha1('Today is Christmas!').hexdigest()
'36836f719949547d3006aa46e6c5b64424d49eb3'
sage: hashlib.sha1('Today is Cristmas!').hexdigest()
'cfa8971d311749fb38e8b16db41e66d76a2fd098'
sage: hashlib.sha224('Today is Christmas!').hexdigest()
'0f452a8c03228ec8c64c7fb1edf687cceca11f313a86979243bd1c07'
sage: hashlib.sha256('Today is Christmas!').hexdigest()
'e01a896262d5bf8850f1a2f9cc5019a4b1c1f20fac6943974f25d433a518a504'
sage: hashlib.algorithms ('md5', 'sha1',
'sha224', 'sha256', 'sha384', 'sha512')
sage: hashlib.algorithms_available
'DSA',
'DSA-SHA',
'MD4',
'MD5',
'RIPEMD160',
'SHA',
'SHA1',
'SHA224',
'SHA256',
'SHA384',
'SHA512',
'dsaEncryption',
'dsaWithSHA',
'ecdsa-with-SHA1',
'md4',
'md5',
'ripemd160',
'sha',
'sha1',
'sha224',
'sha256',
'sha384',
```

```
'sha512',
'whirlpool'
sage: hashlib.sha1('a').hexdigest()
'86f7e437faa5a7fce15d1ddcb9eaeaea377667b8'
sage: hashlib.ripemd160('a').hexdigest()
---------------------------------------------------------------------
AttributeError Traceback (most recent call last)
<ipython-input-1-8b15933388b5> in <module>()
 1 import hashlib
----> 2 hashlib.ripemd160('a').hexdigest()
AttributeError: 'module' object has no attribute 'ripemd160'
---------------------------------------------------------------------
sage: r = hashlib.new('ripemd160')
sage:r.update("a")
sage:r.hexdigest()
'0bdc9d2d256b3ee9daae347be6f4dc835a467ffe'
```

Το σημαντικό με αυτήν την μέθοδο είναι ότι ακόμα και αν αλλαχθεί το παραμικρό bit στην συνάρτηση, τότε η συνάρτηση θα παράξει εντελώς διαφορετικό αποτέλεσμα.

Σύγχρονοι αλγόριθμοι διασποράς

Πολύ νέοι αλγόριθμοι διασποράς εμφανίστηκαν τα τελευταία χρόνια, οι οποίοι βασίζονται στο τελευταίο πρότυπο του $SHA-3$. Αναφορικά υπάρχουν πέντε βασικοί νέοι αλγόριθμοι όπως οι: BLAKE, Grøstl, JH,Keccak και Skein. Από όλους ο είναι ο πιο εύκολος καθώς βασίζεται στο πρότυπο των Merkle και Damgård.

2.1.5 Αυθεντικοποίηση των Συναρτήσεων Διασποράς

Ο πιο σημαντικός σκοπός των συναρτήσεων διασποράς είναι η πιστοποίηση αυθεντικότητας του μηνύματος, δηλαδή η πιστοποίηση προέλευσης του. Αν μια συνάρτηση διασποράς χρησιμοποιείται για την πιστοποίηση αυθεντικότητας μηνύματος, τότε λέγεται κώδικας πιστοποίησης αυθεντικότητας μηνύματος (ή MAC – Message Authentication Code) [31] [32]. Η MAC είναι η πιο σύνηθες συμμετρική τεχνική για την πιστοποίηση της αυθεντικότητας μηνύματος και την προστασία της ακεραιότητας, σε πρωτόκολλα όπως τα SSL/TLS και IPSec. Τυπικά, τα μυστικά κλειδιά k χρησιμοποιούνται για την παραμετροποίηση των συναρτήσεων διασποράς [28] [31]. Έτσι, οι MAC είναι οικογένειες συναρτήσεων διασποράς [32].

Η συνήθης μέθοδος μετατροπής μιας κρυπτογραφικής συνάρτησης διασποράς σε ένα MAC είναι η λεγόμενη HMAC [31] [28]. Και τέλος μπορεί να εφαρμοστεί σε μια συνάρτηση διασποράς h η οποία προκύπτει από μια συνάρτηση συμπίεσης f χρησιμοποιώντας τη μέθοδο των Merkle–Damgård [31]. Ο πιο απλός τρόπος δημιουργίας MAC είναι $M = H(k||H(k||m))$. Με δεδομένα το κλειδί και το μήνυμα,η MAC μπορεί να δημιουργηθεί με τα συγκεκριμένα βήματα:

1. Σύνοψη του κλειδιού με το μήνυμα.
2. Τοποθέτηση του κλειδιού μπροστά από τη σύνοψη.
3. Σύνοψη ξανά του προηγούμενου αποτελέσματος.

Από την άλλη το σχήμα HMAC έχει τα εξής βήματα κατασκευής:

1. Συμπλήρωση μηδενικών στο τέλος του κλειδιού k για να δημιουργηθεί μια δυαδική συμβολοσειρά μεγέθους 64 bit.
2. XOR το αλφαριθμητικό από το προηγούμενο βήμα με τη δυαδική συμβολοσειρά 00110110, και αυτό επαναλαμβάνεται 64 φορές.
3. Αποθηκεύουμε στο τέλος του μηνύματος m το προηγούμενο αποτέλεσμα και περνά από μια συνάρτηση διασποράς.
4. XOR τη σύνοψη από το βήμα 1 με τη δυαδικό 01011100 και επαναλαμβάνεται αυτό 64 φορές.
5. Αποθηκεύουμε στο τέλος της σύνοψης από το βήμα 4 στη 64-$byte$ συμβολοσειρά που παράχθηκε στο προηγούμενο βήμα.
6. Διασπορά του προηγούμενου βήματος.

Αν τα 64 αντίγραφα του 00110110 μπορούν να γραφούν στο δεκαεξαδικό σύστημα ως '36' και τα 64 αντίγραφα του 01011100 ως '$5C$' το HMAC μπορεί να γραφεί ως [29] $HMAC(m,k) = H(k \oplus \text{"}5C\text{"}||H(k \oplus \text{"}36\text{"}||m)$ Η χρησιμότητα της MAC μπορεί να φανεί μέσα από το εξής παράδειγμα, έστω ότι η Άλις θέλει να στείλει ένα μήνυμα στον Μπομπ, χρησιμοποιεί ένα κλειδί γνωστό και στους δυο και έπειτα δημιουργεί το MAC χρησιμοποιώντας το m και το k, και στέλνει και το μήνυμα και το MAC στον Μπομπ. Όταν ο Μπομπ τα λάβει, τότε υπολογίζει το MAC από το κωδικοποιημένο μήνυμα m' χρησιμοποιώντας το k, και το συγκρίνει με το MAC που του έστειλε η Άλις. Αν τα δυο MAC είναι ίδια τότε ο Μπομπ γνωρίζει ότι το μήνυμα που έλαβε είναι γνήσιο [31].

Στο δίκτυο του blockchain, οι κρυπτογραφικές συναρτήσεις διασποράς έχουν πολλές εφαρμογές και θα μπορούσε κάνεις να τις χαρακτηρίσει την βάση για την υλοποίηση του. Οι συναρτήσεις διασποράς έχουν τις εξής ιδιότητες εντός του δικτύου:

- Δημιουργία διεύθυνσης.
- δημιουργία μοναδικών αναγνωριστικών.
- Εξασφάλιση των δεδομένων του μπλοκ. Ένας κόμβος που θα δημοσιευτεί θα διασπείρει τα δεδομένα του μπλοκ, δημιουργώντας έτσι μια σύνοψη που θα αποθηκευτεί μέσα στην επικεφαλίδα του μπλοκ [18].

- Εξασφάλιση της κεφαλίδας του μπλοκ. Ένας κόμβος δημοσίευσης θα διασπείρει την κεφαλίδα του μπλοκ. Εάν το δίκτυο blockchain χρησιμοποιεί συναινετικό μοντέλο της απόδειξης εργασίας, ο κόμβος έκδοσης θα χρειαστεί να διασπείρει την κεφαλίδα του μπλοκ με διαφορετικά τυχαίο αριθμό μοναδικής χρήσης μέχρι να εκπληρωθούν οι απαιτήσεις του παζλ. Η ανάκτηση της τρέχουσας σύνοψης του μπλοκ θα συμπεριληφθεί στην κεφαλίδα του επόμενου μπλοκ [34] [1].

2.2 Ελλειπτικές Καμπύλες

Η κρυπτογραφία ελλειπτικής καμπύλης (ECC) είναι το νεότερο μέλος των τριών οικογενειών καθιερωμένων αλγορίθμων δημόσιου κλειδιού [32] [28]. Το ECC βασίζεται στο γενικευμένο πρόβλημα διακριτού λογαρίθμου, έτσι ώστε πρωτόκολλα DL όπως η ανταλλαγή κλειδιών Diffie-Hellman να μπορούν να υλοποιηθούν χρησιμοποιώντας ελλειπτικές καμπύλες [32] [30]. Οποιοδήποτε πολυώνυμο-εξίσωση το οποίο συσχετίζει το y σε σχέση με το q,τότε μπορεί να αναπαρασταθεί ως μια καμπύλη. Με τον όρο "καμπύλη" εννοείται το σύνολο των σημείων (x, y) που είναι λύσεις των εξισώσεων. Για παράδειγμα, το σημείο $(x = r, y = 0)$ πληρεί την εξίσωση ενός κύκλου και είναι, συνεπώς, στο σύνολο [30]. Μια ελλειπτική καμπύλη είναι ένας ειδικός τύπος πολυωνυμικής εξίσωσης [30]. Οι ελλειπτικές καμπύλες το σύνολο ορισμού τους δεν είναι οι πραγματικοί αριθμοί αλλά ένα πεπερασμένο πεδίο [32] [30]. Μια ελλειπτική καμπύλη είναι βασικά ένας τύπος πολυωνυμικής εξίσωσης γνωστής ως η εξίσωση Weierstrass, η οποία παράγει μια καμπύλη πάνω από ένα πεπερασμένο πεδίο [32] [35] [36]. Ουσιαστικά οι ελλειπτικές καμπύλες είναι ορισμένες στο σώμα Z_p όπου p > 3 και p πρώτος αριθμός. Ορισμός της ελλειπτικής καμπύλης [30]: Η ελλειπτική καμπύλη ορισμένη στο Z_p για κάποιον πρώτο ακέραιο $p > 3$, είναι το σύνολο των στοιχείων $(x, y) \in Z_p \times Z_p$,τα οποία ικανοποιούν την εξίσωση [30]: $y^2 \equiv x^3 + ax + b(modb)$ όπου $a, b \in Z_p$ και $4a^3 + 27b^2 \neq 0(\text{ mod } p)$. Δύο βασικά πορίσματα σε σχέση με τον παραπάνω ορισμό είναι τα εξής [30] [37]: Πρώτον, η ελλειπτική καμπύλη είναι συμμετρική σε σχέση με τον άξονα x. Αυτό προκύπτει άμεσα από το γεγονός ότι για όλες τις τιμές x_i που βρίσκονται στην ελλειπτική καμπύλη, και τα δύο αποτελεσματα, $y_i = \sqrt{(x_i)^3 + ax_i + b}$, $y_i^{'} = \sqrt{(x_i)^3 + ax_i + b}$ είναι οι λύσεις. Δεύτερον, υπάρχει μια τομή με τον άξονα x. Αυτό προκύπτει από το γεγονός ότι είναι μια κυβική εξίσωση αν λυθεί ως προς $y = 0$ το οποίο έχει μία πραγματική λύση (την τομή με τον άξονα x) και δύο σύνθετες λύσεις [32] [38].

Παράδειγμα 1. Εφαρμογή των ελλειπτικών καμπυλών στο σώμα των ρητών αριθμών $\mathbb{Q}$ Έστω η καμπύλη **E** με εξίσωση:

$$y^2 = x^3 - 2x + 4$$

και έστω η ελλειπτική καμπύλη **F** με εξίσωση:

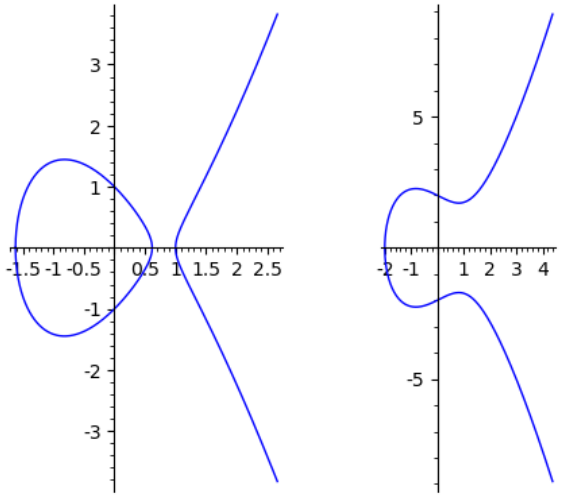
$$y^2 = x^3 - 2x + 1$$

□

Στο Sage, η εντολή **EllipticCurve**, δημιουργεί τις ελλειπτικές καμπύλες. Η συνάρτηση **plot** δημιουργεί τα γραφικά των καμπύλων, όπως φαίνεται στο Σχήμα 2.3. Στη γραφική παράσταση 2.3α′ αναπαρίσταται η ελλειπτική καμπύλη $y^2 = x^3 - 2x + 4$ και ορισμένη στο σύνολο των ρητών $\mathbb{R}$. Στη γραφίκη παράσταση 2.3β′ απεικονίζεται η ελλειπτική καμπύλη $y^2 = x^3 - 2x + 1$ στο σύνολο των ρητών $\mathbb{R}$.

```
sage: G = EllipticCurve([-2,1])
sage: print G
Elliptic Curve defined by y^2 = x^3 - 2*x + 1 over Rational Field
sage: G.plot(aspect_ratio=1)

sage: E = EllipticCurve([-2,4])
sage: print E
Elliptic Curve defined by y^2 = x^3 - 2*x + 4 over Rational Field
sage: E.plot(aspect_ratio=1)
```



(α′) Ελλειπτική καμπύλη $y^2 = x^3 - 2x + 1$

(β′) Ελλειπτική καμπύλη $y^2 = x^3 - 2x + 4$

Σχήμα 2.3: Ελλειπτικές καμπύλες στο σύνολο των ρητών αριθμών

Στο blockchain, όμως, προτιμάτε η χρήση ελλειπτικών καμπυλών που ορίζονται μέσα σε ένα πεπερασμένο σώμα, δηλαδή σε πεπερασμένο πλήθος στοιχείων ή αλλιώς, σε μια ομάδα Galois-GF [32] [39]. Τα στοιχεία στα πεπερασμένα σώματα ή $GF(2^m)$ δεν αναπαριστώνται

ως ακέραιοι αλλά ως πολυώνυμα, με τους συντελεστές τους στο $GF(2)$. Τα πολυώνυμα έχουν μέγιστο βαθμό $m-1$, έτσι ώστε να υπάρχουν συνολικά συντελεστές m για κάθε στοιχείο [32] [39]. Οι ελλειπτικές καμπύλες στα πεπερασμένα σώματα δεν διαφοροποιούνται οι ιδιότητες τους ιδιαίτερα σε σχέση με αυτές που είναι ορισμένες στο $\mathbb{R}$ παρά μόνο στον τρόπο που αναπαρίστανται.

Παράδειγμα 2.

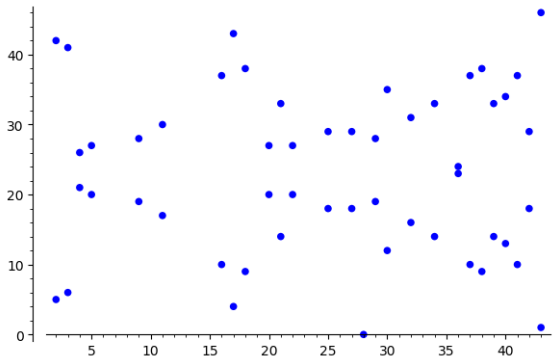
Έστω η ελλειπτική καμπύλη που ορίζεται στο $\mathbb{Z}_{17}$ με την εξίσωση:

$$y^2 = x^3 - 8x + 33$$

□

```
sage: S = EllipticCurve(GF(47),[-8,33])
sage: print S
Elliptic Curve defined by y^2 = x^3 + 39*x + 7 over Finite
Field of size 47
sage: print S.is_on_curve(7,3)
True
sage: print S.cardinality()
54
sage: print S.order()
54
sage: print S.points()
sage: S.plot(pointsize=30)
[(0 : 1 : 0), (2 : 5 : 1), (2 : 42 : 1), (3 : 6 : 1),
(3 : 41 : 1), (4 : 21 : 1), (4 : 26 : 1), (5 : 20 : 1), (5 : 27 : 1),
(9 : 19 : 1), (9 : 28 : 1), (11 : 17 : 1), (11 : 30 : 1), (16 : 10 : 1),
(16 : 37 : 1), (17 : 4 : 1), (17 : 43 : 1), (18 : 9 : 1), (18 : 38 : 1),
(20 : 20 : 1), (20 : 27 : 1), (21 : 14 : 1), (21 : 33 : 1), (22 : 20 : 1),
(22 : 27 : 1), (25 : 18 : 1), (25 : 29 : 1), (27 : 18 : 1), (27 : 29 : 1),
(28 : 0 : 1), (29 : 19 : 1), (29 : 28 : 1), (30 : 12 : 1), (30 : 35 : 1),
(32 : 16 : 1), (32 : 31 : 1), (34 : 14 : 1), (34 : 33 : 1), (36 : 23 : 1),
(36 : 24 : 1), (37 : 10 : 1), (37 : 37 : 1), (38 : 9 : 1), (38 : 38 : 1),
(39 : 14 : 1), (39 : 33 : 1), (40 : 13 : 1), (40 : 34 : 1), (41 : 10 : 1),
(41 : 37 : 1), (42 : 18 : 1), (42 : 29 : 1), (43 : 1 : 1), (43 : 46 : 1)]
```

Πρόσθεση σημείων Η πρόσθεση δύο σημείων της ελλειπτικής καμπύλης στο Z_p ορίζεται με τον ίδιο τρόπο όπως και στους πραγματικούς αριθμούς. Έστω δύο σημεία



Σχήμα 2.4: Ελλειπτική καμπύλη στο πεπερασμένο σώμα $\mathbb{F}_{47}$

$R = (x_1, y_1)$, $Q = (x_2, y_2)$, της ελλειπτικής καμπύλης $y^2 \equiv x^3 + ax + b(\text{mod } p)$. Το σημείο $P+Q = (x_3, y_3)$ το οποίο είναι επίσης σημείο της καμπύλης, θα έχει συντεταγμένες: $x_3 \equiv \lambda^2 - x_1 - x_2(\text{mod } p)$, $y_3 \equiv \lambda(x_1 - x_3) - y_1(modp)$ όπου:

$$\lambda \equiv \left\{ \begin{array}{ll} \frac{(y_2-y_1)}{(x_2-x_1)}(\text{mod } p), & \text{εάν } Q \neq P \\ \frac{3(x_1)^2+a}{2y_1}(\text{mod } p), & \text{εάν } Q = P \end{array} \right\}$$

Επίσης μια πολύ σημαντική ιδιότητα στις ελλειπτικές καμπύλες στο Z_p, είναι ότι τα σημεία της ελλειπτικης καμπύλης μαζί με το σημείο $\mathbf{O}$ ορίζουν κυκλική υποομάδα. Αυτό σημαίνει ότι οποιοδήποτε σημείο ανήκει στην ελλειπτική καμπύλη εκτός του $\mathbf{O}$, είναι γεννήτορας αυτής. Δηλαδή, δοθέντος κάποιου σημειου R της καμπύλης, η διαδοχική πρόσθεση του R στον εαυτό του, θα διατρέξει όλα τα σημεία της καμπύλης (για παράδειγμα, $2R = R+R \ldots nR = \mathbf{O}$). Το πρόβλημα διακριτού λογαρίθμου στο ECC βασίζεται στην ιδέα ότι, κάτω από συγκεκριμένες συνθήκες, όλα τα σημεία σε μια ελλειπτική καμπύλη σχηματίζουν μια κυκλική ομάδα [32].Σε μια ελλειπτική καμπύλη, το δημόσιο κλειδί είναι ένα τυχαίο πολλαπλάσιο του σημείου γεννήτορας, ενώ το ιδιωτικό κλειδί είναι ένας τυχαία επιλεγμένος ακέραιος που χρησιμοποιείται για τη δημιουργία του πολλαπλάσιου [40]. Με άλλα λόγια, ένα ιδιωτικό κλειδί είναι ένας τυχαία επιλεγμένος ακέραιος, ενώ το δημόσιο κλειδί είναι ένα σημείο στην καμπύλη [40]. Το πρόβλημα του διακριτού λογαρίθμου χρησιμοποιείται για να βρει το ιδιωτικό κλειδί (ακέραιο) όπου ο ακέραιος αυτός εμπίπτει σε όλα τα σημεία της ελλειπτικής καμπύλης [40]. Για μπορέσει να ρυθμιστεί το κρυπτοσύστημα του διακριτού λογαρίθμου είναι σημαντικό να είναι γνωστή η τάξη της ομάδας. Αν και γνωρίζοντας τον ακριβή αριθμό των σημείων σε μια καμπύλη είναι ένα πολύπλοκο έργο, γίνεται να γνωρίζουμε τον αριθμό αυτόν κατά προσέγγιση λόγω του θεωρήματος Hasse, το οποίο αναφέρει ότι [32] [36].:

Θεώρημα 1 (Θεώρημα του Hasse). *Δεδομένης μιας ελλειπτικής καμπύλης Emodulop, ο αριθμός των σημείων στην καμπύλη υποδηλώνεται με Έ και οριοθετείται από:* $p+1-2\sqrt{p} \leq \#E \leq p+1+2\sqrt{p}$.

Το θεώρημα Hasse, δηλώνει ότι ο αριθμός των σημείων κυμαίνεται κατά προσέγγιση κοντά στον πρώτο αριθμού ρ [32]. Αυτό έχει σημαντικές πρακτικές συνέπειες. Για παράδειγμα,

έστω ελλειπτική καμπύλη με 2^160 στοιχεία, τότε το πρώτο αριθμό μήκος περίπου 160 bit [32].

Ορισμός 2. *Έστω μια ελλειπτική καμπύλη ορισμένη στο Z_p. 'Εστω ένα σημείο R της καμπύλης και ένα σημείο Q το οποίο αποτελεί βαθμωτό γινόμενο του R. Το πρόβλημα του διακριτού λογαρίθμου στην ελλειπτική καμπύλη είναι ο καθορισμός της λύσης n, όπου $n1 \leq n \leq \#E$, τέτοιο ώστε να ισχύει [30] [32]: $nP = Q$.*

Εδώ, το Q είναι το δημόσιο κλειδί (ένα σημείο στην καμπύλη), και n είναι το ιδιωτικό κλειδί. Αυτό σημαίνει ότι, το δημόσιο κλειδί είναι ένα τυχαίο πολλαπλάσιο του γεννήτορα, ενώ το ιδιωτικό κλειδί είναι ο ακέραιος που χρησιμοποιείται για τη δημιουργία του πολλάσιου.Το "Ε αντιπροσωπεύει τη σειρά της ελλειπτικής καμπύλης, που σημαίνει τον αριθμό των σημείων που υπάρχουν στην κυκλική ομάδα της ελλειπτικής καμπύλης [32]. Μια κυκλική ομάδα σχηματίζεται από ένα συνδυασμό σημείων στην ελλειπτική καμπύλη και το σημείο του άπειρου [40]. Το blockchain και πιο συγκεκριμένα το Bitcoin, αλλά και κάποιες πλατφόρμες του Ethereum χρησιμοποιούν ένα συγκεκριμένο αλγόριθμο ελλειπτικών καμπυλών και συγκεκριμένα τον αλγόριθμο Secp256k1 [40], το οποίο ιδρύθηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ (NIST).Το Secp256k1 δεν χρησιμοποιήθηκε σχεδόν ποτέ πριν το Bitcoin γίνει δημοφιλής, αλλά τώρα κερδίζει τη δημοτικότητα χάρη στις πολλές ωραίες ιδιότητές της. Οι συχνότερα χρησιμοποιούμενες καμπύλες έχουν τυχαία δομή, αλλά το Secp256k1 κατασκευάστηκε με ειδικό μη τυχαίο τρόπο που επιτρέπει ιδιαίτερα αποτελεσματικό υπολογισμό. Ως αποτέλεσμα, είναι συχνά περισσότερο από 30% ταχύτερα από άλλες καμπύλες, εάν η εφαρμογή βελτιστοποιηθεί επαρκώς. Επίσης,οι σταθερές του Secp256k1 επιλέχθηκαν με έναν προβλέψιμο τρόπο, γεγονός που μειώνει σημαντικά την πιθανότητα ο δημιουργός της καμπύλης να εισάγει οποιοδήποτε είδος 'πίσω πόρτας' στην καμπύλη [41].

Κρυπτογράφηση δημόσιου και ιδιωτικού κλειδιού με ελλειπτικές καμπύλες

Ιδιωτικό Κλειδί Ένα ιδιωτικό κλειδί είναι απλά ένας αριθμός, που επιλέγεται τυχαία. Το ιδιωτικό κλειδί χρησιμοποιείται για τη δημιουργία υπογραφών που αποδεικνύουν την ιδιοκτησία των κεφαλαίων που χρησιμοποιούνται σε μια συναλλαγή στο Bitcoin και στο Ethereum. Το ιδιωτικό κλειδί πρέπει να παραμένει μυστικό, διότι η αποκάλυψή του σε τρίτους ισοδυναμεί με την εξασφάλιση του ελέγχου των προσωπικών στοιχείων ή κεφαλαίων από αυτούς τους τρίτους. Το ιδιωτικό κλειδί πρέπει επίσης να υποστηρίζεται και να προστατεύεται από τυχαία απώλεια. Εάν χαθεί, δεν μπορεί να ανακτηθεί και οποιαδήποτε στοιχεία περιέχει, χάνονται για πάντα. Στο Ethereum ένα ιδιωτικό κλειδί μπορεί να είναι ένας οποιοσδήποτε μη μηδενικός αριθμός μέχρι έναν πολύ μεγάλο αριθμό, ελαφρώς μικρότερο από 2^256 - ένας 78-ψήφιος αριθμός, περίπου 1.158×10^77 [18]. Η δημιουργία ενός ιδιωτικού κλειδιού είναι η τυχαία επιλογή 256-bit κλειδιού, το οποίο πετυχαίνεται μέσω της σύνοψης ενός πολύ μεγαλύτερου αριθμου σε πλήθος bit (πάνω από 256-bit) με τον αλγόριθμο SHA-256 ή

Keccak-256. Μια πολύ σημαντική λεπτομέρεια είναι ότι η δημιουργία του ιδιωτικού κλειδιού δεν γίνεται στο διαδίκτυο αλλά, τοπικά.

Δημόσιο Κλειδί Το δημόσιο κλειδί υπολογίζεται από το ιδιωτικό κλειδί χρησιμοποιώντας τον πολλαπλασιασμό της ελλειπτικής καμπύλης, που πρακτικά είναι μη αναστρέψιμος: $K_{pub} = k_{pr} * G$, όπου k_{pr} είναι το ιδιωτικό κλειδί, G είναι ένα σταθερό σημείο που ονομάζεται σημείο γεννήτορας, K_pub είναι το δημόσιο κλειδί που προκύπτει και το σύμβολο '' είναι ο ειδικός πολλαπλασιασμός της ελλειπτικής καμπύλης [18]. Το σημείο γεννήτορας ορίζεται ως μέρος του προτύπου secp256k1 και είναι το ίδιο για όλες τις εφαρμογές του secp256k1 και όλα τα κλειδιά που προέρχονται από αυτή την καμπύλη χρησιμοποιούν το ίδιο σημείο G. Επειδή το σημείο γεννήτριας είναι πάντα το ίδιο για όλους τους χρήστες του Ethereum, ένα ιδιωτικό κλειδί k πολλαπλασιασμένο με G θα έχει πάντα ως αποτέλεσμα το ίδιο κοινό κλειδί K [34].

Ψηφιακές Υπογραφές με ECDSA

Το πρότυπο ECDSA ορίζεται για ελλειπτικές καμπύλες πάνω στο σώμα πρώτων αριθμών Z_p και Galois $GF(2^m)$.Η δημιουργία κλειδιών στον ECDSA ακολουθούν τα εξής βήματα [32]:

Ορισμός 3. *1. Χρήση μιας ελλειπτικής καμπύλης E που έχει τα εξής χαρακτηριστικά a) έχει ένα modulus p, β)έχει συντελεστές a και b, γ) έχει ένα σημείο A το οποίο είναι το σημείο γεννήτορας της κυκλικής ομάδας των συντεταγμένων πρώτων αριθμών q.*

2. *Επιλογή ενός τυχαίου σημείου* $d, 0 < d < q$

3. *Υπολογισμός του* $B = dA$. *Οπότε τα κλειδιά είναι:* $k_{pub} = (p, a, b, q, A, B)$ *και* $k_{pr} = (d)$.

Έτσι έχει δημιουργηθεί ένα πρόβλημα διακριτού λογαρίθμου όπου ο ακέραιος d είναι το ιδιωτικό κλειδί και το αποτέλεσμα του βαθμωτού πολλαπλασιασμού, και το σημείο B είναι το δημόσιο κλειδί [32]. Επίσης η κυκλική ομάδα έχει μια τάξη q η οποία θα πρέπει να έχει μέγεθος τουλάχιστον 160 bit. Μια υπογραφή ECDSA αποτελείται από ένα ζεύγος ακεραίων (r, s). Κάθε τιμή έχει το ίδιο μήκος bit με το q, πράγμα που κάνει για αρκετά συμπαγείς υπογραφές. Χρησιμοποιώντας το δημόσιο και ιδιωτικό κλειδί, η υπογραφή για ένα μήνυμα ξ υπολογίζεται ως εξής:

1. Επιλογή του εφήμερου κλειδιού, που είναι ένας τυχαίος ακέραιος αριθμός, $k_e, 0 < k_e < q$.

2. Υπολογισμός του $R, R = k_e A$.

3. $r = x_R$.

4. Υπολογσιμός του $s \equiv (h(x) + d * r)(k_E)^{-}1 \bmod q$.

Στο βήμα 3 η συντεταγμένη χ του σημείου R ορίζεται στην μεταβλητή r. Το μήνυμα χ πρέπει να περάσει μέσα από μια συνάρτηση διασποράς h ώστε να υπολογιστεί το s [32]. Το μήκος της εξόδου της συνάρτησης διασποράς πρέπει να είναι τουλάχιστον όσο το q. Οπότε η διαδικασία της επαλήθευσης της υπογραφής με ECDSA είναι η εξής [32]:

1. Υπολογισμός της βοηθητικής τιμής $w \equiv s^{-1} \bmod *q$
2. Υπολογισμός της βοηθητικής τιμής $u_1 \equiv w * h(x) \bmod q$.
3. Υπολογισμός της βοηθητικής τιμής $u_2 \equiv w * r \bmod q$.
4. Υπολογισμός $P = (u_1 A) + (u_2) * B$.
5. Και τέλος η επαλήθευση με $ver_{k_{pub}}(x,(r,s))$,όπου:

$$x_P \left\{ \begin{array}{ll} \equiv r(\bmod\ q), & \Rightarrow \text{επιβεβαιωμένη υπογραφή} \\ \not\equiv r(\bmod\ q), & \Rightarrow \text{μη επιβεβαιωμένη υπογραφή} \end{array} \right\}$$

.

Στο 5ο βήμα, το x_P δηλώνει τη συντεταγμένη x του σημείου R. Στην επαλήθευση δέχεται μια υπογραφή (r,s) μόνο εάν το x_P έχει την ίδια τιμή με την παράμετρο της υπογραφής, δηλαδή r modulo q. Διαφορετικά, η υπογραφή θεωρείται άκυρη [32].

Απόδειξη. Αποδεικνύεται ότι μια υπογραφή (r,s) ικανοποιεί την προϋπόθεση επαλήθευσης $r \equiv x_P \bmod q$. Έστω η παράμετρος υπογραφής s [32]: $s \equiv (h(x) + d_r) * k_E^{-1} \bmod q$

Το οποίο ισούται με: $k_E \equiv s^{-1}h(x) + ds^{-1}r \bmod q$ Έστω ότι το δεξιό μέρος της εξίσωσης εκφράζεται ως προς u_1 και u_2, $k_E \equiv u_1 + d \times u_2 \bmod q$ Εφόσον το σημείο A παράγει μια κυκλική ομάδα της τάξης q, μπορούμε να πολλαπλασιάσουμε και τις δύο πλευρές της εξίσωσης με το A: $k_E \times A = (u_1 + d \times u_2) \times A$. Επειδή ισχύει η προσεταιριστική ιδιότητα στις ομάδες: $k_E \times A = u_1 \times A + d \times u_2 \times A$,

$k_E \times A = u_1 \times A + u_2 \times B$.

□

Οπότε εάν χρησιμοποιηθεί το σωστό κλειδί τότε το κλειδί $k_E \times A$ θα ισούται με το άθροισμα $u_1 \times A + u_2 \times B$, το οποίο ισχύει [32]. Στο Ethereum και στο Bitcoin είναι απαραίτητη η χρήση του μοντέλου ECDSA καθώς είναι ο μοναδικός τρόπος που χρησιμοποιούνται για την ταυτοποίηση του χρήστη (του ιδιωτικού και δημόσιου κλειδιού του) και την δημιουργία της διεύθυνσής του χρήστη [32]. Πιο συγκεκριμένα στο Ethereum ισχύει το εξής [42]:

Ορισμός 4. *Για ένα δεδομένο ιδιωτικό κλειδί p_r, η διεύθυνση Ethereum $A(p_r)$ μεγέθους 160-bit, ορίζεται ως τα τελευταία 160-bits από τα δεξιά, της συνάρτησης διασποράς Keccak που εφαρμόζεται στο αντίστοιχο δημόσιο κλειδί του του αλγορίθμου ECDSA του χρήστη [42]:* $A(p_r) = B96 \ldots 255(KEC(ECDSAPUBKEY(p_r)))$.

Κεφάλαιο 3

Το πρότυπο του Blockchain

Σε αυτό το Κεφάλαιο θα μελετήσουμε την δομή και την αρχιτεκτονική του Bitcoin blockchain, που ήταν και το πρώτο blockchain που δημιουργήθηκε. Θα παρατηρήσουμε αυτήν την τεχνολογία από την τεχνικής της πλευρά και δεν θα ασχοληθούμε με το οικονομικό κομμάτι του Bitcoin και τα κρυπτονομίσματα.

3.1 Τα επίπεδα του Blockchain

Αρχικά, πριν να ξεκινήσουμε την περιγραφή του blockchain και την λειτουργικότητα του, θα πρέπει να δεχτούμε ότι ένα λειτουργικό σύστημα είναι ένα σύνολο από διαφορετικά επίπεδα. Για αρχή, μπορούμε να διακρίνουμε το επίπεδο εφαρμογής και το επίπεδο λειτουργικότητας, καθώς και τις οπτικές του τι κάνει εάν σύστημα και το πως το κάνει. Το τι κάνει μια εφαρμογή (λειτουργική - functional) στο επίπεδο εφαρμογής, είναι τα πιο προφανή στοιχεία ενός συστήματος (γιατί εξυπηρετούν τους χρήστες), ενώ το πως κάνει κάτι μια εφαρμογή (μη-λειτουργική - nonfunctional) σε επίπεδο λειτουργικότητας δεν θεωρούνται τόσο σημαντικά. Πολύ σημαντικά επίσης είναι τα τρία συστατικά στοιχεία της μη λειτουργικής πλευράς ενός συστήματος τα οποία είναι [23] :

1. **Ακεραιότητα δεδομένων**: Τα δεδομένα που χρησιμοποιεί ένα σύστημα είναι ολοκληρωμένα, σωστά και δεν δέχονται αμφιβολία.

2. **Ακεραιότητα συμπεριφοράς**: Το σύστημα συμπεριφέρεται όπως πρέπει χωρίς λογικά λάθη.

3. **Ασφάλεια**: Το σύστημα έχει την ικανότητα να περιορίζει την πρόσβαση στα δεδομένα του μόνο στους εγκεκριμένους χρήστες.

Οπότε οι περισσότερες αποτυχίες του λογισμικού οφείλονται σε χαμένες πληροφορίες ή μη λογική συμπεριφορά συστήματος ή παράνομη προσπέλαση δεδομένων και δημιουργούνται από παραβιασμένη ακεραιότητα.

Όπως και τα πρωτόκολα TCP/IP και OSI χωρίζονται σε επίπεδα στοίβας, έτσι και η τεχνολογία blockchain χωρίζεται και αυτό σε επίπεδα. Η πολυεπίπεδη προσέγγιση στη στοίβα TCP/IP είναι στην πραγματικότητα ένα πρότυπο για την επίτευξη ενός ανοιχτού συστήματος [43]. Η κατοχύρωση των αφαιρετικών επιπέδων βοηθά στην καλύτερη κατανόηση της στοίβας [43]. Επίσης, το ότι είναι πιο αφαιρετικά τα επίπεδα μεταξύ τους καθιστά το σύστημα πιο ανθεκτικό και εύκολο στη συντήρησή του [43]. Στο blockchain, δεν υπάρχουν ακόμη συμφωνημένα παγκόσμια πρότυπα που θα διαχωρίζουν με σαφήνεια τα τμήματα του σε ξεχωριστά στρώματα. Απαιτείται σίγουρα μια πολυεπίπεδη αρχιτεκτονική, αλλά προς το παρόν αυτό είναι ακόμα ΄ρευστό΄. Όπως φαίνεται στην Εικόνα 3.1, τα επίπεδα του blockchain χωρίζονται σε πέντε συνολικά επίπεδα, το επίπεδο της εφαρμογής, της εκτέλεσης, τη σημασίας, της διάδοσης και της συναίνεσης.

Επίπεδο Εφαρμογής Αυτό είναι το επίπεδο όπου προγραμματίζονται οι λειτουργίες και δημιουργείται μια εφαρμογή για τους χρήστες. Συνήθως περιλαμβάνει μια δομή δεδομένων τύπου στοίβας για την ανάπτυξη λογισμικού, όπως για παράδειγμα είναι η διεπαφη με τον χρήστη. Για τις εφαρμογές που αντιμετωπίζουν το blockchain ως σύστημα υποστήριξης, αυτές οι εφαρμογές ενδέχεται να χρειαστεί να φιλοξενούνται σε ορισμένους διακομιστές ιστού και μπορεί να απαιτούν ανάπτυξη εφαρμογών ιστού ή άλλες παρόμοιες τεχνολογίες [43].

Επίπεδο Εκτέλεσης Το επίπεδο εκτέλεσης αφορά τις εκτελέσεις των εντολών που δημιουργούνται από το επίπεδο εφαρμογής και εφαρμόζονται σε όλους τους κόμβους ενός δικτύου blockchain [43]. Ένα πρόγραμμα ή ένα σενάριο πρέπει να εκτελεστεί για να διασφαλιστεί η σωστή εκτέλεση της συναλλαγής. Όλοι οι κόμβοι σε ένα δίκτυο blockchain πρέπει να εκτελέσουν τα προγράμματα ανεξάρτητα ο ένας από τον άλλον. Η καθοριστική εκτέλεση προγραμμάτων στο ίδιο σύνολο εισόδου και συνθηκών παράγει πάντα την ίδια έξοδο σε όλους τους κόμβους, πράγμα που βοηθά στην αποφυγή ασυμφωνιών [43].

Επίπεδο Σημασίας Το Επίπεδο Σημασίας είναι ένα λογικό επίπεδο επειδή υπάρχει οργάνωση στις συναλλαγές και στα μπλοκ [43]. Μια συναλλαγή, είτε έγκυρη είτε άκυρη, έχει ένα σύνολο οδηγιών που μεταφέρεται μέσω του επιπέδου εκτέλεσης, αλλά επικυρώνεται στο επίπεδο αυτό [43]. Για την χρήση του Bitcoin, πρέπει να χρησιμοποιηθεί μία ή περισσότερες προηγούμενες συναλλαγές και δεν υπάρχει λογαριασμός χρήστη [43]. Αυτό σημαίνει ότι όταν κάποιος πραγματοποιεί μια συναλλαγή, χρησιμοποιεί το ποσό που έχει δεχθεί από προηγούμενες συναλλαγές του και πρέπει το άθροισμα τους να είναι τουλάχιστον ίσο με το ποσό που θέλει ξοδέψει. Αυτή η συναλλαγή πρέπει να επικυρωθεί από όλους τους κόμβους που διέρχονται προηγούμενες συναλλαγές για να διαπιστώσουν εάν πρόκειται για νόμιμη συναλλαγή [43]. Το Ethereum, από την άλλη πλευρά, έχει το σύστημα λογαριασμών και δεν βασίζεται στην λογική της προηγούμενης συναλλαγής, όπως συμβαίνει στο Bitcoin [43].

Ένα μπλοκ περιέχει συνήθως μια ομάδα συναλλαγών και ορισμένα έξυπνα συμβόλαια. Οι δομές δεδομένων όπως το δέντρο Merkle ορίζονται σε αυτό το επίπεδο [43]. Επίσης, σε αυτό το επίπεδο ορίζεται το πως θα συνδέονται τα μπλοκ μεταξύ τους. Όλα τα μπλοκ περιέχουν την σύνοψη του προηγούμενου μπλοκ, μέχρι το πρώτο μπλοκ που δημιουργήθηκε ποτέ, δηλαδή το μπλοκ ΄γέννεση΄ (genesis [43]).

Επίπεδο Διάδοσης Το Επίπεδο Διάδοσης είναι το ομότιμο επίπεδο επικοινωνίας (peer-to-peer) που επιτρέπει στους κόμβους να ανακαλύπτουν το ένα το άλλο και να επικοινωνούν και να συγχρονίζονται μεταξύ τους σε σχέση με την τρέχουσα κατάσταση του δικτύου [43]. Όταν γίνεται μια συναλλαγή, γνωρίζουμε ότι μεταδίδεται σε ολόκληρο το δίκτυο. Ομοίως, όταν ένας κόμβος θέλει να προτείνει ένα έγκυρο μπλοκ, αυτό μεταδίδεται αμέσως σε ολόκληρο το δίκτυο, έτσι ώστε οι άλλοι κόμβοι να μπορούν να βασιστούν σε αυτό, θεωρώντας το ως το τελευταίο μπλοκ [43]. Επομένως, η διάδοση μιας συναλλαγής ή μπλοκ στο δίκτυο ορίζεται σε αυτό το επίπεδο, πράγμα που διασφαλίζει τη σταθερότητα ολόκληρου του δικτύου. Με το σχεδιασμό, τα περισσότερα blockchain σχεδιάζονται έτσι ώστε να προωθούν αμέσως μια συναλλαγή ή μπλοκ σε όλους τους κόμβους με τους οποίους συνδέονται άμεσα [43].

Επίπεδο Συναίνεσης Το Επίπεδο Συναίνεσης είναι συνήθως το βασικότερο επίπεδο για τα περισσότερα συστήματα blockchain δίκτυα [43]. Ο πρωταρχικός σκοπός αυτού του επιπέδου είναι να συμφωνήσουν όλοι οι κόμβοι μεταξύ τους για την κατάσταση του κατάσοτιχου του δικτύου [43]. Θα μπορούσαν να υπάρξουν διαφορετικοί τρόποι επίτευξης συναίνεσης μεταξύ των κόμβων, ανάλογα με την περίπτωση χρήσης [43]. Η ασφάλεια του blockchain είναι ενσωματωμένη σε αυτό το στρώμα. Στο Bitcoin ή στο Ethereum, η συναίνεση επιτυγχάνεται με τις κατάλληλες τεχνικές κινήτρων που ονομάζονται έξόρυξή΄ [43]. Για να είναι αυτοσυντηρούμενο ένα δημόσιο blockchain, πρέπει να υπάρχουν κάποιοι μηχανισμοί παροχής κινήτρων που όχι μόνο βοηθούν στη διατήρηση του δικτύου ζωντανές αλλά και επιβάλλουν ομοφωνία [43]. Τα Bitcoin και Ethereum χρησιμοποιούν ένα μοντέλο συναίνεσης, αυτό της Απόδειξη Εργασίας (PoW) [43]. Μόλις προταθεί αυτό το μπλοκ και διαδοθεί σε όλους τους κόμβους, ελέγχουν για να δουν αν είναι έγκυρο μπλοκ με όλες τις νόμιμες συναλλαγές και ότι το παζλ (PoW) επιλύθηκε σωστά. Στην συνέχεια, προσθέτουν αυτό το μπλοκ στο δικό τους αντίγραφο του blockchain και ΄χτίζουν΄ πάνω σε αυτό [43].

3.2 Αρχιτεκτονική

Υπάρχουν δυο ειδών αρχιτεκτονικές λειτουργικού συστήματος, το κεντροποιημένο σύστημα, όπου όλοι οι κόμβοι είναι συνδεδεμένοι με έναν κεντρικό και το κατανεμημένο σύστημα, όπου όλοι οι κόμβοι είναι συνδεδεμένοι ο ένας με τον άλλον έμμεσα. Τα θετικά του κατανεμημένου συστήματος είναι [23]:

Σχήμα 3.1: Τα επίπεδα του blockchain

- **Υψηλότερη υπολογιστική ισχύς:** Δηλαδή η ισχύς όλων τον υπολογιστών-κόμβων σχετίζονται μεταξύ τους και παράγουν συνολικά μεγαλύτερη υπολογιστική ισχύ.

- **Μικρότερο κόστος:** Η διατήρηση και επισκευή ενός επιμέρους κομματιού του κατανεμημένου συστήματος είναι πολύ πιο φθηνό από την επισκευή ενός υπερυπολογιστή.

- **Μεγαλύτερη αξιοπιστία:** Αν ένας κόμβος αποτύχει ή χαλάσει τότε οι υπόλοιποι κόμβοι μπορούν να αναλάβουν την εργασία του, ενώ σε ένα κεντροποιημένο σύστημα άμα χαλάσει ο κεντρικός υπολογιστής τότε καταρρέει όλο το σύστημα αυτό.

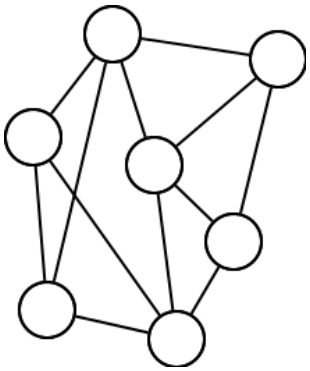
- **Ικανότητα να αναβαθμίζεται φυσικά:** Η υπολογιστική ισχύς ενός τέτοιου συστήματος μπορεί να αυξηθεί πολύ εύκολα αν κάνεις συνδέσει επιπλέον υπολογιστές, ενώ ένας μεμονωμένος υπολογιστής για να αυξήσει την υπολογιστική του ισχύ πρέπει να αντικατασταθεί εξολοκλήρου.

Παρόλα αυτά, ένα κατανεμημένο σύστημα περιλαμβάνει και αρκετά αρνητικά σε σχέση με έναν αυτόνομο υπολογιστή όπως [23]:

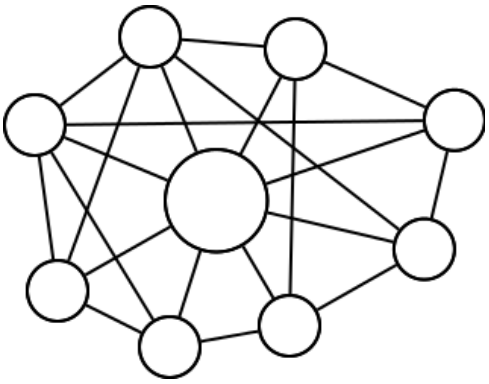
- **Έλλειψη συντονισμού.** Τα κατανεμημένα συστήματα δεν έχουν μια κεντρική οντότητα να συντονίζει τα επιμέρους μέλη του οπότε, τα μέλη αυτά πρέπει να αυτό-συντονίζονται το οποίο είναι αρκετά δαπανηρό.

- **Χάσιμο χρόνου επικοινωνίας.** Τα κατανεμημένα συστήματα πρέπει να επικοινωνούν μεταξύ τους, όμως αυτή η διαδικασία σπαταλάει πολύτιμο χρόνο και υπολογιστική ισχύ.

- **Εξάρτηση δικτύου.** Ένα τέτοιο σύστημα χρειάζεται απαραιτήτως ένα δίκτυο μέσω του οποίου θα γίνεται η εσωτερική επικοινωνία. Κάθε δίκτυο όμως έχει τα δικά του μειονεκτήματα.



Σχήμα 3.2: Κατανεμημένο Σύστημα



Σχήμα 3.3: Υβριδικό Σύστημα

- **Μεγαλύτερη πολυπλοκότητα.** Η επίλυση των προηγούμενων αρνητικών χαρακτηριστικών ενός κατανεμημένου συστήματος απαιτεί μεγάλη πολυπλοκότητα.

- **Θέματα ασφάλειας.** Από την στιγμή που ένα κατανεμημένο σύστημα απαιτεί δίκτυο τότε υπάρχει ο κίνδυνος μη ασφαλής μετάδοσης του μηνύματος.

Στην πραγματικότητα όμως τα σύγχρονα συστήματα χρησιμοποιούν έναν συνδυασμό και των δυο τύπων συστήματος.

Όταν δημιουργούμε μια εφαρμογή μπορούμε να διαλέξουμε οποιαδήποτε αρχιτεκτονική. Όμως και οι δυο έχουν αρνητικά και θετικά, τα οποία επηρεάζουν την λειτουργική και μη λειτουργική πλευρά της εφαρμογής και δεν αποδίδουν πλήρη ακεραιότητα. Το blockchain έρχεται λοιπόν να λύσει αυτό το πρόβλημα καθώς μπορεί να αποδώσει πλήρη ακεραιότητα σε ένα κατανεμημένο σύστημα και μπορεί να πετύχει τη μη λειτουργικότητα σε επίπεδο 'εφαρμογής'.

3.2.1 Ομότιμα Συστήματα

Ένα ομότιμο σύστημα (peer-to-peer) είναι ένα κατανεμημένο σύστημα, που αποτελείται από κόμβους που διαμοιράζει άμεσα τους πόρους τους. Το blockchain χρησιμοποιείται σε αυτά τα συστήματα για να αποδώσει ακεραιότητα. Η ακεραιότητα και εμπιστοσύνη στο σύστημα είναι τα δυο βασικότερα χαρακτηριστικά στα ομότιμα συστήματα [23]. *Ακεραιότητα* είναι μια μη λειτουργική πλευρά του συστήματος. Αυτή πρέπει να είναι ασφαλής και χωρίς λάθη, καθώς αυτό επιτυγχάνεται πολύ εύκολα, εάν είναι γνωστός ο αριθμός των κόμβων και το κατά πόσο έμπιστοι είναι αυτοί. Η *Αξιοπιστία* αφορά το κατά πόσο ο ανθρώπινος παράγοντας είναι εμπιστεύσιμος/αξιόπιστος, καθώς αυτό θα αποδείξει το αν αξίζει να εμπιστευτεί ένας καινούργιος χρήστης το σύστημα. Παρόλα αυτά για να επιτευχθούν αυτά τα δυο πρέπει να ξεπεραστούν δυο πολύ βασικοί κίνδυνοι, οι οποίοι είναι [23] :

- **Τεχνικά Σφάλματα.** Δηλαδή υλισμικά και λογισμικά λάθη που υπάρχουν σε ένα σύστημα και στο δίκτυο του.

- **Κακόβουλοι Χρήστες.** Όπου είναι χρήστες οι οποίοι επιδιώκοντας τους δικούς τους σκοπούς βλάπτουν το σύστημα ή τους άλλους χρήστες.

3.3 Ιδιοκτησία

Αρχικά για να υπάρχει η έννοια της ιδιοκτησίας πρέπει να ισχύουν τρεις συνθήκες ταυτόχρονα [23]:

1. Πρέπει να υπάρχει η ταυτότητα του ιδιοκτήτη
2. Απόδειξη ότι το αντικείμενο έχει αγοραστεί
3. Και η σύνδεση των δυο παραπάνω μεταξύ τους.

Με μια ιστορική προσέγγιση μπορούμε να παρατηρήσουμε ότι, είναι δύσκολο κάποιος να αποδείξει ότι του ανήκει κάτι, πάρα μόνον αν έχει μάρτυρες που να το εξακριβώνουν. Σήμερα πλέον υπάρχουν επίσημα έγγραφα που αποδεικνύουν ότι κάτι ανήκει σε κάποιον (π.χ. ένα σπίτι μέσα από συμβολαιογραφική πράξη - κατάστιχο και αρχεία).

Σχήμα 3.4: Ιδιοκτησία

Στο παραπάνω Σχήμα 3.4 οι οντότητες των πάνω επιπέδων είναι πιο γενικές από αυτές των κάτω. Οι κάτω οντότητες είναι σε άμεση συσχέτιση με τις αμέσως πάνω. Για παράδειγμα, η απόδειξη της ιδιοκτησίας απαιτεί την ταυτοποίηση των στοιχείων, την αυθεντικοποίηση στοιχείων και την εξουσιοδότηση, για να επιβεβαιώσουν τον νόμιμο κάτοχο της ιδιοκτησίας.

Οι χαμηλότερες οντότητες αναπαριστούν το επίπεδο της λειτουργικότητας. Οι τρεις βασικές έννοιες της ασφάλειας είναι οι εξής [23]:

- **Ταυτοποίηση.** Με την ταυτοποίηση εννοείται όταν κάποιος ισχυρίζεται ότι είναι κάποιος συγκεκριμένος. Η ταυτοποίηση δεν αποδεικνύει το ποιος είναι πραγματικά καθώς δεν εμπεριέχει κάποια απόδειξη.

- **Αυθεντικοποίηση.** Ο σκοπός της αυθεντικοποίησης είναι να αποτρέψει κάποιον να ισχυριστεί ότι είναι κάποιος άλλος. Αυθεντικοποίηση σημαίνει ότι υπάρχουν αποδείξεις για το πιος πραγματικά είναι. Η απόδειξη είναι μοναδική για τον κάθε άνθρωπο (π.χ. Α.Τ.).

- **Εξουσιοδότηση.** Με την εξουσιοδότηση εννοείται, η εκχώρηση του δικαιώματος από έναν χρήστη σε έναν άλλον, για μια συγκεκριμένη ενέργεια, την οποία έχει μόνο ο πρώτος χρήστη. Η εξουσιοδότηση έπεται της επιτυχημένης ταυτοποίησης και αυθεντικοποίησης του χρήστη.

Στο παρακάτω σχήμα 3.5 φαίνεται πως η απόδειξη και η μεταβίβαση της ιδιοκτησίας είναι σχετικές με ένα κατάστιχο.

Σχήμα 3.5: Οντότητες ενός Κατάστιχου

Το παραπάνω Σχήμα 3.5 απεικονίζει ένα κατάστιχο που πρέπει να εκπληρώσει δυο αντίθετους ρόλους, ο ένας είναι να αποδεικνύει την ιδιοκτησία διαβάζοντας το ιστορικό δεδομένων, και ο άλλος να καταγράψει την οποιαδήποτε μεταβίβαση της ιδιοκτησίας. Οπότε, υπάρχει σύγκρουση μεταξύ της διαφάνειας της ιδιοκτησίας, καθώς μόνο έτσι μπορεί να αποδειχτεί η ιδιοκτησία και της ιδιωτικότητας των προσωπικών δεδομένων του ιδιοκτήτη. Αυτή η σύγκρουση υπάρχει και στο blockchain, καθώς αποτελεί ένα κατανεμημένο ομότιμο σύστημα με μια δομή κατάστιχου και μπορεί να διαβαστεί από τον οποιοδήποτε [23]. Το blockchain έλυσε αυτήν την σύγκρουση μεταξύ διαφάνειας και ιδιωτικότητας και έχει κάποια κοινά χαρακτηριστικά με το κατάστιχο όπως για παράδειγμα [23]:

- Ένα κατάστιχο χρησιμοποιείται για την διατήρηση των τίτλων ιδιοκτησίας το οποίο είναι ίδιο με την δομή του blockchain και αποθηκεύει τα δεδομένα.
- Τα κατάστιχα αποθηκεύονται σαν κόμβοι σε ένα ομότιμο σύστημα
- Ακεραιότητα σε αυτό το σύστημα είναι η ικανότητα να δηλώνει κάποιος την πραγματική

του ιδιοκτησία

- Η κρυπτογραφία είναι απαραίτητη για να δημιουργηθούν έμπιστα μέσα ταυτοποίησης, αυθεντικοποίησης και εξουσιοδότησης, τα οποία εξασφαλίζουν την ασφάλεια των δεδομένων.

Τα κεντροποιημένα κατάστιχα έχουν ελαττώματα, όπως ότι χρειάζεται αντίγραφα σε περίπτωση απώλειας, επικυρώνει συναλλαγές, να περιλαμβάνει όλες τις εξακριβωμένες συναλλαγές και να μην τροποποιεί το ιστορικό τους. Υπάρχουν όμως και τα κατανεμημένα κατάστοιχα που διαφέρουν από τα κατάστοιχα που αναφέρονται παραπάνω.Η λειτουργία των κατανεμημένων κατάστιχων DLT είναι θεμελιωδώς διαφορετική από ένα δημόσιο blockchain. Τα DLT δεν εκτελούν εξόρυξη, καθώς όλοι οι συμμετέχοντες έχουν ήδη ελεγχθεί και είναι γνωστοί στο δίκτυο και δεν υπάρχει απαίτηση για εξόρυξη ώστε να υπάρξει το το δίκτυο. Επίσης, δεν υπάρχει έννοια για το ψηφιακό νόμισμα [40]. Σε ένα δημόσιο blockchain, η πρόσβαση είναι ανοιχτή σε όλους και απαιτεί κάποια μορφή κινήτρου και επίδρασης δικτύου για να αναπτυχθεί [40]. Αντίθετα, σε ένα DLT, δεν υπάρχουν τέτοιες απαιτήσεις. Είναι δυνατή η κατασκευή πιστοποιημένων DLT με την χρήση του Ethereum σε ιδιωτικές εγκαταστάσεις κοινοπραξιών, για την λειτουργία χρηματοπιστωτικού συστήματος [40]. Το βασικό όφελος των κατανεμημένων κατάστιχων είναι ότι είναι πολύ ταχύτερα και πιο εύχρηστα [40].

3.4 Το πρόβλημα της διπλής κατανάλωσης

Σε ένα ομότιμο σύστημα, όταν γίνεται μια ανταλλαγή μεταξύ ενός Α και ενός Β, τότε υπάρχει μια μεγάλη καθυστέρηση για να ενημερωθούν όλοι οι χρήστες ότι ο Β πήρε κάτι από τον Α. Σε αυτήν την περίπτωση ένας κακόβουλος Α θα μπορούσε να πάει να ανταλλάξει το ίδιο ακριβώς αντικείμενο με έναν Γ όπου δεν ενημερώθηκε για την ανταλλαγή μεταξύ των δυο πρώτων, αλλά αυτό το αντικείμενο πρέπει να το έχει στην κατοχή του μόνο ένας, οπότε προκύπτει το πρόβλημα της διπλής κατανάλωσης. Αυτό το πρόβλημα υποδιαιρείται σε τρία υπο-προβλήματα που όμως στο blockchain έχουν βρει λύση [23]:

- **Αντιγραφή ψηφιακών αγαθών.** Ένα ψηφιακό αγαθό μπορεί να αντιγράφει αρκετά εύκολα χωρίς να το παρατηρήσει κάνεις. Η λύση έπεται στην φύση της ιδιοκτησίας, δηλαδή, η σύνδεση του συγκεκριμένου αντικειμένου με τον ιδιοκτήτη. Αυτό μπορεί να επιτευχθεί με ένα κατάστιχο επιτρέποντας έτσι αυτό το αντικείμενο να ανταλλάσσετε 1 φορά κάθε φορά.

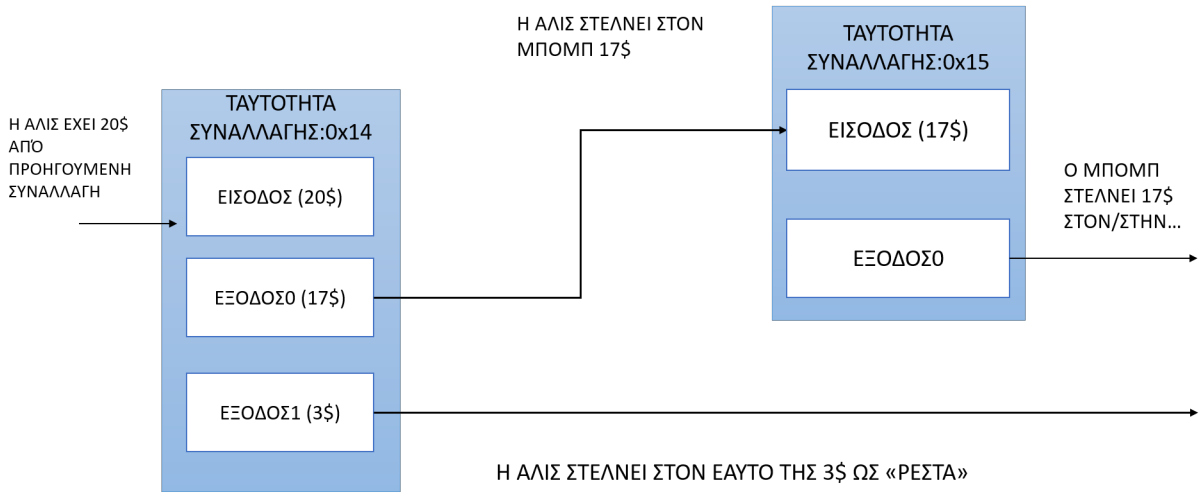
- **Ομότιμα συστήματα.** Σε ένα ομότιμο σύστημα που χρησιμοποιούνται κατάστιχα μπορεί να χρειαστεί πολύ χρόνο για να περαστεί η πληροφορία, ότι έγινε η ανταλλαγή μεταξύ δυο χρηστών, οπότε έχουμε το πρόβλημα της διπλής κατανάλωσης [23]. Το blockchain όμως κρύβει την λύση σε αυτό το πρόβλημα μέσα στην δομή του και την αρχιτεκτονική του.

- **Παραβίαση ακεραιότητας σε ομότιμα συστήματα.** Η διαχείριση των δεδομένων σε ένα ομότιμο σύστημα γίνεται από τους ίδιους τους χρήστες οπότε το πρόβλημα της διπλής κατανάλωσης είναι εύκολα υλοποιήσιμο σε ένα τέτοιο σύστημα. Εδώ η λύση εξαρτάται από την φύση του ομότιμου συστήματος.

3.5 Συναλλαγές

Η συναλλαγή είναι η καταγραφή της μεταφοράς περιουσιακών στοιχείων (π.χ. κρυπτονομίσματα) μεταξύ δύο οντοτήτων. Μια συναλλαγή προϋποθέτει τουλάχιστον τα παρακάτω πεδία [23]:

- **Ποσότητα:** Η συνολική ποσότητα των ψηφιακών αγαθών που θα μεταφερθούν
- **Είσοδος:** Μια λίστα από ψηφιακά περιουσιακά στοιχεία που θα μεταφερθούν. Το κάθε ψηφιακό περιουσιακό στοιχείο είναι μοναδικό και μπορεί να έχει διαφορετικές τιμές από αλλά αγαθά. Παρόλα αυτά, τα υπάρχοντα ψηφιακά περιουσιακά στοιχεία δεν μπορούν να δημιουργήσουν υλικά αγαθά, ενώ τα ψηφιακά περιουσιακά στοιχεία μπορούν να διαιρεθούν σε νέα ψηφιακά περιουσιακά στοιχεία ή να προστεθούν σε λιγότερα.
- **Έξοδος:** Αναφέρεται στους λογαριασμούς που θα λάβουν τα ψηφιακά περιουσιακά στοιχεία. Κάθε έξοδος περιλαμβάνει την τιμή που πρέπει να μεταφερθεί στον νέο κάτοχο, την ταυτότητα του νέου παραλήπτη, και μια σειρά από όρους που πρέπει να ικανοποιεί ο παραλήπτης.
- **ID Συναλλαγής/Σύνοψη**: Ένα μοναδικό κλειδί για κάθε συναλλαγή. Κάποια blockchain χρησιμοποιούν ένα ID, ενώ άλλα τη σύνοψη ως κλειδί για μια συναλλαγή.



Σχήμα 3.6: Παράδειγμα μιας Συναλλαγής.

Ο καθορισμός της εγκυρότητας μιας συναλλαγής είναι πολύ σημαντικός, δεδομένου ότι μπορεί κάποιος να ισχυρίζεται ότι έγινε μια συναλλαγή, ενώ αυτή δεν πραγματοποιήθηκε ποτέ [23].

Ασύμμετρη Κρυπτογραφία

Στην ασύμμετρη κρυπτογραφία έχουμε δυο κλειδιά, το δημόσιο και το ιδιωτικό, που συνδέονται με μαθηματικό τρόπο. Το δημόσιο κλειδί σε αντίθεση με το ιδιωτικό είναι γνωστό σε όλους. Η ασύμμετρη κρυπτογραφία έχει τις εξής εφαρμογές στο blockchain [23]:

- Τα ιδιωτικά κλειδιά χρησιμοποιούνται για την υπογραφή των συναλλαγών.
- Τα δημόσια κλειδιά χρησιμοποιούνται για να σηματοδοτούν την διεύθυνση προέλευσης, επιτρέποντας την ψευδο-ανωνυμία.
- Τα δημόσια κλειδιά χρησιμοποιούνται για να επαληθεύουν τις υπογραφές με τα ιδιωτικά κλειδιά.
- Η ασύμμετρη κρυπτογραφία δίνει την δυνατότητα στον χρήστη που ανταλλάσει το αγαθό να εξακριβώνει, ότι έχει στην κατοχή του το ιδιωτικό κλειδί που επαληθεύει την υπογραφή.

Η διεύθυνση ενός χρήστη είναι ένα αλφαριθμητικό, το οποίο προέρχεται από το δημόσιο κλειδί του, περνώντας το μέσα από τη συνάρτηση διασποράς μαζί με άλλα δεδομένα.

$$\text{δημόσιο κλειδί} \rightarrow \text{συνάρτηση διασποράς} \rightarrow \text{διεύθυνση}$$

Οι χρήστες μπορούν να παράγουν πολλά ζευγάρια ιδιωτικών και δημόσιων κλειδιών, τα οποία επιτρέπουν πολλά επίπεδα ψευδο-ανωνυμίας. Οι διευθύνσεις λειτουργούν ως δημόσια ταυτότητα στο blockchain για ένα χρήστη και πολλές φορές μετατρέπεται σε QR code για διευκόλυνση [23]. Το ιδιωτικό κλειδί παράγεται με ασφαλή τρόπο μέσω μιας τυχαίας συνάρτησης και αποθηκεύεται σε ένα ψηφιακό *πορτοφόλι*.

3.6 Μπλοκ

Το blockchain δημιουργήθηκε μαζί με το Bitcoin, οπότε η αρχιτεκτονική του Bitcoin αποτελεί το πρότυπο του blockchain. Το κάθε blockchain έχει τη δική του αρχιτεκτονική και συστατικά στοιχεία. Το μπλοκ που περιγράφεται σε αυτήν την ενότητα παρουσιάζει το μπλοκ του Bitcoin. Οι χρήστες δικτύου blockchain υποβάλλουν υποψήφιες συναλλαγές στο δίκτυο blockchain μέσω ενός λογισμικού (web εφαρμογές, εφαρμογές smartphone, ψηφιακά πορτοφόλια, υπηρεσίες ιστού, κ.λ.π.) [20]. Το λογισμικό στέλνει αυτές τις συναλλαγές σε ένα κόμβο ή κόμβους στο δίκτυο blockchain. Οι κατανεμημένες συναλλαγές στη συνέχεια περιμένουν σε μια ουρά, μέχρι να προστεθούν στο blockchain από έναν κόμβο εξόρυξης. Οι

κόμβοι εξόρυξης είναι το υποσύνολο των κόμβων που διατηρούν το blockchain ενεργό και δημοσιεύουν νέα μπλοκ [20].

Οι συναλλαγές προστίθενται στο blockchain, όταν ένας κόμβος εξόρυξης δημοσιεύει ένα μπλοκ. Ένα μπλοκ περιλαμβάνει ένα σύνολο επικυρωμένων συναλλαγών [20]. Η «επαλήθευση» διασφαλίζεται με την κρυπτογραφική υπογραφή της συναλλαγής από τους χρήστες (που αναφέρονται στις τιμές εισόδου της συναλλαγής) [20]. Αυτό επαληθεύει ότι οι συναλλασσόμενοι είχαν πρόσβαση στο ιδιωτικό κλειδί που θα μπορούσε να υπογράψει τις συγκεκριμένες συναλλαγές [1]. Οι άλλοι κόμβοι εξόρυξης θα ελέγξουν την εγκυρότητα όλων των συναλλαγών σε ένα δημοσιευμένο μπλοκ και δεν θα αποδεχθούν ένα μπλοκ, εάν περιέχει τυχόν μη έγκυρες συναλλαγές. Μετά τη δημιουργία, κάθε μπλοκ έχει περάσει από τη συνάρτηση διασποράς δημιουργώντας έτσι μια επιτομή που αντιπροσωπεύει το μπλοκ. Η δομή ενός μπλοκ είναι αρκετά περίπλοκη, και ειδικότερα τα πεδία του περιλαμβάνουν τα ακόλουθα [20] [1]:

- Τον αριθμό του μπλοκ, γνωστό και ως *ύψος*.
- Την σύνοψη του.
- Τη σύνοψη του προηγούμενου μπλοκ. Το οποίο δημιουργεί και την εικονική αλυσίδα του blockchain.
- Τη διασπορά του Merkle tree root.
- Το μέγεθός του.
- Την τιμή του τυχαίου αριθμού μοναδικής χρήσης (*nonce*), η οποία είναι ένα νούμερο που χρησιμοποιείται από τον κόμβο εξόρυξης για να λύσει το παζλ διασποράς ώστε να δημοσιεύσουν το μπλοκ.
- Μια λίστα από συναλλαγές που περιλαμβάνονται στο μπλοκ.

Σχήμα 3.7: Δομή ενός Μπλοκ

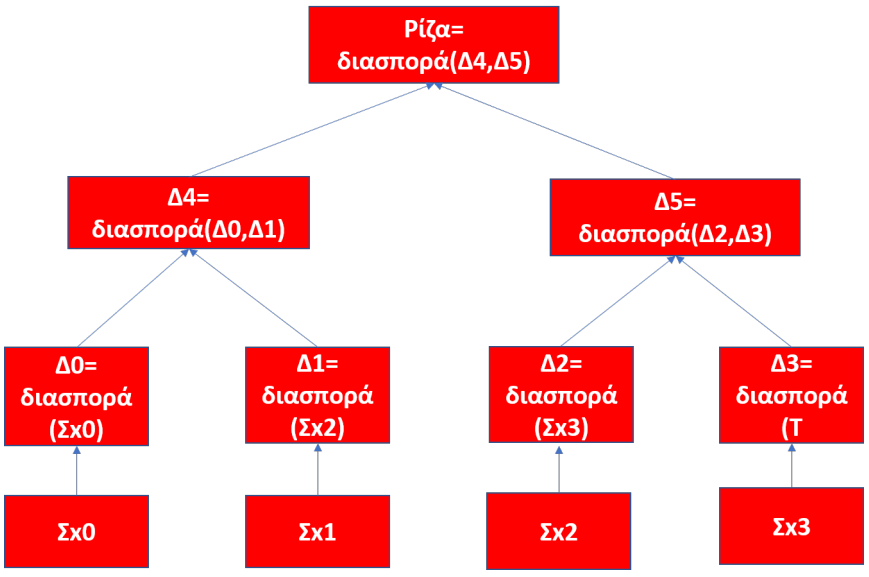
Η κεφαλίδα του μπλοκ είναι 80 *byte*, ενώ ο μέσος όρος των συναλλαγών είναι τουλάχιστον 250 *byte* και ο μέσος όρος μπλοκ περιέχει περισσότερες από 500 συναλλαγές. Ένα πλήρες μπλοκ, με όλες τις συναλλαγές είναι 1.000 φορές μεγαλύτερο από την κεφαλίδα του μπλοκ [34].

Η ταυτοποίηση ενός μπλοκ γίνεται συνήθως από την επικεφαλίδα του. Υπάρχουν δύο τρόποι για την ταυτοποίηση του μπλοκ. Ο πρώτος και βασικός τρόπος είναι μέσω της αναγνώρισης του ψηφιακού δαχτυλικού αποτυπώματος που παρήχθη από την διπλή σύνοψη του μπλοκ με τον αλγόριθμο SHA256 [34]. Αυτό έχει μήκος 32 *byte* και αναφέρεται ως η *σύνοψη της επικεφαλίδας του μπλοκ*. Για παράδειγμα η επικεφαλίδα του πρώτου μπλοκ του Bitcoin είναι το 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f (Εικόνα 4.1). Η σύνοψη της επικεφαλίδας του μπλοκ είναι μοναδική και κάθε κόμβος μπορεί να επαληθεύσει την εγκυρότητα του μπλοκ με την επανεκτέλεση της σύνοψης της επικεφαλίδας του μπλοκ [34]. Η σύνοψη του μπλοκ δεν αποθηκεύεται στο δίκτυο του blockchain αλλά, υπολογίζεται από τον κάθε κόμβο την στιγμή που ο αυτός λαμβάνει το κάθε μπλοκ. Η σύνοψη του μπλοκ αποθηκεύεται στην προσωπική βάση δεδομένων του κόμβου ως μέτρο επιτάχυνσης της ευρετηριοποίησης του μπλοκ.

Ο δεύτερος τρόπος της ταυτοποίησης του μπλοκ είναι μέσω του ύψους του μπλοκ (block height). Το πρώτο μπλοκ που δημιουργήθηκε έχει ύψος 0 (Εικόνα 4.1). Κάθε μπλοκ προστίθεται στην κορυφή από το πρώτο μπλοκ μια θέση πιο πάνω από το αμέσως προηγούμενο. Ενώ η σύνοψη του μπλοκ είναι μοναδική για κάθε μπλοκ, πολλές φορές τυγχάνει 2 μπλοκ να έχουν το ίδιο ύψος. Αυτό αποτελεί πρόβλημα στο blockchain γιατί δημιουργεί σύγκρουση μεταξύ των μπλοκ. Ο τρόπος αντιμετώπισης περιγράφεται παρακάτω.

Merkle Trees Αντί να αποθηκεύεται η σύνοψη κάθε συναλλαγής στην κεφαλίδα ενός μπλοκ, χρησιμοποιείται μια δομή δεδομένων γνωστή ως δέντρο Merkle και αυτή διαθέτει την σύνοψη όλων των συναλλαγών του blockchain [1] [34] [40]. Ένα δέντρο Merkle (ή αλλιώς δυαδικό δέντρο διασποράς ενώνει τις τιμές διασποράς των δεδομένων και τα κατηγοριοποιεί σε γονείς και παιδιά, μέχρι ότου να φτάσει στη μια και μοναδική ρίζα του δέντρου (δηλαδή μια σύνοψη ρίζας του Merkle). Η ρίζα είναι ένας αποτελεσματικός μηχανισμός που χρησιμοποιείται για την σύνοψη των συναλλαγών σε ένα μπλοκ και για την επαλήθευση της παρουσίας μιας συναλλαγής σε ένα μπλοκ. Ο αλγόριθμος διασποράς που χρησιμοποιείται στα δέντρα Merkle του Bitcoin είναι το SHA-256 και εφαρμόζεται δύο φορές συνεχόμενα. Το δέντρο Merkle έχει δομή από κάτω προς τα πάνω. Αυτή η δομή διασφαλίζει ότι τα δεδομένα που έχουν σταλεί στο κατανεμημένο σύστημα είναι έγκυρα. Ένα δέντρο Merkle 3.8 έχει τις εξής ιδιότητες [20]:

- Η κάτω σειρά αντιπροσωπεύει τα δεδομένα που πρέπει να συνοψιστούν, στο blockchain αυτά είναι τα δεδομένα της συναλλαγής.
- Η δεύτερη στην κάτω σειρά δείχνει ότι τα δεδομένα έχουν περάσει από τη συνάρτηση διασποράς και έχουν παράξει τη σύνοψη.
- Στη συνέχεια, τα δεδομένα από τη δεύτερη σειρά που έχουν συνοψιστεί, ενώνονται διαδοχικά, και από αυτήν τη νέα τιμή δημιουργείται μια νέα σύνοψη που αποθηκεύεται στα φύλλα της 3ης σειράς από το τέλος.
- Τελικά, η ρίζα δείχνει τη σύνοψη του συνδυασμού των δυο πεδίων της. Άρα, η ρίζα είναι η σύνοψη όλων των προηγούμενων συνδυασμών και διασπορών που έγιναν μέσα στο δέντρο.



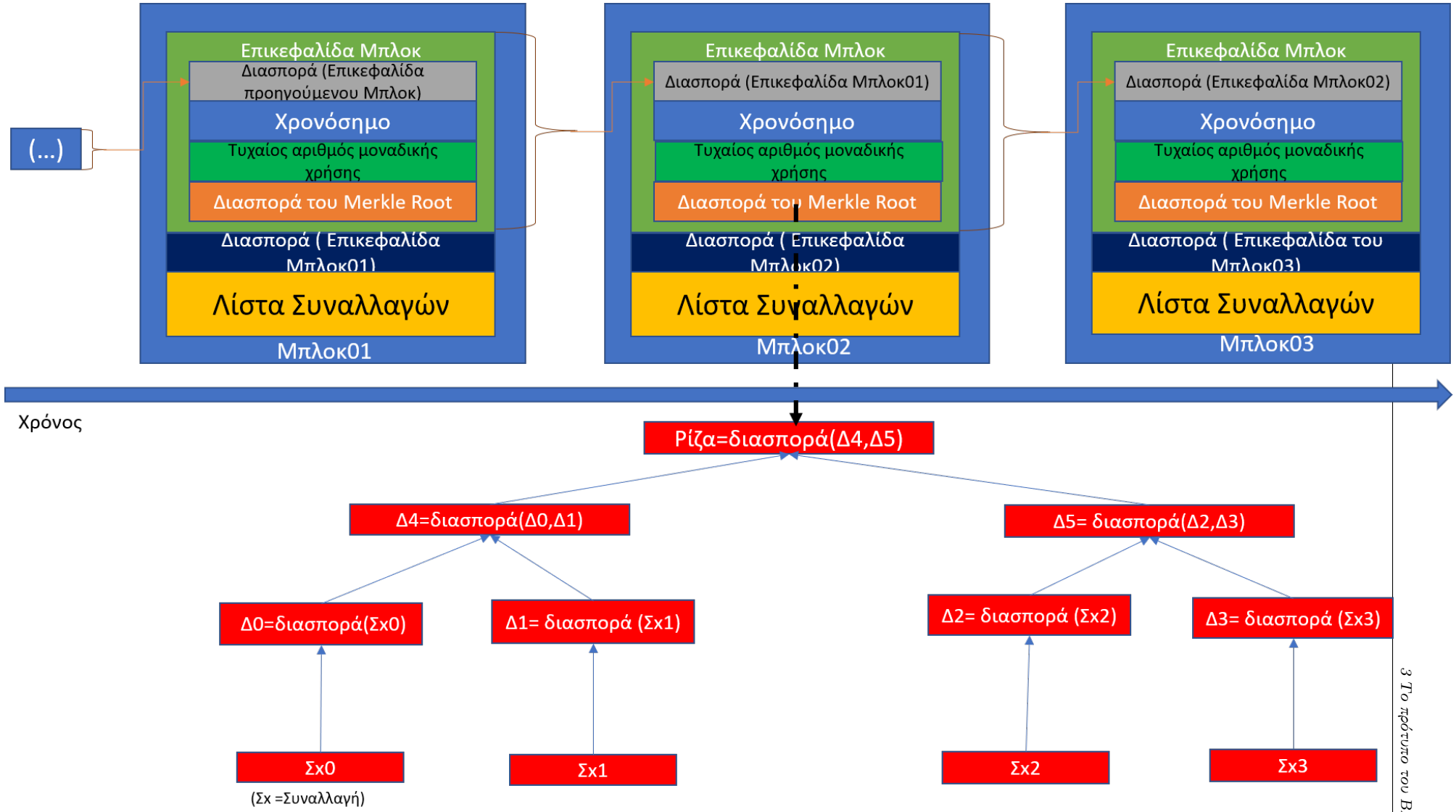
Σχήμα 3.8: Δομή ενός Merkle Tree

Στο Σχήμα 3.8 φαίνεται ότι η τελευταία σειρά των φύλλων του δέντρου περιέχουν τις συναλλαγές του μπλοκ (από Σχ0 έως Σχ3). Η ρίζα του δέντρου Merkle αποθηκεύεται στην επικεφαλίδα του μπλοκ, όπως φαίνεται στο παρακάτω σχήμα 3.9.

Η σύνοψη της επικεφαλίδας του μπλοκ είναι αποθηκευμένη τόσο στο ίδιο το μπλοκ, όσο και στο επόμενο. Αυτό επιβεβαιώνει ότι η συναλλαγή είναι αμετάβλητη, καθώς η σύνοψη της ρίζας Merkle δεν θα είναι ίδια στην περίπτωση που γίνει μια αλλαγή στις συναλλαγές.

Όταν N στοιχεία δεδομένων συνοψίζονται σε ένα δέντρο Merkle ο έλεγχος για το εάν υπάρχει ένα στοιχείο στο δέντρο γίνεται το πολύ με $2 * \log_2 N$ υπολογισμούς [34]. Η ρίζα του δέντρου, όπως και κάθε φύλλο του δέντρου, έχει μέγεθος 32 *bytes*. Για να αποδειχθεί ότι μια συγκεκριμένη συναλλαγή περιλαμβάνεται σε ένα μπλοκ, ένας κόμβος χρειάζεται μόνο να υπολογίζει $\log 2N$ των 32-*byte* διασπορές, αποτελώντας μια *διαδρομή ελέγχου ταυτότητας* ή αλλιώς μια *διαδρομή Merkle* που συνδέει τη συγκεκριμένη συναλλαγή με τη ρίζα του δέντρου [34]. Αυτό επιτρέπει στους κόμβους του Bitcoin να παράγουν αποτελεσματικά διαδρομές 10 ή 12 διασπορών με μέγεθος 320 με 384 *bytes*, οι οποίες μπορούν να παρέχουν απόδειξη μιας μόνο συναλλαγής μέσα σε χιλιάδες συναλλαγές [34].

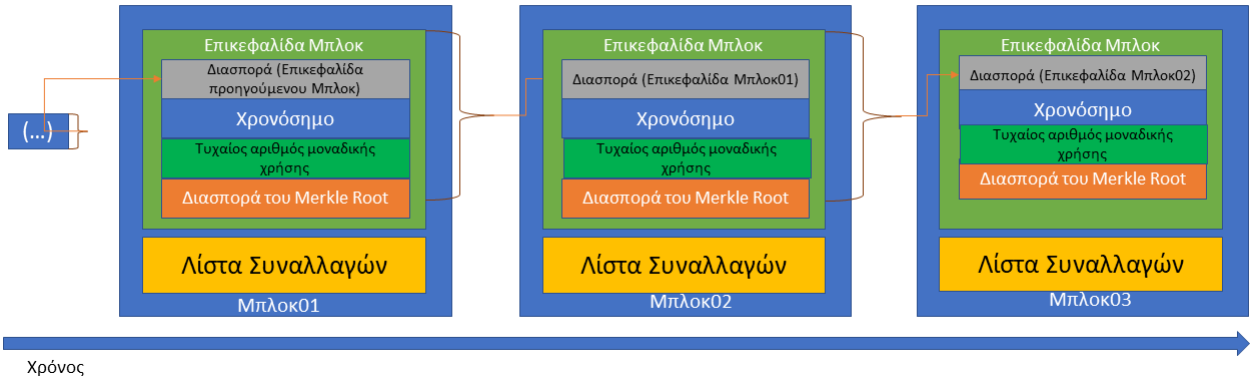
Τα Merkle Trees χρησιμοποιούνται πολύ και από τους SPV (simplified payment verification) κόμβους. Αυτοί οι κόμβοι δεν έχουν όλες τις συναλλαγές και δεν διαθέτουν όλα τα πλήρη μπλοκ, αλλά κατεβάζουν μόνο τις επικεφαλίδες των μπλοκ. Προκειμένου να επαληθευτεί ότι μια συναλλαγή περιλαμβάνεται σε ένα μπλοκ, χρησιμοποιούν μια διαδρομή Merkle [34].



Σχήμα 3.9: Το Blockchain με το Merkle Tree

3.7 Η σύνδεση των μπλοκ

Τα μπλοκ είναι αλυσιδωτά συνδεδεμένα μεταξύ τους ή αλλιώς επάλληλα μπλοκ. Κάθε μπλοκ περιέχει τη σύνοψη της κεφαλίδας του προηγούμενου μπλοκ, σχηματίζοντας έτσι το blockchain [20]. Έστω ότι παραβιάζεται ένα μπλοκ το οποίο έχει δημοσιευτεί, τότε αυτό παράγει μια νέα τιμή διασποράς (από τη στιγμή που είναι πολύ δύσκολο να γίνει μια σύγκρουση) [1]. Αυτό με τη σειρά του θα προκαλούσε τη διαφοροποίηση των τιμών διασποράς σε όλα τα επόμενα μπλοκ, δεδομένου ότι περιλαμβάνουν τη σύνοψη του προηγούμενου μπλοκ. Έτσι καθίσταται δυνατή η ανίχνευση και απόρριψη αλλαγμένων μπλοκ [1]. Η Εικόνα 3.10 απεικονίζει την αφαιρετική δομή μιας αλυσίδας από μπλοκ.



Σχήμα 3.10: Μια αλυσίδα από μπλοκ

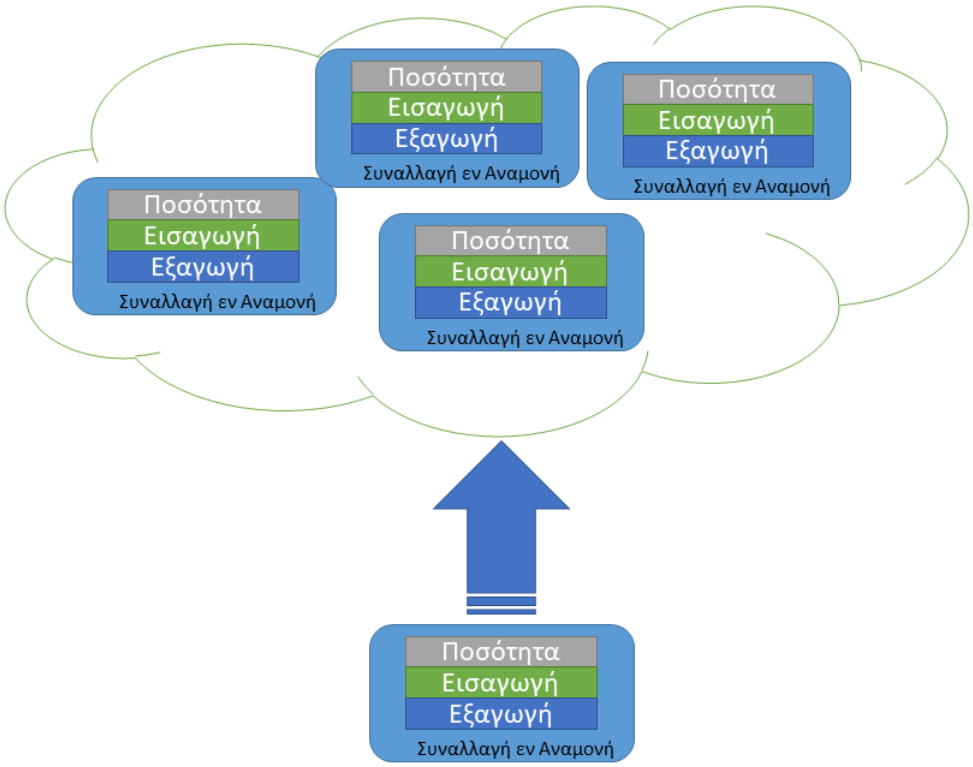
Στο Bitcoin ο υπολογισμός της σύνοψης του μπλοκ χρειάζεται μεγάλη υπολογιστική ισχύς και μεγάλο κόστος ενέργειας. Έτσι, σε περίπτωση επίθεσης στο blockchain, ο επιτιθέμενος θα πρέπει να υπολογίσει όλη την αλυσίδα μέχρι και το τελευταίο μπλοκ, ώστε να αλλάξει την αλυσίδα. Αυτό είναι πρακτικά αδύνατον πρώτον για οικονομικούς λόγους και δεύτερον είναι εκ φύσεως αδύνατον να χρησιμοποιήσει τόσο μεγάλη υπολογιστική ισχύ.

3.8 Η λειτουργία του blockchain - Bitcoin

Το blockchain διατηρείται με τη συναίνεση ενός συνόλου υπολογιστών που χρησιμοποιούν λογισμικό blockchain, οι οποίοι ονομάζονται κόμβοι εξόρυξης [20]. Δεν υπάρχει κεντρική αρχή που να καθορίζει ποιος κόμβος δημοσιεύει το επόμενο μπλοκ στο blockchain. Κάθε κόμβος διατηρεί ένα αντίγραφο του blockchain και μπορεί να προτείνει ένα νέο μπλοκ στους άλλους κόμβους εξόρυξης [20]. Μη έγκυρα μπλοκ θα ανιχνευθούν και απορριφθούν, καθώς είναι δύσκολο αφενός να υπολογιστεί ένα έγκυρο μπλοκ, αφετέρου είναι υπολογιστικά εύκολο να επαληθευτεί κάποιο [20]. Η εξόρυξη είναι, μια εκ προθέσεως, τεράστια εργασία που απαιτεί μεγάλες ποσότητες επεξεργασίας, μνήμης ή και των δύο, αναλόγως κάθε φορά με την εφαρμογή του blockchain [1].

Οποιοσδήποτε υπολογιστής τρέχει blockchain θεωρείται ως *κόμβος* του blockchain. Υπάρχουν δυο τύποι κόμβων, οι *ολόκληροι* - *full* κόμβοι, που αποθηκεύουν τα δεδομένα του blockchain, τα μεταφέρουν σε άλλους κόμβους και επικυρώνουν τους νέους κόμβους και οι *ελαφρείς* - light κόμβοι, που δεν χρειάζεται να αποθηκεύουν ολόκληρα αντίγραφα του blockchain και συχνά μεταφέρουν τα δεδομένα τους στους ολόκληρους κόμβους [20]. Η επικύρωση είναι απόρροια του γεγονότος ότι η μορφή του μπλοκ είναι σωστή, όλα τα κλειδιά διασποράς στο νέο μπλοκ έχουν υπολογιστεί σωστά, το νέο μπλοκ περιέχει το κλειδί διασποράς του προηγούμενου μπλοκ και κάθε συναλλαγή στο μπλοκ είναι έγκυρη και υπογεγραμμένη από τα κατάλληλα μέρη [20]. Οι ελαφρείς κόμβοι συνήθως βρίσκονται στα έξυπνα κινητά και στα IoT συστήματα με χαμηλή υπολογιστική ισχύ και μικρή μνήμη. Οποιοσδήποτε κόμβος μπορεί να προτείνει νέες συναλλαγές, οι οποίες διαδίδονται μεταξύ των κόμβων μέχρι να προστεθούν τελικά σε ένα μπλοκ [20].

Στο σχήμα 3.11 φαίνεται μια συναλλαγή του blockchain που έχουν αποθηκευτεί σε ένα κόμβο εξόρυξης μέσα σε μια «πισινά» συναλλαγών, περιμένοντας να εκχωρηθεί σε ένα μπλοκ.



Σχήμα 3.11: Μια συναλλαγή θα προστεθεί σε μια αχρησιμοποίητη ομάδα συναλλαγών.

Όταν οι κόμβοι εξόρυξης δημιουργούν ένα νέο υποψήφιο μπλοκ, τοποθετούν μέσα του ένα σύνολο μη δαπανημένων συναλλαγών [1]. Μετά την επικύρωση των συναλλαγών, ένας κόμβος θα τις προσθέσει στη *δεξαμενή μνήμης* ή στο *σύνολο συναλλαγών*, όπου οι συναλλαγές περιμένουν έως ότου μπορούν να συμπεριληφθούν (να εξορυχθούν) σε ένα μπλοκ. Οι κόμβοι μπορούν έτσι, να λάβουν ένα συνδυασμό παλαιότερων συναλλαγών που είναι σε

αναμονή ή νεότερες συναλλαγές που προσφέρουν υψηλότερη πληρωμή [20]. Ο κόμβος εξόρυξης ελέγχει την εγκυρότητα κάθε συναλλαγής και οι άλλοι κόμβοι θα απορρίψουν το μπλοκ σε περίπτωση που συμπεριλήφθηκαν μη έγκυρες συναλλαγές [20] στο μπλοκ. Σε αυτό το σημείο, ο κόμβος εξόρυξης συμπληρώνει όλες τις πληροφορίες που απαιτούνται από τη δομή του μπλοκ εκτός από τον τυχαίο αριθμό μοναδικής χρήσης [20].

Ορισμένα συστήματα blockchain απαιτούν δαπάνη χρόνου και προσπάθειας για να δημιουργήσουν το επόμενο μπλοκ [20]. Για τα συστήματα τα οποία απαιτούν χρόνο και προσπάθεια, ο κόμβος εξόρυξης υπολογίζει πολλούς τυχαίους αριθμούς μοναδικής χρήσης, για να λύσει ένα υπολογιστικά δύσκολο παζλ [1]. Ο κόμβος εξόρυξης που θα νικήσει αποκτά το δικαίωμα δημοσίευσης του επόμενου μπλοκ. Συνήθως, οι κόμβοι εξόρυξης δοκιμάζουν πολλούς τυχαίους αριθμούς μοναδικής χρήσης, πριν λύσουν ένα παζλ [20]. Μόλις λυθεί ένα παζλ με ένα συγκεκριμένο τυχαίο αριθμό μοναδικής χρήσης, ο κόμβος δημιουργεί μία τιμή διασποράς των δεδομένων του μπλοκ και το αποθηκεύει στο ίδιο το μπλοκ. Στη συνέχεια, το μπλοκ αποστέλλεται σε άλλους κόμβους για επαλήθευση. Αν όλα επαληθευτούν, οι κόμβοι το αποδέχονται ως το τελευταίο μπλοκ και συνεχίζουν στο επόμενο [20] [1].

3.9 Forking

Οι αλλαγές στις αποδόσεις και οι τεχνολογικές ενημερώσεις μπορεί να είναι δύσκολες στις καλύτερες στιγμές [20] [34]. Οι αλλαγές στο πρωτόκολλο και στη δομή ενός δικτύου blockchain ονομάζονται forks δηλαδή, διαχωρισμός ή διακλάδωση. Μπορούν να χωριστούν σε δύο κατηγορίες: στα soft forks και στα hard forks [20] [34]. Για ένα soft fork, αυτές οι αλλαγές είναι συμβατές με κόμβους που δεν έχουν ενημερωθεί και επιτρέπει τη διαλειτουργικότητα της αλυσίδας. Για ένα hard fork, αυτές οι αλλαγές «σπάνε» την διαλειτουργικότητα, επειδή οι κόμβοι που δεν έχουν ενημερωθεί θα απορρίψουν τα μπλοκ μετά τις αλλαγές και ουσιαστικά τη διαχωρίζει [20] [34]. Αυτό μπορεί να οδηγήσει σε διάσπαση στο δίκτυο δημιουργώντας πολλαπλές εκδόσεις του ίδιου. Τα δίκτυα αυτά, μπορούν να μετριάσουν τα προβλήματα του forking απαιτώντας ενημερώσεις λογισμικού [20] [40].

3.9.1 Soft Forks

Ένα soft fork είναι μια αλλαγή σε μια εφαρμογή blockchain που επιτρέπει τη διαλειτουργικότητα [20] [34]. Οι μη ενημερωμένοι κόμβοι μπορούν να συνεχίσουν να πραγματοποιούν συναλλαγές με ενημερωμένους κόμβους [1] [40]. Αν οι κόμβοι δεν χρησιμοποιήσουν την ενημέρωση, τότε αυτή δεν θα τηρηθεί [20] [34]. Ένα παράδειγμα ενός soft fork θα είχαμε, εάν ένα blockchain αποφάσιζε να μειώσει το μέγεθος των μπλοκ (για παράδειγμα από 1,0 MB σε 0,5 MB) [20] [34]. Οι ενημερωμένοι κόμβοι θα προσάρμοζαν το μέγεθος του μπλοκ και θα συνέχιζαν να δημοσιεύουν μπλοκ κανονικά [1] [34]. Οι μη ενημερωμένοι κόμβοι θα θεωρούσαν αυτά τα μπλοκ ως έγκυρα, δεδομένου ότι, η πραγματοποιηθείσα αλλαγή δεν

παραβιάζει τους κανόνες τους (δηλαδή, το μέγεθος του μπλοκ να είναι στο μέγιστο επιτρεπόμενο όριο). Ωστόσο, εάν ένας μη ενημερωμένος κόμβος δημιουργούσε ένα μπλοκ με μέγεθος μεγαλύτερο από 0,5 MB, οι ενημερωμένοι κόμβοι θα το απέρριπταν ως μη έγκυρο [20].

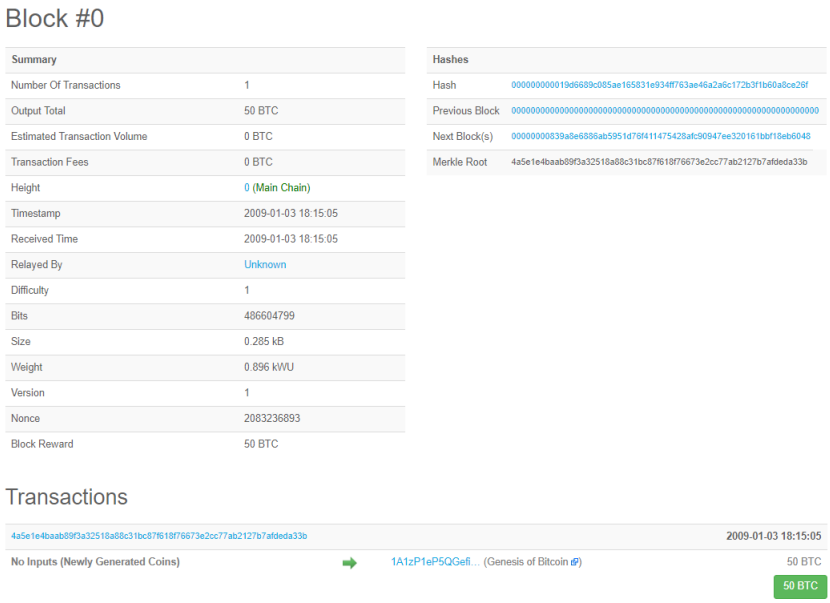
3.9.2 Hard Forks

Ένα hard fork είναι μια αλλαγή σε μια εφαρμογή blockchain που δεν είναι επιτρέπει τη διαλειτουργικότητα [20] [34]. Σε ένα συγκεκριμένο χρονικό σημείο, όλοι οι κόμβοι θα πρέπει να αλλάξουν χρησιμοποιώντας το ενημερωμένο πρωτόκολλο. Επιπλέον, όλοι οι κόμβοι θα πρέπει να αναβαθμιστούν στο νέο πρωτόκολλο, έτσι ώστε να μην απορρίπτουν τα νεοσυσταθέντα μπλοκ [20] [34]. Οι μη ενημερωμένοι κόμβοι δεν μπορούν να συνεχίσουν να πραγματοποιούν συναλλαγές στο ενημερωμένο blockchain, επειδή έχουν προγραμματιστεί να απορρίψουν οποιοδήποτε μπλοκ δεν ακολουθεί τις νέες προδιαγραφές [1] [40]. Είναι σημαντικό, επίσης, να σημειωθεί ότι, ενώ τα περισσότερα hard forks είναι σκόπιμα, τα σφάλματα λογισμικού ενδέχεται να προκαλέσουν ακούσια hard forks. Εάν εντοπιστεί κάποια ατέλεια σοβαρή στο λογισμικό του blockchain, τότε η μόνη λύση είναι να δημιουργηθεί ένα hard fork [20] [34]. Στα κρυπτονομίσματα, εάν υπάρχει ένα hard fork και το blockchain χωριστεί στα δύο, τότε οι χρήστες θα έχουν ανεξάρτητα νομίσματα και στα δύο forks [20] [34]. Συνεπώς η παλιά δεν μπορεί να ξαναχρησιμοποιηθεί, αφού οι δύο αλυσίδες δεν είναι πλέον συμβατές. Στην περίπτωση του Ethereum που δέχτηκε hard fork, η πλειοψηφία των χρηστών μεταφέρθηκε στο νέο fork, ενώ το παλιό fork μετονομάστηκε σε Ethereum Classic και συνέχισε να λειτουργεί ανεξάρτητα [1] [40].

Κεφάλαιο 4

Μοντέλα Συναίνεσης

Ένα βασικό στοιχείο στην ομαλή λειτουργία του blockchain είναι το μοντέλο συναίνεσης (consensus model) που χρησιμοποιεί. Το μοντέλο συναίνεσης είναι αυτό που αποφασίζει ποιος και πότε ένας χρήστης θα εκδώσει ένα μπλοκ και όλοι οι χρήστες συναινούν σε αυτούς τους κανόνες. Όταν ένας χρήστης συνδέεται για πρώτη φορά σε ένα δίκτυο blockchain, τότε αυτός αυτόματα συμφωνεί με τους κανόνες του συγκεκριμένου δικτύου και προσαρτά καινούργια μπλοκ μετά από το genesis μπλοκ. Το genesis μπλοκ είναι το πρώτο μπλοκ που δημιουργήθηκε στο δίκτυο και υπακούει στους κανόνες του εκάστοτε μοντέλου συναίνεσης.



Σχήμα 4.1: Το πρώτο μπλοκ

Κάθε μοντέλο συναίνεσης έχει τις εξής ιδιότητες [40]:

- Η αρχική κατάτσταση του συστήματος με τους κανόνες του αποφασίζεται στο genesis μπλοκ.
- Οι χρήστες συμφωνούν με τους κανόνες του μοντέλου συναίνεσης από τη στιγμή που προσαρτούν νέο μπλοκ.

- Κάθε μπλοκ είναι συνδεδεμένο με τη σύνοψη της επικεφαλίδας του προηγούμενου μπλοκ (εκτός από το genesis μπλοκ που δεν έχει προηγούμενο)
- Οι χρήστες μπορούν να επαληθεύσουν κάθε μπλοκ ξεχωριστά.

4.1 Μοντέλο συναίνεσης Proof of work

Στο μοντέλο της Απόδειξης Εργασίας Proof-of-Work - PoW, οι χρήστες που δημοσιεύουν το επόμενο μπλοκ είναι αυτοί που θα λύσουν πρώτοι ένα υπολογιστικά δύσκολο παζλ [18]. Η λύση αυτού του παζλ είναι και η απόδειξη της εργασίας τους [22]. Η επίλυση του παζλ είναι υπολογιστικά αρκετά δύσκολη, όμως, η επαλήθευση της λύσης του είναι εύκολη [40]. Αυτό επιτρέπει σε όλους τους υπόλοιπους πλήρεις κόμβους να επαληθεύσουν οποιοδήποτε επόμενο προτεινόμενο μπλοκ, ενώ οποιοδήποτε μπλοκ δεν επαληθεύεται, θα απορρίπτεται. Το συνηθέστερο πρόβλημα που ζητείται για το παζλ είναι η εύρεση μικρότερης τιμής διασποράς από μια συγκεκριμένη τιμή [40]. Έπειτα οι κόμβοι εξόρυξης κάνουν μικρότερες αλλαγές στο ίδιο το μπλοκ (συγκεκριμένα στην τιμή τυχαίας μοναδικής τιμής) προσπαθώντας να βρουν μια διασπορά ενός μπλοκ που να πληροί τα προαπαιτούμενα [34]. Για κάθε απόπειρα, ο κόμβος εξόρυξης πρέπει να υπολογίζει τη σύνοψη για ολόκληρη την κεφαλίδα του μπλοκ, η οποία είναι μια υπολογιστικά χρονοβόρα διαδικασία [1]. Η απαιτούμενη τιμή της διασποράς μπορεί να τροποποιηθεί με την πάροδο του χρόνου, για να προσαρμόσει τη δυσκολία και να επηρεάσει τη συχνότητα δημοσίευσης των μπλοκ. Επίσης, αξιοσημείωτο είναι ότι η λύση ενός παζλ δεν επηρεάζει την πιθανότητα να λύσει άλλα παζλ στο παρόν ή στο μέλλον, καθώς αυτά είναι ανεξάρτητα μεταξύ τους [22]. Το παζλ πρέπει να πληροί κάποιες προϋποθέσεις για να λυθεί και να είναι έγκυρο. Αρχικά όλα τα παζλ χρησιμοποιούν τον SHA-256 αλγόριθμο και ο υπολογιστής πρέπει να βρει την τιμή διασποράς που ζητείται κάθε φορά και πληροί τις προϋποθέσεις [20, 22, 34]. Για παράδειγμα, έστω:

SHA256 (“blockchain” + nonce) = Σύνοψη που να ξεκινάει με τη συμβολοσειρά ‘000000’.

Το αλφαριθμητικό “blockchain” συνδέεται με την τυχαία τιμή μοναδικής χρήσης και τότε όλο αυτό παράγει μια σύνοψη. Αυτή η διαδικασία θα επαναληφθεί 10.730.896 φορές, έως ότου βρει μια τιμή διασποράς που να ξεκινάει με έξι μηδενικά (σε έναν υπολογιστή παλαιού τύπου χρειάζεται περίπου 54 δευτερόλεπτα) [34]. Με την αύξηση των συνεχόμενων μηδενικών “0000000” αυξάνεται και η δυσκολία εύρεσης της συγκεκριμένης τιμής (στον ίδιο υπολογιστή χρειάστηκε 1 ώρα, 18 λεπτά και 12 δευτερόλεπτα) [1]. Όταν ένας κόμβος «ωριμάσει» και είναι έτοιμος να δημοσιευτεί, τότε στέλνει το μπλοκ του, με την επικυρωμένη τυχαία τιμή μοναδικής χρήσης, σε ένα πλήρη κόμβο στο δίκτυο του blockchain [34]. Ο παραλήπτης του πλήρη κόμβου επιβεβαιώνει ότι το νέο μπλοκ πληροί τις προϋποθέσεις του παζλ, το προσθέτει αυτό το μπλοκ στο αντίγραφο του blockchain και το διαμοιράζει στους υπόλοιπους ομότιμους κόμβους [18]. Με αυτόν τον τρόπο το μπλοκ μεταφέρεται γρήγορα και κατανεμημένα στο

δίκτυο και η επαλήθευση της τυχαίας τιμής μοναδικής χρήσης καθίσταται εύκολη, καθώς χρειάζεται μόνο μία τιμή διασποράς, που όταν ελεγχθεί θα λύνει το παζλ [34].

Για παράδειγμα, έστω ότι ο Μπομπ αγόρασε ένα προϊόν και πλήρωσε με bitcoin. Τότε, την συναλλαγή αυτήν την δέχεται ένας κόμβος εξόρυξης ο οποίος την βρήκε μέσα από την δεξαμενή των συναλλαγών. Ο κόμβος εξόρυξης θα συνεχίσει να δέχεται συναλλαγές μέχρι να συγκεντρώσει ένα πλήθος συναλλαγών. Στην διάρκεια που συλλέγει συναλλαγές, δέχεται και την δημοσίευση νέων μπλοκ από τους άλλους κόμβους. Έτσι, αν προσπαθούσε να εξορύξει το 50ο μπλοκ στο blockchain και κάποιος άλλος τον πρόλαβε και το πιο γρήγορα από αυτόν, γιατί έλυσε πιο γρήγορα το το παζλ, τότε το μπλοκ του θα διαγωνιστεί με τους υπόλοιπους κόμβους για να πάρει την θέση του 51ου μπλοκ. Οπότε, δέχεται το 50ο μπλοκ, το επαληθεύει και θα αφαιρέσει οποιαδήποτε συναλλαγή ήταν στην δεξαμενή συναλλαγών (ακόμα και αυτές που είχε προσθέσει στο μπλοκ του). Οπότε, προσθέτει νέες συναλλαγές στο μπλοκ από την ενημερωμένη δεξαμενή μαζί με την συναλλαγή του Μπομπ και σε 10 λεπτά, ο κόμβος εξόρυξης υπολογίζει πολλούς τυχαίους αριθμούς μοναδικής χρήσης, για να λύσει ένα υπολογιστικά δύσκολο παζλ. Στην συνέχεια βρίσκει την τυχαία τιμή μοναδικής χρήσης για το συγκεκριμένο μπλοκ και αμέσως το δημοσιεύει στους άλλους κόμβους. Αυτοί το δέχονται το επαληθεύουν αφαιρούν από την δεξαμενή την συναλλαγή του Μπομπ και έτσι συνεχίζει η αλυσίδα. Αμέσως μετά, ο κόμβος εξόρυξης δημιουργεί ένα κενό μπλοκ (candidate block) δηλαδή, μπλοκ χωρίς έγκυρο PoW για την 52η θέση του blockchain και ξανά κάνει την ίδια λειτουργία από την αρχή [34].

Σε πολλά δίκτυα blockchain τύπου PoW οι κόμβοι που δημοσιεύονται έχουν την τάση να οργανώνονται σε ομάδες που ονομάζονται «πισίνες-pools» ή «κολεκτίβες», οι οποίες επιλύουν συλλογικά τα παζλ. Αυτό συμβαίνει επειδή είναι δυνατή η διάσπαση του έργου μεταξύ δύο ή περισσοτέρων κόμβων σε μια κολεκτίβα για να μοιραστούν την εργασία αλλά και τις ανταμοιβές. Ένα παράδειγμα, κατά το οποίο χωρίζεται η εργασία σε τέσσερις διαφορετικούς κόμβους και ο καθένας παίρνει ένα ίσο ποσό από το εύρος τυχαίων τιμών μοναδικής χρήσης για έλεγχο [20]:

- Node 1: check nonce 0000000000 to 0536870911
- Node 2: check nonce 0536870912 to 1073741823
- Node 3: check nonce 1073741824 to 1610612735
- Node 4: check nonce 1610612736 to 2147483647

Το παράδειγμα με τα εφτά μηδενικά χρειάστηκε μόλις 10 λεπτά και 14 δεύτερα για να λυθεί, καθώς η εργασία χωρίστηκε τώρα σε τέσσερις υπολογιστές που παράλληλα υπολόγιζαν τιμές διασποράς [40].

4.2 Μοντέλο συναίνεσης Proof of Stake - PoS

Το μοντέλο της Απόδειξης Συμμετοχής (Proof of Stake) βασίζεται στην ιδέα ότι, όσο περισσότερο συμμετέχει (δηλαδή έχει μετοχές-stake του δικτύου) κάποιος τόσο περισσότερο αυτός ο χρήστης θα θέλει να πετύχει το σύστημα και όχι να το υπονομεύσει. Η συμμετοχή είναι η ποσότητα κρυπτονομισμάτων που έχει επενδύσει σε ένα δίκτυο blockchain [18]. Η συμμετοχή έχει την έννοια του στοιχήματος-μετοχής, δηλαδή, όταν ένας χρήστης στοιχηματίσει τα νομίσματά του τότε δεν μπορεί να τα επαναχρησιμοποιήσει για ένα χρονικό διάστημα [20]. Σε αυτό το μοντέλο η πιθανότητα ενός χρήστη να δημοσιεύσει ένα νέο μπλοκ είναι ανάλογη με τη συμμετοχή του σε αυτό το δίκτυο [20]. Αυτό το μοντέλο συναίνεσης δεν καταναλώνει ανάλογους πόρους με το PoW (χρόνο, ηλεκτρική ενέργεια, επεξεργαστική ισχύ), καθώς όλα τα κρυπτονομίσματα έχουν κατανεμηθεί στους χρήστες [20]. Έτσι μερικά δίκτυα αποφάσισαν να μην ανταμείβουν τη δημιουργία ενός νέου μπλοκ [1]. Υπάρχουν διάφοροι μέθοδοι σύμφωνα με τις οποίες ένα δίκτυο διαχειρίζεται τις συμμετοχές [20]. Οι πιο γνωστές, ωστόσο είναι οι εξής τέσσερις [20]:

1. Η τυχαία επιλογή του χρήστη δημοσίευσης. Αυτό το δίκτυο επιλέγει τυχαία ένα χρήστη για να δημοσιεύσει το επόμενο μπλοκ (chain-based PoS). Το δίκτυο επιλέγει τον χρήστη με βάση το ποσοστό της συμμετοχής του, δηλαδή, αν ένας χρήστης έχει 30% συμμετοχή τότε έχει 30% πιθανότητες να επιλεγεί για την δημοσίευση του επόμενου μπλοκ.

2. Η πολυφασική ψηφοφορία. Η επιλογή του επόμενου μπλοκ γίνεται με ψηφοφορία, η οποία περιλαμβάνει πολλές φάσεις (Byzantine fault tolerance PoS). Το δίκτυο θα επιλέξει αρκετούς συμμετέχοντες χρήστες για τη δημιουργία του επόμενου μπλοκ. Όλοι οι συμμετέχοντες χρήστες ψηφίζουν για το προτεινόμενο μπλοκ. Πολλές ψηφοφορίες μπορεί να προκύψουν πριν από την απόφαση. Αυτή μέθοδος επιτρέπει σε όλους τους χρήστες να συμμετέχουν στην δημοσίευση του επόμενου μπλοκ.

3. Coin aging συστήματα. Η επιλογή του χρήστη γίνεται με βάση τον χρόνο. Μετά από ένα συγκεκριμένο χρονικό διάστημα που η συμμετοχή έχει "στοιχηματιστεί", δίνει ένα πλεονέκτημα στον χρήστη της για να δημοσιεύσει το επόμενο μπλοκ. Στη συνέχεια, η συμμετοχή μηδενίζει τον χρόνο που έχει "στοιχηματιστεί" και ο χρήστης δεν μπορεί να τη χρησιμοποιήσει παρά μόνο μετά την παρέλευση ενός συγκεκριμένου χρονικού διαστήματος. Αυτή η μέθοδος επιτρέπει στους χρήστες με περισσότερες συμμετοχές να δημοσιεύουν περισσότερα μπλοκ, χωρίς όμως να κυριαρχούν στο δίκτυο, καθώς υπάρχει και ένα μέγιστο όριο στην πιθανότητα επιτυχίας.

Ένα πρόβλημα που ίσως προκύψει με το συγκεκριμένο μοντέλο συναίνεσης είναι γνωστό και ως "nothing at stake" δηλαδή, αν ένας χρήστης συμμετέχει σε πολλαπλά ανταγωνιστικά δίκτυα [1]. Αυτό αυτόματα αυξάνει τις πιθανότητες του χρήστη να κερδίσει τις ανταμοιβές

του κάθε δικτύου και να μην αφιερώσει τον απαραίτητο χρόνο στο κάθε παρακλάδι του δικτύου. Σε αυτή τη μέθοδο οι πλούσιοι χρήστες με τις περισσότερες συμμετοχές κερδίζουν περισσότερα, όμως, η απόκτηση της πλειονότητας των ψηφιακών αγαθών είναι πολύ δαπανηρή έως και αδύνατη [20].

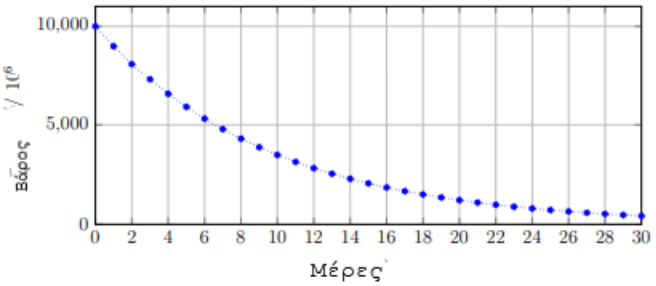
4.3 Περισσότερα μοντέλα συναίνεσης

Τα δυο βασικά και πιο γνωστά και λειτουργικά μοντέλα συναίνεσης αναφέρθηκαν παραπάνω. Υπάρχουν, ωστόσο, αρκετά ακόμα τέτοια μοντέλα που είτε δεν έχουν χρησιμοποιηθεί ακόμα είτε λειτουργούν κάτω από προϋποθέσεις. Ενδεικτικά αναφέρουμε τα εξής:

- **Proof of Burn - PoB**. Με την Απόδειξη Καύσης ή Καταστροφής οι κόμβοι εξόρυξης δεν πληρώνουν για ηλεκτρικό ρεύμα ή υλικό υπολογιστή καθώς 'καίνε' τα νομίσματά τους, ώστε να πάρουν το προνόμιο να προτείνουν το επόμενο μπλοκ. Αρχικά, προτάθηκε από τον Iain Stewart το 2012 [3], η απόδειξη καύσης αποτελεί μηχανισμό για την καταστροφή του κρυπτονομίσματος αμετάκλητα και αποδεδειγμένα [44] [3]. Η ικανότητα δημιουργίας πειστικών αποδείξεων άλλαξε την πρακτική αυτή από μια περιθωριακή πράξη σε μια λογική και δυνητικά χρήσιμη προσπάθεια [44]. Έχει πιστοποιηθεί από τότε ότι τα μεταδεδομένα της επιλογής του χρήστη μπορούν να αποδίδονται με μοναδικό τρόπο σε μια πράξη καύσης, επιτρέποντας σε κάθε "καύση" να προσαρμόζεται σε ένα συγκεκριμένο σκοπό [44] [3]. Καύση νομισμάτων σημαίνει ότι τα στέλνουν σε μια διεύθυνση και εκεί χάνονται οριστικά. Όσο περισσότερα νομίσματα καταστρέφει ο κόμβος, τόσο μεγαλύτερες είναι οι πιθανότητες να επιλεχθεί για την εξόρυξη του επόμενου μπλοκ [44].

- **Proof of Importance - PoI**. Στην περίπτωση αυτή δεν λαμβάνεται μόνο υπόψη η ποσότητα των νομισμάτων που διαθέτει ένας κόμβος εξόρυξης, αλλά και η εκτίμηση της σπουδαιότητας της δραστηριότητας και του αριθμού των συναλλαγών. Αυτή η παραλλαγή των παραπάνω μηχανισμών προσφέρει μια ευρύτερη δυνατότητα για τη ¨σπουδαιότητα' των κόμβων, ώστε να επιλέξει τον κόμβο που μπορεί να προτείνει το επόμενο μπλοκ. Πιο αναλυτικά, η Απόδειξη Σπουδαιότητας είναι ο αλγόριθμος συναίνεσης της τεχνολογίας blockchain που χρησιμοποιείται από την εταιρία NEM [5]. Σε αυτό το μοντέλο ο κάθε λογαριασμός έχει μια βαθμολογία σπουδαιότητας που αντιπροσωπεύει τη συνολική σημασία που έχει για την οικονομία της εταιρίας NEM [5]. Λογαριασμοί με υψηλότερη βαθμολογικά σπουδαιότητα έχουν μεγαλύτερες πιθανότητες για να συλλογής (harvest) ενός μπλοκ, δηλαδή δημοσίευσης ενός νέου μπλοκ [5]. Με δεδομένο ότι όλες οι συναλλαγές της Nem είναι δημόσιες, το γράφημα συναλλαγής της οικονομίας της μπορεί να υπολογιστεί με ακρίβεια [5]. Άρα, η βασική καινοτομία της Απόδειξης Σπουδαιότητας είναι ότι το γράφημα των συναλλαγών μπορεί να χρησιμοποιηθεί για την καταγραφή και την αποσαφήνιση των εισροών για έναν οποιοδήποτε

λογαριασμό [5]. Επειδή σε αυτό το δίκτυο υπάρχει μεγάλη διαφάνεια, οι πληροφορίες αυτές με τις μεταφορές μεταξύ των λογαριασμών μπορούν να χρησιμοποιηθούν για τη αξιολόγηση της σπουδαιότητας των λογαριασμών [5]. Τέλος, ο πίνακας outlink 4.2 που ορίζει το γράφημα των συναλλαγών είναι σημαντικός και χρησιμοποιείται στον υπολογισμό της σπουδαιότητας του χρήστη [5]. Ο πίνακας outlink 4.2 ουσιαστικά περιγράφει τη σταθμισμένη καθαρή ροή ενός λογαριασμού τις τελευταίες 30 ημέρες, άρα μόνον οι αμιγείς μεταφορές συμβάλλουν στη σπουδαιότητα του λογαριασμού αυτού [5].



Σχήμα 4.2: Ο πίνακας outlink που υπολογίζει την σημαντικότητα των χρηστών στο PoI [5]

- **Round Robin**. Αυτό το μοντέλο συναίνεσης χρησιμοποιείται συχνά για ιδιωτικά blockchain και ονομάζεται Round Robin, όπου οι κόμβοι παίρνουν σειρά για τη δημιουργία μπλοκ [1]. Αν ένας κόμβος εξόρυξης δεν είναι διαθέσιμος όταν έρθει η σειρά του, τότε ένας τυχαίος διαθέσιμος κόμβος μπορεί να δημοσιεύει το μπλοκ [20]. Αυτό το μοντέλο εξασφαλίζει ότι κανένας κόμβος δεν δημιουργεί την πλειονότητα των μπλοκ, δεν διαθέτει κρυπτογραφικά παζλ και έχει χαμηλές απαιτήσεις ενέργειας [20].

- **Proof of Elapsed Time (PoET)**. Η Intel παρουσίασε ένα εναλλακτικό πρωτόκολλο συναίνεσης, που ονομάζεται ¨απόδειξη του χρόνου που καταναλώθηκε¨. Κάθε κόμβος δημοσίευσης ζητά ένα χρόνο αναμονής από ένα ασφαλές υλικό χρόνου που βρίσκεται στο σύστημα του υπολογιστή [1]. Η προέλευση του χρόνου από ασφαλές υλικό θα δημιουργήσει μια τυχαία τιμή χρόνου αναμονής και θα την επιστρέψει στο λογισμικό κόμβου δημοσίευσης [20]. Δεν απαιτείτε η λύση κάποιου παζλ, χρησιμοποιείται ένα έμπιστο περιβάλλον εκτέλεσης (TEE) για να εξασφαλιστεί ότι τα μπλοκ δημιουργούνται με τυχαίο τρόπο. Βασίζεται σε εγγυημένο χρόνο αναμονής που παρέχεται από το TEE [45]. Το μειονέκτημα σε αυτό το μοντέλο είναι η ανάγκη του για εξειδικευμένο υλικό και η εμπιστοσύνη από έναν τρίτο [45].

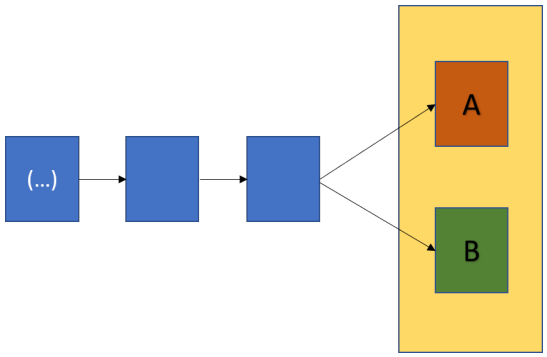
- **Proof of Authority**. Η Απόδειξη Αρχής (αναφέρεται επίσης και ως Proof of Identity) βασίζεται στη χρήση επιβεβαιωμένων συναλλαγών και κόμβων μέσω επικυρωμένων λογαριασμών, γνωστών και ως validators [1, 12]. Οι κόμβοι δημοσίευσης, δηλαδή, πρέπει να έχουν αποδεδειγμένη και επαληθευμένη την ταυτότητά τους εντός

του δικτύου, δηλαδή, οι υπόλοιποι κόμβοι του έδωσαν το δικαίωμα (τον εξουσιοδότησαν) να δημοσιεύει νέα μπλοκ. Η ιδέα είναι ότι ο κόμβος δημοσίευσης χρησιμοποιεί την επιβεβαιωμένη και αυθεντική ταυτότητά του για να δημοσιεύσει νέα μπλοκ. Οι χρήστες του δικτύου επηρεάζουν άμεσα τη φήμη ενός κόμβου δημοσίευσης βάσει της συμπεριφοράς του [12]. Κατά συνέπεια, είναι προς το συμφέρον ενός κόμβου δημοσίευσης να διατηρεί υψηλή φήμη [1]. Αυτός ο αλγόριθμος ισχύει μόνο για δίκτυα blockchain με υψηλό επίπεδο εμπιστοσύνης ανάμεσα στους κόμβους.

- **Proof of Cooperation**. Στις 18 Ιουλίου 2017 ο νέος αλγόριθμος «Απόδειξη Συνεργασίας - Proof of Cooperation» εισήχθη στην FairCoin και κατά επέκταση ένα blockchain εξοικονόμησης ενέργειας που χρησιμοποιεί τη συνεργασία αντί του ανταγωνισμού [4]. Οι κανόνες συναίνεσης καθορίζουν ποιοι συνεργατικά επικυρωμένοι κόμβοι (Collaboratively Validated Nodes) πρέπει να δημιουργήσουν το επόμενο μπλοκ [4]. Κάθε CVN εγκρίνει το CVN υπογράφοντας ψηφιακά ένα τμήμα δεδομένων, το οποίο περιέχει το μοναδικό αναγνωριστικό του [4]. Αφού το αντίστοιχο CVN λάβει όλες τις απαραίτητες υπογραφές, παίρνει εκκρεμείς συναλλαγές και σχηματίζει ένα νέο μπλοκ, το οποίο στη συνέχεια αποθηκεύεται στην αμετάβλητη και κατανεμημένη βάση δεδομένων blockchain [4]. Η δημιουργία μπλοκ είναι σχεδόν ανέξοδη, για αυτό και τα CVNs μπορούν να λειτουργήσουν σε ένα Raspberry pi 3 που καταναλώνει πολύ λίγα watt και δεν χάνει ενέργεια ή υπολογιστικούς πόρους. Ακόμα κι αν το δίκτυο των CVNs μεγαλώσει, η κατανάλωση ισχύος θα παραμείνει πολύ χαμηλή [4].

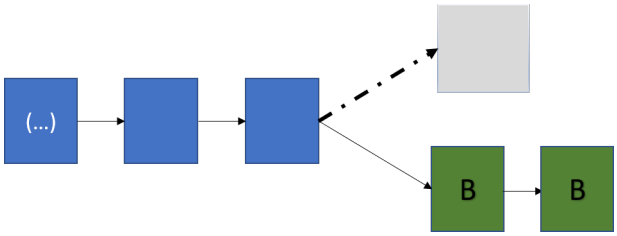
4.4 Συγκρούσεις και Λύσεις Κατάστιχων

Ένα πρόβλημα που προκύπτει από τη χρήση των μοντέλων συναίνεσης είναι αυτό της συμφόρησης [20]. Σε πολλά δίκτυα είναι πιθανό πολλοί χρήστες να δημοσιεύουν νέα μπλοκ ταυτόχρονα. Αυτό προκαλεί την ύπαρξη πολλών διαφορετικών εκδοχών του blockchain τη δεδομένη χρονική στιγμή. Σε ορισμένα συστήματα εντός των κατανεμημένων δικτύων, έχουν την τάση να είναι πίσω από πληροφορίες ή να έχουν εναλλακτικές πληροφορίες. Αυτό εξαρτάται από την καθυστέρηση του δικτύου μεταξύ των κόμβων και την εγγύτητα των ομάδων κόμβων [1]. Ένα σημαντικό έργο επιτελείται από τα μοντέλα συναίνεσης είναι η επίλυση συγκρούσεων των δεδομένων. Για παράδειγμα έστω ο κόμβος X δημιουργεί ένα μπλοκ(X) με συναλλαγές ‘1,‘2,‘3 και στη συνέχεια τις δημοσιεύει σε άλλους κόμβους. Ύστερα ο κόμβος Y δημιουργεί το μπλοκ(Y) με συναλλαγές ‘1,‘2,‘4, και τις δημοσιεύει σε άλλους κόμβους. Έτσι προκύπτει σύγκρουση μεταξύ του κόμβου X και Y, καθώς ο πρώτος περιλαμβάνει τη συναλλαγή ‘3 και όχι ‘4 και το αντίστροφο συμβαίνει με τον Y [20]. Αυτή η σύγκρουση δημιουργεί προσωρινά δυο διαφορετικές εκδοχές του blockchain, όπως εμφαίνεται στην παρακάτω Εικόνα 4.3. Αυτές οι εκδοχές δεν είναι απαραίτητα “λανθασμένες” αλλά δημιουργήθηκαν με τις πληροφορίες που διέθετε ο κάθε κόμβος. Εάν οι συναλλαγές διέθεταν



Σχήμα 4.3: Σύγκρουση Συναλλαγών

μεταφορά κρυπτονομισμάτων, τότε σε αυτή την περίπτωση, μπορεί και οι δυο συναλλαγές και να μην σταλθούν αλλά και οι δύο να σταλθούν [1]. Αυτές οι συγκρούσεις συνήθως αντιμετωπίζονται πολύ γρήγορα. Τα περισσότερα δίκτυα blockchain θα περιμένουν μέχρι να δημοσιευθεί το επόμενο μπλοκ και θα χρησιμοποιήσουν την αλυσίδα αυτή ως "επίσημη", καθώς έλαβε το επόμενο έγκυρο μπλοκ και είναι η πιο ¨μακρυά' αλυσίδα. Κάθε συναλλαγή που υπήρχε στο μπλοκ(X), αλλά δεν υπάρχει στην αλυσίδα μπλοκ(Y), επιστρέφεται στην "πισίνα" - δεξαμενή συναλλαγών που πρόκειται να δημοσιευτούν [1]. Το σύνολο των υπό δημοσίευση συναλλαγών διατηρείται τοπικά σε κάθε κόμβο, καθώς δεν υπάρχει κεντρικός διακομιστής στην αρχιτεκτονική [20]. Επομένως, η σύγκρουση λύθηκε με την μέθοδο της αλυσίδας που χρειάστηκε περισσότερη ενέργεια για να παραχθεί. Αυτή η μέθοδος υπάρχει κυρίως στο μοντέλο συναίνεσης *Απόδειξη Εργασίας*, ενώ τα άλλα μοντέλα συναίνεσης διαθέτουν διαφορετικές λειτουργίες για την επίλυση των συγκρούσεων. Λόγω της πιθανότητας



Σχήμα 4.4: Επίλυση Σύγκρουσης

αντικατάστασης ενός μπλοκ, μια συναλλαγή δεν γίνεται αποδεκτή ως επιβεβαιωμένη μέχρι να δημιουργηθούν αρκετά επιπλέον μπλοκ πάνω από το μπλοκ που περιέχει τη συναλλαγή από την οποία δημιουργήθηκε η σύγκρουση [20]. Επίσης, ορισμένα blockchain κλειδώνουν συγκεκριμένα παλαιότερα μπλοκ στο λογισμικό του blockchain δημιουργώντας έτσι σημεία ελέγχου(check points), για να διασφαλιστεί ότι αυτό δεν μπορεί ποτέ να συμβεί [20].

4.5 Πίνακας Σύγκρισης Αλγορίθμων Συναίνεσης

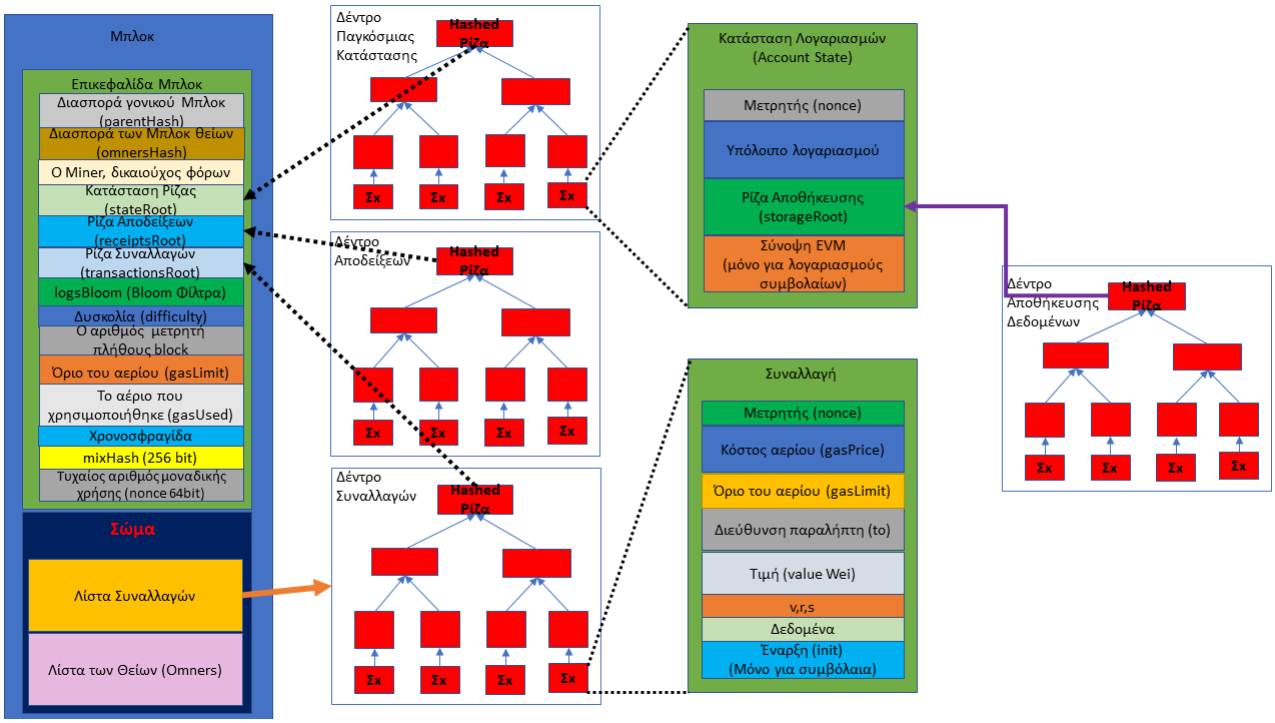
Αλγόριθμος	Αντοχή σε Επιθέσεις	Εξοικονόμηση Ενέργειας	Πλεονεκτήματα Μειονεκτήματα/Υλοποίηση	Στόχοι	Υλοποιήσεις
PoW	25% Υπολογιστικής Ισχύς	Όχι	+Δύσκολο να πραγματοποιηθεί DoS από επιτηδείους. -Υπολογιστικά ακριβό. -Επίθεση 51% της υπολογιστικής ισχύος. ◇ Γλώσσες: Golang, C++, Solidity, Vyper, LLL	Να επιτρέψει τις συναλλαγές μεταξύ μη έμπιστων συμμετεχόντων, μέσω της επίλυσης ενός πολύ δύσκολου παζλ για την δημοσίευση νέων μπλοκ	Bitcoin, Litecoin, ZCash, Ethereum
PoS	50% του μεριδίου -(Stake)	Ναι	+Ανοιχτό σε όσους θέλουν να συμμετέχουν στο σύστημα. -Αυτοί που κατέχουν τα μερίδια ελέγχουν το σύστημα. -Επίθεση 51% με την απόκτηση της οικονομικής ισχύος. -Sybil Attack [46] ◇ Γλώσσες: Michaleson	Να επιτρέψει τις συναλλαγές μεταξύ μη έμπιστων συμμετεχόντων, μέσω ενός πολύ λιγότερο υπολογιστικού φραγμού για την δημοσίευση νέων μπλοκ	Peercoin, Tezos, Tendermint
PoI	Άγνωστο	Ναι	+Γρήγορο και εξοικονομεί ενέργεια. +Δεν λαμβάνεται υπόψιν μόνο το μερίδιο του χρήστη αλλά και το πόσο ενεργός είναι στο σύστημα. -Είναι το ίδιο ευάλωτο με το PoS ◇ Γλώσσες: Java	Να επιτρέψει τις συναλλαγές μεταξύ μη έμπιστων συμμετεχόντων, όπου οι χρήστες δημοσιεύουν νέα μπλοκ ανάλογα της σημαντικότητα τους.	XEM
Round Robin	Μη Έμπιστο	Ναι	+Εύκολο στην εκμάθηση +Πολύ μικρή υπολογιστική ισχύς. -Απαιτεί υψηλού βαθμού εμπιστοσύνη μεταξύ των χρηστών. ◇ Γλώσσες: C++	Δημοσίευση μπλοκ σε αξιόπιστους κόμβους.	Multichain
PoET	Άγνωστο	Ναι	+Χαμηλή κατανάλωση ενέργειας. -Χρήση ειδικού υλικού για την καταγραφή του χρόνου το οποίο να μην έχει παραβιαστεί. -Ο συγχρονισμός του χρόνου είναι ουσιαστικά αδύνατος στα κατανεμημένα συστήματα [47]. ◇ Γλώσσες: Python	Να δημιουργήσει ένα πιο οικονομικό μοντέλο συναίνεσης, μειώνοντας το οικονομικό κόστος που σχετίζεται με την μεγάλη ασφάλεια που προσφέρει το PoW.	Hyperledger Sawtooth Lake
PoB	25% Υπολογιστικής Ισχύς	Όχι	+ Πιο οικολογικό από το PoW - πρέπει να δημιουργηθούν Bitcoins για να τα "κάψει", άρα απαιτείται μεγαλύτερη ενέργεια από το PoS ◇ Γλώσσες: Golang, C++, Solidity, Serpent, LLL	Να επιτρέψει την συναλλαγή μεταξύ μη έμπιστων χρηστών, μέσω της καταστροφής νομισμάτων το οποίο απαιτεί υπολογιστική ισχύ.	Slimcoin.
PoC	Άγνωστο	Ναι	+ Χαμηλός φόρος συναλλαγής (transaction fee και γρήγορες συναλλαγές. +Χαμηλή κατανάλωση ισχύος. -Κληρονομεί τα μειονεκτήματα του μοντέλου Round Robin, καθώς βασίζεται σε αυτό. ◇ Γλώσσες: C++.	Δημιουργία ενός φιλικού προς το περιβάλλον αλγορίθμου συναίνεσης (300watt/y). Λειτουργεί μέσω τις συνεργασίας των κόμβων	FairCoin .
PoA	50% του online Stake	Μερικώς	+Γρήγορη επιβεβαίωση +Επιτρέπει την εντατική παραγωγή μπλοκ +Μπορεί να χρησιμοποιηθεί σε sidechains -Βασίζεται στην παραδοχή ότι ο τρέχων εξουσιοδοτημένος κόμβος δεν έχει παραβιαστεί -Πιθανότητα μοναδικού (κεντρικού) σημείου αποτυχίας. ◇ Γλώσσες: Solidity, Java, Python.	Για να δημιουργηθεί ένα κεντροποιημένος αλγόριθμος συναίνεσης ώστε να ελαχιστοποιηθεί η δημιουργία μπλοκ και το ποσοστό επιβεβαίωσης	POA Chain Συστήματα που χρησιμοποιούν Parity

Πίνακας 4.1: Σύγκριση Μοντέλων Συναίνεσης [1, 2, 3, 4, 5].

Κεφάλαιο 5

Αποκεντρωμένες τεχνολογίες σε Ethereum Blockchain

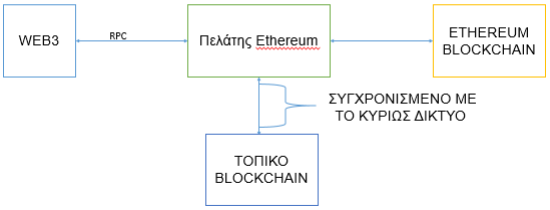
Το Bitcoin ήταν το πρώτο blockchain αλλά όχι το τελευταίο. Στην παρούσα ενότητα μελετάμε το Ethereum blockchain το οποίο είναι εμπνευσμένο από το Bitcoin και προτάθηκε το 2015 από τους Gavin Wood & Vitalik [42]. Χρησιμοποιεί το μοντέλο συναίνεσης της απόδειξης εργασίας [18] και αποτελεί ένα permissionless blockchain [42]. Το Ethereum blockchain χρησιμοποιεί endpoints και λειτουργεί με JSON-RPC API το οποίο υποστηρίζεται, από το Ethereum Web3 Api δηλαδή, από την βιβλιοθήκη web3.js. Τα χαρακτηριστικά της δομής του Ethereum φαίνονται στην παρακάτω Εικόνα 5.1.



Σχήμα 5.1: Η δομή του Ethereum

5.1 Ethereum

Το δίκτυο Ethereum είναι ένα δίκτυο peer-to-peer όπου οι κόμβοι συμμετέχουν στο blockchain και συμβάλουν στον μηχανισμό συναίνεσης [18]. Το Ethereum χωρίζεται σε 2 είδη δικτύων, το κυρίως δίκτυο (mainnet) στο οποίο γίνονται όλες οι δημοσιεύσεις και αφορά την κύρια αλυσίδα του Ethereum και το δίκτυο δοκιμών (testnet), όπου αφορά μια διαφορετική αλυσίδα ξεχωριστή από την κύρια και συνήθως την χρησιμοποιούν οι προγραμματιστές για να δοκιμάσουν τα έξυπνα συμβόλαια τους πως δουλεύουν (π.χ Ropsten) [40]. Το Ethereum αποτελείται από διάφορα συστατικά. Στον πυρήνα, υπάρχει το Ethereum blockchain που εκτελεί το peer-to-peer δίκτυο. Ύστερα, υπάρχει ο client του Ethereum(για παράδειγμα το Geth), το οποίο εκτελείται στους κόμβους και συνδέεται με το ομότιμο (peer-to-peer) δίκτυο, από όπου το blockchain μεταφορτώνεται και αποθηκεύεται τοπικά [40] [18]. Το τοπικό αντίγραφο του blockchain συγχρονίζεται τακτικά με το δίκτυο. Επίσης, ένα άλλο στοιχείο του Ethereum είναι η βιβλιοθήκη web3.js που επιτρέπει την αλληλεπίδραση με τον πελάτη Geth μέσω της διεπαφής Remote Procedure Call (RPC) [40].



Σχήμα 5.2: Το "οικοσύστημα" του Ethereum

5.2 Ψηφιακά Πορτοφόλια

Το ψηφιακό πορτοφόλι είναι μια εφαρμογή που χρησιμεύει ως κύρια διεπαφή με τον χρήστη. Το πορτοφόλι ελέγχει την πρόσβαση στα χρήματα του λογαριασμού του χρήστη, τη διαχείριση κλειδιών και διευθύνσεων, την παρακολούθηση του υπολοίπου του και τη δημιουργία και υπογραφή των συναλλαγών του [34].

Το πορτοφόλι περιέχει μόνο τα δημόσια κλειδιά του χρήστη. Τα κρυπτονομίσματα καταγράφονται στο blockchain [34]. Οι χρήστες ελέγχουν τα κρύπτονομίσματα στο δίκτυο υπογράφοντας συναλλαγές με τα κλειδιά τους. Τα νομίσματα αποθηκεύονται στο blockchain με τη μορφή εξόδων της συναλλαγής [34]. Υπάρχουν δύο κύριοι τύποι πορτοφολιών, που διακρίνονται από το εάν τα κλειδιά που περιλαμβάνουν σχετίζονται μεταξύ τους ή όχι [18]. Ο πρώτος τύπος είναι το μη καθοριστικό πορτοφόλι nondeterministic wallet, όπου κάθε κλειδί παράγεται από έναν τυχαίο αριθμό κάθε φορά γνωστό και ως 'Just a Bunch Of Keys' [34]. Ο δεύτερος τύπος πορτοφολιού είναι ένα ντετερμινιστικό-καθορισμένο πορτοφόλι, όπου όλα

τα κλειδιά προέρχονται από ένα μόνο κύριο κλειδί, γνωστό ως σπόρο. Όλα τα κλειδιά σε αυτόν τον τύπο πορτοφολιού συνδέονται μεταξύ τους και μπορούν να δημιουργηθούν και πάλι αν έχει κάποιον αρχικό σπόρο [18]. Για να γίνει ευκολότερη η χρήση των ντετερμινιστικών πορτοφολιών, οι σπόροι κωδικοποιούνται ως αγγλικές λέξεις, γνωστές ως κωδικές μνημονικές λέξεις mnemonic code words. Οποιοσδήποτε έχει στην κατοχή του αυτές τις λέξεις και την σειρά τους μπορεί να αναπαράγει τον σπόρο [34].

5.2.1 Μη καθορισμένα πορτοφόλια

Στα Bitcoin, Ethereum τα πρώτα πορτοφόλια ήταν συλλογές τυχαία παραγόμενων ιδιωτικών κλειδιών. Αυτά τα πορτοφόλια έχουν αντικατασταθεί από ντετερμινιστικά πορτοφόλια, επειδή είναι δύσκολη η διαχείριση τους (δημιουργία αντιγράφων ασφαλείας). Το μειονέκτημα των τυχαίων κλειδιών είναι ότι, πρέπει να διατηρείται αντίγραφο για κάθε κλειδί [18]. Αν χαθεί το πορτοφόλι τότε αυτόματα χάνονται και οι οικονομίες που περιείχε αυτό. Αυτό έρχεται σε άμεση αντίθεση με την αρχή της αποφυγής επαναχρησιμοποίησης διευθύνσεων, χρησιμοποιώντας κάθε διεύθυνση bitcoin για μία μόνο συναλλαγή [18]. Η επαναχρησιμοποίηση της ίδιας διεύθυνσης μειώνει την ιδιωτικότητα, καθώς συνδυάζοντας πολλαπλές συναλλαγές και διευθύνσεις μεταξύ τους, μειώνεται η ψευδο-ανωνυμία. Στην περίπτωση του Ethereum τα μη καθορισμένα πορτοφόλια ¨τύπου 0' είναι τα δυσκολότερα να αντιμετωπιστούν, επειδή δημιουργούν ένα νέο αρχείο πορτοφολιού για κάθε νέα διεύθυνση με έναν τρόπο 'just in time' [18]. Παρόλα αυτά υπάρχουν πολλοί πελάτες του Ethereum που χρησιμοποιούν ένα αρχείο αποθήκευσης του κλειδιού το οποίο έχει JSON μορφή και περιέχει ένα κρυπτογραφημένο ιδιωτικό κλειδί [34] [18]. Παράδειγμα:


```
{
"address":"c10674bfce6a9933db3dd6f4ee895b8910ab5b78",
 "crypto":{
 "cipher":"aes-128ctr",
 "ciphertext":"c5ba1529dffdaf1e2b4439dd41e4e12eb6a1310fbf0761004ab9efba4d27851e",
 "cipherparams":{
 "iv":"669df88f19708a17c930ce45c04ec36e"},
 "kdf":"scrypt",
 "kdfparams":{"dklen":32,"n":262144,
 "p":1,"r":2,
 "salt":"7807232bb72a2cf2a20af95195d6fb3d6e0fdff76e521aa30504ee22a6d506d5"},
 "mac":"ee3ee3af662b4b4508c975df89b3914e0aaac5556c65944f6ca47e5b7319de4e"},
 "id":"7a551706-e627-40af-b9c9-0fce3940d4cf",
 "version":3
}
```


Ντετερμινιστικά-καθορισμένα πορτοφόλια

Τα ντετερμινιστικά ή seeded πορτοφόλια είναι πορτοφόλια τα οποία περιέχουν ιδιωτικά κλειδιά τα οποία προέρχονται από ένα κοινό σπόρο, με τη χρήση μιας μονόδρομης συνάρτησης διασποράς [34]. Ο σπόρος είναι ένας τυχαία παραγόμενος αριθμός που συνδυάζεται με άλλα

δεδομένα [18]. Σε ένα ντετερμινιστικό πορτοφόλι, ο σπόρος είναι επαρκής για να ανακτήσει όλα τα παράγωγα κλειδιά και ως εκ τούτου αρκεί ένα μόνο αντίγραφο ασφαλείας κατά το χρόνο δημιουργίας [40]. Ο σπόρος είναι επίσης επαρκής για την εξαγωγή ή την εισαγωγή πορτοφολιού, επιτρέποντας την εύκολη μετακίνηση όλων των κλειδιών του χρήστη μεταξύ διαφορετικών υλοποιήσεων πορτοφολιού [34].

5.2.2 Ιεραρχικά Ντετερμινιστικά Πορτοφόλια HD (BIP-32 BIP-44)

Τα ντετερμινιστικά πορτοφόλια αναπτύχθηκαν για να καταστήσουν εύκολη την εξαγωγή πολλών κλειδιών από έναν ενιαίο ΄σπόρο΄ [18]. Η πιο προηγμένη μορφή ντετερμινιστικών πορτοφολιών είναι το ιεραρχικό πορτοφόλι HD που ορίζεται από το πρότυπο BIP-32 [34] [18]. Τα πορτοφόλια HD περιέχουν κλειδιά που παράγονται σε μια δομή δέντρου, έτσι ώστε ένα γονικό κλειδί να μπορεί να παράγει μια σειρά παιδιών-κλειδιών, καθένα από τα οποία μπορεί να αποφέρει μια σειρά από κλειδιά-εγγόνια και ούτω καθεξής, σε ένα άπειρο βάθος [18]. Τα πορτοφόλια HD προσφέρουν δύο σημαντικά πλεονεκτήματα σε σχέση με τα τυχαία (μη καθορισμένα) κλειδιά [34]:

- Η δομή του δέντρου μπορεί να χρησιμοποιηθεί για να εκφράσει μια πρόσθετη οργανωτική σημασία, όπως όταν χρησιμοποιείται ένα συγκεκριμένο κλαδί δευτερευόντων κλειδιών για την είσοδο εισερχόμενων πληρωμών και χρησιμοποιείται ένα διαφορετικό κλαδί για να λαμβάνει την αλλαγή από τις εξερχόμενες πληρωμές [34].

- Οι χρήστες μπορούν να δημιουργήσουν μια σειρά δημόσιων κλειδιών χωρίς να έχουν πρόσβαση στα αντίστοιχα ιδιωτικά κλειδιά [34]. Αυτό επιτρέπει στα πορτοφόλια HD να χρησιμοποιούνται σε έναν μη ασφαλή διακομιστή δημιουργώντας ένα διαφορετικό δημόσιο κλειδί για κάθε συναλλαγή [34].

5.2.3 Σπόροι και μνημονικοί κωδικοί (BIP-39)

Υπάρχουν πολλοί τρόποι για την κωδικοποίηση ενός ιδιωτικού κλειδιού για την δημιουργία αντιγράφων ασφαλείας και ανάκτηση τους [34]. Πλέον προτιμάτε μια μέθοδος συνδυασμού από μια σειρά αγγλικών λέξεων που όταν τοποθετηθούν στην σωστή σειρά εξάγουν το ιδιωτικό κλειδί [34] [18]. Αυτό είναι γνωστό ως μνημονικό (mnemonic) και ορίζεται από το BIP-39. Σήμερα, τα περισσότερα πορτοφόλια Bitcoin, Ethereum χρησιμοποιούν αυτό το πρότυπο και μπορούν να εισάγουν και να εξάγουν τους σπόρους για την αποθήκευση και την ανάκτηση λογαριασμών, χρησιμοποιώντας μόνο τα μνημονικά [34]. Παράδειγμα με Ethereum ιδιωτικό κλειδί: 2304305F9FCC0F50E8A213AF903C3E416D959B9AF0951EBAE745217D8C4A15A και το αντίστοιχο μνημονικό του sock pact twice doctor kite track lonely axis able climb crumble hidden copper into parent

Το πλεονέκτημα με το μνημονικό είναι ότι, ο κατάλογος των γνωστών λέξεων είναι αρκετά εύκολο να αντιμετωπιστεί, επειδή υπάρχει πλεόνασμα στη συγγραφή λέξεων.

Βέλτιστες Πρακτικές Πορτοφολιού Καθώς έχει ωριμάσει η τεχνολογία των πορτοφολιών, έχουν προκύψει ορισμένα κοινά πρότυπα του κλάδου που καθιστούν τα πορτοφόλια σε γενικές γραμμές διαλειτουργικά, εύχρηστα, ασφαλή και ευέλικτα [34]. Αυτά τα πρότυπα επίσης επιτρέπουν στα πορτοφόλια να παράγουν κλειδιά για διάφορα κρυπτονομίσματα, όλα από ένα μόνο μνημονικό. [18] Αυτά τα κοινά πρότυπα είναι:

- Οι μνημονικές κωδικές λέξεις, στην βάση του BIP-39.
- Τα πορτοφόλια HD, στην βάση του BIP-32.
- Η δομή πορτοφολιού πολλαπλών χρήσεων HD, βασισμένη στο BIP-43.
- Τα πολλαπλά πορτοφόλια με πολλαπλούς λογαριασμούς, στην βάση του BIP-44.

Τα πρότυπα υιοθετήθηκαν από ένα ευρύ φάσμα λογισμικού και υλικού, καθιστώντας όλα αυτά τα πορτοφόλια διαλειτουργικά [18]. Ένας χρήστης μπορεί να εξάγει ένα μνημονικό που δημιουργείται σε ένα από αυτά τα πορτοφόλια και να το εισάγει σε άλλο πορτοφόλι, ανακτώντας όλες τις συναλλαγές, τα κλειδιά και τις διευθύνσεις του [34]. Ορισμένα παραδείγματα πορτοφολιών λογισμικού που υποστηρίζουν αυτά τα πρότυπα περιλαμβάνουν τα Breadwallet, Copay, Metamask και το Mycelium [18]. Παραδείγματα από υλικά hardware πορτοφόλια, που υποστηρίζουν αυτά τα πρότυπα περιλαμβάνουν τα Keepkey, Ledger, Trezor.

5.3 Λογαριασμοί

Όπως σε όλα τα blockchain, έτσι και στο Ethereum υπάρχουν κλειδιά και λογαριασμοί. Πριν όμως την περιγραφή τους, είναι πολύ σημαντικό να γίνει αντιληπτή η έννοια της παγκόσμιας κατάστασης (world state ή απλά state).

World State Η Παγκόσμια Κατάσταση είναι μια χαρτογράφηση μεταξύ διευθύνσεων δηλαδή, αναγνωριστικά των 160 bit και (καταστάσεων) λογαριασμών και αποτελεί το ανώτερο επίπεδο του Ethereum [42]. Το World State δεν είναι αποθηκευμένο στο blockchain, η ¨παγκόσμια κατάσταση' διατηρεί αυτή τη χαρτογράφηση σε ένα τροποποιημένο δέντρο Merkle Patricia [42]. Το trie απαιτεί μία βάση δεδομένων που διατηρεί μια χαρτογράφηση μεταξύ πινάκων byte με αντίστοιχους πίνακες byte [42]. Αυτή η βάση δεδομένων ονομάζεται "η βάση δεδομένων της κατάστασης" [42]. Αυτό έχει πολλά οφέλη όπως, ο κόμβος ρίζα αυτής της δομής εξαρτάται κρυπτογραφικά από όλα τα εσωτερικά δεδομένα και ως εκ τούτου η σύνοψη του μπορεί να χρησιμοποιηθεί ως ασφαλής αναγνωριστικό για ολόκληρη την κατάσταση του

συστήματος [42]. Επίσης, δεδομένου ότι αποτελεί μια αμετάβλητη δομή δεδομένων, αυτό επιτρέπει την ανάκληση οποιασδήποτε προηγούμενης κατάστασης, μέσω της αλλαγής της σύνοψης της ρίζας [42]. Εφόσον αποθηκεύονται όλες αυτές οι ρίζες στο blockchain και έτσι μπορεί να επιστρέψει μια παλιά κατάσταση [42].

Κατηγορίες λογαριασμών Από την άλλη, στο χαμηλότερο επίπεδο υπάρχουν οι διευθύνσεις Ethereum που αντιπροσωπεύουν κάποιους λογαριασμούς που περιλαμβάνουν ένα υπόλοιπο σε Ether, ένα nonce (που αντιπροσωπεύει τον αριθμό-μετρητή των συναλλαγών που αποστέλλονται επιτυχώς από αυτόν τον λογαριασμό), το storage του λογαριασμού (που είναι μόνιμος χώρος αποθήκευσης δεδομένων και χρησιμοποιείται μόνο από τα έξυπνα συμβόλαια) και το program code του λογαριασμού [18].

Επομένως, οι λογαριασμοί είναι ένα από τα βασικά χαρακτηριστικά του δικτύου. Υπάρχουν 2 ειδών λογαριασμοί: 1) οι λογαριασμοί των χρηστών Externally Owned Accounts (EOAs), 2) οι λογαριασμοί των έξυπνων συμβολαίων Contract Accounts (CAs) [42, 18]. Η πρώτη κατηγορία των λογαριασμών μοιάζει πολύ με αυτές από το bitcoin δηλαδή διατηρούν ένα υπόλοιπο σε Ether. Αυτά είναι ικανά να στείλουν συναλλαγές και επίσης, ελέγχονται από ιδιωτικά κλειδιά, δεν εμπεριέχουν κώδικα, έχουν αποθηκευμένη την τιμή του κλειδιού και πάντα σχετίζονται με ανθρώπους [40, 18]. Στην 2η περίπτωση των λογαριασμών, που αφορούν τα έξυπνα συμβόλαια, έχουν κάποια διαφορετικά χαρακτηριστικά σε σχέση με την 1η κατηγορία δηλαδή, έχουν υπόλοιπο σε Ether, όμως συσχετίζονται πάντα με κάποιον κώδικα, δεν μπορούν να εκτελέσουν κάποια συναλλαγή από μόνα τους, αλλά τα ίδια εκτελούν τον κώδικα, διατηρούν την κατάσταση τους πάντοτε ίδια, δεν συσχετίζονται με ανθρώπους και περιέχουν κάποια τιμή κλειδιού [40, 18]. Τέλος, όταν ο προορισμός μιας συναλλαγής είναι μια διεύθυνση έξυπνου συμβολαίου, αυτό προκαλεί την εκτέλεση του έξυπνου συμβολαίου στο EVM τροποποιώντας έτσι την κατάσταση της.

5.4 Συναλλαγές

Το Ethereum, όπως και κάθε άλλο blockchain, είναι ένα δίκτυο που βασίζεται στις συναλλαγές (transaction driven state machine). Μια συναλλαγή είναι μια ενιαία κρυπτογραφικά υπογεγραμμένη εντολή που έχει κατασκευαστεί από έναν εξωτερικό παράγοντα στο Ethereum. Ενώ υποτίθεται ότι ο τελικός εξωτερικός παράγοντας θα είναι ανθρώπινος, θα χρειαστεί να χρησιμοποιηθούν εργαλεία λογισμικού για την κατασκευή και τη διάδοση της συναλλαγήςEyellow. Υπάρχουν δύο τύποι συναλλαγών: εκείνες που έχουν ως αποτέλεσμα κλήσεις μηνυμάτων και αυτές που οδηγούν στη δημιουργία νέων διευθύνσεων/λογαριασμών με σχετικό κώδικα προγραμματισμού (γνωστό ως «δημιουργία συμβολαίου») [42].

5.4.1 Συναλλαγές μηνυμάτων

Η βασική ιδέα είναι ότι στο blockchain Ethereum, μια κατάσταση "γένεσης" genesis-state μετατρέπεται σε τελική κατάσταση, σταδιακά, μέσα από την εκτέλεση επάλληλων συναλλαγών [18]. Ο τελικός μετασχηματισμός δημοσιεύετε στην παγκόσμια κατάσταση του blockchain [40]. Για παράδειγμα, έστω ένας χρήστης ζητάει χρήματα από έναν άλλον ή ο αποστολέας απλώς αποφασίζει να στείλει τα χρήματα του στον παραλήπτη. Το αίτημα αυτό μπορεί να ολοκληρωθεί, εφόσον ο παραλήπτης στείλει πρώτα την διεύθυνση Ethereum του στον αποστολέα. Η αποστολή της διεύθυνσης μπορεί να γίνει είτε σαν μορφή πλαιντεξτ, είτε ενθυλακωμένη μέσα σε ένα QR code [43]. Στην 2η περίπτωση ο αποστολέας απλώς σκανάρει μέσω του κινητού του τον κωδικό, με αποτέλεσμα τα χρήματα να μεταφερθούν από το Ethereum πορτοφόλι του στην διεύθυνση που σκάναρε (εφόσον αυτός πρώτα την εγκρίνει) [43]. Πριν προλάβει να ενημερωθεί ο παραλήπτης ότι στο πορτοφόλι του προστέθηκαν χρήματα πρέπει να γίνουν κάποιες ενέργειες πρώτα στο δίκτυο του Ethereum [43] [40].

Αρχικά, εφόσον η συναλλαγή δημιουργήθηκε στο λογισμικό του πορτοφολιού του αποστολέα, αυτή δημοσιεύετε στο δίκτυο του Ethereum και υπογράφεται ψηφιακά από τον αποστολέα, για να αποδείξει ότι είναι ο ιδιοκτήτης των Ether [18]. Στην συνέχεια η συναλλαγή παραλαμβάνεται από τους mining κόμβους, ώστε να την επιβεβαιώσουν, ενώ στην συνέχεια θα την συμπεριλάβουν στο μπλοκ. Αφού εγκριθεί και προστεθεί στο μπλοκ, τότε ξεκινάει η λειτουργία του μοντέλου συναίνεσης "Απόδειξη Εργασίας" [18]. Μόλις ο miner λύσει το παζλ της Απόδειξης, τότε με ένα νέο nonce, αυτό το μπλοκ μεταδίδεται αμέσως στους υπόλοιπους κόμβους και στη συνέχεια επαληθεύουν το μπλοκ αυτό. Εάν περάσουν όλοι οι έλεγχοι, τότε αυτό το μπλοκ προστίθεται στο blockchain και οι miners πληρώνονται ανάλογα την εργασία που κατέβαλαν. Τελικά, ο παραλήπτης ενημερώνεται για την προσθήκη των χρημάτων στο πορτοφόλι του [18].

Η παραπάνω διαδικασία είναι η μία μορφή συναλλαγής του Ethereum, δηλαδή η συναλλαγή μηνυμάτων. Ένα μήνυμα είναι ένα πακέτο δεδομένων που μεταφέρεται μεταξύ δύο λογαριασμών. Αυτό το πακέτο δεδομένων περιέχει δεδομένα και μια τιμή (σε Ether). Μπορεί είτε να αποσταλεί μέσω του έξυπνου συμβολαίου, είτε από εξωτερικό παράγοντα, υπό τη μορφή συναλλαγής που έχει υπογραφεί ψηφιακά από τον αποστολέα. Οπότε όπως φαίνεται και στην Εικόνα 5.1, η δομή της συναλλαγής μηνυμάτων περιλαμβάνει τα εξής στοιχεία [42] [40]:

1. Τον αποστολέα recipient.
2. Το τρέχον βάθος της στοίβας δημιουργίας μηνύματος ή μετρητής nonce.
3. Τον παραλήπτη (το οποίο είναι ένα συστατικό του μηνύματος).
4. Το διαθέσιμο αέριο Gas limit.
5. Την τιμή του αερίου Gas price.

6. v,r,s. Τιμές που αντιστοιχούν στην υπογραφή της συναλλαγής και χρησιμοποιούνται για τον προσδιορισμό του αποστολέα της συναλλαγής.

7. Την τιμή value(σε Ether).

8. Τα δεδομένα data εισόδου της κλήσης.

Οι κλήσεις μηνυμάτων παράγουν επίσης δεδομένα εξόδου, τα οποία δεν χρησιμοποιούνται όταν εκτελούνται συναλλαγές, παρά μόνο όταν καλούνται από την VM [42]. Οπότε, η κλήση μηνύματος είναι η πράξη μετάδοσης ενός μηνύματος από έναν λογαριασμό στον άλλο. Εάν ο λογαριασμός προορισμού έχει έναν σχετικό κώδικα EVM, τότε η εικονική μηχανή θα ξεκινήσει μόλις λάβει το μήνυμα για να εκτελέσει τις απαιτούμενες λειτουργίες [42].

5.4.2 Συναλλαγές δημιουργίας έξυπνων συμβολαίων

Η άλλη μορφή συναλλαγής είναι η δημιουργία έξυπνων συμβολαίων. Η βασική ομοιότητα με τις συναλλαγές μηνυμάτων είναι ότι, τα συμβόλαια μπορούν να στείλουν μηνύματα σε άλλα συμβόλαια, καθώς τα μηνύματα υπάρχουν μόνο στο περιβάλλον εκτέλεσης και δεν αποθηκεύονται ποτέ [42]. Ωστόσο, η κύρια διαφορά είναι ότι αυτά παράγονται από τα έξυπνα συμβόλαια, ενώ οι συναλλαγές παράγονται από εξωτερικούς λογαριασμούς στο περιβάλλον του Ethereum [42]. Οι συναλλαγές που δημιουργούν συμβόλαια έχουν και αυτές τα ίδια στοιχεία με την συναλλαγή μηνύματος αλλά αντί για δεδομένα data, διαθέτει ένα άλλο πεδίο το οποίο είναι το init δηλαδή μια διάταξη από byte απεριόριστου μεγέθους που καθορίζει τον κώδικα της EVM για τη διαδικασία αρχικοποίησης λογαριασμού. Το init, δηλαδή η αρχικοποίηση, εκτελείται μόνο μία φορά στη δημιουργία λογαριασμού [42].

Εφόσον υπάρξει δημιουργία συμβολαίου, μετά την εκτέλεση της EVM, τότε από αυτήν την συναλλαγή δημιουργείται η διεύθυνση του συμβολαίου. Οπότε οι διευθύνσεις αυτές είναι τα δεξιά 160-bit της σύνοψης Keccak 256-bit του RLP (δηλαδή την κατάσταση του λογαριασμού) [42] [40].

5.5 Το Μπλοκ στο Ethereum

Το μπλοκ στο Ethereum είναι λίγο διαφορετικό σε σχέση με την μορφή μπλοκ που περιγράφεται στην 3η ενότητα. Το μπλοκ του Ethereum είναι μια συλλογή πολλών σχετικών πληροφοριών στην επικεφαλίδα - header του μπλοκ, μαζί με πληροφορίες για την απαιτούμενη συναλλαγή κάθε φορά, καθώς και headers από τα αδέλφια μπλοκ του γονέα, δηλαδή τα μπλοκ θείοι(ommers)Eyellow [40]. Το Ethereum συνήθως χρησιμοποιεί την συνάρτηση διασποράς keccak-256 που αποτελεί μέρος της κατηγορίας SHA-3 συναρτήσεων διασποράς. Οπότε και όλα τα στοιχεία που συντελούν ένα μπλοκ είναι κρυπτογραφημένα σε τέτοια συνάρτηση διασποράς. Αναφορικά τα μέρη που απαρτίζουν ένα μπλοκ, όπως φαίνεται και στην Εικόνα 5.1, είναι τα εξής [42]:

- Η σύνοψη του header του γωνικού μπλοκ.
- Η σύνοψη του header των ommers.
- Ο δικαιούχος. Δηλαδή, η 160-bit διεύθυνση στην οποία μεταφέρονται όλα τα τέλη που εισπράττονται από την επιτυχή εξόρυξη του μπλοκ αυτού.
- Τα stateRoot, transactionsRoot και receiptsRoot. Δηλαδή, οι τιμές διασποράς του κόμβου-ρίζα που αφορούν αντίστοιχα την περάτωση, την λίστα και την απόδειξη της κάθε συναλλαγής.
- logsBloom. Το φίλτρο Bloom που αποτελείται από πληροφορίες που αφορούν το ευρετήριο και αυτές περιέχονται σε κάθε καταχώριση από την παραλαβή κάθε συναλλαγής στον κατάλογο συναλλαγών.
- Δυσκολία difficulty. Μια βαθμωτή τιμή που αντιστοιχεί στο επίπεδο δυσκολίας αυτού του μπλοκ.
- Αριθμός number. Μια βαθμωτή τιμή ίση με τον αριθμό των μπλοκ των προγόνων.
- gasLimit. Μια βαθμωτή τιμή ίση με το τρέχον όριο της δαπάνης αερίου ανά μπλοκ.
- GasUsed. Μια βαθμωτή τιμή ίση με το συνολικό αέριο που χρησιμοποιήθηκε για τις συναλλαγές σε αυτό το μπλοκ.
- Η Χρονοσφραγίδα στην αρχή του μπλοκ.
- extraData. Μια αυθαίρετη συστοιχία byte που περιέχει δεδομένα σχετικά με αυτό το μπλοκ. Αυτό πρέπει να είναι 32 bytes ή λιγότερα.
- mixHash. Μία σύνοψη της τάξεως των 256-*bit* που αποδεικνύει ότι έχει χρησιμοποιηθεί επαρκής υπολογιστική ισχύς σε αυτό το μπλοκ.
- nonce. Μια τιμή 64-bit που σε συνδυασμό με το mixhash, αποδεικνύει ότι έχει πραγματοποιηθεί επαρκής υπολογισμός σε αυτό το μπλοκ. Δεν έχει σχέση με το nonce της 3ης ενότητας.

Ένα μπλοκ στο Ethereum θεωρείται έγκυρο όταν αυτό ακολουθεί κάποιες συγκεκριμένες προϋποθέσεις, δηλαδη [40]:

- Πρέπει να σχετίζεται με τα αδέλφια του γονικού κόμβου (δηλαδή τους θείους του) και τις συναλλαγές, αυτό σημαίνει ότι όλοι οι ommers ικανοποιούν την ιδιότητα ότι είναι όντως θείοι και επίσης το PoW των θείων πρέπει να είναι έγκυρο.
- Πρέπει ο γονέας του μπλοκ (προηγούμενο μπλοκ) να υπάρχει και να είναι έγκυρος (η σύνοψη του μπλοκ).

- Πρέπει να ισχύει η χρονοσφραγίδα του μπλοκ. Αυτό σημαίνει ότι η χρονοσφραγίδα του τρέχοντος μπλοκ πρέπει να είναι υψηλότερη από τη χρονική σήμανση του γονικού μπλοκ. Επίσης, θα πρέπει να έχει δημιουργηθεί σε λιγότερο από 15 λεπτά μετά από τον γονέα του.

- Εάν αποτύχει οποιοσδήποτε από αυτούς τους ελέγχους, το μπλοκ θα απορριφθεί [40].

Κατά την διαδικασία την ολοκλήρωσης ενός μπλοκ στο Ethereum γίνεται η επικύρωση του μπλοκ και η κατανομή των των κερδών από την εξόρυξη του μπλοκ. Για να θεωρηθεί ότι ένα μπλοκ έχει ολοκληρωθεί με επιτυχία, πρέπει να ακολουθηθούν τα έξης 4 βήματα [40]:

1. Η Επικύρωση ommers. Η διαδικασία επικύρωσης των κεφαλίδων των προηγούμενων μπλοκ ελέγχει αν η κεφαλίδα είναι έγκυρη και αν η σχέση του ommer με το τρέχον μπλοκ ικανοποιεί το μέγιστο βάθος των έξι μπλοκ. Ένα μπλοκ μπορεί να έχει μέχρι και δύο ommers.

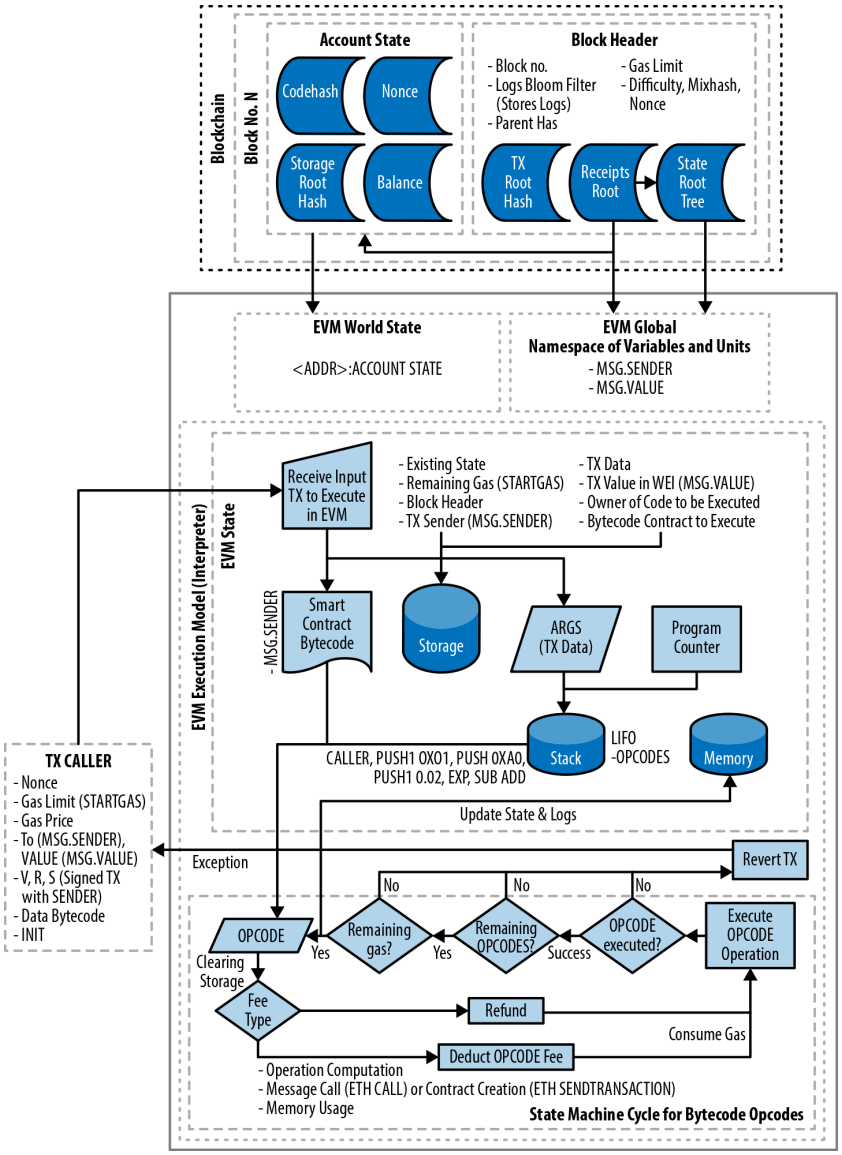
2. Η Επικύρωση των συναλλαγών. Η διαδικασία αυτή περιλαμβάνει έναν έλεγχο, για το εάν το συνολικό αέριο που χρησιμοποιείται στο μπλοκ είναι ίσο με την τελική κατανάλωση αερίου μετά την τελευταία συναλλαγή.

3. Η απόδοση ανταμοιβής. Γίνεται η ενημέρωση του λογαριασμό του δικαιούχου με το υπόλοιπο της ανταμοιβής. Στο Ethereum, δίνεται επίσης ανταμοιβή στους miners των προηγούμενων μπλοκ, το οποίο είναι το 1/32 της ανταμοιβής μπλοκ. Οι θείοι που περιλαμβάνονται στα μπλοκ λαμβάνουν επίσης 7/8 της συνολικής ανταμοιβής μπλοκ. Η τρέχουσα ανταμοιβή είναι 3 Ether.

4. Επαλήθευση κατάστασης και του nonce.

5.6 EVM

Το EVM είναι το σύστημα του Ethereum που χειρίζεται και εκτελεί τα έξυπνα συμβόλαια. Οι απλές συναλλαγές τιμών (value) μεταξύ δύο EOA δεν χρειάζεται να χρησιμοποιήσουν την EVM, αλλά οποιαδήποτε άλλη συναλλαγή θα πρέπει να υπολογιστεί από την EVM και στην συνέχεια να ενημερώσει την κατάσταση της [18]. Αν το δούμε μακροσκοπικά, το EVM μπορεί να θεωρηθεί ως ένας παγκόσμιος αποκεντρωμένος υπολογιστής που περιέχει εκατομμύρια εκτελέσιμα αντικείμενα, το καθένα με το δικό του μόνιμο χώρο αποθήκευσης δεδομένων [18]. Ένας από τους βασικούς λόγους όπου το Ethereum είναι ασφαλές, είναι γιατί η Εικονική Μηχανής της είναι εντελώς απομονωμένη [42]. Οι αλλαγές της κατάστασης του Ethereum γίνονται από την εικονική μηχανή του Ethereum (EVM). Η Εικονική Μηχανή του Ethereum είναι μια μηχανή εκτέλεσης που βασίζεται στην λειτουργία της στοίβας



Σχήμα 5.3: Η ολοκληρωμένη απεικόνιση της λειτουργίας της Εικονικής Μηχανής του Ethereum [18]

(συγκεκριμένα το Last In, First Out (LIFO)) που εκτελεί εντολές bytecode για να μεταχηματίσει την κατάσταση του συστήματος από μια κατάσταση στην άλλη [18].Το μέγεθος της στοίβας περιορίζεται στα 1024 στοιχεία [40]. Το μέγεθος μιας λέξης στην εικονική μηχανή έχει οριστεί σε 256-bit για την κάθε μία, ώστε να μπορεί να δέχεται το μέγεθος των συναρτήσεων διασποράς όπως η Keccak-256, αλλά και υπολογισμούς με ελλειπτικές καμπύλες. Η αρχιτεκτονική της EVM 5.3 διαθέτει κάποια διευθυνσιοδοτούμενα στοιχεία, όπως α) το αμετάβλητο *program code ROM*, το οποίο διαθέτει το bytecode του έξυπνου συμβολαίου που πρόκειται να εκτελεστεί, β) η πτητική memory μεταβλητή και γ) η σταθερή μεταβλητή storage που αποτελεί μέρος της κατάστασης του Ethereum [18].

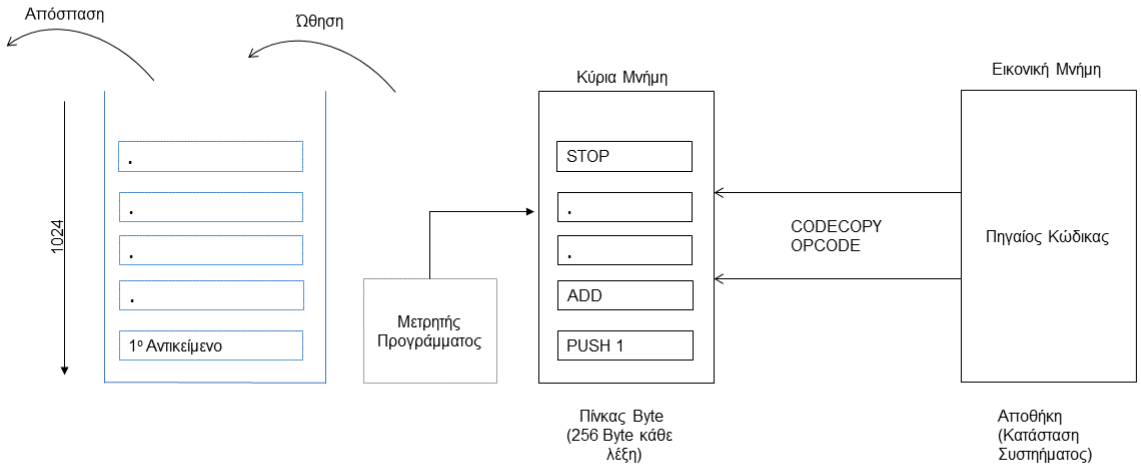
Το *σύνολο οδηγιών της EVM* ή αλλιώς οι λειτουργίες bytecode εκτελούν όλες τις λειτουργίες που μπορεί να χρειαστεί κανείς, όπως i) αριθμητικές λειτουργίες, ii) κλήσεις μηνυμάτων, iii) πρόσβαση στην μνήμη, στο storage και στην στοίβα, iv) έλεγχο στις λει-

τουργίες ροής αλλά και πολλές άλλες λειτουργίες [18]. Σε αντίθεση με το bytecode, η EVM έχει πρόσβαση στις πληροφορίες των λογαριασμών και των μπλοκ. Τα opcodes της EVM είναι οι λειτουργίες που διαθέτει όπως για παράδειγμα η λειτουργία *'DIV'*, που διαιρεί δύο ακέραιους αριθμούς ή η λειτουργία *'BALANCE'*, που επιστρέφει το διαθέσιμο υπόλοιπο του δοθέντος λογαριασμού [18, 42]. Όλες οι λειτουργίες αλληλεπιδρούν με την στοίβα και τα αποτελέσματα τους τα τοποθετούν στην κορυφή της [18].

Το Ethereum αποτελεί ένα transaction-based state machine δηλαδή, ένα σύστημα που βασίζεται στις συναλλαγές, το οποίο αντικατοπτρίζει το γεγονός ότι εξωτερικοί παράγοντες (δηλαδή, κάτοχοι λογαριασμών) ξεκινούν μεταβάσεις κατάστασης με την δημιουργία συναλλαγών [18].

Η EVM αποτελεί ένα Turing πλήρης σύστημα αλλά επίσης, περιορίζεται από την ποσότητα αερίου που απαιτείται για την εκτέλεση οποιασδήποτε εντολής. Αυτό σημαίνει ότι οι ατέρμονες βρόχοι μπορούν να οδηγήσουν σε επιθέσεις άρνησης εξυπηρέτησης, όμως δεν γίνεται να πραγματοποιηθούν αυτές οι επιθέσεις, λόγω του περιορισμού στην χρήση αερίου [40]. Πρακτικά αντιμετωπίζεται καθώς για την ανάπτυξη και δημοσίευση ενός συμβολαίου το Ethereum χρησιμοποιεί ένα όριο που ορίζεται ως κατανάλωση αερίου και συσσωρεύει το κόστος των συναλλαγών ώστε αυτές να είναι πεπερασμένες. Το όριο στην κατανάλωση του αερίου κατά την ανάπτυξη ενός έξυπνου συμβολαίου φαίνεται και στα διαγράμματα της μελέτης των Tonelli et al [48]. Στη συγκεκριμένη έρευνα, μελετήθηκαν 12.094 έξυπνα συμβόλαια και συγκρίθηκαν με βάση τις καθολικές μετρικές και μετρικές που αφορούν μόνο αποκεντρωμένες εφαρμογές (κλήσεις από και προς άλλες διευθύνσεις, εσωτερικές κλήσεις στο έξυπνο συμβόλαιο, κατανάλωση αερίου, συναλλαγή κρυπτονομισμάτων και bytecode/ABI). Σε όλες τις παραπάνω μετρικές φαίνεται ότι φτάνουν σε ένα άνω όριο και αυτό οφείλεται στον περιορισμό του αερίου που μπορεί να καταναλωθεί από τα έξυπνα συμβόλαια. Το έξυπνο συμβόλαιο είναι πολύ σημαντικό κομμάτι στις αποκεντρωμένες εφαρμογές καθώς λειτουργεί ως η βάση δεδομένων για τις εφαρμογές αυτές. Όλα τα δεδομένα που αποθηκεύονται σε ένα συμβόλαιο αποθηκεύονται μοναδικά στην συγκεκριμένη διεύθυνση δηλαδή, στην κατάστασή του και επιστρέφονται από αυτή. Επίσης, η Solidity μεταγλωττίζεται σε χαμηλό επίπεδο γλώσσας προγραμματισμού, δηλαδή σε bytecode, με την βοήθεια της EVM.

Η EVM υποστηρίζει επίσης χειρισμό εξαιρέσεων, δηλαδή σε περίπτωση που προκύψουν εξαιρέσεις, τότε η μηχανή θα σταματήσει αμέσως και θα επιστρέψει το σφάλμα εκτέλεσης [40] [18]. Ο κώδικας που εκτελείται στην EVM δεν έχει πρόσβαση σε εξωτερικούς πόρους, όπως ένα δίκτυο ή μία βάση δεδομένων και το καθιστά εξαιρετικά ασφαλές.



Σχήμα 5.4: Η αφαιρετική απεικόνιση της λειτουργίας της Εικονικής Μηχανής του Ethereum

5.7 Έξυπνο Συμβόλαιο

Ο όρος έξυπνο συμβόλαιο είναι ένας όρος παλιός και με ιστορική σημασία. Στη δεκαετία του 1990, ο κρυπτογράφος Nick Szabo επινόησε τον όρο αυτόν και τον όρισε ως ¨ένα σύνολο υποσχέσεων, που καθορίζονται σε ψηφιακή μορφή, συμπεριλαμβανομένων των πρωτοκόλλων εντός των οποίων οι οντότητες εκτελούν άλλες υποσχέσεις' [18]. Από τότε, η έννοια των έξυπνων συμβολαίων έχει εξελιχθεί. Τα 4 βασικά χαρακτηριστικά των έξυπνων συμβολαίων είναι τα εξής [18]:

- Αποτελούν προγράμματα υπολογιστών και δεν έχουν καμία νομική ιδιότητα.
- Είναι σταθερά. Από την στιγμή που αναπτύσσονται στο blockchain δεν μπορεί ο πηγαίος κώδικας τους να αλλάξει, κάτι το οποίο γίνεται στα υπόλοιπα λογισμικά.
- Έιναι ντετερμινιστικά. Τα αποτέλεσμα της εκτέλεσης των έξυπνων συμβολαίων είναι ίδιο για όλους όσους το εκτελούν.
- Περιέχει λειτουργίες της EVM. Τα έξυπνα συμβόλαια λειτουργούν με περιορισμένο περιεχόμενο εκτέλεσης. Μπορούν να έχουν πρόσβαση στην κατάστασή τους, στο περιεχόμενο της συναλλαγής που το κάλεσε και πληροφορίες για τα πρόσφατα μπλοκ.

Ένα έξυπνο συμβόλαιο είναι μια συλλογή από κώδικα και δεδομένα, που αναπτύσσεται σε ένα blockchain [1]. Οι συναλλαγές στο blockchain μπορούν να στείλουν δεδομένα στις

δημόσιες μεθόδους, που προσφέρονται από το έξυπνο συμβόλαιο. Το συμβόλαιο εκτελεί την κατάλληλη μέθοδο με τα δεδομένα που έδωσε ο χρήστης για την εκτέλεση μιας υπηρεσίας [1]. Ο κώδικας, ο οποίος βρίσκεται στο blockchain είναι αμετάβλητος και ως εκ τούτου μπορεί να χρησιμοποιηθεί ως αξιόπιστη τρίτη οντότητα για οικονομικές συναλλαγές, που είναι πιο πολύπλοκες από την απλή αποστολή κεφαλαίων μεταξύ λογαριασμών [1]. Ένα έξυπνο συμβόλαιο μπορεί να πραγματοποιήσει υπολογισμούς, να αποθηκεύσει πληροφορίες και να στείλει αυτόματα χρήματα σε άλλους λογαριασμούς [1]. Στην πράξη, όταν όλοι οι κόμβοι εξόρυξης κάνουν εξόρυξη τα νέα μπλοκ, εκτελούν το έξυπνο συμβόλαιο ταυτόχρονα [1]. Συχνά, ο χρήστης που δημοσιεύει μια συναλλαγή σε ένα έξυπνο συμβόλαιο, θα πρέπει να πληρώσει για το κόστος της εκτέλεσης κώδικα και επιπλέον των τελών συναλλαγής [1]. Υπάρχει ένα όριο για το πόσο χρόνο εκτέλεσης μπορεί να καταναλωθεί από μια κλήση σε ένα έξυπνο συμβόλαιο [20]. Σε περίπτωση υπέρβασης αυτού του ορίου, η εκτέλεση διακόπτεται και η συναλλαγή απορρίπτεται. Αυτός ο μηχανισμός όχι μόνο επιβραβεύει τους "miners" για την εκτέλεση του κώδικα του έξυπνου συμβολαίου, αλλά επίσης αποτρέπει τους κακόβουλους χρήστες να εισχωρήσουν στα έξυπνα συμβόλαια και να προκαλέσουν την άρνηση εξυπηρέτησης στους κόμβους εξόρυξης [1].

Τα έξυπνα συμβόλαια δεν μπορούν να εκτελεστούν από μόνα τους ή να τρέχουν στο υπόβαθρο. Οι συναλλαγές είναι *atomic*, ασχέτως με τα συμβόλαια που καλούν. Οι συναλλαγές εκτελούνται στο σύνολο τους και μεταβάλλουν την παγκόσμια κατάσταση μόνο όταν εκτελούνται επιτυχώς. Σε αντίθετη περίπτωση, η παγκόσμια κατάσταση δεν επηρεάζεται και το έξυπνο συμβόλαιο επιστρέφει στην προηγούμενη κατάσταση του [18].

Σε ένα DApp, τα έξυπνα συμβόλαια χρησιμοποιούνται για την αποθήκευση της επιχειρησιακής λογικής (κώδικα προγράμματος). Ένα έξυπνο συμβόλαιο, πρακτικά, αντικαθιστά ένα server-side στοιχείο σε μια κεντροποιημένη εφαρμογή [18]. Μία από τις κύριες διαφορές είναι ότι κάθε υπολογισμός που εκτελείται σε ένα έξυπνο συμβόλαιο είναι πολύ ακριβός και πρέπει να διατηρείται όσο το δυνατόν μικρότερος. Επομένως, είναι σημαντικό να προσδιοριστούν οι πτυχές της εφαρμογής που χρειάζονται μια αξιόπιστη και αποκεντρωμένη πλατφόρμα εκτέλεσης [40]. Το Ethereum επιτρέπει τη δημιουργία αρχιτεκτονικών μέσα από τα έξυπνα συμβόλαια, τα οποία δημιουργούν ένα δίκτυο μεταξύ τους, διαβάζοντας και γράφοντας τις δικές τους μεταβλητές, με την πολυπλοκότητα τους να περιορίζεται μόνο από το όριο του αερίου (gas-limit) [18] [40]. Μπορεί να αυτοκαταστραφεί ένα έξυπνο συμβόλαιο εάν έχει προγραμματιστεί με ένα opcode, SELFDESTRUCT, αλλά εκτός από την πλήρη κατάργηση, ο κώδικας δεν μπορεί να αλλάξει με οποιονδήποτε τρόπο [18]. Ένα ακόμα σημαντικό μειονέκτημα των έξυπνων συμβολαίων είναι το μέγεθος των αποκεντρωμένων εφαρμογών. Ένα πολύ μεγάλο έξυπνο συμβόλαιο μπορεί να κοστίσει πολύ αέριο για την ανάπτυξη και τη χρήση του [18]. Επομένως, ορισμένες εφαρμογές ενδέχεται να διαθέτουν μια υπολογιστική διαδικασία εκτός αλυσίδας καθώς και εξωτερική αποθήκευση δεδομένων εκτός αλυσίδας.

ERC20 Για την εφαρμογή μας επιλέξαμε το έξυπνο συμβόλαιο του ERC20 token που είναι δημόσιο [49]. Η λειτουργία του βασίζεται στην δημιουργία ενός πλήθους «ψευδό-κρυπτονομισμάτων» που ανήκουν και διαχειρίζονται από αυτόν που ανέπτυξε το έξυπνο συμβόλαιο και λειτουργούν όπως ένα κοινό κρυπτονόμισμα. Τα νομίσματα αυτά δημιουργούνται μια φορά και δεν μπορούν να ξανά παραχθούν ή να μεταφερθούν χωρίς την έγκριση του δημιουργού. Όλες οι συναλλαγές των νομισμάτων είναι αλληλένδετες με την διεύθυνση του συμβολαίου, δηλαδή η λίστα των συναλλαγών που έχουν πραγματοποιηθεί με αυτό το token εμφανίζεται στην διεύθυνση του συμβολαίου. Έτσι, υπάρχει η δυνατότητα επαλήθευσης της μεταφοράς μεταξύ της διεύθυνσης του αποστολέα και του παραλήπτη, δηλαδή υπάρχει διαφάνεια στις συναλλαγές. Τελικά, το ποσό των token που στέλνετε κάθε φορά στον παραλήπτη, αφαιρείται από το υπόλοιπο του αποστολέα και υπάρχει διαφάνεια στο υπόλοιπο τους.

5.7.1 Αποθήκευση δεδομένων

Λόγω του υψηλού κόστους αερίου και του χαμηλού ορίου αερίου μπλοκ, τα έξυπνα συμβόλαια δεν είναι κατάλληλα για την αποθήκευση ή την επεξεργασία μεγάλου όγκου δεδομένων. Ως εκ τούτου, οι περισσότερες αποκεντρωμένες εφαρμογές αποθηκεύουν τα ογκώδη δεδομένα από την αλυσίδα του Ethereum σε μια δομή αποθήκευσης δεδομένων [18]. Αυτή η δομή μπορεί να είναι κεντροποιημένη (για παράδειγμα, μια τυπική βάση δεδομένων) ή τα δεδομένα αυτά μπορούν να είναι αποκεντρωμένα δηλαδή, αποθηκευμένα σε μια πλατφόρμα P2P όπως [18]:

- Η IPFS. Το Inter-Planetary File System -IPFS είναι ένα αποκεντρωμένο σύστημα αποθήκευσης με διευθυνσιοδότηση περιεχομένου (δηλαδή κάθε αντικείμενο του περιεχομένου είναι κρυπτογραφημένο με συνάρτηση διασποράς) που διανέμει τα αποθηκευμένα αντικείμενα μεταξύ των χρηστών σε ένα δίκτυο peer-to-peer. Η ανάκτηση οποιοδήποτε αρχείου από οποιονδήποτε κόμβο IPFS γίνεται μέσω του κλειδιού τους. Το IPFS στοχεύει στην αντικατάσταση του HTTP ως το πρωτόκολλο επιλογής για την παράδοση εφαρμογών ιστού. Αντί να αποθηκεύει μια εφαρμογή ιστού σε ένα μόνο διακομιστή, τα αρχεία αποθηκεύονται σε IPFS και μπορούν να ανακτηθούν από οποιονδήποτε κόμβο IPFS.

- Η πλατφόρμα Swarm. Η Swarm δημιουργήθηκε από το Ίδρυμα Ethereum, ως μέρος της πλατφόρμας εργαλείων Go-Ethereum. Όπως και το IPFS, έτσι και εδώ η πρόσβαση σε οποιοδήποτε αρχείο Swarm γίνεται με την απλή αναφορά σε αυτό μέσω ενός κλειδιού διασποράς. Το Swarm επιτρέπει την πρόσβαση σε έναν ιστότοπο από ένα αποκεντρωμένο σύστημα P2P, αντί ενός κεντρικού διακομιστή ιστού.

Η αποκεντρωμένη αποθήκευση P2P είναι ιδανική για την αποθήκευση και τη διανομή μεγάλων στατικών στοιχείων, όπως εικόνων, βίντεο και των πόρων της διεπαφής ιστού της

εφαρμογής. Επίσης η επικοινωνία μεταξύ των διαδικασιών μιας αποκεντρωμένης εφαρμογής γίνεται μέσω του εργαλείου Whisper που ανήκει στην πλατφόρμα εργαλείων Go-Ethereum.

5.8 Απεκοντρωμένες εφαρμογές - dApp

Ένα dApp είναι μια εφαρμογή που είναι ως επί το πλείστον ή εξ ολοκλήρου αποκεντρωμένη. Πιθανές πτυχές μιας εφαρμογής που μπορεί να είναι αποκεντρωμένες [40]:

- Το Backend (συστήμα υποστήριξης).
- Το Frontend (διεπαφή χρήστη).
- Η Αποθήκευση δεδομένων.
- Οι επικοινωνίες των μηνυμάτων.

Καθένα από αυτά μπορεί να είναι κάπως κεντροποιημένο ή κάπως αποκεντρωμένο. Για παράδειγμα, ένα frontend μπορεί να αναπτυχθεί ως εφαρμογή ιστού που εκτελείται σε κεντρικό διακομιστή ή ως εφαρμογή για κινητά που εκτελείται σε μια συσκευή [18]. Το backend και η αποθήκευση δεδομένων μπορούν να βρίσκονται σε ιδιωτικούς διακομιστές και βάσεις δεδομένων ή αντίθετα, μπορεί να χρησιμοποιηθεί ένα έξυπνο συμβόλαιο και αποθήκευση να γίνεται σε ένα δίκτυο P2P [18]. Υπάρχουν πολλά πλεονεκτήματα στη δημιουργία ενός dApp που μια τυπική κεντροποιημένη αρχιτεκτονική δεν μπορεί να προσφέρει [18]:

1. Ανθεκτικότητα. Επειδή η επιχειρησιακή λογική ελέγχεται από ένα έξυπνο συμβόλαιο, το backend του dApp θα είναι πλήρως κατανεμημένο και θα λειτουργεί πάνω σε μια πλατφόρμα blockchain, οπότε η εφαρμογή θα είναι πάντα διαθέσιμη. Σε αντίθετη περίπτωση μια εφαρμογή dApp που αναπτύσσεται σε έναν κεντροποιημένο διακομιστή, θα συνεχίσει να είναι διαθέσιμη όσο η πλατφόρμα είναι σε λειτουργία.

2. Διαφάνεια. Ο on-chain χαρακτήρας ενός dApp επιτρέπει σε όλους να επιθεωρήσουν τον κώδικα και να είναι πιο σίγουροι για τη λειτουργία του. Οποιαδήποτε αλληλεπίδραση με το dApp θα αποθηκευτεί για πάντα στο blockchain.

3. Αντίσταση στην λογοκρισία. Όσο ένας χρήστης έχει πρόσβαση σε έναν κόμβο Ethereum, τόσο αυτός θα είναι σε θέση να αλληλεπιδράσει με ένα dApp χωρίς παρεμβολές από οποιοδήποτε κεντρικό έλεγχο. Κανένας πάροχος υπηρεσιών, ούτε καν ο ιδιοκτήτης του έξυπνου συμβολαίου, μπορεί να αλλάξει τον κώδικα μόλις δημοσιευθεί στο δίκτυο.

Στο οικοσύστημα Ethereum όπως υπάρχει σήμερα, υπάρχουν πολύ λίγες πραγματικά αποκεντρωμένες εφαρμογές καθώς, οι περισσότεροι εξακολουθούν να βασίζονται σε κεντροποιημένες υπηρεσίες και διακομιστές για κάποιο μέρος της λειτουργίας τους [18].

5.8.1 Εργαλεία για την δημιουργία Έξυπνου Συμβολαίου

Geth

Το Go Ethereum είναι μία από τις τρεις πρωτότυπες υλοποιήσεις-πελάτη (μαζί με C ++ και Python) του Ethereum. Είναι γραμμένο σε Go, πλήρως ανοικτού κώδικα και έχει άδεια χρήσης υπό το GNU LGPL v3 [50].

MetaMask

Το MetaMask είναι ένα ψηφιακό πορτοφόλι και λειτουργεί ως προέκταση στο πρόγραμμα περιήγησης στο διαδίκτυο (Chrome, Firefox, Opera, Brave Browser). Δηλαδή είναι απαραίτητη η ύπαρξη ενός ψηφιακού πορτοφολιού και το MetaMask είναι το πιο φιλικό για τον χρήστη. Είναι εύκολο στη χρήση και βολικό για δοκιμές, καθώς είναι σε θέση να συνδεθεί με διάφορους κόμβους του Ethereum και δοκιμαστικά blockchain. Το MetaMask είναι ένα ψηφιακό πορτοφόλι, που απαιτεί τον χρήστη να δημιουργήσει σε αυτό έναν λογαριασμό. Από την στιγμή που δημιουργήσει έναν λογαριασμό στο MetaMask ή εισάγει έναν παλιό λογαριασμό που διατηρεί σε αυτό, μπορεί να συνδεθεί με μια αποκεντρωμένη εφαρμογή, εφόσον αποδεχτεί το μήνυμα σύνδεσης και πρόσβασης στο αναδυόμενο παράθυρο από το MetaMask, κατά την είσοδο του στην εφαρμογή αυτή. Η δημιουργία λογαριασμού στο MetaMask είναι αρκετά απλή. Ο χρήστης δημιουργεί το δικό του κωδικό πρόσβασης και θα πρέπει να αποθηκεύσει σε ασφαλές σημείο την φράση "σπόρο", η οποία δίνεται για λόγους ασφαλείας και μόνο με αυτόν μπορεί να επαναφέρει τον λογαριασμό του. Η διεπαφή του MetaMask επιτρέπει στον χρήστη την εναλλαγή των Ethereum δικτύων και όχι μόνο. Μπορεί να συνδεθεί στο κεντρικό δίκτυο, σε τοπικό δίκτυο ή σε δίκτυο δοκιμών. Το MetaMask είναι υπεύθυνο μόνο για την διαχείριση των λογαριασμών του στο Ethereum, η σύνδεση με τους κόμβους του δικτύου γίνεται μέσω της εφαρμογής Infura, η οποία εκτελείται στο σύστημα υποστήριξης του το MetaMask και ο χρήστης δεν ασχολείται ποτέ με αυτήν την εφαρμογή [51].

Γλώσσες προγραμματισμού

Στο σύστημα υποστήριξης

- Serpent. Αυτή είναι μια απλή και καθαρή γλώσσα τύπου Python. Δεν χρησιμοποιείται πλέον για την ανάπτυξη συμβάσεων και δεν υποστηρίζεται πλέον από την κοινότητα [18].

- Solidity. Κατασκευάστηκε από τον Dr. Gavin Wood. Αυτή η γλώσσα έχει πλέον γίνει σχεδόν πρότυπο για τη συγγραφή έξυπνων συμβολαίων για το Ethereum. Ουσιαστικά είναι μια διαδικαστική γλώσσα προγραμματισμού με σύνταξη που είναι παρόμοια με JavaScript, C++ ή Java [40] [18]. Πρόκειται για μια στατικά πληκτρολογούμενη

γλώσσα, πράγμα που σημαίνει ότι ο έλεγχος των μεταβλητών στη Solidity διεξάγεται κατά το χρόνο σύνταξης [18]. Κάθε μεταβλητή, είτε η κατάσταση είτε η τοπική, πρέπει να προσδιορίζεται με έναν τύπο στο χρόνο σύνταξης. Αυτό είναι επωφελές καθώς επικύρωση και έλεγχος του συμβολαίου ολοκληρώνεται κατά τον χρόνο σύνταξης του, και ορισμένοι τύποι σφαλμάτων, μπορούν να αντιμετωπιστούν νωρίτερα,δηλαδή κατά την ανάπτυξη του συμβολαίου αντί στο χρόνο εκτέλεσης του, το οποίο είναι δαπανηρό [18]. Άλλα χαρακτηριστικά της γλώσσας είναι η κληρονομικότητα, οι βιβλιοθήκες και η δυνατότητα ορισμού σύνθετων τύπων δεδομένων. Η Solidity είναι συμβολαιοστρεφές γλώσσα προγραμματισμού,τα συμβόλαια είναι ισοδύναμα με την έννοια των τάξεων σε άλλες αντικειμενοστρεφείς γλώσσες προγραμματισμού [18].

- Vyper. Αυτή η γλώσσα είναι μια πειραματική γλώσσα τύπου Python που αναπτύσσεται με επίκεντρο την ασφάλεια, την απλότητα και την ελεγκτικότητα στην ανάπτυξη των έξυπνων συμβολαίων [18].

Στη διεπαφή με τον χρήστη Η διεπαφή με τον χρήστη μπορεί να γίνει με οποιαδήποτε ευρέως γνωστή γλώσσα προγραμματισμού που χρησιμοποιείται για να δημιουργηθεί μια ιστοσελίδα, όπως για παράδειγμα η Django (Python), HTML,CSS (Bootstrap), Javascript (Jquery, VueJS, Angular, Js-React,Gatsby), PHP, C# και πολλά ακόμα εργαλεία. Όμως για μπορέσει η διαδικτυακή εφαρμογή να επικοινωνεί με το Ethereum, πρέπει να προστεθεί σε αυτήν μία βιβλιοθήκη της Javascript δηλαδή, η βιβλιοθήκη Web3, καθώς και οι απαραίτητες συναρτήσεις που προσφέρει η συγκεκριμένη βιβλιοθήκη. Η συντριπτική πλειοψηφία των λειτουργιών που σχετίζονται με το πορτοφόλι και το κόμβο παρέχονται από το αντικείμενο web3, το οποίο έχει σχέση με την βιβλιοθήκη web3.js. Ουσιαστικά, η βιβλιοθήκη web3.js είναι μια συλλογή από συγκεκριμένες λειτουργίες για το Ethereum. Λειτουργεί ως ένα API της JavaScript το οποίο είναι συμβατό με το Ethereum και επικοινωνεί με τους χρήστες μέσω ενός JSON-RPC. Το JSON-RPC είναι πρωτόκολλο κλήσης απλής διαδικασίας, ελαφρού βάρους (light-weight RPC). Κατά κύριο λόγο αυτή η λεπτομέρεια ορίζει διάφορες δομές δεδομένων και τους κανόνες της επεξεργασίας τους. Είναι ένας αγνωστικός τρόπος μεταφοράς, καθώς μπορεί να χρησιμοποιηθεί είτε μέσα στην ίδια διαδικασία, είτε πάνω από τους υποδοχείς sockets,είτε μέσω του HTTP [18].

Μεταγλωττιστές

Οι μεταγλωττιστές χρησιμοποιούνται για τη μετατροπή πηγαίου κώδικα υψηλού επιπέδου έξυπνου συμβολαίου στη μορφή που να μπορεί να το αντιληφθεί το περιβάλλον εκτέλεσης του Ethereum. Υπάρχει ο solc μεταγλωττιστής ο οποίος μετατρέπει την solidity από μια γλώσσα υψηλού επιπέδου σε bytecode Virtual Machine (EVM). Ο solc αφορά κυρίως linux και macos συστήματα [18]. Υπάρχει όμως και ένας μεταγλωττιστής ο οποίος βρίσκεται στο διαδίκτυο και δεν χρειάζεται να εγκατασταθεί τοπικά στον υπολογιστή, και αυτό είναι το

Remix [18]. Το Remix είναι ένα ισχυρό εργαλείο ανοιχτού κώδικα που βοηθάει στην γραφή των έξυπνων συμβολαίων σε Solidity, απευθείας από το πρόγραμμα περιήγησης. Ο πηγαίος κώδικας του Remix είναι γραμμένος σε κώδικα JavaScript. Το Remix υποστηρίζει επίσης δοκιμές, εντοπισμό σφαλμάτων και ανάπτυξη έξυπνων συμβολαίων[1]. Πρόκειται για ένα IDE πλούσιο σε δυνατότητες το οποίο δεν χρειάζεται να χρησιμοποιεί την δημόσια έκδοση του blockchain [18]. Το Remix διαθέτει διάφορες λειτουργίες, όπως η αλληλεπίδραση των συναλλαγών, οι επιλογές σύνδεσης με το JavaScript VM, η διαμόρφωση του περιβάλλοντος εκτέλεσης, τον εντοπισμό των σφαλμάτων που προκύπτουν από τα έξυπνα συμβόλαια, η τυπική επαλήθευση και η ανάλυση [18]. Μπορεί να ρυθμιστεί έτσι ώστε να συνδέεται με τα περιβάλλοντα εκτέλεσης όπως το JavaScript VM, το injected Web3 και το MetaMask πορτοφόλι [18]. Το Remix διαθέτει επίσης ένα εργαλείο εντοπισμού σφαλμάτων για το EVM, το οποίο είναι ένα πολύ ισχυρό εργαλείο και μπορεί να χρησιμοποιηθεί για να εκτελέσει λεπτομερή ανίχνευση και ανάλυση στο bytecode EVM [18].

Περιβάλλον δοκιμών

Για να μπορέσει ένας προγραμματιστής να δοκιμάσει τα έξυπνα συμβόλαια του ότι δουλεύουν σωστά όπως ακριβώς θέλει, θα πρέπει να τα δοκιμάσει να τα εκτελέσει στο δίκτυο του blockchain. Όμως, επειδή η εκτέλεση κάθε συναλλαγής στην κύρια αλυσίδα κοστίζει, για αυτόν τον λόγο δημιουργήθηκαν αρκετές παράλληλες αλυσίδες, οι οποίες απευθύνονται μόνο σε προγραμματιστές. Ουσιαστικά σε αυτές τις παράλληλες αλυσίδες μπορεί ο οποιοσδήποτε να εκτελέσει τα έξυπνα συμβόλαια του όπως ακριβώς γίνεται και στο κυρίος δίκτυο, μόνο που σε αυτήν την περίπτωση δεν υπόκειται ο προγραμματιστής σε καμία οικονομική επιβάρυνση μιας και χρησιμοποιεί ψευδο νομίσματα που του τα προσφέρει το εκάστοτε δίκτυο. Υπάρχουν αρκετά δίκτυα για την επίτευξει δοκιμών, μερικά από αυτά είναι το Ropsten, το Rinkeby και το Kovan. Το πιο γνωστό από όλα είναι το Ropsten, το οποίο χρησιμοποιούν οι περισσότεροι προγραμματιστές. Το Metamask υποστηρίζει και τα τρία προαναφερθείσα δίκτυα.

Truffle - Ganache

Το Truffleείναι ένα περιβάλλον ανάπτυξης εφαρμογών που διευκολύνει και απλοποιεί τη δοκιμή και την ανάπτυξη των έξυπνων συμβολαίων στο Ethereum [40]. Το Truffle προσφέρει την μεταγλώττιση των συμβολαίων και τη σύνδεση τους με ένα αυτοματοποιημένο περιβάλλον που επιτρέπονται οι δοκιμές των συμβολαίων, χρησιμοποιώντας τις δομές Mocha και το Chai. Επίσης διευκολύνει την ανάπτυξη των συμβολαίων σε οποιοδήποτε ιδιωτικο,δημόσιο, δίκτυο δοκιμής Ethereum [40]. Αυτές οι δοκιμές εκτελούνται σε συνδυασμό με το Ganache [18]. Το Ganacheείναι ένα τοπικό δοκιμαστικό blockchain που μπορεί να χρησιμοποιηθεί για την ανάπτυξη έξυπνων συμβολαίων. Διατίθεται ως εφαρμογή με γραφικό περιβάλλον για τον χρήστη, το οποίο λειτουργεί σε όλα τα λειτουργικά συστήματα (Windows, macOS, Linux

[1]πηγή: remix-ide.readthedocs.io/en/latest/

αλλά και ως πρόγραμμα γραμμής εντολών) [18]. Το Ganacheείναι η τελευταία προσθήκη στην πληθώρα εργαλείων και βιβλιοθηκών που αναπτύχθηκαν για το Ethereum. Το Ganache είναι φτιαγμένο με JavaScript του Ethereum blockchain, με ενσωματωμένο εξερευνητή μπλοκ και εξόρυξη, κάνοντας τη δοκιμή τοπικά στο σύστημα, πολύ εύκολη [18].

5.8.2 Αέριο - (Gas)

Το αέριο είναι η μονάδα του Ethereum, το οποίο χρησιμεύει στην μέτρηση των πόρων υπολογιστικής και αποθήκευσης, που απαιτούνται για την εκτέλεση ενεργειών στο μπλοκ του Ethereum, μέσω των έξυπνων συμβολαίων [18]. Κάθε πράξη που εκτελείται από ένα έξυπνο συμβόλαιο κοστίζει μια καθορισμένη ποσότητα αερίου για παράδειγμα: [18]

- Η προσθήκη δύο αριθμών κοστίζει 3 gas.
- Ο υπολογισμός μιας συνάρτησης διασποράς Keccak-256 κοστίζει 30 gas + 6 gas για κάθε 256 bits δεδομένων που έχουν παραχθεί από αυτην την συνάρτηση διασποράς.
- Η αποστολή μιας συναλλαγής κοστίζει 21.000 gas.

Το αέριο είναι ένα συστατικό - πυλώνας του Ethereum και εξυπηρετεί έναν διπλό ρόλο: *i*) ως απόθεμα μεταξύ της (μεταβαλλόμενης) τιμής του Ethereum και της ανταμοιβής προς τους miners για το έργο που επιτελούν και *ii*) ο άλλος ως άμυνα κατά των DOS επιθέσεων των έξυπνων συμβολαίων στο Ethereum [18]. Προκειμένου να αποφευχθεί ένας τυχαίος ή κακόβουλος βρόχος ή άλλη υπολογιστική σπατάλη στο δίκτυο, ο εκκινητής της κάθε συναλλαγής πρέπει να ορίσει ένα όριο στο ποσό είναι διατεθειμένο να πληρώσει [18]. Το σύστημα αερίου αποθαρρύνει έτσι τους εισβολείς από την αποστολή μηνυμάτων "spam", καθώς έτσι πρέπει να πληρώνουν αναλογικά για τους υπολογιστικούς πόρους, το εύρος ζώνης και τους πόρους αποθήκευσης που καταναλώνουν [18]. Κάθε opocode που εκτελείται, έχει και ένα κόστος σε αέριο που, κατά την εκτέλεση, αφαιρείται από το όριο του ποσού που ανέθεσε ο εκκινητής στην αρχή της συναλλαγής. Εάν τελειώσει το αέριο πριν την ολοκλήρωση της συναλλαγής, τότε η συναλλαγή ακυρώνεται, εμφανίζεται το μήνυμα out-of gas exception και το ποσό επιστρέφεται μέσω της EVM εκτός από το κόστος συναλλαγής, το οποίο μετατράπηκε σε λειτουργικά έξοδα των minners [18]. Εάν το EVM φτάσει στο τέλος της εκτέλεσης με επιτυχία, χωρίς να εξαντληθεί το αέριο, το κόστος του gas που καταβάλλεται στον minner ως τέλος συναλλαγής, μετατρέπεται σε Ether με βάση την τιμή αερίου που υπολογίζεται μέσω της εξής συνάρτησης [18]:

$$\text{φόρος του miner} = \text{κόστος gas} * \text{τιμή gas}.$$

Το αέριο που περίσσεψε από την συναλλαγή (ουσιαστικά τα "ρέστα") επιστρέφονται με παρόμοια διαδικασία στον αποστολέα, δηλαδή μετατρέπεται σε Ether με βάση την τιμή του αέριου που ορίστηκε κατα την διαδικασία τη συναλλαγής [18]:

υπόλοιπο αέριο = όριο αερίου - κόστος αερίου επιστρεφόμενος Ether = αέριο που απομένει * την τιμή του.

Κόστος αερίου έναντι της Τιμής αερίου

Το κόστος του αέριου είναι ένα μέτρο για τον υπολογισμό της ισχύος και της αποθήκευσης που χρησιμοποιείται από την EVM, ενώ η τιμή του αέριου μετράται σε Ether [18]. Όταν εκτελείται μια συναλλαγή, ο αποστολέας καθορίζει την τιμή του αερίου που είναι διατεθειμένος να πληρώσει (σε Ether) για κάθε μονάδα αερίου, όπου η αγορά αποφασίζει τη σχέση μεταξύ της τιμής των Ether και του κόστους του υπολογισμού των εργασιών, δηλαδή ισχύει πάντα ότι [18]:

φόρος συναλλαγής = σύνολο αερίου που χρησιμοποιήθηκε * τιμή αερίου που πληρώθηκε (σε Ether).

Οι miners, συνήθως επιλέγουν αυτήν την συναλλαγή που προσφέρει το περισσότερο αέριο, οπότε έχει προτεραιότητα σε σχέση με άλλες συναλλαγές που προσφέρουν λιγότερο αέριο [18]. Στην πράξη, ο αποστολέας μιας συναλλαγής θα ορίσει ένα όριο αέριου το οποίο είναι μεγαλύτερο ή ίσο με την ποσότητα αέριου που αναμένεται να χρησιμοποιηθεί [18]. Αν το όριο είναι υψηλότερο από το ποσό που καταναλώνεται, ο αποστολέας θα λάβει επιστροφή του επιπλέον ποσού, καθώς οι miners πληρώνονται μόνο για την εργασία που πραγματικά εκτελούν. Η διαφορά μεταξύ του κόστους του αέριου και της τιμής του αέριου είναι η εξής [18]:

- Το κόστος αέριου είναι ο αριθμός μονάδων αέριου που απαιτούνται για την εκτέλεση μιας συγκεκριμένης λειτουργίας.
- Η τιμή του αερίου είναι η ποσότητα Ether που είναι διατεθειμένος ο αποστολέας να πληρώσει ανά μονάδα αέριου όταν στέλνει τη συναλλαγή του στο δίκτυο Ethereum [18].
- Το όριο αέριου που χωράει σε ένα Μπλοκ και αυτό αποτελεί τη μέγιστη ποσότητα αέριου που μπορεί να καταναλωθεί από όλες τις συναλλαγές σε αυτό το μπλοκ, περιορίζοντας έτσι το πλήθος των συναλλαγών που μπορούν να χωρέσουν σε ένα μπλοκ [18].

Για παράδειγμα, έστω 5 συναλλαγές των οποίων τα όρια αέριου έχουν οριστεί σε 15.000, 15.000, 20.000, 25.000 και 25.000. Εάν το όριο του μπλοκ αέριου είναι 85.000, τότε οποιεσδήποτε τέσσερις από αυτές τις συναλλαγές μπορούν να χωρέσουν σε ένα μπλοκ, ενώ το πέμπτο θα πρέπει να περιμένει για ένα μελλοντικό μπλοκ,ενώ οι miners αποφασίζουν για το ποιες θα συμπεριληφθούν στο μπλοκ καθώς επίσης ορίζουν δημοκρατικά με συντελεστή ψήφου $0,0976\%$ για το όριο αέριου του κάθε μπλοκ. Εάν ένας miner προσπαθήσει να συμπεριλάβει μια συναλλαγή που απαιτεί περισσότερο αέριο από το τρέχον όριο αέριου του μπλοκ,

το οποίο θα απορριφθεί από το δίκτυο και θα εμφανίσει το μήνυμα σφάλματος transaction exceeds block gas limit [18]. Σύμφωνα με το etherscan.io το όριο αέριου του μπλοκ στο δίκτυο Ethernet είναι 8 εκατομμύρια gas, που σημαίνει ότι περίπου 380 συναλλαγές (κάθε μία που καταναλώνουν 21.000 αέριο) θα μπορούσαν να χωρέσουν σε ένα μπλοκ [18].

5.9 Αποκεντρωμένες εφαρμογές

Πρόσληψη Υπαλλήλων Η εταιρία μπορεί να λάβει εύκολα πολλές πληροφορίες για τον υποψήφιο υπάλληλο σε πολύ λίγα λεπτά από πολλές πήγες και υπηρεσίες όπως είναι το ποινικό μητρώο και όλες οι πληροφορίες θα ήταν αδιαμφισβήτητες [52].

Εφοδιαστική Αλυσίδα Το blockchain επιτρέπει στον οποιονδήποτε να ελέγξει το προϊόν από ποια στάδια πέρασε για να φτάσει στον καταναλωτή επιτρέποντας έτσι να επιβεβαίωση την γνησιότητα και την ποιότητα του προϊόντος και την πάταξη του λαθρεμπορίου μέσω ενός ¨σκαναρίσματος' QR code [52]

Προστασία της Πνευματικής Ιδιοκτησίας Ο ιδιοκτήτης των πνευματικών δικαιωμάτων μπορεί να χρησιμοποιήσει εύκολα ιστοσελίδες όπως είναι το **binded.com** ή το **copytrack.com** για να ανεβάσει το υλικό του (π.χ. φωτογραφίες) και με μια απλή ψηφιακή υπογραφή να καταχωρήσει τα πνευματικά δικαιώματα ενώ μπορεί να παράσχει τη νόμιμη αναπαραγωγή του υλικού σε τρίτους μέσω της επίτευξης κάποιας συμφωνίας [52].

Εντοπισμός Όπλων Το blockchain μπορεί να βοηθήσει στον εντοπισμό των όπλων, καθώς αποθηκεύει τις πληροφορίες από την παραγωγή του όπλου μέχρι και την αγορά του από τον τελευταίο πελάτη, και αυτό θα μπορούσε να είναι προσβάσιμο από την αστυνομία και τους πολίτες των όπλων [52]. Υπάρχει ήδη μια εφαρμογή υπό κατασκευή το blocksafe, το οποίο έχει εγκαταστήσει στα νέα όπλα αισθητήρες και ένα αποκεντρωμένο VPN, όπου επιτρέπει στο όπλο να στέλνει και να δέχεται δεδομένα από το blockchain. Το σύστημα μπορεί να εντοπίσει την τοποθεσία του όπλου, αλλά και να λάβει δεδομένα σε πραγματικό χρόνο το που και το πότε και με πια κλήση ακόμα πυροβόλησε το όπλο [52].

Αποθήκευση Προσωπικών Δεδομένων Αντί να υπάρχουν διαφορετικά έγγραφα όπως, η αστυνομική ταυτότητα, το δίπλωμα οδήγησης και Α.Φ.Μ, θα μπορούσε να υπάρχει μια ψηφιακή ταυτότητα με την τεχνολογία του blockchain για να αντικαταστήσει [52]. Έτσι, ο πραγματικός ιδιοκτήτης μπορεί να έχει πρόσβαση σε αυτά τα δεδομένα μέσα από βιομετρική ανάλυση των χαρακτηριστικών του, οπότε στην περίπτωση μιας θεομηνίας ή καταστροφής, τα στοιχεία του θα παραμείνουν ασφαλή [52].

Παιχνίδια

Play2win

Πρόκειται για μια εικονική χαρτοπαικτική λέσχη που εφαρμόστηκε με ένα έξυπνο συμβόλαιο του Ethereum. Έχει 1000 ενεργούς χρήστες καθημερινά. Οι παίκτες στοιχηματίζουν Ether παίζοντας διάφορα παιχνίδια καζίνο και μπορούν να κερδίσουν ή να χάσουν Ether. Το έξυπνο συμβόλαιο καθορίζει τους νικητές και τους ηττημένους. Σε αυτό το παιχνίδι, στο έξυπνο συμβόλαιο καθορίζεται το σύστημα παραγωγής τυχαίων αριθμών που χρησιμοποιείται για τον προσδιορισμό των νικητών. Ο αλγόριθμος του γεννήτορα τυχαίων αριθμών βασίζεται, στον αριθμό δεδομένων στο μπλοκ, στη σύνοψη του, στον χρόνο επιβεβαίωσης της συναλλαγής και στην τρέχουσα δυσκολία του μπλοκ[2].

0x-Universe

Το 0x-Universe είναι ένα συλλεκτικό παιχνίδι όπου οι παίκτες κατασκευάζουν διαστημόπλοια και αποικίζουν πλανήτες. Έχει 700 ενεργούς χρήστες όλο το 24ώρο. Κάθε πλανήτης είναι ένα ψηφιακό στοιχείο που αποθηκεύεται στο blockchain. Υπάρχει ένας πεπερασμένος αριθμός πλανητών και ο καθένας έχει ένα μοναδικό σχέδιο και προσφέρει διαφορετικούς πόρους. Το παιχνίδι χρεώνει ένα τέλος συναλλαγής 5% κάθε φορά που ένας πλανήτης αγοράζεται ή πωλείται στην αγορά του. Οι πλανήτες είναι τακτική περιουσιακά στοιχεία ERC721 που μπορούν να αγοραστούν και να πωληθούν σε άλλα χρηματιστήρια όπως το Opensea[3]

Υγεία

EDNA

Τα μέλη της EDNA είναι πρακτικά ιδιοκτήτες ενός καταστήματος, με την έννοια ότι, χρησιμοποιούν τις κρυπτογραφικές τεχνολογίες της εταιρείας με σκοπό να ασφαλίσουν τα γενετικά τους δεδομένα στο blockchain και μπορούν να τα πουλήσουν σε όσους ερευνητές θέλουν με αντίτιμο μια αμοιβή. Χρησιμοποιούν δηλαδή, τα έξυπνα συμβόλαια ώστε να μπορούν να μοιράζονται τα δεδομένα τους με τους ερευνητές για αυτό πληρώνονται. Τέλος με την λειτουργία του EDNA διαπράττεται και φιλανθρωπικό έργο με σκοπό την καταπολέμηση του εμπορίου λευκής σαρκός.[4].

HEALTHEREUM

Ο στόχος του HEALTHEREUM είναι να κάνει πιο φιλική για τον χρήστη την εμπειρία του με την ηλεκτρονική υγειονομική περίθαλψη. Η πλατφόρμα εμπλουτίζει τις αλληλεπιδράσεις

[2]περισσότερα εδώ https://playtowin.io/
[3]περισσότερα εδώ 0xuniverse.com/
[4]περισσότερα εδώ edna.life/

παροχέα-ασθενή, διευκολύνει τη συνεχή ανατροφοδότηση, προωθεί την συνεχή δέσμευση των ασθενών και εξουσιοδοτεί την κατοχή των ιατρικών δεδομένων. Η πλατφόρμα διαχείρισης Healthereum Patient Behavior Management είναι ένα εργαλείο επικοινωνίας που προσφέρει στους παρόχους υγειονομικής περίθαλψης ένα μέσο για την επίλυση κρίσιμων προβλημάτων της υγειονομικής περίθαλψης. [5].

Διακυβέρνηση

Marriage On Theblock

Ο στόχος του Marriage On Theblock είναι να μπορέσει να καταργήσει μερικές από τις βασικές λειτουργίες του ληξιαρχείου όπως είναι η δήλωση του γάμου ή η λύση του γάμου. Η καταχώρηση των στοιχείων του γάμου στο blockchain έχει πολλά θετικά, όπως για παράδειγμα, μπορούν οι σύζυγοι να το διαβάσουν το δικαιολογητικό και να πάρουν ένα αντίγραφο μέσα σε λίγα δευτερόλεπτα ακόμα και από την άνεση του σπιτιού. Ακόμα δεν χρειάζεται να περιμένουν στην ουρά του ληξιαρχείου για μία αίτηση, μιας και γίνεται πλέον ηλεκτρονικά και μπορούν να αλλάξουν την κατάσταση του γάμου τους οποιαδήποτε στιγμή το θελήσουν.[6].

Kleros

Το Kleros είναι ένα δικαστικό σύστημα. Τα έξυπνα συμβόλαια πρέπει να ορίσουν τον κριτή ως τον διαιτητή τους. Όταν αυτοί επιλέγουν, οι δημιουργοί συμβολαίων επιλέγουν πόσοι δικαστές και ποιο δικαστήριο θα αποφασίσει τη σύμβασή τους σε περίπτωση εμφάνισης διαφωνίας. Η ιδέα είναι ότι θα επιλέξουν έναν τύπο δικαστηρίου εξειδικευμένο στο θέμα των συμβολαίων. Ένα συμβόλαιο ανάπτυξης λογισμικού θα επιλέξει ένα δικαστήριο ανάπτυξης λογισμικού, ένα ασφαλιστικό συμβόλαιο θα επιλέξει ένα ασφαλιστικό δικαστήριο κλπ. Η ομάδα του Kleros έχει αναπτύξει μια σειρά τυποποιημένων συμβάσεων χρησιμοποιώντας τον Kleros ως μηχανισμό επίλυσης διαφορών[7]

Εκπαίδευση

Disciplina: Blockchain for Education

Το 2018 ιδρύθηκε το Disciplina [53],το οποίο ήταν το πρώτο blockchain που δημιούργησε ένα ενοποιημένο σύστημα για την επαλήθευση ακαδημαϊκών τίτλων αλλά και την οργάνωση των ακαδημαϊκών λειτουργιών. Η ιδέα αποτελείτε από ένα ιδιωτικό και από ένα δημόσιο blockchain δικιάς τους τεχνολογίας. Στο ιδιωτικό blockchain υπάρχουν 2 βασικοί ρόλοι αυτός του Student και αυτός του Educator. Σε αυτό αποθηκεύονται όλες διαδικασίες που εκτελούνται ανάμεσα σε αυτούς τους 2 ρόλους, όπως για παράδειγμα η ανάθεση εργασιών,

[5]περισσότερα εδώ healthereum.com/
[6]περισσότερα εδώ www.marriageontheblock.com/
[7]περισσότερα εδώ kleros.io/en/

οι εβδομαδιαίοι βαθμοί αλλά και ο τελικός βαθμός. Ο Educator μπορεί να είναι είτε ένας καθηγητής είτε και ένα ολόκληρο ακαδημαϊκό ίδρυμα. Επειδή όμως όπως αναφέρετε στο άρθρο των Kuvshinov et al, υπάρχει πιθανότητα τα στοιχεία που θέτει ο Educator στην αλυσίδα να παραβιαστούν, οπότε χρειάζεται και ο τρίτος ρόλος, ο Witnesses ο οποίος, δέχεται ως μεταβλητές τις επικεφαλίδες των συναλλαγών που επιτεύχθηκαν από τον Educator και τις δημοσιεύει στο δημόσιο blockchain. Υπάρχει και ο ρόλος των Recruiters οι οποίοι, είναι οι οντότητες που ενδιαφέρονται να συλλέξουν δεδομένα σχετικά με μαθητές από εκπαιδευτικά ιδρύματα. Αγοράζουν αυτά τα δεδομένα από τους Educators χρησιμοποιώντας ένα ασφαλές πρωτόκολλο αποκάλυψης δεδομένων. Η επαλήθευση των ακαδημαϊκών τίτλων γίνεται χωρίς να χρειάζεται να επέμβει κάποιος από τους παραπάνω ρόλους, αρκεί ο φοιτητής να καταθέσει μερικές πληροφορίες, όπως: το δημόσιο κλειδί του και του Educator, το χ μάθημα και την σύνοψη της συναλλαγής του, το μονοπάτι του Merkle tree της ιδιωτικής συναλλαγής (Ppriv = path(Tpriv, Mpriv)), και τον αριθμό του μπλοκ όπως και το μονοπάτι του Merkle tree της δημόσιας συναλλαγής. Ο συνδυασμός και ο έλεγχος όλων των παραπάνω είναι αρκετά για να επαληθεύσουν ότι η συναλλαγή μεταξύ του Educator και του φοιτητή είναι πραγματική και αληθινή.

Verde

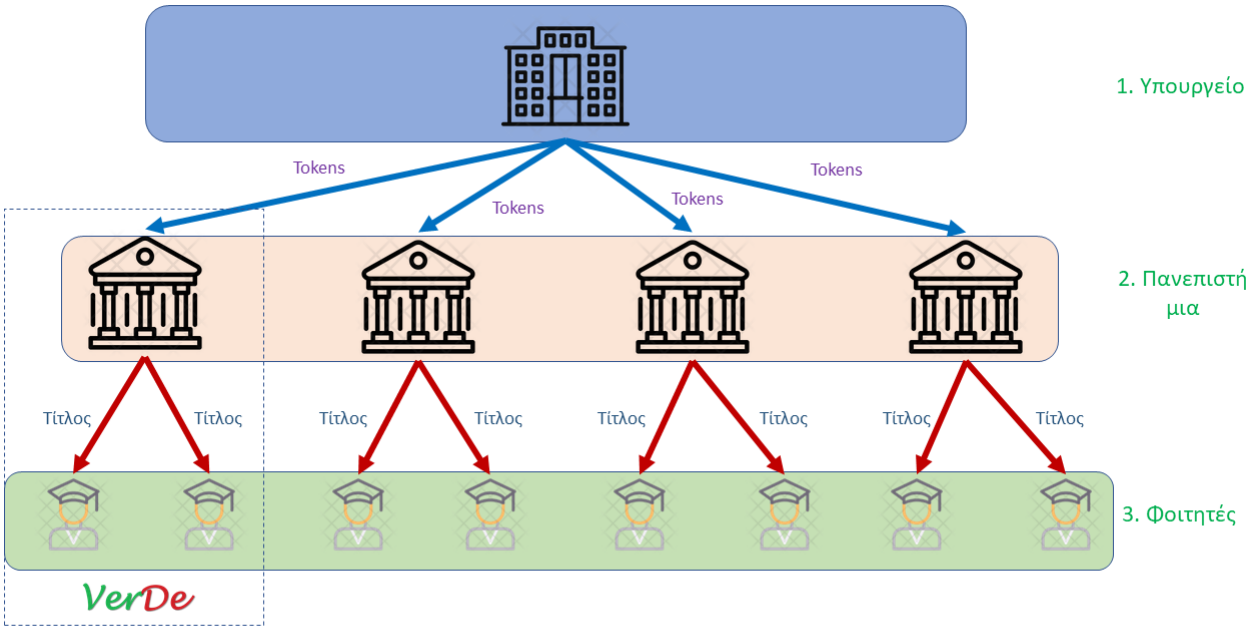
Όπως αναφέρθηκε και σε όλες τις παραπάνω ενότητες, το δυνατότερο σημείο της τεχνολογίας blockchain είναι η φερεγγυότητα και η αυθεντικότητα των συναλλαγών της. Η εφαρμογή Verde χρησιμοποιεί την πλατφόρμα του Ethereum και έχει ως σκοπό την πάταξη της πλαστογραφίας των ακαδημαϊκών τίτλων.

Κεφάλαιο 6

Η αποκεντρωμένη εφαρμογή Verde

Όπως αναφέρθηκε και στην εισαγωγή, αρκετά συχνά τα ειδησεογραφικά πρακτορεία αναφέρουν και από ένα περιστατικό για την ανακάλυψη πλαστών πτυχίων στον δημόσιο τομέα και όχι μόνο. Επειδή τα πλαστά πτυχία είναι ένα συχνό φαινόμενο στην ελληνική επικράτεια, υπάρχει η ανάγκη της αντιμετώπισης αυτής της παράνομης πράξης με τον καλύτερο τρόπο ο οποίος είναι η πρόληψη. Η εφαρμογή Verde είναι ένα μέσο επαλήθευσης για την καταπολέμηση της πλαστογραφίας των πανεπιστημιακών πτυχίων. Κατά την αποφοίτηση του φοιτητή η πανεπιστημιακή μονάδα θα δημοσιεύει του βαθμούς του στο δίκτυο του Ethereum και αυτά τα στέλνει στο ψηφιακό πορτοφόλι του απόφοιτου, έτσι ώστε τα στοιχεία του να μην μπορούν να παραποιηθούν. Με την σειρά, η εταιρεία είτε δημόσια, είτε ιδιωτική, μπορεί εύκολα να επαληθεύσει την εγκυρότητα του πτυχίου του πρώην φοιτητή μιας και όταν η διεύθυνση του ψηφιακού πορτοφολιού του καταχωρηθεί στην διαδικτυακή εφαρμογή του Verde, τότε αυτό αυτόματα εμφανίζει όλα τα στοιχεία και τα μαθήματα του φοιτητή που καταχώρησε η πανεπιστημιακή μονάδα στο blockchain.

Η λογική της λειτουργίας της εφαρμογής Verde φαίνεται στην Εικόνα 6.1, δηλαδή ότι υπάρχουν τρεις οντότητες-επίπεδα, 1) το υπουργείο, 2) τα ακαδημαϊκά ιδρύματα και 3) οι φοιτητές. Το πρώτο επίπεδο είναι υπεύθυνο για την κατανομή των ECTS tokens στα ιδρύματα και αυτά στην συνέχεια να τα μοιράσει στους πτυχιούχους φοιτητές. Αυτό το τρίπτυχο είναι πολύ σημαντικό γιατί, η κεντρική αρχή ορίζει πιο πανεπιστήμιο θα μπορεί να μοιράζει τα ECTS tokens με αποτέλεσμα, να μπορεί το ίδιο να ανακαλέσει τυχόν παραβάσεις του ιδρύματος ή του φοιτητή. Έτσι, όλα τα ECTS tokens έχουν μια κοινή αρχή και έναν που να τα εκδίδει και έτσι επιτυγχάνεται η μέγιστη διασφάλιση της ακεραιότητας των δεδομένων, άρα και της επαλήθευσης τους. Στα πλαίσια της πτυχιακής εργασίας, δεν υλοποιήθηκε αυτή η διαδικασία πλήρως, αλλά η εφαρμογή θα μπορούσε να παρομοιαστεί με μία συναλλαγή μεταξύ του επιπέδου 2 και 3, καθώς έχει σημασία ποιος αναπτύσσει το έξυπνο συμβόλαιο στο blockchain αλλά, αντί για να αναπτύσσει το έξυπνο συμβόλαιο το υπουργείο, το αναπτύσσει το ακαδημαϊκό ίδρυμα. Σε επίπεδο έξυπνων συμβολαίων έχει δημιουργηθεί η συγκεκριμένη λειτουργία, δηλαδή ότι ο ιδρυτής των ECTS tokens επιτρέπει σε έναν άλλον λογαριασμό να χρησιμοποιήσει και να μοιράσει τα tokens που του στέλνει.



Σχήμα 6.1: Τα επίπεδα της εφαρμογής

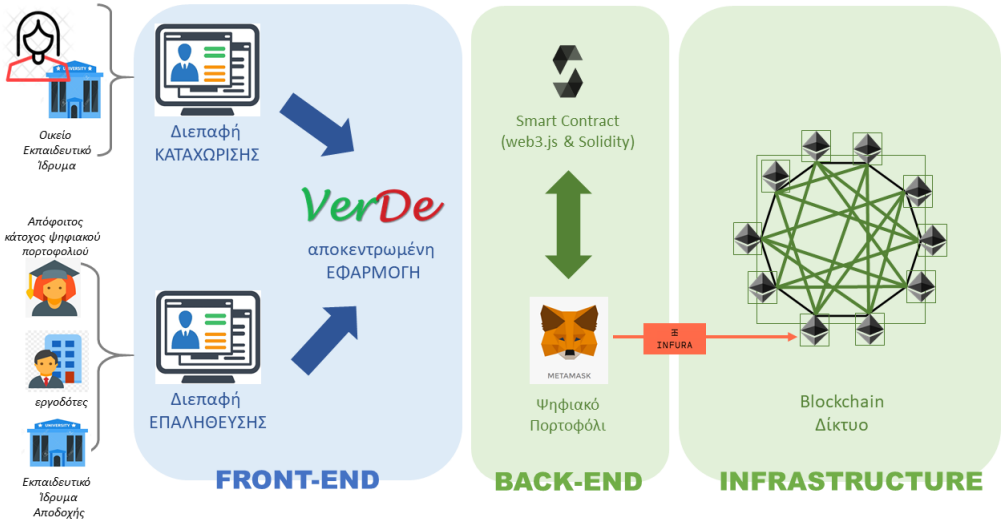
6.1 Η Αρχιτεκτονική της εφαρμογής Verde

Στην παρούσα ενότητα παρουσιάζεται η αρχιτεκτονική της αποκεντρωμένης εφαρμογής Verde. Η συγκεκριμένη εφαρμογή, όπως όλες οι αποκεντρωμένες διαδικτυακές εφαρμογές, αποτελείται από τρία βασικά συστατικά στοιχεία: (α) το συστατικό τη παρουσίασης, (β) το συστατικό του ελέγχου, και (γ) το συστατικό επικοινωνίας με το blockchain. Το πρώτο, αποτελεί την διεπαφή με τον χρήστη 6.2 και διαβάζει τα στοιχεία που του καταχωρεί. Το τρίτο λειτουργεί με την βιβλιοθήκη web3.js και επικοινωνεί με το blockchain του Ethereum [54]. Το συστατικό του ελέγχου ενώνει τα δύο παραπάνω και λειτουργεί ως ο «εγκέφαλος» της εφαρμογής [54]. Ακολουθεί η αναλυτική περιγραφή της προτεινόμενης αρχιτεκτονικής πάνω στην οποία υλοποιήθηκε η εφαρμογή Verde.

6.1.1 Σκοπός της εφαρμογής

Η εφαρμογή Verde βασιζόμενη στην αξιοπιστίας του Ethereum blockchain επαληθεύει τους ακαδημαϊκούς τίτλους χωρίς να χρειάζεται η παρέμβαση της ακαδημαϊκής μονάδας κάθε φορά. Αποτελείται από 2 διεπαφές που είναι το front-end της: 1) τη διεπαφή καταχώρισης των δεδομένων στο Ethereum, και 2) τη διεπαφή επαλήθευσης των δεδομένων, όπως φαίνεται στην, Σχήμα 6.2. Η ύπαρξη 2 διεπαφών έχει ως στόχο την απομόνωση της διεπαφής καταχώρισης την οποία διαχειρίζεται κάθε ακαδημαϊκή μονάδα ξεχωριστά και μοναδικά από τη διεπαφή επαλήθευσης που είναι δημόσια και κατά συνέπεια προσβάσιμη από κάθε ενδιαφερόμενο. Η σύνδεση του back-end με το front-end επιτυγχάνεται μέσω της βιβλιοθήκης

web3.js, που εγκαθίσταται στις διεπαφές και αποτελεί το back-end της εφαρμογής μαζί με το έξυπνο συμβόλαιο, Σχήμα 6.2. Η λειτουργικότητα της εφαρμογής και η ιδιότητα της αποκέντρωσης επιτυγχάνεται πρακτικά με το έξυπνο συμβόλαιο. Όμως, για να επιτευχθεί η σύνδεση με το blockchain, χρειάζεται ένα ψηφιακό πορτοφόλι και η σύνδεση με έναν πλήρη κόμβο του. Το ψηφιακό πορτοφόλι περιλαμβάνει το υπόλοιπο των κεφαλαίων του χρήστη και το κόστος των συναλλαγών αφαιρείται από αυτό («φιλτράρει» τις συναλλαγές) ενώ, ο πλήρης κόμβος (ολόκληρα μπλοκ) ενημερώνεται για τα μπλοκ του blockchain και παράλληλα δημιουργεί νέα. Την επικοινωνία των 2 παραπάνω καλύπτει η εφαρμογή MetaMask που αποτελεί επίσης τμήμα του back-end της εφαρμογής Verde. Το MetaMask αναπτύχθηκε από την εταιρεία ConsenSys και αποτελεί διαδικτυακή εφαρμογή (επέκτασης περιηγητή) ψηφιακού πορτοφολιού. Επίσης, η σύνδεση με τους κόμβους του δικτύου Ethereum γίνεται μέσω της εφαρμογής Infura, η οποία εκτελείται στο back-end του MetaMask. Τέλος η εφαρμογής Verde ακολουθεί την νομοθεσία του GDPR και διαθέτει και λειτουργία ανάκλησης των ακαδημαϊκών τίτλων.



Σχήμα 6.2: Η αφαιρετική δομή της εφαρμογής

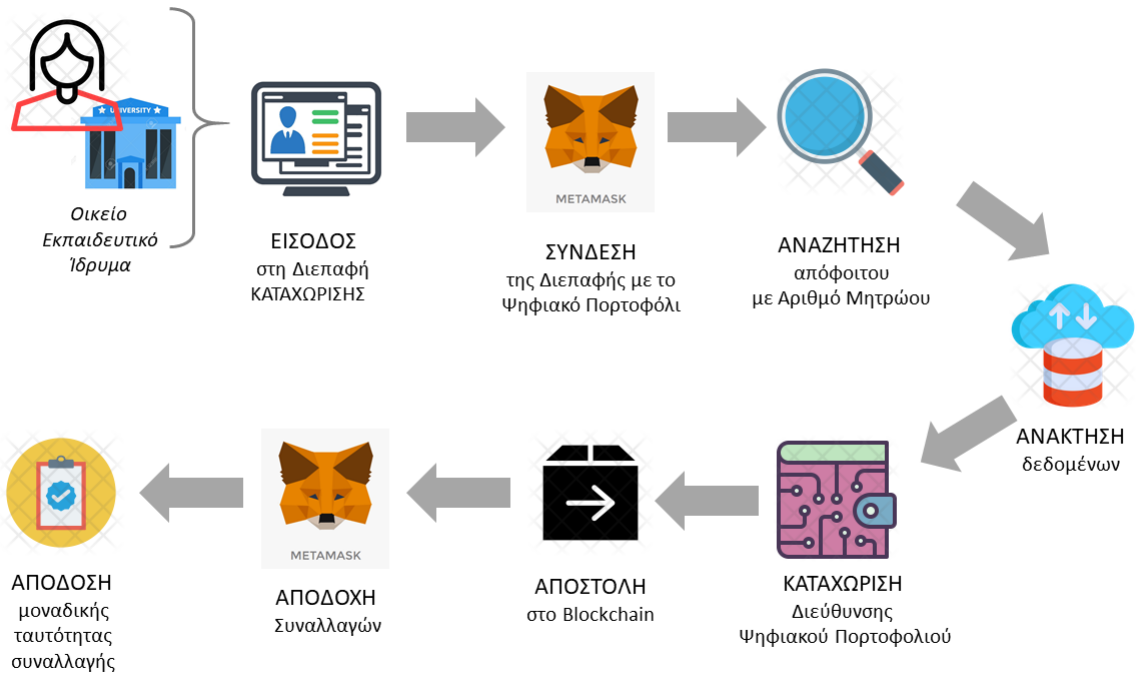
Δημιουργήσαμε την εφαρμογή Verde στο περιβάλλον του Ethereum γιατί, είναι το δεύτερο μεγαλύτερο blockchain δίκτυο αυτήν την στιγμή [55] σε χρηματιστηριακή αξία, σε πλήθος κόμβων και συχνότητα συναλλαγών, ενώ επιπλέον είναι δημόσιο (permissionless), δεν χρειάζεται να δημιουργήσουμε εμείς τους κόμβους και έχει μεγάλη κοινότητα που το υποστηρίζει.

6.1.2 Αρχιτεκτονική της διεπαφής καταχώρισης

Ο σκοπός της διεπαφής καταχώρισης είναι η αποστολή των κρυπτογραφημένων δεδομένων του φοιτητή από την ακαδημαϊκή μονάδα στο δίκτυο του Ethereum προκειμένου αργότερα

να είναι εφικτή η αποκρυπτογράφηση και η επαλήθευση των στοιχείων του ακαδημαϊκού του τίτλου. Τα στοιχεία αυτά περιλαμβάνουν το ονοματεπώνυμο, όνομα πατέρα, μητέρας και την ημερομηνία γέννησης ενός φοιτητή και είναι τα απολύτως απαραίτητα για την ταυτοποίησή του. Επιπλέον, ωστόσο, περιλαμβάνουν τις πληροφορίες του Τμήματος, των μαθημάτων, των πιστωτικών μονάδων (ECTS) και των βαθμολογιών σε κάθε μάθημα. Όλα τα παραπάνω στοιχεία είναι απαραίτητα για την επαλήθευση του ακαδημαϊκού τίτλου και την ταύτιση του με τον φοιτητή. Οπότε, οι λειτουργίες της εφαρμογής Verde πρέπει να έχουν την δυνατότητα να προβάλουν τα παραπάνω στοιχεία για να είναι ο τίτλος επαληθευμένος. Για να μπορέσει όμως να συμβεί η προβολή, θα πρέπει πρώτα να καταχωρηθούν στο blockchain λειτουργία που επιτελείται μέσω της διεπαφής καταχώρισης.

Η μεταφορά στο blockchain γίνεται πάντα μεταξύ ενός αποστολέα και ενός παραλήπτη, δηλαδή μεταξύ των διευθύνσεων του ψηφιακού πορτοφολιού της ακαδημαϊκής μονάδας και του φοιτητή, ενώ το μέσο είναι το Ethereum. Οποιαδήποτε ακαδημαϊκή μονάδα θελήσει να χρησιμοποιήσει την συγκεκριμένη διεπαφή, μπορεί, αρκεί να διαθέτει το δικό της ψηφιακό πορτοφόλι στο Ethereum. Τα βήματα για την πραγματοποίηση της καταχώρησης των στοιχείων και μεταφοράς στο blockchain είναι 8 και φαίνονται στο παρακάτω Σχήμα 6.3.

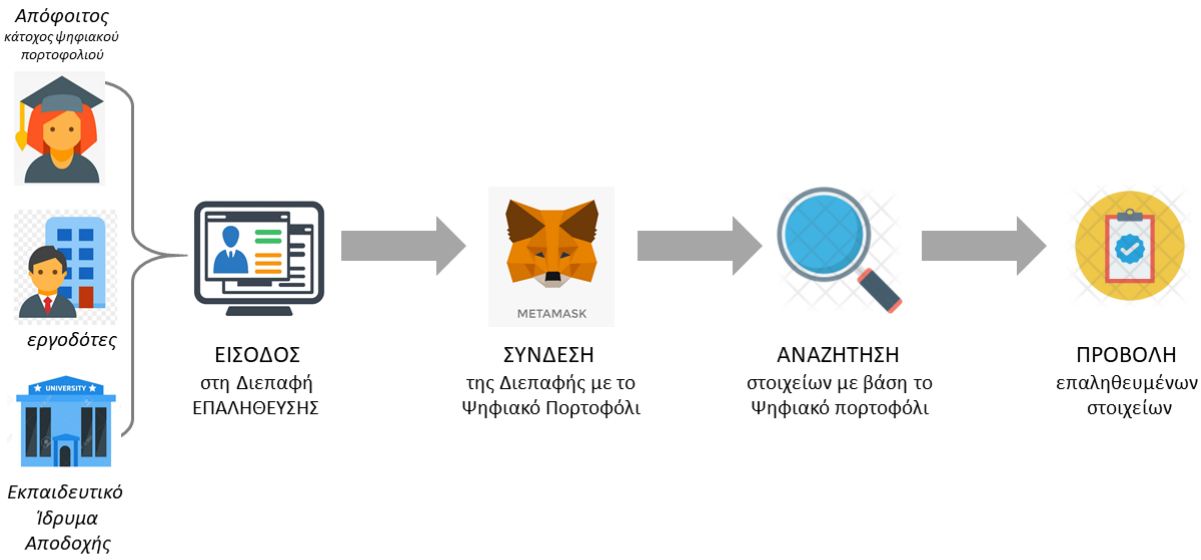


Σχήμα 6.3: Διαδικασία καταχώρισης των στοιχείων του φοιτητή από την οικεία ακαδημαϊκή μονάδα

6.1.3 Αρχιτεκτονική της διεπαφής επαλήθευσης

Η διεπαφή επαλήθευσης είναι επίσης εύχρηστη και απαιτεί μόλις 4 βήματα για να ολοκληρώσει την λειτουργία της 6.4. Βασίζεται στην αναζήτηση της διεύθυνσης του ψηφιακού πορτο-

φολιού του αποφοίτου. Η αναζήτηση ανακτά από το Ethereum, πιο συγκεκριμένα από την κατάσταση του έξυπνου συμβολαίου, τις κρυπτογραφημένες πληροφορίες που σχετίζονται με τον απόφοιτο και στην συνέχεια τις αποκρυπτογραφεί. Πρόκειται για τις πληροφορίες που μετέφερε στο Ethereum η διεπαφή καταχώρισης. Συνεπώς, οι πληροφορίες που επιστρέφονται είναι τα προσωπικά στοιχεία του αποφοίτου και οι πληροφορίες των μαθημάτων που διεκπεραίωσε κατά την διάρκεια των σπουδών του. Από τα παραπάνω αντιλαμβανόμαστε ότι, η διεπαφή αυτή έχει ως σκοπό την επαλήθευση των δεδομένων του ακαδημαϊκού τίτλου, του υποψήφιου εργαζομένου ή μεταπτυχιακού φοιτητή. Με αυτόν τον τρόπο, οι ακαδημαϊκές μονάδες ωφελούνται σε λειτουργικό χρόνο και κόστος, αφού αυτόν τον ρόλο τον ανέλαβε το Ethereum blockchain. Ο λόγος που είναι τόσο ισχυρό αυτό το διαπιστευτήριο είναι γιατί τα δεδομένα στο blockchain δεν μπορούν να αλλοιωθούν.



Σχήμα 6.4: Διαδικασία επαλήθευσης του ακαδημαϊκού τίτλου ενός αποφοίτου

6.1.4 Αρχιτεκτονική του έξυπνου συμβολαίου

Το έξυπνο συμβόλαιο αποτελεί το back-end της αποκεντρωμένης εφαρμογής. Οι χρήστες δεν έρχονται ποτέ σε επαφή με τον κώδικα του έξυπνου συμβολαίου και ούτε αλληλεπιδρούν άμεσα με αυτό. Το συμβόλαιο είναι πολύ σημαντικό για την εφαρμογή γιατί εκτελεί τις λειτουργίες καταχώρισης και επαλήθευσης των ακαδημαϊκών τίτλων. Οι λειτουργίες που χρειάζεται να έχει είναι οι εξής:

- Αποθηκεύει τα κρυπτογραφημένα προσωπικά στοιχεία του φοιτητή στο έξυπνο συμβόλαιο (όνομα, επίθετο, όνομα μητέρας και πατέρα, τόπος καταγωγής, ημερομηνία γέννησης).

- Αποθηκεύει τους βαθμούς, τα κρυπτογραφημένα μαθήματα, τον μέσο όρο και τα ECTS του φοιτητή.
- Δημιουργεί τα «ψευδό-κρυπτονομίσματα» με όνομα ECTS, με σκοπό την αποστολή του πλήθους που συγκέντρωσε ο φοιτητής, κατά την διάρκεια των σπουδών του.
- Επιστρέφει τα κρυπτογραφημένα στοιχεία του φοιτητή.
- Επιστρέφει τους βαθμούς, τα κρυπογραφημένα μαθήματα, τον μέσο όρο και τα ECTS του φοιτητή.
- Χρησιμοποιεί το token ERC20 για την δημιουργία των ECTS. Η εφαρμογή δημιουργεί ένα πλήθος τέτοιων ECTS ενός πολύ μεγάλου αριθμού, όπου το ακέραιο μέρος του είναι ένας 7-ψήφιος αριθμός και το δεκαδικό του μέρος ένας 18-ψήφιος. Η χρήση του έχει ως σκοπό την διπλή επαλήθευση των στοιχείων του φοιτητή, λόγω της διαφάνειας του. Το έξυπνο συμβόλαιο από την στιγμή που αναπτύσσεται στο blockchain δεν μπορεί να αλλάξει. Επομένως, είναι σημαντικό οι λειτουργίες του να είναι αυστηρά καθορισμένες, να γίνουν δοκιμές προς μελέτη όλων των πιθανών περιπτώσεων και να δοθεί μεγάλη προσοχή στην υλοποίηση του.

6.2 Υλοποίηση της εφαρμογής Verde

Σε αυτήν την ενότητα θα εξετάσουμε τις λεπτομέρειες υλοποίησης της εφαρμογής Verde. Οι διεπαφές δημιουργήθηκαν με κώδικα HTML, CSS (Bootstrap), Javascript (Jquerry) και PHP. Το έξυπνο συμβόλαιο είναι γραμμένο στην γλώσσα προγραμματισμού Solidity 0.5.7 και αναπτύχθηκε στο περιβάλλον Remix, στο δίκτυο του Ropsten.

6.2.1 Υλοποίηση της διεπαφής καταχώρισης

Η διεπαφή καταχώρισης[1] είναι εύχρηστη και υλοποιήθηκε με χρήση PHP. Η εφαρμογή χρησιμοποιεί 4 διαφορετικές φόρμες HTML για την συλλογή όλων των στοιχείων εκείνων που απαιτούνται για την επαλήθευση του ακαδημαϊκού τίτλου ενός φοιτητή:

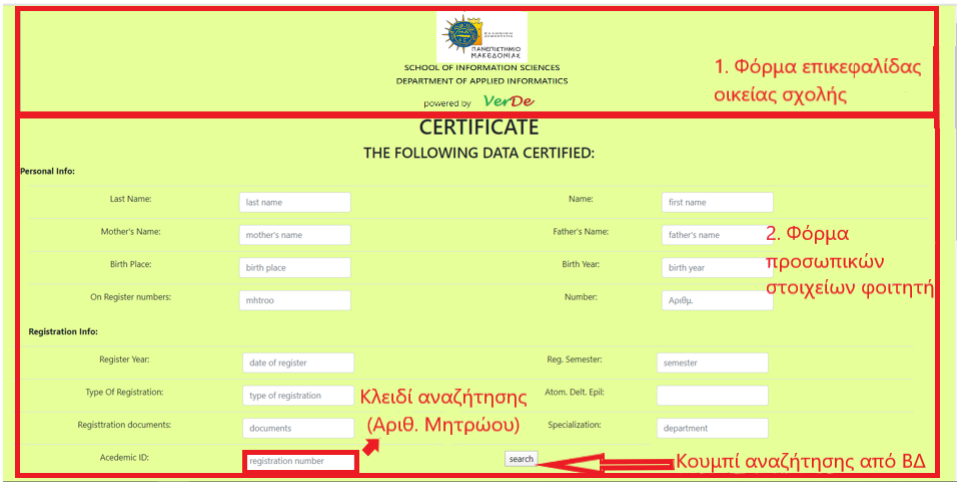
1. Η πρώτη περιέχει το λογότυπο του πανεπιστημίου και τον τίτλο της σχολής Σχήμα 6.5.
2. Η δεύτερη αποτελείται από τα πεδία για την συμπλήρωση των προσωπικών στοιχείων του φοιτητή και την αναζήτηση του φοιτητή στην βάση δεδομένων του πανεπιστημίου. Μόλις ενεργοποιηθεί η αναζήτηση, εκτελείται ένα Mysql αίτημα από τον κώδικα της PHP και επιστρέφει όλα τα στοιχεία του φοιτητή που έχει το συγκεκριμένο αριθμό

[1] η εφαρμογή είναι δημοσιευμένη στην διεύθυνση: https://dry-sierra-28168.herokuapp.com/index.php

μητρώου. Εάν η ανάκτηση είναι επιτυχής τότε, συμπληρώνονται τα πεδία με τα στοιχεία του φοιτητή. Σε αντίθετη περίπτωση η ανάκτηση δεν θα επιστρέψει τίποτα 6.5.

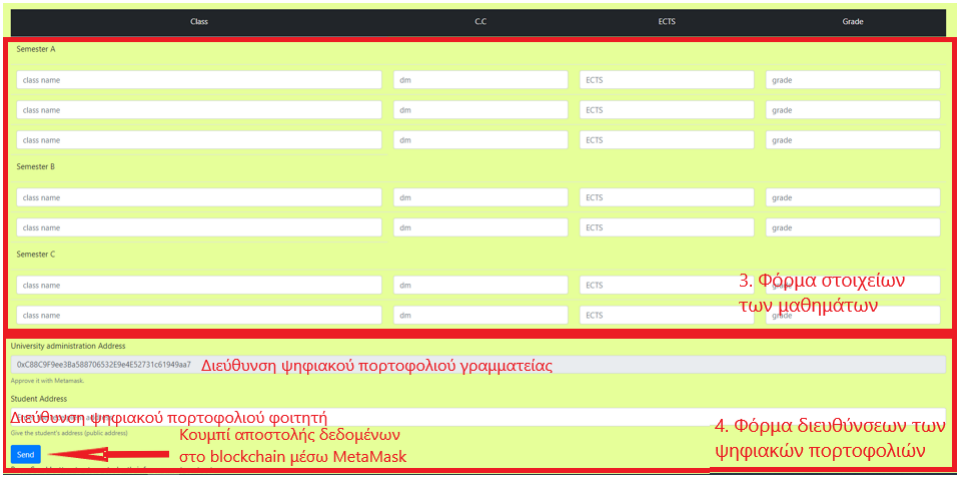
3. Η τρίτη φόρμα περιέχει τον πίνακα με τα μαθήματα που ολοκλήρωσε με επιτυχία ο φοιτητής κατά την διάρκεια των σπουδών του (ονόματα μαθημάτων, διδακτικές μονάδες - ECTS, βαθμολογίες). Τα στοιχεία αυτά ανακτώνται με την αναζήτηση του προηγούμενου βήματος και συμπληρώνονται με την βοήθεια της PHP Σχήμα 6.6.

4. Η τέταρτη περιλαμβάνει τα πεδία συμπλήρωσης των διευθύνσεων των ψηφιακών πορτοφολιών και την αποστολή όλων των δεδομένων στο Ethereum. Η διεύθυνση ψηφιακού πορτοφολιού είναι μοναδική για κάθε Ακαδημαϊκό Ίδρυμα και ως εκ τούτου το αντίστοιχο πεδίο προσυμπληρωμένο, ενώ η διεύθυνση ψηφιακού πορτοφολιού του φοιτητή είναι και πάλι μοναδική αλλά την προσκομίζει ο φοιτητής προκειμένου να γίνει ενημέρωση του πορτοφολιού του με τα στοιχεία του τίτλου που πρόκειται να του αποδοθεί Σχήμα 6.6. Πριν την ολοκλήρωση της αποστολής πρέπει να γίνει δεκτό το κόστος των συναλλαγών από το MetaMask. Με την ολοκλήρωση και τη τελευταίας συναλλαγής εμφανίζεται το μοναδικό αναγνωριστικό της (transaction id) όπως φαίνεται στο Σχήμα 6.7.

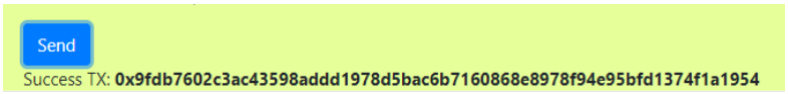


Σχήμα 6.5: Οι φόρμες 1 και 2 της διεπαφής και η λειτουργία ανάκτησης δεδομένων από την ΒΔ

Η αποστολή των δεδομένων στο blockchain υλοποιήθηκε με χρήση της βιβλιοθήκης web3.js. Στο Σχήμα 6.8, περιγράφεται το τμήμα του κώδικα της βιβλιοθήκης web3.js που είναι υπεύθυνο για την αποστολή των προσωπικών στοιχείων στο Ethereum. Ο κώδικας στην πρώτη γραμμή καλεί μία μέθοδο του έξυπνου συμβολαίου με όνομα “setStudent”. Στην πρώτη παρένθεση περιλαμβάνει τα στοιχεία-ορίσματα της μεθόδου αυτής. Η συνάρτηση “.send” μεταφέρει/αποθηκεύει τα δεδομένα στο έξυπνο συμβόλαιο και χρεώνει το κόστος συναλλαγής στην διεύθυνση του αποστολέα (fromAddress). Ο υπόλοιπος κώδικας αφορά την διαχείριση και εμφάνιση των μηνυμάτων επιτυχίας/αποτυχίας της συναλλαγής με το



Σχήμα 6.6: Οι φόρμες 3 και 4 και η λειτουργία αποστολής δεδομένων στο blockchain



Σχήμα 6.7: Η ταυτότητα μιας επιτυχημένης συναλλαγής (transaction id) σε δεκαεξαδική μορφή

Ετηερευμ. Το Σχήμα 6.9 αφορά τον κώδικα της αποστολής των μαθημάτων του φοιτητή στο Ethereum και έχει τον ίδιο τρόπο λειτουργίας με την προηγούμενη μέθοδο.

```
Contract.methods.setStudent(toAddress,lastname,name,fname,mname,birthyear,registeryear,specialization).send({from: fromAddress},
function(error, result) {
 if (error) {
     console.log('error: ' + error);
$('#deposit-result').html('<b>Error: </b>' + error);
 else {
 $('#deposit-result').html('Success TX: <b>' + result + '</b>');
```

Σχήμα 6.8: Αποστολή προσωπικών στοιχείων στο Ethereum

```
Contract.methods.setStudentGrades(toAddress,alldata).send({from: fromAddress},
function(error,result){
    if (error) { console.log('error: ' + error);
            $('#deposit-result').html('<b>Error: </b>' + error);}
    else {  $('#deposit-result').html('Success TX: <b>' + result + '</b>');}
```

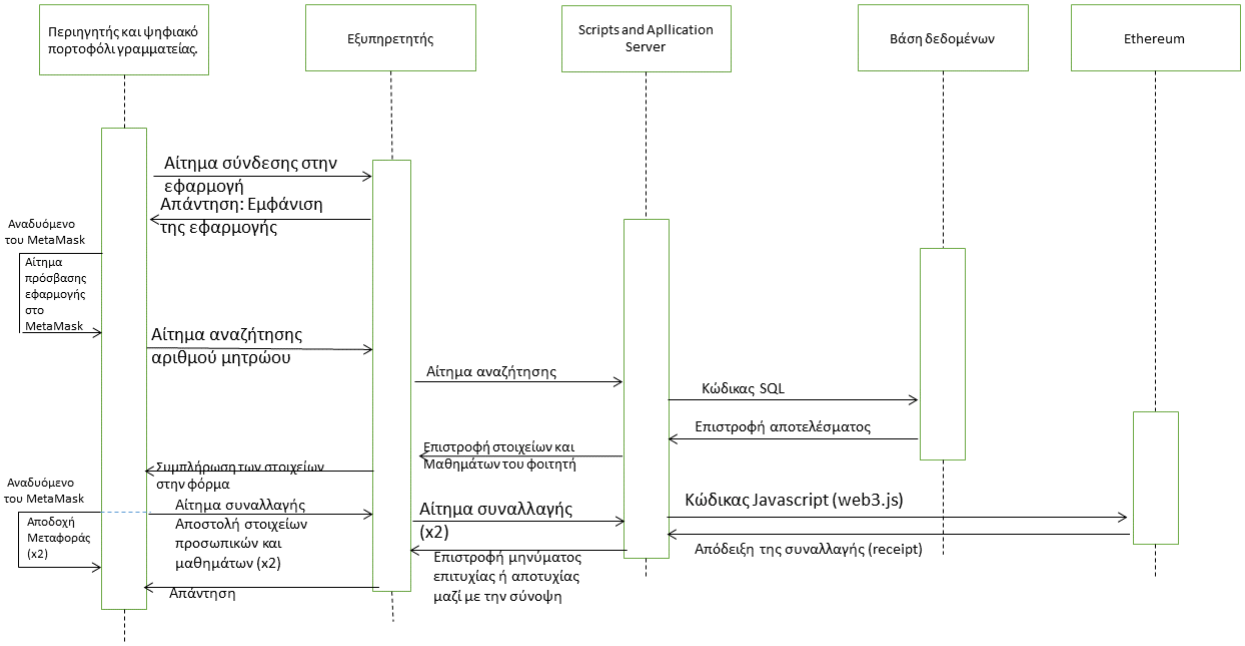
Σχήμα 6.9: Αποστολή των στοιχείων των μαθημάτων που διεκπεραίωσε με επιτυχία ο φοιτητής

Ο κώδικας των παραπάνω εικόνων εκτελείται στην περίπτωση που ενεργοποιηθεί το «Send» του Σχήματος 6.6. Σε αυτήν την περίπτωση, εμφανίζεται το MetaMask με δύο συναλλαγές σε αναμονή. Η κάθε συναλλαγή ζητάει την αποδοχή της απόδοσης του φόρου αποστολής στο Ethereum. Μετά την έγκριση, οι miners στο Ethereum εκτελούν την διαδικασία της εξόρυξης (mining) και στην περίπτωση επιτυχίας, εμφανίζεται στο τέλος της διεπαφής η ταυτότητα της συναλλαγής (Σχήμα 6.7). Η ανάπτυξη του συμβολαίου κοστίζει

περίπου 13$ και η αποθήκευση κάθε φοιτητή 3$ την φορά. Το κόστος αυξομειώνεται ανάλογα τον αριθμό των δεδομένων που αποθηκεύουμε στο Ethereum και την τιμή του Ether την δεδομένη στιγμή και όχι με βάση τον αριθμό των tokens που στέλνονται στους φοιτητές.

Επίσης, χρησιμοποιήθηκε το εργαλείο της Javascript, cryptojs [56], ώστε να κρυπτογραφηθούν τα στοιχεία των φοιτητών (όνομα μαθημάτων και προσωπικά δεδομένα) με τον αλγόριθμο AES το οποίο έχει ως συμμετρικό κλειδί την διεύθυνση του ψηφιακού του πορτοφολιού. Έτσι, επιτυγχάνεται η διεπαφή να ακολουθεί της οδηγίες του GDPR. Βέβαια, αυτό έχει το μειονέκτημα ότι αύξησε το κόστος της συναλλαγής (από 0.3 σε 3 ευρώ) γιατί αυξήθηκαν το πλήθος των ψηφίων που θα αποθηκευτούν στο blockchain.

Οπότε για να αντιληφθούμε καλύτερα την διαδικασία που πραγματοποιείται κατά την διαδικασία λειτουργίας αυτής της διεπαφής αρκεί να παρατηρήσουμε την Εικόνα 6.10, καθώς φαίνεται το διάγραμμα ακολουθίας της διεπαφής.



Σχήμα 6.10: Διάγραμμα ροής της διεπαφής καταχώρησης

6.2.2 Υλοποίηση της διεπαφής επαλήθευσης

Η πρόσβαση και η χρήση της διεπαφής μπορεί να γίνει με την εγκατάσταση του MetaMask στον περιηγητή του χρήστη, αλλά αυτό είναι προαιρετικό μιας και η διεπαφή διαθέτει ένα ειδικό εργαλείο fortmatic.js [57] το οποίο αλληλεπιδρά με το Ethereum και αντικαθιστά έτσι την λειτουργία του Metamask. Το Metamask χρησιμοποιείται σε περίπτωση που χρειαστεί η εφαρμογή να αναπτυχθεί και σε άλλα blockchain. Επίσης, η διεπαφή αποκρυπτογραφεί τα δεδομένα του φοιτητή με τον αλγόριθμο AES και συμμετρικό κλειδί την διεύθυνση του ψηφιακού πορτοφολιού που καταχωρεί ο χρήστης στην διεπαφή.

Σχεδιαστικός στόχος ήταν η ευχρηστία και ευκολία στην πρόσβαση. Χρησιμοποιεί δύο φόρμες HTML: την φόρμα για την αναζήτηση της διεύθυνσης του ψηφιακού πορτοφολιού ενός αποφοίτου και τη φόρμα με τα δεδομένα του που εμφανίζεται μετά την αναζήτηση. Επιπλέον, υπάρχει δυνατότητα να γίνει η επαλήθευση με QR code λόγω της συνδυαστικής λειτουργίας του fortmatic.js αλλά και του κώδικα Javascript. Έτσι, όταν υπάρχει μια παράμετρος search στο url της διεπαφής επαλήθευσης και το search αυτό είναι ίσον με το ψηφιακό πορτοφόλι του φοιτητή, τότε επιστρέφεται στο πεδίο αναζήτησης το ψηφιακό πορτοφόλι και μπορεί έτσι να γίνει η αναζήτηση του χωρίς την χρήση του MetaMask. Οπότε, το QR code δεν είναι τίποτα άλλο παρά το url της διεπαφής επαλήθευσης και η παράμετρος με την διεύθυνση του ψηφιακού πορτοφολιού του φοιτητή.

Σχήμα 6.11: Η διεπαφή επαλήθευσης πριν την ενεργοποίηση του «Search»

Οι δύο βασικές λειτουργίες που εκτελεί η διεπαφή αυτή, είναι η κλήση και η εμφάνιση των:

- Κρυπτογραφημένων προσωπικών στοιχείων του αποφοίτου και η αποκρυπτογράφηση τους (Σχήμα 6.12).
- Κρυπτογραφημένων μαθημάτων που διεκπεραίωσε με επιτυχία ο απόφοιτος και η αποκρυπτογράφηση τους. (Σχήμα 6.13)

```
Contract.methods.getStudent(fromAddress).call(
    function(error, result) {
    if (error) { console.log('error: ' + error); }
    else { console.log(result);
```

Σχήμα 6.12: Εμφάνιση προσωπικών στοιχείων του αποφοίτου

```
Contract.methods.getGradesOfStudent(fromAddress).call(
    function(error, result) {
        if (error) {console.log('error: ' + error);
        } else {
```

Σχήμα 6.13: Εμφάνιση στοιχείων των μαθημάτων του αποφοίτου

Οι δύο παραπάνω συναλλαγές έχουν ως κοινό σημείο την διεύθυνση του ψηφιακού πορτοφολιού του αποφοίτου (fromAddress). Οι συναλλαγές είναι ήδη αποθηκευμένες στην κατάσταση του έξυπνου συμβολαίου και επιστρέφονται από αυτή. Οι κλήσεις για την ανάκτηση και επαλήθευση αυτών των πληροφοριών δεν έχουν κάποιο κόστος, καθώς δεν απαιτούν την εκτέλεση υπολογισμών από κάποιο miner του blockchain. Τέλος, η διεπαφή χρησιμοποιεί ένα σημαντικό εργαλείο, το obfuscator [58], το οποίο μετατρέπει τον κώδικα Javascript σε μη αναγνωρίσιμη από τον άνθρωπο μορφή, αλλά συνεχίζει ο περιηγητής να διαβάζει τον κώδικα αυτό. Με αυτό το εργαλείο επιτυγχάνεται η μερική κρυπτογράφηση του κώδικα της διεπαφής, έτσι ώστε, να μην αναγνωρίσει κάποιος τρίτος τον τρόπο που γίνεται η αποκρυπτογράφηση των δεδομένων του φοιτητή.

6.2.3 Υλοποίηση του έξυπνου συμβολαίου

Το έξυπνο συμβόλαιο αποτελεί το back-end το οποίο αναπτύχθηκε από τους δημιουργούς της εφαρμογής και είναι το πρώτο από τα δύο συστατικά του backend και είναι γραμμένο σε κώδικα Solidity. Το έξυπνο συμβόλαιο έχει την έννοια του ρυθμιστή των δεδομένων που η ακαδημαϊκή μονάδα εισάγει σε αυτό μέσω της εφαρμογής - frontend. Το έξυπνο συμβόλαιο θα μπορούσε να παρομοιαστεί με την βάση δεδομένων της μονάδας που αποθηκεύει τα δεδομένα με αποκεντρωμένο τρόπο. Ο λόγος που υπάρχει τέτοια παρομοίωση είναι ότι, τα δεδομένα αποθηκεύονται μοναδικά στην κατάσταση της συγκεκριμένης διεύθυνσης (Contract Account) που παρήχθη από την διαδικασία εξόρυξης - mining του έξυπνου συμβολαίου, όμως αποθηκεύει τα δεδομένα στο δίκτυο blockchain του Ethereum και όχι σε κάποια ιδιωτική βάση δεδομένων. Το έξυπνο συμβόλαιο αποτελείται από δύο αρχεία Solidity, το UomToken, το οποίο είναι τα αντίστοιχα ECTS του χρήστη, και το StudentGrades, που περιέχει τον κώδικα που είναι υπεύθυνος για την αποθήκευση των δεδομένων των φοιτητών. Στο Σχήμα 6.14 παριστάνεται το συμβόλαιο UomToken στην Ενοποιημένη Γλώσσα Σχεδίασης Προτύπων (UML). Αυτό το συμβόλαιο είναι η γονέας του συμβολαίου StudentGrades ώστε το δεύτερο να κληρονομεί τις μεθόδους που έχουν δηλωθεί στο πρώτο. Αποτελεί κομμάτι από το πρότυπο του ERC20 token [49], το οποίο έχει τροποποιηθεί στα πλαίσια της εφαρμογής και το πιο βασικό είναι ότι αυτές τις μονάδες (που παρομοιάζονται με τα ECTS), μπορούν μόνο από την ακαδημαϊκή μονάδα (συγκεκριμένα η μοναδική διεύθυνση -πορτοφόλι της γραμματείας) να μεταφερθούν στον φοιτητή. Η σχέση αυτή είναι μονόδρομη, τα tokens αυτά, δεν μπορούν να επιστραφούν, να τροποποιηθούν ή να μεταφερθούν σε

τρίτο λογαριασμό[2]. Το αρχείο *UomToken.sol* περιλαμβάνει 3 βασικά υπό-συμβόλαια και μία βιβλιοθήκη:

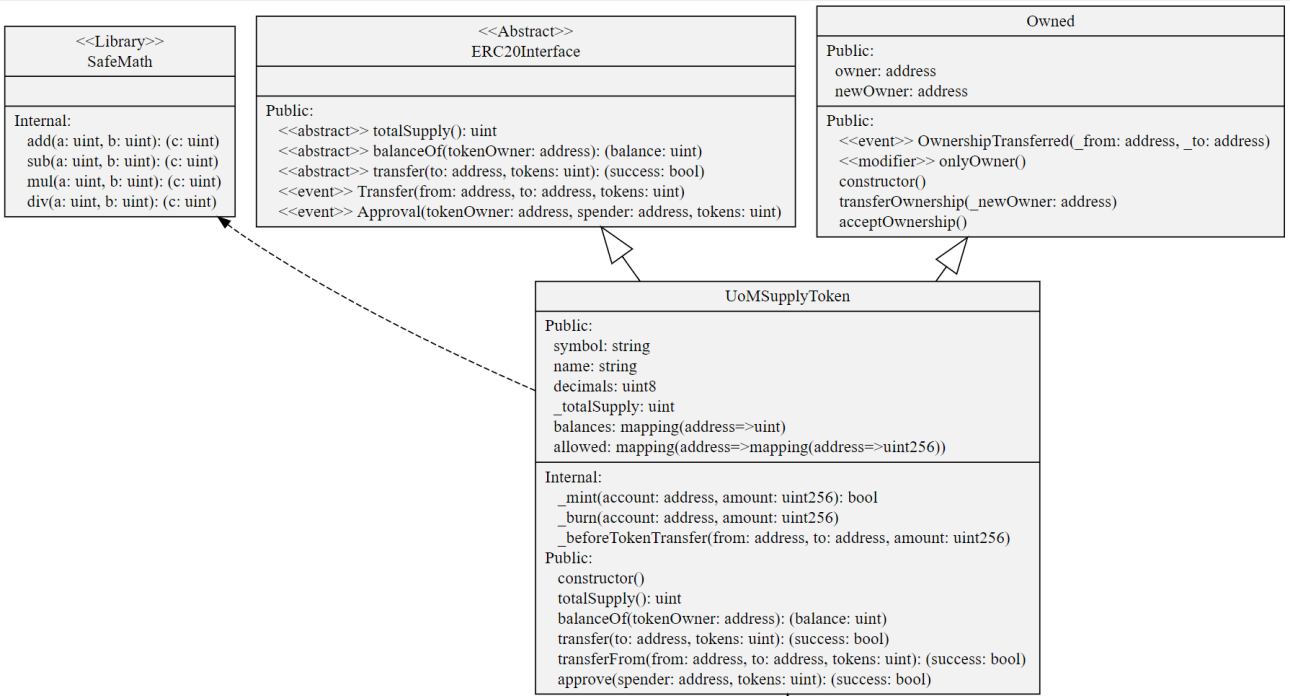
- Το συμβόλαιο *ERC20Interface*. Είναι το συμβόλαιο που δηλώνει τις τρεις συναρτήσεις, την συνάρτηση που επιστρέφει το υπόλοιπο των πιστωτικών μονάδων που μπορεί να προσφέρει ακόμα το πανεπιστημιακό ίδρυμα, το σύνολο των πιστωτικών μονάδων που έχει η εισαγόμενη διεύθυνση στην κατοχή της και η συνάρτηση μεταφοράς των πιστωτικών μονάδων από το πανεπιστημιακό ίδρυμα στον αντίστοιχο φοιτητή.

- Το συμβόλαιο *Owned*. Έχει έναν κατασκευαστή, έναν τροποποιητή και δύο συναρτήσεις που αφορούν την μεταβίβαση της ιδιοκτησίας των νομισμάτων (συνήθως από το ίδρυμα στον ιδιώτη).

- Το συμβόλαιο *UoMSupplyToken*. Στο συμβόλαιο ERC20Interface αναφέραμε ότι δηλώθηκαν οι 3 συναρτήσεις, αλλά σε αυτό το συμβόλαιο ορίζονται. Πέρα όμως από τις τρεις συναρτήσεις που περιλαμβάνει, έχει και έναν κατασκευαστή όπου είναι η βασική λειτουργία του έξυπνου συμβολαίου. Μέσα στον κατασκευαστή ορίζονται: α) το όνομα του token, β) το σύμβολο τους, γ) τον αριθμό των πιστωτικών μονάδων που θα έχει κατα την εκκίνηση του συμβολαίου ο λογαριασμός (του πανεπιστημίου), δ) η μεταφορά των μονάδων αυτών στην διεύθυνση που δημιούργησε το συγκεκριμένο έξυπνο συμβόλαιο (δηλαδή η διεύθυνση του πανεπιστημίου ή του υπουργείου παιδείας). Τέλος, διαθέτει και άλλες λειτουργίες όπως η _mint που δημιουργεί καινούργια tokens και τα στέλνει στον φοιτητή, η _burn που υπάρχει για να ανακαλέσει και να καταστρέψει τα tokens του φοιτητή, καθώς και οι *transferOf* και *approve* για μελλοντική χρήση δηλαδή, όταν ολοκληρωθεί η επιχειρησιακή λογική της εφαρμογής και μια κεντρική οντότητα θα μπορεί να μοιράσει τα νομίσματα της στα ιδρύματα και αυτά με την σειρά τους, στους πτυχιούχους φοιτητές.

- Η βιβλιοθήκη *SafeMath*. Η βιβλιοθήκη αυτή ορίζει με ασφάλεια τις γνωστές μαθηματικές πράξεις. Προσφέρει ασφάλεια μιας και δέχεται μόνο ακέραιους αριθμούς και επιστρέφει μόνο ακέραιους αριθμούς.

[2]αυτή η ιδιότητα φαίνεται στις γραμμές 106-107 του κώδικα https://gist.github.com/gmixoulis/0225779d6b8c75f025cacc2720e701fd



Σχήμα 6.14: Το συμβόλαιο UomToken σε UML

Η καινοτομία της εφαρμογής Verde έγκειται στο αρχείο StudentGrades.sol. Οι λειτουργίες που περιλαμβάνει είναι η αποθήκευση των στοιχείων των φοιτητών, η αποθήκευση των βαθμών στο εκάστοτε μάθημα των φοιτητών μαζί και οι πιστωτικές μονάδες που τα συνοδεύουν. Στο Σχήμα 6.15 παριστάνεται το έξυπνο συμβόλαιο σε UML. Το συμβόλαιο αυτό περιλαμβάνει εφτά συναρτήσεις, πέντε δομές δεδομένων τύπου hashmap (mapping = hashmap) και μία δομή δεδομένων με όνομα Student στο οποίο καταχωρούνται τα στοιχεία του φοιτητή. Οι πέντε βασικές συναρτήσεις που περιλαμβάνει είναι οι εξής:

- Η συνάρτηση *setStudent*. Δέχεται σαν όρισμα όλα τα στοιχεία του φοιτητή και επιστρέφει μια δυαδική τιμή σε περίπτωση που καταχωρηθούν με επιτυχία τα στοιχεία του φοιτητή ή σε περίπτωση που η διαδικασία αποτύχει. Ειδικότερα όμως υπάρχει μία μεταβλητή τύπου mapping, η students, όπου έχει σαν κλειδί την διεύθυνση του αποφοίτου και σαν τιμή την δομή Student. Με αυτό τον τρόπο, η συγκεκριμένη διεύθυνση δεσμεύει, μέσω του mapping, όλα τα στοιχεία του φοιτητή, καθώς και τα μαθήματα του που αποθηκεύονται από την λειτουργία της αμέσως επόμενης συνάρτησης.

- Η συνάρτηση *setStudentGrades*. Δέχεται ως όρισμα ένα πίνακα που περιλαμβάνονται μέσα σε αυτόν τα κρυπτογραφημένα μαθήματα που ολοκλήρωσε με επιτυχία και έναν πίνακα που περιλαμβάνονται σε αυτόν οι βαθμοί του αποφοίτου, και οι διδακτικές μονάδες που είχε το κάθε μάθημα. Επιστρέφει μια δυαδική τιμή ανάλογα με το αν ολοκληρώθηκε η λειτουργία της συνάρτησης με επιτυχία ή όχι. Η δομή δεδομένων Student περιλαμβάνει μια μεταβλητή τύπου mapping με όνομα grades. Σε αυτόν τον χάρτη διασποράς αποθηκεύονται τα ονόματα και οι βαθμοί των μαθημάτων, που εκτε-

λείται από την λειτουργία αυτής συνάρτησης. Επίσης, υπολογίζει τον μέσο όρο και το σύνολο των ECTS που προκύπτουν από τα μαθήματα. Ο μέσος όρος αποθηκεύεται στην μεταβλητή AvgOfStuddent, η οποία δέχεται ως κλειδί την διεύθυνση του πορτοφολιού και ως τιμή έναν αριθμο (τον μέσο όρο). Τέλος μεταφέρει το σύνολο των ECTS στον φοιτητή. Είναι ορισμένη τύπου payable ώστε να μπορεί να στέλνει τα ECTS στον φοιτητή.

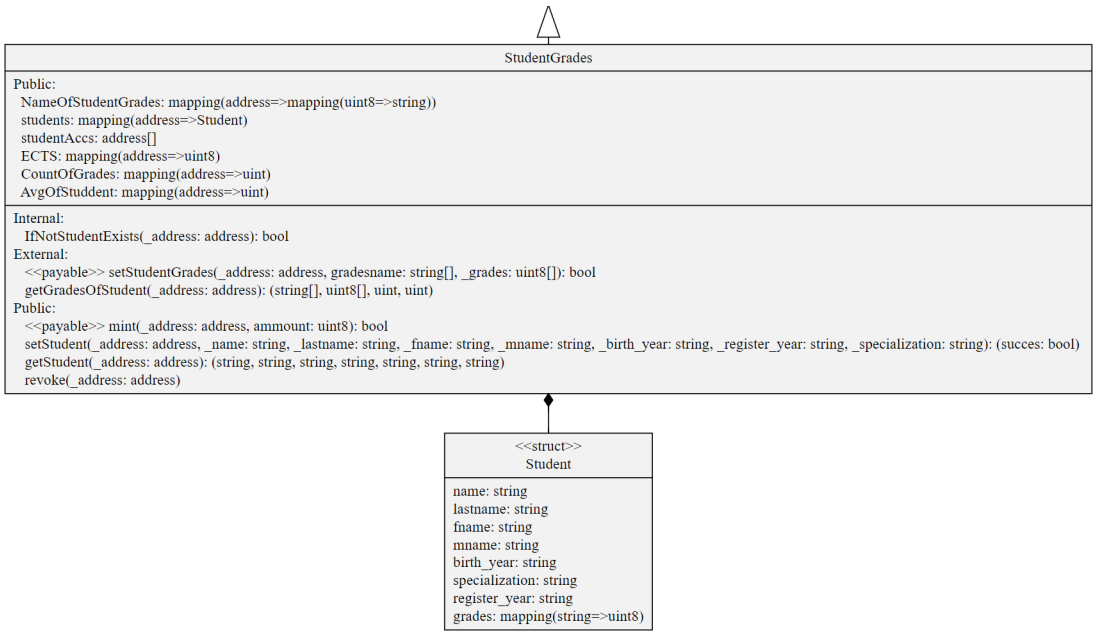
- Η συνάρτηση *getStudent*. Δέχεται ως όρισμα την διεύθυνση του αποφοίτου και επιστρέφει τα στοιχεία του.

- Η συνάρτηση *getGradesOfStudent*. Δέχεται ως όρισμα την διεύθυνση του αποφοίτου και επιστρέφει τους βαθμούς του,τις πιστωτικές μονάδες ECTS και τον μέσο όρο του.

- Η συνάρτηση *IfNotStudentExists*. Δέχεται ως όρισμα την διεύθυνση του αποφοίτου και επιστρέφει μια δυαδική τιμή (αληθές ή ψευδές) σε περίπτωση που η διεύθυνση αυτή υπάρχει ή όχι καταχωρημένη στο συμβόλαιο και συγκεκριμένα στον χάρτη διασποράς studentAccs.

- Η συνάρτηση *mint*, που θα χρησιμοποιήτε μόνο όταν τελειώσουν όλα τα tokens που διαθέτει το ίδρυμα στην κατοχή του, μιας και αυτή δημιουργεί νέα tokens και τα στέλνει στους παραλήπτες.

- Η συνάρτηση *revoke* για την ανάκληση και διαγραφή των δεδομένων του φοιτητή από το έξυπνο συμβόλαιο.



Σχήμα 6.15: Το συμβόλαιο StudentGrades σε UML

6.3 Σύγκριση της Verde έναντι παρόμοιων εφαρμογών

Η πλαστογράφηση των ακαδημαϊκών τίτλων είναι μια ανήθικη και πολλές φορές επικίνδυνη πράξη. Η σημασία της γρήγορης και αποτελεσματικής επαλήθευσης τους είναι ουσιαστική. Σήμερα το Ελληνικό κράτος έχει δημιουργήσει μια νομοθεσία για την αντιμετώπιση της πλαστογραφίας. Σύμφωνα με το Αρ.Πρωτ.ΔΙΔΑΔ/Φ.34.1/86/οικ.31792/08-12-2014, το ελληνικό δημόσιο προτρέπει τον εκάστοτε φορέα να επαλήθευση μόνος του τους ακαδημαϊκούς τίτλους που του προσφέρονται με την μορφή δικαιολογητικών για του υποψήφιους εργαζόμενους. Πιο συγκεκριμένα η νομοθεσία γράφει ότι: *"Για το σκοπό αυτό οι υπηρεσίες αποστέλλουν σύμφωνα με το επισυναπτόμενο υπόδειγμα, στους αρμόδιους φορείς με φαξ ή με ηλεκτρονικό ταχυδρομείο αντίγραφα των τίτλων των υποψηφίων για τη διαπίστωση της γνησιότητας τους"*. Από τα παραπάνω αντιλαμβανόμαστε ότι η ισχύουσα νομοθεσία δεν είναι επαρκής και αρκετά χρονοβόρα, καθώς χρειάζεται αρκετός χρόνος αλλά και κόστος να για διεκπεραιωθεί και είναι αμφίβολο αν τελικά θα υπάρξει κάποια απάντηση από το ακαδημαϊκό ίδρυμα. Έτσι, λόγο του κενού που αφήνει πίσω αυτή η νομοθεσία δημιούργησε την ανάγκη για την εξεύρεση μιας λύσης. Λύσεις προήλθαν τόσο από ινστιτούτα όσο και από ιδιώτες, που και οι δυο έχουν το εξής κοινό, χρησιμοποίησαν την τεχνολογία βλοςκςηαιν καθώς διασφαλίζει την εγκυρότητα των πληροφοριών.

UNIC Η πρώτη λύση εμφανίστηκε από το πανεπιστήμιο της Νικοσίας το 2014 [6, 59]. Η συγκεκριμένη λύση ουσιαστικά στέλνει τα μεταδεδομένα του PDF του πιστοποιητικού στο Bitcoin. Ύστερα ενσωματώνει μερικές πληροφορίες στα μεταδεδομένα όπως η ψηφιακή διεύθυνση του αποστολέα που δημοσίευσε το πιστοποιητικό και η σύνοψη του merkle root του blockchain στο οποίο αποθηκευτήκαν τα μεταδεδομένα του πιστοποιητικού. Η επαλήθευση του αρχείου PDF γίνεται μέσω της πλατφόρμας που έχει δημιουργήσει το πανεπιστήμιο με τον έλεγχο των μεταδιδόμενων του αρχείου αυτού. Ο τρόπος για να ανακληθεί ένα πιστοποιητικό σε περίπτωση που το επιβάλει ο νόμος, είναι ο Credentialing meta-protocol. Με αυτόν τον τρόπο δημοσιεύεται μια νέα συναλλαγή στο blockchain που να αναιρεί την εγκυρότητα του πιστοποιητικού μέσω της εκχώρησης των κατάλληλων δεδομένων στο OPCODE του Bitcoin. Όταν τοποθετείται το πιστοποιητικό στην πλατφόρμα για την επαλήθευση του, θα πρέπει να ελέγχονται και οι μελλοντικές συναλλαγές που έχουν σχέση με την ακύρωση των πιστοποιητικών. Η συναλλαγή για την ακύρωση των πιστοποιητικών χωράει μόνο δύο πιστοποιητικά την φορά.

Blockcerts Το Blockcerts [7] ιδρύθηκε το 2015, είναι έργο των Media Lab Learning Initiative και των Learning Machine, όπου δημιούργησαν μία πλατφόρμα για την επαλήθευση των ακαδημαϊκών τίτλων. Τα πιστοποιητικά του Blockcerts ακολουθεί τα πρότυπα του Open Badges δηλαδή, μια ομάδα προδιαγραφών και ανοιχτών τεχνικών προτύπων που ανα-

πτύχθηκαν από το Mozilla Foundation. Μεταφέρει τις πληροφορίες του πτυχίου στο Bitcoin μέσω του πεδίου OPRETURN [60] ή στο Ethereum ανάλογα τον πελάτη, και η επαλήθευση γίνεται με την ταύτιση των Merkle Tree Root. Ακόμη, χρησιμοποιούν την τεχνολογία των Merkle Trees για να αποδώσουν πιστοποιητικά εκτός ακαδημαϊκών τίτλων. Είναι απαραίτητο και το ίδρυμα που εκδίδει το πιστοποιητικό αλλά και ο χρήστης να έχουν τα δικά τους κλειδιά για την επίτευξη της συναλλαγής. Η διαδικασία καταχώρησης και επαλήθευσης ενός ακαδημαϊκού τίτλου είναι η εξής: Αρχικά το πανεπιστήμιο χρησιμοποιεί το ειδικό εργαλείο των Blockcerts και μετατρέπει το πτυχίο του φοιτητή σε μια JSON μορφή, το οποίο το υπογράφει με το δημόσιο κλειδί του. Στην συνέχεια το εργαλείο δημιουργεί την σύνοψη του αρχείου και το στέλνει στο blockchain και το υπογεγραμμένο αρχείο στον φοιτητή. Εάν το πανεπιστήμιο ήθελε να στείλει μια δέσμη από πτυχία τότε αυτά τοποθετούνται σε ένα Merkle tree και το path της σύνοψης του κάθε πτυχίου αναγράφονται στο JSON αρχείο. Οπότε η επαλήθευση γίνεται με την μεταφόρτωση του αρχείο στην ιστοσελίδα τους και ουσιαστικά γίνεται η αναζήτηση της συγκεκριμένης σύνοψης στο έξυπνο συμβόλαιο τους. Η ανάκληση ενός πιστοποιητικού γίνεται μέσω αναζήτησης μιας online λίστας που διαθέτουν στον εξυπηρετητή της ιστοσελίδας τους. Τέλος, υπάρχουν πολλές περιπτώσεις χρήσης στον πραγματικό κόσμο όπου έχει χρησιμοποιηθεί η τεχνολογία Blockcerts, όπως: α) Central New Mexico Community College, β) το National Training Agency, Bahamas, Institute for Tourism Studies in Malta και το πιλοτικό πρόγραμμα του Federation of State Medical Boards (FSMB) [61, 62].

EchoLink Η EchoLink [8] αποτελεί μια Ethereum blockchain πλατφόρμα που χρησιμοποιεί ένα έξυπνο συμβόλαιο βασισμένο στο ERC20 token. Από όλες τις προτάσεις η EchoLink είναι η πιο κοντινή προσέγγιση στην εφαρμογή Verde καθώς χρησιμοποιούν και τα δύο το έξυπνο συμβόλαιο ERC20 token, λειτουργούν κάτω από την ίδια λογική στον λειτουργικό σκοπό τους και χρησιμοποιούν το Ethereum blockchain. Όμως η διαφορά έγκειται στο γεγονός ότι, η πλατφόρμα EchoLink αποθηκεύει τα στοιχεία του αποστολέα (ακαδημαϊκό ίδρυμα), του παραλήπτη (φοιτητή), την ώρα δημιουργίας του πιστοποιητικού, της διεύθυνσης του αρχείου PDF του πιστοποιητικού και το αρχείο της φωτογραφίας του παραλήπτη στο Ethereum και όχι τα δεδομένα του πτυχίου του. Τα αρχεία αποθηκεύονται σε ένα Διαπλανητικό Σύστημα Αρχείων (InterPlanetary File System - "IPFS"), το οποίο είναι πρωτόκολλο και δίκτυο σχεδιασμένο για να δημιουργήσει μια μέθοδο peer-to-peer για την αποθήκευση και την κοινή χρήση υπερμέσων σε κατανεμημένο σύστημα αρχείων. Τα προσωπικά δεδομένα του αποστολέα και του παραλήπτη είναι αποθηκευμένα στην βάση δεδομένων της εταιρείας το οποίο εγείρει αμφιβολίες για τον τρόπο που τα διαχειρίζεται αυτά τα στοιχεία και κατά πόσο είναι ασφαλές από επιθέσεις. Στο άρθρο της EchoLink δεν υπάρχει κάποια μέθοδος για την ανάκληση των πιστοποιητικών σε περίπτωση που χρειαστεί.

TrueRec Το TrueRec [9] είναι δημιούργημα της εταιρίας SAP και παρουσιάστηκε στο κοινό το 2017. Το TrueRec χρησιμοποιεί έξυπνο συμβόλαιο ανεπτυγμένο στο Ethereum. Η εταιρία δημιούργησε ένα ψηφιακό πορτοφόλι για την αποθήκευση επαγγελματικών και ακαδημαϊκών τίτλων. Κάθε ίδρυμα πρέπει να ανήκει στο δίκτυο του TrueRec για να μπορεί να χρησιμοποιήσει την εφαρμογή. Η διαδικασία καταχώρησης και επαλήθευσης έχει ως εξής: όταν ένα ίδρυμα δημοσιεύει τους ακαδημαϊκούς του τίτλους μέσω του TrueRec, ένα ψηφιακό δακτυλικό αποτύπωμα προστίθεται στο blockchain. Το TrueRec στέλνει τα έγγραφα στον χρήστη ως αρχείο.TRU, το οποίο ο χρήστης εισάγει εύκολα στην εφαρμογή TrueRec μέσα από την κινητή συσκευή του. Οι χρήστες μπορούν να μοιράζονται τα έγγραφα τους απευθείας από την εφαρμογή TrueRec. Οι παραλήπτες μπορούν να επαληθεύσουν τα διαπιστευτήρια συγκρίνοντας το έγγραφο.TRU με το δακτυλικό του αποτύπωμα στο blockchain. Δεν αναφέρεται πουθενά αν περιλαμβάνει ένα σύστημα ανάκλησης των πτυχίων.

University of Zurich BlockChain (UZHBC) Το UZHBC [10] είναι η λύση που πρότεινε το πανεπιστήμιο της Ζυρίχης και έχει εφαρμογή μόνο στο ίδρυμα τους. Χρησιμοποιεί και αυτό έξυπνο συμβόλαιο ανεπτυγμένο στο Ethereum. Σύμφωνα με τους Jerinas Gresch et al. η διαδικασία καταχώρησης και επαλήθευσης είναι η εξής: Αρχικά το ίδρυμα πρέπει να δημιουργήσει το ψηφιακό πτυχίο. Ύστερα, το back-end δέχεται το PDF πτυχίο ως είσοδο για τη δημιουργία μια σύνοψης που θα αντιστοιχεί στο πτυχίο. Αυτή η σύνοψη θα αποθηκευτεί σε ένα έξυπνο συμβόλαιο, χωρίς δυνατότητα ανάκλησης, το οποίο θα δημοσιευτεί στο Ethereum. Ένας τρίτος που θέλει να επαληθεύσει τα στοιχεία του πρώην φοιτητή, λαμβάνει από αυτόν το δίπλωμα του και στην συνέχεια χρησιμοποιεί το front-end του ιδρύματος, το οποίο παίρνει το ψηφιακό δίπλωμα ως είσοδο για να ελέγξει την αυθεντικότητα του. Αυτή η σύνοψη θα συγκριθεί με όλες τις υπόλοιπες συνόψεις που περιέχονται στο έξυπνο συμβόλαιο. Εάν υπάρχει, η επαλήθευση θα επιστρέψει ένα μήνυμα επιτυχίας και θα ενημερώσει την εταιρεία ότι το δίπλωμα είναι αυθεντικό. Εάν δεν υπάρξει αντιστοιχία, το σύστημα δίνει επίσης κάποιο μήνυμα αποτυχίας.

BCDiploma Το BCDiploma δημιουργήθηκε το 2018 από την ομάδα Blockchain Certified Data -bcd [13]. Η ιδέα τους βασίζεται σε τρία έξυπνα συμβόλαια δημοσιευμένα στο Ethereum και δύο εφαρμογές: της καταχώρησης (Crypto App) και της επαλήθευσης(Reader App). Τα έξυπνα συμβόλαια είναι τα εξής: 1) το SmartValidation το οποίο διασφαλίζει ότι η ταυτότητα του σχολείου έχει επαληθευτεί, το SmartIdentification όπου είναι υπεύθυνο για την έκδοση του πιστοποιητικού της ταυτότητας του σχολείου και 3) το SmartPublication όπου δημοσιεύει τον ακαδημαϊκό τίτλο στο Ethereum. Ουσιαστικά το πρώτο αποθηκεύει τα στοιχεία του πανεπιστημίου ώστε αν χρειαστεί κάποιος να τα αναζητήσει να είναι διαθέσιμα μέσω αυτού του συμβολαίου, το δεύτερο δημιουργεί το ID Certificate του πανεπιστημίου, δηλαδή το μόνιμο κλειδί του πανεπιστημίου, το οποίο είναι προαπαιτούμενο ώστε να μπορέσει αυτό να δημοσιεύσει στο Ethereum, και το τρίτο δημοσιεύει τα συμπιεσμένα και κρυπτογρα-

φημένα (με AES), για λόγο κόστους αερίου, στοιχεία του φοιτητή στο blockchain εφόσον αυτά έχουν πρώτα κρυπτογραφηθεί μέσω της εφαρμογής τους Crypto App. Οπότε, το Crypto App, κάθε φορά που δέχεται ένα πτυχίο (είτε σε μορφή αρχείου είτε σε API) στέλνει τα κρυπτογραφημένα στοιχεία στο SmartPublication το οποίο, ελέγχει την εγκυρότητα του ID του πανεπιστημίου και στην συνέχεια τα δημοσιεύει στο δίκτυο. Στο τέλος της προηγούμενης διαδικασίας το Crypto App δημιουργεί και αποθηκεύει τα persistence keys του διπλώματος τοπικά στο πανεπιστήμιο, επιστρέφει το URL του πτυχίου το οποίο αποτελείται από το κλειδί (Diploma's key) και τον αριθμό του διπλώματος, στην συνέχεια διαγράφει αυτά τα στοιχεία από την μνήμη της εφαρμογής. Άρα, ένας τρίτος που θέλει να επαληθεύσει ένα δίπλωμα χρειάζεται να εισάγει το URL του διπλώματος στο Reader App, η αποκρυπτογράφηση των στοιχείων γίνεται στο back-end της εφαρμογής, με την χρήση του Diploma's key, του persistence key και του μόνιμου κλειδιού του πανεπιστημίου. Όλα αυτά τα κλειδιά περνάνε ως παράμετρος στο αλγόριθμο AES και αποκρυπτογραφούν τα στοιχεία του φοιτητή. Οι συγγραφείς αναφέρουν ότι η εφαρμογή ακολουθεί την GDPR νομοθεσία. Εάν ο φοιτητής θελήσει να διαγραφεί από την εφαρμογή, τότε το πανεπιστήμιο είναι υποχρεωμένο να διαγράψει τα persistence keys, αλλά τα κρυπτογραφημένα προσωπικά του δεδομένα παραμένουν στο Ethereum.

GRNET Η ελληνική ιδέα για τις "Προχωρημένες κρυπτογραφικές υπηρεσίες στα ψηφιακά ακαδημαϊκά διπλώματα" του Δημήτρη Μητρόπουλου, συστήθηκε στο κοινό το 2018 υπό την αιγίδα του GRNET [63, 11] στα πλαίσια του Ευρωπαϊκού προγράμματος Horizon 2020, όπου συμμετέχουν σε αυτό το πρόγραμμα άλλα 14 κράτη-μέλη της Ευρώπης (παράδειγμα με την αντίστοιχη λύση του Βελγίου [64]. Η ιδέα αυτή υλοποιείται στο ιδιωτικό-permissioned Cardano blockchain αλλά και στο Hyperledger blockchain. Το έργο είναι αξιοσημείωτο επειδή είναι η πρώτη επίσημη περίπτωση χρήσης του Cardano blockchain, χρησιμοποιεί ένα μοντέλο συναίνεσης Proof-of-Authority και πιο συγκεκριμένα χρησιμοποιεί το zero-knowledge protocol και αναπτύσσεται με την εταιρία IOHK, την δημιουργό του Cardano blockchain. Το παραπάνω πρωτόκολλο είναι μια μέθοδος με την οποία μια οντότητα μπορεί να αποδείξει σε μία άλλη οντότητα ότι γνωρίζει μια τιμή x, χωρίς να αποκαλύψει οποιαδήποτε πληροφορία εκτός από το γεγονός ότι γνωρίζει την τιμή ξ [65]. Σύμφωνα με τον κ. Μητρόπουλο, το blockchain θα *μπορούν* να προσπελάσουν εξουσιοδοτημένες οντότητες (χωρίς αυτό να είναι απαραίτητο) και επίσης, δεν θέλουν να καταγράφουν *μόνο* το γεγονός της απονομής ενός πτυχίου, αλλά και όλου του ιστορικού της χρησιμοποίησης του (ή ανάκλησής του). Οι κόμβοι του blockchain είναι τα διάφορα ελληνικά ακαδημαϊκά ιδρύματα (NTUA, AUEB) και το ίδρυμα *αποδεικνύει* σε έναν φορέα (όπως ο GRNET) πως όντως έχει πτυχίο ο απόφοιτος.Στο δίκτυο blockchain αποθηκεύονται τα κρυπτογραφημένα μεταδεδομένα. Στην συγκεκριμένη φάση αποθηκεύουν μόνο τις συνόψεις των ακαδημαϊκών τίτλων στο δίκτυο αλλά έχουν την δυνατότητα να αποθηκεύσουν ολόκληρα τα πτυχία σε κρυπτογραφημένη μορφή.

Cerberus Το Cerberus [12] αποτελεί μελέτη των Tariq et al [12]. Δημιούργησαν ένα δικό τους ιδιωτικό δίκτυο blockchain με την βοήθεια του Ethereum Parity ώστε να μπορούν να εκτελούν έξυπνα συμβόλαια. Το μοντέλο συναίνεσης που χρησιμοποιούν είναι το Proof-of-Authority. Οι κόμβοι του blockchain είναι τα ακαδημαϊκά ιδρύματα αλλά και η οντότητα Observer η οποία ελέγχει κάθε διαδικασία στο σύστημα και ελέγχει την ακεραιότητα του συστήματος. Η λογική της επαλήθευσης είναι ότι δεν χρειάζεται ούτε ο επαληθευτής αλλά ούτε και αυτός που επαληθεύεται να διατηρούν κλειδιά και ψηφιακό πορτοφόλι στο blockchain και η επαλήθευση γίνεται με το QR code που αναγράφεται πάνω στο πτυχίο. Η διαδικασία της καταχώρησης των δεδομένων ενός φοιτητή στο Cerberus δίκτυο έχει ως εξής: αρχικά το ψηφιακό fingerprint του πτυχίου του φοιτητή μεταφέρετε στο δίκτυο μέσω μιας συναλλαγής σε αυτό, όπου το ίδρυμα το υπογράφει ψηφιακά μέσω του university registar στο δίκτυο και επαληθεύτε η εγκυρότητα της συναλλαγής από το accreditation body (δηλαδή, η οντότητα που είναι υπεύθυνη για την διατήρηση του συστήματος) και στην συνέχεια προστίθεται στο blockchain. Η διαδικασία της καταχώρησης όμως είναι λίγο πιο περίπλοκη. Αρχικά όλα τα στοιχεία του πτυχίου του φοιτητή καθώς και τα προσωπικά του δεδομένα, το καθένα ξεχωριστά περνάνε μέσα από μια συνάρτηση διασποράς SHA2 και δημιουργούν το student-info, που αποτελεί φύλλο του Merkle tree. Κάθε φύλλο του δέντρου αποτελείται ουσιαστικά και από ένα πτυχίο και όλα μαζί έχουν μια κοινή ρίζα batch Merkle root. Οπότε η επαλήθευση των τίτλων, γίνεται μέσω μιας κινητής εφαρμογής και του ελέγχου του QR code. Αυτό, περιλαμβάνει πληροφορίες όπως τα στοιχεία του πτυχίου, το fingerprint των δεδομένων του φοιτητή, τον αριθμό του μπλοκ, το ID της συναλλαγής και τις διευθύνσεις των αδελφικών φύλλων. Άρα, η κινητή εφαρμογή του χρήστη υπολογίζει όλα τα παραπάνω δεδομένα και δημιουργεί μία σύνοψη μιας ρίζας Merkle tree. Αυτή αναζητείται στο δίκτυο του Cerberus και αν υπάρχει τότε η επαλήθευση ήταν επιτυχής.Το Cerberus διαθέτει επίσης και ένα σύστημα ανάκλησης των πτυχίων ακόμα και μαζικής ανάκλησης. Η ανάκληση πρέπει να εγκριθεί από δύο τουλάχιστον κόμβους και η διαδικασία εκτελείται από δύο έξυπνα συμβόλαια.

Blockchain for Education: Lifelong Learning Passport Το project των Kolvenbach et al. [14] χρησιμοποιεί δύο έξυπνα συμβόλαια στο Ethereum blockchain με σκοπό την επαλήθευση των ακαδημαϊκών τίτλων. Το πρώτο έξυπνο συμβόλαιο (IdentityMgmt) υποστηρίζει τη διαχείριση ταυτοτήτων στην πλατφόρμα του Blockchain for Education και η δεύτερη (CertMgmt) διαχειρίζεται τον κύκλο ζωής των ακαδημαϊκών τίτλων που εκδίδονται μέσω του blockchain. Η αρχή διαπίστευσης καταγράφει τα δημόσια κλειδιά των αρχών πιστοποίησης στο IdentityMgmt συμβόλαιο, ώστε να μπορεί να καταχωρήσει μετά μέσα από αυτό, τα δημοσιεύσιμα στοιχεία του φοιτητή στο blockchain. Οπότε, το ακαδημαϊκό ίδρυμα συγκεντρώνει όλα τα δεδομένα του φοιτητή, καταχωρεί το πτυχίο του στο document management system καθώς και το δακτυλικό αποτύπωμα αυτού, στο blockchain. Ο φοιτητής πρέπει να εγγραφεί στο σύστημα διαχείρισης εγγράφων, ώστε στη συνέχεια, να μπορούν να κοινοποιηθούν σε πιθανούς εργοδότες που θα μπορούν να επαληθεύσουν την

εγκυρότητα αυτών των πιστοποιητικών. Το άλλο έξυπνο συμβόλαιο εξυπηρετεί στην διαχείριση των ψηφιακών ακαδημαϊκών τίτλων, την αποθήκευση των πληροφοριών των πτυχίων, την κρυπτογράφηση του πτυχίου και επίσης, διαθέτει λειτουργικότητα όπως η ανάκληση των ακαδημαϊκών τίτλων. Αυτό το έξυπνο συμβόλαιο διαχειρίζεται δύο διαφορετικά συστήματα, το InterPlanetary Filesystem (IPFS) που χρησιμοποιείται ως δημόσιος κατανεμημένος χώρος αποθήκευσης, για ανάγνωση πληροφοριών των αρχών πιστοποίησης και επίσης, αποθηκεύονται σε αυτό οι ακαδημαϊκοί τίτλοι, έτσι ώστε να μην δημοσιεύονται τα προσωπικά δεδομένα των φοιτητών στο Ethereum.Η διαδικασία καταχώρησης και επαλήθευσης είναι η εξής: Αρχικά, το ίδρυμα εισέρχεται στο Web-based groupware system - BSCW και βρίσκει το πτυχίο που θέλει. Ύστερα, το πτυχίο μεταφέρετε στο Ethereum ως αποτέλεσμα της λειτουργίας του CertMgmt και στέλνει στον φοιτητή το πτυχίο του με δύο τρόπους, ως JSON μορφή και ως PDF, το οποίο περιλαμβάνει στα μεταδεδομένα του την ταξινομημένη JSON μορφή του πτυχίου. Ο φοιτητής αποθηκεύει αυτά τα αρχεία τοπικά αλλά και εισαγάγει τα πιστοποιητικά του στο BSCW στον προσωπικό του φάκελο. Έτσι, η επαλήθευση γίνεται με την εισαγωγή του PDF ή του JSON αρχείου στο BSCW σύστημα και αν είναι επιτυχής η εύρεση της συγκεκριμένης σύνοψης στο σύστημα τότε, επιστρέφεται στην διεπαφή το μήνυμα επιτυχίας και πληροφορίες για το ακαδημαϊκό ίδρυμα και για την κατάσταση του πτυχίου.

EduCTX Η εφαρμογή EduCTX είναι μια παγκόσμια πλατφόρμα πιστωτικών μονάδων για την τριτοβάθμια εκπαίδευση. Αυτή η πλατφόρμα βασίζεται στην έννοια του Ευρωπαϊκού συστήματος διδακτικών μονάδων τριτοβάθμιας εκπαίδευσης (ECTS). Αποτελεί ένα παγκόσμιο, αποκεντρωμένο σύστημα πιστωτικών μονάδων τριτοβάθμιας εκπαίδευσης και ένα σύστημα ταξινόμησης που δημιουργεί μια παγκοσμιοποίηση για τους φοιτητές και τα ιδρύματα τριτοβάθμιας εκπαίδευσης καθώς και για άλλους πιθανούς ενδιαφερόμενους, όπως εταιρείες, ιδρύματα και οργανισμούς [15]. Αυτή η εφαρμογή βασίζεται σε ένα παγκόσμιο ομότιμο κατανεμημένο δίκτυο. Το EduCTX επεξεργάζεται, διαχειρίζεται και ελέγχει τα ECTX tokens, τα οποία αντιπροσωπεύουν τις πιστωτικές μονάδες που οι φοιτητές κερδίζουν για τα ολοκληρωμένα μαθήματα τους, όπως ακριβώς τα ECTS. Τα ιδρύματα τριτοβάθμιας εκπαίδευσης είναι οι ομότιμοι χρήστες του blockchain [15]. Το EduCTX χρησιμοποιεί μια δημόσια πλατφόρμα blockchain και συγκεκριμένα την πλατφόρμα ARK (το οποίο λειτουργεί με το DPoS μοντέλο συναίνεσης). Υπάρχουν δύο διαφορετικές λειτουργίες σε αυτήν την εφαρμογή, η μία για να καταχωρεί τα πανεπιστήμια που λειτουργούν ως κόμβοι του blockchain και η άλλη είναι η καταχώρηση των πιστωτικών μονάδων (ECTX tokens) στους φοιτητές εφόσον, ο καθηγητής του εκάστοτε μαθήματος επιτρέψει την απαλλαγή του φοιτητή από το μάθημα, μέσω της επιτυχίας του στο μάθημα αυτό. Οπότε, η επαλήθευση του ακαδημαϊκού τίτλου πραγματοποιείται απλώς προβάλλοντας το ποσό των ECTX tokens που έχει ο φοιτητής στην κατοχή του. Είναι σημαντικό ότι ο κάθε φοιτητής είναι ανώνυμος για λόγους προσωπικών δεδομένων. Ένας φοιτητής έχει μοναδική διεύθυνση - ψηφιακό πορτοφόλι του και αυτή η

διεύθυνση θα αποθηκεύσει και θα λάβει τα EduCTX tokens, δηλαδή την πιστωτική αξία σε ECTS, μετά την επιτυχή ολοκλήρωση του μαθήματος. Η συγκεκριμένη διεύθυνση αφορά μόνο το οικοσύστημα του EduCTX.

Όλα τα παραπάνω συστήματα όμως διαθέτουν πολλούς περιορισμούς που η εφαρμογή Verde έχει καταφέρει και έχει επιλύσει. Αρχικά, η λύση του UZHBC περιορίζεται στην αποκλειστική χρήση από το ίδρυμα της. Επίσης, αυτό και οι λύσεις των UNIC(Block.co), TruRec και το BCDiploma απαιτούν από τον χρήστη να διατηρεί σε ασφαλές σημείο ένα αρχείο το οποίο είναι το μοναδικό που μπορεί να επαληθεύσει το δίπλωμα του. Οπότε, εάν χαθεί μαζί με αυτό θα χαθεί και η ικανότητα της επαλήθευσης. Τα περισσότερα από αυτά τα συστήματα διατηρούν το απόρρητο των δεδομένων των φοιτητών. Το EchoLink είναι η μοναδική εξαίρεση δεδομένου ότι προσλαμβάνει πλατφόρμα και προσφέρει πρόσβαση προβολής σε εγγεγραμμένους χρήστες. Το πρόβλημα της δέσμευσης αποθηκευτικού χώρου για το blockchain (scalability από την πλευρά του πελάτη) δεν λύνεται από τις περισσότερες προτάσεις καθώς όσοι χρησιμοποιούν permissioned blockchain όπως το GRNET, Cerberus, το βάρος του όγκου δεδομένων το επωμίζονται οι εξυπηρετητές τους με αποτέλεσμα να χρειάζονται συνεχώς επέκταση μνήμης, επομένως απαιτείται και μια σχετικά σύγχρονη τεχνολογία για να μπορέσουν να εκτελέσουν το δίκτυο του blockchain. Το πρόβλημα του scalability από την πλευρά του blockchain δηλαδή, το κόστος της συναλλαγής, το λύνει μόνο το Blockcerts καθώς, διαθέτει σύστημα μαζικής αποστολής πτυχίων στο blockchain. Όσοι χρησιμοποιούν το IPFS (όπως το Blockchain for Education, EchoLink) σύστημα αποθήκευσης κινδυνεύουν από το να χαθεί κάποιο κομμάτι του του αρχείου του ακαδημαϊκού τίτλου μιας, καθώς το IPFS είναι η αποθήκευση αρχείων σε P2P περιβάλλον, οπότε αν κάποιος κόμβος διαγράψει τα αρχεία που διαθέτει και δεν υπάρχουν αντίγραφα από το συγκεκριμένο κομμάτι σε άλλο κόμβο, τότε το πτυχίο πρακτικά διαγράφεται. Ο μοναδικός τρόπος για να διατηρηθούν αυτά τα αρχεία στο IPFS είναι με την μέθοδο του Pinning [66] το όποιο όμως προϋποθέτει την διάθεση μιας αμοιβής. Πολύ βασικό επίσης είναι το σύστημα ανάκλησης των πτυχίων. Λίγες είναι οι εφαρμογές που έχουν φροντίσει για αυτό το φαινόμενο όπως, οι GRNET, Cerberus, Block.co, BCDiploma και η Blockchain for Education. Όμως κανένας από τους παραπάνω δεν διαγράφει οριστικά τα δεδομένα του χρήστη από το blockchain.

Η εφαρμογή Verde έχει καταφέρει και έχει επιλύσει τους περισσότερους από τους παραπάνω περιορισμούς. Αρχικά, η επαλήθευση γίνεται με τα ίδια τα στοιχεία του φοιτητή στην διεπαφή επαλήθευσης, οπότε δεν απαιτείτε από τον φοιτητή να διατηρεί αποθηκευμένο κάποιο έγγραφο με σκοπό την επαλήθευση της ακαδημαϊκής του επάρκειας. Η εφαρμογή μας ακολουθεί της οδηγίες του GDPR καθώς, στέλνει τα δεδομένα των χρηστών κρυπτογραφημένα με την χρήση του AES. Επίσης, η λογική της εφαρμογής βασίζεται στο γεγονός ότι, η 4η βιομηχανική επανάσταση περιλαμβάνει την τεχνολογία blockchain, οπότε, μελλοντικά όλοι θα διατηρούν ψηφιακά πορτοφόλια, οπότε η εφαρμογή χρησιμοποιεί αυτήν την πρόβλεψη και στέλνει τα στοιχεία του πτυχίου και τα tokens στην προσωπική διεύθυνση του ψηφιακού

πορτοφολιού του φοιτητή. Οπότε, εάν κάποιος συγκαταλέγεται στους *κρυπτοσκεπτικιστές* και δεν θέλει να διατηρεί ψηφιακό πορτοφόλι, τότε η εφαρμογή το έχει προβλέψει και μπορεί να δουλέψει και με QR code εκτυπωμένο πάνω στο δίπλωμα του φοιτητή. Οπότε δεν απαιτείται, διατηρούν και οι 2 πλευρές ειδικά κλειδιά για να μπορούν να συμμετέχουν στο δίκτυο. Πολύ βασικό επίσης είναι ότι η εφαρμογή Verde είναι διαδικτυακή, δεν χρειάζεται το ίδρυμα να αγοράσει κάποιο ειδικό εξοπλισμό και δεν χρειάζεται επέκταση μνήμης στους εξυπηρετητές της. Το αντίθετο ισχύει δηλαδή, από την στιγμή που όλα τα δεδομένα του φοιτητή δημοσιεύονται στο blockchain δεν χρειάζεται πλέον να τα διατηρεί το ίδρυμα στην βάση δεδομένων της, το μόνο που χρειάζεται πλέον να αποθηκεύει είναι η διεύθυνση του ψηφιακού του πορτοφολιού. Η λειτουργικότητα της εφαρμογής μας είναι ότι μια κεντρική αρχή μοιράζει στα ακαδημαϊκά ιδρύματα και τις σχολές, τα tokens και μπορούν με την σειρά τους να τα δίνουν στους αποφοίτους τους, οπότε η κάθε σχολή είναι υποχρεωμένη στην ιστοσελίδα της να έχει την επίσημη διεύθυνση του ψηφιακού πορτοφολιού με την οποία δημοσιεύει τα πτυχία στο blockchain, για λόγους επαλήθευσης και γνησιότητας των δεδομένων (στα πλαίσια της πτυχιακής εργασίας δεν αναπτύχθηκε τέτοια εφαρμογή, όμως σε επίπεδο του έξυπνου συμβολαίου των tokens, υπάρχει τέτοια λειτουργία. Όμως η επαλήθευση δεν τελειώνει μόνο στα στοιχεία καθώς, τα tokens έχουν μια κοινή διεύθυνση από την οποία μεταφέρονται στους φοιτητές. Άρα, μπορεί κάποιος να ελέγξει την συναλλαγή των tokens στο ψηφιακό πορτοφόλι του φοιτητή και να επαληθεύσει έτσι την γνησιότητα του ακαδημαϊκού τίτλου.

6.3.1 Πίνακας Σύγκρισης Προτάσεων

Στον παρακάτω Πίνακα 6.1 συγκρίνονται οι παραπάνω προτάσεις, όπου στις γραμμές του υπάρχουν οι προτάσεις και στις στήλες του, οι διάφορες ιδιότητες των αποκεντρωμένων εφαρμογών. Πιο αναλυτικά οι στήλες είναι οι εξής:

- Το Blockchain με το οποίο λειτουργεί η πρόταση.
- Το μοντέλο συναίνεσης που χρησιμοποιείται από το Blockchain.
- Το είδος του Blockchain, δηλαδή αν είναι δημόσιο ή όχι.
- Αν ακολουθεί τους κανόνες του GDPR, δηλαδή αν δημοσιεύει κρυπτογραφημένα τα στοιχεία στο Blockchain.
- Η διαφάνεια στην διαδικασία καταχώρησης και επαλήθευσης των πτυχίων, ο τρόπος που επιτυγχάνεται και η ανάλυση τους στα άρθρα.
- Την δικλείδα ασφαλείας της επαλήθευσης των πτυχίων. Αναφέρεται στην δυνατότητα μιας εφαρμογής να επαληθεύει με δύο ή περισσότερους τρόπους του ακαδημαϊκούς τίτλους, όπως για παράδειγμα η εφαρμογή Verde εμφανίζει τα δεδομένα του φοιτητή

στην διεπαφή, το οποίο αποτελεί τον πρώτο τρόπο επαλήθευσης, αλλά εμφανίζονται με την μορφή ECTS τα tokens που αποτελούν τον δεύτερο τρόπο επαλήθευσης μιας και τα tokens έχουν όλα κοινό έξυπνο συμβόλαιο και μπορεί εύκολα να ελεγχθούν τόσο οι συναλλαγές όσο και η οντότητα που τα εκδίδει. Τέλος, το accreditation body του Cerbrus επιβλέπει κάθε δημοσίευση του ιδρύματος και ελέγχει την εγκυρότητα του, κάτι που λειτουργεί πάλι σαν δικλείδα ασφαλείας.

- Την διαπίστευση του συστήματος. Πιο συγκεκριμένα Η διαπίστευση είναι η επίσημη αναγνώριση από έναν αρμόδιο αναγνωρισμένο φορέα ο οποίος ονομάζεται οργανισμός διαπίστευσης (accreditation body).Η διαπίστευση στις παραπάνω προτάσεις είναι το φαινόμενο κατα το οποίο μια αρχή επιτρέπει στα ιδρύματα να συμμετέχουν στο δίκτυο ή στην εφαρμογή και τα στοιχεία των ιδρυμάτων επαληθεύονται από αυτήν την αρχή.

- Ο τρόπος με τον οποίο γίνεται η επαλήθευση των διπλωμάτων και αν απαιτείται η χρήση της διεύθυνσης του ψηφιακού πορτοφολιού του φοιτητή ή ένα αρχείο που διαθέτει.

- Η ικανότητα της εφαρμογής για να επιτελέσει την ανάκληση των πτυχίων.

- Πόσο φιλική είναι προς τον χρήστη η διεπαφή.

- Πόσο καλή είναι η πρόσβαση στην εφαρμογή και στον οδηγό χρήσης.

- Η προσαρμοστικότητα είναι η ιδιότητα της εφαρμογής να μπορεί να προσαρμόζεται στους πόρους που διαθέτει το ίδρυμα. Για παράδειγμα αν μπορεί η εφαρμογή να εκτελεστεί σε ένα περιβάλλον με πολύ χαμηλούς υπολογιστικούς πόρους, με απαρχαιωμένους υπολογιστές και συστήματα, με την συγκεκριμένη κατάσταση των ιδρυμάτων (δηλαδή ότι έχει αποθηκευμένα όλα τα δεδομένα των φοιτητών στην βάση δεδομένων της και πως μπορούν τα χειρόγραφα-μη-ψηφιοποιημένα πτυχία να δημοσιευτούν στο blockchain) και αν γίνεται η λειτουργικότητα της εφαρμογής να χρησιμοποιηθεί για μία παρόμοια διεργασία (π.χ αποθήκευση στοιχείων υπαλλήλων). Το τελευταίο χαρακτηριστικό που αναφέρθηκε μπορεί να επιτευχθεί με την χρήση των έξυπνων συμβολαίων.

Προτάσεις	Χαρακτηριστικά			Ιδιότητες Ασφάλειας			Ιδιότητες Συστήματος				Ευχρηστία	
	Blockchain	Μοντέλο συναίνεσης	Είδος Blockchain	GDPR	Διαφάνεια	Δικλείδα Ασφαλείας Επαλήθευσης	Διαπίστευση	Επαλήθευση	Ανάκληση	Εμπειρία χρήστη	Προσβασιμότητα	Προσαρμοστικότητα
UNIC	Bitcoin	PoW	Permissionless	Ναι	Ναι	Όχι	Όχι	Με χρήση αρχείου	Ναι,Μερικώς	Πολύ καλή	Πολύ καλή	Όχι
Blockcerts	Ethereum, Bitcoin	PoW	Permissionless	Ναι	Ναι	Όχι	Όχι	Με χρήση αρχείου	Ναι,Μερικώς	Πολύ καλή	Πολύ καλή	Ναι, Μερικώς
EchoLink	Ethereum	PoW	Permissionless	Ναι	Ναι	Όχι	Όχι	Με χρήση κλειδιού	Όχι	Καλή	Καλή	Ναι
TrueRec	Ethereum	PoW	Permissionless	Ναι	Ναι	Όχι	Ναι	Με χρήση αρχείου	Όχι	Καλή	Καλή	Όχι
UZHBC	Ethereum	PoW	Permissionless	Ναι	Ναι	Όχι	Όχι	Με χρήση αρχείου	Όχι	Πολύ καλή	Πολύ καλή	Όχι
BCDiploma	Ethereum	PoW	Permissionless	Ναι	Ναι	Όχι	Όχι	Με χρήση αρχείου	Ναι,Μερικώς	Πολύ καλή	Πολύ καλή	Ναι, Μερικώς
GRNET	Cardano	PoA	Permissioned	Ναι	Ναι	Όχι	Ναι	?	Ναι,-	?	?	Όχι
Cerberus	Ethereum (Parity)	PoA	Permissioned	Ναι	Ναι	Ναι	Ναι	Με χρήση αρχείου	Ναι,Μερικώς	Πολύ καλή	Πολύ καλή	Όχι
Blockchain4Edu	Ethereum	PoW	Permissionless	Ναι	Ναι	Όχι	Ναι	Με χρήση αρχείου	Ναι,Μερικώς	Πολύ καλή	Πολύ καλή	Ναι, Μερικώς
EduCTX	ARK	DPoS	Permissioned	Ναι	Ναι	Όχι	Ναι	Με χρήση αρχείου	Όχι	Πολύ καλή	Πολύ καλή	Όχι
Verde	Ethereum	PoW	Permissionless	Ναι	Ναι	Ναι	Ναι	Με χρήση κλειδιού	Ναι,Απόλυτα	Πολύ καλή	Πολύ καλή	Ναι

Πίνακας 6.1: Σύγκριση Προτάσεων [6, 7, 8, 9, 10, 11, 12, 13, 14, 15]

6.4 Σύγκριση στο μέσο ανάπτυξης της εφαρμογής Verde

Σε αυτήν την ενότητα θα δούμε πως η εφαρμογής Verde μπορεί να αναπτυχθεί και από άλλες πλατφόρμες blockchain που περιλαμβάνουν EVM για την εκτέλεση των έξυπνων συμβολαίων. Η επιλογή μας για την μελέτη της παραπάνω πρότασης είναι η πλατφόρμα RSK που αποτελεί sidechain του Bitcoin.

6.4.1 RSK

Στα πλαίσια της έρευνας ήταν εύλογο να αναρωτηθούμε ποια πλατφόρμα είναι καλύτερη για την δημιουργία έξυπνων συμβολαίων, την κατασκευή αποκεντρωμένων εφαρμογών, ποια έχει το πιο φιλικό για τον χρήστη (και τον προγραμματιστή) περιβάλλον για την ανάπτυξη εφαρμογών και τελικά ποια είναι η πιο οικονομική λύση. Υπάρχουν πάρα πολλές πλατφόρμες blockchain που θα μπορούσαμε να μελετήσουμε όπως το Counterparty, EOS ή ιδιωτικά blockchain όπως Hyperledger Besu/Sawtooth/Burrow. Στα πλαίσια της πτυχιακής μελετήθηκαν τα περισσότερα από τα παραπάνω σε επίπεδο πειραμάτων όμως δεν αναπτύχθηκαν. Η πλατφόρμα που διαλέξαμε είναι η πλατφόρμα RookStock - RSK και αποτελεί sidechain του Bitcoin. Το RootStock - RSK δημιουργήθηκε το 2015 και λάνσαρε το mainnet του το 2018. Το RSK είναι μια πλατφόρμα που επιτρέπει την εκτέλεση έξυπνων συμβολαίων που χρησιμοποιούν το bitcoin ως εγγενές περιουσιακό στοιχείο, επεκτείνοντας έτσι την εμβέλειά του στην χρήση από τα dApps. Το Το δίκτυο RSK έχει κάποιες βελτιώσεις σε σύγκριση με το Bitcoin, όπως γρηγορότερες συναλλαγές και καλύτερη επεκτασιμότητα. Αυτό είναι μια εξέλιξη δύο τεχνολογιών, του QixCoin (από τους ιδρυτές του RSK) και του Ethereum. Το RSK κληρονομεί πολλές βασικές έννοιες από το Ethereum, όπως τη μορφή των λογαριασμών, τη διεπαφή του VM και το web3. Από τον Ιανουάριο του 2019, το RSK αποτελεί τουλάχιστον το 40% του ρυθμού διασποράς του Bitcoin. Για να μπορέσουν οι χρήστες να χρησιμοποιούν τα Bitcoin εντός και εκτός από το RSK, αυτό διαθέτει μια αμφίδρομη(two-way-peg) λειτουργία που του επιτρέπει να αλληλεπιδρά με το Bitcoin. Όταν τα Bitcoins μεταφέρονται στο RSK blockchain, μετατρέπονται σε Smart Bitcoins (ticker RBTC1). Τα έξυπνα Bitcoin είναι ισοδύναμα με τα Bitcoin που υπάρχουν στο RSK blockchain και μπορούν να μετατραπούν ξανά σε Bitcoin οποιαδήποτε στιγμή θελήσει ο χρήστης, χωρίς επιπλέον κόστος, εκτός από τα τυπικά τέλη συναλλαγών. Το RBTC είναι το νόμισμα που χρησιμοποιείται από το RSK για την πληρωμή των miners για την επεξεργασία συναλλαγών και έξυπνων συμβολαίων. Πρέπει να διασαφηνιστεί ότι το RSK δεν εκδίδει νέο νόμισμα, όλα τα RBTC δημιουργούνται από τα Bitcoin. Το RSK περιλαμβάνει τέσσερα βασικά χαρακτηριστικά:

- Την ντετερμινιστική Τούρινγκ πλήρες εικονική μηχανή RVM. Συγκεκριμένα το RVM αποτελεί μια εκδοχή του EVM, καθώς μοιάζουν σε επίπεδο opcode για να μπορεί να

εκτελεί και τα έξυπνα συμβόλαια του Ethereum. Τα έξυπνα συμβόλαια εκτελούνται από όλους τους πλήρης κόμβους του δικτύου.

- Την αμφίδρομη λειτουργία του Sidechain του Bitcoin. Το Sidechain αποτελεί μια εκδοχή του Blockchain που το κρυπτονόμισμα του έχει σχεδόν υιοθετηθεί μονόδρομα από το Sidechain και οι συναλλαγές γίνονται με την αποθήκευση των αποδείξεων των συναλλαγών. Η αμφίδρομη υιοθέτηση (two-way peg) γίνεται όταν δύο κρυπτονομίσματα μπορούν να ανταλλαχθούν ελεύθερα, αυτόματα χωρίς την διαπραγμάτευση της τιμής των κρυπτονομισμάτων. Η λογική της λειτουργίας αυτής είναι αρκετά απλή: Όταν ένα ποσό κρυπτονομισμάτων ανταλλάσσονται από BTC σε RBTC, τότε αυτά κλειδώνονται στο δίκτυο του Bitcoin και ξεκλειδώνονται στο δίκτυο του RSK και αυτό ισχύει αμφίδρομα. Η παραπάνω λειτουργία εκτελείται με την βοήθεια μιας τρίτης οντότητας (STTP), που ονομάζεται Federation, καθώς το δίκτυο του Bitcoin δεν είναι Τούρινγκ πλήρες.

- Ένα ιδιαίτερο μοντέλο συναίνεσης, Merged mining. Το Merged mining είναι μια τεχνική που επιτρέπει στους miners να εξορύσσουν άλλα κρυπτονομίσματα, ταυτόχρονα, με σχεδόν μηδενικό οριακό κόστος. Η ίδια υποδομή εξόρυξης που χρησιμοποιείται για την εξόρυξη των Bitcoins, χρησιμοποιείται και για την εξόρυξη RSK ταυτοχρόνως. Αυτό σημαίνει ότι, καθώς το RSK επιβραβεύει τους miners με επιπλέουν τέλη συναλλαγών

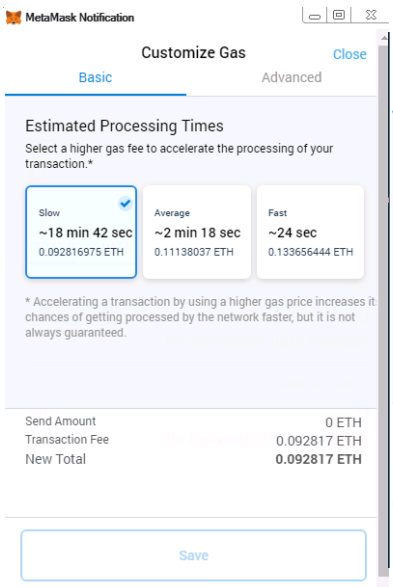
- Ένα δίκτυο χαμηλής καθυστέρησης για τις γρήγορες μεταφορές. Το συγκεκριμένο δίκτυο μοιάζει με την λειτουργία του soft fork του Bitcoin, Lightning δίκτυο. Παρόλο που διαθέτει γρήγορες off-chain συναλλαγές, προσφέρει και αρκετά γρηγορότερες on-chain συναλλαγές με την χρήση των DECOR+ και FastBlock5 πρωτοκόλλων, τα οποία επιτρέπουν την επίτευξη της δημιουργίας μπλοκ κατά μέσο όρο τα δεκαπέντε δευτερόλεπτα ώστε να μην δημιουργούνται κίνητρα για centralized - selfish mining.

Τέλος δύο επίσης πολύ σημαντικά του RSK είναι: α) οι απόρρητες συναλλαγές, με τον ίδιο τρόπο που το προσφέρει το Bitcoin, δηλαδή, την ψευδό-ανωνυμία και β) καλύτερη επεκτασιμότητα σε σχέση με το Bitcoin, καθώς χρησιμοποιεί το πρωτόκολλο LTCP το οποίο του επιτρέπει το μέγεθος κάθε συναλλαγής να είναι ίσο με το ένα πεντηκοστό με μια ίδια συναλλαγή στο Bitcoin.

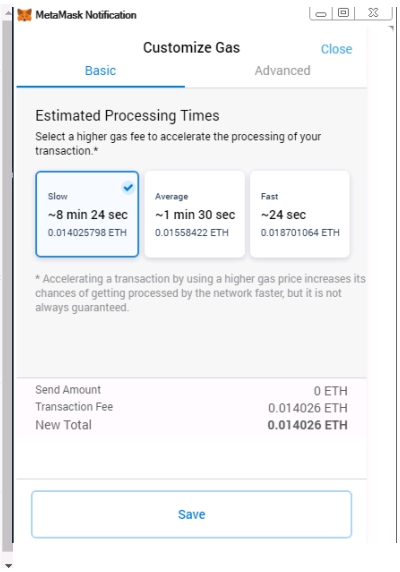
6.4.2 Σύγκριση με το Ethereum

Καθώς διαλέξαμε μια πλατφόρμα αρκετά κοντά με το Ethereum μπορούμε συγκρίνουμε αρκετές λειτουργίες και έτσι να συμπεράνουμε ποια πλατφόρμα είναι καλύτερη για την ανάπτυξη της εφαρμογής Verde. Για να μπορέσουμε να αναπτύξουμε την εφαρμογή μας στο RSK αρκεί να συνδέσουμε το Metamask με το RSK testnet[3] και να αναπτύξουμε το έξυπνο

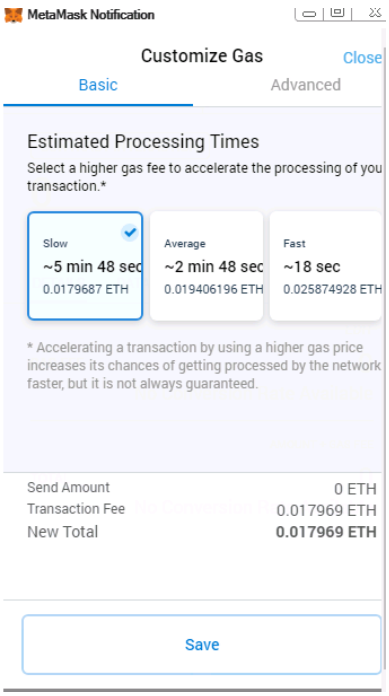
[3]περισσότερες λεπτομέρειες εδώ: https://developers.rsk.co/wallet/use/metamask/



Σχήμα 6.16: Ανάπτυξη συμβολαίου



Σχήμα 6.17: Αποστολή στοιχείων φοιτητή



Σχήμα 6.18: Αποστολή μαθημάτων φοιτητή

συμβόλαιο μέσω του remix.ethereum.org στο δίκτυο του RSK testnet. Ήδη οι πρώτες διαφορές φαίνονται από την ανάπτυξη του έξυπνου συμβολαίου στο δίκτυο. Οι παρακάτω Εικόνες 6.16, 6.17, 6.18 προέρχονται από την διεπαφή της εφαρμογής Metamask την ώρα που εκτελούνται οι εξής ενέργειες της ανάπτυξης συμβολαίου, της αποστολής των στοιχείων του φοιτητή και η αποστολή των μαθημάτων του. Το ένα RBTC ισούται με ένα BTC οπότε αφού η ανάπτυξη του συμβολαίου κοστίζει 0.09 RBTC αυτό ισούται με 746,30 ευρώ. Ενώ η αποστολή των δεδομένων του φοιτητή κοστίζουν συνολικά περίπου 0.031 RBTC δηλαδή 257 ευρώ. Επίσης, διαφορές βλέπουμε και στους χρόνους εκτελέσεις των συναλλαγών, όπου η αποστολή των δεδομένων του φοιτητή στο Ethereum θέλει περίπου 3 λεπτά ενώ στο RSK χρειάζεται περίπου 8 λεπτά, σύμφωνα πάντα με την διεπαφή του Metamask.

Το πόσο φιλικό για τον χρήστη είναι η ιστοσελίδα κρίθηκε από το πόσο εύκολο είναι να έχει πρόσβαση κάποιος σε κάποιες κατηγορίες, όπως η κατηγορία με τα ERC 20 tokens, όπου στο RSK δεν υπάρχει τέτοια δυνατότητα αλλά και από την αισθητική της σελίδας.

Από τα παραπάνω αντιλαμβανόμαστε ότι η καλύτερη επιλογή για την εφαρμογή Verde είναι το Ethereum εκτός από δύο κατηγορίες που υστερεί σε σχέση με το RSK οι οποίες είναι: α)το είδος της αλυσίδας, μιας και το RSK λειτουργεί ως το side-chain του Bitcoin που σημαίνει ότι εξοικονομεί υπολογιστική δύναμη από την κύρια αλυσίδα σε αντίθεση με τις εφαρμογές που βασίζονται στο Ethereum, και β) οι το μέγεθος του blockchain το οποίο αφορά τους πλήρης κόμβους.

Blockchains / Χαρακτηριστικά		Ethereum	RSK
Γενικά	Κρυπτονόμισμα	ETH	RBTC
	Εταιρία	Ethereum Foundation	RSK Labs
	Πλατφόρμα	Ethereum	Bitcoin
Blockchain	Μοντέλο Συναίνεσης	PoW (αναμένεται) το Casper-PoS	Merged-mining
	Συναλλαγές / δευτ.	15-25	15-25
	Δημιουργία μπλοκ / δευτ.	10-20	15-30
	Είδος αλυσίδας	κύρια	side
	Γλώσσα προγραμματισμού	Solidity	Solidity
	Συν. Μέγεθος	>1.5TB	∼2GB
Verde	Κόστος Ανάπτυξης	∼14 ευρώ	∼746 ευρώ
	Κόστος Συναλλαγής	∼6 ευρώ	∼257 ευρώ
	Εκτίμηση Χρόνου Συναλλαγής	3 λεπτά	8 λεπτά
Χρηστικότητα	Ιστοσελίδα Επαλήθευσης Συναλλαγών	etherscan.io	explorer.rsk.co
	Φιλικό προς τον Χρήστη	Πολύ καλό	Καλό

Πίνακας 6.2: Σύγκριση πλατφόρμας ανάπτυξης της εφαρμογής Verde [16, 17]

Κεφάλαιο 7

Συμπεράσματα

7.1 Συμπέρασμα

Στην παρούσα εργασία παρουσιάστηκε η τεχνολογία blockchain, η δομή της και τα συστατικά της στοιχεία, η κρυπτογραφία πίσω από το blockchain με τη βοήθεια λογισμικού ανοιχτού κώδικα Sage, οι χρήσεις του blockchain σήμερα, καθώς και ένα παράδειγμα πρόληψης κατά της πλαστογραφίας πανεπιστημιακών πτυχίων. Η παρούσα εργασία είχε και διδακτικό σκοπό, καθώς η ελληνική βιβλιογραφία είναι ακόμα σε αρχικό στάδιο. Μέσω αυτής της εργασίας έγιναν κατανοητά το τι σημαίνει blockchain, πως μοιάζει ένα blockchain στην πράξη και γιατί είναι τόσο ασφαλές να το χρησιμοποιήσει κάποιος, τα διάφορα blockchain που υπάρχουν σήμερα και είναι ευρέως γνωστά και αξίζουν στο χρηματηστήριο πάνω από 100 δις δολάρια[1]. Η συγκεκριμένη εργασία δεν μελετήθηκε μόνο θεωρητικά αλλά και πρακτικά με τη δημιουργία της εφαρμογής Verde. Είχε ως σκοπό τη σφαιρική κατανόηση των δικτύων blockchain και να δείξει ότι είναι μια τεχνολογία που θα φέρει μια νέα τεχνολογική επανάσταση, καθώς και να ερευνήσει μέσω της σύγκρισης τα μοντέλα συναίνεσης, τις εφαρμογές επαλήθευσης ακαδημαϊκών τίτλων με την εφαρμογή Verde και την σύγκριση της πλατφόρμας ανάπτυξης της εφαρμογής μας.

Το ενδιαφέρον της παρούσας εργασίας εντοπίζεται τόσο από τη σκοπιά και από την επιστήμη της Κρυπτογραφίας και των μαθηματικών, όσο και από τη σκοπιά της επιστήμης των Υπολογιστών και Μηχανικής. Ανακεφαλαιώνοντας, έγινε προσπάθεια της παρουσίασης της αρχιτεκτονικής του blockchain καθώς και σε ποιες τεχνολογίες βασίζεται αυτό, στη συνέχεια έγινε προσπάθεια υλοποίησης μιας αποκεντρωμένης εφαρμογής, ώστε να αποδείξουμε ότι δεν είναι μια θεωρητική τεχνολογία, αλλά πρακτική και εύχρηστη. Παράλληλα χρησιμοποιήθηκε κώδικας ανοιχτού λογισμικού για την απόδειξη των κρυπτογραφικών στοιχείων του blockchain. Αυτή η εργασία μπορεί να αποτελέσει εγχειρίδιο μελέτης και έρευνας της τεχνολογίας blockchain της οποίας αναλύθηκε τόσο η κρυπτογραφία της στο Sage, η δομή της και τα επίπεδα της, ο κώδικας Solidity που χρησιμοποιήθηκε για την ανάπτυξη

[1] πηγή: coinmarketcap.com/currencies/bitcoin/

της αποκεντρωμένης εφαρμογή, όσο και η έρευνα με την μέθοδο της σύγκρισης που πραγματοποιήθηκε για καίριες τεχνολογίες στο blockchain. Έτσι έγινε κατανοητό το θεωρητικό κομμάτι αυτής της τεχνολογίας, σε συνδυασμό με τα μαθηματικά που προκύπτουν από την κρυπτογραφία και με την προγραμματιστική του υλοποίηση σε υπολογιστικό περιβάλλον, για τη μέγιστη και πρακτικότερη κατανόησή τους.

7.2 Μελλοντικές προοπτικές έρευνας

Η παρούσα μελέτη εστίασε γενικά στην τεχνολογία blockchain, μια καινούργια τεχνολογία που έχει μελλοντικές προοπτικές, καθώς θα είναι μια τεχνολογία που θα επιβιώσει και θα ακμάσει μακροπρόθεσμα. Είναι πολύ σημαντικό ότι παράλληλα με την ανάπτυξη των IOT συστημάτων ή την ανάπτυξη της τεχνολογίας των μεγάλων δεδομένων και της τεχνητής νοημοσύνης, αναπτύσσονται και οι κβαντικοί υπολογιστές που θα μετατρέψουν την επιστήμη των υπολογιστών σε μια νέα επιστήμη μιας, και θα είναι κάτι πολύ διαφορετικό με αυτό που υπάρχει σήμερα. Η ανάπτυξη των κβαντικών υπολογιστών θα καταργήσει πολλά κρυπτοσυστήματα που γνωρίζουμε σήμερα, καθώς η παραγοντοποίηση μεγάλων ακέραιων αριθμών θα γίνεται σε δευτερόλεπτα, άρα το κρυπτοσύστημα του RSA δεν θα υφίσταται πλέον, ενώ το ίδιο θα συμβεί και στις ελλειπτικές καμπύλες. Παρόλο που η εξέλιξη των κβαντικών υπολογιστών θα φέρει καινούργια δεδομένα στην επιστήμη της πληροφορικής και της κρυπτογραφίας, δεν ισχύει το ίδιο για τη τεχνολογία blockchain, μιας και ο πυρήνας της βασίζεται στον κρυπταλγόριθμο SHA−256. Πιο συγκεκριμένα, ο αλγόριθμος του Grover[2] μπορεί να χρησιμοποιηθεί, για να βρει μια σύγκρουση σε μια συνάρτηση διασποράς σε βήματα τετραγωνικής ρίζας του αρχικού μήκους της. Συνεπώς ένα κρυπτοκείμενο το οποίο έχει μήκος 2^{256}, πλέον θα έχει μήκος 2^{128} [67]. Άρα, θα παραμείνει ασφαλές μιας και ένα κρυπτοκείμενο με μήκος 2^{128} απαιτεί αρκετό χρόνο για την αποκρυπτογράφηση του.

Η επιπλέον μελέτη έχει ως στόχο να διευρυνθεί και να συγκριθεί από προγραμματιστική οπτική το κατά πόσο μπορεί να βελτιωθεί η εφαρμογή Verde, ώστε να σταθεί από μόνη της ως μια πλέον εμπορική εφαρμογή και κατά πόσο είναι ασφαλές να χρησιμοποιηθεί από μια κρατική μηχανή. Αρχικά, θα πρέπει να μελετηθεί από την πλευρά της ασφάλειας των έξυπνων συμβολαίων για το κατά πόσο είναι απαραβίαστο και ανθεκτικό από επιθέσεις. Η ασφάλεια των έξυπνων συμβολαίων είναι μια πολύ καινούργια μελέτη που ακόμα βρίσκεται σε πολύ αρχικό στάδιο [68]. Ένα παράδειγμα αδυναμίας στο έξυπνο συμβόλαιο της εφαρμογής Verde είναι οι δύο συναρτήσεις καταχώρησης των δεδομένων των στοιχείων των φοιτητών και των μαθημάτων τους. Το πρόβλημα στις δύο συναρτήσεις αυτές είναι ότι, μπορεί να γεμίσει με δεδομένα μία από τις δύο συναρτήσεις χωρίς να υπάρχει κατάλληλη ενημέρωση στην άλλη, οπότε αν μετά το πρώτο οκ της αποστολής των στοιχείων του φοιτητή στο blockchain ακυρωθεί η δεύτερη συναλλαγή, τότε η επαλήθευση των δεδομένων θα είναι άκυρη. Επίσης,

[2] περισσότερες πληροφορίες, *en.wikipedia.org/wiki/Grover's_algorithm*

έχουν βρεθεί αδυναμίες στο έξυπνο συμβόλαιο του ERC20 token που θα πρέπει να διερευνηθούν στο μέλλον [69]. Από την άλλη, υπάρχουν αδυναμίες και σε επίπεδο διεπαφών. Η κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων των φοιτητών γίνεται στις διεπαφές με ένα συγκεκριμένο εργαλείο το οποίο το διαχειρίζεται μία τρίτη οντότητα, άγνωστη προς τα εμάς. Επίσης, το εργαλείο που κάνει δυσανάγνωστο τον κώδικα Javascript της διεπαφής, για να μην μπορεί κάποιος να μαντέψει εύκολα τον τρόπο που γίνεται η αποκρυπτογράφηση των δεδομένων των φοιτητών, δεν είναι και η πιο βέλτιστη λύση, καθώς πάλι μπορεί κάποιος να αναλύσει τον κώδικα και να τον μετατρέψει σε ευανάγνωστο κώδικα, αν το θέλει πραγματικά. Η λύση σε αυτό το πρόβλημα είναι να μπει και δεύτερο κλειδί (πχ το ιδιωτικό κλειδί του χρήστη) που θα το έχει μόνο ο χρήστης και κάθε φορά που θα θέλει να επαληθεύσει κάποιος το πτυχίο του, θα πρέπει να διαθέτει και το δημόσιο και το ιδιωτικό κλειδί, γιατί η κρυπτογράφηση τους θα γίνεται με την σύνοψη των δύο αυτών κλειδιών.

Αναφορικά με την τεχνολογία blockchain υπάρχουν πολλά που θα μπορούσαν να μελετηθούν στο μέλλον και να ερευνηθούν περισσότερο. Το blockchain χρησιμοποιεί ένα ευρύ φάσμα ιδεών και αρχών της μηχανικής λογισμικού και της επιστήμης των υπολογιστών, όπως οι συναρτήσεις διασποράς, δομές δεδομένων, αποθήκευση δεδομένων, κρυπτογραφία, αρχιτεκτονικές δικτύων, επικοινωνία μεταξύ υπολογιστών και υπολογιστικά παζλ. Κάθε μία από αυτές τις έννοιες και τεχνολογίες υπήρξε και εξακολουθεί να είναι αντικείμενο της έρευνας. Ως αποτέλεσμα αυτού, μπορούν να δημιουργηθούν διαφορετικές εκδοχές του blockchain μόνο με τη χρήση διαφορετικών συναρτήσεων διασποράς, κρυπτογραφικών μεθόδων για τη δημιουργία κλειδιών ή υπολογιστικών παζλ που χρησιμοποιούνται κατά την τεκμηρίωση της εργασίας [23].

Το βασικότερο πρόβλημα που αντιμετωπίζει η τεχνολογία αυτή είναι η επεκτασιμότητα της αλυσίδας. Ήδη μέχρι σήμερα η αλυσίδα με τους πλήρεις κόμβους έχει φτάσει στο μέγεθος της τάξεως των 3,6 TB [3]. Είναι ένα μέγεθος μη αμελητέο, το οποίο αυξάνεται καθημερινά με γραμμική πρόοδο. Ήδη έχουν ξεκινήσει έρευνες πάνω σε αυτό το πρόβλημα με λύσεις όπως οι παράλληλες αλυσίδες, ώστε να μειωθεί ο όγκος των δεδομένων στην κύρια αλυσίδα [70]. Μία λύση σε αυτό το πρόβλημα είναι μέσω των side-chains, ώστε οι απολύτως απαραίτητες πληροφορίες να καταγράφονται στο κυρίως δίκτυο (πχ RSK και Plasma [71]).

Το πρόβλημα της καταπάτησης των προσωπικών δεδομένων και η αμφιβολία που απορρέει από το blockchain για το αν είναι απολύτως νόμιμο, απασχολεί έντονα τους νομικούς. Στην επιστήμη της πληροφορίας οι χρήστες πρέπει να έχουν την ιδιωτικότητά τους προστατευμένη, κάτι στο οποίο η τεχνολογία blockchain επιδέχεται βελτιώσεις, καθώς βασίζεται στην ιδέα ότι όλοι έχουν πρόσβαση στο ιστορικό των συναλλαγών του καθενός για να νομιμοποιείται η επόμενη συναλλαγή. Τα ιδιωτικά blockchain περιορίζουν την πρόσβαση ανάγνωσης και ως εκ τούτου δεν μπορούν πλέον να χρησιμοποιηθούν από όλους, για να αποσαφηνίσουν την ιδιοκτησία βάσει του ιστορικού των δεδομένων συναλλαγών [23]. Μια άλλη προσέγγιση είναι η *μηδενική απόδειξη γνώσης* (zero-proof knowledge), η οποία επιτρέπει στον οποιοδήποτε να

[3] η ενημερωμένη εκδοχή αυτού του νούμερου στο https://etherscan.io/chartsync/chainarchive

αποδείξει την ορθότητα των συναλλαγών του, χωρίς να έχει πλήρη πρόσβαση στα δεδομένα [23].

Τέλος, αυτό που ενδιαφέρει περισσότερο τους κόμβους σε ένα δίκτυο blockchain είναι το μοντέλο συναίνεσης κάτω από το οποίο θα πρέπει να συμφωνούν και να τηρούν όλοι. Το καλύτερο μοντέλο βρίσκεται ακόμα υπό έρευνα και μελέτη, μιας και ακόμα δεν έχει ανακαλυφθεί. Η απόδειξη της εργασίας φάνηκε στην αρχή ότι είναι μια καλή πρακτική, που εφαρμόζεται σε ένα δίκτυο στο οποίο κανένας κόμβος δεν έχει εμπιστοσύνη στον άλλον και διανέμει τα κέρδη δίκαια σε αυτούς που εργάστηκαν πραγματικά την πραγματοποίηση μιας συναλλαγής. Όμως, το πρόβλημα δημιουργήθηκε με την υπερ-κατανάλωση ενέργειας που προκαλεί αυτό το μοντέλο, καθώς πρέπει οι μηχανές να δουλεύουν συνεχώς σε υψηλές αποδόσεις. Δημιουργεί, έτσι, ένα περιβαλλοντολογικό αποτύπωμα πολύ μεγάλο για έναν πλανήτη ήδη βεβαρημένο με την κλιματική καταστροφή. Η εναλλακτική αυτού του μοντέλου είναι η Απόδειξη Συμμετοχής που φαίνεται ως μια καλή πρακτική σε σχέση με την Απόδειξη Εργασίας, όμως υπάρχουν ακόμα προκλήσεις που περιγράφηκαν σε αυτήν τη μελέτη που πρέπει να διερευνηθούν. Εντελώς διαφορετικοί αλγόριθμοι για την εξεύρεση συναίνεσης είναι τα μοντέλα Paxos [72] και Raft [73]. Αναπτύχθηκαν πολύ πριν από την εμφάνιση του blockchain [23]. Μία σημαντική πρόκληση με τους εναλλακτικούς μηχανισμούς συναίνεσης είναι ότι είναι συχνά εννοιολογικά πιο περίπλοκοι και επομένως πιο δύσκολο να αποδειχθούν επίσημα. Εάν υπάρχει ένα ελάττωμα σε επίπεδο θεωρίας παιγνίων σε αυτά, τότε θα μπορούσε να καταστρέψει το blockchain και ως εκ τούτου θα κλονίσει την εμπιστοσύνη σε αυτό [23].

Το μέλλον επιφυλάσσει πολλά, το μόνο σίγουρο είναι ότι η τεχνολογία του blockchain ανάγεται σε αυτό. Ήδη τα πιο ανεπτυγμένα κράτη έχουν αρχίσει να υιοθετούν την ιδέα του blockchain και να την υλοποιούν σε πολλές περιπτώσεις. Χαρακτηριστικό παράδειγμα αποτελεί η Γερμανία που εξέδωσε επίσημη ανακοίνωση για τα επόμενα βήματα που θα κάνει για τη δημιουργία μιας οικονομίας που θα συμπεριλαμβάνει τα κρυπτονομίσματα[4].

Κατά συνέπεια η περαιτέρω έρευνα είναι απαραίτητη, ώστε να επιλυθούν όλα τα ζητήματα που προκύπτουν στο blockchain και να οδηγήσουν σε μια τεχνολογία που θα μπορεί να χρησιμοποιηθεί ευρέως και να καταστεί όσον το δυνατόν πιο αποδοτική.

[4]περισσότερελες λεπτομέρειες για την ανακοίνωση, www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/blockchain-strategy.pdf

Παράρτημα Α΄

Πίνακας ορολογίας

Ορολογία	Μετάφραση	Σχόλια
Blockchain Technology	Τεχνολογία Επάλληλων Μπλοκ	
nonce	Τυχαίος αριθμός μοναδικής χρήσης	
Proof of Stake	Απόδειξη Συμμετοχής	
Consensus Model	Μοντέλο Συναίνεσης	
Proof of Burn	Απόδειξη Καύσης ή Καταστροφής	
Proof of Importance	Απόδειξη Σπουδαιότητας	
Ether	Αιθέριο	όμοια με το δολάριο
Ledger	Κατάστιχο	
Mining	Εξόρυξη	
Wallet	Ψηφιακό Πορτοφόλι	
Smart Contract	Έξυπνο Συμβόλαιο	
Gas	Αέριο	
Hash Functions	Συναρτήσεις Διασποράς	
Ethereum Virtual Machine	Εικονική Μηχανή Ethereum	
Decentralized Application	Αποκεντρωμένη Εφαρμογή	
Centralized Application	Κεντροποιημένη Εφαρμογή	Εφαρμογή που ποιήθηκε με κέντρο
Cryptocurrency	Κρυπτονόμισμα	
Forking	Διακλάδωση	

Πίνακας Α΄.1: Πίνακας μετάφρασης

Bibliography

[1] Dylan Yaga-Peter Mell-Nik Roby-Karen Scarfone, "Blockchain technology overview," *NISTIR 8202*, January 2018.

[2] Nutthakorn Chalaemwongwan Werasak Kurutach, "State of the art and challenges facing consensus protocols on blockchain," 2018.

[3] SlimCoin, "A peer-to-peer crypto-currency with proof-of-burn,mining without powerful hardware," 2014.

[4] https://fair-coin.org/en/faircoin-2-revision-one-most-promising cryptocurrencies, "Faircoin whitepaper," .

[5] nem.io, "Technical reference," 2018.

[6] Konstantinos Karasavvas, "Revoking Records in an Immutable Ledger: A Platform for Issuing and Revoking Official Documents on Public Blockchains," in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, Zug, June 2018, pp. 105–111, IEEE.

[7] Marco Baldi, Franco Chiaraluce, Migelan Kodra, and Luca Spalazzi, "Security analysis of a blockchain-based protocol for the certification of academic credentials," *arXiv:1910.04622 [cs]*, Oct. 2019, arXiv: 1910.04622.

[8] Steve X Chen and EchoLink Team, "Building A High-Trust Economy," p. 22.

[9] "Meet TrueRec by SAP: Trusted Digital Credentials Powered by Blockchain," July 2017, Library Catalog: news.sap.com Section: Industries.

[10] Jerinas Gresch, Bruno Rodrigues, Eder Scheid, Salil S. Kanhere, and Burkhard Stiller, "The Proposal of a Blockchain-Based Architecture for Transparent Certificate Handling," in *Business Information Systems Workshops*, Witold Abramowicz and Adrian Paschke, Eds., vol. 339. Springer International Publishing, Cham, 2019, Series Title: Lecture Notes in Business Information Processing.

[11] Dimitris Mitropoulos, "Grnet," .

[12] Aamna Tariq, Hina Binte Haq, and Syed Taha Ali, "Cerberus: A Blockchain-Based Accreditation and Degree Verification System," *arXiv:1912.06812 [cs]*, Dec. 2019, arXiv: 1912.06812.

[13] "Bcdiploma," .

[14] Wolfgang Gräther, Sabine Kolvenbach, Rudolf Ruland, Julian Schütte, Christof Torres, and Florian Wendland, "Blockchain for Education: Lifelong Learning Passport," 2018, Publisher: European Society for Socially Embedded Technologies (EUSSET).

[15] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "Eductx: A blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112–5127, 2018.

[16] Sergio Demian Lerner, "Rsk bitcoin powered smart contracts," 2019.

[17] "Smart Contract Platforms Comparison: RSK vs Ethereum vs EOS vs Cardano," Library Catalog: blockgeeks.com.

[18] Gavin Wood Andreas M. Antonopoulos Dr, *Mastering Ethereum*, O'Reilly.

[19] Leslie Lamport, "The part-time parliament," *ACM Trans. Comput. Syst.*, vol. 16, no. 2, pp. 133–169, May 1998.

[20] Dylan Yaga Peter Mell Nik Roby Karen Scarfone, "Blockchain technology overview," *NISTIR 8202*, October 2018.

[21] Leslie Lamport, Robert Shostak, and Marshall Pease, "The Byzantine Generals Problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 20.

[22] Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009.

[23] Daniel Drescher, *BLOCKCHAIN BASICS A NON-TECHNICAL INTRODUCTION IN 25 STEPS*, Apress, 2017.

[24] "Dieythynths klinikhs xeiroyrgoyse gia xronia xwris ptyxio," http://newpost.gr/ellada/500068/dieythynths-klinikhs-xeiroyrgoyse-gia-xronia-xwris-ptyxio.

[25] "Sto elegktiko synedrio h epistrofh apodoxwn noshleytrias gia plasto ptyxio | Kathimerini," https://www.kathimerini.gr/1063512/article/epikairothta/ellada/sto-elegktiko-synedrio-h-epistrofh-apodoxwn-noshleytrias-gia-plasto-ptyxio.

[26] "To stithoskopio den kanei ton giatro | Kathimerini," https://www.kathimerini.gr/770855/article/epikairothta/ellada/to-sth8oskopio-den-kanei-ton-giatro.

[27] Eleftheria, "Messinia 10 mines fylakisi giati eixe plasto ptyxio!," https://eleftheriaonline.gr/local/koinonia/dikastiko/item/125650-messinia-10-mines-fylakisi-giati-eixe-plasto-ptyxio.

[28] Lawrence C. Washington Wade Trappe, *Introduction to Cryptography with Coding Theory*, Pearson.

[29] H. Knebl H. Delfs, *Introduction to Cryptography - Principles and Applications*, Springer.

[30] ΓΧ Κάτος, ΒΑ Στεφανίδης, "Τεχνικές κρυπτογραφίας και κρυπτανάλυσης," *Εκδόσεις Ζυγός*, 2003.

[31] Alasdair McAndrew, *Introduction to Cryptography with Open-Source Software*, CRC Press, 2011.

[32] Christof Paar Jan Pelzl, *Understanding Cryptography*, Springer, 2010.

[33] L.C. Washington W. Trappe, *Introduction to Cryptography with Coding Theory*, Pearson.

[34] Andreas M. Antonopoulos, *Mastering Bitcoin*, O'Reilly.

[35] Darrel Hankerson, Alfred J Menezes, and Scott Vanstone, *Guide to elliptic curve cryptography*, Springer Science & Business Media, 2006.

[36] Lawrence C Washington, *Elliptic curves: number theory and cryptography*, CRC press, 2008.

[37] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, vol. 84, Springer Science & Business Media, 2013.

[38] Vicente Munoz, "Everyday cryptography: fundamental principles and applications [book review]," 2013.

[39] William Stein, *Elementary number theory: primes, congruences, and secrets: a computational approach*, Springer Science & Business Media, 2008.

[40] Imran Bashir, *Mastering Blockchain*, Packt, 2018.

[41] https://en.bitcoin.it/wiki/Secp256k1, "Secp256k1," .

[42] DR. GAVIN WOOD, "Ethereum - a secure decentralised generalised transaction ledger byzantium version," 2019.

[43] Priyansu Sekhar Panda Bikramaditya Singhal, Gautam Dhameja, *Beginning Blockchain*, Apress, 2018.

[44] Dionysis Zindros1 Kostis Karantias, Aggelos Kiayias1, "Proof-of-burn," 2019.

[45] "PoET 1.0 Specification — Sawtooth v1.0.5 documentation," https://sawtooth.hyperledger.org/docs/core/releases/1.0/architecture/poet.html.

[46] S. Zhang and J. Lee, "Double-spending with a sybil attack in the bitcoin decentralized network," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 10, pp. 5715–5722, 2019.

[47] R. Stockton Gaines-Leslie Lamport, "Time, clocks, and theordering of events in a distributed system," 1978.

[48] Roberto Tonelli, Giuseppe Destefanis, Michele Marchesi, and Marco Ortu, "Smart Contracts Software Metrics: a First Study," *arXiv:1802.01517 [cs]*, Feb. 2018, arXiv: 1802.01517.

[49] "ERC20 Token Standard – Ethereum Smart Contracts – BitcoinWiki," .

[50] "Go Ethereum," https://geth.ethereum.org/.

[51] "Introduction metamask docs," https://docs.metamask.io/guide/#why-metamask.

[52] Rozenfeld Monica, "Five surprising applications of blockchain technology.," 13 Aug. 2018.

[53] Kirill Kuvshinov, Ilya Nikiforov, Jonn Mostovoy, Dmitry Mukhutdinov, and Vladislav Podtelkin, "Disciplina: Blockchain for Education," p. 17.

[54] Daniel Zinca and Vlad-Andrei Negrean, "Development of a Road Tax Payment Application using the Ethereum Platform," in *2018 International Symposium on Electronics and Telecommunications (ISETC)*, Timisoara, Nov. 2018, pp. 1–4, IEEE.

[55] "Ethereum (ETH) price, charts, market cap, and other metrics," .

[56] "brix/crypto-js," May 2020, original-date: 2013-04-08T20:16:40Z.

[57] "Formatic," Library Catalog: docs.fortmatic.com.

[58] "javascript-obfuscator/javascript-obfuscator," May 2020, original-date: 2016-05-09T08:16:53Z.

[59] "Blockchain Certificate Validation," .

[60] "blockchain-certificates/cert-issuer," .

[61] "Customer Story FSMB | Hyland Credentials," .

[62] "Blockchain for Vocational Training Certification:," Library Catalog: www.hylandcredentials.com.

[63] "Cardano Blockchain's First Use Case: Proof of University Diplomas in Greece," .

[64] "European self sovereign identity framework," .

[65] "Zero-knowledge proof," Apr. 2020, Page Version ID: 953938349.

[66] "IPFS Documentation," Library Catalog: docs.ipfs.io.

[67] Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, and Audun Jøsang, "The Impact of Quantum Computing on Present Cryptography," *ijacsa*, vol. 9, no. 3, 2018, arXiv: 1804.00200.

[68] Sarwar Sayeed, Hector Marco-Gisbert, and Tom Caira, "Smart Contract: Attacks and Protections," *IEEE Access*, vol. 8, pp. 24416–24427, 2020.

[69] "sec-bit/awesome-buggy-erc20-tokens," May 2020, original-date: 2018-06-16T01:39:18Z.

[70] Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Sirer, Dawn Song, and Roger Wattenhofer, "On scaling decentralized blockchains (a position paper)," 02 2016.

[71] Georgios Konstantopoulos, "Plasma cash: Towards more efficient plasma constructions," 2019.

[72] Leslie Lamport, "The part-time parliament," *ACM Trans. Comput. Syst.*, vol. 16, no. 2, pp. 133–169, May 1998.

[73] Diego Ongaro and John Ousterhout, "In search of an understandable consensus algorithm," p. 305–320, 2014.