ΠΟΛΥΤΕΧΝΕΙΟ
ΚΡΗΤΗΣ

ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ ΠΑΡΑΓΩΓΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ

Διπλωματική εργασία

Θέμα: Αξιολόγηση Κρυπτονομισμάτων

Επιμελητής εργασίας: Αναστάσιος Τζουλουχάς

Επιβλέπων καθηγητής: Νικόλαος Ματσατσίνης

Τριμελής Επιτροπή

Ματσατσίνης Νικόλαος

Ζοπουνίδης Κωνσταντίνος

Τσαφαράκης Στέλιος

ΠΕΡΙΛΗΨΗ

Η διπλωματική αυτή εργασία έχει ως σκοπό αρχικά να παρουσιάσει αναλυτικά τι είναι και πως λειτουργούν τα κρυπτονομίσματα και στη συνέχεια να προχωρήσει στην πολυκριτήρια αξιολόγηση αυτών των νομισμάτων με βάση ένα σύνολο κριτηρίων – χαρακτηριστικών. Για να επιτευχθεί αυτό, θα γίνει αρχικά καταγραφή αυτών των ηλεκτρονικών νομισμάτων, των χαρακτηριστικών τους καθώς και της υφιστάμενης κατάστασης του χώρου. Επίσης, καταγράφονται και περιγράφονται οι παράγοντες που τα επηρεάζουν καθώς και τα δυνατά και αδύνατα σημεία τους. Ακολούθως, γίνεται ανάλυση και αξιολόγηση των χαρακτηριστικών τους με εφαρμογή μεθόδων ανάλυσης δεδομένων, πολυκριτήριας ανάλυσης αλλά και τεχνικών εξόρυξης γνώσης από δεδομένα (data mining). Χρησιμοποιείται το εργαλείο εξόρυξης δεδομένων Weka 3.6 καθώς και το Gaia Virtual Promethee.

Κατάλογος περιεχομένων

Κατάλογος εικόνων

1. ΕΙΣΑΓΩΓΗ

1.1 ΧΡΗΜΑ ΚΑΙ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ

Τα “χρήματα" έχουν τρία βασικά χαρακτηριστικά: αποτελούν ένα αποθηκευτικό μέσο αξίας, μια λογιστική μονάδα και ένα μέσο ανταλλαγής - αν και το χρήμα δεν είναι υποχρεωτικό να αποτελεί νόμιμη μονάδα. Εκ πρώτης όψεως τα κρυπτο-νομίσματα θα μπορούσε να θεωρηθεί ότι πληρούν όλα τα χαρακτηριστικά του χρήματος, όπως ορίστηκαν παραπάνω. Αποτελούν μια πιθανή αποθήκη αξίας, αν και πολύ ασταθής. Θα μπορούσαν να χρησιμοποιηθούν ως λογιστική μονάδα και, με την πρώτη γνωστή λιανικής μορφή τους - το Bitcoin, μπορούν να χρησιμοποιηθούν ως μέσο ανταλλαγής για όποιον επιθυμεί να τα αποδεχθεί. Σε αυτό το τελευταίο ρόλο, έχουν σημαντικά πλεονεκτήματα, δεδομένου ότι μπορούν να χωριστούν ψηφιακά για κάθε μέγεθος της συναλλαγής και να αποφεύγουν τα υψηλά τέλη που χρεώνονται από εταιρείες πιστωτικών καρτών. Αλλά είναι πιθανό ότι ο κύριος λόγος που τα κρυπτο-νομίσματα "απογειώνονται" σε δημοτικότητα ως μέσο πληρωμής, οφείλεται στην δυνατότητα της ανωνυμίας. Ο υψηλός βαθμός ανωνυμίας, αποτελεί χαρακτηριστικό με μεγάλα πλεονεκτήματα για παράνομες δραστηριότητες, όπως το ξέπλυμα χρήματος, την αποφυγή των δημοσιονομικών κανονισμών, τη χρηματοδότηση της τρομοκρατίας και τη φοροδιαφυγή (Blundell-Wignall, 2014).

Η οικονομική κρίση οδήγησε σε απώλεια εμπιστοσύνης σε πολλούς ενδιάμεσους χρηματοπιστωτικούς οργανισμούς, πλατφόρμες συναλλαγών και συστήματα πληρωμών. Η βασική καινοτομία στην οποία βασίστηκαν τα κρυπτο-νομίσματα είναι το χαρακτηριστικό των συναλλαγών που δεν βασίζονται στην εμπιστοσύνη (η δυνατότητα να αποφευχθεί η ανάγκη για ένα έμπιστο τρίτο μέρος). Η ανταλλαγή είναι πάντα δυνατή – για παράδειγμα οι υαλοκαθαριστές μπορούν να διαπραγματευτούν με τα καταστήματα και τα ιατρεία για την ανταλλαγή ωρών καθαρισμού με αγαθά και υπηρεσίες. Ωστόσο, η ανταλλαγή είναι ένα φτωχό μέσο

ανταλλαγής και μια υπηρεσία, όπως ο καθαρισμός, δεν μπορεί να αποθηκευτεί επιτυχώς (και ως εκ τούτου δεν υπάρχει αποθήκευση της αξίας). Μάρκες καζίνο, αεροπορικά μίλια, πιστώσεις Amazon, χρήματα Disney θα μπορούσαν επίσης να χρησιμοποιηθούν για ορισμένες λειτουργίες εκτός της πρωτογενούς σκοπούμενης χρήση τους, αλλά όχι με τα πιθανά χαρακτηριστικά ευχρηστίας των κρυπτο-νομισμάτων στην ψηφιακή εποχή (CFA, 2015).

Από την άλλη πλευρά, τα κρυπτο-νομίσματα δεν μπορούν να αποτελέσουν μια εναλλακτική λύση για το νόμιμο νόμισμα, για τον απλό λόγο (όπως θα εξηγηθεί παρακάτω) ότι οι άνθρωποι πρέπει να πληρώνουν τους φόρους τους. Αυτό προστατεύει τα υπάρχοντα νομίσματα από αντικατάσταση, και ο φόβος της απώλειας του νομισματικού ελέγχου δεν θα πρέπει να χρησιμοποιείται ως επιχείρημα για την πρόληψη της κυκλοφορίας των Bitcoins ως παράλληλα νομίσματα. Ωστόσο, η τεχνολογία των ψηφιακών πρωτοκόλλων πληρωμών δεν θα πρέπει να συγχέεται με το θέμα "παράλληλο νόμισμα". Όσον αφορά τη λειτουργία του νομίσματος, υπάρχουν δύο πιθανά ζητήματα πολιτικής: (α) θέματα προστασίας των καταναλωτών: π.χ. ηλεκτρονική κλοπή, η κατάρρευση της αξίας των κρυπτο-νομισμάτων για παράδειγμα λόγω της εμφάνισης των υποκατάστατων, η χρήση της εξουσίας της κυβέρνησης για την απαγόρευσή τους, κλπ .και (β) τα χαρακτηριστικά της ανωνυμίας που επιτρέπει την επέκταση των παράνομων δραστηριοτήτων, όπως η φοροδιαφυγή και το ξέπλυμα χρήματος. Η ψηφιακή τεχνολογία μεταφοράς, από την άλλη πλευρά, θα μπορούσε να παίξει κοινωνικά χρήσιμους ρόλους (Blundell-Wignall, 2014).

1.2 Ορισμος κρυπτονομισματων μεσω του Bitcoin

Όσον αφορά το Bitcoin, οι ιδρυτές του παρείχαν στην αγορά αλγορίθμους για την πρόωρη εξόρυξη (mining) που έχουν συγκεντρώσει το πρώτο απόθεμα Bitcoins. Οι κάτοχοι των αποθεμάτων αυτών επωφελήθηκαν από τις μεταγενέστερες αυξήσεις των τιμών. Με τη χρήση ηλεκτρονικών υπολογιστών και εντατικά αναλαμβάνοντας το υψηλό κόστος ηλεκτρικής ενέργειας, εν συνεχεία οι συμμετέχοντες μπορούσαν

να εξορύξουν Bitcoins, εκ των οποίων συνολικά 21 εκατομμύρια είναι ο σταθερός εφοδιασμός. Η συνάρτηση προσφοράς για τα νομίσματα απλώνεται με τη μείωση του μεγέθους του μπλοκ και μέσω ενός αλγόριθμου με τον οποίο η εύρεση τους γίνεται πολύ πιο δύσκολη, αν βρίσκονται πολύ γρήγορα. Μπορεί να πάρει πολλά χρόνια για να γίνει εξόρυξη όλων των Bitcoin. Οι συναλλαγές Bitcoins γίνονται στην online αγορά και ο καθένας μπορεί να τα αγοράσει στη συναλλαγματική ισοτιμία με το δολάριο από τις πλατφόρμες Bitcoin (όπως η Coinbase), αν και η τιμή έχει αποδειχθεί ότι είναι πολύ ασταθής μέχρι σήμερα (FinCen, 2013).

Η ψηφιακή τεχνολογία μεταφοράς είναι πολύ ενδιαφέρουσα. Υπάρχει ένα open source κλειδί κρυπτολογίας, ένα δημόσιο και ένα ιδιωτικό. Οι Bitcoin συναλλαγές μεταβιβάζουν την κυριότητα του νομίσματος από τη μια δημόσια διεύθυνση στην άλλη, αλλά απαιτείται ένα ιδιωτικό κλειδί για την αποκρυπτογράφηση των Bitcoins και την περαιτέρω κατανάλωση τους. Τα δημόσια και τα ιδιωτικά κλειδιά είναι αλφαριθμητικές ακολουθίες που βασίζονται σε εξελιγμένη κρυπτογράφηση: Οι τυχαίοι αριθμοί και τα γράμματα στα δημόσια κλειδιά προέρχονται από την εφαρμογή της συνάρτησης "hash". Η ταυτοποίηση είναι σαν τη λήψη δακτυλικών αποτυπωμάτων - μπορεί να υπάρχει μόνο μία γεννήτρια μεταβίβασης από μια δεδομένη διεύθυνση (αν και φυσικά η αποθήκευση ιδιωτικών ακολουθιών ταυτοποίησης σε απευθείας σύνδεση ανοίγει το δρόμο για την κλοπή και την απάτη, όπως σε όλα τα ζητήματα, όπου εμπλέκονται χρήματα και το διαδίκτυο). Τα Bitcoins με τη μορφή των δημόσιων κλειδιών αποθηκεύονται σε "πορτοφόλια", στο σκληρό δίσκο του υπολογιστή και μπορούν να προσπελαστούν μόνο με το ιδιωτικό κλειδί. Η ασφάλεια από hacking αυξάνεται με την χρήση της off-line ψυχρής αποθήκευσης, και οι υπηρεσίες αυτές παρέχονται από τις πλατφόρμες συναλλαγών. Τα πορτοφόλια που αποθηκεύονται με σύνδεση στο Διαδίκτυο, ή συνδέονται με μια εφαρμογή smartphone, είναι παρόμοια με μετρητά, και τα Bitcoins μπορούν να μετακινηθούν από τη ψυχρή αποθήκευση στα κινητά πορτοφόλια, όπως απαιτείται (FinCen, 2013).

Οι συναλλαγές καταγράφονται στην "αλυσίδα μπλοκ", η οποία είναι το κλειδί για την καινοτομία στην τεχνολογία αυτή - δηλαδή, μια τεχνολογία που εξαλείφει την ανάγκη για ένα έμπιστο τρίτο μέρος και ενδιάμεσες δαπάνες που συνδέονται με τα

εν λόγω ιδρύματα (τράπεζες, εταιρείες πιστωτικών καρτών, εταιρείες πληρωμής, μη τραπεζικούς χρηματοπιστωτικούς διαμεσολαβητές).

Η αλυσίδα μπλοκ είναι μια δημόσια βάση δεδομένων (γιγάντιο καθολικό βιβλίο), που συντηρείται ανοιχτά από τους υπολογιστές σε όλο τον κόσμο - είναι μια διαδοχική καταγραφή όλων των συναλλαγών και της τρέχουσας ιδιοκτησίας. Αυτή η παρακολούθηση και ο έλεγχος των συναλλαγών υποστηρίζονται από την αποκεντρωμένη υπολογιστική ισχύ που παράγεται από τη δραστηριότητα της «εξόρυξης», και αυτή η δραστηριότητα ανταμείβεται σε Bitcoin αμοιβές. Η αλυσίδα μπλοκ επιτρέπει στους συμμετέχοντες να ελέγξουν κατά πόσον οι διαβιβάσεις νομισμάτων προέρχονται από τους πραγματικούς τους ιδιοκτήτες και αποφεύγει προβλήματα όπως οι διπλές δαπάνες - το ίδιο κλάσμα Bitcoin δεν μπορεί να περάσει πάνω από μία φορά.

Αυτή η τεχνολογία Bitcoin έχει γεννήσει μια ταχέως αναπτυσσόμενη βιομηχανία καινοτομιών κρυπτο-νομισμάτων που χρησιμοποιούν ανεξάρτητες μεθόδους αλυσίδας μπλοκ (π.χ. Bitcoin, Litecoin, dogecoin, NXT, BitShares και Ethereum).

Άλλα πρωτόκολλα είναι χτισμένα στην κορυφή της αλυσίδας μπλοκ Bitcoin και εκτελούν ενδιαφέροντα πράγματα, όπως και οι μάρκες που ταυτίζονται με συγκεκριμένα στοιχεία ενεργητικού για εμπορικούς σκοπούς (Coloured Coins, Mastercoin, και Counterparty). Η τεχνολογία Αλυσίδα Block έχει ένα σημαντικό πρόβλημα επεκτασιμότητας, όμως, σχετίζεται με την υπολογιστική ισχύ που απαιτείται για να υπολογίσει εκ νέου το ιστορικό όλων των συναλλαγών, ένα πρόβλημα το οποίο μεγαλώνει καθώς η χρήση Bitcoins γίνεται πιο διαδεδομένη.

1.3 ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΠΡΟΒΛΗΜΑΤΟΣ

Τα κρυπτονομίσματα είναι φυσικά πρϋπολογισμένα αρχεία που χρησιμοποιούν ζεύγη δημόσιου - ιδιωτικού κλειδιού που δημιουργείται γύρω από ένα συγκεκριμένο αλγόριθμο κρυπτογράφησης. Το κλειδί εκχωρεί την κυριότητα του κάθε ζεύγους κλειδιών, ή «νόμισμα», στο πρόσωπο που έχει στην κατοχή του το ιδιωτικό κλειδί. Αυτά τα ζεύγη κλειδιών αποθηκεύονται σε ένα αρχείο με το όνομα

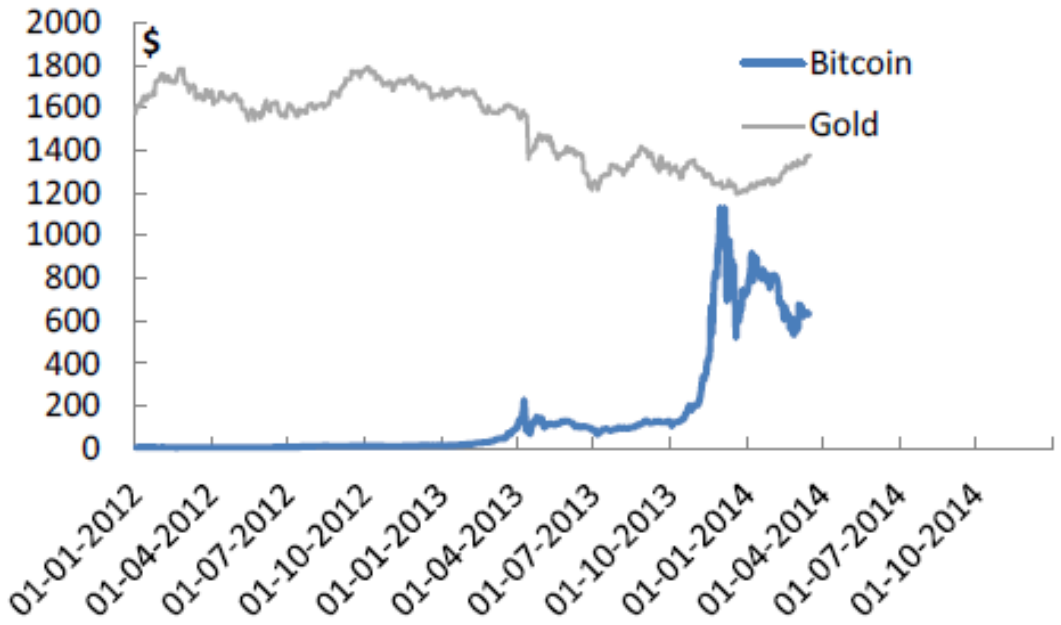
wallet.dat, το οποίο βρίσκεται σε ένα προεπιλεγμένο κρυφό κατάλογο στο σκληρό δίσκο του ιδιοκτήτη. Τα ιδιωτικά κλειδιά αποστέλλονται στους χρήστες που χρησιμοποιούν δυναμικές διευθύνσεις πορτοφολιών που δημιουργούνται από τους χρήστες που ασχολούνται με συναλλαγές. Η διεύθυνση πληρωμής προορισμού είναι το δημόσιο κλειδί του ζεύγους κλειδιών του κρυπτονομίσματος. Υπάρχει ένα πεπερασμένο ποσό των διαθέσιμων κρυπτονομισμάτων στο δίκτυο, και η αξία της κάθε μονάδας έχει ανατεθεί με βάση την προσφορά και τη ζήτηση, καθώς και οι διακυμάνσεις των επιπέδων δυσκολίας που απαιτείται για την εξόρυξη κάθε νομίσματος. Το αρχείο wallet.dat είναι το πιο σημαντικό αρχείο της αρχιτεκτονικής λογισμικού των κρυπτονομισμάτων, καθώς σε αυτό είναι αποθηκευμένο το φυσικό κρυπτογραφικό αρχείο του ιδιωτικού κλειδιού. Η αποκεντρωμένη φύση του πρωτοκόλλου ανοιχτού κώδικα εξασφαλίζει ότι ο έλεγχος του δικτύου παραμένει στα χέρια των χρηστών. Οι συναλλαγές εξαρτώνται από τους συμμετέχοντες στο δίκτυο, και ο χρήστης είναι υπεύθυνος για την ασφάλεια των δικών του οικονομικών και δεδομένων, χωρίς την ανάγκη εξάρτησης από τρίτα μέρη, όπως τα τραπεζικά ιδρύματα (Ahamad et al., 2013).

Για παράδειγμα, το Bitcoin λειτουργεί ως ένα p2p πρωτόκολλο κοινής χρήσης αρχείων, και ως εκ τούτου η ιδέα είναι παρόμοια με τη τεχνολογία .torrent. Το δίκτυο p2p στηρίζεται στη συμμετοχή των χρηστών για την επιτυχή ανταλλαγή εμπιστευτικών δεδομένων. Κάθε συναλλαγή επιβεβαιώνεται με κλειδί επαλήθευσης για πολλαπλούς κόμβους του δικτύου, πριν φτάσει στον προορισμό της. Αυτή η crowdsourced διαδικασία επαλήθευσης του κλειδιού εγγυάται την ακεραιότητα της μεταφοράς δεδομένων. Το πιο δημοφιλές κρυπτονόμισμα είναι το Bitcoin, αλλά υπάρχουν και εναλλακτικές λύσεις, όπως το Litecoin που γρήγορα κερδίζει έδαφος στην αγορά. Ο πηγαίος κώδικας για αυτά τα προγράμματα, καθώς και ο κωδικός για άλλα κρυπτονομίσματα, είναι διαθέσιμος στο κοινό (Segendorf, 2014).

Το Bitcoin είναι πραγματικά τρία πράγματα. Πρώτον, είναι ένα πρωτόκολλο (ή σύνολο κανόνων) που ορίζει τον τρόπο που θα πρέπει να λειτουργεί το δίκτυο. Δεύτερον, είναι ένα έργο λογισμικού που υλοποιεί το εν λόγω πρωτόκολλο. Τρίτον, είναι ένα δίκτυο υπολογιστών και συσκευών που τρέχουν το λογισμικό που

χρησιμοποιεί το πρωτόκολλο για να δημιουργήσει και να διαχειριστεί το νόμισμα Bitcoin (Segendorf, 2014).

Η Εικόνα 1 παρουσιάζει την τιμή Bitcoin σε σύγκριση με την τιμή του χρυσού. Η τιμή είναι μονοψήφια, το 2012, περίπου $ 100 για ένα μεγάλο μέρος του 2013 και στη συνέχεια κινείται γρήγορα στα $ 1.100 στο τέλος του έτους και καταρρέει προς το εύρος $ 500- $ 800 για τους πρώτους μήνες του 2014.



Εικόνα 1: Οι τιμές του Bitcoin σε σύγκριση με τις τιμές του χρυσού 2012-2014 (Πηγές: Datastream, Bitcoincharts.com.)

Τέτοιες ακραίες υψηλές τιμές μπορούν να εξηγηθούν από την έντονη ανελαστική ζήτηση και τη στενότητα προσφοράς. Υποθέτοντας ότι η ανωνυμία είναι σημαντική για ορισμένους συμμετέχοντες στην αγορά ώστε να αποφύγουν τους φόρους ή να ξεπλύνουν χρήματα, η ζήτηση μπορεί να υπερβεί την προσφορά και την εξόρυξη. Η πλευρά της προσφοράς μπορεί να είναι ένας σημαντικός παράγοντας. Για παράδειγμα, η δυσκολία της εξόρυξης μπορεί ξαφνικά να επιταχυνθεί ή οι εξορυκτές θα μπορούσαν να συμμετέχουν σε συμπεριφορές καρτέλ. Εναλλακτικά, η κερδοσκοπική ζήτηση ενδέχεται να εισέλθει στην αγορά, όπου κάθε συμμετέχων μπορεί να αγοράζει σε 10 ή 20 φορές το κόστος εξόρυξης πιστεύοντας ότι δεν έχει

σημασία, εφ 'όσον κάποιος άλλος είναι πρόθυμος να πληρώσει περισσότερο από αυτό - θεωρία "greater fool” (Segendorf, 2014).

Κρίνοντας από την ξαφνική και απότομη διόγκωση των συναλλαγών γύρω από το χρόνο της εκτίναξης των τιμών, η θεωρία "greater fool” είναι ίσως η σημαντικότερη αιτία. Η πρόσφατη αστάθεια των τιμών σίγουρα φαίνεται να έχει μικρή σχέση με την εύλογη αξία - και μέρος του προβλήματος για την αποτίμηση ενός κρυπτο-νομίσματος είναι ότι πρόκειται για μια τεχνολογία και όχι μια επιχείρηση με έναν ισολογισμό ή ένα νόμισμα που υποστηρίζεται από ένα εμπόρευμα.

Μέρος λοιπόν της αιτίας που προκαλεί ασταθή τιμή στα Bitcoin είναι ότι δεν υπάρχει σαφής εγγενής αξία ή συμφωνημένη μέθοδος αξιολόγησης, και σίγουρα δεν υπάρχει μια κεντρική τράπεζα Bitcoin, έτοιμη να παρέμβει για να καταστεί πιο σταθερή η τιμή, η οποία βέβαια θα παραβίαζε το στοιχείο της σταθερής προσφοράς.

Σε αυτά τα πλαίσια, στην παρούσα εργασία θα παρουσιαστούν τα χαρακτηριστικά των δημοφιλέστερων κρυπτονομισμάτων και θα επιχειρηθεί συγκριτική αξιολόγηση των χαρακτηριστικών τους (Segendorf, 2014).

1.4 ΣΚΟΠΟΣ ΤΗΣ ΕΡΓΑΣΙΑΣ

Στην παρούσα εργασία θα γίνει αναλυτική παρουσίαση των κρυπτονομισμάτων και της λειτουργίας τους, καταγραφή αυτών των ηλεκτρονικών νομισμάτων, των χαρακτηριστικών τους καθώς και της υφιστάμενης κατάστασης του χώρου. Στη βιβλιογραφική επισκόπηση θα γίνει καταγραφή της υφιστάμενης κατάστασης, με καταγραφή των μεθόδων και των κριτηρίων αξιολόγησης που χρησιμοποιούνται σήμερα. Στη συνέχεια αυτής της ανάλυσης, καταγράφονται και περιγράφονται οι παράγοντες που τα επηρεάζουν καθώς και τα δυνατά και αδύνατα σημεία τους. Τέλος, αναλύονται και αξιολογούνται τα χαρακτηριστικά τους με εφαρμογή μεθόδων ανάλυσης δεδομένων, πολυκριτήριας ανάλυσης αλλά και τεχνικών

εξόρυξης γνώσης από δεδομένα (data mining) με το εργαλείο εξόρυξης δεδομένων Weka 3.6.

1.5 ΟΡΓΑΝΩΣΗ ΤΗΣ ΕΡΓΑΣΙΑΣ

Στο πρώτο Κεφάλαιο έγινε μια πρώτη εισαγωγή στο θέμα των κρυπτονομισμάτων, παρουσιάστηκε η συσχέτιση τους με την έννοια του χρήματος και επιχειρήθηκε ο ορισμός τους με βάση το Bitcoin. Επίσης στοιχειοθετήθηκε το πρόβλημα αξιολόγησης των κρυπτονομισμάτων και οι συνέπειες αστάθειας στη τιμή τους, που αυτό επιφέρει.

Τα βασικά χαρακτηριστικά των κρυπτο-νομισμάτων περιγράφονται στο Κεφάλαιο 2, χρησιμοποιώντας το Bitcoin ως το κύριο παράδειγμα. Στο κεφάλαιο αυτό παρουσιάζονται τα χαρακτηριστικά και η λειτουργία των υπαρχόντων κρυπτονομισμάτων βάσει της βιβλιογραφικής επισκόπησης. Επίσης γίνεται λόγος για την εξόρυξη των κρυπτονομισμάτων, τις μεθόδους που τη διέπουν αλλά και τη σημασία της. Θα γίνει καταγραφή της υφιστάμενης κατάστασης, με καταγραφή των μεθόδων και των κριτηρίων αξιολόγησης που χρησιμοποιούνται σήμερα.

Στο Κεφάλαιο 3 γίνεται μοντελοποίηση του προβλήματος και κατασκευή ενός συνόλου κριτηρίων – χαρακτηριστικών με στόχο την υλοποίησης σύγκρισης και αξιολόγησης των εναλλακτικών επιλογών.

Στο Κεφάλαιο 4 τα χαρακτηριστικά των κρυπτονομισμάτων, ως αποτέλεσμα της καταγραφής του Κεφαλαίου 3, εισάγονται σε κατάλληλα εργαλεία (Excel, Weka 3.6) και τα αποτελέσματα της διαδικασίας αξιολόγησης με πολυκριτηριακές μεθόδους παρουσιάζονται και αιτιολογούνται αναλυτικά. Τέλος, στο Κεφάλαιο 5 παρουσιάζονται τα συμπεράσματα της εργασίας.

1.6 ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ- ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ

Η επιλογή των συγκεκριμένων 2 λογισμικών, έγινε κατα κύριο λόγο με βάση τα δεδομένα του προβλήματος μας καθώς και των 'ευκολιών' που αυτά μας προσφέρουν. Πιο συγκεκριμένα το weka, περιέχει μια συλλογή από εργαλεία οπτικοποίησης και αλγορίθμους για την ανάλυση δεδομένων και την προγνωστική μοντελοποίηση(οπως ακριβώς και θέλουμε για το πρόβλημα που αντιμετωπίζουμε), μαζί με γραφικές διεπαφές χρήστη για εύκολη πρόσβαση σε αυτές τις λειτουργίες.

Πιο αναλυτικά,

- Το λογισμικό weka είναι δωρεάν (GNU γενική άδεια δημόσιας χρήσης)
- Φορητότητα (γλώσσα προγραμματισμού java οπότε και τρέχει σε οποιαδήποτε σύγχρονη υπολογιστική πλατφόρμα
- Μια ολοκληρωμένη συλλογή δεδομένων προεπεξεργασίας καθώς και τεχνικές μοντελοποίησης, και τα 2 πολύ χρησιμα για τη φύση του προβλήματος που αντιμετωπίζουμε
- Αρκετά εύκολο και κατανοητό στη χρήση του(γραφικές διεπαφές χρήστη)

Το Weka υποστηρίζει διάφορες βασικές διεργασίες εξόριξης δεδομένων πιο συγκεκριμένα, προεπεξεργασία δεδομένων, ομαδοποίηση(χρήσιμη-αναγκαία για το προβλημα μας), ταξινόμηση, παλινδρόμηση, απεικόνιση, και την δυνατότητα επιλογής. Όλες οι τεχνικές του Weka στηρίζονται στην υπόθεση ότι τα δεδομένα είναι διαθέσιμα ως ένα απλό αρχείο ή συσχέτιση, όπου κάθε σημείο δεδομένων περιγράφεται από ένα σταθερό αριθμό των χαρακτηριστικών: κανονικά, αριθμητικά ή ονομαστικά χαρακτηριστικά(τα δικά μας χαρακτηριστικά είναι όλων των παραπάνω τύπων) , αλλά και κάποιοι άλλοι τύποι χαρακτηριστικών υποστηρίζονται επίσης). Το Weka παρέχει πρόσβαση σε SQL βάσεις δεδομένων , χρησιμοποιώντας Java Database Connectivity και μπορεί να επεξεργαστεί το αποτέλεσμα που επιστρέφονται από ένα ερώτημα βάσης δεδομένων. Δεν είναι ικανό για εξόρυξη από πολυ-σχεσιακές βάσεις δεδομένων, αλλά υπάρχει ξεχωριστό λογισμικό για τη μετατροπή μιας συλλογής συνδεδεμένων πινάκων της βάσης

δεδομένων σε έναν πίνακα που είναι κατάλληλος για επεξεργασία χρησιμοποιώντας το Weka.

ΜΕΘΟΔΟΙ PROMETHEE

Οι μέθοδοι που ανήκουν στην οικογένεια αυτή άρχισαν να αναπτύσσονται στα μέσα της δεκαετίας του 1980. Οι PROMETHEE I και II αποτελούν δύο από τις δημοφιλέστερες μεθόδους στο χώρο της πολυκριτήριας ανάλυσης. Οι δύο αυτές μέθοδοι είναι ίδιες όσον αφορά το στάδιο ανάπτυξης της σχέσης υπεροχής και διαφέρουν μόνο στη φάση της εκμετάλλευσης της σχέσης που αναπτύσσεται.

Γενικά, οι μέθοδοι PROMETHEE απαιτούν τον καθορισμό μίας ορισμένης συνάρτησης προτίμησης για κάθε κριτήριο. Αυτή η συνάρτηση χρησιμοποιείται για να υπολογιστεί ο βαθμός προτίμησης που σχετίζεται με την καλύτερη εναλλακτική στην περίπτωση των ανά ζεύγος συγκρίσεων. Οι PROMETHEE υπολογίζουν θετικές και αρνητικές ροές προτίμησης για κάθε εναλλακτική. Η θετική ροή εκφράζει το κατά πόσο μία εναλλακτική είναι η κυρίαρχη (δύναμη) ως προς τις άλλες, και η αρνητική το κατά πόσο κυριαρχείται από τις υπόλοιπες. Η PROMETHEE I βασιζόμενη σε αυτές τις ροές μας οδηγεί σε μία μερική κατάταξη, ενώ η PROMETHEE II μας δίνει μία πλήρη κατάταξη που βασίζεται στην εξισορρόπηση των δύο ποών προτίμησης.

Το πρώτο στάδιο της ανάπτυξης της σχέσης υπεροχής ξεκινάει με τον προσδιορισμό του δείκτη προτίμησης (preference index) $\pi(x_i,x_j)$ για κάθε ζεύγος εναλλακτικών δραστηριοτήτων x_i και x_j , που ορίζεται ως:

$$\pi(x_i,x_j)=\sum_{k=1}^{n} w_k\, p_k(x_i, x_j) \quad \text{.....(6)}$$

Ο δείκτης αυτός ορίζεται με παρόμοιο τρόπο με το δείκτη συμφωνίας στις μεθόδους ELECTRE.

Ο μερικός δείκτης προτίμησης $p_k(x_i, x_j)$ για το κριτήριο x_k ορίζεται σε συνάρτηση της διαφοράς x_{ik}-x_{jk} μεταξύ των επιδόσεων των δύο εναλλακτικών στο κριτήριο x_k. Ειδικότερα:

$$p_k(x_i, x_j) = \begin{cases} 0 & x_{ik} < x_{jk} \\ h_k(x_{ik} - x_{jk}) & x_{ik} \geq x_{jk} \end{cases} \quad \text{.....(7)}$$

Υπάρχουν έξι περιπτώσεις γενικευμένων κριτηρίων για τη μορφή της συνάρτησης h_k (generalised criteria). Συγκεκριμένα:

1. Το σύνηθες κριτήριο (usual criterion): ο αποφασίζων είναι αδιάφορος μεταξύ δύο εναλλακτικών x_i και x_j στο κριτήριο $x_κ$ αν και μόνο αν $x_{iκ} = x_{jκ}$. Σε άλλη περίπτωση, αν $x_{iκ} > x_{jκ}$, ο αποφασίζων θεωρεί ότι υπάρχει σαφής προτίμηση της x_i έναντι της x_j . Οπότε η συνάρτηση h_k ορίζεται ως:

$$h_k(x_{ik} - x_{jk}) = \begin{cases} 0, & x_{ik} = x_{jk} \\ 1, & x_{ik} > x_{jk} \end{cases} \quad \text{.....(i)}$$

2. Το σχεδόν κριτήριο (quasi criterion): με βάση αυτό το κριτήριο, ο αποφασίζων θεωρεί ότι υπάρχει αδιαφορία μεταξύ των δύο εναλλακτικών x_i και x_j στο κριτήριο x_k, όταν η διαφορά x_{ik}-x_{jk} δεν υπερβαίνει ένα κατώφλι αδιαφορίας q_k. Διαφορετικά υπάρχει σαφής προτίμηση. Στην περίπτωση αυτού του κριτηρίου θα πρέπει να οριστεί το κατώφλι αδιαφορίας. Τότε, η η συνάρτηση h_k ορίζεται ως:

$$h_k(x_{ik} - x_{jk}) = \begin{cases} 0, & x_{ik} - x_{jk} < q_k \\ 1, & x_{ik} - x_{jk} \geq q_k \end{cases} \quad \text{.....(ii)}$$

3. Το γραμμικής προτίμησης κριτήριο (criterion with linear preference) : ο αποφασίζων θεωρεί ότι εφόσον η διαφορά x_{ik}-x_{jk} είναι μικρότερη από ένα

κατώφλι προτίμησης p_k, τότε η προτίμηση του για την x_i αυξάνει γραμμικά συναρτήσει της διαφοράς x_{ik}-x_{jk}. Όταν αυτή η διαφορά ξεπερνάει το κατώφλι προτίμησης p_k, τότε θα έχουμε σαφή προτίμηση. Η συνάρτηση h_k ορίζεται ως:

$$h_k(x_{ik}-x_{jk}) = \begin{cases} 1, & x_{ik}-x_{jk} \geq p_k \\ \dfrac{x_{ik}-x_{jk}}{p_k}, & x_{ik}-x_{jk} < p_k \end{cases} \quad \text{.....(iii)}$$

4. Το κριτήριο επιπέδου (level criterion) : στην περίπτωση αυτή χρησιμοποιούμε κατώφλι αδιαφορίας και κατώφλι προτίμησης. Εφόσον η διαφορά x_{ik}-x_{jk} βρίσκεται μεταξύ του διαστήματος $[q_k, p_k]$, τότε υπάρχει μία ελαφριά προτίμηση για την εναλλακτική x_i. Στις άλλες περιπτώσεις ισχύουν τα ίδια με τα δύο προηγούμενα κριτήρια. Δηλαδή, όταν η διαφορά x_{ik}-x_{jk} είναι μικρότερη από το κατώφλι αδιαφορίας q_k, τότε υπάρχει αδιαφορία ανάμεσα στις δύο εναλλακτικές. Όταν η διαφορά x_{ik}-x_{jk} είναι μεγαλύτερη από το κατώφλι προτίμησης p_k, τότε η προτίμηση είναι σαφώς για το x_i. Η συνάρτηση h_k ορίζεται ως:

$$h_k(x_{ik}-x_{jk}) = \begin{cases} 0 & x_{ik}-x_{jk} < q_k \\ 0{,}5 & x_{ik}-x_{jk} \in [q_k, p_k] \\ 1 & x_{ik}-x_{jk} > p_k \end{cases} \quad \text{.....(iv)}$$

5. Το γραμμικής προτίμησης και περιοχής αδιαφορίας (criterion with linear preference and indifference area) : ο αποφασίζων θεωρεί ότι η προτίμηση του αυξάνεται γραμμικά από την αδιαφορία στη σαφή προτίμηση, όταν η διαφορά x_{ik}-x_{jk} βρίσκεται ανάμεσα στο όριο αδιαφορίας και το όριο προτίμησης. Η συνάρτηση h_k ορίζεται ως:

$$h_k(x_{ik}-x_{jk}) = \begin{cases} 0 & x_{ik}-x_{jk} < q_k \\ \dfrac{x_{ik}-x_{jk}-q_k}{p_k-q_k} & x_{ik}-x_{jk} \in [q_k, p_k] \\ 1 & x_{ik}-x_{jk} > p_k \end{cases} \quad \text{.....(v)}$$

6. Το κριτήριο του Gauss (Gaussian criterion): οι προτιμήσεις σε αυτήν την περίπτωση περιγράφονται από μία συνεχή συνάρτηση με τη μορφή :

$$h_k(x_{ik} - x_{jk}) = 1 - \exp\left[-\frac{(x_{ik} - x_{jk})^2}{2\sigma^2}\right] \quad \text{.....(vi)}$$

όπου σ είναι η παράμετρος που καθορίζει το σημείο αλλαγής στην καμπή της συνάρτησης.

Ο καθορισμός της συνάρτησης h_k βοηθάει στον υπολογισμό του δείκτη προτίμησης $\pi(x_i, x_j)$ για κάθε ζεύγος εναλλακτικών. Ο δείκτης προτίμησης παίρνει τιμές από το 0 έως το 1 έτσι ώστε:

1.$\pi(x_i,x_j) \approx 0 \Rightarrow$ οριακή υπεροχή της x_i έναντι της x_j

2. $\pi(x_i,x_j) \approx 1 \Rightarrow$ ισχυρή υπεροχή της x_i έναντι της x_j.

Εκμεταλλευόμενοι τη σχέση υπεροχής, υπολογίζονται τα ακόλουθα μεγέθη:

1. Ροή εισόδου (entering flow): $\phi^-(x_i) = \sum_{\forall x_j \in A} \pi(x_j x_i)$ .....(8)
2. Ροή εξόδου (leaving flow): $\phi^+(x_i) = \sum_{\forall x_j \in A} \pi(x_i, x_j)$ .....(9)
3. Καθαρή ροή (net flow): $\phi(x_i) = \phi^+(x_i) - \phi^-(x_i)$.....(10)

Η ροή εξόδου $\phi^+(x_i)$ δείχνει την υπεροχή της εναλλακτικής x_i ως προς τις υπόλοιπες εναλλακτικές και η ροή εισόδου $\phi^-(x_i)$ δείχνει την υπεροχή όλων των υπόλοιπων εναλλακτικών έναντι x_i. Η καθαρή ροή είναι ένα συνολικό μέγεθος αξιολόγησης της εναλλακτικής x_i έναντι όλων των υπόλοιπων εναλλακτικών.

Στην PROMETHEE I οι παραπάνω ροές χρησιμοποιούνται στην ανάπτυξη δύο κατατάξεων. Η πρώτη κατάταξη Z_1 αναπτύσσεται βάσει των ροών εξόδου έτσι ώστε:

$x_i P_1 x_j \Leftrightarrow \phi^-(x_i) < \phi^-(x_j)$

$x_i I_1 x_j \Leftrightarrow \phi^-(x_i) = \phi^-(x_j)$

Η δεύτερη κατάταξη Z_2 αναπτύσσεται βάσει των ροών εξόδου έτσι ώστε:

$x_i P_2 x_j \Leftrightarrow \phi^+(x_i) < \phi^+(x_j)$

$x_i I_2 x_j \Leftrightarrow \phi^+(x_i) = \phi^+(x_j)$

Η τελική κατάταξη προκύπτει ως η τομή των δύο κατατάξεων ως εξής:

$$x_i P x_j \Leftrightarrow \begin{matrix} (x_i P_1 x_i) \wedge (x_i P_2 x_i) \\ (x_i P_1 x_i) \wedge (x_i I_2 x_i) \\ (x_i I_1 x_i) \wedge (x_i P_2 x_i) \end{matrix}$$

$$x_i I x_j \Leftrightarrow (x_i I_1 x_i) \wedge (x_i I_2 x_i)$$

$x_i R x_j \Leftrightarrow$ σε διαφορετική περίπτωση

Στην PROMETHEE II, αντίθετα, υπάρχει μόνο μία κατάταξη για τις εναλλακτικές, η οποία γίνεται βάση τις συνολικές τους ροές και η οποία είναι πλήρης (δηλαδή δεν λαμβάνουμε υπόψη τη σχέση ασυγκριτικότητας). Αυτή η κατάταξη ορίζεται ως εξής:

$x_i P x_j \Leftrightarrow \phi(x_i) > \phi(x_j)$

$x_i I x_j \Leftrightarrow \phi(x_i) = \phi(x_j)$.

2 ΚΑΤΑΓΡΑΦΗ ΥΦΙΣΤΑΜΕΝΗΣ ΚΑΤΑΣΤΑΣΗΣ

2.1 ΤΙ ΕΙΝΑΙ ΤΟ BITCOIN;

Το Bitcoin είναι ένα λεγόμενο εικονικό νόμισμα, που έχει επινοηθεί για ανώνυμες πληρωμές που πραγματοποιούνται εξ' ολοκλήρου ανεξάρτητα από κυβερνήσεις και τράπεζες. Τα τελευταία χρόνια, το Bitcoin έχει προκαλέσει μεγάλη προσοχή σε διάφορα μέτωπα. Οι Bitcoin πληρωμές βασίζεται σε μια νέα ενδιαφέρουσα τεχνική λύση και λειτουργούν διαφορετικά από τις παραδοσιακές πληρωμές. Σε ορισμένες περιπτώσεις πληρωμής, το Bitcoin μπορεί να φέρει οφέλη με τη μορφή της μείωσης του κόστους, της ταχύτητας, της ανωνυμίας, κλπ πέρα από τις παραδοσιακές μεθόδους πληρωμής. Ωστόσο, η χρήση μπορεί επίσης να είναι πιο επικίνδυνη επειδή το Bitcoin δεν καλύπτεται άμεσα από τους νόμους που διέπουν άλλες πληρωμές μεσολάβησης. Η ασθενής προστασία των καταναλωτών είναι επίσης ένας λόγος για τον οποίο μπορεί να είναι δύσκολο για το Bitcoin να γίνει γενικά αποδεκτό και βιώσιμο ως μέσο πληρωμής. Η χρήση του Bitcoin για τις πληρωμές είναι σε χαμηλά επίπεδα σήμερα, και παρόλο που το μέλλον του Bitcoin είναι αβέβαιο, είναι μια ενδιαφέρουσα καινοτομία (Goldman Sachs, 2014).

Πολλές περιοχές έχουν υποστεί ταχεία τεχνολογική πρόοδο τα τελευταία χρόνια. Οι ανάγκες μας όσον αφορά την πραγματοποίηση πληρωμών βρίσκονται επίσης στο στάδιο μετασχηματισμού. Για παράδειγμα, τα νοικοκυριά κάνουν online αγορές σε μεγάλη έκταση, καθώς και το ποσό των διασυνοριακών πληρωμών βρίσκεται σε άνοδο. Οι λύσεις πληρωμών, ιδίως για πρόσωπο-με-πρόσωπο πληρωμές, ωστόσο, δεν έχουν εξελιχθεί τόσο γρήγορα. Το Bitcoin μπορεί να θεωρηθεί ως απάντηση στην έλλειψη τέτοιων λύσεων πληρωμών και συχνά αποτέλεσε θέμα συζήτησης στα μέσα μαζικής ενημέρωσης, στους χώρους εργασίας και μεταξύ φίλων κατά τα τελευταία χρόνια. Διάφοροι παράγοντες έχουν προκάλεσε την περιέργεια για το πώς λειτουργεί το κρυπτο-νόμισμα, όπως η υποτιθέμενη ανωνυμία για τους χρήστες, το γεγονός ότι οι τράπεζες δεν εμπλέκονται στις πληρωμές και η ικανότητα να υλοποιούνται πληρωμές σε όλο τον κόσμο. Ταυτόχρονα, είναι δύσκολο να καταλάβουμε τι είναι πραγματικά το Bitcoin, και πώς λειτουργεί (Richardson et al., 2013).

2.2 Το ΕΙΚΟΝΙΚΟ ΝΟΜΙΣΜΑ

Το Bitcoin είναι γνωστό ως ένα εικονικό νόμισμα. Ένα εικονικό νόμισμα είναι ένα μέσο πληρωμής. Δηλαδή, οι μονάδες του εικονικού νομίσματος αντιπροσωπεύουν μια αξία. Προορίζεται για χρήση σε πληρωμές εντός ορισμένης εικονικής κοινότητας, όπως μια συγκεκριμένη ιστοσελίδα, ή σε ένα δίκτυο χρηστών με ειδικό λογισμικό για τη διαχείριση του εικονικού νομίσματος και την πραγματοποίηση πληρωμών. Αυτό το είδος της εικονικής κοινότητας μπορεί επομένως να πούμε ότι μοιάζει με μια εθελοντική συμφωνία για τη χρήση ενός συγκεκριμένου στοιχείου ως μέσο πληρωμής. Αυτή είναι μια σημαντική διαφορά με τα εθνικά νομίσματα. Τα εθνικά νομίσματα έχουν καθιερωθεί βάσει νόμου ότι αποτελούν τη νομισματική μονάδα της εκάστοτε χώρας. Το εικονικό νόμισμα έχει έτσι μια διαφορετική λογιστική μονάδα από ό, τι τα εθνικά νομίσματα. Για το Bitcoin, η λογιστική μονάδα είναι το ίδιο το Bitcoin. Ο εκδότης του εικονικού νομίσματος μπορεί να είναι μια μη χρηματοοικονομική εταιρεία ή ακόμα και ένας ιδιώτης, αλλά ο εν λόγω εκδότης δεν είναι υπό τον έλεγχο της κυβερνητικής αρχής. Η έκδοση του εικονικού νομίσματος, επομένως, δεν είναι μια κυβερνητικά ρυθμιζόμενη δραστηριότητα. Ωστόσο, κάθε εικονικό νόμισμα έχει κάποιο είδος κανόνων που διέπουν το πού και πώς μπορεί να χρησιμοποιηθεί, καθώς και κάποια μορφή τεχνικής υποδομής στην οποία διενεργούνται οι πληρωμές (Richardson et al., 2013).

Το εικονικό νόμισμα, το δικό του σύνολο κανόνων και η τεχνική υποδομή σε συνδυασμό σχηματίζουν ένα μικρό σύστημα πληρωμών, εφεξής καθεστώς εικονικού νομίσματος.

Υπάρχει ένας μεγάλος αριθμός καθεστώτων, που έχουν δημιουργηθεί, και λειτουργούν, με διαφορετικούς τρόπους. Μπορούν να κατανέμονται σε διάφορες κατηγορίες ανάλογα με το βαθμό στον οποίο είναι δυνατόν να αγοράζουν και να πωλούν το εικονικό νόμισμα. Εδώ, μπορούμε να τα διαχωρίσουμε σε συστήματα εικονικού νομίσματος που είναι κλειστά, με μονόδρομη ροή και αμφίδρομες ροές. Στα κλειστά συστήματα εικονικού νομίσματος, τα εικονικά νομίσματα δεν αγοράζονται ούτε πωλούνται, αλλά μόνο κερδίζονται και χρησιμοποιούνται σε ορισμένες ιστοσελίδες (όπως το World-of-Warcraft Gold). Αν το εικονικό νόμισμα μπορεί να αγοραστεί για εθνικό νόμισμα, αλλά δεν ανταλλάσσεται πίσω, το σύστημα έχει μια μονόδρομη ροή (όπως τα νομίσματα Amazon). Όταν το εικονικό

νόμισμα μπορεί τόσο να αγοράζεται όσο και να πωλείται και να χρησιμοποιείται έξω από μια συγκεκριμένη ιστοσελίδα, το καθεστώς έχει αμφίδρομες ροές. Όπως εξηγείται παρακάτω, το Bitcoin είναι ένα παράδειγμα ενός καθεστώτος με αμφίδρομες ροές. Ωστόσο, οι κατηγορίες αυτές μπορούν να επικαλύπτονται (Sharf, 2013).

Μια περαιτέρω διάκριση που μπορεί να γίνει είναι εάν το εικονικό νόμισμα είναι κεντρικό ή αποκεντρωμένο. Όπως και με τα χαρτονομίσματα και τα κέρματα, οι πληρωμές με μονάδες εικονικού νομίσματος γίνονται μέσω αλλαγής της ιδιοκτησίας τους. Ως εκ τούτου, η ιδιοκτησιακή δομή πρέπει να εγγραφεί κάπου, αλλιώς θα μπορούσε να είναι δελεαστικό για έναν κάτοχο εικονικού νομίσματος να το αντιγράψει και να το χρησιμοποιήσει πολλές φορές. Ένα κεντρικό καθεστώς εικονικού νομίσματος έχει ένα κεντρικό σύστημα για τον έλεγχο και την εκτέλεση των συναλλαγών, συχνά με τον εκδότη. Στην πράξη, ο τελευταίος διαχειρίζεται το σύνολο των λογαριασμών, μέσω των οποίων γίνονται οι πληρωμές. Σε ένα αποκεντρωμένο σύστημα, όπως το Bitcoin, οι συναλλαγές αντίθεντα επαληθεύονται και εκτελούνται μέσω του δικτύου των χρηστών που πραγματοποιούν κάποιο είδος δραστηριότητας για το σκοπό αυτό. Το δικαίωμα να εγγραφούν τα γεγονότα έτσι ανατίθενται στους συμμετέχοντες του δικτύου. Τα αποκεντρωμένα συστήματα μπορεί να βασίζονται στην ανταλλαγή κρυπτογραφημένων μηνυμάτων και ως εκ τούτου συνήθως ονομάζονται κρυπτονομίσματα. Η ανωνυμία και η ασφάλεια που παρέχονται από τα αποκεντρωμένα συστήματα κρυπτονομισμάτων είναι οι θεμελιώδεις έννοιες στις οποίες στηρίζεται το Bitcoin (Sharf, 2013).

2.3 Η ΛΕΙΤΟΥΡΓΙΑ ΤΟΥ BITCOIN

Το Bitcoin είναι ένα αποκεντρωμένο σύστημα εικονικού νομίσματος με αμφίδρομη ροή, και κρυπτονομίσματα. Επινοήθηκε ώστε να είναι ανεξάρτητο από τις κυβερνήσεις, τις τράπεζες και άλλα ιδρύματα. Σε γενικό επίπεδο, το Bitcoin λειτουργεί μάλλον σαν ένα είδος ηλεκτρονικών μετρητών.

Τα Bitcoins μπορούν να αγοραστούν σε ειδικές ιστοσελίδες, όπου ανταλλάσσονται με εθνικό νόμισμα. Η συναλλαγματική ισοτιμία για Bitcoin προσδιορίζεται από την αγορά ως συνάρτηση της προσφοράς και της ζήτησης. Οι Bitcoin πληρωμές μπορούν να γίνουν μεταξύ οποιωνδήποτε μερών με τον απαραίτητο λογισμικό για τον υπολογιστή, smartphone ή tablet. Το λογισμικό αυτό ονομάζεται πορτοφόλι. Ωστόσο, το Bitcoin δεν πρέπει να θεωρείται ως ένα είδος ψηφιακών μετρητών. Ο λόγος είναι ότι τα Bitcoins δεν είναι ψηφιακές μονάδες αποθηκευμένης αξίας π.χ. σε έναν υπολογιστή. Ένα Bitcoin ως εκ τούτου δεν είναι ένα ψηφιακό σημείωμα ή ένα νόμισμα και δεν θα πρέπει να συγκριθεί με την τακτική χαρτονομισμάτων και κερμάτων. Αντίθετα, το Bitcoin θα πρέπει να θεωρηθεί ως ένα είδος κεφαλαίων σε λογαριασμό. Όταν γίνει η πληρωμή, ο πληρωτής δεν αποστέλλει ψηφιακά χαρτονομίσματα και κέρματα στον παραλήπτη. Μάλλον, η πληρωμή γίνεται με τη χρέωση του λογαριασμού του αποστολέα και την πίστωση του λογαριασμού του δικαιούχου. Οι πληρωμές γίνονται μέσω της ανταλλαγής κρυπτογραφημένων μηνυμάτων και επαληθεύονται μέσα στο δίκτυο του χρήστη. Η διαδικασία αυτή περιγράφεται στη συνέχεια (Blundell-Wignall, 2014).

2.3.1 Η ασύμμετρη κρυπτογράφηση για ασφαλείς πληρωμές

Ας ξεκινήσουμε με την εξήγηση της έννοιας “ασύμμετρη κρυπτογράφηση” και πώς ο αποστολέας (άτομο Α) και ο δικαιούχος (άτομο Β) των κρυπτογραφημένων μηνυμάτων μπορούν να προσδιοριστούν με ασφάλεια. Η ασύμμετρη κρυπτογράφηση βασίζεται στο ότι τα άτομα Α και Β έχουν δύο κλειδιά κρυπτογράφησης το κάθε ένα. Τα κλειδιά κρυπτογράφησης είναι μοναδικά και κανείς δεν μπορεί να έχει τα ίδια κλειδιά με οποιονδήποτε άλλον. Ένα από τα κλειδιά είναι δημόσιο, με άλλα λόγια θα μπορούσε να γίνει δημοσίως γνωστό. Το άλλο είναι ιδιωτικό, ή μυστικό με άλλα λόγια. Όταν ο Α θέλει να στείλει ένα κρυπτογραφημένο μήνυμα στον Β, ο ίδιος χρησιμοποιεί το δημόσιο κλειδί του Β για να κρυπτογραφήσει το μήνυμα, το οποίο μπορεί στη συνέχεια να απο-κρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί του Β. Έτσι, ο Β είναι το μόνο πρόσωπο που μπορεί να διαβάσει το μήνυμα (Blundell-Wignall, 2014).

Η ασύμμετρη κρυπτογράφηση μπορεί επίσης να χρησιμοποιηθεί για υπογραφή. Αν ο Α χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει ένα μήνυμα, αυτό μπορεί να αποκρυπτογραφηθεί μόνο χρησιμοποιώντας το δημόσιο κλειδί του Α. Το πρόσωπο που αποκρυπτογραφεί το μήνυμα μπορεί τότε να είναι σίγουρο, ότι το μήνυμα απεστάλη από το Α - κανείς άλλος δεν έχει πρόσβαση στο ιδιωτικό κλειδί του Α (Blundell-Wignall, 2014).

Ας υποθέσουμε ότι ο Α οφείλει να καταβάλει 1 Bitcoin (BTC) στο Β. Οι Α και Β και οι δύο έχουν τα πορτοφόλια τους στους υπολογιστές τους, όπως και κάθε πορτοφόλι έχει ένα ιδιωτικό και ένα δημόσιο κλειδί κρυπτογράφησης. Ένα πορτοφόλι σχετίζεται με το δημόσιο κλειδί κρυπτογράφησης, το οποίο χρησιμεύει ως μια διεύθυνση ή έναν αριθμό λογαριασμού. Οι Α και Β επικοινωνούν μέσα από τα πορτοφόλια τους.

2.3.2 Η συναλλαγή επιβεβαιώνεται από το δίκτυο

Η συναλλαγή ξεκινά από την αποστολή του δημοσίου κλειδιού κρυπτογράφησης του Β (αριθμός λογαριασμού) στον Α. Ο Α, ή, ακριβέστερα, το πορτοφόλι Α, γράφει τώρα την εντολή πληρωμής για 1 BTC στο Β και το υπογράφει με το ιδιωτικό κλειδί του Α. Η διαταγή πληρωμής εκδίδεται στο δίκτυο των χρηστών Bitcoin. Θα μπορούσε κανείς να πει ότι η συναλλαγή μεταξύ των Α και Β προτείνεται στο δίκτυο, το οποίο πρέπει τώρα να επιβεβαιώσει / επαληθεύσει την συναλλαγή για να είναι έγκυρη. Η μέθοδος που χρησιμοποιείται για να στείλει το μήνυμα προς το δίκτυο βασίζεται σε τεχνολογία παρόμοια με αυτή του διαμοιρασμού αρχείων (BitTorrent), η οποία είναι κοινή για τη διάδοση / ανταλλαγή ταινιών, μουσικής, κ.λπ. σε απευθείας σύνδεση (Blundell-Wignall, 2014).

Η διαδικασία επαλήθευσης έχει ως εξής: Κάθε δεκάλεπτο, ένας ορισμένος τύπος των συμμετεχόντων στο δίκτυο Bitcoin συγκεντρώνει τις συναλλαγές που προτείνονται στο τελευταίο δεκάλεπτο. Αυτό συμβαίνει αυτόματα, και ο γύρος των

συναλλαγών που συγκεντρώνονται ονομάζεται «μπλοκ» και οι ειδικές συμμετέχοντες καλούνται "miners". Έχουν το καθήκον να ελέγχουν τη συναλλαγή με την προσθήκη του νέου μπλοκ (οι συναλλαγές) σε κάτι που είναι γνωστό ως blockchain ή αλυσίδα μπλοκ, ο οποίος είναι ο επίσημος κατάλογος ή μητρώο πιστοποιημένων συναλλαγών Bitcoin. Επειδή το blockchain περιέχει πληροφορίες σχετικά με τα πορτοφόλια που αποστέλλουν, τα πορτοφόλια που λαμβάνουν και τα ποσά, μπορεί να χρησιμοποιηθεί για να ελέγξει πόσες μονάδες BTC ανήκουν σε ένα συγκεκριμένο πορτοφόλι. Είναι η ίδια λειτουργία με τον υπολογισμό του υπολοίπου ενός τραπεζικού λογαριασμού αν κάποιος έχει πρόσβαση σε όλες τις εισερχόμενες και εξερχόμενες συναλλαγές του εν λόγω λογαριασμού. Ένα πορτοφόλι μπορεί συνεπώς να θεωρηθεί ως ένας λογαριασμός, για τον οποίο το δημόσιο κλειδί χρησιμεύει ως αριθμός λογαριασμού για το πορτοφόλι. Μια συναλλαγή Bitcoin δεν είναι εντελώς ανώνυμη. Επειδή προστίθεται στο blockchain, είναι ονομαστική και άμεσα διαθέσιμη στο διαδίκτυο. Επομένως, είναι αρκετά απλό να προσδιορίσει κανείς τα πορτοφόλια μεταξύ των οποίων έχει γίνει μια συναλλαγή. Ωστόσο, είναι πολύ δύσκολο να συνδεθούν πορτοφόλια σε μεμονωμένους χρήστες, πράγμα που σημαίνει ότι η συναλλαγή είναι στην πράξη ανώνυμη (Blundell-Wignall, 2014).

Οι πληρωμές ελέγχονται μέσω των miners, με την επίλυση ενός μαθηματικού προβλήματος για το οποίο η λύση είναι δύσκολο να υπολογιστεί, αλλά είναι εύκολο να επιβεβαιωθεί εφόσον υπολογιστεί. Για να κατανοήσουμε καλύτερα την επαλήθευση, η έννοια "συνάρτηση κατακερματισμού" πρέπει να εξηγηθεί. Μια συνάρτηση hash είναι μια συνάρτηση που μετατρέπει έναν αριθμό ή κείμενο με αυθαίρετο μήκος σε ένα αριθμό με δεδομένο μήκος. Για παράδειγμα, τα επιμέρους στοιχεία σε μια σειρά μπορεί να προστεθούν μαζί και όταν το άθροισμα υπερβαίνει ένα μονοψήφιο αριθμό, τα συστατικά του αθροίσματος προστίθενται μαζί, και ούτω καθεξής. Ο αριθμός 678910 είναι επομένως 6 + 7 + 8 + 9 + 1 + 0 = 31, και 31 είναι 3 + 1 = 4. Ως εκ τούτου, ο πολυ-ψήφιος αριθμός έχει μετατραπεί σε ένα μονοψήφιο αριθμό. Έστω ότι x χαρακτηρίζει το πρωτότυπο blockchain, y οι συναλλαγές που πρέπει να ελέγχονται και z ένας διαφορετικός αριθμός. Το μαθηματικό πρόβλημα που πρέπει να επιλυθεί μπορεί να διατυπωθεί ως f (x, y, z) ≤v όπου f είναι μία συνάρτηση κατακερματισμού και είναι μια περίπτωση της εύρεσης ενός αριθμού z

έτσι ώστε η συνάρτηση κατακερματισμού να λαμβάνει μια χαμηλότερη τιμή από ν όπου ν μπορεί σε αυτή την περίπτωση να ερμηνεύεται ως ο βαθμός δυσκολίας της συνάρτησης hash.

Οι miners ανταγωνίζονται μεταξύ τους για το ποιος μπορεί να βρει μια λύση ταχύτερα. Όταν ένας ανθρακωρύχος έχει βρει μια λύση, η προτεινόμενη λύση έχει αποσταλεί στο δίκτυο, στο οποίο οι άλλοι miners μπορούν απλά να εξακριβώσουν κατά πόσον ή όχι η λύση είναι σωστή. Η απόφαση να γίνει αποδεκτή μια λύση λαμβάνεται κατά πλειοψηφία, με την οποία η δύναμη της ψήφου ενός miner εξαρτάται από το βαθμό της ικανότητας υπολογισμού, ή την υπολογιστική ισχύ, που φέρνει στο δίκτυο. Όταν μια λύση υποστηρίζεται από τους miners που αντιπροσωπεύουν την πλειοψηφία της υπολογιστικής ισχύος του δικτύου, η λύση αυτή θεωρείται ότι γίνεται αποδεκτή. Οι προτεινόμενες συναλλαγές προστίθενται τώρα στο blockchain, η οποία καθίσταται κατά ένα μπλοκ μεγαλύτερη. Τώρα που η συναλλαγή μεταξύ των A και B έχει γίνει αποδεκτή, ο B είναι ο ιδιοκτήτης του μεταβιβαζόμενου 1 BTC με το οποίο πιστώθηκε το πορτοφόλι του. Ταυτόχρονα, 1 BTC έχει χρεωθεί στο πορτοφόλι του A (Blundell-Wignall, 2014).

2.3.3 Οι miners λαμβάνουν νέα Bitcoins για τη προσπάθεια τους

Το κίνητρο για τους miners να επενδύσουν υπολογιστική ισχύ στη διαδικασία επαλήθευσης είναι ότι, ως αποζημίωση, μπορούν να δημιουργήσουν νέα Bitcoins. Η διαδικασία έχει ως εξής: ο miner που επέλυσε το hash function πιο γρήγορα, με άλλα λόγια, που υπολόγισε πρώτος το z, ως ανταμοιβή προσθέτει μια επιπλέον «συναλλαγή» στο μπλοκ που θα επαληθευτεί (y). Η συναλλαγή αυτή πιστώνει το πορτοφόλι του miner με N ποσό BTC χωρίς να χρεώνεται το πορτοφόλι κάποιου άλλου. Με άλλα λόγια, N ποσό νέων Bitcoins δημιουργείται με ιδιοκτήτη τον miner που επέλυσε πρώτος τη συνάρτηση hash (FinCen, 2013).

Κάθε δεύτερη εβδομάδα, το σύνολο των κανόνων (το πρωτόκολλο) που διέπουν το Bitcoin ρυθμίζει το βαθμό δυσκολίας της συνάρτησης κατακερματισμού και το ποσό των Bitcoins (N) που δημιουργούνται σε κάθε έλεγχο. Η προσαρμογή γίνεται για να

εξασφαλισθεί ότι το δίκτυο μπορεί να ελέγξει τις συναλλαγές μία φορά κάθε δέκα λεπτά. Αν αυξάνεται η υπολογιστική ισχύ του δικτύου, το ίδιο θα συμβεί και στο βαθμό δυσκολίας, και το αντίστροφο. Το ποσό των Bitcoins που δημιουργούνται μειώνεται με την πάροδο του χρόνου, καθώς ο N μειώνεται κατά το ήμισυ μετά από 210.000 μονάδες, που ισοδυναμεί με περίπου 4 έτη. Το αρχικό ποσό ήταν N = 50 και τώρα είναι N = 25. Επειδή ο N ελαττώνεται με την πάροδο του χρόνου, υπάρχει ένα ανώτατο όριο 21 εκατομμύρια στον αριθμό των Bitcoins που μπορούν να υπάρχουν. Το όριο αυτό μπορεί να θεωρηθεί ως ένα μαθηματικό όριο που ποτέ δεν επιτυγχάνεται, ακόμη και αν το ποσό των BTC μπορεί να φθάσει αυθαίρετα κοντά. Στις 30 Ιουνίου 2014 υπήρχαν περίπου 13 εκατομμύρια BTC (FinCen, 2013).

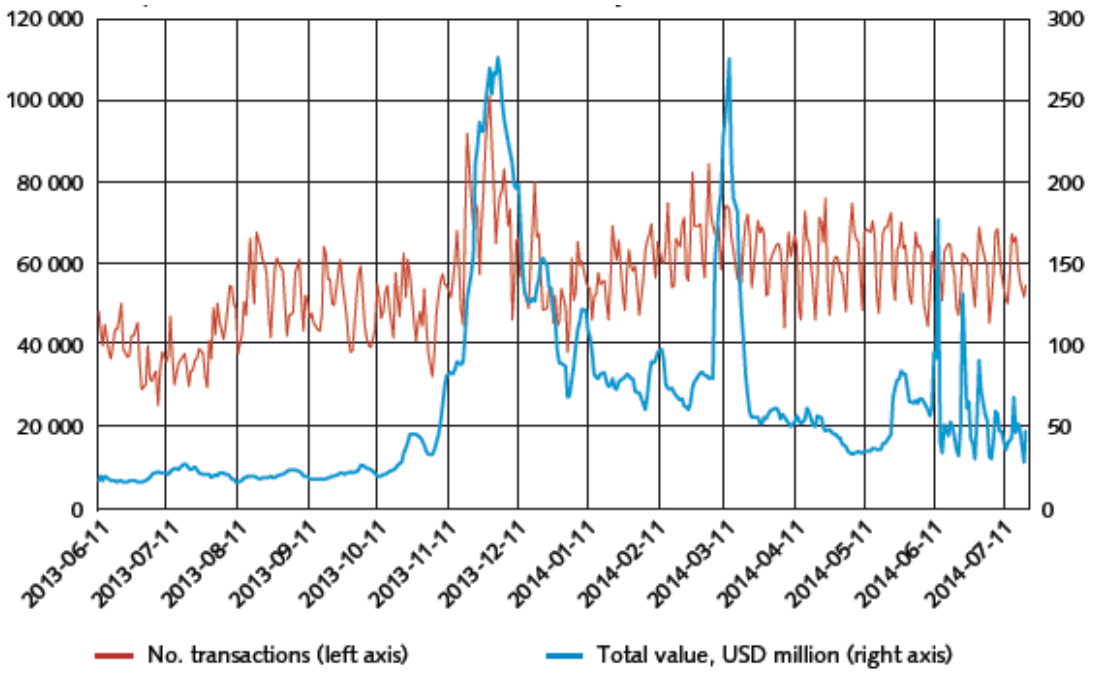
Εξαιτίας αυτού του τρόπου δημιουργίας νέων Bitcoins, σε αντίθεση με τα εθνικά νομίσματα που εκδίδονται από κεντρικές τράπεζες, δεν υπάρχει κάποιος κεντρικός εκδότης Bitcoin - η δημιουργία νέων Bitcoins διέπεται από το πρωτόκολλο Bitcoin. Ως εκ τούτου, το Bitcoin δεν αποτελεί χρηματική απαίτηση προς άλλο μέρος. Η αξία του Bitcoin επομένως, δεν στηρίζεται σε κανένα είδος απαίτησης ή υποκείμενης αξίας. Αντίθετα, η αγοραία αξία του εξαρτάται εξ ολοκλήρου από την προσδοκία ότι μπορεί να χρησιμοποιηθεί σε μελλοντικές συναλλαγές (FinCen, 2013).

Η πληρωμή Bitcoin δεν είναι μια πληρωμή σε πραγματικό χρόνο. Η πληρωμή μπορεί να διαρκέσει έως και δέκα λεπτά για πληρωμές που πρέπει να ελεγχθούν, και ο γενικός κανόνας είναι ότι πρέπει κανείς να περιμένει έξι γύρους επιβεβαίωσης για να βεβαιωθεί ότι η πληρωμή πράγματι προστίθεται στο blockchain. Η απόκτηση επιβεβαίωσης για μια πληρωμή Bitcoin μπορεί έτσι να διαρκέσει έως και μία ώρα περίπου. Ανάλογα με την κατάσταση, αυτό μπορεί να γίνει αντιληπτό ως ένα μεγάλο ή μικρό χρονικό διάστημα. Αξίζει επίσης να σημειωθεί ότι, λόγω της τεχνολογίας κοινής χρήσης αρχείων και τη διαδικασία επαλήθευσης, δεν υπάρχει κεντρική θέση αποθήκευσης για το blockchain. Κάθε συμμετέχων στο δίκτυο έχει πληροφορίες σχετικά με το σύνολο ή μέρος του blockchain.(FinCen, 2013)

2.4 Η ΕΚΤΑΣΗ ΤΗΣ ΧΡΗΣΗΣ ΤΟΥ BITCOIN

Υπάρχουν στατιστικά στοιχεία σχετικά με όλες τις συναλλαγές που γίνονται με τη χρήση Bitcoin από το 2009 και μετά. Αυτά τα στατιστικά στοιχεία προέρχονται από την blockchain και είναι διαθέσιμα σε όλους. Ορισμένες αναλύσεις είναι διαθέσιμες στο διαδίκτυο και παρέχουν μια επισκόπηση της παγκόσμιας χρήσης Bitcoin. Ωστόσο, δεν είναι δυνατόν να δούμε την έκταση της χρήσης σε μια συγκεκριμένη χώρα, επειδή δεν μπορούν συνήθως να εντοπιστούν οι κάτοχοι wallets μεταξύ των οποίων έγιναν συναλλαγές (Segendorf, 2014).

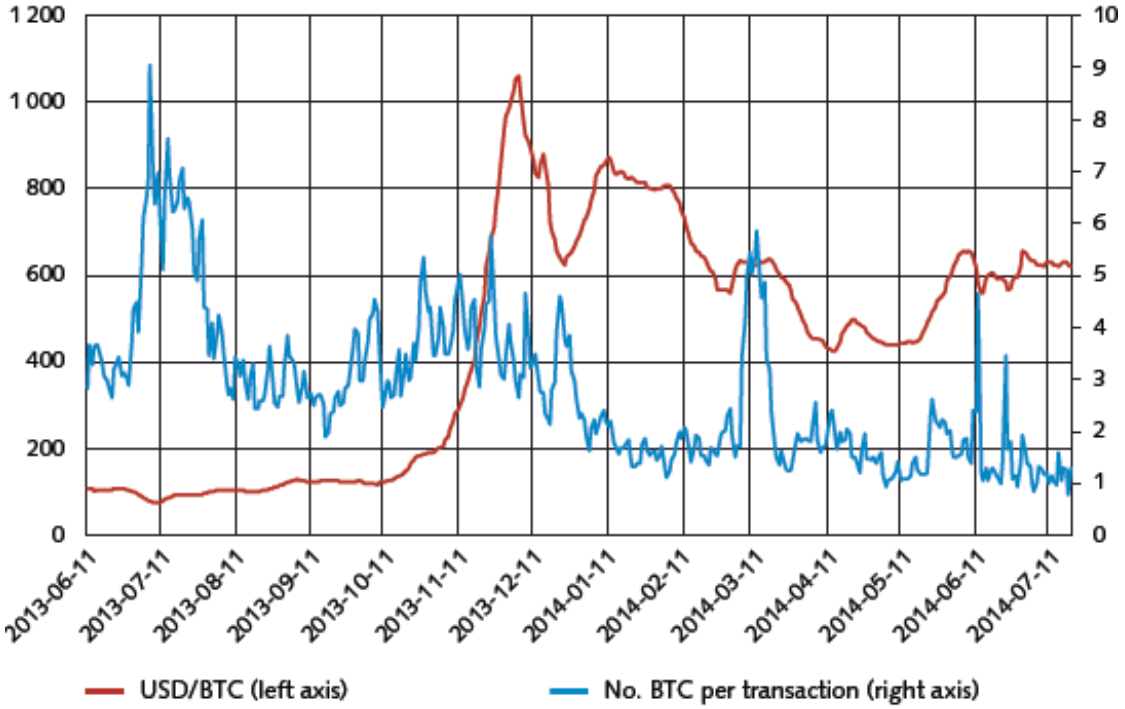
Κατά το 2013, γίνονταν σχεδόν 60.000 συναλλαγές Bitcoin ανά ημέρα. Στα χαμηλότερα επίπεδα, υπήρχαν 28.000 ανά ημέρα, και μόλις πάνω από 100.000 το στα υψηλότερα επίπεδα. Αυτό ισοδυναμεί με περίπου 0,1 τοις χιλίοις του αριθμού των πληρωμών με κάρτα. Η συνολική αξία, που μετράται σε εκατομμύρια USD, επίσης ποικίλει σημαντικά - εν μέρει λόγω μεγάλων διακυμάνσεων των συναλλαγματικών ισοτιμιών. Κατά μέσο όρο, η συνολική αξία ήταν κάτι περισσότερο από περίπου 64 εκατομμύρια δολάρια ανά ημέρα (Segendorf, 2014).



Εικόνα 2: Αριθμός των συναλλαγών Bitcoin και αξία συναλλαγών (εκατ. USD) ανά ημέρα. Η περίοδος εκτείνεται από 11 Ιουνίου, 2013 ως 21 Ιουλίου, 2014 (Πηγή: blockchain.info)

Η Εικόνα 2 δείχνει τον αριθμό των συναλλαγών ανά ημέρα και τη συνολική αξία των συναλλαγών. Η μέση αξία των συναλλαγών, που μετράται στο BTC, έχει μειωθεί κάπως με την πάροδο του χρόνου, πιθανώς επειδή η συναλλαγματική ισοτιμία ανατιμήθηκε απότομα το φθινόπωρο του 2013. Η Εικόνα 3 δείχνει τη συναλλαγματική ισοτιμία και τον αριθμό των Bitcoins ανά συναλλαγή. Η αύξηση της αξίας συναλλαγών το φθινόπωρο του 2013 συχνά εξηγείται από την αυξημένη ζήτηση για Bitcoin από την Κίνα (Segendorf, 2014).

Μόνο το 4% του συνόλου των Bitcoins διακινούνται εντός μιας εβδομάδας από τους κατόχους τους. Εάν το χρονικό διάστημα παρατείνεται σε τρεις μήνες, ένα επιπλέον 24% είναι διαπραγματεύσιμο. Μόνο μετά από έξι μήνες έχουν περισσότερες από τις μισές έχουν αντικείμενο διαπραγμάτευσης. Περίπου το 38% διατηρούνται για πάνω από ένα χρόνο. Οι κάτοχοι Bitcoin ως εκ τούτου, δεν φαίνεται να κάνουν συναλλαγές ιδιαίτερα συχνά. Θα πρέπει επίσης να αναφερθεί σε αυτό το πλαίσιο ότι πολλοί miners, ιδιαίτερα των μεγάλων φορέων ή εκείνων που συνεργάζονται σε ομάδες, συχνά ανταλλάσσουν τα Bitcoins που κερδίζουν σε εθνικό νόμισμα αμέσως για την κάλυψη των εξόδων τους. Το γεγονός ότι μόνο ένα μικρό ποσοστό του συνόλου των Bitcoins φαίνεται να χρησιμοποιείται για συναλλαγές, υποδηλώνει ότι οι περισσότεροι από αυτούς κρατούνται για πιο μακροπρόθεσμη χρήση, όπως η ανταλλαγή νομίσματος ή η αποταμίευση (Segendorf, 2014).



Εικόνα 3: Συναλλαγματική ισοτιμία USD / BTC και ο μέσος αριθμός των BTC ανά συναλλαγή. Η περίοδος εκτείνεται από 11 Ιουνίου, 2013 ως 21 Ιουλίου, 2014 (Πηγή: blockchain.info)

2.5 ΜΠΟΡΕΙ ΤΟ BITCOIN ΝΑ ΛΕΙΤΟΥΡΓΗΣΕΙ ΣΑΝ ΝΟΜΙΣΜΑ;

Ένα νόμισμα έχει τρεις λειτουργίες. Πρώτον, χρησιμεύει ως μέσο πληρωμής, με τη μορφή χαρτονομισμάτων και κερμάτων. Δεύτερον, χρησιμεύει ως λογιστική μονάδα που χρησιμοποιείται για να εκφράσει τις τιμές, την εξοικονόμηση, υποθήκες. Τρίτον, συμβάλλει στη διατήρηση της αξίας αποταμίευσης (Segendorf, 2014).

Θεωρητικά, μπορεί να ειπωθεί ότι το Bitcoin πληροί τους τρεις ρόλους ενός νομίσματος, αλλά στην πράξη αυτό δεν συμβαίνει. Ο ρόλος του ως μέσου πληρωμών προϋποθέτει ότι υπάρχει ευρεία αποδοχή για το νόμισμα στην κοινωνία, αλλιώς είναι δύσκολο να το χρησιμοποιήσει κανείς για να κάνει τις πληρωμές. Σε πολλές χώρες, δεν υπάρχει τέτοια ευρεία αποδοχή και οι δυνατότητες χρήσης Bitcoin ως μέσο πληρωμής, επομένως, είναι πολύ περιορισμένη στην πράξη. Ομοίως, είναι ασυνήθιστο οι τιμές να εκφράζονται σε Bitcoin, αν και αυτό συμβαίνει. Επομένως, δεν μπορεί να λεχθεί ότι το Bitcoin χρησιμεύει ως γενικώς

αποδεκτή λογιστική μονάδα. Τέλος, η υψηλή μεταβλητότητα της συναλλαγματικής ισοτιμίας Bitcoin το καθιστά ακατάλληλο για τη διατήρηση της αξίας, επειδή η αγοραστική δύναμη του μπορεί πολύ γρήγορα να μειωθεί και ένα μεγάλο μέρος της αξίας τότε χάνεται. Μια άλλη διαφορά μεταξύ του Bitcoin και των παραδοσιακών εθνικών νομισμάτων, είναι ότι τα τελευταία απολαμβάνουν ειδικό νομικό καθεστώς στη χώρα έκδοσής τους.

2.6 ΕΝΑΛΛΑΚΤΙΚΑ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ

Το Bitcoin είναι το πιο γνωστό κρυπτονόμισμα. Εισήχθηκε στις αρχές του 2009 και έχει κεφαλαιοποίηση περίπου 4,5 δις USD. Το Bitcoin είναι σαφώς πιο δημοφιλές από τα 300 ή άλλα κρυπτονομίσματα που υπάρχουν, πολλά από τα οποία βασίζονται στον open-source code του Bitcoin (CFA, 2015).

Τα άλλα κρυπτονομίσματα αναφέρονται συνολικά ως altcoins (εναλλακτικά κρυπτονομίσματα) και πολλά από αυτά είναι παράγωγα του πρωτοκόλλου Bitcoin. Παραλλαγές περιλαμβάνουν τη χρήση των διαφόρων λειτουργιών κατακερματισμού και των διαφορετικών χρόνων ενημέρωσης του blockchain, καθώς και εννοιολογικές διαφορές, όπως η απεριόριστη προσφορά χρήματος και οι εναλλακτικές λύσεις για το πρωτόκολλο απόδειξης της εργασίας (proof-of-work). Για να θέσουμε αυτά τα altcoins σε μια προοπτική, το δεύτερο μεγαλύτερο κρυπτονόμισμα, ονόματι Ripple, έχει χρηματιστηριακή αξία περίπου $ 140 εκατομμύρια και ακολουθείται από το Litecoin με κεφαλαιοποίηση περίπου $ 125 εκατομμύρια (CFA, 2015).

2.6.1 Κρυπτονόμισμα Ripple

Το Ripple είναι ένα σύστημα διακανονισμού σε πραγματικό χρόνο (RTGS), ανταλλακτήριο συναλλάγματος και δίκτυο εμβασμάτων που δημιουργήθηκε από τη Ripple Labs. Επίσης καλείται Πρωτόκολλο Συναλλαγών Ripple (RTXP) και είναι κτισμένο επάνω σε ένα κατανεμημένο open source πρωτόκολλο του Internet, καθολικής συναίνεσης και το μητρικό νόμισμα ονομάζεται XRP (Ripple).

Κυκλοφόρησε το 2012, και φιλοδοξεί να επιτρέψει τις ασφαλείς, άμεσες και σχεδόν δωρεάν παγκόσμιες χρηματοοικονομικές συναλλαγές οποιουδήποτε μεγέθους χωρίς χρέωση. Υποστηρίζει τις μάρκες που αντιπροσωπεύουν νόμισμα fiat, κρυπτονομίσματα, εμπόρευμα ή οποιαδήποτε άλλη μονάδα αξίας, όπως μίλια πτήσεων ή λεπτά κινητής τηλεφωνίας. Στον πυρήνα του, το ripple είναι βασισμένο γύρω από μια κοινή, δημόσια βάση δεδομένων, η οποία χρησιμοποιεί μια διαδικασία συναίνεσης που επιτρέπει τις πληρωμές, τις ανταλλαγές και το έμβασμα σε μια κατανεμημένη διαδικασία. Η ασφάλεια του αλγορίθμου συναίνεσης Ripple αμφισβητήθηκε από τους αντιπάλους το 2014. Από το 2014, το ripple είναι το δεύτερο μεγαλύτερο κρυπτονόμισμα με βάση την κεφαλαιοποίηση, μετά από Bitcoin.

Επί του παρόντος εφαρμόζεται από εταιρείες όπως η Τράπεζα Fidor, και το πρωτόκολλο υιοθετείται όλο και περισσότερο από τις τράπεζες και τα δίκτυα πληρωμών, ως η τεχνολογία των υποδομής, με την αμερικανική Banker να εξηγεί ότι «από την οπτική γωνία των τραπεζών, τα καθολικά συστήματα όπως το Ripple έχουν μια σειρά από πλεονεκτήματα σε σχέση με τα κρυπτονομίσματα όπως το Bitcoin, συμπεριλαμβανομένων της τιμής και της ασφάλειας.

Οι ιδρυτές του Ripple δημιούργησαν το αρχικό καθολικό σύστημα με 100 δισ XRP. Οι ιδρυτές έχουν μια κερδοσκοπική εταιρία που ονομάζεται Ripple Labs και κατέχε80 δισ XRP. Η Ripple Labs σκοπεύει να δώσει πάνω από 50 δισεκατομμύρια XRP. Το υπόλοιπο θα χρησιμοποιηθεί για τη χρηματοδότηση της Ripple Labs, για εργασίες που περιλαμβάνουν συμβολή κώδικα στο δίκτυο ανοικτού κώδικα και προώθηση του δικτύου.

Ακόμα και αν Ripple Labs κλείσει, το δίκτυο Ripple θα συνεχιστεί. Επειδή το Ripple είναι ένα δίκτυο P2P, δεν λειτουργεί από τη Ripple Labs, αλλά από τις συνδυασμένες προσπάθειες όλων των υπολογιστών που εκτελούν το λογισμικό διακομιστή Το δίκτυο Ripple δεν μπορεί να κλείσει χωρίς να κλείνει ολόκληρο το Internet.

2.6.2 Κρυπτονόμισμα Litecoin

Το Litecoin (LTC) μπορεί να θεωρηθεί το ασημένιο πρότυπο των κρυπτονομισμάτων, καθώς είναι το δεύτερο πιο δημοφιλές κρυπτονόμισμα τόσο στις συναλλαγές όσο και στην εξόρυξη. Το Litecoin κάνει χρήση του αλγορίθμου κρυπτογράφησης Scrypt, σε αντίθεση με τον αλγόριθμο SHA-256 που χρησιμοποιεί το Bitcoin. Ένας από τους στόχους του Litecoin είναι να επιβεβαιώσει τις συναλλαγές με μεγαλύτερη ταχύτητα από ότι το δίκτυο Bitcoin, καθώς και να κάνει χρήση ενός αλγόριθμου που είναι ανθεκτικός σε επιταχυνόμενες τεχνολογίες εξόρυξης υλικού, όπως η ASIC. Ο αλγόριθμος Scrypt είναι ανθεκτικός στην εξόρυξη ASIC λόγω των υψηλών απαιτήσεων σε μνήμη RAM. Το συνολικό ποσό των Litecoin που είναι διαθέσιμα για εξόρυξη και κυκλοφορία είναι τέσσερις φορές το ποσό του Bitcoin (Ahamad et al., 2013).

Το Litecoin έχει τρεις βασικές διαφορές από το Bitcoin (Ahamad et al., 2013):

- Το δίκτυο Litecoin στοχεύει να επεξεργαστεί ένα μπλοκ κάθε 2,5 λεπτά, αντί για τα 10 λεπτά του Bitcoin, και έτσι οι κατασκευαστές του ισχυρίζονται ότι επιτυγχάνεται ταχύτερη επιβεβαίωση της συναλλαγής. Ένα μειονέκτημα είναι η μεγαλύτερη πιθανότητα ορφανών μπλοκ. Τα πλεονεκτήματα μπορεί να περιλαμβάνουν μεγαλύτερη αντίσταση σε μια διπλή επίθεση δαπανών κατά την ίδια περίοδο, όπως Bitcoin. Ωστόσο, το συνολικό έργο είναι μια εκτίμηση. Για παράδειγμα, εάν το δίκτυο Litecoin έχει συγκριτικά δέκα φορές λιγότερη υπολογιστική εργασία ανά μπλοκ από το δίκτυο Bitcoin η επιβεβαίωση Bitcoin είναι περίπου δέκα φορές πιο δύσκολο να αντιστραφεί, ακόμα και αν το δίκτυο Litecoin είναι πιθανό να προσθέσει επιβεβαίωση μπλοκ με ένα ρυθμό τέσσερις φορές γρηγορότερα.
- Το Litecoin χρησιμοποιεί scrypt για την επιβεβαίωση της εργασίας του αλγορίθμου, μια συνάρτηση διαδοχικής μνήμης που απαιτεί ασυμπτωτικά περισσότερη μνήμη από έναν αλγόριθμο ο οποίος δεν είναι memory-hard.
- Το δίκτυο Litecoin μπορεί να παράγει ως 84 εκατομμύρια litecoins, ή τέσσερις φορές τις μονάδες νομίσματος που μπορούν να εκδοθούν από το δίκτυο Bitcoin.

Ο αρχικός προορισμός του scrypt ήταν να επιτραπεί η ταυτόχρονη εξόρυξη Bitcoin και Litecoin. Η επιλογή να χρησιμοποιηθεί scrypt ήταν επίσης εν μέρει για να αποφευχθεί το πλεονέκτημα της εξόρυξης μέσω κάρτας γραφικών (GPU), FPGA και ASIC έναντι της εξόρυξης CPU.

Λόγω της χρήσης του αλγορίθμου scrypt από το Litecoin, οι συσκευές FPGA και ASIC που έχουν κατασκευαστεί για την εξόρυξη Litecoin είναι πιο περίπλοκες και πιο ακριβές σε σύγκριση με το Bitcoin, το οποίο χρησιμοποιεί SHA-256.Ωστόσο, τον Μάρτιο του 2015, η εξόρυξη ASIC είναι ευρέως διαθέσιμη και αποτελεί την κύρια μέθοδο εξόρυξης Litecoin.

2.6.3 Κρυπτονόμισμα Dogecoin

Το Dogecoin έχει ως λογότυπο μια εικόνα του σκύλου Shiba Inu από το μιμίδιο "Doge" του Διαδικτύου. Εισήχθη στις 8 Δεκεμβρίου, 2013. Ξεκίνησε ως ένα “αστείο νόμισμα” στα τέλη του 2013, και ανέπτυξε γρήγορα τη δική του online κοινότητα. Έφτασε σε κεφαλαιοποίηση 60 εκατομμύρια δολάρια ΗΠΑ τον Ιανουάριο του 2014. Από το Σεπτέμβριο του 2015, είχε κεφαλαιοποίηση των 12,5 εκατομμυρίων δολαρίων ΗΠΑ.

Σε σύγκριση με τα άλλα κρυπτονομίσματα, το dogecoin έχει ένα γρήγορο αρχικό πρόγραμμα παραγωγής νομίσματος: 100 δισεκατομμύρια κέρματα έχουν κυκλοφορήσει μέχρι τα μέσα του 2015, με επιπλέον 5.256.000.000 κέρματα στη συνέχεια κάθε χρόνο. Στις 30 Ιουνίου 2015, εξορύχθηκε το εκατοστό δισεκατομμύριο dogecoin. Αν και υπάρχουν μερικές εμπορικές εφαρμογές, το νόμισμα έχει κερδίσει έδαφος ως ένα σύστημα ανατροπής του Διαδικτύου, στην οποία οι χρήστες των social media χορηγούν dogecoin συμβουλές σε άλλους χρήστες για την παροχή ενδιαφέροντος ή αξιοσημείωτου περιεχομένου. Πολλά μέλη της κοινότητας dogecoin, καθώς και τα μέλη των άλλων κοινοτήτων κρυπτονομισμάτων, χρησιμοποιούν τη φράση "To the moon!" για να περιγράψουν τη συνολική άποψη της αύξησης της αξίας του νομίσματος.

Όπως τα Bitcoin και Litecoin, το dogecoin λειτουργεί χρησιμοποιώντας κρυπτογραφία δημόσιου κλειδιού, στο οποίο κάποιος χρήστης δημιουργεί ένα ζεύγος κλειδιών κρυπτογράφησης: ένα δημόσιο και ένα ιδιωτικό. Μόνο το ιδιωτικό κλειδί μπορεί να αποκωδικοποιήσει πληροφορίες που κρυπτογραφεούνται με το δημόσιο κλειδί. Ως εκ τούτου, ο ιδιοκτήτης των κλειδιών μπορεί να διανείμει το δημόσιο κλειδί ανοιχτά, χωρίς φόβο ότι ο καθένας θα είναι σε θέση να το χρησιμοποιήσει για να αποκτήσει πρόσβαση στις κρυπτογραφημένες πληροφορίες. Όλες οι διευθύνσεις dogecoin είναι hashes του δημόσιου κλειδιού. Σε αντίθεση με τις Bitcoin διευθύνσεις, οι οποίες αποτελούνται από 27-33 χαρακτήρες, οι διευθύνσεις dogecoin αποτελούνται από μια σειρά από 34 αριθμούς και γράμματα (κεφαλαία ή μικρά), αρχίζοντας με το γράμμα D. Ένα δημόσιο κλειδί είναι η διεύθυνση dogecoin στην οποία άλλοι χρήστες μπορούν να στείλουν Dogecoins . Ένα ιδιωτικό κλειδί, ωστόσο, επιτρέπει την πλήρη πρόσβαση στο πορτοφόλι dogecoin και θα πρέπει να τηρείται απόρρητο και ασφαλές. Το Dogecoin κατέχει το ρεκόρ για τις περισσότερες συναλλαγές ανά ημέρα σε σχέση με κάθε κρυπτονόμισμα, και κορυφώθηκε σε 2,5 φορές περισσότερες πράξεις από όλα τα άλλα κρυτπονομίσματα τον Δεκέμβριο του 2013.

Η εφαρμογή εξόρυξης dogecoin διαφέρει από το Litecoin σε διάφορες παραμέτρους. Ο χρόνος μπλοκ του dogecoin είναι 1 λεπτό, σε αντίθεση με το Litecoin που είναι 2,5 λεπτά. Ο χρόνος επαναστόχευσης δυσκολίας είναι μία φορά ανά μπλοκ και η ανταμοιβή είναι σταθερή με βάση ένα προκαθορισμένο πρόγραμμα μπλοκ. Ωστόσο, όταν εισήχθη για πρώτη φορά το dogecoin, η εκ νέου στοχοθέτηση δυσκολίας ήταν μία φορά κάθε τέσσερις ώρες, και η ανταμοιβή ήταν ένας τυχαίος αριθμός μεταξύ 0 και κατ 'ανώτατο όριο που ορίζεται από το χρονοδιάγραμμα μπλοκ. Σύμφωνα με το σύστημα στο οποίο διανεμήθηκε ένας τυχαίος αριθμός νομισμάτων, τα οφέλη υπολογίστηκαν με τη χρήση ψευδο-γεννήτριας τυχαίων αριθμών Mersenne Twister. Ενώ η αρχική εφαρμογή του dogecoin προορίζεται για να υπάρξει ένας σταθερός αριθμός κερμάτων ανά μπλοκ από το μπλοκ 600.001 και μετά μόνο (παροχή 10.000 νομίσματα ανά μπλοκ), οι αλγόριθμοι dogecoin άλλαξαν ξεκινώντας από το μπλοκ 145000 έτσι ώστε μια να

δίνεται μια σταθερή αμοιβή πάντα (παροχή 250.000 κέρματα ανά κατηγορία μέχρι το μπλοκ 200.001).

Στις 12 Μάρτη του 2014, ανακοινώθηκε η έκδοση dogecoin 1.6. Στη νέα έκδοση επιτρέπεται να υπάρχει μια σταθερή αμοιβή ανά μπλοκ, και εισήχθηκε ένας νέος αλγόριθμος δυσκολίας που ονομάζεται DigiShield. Ο κύριος στόχος του νέου αλγορίθμου δυσκολίας, ο οποίος εγκρίθηκε από το altcoin Digibyte, ήταν να εμποδίσει την εξόρυξη και τη κερδοφορία από τα multipools, τα οποία μειώνουν την τιμή του νομίσματος δραστικά, και αναγκάζουν τους single-coin miners να έρθουν αντιμέτωποι με την αύξηση της δυσκολίας που τα multipools επιφέρουν. Χάρη στη σχεδόν άμεση αλλαγή του αλγορίθμου, οποιαδήποτε multipool εισέρχονται στο δίκτυο dogecoin θα φύγει αμέσως, καθώς η δυσκολία εξόρυξης θα ανέβει σημαντικά, προκαλώντας πτώση της αποδοτικότητας και, εν τέλει, την απουσία multipools.

Σε αντίθεση με τα άλλα κρυπτονομίσματα (όπως το Bitcoin), δεν υπάρχει όριο στο πόσα Dogecoins μπορούν να παραχθούν.

2.7 ΠΕΡΑ ΑΠΟ ΤΟΝ BITCOIN: CRYPTO 2.0

Οι προγραμματιστές του Bitcoin επικρίνονται συχνά ότι είναι αργοί και συντηρητικοί, το οποίο είναι αναμενόμενο δεδομένου ότι το οικοσύστημα Bitcoin είναι πλέον πολύ μεγάλο και πολύ σημαντικό για πειράματα. Ως εκ τούτου, η ανάπτυξη κρυπτο-νομισμάτων συμβαίνει εκτός Bitcoin. Αυτό δημιουργεί ένα άλλο ζήτημα για τις ρυθμιστικές αρχές, το γεγονός ότι η κρυπτο-καθολική πλατφόρμα εξελίσσεται ταχύτατα στις τεχνολογίες δεύτερης γενιάς ή "Crypto 2.0" στις οποίες το πρωτόκολλο Bitcoin εφαρμόζεται σε άλλες εφαρμογές εκτός από τα κρυπτο-νομίσματα. Οι όροι που χρησιμοποιούνται συνήθως για αυτές τις εφαρμογές είναι "έξυπνες συμβάσεις» ή “έξυπνη ιδιοκτησία”. Μια ομάδα προγραμματιστών που είναι γνωστή ως Ethereum καλεί τις τεχνολογίες αυτές τα “δομικά στοιχεία LEGO της κρυπτο-χρηματοδότησης”. Το λογισμικό τους θα επιτρέψει στους χρήστες εύκολα και φθηνά να δημιουργήσουν τα δικά τους κρυπτο-καθολικά περιουσιακά στοιχεία.

Στην πραγματικότητα, κάθε εφαρμογή που αφορά τα δικαιώματα ιδιοκτησίας θα μπορούσε να διαπραγματεύεται με τη χρήση της κρυπτο-καθολικής αρχής του Bitcoin (εξ ου και “έξυπνες συμβάσεις”).

Μέχρι σήμερα, η μεγαλύτερη πρόοδος έχει σημειωθεί στον τομέα των αποκεντρωμένων ανταλλαγών κρυπτονομισμάτων. Το κίνητρο για τη δημιουργία των "trustless" αποκεντρωμένων ανταλλαγών ήταν σε μεγάλο βαθμό η αποφυγή της επανάληψης της κρίσης Mt.Gox. Ένα εξέχον παράδειγμα αυτής της δυνατότητας δεύτερης γενιάς είναι το NXT, το οποίο είναι ένα οικοσύστημα κρυπτο-νομίσματος που έχει αποκεντρωμένη ανταλλαγή. Αυξάνεται με ταχείς ρυθμούς και πρόσφατα έγινε το έκτο μεγαλύτερο κρυπτο-νόμισμα σε κυκλοφορία με κεφαλαιοποίηση περί τα $24 εκατομμύρια. Η λειτουργικότητα ανταλλαγής του NXT είναι ανοιχτή σε οποιονδήποτε τύπο κρυπτο-νομίσματος, συμπεριλαμβανομένων των bitcoins.

Με την απομάκρυνση από την νομισματική πλευρά του Bitcoin, αναπτύσσονται χρωματισμένα κέρματα, τα οποία είναι ψηφιακά νομίσματα που εκδίδονται για να αντιπροσωπεύουν ένα συγκεκριμένο περιουσιακό στοιχείο, όπως η ακίνητη περιουσία, η τέχνη, τα εμπορεύματα, οι μετοχές, τα ομόλογα ή τα παράγωγα. Τα κέρματα αυτά μπορούν στη συνέχεια να ανταλλαγούν χρησιμοποιώντας το πρωτόκολλο Bitcoin. Για παράδειγμα, ένας διαχειριστής χαρτοφυλακίου θα μπορούσε να εκδώσει χρωματιστά κέρματα για να αντιπροσωπεύουν την ιδιοκτησία ενός τμήματος ενός χαρτοφυλακίου μετοχών, το οποίο μπορεί στη συνέχεια να ανταλλαγεί σε μια αποκεντρωμένη ανταλλαγή. Τα κέρματα αυτά θα πρέπει να υποστηρίζονται από μια πραγματική θέση στο ίδιο χαρτοφυλάκιο μετοχών.

Ένα άλλο παράδειγμα της δύναμης αυτής της τεχνολογίας δίνεται από το Blackcoin, έναν ανταγωνιστή του NXT. Το Blackcoin ξεκίνησε εστιάζοντας στις έξυπνες συμβάσεις που θα μπορούσαν να χρησιμοποιηθούν για να ασχοληθούν με τα αγαθά και τις υπηρεσίες σε ένα κατανεμημένο-καθολικό πλαίσιο. Στο Blackcoin, δύο μέρη μπορούν να συνάψουν μια σύμβαση όπου ο αγοραστής καταθέτει τα χρήματα σε λογαριασμό μεσεγγύησης, προκειμένου να ελευθερωθούν όταν και τα δύο μέρη συμφωνούν ότι η σύμβαση έχει εκπληρωθεί. Για την αποφυγή της απάτης, και οι δύο πλευρές απαιτείται να δημοσιεύσουν μια κατάθεση που χάνεται από τις δύο

πλευρές, εάν κάθε πλευρά θεωρεί ότι η σύμβαση είναι ανεκπλήρωτη. Αυτό έχει σχεδιαστεί για να κάνει τις απάτες συμβάσεων ασύμφορες.

Τόσο το NXT όσο και το Blackcoin συγκλίνουν στα χαρακτηριστικά τους, με όλα τα πρωτόκολλα δεύτερης γενιάς που έχουν ως ευρύτερο στόχο τη δημιουργία μιας αποκεντρωμένης αγοράς για τα νομίσματα, τα περιουσιακά στοιχεία, τα αγαθα, τις υπηρεσίες και τις συμβάσεις. Με τη σειρά τους, αυτά τα χαρακτηριστικά δημιουργούν μια νέα γενιά Αποκεντρωμένων Αυτόνομων Επιχειρήσεων (DACs). Ρύθμιση των εν λόγω επιχειρήσεων είναι πιθανό να θέσει σημαντικές προκλήσεις για τις ρυθμιστικές αρχές καθώς δεν μπορεί να υπάρχει ένας προφανής ιδιοκτήτης που θα μπορούσε να αναλάβει τη νομική ευθύνη. Για παράδειγμα, εάν μια εταιρεία αυξάνει τη χρηματοδότηση με την έκδοση κρυπτο-ιδίων κεφαλαίων, μπορεί να είναι αδύνατο να επιβάλλει όρια ξένης ιδιοκτησίας.

Τα πρωτόκολλα και οι ανταλλαγές δεύτερης γενιάς τείνουν να είναι ανοιχτά σε κάθε κρυπτο-νόμισμα, ώστε να μην προαναγγέλλουν το τέλος του Bitcoin, και να μπορούν να διαπραγματεύονται με επιτυχία και να χρησιμοποιούνται στα περισσότερα οικοσυστήματα λόγω της δεσπόζουσας θέσης τους στην αγορά. Οι προγραμματιστές του Bitcoin λένε ότι θα περιμένουν να δουν τη λειτουργικότητα της δεύτερης γενιάς και, στη συνέχεια, απλά θα τη προσθέσουν στο πρωτόκολλο Bitcoin.

Είναι πιθανό ότι το πρωτόκολλο Bitcoin θα μπορούσε τελικά να οδηγήσει στην πλήρη αποκέντρωση και την αποδιαμεσολάβηση των δικαιωμάτων παγκόσμιας ιδιοκτησίας. Αυτό είναι σίγουρα το χαρακτηριστικό που οι πιο ιδεαλιστικοί υπέρμαχοι της τεχνολογίας βλέπουν στο μέλλον. Μια αναλογία που συχνά δίνουν είναι ο αντίκτυπος που είχε η κοινή χρήση αρχείων στην μουσική βιομηχανία στα τέλη της δεκαετίας του 1990 και στις αρχές της δεκαετίας του 2000. Ωστόσο, όπως συνέβη και με τη μουσική βιομηχανία, είναι απίθανο ότι η νέα τεχνολογία θα ανταποκρίνεται στους υψηλούς κοινωνικο-πολιτικούς στόχους των υποστηρικτών της. Είναι πιο πιθανό ότι το Bitcoin θα αναγκάσει τους κατεστημένους φορείς στον χρηματοπιστωτικό τομέα, συμπεριλαμβανομένων των ρυθμιστικών αρχών, να προσαρμόσυν τον τρόπο που κάνουν τις επιχειρήσεις.

3 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ

3.1 Η ΣΧΕΣΗ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ ΜΕ ΤΟ ΧΡΗΜΑ

Από νομική άποψη, τίθεται το ερώτημα τι είναι τα κρυπτονομίσματα, και αν / πώς θα πρέπει να ρυθμιστεί το σύστημα. Τα κρυπτονομίσματα ορίζονται ως ένα ψηφιακό νόμισμα. Ωστόσο, ο όρος αυτός ισχύει μόνο στην καθομιλουμένη χρήση τους. Η χρήση του όρου «νόμισμα» από οικονομολόγους (και, κατά συνέπεια, στη νομολογία) περιορίζεται στα εγκεκριμένα από το κράτος χρήματα. Μερικοί συγγραφείς ορίζουν το νόμισμα ώστε να περιλαμβάνει μόνο χαρτονομίσματα και κέρματα (Mishkin, 2004) (Campbell & Campbell, 1988). Μετά από αυτόν τον ορισμό, ο όρος ψηφιακό νόμισμα δεν έχει νόημα.

3.1.1 Ηλεκτρονικά χρήματα και χρήματα

Στα κράτη-μέλη της Ευρωπαϊκής Ένωσης, η οδηγία 2009/110 / ΕΚ του Συμβουλίου του Ευρωπαϊκού Κοινοβουλίου ορίζει την έννοια του «ηλεκτρονικού χρήματος», η οποία, με την πρώτη ματιά, φαίνεται να χαρακτηρίζει τα κρυπτονομίσματα πιο σωστά.

Σύμφωνα με το άρθρο 2 της οδηγίας, ως ηλεκτρονικό χρήμα νοείται το ηλεκτρονικό, μεταξύ άλλων και μαγνητικό υπόθεμα της νομισματικής αξίας αντιπροσωπευόμενο από απαίτηση έναντι του εκδότη, η οποία έχει εκδοθεί κατόπιν παραλαβής χρηματικού ποσού για τον σκοπό της πραγματοποίησης πράξεων πληρωμών [...], και η οποία είναι αποδεκτή από ένα φυσικό ή νομικό πρόσωπο διαφορετικό από τον εκδότη ηλεκτρονικού χρήματος.

Για την εκπλήρωση αυτού του ορισμού, το σύστημα κρυπτονομισμάτων θα πρέπει να χρησιμοποιεί μια ηλεκτρονική αποθήκευση της νομισματικής αξίας. Στην πραγματικότητα, ένας πελάτης κρυπτονομισμάτων αποθηκεύει ζεύγη κλειδιών που αντιπροσωπεύουν λογαριασμούς. Τα υπόλοιπα των λογαριασμών δεν

ανταποκρίνονται σε μια σταθερή τιμή σε κάθε εξωτερικό νόμισμα, αλλά έχουν νόημα μόνο στο πλαίσιο του συστήματος. Ωστόσο, αυτό δεν αποκλείει την αναπαράσταση μιας χρηματικής αξίας. Τα ζεύγη κλειδιών δεν αντιπροσωπεύουν ηλεκτρονικά νομίσματα, δεδομένου ότι η αξία που συνδέεται με ένα ζεύγος κλειδιών καθορίζεται μόνο από την παρακολούθηση των προηγούμενων συναλλαγών και από την άποψη αυτή, το κρυπτονόμισμα είναι συγκρίσιμο με το λογιστικό χρήμα. Θεωρούμε ακόμα ότι το κρυπτονόμισμα χρησιμοποιεί ηλεκτρονικά αποθηκευμένη νομισματική αξία: η αξία του λογαριασμού ενός χρήστη μπορεί εύκολα να υπολογιστεί χρησιμοποιώντας την αποθηκευμένη πληροφορία, και από την πλευρά του χρήστη, δεν υπάρχει μεγάλη διαφορά από τη χρήση άλλων συστημάτων ηλεκτρονικής πληρωμής.

Για να χαρακτηριστεί ως ηλεκτρονικό χρήμα, ωστόσο, θα πρέπει να υπάρχει απαίτηση έναντι του εκδότη. Ο Ευρωπαίος νομοθέτης προφανώς σκεπτόταν συστήματα πληρωμών που λειτουργούν από έναν εκδότη. Ενώ το κρυπτονόμισμα είναι ένα αποκεντρωμένο σύστημα, υπάρχουν οντότητες που θα μπορούσαν να θεωρηθούν ως εκδότες: Οι miners λαμβάνουν μια ανταμοιβή μπλοκ, αφού ολοκληρώσουν την απόδειξη της εργασίας, και με αυτό, θα δημιουργήσουν νέα κρυπτονομίσματα.

Κατά συνέπεια, τα κρυπτονομίσματα δεν πληρούν τον ορισμό του ηλεκτρονικού χρήματος στην Ευρωπαϊκή Ένωση.

Στη συνέχεια, θα συζητήσουμε ποιες ιδιότητες του χρήματος είναι κοινές για το κρυπτονόμισμα. Δεν υπάρχει γενικά αποδεκτός ορισμός του όρου (Proctor, 2005). Η χρήση του διαφέρει μεταξύ των διαφόρων τομέων του δικαίου (π.χ. μεταξύ των ποινικών διατάξεων που αφορούν τα πλαστά χρήματα, και τους τραπεζικούς κανονισμούς).

Πολλοί από αυτούς τους ορισμούς, για παράδειγμα στο ποινικό δίκαιο, απαιτούν τα χρήματα να εκδίδονται από το κράτος ή από εξουσιοδοτημένο πρακτορείο. Αυτό προφανώς δεν είναι η περίπτωση του κρυπτονομίσματος. Οι οικονομικοί ορισμοί των χρημάτων απαιτούν την ευρεία αποδοχή τους. Για παράδειγμα, ο (Mishkin, 2004) ορίζει τα χρήματα ως “κάτι που είναι γενικά αποδεκτό στην πληρωμή αγαθών

ή υπηρεσιών ή για την αποπληρωμή των χρεών" (Proctor, 2005). Το κρυπτονόμισμα δεν είναι "γενικά αποδεκτό" και η έλλειψη ευρείας αποδοχής υπήρξε επίσης ένας λόγος ώστε η Αρχή του Ηνωμένου Βασιλείου για τις χρηματοπιστωτικές υπηρεσίες και η σουηδική Finansinspektionen να ταξινομήσουν το κρυπτονόμισμα ως μη χρήμα.

Ακόμα κι αν το κρυπτονόμισμα δεν χαρακτηρίζεται ως χρήμα, σύμφωνα με τους περισσότερους ορισμούς, θα ρίξουμε μια ματιά στις λειτουργίες του χρήματος από οικονομική άποψη (Mishkin, 2004), τις οποίες συμμερίζεται επίσης η Ευρωπαϊκή Κεντρική Τράπεζα (Ευρωπαϊκή Κεντρική Τράπεζα, 2012) και η γερμανική Bundesbank (Bundesbank, 2013):

- Τα χρήματα μπορούν να χρησιμοποιηθούν ως μέσο αποθήκευσης αξίας. Κεκτημένα κρυπτονομίσματα δεν πρέπει να δαπανηθούν αμέσως, κατ 'αρχήν, τα βασικά ζεύγη μπορούν να αποθηκευτούν για χρόνια πριν από την ανάκτηση της αξίας τους. Η αξία των κρυπτονομισμάτων αλλάζει με το χρόνο. Το ίδιο ισχύει και για τα συμβατικά νομίσματα (αν και διακυμάνσεις είναι συνήθως λιγότερο ακραίες στην περίπτωση αυτή). Με τη φραγή του υπερπληθωρισμού, οι διακυμάνσεις της αξίας δεν εμποδίζουν την εκπλήρωση της αποθήκευσης της λειτουργίας αξία.
- Τα χρήματα χρησιμεύουν ως μέσο συναλλαγής. Προϊόντα ή υπηρεσίες μπορούν να ανταλλαγούν με τα κρυπτονομίσματα, αντί της άμεσης ανταλλαγής εμπορευμάτων.
- Τέλος, το χρήμα λειτουργεί ως λογιστική μονάδα.

3.1.2 Μέσο συναλλαγής

Η λειτουργία του χρήματος ως "μέσο συναλλαγής" περιγράφει τη χρήση του στο εμπόριο για να αποφεύγεται η χρήση του συστήματος άμεσης ανταλλαγής.

Ο (Proctor, 2005) αναφέρει την περιγραφή από την περίπτωση της Μος κατά Χάνκοκ ως ίσως ο πιο γνωστός δικαστικός ορισμός του χρήματος ως μέσο ανταλλαγής: Τα

χρήματα είναι αυτά που περνούν ελεύθερα από χέρι σε χέρι στην κοινότητα για την τελική απόρριψη των χρεών και την πλήρη εξόφληση των εμπορευμάτων, που γίνονται ισότιμα αποδεκτά χωρίς αναφορά στον χαρακτήρα ή την πιστωτική ικανότητα του προσώπου που τα προσφέρει, χωρίς την πρόθεση του προσώπου που τα δέχεται να το καταναλώσει ή να τα εφαρμόσει σε οποιαδήποτε άλλη χρήση, εκτός από να τα προσφέρει σε άλλους για την απαλλαγή από χρέη ή την πληρωμή των εμπορευμάτων.

Η απαλλαγή από το χρέος είναι σίγουρα εφικτή με τα κρυπτονομίσματα, καθώς ο πιστωτής είναι ελεύθερος να δεχθεί Bitcoin - αν και δεν υπάρχει καμία υποχρέωση να το πράξει. Το κρίσιμο ερώτημα είναι αν το Bitcoin πράγματι χρησιμοποιείται για το σκοπό αυτό, δηλαδή την πληρωμή των εμπορευμάτων - ακόμη και αν δεν είναι νόμιμο χρήμα. Δεδομένου ότι υπάρχουν έμποροι που δέχονται Bitcoin, και το σύστημα Bitcoin έχει σχεδιαστεί για το σκοπό αυτό, καταλήγουμε στο συμπέρασμα ότι το Bitcoin μπορεί να εκπληρώσει το τη λειτουργία του μέσου ανταλλαγής. Την άποψη αυτή συμμερίζεται και η σουηδική Finansinspektion, η οποία θεωρεί τα Bitcoin ως (ρυθμιζόμενα) μέσα πληρωμής από τα τέλη του 2012, και η Ευρωπαϊκή Κεντρική Τράπεζα.

Ωστόσο, η πραγματική χρήση του Bitcoin ως μέσο συναλλαγής είναι πολύ περιορισμένη από τα μέσα του 2013. Αυτή η έλλειψη πραγματικής χρήσης είναι ο λόγος που η βρετανική Αρχή Χρηματοπιστωτικών Υπηρεσιών δεν εξέτασε το Bitcoin ως χρήμα.

3.1.3 Λογιστική μονάδα

Δεν υπάρχει νομικός ορισμός του όρου «λογιστική μονάδα», αλλά η λειτουργία της λογιστικής μονάδας είναι σαφής στην οικονομική βιβλιογραφία (Mishkin, 2004): Οι τιμές των αγαθών και των υπηρεσιών που μπορεί να εκφραστούν ή με άλλα λόγια, η αξία τους μπορεί να μετρηθεί χρησιμοποιώντας τη λογιστική μονάδα. Η έκφραση τιμών χρησιμοποιώντας τη μονάδα "Bitcoin" είναι πολύ ασυνήθιστη. Ακόμα και οι online λιανοπωλητές αποδεχθούν το Bitcoin, οι τιμές συνήθως αναφέρονται σε

Δολάρια ΗΠΑ, και η συναλλαγματική ισοτιμία εφαρμόζεται όταν γίνεται η πραγματική πληρωμή. Κατ 'αρχήν, το Bitcoin θα μπορούσε να χρησιμοποιηθεί ως μια λογιστική μονάδα: αυτό ισχύει για κάθε αγαθό. Το αγαθό δεν χρειάζεται καν να είναι διαθέσιμο ή διαχειρίσιμο, εφ 'όσον μπορεί να προσδιοριστεί η σχέση της αξίας του με την αξία των άλλων αγαθών. Προσπαθώντας να βρεθεί μια σωστή οριοθέτηση του όρου «λογιστική μονάδα», θεωρούμε το παράδειγμα της ΕΤΔ, που ορίζεται από το Διεθνές Νομισματικό Ταμείο με βάση την αξία πολλών νομισμάτων. Έχουν ομόφωνα θεωρηθεί ως λογιστική μονάδα. Η μόνη διαφορά μεταξύ ΕΤΔ και των αυθαίρετων αγαθών, όπως ένα κιλό σιτάρι, είναι η προβλεπόμενη και η πραγματική χρήση: το ΕΤΔ έχει ως ειδικό σκοπό να χρησιμοποιηθεί ως λογιστική μονάδα, δηλαδή να εκφράσει την αξία ορισμένων άλλων αγαθών. Ενώ τα ΕΤΔ παίζουν ρόλο μόνο σε ένα πολύ στενό τομέα, χρησιμοποιούνται στην πραγματικότητα για το σκοπό αυτό. Η κατάσταση είναι παρόμοια και για το Bitcoin. Ενώ το αρχικό άρθρο Bitcoin από το Nakamoto επικεντρώνεται στις τεχνικές πτυχές του ηλεκτρονικού συστήματος πληρωμών, το γεγονός ότι το Bitcoin αποτελεί μια λογιστική μονάδα είναι εγγενές στο σχεδιασμό του. Επιπλέον, η κερδοσκοπία με Bitcoin (εκμεταλλευόμενη την μεταβολή των συναλλαγματικών ισοτιμιών με νομίσματα όπως το δολάριο ή το ευρώ) στην πραγματικότητα λαμβάνει χώρα και εκμεταλλεύεται το γεγονός ότι το Bitcoin είναι μια ανεξάρτητη λογιστική μονάδα. Καταλήγουμε στο συμπέρασμα ότι το Bitcoin πληροί αυτή τη λειτουργία.

Για να συνοψίσουμε, το Bitcoin δεν αποτελεί ηλεκτρονικό χρήμα κατά την έννοια της οδηγίας 2009/110/ΕΚ του Συμβουλίου του Ευρωπαϊκού Κοινοβουλίου. Θεωρούμε ότι Bitcoin έχει τη δυνατότητα να εκπληρώσει όλους τους καθορισμένους ρόλους των χρημάτων στη θεωρία, αλλά δεν έχει την ευρεία αποδοχή των πραγματικών χρημάτων.

3.2 ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΟΥ

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, παρουσιάζει ένα μοναδικό πρόβλημα με μια λύση που δεν είναι προφανής. Πρώτον, 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, έτσι ώστε η ημερομηνία της συναλλαγής να καταγράφεται. Ο νέος αυτός κώδικας αντιπροσωπεύει το κέρμα και τη διαδρομή του μέσω του δικτύου. Αυτός ο κώδικας στη συνέχεια μεταδίδεται σε όλους τους κόμβους του δικτύου (υπολογιστές που είναι συνδεδεμένοι και να τρέχει 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. 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, του χρόνου, ή η προσωρινή παράδοση του νομίσματος, και αντιπροσωπεύει το κόστος για την ασφάλεια του δικτύου. Οι χρήστες που κάνουν εξόρυξη κρυπτονομισμάτων - εκείνοι που κατέχουν τον υποκείμενο πόρο, και ως εκ τούτου μπορούν να τον δαπανήσου – 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 της υποκείμενης οικονομίας του νομίσματος. Οι επόμενες παράγραφοι θα

παρουσιάσουν αναλυτικά τους πιο ευρέως χρησιμοποιούμενους μηχανισμούς στη βιομηχανία των κρυπτονομισμάτων.

3.2.1 Proof-of-work

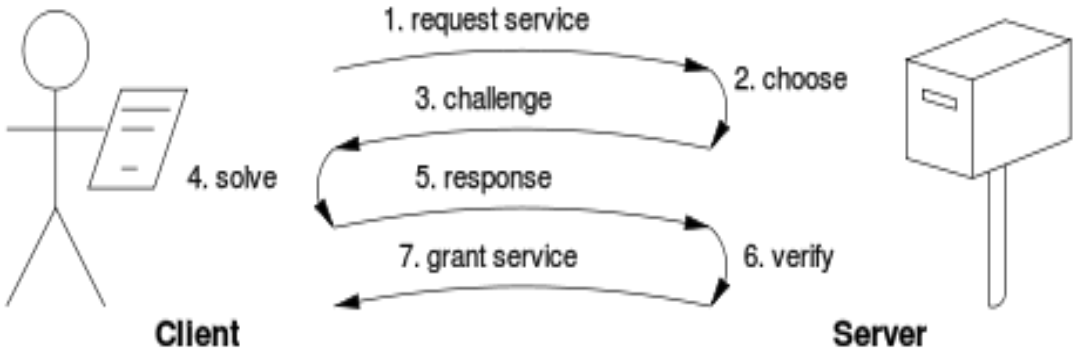
Ένα σύστημα απόδειξης εργασίας (POW) ή πρωτόκολλο, ή λειτουργία, είναι ένα οικονομικό μέτρο για την αποτροπή επιθέσεων άρνησης παροχής υπηρεσίας και άλλων καταχρήσεων των υπηρεσιών, όπως το spam σε ένα δίκτυο, απαιτώντας κάποια εργασία από τον αιτούντα υπηρεσία, που συνήθως σημαίνει ότι χρόνο επεξεργασίας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

Ένα βασικό χαρακτηριστικό των συστημάτων αυτών είναι η ασυμμετρία τους: η εργασία πρέπει να είναι μέτρια σκληρή (αλλά εφικτή) από την πλευρά του αιτούντος, αλλά εύκολη να ελεγχθεί για τον πάροχο υπηρεσιών. Η ιδέα αυτή είναι επίσης γνωστή ως μια συνάρτηση κόστους της CPU, παζλ πελάτη, υπολογιστικό παζλ ή λειτουργία τιμολόγηση της CPU. Είναι διαφορετική από το CAPTCHA, το οποίο προορίζεται για έναν άνθρωπο να λύσει γρήγορα, παρά έναν υπολογιστή.

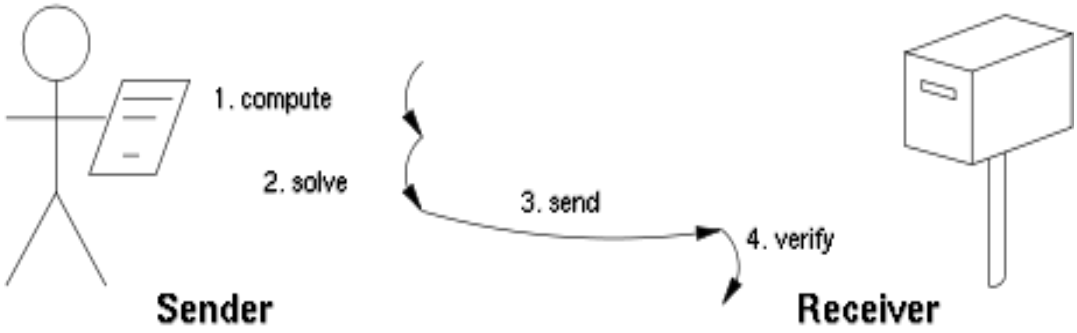
Υπάρχουν δύο κατηγορίες πρωτοκόλλων απόδειξης της εργασίας:

- 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 και να ελέγχεται 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 δύνανται να ορίζονται εάν το πρωτόκολλο πρόκλησης-απόκρισης έχει μια γνωστή λύση (επιλέγεται από τον πάροχο), ή είναι γνωστό ότι υπάρχει μέσα σε ένα οριοθετημένο χώρο αναζήτησης.

- Πρωτόκολλα λύσης-επαλήθευσης δεν δεσμεύουν μια τέτοια σύνδεση: ως εκ τούτου 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 μη οριοθετημένες πιθανολογικές επαναληπτικές διαδικασίες, όπως μετρητές κατακερματισμού (Hashcash).



Εικόνα 4. Πρωτόκολλα πρόκλησης-απόκρισης



Εικόνα 5. Πρωτόκολλα λύσης-επαλήθευσης

Πρωτόκολλα γνωστής λύσης τείνουν να έχουν ελαφρώς χαμηλότερη διακύμανση από τα unbounded πιθανολογικά πρωτόκολλα, επειδή η διακύμανση της ορθογώνιας διανομής είναι μικρότερη από την διακύμανση της κατανομής Poisson (με την ίδια μέση τιμή). Μια γενική τεχνική για τη μείωση της διακύμανσης είναι η χρήση πολλαπλών ανεξάρτητων υπο-προκλήσεων, καθώς ο μέσος όρος των πολλαπλών δειγμάτων θα έχει χαμηλότερη διακύμανση.

Υπάρχουν επίσης συναρτήσεις σταθερού κόστους. Επιπλέον, οι βασικές λειτουργίες που χρησιμοποιούνται από τα συστήματα αυτά μπορεί να είναι:

- Συνδεδεμένα με τη CPU εφόσον ο υπολογισμός τρέχει με την ταχύτητα του επεξεργαστή, η οποία ποικίλλει σημαντικά στο χρόνο, καθώς και από το high-end server για τις low-end φορητές συσκευές.
- Συνδεδεμένα με τη Μνήμη όταν η ταχύτητα υπολογισμού δεσμεύεται από κύριες προσβάσεις μνήμης (είτε λανθάνουσες ή στο εύρος ζώνης), η απόδοση των οποίων αναμένεται να είναι λιγότερο ευαίσθητη στην εξέλιξη του hardware.
- Συνδεδεμένα με το Δίκτυο, εάν ο πελάτης πρέπει να εκτελέσει μερικούς υπολογισμούς, αλλά πρέπει να συλλέξει κάποιες μάρκες από απομακρυσμένους διακομιστές πριν απευθυνθεί στον τελικό φορέα παροχής υπηρεσιών. Με αυτή την έννοια το έργο δεν εκτελείται όντως από τον αιτούντα, αλλά συνεπάγεται καθυστερήσεις ούτως ή άλλως, λόγω της καθυστέρησης να πάρει τις απαιτούμενες μάρκες.

Τέλος, ορισμένα συστήματα POW προσφέρουν συντόμευση υπολογισμών που επιτρέπουν στους συμμετέχοντες που γνωρίζουν ένα μυστικό, συνήθως ιδιωτικό κλειδί, να δημιουργήσουν φτηνά POW. Το σκεπτικό είναι ότι οι κάτοχοι λίστας αλληλογραφίας μπορούν να δημιουργήσουν σφραγίδες για κάθε δικαιούχο, χωρίς να συνεπάγεται υψηλό κόστος. Αν ένα τέτοιο χαρακτηριστικό είναι επιθυμητό εξαρτάται από το σενάριο χρήσης.

Ο επιστήμονας υπολογιστών Hal Finney (2007) βασίστηκε στην ιδέα απόδειξης της εργασίας, αποδίδοντας ένα σύστημα που εκμεταλλεύεται επαναχρησιμοποιήσιμη απόδειξη της εργασίας («RPOW»). Είχε ήδη καθιερωθεί η ιδέα της δημιουργίας επαναχρησιμοποιήσιμων αποδείξεων-της-εργασίας για κάποιο πρακτικό σκοπό το 1999. Σκοπός του Finney με τη χρήση RPOW ήταν ως συμβολική χρήματα. Ακριβώς όπως η τιμή χρυσού νομίσματος είναι πιθανό να υποστηρίζεται από την αξία του χρυσού που απαιτείται για να κατασκευαστεί το νόμισμα, η αξία ενός διακριτικού

RPOW είναι εγγυημένη από την αξία των πραγματικών πόρων που απαιτούνται για την δημιουργία μιας συμβολικής POW. Στην έκδοση της RPOW του Finney, η συμβολική POW αποτελεί ένα κομμάτι του μετρητή κατακερματισμού.

Ένας δικτυακός τόπος μπορεί να απαιτήσει ένα συμβολικό POW αντάλλαγμα της υπηρεσίας. Η απαίτηση συμβολικού POW από τους χρήστες θα αναστείλει την επιπόλαιη ή υπερβολική χρήση της υπηρεσίας, απαλλάσσοντας υποκείμενους πόρους της υπηρεσίας, όπως το εύρος ζώνης στο Internet, ο υπολογισμός, ο χώρος στο δίσκο, η ηλεκτρική ενέργεια και τα γενικά διοικητικά έξοδα.

Το σύστημα RPOW του Finney διαφέρει από ένα POW σύστημα στο ότι επιτρέπει τη τυχαία ανταλλαγή μαρκών χωρίς να επαναληφθούν οι εργασίες που απαιτούνται για τη δημιουργία τους. Αφού κάποιος περάσει μια συμβολική POW σε μια ιστοσελίδα, ο φορέας εκμετάλλευσης του δικτυακού τόπου θα μπορούσε να ανταλλάξει το POW για ένα νέο, μη χρησιμοποιηθέν συμβολικό RPOW, το οποίο θα μπορούσε στη συνέχεια να δαπανηθούν σε κάποια ιστοσελίδα τρίτου ομοίως εξοπλισμένη για να δεχτεί μάρκες RPOW. Αυτό θα εξοικονομήσει πόρους που διαφορετικά θα χρειαζόταν για τη δημιουργία μιας συμβολικής POW. Η αντι-πλαστή περιουσία του διακριτικού RPOW είναι εγγυημένη από απομακρυσμένη πιστοποίηση. Ο διακομιστής RPOW που ανταλλάσσει ένα μεταχειρισμένο RPOW κουπόνι με ένα νέο ίσης αξίας χρησιμοποιεί απομακρυσμένη πιστοποίηση για να επιτρέψει σε κάθε ενδιαφερόμενο να εξακριβώσει τι λογισμικό εκτελείται στο διακομιστή RPOW. Δεδομένου ότι ο πηγαίος κώδικας για το λογισμικό RPOW του Finney δόθηκε στη δημοσιότητα (στο πλαίσιο μιας άδειας τύπου BSD), κάθε προγραμματιστής με επαρκής γνώση θα μπορούσε, κατά την επιθεώρηση του κώδικα, να βεβαιωθεί ότι το λογισμικό (και, κατ 'επέκταση, ο διακομιστής RPOW) ουδέποτε εξέδωσε ένα νέο κουπόνι εκτός σε αντάλλαγμα για μια συμβολική RPOW ίσης αξίας.

Μέχρι το 2009, το σύστημα Finney ήταν το μόνο σύστημα RPOW που είχε υλοποιηθεί, αλλά ποτέ δεν είδε οικονομικά σημαντική χρήση. Το 2009, το δίκτυο Bitcoin πήγε σε απευθείας σύνδεση. Το Bitcoin είναι ένα κρυπτονόμισμα απόδειξης εργασίας που, όπως το RPOW του Finney, βασίζεται επίσης στον μετρητή κατακερματισμού POW. Αλλά η προστασία στο Bitcoin παρέχεται από ένα

αποκεντρωμένο P2P πρωτόκολλο για την παρακολούθηση της μεταφοράς των κερμάτων, σε αντίθεση με το υλικό εμπιστοσύνης στη λειτουργία των υπολογιστών που χρησιμοποιούνται από το RPOW. Το Bitcoin έχει καλύτερη αξιοπιστία, επειδή προστατεύεται από τον υπολογισμό. Το RPOW προστατεύεται από τα ιδιωτικά κλειδιά αποθηκεύονται στο υλικό TPM και οι κατασκευαστές κατέχουν τα ιδιωτικά κλειδιά TPM. Οι χάκερ που κλέβουν ένα βασικό κατασκευαστή TPM, ή οποιονδήποτε ικανό να αποκτήσει το κλειδί με την εξέταση του ίδιου του TPM chip, θα μπορούσαν να ανατρέψουν αυτή τη διαβεβαίωση. Τα Bitcoins εξορύσσονται χρησιμοποιώντας το μετρητή κατακερματισμού με λειτουργία απόδειξης της εργασίας από μεμονωμένους κόμβους και επαληθεύονται από το αποκεντρωμένο δίκτυο P2P Bitcoin.

Άλλα κρυπτονομίσματα χρησιμοποιούν διαφορετικούς αλγορίθμους κατακερματισμού, καθώς και προνομιακές αλυσίδες ως απόδειξη της εργασίας. Στον παρακάτω πίνακα δίνονται οι αλγόριθμοι hash και timestamping για τα πιο γνωστά κρυπτονομίσματα.

Release	Active	Currency	Symbol	Hash Algorithm	Timestamping
2014	Active	Auroracoin	AUR	Scrypt	POW
2009	Active	Bitcoin	BTC	SHA-256d	POW
2014	Active	BlackCoin	BC, BLK	Scrypt	POS
2014	Inactive	Coinye	KOI, COYE	Scrypt	POW
2014	Active	Dash	DASH	X11	POW & POS
2013	Active	Dogecoin	DOGE	Scrypt	POW
2014	Active	DigitalNote	XDN	CryptoNight	POW
2015	Active	Ethereum	ETH	Dagger Hashimoto	POW
2011	Active	Litecoin	LTC	Scrypt	POW
2013	Active	Mastercoin	MSC	SHA-256d	N/A

2014	Active	MazaCoin	MZC	SHA-256d	POW
2014	Active	Monero	XMR	CryptoNight	POW
2011	Active	Namecoin	NMC	SHA-256d	POW
2013	Active	Nxt	NXT	SHA-256d	POS
2012	Active	Peercoin	PPC	SHA-256d	POW & POS
2013	Active	Emercoin	EMC	SHA-256	POW & POS
2014	Active	PotCoin	POT	Scrypt	POW
2013	Active	Primecoin	XPM	1CC/2CC/TWN	POW
2013	Active	Ripple	XRP[32]	ECDSA	Consensus
2014	Active	Titcoin	TIT	SHA-256d	POW
Unreleased	Inactive	Zerocoin			

3.2.2 Proof-of-stake

Η απόδειξη της συμμετοχής (proof-of-stake) είναι μια μέθοδος με την οποία ένα δίκτυο blockchain κρυπτονομισμάτων αποσκοπεί στην επίτευξη διανεμημένης συναίνεσης. Αν και η μέθοδος απόδειξης της εργασίας ζητά από τους χρήστες να τρέχουν επανειλημμένα αλγόριθμοι κατακερματισμού για την επικύρωση των ηλεκτρονικών συναλλαγών, η απόδειξη της συμμετοχής ζητά από τους χρήστες 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.

Η απόδειξη της εργασίας βασίζεται στη χρήση της ενέργειας. Σύμφωνα με ένα χειριστή εξόρυξης Bitcoin, η κατανάλωση ενέργειας ανήλθε στις 240kWh ανά Bitcoin το 2014 (ισοδύναμο με 16 γαλόνια φυσικού αερίου). Επιπλέον, οι δαπάνες της ενέργειας σχεδόν πάντα καταβάλλονται σε μη-κρυπτονόμισμα, εισάγοντας σταθερή

πτωτική πίεση στην τιμή. Η μέθοδος απόδειξης της συμμετοχής μπορεί να είναι αρκετές χιλιάδες φορές πιο αποδοτική.

Τα κίνητρα της γεννήτριας μπλοκ είναι επίσης διαφορετικά. Υπό την απόδειξη της εργασίας, η γεννήτρια μπορεί δυνητικά να μην κατέχει κανένα από τα νομίσματα που παράγονται από την εξόρυξη. Το κίνητρο του ανθρακωρύχου είναι μόνο να μεγιστοποιήσουν τα δικά του κέρδη. Δεν είναι σαφές αν αυτή η ανισότητα μειώνει ή αυξάνει τους κινδύνους ασφαλείας. Στην Απόδειξη της συμμετοχής, αυτοί που φυλάσσουν τα νομίσματα είναι πάντα αυτοί που κατέχουν τα νομίσματα (αν και αρκετά κρυπτονομίσματα επιτρέπουν ή επιβάλλουν τον δανεισμό της δυνατότητας συμμετοχής σε άλλους κόμβους).

3.2.3 Υβριδικός μηχανισμός POW/POS

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. Οι Sunny King και Scott Nadal (2013), στο εγχειρίδιο "PPCoin: Peer-to-Peer Crypto-Νόμισμα με απόδειξη-της-Συμμετοχής", είναι οι πρώτοι που προτείνουν και στη συνέχεια εφαρμόζουν ένα τέτοιο υβριδικό σύστημα POW / POS. Σε αυτόν τον υβριδικό σχεδιασμό, η παραγωγή μπλοκ, αντί να βασίζεται σε μία CPU ανά ψήφο, βασίζεται στην έννοια του πλήθους νομισμάτων ή coinage. Το coinage είναι περίπου το πλήθος νομισμάτων ενός ιδιοκτήτη πολλαπλασιασμένο με το χρόνο της κυριότητας από τον σημερινό ιδιοκτήτη του νομίσματος. Η παραγωγή μπλοκ πηγαίνει έτσι στο μπλοκ με το πιο πολλά νομίσματα (ανάλογα με το coinage). Περαιτέρω, τα νομίσματα κόβονται κατά μία ποσοστιαία μονάδα της κατανάλωσης ανά έτος, η οποία λειτουργεί ως επιτόκιο για το νόμισμα. Το κύριο πλεονέκτημα, ωστόσο, είναι ότι αυτό το σύστημα δεν βασίζεται σε υψηλή κατανάλωση ενέργειας μακροπρόθεσμα. Ως εκ τούτου, 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.

3.2.4 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. Τα μηνύματα σε αυτή την περίπτωση είναι συναλλαγές. Αυτό το σύστημα είναι ανθεκτικό στην κατηγορία των αποτυχιών που είναι γνωστή ως προβλήματα Byzantine Generals και ως εκ τούτου θεωρείται ανθεκτικό στην οικογένεια προβλημάτων Byzantine. Σε αυτού του τύπου τα προβλήματα, ο βυζαντινός στρατός διχάζεται ανάμεσα σε πολλούς υπαξιωματικούς που λαμβάνουν εντολή για επίθεση ή υποχώρηση από έναν γενικό διοικητή. Ωστόσο, υπάρχει ένας αριθμός των προδοτών - ενδεχομένως ο ίδιος ο γενικός διοικητής - αλλά όλοι οι πιστοί στρατηγοί πρέπει να καταλήξουν σε συμφωνία μεταξύ τους, ενώ θα πρέπει να αποκλείσουν τους προδότες για να αποτρέψουν τα σχέδια τους. Το πρόβλημα είναι ότι οι πιστοί υπαξιωματικοί πρέπει να καταλήξουν σε συναίνεση σχετικά με το ποια εντολή να υπακούσουν, στέλνοντας μεταξύ τους υπογεγραμμένα μηνύματα. Διάφοροι αλγόριθμοι έχουν προταθεί ως αποτελεσματικοί για το ανωτέρω πρόβλημα.

Τα κατανεμημένα δίκτυα που δημιουργούνται από τα κρυπτονομίσματα Ripple και Stellar αντιμετωπίζουν ένα πρόβλημα ανάλογο με το παραπάνω. Πρώτον, 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 ο

διακομιστής επικοινωνεί μόνο με τους κόμβους στο UNL του. Αυτό επιτρέπει στους διακομιστές να είναι σε επαφή μόνο με αξιόπιστους διακομιστές. Κάθε διακομιστής μπορεί να μεταδώσει τις συναλλαγές, και οι διακομιστές ψηφίζουν επί των συναλλαγών. 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.

Στον πίνακα 3-1 παρουσιάζονται τα κύρια χαρακτηριστικά του κάθε μηχανισμού ασφαλείας (Mazieres, 2015).

Πίνακας 1 Τα κύρια χαρακτηριστικά κάθε μηχανισμού ασφαλείας (Mazieres, 2015)

Μηχανισμός	**Αποκεντρωμένος Έλεγχος**	**Χαμηλή Καθυστέρηση**	**Ευέλικτη Εμπιστοσύνη**	**Μακροπρόθεσμο Χαμηλό Κόστος Ενέργειας**
PoW	x			
PoS	x	μπορεί		x
Consensous (Byzantine)	x	x	x	x
PoS/PoW	x	μπορεί		x

3.3 ΑΛΓΟΡΙΘΜΟΙ HASH

Εκτός από το μηχανισμό ασφαλείας του δικτύου, οι αλγόριθμοι κατακερματισμού (hash) επηρεάζουν επίσης τα κρυπτονομίσματα. Για τον μηχανισμό Pow, ο αλγόριθμος κατακερματισμού και η δυσκολία στόχευσης του κατακερματισμού υπαγορεύουν πόσα hashes - πόση ενέργεια - αναμένεται να δαπανηθεί. Επειδή οι χρήστες που εξορυγνύουν κρυπτονομίσματα έχουν κίνητρα να βρίσκουν και να χρησιμοποιούν όλο και πιο ισχυρό εξοπλισμό πληροφορικής, έχει δημιουργηθεί μεγάλος ανταγωνισμός σχετικά με τον εξοπλισμό. Για παράδειγμα, η εξόρυξη αρχικά πραγματοποιούταν από την CPU (Κεντρική Μονάδα Επεξεργασίας). Ωστόσο, οι ίδιες λειτουργίες θα μπορούσαν να εκτελούνται από τη GPU (Graphics Processing Unit) με πολύ ταχύτερο ρυθμό. Οι GPUs, στη συνέχεια, έδωσαν τη θέση τους στην εφαρμογή ολοκληρωμένων κυκλωμάτων ειδικού σκοπού (ASIC), με σκοπό τη διενέργεια εξόρυξης κρυπτονομισμάτων Pow σε απίστευτες ταχύτητες - μεγέθη υψηλότερα από ό, τι θα μπορούσαν μέσω GPUs. 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. Ωστόσο, αυτό δεν ισχύει, καθώς οι ASICs μπορούν να σχεδιαστούν για την εκτέλεση κάθε αλγορίθμου κατακερματισμού. Το υψηλό κόστος αυτής της διαδικασία είναι ένα μειονέκτημα, και πρέπει να δοθούν επαρκή κίνητρα σε αυτούς που κάνουν εξόρυξη κρυπτονομισμάτων, για την κατασκευή των ASIC για ένα συγκεκριμένο αλγόριθμο κατακερματισμού πλην του SHA-256, όπως Scrypt. Υπήρξε μια δραματική αύξηση στον αριθμό των giga hashes ανά δευτερόλεπτο στο δίκτυο Bitcoin.

Ένα άλλο πρόβλημα είναι οι οικονομίες κλίμακας που δημιουργούνται. Για να είναι αποκεντρωμένος ο έλεγχος, τα νομίσματα πρέπει να έχουν κατανεμημένη την ασφάλεια μεταξύ πολλών χρηστών. Ωστόσο, οι επενδυτές μικρής κλίμακας βλέπουν πλέον ως επικερδή τη σύνδεση των υπολογιστών του σπιτιού τους το δίκτυο κρυπτονομισμάτων, δεδομένου ότι τότε θα αναγκαστούν να ανταγωνιστούν με πολύ πιο γρήγορα ASICs. Ως εκ τούτου, αυτός ο ανταγωνισμός εξοπλισμών είχε ως

αποτέλεσμα κατ 'ουσίαν, τη συγκέντρωση του ελέγχου του δικτύου στα χέρια των μεγαλύτερων miners.

3.3.1 Scrypt

Στην κρυπτογραφία, το scrypt είναι μια λειτουργία προέλευσης κλειδιών που βασίζεται σε κωδικό πρόσβασης. Ο αλγόριθμος σχεδιάστηκε ειδικά για να καταστήσει δαπανηρές τις εκτελέσεις επιθέσεων μεγάλης κλίμακας σε υλικό υπολογιστών που απαιτούν μεγάλες ποσότητες μνήμη. Το 2012, ο αλγόριθμος scrypt δόθηκε στη δημοσιότητα από το IETF ως ένα σχέδιο Διαδικτύου, που προορίζεται να γίνει μια ενημερωτική RFC. Μια απλοποιημένη εκδοχή του scrypt χρησιμοποιείται ως ένα σύστημα απόδειξης της εργασίας από μια σειρά κρυπτονομίσματα, όπως το Litecoin.

Μια λειτουργία προέλευσης κλειδιών που βασίζεται σε κωδικό πρόσβασης (με βάση τον κωδικό KDF) έχει σχεδιαστεί για να είναι υπολογιστικά εντατική, ώστε να πάρει ένα σχετικά μεγάλο χρονικό διάστημα για να υπολογιστεί (ας πούμε της τάξης των μερικών εκατοντάδων χιλιοστών του δευτερολέπτου). Εξουσιοδοτημένοι χρήστες πρέπει μόνο να εκτελέσουν τη συνάρτηση 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 και να γίνουν σημαντικές και, ιδανικά, απαγορευτικές.

Προηγούμενες λειτουργίες που βασίζονται σε κωδικό πρόσβασης KDFs (όπως το δημοφιλές PBKDF2) έχουν σχετικά χαμηλές απαιτήσεις πόρων, που σημαίνει ότι δεν χρειάζονται περίτεχνα υλικό ή πολύ μνήμη για να εκτελεστούν. Είναι, συνεπώς, εύκολο και φτηνό να υλοποιηθούν από άποψη υλικού (για παράδειγμα, σε ένα ASIC ή ακόμα και ένα FPGA). Αυτό επιτρέπει σε έναν εισβολέα με επαρκείς πόρους να ξεκινήσει μια μεγάλης κλίμακας επίθεση παράλληλα με την οικοδόμηση εκατοντάδων ή ακόμα και χιλιάδων εφαρμογών του αλγορίθμου σε υλικό και με κάθε αναζήτηση να υπάρχει ένα διαφορετικό υποσύνολο του κλειδιού χώρου. Αυτό

χωρίζει το ποσό του χρόνου που απαιτείται για να ολοκληρωθεί μια επίθεση από τον αριθμό των διαθέσιμων εφαρμογών, πολύ πιθανόν υλοποιώντας τες 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 ένα μεγάλο ποσό της μνήμης σε σύγκριση με άλλα KDFs, καθιστώντας το μέγεθος και το κόστος μιας εφαρμογής υλικού πολύ πιο ακριβή, και επομένως περιορίζουν την ποσότητα του παραλληλισμού ένας εισβολέας, για μια δεδομένη ποσότητα των χρηματοδοτικών πόρων.

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 ψευδο-τυχαία σειρά και συνδυάζονται για να παράγουν το παράγωγο κλειδί. Μία απλή εφαρμογή θα πρέπει να κρατήσει το σύνολο του φορέα σε μνήμη τυχαίας προσπέλασης, 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 αλγορίθμους υπολογιστή: μπορείτε να αυξήσετε την ταχύτητα με το κόστος χρήσης περισσότερης μνήμης, ή να μειώσετε τις απαιτήσεις σε μνήμη με το κόστος της εκτέλεσης περισσοτέρων από τις εργασίες και τη μείωση της ταχύτητας. Η ιδέα πίσω από το scrypt είναι να κάνει σκόπιμα αυτό το trade-off δαπανηρό σε 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.

3.3.2 SHA-2

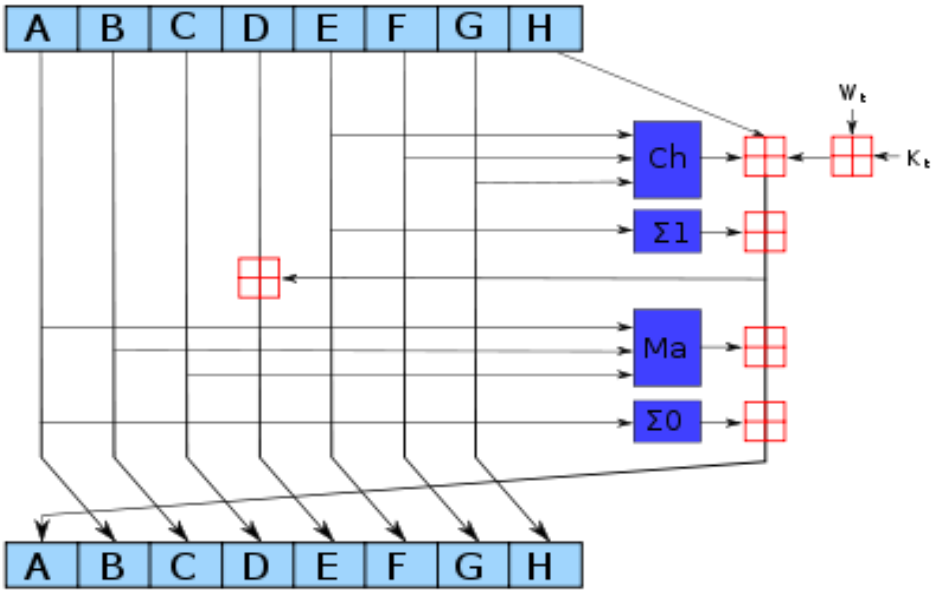
Ο SHA-2 (Secure Hash Algorithm 2) είναι ένα σύνολο κρυπτογραφικών hash λειτουργίών που σχεδιάστηκε από την NSA. Οι λειτουργίες κρυπτογράφησης hash είναι μαθηματικές πράξεις που εκτελούνται σε ψηφιακά δεδομένα? με τη σύγκριση της υπολογιζόμενης "hash" (η έξοδος από την εκτέλεση του αλγορίθμου) με μια 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 των κρυπτογραφικών hash λειτουργιών είναι η αντίσταση η σύγκρουσή τους: 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, SHA-1. Η οικογένεια SHA-2 αποτελείται από έξι hash λειτουργίες με digests (τιμές hash) που είναι 224, 256, 384 ή 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, 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 ακρωτηριασμένες εκδοχές των δύο πρώτων, υπολογίζονται με διαφορετικές αρχικές τιμές. Οι SHA-512/224 και SHA-512/256 είναι επίσης ακρωτηριασμένες 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 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 αφομοιώνει 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 τον αρχικό SHA-1 αλγόριθμο, με σύγχρονες τεχνικές σημειογραφίας σύμφωνες με αυτές που περιγράφει η εσωτερική λειτουργία της οικογένειας SHA-2.



Εικόνα 6. Μία επανάληψη στη λειτουργία συμπίεσης της οικογένειας SHA-2.

3.3.3 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 πιστεύεται 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 εκτελέσεις 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 τονECDSA: 4t bits, όπου t είναι το επίπεδο ασφάλειας που μετράται σε bits, δηλαδή, περίπου 320 bits για ένα επίπεδο ασφάλειας του 80 bits.

3.3.4 Cryptonight

Ο CryptoNight είναι ένας αλγόριθμος απόδειξη της εργασίας (PoW). Είναι σχεδιασμένος για να είναι κατάλληλος για τους απλούς επεξεργαστές υπολογιστών, αλλά προς το παρόν δεν υπάρχουν συσκευές ειδικού σκοπού για την εξόρυξη. Ως εκ τούτου, ο CryptoNight μπορεί να εξορύσσεται μόνο μέσω της CPU προς το παρόν. Ο CryptoNight εφαρμόστηκε αρχικά στη βάση κώδικα CryptoNote.

Βασικές αρχές

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:

- Ταιριάζει στη μνήμη cache L3 (ανά πυρήνα) των σύγχρονων επεξεργαστών.
- Ένα MB εσωτερικής μνήμης είναι μη αποδεκτό από τις σύγχρονες ASICs.
- 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 απαιτήσει αύξηση των επαναλήψεων, η οποία με τη σειρά της συνεπάγεται μια συνολική αύξηση του χρόνου. "Βαριές" κλήσεις σε ένα δίκτυο p2p μπορεί να οδηγήσουν σε σοβαρές αδυναμίες, επειδή οι κόμβοι είναι υποχρεωμένοι να ελέγχουν την απόδειξη εργασίας κάθε νέου μπλοκ. Αν ένας κόμβος ξοδεύει σημαντικό ποσό χρόνου σε κάθε αξιολόγηση hash, μπορεί εύκολα να γίνει DDoS από μια πληθώρα πλαστών αντικειμένων με αυθαίρετα δεδομένα έργου (τιμές nonce).

3.3.5 Αλγόριθμος X11

Αυτοί οι νέοι και κερδοφόροι αλγόριθμοι είναι πολύ δημοφιλείς από το 2014 στην εξόρυξη GPU.

Αυτοί οι αλγόριθμοι κρυπτονομισμάτων έχουν δημιουργηθεί ειδικά για την εξόρυξη GPU και είναι σε θέση να παρέχουν μια καλή κερδοφορία στην κοινότητα μετά την άνοδο των μεγάλων ASICs για το Scrypt. Φαίνεται ότι κάθε αποτέλεσμα από έναν υπο-αλγόριθμο κατόπιν περνιέται στον επόμενο υπο-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, η οποία χρησιμοποιείται για τους υπολογισμούς στον μηχανισμό απόδειξης της εργασίας ώστε να υπάρχει ασφάλεια στο δίκτυο ορισμένων κρυπτονομισμάτων.

Είναι γνωστός ως αλυσιδωτός αλγόριθμος επειδή χρησιμοποιεί 11 διαφορετικούς αλγορίθμους που είναι συνδεδεμένοι μεταξύ τους. Αυτοί είναι: Blake, bmw, groestl, JH, keccak, skein, luffa, cubehash, shavite, simd, και echo.

Είναι ανθεκτικός στην υλοποίηση ASIC και κατάλληλος τόσο για την εξόρυξη CPU όσο και για εξόρυξη GPU. Το πρώτο κρυπτονόμισμα που χρησιμοποίησε τον X11 στο δίκτυο του ήταν το Darkcoin, που από τότε έχει αλλάξει το όνομα του σε «Dashcoin».

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 αναπτύξει ειδικό υλικό, που ονομάζεται ASICs, για την εξόρυξη κερμάτων όπου χρησιμοποιούνται οι αλγόριθμοι εξόρυξης SHA-256 και Scrypt. 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 χρήστεςνα 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 γίνονται φυσικά υποστηρικτές του, και μπορεί να αυξήσει την πιθανότητα τα κρυπτονομίσματα που εξορύσσονται να υφίστανται άμεσο «ντάμπινγκ», καθώς οι επιχειρήσεις θα πρέπει να καλύπτουν το κόστος και να λαμβάνουν τα κέρδη, ενώ οι ιδιώτες όχι.

Με το σχεδιασμό του αλγορίθμου X11 που είναι κατάλληλος για χρήση σε επεξεργαστές CPU γενικού σκοπού και συνήθεις κάρτες γραφικών GPU, και με τη διέλευση μέσω πολλών διαφορετικών αλγορίθμων και όχι χρησιμοποιώντας ένα ενιαίο αλγόριθμο, δημιουργείται δυσκολία στους κατασκευαστές να αναπτύξουν ASIC, για τα νομίσματα τα οποία χρησιμοποιούν αυτόν τον αλγόριθμο. Αν και είναι πιθανό ότι το ASIC, τελικά θα παραχθεί, τα X11 κέρματα αναμένεται να παραμείνουν ανθεκτικά στο ASIC για τουλάχιστον το βραχυπρόθεσμο και μεσοπρόθεσμο μέλλον. Η χρήση των 11 διαφορετικών αλγορίθμων αυξάνει επίσης

την ασφάλεια των νομισμάτων χρησιμοποιώντας τη μέθοδο αυτή κατά τις βίαιες επιθέσεις. 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 Scrypt είναι το γεγονός ότι είναι λιγότερο εντατικός και ως εκ τούτου χρησιμοποιεί λιγότερη ηλεκτρική ενέργεια. Οι υπολογιστές που εκτελούν άλλους αλγόριθμους τείνουν να αυξάνουν τη θερμοκρασία του και να χρησιμοποιήούν 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 καθώς και υποβαθμίζει τη συνολική απόδοση.

3.4 ΜΕΤΑΒΛΗΤΕΣ ΑΞΙΟΛΟΓΗΣΗΣ ΕΓΓΕΝΟΥΣ ΑΞΙΑΣ

Αν ο όγκος των συναλλαγών αυξηθεί πολύ, τότε η ισοτιμία από δολάρια σε bitcoins πρέπει να αυξηθεί πάρα πολύ, επειδή κάθε Bitcoin μπορεί να χρησιμοποιηθεί μόνο συγκεκριμένες φορές την ημέρα. Η αγοραία αξία όλων των bitcoins πρέπει να είναι αρκετή για να στηρίξει τον όγκο των συναλλαγών.

Η εγγενής αξία μετριέται συνήθως με τη χρήση της μεθόδου των προεξοφλημένων ταμειακών ροών. Αυτή είναι η ιδέα που μπορεί να εκτιμήσει την εγγύηση σήμερα με την προεξόφληση των μελλοντικών ταμειακών ροών στην παρούσα αξία τους. Στην περίπτωση του Paypal ή Western Union, οι επιχειρήσεις παράγουν έσοδα, χρεώνοντας για τις υπηρεσίες μετάδοσης χρήματος, τα οποία στη συνέχεια χρησιμοποιούνται για να εξοφλήσουν τα έξοδα και τελικά να δημιουργήσουν μια ταμειακή ροή για τους επενδυτές. Στην περίπτωση των κρυπτονομισμάτων χρησιμοποιείται ένας αλγόριθμος απόδειξης της εργασίας (proof-of-work), δεν υπάρχουν ταμειακές ροές, ούτε μερίσματα που καταβάλλονται στους κατόχους.

Ταχύτητα (velocity): Ο ρυθμός κινητικότητας των νομισμάτων μεταξύ διαφόρων κατόχων, έναντι της συσσώρευσης. Η ταχύτητα αντιπροσωπεύει τον αριθμό των φορών που κάθε νόμισμα δαπανάται σε ένα χρόνο. Αν ο αριθμός αυτός αυξάνεται, η χρήση του κάθε επιμέρους νομίσματος αυξάνεται τελικά, μειώνοντας την αξία του κάθε νομίσματος. Αυτό είναι επειδή χρειάζονται λιγότερα νομίσματα, τα οποία τώρα κινούνται γρηγορότερα μεταξύ των συναλλαγών, για να διατηρηθεί το ίδιο επίπεδο συναλλακτικής δραστηριότητας.

Κεφαλαιοποίηση (capitalization): Η συνολική αξία αγοράς σε δολάρια όλων των μετοχών της εταιρείας (ή των στοιχείων του ενεργητικού). Η κεφαλαιοποίηση υπολογίζεται πολλαπλασιάζοντας τις μετοχές μιας εταιρείας με την τρέχουσα τιμή της αγοράς μίας μετοχής. Η επενδυτική κοινότητα χρησιμοποιεί αυτόν τον αριθμό για να προσδιοριστεί το μέγεθος της εταιρείας, σε αντίθεση με τις πωλήσεις ή τα συνολικά στοιχεία του ενεργητικού.

Εικόνα 7. Κεφαλαιοποίηση Bitcoin για την περίοδο 2013-2015 (blockchain.info).

Ζήτηση (demand): Η αξία ζήτησης οδηγείται από τη χρησιμοποίηση των κρυπτονομισμάτων ως ένα δίκτυο ή νόμισμα πληρωμής. Σε κάθε δεδομένο σημείο, υπάρχει μια απαιτούμενη κεφαλαιοποίηση για να διατηρήσει ένα ορισμένο επίπεδο συναλλακτικής δραστηριότητας. Αυτό θα περιλαμβάνει τις συναλλαγές που

θεωρούνται πληρωμές, όπως αγορές και εμβάσματα, αλλά θα αποκλειστούν οι κερδοσκοπικές συναλλαγές FX στις συναλλαγές καθώς αυτές δεν προσθέτουν αξία στην χρήση των κρυπτονομισμάτων ως ένα δίκτυο πληρωμών. Η ιδέα πίσω από τον παρακάτω τύπο βασίζεται στην ποσοτική θεωρία του χρήματος:

$$Συνολική\ Δαπάνη = Ταχύτητα\ x\ Κεφαλαιοποίηση$$

Επομένως για να υπολογίσουμε την απαιτούμενη κεφαλαιοποίηση ενός κρυπτονομίσματος για να καλύπτονται οι συναλλαγές:

$$Απαιτούμενη\ Κεφαλαιοποίηση = \frac{Συνολική\ Δαπάνη}{Ταχύτητα}$$

Ωστόσο, η απαιτούμενη κεφαλαιοποίηση εδώ είναι διαφορετική από ότι απλά ο πολλαπλασιασμός της τιμής ανά κέρμα με τον αριθμό των νομισμάτων. Επειδή δεν συμμετέχουν όλα τα νομίσματα στη συντήρηση της απαιτούμενης κεφαλαιοποίησης της αγοράς, οι υπολογισμοί γίνονται πάντα με υπερεκτίμηση.

Προσφορά (supply): Η προμήθεια στα κρυπτονομίσματα παραδοσιακά θεωρείται απλά ως τα νομίσματα που υπάρχουν διαθέσιμα ως προϊόντα εξόρυξης. Αυτό, ωστόσο, δεν λαμβάνει υπόψη το γεγονός ότι κέρματα έχουν χαθεί με τη πάροδο του χρόνου, κέρμα παρακρατούνται από τη διανομή και δεν έχουν χρησιμοποιηθεί για συναλλαγές, δηλαδή νομίσματα που χρησιμοποιούνται ως μέσο αποθήκευσης αξίας. Το 2013, οι ερευνητές υπολόγισαν ότι μέχρι και το 64% των bitcoins παρέμεινε σε αποθήκευση. Πολλά άτομα έχουν αρχίσει να χρησιμοποιούν τα Bitcoin ως μέσα μακροπρόθεσμης αποθήκευσης αξίας, με αποτέλεσμα την λήψη τους από την κυκλοφορία προς χρήση στις συναλλαγές.

Μεταξύ κρυπτονομισμάτων όπως τα Ripple και Auroracoin, το μοντέλο διανομής δημιουργεί μια υπερεκτίμηση της πραγματικής κεφαλαιοποίησης, που απαιτείται για τη διατήρηση συναλλακτικής δραστηριότητας. Σύμφωνα με τα μοντέλα αυτά, ένα σημαντικό μέρος των κρυπτονομισμάτων παρακρατείται για το μέλλον της διανομής, αλλά εξακολουθεί να ληφθεί υπόψη και η τακτική του τύπου:

$$Τιμή\ ανά\ νόμισμα\ x\ Υπάρχοντα\ Νομίσματα = Κεφαλαιοποίηση$$

Ρίχνοντας μια πιο προσεκτική ματιά στο νόμισμα Ripple (XRP), θα δείτε ότι κατά την έναρξη, δημιουργήθηκαν κατ 'ανώτατο όριο 100 δισ. XRP, με 20 δισ. να διατηρούνται από τους ιδρυτές και τους επενδυτές, 25 δισ να παρακρατούνται από την εταιρία, και 55 δισ. που έχουν προγραμματιστεί να τεθούν σε απελευθέρωση συναρτήσει του χρόνου. Από τις 11 Απριλίου του 2014, περίπου 7.580 εκατομμύρια XRP έχουν διανεμηθεί. Με την εισαγωγή πρόσθετων XRP στη διανομή, η αξία του κάθε XRP θα μειωθεί καθώς θα υπάρχουν περισσότερα διαθέσιμα XRP που χρησιμοποιούνται εντός του δικτύου πληρωμών.

Το Auroracoin (AUR) υπέστη ένα παρόμοιο πρόβλημα, όπου το 50% της συνολικής AUR επρόκειτο να διανεμηθεί στους πολίτες της Ισλανδίας. Αυτό σήμαινε ότι αν και το 1% εξήχθη λίγο μετά την απελευθέρωσή, οι αντιπροσωπευτικές κεφαλαιοποιήσεις της αγοράς έφτασαν στο 98% των κερμάτων που δεν ήταν σε κυκλοφορία. Αυτό οδήγησε το AUR να αναπτυχθεί πέρα από την κεφαλαιοποίηση της αγοράς των Litecoin (LTC). Τελικά, η αρχική έκδοση των αχρησιμοποίητων κερμάτων στην Ισλανδία οδήγησε σε μείωση της τιμής του κάθε AUR πάνω από 45%, έναντι του Bitcoin η οποία παρέμεινε σταθερή κατά την ίδια περίοδο, γεγονός που αποδεικνύει τη μειωτική επίδραση.

Μια συχνά αναφερόμενη περίπτωση χρήσης για το Bitcoin είναι η δυναμική του ως μέσο αποθήκευσης αξίας, ειδικά σε χώρες όπως η Βενεζουέλα και η Αργεντινή, όπου ο ρυθμός πληθωρισμού υπολογίστηκε σε 56,2% και 20,8% για το 2013. Καθώς η υιοθέτηση του Bitcoin αρχίζει να αυξάνεται, οι καθημερινές συναλλαγές με Bitcoin φυσικά, θα αρχίσουν να αυξάνονται. Η επίδραση στη ζήτηση θα αλλάξει με την αυξημένη χρήση του δικτύου πληρωμών, ενώ η επίδραση στην προσφορά θα αλλάξει με την αυξημένη χρήση του Bitcoin εκφρασμένης σε αποταμιεύσεις και επενδύσεις.

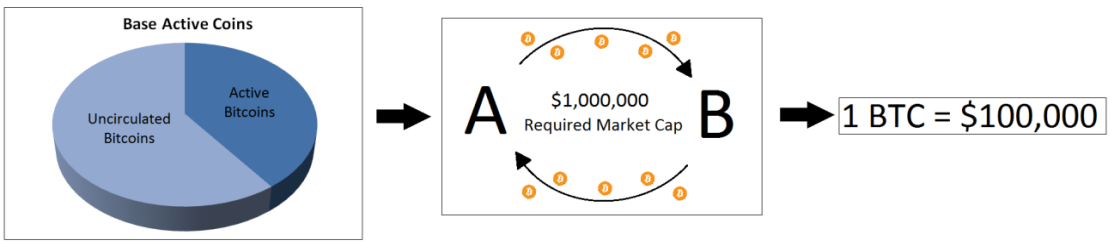
Ψάχνοντας για άλλα παραδείγματα της αλλαγής της προσφοράς, η δεύτερη αγορά του Bitcoin Investment Trust είναι ένα παράδειγμα μιας περίπτωσης χρήσης που θα μειώσει τον αριθμό των ενεργών κερμάτων. Καθώς αυξάνουν τις εκμεταλλεύσεις τους, ο αριθμός των bitcoins σε κυκλοφορία για συναλλακτική χρήση μειώνεται. Το ίδιο ισχύει και για τα hedge funds και τους θεσμικούς κατόχους. Μακροχρόνια, καθώς το θεσμικό ενδιαφέρον αυξάνεται το και τα funds αρχίζουν να αγοράζουν

bitcoins για επενδυτικά οχήματα, η εγγενής αξία φυσικά, θα αυξηθεί λόγω της μείωσης των ενεργών κερμάτων. Ωστόσο, εάν τα κατασχεθέντα νομίσματα χρησιμοποιούνται κυρίως ως αποταμίευση όταν κατάσχεται, δεν θα υπάρξει καμία επίπτωση στην εγγενή αξία. Ομοίως, οι πωλήσεις από το ένα ίδρυμα στο άλλο δεν θα έχουν ευρείας κλίμακας επιπτώσεις στην εγγενή αξία. Μόνο όταν αυτές οι εκμεταλλεύσεις πωλούνται στο κοινό, η δραστική καταμέτρηση των κερμάτων θα αυξηθεί, μειώνοντας την εγγενή αξία λόγω της αραίωσης.

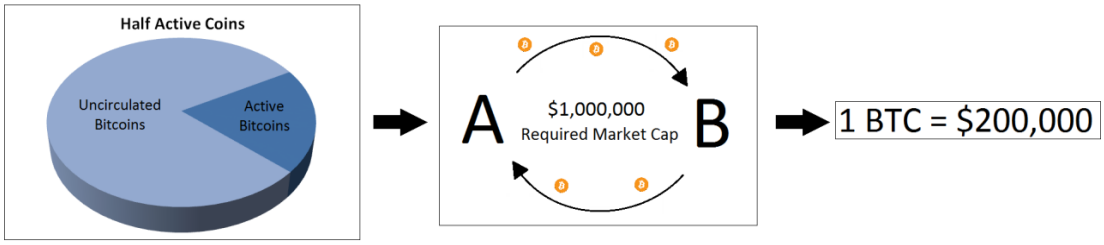
Τέλος, οι αυξήσεις των χαμένων bitcoins θα αυξάνουν πάντα την εγγενή αξία, δεδομένου ότι αποσύρονται μόνιμα από την κυκλοφορία προς χρήση στις συναλλαγές. Αυτό περιλαμβάνει την απώλεια των ιδιωτικών κλειδιών και οποιαδήποτε χρήση συστημάτων proof-of-burn, όπου τα bitcoins αποστέλλονται σε δημόσιες διευθύνσεις, χωρίς ένα γνωστό ιδιωτικό κλειδί.

Παράδειγμα προσφοράς

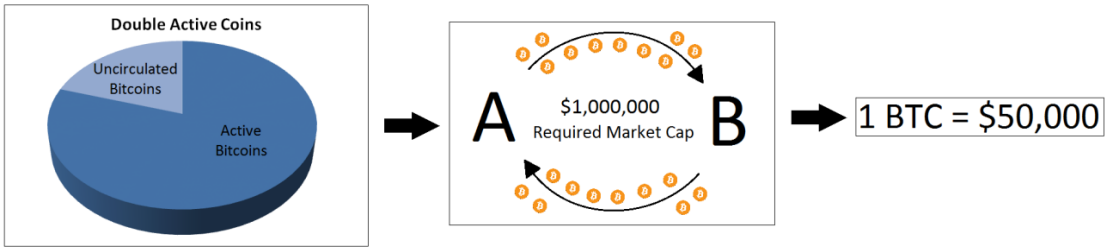
Εάν υποθέσουμε ότι υπάρχουν 10 BTC ως ενεργά νομίσματα και η απαιτούμενη κεφαλαιοποίηση για να καλυφθεί η συναλλαγματική δραστηριότητα ανέρχεται στο $1 εκατ., τότε 1 BTC = $ 100.000



Εάν 5 από αυτά τα ενεργά νομίσματα αποσυρθούν από την κυκλοφορία για την μακροχρόνια αποθήκευση αξίας, τότε μένουν 5 ενεργά νομίσματα για να καλύψουν την απαιτούμενη κεφαλαιοποίηση, ως εκ τούτου 1 BTC = $ 200.000



Εάν στην συνέχεια ένας μεγάλος οργανισμός αποφασίσει να πουλήσει 15 BTC στην αγορά, ο αριθμός των ενεργών νομισμάτων θα τετραπλασιαστεί και έτσι 1 BTC = $ 50.000



Μια μέθοδος υπολογισμού των ενεργών νομισμάτων είναι η δημιουργία παραδοχών με βάση την ηλικία των νομισμάτων. Για παράδειγμα, μπορείτε να υποθέσετε ότι τα κέρματα που δεν έχουν αλλάξει διευθύνσεις στα τελευταία δύο χρόνια έχουν χαθεί ή χρησιμοποιούνται ως μια μακροπρόθεσμη αποθήκη αξίας. Αυτά τα ανενεργά κέρματα θα πρέπει να αφαιρεθούν από την τρέχουσα συνολική προσφορά των κερμάτων για να μετρηθούν τα ενεργά νομίσματα.

Ωστόσο, ο υπολογισμός του ακριβούς αριθμού των ενεργών νομισμάτων είναι δύσκολος λόγω της φύσης του αρχικού πρωτοκόλλου Bitcoin, όπου εταιρείες όπως η Coinbase έχουν την επιμέλεια των bitcoins και έχουν ανοικτές συναλλαγές blockchain μεταξύ λογαριασμών. Ενώ μπορούν να συμβούν συναλλαγές, δεν θα εμφανίζονται στο blockchain. Κατά συνέπεια, αυτό θα σήμαινε ότι ένα ενιαίο πορτοφόλι μπορεί να έχει ανενεργά νομίσματα που εξακολουθούν να χρησιμοποιούνται για τις συναλλαγές και διαφορετικά θα θεωρούνται δραστικές.

Μακροπρόθεσμα, η blockchain μπορεί να αναλυθεί για να καταλάβουμε ποια πορτοφόλια έχουν χαθεί με πολύ εκτεταμένες περιόδους αδράνειας. Επίσης, τα στατιστικά στοιχεία της βιομηχανίας μπορεί να χρησιμοποιηθούν για την εκτίμηση

των θεσμικών εκμεταλλεύσεων και την προσωπική αποταμίευση ως ποσοστό επί του των νομισμάτων.

Η κεφαλαιοποίηση, τα ενεργά νομίσματα και η συναλλαγματική αξία για τα κρυπτονομίσματα δίνονται στον ακόλουθο πίνακα (στοιχεία Οκτωβρίου 2015):

Πίνακας 2. Στοιχεία κεφαλαιοποίησης για κρυπτονομίσματα (Πηγή: coinmarketcap.com)

Currency	**Symbol**	**Market Cap. ($)**	**Price ($)**	**Active Coins**
Auroracoin	AUR	113831	0.0155206299	7334174
Bitcoin	BTC	3910389068	265.1691009051	14746775
BlackCoin	BC, BLK	1825447	0.0243265897	75039166
Dash	DASH	13829801	2.3388177115	5913159
Dogecoin	DOGE	11969056	0.000117944	101480840780
DigitalNote	XDN	814357	0.0001189119	6848404243
Ethereum	ETH	33347999	0.4500727549	74094685
Litecoin	LTC	131240857	3.0652321471	42815960
Mastercoin	MSC	1623205	2.9601353138	548355
MazaCoin	MZC	45752	5.56838154367289E-005	821639100
Monero	XMR	3755518	0.3850679062	9752872
Namecoin	NMC	4533552	0.3567198049	12709000
Nxt	NXT	6852920	0.0068529399	999997096
Peercoin	PPC	8203255	0.3612678394	22706851
Emercoin	EMC	1053999	0.029021909	36317356
PotCoin	POT	154239	0.0007290053	211574598

Primecoin	XPM	706575	0.059036156	11968513
Ripple	XRP[32]	154699921	0.00466579	33156211683
Titcoin	TIT	15224	0.000419304	36307790

Επομένως η αξία κάθε νομίσματος (η συναλλαγματική αξία σε $) υπολογίζεται με βάση τον ακόλουθο τύπο:

$$Αξία = \frac{Συνολική\ Δαπάνη}{Ταχύτητα\ x\ Ενεργά\ νομίσματα}$$

Εφαρμόζοντας τον παραπάνω τύπο προκύπτουν οι ακόλουθοι πίνακες.

Πίνακας 3. Μεταβολή USD/coin βάση της ταχύτητας και του % ανενεργών νομισμάτων (Πηγή: Συγγραφέας) – Ανενεργά νομίσματα 30%

			Long term Savings – 30%			
			Velocity (coins)			
Currency	**Active Coins**	**Volume $ (24h)**	**10**	**20**	**50**	**100**
Auroracoin	7334174	172	0.00122	0.00061	0.00024	0.00012
Bitcoin	14746775	28486100	100.72	50.36	20.14	10.07
BlackCoin	75039166	6267	0.00435	0.00218	0.00087	0.00044
Dash	5913159	60018	0.52925	0.26462	0.10585	0.05292
Dogecoin	101480840780	37128	0.00002	0.00001	0.000004	0.000002
DigitalNote	6848404243	3736	0.00003	0.00001	0.00001	0.00000
Ethereum	74094685	610317	0.42950	0.21475	0.08590	0.04295
Litecoin	42815960	959500	1.16851	0.58426	0.23370	0.11685
Mastercoin	548355	217	0.02063	0.01032	0.00413	0.00206

MazaCoin	821639100	177	0.00001	0.00001	0.000002	0.000001
Monero	9752872	31800	0.17002	0.08501	0.03400	0.01700
Namecoin	12709000	10436	0.04282	0.02141	0.00856	0.00428
Nxt	999997096	36828	0.00192	0.00096	0.00038	0.00019
Peercoin	22706851	14938	0.03430	0.01715	0.00686	0.00343
Emercoin	36317356	352	0.00051	0.00025	0.00010	0.00005
PotCoin	211574598	231	0.00006	0.00003	0.00001	0.00001
Primecoin	11968513	5768	0.02513	0.01256	0.00503	0.00251
Ripple	33156211683	449811	0.00071	0.00035	0.00014	0.00007
Titcoin	36307790	88	0.00013	0.00006	0.00003	0.00001

Πίνακας 4. Μεταβολή USD/coin βάση της ταχύτητας και του % ανενεργών νομισμάτων (Πηγή: Συγγραφέας) – Ανενεργά νομίσματα 50%

			Long term Savings –50%			
			Velocity (coins)			
Currency	**Active Coins**	**Volume $ (24h)**	**10**	**20**	**50**	**100**
Auroracoin	7334174	172	0.00171	0.00086	0.00034	0.00017
Bitcoin	14746775	28486100	141.01	70.51	28.20	14.10
BlackCoin	75039166	6267	0.00610	0.00305	0.00122	0.00061
Dash	5913159	60018	0.74094	0.37047	0.14819	0.07409
Dogecoin	101480840780	37128	0.00003	0.00001	0.00001	0.000003
DigitalNote	6848404243	3736	0.00004	0.00002	0.00001	0.000004

Ethereum	74094685	610317	0.60130	0.30065	0.12026	0.06013
Litecoin	42815960	959500	1.63592	0.81796	0.32718	0.16359
Mastercoin	548355	217	0.02889	0.01444	0.00578	0.00289
MazaCoin	821639100	177	0.00002	0.00001	0.000003	0.000002
Monero	9752872	31800	0.23802	0.11901	0.04760	0.02380
Namecoin	12709000	10436	0.05994	0.02997	0.01199	0.00599
Nxt	999997096	36828	0.00269	0.00134	0.00054	0.00027
Peercoin	22706851	14938	0.04802	0.02401	0.00960	0.00480
Emercoin	36317356	352	0.00071	0.00035	0.00014	0.00007
PotCoin	211574598	231	0.00008	0.00004	0.00002	0.00001
Primecoin	11968513	5768	0.03518	0.01759	0.00704	0.00352
Ripple	33156211683	449811	0.00099	0.00050	0.00020	0.00010
Titcoin	36307790	88	0.00018	0.00009	0.00004	0.00002

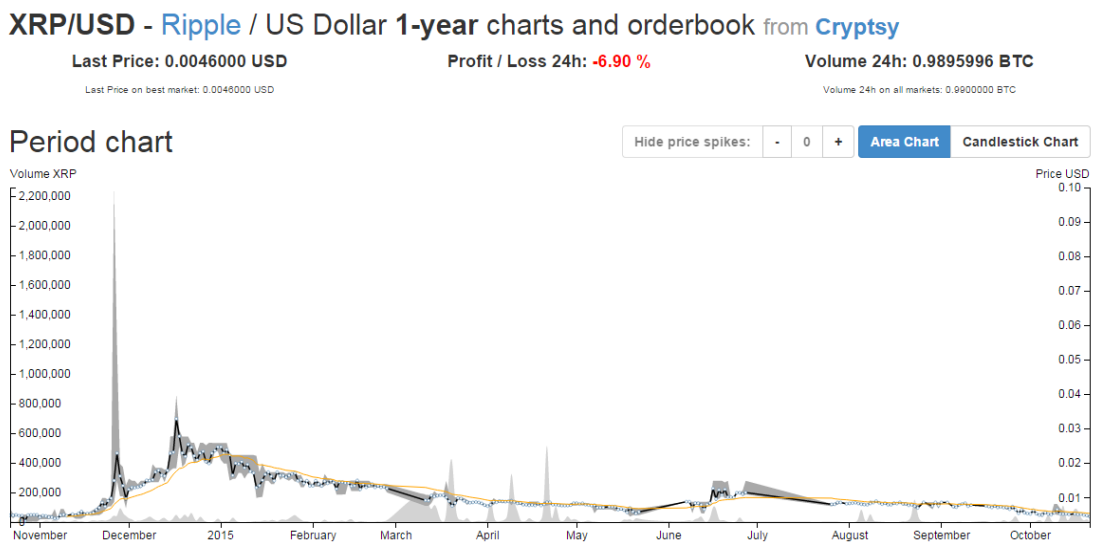
Στη συνέχεια δίνονται σε διαγράμματα οι μεταβολές των ισοτιμιών διαφόρων κρυπτονομισμάτων για την περίοδο του τελευταίου έτους. Στις εικόνες 7 και 8 παρουσιάζεται η διακύμανση για το Bitcoin τις τελευταίες 5 μέρες και τον τελευταίο χρόνο, ενώ στη συνέχεια, στις εικόνες 9-12 δίνονται οι διακυμάνσεις για τα νομίσματα Litecoin, Nxt, Ripple, Dogecoin.

Εικόνα 8. Μεταβολή της τιμής BTC/USD την περίοδο 17/10-21/10/2015 (cryptocoincharts.info)

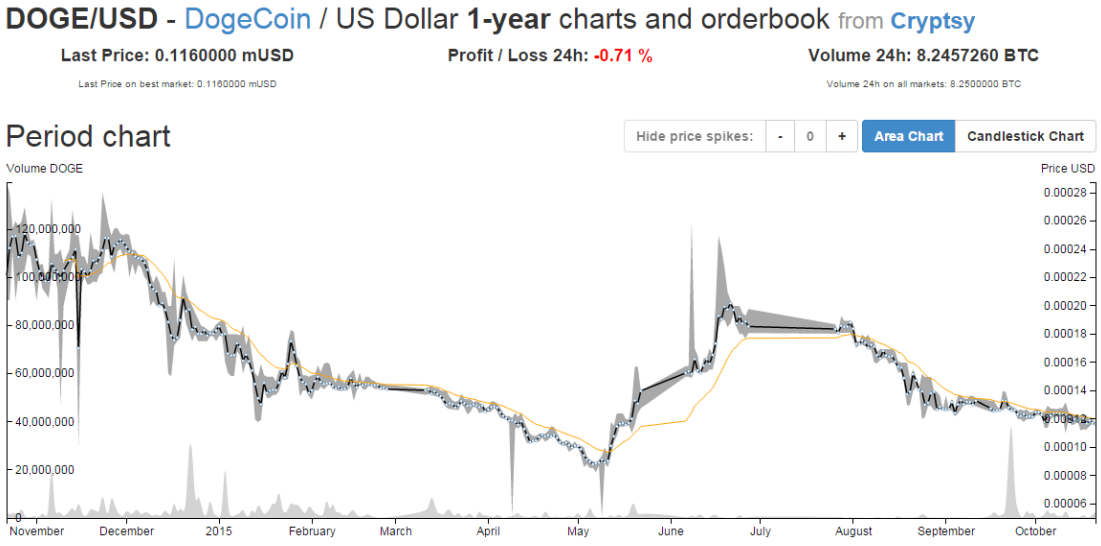
Εικόνα 9. Ετήσια μεταβολή της τιμής BTC/USD την περίοδο 11/2014-10/2015 στο Bitstamp (cryptocoincharts.info).

Εικόνα 10. Ετήσια μεταβολή της τιμής LTC/USD την περίοδο 11/2014-10/2015 στο Bitstamp (cryptocoincharts.info).

Εικόνα 11. Ετήσια μεταβολή της τιμής NXT/USD την περίοδο 11/2014-10/2015 στο Bitstamp (cryptocoincharts.info).



Εικόνα 12. Ετήσια μεταβολή της τιμής XRP/USD την περίοδο 11/2014-10/2015 στο Bitstamp (cryptocoincharts.info).



Εικόνα 13. Ετήσια μεταβολή της τιμής DOGE/USD την περίοδο 11/2014-10/2015 στο Bitstamp (cryptocoincharts.info).

4 ΜΕΘΟΔΟΛΟΓΙΑ ΑΞΙΟΛΟΓΗΣΗΣ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ

Το πρόβλημα που έχω να αντιμετωπίσω είναι αρκετά δύσκολο στην κατανόηση του, καθώς και στην κατάληξη σε μια απόφαση. Δεν υπάρχει κάποια μεθοδολογία για τον τρόπο που θα πρέπει να αξιολογείται ένα κρυπτονόμισμα, πόσο μάλλον για τα κριτήρια που θα παίξουν ρόλο στη σύγκριση αυτών μεταξύ τους και στην κατάληξη μιας σχέσης υπεροχής. Με τη βοήθεια των 2 λογισμικών, διευκρινίζοντας τα κριτήρια που θα παίξουν ρόλο στη σύγκριση, θα είμαι σε θέση να βρώ λύση στο πρόβλημα που αντιμετωπίζουμε.

4.1 ΚΡΙΤΗΡΙΑ ΑΞΙΟΛΟΓΗΣΗΣ

4.1.1 Ανασκόπηση βιβλιογραφίας

Ο Gourov (2014), ανέλυσε την εγγενή αξία των κρυπτονομισμάτων και πρότεινε τις μεταβλητές που καθορίζουν την εγγενή αξία κάθε κρυτπονομίσματος ως εξής:

- Ταχύτητα
- Κεφαλαιοποίηση
- Ζήτηση
- Προσφορά

Με βάση τις τιμές των παραπάνω μεταβλητών και την χρήση των κατάλληλων εξισώσεων, όπως παρουσιάζονται στην παράγραφο 3.3, μπορεί να υπολογιστεί η εγγενής αξία κάθε κρυπτονομίσματος.

Οι Badev & Chen (2014) προσπάθησαν να παρέχουν τεχνικά στοιχεία ώστε να γίνει κατανοητή η λειτουργία των κρυπτονομισμάτων και κατέγραψαν τις μεταβλητές που σχετίζονται με τον βαθμό χρησιμοποίησης και τη χρηστικότητα των κρυπτονομισμάτων. Η εμπειρική τους ανάλυση βασίζεται σε δημόσια διαθέσιμα δεδομένα συναλλαγών. Εξετάζουν τις διάφορες μορφές χρησιμοποίησης των κρυτπονομισμάτων και βρίσκουν ότι λιγότερο από 50% των διαθέσιμων

κρυπτονομισμάτων που βρίσκονται σε κυκλοφορία, πραγματικά χρησιμοποιούνται σε συναλλαγές. Οι μισές από αυτές τις συναλλαγές, αντιστοιχούν σε λιγότερο από 1.000 δολάρια και σχετίζονται με τον τζόγο και τα ηλεκτρονικά τυχερά παιχνίδια. Οι συναλλαγές μεγαλύτερου όγκου κρυπτονομισμάτων (πάνω από 40.000 δολάρια), είναι πολύ σπανιότερες και δεν αφορούν πληρωμές για αγαθά και υπηρεσίες. Για την ανάλυση χρησιμοποιούνται οι παρακάτω μεταβλητές:

- Όγκος συναλλαγών ανά ημέρα (πλήθος κρυπτονομισμάτων)
- Αξία συναλλαγών ανά ημέρα σε USD
- Μέση ημερήσια αξία σε USD
- Ταχύτητα
- Δείκτης συναλλάγματος USD/BTC

Ο Farell (2015) υποστηρίζει ότι η αγορά των κρυπτονομισμάτων έχει εξελιχθεί ασταθώς και με πρωτοφανή ταχύτητα κατά τη διάρκεια σύντομης ζωής της. Από την κυκλοφορία του πρωτοπόρου Bitcoin τον Ιανουάριο του 2009, έχουν αναπτυχθεί περισσότερα από 550 κρυπτονομίσματα, η πλειονότητα των οποίων είχε περιορισμένη επιτυχία. Στη συνέχεια υποστηρίζει ότι η ερευνητική δραστηριότητα στο πεδίο των κρυπτονομισμάτων εξακολουθεί να σπανίζει με την πλειοψηφία της να επικεντρώνεται μεμονωμένα στο Bitcoin αντί να παρέχει πιο διαφοροποιημένη εξάπλωση στα διάφορα κρυπτονομίσματα, συμπεριλαμβανομένων των νέων κερμάτων, της τεχνολογικής εξέλιξης, και της ενίσχυσης της κυβερνητικής ρύθμισης των αγορών. Αν και η ρευστότητα του κλάδου, ασφαλώς, αποτελεί πρόκληση για την έρευνα, μια διεξοδική αξιολόγηση του κλάδου των κρυπτονομισμάτων είναι απαραίτητη.

Ο Farell (2015) επιδιώκει να παρέχει μια συνοπτική αλλά περιεκτική ανάλυση του κλάδου των κρυπτονομισμάτων με ιδιαίτερη ανάλυση του Bitcoin, που αποτελεί το πρώτο αποκεντρωμένο κρυπτονόμισμα. Ιδιαίτερη προσοχή δίνεται στην εξέταση των θεωρητικών οικονομικών διαφορών μεταξύ των σημερινών νομισμάτων.

Αρχικά ο Farell (2015) παρέχει μια επισκόπηση της βιομηχανίας και μια σε βάθος οικονομική ανάλυση που σχετίζεται με τα κρυπτονομίσματα, τη στεγανοποίηση των σημαντικών νομισμάτων από τους μηχανισμούς του πρωτοκόλλου ασφάλειας του δικτύου, και τις μακροπρόθεσμες επιπτώσεις που συνεπάγονται τα παραπάνω. Δίνεται ιδιαίτερη προσοχή στο πρωτόκολλο ασφάλειας του δικτύου. Παρουσιάζονται οι μηχανισμοί απόδειξης εργασίας (Pow), που χρησιμοποιείται στο πρωτόκολλο Bitcoin και διάφορα altcoins, ο μηχανισμός απόδειξης της συμμετοχής (PoS) που εφαρμόστηκε για πρώτη φορά από Peercoin το 2011 και βασίζεται σε ένα μηχανισμό λιγότερο ενεργοβόρας ασφάλειας σε σύγκριση με τον Pow. Επίσης παρουσιάζονται μηχανισμός Pow / POS (υβριδικός) και ο μηχανισμός συνέναισης.

Ο Farell (2015) παρουσιάζει τα αποτελέσματα μιας συστηματικής ανασκόπησης των 21 κρυπτονομισμάτων και παρέχει μια επισκόπηση των παραγόντων που επηρεάζουν την ανάπτυξη της βιομηχανίας, εστιάζοντας σε μεγάλο βαθμό στο κανονιστικό περιβάλλον. Τέλος, αναδεικνύονται η δημόσια αντίληψη και η αποδοχή των κρυπτονομισμάτων ως ένα σύστημα πληρωμών στο σημερινό περιβάλλον λιανικής πώλησης. Στην ανάλυση συμμετέχουν τα κρυπτονομίσματα που έχουν κεφαλαιοποίηση τουλάχιστον 1 εκατομμύριο δολάρια τον Απρίλιο του 2015 και έχουν διανεμηθεί πριν από τον Ιανουάριο του 2015, ώστε να υπάρχει αρκετός χρόνος ωρίμανσης. Τα δεδομένα συλλέχθηκαν από τα εγχειρίδια των κρυπτονομισμάτων, και για όσα δεν υπήρχαν εγχειρίδια, ελήφθησαν δεδομένα από έγκυρες ιστοσελίδες. Τα βασικά κριτήρια αξιολόγησης, που χρησιμοποιούνται στην ανάλυση του Farell (2015) είναι τα εξής:

- Κεφαλαιοποίηση
- Αλγόριθμος hash
- Μηχανισμός ασφαλείας
- Προσφορά
- Αντιπληθωριστικότητα

4.1.2 Επιλογή κριτηρίων για την παρούσα ανάλυση

Στην παρούσα ανάλυση, θα χρησιμοποιηθούν τα κριτήρια που παρουσιάζονται στην ανάλυση του Farell (2015). Επιπλέον αυτών, θα χρησιμοποιηθούν τα στοιχεία της αξίας σε USD, της αλλαγής αυτής της τιμής και του όγκου των συναλλαγών το 24ωρο της 18^{ης} Δεκεμβρίου 2015. Επελέγησαν κρυπτονομίσματα που έχουν κεφαλαιοποίηση τουλάχιστον 1 εκατομμύριο δολάρια τον Δεκέμβριο του 2015 και έχουν διανεμηθεί πριν από τον Ιανουάριο του 2015, ώστε να υπάρχει αρκετός χρόνος ωρίμανσης. Πηγή δεδομένων είναι οι διαδικτυακοί τόποι coinmarketcap.com και cryptocoin.cc. Ο πίνακας με τα κρυπτονομίσματα και τις μεταβλητές αξιολόγησης παρουσιάζεται στο Παράρτημα Α.

Επειδή η βιομηχανία των κρυπτονομισμάτων είναι ακόμα στην αρχή της, και οι παράγοντες που την επηρεάζουν αλλάζουν σε καθημερινή βάση, υπάρχουν λίγες ολοκληρωμένες ή πλήρως ενημερωμένες ακαδημαϊκές πηγές σχετικά με το θέμα. Δεδομένου αυτού, τα περισσότερα στοιχεία που αναλύονται προέρχονται από τις επίσημες ιστοσελίδες των κρυπτονομισμάτων, οι άλλες διαδικτυακές πηγές που παρουσιάζουν πληροφορίες για όλα τα κρυπτονομίσματα.

4.2 ΜΕΘΟΔΟΣ ΑΞΙΟΛΟΓΗΣΗΣ

Από την βιβλιογραφική ανασκόπηση προέκυψε ότι ως τώρα οι αναλύσεις και αξιολογήσεις των κρυπτονομισμάτων γίνονται ποιοτικά, με θεωρητική ανάλυση των πρωτογενών δεδομένων. Αυτό οφείλεται στην μεγάλη μεταβλητότητα των χαρακτηριστικών των κρυπτονομισμάτων καθώς και την περιορισμένη ερευνητική δραστηριότητα στον τομέα, που προέρχεται από την έλλειψη κυβερνητικών ρυθμιστικών πλαισίων και ευρύτερης αποδοχής.

Στόχος της συγκεκριμένης ανάλυσης είναι η αξιολόγηση των κρυπτονομισμάτων με βάση τις μεταβλητές που επελέγησαν, με στόχο να εξαχθούν συμπεράσματα της συσχέτισης μεταξύ των μεταβλητών. Συγκεκριμένα επιλέγονται οι εξής μεταβλητές:

- Αλγόριθμος hash
- Μηχανισμός ασφαλείας
- Προσφορά
- Αντιπληθωριστικότητα
- Όγκος συναλλαγών
- Αλλαγή στην αξία
- Αντιπληθωρισμός
- Χρονολογία έκδοσης
- Κεφαλαιοποίηση σε $
- Αξία σε $

Η ανάλυση είναι πολυκριτηριακή, δηλαδή χρησιμοποιεί πολλές μεταβλητές και αξιολογεί την βαρύτητα της επίδρασης τους στις ανεξάρτητες μεταβλητές.

Για την επιλογή των λογισμικών έχουμε:

Η ανάλυση θα γίνει με 2 λογισμικά: το Weka καθως και το Virtual Promethee. Το Weka είναι μια πλατφόρμα εργασίας (workbench), η οποία περιέχει μια συλλογή από εργαλεία απεικόνισης και αλγορίθμων για την ανάλυση δεδομένων και την προγνωστική μοντελοποίηση, μαζί με γραφικά περιβάλλοντα χρήστη για εύκολη πρόσβαση σε αυτές τις λειτουργίες. Η αρχική μη-Java έκδοση του Weka ήταν ένα Tcl / Tk front-end μοντελοποίησης αλγορίθμων (ως επί το πλείστον από τρίτους) που εφαρμόστηκαν σε άλλες γλώσσες προγραμματισμού, καθώς και επιχειρήσεις κοινής ωφέλειας προεπεξεργασία των δεδομένων σε C, και ένα σύστημα που βασίζεται σε Makefile για πειράματα μηχανικής μάθησης. Αυτή η αρχική έκδοση είχε αρχικά σχεδιαστεί ως ένα εργαλείο για την ανάλυση των δεδομένων από γεωργικές περιοχές, αλλά η πιο πρόσφατη πλήρως το Java-based έκδοση (Weka 3), για την

οποία η ανάπτυξη ξεκίνησε το 1997, χρησιμοποιείται πλέον σε πολλά διαφορετικά προβλήματα, ιδίως για εκπαιδευτικούς σκοπούς και την έρευνα.

Τα πλεονεκτήματα του Weka είναι τα εξής:

- Η δωρεάν διάθεση υπό την GNU General Public License.
- Φορητότητα, δεδομένου ότι εφαρμόζεται πλήρως στη γλώσσα προγραμματισμού Java και ως εκ τούτου λειτουργεί σχεδόν σε κάθε σύγχρονη υπολογιστική πλατφόρμα.
- Μια ολοκληρωμένη συλλογή τεχνικών προεπεξεργασίας των δεδομένων και μοντελοποίησης.
- Ευκολία στη χρήση, λόγω γραφικής διεπαφής χρήστη.

Το Weka υποστηρίζει αρκετές τυπικές εργασίες εξόρυξης δεδομένων, πιο συγκεκριμένα, προεπεξεργασία δεδομένων, ομαδοποίηση, ταξινόμηση, οπισθοδρόμηση, οπτικοποίηση, και επιλογή χαρακτηριστικών. Όλες οι τεχνικές Weka στηρίζονται στην υπόθεση ότι τα δεδομένα είναι διαθέσιμα ως ένα απλό αρχείο ή σχέση, όπου κάθε σημείο δεδομένων περιγράφεται από ένα σταθερό αριθμό των χαρακτηριστικών των δεδομένων (συνήθως, αριθμητικά ή ονομαστικά χαρακτηριστικά, αλλά και ορισμένα άλλα είδη χαρακτηριστικών που υποστηρίζονται επίσης). Το Weka παρέχει πρόσβαση σε βάσεις δεδομένων SQL χρησιμοποιώντας την Java Database Connectivity και μπορεί να επεξεργαστεί το αποτέλεσμα που επιστρέφεται από ένα ερώτημα βάσης δεδομένων. Δεν είναι σε θέση για την υλοποίηση πολυ-σχεσιακής εξόρυξης δεδομένων, αλλά υπάρχει ξεχωριστό λογισμικό για τη μετατροπή μιας συλλογής συνδεδεμένων πινάκων της βάσης δεδομένων σε ένα ενιαίο πίνακα που είναι κατάλληλος για επεξεργασία χρησιμοποιώντας το Weka. Ένας άλλος σημαντικός τομέας που επί του παρόντος δεν καλύπτεται από τους αλγορίθμους που περιλαμβάνεται στην έκδοση του Weka είναι η μοντελοποίηση ακολουθίας.

Σχετικα με το virtual promethee:

Η μέθοδος PROMETHEE (Preference Ranking Organization METHod for Enrichment Evaluations) αναπτύχθηκε στα μέσα της δεκαετίας του ΄80 από τους Brans & Vincke [1985] και ανήκει στην κατηγορία των μεθόδων σχέσεων υπεροχής (outranking relations methods).

Σε αυτές η κατάταξη των εναλλακτικών σεναρίων είναι εφικτή μέσω των ανά ζεύγος συγκρίσεων των επιδόσεων των εναλλακτικών σεναρίων ως προς τα κριτήρια της ανάλυσης.

Η μέθοδος περιλαμβάνει διάφορες παραλλαγές για την αντιμετώπιση διαφορετικών προβληματικών απόφασης.

Αναλυτικότερα, ως PROMETHEE I παρέχει τη μερική (partial) κατάταξη των εναλλακτικών σεναρίων, ενώ ως PROMETHEE II την πλήρη (complete) κατάταξή τους [Brans & Vincke 1985, Brans et al. 1986].

Η PROMETHEE III επιτρέπει την προσέγγιση προβλημάτων σε στοχαστικό περιβάλλον απόφασης, ενώ η PROMETHEE IV την αντιμετώπιση προβλημάτων αξιολόγησης μεγάλου αριθμού εναλλακτικών σεναρίων. Επιπλέον, η μέθοδος παρέχει το πλαίσιο για την αντιμετώπιση προβλημάτων κατανομής πόρων (PROMETHEE V), τη διενέργεια αναλύσεων ευαισθησίας (PROMETHEE VI), καθώς και τη γραφική απεικόνιση του προβλήματος απόφασης (GAIA: Geometrical Analysis for Interactive Assistance).

Αναλυτικότερα για τη μεθοδο, εχουμε το εξης παραδειγμα:

Πολυκριτηριακή Ανάλυση: η Μέθοδος PROMETHEE II

Η οικογένεια μεθόδων PROMETHEE Η εφαρμογή της μεθόδου PROMETHEE ακολουθεί τα παρακάτω στάδια:

1. Οι εναλλακτικές επιλογές συγκρίνονται ανά ζεύγη και για κάθε κριτήριο. Η προτίμηση εκφράζεται από έναν αριθμό Π(α,b), μεταξύ του διαστήματος [0,1] (0 για απουσία προτίμησης ή παρουσία αδιαφορίας και 1 για 95 αυστηρή προτίμηση). Η

συνάρτηση που συνδέει τη διαφορά απόδοσης με την προτίμηση δύναται να καθοριστεί από τον λήπτη απόφασης και ονομάζεται γενικευμένο κριτήριο (Brans et al, 1986). Στις περισσότερες εφαρμογές έχει γραμμική μορφή. Περισσότερα για τη μορφή της συνάρτησης αυτής θα ακολουθήσουν παρακάτω.

2. Ένας πολυκριτηριακός Δείκτης Προτίμησης [π(α,b)] σχηματίζεται για κάθε ζεύγος δράσεων ως ο σταθμισμένος μέσος των αντίστοιχων προτιμήσεων που έχουν υπολογιστεί στο προηγούμενο στάδιο για κάθε κριτήριο. Ο δείκτης π(α,b) (στο διάστημα [0,1]) εκφράζει τη συνολική προτίμηση της δράσης α σε σχέση με τη b (λαμβάνοντας υπόψη το σύνολο των κριτηρίων αξιολόγησης).

Πιο συγκεκριμένα, η κατάταξη των εναλλακτικών επιλογών δύναται να επιτευχθεί σύμφωνα με:

• Το αδιαστατοποιημένο άθροισμα των δεικτών Π(α,i), δηλώνοντας την προτίμηση της δράσης α σε σχέση με τις υπόλοιπες. Η τιμή αυτή ονομάζεται ροή εκροής φ+ (α) και δηλώνει το πόσο καλή είναι η εναλλακτική αυτή δράση. Όσο μεγαλύτερη είναι η ροή εκροής για μία δράση, τόσο καλύτερη θεωρείται.

• Το αδιαστατοποιημένο άθροισμα των δεικτών Π(i,α), δηλώνοντας την προτίμηση όλων των άλλων εναλλακτικών επιλογών συγκρινόμενες με την α. Η τιμή αυτή ονομάζεται ροή εισροής φ- (α) και δηλώνει το πόσο υποδεέστερη εμφανίζεται η επιλογή α σε σχέση με της υπόλοιπες. Όσο μεγαλύτερη είναι η ροή εισροής της δράσης, τόσο χειρότερη θεωρείται.

Η μέθοδος PROMETHEE II

Το μεγαλύτερο πλεονέκτημά των μεθόδων PROMETHEE (Preference Ranking Organization METHod for Enrichment Evaluations) αποτελεί η ενοποίηση όλων των σύγχρονων απόψεων μοντελοποίησης της προτίμησης με έναν απλό τρόπο. Η

μέθοδος PROMETHEE II επιτρέπει την πλήρη κατάταξη των εναλλακτικών δράσεων, μέσω της χρησιμοποίησης της καθαρής ροής (διαφορά μεταξύ των ροών εκροής και εισροής). Πιο συγκεκριμένα, έστω ότι gj(α) είναι η απόδοση της δράσης α σύμφωνα με το κριτήριο j, τότε μπορούμε να υπολογίσουμε τη διαφορά των αποδόσεων των 96 εναλλακτικών α και b ως dj(α,b) = gj(α) – gj(b). Οι τιμές των κατωφλίων pi και qi ορίζονται της παρακάτω: pj[gj(α)], το Όριο Προτίμησης της τιμής του κριτηρίου gj για την δράση α qj[gj(α)], το Όριο Αδιαφορίας της τιμής του κριτηρίου gj για την δράση α

Ο δείκτης προτίμησης Πj(α,b) ∈ [0,1], που περιγράφει την ένταση της προτίμησης της δράσης α σε σχέση με την b σύμφωνα με το κριτήριο j, ορίζεται ως εξής:

Πj(α,b) = 0, όταν dj(α,b) ≤ qj[gj(b)] (1)

Πj(α,b)=1, όταν dj(α,b) ≥ pj[gi(b)] (2)

Πj(α,b)=(gj(α)-gj(b)-qj[vj(b)])/(pj[gj(b)]-qj[gj(b)]), (3)

όταν qj[gj(b)]<dj(α,b)

Ο Αποφασίζων καθορίζει τους βαθμούς βαρύτητας των κριτηρίων, σύμφωνα με την προτίμησή του, W=(w1, w2…wn), και ο συνολικός βαθμός υπεροχής σύμφωνα με όλα τα κριτήρια, υπολογίζεται από την παρακάτω σχέση:

$$\pi(\alpha,b)=\sum_j w_j\Pi_j(\alpha,b)\Big/\sum_j w_j$$

Στη συνέχεια υπολογίζονται οι θετικές και αρνητικές ροές, οι οποίες χρησιμοποιούνται για την κατασκευή της τελικής κατάταξης των εναλλακτικών:

$$\phi^+(\alpha)=\sum_{b\neq\alpha}\pi(\alpha,b)/(n-1),$$

$$\phi^-(\alpha)=\sum_{b\neq\alpha}\pi(b,\alpha)/(n-1),$$

Κατά την εφαρμογή της μεθόδου PROMETHEE II, η καθαρή ροή της κάθε δράσης δύναται να υπολογισθεί σύμφωνα με τη σχέση:

$$\varphi(\alpha) = \varphi^{+}(\alpha)\text{-}\varphi^{-}(\alpha)$$

ή αναλυτικότερα από την:

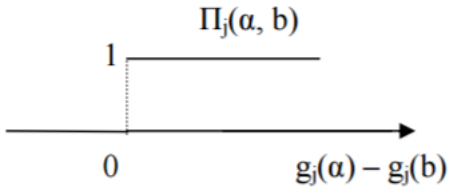
$$\phi(\alpha) = \sum_{j} \sum_{b \neq a} (w_j(\Pi_j(\alpha,b) - \Pi_j(b,\alpha))) / \left(\sum_{j} w_j(n-1) \right),$$

Η τιμή της καθαρής ροής της κάθε εναλλακτικής δράσης, χρησιμοποιείται για την εξαγωγή της τελικής κατάταξης των επιλογών.

Ο εκάστοτε Αποφασίζων, και σύμφωνα με τον τρόπο που η προτίμησή του μεταβάλλεται με την αύξηση της διαφοράς gj(α) – gj(b), θέτει για κάθε κριτήριο τη μορφή που έχει η συνάρτηση Πj (γενικευμένο κριτήριο). Οι παράμετροι που εκτιμούνται ερμηνεύονται απλά, μιας και αντιπροσωπεύουν όρια αδιαφορίας και προτίμησης. Συνήθως χρησιμοποιούνται έξι τύποι γενικευμένου κριτηρίου (Brans et al, 1986):

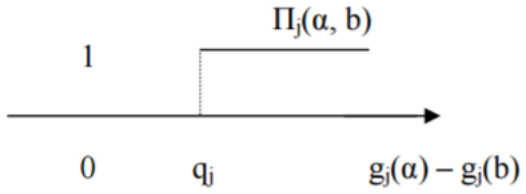
1η μορφή

Άμεση αυστηρή προτίμηση (κλασσικό κριτήριο). Δεν είναι απαραίτητος ο προσδιορισμός καμιάς παραμέτρου



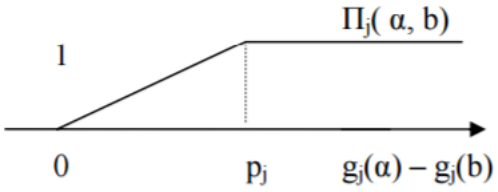
2η μορφή

Υπάρχει όριο αδιαφορίας που πρέπει να προσδιορισθεί



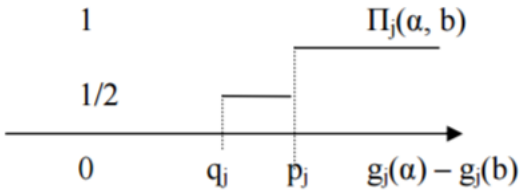
3η μορφή

Η προτίμηση αυξάνεται μέχρι το όριο προτίμησης που πρέπει να προσδιορισθεί



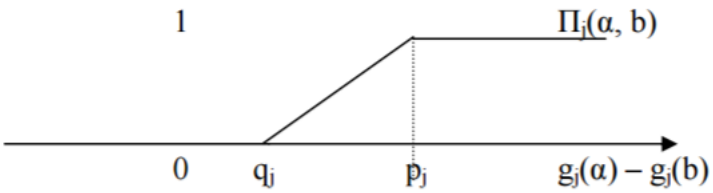
4η μορφή

Υπάρχει όριο αδιαφορίας και προτίμησης. Στο μεταξύ τους διάστημα η προτίμηση ισούται με το μέσο όρο τους



5η μορφή

Υπάρχουν όρια αδιαφορίας και προτίμησης. Στο διάστημα μεταξύ τους η προτίμηση αυξάνεται αναλογικά (η συνηθέστερη περίπτωση)



Από μαθηματικής άποψης, οι μορφές 1,2 και 3 είναι ειδικές περιπτώσεις της 5. Άλλες μορφές γενικευμένων κριτηρίων είναι δυνατόν να εισαχθούν, όμως γενικά αυτές οι έξι περιπτώσεις κρίνονται επαρκείς για την κάλυψη μεγάλου αριθμού πιθανών συμπεριφορών.

Το μεγαλύτερο πλεονέκτημα της μεθόδου PROMETHEE είναι το γεγονός πως ενοποιεί όλες τις σύγχρονες απόψεις μοντελοποίησης της προτίμησης με έναν απλό τρόπο. Ωστόσο, λείπει μία στιβαρή θεωρητική βάση που θα επέτρεπε την καλύτερη κατανόηση των υποθέσεων πάνω στις οποίες στηρίζεται

Ειδικότερα, η μέθοδος PROMETHEE που θα χρησιμοποιηθεί θα είναι η PROMETHEE II, η οποία παρέχει τη δυνατότητα μιας ολοκληρωμένης αξιολόγησης με βάση την τιμή της μεταβλητή Phi(Φ).[1] Η υπομέθοδος αυτή μας δίνει τόσο μεγαλύτερη τιμή Φ, όσο καλύτερη είναι η επιλογή στην οποία αντιστοιχείται η τιμή αυτή για τα επιλεγμένα και εκάστοτε σταθμισμένα κριτήρια.

4.3 ΚΩΔΙΚΟΠΟΙΗΣΗ ΔΕΔΟΜΕΝΩΝ

Τα πραγματικά δεδομένα που πρέπει να κωδικοποιηθούν για τα πρόβλημά μας είναι τα εξής:

1. **Αλγόριθμος hash(**αλγόριθμοι κατακερματισμού όπως αναφέρω στο κεφάλαιο 3.3)
2. **Μηχανισμός ασφάλειας**(όπως αναφέρω στο κεφάλαιο 3.2)
3. **Κεφαλαιοποίηση**
4. **Αξία του κρυπτονομίσματος βασισμένη στο δολλάριο**
5. **Προσφορά**(πλήθος νομισμάτων)
6. **Όγκος συναλλαγών στις 24 ώρες**
7. **Αλλαγή στην αξία**(μέσα στο 24ωρο)
8. **Αντιπληθωρισμός**

Για να γίνει η ανάλυση τα ποιοτικά δεδομένα του πίνακα θα πρέπει να κωδικοποιηθούν. Η κωδικοποίηση γίνεται ως εξής:

Αλγόριθμος hash	**Κωδικός**
SHA-256d	1
ECDSA	2
Scrypt	3
Cryptonight	4

X11	5
X13	6
1CC/2CC/TWN	7
N/A	8

Μηχανισμός ασφαλείας	**Κωδικός**
POW	1
CONSENSUS	2
POS	3
POW/POS	4
N/A	5

Αντιπληθωρισμός	**Κωδικός**
ΝΑΙ	1
ΟΧΙ	2
N/A	3

Ο πίνακας με τα κωδικοποιημένα δεδομένα, δίνεται στο Παράρτημα Β.

4.4 ΜΟΝΤΕΛΟΠΟΙΗΣΗ ΣΤΑ WEKA-PROMETHEE

Αρχικά ελέγξαμε τη βάση δεδομένων και επιβεβαιώσαμε ότι δεν υπάρχουν ελλιπή δεδομένη, ή δεδομένα που βρίσκονται εκτός του πεδίου ορισμού των μεταβλητών στις οποίες αντιστοιχούν, βάσει του ορισμού των μεταβλητών αυτών.

Η προπαρασκευή των δεδομένων λοιπόν σχετίζεται με την βελτίωση της απόδοσης των αλγορίθμων που θα χρησιμοποιήσουμε παρακάτω και έχει να κάνει με τη λειτουργία Attribute Selection (Επιλογή Χαρακτηριστικών).

Η επιλογή χαρακτηριστικών είναι μια διαδικασία με την οποία μπορούμε αυτόματα να κάνουμε αναζήτηση για το καλύτερο υποσύνολο χαρακτηριστικών γνωρισμάτων που χρησιμοποιούνται στη βάση δεδομένων. Η έννοια του «καλύτερου» είναι σχετική με το πρόβλημα που προσπαθούμε να λύσουμε, αλλά συνήθως σημαίνει υψηλότερη ακρίβεια.

Ένας χρήσιμος τρόπος για να σκεφτούμε το πρόβλημα της επιλογής χαρακτηριστικών είναι η αναζήτηση στο χώρο κατάστασης. Ο χώρος αναζήτησης είναι διακριτός και αποτελείται από όλους τους πιθανούς συνδυασμούς των χαρακτηριστικών που θα μπορούσαμε να επιλέξουμε από το σύνολο δεδομένων. Ο στόχος είναι να περιηγηθούμε μέσα από το χώρο αναζήτησης και να εντοπίσουμε τον καλύτερο συνδυασμό που βελτιώνει την απόδοση σε σχέση με την επιλογή των χαρακτηριστικών.

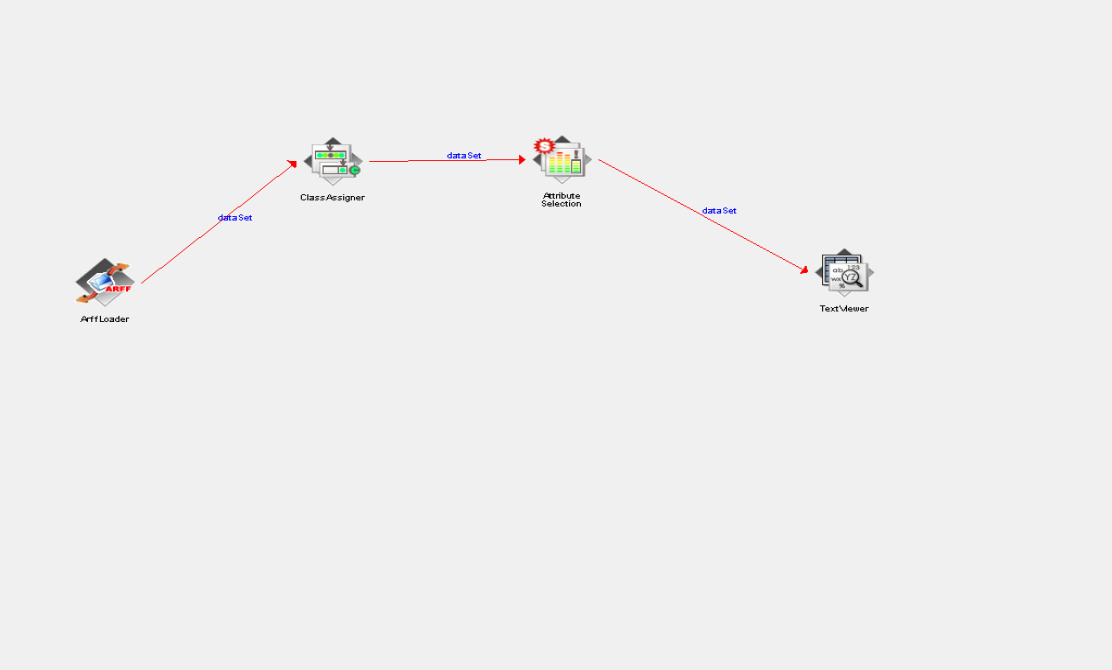
Τρία βασικά πλεονεκτήματα της εκτέλεσης επιλογής χαρακτηριστικών για τα δεδομένα είναι:

- Μείωση υπερπροσαρμογής: Λιγότερα πλεονάζοντα δεδομένα οδηγούν σε μικρότερη επιρροή του θορύβου στη λήψη αποφάσεων.
- Βελτίωση Ακρίβειας: Λιγότερα παραπλανητικά στοιχεία σημαίνουν βελτίωση στην ακρίβεια μοντελοποίησης.

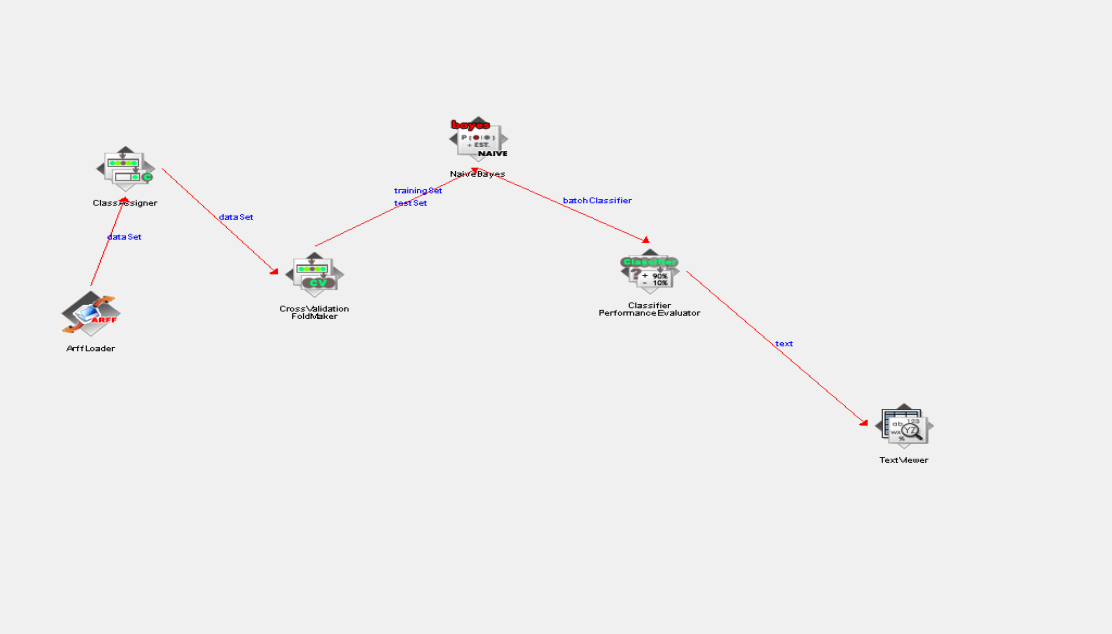
- Μείωση χρόνου εκπαίδευσης: Λιγότερα δεδομένα σημαίνει ότι οι αλγόριθμοι εκπαιδεύονται γρηγορότερα.

Στη συνέχεια, στο Knowledge Flow Layout του προγράμματος Weka δημιουργούμε τρία αρχεία. Το πρώτο αφορά το Attribute Selection, το δεύτερο το Classification και το τρίτο το Prediction.

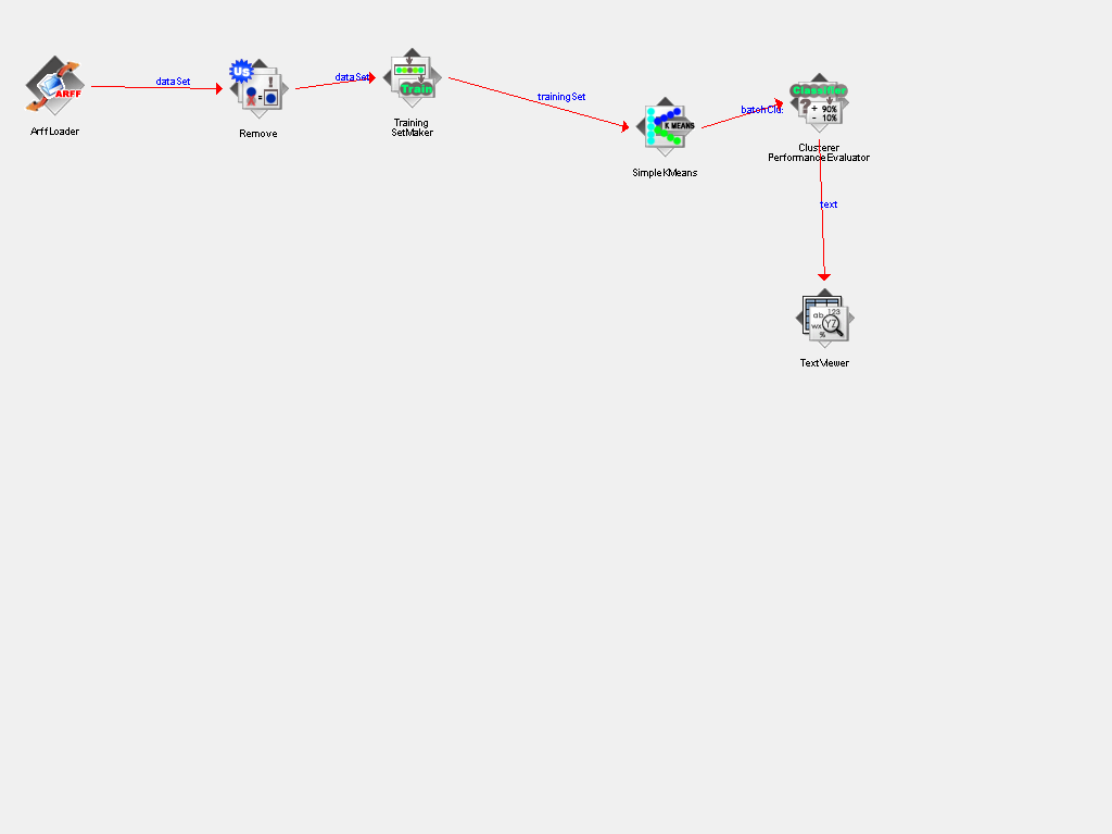
Η επιλογή χαρακτηριστικών γίνεται για έναν classifier Naivebayes. Η διαδικασία της επιλογής χαρακτηριστικών φαίνεται στην Εικόνα 14.



Εικόνα 14 Μοντέλο επιλογής χαρακτηριστικών στο Weka



Εικόνα 15 Μοντέλο κατηγοριοποίησης στο Weka



Εικόνα 16 Μοντέλο ομαδοποίησης στο Weka

Για την είσοδο των δεδομένων μας στα μοντέλα που δημιουργήσαμε, χρησιμοποιούμε το module arffloader. Αυτό σημαίνει ότι τα δεδομένα μας πρέπει να τα εισάγουμε με ένα αρχείο τύπου arff που έχει την εξής δομή:

@relation cryptocoins

@attribute release numeric

@attribute hash {SHA-256d, ECDSA, Scrypt, X13, CryptoNight, X11, 1CC/2CC/TWN, N/A}

@attribute security {POW, POS, POW/POS, Consensus, N/A}

@attribute capitalization numeric

@attribute value numeric

@attribute supply numeric

@attribute volume numeric

@attribute changenumeric

@attribute deflation {YES, NO, N/A}

@data

…….

…

.

Το Weka ‘πραγματοποιεί’ εξόρυξη δεδομένων. Στην προκειμένη περίπτωση, ενδιαφερόμαστε για μια απλή συσταδοποίηση(clustering) των «πλειάδων» των

δεδομένων, δηλαδή για κάθε δεκάδα τιμών των μεταβλητών. Η μεταβλητή «κλάσης», όπως λέγεται σε αυτό το συγκείμενο, είναι η μεταβλητή του ίδιου του κρυπτονομίσματος(Litecoin). Είναι βεβαίως γνωστό ότι στην μέθοδο της συσταδοποίησης δεν υπάρχει μεταχείριση τέτοιου τύπου μεταβλητής, αλλά όλες χρησιμοποιούνται εξίσου για τον υπολογισμό των clusters.

Η ανάλυση συστάδων διευθετεί ένα σύνολο μεταβλητών ή παρατηρήσεων σε συγκεκριμένες ομάδες οι οποίες διαθέτουν κατ΄ ιδίαν κοινά χαρακτηριστικά, ευκρινώς διαφοροποιημένα από εκείνα των άλλων ομάδων. Η απόσταση των στοιχείων στο χώρο μετρείται με τους ειδικούς συντελεστές ομοιότητας και η σύνδεσή τους προς δημιουργία συστάδων με ομοειδές περιεχόμενο τιμών εκάστη πραγματοποιείται με ειδικές μεθόδους διασύνδεσης, ιεραρχικού ή μη χαρακτήρα. Περιγράφονται διεξοδικά οι τόποι εκτίμησης των αποστάσεων των στοιχείων και η συνένωσή τους σε μικρές συστάδες με ολοένα αυξανόμενο αριθμό στοιχείων μέχρι την ολοκλήρωσή τους σε μία τελική σύνθεση συστάδας. Επισημαίνονται επίσης τα κριτήρια της ορθής επιλογής του αριθμούς των συστάδων και η αποτελεσματικότητά της επιλεγμένης μεθόδου. Η ανάλυση συστάδων δρα επικουρικά με τις αναλύσεις κοινών παραγόντων και κύριων συνιστωσών, και η μελέτη περίπτωσης της ανάλυσης συστάδων αποτελεί επέκταση και συγκερασμό των παραπάνω αναλύσεων.

Η μελέτη ταξιδόμησης των στοιχείων, όπως ήδη διαφαίνεται, απαιτεί επιτακτικά τη συνδυαστική γνώση των ανα- λύσεων κοινών παραγόντων και κύριων συνιστωσών και επιπρόσθετα την ανάλυση διακύμανσης μεταξύ των ομάδων για την στατιστική εκτίμηση των διαφορετικών δράσεων των μεταβλητών μεταξύ των ομάδων.

Η ανάλυση συστάδων ή ταξιδόμησης των στοιχείων (Cluster analysis) εφαρμόζεται με τέτοιο τρόπο ώστε να εντάσσονται σε ίδιες συστάδες (ομάδες) στοιχεία (παρατηρήσεις) περισσότερα όμοια μεταξύ τους παρά σε οποιεσ- δήποτε άλλες (Aldenderfer & Blashfield, 1984, Everitt, 1993). Αυτό επιτυγχάνεται με την

επισταμένη επιλογή και διευθέτηση των στοιχείων σε ομάδες παρατηρήσεων με συγγενικά χαρακτηριστικά και με τις ακόλουθες ιδιότητες:

- Κάθε ομάδα διαθέτει ομοειδή σύσταση σε σχέση με κάποια χαρακτηριστικά, δηλαδή οι παρατηρήσεις σε αυτές έχουν τιμές σχεδόν όμοιες μεταξύ τους
- Κάθε ομάδα οφείλει να διαφέρει από τις υπόλοιπες ως προς ίδια χαρακτηριστικά, δηλαδή οι τιμές μιας ομάδας θα πρέπει να διαφέρουν σε μέγεθος κλίμακας από τις τιμές άλλων ομάδων.

Η ανάλυση συστάδων πραγματοποιείται με τη χρήση πολυάριθμων αλγορίθμων με τελείως διαφορετικές ιδιότητες μεταξύ τους ως προς τον τρόπο λειτουργίας και το βαθμό απόδοσής τους και επεξεργάζεται συστάδες οι οποίες εννοιολογικά σημαίνουν αποστάσεις μεταξύ των στοιχείων, πυκνές περιοχές με σημεία στο χώρο, ειδικές κατανομές στοιχείων κτλ. Η διαλογή των στοιχείων στις ομάδες γίνεται με τέτοιο τρόπο ώστε η σύνδεση μεταξύ δύο στοιχείων να μεγιστοποιείται στην περίπτωση που ανήκουν στην ίδια ομάδα, ειδάλλως να ελαχιστοποιείται. Με τον τρόπο αυτόν η ανάλυση συστάδων προάγει την ανεύρεση ειδικών σχέσεων μεταξύ των στοιχείων, χωρίς να παρέχει ανάλογες εξηγήσεις ή ερμηνείες, χωρίς δηλαδή να εξηγεί την ύπαρξη σχέσεων. Ένα άλλο χαρακτηρι- στικό της μεθόδου είναι ότι δεν απαιτεί καμία a priori υπόθεση για να ξεκινήσει τη διερευνητική διαδικασία στα στοιχεία γι’ αυτό και δεν απαιτείται η εφαρμογή στατιστικών ελέγχων για τη σημαντικότητα των αποτελεσμάτων που εξάγονται.

Πέραν της προσεκτικής επιλογής ενός αλγόριθμου ακολουθεί και η ρύθμιση ορισμένων παραμέτρων, όπως ο τύπος μέτρησης των αποστάσεων, κάποιο αριθμητικό όριο στοιχείων που πρέπει να έχει μία συστάδα ή ο επιτρεπτός αριθμός των συστάδων τελικής αποδοχής. Επομένως, η ανάλυση ταξιδόμησης δεν αναμένεται να τελεσφορεί ως μία αυτόματη διαδικασία αλλά ως μία επαναληπτική διαδραστική διεργασία βελτιστοποίησης της ταυτοποίησης των στοιχείων με την εφαρμογή δοκιμασίας και αποτυχίας, η οποία ενδέχεται να απαιτήσει και επαναρρύθμιση των αρχικών παραμέτρων.

Η συσταδοποίηση συχνά επιχειρείται και ως ενδιάμεσο στάδιο μεταξύ της παραγοντικής ανάλυσης και της διακριτικής. Αρχικά οργανώνεται παραγοντική ανάλυση για να περιορίσει τις διαστάσεις των δεδομένων και κατ' επέκταση των μεταβλητών, διευκολύνοντας ποιοτικά την εκτέλεση της συσταδοποίησης αφού συμβάλλει επιπρόσθετα και στη μείωση της πολυσυγγραμικότητας των μεταβλητών. Ακολουθεί η ταυτοποίηση των μετα- βλητών σε συστάδες και, τελικά, αναλαμβάνει η διακριτική ανάλυση να ελέγξει την προσαρμογή του μοντέλου της συσταδοποίησης και να περιγράψει στατιστικά τις συστάδες. Η χρήση της τελευταίας ενθαρρύνεται πολύ, καθόσον η συσταδοποίηση δεν διαθέτει κριτήρια μέτρησης της καλής προσαρμογής του επιχειρούμενου μοντέλου και βασίζεται ουσιαστικά στη διακριτική ανάλυση να διαπιστώσει αν οι δημιουργούμενες ομάδες είναι στατιστικά σημαντικές και επίσης αν οι μεταβλητές διαφοροποιούνται με σαφήνεια ως προς τη δράση τους μεταξύ των συστάδων. Επισημαίνεται, πάραυτα, ότι ο διαχωρισμός των δεδομένων σε ομάδες μπορεί να μην καταλήγει σε κάποια ουσιαστική ερευνητική ερμηνεία, και επομένως η ορθή επιλογή των συστάδων να έχει απλώς υποθετικό χαρακτήρα. Επιπρόσθετα, η συνεπικουρία της διακριτικής ανάλυσης προσβλέπει στην οικοδόμηση ενός προβλε- πτικού μοντέλου συσταδοποίησης επιτρέποντας την εισαγωγή τιμών από νέες παρατηρήσεις και την αξιολόγηση της αξιοπιστίας διαχωρισμού των στοιχείων (μελών) στις συστάδες.

Τρεις διαφορετικές τακτικές διασύνδεσης των στοιχείων είναι γνωστές, η καθεμία των οποίων ακολουθεί συγκε- κριμένους κανόνες επιλογής:

1. Ομαδοποίηση με άγνωστο αριθμό τελικών συστάδων, εφαρμοζόμενη είτε στον πίνακα ομοιότητας των δειγμά- των SxS είτε στον πίνακα ομοιότητας των μεταβλητών VxV (δενδρική ταξινόμηση-tree clustering).

2. Ομαδοποίηση με συγκεκριμένο αριθμό k συστάδων (ταξιδόμηση k τελικών ομάδων- k-means clustering).

3. Ταυτόχρονη ομαδοποίηση δειγμάτων και μεταβλητών (διασύνδεση διπλής κατεύθυνσης -two-way joining). Ανεξαρτήτως επιλογής αλγορίθμων, επιζητείται πάντοτε η ίδια στρατηγική δηλαδή η δημιουργία ομάδων στοιχείων, αλλά με τη σύνθεση διαφορετικών μοντέλων ομαδοποίησης, η οποία οδηγεί αναπόφευκτα και στην επιλογή εξειδικευμένων αλγορίθμων.

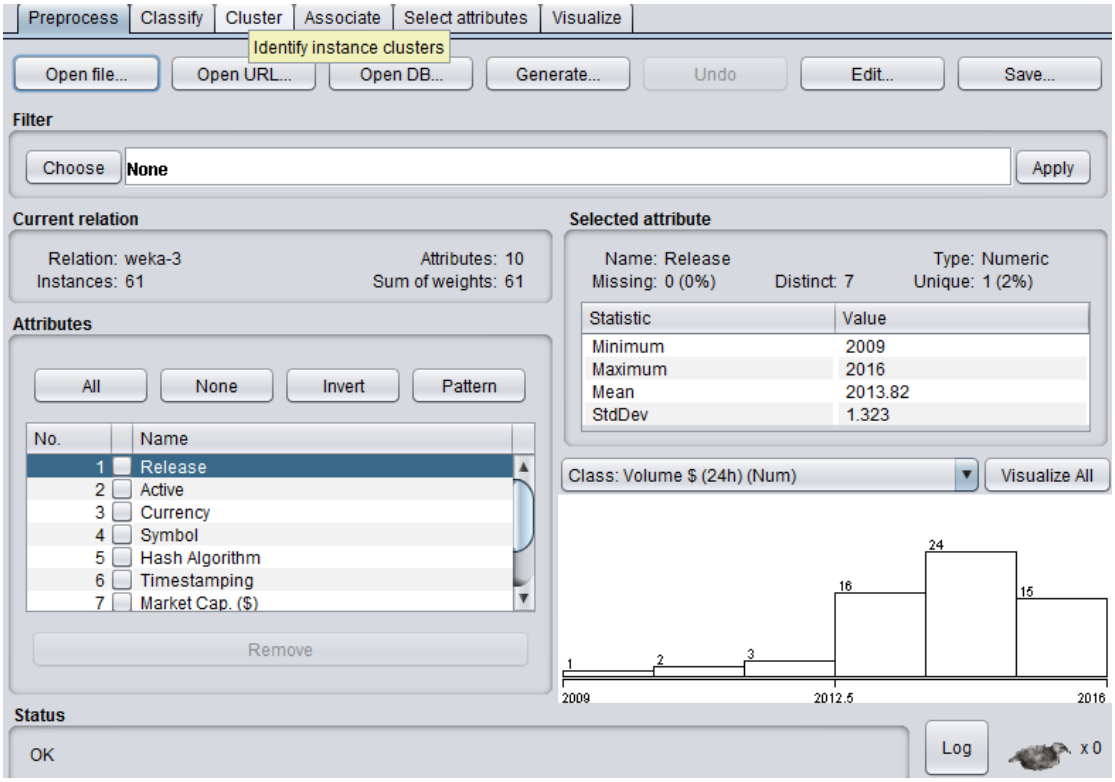
Συσταδοποίηση με τη χρήση του Weka

Η διαδικασία του clustering ή συσταδοποίησης με τη χρήση του Weka δεν είναι ιδιαίτερα σύνθετη, αλλά αποτελείται από ορισμένα βασικά βήματα.

1.GUI(Γραφικό Περιβάλλον Χρήστη) του Weka

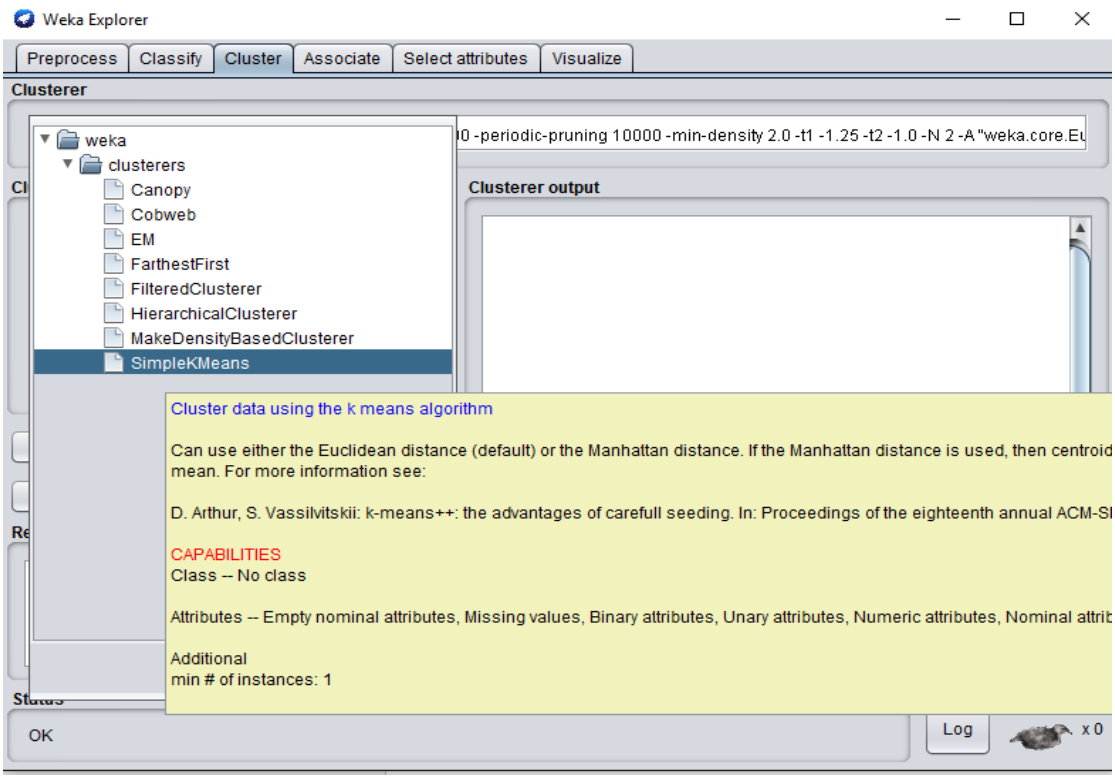
Πρώτο βήμα που πρέπει να υλοποιηθεί από το μενού του βασικού GUI(εικόνα 1) είναι η επιλογή του Explorer και κατόπιν η εισαγωγή των δεδομένων, τύπου .csv ή .arff.

2. Επιλογή συσταδοποίησης(clustering)



Δεύτερο βήμα, μετά τυχόν προεπεξεργασία των δεδομένων, είναι η επιλογή της συσταδοποίησης(εικόνα 2). Από εδώ μεταφερόμαστε σε μια νέο οθόνη, στην οποία θα πρέπει να γίνουν οι κατάλληλες παραμετροποιήσεις. Ειδικότερα, θα πρέπει να επιλεγεί μέθοδος συσταδοποίησης. Η δική μας επιλογή θα είναι ο αλγόριθμος *"Simple K-means"*(Εικόνα 3).

3. Επιλογή αλγορίθμου συσταδοποίησης



Στις περιπτώσεις που επιζητείται η συσσώρευση των στοιχείων σε συγκεκριμένο αριθμό ομάδων k, τότε εφαρμό- ζεται η ταξιδόμηση των k μέσων ως τεχνική βέλτιστης αναζήτησης αυτών: ανεύρεση των κέντρων k ομάδων και κατανομή των στοιχείων στο πλησιέστερο κέντρο ομάδας με τρόπο ώστε το τετράγωνο των αποστάσεων των στοι- χείων από την ομάδα να ελαχιστοποιείται. Αρχικά, ο αλγόριθμος προσδιορίζει k κέντρα συστάδων αντιπροσωπευ- τικά N σημείων (k<N), και ακολούθως κάθε σημείο, με τη χρήση των επαναληπτικών δοκιμών, διευθετείται σε μία από τις k συστάδες και κάθε κέντρο αποτελεί το μέσο όρο των ενταγμένων σημείων (Bishop, 1995). Η εκτέλεση πραγματοποιείται με τον αλγόριθμο του Lloyd (Hartigan & Wong, 1979) με μείζον μειονέκτημα της μεθόδου τον ορισμό εξαρχής συγκεκριμένων ομάδων στα στοιχεία, καθότι ο αλγόριθμος προτιμά να δημιουργεί ισομεγέθεις συστάδες (με ίδιο περίπου αριθμό περίπου στοιχείων) οδηγώντας έτσι στη λανθασμένη οριοθέτηση μεταξύ των ομάδων αφού βελτιστοποιεί τα κέντρα των ομάδων και όχι τα όρια αυτών. Διαθέτει όμως σοβαρά πλεονεκτήματα:

α) Όταν οι μεταβλητές είναι πολυπληθείς, η συσταδοποίηση k μέσων αποδεικνύεται υπολογιστικά πολύ ταχύτερη των ιεραρχικών με την προϋπόθεση ότι απαιτείται μικρός αριθμός ομάδων.

β) Παράγει συστάδες πιο ομοιογενείς (συμπαγείς) συγκριτικά με αυτές των ιεραρχικών μεθόδων και ειδικότερα όταν έχουν σφαιρική μορφή, διότι αποσπά τα στοιχεία στο χώρο συγκροτώντας ειδικές δομές οι οποίες το συνθέτουν.

Σύμφωνα με την συσταδοποίηση των k μέσων όλα τα στοιχεία (παρατηρήσεις) τοποθετούνται σε μία αρχι- κή συστάδα και ο αλγόριθμος θα μετακινήσει τα στοιχεία σε διάφορες συστάδες με στόχο την ελαχιστοποίηση των αποστάσεων μέσα σε κάθε συστάδα και τη μεγιστοποίηση αυτών μεταξύ των συστάδων. Υπάρχουν τρεις τρόποι υλοποίησης της παραπάνω διαδικασίας:

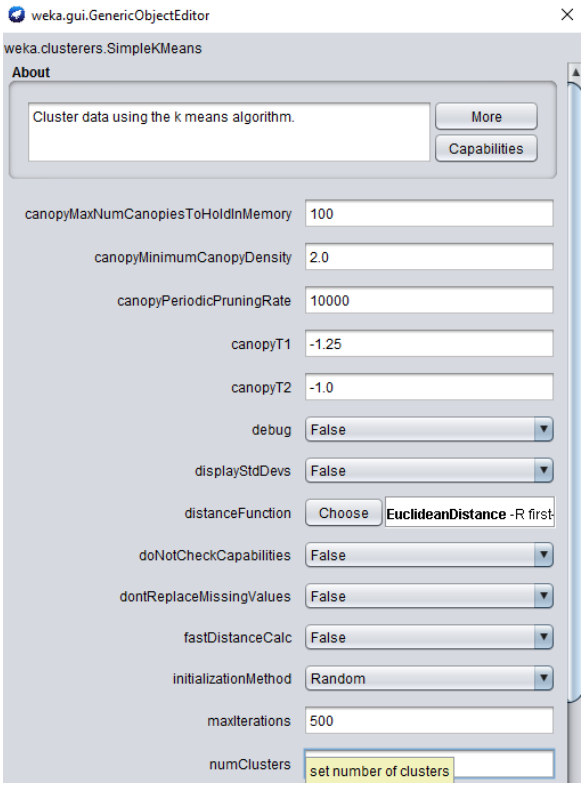
1. Επιλογή των Ν πρώτων παρατηρήσεων ως κέντρα k αρχικών συστάδων. Επομένως η θέση και τιμή των πρώτων παρατηρήσεων είναι ζωτικής σημασίας και θα πρέπει αυτές να τοποθετούνται με περίσκεψη από τον ερευνητή.

2. Επιλογή του αλγόριθμου κάποιων αρχικών παρατηρήσεων ως πρώτα κέντρα συστάδων και με επαναληπτική διαδικασία δοκιμών, τελική διευθέτηση όλων των στοιχείων στις συστάδες εξασφαλίζοντας ελάχιστη απόστα- ση αυτών από τα κέντρα τους και μέγιστη μεταξύ των συστάδων (συνηθέστερη επιλογή).

3. Οι τιμές των αποστάσεων μεταξύ όλων των στοιχείων διατάσσονται αυξητικά και ακολούθως επιλέγονται μερικές αποστάσεις ως αρχικά κέντρα συστάδων κατά σταθερά διαστήματα της κατάταξης.

Το επόμενο ζήτημα που πρέπει να διευκρινισθεί αφορά το πλήθος των clusters. (Εικόνα 4)

4. Επιλογή αριθμού clusters



Αυτή η επιλογή γίνεται με καθορισμό της παραμέτρου numClusters. Οι επιλογές που έχουν γίνει για τους σκοπούς αυτής της μελέτης είναι διαδοχικά 2, 3 και 4 clusters. Στις παρακάτω τρεις παραγράφους θα παρατεθούν και σχολιαστούν τα αποτελέσματα. Επισημαίνεται ότι για την εξαγωγή των παρακάτω αποτελεσμάτων επιλέχθηκε, όπως προτείνεται για αυτές τις περιπτώσεις, το *«σύνολο εκπαίδευσης»* (*«training set»)* των δεδομένων και, επιπλέον, ότι τα σημεία γύρω από τα οποία συσταδοποιούνται τα δεδομένα ονομάζονται “centroids”.

Α)Συσταδοποίηση με 2 clusters

4.4.1 Δημιουργία δύο ομάδων

Στη συνέχεια τα δεδομένα ομαδοποιούνται σε δύο ομάδες, έχοντας αφαιρέσει τα χαρακτηριστικά που δεν συμβάλλουν στην ομαδοποίηση (όπως εξηγείται στην παράγραφο 5.1) και προκύπτουν τα εξής:

Πίνακας 5 Ομαδοποίηση δεδομένων σε δύο ομάδες

Χαρακτηριστικό	Full Data	Ομάδες	
	27	14	13
Αλγόριθμος hash	SHA-256d	SHA-256d	N/A
Μηχανισμός ασφαλείας	POW	POW	POS
Προσφορά	2635931380.963	4482704384.8571	647098915.2308
Αλλαγή	0.787	3.2886	-1.9069
Αποπληθωρισμός	N/A	YES	N/A

Ο παραπάνω πίνακας δείχνει τα αποτελέσματα της ομαδοποίησης. Δίνονται οι πιο πιθανές τιμές των μεταβλητών για το σύνολο των κρυπτονομισμάτων και για κάθε ομάδα κρυπτονομισμάτων. Τα αποτελέσματα αυτά σημαίνουν ότι τα κρυπτονομίσματα της βάσης δεδομένων χαρακτηρίζονται από αλγόριθμο κατακερματισμού (hash) τύπου SHA-256d, μηχανισμό ασφαλείας POW και διαθέσιμη προσφορά νομισμάτων περί τα 2635 εκατομμύρια. Η αλλαγή 24ώρου στην αξία των κρυπτονομισμάτων είναι κατά βάση θετική και ίση με 0,78%, ενώ η δυνατότητα αποπληθωρισμού είναι αβέβαιη.

Μέσα σε αυτή την πλήρη ομάδα με τα παραπάνω χαρακτηριστικά, μπορούμε να ξεχωρίσουμε 2 ομάδες. Η πρώτη περιλαμβάνει 14 κρυπτονομίσματα με αλγόριθμο κατακερματισμού (hash) τύπου SHA-256d, μηχανισμό ασφαλείας POW και διαθέσιμη προσφορά νομισμάτων περί τα 4482 εκατομμύρια. Η αλλαγή 24ώρου στην αξία των κρυπτονομισμάτων είναι θετική και ίση με 3,29%, ενώ υπάρχει δυνατότητα αποπληθωρισμού. Η δεύτερη ομάδα περιλαμβάνει 13 κρυπτονομίσματα με κάποιον άγνωστο αλγόριθμο κατακερματισμού (hash), μηχανισμό ασφαλείας POS και διαθέσιμη προσφορά νομισμάτων περί τα 647 εκατομμύρια. Η αλλαγή 24ώρου στην αξία των κρυπτονομισμάτων είναι αρνητική και ίση με -1.9%, ενώ δεν υπάρχει δυνατότητα αποπληθωρισμού.

Το σφάλμα ομαδοποίησης είναι 38%. Δημιουργώντας περισσότερες ομάδες, θα μειωθεί το σφάλμα ομαδοποίησης.

Final cluster centroids:

		Cluster#	
Attribute	*Full Data*	*0*	*1*
	(61.0)	*(20.0)*	*(41.0)*
Release	*2013.8197*	*2014.1*	*2013.6829*
Active	*Active*	*Active*	*Active*
Currency	*Auroracoin*	*BlackCoin*	*Auroracoin*
Symbol	*AUR*	*BC, BLK*	*AUR*
Hash Algorithm	*Scrypt*	*Scrypt*	*Scrypt*
Timestamping	*POW*	*POW & POS*	*POW*
Market Cap. ($)	*83799109.5738*	*22587771.75*	*113658298.7561*
Price ($)	*18058813412158.633*	*26494765126414.527*	*13943715014960.643*

Active Coins 10774918558.9508 300733660.1 15884277046.1951

Volume $ (24h) 626751.4262 74409 896186.7561

=== Model and evaluation on training set ===

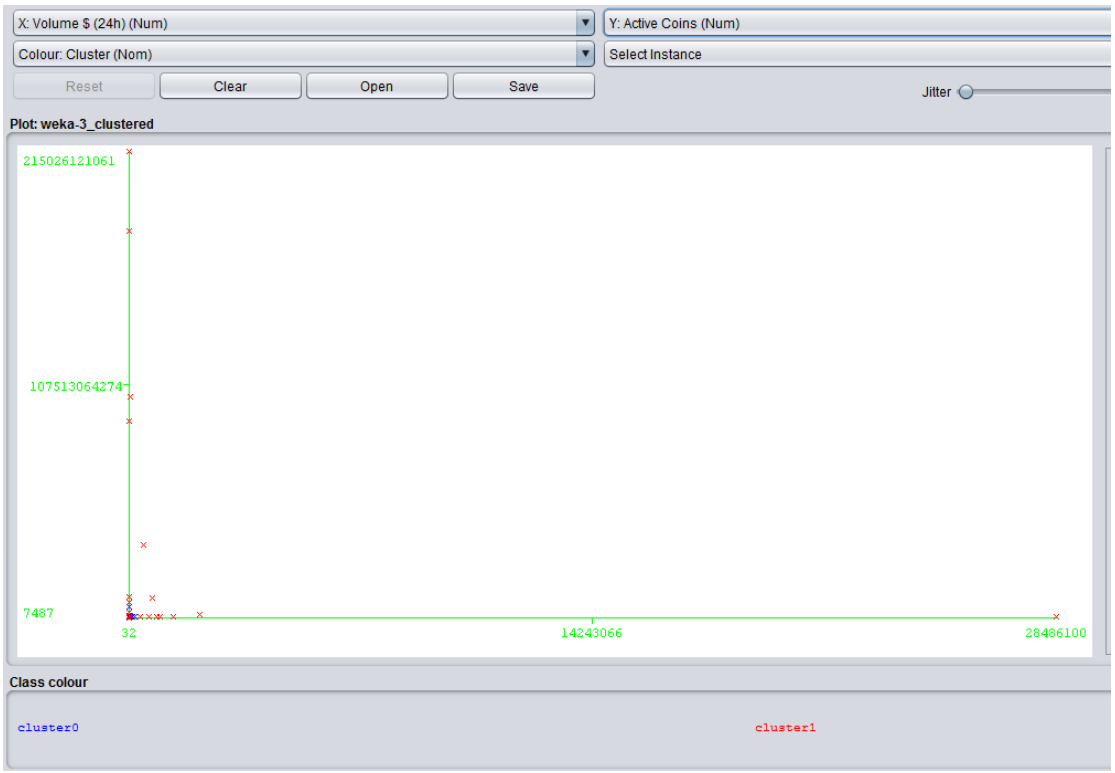
Clustered Instances

0 20 (33%)

1 41 (67%)

Παρατηρείται χαρακτηριστικά ότι η πρώτη συστάδα στην οποία ανήκει το 33% των παρατηρήσεων έχει ως κεντρικό σημείο(centroid) με νόμισμα το *BlackCoin*, ενώ η δεύτερη, με διπλάσιο ποσοστό παρατηρήσεων(67%) έχει ως νόμισμα το *Auroracoin,* Παρακάτω βλέπουμε τα αποτελέσματα της οπτικοποίησης(επιλογή *«Visualize results»*) των Clusters για δύο συγκεκριμένες μεταβλητές, τις *«Volume»* και *«Active coins»*

5. Οπτικοποίηση διάδας συστάδων



Στο τελευταίο tab του WEKA Explorer παρέχονται εργαλεία οπτικοίησης των δεδομένων. Η οπτικοποίηση είναι πολύ χρήσιμη στην πράξη, καθώς επιτρέπει στον χρήστη να κατανοήσει με εύκολο και γρήγορο τρόπο τη διασπορά των παρατηρήσεων. Το παράθυρο αυτό περιέχει έναν πίνακα διαγραμμάτων διασποράς για όλα τα δυνατά ζεύγη των χαρακτηριστικών των δεδομένων. ν. Εάν στα δεδομένα υπάρχει γνώρισμα κλάσης, όπως στα δεδομένα του παραδείγματος, ο χρήστης ορίζει το πεδίο κλάσης και οι παρατηρήσεις χρωματίζονται ανάλογα. Επιπλέον, ο χρήστης μπορεί να αλλάξει το μέγεθος του πίνακα διαγραμμάτων και το μέγεθος των σημείων, καθώς και να επιλέξει γνωρίσματα ή/και υποσύνολο των παρατηρήσεων. Ο χρήστης μπορεί να αλλάξει τις μεταβλητές των αξόνων Χ και Υ από τα αντίστοιχα πεδία και να ορίσει το γνώρισμα κλάσης, ώστε οι παρατηρήσεις να χρωματιστούν ανάλογα. Στο δεξιό τμήμα του παρά- θυρου παρουσιάζονται οι κατανομές των παρατηρήσεων για σταθερή μεταβλητή στον άξονα Υ και διάφορες μεταβλητές στον άξονα Χ.

Β)Συσταδοποίηση με 3 clusters

4.4.2 Δημιουργία τριών ομάδων

Στη συνέχεια τα δεδομένα ομαδοποιούνται σε τρεις ομάδες, έχοντας αφαιρέσει τα χαρακτηριστικά που δεν συμβάλλουν στην ομαδοποίηση (όπως εξηγείται στην παράγραφο 5.1) και προκύπτουν τα εξής:

Πίνακας 6 Ομαδοποίηση δεδομένων σε τρεις ομάδες

Χαρακτηριστικό	**Ομάδες**		
	11	5	11
Αλγόριθμος hash	SHA-256d	N/A	Scrypt
Μηχανισμός ασφαλείας	POW	N/A	POS
Προσφορά	5698683617.4545	1477843249.8	99582840.4545
Αλλαγή	1.69	0.904	-0.17
Αποπληθωρισμός	N/A	YES	N/A

Ο παραπάνω πίνακας δείχνει τα αποτελέσματα της ομαδοποίησης. Δίνονται οι πιο πιθανές τιμές των μεταβλητών για το σύνολο των κρυπτονομισμάτων και για κάθε ομάδα κρυπτονομισμάτων. Τα αποτελέσματα για τα κρυπτονομίσματα της βάσης δεδομένων είναι όμοια με αυτά της παραγράφου 5.2.1.

Από τη βάση δεδομένων με τα παραπάνω χαρακτηριστικά, μπορούμε να ξεχωρίσουμε 3 ομάδες. Η πρώτη περιλαμβάνει 11 κρυπτονομίσματα με αλγόριθμο κατακερματισμού (hash) τύπου SHA-256d, μηχανισμό ασφαλείας POW και διαθέσιμη προσφορά νομισμάτων περί τα 5698 εκατομμύρια. Η αλλαγή 24ώρου στην αξία των κρυπτονομισμάτων είναι θετική και ίση με 1.6%, ενώ υπάρχει δυνατότητα αποπληθωρισμού.

Η δεύτερη ομάδα περιλαμβάνει 5 κρυπτονομίσματα με κάποιον άγνωστο αλγόριθμο κατακερματισμού (hash), άγνωστο μηχανισμό ασφαλείας και διαθέσιμη προσφορά νομισμάτων περί τα 1477 εκατομμύρια. Η αλλαγή 24ώρου στην αξία των κρυπτονομισμάτων είναι θετική και ίση με 0.9%, ενώ η δυνατότητα αποπληθωρισμού είναι αβέβαιη.

Η τρίτη ομάδα περιλαμβάνει 11 κρυπτονομίσματα με αλγόριθμο κατακερματισμού (hash) τύπου Scrypt, μηχανισμό ασφαλείας POS και διαθέσιμη προσφορά νομισμάτων περί τα 99 εκατομμύρια. Η αλλαγή 24ώρου στην αξία των

κρυπτονομισμάτων είναι αρνητική και ίση με 0.17%, ενώ η δυνατότητα αποπληθωρισμού είναι αβέβαιη.

Το σφάλμα ομαδοποίησης είναι 34%.

Τα αποτελέσματα που λαμβάνονται από το Weka για σχηματισμό τριάδας clusters είναι τα ακόλουθα:

Final cluster centroids:

		Cluster#		
Attribute	Full Data	0	1	2
	(61.0)	(8.0)	(41.0)	(12.0)
Release	2013.8197	2014.5	2014	2012.75
Active	Active	Active	Active	Active
Currency	Auroracoin	Dash	Auroracoin	Bitcoin
Symbol	AUR	DASH	AUR	BTC
Hash Algorithm	Scrypt	Scrypt	Scrypt	SHA-256d
Timestamping	POW	POW & POS	POW	Consensus
Market Cap. ($)	83799109.5738	50116479.875	14299935.0488	343709709
Price ($)	18058813412158.633	29235221393507.215	7476175968494.731	46765219357111.28
Active Coins	10774918558.9508	24497138.125	15011670563.6341	3466296823.5
Volume $ (24h)	626751.4262	155046.375	188368.0732	2439031.25

Clustered Instances

0 8 (13%)

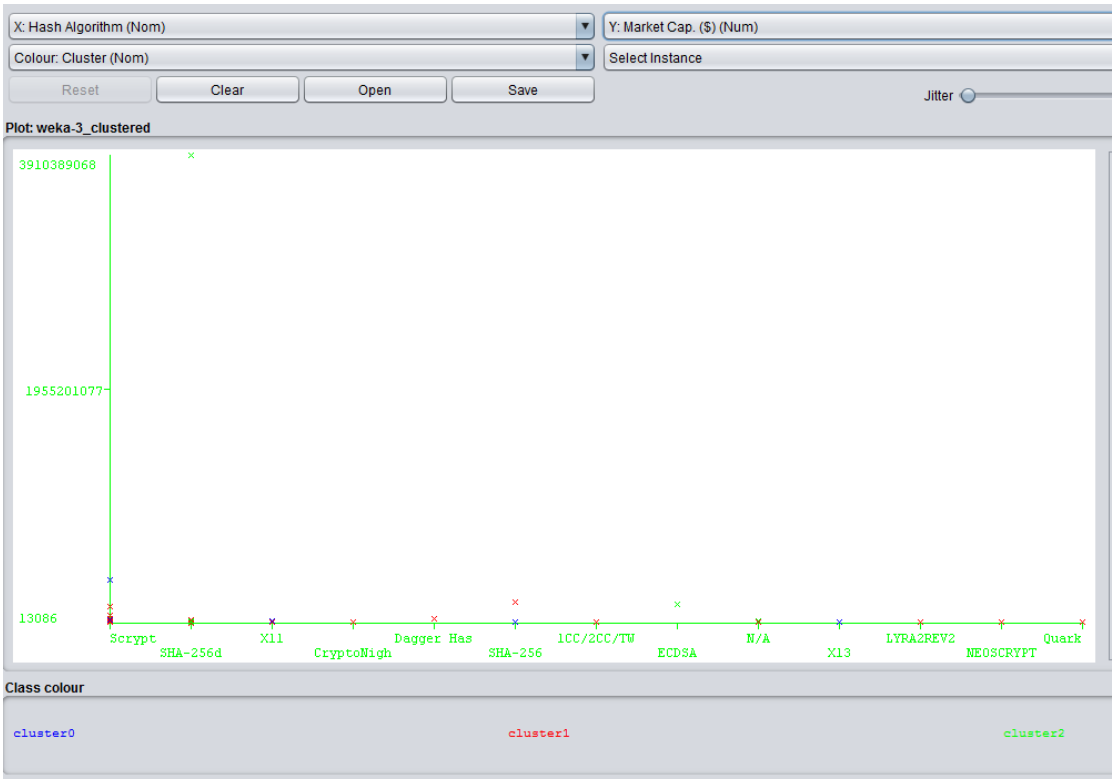
1 41 (67%)

2 12 (20%)

Από τα παραπάνω αποτελέσματα προκύπτει ότι η μεγαλύτερη συστάδα της προηγούμενης εκτέλεσης παραμένει και είναι πάλι η δεύτερη που περιλαμβάνει το 67% των παρατηρήσεων, ενώ η πρώτη φαίνεται να διασπάται σε δύο, την πρώτη και την τρίτη, οι οποίες περιλαμβάνουν η μία το 13% και η άλλη το 20% των παρατηρήσεων.

Από τις δύο νέες συστάδες, η μία διαθέτει ως κρυπτονόμισμα το Dash, ενώ η άλλη το Bitcoin. Στην παρακάτω εικόνα, έχουμε την οπτικοποίηση των τριών clusters για τις μεταβλητές –αυτή τη φορά- *"Hash Algorithm"*, που είναι ονομαστική(nominal), και *"Market Cap.($)"*, που είναι αριθμητική(numerical).

6. Οπτικοποίηση τριάδας συστάδων



Γ)Συσταδοποίηση με 4 clusters

4.4.3 Δημιουργία τεσσάρων ομάδων

Στη συνέχεια τα δεδομένα ομαδοποιούνται σε τέσσερις ομάδες, έχοντας αφαιρέσει τα χαρακτηριστικά που δεν συμβάλλουν στην ομαδοποίηση (όπως εξηγείται στην παράγραφο 5.1) και προκύπτουν τα εξής:

Χαρακτηριστικό	**Ομάδες**			
	9	4	5	9
Αλγόριθμος hash	SHA-256d	N/A	N/A	Scrypt
Μηχανισμός ασφαλείας	POW	N/A	POS	POW/ POS
Προσφορά	6961844637.5556	1844133529.5	175922128.8	28600087.3333
Αλλαγή	2	-0.37	-3.37	2.29
Αποπληθωρισμός	N/A	YES	N/A	N/A

Πίνακας 7 Ομαδοποίηση δεδομένων σε τρεις ομάδες

Ο παραπάνω πίνακας δείχνει τα αποτελέσματα της ομαδοποίησης. Δίνονται οι πιο πιθανές τιμές των μεταβλητών για το σύνολο των κρυπτονομισμάτων και για κάθε ομάδα κρυπτονομισμάτων. Τα αποτελέσματα για τα κρυπτονομίσματα της βάσης δεδομένων είναι όμοια με αυτά της παραγράφου 5.2.1.

Από τη βάση δεδομένων με τα παραπάνω χαρακτηριστικά, μπορούμε να ξεχωρίσουμε 4 ομάδες. Η πρώτη περιλαμβάνει 9 κρυπτονομίσματα με

αλγόριθμο κατακερματισμού (hash) τύπου SHA-256d, μηχανισμό ασφαλείας POW και διαθέσιμη προσφορά νομισμάτων περί τα 6961 εκατομμύρια. Η αλλαγή 24ώρου στην αξία των κρυπτονομισμάτων είναι θετική και ίση με 2%, ενώ η δυνατότητα αποπληθωρισμού είναι αβέβαιη.

Η δεύτερη ομάδα περιλαμβάνει 4 κρυπτονομίσματα με κάποιον άγνωστο αλγόριθμο κατακερματισμού (hash), άγνωστο μηχανισμό ασφαλείας και διαθέσιμη προσφορά νομισμάτων περί τα 1844 εκατομμύρια. Η αλλαγή 24ώρου στην αξία των κρυπτονομισμάτων είναι αρνητική και ίση με -0.37%, ενώ η δυνατότητα αποπληθωρισμού είναι θετική.

Η τρίτη ομάδα περιλαμβάνει 5 κρυπτονομίσματα με κάποιον άγνωστο αλγόριθμο αλγόριθμο κατακερματισμού (hash), μηχανισμό ασφαλείας POS και διαθέσιμη προσφορά νομισμάτων περί τα 175 εκατομμύρια. Η αλλαγή 24ώρου στην αξία των κρυπτονομισμάτων είναι αρνητική και ίση με -3.37%, ενώ η δυνατότητα αποπληθωρισμού είναι αβέβαιη.

Το σφάλμα ομαδοποίησης είναι 30%.

Τέλος, τα αποτελέσματα(Log) που λαμβάνονται από το Weka για σχηματισμό τεσσάρων clusters είναι τα παρακάτω:

Final cluster centroids:

		Cluster#			
Attribute	Full Data	0	1	2	3
		(61.0)	(8.0)	(33.0)	(3.0)	(17.0)
Release	2013.8197	2014.5	2014.0303	2012.6667	2013.2941
Active	Active	Active	Active	Active	Active
Currency	Auroracoin	Dash	Auroracoin	Mastercoin	Bitcoin

Symbol	AUR	DASH	AUR	MSC	BTC
Hash Algorithm	Scrypt	Scrypt	Scrypt	SHA-256d	SHA-256d
Timestamping	POW	POW & POS	POW	N/A	POW
Market Cap. ($)	83799109.5738	50116479.875	21556838.2424	4328729	234497176.2353
Price ($)	18058813412158.633	29235221393507.215	9288582263887.387	98671177126740.2	15598182406183.234
Active Coins	10774918558.9508	24497138.125	19609641618	846392051.6667	436276790.7059
Volume $ (24h)	626751.4262	155046.375	244257.8182	22484	1697853.2941

Clustered Instances

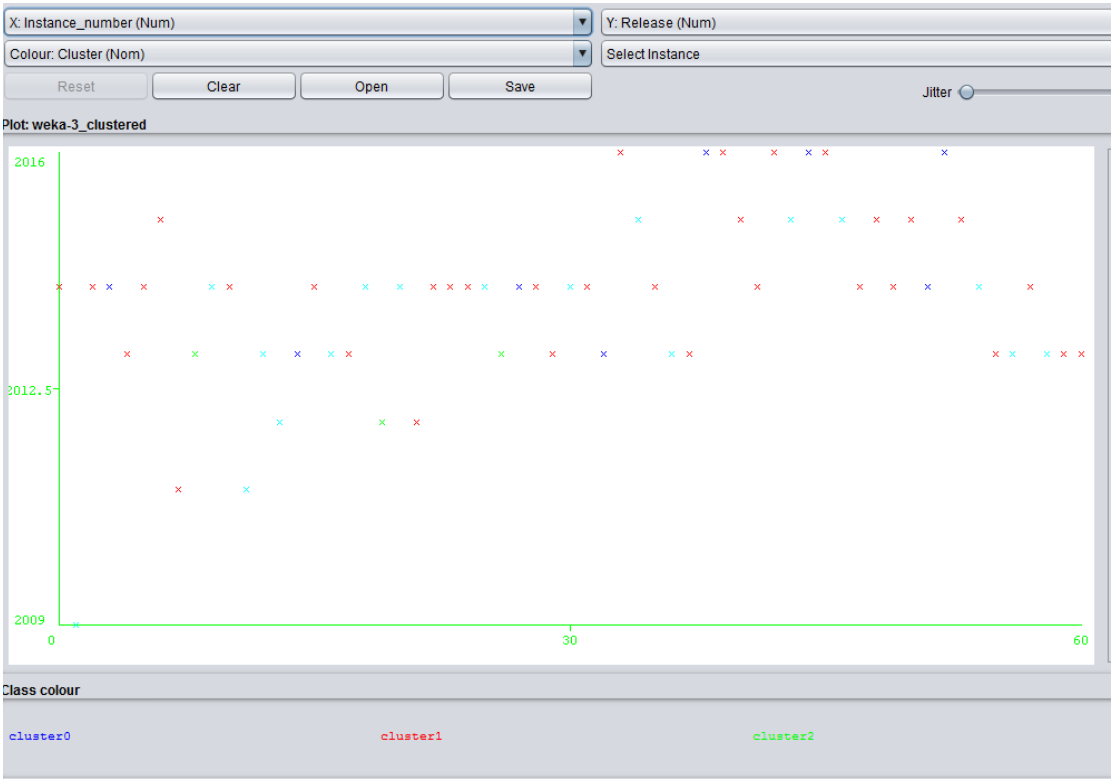
0	**8 (13%)**
1	**33 (54%)**
2	**3 (5%)**
3	**17 (28%)**

Εδώ παρατηρείται μια διαφορετική εικόνα. Φαίνεται ότι η αρχική δεύτερη συστάδα «εκπροσωπείται» από την νέα $1^{η}$ και $2^{η}$ συστάδα(0 και 1), οι οποίες συγκεντρώνουν συνολικά το 67% των παρατηρήσεων, ενώ η αρχική πρώτη συστάδα από την $3^{η}$ και $4^{η}$, που και πάλι συγκεντρώνουν ως σύνολο το 33% των παρατηρήσεων. Πλέον, τα νομίσματα της κάθε μίας είναι τα εξής, από το cluster 0 έως το cluster 4:

Auroracoin	***Dash***	***Auroracoin***	***Mastercoin***

Η οπτικοποίηση αυτού του cluster για τις αριθμητικές μεταβλητές *«Instance_number»* και *«Release»* είναι η ακόλουθη:

7. Οπτικοποίηση τετράδας clusters



Αξιοποιώντας την βάση δεδομένων που δημιουργήσαμε, αναλύουμε τα δεδομένα των χαρακτηριστικών για τα διαφορετικά κρυπτονομίσματα που εισήχθησαν στην αγορά πριν το 2015 και έχουν κεφαλαιοποίηση άνω του 1 εκατομμυρίου δολαρίων. Οι είσοδοι του μοντέλου είναι η αρχική βάση δεδομένων και οι ρυθμίσεις που γίνονται αφορούν σε classifier τύπου Naivebayes. Τα χαρακτηριστικά που επελέγησαν, για τη βέλτιστη ομαδοποίηση είναι η Προσφορά, ο Μηχανισμός

ασφάλειας, ο Αλγόριθμος hash, ο Αποπληθωρισμός και η Αλλαγή αξίας 24h (%). Το σύνολο των χαρακτηριστικών αυτών συμφωνούν με την ανάλυση του Farell (2015), εκτός από την αλλαγή αξίας 24h (%), που προστίθεται στη δική μας ανάλυση.

Κατά την ομαδοποίηση, παρατηρούμε ότι το σφάλμα μειώνεται αυξάνοντας το πλήθος των ομάδων, καθώς έτσι επιτυγχάνεται μεγαλύτερη ακρίβεια στην ομαδοποίηση.

Σε κάθε ομαδοποίηση, η ομάδα με αλγόριθμο κατακερματισμού (hash) τύπου SHA-256d και μηχανισμό ασφαλείας POW συνδέεται με υψηλή προσφορά και θετική αλλαγή της ισοτιμίας του κρυπτονομίσματος σε δολάρια αμερικής. Η δυνατότητα αποπληθωρισμού επίσης συνδέεται με τη θετική αλλαγή της ισοτιμίας. Ο μηχανισμός ασφαλείας POS, αντίθετα, συσχετίζεται με πολύ αρνητικές αλλαγές ισοτιμίας και περιορισμένη προσφορά κρυπτονομισμάτων. Ο αλγόριθμος scrypt με μηχανισμό ασφαλείας POW/POS συσχετίζεται με αύξηση της ισοτιμίας και υψηλή προσφορά νομισμάτων.

Το δεύτερο λογισμικό που θα χρησιμοποιηθεί είναι το *«Visual Promethee»*. Το λογισμικό αυτό, το οποίο είναι, όπως και το Weka, δωρεάν διαθέσιμο από την αντίστοιχη σελίδα στο Διαδίκτυο[2], υλοποιεί την μέθοδο της πολυκριτηριακής ανάλυσης PROMETHEE (Preference Ranking Organization Method For Enrichment Evaluation). Για την μέθοδο αυτή, θα πρέπει να θεωρηθούν ορισμένες ομάδες κριτηρίων, με συγκεκριμένη προτεραιότητα ή ιεραρχία μεταξύ τους, από τις οποίες θα προκύψει μια συγκεκριμένη αξιολόγηση και κατάταξη(Ranking) των κρυπτονομισμάτων μεταξύ τους. Αρχικά θα υλοποιηθεί η μέθοδος συσταδοποίησης μέσα από το λογισμικό Weka.

[2] http://www.promethee-gaia.net/software.html

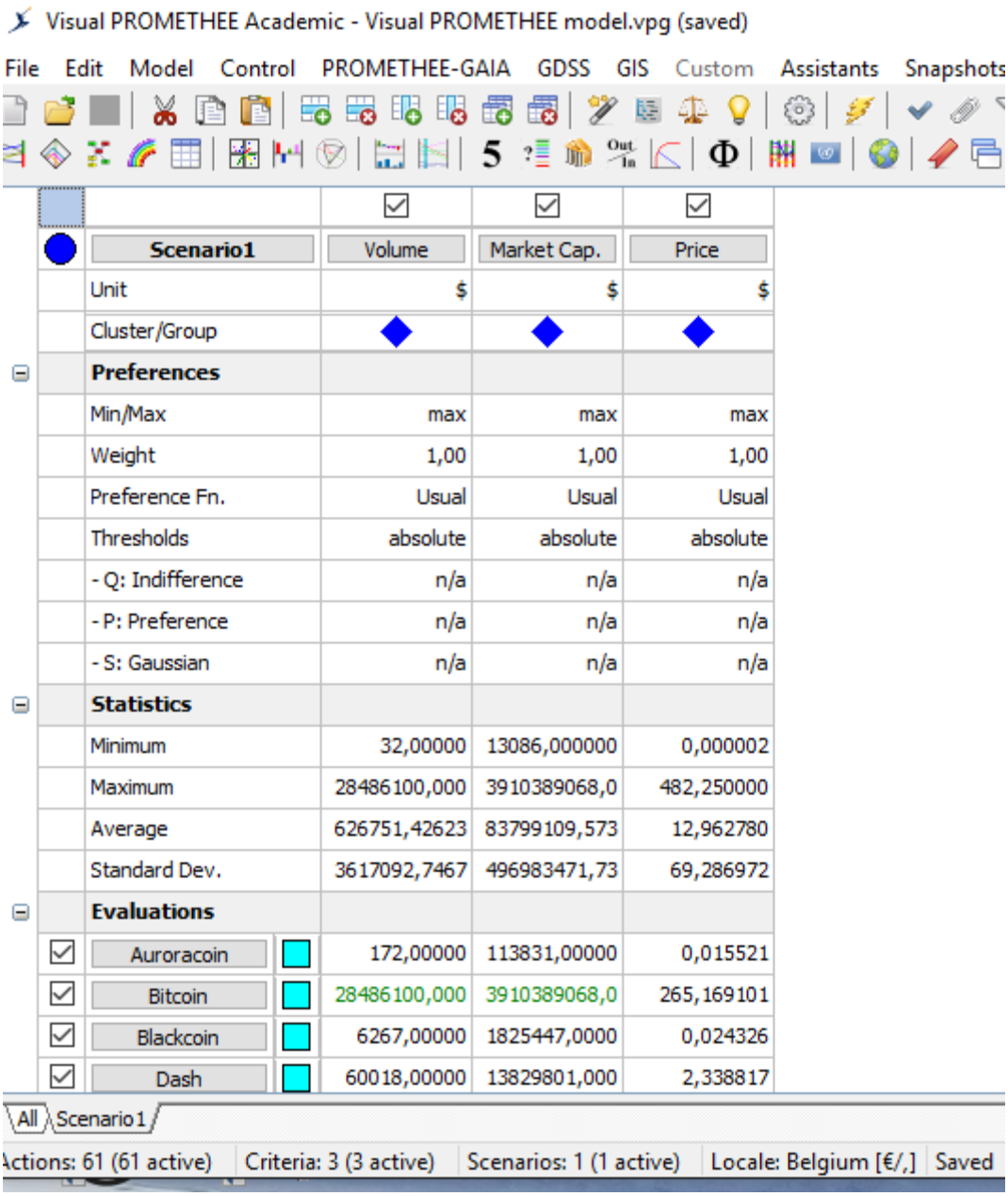
Όπως αναφέρθηκε και στην εισαγωγή στο κεφάλαιο αυτό, στην παράγραφο αυτή θα πραγματοποιηθεί μία προσπάθεια κατάταξης(ranking) με την μέθοδο πολυκριτηριακής ανάλυσης PROMETHEE(Preference Ranking Organization Method For Enrichment Evaluation) και με το λογισμικό Visual Promethee.

Ειδικότερα, η μέθοδος PROMETHEE που θα χρησιμοποιηθεί θα είναι η PROMETHEE II, η οποία παρέχει τη δυνατότητα μιας ολοκληρωμένης αξιολόγησης με βάση την τιμή της μεταβλητή Phi(Φ).[3] Η υπομέθοδος αυτή μας δίνει τόσο μεγαλύτερη τιμή Φ, όσο καλύτερη είναι η επιλογή στην οποία αντιστοιχείται η τιμή αυτή για τα επιλεγμένα και εκάστοτε σταθμισμένα κριτήρια.

Στην παρακάτω εικόνα παρατηρούμε το αντίστοιχο συμπληρωμένο «σενάριο» στο Visual Promethee.

[3] http://www.otlet-institute.org/wikics/PROMETHEE.html

8. Συμπληρωμένο σενάριο στο Visual Promethee



Υπάρχουν τρία στοιχεία που πρέπει να προσεχθούν και τα οποία διακρίνονται στην Εικόνα 8. Πρόκειται για τα εξής:

i)**actions**: διακρίνονται εν μέρει στο κάτω μέρος της οθόνης. Συνολικά είναι 61 και είναι το **σύνολο των κρυπτονομισμάτων**, τα οποία θα αξιολογηθούν και καταταγούν κατά PROMETHEE

ii)**criteria:** πρόκειται για τα κριτήρια που θα χρησιμοποιηθούν και τα οποία θα πρέπει να επιλεχθούν ως κριτήρια αξιολόγησης από τις διαθέσιμες τιμές των μεταβλητών που υπάρχουν.

Προσδιορίζοντας τα βάρη των κριτηρίων με βάση πολλαπλές μορφές προτιμήσεων

Σύμφωνα με τους Zhang και Ma, στις πολυκριτηριακές μεθόδους λήψης αποφάσεων, οι λήπτες αποφάσεων πάντα δίνουν πληροφορίες προτίμησης εναλλακτικών, κριτηρίων ή πινάκων αποφάσεων. Καθώς οι διάφοροι λήπτες αποφάσεων μπορεί να έχουν άλλη κουλτούρα, άλλη εκπαίδευση ή ένα διαφορετικό σύστημα αξιών, μπορεί να εκφράζουν τις προτιμήσεις τους με διαφορετικές μορφές. Για να υπάρχει περισσότερη ελαστικότητα στο σύστημα, διάφορες μορφές προτιμήσεων έχουν ληφθεί υπόψη από τους Zhang και Ma στην προσπάθειά τους να αναπτύξουν μία νέα προσέγγιση προσδιορισμού των βαρών των κριτηρίων: τάξεις προτίμησης, τιμές χρησιμότητας και πολλαπλή σχέση προτίμησης, επιλεγμένα υποσύνολα, κανονική σχέση προτίμησης ασαφώς επιλεγμένου υποσυνόλου, σχέση ασαφούς προτίμησης, όροι γλωσσολογίας και σύγκριση ανά ζεύγη. Οι διάφορες μορφές προτίμησης ενοποιούνται σε μία πολλαπλή σχέση προτίμησης. Στη συνέχεια, γίνεται συγκέντρωση των προτιμήσεων και ακολουθεί διαδικασία εκμετάλλευσης των πληροφοριών αυτών ώστε να προσδιοριστούν τα βάρη των κριτηρίων.

Προκειμένου να διευκολυνθεί η περιγραφή της προτεινόμενης μεθόδου από τους Zhang και Ma οι ακόλουθες υποθέσεις και μετασχηματισμοί έχουν γίνει:

- Οι εναλλακτικές θεωρείται ότι είναι γνωστές: έστω $S=\{S_1,S_2,\ldots,S_m\}$ με $m\geq 2$ δηλώνει το σύνολο των πιθανών εναλλακτικών.
- Τα κριτήρια θεωρούνται ότι είναι γνωστά: έστω $C=\{C_1,C_2,\ldots,C_n\}$ με $n\geq 2$ δηλώνει το σύνολο των κριτηρίων, τα οποία θεωρούνται ότι είναι προσθετικά ανεξάρτητα.
- Ο συντελεστής βαρύτητας των κριτηρίων είναι άγνωστος: έστω $w=(w_1,w_2,\ldots,w_n)^T$ είναι ο συντελεστής βαρύτητας των κριτηρίων, όπου $\sum_{j=1}^{n} w_j = 1$, $w_j\geq 0$, $j=1,\ldots,n$ και w_j δηλώνει το βάρος του κριτηρίου C_j.
- Οι λήπτες αποφάσεων είναι γνωστοί: έστω $E=\{e_1,e_2,\ldots,e_k\}$δηλώνει το σύνολο των K (K≥2) ληπτών αποφάσεων.

- *Ενοποίηση των μορφών προτίμησης σε μία σχέση πολλαπλασιαστικής προτίμησης*

Οι προτιμήσεις των ληπτών αποφάσεων για τα κριτήρια μπορούν να περιγραφούν από μία θετική σχέση προτίμησης. Η ένταση της προτίμησης μετράται από μία κλίμακα , όπως αυτή του Saaty (1980), ο οποίος χρησιμοποιεί μία κλίμακα από το 1 έως το 9. Με το «1» δηλώνει ότι ο λήπτης αποφάσεων είναι αδιάφορος μεταξύ δύο κριτηρίων ενώ με το «9» δηλώνει την ισχυρή προτίμηση του λήπτη για ένα κριτήριο. Οι ενδιάμεσες προτιμήσεις δηλώνονται με το «2», «3», «4»,..., «8». Ο πίνακας της σχέσης προτίμησης θεωρείται ότι είναι αντίστροφος πολλαπλασιαστικός (Saaty, 1980).

Άλλες μορφές προτίμησης:

1) ***Τάξεις προτίμησης*** ή διαταγμένος συντελεστής. Οι Zhang και Ma θεωρούν ότι $O^k=\{o^k(1),\ldots,o^k(n)\}$ δηλώνει το συντελεστή που χρησιμοποείται από έναν λήπτη αποφάσεων για να εκφράσει την προτίμησή του στα κριτήρια (Chiclana et al., 1998, Herrera at al., 2001). Το $o^k(.)$ είναι μία συνδυαστική συνάρτηση πάνω στο σύνολο {1,...,n} και $o^k(i)$ αναπαριστά τη θέση κατάταξης του κριτηρίου C_i, i=1,2,…,n. Τα κριτήρια κατατάσσονται από το καλύτερο στο χειρότερο.

Οι Herrera at al., (2001) μελέτησαν τις μεθόδους μετασχηματισμού ενός διαταγμένου συντελεστή σε μία σχέση πολλαπλασιαστικής προτίμησης. Κοινώς, οι τάξεις προτίμησης O^k μπορούν να μετασχηματιστούν σε σχέσεις πολλαπλασιαστικής προτίμησης στα κριτήρια C_i και C_j ως εξής (Herrera at al., 2001):

$$P^k_{ij}=9^{u^k_i-u^k_j}, \text{ με } i,j= 1,\ldots,n \quad \ldots\ldots(1)$$

Όπου $u^k_i=v(n-o^{k(i)})$ και $u^k_j=v(n-o^{k(j)})$ είναι τιμές χρησιμότητας συσχετιζόμενες με τα κριτήρια C_i και C_j αντίστοιχα, με μία αύξουσα συνάρτηση όπως η $u^k_i=(n-o^{k(i)})/(n-1)$.

2) ***Τιμή χρησιμότητας*** ή ένας συντελεστής χρησιμότητας. Έστω $U^k=(u^k_1,u^k_2,\ldots,u^k_n)$ είναι ένας συντελεστής χρησιμότητας που παρέχεται από τον λήπτη αποφάσεων e_k, $e_k \in E$. Όπου $u^k_i \in [0,1]$, i=1,…,n και u^k_i αναπαριστά την τιμή χρησιμότητας που δίνεται από τον λήπτη e_k στο κριτήριο C_i.

Επίσης, οι Herrera at al., (2001) ανέλυσαν τις μεθόδους μετασχηματισμού ενός συντελεστή χρησιμότητας σε μία σχέση πολλαπλασιαστικής προτίμησης. Ο συντελεστής χρησιμότητας $U^k=(u^k_1,u^k_2,\ldots,u^k_n)$ μπορεί να μετασχηματιστεί σε σχέση πολλαπλασιαστικής προτίμησης για τα κριτήρια C_i και C_j ως εξής (Herrera at al., 2001):

$$p^k_{ij}=\frac{u_i^k}{u_j^k}, \text{ με } i,j= 1,\ldots,n \quad (2)$$

3) ***Ένας συντελεστής γλωσσολογικών όρων στο κριτήριο C.*** Έστω $L^k=(l^k_1, l^k_2,\ldots,l^k_n)$ είναι ένας συντελεστής γλωσσολογικών όρων που δίνεται από τον λήπτη αποφάσεων e_k, ως γλωσσολογική εκτίμηση του κριτηρίου C_i, i=1,…,n, $e_k \in E$.

Οι Zhang και Ma υποθέτουν ότι σε δύο κριτήρια C_i και C_j αποδίδονται οι γλωσσολογικοί όροι $l^k_i=(u_i,a_i,\beta_i)$ και $l^k_j=(u_j,a_j,\beta_j)$ αντίστοιχα. Για χάριν ευκολίας, χρησιμοποιούν την ακόλουθη συνάρτηση για το μετασχηματισμό των όροι $l^k_i=(u_i,a_i,\beta_i)$ και $l^k_j=(u_j,a_j,\beta_j)$ σε σχέσεις πολλαπλασιαστικής προτίμησης στα κριτήρια C_i και C_j:

$$p^k_{ij}=9^{u_i-u_j}, \quad \text{με } i,j=1,\ldots,n \quad (3)$$

4) ***Ένα υποσύνολο κριτηρίων C.*** Έστω $\bar{C}=\{C_{i\_1},C_{i\_2},\ldots,C_{i\_t}\}$ είναι ένα επιλεγμένο υποσύνολο των κριτηρίων C που χρησιμοποιείται από ένα λήπτη αποφάσεων e_k, $e_k \in E$ για να εκφράσει την προτίμησή του σε ένα μέρος των κριτηρίων. $\bar{C} \subset C$, i_t<n. Τα κριτήρια στο $\bar{C}$ είναι ισοδύναμα και κυριαρχούν αυτών στα αριστερά του C. Τα κριτήρια στο $C/\bar{C}$ είναι επίσης ισοδύναμα μεταξύ τους.

Δεδομένου του επιλεγμένου υποσυνόλου των κριτηρίων C, $\bar{C}=\{C_{i\_1},C_{i\_2},\ldots,C_{i\_t}\}$, η σχέση πολλαπλασιαστικής προτίμησης σε οποιαδήποτε δύο κριτήρια C_i και C_j στο C μπορεί να οριστεί ως εξής:

p^k_{ij}=9 και $p^k_{jι}$=1/9, i,j=1,…,n;i≠j, if $C_i \in \bar{C}$, $C_j \in C/\bar{C}$
……..(4)

p^k_{ij}= $p^k_{jι}$=1, i,j=1,…,n, σε οποιαδήποτε άλλη περίπτωση.....(5)

5) ***Ένα ασαφώς επιλεγμένο υποσύνολο των κριτηρίων C.*** Έστω $\tilde{C}$ ={C_{i_1}, $l^k_{i\_1}$), (C_{i_2},$l^k_{i\_2}$),…,(C_{i_q},$l^k_{i\_q}$)}, i_q<n, είναι ένα ασαφώς επιλεγμένο υποσύνολο του C που χρησιμοποιείται από έναν λήπτη αποφάσεων e_k, $e_k \in$ E για να εκφράσει την προτίμησή του σε ένα υποσύνολο κριτηρίων χρησιμοποιώντας γλωσσολογικούς όρους. Σύμφωνα με τους Zhang και Ma (_) το $l^k_{i\_r}$ είναι γλωσσολογικός όρος όπου i_r=1,...,i_q.

Για παράδειγμα, ένας λήπτης αποφάσεων θεωρεί ότι το κριτήριο C_i είναι «καλό», το C_j είναι «πολύ καλό» και τα κριτήρια C_h και C_l είναι και τα δύο «μέτρια». Για οποιαδήποτε δύο κριτήρια C_i και C_j στο C, εάν και τα δύο ανήκουν στο $\tilde{C}$, όπου l^k_i=(u_i,a_i,β_i) και l^k_j=(u_j,a_j,β_j), η σχέση πολλαπλασιαστικής προτίμησης πάνω σε αυτά μπορεί να οριστεί ως εξής:

$p^k_{ij}=9^{u_i - u_j}$, με i,j=1,…,n;i≠j……(6)

Εάν κανένα από τα δύο κριτήρια C_i και C_j δεν ανήκουν στο $\tilde{C}$, τότε
p^k_{ij}=1, με i,j=1,…,n;i≠j.....(7)

Εάν το κριτήριο C_i ανήκει στο $\tilde{C}$ και το C_jδεν ανήκει στο $\tilde{C}$, τότε

$p^k_{ij}=9^{u_i - 0,5}$, με i,j=1,…,n;i≠j.....(8)

6) ***Σχέση κανονικής προτίμησης.*** Η σχέση κανονικής προτίμησης στα κριτήρια μπορεί να δοθεί από έναν λήπτη αποφάσεων για να εκφράσει τις αυστηρές προτιμήσεις του ανάμεσα στα κριτήρια. Για παράδειγμα, ο λήπτης αποφάσεων e_k, προτιμάει το κριτήριο Ci από το κριτήριο C_j και προτιμάει το κριτήριο C_c από τα κριτήρια C_t και C_h. Σε αυτή την περίπτωση, για τα κριτήρια

με αυστηρές σχέσεις προτίμησης, οι σχέσεις πολλαπλασιαστικής προτίμησης είναι 9 έναντι 1/9. Επομένως,

p^k_{ij}=9 και p^k_{jl}=1/9;p^k_{cl}=9 και p^k_{lc}=1/9;p^k_{ic}=1και p^k_{lh}=1.

7) ***Σχέση ασαφούς προτίμησης.*** Η σχέση προτίμησης του λήπτη αποφάσεων περιγράφεται από μία διμερή ασαφή σχέση F στο C, όπου η F είναι μία χαρτογράφηση CxC → [0,1] και το f_{ij} δηλώνει το βαθμό προτίμησης του κριτηρίου C_i στο κριτήριο Cj. H F θεωρείται ότι είναι συνδυαστική εξ ορισμού (Chiclana et al., 1998;Kacprzyk, 1992), (i) $f_{ij}+f_{ji}=1$, i,j=1,…,n;i≠j και (ii) f_{ii}=- (το '-' χρησιμοποιείται για να δείξει ότι ο λήπτης αποφάσεων δε χρειάζεται να δώσει καμία πληροφορία προτίμησης για το κριτήριο C_i), $\forall$ i.

Οι σχέσεις ασαφούς προτίμησης μπορούν να μετασχηματιστούν σε σχέσεις πολλαπλασιαστικής προτίμησης ως εξής:

$p^k_{ij}=\frac{f^k_{ij}}{f^k_{ji}}$, i,j=1,…,n……………………………………………………………(9)

Καθορίζοντας τα βάρη των κριτηρίων-Η μέθοδος του Simos (1990)

Στα πλαίσια των μεθόδων λήψης αποφάσεων ο καθορισμός των βαρών των διαφόρων κριτηρίων είναι δύσκολη υπόθεση. Διάφορες μέθοδοι μπορούν να χρησιμοποιηθούν για το σκοπό αυτό, όπως αναφέρουν οι Figueira και Roy (2002). Ο J.Simos πρότεινε μια πολύ απλή διαδικασία ώστε ο λήπτης αποφάσεων να ορίσει κατάλληλες αριθμητικές τιμές για τα βάρη, χρησιμοποιώντας κάρτες.

Σύμφωνα με τον Simos (1990), η τεχνική αυτή επιτρέπει στον λήπτη αποφάσεων (ακόμη κι όταν δεν έχει εμπειρία στη λήψη αποφάσεων) να αναλογιστεί τον τρόπο με τον οποίο θα εκφράσει την ιεράρχηση των διαφόρων κριτηρίων ενός συνόλου F στα πλαίσια ενός συγκεκριμένου προβλήματος. Η μέθοδος αυτή στοχεύει επίσης να μεταδώσει στον αναλυτή όλες τις πληροφορίες που χρειάζεται ώστε να οριστούν αριθμητικές τιμές στα βάρη κάθε κριτηρίου του συνόλου F. Η διαδικασία αυτή έχει εφαρμοστεί σε διάφορα πραγματικά προβλήματα και έχει γίνει αποδεκτή από πολλούς λήπτες αποφάσεων, γεγονός το οποίο δείχνει ότι οι πληροφορίες που γίνονται διαθέσιμες μέσω αυτής της διαδικασίας είναι ιδιαίτερα σημαντικές όσον

αφορά τις προτιμήσεις του λήπτη αποφάσεων. Ωστόσο, η μέθοδος του Simos έχει ορισμένα μειονεκτήματα: 1) βασίζεται σε μία μη-πραγματική υπόθεση. Αυτό προκύπτει από την έλλειψη ουσιωδών πληροφοριών , όπως τονίζεται από τον Scharlig (1996), 2) οδηγεί στην ελλιπή επεξεργασία στοιχείων της ίδιας σημαντικότητας (δηλαδή του ίδιου βάρους).

Η κύρια καινοτομία της μεθόδου αυτής του Simos (1990) έγκειται στη συσχέτιση μίας «κάρτας» με κάθε ένα κριτήριο. Το γεγονός ότι το άτομο που εξετάζεται πρέπει να χειριστεί τις κάρτες ώστε να τις κατατάξει εισάγοντας ορισμένες άσπρες κάρτες, επιτρέπει τη βαθύτερη κατανόηση του σκοπού της διαδικασίας αυτής.

Η συγκέντρωση των απαραίτητων πληροφοριών γίνεται σε τρία στάδια, ‘οπως αναφέρουν οι Figueira και Roy (2002):

1) Ένα πακέτο με n κάρτες δίνεται στο άτομο υπό εξέταση (τον χρήστη). Πάνω σε κάθε κάρτα γράφεται το όνομα κάθε κριτηρίου που ανήκει στο σύνολο κριτηρίων F μαζί με οποιαδήποτε συμπληρωματική πληροφορία που κρίνεται απαραίτητη. Επομένως, τα κριτήρια είναι επίσης n. Μαζί με τις κάρτες αυτές παρέχεται και ένα πακέτο με άσπρες κάρτες, ο αριθμός των οποίων εξαρτάται από τις ανάγκες του χρήστη.

2) Ο χρήστης, όπως εξηγούν οι Figueira και Roy (2002), ζητείται να κατατάξει τις κάρτες αυτές (δηλαδή τα κριτήρια) με αύξουσα σειρά από τη λιγότερο σημαντική στην πιο σημαντική, ανάλογα δηλαδή με τη σημαντικότητα που θέλει να αποδώσει σε κάθε κριτήριο. Το πρώτο κριτήριο στην κατάταξη είναι το λιγότερο σημαντικό και το τελευταίο είναι το πιο σημαντικό. Εάν κάποια κριτήρια είναι εξίσου σημαντικά για τον χρήστη, θα πρέπει να οριστεί ένα υποσύνολο καρτών.

3) Ο χρήστης ζητείται να αναλογιστεί το γεγονός ότι η σημαντικότητα δύο διαδοχικών κριτηρίων μπορεί να είναι σχεδόν ίδια. Στον καθορισμό των βαρών πρέπει να ληφθεί υπόψη αυτή η ελάχιστη διαφορά, για το λόγο αυτό ο χρήστης ζητείται να εισάγει τόσες περισσότερες άσπρες κάρτες μεταξύ δύο διαδοχικών καρτών όσο μεγαλύτερη είναι και η διαφορά της σημαντικότητας μεταξύ των κριτηρίων. Καμία άσπρη κάρτα σημαίνει ότι τα δύο κριτήρια δεν έχουν τα ίδια βάρη και ότι η διαφορά μεταξύ των βαρών μπορεί να οριστεί ως η μονάδα μέτρησης u μεταξύ των τάξεων. Μία κάρτα σημαίνει διαφορά 2u, δύο κάρτες σημαίνει διαφορά 3u κ.ο.κ.

Ο προσδιορισμός των βαρών των κριτηρίων σύμφωνα με τον Simos

Τη συγκέντρωση των πληροφοριών ακολουθεί ο καθορισμός των βαρών των κριτηρίων. Ο τρόπος που προτείνει ο Simos για την επεξεργασία των συγκεντρωμένων πληροφοριών αναλύεται από τους Maestre et al. (1994) με τη χρήση ενός παραδείγματος.

Ας θεωρήσουμε ένα σύνολο κριτηρίων F με 12 κριτήρια:

F={a,b,c,d,e,f,g,h,i,k,l}

Ας υποθέσουμε ότι ο χρήστης ομαδοποιεί τις κάρτες που συσχετίζονται με τα κριτήρια της ίδιας σημαντικότητας (ίδιο βάρος) σε 6 διαφορετικά υποσύνολα. Προκειμένου ο Simos (1990) να μετατρέψει τις τάξεις σε βάρη, προτείνει τον ακόλουθο αλγόριθμο:

1) Κατάταξη των υποσυνόλων από το λιγότερο καλό στο πιο καλό με τη χρήση των άσπρων καρτών.
2) Απόδοση μίας *θέσης (βάρους κατά τον Simos)* σε κάθε κριτήριο και σε κάθε άσπρη κάρτα: η κάρτα με τη μικρότερη κατάταξη παίρνει τη θέση 1, η επόμενη τη θέση 2 κ.ο.κ.
3) Προσδιορισμός του *μη-κανονικοποιημένου βάρους* (*μέσο βάρος κατά τον Simos)* κάθε τάξης διαιρώντας το άθροισμα των θέσεων της τάξης αυτής με το συνολικό αριθμό των κριτηρίων που ανήκουν στην τάξη αυτή.
4) Προσδιορισμός του *κανονικού βάρους (σχετικό βάρος κατά τον Simos)* κάθε κριτηρίου διαιρώντας το μη κανονικοποιημένο βάρος της τάξης με το συνολικό άθροισμα των θέσεων των κριτηρίων (χωρίς να ληφθούν υπόψη οι άσπρες κάρτες).

Στη περίπτωση που μελεταμε, έγιναν οι σχετικές ερωτήσεις για τα βάρη των κριτηρίων σε μια ομάδα ατόμων τα οποία έχουν γνώσεις για το θέμα μας, καθώς επίσης και έχουν αγοράσει κάποια απο τα κρυπτονομίσματα.

Η επιλογή των κριτηρίων έγινε με βάση τη δική τους κρίση καθώς και βασιζόμενος σε πληροφορίες που συγκέντωσα για τα κρυπτονομίσματα και απο το πόσο σημαντικο είναι κάθε κριτήριο για μία μονάδα νομίσματος.

Τα κριτήρια που έχουν επιλεχθεί για τη συγκεκριμένη ερευνητική μελέτη είναι τρία και όλα τους αριθμητικά: πρώτον, είναι ο όγκος των χρηματιστηριακών συναλλαγών(**Volume**), ένα πολύ σημαντικό κριτήριο για την συναγωγή συμπερασμάτων για την χρηματοοικονομική αξία ενός προϊόντος εισηγμένου στο χρηματιστήριο, όπως ενός νομίσματος. Σε αυτό το κριτήριο το βάρος(weight) που έχει τεθεί είναι 2,00.

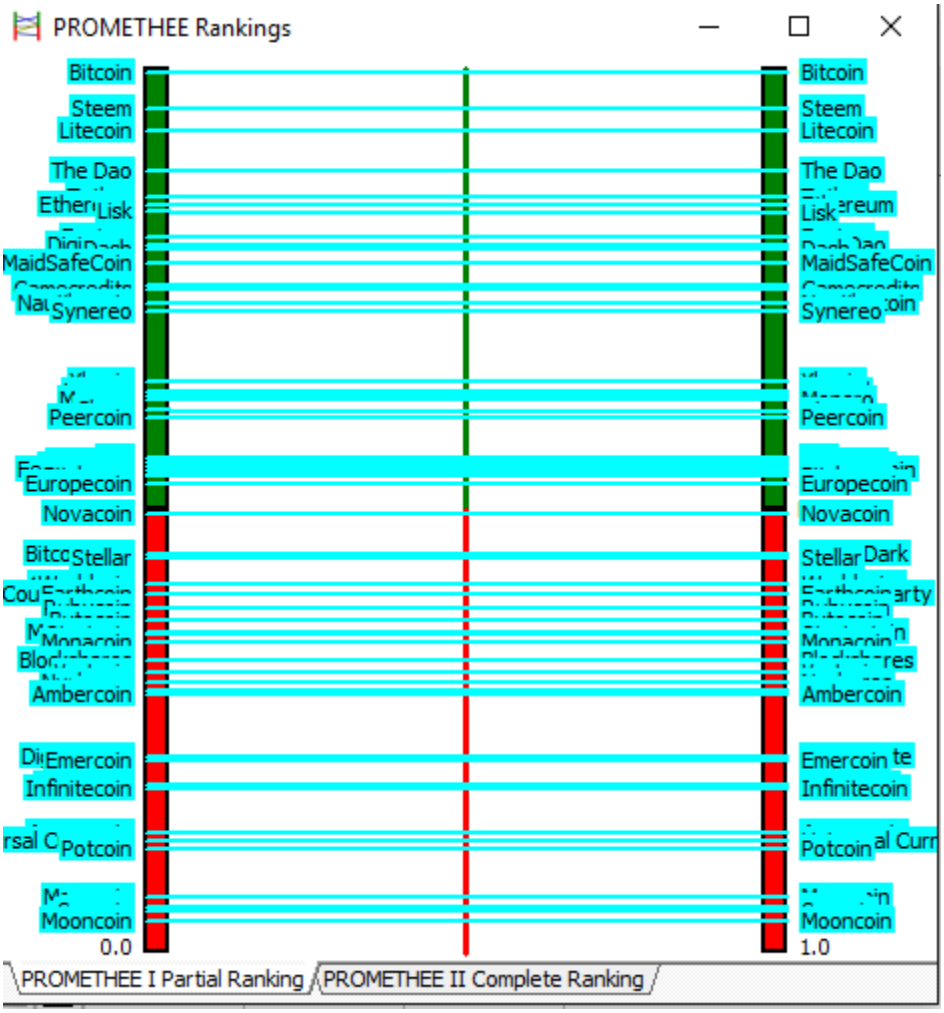
Σαν ‘αποφασίζων’ στο πρόβλημα μου θα ορίσω αυτό το κριτήριο δηλαδή τον όγκο των χρηματιστηριακών συναλλαγών. Κατα τη γνώμη μου, η επιλογή αυτή είναι θεμιτή αφού το κριτήριο αυτό περιγράφει την ποσότητα απο κάθε νόμισμα που ‘κινείται’ στην αγορά, άρα με λίγα λόγια μια ‘προτίμηση’ που πηγάζει απο το κοινό.

Τα δύο υπόλοιπα κριτήρια είναι η κεφαλαιοποίηση της αγοράς(**Market Cap.** ή Market Capitalization) και, τέλος, η τιμή τους στην αγορά(**Price**). Τα δύο αυτά κριτήρια είναι αλληλένδετα, εφόσον η κεφαλαιοποίηση δεν είναι άλλο από το γινόμενο του αριθμητικού πλήθους των μετοχών και στην προκειμένη περίπτωση του συνόλου των κυκλοφορούντων κρυπτονομισμάτων επί την τιμή αγοράς του καθενός.

Επειδή αυτά τα κριτήρια είναι αλληλένδετα και επομένως η «πληροφορία» που φέρουν είναι παρεμφερής, θεωρήθηκε σκόπιμο και καλύτερη προσέγγιση το βάρος τους ως κριτηρίων να είναι ίσο με 1,00 για το καθένα. Παρ'όλ'αυτά, θα εξεταστεί και μια εναλλακτική περίπτωση με ίσα βάρη για κάθε ένα από τα κριτήρια. Οι σταθμίσεις αυτές αντιστοιχούν στο τρίτο από τα στοιχεία που προαναφέρθηκαν και το οποίο είναι οι ***«προτιμήσεις»*****(Preferences)**

Εφόσον έχουν λοιπόν εισαχθεί όλα τα στοιχεία στον πίνακα "Evaluations", πλέον είναι εφικτή η κατάταξή τους με βάση τα πρότυπα PROMETHEE I και PROMETHEE II. Δεδομένης της προτίμησής μας στο δεύτερο, όπως εξηγήθηκε αρχικά, επιλέξαμε από το μενού την εξαγωγή των αποτελεσμάτων για τις κατατάξεις PROMETHEE, δηλαδή την επιλογή **"Promethee Rankings"**, η οποία βρίσκεται πρώτη στα αριστερά στην κάτω σειρά των εικονιδίων, και το αποτέλεσμα είναι αυτό της παρακάτω εικόνας(Εικόνα 9):

9. Κατατάξεις PROMETHEE II



Με δεδομένο ότι στην μέθοδο PROMETHEE II, η κατάταξη βασίζεται στην υψηλότερη τιμή του Φ, η οποία δίνεται στην εικόνα 9, τις καλύτερες θέσεις λαμβάνουν τα εξής κρυπτονομίσματα:

1)Bitcoin

2)Steem

3)Litecoin

4)The Dao

5)Tether

6)Ethereum

7)Lisk

Αντιθέτως, στην τελευταία θέση βρίσκεται το Mooncoin.

10. Κατατάξεις κατά PROMETHE-εναλλακτικές προτιμήσεις(preferences)

Προκειμένου να έχουμε μια πληρέστερη εικόνα των επιδόσεων των κρυπτονομισμάτων, πραγματοποιείται και μια επιπλέον εναλλακτική κατάταξη και αξιολόγηση. Έτσι, αντί του βάρους(weight) 2,00 στο πρώτο κριτήριο του όγκου των συναλλαγών(Volume), ανατέθηκε βάρος 1,00. Με αυτόν τον τρόπο, τις καλύτερες θέσεις λαμβάνουν τα ακόλουθα, κατά σειρά, κρυπτονομίσματα:

1)Bitcoin

2)Steem

3)Litecoin

4)The Dao

5)Digix Dao

6)Factom

Οι διαφορές παρατηρούνται με εντονοποιημένους(bold) χαρακτήρες κάτω από την $4^{η}$ θέση της βέλτιστης βαθμολογίας **Phi,** ενώ και πάλι την τελευταία θέση καταλαμβάνει το κρυπτονόμισμα *Mooncoin*. Πιστοποιείται λοιπόν ότι και με τα δύο είδη κριτηρίων τις καλύτερες επιδόσεις έχουν τα κρυπτονομίσματα Bitcoin, Steem, Litecoin και The Dao.

Με την ανάλυση των αποτελεσμάτων και της παραπάνω εναλλακτικής στάθμισης των κριτηρίων, ολοκληρώνεται αυτό το κεφάλαιο, το οποίο αφιερώθηκε στην μελέτη της συσταδοποίησης και κατάταξης-αποτίμησης των κρυπτονομισμάτων, με βάση τα λογισμικά Weka και Visual Promethee αντίστοιχα.

5 ΑΠΟΤΕΛΕΣΜΑΤΑ

5.1 ΕΠΙΛΟΓΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ

Αρχικά θα πρέπει να επιλέξουμε τα χαρακτηριστικά των κρυπτονομισμάτων που θα συμμετάσχουν στην κατηγοριοποίηση μας. Η διαδικασία αυτή είναι σημαντική, ούτως ώστε να λάβουμε ένα σύνολο δεδομένων που θα μας βοηθήσει στο να δημιουργήσουμε ομαδοποίηση των δεδομένων με μεγάλη ακρίβεια. Αυτό γίνεται με το μοντέλο attribute selection. Οι είσοδοι του μοντέλου είναι η αρχική βάση δεδομένων και οι ρυθμίσεις που γίνονται αφορούν σε classifier τύπου Naivebayes.

Η διαδικασία αυτή εκτελείται για όλες τις κατηγορικές μεταβλητές (αλγόριθμος, hash, ασφάλεια και αποπληθωρισμός). Τα αποτελέσματα παρουσιάζονται στο Παράρτημα Γ.

Τα χαρακτηριστικά που επιλέγονται, καθώς εκτιμάται ότι θα μας δώσουν καλή κατηγοριοποίηση είναι τα εξής:

- Προσφορά
- Μηχανισμός ασφάλειας
- Αλγόριθμος hash
- Αποπληθωρισμός
- Αλλαγή αξίας 24h (%)

5.2 ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ – ΟΜΑΔΟΠΟΙΗΣΗ

Αρχικά χρησιμοποιείται το μοντέλο της κατηγοριοποίησης, ώστε να προκύψει η ακρίβεια της κατηγοριοποίησης που φτάνει το 60% (Παράρτημα Γ).

5.2.1 Δημιουργία δύο ομάδων

Στη συνέχεια τα δεδομένα ομαδοποιούνται σε δύο ομάδες, έχοντας αφαιρέσει τα χαρακτηριστικά που δεν συμβάλλουν στην ομαδοποίηση (όπως εξηγείται στην παράγραφο 5.1) και προκύπτουν τα εξής:

Χαρακτηριστικό	**Full Data**	**Ομάδες**	
	27	14	13
Αλγόριθμος hash	SHA-256d	SHA-256d	N/A
Μηχανισμός ασφαλείας	POW	POW	POS
Προσφορά	2635931380.963	4482704384.8571	647098915.2308
Αλλαγή	0.787	3.2886	-1.9069
Αποπληθωρισμός	N/A	YES	N/A

Πίνακας 8 Ομαδοποίηση δεδομένων σε δύο ομάδες

Ο παραπάνω πίνακας δείχνει τα αποτελέσματα της ομαδοποίησης. Δίνονται οι πιο πιθανές τιμές των μεταβλητών για το σύνολο των κρυπτονομισμάτων και για κάθε ομάδα κρυπτονομισμάτων. Τα αποτελέσματα αυτά σημαίνουν ότι τα κρυπτονομίσματα της βάσης δεδομένων χαρακτηρίζονται από αλγόριθμο κατακερματισμού (hash) τύπου SHA-256d, μηχανισμό ασφαλείας POW και διαθέσιμη προσφορά νομισμάτων περί τα 2635 εκατομμύρια. Η αλλαγή 24ώρου στην αξία των κρυπτονομισμάτων είναι κατά βάση θετική και ίση με 0,78%, ενώ η δυνατότητα αποπληθωρισμού είναι αβέβαιη.

Μέσα σε αυτή την πλήρη ομάδα με τα παραπάνω χαρακτηριστικά, μπορούμε να ξεχωρίσουμε 2 ομάδες. Η πρώτη περιλαμβάνει 14 κρυπτονομίσματα με αλγόριθμο κατακερματισμού (hash) τύπου SHA-256d, μηχανισμό ασφαλείας POW και διαθέσιμη προσφορά νομισμάτων περί τα 4482 εκατομμύρια. Η αλλαγή 24ώρου στην αξία των κρυπτονομισμάτων είναι θετική και ίση με 3,29%, ενώ υπάρχει δυνατότητα αποπληθωρισμού. Η δεύτερη ομάδα περιλαμβάνει 13 κρυπτονομίσματα με κάποιον άγνωστο αλγόριθμο κατακερματισμού (hash), μηχανισμό ασφαλείας POS και διαθέσιμη προσφορά νομισμάτων περί τα 647 εκατομμύρια. Η αλλαγή 24ώρου στην αξία των κρυπτονομισμάτων είναι αρνητική και ίση με -1.9%, ενώ δεν υπάρχει δυνατότητα αποπληθωρισμού.

Το σφάλμα ομαδοποίησης είναι 38%. Δημιουργώντας περισσότερες ομάδες, θα μειωθεί το σφάλμα ομαδοποίησης.

5.2.2 Δημιουργία τριών ομάδων

Στη συνέχεια τα δεδομένα ομαδοποιούνται σε τρεις ομάδες, έχοντας αφαιρέσει τα χαρακτηριστικά που δεν συμβάλλουν στην ομαδοποίηση (όπως εξηγείται στην παράγραφο 5.1) και προκύπτουν τα εξής:

Πίνακας 9 Ομαδοποίηση δεδομένων σε τρεις ομάδες

Χαρακτηριστικό	**Ομάδες**		
	11	5	11
Αλγόριθμος hash	SHA-256d	N/A	Scrypt
Μηχανισμός ασφαλείας	POW	N/A	POS
Προσφορά	5698683617.4545	1477843249.8	99582840.4545
Αλλαγή	1.69	0.904	-0.17
Αποπληθωρισμός	N/A	YES	N/A

Ο παραπάνω πίνακας δείχνει τα αποτελέσματα της ομαδοποίησης. Δίνονται οι πιο πιθανές τιμές των μεταβλητών για το σύνολο των κρυπτονομισμάτων και για κάθε ομάδα κρυπτονομισμάτων. Τα αποτελέσματα για τα κρυπτονομίσματα της βάσης δεδομένων είναι όμοια με αυτά της παραγράφου 5.2.1.

Από τη βάση δεδομένων με τα παραπάνω χαρακτηριστικά, μπορούμε να ξεχωρίσουμε 3 ομάδες. Η πρώτη περιλαμβάνει 11 κρυπτονομίσματα με αλγόριθμο κατακερματισμού (hash) τύπου SHA-256d, μηχανισμό ασφαλείας POW και διαθέσιμη προσφορά νομισμάτων περί τα 5698 εκατομμύρια. Η αλλαγή 24ώρου στην αξία των κρυπτονομισμάτων είναι θετική και ίση με 1.6%, ενώ υπάρχει δυνατότητα αποπληθωρισμού.

Η δεύτερη ομάδα περιλαμβάνει 5 κρυπτονομίσματα με κάποιον άγνωστο αλγόριθμο κατακερματισμού (hash), άγνωστο μηχανισμό ασφαλείας και διαθέσιμη προσφορά νομισμάτων περί τα 1477 εκατομμύρια. Η αλλαγή 24ώρου στην αξία των κρυπτονομισμάτων είναι θετική και ίση με 0.9%, ενώ η δυνατότητα αποπληθωρισμού είναι αβέβαιη.

Η τρίτη ομάδα περιλαμβάνει 11 κρυπτονομίσματα με αλγόριθμο κατακερματισμού (hash) τύπου Scrypt, μηχανισμό ασφαλείας POS και διαθέσιμη προσφορά νομισμάτων περί τα 99 εκατομμύρια. Η αλλαγή 24ώρου στην αξία των

κρυπτονομισμάτων είναι αρνητική και ίση με 0.17%, ενώ η δυνατότητα αποπληθωρισμού είναι αβέβαιη.

Το σφάλμα ομαδοποίησης είναι 34%.

5.2.3 Δημιουργία τεσσάρων ομάδων

Στη συνέχεια τα δεδομένα ομαδοποιούνται σε τέσσερις ομάδες, έχοντας αφαιρέσει τα χαρακτηριστικά που δεν συμβάλλουν στην ομαδοποίηση (όπως εξηγείται στην παράγραφο 5.1) και προκύπτουν τα εξής:

Χαρακτηριστικό	**Ομάδες**			
	9	4	5	9
Αλγόριθμος hash	SHA-256d	N/A	N/A	Scrypt
Μηχανισμός ασφαλείας	POW	N/A	POS	POW/ POS
Προσφορά	6961844637.5556	1844133529.5	175922128.8	28600087.3333
Αλλαγή	2	-0.37	-3.37	2.29
Αποπληθωρισμός	N/A	YES	N/A	N/A

Πίνακας 10 Ομαδοποίηση δεδομένων σε τρεις ομάδες

Ο παραπάνω πίνακας δείχνει τα αποτελέσματα της ομαδοποίησης. Δίνονται οι πιο πιθανές τιμές των μεταβλητών για το σύνολο των κρυπτονομισμάτων και για κάθε ομάδα κρυπτονομισμάτων. Τα αποτελέσματα για τα κρυπτονομίσματα της βάσης δεδομένων είναι όμοια με αυτά της παραγράφου 5.2.1.

Από τη βάση δεδομένων με τα παραπάνω χαρακτηριστικά, μπορούμε να ξεχωρίσουμε 4 ομάδες. Η πρώτη περιλαμβάνει 9 κρυπτονομίσματα με αλγόριθμο κατακερματισμού (hash) τύπου SHA-256d, μηχανισμό ασφαλείας POW και διαθέσιμη προσφορά νομισμάτων περί τα 6961 εκατομμύρια. Η αλλαγή 24ώρου στην αξία των κρυπτονομισμάτων είναι θετική και ίση με 2%, ενώ η δυνατότητα αποπληθωρισμού είναι αβέβαιη.

Η δεύτερη ομάδα περιλαμβάνει 4 κρυπτονομίσματα με κάποιον άγνωστο αλγόριθμο κατακερματισμού (hash), άγνωστο μηχανισμό ασφαλείας και διαθέσιμη προσφορά νομισμάτων περί τα 1844 εκατομμύρια. Η αλλαγή 24ώρου στην αξία των κρυπτονομισμάτων είναι αρνητική και ίση με -0.37%, ενώ η δυνατότητα αποπληθωρισμού είναι θετική.

Η τρίτη ομάδα περιλαμβάνει 5 κρυπτονομίσματα με κάποιον άγνωστο αλγόριθμο αλγόριθμο κατακερματισμού (hash), μηχανισμό ασφαλείας POS και διαθέσιμη προσφορά νομισμάτων περί τα 175 εκατομμύρια. Η αλλαγή 24ώρου στην αξία των κρυπτονομισμάτων είναι αρνητική και ίση με -3.37%, ενώ η δυνατότητα αποπληθωρισμού είναι αβέβαιη.

Το σφάλμα ομαδοποίησης είναι 30%.

5.3 ΑΝΑΛΥΣΗ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Αξιοποιώντας την βάση δεδομένων που δημιουργήσαμε, αναλύουμε τα δεδομένα των χαρακτηριστικών για 27 διαφορετικά κρυπτονομίσματα που εισήχθησαν στην αγορά πριν το 2015 και έχουν κεφαλαιοποίηση άνω του 1 εκατομμυρίου δολαρίων. Οι είσοδοι του μοντέλου είναι η αρχική βάση δεδομένων και οι ρυθμίσεις που γίνονται αφορούν σε classifier τύπου Naivebayes. Τα χαρακτηριστικά που επελέγησαν, για τη βέλτιστη ομαδοποίηση είναι η Προσφορά, ο Μηχανισμός ασφάλειας, ο Αλγόριθμος hash, ο Αποπληθωρισμός και η Αλλαγή αξίας 24h (%). Το σύνολο των χαρακτηριστικών αυτών συμφωνούν με την ανάλυση του Farell (2015), εκτός από την αλλαγή αξίας 24h (%), που προστίθεται στη δική μας ανάλυση.

Κατά την ομαδοποίηση, παρατηρούμε ότι το σφάλμα μειώνεται αυξάνοντας το πλήθος των ομάδων, καθώς έτσι επιτυγχάνεται μεγαλύτερη ακρίβεια στην ομαδοποίηση.

Σε κάθε ομαδοποίηση, η ομάδα με αλγόριθμο κατακερματισμού (hash) τύπου SHA-256d και μηχανισμό ασφαλείας POW συνδέεται με υψηλή προσφορά και θετική αλλαγή της ισοτιμίας του κρυπτονομίσματος σε δολάρια αμερικής. Η δυνατότητα αποπληθωρισμού επίσης συνδέεται με τη θετική αλλαγή της ισοτιμίας. Ο μηχανισμός ασφαλείας POS, αντίθετα, συσχετίζεται με πολύ αρνητικές αλλαγές ισοτιμίας και περιορισμένη προσφορά κρυπτονομισμάτων. Ο αλγόριθμος scrypt με μηχανισμό ασφαλείας POW/POS συσχετίζεται με αύξηση της ισοτιμίας και υψηλή προσφορά νομισμάτων.

6 ΣΥΜΠΕΡΑΣΜΑΤΑ

Παρά το γεγονός ότι η ιδέα των ηλεκτρονικών νομισμάτων χρονολογείται από τα τέλη της δεκαετίας του 1980, το Bitcoin, που ξεκίνησε το 2009, είναι το πρώτο επιτυχημένο αποκεντρωμένο κρυπτονόμισμα. Εν ολίγοις, ένα κρυπτονόμισμα είναι ένα εικονικό σύστημα κερμάτων που λειτουργεί σαν ένα τυπικό νόμισμα, επιτρέποντας στους χρήστες να κάνουν εικονικές πληρωμές για αγαθά και υπηρεσίες χωρίς κεντρική αξιόπιστη αρχή. Τα κρυπτονομίσματα βασίζονται στην μετάδοση των ψηφιακών πληροφοριών, με τη χρήση κρυπτογραφικών μεθόδων για τη διασφάλιση της νομιμότητας των συναλλαγών. Το Bitcoin ενίσχυσε την ανάπτυξη της ψηφιακής αγοράς νομισμάτων, αποκεντρώνοντας το κρυπτονόμισμα και απελευθερώνοντας το από ιεραρχικές δομές εξουσίας. Οι ιδιώτες και οι επιχειρήσεις συναλλάσσονται με το ηλεκτρονικά νομίσματα σε ένα δίκτυο peer-to-peer. Το Bitcoin προσέλκυσε τη προσοχή του ευρύ κοινού από το 2011, και διάφορα εναλλακτικά κρυπτονομίσματα - μια γενική ονομασία για όλα τα άλλα ψηφιακά νομίσματα μετά Bitcoin - εμφανίστηκαν σύντομα.

Το Litecoin κυκλοφόρησε το φθινόπωρο του 2011, κερδίζοντας μέτρια επιτυχία και απολαμβάνοντας την υψηλότερη κεφαλαιοποίηση μετά το Bitcoin μέχρι να ξεπεραστεί από το Ripple στις 4 Οκτωβρίου, 2014. Το Litecoin χρησιμοποιεί ένα τροποποιημένο πρωτόκολλο Bitcoin, αυξάνοντας την ταχύτητα των συναλλαγών με την ιδέα ότι θα ήταν πιο κατάλληλο για καθημερινές συναλλαγές. Το Ripple, που ξεκίνησε το 2013, παρουσιάζει ένα εντελώς μοναδικό μοντέλο σε σχέση με αυτό που χρησιμοποιείται από Bitcoin και σήμερα διατηρεί τη δεύτερη υψηλότερη κεφαλαιοποίηση. Ένα άλλο σημαντικό κρυπτονόμισμα στην εξελικτική αλυσίδα των ψηφιακών νομισμάτων, είναι το Peercoin, που χρησιμοποιεί μια επαναστατική τεχνολογική ανάπτυξη για να εξασφαλίσει και να διατηρήσει την εξόρυξη νομισμάτων. Το Peercoin συγχωνεύει την τεχνολογία Pow που χρησιμοποιείται από Bitcoin και Litecoin μαζί με το δικό του μηχανισμό PoS, καταλήγοντας έτσι σε έναν υβριδικό μηχανισμό ασφαλείας POW/POS. Πιο πρόσφατα εισήχθησαν στην αγορά τα κρυπτονομίσματα NuShares / NuBits (Αύγουστος 2014), τα οποία βασίζονται σε

ένα μοντέλο διπλού νομίσματος που έχει σχεδόν εξ ολοκλήρου διαχωριστεί από το πρότυπο του ενιαίου νομίσματος που χρησιμοποιείται από τα προηγούμενα νομίσματα.

Η βιομηχανία των κρυπτονομισμάτων αποτελείται από περίπου 550 νομίσματα με διαφορετικές βάσεις χρηστών και όγκο εμπορικών συναλλαγών. Λόγω της υψηλής μεταβλητότητας της ίδιας της αγοράς και των συνεχώς νέων εισαγόμενων νομισμάτων, η μεταβλητότητα της απόδοσης του κάθε κρυπτονομίσματος είναι μεγάλη. Επίσης, λόγω της έλλειψης ρυθμιστικών πλαισίων, της περιορισμένης αποδοχής και του μικρού χρόνου ωρίμανσης της αγοράς, δεν γίνεται συστηματική ακαδημαϊκή έρευνα και δεν υπάρχει μεγάλος όγκος επιστημονικής βιβλιογραφίας σχετικά με την αξιολόγηση των νομισμάτων.

Στην παρούσα εργασία, στόχος ήταν η διερεύνηση των χαρακτηριστικών και η αξιολόγηση των κρυπτονομισμάτων με βάση τις μεταβλητές που επελέγησαν, με στόχο να εξαχθούν συμπεράσματα της συσχέτισης μεταξύ των μεταβλητών. Για την ανάλυση επελέγησαν κρυπτονομίσματα που έχουν κεφαλαιοποίηση τουλάχιστον 1 εκατομμύριο δολάρια τον Δεκέμβριο του 2015 και έχουν διανεμηθεί πριν από τον Ιανουάριο του 2015, ώστε να υπάρχει αρκετός χρόνος ωρίμανσης. Πηγή δεδομένων είναι οι διαδικτυακοί τόποι coinmarketcap.com και cryptocoin.cc.

Η ανάλυση έγινε με το λογισμικό Weka, που είναι μια πλατφόρμα εργασίας η οποία περιέχει μια συλλογή από εργαλεία απεικόνισης και αλγορίθμων για την ανάλυση δεδομένων και την προγνωστική μοντελοποίηση, μαζί με γραφικά περιβάλλοντα χρήστη για εύκολη πρόσβαση σε αυτές τις λειτουργίες. Τα στάδια ανάλυσης περιλαμβάνουν την επιλογή χαρακτηριστικών, την κατηγοριοποίηση και την ομαδοποίηση. Από την ανάλυση προέκυψαν χρήσιμα συμπεράσματα σχετικά με την συσχέτιση των χαρακτηριστικών των κρυπτονομισμάτων. Συγκεκριμένα βρέθηκε ότι η ομάδα με αλγόριθμο κατακερματισμού (hash) τύπου SHA-256d και μηχανισμό ασφαλείας POW συνδέεται με υψηλή προσφορά και θετική αλλαγή της ισοτιμίας του κρυπτονομίσματος σε δολάρια αμερικής. Επίσης, ο αλγόριθμος scrypt με μηχανισμό ασφαλείας POW/POS συσχετίζεται με αύξηση της ισοτιμίας και υψηλή προσφορά νομισμάτων.

7 ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Ahamad S., Nair, M. and Varghese, B., (2013) " A Survey on Crypto Currencies" Proc. of Int. Conf. on Advances in Computer Science, AETACS.
2. Anonymous. 4/17/14. "BlackCoin rolls out fantastic features as its value skyrockets more than 215% in one week." PR Web. Accessed on 4/22/14. http://www.prweb.com/releases/2014/04/prweb11772516.htm.
3. Badev and Chen (2014). Bitcoin: Technical Background and Data Analysis. Finance and Economics Discussion Series, Divisions of Research & Statistics and Monetary Affairs, Federal Reserve Board, Washington, D.C.
4. Benaloh, J., Michael de Mare (1994) One-way Accumulators: A Decentralized Alternative to Digital Signatures. In EUROCRYPT '93, Lecture Notes in Computer Science, 765: 274–85. www.cs.stevens.edu/~mdemare/pubs/owa.pdf
5. Bennenbroek, N. (2014) Bitcoin 101: A Primer. UBS
6. Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M. (2014) Zerocash: Decentralized Anonymous Payments from Bitcoin. In IEEE Symposium on Security and Privacy (Oakland). zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf
7. Ben-Sasson, E., Chiesa, A., Genkin, D., Tromer, E., Virza, M. (2013) SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge. In Proceedings of the 33rd Annual International Cryptology Conference, CRYPTO '13: 90–108. eprint.iacr.org/2013/507.pdf
8. Bernstein, D. (2014) Irrelevant Patents on Elliptic-curve Cryptography, retrieved July 2014, cr.yp.to/ecdh/patents.html
9. Bernstein, D., Buchmann, J., Dahmen, E. (2008) Post-Quantum Cryptography. Springer.

10. Bitcoin Documentation (2014) Working with Micropayment Channels, retrieved July 2014, bitcoinj.github.io/working-with-micropayments

11. Bloom, B. (1970) “Space/Time Trade-off in Hash Coding with Allowable Errors.” Communications of the ACM, 13(7): 422–6.

12. Blundell-Wignall, A. (2014), “The Bitcoin Question: Currency versus Trust-less Transfer Technology”, *OECD Working Papers on Finance, Insurance and Private Pensions*, No. 37, OECD Publishing. http://dx.doi.org/10.1787/5jz2pwjd9t20-en

13. Bradbury, D. (2014b) Bitcoin Core Development Falling Behind, Warns BitcoinJ’s Mike Hearn. CoinDesk. www.coindesk.com/bitcoin-core-development-falling-behind-warns-mike-hearn/

14. Brands, S. (1993) Untraceable Off-line Cash in Wallets with Observers.

15. Brito, J., Castillo, A. (2013) Bitcoin—A Primer for Policymakers. Mercatus Center, George Mason University. mercatus.org/sites/default/files/Brito_BitcoinPrimer_embargoed.pdf

16. Brito, J., Shadab, H., Castillo, A. (2014) Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling.

17. Brown, R. (2013) A Simple Explanation of How Money Moves around the Banking System. gendal.wordpress.com/2013/11/24/a-simple-explanation-of-how-money-moves-around-the-bankingsystem/

18. Brown, R. (2014a) How I Explain Bitcoin and Cryptocurrencies to New Audiences. gendal.wordpress.com/2014/03/27/how-i-explain-bitcoin-and-cryptocurrencies-to-new-audiences/

19. Brown, R. (2014b) A Decentralized Securities Trading and Settlement System is Being Built Hidden in Plain Sight. gendal.wordpress.com/2014/06/10/a-decentralized-securities-tradingand-settlement-system-is-being-built-hidden-in-plain-sight/

20. Brown, R. (2014c) Who Will Decide the Future of Retail Payments?. IBM Insights on Business. insights-on-business.com/banking/who-will-decide-the-future-of-retail-payments/

21. Bruce, J.D. (2013) Purely P2P Crypto-Currency with Finite Mini-Blockchain. www.bitfreak.info/files/pp2p-ccmbc-rev1.pdf

22. Buterin, V. (2013a) Bitcoin Network Shaken by Blockchain Fork. Bitcoin Magazine. bitcoinmagazine.com/3668/bitcoin-network-shaken-by-blockchain-fork/

23. Buterin, V. (2013b) Critical Vulnerability Found In Android Wallets. Bitcoin Magazine. bitcoinmagazine.com/6251/critical-vulnerability-found-in-android-wallets/

24. Buterin, V. (2013c) Introducing Ripple. Bitcoin Magazine. bitcoinmagazine.com/3506/introducingripple/

25. Buterin, V. (2013d) Why The Bitcoin Greenlist is Structurally Dangerous to the Bitcoin Ecosystem. bitcoinmagazine.com/8204/why-the-bitcoin-greenlist-is-structurally-dangerous-to-the-bitcoinecosystem/

26. Caesar, C. 5/8/14. “Bitcoins for Political Donations?” Boston.com. Accessed on 5/8/2014. http://www.boston.com/news/politics/2014/05/08/bitcoins-for-political-donations/T0gHDLPyicHMEOAp9FOUoO/story.html?rss_id=Top-GNP.

27. CFA (2015) “CRYPTO-CURRENCIES-Intellectual Curiosity or the Future of Finance?” Policy Brief.

28. Delono, John. November 9, 2013. Bitcoin Simply Cannot Replace Fiat. DOI= http://letstalkbitcoin.com/bitcoinsimply-cannot-replace-fiat/.

29. Farell (2015). An Analysis of the Cryptocurrency Industry. Wharton Research Scholars Journal. Paper 130.

    http://repository.upenn.edu/wharton_research_scholars/130

30. FinCen (2013), “Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies”.

31. Friedman, M. and A. Schwartz (1963). *A Monetary History of the United States, 1867-1960*. Princeton: Princeton University Press.

32. Goldman Sachs (2014), "All About Bitcoin", in *Top of Mind*, March 11.

33. Gourov (2014). Measuring the Intrinsic Value of Cryptocurrency. Proposed valuation methodology for Digital Currencies. [online] https://www.dropbox.com/s/9l63jc4yldnaeu7/Measuring%20the%20Intrinsic%20Value%20of%20Cryptocurrency.pdf

34. Greydon, (2014). What is Cryptocurrency. US Consumer Research Survey. https://www.cryptocoinsnews.com/cryptocurrency/

35. Jerry Brito and Andrea Castillo (2013). "Bitcoin: A Primer for Policymakers". Mercatus Center. George Mason University. Retrieved 22 October 2013

36. Meiklejohn, S.; Pomarole, M.; Savage, S. "A fistful of Bitcoins: Characterizing payments among men with no names." University of California, San Diego. Accessed on 4/27/14. http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf.

37. Newcomb, A. 5/7/2014. "5 Bitcoin Warning Signs In New Federal Investor Alert." ABC News. Accessed on 5/8/14. http://abcnews.go.com/blogs/business/2014/05/5-bitcoin-warning-signs-in-new-federal-investor-alert/.

38. Pagliery, Jose. September 26, 2014. Paypal now lets shops accept Bitcoin. http://money.cnn.com/2014/09/26/technology/paypalbitcoin/.

39. Philips, Matthew. March 20, 2014. Bitcoin Isn't Banned in China—and It's Quickly Gaining Ground. Program. http://www.businessweek.com/articles/2014-03-20/btcchinas-bobby-lee-Bitcoin-isnt-really-banned-in-china-andits-quickly-gaining-ground.

40. Richardson, G., A. Komai and M. Gou (2013), "Roosevelt's Gold Program: Spring 1933", in: 100 Years of the Federal Reserve System, http://www.federalreservehistory.org/Events/DetailView/24.

41. Segendorf, B. (2014) " What is Bitcoin?" Sveriges Riksbank Economic Review.

42. Sharf, S. (2013) “Bitcoin Gets Valued: Bank of America Puts a Price Target on the Virtual Tender”, Forbes Magazine, 12 May 2013.

43. The Bitcoin Foundation (2014a) Bitcoin Developer Guide, retrieved July 2014, bitcoindev.us.to/en/developer-guide

44. The Bitcoin Foundation(2014b) Bitcoin Developer Reference, retrieved July 2014, bitcoindev.us.to/en/developer-reference

ΠΑΡΑΡΤΗΜΑ Α

Έκδοση	Όνομα	Αλγόριθμος Hash	Μηχανισμός ασφαλείας	Κεφαλαιο-ποίηση ($)	Αξία ($)	Προσφορά (πλήθος νομισμάτων)	Όγκος συναλλαγών (24h)	Αλλαγή στην αξία (24h) %	Αντιπλη-θωρισμός
2009	Bitcoin	SHA-256d	POW	6960918625	464,69	14.979.575	42451700	1,14	NAI
2013	Ripple	ECDSA	Consensus	212823563	0,006346	33.537.439.933	580599	-1,85	NAI
2011	Litecoin	Scrypt	POW	164072041	3,76	43.668.235	1168340	0,34	NAI
2014	Dogecoin	Scrypt	POW	16134235	0,000158	102.292.155.305	130831	2,99	ΟΧΙ
2014	Dash	X11	POW & POS	15910032	2,62	6.071.604	22555	1,14	NAI
2012	Peercoin	SHA-256d	POW & POS	10166373	0,444987	22.846.450	33617	-1,41	ΟΧΙ
2014	BitShares	N/A	N/A	9415373	0,003713	2.535.621.961	24452	0,56	N/A
2014	Stellar	N/A	Consensus	9032070	0,001867	4.837.356.606	7598	0,96	ΟΧΙ
2013	Nxt	SHA-256d	POS	6703841	0,006704	999.997.096	9205	3,73	NAI
2011	Namecoin	SHA-256d	POW	6431007	0,488374	13.168.200	12529	10,45	NAI
2012	Bytecoin	CryptoNight	POW	5540150	0,000031	178.051.130.022	6282	0,8	NAI
2014	Monero	CryptoNight	POW	5177458	0,496892	10.419.684	15497	-1,25	NAI
2014	NuShares	N/A	POS	4111817	0,005015	819.887.419	693	-1,8	NAI
2014	Rubycoin	Scrypt	POS	2727380	0,121168	22.509.074	1711	-2,93	N/A
2014	Clams	N/A	POS	2645483	1,76	1.501.358	17873	-2,44	N/A
2013	EmerCoin	SHA-256	POW & POS	2236374	0,060928	36.705.368	3165	0,47	N/A
2014	BlackCoin	Scrypt	POS	2227110	0,029634	75.153.622	27366	4,49	ΟΧΙ
2014	Counterparty	SHA-256d	POS	2075936	0,789625	2.629.015	724	2,54	NAI
2013	YbCoin	N/A	N/A	1947609	0,647942	3.005.839	42783	-2,99	N/A
2014	AmberCoin	X13	POW & POS	1801885	0,041869	43.035.845	557	-4,66	N/A
2014	MonaCoin	Scrypt	Consensus	1621837	0,061659	26.303.250	3191	-1,1	NAI
2013	CasinoCoin	Scrypt	POW	1447056	0,043382	33.356.215	9297	22,53	N/A
2014	Startcoin	X11	POW	1434915	0,04039	35.526.491	5662	-10,8	N/A
2014	BlockShares	N/A	POS	1213567	6,51	186.302	109	1,14	N/A
2013	Novacoin	Scrypt	POW & POS	1170965	0,939552	1.246.301	11383	-6,79	N/A
2013	Mastercoin (Omni)	SHA-256d	N/A	1039873	1,89	549.712	49		N/A
2013	Primecoin	1CC/2CC/TWN	POW	1015281	0,080056	12.682.131	5005	5,99	N/A

ΠΑΡΑΡΤΗΜΑ Β

Έκδοση	Αλγόριθμος Hash	Μηχανισμός ασφαλείας	Κεφαλαιο-ποίηση ($)	Αξία ($)	Προσφορά (πλήθος νομισμάτων)	Όγκος συναλλαγών (24h)	Αλλαγή στην αξία (24h) %	Αντιπλη-θωρισμός
2009	1	1	6960918625	464,69	14979575	42451700	1,14	1
2013	2	2	212823563	0,006346	3,35E+10	580599	-1,85	1
2011	3	1	164072041	3,76	43668235	1168340	0,34	1
2014	3	1	16134235	0,000158	1,02E+11	130831	2,99	2
2014	5	4	15910032	2,62	6071604	22555	1,14	1
2012	1	4	10166373	0,444987	22846450	33617	-1,41	2
2014	8	5	9415373	0,003713	2,54E+09	24452	0,56	3
2014	8	2	9032070	0,001867	4,84E+09	7598	0,96	2
2013	1	3	6703841	0,006704	1E+09	9205	3,73	1
2011	1	1	6431007	0,488374	13168200	12529	10,45	1
2012	4	1	5540150	0,000031	1,78E+11	6282	0,8	1
2014	4	1	5177458	0,496892	10419684	15497	-1,25	1
2014	8	3	4111817	0,005015	8,2E+08	693	-1,8	1
2014	3	3	2727380	0,121168	22509074	1711	-2,93	3
2014	8	3	2645483	1,76	1501358	17873	-2,44	3
2013	1	4	2236374	0,060928	36705368	3165	0,47	3
2014	3	3	2227110	0,029634	75153622	27366	4,49	2
2014	1	3	2075936	0,789625	2629015	724	2,54	1
2013	8	5	1947609	0,647942	3005839	42783	-2,99	3

2014	6	4	1801885	0,041869	43035845	557	-4,66	3
2014	3	2	1621837	0,061659	26303250	3191	-1,1	1
2013	3	1	1447056	0,043382	33356215	9297	22,53	3
2014	5	1	1434915	0,04039	35526491	5662	-10,8	3
2014	8	3	1213567	6,51	186302	109	1,14	3
2013	3	4	1170965	0,939552	1246301	11383	-6,79	3
2013	1	5	1039873	1,89	549712	49		3
2013	7	1	1015281	0,080056	12682131	5005	5,99	3

ΠΑΡΑΡΤΗΜΑ Γ

Επιλογή των χαρακτηριστικών με τα οποία σχετίζεται ο αποπληθωρισμός:

@attribute hash {SHA-256d,ECDSA,Scrypt,X13,CryptoNight,X11,1CC/2CC/TWN,N/A}

@attribute change numeric

@attribute deflation {YES,NO,N/A}

@data

SHA-256d,1.14,YES

ECDSA,-1.85,YES

Scrypt,0.34,YES

Scrypt,2.99,NO

X11,1.14,YES

SHA-256d,-1.41,NO

N/A,0.56,N/A

N/A,0.96,NO

SHA-256d,3.73,YES

SHA-256d,10.45,YES

CryptoNight,0.8,YES

CryptoNight,-1.25,YES

N/A,-1.8,YES

Scrypt,-2.93,N/A

N/A,-2.44,N/A

SHA-256d,0.47,N/A

Scrypt,4.49,NO

SHA-256d,2.54,YES

N/A,-2.99,N/A

X13,-4.66,N/A

Scrypt,-1.1,YES

Scrypt,22.53,N/A

X11,-10.8,N/A

N/A,1.14,N/A

Scrypt,-6.79,N/A

SHA-256d,0,N/A

1CC/2CC/TWN,5.99,N/A

Επιλογή των χαρακτηριστικών με τα οποία σχετίζεται ο αλγόριθμος hash:

@attribute supply numeric

@attribute change numeric

@attribute deflation {YES,NO,N/A}

@attribute hash {SHA-256d,ECDSA,Scrypt,X13,CryptoNight,X11,1CC/2CC/TWN,N/A}

@data

14979575,1.14,YES,SHA-256d

33537439933,-1.85,YES,ECDSA

43668235,0.34,YES,Scrypt

10229200000,2.99,NO,Scrypt

6071604,1.14,YES,X11

22846450,-1.41,NO,SHA-256d

2535621961,0.56,N/A,N/A

4837356606,0.96,NO,N/A

999997096,3.73,YES,SHA-256d

13168200,10.45,YES,SHA-256d

17805100000,0.8,YES,CryptoNight

10419684,-1.25,YES,CryptoNight

819887419,-1.8,YES,N/A

22509074,-2.93,N/A,Scrypt

1501358,-2.44,N/A,N/A

36705368,0.47,N/A,SHA-256d

75153622,4.49,NO,Scrypt

2629015,2.54,YES,SHA-256d

3005839,-2.99,N/A,N/A

43035845,-4.66,N/A,X13

26303250,-1.1,YES,Scrypt

33356215,22.53,N/A,Scrypt

35526491,-10.8,N/A,X11

186302,1.14,N/A,N/A

1246301,-6.79,N/A,Scrypt

549712,0,N/A,SHA-256d

12682131,5.99,N/A,1CC/2CC/TWN

Επιλογή των χαρακτηριστικών με τα οποία σχετίζεται ο μηχανισμός ασφάλειας:

@attribute hash {SHA-256d,ECDSA,Scrypt,X13,CryptoNight,X11,1CC/2CC/TWN,N/A}

@attribute change numeric

@attribute deflation {YES,NO,N/A}

@attribute security {POW,POS,POW/POS,Consensus,N/A}

@data

SHA-256d,1.14,YES,POW

ECDSA,-1.85,YES,Consensus

Scrypt,0.34,YES,POW

Scrypt,2.99,NO,POW

X11,1.14,YES,POW/POS

SHA-256d,-1.41,NO,POW/POS

N/A,0.56,N/A,N/A

N/A,0.96,NO,Consensus

SHA-256d,3.73,YES,POS

SHA-256d,10.45,YES,POW

CryptoNight,0.8,YES,POW

CryptoNight,-1.25,YES,POW

N/A,-1.8,YES,POS

Scrypt,-2.93,N/A,POS

N/A,-2.44,N/A,POS

SHA-256d,0.47,N/A,POW/POS

Scrypt,4.49,NO,POS

SHA-256d,2.54,YES,POS

N/A,-2.99,N/A,N/A

X13,-4.66,N/A,POW/POS

Scrypt,-1.1,YES,Consensus

Scrypt,22.53,N/A,POW

X11,-10.8,N/A,POW

N/A,1.14,N/A,POS

Scrypt,-6.79,N/A,POW/POS

SHA-256d,0,N/A,N/A

1CC/2CC/TWN,5.99,N/A,POW

Αποτελέσματα κατηγοριοποίησης, όταν συμμετέχουν όλα τα χαρακτηριστικά:

=== Evaluation result ===

Scheme: NaiveBayes

Relation: cryptocoins

Correctly Classified Instances	16	59.2593 %
Incorrectly Classified Instances	11	40.7407 %
Kappa statistic	0.3371	
Mean absolute error	0.3026	
Root mean squared error	0.5026	
Relative absolute error	72.4924 %	
Root relative squared error	109.8246 %	
Total Number of Instances	27	

=== Detailed Accuracy By Class ===

	TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Class
	0.273	0	1	0.273	0.429	0.693	YES
	0.5	0.13	0.4	0.5	0.444	0.587	NO
	0.917	0.533	0.579	0.917	0.71	0.733	N/A
Weighted Avg.	0.593	0.256	0.724	0.593	0.556	0.695	

=== Confusion Matrix ===

a	b	c	<-- classified as
3	2	6	a = YES
0	2	2	b = NO
0	1	11	c = N/A

Δημιουργία cluster:

=== Evaluation result for traininginstances ===

Scheme: SimpleKMeansRelation: cryptocoins-weka.filters.unsupervised.attribute.Remove-R1,4,5,7

kMeans

======

Number of iterations: 3

Within cluster sum of squared errors: 38.80414018126379

Missing values globally replaced with mean/mode

Cluster centroids:

		Cluster#	
Attribute	Full Data	0	1
	(27)	(14)	(13)
hash	SHA-256d	SHA-256d	N/A
security	POW	POW	POS
supply	2635931380.963	4482704384.8571	647098915.2308
change	0.787	3.2886	-1.9069
deflation	N/A	YES	N/A

Clustered Instances

0	14 (52%)
1	13 (48%)

=== Evaluation result for traininginstances ===

Scheme: SimpleKMeansRelation: cryptocoins-weka.filters.unsupervised.attribute.Remove-R1,4,5,7

kMeans

======

Number of iterations: 5

Within cluster sum of squared errors: 34.87819570646174

Missing values globally replaced with mean/mode

Cluster centroids:

		Cluster#		
Attribute	Full Data	0	1	2
	(27)	(11)	(5)	(11)
hash	SHA-256d	SHA-256d	N/A	Scrypt
security	POW	POW	N/A	POS
supply	2635931380.963	5698683617.4545	1477843249.8	99582840.4545
change	0.787	1.6927	0.904	-0.1718
deflation	N/A	YES	N/A	N/A

Clustered Instances

0 11 (41%)

1 5 (19%)

2 11 (41%)

=== Evaluation result for traininginstances ===

Scheme: SimpleKMeansRelation: cryptocoins-weka.filters.unsupervised.attribute.Remove-R1,4,5,7

kMeans

======

Number of iterations: 4

Within cluster sum of squared errors: 30.708021405526885

Missing values globally replaced with mean/mode

Cluster centroids:

Cluster#

Attribute Full Data 0 1 2 3

(27) (9) (4) (5) (9)

==========

==========

hash	SHA-256d	SHA-256d	N/A	N/A	Scrypt
security	POW	POW	N/A	POS	POW/POS
supply	2635931380.963	6961844637.5556	1844133529.5	175922128.8	28600087.3333
change	0.787	2.0989	-0.3675	-3.366	2.2956
deflation	N/A	YES	N/A	N/A	N/A

Clustered Instances

0	9 (33%)
1	4 (15%)
2	5 (19%)
3	9 (33%)