ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΣΤΗ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ

<u>Διπλωματική Εργασία</u>

ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ, Η ΠΕΡΙΠΤΩΣΗ ΤΟΥ BITCOIN ΚΑΙ ΕΝΑ ΜΟΝΤΕΛΟ ΑΠΟΤΙΜΗΣΗΣ ΤΗΣ ΑΞΙΑΣ ΤΟΥ

του

ΣΤΥΛΙΑΝΟΣ ΣΥΜΕΩΝΙΔΗΣ

Υποβλήθηκε ως απαιτούμενο για την απόκτηση του μεταπτυχιακού διπλώματος ειδίκευσης στη Διοίκηση Επιχειρήσεων με εξειδίκευση στη Χρηματοοικονομική Διοίκηση

Σεπτέμβριος, 2018

Ευχαριστώ την οικογένειά μου, τους συμφοιτητές και φίλους που μαζί ολοκληρώσαμε αυτόν τον κύκλο.

Περίληψη (Abstract)

Ο Satoshi Nakamoto (έχει αποδειχθεί ότι αποτελεί ψευδώνυμο) το 2009 δημοσίευσε την έρευνά του και ξεκίνησε την λειτουργία του πρώτου κρυπτονομίσματος, του Bitcoin. Από τότε έχουν περάσει αρκετά χρόνια, ωστόσο η διάδοση επήλθε το τελευταίο χρονικό διάστημα. Οι υποστηρικτές του το θεωρούν το μέλλον, ενώ οι επικριτές του απάτη. Σκοπός της παρούσης εργασίας δεν είναι να απαντηθεί το ερώτημα που γεννάται, αλλά να δημιουργηθεί μια ολοκληρωμένη έρευνα η οποία να περιέχει τα τεχνικά και οικονομικά χαρακτηριστικά του κρυπτονομίσματος, ενώ ταυτόχρονα να μελετάει την απόδοσή του, σε σχέση με διάφορα επενδυτικά προϊόντα, καταλήγοντας στην δημιουργία ενός μοντέλου αποτίμησης της αξίας του.

Στο κεφάλαιο των τεχνικών χαρακτηριστικών μελετώνται στοιχεία όπως η δομή ενός Block συναλλαγών, η επαναστατική τεχνολογία της Blockchain, οι τεχνικές κρυπτογράφησης και τα πορτοφόλια Bitcoin. Καθώς και η πρωτότυπη διαδικασία της εξόρυξης.

Το κεφάλαιο της οικονομικής παρουσίασης περιέχει την ανάλυση του κρυπτονομίσματος με βάση τις λειτουργίες του Mankiw, ενδιαφέρουσες οικονομικές ιδιαιτερότητες όπως η έλλειψη κεντρικής οικονομικής αρχής και η αποπληθωριστική οικονομία. Ενώ ολοκληρώνεται με μια περιγραφή της παρούσης κατάστασης, όσον αφορά το θεσμικό πλαίσιο κανόνων και τα ανταλλακτήρια κρυπτονομισμάτων.

Η μελέτη συσχετίσεων πραγματοποιείται ανάμεσα στο Bitcoin και σε 17 ακόμη επενδυτικά προϊόντα για 4 διαφορετικές χρονικές περιόδους, ενώ επιπρόσθετα μελετάται και ο δείκτης EPU (Economic Policy Uncertainty Index). Το μοντέλο αποτίμησης αξίας υλοποιείται με την μέθοδο γραμμικής παλινδρόμησης, χρησιμοποιώντας την τεχνική των ελαχίστων τετραγώνων (OLS). Αποτελείται από 6 ανεξάρτητες μεταβλητές, το αργό πετρέλαιο, το παλλάδιο, τον δείκτη S&P 500, τον δείκτη Euro Index, την Nvidia και την απόδοση των έντοκων γραμματίων των Η.Π.Α. τρίμηνης διάρκειας.

Πίνακας Περιεχομένων

Πίνακας Εικονογραφήσεων

Κατάλογος Πινάκων

Κατάλογος Εικόνων

Εισαγωγή

Το Bitcoin είναι ένα αποκεντρωμένο ψηφιακό νόμισμα με σκοπό την υποστήριξη ηλεκτρονικών συναλλαγών, το οποίο συνδυάζει στο πρωτόκολλό του πληθώρα τεχνολογιών και μεθόδων της επιστήμης της Πληροφορικής. Η μονάδα μέτρησης ονομάζεται bitcoin(s), δεν έχει κάποια φυσική μορφή αλλά μόνο ηλεκτρονική και χρησιμοποιείται για να μεταφερθεί αξία εντός του ηλεκτρονικού οικοσυστήματος. Ο κώδικας του πρωτοκόλλου είναι ελεύθερος και διανέμεται μέσω του διαδικτύου καθώς το Bitcoin ανήκει στα έργα ανοιχτού λογισμικού.

Ιστορικά το Bitcoin πραγματοποίησε την εμφάνισή του το 2009, όταν ο Satoshi Nakamoto δημοσίευσε το άρθρο του, με τίτλο "Bitcoin – a peer to peer electronic cash system". Ωστόσο το ενδιαφέρον του επενδυτικού και επιστημονικού κοινού το έχει "κερδίσει" τα τελευταία χρόνια και κυρίως από το 2017 και έπειτα. Δηλαδή από την χρονική στιγμή κατά την οποία τα μέσα μαζικής ενημέρωσης άρχισαν να ασχολούνται έντονα με το οικονομικό φαινόμενο που δημιούργησε.

Με την πάροδο των χρόνων δημιουργήθηκαν και άλλα παρόμοια ψηφιακά νομίσματα, όλα μαζί αναφέρονται με τον όρο κρυπτονομίσματα και αποτελούν έναν ξεχωριστό κλάδο επενδυτικών προϊόντων. Η αγορά που έχει δημιουργηθεί όμως είναι ακόμη σε σχετικά πρώιμο στάδιο και δεν έχει καταφέρει να περάσει στο στάδιο της ωρίμανσης. Με αποτέλεσμα οι έντονες μεταβολές και η αστάθεια να δυσχεραίνουν την διαδικασία ανάλυσης.

Σκοπός της παρούσης εργασίας είναι η τεχνική και οικονομική κατανόηση του Bitcoin αλλά και των κρυπτονομισμάτων γενικότερα, ώστε να δημιουργηθεί ένα μοντέλο αποτίμησης και πρόβλεψης της αξίας του.

Ο σκοπός υλοποιείται, με την επίτευξη καλώς ορισμένων στόχων:

- Την ολοκληρωμένη τεχνική παρουσίαση των μεθοδολογιών και τεχνολογιών στις οποίες βασίζεται η λειτουργία του κρυπτονομίσματος, χωρίς να πραγματοποιείται εμβάθυνση που ξεπερνάει τα όρια και συνάδει με σύγγραμμα του τομέα της επιστήμης των υπολογιστών.
- Την παρουσίαση και ανάλυση των ιδιαίτερων οικονομικών χαρακτηριστικών που εμφανίζει το Bitcoin, τα οποία το διαφοροποιούν κατά πολύ μεγάλο βαθμό από τα συνήθη επενδυτικά προϊόντα.

- Την μελέτη των συσχετίσεων που παρουσιάζει το Bitcoin με διάφορα χρηματοοικονομικά προϊόντα, τα οποία κατανέμονται σε όλους τους γνωστούς επενδυτικούς κλάδους.
- Την υλοποίηση μοντέλου γραμμικής παλινδρόμησης, βασισμένο στην τεχνική των ελαχίστων τετραγώνων, το οποίο να παρουσιάζει τα βέλτιστα στατιστικά αποτελέσματα σε σχέση με τα προς μελέτη επιλεγμένα χρηματοοικονομικά προϊόντα.

Τεχνική Παρουσίαση του Bitcoin

Τα κρυπτονομίσματα γενικότερα και ειδικότερα το Bitcoin, από κατασκευαστικής και δομικής άποψης αποτελούν προϊόντα του κλάδου της Πληροφορικής. Η χρήση τους προσανατολίζεται στην υποστήριξη του τομέα των ηλεκτρονικών συναλλαγών. Για να μπορέσει να κατανοήσει κάποιος τον ρόλο και την λειτουργία τους εκτός από οικονομικές γνώσεις, χρειάζεται και βασικές γνώσεις της επιστήμης των υπολογιστών.

Στο πρώτο κεφάλαιο της παρούσης εργασίας και πριν την έναρξη οικονομικής προσέγγισης και ανάλυσης του φαινομένου, με το όνομα Bitcoin. Πραγματοποιείται παρουσίαση των βασικών τεχνικών χαρακτηριστικών του κρυπτονομίσματος, χωρίς να υπάρχει η εμβάθυνση σε τεχνολογικούς όρους που μπορεί να αποπροσανατολίσουν τον αναγνώστη. Θεωρήθηκε απαραίτητο καθώς μια επιτυχημένη προσέγγιση και ανάλυση του Bitcoin, βασίζεται στην κατανόηση της φύσης και της λειτουργίας του.

Η τεχνική παρουσίαση είναι απαραίτητη και για έναν ακόμη λόγο. Το Bitcoin, έχει καταφέρει να εισάγει τεχνολογίες οι οποίες μπορούν να επιφέρουν επαναστατικά αποτελέσματα στην διαχείριση και λειτουργία μεγάλων επιχειρησιακών κλάδων. Με κύριο παράδειγμα την τεχνολογία της Blockchain.

Δίκτυο του Bitcoin

Το πρωτόκολλο του Bitcoin έχει δημιουργηθεί με σκοπό να λειτουργεί σε ένα δίκτυο αρχιτεκτονικής peer-to-peer (P2P) (Nakamoto, 2008). Η αρχιτεκτονική P2P υποδηλώνει ότι όλες οι υπολογιστικές συσκευές, οι οποίες εκτελούν το πρωτόκολλο δημιουργούν ένα δίκτυο ομότιμων κόμβων. Παράδειγμα γνωστής σε όλους υπηρεσίας, η οποία χρησιμοποιεί P2P αρχιτεκτονική είναι ο διαμοιρασμός αρχείων με χρήση Torrents. Σε ένα P2P δίκτυο όλοι οι κόμβοι είναι "ίσοι", για τον λόγο αυτό αποκαλούνται ομότιμοι, ενώ ταυτόχρονα απουσιάζουν ειδικοί κόμβοι, με αυξημένες δικαιοδοσίες και αρμοδιότητες. Αντίστοιχα η έννοια της ιεραρχίας δεν νοείται στο πλαίσιο της συγκεκριμένης αρχιτεκτονικής. Πρωταρχικός σκοπός όλων των κόμβων είναι να μοιραστούν τον φόρτο παροχής υπηρεσιών για την λειτουργία του κρυπτονομίσματος.

Η χρήση της τοπολογίας P2P δεν αφορά μόνο την αρχιτεκτονική του δικτύου, αλλά συμβαδίζει και με ένα από τα βασικά αξιώματα του Bitcoin. Την αποκέντρωση του ελέγχου του ψηφιακού νομίσματος. Δηλαδή την έλλειψη κεντρικής αρχής, η οποία θα εγγυάται για την πραγματοποίηση και την αξιοπιστία των συναλλαγών.

Χαρακτηριστικό το οποίο μπορεί να πραγματοποιηθεί εντός ενός δικτύου ομότιμων κόμβων.

Κόμβοι, διαφορετικοί τύποι και ρόλοι

Κόμβος του δικτύου Bitcoin αποκαλείται οποιαδήποτε συνδεδεμένη συσκευή εκτελεί το πρωτόκολλό του. Παρόλο που οι κόμβοι ονομάζονται ομότιμοι υπάρχουν συσκευές διαφορετικού τύπου εντός του δικτύου, οι οποίες διαδραματίζουν και διαφορετικό ρόλο. Ένας κόμβος του δικτύου παρέχει υπηρεσίες που αποτελούν συνδυασμό των παρακάτω βασικών λειτουργιών:

- Λειτουργία δρομολόγησης δικτύου.
- Λειτουργία πλήρους Blockchain.
- Λειτουργία εξόρυξης.
- Λειτουργία υπηρεσιών πορτοφολιού.

Οι παραπάνω λειτουργίες αποτελούν και τον δομικό άξονα, βάση του οποίο είναι σχεδιασμένη η τεχνική παρουσίαση του Bitcoin, που πραγματοποιείται στο πρώτο μέρος της παρούσης εργασίας.

Για κάθε κόμβο η λειτουργία της δρομολόγησης του δικτύου είναι απαραίτητη ώστε να μπορεί να συμμετέχει στο δίκτυο. Οι ενέργειες τις οποίες πραγματοποιεί κάθε κόμβος συνοψίζονται στο γεγονός ότι θα πρέπει να επικυρώνει και να αναμεταδίδει συναλλαγές και Block συναλλαγών, ενώ ταυτόχρονα να ανακαλύπτει και να διατηρεί συνδέσεις με άλλους κόμβους.

Για να θεωρηθεί ένας κόμβος του δικτύου πλήρης, θα πρέπει να υποστηρίζει και τις τέσσερις παραπάνω λειτουργίες. Ωστόσο αυτό που ξεχωρίζει τις περισσότερες φορές τους πλήρεις κόμβους από τους υπόλοιπους είναι ότι διατηρούν μια ενημερωμένη και με όλες τις συναλλαγές που έχουν πραγματοποιηθεί ποτέ Blockchain. Με αποτέλεσμα να έχουν την δυνατότητα επικύρωσης συναλλαγών χωρίς να χρειάζεται να ανταλλάξουν δεδομένα με κανέναν άλλο κόμβο του δικτύου. Τα πρώτα χρόνια του Bitcoin, όλοι οι κόμβοι ήταν πλήρεις, ωστόσο ταυτόχρονα με την διάδοσή του, εμφανίσθηκαν κόμβοι με διαφορετικές υπολογιστικές δυνατότητες οι οποίοι αντί για την πλήρη Blockchain διατηρούν μόνο τα hash values των κεφαλών όλων των Block συναλλαγών. Αυτή η τακτική δεσμεύει χίλιες φορές περίπου λιγότερο αποθηκευτικό χώρο σε σχέση με την διατήρηση μιας πλήρους ενημερωμένης Blockchain. Οι νέοι κόμβοι αυτού του τύπου, ονομάζονται Simplified Payment Verification (SPV) κόμβοι. (Antonopoulos, 2017)

Όταν ένας κόμβος συμμετέχει στο δίκτυο του Bitcoin για πρώτη φορά, θα πρέπει να ανακαλύψει άλλους ενεργούς κόμβους του δικτύου και να συνδεθεί μαζί τους. Η αρχή πραγματοποιείται με την ανακάλυψη ενός τυχαίου ήδη ενεργού κόμβου του δικτύου. Με τον ήδη ενεργό κόμβο ανταλλάσσονται πληροφορίες σχετικές με την Blockchain και τις διευθύνσεις άλλων ενεργών κόμβων. Ο νέος κόμβος πρέπει να δημιουργήσει το δικό του αντίγραφο της Blockchain επιβεβαιώνοντας τα δεδομένα που λαμβάνει από τους λοιπούς ενεργούς κόμβους με τους οποίους έχει ήδη συνδεθεί. Ισχύει για την περίπτωση που ο νέος κόμβος υποστηρίζει την λειτουργία πλήρους Blockchain και απαιτείται μια ιδιαίτερα χρονοβόρα διαδικασία. Η γεωγραφική απόσταση των συνδεδεμένων κόμβων στο δίκτυο του Bitcoin είναι τυχαία, καθώς η P2P αρχιτεκτονική δεν διασφαλίζει γεωγραφική εγγύτητα στις συνδέσεις που δημιουργούνται.

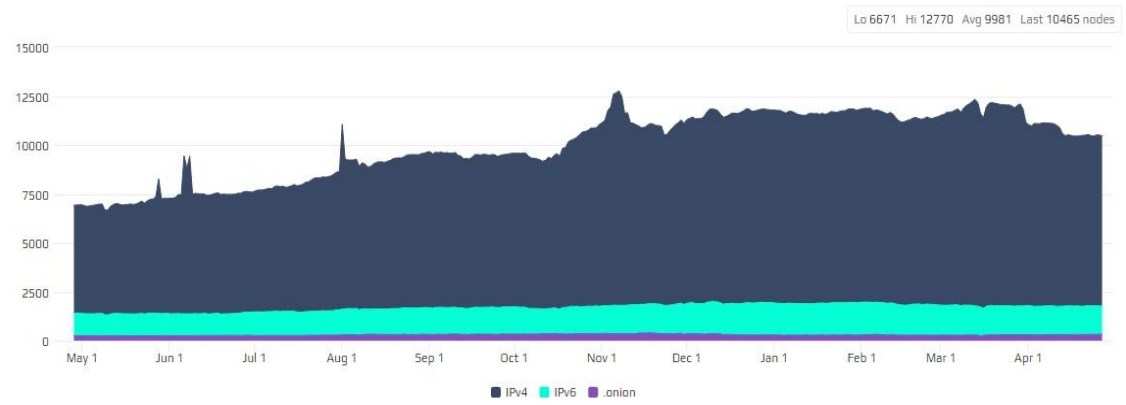
Στην περίπτωση των SPV κόμβων, πραγματοποιείται ανάκτηση δεδομένων από πλήρεις κόμβους του δικτύου, σχετικά με τις συναλλαγές. Η μετάδοση των δεδομένων αυτών υποστηρίζεται από Bloom Filters. Τα συγκεκριμένα φίλτρα αναζήτησης διαθέτουν το χαρακτηριστικό ότι περιγράφουν ένα ικανοποιητικό μοτίβο αναζήτησης δίχως να εκθέτουν τα αρχικά δεδομένα, προστατεύοντας την ιδιωτικότητα των συναλλαγών και τις διευθύνσεις των πορτοφολιών. Ωστόσο ακόμη και με την χρήση των συγκεκριμένων φίλτρων οι SPV κόμβοι είναι αισθητά λιγότερο ασφαλείς σε σχέση με τους πλήρεις κόμβους. (Antonopoulos, 2017)

Οι κόμβοι εξόρυξης ανταγωνίζονται συνεχώς ποιος θα καταφέρει να προσθέσει το επόμενο Block στην Blockchain, ώστε να επιβραβευτούν με τα νέα bitcoins και τις εκάστοτε χρεώσεις. Ιδιαίτερα ενδιαφέρον στοιχείο είναι ότι πλέον διαθέτουν υλικό ειδικά σχεδιασμένο ώστε να επιλύει το πρόβλημα του αλγορίθμου Proof-of-Work, σε αντίθεση με τα πρώτα χρόνια που γινόταν χρήση οικιακών υπολογιστών. Ένας κόμβος εξόρυξης μπορεί να είναι και πλήρης κόμβος. Η διαδικασία της εξόρυξης αποτελεί ξεχωριστό κεφάλαιο της εργασίας, στο οποίο πραγματοποιείται αναλυτική παρουσίαση της διαδικασίας.

Οι κόμβοι που υποστηρίζουν τις λειτουργίες πορτοφολιού είναι κυρίως πλήρεις κόμβοι. Ωστόσο η δημιουργία πορτοφολιών για κινητές συσκευές υποστηρίζεται συνήθως από SPV κόμβους.

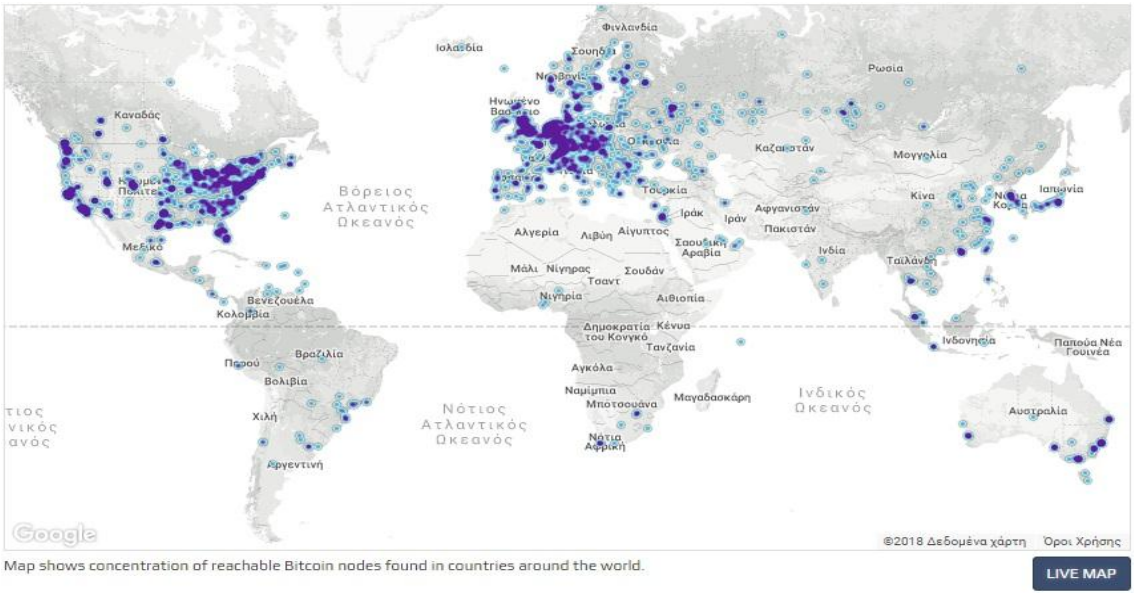
Κύριο και ευρύτερο δίκτυο Bitcoin

Το κύριο δίκτυο του Bitcoin τον τελευταίο χρόνο (από 28/04/2017 έως 28/04/2018), κατά μέσο όρο, περιελάμβανε 9.981 συνδεδεμένους κόμβους, οι οποίοι εκτελούσαν το πρωτόκολλο του Bitcoin, χρησιμοποιώντας P2P αρχιτεκτονική. Ένα ποσοστό των κόμβων, οι οποίοι διατηρούν μόνο την πλήρως ενημερωμένη Blockchain, ανήκουν σε εταιρείες που δεν συμμετέχουν στις βασικές λειτουργίες του ηλεκτρονικού νομίσματος αλλά παρέχουν παράλληλες υπηρεσίες, όπως είναι σελίδες ανάλυσης Block συναλλαγών, online πορτοφόλια, σελίδες παρακολούθησης συναλλαγών, σελίδες ανάλυσης δικτύου και άλλες. Το διάγραμμα που ακολουθεί ανήκει σε μια σελίδα ανάλυσης δικτύου και παρουσιάζει τον αριθμό των συνδεδεμένων κόμβων στο κύριο δίκτυο.



Εικόνα 1: Δεδομένα συνδεδεμένων κόμβων στο δίκτυο (28/04/2017-28/04/2018)

Στην συγκεκριμένη ιστοσελίδα υπάρχουν πολλές ενδιαφέρουσες πληροφορίες για το δίκτυο του Bitcoin. Στον παρακάτω χάρτη παρουσιάζεται η διασπορά των κόμβων σε παγκόσμιο επίπεδο στις 28/04/2018.



Εικόνα 2: Παγκόσμιος χάρτης διασποράς συνδεδεμένων κόμβων (28/04/2018)

Για την ίδια ημερομηνία ο παρακάτω πίνακας εμπεριέχει τις πρώτες οκτώ χώρες σε συνδεδεμένους κόμβους στο δίκτυο του Bitcoin.

Πίνακας 1: Κατανομή συνδεδεμένων κόμβων ανά χώρα (28/04/2018)

Χώρα	Συνδεδεμένοι Κόμβοι
Η.Π.Α.	2.552 (24,47%)
Γερμανία	2019 (16,36%)
Κίνα	718 (6,88%)
Γαλλία	684 (6,56%)
Ολλανδία	486 (4,66%)
Καναδάς	394 (3,78%)
Ηνωμένο Βασίλειο	387 (3,71%)
Ρωσία	358 (3,43%)

**Πηγή: https://bitnodes.earn.com*

Εκτός από το κύριο δίκτυο του Bitcoin υπάρχει και το ευρύτερο δίκτυο. Σε αυτό συμμετέχουν κόμβοι οι οποίοι δεν εκτελούν το πρωτόκολλο του Bitcoin αλλά διαφορετικά πρωτόκολλα τα οποία έχουν σχεδιαστεί ώστε να μπορούν να συνεργάζονται με το κύριο πρωτόκολλο του Bitcoin, χωρίς όμως να επιτελούν κάποια από τις βασικές του λειτουργίες. Παραδείγματα τέτοιων πρωτοκόλλων είναι τα mining pools, τα οποία θα αναλυθούν στο κεφάλαιο της εξόρυξης και κάποιες εκδόσεις πορτοφολιών με μικρές υπολογιστικές απαιτήσεις.

Το συνολικό μέγεθος του δικτύου του Bitcoin δημιουργεί καθυστερήσεις στην αναμετάδοση των δεδομένων. Στοιχείο το οποίο μπορεί να αποτελέσει πηγή προβλημάτων για την διαδικασία της εξόρυξης, διότι η χρονική ακρίβεια και η ταχύτητα είναι ιδιαίτερα σημαντικές. Ωστόσο η δημιουργία ενός παράλληλου δικτύου που να εξυπηρετεί τους miners και τα mining pools έδωσε λύση στο συγκεκριμένο ζήτημα. Το δίκτυο αυτό ονομάζεται Fast Internet Bitcoin Relay Engine (FIBRE) και δημιουργήθηκε από τον Matt Corallo το 2016.

Η τεχνολογία της Blockchain

Η επαναστατική τεχνολογία που εισήγαγε το πρωτόκολλο του Bitcoin, είναι η μεθοδολογία και οι τεχνικές με τις οποίες διαχειρίζεται τις συναλλαγές των χρηστών του δικτύου του. Η επονομαζόμενη Blockchain, χρήση της οποίας μπορεί να υπάρξει και σε άλλες περιπτώσεις εκτός από ένα ηλεκτρονικό μέσο συναλλαγών. (Catalini, et al., 2017) Στην ενότητα αυτή θα παρουσιαστεί και θα αναλυθεί ο τρόπος λειτουργίας της Blockchain, ενώ ταυτόχρονα θα μελετηθούν στοιχεία τα οποία προσέδωσαν στο

Bitcoin ανταγωνιστικό πλεονέκτημα, σε αντίθεση με προγενέστερες προσπάθειες για την δημιουργία ενός ηλεκτρονικού νομίσματος ευρείας αποδοχής.

Επί της ουσίας η Blockchain αποτελεί τις μεθόδους, τους κανόνες και τις αλγοριθμικές τεχνικές με βάση τις οποίες πραγματοποιείται η διαχείριση της βάσης δεδομένων όλων των συναλλαγών που πραγματοποιήθηκαν με χρήση Bitcoin από την πρώτη (2009), μέχρι και την πιο πρόσφατη. Καθώς και μια μεθοδολογία η οποία εγγυάται την απόλυτη ασφάλεια και λειτουργία του ηλεκτρονικού νομίσματος. Ορίζοντας την Blockchain με προγραμματιστικούς όρους, θα λέγαμε ότι αποτελεί μια διατεταγμένη δομή δεδομένων, που χρησιμοποιεί συνδεδεμένες προς τα πίσω λίστες από Block συναλλαγών. (Antonopoulos, 2017)

Όλοι οι συνδεδεμένοι κόμβοι του δικτύου διατηρούν το προσωπικό τους αντίγραφο από την Blockchain και καθώς εκτελούν το πρωτόκολλο του Bitcoin η διαχείριση της αλυσίδας διέπεται από συγκεκριμένους κοινούς κανόνες και τεχνικές.

Το πρωτόκολλο με βάση το οποίο λειτουργεί το Bitcoin καθορίζει ότι οι συναλλαγές συγκεντρώνονται σε Blocks τα οποία ανανεώνονται και επεξεργάζονται (εξορύσσονται) από το δίκτυο κάθε 10 λεπτά, περίπου, ανεξαρτήτου της υπολογιστικής ισχύος του δικτύου αλλά και τον όγκο των συναλλαγών. Η Blockchain αποτελεί την "αλυσίδα", η οποία συνδέει όλο αυτό το πλήθος των Blocks, το οποίο αυξάνεται συνεχώς. Με αρχή το πρώτο Block που δημιουργήθηκε ποτέ, το οποίο ονομάζεται Genesis Block και αποτελεί τον "πρόγονο" οποιουδήποτε άλλου Block συναλλαγών. (Nakamoto, 2008)

Η δομή ενός Block συναλλαγών

Ένα Block συναλλαγών αποτελείται από τέσσερα δομικά πεδία, τα οποία παρουσιάζονται στον παρακάτω πίνακα.

Πίνακας 2: Δομικά πεδία ενός Block συναλλαγών

Πεδίο	Περιγραφή
Μέγεθος του Block	Το μέγεθος του Block σε bytes.
Κεφαλή του Block	Πεδίο που περιέχει δομικά στοιχεία για την εκτέλεση των αλγορίθμων του προτύπου.
Μετρητής συναλλαγών	Ο αριθμός των συναλλαγών που περιέχει το συγκεκριμένο Block.
Συναλλαγές	Οι συναλλαγές ανάμεσα σε διευθύνσεις πορτοφολιών και ο όγκος της κάθε συναλλαγής σε bitcoins.

Από τα παραπάνω πεδία, η "Η κεφαλή του Block" χρήζει εκτενέστερης ανάλυσης καθώς το περιεχόμενο της χρησιμοποιείται σε βασικές μεθόδους και τεχνικές του

πρωτοκόλλου. Τα πεδία που με την σειρά τους αποτελούν την κεφαλή του Block παρουσιάζονται στον παρακάτω πίνακα.

Πίνακας 3: Δομικά πεδία της κεφαλής ενός Block συναλλαγών

Πεδίο	Περιγραφή
Έκδοση	Αναφέρεται στην έκδοση του πρωτοκόλλου του Bitcoin, που χρησιμοποιείται.
Hash value του προηγούμενου Block	Συνδέει το τρέχον Block με τον πρόγονό του, δημιουργώντας αλυσιδωτή σχέση. Αναφέρεται στο hash value της κεφαλής του προγόνου.
Ρίζα Merkle	Αφορά το hash value της ρίζας του αλγορίθμου των Merkle Trees, που χρησιμοποιείται για την ταχύτερη διαχείριση των συναλλαγών.
Χρονική σφραγίδα	Προσδίδει στην δημιουργία του Block μια ακριβή χρονική στιγμή.
Στόχος δυσκολίας	Αναφέρεται στο πόσο υπολογιστικά επιβαρυμένη θα είναι η εκτέλεση του αλγορίθμου κατακερματισμού, ώστε να διατηρείται η χρονική απόσταση ανάμεσα στην δημιουργία δύο Block. Εξαρτάται από την συνολική υπολογιστική ισχύ του δικτύου.
Nonce (Τυχαίος αριθμός)	Χρησιμοποιείται για την εκτέλεση του αλγορίθμου της κατηγορίας Proof-of-Work.

Δύο είναι τα στοιχεία τα οποία ξεχωρίζουν ένα Block συναλλαγών από κάποιο άλλο. Το πρώτο είναι το ψηφιακό του αποτύπωμα, το οποίο το χαρακτηρίζει μοναδικά, χωρίς να υπάρχει καμία αμφιβολία. Με τον όρο ψηφιακό αποτύπωμα εννοούμε το αποτέλεσμα της διπλής εκτέλεσης του αλγορίθμου SHA256 αν σαν είσοδο θέσουμε το πεδίο της κεφαλής του Block (Antonopoulos, 2017). Το αποτέλεσμα της διαδικασίας δεν περιέχεται σε κάποιο πεδίο του Block αλλά υπολογίζεται από τον κάθε κόμβο του δικτύου όταν αυτός το κρίνει απαραίτητο. Το δεύτερο στοιχείο είναι το ύψος (height) του κάθε Block. Το χαρακτηριστικό του ύψους δηλώνει την θέση που κατέχει το συγκεκριμένο Block στην Blockchain, δηλαδή την απόσταση του από το Genesis Block. Για παράδειγμα στις *01/07/2018* στις *14:11* το ύψος του επόμενου Block συναλλαγών, το οποίο θα έπαιρνε θέση για επεξεργασία ήταν, *530.037*. Σε κάποιες περιπτώσεις και για σύντομη σχετικά χρονική διάρκεια το ύψος, μπορεί να μην χαρακτηρίζει ένα Block μοναδικά. Αυτό συμβαίνει όταν υπάρχει διάσπαση της

αλυσίδας σε δύο υποαλυσίδες (soft fork). Σε αυτή την περίπτωση δύο Block έχουν ακριβώς το ίδιο ύψος, έως ότου επιλυθεί η διάσπαση και υπερισχύσει το ένα από τα δύο υποτμήματα της αλυσίδας. Πληροφορίες για τα Block και το περιεχόμενο τους αλλά και συνολικά για την Blockchain είναι προσβάσιμες από την ιστοσελίδα *"www.blockchain.com"*.

Το στοιχείο που προσέδωσε ανταγωνιστικό πλεονέκτημα στο Bitcoin είναι το γεγονός ότι η τεχνολογία Blockchain που εφαρμόζεται στο πρωτόκολλο, έχει σχεδιαστεί ώστε να μπορεί να επιλύει με ικανοποιητικό τρόπο όλα τα πιθανά ζητήματα που ενδεχομένως να επηρεάσουν την λειτουργία του. Το επίτευγμα αυτό πιστώνεται κατά κύριο λόγο στο άτομο ή στα άτομα τα οποία βρίσκονται πίσω από το ψευδώνυμο Satoshi Nakamoto αλλά και στην διεθνή κοινότητα που έχει αναπτυχθεί. Στην συνέχεια παρουσιάζονται οι βασικές τεχνικές και μέθοδοι που χρησιμοποιούνται στην τεχνολογία Blockchain του Bitcoin.

Κρυπτογράφηση (Hash Functions)

Η κρυπτογράφηση στοιχείων που μεταδίδονται στο δίκτυο, διατηρεί τα υψηλά επίπεδα ασφάλειας τα οποία πρέπει να χαρακτηρίζουν ένα ηλεκτρονικό νόμισμα. Με σκοπό κακόβουλες ενέργειες μεμονωμένων χρηστών να μην μπορούν να επηρεάσουν την λειτουργία του συστήματος. Για να επιτευχθεί ο σκοπός της κρυπτογράφησης χρησιμοποιούνται συναρτήσεις κατακερματισμού (hash functions). Η λειτουργία των συναρτήσεων αυτών είναι να επιδέχονται μια αυθαίρετη είσοδο, ανεξαρτήτου μεγέθους και να παράγουν μια έξοδο συγκεκριμένου μεγέθους, μικρότερου της αρχικής εισόδου (hash value). Ενώ επιπρόσθετα διατηρούν και συγκεκριμένες ιδιότητες:

- Η ίδια είσοδος θα πρέπει να παράγει πάντα το ίδιο αποτέλεσμα.
- Από την έξοδο του αλγορίθμου θα πρέπει να είναι υπολογιστικά αδύνατο για κάποιον, να επιστρέψει στα δεδομένα της εισόδου.
- Μικρές αλλαγές στα δεδομένα εισόδου να επιφέρουν μεγάλες αλλαγές στα αποτελέσματα της εξόδου.

Συγκεκριμένα, το πρωτόκολλο του Bitcoin κάνει χρήση του αλγορίθμου SHA256^2, που σημαίνει διπλή χρήση του αλγορίθμου SHA256. Ο SHA256 ανήκει στην οικογένεια αλγορίθμων SHA-2, τους οποίους έχει σχεδιάσει η NSA (National Security Agency – US Government) και τους έχει δημοσιοποιήσει το NIST (National Institute of

Standards and Technology), το 2001 (Franco, 2015). Η έξοδος του αλγορίθμου είναι μεγέθους 256 bits, δικαιολογώντας και την ονομασία.

Οι αλγόριθμοι κρυπτογράφησης θεωρούνται αποτελεσματικοί και αδύνατο να αντιστραφεί η λειτουργία τους, με βάση τις δυνατότητες των υπολογιστικών συστημάτων που υπάρχουν σήμερα. Στο μέλλον με την αύξηση των δυνατοτήτων των υπολογιστικών συστημάτων, θα πρέπει να υπάρξει και ταυτόχρονη αναθεώρηση της σχεδίασης των αλγορίθμων κρυπτογράφησης διότι σε αντίθετη περίπτωση δεν θα μπορούν να επιτελέσουν αποδοτικά το έργο τους.

Αλγόριθμος εξόρυξης της κατηγορίας Proof-of-Work

Η σύνδεση στην Blockchain του επόμενου Block συναλλαγών απαιτεί από τους κόμβους την εκτέλεση ενός απαιτητικού αλγορίθμου και την επίλυση ενός προβλήματος της κατηγορίας Proof-of-Work. Η συγκεκριμένη κατηγορία αλγορίθμων εμπεριέχει την επίλυση αναλογικά δύσκολων προβλημάτων που απαιτούν υπολογίσιμη υπολογιστική ισχύ, των οποίων όμως η λύση είναι εύκολο να επιβεβαιωθεί (Asharaf, et al., 2017). Ένα γνωστό παράδειγμα αλγορίθμου που ανήκει σε αυτήν την κατηγορία είναι οι διαδεδομένοι από την χρήση τους στο διαδίκτυο, Captcha Codes. Ωστόσο το πρωτόκολλο του Bitcoin χρησιμοποιεί το σύστημα hashcash που βασίζεται στον αλγόριθμο SHA256 (Nakamoto, 2008). Η ανάλυση της διαδικασίας είναι ιδιαίτερα σημαντική, στην περίπτωση του Bitcoin καθώς σχετίζεται με την δημιουργία νέων νομισμάτων, δηλαδή την προσφορά χρήματος της οικονομίας του. Για τον λόγο αυτό θα την μελετήσουμε ξεχωριστά στο κεφάλαιο της εξόρυξης (mining).

Διάσπαση αλυσίδας (fork)

Η λειτουργία του συστήματος του Bitcoin υποστηρίζεται από μηχανήματα τα οποία προσφέρουν την υπολογιστική τους ισχύ. Τα μηχανήματα αποκαλούνται miners και η μετάφραση του όρου στα ελληνικά ως "ανθρακωρύχοι", δεν αποδίδει κατάλληλα το νόημα. Η περιγραφή της λειτουργίας της εξόρυξης (mining), όπως αναφέρθηκε και προηγουμένως, θα πραγματοποιηθεί σε μεταγενέστερο κεφάλαιο της παρούσης εργασίας. Ωστόσο στο σημείο αυτό θα αναφερθούμε σε ένα ζήτημα το οποίο δημιουργείται όταν δύο miners προσθέτουν στην αλυσίδα ακριβώς την ίδια χρονική στιγμή ένα νέο Block συναλλαγών. Με αποτέλεσμα για περιορισμένο χρονικό διάστημα να δημιουργείται διάσπαση της Blockchain, σε δύο υποαλυσίδες. Το φαινόμενο αυτό ονομάζεται με τον αγγλικό όρο "fork" και δεν συμβαίνει ιδιαίτερα

συχνά. Συγκεκριμένα οι μετρήσεις που έχουν πραγματοποιηθεί, δείχνουν ότι η πιθανότητα του να συμβεί είναι περίπου 2%, δηλαδή μια φορά ανά 50 block που επεξεργάζονται.

Η επίλυση του ζητήματος θα μπορούσε να είναι μια δύσκολη διαδικασία η οποία θα είχε ως αποτέλεσμα την καθυστέρηση της λειτουργίας του δικτύου. Ωστόσο γίνεται χρήση μεθοδολογίας, η οποία δεν απαιτεί τη συμμετοχή κάποιου εξωτερικού μηχανισμού που να διευθετεί το ζήτημα, αλλά δίνει την δυνατότητα στους κόμβους του δικτύου να το επιλύσουν από μόνοι τους. Αναλυτικότερα όταν οι κόμβοι του δικτύου αντιληφθούν την ύπαρξη διάσπασης στην αλυσίδα, θεωρούν ως έγκυρη την υποαλυσίδα την οποία υποστηρίζει το μεγαλύτερο ποσοστό των κόμβων. Το τμήμα της αλυσίδας το οποίο δεν θεωρείται έγκυρο καταργείται αμέσως και οι κόμβοι που το υποστήριζαν εναρμονίζονται με την πλειοψηφία. Ωστόσο οι συναλλαγές δεν χάνονται, επιστρέφουν και λαμβάνουν θέση στο επόμενο Block το οποίο θα επεξεργαστεί, ώστε να αποκτήσουν την τελική τους θέση στην Blockchain. Αξίζει να αναφερθεί πως η πιθανότητα να πραγματοποιηθεί διάσπαση σε περισσότερα από δύο υποτμήματα είναι εξαιρετικά μικρή.

Το φαινόμενο και η επίλυση που περιγράφηκε, αποτελεί την συνηθισμένη περίπτωση ενός “soft fork”. Ωστόσο υπάρχουν και περιπτώσεις στις οποίες πραγματοποιείται διάσπαση στην Blockchain λόγω δομικών αλλαγών στο πρωτόκολλο του κρυπτονομίσματος (hard fork), τότε η επίλυση απαιτεί την εξωτερική παρέμβαση και επιπρόσθετες ενέργειες διαχείρισης. Γνωστή περίπτωση ενός hard fork στην Blockchain του Bitcoin, είναι η δημιουργία το 2017 του κρυπτονομίσματος “Bitcoin Cash”, το οποίο αποτελεί ένα ξεχωριστό και ανεξάρτητο κρυπτονόμισμα, διατηρώντας ωστόσο δομικές ομοιότητες με το Bitcoin.

Αριθμός των Block και μέθοδος εξακρίβωσης συναλλαγών (Merkle Trees)

Η δημοτικότητα που απέκτησε αλλά και η εκτεταμένη χρήση του Bitcoin, έχει ως αποτέλεσμα ο αριθμός των συναλλαγών που πραγματοποιούνται καθημερινά να αυξάνεται ραγδαία. Αναλογιζόμενος κανείς ότι στην Blockchain διατηρούνται όλες οι συναλλαγές που έχουν πραγματοποιηθεί με την χρήση του κρυπτονομίσματος, γίνεται εύκολα κατανοητό ότι αναφερόμαστε σε έναν τεράστιο όγκο δεδομένων συναλλαγών. Στις συναλλαγές αυτές θα πρέπει να ανατρέξει ένας κόμβος, όταν χρειάζεται να πραγματοποιήσει την επιβεβαίωση μια νέας συναλλαγής. Για την υπολογιστικά αρτιότερη αναζήτηση και επιβεβαίωση των συναλλαγών, από το πρωτόκολλο του

Bitcoin γίνεται χρήση του αλγορίθμου των Merkle Trees (Asolo, 2018). Η ανάλυση της λειτουργίας του αλγορίθμου δεν συνάδει με το περιεχόμενο της συγκεκριμένης εργασίας, καθώς αποτελεί χωρίο της επιστήμης της πληροφορικής. Ωστόσο ενδιαφέρον παρουσιάζει η αποδοτικότητα του συγκεκριμένου αλγορίθμου.

Πίνακας 4: Αποδοτικότητα του αλγορίθμου "Merkle Trees"

Αριθμός Συναλλαγών	Μέγεθος Δεδομένων	Υπολογισμοί για την εξακρίβωση με χρήση των Merkle Trees	Μέγεθος δεδομένων για την εκτέλεση των Merkle Trees
16 συναλλαγές	4 kilobytes	4 υπολογισμοί	128 bytes
512 συναλλαγές	128 kilobytes	9 υπολογισμοί	288 bytes
2.048 συναλλαγές	512 kilobytes	11 υπολογισμοί	352 bytes
65.535 συναλλαγές	16 megabytes	16 υπολογισμοί	512 bytes

Παρατηρούμε ότι ενώ ο αριθμός των συναλλαγών αυξάνεται από τις 16 στις 65.535, με αποτέλεσμα να αυξάνεται ραγδαία το μέγεθος της βάσης δεδομένων από 4 kilobytes σε 16 megabytes. Ο αλγόριθμος των Merkle Trees απαιτεί ελάχιστα μεγαλύτερο όγκο δεδομένων, για να μπορεί να επιβεβαιώσει την ύπαρξη αυτών των συναλλαγών, από 128 bytes για τις 16 συναλλαγές σε 512 bytes για τις 65.535 συναλλαγές. Προσδίδοντας στο πρωτόκολλο του Bitcoin ένα ακόμη ανταγωνιστικό πλεονέκτημα όσον αφορά την ταχύτητα και τον όγκο των δεδομένων που απαιτούνται για την διαδικασία επιβεβαίωσης της ύπαρξης συγκεκριμένων συναλλαγών στην Blockchain του.

Λοιπές αλυσίδες για δοκιμές

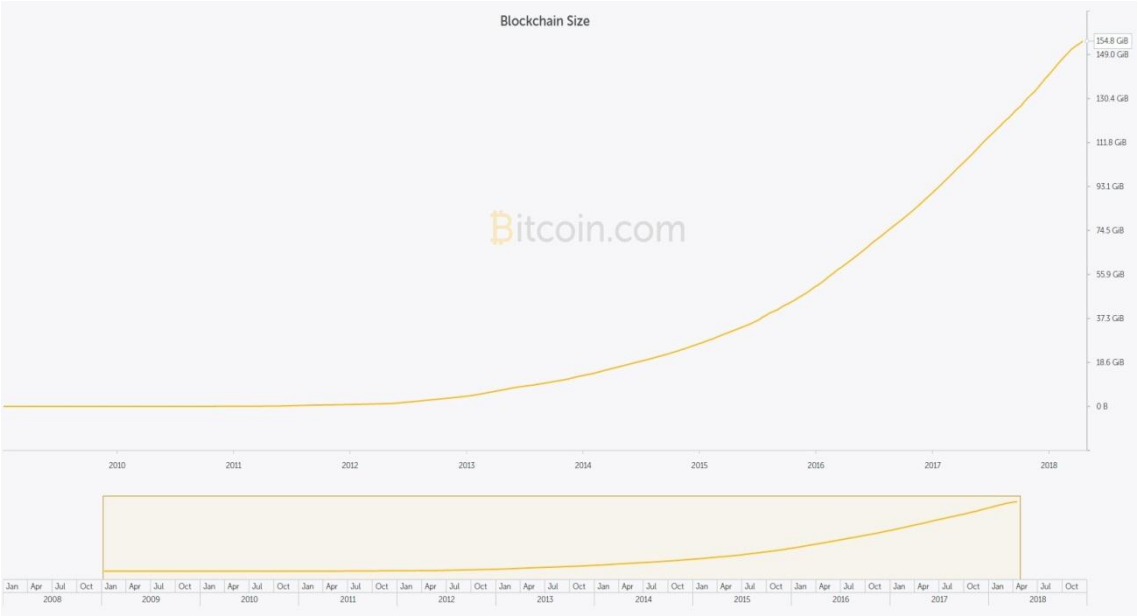
Η κύρια αλυσίδα την οποία δημιούργησε και αρχικοποίησε ο Satoshi Nakamoto με το Genesis Block το 2009, ονομάζεται mainnet. Ωστόσο υπάρχουν και άλλες αλυσίδες που λειτουργούν ταυτόχρονα στο δίκτυο του Bitcoin, με σκοπό πειραματικό, ώστε να πραγματοποιούνται δοκιμές σε νέες ιδέες. Αυτές είναι η testnet, η segnet και η regtest. Τα νομίσματα που δημιουργούνται με χρήση αυτών των αλυσίδων δεν έχουν καμία αξία.

Επεκτασιμότητα της Blockchain και τα κυριότερα προβλήματα

Η Blockchain είναι μια τεχνολογία σχεδιασμένη ώστε να μπορεί να αντιμετωπίσει σχεδόν όλα τα ζητήματα που τίθενται στην καθημερινή της λειτουργία αποτελεσματικά, καθώς ο όγκος των συναλλαγών παραμένει σχετικά περιορισμένος. Ωστόσο στην περίπτωση την οποία μελετάμε και αφορά ένα παγκόσμιο νόμισμα ηλεκτρονικών

συναλλαγών, ρόλο τον οποίο επιδιώκει να διαδραματίσει το Bitcoin, ο καθημερινός όγκος των συναλλαγών προσεγγίζει δυσθεώρητα ύψη. Αυτή η αύξηση της τάξης μεγέθους εμφάνισε και τα σημεία στα οποία υστερεί η Blockchain και σχετίζονται κυρίως με την ταχύτητα και το μέγεθός της. (Blockgeeks: Guides, 2017)

Στο παρακάτω διάγραμμα παρουσιάζεται το συνολικό μέγεθος της Blockchain με την πάροδο των ετών. Δεδομένα τα οποία διατηρούνται σε κάθε πλήρη κόμβο του δικτύου ξεχωριστά, ώστε να μπορεί το πρωτόκολλο του Bitcoin να εκτελεστεί.



Εικόνα 3: Το μέγεθος της Blockchain του Bitcoin (σε GB)

Την περίοδο στην οποία συντάσσεται η παρούσα εργασία το μέγεθος της Blockchain ξεπερνάει τα 150 GB. Ο συγκεκριμένος όγκος δεδομένων δεν είναι απαγορευτικός, καθώς οι κόμβοι του δικτύου αποτελούν συστήματα υψηλών υπολογιστικών δυνατοτήτων. Ωστόσο μέσω του διαγράμματος γίνεται αντιληπτό ότι η μεταβολή του μεγέθους της Blockchain, προσεγγίζει έναν λογαριθμικό ρυθμό αύξησης. Με αποτέλεσμα σε λίγα χρόνια και σε περίπτωση που ο τρόπος λειτουργίας παραμείνει ίδιος, το μέγεθός της δεν θα μπορεί να είναι υπολογιστικά διαχειρίσιμο.

Οι άμεσοι ανταγωνιστές του Bitcoin στις ηλεκτρονικές συναλλαγές, είναι το PayPal και η Visa και στον τομέα της ταχύτητας φαίνεται να υπερέχουν. Ορίζοντας την ταχύτητα ως τις συναλλαγές που πραγματοποιεί το κάθε σύστημα ανά δευτερόλεπτο. Καταλήγουμε στα εξής αποτελέσματα.

Πίνακας 5: Ταχύτητα συστημάτων ηλεκτρονικών συναλλαγών

Σύστημα συναλλαγών	Συναλλαγές ανά δευτερόλεπτο
PayPal	193 συναλλαγές.
Visa	1667 συναλλαγές.
Bitcoin	7 συναλλαγές.

Φυσικά αναφερόμαστε σε συστήματα με εντελώς διαφορετική αρχιτεκτονική και το καθένα έχει συγκεκριμένα πλεονεκτήματα και τα ανάλογα μειονεκτήματα, ωστόσο ο τομέας της ταχύτητας είναι κοινός και εξίσου σημαντικός. Ένας ανασταλτικός παράγοντας για την ταχύτητα με την οποία πραγματοποιούνται οι συναλλαγές στο Bitcoin είναι το μέγιστο μέγεθος του κάθε Block συναλλαγών, το οποίο έχει οριστεί από τον Satoshi Nakamoto στο 1 MB και δεν έχει αλλάξει μέχρι και σήμερα, παρά τις συζητήσεις και τις προτάσεις που έχουν πραγματοποιηθεί στην κοινότητα. Ωστόσο ένα μέρος της κοινότητας επιθυμούσε την αλλαγή, με αποτέλεσμα το 2017 να πραγματοποιηθεί hard fork στην Blockchain του Bitcoin και να δημιουργηθεί ένα νέο κρυπτονόμισμα, το Bitcoin Cash, στο οποίο διατηρήθηκαν όλα σχεδόν τα βασικά χαρακτηριστικά του Bitcoin αλλά αυξήθηκε το μέγιστο μέγεθος ενός Block συναλλαγών.

Μελλοντικά σχέδια εξέλιξης της Blockchain

Το Bitcoin φανερώνει την δυναμική φύση του καθώς οι διαβουλεύσεις στην κοινότητα για νέες ιδέες και συγκεκριμένες προτάσεις δεν σταματάνε ποτέ. Οι κυριότερες αυτή την περίοδο είναι:

1. Η δημιουργία παράλληλων αλυσίδων οι οποίες θα υποστηρίζουν την λειτουργία της Blockchain. Είναι μια ιδέα η οποία υπάρχει εδώ και αρκετό καιρό, ωστόσο ακόμη δεν έχει προχωρήσει στο στάδιο υλοποίησης. Παράδειγμα τέτοιας αλυσίδας είναι η SegWit.
2. Η αλλαγή από αλγορίθμους της κατηγορίας Proof-of-Work, σε αλγορίθμους της κατηγορίας Proof-of-Stake. Αρχικά με συνδυαστική μορφή και ταυτόχρονη λειτουργία. Ενώ μελλοντικά, με σκοπό την πλήρη χρήση αλγορίθμων Proof-of-Stake.
3. Η δημιουργία καναλιού συναλλαγών εξωτερικά της Blockchain, ανάμεσα σε χρήστες οι οποίοι συναλλάσσονται συχνά και έχει δημιουργηθεί κλίμα αμοιβαίας εμπιστοσύνης ανάμεσά τους. Με την ολοκλήρωση των συναλλαγών και τον

τερματισμό του καναλιού, δηλώνεται στην Blockchain μια συνολική συναλλαγή, η οποία αποτελεί το άθροισμα των επιμέρους. (Lightning Networks)

4. Εσωτερική διάσπαση του Block συναλλαγών σε τμήματα τα οποία διαθέτουν κοινά χαρακτηριστικά, αυξάνοντας την ταχύτητα με την οποία επιβεβαιώνονται οι συναλλαγές. (Sharding)

Κρυπτογραφία και Πορτοφόλια

Το Bitcoin αποτελεί τον κύριο εκφραστή των κρυπτονομισμάτων και όπως φανερώνει το πρώτο συνθετικό της λέξης, η κρυπτογραφία διαδραματίζει έναν ιδιαίτερα σημαντικό ρόλο. Χωρίς αυτήν το Bitcoin δεν θα μπορούσε να υπάρξει.

Κρυπτογραφία είναι η επιστήμη η οποία διασφαλίζει την ασφαλή επικοινωνία δύο χρηστών, παρόλο που κάποιος τρίτος μπορεί να καταγράφει τα μηνύματά τους ή και να ελέγχει το κανάλι επικοινωνίας. Με την πάροδο των χρόνων έχουν αναπτυχθεί πολλές διαφορετικές τεχνικές και τα αντίστοιχα εργαλεία κρυπτογράφησης. Το Bitcoin χρησιμοποιεί τρεις από αυτές:

- Κρυπτογράφηση Δημοσίου Κλειδιού. Χρήση της μεθόδου πραγματοποιείται στην διαχείριση των συναλλαγών.
- Συναρτήσεις Κατακερματισμού. Η Blockchain χρησιμοποιεί συναρτήσεις κατακερματισμού για να διατηρήσει τα δεδομένα της ασφαλή.
- Κρυπτογράφηση Συμμετρικού Κλειδιού. Τα περισσότερα είδη πορτοφολιών χρησιμοποιούν την συγκεκριμένη μέθοδο για να προστατέψουν τα ιδιωτικά κλειδιά των χρηστών.

Το Bitcoin δεν έχει φυσική μορφή, οπότε η ιδιοκτησία επιβεβαιώνεται μέσω ψηφιακών κλειδιών, διευθύνσεων πορτοφολιών και ψηφιακών υπογραφών. Υπεύθυνα για την δημιουργία και την αποθήκευση των ψηφιακών κλειδιών είναι κάποιες σχετικά απλές βάσεις δεδομένων, οι οποίες ονομάζονται πορτοφόλια. Τα ψηφιακά κλειδιά και το λογισμικό το οποίο τα διαχειρίζεται είναι εντελώς ανεξάρτητα από το πρωτόκολλο του Bitcoin και το δίκτυό του. Ενώ η χρήση τους ενεργοποιεί ενδιαφέροντα χαρακτηριστικά του κρυπτονομίσματος, όπως είναι ο αποκεντρωμένος έλεγχος, η επιβεβαίωση ιδιοκτησίας και το κρυπτογραφικό μοντέλο ασφάλειας.

Οι συναλλαγές των bitcoins για να μπορέσουν να επιβεβαιωθούν και να προστεθούν στην Blockchain, πρέπει να είναι ψηφιακά υπογεγραμμένες από κάποιο κρυφό κλειδί. Ο κάτοχος του κρυφού κλειδιού επί της ουσίας έχει τον έλεγχο των κρυπτονομισμάτων.

Τα κλειδιά δημιουργούνται σε ζευγάρια, το ιδιωτικό (κρυφό) κλειδί και το δημόσιο. Σε αντιστοίχιση με το τραπεζικό σύστημα, το δημόσιο κλειδί είναι ότι το IBAN ενός τραπεζικού λογαριασμού, ενώ το ιδιωτικό κλειδί έχει όμοιο ρόλο με το κρυφό κωδικό PIN μιας πιστωτικής κάρτας. Τα ψηφιακά κλειδιά είναι αποθηκευμένα σε αρχεία και η διαχείριση τους πραγματοποιείται από το λογισμικό του πορτοφολιού, οπότε ένας χρήστης του Bitcoin σχεδόν ποτέ δεν έρχεται σε επαφή μαζί τους. Αντίθετα ένας χρήστης χρησιμοποιεί για τις συναλλαγές τις διευθύνσεις των πορτοφολιών, οι οποίες αντιστοιχούν με το όνομα του εντολέα σε μια επιταγή, όταν αναφερόμαστε στο τραπεζικό σύστημα.

Κρυπτογράφηση δημοσίου κλειδιού

Η κρυπτογράφηση δημόσιου κλειδιού εφευρέθηκε το 1970 και αποτελεί πηγή για την ασφάλεια υπολογιστικών συστημάτων και πληροφοριών. Η μέθοδος έχει εξελιχθεί και χρησιμοποιούνται διαφορετικά μαθηματικά εργαλεία σε σχέση με την αρχική έκδοση. Το Bitcoin χρησιμοποιεί την κρυπτογράφηση δημόσιου κλειδιού με σκοπό να δημιουργήσει, ξεκινώντας από ένα τυχαίο ιδιωτικό κλειδί, ένα μοναδικό δημόσιο κλειδί. Το δημόσιο κλειδί χρησιμοποιείται για να λάβει ένας χρήστης κρυπτονομίσματα στο πορτοφόλι του, ενώ το ιδιωτικό κλειδί για να υπογράψει ψηφιακά μια συναλλαγή. Ανάμεσα στα δύο κλειδιά υπάρχει μαθηματική σχέση, η οποία επιτρέπει στο ιδιωτικό κλειδί να υπογράφει τις συναλλαγές και η επικύρωση της υπογραφής να πραγματοποιείται με χρήση του δημοσίου κλειδιού χωρίς να αποκαλύπτεται το ιδιωτικό κλειδί.

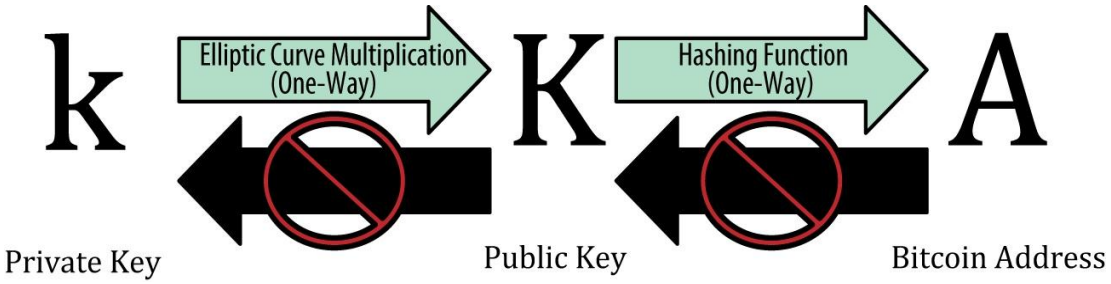
Όταν ένας χρήστης επιθυμεί να ξοδέψει τα κρυπτονομίσματά του παρουσιάζει το δημόσιο κλειδί και μια συναλλαγή υπογεγραμμένη από το ιδιωτικό κλειδί του. Με αυτά τα δύο στοιχεία οποιοσδήποτε κόμβος στο δίκτυο του Bitcoin μπορεί να επιβεβαιώσει αν η συναλλαγή είναι έγκυρη και αν ο χρήστης όντως κατέχει τα κρυπτονομίσματα τα οποία επιθυμεί να ξοδέψει την δεδομένη χρονική στιγμή.

Δημόσιο/Ιδιωτικό κλειδί – Διευθύνσεις

Το ιδιωτικό κλειδί, το δημόσιο κλειδί και η διεύθυνση ενός χρήστη συνδέονται αναμεταξύ τους. Αρχικά το ιδιωτικό κλειδί αποτελεί ένα αριθμό ο οποίος επιλέγεται τυχαία. Στην συνέχεια με χρήση της κρυπτογραφικής μαθηματικής συνάρτησης, πολλαπλασιασμός ελλειπτικής καμπύλης, δημιουργείται από το ιδιωτικό το αντίστοιχο δημόσιο κλειδί. Με τον ίδιο τρόπο από το δημόσιο κλειδί με χρήση μιας

κρυπτογραφικής συνάρτησης κατακερματισμού παράγεται η Bitcoin διεύθυνση του χρήστη. Αξίζει να αναφερθεί ότι οι συναρτήσεις που χρησιμοποιούνται είναι μίας διαδρομής και δεν αντιστρέφονται, δηλαδή από την διεύθυνση δεν μπορούμε να επιστρέψουμε στο δημόσιο κλειδί και αντίστοιχα από το δημόσιο κλειδί στο ιδιωτικό.

**Πηγή: Antonopoulos A. (2017): Mastering Bitcoin*



Εικόνα 4: Συσχέτιση ιδιωτικού, δημοσίου κλειδιού και διεύθυνσης Bitcoin

Το ιδιωτικό κλειδί είναι απλά ένας αριθμός που επιλέγεται τυχαία. Η ιδιοκτησία και ο έλεγχος αυτού του αριθμού συνδέει τον χρήστη με τα κρυπτονομίσματα τα οποία συσχετίζονται με την συγκεκριμένη διεύθυνση. Για τον λόγο αυτό το ιδιωτικό κλειδί πρέπει να παραμένει κρυφό συνεχώς και η γνωστοποίηση του κλειδιού σε κάποιον τρίτο, αντιστοιχεί με την μεταφορά του ελέγχου των κρυπτονομισμάτων σε αυτόν. Επίσης σε περίπτωση απώλειας του ιδιωτικού κλειδιού, τα κρυπτονομίσματα που συνδέονται με την συγκεκριμένη διεύθυνση είναι μη ανακτήσιμα και η δυνατότητα χρήσης τους χάνεται για πάντα.

Η Bitcoin διεύθυνση είναι μια σειρά από ψηφία και χαρακτήρες, η οποία μπορεί να κοινοποιηθεί σε οποιονδήποτε, με σκοπό την αποστολή κρυπτονομισμάτων προς την συγκεκριμένη διεύθυνση. Όλες οι διευθύνσεις που δημιουργούνται από τα αντίστοιχα δημόσια κλειδιά ξεκινούν με το ψηφίο "1".

Πορτοφόλια Bitcoin

Στην περίπτωση του Bitcoin η λέξη "πορτοφόλι" ανάλογα με την οπτική γωνία ανάλυσης του κρυπτονομίσματος περιγράφει διαφορετικά πράγματα. Για έναν καθημερινό χρήστη του κρυπτονομίσματος το πορτοφόλι είναι μια εφαρμογή που αποτελεί το κύριο περιβάλλον με το οποίο έρχεται σε επαφή. Το πορτοφόλι παρέχει πρόσβαση στα νομίσματα του χρήστη, διαχειρίζεται τα κλειδιά και τις διευθύνσεις του, ενώ μέσω αυτού μπορεί να δημιουργήσει και να υπογράψει ψηφιακά συναλλαγές. Αντίθετα, από την οπτική ενός προγραμματιστή το πορτοφόλι είναι μια δομή δεδομένων, η οποία υλοποιείται με χρήση δομημένων αρχείων ή απλών βάσεων δεδομένων.

Πριν ξεκινήσει η ανάλυση και η παρουσίαση των πορτοφολιών Bitcoin, σημαντικό θα είναι να αναφερθεί η βασική παρανόηση στην οποία υποπίπτουν οι αρχάριοι χρήστες. Τα πορτοφόλια Bitcoin δεν περιέχουν κρυπτονομίσματα. Στην πραγματικότητα τα πορτοφόλια περιέχουν μόνο κλειδιά. Τα κρυπτονομίσματα είναι καταγεγραμμένα στην Blockchain, η οποία διατηρείται από το δίκτυο του Bitcoin. Οι χρήστες διαχειρίζονται τα κρυπτονομίσματά τους με το να υπογράφουν ψηφιακά συναλλαγές χρησιμοποιώντας τα κλειδιά που είναι αποθηκευμένα στο πορτοφόλι τους.

Με σκοπό να αποτρέψουν μη εξουσιοδοτημένους χρήστες από το να έχουν πρόσβαση στα κρυπτονομίσματα τα περισσότερα πορτοφόλια κρυπτογραφούν τα ιδιωτικά κλειδιά τα οποία διατηρούν αποθηκευμένα. Η μέθοδος κρυπτογράφησης ονομάζεται συμμετρικού κλειδιού και βασίζεται σε έναν κωδικό τον οποίο θέτει και χρησιμοποιεί ο νόμιμος χρήστης ώστε να έχει πρόσβαση στα κρυπτονομίσματά του. Αναλυτικότερα το πορτοφόλι απαιτεί από τον νόμιμο χρήστη τον κωδικό πρόσβασης όταν χρειάζεται να υπογράψει ψηφιακά μια συναλλαγή, ώστε να μπορέσει να αποκρυπτογραφήσει το ιδιωτικό κλειδί και να το χρησιμοποιήσει. Με το πέρας της υπογραφής το ιδιωτικό κλειδί επιστρέφει στην κρυπτογραφημένη κατάσταση και όλα τα υπόλοιπα δεδομένα διαγράφονται. Ο όρος συμμετρικό αναφέρεται στο γεγονός ότι ο ίδιος κωδικός χρησιμοποιείται κατά την διάρκεια της κρυπτογράφησης αλλά και της αποκρυπτογράφησης των ιδιωτικών κλειδιών. (Franco, 2015)

Η συγκεκριμένη μεθοδολογία θεσπίζει ένα αρχικό επίπεδο ασφάλειας σε περίπτωση που ένας κακόβουλος χρήστης αποκτήσει αντίγραφο του πορτοφολιού κάποιου χρήστη. Ωστόσο η ισχύς της μεθόδου σχετίζεται άμεσα με τον κωδικό πρόσβασης τον οποίο έχει θέσει ο νόμιμος χρήστης και επειδή ο χρήστης αποτελεί έναν άνθρωπο η πολυπλοκότητα του κωδικού που επιλέγει είναι υπολογιστικά περιορισμένη.

Ντετερμινιστικά / Μη ντετερμινιστικά πορτοφόλια.

Τα πρώτα πορτοφόλια Bitcoin που σχεδιάστηκαν λειτουργούσαν με μη ντετερμινιστική τεχνολογία και αποτελούσαν συλλογές από τυχαία ιδιωτικά κλειδιά, τα οποία δεν σχετίζονταν αναμεταξύ τους και μπορούσαν να χρησιμοποιηθούν μόνο μια φορά. Η μη συσχέτιση των ιδιωτικών κλειδιών είχε ως αποτέλεσμα την αυξημένη ασφάλεια των συγκεκριμένων πορτοφολιών, ωστόσο είχε σημαντικά μειονεκτήματα που αφορούσαν κυρίως την ευκολία της χρήσης τους. Αναλυτικότερα οι χρήστες έπρεπε να δημιουργούν ανά τακτά χρονικά διαστήματα αντίγραφα ασφαλείας διότι σε περίπτωση απώλειας του πορτοφολιού δεν υπήρχε δυνατότητα ανάκτησης των ιδιωτικών κλειδιών.

Ενώ ταυτόχρονα η διαχείριση και η χρήση των ιδιωτικών κλειδιών αντιμετώπιζε ζητήματα. Σήμερα μη ντετερμινιστικά πορτοφόλια χρησιμοποιούνται κυρίως για δοκιμές ή σε μεμονωμένες περιπτώσεις.

Τα μειονεκτήματα των μη ντετερμινιστικών πορτοφολιών επιλύθηκαν από τα νεότερα ντετερμινιστικά πορτοφόλια θυσιάζοντας ένα μέρος της ασφάλειάς τους. Η βασική σχεδιαστική διαφορά έγκειται στο γεγονός ότι όλα τα ιδιωτικά κλειδιά του πορτοφολιού δημιουργούνται από ένα μοναδικό κύριο κλειδί το οποίο ονομάζεται "σπόρος" (seed). Με αποτέλεσμα να υπάρχει συσχέτιση ανάμεσα στα ιδιωτικά κλειδιά, η οποία προσφέρει μια εναλλακτική μέθοδο ανάκτησης σε περίπτωση που κάποιο ιδιωτικό κλειδί χαθεί ή καταστραφεί, ενώ απαιτείται η διατήρηση μόνο ενός αντιγράφου ασφαλείας από τον χρήστη.

Τα βασικά πλεονεκτήματα των ντετερμινιστικών πορτοφολιών, είναι:

- ✓ Λιγότερα αντίγραφα ασφαλείας. Σε αντίθεση με τα μη ντετερμινιστικά πορτοφόλια που χρειάζονταν ανανέωση του αντιγράφου ασφαλείας κάθε φορά που ένα νέο τυχαίο ιδιωτικό κλειδί είχε δημιουργηθεί, τα ντετερμινιστικά απαιτούν ένα αντίγραφο ασφαλείας που διατηρεί το κύριο κλειδί (seed).
- ✓ Αντίγραφα ασφαλείας μικρότερου μεγέθους. Τα ντετερμινιστικά πορτοφόλια απαιτούν την διατήρηση αντιγράφου ασφαλείας μόνο του κύριου κλειδιού, μειώνοντας κατά πολύ μεγάλο βαθμό το μέγεθος του αντιγράφου.
- ✓ Η δημιουργία νέων διευθύνσεων δεν απαιτεί την γνωστοποίηση του ιδιωτικού κλειδιού. Δυνατότητα που προστέθηκε στις τελευταίες εκδόσεις ντετερμινιστικών πορτοφολιών και αυξάνει την ασφάλεια των ιδιωτικών κλειδιών.

Υπάρχουν διάφορες μέθοδοι με τις οποίες μπορούν να δημιουργηθούν τα ιδιωτικά κλειδιά από τον "σπόρο", ωστόσο η πιο διαδεδομένη ονομάζεται κώδικας μνημονικών λέξεων και βασίζεται σε 12 λέξεις κλειδιά τις οποίες θέτει ο χρήστης κατά την περίοδο αρχικοποίησης του πορτοφολιού του αλλά και στην συνάρτηση κατακερματισμού SHA256.

Offline / Online πορτοφόλια

Οι περισσότερες συσκευές οι οποίες εκτελούν λογισμικό πορτοφολιού Bitcoin είναι συνδεδεμένες στο διαδίκτυο, ώστε να μπορούν να επικοινωνούν με το υπόλοιπο δίκτυο του Bitcoin και να ανταλλάσουν χρήσιμες για την λειτουργία τους πληροφορίες. Σε αυτή την περίπτωση τα πορτοφόλια χαρακτηρίζονται "online". Ωστόσο από την στιγμή

που κάποια συσκευή είναι συνδεδεμένη στο διαδίκτυο ενέχει τον κίνδυνο να εκτεθεί σε ενέργειες κακόβουλων χρηστών του διαδικτύου. Σε συνδυασμό με το γεγονός ότι τα διάφορα είδη πορτοφολιών είναι ευαίσθητα σε επιθέσεις κακόβουλων χρηστών αλλά και γιατί μπορεί να εμπεριέχουν ιδιωτικά κλειδιά τα οποία να σχετίζονται με μεγάλης αξίας κρυπτονομίσματα, έχουν δημιουργηθεί πορτοφόλια και μέθοδοι, που δεν απαιτούν την συνεχή σύνδεση στο διαδίκτυο. Η κατηγορία αυτή ονομάζεται ως "offline" πορτοφόλια. Ένας γενικός κανόνας ασφαλείας ο οποίος προτείνεται είναι σε "online" πορτοφόλια να αποθηκεύονται κρυπτονομίσματα για καθημερινή χρήση, ενώ "offline" πορτοφόλια να προτιμούνται όταν τα ιδιωτικά κλειδιά σχετίζονται με μεγαλύτερης αξίας διευθύνσεις.

Ψυχρή αποθήκευση (cold storage)

Μια κατηγορία offline μεθόδων με τις οποίες προστατεύονται ιδιωτικά κλειδιά είναι η ψυχρή αποθήκευση (cold storage). Τα ιδιωτικά κλειδιά στην περίπτωση αυτή δεν είναι προσβάσιμα μέσω διαδικτύου και η χρήση τους απαιτεί την εισαγωγή τους σε κάποιο online ή offline πορτοφόλι. Ωστόσο οι συγκεκριμένες μέθοδοι αποτελούν τους ασφαλέστερους τρόπους διατήρησης ιδιωτικών κλειδιών. Υπάρχουν επιχειρήσεις παγκοσμίου βεληνεκούς οι οποίες δραστηριοποιούνται στο τομέα της ψυχρής αποθήκευσης ιδιωτικών κλειδιών, τα οποία σύμφωνα με έρευνες, συσχετίζονται με κρυπτονομίσματα αξίας περίπου 10 δισεκατομμυρίων δολαρίων (με μέση ισοτιμία Απριλίου 2018, ανάμεσα σε δολάριο Η.Π.Α. και Bitcoin). (Metcalf, 2018)

Στην ψυχρή αποθήκευση χρησιμοποιούνται:

Εξωτερικά μέσα αποθήκευσης: Με την ίδια λογική με την οποία μπορούμε να αποθηκεύσουμε ένα αρχείο ήχου ή μια ταινία σε ένα εξωτερικό μέσο αποθήκευσης, όμοια μπορούμε να αποθηκεύουμε ιδιωτικά κλειδιά σε USB flash drives ή σε σκληρούς δίσκους. Επιπρόσθετα μπορούμε να αυξήσουμε την ασφάλεια κρυπτογραφώντας το εξωτερικό μέσο αποθήκευσης. Η χρήση των συσκευών αυτών έχει δύο τρωτά σημεία. Το πρώτο είναι ότι μπορούν να τεθούν εκτός λειτουργίας λόγω τεχνικών προβλημάτων και το δεύτερο ότι είναι απαραίτητο να εισάγουμε τα κλειδιά σε κάποιο πορτοφόλι για να μπορέσουμε να τα χρησιμοποιήσουμε.

Χάρτινα πορτοφόλια: Τα ιδιωτικά κλειδιά μπορούν να εκτυπωθούν σε ένα κομμάτι χαρτί, την ιδιότητα αυτή χρησιμοποιούν τα χάρτινα πορτοφόλια. Τα οποία ονομάζονται πορτοφόλια αλλά επί τεχνικής άποψης δεν αποτελούν τέτοια. Συνήθως μαζί με το ιδιωτικό κλειδί εκτυπώνονται και το δημόσιο κλειδί αλλά και η διεύθυνση Bitcoin. Τα

ιδιωτικά κλειδιά είναι 256 bit (32 byte) ακέραιοι και μπορούν να παρουσιαστούν με διαφορετικές τεχνικές.

Η εκτύπωση στο χαρτί εκτός από την απευθείας μορφή κειμένου μπορεί να πραγματοποιηθεί με την χρήση QR code. Αντίστοιχα τα μειονεκτήματα της συγκεκριμένης μεθόδου σχετίζονται με την φυσική φθορά ή απώλεια του χάρτινου πορτοφολιού.

Offline πορτοφόλια

Η λειτουργία ενός offline πορτοφολιού απαιτεί την συνεργασία δύο συσκευών, μιας συνδεδεμένης στο διαδίκτυο και μιας που να παραμένει συνεχώς offline. Στην συνδεδεμένη συσκευή διατηρούνται το δημόσιο κλειδί και η διεύθυνση Bitcoin, ενώ στην offline το ιδιωτικό κλειδί του χρήστη. Οι συναλλαγές δημιουργούνται στην συνδεδεμένη συσκευή, ωστόσο δεν μπορούν να υπογραφούν ψηφιακά από την ίδια, διότι δεν διατηρεί αντίγραφο του ιδιωτικού κλειδιού. Με αποτέλεσμα οι συναλλαγές για να υπογραφούν ψηφιακά και να θεωρούνται έγκυρες να πρέπει να αποσταλούν στην offline συσκευή. Συνήθως η επικοινωνία της συνδεδεμένης συσκευής με την offline πραγματοποιείται μέσω USB θύρας ή εκτυπωμένων QR code, σημείο το οποίο αποτελεί και το σχετικά ευάλωτο των offline πορτοφολιών.

Συνοψίζοντας οι online συσκευές διατηρούν το ισοζύγιο των κρυπτονομισμάτων που κατέχει ο χρήστης και δημιουργούν συναλλαγές. Αντίστοιχα οι offline συσκευές επειδή δεν μπορούν να επικοινωνήσουν με το δίκτυο του Bitcoin δεν είναι δυνατό να διατηρούν αυτές τις πληροφορίες. Ο ρόλος τους είναι να υπογράφουν ψηφιακά τις συναλλαγές που τους αποστέλλουν οι συνδεδεμένες συσκευές. Σε περίπτωση που η συνδεδεμένη συσκευή εκτεθεί σε ενέργειες κακόβουλων χρηστών, μειώνεται η ιδιωτικότητα του πορτοφολιού αλλά όχι η ασφάλειά του.

Έχει δημιουργηθεί ένα καινούργιο κομμάτι στην βιομηχανία ηλεκτρονικών συσκευών, το οποίο ειδικεύεται σε hardware πορτοφόλια. Δηλαδή συσκευές οι οποίες μοιάζουν εξωτερικά και λειτουργικά με USB flash drives αλλά επιπρόσθετα επιτελούν την λειτουργία της ψηφιακής υπογραφής συναλλαγών. Τα πιο διαδεδομένα hardware πορτοφόλια που κυκλοφορούν αυτή την στιγμή στην αγορά είναι το Ledger Nano S, το Trezor και το KeepKey.

Εικόνα 5: Παράδειγμα ενός Hardware Bitcoin Wallet

Από την άλλη πλευρά τον ρόλο της συνδεδεμένης συσκευής μπορεί να επιτελέσει οποιοσδήποτε ηλεκτρονικός υπολογιστής ο οποίος έχει πρόσβαση στο διαδίκτυο και εκτελεί το λογισμικό του πορτοφολιού, ώστε να μπορεί να επικοινωνεί με την offline συσκευή. Με σκοπό να αποστέλλει συναλλαγές και να τις λαμβάνει πίσω υπογεγραμμένες ψηφιακά από το ιδιωτικό κλειδί.

Online πορτοφόλια

Ένας χρήστης με την βοήθεια ενός προγράμματος φυλλομετρητή (browser) μπορεί να δημιουργήσει το προσωπικό του online πορτοφόλι, καθώς τα online πορτοφόλια αποτελούν λογαριασμούς (accounts) σε κάποιον εξωτερικό πάροχο. Ο πάροχος είναι υπεύθυνος για την προστασία των κλειδιών, την διαχείριση των διευθύνσεων και την υλοποίηση των συναλλαγών. Οι νέοι χρήστες χρειάζεται μόνο να συμπληρώσουν και να επιβεβαιώσουν τα ζητούμενα προσωπικά στοιχεία. Τα online πορτοφόλια μειώνουν σε μεγάλο βαθμό τα εμπόδια εισαγωγής νέων χρηστών στην αγορά των κρυπτονομισμάτων, χαρακτηριστικό το οποίο αποτελεί και το βασικό τους πλεονέκτημα.

Η χρήση ενός online πορτοφολιού μοιάζει σε μεγάλο βαθμό με την online τραπεζική και τις εφαρμογές web banking που προσφέρουν τα τραπεζικά ιδρύματα. Διότι οι "καταθέσεις" διαχειρίζονται από κάποιον τρίτο. Σε αντίθεση με τα τραπεζικά ιδρύματα οι πάροχοι υπηρεσιών online πορτοφολιών δεν μπορούν να εγγυηθούν για τα κρυπτονομίσματα των χρηστών τους. Στοιχείο ιδιαίτερα αρνητικό αν αναλογιστεί κανείς πως εταιρείες που παρέχουν τέτοιου είδους υπηρεσίες αποτελούν τον νούμερο

ένα στόχο κακόβουλων χρηστών. Επιτυχημένες επιθέσεις είχαν ως αποτέλεσμα πολλοί χρήστες να χάσουν τα κρυπτονομίσματά τους και η τιμή του Bitcoin να δεχθεί ισχυρά πλήγματα.

Οι μέθοδοι με τις οποίες προστατεύουν οι εταιρείες τα ιδιωτικά κλειδιά είναι παρόμοιες με τις μεθόδους που έχουν στην διάθεση τους και οι μεμονωμένοι χρήστες. Για τον λόγο αυτό, όπως είχε τονιστεί και προηγουμένως, τα online πορτοφόλια προτείνεται να χρησιμοποιούνται για κρυπτονομίσματα απαραίτητα για καθημερινές συναλλαγές και όχι για ιδιωτικά κλειδιά που σχετίζονται με μεγάλες χρηματικές αξίες. Όσον αφορά την ανωνυμία των χρηστών online πορτοφολιών υπάρχει ένα θετικό και ένα αρνητικό στοιχείο. Το θετικό στοιχείο είναι ότι οι διευθύνσεις Bitcoin διαχειρίζονται από τον πάροχο οπότε δεν υπάρχει άμεση συσχέτιση κάποιου χρήστη με μια διεύθυνση Bitcoin, αυξάνοντας έτσι την ανωνυμία. Ωστόσο οι πάροχοι για να επιβεβαιώσουν και να επιτρέψουν την χρήση υπηρεσιών online πορτοφολιών απαιτούν από τους χρήστες περισσότερες προσωπικές πληροφορίες από αυτές που είναι απαραίτητες για την συμμετοχή τους στην οικονομία του Bitcoin, μειώνοντας την ανωνυμία τους.

Μια νέα κατηγορία online πορτοφολιών είναι τα λεγόμενα υβριδικά. Το χαρακτηριστικό που τα κάνει να διαφέρουν από τα κλασικά online πορτοφόλια είναι ότι ενώ όλες οι διαδικασίες και οι ενέργειες πραγματοποιούνται μέσω των υπηρεσιών που προσφέρουν οι πάροχοι, τα ιδιωτικά κλειδιά των χρηστών δεν φυλάσσονται από τους παρόχους αλλά είναι αποθηκευμένα στον προσωπικό υπολογιστή ή στο smart phone του χρήστη. Μειώνοντας τον κίνδυνο που σχετίζεται με την απώλεια δεδομένων λόγω υπαιτιότητας του παρόχου.

Διαδικασία εξόρυξης Bitcoin (mining)

Η διαδικασία που θα μελετηθεί στο συγκεκριμένο κεφάλαιο ονομάζεται “εξόρυξη”. Η ονομασία μπορεί να οδηγήσει τους αναγνώστες σε παραπλανητικούς συνειρμούς, καθώς συσχετίζοντας τον όρο με την διαδικασία εξαγωγής πολύτιμων λίθων από το υπέδαφος, μπορεί να θεωρηθεί ότι η δημιουργία νέων νομισμάτων Bitcoin είναι ο κύριος σκοπός της εξόρυξης. Παρόλο που η συγκεκριμένη ανταμοιβή αποτελεί το βασικό κίνητρο της διαδικασίας, ο κύριος σκοπός της δεν είναι αυτός. Η εξόρυξη είναι ο μηχανισμός που εξασφαλίζει την αποκέντρωση του συστήματος του Bitcoin. Είναι η εφεύρεση η οποία το κάνει μοναδικό, ένας αποκεντρωμένος μηχανισμός ασφάλειας που αποτελεί την βάση ενός peer-to-peer ψηφιακού νομίσματος. (Antonopoulos, 2017)

Η εξόρυξη διασφαλίζει την εύρυθμη λειτουργία του συστήματος του Bitcoin και ουσιαστικά αντικαθιστά την κεντρική αρχή που διαθέτουν τα τραπεζικά συστήματα. Αντίστοιχα η δημιουργία νέων νομισμάτων Bitcoin μέσω της διαδικασίας της εξόρυξης εκτός από ένα ισχυρό κίνητρο συμμετοχής στην διαδικασία, αποτελεί και την προσφορά χρήματος της ηλεκτρονικής οικονομίας που σχηματίζεται.

Αναλυτικότερα η διαδικασία της εξόρυξης περιλαμβάνει την επικύρωση των συναλλαγών που εντάσσονται στα Block συναλλαγών και την προσθήκη τους στο παγκόσμιο αρχείο της Blockchain. Όπως έχει περιγραφεί και σε προηγούμενο στάδιο της εργασίας ένα νέο Block συναλλαγών προχωράει στο στάδιο της εξόρυξης κατά μέσο όρο κάθε 10 λεπτά. Οι συναλλαγές από την στιγμή που προστίθενται στην Blockchain θεωρούνται επιβεβαιωμένες και οι ιδιοκτήτες των διευθύνσεων που λαμβάνουν τα κρυπτονομίσματα έχουν το δικαίωμα να τα χρησιμοποιήσουν.

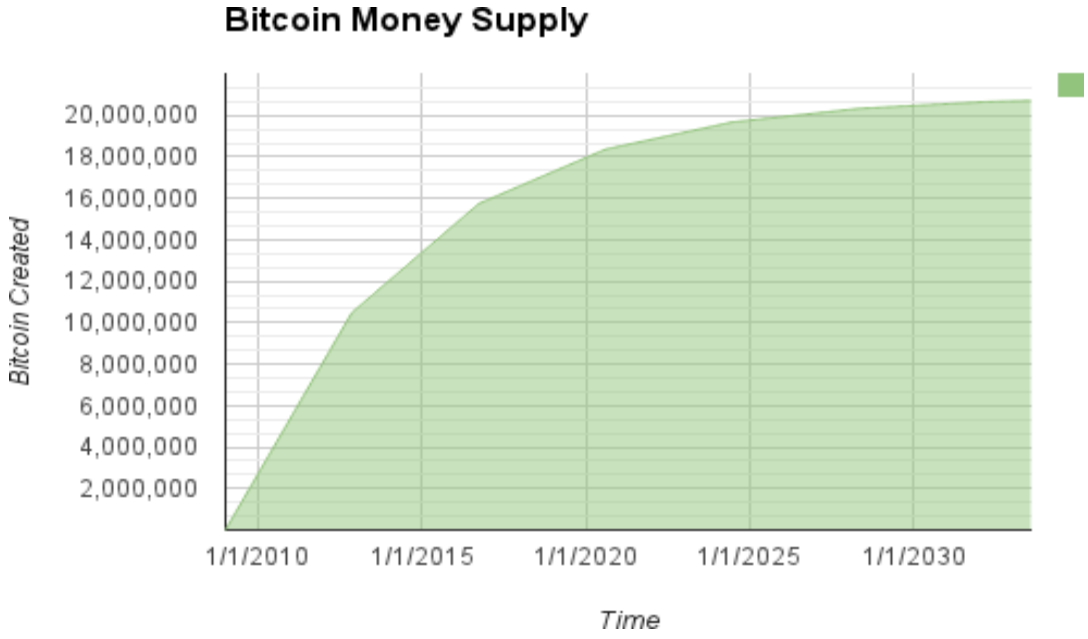
Τα άτομα που προσφέρουν την υπολογιστική ισχύ των μηχανημάτων τους και συμμετέχουν στην διαδικασία της εξόρυξης ανταγωνίζονται για την επίλυση ενός σύνθετου μαθηματικού προβλήματος που βασίζεται σε κρυπτογραφικό αλγόριθμο κατακερματισμού. Η λύση του προβλήματος της κατηγορίας Proof-of-Work περιλαμβάνεται στην κεφαλή του Block συναλλαγών, με σκοπό να λειτουργεί ως πειστήριο ότι το συγκεκριμένο άτομο κατέβαλε σημαντική υπολογιστική προσπάθεια. Ο ανταγωνισμός που δημιουργείται ανάμεσα στα διαφορετικά μηχανήματα που προσπαθούν να επιλύσουν το πρόβλημα και να κερδίσουν την επιβράβευση είναι η κεντρική ιδέα του μοντέλου ασφάλειας του Bitcoin. Συγκεκριμένα η επιβράβευση περιλαμβάνει δύο στοιχεία. Το πρώτο είναι τα νέα νομίσματα Bitcoin που δημιουργούνται με την ολοκλήρωση των εξόρυξης ενός νέου Block συναλλαγών και το δεύτερο οι χρεώσεις τις οποίες καταβάλουν οι χρήστες για να προσθέσουν τις συναλλαγές τους στο επόμενο Block που θα εξορυχτεί. (BitcoinWiki, 2016)

Δημιουργία νέων νομισμάτων (προσφορά χρήματος) και χρεώσεις

Η διαδικασία ονομάζεται “εξόρυξη” διότι η δημιουργία νέων νομισμάτων Bitcoin ως επιβράβευση για την συμμετοχή, έχει σχεδιαστεί ώστε να προσομοιώνει την εξέλιξη φθινόντων στοιχείων, όπως είναι τα πολύτιμα μέταλλα. Η προσφορά χρήματος στην οικονομία του Bitcoin λειτουργεί μέσω της διαδικασίας της εξόρυξης και λειτουργεί ως καθ’ ομοίωση του τρόπου με τον οποίο οι κεντρικές τράπεζες αποφασίζουν την εκτύπωση νέου χρήματος. Η μέγιστη ανταμοιβή με την οποία μπορεί να αμειφτεί κάποιος συμμετέχοντας ως επιβράβευση για την εξόρυξη ενός νέου Block συναλλαγών

μειώνεται περίπου ανά τέσσερα χρόνια (ή διαφορετικά ανά 210.000 Blocks). Στο ξεκίνημα του Bitcoin, Ιανουάριος 2009, η αμοιβή για την εξόρυξη ενός νέου Block συναλλαγών ήταν 50 νέα bitcoins. Τον Νοέμβριο του 2012 μειώθηκε στα μισά, δηλαδή 25 bitcoins. Αντίστοιχα το ίδιο συναίβει και τον Ιούλιο του 2016, 12,5 νέα bitcoins. Το 2020 προβλέπεται να υπάρξει η επόμενη μείωση της ανταμοιβής. Βασισμένη σε αυτή την μεθοδολογία, η ανταμοιβή με νέα bitcoins θα μειώνεται εκθετικά περίπου μέχρι το έτος 2140, όπου τότε θα ολοκληρωθεί η δημιουργία όλων των Bitcoin νομισμάτων που θα κυκλοφορήσουν (20,99999998 εκατομμύρια). Μετά το 2140 δεν θα δημιουργηθούν ξανά νέα bitcoins.

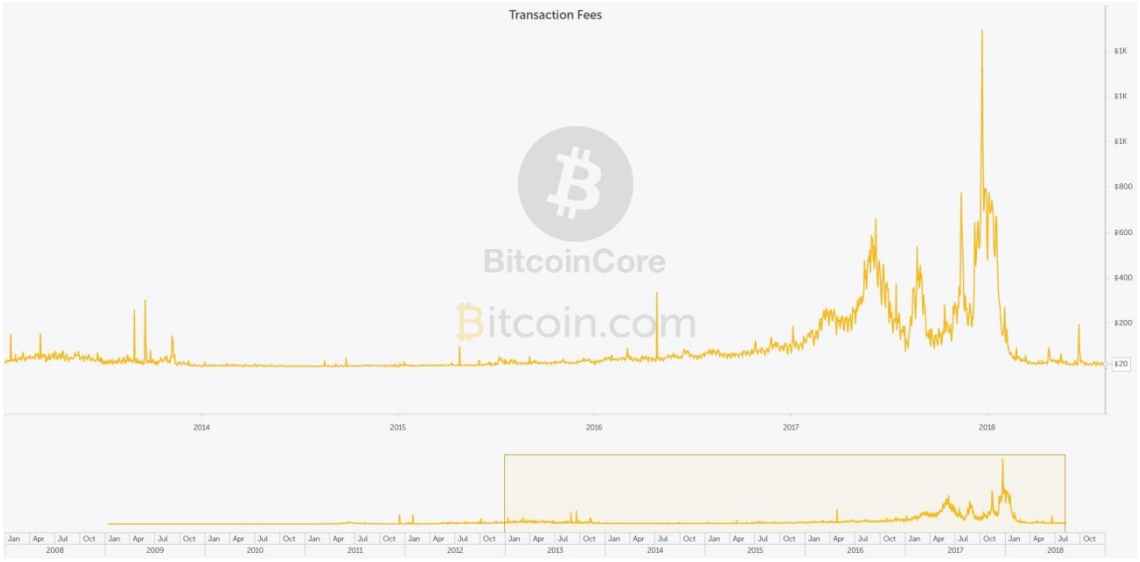
**Πηγή: Antonopoulos A. (2017): Mastering Bitcoin*



Εικόνα 6: Προσφορά χρήματος στην οικονομία του Bitcoin

Το δεύτερο στοιχείο με το οποίο αμείβεται κάποιος που συμμετέχει στην διαδικασία της εξόρυξης, είναι οι χρεώσεις που προκύπτουν για την διεκπεραίωση των συναλλαγών. Αναλυτικότερα κάθε συναλλαγή μπορεί να περιλαμβάνει χρέωση, η οποία υπολογίζεται από την διαφορά ανάμεσα στο ποσό πίστωσης και στο ποσό χρέωσης των διευθύνσεων που συμμετέχουν στην συγκεκριμένη συναλλαγή. Το άθροισμα των διαφορών που προκύπτουν από τις συναλλαγές ενός Block αποδίδονται στο άτομο που θα καταφέρει να εξορύξει το συγκεκριμένο Block συναλλαγών. Σήμερα, οι χρεώσεις αποτελούν ένα πολύ μικρό ποσοστό της συνολικής επιβράβευσης, περίπου 0,5%, καθώς τα νέα bitcoins είναι πολύ μεγαλύτερης αξίας. Ωστόσο η εκθετική μείωση των νέων bitcoins που θα αποδίδονται ως ανταμοιβή αλλά και η ταυτόχρονη αύξηση του αριθμού των συναλλαγών που θα περιέχονται σε ένα Block συναλλαγών θα έχει ως αποτέλεσμα να αυξάνεται διαχρονικά η επιβράβευση μέσω χρεώσεων. Σταδιακά το στοιχείο των

χρεώσεων θα αυξάνει την δυναμική του ενώ μετά το έτος 2140 περίπου, θα αποτελεί το μοναδικό στοιχείο επιβράβευσης για όσους συμμετέχουν στην διαδικασία της εξόρυξης. (Huberman, et al., 2017)



Εικόνα 7: Επιπρόσθετες χρεώσεις συναλλαγών **Bitcoin**

Η πεπερασμένη και φθίνουσα δημιουργία νέων νομισμάτων Bitcoin έχει ως αποτέλεσμα μια σταθερή προσφορά χρήματος, η οποία αντιστέκεται στις πληθωριστικές τάσεις. Σε αντίθεση με τα εκτυπώσιμα νομίσματα (fiat currencies), των οποίων η προσφορά μπορεί να αυξηθεί, θεωρητικά σε άπειρο βαθμό, μέσω της εκτύπωσης νέων νομισμάτων από την κεντρική τράπεζα. Η σημαντική αυτή οικονομική ιδιότητα του Bitcoin θα αναλυθεί εκτενέστερα στην συνέχεια της παρούσης εργασίας, στο τμήμα της οικονομικής ανάλυσης του κρυπτονομίσματος. (Ma, et al., 2018)

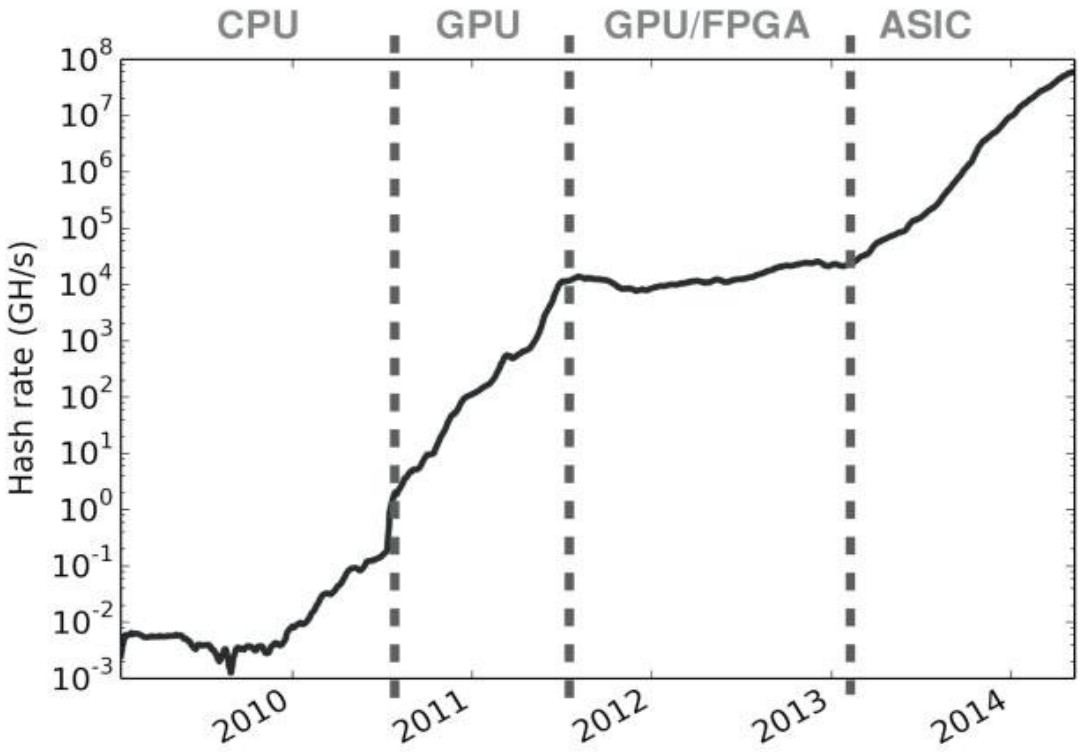
Εξοπλισμός εξόρυξης (Από τις CPUs στα ASICs)

Σε προηγούμενο κεφάλαιο της παρούσης εργασίας αναλύθηκε το δίκτυο του Bitcoin και η peer-to-peer αρχιτεκτονική του, οποιοσδήποτε μπορεί να γίνει μέλος του δικτύου χωρίς να χρειάζεται την άδεια και την έγκριση κανενός. Δηλαδή δεν υπάρχουν εμπόδια εισαγωγής και κανείς δεν μπορεί να απαγορέψει ή να περιορίσει την εισαγωγή νέων ατόμων. Σε περίπτωση που οι νέοι συμμετέχοντες επιθυμούν να συμμετέχουν στην διαδικασία της εξόρυξης μπορούν να ξεκινήσουν αμέσως.

Σήμερα η συνολική υπολογιστική ισχύς του δικτύου του Bitcoin υπολογίζεται περίπου στα 30.000.000 TH/s (= 30.000 PH/s), διατηρώντας λογαριθμικό ρυθμό αύξησης. Η διαχρονική πορεία της υπολογιστικής ισχύς του δικτύου χωρίζεται σε εποχές, τις οποίες καθόρισαν δύο σημαντικοί παράγοντες:

- Η ραγδαία αύξηση της τιμής του Bitcoin, αποτέλεσε κίνητρο για επενδύσεις στον τομέα της εξόρυξης.
- Η πρόοδος της τεχνολογίας που αφορά τις συσκευές εξόρυξης. Καθώς οι κατασκευαστές κατάφεραν να σχεδιάσουν και να υλοποιήσουν ολοκληρωμένα κυκλώματα (chips), τα οποία χαρακτηρίζονται από καλύτερη αποδοτικότητα.

**Πηγή: Franco P. (2015): Understanding Bitcoin*



Εικόνα 8: Hash rate του δικτύου Bitcoin και εποχές εξόρυξης

Η κάθε εποχή συνδέεται με συγκεκριμένες συσκευές, τις οποίες χρησιμοποιούσαν για την διαδικασία της εξόρυξης. Σε αρχικό στάδιο γινόταν χρήση των επεξεργαστών (CPUs) των ηλεκτρονικών υπολογιστών. Στην συνέχεια η ανάπτυξη της τεχνολογίας στις κάρτες γραφικών (GPUs), οδήγησε τον τομέα στην δικιά τους κατεύθυνση. Μέχρις ότου δημιουργήθηκαν ειδικά σχεδιασμένα ολοκληρωμένα κυκλώματα (chips) για την διαδικασία της εξόρυξης (FPGAs), ενώ λογική εξέλιξη ήταν και η υλοποίηση μηχανημάτων ειδικά σχεδιασμένων (ASICs) ώστε να επιλύουν προβλήματα που βασίζονται στον αλγόριθμο κατακερματισμού SHA256. (Franco, 2015)

CPUs (Central Processing Units): Ονομάζονται οι κεντρικές μονάδες επεξεργασίας των ηλεκτρονικών υπολογιστών ή και γενικότερα των εξελιγμένων ηλεκτρονικών συσκευών. Είναι συσκευές γενικού χαρακτήρα και δεν ειδικεύονται στην επεξεργασία συγκεκριμένου τύπου δεδομένων. Στα πρώτα χρόνια του Bitcoin, από το 2009 έως και το καλοκαίρι του 2010, η εξόρυξη πραγματοποιούταν εξ' ολοκλήρου από τις CPUs. Η

αύξηση της συνολικής επεξεργαστικής ισχύος του δικτύου ήταν αποτέλεσμα της συμμετοχής μεγαλύτερου αριθμού ηλεκτρονικών συσκευών στο δίκτυο. Ένας επεξεργαστής που κυκλοφορούσε εκείνη την χρονική περίοδο μπορούσε να προσφέρει υπολογιστική ισχύ περίπου 20 MH/s.

GPUs (Graphics Processing Units): Ονομάζονται οι μονάδες επεξεργασίας γραφικών. Ειδικά σχεδιασμένα ολοκληρωμένα κυκλώματα (chips) που χρησιμοποιούνται στην επεξεργασία δεδομένων απεικόνισης γραφικών. Λόγω της αυξημένης υπολογιστικής δυνατότητας των GPUs, υπάρχει η τάση στην επιστήμη των υπολογιστών να χρησιμοποιούνται και για επεξεργασία δεδομένων διαφορετικού τύπου από τον καθιερωμένο. Μετά τα μέσα του 2010, κυκλοφόρησαν αλγόριθμοι οι οποίοι χρησιμοποιούσαν τις GPUs για την διαδικασία εξόρυξης Bitcoin. Με αποτέλεσμα η εξόρυξη με χρήση των CPUs να τεθεί εκτός αγοράς διότι αποτελούσε μια μη οικονομικά αποδοτική λύση. Οι GPUs είναι αποδοτικότερες στην διαδικασία εξόρυξης Bitcoin επειδή ο σχεδιασμός τους επιτρέπει την ταχύτερη επίλυση προβλημάτων που σχετίζονται με τον αλγόριθμο SHA256. Στην ηλεκτρονική εγκυκλοπαίδεια του Bitcoin υπάρχει εκτενέστερη ανάλυση των λόγων που οι GPUs είναι αποδοτικότερες από τις CPUs για την διαδικασία της εξόρυξης. Τα τελευταία μοντέλα GPUs που κυκλοφορούνε έχουν την δυνατότητα να προσφέρουν υπολογιστική ισχύ περίπου 700 MH/s. (BitcoinWiki, 2013)

FPGAs (Field Programmable Gate Arrays): Αποτελούν ολοκληρωμένα κυκλώματα (chips) σχεδιασμένα ώστε να προγραμματίζονται για την επίλυση συγκεκριμένων προβλημάτων. Από τα μέσα του 2011 τέτοιου είδους ολοκληρωμένα κυκλώματα εισήχθησαν στην αγορά εξόρυξης του Bitcoin ώστε να συναγωνιστούν τις GPUs. Ωστόσο δεν κατάφεραν να τις εκτοπίσουν διότι οι GPUs διέθεταν πλεονέκτημα όσον αφορά το κόστος ανά GH/s αλλά και στην μεταπολιτική αξία. Ενώ τα FPGAs πλεονεκτούσαν στον τομέα της κατανάλωσης ενέργειας. Ένα τυπικό FPGA προσέφερε υπολογιστική ισχύ της τάξεως του 1 GH/s.

ASICs (Application Specific Integrated Circuit): Αποτελούν μηχανήματα τα οποία διαθέτουν ολοκληρωμένα κυκλώματα (chips) για να επιτελούν επεξεργασία δεδομένων για συγκεκριμένες εφαρμογές. Σε αντίθεση με τις CPUs και τις GPUs που είναι γενικότερου χαρακτήρα. Αναλυτικότερα για τις ανάγκες της εξόρυξης Bitcoin σχεδιάστηκαν ολοκληρωμένα κυκλώματα τα οποία επιλύουν προβλήματα βασισμένα στην λογική του αλγορίθμου SHA256. Με αποτέλεσμα να επιτευχθεί υπολογιστική

ισχύ πολλών τάξεων μεγέθους μεγαλύτερη σε σχέση με την μέχρι τότε τεχνολογία. Τα πρώτα ASICs εμφανίστηκαν στις αρχές του 2013 και αποτελούν τα μηχανήματα που χρησιμοποιούνται μέχρι και σήμερα για την εξόρυξη Bitcoin.

Με την πάροδο των χρόνων οι τεχνολογικές αλλαγές στον εξοπλισμό εξόρυξης, αποτέλεσαν την αιτία για εκθετική αύξηση ή ακόμη και άλματα της συνολικής υπολογιστικής ισχύος του δικτύου του Bitcoin. Καθώς γράφεται η παρούσα εργασία η εποχή των ASICs βρίσκεται σε εξέλιξη. Νέες τεχνολογικές αλλαγές στον σχεδιασμό των ολοκληρωμένων κυκλωμάτων (chips) θα επιφέρουν σημαντικές αλλαγές στο περιβάλλον της διαδικασίας εξόρυξης. (Taylor, 2013)

Το δίκτυο του Bitcoin αποτελεί ένα από τα ισχυρότερα υπολογιστικά δίκτυα στον κόσμο. Η υπολογιστική ισχύ που συγκεντρώνεται χρησιμοποιείται ώστε να αυξάνεται η ασφάλεια της Blockchain και του δικτύου γενικότερα. Επιθέσεις της κατηγορίας, 51% Attack, θεωρούνται πλέον εξαιρετικά δύσκολες έως και αδύνατες, καθώς η υλοποίησή τους απαιτεί τεράστιες επενδύσεις σε εξοπλισμό εξόρυξης. Αξίζει να σημειωθεί ωστόσο πως η συνολική υπολογιστική ισχύ του δικτύου του Bitcoin αποτελεί ένα δυναμικά μεταβαλλόμενο μέγεθος του οποίου οι μεταβολές σχετίζονται σε μεγάλο βαθμό με την τιμή του Bitcoin. Διότι, για παράδειγμα, μια μείωση της τιμής του Bitcoin καθιστά πολλά μηχανήματα εξόρυξης παλαιότερης τεχνολογίας μη αποδοτικά με αποτέλεσμα οι ιδιοκτήτες να τερματίζουν την λειτουργία τους. Ενέργεια η οποία μειώνει την συνολική υπολογιστική ισχύ του δικτύου.

Επιχειρήματα επικριτών

Οι επικριτές του Bitcoin βασίζουν την ρητορική τους σε δύο στοιχεία που σχετίζονται με την διαδικασία την εξόρυξης και την τεχνολογία που χρησιμοποιείται. Αρχικά η υπολογιστική ισχύς του δικτύου παράγεται κατά συντριπτική πλειοψηφία από μηχανήματα ASICs. Τα συγκεκριμένα μηχανήματα είναι σχεδιασμένα και κατασκευασμένα ώστε να αποδίδουν στην επίλυση προβλημάτων που βασίζονται στον αλγόριθμο SHA256. Γεγονός το οποίο σημαίνει ότι στην περίπτωση που το Bitcoin αποτύχει, τα μηχανήματα αυτά ουσιαστικά είναι άχρηστα και οι υπολογιστικές τους ικανότητες δεν μπορούν να χρησιμοποιηθούν σε άλλους τομείς.

Το δεύτερο σημείο σχετίζεται με την κατανάλωση ενέργειας και τις περιβαλλοντικές επιπτώσεις που έχει στον πλανήτη. Εκ πρώτης όψεως το επιχείρημα φαίνεται σωστό καθώς η ραγδαία αύξηση της τιμής του Bitcoin είχε ως αποτέλεσμα να επενδυθούν

χρήματα σε υπολογιστικά μηχανήματα τα οποία καταναλώνουν συγκριτικά μεγάλες ποσότητες ενέργειας. Η παραγωγή ενέργειας συνήθως συνδέεται με αρνητικές επιπτώσεις στο φυσικό περιβάλλον, οπότε η αύξηση της παγκόσμιας κατανάλωσης ενέργειας λόγω της συμμετοχής στην διαδικασία εξόρυξης του Bitcoin είναι επιβλαβής για τον πλανήτη. Ωστόσο το συγκεκριμένο επιχείρημα δεν λαμβάνει υπόψη δύο σημαντικές μεταβλητές.

Η πρώτη είναι ότι για την συμμετοχή στην διαδικασία της εξόρυξης σημαντικό ρόλο διαδραματίζει το κόστος της ενέργειας που καταναλώνεται. Με αποτέλεσμα τα μηχανήματα να συγκεντρώνονται σε περιοχές του πλανήτη όπου η παραγωγή ενέργειας έχει χαμηλό κόστος. Στα μέρη εκείνα οι ενεργειακοί πόροι βρίσκονται σε αφθονία, οπότε και η διαδικασία παραγωγής ενέργειας δεν χρησιμοποιεί μεθόδους επιβλαβείς για το περιβάλλον.

Αντίστοιχα η δεύτερη είναι ότι η ενέργεια που καταναλώνεται από το δίκτυο του Bitcoin δεν είναι άνευ ουσίας, καθώς αυξάνει την ασφάλεια της Blockchain και του κρυπτονομίσματος γενικότερα. Δίκτυα αντίστοιχου μεγέθους με παρόμοιο ρόλο καταναλώνουν ενέργεια λιγότερο αποδοτικά για να υλοποιήσουν τον σκοπό τους. Επιχείρημα το οποίο βασίζεται στο γεγονός ότι η τεχνολογία της Blockchain είναι η ασφαλέστερη μέθοδος που έχει ανακαλυφθεί ποτέ με σκοπό να υποστηρίζει αντίστοιχα δίκτυα συναλλαγών.

Περισσότερες πληροφορίες για την κατανάλωση ενέργειας του δικτύου Bitcoin στην ιστοσελίδα *“https://digiconomist.net/bitcoin-energy-consumption”*.

Προσαρμογή δυσκολίας

Ο εμπνευστής του Bitcoin, Satoshi Nakamoto, επιθυμούσε την δημιουργία ενός μέσου συναλλαγής το οποίο θα διατηρεί σταθερή προσφορά χρήματος διαχρονικά. Γεγονός που θα διαταράσσονταν από την ραγδαία εξέλιξη της τεχνολογίας εξόρυξης, στην περίπτωση που δεν είχε προβλεφθεί η σύνδεση της δυσκολίας επίλυσης του προβλήματος εξόρυξης ενός Block συναλλαγών με την συνολική υπολογιστική ισχύ του δικτύου Bitcoin. Για να παρουσιάσουμε την συγκεκριμένη ιδιαιτερότητα του Bitcoin θα πρέπει να πραγματοποιήσουμε μια σχετική εμβάθυνση στην έννοια της εξόρυξης.

Όταν ολοκληρώνεται ένα Block συναλλαγών και θεωρείται υποψήφιο προς εξόρυξη, ξεκινάνε οι συσκευές εξόρυξης του δικτύου Bitcoin να ανταγωνίζονται για το ποια θα

μπορέσει να βρει πρώτη την λύση του προβλήματος του Proof-of-Work αλγόριθμου που χρησιμοποιεί το πρωτόκολλο. Με σκοπό να εγκρίνουν το συγκεκριμένο Block συναλλαγών, να το προσθέσουν στην Blockchain και τελικώς να επιβραβευθούν για την προσπάθεια την οποία κατέβαλαν. Όπως έχει αναφερθεί και σε άλλα σημεία της παρούσης εργασίας η διαδικασία της εξόρυξης και συγκεκριμένα ο Proof-of-Work αλγόριθμος βασίζεται στην κρυπτογραφική συνάρτηση SHA256.

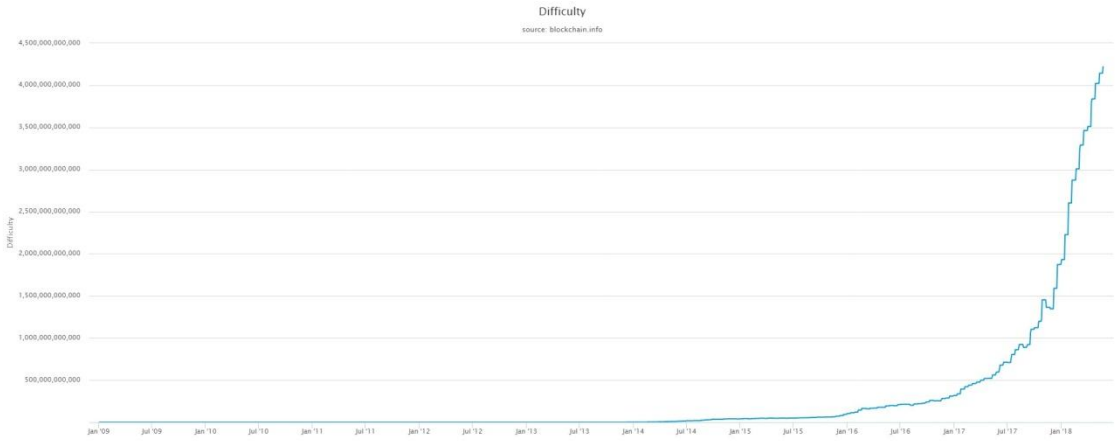
Από την προγραμματιστική οπτική η εξόρυξη ενός Block συναλλαγών δεν είναι τίποτα άλλο παρά η επανειλημμένη προσπάθεια για κατακερματισμό της κεφαλής του Block συναλλαγών, έως ότου το προκύπτον αποτέλεσμα κατακερματισμού διαθέτει συγκεκριμένα χαρακτηριστικά τα οποία έχουν καθοριστεί εκ των προτέρων. Σε κάθε νέα προσπάθεια κατακερματισμού μεταβάλλεται μόνο μια παράμετρος, η οποία ονομάζεται αριθμός “nonce”. Το αποτέλεσμα κατακερματισμού δεν μπορεί να καθοριστεί εκ των προτέρων αλλά ούτε να δημιουργηθεί κάποιο πρότυπο το οποίο να βοηθάει στην διαδικασία επίλυσης του συγκεκριμένου προβλήματος. Η μόνη μέθοδος για να βρεθεί λύση η οποία να διαθέτει τα απαιτούμενα χαρακτηριστικά είναι η συνεχής δοκιμή τυχαίων εισόδων, έως ότου εμφανιστεί το κατάλληλο αποτέλεσμα.

Το αποτέλεσμα κατακερματισμού ονομάζεται διαφορετικά και ψηφιακό αποτύπωμα μιας εισόδου. Για κάθε συγκεκριμένη είσοδο το ψηφιακό της αποτύπωμα θα είναι πάντα το ίδιο και οποιοσδήποτε θα μπορεί να επιβεβαιώσει με ευκολία την μεταξύ τους σύνδεση. Το βασικό χαρακτηριστικό ενός κρυπτογραφικού αλγορίθμου κατακερματισμού είναι το γεγονός ότι θεωρείται υπολογιστικά αδύνατο να βρεθούνε δύο είσοδοι οι οποίες θα έχουν ακριβώς το ίδιο ψηφιακό αποτύπωμα (collision).

Για να θεωρηθεί ένα ψηφιακό αποτύπωμα ως ικανοποιητικό θα πρέπει να διαθέτει συγκεκριμένα χαρακτηριστικά τα οποία έχουν καθοριστεί εκ των προτέρων. Για παράδειγμα έστω ότι το ψηφιακό αποτύπωμα χρησιμοποιεί το δεκαεξαδικό σύστημα απεικόνισης και εμείς έχουμε καθορίσει ότι επιθυμούμε το πρώτο σύμβολο να είναι το «0». Αυτόματα ο περιορισμός που θέσαμε έχει ως αποτέλεσμα ότι για να βρεθεί το κατάλληλο ψηφιακό αποτύπωμα απαιτούνται κατά μέσο όρο 16 προσπάθειες κατακερματισμού. Διότι οι πιθανές διαφορετικές τιμές που μπορεί να πάρει το πρώτο σύμβολο είναι 16, άρα και η πιθανότητα να είναι «0», είναι 1 / 16.

Στην περίπτωση του Bitcoin οι περιορισμοί που θέτονται είναι πολυπλοκότεροι και επιλέγονται με βάση την συνολική υπολογιστική ισχύ του δικτύου, ώστε να απαιτούνται περίπου 10 λεπτά μέχρις ότου βρεθεί ένα ψηφιακό αποτύπωμα το οποίο να

καλύπτει τους περιορισμούς που έχουν τεθεί. Οι περιορισμοί που τίθενται για τα χαρακτηριστικά του ψηφιακού αποτυπώματος ονομάζονται διαφορετικά και δυσκολία της διαδικασίας εξόρυξης. Οπότε όταν αναφερόμαστε σε αναπροσαρμογή της δυσκολίας εξόρυξης, ουσιαστικά πραγματοποιούμε μεταβολές στους περιορισμούς του ψηφιακού αποτυπώματος. Η διαδικασία αναπροσαρμογής εκτελείται αυτόματα και ανεξάρτητα σε κάθε κόμβο του δικτύου κάθε 2.016 Block συναλλαγών. Η εξόρυξη του συγκεκριμένου αριθμού Block συναλλαγών απαιτεί περίπου δύο εβδομάδες και σε περίπτωση που η μέση απαιτούμενη χρονική διάρκεια για την εξόρυξη ενός Block είναι μικρότερη των 10 λεπτών, η δυσκολία αυξάνεται. Στην αντίθετη περίπτωση η δυσκολία μειώνεται.



Εικόνα 9: Δυσκολία εξόρυξης Block συναλλαγών

Να σημειωθεί ότι η αναπροσαρμογή της δυσκολίας είναι ανεξάρτητη του αριθμού συναλλαγών ή της αξίας των συναλλαγών. Αυτό σημαίνει ότι η απαιτούμενη υπολογιστική ισχύς του δικτύου και επομένως η ηλεκτρική ενέργεια που απαιτείται για την διατήρηση της ασφάλειας του Bitcoin μέσω της διαδικασίας εξόρυξης είναι ανεξάρτητη του αριθμού συναλλαγών. Δηλαδή η χρήση του Bitcoin μπορεί να κλιμακωθεί, να γίνει ευρύτερη και η απαιτούμενη υπολογιστική ισχύς για την διαδικασία εξόρυξης να παραμείνει ακριβώς η ίδια. Η διαχρονική αύξηση της δυσκολίας εξόρυξης του Bitcoin, μεταφράζεται ως συνεχής αύξηση της συνολικής υπολογιστικής ισχύος των μηχανημάτων που συμμετέχουν στο δίκτυο εξόρυξης και τα οποία ανταγωνίζονται με σκοπό να κερδίσουν την προβλεπόμενη ανταμοιβή. Έως ότου το μεγαλύτερο ποσοστό της υπολογιστικής ισχύος του δικτύου εξόρυξης αποδίδεται σε τίμιους συμμετέχοντες, επιθέσεις του τύπου “takeover” με στόχο το δίκτυο του Bitcoin θεωρούνται υπολογιστικά αδύνατες.

Η δυσκολία της εξόρυξης επηρεάζεται έμμεσα από το κόστος της ηλεκτρικής ενέργειας αλλά και την συναλλαγματική ισοτιμία του Bitcoin. Τα συστήματα εξόρυξης μετατρέπουν την ηλεκτρική ενέργεια σε επεξεργαστική ισχύ για το δίκτυο, ωστόσο η απόδοσή τους σχετίζεται με την δεδομένη τεχνολογία κατασκευής ολοκληρωμένων κυκλωμάτων. Το κύριο μέγεθος που επηρεάζει την αγορά εξόρυξης Bitcoin είναι η τιμή ανά kWh ηλεκτρικού ρεύματος, επειδή καθορίζει την κερδοφορία της διαδικασίας εξόρυξης και επομένως τα κίνητρα εισόδου ή εξόδου των συμμετεχόντων στην αγορά.

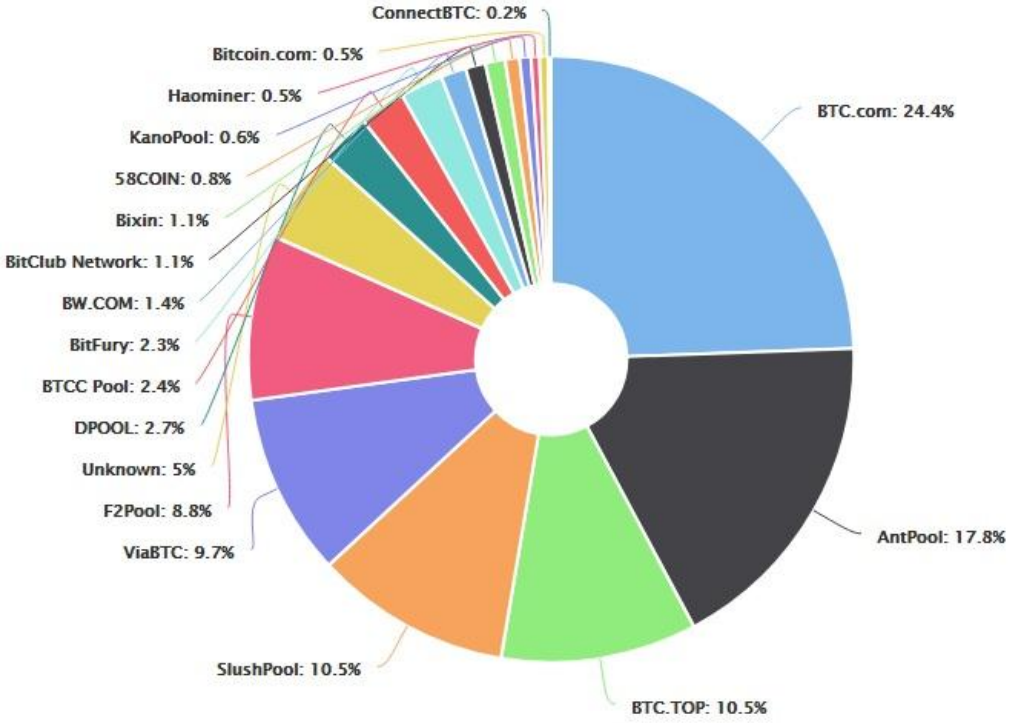
Δεξαμενές εξόρυξης (mining pools)

Σε ένα τόσο έντονα ανταγωνιστικό περιβάλλον, όπως είναι η αγορά εξόρυξης Bitcoin, μεμονωμένοι συμμετέχοντες που εργάζονται μόνοι τους δεν μπορούν να επιβιώσουν. Διότι η πιθανότητα να καταφέρουν να εξορύξουν ένα Block συναλλαγών πρώτοι, ώστε να λάβουν την επιβράβευση, είναι πάρα πολύ μικρή και αγγίζει τα όρια του τζόγου. Ακόμη και τα αποδοτικότερα ASICs που κυκλοφορούν, δεν μπορούν να ανταγωνιστούν επαγγελματικές εγκαταστάσεις που διαθέτουν δεκάδες χιλιάδες τέτοιου είδους μηχανήματα και βρίσκονται δίπλα σε εργοστάσια παραγωγής ηλεκτρικού ρεύματος. Για τον λόγο αυτό από το 2010 και έπειτα, ξεκίνησε η συνεργασία των μεμονωμένων χρηστών και η δημιουργία δεξαμενών εξόρυξης (mining pools). Η λογική με την οποία λειτουργούν οι δεξαμενές εξόρυξης είναι σχετικά απλή. Οι μεμονωμένοι χρήστες προσφέρουν την υπολογιστική ισχύ τους στην δεξαμενή εξόρυξης και επιβραβεύονται ανάλογα με αυτή. Η επιβράβευση είναι μικρότερη σε σχέση με την μεμονωμένη εργασία, ωστόσο παραμένει σταθερή σε καθημερινή βάση, μειώνοντας έτσι την αβεβαιότητα και τον συνολικό κίνδυνο.

Οι δεξαμενές εξόρυξης συντονίζουν εκατοντάδες χιλιάδες μεμονωμένους χρήστες, χρησιμοποιώντας ειδικά διαμορφωμένα πρωτόκολλα. Οι μεμονωμένοι χρήστες για να συμμετέχουν σε μια δεξαμενή εξόρυξης, απαιτείται να δημιουργήσουν έναν λογαριασμό στην σελίδα της δεξαμενής και να πραγματοποιήσουν τις κατάλληλες ρυθμίσεις στον εξοπλισμό εξόρυξης που κατέχουν. Ο εξοπλισμός εξόρυξης παραμένει συνδεδεμένος με τον server της δεξαμενής καθ’ όλη την διάρκεια λειτουργίας του. Καθώς πρέπει να υπάρχει συγχρονισμός ανάμεσα σε όλους τους συνδεδεμένους εξοπλισμούς. Με αποτέλεσμα η προσπάθεια που απαιτείται για την εξόρυξη ενός Block συναλλαγών να διαμοιράζεται, όπως και η συνολική επιβράβευση.

Στις μέρες μας η διαδικασία εξόρυξης νέων Block συναλλαγών πραγματοποιείται κατά κύριο λόγο από δεξαμενές εξόρυξης, οι οποίες διαχειρίζονται την υπολογιστική ισχύ

εκατοντάδων χιλιάδων μεμονωμένων χρηστών. Η κυριαρχία των δεξαμενών εξόρυξης μειώνει την αποκέντρωση του δικτύου του Bitcoin, ωστόσο προσφέρει την δυνατότητα σε πολλούς μεμονωμένους χρήστες να συμμετέχουν σε αυτό.



Εικόνα 10: Κατανομή υπολογιστικής ισχύος ανά Mining Pool (30/05 - 02/06/2018)

Οικονομική Παρουσίαση του Bitcoin

Το Bitcoin είναι μια οντότητα με ιδιαίτερα οικονομικά χαρακτηριστικά, τα οποία διαφέρουν από τις νόρμες του σύγχρονου οικονομικού περιβάλλοντος. Στο κεφάλαιο αυτό μελετώνται και παρουσιάζονται τα βασικά οικονομικά χαρακτηριστικά του κρυπτονομίσματος. Η παρουσίαση ξεκινά με την ανάλυση του Bitcoin ως προς τις λειτουργίες του Mankiw. Συνεχίζει με το χαρακτηριστικό της αποπληθωριστικής οικονομίας. Ενώ έπειτα πραγματοποιείται παρουσίαση της κατάστασης που επικρατεί την χρονική περίοδο συγγραφής της παρούσης εργασίας, ως προς τα ανταλλακτήρια, τα ρυθμιστικά πλαίσια των κρατών αλλά και τα εναλλακτικά κρυπτονομίσματα.

Για την πληρέστερη κατανόηση είναι σημαντική η γνώση των βασικών τεχνικών χαρακτηριστικών του Bitcoin, καθώς εξηγούν συγκεκριμένες συμπεριφορές, που αιτιολογούν κάποια ιδιαίτερα οικονομικά χαρακτηριστικά.

Το Bitcoin ως προς τις λειτουργίες του Mankiw

Η δημιουργία και η διάδοση των κρυπτονομισμάτων πρόσθεσε ένα νέο κεφάλαιο στην επιστήμη των οικονομικών. Το Bitcoin και γενικότερα τα κρυπτονομίσματα αποτελούν την νεότερη προσθήκη στην λίστα των οντοτήτων που επιτέλεσαν τον ρόλο του χρήματος στην ανθρώπινη ιστορία. Καθώς ικανοποιούν τις βασικές τεχνικές ιδιότητες. Είναι:

- Ανθεκτικά στον χρόνο.
- Διαιρετέα σε μικρότερα τμήματα.
- Ανταλλάξιμα.
- Εύκολα να μεταφερθούν.
- Αδύνατο να πλαστογραφηθούν.

Ωστόσο εκτός από τις βασικές τεχνικές ιδιότητες για να επιτελέσει μια οντότητα τον ρόλο του χρήματος, σύμφωνα με τους μοντέρνους οικονομολόγους, θα πρέπει να υποστηρίζει επιπλέον λειτουργίες. (Mankiw, 2009)

1. Να αποθηκεύει αξία, δηλαδή η χρήση τους να μεταφέρει αγοραστική δύναμη από το παρόν στο μέλλον.
2. Να αποτελεί λογιστική μονάδα, δηλαδή η αξία άλλων αγαθών και υπηρεσιών να παρατίθενται ως προς την συγκεκριμένη χρηματική μονάδα.

3. Να αποτελεί μέσο συναλλαγής, δηλαδή να μπορεί να ανταλλάσσεται για αγαθά και υπηρεσίες.

Πολλοί οικονομολόγοι σε άρθρα τους και συζητήσεις επικεντρώνονται γύρω από αυτές τις τρεις λειτουργίες και τον βαθμό στον οποίο το Bitcoin τις ικανοποιεί. Προσπαθώντας να απαντήσουν στο θεμελιώδες ερώτημα, αν το Bitcoin αποτελεί ένα νέο νόμισμα ή όχι. Οι επικριτές του Bitcoin υποστηρίζουν ότι οι λειτουργίες αυτές δεν εξυπηρετούνται από το κρυπτονόμισμα, για τον λόγο αυτό το χαρακτηρίζουν ως απάτη. Αντίθετα οι υποστηρικτές του Bitcoin δίνουν μια ευρύτερη διάσταση. Αντιτίθενται στην ρήση, χρήμα ή τίποτα, η οποία σημαίνει πως είτε το Bitcoin πρέπει να θεωρείται νόμισμα είτε είναι ένα τίποτα και υποστηρίζουν πως οι τρεις λειτουργίες δεν είναι αναγκαίο να ικανοποιούνται στον απόλυτο βαθμό αλλά σημασία έχει το γεγονός ότι το Bitcoin έχει αξία. (Graf, 2013) Στο πλαίσιο του συγκεκριμένου κεφαλαίου θα περιγραφεί η συμπεριφορά του Bitcoin, όσον αφορά τις τρεις λειτουργίες του Mankiw και θα συγκεντρωθούν τα θετικά και αρνητικά στοιχεία του κρυπτονίμασματος για κάθε μία ξεχωριστά.

Αποθήκη αξίας

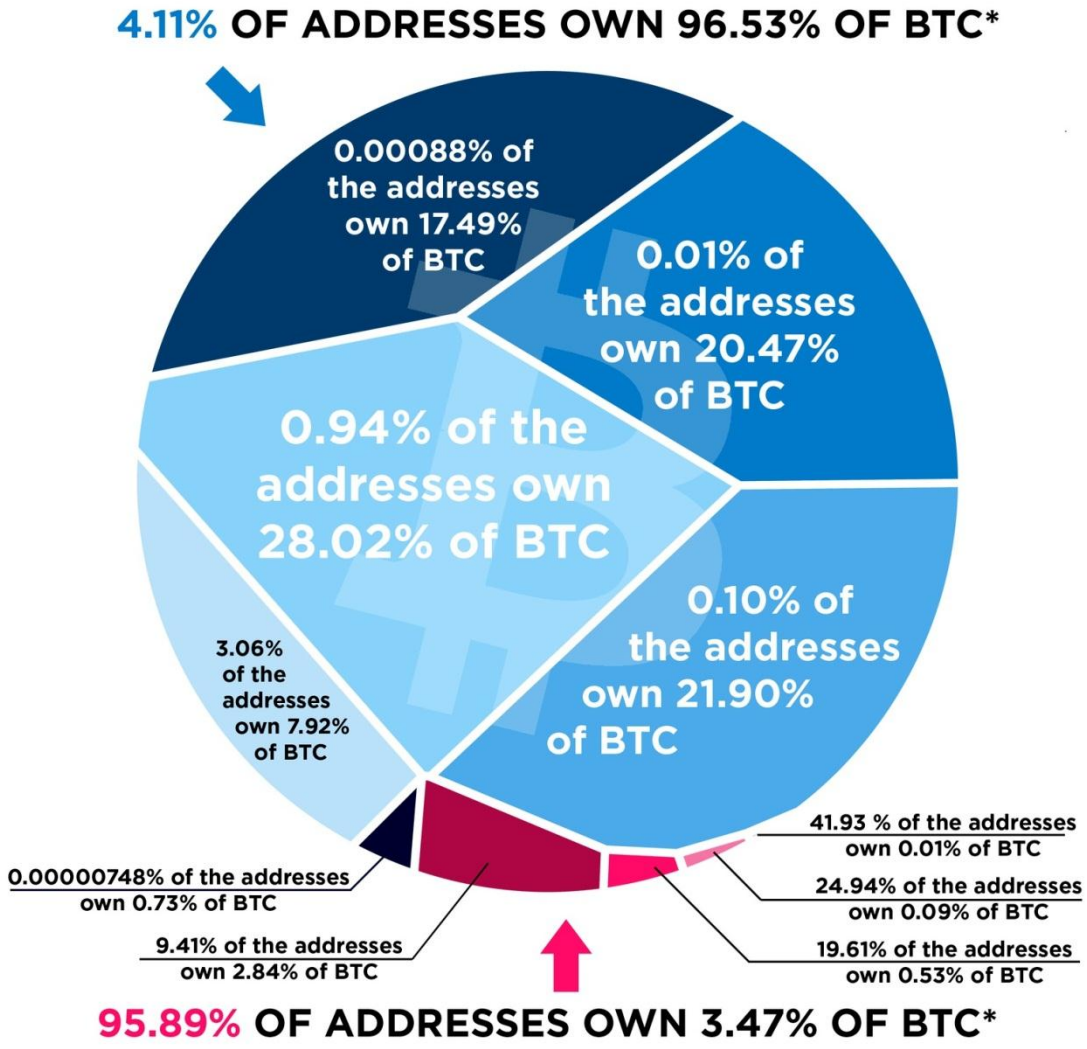
Η αποθήκευση αξίας συνεπάγεται μεταφορά αγοραστικής δύναμης από το παρόν σε μια μελλοντική χρονική στιγμή. Όταν μια οντότητα παρουσιάζει μεγάλη μεταβλητότητα στην τιμή της, τότε δεν θεωρείται ικανοποιητική αποθήκη αξίας. Όπως φαίνεται και στο παρακάτω διάγραμμα η μεταβλητότητα αποτελεί ένα βασικό χαρακτηριστικό της τιμής του Bitcoin.

Εικόνα 11: Η ισοτιμία USD / BTC (12/08/2017 - 12/08/2018)

Για τον λόγο αυτό οι περισσότεροι οικονομολόγοι κατατάσσουν το Bitcoin στην κατηγορία των επενδύσεων με υψηλό κίνδυνο παρά στα σταθερά μέσα αποθήκευσης

αξιών. Με βάση την συγκεκριμένη οπτική η τιμή του Bitcoin παρουσιάζει ομοιότητες με την ευμετάβλητη παρουσία μιας start-up επιχείρησης.

Μια ακόμη ενδιαφέρουσα παρατήρηση, είναι το γεγονός ότι το Bitcoin παρουσιάζει μικρή κινητικότητα, δηλαδή ο όγκος των συναλλαγών που πραγματοποιούνται είναι αρκετές φορές μικρότερος σε σχέση με τα bitcoins που έχουν εξορυχτεί και βρίσκονται σε κυκλοφορία. Το συγκεκριμένο στοιχείο οδηγεί στο συμπέρασμα ότι ο μεγαλύτερος όγκος των bitcoins συγκεντρώνεται σε ένα περιορισμένο αριθμό διευθύνσεων, οι οποίες παραμένουν για μεγάλο χρονικό διάστημα αδρανείς. (Ron, et al., 2013) Η παρακάτω εικόνα παρουσιάζει την συγκέντρωση του Bitcoin σε σχέση με το πλήθος των διευθύνσεων.



Εικόνα 12: Η συσσώρευση του Bitcoin σε σχέση με τις διευθύνσεις

Οι λειτουργίες ενός νομίσματος, ως αποθήκη αξίας και ως μέσο συναλλαγής, παρουσιάζουν μεγάλη συσχέτιση. Διότι κανείς δεν θα χρησιμοποιούσε ένα μέσο συναλλαγής το οποίο δεν έχει καμία αξία και αντίστροφα κανένας δεν θα

χρησιμοποιούσε ένα μέσο ως αποθήκη αξίας αν δεν συμμετείχε στην πραγματοποίηση συναλλαγών. Προϋπόθεση λοιπόν για την διάδοση και ανάπτυξη του Bitcoin είναι η ύπαρξη ισορροπίας ανάμεσα στις δύο αυτές λειτουργίες.

Πλεονεκτήματα

i. Τα bitcoins δεν μπορούν να κατασχεθούν, δεν υπόκεινται σε περιορισμούς κεφαλαίων και δεν μπορούν να φορολογηθούν δυσανάλογα. Σε αντίθεση με τα παραστατικά νομίσματα που ελέγχονται μέσω του συστήματος των τραπεζών. Κανείς δεν μπορεί να απαγορέψει, με οποιονδήποτε τρόπο σε έναν χρήστη, την πρόσβαση και χρήση των bitcoins του.
ii. Δεν υπάρχουν κόστη αποθήκευσης για τα bitcoins. Η αγορά και αρχικοποίηση ενός πορτοφολιού Bitcoin μπορεί να κοστίζει. Ωστόσο στην συνέχεια δεν υπάρχουν επιπρόσθετα κόστη.
iii. Τα bitcoins είναι εύκολο να μεταφερθούν. Τα ιδιωτικά κλειδιά μπορούν να αποθηκευτούν σε μια φορητή μονάδα αποθήκευσης, που καταλαμβάνει ελάχιστο χώρο.
iv. Η προσφορά χρήματος στην οικονομία του Bitcoin καθορίζεται με βάση έναν αλγόριθμο και δεν επηρεάζεται από μεμονωμένες αποφάσεις. Αντίθετα με τα παραστατικά νομίσματα των οποίων την έκδοση καθορίζουν οι κεντρικές τράπεζες.
v. Το Bitcoin χρησιμοποιεί αλγορίθμους κρυπτογράφησης για την ασφάλειά του. Με τις υπάρχουσες υπολογιστικές δυνατότητες είναι αδύνατο να παραβιαστούν.
vi. Όλες οι συναλλαγές που πραγματοποιούνται διατηρούνται στην Blockchain και το ιστορικό είναι προσβάσιμο οποιαδήποτε στιγμή από τον καθένα.
vii. Λόγω της σταθερής προσφοράς χρήματος, η οικονομία του Bitcoin δεν παρουσιάζει πληθωριστικές τάσεις. Στοιχείο που θα παρουσιαστεί αναλυτικότερα και στην συνέχεια της εργασίας.

Μειονεκτήματα

i. Το Bitcoin χρησιμοποιεί κώδικα ανοιχτού λογισμικού, το οποίο σημαίνει ότι το σύνολο του πρωτοκόλλου είναι διαθέσιμο μέσω του διαδικτύου και προσβάσιμο από οποιονδήποτε το επιθυμεί. Ταυτόχρονα είναι σχετικά εύκολη και κατοχυρωμένη νομικά η μερική αλλαγή του κώδικα και η δημιουργία αντιγράφων. Με αποτέλεσμα ήδη να έχει υλοποιηθεί μεγάλος αριθμός υποκατάστατων. Το Bitcoin ήταν το πρώτο κρυπτονόμισμα που τέθηκε σε λειτουργία, γεγονός που του προσέδωσε ένα ισχυρό ανταγωνιστικό πλεονέκτημα έναντι των υπολοίπων. Ωστόσο το ποσοστό που κατέχει στην αγορά κρυπτονομισμάτων μειώνεται με την πάροδο

του χρόνου, καθώς εμφανίζονται νεότερα κρυπτονομίσματα με ανταγωνιστικά χαρακτηριστικά.

ii. Η μεταβλητότητα που παρουσιάζει η τιμή του Bitcoin, έχει ως αποτέλεσμα να μειώνεται η αξιοπιστία του κρυπτονομίσματος ως αποθήκη αξίας. Καθώς δεν υπάρχει κάποια κεντρική αρχή η οποία να ελέγχει την προσφορά χρήματος στην οικονομία του Bitcoin, με σκοπό να διατηρεί σχετικά σταθερή την αξία του κρυπτονομίσματος.

iii. Η προσφορά χρήματος στην οικονομία του Bitcoin δεν μπορεί να χειραγωγηθεί, ελέγχεται από το πρωτόκολλο και παραμένει αμετάβλητη κάτω από οποιεσδήποτε συνθήκες.

iv. Η διατήρηση bitcoins δεν προσφέρει υψηλό επίπεδο προστασίας έναντι του πληθωρισμού. Καθώς στην περίπτωση που η τιμή του Bitcoin έναντι των παραστατικών νομισμάτων αυξηθεί, τα κέρδη που παρουσιάζονται είναι φορολογητέα.

v. Στο Bitcoin δεν υπάρχει μια κεντρική αρχή η οποία να καθορίζει την νομιμότητα των πράξεων και το σύνολο των χρηστών να αποδέχεται τις αποφάσεις της.

vi. Πολλές κυβερνήσεις και διεθνείς μηχανισμοί απαγορεύουν την χρήση του Bitcoin στα όρια της δικαιοδοσίας τους, διότι δεν διαθέτουν την δυνατότητα ελέγχου της λειτουργίας του.

vii. Το Bitcoin δεν διαθέτει κάποια φυσική υποστήριξη που να εγγυάται ένα μέρος της αξίας του. Υπό μια έννοια τον συγκεκριμένο ρόλο αναλαμβάνει ο proof-of-work αλγόριθμος που εκτελείται από τους υποστηρικτές της διαδικασίας εξόρυξης.

viii. Το Bitcoin δεν διαθέτει οριακό κόστος παραγωγής, ώστε να σταθεροποιεί την τιμή του. Για τον λόγο αυτό όταν κυριαρχούν τάσεις μείωσης της τιμής του, τα αποτελέσματα είναι εντονότερα.

ix. Δεν υπάρχει διασφάλιση καταθέσεων στην οικονομία του Bitcoin. Όταν για οποιονδήποτε λόγο ένας χρήστης χάνει την δυνατότητα διαχείρισης των bitcoins του, δεν υπάρχει τρόπος να την ανακτήσει.

Λογιστική μονάδα

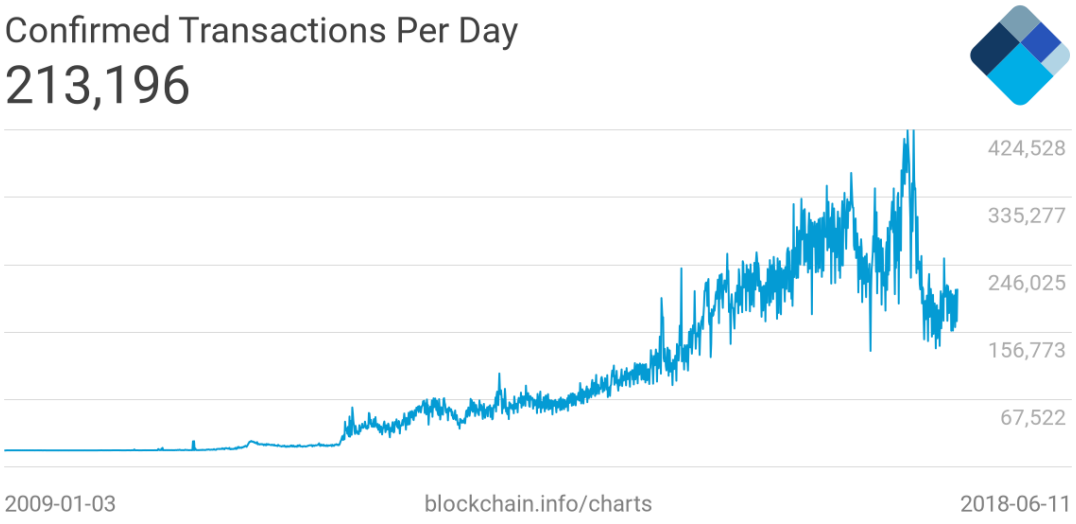
Γενικά το Bitcoin δεν θεωρείται μια ικανοποιητική λογιστική μονάδα. Αν και χρησιμοποιείται στις συναλλαγές πολλών προϊόντων και υπηρεσιών, λίγα από αυτά παραθέτουν την αξία τους απευθείας σε μονάδες Bitcoin. Τα περισσότερα αξιολογούνται σε κάποιο παραστατικό νόμισμα και στην συνέχεια η τιμή τους μετατρέπεται σε μονάδες Bitcoin. Κύρια αιτία της συγκεκριμένης επιλογής είναι το

γεγονός ότι το Bitcoin παρουσιάζει πολύ μεγάλη μεταβλητότητα, οπότε είναι ιδιαίτερα δύσκολη η αξιολόγηση προϊόντων και υπηρεσιών απευθείας σε μονάδες Bitcoin. Μια μελλοντική σταθεροποίηση της τιμής του θα οδηγούσε όλο και περισσότερους εμπόρους στην χρήση του ως κύρια λογιστική μονάδα.

Ωστόσο ενώ δεν υφίσταται οικονομία που να χρησιμοποιεί ως μοναδικό μέσο συναλλαγής το Bitcoin, υπάρχει ένας πολύ μικρός τομέας της βιομηχανίας που ήδη λειτουργεί με το Bitcoin ως κύρια και μοναδική λογιστική μονάδα. Ο τομέας αυτός περιλαμβάνει τις συσκευές εξόρυξης και κάποια ήδη offline πορτοφολιών.

Μέσο συναλλαγής

Οι χρήστες που αποδέχονται το Bitcoin συνεχώς αυξάνονται και υπάρχει η πεποίθηση, ακόμη και ανάμεσα στους επικριτές του, ότι το Bitcoin μπορεί μελλοντικά να λειτουργεί ως ένα παγκόσμιο μέσο συναλλαγών. Στην παρακάτω εικόνα παρατηρούμε τον ημερήσιο αριθμό συναλλαγών που πραγματοποιούνται με χρήση του Bitcoin.

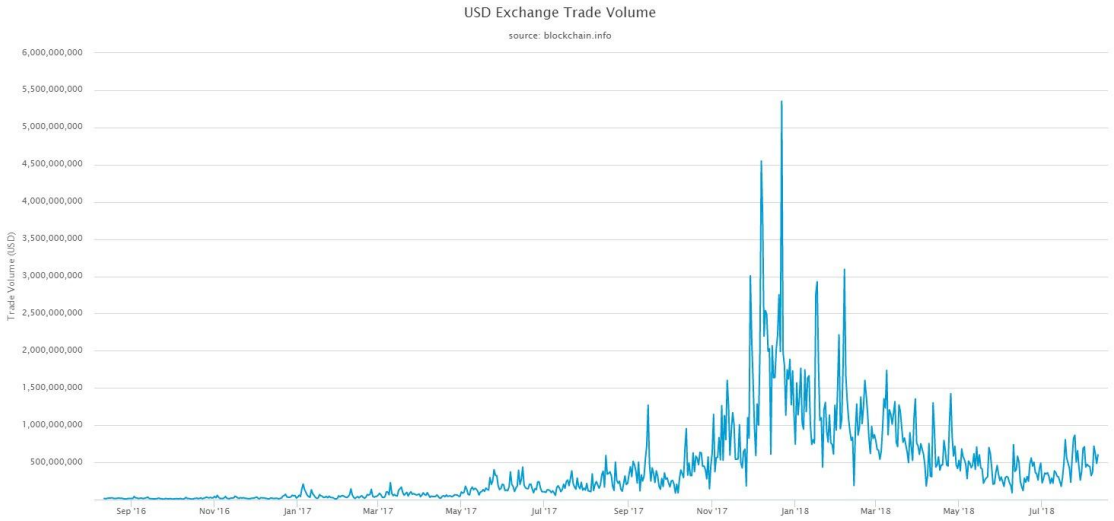


Εικόνα 13: Αριθμός ημερήσιων συναλλαγών Bitcoin

Οι περισσότεροι οικονομολόγοι συμφωνούν ότι το Bitcoin διαθέτει σχετικά μικρή βάση χρηστών, ώστε να θεωρείται παγκόσμιο μέσο συναλλαγών. Για να εισαχθεί στην συγκεκριμένη κατηγορία θα πρέπει να επιτύχει μια κρίσιμη μάζα χρηστών. Η κρίσιμη μάζα είναι το σημείο εκείνο με το πέρας του οποίου τα οφέλη των νέων χρηστών ξεπερνούν τα κόστη υιοθέτησης της νέας τεχνολογίας. Συγκεκριμένα για τις τεχνολογίες που σχετίζονται με την επιστήμη της πληροφορικής, όπως είναι τα ψηφιακά νομίσματα, τα οφέλη των νέων χρηστών επηρεάζονται από τον συνολικό αριθμό των χρηστών που έχουν ήδη υιοθετήσει την χρήση της συγκεκριμένης τεχνολογίας, καθώς δημιουργούνται περισσότερες ευκαιρίες για την υλοποίηση

συναλλαγών. Καταλήγουμε στο συμπέρασμα ότι τα οφέλη του συνόλου των χρηστών αυξάνονται δραματικά με την ταυτόχρονη αύξηση του συνολικού αριθμού των χρηστών. Το φαινόμενο αυτό είναι γνωστό ως επίδραση του διαδικτύου. (Varian, 2003) Από το σημείο και έπειτα, που μια τεχνολογία επιτυγχάνει την κρίσιμη μάζα της, η θετική ανάδραση και η υιοθέτησή της, την οδηγούν σε εκρηκτική ανάπτυξη.

Αν και έχουν περάσει σχεδόν δέκα χρόνια από την δημιουργία του Bitcoin, η κρίσιμη μάζα της ευρείας υιοθέτησης του κρυπτονομίσματος ως μέσο συναλλαγής δεν έχει ακόμη επιτευχθεί. Η συγκεκριμένη παρατήρηση βασίζεται και στην πορεία την οποία ακολουθεί η τιμή του Bitcoin καθώς αντί για έντονη και συνεχή αύξηση, η οποία θα μας οδηγούσε στο συμπέρασμα ότι έχει επιτευχθεί η κρίσιμη μάζα, παρατηρούμε κυκλικές συμπεριφορές. Δηλαδή έντονες θετικές τάσεις έχουν ως επακόλουθο έντονες αρνητικές και το αντίστροφο. Αναλυτικότερα στα τέλη του 2017, κυρίως λόγω της προβολής του Bitcoin από τα μέσα ενημέρωσης, παρατηρήθηκε ραγδαία αύξηση της τιμής του, η οποία στις *16/12/2017* κατέγραψε την μέγιστη τιμή των *19.499 USD/BTC*. Ωστόσο η κυκλική συμπεριφορά και η αντιστροφή του κλίματος λόγω αρνητικών ειδήσεων αλλά και οργανωμένων απαγορεύσεων είχε ως αποτέλεσμα, έξι μήνες σχεδόν αργότερα, η τιμή του να προσπαθεί να σταθεροποιηθεί κοντά στα *7.000 USD/BTC*. (Athey, et al., 2016)



Εικόνα 14: Όγκος σε USD των ημερήσιων συναλλαγών Bitcoin

Το Bitcoin αποτελεί ένα διαδικτυακό μέσο συναλλαγών. Ο συγκεκριμένος τομέας παρουσιάζει έντονο ανταγωνισμό, του οποίου η ένταση αναμένεται να αυξηθεί τα επόμενα χρόνια καθώς οι ισχυρές εταιρείες του χώρου της πληροφορικής προβλέπεται να επικεντρώσουν τις προσπάθειές τους στην δημιουργία νέων συστημάτων

διαδικτυακών συναλλαγών. Ωστόσο μέχρι να πραγματοποιηθούν οι νέες προσθήκες, το Bitcoin ανταγωνίζεται τα συστήματα συναλλαγών που υποστηρίζουν εταιρείες όπως η PayPal, η Mastercard και η Visa. Οι συγκεκριμένες εταιρείες βασίζουν την λειτουργία τους σε ιδιωτικά συστήματα υποδομών, ενώ τα έσοδα τους προέρχονται κυρίως από τα κόστη συναλλαγών που καλούνται να καλύψουν οι χρήστες των συστημάτων τους. Σε αυτά τα δύο σημεία εντοπίζονται και τα κύρια ανταγωνιστικά πλεονεκτήματα του Bitcoin, καθώς αντιπαραθέτει την διαδικασία της εξόρυξης και μηδενικά κόστη συναλλαγών. (Grinberg, 2011)

Το δίκτυο εξόρυξης του Bitcoin διαθέτει μεγαλύτερη υπολογιστική ισχύ και υψηλότερα επίπεδα ασφαλείας σε σχέση με οποιοδήποτε ιδιωτικό σύστημα υποδομών. Για να διατηρήσει όμως το Bitcoin το ανταγωνιστικό πλεονέκτημα της εξόρυξης θα πρέπει η διαδικασία να είναι επικερδής για τους χρήστες που την υποστηρίζουν. Στο σημερινό επίπεδο τιμών στο οποίο κυμαίνεται το Bitcoin η εξόρυξη είναι οριακά επικερδής για τους περισσότερους χρήστες. Αντίστοιχα, ανησυχητικό στοιχείο είναι και το γεγονός ότι η κερδοφορία των χρηστών που υποστηρίζουν την εξόρυξη βασίζεται κατά 99% στην δημιουργία νέων νομισμάτων και κατά 1% στα κόστη συναλλαγών. Η δημιουργία νέων νομισμάτων είναι σχεδιασμένη να φθίνει με την πάροδο των χρόνων, οπότε η αναθεώρηση του ρόλου που θα διαδραματίζουν τα κόστη συναλλαγών στην οικονομία του Bitcoin θεωρείται επιβεβλημένη. (Huberman, et al., 2017)

Πλεονεκτήματα

i. Οι χρήστες του Bitcoin δεν κινδυνεύουν από παραβιάσεις ασφαλείας του δικτύου. Η πραγματοποίηση μιας παραβίασης στο δίκτυο του Bitcoin δεν μπορεί να επιφέρει απώλειες στους χρήστες. Ο μόνος τρόπος για να πληγούν οι τελικοί χρήστες είναι μέσω της απώλειας των ιδιωτικών κλειδιών τους, τα οποία τους προσφέρουν πρόσβαση στα κρυπτονομίσματά τους.
ii. Τα κόστη για την υλοποίηση των συναλλαγών είναι χαμηλότερα, συνήθως μηδενικά, σε σύγκριση με τα αντίστοιχα των ανταγωνιστικών εταιρειών.
iii. Οι έμποροι που χρησιμοποιούν το Bitcoin προστατεύονται από απάτες της κατηγορίας charge-back. Ωστόσο τέτοιου είδους απάτης μπορούν να πέσουν θύματα και οι καταναλωτές.
iv. Οι συναλλαγές με χρήση του Bitcoin πραγματοποιούνται σχεδόν αμέσως. Μεγάλη διαφορά αν αναλογιστεί κανείς πως οι μεταφορές ανάμεσα σε τραπεζικούς λογαριασμούς απαιτούν μερικές μέρες για να υλοποιηθούν.

v. Το σύνολο της τεχνολογίας βασίζεται στην ψηφιακή τεχνολογία, χωρίς να συνδέεται με παραστατικά νομίσματα.

vi. Στις εμπορικές συναλλαγές που πραγματοποιούνται με χρήση του Bitcoin το άτομο που εγκρίνει την συναλλαγή είναι ο πελάτης, ενώ στα ανταγωνιστικά συστήματα συναλλαγών είναι ο πωλητής. Γεγονός που μπορεί να οδηγήσει στην μείωση της απάτης κατά την διάρκεια πραγματοποίησης των συναλλαγών.

vii. Το Bitcoin παρέχει υψηλά επίπεδα ανωνυμίας.

viii. Το Bitcoin είναι ένα νέο σύστημα συναλλαγών, εντελώς ανεξάρτητο από το κλασικό τραπεζικό περιβάλλον. Γεγονός το οποίο προσφέρει ανθεκτικότητα στην παγκόσμια οικονομία σε περιόδους κρίσης, καθώς αποτελεί ένα παράλληλο σύστημα συναλλαγών.

Μειονεκτήματα

i. Ο σχεδιασμός του Bitcoin ταιριάζει περισσότερο με συναλλαγές μεγάλης αξίας, οι οποίες πραγματοποιούνται συνήθως από επιχειρήσεις και όχι τόσο με καθημερινές μικροσυναλλαγές που πραγματοποιούν απλοί χρήστες.

ii. Η αγορά του Bitcoin παρουσιάζει μικρότερη ρευστότητα σε σχέση με τις παγκόσμιες αγορές παραστατικών νομισμάτων. Επίσης το βάθος της είναι πολύ μικρότερο συγκριτικά με την FOREX.

iii. Δεν παρέχεται η δυνατότητα στους χρήστες του Bitcoin να πιστωθούν στην διεύθυνσή τους ένα χρηματικό ποσό το οποίο να αποπληρώσουν σε μελλοντική χρονική στιγμή.

iv. Το νομικό πλαίσιο και η αυστηρότερη φορολόγηση του Bitcoin, πιθανόν να αυξήσουν τα έμμεσα κόστη συναλλαγών.

v. Η οριστικοποίηση μιας συναλλαγής με χρήση του Bitcoin μπορεί να διαρκέσει έως και δέκα λεπτά. Στην περίπτωση των καθημερινών συναλλαγών, για παράδειγμα σε ένα εμπορικό κέντρο, το συγκεκριμένο χρονικό περιθώριο θεωρείται απαγορευτικό.

vi. Η χρήση του Bitcoin ως μοναδικό παγκόσμιο νόμισμα πρέπει να θεωρείται αδύνατη, καθώς είναι πολύ πιθανό να αντιμετωπίσει προβλήματα επεκτασιμότητας. Ωστόσο μπορεί να εξελιχθεί σε ένα ιδιαίτερα χρήσιμο παράλληλο μέσο συναλλαγών.

vii. Οι κυβερνήσεις και οι ισχυρές πολυεθνικές εταιρείες έχουν την δυνατότητα να αναπτύξουν αντίστοιχου σχεδιασμού μέσα συναλλαγών, τα οποία να ανταγωνιστούν επάξια το Bitcoin.

Τα τελευταία χρόνια αναπτύσσονται θεωρίες στον χώρο των οικονομικών επιστημών, οι οποίες υποστηρίζουν ότι πλέον οι τρεις λειτουργίες του Mankiw δεν είναι τόσο στενά συνδεδεμένες και οπότε δεν απαιτείται η ικανοποίησή τους στον απόλυτο βαθμό, από μια οντότητα, για να θεωρείται νομισματική μονάδα. Η συγκεκριμένη οπτική βασίζεται και στην περίπτωση του Bitcoin, καθώς η τεχνολογία που εισάγει αλλά και ο τρόπος λειτουργίας του διαφέρουν σε πολύ μεγάλο βαθμό από τις γνωστές περιπτώσεις πάνω στις οποίες βασίστηκαν οι κλασσικές θεωρίες των οικονομικών επιστημών.

Το Bitcoin ως επενδυτικό προϊόν

Όπως αναφέρθηκε και προηγουμένως το προφίλ κινδύνου/απόδοσης της επένδυσης σε Bitcoin παρουσιάζει περισσότερες ομοιότητες με την επένδυση σε start-up επιχειρήσεις παρά σε σταθερά προϊόντα αποθήκευσης αξίας. Τα κύρια πλεονεκτήματα του Bitcoin σε σχέση με παρόμοια επενδυτικά προϊόντα είναι:

- ✓ Η ρευστότητά του.
- ✓ Η ευκολία επένδυσης σε αυτό.
- ✓ Ο χαμηλός βαθμός συσχέτισής του με τα υπόλοιπα επενδυτικά προϊόντα.

Το Bitcoin ενώ υπάρχει από το 2009 αποτελεί μια σχετικά νέα αγορά η οποία άρχισε να προβάλλεται από τα μέσα ενημέρωσης κυρίως από το 2017 και έπειτα. Ταυτόχρονα οι έννοιες που εισάγει και η τεχνολογία που χρησιμοποιεί είναι δυσνόητες για τον μέσο επενδυτή, ο οποίος διαθέτει περιορισμένες γνώσεις σχετικές με τον τομέα της επιστήμης της πληροφορικής. Με αποτέλεσμα να παρουσιάζει αυξημένη μεταβλητότητα και να μην έχει επιτευχθεί κατάσταση σταθεροποίησης της τιμής του.

Όμοια με μια start-up επιχείρηση, υπάρχει η πιθανότητα το Bitcoin να διαδοθεί ακόμη περισσότερο και να κατακτήσει ένα κομμάτι της αγοράς πληρωμών. Ενώ αντίστοιχα υπάρχει και η πιθανότητα να αποτύχει και η αξία του σε βάθος χρόνου να μηδενιστεί. Κάποια πιθανά σενάρια που θα μπορούσαν να οδηγήσουν το Bitcoin σε αποτυχία και μηδενισμό της αξίας του, είναι τα εξής:

- Να εμφανιστεί ένα κενό ασφαλείας το οποίο να οδηγήσει στην απώλεια bitcoins και διευθύνσεων από μεγάλο αριθμό χρηστών.
- Να πραγματοποιηθεί οργανωμένη επίθεση στο δίκτυο του Bitcoin που θα έχει ως αποτέλεσμα στην απώλεια της εμπιστοσύνης των χρηστών.
- Μια ανταγωνιστική τεχνολογία να επικρατήσει αντικαθιστώντας την χρήση του Bitcoin.

- Το Bitcoin δεν μπορεί να επιβιώσει σε έναν κόσμο χωρίς ηλεκτρισμό και δικτύωση.

Αποπληθωριστική οικονομία

Οι κλασικές οικονομίες βασίζουν την λειτουργία τους σε κάποιο παραστατικό νόμισμα (π.χ. Δολάριο ΗΠΑ, Ευρώ, Γιέν κ.ά.). Η προσφορά χρήματος στην οικονομία ελέγχεται με την χρήση κεντρικών τραπεζών, οι οποίες αποφασίζουν για το εάν και το πότε θα πρέπει να εκτυπώσουν και να διαθέσουν στο κοινό, με την βοήθεια των τραπεζικών χορηγήσεων, νέο χρήμα. Μια κεντρική τράπεζα, σε περιόδους που δεν υπάρχει κρίση, στοχεύει στην διατήρηση ενός σταθερού και χαμηλής εντάσεως πληθωρισμού. Οι συγκεκριμένες οικονομικές συνθήκες θεωρούνται από τους οικονομολόγους ως οι κατάλληλες για την επίτευξη υψηλού ρυθμού ανάπτυξης. Διότι η συγκέντρωση χρήματος αποτελεί λανθασμένη επιλογή καθώς συνεπάγεται μείωση της αγοραστικής του ισχύος, οπότε τα χρήματα δεν αποθηκεύονται και χρησιμοποιούνται για την κατανάλωση αγαθών και υπηρεσιών είτε για την υλοποίηση νέων επενδύσεων.

Ωστόσο μπορεί να υπάρξει και ένα οικονομικό σύστημα το οποίο να χαρακτηρίζεται από σταθερά φθίνουσα, με την πάροδο των χρόνων, προσφορά χρήματος. Συνοδευόμενο φυσικά από αρκετές συνέπειες. Η σημαντικότερη από αυτές είναι το γεγονός ότι ένας οικονομικός σχεδιασμός με τα συγκεκριμένα χαρακτηριστικά παρουσιάζει εγγενείς αποπληθωριστικές τάσεις. Ο αποπληθωρισμός είναι το φαινόμενο κατά το οποίο οι πολίτες συγκεντρώνουν χρήματα σταματώντας τις επενδύσεις και την κατανάλωση αγαθών και υπηρεσιών, καθώς αναμένουν μείωση του επιπέδου τιμών. Είναι η ακριβώς αντίθετη κατάσταση από τον πληθωρισμό, διότι λόγω της μείωσης των τιμών τα χρήματα που έχουν συγκεντρωθεί, στο μέλλον θα παρουσιάσουν αυξημένη αγοραστική ισχύ. Στα κλασικά οικονομικά συστήματα ο αποπληθωρισμός θεωρείται ως καταστροφή και πρέπει να αποφεύγεται με κάθε τρόπο. Παράδειγμα των συνεπειών του αποπληθωρισμού αποτελεί η "χαμένη δεκαετία" της Ιαπωνίας, όταν η κατακόρυφη μείωση της ζήτησης του Γιεν οδήγησε την ιαπωνική οικονομία σε ένα φαύλο αποπληθωριστικό κύκλο. (Graf, 2014)

Σε αντίθεση με τις βασικές οικονομικές αρχές, το Bitcoin εφαρμόζει έναν οικονομικό σχεδιασμό με σταθερά φθίνουσα προσφορά χρήματος στην οικονομία του. Οι ειδικοί που μελετούν το Bitcoin υποστηρίζουν πως ο αποπληθωρισμός δεν πρέπει να θεωρείται κακός εσαεί. Στα κλασικά οικονομικά συστήματα συνδέεται με την ταυτόχρονη και ραγδαία μείωση της ζήτησης. Διότι η δυνατότητα εκτύπωσης απεριόριστου νέου χρήματος, ταυτίζει τον αποπληθωριστικό κύκλο με την ταυτόχρονη κατάρρευση της

ζήτησης. Ωστόσο η περίπτωση του οικονομικού μοντέλου του Bitcoin είναι διαφορετική καθώς ο αποπληθωρισμός δεν είναι αποτέλεσμα της μείωσης της ζήτησης αλλά μιας προβλέψιμα περιορισμένης προσφοράς χρήματος.

Το θετικό στοιχείο του αποπληθωρισμού είναι φυσικά το γεγονός ότι αποτελεί το αντίθετο του πληθωρισμού. Ο πληθωρισμός προκαλεί μια αργή αλλά αναπόφευκτη υποβάθμιση του νομίσματος. Ταυτόχρονα λειτουργεί και ως μια μορφή κρυφής φορολόγησης, η οποία τιμωρεί τους αποταμιευτές προκειμένου να διασώσει του οφειλέτες, συμπεριλαμβανομένων και των μεγαλύτερων, σε παγκόσμιο επίπεδο, οφειλετών που είναι οι ίδιες οι κυβερνήσεις. Στα νομίσματα που υπόκεινται σε κυβερνητικό έλεγχο, ελλοχεύει ο ηθικός κίνδυνος της απεριόριστης έκδοσης χρεωστικών τίτλων, των οποίων η αποπληρωμή στηρίζεται στο "κούρεμα" των καταθέσεων των αποταμιευτών. Μένει να ανακαλύψουμε στο μέλλον αν ο αποπληθωριστικός οικονομικός σχεδιασμός του Bitcoin θα αποθαρρύνει μια ταχεία ανάπτυξη της οικονομίας του ή θα αποτελέσει πλεονέκτημα λόγω της προστασίας που προσφέρει έναντι του πληθωρισμού και της συνεχούς υποβάθμισης της αξίας του νομίσματος.

Ανταλλακτήρια και κυβερνοεπιθέσεις

Οι νέοι χρήστες που επιθυμούν να συμμετέχουν στην οικονομία του Bitcoin πρέπει να υλοποιήσουν δύο προαπαιτούμενα βήματα. Το πρώτο είναι η δημιουργία του προσωπικού τους πορτοφολιού. Μια απλή διαδικασία με μηδαμινό κόστος, καθώς τα περισσότερα είδη πορτοφολιών, όπως έχουμε αναλύσει προηγουμένως, προσφέρονται δωρεάν στους νέους χρήστες. Ενώ το δεύτερο είναι η προμήθεια των νέων χρηστών με τα πρώτα τους bitcoins. Υπάρχουν διάφοροι τρόποι να προμηθευτεί ένας νέος χρήστης τα πρώτα του bitcoins. Όταν αναφερόμαστε για έναν μικρό αριθμό bitcoins υπάρχουν απλές και χωρίς κόστος επιλογές, όπως:

- Η εύρεση ενός γνωστού που θα μεταφέρει στην διεύθυνση του νέου χρήστη τα πρώτα του bitcoins.
- Η προσφορά ενός αγαθού ή μιας υπηρεσίας, από τον νέο χρήστη, με την αμοιβή να πραγματοποιείται με χρήση Bitcoin.
- Και όποιον άλλον τρόπο μπορεί να εμπνευστεί ένας νέος χρήστης για να προμηθευτεί τα πρώτα του κρυπτονομίσματα.

Ωστόσο τις περισσότερες φορές οι νέοι χρήστες, ιδιαίτερα όταν αναφερόμαστε σε επενδυτικές επιλογές, επιθυμούν την προμήθεια μεγάλης αξίας bitcoins, τα οποία είναι θεωρητικά αδύνατο να βρεθούν με τις παραπάνω τακτικές. Η έλλειψη μιας κεντρικής αρχής και ενός τραπεζικού συστήματος δημιουργεί ένα κενό στην οικονομία του Bitcoin, το οποίο καλύπτουν ιδιωτικές εταιρείες. Τα επονομαζόμενα ανταλλακτήρια. Φυσικά οι συναλλαγές με τις συγκεκριμένες εταιρείες δεν πραγματοποιούνται δωρεάν και κοστολογούνται ανάλογα με τον τιμοκατάλογο της εκάστοτε εταιρείας.

Κάθε ανταλλακτήριο διατηρεί τις δικές του τιμές αγοράς και πώλησης Bitcoin, οι οποίες προσαρμόζονται στην προσωπική προσφορά και ζήτηση που υπάρχει την δεδομένη χρονική στιγμή και συνήθως διαφέρουν από τις αντίστοιχες τιμές των υπολοίπων ανταλλακτηρίων. Οπότε δημιουργείται ένα ζήτημα, καθώς σε παγκόσμιο επίπεδο υπάρχουν αρκετές διαφορετικές ισοτιμίες ανάμεσα σε Bitcoin και USD, για παράδειγμα. Ωστόσο για την αποφυγή παρερμηνειών αλλά και για την ύπαρξη μιας κοινής συνιστάμενης ανάμεσα σε όλα τα ανταλλακτήρια, έχουν δημιουργηθεί από τις μεγάλες οικονομικές ιστοσελίδες, δείκτες οι οποίοι συνήθως υλοποιούνται ως μέσοι όροι των τιμών των διαφορετικών ανταλλακτηρίων αναλογικά με το ποσοστό τους επί του παγκόσμιου όγκου συναλλαγών. Στην συγκεκριμένη εργασία χρησιμοποιείται ο δείκτης του yahoo.finance, ο οποίος λαμβάνει τα δεδομένα του από την ιστοσελίδα *"www.cryptocompare.com"*.

Η λίστα με τα ανταλλακτήρια, τα οποία είχαν ποσοστό μεγαλύτερο από το *3%* του παγκόσμιου όγκου συναλλαγών το τελευταίο εξάμηνο *(23/12/2017-23/06/2018)*, με βάση την σελίδα "*bitcoinity.org"* είναι η εξής:

Πίνακας 6: Κατανομή των ανταλλακτηρίων Bitcoin (23/12/2017 - 23/06/2018)

Όνομα	Νομίσματα Συναλλαγών	Όγκος Συναλλαγών (bitcoins)	Ποσοστό επί του Συνόλου
Bitfinex	USD	8.526.670	30,60%
GDAX	CAD, EUR, GBP, USD	3.913.602	14,05%
bitFlyer	JPY	3.438.727	12,34%
Bitstamp	EUR, USD	3.205.144	11,50%
Kraken	CAD, EUR, GBP, JPY, KRW, USD	3.049.005	10,94%
HitBTC	EUR, USD	1.207.066	4,33%
Gemini	USD	1.186.380	4,26%
Bit-x	EUR, GBP, USD	856.224	3,07%

Για να μπορούν τα ανταλλακτήρια Bitcoin να υποστηρίξουν την λειτουργία τους, πραγματοποιώντας καθημερινές συναλλαγές, επιβάλλεται να διατηρούν διευθύνσεις Bitcoin που να συνδέονται με κρυπτονομίσματα μεγάλης συνολικής αξίας. Για τον λόγο

αυτό πολλές φορές γίνονται στόχος συντονισμένων επιθέσεων. Τις περισσότερες φορές οι επιθέσεις αποτυγχάνουν, ωστόσο έχουν πραγματοποιηθεί αρκετές επιτυχημένες απόπειρες με λεία κρυπτονομίσματα αρκετά μεγάλης χρηματικής αξίας. Οι κυριότερες ηλεκτρονικές επιθέσεις/ληστείες μετά το 2012 είναι οι εξής (Tan, et al., 2018):

2012

Η πρώτη άξια αναφοράς επίθεση σε ανταλλακτήριο κρυπτονομισμάτων. Το ανταλλακτήριο BitFloor, που εδρεύει στην Νέα Υόρκη, δέχεται επίθεση η οποία είχε ως λεία bitcoins αξίας 250.000$. Τον Απρίλιο του 2013 το συγκεκριμένο ανταλλακτήριο ανακοίνωσε ότι θα αποζημιώσει τους πληγέντες χρήστες.

2014

Ένα από τα μεγαλύτερα ανταλλακτήρια Bitcoin εκείνη την περίοδο στον κόσμο, το Mt.Gox, ανακοίνωσε την απώλεια κρυπτονομισμάτων συνολικής αξίας 480 εκατ.USD και η εταιρεία δήλωσε άμεσα πτώχευση.

2015

Το ανταλλακτήριο Bitstamp, μέσω του γενικού διευθυντή του, ανακοίνωσε πως οι χρήστες του είναι πλέον ασφαλείς, έπειτα από την κλοπή κρυπτονομισμάτων αξίας 5 εκατ. USD. Ενώ την ίδια χρονιά αποκαλύφθηκε σκάνδαλο κατάχρησης κατασχεμένων bitcoins, στο οποίο εμπλέκονταν δύο πρώην ομοσπονδιακοί πράκτορες που συμμετείχαν στην υπόθεση ανταλλαγής ναρκωτικών “Silk Road”.

2016

Το ανταλλακτήριο Gatecoin, που εδρεύει στο Hong Kong, ανακοίνωσε την απώλεια κρυπτονομισμάτων αξίας 2 εκατ. USD έπειτα από κυβερνοεπίθεση. Αντίστοιχα και το ανταλλακτήριο Bitfinex ανακοίνωσε την κλοπή 119.756 bitcoins, αξίας 65 εκατ. USD. Τον Απρίλιο του 2017 το σύνολο των χρηστών είχε αποζημιωθεί.

2017

Τα προσωπικά στοιχεία και τα στοιχεία συναλλαγών 30.000 χρηστών του ανταλλακτηρίου Bithumb, υποκλέπτονται, με την ρυθμιστική αρχή της Νοτίου Κορέας να επιβάλει χρηματικό πρόστιμο στην εταιρεία. Την ίδια περίοδο μια ομάδα προγραμματιστών, ανακάλυψε ένα κενό ασφαλείας στο λογισμικού ενός πορτοφολιού Bitcoin και προσπάθησε να ξεπλύνει κλεμμένα κρυπτονομίσματα, αξίας 30 εκατ. USD.

Μερικά λεπτά μετά την ανακοίνωση του ανταλλακτηρίου CoinDash ότι ξεκινάει την προσφορά του δικού του κρυπτονομίσματος, συντονισμένη ηλεκτρονική επίθεση είχε

ως αποτέλεσμα να κλαπούν κρυπτονομίσματα αξίας 6,6 εκατ. USD. Το Ισραηλινό ανταλλακτήριο τερμάτισε πρόωρα το σχέδιο για δικό του κρυπτονόμισμα. Ενώ η επιχείρηση που βρίσκεται πίσω από το Tether, ανακοίνωσε ότι δέχθηκε επίθεση. Τα κρυπτονομίσματα που μεταφέρθηκαν σε μη εξουσιοδοτημένη διεύθυνση, ήταν αξίας 31 εκατ. USD.

Η πλατφόρμα εξόρυξης NiceHash δέχθηκε επίθεση, με αποτέλεσμα να κλαπούν bitcoins αξίας 63 εκατ. USD. Η εταιρεία προσέφερε εκτενείς λεπτομέρειες, ώστε το συμβάν να μελετηθεί από την κοινότητα. Στα τέλη του έτους, το ανταλλακτήριο Youbit, ανακοίνωσε την πρόθεσή του να δηλώσει χρεοκοπία, λίγες ώρες μετά την ηλεκτρονική επίθεση που δέχθηκε που είχε ως αποτέλεσμα να κλαπεί το 17% των περιουσιακών του στοιχείων.

2018

Το ιαπωνικό ανταλλακτήριο Coincheck Inc. υπέστη ληστεία με λεία κρυπτονομίσματα αξίας 500 εκατ. USD. Η επίδραση των ηλεκτρονικών επιθέσεων στην ψυχολογία των επενδυτών είναι πλέον τεράστια. Συγκεκριμένα η κεφαλαιοποίηση της αγοράς των κρυπτονομισμάτων μειώθηκε κατά 42 δισεκατ. USD, έπειτα από την ανακοίνωση του ανταλλακτηρίου Coinrail ότι ένα μέρος των ηλεκτρονικών του νομισμάτων εκλάπη, χωρίς να υπάρχουν ακριβείς μετρήσεις.

Γίνεται εύκολα κατανοητό ότι τα ανταλλακτήρια αποτελούν έναν από τους κυριότερους στόχους των hackers αυτή την χρονική περίοδο, καθώς μπορούν να αποφέρουν κλοπιμαία πολύ μεγάλης χρηματικής αξίας. Κάθε φορά που ένα νέο συμβάν ανακοινώνεται και ανάλογα με το μέγεθος της ληστείας αλλά και της προβολής που θα τύχει από τα μέσα μαζικής ενημέρωσης, πραγματοποιείται μια αναταραχή στην αγορά των κρυπτονομισμάτων καθώς αποκαλύπτονται προβλήματα ασφαλείας τα οποία υπάρχουν. Αν και τα προβλήματα δεν σχετίζονται με το πρωτόκολλο του Bitcoin αλλά με τα συστήματα ασφαλείας των εταιρειών που διαχειρίζονται τα κρυπτονομίσματα. Πάραυτα η τιμή του Bitcoin επηρεάζεται και δέχεται έντονες πιέσεις.

Ρυθμιστικά πλαίσια σχετικά με τα κρυπτονομίσματα

Η αυξημένη ζήτηση και η διάδοση των κρυπτονομισμάτων, τα τελευταία χρόνια, δημιουργούν την επιτακτική ανάγκη για την καθιέρωση ενός ρυθμιστικού πλαισίου, βασισμένο στο διεθνές δίκαιο, το οποίο να διέπει την λειτουργία τους και να οριοθετεί με ξεκάθαρο τρόπο την συμμετοχή τους στην οικονομική καθημερινότητα των πολιτών.

Ωστόσο η πολύπλοκη τεχνολογία, τα αντικρουόμενα συμφέροντα αλλά και η εγγενής δυσκολία του ζητήματος, αποτελούν εμπόδια τα οποία μέχρι στιγμής δεν έχουν ξεπεραστεί και οδηγούν τις επιμέρους κυβερνήσεις των κρατών στην θέσπιση μη συντονισμένων και όχι ξεκάθαρων κανόνων, ανάλογα με την θέση την οποία υποστηρίζουν επί του θέματος. Στο σημείο αυτό θα παρουσιαστούν οι οπτικές επί των κρυπτονομισμάτων και οι πολιτικές για τα ανταλλακτήρια, που ακολουθούν οι χώρες του κόσμου με την εντονότερη επιρροή στην οικονομία των κρυπτονομισμάτων και κάποιοι διεθνείς οργανισμοί. (Rooney, 2018)

Η οπτική επί των κρυπτονομισμάτων δηλώνει κατά πόσο μια χώρα ή ένας οργανισμός θεωρεί, με βάση την νομοθεσία και τους κανόνες που διέπουν την λειτουργία του, την χρήση ενός κρυπτονομίσματος ως μέσο συναλλαγής, νόμιμη ή όχι. Η ομαδοποίηση των χωρών και των οργανισμών με βάση την οπτική τους επί των κρυπτονομισμάτων, πραγματοποιείται σε τρία σύνολα. Αναλυτικότερα:

Νόμιμο μέσο συναλλαγών: Ιαπωνία, Ελβετία.

Μη νόμιμο μέσο συναλλαγών: Νότια Κορέα, Σιγκαπούρη, Ινδία, Ευρωπαϊκή Ένωση (E.U.), Ηνωμένο Βασίλειο (U.K.), Κίνα

Εξαρτάται από τις επιμέρους νομοθεσίες:

- Η παγκόσμια ρυθμιστική αρχή (G-20), θεωρεί τα κρυπτονομίσματα ως νόμιμο μέσο συναλλαγών αλλά δεν υποχρεώνει τις επιμέρους χώρες για την αποδοχή τους.
- Οι Ηνωμένες Πολιτείες της Αμερικής (U.S.A.), θεωρούν τα κρυπτονομίσματα ως μη νόμιμο μέσο συναλλαγών, αλλά η τελική απόφαση εξαρτάται από την νομοθεσία της εκάστοτε πολιτείας.

Η πολιτική για τα ανταλλακτήρια είναι ένα σχετικά πολυπλοκότερο ζήτημα σε σχέση με την οπτική επί των κρυπτονομισμάτων. Καθώς οι περισσότερες χώρες επιθυμούν την λειτουργία ανταλλακτηρίων στην επικράτειά τους, ώστε να τους παρέχεται η δυνατότητα για άμεση φορολόγηση, η οποία προσφέρει υψηλά έσοδα στον κρατικό προϋπολογισμό. Με αποτέλεσμα να εμφανίζεται το εξής παράδοξο. Χώρες οι οποίες θεωρούν μη νόμιμη την χρήση κρυπτονομισμάτων, να υποστηρίζουν την νόμιμη λειτουργία των ανταλλακτηρίων. Συγκεκριμένα:

Νόμιμη λειτουργία: Ιαπωνία, Ηνωμένες Πολιτείες της Αμερικής (U.S.A.), Ηνωμένο Βασίλειο (U.K.), Νότια Κορέα, Ευρωπαϊκή Ένωση (E.U.), Σιγκαπούρη, Ινδία, Ελβετία.

Παράνομη λειτουργία: Κίνα.

Η ειδική περίπτωση της Ρωσίας

Η Ρωσία αποτελεί μια ιδιάζουσα περίπτωση σε πολλά ζητήματα, δεν θα μπορούσε να διαφέρει και στην περίπτωση των κρυπτονομισμάτων. Καθώς από τις αρχές του έτους έχει τεθεί, από τον υπουργό οικονομικών της χώρας, για διαβούλευση ένα σχέδιο νόμου σχετικό με το θεσμικό πλαίσιο που θα διέπει την δημιουργία, την έκδοση, την αποθήκευση και την κυκλοφορία των κρυπτονομισμάτων. Ταυτόχρονα καθορίζεται με συγκεκριμένα βήματα και υποχρεώσεις η υλοποίηση ενός ICO (Initial Coin Offering) και η δημιουργία και η διακίνηση ενός νέου token. (Helms, 2018)

Εναλλακτικά κρυπτονομίσματα

Τα δεδομένα του συγκεκριμένου κεφαλαίου, βασίζονται στα στοιχεία της σελίδας *"coinmarketcap.com"*, με ημερομηνία πρόσβασης στις *25/06/2018*.

Ο γενικός όρος κρυπτονομίσματα είναι θεωρητικά εσφαλμένος, διότι σήμερα τα περισσότερα από αυτά δεν λειτουργούν ως νομίσματα, σύμφωνα με τον ορισμό των λειτουργιών που αποδίδει ο Mankiw. Ωστόσο ο τίτλος δόθηκε στην συγκεκριμένη κατηγορία οντοτήτων με βάση τα χαρακτηριστικά τα οποία διέθετε το πρώτο κρυπτονόμισμα που δημιουργήθηκε ποτέ και δεν ήταν άλλο από το Bitcoin.

Πλέον τα κρυπτονομίσματα κατηγοριοποιούνται σε δύο ομάδες:

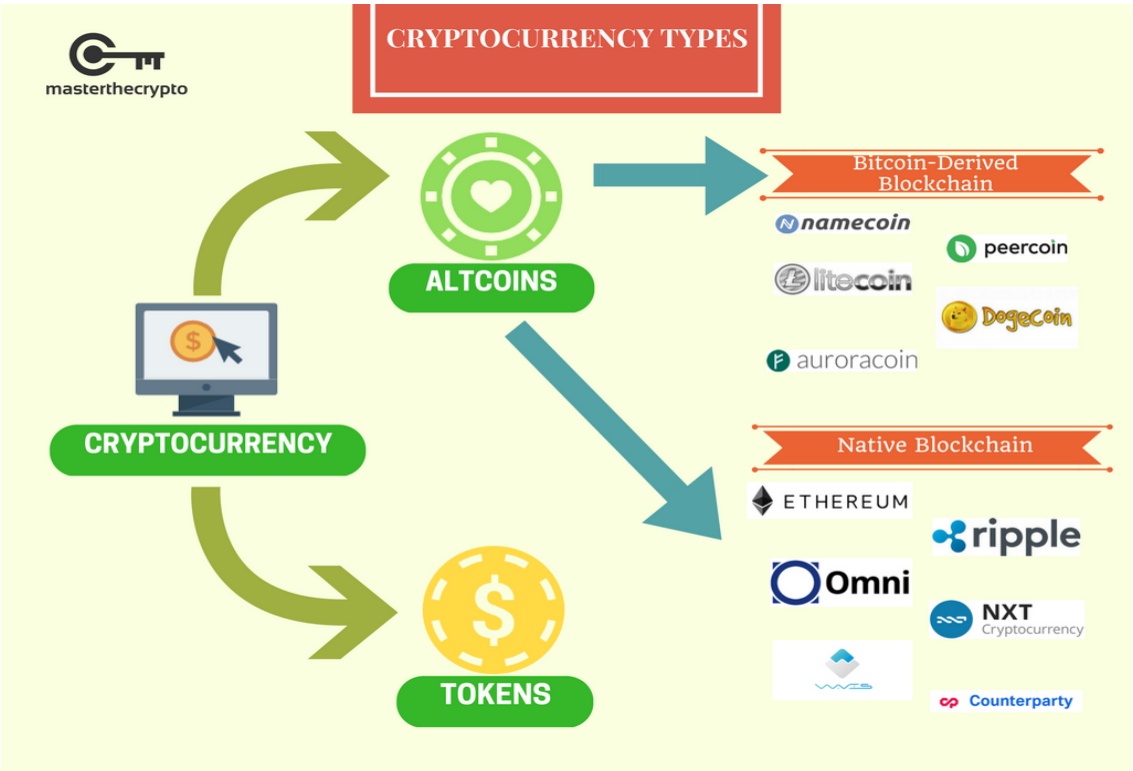
- Τα Alternative Currency Coins (Altcoins).
- Τα Tokens.

Τα περισσότερα Altcoins αποτελούν απομιμήσεις του Bitcoin και δημιουργήθηκαν από μεταβολές που πραγματοποιήθηκαν στο πρωτόκολλο του Bitcoin (hard forks), οι οποίες τους προσέδωσαν διαφορετικά χαρακτηριστικά σε σχέση με το αρχικό. Η τεχνολογία Blockchain που χρησιμοποιούν μπορεί να είναι όμοια με αυτή του Bitcoin, αλλά υπάρχουν και Altcoins τα οποία έχουν αναπτύξει την δικιά τους τεχνολογία Blockchain. Η συγκεκριμένη διαφοροποίηση αποτελεί και μια εσωτερική κατηγοριοποίηση των Altcoins σε δύο υποκατηγορίες. (MasterTheCrypto, 2017)

Με την σειρά τους, τα Tokens αποτελούν μια ψηφιακή αναπαράσταση ενός συγκεκριμένου περιουσιακού στοιχείου, το οποίο πρέπει να είναι ανταλλάξιμο και εμπορεύσιμο. Τα περιουσιακά στοιχεία μπορεί να είναι από χρηματιστηριακά εμπορεύματα, μέχρι και πόντοι πιστότητας ή και άλλα κρυπτονομίσματα. Η δημιουργία

των Tokens δεν απαιτεί την ανάπτυξη νέου πρωτοκόλλου ή νέας τεχνολογίας, για αυτό και θεωρείται ευκολότερη σε σχέση με τα Altcoins. Υπάρχουν πλατφόρμες που έχουν σχεδιαστεί ώστε να υποστηρίζουν την υλοποίηση νέων Tokens, οι πιο γνωστές από αυτές είναι η Ethereum και η Waves. Η δυνατότητα δημιουργίας νέων Tokens βασίζεται στα Smart Contracts, τα οποία είναι κώδικες ηλεκτρονικών υπολογιστών που εκτελούνται από μόνοι τους χωρίς να χρειάζονται την υποστήριξη τρίτων για να λειτουργήσουν. Τα Tokens δημιουργούνται και διατίθενται στο κοινό μέσω των Initial Coin Offerings (ICOs), οι οποίες είναι μέθοδοι χρηματοδότησης όμοιες με τα Initial Public Offerings (IPOs) που πραγματοποιούνται για μετοχές. (MasterTheCrypto, 2017)

Συνοψίζοντας η κύρια διαφορά ανάμεσα στα Altcoins και τα Tokens εντοπίζεται στην δομή τους. Τα Altcoins είναι ξεχωριστά νομίσματα με την δική τους τεχνολογία Blockchain, ενώ τα Tokens λειτουργούν βασιζόμενα σε ήδη υπάρχουσα τεχνολογία Blockchain, η οποία διευκολύνει την δημιουργία αποκεντρωμένων εφαρμογών.



Εικόνα 15: Οι τύποι των κρυπτονομισμάτων

Το Bitcoin ήταν το πρώτο κρυπτονόμισμα που τέθηκε σε λειτουργία, ωστόσο τα τελευταία χρόνια έχει αυξηθεί ο συνολικός αριθμός τους. Σήμερα είναι περισσότερα από 1.500, δημιουργώντας μια ξεχωριστή αγορά, της οποίας ο ημερήσιος όγκος συναλλαγών ξεπερνάει τα 16 δις. USD. Με βάση την συνολική κεφαλαιοποίηση, το μέγεθος της αγοράς των κρυπτονομισμάτων υπολογίζεται σε περισσότερα από 250

δισεκατομμύρια USD. Ηγέτης της αγοράς παραμένει το Bitcoin, αλλά με την πάροδο των χρόνων το ποσοστό του επί της συνολικής κεφαλαιοποίησης της αγοράς μειώνεται, παρότι η αξία του αυξάνεται. Σήμερα αγγίζει το 41,7%, διατηρώντας την τεράστια επιρροή του στον κλάδο. Ωστόσο εκτός από το Bitcoin υπάρχουν και άλλα γνωστά στο ευρύ κοινό κρυπτονομίσματα. Θα παρουσιαστούν τα κρυπτονομίσματα με κεφαλαιοποίηση μεγαλύτερη από 3 δισεκατομμύρια USD, την δεδομένη χρονική στιγμή.

Πίνακας 7: Η κεφαλαιοποίηση των μεγαλύτερων κρυπτονομισμάτων

Όνομα	Κεφαλαιοποίηση
Bitcoin	105.054.723.228 $
Ethereum	45.883.388.809 $
Ripple	18.761.374.882 $
Bitcoin Cash	12.808.496.170 $
EOS.IO	7.194.261.239 $
Litecoin	4.617.531.512 $
Stellar	3.604.917.860 $
Cardano	3.437.307.304 $

Ethereum

Το Ethereum αποτελεί μια ανοιχτού λογισμικού, δημόσια, που βασίζεται στην τεχνολογία της Blockchain αποκεντρωμένη πλατφόρμα, η οποία προσφέρει την δυνατότητα στους χρήστες της να δημιουργούν "έξυπνα συμβόλαια" (smart contract). Ένα smart contract είναι ένα κομμάτι κώδικα το οποίο επιτρέπει την ακριαία πραγματοποίηση ενεργειών, όταν τα κριτήρια που έχουν ορισθεί ικανοποιηθούν. Επίσης οι εφαρμογές εκτελούνται από την πλατφόρμα ακριβώς όπως έχουν προγραμματιστεί χωρίς καμία πιθανότητα διακοπής, λογοκρισίας, απάτης ή παρεμβολής τρίτων.

Για την υποστήριξη του Ethereum και ως επιβράβευση στα άτομα που βοηθούν στην διατήρηση της Blockchain του αλλά και στην ασφαλή λειτουργία του δικτύου του, έχει δημιουργηθεί το κρυπτονόμισμα Ether, το οποίο διαπραγματεύεται στις διεθνείς αγορές. *"https://www.ethereum.org/"*

Ripple

Το Ripple είναι ένα πρωτόκολλο συναλλαγών πραγματικού χρόνου, ένα δίκτυο ανταλλαγής νομισμάτων και εμβασμάτων που δημιουργήθηκε από την ομώνυμη

εταιρεία. Η λειτουργία του βασίζεται σε ένα ανοιχτού κώδικα, κατανεμημένο, διαδικτυακό πρωτόκολλο και υποστηρίζεται από το κρυπτονόμισμα XRP. Επιτρέπει άμεσες, ασφαλείς και σχεδόν ελεύθερες παγκόσμιες οικονομικές συναλλαγές οποιουδήποτε μεγέθους χωρίς χρεώσεις επιστροφής χρημάτων. Στο πυρήνα του υπάρχει μια κοινόχρηστη, κρυπτογραφημένη και δημόσια βάση δεδομένων καταγραφής συναλλαγών, η οποία επιτρέπει πληρωμές, ανταλλαγές και εμβάσματα ανάμεσα στους χρήστες.

Χρησιμοποιείται ήδη από ισχυρές πολυεθνικές εταιρείες και τραπεζικούς κολοσσούς, όπως η UniCredit, η UBS και η Santander, ενώ υπάρχει η προοπτική να ξεπεράσει την Visa, την MasterCard, την PayPal και τις υπόλοιπες διαδεδομένες εταιρείες του χώρου. *"https://ripple.com/"*

Bitcoin Cash

Το Bitcoin Cash είναι το αποτέλεσμα του hard fork που πραγματοποιήθηκε στην Blockchain του Bitcoin. Η εξήγηση των όρων πραγματοποιήθηκε στο κεφάλαιο της τεχνολογικής ανάλυσης της Blockchain. Η κύρια διαφορά που οδήγησε την κοινότητα στην δημιουργία του Bitcoin Cash, ήταν η αύξηση του μεγέθους του Block συναλλαγών.

EOS.IO

Η ιδιωτική εταιρεία block.one μέσω της πλατφόρμας του Ethereum ανακοίνωσε το μελλοντικό της σχέδιο για την δημιουργία ενός αποκεντρωμένου λειτουργικού συστήματος που θα υποστηρίζει βιομηχανικές εφαρμογές ευρείας κλίμακας, με σκοπό την εξάλειψη του κόστους συναλλαγών αλλά και την υλοποίηση εκατομμυρίων συναλλαγών ανά δευτερόλεπτο. Για την χρηματοδότηση του σχεδίου εξέδωσε ICO (Initial Coin Offering) και το token που διένειμε στους επενδυτές είναι το EOS.IO. Σύμφωνα με την ανακοίνωση της εταιρείας συγκεντρώθηκαν περισσότερα από ένα δισεκατομμύριο USD για την υλοποίηση του σχεδίου. Ανάλογα με το ποσοστό των tokens που κατέχει ένας χρήστης θα μπορεί να χρησιμοποιεί το αντίστοιχο ποσοστό από τις δυνατότητες του συστήματος που θα δημιουργηθεί. *"https://eos.io/"*

Litecoin

Ο σχεδιασμός του Litecoin βασίστηκε στο πρωτόκολλο του Bitcoin, με βασικό στόχο να δημιουργηθεί ένα κρυπτονόμισμα που θα πραγματοποιεί τον ίδιο αριθμό συναλλαγών σε μικρότερο χρονικό διάστημα. Ώστε να αντιμετωπιστεί ένα βασικό μειονέκτημα του Bitcoin, το οποίο είναι η μειωμένη αποδοτικότητά του στην

διεκπεραίωση καθημερινών συναλλαγών μικρής αξίας αλλά αυξημένης συχνότητας. Η εξόρυξη ενός Block συναλλαγών με χρήση Litecoin πραγματοποιείται σε 2,5 λεπτά. Ωστόσο διαφοροποίηση υπήρξε και στον αλγόριθμο κατακερματισμού, με αποτέλεσμα ο εξοπλισμός εξόρυξης του Litecoin να είναι πολυπλοκότερος και πιο ακριβός σε σχέση με τον αντίστοιχο του Bitcoin. *"https://litecoin.com/"*

Stellar

Το Stellar δημιουργήθηκε από άτομα που σχετίζονταν με το ανταλλακτήριο Mt. Gox και την Ripple. Αποτελεί ένα αποκεντρωμένο δίκτυο πληρωμών που λειτουργεί με την τεχνολογία της Blockchain. Το πρωτόκολλό του χρησιμοποιεί το ομώνυμο κρυπτονόμισμα, το οποίο αλλιώς ονομάζεται και Lumens ή XLM. Η λειτουργία του υποστηρίζεται και από το μη κερδοσκοπικό οργανισμό "Stellar Development Foundation". *"https://www.stellar.org/"*

Cardano

Το Cardano αποτελεί μια κατανεμημένη υπολογιστική πλατφόρμα που χρησιμοποιεί την τεχνολογία της Blockchain και το κρυπτονόμισμα Ada. Στοχεύει στην υλοποίηση έξυπνων συμβολαίων, αποκεντρωμένων εφαρμογών, πλευρικών αλυσίδων, υπολογισμών πολλών τμημάτων και μεταδεδομένων. Η χρήση αλγορίθμου της κατηγορίας Proof-of-Stake, έχει ως αποτέλεσμα την καλύτερη ενεργειακή απόδοση του δικτύου, ενώ ταυτόχρονα επιτρέπει την βέλτιστη διαχείριση των πόρων και την μείωση του κόστος διατήρησης της Blockchain. *"https://www.cardano.org/en/home/"*

Πίνακας 8: Πίνακας βασικών χαρακτηριστικών κρυπτονομισμάτων

Όνομα	Χρονολογία	Είδος	Αλγόριθμος Κατακερματισμού	Εξόρυξη	Μέγιστη Προσφορά
Bitcoin	2009	Coin	SHA-256	Ναι	Ναι
Ethereum	2015	Coin	Ethash	Ναι	Όχι
Ripple	2012	Coin	SHA-512	Όχι	Ναι
Bitcoin Cash	2017	Coin	SHA-256	Ναι	Ναι
EOS.IO	2017	Token (Ethereum)	-	Όχι	Ναι
Litecoin	2011	Coin	Scrypt	Ναι	Ναι
Stellar	2014	Coin	(Proof-of-Stake)	Όχι	Ναι
Cardano	2017	Coin	(Proof-of-Stake)	Όχι	Ναι

Ανάλυση Συσχετίσεων και Μοντέλο Αποτίμησης Αξίας

Στην οικονομική επιστήμη, εκτός από την κατανόηση μιας οντότητας ως προς τα τεχνικά και οικονομικά χαρακτηριστικά της, είναι σημαντική και η μελέτη της συμπεριφοράς της σε σχέση με τις υπόλοιπες οντότητες του οικονομικού περιβάλλοντος. Με σκοπό να μπορεί να αποτιμηθεί η πραγματική της αξία και να προβλεφθεί η πορεία της στο μέλλον.

Στο παρόν κεφάλαιο πραγματοποιείται μελέτη της συσχέτισης του Bitcoin με διάφορα χρηματοοικονομικά προϊόντα από όλους σχεδόν τους επενδυτικούς κλάδους. Η μελέτη βασίζεται στην απόδοση των επενδυτικών προϊόντων, με σκοπό να αποκαλυφθούν σχέσεις οι οποίες θα επιτρέψουν την δημιουργία ενός μοντέλου αποτίμησης της αξίας του Bitcoin, το οποίο θα πλησιάζει όσο το δυνατό περισσότερο την πραγματική συμπεριφορά του κρυπτονομίσματος.

Συσχέτιση του Bitcoin με διάφορα χρηματοοικονομικά προϊόντα

Η πληθώρα των επενδυτικών προϊόντων και η παγκοσμιοποιημένη αγορά, τείνει να αυξάνει τον βαθμό δυσκολίας εύρεσης συσχετίσεων ανάμεσα στα επενδυτικά προϊόντα. Ταυτόχρονα, τα κρυπτονομίσματα αποτελούν συγκριτικά νέα προϊόντα και με ιδιαίτερα ταχεία διάδοση, με αποτέλεσμα να παρουσιάζονται εντονότερες μεταβολές στην τιμή τους, αυξάνοντας ακόμη περισσότερο το επίπεδο δυσκολίας. Για να σχηματιστεί μια σφαιρική εικόνα γύρω από την συσχέτιση του Bitcoin, επιλέχθηκαν κατηγορίες επενδυτικών προϊόντων που καλύπτουν σχεδόν όλο το φάσμα της παγκόσμιας αγοράς, συγκεκριμένα:

- Χρηματιστηριακά Εμπορεύματα
- Δείκτες Χρηματιστηριακών Αγορών
- Δείκτες Νομισμάτων FOREX
- Μεμονωμένες Μετοχές Εταιρειών Τεχνολογίας
- Εναλλακτικά Κρυπτονομίσματα
- Έντοκα Γραμμάτια

Για να μπορέσει να αποτυπωθεί ακόμη καλύτερα ο διεθνής χαρακτήρας του Bitcoin, επιλέχθηκαν συνολικά δεκαεπτά προϊόντα τα οποία ανήκουν στις παραπάνω κατηγορίες και είτε συμμετέχουν σε αγορές παγκόσμιου χαρακτήρα, είτε ο συνδυασμός τους καλύπτει το μεγαλύτερο κομμάτι της παγκόσμιας αγοράς. Αναλυτικότερα:

Χρηματιστηριακά Εμπορεύματα

- Χρυσός
- Ακατέργαστο Πετρέλαιο
- Παλλάδιο

Ο χρυσός αποτελεί ένα από τα σπανιότερα μεταλλεύματα που βρίσκονται στο υπέδαφος της γης, με αποτέλεσμα να θεωρείται διαχρονικά μεγάλης αξίας. Η λειτουργία των πρώτων οργανωμένων οικονομιών βασίστηκε στον χρυσό, ενώ σήμερα πολλά κράτη αλλά και τραπεζικά ιδρύματα διατηρούν αποθέματα χρυσού ως διασφάλιση ενός μέρους της αξίας των χρημάτων των πελατών τους. Σε πολλές φάσεις της παγκόσμιας οικονομίας και ειδικότερα σε περιόδους κρίσης και υποτίμησης αξιών, ο χρυσός αποτέλεσε διέξοδο για τους επενδυτές και ένα προϊόν διαφοροποίησης από την αρνητική πορεία των αγορών, ρόλο τον οποίο ενδεχομένως να διαδραματίσει το Bitcoin σε αντίστοιχες μελλοντικές καταστάσεις. Αντίστοιχα η διαδικασία εξόρυξης του χρυσού αλλά και ο ρυθμός δημιουργίας νέων αποθεμάτων, αποτέλεσε πηγή έμπνευσης για την διαδικασία "εξόρυξης" του Bitcoin.

Το ακατέργαστο πετρέλαιο είναι η πρώτη ύλη για τα καύσιμα που χρησιμοποιούνται κατά κύριο λόγο στο σύγχρονο πολιτισμό. Η τιμή του επηρεάζει το κόστος λειτουργίας για ένα μεγάλο μέρος των παραγωγικών διαδικασιών. Ο έλεγχος των κοιτασμάτων του αποτέλεσε και αποτελεί ένα σημείο σύγκρουσης των ισχυρών κρατών του πλανήτη. Ενώ ενδιαφέρον στοιχείο είναι το γεγονός ότι η τιμή του, κυρίως τα τελευταία χρόνια, παρουσιάζει σημάδια χειραγώγησης σε παγκόσμιο επίπεδο, καθώς διεθνείς οργανισμοί όπως ο OPEC και πανίσχυρα κράτη όπως οι Η.Π.Α και η Ρωσία ελέγχουν τα αποθέματα αλλά και τον ρυθμό προσφοράς του πετρελαίου στην διεθνή αγορά. Γεγονός είναι ότι δεν παρουσιάζει κάποια εμφανή σχέση με το Bitcoin, ωστόσο επηρεάζει σε μεγάλο βαθμό την πορεία της παγκόσμιας οικονομίας. Με πολλά κράτη και μεγάλες επιχειρήσεις να επηρεάζονται άμεσα από την πορεία της τιμής του.

Το παλλάδιο δεν αποτελεί ένα από τα γνωστά χρηματιστηριακά εμπορεύματα, ωστόσο όμοια με το Bitcoin, η αξία του αυξήθηκε κατά πολύ μεγάλο βαθμό τα τελευταία χρόνια. Η κύρια αιτία της ανοδικής πορείας της τιμής του είναι η προσπάθεια για μείωση των εκπομπών του διοξειδίου του άνθρακα από του κινητήρες εσωτερικής καύσης των αυτοκινούμενων μέσων. Το παλλάδιο χρησιμοποιείται στους καταλύτες που μειώνουν τις εκπομπές. Ως γνωστό η περιβαλλοντική συνείδηση έχει αυξηθεί και η νομοθεσία έχει γίνει πιο αυστηρή αναγκάζοντας τις αυτοκινητοβιομηχανίες να

επενδύσουν στον τομέα των καταλυτών. Το παλλάδιο όπως και το Bitcoin για διαφορετικούς λόγους έχουν κινήσει το ενδιαφέρον του επενδυτικού κόσμου.

Δείκτες Χρηματιστηριακών Αγορών

- S&P 500
- Nasdaq 100
- Hang Seng 50
- Europe 50

Ο S&P 500 αποτελεί τον χρηματιστηριακό δείκτη που δημιούργησε η Standard & Poor's και στον οποίο συμμετέχουν οι 500 εταιρείες του NYSE και του Nasdaq με την μεγαλύτερη κεφαλαιοποίηση. Θεωρείται ένας από τους σημαντικότερους χρηματιστηριακούς δείκτες σε παγκόσμιο επίπεδο καθώς η πορεία του δίνει την εικόνα της αμερικανικής οικονομίας, η οποία πλησιάζει σε μεγαλύτερο βαθμό την πραγματικότητα. Η αμερικάνικη οικονομία είναι η πιο ισχυρή σε παγκόσμιο επίπεδο και αυτή που κατά κύριο λόγο καθορίζει την πορεία της παγκόσμιας οικονομίας.

Ο Nasdaq 100 είναι ένας χρηματιστηριακός δείκτης στον οποίο συμμετέχουν οι 100 μεγαλύτερες σε κεφαλαιοποίηση εταιρείες του Nasdaq, οι οποίες όμως δεν δραστηριοποιούνται στον τομέα των χρηματοπιστωτικών υπηρεσιών. Διατηρεί συγκεκριμένους κανόνες ώστε να περιορίζεται η επιρροή των μεγαλύτερων εταιρειών, ενώ οι επιχειρήσεις που συμμετέχουν δεν είναι αναγκαίο να εδρεύουν στις Η.Π.Α. Αποτελεί τον πληρέστερο δείκτη για τις εταιρείες τεχνολογίας. Ο κλάδος των τεχνολογικών εταιρειών έχει καθιερωθεί ως ο ισχυρότερος τα τελευταία χρόνια. Πρακτικά και το Bitcoin είναι ένα ακόμη τεχνολογικό προϊόν, με αποτέλεσμα οι εταιρείες τεχνολογίας να μην μπορούν να απουσιάζουν από την ανάλυσή του.

Η Νότια Κορέα αποτελεί μια σημαντική χώρα στην οικονομία των κρυπτονομισμάτων, όπως έχουμε αναφέρει και στην οικονομική περιγραφή του Bitcoin που πραγματοποιήθηκε σε προηγούμενο κεφάλαιο. Για τον λόγο αυτό επιλέχθηκε ο δείκτης Hang Seng 50, με σκοπό να αναλυθεί η συσχέτιση της οικονομίας της Νοτίου Κορέας με την πορεία του Bitcoin. Στον συγκεκριμένο δείκτη συμμετέχουν οι 50 μεγαλύτερες σε κεφαλαιοποίηση εταιρείες του χρηματιστηρίου της Νοτίου Κορέας, οι οποίες αθροιστικά διατηρούν ποσοστό μεγαλύτερο από το 50% της συνολικής κεφαλαιοποίησης του εν λόγω χρηματιστηρίου. Επιπρόσθετα τα περισσότερα και πιο επιτυχημένα ICOs (Initial Coin Offerings) πραγματοποιούνται στην Νότια Κορέα.

Ο Europe 50 είναι ένας χρηματιστηριακός δείκτης, ο οποίος δημιουργήθηκε από την STOXX Ltd. Στον συγκεκριμένο δείκτη συμμετέχουν οι 50 εταιρείες της ευρωζώνης με την μεγαλύτερη κεφαλαιοποίηση ανεξαρτήτου κράτους. Κάθε εταιρεία μπορεί να διατηρεί μέγιστο βάρος επί του δείκτη έως 10%, ενώ κάθε Σεπτέμβριο πραγματοποιείται αναθεώρηση των εταιρειών που συμμετέχουν. Σκοπός του δείκτη είναι να προβάλει μια εικόνα της οικονομικής πορείας της ευρωζώνης συνολικά. Η Ευρωζώνη, με βάση το οικονομικό πρίσμα ανάλυσης, αποτελεί το αντίβαρο των Η.Π.Α. στο παγκόσμιο οικονομικό γίγνεσθαι.

Δείκτες Νομισμάτων FOREX

- USD Index
- EURO Index

Η αγορά FOREX αποτελεί ένα μεγάλο κομμάτι των καθημερινών παγκόσμιων οικονομικών συναλλαγών, για τον λόγο αυτό κρίθηκε απαραίτητο να συμμετέχουν μεγέθη της στην ανάλυση συσχετίσεων του Bitcoin. Ωστόσο η χρήση μεμονωμένων ισοτιμιών δεν θα προσέφερε μια πλήρη εικόνα. Για τον λόγο αυτό επιλέχθηκαν δυο δείκτες που αντικατοπτρίζουν την πορεία των δύο σημαντικότερων νομισμάτων του πλανήτη, του USD και του EURO.

Οι δύο αυτοί δείκτες υλοποιούνται ως “καλάθια” ισοτιμιών ανάμεσα στο εκάστοτε νόμισμα και στα σημαντικότερα νομίσματα με τα οποία πραγματοποιούνται συναλλαγές. Το βάρος της κάθε ισοτιμίας υπολογίζεται με την χρήση σταθμισμένου γεωμετρικού μέσου όρου, της αξίας των συναλλαγών που υλοποιούνται με το εκάστοτε νόμισμα ως προς το σύνολο των συναλλαγών. Προσφέρουν ικανοποιητική εικόνα για την θέση ισχύος την οποία διακατέχουν τα παγκόσμια νομίσματα.

Μεμονωμένες Μετοχές Εταιρειών Τεχνολογίας

- Nvidia
- Apple
- Amazon

Η Nvidia αποτελεί αμερικάνικη εταιρεία με κύρια δραστηριότητα την κατασκευή ολοκληρωμένων κυκλωμάτων (chips) για την επεξεργασία δεδομένων γραφικής απεικόνισης. Προϊόντα της χρησιμοποιήθηκαν τα προηγούμενα χρόνια στην διαδικασία της εξόρυξης Bitcoin, ωστόσο σήμερα θεωρούνται μη αποδοτικά, λόγω της εξέλιξης των ASICs. Η εταιρεία παρακολουθεί τις εξελίξεις στον τομέα της εξόρυξης ενώ έχει

δηλώσει ξεκάθαρο ενδιαφέρον για την υλοποίηση προϊόντων και υπηρεσιών που θα βασίζονται στην τεχνολογία Blockchain. Με το επενδυτικό κοινό να υποστηρίζει την συγκεκριμένη προοπτική και η τιμή της μετοχής της να παρουσιάζει σταθερή άνοδο.

Η Apple είναι ο μεγαλύτερος κατασκευαστής συσκευών τεχνολογίας σε παγκόσμιο επίπεδο και ένας από τους ισχυρότερους ομίλους εταιρειών. Σχετικά με τα κρυπτονομίσματα δεν έχει παρουσιάσει κάποια δραστηριότητα, εκτός από την απαγόρευση εφαρμογών που υποστηρίζουν την διαδικασία εξόρυξης Bitcoin με την χρήση των κινητών συσκευών της. Ωστόσο ως εταιρεία τεχνολογίας παρατηρεί τις εξελίξεις αναφορικά με την τεχνολογία της Blockchain και είναι πολύ πιθανό να υλοποιήσει το δικό της σύστημα πληρωμών χρησιμοποιώντας την συγκεκριμένη τεχνολογία.

Η Amazon αυτή την στιγμή είναι η επιχείρηση με την μεγαλύτερη αξία σε παγκόσμιο επίπεδο και ο ιδρυτής της "Jeff Bezos", ο πλουσιότερος άνθρωπος του πλανήτη. Την κύρια δραστηριότητά της αποτελεί το ηλεκτρονικό εμπόριο, τομέας ο οποίος μπορεί να εξελιχθεί εφαρμόζοντας μεθόδους και τεχνικές βασισμένες στην τεχνολογία της Blockchain. Ενώ αντίστοιχα μεγάλο ενδιαφέρον θα παρουσίαζε η δημιουργία ενός συστήματος πληρωμών για τις δραστηριότητές της το οποίο θα υποστηριζόταν από το δικό της κρυπτονόμισμα.

Εναλλακτικά Κρυπτονομίσματα

- Ether
- XRP
- Bitcoin Cash
- EOS

Το Ether αποτελεί το δεύτερο μεγαλύτερο σε κεφαλαιοποίηση κρυπτονόμισμα. Δημιουργήθηκε με σκοπό να υποστηρίζει την πλατφόρμα Ethereum, η οποία χρησιμοποιείται για την υλοποίηση "έξυπνων συμβολαίων" (smart contracts).

Το XRP είναι το κρυπτονόμισμα που υποστηρίζει το πρωτόκολλο πληρωμών της Ripple. Το πρωτόκολλο ήδη χρησιμοποιείται από ισχυρές πολυεθνικές εταιρείες.

Το Bitcoin Cash αποτελεί ένα ξεχωριστό κρυπτονόμισμα, το οποίο δημιουργήθηκε από την διάσπαση της Blockchain (hard fork) του Bitcoin, με σκοπό να διατηρεί διαφορετικά χαρακτηριστικά, καλύπτοντας τα θεωρητικά μειονεκτήματα του Bitcoin.

Το EOS είναι το token που δημιουργήθηκε για την υλοποίηση του πιο επιτυχημένου ICO (Initial Coin Offering), που έχει πραγματοποιηθεί μέχρι και σήμερα. Το σχέδιο που υποστηρίζει το EOS, επιθυμεί την υλοποίηση ενός αποκεντρωμένου λειτουργικού συστήματος για βιομηχανική χρήση.

Η παρουσίαση των εναλλακτικών κρυπτονομισμάτων στο σημείο αυτό ήταν σύντομη καθώς έχουν αναλυθεί σε προγενέστερο κεφάλαιο της παρούσης εργασίας και συγκεκριμένα στο κεφάλαιο "Εναλλακτικά κρυπτονομίσματα" της οικονομικής παρουσίασης του Bitcoin.

Έντοκα Γραμμάτια

- Έντοκο γραμμάτιο των Η.Π.Α. (3-μηνης διάρκειας)

Η έκδοση γραμματίων σύντομης διάρκειας αποτελεί τον βασικό μηχανισμό βραχυχρόνιας χρηματοδότησης των κρατών. Τα γραμμάτια μπορεί να έχουν διαφορετικές διάρκειες ωρίμανσης ανάλογα με το βάθος του ορίζοντα χρηματοδότησης που επιθυμείται. Στο πλαίσιο της εργασίας επιλέχθηκε η μελέτη του έντοκου γραμματίου των Η.Π.Α. με περίοδο ωρίμανσης τους τρείς μήνες. Οι Η.Π.Α. είναι η χώρα με την ισχυρότερη οικονομία και οι πολιτικές που ακολουθεί επηρεάζουν έντονα την πορεία των χρηματιστηριακών προϊόντων. Συγκεκριμένα η απόδοση του έντοκου γραμματίου δηλώνει την εμπιστοσύνη που έχει το επενδυτικό κοινό απέναντι στις οικονομικές πολιτικές του εκάστοτε κράτους και στην δυνατότητά του να αποπληρώνει τα χρέη του.

Η λειτουργία των κρατικών μηχανισμών συνδέεται άμεσα και με την πορεία του κλασικού τραπεζικού συστήματος που κυριαρχεί στην οικονομική ζωή του πλανήτη. Τα κρυπτονομίσματα αποτελούν μια οντότητα η οποία προσφέρει εναλλακτική λύση σε περίπτωση που το παρόν σύστημα βρεθεί σε καθοδική πορεία. Καθώς δεν συνδέονται με κανέναν τρόπο μαζί του. Επενδυτές οι οποίοι δραστηριοποιούνται στον τομέα των κρατικών γραμματίων πιθανότατα να διατηρούν στα χαρτοφυλάκιά τους κρυπτονομίσματα με σκοπό να αντισταθμίσουν τον κίνδυνο αυτόν.

Χαρακτηριστικά ανάλυσης συσχετίσεων

Η διαδικασία ανάλυσης των συσχετίσεων της απόδοσης του Bitcoin βασίστηκε σε ημερήσιες τιμές κλεισίματος όλων των επενδυτικών προϊόντων. Η συγκέντρωση των δεδομένων πραγματοποιήθηκε μέσω τριών εγκεκριμένων διαδικτυακών πηγών:

- ✓ https://finance.yahoo.com/
- ✓ https://www.investing.com/
- ✓ https://fred.stlouisfed.org/

Τα δεδομένα αναλύθηκαν για τέσσερις διαφορετικές χρονικές περιόδους, καθώς το Bitcoin εμφάνισε έντονη κυκλική συμπεριφορά τον τελευταίο χρόνο. Δηλαδή μεγάλη άνοδος της τιμής του ακολουθήθηκε από έντονα πτωτική τάση. Από όταν ξεκίνησε η διάδοσή του κυρίως λόγω της έντονης ενασχόλησης των μέσων μαζικής ενημέρωσης, από την πορεία της τιμής του εκλείπουν τάσεις σχετικής σταθερότητας. Γεγονός το οποίο δημιουργεί αρκετά εμπόδια στην διαδικασία ανάλυσης του κρυπτονομίσματος. Οι χρονικές περίοδοι για τις οποίες αναλύθηκαν τα δεδομένα είναι οι εξής:

- ❖ 5 χρόνια (1.825 παρατηρήσεις).
- ❖ 1 χρόνος (365 παρατηρήσεις).
- ❖ $1^{ο}$ εξάμηνο τελευταίου έτους (183 παρατηρήσεις) – Έντονα ανοδική τάση της τιμής του Bitcoin.
- ❖ $2^{ο}$ εξάμηνο τελευταίου έτους (182 παρατηρήσεις) – Έντονα καθοδική τάση της τιμής του Bitcoin.

Οι τιμές των προϊόντων που χρησιμοποιούνται στην ανάλυση των συσχετίσεων όπως και η τιμή του Bitcoin υπολογίζονται σε USD, εξαίρεση αποτελούν δύο προϊόντα των οποίων η αξία ήταν διαθέσιμη σε EURO. Αυτοί είναι οι δείκτες Europe 50 και EURO Index.

Η συσχέτιση της απόδοσης του Bitcoin συγκριτικά με την απόδοση των υπόλοιπων επενδυτικών προϊόντων που επιλέχθηκαν, πραγματοποιήθηκε με την χρήση του συντελεστή r του Pearson. Ο συγκεκριμένος συντελεστής αποτελεί ένα μέτρο γραμμικής συσχέτισης μεταξύ δύο μεταβλητών. Οι τιμές που παίρνει ανήκουν στο κλειστό διάστημα -1 έως +1. Για το -1 ισχύει τέλεια αρνητική συσχέτιση, για το +1 τέλεια θετική συσχέτιση, ενώ για το 0 δεν υπάρχει γραμμικός συσχετισμός ανάμεσα στις δύο μεταβλητές.

Αποτελέσματα συσχετίσεων Bitcoin και επενδυτικών προϊόντων

Η ξεχωριστή φύση του Bitcoin και ο ιδιαίτερος τρόπος λειτουργίας του, ταυτόχρονα με την έλλειψη σταθερότητας της τιμής του, συνέθεσαν ένα επενδυτικό προϊόν με μοναδικά χαρακτηριστικά. Λογικό επακόλουθο ο βαθμός συσχέτισής του με τα υπόλοιπα προϊόντα της αγοράς να είναι πολύ μικρός. Για τον σκοπό της εργασίας

αναλύθηκαν τα τελευταία πέντε έτη και όχι το σύνολο των ετών από την δημιουργία του Bitcoin (2009), καθώς τα πρώτα χρόνια χαρακτηρίστηκαν από έλλειψη επενδυτικού ενδιαφέροντος. Η γενική αριθμητική εικόνα με βάση τον συντελεστή r του Pearson, δείχνει έλλειψη συσχέτισης του Bitcoin με τα επιλεγμένα επενδυτικά προϊόντα, καθώς ο συντελεστής κατά κύριο λόγο παίρνει τιμές πολύ κοντά στο μηδέν. Με την μέγιστη τιμή του να μην ξεπερνάει το 0,162 σε απόλυτο βαθμό.

Αποτελέσματα συσχετίσεων (5 χρόνια)

Για τον πίνακα αποτελεσμάτων (5 χρόνια), βλέπε προσάρτημα σελίδα 92.

Τα τελευταία πέντε χρόνια, από τις κατηγορίες προϊόντων που μελετήθηκαν, το Bitcoin παρουσιάζει χαμηλότερα επίπεδα συσχέτισης με την κατηγορία των χρηματιστηριακών εμπορευμάτων και το έντοκο γραμμάτιο. Τα χρηματιστηριακά εμπορεύματα χαρακτηρίζονται από μακροχρόνια σταθερότητα όσον αφορά την τιμή τους και από σχετικά μικρές ημερήσιες μεταβολές. Δύο χαρακτηριστικά τα οποία διαφέρουν άρδην από την συμπεριφορά της τιμής του Bitcoin. Το αρνητικό πρόσημο στον συντελεστή που συνδέει το Bitcoin με τον χρυσό μπορεί να δικαιολογηθεί από το γεγονός ότι σε κάποιες περιπτώσεις και τα δύο προϊόντα διαδραματίζουν τον ρόλο της αντιστάθμισης των επιπτώσεων από την ύπαρξη κρίσεων στον παρόν οικονομικό σύστημα. Αντίστοιχα το έντοκο γραμμάτιο παρουσίασε ραγδαία αύξηση της απόδοσής του σε σταθερή κλίμακα τα τελευταία 5 χρόνια. Καθώς από επίπεδα πολύ κοντά στο 0, η απόδοσή του το τελευταίο χρονικό διάστημα έχει πλησιάσει το 2. Ωστόσο το χαρακτηριστικό το οποίο οφείλεται κυρίως για το μικρό βαθμό συσχέτισής του με τα υπόλοιπα προϊόντα είναι η μεγάλη τυπική απόκλιση που παρουσιάζει. Λογικό αν αναλογιστεί κανείς ότι σε επίπεδα τιμών πολύ μικρά, οι ποσοστιαίες μεταβολές είναι τεράστιες ακόμη και σε καθημερινή βάση. Αντίθετα η μεγαλύτερη συσχέτιση εμφανίζεται ανάμεσα στο Bitcoin και τους αμερικάνικους χρηματιστηριακούς δείκτες. Με τους επενδυτές να βλέπουν στο Bitcoin και τα υπόλοιπα κρυπτονομίσματα, ως μια ακόμη επενδυτική ευκαιρία.

Από τους δείκτες νομισμάτων FOREX παρατηρείται μεγαλύτερη συσχέτιση του Bitcoin με την πορεία της τιμής του USD παρά με την πορεία του EURO. Ενδιαφέρον στοιχείο είναι ότι παρότι την μικρή τιμή του συντελεστή r, η συσχέτιση με το USD είναι πέντε φορές μεγαλύτερη σε σχέση με την συσχέτιση με το EURO. Σε παγκόσμιο επίπεδο, οι συναλλαγές των ανταλλακτηρίων πραγματοποιούνται κατά κύριο λόγο ανάμεσα σε USD και Bitcoin, ενώ τα υπόλοιπα παραστατικά νομίσματα διαδραματίζουν

δευτερεύοντα ρόλο. Οι τρεις τεχνολογικές εταιρείες που επιλέχθηκαν συσχετίζονται κατά μικρότερο βαθμό με το Bitcoin αλλά με αρνητική κατεύθυνση.

Δεν υπάρχει μελέτη συσχέτισης του Bitcoin με τα υπόλοιπα εναλλακτικά κρυπτονομίσματα καθώς και τα τρία που επιλέχθηκαν έχουν περίοδο ύπαρξης μικρότερη των πέντε χρόνων.

Αποτελέσματα συσχετίσεων (1 χρόνο)

Για τον πίνακα αποτελεσμάτων (1 χρόνος), βλέπε προσάρτημα σελίδα 93.

Τον τελευταίο χρόνο η τιμή του Bitcoin παρουσίασε έντονα κυκλική συμπεριφορά. Ραγδαία αύξηση το πρώτο εξάμηνο μέχρι το τέλος του 2017 και μετέπειτα απότομη μείωση. Η συμπεριφορά αυτή είχε ως αποτέλεσμα τα επίπεδα συσχέτισης προς όλα τα υπόλοιπα επενδυτικά προϊόντα να είναι χαμηλότερα σε σχέση με την περίοδο της τελευταίας πενταετίας. Ωστόσο υπήρξαν και εξαιρέσεις. Η συσχέτιση του Bitcoin με το παλλάδιο αυξήθηκε διότι τον τελευταίο χρόνο η τιμή του παλλαδίου ακολούθησε έντονα ανοδική τάση, επηρεασμένη από την έντονη αύξηση της ζήτησής του, κυρίως λόγω της χρήσης του στους καταλύτες των κινητήρων εσωτερικής καύσης. Παρόμοια περίπτωση αποτελεί και το έντοκο γραμμάτιο, καθώς σε αντίθεση με την πενταετία, για τον τελευταίο χρόνο η τυπική του απόκλιση κινείται σε χαμηλότερα επίπεδα. Η αλλαγή κατεύθυνσης της συσχέτισης οφείλεται στην καθοδική πορεία του Bitcoin στο $2^{ο}$ εξάμηνο του έτους.

Αλλαγή παρατηρήθηκε και στους δείκτες νομισμάτων FOREX. Συγκεκριμένα η συσχέτιση του Bitcoin με το EURO ξεπέρασε την συσχέτισή του με το USD. Η μεταβολή αυτή κυρίως οφείλεται στην πτωτική πορεία που ακολούθησε το USD το τελευταίο χρονικό διάστημα. Η μείωση της δυναμικής του USD ήταν έντονη και με την σειρά της οφείλεται στην εκλογή του προέδρου Trump και στις οικονομικές πολιτικές που ακολουθήθηκαν για ένα "φθηνότερο" USD. Τα υπόλοιπα δεδομένα που σχετίζονται με τους δείκτες νομισμάτων FOREX παρέμειναν σχετικά σταθερά. Αντίστοιχα η συσχέτιση του Bitcoin με τον δείκτη του Νότιου Κορεάτικου χρηματιστηρίου παρουσίασε μεταβολή στην κατεύθυνση του από θετική τα τελευταία πέντε χρόνια σε αρνητική για τον τελευταίο χρόνο.

Την εμφάνισή τους στην συγκεκριμένη χρονική περίοδο πραγματοποιούν και τα εναλλακτικά κρυπτονομίσματα, καθώς Ethereum, XRP και EOS έχουν ξεπεράσει τον

έναν χρόνο ύπαρξης. Ωστόσο με εξαίρεση το Ethereum η συσχέτιση που παρουσιάζουν με το Bitcoin κινείται σε πολύ χαμηλά επίπεδα.

Αποτελέσματα συσχετίσεων (1^{ο} εξάμηνο τελευταίου χρόνου)

Για τον πίνακα αποτελεσμάτων (1^{ο} εξάμηνο τελευταίου χρόνου), βλέπε προσάρτημα σελίδα 94.

Το πρώτο εξάμηνο του τελευταίου έτους η πορεία της παγκόσμιας οικονομίας ήταν ιδιαίτερα ανοδική, φυσικά και δεν πλησίασε τα επίπεδα αύξησης της τιμής του Bitcoin, ωστόσο υπήρξε ένα κλίμα ανάπτυξης και ευφορίας. Αποτέλεσμα ήταν να αυξηθούν και τα γενικά επίπεδα συσχέτισης των επιλεγμένων επενδυτικών προϊόντων με το Bitcoin. Συγκεκριμένα παρατηρήθηκε έντονη αύξηση της συσχέτισης του Bitcoin με το ακατέργαστο πετρέλαιο. Καθώς το πρώτο εξάμηνο του τελευταίου χρόνου οι πολιτικές του OPEC για μείωση των παγκόσμιων αποθεμάτων πετρελαίου και η συμφωνία για συνέχισή τους για τον επόμενο χρόνο είχε ως αποτέλεσμα η τιμή του να αυξηθεί σε ιστορικές για τα τελευταία χρόνια τιμές. Αύξηση συσχέτισης και ταυτόχρονα θετική κατεύθυνση παρατηρείται και ανάμεσα στο έντοκο γραμμάτιο και το Bitcoin. Με τα δύο προϊόντα να ακολουθούν έντονα ανοδική πορεία.

Στην κατηγορία των αμερικανικών χρηματιστηριακών δεικτών παρατηρείται αλλαγή καθώς ο Nasdaq 100 ξεπερνάει σε επίπεδα συσχέτισης με το Bitcoin τον S&P 500, αποτέλεσμα το οποίο οφείλεται στην ανάπτυξη που παρουσίασαν οι τεχνολογικές εταιρείες στο συγκεκριμένο χρονικό διάστημα. Αναλυτικότερα η κατεύθυνση της συσχέτισης των επιλεγμένων τεχνολογικών εταιρειών μεταβλήθηκε από αρνητική σε θετική και το επίπεδό της συσχέτισής τους με το Bitcoin αυξήθηκε αισθητά.

Μεγάλη τιμή συσχέτισης ανάμεσα στο Bitcoin και τα επιλεγμένα επενδυτικά προϊόντα παρατηρείται στην συγκεκριμένη χρονική περίοδο και είναι ανάμεσα στον δείκτη FOREX του USD και το Bitcoin. Το USD στο πρώτο εξάμηνο του τελευταίου έτους παρέμεινε σχετικά σταθερό με ελαφρά πτωτική τάση με αποτέλεσμα η τυπική απόκλιση των ημερήσιων μεταβολών του να παραμένει σε πολύ χαμηλά επίπεδα. Παρόμοια συμπεριφορά εμφάνισε και η τιμή του Bitcoin τους πρώτους μήνες του τελευταίου εξαμήνου πριν ξεκινήσει η ραγδαία αύξηση που εκτόξευσε την αξία του στα μέχρι στιγμής ανώτερα επίπεδα που έχει φτάσει.

Αποτελέσματα συσχετίσεων ($2^{ο}$ εξάμηνο τελευταίου χρόνου)

Για τον πίνακα αποτελεσμάτων ($2^{ο}$ εξάμηνο τελευταίου χρόνου), βλέπε προσάρτημα σελίδα 95.

Το δεύτερο εξάμηνο του τελευταίου έτους, έπειτα από την ραγδαία αύξηση που οδήγησε στα υψηλότερα επίπεδα της τιμής του Bitcoin, υπήρξε μια αντιστροφή του κλίματος και έντονη μείωση της αξίας του. Συμπεριφορά αντίθετη από την πορεία των τιμών της πλειονότητας των επιλεγμένων επενδυτικών προϊόντων. Με αποτέλεσμα τα γενικότερα επίπεδα συσχέτισης να μειωθούν ξανά και η κατεύθυνση των συσχετίσεων να μεταβληθεί, με τα περισσότερα προϊόντα να εμφανίζουν αρνητικές τιμές.

Αναλυτικότερα τα χρηματιστηριακά εμπορεύματα για πρώτη φορά παρουσίασαν αρνητική συσχέτιση με το Bitcoin καθώς οι τιμές τους στην συγκεκριμένη χρονική περίοδο είτε παρέμειναν σχετικά σταθερές είτε αυξήθηκαν. Οι επιλεγμένες εταιρείες τεχνολογίας, όπως και ο χρηματιστηριακός δείκτης Nasdaq 100 συνέχισαν την ανοδική πορεία του πρώτου εξαμήνου και η τιμή του δείκτης r με το Bitcoin πέρασε σε επίπεδα αρνητικής συσχέτισης. Ειδικά στην περίπτωση της Nvidia η αρνητική συσχέτιση είναι σχετικά έντονη καθώς η συγκεκριμένη εταιρεία παρουσίασε το δεύτερο εξάμηνο του τελευταίου έτους μεγαλύτερα από τα αναμενόμενα κέρδη και η αξία των μετοχών της αυξήθηκε έντονα, δηλαδή ακριβώς αντίθετη πορεία από την τιμή του Bitcoin, η οποία μειώθηκε κατά πολύ μεγάλο ποσοστό πριν σταθεροποιηθεί σχετικά στα μειωμένα επίπεδα.

Αντίθετα από τον Nasdaq 100, ο οποίος συνέχισε την ανοδική πορεία του, ο δείκτης S&P 500 παρουσίασε μεμονωμένες απώλειες καθώς είχε φτάσει σε πολύ υψηλά επίπεδα στις αρχές του 2018, για τον λόγο αυτόν η συσχέτισή του με το Bitcoin είναι θετικής κατεύθυνσης αλλά όχι ιδιαίτερα υψηλού επιπέδου. Όσον αφορά τους δείκτες νομισμάτων FOREX, ο δείκτης του USD παρουσιάζει αρνητική συσχέτιση με το Bitcoin, καθώς το USD εμφάνισε σημάδια ανάκαμψης την συγκεκριμένη χρονική περίοδο.

Στα εναλλακτικά κρυπτονομίσματα προστέθηκε και το Bitcoin Cash το οποίο εμφανίζει σχετικά υψηλότερα επίπεδα συσχέτισης με το Bitcoin, καθώς η σύνδεσή τους είναι τεράστια, με το Bitcoin Cash να αποτελεί αποτέλεσμα ενός hard fork που πραγματοποιήθηκε στην Blockchain του Bitcoin. Φαινόμενο το οποίο έχει περιγραφεί σε προηγούμενα κεφάλαια της παρούσης εργασία.

Η μεγαλύτερη τιμή συσχέτισης από την μελέτη των επιλεγμένων χρηματιστηριακών προϊόντων παρατηρείται την συγκεκριμένη χρονική περίοδο και είναι ανάμεσα στο έντοκο γραμμάτιο των Η.Π.Α. και το Bitcoin. Τα δύο προϊόντα κινήθηκαν με αντίθετες πορείες. Το Bitcoin έχανε μεγάλο μέρος της αξίας του, ενώ το έντοκο γραμμάτιο συνέχιζε την σταθερά ανοδική πορεία της απόδοσής του, μειώνοντας έντονα την τιμή του.

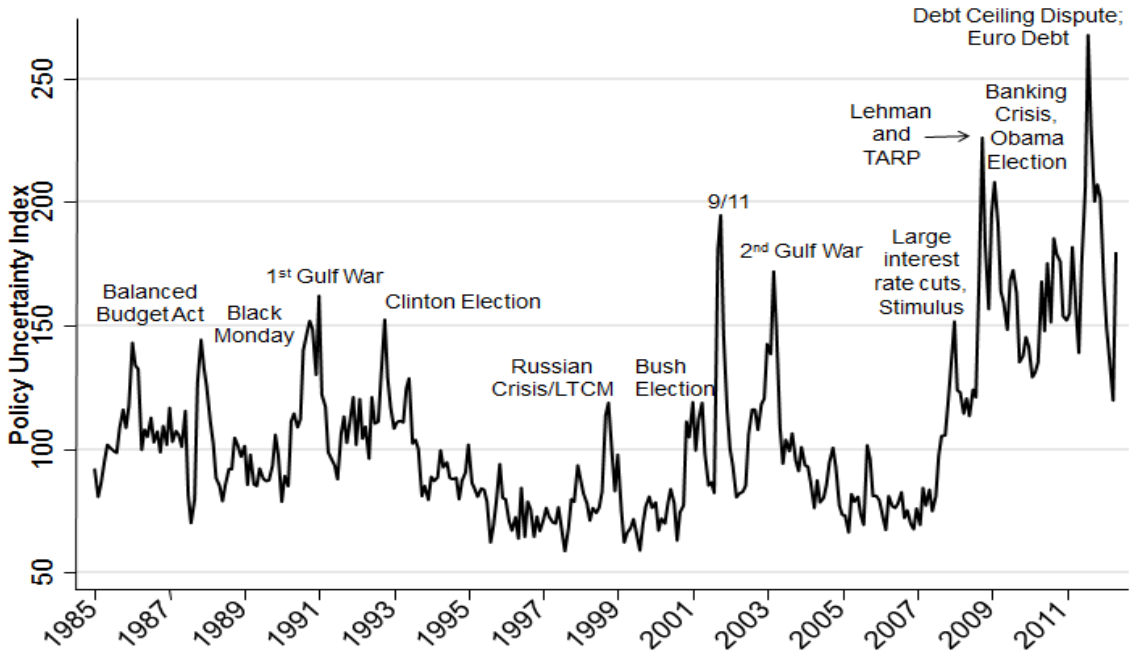
Συσχέτιση του Bitcoin με τον δείκτη Economic Policy Uncertainty (E.P.U.)

Στο πρώτο κομμάτι της ανάλυσης της συσχέτισης του Bitcoin πραγματοποιήθηκε σύγκριση της απόδοσής του με τις αποδόσεις άλλων χρηματοοικονομικών προϊόντων. Ωστόσο ανάλυση συσχέτισης μπορεί να υλοποιηθεί συγκρίνοντας το Bitcoin και με άλλους ειδικούς δείκτες που έχουν δημιουργηθεί. Για τον σκοπό της συγκεκριμένης εργασίας επιλέχθηκε ο δείκτης «Economic Policy Uncertainty (EPU)». (Baker, et al., 2016)

Αναλυτικότερα ο δείκτης EPU, προσπαθεί να ποσοτικοποιήσει την αβεβαιότητα που υπάρχει γύρω από μια οικονομική πολιτική που ακολουθείται, προσεγγίζοντας με αυτόν τον τρόπο την αβεβαιότητα για το οικονομικό περιβάλλον γενικότερα. Τα αποτελέσματά του βασίζονται σε τρία βασικά συστατικά:

i. Στην συχνότητα με την οποία εμφανίζονται δημοσιεύματα, σε ειδικά επιλεγμένες εφημερίδες σε παγκόσμιο επίπεδο, τα οποία αναφέρονται σε οικονομική αβεβαιότητα.
ii. Στις εκθέσεις των εκάστοτε υπουργείων οικονομικών των χωρών, οι οποίες περιέχουν καταλόγους με τις διατάξεις του κώδικα που προβλέπεται να μεταβληθούν ή να καταργηθούν τα επόμενα χρόνια.
iii. Στις διαφορές που παρατηρούνται ανάμεσα στις προβλέψεις τις οποίες υλοποιούν αναγνωρισμένοι σύμβουλοι επιχειρήσεων, για την κατάσταση και την πορεία του οικονομικό περιβάλλοντος.

Τα αποτελέσματα παρουσιάζουν σύνδεση του συγκεκριμένου δείκτη με την ύπαρξη αναταραχών στο οικονομικό περιβάλλον. Καθώς ακραία υψηλές τιμές εμφανίζονται ταυτόχρονα με την ύπαρξη γεγονότων που μεταβάλουν την σταθερή οικονομική πορεία.



Εικόνα 16: Δείκτης EPU και σημαντικά οικονομικά γεγονότα

Περισσότερες πληροφορίες για τον δείκτη Economic Policy Uncertainty (EPU), στην επίσημη ιστοσελίδα του: *"http://www.policyuncertainty.com/index.html"*

Στην ανάλυση πραγματοποιήθηκαν συγκρίσεις οι οποίες βασίζονταν σε μηνιαίες τιμές αλλά και ημερήσιες τιμές του δείκτη ανάλογα με την διαθεσιμότητα των δεδομένων. Το χρονικό εύρος αφορούσε την τελευταία πενταετία, ενώ επιλέχθηκαν δείκτες χωρών οι οποίες καλύπτουν μεγάλο μέρος της παγκόσμιας οικονομικής δραστηριότητας. Σε αντιστοίχηση με την ανάλυση που προηγήθηκε, η συσχέτιση υπολογίζεται σύμφωνα με τον δείκτη r του Pearson.

Ημερήσιες τιμές δεδομένων:

- Δείκτης EPU των Ηνωμένων Πολιτειών Αμερικής
- Δείκτης EPU του Ηνωμένου Βασιλείου

Μηνιαίες τιμές δεδομένων:

- Παγκόσμιος Δείκτης EPU
- Δείκτης EPU των Ηνωμένων Πολιτειών Αμερικής
- Δείκτης EPU της Νοτίου Κορέας
- Δείκτης EPU της Κίνας
- Δείκτης EPU της Ευρωπαϊκής Ένωσης
- Δείκτης EPU της Ρωσίας

Αποτελέσματα συσχετίσεων Bitcoin και Economic Policy Uncertainty (E.P.U.)

Ημερήσιες τιμές δεδομένων:

Πίνακας 9: Αποτελέσματα συσχετίσεων Bitcoin-EPU (ημερήσιες τιμές)

Pearson's r	USA EPU	UK EPU
Bitcoin	0,00343656	-0,01227419

Ο δείκτης EPU παρουσιάζει αρκετά μεγάλη τυπική απόκλιση στην καθημερινή μεταβολή της τιμής του, στην συγκεκριμένη περίπτωση ξεπερνούσε το 0,5 ενώ αντίστοιχα η τυπική απόκλιση του Bitcoin πλησίαζε το 0,06. Σε συνδυασμό με την συγκριτικά μικρή τιμή της συνδιακύμανσης των μεγεθών, το αποτέλεσμα του δείκτη r του Pearson παρουσίασε τιμές πολύ κοντά στο μηδέν, δηλαδή την έλλειψη συσχέτισης ανάμεσα στα μεγέθη. Με θετικό πρόσημο για τις Η.Π.Α. και αρνητικό για το Ηνωμένο Βασίλειο. Για τον λόγο αυτό όσον αφορά την μελέτη του δείκτη EPU η χρήση μηνιαίων τιμών θεωρείται καταλληλότερη καθώς παρουσιάζει την τάση που υπάρχει στο οικονομικό περιβάλλον, χωρίς να εμπεριέχει τις έντονες καθημερινές μεταβολές, που πιθανόν να οφείλονται στα ημερήσια δημοσιεύματα των εφημερίδων.

Μηνιαίες τιμές δεδομένων:

Πίνακας 10: Αποτελέσματα συσχετίσεων Bitcoin-EPU (μηνιαίες τιμές)

Pearson's r	Global EPU	USA EPU	South Korea EPU	China EPU	Europe EPU	Russia EPU
Bitcoin	0,10562	0,25631	-0,16695	-0,00159	0,15538	-0,08445

Οι τιμές του Pearson's r για τα μηνιαία δεδομένα του Bitcoin και του δείκτη EPU, αγγίζουν υψηλότερα επίπεδα υποδηλώνοντας εντονότερη συσχέτιση, είτε όμοιας είτε αντίθετης κατεύθυνσης. Σε αντίθεση με ότι έχει μελετηθεί μέχρι στιγμής.

Η οικονομική κρίση του 2008 και οι προεκτάσεις της είχαν ως αποτέλεσμα τα τελευταία χρόνια τα επίπεδα τιμών του δείκτη EPU να αυξηθούν σε παγκόσμιο επίπεδο. Καθώς η εμπιστοσύνη των πολιτών έναντι του οικονομικού συστήματος αλλά και του συνόλου των οικονομικών πολιτικών των κυβερνήσεων έχει μειωθεί. Μια μέθοδος αντιστάθμισης των επιπτώσεων της ύπαρξης κρίσεων στο παρών οικονομικό σύστημα, αποτελεί η μακροχρόνια επένδυση σε Bitcoin και στα κρυπτονομίσματα γενικότερα. Διότι η οικονομία των κρυπτονομισμάτων είναι πλήρως αποκεντρωμένη και η λειτουργία τους δεν σχετίζεται με το παρών οικονομικό σύστημα. Σε περίπτωση που η αξιοπιστία του οικονομικού συστήματος συνεχίζει να μειώνεται όλο και μεγαλύτερος

αριθμός επενδυτών θα διατηρεί κρυπτονομίσματα στα χαρτοφυλάκιά του. Αυξάνοντας την συσχέτιση ανάμεσα στα δύο μεγέθη. Στα χρόνια πριν δημιουργηθούν τα κρυπτονομίσματα τον συγκεκριμένο ρόλο αναλάμβανε η επένδυση στον χρυσό και στα υπόλοιπα πολύτιμα μέταλλα. Ωστόσο τα τελευταία χρόνια παρατηρείται συσχέτιση της τιμής των πολύτιμων μετάλλων με την πορεία της παγκόσμιας αγοράς, στοιχείο που υποδηλώνει την παύση του παραπάνω δεσμού.

Ο δείκτης EPU των Η.Π.Α. παρουσιάζει την μεγαλύτερη συσχέτιση με το Bitcoin, γεγονός που δικαιολογείται από δύο δεδομένες καταστάσεις. Πρώτον, το μεγαλύτερο ποσοστό ημερησίων συναλλαγών κρυπτονομισμάτων πραγματοποιείται στις Η.Π.Α και δεύτερον, το νομικό πλαίσιο που σχετίζεται με τα κρυπτονομίσματα στις περισσότερες πολιτείες των Η.Π.Α. είναι ενθαρρυντικό όσον αφορά την χρήση τους. Όμοια και ο δείκτης EPU των ευρωπαϊκών κρατών εμφανίζει συσχέτιση με το Bitcoin, καθώς οι ευρωπαίοι επενδυτές επλήγησαν έντονα από τις επιπτώσεις της πρόσφατης οικονομικής κρίσης και αναγνωρίζουν την αντιστάθμιση που μπορούν να προσφέρουν τα κρυπτονομίσματα.

Στις περισσότερο κλειστές και ελεγχόμενες οικονομίες όπως είναι αυτές της Ρωσίας και της Κίνας η χρήση των κρυπτονομισμάτων δεν είναι διαδεδομένη και το νομικό πλαίσιο των χωρών την περιορίζει έντονα. Με αποτέλεσμα να παρουσιάζουν πολύ χαμηλά επίπεδα συσχέτισης οι αντίστοιχοι δείκτες EPU με το Bitcoin.

Η περίπτωση της Νοτίου Κορέας είναι ιδιαίτερη καθώς τα κρυπτονομίσματα χρησιμοποιούνται περισσότερο ως παράλληλο νόμισμα στις καθημερινές οικονομικές συναλλαγές παρά ως επενδυτικά προϊόντα και αντισταθμιστές κινδύνου. Τα μεγαλύτερα ανταλλακτήρια εδρεύουν στην συγκεκριμένη χώρα, στην οποία πραγματοποιούνται και τα περισσότερα και πιο επιτυχημένα ICOs (Initial Coin Offerings).

Ο δείκτης Global EPU αποτελεί σταθμισμένο μέσο όρο των υπόλοιπων δεικτών των επιμέρους χωρών, οπότε η τιμή του δεν επηρεάζεται από επιπλέον παράγοντες από αυτούς που έχουν παρουσιαστεί.

Για διάγραμμα με τις μεταβολές της απόδοσης του Bitcoin και του δείκτη USA EPU, βλέπε προσάρτημα σελίδα 96.

Μοντέλο αποτίμησης αξίας Bitcoin

Ο σχεδιασμός και η υλοποίηση μοντέλων πρόβλεψης είναι μια διαδικασία η οποία δεν τελειώνει ποτέ. Ο κάθε ενδιαφερόμενος έχει την δυνατότητα να επιλέξει τα δικά του δεδομένα, για τις χρονικές περιόδους που επιθυμεί και να εξάγει το στατιστικά αρτιότερο μοντέλο με βάση τις επιλογές του. Το μοναδικό όριο είναι η φαντασία του μελετητή. Στην βιβλιογραφία υπάρχουν αρκετά μοντέλα που αφορούν την πρόβλεψη της τιμής του Bitcoin άλλα πολυπλοκότερα άλλα πιο απλοποιημένα, ωστόσο κανένα δεν μπορεί να θεωρηθεί περιττό καθώς καλύπτει διαφορετικό φάσμα επιλογών. Στο πλαίσιο της συγκεκριμένης εργασίας η δημιουργία του μοντέλου αποτίμησης της αξίας του Bitcoin βασίζεται σε διάφορα χρηματοοικονομικά προϊόντα που μελετήθηκαν στο κεφάλαιο των συσχετίσεων.

Χαρακτηριστικά επιλογής ανεξάρτητων μεταβλητών

Τα χρηματοοικονομικά προϊόντα που μελετήθηκαν στο κεφάλαιο των συσχετίσεων ήταν συνολικά δεκαεπτά. Προφανώς και δεν θα μπορούσαν να χρησιμοποιηθούν όλα σε ένα μοντέλο πρόβλεψης ως ανεξάρτητες μεταβλητές. Καθώς το πλήθος τους είναι αυξημένο, ενώ ταυτόχρονα δημιουργούνται συσχετίσεις μεταξύ τους λόγω των εκάστοτε παρόμοιων χαρακτηριστικών τους. Για να αποφευχθεί η συμμετοχή δύο ή και παραπάνω αλληλοσχετιζόμενων προϊόντων στο μοντέλο πρόβλεψης, θεσπίστηκαν επτά κανόνες επιλογής των ανεξάρτητων μεταβλητών, συγκεκριμένα:

- Μη χρησιμοποίηση εναλλακτικών κρυπτονομισμάτων.
- Επιλογή ενός εκ των S&P 500 και Nasdaq 100.
- Επιλογή ενός εκ των Euro Index και USD Index.
- Επιλογή μιας εκ των Nvidia, Apple και Amazon.
- Το πολύ ένας δείκτης EPU.
- Από 4 έως 6 ανεξάρτητες μεταβλητές.
- Χρήση ημερήσιων δεδομένων των τελευταίων 5 χρόνων.

Το Bitcoin είναι το πρώτο κρυπτονόμισμα που δημιουργήθηκε αλλά και το πιο διαδεδομένο, με αποτέλεσμα να κατέχει ποσοστό μεγαλύτερο του 40% της συνολικής αγοράς κρυπτονομισμάτων, σε όρους κεφαλαιοποίησης. Ταυτόχρονα η δημιουργία πολλών μεταγενέστερων κρυπτονομισμάτων βασίζεται στα χαρακτηριστικά και τις λειτουργίες του Bitcoin. Παρατηρώντας τις ημερήσιες μεταβολές των οντοτήτων της συγκεκριμένης αγοράς εξάγεται το συμπέρασμα ότι το Bitcoin επηρεάζει την πορεία

των υπόλοιπων εναλλακτικών κρυπτονομισμάτων και όχι το αντίστροφο. Γεγονός το οποίο απαγορεύει την χρήση τους ως ανεξάρτητες μεταβλητές σε ένα μοντέλο πρόβλεψης της τιμής του Bitcoin.

Οι δείκτες S&P 500 και Nasdaq 100 είναι δύο δείκτες των αμερικανικών χρηματιστηρίων. Συγκεκριμένα στον S&P 500 συμμετέχουν οι 500 μεγαλύτερες σε κεφαλαιοποίηση εταιρείες του NYSE και του Nasdaq, ενώ στον Nasdaq 100 συμμετέχουν οι 100 μεγαλύτερες σε κεφαλαιοποίηση εταιρείες του Nasdaq που όμως δεν ανήκουν στον κλάδο των χρηματοπιστωτικών ιδρυμάτων. Είναι εμφανές ότι ο S&P 500 είναι ένας πιο γενικός δείκτης στον οποίο συμμετέχουν πολλά από τα συστατικά του Nasdaq 100. Αντίστοιχα ο Nasdaq 100 αποτελεί έναν δείκτη ο οποίος επικεντρώνεται στην πορεία των αμερικανικών τεχνολογικών εταιρειών. Λογικό επακόλουθο είναι η τιμή του συντελεστή Pearson's r των δύο δεικτών για την τελευταία πενταετία, να αγγίζει το 0,924, δηλαδή σχεδόν την απόλυτη συσχέτιση. Λόγω της παραπάνω σχέσης, η ταυτόχρονη χρήση και των δύο σε ένα μοντέλο πρόβλεψης θεωρείται λανθασμένη.

Οι δείκτες Euro Index και USD Index αποτελούν "καλάθια" σταθμισμένων ισοτιμιών των δύο ισχυρότερων νομισμάτων παγκοσμίως. Ο λόγος για τον οποίο δεν μπορούν να χρησιμοποιηθούν ταυτόχρονα σε ένα μοντέλο πρόβλεψης είναι το γεγονός ότι η τιμή τους επηρεάζεται κατά πολύ μεγάλο ποσοστό από την ισοτιμία USD / Euro. Καθώς και για τους δύο δείκτες ο μεγαλύτερος όγκος συναλλαγών είναι αυτός που πραγματοποιείται ανάμεσα στις Η.Π.Α. και την Ευρωπαϊκή Ένωση.

Οι εταιρείες Nvidia, Apple και Amazon είναι τρεις πολυεθνικές εταιρείες με έδρα τις Η.Π.Α. Δραστηριοποιούνται στον τεχνολογικό τομέα ωστόσο με διαφορετική ειδίκευση. Η Nvidia ειδικεύεται στην σχεδίαση και κατασκευή ολοκληρωμένων κυκλωμάτων (chips) για την επεξεργασία δεδομένων γραφικής απεικόνισης, η Apple στην κατασκευή εξελιγμένων ηλεκτρονικών συσκευών και των αντίστοιχων λειτουργικών συστημάτων, ενώ η Amazon στο ηλεκτρονικό εμπόριο. Η εξέλιξη τους τα τελευταία χρόνια ραγδαία και η πορεία τους επηρεασμένη από την άνοδο του τεχνολογικού κλάδου. Επιπρόσθετα και οι τρεις συμμετέχουν στον υπολογισμό των δεικτών S&P 500 και Nasdaq 100 των αμερικανικών χρηματιστηρίων. Λόγω της μεταξύ τους σύνδεσης, η χρήση μόνο μιας εκ των τριών εταιρειών στο μοντέλο πρόβλεψης θεωρήθηκε επιβεβλημένη. Επιλογή η οποία δικαιολογείται και από το γεγονός ότι ο συντελεστής συσχέτισης r, ανάμεσα στις τρεις εταιρείες λαμβάνει τιμές

κοντά στο 0,3. Δηλαδή αρκετές φορές εντονότερη συσχέτιση αναλογικά με τις υπόλοιπες τιμές των προς μελέτη επενδυτικών προϊόντων.

Το πιο έντονα μεταβαλλόμενο συστατικό στοιχείο του υπολογισμού των δεικτών EPU για τις διάφορες χώρες, είναι τα οικονομικά δημοσιεύματα των εκάστοτε εφημερίδων. Ωστόσο τα δημοσιεύματα υπάρχει πιθανότητα να επηρεάζονται από οικονομικά γεγονότα παγκόσμιου βεληνεκούς. Για τον λόγο αυτό παρατηρείται μια ταυτόχρονη τις περισσότερες φορές πορεία στους δείκτες EPU των διάφορων χωρών. Για να αποφευχθεί το γεγονός παραπάνω από μια μεταβλητές του μοντέλου να επηρεάζονται από την ίδια αιτία, επιλέχθηκε η χρήση του πολύ ενός δείκτη EPU.

Γραμμικό μοντέλο παλινδρόμησης

Κατά την διάρκεια επεξεργασίας των δεδομένων χρησιμοποιήθηκαν τα λογισμικά πακέτα MS Office, SPSS και το λογισμικό Gretl. Για τον υπολογισμό του γραμμικού μοντέλου πρόβλεψης της τιμής του Bitcoin εκτελέστηκαν παλινδρομήσεις ελαχίστων τετραγώνων (OLS) για όλους τους πιθανούς συνδυασμούς ανεξάρτητων μεταβλητών, με βάση πάντα τους προαναφερθέντες κανόνες επιλογής. Το τελικό μοντέλο περιλαμβάνει τις εξής έξι ανεξάρτητες μεταβλητές:

- ✓ Αργό πετρέλαιο
- ✓ Παλλάδιο
- ✓ Euro Index
- ✓ S&P 500
- ✓ Nvidia
- ✓ Έντοκο γραμμάτιο των Η.Π.Α. (3-μηνης διάρκειας)

Στο σημείο αυτό αξίζει να σημειωθεί ότι για την εκτέλεση των παλινδρομήσεων χρησιμοποιήθηκε χρονική υστέρηση των ανεξάρτητων μεταβλητών σε σχέση με τις τιμές της εξαρτημένης μεταβλητής κατά μια χρονική περίοδο, δηλαδή μια ημέρα, καθώς τα προς επεξεργασία δεδομένα ήταν ημερήσιας συχνότητας.

Για τις παραπάνω ανεξάρτητες μεταβλητές υπολογίστηκαν οι αντίστοιχοι συντελεστές, ενώ ταυτόχρονα και ο σταθερός όρος ήταν με βάση τα αποτελέσματα, στατιστικά σημαντικός. Η τελική γραμμική εξίσωση του μοντέλου έχει την εξής μορφή:

$$BTC_{price} = -11.410{,}1 - 38{,}38 * crudeOil_{price} + 6{,}315 * palladium_{price} - 1{,}289 * S\&P500 + 125{,}083 * euroIndex + 70{,}751 * nvidia_{price} - 5.078{,}56 * yield3mUSAtrBill$$

Στατιστικός έλεγχος του μοντέλου

Ο στατιστικός έλεγχος του μοντέλου αποτίμησης της αξίας του Bitcoin, βασίστηκε στην μελέτη και σύγκριση των εξής στατιστικών μεγεθών:

- Τα p-values των ανεξάρτητων μεταβλητών.
- Το adjusted R^2 του μοντέλου.
- Τον πίνακα συσχετίσεων των ανεξάρτητων μεταβλητών.
- Τον έλεγχο "Durbin-Watson", για τα υπολείμματα του μοντέλου.

Για να θεωρείται μια ανεξάρτητη μεταβλητή ή ο σταθερός όρος ενός γραμμικού μοντέλου παλινδρόμησης στατιστικά σημαντικός, θα πρέπει το p-value του να παίρνει τιμές μικρότερες του 0.05, όταν αναφερόμαστε στο σύνηθες διάστημα εμπιστοσύνης του 95%. Τα αποτελέσματα για το συγκεκριμένο μοντέλο παρουσιάζονται στον παρακάτω πίνακα.

Πίνακας 11: Τα p-values των ανεξάρτητων μεταβλητών και του σταθερού όρου (ημερήσιο μοντέλο)

Σταθερός όρος / Ανεξάρτητες μεταβλητές	*p-value (95%)*
Σταθερός όρος	$9{,}23 * e^{-23}$
Αργό πετρέλαιο	$2{,}87 * e^{-41}$
Παλλάδιο	$8{,}16 * e^{-31}$
S&P 500	$2{,}88 * e^{-8}$
Euro Index	$1{,}90 * e^{-33}$
Nvidia	$2{,}47 * e^{-96}$
Έντοκο γραμμάτιο Η.Π.Α. (3 μηνών)	$8{,}38 * e^{-35}$

Όλες οι ανεξάρτητες μεταβλητές και ο σταθερός όρος παρουσιάζουν ιδιαίτερα μικρές τιμές στο p-value, οπότε όλες θεωρούνται ιδιαίτερα στατιστικά σημαντικές. Ωστόσο παρατηρείται ότι από τα επιλεγμένα στοιχεία η λιγότερο στατιστικά σημαντική ανεξάρτητη μεταβλητή και με αρκετή σχετικά διαφορά είναι ο δείκτης S&P 500.

Ο συντελεστής R^2 υπολογίζει το ποσοστό της μεταβλητότητας της εξαρτημένης μεταβλητής την οποία εξηγεί το μοντέλο. Σε περιπτώσεις που οι ανεξάρτητες μεταβλητές είναι περισσότερες από μια ο συντελεστής adjusted R^2 είναι καταλληλότερος για μελέτη, καθώς προσαρμόζει τα αποτελέσματα των μετρήσεων με τον αριθμό των ανεξάρτητων μεταβλητών. Στην επιστήμη της στατιστικής δεν υπάρχει ένα επίπεδο ικανοποιητικής τιμής για τον συγκεκριμένο συντελεστή καθώς εξαρτάται από το είδος και την μορφολογία των δεδομένων. Ωστόσο όταν αναφερόμαστε σε ίδιου είδους δεδομένα ένα μοντέλο με μεγαλύτερο adjusted R^2 θεωρείται καλύτερο. Οι έγκυρες τιμές του συντελεστή βρίσκονται στο διάστημα 0 έως +1. Για το μοντέλο της

εργασίας οι τιμές των συντελεστών R^2 και Adjusted R^2 παρουσιάζονται στον παρακάτω πίνακα.

Πίνακας 12: Οι τιμές R^2 και adjusted R^2 του ημερήσιου μοντέλου

R^2	Adjusted R^2
0,833156	0,832605

Οι τιμές των συντελεστών μπορούν να θεωρηθούν ιδιαίτερα ικανοποιητικές, καθώς σχεδόν το 84% της μεταβλητότητας της τιμής του Bitcoin μπορεί να εξηγηθεί από το μοντέλο. Γεγονός που τονίζει την ποιότητα του μοντέλου, καθώς αναφερόμαστε σε ένα επενδυτικό προϊόν το οποίο χαρακτηρίζεται από έντονη μεταβλητότητα και αστάθεια της τιμής του.

Οι ανεξάρτητες μεταβλητές ενός μοντέλου γραμμικής παλινδρόμησης θα πρέπει να μην συσχετίζονται αναμεταξύ τους. Με σκοπό οι μεταβολές μιας ανεξάρτητης μεταβλητής να μην επηρεάζουν τις υπόλοιπες ανεξάρτητες μεταβλητές αλλά μόνο την εξαρτημένη μεταβλητή του μοντέλου. Για να ελεγχθούν τα επίπεδα συσχέτισης δημιουργήθηκε ο πίνακας συσχετίσεων των ανεξάρτητων μεταβλητών του μοντέλου. (βλέπε προσάρτημα σελίδα 97)

Ο υπολογισμός των συσχετίσεων πραγματοποιείται με την χρήση του συντελεστή Peatson’s r και οι τιμές σε όλον τον πίνακα, σε απόλυτο βαθμό, είναι μικρότερες του 0,05. Ικανοποιητικό αποτέλεσμα καθώς παρατηρούνται επίπεδα ιδιαίτερα χαμηλής συσχέτισης μεταξύ των ανεξάρτητων μεταβλητών.

Ο έλεγχος των Durbin-Watson εξετάζει, σε μοντέλα παλινδρόμησης βασισμένα σε δεδομένα χρονικών σειρών, όπως αυτό που υλοποιήθηκε στο πλαίσιο της συγκεκριμένης εργασίας, το βαθμό αυτοσυσχέτισης των καταλοίπων του μοντέλου. Όσο χαμηλότερο είναι το αποτέλεσμα στο συγκεκριμένο έλεγχο τόσο μεγαλύτερη είναι η αυτοσυσχέτιση των καταλοίπων. Στην ιδεατή περίπτωση το αποτέλεσμα πρέπει να βρίσκεται κοντά στο 2, ώστε να εκλείπει η αυτοσυσχέτιση των καταλοίπων από το μοντέλο.

Το αποτέλεσμα του μοντέλου της παρούσης εργασίας στον έλεγχο των Durbin-Watson ήταν 0,0516. Η τιμή βρίσκεται μακριά από το ιδεατό επίπεδο του 2 και υποδηλώνει αυτοσυσχέτιση των καταλοίπων του μοντέλου.

Για να μπορέσει να μελετηθεί η αιτία της χαμηλής τιμής του μοντέλου στον έλεγχο Durbin-Watson, αποθηκεύτηκαν τα κατάλοιπα σε μια νέα μεταβλητή και απεικονίστηκαν σε γραφική παράσταση ως προς τον χρόνο.

Εικόνα 17: Γραφική παράσταση των καταλοίπων του μοντέλου

Από το διάγραμμα γίνεται εμφανές ότι τα πρώτα χρόνια της ανάλυσης, δηλαδή μέχρι τα μέσα του 2017 τα κατάλοιπα του μοντέλου είναι περιορισμένα. Προσδίδοντας στο μοντέλο ένα ικανοποιητικό αποτέλεσμα προβλεπτικής ικανότητας. Ωστόσο από τα μέσα του 2017 και κυρίως την χρονική περίοδο από τα τέλη του 2017 έως και τους πρώτους μήνες του 2018, τα κατάλοιπα αυξάνονται έντονα και η προβλεπτική ικανότητα του μοντέλου περιορίζεται. Η αλλαγή στην συμπεριφορά των καταλοίπων συμβαδίζει με την ραγδαία διάδοση του Bitcoin, κατά την ίδια χρονική περίοδο, λόγω της ενασχόλησης των μέσων μαζικής ενημέρωσης και του αυξημένου ενδιαφέροντος του επενδυτικού κοινού.

Στην συγκεκριμένη περίοδο οι μεταβολές της τιμής του Bitcoin ακόμη και σε καθημερινή κλίμακα ήταν τεράστιες. Για παράδειγμα στο διάστημα από τις *06/12/2017* έως τις *08/12/2017*, η τιμή του Bitcoin αυξήθηκε κατά *40%*. Μεταβολές τέτοιου επιπέδου σε τόσο σύντομο χρονικό διάστημα δεν μπορούν να προβλεφθούν από κάποιο μοντέλο πρόβλεψης και δη γραμμικό. Ενώ ταυτόχρονα η πορεία της παγκόσμιας οικονομίας παρέμενε σε σταθερά επίπεδα χωρίς να υπάρχουν ενδείξεις για ακραίες μεταβολές στις τιμές των ανεξάρτητων μεταβλητών του μοντέλου.

Για την αντιμετώπιση του φαινομένου εκτελέστηκε η διαδικασία AR(1) για χρονοσειρές, με την μέθοδο των Cochrane-Orcutt. Ωστόσο το αποτέλεσμα δεν κρίθηκε ικανοποιητικό διότι μπορεί το αποτέλεσμα στον έλεγχο των Durbin-Watson να άγγιζε το 1,87 αλλά οι στατιστικά σημαντικές μεταβλητές του μοντέλου ήταν μόλις δύο, η Nvidia και το έντοκο γραμμάτιο των Η.Π.Α (3 μηνών). Ο έλεγχος Dickey-Fuller για την μεταβλητή των καταλοίπων, με βάση το κριτήριο AIC, είχε ως αποτέλεσμα ότι η υπόθεση για έλλειψη στατικότητας δεν μπορεί να απορριφθεί.

Μοντέλο μηνιαίων τιμών

Με σκοπό την πραγματοποίηση ελέγχου ευρωστίας του μοντέλου, μελετήθηκε και το γραμμικό μοντέλο παλινδρόμησης το οποίο βασίζεται σε μηνιαίες τιμές των ίδιων ανεξάρτητων μεταβλητών. Η μελέτη βασίστηκε στην ίδια χρονική περίοδο, των πέντε ετών δηλαδή των 60 παρατηρήσεων. Για την ανάλυση των ανεξάρτητων μεταβλητών, όπως και στην περίπτωση του ημερήσιου μοντέλου, χρησιμοποιήθηκε χρονική υστέρηση μιας περιόδου. Τα στατιστικά αποτελέσματα της παλινδρόμησης για το μηνιαίο μοντέλο παρουσιάζονται στην συνέχεια.

Πίνακας 13: Τα p-values των ανεξάρτητων μεταβλητών και του σταθερού όρου (μηνιαίο μοντέλο)

Σταθερός όρος / Ανεξάρτητες μεταβλητές	*p-value (95%)*
Σταθερός όρος	0,0049
Αργό πετρέλαιο	0,0051
Παλλάδιο	0,2742
S&P 500	0,9272
Euro Index	0,0004
Nvidia	0,0002
Έντοκο γραμμάτιο Η.Π.Α. (3 μηνών)	0,0264

Με βάση τις τιμές p-value των ανεξάρτητων μεταβλητών και του σταθερού όρου, για το μοντέλο των μηνιαίων τιμών, το παλλάδιο και ο δείκτης S&P 500 δεν αποτελούν στατιστικά σημαντικές μεταβλητές, εν αντιθέσει με το μοντέλο ημερήσιων τιμών. Οι τιμές p-value αναφέρονται σε διάστημα εμπιστοσύνης 95%.

Πίνακας 14: Τα σημαντικότερα στατιστικά στοιχεία (μηνιαίο μοντέλο)

R^2	Adjusted R^2	Durbin-Watson
0,86893	0,85409	0,92956

Αντίστοιχα, με το μοντέλο ημερήσιων τιμών, οι συντελεστές R^2 και προσαρμοσμένο R^2, παραμένουν σε υψηλά επίπεδα. Τονίζοντας ότι και το μηνιαίο μοντέλο γραμμικής παλινδρόμησης καταφέρνει να εξηγεί μεγάλο ποσοστό της μεταβλητότητας της

εξαρτημένης μεταβλητής του. Ωστόσο η μεγαλύτερη διαφορά ανάμεσα στο ημερήσιο και το μηνιαίο μοντέλο είναι η αυξημένη τιμή του μηνιαίου μοντέλου στον έλεγχο των Durbin-Watson. Καθώς πλησιάζει την μονάδα, αρκετές τάξεις μεγέθους μεγαλύτερη σε σχέση την αντίστοιχη τιμή του ημερήσιου μοντέλου. Γεγονός το οποίο μπορεί να δικαιολογηθεί από τον μικρότερο αριθμό παρατηρήσεων. Διότι οι 60 παρατηρήσεις του μηνιαίου μοντέλου, μειώνουν τον αριθμό των καταλοίπων που παρουσιάζουν αυξημένες τιμές και ταυτόχρονα την έκθεση του μηνιαίου μοντέλου στο ζήτημα των έντονων μεταβολών που παρουσίασε το Bitcoin τον τελευταίο χρόνο. Λόγω της σχεδόν ικανοποιητικής τιμής στον έλεγχο των Durbin-Watson, το μηνιαίο μοντέλο παρουσιάζει μικρότερο ελάττωμα, όσον αφορά τα κατάλοιπά του.

Συμπεράσματα, Περιορισμοί Μελέτης και Προτάσεις

Το Bitcoin και τα κρυπτονομίσματα γενικότερα, έχουν καταφέρει να δημιουργήσουν έναν επιστημονικό κλάδο, ο οποίος τοποθετείται ανάμεσα στις επιστήμες των Οικονομικών και της Πληροφορικής. Ο τομέας μπορεί να βρίσκεται ακόμη σε πρώιμο στάδιο και τα στοιχεία του να μην έχουν φτάσει σε σημείο πλήρους ωριμότητας, ωστόσο η πρόοδος της τεχνολογίας και η αύξηση της εξάρτησης της καθημερινότητας των ανθρώπων από τεχνολογικά προϊόντα πάσης φύσεως, εγγυάται ότι ο συγκεκριμένος τομέας θα διογκώνεται, ενώ ταυτόχρονα όλο και περισσότερα στοιχεία του θα κεντρίζουν το ενδιαφέρον της επιστημονικής κοινότητας αλλά και των επενδυτών.

Οι υποθέσεις και οι θεωρητικές προβλέψεις είναι χρήσιμες αλλά χρησιμότερα αποδεικνύονται τα απτά συμπεράσματα. Για τον λόγο αυτό στην συνέχεια περιγράφονται τα βασικά συμπεράσματα και οι προτάσεις για μελλοντικές έρευνες, βασισμένα πάντα στην κεντρική δομή της παρούσης εργασίας.

Συμπεράσματα

Αρχικά η μελέτη επικεντρώθηκε στα τεχνικά χαρακτηριστικά του Bitcoin. Συνθέτοντας μια γενική εικόνα, από προγραμματιστικής άποψης το πρωτόκολλο του Bitcoin δεν είναι ιδιαίτερα πολύπλοκο, ωστόσο συνδυάζει με άψογο τρόπο μεθόδους και τεχνολογίες που για πρώτη φορά χρησιμοποιήθηκαν στο πλαίσιο ενός ηλεκτρονικού νομίσματος. Αντίστοιχα ο “ελεύθερος-ανοιχτός” χαρακτήρας της διανομής του κώδικά του, εμφάνισε πολύ σημαντικά πλεονεκτήματα. Καθώς έχει δημιουργηθεί μια ενεργή κοινότητα η οποία υποστηρίζει το κρυπτονόμισμα και συνεχώς προτείνει και εφαρμόζει αλλαγές οι οποίες βελτιώνουν την απόδοσή του. Ενώ ταυτόχρονα έχουν δημιουργηθεί αμέτρητα κρυπτονομίσματα τα οποία βασίζονται στις λειτουργίες και τις τεχνικές του Bitcoin. Όλα μαζί έχουν καταφέρει να σχηματίσουν μια κοινή αγορά με παγκόσμια απήχηση.

Όσον αφορά το δίκτυο του Bitcoin αποδεικνύεται πως μια κεντρική αρχή διαχείρισης ενός ηλεκτρονικού μέσου συναλλαγής δεν είναι απαραίτητη και ότι ένα αποκεντρωμένο ηλεκτρονικό νόμισμα μπορεί να λειτουργήσει χωρίς προβλήματα. Η peer-to-peer αρχιτεκτονική που χρησιμοποιείται φανερώνει την έννοια της ισότητας, ωστόσο δεν είναι κάτι νέο καθώς χρησιμοποιείται από διάφορες διαδικτυακές υπηρεσίες.

Η επαναστατική πρωτοτυπία που εισήγαγε η διάδοση του Bitcoin, ήταν σίγουρα η τεχνολογία της Blockchain. Μια τεχνολογία με την χρήση της οποίας υλοποιούνται οι συναλλαγές του κρυπτονομίσματος. Η Blockchain λειτουργεί σε ένα περιβάλλον απόλυτης έλλειψης εμπιστοσύνης. Χωρίς να υπάρχει κεντρική αρχή η οποία να επιβεβαιώνει τις συναλλαγές, καταφέρνει να υποστηρίζει την λειτουργία ενός ηλεκτρονικού νομίσματος, κάνοντας χρήση εξελιγμένων δομών κρυπτογράφησης, οι οποίες επιπρόσθετα προστατεύουν το κρυπτονόμισμα από κακόβουλους χρήστες. Συμμετοχή της συγκεκριμένης τεχνολογίας μελετάται ήδη σε διάφορους τομείς και σε πληθώρα εφαρμογών. Καθώς έχει την δυνατότητα να εξελίξει την λειτουργία και να αυξήσει σημαντικά τις δυνατότητες των ολοκληρωμένων συστημάτων διαχείρισης.

Σημαντικό ρόλο στο οικοσύστημα του Bitcoin διαδραματίζει η διαδικασία της εξόρυξης. Η εξόρυξη διασφαλίζει την απρόσκοπτη και χωρίς κινδύνους λειτουργία του Bitcoin, ενώ ταυτόχρονα αποτελεί την μέθοδο προσφοράς χρήματος στην οικονομία του. Είναι μια ιδιαίτερα απαιτητική, ως προς την χρήση υπολογιστικών πόρων, διαδικασία. Ωστόσο αποτελεί την βέλτιστη μέθοδο για να διασφαλιστεί η λειτουργία ενός ηλεκτρονικού νομίσματος. Ο εξοπλισμός εξόρυξης αποτελείται από ειδικά σχεδιασμένα μηχανήματα, τα οποία προσφέρουν υψηλά επίπεδα απόδοσης αλλά μπορούν να χρησιμοποιηθούν μόνο σε περιορισμένες κατηγορίες προβλημάτων.

Στο κεφάλαιο της οικονομικής παρουσίασης αρχικά υπήρξε ανάλυση του Bitcoin ως προς τις τρεις λειτουργίες του Mankiw οι οποίες χαρακτηρίζουν ένα νόμισμα. Παρατηρήθηκε ότι το Bitcoin δεν καλύπτει πλήρως όλα τα κριτήρια. Ωστόσο το γεγονός αυτό μπορεί να οφείλεται στο ότι τα κρυπτονομίσματα έχουν δημιουργήσει νέα δεδομένα και απαιτήσεις στον τομέα των ηλεκτρονικών νομισμάτων. Καθώς διαφέρουν παρασάγγας από τις περιπτώσεις τις οποίες μελέτησαν οι οικονομολόγοι για να συντάξουν τις σύγχρονες θεωρίες της επιστήμης των οικονομικών.

Το στοιχείο που διαφοροποιεί το Bitcoin από τα υπόλοιπα νομίσματα, είναι η έλλειψη κεντρικής αρχής. Χωρίς κεντρική αρχή την προσφορά χρήματος στην οικονομία καθορίζουν συγκεκριμένοι και δεδομένοι κανόνες. Το Bitcoin χαρακτηρίζεται από σταθερά φθίνουσα προσφορά χρήματος, γεγονός το οποίο δημιουργεί αποπληθωριστικές τάσεις. Το στοίχημα του Bitcoin είναι, με βάση έναν μακροχρόνιο ορίζοντα, αν σε μια οικονομία που βασίζεται σε αυτό, μπορούν να συνδυαστούν αποπληθωριστικές τάσεις ταυτόχρονα με θετικούς ρυθμούς ανάπτυξης.

Η διάδοση των κρυπτονομισμάτων οδήγησε στην ανάπτυξη μιας νέας μεθόδου χρηματοδότησης φιλόδοξων σχεδίων. Τα επονομαζόμενα ICOs (Initial Coin Offerings). Τα ICOs επί της ουσίας είναι μια διαδικασία ανταλλαγής tokens έναντι κάποιου χρηματικού αντιτίμου, ώστε να μπορέσει να χρηματοδοτηθεί ένα φιλόδοξο σχέδιο. Σε περίπτωση επιτυχημένης υλοποίησης του σχεδίου τα tokens αποκτούν μεγαλύτερη αξία, ενώ στην περίπτωση που δεν υλοποιηθεί ανταλλάσσονται ξανά, έναντι προσυμφωνημένου αντιτίμου. Φυσικά η έλλειψη ενός κοινά αποδεκτού ρυθμιστικού πλαισίου από σχεδόν όλα τα κράτη του κόσμου δημιουργεί προβλήματα στην περαιτέρω διάδοση των κρυπτονομισμάτων και στην υλοποίηση επιτυχημένων ICOs. Καθώς οι εκάστοτε κυβερνήσεις λειτουργούν ανάλογα με τα προσωπικά τους συμφέροντα.

Όσον αφορά τον τομέα της ασφάλειας, ιδιαίτερο ζήτημα αποτελούν οι κυβερνοεπιθέσεις σε ανταλλακτήρια και σε εταιρείες διαχείρισης online πορτοφολιών. Καθώς στην περίπτωση που στεφθούν με επιτυχία και δημοσιευτούν στον τύπο επηρεάζουν έντονα την τιμή του Bitcoin. Γεγονός το οποίο αποτελεί λανθασμένη αντίδραση των επενδυτών διότι μια επιτυχημένη κυβερνοεπίθεση φανερώνει την αδυναμία των ιδιωτικών εταιρειών σε θέματα ασφαλείας και όχι ένα πιθανό κενό στο πρωτόκολλο του κρυπτονομίσματος.

Παρατηρώντας την αγορά κρυπτονομισμάτων γίνεται εύκολα κατανοητό ότι ενώ αποτελείται από μια μεγάλη πληθώρα εναλλακτικών κρυπτονομισμάτων, τα περισσότερα εξ' αυτών επηρεάζονται έντονα από την πορεία του Bitcoin και λιγότερο από άλλους εξωγενείς παράγοντες. Για τον λόγο αυτόν, με βάση την δεδομένη κατάσταση στην αγορά κρυπτονομισμάτων, η ενασχόληση με το Bitcoin διατηρεί καλύτερο θεωρητικό και πρακτικό υπόβαθρο σε σχέση με οποιοδήποτε άλλο κρυπτονόμισμα.

Με βάση την μελέτη συσχετίσεων που πραγματοποιήθηκε ανάμεσα στο Bitcoin και σε 17 άλλα χρηματοοικονομικά προϊόντα παρατηρήθηκαν, ως γενική εικόνα, μικρά αριθμητικά επίπεδα συσχέτισης, τα οποία κυρίως οφείλονται στις ιδιαίτερα έντονες μεταβολές της τιμής του κρυπτονομίσματος και στην εμφάνιση κυκλικής συμπεριφοράς. Έντονη άνοδος από τα τέλη του 2017 έως και τους πρώτους μήνες του 2018, την οποία ακολούθησε έντονη πτώση μέχρι και τις αρχές του καλοκαιριού του 2018. Ωστόσο ανά περιόδους εμφανίστηκαν συσχετίσεις αναλογικά αυξημένες, οι οποίες βοήθησαν στην υλοποίηση της έρευνας. Στην περίπτωση του δείκτη EPU,

καταγράφηκαν ενθαρρυντικά αποτελέσματα καθώς τα αριθμητικά επίπεδα συσχέτισης αυξήθηκαν σημαντικά. Ωστόσο ο δείκτης EPU δεν χρησιμοποιήθηκε στο τελικό μοντέλο αποτίμησης της αξίας του κρυπτονομίσματος.

Όσον αφορά το μοντέλο αποτίμησης της αξίας του Bitcoin, θεσπίστηκαν συγκεκριμένοι κανόνες επιλογής των ανεξάρτητων μεταβλητών και χρησιμοποιήθηκε η ανάλυση παλινδρόμησης βασισμένη στην μέθοδο ελαχίστων τετραγώνων. Το τελικό μοντέλο διαθέτει έξι ανεξάρτητες μεταβλητές. Το αργό πετρέλαιο, το παλλάδιο, τον δείκτη S&P 500, τον δείκτη EuroIndex, την Nvidia και την απόδοση του έντοκου γραμματίου των Η.Π.Α. διάρκειας 3 μηνών. Τα στατιστικά στοιχεία του μοντέλου κρίνονται ικανοποιητικά αν αναλογιστεί κανείς τις ιδιαιτερότητες της πορείας της τιμής του Bitcoin, οι οποίες δυσκολεύουν την διαδικασία της ανάλυσής του και την προσπάθεια για την δημιουργία ικανοποιητικών μοντέλων πρόβλεψης. Ενώ για λόγους ελέγχου ευρωστίας υλοποιήθηκε και το αντίστοιχο μοντέλο που αναφέρεται σε μηνιαίες τιμές δεδομένων.

Περιορισμοί / Αδυναμίες Μελέτης

Τα κρυπτονομίσματα γενικότερα και ειδικότερα ο κύριος εκπρόσωπός τους, το Bitcoin, βρίσκονται στην αιχμή των οικονομικών και τεχνολογικών εξελίξεων. Υποδηλώνοντας ότι μια μικρή μεταβολή του περιβάλλοντος, είτε αυτό είναι οικονομικό είτε τεχνολογικό, μπορεί να ακυρώσει βασικές αρχές και δεδομένα στα οποία βασίστηκε η συγγραφή της παρούσης εργασίας. Επηρεάζοντας με αυτό τον τρόπο την διαδικασία εξαγωγής των τελικών συμπερασμάτων. Ταυτόχρονα η περαιτέρω μελέτη και κατανόηση των εξελίξεων του τεχνολογικού περιβάλλοντος απαιτεί επιπρόσθετες και εξειδικευμένες γνώσεις της επιστήμης των υπολογιστών. Καθώς το Bitcoin αποτελεί μια οντότητα άρδην συνδεδεμένη με τον τομέα της πληροφορικής.

Αντίστοιχα, η οικονομική επιστήμη βασίζει την ανάλυση των χρηματοοικονομικών προϊόντων σε αρχές και κανόνες, τους οποίους έχουν θεσπίσει διακεκριμένοι επιστήμονες εδώ και αρκετά χρόνια. Ωστόσο η χρονική απόκλιση και τα ιδιαίτερα οικονομικά χαρακτηριστικά που παρουσιάζει το Bitcoin, παρατηρήθηκε ότι σε κάποιες περιπτώσεις δημιουργούν ασυμβατότητες ανάμεσα σε κοινά αποδεκτά αρχές και στα οικονομικά δεδομένα του κρυπτονομίσματος.

Όσον αφορά το τελευταίο κομμάτι της παρούσης εργασίας, το οποίο αναφέρεται στο μοντέλο αποτίμησης της αξίας του Bitcoin. Η έρευνα περιορίστηκε από το γεγονός ότι

η ανάλυση των χρηματοοικονομικών προϊόντων δεν πραγματοποιήθηκε με την χρήση εξειδικευμένων λογισμικών, τα οποία διαθέτουν χρηματιστηριακές εταιρείες και επενδυτικές τράπεζες, αλλά με την υλοποίηση αλγοριθμικών τεχνικών οι οποίες απαιτούν μια σχετικά χρονοβόρα και απαιτητική διαδικασία. Για τον λόγο αυτόν το πλήθος των προς μελέτη χρηματοοικονομικών προϊόντων άγγιξε τα 17 προϊόντα και όχι κάποιες εκατοντάδες.

Αδυναμία, επιπρόσθετα, μπορούν να χαρακτηριστούν οι περιορισμένες, αλλά πολύ έντονες, μεταβολές της τιμής του Bitcoin το τελευταίο χρονικό διάστημα, ακόμη και σε ημερήσιο επίπεδο. Καθώς τα πρότυπα τεχνικής ανάλυσης που χρησιμοποιήθηκαν στην παρούσα εργασία υστερούν στην διαχείριση ακραίων τιμών. Στην συνέχεια ακολουθούν προτάσεις για μελλοντικές έρευνες ή για περαιτέρω ανάλυση της παρούσης εργασίας, οι οποίες βασίζονται στους περιορισμούς και τις αδυναμίες της εν λόγω μελέτης.

Προτάσεις

Οι προτάσεις για μελλοντικές έρευνες κατατάσσονται σε κατηγορίες σύμφωνα με την δομή του κυρίως κειμένου.

Προτάσεις τεχνικής ανάλυσης:

- Να μελετηθεί για το αν μπορεί και με ποιον τρόπο να χρησιμοποιηθεί η τεχνολογία της Blockchain σε διαφορετικούς τεχνολογικούς τομείς και να προταθούν εφαρμογές της.
- Να μελετηθούν αναλυτικότερα οι νέες τεχνολογικές προσθήκες που βρίσκονται στο στάδιο διαβούλευσης από την κοινότητα του Bitcoin (sharding, lighting network, SegWit, αλγόριθμος της κατηγορίας Proof-of-Stake κ.α.) και να υπολογιστεί η επίδρασή τους στην αποδοτικότητα του κρυπτονομίσματος.
- Να ερευνηθούν πιθανά μειονεκτήματα της τεχνολογίας του Bitcoin, σε σχέση με άλλα συστήματα ηλεκτρονικών συναλλαγών.
- Να ερευνηθεί η σχεδόν μονοπωλιακή αγορά εξοπλισμού εξόρυξης Bitcoin και να αναλυθεί το κατά πόσο οι “miners” έχουν την δυνατότητα να χειραγωγούν την τιμή του Bitcoin στην διεθνή αγορά.

Προτάσεις οικονομικής ανάλυσης:

- Να μελετηθεί η δυνατότητα ύπαρξης μιας οικονομίας εξαρτημένης από κάποιο κρυπτονόμισμα, η οποία να συνδυάζει δεδομένη και φθίνουσα με την πάροδο των χρόνων προσφορά χρήματος.
- Να ερευνηθεί η περίπτωση της Βενεζουέλας και το κατά πόσο και με ποιον τρόπο το Petro μπορεί να βοηθήσει στην διάσωσή της.
- Να αναλυθούν τα επίπεδα ασφαλείας των ανταλλακτηρίων και των εταιρειών διαχείρισης online πορτοφολιών, με σκοπό να ανακαλυφθούν μειονεκτήματα και να αυξηθεί το επίπεδο προστασίας των χρηστών.
- Να μελετηθεί ποιος θα ήταν ο βέλτιστος τρόπος θέσπισης ενός κοινά αποδεκτού ρυθμιστικού πλαισίου σχετικά με τα κρυπτονομίσματα και τα ICOs.

Προτάσεις σχετικές με την διαδικασία ανάλυσης συσχετίσεων και με το μοντέλο αποτίμησης αξίας:

- Να χρησιμοποιηθούν στην ανάλυση συσχετίσεων διαφορετικοί συνδυασμοί χρηματοοικονομικών προϊόντων αλλά και διάφορων άλλων ειδικών δεικτών (π.χ. αριθμός ημερήσιων συναλλαγών Bitcoin, τα search rates της Google κ.α.)
- Να μελετηθούν οι συσχετίσεις με διαφορετικές χρονικές περιόδους σε σχέση με την παρούσα εργασία.
- Να μελετηθεί ένας διαφορετικός τρόπος διαχείρισης της κυκλικής συμπεριφοράς της τιμής του Bitcoin όσον αφορά το μοντέλο αποτίμησης της αξίας του.
- Να ερευνηθεί ένας συνδυασμός μοντέλων πρόβλεψης. Ένα για την περίοδο σχετικής σταθερότητας της τιμής του και ένα για την περίοδο έντονων μεταβολών.
- Να χρησιμοποιηθεί ανάλυση η οποία δεν βασίζεται σε γραμμικά μοντέλα παλινδρόμησης.

Κατάλογος Αναφορών

Άρθρα

Athey, S., Parashkevov, I., Sarukkai, V., & Xia, J. (2016, August 1). Bitcoin Pricing, Adoptiona and Usage: Theory and Evidence. σσ. 1-70.

Baker, S., Bloom, N., & Davis, S. (2016, March 10). Measuring Economic Policy Uncertainty. p. 79.

Catalini, C., & Gans, J. (2017). Some Simple Economics of the Blockchain. 1-32.

Graf, K. (2013). *On the origins of Bitcoin: Stages of monetary evolution.*

Graf, K. (2014, October 20). Commodity, scarcity and monetary value theory in light of Bitcoin. *Prices & Markets*.

Grinberg, R. (2011). Bitcoin: An Innovative Alternative Digital currency. *Hastings Science & Technology Law Journal*, 159-207.

Huberman, G., Leshno, J., & Moallemi, C. (2017). Monopoly without a monopolist: An Economic analysis of the bitcoin payment system. *Bank of Finland Research Discussion Papers*, 1-56.

Ma, J., Gans, J., & Tourky, R. (2018). Market Structure in Bitcoin Mining. 1-24.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. 1-9.

Ron, D., & Shamir, A. (2013). Quantitative Analysis of the Full Bitcoin Transaction Graph. *Financial Cryptography and Data Security*, σσ. 6-24.

Taylor, M. B. (2013). Bitcoin and The Age of Bespoke Silicon. *International Conference on Compilers, Architecture and Synthesis for Embedded Systems*, 1-10.

Βιβλία

Antonopoulos, A. (2017). *Masteting Bitcoin: Programming the Open Blockchain.* Sebastopol, California, USA: O' Reilly Media, Inc.

Asharaf, S., & Adarsh, S. (2017). *Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities.* Hershey, USA: IGI-Global.

Franco, P. (2015). *Understanding Bitcoin: Cryptography, engineering and economics.* Chichester, West Sussex, United Kingdom: John Wiley & Sons Ltd.

Mankiw, G. (2009). *Macroeconomics 7th Edition.* New York, USA: Worth Publishers.

Varian, H. (2003). *The Economics of Information Technology.*

Ηλεκτρονικές Πηγές

Asolo, B. (2018, July 29). *Merkle Tree & Merkle Root Explained*. Ανάκτηση August 1, 2018, από Mycryptopedia: https://www.mycryptopedia.com/merkle-tree-merkle-root-explained/

BitcoinWiki. (2013, January 8). Retrieved August 1, 2018, from Why a GPU mines faster than a CPU: https://en.bitcoin.it/wiki/Why_a_GPU_mines_faster_than_a_CPU

BitcoinWiki. (2016, May 15). Retrieved July 28, 2018, from Proof of Work: https://en.bitcoin.it/wiki/Proof_of_work

Blockgeeks: Guides. (2017). Retrieved August 2, 2018, from Blockchain Scalability: When, Where, How?: https://blockgeeks.com/guides/blockchain-scalability/

MasterTheCrypto. (2017, August 7). Retrieved June 25, 2018, from Coins, Tokens & Altcoins: What's the difference?: https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/

Helms, K. (2018, January 26). *news.bitcoin*. Retrieved August 4, 2018, from Russia Finalizes Federal Law on Cryptocurrency Regulation: https://news.bitcoin.com/russia-finalizes-federal-law-cryptocurrency-regulation/

Metcalf, T. (2018, May 9). *Bloomberg Articles*. Retrieved July 28, 2018, from The Wealthy Are Hoarding $10 Billion of Bitcoin on Bunkers: https://www.bloomberg.com/news/articles/2018-05-09/bunkers-for-the-wealthy-are-said-to-hoard-10-billion-of-bitcoin

Rooney, K. (2018, March 27). *CNBC*. Retrieved August 4, 2018, from Your guide to cryptocurrency regulations around the world and where they are headed: https://www.cnbc.com/2018/03/27/a-complete-guide-to-cyprocurrency-regulations-around-the-world.html

Tan, A., & Nakamura, Y. (2018, June 20). *Bloomberg Articles*. Retrieved July 29, 2018, from Cryptocurrency Markets Are Juicy Targets for Hackers: Timeline: https://www.bloomberg.com/news/articles/2018-06-20/cryptocurrency-markets-are-juicy-targets-for-hackers-timeline

Προσάρτημα

Πίνακας 15: Αποτελέσματα μελέτης συσχετίσεων (5 χρόνια)

Συνδιακυμάνσεις	*Bitcoin*	*Crude Oil*	*Palladium*	*Gold*	*S&P-500*	*Nasdaq-100*	*HangSeng-50*	*USD Index*	*Euro Index*	*Nvidia*	*Apple*	*Amazon*	*3m. US Tr. Bills*
Bitcoin	1	2,5718E-05	6,14532E-06	-9,51114E-06	4,60175E-05	3,73469E-05	1,67777E-06	1,55278E-05	2,84073E-06	-3,54604E-05	-2,13907E-05	-4,6304E-05	-7,30669E-05
Crude Oil		1	8,64841E-06	3,36553E-06	7,47691E-06	5,85375E-06	6,76255E-06	-2,19866E-06	-1,56917E-06	-1,0997E-05	-9,24553E-06	-3,4464E-06	-0,000144585
Palladium			1	-3,85512E-06	2,02277E-06	1,62051E-06	-8,05988E-06	2,05199E-06	1,35719E-06	1,81383E-05	1,30856E-05	6,0037E-06	-7,51444E-05
Gold				1	-1,41463E-06	-1,08647E-06	-5,27848E-06	3,21698E-07	9,27478E-07	5,97372E-06	-2,7111E-06	1,78984E-06	-9,48078E-05
S&P-500					1	8,77669E-05	2,57719E-06	6,52358E-07	6,46428E-07	-9,98333E-06	-1,09979E-06	2,58955E-06	-6,57276E-06
Nasdaq-100						1	2,16644E-06	6,46932E-07	9,28535E-07	-1,15067E-05	2,7888E-07	3,2801E-06	-4,37785E-05
HangSeng-50							1	-2,79084E-07	-8,33245E-07	-1,16859E-06	-3,27186E-06	-4,58359E-06	-3,72274E-06
USD Index								1	-7,24023E-07	2,77519E-06	-3,45596E-06	5,66181E-07	4,62683E-05
Euro Index									1	-7,3159E-07	1,88359E-06	1,93929E-06	1,39937E-05
Nvidia										1	0,000126073	0,000147281	-4,00924E-05
Apple											1	9,79224E-05	9,73707E-05
Amazon												1	4,04935E-05
3m. US Tr. Bills													1
Pearson R	*Bitcoin*	*Crude Oil*	*Palladium*	*Gold*	*S&P-500*	*Nasdaq-100*	*HangSeng-50*	*USD Index*	*Euro Index*	*Nvidia*	*Apple*	*Amazon*	*3m. US Tr. Bills*
Bitcoin	1	0,01883611	0,005709725	-0,014574832	0,07697184	0,054343757	0,002149229	0,051668822	0,011539878	-0,023333160	-0,020540011	-0,03643177	-0,004324558
Crude Oil		1	0,025467227	0,016345547	0,039637478	0,026996279	0,027455885	-0,023187450	-0,020203037	-0,022933907	-0,028137342	-0,008594150	-0,027121856
Palladium			1	-0,023751983	0,013603374	0,009480646	-0,041511573	0,027452666	0,022166783	0,047986397	0,050519823	0,018992062	-0,017881694
Gold				1	-0,015690694	-0,010483417	-0,044838428	0,007098368	0,024984241	0,026065485	-0,017262909	0,009338313	-0,037209759
S&P-500					1	0,924389235	0,023896080	0,015712129	0,019007307	-0,047548277	-0,007643933	0,014747446	-0,002815780
Nasdaq-100						1	0,017474811	0,013554804	0,023751120	-0,047675614	0,001686201	0,016250434	-0,016315374
HangSeng-50							1	-0,005147839	-0,018763508	-0,004262481	-0,017415709	-0,019991167	-0,001221390
USD Index								1	-0,042350943	0,026294296	-0,047784243	0,006414420	0,039431582
Euro Index									1	-0,008462299	0,031794564	0,026822310	0,014559455
Nvidia										1	0,344706844	0,329957880	-0,006756687
Apple											1	0,320140699	0,023946730
Amazon												1	0,008159981
3m. US Tr. Bills													1

Πίνακας 16: Αποτελέσματα μελέτης συσχετίσεων (1 χρόνος)

Συνδιακυμάνσεις	*Bitcoin*	*Crude Oil*	*Palladium*	*Gold*	*S&P-500*	*Nasdaq-100*	*HangSeng-50*	*Europe-50*	*USD Index*	*Euro Index*	*Nvidia*	*Apple*	*Amazon*	*Ethereum*	*XRP*	*EOS*	*3m. US Tr. Bills*
Bitcoin	1	6,59567E-06	1,97683E-05	-1,7008E-06	1,92716E-05	1,27491E-05	-1,05837E-05	2,05956E-06	6,858E-06	5,78254E-06	-4,00816E-05	-5,15459E-07	-5,57939E-06	0,000131838	0,000116239	2,38568E-05	-1,88525E-05
Crude Oil		1	-4,19685E-06	-1,03626E-07	1,67176E-06	7,79354E-06	2,77186E-06	1,06348E-06	-5,2808E-07	-2,04394E-06	3,06348E-05	-8,64583E-06	4,15708E-06	3,02111E-05	0,000104297	9,57987E-05	-3,72715E-06
Palladium			1	3,00671E-06	2,54345E-06	4,06913E-06	-1,75231E-06	4,67445E-06	-2,03902E-06	1,4832E-06	3,20328E-05	1,85305E-05	4,97763E-06	-5,32198E-05	1,18703E-05	-7,14909E-05	2,25053E-05
Gold				1	-1,22845E-06	-7,58535E-07	3,14326E-06	1,68726E-06	1,25257E-06	2,41042E-07	1,02668E-05	5,8756E-06	2,55499E-06	-1,2575E-05	3,55183E-05	5,10648E-05	-1,15743E-05
S&P-500					1	5,89585E-05	8,66197E-07	-2,92446E-06	-2,35687E-06	2,86797E-07	-1,73001E-05	-7,28091E-06	-8,55082E-07	8,00731E-06	2,8013E-05	8,31528E-06	-2,41227E-06
Nasdaq-100						1	1,80568E-06	-4,52527E-06	-1,53994E-06	2,37009E-07	-1,52047E-05	-6,29652E-06	1,08165E-06	-1,48006E-05	1,95491E-05	5,35618E-07	2,91291E-07
HangSeng-50							1	-2,02174E-06	-2,8114E-07	-4,74272E-07	1,48863E-05	-5,26373E-07	-6,84787E-07	3,12868E-05	3,6144E-06	4,89428E-05	1,21674E-05
Europe-50								1	-1,42816E-06	-2,59574E-08	3,67907E-06	7,15686E-06	-1,03667E-06	1,23067E-05	1,17892E-05	-4,90199E-05	-7,94351E-06
USD Index									1	-2,07865E-08	1,7747E-06	-9,52474E-07	-1,65104E-06	1,31296E-06	-1,14451E-05	1,03153E-05	-9,65094E-07
Euro Index										1	-3,04236E-06	4,36743E-06	1,51711E-06	-3,34121E-06	1,11542E-05	-5,33484E-06	-2,27613E-06
Nvidia											1	0,000144328	0,000168037	-6,60206E-05	1,79985E-05	4,81691E-06	4,45824E-05
Apple												1	9,52378E-05	1,64455E-05	4,64626E-06	-4,26445E-05	1,12973E-05
Amazon													1	-1,21649E-05	7,95777E-05	-0,000101168	4,47998E-06
Ethereum														1	0,003242044	0,003851948	9,08849E-05
XRP															1	0,00419141	0,000122193
EOS																1	0,000142260
3m. US Tr. Bills																	1

Pearson R	*Bitcoin*	*Crude Oil*	*Palladium*	*Gold*	*S&P-500*	*Nasdaq-100*	*HangSeng-50*	*Europe-50*	*USD Index*	*Euro Index*	*Nvidia*	*Apple*	*Amazon*	*Ethereum*	*XRP*	*EOS*	*3m. US Tr. Bills*
Bitcoin	1	0,007674841	0,026541977	-0,005104406	0,050668052	0,025127269	-0,020606021	0,006002718	0,033825040	0,036359228	-0,029174070	-0,000739617	-0,006901763	0,038979392	0,024964698	0,004526792	-0,016807078
Crude Oil		1	-0,019366514	-0,001068868	0,01510616	0,052791560	0,018547754	0,010652897	-0,008951672	-0,044170076	0,076635482	-0,042636601	0,017673628	0,030698908	0,076985441	0,062474324	-0,011419946
Palladium			1	0,035785043	0,026518984	0,031804280	-0,013529656	0,054028450	-0,039882303	0,036983924	0,092462208	0,105443107	0,024418214	-0,062399990	0,010110022	-0,053795597	0,079565806
Gold				1	-0,028629869	-0,013252194	0,054248014	0,043591573	0,054763139	0,013434879	0,066242129	0,074732763	0,028016189	-0,032956933	0,067619612	0,085890596	-0,091467196
S&P-500					1	0,902363065	0,013096126	-0,066189517	-0,090270450	0,014003595	-0,097784086	-0,081127320	-0,008213912	0,018384387	0,046720006	0,012252495	-0,016700080
Nasdaq-100						1	0,020465213	-0,076778295	-0,044214500	0,008675220	-0,064424252	-0,052593532	0,007788998	-0,025473697	0,024441125	0,000591634	0,001511715
HangSeng-50							1	-0,033885131	-0,007973960	-0,017148786	0,062308577	-0,004343268	-0,004871236	0,053194379	0,004463963	0,053404514	0,062377986
Europe-50								1	-0,060638035	-0,001405028	0,023052439	0,088402084	-0,011039295	0,031323059	0,021796507	-0,080071558	-0,060962581
USD Index									1	-0,001904019	0,018817902	-0,019909474	-0,029752517	0,005655079	-0,035808517	0,028513642	-0,012533931
Euro Index										1	-0,041125470	0,116382482	0,034852890	-0,018346234	0,044490073	-0,018799624	-0,037685171
Nvidia											1	0,445212278	0,446871478	-0,041964094	0,008310273	0,001964952	0,085446084
Apple												1	0,499285396	0,020606625	0,004229052	-0,034293183	0,042683938
Amazon													1	-0,013141067	0,062444235	-0,070136950	0,014592376
Ethereum														1	0,608050965	0,638272190	0,070755829
XRP															1	0,504505581	0,069102985
EOS																1	0,071078488
3m. US Tr. Bills																	1

Πίνακας 17: Αποτελέσματα μελέτης συσχετίσεων (εξάμηνο ανόδου)

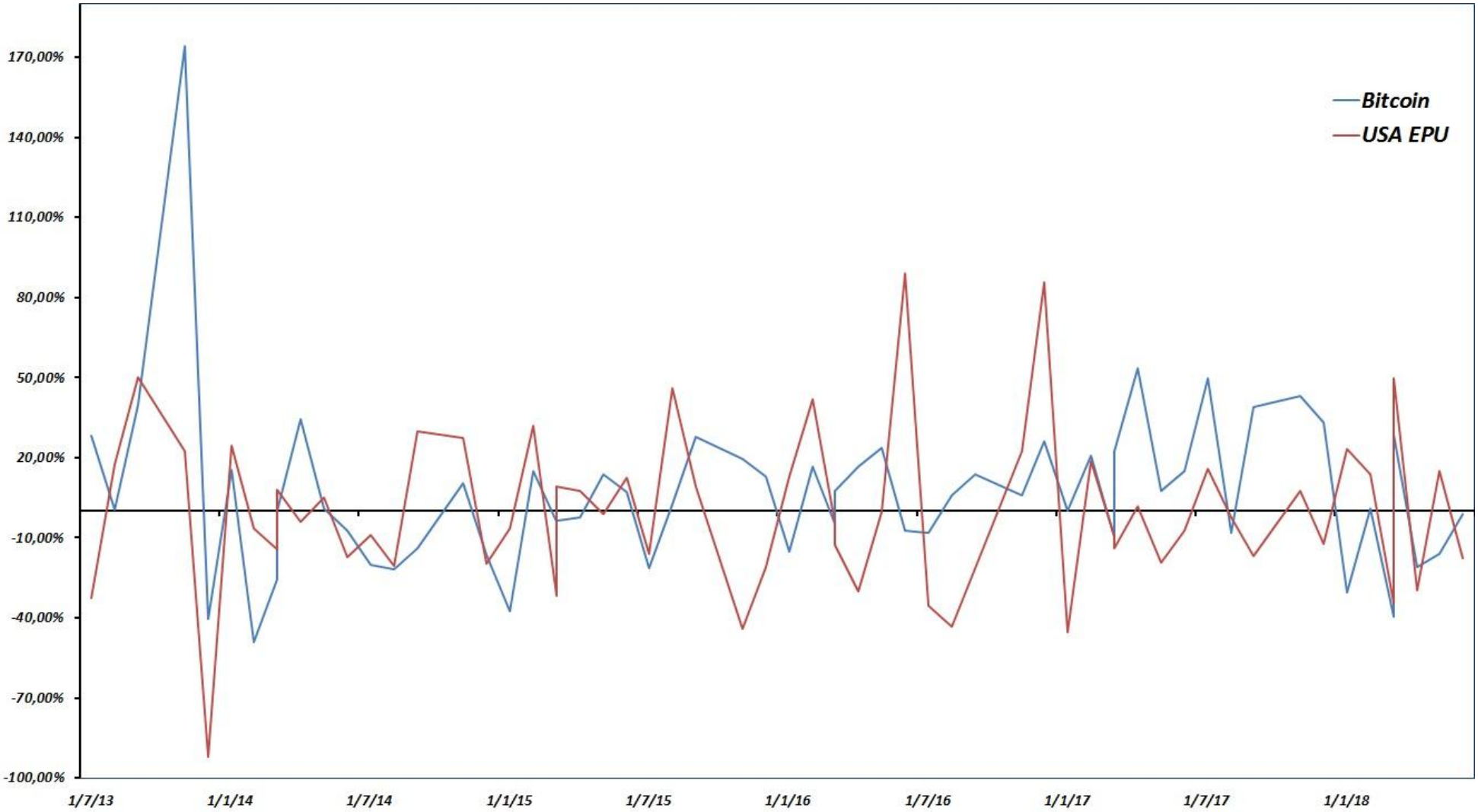
Συνδιακυμάνσεις	*Bitcoin*	*Crude Oil*	*Palladium*	*Gold*	*S&P-500*	*Nasdaq-100*	*HangSeng-50*	*Europe-50*	*USD Index*	*Euro Index*	*Nvidia*	*Apple*	*Amazon*	*Ethereum*	*XRP*	*EOS*	*3m. US Tr. Bills*
Bitcoin	1	6,11579E-05	3,86109E-05	5,53264E-06	5,76283E-06	3,74893E-05	-5,87825E-06	-1,39773E-05	2,68108E-05	5,59391E-06	2,90975E-05	3,034E-05	8,71474E-06	6,98842E-05	-4,87944E-05	2,55197E-05	9,31851E-05
Crude Oil		1	2,0887E-06	1,17119E-05	-1,69692E-06	5,96367E-06	3,32505E-06	3,12181E-06	1,22044E-06	-3,82795E-06	5,07065E-05	8,23979E-06	1,23967E-05	8,15258E-05	0,000274903	0,000270612	-1,35414E-05
Palladium			1	-1,91115E-06	3,77241E-06	6,59154E-06	-1,10672E-05	-4,85654E-06	-2,20862E-06	2,87779E-06	4,79055E-05	2,75386E-05	2,3866E-05	-8,79561E-05	7,78965E-06	-9,7894E-05	2,83909E-05
Gold				1	-8,77986E-07	-1,92598E-06	5,22302E-06	-2,26115E-06	1,1336E-06	5,52296E-07	8,2354E-07	4,48924E-06	-2,19548E-06	-2,99034E-05	7,22971E-05	8,68518E-05	-1,05454E-05
S&P-500					1	2,35997E-05	2,16977E-06	-3,37931E-06	-4,06585E-07	3,74633E-07	-4,50833E-06	-4,8713E-06	-1,03473E-06	-1,05859E-05	2,06904E-06	1,36992E-05	7,38466E-06
Nasdaq-100						1	4,25113E-06	-4,82726E-06	-5,28819E-07	3,25093E-07	-1,26788E-06	-7,68965E-06	1,89873E-07	-1,50385E-05	1,37113E-05	3,23635E-05	1,46191E-05
HangSeng-50							1	6,83536E-07	-6,88916E-07	-1,93077E-06	1,09693E-05	5,09384E-06	-5,30702E-07	2,71564E-05	-1,66719E-05	9,0052E-06	8,25686E-06
Europe-50								1	-1,4876E-06	1,00321E-06	7,60717E-06	4,92888E-06	4,80946E-06	-2,35435E-05	4,41862E-06	-7,20851E-05	-5,384E-06
USD Index									1	-5,78685E-07	1,41354E-06	-2,90057E-06	-1,70847E-06	2,43186E-05	-1,88079E-05	3,88896E-05	3,15749E-06
Euro Index										1	-3,58043E-06	2,3483E-06	1,90352E-06	-9,07431E-06	1,57309E-05	-3,02983E-05	4,07093E-07
Nvidia											1	0,000106245	8,77896E-05	-3,29421E-05	7,279E-05	0,000197369	6,82992E-05
Apple												1	6,14496E-05	-3,40484E-06	-5,478E-05	-5,31741E-05	4,43351E-06
Amazon													1	1,44525E-05	7,97532E-05	-9,28721E-05	-1,66816E-06
Ethereum														1	0,003065508	0,003890858	3,17056E-05
XRP															1	0,003924067	0,000103663
EOS																1	2,2916E-05
3m. US Tr. Bills																	1

Pearson R	*Bitcoin*	*Crude Oil*	*Palladium*	*Gold*	*S&P-500*	*Nasdaq-100*	*HangSeng-50*	*Europe-50*	*USD Index*	*Euro Index*	*Nvidia*	*Apple*	*Amazon*	*Ethereum*	*XRP*	*EOS*	*3m. US Tr. Bills*
Bitcoin	1	0,066564082	0,053812595	0,014353965	0,022904807	0,099314655	-0,014918267	-0,046216381	0,125509258	0,031761579	0,018899248	0,046687878	0,014611512	0,018790078	-0,008719642	0,004379857	0,067146783
Crude Oil		1	0,010488737	0,109481161	-0,024301143	0,056923762	0,030404850	0,037192346	0,020585316	-0,078311539	0,118666146	0,045685537	0,074889551	0,078980109	0,177003569	0,167342224	-0,035157223
Palladium			1	-0,022876742	0,069178201	0,080566194	-0,129589419	-0,074090234	-0,047703165	0,075388549	0,143560340	0,195519744	0,184620502	-0,109112531	0,006422529	-0,077517681	0,094388290
Gold				1	-0,029971187	-0,043821121	0,113845928	-0,064213915	0,045577496	0,026932936	0,004594093	0,059331809	-0,031615234	-0,069054960	0,110962149	0,128023414	-0,065262954
S&P-500					1	0,822601677	0,072453804	-0,147020810	-0,025043422	0,027987810	-0,038528506	-0,098630195	-0,022826835	-0,037450267	0,004864894	0,030935392	0,070014182
Nasdaq-100						1	0,094616513	-0,139980352	-0,021710279	0,016187740	-0,007222061	-0,103773825	0,002791868	-0,035460706	0,021488175	0,048711586	0,092382638
HangSeng-50							1	0,018988552	-0,027094948	-0,092102663	0,059858616	0,065855233	-0,007475625	0,061344714	-0,025030471	0,012984791	0,049986233
Europe-50								1	-0,076227575	0,062350482	0,054084469	0,083022700	0,088266652	-0,069291687	0,008643218	-0,135422512	-0,042466278
USD Index									1	-0,050919012	0,014228209	-0,069170888	-0,044391396	0,101330482	-0,052085861	0,103435788	0,035259265
Euro Index										1	-0,043711649	0,067922649	0,059988827	-0,045860096	0,052839060	-0,097740744	0,005513718
Nvidia											1	0,351537158	0,316489455	-0,019044798	0,027968902	0,072834956	0,105820525
Apple												1	0,524848984	-0,004663597	-0,049868394	-0,046490019	0,016274253
Amazon													1	0,021568431	0,079104842	-0,088470144	-0,006671803
Ethereum														1	0,487602614	0,594382060	0,020335275
XRP															1	0,398415150	0,044189158
EOS																1	0,009381869
3m. US Tr. Bills																	1

Πίνακας 18: Αποτελέσματα μελέτης συσχετίσεων (εξάμηνο πτώσης)

Συνδιακυμάνσεις	Bitcoin	Crude Oil	Palladium	Gold	S&P-500	Nasdaq-100	HangSeng-50	Europe-50	USD Index	Euro Index	Nvidia	Apple	Amazon	Ethereum	XRP	Bitcoin Cash	EOS	3m. US Tr. Bill
Bitcoin	1	-3,04651E-05	-1,96983E-05	-9,97936E-06	3,21645E-05	-1,12756E-05	-2,55400E-05	1,73324E-05	-9,63539E-06	3,49748E-06	-1,25975E-04	-3,48645E-05	-4,33720E-06	1,21449E-04	6,12117E-05	3,83138E-04	-6,99592E-05	-1,32715E-04
Crude Oil		1	-7,97546E-06	-1,17986E-05	5,19304E-06	9,60609E-06	3,54794E-06	-8,06490E-07	-2,77073E-06	8,81824E-08	1,27674E-05	-2,51891E-05	-6,21983E-06	-9,60679E-06	-3,86901E-05	-5,12457E-05	-6,74967E-05	6,46604E-06
Palladium			1	8,06606E-06	1,29331E-06	1,80937E-06	6,04581E-06	1,45088E-05	-1,44306E-06	-1,86894E-07	1,40368E-05	9,29856E-06	-1,19720E-05	-2,06678E-05	-2,10918E-05	-2,45177E-05	-5,94821E-05	1,74263E-05
Gold				1	-1,63763E-06	3,51483E-07	1,00642E-06	5,48971E-06	1,45134E-06	-1,38178E-07	1,95956E-05	7,16976E-06	7,62684E-06	-8,36076E-08	-1,12336E-06	-2,59092E-05	1,47900E-05	-1,31045E-05
S&P-500					1	9,48186E-05	-4,94984E-07	-2,55158E-06	-4,29313E-06	1,67167E-07	-3,03913E-05	-9,80349E-06	-5,26016E-07	2,47155E-05	5,36140E-05	1,17301E-04	2,44645E-06	-1,24400E-05
Nasdaq-100						1	-5,79016E-07	-4,33533E-06	-2,55989E-06	1,37060E-07	-2,92685E-05	-4,97075E-06	1,98633E-06	-1,65961E-05	2,77604E-05	8,70145E-05	-3,08819E-05	-1,43400E-05
HangSeng-50							1	-4,80146E-06	3,85857E-07	8,05687E-07	1,77179E-05	-6,41756E-06	3,05414E-07	3,05534E-05	7,37369E-06	8,67317E-05	8,24941E-05	1,61243E-05
Europe-50								1	-1,28737E-06	-1,14743E-06	-5,04062E-07	9,26083E-06	-6,58274E-06	4,17593E-05	2,03844E-05	2,00444E-05	-2,65377E-05	-1,11747E-05
USD Index									1	6,24111E-07	2,60551E-06	1,12911E-06	-2,07203E-06	-1,82273E-05	9,39445E-07	-2,36394E-06	-1,60133E-05	-4,92221E-06
Euro Index										1	-2,85758E-06	6,31621E-06	1,49310E-06	-7,31752E-07	3,27449E-06	2,30643E-05	1,80852E-05	-5,18211E-06
Nvidia											1	0,000182931	0,000251649	-0,000112151	-0,000061571	-0,000327338	-0,000199567	0,000020475
Apple												1	0,000130271	0,000030787	0,000060635	-0,000037639	-0,000034444	0,000017851
Amazon													1	-2,45279E-05	1,02763E-04	-1,08849E-04	-9,96389E-05	1,14060E-05
Ethereum														1	0,003382225	0,003618675	0,003788159	0,000134928
XRP															1	0,003938852	0,004332190	0,000145963
Bitcoin Cash																1	0,004736472	0,000105173
EOS																	1	0,000262662
3m. US Tr. Bill																		1

Pearson R	Bitcoin	Crude Oil	Palladium	Gold	S&P-500	Nasdaq-100	HangSeng-50	Europe-50	USD Index	Euro Index	Nvidia	Apple	Amazon	Ethereum	XRP	Bitcoin Cash	EOS	3m. US Tr. Bill
Bitcoin	1	-0,038963134	-0,026690790	-0,036180540	0,072277005	-0,019633302	-0,044512704	0,048007219	-0,051427220	0,025125497	-0,106038109	-0,049014540	-0,004740722	0,041667931	0,017517993	0,101216851	-0,015127119	-0,161092451
Crude Oil		1	-0,034417955	-0,136237977	0,037165536	0,053271686	0,019694072	-0,007114484	-0,047099289	0,002017611	0,034227812	-0,112784422	-0,021652568	-0,010497423	-0,035265170	-0,043117277	-0,046482579	0,024997092
Palladium			1	0,098675950	0,009806277	0,010630628	0,035554558	0,135599327	-0,025988852	-0,004530342	0,039867978	0,044109682	-0,044154800	-0,023926596	-0,020367604	-0,021855221	-0,043398536	0,071373753
Gold				1	-0,033224252	0,005525544	0,015836452	0,137282337	0,069937696	-0,008962226	0,148920855	0,091004478	0,075265503	-0,000258983	-0,002902583	-0,061797279	0,028873289	-0,143612329
S&P-500					1	0,923877415	-0,004827487	-0,039548028	-0,128222676	0,006720109	-0,143151341	-0,077123880	-0,003217368	0,047451007	0,085860838	0,173407682	0,002960161	-0,084497334
Nasdaq-100						1	-0,004375740	-0,052067684	-0,059243796	0,004269400	-0,106825938	-0,030301286	0,009414229	-0,024689560	0,034448788	0,099675341	-0,028954286	-0,075474550
HangSeng-50							1	-0,057720388	0,008938351	0,025120784	0,064729029	-0,039157839	0,001448878	0,045496220	0,009158874	0,099445092	0,077418015	0,084946131
Europe-50								1	-0,047393582	-0,056856440	-0,002926545	0,089801409	-0,049628771	0,098822002	0,040238337	0,036524450	-0,039579219	-0,093558309
USD Index									1	0,059592148	0,029150155	0,021098246	-0,030102278	-0,083118754	0,003573466	-0,008300483	-0,046021420	-0,079411512
Euro Index										1	-0,043030926	0,158855061	0,029196242	-0,004491339	0,016764738	0,109003902	0,069958285	-0,112529145
Nvidia											1	0,539078052	0,576572613	-0,080655635	-0,036935908	-0,181266756	-0,090452949	0,052094937
Apple												1	0,498501640	0,036980052	0,060751606	-0,034811798	-0,026074449	0,075856714
Amazon													1	-0,022905888	0,080050393	-0,078271149	-0,058643470	0,037684970
Ethereum														1	0,826998920	0,816771236	0,699829945	0,139929556
XRP															1	0,741586454	0,667595108	0,126267355
Bitcoin Cash																1	0,673765933	0,083985346
EOS																	1	0,171675454
3m. US Tr. Bill																		1



Εικόνα 18: Διάγραμμα μεταβολών απόδοσης Bitcoin και USA EPU

Πίνακας 19: Πίνακας συσχετίσεων ανεξάρτητων μεταβλητών μοντέλου

Συνδιακυμάνσεις	*Palladium*	*S&P 500*	*3m USA Tr. Bill*	*Euro Index*	*Nvidia*	*Crude Oil*
Palladium	1	7,60040E-07	-7,92230E-05	1,28353E-06	1,81882E-05	9,42009E-06
S&P 500		1	-7,87029E-06	7,24175E-07	-8,61352E-06	8,70307E-06
3m USA Tr. Bill			1	1,46708E-05	-4,25427E-05	-1,52274E-04
Euro Index				1	-7,36109E-07	-1,45657E-06
Nvidia					1	-1,10335E-05
Crude Oil						1
Pearson's R	*Palladium*	*S&P 500*	*3m USA Tr. Bill*	*Euro Index*	*Nvidia*	*Crude Oil*
Palladium	1	0,005083829	-0,018260343	0,020530319	0,047829953	0,027421025
S&P 500		1	-0,003287860	0,020994200	-0,041054093	0,045916277
3m USA Tr. Bill			1	0,014655936	-0,006987225	-0,027683545
Euro Index				1	-0,008389856	-0,018376509
Nvidia					1	-0,022885631
Crude Oil						1