ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ ΣΧΟΛΗ
ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ Μ/Υ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ Μ/Υ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ & ΤΕΧΝΟΛΟΓΙΑΣ
ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

Διερεύνηση χρήσης πολυκριτήριας ανάλυσης για την αξιολόγηση κρυπτονομισμάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Κυριάκου Ανέστη
Α.Μ. 03202906

Επιβλέπων : Χάρης Δούκας
Αναπληρωτής Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούνιος 2020

(Υπογραφή)

.....

Κυριάκος Ανέστης

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Τεχνολογίας Η/Υ Πανεπιστημίου Πατρών

Περίληψη

Στόχος της παρούσας εργασίας είναι να γίνει μια συνοπτική παρουσίαση της τεχνολογίας του Blockchain και βασικών εννοιών ορισμένων σημαντικών κρυπτονομισμάτων που θα καταλήξει σε μια πολυδιάστατη πολυκριτηριακή μελέτη. Μέσα από την παραπάνω μελέτη γίνεται μια προσέγγιση του προβλήματος επιλογής του καταλληλότερου, υπό το αυστηρώς ορισμένο πλαίσιο και τα επιλεγμένα από τον αποφασίζοντα κριτήρια.

Στο πρώτο κεφάλαιο της εργασίας γίνεται μια σύντομη αλλά κατά το δυνατόν περιεκτική εισαγωγή στις βασικότερες έννοιες που απαιτούνται για τη μελέτη των κρυπτονομισμάτων και απαντώνται βασικά ερωτήματα όπως τι είναι το blockchain, πως χρησιμοποιείται αυτή η τεχνολογία για τη δημιουργία κρυπτονομισμάτων, ποια τα οφέλη και οι κίνδυνοι από τη χρήση τους κ.α. Το κεφάλαιο κλείνει με την αιτιολόγηση για την επιλογή της πολυκριτηριακής ανάλυσης βασιζόμενοι στα θετικά και τα αρνητικά της.

Στο επόμενο κεφάλαιο γίνεται μια σύντομη αναφορά στα σημαντικότερα χαρακτηριστικά (ιστορικά και τεχνικά) των 7 κρυπτονομισμάτων που θα μας απασχολήσουν στην συνέχεια της εργασίας: του Bitcoin, του Ethereum, του Ripple, του Bitcoin Cash, του Litecoin, του Dash και του Monero. Αναφέρονται επίσης και οικονομικά στοιχεία που δείχνουν την πορεία του νομίσματος από τη στιγμή δημιουργίας του έως και σήμερα.

Ακολουθεί το κεφάλαιο της ανάλυσης όπου περιγράφεται η λογική πίσω από την επιλογή των κριτηρίων αλλά και των εναλλακτικών μέσα από τα εκατοντάδες διαθέσιμα κρυπτονομίσματα. Στην συνέχεια παρατίθενται όλοι οι πίνακες των υπολογισμών για τον ορισμό των απαραίτητων βαρών ενώ στη συνέχεια περιγράφονται οι 3 μέθοδοι που χρησιμοποιήθηκαν για η σύγκριση και κατάταξη των εναλλακτικών μας.

Τέλος σειρά έχουν τα συμπεράσματα της μελέτης όπου γίνεται μια προσπάθεια να ερμηνευτούν τα αποτελέσματα των 3 μεθόδων καθώς και να γίνει μια σύγκριση ανάμεσα τους. Η εργασία κλείνει με τη βιβλιογραφία στην οποία βασιστήκαμε για να συλλέξουμε τα απαραίτητα δεδομένα για την εκπόνηση της εργασίας.

Λέξεις Κλειδιά: Κρυπτονομίσματα, Πολυκριτήρια Ανάλυση, Χρηματοοικονομική Ανάλυση, Αξιολόγηση, Σχέσεις Υπεροχής, Μηχανισμός Συναίνεσης

Abstract

The aim of this thesis is to provide a brief overview of Blockchain technology and key concepts of some important cryptocurrencies that will lead to a multidimensional multicriteria study. Through the above study, an approach is made to the problem of selecting the most appropriate, strictly defined framework and the criteria selected by the decision maker.

The first chapter of the paper provides a brief but comprehensive introduction to the basic concepts required for the study of cryptocurrencies and answers key questions such as what is blockchain, how is this technology used to create cryptocurrencies, what are the benefits and risks from their use etc. The chapter closes with the justification for choosing the multicriteria analysis based on its pros and cons.

The next chapter gives a brief overview of the most important features (historical and technical) of the 7 cryptocurrencies that were selected: Bitcoin, Ethereum, Ripple, Bitcoin Cash, Litecoin, Dash and Monero. There are also financial data that show the course of the currency from its creation until today.

The following chapter is related to the multicriteria analysis which describes the logic behind the selection of the criteria as well as the alternatives through the hundreds of available cryptocurrencies. Next come all the tables of the calculations for the definition of the necessary weights and then the 3 methods used for the comparison and classification of our alternatives are described.

Finally, the conclusions of the study are given, where an attempt is made to interpret the results of the 3 methods as well as to make a comparison between them. The work closes with the bibliography on which we relied to collect the necessary data for the elaboration of our thesis.

Keywords: Cryptocurrency, Blockchain, Bitcoin, Ethereum, Bitcoin Cash, Litecoin, Monero, Dash, Ripple, Multicriteria, MAUT, Electre, Promethee

ΕΥΧΑΡΙΣΤΙΕΣ

Για την εκπόνηση της παρούσας εργασίας θα ήθελα να ευχαριστήσω καταρχάς τον επιβλέποντα καθηγητή κ. Χάρη Δούκα για την άψογη συνεργασία και καθοδήγηση του καθ' όλη τη διαδικασία προετοιμασίας και συγγραφής της. Επιπλέον τους συν διδάσκοντες του μαθήματος «Πολυκριτηριακά Συστήματα Υποστήριξης Αποφάσεων» κυρίους Παναγιώτη Ξυδώνα και Ιωάννη Ψαρά καθώς το συγκεκριμένο μάθημα υπήρξε η αφορμή για την ενασχόληση μου με το θέμα ενώ ταυτόχρονα λειτούργησε και σαν πολύτιμη πηγή πληροφοριών για την εργασία.
Τέλος θα ήθελα να ευχαριστήσω την οικογένεια μου και όλους τους φίλους μου για την υποστήριξη τους κατά τη διάρκεια όλου του προγράμματος σπουδών του μεταπτυχιακού. Ειδική μνεία αξίζει στον Στέλιο και τον Θοδωρή που υπήρξαν καλοί συνεργάτες μου στο σύντομο «ταξίδι» που κάναμε στο κόσμο του mining και του Ethereum.

Πίνακας περιεχομένων

1 Εισαγωγή

1.1 Τι είναι κρυπτονόμισμα

Το κρυπτονόμισμα είναι ένα ψηφιακό περιουσιακό στοιχείο που έχει σχεδιαστεί για να λειτουργεί ως μέσο ανταλλαγής, χρησιμοποιεί ισχυρές μεθόδους κρυπτογραφίας για την εξασφάλιση και επαλήθευση οικονομικών συναλλαγών μεταξύ των μελών ενός δικτύου και χρησιμοποιεί έναν αποκεντρωμένο έλεγχο σε αντίθεση με τα υπόλοιπα νομίσματα τα οποία ελέγχονται από μία κεντρική αρχή. Αυτός ο αποκεντρωμένος έλεγχος κάθε κρυπτονομίσματος λειτουργεί μέσω της κατανεμημένης τεχνολογίας, γνωστή ως Blockchain, που χρησιμεύει ως βάση δεδομένων των οικονομικών συναλλαγών που πραγματοποιούνται. Το πρώτο αποκεντροποιημένο ψηφιακό νόμισμα ήταν το Bitcoin το οποίο κυκλοφόρησε ως λογισμικό ανοιχτού κώδικα το 2009, κατόπιν μετά την κυκλοφορία του έχουν δημιουργηθεί πάνω από 4000 εναλλακτικές παραλλαγές νομισμάτων (altcoins) ορισμένες εκ των οποίων θα αναφερθούν στη συνέχεια σε μια προσπάθεια να γίνουν κατανοητά στον αναγνώστη τα διαφόρων τύπου κρυπτονομίσματα. [3]

1.2 Blockchain Technology

1.2.1 Ορισμός

Η τεχνολογία blockchain είναι ουσιαστικά μια κατανεμημένη βάση δεδομένων, η οποία διατηρεί αμετάβλητη μια καθολική βάση δεδομένων όλων των συναλλαγών που πραγματοποιούνται μεταξύ των μελών ενός δικτύου. Το blockchain επιτρέπει την εγγραφή, με χρονική σειρά, όλων αυτών των συναλλαγών και κάθε μέλος-κόμβος στο δίκτυο είναι υπεύθυνος για τη συντήρηση και τη συνεχή επαλήθευση τους. Αποτελεί δηλαδή μια

χρονολογική βάση δεδομένων των συναλλαγών οι οποίες καταγράφονται από ένα δίκτυο υπολογιστών. Η τεχνολογία blockchain περιλαμβάνει την δημιουργία ψηφιακών νομισμάτων (tokens) για ψηφιακά αρχεία, όπως έγγραφα ή συναλλαγές εκ των οποίων οι ψηφιακές μάρκες μπορούν να θεωρηθούν ως ψηφιακά δακτυλικά αποτυπώματα των αρχείων. Αυτά τα δακτυλικά αποτυπώματα αποθηκεύονται σε ομάδες που ονομάζονται "blocks". Τα μεμονωμένα block συνδέονται έπειτα σε μια αλυσίδα από blocks και κάθε επόμενο block είναι ψηφιακά διακριτό από το προηγούμενο μπλοκ. Αυτό καθίσταται αδύνατη την τροποποίηση των πληροφοριών σε ένα παλιό block στην αλυσίδα προσθέτοντας μόνο νέα μπλοκ. Η κύρια ιδέα πίσω από την τεχνολογία blockchain είναι η εγγραφή, η επικύρωση και η μεταφορά κάθε είδους συμβολαίων και περιουσιακών στοιχείων χωρίς την ανάγκη οποιουδήποτε διαμεσολαβητή. Η πρώτη εμφάνιση του blockchain πραγματοποιήθηκε το 2008 από ένα ανώνυμο άτομο ή ομάδα με το όνομα Satoshi Nakamoto με την δημοσίευση ενός paper με τίτλο «*Bitcoin: A Peer-to-Peer Electronic Cash System*». Το Bitcoin γεννήθηκε όταν ο Satoshi Nakamoto έλυσε ένα σύνθετο πρόβλημα που εξασφάλιζε ότι σε μια συγκεκριμένη χρονική στιγμή θα μπορούσε να μεταφερθεί ένα block περιουσιακών στοιχείων σε ένα μόνο άτομο, χωρίς την ανάγκη ελέγχου από κάποιον τρίτο. Μετά το 2009 εδραιώθηκε η έννοια του κατανεμημένου blockchain ως ένα λογισμικό ανοιχτού κώδικα και ως η βασική τεχνολογία πίσω από το πρώτο ψηφιακό νόμισμα [19].

Εντός του συστήματος του blockchain τόσο το συνάλλαγμα που χρησιμοποιείται όσο και τα στοιχεία που συναλλάσσονται και οι πληροφορίες των συναλλασσόμενων αποκτούν πλέον ψηφιακή μορφή. Η δομή και τα λειτουργικά στοιχεία αυτής της τεχνολογίας αλλάζουν ριζικά τον τρόπο πραγματοποίησης των συναλλαγών. Πλέον δεν υπάρχει η ανάγκη για ενδιάμεσους φορείς, ενισχύεται η διαφάνεια, ενώ παράλληλα μειώνεται δραστικά το κόστος και ο χρόνος διεκπεραίωσης των διαδικασιών, και αντίστοιχα ο κίνδυνος μη ολοκλήρωσης τους.

Το blockchain έχει δημιουργήσει νέες δυνατότητες εφαρμόζοντας την ήδη υπάρχουσα τεχνολογία, για να λειτουργήσει ορθά ένα σύστημα όπως αυτό του ηλεκτρονικού χρήματος, χωρίς εποπτεία από κεντρικές αρχές, θα πρέπει να θεσπιστούν μέτρα για την ασφάλεια και την πρόληψη των συναλλαγών του δικτύου από πλαστογράφηση δεδομένων, αλλοίωση πληροφοριών σχετικά με τις πληρωμές και επιθέσεις από κακόβουλους χρήστες. Για να συμβεί αυτό έχουν ενσωματωθεί στο blockchain σημαντικές τεχνολογίες για την εύρυθμη λειτουργία του (*peer-to-peer network, hash algorithms, proof-of-work και proof-of-stake*). [1]

1.2.2 Σημαντικές ορολογίες

Hash Algorithm

Η τεχνολογία Blockchain βασίζεται ως επί το πλείστο σε hash συναρτήσεις. Μία hash συνάρτηση είναι ένας μαθηματικός αλγόριθμος που έχει σαν είσοδο τυχαία δεδομένα τα οποία μετατρέπει σε μια αντίστοιχη έξοδο. Το κύριο χαρακτηριστικό γνώρισμα της είναι η εξαιρετικά δύσκολη αναδημιουργία των δεδομένων εισόδου από την έξοδο της μόνο. Ο μηχανισμός αυτός χαρακτηρίζεται από το γεγονός ότι λαμβάνεται η ίδια τιμή εξόδου από τα ίδια δεδομένα εισόδου και έστω και η παραμικρή διαφορά στα αρχικά δεδομένα θα οδηγήσουν σε εντελώς διαφορετική τιμή εξόδου. Αξιοποιώντας τα χαρακτηριστικά αυτά η συνάρτηση hash χρησιμοποιείται για την ανίχνευση παραποίησης δεδομένων.

Ορισμένες από τις βασικότερες ιδιότητες επομένως των hash functions είναι οι εξής:

- Το αποτέλεσμα που θα παράγει η ίδια είσοδος, θα πρέπει να είναι πάντα ίδιο.
- Για κάποιο χρήστη, θα πρέπει να είναι υπολογιστικά αδύνατο να επιστρέψει στα δεδομένα της εισόδου από την έξοδο του αλγόριθμου.
- Τα αποτελέσματα της εξόδου θα δέχονται μεγάλες αλλαγές από κάποιες μικρές αλλαγές στα δεδομένα εισόδου.

Το χαρακτηριστικότερο παράδειγμα αποτελεί το πρωτόκολλο του Bitcoin που χρησιμοποιεί τον αλγόριθμο SHA256^2, δηλαδή γίνεται διπλή χρήση του αλγορίθμου SHA 256. Η οικογένεια αλγορίθμων SHA-2, στην οποία ανήκει και ο SHA 256, έχει σχεδιαστεί από την NSA (National Security Agency – US Government) και το 2001 δημοσιοποιήθηκαν από το NIST (National Institute of Standards and Technology). Η ονομασία προέκυψε από την έξοδο του αλγορίθμου που είναι μεγέθους 256 bits. Οι αλγόριθμοι κρυπτογράφησης βασίζονται στις δυνατότητες των υπολογιστικών συστημάτων που υπάρχουν σήμερα, θεωρούνται αποτελεσματικοί και η λειτουργία τους δεν μπορεί να αντιγραφεί. Στο προσεχές μέλλον, λόγω της αύξησης των δυνατοτήτων των υπολογιστικών συστημάτων, πιθανότατα θα πρέπει να αναθεωρηθεί η σχεδίαση των αλγορίθμων κρυπτογράφησης διότι, αντίθετα δεν θα μπορούν να επιτελέσουν αποδοτικά το έργο του λόγω της χαμηλής πολυπλοκότητάς τους [6].

Nodes

Οι κόμβοι είναι το βασικότερο στοιχείο του δικτύου των blockchain εφαρμογών, καθώς διασφαλίζουν τη λειτουργία και την επιβίωσή του. Ένας κόμβος μπορεί να είναι οποιαδήποτε ενεργή ηλεκτρονική συσκευή, συμπεριλαμβανομένου ενός υπολογιστή, ενός τηλεφώνου ή ακόμα και ενός εκτυπωτή, εφόσον είναι συνδεδεμένη στο διαδίκτυο και ως εκ τούτου έχει διεύθυνση δικτύου (public IP address). Ο ρόλος ενός κόμβου είναι να υποστηρίζει το δίκτυο διατηρώντας ένα αντίγραφο της αλυσίδας blockchain και, σε ορισμένες περιπτώσεις, να επεξεργάζεται τις συναλλαγές. Κάθε κρυπτονόμισμα έχει τους δικούς του κόμβους οι οποίοι ως επιμέρους τμήματα του blockchain συνεισφέρουν τους υπολογιστικούς τους πόρους για την αποθήκευση και την επικύρωση των συναλλαγών τους. Η επεξεργασία αυτών των συναλλαγών τις περισσότερες φορές απαιτεί μεγάλες ποσότητες υπολογιστικής και επεξεργαστικής ισχύος.

Transactions

Τα transactions είναι πακέτα δεδομένων τα οποία αποθηκεύουν πληροφορίες, όπως για παράδειγμα νομισματικές πληροφορίες για κρυπτονομίσματα ή για άλλες αποκεντρωμένες εφαρμογές. Η ακεραιότητα ενός transaction ελέγχεται από αλγοριθμικούς κανόνες και κρυπτογραφικές τεχνικές. Ένα transaction αποστέλλεται σε έναν κόμβο που είναι συνδεδεμένος με το blockchain δίκτυο και έπειτα επικυρώνεται και προωθείται σε άλλους κόμβους του δικτύου. Επίσης, οι κόμβοι επικυρώνουν και προωθούν το transaction στους δικούς τους peers μέχρι αυτό να φτάσει στο σύνολο τον κόμβων του δικτύου.

Mining

Ο όρος mining αντιστοιχεί στη διαδικασία της πιστοποίησης των συναλλαγών και προσθήκης νέων μπλοκ συναλλαγών στη blockchain. Παράλληλα, είναι και ο μηχανισμός εισόδου νέων νομισμάτων στο δίκτυο. Η διαδικασία του mining δεν υλοποιείται σε όλα τα κρυπτονομίσματα (υπάρχουν και κρυπτονομίσματα που δεν γίνονται mine) καθώς επίσης, δεν έχει ούτε τα ίδια χαρακτηριστικά σε κάθε κρυπτονόμισμα που υλοποιεί mining. Κεντρικό και καθοριστικό ρόλο στη διαδικασία του mining αναλαμβάνουν συγκεκριμένοι κόμβοι, ο οποίοι

ονομάζονται miners. Το δίκτυο κάθε κρυπτονομίσματος παρέχει κίνητρο για τη συμμετοχή περισσότερων miner με τη μορφή ανταμοιβής (reward) για τις πολύτιμες υπηρεσίες τους. Η ανταμοιβή αυτή μεταφράζεται σε μέρος των νομισμάτων που γίνονται mining.

Πρακτικά όταν πραγματοποιείται μία συναλλαγή μεταξύ δύο μελών ενός δικτύου Blockchain αυτή θα πρέπει να επικυρωθεί από τα υπόλοιπα μέλη του δικτύου. Η συναλλαγή αυτή καταγράφεται σε ένα block και σφραγίζεται μέσω της μίας hash συνάρτησης και θα κατοχυρωθεί όταν επικυρωθεί από το δίκτυο. Η συνάρτηση hash παράγει μια καθορισμένη σειρά δεδομένων από μια αυθαίρετη είσοδο την οποία γνωρίζει μόνο ο κόμβος που πραγματοποιεί την συναλλαγή ενώ στην συνέχεια οι υπόλοιποι κόμβοι του Blockchain θα πρέπει μέσω πολύπλοκων μαθηματικών αλγορίθμων να επιλύσουν το αρχικό πρόβλημα της συνάρτησης hash. Ο πρώτος κόμβος που θα επιλύσει πρώτος το πρόβλημα θα επικυρώσει την συναλλαγή και το συγκεκριμένο block θα προστεθεί στην υπόλοιπη αλυσίδα προηγούμενων block δημιουργώντας μία αλυσίδα. Ως ανταμοιβή για την εργασία το σύστημα παράγει ένα νέο νόμισμα το οποίο το λαμβάνει ο κόμβος που έκανε και την επικύρωση. Το κάθε νέο νόμισμα περιλαμβάνει το ψηφιακό αποτύπωμα των προηγούμενων νομισμάτων αυτό συμβαίνει ώστε να αποφευχθεί οποιαδήποτε αλλοίωση στα block των συναλλαγών.

Το τρέχον hash rate μόνο για τη περίπτωση του Bitcoin mining ανέρχεται σε περίπου 120000000 TH/s. Αναλογιζόμαστε το μέγεθος της υπολογιστικής ισχύος, η οποία έχει συσσωρευτεί στα δίκτυα, αν προσθέσουμε τις περιπτώσεις όλων των κρυπτονομισμάτων (αν και το bitcoin είναι με μεγάλη διαφορά ο μεγαλύτερος mining crypto παίχτης στην αγορά). Βέβαια, οι ρυθμοί προέκυψαν εν μέσω της ραγδαίας ανάπτυξης του εξοπλισμού για τη διαδικασία του mining, αλλά και της προσέλκυσης πολλών νέων χρηστών. Υπάρχουν 4 βασικές τεχνολογίες hardware που χρησιμοποιούνται στο mining ανά περίπτωση:

i. CPU: αποτελούν τη κλασσική κεντρική μονάδα επεξεργασίας (Central Processing Unit), η οποία είναι ενσωματωμένη σε υπολογιστές και άλλες συσκευές. Κατά την κυκλοφορία του Bitcoin, το mining υλοποιούνταν αποκλειστικά από CPUs. Καθώς ήταν και το μόνο κρυπτονόμισμα σε λειτουργία μέχρι τότε.

ii. GPU: αποτελούν τη μονάδα επεξεργασίας γραφικών (Graphics Processing Unit). Η δομή τους και η δυνατότητα γρήγορης προσπέλασης δεδομένων λόγω παράλληλης εκτέλεσης, οδηγεί στο να πάρουν προβάδισμα σε σχέση με τα CPUs κυρίως όσον αφορά συγκεκριμένα νομίσματα (Ethereum).

iii. FPGAs: αποτελούν ειδικά σχεδιασμένο υλικό, που εστιάζει στην εκτέλεση μίας συγκεκριμένης εργασίας. Ανταγωνίζονται σε hash rate τα GPUs ενώ ταυτόχρονα καταναλώνουν αρκετά λιγότερη ενέργεια.

iv. ASICs: αποτελούν ειδικά σχεδιασμένο υλικό για τη διαδικασία του mining. Σχεδιάζεται με τέτοιο τρόπο, ώστε να παράγουν το μέγιστο δυνατό πλήθος από hashes μέσω παράλληλης εκτέλεσης hash function. Είναι ο μόνος τρόπος πλέον για να μπορέσει ένας χρήστης να υλοποιήσει επιτυχές bitcoin mining.

Όσοι χρήστες διαθέτουν τον αντίστοιχο εξοπλισμό έχουν τη δυνατότητα να υλοποιήσουν από μόνοι του mining κάτι που ορίζεται ως solo mining**.** Ωστόσο, λόγω της συσσώρευσης τεράστιας υπολογιστικής ισχύος μέσα στο δίκτυο παγκοσμίως και συνεχούς ανανέωσης της τεχνολογίας, το mining γίνεται οικονομικά ασύμφορο για μεμονωμένους χρήστες. Για αυτό το λόγο, εμφανίστηκε το pool mining**.** Στη περίπτωση αυτή μια ομάδα από miners συνεισφέρουν την υπολογιστική τους δύναμη στο pool, με σκοπό να μοιραστούν τα rewards, που θα αποφέρει η διαδικασία. Η κατανομή του reward σε κάθε χρήστη στο pool mining είναι ανάλογη της συνεισφοράς της υπολογιστικής δύναμης στο pool. Παράλληλα,

κάθε χρήστης για τη συμμετοχή του στο pool, είναι υποχρεωμένος να καταβάλλει ένα μικρό ποσοστό των κερδών στο διαχειριστή ως έξοδα λειτουργίας και χρήσης.

Ωστόσο λόγω της προαναφερθείσας αύξησης της πολυπλοκότητας του mining οι χρήστες χρησιμοποιούν όλο και πιο ισχυρό εξοπλισμό πληροφορικής με αποτέλεσμα να έχει δημιουργηθεί μεγάλος ανταγωνισμός σχετικά με τον εξοπλισμό. Για παράδειγμα, η εξόρυξη αρχικά πραγματοποιούταν από την CPU ωστόσο, οι ίδιες λειτουργίες θα μπορούσαν να εκτελούνται και από τη GPU με πολύ ταχύτερο ρυθμό. Οι GPUs, στη συνέχεια, έδωσαν τη θέση τους στην εφαρμογή ολοκληρωμένων κυκλωμάτων ειδικού σκοπού (ASIC), με σκοπό το mining κρυπτονομισμάτων σε ταχύτητες πολύ υψηλότερες από ό, τι θα μπορούσαν μέσω GPUs ή CPUs. Ο αλγόριθμος SHA-256 που χρησιμοποιείται στο δίκτυο Bitcoin και διάφορα εναλλακτικά κρυπτονομίσματα δεν μπορεί να ανταποκριθεί στις εναλλαγές εξοπλισμού, και πολλά νομίσματα έχουν εισαγάγει εναλλακτικούς αλγορίθμους κατακερματισμού που συχνά έχουν ως πλεονέκτημα την ανθεκτικότητα σε ASIC (με χαρακτηριστικότερο παράδειγμα το Ethereum). [19]

1.2.3 Σημαντικοί Hash Algorithms

SHA-2

Ο SHA-2 (Secure Hash Algorithm 2) είναι ένα σύνολο hash algorithms που σχεδιάστηκε από την NSA. Ο εν λόγω αλγόριθμος κρυπτογράφησης χρησιμοποιεί μαθηματικές πράξεις που εκτελούνται σε ψηφιακά δεδομένα. Με τη σύγκριση της υπολογιζόμενης "hash" (η έξοδος από την εκτέλεση του αλγορίθμου) με μια γνωστή και αναμενόμενη τιμή hash, ένα άτομο μπορεί να προσδιορίσει την ακεραιότητα των δεδομένων. Για παράδειγμα, υπολογίζοντας το hash του αρχείου λήψης και συγκρίνοντας το αποτέλεσμα το οποίο έχει ήδη δημοσιευθεί με το αποτέλεσμα hash μπορεί να δείξει αν η λήψη έχει τροποποιηθεί ή παραποιηθεί. Μια βασική πτυχή γενικά των κρυπτογραφικών hash λειτουργιών είναι η αρχή της ντετερμινιστικότητας: κανείς δεν πρέπει να μπορεί να βρει δύο διαφορετικές τιμές εισόδου που έχουν ως αποτέλεσμα την ίδια έξοδο hash.

Ο SHA-2 περιλαμβάνει σημαντικές αλλαγές από τον προκάτοχό του τον SHA-1. Η οικογένεια SHA-2 αποτελείται από έξι hash λειτουργίες με digests (τιμές hash) που είναι 224, 256, 384 ή 512 bits. Αντίστοιχα προκύπτουν οι παραλλαγές του αλγορίθμου SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 και SHA -512/256. Οι SHA-256 και SHA-512 είναι νέες λειτουργίες hash που υπολογίζονται με λέξεις 32-bit και 64-bit, αντίστοιχα. Χρησιμοποιούν διαφορετικά ποσά μετατόπισης και πρόσθετες σταθερές, αλλά οι δομές τους είναι σχεδόν ταυτόσημες με άλλο τρόπο, που διαφέρουν μόνο στον αριθμό των γύρων. Οι SHA-224 και SHA-384 είναι απλά αποκομμένες εκδοχές των δύο πρώτων που υπολογίζονται με διαφορετικές αρχικές τιμές. Οι SHA-512/224 και SHA-512/256 είναι επίσης αποκομμένες εκδοχές του SHA-512, αλλά οι αρχικές τιμές παράγονται χρησιμοποιώντας τη μέθοδο που περιγράφεται στο FIPS PUB 180-4.

Ο SHA-2 δημοσιεύθηκε το 2001 από το NIST (National Institute of Standards & Technology of the USA) ως ένα ομοσπονδιακό πρότυπο των ΗΠΑ (FIPS). Η οικογένεια των αλγορίθμων SHA-2 είναι κατοχυρωμένη με δίπλωμα ευρεσιτεχνίας στις ΗΠΑ. Με τη δημοσίευση του FIPS PUB 180 - 2, το NIST προσθέτει τρεις λειτουργίες κατακερματισμού στην οικογένεια SHA. Οι αλγόριθμοι είναι γνωστοί συλλογικά ως SHA-2, όνομα που βασίζεται τα μήκη τους (σε bits): SHA-256, SHA-384 και SHA-512. Το 2002, το FIPS PUB

180 - 2 έγινε το νέο Secure Hash πρότυπο, αντικαθιστώντας το FIPS PUB 180-1, το οποίο κυκλοφόρησε τον Απρίλιο του 1995. Το επικαιροποιημένο πρότυπο περιλαμβάνεται στον αρχικό SHA-1 αλγόριθμο, με σύγχρονες τεχνικές σημειογραφίας σύμφωνες με αυτές που περιγράφει η εσωτερική λειτουργία της οικογένειας SHA-2. [8]

Ethash

Ο αλγόριθμος αυτός είναι πίσω από το δεύτερο παγκοσμίως σε κυκλοφορία (circulation) κρυπτονομίσματος, δηλαδή του Ethereum, και αποτελεί μία τροποποιημένη έκδοση του αλγορίθμου Dagger Hashimoto. Οι miners παράγουν νέα μπλοκ και το υπόλοιπο δίκτυο ελέγχει την εγκυρότητά τους. Ένα μπλοκ θεωρείται έγκυρο, αν και μόνο αν, ικανοποιεί τα κριτήρια του proof of work (βλέπε παρακάτω) για μία δεδομένη τιμή δυσκολίας. Το Ethash σκοπεύει να περάσει σε ένα νέο στάδιο και να αξιοποιήσει ένα νέο αλγόριθμο για το mining. Ο αλγόριθμος αυτός ονομάζεται Casper και ανήκει στην ομάδα των proof-of-stake (βλέπε παρακάτω). Σε γενικές γραμμές η τιμή πολυπλοκότητας για τον αλγόριθμο Ethash προσαρμόζεται δυναμικά, έτσι ώστε να παράγεται ένα νέο μπλοκ κάθε 12 δευτερόλεπτα. Επομένως, το block time για του ethereum επιδιώκεται να διατηρείται στα 12 λεπτά.

Ο Ethash ακολουθεί την εξής λογική:

- Επιλέγει μία σειρά από τυχαία δεδομένα, τα οποία βρίσκονται αποθηκευμένα σε ένα μεγάλο dataset (με το όνομα DAG).
- Επιλέγει τυχαία ορισμένες συναλλαγές από οποιοδήποτε μπλοκ.
- Τα 2 παραπάνω δεδομένα αποτελούν είσοδο για τη κρυπτογραφική συνάρτηση Keccak-256, η οποία παράγει ένα hash value.
- Το παραγόμενο hash value για να είναι έγκυρο(και άρα να είναι νικητής και ο αντίστοιχος miner), χρειάζεται να βρίσκεται κάτω από όριο που ορίζει τη πολυπλοκότητα της διαδικασίας.
- Ο πρώτος miner, ο οποίος καταφέρνει να βρει ένα "έγκυρο" hash value, είναι και αυτός που λαμβάνει το transaction reward και τα υπόλοιπα τέλη της συναλλαγής.

Η παραπάνω διαδικασία απαιτεί την αποθήκευση ολόκληρου του DAG αρχείου, ώστε να είναι σε θέση κάθε φορά ο miner να επιλέγει τυχαία δεδομένα από αυτό. Αυτό σημαίνει πως το υπολογιστικό πρόβλημα το οποίο επιλύεται στον Ethash δεν απαιτεί μεγάλη υπολογιστική ταχύτητα άρα και υπολογιστική ισχύ. Αντίθετα εξαρτάται την απαιτούμενη ποσότητα μνήμης, η οποία χρησιμοποιείται για την αποθήκευση και ανάκτηση των δεδομένων. Ο αλγόριθμος Ethash, δηλαδή, θεωρείται memory-oriented hash protocol. Βασιζόμενοι στα παραπάνω είναι εύκολο να αντιληφθούμε γιατί ο συγκεκριμένος αλγόριθμος αποδίδει πολύ καλύτερα με τη χρήση GPU αντί για CPU, η καθεμία εκ των οποίων διαθέτει τη δική της dedicated μνήμη για πολύπλοκες και ταχύτατες υπολογιστικές πράξεις. [11]

Scrypt

Ο αλγόριθμος Scrypt είναι μια λειτουργία προέλευσης κλειδιών που βασίζεται σε κωδικό πρόσβασης (passwords). Σχεδιάστηκε ειδικά για να καταστήσει δαπανηρές τις επιθέσεις μεγάλης κλίμακας σε υλικό υπολογιστών που απαιτούν μεγάλες ποσότητες μνήμης. Το 2012, ο αλγόριθμος Scrypt δόθηκε στη δημοσιότητα από το IETF (Internet Engineering Task Force) και προορίζεται να γίνει ο διάδοχος του RFC (Request for Comments). Μια απλοποιημένη εκδοχή του Scrypt χρησιμοποιείται ως αλγόριθμος κρυπτογράφησης σε μια σειρά από κρυπτονομίσματα, με διασημότερο όλων το Litecoin. Μια λειτουργία προέλευσης κλειδιών που βασίζεται σε κωδικό πρόσβασης (με βάση τον κωδικό KDF) έχει σχεδιαστεί για

να είναι υπολογιστικά πολύπλοκη, ώστε να απαιτείται ένα σχετικά μεγάλο χρονικό διάστημα για να υπολογιστεί (ας πούμε της τάξης μερικών εκατοντάδων χιλιοστών του δευτερολέπτου). Εξουσιοδοτημένοι χρήστες οφείλουν να εκτελέσουν τη συνάρτηση μόνο μία φορά ανά λειτουργία (π.χ. έλεγχος ταυτότητας), και έτσι ο χρόνος που απαιτείται είναι αμελητέος. Ωστόσο, μια επίθεση θα ήταν πιθανόν να χρειαστεί να εκτελεστεί η λειτουργία δισεκατομμύρια φορές, οπότε οι απαιτήσεις χρόνου γίνονται ουσιαστικά απαγορευτικές.

Προηγούμενες λειτουργίες που βασίζονται αντίστοιχα σε κωδικό πρόσβασης KDFs (όπως το δημοφιλές PBKDF2) έχουν σχετικά χαμηλές απαιτήσεις πόρων, που σημαίνει ότι δεν χρειάζονται ισχυρό hardware ή πολύ μνήμη για να εκτελεστούν. Είναι, συνεπώς, εύκολο και φτηνό να υλοποιηθούν από άποψη υλικού σε ένα ASIC ή ακόμα και ένα FPGA. Αυτό επιτρέπει σε έναν επίδοξο εισβολέα με επαρκείς πόρους να ξεκινήσει μια μεγάλης κλίμακας επίθεση παράλληλα με την υλοποίηση εκατοντάδων ή ακόμα και χιλιάδων εφαρμογών του αλγορίθμου. Επομένως διαχωρίζεται το ποσό του χρόνου που απαιτείται για να ολοκληρωθεί μια επίθεση από τον αριθμό των διαθέσιμων εφαρμογών, με μεγάλη πιθανότητα να υλοποιηθούν σε ένα εύλογο χρονικό διάστημα.

Η λειτουργία Scrypt έχει σχεδιαστεί για να εμποδίσει τέτοιες προσπάθειες, αυξάνοντας τις απαιτήσεις των πόρων του αλγορίθμου. Συγκεκριμένα, ο αλγόριθμος έχει σχεδιαστεί για να χρησιμοποιεί πολύ μεγαλύτερους πόρους μνήμης σε σύγκριση με άλλα KDFs, καθιστώντας το μέγεθος και το κόστος του hardware πολύ πιο ακριβό. Οι μεγάλες απαιτήσεις σε μνήμη του Scrypt προέρχονται από ένα μεγάλο διάνυσμα των χορδών ψευδοτυχαίων bit που παράγονται ως μέρος του αλγόριθμου. Μόλις παράγεται ο φορέας, τα στοιχεία είναι προσβάσιμα σε μία ψευδό-τυχαία σειρά και συνδυάζονται για να παράγουν το αντίστοιχο κλειδί. Μία απλή εφαρμογή θα πρέπει να δεσμεύει το σύνολο του φορέα σε μνήμη RAM, έτσι ώστε να μπορεί να έχει πρόσβαση, όπως απαιτείται.

Επειδή τα στοιχεία του διανύσματος παράγονται αλγοριθμικά, κάθε στοιχείο θα μπορούσε να παραχθεί ταυτόχρονα με την κανονική λειτουργία, με την αποθήκευση μόνο ενός στοιχείου μνήμης κάθε φορά και ως εκ τούτου τη μείωση των απαιτήσεων μνήμης. Εντούτοις, η παραγωγή του κάθε στοιχείου προορίζεται να είναι υπολογιστικά δαπανηρή, και τα στοιχεία αναμένεται να προσπελαστούν πολλές φορές καθ' όλη την εκτέλεση της λειτουργίας. Έτσι, υπάρχει ένα σημαντικό κόστος στην ταχύτητα, ώστε να απαλλαγούμε από τις μεγάλες απαιτήσεις σε μνήμη.

Αυτό το είδος του κόστους χρόνου-μνήμης υπάρχει συχνά σε αντίστοιχους υπολογιστικούς αλγορίθμους: μπορείτε να αυξήσετε την ταχύτητα με το κόστος χρήσης περισσότερης μνήμης, ή να μειώσετε τις απαιτήσεις σε μνήμη με το κόστος της μείωσης της ταχύτητας. Η ιδέα πίσω από το scrypt είναι να κάνει σκόπιμα αυτό το trade-off δαπανηρό προς κάθε κατεύθυνση. Έτσι, ένας εισβολέας θα μπορούσε να χρησιμοποιήσει μια εφαρμογή που δεν απαιτεί πολλούς πόρους, αλλά τρέχει πολύ αργά, ή να χρησιμοποιήσει μια εφαρμογή που τρέχει πιο γρήγορα, αλλά έχει πολύ μεγάλες απαιτήσεις σε μνήμη και, επομένως, είναι πιο ακριβή στην παραλληλοποίηση. [14]

CryptoNight

Ο αλγόριθμος CryptoNight είναι σχεδιασμένος για να εκτελείται καλυτέρα σε απλούς επεξεργαστές υπολογιστών, αλλά προς το παρόν δεν υπάρχουν συσκευές ειδικού σκοπού (ASIC) για το mining. Ως εκ τούτου, τα νομίσματα που χρησιμοποιούν CryptoNight μπορούν να εξορύσσονται μόνο μέσω της CPU προς το παρόν. Ο CryptoNight βασίζεται στη τυχαία πρόσβαση στην «αργή» μνήμη και δίνει έμφαση στη λανθάνουσα κατάσταση εξάρτησης. Κάθε νέο μπλοκ εξαρτάται από όλα τα προηγούμενα μπλοκ (σε αντίθεση, για παράδειγμα, με τον Scrypt).

Ο αλγόριθμος απαιτεί περίπου 2 Mb ανά περίπτωση επομένως υλοποιείται στη μνήμη cache L3 (ανά πυρήνα) των σύγχρονων επεξεργαστών. Ένα MB εσωτερικής μνήμης είναι μη αποδεκτό από τις σύγχρονες ASICs ενώ αντίθετα οι GPUs μπορούν να εκτελέσουν εκατοντάδες ταυτόχρονων περιπτώσεων, αλλά περιορίζονται με άλλους τρόπους. Η μνήμη GDDR5 είναι πιο αργή από την cache L3 της CPU και αξιοσημείωτη για το εύρος ζώνης της, και τη μη τυχαία ταχύτητα πρόσβασης. Σημαντική επέκταση θα απαιτούσε αύξηση των επαναλήψεων, η οποία με τη σειρά της συνεπάγεται μια συνολική αύξηση του χρόνου. "Βαριές" κλήσεις σε ένα δίκτυο peer2peer μπορεί να οδηγήσουν σε σοβαρές αδυναμίες, επειδή οι κόμβοι είναι υποχρεωμένοι να ελέγχουν τα διαπιστευτήρια κάθε νέου μπλοκ. Αν ένας κόμβος ξοδεύει σημαντική ποσότητα χρόνου στην αξιολόγηση κάθε hash, μπορεί εύκολα να γίνει στόχος επίθεσης DDoS από μια πληθώρα πλαστών αντικειμένων με αυθαίρετα δεδομένα έργου (τιμές nonce). [16]

ECDSA

Στην κρυπτογραφία, ο αλγόριθμος ελλειπτικής καμπύλης ψηφιακής υπογραφής (ECDSA) αποτελεί μια παραλλαγή του αλγορίθμου ψηφιακής υπογραφής (DSA) που χρησιμοποιεί κρυπτογραφία ελλειπτικών καμπυλών. Όπως και με τη κρυπτογραφία ελλειπτικής καμπύλης γενικά, το μέγεθος bit του δημόσιου κλειδιού που θεωρείται ότι είναι αναγκαίο για τον ECDSA είναι περίπου δύο φορές το μέγεθος του επιπέδου ασφάλειας σε bits. Για παράδειγμα, σε ένα επίπεδο ασφάλειας των 80 bits (δηλαδή όταν ο εισβολέας πρέπει ισοδύναμα να εκτελέσει περίπου 2^{80} ενέργειες για να βρει το ιδιωτικό κλειδί) το μέγεθος ενός δημόσιου κλειδιού DSA είναι τουλάχιστον 1024 bits, ενώ το μέγεθος ενός δημόσιου κλειδιού ECDSA θα είναι 160 bits. Από την άλλη πλευρά, το μέγεθος της υπογραφής είναι το ίδιο τόσο για τον DSA, όσο και για τον ECDSA: 4t bits, όπου t είναι το επίπεδο ασφάλειας που μετριέται σε bits, δηλαδή, περίπου 320 bits για ένα επίπεδο ασφάλειας των 80 bits. [12]

Αλγόριθμοι X11

Αυτοί οι νέοι και κερδοφόροι αλγόριθμοι είναι πολύ δημοφιλείς από το 2014 στην εξόρυξη με χρήση GPU. Έχουν δημιουργηθεί ειδικά για GPU και είναι σε θέση να παρέχουν μια καλή κερδοφορία στην κοινότητα μετά την άνοδο των μεγάλων ASICs οι οποίοι είναι επικεντρωμένοι σε πιο ευάλωτους αλγορίθμους. Η φιλοσοφία τους βασίζεται στην αρχή ότι κάθε αποτέλεσμα από έναν υπό-αλγόριθμο στην συνέχεια περνάει στον επόμενο υπό-αλγόριθμο. Η δημιουργία ASIC, αφιερωμένου για αυτή την οικογένεια αλγορίθμων δυσχεραίνει από το γεγονός ότι το υλικό θα πρέπει να έχει λογικές πύλες για κάθε αλγόριθμο σε ολόκληρο το τσιπ, αυξάνοντας έτσι δραστικά τη πολυπλοκότητα της κατασκευής. Από την άλλη πλευρά, οι αλγόριθμοι X11-X15 χρησιμοποιούν μόνο 536MB RAM (περίπου), και αυτό μπορεί να αποσβέσει ένα μέρος του κόστους των λογικών πυλών.

Ο X11 είναι το όνομα μιας αλυσίδας αλγόριθμου κατακερματισμού βασισμένο στην PoW (Proof of Work) αρχιτεκτονική. Είναι γνωστός και ως αλυσιδωτός αλγόριθμος επειδή χρησιμοποιεί 11 διαφορετικούς αλγορίθμους που είναι συνδεδεμένοι μεταξύ τους (Blake, BMW, Groestl, JH, Keccak, Skein, Luffa, Cubehash, Shavite, Simd, Echo). Το πρώτο κρυπτονόμισμα που χρησιμοποίησε τον X11 ήταν το Darkcoin, που από τότε έχει αλλάξει το όνομα του σε Dash.

Ο X11 αναπτύχθηκε προκειμένου να ξεπεραστούν κάποια σημαντικά μειονεκτήματα που συνδέονται με τους ήδη χρησιμοποιούμενους αλγορίθμους κατακερματισμού όπως ο SHA-256 (Bitcoin) ή ο Scrypt (Litecoin, Dogecoin). Το μεγαλύτερο από αυτά τα μειονεκτήματα ήταν το γεγονός ότι οι εταιρείες ηλεκτρονικών ειδών είχαν ήδη αναπτύξει ειδικό υλικό (ASIC), για το mining όπου χρησιμοποιούνται οι δημοφιλέστεροι αλγόριθμοι

εξόρυξης (π.χ. SHA-256). Αυτό είχε ως αποτέλεσμα να καταστήσει τα δίκτυα πιο συγκεντρωτικά – να ελέγχονται δηλαδή από μια μικρή ομάδα ισχυρών miners, ενώ το αρχικό όραμα των δικτύων κρυπτονομισμάτων ήταν διαφορετικό. Στόχος ήταν αρχικά, οι απλοί χρήστες να μπορούν να πάρουν μέρος στην ενίσχυση της ασφάλειας του δικτύου και να κερδίζουν ανταμοιβές μέσω της εξόρυξης. Ο συγκεντρωτισμός της εξόρυξης μειώνει την ασφάλεια του δικτύου, μειώνει τον αριθμό των ανθρώπων που συμμετέχει στη λειτουργία του δικτύου και μπορεί να αυξήσει την πιθανότητα τα κρυπτονομίσματα που εξορύσσονται να υφίστανται άμεσο dumping. Επιπρόσθετα η χρήση των 11 διαφορετικών αλγορίθμων αυξάνει την ασφάλεια των νομισμάτων. Οι επιθέσεις εναντίον νομισμάτων, όπως το Bitcoin, τα οποία χρησιμοποιούν άλλους αλγόριθμους δεν είναι δυνατή, αλλά μπορεί ενδεχομένως να είναι δυνατή σε κάποιο σημείο στο μέλλον. Ένα άλλο πρόσθετο όφελος αυτού του αλγορίθμου σε σύγκριση με τον αλγόριθμο SHA-256 και τον αλγόριθμο Ethash είναι το γεγονός ότι είναι λιγότερο έντονος και ως εκ τούτου λιγότερο ενεργοβόρος. Οι υπολογιστές που εκτελούν άλλους αλγόριθμους τείνουν να αυξάνουν τη θερμοκρασία του και να χρησιμοποιούν πολλή ηλεκτρική ενέργεια. Για παράδειγμα, μια κάρτα γραφικών που τρέχει τον αλγόριθμο Scrypt θα παράγει 30% περισσότερη θερμότητα από την ίδια κάρτα που εκτελεί τον αλγόριθμο X11 - και αυτή η υπερβολική θερμότητα μειώνει την διάρκεια ζωής του υλικού και υποβαθμίζει τη συνολική απόδοση. [17]

1.2.4 Μηχανισμοί εξασφάλισης συναίνεσης

Ίσως το μεγαλύτερο τεχνολογικό επίτευγμα του Bitcoin (και η εκ των ων ουκ άνευ για κάθε κρυπτονόμισμα) είναι η κατασκευή ενός συστήματος συναλλαγών peer-to- peer που στηρίζεται στην κρυπτογραφική απόδειξη αντί για την εμπιστοσύνη. Ωστόσο, αντικαθιστώντας μια κεντρική αρχή, παρουσιάζεται ένα σοβαρό πρόβλημα: το νόμισμα θα πρέπει να είναι σε θέση να αλλάζει κατόχους. Οι συναλλαγές καταγράφονται με το συνδυασμό των ψηφιακών υπογραφών από κάθε μέλος και μία χρονοσήμανση (timestamp), έτσι ώστε η ημερομηνία της συναλλαγής να καταγράφεται. Ο νέος αυτός κώδικας αντιπροσωπεύει το νόμισμα και τη διαδρομή του μέσω του δικτύου. Αυτός ο κώδικας στη συνέχεια μεταδίδεται σε όλους τους κόμβους του δικτύου δηλαδή τους υπολογιστές που είναι συνδεδεμένοι και τρέχουν το λογισμικό του δικτύου των κρυπτονομισμάτων. Ωστόσο, είναι απαραίτητο η πλειοψηφία των κόμβων να συμφωνήσουν σχετικά με τις συναλλαγές που έχουν συμβεί, αλλιώς μπορεί να προκύψουν διπλές δαπάνες και denial-of-service (DoS). Ο μηχανισμός που χρησιμοποιείται για την επίτευξη συναίνεσης μεταξύ των κόμβων ενισχύει την ακεραιότητα του συστήματος επαληθεύοντας ότι η συναλλαγή είναι πράγματι νόμιμη. Ως εκ τούτου, οι συναλλαγές επαληθεύονται, και το σύστημα καθίσταται ασφαλές, από την εφαρμογή ορισμένων μηχανισμών που καθιστούν υπερβολικά δαπανηρή την παραβίαση της ακεραιότητας του συστήματος. Η βασική αρχή ενός τέτοιου μηχανισμού είναι η αναγκαιότητα της δαπάνης πόρων κατά την επιβεβαίωση των συναλλαγών. Σε αυτό το σημείο αξίζει να υπερτονίσουμε την αναγκαιότητα της κατανομής της υπολογιστικής ισχύος σε πολλούς χρήστες καθώς όπως γίνεται εύκολα αντιληπτό από τα προηγούμενα ένας χρήστης με απόλυτη πλειοψηφία στην επαλήθευση της αλυσίδας είναι ικανός να αλλοιώσει κατά το δοκούν την πορεία του blockchain.

Διάφορα κρυπτονομίσματα έχουν αναπτύξει νέα εργαλεία για τη χρήση ως μέσο ασφάλειας του δικτύου. Ο πόρος που πρέπει να καταναλώνεται μπορεί να είναι ένας

συνδυασμός ηλεκτρικής ενέργειας και χρόνου ή η προσωρινή κατοχή του νομίσματος, και αντιπροσωπεύει το κόστος για την ασφάλεια του δικτύου. Οι χρήστες που κάνουν εξόρυξη κρυπτονομισμάτων εργάζονται για την ασφάλεια του δικτύου, και αμείβονται για την εργασία τους με τη μορφή συναλλαγών ή νέων κρυπτονομισμάτων. Ο μηχανισμός που χρησιμοποιείται για την εξασφάλιση της ακεραιότητας του δικτύου καθορίζει τον πόρο και τη μέθοδο που χρησιμοποιείται για την αμοιβή τους. Έτσι, ο υποκείμενος μηχανισμός της ασφάλειας του δικτύου κάθε κρυπτονομίσματος έχει σημαντική επίπτωση επί στην οικονομία του νομίσματος. Οι επόμενες παράγραφοι θα παρουσιάσουν αναλυτικά τους πιο ευρέως χρησιμοποιούμενους μηχανισμούς στη βιομηχανία των κρυπτονομισμάτων.

Proof of Work (PoW)

Ένα σύστημα απόδειξης εργασίας (POW) ή πρωτόκολλο, ή λειτουργία, είναι ένα οικονομικό μέτρο για την αποτροπή επιθέσεων άρνησης παροχής υπηρεσίας (DoS) και άλλων καταχρήσεων των υπηρεσιών, όπως το spam σε ένα δίκτυο, απαιτώντας κάποια εργασία από τον αιτούντα υπηρεσία, που συνήθως σημαίνει ότι χρόνο επεξεργασίας από έναν υπολογιστή.

Η ιδέα του PoW παρουσιάστηκε πρώτη φορά το 1993 ως μία τεχνική για την αντιμετώπιση του spam στις υπηρεσίες email. Με λίγα λόγια απαιτούσε από τον αποστολέα του mail να υπολογίσει τη λύση ενός μαθηματικού puzzle, με σκοπό να αποδείξει πως έχει δαπανήσει ορισμένη υπολογιστική ισχύ για την ενέργεια αυτή. Το PoW προτάθηκε αυτοτελώς το 1997, μέσω του αλγορίθμου hashcash, πάλι με σκοπό την αντιμετώπιση του spam. Στη περίπτωση του hashcash, το υπολογιστικό πρόβλημα περιλάμβανε την εύρεση μιας hash τιμής-λύσης μέσω της συνάρτησης SHA-1, η οποίο θα ξεκινούσε από τουλάχιστον 20 συνεχόμενα μηδενικά. Αυτό προφανώς απαιτούσε συνεχόμενους υπολογισμούς με κόστος αρκετή υπολογιστική ισχύ. Ο Satoshi Nakamoto λοιπόν βασιζόμενος στην παραπάνω μεθοδολογία δημιούργησε το Bitcoin το 2008.

Ένα βασικό χαρακτηριστικό των συστημάτων αυτών είναι η ασυμμετρία τους: η εργασία πρέπει να είναι αρκετά σκληρή (αλλά εφικτή) από την πλευρά του αιτούντος, αλλά εύκολη να ελεγχθεί για τον πάροχο υπηρεσιών. Αξίζει να σημειωθεί ότι είναι διαφορετική από το CAPTCHA, το οποίο προορίζεται για έναν άνθρωπο να λύσει γρήγορα, παρά έναν υπολογιστή.

Σε γενικές γραμμές, το πρωτόκολλο αυτό ορίζεται από 3 βασικές διαδικασίες.

1. Την επιβεβαίωση των μπλοκ και έτσι και του blockchain. Κατά τη διάρκεια της διαδικασίας αυτής ελέγχονται αν τηρούνται όλες οι προδιαγραφές για το δοσμένο στιγμιότυπο του blockchain. Ελέγχεται, δηλαδή, αν κάθε μπλοκ περιλαμβάνει ένα έγκυρο PoW και ότι δεν υπάρχει κάποια διχογνωμία ανάμεσα στις συναλλαγές.
2. Τη σύγκριση ανάμεσα στα στιγμιότυπα των blockchain και στην επέκταση της. Η διαδικασία αυτή περιλαμβάνει τη σύγκριση ανάμεσα στο μήκος ενός συνόλου από στιγμιότυπα blockchain, τα οποία λαμβάνονται από άλλους ομότιμους χρήστες. Μέσα από αυτό το στάδιο, υιοθετείται η μεγαλύτερη σε μήκος εκδοχή των προτεινόμενων blockchain.
3. Την αναζήτηση ενός έγκυρου PoW, η οποία είναι και η κύρια και πιο απαιτητική διαδικασία

Υπάρχουν δύο κατηγορίες πρωτοκόλλων απόδειξης της εργασίας:

- Πρωτόκολλα πρόκλησης-απόκρισης: αναλαμβάνουν άμεση διαδραστική σχέση μεταξύ του αιτούμενου (client) και του παρόχου (server). Ο πάροχος επιλέγει μια πρόκληση, δηλαδή ένα στοιχείο σε ένα σύνολο με μια ιδιότητα, ο αιτών κρίνει τη

σχετική απόκριση στο σύνολο, η οποία αποστέλλεται πίσω ώστε να ελεγχθεί από τον πάροχο. Δεδομένου ότι η πρόκληση θα επιλεγεί επί τόπου από τον πάροχο, η δυσκολία της μπορεί να προσαρμοστεί στο φορτίο της. Οι εργασίες από την πλευρά του αιτούντος δύναται να ορίζονται εάν το πρωτόκολλο πρόκλησης-απόκρισης έχει μια γνωστή λύση ή είναι γνωστό ότι υπάρχει μέσα σε ένα οριοθετημένο χώρο αναζήτησης.

- Πρωτόκολλα λύσης-επαλήθευσης: δεν δεσμεύουν τη σύνδεση μεταξύ αιτούντα και παρόχου επομένως το πρόβλημα πρέπει να αυτο-επιβληθεί πριν αναζητηθεί λύση από τον αιτούντα, και ο πάροχος πρέπει να ελέγχει τόσο την επιλογή του προβλήματος και τη λύση. Τα περισσότερα τέτοια συστήματα είναι μη οριοθετημένες πιθανολογικές επαναληπτικές διαδικασίες, όπως οι μετρητές κατακερματισμού (Hashcash).

Η PoW μεθοδολογία θεωρείται computation-intensive, καθώς για να ανταπεξέλθει κάποιος στον ανταγωνισμό για την εύρεση ενός έγκυρου PoW, χρειάζεται να διαθέτει όσο το δυνατό μεγαλύτερο hash rate. Αυτό το χαρακτηριστικό αποτρέπει τις επιθέσεις Sybil από κακόβουλους χρήστες. Από την άλλη μεριά, το οικονομικό κόστος μέσω της κατανάλωσης ισχύος, καθιστά αδύνατο για οποιοδήποτε κόμβο να συμμετάσχει στο δίκτυο χωρίς να επιβαρυνθεί με κάποιο κόστος. Το παραπάνω κόστος αντισταθμίζεται με κίνητρα όπως το reward ή τα transaction fees για την εκτέλεση του αλγορίθμου.

Τέλος ορισμένα συστήματα POW προσφέρουν συντόμευση υπολογισμών που επιτρέπουν στους συμμετέχοντες που γνωρίζουν ένα μυστικό, συνήθως ιδιωτικό κλειδί, έτσι ώστε να δημιουργήσουν φτηνότερα PoW εργασίες. Το σκεπτικό είναι ότι οι κάτοχοι αυτών των κλειδιών μπορούν να δημιουργήσουν σφραγίδες για κάθε δικαιούχο, χωρίς να συνεπάγεται υψηλό κόστος. Αν ένα τέτοιο χαρακτηριστικό είναι επιθυμητό εξαρτάται από το σενάριο χρήσης. Ένα τέτοιο σενάριο είναι η περίπτωση που ένας δικτυακός τόπος μπορεί να απαιτήσει ένα συμβολικό PoW αντάλλαγμα για την παροχή της υπηρεσίας. Η απαίτηση συμβολικού PoW από τους χρήστες θα αναστείλει την επιπόλαιη ή υπερβολική χρήση της υπηρεσίας, απαλλάσσοντας κομβικούς πόρους της υπηρεσίας, όπως το εύρος ζώνης, ο υπολογισμός, ο χώρος στο δίσκο, η ηλεκτρική ενέργεια και τα γενικά λειτουργικά έξοδα.

Το παραπάνω σύστημα RPOW (Reusable Proof of Work) διαφέρει από ένα PoW σύστημα στο ότι επιτρέπει τη τυχαία ανταλλαγή token χωρίς να επαναληφθούν οι εργασίες που απαιτούνται για τη δημιουργία τους. Αφού κάποιος περάσει μια συμβολική PoW ταυτοποίηση σε μια ιστοσελίδα, ο φορέας εκμετάλλευσης του δικτυακού τόπου θα μπορούσε να ανταλλάξει το PoW για ένα νέο, μη χρησιμοποιημένο συμβολικό RPoW, το οποίο θα μπορούσε στη συνέχεια να χρησιμοποιηθεί σε κάποια ιστοσελίδα τρίτου η οποία βασίζεται στην ίδια μεθοδολογία ελέγχου εγκυρότητας. Αυτό θα εξοικονομήσει πόρους που διαφορετικά θα χρειαζόταν για τη δημιουργία μιας ακόμα PoW εργασίας. Ο διακομιστής RPoW που ανταλλάσσει ένα μεταχειρισμένο RPoW token με ένα νέο ίσης αξίας χρησιμοποιεί απομακρυσμένη πιστοποίηση για να επιτρέψει σε κάθε ενδιαφερόμενο να εξακριβώσει τι λογισμικό εκτελείται στο διακομιστή RPoW. [20]

Proof of Stake (PoS)

Το PoS αποτελεί τη δεύτερη βασική κατηγορία αλγορίθμων consensus για blockchain. Οι χρήστες-κόμβοι σε αυτά τα συστήματα ονομάζονται validators. Η συγκεκριμένη οικογένεια αλγορίθμων βασίζεται στο απόθεμα νομισμάτων (stake) που επιλέγει να δεσμεύσει ένας validator στο δίκτυο. Κάθε validator εκτελεί μία ειδική συναλλαγή, που

δεσμεύει ένα πόσο από κρυπτονομίσματα ως προκαταβολή ενώ μόνο οι validators έχουν τη δυνατότητα να δημιουργήσουν νέα μπλοκ και να αποφασίσουν μέσω του consensus ποιο θα συμπεριληφθεί στο blockchain. Στη διαδικασία του consensus, οι validators δε ψηφίζουν ισότιμα, αλλά το ποσοστό της συμμετοχής στην απόφαση είναι ανάλογο του μεγέθους του stake που έχει θέσει ως προκαταβολή. Η πιθανότητα για έναν validator να είναι αυτός που θα λάβει το reward, είναι ανάλογη του κλάσματος του μεγέθους του stake διαιρεμένου με το συνολικό αριθμό νομισμάτων σε κυκλοφορία. Όπως γίνεται εύκολα αντιληπτό όσο μεγαλύτερο ποσό θέτει ως προκαταβολή, τόσο αυξάνεται η πιθανότητα για επιτυχία. Όποιος validator παραβιάζει τους κανονισμούς του consensus, παρακρατείται το ποσό που έχει θέσει ως stake.

Αν και η μέθοδος απόδειξης της εργασίας ζητά από τους validators να τρέχουν επανειλημμένα αλγόριθμους κατακερματισμού για την επικύρωση των ηλεκτρονικών συναλλαγών, η απόδειξη της συμμετοχής προϋποθέτει να αποδείξουν την κυριότητα σε ένα ορισμένο ποσό του νομίσματος («συμμετοχής» τους στο νόμισμα). Το Peercoin ήταν το πρώτο κρυπτονόμισμα που χρησιμοποίησε την απόδειξη συμμετοχής. Άλλες εξέχουσες εφαρμογές βρίσκονται στα BitShares, NXT, BlackCoin, NuShares / NuBits και Qora. Σε αυτό το σημείο αξίζει να σημειωθεί ότι σύμφωνα με Bitcoin miners, η κατανάλωση ενέργειας ανήλθε στις 240kWh ανά Bitcoin το 2014 (ισοδύναμο με 16 γαλόνια φυσικού αερίου με τις τότε τιμές). Επιπλέον, οι δαπάνες της ενέργειας σχεδόν πάντα καταβάλλονται σε μη-κρυπτονόμισμα, εισάγοντας σταθερή πτωτική πίεση στην τιμή. Επομένως η PoS μέθοδος μπορεί να είναι αρκετές χιλιάδες φορές πιο αποδοτική.

Η πιθανότητα ένας validator να δημιουργήσει ένα νέο μπλοκ επιτυχώς εξαρτάται από τη ποσότητα των νομισμάτων που διαθέτει (από το μέγεθος του stake), και όχι από τη υπολογιστική ισχύ που δαπανά. Με αυτό το τρόπο, ελαχιστοποιείται το κόστος σε ενέργεια για κάθε συναλλαγή και μπλοκ και αποδίδεται η δυνατότητα απόφασης μόνο στους κόμβους όπου διαθέτουν stake μέσα στο δίκτυο. Δηλαδή, μόνο εάν ένας χρήστης διαθέτει ένα ποσό από νομίσματα μπορεί να συμμετάσχει στις διαδικασίες ενημέρωσης του blockchain (όπως ο έλεγχος της εγκυρότητας των συναλλαγών και η δημιουργία νέων μπλοκ). Αυτό έρχεται σε αντίθεση με τις περιπτώσεις του PoW, όπου κάθε χρήστης έχει τη δυνατότητα να αναλάβει του ρόλο του miner. Στη περίπτωση του PoS, δεν απαιτείται καθόλου υπολογιστική δύναμη για την επίλυση ενός υπολογιστικού προβλήματος. Επίσης, δεν υπάρχουν rewards μέσα από τη μορφή της δημιουργίας χρήματος καθώς οι κόμβοι συλλέγουν τα transaction fees. Από τη στιγμή που συμβαίνει κάτι τέτοιο, το ενδεχόμενο για τη δημιουργία κενών μπλοκ είναι σχετικά απίθανο, καθώς οι nodes έχουν ως κίνητρο τη ενσωμάτωση όσο το δυνατό περισσότερων transactions, ώστε να μεγιστοποιήσουν τα κέρδη τους. [20,5]

Hybrid PoW / PoS

Τα συστήματα που αξιοποιούν hybrid PoW/PoS επιδιώκουν να συνδυάσουν τα πλεονεκτήματα κάθε σχεδιασμού. Ένα υβριδικό σύστημα Pow / PoS χρησιμοποιεί τον μηχανισμό PoW για την αρχική κοπή και διανομή κερμάτων. Δηλαδή, ο PoW επιτρέπει στο δίκτυο τη διανομή των νέων κερμάτων προς εκείνους που εξορυγνύουν νομίσματα. Ωστόσο, με την πάροδο του χρόνου, ο μηχανισμός PoS σβήνει τον μηχανισμό Pow, δημιουργώντας ένα μακροπρόθεσμα ενεργειακά αποδοτικό κρυπτονόμισμα. Σε αυτό το σχεδιασμό, η δημιουργία νέων μπλοκ, βασίζεται στο παράγοντα coinage. Το coinage είναι περίπου το πλήθος νομισμάτων ενός ιδιοκτήτη πολλαπλασιασμένο με το χρόνο της κυριότητας από τον σημερινό ιδιοκτήτη του νομίσματος. Έτσι, η δημιουργία νέων μπλοκ πριμοδοτεί τα μπλοκ με το μεγαλύτερο coinage. Επίσης, τα νομίσματα μπαίνουν σε κυκλοφορία είναι το 1% των νομισμάτων που έχουν δαπανηθεί μέσα σε ένα coin-year. Το βασικό πλεονέκτημα είναι πως

δεν απαιτείται μεγάλη κατανάλωση ενέργειας ενώ επιπρόσθετα το σχέδιο είναι οικονομικά ανταγωνιστικό σε σύγκριση με εκείνο που βασίζεται σε PoW και αποφεύγει το πρόβλημα της διανομής που είναι συνυφασμένο με τη PoS. [20]

Μηχανισμός συναίνεσης (Byzantine Consensus)

Τα κρυπτονομίσματα Ripple και Stellar διαθέτουν έναν εξ ολοκλήρου εναλλακτικό μηχανισμό ασφαλείας, που αποτελεί υλοποίηση του πρωτοκόλλου «Byzantine Consensus». Η υποδομή των νομισμάτων είναι αυτή ενός κατανεμημένου δικτύου, όπου κάθε server του δικτύου είναι αντιμέτωπος με το πρόβλημα του να αποφασίσει αν οι άλλοι διακομιστές στο δίκτυο αποστέλλουν έγκυρα μηνύματα που στη συγκεκριμένη περίπτωση αντιστοιχούν σε συναλλαγές μεταξύ χρηστών.

Τα κατανεμημένα δίκτυα που δημιουργούνται από τα κρυπτονομίσματα Ripple και Stellar αντιμετωπίζουν το εξής πρόβλημα: άτομα που εμπλέκονται με ένα από αυτά τα νομίσματα θα πρέπει να ενταχθούν σε ένα διακομιστή. Κάθε διακομιστής στο δίκτυο βρίσκεται αντιμέτωπος με το πρόβλημα του να αποφασίσουν αν άλλοι servers στο δίκτυο στέλνουν ακριβή "μηνύματα", το οποίο στην προκειμένη περίπτωση είναι συναλλαγές. Το πρωτόκολλο Ripple απαιτεί ότι οι οικονομικές οντότητες εντάσσονται σε ένα διακομιστή. Κάθε διακομιστής διατηρεί μια λίστα με μοναδικούς Κόμβος (UNL), σύμφωνα με την οποία επικοινωνεί μόνο με τους κόμβους στο UNL του κάτι που επιτρέπει στους διακομιστές να είναι σε επαφή μόνο με άλλους αξιόπιστους διακομιστές. Κάθε διακομιστής μπορεί να μεταδώσει τις συναλλαγές, επί των οποίων και ψηφίζουν. Ωστόσο, οι διακομιστές ψηφίζουν μόνο για συναλλαγές που προέρχονται από άλλους κόμβους του UNL. Κάθε λίγα δευτερόλεπτα, όλοι οι διακομιστές στέλνουν μηνύματα εμπρός και πίσω, έως ότου ο αλγόριθμος να τερματιστεί με συναίνεση ή αδυναμία να επιτευχθεί συναίνεση. Ο συγκεκριμένος αλγόριθμος που χρησιμοποιείται στο δίκτυο Ripple απαιτεί ότι η συναλλαγή γίνεται αποδεκτή από το 80 τοις εκατό των servers, προκειμένου για την επίτευξη συναίνεσης. Αυτός ο μηχανισμός ασφαλείας είναι πιο ενεργειακά αποδοτικός από το μηχανισμό Pow, απαιτεί τουλάχιστον μια επίθεση 80% στο δίκτυο, προκειμένου να παραβιαστεί η ασφάλεια του δικτύου (ο αλγόριθμος τερματίζει χωρίς συναίνεση, εάν δεν υπάρχει συμφωνία 80%), επιτρέπει ευέλικτη εμπιστοσύνη, και προσφέρει γρηγορότερους χρόνους συναλλαγής.

1.3 Οφέλη και κίνδυνοι κρυπτονομισμάτων

Τα κρυπτονομίσματα και ειδικότερα το bitcoin είναι αδιαμφισβήτητα το μέλλον, όχι μόνο ως μέσο ψηφιακών συναλλαγών, αλλά και της τεχνολογίας που αυτά κρύβουν. Εμφανίζουν πληθώρα πλεονεκτημάτων και παρέχουν σημαντικά οφέλη στους καταναλωτές. Παρ' όλα αυτά, παρουσιάζουν και κάποια μειονεκτήματα που επιβάλλεται να παρουσιαστούν, ώστε να μπορέσουμε μελλοντικά να μειώσουμε τους κινδύνους που ενδεχομένως να κρύβει η αλόγιστη χρήση τους. [4]

1.3.1 Οφέλη

Χαμηλά τέλη

Προς το παρόν οι πληρωμές με ψηφιακά νομίσματα γίνονται είτε με μηδενικά είτε με εξαιρετικά χαμηλά τέλη. Αυτό συμβαίνει μιας και υπάρχει απουσία από μεσάζοντες, που εμφανίζονται σε άλλες μορφές συναλλαγών. Επιγραμματικά μπορεί να αναφερθεί ότι κατά τη χρήση τραπεζικών καρτών υπάρχουν τα διοικητικά έξοδα και όπως και κατά τη χρήση του ευρέως χρησιμοποιημένου PayPal (και αντίστοιχων προπληρωμένων καρτών), υπάρχει η νόμιμη προμήθεια. Τέτοιου είδους κόστη δεν επιβαρύνουν τους χρήστες των ψηφιακών νομισμάτων και ταυτόχρονα προτιμώνται και από τους εμπόρους μιας και οι αποδέκτες της μεταφοράς δεν επιβαρύνονται για τις συναλλαγές. Ωστόσο σε ορισμένες μόνο περιπτώσεις για την εξασφάλιση προτεραιότητας στην διεκπεραίωση των συναλλαγών τους, οι χρήστες είναι πιθανό να συμπεριλάβουν τέλη, οδηγώντας έτσι στην γρηγορότερη επικύρωση των συναλλαγών από το δίκτυο (Gas amount for Ethereum).

Διαφάνεια κανόνων και συναλλαγών

Οποιαδήποτε συναλλαγή έχει εκτελεστεί στο δίκτυο είναι διαφανής και δημόσια διαθέσιμη. Για τον λόγο αυτό, όλοι μπορούν να εξετάσουν όποια διεύθυνση επιθυμούν και να δουν όλες τις συναλλαγές που έχουν εκτελεστεί με αυτή, το πλήθος των κρυπτονομισμάτων που έχουν μετακινηθεί, καθώς και το που έχουν σταλεί. Η διαφάνεια αυτή ισχύει για όλες τις συναλλαγές που έχουν εκτελεστεί ποτέ. Επίσης, το ίδιο ισχύει και για τους κανόνες στους οποίους συναινούν οι χρήστες και δουλεύει το λογισμικό. Μέσα στο λογισμικό δεν υπάρχουν κρυφοί κανόνες και δεν θα υπάρξουν, μιας και οι χρήστες δεν θα το αποδέχονταν

Ελευθερία πληρωμών

Είναι δυνατή η αποστολή ή η λήψη οποιουδήποτε χρηματικού ποσού άμεσα, οπουδήποτε στο κόσμο, οποιαδήποτε στιγμή. Δε μπορεί κάποια κεντρική εξουσία είτε να ασκήσει νομισματική πολιτική δεσμεύοντας χρήματα πολιτών είτε να προκαλέσει τυχόν κωλύματα (λόγω γραφειοκρατίας, αργιών κλπ.). Αυτό συμβαίνει λόγω του ότι υπάρχει απουσία ελεγκτικού φορέα (τράπεζες κυβερνήσεις), μειώνοντας ταυτόχρονα το κόστος των συναλλαγών μιας και παρέχεται ασφάλεια για τήρηση των κανόνων ασφαλείας όλο το 24ώρο χωρίς την παρουσία του. Τα κρυπτονομίσματα επιτρέπουν τον πλήρη έλεγχο των χρημάτων στους χρήστες τους.

Απουσία κρατικών φόρων συναλλαγής

Τα αποκεντρωμένα ψηφιακά νομίσματα και η ανωνυμία που παρέχουν δυσχεραίνει το έργο των κυβερνήσεων ως προς την φορολογία σε τυχόν εισφορές συναλλαγών, κάτι το οποίο βρίσκεται μόνο στην ευχέρεια του συναλλασσόμενου να το δηλώσει. Μάλιστα το Ευρωπαϊκό Δικαστήριο στην τελευταία του απόφαση αναφέρει πως δεν μπορεί να φορολογηθεί ως κατοχή περιουσιακού στοιχείου ή ως νόμισμα.

Αντίγραφα ασφαλείας/Φορητότητα

Οι κωδικοί πρόσβασης, τα πορτοφόλια αποθήκευσης και τα κρυπτονομίσματα, ανεξάρτητα από το πλήθος τους, μπορούν να μεταφερθούν εύκολα, να απομνημονευτούν ή ακόμη και να καταγραφούν σε χαρτί, καθώς είναι πολύ μικρά σε μέγεθος. Ακόμη, σε

περίπτωση καταστροφής των αρχικών, τα στοιχεία των διαθέσιμων κρυπτονομισμάτων μπορούν να αντιγραφούν για να υπάρχουν αντίγραφα ασφαλείας, κάτι που δεν μπορεί να συμβεί για τις συμβατικές αξίες. Αυτό βέβαια σημαίνει, πως αν κάποιο από τα αντίγραφα παραβιαστεί, παραβιάζονται και όλα τα υπόλοιπα.

Υποδιαιρέσεις

Επιτυγχάνεται η διευκόλυνση των μικροπληρωμών, όπου αποτελεί πρόβλημα για το παραδοσιακό χρηματοπιστωτικό σύστημα, βελτιώνοντας έτσι την αποτελεσματικότητα των πληρωμών. Κάθε *Bitcoin* μπορεί να υποδιαιρεθεί σε έως και 8 δεκαδικά ψηφία (0,00000001) τα λεγόμενα *Satoshi*. Η προσθήκη περισσότερων ακόμα δεκαδικών ψηφίων επαφίεται στην συναίνεση των χρηστών του δικτύου.

Μη πληθωριστικό νόμισμα

Τα συμβατικά νομίσματα υφίστανται κάποιες πληθωριστικές πιέσεις, όμως λόγω του ακριβή αριθμού δημιουργίας των κρυπτονομισμάτων, της οριοθέτησης του χρόνου παραγωγής τους και της σταδιακής αύξησης της δυσκολίας εξόρυξης (mining) τους δεν ισχύει το ίδιο γι' αυτά. Όπως επίσης δεν διατρέχουν και τους αντίστοιχους οικονομικούς κινδύνους.

Νόμισμα παγκόσμιας εμβέλειας

Τα ψηφιακά νομίσματα καθίστανται σαν νομίσματα παγκόσμιας εμβέλειας μιας και καθίσταται δυνατή η μετάβαση σε οποιοδήποτε μέρος του κόσμου χωρίς να απαιτείται η χρήση μετρητών ή πιστωτικών καρτών, χωρίς να υφίσταται και κίνδυνος κλοπής.

Λιγότεροι κίνδυνοι για τους εμπόρους

Οι συναλλαγές με κρυπτονομίσματα δεν περιέχουν ευαίσθητα προσωπικά δεδομένα ή προσωπικές πληροφορίες των πελατών επομένως είναι ασφαλείς και μη αναστρέψιμες. Έτσι, οι έμποροι προστατεύονται από ζημίες που συνήθως οφείλονται σε δόλιους αντιλογισμούς χρέωσης ή σε απάτες. Οι έμποροι, με αυτό τον τρόπο, επεκτείνονται εύκολα σε νέες αγορές παρόλα τα υψηλά ποσοστά απάτης ή την μη διαθεσιμότητα πιστωτικών καρτών. Το καθαρό κέρδος που υπάρχει ως αποτέλεσμα, είναι λιγότερα διοικητικά κόστη, μεγαλύτερες αγορές και φυσικά, χαμηλότερα κόστη.

Συναινετική φύση χρήσης

Η αλλαγή οποιουδήποτε χαρακτηριστικού του λογισμικού ή των κανόνων του, έχει εφαρμογή μόνο όταν τις δεχθεί η κοινότητα που απαρτίζει το δίκτυο. Έτσι, επιτυγχάνεται η αποφυγή κακόβουλων αλλαγών που θα μπορούσαν να αλλάξουν άρδην το λογισμικό, αλλά υπάρχει ευελιξία και μεγάλη ταχύτητα αντίδρασης σε περίπτωση που εντοπιστούν σφάλματα ή απρόβλεπτες αστοχίες κατά τη λειτουργία.

Παροχή ελέγχου και ασφάλειας

Ο πλήρης έλεγχος των συναλλαγών βρίσκεται στους χρήστες των κρυπτονομισμάτων. Σε διάφορες μεθόδους πληρωμής, οι έμποροι μπορούν να επιβάλλουν κάποιες απαραίτητες ή ανεπιθύμητες χρεώσεις, όμως στην συγκεκριμένη είναι ανέφικτο. Η σύνδεση των προσωπικών πληροφοριών με την κάθε συναλλαγή για τις πληρωμές με κρυπτονομίσματα δεν χρειάζεται κάτι που καθιστά τα κρυπτονομίσματα αδύνατο να κλαπούν από τρίτους.

Ταχύτητα & ευκολία συναλλαγών

Οι σαφείς οδηγίες και τα απλά βήματα που είναι διαθέσιμα στο κοινό, για την ορθή χρήση των κρυπτονομισμάτων περιορίζει τη δυσκολία στη χρήση της τεχνολογίας αυτής. Ταυτόχρονα η εισαγωγή στον κόσμου των κρυπτονομισμάτων απαιτεί απλά τη χρήση ενός δωρεάν λογισμικού σε Smartphone ή υπολογιστή και σύνδεση στο διαδίκτυο. Η επιβεβαίωση της συναλλαγής από το δίκτυο του ψηφιακού νομίσματος, ολοκληρώνεται εντός ολίγων λεπτών, οποιαδήποτε στιγμή της ημέρας και άμεσα ανακοινώνεται ταυτόχρονα σε όλο δίκτυο ανά τον πλανήτη.

1.3.2 Κίνδυνοι

Πέρα από τα παραπάνω πλεονεκτήματα που αναφέρθηκαν και αναπτύχθηκαν, τα κρυπτονομίσματα έχουν κάποιους κινδύνους ή απειλές. [4]

Διευκόλυνση παράνομων δραστηριοτήτων

Λόγω της ανωνυμίας που φέρουν τα κρυπτονομίσματα, επιτρέπουν την απάτη και διάφορες άλλες εγκληματικές δραστηριότητες. Τα έσοδα από πλαστογράφηση και από παράνομες δραστηριότητες, έχουν την δυνατότητα να νομιμοποιηθούν στα συμβατικά νομίσματα (ξέπλυμα μαύρου χρήματος). Τα κρυπτονομίσματα, μεγεθύνουν αυτούς τους κινδύνους, καθώς η ανταλλαγή τους γίνεται αποκλειστικά και μόνο ανώνυμα και κυριαρχεί σε σκοτεινά δίκτυα που αφορούν την κυκλοφορία ναρκωτικών. Η ικανότητα οποιουδήποτε οικονομικού φορέα να συναλλάσσεται με κρυπτονομίσματα ακόμα και για νόμιμους λόγους, τερματίστηκε από την προσπάθεια να επιβληθεί ο νόμος για να διακοπούν αυτά τα δίκτυα.

Βαθμός αποδοχής

όσον αφορά την χρήση των κρυπτονομισμάτων, μεγάλο μέρος του παγκόσμιου πληθυσμού δεν γνωρίζει επαρκή στοιχεία, ή ακόμη και καθόλου για αυτήν. Παρόλο που πολλές επιχειρήσεις, για να αποκτήσουν τα οφέλη που προαναφέρθηκαν, δέχονται τα κρυπτονομίσματα ως πληρωμή, ο αριθμός τους είναι περιορισμένος. Για να αλλάξει αυτό απαιτείται η πληροφόρηση και η εκπαίδευση στη χρήση του ψηφιακού νομίσματος.

Υποδιαίρεση

Αυτό που νωρίτερα παρουσιάστηκε σαν πλεονέκτημα μπορεί να θεωρηθεί εξίσου και μειονέκτημα των κρυπτονομισμάτων καθώς δυσχεραίνουν τις επιχειρήσεις κυρίως κατά τη μετατροπή τους σε φυσικά νομίσματα.

Συνεχής εξέλιξη

Το λογισμικό και οι λειτουργίες κρυπτογράφησης (αλγόριθμοι) των ψηφιακών νομισμάτων βρίσκονται σε συνεχή εξέλιξη με σκοπό καλύτερες παρεχόμενες υπηρεσίες στους χρήστες καθώς και μεγαλύτερη ασφάλεια. Συνεχώς αναπτύσσονται νέα χαρακτηριστικά και παροχές που δεν είναι διαθέσιμα για όλους. Επί της ουσίας, ασφάλιση δεν παρέχεται από καμία, σχεδόν, επιχείρηση. Αυτού του είδους η εξέλιξη καθιστά τα κρυπτονομίσματα σε πορεία προς την ωρίμανση τους.

Μεγάλος ανταγωνισμός

Το πρώτο αποκεντρωμένο κρυπτονόμισμα, το Bitcoin, βασίζεται σε ανοιχτό κώδικα καθιστώντας εύκολη την αντιγραφή του άρα τελικά και την δημιουργία νέων κρυπτονομισμάτων με τα ίδια χαρακτηριστικά. Αυτό επιφέρει σύγχυση στον νέο χρήστη και ενισχύει τους φόβους του για τη σταθερότητα των τιμών εξαιτίας και του μεγάλου ανταγωνισμού των διαφόρων κρυπτονομισμάτων.

Μεταβλητότητα

Οι επιχειρήσεις που χρησιμοποιούν τα κρυπτονομίσματα και ο όγκος που ανταλλάσσεται είναι πολύ μικρός συγκριτικά με τον αριθμό που θα μπορούσε να είναι. Οι τιμές των κρυπτονομισμάτων, για αυτό τον λόγο, επηρεάζονται άμεσα και σε μεγάλο βαθμό από τις δραστηριότητες των επιχειρήσεων ή από τις μεταβολές στις αγορές.

Νομικό πλαίσιο

Το νομικό πλαίσιο από χώρα σε χώρα διαφέρει, καθιστώντας αυτήν την ποικιλομορφία στην αντιμετώπιση του ψηφιακού νομίσματος ως μειονέκτημα. Πολλές χώρες δεν απαγορεύουν την χρήση κρυπτονομισμάτων αλλά ταυτόχρονα δεν τα θεωρούν νόμιμα. Άλλες χώρες επίσης περιορίζουν την χρήση τους και δεν παρέχουν άδεια σε επιχειρήσεις ανταλλακτηρίων ψηφιακών νομισμάτων. Ωστόσο σε τελευταίες εξελίξεις στο χρηματοπιστωτικό σύστημα τα κρυπτονομίσματα τείνουν να χαρακτηριστούν χρηματιστηριακό προϊόν και όχι νόμισμα κάτι που έχει ανακόψει την ραγδαία άνοδο τους στις αρχές του 2018.

Μη φυσική μορφή

Τα κρυπτονομίσματα υστερούν εκ προοιμίου από το φυσικό χρήμα λόγω του μη απτού χαρακτήρα τους. Κάποια κρυπτονομίσματα έκαναν την εμφάνιση τους σε φυσική μορφή, όμως γρήγορα εξαντλήθηκαν λόγω του περιορισμένου χαρακτήρα τους ενώ άλλα που επρόκειτο να τυπωθούν γρήγορα ανεστάλησαν.

Φορολογικό πλαίσιο

Η φορολογική πολιτική των κυβερνήσεων για τα κρυπτονομίσματα είναι ότι αν και δεν αποτελεί νόμιμο χρήμα, μπορεί να αποτελέσει εισόδημα, γι’ αυτό και ο χρήστης φορολογείται. Από κει και πέρα όμως και παρά τα μέτρα φορολόγησης τους, η χρήση των ψηφιακών νομισμάτων, λόγω της φύσης τους και λόγω των διαφόρων μεθόδων απόκρυψης των συναλλαγών, καθιστούν τα κρυπτονομίσματα ως μία διέξοδο προς το ξέπλυμα και την φοροδιαφυγή. Η δήλωση των εσόδων των κρυπτονομισμάτων επαφίεται στην ηθική ευχέρεια του χρήστη. Τυπικό παράδειγμα αποτελούν οι miners οι οποίοι δεν φορολογούνται για το εισόδημα που λαμβάνουν ως αντάλλαγμα στην παροχή της υπολογιστικής τους ισχύος.

1.4 Γιατί πολυκριτηριακή ανάλυση

1.4.1 Γενικά

Η πολυκριτηριακή ανάλυση αποτελεί μία εφαρμογή της Επιχειρησιακής Έρευνας που επιχειρεί να βοηθήσει στη λήψη αποφάσεων που πραγματοποιούνται από τη Διοίκηση ενός οργανισμού, δημόσιου ή ιδιωτικού. Η αξία της πολυκριτηριακής ανάλυσης βασίζεται στο γεγονός ότι οι διαθέσιμες επιλογές σε ένα πολυκριτηριακό πρόβλημα παρουσιάζουν άριστη επίδοση μόνο ως προς έναν ή περισσότερους, αλλά ποτέ ως προς όλους τους στόχους. Είναι αναγκαίος λοιπόν ένας συμβιβασμός μεταξύ των αλληλοσυγκρουόμενων στόχων. Αν αναλογιστούμε το πλήθος των εφαρμογών που έχουν να κάνουν με τη πολυκριτηριακή ανάλυση συμβιβαζόμαστε με το γεγονός ότι ο κύριος στόχος δεν είναι να ανακαλύψουμε μια λύση αλλά να δημιουργήσουμε ή να κατασκευάσουμε κάτι το οποίο να θεωρείται ικανό να βοηθήσει κάποιον ενδιαφερόμενο να λάβει μέρος στη διαδικασία λήψης της απόφασης, άλλοτε για να διαμορφώσει και άλλοτε για να μεταβάλλει τις προτιμήσεις του ή να αποφασίσει σε συμφωνία με τους τελικούς του στόχους. [21]

Η πολυκριτηριακή θεωρία αποφάσεων συμβαδίζει με τα προβλήματα της καθημερινής μας ζωής. Αυτή η αντιστοιχία ερμηνεύει σε μεγάλο βαθμό την ανάδειξη πλήθους πολυκριτηριακών μεθοδολογιών, οι οποίες παρουσιάζουν σημαντικές διαφοροποιήσεις μεταξύ τους. Οι διαφορές αυτές επικεντρώνονται στον ορισμό κυρίως του προβλήματος απόφασης καθώς και στη χρήση ή μη σεναρίων στο περιβάλλον απόφασης. Επιπλέον πολυπλοκότητα υπεισέρχεται με την εισαγωγή διαφορετικών μαθηματικών μοντέλων καθώς η μαθηματική εφαρμογή στο πολυκριτηριακό σύστημα απόφασης εντοπίζεται κυρίως στην ποσοτικοποίηση των εκάστοτε προτιμήσεων. Τελικά αυτή η ποσοτικοποίηση εκφράζεται μέσω δυαδικών σχέσεων με αποτέλεσμα διαφορετικές μαθηματικές μέθοδοι να οδηγούν και σε διαφορετικές μεθοδολογίες.

Ακολουθεί μια τυπική λίστα με χαρακτηριστικές πολυκριτηριακές μεθόδους προσέγγισης προβλημάτων:

- Analytic hierarchy process (AHP)
- Analytic network process (ANP)
- Inner product of vectors (IPV)
- Multi-attribute value theory (MAVT)
- Multi-attribute utility theory (MAUT)
- Multi-Attribute Global Inference of Quality (MAGIQ)
- Goal programming
- ELECTRE (Outranking)
- ELECTRE I (with/without veto)
- ELECTRE Tri
- ELECTRE III
- PROMETHÉE (Outranking)
- Data envelopment analysis
- The evidential reasoning approach
- Dominance-based Rough Set Approach (DRSA)
- Aggregated Indices Randomization Method (AIRM)
- Nonstructural Fuzzy Decision Support System (NSFDSS)
- Grey relational analysis (GRA)

- Superiority and inferiority ranking method (SIR method)
- Potentially All Pairwise Rankings of all possible Alternatives (PAPRIKA)
- Value Engineering (VE)
- Value analysis (VA)

Δύο από τους γνωστότερους τύπους πολυκριτηριακών μεθόδων είναι οι Σχέσεις υπεροχής (Outranking Methods) και οι Σχέσεις πολλαπλών χαρακτηριστικών και χρησιμότητας (Multiattribute Utility and Value Theories/MAUT).

Οι πολυκριτηριακές μέθοδοι που είναι βασισμένες σε σχέσεις υπεροχής χρησιμοποιούν την ανά ζεύγη σύγκριση των επιλογών σε κάθε μεμονωμένο κριτήριο με βάση τις επιδόσεις τους και τις ενδοκριτηριακές προτιμήσεις του λήπτη απόφασης. Η σύγκριση στην αρχική κλίμακα μέτρησης των επιδόσεων (ποσοτική ή ποιοτική) γίνεται χωρίς αναγωγή στο διάστημα [0,1]. Ο δείκτης που προκύπτει από τη σύγκριση συντίθεται σε ένα συνολικό δυαδικό δείκτη λαμβάνοντας υπόψη τους συντελεστές βαρύτητας των κριτηρίων. Οι δυαδικοί δείκτες χαρακτηρίζουν ζεύγη επιλογών (a, b) και προσδιορίζουν στο διάστημα [0,1] το βαθμό στον οποίο ισχύει η υπόθεση: «η λύση a είναι τουλάχιστον τόσο καλή όσο και η λύση b». Ανάλογα με τη μέθοδο και τον τρόπο υπολογισμού τους, οι δείκτες διακρίνονται σε δείκτες προτίμησης ή δείκτες συμφωνίας (ως προς την υπόθεση). Τέλος διενεργείται επεξεργασία των δεικτών ώστε να προκύψουν σχέσεις υπεροχής και η τελική κατάταξη των εναλλακτικών λύσεων. Οι πιο γνωστές μέθοδοι υπεροχής είναι οι ELECTRE και PROMETHEE.

Οι πολυκριτηριακές μέθοδοι που είναι βασισμένες σε σχέσεις πολλαπλών χαρακτηριστικών και χρησιμότητας εφαρμόζουν την απόδοση μίας βοηθητικής μεταβλητής σε κάθε πράξη, η οποία αναπαριστά την προτίμηση (preferability) της εκάστοτε πράξης. Θεωρούνται αρκετά απλοί μέθοδοι και χρησιμοποιούνται ακόμα κα για να υπολογιστεί ο σταθμικός μέσος ενός συνόλου. Χαρακτηριστικά παραδείγματα διαδικασιών που στηρίζονται στην λογική της MAUT είναι η μέθοδος UTA η οποία έχει ως βασική της φιλοσοφία τη συγκέντρωση και το διαχωρισμό (aggregation-disaggregation) και το γραμμικό προγραμματισμό, η AHP (Analytic Hierarchy Process) η οποία χρησιμοποιεί τη σύγκριση κατά ζεύγη και την κρίση του ατόμου για να καταγράψει τα κριτήρια, η ANP (Analytic Network Process) που σχηματίζει λόγους προτεραιότητας (priority ratio) από τους μεμονωμένους λόγους των στοιχείων που επηρεάζουν τα κριτήρια και τέλος η MACBETH (Measuring Attractiveness by a Categorical Based Evaluation Technique) η οποία με τη σειρά της απαιτεί ποιοτικές κρίσεις πάνω στις διαφορές των τιμών ελκυστικότητας των πράξεων μεταξύ τους.

1.4.2 Πλεονεκτήματα

Η χρήση των πολυκριτηριακών μεθόδων σε προβλήματα λήψης αποφάσεων συνοδεύεται από ένα πλήθος πλεονεκτημάτων τα οποία παρουσιάζονται στη συνέχεια [22]:

- Διευκολύνει την αναπαράσταση πολυδιάστατων προβλημάτων
- Είναι ιδιαίτερα ευέλικτη και επιτρέπει τη διαφορετική επίδραση των παραγόντων στο τελικό αποτέλεσμα.
- Απλοποιεί τη διαδικασία όταν είναι αναγκαία η αξιολόγηση μη μετρήσιμων μεγεθών (π.χ. περιβαλλοντικών ή κοινωνικών επιπτώσεων).

- Είναι ανοιχτή στην ανάλυση και την αλλαγή, αν είναι απαραίτητο, της επιλογής των στόχων και των κριτηρίων που επιλέγει οποιαδήποτε ομάδα ληπτών αποφάσεων
- Όταν χρησιμοποιούνται τα σκορ και τα βάρη είναι αναλυτικά και διαμορφώνονται σύμφωνα με συγκεκριμένες τεχνικές.
- Είναι δυνατό να επαληθευτούν από άλλες πηγές πληροφόρησης για τις σχετικές τιμές και αν είναι απαραίτητο να διαφοροποιηθούν.
- Μπορεί να υπολογισθεί η αποδοτικότητα της από ειδικούς ώστε να μην γίνεται απαραίτητα από τους λήπτες αποφάσεων
- Είναι ένα σημαντικό μέσο επικοινωνίας ανάμεσα στους λήπτες των αποφάσεων καθώς επίσης σε ορισμένες περιπτώσεις μεταξύ των ληπτών αποφάσεων της κοινότητας.

1.4.3 Μειονεκτήματα

Ωστόσο εκτός από τα προφανή πλεονεκτήματα εντοπίζονται και κίνδυνοι από τη χρήση των πολυκριτηριακών μεθόδων που μπορεί να οδηγήσουν σε εσφαλμένο αποτέλεσμα τον αποφασίζοντα [22]:

- Οι συντελεστές βαρύτητας συχνά αποφασίζονται από ένα άτομο ή ένα ενδιαφερόμενο φορέα
- Συχνά η βαθμολόγηση των παραμέτρων και των συντελεστών βαρύτητας καθίσταται πολύπλοκη
- Αδυνατίζει την επίδραση του παράγοντα «χρόνου»
- Δεν οδηγεί σε βέλτιστες λύσεις, αλλά σε «συμβιβαστικές»

2 Κρυπτονομίσματα

Παρακάτω θα επιχειρήσουμε να κάνουμε μια σύντομη παρουσίαση των νομισμάτων που επιλέξαμε. Τα κριτήρια επιλογής των συγκεκριμένων κρυπτονομισμάτων από τα πάνω από 5000 διαθέσιμα προς μελέτη θα αναλυθούν σε επόμενο κεφάλαιο.

2.1 Bitcoin

Αν και όπως θα προσπαθήσουμε να αναλύσουμε και παρακάτω δεν υπάρχουν αρκετά στοιχεία γύρω από το πρόσωπο και τη δραστηριότητα του δημιουργού του Bitcoin, έχουμε τη δυνατότητα να κάνουμε κάποιες ασφαλείς εκτιμήσεις για τα κίνητρα του με βασικό κριτήριο το paper που δημοσίευσε ο ίδιος. Ο συγγραφέας του paper περιγράφει πως το ηλεκτρονικό εμπόριο και οι συναλλαγές που πραγματοποιούνται σήμερα βασίζονται στο σύνολο τους σε τραπεζικά και οικονομικά ιδρύματα τα οποία καταδεικνύει ως υπεύθυνα για τις 2 βασικότερες λειτουργίες μιας συναλλαγής: την επεξεργασία της και τον έλεγχο της εγκυρότητας. Ακολουθείται επομένως η σχέση client-server με κάποιο διαμεσολαβητή, το ρόλο του οποίου αναλαμβάνει μια κεντρική αρχή που είναι υπεύθυνη για την αλληλεπίδραση μεταξύ των χρηστών. Αρκεί η αμοιβαία εμπιστοσύνη από όλους τους χρήστες στην κεντρική αρχή ώστε όλες οι συναλλαγές να πραγματοποιούνται αρμονικά.

Βέβαια, το παραπάνω μοντέλα χαρακτηρίζεται από ποικίλα μειονεκτήματα λόγω της φύσης τους. Για παράδειγμα, σε ένα ανάλογο διαδικτυακό μοντέλο, μία τράπεζα ή κάποιος άλλος οργανισμός όπως μια κρατική υπηρεσία παίζει το ρόλο του διαμεσολαβητή στη πραγματοποίηση συναλλαγών. Παράλληλα, οι συγκεκριμένοι θεσμοί διαθέτουν την ισχύ για να επιβάλλουν το πάγωμα της κίνησης του λογαριασμού και να θέσουν όρια στα ποσά που διακινούνται στις συναλλαγές, δημιουργώντας έτσι εμπόδια στους χρήστες. Επίσης, οι χρήστες είναι υπόλογοι στη κρατική νομοθεσία και την φορολογία που επιφέρεται με αυτές, αλλά και ευάλωτοι σε αποσταθεροποιήσεις πχ κούρεμα καταθέσεων σε κρίσιμες καταστάσεις ή όρια στην πιστοληπτική ικανότητα. Χαρακτηριστικό παράδειγμα αποτελεί η χώρα μας στην οποία εφαρμόστηκαν και τα 2 παραπάνω μέτρα στο διάστημα 2010-15. Επιπρόσθετα, ένα ανάλογο διαδικτυακό μοντέλο απαιτεί πληροφορίες για τους πελάτες και τους αγοραστές,

έτσι ώστε να εξασφαλίζεται η μετάκληση της συναλλαγής για τους χρήστες στην περίπτωση που δημιουργηθούν διενέξεις ανάμεσα σε πωλητές και αγοραστές από την αγορά ενός προϊόντος που δεν έφτασε ποτέ στα χέρια του αγοραστή είτε από λάθος είτε από απάτη του πωλητή. Αυτό επιβαρύνει με επιπλέον κόστος τις συναλλαγές και ειδικότερα όταν στόχος μας είναι οι πολλές μικρές και έξυπνες συναλλαγές. [18]

Για αυτούς και άλλους λιγότερο σημαντικούς λόγους δημιουργήθηκε η ανάγκη για ένα σύστημα ηλεκτρονικών πληρωμών που θα βασίζεται στην κρυπτογραφικές τεχνικές απόδειξης, παρά στην αμοιβαία εμπιστοσύνη σε ένα κεντρικό διαμεσολαβητή. Με αυτό τον τρόπο επιτρέπεται σε οποιοδήποτε ζευγάρι χρηστών να συναλλάσσεται απευθείας, χωρίς τη διαμεσολάβηση ενός τρίτου έμπιστου προσώπου (τραπεζικό ίδρυμα). Σε αυτό το σύστημα οι πωλητές θα προστατεύονται από απάτες, καθώς οι συναλλαγές δε θα μπορούν να αντιστραφούν, αλλά και οι αγοραστές θα προστατεύονται από μηχανισμούς χρηματικής εγγύησης. Τα παραπάνω πλαίσιο αποτέλεσε τη βασική αιτία για τη δημιουργία των κρυπτονομισμάτων και ειδικότερα του πρώτου εξ αυτών δηλαδή του Bitcoin.

Κατά πάσα πιθανότητα στόχος του δημιουργού του Bitcoin ήταν να φέρει ριζικές αλλαγές στην οικονομία με αυτό τον τρόπο, έχοντας στην άκρη του μυαλού του την αποτυχία και τις επικίνδυνες συνέπειες που επιφέρει η κατάρρευση του τραπεζικού συστήματος. Πρόθεση του δεν ήταν να στοχοποιήσει ευθέως τους μεγάλους τραπεζικούς οργανισμούς, κάτι που θα στοχοποιούσε και θα δυσχέραινε την ανάπτυξη του νέου νομίσματος. Αντίθετα επιδίωξε να τους παρακάμψει, διαμορφώνοντας ένα δίκτυο γρηγορότερων, φθηνότερων και δίχως όρια συναλλαγών. Οι ημερομηνίες έκδοσης των πρώτων νομισμάτων αλλά και του founding paper έρχονται σε ημερομηνίες ορόσημα για την παγκόσμια οικονομία. Το λογισμικό του bitcoin ξεκίνησε να λειτουργεί στις 9 Ιανουαρίου του 2009, και το πρώτο μπλοκ δημιουργήθηκε στις 03/01/2009, ενώ το paper δημοσιεύθηκε στις 31/10/2008. Οι ημερομηνίες αυτές έρχονται μετά ακριβώς από το ξέσπασμα της παγκόσμιας χρηματοπιστωτικής κρίσης, που ξεκίνησε το 2008 στις ΗΠΑ, με αφετηρία την κατάρρευση του συστήματος των ενυπόθηκων στεγαστικών δανείων, που συμπαρέσυρε όλο το παγκόσμιο χρηματοπιστωτικό σύστημα. [8]

Δημιουργός του Bitcoin θεωρείται πως είναι ο Satoshi Nakamoto [9]. Πρόκειται για πρόσωπο αγνώστων λοιπών στοιχείων με αρκετές θεωρίες συνομωσίας γύρω από τη πραγματική ταυτότητα του. Είναι άγνωστη η εθνικότητα του, το πραγματικό του όνομα, οι σπουδές του και η επαγγελματική του δραστηριότητα. Σίγουρα το όνομα αυτό αποτελεί ψευδώνυμο ενώ επίσης είναι σχεδόν βέβαιο ότι πρόκειται για ομάδα ατόμων και όχι ένα μεμονωμένο προγραμματιστή-οικονομολόγο. Το όνομα Satoshi Nakamoto εμφανίζεται ως ο συγγραφέας της πρώτης επιστημονικής έκθεσης για το πρωτόκολλο λειτουργίας του bitcoin. Στις 31/10/2008 ο ίδιος ανακοίνωσε τη δημιουργία του Bitcoin σε διαδικτυακό φόρουμ ενώ επίσης ο Satoshi Nakamoto δημοσίευσε το ιστορικό πλέον paper “Bitcoin: A Peer-to-Peer Electronic Cash System”, που συνοδεύτηκε με την αρχή μιας νέας εποχής και ενός νέου κλάδου. Στη συνέχεια κυκλοφόρησε τη πρώτη έκδοση του Bitcoin λογισμικού στις 03/01/2009 όταν και εμφανίστηκε και επίσημα το block 0 (γνωστό και ως genesis block), ξεκινώντας έτσι την blockchain του bitcoin. Το πρώτο διάστημα μετά την αρχική έκδοση του συμμετείχε με άλλους προγραμματιστές στη βελτίωση και τη συντήρηση του project ενώ είναι αξιοσημείωτο ότι όλη η επικοινωνία ανάμεσα στα μέλη της κοινότητας που δούλευαν στο project γινόταν μέσα από κρυπτογραφημένα μέιλ, προστατεύοντας έτσι κάθε πληροφορία που έχει σχέση με την πραγματική του ταυτότητα. Στις πρώτες μέρες ύπαρξης και λειτουργίας του Bitcoin, υπήρχαν μόνο ελάχιστοι χρήστες που συμμετείχαν στο δίκτυο προσφέροντας την υπολογιστική τους ισχύ για τη σημαντικότερη διεργασία του δικτύου: το

mining. Οι απαιτήσεις σε hardware για το mining ήταν ακόμα αρκετά χαμηλές και έτσι κάθε χρήστης είχε τη δυνατότητα να μαζέψει για τον εαυτό του πλήθος νομισμάτων. Ο ίδιος ο Nakamoto φέρεται να έχει εξορύξει πάνω από 1 εκατομμύριο νομίσματα με το εξωφρενικότερο όλων όμως ότι κανένα από αυτά δεν έχει χρησιμοποιηθεί σε κάποιο transaction. Λαμβάνοντας υπόψη την κρυψίνοια του δημιουργού είναι εύκολα αντιληπτό ότι στόχος του ήταν να μην είναι δυνατόν με κανένα τρόπο να οδηγηθεί κάποιος στο πραγματικό πρόσωπο, που κρύβεται πίσω από το ψευδώνυμο Satoshi Nakamoto. Από τα τέλη του 2010, άρχισε να φθίνει η συμμετοχή του στην κοινότητα ενώ η τελευταία εμφάνισή του έγινε την άνοιξη του 2011, και έκτοτε δεν έχει δώσει άλλα σημεία ζωής.

Η τρέχουσα ονομαστική αξία του Bitcoin είναι $9.564,15 και το συνολικό πλήθος των νομισμάτων σε κυκλοφορία είναι 18.391.518 BTC. Αυτό οδηγεί σε μια τρέχουσα κεφαλαιοποίηση της τάξης των $175.899.236.879. Από την εμφάνιση του BTC σε κυκλοφορία μέχρι και τον Ιούλιο του 2017, η ονομαστική αξία του BTC και αντίστοιχα ο δείκτης κεφαλαιοποίησης του κυμαίνονταν σε χαμηλά επίπεδα. Από τον Ιούλιο του 2017 μέχρι και τα μέσα του Δεκεμβρίου του 2017, παρουσιάστηκε μία ταχεία άνοδος στην ονομαστική του αξία. Αξίζει σε αυτό το σημείο να σημειωθεί, όπως θα φανεί και παρακάτω στην τρέχουσα εργασία, ότι η άνοδος και η πτώση του Bitcoin συμπαρασύρει σε μεγάλο βαθμό την κίνηση της συντριπτικής πλειοψηφίας των υπολοίπων κρυπτονομισμάτων, χωρίς αυτό να σημαίνει ότι και πολλοί άλλοι εξωγενείς παράγοντες δεν παίζουν ρόλο στην πορεία της τιμής τους. Ύστερα από τη περίοδο όπου παρατηρήθηκε η υψηλότερη τιμή του, παρατηρούμε σύντομες περιόδους συνεχών αυξομειώσεων. Η ονομαστική αξία του BTC παρουσίασε ιστορικό υψηλό στις 17/12/2017, προσεγγίζοντας τα $ 20.089 με την αξία αυτή να αντιστοιχεί σε Market Cap της τάξης των $ 336.433.998.575 ενώ το ιστορικό χαμηλό στις 05/07/2013, φτάνοντας τα $ 65,53. Η αξία αυτή αντιστοιχούσε σε Market Cap της τάξης των $ 745.297.638. Παρ ’όλα αυτά το BTC διατηρεί εδώ και χρόνια τη υψηλότερη θέση στη κατάταξη των κρυπτονομισμάτων με βάση το Market Cap με αποτέλεσμα να εντάσσεται στα large cap κρυπτονομίσματα. [7,23]

Όπως αναφέραμε και νωρίτερα το πρωτόκολλο του Bitcoin, όπως και των υπόλοιπων κρυπτονομισμάτων, λειτουργεί αποκεντρωμένα, χωρίς την ύπαρξη και τη διαμεσολάβηση μίας κεντρικής αρχής (π.χ. τράπεζα). Η νομισματική πολιτική του Bitcoin αποτελεί το σύνολο των κανόνων, με τους οποίους εισέρχονται νέα νομίσματα (BTC) στο δίκτυο κάτι που βασίζεται στο ρυθμό παραγωγής νέων νομισμάτων. Κάθε νέο νόμισμα που αδυνατεί να ακολουθήσει τους κανόνες που έχουν οριστεί για κάποιο λόγο (έλλειψη γνησιότητας) απορρίπτεται και έτσι δεν εισέρχεται στην αλυσίδα του Blockchain και δεν αποκτά αξία. Παρ ’όλα αυτά το πρωτόκολλο του Bitcoin μπορεί να θέσει σε κυκλοφορία συγκεκριμένο αριθμό κρυπτονομισμάτων κάτι που έρχεται σε αντίθεση με το παραδοσιακό τραπεζικό σύστημα και τις νομισματικές πολιτικές που ακολουθούνται σε όλες τις οικονομίες του κόσμου. Με βάση το χρηματοοικονομικό σύστημα που επικρατεί σήμερα, δεν υπάρχει ανώτατο όριο στη ποσότητα του χρήματος που μπορεί να κοπεί και να κυκλοφορήσει. Άσχετα με αυτό ωστόσο είναι γνωστό ότι τα χρήματα δεν κόβονται αυθαίρετα και ανεξέλεγκτα καθώς ο ρυθμός δημιουργίας ελέγχεται με βάση συγκεκριμένους κανονισμούς. Από την άλλη μεριά ο μόνος τρόπος με τον οποίο τίθονται σε κυκλοφορία νέα νομίσματα στη πλατφόρμα του Bitcoin είναι μέσω της διαδικασίας του mining. Μέσω αυτής της διαδικασίας κάθε φορά που επιβεβαιώνεται ένα μπλοκ συναλλαγών και εισέρχεται στο blockchain εισέρχονται στο δίκτυο νέα νομίσματα. Είναι εύκολα κατανοητό επομένως ότι ο χρόνος δημιουργίας ενός νέου μπλοκ εξαρτάται άμεσα με των αριθμό των νέων νομισμάτων που τίθονται σε κυκλοφορία. Το πρωτόκολλο του Bitcoin (όπως και τα περισσότερα πρωτόκολλα που

βασίζονται στον PoW μηχανισμό) πρέπει να διατηρεί το ρυθμό δημιουργίας ενός νέου μπλοκ σταθερό στα 10 λεπτά περίπου, ανεξάρτητα από τη συνολική υπολογιστική ισχύ που συνεισφέρει στο mining. Καταλαβαίνουμε λοιπόν ότι η διαδικασία σταθεροποίησης του ρυθμού δημιουργίας νέων νομισμάτων επιτυγχάνεται μέσω της αναπροσαρμογής της δυσκολίας της λύσης του αλγορίθμου του mining.

Ο ρυθμός δημιουργίας νέων μπλοκ ρυθμίζεται κάθε 2016 μπλοκ κάτι που σημαίνει πως αν προστίθεται 1 μπλοκ κάθε 10 λεπτά στη blockchain, ο ρυθμός δημιουργίας νέων μπλοκ ρυθμίζεται κάθε 2 εβδομάδες. Το πλήθος των bitcoin που δημιουργούνται ανά μπλοκ(και άρα το reward του miner για την αποτελεσματική δραστηριότητα του) είναι ρυθμισμένο να μειώνεται με ρυθμούς γεωμετρικής προόδου, με μείωση στο μισό κάθε 210.000 μπλοκ, ή κάθε 4 χρόνια προσεγγιστικά. Η διαδικασία αυτή ονομάζεται halving και αξίζει να σημειωθεί ότι κατά τη συγγραφή της παρούσας εργασίας έλαβε χώρα το τρίτο halving στην ιστορία του Bitcoin. Γίνεται εύκολα αντιληπτό ότι το ίδιο το πρωτόκολλο προφυλάσσεται από τη γρήγορη εξάντληση των αποθεμάτων του bitcoin και από φαινόμενα πληθωρισμού.

Οι παραπάνω κανόνες, όπως η μείωση του reward κάθε 4 χρόνια, αποτελούν αυθαίρετες συμβάσεις οι οποίες εξυπηρετούν τη βιωσιμότητα του νομίσματος ενώ ο δημιουργός του Bitcoin ποτέ δεν δικαιολόγησε τη λογική πίσω από την επιλογή του μεγέθους αυτών των σταθερών. Διάφορες εκτιμήσεις που έχουν γίνει γύρω από αυτές τις σταθερές καταλήγουν στο ότι με αυτό τον ρυθμό εξόρυξης, το συνολικό πλήθος των Satoshis (η μικρότερη υποδιαίρεση του Bitcoin 10^{-8}) που μπορούν να εξορυχθούν προσεγγίζει τη μέγιστη χωρητικότητα ενός 64-bit αριθμού κινητής υποδιαστολής. Με παρόμοιο τρόπο ορίζεται και το άνω όριο των νομισμάτων που μπορούν να δημιουργηθούν το οποίο κατά προσέγγιση είναι 21.000.000 BTC (για την ακρίβεια 20.999.999,9769 BTC). Από αυτά πάνω 18 εκατομμύρια βρίσκονται ήδη σε κυκλοφορία.

Ο ακριβής ρυθμός μείωσης του reward από το mining δε μπορεί να υπολογιστεί με ασφάλεια καθώς οι μεταβολές στην συνολική υπολογιστική ισχύ του συστήματος επηρεάζουν άμεσα και το difficulty του mining. Για παράδειγμα μια ξαφνική απομάκρυνση των μεγάλων miner από το δίκτυο του Bitcoin θα είχε τρομερές επιπτώσεις στη δυσκολία του αλγορίθμου. Ενδιαφέρον παρουσιάζει το γεγονός πως αν η συνολική υπολογιστική ισχύ είχε παραμείνει σταθερή από τη στιγμή της εξόρυξης των πρώτων νομισμάτων τότε το τελευταίο νόμισμα θα εξορυσσόταν περίπου το Δεκέμβριο του 2140. Επειδή όμως δεν μπορούμε να προβλέψουμε με σιγουριά τις μεταβολές που θα γίνουν στις τεχνικές λεπτομέρειες του πρωτοκόλλου του bitcoin, είναι αδύνατο να υπολογίσουμε την ακριβή ημερομηνία εξόρυξης του τελευταίου νομίσματος. Τα νομίσματα που δεν έχουν ακόμα τεθεί σε κυκλοφορία βρίσκονται μέσα ένα pool έως ότου ο επόμενος miner τα εξορύξει.

Το μεγαλύτερο μέρος του reward που λαμβάνει ένας miner προέρχεται από τη βασική του εργασία δηλαδή να δημιουργεί νέα μπλοκ έγκυρων συναλλαγών και να τα τοποθετεί στην αλυσίδα του blockchain. Μικρότερο μέρος της ανταμοιβής προέρχεται από τα τέλη που συνοδεύουν τις συναλλαγές. Επομένως όταν εξαντληθούν όλα τα αποθέματα των νομισμάτων, τα τέλη συναλλαγών θα αποτελούν το βασικό κίνητρο για τους miners να συμμετέχουν στο δίκτυο και να συνεχίζουν τη δραστηριότητά τους, που αποτελεί τη ραχοκοκαλιά του δικτύου. Προκύπτει επομένως το εξής εύλογο ερώτημα: σε περίπτωση που οι miners ανταμείβονται μόνο από τα τέλη συναλλαγών, δεν είναι λογικό αυτά να αυξηθούν με αποτέλεσμα να χαθεί ένα από τα βασικά πλεονεκτήματα του BTC που είναι τα χαμηλά τέλη; Η λύση σε αυτό το μελλοντικό πρόβλημα δεν έχει ακόμα δοθεί. [24]

Αξίζει να σημειωθεί ότι δεν είναι δυνατόν όλο το πλήθος των νομισμάτων να ξοδευτεί στο σύνολο του. Το συνολικό απόθεμα των νομισμάτων που μπορούν να ξοδευτούν θα είναι πάντα μικρότερο σε σχέση με το πλήθος των νομισμάτων που μπορούν να εξορυχθούν λόγω

διάφορων τεχνικών ανεπαρκειών και ζημιών όπως μη αναστρέψιμες βλάβες σε σκληρούς δίσκους με απώλεια δεδομένων, κακόβουλων ενεργειών όπως τη κλοπή ιδιωτικών κλειδιών, αλλά και λόγω οικειοθελούς καταστροφής. Επίσης νομίσματα μπορεί να χαθούν όταν οι συνθήκες των συναλλαγών πάψουν να είναι πλέον γνωστές. Για παράδειγμα, για να πραγματοποιηθεί μία συναλλαγή σε μία συγκεκριμένη διεύθυνση, απαιτείται ένα ιδιωτικό κλειδί το οποίο σε περίπτωση που χαθεί για οποιοδήποτε λόγο, τα νομίσματα που συμμετείχαν στη συναλλαγή θεωρούνται χαμένα. Είναι θεωρητικά αδύνατο να βρεθεί ξανά κλειδί που να ταιριάζει στην περίπτωση αυτή. Τέλος τα νομίσματα μπορούν να καταστραφούν οικειοθελώς με χαρακτηριστικότερο παράδειγμα τα στοιχεία των νομισμάτων που τροποποιούνται ώστε να αδύνατο να τα ξοδέψουμε.

2.2 Bitcoin Cash

Η δημιουργία του Bitcoin Cash προήλθε από τη μακρά διαφωνία μεταξύ μελών της ψηφιακής κοινότητας του Bitcoin που αφορούσε κάποιες προτεινόμενες αλλαγές για ταχύτερες συναλλαγές ανάμεσα στους χρήστες. Οι εν λόγω διαφωνούντες προγραμματιστές και οι αντίστοιχοι miners χώρισαν στα δύο τον κώδικα λογισμικού του Bitcoin, προκαλώντας μια «διακλάδωση» (hard fork) στο blockchain του. Έτσι τελικά δημιουργήθηκε η καινούργια αλυσίδα το λεγόμενο Bitcoin Cash.

Αν και το Bitcoin Cash χαρακτηρίζεται ως μια δεύτερη πολύ παρόμοια εκδοχή του Bitcoin, διαθέτει μία αρκετά σημαντική διαφορά: το μέγεθος των blocks. Το μέγεθος των blocks αυξήθηκε από το 1 MB που ήταν ως τότε στο Bitcoin σε 8 MB πετυχαίνοντας το στόχο που είχαν θέσει εξαρχής οι miners, που δεν ήταν άλλος από την αύξηση των συναλλαγών. Ορισμένες αισιόδοξες εκτιμήσεις προβλέπουν ότι το νέο αυτό παρακλάδι του Bitcoin Θα μπορέσει μελλοντικά να ανταγωνιστεί κολοσσούς όπως οι VISA, MasterCard και PayPal από πλευράς πλήθους συναλλαγών.

Ένα ζήτημα το οποίο είναι υπό συζήτηση, και τελικά μόνο ο χρόνος είναι ικανός να το ξεκαθαρίσει, αφορά στους χρήστες του Bitcoin Cash καθώς με την αύξηση του μεγέθους των block, απαιτείται και ανάλογη αύξηση της υπολογιστικής ισχύος. Αυτή η αύξηση μπορεί να οδηγήσει στην περιθωριοποίηση των «μικρών» miners και την ταυτόχρονη εδραίωση και συγκέντρωση της υπολογιστικής ισχύος του Bitcoin Cash, στα χέρια μεγάλων εταιριών που διαθέτουν πόρους για τον εξοπλισμό που απαιτείται. Αυτό έρχεται σε ευθεία αντίθεση με τον αρχικό στόχο τον κρυπτονομισμάτων που είναι η κατανομή της υπολογιστικής ισχύος σε όσους το δυνατόν περισσότερους χρήστες ώστε να διασφαλιστεί και η ακεραιότητα του blockchain.

Το Bitcoin Cash ξεκίνησε την διαπραγμάτευσή του στην αγορά στα τέλη Ιουλίου του 2017. Στις 03/08/2017 η τιμή του BCH ήταν $399,00 εμφανίζοντας τεράστια αύξηση λίγους μήνες αργότερα η οποία έφτασε το ποσοστό του 929%, στις 20/12/2017 όπου το ένα BCH κόστιζε $4.104,3. Στις 15 Νοεμβρίου 2018, πραγματοποιήθηκε ένας ακόμη διαχωρισμός του Bitcoin Cash μέσω και πάλι hard forking. Τα 2 νέα νομίσματα Bitcoin Cash και Bitcoin SV. Στις 15 Νοεμβρίου 2018 το Bitcoin Cash διαπραγματεύτηκε στα 289 $ περίπου, από 425,01 $ στις 14 Νοεμβρίου πριν το διαχωρισμό, και το Bitcoin SV διαπραγματεύτηκε στα 96,50 $ περίπου. Η διάσπαση προήλθε από αυτό που περιεγράφηκε ως "εμφύλιος πόλεμος" σε δύο

ανταγωνιστικά στρατόπεδα του Bitcoin Cash. Το πρώτο στρατόπεδο, υποστηριζόμενο από τον επιχειρηματία Roger Ver και τον Jihan Wu της Bitmain, προώθησε το λογισμικό με τίτλο Bitcoin ABC το οποίο θα διατηρούσε το μέγεθος του μπλοκ στα 32MB. Το δεύτερο στρατόπεδο με επικεφαλής τον Craig Steven Wright και τον δισεκατομμυριούχο Calvin Ayre παρουσίασε μια ανταγωνιστική έκδοση λογισμικού στη οποία βασίστηκε το Bitcoin SV (Satoshi Vision), που θα αύξανε το όριο μεγέθους του μπλοκ στα 128MB.

Πλέον η τιμή του BCH έχει κυμαίνεται κοντά στα $236, με τρομερά ποσοστά διακύμανσης όμως (κάτι που ισχύει για τη συντριπτική πλειοψηφία των κρυπτονομισμάτων). Στην αγορά κυκλοφορούν σήμερα (5/2020) περίπου 18,4 εκατομμύρια Bitcoin Cash, από το όριο των 21 εκατομμυρίων. [2]

2.3 Ethereum

Πριν προσπαθήσουμε να περιγράψουμε το σκοπό για τον οποίο σχεδιάστηκε η πλατφόρμα του Ethereum, στην οποία βασίζεται το ether, θα προσπαθήσουμε να αναλύσουμε το σκοπό ανάπτυξης του Bitcoin, αλλά και τα ίδια τα χαρακτηριστικά του διαδικτύου. Βασική επιδίωξη κατά τη δημιουργία του Bitcoin ήταν να δημιουργηθεί ένα peer2peer και ανοικτού κώδικα σύστημα το οποίο θα αξιοποιεί κρυπτονομίσματα με τη χρήση κρυπτογραφίας και κυρίως της τεχνολογίας Blockchain. Κύριο χαρακτηριστικό του είναι ο αποκεντρωμένος χαρακτήρας του, κάτι που συνεπάγεται ότι δεν υπάρχει ούτε κάποια κεντρική αρχή που να ρυθμίζει το δίκτυο των χρηστών και την υποδομή του συστήματος, ούτε κάποιος διαμεσολαβητής για τις συναλλαγές των χρηστών. Με αυτό το τρόπο, δημιουργήθηκε μία πλήρως ανεξάρτητη peer2peer εκδοχή κρυπτονομισμάτων. Στο ιδανικό σενάριο της ευρείας χρήσης του Bitcoin, ως πλατφόρμα ηλεκτρονικών συναλλαγών, από τη πλειοψηφία των χρηστών του διαδικτύου εφαρμογές όπως το PayPal ή το OnLine banking των τραπεζών θα δέχονταν σοβαρότατο πλήγμα και πιθανώς θα παραγκωνίζονταν και τελείως.

Το βασικό πρόβλημα στο ζήτημα της ύπαρξης μιας κεντρικής αρχής ως διαμεσολαβητής στο client-server μοντέλο σχετίζεται με την εξουσία και την ισχύ που έχει αυτή η αρχή πάνω στο δίκτυο, στους χρήστες και στα ίδια τα δεδομένα. Η κεντρική αυτή αρχή από τη μία αξιοποιεί εξειδικευμένο προσωπικό και εξοπλισμό για την ποιοτική και άμεση εξυπηρέτηση των χρηστών ενώ από την άλλη έχει τη πλήρη έλεγχο σε όλες τις ενέργειες των χρηστών και μπορεί να αποκτήσει πρόσβαση σε προσωπικά μας δεδομένα. Για παράδειγμα, μία τράπεζα, μπορεί να διατηρεί τα τραπεζικά αποθέματα ασφαλή, αλλά μπορεί επίσης να μπλοκάρει τις αναλήψεις ή να εκθέσει τα προσωπικά μας δεδομένα, όπως το ιστορικό συναλλαγών, ονοματεπώνυμο και στοιχεία επικοινωνίας σε τρίτους. Από τη στιγμή που το κοινό θα εμπιστευόταν και χρησιμοποιούσε μαζικά ένα peer2peer σύστημα συναλλαγών, οι υπηρεσίες που βασίζονται σε μία κεντρική αρχή όπως οι τραπεζικοί οργανισμοί θα οδηγούνταν σταδιακά σε απαξίωση από το κοινό. [11]

Εδώ εντάσσεται και η αντιπαράθεση για τον ίδιο των χαρακτήρα του διαδικτύου. Είναι ευρέως διαδεδομένη η άποψη πως το διαδίκτυο έχει αποκεντρωμένο χαρακτήρα κάτι το οποίο όμως δεν έχει καμία σχέση με την πραγματικότητα. Τεχνολογικοί κολοσσοί, όπως η Google, η Amazon το Facebook, και αρκετοί άλλοι ασκούν μεγάλη επιρροή και έλεγχο πάνω στο διαδίκτυο. Όλα τα προσωπικά μας δεδομένα, κωδικοί, ιστορικά αναζήτησης, συναλλαγές, ιατρικές και προσωπικές πληροφορίες, βρίσκονται αποθηκευμένα σε clouds και servers που

ελέγχονται από τις προαναφερθείσες επιχειρήσεις. Μπορεί επομένως να απολαμβάνουμε ποιοτικές υπηρεσίες και εφαρμογές, αλλά ελλοχεύει ο κίνδυνος όλα αυτά τα δεδομένα μπορεί να αξιοποιηθούν με ή χωρίς τη συγκατάθεση μας για θεμιτούς και αθέμιτους σκοπούς όπως στοχευμένες διαφημίσεις και προτάσεις, κλοπές, απάτες, χειραγώγηση κοινού και πολιτική επιρροή. Έτσι, το διαδίκτυο έπρεπε να αποκεντρωθεί, ώστε να μην είναι πλήρως ελέγξιμο από αυτές τις επιχειρήσεις. Το γεγονός αυτό αποτέλεσε το βασικό κίνητρο του δημιουργού του Ethereum ο οποίος προσπάθησε να αναπτύξει μία πλατφόρμα στην οποία είναι δυνατή η σχεδίαση αποκεντρωμένων υπηρεσιών καθώς και του αντίστοιχου νομίσματος. Επομένως, θα ήταν εφικτό να επαναπροσδιορίσουμε το μοντέλο client-server, καθιστώντας αχρείαστους τους διαμεσολαβητές και τα third parties. Στην ουσία αποτελεί μία γενίκευση της σκεπτικού που υπάρχει πίσω από το bitcoin μέσω του συνδυασμού2 παραγόντων:

1) μόνο ο δημιουργός έχει έλεγχο (προσθήκη, επεξεργασία, διαγραφή) πάνω στα δεδομένα που δημιουργεί και εισάγει

2) τα δεδομένα αυτά μπορούν να μεταδοθούν σχεδόν ακαριαία στο δίκτυο, ενημερώνοντας άμεσα όλους τους ενδιαφερόμενους χρήστες.

Ο πατέρας και δημιουργός του project του Ethereum είναι ο Vitalik Buterin [10], προγραμματιστής που γεννήθηκε το 1994 στη Ρωσία και μεγάλωσε στον Καναδά. Ο Buterin συνέγραψε τη σχετική επιστημονική αναφορά κατά την εισήγηση του Ethereum ενώ είναι συνεργάτης και του περιοδικού Bitcoin Magazine. Στη διαδρομή της ανάπτυξης του Ethereum, μία σειρά από ερευνητές συνέβαλλαν καθοριστικά στην επιτυχία της πλατφόρμας όπως ο Dr Gavin Good που θεωρείται συνιδρυτής καθώς συνέγραψε το yellow paper για το Ethereum. Συγκεκριμένα, περιέγραψε τις τεχνικές λεπτομέρειες για όλη τη λειτουργία του EVM (ethereum virtual machine) που διαχειρίζεται όλο το ledger και εκτελεί τα smart contracts. Επίσης ο Dr. Joseph Lubin (θεωρείται και αυτός συνιδρυτής) βοήθησε στην εξάπλωση του κρυπτονομίσματος μέσω συγκεκριμένης start-up εταιρείας, που αξιοποιεί τη πλατφόρμα του Ethereum για τη σχεδίαση αποκεντρωμένων εφαρμογών. Πέρα από τους επώνυμους συνεργάτες ωστόσο, υπήρξαν και αρκετοί υποστηρικτές που βοήθησαν στα πρώτα βήματα του project. Το εγχείρημα είχε ανάγκη από οικονομική στήριξη γι' αυτό και διάφοροι ενδιαφερόμενοι συνεισέφεραν στο Ethereum με την αγορά Ether. Με αυτό το τρόπο συγκεντρώθηκαν πάνω από 18 εκ δολάρια για να εκκινήσει και να αναπτυχθεί η λειτουργία της πλατφόρμας.

Η τρέχουσα ονομαστική αξία του Ether είναι $ 207.55 και το σύνολο των νομισμάτων που βρίσκονται σε κυκλοφορία είναι περίπου 111 εκατομμύρια Ether. Το τρέχον Market Capitalization κυμαίνεται γύρω στα 23.063.500.000 δολάρια επομένως εύκολα καταλαβαίνει κανείς ότι ανήκει στα large cap κρυπτονομίσματα. Από την εμφάνιση της πλατφόρμας του Ethereum, η ονομαστική αξία του Ether βρισκόταν σε χαμηλά επίπεδα. Από την άνοιξη του 2017 όμως άρχισε να παρουσιάζει σταδιακή αύξηση με αποκορύφωμα τον Ιανουάριο του 2018. Από εκεί και μετά, παρουσιάζει συνεχώς αυξομειώσεις σε χαμηλότερα επίπεδα.

Η ονομαστική αξία του Ether (ETH) παρουσίασε ιστορικό υψηλό, τα $1432,88, στις 13/01/2018. Η αξία αυτή αντιστοιχούσε σε $35.400.735.922 Market Capitalization. Από την άλλη το ιστορικό χαμηλό ήταν τα $0,420897, στις 21/10/2015. Η αξία αυτή αντιστοιχούσε σε $33.150.826 Market Capitalization. [7]

Η ετήσια έκδοση νομισμάτων για το δίκτυο του Ethereum προσεγγίζει περίπου το 4,5% των συνολικά διαθέσιμων κρυπτονομισμάτων. Το reward για κάθε μπλοκ είναι 2 Ether και ένα επιπρόσθετο 1,75 Ether για το uncle μπλοκ. Επίσης, προστίθενται και άλλα τέλη συναλλαγών στο reward ενός miner, το λεγόμενο και Gas. Κάθε μπλοκ που παράγεται στο δίκτυο του Ethereum επιβραβεύει με ένα ποσό-ανταμοιβή τον επιτυχημένο miner ενώ ο ίδιος

λαμβάνει περίπου 75% του reward του μπλοκ για κάθε uncle μπλοκ. Από τη λειτουργία του Ethereum, το block reward έχει λάβει τις εξής τιμές:

Block 0 μέχρι και Block 4,369,999: 5 Ether

Block 4,370,000 μέχρι και 7,280,000: 3 Ether

Block 7,280,000 έως τώρα: 2 Ether

Οι μεταβολές δε προέκυψαν από κάποιο εσωτερικό κανονισμό του πρωτοκόλλου, όπως για παράδειγμα στη περίπτωση του Bitcoin (το γνωστό και ως halving). Αντιθέτως, προτάθηκαν για μία σειρά από τεχνικούς και οικονομικούς λόγους και υιοθετήθηκαν εν τέλει. Όπως είναι αναμενόμενο ο ρυθμός έκδοσης νέων νομισμάτων επηρέασε και τη ταχύτητα παραγωγής των μπλοκ.

Τέλος θα αναφερθούμε στις συναλλαγές που υποστηρίζονται από το Ethereum. Με τον όρο transaction (συναλλαγή) στη πλατφόρμα του Ethereum αναφερόμαστε σε ένα πακέτο δεδομένων με ψηφιακή υπογραφή. Το πακέτο αυτό περιλαμβάνει ένα μήνυμα, το οποίο χρειάζεται να σταλεί σε έναν externally owned account. Μία transaction περιλαμβάνει το αναγνωριστικό για τον παραλήπτη, μία υπογραφή η οποία λειτουργεί ως αναγνωριστικό για τον αποστολέα, την ποσότητα του ether που μεταβιβάζεται από τον αποστολέα στον παραλήπτη, ένα προαιρετικό data field, ένα παράγοντα με το όνομα STARTGAS, ο οποίος αντιστοιχεί στον μέγιστο αριθμό υπολογιστικών βημάτων που απαιτούνται για την εκτέλεση της συναλλαγής και ένα παράγοντα, με όνομα GASPRICE, ο οποίος αντιστοιχεί στο χρηματικό τέλος, το οποίο πληρώνει ο αποστολέας σε κάθε υπολογιστικό βήμα. Οι 3 πρώτοι παράγοντες είναι κοινοί σε κάθε κρυπτονόμισμα ενώ το data field αξιοποιείται στις περιπτώσεις, όπου έχουμε υλοποίηση smart contract.

2.4 Ripple

Όπως είναι γνωστό το πρωτόκολλο HTTP συνέβαλε στη γιγάντωση του διαδικτύου, επιτρέποντας την άμεση και ταχύτατη επικοινωνία ανάμεσα στους χρήστες. Ωστόσο, μία σειρά από άλλα συστήματα, με χαρακτηριστικότερο παράδειγμα το τραπεζικό, δεν επιτρέπει τη ταχύτατη μετάδοση των συναλλαγών. Ο βασικός λόγος σχετίζεται με τα απαρχαιωμένα συστήματα που αξιοποιούν οι τραπεζικοί οργανισμοί για τις συναλλαγές. Παράλληλα, μία σειρά από εφαρμογές μεταφοράς χρημάτων, όπως το Swift, το MoneyGram και η Western Union παρέχουν εκτός από αργές, αξιοσημείωτα ακριβές υπηρεσίες στους χρήστες.

Στα παραπάνω μειονεκτήματα έρχεται να προστεθεί και η ίδια η δομή του τραπεζικού συστήματος. Δεν υπάρχει ένα ενιαίο δίκτυο στο οποίο συμμετέχουν όλες οι τράπεζες και μέσω του οποίου πραγματοποιούν τις μεταξύ τους συναλλαγές με αποτέλεσμα να μην υπάρχει ευθεία επικοινωνία ανάμεσα στους τραπεζικούς οργανισμούς. Από την άλλη, η επικοινωνία αυτή συχνά απαιτεί μία σειρά από ενδιάμεσους κόμβους, ώστε να πραγματοποιηθεί με επιτυχία, κάτι που καθιστά τη προαναφερθείσα διασύνδεση χρονοβόρα και δαπανηρή για τους χρήστες. [13]

Ακόμα και να υπήρχε ευθεία επικοινωνία ανάμεσα στους τραπεζικούς οργανισμούς, δεν είναι εγγυημένο ότι υπάρχουν και τα ανάλογα αποθέματα για να πραγματοποιηθεί μία συναλλαγή. Στην περίπτωση που 2 χρήστες θέλουν να μεταφέρουν μεταξύ τους ένα χρηματικό ποσό για το οποίο υπάρχει επάρκεια αποθέματος και στις 2 τράπεζες το πρόβλημα είναι αρκετά εύκολο. Τί γίνεται στην περίπτωση που η μεταφορά του ποσού πρέπει να γίνει

ανάμεσα σε 2 τραπεζικούς οργανισμούς 2 διαφορετικών χωρών με διαφορετικό νόμισμα. Σε αυτή τη περίπτωση θα χρειαστεί να μετατραπεί το ποσό από το ένα νόμισμα στο άλλο. Ωστόσο, συχνά κάτι τέτοιο δεν είναι εφικτό, καθώς είναι αδύνατο κάθε τράπεζα να διαθέτει επαρκές συνάλλαγμα για κάθε συναλλαγή. Με βάση τα παραπάνω, παρατηρούμε πως προκύπτει μία πολύπλοκη κατάσταση με κόστος χρόνου και χρήματος.

Σε αυτήν την πολύπλοκη κατάσταση, ήρθε να δώσει τη λύση το δίκτυο και το πρωτόκολλο του Ripple. Βασικό κίνητρο της ανάπτυξής τους ήταν η απευθείας πραγματοποίηση συναλλαγών ανάμεσα στους τραπεζικούς οργανισμούς και η μείωση των τελών ανάμεσα στις συναλλαγές. Τα Ripple Labs, είχαν ως στόχο τη δημιουργία του "Internet of Value", μια πρωτοποριακή μέθοδο πραγματοποίησης συναλλαγών το ίδιο ταχύτατα, όπως μεταφέρεται η πληροφορία. Μέσα από το RippleNet, ένας χρήστης δεν θα περιμένει αλλά ούτε θα χρεωθεί υπερβολικά για την τέλεση μιας συναλλαγής. Γι' αυτό ακριβώς το λόγο θεωρείται ότι η φιλοσοφία γύρω από το RippleNet απέχει αρκετά από αυτή του Bitcoin. Στη περίπτωση του Ripple, δημιουργήθηκε ένα δίκτυο, ώστε να βελτιώσει την αποτελεσματικότητα του τραπεζικού συστήματος ενώ με τη περίπτωση του Bitcoin επιχειρείται η παράκαμψη του για τη πραγματοποίηση ανεξάρτητων από χρηματοπιστωτικά ιδρύματα συναλλαγών.

Υπάρχει μία σύγχυση γύρω από το Ripple, καθώς πολλές φορές το κρυπτονόμισμα, η πλατφόρμα και η εταιρεία που τη συντηρεί ταυτίζονται λανθασμένα. Αν θέλουμε να είμαστε ακριβείς το Ripple αντιστοιχεί στην ονομασία της εταιρίας, που παρέχει υπηρεσίες για την αποστολή χρημάτων παγκοσμίως, ο όρος XRP αντιστοιχεί στο ψηφιακό νόμισμα που υιοθετείται στις συναλλαγές ενώ το πρωτόκολλο που χρησιμοποιείται από τους nodes του δικτύου ονομάζεται rippled. Πολλές φορές χρησιμοποιούμε καταχρηστικά τον όρο Ripple για τη περιγραφή είτε της πλατφόρμας δικτύου είτε του νομίσματος που αξιοποιεί κάτι το οποίο όμως δεν είναι σωστό και πολλές φορές οδηγεί σε παρανοήσεις. [12]

Η ανάπτυξη της πλατφόρμας και του δικτύου του Ripple, όπως και για τα περισσότερα κρυπτονομίσματα, δεν έγινε αποκλειστικά από ένα άτομο αλλά πιστώνεται σε μία σειρά από πρόσωπα. Πρώτος, ο Ryan Fugger συνέλαβε την ιδέα το 2004, εργαζόμενος πάνω σε ένα σύστημα ηλεκτρονικών συναλλαγών στο Βανκούβερ ενώ βασιζόμενος πάνω σε αυτή την ιδέα ανέπτυξε τη πρώτη εφαρμογή του συστήματος, το RipplePay.com. Στη συνέχεια το Μάιο του 2011 ο Jed McCaleb ξεκίνησε την ανάπτυξη ενός συστήματος ψηφιακών νομισμάτων για το οποίο ο έλεγχος για την εγκυρότητα των συναλλαγών θα βασιζόταν σε αλγόριθμο εξασφάλισης συναίνεσης (consensus algorithm), και όχι μέσα από τη διαδικασία του mining. Ο Jed McCaleb είναι Αμερικάνος προγραμματιστής και επιχειρηματίας. Μέχρι το 2013, διατηρούσε τη θέση του CTO της Ripple ενώ αργότερα συμμετείχε στην ίδρυση ενός άλλου πολύ δημοφιλούς κρυπτονομίσματος, του Stellar. Ο ίδιος έχει υπάρξει δημιουργός της P2P εφαρμογής του eDonkey.

Τον Αύγουστο του 2012, ο Jed McCaleb μαζί με τον Chris Larsen προσέγγισαν τον Ryan Fugger, ώστε να αξιοποιήσουν την προ οκταετίας ιδέα του. Ο Chris Larsen είναι επιχειρηματίας ο οποίος αποτέλεσε συνιδρυτής μίας σειράς από start-ups, που σχετίζονται με P2P εφαρμογές δανεισμού. Ο ίδιος το 1996, συνίδρυσε την E-Loan, μία αρκετά επιτυχημένη επιχείρηση ηλεκτρονικών δανείων Έπειτα από συμφωνία και των 3 προχώρησαν στο στήσιμο μιας εταιρείας η οποία ξεκίνησε την ανάπτυξη του πρωτοκόλλου του Rippled(RTXP) και του δικτύου των συναλλαγών. Τον Σεπτέμβριο του 2013 η εταιρεία αυτή παίρνει το γνωστό σημερινό της όνομα (Ripple Labs) ενώ την ίδια περίοδο, ο CTO της εταιρείας, Stefan Thomas, ανακοινώνει το source code για την υλοποίηση των κόμβων του P2P δικτύου.

Η τρέχουσα ονομαστική αξία του XRP είναι $0.205253 και το συνολικό πλήθος των νομισμάτων σε κυκλοφορία είναι περίπου 44.112.800.000 XRP. Αυτό αντιστοιχεί σε ένα

τρέχον Market Capitalization της τάξης των $9.054.284.538. Από την εμφάνιση του XRP μέχρι και το καλοκαίρι του 2017, η ονομαστική του αξία και αντίστοιχα το Market Cap του βρίσκονταν σε χαμηλά επίπεδα. Από εκείνο το σημείο και έπειτα συμπαρασυρόμενο από την άνοδο και των υπόλοιπων κρυπτονομισμάτων, η αξία του εκτινάχθηκε. Στη συνέχεια, παρουσίαζε αυξομειώσεις, σε σταθερά χαμηλότερα όμως επίπεδα. Η ονομαστική αξία του XRP παρουσίασε ιστορικό υψηλό ($3,84) στις 04/01/2018 που αντιστοιχούσε σε 123.834.712.592$ αξία κεφαλαιοποίησης ενώ το ιστορικό χαμηλό ($0.002802) παρατηρήθηκε στις 07/07/2014 με αξία κεφαλαιοποίησης τα 24.096.300$. Το XRP κατατάσσεται στα large cap νομίσματα.

Σε αντίθεση με άλλα κρυπτονομίσματα, τα Ripple Labs έχουν επιλέξει να τροφοδοτήσουν το δίκτυο του Ripple με ένα συνολικό απόθεμα 100.000.000.000 νομίσματα XRP. Το Ripple δε διαθέτει διαδικασία mining επομένως όλο το παραπάνω ποσό έχει δημιουργηθεί από τους ιδρυτές του κρυπτονομίσματος πριν από την κυκλοφορία του. Τα υπάρχοντα Ripple έχουν κατανεμηθεί ως εξής [7]:

- 20 δις νομίσματα XRP έχουν προσφερθεί του ιδρυτές Jec Macaleb, Chris Larsen και Arthur Britto.
- 7 δις νομίσματα XRP έχουν δωρισθεί στη Ripple Labs.
- 20 δις νομίσματα XRP έχουν αποτελέσει αντικείμενο αγοράς για εταιρίες και ιδιώτες.
- 57 δις νομίσματα XRP είχαν δεσμευτεί σε smart contract το 2019.

Με βάση το τελευταίο, κάθε χρόνο θα μεταφέρονται στο δίκτυο περίπου 1 δις νομίσματα XRP, έως ότου εξαντληθούν, προσεγγίζοντας τα 100 δις. Κάθε νόμισμα XRP έχει τη δυνατότητα να διαιρεθεί σε μικρότερες μονάδες, που φτάνουν μέχρι και τα 6 δεκαδικά ψηφία. Όπως γίνεται εύκολα αντιληπτό η μικρότερη δυνατή μονάδα είναι στα 0.000001 XRP.

Προκειμένου να αποφευχθούν φαινόμενα spam από τους νέους χρήστες απαιτείται το ποσό των 20 XRP ως ελάχιστη πρώτη κατάθεση. Η παραπάνω minimum κατάθεση δίνει αυτόματα πρόσβαση στο wallet του XRP για κάθε νέο χρήστη. Αντίστοιχα με άλλα κρυπτονομίσματα για κάθε συναλλαγή δεσμεύεται ένα μικρό ποσό σαν τέλος. Το ιδιαίτερο με το XRP είναι ότι τα τέλη αυτά αντιστοιχούν πλέον σε νομίσματα, που δε μπορούμε να τα αξιοποιήσουμε ξανά. Όπως είναι εύκολα αντιληπτό αυτή η στρατηγική οδηγεί στη σταδιακή μείωση των αξιοποιήσιμων νομισμάτων. Θεωρητικά, όσο μειώνεται το πλήθος των νομισμάτων σε κυκλοφορία, τόσο μεγαλύτερη αξία θα αποκτήσουν με το πέρασμα του χρόνου (θεωρία προσφοράς και ζήτησης). Ακόμα δεν έχει οριστεί κάποιος τρόπος για να κυκλοφορήσουν νέα και παραπάνω νομίσματα στο δίκτυο παρόλο που έχουν υπάρξει ορισμένες προτάσεις για αυτό το σενάριο, αλλά απέχουμε ακόμα από αυτό το σημείο.

2.5 Litecoin

Ο «μικρός αδερφός» του Bitcoin δημιουργήθηκε το 2011 από τον Charlie Lee, ο οποίος εμπνεόμενος από το Bitcoin, δημιούργησε και παρουσίασε τη δική του εκδοχή του διάσημου κρυπτονομίσματος. Το Litecoin είναι ένα peer-to-peer κρυπτονόμισμα, που χρησιμοποιεί

τεχνολογία blockchain για τις συναλλαγές. Το Litecoin (LTC) μπορεί να θεωρηθεί το ένας από τους μεγαλύτερους παίχτες στην αγορά των κρυπτονομισμάτων, καθώς είναι το δεύτερο πιο δημοφιλές κρυπτονόμισμα στο mining και αρκετά υψηλά επίσης σε προτίμηση όσον αφορά τις συναλλαγές. Το Litecoin κάνει χρήση του αλγορίθμου κρυπτογράφησης Scrypt, σε αντίθεση με το Bitcoin που χρησιμοποιεί τον SHA-256.

Το όραμα του δημιουργού του είναι να το χρησιμοποιούν οι άνθρωποι για τις καθημερινές τους συναλλαγές καθώς και να κάνει χρήση ενός αλγόριθμου που είναι ανθεκτικός σε επιταχυνόμενες τεχνολογίες εξόρυξης υλικού (ASIC). Αυτό επιτυγχάνεται από το γεγονός ότι ο αλγόριθμος Scrypt είναι ανθεκτικός στην εξόρυξη ASIC λόγω των υψηλών απαιτήσεων σε μνήμη RAM.

Η προμήθεια που απαιτείται για συναλλαγές διαμέσου του Litecoin είναι σε πολύ χαμηλά επίπεδα σε σχέση με τον ανταγωνισμό, πράγμα το οποίο βοηθάει στο να γίνει πραγματικότητα το όραμα του δημιουργού του. Ενδεικτικά για μία συναλλαγή με Litecoin (ανεξαρτήτως ποσού) θα απαιτηθεί προμήθεια $0,1 όταν το Bitcoin θα «ζητήσει» προμήθεια περίπου $13.

Επιπλέον πλεονέκτημα του Litecoin σε σχέση με το Bitcoin είναι η ταχύτητα. Στο Bitcoin, όπως έχει ήδη αναφερθεί, ο μέσος χρόνος επιβεβαίωσης της συναλλαγής υπερβαίνει τα 10 λεπτά, ενώ στο Litecoin απαιτούνται μόνο 2,5 λεπτά. Ωστόσο αυτό δεν έρχεται με μηδενικό κόστος: η πιθανότητα ορφανών μπλοκ είναι σαφώς μεγαλύτερη σε σχέση με το Bitcoin. Μία επιπλέον διαφορά ανάμεσα στα δύο κρυπτονομίσματα είναι το όριο των νομισμάτων που μπορούν να κυκλοφορήσουν. Στην αγορά, στα μέσα του 2019, βρίσκονται σε κυκλοφορία περίπου 18,3 εκατομμύρια BTC με όριο τα 21 εκατομμύρια, ενώ βρίσκονται σε κυκλοφορία 63 εκατομμύρια LTC με όριο τα 84 εκατομμύρια. [14]

Το Litecoin από τη στιγμή που βγήκε στην αγορά έχει καταφέρει και έχει κερδίσει ένα σημαντικό μερίδιο στην πίτα της κεφαλαιοποίησης. Το 2013 είχε καταφέρει και είχε κερδίσει ένα μερίδιο της τάξης του 4% ενώ εντός του 2019, με αρκετά αξιόλογο ανταγωνισμό έχει καταφέρει και έχει σταθεροποιηθεί στην 5η θέση από πλευράς κεφαλαιοποίησης με μερίδιο περίπου 2,5%. Τέλος αξίζει να αναφερθεί πως εντός του 2017 το Litecoin εμφάνισε κέρδη ανά μονάδα γύρω στο 7000%. [7]

2.6 Dash

Μπορεί το Bitcoin να αποτελεί το πλέον διαδεδομένο μέσο ηλεκτρονικών συναλλαγών ωστόσο διαθέτει ορισμένα σημαντικά μειονεκτήματα. Δύο βασικές του ελλείψεις που αποθαρρύνουν πολλούς χρήστες από την υιοθέτηση του είναι η αργή επεξεργασία των συναλλαγών και η απουσία πλήρους ανωνυμίας και ιδιωτικότητας. Πάνω σε αυτή την ανάγκη λοιπόν βασίστηκε η ανάπτυξη ενός νέου κρυπτονομίσματος ως μέσο ηλεκτρονικών συναλλαγών με μηχανισμό αντίστοιχο του Bitcoin, το οποίο θα αντιμετώπιζε αυτά τα ζητήματα, δηλαδή θα εξασφάλιζε τη δυνατότητα για άμεσες συναλλαγές με χαμηλά τέλη και από την άλλη θα αποτελούσε ένα ασφαλές περιβάλλον πλήρους ιδιωτικότητας για τους χρήστες. Αποτέλεσμα αυτού του κενού στην αγορά ήταν η δημιουργία του Dash.

Το Dash κυκλοφόρησε τον Ιανουάριο του 2014 από τον Evan Duffeld έναν προγραμματιστή με καταγωγή από τις ΗΠΑ. Πριν ασχοληθεί με το Dash, ο Evan Duffeld εργάστηκε σε πολλές εταιρείες, που δραστηριοποιούνταν στον κλάδο της Πληροφορικής με

ειδίκευση στις τεχνολογίες αιχμής. Η αρχική ονομασία του Dash ήταν Xcoin και ο δημιουργός του είχε επισημάνει τα μειονεκτήματα στη χρήση του Bitcoin που τον ώθησαν στην ανάπτυξη ενός νέου κρυπτονομίσματος. Ωστόσο, επειδή γνώριζε πως δε θα μπορούσε να πείσει την ομάδα ανάπτυξης του Bitcoin για τα υπαρκτά του μειονεκτήματα και την ανάγκη ορισμένων αλλαγών, το πρωτόκολλο του Bitcoin ωθήθηκε σε ένα hard fork που σηματοδότησε τη γέννηση του Xcoin.

Το πρώτο διάστημα κυκλοφορίας του υπήρξε δυσπιστία γύρω από τη χρήση του. Αυτό οδήγησε στην αναδιαμόρφωση του και στην επαναφορά στη κυκλοφορία με το όνομα Darkcoin. Βέβαια, και πάλι αντιμετωπίστηκε με καχυποψία, καθώς λόγω της ισχυρής ανωνυμίας του γινόταν ευρεία χρήση του στην αγορά του Dark Net. Το Μάρτιο του 2015, ανακατασκευάστηκε ξανά και επανακυκλοφόρησε με το σημερινό του όνομα Dash (συντόμευση του όρου digital cash). Από τον Αύγουστο του 2016, το Dash σε μια προσπάθεια αποκατάστασης του ονόματος του αποσύρθηκε από τις συναλλαγές στο Dark Net. [15]

Το τρέχον Market Capitalization που παρουσιάζει το Dash ανέρχεται περίπου στα $704.300.000. Ο τρέχων αριθμός νομισμάτων από την άλλη είναι περίπου 9.500.000 DASH και η τρέχουσα αξία του $74.5100 Η αξία του DASH παρουσίασε ιστορικό υψηλό στις 20/12/2017, φτάνοντας στα $1.642,22 το οποίο αντιστοιχούσε σε αξία κεφαλαιοποίησης της τάξης των $638.744.422 USD ενώ το ιστορικό χαμηλό παρατηρείται στις 14/02/2014, φτάνοντας στα $0,213899 και αντιστοιχούσε σε αξία κεφαλαιοποίησης της τάξης των $ 1.233.615 USD. Το DASH, από τη κυκλοφορία του μέχρι και το Φεβρουάριο του 2017, παρουσιάζει χαμηλές πτήσεις, με χαμηλό Market cap. Στη συνέχεια και μέχρι τα μέσα Δεκεμβρίου του 2017, παρουσιάζει ταχύτατα ανοδική πορεία, προσεγγίζοντας το ιστορικό υψηλό Market cap του. Από εκεί και μετά παρουσιάζει συνεχείς αυξομειώσεις, χωρίς να έχει καταφέρει να προσεγγίσει ένα σταθερό ρυθμό αύξησης. [7]

Τα νέα νομίσματα Dash παράγονται μέσα από τη διαδικασία του mining με τη μορφή reward block. Για να διασφαλιστεί ότι δε θα προκύψει μία γρήγορη εξάντληση, το reward του μπλοκ μειώνεται σταδιακά μέσω ρυθμού που ορίζεται από το ίδιο το πρωτόκολλο. Το Dash τις πρώτες μέρες ύπαρξης του παρείχε ένα reward των 5 DASH, αριθμός ο οποίος μειώνεται με ένα ρυθμό της τάξης του 7,14% για κάθε 210240 μπλοκ (αντιστοιχεί σε 383 ημέρες). Το τρέχον reward είναι 3,10663 DASH. Διαπιστώνεται ότι όταν η μείωση του reward είναι μικρή κάθε χρόνο, επιτυγχάνεται μια ομαλότερη μετάβαση σε ένα μοντέλο που βασίζεται στα τέλη των συναλλαγών .Τα συνολικά νομίσματα του Dash είναι το άθροισμα μιας γεωμετρικής σειράς, όπως και στη περίπτωση του Bitcoin, αλλά ο τελικός αριθμός κερμάτων που θα κυκλοφορήσουν είναι ακόμα αβέβαιος. Με βάση τις μέχρι τώρα εκτιμήσεις, το max supply του Dash προβλέπεται να φτάσει το πολύ τη τιμή των 18,900,000 κρυπτονομισμάτων. Το Dash θα συνεχίσει να κόβει νομίσματα για περίπου 192 χρόνια έως ότου η εξόρυξη ενός και μόνο νομίσματος διαρκεί πάνω από ένα ημερολογιακό έτος. Μετά το 2209 θα δημιουργηθούν μόνο 14 DASH ενώ η διαδικασία για να δημιουργηθεί το τελευταίο DASH θα διαρκέσει 231 χρόνια, αρχίζοντας από το 2246 και λήγοντας όταν η παραγωγή νέων νομισμάτων σταματήσει εντελώς το 2477.

Το reward για κάθε μπλοκ δε προορίζεται μόνο για τον miner, αλλά κατανέμεται ως εξής:

- Ο masternode και ο επιτυχών miner λαμβάνουν το 45% (δηλαδή περίπου 1,3995 DASH) του reward έκαστος.
- Το 10% του reward του μπλοκ προορίζεται για τις προτάσεις προϋπολογισμού οι οποίες γίνονται μέσω της κοινότητας του Dash. Πιο συγκεκριμένα, μέσω του Dash Forum, γίνονται προτάσεις για χρηματοδότηση, με

σκοπό την περαιτέρω ανάπτυξη της πλατφόρμας. Οι masternodes ψηφίζουν πάνω στις προτάσεις αυτές με θετική ή αρνητική ψήφο και εάν υπάρχει έγκριση, δηλαδή αν τα «ναι» είναι πάνω από 10%, το ποσό που έχει συγκεντρωθεί στο budget καταβάλλεται απευθείας από το blockchain.

Ένα από τα κομβικά ζητήματα που έρχεται να λύσει το Dash είναι το κόστος της διεξαγωγής συναλλαγών. Το κόστος των συναλλαγών με bitcoin καθορίζεται από μια σειρά παραγόντων μεταξύ των οποίων είναι το μέγεθος του block καθώς και η χρονική στιγμή που διεξάγεται η συναλλαγή. Το Dash από την άλλη ελαχιστοποιεί τα τέλη συναλλαγής που σύμφωνα με το μέσο όρο που το ίδιο το νόμισμα δημοσιοποίησε φτάνουν το 0,0264 δολάρια, ξεπερνώντας μάλιστα και άλλα κρυπτονομίσματα γνωστά για τα χαμηλά τέλη συναλλαγών όπως το Litecoin.

Οι συναλλαγές στο δίκτυο Dash εγγράφονται σε blocks του blockchain με το μέγεθος κάθε συναλλαγής να μετράται σε bytes. Είναι αξιοσημείωτο το γεγονός ότι ο αριθμός των bytes Που απαιτούνται για το νέο κρίκο της αλυσίδας του blockchain δεν εξαρτάται από το μέγεθος του ποσού που περιλαμβάνει η συναλλαγή. Το μέγεθος της συναλλαγής ωστόσο επηρεάζεται από τον αριθμό των διευθύνσεων εισόδου και εξόδου που συμμετέχουν στη συναλλαγή. Κάθε νέο μπλοκ παράγεται από έναν miner, ο οποίος πληρώνεται με rewards για την ολοκλήρωση της εργασίας του. Ο περιορισμός του μεγέθους των μπλοκ βοηθά στην αποφυγή του ενδεχόμενου να γεμίσει το δίκτυο με spam συναλλαγές. Καθώς αυξάνεται ο όγκος συναλλαγών, ο ελεύθερος χώρος σε κάθε μπλοκ περιορίζεται και με γνώμονα ότι οι miners δεν είναι υποχρεωμένοι να συμπεριλάβουν όλες τις υπάρχουσες συναλλαγές στα blocks που παράγουν, αφού τα blocks γεμίσουν, μπορεί να συμπεριληφθεί ένα προαιρετικό τέλος συναλλαγής ως κίνητρο στον miner για να επεξεργαστεί τη συναλλαγή. Τα περισσότερα wallets περιλαμβάνουν ένα προεπιλεγμένο μικρό τέλος, παρόλο που ορισμένοι miners επεξεργάζονται συναλλαγές ακόμη και αν δεν συμπεριλαμβάνονται τέλη.

Το άλλο βασικό πλεονέκτημα της πλατφόρμας του Dash, δηλαδή αυτό της πλήρους ανωνυμίας, επιτυγχάνεται μέσω της υπηρεσίας PrivateSend, που επιπροσθέτως εγγυάται την ασφάλεια των συναλλαγών. Με αυτό το τρόπο, παρέχεται και πλήρης ιδιωτικότητα στη προέλευση των πόρων του χρήστη μέσω της ετερογενοποίησης των νομισμάτων, καθώς όλα τα νομίσματα Dash που έχει στην κατοχή του κάποιος αναγνωρίζονται ως μια διαφορετική "εισροή" (input), δηλαδή ως διακριτά και ξεχωριστά νομίσματα.

Το δίκτυο του Dash, σε αντίθεση με άλλα κρυπτονομίσματα, διαχωρίζεται σε δύο επίπεδα. Το πρώτο επίπεδο περιλαμβάνει τους miners και τη δραστηριότητά τους, η οποία είναι ίδια με αυτή του Bitcoin δηλαδή η συνεχής εκτέλεση ενός Proof of Work αλγόριθμου για την πιστοποίηση συναλλαγών, την ένταξη τους σε μπλοκ και την εισαγωγή τους στο blockchain. Μέσω αυτής της διαδικασίας, οι miners λαμβάνουν το 45% του block reward. Τα βήματα του PoW αλγορίθμου του Dash που περιεγράφηκαν εν συντομία προηγουμένως αναλύονται διεξοδικά παρακάτω:

- Κάθε miner συλλέγει τυχαία συναλλαγές του δικτύου
- Ο miner επικυρώνει όλες αυτές τις συναλλαγές και με τη σειρά τους εντάσσονται σε ένα υποψήφιο μπλοκ.
- Το hash value του block header εισέρχεται στο υποψήφιο μπλοκ.
- Κάθε miner προσπαθεί να επιλύσει το proof of work πρόβλημα. Κάθε επιτυχημένη λύση μεταδίδεται σε όλο το δίκτυο.
- Το νεοεισελθέν proof of work ελέγχεται ως προς την εγκυρότητα από το υπόλοιπο δίκτυο.

- Αν υπάρχει συναίνεση ως προς την εγκυρότητα του μπλοκ από όλους τους κόμβους του δικτύου, το μπλοκ εισέρχεται επιτυχημένα στο blockchain.

Η διαδικασία του PoW του DASH είναι παρόμοια με αυτή του Bitcoin. Αρχικά ορίζεται μία τιμή για το nonce. Στη συνέχεια ο miner υπολογίζει συνεχώς το hash value του block header μέσω της hash συνάρτησης X11 και ελέγχει αν το παραγόμενο hash value είναι κάτω από ένα προκαθορισμένο όριο. Αν είναι κάτω από αυτό το όριο, ο miner έχει επιτυχώς υπολογίσει ένα proof of work και μεταδίδει το μπλοκ που συνθέτει, μαζί με το proof of work, στο υπόλοιπο δίκτυο.

Σε κάθε μπλοκ, το δίκτυο χρησιμοποιεί το επίπεδο δυσκολίας των τελευταίων 24 μπλοκ και τον αριθμό δευτερολέπτων που έχουν περάσει μεταξύ της δημιουργίας του πρώτου και του τελευταίου από αυτά τα 24 μπλοκ . Η ιδανική τιμή είναι 3600 sec (μία ώρα). Σε περίπτωση που χρειαστεί λιγότερο από μία ώρα για να δημιουργηθούν τα 24 μπλοκ, η αναμενόμενη τιμή του βαθμού δυσκολίας αυξάνεται, έτσι ώστε τα επόμενα 24 μπλοκ να χρειαστούν ακριβώς μία ώρα για να δημιουργηθούν αν ελέγχονται τα hash values με τον ίδιο ρυθμό. Εάν χρειάστηκε πάνω από μία ώρα για να δημιουργηθούν τα blocks, η αναμενόμενη τιμή του βαθμού δυσκολίας μειώνεται για τον ίδιο λόγο.

Αυτή η μέθοδος υπολογισμού του difficulty (Dark Gravity Wave) γράφτηκε από τον δημιουργό του Dash, Evan Duffield, για να διορθώσει πιθανές κακόβουλες προσπάθειες εκμετάλλευσης του προηγούμενου αλγόριθμου που χρησιμοποιούνταν για τον υπολογισμό του difficulty (Kimoto Gravity Well). Το Dark Gravity Wave είναι ένας ανοιχτού κώδικα αλγόριθμος προσαρμοζόμενης δυσκολίας για κρυπτονομίσματα που βασίζονται στο Bitcoin. Χρησιμοποιήθηκε για πρώτη φορά στο Dash και σε γενικές γραμμές θα λέγαμε ότι το Dark Gravity Wave είναι παρόμοιο με το Kimoto Gravity Well, προσαρμόζοντας τα επίπεδα δυσκολίας σε κάθε μπλοκ βάσει στατιστικών στοιχείων από πρόσφατα εντοπισμένα μπλοκ. Αυτό καθιστά δυνατή την έκδοση μπλοκ με αρκετά σταθερούς χρόνους, ακόμη και αν η hashing power έχει υψηλές διακυμάνσεις.

Το δεύτερο επίπεδο περιλαμβάνει τη λειτουργία των Masternodes. Οι Masternodes δεν πραγματοποιούν mining, ούτε το υλικό του mining μπορεί να χρησιμοποιηθεί για τη λειτουργικότητα των Masternode, παρ' όλα αυτά υποστηρίζουν μία σειρά από πολύτιμες λειτουργίες του δικτύου όπως:

- Επιτρέπουν τη εκτέλεση άμεσων συναλλαγών (Instant Send)
- Επιτρέπουν τη πλήρη ιδιωτικότητα στις συναλλαγές (Private Send)
- Αποφασίζουν μέσω μοναδικής ψήφου για το κάθε Masternode για βασικά ζητήματα του δικτύου (αλλαγές ή ανάπτυξη του δικτύου)
- Έχουν τη δυνατότητα να απορρίψουν ένα μπλοκ είτε λόγω λανθασμένης διαμόρφωσης είτε λόγω κακόβουλης χρήσης παλαιότερης έκδοσης λογισμικού από το miner.
- Προστατεύει το blockchain από τις 51% επιθέσεις.

Οι υπηρεσίες αυτές προσφέρουν το 45% του block reward σε έναν masternode. Το σύστημα των Masternode λειτουργεί με ένα τρόπο, ο οποίος ονομάζεται Proof of Service (PoSe) μέσω του οποίου κάθε χρήστης μπορεί να λάβει το ρόλο του Masternode, αρκεί να καταθέσει το ποσό των 1000 Dash. Το ποσό αυτό δε θεωρείται stake, καθώς δεν παρακρατείται αν λειτουργήσει κακόβουλα ο Masternode, ούτε κλειδώνεται επίσης. Κάθε χρήστης, ο οποίος λειτουργεί έναν masternode, έχει τη δυνατότητα κάθε στιγμή να ξοδέψει μέρος αυτού του ποσού κάτι όμως που οδηγεί σε πλήρη απενεργοποίηση και διαγραφή του.

Με βάση τα παραπάνω, καταλήγουμε πως το δίκτυο του Dash συνδυάζει τη λειτουργικότητα του Proof of Work και του Proof of Service. Το πρωτόκολλο του Dash αξιοποιεί τον αλγόριθμο X11 ως hash function, όπου μια είσοδος αυθαίρετου μεγέθους

περνάει μέσα από 11 ανεξάρτητες hash functions σε έναν αλγόριθμο. Όταν υποβάλλεται μία τιμή, η πρώτη συνάρτηση παράγει ένα hash, το οποίο στη συνέχεια υποβάλλεται στην επόμενη συνάρτηση για να παράξει ένα άλλο hash. Αυτή η διαδικασία επαναλαμβάνεται μέχρι την τελευταία συνάρτηση που χρησιμοποιεί ο αλγόριθμος. Οι συναρτήσεις αυτές είναι οι BLAKE, BMW, Grøsti, JH, Keccak, Skein, Luffa, CubeHash, SHAvite-3, SIMD και ECHO. Θεωρούνται από τις πιο ασφαλείς τεχνικές κρυπτογράφησης που υπάρχουν. [17]

2.7 Monero

Το Monero είναι ένα κρυπτονόμισμα με λογισμικό ανοιχτού κώδικα. Ο δημιουργός του, ακριβώς όπως και στην περίπτωση του Bitcoin, είναι άγνωστος. Πρωτοπαρουσιάστηκε τον Απρίλιο του 2014, έχοντας σαν απόλυτη προτεραιότητα την ανωνυμία και την ιδιωτικότητα στις συναλλαγές. Αυτό το επιτυγχάνει μέσω μιας εξειδικευμένης ιδιότητας της κρυπτογραφίας (ring signatures) καθιστώντας τις συναλλαγές σχεδόν αδύνατο να ανιχνευθούν, από την ταυτότητα του αποστολέα και του δέκτη, έως και το συνολικό ποσό της συναλλαγής.

Σε αντίθεση με πολλά κρυπτονομίσματα που είναι χρησιμοποιούν αλγόριθμους αντίστοιχους με αυτόν του Bitcoin, το Monero βασίζεται στον αλγόριθμο CryptoNight, ο οποίος προέρχεται από το πρωτόκολλο cryptonote. Συγκεκριμένα, τα ring signatures που χρησιμοποιούνται στο cryptonote αναμιγνύουν την είσοδο του αποστολέα με μια ομάδα άλλων, καθιστώντας εκθετικά πιο δύσκολη τη δημιουργία συνδέσμου μεταξύ τρέχουσας και επόμενης συναλλαγής. Από την αρχική ανάπτυξή του από το πρωτόκολλο cryptonote, το Monero έχει αποκλίνει σε πολλά χαρακτηριστικά.

Εύκολα θα μπορούσε να συμπεράνει κανείς, πως το Monero λόγο της ιδιωτικότητας αυτής που προσφέρει, μπορεί να αποτελέσει ένα εργαλείο για παράνομες ενέργειες εντός του κυβερνοχώρου. Το Monero είναι προϊόν εξόρυξης, με την πλατφόρμα να επιβραβεύει τον κάθε miner με 7,46 XMR σε κάθε εξόρυξη. Ο χρόνος επίλυσης του block είναι στα 2 λεπτά καθιστώντας το τρίτο γρηγορότερο κρυπτονόμισμα σε αυτόν τον τομέα με το Ripple και το Ethereum, να καταλαμβάνουν την πρώτη και δεύτερη θέση αντίστοιχα.

Την στιγμή που γράφεται η παρούσα διατριβή το ποσό των κρυπτονομισμάτων που βρίσκονται στην αγορά είναι περίπου 19 εκατομμύρια XMR και σε αντίθεση με τα περισσότερα κρυπτονομίσματα, δεν υπάρχει κάποιος περιορισμός στον αριθμό τους που θα κυκλοφορήσει στην αγορά. Εντός του 2017 το Monero εμφάνισε κέρδη έως και περίπου 3000% καθιστώντας το, το 7ο ισχυρότερο κρυπτονόμισμα σε μερίδιο κεφαλαιοποίησης αγοράς. Την ίδια χρονιά εμφανίστηκαν 3 μεγάλες απειλές για το απόρρητο των χρηστών του Monero. Η πρώτη βασίζεται στη μόχλευση των zero level ring signature και στην δυνατότητα που προσφέρει να είναι ορατά τα εξερχόμενα ποσά των συναλλαγών. Η δεύτερη, που περιγράφεται ως "Leveraging Output Merging", περιλαμβάνει παρακολούθηση συναλλαγών όπου δύο εξερχόμενες συναλλαγές ανήκουν στον ίδιο χρήστη, όπως όταν ένας χρήστης στέλνει τα χρήματα στον εαυτό του ("churning"). Τέλος, η τρίτη απειλή, η “Temporal Analysis”, δείχνει ότι η πρόβλεψη της σωστής εξόδου σε ένα ring signature θα μπορούσε ενδεχομένως να είναι ευκολότερη από ό, τι πιστεύαμε ως τώρα. Η ομάδα ανάπτυξης του Monero είχε αντιμετωπίσει την πρώτη ανησυχία ήδη από τον Ιανουάριο του 2017 με την εισαγωγή του Ring Confidential Transactions (RingCT) καθώς και την υποχρέωση ενός

ελάχιστου μεγέθους ring signatures στην αναβάθμιση πρωτοκόλλου του Μαρτίου 2016. Οι προγραμματιστές του Monero σημείωσαν επίσης ότι τα Monero Research Labs, το ακαδημαϊκό και ερευνητικό τους σκέλος, έχουν ήδη σημειώσει και περιγράφουν την ανεπάρκεια σε δύο δημόσια ερευνητικά έγγραφα το 2014 και το 2015. [16]

3 Πολυκριτηριακή ανάλυση

3.1 Παρουσίαση και μελέτη δεδομένων

Την στιγμή που γράφεται η συγκεκριμένη εργασία (5/2020) κυκλοφορούν στην αγορά πάνω από 1600 διαφορετικά κρυπτονομίσματα εκ των οποίων όμως ελάχιστα αποτελούν αξιόπιστες και μακροπρόθεσμα αποδοτικές λύσεις στα μάτια ενός επενδυτή. Νομίσματα λιγότερο γνωστά και χαμηλής σχετικά κεφαλαιοποίησης μπορεί να επιφέρουν σε λίγες περιπτώσεις υπερβολικά πολλά κέρδη αλλά συχνά ενέχει ο κίνδυνος είτε της απάτης είτε της συνεχούς πορείας του κρυπτονομίσματος στο φάσμα της πλήρους αφάνειας. Για την παρούσα εργασία επομένως θεωρήθηκε χρήσιμο να γίνει μια μετριοπαθής επιλογή ανάμεσα σε κρυπτονομίσματα που πληρούν κάποια βασικά ON-OFF κριτήρια:

a. Ανήκουν στα TOP 25 από άποψη δείκτη κεφαλαιοποίησης. Θεωρείται σημαντικός παράγοντας ευστάθειας και αναγνωρισιμότητας του κρυπτονομίσματος
b. Έχουν τουλάχιστον 5 χρόνια ύπαρξης. Ο χρόνος ύπαρξης αντικατοπτρίζει την ευστάθεια του δικτύου και το ενδιαφέρον των miners σε βάθος χρόνου. Εξαίρεση στη μελέτη μας αποτελεί το Bitcoin cash (3 ετών) το οποίο αποτελεί ωστόσο στενό «συγγενή» του βασιλιά των κρυπτονομισμάτων Bitcoin κάτι που εγγυάται την ενασχόληση του κοινού μαζί του
c. Χρησιμοποιούν PoW τεχνική mining. Η συγκεκριμένη επιλογή έγινε γιατί τα σημαντικότερα εκ των κρυπτονομισμάτων χρησιμοποιούν το PoW ενώ αποτελεί και την παλαιότερη εκ των μεθόδων που παρουσιάστηκαν παραπάνω. Εξαίρεση αποτελεί το Ripple το οποίο όμως δεν γινόταν να παραλειφθεί όντας το τρίτο σε κεφαλαιοποίηση νόμισμα
d. Έχουν μεγάλη βάση χρηστών. Η άντληση πληροφοριών (ειδικά τεχνικών) ακόμα και για τα large cap νομίσματα εξαρτάται πλήρως από το ενδιαφέρον της κοινότητας και

τα forum και site που υπάρχουν από ενεργούς χρήστες, επενδυτές και γενικότερα θιασώτες των εκάστοτε νομισμάτων

Με βάση λοιπόν όλα τα παραπάνω καταλήξαμε στην επιλογή των εξής 7 κρυπτονομισμάτων τα οποία αποτελούν τις εναλλακτικές του προβλήματος μας:

- Bitcoin
- Ethereum
- Bitcoin Cash
- Ripple
- Monero
- Dash
- Litecoin

Τα παραπάνω κρυπτονομίσματα αναλύθηκαν θεωρητικά σε προηγούμενο κεφάλαιο. Ακολουθεί ωστόσο ένας συγκεντρωτικός πίνακας όπου παρουσιάζονται οι σημαντικότερες πληροφορίες για όλα τα παραπάνω

	BTC	ETH	XRP	BCH	LTC	XMR	DASH
Τιμή αγοράς ($)	9207.72	207.55	0.199879	235.1	44.13	64.66	74.51
Κεφαλαιοποίηση (εκ. $)	169407.3	23063.5	8823.6	4329.5	2861.9	1135.3	704.3
Ποσότητα σε κυκλοφορία (εκ. $)	18.4	111	44112.8	18.4	64.8	17.6	9.5
Μέγιστη ποσότητα (εκ. $)	21	NA	100000	21	84	NA	18.9
Ποσοστό κυκλοφορίας (%)	87.54		44.11	87.69	77.14		49.97
3μηνιαία μεταβολή (%)	-6.37	-23.35	-28.66	-40.73	-43.84	-23.34	-30.39
6μηνιαία μεταβολή (%)	28.86	41.53	-9.25	11.57	-3.72	29.4	49.03
Ετήσια μεταβολή (%)	14.87	-16.66	-47.99	-42.57	-56.06	-25.7	-52.5
Εξόρυξη	Ναι	Ναι	Όχι	Ναι	Ναι	Ναι	Ναι
Χρόνος Block (second)	600	14	3.5	600	150	120	150
Ανιχνεύεται	Όχι	Όχι	Όχι	Όχι	Όχι	Ναι	Ναι
Θέση (βάση κεφαλαιοποίησης)	1	2	4	5	7	16	23
Έτος κυκλοφορίας	2008	2015	2012	2017	2011	2014	2014

Σε αυτό το σημείο είναι πολύ σημαντικό να αναφέρουμε ότι η προσέγγιση του προβλήματος επιλογής ανάμεσα στα κρυπτονομίσματα έγινε με καθαρά χρηματοοικονομικά κριτήρια, όπως φαίνεται ξεκάθαρα και από τον παραπάνω πίνακα. Πρόκειται επομένως για μια χρηματοοικονομική αξιολόγηση που βασίστηκε σε μεθόδους πολυκριτήριας ανάλυσης.

Επόμενο βήμα αποτελεί ο ορισμός των κριτηρίων βάση των οποίων θα κατηγοριοποιήσουμε τις εναλλακτικές μας. Τα κριτήρια και η σωστός ορισμός και κατάταξη τους αποτελεί ίσως το σημαντικότερο βήμα σε μια πολυκριτηριακή μελέτη. Συχνά η παραπάνω απόφαση εμπίπτει στην κρίση του αποφασίζοντα επομένως μπορεί να υπάρξουν μεγάλες διαφοροποιήσεις κατά περίπτωση. Το σημαντικότερο είναι να οριστεί ο στόχος της μελέτης, δηλαδή στην περίπτωση μας ποια ποιοτικά χαρακτηριστικά είναι σημαντικά για τη βέλτιστη επιλογή εναλλακτικής και ποια κριτήρια τα αντιπροσωπεύουν καλύτερα. Έχοντας όλα τα παραπάνω υπόψη επιλέχθηκαν κατά σειρά αύξουσας σημαντικότητας (από το λιγότερο σημαντικό στο περισσότερο) τα παρακάτω κριτήρια:

1. Έτη ύπαρξης του νομίσματος: Αποτελεί ένα βαθμό αξιοπιστίας του νομίσματος καθώς δείχνει πόσα χρόνια έχει καθιερωθεί στην αγορά. Επίσης συνδέεται με το ρίσκο στην επιλογή του καθώς τα αρχαιότερα κρυπτονομίσματα είναι και λιγότερο πιθανό να αποτελούν scams ή να παρουσιάσουν κατακόρυφη απαξίωση. Είναι κριτήριο μεγιστοποίησης
2. Κεφαλαιοποίηση σε εκ. δολάρια: Είναι η τρέχουσα κεφαλαιοποίηση του κρυπτονομίσματος. Ομοίως με το πρώτο κριτήριο τα large cap νομίσματα τείνουν να είναι πιο αποδοτικά και σταθερά ενώ εμπεριέχουν και μικρότερο ρίσκο. Είναι κριτήριο μεγιστοποίησης
3. Εκ. δολάρια που εξορύχθηκαν τον τελευταίο χρόνο: Αποτελεί ένα συνδυαστικό κριτήριο που συνδυάζει το πόσα νομίσματα έγιναν mine σε ένα έτος (ενδιαφέρον της κοινότητας) και τη μέση τιμή του νομίσματος τον τελευταίο χρόνο. Επειδή ακριβώς δίνει την εικόνα του ενδιαφέροντος το τελευταίο έτος τοποθετείται υψηλότερα από το δείκτη κεφαλαιοποίησης. Είναι κριτήριο μεγιστοποίησης
4. % αλλαγή της τιμής το τελευταίο τρίμηνο: Δείκτης μεταβολής της αξίας σε $ τους τελευταίους 3 μήνες. Είναι κριτήριο μεγιστοποίησης
5. % αλλαγή της τιμής το τελευταίο εξάμηνο: Δείκτης μεταβολής της αξίας σε $ τους τελευταίους 6 μήνες. Είναι κριτήριο μεγιστοποίησης
6. % αλλαγή της τιμής το τελευταίο δωδεκάμηνο: Δείκτης μεταβολής της αξίας σε $ τους τελευταίους 12 μήνες. Είναι αξιοσημείωτη η σειρά προτίμησης των τελευταίων 3 δεικτών καθώς θεωρούμε τη μεταβολή της τιμής το σημαντικότερο παράγοντα με έμφαση στο μεγαλύτερο διάστημα. Είναι κριτήριο μεγιστοποίησης

Έπειτα από τον ορισμό των κριτηρίων λοιπόν προκύπτει ο παρακάτω πίνακας ο οποίος είναι μια πιο ευανάγνωστη και καλύτερα επεξεργάσιμη μορφή των συγκεντρωτικών δεδομένων.

Cryptocurrencies		**Criteria**					
Crypto Abbreviation	**Crypto Name**	**Years Active**	**million $ Capitalization**	**million $ mined last year**	**% 3month change**	**% 6month change**	**% 12month change**
BTC	Bitcoin	12	169407.30	6889.40	-6.37	28.86	14.87
ETH	Ethereum	5	23063.50	1141.48	-23.35	41.53	-16.66
XRP	Ripple	8	8823.60	617.14	-28.66	-9.25	-47.99
BCH	Bitcoin Cash	3	4329.50	225.56	-40.73	11.57	-42.57
LTC	Litecoin	9	2861.90	202.39	-43.84	-3.72	-56.06
XMR	Monero	6	1135.30	53.09	-23.34	29.40	-25.70
DASH	Dash	6	704.30	92.55	-30.39	49.03	-52.50
min value		3	704.30	53.09	-43.84	-9.25	-56.06
max value		12	169407.30	6889.40	-6.37	49.03	14.87
Objective function per criteria		**maximize**	**maximize**	**maximize**	**maximize**	**maximize**	**maximize**

Με βάση τον παραπάνω πίνακα λοιπόν θα γίνει μια προσπάθεια κατάταξης των εναλλακτικών κρυπτονομισμάτων με χρήση των εξής γνωστών μεθόδων: MAUT, Electre I with Veto και Promethee.

3.2 Καθορισμός βαρών

Πριν από τη παρουσίαση οποιασδήποτε μελέτης θα πρέπει να προχωρήσουμε και σε ένα ακόμα πολύ σημαντικό βήμα, που δεν είναι άλλο από την επιλογή του βάρους για κάθε κριτήριο. Για να μην γίνει αυθαίρετα από τον αποφασίζοντα χωρίς κάποια μεθοδολογία η παραπάνω επιλογή, αποφασίστηκε να χρησιμοποιηθούν οι μέθοδοι της AHP και της Εντροπίας. Για όλες τις μεθόδους στη συνέχεια θα υπολογιστούν τα αποτελέσματα με χρήση 2 σετ βαρών: βάρη που βασίζονται αποκλειστικά στην AHP μέθοδο και βάρη που είναι ισόποσα σταθμισμένα ανάμεσα σε AHP και Εντροπία

3.2.1 Υπολογισμός βαρών με χρήση της AHP

Η AHP αποτελεί και η ίδια πολυκριτήρια θεωρία χρησιμότητας την οποία όμως θα χρησιμοποιήσουμε για να υπολογίσουμε τη βαρύτητα του κάθε κριτηρίου. Ουσιαστικά θα συγκρίνουμε όλα τα κριτήρια μεταξύ τους και ο βαθμός προτίμησης θα μεταφράζεται σε μια αριθμητική τιμή όπως φαίνεται παρακάτω.

Value	Preference
1	Equally Preferred
2	Equally to Moderately Preferred
3	Moderately Preferred
4	Moderately to Strongly Preferred
5	Strongly Preferred
6	Strongly to Very Strongly Preferred
7	Very Strongly Preferred
8	Very Strongly to Extremely Preferred
9	Extremely Preferred

Με βάση τα παραπάνω λοιπόν προκύπτει ο ακόλουθος πίνακας:

Criteria comparison matrix	Years Active	million $ Capitalization	million $ mined last year	% 3month change	% 6month change	% 12month change
Years Active	1.00	0.33	0.25	0.17	0.14	0.13
million $ Capitalization	3.00	1.00	0.50	0.25	0.20	0.17
million $ mined last year	4.00	2.00	1.00	0.33	0.25	0.20
% 3month change	6.00	4.00	3.00	1.00	0.50	0.33
% 6month change	7.00	5.00	4.00	2.00	1.00	0.50
% 12month change	8.00	6.00	5.00	3.00	2.00	1.00
Sum	29.00	18.33	13.75	6.75	4.09	2.33

Στον πίνακα αυτό συγκρίνονται ένα προς ένα με όλους τους πιθανούς συνδυασμούς όλα τα κριτήρια μεταξύ τους. Οι τιμές του πίνακα αντικατοπτρίζουν την προτίμηση του κριτηρίου της κάθε γραμμής έναντι του αντίστοιχου κριτηρίου της κάθε στήλης. Στον παρακάτω πίνακα φαίνεται η κανονικοποιημένη μορφή των παραπάνω:

Normalized matrix	Years Active	million $ Capitalization	million $ mined last year	% 3month change	% 6month change	% 12month change	AHP Weights	Consistency factor
Years Active	0.03	0.02	0.02	0.02	0.03	0.05	0.03	6.09
million $ Capitalization	0.10	0.05	0.04	0.04	0.05	0.07	0.06	6.04
million $ mined last year	0.14	0.11	0.07	0.05	0.06	0.09	0.09	6.13
% 3month change	0.21	0.22	0.22	0.15	0.12	0.14	0.18	6.32
% 6month change	0.24	0.27	0.29	0.30	0.24	0.22	0.26	6.38
% 12month change	0.28	0.33	0.36	0.44	0.49	0.43	0.39	6.35

Τα βάρη που προκύπτουν φαίνονται παραπάνω. Υπολογίστηκε επίσης ο δείκτης συνέπειας των βαρών που δείχνει πόσο συνεπείς οι συγκρίσεις μεταξύ όλων των κριτηρίων από τον αποφασίζοντα. Τα αποτέλεσμα αποδεικνύουν την ορθότητα της σύγκρισης.

3.2.2 Υπολογισμός βαρών με συνδυασμό AHP και Εντροπίας

Για το επόμενο σετ βαρών, όπως αναφέραμε και παραπάνω, θα λάβουμε υπόψη μας και την εντροπία του συστήματος σε συνδυασμό με την AHP. Η εντροπία αντιπροσωπεύει το εύρος διακύμανσης των τιμών για το κάθε κριτήριο. Ένα κριτήριο που ο αποφασίζοντας θεωρεί σημαντικό μπορεί να μην είναι χρήσιμο σε μια αξιολόγηση αν όλες οι εναλλακτικές είναι σχεδόν ταυτόσημες στο κριτήριο αυτό. Αντίθετα ένα κριτήριο χαμηλότερης βαρύτητας κατά τον αποφασίζοντα μπορεί να παρουσιάζει μεγάλες αποκλίσεις στις διάφορες τιμές των εναλλακτικών κάτι που σημαίνει ότι αυξάνεται η σημαντικότητα του στην εξαγωγή του τελικού αποτελέσματος.

Ακολουθούν κατά σειρά οι πίνακας των αρχικών μας δεδομένων (μορφοποιημένος κατάλληλα για τους υπολογισμούς), ο κανονικοποιημένος ως προς την καλύτερη τιμή πίνακας και ο πίνακας των λόγων ως προς τη μέγιστη τιμή των στοιχείων του κανονικοποιημένου.

Cryptocoin	**Criteria**					
	Years Active	**million $ Capitalization**	**million $ mined last year**	**% 3month change**	**% 6month change**	**% 12month change**
BTC	12	169407.3	6889.3977	-6.37	28.86	14.87
ETH	5	23063.5	1141.4752	-23.35	41.53	-16.66
XRP	8	8823.6	617.13598	-28.66	-9.25	-47.99
BCH	3	4329.5	225.56377	-40.73	11.57	-42.57
LTC	9	2861.9	202.38737	-43.84	-3.72	-56.06
XMR	6	1135.3	53.08995	-23.34	29.4	-25.7
DASH	6	704.3	92.549263	-30.39	49.03	-52.5
Max Values	12	169407.3	6889.3977	-6.37	49.03	14.87

Normalization of data acc. to best values per criteria (Xij/Xj*)						
Cryptocoin	**Criteria**					
	Years Active	**million $ Capitalization**	**million $ mined last year**	**% 3month change**	**% 6month change**	**% 12month change**
BTC	1	1	1	1.00	0.66	1.00
ETH	0.4167	0.1361423	0.1656858	0.56	0.87	0.56
XRP	0.7	0.0520851	0.1	0.42	0.02	0.13
BCH	0.25	0.0	0.0327407	0.11	0.37	0.20
LTC	0.75	0.0168936	0.0293766	0.03	0.11	0.01
XMR	0.5	0.0	0.007706	0.56	0.67	0.44
DASH	0.5	0.0	0.0134336	0.38	1.00	0.06
Sum (D)	4.0833	1.2415368	1.3385204	3.046529763	3.6971997	2.40247463

Matrix of Xij/Dj						
Cryptocoin	**Criteria**					
	Years Active	**million $ Capitalization**	**million $ mined last year**	**% 3month change**	**% 6month change**	**% 12month change**
BTC	0.24	0.81	0.75	0.33	0.18	0.42
ETH	0.10	0.11	0.12	0.18	0.24	0.23
XRP	0.16	0.04	0.07	0.14	0.00	0.05
BCH	0.06	0.02	0.02	0.04	0.10	0.08
LTC	0.18	0.01	0.02	0.01	0.03	0.01
XMR	0.12	0.01	0.01	0.18	0.18	0.18
DASH	0.12	0.00	0.01	0.12	0.27	0.03

Με βάση τον τελευταίο πίνακα προκύπτουν τα βάρη βασιζόμενα στην εντροπία των εναλλακτικών ανά κριτήριο. Στον πίνακα που ακολουθεί συμπεριλαμβάνεται επίσης τα βάρη που προέκυψαν μέσω της μεθόδου AHP καθώς και τα τελικά συνδυαστικά βάρη που θα χρησιμοποιήσουμε στη συνέχεια.

Criteria	**AHP Weights**	**Entropy - H**	**Weight - λ**	**AHP+Entropy Weights**
Years Active	0.03	0.96	0.02	0.03
million $ Capitalization	0.06	0.38	0.37	0.21
million $ mined last year	0.09	0.47	0.31	0.20
% 3month change	0.18	0.86	0.08	0.13
% 6month change	0.26	0.86	0.08	0.17
% 12month change	0.39	0.77	0.13	0.26
Sum	1.00	4.30	1.00	1.00

3.3 Μέθοδοι πολυκριτηριακής μελέτης

3.3.1 MAUT

Η πρώτη μέθοδος που επιλέχθηκε να χρησιμοποιηθεί είναι η MAUT (Multi Attribute Utility Theory) μια πολυκριτηριακή θεωρία χρησιμότητας. Από την κατηγοριοποίηση της μεθόδου γίνεται αντιληπτό ότι με την παραπάνω θα έχουμε κατάταξη όλων των εναλλακτικών νομισμάτων κατά σειρά προτίμησης. Έπειτα από τη μορφοποίηση των

δεδομένων, κατά τη γνωστή διαδικασία, στην επιθυμητή μορφή παίρνουμε τον παρακάτω πίνακα

Cryptocoin	**Criteria**					
	Years Active	**million $ Capitalization**	**million $ mined last year**	**% 3month change**	**% 6month change**	**% 12month change**
BTC	12	169407.3	6889.3977	-6.37	28.86	14.87
ETH	5	23063.5	1141.4752	-23.35	41.53	-16.66
XRP	8	8823.6	617.13598	-28.66	-9.25	-47.99
BCH	3	4329.5	225.56377	-40.73	11.57	-42.57
LTC	9	2861.9	202.38737	-43.84	-3.72	-56.06
XMR	6	1135.3	53.08995	-23.34	29.4	-25.7
DASH	6	704.3	92.549263	-30.39	49.03	-52.5
Max Values	12	169407.3	6889.3977	-6.37	49.03	14.87
Min Values	3	704.3	53.08995	-43.84	-9.25	-56.06
AHP Weights	0.03	0.06	0.09	0.18	0.26	0.39
AHP+Entropy Weights	0.03	0.21	0.20	0.13	0.17	0.26

Στη συνέχεια αν εφαρμόσουμε τη MAUT για πρόβλημα μεγιστοποίησης ως προς όλα τα κριτήρια παίρνουμε τον ακόλουθο πίνακα. Αξίζει να σημειώσουμε ότι ο πίνακας περιέχει κατάταξη των εναλλακτικών και για τα 2 σετ βαρών που υπολογίσαμε.

Cryptocoin			
	MAUT Score (AHP w)		**MAUT Score (AHP+Entropy w)**
BTC	0.910	BTC	0.941
ETH	0.567	ETH	0.431
XMR	0.445	XMR	0.305
DASH	0.354	DASH	0.241
BCH	0.185	BCH	0.131
XRP	0.143	XRP	0.123
LTC	0.048	LTC	0.041

Από τη συγκεκριμένη μέθοδο λοιπόν καταλήγουμε στο συμπέρασμα και για τα 2 σετ βαρών ότι: **BTC> ETH> XMR> DASH> BCH> XRP> LTC**

3.3.2 Electre I with Veto

Η επόμενη μέθοδος αξιολόγησης των κρυπτονομισμάτων είναι η Electre I with veto, μια υβριδική έκδοση της Electre I που βρίσκει πολύ καλή εφαρμογή στα πρόβλημα επιλογής κρυπτονομισμάτων. Ειδικά για τα κριτήρια που απεικονίζουν την ποσοστιαία διαφορά στην αυξομείωση της τιμής του κάθε νομίσματος (τα οποία όπως έχουμε αναφέρει και νωρίτερα θεωρούνται τα σημαντικότερα) θέτουμε βέτο την ποσοστιαία διαφορά των 25%. Δηλαδή για εναλλακτικές που έχουν για κάποιο από τα 3 αυτά κριτήρια ποσοστιαία διαφορά πάνω από 25% στα δεδομένα, τότε το αποτέλεσμα του πίνακα συμφωνίας δεν θα θεωρείται αξιόπιστο, όσο υψηλό σκορ και αν έχει.

Ακολουθούν κατά σειρά ο τροποποιημένος πίνακας δεδομένων για την Electre I with Veto και οι πίνακες συμφωνίας/ασυμφωνίας για τα σετ βαρών με AHP και με AHP + Entropy αντίστοιχα:

Cryptocoin	**Criteria**					
	Years Active	**million $ Capitalization**	**million $ mined last year**	**% 3month change**	**% 6month change**	**% 12month change**
BTC	12	169407.3	6889.398	-6.37	28.86	14.87
ETH	5	23063.5	1141.475	-23.35	41.53	-16.66
XRP	8	8823.6	617.136	-28.66	-9.25	-47.99
BCH	3	4329.5	225.564	-40.73	11.57	-42.57
LTC	9	2861.9	202.387	-43.84	-3.72	-56.06
XMR	6	1135.3	53.090	-23.34	29.40	-25.70
DASH	6	704.3	92.549	-30.39	49.03	-52.50
Max Values	12	169407.3	6889.398	-6.37	49.03	14.87
Min Values	3	704.3	53.090	-43.84	-9.25	-56.06
Veto	-	-	-	25.00	25.00	25.00
AHP Weights	0.031	0.059	0.086	0.176	0.260	0.388
AHP+Entropy Weights	0.027	0.212	0.200	0.129	0.172	0.261
Target	**maximize**	**maximize**	**maximize**	**maximize**	**maximize**	**maximize**

Πίνακας Συμφωνίας/Ασυμφωνίας with AHP weights		
	Πίνακας Συμφωνίας	**Πίνακας Ασυμφωνίας**

Cryptocoin	BTC	ETH	XRP	BCH	LTC	XMR	DASH	BTC	ETH	XRP	BCH	LTC	XMR	DASH
BTC	1.000	0.740	1.000	1.000	1.000	0.740	0.740	0	0	0	0	0	0	0
ETH	0.260	1.000	0.969	1.000	0.969	0.793	0.709	1	0	0	0	0	0	0
XRP	0.000	0.031	1.000	0.352	0.709	0.175	0.740	1	1	0	0	0	1	1
BCH	0.000	0.000	0.648	1.000	0.969	0.145	0.533	1	1	0	0	0	0	1
LTC	0.000	0.031	0.291	0.031	1.000	0.175	0.175	1	1	0	0	0	1	1
XMR	0.260	0.207	0.825	0.855	0.825	1.000	0.654	1	0	0	0	0	0	0
DASH	0.260	0.291	0.260	0.467	0.825	0.377	1.000	1	1	0	0	0	1	0

Πίνακας Συμφωνίας/Ασυμφωνίας with AHP+Entropy weights														
	Πίνακας Συμφωνίας							Πίνακας Ασυμφωνίας						
Cryptocoin	BTC	ETH	XRP	BCH	LTC	XMR	DASH	BTC	ETH	XRP	BCH	LTC	XMR	DASH
BTC	1.000	0.828	1.000	1.000	1.000	0.828	0.828	0	0	0	0	0	0	0
ETH	0.172	1.000	0.973	1.000	0.973	0.845	0.802	1	0	0	0	0	0	0
XRP	0.000	0.027	1.000	0.567	0.802	0.439	0.828	1	1	0	0	0	1	1
BCH	0.000	0.000	0.433	1.000	0.973	0.412	0.673	1	1	0	0	0	0	1
LTC	0.000	0.027	0.198	0.027	1.000	0.439	0.439	1	1	0	0	0	1	1
XMR	0.172	0.155	0.561	0.588	0.561	1.000	0.629	1	0	0	0	0	0	0
DASH	0.172	0.198	0.172	0.327	0.561	0.398	1.000	1	1	0	0	0	1	0

Αξίζει να σημειώσουμε ότι στους πίνακες ασυμφωνίας με πορτοκαλί χρώμα είναι τα κελιά όπου εντοπίστηκε ασυμφωνία μεταξύ των εναλλακτικών. Τέλος θέτοντας ως δείκτη σχέσης υπεροχής S κατά σειρά 1, 0.9 και 0.8 παίρνουμε τους 2 παρακάτω πίνακες (οι διάφορες αποχρώσεις του μπλε συμβολίζουν τις διαφορετικές τιμές του S):

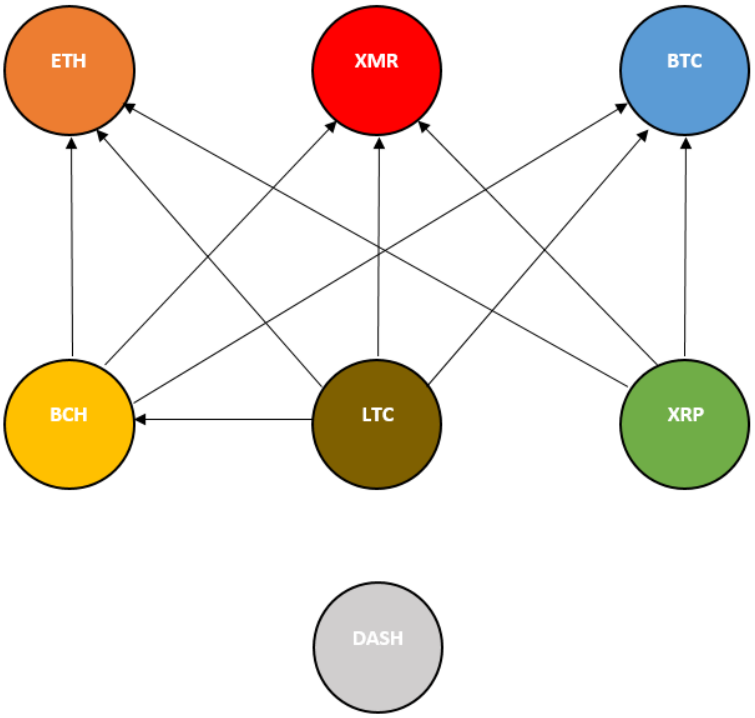
AHP weights		
S=1.0	S=0.9	S=0.8
BTC>XRP	BTC>XRP	BTC>XRP
BTC>BCH	BTC>BCH	BTC>BCH

BTC>LTC	BTC>LTC	BTC>LTC
ETH>BCH	ETH>BCH	ETH>BCH
	ETH>XRP	ETH>XRP
	ETH>LTC	ETH>LTC
	BCH>LTC	BCH>LTC
		XMR>XRP
		XMR>BCH
		XMR>LTC

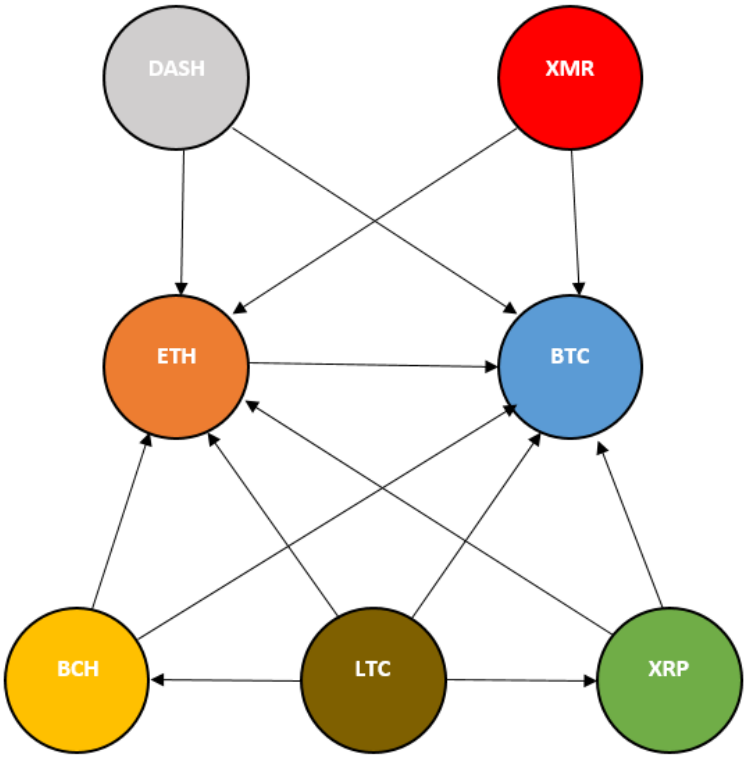
AHP & Entropy weights		
S=1.0	**S=0.9**	**S=0.8**
BTC>XRP	BTC>XRP	BTC>XRP
BTC>BCH	BTC>BCH	BTC>BCH
BTC>LTC	BTC>LTC	BTC>LTC
ETH>BCH	ETH>BCH	ETH>BCH
	ETH>XRP	ETH>XRP
	ETH>LTC	ETH>LTC
	BCH>LTC	BCH>LTC
		BTC>ETH
		BTC>XMR
		BTC>DASH
		ETH>XMR
		ETH>DASH
		XRP>LTC
		XRP>DASH

Ομοίως με πριν με πορτοκαλί χρωματίζονται οι εναλλακτικές που απορρίπτονται λόγω βέτο (μόνο μία). Παρατηρούμε ότι όσο ελαστικότεροι γινόμαστε μειώνοντας το S τόσο πιο πολλές σχέσεις υπεροχής λαμβάνουμε. Θεωρώντας λοιπόν ότι για S=0.8 έχουμε ένα ικανοποιητικό επίπεδο συμφωνίας προκύπτουν τα παρακάτω διαγράμματα προτίμησης για τις 2 υποπεριπτώσεις.

AHP weights



AHP+Entropy weights



3.3.3 *Promethee*

Τελευταία αφήσαμε την πολυκριτηριακή ανάλυση με τη μεγαλύτερη παραμετροποίηση (λόγω της επιλογής μεθόδου ανά κριτήριο) η οποία έχει και ένα ακόμα πολύ σημαντικό πλεονέκτημα: παρόλο που ανήκει στις μεθόδους σχέσεων υπεροχής κάνει κατάταξη των εναλλακτικών με τη χρήση των ροών εισόδου και εξόδου. Ακολουθεί ο τροποποιημένος πίνακας δεδομένων καθώς και οι πίνακες ροών για τα σετ βαρών με AHP και με AHP + Entropy αντίστοιχα:

Cryptocoin	**Criteria**					
	Years Active	**million $ Capitalization**	**million $ mined last year**	**% 3month change**	**% 6month change**	**% 12month change**
BTC	12	169407.3	6889.398	-6.37	28.86	14.87
ETH	5	23063.5	1141.475	-23.35	41.53	-16.66
XRP	8	8823.6	617.136	-28.66	-9.25	-47.99
BCH	3	4329.5	225.564	-40.73	11.57	-42.57
LTC	9	2861.9	202.387	-43.84	-3.72	-56.06
XMR	6	1135.3	53.090	-23.34	29.40	-25.70
DASH	6	704.3	92.549	-30.39	49.03	-52.50
Max Values	12	169407	6889	-6	49	15
Min Values	3	704	53	-44	-9	-56
Promethe Criteria Type	1	3	2	5	5	5
q - bottom limit	-	-	500	10	10	10
p - upper limit	-	20000	-	40	40	40
AHP Weights	0.031	0.059	0.086	0.176	0.260	0.388
AHP+Entropy Weights	0.027	0.212	0.200	0.129	0.172	0.261
Target	**maximize**	**maximize**	**maximize**	**maximize**	**maximize**	**maximize**

AHP weights

Final Ranking	BTC	ETH	XRP	BCH	LTC	XMR	DASH	Sum	Φ+
BTC	0.000	0.495	0.880	0.770	0.921	0.605	0.646	4.316	0.719
ETH	0.023	0.000	0.664	0.594	0.847	0.163	0.479	2.771	0.462
XRP	0.000	0.031	0.000	0.056	0.048	0.139	0.141	0.414	0.069
BCH	0.000	0.000	0.094	0.000	0.095	0.009	0.011	0.209	0.035
LTC	0.000	0.031	0.031	0.031	0.000	0.036	0.037	0.165	0.027
XMR	0.000	0.031	0.407	0.231	0.526	0.000	0.219	1.414	0.236
DASH	0.088	0.031	0.260	0.271	0.280	0.083	0.000	1.014	0.169
Sum	0.111	0.618	2.336	1.952	2.717	1.036	1.532		
Φ-	0.019	0.103	0.389	0.325	0.453	0.173	0.255		
Φ	0.701	0.359	-0.320	-0.291	-0.425	0.063	-0.086		

AHP+Entropy weights

Final Ranking	BTC	ETH	XRP	BCH	LTC	XMR	DASH	Sum	Φ+
BTC	0.000	0.656	0.913	0.846	0.947	0.730	0.760	4.851	0.809
ETH	0.015	0.000	0.708	0.710	0.884	0.424	0.637	3.378	0.563
XRP	0.000	0.027	0.000	0.083	0.085	0.308	0.313	0.816	0.136
BCH	0.000	0.000	0.062	0.000	0.076	0.034	0.038	0.210	0.035
LTC	0.000	0.027	0.027	0.027	0.000	0.045	0.050	0.175	0.029
XMR	0.000	0.027	0.271	0.163	0.355	0.000	0.151	0.966	0.161
DASH	0.058	0.027	0.172	0.185	0.186	0.055	0.000	0.684	0.114
Sum	0.073	0.763	2.153	2.014	2.534	1.596	1.948		
Φ-	0.012	0.127	0.359	0.336	0.422	0.266	0.325		
Φ	0.796	0.436	-0.223	-0.301	-0.393	-0.105	-0.211		

Με βάση τους παραπάνω πίνακες εύκολα προκύπτει η κατάταξη των εναλλακτικών κατά σειρά προτίμησης με βάση τα σκορ που φαίνονται παραπάνω.

AHP weights	
Cryptocoin	**Φ**
BTC	0.701
ETH	0.359

AHP+Entropy weights	
Cryptocoin	**Φ**
BTC	0.796
ETH	0.436

XMR	0.063
DASH	-0.086
BCH	-0.291
XRP	-0.320
LTC	-0.425

XMR	-0.105
DASH	-0.211
XRP	-0.223
BCH	-0.301
LTC	-0.393

Από την τελευταία μέθοδο λοιπόν καταλήγουμε στο συμπέρασμα και για καθένα από τα 2 σετ βαρών αντίστοιχα ότι:

BTC> ETH> XMR> DASH> BCH> XRP> LTC

BTC> ETH> XMR> DASH> XRP> BCH> LTC

4 Συμπεράσματα

Στο τελευταίο μέρος της εργασίας θα προχωρήσουμε στην εξαγωγή και στο σχολιασμό ορισμένων χρήσιμων συμπερασμάτων που προκύπτουν από τα αποτελέσματα των 3 μεθόδων με τους οποίους προσεγγίστηκε το πρόβλημα της επιλογής κρυπτονομίσματος. Με βάση λοιπόν όλα τα παραπάνω καταλήγουμε στις εξής διαπιστώσεις:

- Είναι απόλυτα ασφαλές να πούμε ότι το BTC είναι η βέλτιστη επιλογή κρυπτονομίσματος με βάση τον τρόπο ορισμού του προβλήματος και των εναλλακτικών. Έχει το καλύτερο σκορ σε MAUT και Promethee ανεξαρτήτως των σετ βαρών που χρησιμοποιούμε ενώ για την Electre I with veto το ίδιο ισχύει για την υποπερίπτωση όπου λαμβάνουμε υπόψη την εντροπία στα βάρη (υπερισχύει μια προς μια έναντι όλων των άλλων νομισμάτων). Δεν φαίνεται να έχουμε το ίδιο απόλυτο σκορ στην άλλη υποπερίπτωση της Electre I with veto όπου υπερισχύει μόνο των XRP, BCH και LTC ωστόσο αυτό σε καμία περίπτωση δεν υποβαθμίζει την ξεκάθαρη επιλογή του BTC έναντι των υπολοίπων νομισμάτων
- Εξίσου ασφαλές αποτέλεσμα μπορούμε να εξάγουμε και για το δεύτερο κατά σειρά προτίμηση νόμισμα που είναι το ETH. Τα σκορ του σε MAUT και Promethee είναι το ίδιο ξεκάθαρα με αυτά του BTC ενώ σε γενικές γραμμές ακολουθεί την ίδια συμπεριφορά ως προς τις σχέσεις υπεροχής όσον αφορά την Electre I with veto, όπου υπερτερεί όλων των εναλλακτικών (εκτός BTC) για το δεύτερο κατά σειρά σετ βαρών. Σε αυτό το σημείο αξίζει να αναφέρουμε ότι το γεγονός ότι και οι 3 μέθοδοι συνηγορούν κατηγορηματικά για την πρώτη και δεύτερη θέση στο πρόβλημα επιλογής νομίσματος είναι μια σαφής ένδειξη αφενός της ασφάλειας αυτού του αποτελέσματος και αφετέρου της ορθής επιλογής κριτηρίων και ορισμού του προβλήματος. Δηλαδή όταν ανεξαρτήτως μεθόδου έχουμε παρόμοια αποτελέσματα τότε συνηγορούμε στη διαπίστωση ότι το πρόβλημα έχει εξαρχής οριστεί στην σωστή του βάση
- Για τη επόμενη ομάδα νομισμάτων τα αποτελέσματα τείνουν σαφώς προς μια κατεύθυνση αλλά σε καμία περίπτωση δεν είναι τόσο κατηγορηματικά όσο για το BTC και ETH. Σύμφωνα λοιπόν με τα αποτελέσματα το XMR δείχνει να είναι η τρίτη καλύτερη εναλλακτική και το DASH η τέταρτη κατά MAUT και Promethee. Στην ίδια ομάδα ανήκει και το LTC η οποία κατατάσσεται ως η

χειρότερη εναλλακτική όλων. Μάλιστα το LTC καταλαμβάνει τη τελευταία θέση και με βάση στοιχεία που προκύπτουν από την Electre I with veto καθώς υστερεί σε σύγκριση έναντι πολλών άλλων νομισμάτων (BTC, ETH, BCH, XMR, XRP). Επίσης σύμφωνα με την Electre I with veto το XMR υπερισχύει έναντι αρκετών άλλων εναλλακτικών (XRP, BCH, LTC) κάτι που ισχυροποιεί την κατάταξη του ως τρίτη εναλλακτική. Δεν μπορούμε να πούμε ωστόσο το ίδιο και για το DASH.

- Στην τρίτη και τελευταία ομάδα νομισμάτων ανήκουν τα BCH και XRP τα οποία εμπεριέχουν και τη μεγαλύτερη αβεβαιότητα ως προς την κατάταξη τους. Τα BCH και XRP καταλαμβάνουν την πέμπτη και έκτη κατά σειρά θέση σύμφωνα με τη MAUT και τη Promethee, μόνο όμως όταν χρησιμοποιήσουμε τα το σετ βαρών κατά AHP. Αντίθετα για το σετ βαρών κατά AHP και εντροπία καταλαμβάνουν τις αντίθετες ακριβώς θέσεις. Επίσης κατά την Electre I with veto και οι 2 υπερισχύουν του LTC αλλά δεν λαμβάνουμε καμία άλλη πληροφορία σχετικά με τη μεταξύ τους σύγκριση.
- Αν λοιπόν χρειαζόταν να καταλήξουμε σε ένα τελικό πίνακα κατάταξης βασιζόμενοι στα αποτελέσματα όλων των μεθόδων θα είχαμε τον παρακάτω:

Rank	Cryptocoin
1	BTC
2	ETH
3	XMR
4	DASH
5	BCH
6	XRP
7	LTC

- Το πιο ενδιαφέρον στοιχείο που παρατηρήθηκε από τα εν λόγω αποτελέσματα είναι η διαφοροποίηση στη σειρά προτίμησης των νομισμάτων σε σχέση με το πιο χαρακτηριστικό κριτήριο αξιολόγησης τους για έναν απλό παρατηρητή: το δείκτη κεφαλαιοποίησης. Δηλαδή παρόλο που τα 2 πρώτα σε δείκτη κεφαλαιοποίησης νομίσματα είναι και αυτά που προηγούνται στη κατάταξη (BTC και ETH με αυτή τη σειρά) από εκεί και πέρα έχουμε αξιοσημείωτες διαφοροποιήσεις. Το πιο αξιοσημείωτο όλων αποτελεί το XRP το οποίο παρόλο που είναι τέταρτο σε κεφαλαιοποίηση (μέχρι πρόσφατα ήταν τρίτο) υστερεί ένα σχεδόν όλων των άλλων εναλλακτικών εκτός του LTC. Επίσης το LTC που είναι έβδομο σε κεφαλαιοποίηση κατατάσσεται ως η χειρότερη εναλλακτική. Το ίδιο ισχύει αλλά σε μικρότερο βαθμό και για το BCH που είναι πέμπτο σε κεφαλαιοποίηση αλλά υστερεί σε σχέση με το XMR και το DASH, τα οποία αποτελούν τους άτυπους νικητές της σύγκρισης. Μπορεί λοιπόν να εντοπίζονται σ χαμηλότερες θέσεις στο δείκτη κεφαλαιοποίησης (17 και 22) ωστόσο από το αποτέλεσμα της ανάλυσης προκύπτει ότι υπερτερούν σαφώς έναντι όλων των υπολοίπων (εκτός των 2 «γιγάντων»)
- Όπως έχουμε αναφέρει και στην αρχή της παρούσας εργασίας στόχος μας είναι η κατάταξη των κρυπτονομισμάτων σε σειρά προτίμησης βασιζόμενοι σε συγκεκριμένα κριτήρια. Το επόμενο ερώτημα που εύλογα προκύπτει είναι το εξής: αν κάποιος επενδυτής θέλει να κατανείμει το χαρτοφυλάκιο του ανάμεσα σε αυτά τα κρυπτονομίσματα, ποιος θα ήταν ο βέλτιστος τρόπος ώστε να του

επιφέρει το μέγιστο δυνατό κέρδος. Αυτό θα ήταν ένα εντελώς ξεχωριστό πρόβλημα το οποίο ενδεχομένως να ενσωμάτωνε άλλα κριτήρια βασισμένα στην αξιολόγηση του αποφασίζοντα σχετικά με το ενεχόμενο ρίσκο, το μακροπρόθεσμο ή βραχυπρόθεσμο χαρακτήρα της επένδυσης, το ποσό της επένδυσης κ.α. Μια τέτοιου είδους μελέτη απαιτεί και τα αντίστοιχα λογισμικά ώστε να διεκπεραιωθεί (π.χ. Weka, Virtual Promethee)

- Μια ενδιαφέρουσα παραλλαγή της παρούσας εργασίας θα αποτελούσε μια πιο «ριψοκίνδυνη» κατάταξη όχι τόσο δημοφιλών νομισμάτων χαμηλότερης κεφαλαιοποίησης με στόχο το βραχυπρόθεσμο κέρδος από τη πρόβλεψη ενός πιθανού μελλοντικού peak στη τιμή του νομίσματος. Σε αυτή τη περίπτωση θα δίνονταν ακόμη μεγαλύτερο βάρος στα κριτήρια που αφορούσαν τη ποσοστιαία μεταβολή της τιμής του νομίσματος ενώ ενδέχεται να μεταβάλλονταν και τα διαστήματα παρατήρησης των αλλαγών (από μέγιστο βάθος 12 μηνών να πηγαίναμε σε μέγιστο βάθος 6 μηνών). Με την κατάλληλη τροποποίηση της φόρμας υπολογισμών η ανάλυση μπορεί να επεκταθεί εύκολα για παραπάνω εναλλακτικές και κριτήρια

5 Βιβλιογραφία

1. Farell (2015), An Analysis of the Cryptocurrency Industry. Wharton Research Scholars Journal. Paper 130. http://repository.upenn.edu/wharton_research_scholars/130
2. URL: https://www.bitcoincash.org/
3. Greydon, (2014), What is Cryptocurrency. US Consumer Research Survey. https://www.cryptocoinsnews.com/cryptocurrency/
4. Bunjaku F., Gorgieva-Trajkovska O., Miteva-Kacarski E. (2017), "Cryptocurrencies – advantages and disadvantages", Journal of Economics Vol. 2
5. Wai Yan Maung Maung Thin, Naipeng Dong, Guangdong Bai, and Jin Song Dong (2018), "Formal Analysis of a PoS Blockchain"
6. Rajeev Sobti, G. Geetha (2012), Cryptographic Hash Functions: A Review
7. Market capitalization of cryptocurrencies, https://coinmarketcap.com/
8. Block, https://en.bitcoin.it/wiki/Block
9. Satoshi Nakamoto (2008), "Bitcoin: A peer-to-peer electronic cash system"
10. Vitalik Buterin (2013), "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform"
11. URL: https://docs.ethhub.io/
12. URL: https://xrpl.org/concepts.html
13. David Schwartz, Noah Youngs, and Arthur Britto (2014), "The Ripple protocol consensus algorithm", Ripple Labs

14. URL: https://litecoin.org/el/
15. Evan Duffield, Daniel Diaz, Dash: A payments-focused cryptocurrency
16. URL: https://www.getmonero.org/
17. Dash Developer Reference. URL: https://dash-docs.github.io/en/developerreference
18. Μεταξάκης Ε. (2018). Τι ακριβώς είναι το Bitcoin;, http://www.huffingtonpost.gr, 30 Μαΐου 2017. Διαθέσιμο: https://www.huffingtonpost.gr/emmanouil-metaksakis/bitcoin-_b_16866934.html,
19. Anderson A. (2017), Introductory Guide to Cryptocurrencies: The ultimate Guide to Blockchain, Mining, Trading, ICO's, Platforms, Exchanges, etc., 25 Eagles via Publish- Drive.
20. Τραχανάς Γ. Βρεττού Ι. (2019), Κρυπτονομίσματα Τεχνικά χαρακτηριστικά και συγκριτική μελέτη, Πτυχιακή εργασία, Εθνικό και Καποδιστριακό Πανεπιστήμιο
21. Δούκας Χ. Ξυδώνας Π. Ψαρράς Ι. (2017), Πολυκριτηριακά συστήματα υποστήριξης αποφάσεων, Σημειώσεις μαθήματος, Εθνικό Μετσόβιο Πολυτεχνείο Σχολή Ηλ. Μηχανικών και Μηχανικών Η/Υ Τομέας Ηλ. Βιομηχανικών Διατάξεων & Συστημάτων Αποφάσεων
22. Ζοπουνίδης Κ. Δούμπος Μ. (2001), Πολυκριτήριες τεχνικές ταξινόμησης: Θεωρία και Εφαρμογές
23. Polasik M. (2014), Price fluctuations and the use of Bitcoin: An empirical Inquiry. International Journal of Electronic Commerce, 20:1, 9-49, DOI: 10.1080/10864415.2016.1061413.
24. Zahid M. (2015), Bitcoins: Mining, Transactions, Security Challenges and Future of this currency, [e-book] Universals-Publishers.