Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Πολλαπλοί Τρόποι Λειτουργίας Συστημάτων Κρυπτονομίσματος

Πλούταρχος Παπαγεωργίου

Επιβλέπων Καθηγητής
Νικόλαος Σκλάβος

Μάιος 2021

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Πολλαπλοί Τρόποι Λειτουργίας Συστημάτων Κρυπτονομίσματος

Πλούταρχος Παπαγεωργίου

Επιβλέπων Καθηγητής
Νικόλαος Σκλάβος

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2021

Περίληψη

Το θέμα των κρυπτονομισμάτων αποτελεί ένα φλέγον ζήτημα τα τελευταία χρόνια, αφού μετά το 2018 και την εκτόξευση της τιμής τους, προσέλκυσε τόσο το ενδιαφέρον νέων αγοραστών, όσο και το ερευνητικό ενδιαφέρον. Ακολούθησαν πολλές έρευνες και μελέτες πάνω στην κύρια ιδέα πίσω από ένα τέτοιο σύστημα, δηλαδή την αλυσίδα συστοιχιών και την αποκέντρωση του συστήματος. Ωστόσο, δεν φαίνεται να ερευνήθηκε αρκετά μια άλλη πτυχή των συστημάτων κρυπτονομίσματος, η οποία τους επιδίδει ευκαμψία στους συμμετέχοντες και εξοικονόμηση χώρου και χρόνου. Αυτή είναι το πρωτόκολλο πολλαπλών τρόπων λειτουργίας, το οποίο στην ουσία επιτρέπει στους κόμβους που απαρτίζουν ένα δίκτυο κρυπτονομίσματος να λειτουργήσουν πέραν της πλήρης λειτουργίας και σε κάποιο είδος ελαφριάς λειτουργίας. Αν και όλα τα συστήματα κρυπτονομίσματος βασίζονται πάνω στις ίδιες αρχές, το καθένα από αυτά λειτουργεί με τις δικές του διαφοροποιήσεις. Στην παρούσα μεταπτυχιακή διπλωματική, αρχικά επεξηγούνται κάποιες βασικές κρυπτογραφικές έννοιες που συναντιόνται καθ' όλη τη διάρκεια αυτής, σαν εισαγωγή για τον αναγνώστη που δεν έχει έρθει σε επαφή με τις έννοιες αυτές. Στη συνέχεια, αναλύονται σε ξεχωριστά κεφάλαια η λειτουργία του Bitcoin και του Ethereum. Όπου υπάρχει διαφορά είτε στους αλγόριθμους που χρησιμοποιούνται, ή στον τρόπο λειτουργίας, επισημαίνεται εντός του κεφαλαίου του Ethereum. Ακολουθεί το κεφάλαιο του πολλαπλού τρόπου λειτουργίας, στο οποίο επεξηγείται γενικότερα πως ένα σύστημα κρυπτονομίσματος μπορεί να εξυπηρετεί τον ίδια σκοπό, απαρτιζόμενο τόσο από πλήρης κόμβους που αποθηκεύουν όλα τα δεδομένα, όσο και από ελαφριούς κόμβους. Επίσης αναλύεται πως ένας κόμβος σε ελαφριά λειτουργία μπορεί να εκτελέσει τις ίδιες εργασίες με ένα σε πλήρη λειτουργία και γίνεται αναφορά στο πως λειτουργεί αυτό στο Bitcoin και στο Ethereum. Το τελευταίο μέρος της μεταπτυχιακής διατριβής απεικονίζει γραφικά στην απλούστατη του μορφή, πως ένας ελαφρύς κόμβος εκτελεί τις ίδιες λειτουργίες με ένα πλήρη κόμβο.

Summary

The issue of cryptocurrencies has been a burning issue in recent years, as after 2018 and the explosion of their price, it attracted both new buyers and research interest. Many pieces of research and studies followed on the main idea behind such a system, namely the blockchain and the decentralization of the system. However, another aspect of cryptocurrency systems does not seem to have been sufficiently explored, which gives participants flexibility and limits space and time. This is the multi-mode protocol, which essentially allows the nodes that make up a cryptocurrency network to operate either in full mode or in some kind of light mode. Although all cryptocurrency systems are based on the same principles, each one operates in its own way. Firstly, some basic cryptographic concepts are explained, which are encountered throughout this postgraduate thesis. This acts as an introduction for a reader who has not come into contact with these concepts before. Then, the operation of Bitcoin and Ethereum are analyzed in separate chapters. Where there is a difference in either the algorithms used or the mode of operation, it is highlighted and explained within the chapter of Ethereum. This is followed by the chapter on multi-mode operation, which generally explains how a cryptocurrency system can serve the same purpose, consisting of both light and full nodes. It also analyzes how a node in light mode can perform the same tasks as one in full mode and mentions how this works in Bitcoin and Ethereum. The last part of the postgraduate thesis illustrates graphically using a program written in the Java programming language, how any lightweight node can execute the same tasks as any full node.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω αρχικά τον επιβλέπων καθηγητή μου Δρ. Νικόλαο Σκλάβο, καθώς η καθοδήγησή του και οι παροτρύνσεις του ήταν ζωτικής σημασίας. Με καθοδήγησε καθ' όλη τη διάρκεια της συγγραφής της μεταπτυχιακής διπλωματικής και συνέβαλε σημαντικά στον ορθή εκπόνησή της.

Ολοκληρώνοντας τις σπουδές μου ευχαριστώ την οικογένειά μου η οποίοι με στήριξε καθ' όλη τη διάρκεια τόσο του μεταπτυχιακού μου στην Ασφάλεια Υπολογιστών και Δικτύων, όσο και των σπουδών μου γενικότερα. Ιδιαίτερα θα ήθελα να ευχαριστήσω τη γυναίκα μου Άντρεα, η οποία ήταν πάντα δίπλα μου και έδειξε υπομονή και πίστη προς εμένα.

Τέλος, θα ήθελα να ευχαριστήσω το φίλο μου Αντρέα, ο οποίοι συνέβαλε σημαντικά στην υλοποίηση του τελευταίου μέρους της μεταπτυχιακής. Είχα τη βοήθειά του όπου χρειάστηκε, η οποία σε πολλές περιπτώσεις ήταν καταλυτική.

Με εκτίμηση,

Πλούταρχος Παπαγεωργίου

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Το θέμα των συστημάτων κρυπτονομίσματος είναι ένα φλέγον ζήτημα της τελευταίας δεκαετίας, ιδιαίτερα μετά το 2018. Η εκτόξευση της τιμής τους τη χρονιά αυτή, προσέλκυσε τόσο το ενδιαφέρον νέων αγοραστών, όσο και το ανανεωμένο ερευνητικό ενδιαφέρον. Επακόλουθα, έγιναν πολλές μελέτες για τη λειτουργία των κρυπτονομισμάτων γενικότερα, με πρωταγωνιστή το Bitcoin και τα υπόλοιπα κρυπτονομίσματα να ακολουθούν την πορεία που χάραξε ο Satoshi Nakamoto το 2009.

Ως πρώτο μέρος της παρούσας μεταπτυχιακής διπλωματικής, αναλύονται με βάση τις πιο σύγχρονες βιβλιογραφικές πηγές δύο από τα πιο ολοκληρωμένα και διαδεδομένα συστήματα κρυπτονομίσματος. Αρχικά αναλύεται η λειτουργία του Bitcoin, το οποίο εισήγαγε την τεχνολογία της αλυσίδας συστοιχιών στον κόσμο και την ιδέα ενός τελείως αποκεντρωτικού συστήματος κρυπτονομίσματος που δεν εξαρτάται από μια κεντρική οντότητα, αλλά βασίζει την ασφάλειά του σε όλους τους κόμβους που το απαρτίζουν. Στη συνέχεια αναλύεται το Ethereum, το οποίο λειτουργεί διαφορετικά σε κάποιες πτυχές του, ωστόσο ακολουθεί σταθερά το δρόμο που χάραξε το Bitcoin. Στο ίδια Κεφάλαιο επίσης, γίνεται σύγκριση μεταξύ των δύο συστημάτων κρυπτονομίσματος, αναλύονται οι ομοιότητες, εξερευνιούνται οι διαφορές τους και πως αυτές επηρεάζουν την ασφάλεια και την απόδοσή τους.

Το δεύτερο μέρος της μεταπτυχιακής διπλωματικής, αφορά τα πρωτόκολλα πολλαπλών τρόπων λειτουργίας, στα οποία ένα σύστημα κρυπτονομίσματος απαρτίζεται από πλήρης κόμβους και κόμβους σε ελαφριά λειτουργία. Επίσης αποτελεί τον κύριο λόγο που επιλέχθηκαν τα δύο συγκεκριμένα συστήματα κρυπτονομίσματος προς ανάλυση. Οι πολλαπλοί τρόποι λειτουργίας χρησιμοποιούνται τόσο στο Bitcoin, όσο και στο Ethereum και έτσι αποτελούν το καταλληλότερο παράδειγμα αφού χρησιμοποιήθηκαν σε αυτά με επιτυχία για αρκετά χρόνια. Ένας κόμβος που λειτουργεί σε πλήρης λειτουργία, επεξεργάζεται και αποθηκεύει όλα τα δεδομένα του συστήματος κρυπτονομίσματος. Αντιθέτως, ένας κόμβος σε οποιαδήποτε μορφής ελαφριά λειτουργία, αποθηκεύει λιγότερο όγκο δεδομένων και επεξεργάζεται μόνο τα άκρως απαραίτητα για τη δική του λειτουργία. Ως αποτέλεσμα, οι ελαφριοί κόμβοι έχουν

λιγότερες απαιτήσεις σε ενέργεια και υπολογιστική ισχύ και έτσι μπορούν να τρέξουν και σε συσκευές όπως κινητά τηλέφωνα, tablets, κλπ.

Αφού αναλυθεί το θεωρητικό υπόβαθρο του πολλαπλού τρόπου λειτουργίας, ακολουθεί το τελευταίο μέρος της μεταπτυχιακής διπλωματικής το οποίο αφιερώνεται στην υλοποίησή του σε άλλα συστήματα κρυπτονομίσματος. Στα πλαίσια της παρούσας διατριβής, δημιουργήθηκε ένα πρόγραμμα το οποίο εξομοιώνει την εφαρμογή του πολλαπλού τρόπου λειτουργίας στην απλούστερη του μορφή με αρκετές παραδοχές. Πιο συγκεκριμένα, παρουσιάζεται γραφικά το δίκτυο που δημιουργείται μεταξύ των πλήρων και ελαφριών κόμβων και η εξάρτηση των ελαφριών κόμβων από τους πλήρης. Επίσης γραφικά, φαίνεται το περιεχόμενο και το τι αποθηκεύει ένας πλήρης κόμβος σε σύγκριση με τις εκπτώσεις που κάνει ένας κόμβος ελαφριάς λειτουργίας για να μειώσει τον απαιτούμενο αποθηκευτικό χώρο. Ως μέρος της απεικόνισης, ένας ελαφρύς κόμβος παρά τις ελλείψεις που έχει σε σχέση με ένα πλήρη κόμβο, μπορεί και αυτός να πραγματοποιήσει τις ίδιες εργασίες όπως για παράδειγμα την επικύρωση μιας συγκεκριμένης συναλλαγής.

1.1 Σκοπός της μεταπτυχιακής διατριβής

Σκοπός της μεταπτυχιακής διατριβής αυτής είναι η μελέτη των διαφόρων ειδών κρυπτονομισμάτων (Bitcoin, Ethereum) και τα πρωτόκολλα πολλαπλών τρόπων λειτουργίας που χρησιμοποιούνται σε αυτά. Επίσης επισκοπεί στην έρευνα κατά πόσο οι πολλαπλοί τρόποι λειτουργίας μπορούν να εφαρμοστούν γενικότερα και σε άλλα κρυπτονομίσματα. Η διατριβή αναλύει το θέμα με βάση τρεις προσεγγίσεις· αρχικά με την ανάλυση δύο υφιστάμενων κρυπτονομισμάτων, στη συνέχεια με την ανάλυση των πολλαπλών τρόπων λειτουργίας και τέλος στη μελέτη εφαρμογής τους σε νέο σύστημα κρυπτονομίσματος. Για τον τελευταίο σκοπό κρίθηκε χρήσιμο να υλοποιηθεί πρόγραμμα γραμμένο στη Java, το οποίο να εξομοιώνει τη λειτουργία των πολλαπλών τρόπων λειτουργίας σε μια απλή μορφή πως ένας ελαφρύς κόμβος μπορεί να επιβεβαιώσει την ύπαρξη μιας συναλλαγής με τον ίδιο τρόπο όπως ένας πλήρης.

1.2 Δομή της μεταπτυχιακής διατριβής

Η μεταπτυχιακή διπλωματική χωρίζεται σε 7 κεφάλαια συμπεριλαμβανομένου της Εισαγωγής και του Επίλογου. Στο δεύτερο κεφάλαιο αναλύονται κάποιες βασικές κρυπτογραφικές έννοιες, η κατανόηση των οποίων κρίθηκε απαραίτητη για να μπορεί κάποιος να ακολουθήσει τη ροή

των επόμενων κεφαλαίων. Προκειμένου ο αναγνώστης να κατανοήσει πως λειτουργεί πλήρως το Bitcoin ή το Ethereum, οφείλει να γνωρίζει πως λειτουργούν οι συναρτήσεις κατακερματισμού, το δένδρο Merkle, το δυαδικό δένδρο Patricia, καθώς και η Απόδειξη Εργασίας και Μεριδίου. Επίσης γίνεται εισαγωγή σε κάποιες βασικές έννοιες ενός συστήματος κρυπτονομίσματος όπως η συναλλαγή, η συστοιχία και η αλυσίδα συστοιχιών. Ακολούθως, στα κεφάλαια 3 και 4 αναλύονται σε λεπτομέρεια οι λειτουργίες του Bitcoin και Ethereum αντίστοιχα, δύο από τα πιο διαδεδομένα και ολοκληρωμένα συστήματα κρυπτονομίσματος. Πιο συγκεκριμένα αναλύονται οι διάφοροι αλγόριθμοι που απαιτούνται για τη λειτουργία κάθε κρυπτονομίσματος, πως πραγματοποιείται μια συναλλαγή, πως δομούνται οι συστοιχίες και πως υλοποιείται η εξόρυξη μιας καινούργιας συστοιχίας.

Το Κεφάλαιο 5 αναλώνεται στην ανάλυση του θέματος των πολλαπλών τρόπων λειτουργίας. Αρχικά συσχετίζονται ο πλήρης και ο ελαφρύς τρόπος λειτουργίας γενικότερα και στη συνέχεια επεξηγείται πως εφαρμόζονται στο Bitcoin και στο Ethereum. Στο Κεφάλαιο 6 περιγράφεται η λειτουργία του προγράμματος εξομοίωσης των πολλαπλών τρόπων λειτουργίας ξεκινώντας από τις απαιτήσεις που λήφθηκαν υπόψη κατά τη δημιουργία του. Ακολουθεί η επεξήγηση της λειτουργίας του και η επίδειξη της λειτουργίας του με συνδυασμό screenshots και γραπτού κειμένου. Το τελευταίο κεφάλαιο αποτελεί τον Επίλογο της μεταπτυχιακής διπλωματικής, στον οποίο περιέχονται τα συμπεράσματά της και η πιθανή μελλοντική ανάπτυξή αυτής.

1.3 Ερευνητικά Ερωτήματα μεταπτυχιακής διατριβής

Στην παρούσα διατριβή θα επιχειρήσουμε να απαντηθούν τα παρακάτω ερευνητικά ερωτήματα:

- Ποιες οι διαφορές και ομοιότητες στον τρόπο λειτουργίας των διαφόρων ειδών κρυπτονομίσματος;
- Μπορεί να εφαρμοστεί το πρωτόκολλο πολλαπλών τρόπων λειτουργίας σε άλλα κρυπτονομίσματα;

1.4 Σπουδαιότητα της μεταπτυχιακής διατριβής

Τα τελευταία χρόνια οι ερευνητές έχουν δώσει αρκετή έμφαση στη μελέτη των πρωτοκόλλων και λειτουργιών των συστημάτων κρυπτονομίσματος. Ωστόσο, οι προηγούμενες μελέτες-

εργασίες εστιάζονται κυρίως στην μονοδιάστατη έκδοση του πρωτοκόλλου του ψηφιακού νομίσματος, όπου το πρωτόκολλο λειτουργεί μόνο μεταξύ πλήρων κόμβων. Τα πρωτόκολλα πολλαπλών τρόπων λειτουργίας αποτελούν τις νέες ερευνητικές κατευθύνσεις, οι οποίες έχουν προσελκύσει το ενδιαφέρον της ερευνητικής κοινότητας τα τελευταία έτη, ωστόσο δεν αναλύθηκαν εκτεταμένα σε γραπτές αναφορές. Η διατριβή αυτή εστιάζει στην έρευνα των καινοτόμων αυτών πρωτοκόλλων και εξετάζει πως εφαρμόζεται με διαφορετικό τρόπο σε κάθε σύστημα κρυπτονομίσματος. Τέλος, εξετάζει πως μπορεί να υλοποιηθεί το πρωτόκολλο πολλαπλών τρόπων επικοινωνίας και σε άλλα συστήματα κρυπτονομίσματος με τη χρήση ενός προγράμματος εξομοίωσης.

Κεφάλαιο 2
Βασικές Κρυπτογραφικές Έννοιες

Για να κατανοήσει κάποιος τη λειτουργία των κρυπτονομισμάτων, πρέπει πρώτα να γνωρίζει κάποιες βασικές κρυπτογραφικές έννοιες και αρχές πάνω στις οποίες στηρίζονται γενικά όλα τα κρυπτονομίσματα. Κρυπτονόμισμα από κρυπτονόμισμα μπορούν να διαφέρουν στους κρυπτογραφικούς αλγόριθμους που χρησιμοποιούν ή το πως τους εφαρμόζουν στο σύστημά τους, ωστόσο η βασική τους λειτουργία είναι κοινή. Οι βασικές έννοιες που θα αναλυθούν στο παρόν κεφάλαιο είναι οι συναρτήσεις κατακερματισμού (hash functions), η αλυσίδα μπλοκ-συστοιχιών (blockchain), το μπλοκ ως μέρος της αλυσίδας (block), το Merkle-Tree, το Patricia-Tree, η μέθοδος Proof-of-Work και η μέθοδος Proof-of-Stake.

2.1 Αγγλικοί Όροι

Καθ' όλη την παρούσα διατριβή χρησιμοποιούνται κάποιοι αγγλικοί όροι αυτούσιοι όπως αναγράφονται στη βιβλιογραφία, προκειμένου να μην αλλοιωθεί το νόημα και για λόγους απλότητας. Αυτοί οι όροι, οι οποίοι αναφέρονται σε όλο το πλήθος του κειμένου της διατριβής, αναγράφονται πιο κάτω και δίνεται η πιο πιστή ερμηνεία τους στα ελληνικά:

- **Node:** κόμβος ο οποίος είναι μέρος ενός συστήματος κρυπτονομίσματος.
- **Hash functions:** συναρτήσεις κατακερματισμού.
- **Hash or hash value:** τιμή κατακερματισμού, δηλαδή η έξοδος από μια συνάρτηση κατακερματισμού.
- **Hash pointer:** δείκτης κατακερματισμού.
- **UTXO (Unspent Transaction Output):** μια έξοδος συναλλαγής που δεν έχει χρησιμοποιηθεί, δηλαδή αχρησιμοποίητη ποσότητα κρυπτονομίσματος η οποία μπορεί να χρησιμοποιηθεί σε μια άλλη συναλλαγή. (Matt, 2018)

- **Transaction:** συναλλαγή, καταγραφή ενός συμβάντος στο σύστημα, για παράδειγμα αποστολή κρυπτονομίσματος από ένα χρήστη σε άλλο. Σειρά συνεχόμενων συναλλαγών αποτελούν μια συστοιχία (block).
- **Block:** μια συστοιχία ή μπλοκ, το οποίο αναπαριστά ομάδα συναλλαγών (transactions) σε ένα σύστημα κρυπτονομίσματος, οι οποίες συνδέονται μεταξύ τους με χρονολογική σειρά δημιουργώντας μια αλυσίδα (blockchain).
- **Blockchain:** μεταφράζεται ως αλυσίδα συστοιχιών ή αλυσίδα μπλοκ (block) ή αλυσίδα ομάδων συναλλαγών ή αλυσίδα κοινοποιήσεων. Ερμηνεύεται ως ένα κοινό ιστορικό παλαιότερων συναλλαγών σε ένα δίκτυο κρυπτονομίσματος.
- **Άκυρη Διακλάδωση:** μια αλυσίδα που περιλαμβάνει συστοιχίες που δεν έγιναν αποδεκτές από του κόμβους του συστήματος και τρέχει παράλληλα με την έγκυρη αλυσίδα συστοιχιών.
- **Proof-of-Work:** απόδειξη εργασίας, δηλαδή ότι ένας κόμβος στο κρυπτογραφικό σύστημα έχει καταναλώσει ενέργεια για να πραγματοποιηθεί μιας μορφής εργασία.
- **Proof-of-Stake:** απόδειξη κατοχής, δηλαδή ότι ένας κόμβος στο κρυπτογραφικό σύστημα έχει στην κατοχή του ποσότητα του κρυπτονομίσματος.

2.2 Συναρτήσεις Κατακερματισμού (Hash Functions)

Η τεχνολογία της αλυσίδας μπλοκ (blockchain) εξαρτάται σε μεγάλο βαθμό από τις κρυπτογραφικές ιδιότητες των συναρτήσεων κατακερματισμού και είναι μια από τις βασικές έννοιες στις οποίες βασίζει τη λειτουργία της. Μια συνάρτηση κατακερματισμού **H**, είναι ουσιαστικά ένας μαθηματικός αλγόριθμος. Όπως όλους του μαθηματικούς αλγόριθμους, λαμβάνει ένα μήνυμα σαν είσοδο και επιστρέφει ένα άλλο μήνυμα σαν έξοδο (Stampernas, 2018). Το μήνυμα εισόδου μπορεί να αυθαίρετου μεγέθους, ωστόσο το μήνυμα εξόδου έχει σταθερό μήκος ανάλογα με τη συνάρτηση κατακερματισμού που χρησιμοποιείται. Συνήθως το μήνυμα εξόδου έχει μήκος 128, 160, 256 ή 512 bits. Η τιμή κατακερματισμού **h** (hash or hash value), είναι το αποτέλεσμα της λειτουργίας της συνάρτησης κατακερματισμού πάνω στο μήνυμα εισόδου. Μπορεί επίσης να θεωρηθεί ως ένα είδος «δακτυλικού αποτυπώματος» του μηνύματος και έτσι μπορεί να βρεθεί και με την ονομασία σύνοψη μηνύματος (message digest). (McAndrew, 2011)

Στα ολοκληρωμένα συστήματα κρυπτονομίσματος όπως το Bitcoin, Ethereum, Litecoin, Ripple, κλπ., οι συναρτήσεις κατακερματισμού που χρησιμοποιούνται περισσότερο είναι ο SHA-256, RIPEMD-160, Keccak-256 και FNV.

2.2.1 Ιδιότητες-Χρήσεις Συναρτήσεων Κατακερματισμού

Οι συναρτήσεις κατακερματισμού έχουν κάποιες ξεχωριστές ιδιότητες και ως εκ τούτου, έχουν και αντίστοιχες ιδιαίτερες χρήσεις σε ένα σύστημα κρυπτονομίσματος και στην τεχνολογία γενικότερα. Για ολόκληρη τη διατριβή που ακολουθεί θα χρησιμοποιούνται οι εξής συμβολισμοί:

m: το δεδομένα/μήνυμα εισόδου στη συνάρτηση κατακερματισμού (data input)

H: η συνάρτηση κατακερματισμού (hash function)

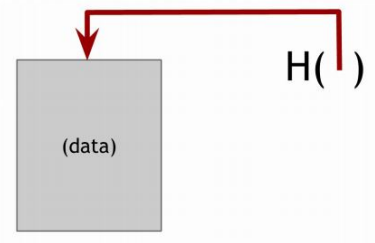
h: η τιμή κατακερματισμού (hash value), έξοδος συνάρτησης κατακερματισμού, **h = H(m)**

Η ιδιότητα στην οποία βασίζεται όλη η λειτουργία τους, είναι ότι οι συναρτήσεις κατακερματισμού είναι εύκολα και γρήγορα υπολογίσιμες από πλευράς υλικού και λογισμικού (hardware and software), αλλά είναι πολύ δύσκολο να αναστραφούν. Έτσι, γνωρίζοντας κάποιος την τιμή κατακερματισμού **h = H(m)**, δεν είναι εφικτό να βρεθεί το μήνυμα από το οποίο προήλθε, έτσι παρέχεται ικανοποιητική ασφάλεια και ανωνυμία για την οντότητα που δημιούργησε την τιμή κατακερματισμού και κατέχει τα αρχικά δεδομένα εισόδου.

Οι συναρτήσεις κατακερματισμού επίσης διασφαλίζουν την ακεραιότητα του μηνύματος, διότι για κάθε μήνυμα που αποτελεί είσοδο σε αυτές, παράγεται πάντα η ίδια έξοδος (ίδια τιμή κατακερματισμού). Ακόμα και η παραμικρή αλλαγή στο αρχικό μήνυμα **m΄ ≠ m**, θα έχει ως αποτέλεσμα μια εντελώς διαφορετική τιμή κατακερματισμού **H΄(m) ≠ H (m)**. Ως αποτέλεσμα, οι συναρτήσεις κατακερματισμού μπορούν να χρησιμοποιηθούν και σαν μηχανισμοί ανίχνευσης λαθών ή κακόβουλης ενέργειας. Γνωρίζοντας την τιμή κατακερματισμού, μπορεί κάποιος δηλαδή να ελέγξει αν το αρχικό μήνυμα έχει αλλοιωθεί από την αρχική του μορφή.

Οι **δείκτες κατακερματισμού** (hash pointers) εκμεταλλεύονται την πιο πάνω χρήσιμη ιδιότητα, προκειμένου να διασφαλίζουν την εγκυρότητα και ορθότητα των δεδομένων. Οι δείκτες περιέχουν την τοποθεσία των δεδομένων και την τιμή κατακερματισμού (hash) που βγαίνει αν εφαρμοστεί η συνάρτηση κατακερματισμού πάνω στα δεδομένα αυτά. Χρησιμοποιούνται στην αρχή κάθε συστοιχίας (block) για να τη συνδέσουν με την προηγούμενη συστοιχία, η οποία σε αυτή την περίπτωση αντιστοιχεί στα δεδομένα πάνω τα οποία θα αποτελέσουν την είσοδο της συνάρτησης κατακερματισμού. Με αυτό τον τρόπο, αν τα δεδομένα της προηγούμενη συστοιχίας αλλοιωθούν (κακόβουλα ή εκ παραδρομής) η τιμή κατακερματισμού θα είναι

διαφορετική από την προηγούμενη και έτσι ελέγχεται η εγκυρότητα και η ορθότητα των δεδομένων. (Fekkes, 2018)



Εικόνα 2.1: Γραφική απεικόνιση **δείκτη κατακερματισμού** *(Fekkes, 2018)*

2.2.2 Κριτήρια Συναρτήσεων Κατακερματισμού

Προκειμένου να έχουν οι συναρτήσεις κατακερματισμού τις πιο πάνω ιδιότητες και χρήσεις στην κρυπτογραφία, πρέπει να ανταποκρίνονται στα πιο κάτω βασικά κριτήρια-προϋποθέσεις (Wang, Duan, & Zhu, 2018) στα οποία είναι γνωστή η συνάρτηση κατακερματισμού που χρησιμοποιείται:

- **Αντίσταση Σύγκρουσης:** δεν είναι υπολογιστικά εφικτό να βρεθούν δύο διαφορετικά μηνύματα **m** και **m΄,** όπου **m ≠ m΄,** έτσι ώστε οι τιμές κατακερματισμού που παράγονται από την ίδια συνάρτηση να είναι ίδιες, δηλαδή **H(m) ≠ H(m΄)**.

- **Αντίσταση Προ-εικόνας:** γνωρίζοντας μια τιμή κατακερματισμού **h**, δεν είναι υπολογιστικά εφικτό να βρεθεί το μήνυμα **m** από το οποίο παράχθηκε, δηλαδή **H(m) = h**.

- **Δεύτερη Αντίσταση Προ-εικόνας:** γνωρίζοντας ένα μήνυμα **m**, δεν είναι υπολογιστικά εφικτό να βρεθεί ένα διαφορετικό μήνυμα **m΄** το οποίο να παράγει την ίδια τιμή κατακερματισμού, δηλαδή **H(m΄) = H(m)**.

Τα πιο πάνω κριτήρια είναι αναγκαία για να έχει μια συνάρτηση κατακερματισμού τις ιδιότητες που χρειάζονται για να είναι χρήσιμη από κρυπτογραφικής έννοιας. Αφού υπάρχουν άπειρα δυνατά μηνύματα εισόδου σε μια συνάρτηση κατακερματισμού και μόνο πεπερασμένος αριθμός τιμών κατακερματισμού (hash values), τότε θεωρητικά υπάρχουν και άπειρα μηνύματα τα οποία παράγουν την ίδια τιμή κατακερματισμού. Η λογική είναι ότι η όποια σύγκρουση είναι υπολογιστικά δύσκολη να βρεθεί. Το ίδιο και για τα πιο πάνω κριτήρια, όπου υπολογιστικά μη εφικτό νοείται υπολογιστικά δύσκολο διότι αν υπάρχει άπειρος χρόνος είναι δυνατόν να μην ισχύουν. (McAndrew, 2011)

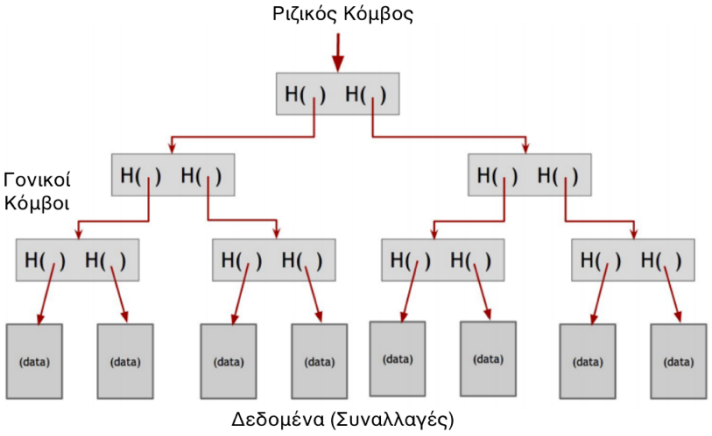
Σύμφωνα με (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2016), μια συνάρτηση κατακερματισμού η οποία χρησιμοποιείται σε μια αλυσίδα συστοιχιών (blockchain), πρέπει να ανταποκρίνεται και στα δύο παρακάτω κριτήρια-ιδιότητες:

- **Απόκρυψη:** δεδομένου ότι μια μυστική τιμή **r** επιλέγεται από μια διανομή υψηλής ελάχιστης εντροπίας, μια συνάρτηση κατακερματισμού **H** (Wood, 2017) (Buterin, 2013)έχει την ιδιότητα της απόκρυψης αν δεδομένου **H (r || m)**, δεν είναι υπολογιστικά εφικτό να βρεθεί το μήνυμα **m**.

- **Φιλικό ως προς το παζλ:** αν για κάθε τιμή κατακερματισμού **h** μήκους **n** bits και δεδομένου ότι μια μυστική τιμή **r** επιλέγεται από μια διανομή υψηλής ελάχιστης εντροπίας, τότε μια συνάρτηση κατακερματισμού ανταποκρίνεται στην ιδιότητα φιλική προς το παζλ όταν δεν είναι εφικτό να βρεθεί το μήνυμα **m** σε σημαντικά μικρότερο από 2^n χρόνο, όπου **h = H (r || m)**.

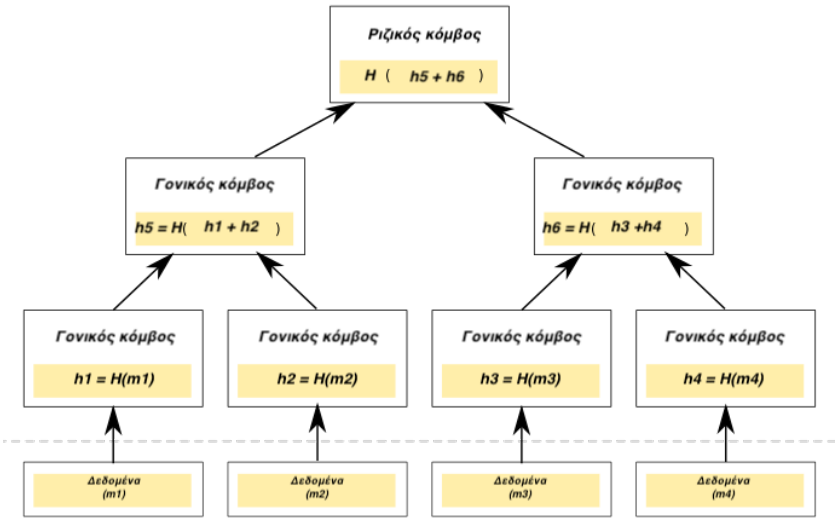
2.3 Δένδρο Merkle

Το **Δένδρο Merkle** είναι ένα δυαδικό δένδρο το οποίο περιέχει στη δομή του δείκτες κατακερματισμού (Βλέπε 2.2.1) και έχει ευρεία χρήση στις τεχνολογίες αλυσίδας συστοιχιών. Το σύνολο των δεδομένων αποτελούν όλα τα φύλλα του δένδρου, δηλαδή όλους τους αρχικούς κόμβους. Ο γονικός κόμβος που βρίσκεται ένα επίπεδο προς τα πάνω περιέχει δύο τιμές κατακερματισμού, μια τιμή κατακερματισμού από ένα φύλλο και μια από ένα άλλο. Κάθε γονικός κόμβος στη συνέχεια ζευγαρώνει τις τιμές κατακερματισμού από δύο κόμβους στο αμέσως πιο κάτω επίπεδο (Fekkes, 2018). Αυτό συνεχίζεται μέχρι να καταλήξει το δένδρο σε ένα μόνο κόμβο ο οποίος ονομάζεται ο **ριζικός κόμβος** και αποτελεί την τιμή κατακερματισμού όλων των κόμβων και έτσι όλων των δεδομένων του Δένδρου Merkle (Βλέπε Εικόνα 2.2).



Εικόνα 2.2: Γραφική απεικόνιση Δένδρου Merkle *(Fekkes, 2018)*

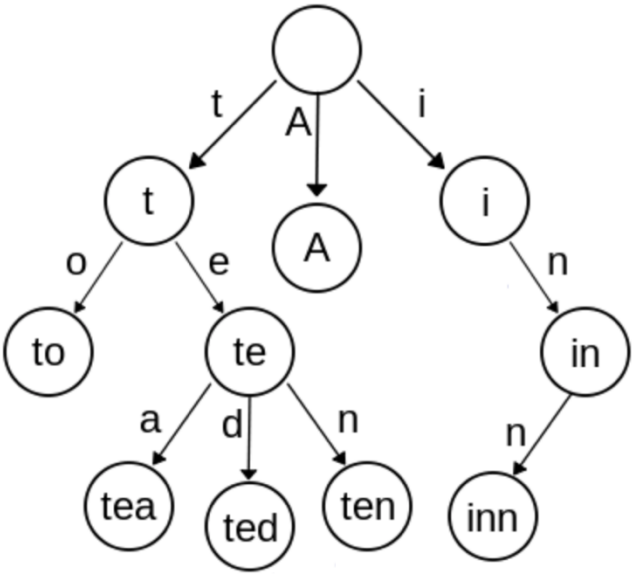
Οι χρήσεις που έχει το Δένδρο Merkle στην κρυπτογραφία είναι πολλές, αλλά συγκεκριμένα στην τεχνολογία αλυσίδας συστοιχιών (blockchain) χρησιμοποιείται για επαλήθευση των συναλλαγών που πραγματοποιήθηκαν στο παρελθόν, δηλαδή αν συμπεριλήφθηκαν στην αλυσίδα. Οι συναλλαγές αποτελούν του αρχικούς κόμβους (φύλλα) στο Δένδρο Merkle και ο ριζικός κόμβος περιέχεται στην επικεφαλίδα της συστοιχίας, που είναι η συνολική τιμή κατακερματισμού όλων των συναλλαγών που καταχωρήθηκαν στη συστοιχία. Έτσι για να επαληθεύσει κάποιος όλες τις συναλλαγές, αρκεί να επαληθεύσει το ριζικό κόμβο (Bashir, 2018). Για να επαληθεύσει κάποιος ότι μια συγκεκριμένη συναλλαγή εμπεριέχεται στο Δένδρο Merkle, πρέπει να ελέγξει τις τιμές κατακερματισμού ξεκινώντας από τον φύλλο που αντιπροσωπεύει τη συναλλαγή που θα ελεγχθεί, μέχρι το ριζικό κόμβο. Αν όλες οι τιμές κατακερματισμού είναι ορθές, τότε η συναλλαγή εμπεριέχεται στο Δένδρο Merkle. Αν υπάρχουν **n** κόμβοι σε ολόκληρο το Δένδρο Merkle, τότε απαιτείται χρόνος log (n) για να επαληθευτούν όλοι οι κόμβοι στη συστοιχία (Fekkes, 2018).



Εικόνα 2.3: Γραφική απεικόνιση Δένδρου Merkle *(Kavalar, 2019)*

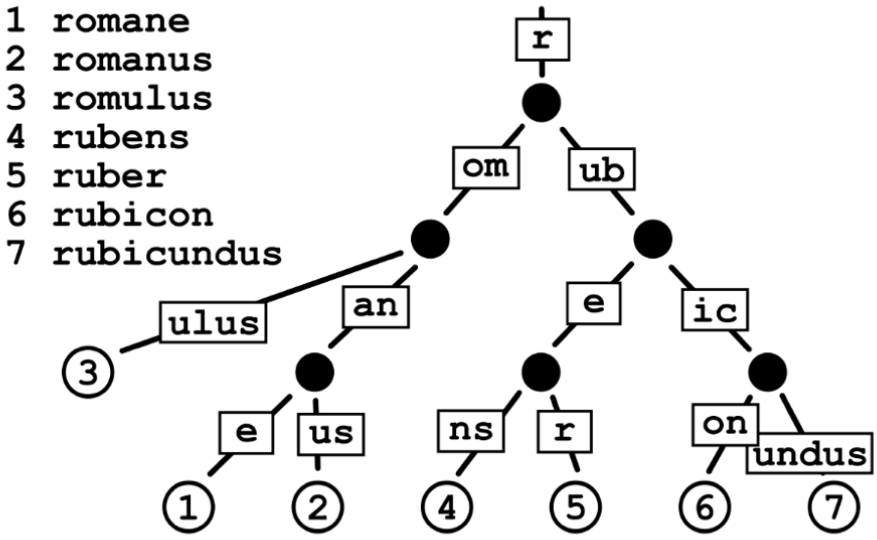
2.4 Δένδρο Patricia

Το **Δένδρο Patricia** είναι ένα δένδρο ακτινών (αλλιώς δένδρο προθέματος) οι ακτίνες μπορούν να είναι είτε μηδέν είτε πάνω από δύο. Αυτό συμβαίνει διότι όποιος κόμβος είναι ο μοναδικός παιδικός κόμβος, τότε αυτός συγχωνεύεται με το γονικό του κόμβο μειώνοντας έτσι τον απαιτούμενο χώρο. Έτσι, ένα Δένδρο Patricia έχει τουλάχιστον δύο ή καθόλου παιδικούς κόμβους και βελτιστοποιεί το χώρο που καταλαμβάνει σε σχέση με ένα δένδρο ακτινών με κανονισμένη δομή (Βλέπε Εικόνα 2.4).



Εικόνα 2.4: Γραφική απεικόνιση Δένδρου Patricia *(Giroux, 2018)*

Χρησιμοποιείται ένα κλειδί σαν μονοπάτι προς ένα κόμβο, το οποίο έχει συνήθως τη μορφή συμβολοσειράς. Η συμβολοσειρά-κλειδί δείχνει το μονοπάτι που ακολουθείται, ξεκινώντας από το ριζικό κόμβο του Δένδρου Patricia μέχρι να φτάσει στα φύλλα, όπου και αποθηκεύεται. Τα κλειδιά ελέγχονται ψηφίο προς ψηφίο και το καθένα από αυτά καταδεικνύει ποιος δρόμος θα ακολουθηθεί σε κάθε επίπεδο, για να καταλήξουμε στον τελικό κόμβο (φύλλο) για τον οποίο αναφέρεται το κλειδί (Fekkes, 2018). Ως εκ τούτου, το κάθε κλειδί προκύπτει από τη θέση του κόμβου και υποδεικνύει το πως μπορεί κάποιος να φτάσει σε αυτόν (Βλέπε Εικόνα 2.5). Ένας τελικός κόμβος σε ένα σύστημα κρυπτονομίσματος μπορεί να είναι οι συναλλαγές που πραγματοποιήθηκαν σε μια συστοιχία ή διάφορα άλλα δεδομένα.

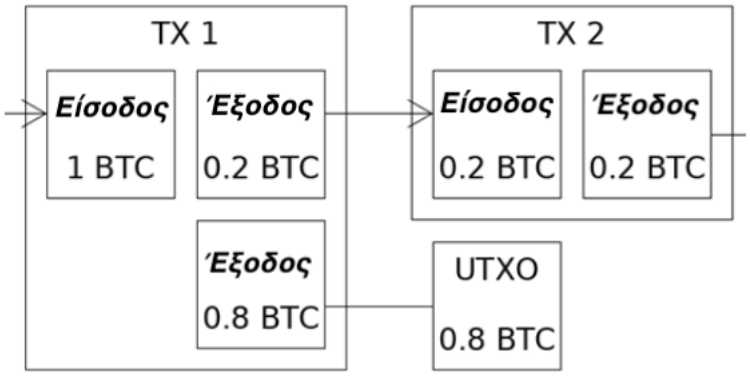


Εικόνα 2.5: Γραφική απεικόνιση Δένδρου Patricia *(Fekkes, 2018)*

2.5 Συναλλαγή

Συναλλαγή είναι μια καταγραφή ενός συμβάντος που έγινε σε ένα σύστημα κρυπτονομίσματος. Συνήθως αναφερόμαστε σε αποστολές ηλεκτρονικού χρήματος από ένα επιβεβαιωμένο κόμβο σου συστήματος (αποστολέα) προς ένα άλλο κόμβο (παραλήπτη). Οποιαδήποτε συναλλαγή αποτελείται από τουλάχιστον μια είσοδο και τουλάχιστον μια έξοδο. Το άθροισμα όλων των τιμών εισόδου μιας συναλλαγής πρέπει να ισούται με το άθροισμα όλων των τιμών εξόδου αυτής, προκειμένου να μην υπάρξει διαρροή ηλεκτρονικού χρήματος (Werner, Lawrenz, & Rausch, 2020). Όσο τηρείται αυτός ο κανόνας δεν χάνεται καμία ποσότητα ηλεκτρονικού νομίσματος και ο μόνος τρόπος να δημιουργηθεί περισσότερο ηλεκτρονικό νόμισμα είναι μέσω της εξόρυξης (mining), η οποία θα εξηγηθεί εκτεταμένα στη συνέχεια.

Για να στείλει ένας κόμβος αριθμό κρυπτονομίσματος σε ένα άλλο κόμβο εντός του συστήματος, τότε πρέπει να έχει στη διάθεσή του κρυπτονόμισμα υπό τη μορφή του **UTXO (Unspent Transaction Output).** Το UTXO είναι μια έξοδος προηγούμενης συναλλαγής η οποία δεν έχει χρησιμοποιηθεί ή ξοδευτεί για οποιοδήποτε λόγο (Matt, 2018). Έτσι, μπορεί ο κόμβος που την έχει στην κατοχή του, να το χρησιμοποιήσει σαν είσοδο για μια συναλλαγή όπως για παράδειγμα να στείλει 2 κρυπτονομίσματα σε ένα άλλο κόμβο. Κάθε UTXO μπορεί να είναι διαφορετικής αξίας σε αριθμό κρυπτονομίσματος (Βλέπε Εικόνα 2.6). Κάθε συναλλαγή έχει ένα μοναδικό αριθμό συναλλαγής (transaction ID) και κάθε είσοδος είναι UTXO 1 το οποίο είναι υπό τον έλεγχο του αποστολέα.

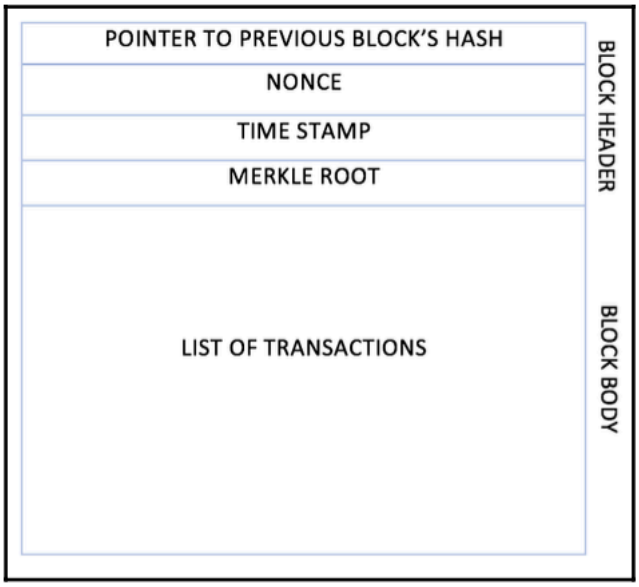


Εικόνα 2.6: *Στην Εικόνα υπάρχουν δύο συναλλαγές στις οποίες υποδεικνύονται οι είσοδοι και οι έξοδοι μαζί με την αξία τους σε Bitcoin (BTC), καθώς και το UTXO που περισσεύει από την πρώτη συναλλαγή.* (Werner, Lawrenz, & Rausch, 2020)

2.6 Συστοιχία (Block)

Μια **Συστοιχία** είναι συναλλαγές που ομαδοποιούνται και οργανώνονται λογικά (Bashir, 2018). Συνεχόμενες συστοιχίες σε χρονολογική σειρά αποτελούν την **Αλυσίδα Συστοιχιών**. Όλες οι συναλλαγές και τα οποιοδήποτε άλλο γεγονός εντός του συστήματος κρυπτονομίσματος αποθηκεύονται στις συστοιχίες οι οποίες απαρτίζουν τα δεδομένα όλης της αλυσίδας. Έτσι, μια **Συστοιχία** αποτελείται από ένα αριθμό συναλλαγών και κάποια άλλα πεδία τα οποία διαφοροποιούνται ανάλογα με τον τύπο του συστήματος κρυπτονομίσματος.

Όλες οι συστοιχίες περιέχουν δείκτες κατακερματισμού (hash pointers) που καταδεικνύουν τη θέση της προηγούμενης συστοιχίας, εκτός από τη **Συστοιχία Γένεσης**. Η Συστοιχία Γένεσης είναι η πρώτη συστοιχία της αλυσίδας συστοιχιών η οποία κωδικοποιείται τη στιγμή που δημιουργείται η αλυσίδα. Γενικότερα, υπάρχουν κάποια πεδία τα οποία είναι απαραίτητα για τη λειτουργικότητα της συστοιχίας όπως: η επικεφαλίδα του μπλοκ που περιέχει συνήθως το δείκτη κατακερματισμού τη σήμανση χρόνου (timestamp), τον κόμβο που το δημιουργεί, το ριζικό κόμβο του Δένδρου Merkle, και το κυρίως μέρος της συστοιχίας το οποίο απαρτίζεται από τις συναλλαγές (Bashir, 2018).

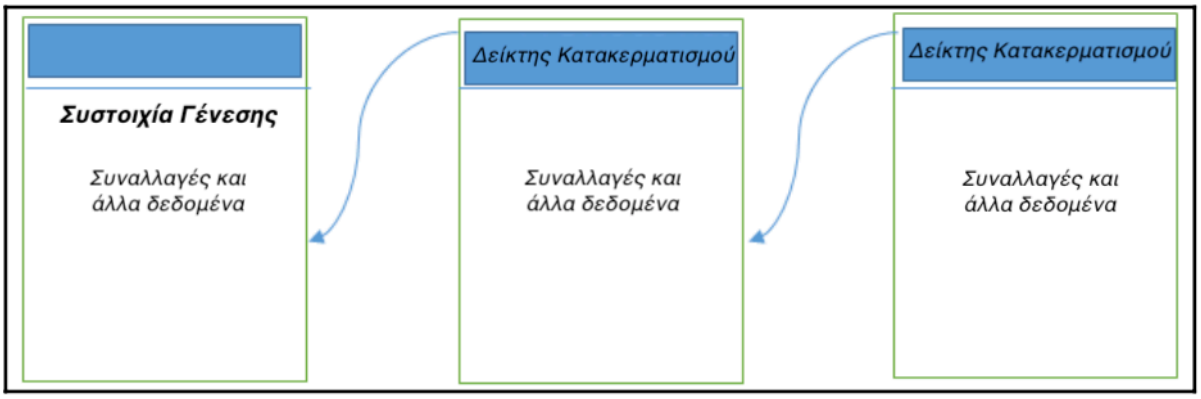


Εικόνα 2.7: Ενδεικτική δομή μιας συστοιχίας όπως δίνεται σε *(Bashir, 2018)*

Όταν πραγματοποιείται μια συναλλαγή, όλοι οι κόμβοι οι οποίοι αντιπροσωπεύουν χρήστες ή τερματικούς υπολογιστές, επαληθεύουν τη συναλλαγή αυτή με συναίνεση και έπειτα αυτή συσσωματώνεται στη συστοιχία. Από τη στιγμή που μια συναλλαγή είναι μέλος της συστοιχίας και κατ' επέκταση της αλυσίδας, είναι αδύνατον να αλλοιωθεί ή να διαγραφεί και έτσι το σύστημα είναι αξιόπιστο για όλους τους χρήστες (Fekkes, 2018).

2.7 Αλυσίδα Συστοιχιών (Blockchain)

Η **Αλυσίδα Συστοιχιών** είναι μια δομή που αποθηκεύει όλες τις εγγραφές, συναλλαγές και γεγονότα εντός των συστοιχιών. Αποτελείται αρχικά από τη Συστοιχία Γένεσης η οποία δημιουργείται πρώτη και στη συνέχεια από άλλες συστοιχίες που δημιουργούνται με τις συναλλαγές που διενεργούν οι κόμβοι του συστήματος (Βλέπε Εικόνα 2.8).

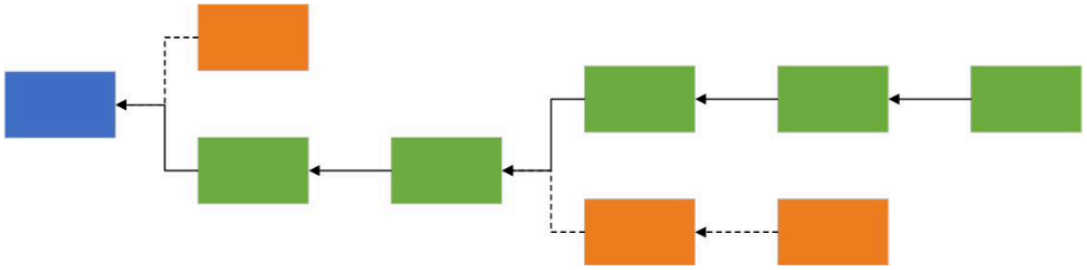


Εικόνα 2.8: Ενδεικτική δομή αλυσίδας συστοιχιών *(Bashir, 2018)*

Όταν πραγματοποιείται μια συναλλαγή στο σύστημα, όλοι οι ενεργοί κόμβοι πρέπει να την επιβεβαιώσουν για να μπορέσει να αποδεχτεί σαν ολοκληρωμένη και να συμπεριληφθεί στην τρέχουσα συστοιχία. Η επιβεβαίωση αφορά κυρίως το κρυπτονόμισμα της συναλλαγής να μην έχει ξοδευτεί διπλά (double spending). Λόγω της λειτουργίας αυτής, το όλο σύστημα κρυπτονομίσματος είναι αποκεντρωτικό, δηλαδή δεν υπάρχει μια έμπιστη οντότητα που ελέγχει τις διαδικασίες στο σύστημα. Αντίθετα όλοι οι κόμβοι πρέπει να συμφωνούν για να συμπεριληφθεί μια συναλλαγή στην αλυσίδα σε ένα δίκτυο peer-to-peer.

Ωστόσο, υπάρχει η πιθανότητα μια συστοιχία να μην επαληθευτεί από όλους τους κόμβους και έτσι να μην συμπεριληφθεί στην αλυσίδα συστοιχιών. Στην περίπτωση της μη αποδεχτής συστοιχίας, δημιουργείται μια παράλληλη αλυσίδα, η οποία αποκαλείται **άκυρη διακλάδωση**. Η αλυσίδα αυτή περιλαμβάνει τα λανθασμένα μπλοκ και έτσι τερματίζεται εκεί, ενώ οι έγκυρες συστοιχίες προστίθενται στην έγκυρη αλυσίδα. Οι υπόλοιποι κόμβοι συνεχίζουν να εργάζονται στη μεγαλύτερη έγκυρη αλυσίδα, εγκαταλείποντας την **άκυρη διακλάδωση** και απαλείφοντας έτσι την ανακρίβεια (Fekkes, 2018). Οι λόγοι για τη μη έγκυρη συστοιχία μπορεί να είναι:

- Ένας κόμβος μπορεί να εξόρυξε ένα μπλοκ την ίδια στιγμή που προστίθενται στην αλυσίδα μπλοκ
- Κάποια μπλοκ μπορεί να μην είναι έγκυρα ή να έχουν κάποιο λάθος και να το αντιλήφθηκε κάποιος κόμβος αφού προστέθηκαν μερικά άλλα μπλοκ μετά από αυτό



Εικόνα 2.9: Αλυσίδα συστοιχιών με απόρριψη συστοιχίας σε δύο περιπτώσεις. Την πρώτη αντιλήφθηκε αμέσως και απορρίφθηκε, αλλά τη δεύτερη προστέθηκε μια συστοιχία μετά από αυτή και στη συνέχεια αποδείχθηκε μη έγκυρη άρα απορρίφθηκαν και οι δύο *(Fekkes, 2018)*. **Μπλε:** Συστοιχία Γένεσης, **Πράσινο:** Έγκυρες Συστοιχίες, **Πορτοκαλί:** Μη έγκυρες Συστοιχίες

2.8 Απόδειξη Εργασίας

Ως **Απόδειξη Εργασίας** αποκαλείται ο αλγόριθμος ο οποίος χειρίζεται τη δημιουργία καινούργιων συστοιχιών σε μια αλυσίδα. Όπως αναλύθηκε πιο πάνω, μια αλυσίδα συστοιχιών αποτελείται από συστοιχίες, οι οποίες αποθηκεύουν μεγάλο αριθμό συναλλαγών. Ο αριθμός αυτός εξαρτάται από το κρυπτονόμισμα. Όταν εξαντληθεί ο αριθμός αυτός σε ένα μπλοκ, ένας από τους κόμβους που συμμετέχουν στο σύστημα κρυπτονομίσματος προτείνει τη δημιουργία του επόμενου μπλοκ, κάτι που ισχύει για όλα τα κρυπτονομίσματα. Προκειμένου να επιλεγεί ο κόμβος που θα προτείνει την επόμενη συστοιχία, χρησιμοποιείται η Απόδειξη Εργασίας. Είναι ουσιαστικά ένας όρος που χρησιμοποιείται στα συστήματα κρυπτονομίσματος και εκφράζεται ως η απόδειξη ότι έχουν δαπανηθεί επαρκής υπολογιστικοί πόροι για να πραγματοποιηθεί μια εργασία (Bashir, 2018).

Η εργασία αυτή είναι ως επί το πλείστον γρίφοι ή μαθηματικά προβλήματα τα οποία είναι δύσκολο να επιλυθούν αλλά η επαλήθευση της λύσης είναι εύκολη. Για να επιτευχθεί αυτό, οι γρίφοι αυτοί έχουν σαν βασική αρχή τις συναρτήσεις κατακερματισμού (Βλέπε 2.2), οι ιδιότητες των οποίων ανταποκρίνονται πλήρως στα χαρακτηριστικά που είναι επιθυμητά σε ένα τέτοιο γρίφο (Fekkes, 2018). Η επίλυσή τους κοστίζει στους κόμβους-χρήστες χρόνο και υπολογιστική ισχύ και έτσι ανταμείβονται αν παρουσιάσουν τη λύση. Με αυτό τον τρόπο αποδεικνύουν ότι την εργασία που έχουν πραγματοποιήσει επιτυχώς, κάτι το οποία είχε υπολογιστικό κόστος υπό τη μορφή ηλεκτρισμού, φθορά υλικών και χρόνου. Ο κόμβος που θα επιλύσει πρώτος το γρίφο, κερδίζει το δικαίωμα να προτείνει το επόμενο μπλοκ πάνω στο οποίο θα αποθηκευτούν οι συναλλαγές που θα γίνουν στο σύστημα καθώς και ορισμένη ποσότητα κρυπτονομίσματος.

Τα συστήματα κρυπτονομίσματος που χρησιμοποιούν την Απόδειξη Εργασίας για να εισάγουν νέες συστοιχίες στην αλυσίδα τους είναι το Bitcoin και το Ethereum, ωστόσο το Ethereum είναι σε ένα μεταβατικό στάδιο προς την Απόδειξη Μεριδίου (Βλέπε Τμήμα 2.9).

2.8.1 Απόδειξη Χρήσιμης Εργασίας

Η ιδέα για ανάγκη της **Απόδειξη Χρήσιμης Εργασίας**, εγείρεται λόγω του ότι η αναζήτηση λύσης στους γρίφους που αναφέρονται πιο πάνω έχει μεγάλες απαιτήσεις σε ενέργεια, η οποία στην ουσία χάνεται μετά την εύρεση της λύσης. Μόνο ένας από τους κόμβους ανταμείβεται για την ενέργεια που σπαταλά, ενώ στην πραγματικότητα όλοι οι κόμβοι που προσπαθούν να βρουν τη λύση του γρίφου σπαταλούν ενέργεια η οποία πάει χαμένη. Η Απόδειξη Χρήσιμης Εργασίας αναφέρεται στο αν η ενέργεια αυτή μπορεί να διοχετευτεί σε μια χρήσιμη εργασία που να ωφελεί την κοινωνία. Έτσι, οι γρίφοι που δίνονται για επίλυση, πρέπει να είναι υπάρχοντα προβλήματα που η λύση τους να επιφέρει κέρδος ταυτόχρονα σε αυτόν που θα βρει τη λύση, αλλά και στην κοινωνία. Υπάρχουν είδη κάποια έργα «εθελοντικής πληροφορικής», αλλά προκειμένου να χρησιμοποιηθούν αυτοί σε ευρεία κλίμακα στα συστήματα κρυπτονομίσματος, εγείρονται ορισμένες προκλήσεις: (Fekkes, 2018)

- Οι κόμβοι δεν έχουν τις ίδιες πιθανότητες να βρουν τη λύση. Για αν λειτουργήσει σωστά η Απόδειξη Χρήσιμης Εργασίας, όλα τα κομμάτια και χώροι του γρίφου οφείλουν να έχουν την ίδια πιθανότητα να καταλήξουν στη λύση. Διαφορετικά, τα άτομα που έχουν περισσότερη υπολογιστική ισχύ από τους υπόλοιπους και είναι πιο γρήγοροι, μπορούν να επιλέξουν ένα χώρο που έχει μεγαλύτερη πιθανότητα για εύρεση της λύσης σε σχέση με άλλους χώρους. Έτσι, αυτοί οι χρήστες θα έχουν πάντα μεγαλύτερη πιθανότητα να βρουν τη λύση σε όλους τους γρίφους.

- Απαιτείται ανεξάντλητος αριθμός γρίφων. Γενικά στα συστήματα κρυπτονομίσματος, όπου τα γεγονότα κινούνται σε ταχύτατους ρυθμούς, πρέπει να υπάρχουν συνεχώς καινούργιοι γρίφοι προς επίλυση, αλλιώς σε μια δεδομένη στιγμή δεν θα υπάρχουν πλέον παζλ προς επίλυση. Αυτό σημαίνει ότι δεν θα μπορούν να προταθούν καινούργιες συστοιχίες από τον ευρίσκων της λύσης και ως ακόλουθο δεν θα μπορούν να πραγματοποιηθούν άλλες συναλλαγές.

- Ο γρίφος πρέπει να παράγεται αλγοριθμικά, χωρίς την ανάγκη για μια κεντρική οντότητα. Μια από τις προϋποθέσεις για τη λειτουργία των συστημάτων κρυπτονομίσματος είναι η αποκεντρωτική δημιουργία και λειτουργία της αλυσίδας συστοιχιών. Στην περίπτωση που μια κεντρική οντότητα διαχειριζόταν τα παζλ, τότε θα μπορούσε να δώσει σε ορισμένους χρήστες μεγαλύτερη πιθανότητα να βρουν τη λύση από άλλους χρήστες.

2.9 Απόδειξη Μεριδίου

Η **Απόδειξη Μεριδίου** είναι μια διαφορετική μέθοδος επιλογής του κόμβου που θα δημιουργήσει το επόμενο μπλοκ στην αλυσίδα συστοιχιών με το να αποδείξει ότι ένας κόμβος ή χρήστης έχει ικανοποιητικό μερίδιο εντός του συστήματος κρυπτονομίσματος. Δηλαδή, όταν ο χρήστης έχει επενδύσει αρκετά στο σύστημα κρυπτονομίσματος, έτσι ώστε οποιαδήποτε κακόβουλη ενέργεια του χρήστη αυτού κατά του συστήματος αντισταθμίζει τα οφέλη που θα έχει από την επίθεση διότι θα τον επηρεάσει περισσότερο η ζημιά που θα προκαλέσει (Bashir, 2018). Για να επιλεγεί ο κόμβος που θα προτείνει το επόμενο μπλοκ, αποδεικνύεται η κατοχή μιας ποσότητας κρυπτονομίσματος αντί για την επίλυση ενός δύσκολου προβλήματος κατακερματισμού. Οι χρήστες που κατέχουν μερίδιο στο σύστημα κρυπτονομίσματος ονομάζονται επικυρωτές, ένας από τους οποίους επιλέγεται να δημιουργήσεις την επόμενη συστοιχία σύμφωνα με την ποσότητα κρυπτονομίσματος που έχουν στην κατοχή τους. Υπάρχουν δύο είδη Απόδειξης Μεριδίου (Fekkes, 2018):

- **Απόδειξη Μεριδίου με βάση την αλυσίδα:** Οι επιλεγμένοι επικυρωτές που κατέχουν επαρκής ποσότητα κρυπτονομίσματος, επιτρέπονται να δημιουργήσουν την επόμενη συστοιχία στην αλυσίδα. Η νεοσύστατη συστοιχία χρησιμοποιείται για να επικυρώσει, να αποθηκεύσεις νέες συναλλαγές και προστίθεται στο τέλος της αλυσίδας έχοντας δείκτη κατακερματισμού προς την προηγούμενη συστοιχία.
- **Απόδειξη Μεριδίου BFT:** Στην Απόδειξη Μεριδίου με βάση την Ανοχή Βυζαντινών Σφαλμάτων, όταν θα προστεθεί νέα συστοιχία στην αλυσίδα, όλοι οι επικυρωτές ψηφίζουν για τη συστοιχία από εκείνες που προτείνονται θα συμπεριληφθεί στην αλυσίδα συστοιχιών. Στο τέλος του γύρου, όλοι οι επικυρωτές αποφασίζουν για το ποιο μπλοκ θα συμπεριληφθεί τελικά και θα έχει συνοχή με τα προηγούμενα.

Μια άλλη έννοια στην Απόδειξη Μεριδίου είναι η ηλικία του νομίσματος, το οποίο προκύπτει με βάση το χρόνο κατοχής και τον αριθμό των κρυπτονομισμάτων που δεν έχουν ξοδευτεί. Σε αυτό το μοντέλο, όσο μεγαλύτερη είναι η ηλικία του νομίσματος, τόσο αυξάνονται οι πιθανότητες για δημιουργία του επόμενου μπλοκ (Bashir, 2018). Το πρώτο κρυπτονόμισμα που χρησιμοποίησε το μοντέλο αυτό είναι το Peercoin και θα ακολουθήσει το Ethereum σε μια εκδοχή της αλυσίδας του ονομαζόμενη Serenity.

Κεφάλαιο 3
Bitcoin

Στο **Bitcoin** μπορούν να εφαρμοστούν αρκετοί ορισμοί όπως πρωτόκολλο, ψηφιακό νόμισμα, πλατφόρμα και λογισμικό. Στην πραγματικότητα είναι ένας συνδυασμός των πιο πάνω που λειτουργούν μαζί σε ένα δίκτυο ομότιμου-ομότιμου (peer to peer network) με σκοπό τη λειτουργεία και διακίνηση του ψηφιακού νομίσματος που ονομάζεται **bitcoin.** Είναι σημαντική η διάκριση μεταξύ **Bitcoin** το οποίο είναι η πλατφόρμα στην οποία στηρίζεται το δίκτυο και **bitcoin** το οποίο αναφέρεται καθαρά στο ψηφιακό νόμισμα (Bashir, 2018).

3.1 Εισαγωγή στο Bitcoin

Ο Satoshi Nakamoto με τη δημιουργία του Bitcoin το 2008, είναι ο πρώτος που εισήγαγε την ιδέα ενός αποκεντρωτικού δικτύου. Η καινοτομία στο νέο είδος δικτύου ήταν το γεγονός ότι οι κόμβοι που συμμετέχουν σε αυτό μπορούσαν να επικοινωνήσουν και να ανταλλάξουν ηλεκτρονικό χρήμα χωρίς να βασίζονται σε μια τρίτη οντότητα για να πραγματοποιήσουν τη συναλλαγή, όπως γίνεται στην περίπτωση των ηλεκτρονικών αγορών μέσω του Διαδικτύου (Nakamoto, 2008). Για να γίνει αυτό εφικτό, χρησιμοποιείται ένας συνδυασμός κρυπτογραφίας δημόσιου κλειδιού, ψηφιακών υπογραφών και συναρτήσεων κατακερματισμού (Βλέπε Κεφάλαιο 2).

Εντός του δικτύου του Bitcoin υπάρχει ένας περιορισμένος αριθμός κρυπτονομίσματος, ο οποίος είναι διαμοιρασμένος ανάμεσα στους κόμβους που το απαρτίζουν. Μια **Συναλλαγή** πραγματοποιείται όταν ένας από αυτούς τους κόμβους στέλνει μια ποσότητα bitcoin σε ένα άλλο. Ο μόνος τρόπος να εισαχθούν περισσότερα ψηφιακά νομίσματα στο σύστημα είναι με τη διαδικασία της **Εξόρυξης.** Οι πιο πάνω λειτουργίες θα αναλυθούν περεταίρω στο παρόν κεφαλαίο. Για όλη τη διατριβή, ως ηλεκτρονικό νόμισμα ορίζεται μια αλυσίδα από ηλεκτρονικές υπογραφές ενώ η ταυτότητα ένας κόμβος στο δίκτυο αντιπροσωπεύεται από διεύθυνσή του, η οποία προέρχεται από το δημόσιο του κλειδί (περισσότερα στο Τμήμα 3.3).

3.1.1 Τιμή και συνολικός αριθμός Bitcoin

Τη στιγμή της δημιουργίας του, 1 ψηφιακό νόμισμα bitcoin το οποίο συμβολίζεται και ως BTC, είχε μηδαμινή αξία. Σύντομα όμως, όσο οι κόμβοι στο δίκτυο ομότιμου-ομότιμου αυξάνονταν σε αριθμό, τόσο αυξανόταν και η ζήτηση για τον περιορισμένο αριθμό, με αποτέλεσμα να αυξάνεται και η τιμή των bitcoins. Τον Δεκέμβριο του 2020 η τιμή του bitcoin έφτασε την ισοτιμία 1BTC = $25 000 (Βλέπε Εικόνα 3.1), τιμή η οποία μεταβάλλεται με απρόβλεπτες μεταβολές.

Ο αριθμός των bitcoin που υπάρχουν στο τέλος του 2020 φτάνουν τα 18 580 000. Τα bitcoin αυτά υφίστανται στα ηλεκτρονικά πορτοφόλια των χρηστών και διακινούνται μέσω των συναλλαγών κατά τις οποίες μετακινείται ποσότητα κρυπτονομίσματος από ένα κόμβο σε ένα άλλο. Ο αριθμός αυτός μπορεί να αλλάξει μόνο όταν οι κόμβοι με μια διαδικασία που λέγεται **Εξόρυξη** κερδίζουν bitcoin σαν ανταμοιβή. Ωστόσο, ο μέγιστος αριθμός bitcoin που μπορεί να υπάρξει είναι 21 000 000. Με το 88,5% του κρυπτονομίσματος να έχει ήδη εξορυχθεί, παραμένουν λιγότερο από 2 500 000 διαθέσιμα για εξόρυξη. Εκτιμάται ότι τη χρονιά 2140 θα εξορυχθεί και το τελευταίο bitcoin (How Many Bitcoins Are There?).

Εικόνα 3.1. *Η μεταβολή στην τιμή 1 BTC από το 2014 μέχρι το 2020 (BitcoinBTC, 2020).*

3.2 Αλγόριθμοι στο Bitcoin

Η λειτουργεία ολόκληρου του δικτύου του Bitcoin, βασίζεται στη λειτουργεία κάποιων βασικών αλγορίθμων και πρωτοκόλλων. Αρχικά, οι συναρτήσεις κατακερματισμού είναι αναγκαίες στην αλυσίδα συστοιχιών και στο Bitcoin χρησιμοποιούνται 2, η SHA-256 και η RIPEMD-160. Στη συνέχεια, αφού χρησιμοποιείται κρυπτογραφία δημόσιου κλειδιού, απαιτείται ένας αλγόριθμος ο οποίος θα παράγει τα δημόσια και ιδιωτικά κλειδιά του δικτύου και στην προκειμένη περίπτωση είναι ο ECDSA με τη χρήση του secp256k1.

3.2.1 SHA-256 και RIPEMD-160

Όπως αναλύθηκε και στο Τμήμα 2.2, οι συναρτήσεις κατακερματισμού παίρνουν ένα μήνυμα εισόδου μεταβλητού μήκους και το μετατρέπουν σε ένα μήνυμα εξόδου σταθερού μήκους, το οποίο πρέπει να έχει συγκεκριμένες ιδιότητες ασφαλείας. Στην περίπτωση του Bitcoin, και οι δύο πιο πάνω συναρτήσεις κατακερματισμού ικανοποιούν τις απαιτήσεις ασφαλείας αλλά έχουν διαφορετική τιμή εξόδου. Όπως καταδεικνύεται και από το όνομά τους η SHA-256 έχει έξοδο 256 bits και η RIPEMD-160 έξοδο 160 bits. Η ιδιότητα της εξόδου σταθερού μήκους είναι αυτή που επιτρέπει σε όλα τα μηνύματα να υπογραφούν ψηφιακά, διότι για να υπογραφεί με το ιδιωτικό κλειδί ένα μήνυμα, πρέπει να είναι συγκεκριμένου μήκους. Έτσι, τις πλείστες φορές αυτό που υπογράφεται ψηφιακά δεν είναι το μήνυμα αλλά η τιμή κατακερματισμού του. Στο Bitcoin, σχεδόν στα πάντα εφαρμόζεται συνάρτηση κατακερματισμού εις διπλούν, είτε διπλά η SHA-256, είτε πρώτα η SHA-256 και στη συνέχεια η RIPEMD-160 για μικρότερη τιμή κατακερματισμού.

3.2.2 secp256k1-ECDSA

Όλες οι διαδικασίες που πραγματοποιούνται στο δίκτυο του Bitcoin χρησιμοποιούν κρυπτογραφία δημόσιου κλειδιού και έτσι απαιτείται η ύπαρξη ενός δημόσιου και ενός ιδιωτικού κλειδιού. Το δύο αυτά κλειδιά παράγονται με κρυπτογραφία ελλειπτικής καμπύλης και πιο συγκεκριμένα με τον αλγόριθμο Elliptic Curve Digital Signature Algorithm (**ECDSA**), ο οποίος είναι μια παραλλαγή του Digital Signature Algorithm (DSA). Με τη χρήση του αλγόριθμου αυτού και της καμπύλης secp256k1 παράγονται ιδιωτικά κλειδιά μήκους 256 bits και δημόσια κλειδιά μήκους 65 bytes σε αποσυμπιεσμένη μορφή και 33 bytes σε συμπιεσμένη μορφή (Bashir, 2018). Το ιδιωτικό κλειδί βρίσκεται στην κατοχή του κόμβου στον οποίο ανήκει και είναι ο μόνος που μπορεί να το χρησιμοποιήσει, ενώ το δημόσιο κλειδί διαδίδεται σε ολόκληρο το δίκτυο.

3.2.3 Λοιποί Αλγόριθμοι

Τα ιδιωτικά κλειδιά συνήθως είναι κωδικοποιημένα με τη χρήση του **Wallet Import Format (WIF)**, το οποίο μετατρέπει τα 256 bits του ιδιωτικού κλειδιού σε μια πιο εύχρηστη σε ψηφιακό πορτοφόλι σειρά χαρακτήρων.

ιδιωτικό κλειδί	A3ED7EC8A03667180D01FB4251A546C2B9F2FE33507C68B7D9D4E1FA5714195201
WIF format	L2iN7umV7kbr6LuCmgM27rBnptGbDVc8g4ZBm6EbgTPQXnj1RCZP

Πίνακας 3.1. *Παράδειγμα μετατροπής ιδιωτικού κλειδιού σε μορφή WIF* (Bashir, 2018).

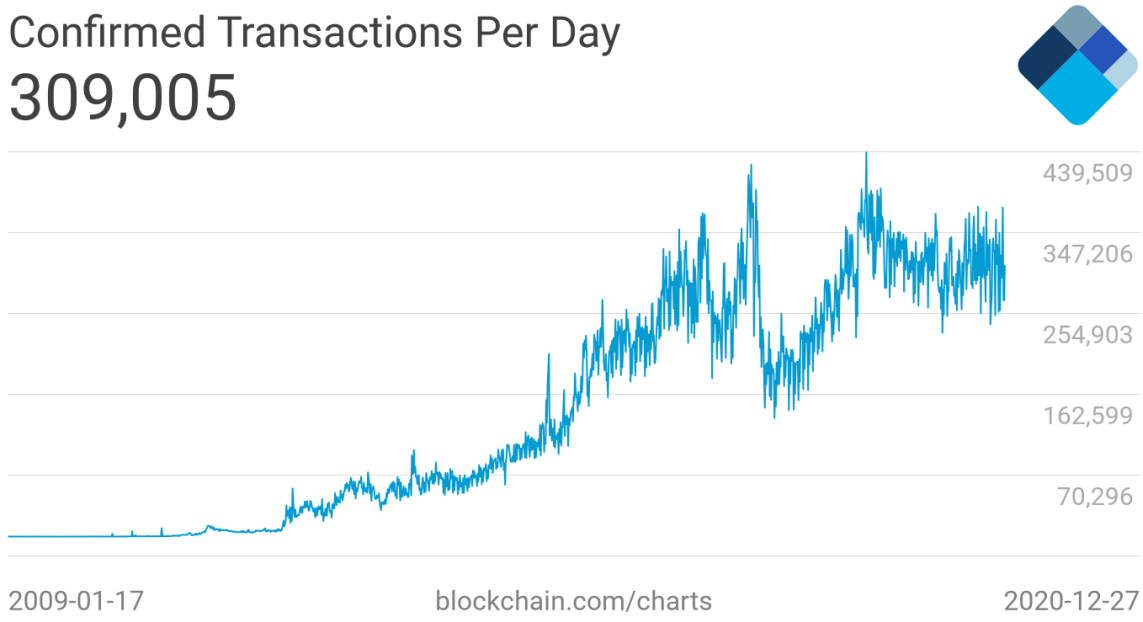
Οι **Διευθύνσεις** των κόμβων που συμμετέχουν στο δίκτυο του Bitcoin δημιουργούνται με την εφαρμογή αρχικά της συνάρτησης κατακερματισμού Sha-256 και στη συνέχεια της RIPEMD-160, πάνω στο δημόσιο κλειδί του κόμβου. Στην τιμή κατακερματισμού που προκύπτει, προστίθενται ο αριθμός έκδοσης και στη συνέχεια κωδικοποιείται με ένα σχήμα κωδικοποίησης Base58Check. Η τελική μορφή μιας **Διεύθυνσης Bitcoin** έχει μήκος 26-35 χαρακτήρες και ξεκινά με το ψηφίο 1 ή 3. Ένα παράδειγμα Διεύθυνσης Bitcoin θα μπορούσε να είναι 1ANAguGG8bikEv2fYsTBnRUmx7QUcK58wt (Bashir, 2018). Αφού η διεύθυνση βασίζεται κυρίως στο δημόσιο κλειδί του κόμβου, το οποίο είναι γνωστό σε ολόκληρο το δίκτυο, τότε όλοι οι κόμβοι γνωρίζουν τη διεύθυνση όλων των υπολοίπων ανά πάσα στιγμή.

Για τη λειτουργεία των συναλλαγών και τη δημιουργία νέων μπλοκ στο Bitcoin, πέραν της εκμετάλλευσης των συναρτήσεων κατακερματισμού σε διάφορους τομείς, γίνεται χρήση και του **Δένδρου Merkle** το οποίο αναλύθηκε στο Τμήμα 2.3. Στο δίκτυο του Bitcoin ο ριζικός κόμβος του Δένδρου Merkle αποτελεί τη συνάρτηση κατακερματισμού όλων των προηγούμενων συναλλαγών, έτσι μπορεί να επαληθευθεί κάποια συναλλαγή ανά πάσα στιγμή.

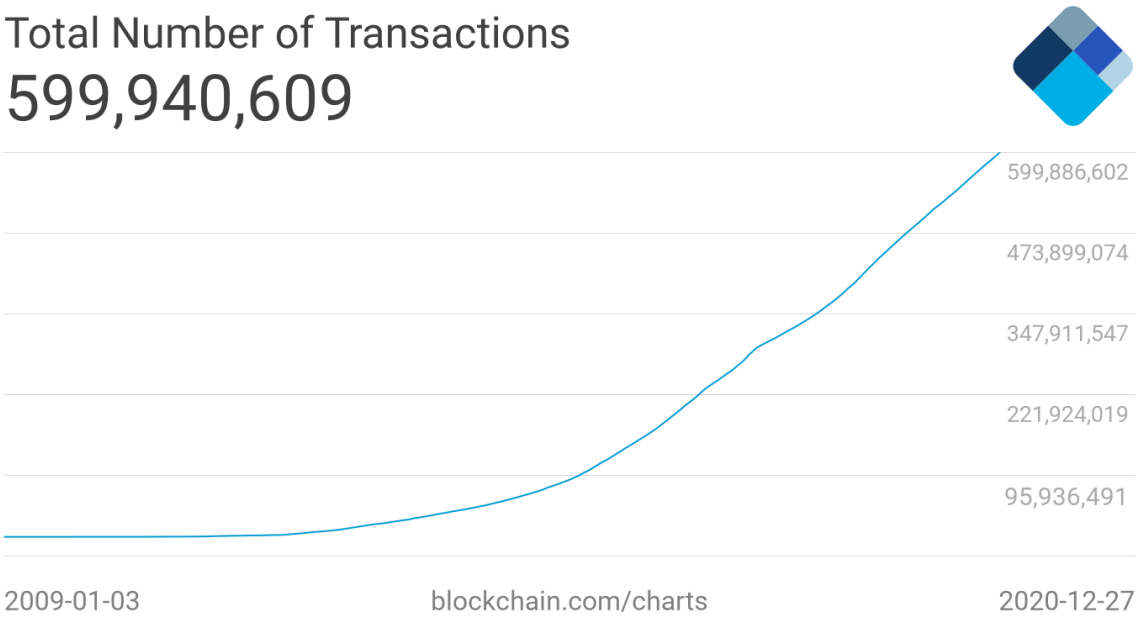
3.3 Συναλλαγές στο Bitcoin

Προκειμένου το δίκτυο κόμβων του Bitcoin να παραμένει ενεργό και να υπάρχει εξέλιξη, οι συναλλαγές είναι απαραίτητες. Είναι αυτές που δίνουν ζωή στο σύστημα και χωρίς αυτές θα παραλύσει. Το πιο απλό παράδειγμα συναλλαγής στο Bitcoin είναι η αποστολή ποσότητας bitcoin από τη **Διεύθυνση Bitcoin** ενός εγγεγραμμένο χρήστη προς μια άλλη, ωστόσο συναλλαγή μπορεί να θεωρηθεί και μια πιο σύνθετη κίνηση στο σύστημα.

Με την ανάπτυξη του Bitcoin και την αύξηση των κόμβων που συμμετέχουν σε αυτό, παρατηρήθηκε ραγδαία αύξηση και στις συναλλαγές που πραγματοποιούνται. Πιο συγκεκριμένα, στο τέλος του 2020 πραγματοποιούνται κατά μέσο όρο 300 000 συναλλαγές την ημέρα σε ολόκληρο το δίκτυο του Bitcoin και το σύνολο των συναλλαγών που έχουν πραγματοποιηθεί φτάνει περίπου τις 600 000 000.



Εικόνα 3.2. *Ο αριθμός των συναλλαγών που πραγματοποιούνται στο Bitcoin ανά ημέρα από το 2009 μέχρι το 2020 (Blockchain Charts, 2021).*



Εικόνα 3.3. *Ο συνολικός αριθμός των συναλλαγών που πραγματοποιούνται στο Bitcoin από το 2009 μέχρι το 2020 (Blockchain Charts, 2021).*

3.3.1 Δομή Συναλλαγής

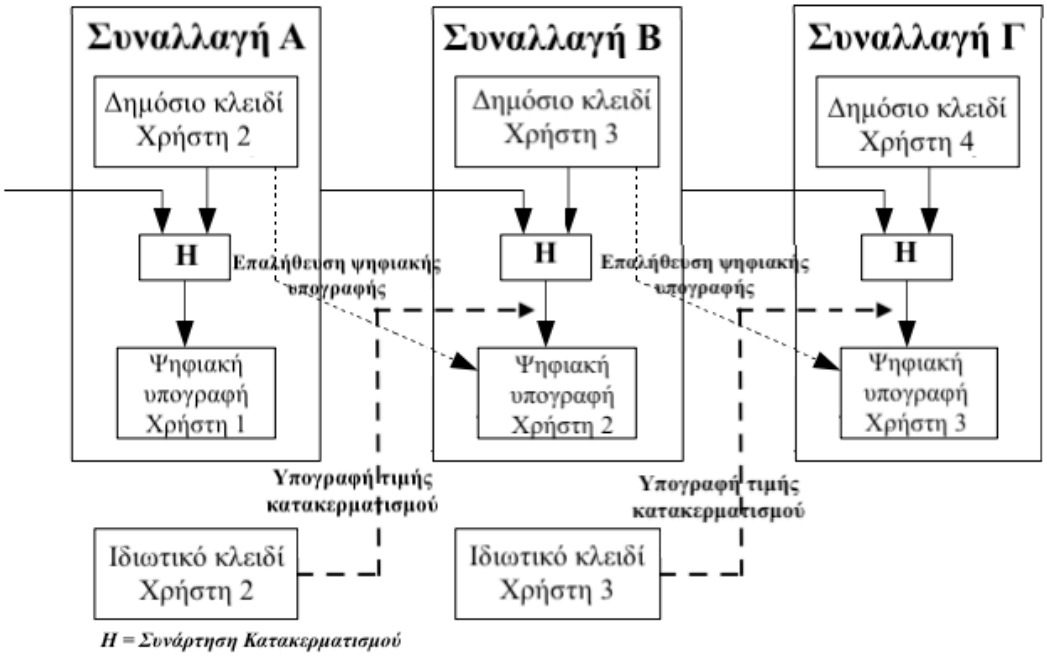
Στην απλούστερη της μορφή, η δομή μιας συναλλαγής περιλαμβάνει τα μεταδεδομένα, τις Εισόδους και τις Εξόδους μιας συναλλαγής. Το συνολικό μήκος μιας συναλλαγής δεν είναι σταθερό και εξαρτάται από τον αριθμό των Εισόδων και τον αριθμό των Εξόδων. Είσοδοι σε μια συναλλαγή πρέπει να είναι **UTXO (Unspent Transaction Output)**, δηλαδή έξοδοι από προηγούμενες συναλλαγές που δεν έχουν ξαναχρησιμοποιηθεί για άλλη συναλλαγή (Βλέπε Κεφάλαιο 2) και μπορεί να είναι περισσότερες έτσι ώστε να προστίθενται στο επιθυμητό ποσό που θα αποσταλεί. Έξοδοι σε μια συναλλαγή μπορεί να υπάρξουν περισσότερες από μία, ανάλογα με το πως θα χρησιμοποιηθούν τα bitcoin και ποια ποσότητα θα χαρακτηριστεί ως UTXO. Οπωσδήποτε όμως, το σύνολο των Εισόδων πρέπει να ισούται με το σύνολο των Εξόδων οποιασδήποτε συναλλαγής. Διαφορετικά θα υπάρχει διαρροή ηλεκτρονικού χρήματος, κάτι που θα αντιστοιχούσε στην πραγματικότητα με το να χαθούν χαρτονομίσματα.

Μέρος	Μέγεθος	Περιγραφή
Αριθμός Εκδοχής	4 bytes	Για διατύπωση κανόνων προς τους miners και τους κόμβους για την επεξεργασία των συναλλαγών
Μετρητής Εισόδου	1-9 bytes	Ο αριθμός των Εισόδων που περιέχονται στη συναλλαγή (θετικός ακέραιος)
Λίστα με τις Εισόδους	Μεταβλητό	Το μέγεθος εξαρτάται από το συνολικό αριθμό των Εισόδων και το μέγεθος αυτών
Μετρητής Εξόδου	1-9 bytes	Ο αριθμός των Εξόδων που περιέχονται στη συναλλαγή (θετικός ακέραιος)
Λίστα με τις Εξόδους	Μεταβλητό	Το μέγεθος εξαρτάται από το συνολικό αριθμό των Εξόδων και το μέγεθος αυτών
Χρόνος Κλειδώματος	4 bytes	Ο συντομότερος χρόνος που η συναλλαγή γίνεται έγκυρη με βάση τον timestamp server

Πίνακας 3.2. *Ενδεικτική δομή συναλλαγής Bitcoin* (Bashir, 2018).

3.3.2 Διενέργεια Συναλλαγής

Για να ολοκληρωθεί μια συναλλαγή στο Bitcoin, απαιτείται η χρήση όλων των αλγόριθμων του Τμήματος 3.2 με την κατάλληλη σειρά. Ένα ηλεκτρονικό νόμισμα ή κρυπτονόμισμα (bitcoin), ορίζεται σαν μια αλυσίδα από ψηφιακές υπογραφές. Για να το αποστείλει ο ιδιοκτήτης σε κάποιον άλλον και να πραγματοποιήσει έτσι μια συναλλαγή Bitcoin, πρέπει να υπογράψει ψηφιακά την τιμή κατακερματισμού της προηγούμενης συναλλαγής και του δημόσιου κλειδιού του αποδέκτη του ψηφιακού νομίσματος (Nakamoto, 2008). Όταν αυτός παραλάβει το πακέτο αυτό, μπορεί να επαληθεύσει την ψηφιακή υπογραφή του αποστολέα χρησιμοποιώντας το δημόσιο του κλειδί του, το οποίο είναι γνωστό σε ολόκληρο το δίκτυο έτσι ώστε όλοι οι κόμβοι να μπορούν να επαληθεύσουν όλες τις συναλλαγές και έτσι να τις συμπεριλάβουν στη συστοιχία που δημιουργούν.



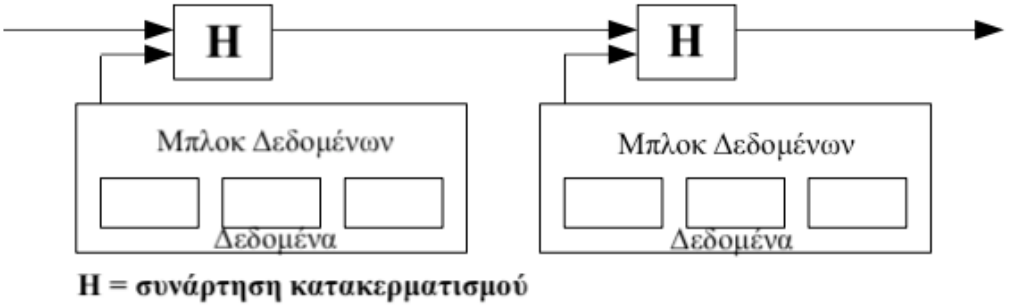
Εικόνα 3.4. *Η εφαρμογή τριών συναλλαγών στη σειρά με το ίδιο ψηφιακό νόμισμα όπως περιγράφεται στην Υποενότητα 3.3.2. Η Συναλλαγή Α αφορά αποστολή του ψηφιακού νομίσματος από το Χρήστη 1 στο Χρήστη 2, η Συναλλαγή Β από το Χρήστη 2 στο Χρήστη 3 και η Συναλλαγή Γ από το Χρήστη 3 προς ένα Χρήστη 4 (Nakamoto, 2008).*

3.3.3 Timestamp Server

Παρόλο που ο παραλήπτης της ποσότητας bitcoin μπορεί με ευκολία να επαληθεύσει με το δημόσιο κλειδί του αποστολέα ότι όντως αυτός έκανε τη συναλλαγή, δεν είναι το ίδιο εύκολο να διακριβώσει αν το ψηφιακό νόμισμα έχει χρησιμοποιηθεί σε πάνω από μια συναλλαγή. Σε μια κανονική ηλεκτρονική αγορά μέσω του διαδικτύου, η λύση σε αυτό το πρόβλημα είναι μια έμπιστη τρίτη οντότητα, συνήθως μια τράπεζα ή χρηματοοικονομικός οργανισμός, που διαχειρίζεται όλες τις συναλλαγές και έτσι μπορεί να ελέγξει ότι δεν γίνεται διπλή χρήση για τα ίδια χρήματα. Σε ένα αποκεντρωτικό σύστημα ωστόσο όπως είναι το Bitcoin, δεν υπάρχει μια κεντρική οντότητα και έτσι πρέπει να υπάρχει ένας άλλος τρόπος να μπορούν όλοι οι κόμβοι να εξακριβώσουν ότι το ψηφιακό νόμισμα που συμπεριλαμβάνεται στη συναλλαγή δεν έχει χρησιμοποιηθεί νωρίτερα σε άλλη συναλλαγή.

Για να γίνει αυτό, πρέπει αρχικά όλες οι συναλλαγές να αναμεταδίδονται δημόσια σε ολόκληρο το δίκτυο και να υπάρχει απόδειξη για το χρόνο διενέργειας της συναλλαγής, έτσι ώστε όλοι οι κόμβοι να συμφωνήσουν σε ένα κοινό ιστορικό συναλλαγών με κριτήριο ποια συναλλαγή πραγματοποιήθηκε πρώτη **(Nakamoto, 2008)**. Ένας **timestamp server** μπορεί να παρέχει την απαραίτητη απόδειξη για το χρόνο διενέργειας της συναλλαγής. Το επιτυγχάνει αυτό

υπολογίζοντας την τιμή κατακερματισμού από ένα μπλοκ αντικειμένων, εφαρμόζοντας χρονική σήμανση πάνω της και με τη ευρεία δημοσίευση της σε ολόκληρο στο δίκτυο του Bitcoin. Με αυτό τον τρόπο, αποδεικνύεται ότι τα δεδομένα υπήρχαν τη δεδομένη χρονική στιγμή αφού συμπεριλαμβάνονται στην τιμή κατακερματισμού. Κάθε χρονική σήμανση περιλαμβάνει την προηγούμενη χρονική σήμανση στην τιμή κατακερματισμού του, δημιουργώντας έτσι μια συνεχόμενη αλυσίδα.



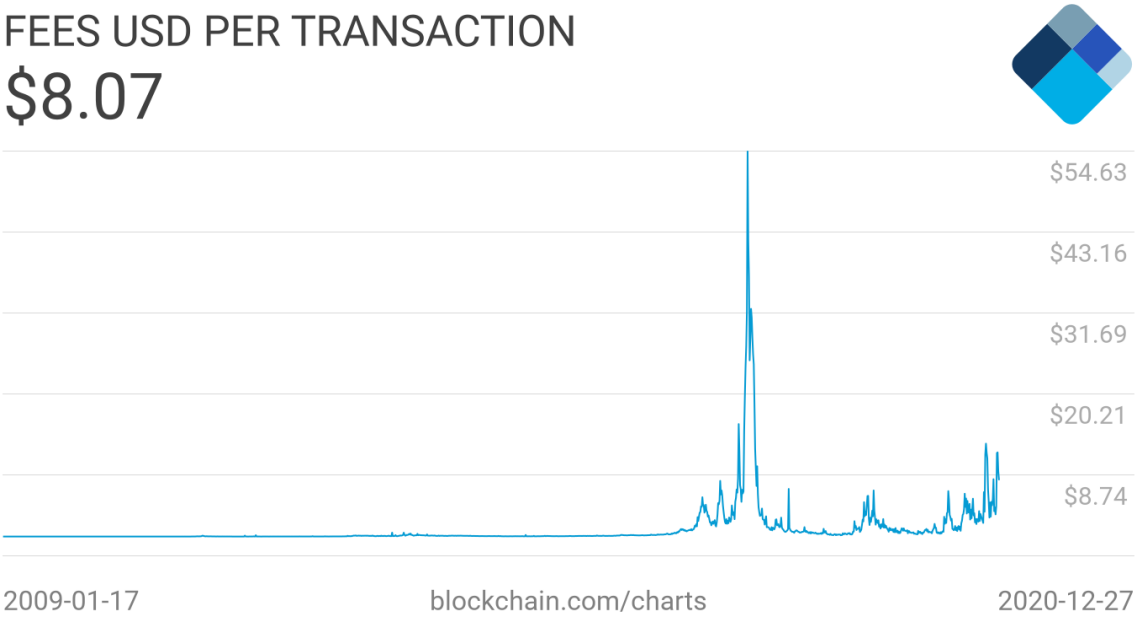
Εικόνα 3.4. *Ενδεικτική εφαρμογή του timestamp server για τοποθέτηση χρονική σήμανσης (Nakamoto, 2008).*

3.3.4 Τέλη Συναλλαγής

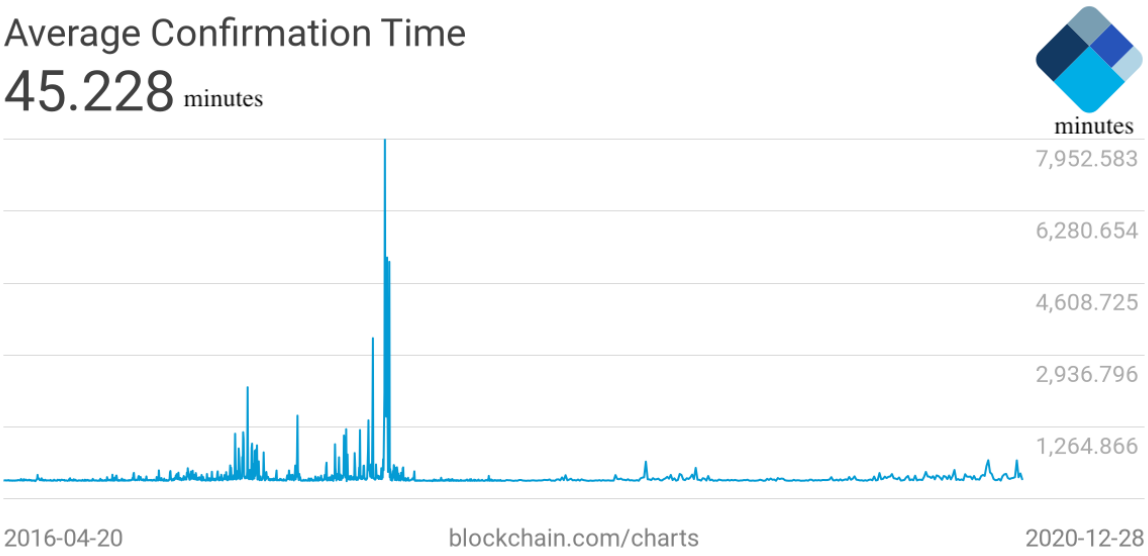
Σε μια συναλλαγή στο Bitcoin, πέραν από την ποσότητα κρυπτονομίσματος που θα αποστείλει, ο κάθε κόμβος χρεώνεται επίσης κάποιο επιπρόσθετο ποσό το οποίο ονομάζεται **Τέλος Συναλλαγής.** Το μέγεθος δεν είναι σταθερό και εξαρτάται από το μέγεθος και το βάρος της συναλλαγής. Ο σκοπός της χρέωσης αυτής είναι να ενθαρρύνουν του miners, οι οποίοι προτείνουν τα νέα μπλοκ στην αλυσίδα, να συμπεριλάβουν τη συναλλαγή στο μπλοκ που δημιουργούν και έτσι να γίνει αποδεκτή η συναλλαγή. Όλες οι συναλλαγές αφού δημοσιευτούν, συλλέγονται σε μια δεξαμενή μνήμης, από την οποία οι miners επιλέγουν ποιες θα συμπεριλάβουν στο μπλοκ τους πρώτα.

Ο χρόνος αποδοχής μιας συναλλαγής στο Bitcoin και ένταξης σε συστοιχία κυμαίνεται από 10 λεπτά μέχρι 12 ώρες **(Bashir, 2018)**, με το μέσο όρο το τέλος του 2020 να είναι περίπου 45 λεπτά. Τα Τέλη Συναλλαγής στο Bitcoin δεν είναι υποχρεωτικά, δηλαδή ακόμα και μια συναλλαγή με μηδενικά τέλη αποστέλλεται στη δεξαμενή μνήμης. Ωστόσο, ο χρόνος που παραμένει η συναλλαγή στη δεξαμενή εξαρτάται από το μέγεθος του τέλους συναλλαγής και τη δραστηριότητα του δικτύου. Αν το δίκτυο είναι συμφορημένο, ο χρόνος αποδοχής των συναλλαγών θα αυξηθεί και οι συναλλαγές με μεγαλύτερα Τέλη Συναλλαγής είναι πιο πιθανόν

να επιλεγούν πρώτες από τους miners, λόγω του μεγαλύτερου κέρδους που θα έχουν από αυτές. Στα τέλη του 2020, για κάθε συναλλαγή χρεώνονται τέλη συναλλαγής αξίας 6,5 ευρώ κατά μέσο όρο.



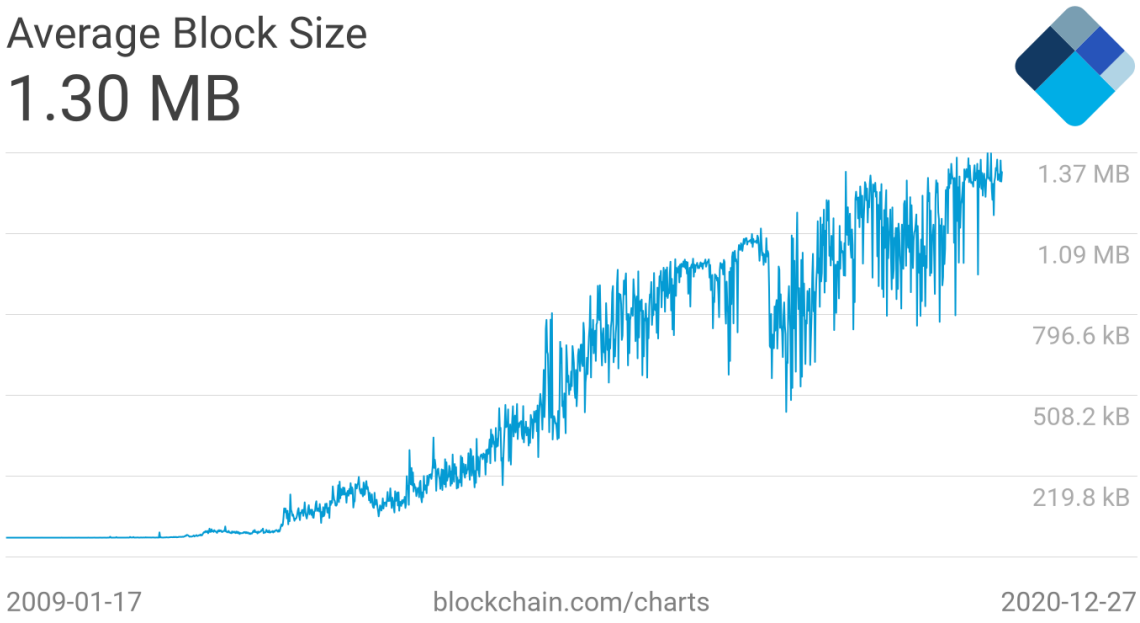
Εικόνα 3.5. *Το μέγεθος του Τέλους μια πραγματοποίηση μιας Συναλλαγής Bitcoin από το 2009 μέχρι το 2020 (Blockchain Charts, 2021).*



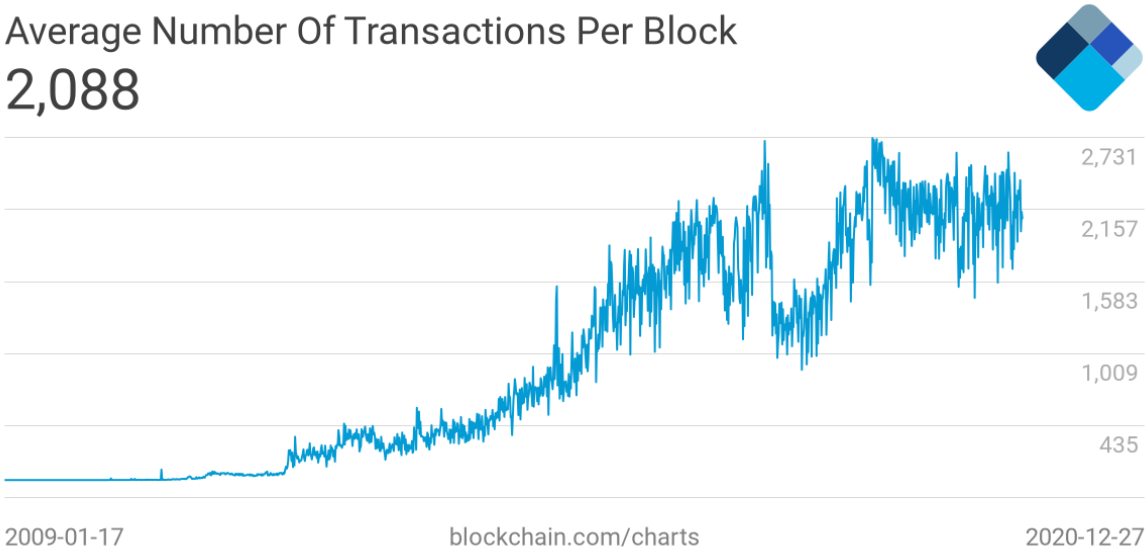
Εικόνα 3.6. *Ο μέσος όρος αποδοχής μιας Συναλλαγής Bitcoin από το 2009 μέχρι το 2020 (Blockchain Charts, 2021).*

3.4 Συστοιχία στο Bitcoin

Όταν μια Συναλλαγή πραγματοποιείται από κάποιο εγγεγραμμένο κόμβο στο σύστημα Bitcoin, δημοσιεύεται σε ολόκληρο το δίκτυο και όλοι οι κόμβοι την προσθέτουν στη νέα συστοιχία που δημιουργείται. Δεδομένου του μεγάλου αριθμού συναλλαγών που πραγματοποιούνται καθημερινά (πάνω από 300 000 την ημέρα), δεν είναι δυνατόν να αποθηκεύονται απευθείας στην αλυσίδα του Bitcoin. Έτσι, ομαδοποιούνται μαζί σε μια συστοιχία Bitcoin, το μέγεθος της οποίας είναι μεταβλητό και στο τέλος του 2020 φτάνει τα 1,3 megabytes. Με βάση το μέγεθος αυτό, σε κάθε συστοιχία τοποθετούνται περίπου 2 000 Συναλλαγές πριν να δημιουργηθεί καινούργια.



Εικόνα 3.7. *Ο μέσος όρος μεγέθους μιας συστοιχίας Bitcoin από το 2009 μέχρι το 2020 (Blockchain Charts, 2021).*



Εικόνα 3.8. *Ο μέσος όρος Συναλλαγών που τοποθετούνται εντός μιας συστοιχίας Bitcoin από το 2009 μέχρι το 2020 (Blockchain Charts, 2021).*

3.4.1 Δομή της Συστοιχίας

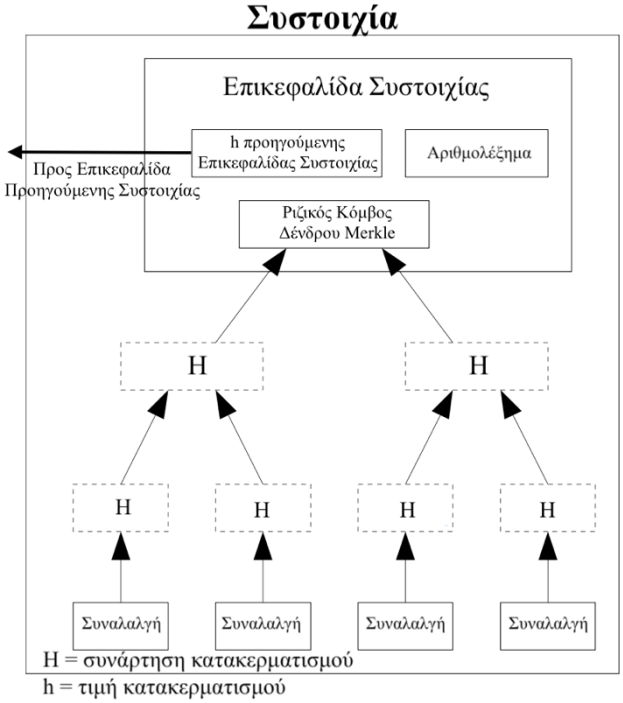
Στην Ενότητα 2.6. αναφέρθηκε μια ενδεικτική δομή συναλλαγής σε τυχαίο σύστημα κρυπτονομίσματος, η οποία είναι μια κοινή γραμμή για όλα τα συστήματα. Στο Bitcoin, μια συστοιχία αποτελείται από 4 γενικά μέρη, το μέγεθος της συστοιχίας, την επικεφαλίδα της συστοιχίας, τον μετρητή των συναλλαγών και τις συναλλαγές (όπως φαίνονται στον Πίνακα 3.3.). Η επικεφαλίδα της Συστοιχίας περιλαμβάνει απαραίτητες πληροφορίες για την επαλήθευση των συναλλαγών και τη λειτουργία ολόκληρης της αλυσίδας συστοιχιών, όπως την έκδοση, την τιμή κατακερματισμού της επικεφαλίδας της προηγούμενης συστοιχίας, τον Ριζικό Κόμβο του Δένδρου Merkle (Βλέπε Ενότητα 2.3.), το timestamp, τον βαθμό δυσκολίας και το αριθμολέξημα (nonce). Άρα εντός μιας Συστοιχίας περιλαμβάνονται 2 δείκτες κατακερματισμού, ένας που συνδέει όλες τις συναλλαγές που έχουν πραγματοποιηθεί εντός της Συστοιχίας και ένας που συνδέει την επικεφαλίδα της τρέχουσας συστοιχίας με την προηγούμενη και κατ' επέκταση με όλη την **Αλυσίδα Συστοιχιών.**

Μέρος	Μέγεθος	Περιγραφή
Μέγεθος Συστοιχίας	4 bytes	Δηλώνει το μέγεθος της Συστοιχίας
Επικεφαλίδα Συστοιχίας	80 bytes	Συμπεριλαμβάνει την έκδοση, την τιμή κατακερματισμού της επικεφαλίδας της προηγούμενης συστοιχίας, τον Ριζικό Κόμβο του Δένδρου Merkle, το timestamp, τον βαθμό δυσκολίας και το αριθμολέξημα (nonce).
Μετρητής Συναλλαγών	1-9 bytes	Δηλώνε τον συνολικό αριθμό των Συναλλαγών
Συναλλαγές	Μεταβλητό	Όλες οι Συναλλαγές που πραγματοποιήθηκαν και συμπεριλήφθηκαν στη Συστοιχία

Πίνακας 3.3. *Ενδεικτική δομή Συστοιχίας Bitcoin* (Bashir, 2018).

Μέρος	Μέγεθος	Περιγραφή
Έκδοση	4 bytes	Ο αριθμός έκδοσης της Συστοιχίας που υποδεικνύει τους κανόνες επικύρωσης
Τιμή κατακερματισμού επικεφαλίδας της προηγούμενης Συστοιχίας	32 bytes	Εφαρμόζεται διπλά η συνάρτηση κατακερματισμού SHA-256 πάνω στην επικεφαλίδα της προηγούμενης Συστοιχίας
Ριζικός Κόμβος του Δένδρου Merkle	32 bytes	Εφαρμόζεται διπλά η συνάρτηση κατακερματισμού SHA-256 πάνω στο Δένδρο Merkle
Timestamp	4 bytes	Δηλώνει το χρόνο δημιουργίας της Συστοιχίας
Βαθμός Δυσκολίας	4 bytes	Ο τρέχον Βαθμός Δυσκολίας για τη συγκεκριμένη Συστοιχία
Αριθμολέξημα (nonce)	4 bytes	Ένας αυθαίρετος αριθμός που μεταβάλλεται συνεχώς για να δημιουργηθεί μια τιμή κατακερματισμού κάτω από το Βαθμό Δυσκολίας της Συστοιχίας

Πίνακας 3.4. *Ενδεικτική δομή Επικεφαλίδας της Συστοιχίας Bitcoin* (Bashir, 2018).



Εικόνα 3.8. *Γραφική απεικόνιση μιας Συστοιχίας Bitcoin (Nakamoto, 2008).*

3.4.2 Δημιουργία της Συστοιχίας

Η αρχική δημιουργία της νέας Συστοιχίας που θα προστεθεί στην Αλυσίδα Συστοιχιών ξεκινά με μια διαδικασία που ονομάζεται **Mining** και θα αναλυθεί στην Ενότητα 3.5. Πιο κάτω αναφέρονται τα στάδια με τα οποία μια συναλλαγή εντάσσεται στο νέο μπλοκ και αυτό εντάσσεται στην Αλυσίδα Συστοιχιών.

- Ένας κόμβος πραγματοποιεί μια συναλλαγή και την αναμεταδίδει στο δίκτυο του Bitcoin.

- Όλοι οι κόμβοι επαληθεύουν τη συναλλαγή και την συμπεριλαμβάνουν στη συστοιχία που δημιουργούν.

- Όλοι οι κόμβοι προσπαθούν να βρουν τη λύση στο πρόβλημα για την Απόδειξη Εργασίας. Μέχρι να βρεθεί η λύση στο πρόβλημα, όλοι οι miners δημιουργούν τη δική τους εκδοχή της νέας Συστοιχίας στην οποία προσθέτουν τις συναλλαγές που επιλέγουν και επαληθεύουν.

- Όταν ένας κόμβος βρει τη λύση Απόδειξης Εργασίας, αναμεταδίδει τη Συστοιχία του σε όλο το δίκτυο.

- Οι υπόλοιποι κόμβοι επαληθεύουν τη Συστοιχία και την αποδέχονται μόνο αν όλες οι Συναλλαγές που συμπεριλαμβάνονται σε αυτή είναι έγκυρες.

- Η αποδοχή της Συστοιχίας εκφράζεται από τους κόμβους με το να προτείνουν νέο μπλοκ στην αλυσίδα, χρησιμοποιώντας την τιμή κατακερματισμού της Συστοιχίας που μόλις αποδέχτηκαν.

3.5 Εξόρυξη Bitcoin

Η Εξόρυξη είναι η διαδικασία κατά την οποία προτείνεται και προστίθενται καινούργια Συστοιχία στην αλυσίδα του Bitcoin. Καθημερινά γίνεται εξόρυξη 144 νέων μπλοκ, δηλαδή 1 μπλοκ κάθε 10 λεπτά περίπου. Στο σύνολο η Αλυσίδα Συστοιχιών του Bitcoin περιλάμβανε 663,513 Συστοιχίες στο τέλος του 2020. Οι εγγεγραμμένοι κόμβοι στο «Slushpool», οι οποίοι συμμετέχουν στη διαδικασία εξόρυξης είναι περίπου 200 000, αλλά στο σύνολό τους υπολογίζονται ότι υπάρχουν πάνω από 1 000 000 (How Many Bitcoins Are There?).

3.5.1 Απαιτήσεις Αλγόριθμου Εξόρυξης

Προκειμένου οι διαδικασίες στο Bitcoin να διατηρούνται ασφαλής και δίκαιες, ο αλγόριθμος Εξόρυξης πρέπει να εξασφαλίζει κάποιες βασικές απαιτήσεις. Ο Αλγόριθμός Εξόρυξης είναι ο αλγόριθμος που χρησιμοποιείται στο πρόβλημα Απόδειξης Εργασίας για την **εξόρυξη** νέων μπλοκ και bitcoin (θα αναλυθεί στην Υποενότητα 3.5.2).

- **Γρήγορη Επαλήθευση:** Ο αλγόριθμος ο οποίος καθορίζει το πρόβλημα που πρέπει να λυθεί για την Απόδειξη Εργασίας, οφείλει να είναι αρκετά δύσκολος και να απαιτεί ένα εύλογο χρονικό διάστημα. Ωστόσο, η επαλήθευση της λύσης πρέπει να μπορεί να γίνει όσο πιο εύκολα και γρήγορα είναι δυνατόν, έτσι ώστε όλοι οι κόμβοι να μπορούν να επικυρώσουν το καινούργιο μπλοκ.

- **Ευπροσάρμοστος Βαθμός Δυσκολίας:** Το πρόβλημα Απόδειξης Εργασίας απαιτείται να προσφέρει μεταβαλλόμενη δυσκολία στους miners, λόγω της ραγδαίας αύξησης της υπολογιστικής ισχύς. Αυτό γίνεται είτε αλλάζοντας ολόκληρο το πρόβλημα, είτε αλλάζοντας το βαθμό δυσκολίας αυτού, με σκοπό να κρατηθεί σταθερός ο χρόνος επίλυσης του προβλήματος και εισαγωγής νέου μπλοκ στην αλυσίδα.

- **Ελευθερία Προόδου:** Όλοι οι miners πρέπει να έχουν ευκαιρία για τη λύση, ανάλογη με την ισχύ κατακερματισμού τους (υπολογισμοί/δευτερόλεπτο). Ωστόσο, ακόμα και κόμβοι με μικρότερη υπολογιστική ισχύ πρέπει να έχουν πιθανότητες να βρουν τη λύση.

3.5.2 Απόδειξη Εργασίας στο Bitcoin

Όταν προτείνεται μια καινούργια Συστοιχία για ένταξη στην αλυσίδα συστοιχιών του Bitcoin, πρέπει ο miner που το προτείνει να αποδείξει ότι έχει ξοδεύει επαρκή ενέργεια και υπολογιστική ισχύ ως **Απόδειξη Εργασίας** (Βλέπε Ενότητα 2.8). Στο Bitcoin, αυτό γίνεται με την επίλυση ενός προβλήματος προ-εικόνας μέρους μιας τιμής κατακερματισμού, με μεταβλητό βαθμός δυσκολίας (Fekkes, 2018). Το πρόβλημα αυτό ικανοποιεί τις απαιτήσεις του Υποτμήματος 3.5.1 και σκοπός του είναι να βρεθεί ένα **Αριθμολέξημα (nonce)**, του οποίου η τιμή κατακερματισμού με διπλό SHA-256 να είναι κάτω από μια συγκεκριμένη τιμή. Με άλλα λόγια, ο miner ψάχνει την προ-εικόνα μιας τιμής κατακερματισμού που να είναι μικρότερη από αυτή που ζητείται στο πρόβλημα Εξόρυξης.

Στο Bitcoin, η ζητούμενη τιμή κατακερματισμού πρέπει να ξεκινά με ένα προκαθορισμένο αριθμό μηδενικών bits, έτσι ώστε οποιοδήποτε Αριθμολέξημα με τιμή κατακερματισμού μικρότερη από αυτή να αποτελεί τη λύση του προβλήματος (Nakamoto, 2008). Η εργασία που απαιτείται για την επίλυση του προβλήματος αυτού είναι εκθετική στον αριθμό των μηδενικών bits που ζητούνται, ενώ η επαλήθευσή του απαιτεί τον υπολογισμό μόνο της τιμής κατακερματισμού της λύσης του προβλήματος. Ο βαθμός δυσκολίας μεταβάλλεται μειώνοντας ή αυξάνοντας τον αριθμό των ζητούμενων μηδενικών στην αρχή της τιμής κατακερματισμού, αυξάνοντας ή μειώνοντας το πλήθος των πιθανών λύσεων και έτσι κάνοντας ευκολότερο ή δυσκολότερο το πρόβλημα αντίστοιχα. Όταν βρεθεί η λύση στο πρόβλημα από ένα κόμβο, τότε αυτός αναμεταδίδει τη Συστοιχία που δημιούργησε, η οποία περιέχει τις Συναλλαγές που επαλήθευσε και συμπεριέλαβε σε αυτή. Οι υπόλοιποι κόμβοι στη συνέχεια επαληθεύουν τη Συστοιχία και τις Συναλλαγές της, την προσθέτουν στην Αλυσίδα Συστοιχιών και συνεχίζουν να χτίζουν πάνω σε αυτή.

3.5.3 Συστήματα Εξόρυξης bitcoin

Από το 2009 που ξεκίνησε τη λειτουργία του το Bitcoin, υπήρξαν διάφορα συστήματα που χειρίζονται τη συνάρτηση κατακερματισμού SHA-256, με σκοπό τη βελτιστοποίηση της Εξόρυξης. Αρχικά, ο υπολογισμός του SHA-256 μπορούσε να γίνει με το τον πιο απλό

υπολογιστή με τη χρήση του **επεξεργαστή** του **(CPU)**. Ωστόσο, αυτή η μέθοδος εξόρυξης εκμεταλλεύτηκε για λίγο περισσότερο από ένα χρόνο λόγω της εισόδου των **καρτών γραφικών (GPU)** στο παιχνίδι. Η Εξόρυξη με κάρτα γραφικών, παρόλο που ήταν πιο επικερδής από τη χρήση του επεξεργαστή, εγκαταλείφθηκε γρήγορα λόγω της ραγδαίας αύξησης του βαθμού δυσκολίας του προβλήματος εξόρυξης. Η νέα μέθοδος εξόρυξης μετά από αυτό ήταν το **Field Programmable Gate Array (FPGA)**, το οποίο ήταν βασικά ένα κύκλωμα το οποίο μπορούσε να προγραμματιστεί για διενέργεια συγκεκριμένων λειτουργιών, όπως σε αυτή την περίπτωση υπολογισμό τιμών κατακερματισμού με SHA-256. Η σχεδίαση όμως των **Application Specific Integrated Circuit (ASIC)**, άφησε τα FPGA στο παρελθόν. Τα ACIS είναι ειδικά διαμορφωμένα εξαρτήματα, τα οποία σχεδιάστηκαν συγκεκριμένα για την εκτέλεση του SHA-256 και τα πολλαπλά ACIS στη σειρά αποτελούν την πιο ευνοϊκή μέθοδο εξόρυξης στο τέλος του 2020. Στο σύνολό τους, υπολογίζεται ότι υπάρχουν περίπου 1 000 000 κόμβοι εξόρυξης (How Many Bitcoins Are There?).

Αφού τα εξαρτήματα **Application Specific Integrated Circuit (ASIC)** δημιουργήθηκαν ειδικά για την εξόρυξη στο Bitcoin, μπορούν να επιλύσουν τα προβλήματα Εξόρυξης πολύ πιο γρήγορα από ένα κανονικό υπολογιστή με αποτέλεσμα να κυριαρχήσουν στο δίκτυο εξόρυξης. Λόγω του κινδύνου αυτού, το πρόβλημα εξόρυξης πρέπει να προσαρμοστεί έτσι ώστε να μειώσει ή να εκμηδενίσει το χάσμα μεταξύ των ASIC και των κανονικών υπολογιστών. Αυτό επιτυγχάνεται μέσω προβλημάτων που η δυσκολία του υπόκειται στη μνήμη και όχι στην υπολογιστική ισχύ. Με αυτόν τον τρόπο ένας κανονικός κόμβος θα έχει ίδια πιθανότητα για εύρεση της λύσης με ένα κόμβο με ASIC και έτσι το πρόβλημα αποκτά **Αντίσταση κατά ASIC** (Fekkes, 2018)**.**

3.5.4 Ανταμοιβή Εξόρυξης

Όπως αναφέρθηκε και πιο πριν, όταν ένας κόμβος βρει τη λύση στο πρόβλημα Απόδειξης Εργασίας, διαδίδει τη Συστοιχία του σε όλους τους κόμβους για αποδοχή στην αλυσίδα και παίρνει μια ποσότητα bitcoin ως αντιστάθμιση του κόστους που είχε και ως ανταμοιβή της προσπάθειας που προσφέρει στο δίκτυο του Bitcoin. Η ποσότητα που προσφέρεται κάθε φορά ξεκίνησε με 50 BTC με τη δημιουργία του Bitcoin το 2009 και μειώνεται στο μισό κάθε 210 000 Συστοιχίες που προσθέτονται στην Αλυσίδα Συστοιχιών. Η πρώτη μείωση σε 25 BTC πραγματοποιήθηκε τον Νοέμβριο του 2012, η δεύτερη μείωση σε 12,5 BTC τον Ιούλιο του 2016 και η τρίτη σε 6,25 BTC τον Μάιο του 2020. Η επόμενη μείωση σε 3,125 BTC υπολογίζεται να γίνει το έτος 2024 όταν η Αλυσίδα Συστοιχιών φτάσει τα 840 000 μπλοκ (Bashir, 2018). Η

ανταμοιβή είναι ο λόγος που οι κόμβοι συμμετέχουν στην αλυσίδα και έτσι εγείρεται η ερώτηση του κίνητρου για τους κόμβους αφού το Bitcoin φτάσει τα 21 000 000 BTC και δεν παράγονται άλλα bitcoin για να προσφερθούν σαν ανταμοιβή. Η απάντηση είναι τα **Τέλη Συναλλαγής**, τα οποία θα αποτελούν την ανταμοιβή του κόμβου που βρίσκει τη λύση (Fekkes, 2018).

Κεφάλαιο 4
Ethereum

Με την κυκλοφορία του **Bitcoin** το 2009, αποδείχτηκε δυνατή η χρήση του διαδικτύου για τη δημιουργία ενός αποκεντρωτικού συστήματος μεταφοράς ηλεκτρονικού χρήματος, το οποίο λειτουργεί με βασική ιδέα την κρυπτογραφική ασφάλεια και δεν έχει ανάγκη μια έμπιστη κεντρική οντότητα (Wood, 2017). Πολλά άλλα κρυπτονομίσματα βασίστηκαν στην Αλυσίδα Συστοιχιών του Bitcoin, όπως και το **Ethereum** το οποίο ορίστηκε από τον Vitalik Buterin τον Νοέμβριο του 2013, κυκλοφόρησε για προ-πώληση το 2014 και στην αγορά το 2015. Ωστόσο, το Ethereum σε αντίθεση με την κλασική λειτουργία της αλυσίδας στο Bitcoin, εκμεταλλεύεται τις ιδιότητες που προσφέρει για να προσφέρει πολλά περισσότερα από απλά μια πλατφόρμα ηλεκτρονικού νομίσματος. Η ενσωματωμένη γλώσσα προγραμματισμού στο Ethereum, επιτρέπει τη ανάπτυξη αυθαίρετων προγραμμάτων υπό τη μορφή των έξυπνων συμβάσεων (Βλέπε 4.1.3), και αποκεντρωμένων εφαρμογών οι οποίες βασίζουν τη λειτουργία τους πάνω στην Αλυσίδα Συστοιχιών, όπως παιχνίδια, διαφόρων ειδών εφαρμογές (apps) και αποκεντρωμένη αποθήκευση αρχείων (Fekkes, 2018).

4.1 Εισαγωγή στο Ethereum

Αφού το Ethereum είναι ένα αποκεντρωτικό σύστημα που χτίζει πάνω στην Αλυσίδα Συστοιχιών, είναι επακόλουθο ότι θα έχει πολλές ομοιότητες με το Bitcoin. Πιο συγκεκριμένα, από την κυκλοφορία του, στο σύστημα του Ethereum υπάρχει μια ποσότητα ηλεκτρονικού χρήματος, το οποίο μπορεί να μεταφερθεί από κόμβο σε κόμβο με μια **Συναλλαγή** και ο μόνος τρόπος δημιουργίας νέας ποσότητας ηλεκτρονικού χρήματος είναι μέσω της διαδικασίας της **Εξόρυξης**. Ωστόσο, πολλές από τις λειτουργίες του Ethereum έχουν διαφοροποιήσεις οι οποίες θα αναλυθούν ακολούθως στο παρόν Κεφάλαιο.

Η βασική μονάδα του ψηφιακού νομίσματος στο Ethereum ονομάζεται **Ether**, το οποίο έχει αρκετές υποδιαιρέσεις για να γίνουν ευκολότερες κάποιες διαδικασίες, όπως αγορά **κρυπτογραφικού καυσίμου** για πραγματοποίηση μιας Συναλλαγής (περισσότερα στο Τμήμα

4.3. Συναλλαγές στο Ethereum). Η χαμηλότερη υποδιαίρεση του Ether είναι το **Wei** (1 Ether = $1x10^9$ Wei), καθώς οι υπόλοιπες υποδιαιρέσεις φαίνονται στον Πίνακα 4.1 σε σχέση με τον αριθμό των Wei που αντιστοιχούν.

Μονάδα Μέτρησης	Αξίας σε Wei	Αριθμός Wei
Wei	1 Wei	1
KWei	$1x10^3$ Wei	1 000
Mwei	$1x10^6$ Wei	1 000 000
Gwei	$1x10^9$ Wei	1 000 000 000
Micro Ether	$1x10^{12}$ Wei	1 000 000 000 000
Milli Ether	$1x10^{15}$ Wei	1 000 000 000 000 000
Ether	$1x10^{18}$ Wei	1 000 000 000 000 000 000

Πίνακας 4.1. *Οι υποδιαιρέσεις του **Ether**, σε αντιστοιχία με την αξία τους σε **Wei**, που είναι η μικρότερη υποδιαίρεση (Bashir, 2018).*

4.1.1 Τιμή και συνολικός αριθμός Ethereum

Η πιο μεγάλη μονάδα στο Ethereum όπως φαίνεται και στον πίνακα 4.1 είναι το **Ether** το οποίο συμβολίζεται ως **ETH.** Ομοίως με το Bitcoin, η αξία του κατά την αρχική του έκδοση ήταν πολύ χαμηλή, κάτι το οποίο άλλαξε πολύ από το 2015 μέχρι το 2021. Το Ether και γενικά το σύστημα κρυπτονομίσματος του Ethereum είναι σε έξαρση το 2021 και μπορούμε να πούμε ότι ακολουθεί την πορεία του Bitcoin με κάποια χρόνια καθυστέρηση. Στις αρχές του 2021 η τιμή του ether έφτασε την ισοτιμία 1 ETH = $1 300 (Βλέπε Εικόνα 4.1).

Κατά την προ-πώληση του Ethereum το 2014 αποφασίστηκε η αρχική ποσότητα Ether που θα εκδοθεί και ο ρυθμός έκδοσής του. Αποφασίστηκε ότι αρχικά θα εκδοθούν 60 000 000 Ether για τους συμμετέχοντες στην προ-πώληση και 12 000 000 για το κόστος ανάπτυξης του Ethereum. Πέραν αυτών, ο μόνος τρόπος να δημιουργηθεί καινούργιο ψηφιακό νόμισμα είναι μέσω της **Εξόρυξης** και της ανταμοιβής που δίνεται στη μορφή του ether (ETH) και αυτή τη στιγμή είναι 4 ETH ανά νέα συστοιχία. Σε αντίθεση με το Bitcoin, ανταμοιβή λαμβάνει και ο κόμβος ο οποίος βρίσκει λύση αλλά η Συστοιχία του δεν περιλαμβάνεται στη αλυσίδα. Ωστόσο, ο ρυθμός έκδοσης περιορίζεται στα 18 000 000 ether το χρόνο, με σκοπό να φτάσει την ποσότητα ether που χάνεται κάθε χρόνο από κακή χρήση, θάνατο των κάτοχων και απώλεια κωδικών (Fekkes, 2018).

Εικόνα 4.1. *Η μεταβολή στην τιμή 1 ETH από το 2015 μέχρι το 2021 (EthereumETH, 2021)*

4.1.2 Λογαριασμοί Ethereum

Προκειμένου να συμμετέχει κάποια οντότητα στο δίκτυο του Ethereum, πρέπει πρώτα να δημιουργήσει ένα **Λογαριασμό Ethereum**, ο οποίος θα έχει τα δικά του κλειδιά, δημόσιο και ιδιωτικό. Με βάση το δημόσιο κλειδί τους, για κάθε λογαριασμό εκδίδεται μια διεύθυνση μήκους 20 bytes για αναγνώρισή του στο δίκτυο, η οποία είναι ουσιαστικά τα τελευταία 160 bits της Keccak τιμής κατακερματισμού του δημόσιου κλειδιού (Bashir, 2018). Υπάρχουν δύο είδη λογαριασμών, ο **Λογαριασμός Εξωτερικής Ιδιοκτησίας** και ο **Λογαριασμός Σύμβασης.** Ένας Λογαριασμός Εξωτερικής Ιδιοκτησίας δεν περιέχει τον **Κώδικα του Ethereum** και μπορεί να στείλει μηνύματα εντός του δικτύου με τη δημιουργία και υπογραφή Συναλλαγών με το ιδιωτικό του κλειδί. Ένας Λογαριασμός Σύμβασης αντιθέτως, περιέχει τον προαναφερόμενο **Κώδικα** ο οποίος ενεργοποιείται κάθε φορά που ο λογαριασμός δέχεται ένα μήνυμα, επιτρέποντάς του να επεξεργαστεί τον εσωτερικό αποθηκευτικό χώρο και να στείλει μηνύματα ή να δημιουργήσει καινούργιες Έξυπνες Συμβάσεις (Buterin, 2013).

Οποιαδήποτε χρονική στιγμή, κάθε λογαριασμός βρίσκεται σε μια κατάσταση η οποία αν και δεν αποθηκεύεται αυτούσιο στην αλυσίδα συστοιχιών, διατηρείται στο τροποποιημένο δένδρο Merkle-Patricia (περισσότερα στο Υποτμήμα 4.2). Η **Κατάσταση Λογαριασμού** περιλαμβάνει τα εξής πεδία (Wood, 2017):

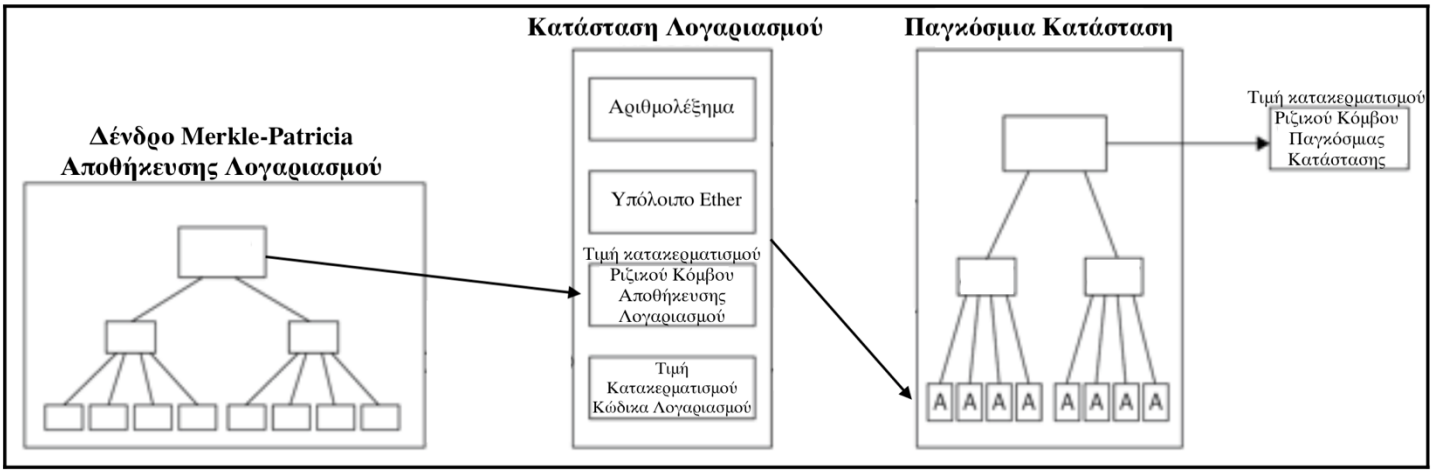
- **Αριθμολέξημα:** μια αυθαίρετη τιμή που μεταβάλλεται συνεχώς. Στους Λογαριασμούς Εξωτερικής Ιδιοκτησίας αντιστοιχεί στον αριθμό των συναλλαγών που αποστάλθηκαν από το λογαριασμό και αυξάνεται κατά ένα με την αποστολή μιας συναλλαγής. Στους Λογαριασμούς Σύμβασης αντιστοιχεί στον αριθμό έξυπνων συμβάσεων που δημιουργήθηκαν από το λογαριασμό.

- **Υπόλοιπο Ether:** μια τιμή η οποία ισούται με τον αριθμό των **Wei** που ανήκουν στο λογαριασμό-διεύθυνση.

- **Τιμή κατακερματισμού Ριζικού Κόμβου Αποθήκευσης:** η τιμή κατακερματισμού που προκύπτει από το ριζικό κόμβο του τροποποιημένου δένδρου Merkle-Patricia, το οποίο περιέχει τον αποθηκευτικό χώρο του λογαριασμού.

- **Τιμή Κατακερματισμού κώδικα:** το πεδίο αυτό είναι αμετάβλητο και περιέχει την Keccak τιμή κατακερματισμού του **Κώδικα** του Λογαριασμού, μήκους 256 bit.

Πέραν από την Κατάσταση Λογαριασμού, υφίσταται και μια **Παγκόσμια Κατάσταση**, η οποία είναι ένας χάρτης που αντιστοιχεί τις διευθύνσεις (μήκους 160 bit) με τις Καταστάσεις Λογαριασμού. Αν και η Παγκόσμια Κατάσταση δεν αποθηκεύεται στην Αλυσίδα Συστοιχιών του Ethereum, θεωρείται ότι η εφαρμογή θα διατηρήσει αυτή τη χαρτογράφηση σε ένα τροποποιημένο Δένδρο Merkle-Patricia (Fekkes, 2018). Ακολούθως, πάνω στο ριζικό κόμβο του Δένδρου της Παγκόσμιας Κατάστασης εφαρμόζεται μια συνάρτηση κατακερματισμού Keccak 256-bit και η τιμή που προκύπτει συμπεριλαμβάνεται στην Επικεφαλίδα της Συστοιχίας.



Εικόνα 4.2. *Απεικονίζεται η σύνδεση αποθηκευτικού χώρου του Λογαριασμού με την Κατάσταση Λογαριασμού, η οποία αντιστοιχείται με τη διεύθυνση του Λογαριασμού εντός του Δένδρου της Παγκόσμιας Κατάστασης και πως η τιμή κατακερματισμού του ριζικού κόμβου του Δένδρου αυτού συμπεριλαμβάνεται στην επικεφαλίδα της Συστοιχίας (Bashir, 2018).*

4.1.3 Έξυπνες Συμβάσεις

Οι **Έξυπνες Συμβάσεις** αφορούν μόνο το ένα είδος Λογαριασμού Ethereum, τους **Λογαριασμούς Σύμβασης.** Εξ' ορισμού μια Έξυπνη Σύμβαση είναι ένα ασφαλές και ασταμάτητο πρόγραμμα υπολογιστή που αντιπροσωπεύει μια συμφωνία που είναι αυτόματα εκτελέσιμη και επιβλητή (Buterin, 2013). Ένας Λογαριασμός Σύμβασης χαρακτηρίζεται από το Έξυπνο Συμβόλαιο, το οποίο περιέχει **κώδικα**. Ο κώδικας αυτός είναι γραμμένος σε μια γλώσσα bytecode χαμηλού επιπέδου με ονομασία «Ethereum virtual machine code (κώδικας EVM)» και εκτελείται αυτόματα όταν ο Λογαριασμός Σύμβασης λαμβάνει ένα μήνυμα ή συναλλαγή. Καινούργιες Έξυπνες Συμβάσεις δημιουργούνται μέσω μιας Συναλλαγής με κενό παραλήπτη και ένα πεδίο εκκίνησης (init field). Το πεδίο αυτό, αναθέτει τον κώδικα EVM για το λογαριασμό που θα δημιουργηθεί και στη συνέχεια απορρίπτεται αφού εκτελείται μόνο μια φορά κατά τη δημιουργία του λογαριασμού (Fekkes, 2018).

4.2 Αλγόριθμοι στο Ethereum

Στο Ethereum, όπως όλα τα δίκτυα κρυπτονομίσματος, βασίζει τη λειτουργία του σε ορισμένα κρυπτογραφικά πρωτόκολλα και αλγόριθμους. Στο Ethereum χρησιμοποιούνται δύο συναρτήσεις κατακερματισμού, η Keccab-256/512 και η FNV (Fowler Noll Vo). Επίσης, ο αλγόριθμος που θα παράγει τα δημόσια και ιδιωτικά κλειδιά του δικτύου είναι ο ECDSA με τη χρήση του secp256k1, ακριβώς με τον ίδιο τρόπος όπως και στο Bitcoin, Άλλοι αλγόριθμοι που χρειάζονται για την ορθή λειτουργία της κρυπτογραφικής αλυσίδας, είναι το τροποποιημένα Δένδρο Merkle-Patricia.

4.2.1 Keccak-256/512 και FNV

Η κύρια κρυπτογραφική συνάρτηση κατακερματισμού που χρησιμοποιείται στο Ethereum είναι η **Keccak-256** με έξοδο μια τιμή κατακερματισμού μήκους 256 bits ή **Keccak-512** με έξοδο μήκους 512 bits. Η προκειμένη συνάρτηση κατακερματισμού ανήκει στην οικογένεια των συναρτήσεων κατακερματισμού SHA-3 και η ιδιότητα που χρησιμοποιείται στην αλυσίδα του Ethereum είναι το σταθερό μήκος εξόδου. Αυτό επιτρέπει την απόδειξη ότι η είσοδος της τιμής κατακερματισμού υφίσταται, χωρίς να αποθηκεύεται αυτή ολόκληρη και ως εκ τούτου, η Keccak-256 χρησιμοποιείται για εξοικονόμηση αποθηκευτικού χώρου. Για παράδειγμα αντί να συμπεριλαμβάνεται ολόκληρο το Δένδρο των Συναλλαγών στην επικεφαλίδα της Συστοιχίας, εφαρμόζεται η Keccak-256 στο ριζικό του κόμβο και η τιμή κατακερματισμού που προκύπτει

συμπεριλαμβάνεται στην επικεφαλίδα. Έτσι, μπορεί οποιοσδήποτε με ένα απλό υπολογισμό Keccak-256 να ελέγξει ότι μια Συναλλαγή συμπεριλήφθηκε στη Συστοιχία, χωρίς να αποθηκεύσει ολόκληρο το Δένδρο στον υπολογιστή του. Η άλλη συνάρτηση κατακερματισμού που χρησιμοποιείται είναι η **Fowler Noll Vo (FNV)**, η οποία κατά κύριο λόγο εφαρμόζεται στον αλγόριθμο της Εξόρυξης (Ethash, περισσότερα στο τμήμα 4.5.1) και αποτελεί μη κρυπτογραφική συνάρτηση. Υπάρχει επιλογή μήκους εξόδου μεταξύ 32, 64, 128, 256, 512, 1024 bits και ο τρόπος λειτουργίας του βασίζεται σε μια αρχική τιμή μεταβολής και πρώτους αριθμούς (Fekkes, 2018).

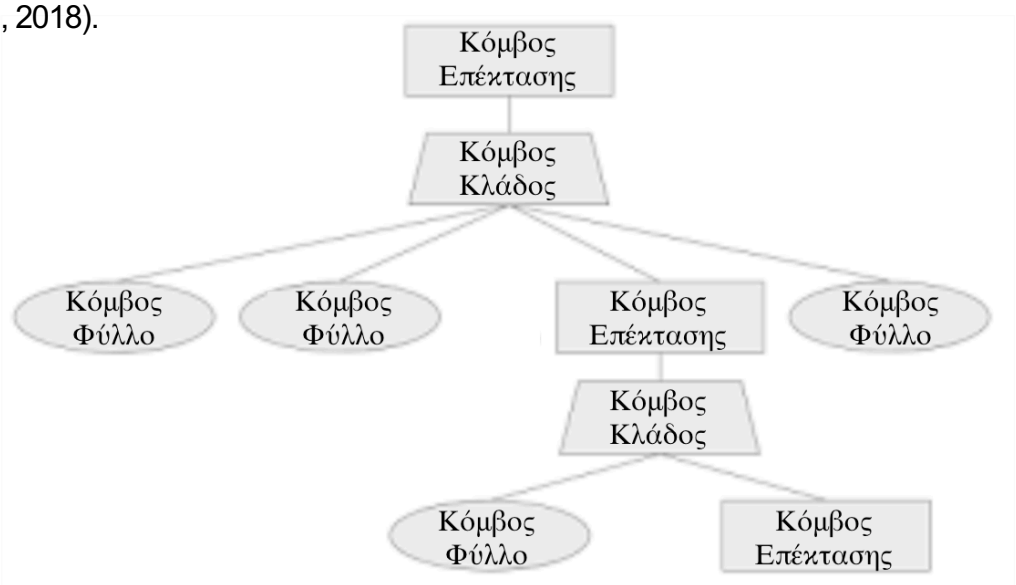
4.2.2 secp256k1-ECDSA

Η χρήση του δημόσιου και ιδιωτικού κλειδιού στο δίκτυο του Ethereum απαιτεί ένα αλγόριθμο ο οποίος θα ορίζει τα κλειδιά αυτά για κάθε κόμβο του δικτύου. Το δύο κλειδιά παράγονται με κρυπτογραφία ελλειπτικής καμπύλης και πιο συγκεκριμένα με τον αλγόριθμο Elliptic Curve Digital Signature Algorithm (**ECDSA**), ο οποίος είναι μια παραλλαγή του Digital Signature Algorithm (DSA). Με τη χρήση του αλγόριθμου αυτού και της καμπύλης secp256k1 παράγονται ιδιωτικά κλειδιά μήκους 256 bits και δημόσια κλειδιά μήκους 512 bits. Η **Διεύθυνση στο Ethereum** είναι τα τελευταία 160 bits της τιμής κατακερματισμού του δημόσιου κλειδιού του κάθε κόμβου (Fekkes, 2018).

4.2.3 Δένδρο Merkle-Patricia

Στο δίκτυο Ethereum χρησιμοποιείται ένα **τροποποιημένο Δένδρο Merkle-Patricia** για την αποθήκευση μιας κατάστασης, είτε αυτή είναι η **Κατάσταση ενός Λογαριασμού**, ή την **Παγκόσμια Κατάσταση**. Συνδυάζει κάποιες ιδιότητες από το Δένδρο Merkle (Τμήμα 2.3) και από το Δένδρο Patricia (Τμήμα 2.4) και προκύπτει ένα Δένδρο Merkle-Patricia που είναι ειδικά προσαρμοσμένο στις ανάγκες του Ethereum. Το Δένδρο αυτό περιέχει 3 είδη κόμβων. Αρχικά, οι **Κόμβοι Φύλλα** αποτελούν του τελικούς κόμβους του Δένδρου, δεν έχουν θυγατρικό κόμβο και περιέχει τη διαδρομή προς αυτόν και μια τιμή ανάλογα με τη χρήση του Δένδρου. Οι γονικοί κόμβοι ονομάζονται **Κόμβοι Κλάδοι** στον καθένα από τους οποίους μπορούν να συνδέονται μέχρι 16 Κόμβοι Φύλλα και επίσης περιέχουν μια τιμή σαν 17ο στοιχείο ενός πίνακα. Το τελευταίο είδος κόμβου είναι οι **Κόμβοι Επέκτασης**, οι οποίοι είναι ουσιαστικά μια συμπιεσμένη μορφή Κόμβων Κλάδων που περιείχαν μόνο ένα θυγατρικό κόμβο. Περιέχουν τη διαδρομή προς αυτούς και την τιμή κατακερματισμού του θυγατρικού τους κόμβου. Στο Δένδρο Merkle-Patricia, κάθε γονικός κόμβος περιέχει την τιμή κατακερματισμού του θυγατρικού του

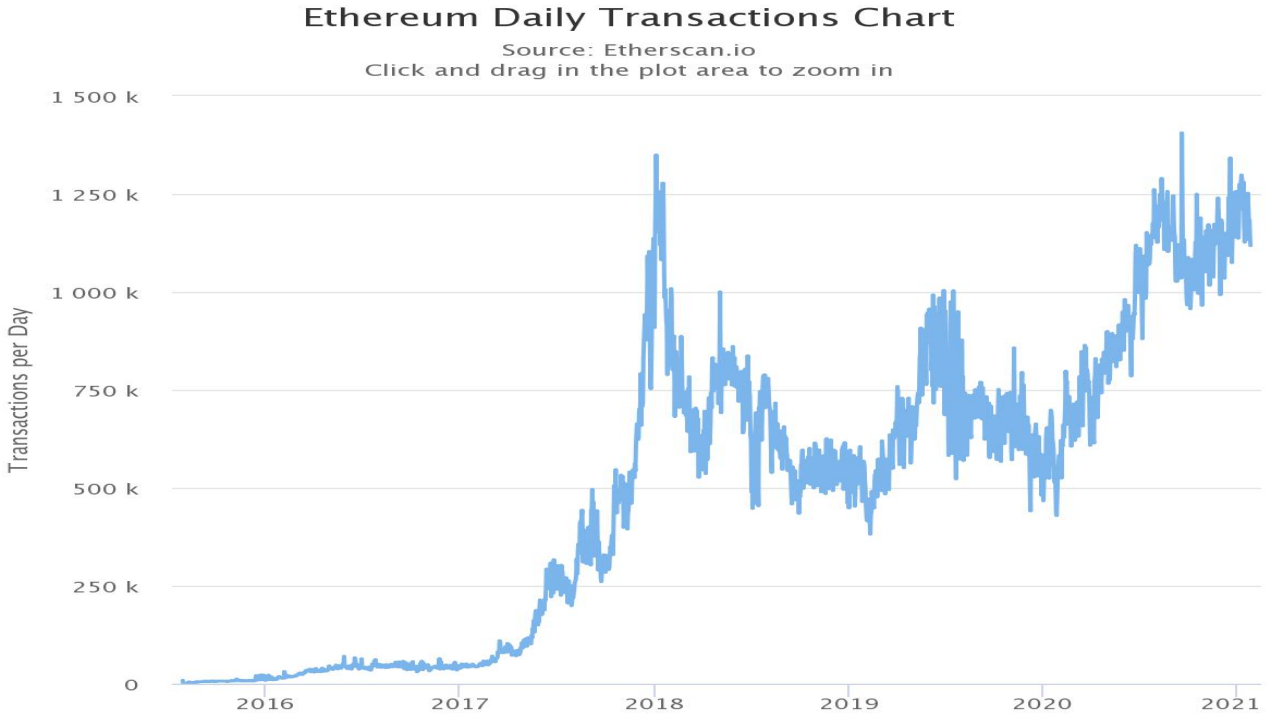
κόμβου και έτσι η τιμή κατακερματισμού αντιπροσωπεύει όλη την κατάσταση του Δένδρου (Kim, 2018).



Εικόνα 4.3. *Ενδεικτική μορφή* ***τροποποιημένου Δένδρου Merkle-Patricia*** *(Kim, 2018).*

4.3 Συναλλαγές στο Ethereum

Παρόλο που το Ethereum δεν είναι όσο διαδεδομένο όσο το Bitcoin, ο αριθμός των Συναλλαγών την ημέρα είναι μεγαλύτερος. Πιο συγκεκριμένα, το 2021 πραγματοποιούνται κατά μέσο όρο περίπου 500 000 συναλλαγές την ημέρα σε ολόκληρο το δίκτυο του Ethereum και το σύνολο των συναλλαγών που έχουν πραγματοποιηθεί φτάνει περίπου τις 985 000 000.



Εικόνα 4.4. *Ο συνολικός αριθμός των συναλλαγών που πραγματοποιούνται στο Ethereum από το 2015 μέχρι το 2021 (Ethereum Charts & Statistics, 2021).*

4.3.1 Είδη Συναλλαγών Ethereum

Μια **Συναλλαγή στο Ethereum** μπορεί να πραγματοποιηθεί τόσο από **Λογαριασμούς Εξωτερικής Ιδιοκτησίας** όσο από **Λογαριασμούς Συμβολαίου,** και ορίζεται ως ένα πακέτο δεδομένων που υπογράφεται ψηφιακά με τη χρήση ιδιωτικού κλειδιού και περιέχει τις απαραίτητες οδηγίες για να πραγματοποιήσει το σκοπό του (Bashir, 2018). Ανάλογα με το σκοπό αυτό, η Συναλλαγή μπορεί να κατηγοριοποιηθεί σε ένα από τα δύο πιο κάτω είδη συναλλαγών :

- **Συναλλαγή Μηνύματος Κλήσης:** παράγεται ένα Μήνυμα Κλήσης που μεταφέρει μηνύματα από ή προς λογαριασμούς συμβολαίου ή λογαριασμούς εξωτερικής ιδιοκτησίας. Όταν ο παραλήπτης είναι λογαριασμού συμβολαίου, με τη λήψη του Μηνύματος Κλήσης ο κώδικας του λογαριασμού εκτελείται για να εκτελεσθούν οι απαραίτητες λειτουργίες. Στην περίπτωση όμως όπου ο αποστολέας είναι ένας λογαριασμός εξωτερικής ιδιοκτησίας, τότε επιστρέφονται σε αυτόν τα δεδομένα που προκύπτουν από την εκτέλεση του κώδικα.

- **Συναλλαγή Δημιουργίας Συμβολαίου:** ο σκοπός αυτού του είδους της συναλλαγής είναι η δημιουργία ενός καινούργιου Λογαριασμού Συμβολαίου με το σχετικό κώδικα. Το **πεδίο εκκίνησης** (init field) είναι ένα πεδίο που υπάρχει μόνο σε αυτού του είδους συναλλαγών και ευθύνεται στον καθορισμό όλων των απαραίτητων χαρακτηριστικών του λογαριασμού που θα δημιουργηθεί. Καθορίζεται δηλαδή η διεύθυνση (160 bits), ο κώδικας (EMV code), το αριθμολέξιμα (αρχικά μηδέν), το υπόλοιπο σε Wei (το ποσό που αποστάλθηκε), η αποθήκευση (αρχικά κενή) και τέλος η τιμή κατακερματισμού του κώδικα του λογαριασμού.

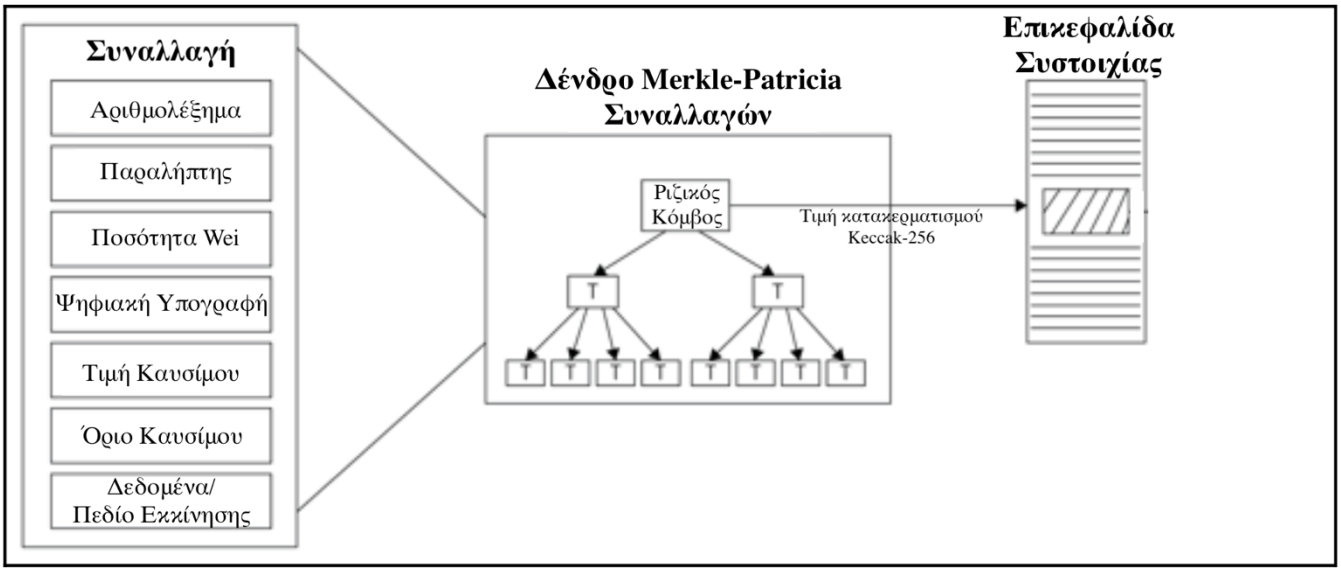
Το **Μήνυμα** στο Ethereum ορίζεται ως το πακέτο δεδομένων που αποστέλλεται από ένα λογαριασμό συμβολαίου προς ένα άλλο λογαριασμό συμβολαίου. Είναι παρόμοιο με τη Συναλλαγή στο Ethereum αλλά στην απλούστερη της μορφή, αφού τα Μηνύματα υφίστανται μόνο στο περιβάλλον εκτέλεσης και δεν αποθηκεύονται ποτέ. Περιέχει μόνο τα πεδία Αποστολέας, Παραλήπτης, ποσότητα Wei που αποστέλλεται, μήνυμα προς λογαριασμό, μέγιστος αριθμός καυσίμου και προαιρετικό πεδίο δεδομένων. Το **Μήνυμα** αποστέλλεται από ένα λογαριασμού συμβολαίου προ ένα άλλο, ενώ η **Συναλλαγή** αποστέλλεται από ένα λογαριασμού εξωτερική ιδιοκτησίας (Bashir, 2018).

4.3.2 Δομή Συναλλαγής Ethereum

Μια Συναλλαγής Ethereum αποτελείται από τα μέρη που υποδεικνύονται στον **Πίνακα 4.2.** και στη συνέχεια αυτή υπογράφεται ψηφιακά με το ιδιωτικό κλειδί του αποστολέα και η ψηφιακή υπογραφή συμπεριλαμβάνεται στη συναλλαγή μαζί με τα υπόλοιπα μέρη ως απόδειξη της εγκυρότητας της συναλλαγής. Όπως και για πολλές άλλες καταστάσεις στο Ethereum, χρησιμοποιείται ένα τροποποιημένο Δένδρο Merkle-Patricia για την αποθήκευση όλων των συναλλαγών της Συστοιχίας. Στη συνέχεια, η τιμή κατακερματισμού Keccak-256 του ριζικού κόμβου του Δένδρου συμπεριλαμβάνεται στην επικεφαλίδα της Συστοιχίας, ενώ οι Συναλλαγές συμπεριλαμβάνονται στο κυρίως σώμα της Συστοιχίας (Βλέπε Εικόνα 4.5).

Μέρος	Συναλλαγή Μηνύματος Κλήσης	Συναλλαγή Δημιουργίας Συμβολαίου	Περιγραφή
Αριθμολέξημα (nonce)	✓	✓	Ένας αριθμός ο οποίος αυξάνεται κάθε φορά που πραγματοποιείται μια συναλλαγή από τον αποστολέα, δηλαδή αντιπροσωπεύει τον αριθμό τον συναλλαγών που αποστάληκαν από τον συγκεκριμένο λογαριασμό και είναι μοναδικός και ξεχωριστός για κάθε συναλλαγή.
Παραλήπτης	✓	✓	Η διεύθυνση του λοαρασμού του παραλήπτη, μήκους 20 byte/160 bits.
Ποσότητα Wei	✓	✓	Η ποσότητα Wei που αποστέλλεται με την συναλλαγή.
Ψηφιακή Υπογραφή	✓	✓	Για επιβεβαίωση ότι ο ιδιοκτήτης του ψηφιακού χρήματος είναι αυτός που το αποστέλλει, το υπογράφει ψηφιακά με το ιδιωτικό του κλειδί και η υπογραφή αυτή συμπεριλαμβάνεται στα δεδομένα της συναλλαγής.
Τιμή καυσίμου	✓	✓	Ο αποστολέας καθορίζει η ποσότητα Wei που θα χρεώνεται για κάθε μονάδα καυσίμου, μέχρι την ολοκλήρωση της συναλλαγής. Αυτή η τιμή, αντιπροσωπεύει δηλαδή την ποσότητα Wei που είναι διαθέσιμος να ξοδεύσει ως μέρος του τέλους συναλλαγής, προκειμένου να πραγματοποιηθεί η συναλλαγή.
Όριο καυσίμου	✓	✓	Για κάθε συναλλαγή, καθορίζεται ένας μέγιστος αριθμός μονάδων καυσίμου για την ολοκλήρωσή της. Μια μονάδα καυσίμου μπορεί να ερμηνευτεί και σαν ένα από τα υπολογιστικά βήματα που πρέπει να ακολουθήσει μια συναλλαγή για να φτάσει στον προορισμό της και να ολοκληρωθεί.
Δεδομένα	✓	×	Το πεδίο αυτό χρησιμοποιείται μόνο στις **Συναλλαγές Μηνύματος Κλήσης** και περιέχει το περιεχόμενο του μηνύματος.
Πεδίο εκκίνησης	×	✓	Περιέχεται μόνο στις **Συναλλαγές Δημιουργίας Συμβολαίου** και περιέχει ένα απεριόριστο πίνακα που καθορίζει τον κώδικα για το λογαριασμό που θα δημιουργηθεί.

Πίνακας 4.2. *Ενδεικτική Δομή Συναλλαγής στο Ethereum, συμπεριλαμβανομένων των πεδίων που είναι μοναδικά στη Συναλλαγή Μηνύματος Κλήσης και στη Συναλλαγή Δημιουργίας Συμβολαίου (Bashir, 2018).*



Εικόνα 4.5. *Απεικονίζεται η διάταξη του **Δένδρου Merkle-Patricia** των Συναλλαγών μιας Συστοιχίας και πως η τιμή κατακερματισμού του ριζικού του κόμβου περιλαμβάνεται στην επικεφαλίδα της Συστοιχίας (Bashir, 2018).*

4.3.3 Διενέργεια Συναλλαγής Ethereum

Κάθε Συναλλαγή Ethereum περιέχει ένα **Αριθμολέξημα**, το οποίο προκειμένου η συναλλαγή να είναι έγκυρη, πρέπει να αντιστοιχεί με το τρέχον Αριθμολέξημα του αποστολέα. Αν αυτό δεν ισχύει, τότε η συναλλαγή δεν είναι έγκυρη και έτσι δεν θα αποσταλεί. Με αυτό τον τρόπο εξασφαλίζεται το σύστημα από τη διπλή δαπάνη του ίδιου κρυπτονομίσματος **(Fekkes, 2018)**. Μετά την πραγματοποίηση μιας έγκυρης συναλλαγής, ο χρόνος αποδοχής της κυμαίνεται μεταξύ 15 δευτερόλεπτα και 5 λεπτά **(How long does an Ethereum transaction really take?, 2019)**.

Για να αποφευχθεί κατάχρηση του δικτύου, όλοι οι υπολογισμοί στο Ethereum υπόκεινται σε χρεώσεις, γνωστές και ως **Τέλη**. Έτσι, κάθε ενέργεια των κόμβων που χρειάζεται προγραμματιστικούς υπολογισμούς, συμπεριλαμβανομένων συναλλαγών, δημιουργία λογαριασμών, μηνύματα, πρόσβαση αποθήκευσης λογαριασμού και χρήση της εικονικής μηχανής, περιλαμβάνει ένα καθολικά συμφωνημένο κόστος, ανάλογο με το **καύσιμο** που επιλέγεται. Το **Καύσιμο** αποτελεί τη βασική μονάδα χρέωσης του δικτύου, πληρώνεται αποκλειστικά με ether (ουσιαστικά Wei) και μπορεί να μετατραπεί ελεύθερα σε καύσιμο και πίσω σε κρυπτονόμισμα. Ο όρος του καυσίμου υφίσταται μόνο για την πραγματοποίηση του υπολογισμού και δεν έχει σταθερή τιμή αλλά καθορίζεται από τον αποστολέα της κάθε συναλλαγής **(Wood, 2017)**.

Κάθε συναλλαγή έχει μια μέγιστη τιμή καυσίμου για την πραγματοποίησή της, το **Όριο Καυσίμου**. Ερμηνεύεται ως ο μέγιστος αριθμός υπολογιστικών βημάτων που είναι διαθέσιμος ο αποστολέας να πληρώσει. Ο αποστολέας αγοράζει το **καύσιμο** για όλα τα υπολογιστικά βήματα πριν την πραγματοποίηση της συναλλαγής, αν και μπορεί να μην καταναλωθεί ολόκληρο το καύσιμο μέχρι το πέρας της συναλλαγής. Αντίθετα, υπάρχει περίπτωση να μην είναι αρκετό για την ολοκλήρωση της συναλλαγής και ως αποτέλεσμα η συναλλαγή να μην είναι έγκυρη. Η τιμή με την οποία αγοράζεται το καύσιμο καθορίζεται επίσης από τον αποστολέα με σκοπό να προσελκύσει του miners για να συμπεριλάβουν τη συναλλαγή του στη Συστοιχία που δημιουργούν. Η τιμή αυτή ονομάζεται **Τιμή Καυσίμου** και είναι το κόστος σε Wei για κάθε μονάδα καυσίμου που αγοράζει ο αποστολέας.

Σε μια επιτυχημένη συναλλαγή, το **καύσιμο** που αγοράστηκε από τον αποστολέα καταναλώνεται για τους υπολογισμούς που είναι αναγκαίοι για την πραγματοποίηση της συναλλαγής. Αν για παράδειγμα καταναλώθηκε η μισή ποσότητα καυσίμου για την ολοκλήρωσή της, η ποσότητα που δεν χρησιμοποιήθηκε μετατρέπεται σε ether και

επιστρέφεται στο λογαριασμό του αποστολέα. Στη συνέχεια, αν η συναλλαγή γίνει αποδεκτή από κάποιο miner, η ποσότητα καυσίμου που καταναλώθηκε πηγαίνει στο λογαριασμό του miner ως ανταμοιβή. Όπως κάθε αποστολέας επιλέγει ελεύθερα την Τιμή Καυσίμου με την οποία θα αγοράσει καύσιμο, κάθε miner επιλέγει ελεύθερα ποιες συναλλαγές θα συμπεριλάβει στη Συστοιχία του. Γενικά οι miners θα επιλέξουν συναλλαγές που τους επιφέρουν το μέγιστο κέρδος. Έτσι ο αποστολέας πρέπει να επιλέξει κατάλληλα την Τιμή καυσίμου για να προσελκύσει τους miners στο να συμπεριλάβουν τη συναλλαγή του στη Συστοιχία και έτσι να είναι έγκυρη. Σε μια αποτυχημένη συναλλαγή, το **καύσιμο** που αγοράστηκε δεν είναι αρκετό για την πραγματοποίηση όλων των υπολογιστικών βημάτων και έτσι την ολοκλήρωση της συναλλαγής. Σε αυτήν την περίπτωση, ολόκληρο το καύσιμο καταναλώνεται και η ποσότητα Wei που αντιστοιχεί σε αυτό δεν επιστρέφεται αλλά μεταφέρεται όλη στο miner **(Wood, 2017)**.

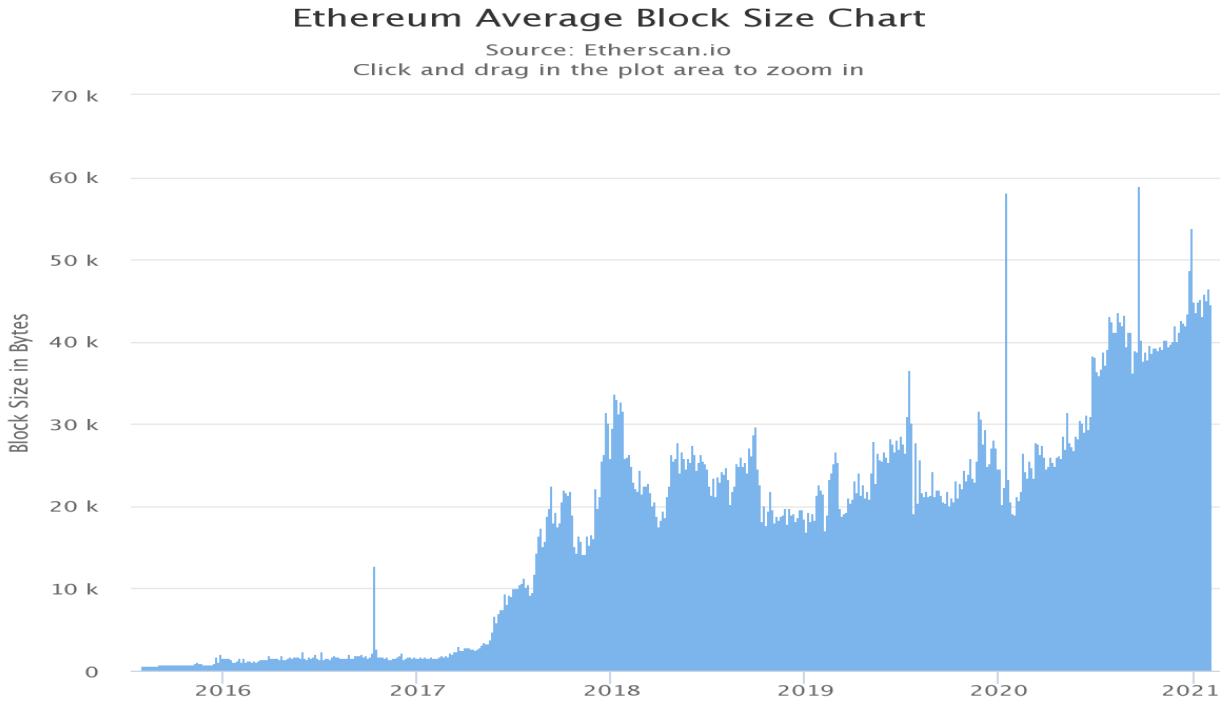
4.3.4 Τέλη Συναλλαγής Ethereum

Σε μια συναλλαγή στο Ethereum, πέραν από την ποσότητα κρυπτονομίσματος που θα αποστείλει (ποσότητα Wei), ο κάθε κόμβος χρεώνεται επίσης το **Τέλος Συναλλαγής** το οποίο προκύπτει από το **Όριο Καυσίμου** και **Τιμή Καυσίμου** που αυτός καθόρισε για τη συναλλαγή του. Ο κύριο σκοπός του Τέλους Συναλλαγής, είναι να δώσει κίνητρο στους miners με την ανταμοιβή που λαμβάνουν, για να συνεχίσουν την εξόρυξη νέων μπλοκ. Επιπρόσθετα, δευτερεύον σκοπός είναι η αποτροπή πιθανών επιθέσεων διότι ο επιτιθέμενος θα πληρώσει για κάθε του κίνηση στο δίκτυο, καθιστώντας έτσι μια επίθεση μη επικερδή. Το Τέλος Συναλλαγής υπολογίζεται ως εξής. Πολλαπλασιάζοντας το Όριο Καυσίμου με την Τιμή Καυσίμου που επιλέχθηκαν, υπολογίζεται η ποσότητα ether που αποκόπτεται αρχικά από το λογαριασμό του αποστολέα.

Έτσι, υφίσταται μια αρχική ποσότητα καυσίμου για την πραγματοποίηση της συναλλαγής. Από την ποσότητα αυτή αποκόπτονται 5 μονάδες καυσίμου για κάθε byte των δεδομένων της συναλλαγής και 1 μονάδα καυσίμου για κάθε υπολογιστικό βήμα μέχρι την ολοκλήρωσή της. Αν το καύσιμο επαρκεί για όλους τους υπολογισμούς και ταυτόχρονα ο αποστολέας έχει στην κατοχή του την ποσότητα κρυπτονομίσματος που θα αποσταλεί στον παραλήπτη, τότε η συναλλαγή θεωρείται έγκυρη και η ποσότητα αυτή μεταφέρεται στο λογαριασμό του παραλήπτη. Συνολικά οι μονάδες καυσίμου που καταναλώθηκαν στο πέρας της συναλλαγής, αποτελούν το **Τέλος της Συναλλαγής** και το καύσιμο που απομένει επιστρέφεται στο λογαριασμό του αποστολέα **(Fekkes, 2018)**.

4.4 Συστοιχία στο Ethereum

Οι Συστοιχίες στο Ethereum έχουν παρόμοια λειτουργία με αυτές στο Bitcoin αλλά δημιουργούνται πολύ πιο γρήγορα κυρίως λόγος του μικρού τους μεγέθους. Συγκεκριμένα, στις αρχές του 2021 το μέγεθος μιας Συστοιχίας Ethereum είναι 16,5 kilobyte σε μέσο όρο και μπορεί να περιέχει 70 συναλλαγές περίπου, ανάλογα με το μέγεθος αυτών (Lewis, 2020).



Εικόνα 4.6. *Το μέγεθος μιας συστοιχίας Ethereum από το 2015 μέχρι το 2021 (Ethereum Charts & Statistics, 2021).*

4.4.1 Δομή της Συστοιχίας Ethereum

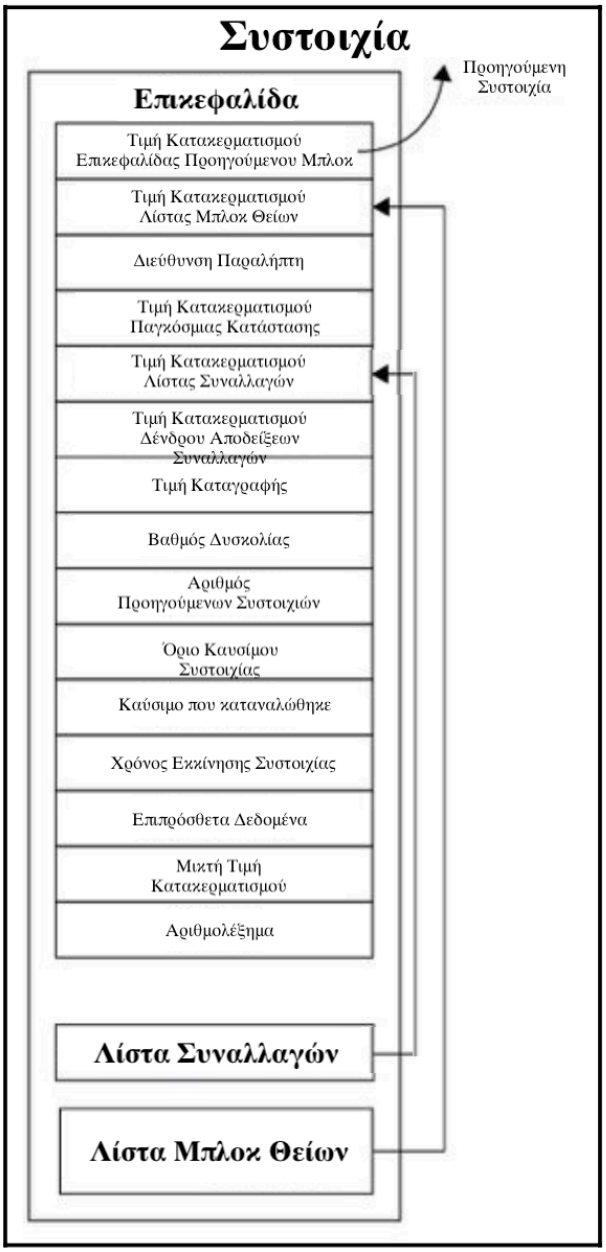
Μια Συστοιχία στο Ethereum αποτελείται γενικά από 3 πεδία, την επικεφαλίδα, τη Λίστα Συναλλαγών και τη Λίστα Επικεφαλίδων Μπλοκ Θείων, τα οποία είναι Μπλοκ που εξορύχθηκαν παράλληλα με το τρέχον μπλοκ της αλυσίδας. Το πιο σύνθετο πεδίο που περιέχει τις πιο σημαντικές πληροφορίες της Συστοιχίας είναι η Επικεφαλίδα. Αυτή αποτελείται από αρκετά πεδία τα οποία αναγράφονται και περιγράφονται στον **Πίνακα 4.4.**

Μέρος	Περιγραφή
Επικεφαλίδα Συστοιχίας	Συμπεριλαμβάνει την Τιμή Κατακερματισμού της Επικεφαλίδας του Προηγούμενου Μπλοκ, την Τιμή Κατακερματισμού της Λίστας Επικεφαλίδων Μπλοκ Θείων, τη Διεύθυνση του παραλήπτη, την Τιμή Κακατερματισμού του Ριζικού Κόμβου της Παγκόσμιας Κατάστασης, την Τιμή Κατακερμαστιμού του Ριζικού Κόμβου του Δέδνρου Συναλλαγών, την Τιμή Κατακερματισμού του Ριζικού Κόμβου του Δέδνρου Αποδείξεων Συναλλαγών, την Τιμή Καταγραφής, το Βαθμό Δυσκολίας, τον Αριθμό Προγούμενων Συστοιχιών, το Όριο Καυσίμου της Συστοιχίας, το Καύσιμο που καταναλώθηκε στη Συστοιχία, το Χρόνο Εκκίνησης της Συστοιχίας, τα Επιπρόσθετα Δεδομένα, τη Μικτή Τιμή Κατακερματισμού και το Αριθμολέξημα.
Λίστα Συναλλαγών	Συμπεριλαμβάνει όλες τις Συναλλαγές που πραγματοποιήθηκαν στη Συστοιχία, σε ένα Δένδρο Merkle. Η τιμή κατακερματισμού του ριζικού κόμβου του Δένδρου συμπεριλαμβάνεται στην Επικεφαλίδα της Συστοιχιάς.
Λίστα Επικεφαλίδων Μπλοκ Θείων	Συμεριλαμβάνετι όλες τις Επικεφαλίδες των Μπλοκ Θείων, δηλαδή των Μπλοκ που Εξορύχθηκαν την ίδια χρονική στιγμή με το Μπλοκ που συμπεριλήφθηκε στην Αλυσίδα Συστοιχιών.

Πίνακας 4.3. *Ενδεικτική δομή Συστοιχίας Ethereum* (Bashir, 2018).

Μέρος	Περιγραφή
Τιμή Κατακερματισμού Επικεφαλίδας της Προηγούμενης Συστοιχίας	Η τιμή κατακερματισμού Keccak-256 της Επικεφαλίδας της Προηγούμενης Συστοιχίας.
Τιμή Κατακερματισμού Λίστας Επικεφαλίδων Μπλοκ Θείων	Η τιμή κατακερματισμού Keccak-256 της Λίστας των Επικεφαλίδων των Μπλοκ Θείων η οποία περιλαμβάνεται στη Συστοιχία.
Διεύθυνση Παραλήπτη Ανταμοιβής	Η διεύθυνση Ethereum μήκους 160 bits του miner που θα λάβει την ανταμοιβή από τα Τέλη Συναλλαγής.
Τιμή Κατακερματισμού Ριζικού Κόμβου της Παγκόσμιας Κατάστασης	Η τιμή κατακερματισμού Keccak-256 του Ριζικού Κόμβου του Δένδρου Παγκόσμιας Κατάστασης.
Τιμή Κατακερματισμού Ριζικού Κόμβου του Δένδρου Συναλλαγών	Η τιμή κατακερματισμού Keccak-256 του Ριζικού Κόμβου του Δένδρου Συναλλαγών.
Τιμή Κατακερματισμού Ριζικού Κόμβου του Δένδρου Αποδείξεων Συναλλαγών	Η τιμή κατακερματισμού Keccak-256 του Ριζικού Κόμβου του Δένδρου Απόδειξης Συναλλαγών.
Τιμή Καταγραφής	Προέρχεται από τις Αποδείξεις Συναλλαγών που πραγματοποιήθηκαν εντός της Συστοιχίας.
Βαθμός Δυσκολίας	Ο τρέχον βαθμός δυσκολίας του Αλγόριμου Εξόρυξης.
Αριθμός Προηγούμενων Συστοιχιών	Ο συνολικός αριθμός προηγούμενων συναλλαγών, με εκκίνησης το μπλοκ γένεσης με αριθμό 0.
Όριο Καυσίμου Συστοιχίας	Ο μέγιστος αριθμός μονάδων καυσίμου που μπορούν να καταναλωθούν στο Μπλοκ.
Καύσιμο που καταναλώθηκε	Η ποσότητα καυσίμου που καταναλώθηκε για όλες τις συναλλαγές της Συστοιχίας.
Χρόνος Εκκίνησης Συστοιχίας	Ο Χρόνος που ο miner ξεκίνησε την εξόρυξη του μπλοκ.
Επιπρόσθετα Δεδομένα	Πεδίο στο οποίο περιέχονται επιπρόσθετα δεδομένα μέγιστου μεγέθους 32 bytes.
Μικτή Τιμή Κατακερματισμού	Μια τιμή κατακερματισμού μήκους 256 bits, η οποία σε συνδιασμό με το Αριθμολέξημα χρησιμοποιείται για την Απόδειξη Εργασίας με τον Αλγόριθμο Εξόρυξης.
Αριθμολέξημα	Ένας αυθαίρετος αριθμός μεγέθους 64 bits, που όταν συνδιαστεί με τη Μικτή Τιμή Κατακερματισμού μπορεί να αποδείξει ότι καταβλήθηκε επαρκής υπολογιστική προσπάθεια για τη δημιουργία της Συστοιχίας.

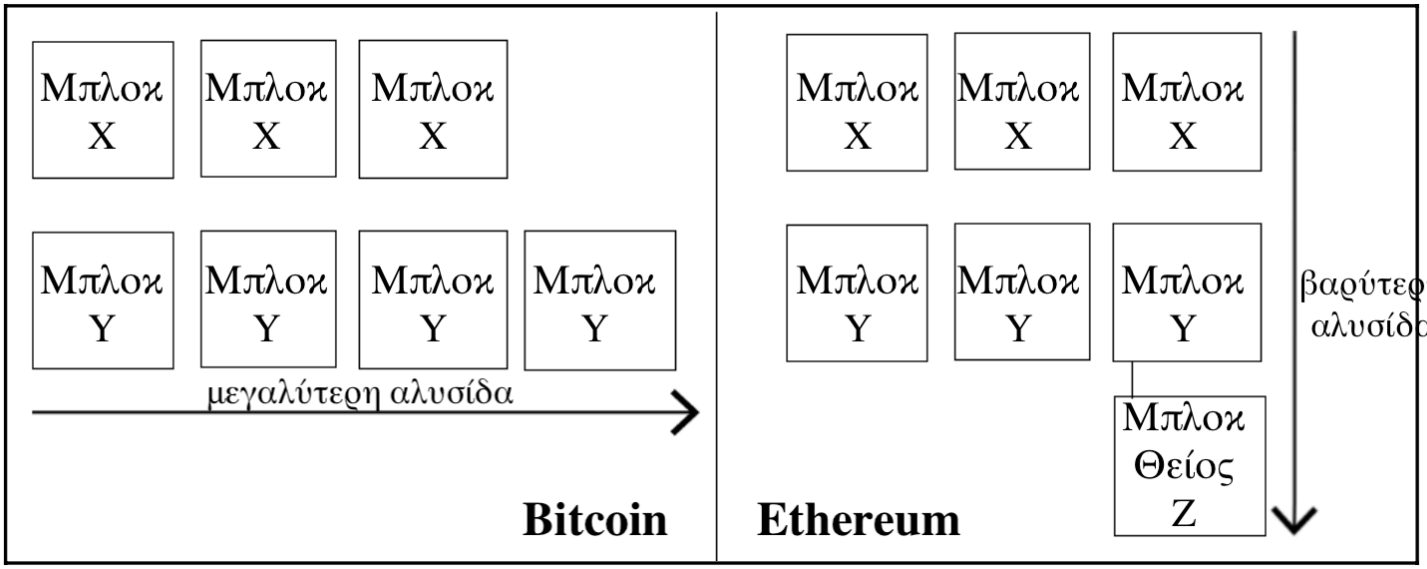
Πίνακας 4.4. *Ενδεικτική δομή Επικεφαλίδας της Συστοιχίας Ethereum* (Bashir, 2018).



Εικόνα 4.7. *Γραφική απεικονιση μιας Συστοιχιας Ethereum (Bashir, 2018).*

4.4.2 Διακλάδωση στην Αλυσίδα Συστοιχιών

Μια **Διακλάδωση** είναι ο διαχωρισμός της Αλυσίδας Συστοιχιών του Ethereum στα δύο. Ο διαχωρισμός αυτός μπορεί να είναι εσκεμμένος στην περίπτωση μιας μεγάλης αναβάθμισης, ή χωρίς πρόθεση λόγω σφαλμάτων στο λογισμικό **(Bashir, 2018)**. Όταν συμβεί αυτό, πρέπει να υπάρχουν κανόνες για το ποια θα είναι η κύρια Αλυσίδα Συστοιχιών. Τότε αυτή θα ονομαστεί **Σκληρή Διακλάδωση** και θα εγκαταλειφθεί από τους κόμβους. Υπάρχουν δύο διαφορετικοί κανόνες, ο κανόνας της **μεγαλύτερης αλυσίδας** και αυτός της **βαρύτερης αλυσίδας**. Στο **Bitcoin** επιλέγεται η μεγαλύτερη αλυσίδα ως η τρέχουσα αλυσίδα, η οποία περιέχει τις περισσότερες Συστοιχίες και έτσι την περισσότερη ποσότητα Απόδειξης Εργασίας. Στο **Ethereum** επιλέγεται η βαρύτερη αλυσίδα ως η κύρια, στην οποία δαπανήθηκε η περισσότερη υπολογιστική ενέργεια. Η κύρια διαφορά με τον κανόνα της μεγαλύτερης αλυσίδας, είναι ότι στον τον υπολογισμό της υπολογιστικής ενέργειας περιλαμβάνονται και Μπλοκ Θείοι. Τα **Μπλοκ Θείοι** είναι ανενεργά μπλοκ με κοινό γονικό κόμβο με το τρέχον μπλοκ της αλυσίδας, ή κοινούς προγόνους μέχρι 6 μπλοκ πίσω. Τα μπλοκ αυτά εξορύχθηκαν την ίδια ακριβώς στιγμή με το καινούργιο μπλοκ, ή δαπάνησε σημαντική υπολογιστική ισχύ κατά την εξόρυξή τους, αλλά δεν συμπεριλήφθηκε στην κύρια Αλυσίδα Συστοιχιών.



Εικόνα 4.8. *Σύγκριση μεγαλύτερης αλυσίδας στο Bitcoin (αριστερά) και βαρύτερης αλυσίδας στο Ethereum (δεξιά). Στην πρώτη περίπτωση, η κύρια αλυσίδα είναι η Y αφού περιλαμβάνει τις περισσότερες Συστοιχίες και έτσι την περισσότερη ποσότητα Απόδειξης Εργασίας. Στη δεύτερη περίπτωση, η κύρια αλυσίδα είναι η Y αν και έχει το ίδιο μήκος με την X, διότι η αλυσίδα Y περιλαμβάνει και το Μπλοκ Θείο Z και έτσι την περισσότερη υπολογιστικής ενέργειας (Bashir, 2018).*

4.5 Εξόρυξη Ethereum

Η Εξόρυξη είναι μια διαδικασία που εκτελείται από τους miners, με την οποία προτείνουν μια καινούργια Συστοιχία και προσπαθούν να την προσθέσουν στην τρέχουσα αλυσίδα του Ethereum. Κατά μέσο όρο η εξόρυξη μιας Συστοιχίας διαρκεί 14,85 δευτερόλεπτα και με αυτό δεδομένο, περίπου 5818 Συστοιχίες προσθέτονται στην αλυσίδα σε μια μέρα λειτουργίας του Ethereum. Στο σύνολο η Αλυσίδα Συστοιχιών του Ethereum περιλαμβάνει 1 800 000 Συστοιχίες τις αρχές του 2021 (Lewis, 2020).

4.5.1 Απόδειξη Εργασίας στο Ethereum

Η εξόρυξη στο Ethereum γίνεται με την επίλυση του Αλγόριθμου Εργασίας **Ethash** (Fekkes, 2018). Ομοίως με το Bitcoin, ο miner προσπαθεί να βρει ένα **Αριθμολέξημα**, το οποίο μετά από κάποιους υπολογισμούς επιστρέφει μια τιμή κάτω από τον επιθυμητό βαθμό δυσκολίας. Πριν τον τελικό υπολογισμό της τιμής αυτής, προηγούνται κάποια υπολογιστικά βήματα που οφείλει να κάνει ο miner και είναι τα εξής:

- **Υπολογισμός Σπόρου:** Ο Σπόρος υπολογίζεται για κάθε συστοιχία με τη σάρωση όλων των επικεφαλίδων των μπλοκ που προηγούνται του καινούργιου. Ο υπολογισμός των τιμών κατακερματισμού του Σπόρου μπορεί να γίνει εκ των προτέρων για πιο γρήγορη εξόρυξη.

- **Υπολογισμός 16 mb προσωρινής μνήμης (cache):** Χρησιμοποιώντας το Σπόρο που υπολογίστηκε προηγουμένως, υπολογίζεται μια ψευδό τυχαία προσωρινή μνήμη με μέγεθος 16 megabytes.

- **Υπολογισμός 1 gb δεδομένων:** Χρησιμοποιώντας την προσωρινή μνήμη που υπολογίστηκε προηγουμένως, δημιουργείται ένα σύνολο δεδομένων μεγέθους 1 gigabyte. Το γεγονός ότι τα δεδομένα εξαρτώνται σε τμήματα της προσωρινής μνήμης, καθιστά την επαλήθευση της Απόδειξης Εργασίας εύκολη και γρήγορη.

- **Εξόρυξη:** Στο τελευταίο βήμα, επιλέγεται ένα **Αριθμολέξημα**, το οποίο συνδυάζεται με τμήματα των δεδομένων, εφαρμόζεται συνάρτηση κατακερματισμού στο συνδυασμό και στο τέλος συμπιέζονται. Η τελική τιμή συγκρίνεται με την επιθυμητή του βαθμού δυσκολίας και αν είναι χαμηλότερη τότε το Αριθμολέξημα είναι έγκυρο.

Όταν βρεθεί ένα έγκυρο Αριθμολέξημα από κάποιο κόμβο, τότε αυτός αναμεταδίδει τη Συστοιχία που δημιούργησε σε ολόκληρο το δίκτυο του Ethereum, η οποία λαμβάνεται από όλους τους κόμβους. Ακολουθεί η επαλήθευση της λύσης, που δεν είναι παρά μόνο η εφαρμογή μιας συνάρτησης κατακερματισμού για να βεβαιωθούν ότι το Αριθμολέξημα παράγει τιμή μικρότερη από την επιθυμητή. Ο αλγόριθμος **Ethash** απαιτεί μεγάλη ποσότητα μνήμης για να επιλυθεί αποτελεσματικά, αλλά ελάχιστη για την επαλήθευση, κάτι που του δίνει **Αντίσταση κατά ASIC** (Υποτμήμα 3.5.3). Επίσης ο αλγόριθμος λειτουργεί με τέτοιο τρόπο ώστε να μπορεί να υπολογιστεί μόνο ένα Αριθμολέξημα την κάθε δεδομένη στιγμή (Fekkes, 2018).

Ο νικητής του αλγόριθμου Απόδειξη Εργασίας Ethash, πιστώνεται στο λογαριασμό του την **Ανταμοιβή Εξόρυξης**, η οποία προέρχεται από πολλαπλούς χώρους:

- Στατική Ανταμοιβή **3.0 ether**, η οποία ποσότητα και προστίθενται στο σύνολο των ether που υπάρχουν συνολικά.

- Όλο το καύσιμο που καταναλώθηκε στις συναλλαγές της Συστοιχίας, το οποίο προέρχεται από τους κόμβους που πραγματοποίησαν οποιοδήποτε είδος συναλλαγής.

- Ανταμοιβή για τα Μπλοκ Θείους που συμπεριλαμβάνονται στη Συστοιχία, η οποία αντιστοιχεί σε 1/32 της ανταμοιβής ανά Μπλοκ με μέγιστο τα 2 Μπλοκ.

4.5.2 Απόδειξη Μεριδίου στο Ethereum

Στον καινούργιο αλγόριθμο εξόρυξης του Ethereum, η δημιουργία της νέας Συστοιχίας βασίζεται στην αρχή του Μεριδίου και κατοχής ποσότητας ether, αντί στην Εργασία. Το βασικό πλεονεκτήματα είναι ότι τόσο οι υπολογισμοί όσο και η επαλήθευση θα πραγματοποιούνται πολύ πιο γρήγορα. Επίσης, δεν θα σπαταλιέται άσκοπα υπολογιστική ισχύς όπως στην Απόδειξη Εργασίας, όπου ο υπολογισμός του Αριθμολεξίματος δεν αποτελούσε Απόδειξη Χρήσιμης Εργασίας και δεν αποσκοπούσε σε κάτι πέραν από την επίλυση του προβλήματος. Ένας κόμβος μπορεί να συμμετέχει στη διαδικασία της **Εξόρυξης με Απόδειξη Μεριδίου** θέτοντας μια ποσότητα ether σαν ποντάρισμα, το οποίο αποτελεί το **Μερίδιό** του μέχρι να αποσυρθεί. Για την ποσότητα αυτή ορίζεται το ελάχιστο των 32 ether και το μέγιστο των 131 072 ether. Η κατάθεση της ποσότητας αυτής ονομάζεται εγγύηση και μετά από αυτή ο κόμβος καθίσταται **εγγυημένος επικυρωτής**.

Για κάθε καινούργια Συστοιχία, δημιουργείται μια λίστα από το σύνολο των εγγυημένων επικυρωτών. Η δημιουργία της λίστας αυτής γίνεται ψευδό τυχαία, κάτι το οποίο εξαρτάται από το ποσό του Μεριδίου που ο κάθε κόμβος κατάθεσε αρχικά. Για παράδειγμα αν ένας κόμβος έχει καταθέσει 10% των συνολικών καταθέσεων τη δεδομένη στιγμή, τότε έχει 10% πιθανότητες να επιλεγεί για να προτείνει την επόμενη Συστοιχία. Ο κόμβος που επιλέγεται για να δημιουργήσει το επόμενο Μπλοκ είναι ο πρώτος της λίστας που δημιουργήθηκε ψευδό τυχαία και αν αυτός δεν ανταποκρίνεται ή δεν απαντήσει σε κάποιο χρονικό διάστημα, τότε επιλέγεται ο επόμενος στη λίστα για να προτείνει την επόμενη Συστοιχία. Για να αποσυρθεί κάποιος εγγυημένος επικυρωτής, οφείλει να περιμένει 10 800 νέες Συστοιχίες για το επόμενο epoch χρόνο, που αντιστοιχεί σε 12 ώρες περίπου. Όταν αποσυρθούν θα πάρουν πίσω την κατάθεσή τους πλην τις ποινές και συν τις ανταμοιβές, δεδομένου ότι οι πράξεις τους ακολουθούσαν όλες τους κανονισμούς.

Ο κόμβος που επιλέγεται από την **Απόδειξη Μεριδίου** του Ethereum για τη δημιουργία της νέας Συστοιχίας, πιστώνεται τις εξής ανταμοιβές:

- **Αρχική Ανταμοιβή** = Συνολική ποσότητα ether πονταρίσματος **x** Συντελεστής Ανταμοιβής **x** Καθορισμένο Χρόνο Συστοιχίας.

- **Τέλη Συναλλαγών:** Όλο το καύσιμο που καταναλώθηκε για την πραγματοποίηση των Συναλλαγών και άλλων υπολογισμών εντός της Συστοιχίας, μετατρέπεται σε ether και πιστώνεται στο λογαριασμό του νικητή της Απόδειξης Μεριδίου.

Κεφάλαιο 5
Πολλαπλοί Τρόποι Λειτουργίας

Στα προηγούμενα κεφάλαια αναλύθηκε ο τρόπος λειτουργίας διαφόρων συστημάτων κρυπτονομίσματος στο σύνολό τους και συγκεκριμένα το Bitcoin και το Ethereum. Όταν το πρωτόκολλο του συστήματος κρυπτονομίσματος έχει ένα μόνο τρόπο λειτουργίας, όλοι οι κόμβοι που συμμετέχουν σε αυτό λειτουργούν με τον ίδιο τρόπο, δηλαδή επικυρώνουν τις συναλλαγές με την ίδια μέθοδο και κατεβάζουν ένα κοινό αντίγραφο της Αλυσίδας Συστοιχιών. Το κεφάλαιο αυτό εισαγάγει την έννοια του **Πολλαπλού Τρόπου Λειτουργίας**, κατά την οποία το πρωτόκολλο του συστήματος κρυπτονομίσματος επιτρέπει στους συμμετέχοντες κόμβους να λειτουργούν με διαφορετικούς τρόπους και ταυτόχρονα να παραμένουν όλοι μέρος του ίδιου συστήματος. Είναι σημαντικό να σημειωθεί ότι τα περισσότερα κύρια κρυπτονομίσματα υποστηρίζουν Πολλαπλούς Τρόπους Λειτουργίας για τους κόμβους που συμμετέχουν σε αυτά.

5.1 Εισαγωγή

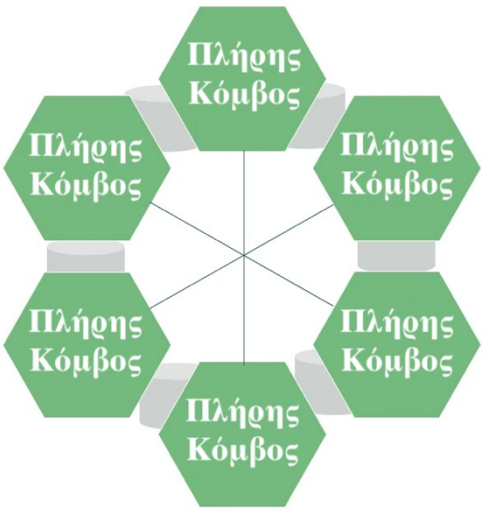
Σε ένα σύστημα κρυπτονομίσματος το οποίο υποστηρίζει Πολλαπλούς Τρόπους Λειτουργίας, οι κόμβοι μπορούν να τρέχουν είτε σε **Πλήρη Λειτουργία**, είτε σε κάποιας μορφής **Ελαφριάς Λειτουργίας**. Αφ' ενός, οι κόμβοι σε Πλήρη Λειτουργία διαχειρίζονται και καταγράφουν ολόκληρο το ιστορικό των συναλλαγών, και είναι επίσης ικανοί να επαληθεύσουν την ακεραιότητα του ιστορικού και την εγκυρότητα των νέων συναλλαγών μόνοι τους, χωρίς να έχουν ανάγκη κάποιον άλλο κόμβο. Οι Κόμβοι σε Ελαφριά Λειτουργία αφ' ετέρου, μπορούν να αποθηκεύουν μόνο ένα μέρος του ιστορικού των συναλλαγών και συνήθως εξαρτώνται από του πλήρης κόμβους για να είναι ενεργά μέλη του συστήματος. Μερικά είδη Ελαφριάς Λειτουργία θεωρούνται η λειτουργία «SPV» και λειτουργία «pruning» του Bitcoin, καθώς και η λειτουργία «WarpSync» του Ethereum (Duong, Chepurnoy, & Zhou, 2018).

Ο κυριότερος σκοπός των Πολλαπλών Τρόπων Λειτουργίας είναι για να αντιμετωπίσει το φλέγον ζήτημα του **Φουσκώματος της Αλυσίδας Συστοιχιών**, στο οποίο τα δεδομένα της Αλυσίδας Συστοιχιών πληθαίνουν υπερβολικά λόγω των νέων συναλλαγών που προστίθενται

συνεχώς σε αυτή. Ως εκ τούτου, γίνεται όλο και δυσκολότερο να αποθηκευτεί ολόκληρη η Αλυσίδα Συστοιχιών σε ένα υπολογιστή, περιορίζοντας έτσι το πεδίο εφαρμογής του συστήματος. Με άλλα λόγια, όλο και λιγότεροι κόμβοι θα έχουν την απαραίτητη κενή μνήμη για να ακολουθήσουν τις εξελίξεις στο σύστημα κρυπτονομίσματος και να αποθηκεύσουν όλα τα δεδομένα. Η ύπαρξη της Ελαφριάς Λειτουργίας επιτρέπει τη σύμπτυξη των δεδομένων του συστήματος, με αποτέλεσμα να απαιτείται λιγότερος αποθηκευτικός χώρος για να είναι ένας κόμβος μέρος αυτού. Ένα επιτυχημένο κρυπτονόμισμα σαν το Bitcoin και το Ethereum, τα οποία υποστηρίζουν Πολλαπλούς Τρόπους Λειτουργίας, επιτρέπουν στους κόμβους να λειτουργούν με διαφορετικό τρόπο ανάλογα με τον αποθηκευτικό χώρο που έχουν και θα έχουν διαθέσιμο. Έτσι, αυξάνεται το πλήθος των χρηστών που μπορούν να συμμετέχουν στο σύστημα, κατακτώντας το αυτόματα πιο δημοφιλές (Duong, Chepurnoy, & Zhou, 2018).

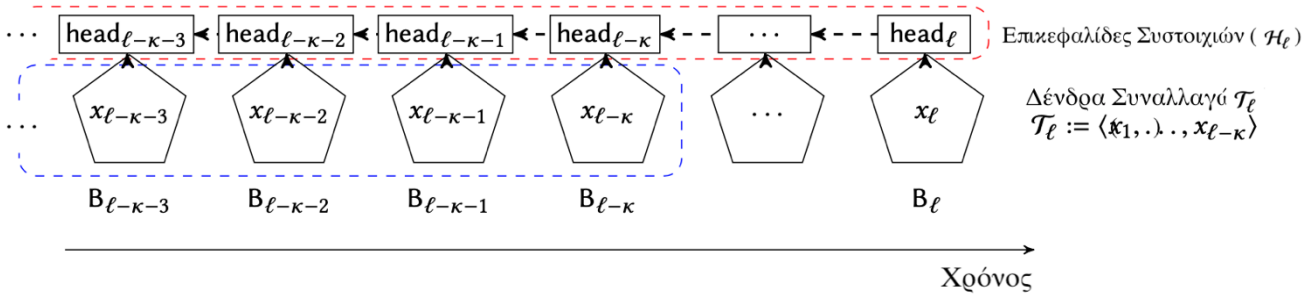
5.2 Πλήρης Λειτουργία

Το πλήθος των δεδομένων ενός συστήματος κρυπτονομίσματος δεν είναι αποθηκευμένα σε ένα κεντρικό υπολογιστή, αλλά σε όλους τους κόμβους που το απαρτίζουν. Το γεγονός αυτό το καταστεί ένα απολύτως αποκεντρωτικό σύστημα, διότι η εγκυρότητα και η ακεραιότητά των δεδομένων του εξασφαλίζεται από τους κύριους κόμβους του συστήματος, οι οποίοι μεταξύ τους έχουν αποθηκευμένη την ίδια εκδοχή των δεδομένων. Οι κόμβοι αυτοί ονομάζονται **Πλήρης Κόμβοι** και αποθηκεύουν όλα τα δεδομένα της Αλυσίδας Συστοιχιών, συμπεριλαμβανομένων όλων των Συναλλαγών, Συστοιχιών και Επικεφαλίδων από την εκκίνηση της Αλυσίδας, ξεκινώντας με το Μπλοκ Γένεσης (Duong, Chepurnoy, & Zhou, 2018). Ο τρόπος λειτουργίας τους είναι η **Πλήρης Λειτουργία** και αποτελούν τους πιο ενεργούς κόμβους του συστήματος. Από αυτούς εξαρτάται η πλήρης επικύρωση των νέων Συναλλαγών και Συστοιχιών που εισάγονται στο σύστημα, σύμφωνα με τους κανόνες συναίνεσης του συστήματος, και κατ' επέκταση η συμπερίληψή τους στην Αλυσίδα Συστοιχιών.



Εικόνα 5.1. *Γραφική απεικόνιση της διάταξης Πλήρων Κόμβων εντός ενός συστήματος κρυπτονομίσματος (Longchamp, Deshpande, & Mehra, 2020).*

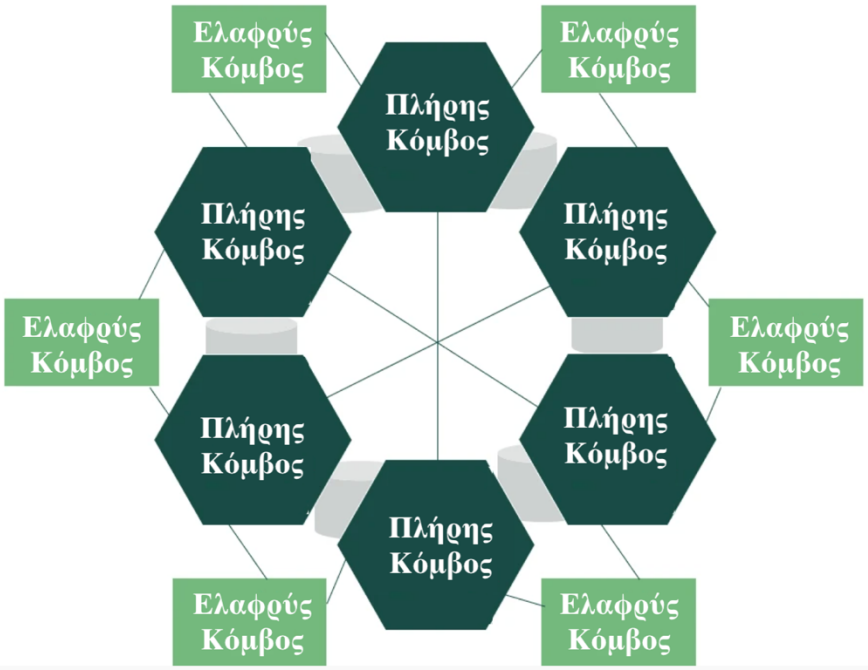
Οι απαιτήσεις σε αποθηκευτικό χώρο και μνήμη για ένα Πλήρη Κόμβο είναι αρκετά μεγάλες, λόγω του ότι απαιτούνται να επεξεργάζονται και να αποθηκεύουν μεγάλη ποσότητα δεδομένων, η οποία συνεχώς αυξάνεται. Ένας κόμβος σε Πλήρη Λειτουργία αποθηκεύει ένα πλήρης αντίγραφο της Αλυσίδας Συστοιχιών (Βλέπε Υποτμήμα 2.7) και έτσι πρέπει να γίνεται λήψη όλων των καινούργιων Συναλλαγών και Συστοιχιών που αναμεταδίδονται στο σύστημα. Αυτό εξασφαλίζει ότι όλοι οι Πλήρης Κόμβοι έχουν ακριβώς την ίδια εκδοχή των δεδομένων και ότι τα δεδομένα δεν ελέγχονται από μια οντότητα αλλά από όλους τους κόμβους ταυτόχρονα. Έτσι, όσο περισσότερους Πλήρης κόμβους περιλαμβάνει ένα σύστημα κρυπτονομίσματος, τόσο πιο αποκεντρωμένο και ασφαλές θεωρείται (Mark, 2018).



Εικόνα 5.2. *Γραφική απεικόνιση της πλήρης Αλυσίδας Συστοιχιών, την οποία έχουν αποθηκευμένη όλοι οι Πλήρης Κόμβοι (Duong, Chepurnoy, & Zhou, 2018).*

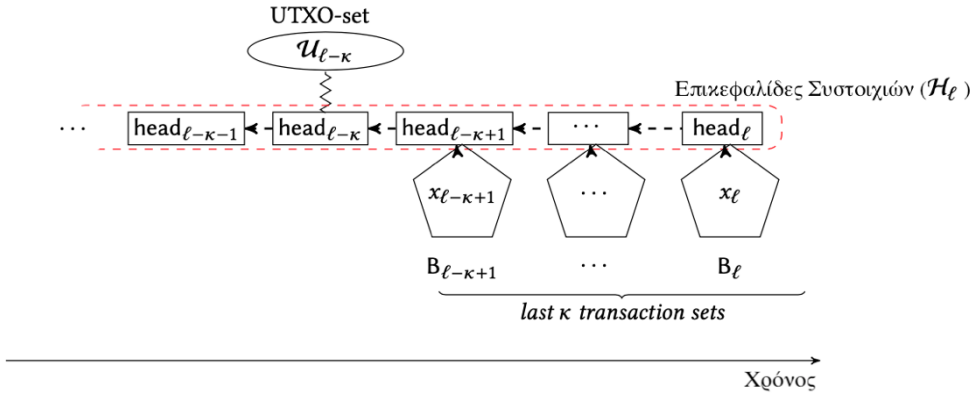
5.3 Ελαφριά Λειτουργία

Οι υπόλοιποι κόμβοι του συστήματος κρυπτονομίσματος ονομάζονται **Ελαφριοί Κόμβοι**, οι οποίοι αν και δεν αποθηκεύουν ολόκληρη την Αλυσίδα Συστοιχιών και τα δεδομένα αυτής, είναι πλήρης συγχρονισμένοι με την τρέχουσα κατάσταση του συστήματος. Ο τρόπος λειτουργίας τους είναι η **Ελαφριά Λειτουργία**, ωστόσο είναι ικανοί ανά πάσα στιγμή να επικυρώσουν την ύπαρξη μιας Συναλλαγή ή να πραγματοποιήσουν οι ίδιοι μια Συναλλαγή. Η επικύρωση σε ένα Ελαφρύ Κόμβο πραγματοποιείται με τη μέθοδο **Απλοποιημένη Επαλήθευση Πληρωμής**, Simplified Payment Verification (SPV) στην αγγλική γλώσσα. Η μέθοδος αυτή επιτρέπει στον κόμβο να επικυρώσει την ύπαρξη μιας Συναλλαγής σε μια Συστοιχία, χωρίς να έχει αποθηκευμένη ολόκληρη την Αλυσίδα Συστοιχιών. Για να είναι όμως αυτό δυνατόν, ένας Ελαφρύς Κόμβος συνδέεται με τουλάχιστον ένα Πλήρη Κόμβο, ο οποίος τον εξυπηρετεί επιτρέποντάς του να συνδεθεί με το σύστημα κρυπτονομίσματος, να μεταδώσει τις συναλλαγές του μέσω αυτού στο σύστημα και να ειδοποιηθεί όταν μια συναλλαγή τον αφορά (Mark, 2018).



Εικόνα 5.3. *Γραφική απεικόνιση της διάταξης Ελαφριών Κόμβων σε σχέση με Πλήρης Κόμβους εντός ενός συστήματος κρυπτονομίσματος (Longchamp, Deshpande, & Mehra, 2020).*

Σε αντίθεση με την Πλήρης Λειτουργία, ένας κόμβος σε Ελαφριά Λειτουργία δεν αποθηκεύει ολόκληρη της Αλυσίδα Συστοιχιών αλλά περιορισμένα στοιχεία αυτής. Στα περισσότερα συστήματα κρυπτονομίσματος αποθηκεύονται μόνο οι Επικεφαλίδες των Συστοιχιών, οι οποίες αποτελούν μια λεπτομερής περίληψη της Συστοιχίας. Οι απαιτήσεις για να τρέχει ένας Ελαφρύς Κόμβος είναι πολύ χαμηλότερες από ενός Πλήρης Κόμβου, με αποτέλεσμα να ελκύονται όλο και περισσότεροι χρήστες να λειτουργήσουν ένα κόμβο σε Ελαφριά Λειτουργία, βοηθώντας ταυτόχρονα την αποκέντρωση και την ανάπτυξη του συστήματος. Η σχέση μεταξύ Πλήρης και Ελαφριών Κόμβων είναι αναγκαία, διότι αν δεν υπήρχε οι Ελαφριοί Κόμβοι δεν θα μπορούσαν να λειτουργήσουν σε ένα σύστημα κρυπτονομίσματος και πιθανόν να οδηγούνταν προς μια κεντρική οντότητα (Mark, 2018). Συνήθως οι Ελαφριοί Κόμβοι είναι ηλεκτρονικά πορτοφόλια σε υπολογιστή ή κάποια έξυπνη συσκευή.



Εικόνα 5.4. *Γραφική απεικόνιση των δεδομένων της Αλυσίδας Συστοιχιών που αποθηκεύει ένας κόμβος σε* ***Ελαφριά Λειτουργία*** *(Duong, Chepurnoy, & Zhou, 2018).*

5.4 Συνεργασία Πλήρης και Ελαφριών Κόμβων

Σε ένα σύστημα κρυπτονομίσματος που όλοι οι κόμβοι έχουν τον ίδια τρόπο λειτουργίας, η επικύρωση και καταγραφή οποιασδήποτε ενέργειας είναι απλή, για παράδειγμα μια νέα Συναλλαγή. Αφού όλοι οι κόμβοι λειτουργούν με τον ίδια τρόπο, θα την επεξεργαστούν με τον ίδια τρόπο, θα την επικυρώσουν με τα ίδια κριτήρια και θα την αποθηκεύσουν στην κοινή τους Αλυσίδα Συστοιχιών. Σε ένα σύστημα κρυπτονομίσματος με **Πολλαπλούς Τρόπους Λειτουργίας** ωστόσο, η σταθερότητα και η ασφάλειά του επίκειται στο αν οι πλήρης και οι ελαφριοί κόμβοι είναι συμβατοί μεταξύ τους. Με απλά λόγια, μια Συναλλαγή πρέπει να γίνεται αποδεκτή ή να απορρίπτεται με τον ίδια τρόπο από κόμβους σε Πλήρη Λειτουργία και από κόμβους σε Ελαφριά Λειτουργία. Αυτή η ιδιότητα αποτελεί προϋπόθεση για να λειτουργήσει ορθά και με ασφάλεια ένα σύστημα κρυπτονομίσματος με Πολλαπλούς Τρόπους Λειτουργίας και ονομάζεται **Ιδιότητα Ορθότητας Συστήματος Πολλαπλών Τρόπων Λειτουργίας** (Duong, Chepurnoy, & Zhou, 2018).

Σε οποιοδήποτε σύστημα κρυπτονομίσματος που υποστηρίζει Πολλαπλούς Τρόπους Λειτουργίας, το δεδομένο είναι ότι οι Πλήρης Κόμβοι του αποθηκεύουν και ελέγχουν τα πάντα στην Αλυσίδα Συστοιχιών, καθώς και τα καινούργια δεδομένα που προστίθενται σε αυτή. Πιο συγκεκριμένα, ελέγχει την ορθότητα μιας Συναλλαγής, της ψηφιακή υπογραφή της, της επικεφαλίδας της Συστοιχίας, των δεικτών κατακερματισμού προς προηγούμενες επικεφαλίδες, της απόδειξης εργασίας της Συστοιχίας, κλπ. Οι Ελαφριοί Κόμβοι αντιθέτως, δεν αποθηκεύουν όλα αυτά τα δεδομένα αλλά κάποια κομμάτια από αυτά. Προκειμένου να ικανοποιείται η Ιδιότητα Ορθότητας Συστήματος Πολλαπλών Τρόπων Λειτουργίας όμως, πρέπει να είναι σε θέση να επικυρώσει την ορθότητα μιας νέας Συναλλαγής για παράδειγμα, με τον ίδιο τρόπο με ένα Πλήρη Κόμβο (Duong, Chepurnoy, & Zhou, 2018). Κάθε σύστημα κρυπτονομίσματος χρησιμοποίησε διαφορετικό τρόπο για να πετύχει την πιο πάνω ιδιότητα, αφού η Ελαφριά Λειτουργίας τους διαφέρει. Στα Υποτμήματα 5.5 και 5.6 θα αναλυθεί πως το Bitcoin και το Ethereum κατάφεραν να ικανοποιήσουν την Ιδιότητα Ορθότητας Συστήματος Πολλαπλών Τρόπων Λειτουργίας για τους Ελαφριούς Κόμβους του συστήματός τους.

5.5 Πολλαπλοί Τρόποι Λειτουργίας στο Bitcoin

Η ιδέα του Πολλαπλού Τρόπου Λειτουργίας εισάχθηκε στο Bitcoin με το αυθεντικό έγγραφο από τον Satoshi Nakamoto το 2008 (Nakamoto, 2008), στο οποίο περιγράφονται δύο Τρόποι Λειτουργίας για τους κόμβους που θα συμμετέχουν στο Bitcoin, ο Πλήρης και ο Απλής

Επαλήθευσης Πληρωμής (SPV). Ένας **Πλήρης Κόμβος** ελέγχει τα πάντα στην αλυσίδα συστοιχιών, από την ορθότητα της Απόδειξης Εργασίας, των δεικτών κατακερματισμού, των ψηφιακών υπογραφών, μέχρι την πλήρωση όλων των κανόνων του συστήματος από μια Συναλλαγή. Επίσης, είναι ζωτικής σημασίας για το σύστημα αφού αποθηκεύουν όλα τα δεδομένα του συστήματος, συμπεριλαμβανομένων ολόκληρη την αλυσίδα συστοιχιών, όλων των Συστοιχιών, όλων των Συναλλαγών και γενικότερα όλο το ιστορικό του συστήματος (Duong, Chepurnoy, & Zhou, 2018).

Οι κόμβοι **Απλής Επαλήθευσης Πληρωμής (SPV)** έχουν πιο ελαφρύ τρόπο λειτουργίας και συνήθως αποτελούν τους χρήστες που έχουν στην ιδιοκτησία τους ψηφιακό νόμισμα και το αποθηκεύουν σε ένα ψηφιακό πορτοφόλι. Για ένα τέτοιο χρήστη ο πιο πάνω τρόπος λειτουργίας είναι ιδανικός, αφού δεν απαιτεί μεγάλη ποσότητα μνήμης για κάτι τόσο απλό όσο η κατοχή μικρής ποσότητας κρυπτονομίσματος. Οι κόμβοι με τρόπο λειτουργίας SPV, αποθηκεύουν μόνο τις επικεφαλίδες των Συστοιχιών της αλυσίδας, κατά το συγχρονισμό τους με το δίκτυο του κρυπτονομίσματος. Όταν απαιτηθεί να επικυρώσουν μια συγκεκριμένη συναλλαγή, την αιτούνται μέσω ενός γειτονικού Πλήρης Κόμβου (Bashir, 2018).

Οι πιο πάνω υπήρξαν οι δύο τρόποι λειτουργίας για το σύστημα του Bitcoin μέχρι την έκδοση του Bitcoin Core 0.11.0 το 2015, στην οποία προστέθηκε ακόμα ένα ελαφρύς τρόπος λειτουργίας, το «pruning mode». Ένας κόμβος σε **Pruning mode** έχει παρόμοιες απαιτήσεις με τον τρόπο λειτουργίας SPV, ωστόσο αλληλοεπιδρά διαφορετικά με την αλυσίδα συστοιχιών. Αρχικά κατεβάζει και επεξεργάζεται όλες τις συστοιχίες όπως θα έκανε ένας πλήρης κόμβος, αλλά τελικά παραμένει μόνο μια σταθερού μήκους κατάληξη της αλυσίδας. Όπως και τον τρόπο λειτουργίας Απλής Επαλήθευσης Πληρωμής, ο τρόπος λειτουργίας pruning εξαρτάται πλήρως από ένα πλήρη κόμβο για να είναι ενεργός, ο οποίος αποθηκεύει το πρόθεμα της συστοιχίας που υπολείπεται στον ελαφρύ κόμβο (Duong, Chepurnoy, & Zhou, 2018).

5.6 Πολλαπλοί Τρόποι Λειτουργίας στο Ethereum

Το Ethereum, βασίστηκε στη λειτουργία SPV του Bitcoin για να δημιουργήσει το δικό του ελαφρύ τρόπο λειτουργίας, τον τρόπο λειτουργίας WarpSync στην έκδοση του Ethereum Parity. Ένας κόμβος που λειτουργεί με **Πλήρης Τρόπο Λειτουργίας**, αποθηκεύει όλα τα δεδομένα και το ιστορικό του δικτύου και επεξεργάζεται κάθε νεοεισερχόμενο δεδομένο. Στο παράδειγμα μιας νέας συναλλαγής, όλοι οι πλήρης κόμβοι στο Ethereum πρέπει να την επικυρώσουν για να θεωρηθεί έγκυρη, προκειμένου αυτή να συμπεριληφθεί σε συστοιχία και

κατ' επέκταση στην αλυσίδα συστοιχιών. Επιπρόσθετα, λόγω του προαναφερθέντος λόγου προκύπτει ότι όλοι οι πλήρης κόμβοι έχουν αποθηκευμένο το ίδιο αντίγραφο της αλυσίδας και έτσι διασφαλίζεται η ασφάλεια του συστήματος.

Ο τρόπος λειτουργίας **WarpSync** του Ethereum μπορεί να θεωρηθεί βελτίωση σε σχέση με τους ελαφριούς τρόπους λειτουργίας του Bitcoin, διότι συνδυάζει την περιορισμένη απαίτηση σε μνήμη με την ικανότητα επικύρωσης συναλλαγές. Δηλαδή οι κόμβοι που λειτουργούν με τρόπο λειτουργίας WarpSync, είναι ελαφριοί κόμβοι οι οποίοι μπορούν από μόνοι τους να επικυρώσουν νέες συναλλαγές χωρίς την ανάγκη ενός πλήρης κόμβου. Λόγω των περιορισμένων απαιτήσεων μπορούν να λειτουργήσουν σε συσκευές μικρής ισχύος όπως κινητά και tablets (Bashir, 2018). Στο σύστημα του Ethereum καθορίζεται μια κατάσταση επικύρωσης συναλλαγής από το πρωτόκολλο, και μια σύνοψη της κατάστασης αυτής περιλαμβάνεται εντός κάθε συστοιχίας. Ένας κόμβος με τρόπο λειτουργίας WarpSync, δεν αποθηκεύει ολόκληρη την αλυσίδα συστοιχιών, ωστόσο αποθηκεύει αριθμό συστοιχιών από το τέλος της αλυσίδας. Επιπρόσθετα, αφού επεξεργαστεί τις συστοιχίες και τις επικεφαλίδες τους, αυτές διαγράφονται και παραμένει μόνο η σύνοψη επικύρωσης αυτών (Duong, Chepurnoy, & Zhou, 2018).

Κεφάλαιο 6
Εξομοίωση Πολλαπλών Τρόπων Λειτουργίας

Στα προηγούμενα κεφάλαια αναλύθηκε ο μονοδιάστατος τρόπος λειτουργίας του Bitcoin και του Ethereum, το πρωτόκολλο πολλαπλών τρόπων λειτουργίας και πως εφαρμόζεται στα δύο αυτά συστήματα κρυπτονομίσματος. Με βάση τα δεδομένα των προηγούμενων κεφαλαίων και τις γνώσεις που αποκτήθηκαν από τις βιβλιογραφικές αναφορές, επιχειρήθηκε να γίνει μια εξομοίωση στην οποία εφαρμόζεται μια απλή μορφή των πολλαπλών τρόπων λειτουργίας . Αποφασίστηκε να δημιουργηθεί ένα πρόγραμμα με γραφικό περιβάλλον (GUI) στη γλώσσα προγραμματισμού Java, το οποίο να απεικονίζει ένα τεχνητό σύστημα κρυπτονομίσματος που υποστηρίζει πολλαπλούς τρόπου λειτουργίας. Τονίζεται ότι το πρόγραμμα εξομοίωσης δεν αποτελεί πραγματικό σύστημα κρυπτονομίσματος και ότι έγιναν αρκετές παραδοχές για την ευκολότερη και πιο κατανοητή λειτουργία του.

6.1 Απαιτήσεις Εξομοίωσης

Προκειμένου η εξομοίωση των Πολλαπλών Τρόπων Λειτουργίας να εξυπηρετεί το σκοπό της και να παρέχει ευχρηστία, πρέπει να τεθούν κάποιες προϋποθέσεις οι οποίες πρέπει να ικανοποιούνται:

- Η δημιουργία ενός εικονικού δικτύου από κόμβους και των αντίστοιχων ενώσεων τους.
- Για σκοπούς της εξομοίωσης μερικοί κόμβοι έχουν πλήρες τρόπο λειτουργίας, ενώ οι κάποιοι άλλοι ελαφρύ τρόπο λειτουργίας.
- Ο κάθε κόμβος πρέπει να έχει την δυνατότητα επικοινωνίας με κάθε άλλο κόμβο στο δίκτυο μέσω τουλάχιστον ενός μονοπατιού.
- Γραφική αναπαράσταση των κόμβων και των περιεχόμενων τους με τρόπο κατανοητό και ευπαρουσίαστο.
- Ο έλεγχος επικύρωσης συναλλαγών από πλήρης και από ελαφριούς κόμβους.

- Χαμηλό κόστος: η εξομοίωση καταναλώνει μηδαμινή ενέργεια και μπορεί να τεθεί σε λειτουργία σε συστήματα με χαμηλή επεξεργαστική ισχύ (hardware).
- Επεκτασιμότητα: το πρόγραμμα μπορεί να επεκταθεί με σχετικά χαμηλό προγραμματιστικό κόστος, με την προϋπόθεση βασικών γνώσεων Java και Java swing.
- Ευχρηστία: το πρόγραμμα παρέχει γραφικό περιβάλλον (GUI) για την ευκολότερη και πιο κατανοητή αλληλεπίδραση με τον χρήστη. Για παράδειγμα, κάνοντας click σε ένα κόμβο, εμφανίζεται σε νέο παράθυρο το περιεχόμενό του.

6.2 Επεξήγηση Εξομοίωσης

Η εξομοίωση έχει υλοποιηθεί με την χρήση της γλώσσας προγραμματισμού Java, και του GUI widget toolkit Java Swing, το οποίο είναι κομμάτι του Java Foundation Classes (JFC). Η δημιουργία ενός γραφικού περιβάλλοντος κρίθηκε απαραίτητη για την πιο ζωντανή απεικόνιση των λειτουργιών και επιπρόσθετα το πρόγραμμα να είναι πιο κατανοητό στον τελικό χρήστη. Το πρόγραμμα αποτελεί μία εξομοίωση της φυσικής λειτουργίας ενός κρυπτονομίσματος, όμως δεν μπορεί να χαρακτηριστεί ως μία ολοκληρωμένη αναπαράσταση πραγματικού συστήματος κρυπτονομίσματος.

6.2.1 Δομή Εξομοίωσης

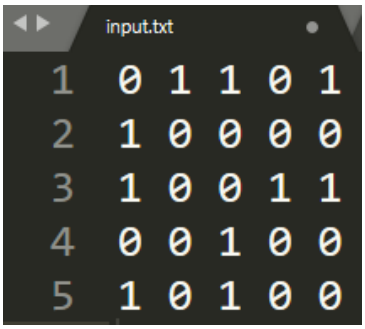
Σε ένα πλήρες δίκτυο κρυπτονομίσματος, μετά το μπλοκ γένεσης ακολουθεί μεγάλος αριθμός μπλοκ οι οποίες απαρτίζουν την αλυσίδα συστοιχιών. Για τους σκοπούς της εξομοίωσης χρησιμοποιείται μόνο ένα μπλοκ με 4 συναλλαγές, το οποίο αποτελεί την ελάχιστη προϋπόθεση για μια ορθή λειτουργία του δικτύου και κατ' επέκταση μια εξομοίωση που πληροί τις απαιτήσεις του Υποτμήματος 6.1. Η ύπαρξη ενός μόνο μπλοκ εξυπηρετεί τον σκοπό της εξομοίωσης και η μελλοντική πρόσθεση περεταίρω συστοιχιών αποσκοπεί αποκλειστικά στην απεικόνιση ενός σεναρίου πιο κοντά στην πραγματικότητα.

Ο χρήστης έχει πρόσβαση στο περιεχόμενο κάθε κόμβου επιλέγοντάς τον με το ποντίκι. Σε συνέχεια επιλογής του κόμβου, προβάλλεται νέα οθόνη με τα στοιχεία τα οποία περιέχει. Στην περίπτωση του πλήρες κόμβου, απεικονίζεται η επικεφαλίδα του μοναδικού μπλοκ, καθώς και οι συναλλαγές του μπλοκ σε μορφή δυαδικού δένδρου. Για τους κόμβους ελαφριάς λειτουργίας η απεικόνιση του περιεχομένου τους αποτελείται μόνο από την επικεφαλίδα του μπλοκ, η οποία

περιέχει το ριζικό κόμβο του δυαδικού δένδρου των συναλλαγών υπό τη μορφή της συνάρτησης κατακερματισμού.

6.2.2 Είσοδοι προγράμματος εξομοίωσης

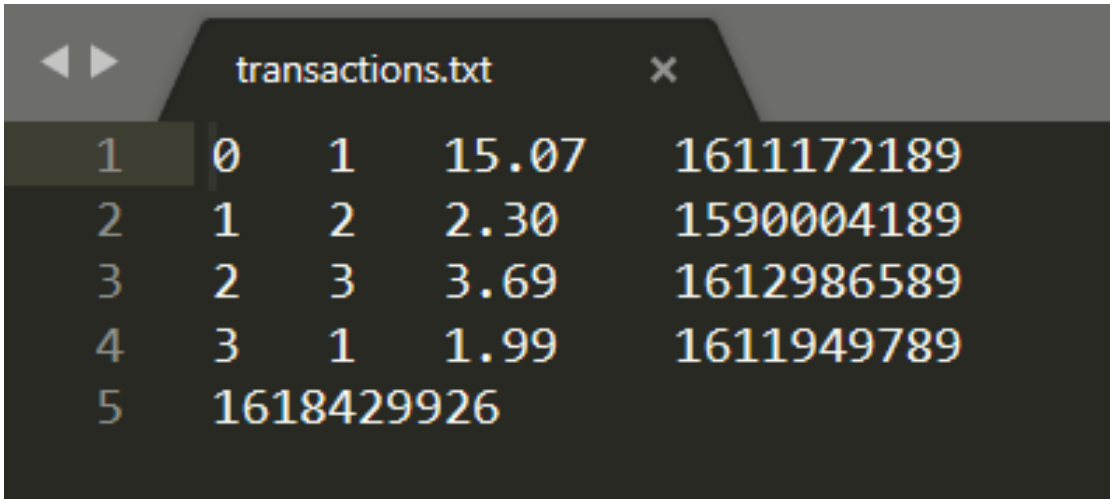
Η υλοποίηση της δομής των κόμβων εξαρτάται από δύο αρχεία εισόδου, μορφής text file. Η απεικόνιση των κόμβων και των ενώσεων τους βασίζεται στην ανάγνωση του αρχείου «input.txt" (βλέπε Εικόνα 6.1). Το αρχείο περιέχει τον πίνακα γειτνίασης των κόμβων και χρησιμοποιείται για να αποθηκευτούν οι γειτονικοί κόμβοι του καθενός από αυτούς. Η θέση (i, j) του πίνακα, όπου i είναι ο αριθμός σειράς και j ο αριθμός στήλης, αναπαριστά την πιθανή ένωση μεταξύ των κόμβων i και j. Για παράδειγμα αν ο αριθμός στην θέση (i, j) είναι '1' τότε υπάρχει ένωση μεταξύ των κόμβων i και j, ενώ αν είναι 0 τότε δεν υπάρχει ένωση μεταξύ των δύο κόμβων. Είναι σημαντικό να σημειωθεί ότι η διαγώνιος αποτελείται από μηδενικά στοιχεία, δηλαδή δεν υπάρχουν ενώσεις των κόμβων με τους εαυτούς του. Επίσης η διαγώνιος αποτελεί άξονα συμμετρίας για τον πίνακα, δηλαδή η τιμή της θέσης (i, j) είναι ίση με της θέσης (j, i).



Εικόνα 6.1. *Το περιεχόμενο του πίνακα γειτνίασης εντός του αρχείου «input.txt».*

Το δεύτερο αρχείο, με όνομα «transactions.txt» (βλέπε Εικόνα 6.2) καθορίζει όλα τα δεδομένα του μοναδικού μπλοκ της αλυσίδας. Οι πρώτες τέσσερις γραμμές αντιπροσωπεύουν τις τέσσερις συναλλαγές που έχουν προκαθοριστεί και δεν δημιουργούνται αυτόματα. Η τελευταία γραμμή είναι ο χρόνος δημιουργίας της συστοιχίας σε μορφή UNIX time. Κάθε στήλη αντιπροσωπεύει με την σειρά της τα ακόλουθα στοιχεία μιας συναλλαγής.

- Αριθμός κόμβου αποστολέα.
- Αριθμός κόμβου παραλήπτη.
- Ποσότητα κρυπτονομίσματος που αποστέλλεται.
- Χρόνος πραγματοποίησης συναλλαγής σε μορφή UNIX time.



Εικόνα 6.2. *Το περιεχόμενο του αρχείου «transactions.txt», οι πρώτες 4 γραμμές αντιπροσωπεύουν τις συναλλαγές του μπλοκ και η πέμπτη το χρόνο δημιουργίας του.*

6.3 Υλοποίηση και Απεικόνιση

Κατά την αρχική αλληλεπίδραση με το πρόγραμμα, ο τελικός χρήστης καλωσορίζεται με ένα παράθυρο όπου υπάρχει η γραφική διάταξη των κόμβων, μερικοί εκ των οποίων βρίσκονται σε πλήρης λειτουργία, ενώ άλλοι σε ελαφριά λειτουργία. Στην συνέχεια καλείται να επιλέξει έναν από τους κόμβους με την χρήση του ποντικιού του, για να μεταβεί σε οθόνη απεικόνισης των περιεχομένων του κόμβου. Στο κάτω μέρος αυτής της οθόνης μπορεί να εκτελεστεί η επικύρωση μιας συναλλαγής. Το τμήμα αυτό χωρίζεται σε τρία υποτμήματα, ένα για καθεμιά από τις πιο πάνω λειτουργίες.

6.3.1 Γραφική αναπαράσταση των κόμβων

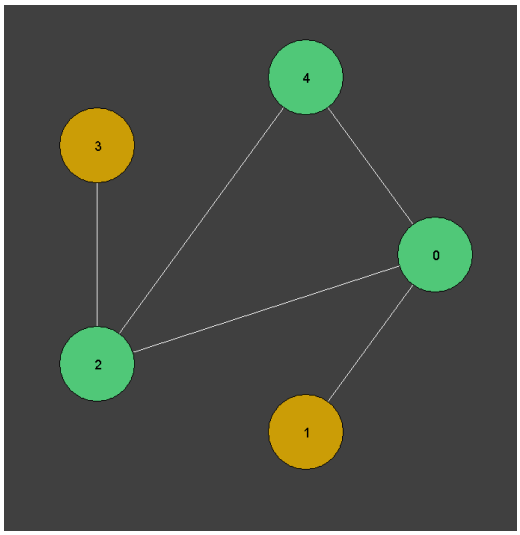
Ακολούθως της ανάγνωσης του αρχείου που περιέχει τον πίνακα γειτνίασης (Βλέπε Υποτμήμα 6.2.2), δημιουργούνται κόμβοι και τοποθετούνται σε κυκλική διάταξη. Ο υπολογισμός της θέσης καθορίζεται ως εξής (βλέπε Εικόνα 6.3):

```
1. for (int i = 0; i < noOfNodes; i++) {
2.    final double angle = Math.toRadians(((double) i / noOfNodes) * 360d);
3.
4.    points[i] = new Point(
5.            (int) (Math.cos(angle) * RADIUS),
6.            (int) (Math.sin(angle) * RADIUS)
7.    );
8. }
```

Εικόνα 6.3. *Το κομμάτι του κώδικα που καθορίζει τη θέση κάθε i κόμβου.*

Χρησιμοποιείται ένα forloop με αριθμό επαναλήψεων όσοι είναι και οι κόμβοι. Η κάθε εκτέλεση του forloop υπολογίζει την θέση την οποία θα λάβει στην οθόνη ο αντίστοιχος κόμβος. Στόχος της γραμμής κώδικα 2 είναι ο υπολογισμός των μοιρών τοποθέτησης του κόμβου στον κύκλο. Για παράδειγμα αν έχουμε 6 κόμβος ο πρώτος κόμβος θα λάβει 0 μοίρες και ο κάθε επόμενος κόμβος θα τοποθετείται στην περίμετρο του κύκλου 60 μοίρες πιο δεξιά από τον προηγούμενο. Ο υπολογισμός του σημείου x και y στην περίμετρο του κύκλου γίνεται στις γραμμές κώδικα 4-7, όπου το RADIUS είναι προκαθορισμένο και αναπαριστά την σταθερή ακτίνα του κύκλου. Με την χρήση του πιο πάνω κώδικα επιτυγχάνεται μια κατανοητή αναπαράσταση των κόμβων, οι οποίοι μοιράζονται ίσα στην περίμετρο του κύκλου ανάλογα με το πλήθος τους.

Με βάση τις ενώσεις που λήφθηκαν από τον πίνακα γειτνίασης του αρχείου «input.txt» υπολογίζονται οι γειτονικοί κόμβοι του κάθε κόμβου. Για πιο εύκολη κατανόηση, οι ενώσεις επικοινωνίας των κόμβων αναπαρίστανται με λευκή γραμμή ένωσης. Για τους σκοπούς και τις ανάγκες της εξομοίωσης αποφασίστηκε ότι θα γίνει χρήση πέντε κόμβων με τις ενώσεις που βλέπουμε στην Εικόνα 6.4.



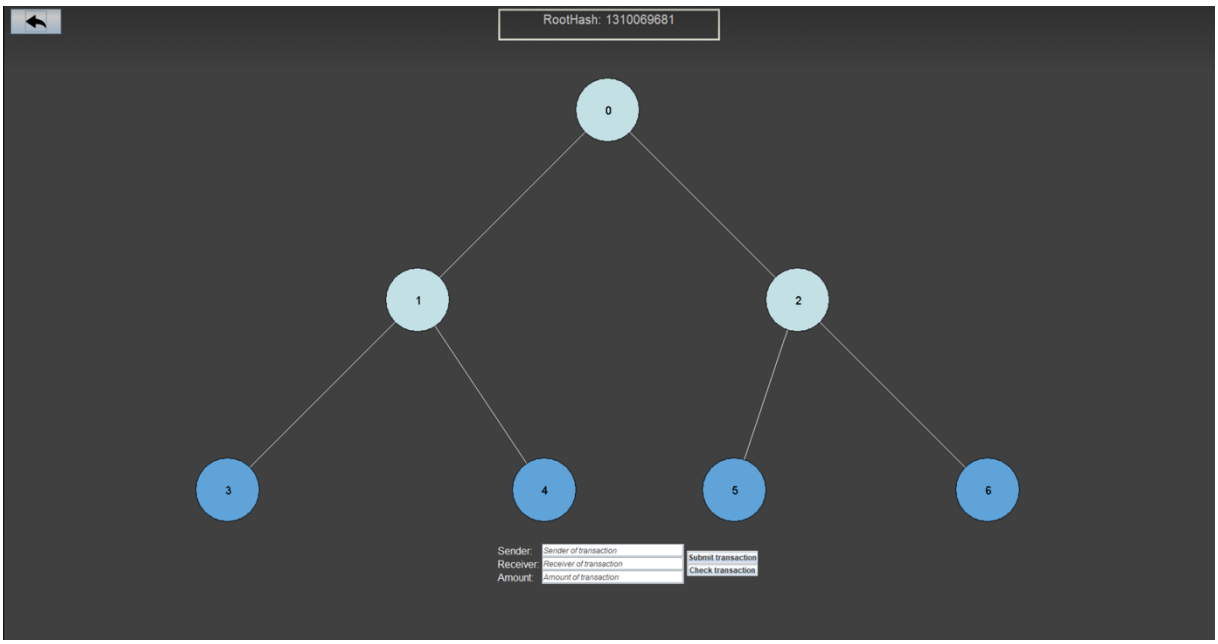
Εικόνα 6.4. *Γραφική απεικόνιση των κόμβων του προγράμματος εξομοίωσης. Οι πράσινοι κόμβοι αντιπροσωπεύουν τους πλήρης και οι κίτρινοι τους ελαφριούς κόμβους.*

Η οπτική διαφοροποίηση των κόμβων που βρίσκονται σε πλήρης και ελαφριά λειτουργία επιτυγχάνεται με την χρήση διαφορετικών χρωμάτων στους κόμβους του κάθε είδος. Οι κόμβοι που βρίσκονται σε ελαφριά λειτουργία έχουν κίτρινο χρώμα, ενώ οι κόμβοι που βρίσκονται σε πλήρης λειτουργία έχουν χρώμα πράσινο. Επίσης μπορεί να παρατηρηθεί ότι οι πλήρεις κόμβοι βρίσκονται σε πλήρες πλέγμα, δηλαδή ο κάθε κόμβος έχει άμεση ένωση με κάθε άλλο πλήρη κόμβο. Οι ελαφριοί κόμβοι ωστόσο, έχουν άμεση ένωση με τουλάχιστον ένα κόμβο που βρίσκεται σε πλήρες λειτουργία, από τον οποίο εξαρτώνται για κάποιες διεργασίες όπως είναι η επικύρωση μίας συναλλαγής.

6.3.2 Περιεχόμενο του επιλεγμένου κόμβου

Σε συνέχεια της επιλογής ενός κόμβου με το αριστερό click στο ποντίκι, ο τελικός χρήστης μεταφέρεται σε οθόνη που παρουσιάζεται το περιεχόμενου του επιλεγμένου κόμβου. Αν επιλεχθεί κόμβος ελαφριάς λειτουργίας, τότε εμφανίζεται στην οθόνη η επικεφαλίδα του κόμβου, η οποία περιέχει τον ριζικό κόμβο. Ο ριζικός κόμβος περιέχει την τελική συνάρτηση κατακερματισμού που προκύπτει από το δυαδικό δένδρο των συναλλαγών. Στην περίπτωση επιλογής κόμβου πλήρης λειτουργίας, πέραν των προαναφερθέντων, εμφανίζεται ολόκληρο το δυαδικό δένδρο των συναλλαγών του οποίου τα φύλλα του δένδρου αναπαριστούν της συναλλαγές.

Τα φύλλα του δένδρου, τα οποία κρατούν τις πληροφορίες των συναλλαγών αναπαρίστανται με μπλε χρώμα ενώ οι κόμβοι των πιο πάνω επιπέδων που διατηρούν πληροφορίες μέχρι το ριζικό κόμβο είναι με απαλό γαλάζιο. (Βλέπε Εικόνα 6.5)



Εικόνα 6.5. *Γραφική απεικόνιση του περιεχομένου ενός πλήρης κόμβου του προγράμματος εξομοίωσης.*

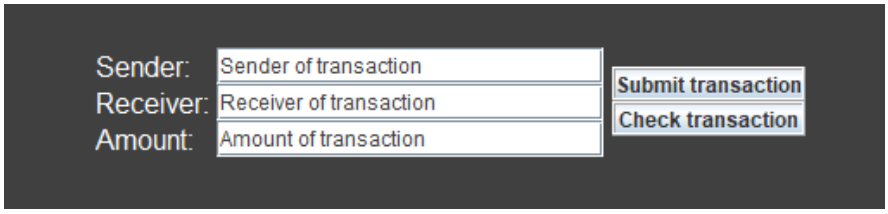
Ο υπολογισμός της συνάρτησης κατακερματισμού κάνει χρήση της μεθόδου διάσχισης "postorder traversal" ως μέθοδο διάσχισης του δένδρου. Δηλαδή για κάθε κόμβο, επισκεπτόμαστε πρώτα τους κόμβους του αριστερού του υπό δένδρου μεταγενέστερα του δεξιού υπό δένδρου και τέλος τον ίδιο τον κόμβο. Γίνεται υπολογισμός της συνάρτησης κατακερματισμού των φύλλων και στην συνέχεια χρησιμοποιείται η πιο κάτω μέθοδος έτσι ώστε να αγνοεί τα φύλλα διασχίζοντας το υπόλοιπο δένδρο προς τα πάνω. Στον κάθε κόμβος που τυγχάνει επίσκεψης, η τιμή κατακερματισμού υπολογίζει ως εξής:

$$hashOfCurrentNode = hash[(hashOfLeftChild) \oplus (hashOfRightChild)]$$

6.3.3 Επικύρωση συναλλαγής

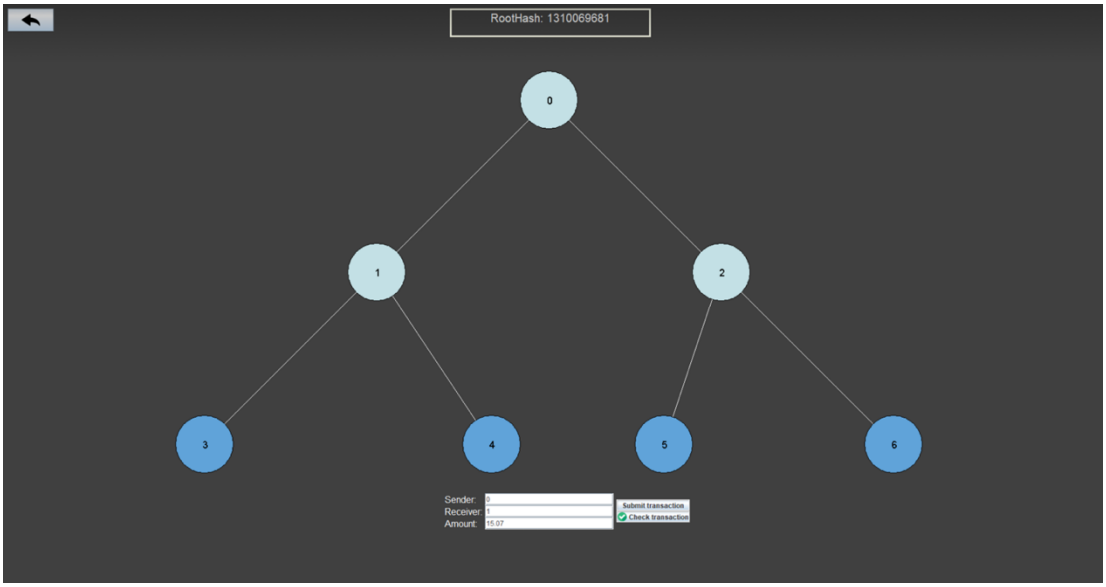
Στο κάτω μέρος της οθόνης του περιεχομένου κάθε κόμβου, βρίσκονται 2 επιλογές για:

- επιβεβαίωση υπάρχουσας συναλλαγής και
- έλεγχο για πραγματοποίηση καινούριας συναλλαγής



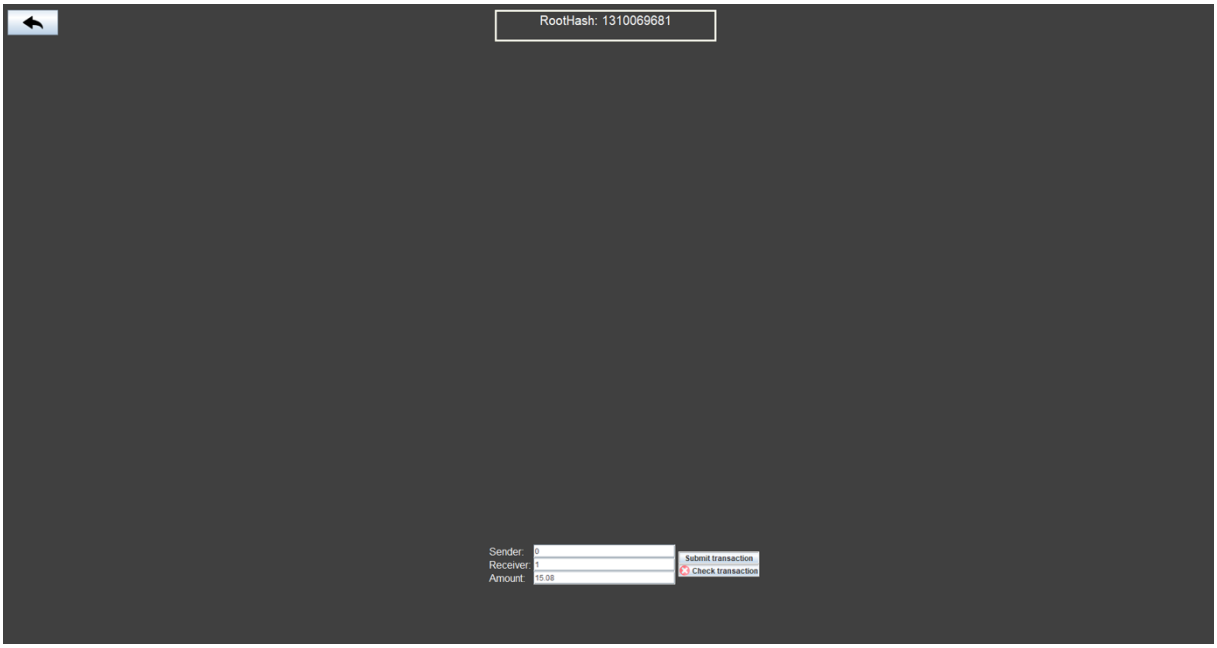
Εικόνα 6.6. *Screenshot του μέρους του παραθύρου στο οποίο γίνεται η επιβεβαίωση πραγματοποίησης συναλλαγής (Check transaction) και η επικύρωση μιας καινούργιας συναλλαγής (Sumbit transaction)*

Στο μέρος αυτό ο χρήστης μπορεί να δηλώσει τον αριθμό του κόμβου αποστολέα, παραλήπτη καθώς και το ποσό της σχετικής συναλλαγής. Ακολούθως, αφού έχει συμπληρώσει τα απαραίτητα στοιχεία, μπορεί να επιλέξει να προβεί σε έλεγχο για υπάρχουσα συναλλαγή με το πάτημα του κουμπιού “Check transaction”. Η ενέργεια αυτή θα ολοκληρωθεί με μια ακολουθία ελέγχων ανάλογα με το είδος του κόμβου, πλήρες ή ελαφρύς. Όπως έχει προαναφερθεί ο χρήστης επιλέγει ένα από τους κόμβους από την αρχική οθόνη του προγράμματος. Αν βρισκόμαστε σε κόμβο πλήρης λειτουργίας, τότε ο κόμβος έχει άμεση πρόσβαση στις συναλλαγές του μπλοκ, άρα θα μπορέσει να ελέγξει τις συναλλαγές, και να επιβεβαιώσει κατά πόσο η συναλλαγή προς έλεγχο υπάρχει εντός του δυαδικού δένδρου, που σημαίνει ότι έχει ολοκληρωθεί στο παρελθόν. Σε περίπτωση εύρεσης της συναλλαγής, τότε θα ενημερωθεί ο χρήστης για την ύπαρξη της με την προσθήκη εικονιδίου ‘√’ (Βλέπε Εικόνα 6.7).



Εικόνα 6.7. *Απεικόνιση θετικού παραδείγματος ελέγχου ύπαρξης συναλλαγής από πλήρη κόμβο.*

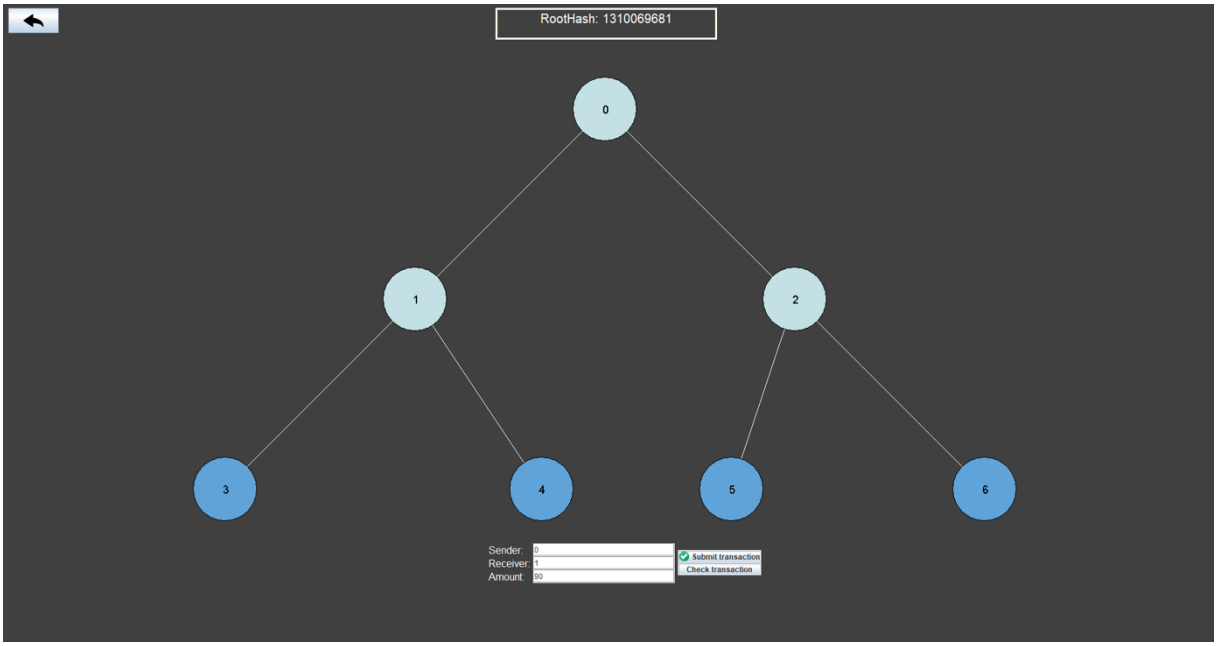
Παρόμοια, στον έλεγχο ύπαρξης συναλλαγής για κόμβο ελαφριάς λειτουργίας, θα πρέπει να υπάρξει πρόσβαση στο δυαδικό δένδρο των συναλλαγών. Καθώς ένας ελαφρύς κόμβος δεν διατηρεί τα δεδομένα των συστοιχιών και συνεπώς των συναλλαγών πρέπει να γίνει ο έλεγχος στα δεδομένα του πλήρη κόμβου με τον οποίο γειτονεύει. Με τη πρόσβαση στο δυαδικό δένδρο των συναλλαγών, θα ακολουθηθεί η ίδια διαδικασία ταυτοποίησης της συναλλαγής και ενημέρωσης της πιθανής ύπαρξης της. Στην περίπτωση αποτυχημένης εύρεσης της συναλλαγής, ο χρήστης ενημερώνεται με την προσθήκη εικονιδίου '☒' (Βλέπε Εικόνα 6.8).



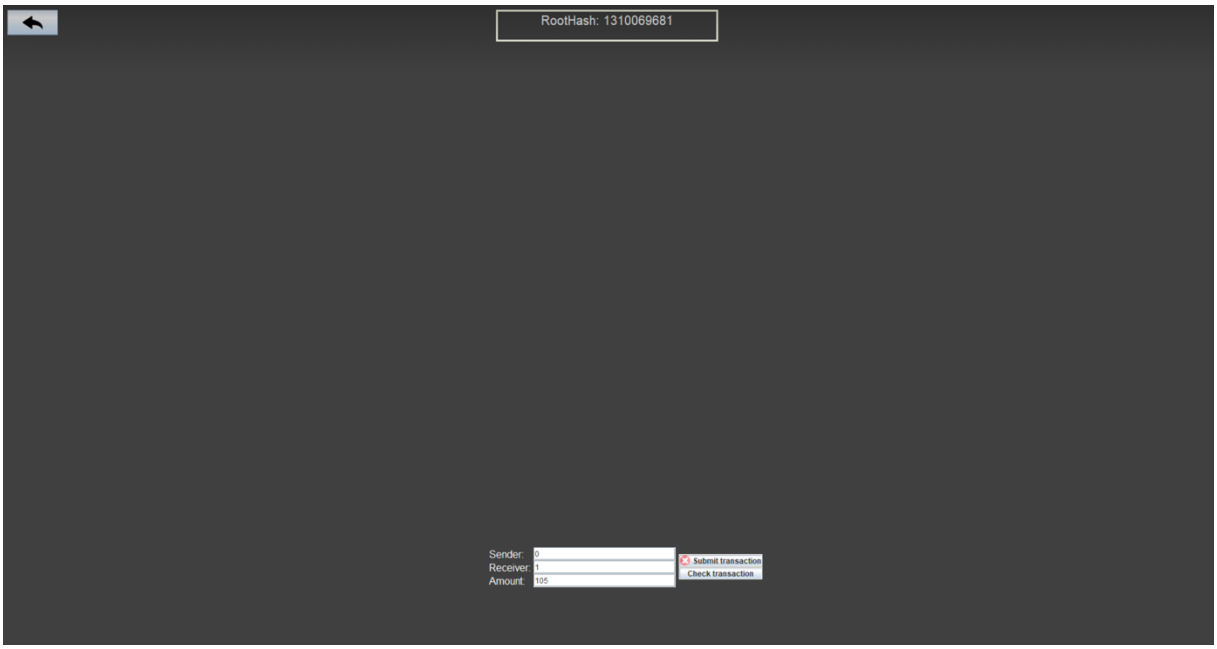
Εικόνα 6.8. *Απεικόνιση αρνητικού παραδείγματος ελέγχου ύπαρξης συναλλαγής από ελαφρύ κόμβο.*

Στα πλαίσια της εξομοίωσης, ο κάθε κόμβος λαμβάνει ένα εικονικό πόσο των 100 κρυπτονομισμάτων κατά την έναρξη του προγράμματος, για σκοπούς ελέγχου πραγματοποίησης καινούργιας συναλλαγής. Με την πρόσθεση των απαραίτητων στοιχείων στα πεδία κειμένων, ο χρήστης μπορεί να πατήσει το κουμπί "Submit transaction" για να ελέγξει κατά πόσο ο αποστολέας διαθέτει το δηλωμένο που θα αποσταλεί και κατ' επέκταση αν μπορεί να πραγματοποιηθεί η συναλλαγή. Για να ελεγχθεί αυτό, θα πρέπει να προσπελάσουμε όλες τις πραγματοποιημένες συναλλαγές και για κάθε συναλλαγή το πόσο που αποστέλλεται θα αφαιρείται από το διαθέσιμο ποσό του αποστολέα, και θα προστίθεται στο διαθέσιμο ποσό του παραλήπτη. Μετά την προσπέλαση όλων των συναλλαγών ο κάθε κόμβος θα έχει το ανανεωμένο διαθέσιμο ποσό του. Αν το πόσο της καινούργιας συναλλαγής που ελέγχεται προς πραγματοποίηση, είναι μικρότερο ή ίσο με το διαθέσιμο ποσό του αποστολέα τότε η συναλλαγή μπορεί να ολοκληρωθεί. Στην περίπτωση επιτυχίας ολοκλήρωσης

συναλλαγής, θα προστεθεί εικονίδιο '✓' (Βλέπε Εικόνα 6.9) και στην περίπτωση αποτυχημένης ολοκλήρωσης της συναλλαγής τότε προστίθεται εικονίδιο '☒' (Βλέπε Εικόνα 6.10).



Εικόνα 6.9. *Απεικόνιση θετικού παραδείγματος ελέγχου για πραγματοποίηση καινούργιας συναλλαγής από πλήρης κόμβο.*



Εικόνα 6.10. *Απεικόνιση αρνητικού παραδείγματος ελέγχου για πραγματοποίηση καινούργιας συναλλαγής από ελαφρύ κόμβο.*

Κεφάλαιο 7
Επίλογος

Το Κεφάλαιο Επίλογος περιέχει κάποια συμπεράσματα που προήλθαν κατά τη συγγραφή της μεταπτυχιακής διπλωματικής, απαντώντας ταυτόχρονα τα ερευνητικά ερωτήματα που τέθηκαν στο Τμήμα 1.3. Ο σκοπός της μεταπτυχιακής διατριβής αρχικά ήταν να αναλυθεί ο μονότροπος, απλός τρόπος λειτουργίας δύο συστημάτων κρυπτονομισμάτων, το Bitcoin και το Ethereum. Επέλεξα για ανάλυση αυτά τα δύο, διότι αποτελούν δύο από τα πιο ολοκληρωμένα συστήματα κρυπτονομίσματος και υποστηρίζουν επιπρόσθετα πολλαπλό τρόπο λειτουργίας πέραν του μονότροπου. Η ανάλυση του Bitcoin και του Ethereum σε συνδυασμό με το Κεφάλαιο «Βασικές Κρυπτογραφικές Έννοιες» που προηγείται, βοηθά τον αναγνώστη να κατανοήσει πως λειτουργά σε γενικές γραμμές ένα σύστημα κρυπτονομίσματος και πιο συγκεκριμένα πως διενεργείται μια συναλλαγή, πως δομείται μια συστοιχία, πως δημιουργείται ένα καινούργιο μπλοκ και ποιοι αλγόριθμοι χρησιμοποιούνται σε κάθε διαδικασία. Παρόλο που οι γενικές κατευθύνσεις για τη λειτουργία ενός συστήματος κρυπτονομίσματος είναι κοινές, κάθε ένα από αυτά έχει τις δικές του ιδιαιτερότητες και διαφοροποιήσεις από τις κατευθύνσεις αυτές. Κατά τη συγγραφή του Κεφαλαίου του Ethereum γίνεται νύξη στις διαφορές τους, απαντώντας έτσι στο πρώτο ερευνητικό ερώτημα της μεταπτυχιακής Τονίζεται ότι τα δύο αυτά κρυπτονομίσματα λειτουργώντας με το δικό τους διαφορετικό τρόπο, μπορούν να επιτύχουν τον ίδιο σκοπό με ίδια ή ακόμα και λιγότερη προσπάθεια.

Άρα συμπεραίνουμε ότι αν κάποιος λειτουργά με διαφορετικό τρόπο από κάποιο άλλο, δεν σημαίνει απαραίτητα ότι δεν θα έχει την ίδια απόδοση. Αντίθετα, μπορεί να εξυπηρετεί το σκοπό του και ταυτόχρονα να καταναλώνει λιγότερη ενέργεια, χώρο και χρόνο. Αυτή είναι και η σκεπτική πάνω στην οποία βασίστηκε ο Πολλαπλός Τρόπος Λειτουργίας συστημάτων κρυπτονομίσματος, ο οποίος αποτελεί το επίκεντρο της μεταπτυχιακής διπλωματικής. Δηλαδή, μπορεί να υπάρξει σε ένα σύστημα κρυπτονομίσματος κάποιος κόμβος σε ελαφριά λειτουργία, ο οποίος να εκτελεί τις λειτουργίες ενός πλήρη κόμβου, έχοντας ταυτόχρονα λιγότερες απαιτήσεις σε

αποθηκευτικό χώρο και υπολογιστική ισχύ. Αυτό επιτυγχάνει αύξηση απόδοσης σε ολόκληρο το σύστημα, διότι μειώνεται ο όγκος των δεδομένων που πρέπει να διοχετεύεται συνεχώς σε όλους του κόμβους του συστήματος και βελτιώνεται ο χρόνος επεξεργασίας και ελέγχου νέων δεδομένων. Την ίδια στιγμή, αυξάνεται η ζήτηση αφού η μείωση των απαιτήσεων δίνει τη δυνατότητα σε περισσότερου χρήστες να ενταχθούν στο σύστημα ως ελαφριοί κόμβοι.

Συμπεραίνουμε ότι ένα σύστημα που περιέχει τόσο πλήρης κόμβους που αποτελούν τη ραχοκοκαλιά του συστήματος, όσο και ελαφριούς κόμβους, μπορεί να θεωρηθεί ως πιο ολοκληρωμένο και αποδοτικότερο σε σχέση με ένα σύστημα που λειτουργεί μονότροπα με μόνο πλήρες κόμβους. Με τη χρήση ενός γραφικού περιβάλλοντος (GUI), το πρόγραμμα εξομοίωσης απεικονίζει γραφικά τη λειτουργία ενός συστήματος κρυπτονομίσματος με πολλαπλούς τρόπους λειτουργίας. Το πρόγραμμα αυτό κάνει αρκετές παραδοχές, αλλά είναι σε θέση να απαντήσει στο δεύτερο ερευνητικό ερώτημα. Πιο συγκεκριμένα, απεικονίζεται μια διάταξη με πλήρης και ελαφριούς κόμβους και πως συνδέονται μεταξύ τους. Επίσης μπορεί να απεικονίσει ότι τόσο ένας κόμβος σε πλήρη λειτουργία, όσο και ένας σε ελαφριά λειτουργία μπορούν να επιβεβαιώσουν την πραγματοποίηση μιας συναλλαγής, αλλά με ελαφρώς διαφορετική λειτουργία. Παρόλα αυτά, υπάρχει αρκετά μεγάλο περιθώριο βελτίωσης του προγράμματος εξομοίωσης πολλαπλών τρόπων λειτουργίας.

7.1 Μελλοντική Ανάπτυξη

Ο σκοπός της ανάπτυξης της εξομοίωσης είναι καθαρά συμπληρωματικής φύσης ως προς την διατριβή αυτή. Δεν μπορεί να κριθεί ως μια πλήρης εξομοίωση της λειτουργίας ενός κρυπτονομίσματος, καθώς παρουσιάζει παραδοχές στα πλαίσια συγκεκριμένων σεναρίων. Το πρόγραμμα της εξομοίωσης μπορεί να αναπτυχθεί περαιτέρω με σκοπό να μπορέσει να συμπεριλάβει περισσότερα σενάρια χρήσης και λειτουργίας ενός κρυπτονομίσματος. Ακόμη ένας σημαντικός τομέας της εξομοίωσης αυτής, ο οποίος μπορεί να αναπτυχθεί σε μεγαλύτερο βαθμό είναι η ευκολία χρήσης. Τηρούνται βασικά κριτήρια ευχρηστίας, όμως υπάρχουν τομείς οι οποίοι θα βοηθήσουν την ευχρηστία αν αναπτυχθούν με διαφορετικό τρόπο.

7.1.1 Πρόσθεση κόμβων και ενώσεων

Αρχικά, μπορούμε να αναγνωρίσουμε ότι η μέθοδος δημιουργίας των κόμβων μέσω ενός text file, καλύπτει τις ανάγκες αυτής της διπλωματικής εργασίας, παρόλα αυτά ένας πιο διαδραστικός τρόπος πρόσθεσης των κόμβων και των ενώσεων τους, κρίνεται καλύτερη λύση. Συνεπώς, προτείνεται η υλοποίηση ενός γραφικού περιβάλλοντος στο οποίο θα επιτρέπει στον χρήστη την πρόσθεση κόμβων. Η πρόσθεση των κόμβων μπορεί να ακολουθήσει παρόμοια διαμόρφωση στην οθόνη, δηλαδή κυκλική διάταξη, και με το πάτημα ενός κουμπιού θα μπορεί να βλέπει ο χρήστης την νέα κυκλική διάταξη που συμπεριλαμβάνει τον καινούριο κόμβο. Για τις ενώσεις των κόμβων μπορεί να ακολουθηθεί η εξής προσέγγιση· η αυτόματη πρόσθεση ενώσεων κατά την πρόσθεση κάποιου κόμβου, η οποία θα τηρεί κριτήρια βάσει το είδος λειτουργίας του κόμβου. Δηλαδή, αν προστεθεί κάποιος κόμβος πλήρης λειτουργίας θα πρέπει αυτόματα να δημιουργούνται οι ενώσεις με κάθε άλλο κόμβο ο οποίος βρίσκεται σε πλήρης λειτουργία. Στην περίπτωση κόμβου ελαφριάς λειτουργίας, τότε θα πρέπει να δημιουργείται «τυχαία» τουλάχιστον μία ένωση με κάποιο κόμβο πλήρης λειτουργίας.

7.1.2 Λειτουργία με περισσότερες συστοιχίες

Όπως έχει προαναφερθεί, η εξομοίωση αυτή λειτουργεί με μόνο μία συστοιχία. Σύμφωνα με την παρούσα λειτουργία, η αναζήτηση κάποιας συναλλαγής γίνεται στα φύλλα του δένδρου συναλλαγών της συστοιχίας, και η πιθανή εύρεση της συναλλαγής οδηγεί στην επιστροφή του hashed root της συστοιχίας στην οποία βρίσκεται η συναλλαγή που αναζητήθηκε.

Η αντίστοιχη λειτουργία εύρεσης συναλλαγής σε σύστημα με περισσότερες συστοιχίες, θα λειτουργούσε ως εξής. Ξεκινώντας από το τελευταίο μπλοκ μίας αλυσίδας συστοιχιών αναζητείται η συναλλαγή που ζητήθηκε από τον χρήστη. Αν δεν βρεθεί η συγκεκριμένη συναλλαγή στο μπλοκ το οποίο βρισκόμαστε, τότε μεταβαίνουμε στο αμέσως προηγούμενο μπλοκ της αλυσίδας, μέσω της ένωσης που υπάρχει βάσει του hash pointer. Ένα βασικό κομμάτι το οποίο απουσιάζει το οποίο απουσιάζει από την δομή δεδομένων της συστοιχίας είναι το hash pointer, το οποίο ενώνει την επικεφαλίδα συστοιχίας με την ακριβώς προηγούμενη συστοιχία. Ως αποτέλεσμα δεν υπάρχει δυνατότητα μετάβασης σε προηγούμενο μπλοκ. Για να είναι δυνατή η λειτουργία με περισσότερες από μια συστοιχίες πρέπει να προστεθεί στην δομή δεδομένων το hashed pointer και να δημιουργείται έτσι μια ολοκληρωμένη αλυσίδα συστοιχιών, εντός της οποίας μπορούμε να αναζητήσουμε συγκεκριμένη συναλλαγή.

7.1.3 Δυναμική πρόσθεση συναλλαγών και συστοιχιών

Με την παρούσα λειτουργία του προγράμματος, υπάρχει μία σταθερή ομάδα συναλλαγών, οι οποίες αποτελούν και την μοναδική συστοιχία. Προτείνεται ως επέκταση του προγράμματος η δημιουργία γραφικού περιβάλλοντος στο οποίο ο χρήστης να προσθέσει αρχικά καινούριες συναλλαγές, οι οποίες θα λαμβάνουν χρόνο διενέργειας τους το τρέχων unix timestamp. Η πρόσθεση περισσότερων συναλλαγών θα γίνεται σε ένα προσωρινό μπλοκ το οποίο όταν ολοκληρωθεί με τον μέγιστο αριθμό συναλλαγών, θα προστεθεί στην αλυσίδα συστοιχιών λαμβάνοντας ως χρόνο δημιουργίας το τρέχων unix timestamp. Επίσης, θα πρέπει να διατηρεί στην επικεφαλίδα του το hashed pointer του αμέσως προηγούμενου μπλοκ.

Με αυτό τον τρόπο, κάθε συναλλαγή ενός κόμβου θα διενεργείται σε μεταγενέστερο χρόνο από την προηγούμενη συναλλαγή, και η κάθε συστοιχία από την αμέσως προηγούμενη συστοιχία. Συμπεραίνουμε ότι η αναζήτηση κάποιας συναλλαγής ακολουθεί ιστορική αναζήτηση ξεκινώντας από την πιο πρόσφατη διενέργεια συναλλαγής στο πιο πρόσφατο μπλοκ.

Βιβλιογραφία

Stampernas, S. (2018). *Blockchain technologies and smart contracts in the context of the Internet of Things.* Piraeus: Univercity of Piraeus.

Werner, R., Lawrenz, S., & Rausch, A. (2020). Blockchain Analysis Tool of a Cryptocurrency. *The 2020 2nd International Conference on Blockchain Technology ICBCT 2020.* Hawaii, USA: Univercity of Hawaii-Hilo.

Duong, T., Chepurnoy, A., & Zhou, H. S. (2018). Multi-mode Cryptocurrency Systems. *Proceedings of ACM Conference (Con- ference'17).* New York, USA: ACM.

Vaneetvelde, K. (2018). *Etherium Projects for Beginners.* Birmingham: Packt Publishing Ltd.

McAndrew, A. (2011). Hash Functions. Στο A. McAndrew, *Introduction to Cryptography with Open-Source Software* (σσ. 267-294). Victoria, Australia: CRC Press.

Fekkes, L. (2018). *Comparting Bitcoin and Ethereum.* Radboud Univercity.

Wang, M., Duan, M., & Zhu, J. (2018). Research on the Security Criteria of Hash Functions in the Blockchain. *BCC '18: Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts*, (σσ. 47-55). Incheon, Republic of Korea.

Bashir, I. (2018). *Mastering Blockchain.* Birmingham, UK: Packt Publishing Ltd.

Matt. (2018, December 20). *Bitcoin's UTXO Set Explained.* Ανάκτηση από www.mycryptopedia.com: https://www.mycryptopedia.com/bitcoin-utxo-unspent-transaction-output-set-explained/

Kavalar, M. (2019, September 24). *Toward Reproductivity: Git*. Ανάκτηση από https://nextjournal.com: https://nextjournal.com/blog/git

Giroux, O. (2018, November 7). *CUDA on Turing Opens New GPU Compute Possibilities*. Ανάκτηση από https://developer.nvidia.com: https://developer.nvidia.com/blog/cuda-turing-new-gpu-compute-possibilities/

Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Ανάκτηση από bitcoin.org: https://bitcoin.org/bitcoin.pdf

BitcoinBTC. (2020, December 26). Ανάκτηση από coindesk.com: https://www.coindesk.com/price/bitcoin

How Many Bitcoins Are There? (χ.χ.). Ανάκτηση από buybitcoinworldwide.com: https://www.buybitcoinworldwide.com/how-many-bitcoins-are-there/#:~:text=There%20are%20currently%2018%2C579%2C275%20bitcoins,adds%206.25%20bitcoins%20into%20circulation.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies.* Princeton, United States: Princeton Univercity Press.

Wood, D. G. (2017). *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER.*

Buterin, V. (2013). *A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM.*

Blockchain Charts. (2021). Ανάκτηση από blockchain.com: https://www.blockchain.com/charts/

EthereumETH. (2021). Ανάκτηση από https://www.coindesk.com: https://www.coindesk.com/price/ethereum

Kim, K. (2018, June 26). *Modified Merkle Patricia Trie — How Ethereum saves a state.* Ανάκτηση από https://medium.com: https://medium.com/codechain/modified-merkle-patricia-trie-how-ethereum-saves-a-state-e6d7555078dd

Ethereum Charts & Statistics. (2021). Ανάκτηση από https://etherscan.io: https://etherscan.io/charts

How long does an Ethereum transaction really take? (2019, June 5). Ανάκτηση από https://ethgasstation.info: https://ethgasstation.info/blog/ethereum-transaction-how-

long/#:~:text=On%20an%20average%20day%2C%20it,pay%20the%20standard%20gas%20price.

Lewis, A. (2020, October 3). *A gentle introduction to Ethereum.* Ανάκτηση από https://bitsonblocks.net/: https://bitsonblocks.net/2016/10/02/gentle-introduction-ethereum/#:~:text=Ethereum%20has%20smaller%20blocks&text=Currently%20the%20maximum%20block%20size,block%20(1%2C500%2C000%20%2F%2021%2C000).

Longchamp, Y., Deshpande, S., & Mehra, U. (2020, August 27). *Classification and importance of nodes in a blockchain network*. Ανάκτηση από https://www.seba.swiss/: https://www.seba.swiss/research/Classification-and-importance-of-nodes-in-a-blockchain-network

Mark. (2018, November 1). *Full Node and Lightweight Node.* Ανάκτηση από www.mycryptopedia.com: https://www.mycryptopedia.com/full-node-lightweight-node/